



Deployment Guide

iOS 6 in Education

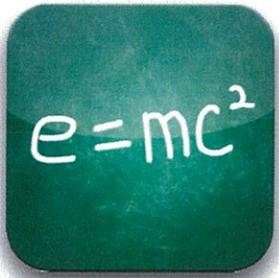
First Edition
December 2012

Contents

iOS in Education	3
System Requirements	5
Preparing for Deployment	6
Preparing a Staging Area	6
Understanding Firewall Requirements	6
Discovering Apps for Learning	6
Contacting Apple	6
AppleCare	6
Apple Professional Services	7
Apple Factory Services	9
Apple Professional Development	9
Wi-Fi Design	11
Planning for Coverage and Density	11
Apple iPad Learning Labs	13
AirPlay, AirPrint and Bonjour	14
Configuration and Management	15
Manual Configuration	15
Configuration Profiles	15
Mobile Device Management	16
Apple Configurator	18
Using Exchange ActiveSync	21
Choosing Management Tools	21
Purchasing Content	22
Credit Cards and iTunes Gift Cards	22
Volume Purchase Program	22
Understanding Program Roles	23
Enrolling in the Volume Purchase Program	24
Understanding Volume Vouchers	24
Using the Volume Purchase Program	24
Volume Pricing	25
Code Distribution Techniques	25
Deployment Strategies	26
Understanding the Tools	26
Managing Documents	27
Personal Ownership	28
Institutional Ownership	29
Layered Ownership	33
Understanding iCloud	36
Apple TV	37
Troubleshooting Resources	38
Summary	39

iOS in Education

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



This guide is designed for those responsible for the deployment of iOS devices, from IT leadership to implementors. 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 devices. Early design decisions, both good and bad, are amplified as a deployment is scaled up. Curriculum and technology leadership as well as those who will implement the design should be included in the planning process. A well-planned iOS deployment will likely incorporate the following steps and questions:

1. Understand the deployment goals.
 - What are the expected outcomes?
2. Assess the infrastructure.
 - Can the LAN and Wi-Fi network support high density of devices?
 - Review server and storage design (local or hosted).
 - Review Apple Configurator station design.
 - Evaluate Internet bandwidth.
3. Plan for support.
 - Will Apple provide project management support from Apple Professional Services?
 - Who will be responsible for post-deployment support?
 - Will Apple provide professional development for implementors?
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 authorized 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 Apple Professional Services execute the rollout?
 - Enroll in the Volume Purchase Program.
 - Consider a Mobile Device Management solution.
 - Download and use Apple Configurator.
5. Execute the purchase.
 - Order the iOS devices, accessories, and related equipment.
 - Purchase apps in volume using the Volume Purchase Program.

6. Prepare for rollout.
 - Prepare a secure space for unpacking devices, activation, and the initial sync.
 - Configure configuration stations, carts, and iOS devices.
7. Perform the initial rollout.
 - Deploy to initial sites.
 - Verify the deployment model.
8. Communicate with stakeholders (the School Board, Board of Trustees, community, and so on).
 - Describe and explain the deployment plan.
 - Reiterate expected outcomes.
9. Scale up the deployment.
 - Expand to remaining sites using best practices.
10. Verify.
 - Collect data and verify deployment fidelity.

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

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

System Requirements

The following resources are where you can find information about the operating system versions and related software that are required to follow the recommendations in this document.

iPhone, iPad, and iPod touch

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

Apple Configurator

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

iTunes

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

OS X

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

Preparing for Deployment

Strategic preparation prior to deployment can 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 inventoried before their delivery to end users, so consider designating a secure location for equipment that has adequate power and networking support.

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 TCP and UDP ports used by Apple support.apple.com/kb/TS1629
- Learn about Apple TV firewall requirements support.apple.com/kb/HT2463

Discovering Apps for Learning

Consider doing research about apps before devices arrive for a more efficient deployment. 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/education/apps

Contacting Apple

To learn more about Apple in education, visit www.apple.com/education or call 800-800-2775 to speak to an Apple education representative.

AppleCare

AppleCare products are available for institutions of every size.

AppleCare Options for iPhone, iPad, or iPod touch

Every iPhone, iPad, and iPod touch comes with complimentary telephone technical support for 90 days from purchase and a one-year limited warranty. The service coverage can be extended to two years from the original purchase date with AppleCare + for iPhone, AppleCare+ for iPad or AppleCare Protection Plan (APP) for iPod touch. You can call Apple's technical support experts as often as you like and get questions answered. There are convenient service options if repair service is needed. In addition, AppleCare+ for iPhone and AppleCare+ for iPad add up to two incidents of accidental damage coverage, each subject to a \$49 service fee.



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

AppleCare iOS Direct Service Program

A benefit of AppleCare+ and the AppleCare Protection Plan, the iOS Direct Service Program screens the units for any hardware faults and, if necessary, directly orders a replacement iPhone, iPad, iPod touch, or in-box accessory, and exchanges it for the failed item at their service location. This provides convenience and cost reduction to organizations. The program is open to businesses/enterprise organizations, education institutions, and U.S., state, and local government agencies.

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

AppleCare Help Desk Support

AppleCare Help Desk Support provides priority access to Apple's senior technical support staff by telephone. It also includes a suite of tools to diagnose and troubleshoot Apple hardware, 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 and 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 for resolution.

- 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 document.

Apple Professional Services

Apple Professional Services experts are among the industry's most experienced and respected. Drawing on decades of experience in education as well as industry certification training, Apple Professional Services helps you leverage your technology investments to make an educational difference.

Apple Professional Services has a complete array of offerings to meet the diverse needs of education institutions, including K-12 schools, school district offices, and universities. Here are a few examples of what Apple Professional Services can help with:

- Assessing, planning, managing, delivering, and supporting a fully mobile learning environment
- Deploying supplemental services for mobile collaboration, communication, and learning
- Creating a new campus-wide technology solution or integrating Apple technology with your existing systems
- Mentoring technical staff and educators so they get the most out of the iOS deployment

In addition to offering solutions for integrating iPhone, iPad, and iPod touch into an education infrastructure, Apple Professional Services can also show you how iOS devices like iPad and iPod touch can transform learning.

Apple Configuration Services

Educational technology deployments require detailed coordination and technical expertise to minimize risk and ensure success. Apple project managers provide coordination and oversight of an entire deployment process from project scope, scheduling, and communications to staging, licensing, and deployment. Apple's expertise in managing these detailed logistics reduces your risk by ensuring timely, successful deployments that meet your educational goals as well as your budget.

Having highly-skilled, experienced engineers assist with an iOS device deployment can help ensure a well-designed deployment. Apple Professional Services engineers work with you to design, plan, configure, and integrate iPad and iPod touch management and deployment strategies in a learning environment. These services are always designed to coach and mentor an organization on the specific deployment, helping staff build self-sufficiency.

Apple Deployment Services

When you're ready to deploy, Apple Deployment Services provides skilled and efficient technicians who apply asset tags, prepare and activate the iOS devices, assemble mobile carts, and even remove all packing materials from your site.

Post-Deployment

Once the deployment is complete, Apple Professional Services can help with maintenance tasks of your solution: product cleaning and repair, new software configuration, remote assistance, regular reevaluation of the infrastructure, and planning for new faculty development and continuing IT skills development.

Getting Started with Integrating iPad and iPod touch

Introduce your organization to iPad and iPod touch deployment techniques. Learn about Apple Configurator hands-on – preparing iOS devices, creating profiles, importing VPP apps, supervising and assigning devices, distributing and collecting documents, and incorporating with existing services. This customized solution provides mentoring for IT staff and educators to ensure successful integration into your learning environment.

Learn More

- For more information about ordering Apple Professional Services, see the [*Contacting Apple*](#) section of this document.

Apple Factory Services

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



Learn More

- For more information about Apple factory service options, see the [Contacting Apple](#) section of this document.

Apple Professional Development

Apple Professional Development offers onsite workshops that range from one to eight days long. These hands-on workshops are tailored to a school's or district's specific needs and are designed to enable attendees to transform teaching and learning using Apple products.

All Apple Professional Development Specialists are educators themselves. That gives them a unique view: they know what's important in the classroom, so they can ensure that workshop participants learn about the institution's Apple products and how they can best serve the educators and students.

Apple Professional Development workshops are flexible, allowing multiple entry points for professional development. You may begin with any workshop category, depending on faculty needs. One-day workshops may be broken into two half-day sessions to accommodate a variety of faculty groupings. Workshops accommodate 20 participants, and incorporate Common Core State Standards or a focus on National Standards. Apple Professional Development is for institutional/group purchase only. After purchasing, discuss implementation options with an Apple Professional Development Specialist.

Available Workshops

Apple Professional Development workshops are offered in several categories including:

- **Start**
Focused on technology skills, these foundational workshops help teachers become confident and comfortable integrating Apple products into their teaching strategies.
- **Learn**
These workshops help teachers apply their skills with specific Apple products to learning activities and approaches to produce effective personal learning for their students.
- **Instruct**
These workshops focus on curricula, content design, and instruction with all Apple products.

- **Lead**

Designed for school and district leaders, Lead workshops focus on issues important to success— visioning, planning, and implementing.

- **Support**

These offerings support teachers beyond workshops and include Expert on Call and the Education Technology Profile.

Learn More

- For more information about Apple Professional Development, see the [Contacting Apple](#) section of this document.

Wi-Fi Design



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

- Required coverage area
- Number and density of devices using the Wi-Fi network
- Types of devices and their Wi-Fi capabilities
- Types and amount of data being transferred
- Security requirements for accessing the wireless network
- Encryption requirements for data passing through 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. This design may differ for 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, 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 in use 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 ten large offices and a conference room on each floor. Fifty employees equipped with MacBook Pros, iPad and iPhone 4S or iPhone 5 devices are spread out over two stories. The MacBook Pros 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 Pros with them. The majority of network access comes from checking email, calendars, and Internet browsing.



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 document.

Recall that some employees use the iPhone 4S while others use the iPhone 5, so a 2.4GHz network must also be available for the iPhone 4S devices. The iPhone 5 will prefer 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

Contrast the district office scenario above with a high school that has 1000 students and 30 teachers in a two-story building. Every student has been issued an iPad, and every teacher has been issued both 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 with 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 will 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. Therefore, 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 document.

If devices that only support the 802.11b or 802.11g standards are required to participate on 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 SSID 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.

The use of hidden SSIDs should be avoided in either design scenario. 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 document.

Note that the above network designs are hypothetical examples. The actual design for an 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.

Apple iPad Learning Labs



An Apple iPad Learning Lab streamlines the management of classroom sets of iPad devices. Each lab can store, charge, and sync up to 30 iPad devices and has room for a MacBook computer. The cart rolls easily around campus, so multiple classes can benefit, and it can be locked to secure the devices when they're not in use. 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.

Note 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 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. If this is done, Wi-Fi is always be available where the 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 minimize 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 strategy for Wi-Fi coverage for Apple iPad Learning Labs.

- Learn more about Apple mobile learning labs
www.apple.com/education/labs

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 or AirPrint 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 that communicating devices 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 document.
- 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: manually on the device, using configuration profiles, using a Mobile Device Management solution, using Apple Configurator and 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 labor intensive. This may be 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; toggle location services; and 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 unauthorized 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. Configuration profiles can optionally be locked so that an end user 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/SMTP Email, CalDAV calendar services, CardDAV and LDAP address book services, Wi-Fi networks, VPN services, and subscribed calendars. 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 the downloading and use of unauthorized apps by enabling the Installing Apps restriction. This restriction also prevents syncing or updating apps in iTunes and must be removed to allow installing new or updated apps.

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

- Learn more about iOS restrictions
support.apple.com/kb/HT4213
- Learn more about iBooks and iBookstore restrictions
support.apple.com/kb/HT5492

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 custom title and icon and can optionally 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 enrollment in a Mobile Device Management 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

Mobile Device Management (MDM) gives education institutions the ability to securely enroll 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, management consoles, additional features, and pricing structures. Evaluate which aspects of MDM solutions are most relevant to your organization before you choose a solution.

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

Requirements

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

Enroll

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

MDM enrollment is both user opt-in and opt-out. Institutions should consider incentives for users to remain managed. For example, require MDM enrollment for Wi-Fi network access by using the MDM solution to automatically provide the wireless credentials. When a user unenrolls from MDM, the device attempts to notify the MDM server.

Configure

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

When combined with enrollment, 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

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

Wipe, Lock, Clear Passcode

When a device is managed, it can be administered by the Mobile Device Management 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

Mobile Device Management 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 VPP app codes with MDM requires the end user to enter Apple ID credentials, which is ideally suited for deployments where end users will permanently own purchased applications.

Apps deployed from an MDM server can be removed remotely by the server or when the user unenrolls from MDM, along with the data associated with each app. If the app was downloaded using a personal Apple ID then it can be downloaded again from the App Store by the end user. Managed apps can optionally 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 document.

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. 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 simplifies creation of configuration profiles, enforcement of restrictions through Mobile Device Management, and deployment of 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 and is also available preinstalled on a Mac mini or Mac Pro. There are no client licenses to purchase or maintain to use the features of OS X Server, which makes Profile Manager the simplest and fastest way to get started with Mobile Device Management.

- Learn more about Profile Manager
www.apple.com/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. Quickly configure and update 30 devices at a time to the latest version of iOS, configure settings, and install apps and data for your students, faculty or staff.

Prepare

Apple Configurator can easily prepare up to 30 devices simultaneously and many more if connected one at a time or in batches. While preparing, any device that is connected to the Mac running Apple Configurator via USB will be configured automatically. To

prepare devices for use, Apple Configurator can supervise devices for greater control by the institution, update or restore the latest version of iOS to devices, restore multiple devices from a master template backup, name devices sequentially, install configuration profiles to devices and install apps to 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 organized 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 to supervised devices running iOS 6 or later. Once a device is supervised these restrictions can be configured via configuration profiles that are delivered via Apple Configurator, MDM or manual download. These restrictions include:

- Single App Mode - Locks user into a single, specified application. If powered down, the specified application will launch at boot. Consider using MDM to enable and disable this setting for dynamic control.
- Global Network Proxy for HTTP - Routes most all device web traffic 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 strongest enforcement. Consider using a PAC file for greater flexibility with this setting.
- Allow Removing Apps - Disabling prevents users from removing apps from the home screen.
- Allow Use of Game Center - Disabling removes Game Center icon from the home screen. Use 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 removes Messages icon from the home screen.
- Allow iBookstore - Disabling prevents access to the iBookstore while allowing use of the iBooks app for reading books and PDFs.
- Allow iBookstore Sexually Explicit Content - Allow prevents access to adult content from the iBookstore.
- Allow Configuration Profiles Installation - Disabling 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 is dependent 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 to 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 app codes the licenses are managed locally. App licenses can be transferred between devices by Apple Configurator. Back up Apple Configurator to preserve the license 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 5 V (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 (Milliamps) at 5 V (Volts) 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 selection of a USB hub. 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. Apple iPad Learning Labs and Apple iPod Learning Labs meet these requirements.

- Learn more about Apple mobile learning labs www.apple.com/education/labs
- 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. Exchange ActiveSync 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 Exchange ActiveSync. If Exchange ActiveSync 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/iphone/business/docs/iOS_EAS_Sep12.pdf

Choosing Management Tools

An iOS deployment may utilize one or more configuration and management tools. Choose the appropriate tools based on your organizations 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 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 and books in volume, education institutions can use the Volume Purchase Program (VPP) and fund purchases via credit card, or PCard. Education institutions in the US can also fund VPP purchases with a purchase order. An institution may choose one or more purchasing methods depending on its needs.

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

Credit Cards and iTunes Gift Cards

Anyone in the U.S. 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 throughout the United States as well as directly from Apple Education Sales. 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.

Additionally, tax-free purchasing is not possible with iTunes Gift Cards or credit cards. Consider the Volume Purchase Program if frequent tax-free app purchasing is required.

Examples of purchases funded by credit card may include school administrators using institutional PCards to purchase apps or books for individual use, instructors purchasing apps or books for use only on their devices, or college 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 allows educational institutions to purchase iOS apps and books 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, United Kingdom and the United States qualify for participation in the Volume Purchase Program. If an institution is tax exempt, it is not charged sales tax when purchasing content through VPP.

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



Program Facilitator



End User

Program Manager

A Program Manager for VPP is responsible for enrolling an institution in VPP. A Program Manager for VPP is also authorized by the educational institution to create and manage Program Facilitator accounts.

Program Facilitator

Program Facilitators can purchase apps and books at the Volume Purchase Program store using credit cards, PCards, and PayPal. In the US, Program Facilitators can also redeem Volume Vouchers through the VPP portal. They can search for and order apps and books in variable quantities, spending up to the current dollar amount credited to their account via redeemed Volume Vouchers.

Program Facilitators can be anyone designated by the Program Manager—for example, deans, professors, researchers, principals, teachers, technology coordinators, or instructional technologists. This role may correlate to the person already responsible for procuring software for your 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 VPP. 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 your education institution to ensure that the Volume Vouchers redeemed with the Program Facilitator account aren't tied to an individual.

End User

For the purposes of VPP, the End User is any iTunes account used to redeem apps and books.

For app purchases, education institutions have the option of redeeming one app code per iTunes authorized 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 authorized user. Note that Apple Configurator requires a valid VPP code for each copy of an app deployed to a device.

For book purchases, an institution may not use a single code to sync an iBookstore product to multiple devices. The iBookstore product may not be used in a library-type lending scenario.

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

- Learn more about iTunes accounts in the [Understanding the Tools](#) section of this document.

Enrolling in the Volume Purchase Program

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

- Learn more about enrolling in VPP
www.apple.com/education/vpp
- Read frequently asked questions about VPP
www.apple.com/education/volume-purchase-program/faq.html
- VPP Support
www.apple.com/support/itunes/vpp

Understanding Volume Vouchers

Volume Vouchers are physical cards in denominations of \$100, \$500, \$1000, \$5000, and \$10,000 that can be used only to purchase apps within the US Education VPP store. They are shipped via Federal Express or UPS, so they can be easily tracked and should arrive within three to five business days from the time of the order.

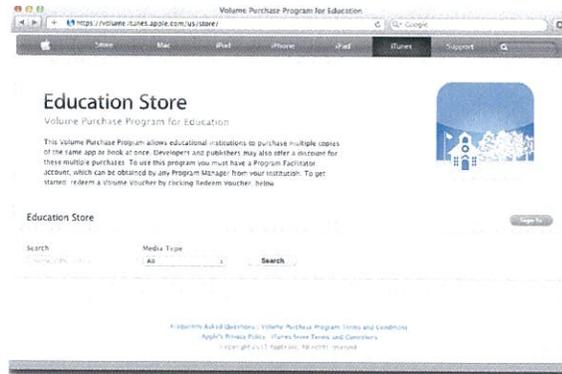
Volume Vouchers can only be used in the US Education VPP store and are not valid for regular iTunes, App Store, or iBookstore downloads. This means that lost or stolen Volume Vouchers cannot be redeemed by anyone who is not a registered user of VPP. Each Volume Voucher can be used by one Program Facilitator account. Purchase multiple vouchers in smaller denominations if funds need to be distributed to multiple Program Facilitators.

Using the Volume Purchase Program

Only Program Facilitators purchase apps and books through the VPP Education 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. Institutions that are eligible for tax-free purchasing aren't charged tax when purchasing via the VPP Education Store or when purchasing Volume Vouchers. Following each purchase, the Program Facilitator receives a spreadsheet that includes a list of redemption codes that can be redeemed by End Users in 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 through VPP. If the developer has enabled volume pricing, education institutions receive 50% off when purchasing 20 or more licenses 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, coordinate and consolidate app purchase requests to reach the volume pricing at 20 or more licenses of an app.

Volume pricing is not available for books or iBooks textbooks.

Code Distribution Techniques

Distribution of redemption codes is the responsibility of the educational institution. Codes can be distributed manually to users, emailed via a mail merge process, or posted to an internal website such as a wiki. Organizations can create their own code distribution website to distribute codes to users. Some Mobile Device Management solutions integrate VPP code redemption into their self-service client applications.

The spreadsheet of codes obtained from 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 VPP frequently asked questions for examples
www.apple.com/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 the primary. Additionally, three security questions must be set first.

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

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

- 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 to an Apple ID
support.apple.com/kb/HT4627

iTunes account passwords should be closely guarded to prevent unauthorized 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/us/app/apple-configurator/id434433123?mt=12
- Learn more about using Apple Configurator
www.apple.com/support/iphone/enterprise/
- Find resources and tutorials on using Apple Configurator
www.apple.com/education/it

Deploying iTunes

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

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

- Learn more about iTunes Store authorization and deauthorization
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 VPP app code then the user will own that app. If the institution's iTunes account is used to redeem the app code then 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 the most requirements and keep in mind that multiple strategies may be used across an organization.

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 Personalization: Are users allowed to personalize 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 personalize 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 VPP app redemption codes in this model, the end user's personal iTunes account retains ownership of the app or textbook license.

Configuration and management tools can be used as part of the deployment to allow the institution to control the settings and configuration of the devices. 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.

A Mobile Device Management solution may be employed for centralized wireless configuration and management as well as for distributing App Store apps and textbooks via VPP redemption codes.

- Learn more about Mobile Device Management in the [Configuration and Management](#) section of this document.

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 general workflow for implementing the Personal Ownership model is:

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 settings and restrictions (for institutionally owned devices).
 - Wi-Fi settings.
 - Global proxy settings.
 - MDM enrollment (for ongoing maintenance).
3. Asset tag or inventory devices as needed.
4. Deploy to end users.
5. Each end user completes Setup Assistant using his or her personal Apple ID.
 - Enable iCloud services.

- Enable iCloud backup.
6. The end user enrolls in MDM (if not using Apple Configurator).
 7. Distribute app and textbook redemption codes to end users, which they redeem using their personal iTunes account.

Transitioning to Supervised Personal Ownership via iCloud

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 back 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 enroll in MDM.

Transitioning to Supervised Personal Ownership via iTunes

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

1. Plug devices into the Mac that will supervise them with Apple Configurator.
2. Open iTunes, accept iTunes device prompts and then back devices up with iTunes.
3. Close iTunes and open Apple Configurator.
4. Supervise with Apple Configurator (this will erase the devices).
5. Close Apple Configurator and open iTunes.
6. iTunes will recognize the devices and offer to restore from the backup taken earlier. Restore all devices from their respective backups.
7. Close iTunes and open Apple Configurator to deploy non-removable configuration profiles and enroll in MDM.
8. Return devices to users to download personal apps directly on the device. App data was restored by iTunes and will reconnect to the apps once they are downloaded.

Institutional Ownership

The Personal Ownership model requires that app licenses are owned by the personal Apple ID of the end user. 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.

Note: iBookstore purchases from the VPP store are not compatible with this deployment model per iBookstore terms and conditions.

- Learn more about the Volume Purchase Program see the [Purchasing Content](#) section of this document.



The Institutional Ownership model is preferred for temporary device usage and is required for deployments in which end users are under 13 years old. Apple Configurator is required for this deployment strategy.

Rather than the end user managing VPP 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 from which it was first prepared by Apple Configurator.

The Assign feature of Apple Configurator can be used with the Institutional Ownership when carts are used. This allows an instructor to check devices out to users for temporary use and then retain their personal data upon check-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 document.

Implementing Institutional Ownership

Implementing an Institutional Ownership model requires that iTunes accounts be created using email addresses 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 you already know the long-term goals.

Configuration Station computers may be deployed as stationary systems or included with a mobile cart. MacBook, MacBook Pro, or 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 document.

1. Prepare the Configuration Station

- Authorize iTunes with the institution's Apple ID.
- Download institution apps via iTunes. For paid apps from VPP, 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 customize 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 authorize 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 master or template device

- Select one new or unconfigured device as the master device.
- Supervise the device with Apple Configurator
 - Name the device (ex: 5th Grade 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.
- Wi-Fi settings.
- Click Prepare.
- Complete Setup Assistant on the device.
 - Skip the Apple ID step when prompted to sign in.
- Customize the device.
 - Organize 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 (ex: 5th Grade Cart - Backup).
- Set the device to restore automatically from the backup created in the previous step.
- Optionally enroll in MDM for ongoing management of devices (only if devices are not assigned).

3. Prepare additional devices

- All options from preparing master device were retained.
- Plug in additional devices, also in a new or unconfigured state.
- Set device names (ex: 5th Grade 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).

- Devices are handed out to students who will maintain them. This scenario is for full-time use of iPads by students under 13 where students use the same iPad each day. Apple Configurator is not checking devices in and out.
- Apps are installed and updated by Apple Configurator.

5. Check out devices to users with the Assign tab in Apple Configurator for temporary use (MDM is not being used).

- Devices are now prepared and can be issued 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 installs and updates may be scheduled quarterly, biannually, or during winter, spring, and summer breaks.

Test existing apps on new versions of iOS before upgrading all devices because some apps may need to be updated before they'll work with a new iOS version. A similar plan may be considered 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 age 13 and over.

Apple Configurator allows an organization to configure settings and restrictions on a device that has not yet completed the iOS Setup Assistant, including MDM enrollment. 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 licenses 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. The freedom to personalize the device is preserved from the Personal Ownership model while the requirement to retain ownership of App Store apps is preserved from the Institutional Ownership model.

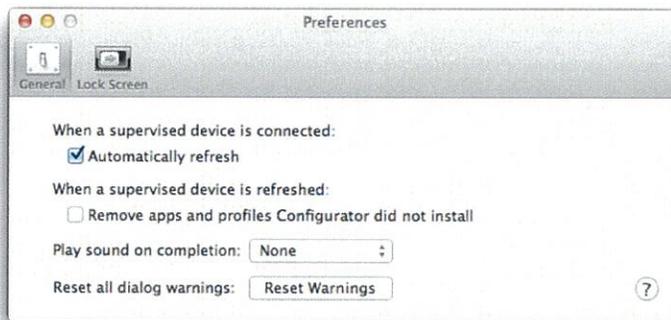
While the App Store is generally disabled in the Institutional Ownership model to prevent personalization, it must be enabled for the Layered Ownership model.

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 personalize 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 in support.apple.com/kb/HT2534.

1. Prepare the Configuration Station

- Authorize iTunes with the institution's Apple ID.
- Download institution apps via iTunes. For paid apps from VPP, 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 customize 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 authorize iTunes.
 - Create device groups in the Supervise tab (if applicable).

2. Prepare devices

- Supervise the devices with Apple Configurator
 - Name the devices (ex: 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:
 - Wi-Fi settings.
 - Do not restrict App Store. Other restrictions are optional.
 - MDM enrollment 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 enrollment profile. Click Yes if prompted.



- Click Prepare to start configuring devices.

3. Issue devices to users.

- Optionally have users manually enroll in MDM if Apple Configurator was not used to automatically enroll 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 authorized the Mac. Once apps and app updates have been downloaded, import the apps into Apple Configurator for installation on client devices.

Note: End users 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 each user's personal iCloud account.

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 from 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 licenses.
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 licenses 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:

- Photo Stream—When a user takes a photo on one device, the user automatically gets it on his or her other devices.
- Documents & Data—Documents and data for apps that work with iCloud are stored.
- Find My iPad—A user can locate his or her iPad on a map, display a message, play a sound, lock the screen, or remotely wipe the data.
- A user's iPad can also be backed up 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 backup. Purchased music, apps, TV shows, and books, as well as photos in Photo Stream, don't count against free space. An iCloud account requires an Apple ID.

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

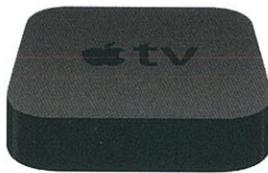
- Learn more about iCloud
www.apple.com/icloud

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 an Apple ID is not created, and the user won't be able to configure any iCloud services.

- Learn more about configuration and management in the [Configuration and Management](#) section of this document.

Apple TV



Instructors will find immediate use for Apple TV in their classrooms. Instead of being tethered to the projector cable, instructors are able to walk around the classroom with their iPad by 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 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 unauthorized 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 is 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 of any AirPlay session. Consider pairing the remote to the Apple TV to avoid unauthorized 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 a proxy using profile
support.apple.com/kb/HT5439
- Learn more about Apple TV
www.apple.com/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 document.

Troubleshooting Resources

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

Summary

This document covers many topics related to iOS deployment in education but certainly not all. The following is a summary of key takeaways from each chapter.

Preparing for Deployment

Plan ahead for an iOS deployment. This includes researching apps, preparing a secure staging area for rollouts, firewall considerations, understanding AppleCare support plans, Apple Professional Services, available Apple factory services, and 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 use of Apple iPad Learning Labs. Consult with a Wi-Fi network provider to determine an optimal design of a Wi-Fi infrastructure to support iOS devices.

Purchasing Apps

Enroll 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 solution, using Apple Configurator and using Exchange ActiveSync. 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: Personal Ownership model, Institutional Ownership model, and 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 11 channels in the United States. However, due to channel interference considerations, only channels 1, 6, and 11 should be used 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 when you design 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 vendors of access points and from country to country, but at least 8 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 11Mbps, while 802.11g provides transmit rates of up to 54Mbps. 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 both 802.11b devices and 802.11g devices are 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 600Mbps. To accomplish this task, several technologies are used.

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 @ 5GHz
- 802.11n @ 2.4GHz
- 802.11n + 802.11a @ 5GHz

- 802.1n + 802.11b/g @ 2.4GHz
- 802.1n + 802.11g @ 2.4GHz
- 802.1n + 802.11b @ 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 configuring channel bonding when using the 2.4GHz band.

Wi-Fi Standards in Apple Products

Support in Apple products for the various Wi-Fi specifications are listed below. The list includes the following details:

- 802.11 compatibility: 802.11b/g, 802.11a, 802.11n
- Frequency band: 2.4GHz or 5GHz
- MCS index: The Modulation and Coding Scheme (MCS) index 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 guard interval is the space (time) between symbols transmitted from one device to another. The 802.11n standard defines a short guard interval of 400ns that allows for faster overall throughput, but devices may utilize a long guard interval of 800ns.

iPhone 5

802.11n @ 2.4GHz and 5GHz

802.11 a/b/g

MCS Index 7 / HD40 / 400ns GI

iPhone 4S

802.11n @ 2.4GHz

802.11 b/g

MCS Index 7 / HD20 / 800ns GI

iPhone 4

802.11n @ 2.4GHz

802.11 b/g

MCS Index 7 / HD20 / 800ns GI

iPhone 3GS

802.11 b/g
MCS Index 7 / HD20 / 800ns GI

iPad (4th Generation) and iPad Mini

802.11n @ 2.4GHz and 5GHz
802.11a/b/g
MCS Index 7 / HD40 / 400ns GI

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

802.11n @ 2.4GHz and 5GHz
802.11a/b/g
MCS Index 7 / HD20 / 800ns GI

iPod touch (5th Generation)

802.11n @ 2.4GHz and 5GHz
802.11 a/b/g
MCS Index 7 / HD40 / 400ns GI

iPod touch (4th Generation)

802.11n @ 2.4GHz
802.11 b/g
MCS Index 7 / HD20 / 800ns GI

MacBook Pro, MacBook Air, and MacBook

802.11n @ 2.4GHz and 5GHz
802.11a/b/g
MCS Index 15 / HD40 / 400ns GI
MCS Index 23 / HD40 / 400ns GI (early 2011 or later MacBook Pro)

MCS Index

MCS Index	Spatial Streams	Modulation	Coding Rate	Data Rate (in Mbps) (GI = 800ns)		Data Rate (in Mbps) (GI = 400ns)	
				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 MAC address, and hiding the network SSID. While using these technologies provided some level of Wi-Fi network security at the time, all of these technologies are now considered insecure and can easily be compromised.

Fortunately, current Wi-Fi standards such as 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 (Wi-Fi Protected Access) 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 data itself 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 user name and password or a 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 name is called the SSID (Service Set ID). 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 the SSID, 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, 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 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 broadcasted 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 IP address using DHCP, it uses a broadcast to request an 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 video conferencing, 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 multicast traffic efficiently and in a way that doesn’t adversely affect other network clients. Unnecessary broadcast traffic can be reduced with configuration changes on the client 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