iOS 6 Education
Deployment Guide

First edition

Micah Baker
Senior Consulting Engineer
Apple Education

Dan Semaya
Senior Consulting Engineer
Apple Education

Tommy Hann
Senior Consulting Engineer
Apple Education

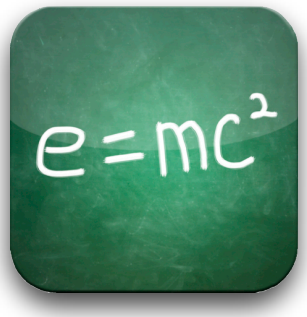
Stephen Cervera
Manager, National Consulting Engineers
Apple Education

Al Tufts
Director, Field Engineering
Apple Education

L521437A-en_AU

Contents

iOS in Education



Learn how to deploy and support iOS devices in an education environment.

This guide is designed for those responsible for deploying iOS devices in education, from IT leaders to implementers. It highlights best practices and considerations relevant to deploying and supporting iOS devices in education environments.

Note: Curriculum design is outside the scope of this document.

It's important to develop and communicate a plan before you deploy iOS devices in an education setting. Early design decisions, both good and bad, are amplified as a deployment is scaled up. The planning process should include curriculum and technology leaders, as well as those who will implement the deployment. A well-planned iOS deployment should incorporate the following steps and questions:

1. Understand the deployment goals.
   - What are the expected outcomes?
2. Assess the infrastructure.
   - Can the Local Area Network (LAN) and Wi-Fi network support a large number and high density of devices?
   - Review server and storage design (local or hosted).
   - Review Apple Configurator station design.
   - Evaluate Internet bandwidth.
3. Plan for support.
   - Who will provide project management support?
   - Who will be responsible for post-deployment support?
   - Will Apple provide professional development for implementers?
4. Plan the rollout.
   - What policies need to be created or revised?
   - Who will get devices and in what order will they be distributed?
   - Will Apple provide professional development for instructors and administrators?
   - What is the training plan for students?
   - Who will be authorised to purchase apps?
   - What data needs to be backed up from iOS devices and how will it be backed up?
   - Which deployment strategies will be used?
   - Will a professional services organisation execute the rollout?
   - Enrol in the Volume Purchase Program.
   - Consider a Mobile Device Management (MDM) solution.
   - Download and use Apple Configurator.
5. Complete the purchase.
   - Order the iOS devices, accessories and related equipment.
   - Purchase apps in volume using the Volume Purchase Program.

6. Prepare for the rollout.
   - Prepare a secure space for unpacking devices, activating them, and completing the initial sync.
   - Set up configuration stations, storage/charging carts and iOS devices.
7. Perform the initial rollout.
   - Deploy to initial sites.
   - Verify the deployment model.
8. Communicate with stakeholders (school leaders, governing bodies, community members and so on).
   - Describe and explain the deployment plan.
   - Reiterate expected outcomes.
9. Scale up the deployment.
   - Expand to remaining sites according to best practices.
10. Verify.
    - Collect data and verify deployment fidelity.

This document focuses on the technical aspects of the steps listed above. Many curriculum-focused resources are available to help in designing classroom workflows for iOS devices.

- Learn more about iPad in education: www.apple.com/au/education/ipad
- Learn more about iPod touch and iPhone in education: www.apple.com/au/education/ipodtouch-iphone
- Find education resources, video tutorials and other guides: www.apple.com/au/education/resources

System Requirements

The following information tells you about the operating system versions and related software that you will need to follow the recommendations in this document.

iPhone, iPad and iPod touch

- Learn more about iPhone specifications: www.apple.com/au/iphone/specs.html
- Learn more about iPad specifications: www.apple.com/au/ipad/specs
- Learn more about iPod touch specifications: www.apple.com/au/ipodtouch/specs.html
- Learn more about Apple TV system specifications: www.apple.com/au/appletv/specs.html
- Learn more about the latest version of iOS: www.apple.com/au/ios

Apple Configurator

- Learn more about Apple Configurator system requirements: itunes.apple.com/au/app/apple-configurator/id434433123?mt=12

iTunes

- Learn more about iTunes system requirements: www.apple.com/au/itunes/download

OS X

- Learn more about OS X system requirements: www.apple.com/au/macosx/specs.html
- Learn more about OS X Server system requirements: www.apple.com/au/macosx/server/specs.html

Preparing for Deployment

Being prepared prior to deployment can help facilitate a smooth rollout. This chapter discusses key preparation options.

Preparing a staging area

Before any equipment arrives, it is helpful to reserve and prepare an appropriate workspace for the deployment. Devices may need to be configured and an inventory taken before the devices are delivered to end-users, so consider designating a secure location with adequate power and networking support for equipment.

Understanding firewall requirements

Confirm that the appropriate firewall ports are open before proceeding with the tasks discussed in this guide. It is also useful to understand what ports iTunes and iOS devices use for various services.

- Learn about well-known Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports used by Apple devices: support.apple.com/kb/TS1629
- Learn about Apple TV firewall requirements: support.apple.com/kb/HT2463

Discovering apps for learning

Consider researching what kinds of apps may be used before the devices arrive, to encourage a more efficient deployment process. Instructors new to iOS may appreciate having a starting point as they choose an app for a specific content area.

- Learn about great learning apps: www.apple.com/au/education/apps

Contacting Apple

To learn more about Apple in education, visit www.apple.com/au/education or call 1300-551-927 to speak to an Apple education representative.

AppleCare

AppleCare products are available for institutions of every size.

AppleCare Options for iPhone, iPad and iPod touch

Every iPhone, iPad and iPod touch comes with complimentary telephone technical support for 90 days from the purchase date, and a one-year limited warranty. The service coverage can be extended to two years from the original purchase date with AppleCare Protection Plan for iPhone, AppleCare Protection Plan for iPad or AppleCare Protection Plan for iPod touch. You can call Apple's technical support experts as often as you like to get questions answered, and there are convenient service options if you need repairs.

- Learn more about AppleCare for iPhone: www.apple.com/au/support/products/iphone.html
- Learn more about AppleCare for iPad: www.apple.com/au/support/products/ipad.html
- Learn more about AppleCare Protection Plan for iPod touch or Apple TV: www.apple.com/au/support/products/ipod.html

AppleCare iOS Direct Service Program

A benefit of AppleCare Protection Plan, the iOS Direct Service Program screens the units for any hardware faults; directly orders a replacement iPhone, iPad, iPod touch or in-box accessory if necessary; and exchanges it for the failed item at the service location. This saves organisations time and expense. The program is open to businesses, enterprise organisations, education institutions, and state or local government agencies.

- Learn more about the iOS Direct Service Program: www.apple.com/au/support/programs/ids

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 issues, allowing institutions to manage resources more efficiently, improve response time and reduce training costs. AppleCare Help Desk Support covers an unlimited number of support incidents for hardware and software diagnosis, troubleshooting and issue isolation, for Apple-based solutions such as iPhone, iPad, iPod touch, iPhone Configuration Utility and iOS.

- Learn more about AppleCare Help Desk Support: www.apple.com/support/products/enterprise/help.html

AppleCare OS Support

AppleCare OS Support includes AppleCare Help Desk Support in addition to enterprise-level incident support—defined as 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 the command-line tools.

- Learn more about AppleCare OS Support: www.apple.com/support/products/enterprise/server.html

Learn More

- For more information about AppleCare, see the *Contacting Apple* section of this guide.

Apple factory services

Before iOS devices are shipped, certain work can be completed at the factory. This can include placing asset tags on devices, or adding text or logo laser engraving on the back of each device.

Learn more

- For more information about Apple factory service options, see the *Contacting Apple* section of this guide.

Apple Professional Development

Apple offers onsite, hands-on workshops tailored to your school or institution's specific needs. These workshops are designed to help you use your Apple products to transform teaching and learning.

All Apple Professional Development Specialists are current or former educators, which gives them a personal understanding of teaching and learning with technology. Because they know what's important in the curriculum, they can ensure that you learn about your Apple products and how they can best serve you and your students.

- Workshops are hands-on and address a wide range of teaching and learning needs.
- All workshops are presented in a context that models technology implementation in a wide variety of curricular styles.
- Offerings are selected depending on faculty needs and participants' prerequisite skills.
- Workshops accommodate 20 participants.

Available workshops

Apple Professional Development workshops are offered in three categories:

- **Foundations**

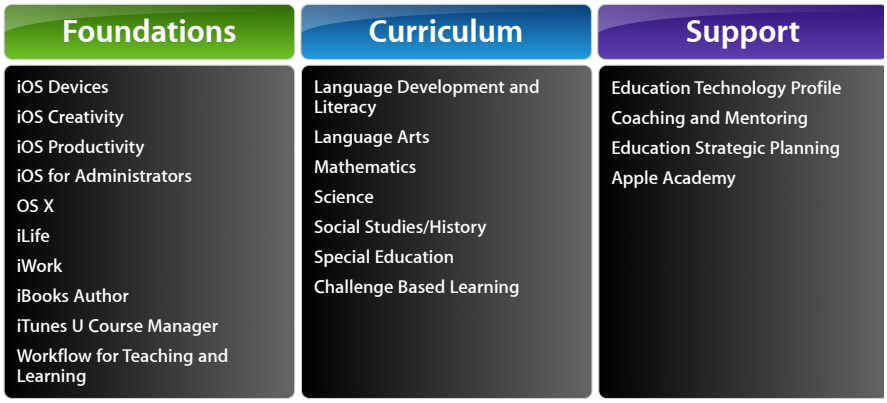
  Focused on basic technology skills, these foundational workshops help teachers become confident and comfortable integrating Apple products into their teaching strategies.

- **Curriculum**

  These workshops focus on curriculum and content design, and instruction using all Apple products.

- **Support**

  These offerings support teachers and administrators in planning technology deployments, and building capacity.



Learn more

- For more information about Apple Professional Development, see the *Contacting Apple* section of this guide.

Wi-Fi Design

When preparing the Wi-Fi infrastructure for an iOS deployment, there are several factors to consider, including:

- the required coverage area
- the number and density of devices that will be using the Wi-Fi network
- the types of devices and their Wi-Fi capabilities
- the types and amount of data being transferred
- security requirements for accessing the wireless network
- encryption requirements for data passing over the air.

Although this list is not exhaustive, it represents some of the most relevant Wi-Fi network design factors.

This chapter may be helpful for network administrators who are responsible for their own deployments, and it may help facilitate discussions with Wi-Fi vendors to ensure an optimal Wi-Fi network design.

Reminder: This chapter focuses on Wi-Fi network design in the United States. These design factors may differ in other countries.

Planning for coverage and density

Although it is critical to provide Wi-Fi coverage where iOS devices will be used, it is also essential to plan for the density of devices in a given area.

Most modern, enterprise-class access points are capable of handling up to 50 Wi-Fi clients (users), although the user experience would likely be disappointing if a single access point had that many devices associated to it. The experience on each device depends on the available wireless bandwidth on the channel being used, and the number of devices sharing the overall bandwidth. As more and more devices use the same access point, the relative network speed for those devices decreases. You should consider the expected usage pattern of the iOS devices as part of your Wi-Fi network design.

Designing for coverage

To illustrate, consider the following scenario of a district office building with 10 large offices and a conference room on each floor. Fifty employees equipped with MacBook Pro, iPad, and iPhone 4S or iPhone 5 are spread out over two stories. The MacBook Pro notebooks are plugged into Ethernet ports when not mobile, while iPad and iPhone devices frequently change locations.

The physical layout of the building encourages informal communication and collaboration. Employees may meet with other employees in conference rooms or in offices. As a result, employees move around the building with iPad and iPhone devices throughout the day, and some employees bring their MacBook Pro with them. The majority of network access comes from checking email and calendars, and browsing the Internet.

In this scenario, Wi-Fi coverage is the highest priority. These mobile users aren't likely to be transferring large amounts of data over the network very often, and the overall density of Wi-Fi devices is somewhat low. A Wi-Fi design could include two or three access points on each floor to provide coverage for the offices, and one access point in each conference room. The MacBook Pro notebooks and iPad devices both support 802.11n at 5GHz, so the access points could be configured for 802.11n at 5GHz. HD40 can be enabled to increase the throughput of MacBook Pro notebooks on the network.

- Learn more about Wi-Fi standards support, including specifications for Apple products, in *Appendix A—Wi-Fi Standards* at the end of this guide.

Remember than in this scenario, some employees use iPhone 4S while others use iPhone 5, so a 2.4GHz network must also be available for the iPhone 4S devices. iPhone 5 prefers the 5GHz network. Because most modern access points support simultaneous dual frequencies, support for both 2.4GHz and 5GHz networks could be enabled. iPhone 4 supports 802.11n, but if other mobile devices don't support 802.11n, 802.11b/g may also need to be enabled.

Designing for density

Compare the district office scenario above with a high school that has 1,000 students and 30 teachers in a two-storey building. Every student has been issued an iPad, and every teacher has been issued a MacBook Air and an iPad. Each classroom holds approximately 35 students and classrooms are adjacent to each other. Throughout the day, students conduct research on the Internet, watch curriculum videos, and copy files to and from a file server on the LAN.

The Wi-Fi network design for this scenario is more complex due to the higher density of mobile devices. Because each classroom has approximately 35 students using iPad devices at any given time during the school day, one access point per classroom could be deployed. Multiple access points should be considered for the common areas to provide adequate coverage. The actual number of access points for the common areas would vary, depending on the density of Wi-Fi devices in those spaces.

iPad is the most common device used in this school, so special attention should be given to that device's technical specifications. iPad supports 802.11n at both 2.4GHz and 5GHz, so the access points throughout the school should be configured for 802.11n at 5GHz. However, in this high-density deployment, in which the majority of devices do not support channel bonding, it may be best to leave channel bonding disabled. This allows for the deployment of more access points without reusing the same channel in nearby locations. With channel bonding enabled (each access point uses two channels), fewer total channels are available.

- Learn more about Wi-Fi standards support, including specifications for Apple products, in *Appendix A—Wi-Fi Standards* at the end of this guide.

If devices that only support the 802.11b or 802.11g standards need to participate in the network, the above design could be modified slightly. One option is to simply enable 802.11g/b if dual-band access points are being deployed. Another option is to provision one Service Set Identifier (SSID—or network identity) using 802.11n at 5GHz for newer devices, and a second SSID at 2.4GHz to support 802.11b and 802.11g devices. However, care should be taken to avoid creating too many SSIDs.

In both scenarios, avoid using hidden SSIDs. It is harder for a Wi-Fi device to rejoin a hidden SSID than a broadcast SSID, and there's very little security benefit in hiding the SSID. Users tend to frequently change location along with their iOS devices, so hidden SSIDs may delay network association time.

- Learn more about Wi-Fi security in *Appendix B—Wireless Security* at the end of this guide.

Note that the above network designs are hypothetical examples. The actual design for an education environment will vary depending on the unique characteristics of the building, user workflows, the specific Wi-Fi devices, security considerations and other factors. Collaborate with a Wi-Fi infrastructure provider to ensure an optimal design.

Mobile carts

Mobile carts can make it easier to manage iPad devices for a whole classroom. Common carts can store, charge and sync up to 30 iPad devices and also have room for a MacBook computer. A cart rolls easily around the school so multiple classes can use it, and it can be locked to secure the devices when they're not in use. This means that instead of students visiting a lab, the lab is brought into the classroom.

Providing Wi-Fi for mobile carts can be more complex, depending on the infrastructure that already exists. There are two ways to design a Wi-Fi network for mobile learning labs: mounting fixed access points to handle the devices wherever they go, or providing an access point that stays with the cart.

Determine in which classrooms or other areas these mobile labs will be used. When designing a fixed Wi-Fi infrastructure for carts, design for both coverage and density to support the number of devices that may be brought into each of those areas. This may mean having an access point per classroom or designated usage area.

If there isn't an existing Wi-Fi infrastructure or there isn't coverage in the designated areas, an access point may be installed on the cart, assuming an Ethernet port is available near the cart. This means that Wi-Fi is always be available where the cart and devices are used.

Installing an access point on every cart can be a challenge if a fixed Wi-Fi infrastructure already exists. A well-designed Wi-Fi infrastructure will have channel usage balanced so that access points in close proximity don't interfere with each other. Transmit power settings will also be configured to minimise overlapping of coverage areas.

If a cart with an access point is moved into an area that is already covered by the fixed Wi-Fi infrastructure, it could cause significant interference in that area, especially if the 2.4GHz frequency is used on both the cart and fixed access points. If the existing Wi-Fi infrastructure operates exclusively on the 2.4GHz frequency, the access point on the cart should be configured to use the 5GHz frequency exclusively to avoid interference.

Consult a Wi-Fi network provider to determine the best Wi-Fi coverage strategy for mobile carts.

Similar challenges arise if users install their own access points. These access points may compete for channels with the fixed Wi-Fi infrastructure.

AirPlay, AirPrint and Bonjour

If AirPlay, AirPrint or iTunes Wi-Fi Sync will be used as part of an iOS deployment, ensure that the Wi-Fi network design supports Bonjour traffic. These services use Bonjour for automatic discovery, which requires communicating devices to be on a single subnet with broadcast traffic enabled.

- Learn more about supporting Bonjour on Wi-Fi networks in *Appendix C—Supporting Bonjour* at the end of this guide.
- Learn more about AirPlay: support.apple.com/kb/HT4437
- Learn more about AirPlay Mirroring: support.apple.com/kb/TS4085
- Learn more about AirPrint: support.apple.com/kb/ht4356

Configuration and Management

There are multiple ways to configure and manage iOS devices including doing so manually on the device, using configuration profiles, using a Mobile Device Management (MDM) solution, using Apple Configurator or using Exchange ActiveSync.

Manual configuration

Restrictions and configuration information can be set directly on each iOS device. This is the simplest configuration method but is more labour intensive, which may make it optimal for small deployments or in self-service scenarios.

Certain restrictions can only be set directly on the device in the Restrictions pane of the Settings app, including the ability to change accounts for iCloud, Mail, Contacts and Calendars; the ability to toggle location services; and the ability to make changes to Find My Friends.

Changes to restrictions set directly on an iOS device are protected by a four-digit restrictions passcode that is independent of the device lock passcode used to prevent unauthorised access to the device. The restrictions passcode can only be set or changed directly on the device.

- Learn more about device restrictions: support.apple.com/kb/HT4213

Configuration profiles

Configuration profiles are XML files that contain device passcode policies, restrictions, account and networking settings, Web Clips, credentials and other settings that permit iPhone, iPad and iPod touch to work with enterprise systems. You can choose to lock configuration profiles so that end-users can't remove them without restoring the device. Configuration profiles can be distributed via the Internet or email, or can be installed over USB using iPhone Configuration Utility or Apple Configurator.

- Learn more about configuration profiles: developer.apple.com/library/ios/featuredarticles/iPhoneConfigurationProfileRef

Configuring accounts and credentials

Configuration profiles can install account and configuration information for use with Exchange ActiveSync; IMAP, POP and SMTP email; CalDAV calendar services and subscribed calendars; CardDAV and LDAP address book services; Wi-Fi networks; and VPN services. Profiles may include account settings as well as credentials for the account.

If a profile that does not include credentials is installed manually on the device, the user is prompted for a password. If a profile that does not include credentials is installed silently via MDM or Apple Configurator, the user is not prompted to enter credentials. Consider directing users to manually download a configuration profile for these account settings. If using Microsoft Exchange, configure the Exchange environment for Autodiscover so that users only need to enter an email address and password to configure services without a profile.

Configuring restrictions

Institutions can prevent users from downloading and using unauthorised apps by enabling the Installing Apps restriction. This restriction also prevents syncing or updating apps in iTunes and must be removed to allow users to install new or updated apps.

Additional restrictions are available to restrict access to device features such as Camera, FaceTime, Siri and more.

- Learn more about restrictions: http://support.apple.com/kb/HT4213

Web Clips

A Web Clip is an icon on the device Home screen that links to a website. Web Clips can optionally launch full-screen web apps and can run offline using HTML 5 local storage.

Configuration profiles can include Web Clips that use a customised title and icon and may be set to be non-removable. Consider including a Web Clip in a large deployment to facilitate future management and configuration of devices. You can use Web Clips to easily direct users to future deployment information, such as new configuration profiles, recommended App Store apps and enrolment in an MDM solution.

- Learn more about Web Clips: www.apple.com/webapps/whatarewebapps.html

iPhone Configuration Utility

iPhone Configuration Utility (iPCU) allows institutions to easily create, maintain, encrypt and install configuration profiles and in-house apps on Mac and Windows. You can also use it to capture device information, including console logs.

- Learn how to use iPhone Configuration Utility: developer.apple.com/library/ios/#featuredarticles/FA_iPhone_Configuration_Utility/Introduction/Introduction.html

Mobile Device Management

MDM gives education institutions the ability to securely enrol devices in an enterprise environment, wirelessly configure and update settings, monitor institution policy compliance, deploy apps, and remotely wipe or lock managed devices. MDM solutions are provided by third parties, offering support for a variety of server platforms, as well as management consoles, additional features and pricing structures. Evaluate which aspects of MDM solutions are most relevant to your organisation before you choose a solution.

- Learn more about Mobile Device Management: www.apple.com/iphone/business/integration/mdm

Requirements

MDM requires devices running iOS 4 and later. Some features only work with specific versions of iOS or require the use of Apple Configurator.

Enrol

Enrolling devices enables cataloguing and asset management. The enrolment process leverages Simple Certificate Enrolment Protocol (SCEP) so iOS devices can perform over-the-air enrolment of identity certificates for authentication to institution services.

Users can opt in or out of MDM enrolment. Institutions should consider incentives for users to remain enrolled in MDM. For example, you can require MDM enrolment for Wi-Fi network access by using the MDM solution to automatically provide the wireless credentials. When a user un-enrols from MDM, the device attempts to notify the MDM server.

Configure

Once a device is enrolled, the MDM server can be dynamically configured with settings and policies. The MDM server accomplishes this by sending configuration profiles to the device, which are then installed silently without the user's intervention.

When combined with enrolment, device configuration provides assurance that only trusted users are accessing institution services and that devices comply with established policies. Configuration profiles can be signed, encrypted and locked, preventing the settings from being altered or shared. This means that if users want to remove management settings, they must opt out of the MDM solution and lose access to the institution's network resources.

Query

An MDM server has the ability to query devices for a variety of information. This includes hardware information such as the serial number, unique device ID (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.

Wipe, lock, clear passcode

When a device is managed, it can be administered by the MDM server through a set of specific actions. Management tasks include changing configuration settings, remotely wiping a device and clearing a passcode lock. Clearing a passcode can be useful in instances where one user creates a passcode on another user's device or if a user forgets his or her passcode.

Managed apps

MDM servers can deploy both App Store app codes and in-house enterprise apps to devices over the air. Paid apps require the Volume Purchase Program.

Deploying Volume Purchase Program app codes with MDM requires the end-user to enter their Apple ID credentials, which means it is ideally suited for deployments where the end-users will permanently own the purchased applications.

Apps deployed from an MDM server can be removed remotely by the server or when the user un-enrols from MDM, along with the data associated with each app. If the app was downloaded using a personal Apple ID then the end-user can download it again from the App Store. Managed apps can be prevented from backing up data to iCloud or iTunes, preventing the data for that app from being recovered if the app is removed and reinstalled.

Apple Push Notification Service

All MDM solutions use the Apple Push Notification Service (APNS) to maintain persistent communication with devices across both public and private networks.

Learn more about APNS:
support.apple.com/kb/HT3576

Learn more about required firewall ports for APNS and other services in the *Understanding Firewall Requirements* section of this guide.

MDM certificates

MDM requires multiple certificates to operate, including an APNS certificate to talk to clients and an SSL certificate to communicate securely. MDM solutions may also sign profiles with a certificate.

Certificates must be renewed from time to time. Most certificates, including an APNS certificate, must be renewed annually. When a certificate expires an MDM server can not communicate with clients until the certificate is updated. Be prepared to update all MDM certificates before they expire.

Profile Manager

OS X Server includes Profile Manager, a server-based solution for remotely managing iOS devices running iOS 4 or later, and Mac systems running OS X Lion or later. Profile Manager makes it easier to create configuration profiles, enforce restrictions through MDM and deploy iOS apps.

Profile Manager also gives users access to a self-service web portal where they can download and install new configuration profiles. Users can use this web portal to perform tasks such as clearing passcodes and remotely locking or wiping devices that are lost or stolen.

OS X Server is available from the Mac App Store and can be used to transform a Mac running OS X into a Server. It is also available preinstalled on a Mac mini or Mac Pro. You don't need to purchase or maintain client licences to use the features of OS X Server, which makes Profile Manager the simplest and fastest way to get started with MDM.

- Learn more about Profile Manager:
  www.apple.com/au/macosx/server
- Get help with Profile Manager:
  help.apple.com/profilemanager

Apple Configurator

Apple Configurator makes it easy to mass configure and deploy iPhone, iPad and iPod touch in a school, business or institution.

Three simple workflows let you prepare new iOS devices for immediate distribution, supervise devices that need to maintain a standard configuration, and assign devices to users. Apple Configurator lets you quickly configure and update 30 devices at a time so they have the latest version of iOS, as well as configure settings and install apps and data for your students, faculty or staff members.

Prepare

Apple Configurator can easily prepare up to 30 devices simultaneously, and many more if the devices are connected one at a time or in batches. In the preparation workflow, any device that is connected via USB to the Mac running Apple Configurator will be configured automatically. To prepare devices for use, Apple Configurator can supervise devices for greater control by the institution; update or restore devices with the latest version of iOS; restore multiple devices from a master template backup; name devices sequentially; and install configuration profiles and apps on devices.

Supervise

A supervised iOS device is owned by the institution. Supervision enables the institution to control additional aspects of the device beyond configuration profiles and restrictions. Supervised devices are prevented from syncing with iTunes on other computers, which helps prevent users from removing required apps. Apple Configurator silently deploys configuration profiles to supervised devices over USB, removing the need to tap the screen to complete installation. Upon reconnecting a supervised device to Apple Configurator, the device is automatically reconfigured back to a desired configuration including apps, configuration profiles and a custom lock screen.

Supervised devices are reconnected to Apple Configurator for app updates. Devices can be organised by group, allowing sets of devices to receive unique apps and management settings.

Supervision requires devices running iOS 5 or later. A device can only be supervised if it has not yet been configured or if it has been reset to factory defaults. Attempting to supervise a user's personally owned iOS device will erase the user's apps and content, and is not recommended.

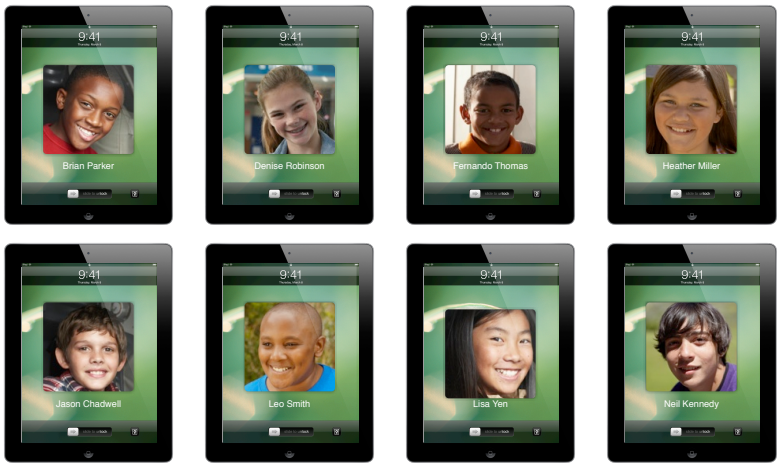
Additional settings and restrictions are available for supervised devices running iOS 6 or later. Once a device is supervised these restrictions can be configured via configuration profiles that are delivered through Apple Configurator, MDM or manual download. These restrictions include:

- Single App Mode — This locks the user into a single, specified application. If the device is powered down, the specified application will launch at startup. Consider using MDM to enable and disable this setting for dynamic control.
- Global Network Proxy for HTTP — This routes almost all web traffic on the device through a specified proxy server or setting. This setting is applied across all Wi-Fi SSIDs and cellular networks. Install this setting via Apple Configurator in a non-removable profile for the strongest enforcement. Consider using a proxy auto-configuration (PAC) file for greater flexibility with this setting.
- Allow Removing Apps — Disabling this setting prevents users from removing apps from the Home screen.

- Allow Use of Game Center — Disabling this setting removes the Game Center icon from the Home screen. Disable this setting in conjunction with disabling both Allow Multiplayer Gaming and Allow Adding Game Center Friends to completely disable Game Center on supervised devices.
- Allow iMessage — Disabling this setting removes Messages icon from the Home screen.
- Allow iBookstore — Disabling this setting prevents access to the iBookstore while allowing use of the iBooks app for reading books and PDFs.
- Allow iBookstore Sexually Explicit Content — Disabling this setting prevents access to adult content from the iBookstore.
- Allow Configuration Profiles Installation — Disabling this setting prevents users from manually installing configuration profiles directly on the device, which includes enrolling in an MDM server.

Assign

Apple Configurator can assign devices to individual users. Users can be created manually in Apple Configurator or imported from a directory service. Checking out a device to an assigned user loads the user's personal settings and data onto the device and can display the user's picture and name on the lock screen. Checking the device back in to Apple Configurator copies the user's personal settings and data onto the Mac running Apple Configurator so the user can check out another device in the future. Users can be created manually in Apple Configurator or imported from a directory service such as Open Directory or Active Directory. Instructors can distribute documents to multiple users and collect those documents. Only supervised devices can be assigned to users in Apple Configurator.



- The amount of time required to check out or check in devices depends on the amount of data consumed by each user. Test your planned assignment workflow before deploying. Assigning devices for long-term checkout, such as an entire school year, removes the need to schedule frequent checking in and out of devices. The use of this feature is not recommended for devices enrolled in an MDM server.

Installing apps with Apple Configurator

Apple Configurator can install in-house enterprise apps and App Store apps. Installing App Store apps with Apple Configurator works best with supervised devices that will exclusively use Apple Configurator for new apps and app updates. Installing paid apps with Apple Configurator works with supervised devices only.

Installing paid apps from the App Store requires redemption codes from the Volume Purchase Program for Education or Business. The Volume Purchase Program is not available in all regions.

Redemption codes for paid apps installed with Apple Configurator are redeemed using the institution's Apple ID. This results in multiple codes for the same app redeemed to one Apple ID, which is unique to Apple Configurator. Once Apple Configurator consumes these app codes the licences are managed locally. App licences can be transferred between devices by Apple Configurator. Apple Configurator will need to be backed up to preserve the licence database.

- Apple Configurator: Backing up and restoring data: support.apple.com/kb/HT5194
- Learn more about VPP app codes and Apple Configurator: support.apple.com/kb/HT5188

Apple Configurator is available for free in the Mac App Store.

Understanding USB

A wide variety of USB-based peripheral devices are available and many have unique power requirements. The USB ports on Apple computers and displays provide 500 mA (milliamps) at 5V (volts) to each port, regardless of whether the port is USB 1.1 or USB 2.0. This is in compliance with USB specifications.

Some Apple peripheral devices, including iPhone, iPad and iPod touch, may request more than 500 mA at 5V from a port, to function or to allow for faster charging.

- Learn more about powering USB peripherals: support.apple.com/kb/HT4049

The experience of syncing and charging multiple devices can vary depending on the USB hub selected. For best results consider products that have the Made for iPhone, Made for iPad, or Made for iPod logo. These logos mean that the accessory has been designed to connect specifically to iPhone, iPad or iPod touch and has been certified to meet Apple performance standards.

- Learn more about the Made for iPhone, Made for iPad, and Made for iPod logos: support.apple.com/kb/ht1665

Using Exchange ActiveSync

iOS devices can communicate directly with Microsoft Exchange Server via Microsoft Exchange ActiveSync (EAS), enabling push email, calendars, contacts and tasks. EAS also provides users with access to the Global Address List (GAL) and provides administrators with passcode policy enforcement and remote wipe capabilities. iOS supports both basic and certificate-based authentication for EAS. If EAS is already enabled, the necessary services are already in place to support iPhone and iPad with no additional configuration required.

- Learn more about Exchange ActiveSync on iOS: images.apple.com/au/iphone/business/docs/iOS_6_EAS_Sep12.pdf

Choosing management tools

An iOS deployment may utilise one or more configuration and management tools. Choose the appropriate tools based on your organisation's needs. Each toolset has unique aspects that may be valuable for a deployment, and some tools can work together.

For example, Apple Configurator can supervise devices owned by the institution, while MDM and Profile Manager offer over-the-air management of devices anywhere on the Internet. Apple Configurator can work with MDM by enabling the MDM server to configure supervised settings remotely.

Purchasing Content

Institutions, teachers and students can choose from a variety of methods for purchasing apps, books and iBooks textbooks. Education users, like all iTunes users, can use credit cards or gift cards to fund individual purchases. To purchase apps in volume, education institutions can use the Volume Purchase Program (VPP) and fund purchases using a credit card.

- Find some great learning apps: www.apple.com/au/education/apps

Credit cards and iTunes Gift Cards

Anyone in Australia aged 13 years or older can purchase apps, books and iBooks textbooks from the iTunes Store with a credit card or an iTunes Gift Card. iTunes Gift Cards are readily available in many retail locations. Credit cards and iTunes Gift Cards share a similar set of advantages and requirements.

Apps and books are purchased one at a time with either of these funding sources, and each can only be purchased once per iTunes account. The entire balance of a gift card must be used by one iTunes account and can't be shared with other iTunes accounts. Therefore, neither of these purchasing methods is appropriate for volume purchasing.

Examples of purchases funded by credit card may include school administrators using institutional credit cards to purchase apps or books for individual use, instructors purchasing apps or books for use only on their devices, or university students using personal credit cards to purchase apps or books that may be required for a particular course. Some institutions may choose to provide gift cards to instructors to allow them to experiment with new apps in the App Store before deciding to purchase in volume using the Volume Purchase Program.

Volume Purchase Program

The Volume Purchase Program (VPP) allows educational institutions to purchase iOS apps in volume and distribute them to students, teachers, administrators and employees (terms and conditions apply). The program also allows app developers to offer special pricing for purchases of 20 apps or more. K–12 and degree-granting higher education institutions in Australia, Canada, France, Germany, Italy, Japan, New Zealand, Spain, the United Kingdom and the United States qualify for participation in the Volume Purchase Program.

VPP Workflow

There are three roles involved in the VPP process: the Program Manager, the Program Facilitator and the end-user. These three roles allow for multiple purchasing and deployment workflows depending on the needs of the education institution.

Understanding program roles

Program Manager

A Volume Purchase Plan Program Manager is responsible for enrolling an institution in the program. They are also authorised by the educational institution to create and manage Program Facilitator accounts.

Program Facilitator

Program Facilitators can purchase apps at the VPP store using credit cards.

Program Facilitators can be anyone designated by the Program Manager — for example, deans, professors, researchers, principals, teachers, technology co-ordinators or instructional technologists. The role of Program Facilitator may go to the person already responsible for procuring software for the institution. The person serving as the Program Manager can also act in this role, although a separate Program Facilitator account is required.

The Program Manager creates a new Apple ID for each Program Facilitator to use exclusively within the VPP store. Existing Apple IDs can't be used within this store. A valid email address that is not currently used as an Apple ID needs to be provided to Apple for each Program Facilitator. This email address should be controlled by the education institution to ensure that the Program Facilitator account isn't tied to an individual.

End-user

For the purposes of the VPP, the end-user is any iTunes account used to redeem app licence codes.

For app purchases, education institutions have the option of redeeming one app code per iTunes-authorised computer, or 'configuration station', and retaining the rest of the codes as proof of purchase. For these configuration stations, the end-user iTunes account may be created using a school-controlled email address, and the configuration station administrator should be an authorised user. Note that Apple Configurator requires a valid VPP code for each copy of an app deployed to a device.

iTunes accounts can be created without a credit card, which may be useful for creating institutional iTunes accounts.

- Learn more about iTunes accounts in the *Understanding the Tools* section of this guide.

Enrolling in the Volume Purchase Program

Education institutions that qualify for enrolment in the VPP can sign up for the program online.

- Learn more about enrolling in the VPP: www.apple.com/au/education/volume-purchase-program

- Read frequently asked questions about the VPP: www.apple.com/au/education/volume-purchase-program/faq.html
- Access VPP support: http://www.apple.com/au/support/itunes/vpp-edu

Using the VPP

Only Program Facilitators can purchase apps through the VPP Store, but anyone can browse the store. This makes it easy for anyone to check pricing at any time, even if that person isn't designated as a Program Facilitator.

When purchasing, the Program Facilitator must enter a value in the quantity field. Following each purchase, the Program Facilitator receives a spreadsheet that includes a list of redemption codes that can be redeemed by end-users using iTunes. The Program Facilitator can download updated versions of the spreadsheet to review which codes have been redeemed.

- Browse the VPP Store: volume.itunes.apple.com

Volume pricing

Many app developers offer volume pricing on their titles sold through the VPP. If the developer has enabled volume pricing, education institutions receive 50 per cent off when purchasing 20 or more licences of an app. The volume pricing is applied per purchase, meaning that previous and future app purchases aren't taken into account.

Reminder: If possible, co-ordinate and consolidate app purchase requests to reach the volume pricing for 20 or more licences of an app.

Code distribution techniques

The education institution is responsible for distributing and redeeming codes. Codes can be distributed manually to users, emailed via a mail merge process or posted to an internal website such as a wiki. Organisations can create their own code distribution website to distribute codes to users. Some MDM solutions integrate VPP code redemption into their self-service client applications.

The spreadsheet of codes obtained from the VPP includes a URL for each unique code. Each URL includes the associated code and can serve as a shortcut for distributing app redemption codes to users. The URL structure is as follows:

https://buy.itunes.apple.com/WebObjects/MZFinance.woa/wa/freeProductCodeWizard?code=REDEMPTIONCODEHERE

Replace *REDEMPTIONCODEHERE* with the actual redemption code for the app.

These URLs can be used to obscure the code from the user when building a code distribution website or service, to create a more seamless integration process.

- Read the VPP frequently asked questions for examples: www.apple.com/au/education/volume-purchase-program/faq.html

Deployment Strategies

There are many ways to deploy iOS devices depending on the desired management outcomes. Before exploring deployment strategies it's important to understand the tools common to all deployment methods.

Understanding the tools

Apple IDs and iTunes accounts

An Apple ID is the login used for just about everything Apple offers, including using iCloud to store content, downloading apps from the App Store, and buying songs, movies and TV shows from the iTunes Store.

Each Apple ID must be created using a unique email address. Account design varies depending on the deployment strategy, and institutions may prefer iTunes Store accounts to be created without a credit card.

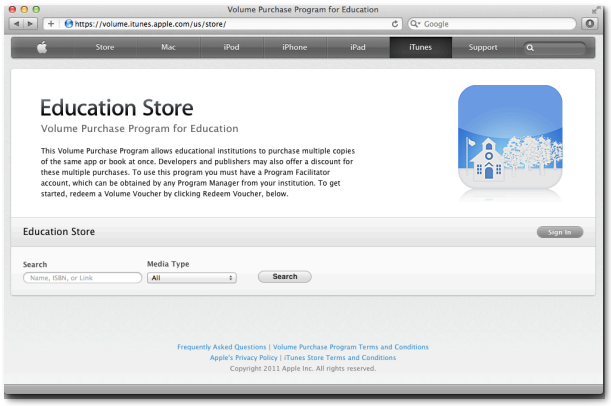
The email address used to create an iTunes Store account is the Apple ID, which allows access to all other Apple services. It isn't necessary to create a new account for each service — just use the same Apple ID.

If a rescue email address is set, all password reset emails will go to that address, not to the primary email address. Additionally, three security questions must be set when creating the account.

- Learn more about the rescue email address: support.apple.com/kb/HT5312

Note: You must be 13 years or older to create an Apple ID and access the iTunes Store in the US and many other countries.

- Learn more about Apple ID: www.apple.com/support/appleid
- Learn more about creating iTunes accounts without a credit card: support.apple.com/kb/HT2534



- Learn more about associating devices and computers with an Apple ID: support.apple.com/kb/HT4627

iTunes account passwords should be closely guarded to prevent unauthorised use. Institution-owned iTunes account passwords should not be shared with end-users.

- Learn more about protecting iTunes accounts: support.apple.com/kb/HT4156
- Learn more about using iTunes: www.apple.com/support/itunes

Modifying iTunes accounts

iTunes account information such as name, password, email address, payment method and billing address can be updated using iTunes.

- Learn more about updating iTunes account information: support.apple.com/kb/HT1918

Deploying Apple Configurator

Apple Configurator is available from the Mac App Store and requires the latest version of iTunes.

- Download Apple Configurator: itunes.apple.com/au/app/apple-configurator/id434433123?mt=12
- Learn more about using Apple Configurator: www.apple.com/au/support/iphone/enterprise/
- Find resources and tutorials about using Apple Configurator: www.apple.com/au/education/resources/information-technology.html

Deploying iTunes

iTunes must be authorised with an iTunes account before Apple Configurator can install apps. Each iTunes account can be authorised for use on up to five computers. To deauthorise a computer, choose Deauthorise Computer from the Store menu in iTunes on that computer.

To simultaneously deauthorise all computers currently associated with an iTunes account, click the Deauthorise All button in the Account Information pane in iTunes. The Deauthorise All button does not appear if there are fewer than five authorised computers for the iTunes account or if this option has been used within the last 12 months. You should carefully plan the authorising and deauthorising of computers to reduce the need to use the Deauthorise All feature in iTunes.

- Learn more about iTunes Store authorisation and deauthorisation: support.apple.com/kb/ht1420

Managing documents

Depending on the capabilities of the app in use, there are many ways to get content in or out of an app. Some common methods for distributing content include wikis or other websites where users can open a posted file directly in an installed app. Some common methods for exporting content from an app include email or a WebDAV file server.

Apple Configurator includes support for document transfer to and from apps that support iTunes file transfers.

Deployment models

A critical question that influences all aspects of an iOS deployment is: "Who should own the apps?" The answer can be the individual end-user, the institution or both.

If the user's personal iTunes account is used to redeem a Volume Purchase Program app code, the user will own that app. If the institution's iTunes account is used to redeem the app code, the institution will own the app.

Develop your deployment strategy before the rollout begins. The questions below form a basic decision tree to assist in selecting a deployment strategy. Select the model or models that meet most of the institution's requirements and keep in mind that multiple strategies may be used across an organisation.

App ownership: Whose apps will be allowed on the device?

- End-user only: consider personal ownership.
- Institution only: consider institutional ownership.
- Both: consider layered ownership.

Device personalisation: Are users allowed to personalise settings and content on their devices?

- Yes: consider personal ownership or layered ownership.
- No: consider institutional ownership.

Personal ownership

The personal ownership model is similar to the typical consumer experience. The education institution may or may not own the iOS device, but the end-user takes responsibility for ongoing maintenance and retains ownership of all apps and content. A personal ownership strategy has the least impact on support resources because many care and maintenance responsibilities are shifted to the end-user. The deployment timeline can be accelerated because little preparation work on devices is required. Users may also be more protective of assigned devices if they can personalise content.

The personal ownership model delivers the optimal user experience for students who are at least 13 years old.

Some educational institutions may prefer that the end-users — whether they are administrators, instructors or students — own their devices or content or both, making a personal ownership strategy attractive. Users may be required to purchase all content, or if an educational institution provides Volume Purchase Program app redemption codes in this model, the-end user's personal iTunes account retains ownership of the app licence.

Configuration and management tools can be used as part of the deployment to allow the institution to control device settings and configuration. Apple Configurator may be used to supervise devices, install configuration profiles and set restrictions if required. Supervised devices cannot sync with iTunes on another computer, so supervision is only recommended if devices are institutionally owned or end-users do not require the ability to sync media from iTunes via USB.

An MDM solution may be employed for centralised wireless configuration and management as well as for distributing App Store apps via Volume Purchase Program redemption codes.

- Learn more about MDM in the *Configuration and Management* section of this guide.

Implementing personal ownership

Implementing a personal ownership model is a straightforward process. Regardless of who owns the device, only a personal iTunes account is used on the device.

The following is a general workflow for implementing the personal ownership model:

1. Ensure devices are running the latest version of iOS. Upgrade with Apple Configurator if necessary.
2. Optionally, supervise and configure devices with Apple Configurator to enable enhanced restrictions (for institutionally owned devices).
   - Wi-Fi settings.
   - Global proxy settings.
   - MDM enrolment (for ongoing maintenance).
3. Asset tag or inventory devices as needed.
4. Deploy to end-users.
5. Have each end-user complete the Setup Assistant using his or her personal Apple ID.
   - Enable iCloud services.
   - Enable iCloud backup.
6. Have the end-user enrol in MDM (if not using Apple Configurator).
7. Distribute app redemption codes to end-users, which they redeem using their personal iTunes account.

Transitioning to supervised personal ownership

Note: This workflow assumes devices are backed up to iCloud.

1. Supervise with Apple Configurator (this will erase the devices) and install a Wi-Fi configuration profile (if necessary).
2. Return devices to end-users (devices should be at the iOS Setup Assistant screen) and have them perform an iCloud restore.
3. The devices will still be supervised, so it will no longer be possible to sync with iTunes. Personal apps and data are recovered with the iCloud restore.
4. Optionally, reconnect to Apple Configurator to deploy non-removable configuration profiles and enrol in MDM.

Institutional ownership

The personal ownership model requires that app licences are owned by the end-user using their personal Apple ID. Institutions that want to retain ownership of purchased apps and prevent end-users from installing personal apps should use the institutional ownership model. Using an institution-controlled iTunes account with Apple Configurator enables education institutions to retain ownership of all app purchases.

- Learn more about the Volume Purchase Program in the *Purchasing Content* section of this guide.

The institutional ownership model is preferred for temporary device usage and is required for deployments in which end-users are younger than 13 years old. Apple Configurator is required for this deployment strategy.

Rather than the end-user managing Volume Purchase Program app redemption codes, the institution performs all app code redemptions on computers running Apple Configurator, using an Apple ID that the institution owns and controls. To receive new or updated apps that the institution has purchased, each iOS device must connect via USB to the computer on which it was first prepared by Apple Configurator.

The Assign feature of Apple Configurator can be used with the institutional ownership model when mobile carts are used. This allows an instructor to check devices out to users for temporary use and then retain their personal data when the device is checked in.

Note: MDM should not be used with the Assign feature.

Apple Configurator can enforce device restrictions to prevent users from installing apps or making other changes to the device configuration. These device restrictions can be automatically refreshed upon connecting to USB.

- Learn more about configuring and managing iOS devices, including available restrictions, in the *Configuration and Management* section of this guide.

Implementing institutional ownership

Implementing an institutional ownership model requires that iTunes accounts be created using email addresses that are under the control of the education institution.

Plan for scalability when designing and configuring configuration stations. It's easier to deploy the first few configuration stations if the long-term goals are known.

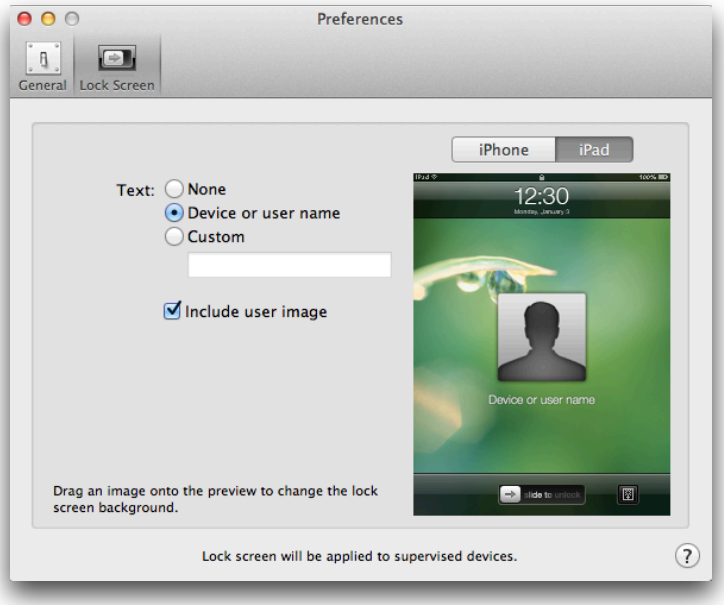
Configuration station computers may be deployed as stationary systems or included with a mobile cart. MacBook Pro and MacBook Air work best with carts because they can run on battery power and are easily stored inside the cart. Desktop computers must be powered off before transporting the cart and may pose a safety hazard while the cart is being moved.

The steps below require a Mac connected to the school network running the latest version of OS X, iTunes and Apple Configurator. The email address for the iTunes account should already have been created, but not the iTunes account itself.

- Learn more about iTunes accounts in the *Understanding the Tools* section of this guide.

1. **Prepare the configuration station**
   - Authorise iTunes with the institution's Apple ID.
   - Download institution apps via iTunes. For paid apps from the Volume Purchase Program redeem the first code for each app to download the app in iTunes.
   - Set Apple Configurator preferences.
     - On the General tab ensure both checkboxes are enabled. The "Remove apps and profiles Configurator did not install" setting must be enabled for the institution ownership model.

     - Click the Lock Screen tab and customise initial wallpaper or Lock Screen text, then close Preferences.



- Import paid apps into Apple Configurator then import app redemption codes.
- When prompted, enter the same Apple ID as was used to authorise iTunes.
- Create device groups in the Supervise tab (if applicable).
- Create users in the Assign tab (only if devices are for temporary use and MDM is not being used).

2. Prepare the master or template device

- Select one new or unconfigured device as the master device.
- Supervise the device with Apple Configurator
  - Name the device (e.g. Year 5 Cart — 1).
  - Set Supervision to ON.
  - Select apps to install from the Apps tab.
  - Select or create configuration profiles. Apple recommends the following configuration profile restrictions and settings for institutional ownership deployments:
    - Disable installing apps.
    - Disable removing apps.
    - Disable iTunes Store.
    - Disable iBookstore.
    - Disable iCloud Backup.
    - Disable Game Center.
    - Disable iMessage.
    - Configure Wi-Fi settings.
  - Click Prepare.
- Complete Setup Assistant on the device.

    - Skip the Apple ID step when prompted to sign in.
- Customise the device.
    - Organise the Home screen icons and place icons in folders, if desired.
    - Set wallpaper and other settings.
- Select the device on the Supervise tab and click Device > Back Up. Name the backup something easily identifiable (e.g. Year 5 Cart — Backup).
- Set the device to restore automatically from the backup created in the previous step.
- Optionally, enrol in MDM for ongoing management of devices (only if devices are not assigned).

3. **Prepare additional devices**
    - Retain all options from preparing the master device.
    - Plug in additional devices, also in a new or unconfigured state.
    - Set device names (e.g. Year 5 Cart — 2) and check the box next to "Number sequentially starting at 2".
    - Click Prepare.
    - Set Restore to the master backup you created.
4. **Issue devices to users for long-term use (Assign tab in Apple Configurator is not being used).**
    - Hand out devices to the students who will maintain them. This scenario is for students under 13 who use the same iPad full time, each day. Apple Configurator is not checking devices in and out.
    - Install and update apps using Apple Configurator.
5. **Check out devices to users with the Assign tab in Apple Configurator for temporary use (MDM is not being used).**
    - Prepare the devices and issue them to end-users. When users are finished simply reconnect to the Mac that originally set them up and click the Check In button on the Assign tab. All user data is backed up to Apple Configurator upon check-in.

Planning for App and iOS updates

Because installing or updating apps for a large number of devices may become time-consuming, consider establishing an install and upgrade schedule. For example, app installation and updates may be scheduled quarterly, biannually or during school holidays.

Test existing apps on new versions of iOS before upgrading all devices; some apps may need to be updated before they'll work with a new iOS version. Consider a similar plan for app updates so that all students and instructors use the same version of any particular app and have the same features available.

Layered ownership

The layered ownership deployment allows for both the end-user and the institution to own their respective content on the same device, and the end-user performs the majority of maintenance tasks on the device. This model is essentially the institutional ownership workflow (with fewer restrictions), followed by the personal ownership workflow.

The layered ownership model offers the end-user full control over his or her content while allowing the institution to retain ownership of purchased apps. This makes it an excellent deployment strategy for all users aged 13 and over.

Apple Configurator allows an organisation to configure settings and restrictions on a device that has not yet completed the iOS Setup Assistant, including MDM enrolment. Once the institution's configuration profiles are installed the device is issued to the end-user with the Setup Assistant still waiting to be completed.

The end-user then uses a personal Apple ID to complete the iOS Setup Assistant, which configures built-in apps and services, including iCloud. The institution then installs and updates App Store apps via Apple Configurator while the end-user manages personal apps and content directly on the device. In the layered ownership model, the end-user does not connect to any computer other than the institution's configuration station since devices are supervised by Apple Configurator. The institution can remove any apps installed via Apple Configurator to reclaim licences for use on other devices.

Allowing end-users to download personal apps and content is more likely to give them a sense of ownership so they may be more apt to protect the iOS devices. This may be helpful in a model where the devices are taken home, and the goal is to both guide and empower the end-users. Students can use their personal accounts to download personal apps at any time. The institution uses Apple Configurator for all app installation and updating. This is also the preferred model for instructors and administrators.

Implementing layered ownership

The implementation of the layered ownership model starts with the same basic requirements of the institutional ownership model followed by the requirements of the personal ownership model. It combines the freedom to personalise the device of the personal ownership model with the requirement to retain ownership of App Store apps of the institutional ownership model.

While the App Store is generally disabled in the institutional ownership model to prevent personalisation, it must be enabled for the layered ownership model.

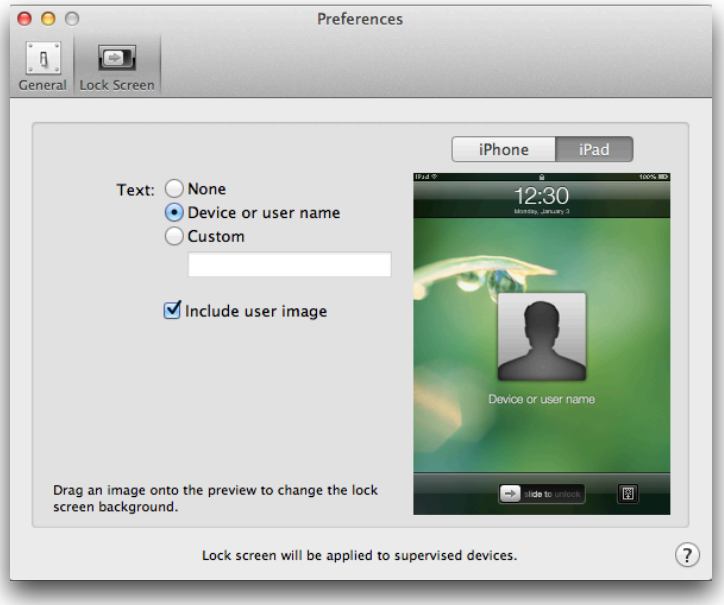
All new or factory default devices running iOS 5 or later start with a screen prompting the user to "Slide to set up". This is the start of the iOS Setup Assistant. The end-user must complete Setup Assistant to automatically personalise their assigned device with a personal Apple ID.

The steps below require a Mac connected to the school network running the latest version of OS X, iTunes and Apple Configurator. The institution's iTunes account should already have been created by following one of the methods found at support.apple.com/kb/HT2534.

1. **Prepare the configuration station**
   - Authorise iTunes with the institution's Apple ID.
   - Download institution apps via iTunes. For paid apps from the Volume Purchase Program, redeem the first code for each app to download the app in iTunes.

- Set Apple Configurator preferences.
  - On the General tab the "Remove apps and profiles Configurator did not install" setting must be disabled for the layered ownership model. This will preserve personal apps, data and configuration profiles (including user-enrolled MDM) on devices when they return to this configuration station for new or updated institution apps.

  - Click the Lock Screen tab and customise the initial wallpaper or Lock Screen text, then close Preferences.



- Download or redeem apps with iTunes and import into Apple Configurator.
  - When prompted, enter the same Apple ID as was used to authorise iTunes.
  - Create device groups in the Supervise tab (if applicable).

2. Prepare devices

- Supervise the devices with Apple Configurator
  - Name the devices (e.g. School iPad — 1) and check the box next to "Number sequentially starting at 1".
  - Set Supervision to ON.
  - Select apps (downloaded and imported earlier) to install from the Apps tab.

- Select or create configuration profiles. Apple recommends the following configuration profile restrictions and settings for layered ownership deployments:
  - Configure the Wi-Fi settings.
  - Do not restrict App Store. Other restrictions are optional.
  - Configure the MDM enrolment profile. Note that if the "Remove apps and profiles Configurator did not install" setting is not disabled in Apple Configurator preferences you will be prompted to disable it upon selecting an MDM enrolment profile. Click Yes if prompted.

  - Click Prepare to start configuring devices.

3. **Issue devices to users**
   - Optionally, have users manually enrol in MDM if Apple Configurator was not used to automatically enrol devices.

   Whenever the institution has new or updated App Store apps to install, download them via iTunes on the configuration station using the same institution iTunes account that authorised the Mac. Once apps and app updates have been downloaded, import the apps into Apple Configurator for installation on client devices.

   Note: End-users can update personal apps directly on their devices.

   If iCloud Backup is enabled, the iOS device automatically backs up all user data and settings over the Internet to the end-user's personal iCloud storage. This can greatly simplify workflows for the institution as the configuration station is only used for setting up new devices and installing new or updated apps.

   All app data is backed up by iCloud regardless of which account was used to purchase the apps. When an iOS device is restored from an iCloud backup, all user data from both personal and institution apps is restored.

Transitioning to supervised layered ownership

Note: This workflow assumes devices are backed up to iCloud.

1. Connect one device at a time to Apple Configurator and save a backup from the Prepare tab (Devices > Back up). Save the backup to a dedicated folder for backups.
2. Turn Supervision to ON and select the Restore drop-down. Click Edit Stored Backups.
3. Hold the Option key and click the + button that appears. Select the backup created in step one and click OK.
4. Supervise device with Apple Configurator with the backup selected. Install any required apps and configuration profiles.

5. Delete the backup from the list and set the restore drop-down to "Do not restore backup".
6. Return the device back to the end-user and have them download personal apps again. The data for personal apps will reconnect to the apps once they are downloaded.

Device replacement

Replacing a functional but damaged device.

Note: This workflow assumes devices are backed up to iCloud.

1. Connect the broken device to Apple Configurator and make a backup.
2. Unsupervise the device. This automatically removes the device from Apple Configurator and returns licences.
3. Prepare the replacement device as if it were new, but also restore from the backup made previously.
4. Issue the replacement device to the end-user. Personal apps need to be reinstalled, but data will be preserved.

Replacing an inaccessible or nonfunctional device.

1. Find the device in the device list on the Supervise tab and hold the Option key then click the Device menu > Remove. This removes the device from the Apple Configurator database. App licences are not returned to Apple Configurator.
2. Follow the steps above for replacing a functional but damaged device.

Understanding iCloud

iCloud is a service that stores a user's content — mail, contacts, calendars, reminders, bookmarks, notes, photos and documents — and wirelessly pushes it to associated devices and computers, automatically keeping everything up to date.

iCloud features include:

- Automatic downloads — new music, app and book purchases are automatically downloaded to the user's devices
- Download previous purchases — the user can view previous iTunes Store and App Store purchases and download them again if needed
- Photo Stream — when the user takes a photo on one device, they automatically get it on their other devices
- Documents and Data — documents and data for apps that work with iCloud are stored in iCloud
- Find My iPad — the user can locate their iPad on a map, display a message, play a sound, lock the screen or remotely wipe the data
- The option of backing up the user's iPad to iCloud.

Reminder: iCloud services are for personal use only and should not be used by institutions. This means the institution shouldn't own or control the Apple ID used for iCloud services. For example, an end-user would be responsible for using Find My iPad to locate a missing iPad using their personal Apple ID.

An iCloud account includes a free mail account and 5GB of storage for mail, documents and backups. Purchased music, apps, TV shows and books, as well as photos in Photo Stream, don't count against this free space. An iCloud account requires an Apple ID.

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

- Learn more about iCloud: www.apple.com/au/icloud

iCloud and other services are all automatically configured to use the Apple ID entered in Setup Assistant. Some services can be disabled through the use of restrictions either entered manually on the device or set via configuration profiles.

Reminder: If the user is under 13 they cannot have an Apple ID, and they won't be able to configure any iCloud services.

- Learn more about configuration and management in the *Configuration and Management* section of this guide.

Apple TV

Instructors will find immediate use for Apple TV in their classrooms. Instead of being tethered to the projector cable, instructors can walk around the classroom with their iPad using AirPlay Mirroring through an Apple TV connected to a TV or projector.

Starting with Apple TV software update 5.2, configuration profiles for Wi-Fi, 802.1X and HTTP proxy settings are supported. These profiles can be installed via Apple Configurator.

AirPlay can be protected by an optional password. Starting with Apple TV software update 5.2, a unique password can be displayed on screen for each attempt to connect. This can prevent inadvertent or unauthorised use of the Apple TV from devices in other rooms. When the on-screen password is used and a device is using AirPlay Mirroring, another device cannot take over the screen until the first device has stopped using AirPlay.

The included Apple TV remote gives the instructor ultimate control over the content displayed. Pressing the "MENU" button on the remote will exit playback in any AirPlay session. Consider pairing the remote to the Apple TV to avoid unauthorised remote control.

Learn more about Apple TV features and configuration:

- Pairing and unpairing the Apple Remote: support.apple.com/kb/HT1555
- How to install a configuration profile: support.apple.com/kb/HT5437
- How to configure 802.1X using a profile: support.apple.com/kb/HT5438
- How to configure a proxy using a profile: support.apple.com/kb/HT5439
- Learn more about Apple TV: www.apple.com/au/appletv

Verify the LAN and Wi-Fi networks are properly configured for features like AirPlay Mirroring.

- Learn more about designing Wi-Fi networks for Apple TV in the *Supporting AirPlay, AirPrint and iTunes Wi-Fi Sync* section of this guide.

Troubleshooting resources

- Learn about troubleshooting steps for iPhone: www.apple.com/au/support/iphone

- Learn about troubleshooting steps for iPad: www.apple.com/au/support/ipad
- Learn about troubleshooting steps for iPod touch: www.apple.com/au/support/ipodtouch
- Learn about troubleshooting steps for Apple TV: www.apple.com/au/support/appletv
- Learn about troubleshooting steps for iTunes: www.apple.com/au/support/itunes

Summary

This guide covers many topics related to iOS deployment in education, but certainly not all of them. The following is a summary of the key points in each chapter.

Preparing for Deployment

Plan ahead for an iOS deployment. This includes researching apps, preparing a secure staging area for rollouts, considering firewall factors, understanding AppleCare support plans, assessing the need for third-party professional services, reviewing available Apple factory services, and considering Apple Professional Development.

Wi-Fi Network Design

Designing Wi-Fi networks requires planning for coverage as well as density of devices within that coverage area. Consideration must also be given to security, Wi-Fi standards and the use of Apple iPad Learning Labs. Consult a Wi-Fi network provider to determine an optimal design of a Wi-Fi infrastructure to support iOS devices.

Purchasing Apps

Enrol in the Volume Purchase Program before devices arrive to begin researching and budgeting for apps that will be part of the deployment. Identify who will fill the Program Manager, Program Facilitator and end-user roles.

Configuration and Management

There are multiple ways to configure and manage iOS devices, including manually on the device, using configuration profiles, using a Mobile Device Management (MDM) solution, using Apple Configurator and using Exchange ActiveSync (EAS). Understand how each configuration and management option can be used prior to deployment.

Deployment Strategies

Determining who will own purchased apps and content will shape the deployment strategy. The three models are the personal ownership model, the institutional ownership model and the layered ownership model.

Appendix A — Wi-Fi Standards

This appendix discusses the Wi-Fi standards related to designing a Wi-Fi network that will include iOS devices. The selection of each Wi-Fi standard impacts the user experience, so a summary of the standards is included.

2.4GHz vs. 5GHz

Wi-Fi networks operating at 2.4GHz allow for 13 channels in Australia. However, due to channel interference considerations, only channels 1, 6 and 11 are recommended for use in a network design.

5GHz signals do not penetrate walls and other barriers as well as 2.4GHz signals, which results in a smaller coverage area. Therefore, 5GHz networks may be preferred in designing for a high density of devices in an enclosed space, such as in classrooms. The number of channels available in the 5GHz band varies among access-point vendors and from country to country, but at least eight channels will always be available.

5GHz channels are non-overlapping, which is a significant departure from the three non-overlapping channels available in the 2.4GHz band. When designing a Wi-Fi network for a high density of iOS devices, the additional channels provided at 5GHz become a strategic planning consideration.

IEEE 802.11b/g

If devices that only support the 802.11b or 802.11g standards are required to participate on the network, 802.11b/g should be included in the Wi-Fi network design.

802.11b provides transmit rates of up to 11 Mbps, while 802.11g provides transmit rates of up to 54 Mbps. Under ideal conditions, the actual data throughput, or the actual speed at which devices will exchange information, is about half the transmit rate. Both technologies are implemented in the 2.4GHz band, the same band at which many cordless phones, microwaves and other wireless devices operate. Note that when 802.11b devices and 802.11g devices are both using the same wireless network, the 802.11b devices cause reduced data throughput for the faster 802.11g clients.

IEEE 802.11a

In contrast to 802.11b/g, the 802.11a standard operates in the 5GHz band. Most notebook computers support this band, but many smaller mobile devices only support 2.4GHz Wi-Fi.

Transfer rates and data throughput when using 802.11a are similar to those with 802.11g.

IEEE 802.11n

The newest 802.11 standard is 802.11n. This standard is capable of transmit rates of up to 600 Mbps. To accomplish this task, 802.11n uses several technologies.

802.11n can use either the 2.4GHz or 5GHz band and is compatible with the 802.11a/b/g standards, so older devices can share the same network as the newer 802.11n devices.

802.11n supports several operating modes:

- 802.11n at 5GHz
- 802.11n at 2.4GHz
- 802.11n and 802.11a at 5GHz

- 802.1n and 802.11b/g at 2.4GHz
- 802.1n and 802.11g at 2.4GHz
- 802.1n and 802.11b at 2.4GHz

Most dual-band access points allow any combination of the above modes.

The 802.11n standard uses a technology called Multiple Input Multiple Output (MIMO) to achieve higher speeds. MIMO supports transmitting multiple streams of data, called spatial streams, simultaneously. To take advantage of these spatial streams, both the access point and client must have multiple radios and antennas. Mac products support multiple spatial streams, while iOS devices support a single spatial stream.

HD40, commonly referred to as wide channels or channel bonding, is another technology used to accomplish faster transmit speeds. Approximately double the amount of data can be transmitted through this single but wider channel. Non-bonded channels are called HD20. Channel bonding should not be used in the 2.4GHz band because there are only three non-overlapping channels available. Thus, many access-point vendors do not allow configuration of channel bonding when using the 2.4GHz band.

Wi-Fi standards in Apple products

Apple product support for the various Wi-Fi specifications is listed below. The list covers:

- 802.11 compatibility: 802.11b/g, 802.11a and 802.11n
- Frequency band: 2.4GHz or 5GHz
- Modulation and Coding Scheme (MCS) index: this defines the maximum transmit rate at which 802.11n devices can communicate. See the MCS index table listed later in this appendix for more information
- Channel bonding: HD20 or HD40
- Guard interval (GI): the space (time) between symbols transmitted from one device to another. The 802.11n standard defines a short GI of 400 nanoseconds, which allows for faster overall throughput, but devices may use a long GI of 800 nanoseconds.

iPhone 5

802.11n at 2.4GHz and 5GHz

802.11 a/b/g
MCS index 7, HT40, 400-nanosecond GI

iPhone 4S

802.11n at 2.4GHz

802.11 b/g
MCS index 7, HT20, 800-nanosecond GI

iPhone 4

802.11n at 2.4GHz

802.11 b/g
MCS index 7, HT20, 800-nanosecond GI

iPhone 3GS

802.11 b/g
MCS index 7, HT20, 800-nanosecond GI

iPad (4th generation) and iPad mini

802.11n at 2.4GHz and 5GHz

802.11a/b/g

MCS index 7, HT40, 400-nanosecond GI

iPad (1st, 2nd and 3rd generation)

802.11n at 2.4GHz and 5GHz

802.11a/b/g

MCS index 7, HT20, 800-nanosecond GI

iPod touch (5th generation)

802.11n at 2.4GHz and 5GHz

802.11 a/b/g

MCS index 7, HT40, 400-nanosecond GI

iPod touch (4th generation)

802.11n at 2.4GHz

802.11 b/g

MCS index 7, HT20, 800-nanosecond GI

MacBook Pro, MacBook Air and MacBook

802.11n at 2.4GHz and 5GHz

802.11a/b/g

MCS index 15, HT40, 400-nanosecond GI

MCS index 23, HT40, 400-nanosecond GI (early 2011 or later MacBook Pro)

MCS index table

MCS index	Spatial streams	Modulation	Coding rate	Data rate in Mbps (GI = 800 ns)		Data rate in Mbps (GI = 400 ns)	
				20MHz	40MHz	20MHz	40MHz
0	1	BPSK	1/2	6.5	13.5	7.2	15.0
1	1	QPSK	1/2	13.0	27.0	14.4	30.0
2	1	QPSK	3/4	19.5	40.5	21.7	45.0
3	1	16-QAM	1/2	26.0	54.0	28.9	60.0
4	1	16-QAM	3/4	39.0	81.0	43.3	90.0
5	1	64-QAM	2/3	52.0	108.0	57.8	120.0
6	1	64-QAM	3/4	58.5	121.5	65.0	135.0
7	1	64-QAM	5/6	65.0	135.0	72.2	150.0
8	2	BPSK	1/2	13.0	27.0	14.4	30.0
9	2	QPSK	1/2	26.0	54.0	28.9	60.0
10	2	QPSK	3/4	39.0	81.0	43.3	90.0
11	2	16-QAM	1/2	52.0	108.0	57.8	120.0
12	2	16-QAM	3/4	78.0	162.0	86.7	180.0
13	2	64-QAM	2/3	104.0	216.0	115.6	240.0
14	2	64-QAM	3/4	117.0	243.0	130.3	270.0
15	2	64-QAM	5/6	130.0	270.0	144.4	300.0
16	3	BPSK	1/2	19.5	40.5	21.7	45.0
17	3	QPSK	1/2	39.0	81.0	43.3	90.0
18	3	QPSK	3/4	58.5	121.5	65.0	135.0
19	3	16-QAM	1/2	78.0	162.0	86.7	180.0
20	3	16-QAM	3/4	117.0	243.0	130.0	270.0
21	3	64-QAM	2/3	156.0	324.0	173.3	360.0
22	3	64-QAM	3/4	175.5	364.5	195.0	405.0
23	3	64-QAM	5/6	195.0	405.0	216.7	450.0
24	4	BPSK	1/2	26.0	54.0	28.9	60.0
25	4	QPSK	1/2	52.0	108.0	57.8	120.0
26	4	QPSK	3/4	78.0	162.0	86.7	180.0
27	4	16-QAM	1/2	104.0	216.0	115.6	240.0
28	4	16-QAM	3/4	156.0	324.0	173.3	360.0
29	4	64-QAM	2/3	208.0	432.0	231.1	480.0
30	4	64-QAM	3/4	234.0	486.0	260.0	540.0
31	4	64-QAM	5/6	260.0	540.0	288.9	600.0

Appendix B — Wireless Security

Over time, several technologies have been developed to protect and secure Wi-Fi networks. Some of the early technologies include WEP (Wired Equivalent Privacy), LEAP (Lightweight Extensible Authentication Protocol), device filtering by media access control (MAC) address and hiding the network service set identifier (SSID). While using these technologies provided some level of Wi-Fi network security when they were developed, all of these technologies are now considered insecure and can easily be compromised.

Fortunately, current Wi-Fi standards such as Wi-Fi Protected Access (WPA) and WPA2 provide technologies for network authentication and encryption to secure data. If these security standards are in place, there is no benefit in implementing any of the legacy technologies.

IEEE 802.11i, WPA and WPA2

WPA and WPA2 refer to a suite of tests that ensure compatibility between various Wi-Fi devices. The actual Wi-Fi security standard is defined by the IEEE in 802.11i. In general, this specification defines two areas of network security: authentication for obtaining access to the network, and encryption of the data as it passes from one Wi-Fi device to another. WPA and WPA2 are commonly used to define which 802.11i options are enabled on the network. The main difference between WPA and WPA2 is the strength of data encryption. WPA2 is preferred over WPA.

PSK vs. Enterprise

Access to a WPA or WPA2 network can be secured with a single password for all users or by providing an individual credential to each user or device. This credential could be in the form of a username and password or a public key infrastructure (PKI) identity (certificate). Using a single password for all devices is referred to as a pre-shared key (PSK). The enterprise version refers to the implementation of 802.1X for individual credentials assigned to each user or device. Regardless of the method used for network authentication and encryption, be sure to use WPA or WPA2 for a secure Wi-Fi network.

Broadcast or hidden SSID

A Wi-Fi network's name is called the SSID (service set identifier). To join a specific wireless network, the user selects the SSID for the desired network from a list of SSIDs being broadcast within the range of the Wi-Fi device. However, it's also possible to hide the SSID so that it does not show up in searches. While there may be a perception that hiding the SSID is more secure than broadcasting it, in reality there is very little security benefit.

Hiding the network SSID means that a user won't see the network in a list of networks within range of the computer or device, but it would take a potential hacker only a few seconds to obtain the name of the network simply by using a computer to listen to information being transmitted by Wi-Fi devices already associated with the hidden SSID. This is possible because even with a hidden SSID, the name of the network is transmitted unencrypted within the data frames.

More important are the practical implications of a hidden SSID. For a Wi-Fi device to rejoin a hidden SSID, it must first locate access points offering that SSID. However, because the SSID is hidden, the Wi-Fi device must visit every known channel and broadcast to it to see if the hidden SSID exists on that channel. After broadcasting, the computer must wait a certain amount of time for responses. If the client has multiple saved hidden SSIDs, it must broadcast on each channel for each of the SSIDs, and wait for a response after every channel broadcast for every SSID.

When finding a broadcast SSID, the computer visits each channel and simply listens for the SSIDs that exist on that channel. It doesn't matter how many saved broadcast SSIDs might exist on a computer, the computer still only has to listen one time on each channel to find them.

Simply put, it's harder for a Wi-Fi device to rejoin a hidden SSID than a broadcast SSID, and there's very little security benefit in hiding the SSID. iOS devices tend to physically move frequently, so hidden SSIDs may delay their network association time.

Appendix C — Supporting Bonjour

Information that is simultaneously transmitted across the network to a specific group of devices at the same time is called multicast traffic. A special case of multicast traffic in which the information is simultaneously transmitted to all network devices is called broadcast traffic. These methods of transmitting data are used in various ways. For example, when a computer obtains an Internet protocol (IP) address using dynamic host configuration protocol (DHCP), it uses a broadcast to request the IP address. By using a broadcast, it insures that the DHCP server will receive the request because the broadcast goes out to all computers.

Apple uses a technology called Bonjour to allow users to find devices and services on a network. Computers and devices with Bonjour automatically broadcast their own services and listen for services being offered by others. A computer might see a printer available for printing, a shared iTunes playlist, an iChat buddy available for videoconferencing or another computer sharing files. iOS devices use Bonjour to discover AirPrint-compatible printers and AirPlay-compatible devices such as Apple TV. Even Windows computers can take advantage of Bonjour if iTunes is installed. Bonjour works with standard connection technologies, including Ethernet and Wi-Fi (802.11). It uses the standard, ubiquitous IP networking protocol for its connections, the same protocol that runs the Internet itself.

Multicast traffic, especially broadcast traffic, can also consume network bandwidth very quickly. Imagine if every time a network device transmitted something on the network the information was sent to every other network device. Because wireless devices receive data at different speeds, broadcast traffic would be broadcast at the speed of the slowest client. Excessive broadcast traffic can cause what is called a 'broadcast storm' and make the network inaccessible. Wi-Fi networks are especially vulnerable to this.

Work with a Wi-Fi network provider to create a network design that allows for efficient multicast traffic in a way that doesn't adversely affect other network clients. Unnecessary broadcast traffic can be reduced with configuration changes on users' devices. This reduces the amount of Bonjour service registrations on the network, and therefore reduces the overall amount of broadcast traffic on the network. Changes can also be made to the network infrastructure, including access points, to allow or filter broadcast traffic.

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