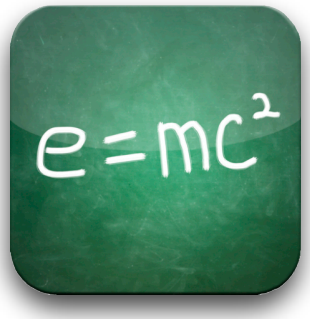
iOS 4 Education Deployment Guide

Contents

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

Note: The information in this guide was current at the time of publication for iOS 4. Check for future revisions to this document for updated information.

Before deploying devices, develop and communicate a plan. Early design decisions, good or bad, are amplified as the deployment is scaled up. Include in the planning process curriculum and technology leadership as well as those who will implement the design. A well-planned iOS deployment will likely incorporate some version of the following steps:

1. Understand the deployment goals.
   - What are the expected outcomes?
2. Assess the infrastructure.
   - Consider the network and Wi-Fi capacity.
   - Review server and storage design (local or hosted).
   - Evaluate Internet bandwidth.
3. Plan for support.
   - Who will support the deployment?
   - What is the professional development plan for implementors?
4. Plan the rollout.
   - What policies will need to be created or revised?
   - Who will get devices and in what order will they be distributed?
   - What is the professional development plan for instructors and administrators?
   - What is the training plan for students?
   - Who will be authorized to purchase apps?
   - Enroll in the App Store Volume Purchase Program (ASVPP).
   - Consider a Mobile Device Management solution.
   - What data needs to be backed up from iOS devices?
   - Which sync strategies will be used?
5. Execute the purchase.
   - Order the iOS devices, accessories, and related equipment.
   - Purchase apps in volume using the ASVPP.
6. Prepare for rollout.
   - Prepare a secure space for unpacking devices, activation, and the initial sync.
   - Configure sync stations, carts, and iOS devices.

7. Perform the initial rollout.
   - Deploy to the initial sites.
   - Verify the deployment model.
8. Communicate with stakeholders (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 the 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 at: www.apple.com/education/ipad
- Learn more about iPod touch and iPhone in education at: www.apple.com/education/ipodtouch-iphone
- Find education resources, video tutorials, and other guides at: www.apple.com/education/resources

iOS Features for Education

The following are some of the features of iPhone, iPad, and iPod touch of special interest to education users:

iBooks—A novel way to buy and read books. Organize your bookshelf by your collection of books. PDFs (such as curriculum, handouts, and student examples) all go on your bookshelf, too. When someone emails you a PDF, open it in iBooks.

Spell check—A built-in dictionary suggests words and corrects spelling.

Mirroring—Video mirroring makes it possible to share what's on your iPad 2 with an even bigger screen and an even bigger audience.

Wireless keyboard support—Pair a Bluetooth-enabled wireless keyboard.

Folders—Organize apps into folders with drag-and-drop simplicity. Get faster access to your favorites and browse and manage thousands of apps.

Accessibility—Control VoiceOver using a Bluetooth-enabled wireless keyboard. iOS 4 also offers out-of-the-box support for over 30 wireless braille displays and many other accessibility features, such as dynamic screen magnification, playback of closed-captioned video, white on black text, and more.

Multitasking—Run your favorite third-party apps, and switch between them instantly, without slowing down the performance of the foreground app or draining the battery unnecessarily.

iTunes U enhancements—Support for over-the-air ePub downloads to iBooks.

AirPrint—Print mail, photos, web pages, and more directly from your iPhone, iPad, or iPod touch to an AirPrint-enabled printer.

AirPlay—Wirelessly stream music, photos, and video to your Apple TV and AirPlay-enabled speakers or receivers.

Finding text on web pages—In Safari, easily find and highlight specific words and phrases on large web pages.

Device restrictions—Restrict features of the device, including the ability to restrict installation or deletion of apps and changes to accounts for Mail, Contacts, and Calendars.

Mobile Device Management—iOS 4 supports Mobile Device Management, giving institutions the ability to manage scaled deployments of iPhone, iPad, and iPod touch.

Find My iPhone, iPad, or iPod touch—Locate your missing iPhone, iPad, or iPod touch on a map, remotely set a passcode lock, or display a message.

Keyboard and dictionary—Choose from more than 30 keyboards and dictionaries.

Mail—See messages from all your accounts in a unified inbox, organize messages by threads, and open attachments in third-party apps.

FaceTime—With a tap, you can make video calls over Wi-Fi from your FaceTime-enabled device to any other FaceTime-enabled device,.

HD video uploads—Upload HD video to YouTube from an iPhone 4, iPad 2, or 4th generation iPod touch.

- Learn more about using these iOS features in the user guides at: http://support.apple.com/manuals

System Requirements

The following is a list of where to find information on the operating system versions and related software required to follow the recommendations in this document.

iPhone, iPad, and iPod touch

- Learn more about iPhone system requirements at: www.apple.com/iphone/specs.html
- Learn more about iPad system requirements at: www.apple.com/ipad/specs
- Learn more about iPod touch system requirements at: www.apple.com/ipodtouch/specs.html
- Learn more about the latest version of iOS at: www.apple.com/ios

iPhone Configuration Utility

- Learn more about iPhone Configuration Utility system requirements at: www.apple.com/support/iphone/enterprise

iTunes

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

Preparing for Deployment

Strategic preparation prior to deployment can facilitate a smooth rollout. Key preparation options are discussed in this chapter.

AppleCare

AppleCare products are available for institutions of every size.

AppleCare Protection Plan for iPhone, iPad, or iPod touch

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

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

AppleCare iOS Direct Service Program

The iOS Direct Service Program, a benefit of the AppleCare Protection Plan, provides convenience and reduces the cost to an organization of supporting its own installed base of devices by screening the units for any hardware faults and, if necessary, directly ordering a replacement iPhone, iPad, iPod touch, or in-box accessory and exchanging it for the failed item at the service location. The program is open to businesses and enterprise organizations, education institutions, and U.S., state, and local government agencies.

- Learn more about the iOS Direct Service Program at: 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 you 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 at: 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 at: www.apple.com/support/products/enterprise/server.html

Learn More

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

Apple Education Professional Services

Apple Education Professional Services is uniquely qualified to help your institution deliver on the promise of educational technology: more effective schools and higher student achievement.

Apple Education 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 Education Professional Services will help you leverage your technology investments to make an educational difference.

Whether you're in a K–12 school, at the district, or on a university campus, Apple Education Professional Services has a complete array of offerings to meet the diverse needs of your institution. Here are a few examples of what Apple can help you do:

- Assess, plan, manage, deliver, and support a fully mobile learning environment.
- Deploy supplemental services for mobile collaboration, communication, media, and learning.
- Create a new campus-wide technology solution or integrate our technology with your existing systems.
- Mentor your technical staff and educators so they get the most out of your iOS deployment.

Apple can offer solutions for integrating iPhone, iPad, and iPod touch into your infrastructure and also show you how iOS devices like iPad and iPod touch can transform learning.

Apple Integration Services

Educational technology deployments require detailed coordination and technical expertise to minimize risk and ensure success.

A successful deployment depends on a solid plan and effective communications. Apple project managers provide coordination and oversight of your entire integration process, from project scope, scheduling, and communications to staging, syncing, and deployment. Our expertise in managing these detailed logistics reduces your risk by ensuring timely, successful deployments that meet your educational goals—and your budget.

Having highly-skilled, experienced engineers assist with your iOS device deployment can help ensure a well-designed deployment. Apple Integration Services engineers work with you to architect, plan, configure, and integrate iPad and iPod touch management and sync strategies in your learning environment. Best of all, our services are always designed to coach and mentor your organization on your specific deployment, helping your staff build self-sufficiency.

Apple Setup Services

When you are ready to deploy, Apple Setup Services provides skilled and efficient technicians that apply asset tags, activate and set up your iOS devices, assemble your mobile carts, and even remove all packing materials from your site. When Apple Setup Services are done, you're ready to run.

Post-Deployment

Once your deployment is complete, it's time to start maintaining your solution: product cleaning and repair, new software configuration, remote assistance, and a regular reevaluation of your infrastructure. It's also a good time to make plans for new faculty development and continuing IT skills development. As always, Apple is ready to help.

Getting Started with Integrating iPad and iPod touch

Apple Education Professional Services offers "Getting Started" solutions tailored to help with your initial iPad and iPod touch deployments. These include building configuration profiles and content libraries, activation, and synchronization. Most importantly, these customized solutions provide mentoring for your IT staff and educators to ensure successful integration into your learning environment.

Learn More

- For more information about ordering Apple Education Professional Services, see the Contacting Apple section of this chapter.

Apple Professional Development

Apple Education's Apple Professional Development offers onsite workshops ranging from one to eight days. These hands-on workshops are tailored to the 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 facilitators are educators themselves. That gives them a unique view: they know what's important in the classroom so they can ensure that you learn about your Apple products and how they can best serve you and your 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 apply toward Continuing Education Units, accommodate 16–20 participants, and incorporate Common Core State Standards. Apple Professional Development is for institutional/group purchase only. After purchase, discuss implementation options with an Apple Professional Development facilitator.

Available Workshops

Apple Professional Development workshops are offered in several categories, including the following:

- **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 and learning activities in content areas to produce effective personal learning for their students.
- **Instruct**
  Focused on curricula design and instruction, these workshops help teachers embrace the range of Apple products in their practice.
- **Lead**
  These workshops for school and district leaders focus on issues important to success—visioning/planning, implementing/managing, and designing curricula.
- **Support**
  Support your teachers beyond workshops with in-class or web coaching and mentoring, technology self-assessments, workshop series, and customized workshop development.

Learn More

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

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 more.

Learn More

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

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 prior to being delivered 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 at: http://support.apple.com/kb/TS1629

Researching Apps for Learning

For a more efficient deployment, consider researching apps before devices arrive.

- Learn about great learning apps at: 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.

Wi-Fi Network Design

As you prepare a 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 factors in Wi-Fi network design. 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; design may differ for other countries.

Planning for Coverage and Density

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

Most modern, enterprise-class access points are capable of handling up to 50 Wi-Fi clients, but 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. Consider the expected usage pattern of the iOS devices as part of a Wi-Fi network design.

Designing for Coverage

As an illustration, consider the following scenario of a district office building with ten large offices and a conference room on each floor. There are 50 employees equipped with MacBook Pro laptops and iPad and iPhone devices spread over two stories. The MacBook Pro computers are plugged into Ethernet ports when not mobile while the iPad and iPhone devices frequently change locations.

The physical layout of the building encourages informal communication and collaboration. Employees may meet with other employees in conference rooms or in offices. As a result, employees move around the building with iPad and iPhone devices throughout the day, and some employees bring their MacBook Pro computer 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 computers 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 the MacBook Pro laptops 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 the employees also use iPhone devices, so a 2.4GHz network must also be available. Most modern access points support simultaneous dual frequencies, so 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 computer 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 iOS devices. Each classroom contains approximately 35 students with iPad devices at any given time during the school day, so 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 being used in this school, so special attention should be given to the technical specifications of that device. Specifically, 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. Though the iPad devices will not benefit from enabling HD40, the MacBook computers will, so this may be enabled as well.

- 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 would be modified slightly. Instead of implementing 802.11n at 5GHz, consider provisioning one SSID using 802.11n at 5GHz for newer devices and another SSID at 2.4GHz to support 802.11b and 802.11g clients.

Avoid the use of hidden SSIDs 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, which means 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 for your environment.

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.

Be sure to 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 is not an existing Wi-Fi infrastructure, or there isn't coverage in the designated areas, if an available Ethernet port is located near the cart, an access point can be installed on the cart to ensure Wi-Fi is always available where the devices are used.

Installing an access point in 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 do not 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.

A Wi-Fi network provider should be consulted to determine the best strategy for Wi-Fi coverage for Apple iPad Learning Labs.

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

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

Supporting AirPlay and AirPrint

If AirPlay and AirPrint will be used as part of an iOS deployment, ensure that the Wi-Fi network design incorporates support for Bonjour traffic.

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

Purchasing Apps

Institutions can choose from a variety of methods to purchase apps. Education users, like all iTunes users, can utilize credit cards or gift cards to fund individual app purchases. To purchase apps in volume, education institutions can use the App Store Volume Purchase Program (ASVPP) and fund purchases via purchase order, credit card, or PCard. If an institution is tax exempt, it is not charged sales tax when purchasing apps through the ASVPP. An institution may choose one or more purchasing methods depending on its needs.

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

Purchasing with a Credit Card or iTunes Gift Card

Anyone can purchase apps from the App 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 are purchased one at a time with either of these funding sources, and each app can only be purchased once per iTunes account. The entire balance of a gift card must be used by one iTunes account and cannot 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 outside of the App Store Volume Purchase Program. Consider the App Store Volume Purchase Program if frequent tax-free app purchasing is required.

Examples of app purchases funded by credit card may include school administrators using institutional PCards to purchase apps for individual use, instructors purchasing apps for use only on their devices, or college students using personal credit cards to purchase apps 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 apps in volume using the App Store Volume Purchase Program.

App Store Volume Purchase Program

The App Store Volume Purchase Program allows educational institutions to buy iOS apps in volume using a Volume Voucher, credit card, or PCard, and then distribute the apps to multiple devices (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 education institutions in the United States qualify for participation in the ASVPP.

ASVPP Workflow

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

Understanding Program Roles

Program Manager

A Program Manager for the ASVPP is an individual authorized by the educational institution to create and manage Program Facilitator accounts. This role is also responsible for enrolling the institution in the program.

Program Facilitator

At the App Store Volume Purchase Program portal, your institution's Program Facilitators search for and purchase apps in volume. Apps can be purchased:

- With credit from Volume Vouchers in the Program Facilitator's account
- Directly with a credit card or PCard

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 the institution. The person serving as the Program Manager can also act in this role, although a separate Program Facilitator account would be required.

The Program Manager creates a new Apple ID for each Program Facilitator to use exclusively within the ASVPP portal. Existing Apple IDs cannot be used within the ASVPP. A valid email address that is not currently used as an Apple ID will need to be provided to Apple for each Program Facilitator. This email address should be controlled by the education institution to ensure that the Volume Vouchers redeemed with the Program Facilitator account are not tied to an individual.

End User

For the purposes of the ASVPP, the End User is any iTunes account used to redeem app codes in the App Store for installing on an iOS device. Education institutions have the option of redeeming one app code per iTunes authorized computer, or "sync station," and retaining the rest of the codes as proof of purchase. Therefore, the End User iTunes account may also be created using a school-controlled email address, and the sync station administrator should be an authorized user.

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 iTunes section of the Sync Strategies chapter of this document.

Enrolling in the App Store Volume Purchase Program

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

- Learn more about enrolling in the ASVPP at: www.apple.com/itunes/education
- Read frequently asked questions about the ASVPP at: www.apple.com/itunes/education/faq

Understanding Volume Vouchers

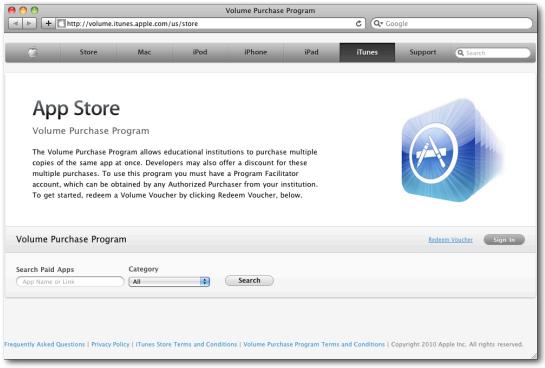
Funding for the ASVPP can be provided by using Volume Vouchers, which are physical cards in denominations of $100, $500, $1000, $5000, and $10,000 that can be used only to purchase apps within the ASVPP portal. They are shipped via Federal Express or UPS, so they can be easily tracked, and should be received within three to five business days from the time of the order.

Volume Vouchers can only be used in the ASVPP portal and are not valid for regular iTunes or App Store downloads. This means that lost or stolen Volume Vouchers cannot be redeemed by those who are not registered users of the ASVPP. 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 App Store Volume Purchase Program

Only Program Facilitators can purchase apps through the ASVPP portal, but anyone can browse the portal. This makes it easy for anyone to check pricing on apps at any time, even if they are not designated as a Program Facilitator.

When purchasing an app, the Program Facilitator must enter a value in the quantity field. Institutions that are eligible for tax-free purchasing are not charged tax when purchasing apps via the ASVPP portal or when purchasing Volume Vouchers. Following each purchase, the Program Facilitator receives a document 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 document to review which codes have been redeemed.



- Browse the ASVPP portal at: http://volume.itunes.apple.com

Volume Pricing

Many developers offer volume pricing on their titles through the ASVPP. If the developer has enabled volume pricing, purchasers 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 are not 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.

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 ASVPP code redemption into their self-service client applications.

The document of codes obtained from the ASVPP 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 ASVPP frequently asked questions for examples: www.apple.com/itunes/education/faq

Configuration and Management

There are three ways to configure and manage iOS devices: manually on the device, using configuration profiles and using a Mobile Device Management solution.

Manually Configuring Devices

Restrictions and configuration information can be set directly on each iOS device. This is the simplest configuration method but requires manually configuring each device. This may be optimal for small deployments or in self-service scenarios.

Certain restrictions can only be set directly on the device in the Settings app. These restrictions include the ability to restrict the deletion of apps, changing of accounts for Mail, Contacts and Calendars, and restricting the use of location services.

- 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.

Configuration settings and restrictions are backed up, persist through restoring a device from a backup, and can be included in a master backup on a centralized iTunes computer. After deployment, restrictions must be changed manually on each device, or an updated master backup must be restored to all devices.

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

Understanding Configuration Profiles

Configuration profiles are XML files that contain device passcode policies, restrictions, account and networking settings, Web Clips and credentials that permit iPhone, iPad and iPod touch to work with enterprise systems. Configuration profiles can optionally be locked so that they cannot be removed by an end user without restoring the device. Configuration profiles can be distributed via web or email or can be installed over USB using iPhone Configuration Utility.

Configuring Accounts and Credentials Using Configuration Profiles

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 does not include credentials the user will be prompted for a password upon manual installation of the profile.

Configuring Restrictions Using Configuration Profiles

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.

- Learn more about updating apps in the *Planning for App and iOS Updates* section of the *Sync Strategies* chapter of this document.

Institutions desiring to restrict internet access may choose to enable the Safari restriction, which removes the Safari icon from the home screen. Several third party filtered web browser apps are available from the App Store.

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

Web Clips

A Web Clip is an icon on the device home screen that links to a web site. Web Clips can optionally launch full screen web applications and can run offline by leveraging HTML 5 local storage.

Configuration profiles may 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. Web Clips can be used 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 about Web Clips at : http://www.apple.com/webapps/whatarewebapps.html

Using iPhone Configuration Utility

iPhone Configuration Utility (iPCU) allows institutions to easily create, maintain, encrypt, and install configuration profiles, in-house applications, and can capture device information including console logs.

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

Using Mobile Device Management Solutions

iOS 4 Mobile Device Management (MDM) capabilities give education institutions the ability to securely enroll devices in an enterprise environment, wirelessly configure and update settings, monitor institution policy compliance, 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 that are most relevant before choosing a solution.

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

Requirements

An institution must be a member of the iOS Developer Enterprise Program, which requires a DUNS number, to use a Mobile Device Management solution. Mobile Device Management requires that devices be running iOS 4 and later.

- Learn about the iOS Developer Enterprise Program at: http://developer.apple.com/programs/ios/enterprise

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, such as requiring MDM enrollment for Wi-Fi network access by using the MDM solution to automatically provide the wireless credentials.

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 automatically without end user 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. Therefore, if users wish 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 ensure that users maintain the appropriate set of applications.

Manage

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.

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 at: http://support.apple.com/kb/HT3576
- Learn more about required firewall ports for APNs and other services in the *Understanding Firewall Requirements* section of the *Preparing for Deployment* chapter of this document.

Profile Manager

Lion Server includes Profile Manager, a server-based solution for remotely managing iOS devices and Mac systems running OS X Lion. Profile Manager simplifies creation of user accounts for mail, calendars, contacts, and chat; enforcement of restrictions through Mobile Device Management; PIN and password policies; and more. Integrated with the Apple Push Notification service, Profile Manager can automatically send out updated configurations wirelessly over the air.

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

- Learn more about Profile Manager at:
  http://www.apple.com/macosx/server/
  http://help.apple.com/profilemanager/

Sync Strategies

After devices are activated, they can be paired with iTunes to sync apps and content. Although there are many possible sync models, the most common education deployments can be grouped into one of two strategies: a personal sync model in which a personally owned iTunes account is used or a centralized sync model in which an institution's iTunes computer, or sync station, is used. In addition, there is a variation of the centralized sync model in which the institution's iTunes sync station is used for syncing while a personal iTunes account is used directly on the device to add personally owned apps and content.

Determining the appropriate sync strategy for an education institution should revolve around who needs to own the iTunes purchases, regardless of where the funding came from. The sync model determines who will retain ownership of the purchased content.

- Learn more about how Apple can assist with iOS sync design and deployment in the Apple Education Professional Services section of the Preparing for Deployment chapter of this document.

Understanding iTunes

iTunes Accounts

An iTunes account is an Apple ID that can be used for various Apple services such as iTunes,and iWork.com. Each iTunes account must be created using a unique email address. Institutions creating multiple centrally managed iTunes accounts may want to consider configuring the email address for each iTunes account to forward to a centrally controlled email address for easier account management. Institutions may prefer iTunes accounts to be created without a credit card.

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

Deploying iTunes

iTunes stores all content in the iTunes library, which resides in the user's home folder. When an iOS device is synced with iTunes, it becomes paired to the iTunes library on that particular computer. This means that the iOS device cannot sync with another computer without first erasing the existing apps or content.

- Learn more about iTunes libraries at: http://support.apple.com/kb/ht1660

Home Sharing can be used to transfer purchased content, including apps, between computers authorized to use the same iTunes account without re-downloading the content from the iTunes Store.

- Learn more about the Home Sharing feature in iTunes at: http://support.apple.com/kb/ht3819

Each iTunes account can be authorized for use on up to five computers, and each computer can sync an unlimited number of iOS devices that you own or control. The easiest way to deauthorize a computer is to choose Store > Deauthorize Computer 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 the iTunes account has fewer than five authorized computers or if this option has been used within the last twelve months. Authorizing and deauthorizing computers should be carefully planned to reduce the need to use the Deauthorize All feature in iTunes.

- Learn more about iTunes Store authorization and deauthorization at: http://support.apple.com/kb/ht1420

iTunes account passwords should be closely guarded to prevent unauthorized use.

- Learn more about protecting iTunes accounts at: http://support.apple.com/kb/HT4156

iTunes is used to name connected iOS devices. Uniquely naming devices can make network identification and ongoing maintenance easier.

- Learn more about renaming devices in iTunes at: http://support.apple.com/kb/ht3965

iTunes is used to back up, restore, and upgrade iOS devices. Devices can only sync with one computer, so plan where devices will be synced before restoring them from a backup.

- Learn more about using iTunes for backups, restores, and iOS upgrades at: http://support.apple.com/kb/HT1414
- Learn more about what is backed up at: http://support.apple.com/kb/HT4079

iOS devices are activated by connecting to a computer that is running iTunes. In a traditional configuration, iTunes activates the device, prompts for a device name, and performs an initial sync of content.

For large rollouts it may be desirable to separate the activation and initial sync tasks to increase workflow efficiency. iTunes can be configured to run in activation-only mode to allow institutions to set up a dedicated activation computer.

With iTunes activation-only mode, connected devices are activated and immediately available for use but are not associated with an iTunes account. iTunes activation-only mode is typically used on a separate computer to activate devices before the initial sync at the assigned sync station.

- Learn how to use iTunes activation-only mode at: http://support.apple.com/kb/HT4335
- Learn more about using iTunes at: http://www.apple.com/support/itunes

Personal Sync

Syncing with a personal iTunes account mirrors the traditional consumer experience. An 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 sync strategy has the least impact on an organization because many care and maintenance responsibilities are shifted to the end user, and users may be more protective of assigned devices if they can personalize them.

Some educational institutions may prefer that the end users—whether they are administrators, instructors, or students—own their devices or subsequent iTunes purchases or both. This would make a personal sync strategy attractive. It may be desirable to activate new iOS devices via iTunes activation-only mode prior to distribution, or the end user may activate his or her own device. If an educational institution provides purchased apps in this sync model, the end user's iTunes account retains ownership of the apps.

Management and configuration tools can be used as part of the deployment to allow the institution to control the settings and configuration of the device. iPhone Configuration Utility can be used to install configurations and set restrictions. An organization can also use a Mobile Device Management solution for centralized wireless configuration and management.

- Learn more about configuration and management in the Configuration and Management chapter of this document.

The implementation of a personal sync model mirrors the traditional consumer experience. Regardless of who owns the device, the end users sync their devices to a computer authorized to use their personal iTunes accounts. The institution may choose to own the device and/or offer centralized activation, configuration, and management services as part of a deployment plan.

Understanding Centralized Sync

Syncing multiple devices to a centrally controlled iTunes account gives education institutions the most control over the apps, content, and the end user experience on each iOS device. Groups of iOS devices are synced and maintained from the same iTunes library on a sync station, which is a computer controlled by the institution. Each iOS device must continue to be synced with the original iTunes library from which it was configured in order to receive new or updated apps purchased by the institution.

Once iOS devices have been paired with a sync station, attempting to sync apps or other content with another computer will cause iTunes to notify the user that the apps and content from the institution's sync station must be erased from the device before the new computer can sync to it. A student missing all of the institution's curriculum apps will quickly stand out when he or she is unable to participate in class projects requiring those apps.

For the best performance and reliability, use the latest version of iTunes and Mac OS X when syncing multiple devices simultaneously. iTunes for Windows works best with only one device connected at a time.

- Learn more about connecting multiple devices to iTunes for Windows at: http://support.apple.com/kb/HT3622

Device restrictions can be enabled to prevent users from installing or deleting apps or making other changes to the device configuration. Some restrictions can only be set manually on each device. Other restrictions and settings can be applied using iPhone Configuration Utility or managed wirelessly via a Mobile Device Management solution.

- Learn more about configuration and management in the Configuration and Management chapter of this document.

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

Understanding Sync Stations

Sync station computers may be deployed as stationary systems or as part of 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.

Determining where devices will be used impacts how institution iTunes accounts are provisioned. In turn, the iTunes account design determines sync station placement. Sync station designs will vary depending on the deployment goals, and more than one sync station design strategy may exist in the same building.

iTunes accounts may be created based on logical groupings within the organization. For example, sharing a generic iTunes account within a department or grade level may facilitate collaboration between instructors in selecting the most effective apps. The examples below describe some possible iTunes account designs, but other configurations may be employed, depending on the needs of the institution.

Designing iTunes Accounts for Grade Level Use

In an elementary school setting where students will store devices in a classroom cart, consider assigning one iTunes account per grade level. A sixth sync station in a grade level would require a new iTunes account because the previous account would have reached the five authorization limit. Therefore, if a school has six to ten classrooms in one grade level, it may be optimal to use one iTunes account for half of the sync stations and a second account for the other half to allow collaboration among instructors sharing each iTunes account.

Additionally, consider naming the email addresses that will be used to create iTunes accounts accordingly. The email address used to create the kindergarten iTunes account could be in the format of *school.itunes.k@xx.k12.xx.us,* the address used to create the 1st grade iTunes account may be in the format of *school.itunes.1st@xx.k12.xx.us* and so on, where *school* is replaced with the actual name or abbreviation of the school. Including the school name within the email address is helpful in large deployments where multiple schools cover the same grade levels. These email addresses are examples, so an alternate naming scheme may be used.

Designing iTunes Accounts for Department Use

Similar design considerations would apply to middle or high schools and higher education. However, in this environment the iTunes accounts would be built around the content areas or academic disciplines instead of grade levels. In a content area scenario, the email addresses used to create iTunes accounts may be in the format of *building.itunes.math@institution.edu,* where *building* is replaced with the actual name or abbreviation of the building. If more than five sync stations are needed in any given department, a number could be appended to the email address for the second account: *building.itunes.math2@institution.edu.* Embedding the building name within the email address is helpful in large deployments where multiple buildings cover the same content areas. These email addresses are examples, so an alternate naming scheme may be used.

Designing iTunes Accounts for School and Home Use

When centrally synced devices are assigned to students to take home, the devices need to be assigned to a sync station. In this scenario, the iTunes account design is more generic than the grade level or department designs. Students could be assigned to a sync station based on their last name, grade level, or other criteria the institution prefers.

The email address used to create the iTunes account for the building could be in the format of *school.itunes@xx.k12.xx.us,* where `school` is replaced with the actual name or abbreviation of the school. This iTunes account can then be authorized on a total of five sync stations to minimize the number of iTunes accounts per building. This email address is an example, so an alternate naming scheme may be used.

For example, if students will be assigned to sync stations based on their last names, consider provisioning a total of five sync stations authorized with the same iTunes account. Students with last names starting with A–E could be assigned to the first sync station, students with last names starting with F–J could be assigned to the second sync station, and so on. Once students are assigned to a sync station, they must continue to use that sync station to get new apps or updates, or the devices may be erased to sync with a new sync station and get different apps.

If more sync stations are needed, this design could be expanded by using more than one iTunes account.

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 at: http://support.apple.com/kb/HT1918

Managing Apps and Content

In the examples above, the sync station design matched the logical grouping of instructors. Additionally, if instructors participate in professional learning communities, they are likely to meet regularly to discuss student data. As discussions turn to what apps are most effective for a particular content area, instructors may benefit from quick access to the most appropriate apps.

The Home Sharing feature in iTunes can facilitate sharing of apps and content between sync stations using the same iTunes account.

Reminder: Verify volume licensing before syncing apps to devices.

- Learn more about Home Sharing in the Understanding iTunes section of this chapter.
- Learn more about volume licensing for syncing apps to multiple devices in the Purchasing Apps chapter of this document.

Implementing Centralized Sync

Implementing a centralized sync model requires that iTunes accounts be created using email addresses under the control of the education institution. Sync stations are strategically placed within the building or in carts and are authorized to use an iTunes account that is not tied to a credit card.

- Learn more about creating iTunes accounts without a credit card in the Understanding iTunes section of this chapter.
- Learn more about iTunes account strategies in the Understanding Sync Stations section of this chapter.

Configuring iTunes

Configure iTunes for optimal syncing with multiple devices prior to first use. In the General pane of iTunes preferences, deselect (if selected) the "Check for new software updates automatically" option. This will prevent software update messages from being displayed as each device is connected.

If end user data from iOS devices does not need to be regularly backed up by the sync station, automatic backups may be disabled.

Disable automatic backups by typing the following in Terminal:

```
defaults write com.apple.iTunes
AutomaticDeviceBackupsDisabled -bool true
```

This will continue to allow devices to sync, but they will not automatically back up. While automatic backups are disabled, all device backups must be performed manually.

Enable automatic backups by typing the following in Terminal:

```
defaults write com.apple.iTunes
AutomaticDeviceBackupsDisabled -bool false
```

After the iTunes sync stations have been configured, apps can be downloaded from the iTunes Store. The institution must already be enrolled in the App Store Volume Purchase Program, which is required for syncing apps to multiple institution-owned devices using one iTunes account.

- Learn more about purchasing and redeeming apps in the Purchasing Apps chapter of this document.

After all required apps have been redeemed and downloaded on the iTunes sync station, the master backup or backups can be created. A master backup acts as a template. To create a master backup, one iOS device is configured exactly the way you want all devices to be configured, and then a backup of that device is created with iTunes. Consult with the appropriate stakeholders to ensure the master backup meets curriculum and IT requirements.

- Learn more about backing up and restoring devices with iTunes in the Understanding iTunes section of this chapter.

Consider setting the restrictions passcode on the master device to prevent students from setting the code later or enabling device restrictions. Setting the restrictions passcode, preventing deletion of apps, disabling location services, and preventing modification of email accounts can only be done directly on the device, so these settings may be part of the master backup.

- Learn more about restrictions in the Configuration and Management chapter of this document.

After the master backup is made with iTunes, additional devices can be connected to the iTunes library and restored from the original backup. When new or not yet configured iOS devices are connected to the computer, iTunes displays a prompt to restore the device from a backup.

- Learn how to build a master backup in the Preparing a Sync Station section of this chapter.

Once the iOS device used to create the master backup is renamed, iTunes renames and replaces the original backup with personalized data from the new end user of the device. Therefore, the master backup may need to be recreated if there is reason to restore all devices synced to that iTunes library.

Alternatively, a copy of the master backup can be made for easy reuse. iTunes device backups are stored in ~/Library/Application Support/MobileDevice/Backup and can be copied to other locations. Making a copy of the master backup may make it easier to reuse that backup in the future. Consider designating a folder on the computer or an external volume to store copies of master backups. If any of these backups are needed, simply copy them back to the folder path listed above and overwrite the existing backup. This operation destroys the personalized backup data for the device used to create the master backup being copied.

Management and configuration tools can be used after each device has been restored from the master template. iPhone Configuration Utility can be used to install configuration settings and restrictions or a Mobile Device Management solution may be used for centralized wireless configuration and management.

If you want to restrict end users from installing additional apps on their iOS devices, consider setting the App Installation restriction. This restriction prevents all app installations, including using iTunes on the institution sync station. A Mobile Device Management solution can facilitate the process of changing the App Installation restriction on multiple devices at once.

- Learn more about restrictions in the Configuration and Management chapter of this document.

Preparing a Sync Station

Plan for scalability when designing and configuring sync stations. It is easier to deploy the first few sync stations if the long term goals are already known.

Before preparing a sync station, be sure to do the following:

- Learn more about iTunes accounts in the Understanding iTunes section of this chapter.
- Learn more about restrictions and configuration profiles in the Configuration and Management chapter of this document.

The steps below require a Mac that is connected to the school network and that has the latest versions of Mac OS X, iTunes, and iPhone Configuration Utility installed. The email address for the iTunes account should already have been created but not the iTunes account itself.

1. Create a new Mac OS X account for the sync station end user.
   a. Consider setting the Full Name to something easily readable by the end user (for example: 1st Grade Sync).
   b. Consider setting the Short Name to match the user name of the iTunes account email address (for example: school.itunes.1st).
2. Log in to the Mac using the Mac OS X account created in step 1.
3. Configure iTunes.
   a. Open iTunes and create a new iTunes account without a credit card using the email address created for it.
   b. Authorize iTunes to use this iTunes account by choosing Store > Authorize This Computer.
   c. Redeem apps purchased through the ASVPP and download required free apps.
   d. Add other media to the iTunes library such as audio, video, ePub documents, PDFs, or podcasts (if applicable).

      Reminder: Verify volume licensing before syncing apps to devices.
4. Build an iOS device master backup.
   a. Designate a device to build the master backup.
   b. Activate and name the device with iTunes (for example: 1st Grade Master iPad).
   c. Sync the device with iTunes to load desired content.
   d. Configure device settings and restrictions, such as app folders and Home screen icon layout (on the device or in iTunes), restrictions passcode (recommended), deleting the Apps restriction (if applicable), the Location restriction (if applicable), and the Accounts restriction (if applicable).
   e. Sync and then back up the device with iTunes.

The sync station has been configured and can now be deployed. The remainder of the devices for this cart can be restored from the master backup upon connection to iTunes. After a device is restored from the master backup, it can be renamed in iTunes and configuration profiles can be installed.

Preparing Multiple Sync Stations

If several sync stations will use the same iTunes account, perform the additional steps below. The additional sync stations must meet the same requirements as the initial sync station.

These instructions make use of Migration Assistant to create additional sync stations and have the same requirements as the Preparing a Sync Station procedure above.

Learn more about Migration Assistant at:
http://support.apple.com/kb/HT4413

On the initial sync station:

1. Enable Home Sharing in iTunes.
2. Open Migration Assistant.
3. Select To another Mac as the migration method and click Continue.

The initial sync station is ready to copy the Mac OS X user account containing the iTunes library content and device backups to the next sync station.

On the additional sync station:

1. Open Migration Assistant.
   a. Select From another Mac and then select Use Network if prompted.
   b. Back on the *initial* sync station, enter the code that appears on the additional sync station and click Continue.
   c. Click Continue and ensure only the Mac OS X user account created for the sync station end user is selected. This will begin the process.
4. Log in to the copied Mac OS X user account.
   a. Open iTunes and authorize the computer to use the same iTunes account as the initial sync station.
   b. Verify iTunes contains the same content and backups as the initial sync station.

Repeat the process above to add sync stations using the same iTunes account. Immediately following this process, all sync stations will have identical apps and content to sync with iOS devices. Afterwards, the sync stations can update apps and content independently of each other. Home Sharing in iTunes can be used to easily copy new and updated apps between sync stations.

Reminder: Verify volume licensing before syncing apps to devices.

- Learn more about Home Sharing in iTunes at:
  http://support.apple.com/kb/ht3819
- Learn more about volume licensing for syncing apps to multiple devices in the Purchasing Apps chapter of this document.

Repeat the Preparing a Sync Station and Preparing Multiple Sync Stations procedures for additional sync stations sharing a different iTunes account.

Planning for App and iOS Updates

Syncing, updating apps, and applying iOS updates for a large number of devices may become time consuming, so consider establishing a sync and upgrade schedule. For example, app or iOS updates could 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 will 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. Some app updates may require a newer iOS version, so do not postpone iOS upgrades indefinitely.

Adding a Personal iTunes Account on Each Device

Syncing with an institution's iTunes account allows an organization to ensure that a prescribed set of apps exists on all iOS devices. The end user may also be empowered to use his or her personal iTunes account to install apps directly on the iOS device after initially syncing with iTunes on the institution's sync station. Additional end user education may be required when a personal iTunes account is used in addition to an institution iTunes account.

Using an institution's iTunes account for syncing and a personal iTunes account to download additional apps directly on the device may be desirable because it allows institutions to purchase and retain ownership of apps while allowing end users to independently explore the App Store on their assigned iOS device.

Allowing end users to install personally purchased apps is more likely to give them a sense of ownership, so they may be more apt to protect their iOS device. This may be helpful in a model in which the devices are taken home, and the goal is to both guide and empower the end users. It may also be preferred for iOS devices provided to instructors and administrators.

- Learn more about changing the signed in iTunes Store account in iOS at: http://support.apple.com/kb/HT1311

Note the following caveats when adding a personal account directly on a device paired with an institution iTunes sync station:

Be sure to sync iOS devices with the institution's sync station before the end user signs in with his or her personal iTunes account directly on the device. If this order of operations is not followed, the iOS device may need to be erased before institution-owned apps can be installed.

Once the end user has downloaded apps on his or her personal account, the device will have apps belonging to two separate accounts. When updates for any of the apps become available, first connect the iOS device to the institution's sync station to download app updates for the institution iTunes account.

The sync station will present the end user with additional dialogs during the sync process. iTunes alerts the user that apps that are not authorized for that sync station cannot be transferred to it and user interaction is required to continue the sync process. Removing all personally purchased apps from the device or selecting the "Do not ask me again" checkbox in the iTunes prompt will eliminate these alerts. The end user can then update all remaining apps belonging to his or her personal iTunes account by using the App Store on the iOS device.

If the end user attempts to update all apps on the list at once, this may include apps belonging to the institution, in which case the user is prompted for the institution iTunes account password.

If an end user repeatedly attempts to use the institution iTunes account with an incorrect password, this may cause the account to be disabled due to excessive failed login attempts. Reactivating the account requires action from someone with access to the email address associated with the institution iTunes account. Educate end users on the app update workflow in this model to reduce the likelihood of this scenario.

- Learn more about activating disabled iTunes accounts at: http://support.apple.com/kb/TS2446

All app data will be backed up by the sync station regardless of which account was used to purchase the apps. If an iOS device is restored from a backup using iTunes on the institution's sync station, the user data from the personally owned apps is restored as well and is automatically available once the apps are re-downloaded directly on the

device using the personal account. Until the personally purchased apps are re-downloaded to the device, the data from those apps can be overwritten if available storage on the device becomes low.

- Learn about using multiple computers to manage music at: http://support.apple.com/kb/HT1202

Finally, when syncing to the institution's iTunes account and then using a personal account directly on the device, the only way to sync to a different computer is to erase the apps and content synced by the institution's sync station. Users should not sync with iTunes on their personal computer if the device is already syncing to an institution sync station.

Choosing a Sync Strategy

A sync strategy should be developed before the rollout begins. The questions below form a basic decision tree to assist in selecting a sync strategy. Select the model or models that meet the most requirements and keep in mind that multiple strategies may be used across an organization.

Application Installation: Who will be allowed to install apps?

- School only: Consider a centralized sync strategy.
- Student only: Consider a personal sync strategy.
- Both: Consider a centralized sync strategy and using a personal iTunes account directly on the iOS device.

Application Updates and Deletions: Are applications allowed to be modified and new ones installed?

Yes: Consider any sync strategy.

No: Consider a centralized sync strategy.

Device Update Frequency: How often should apps or iOS versions be updated on the devices?

- Frequently: Consider a personal sync strategy.
- Infrequently: Consider a centralized sync strategy only or consider a centralized sync strategy and using a personal iTunes account on the iOS device.

iTunes Syncing, Backup, and Restore: Which computer will be used for syncing and backups?

- School-owned: Consider any sync strategy.
- Student-owned: Consider a personal sync strategy.

Troubleshooting Resources

- Learn about troubleshooting steps for iPhone at: www.apple.com/support/iphone
- Learn about troubleshooting steps for iPad at: www.apple.com/support/ipad
- Learn about troubleshooting steps for iPod touch at: www.apple.com/support/ipodtouch
- Learn about troubleshooting steps for iTunes at: 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 understanding AppleCare support plans, Apple Education Professional Services, Apple Professional Development, available Apple factory services, researching apps, preparing a secure staging area for rollouts, and firewall considerations.

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 Mobile 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 App Store 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 three ways to configure and manage iOS devices: manually configuring devices, deploying configuration profiles using iPhone Configuration Utility (iPCU), and using a Mobile Device Management (MDM) solution. Understand how each configuration and management option may be used prior to deployment.

Sync Strategies

There is no one-size-fits-all approach for syncing. Determining who will own purchased apps and content should shape the sync strategy that may include a personal sync model, a centralized sync model, or a centralized sync model using personal accounts directly on the devices. Developing a sync strategy may be the most critical part of an iOS deployment.

Appendix A—Wi-Fi Standards

This section 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 this section includes a summary of the standards.

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 designing for a high density of devices in an enclosed space, such as in classrooms. The number of channels available in the 5GHz band varies among vendors of access points and from country to country, but at least eight channels will always be available.

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

IEEE 802.11b/g

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

802.11b provides data transfer speeds of up to 11Mbps, while 802.11g provides data transfer speeds 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 data 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 laptops support this band, but many smaller mobile devices only support 2.4GHz Wi-Fi.

Transfer speeds 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 speeds of up to 600Mbps. To accomplish this task, several technologies are utilized.

802.11n can utilize 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 multi-radio 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 to support this technology. Mac products support MIMO while iOS devices do not.

HD40, commonly referred to as wide or bonded channels, 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. Many access point vendors do not allow HD40 when using the 2.4GHz band because only three non-overlapping channels are available. iOS devices support HD20 while Mac products support HD40.

Wi-Fi Standards Support 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 actual data rate at which 802.11n devices can communicate. See the MCS index table listed later in this appendix for more information.
- Wide channels: HD20 or HD40.
- Guard interval (GI): The guard interval is the space (time) between symbols or characters of information 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 4

802.11n @ 2.4GHz

802.11 b/g

MCS Index 7 / HD20 / 800ns GI

iPad and iPad 2

802.11n @ 2.4GHz and 5GHz

802.11a/b/g

MCS Index 7 / HD20 / 800ns 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 MacBook Pro only)

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.

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 utilizes 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 at: www.apple.com/support/bonjour