iOS Enterprise Deployment Overview

iOS devices such as iPad and iPhone can transform your business. They can significantly boost productivity and give your employees the freedom and flexibility to work in new ways, whether in the office or on the go.

There are several possible ways to deploy these devices in your organization. Whether you choose to deploy company-owned iOS devices or institute a "bring your own device" (BYOD) policy, it's helpful to consider the steps you'll need to take to ensure that your deployment goes as smoothly as possible.

This document offers guidance on some important considerations for getting the most out of your iOS deployment. You'll need to think about the following:

- **Prepare your infrastructure.** Review your existing infrastructure to make sure it supports iOS devices. iPhone and iPad integrate seamlessly into most standard enterprise IT environments. However, there may be ways to optimize your network environment to support key technologies in iOS.
- **Set up devices.** Consider how you will distribute and set up devices. There are several options—from pre-configuration to employee self-service setup. Explore the possibilities before you get started.
- **Configure and manage devices.** After the initial setup, think about how you'll configure and manage devices on an ongoing basis. With proactive planning and iOS management technologies, you can ensure a baseline of security and control that's seamless and transparent to users.
- **Deploy apps and content.** Keep your users productive and creative with relevant iOS apps and content. With advance planning, you can simplify deployment and deliver apps and content directly to employees' devices over-the-air.
- **Plan for support.** Consider the options for supporting employees with iOS devices. Apple offers several options for support so that you can scale your deployment without additional impact on your IT team.

Prepare Your Infrastructure

As you prepare to deploy iOS devices, evaluate your existing network infrastructure to make sure your organization takes full advantage of everything that iOS offers.

Wi-Fi and networking

Consistent and dependable access to a wireless network is critical to setting up and configuring iOS devices. Confirm that your company's Wi-Fi network can support multiple devices with simultaneous connections from all your users. You may need to configure your web proxy or firewall ports if devices are unable to access Apple's activation servers, iCloud, or the iTunes Store.

Evaluate your VPN infrastructure to make sure users can securely access company resources remotely via their iOS devices. Consider using the VPN On Demand feature of iOS so that a VPN connection is initiated only when needed. If you plan to use per-app VPN, make sure that your VPN gateways support these capabilities, and that you purchase sufficient licenses to cover the appropriate number of users and connections.

You should also make sure that your network infrastructure is set up to work correctly with Bonjour, Apple's standards-based, zero-configuration network protocol. Bonjour enables devices to find services on a network automatically. iOS devices use Bonjour to connect to AirPrint compatible printers and AirPlay compatible devices such as Apple TV. Some apps also use Bonjour to discover other devices for collaboration and sharing.

For more detail on Wi-Fi and networking for enterprise deployments, see the *iOS Deployment Technical Reference*. Appendix A, "Wi-Fi Infrastructure," explains the wireless technologies and standards used by iOS devices, and provides information on designing wireless networks.

Download the iOS Deployment Technical Reference at
www.apple.com/ipad/business/it/deployment.html

Learn more about Bonjour at
www.apple.com/support/bonjour

Mail, calendar, and contacts

If you use Microsoft Exchange, verify that the ActiveSync service is up to date and configured to support all users on the network. If you're using the cloud-based Office 365, ensure that you have sufficient licenses to support the anticipated number of iOS devices that will be connected. If you don't use Exchange, iOS also works with standards-based servers including IMAP, POP, SMTP, CalDAV, CardDAV, and LDAP.

Mobile device management

To wirelessly configure and manage iOS devices, you'll need a mobile device management (MDM) solution. MDM gives organizations the ability to securely enroll devices in the corporate environment, wirelessly configure and update settings, monitor policy compliance, deploy apps, and remotely wipe or lock managed devices.

Several MDM solutions are available to support different server platforms. Each solution offers different management consoles, features, and pricing. Before choosing a solution, refer to the resources listed below to evaluate which MDM features are most relevant to your organization.

In addition to third-party solutions, Apple offers an MDM solution called Profile Manager, a feature of OS X Server. Profile Manager makes it easy to configure iOS devices so they're set up to your organization's specifications. Profile Manager provides three components: a web-based administration tool, a self-service user portal for enrolling devices and downloading configuration profiles, and a mobile device management server.

Learn more about mobile device management (MDM) at
www.apple.com/ipad/business/it/management.html

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

Caching Server

Caching Server is an integrated feature of OS X Server that saves previously requested content, like documents, apps, and books. This helps minimize bandwidth needed to the Internet by hosting content locally. Caching Server speeds up the download and delivery of software through the App Store, Mac App Store, iTunes Store, and iBooks Store. It can also cache software updates for faster downloading to iOS devices.

Learn more about Caching Server at
www.apple.com/osx/server/features/#caching-server

Supporting iTunes

iTunes isn't required for devices with iOS 5 or later, but you may want to support it so users can activate devices, sync media, or back up their devices to a computer.

iTunes supports several deployment configuration options that are appropriate for enterprise use, including disabling access to explicit content, defining which network services users can access within iTunes, and determining whether new software updates are available for users to install.

Learn more about deploying iTunes at
help.apple.com/iosdeployment/itunes

Set Up Devices

After preparing your infrastructure, it's time to plan how you'll deploy iOS devices. Device distribution and setup can be approached in several ways, depending on who owns the device and the preferred deployment scenario.

Deployment scenarios

Personalized device (BYOD). With a bring-your-own-device deployment, the most common scenario is to let users set up their own personal devices using their own Apple IDs. To gain access to corporate resources, users can configure settings manually, install a configuration profile, or more commonly, enroll the device with the organization's MDM solution.

An advantage of using MDM to enroll personal devices is that it allows corporate resources to be kept separate from the user's personal data and apps. IT can enforce settings, monitor corporate compliance, and remove corporate data and apps while leaving personal data and apps on each user's device.

Personalized device (corporate-owned). The personalized device model can also be used when deploying iOS devices that are owned by the organization. IT can configure the device with basic settings before giving it the user, or (as with BYOD) provide instructions or configuration profiles for users to apply themselves.

Alternately, you can have users enroll the device with an MDM solution that provides organizational settings and apps over the air. Once configured, users can personalize the device with their own apps and data, which remain separate from any managed apps the organization provides.

Non-personalized device (shared device). When devices are shared by several people or used for a single purpose (such as in a restaurant or hotel), they are typically configured and managed by an IT administrator rather than an individual user. With a non-personalized device deployment, users generally do not store personal data or have the ability to install apps.

Non-personalized devices are usually supervised with Apple Configurator and enrolled with an MDM solution. This allows the content on the device to be refreshed or restored if modified by a user.

Setup Assistant

Out of the box, iOS users can activate their device, configure basic settings, and start working right away with Setup Assistant in iOS. Beyond basic settings, users can customize their personal preferences like language, location, Siri, iCloud, and Find My iPhone. Setup Assistant also enables the user to create a personal Apple ID if they do not have one already.

Apple ID

An Apple ID is an identity that is used to log in to various Apple services such as FaceTime, iMessage, the iTunes Store, App Store, iBooks Store., and iCloud. These services give users access to a wide range of content to streamline business tasks, increase productivity, and support collaboration.

In order to get the most out of these services, users should use their own Apple ID. If they do not have one, they can create one even before they are provided a device so that configuration can be as quick as possible. In a shared device deployment, when devices are not personalized by the user, a single Apple ID can be used with Apple Configurator to install apps and content on multiple devices.

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

iCloud

iCloud allows users to automatically sync documents and personal content such as contacts, calendars, documents, and photos, and keep them up to date between multiple devices. Users can also back up an iOS device automatically when connected to Wi-Fi and use Find My iPhone to locate a lost or stolen iPhone, iPad, iPod touch, or Mac.

Some services such as Photo Stream, iCloud Keychain, Documents in the Cloud, and Backup can be disabled through the use of restrictions either entered manually on the device or set via configuration profiles. An MDM solution can also prevent managed apps from being backed up to iCloud. This gives users the benefits of using iCloud for personal data while keeping corporate information from being stored in the cloud. Data from corporate accounts such as Exchange, or enterprise in-house apps are not backed up to iCloud.

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

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

Configure and Manage Devices

IT administrators can configure iOS device settings and accounts manually, or over-the-air with mobile device management (MDM) solution. Depending on who owns the devices and how they're deployed, several different configuration workflows and capabilities are possible.

Managed and unmanaged devices

By default, all iOS devices are unmanaged—that is, they are not enrolled in an MDM solution. Unmanaged devices can be configured manually or with configuration profiles installed by the user. Policy enforcement, if any, often comes from Exchange ActiveSync. Exchange ActiveSync also provide the capability to remotely wipe devices of all data.

Alternatively, managed devices are enrolled in an MDM solution and have more comprehensive controls and tools for IT to administer devices over time.

Configuration profiles

A configuration profile is an XML file that allows you to distribute configuration information to an iOS device. Configuration profiles automate the configuration of settings, accounts, restrictions, and credentials. Configuration profiles can be installed through an email attachment, downloaded from a web page, or installed on devices

through Apple Configurator. If you need to configure a large number of devices, or just prefer a low-touch over-the-air deployment model, you can deliver configuration profiles through MDM.

Configuring devices with mobile device management (MDM)

MDM gives organizations the ability to securely enroll personally owned and company-owned devices in an enterprise environment. With an MDM solution in place, IT administrators can configure and update settings, monitor compliance with corporate policies, and remotely wipe or lock managed devices. MDM also enables distribution, management, and configuration of apps purchased through the Volume Purchase Program or developed in-house.

To enable management, devices are enrolled with an MDM server using an enrollment configuration profile. This can be done by the user directly, or for company-owned devices, MDM enrollment can be automated using the Device Enrollment Program (described below). When an administrator initiates an MDM policy, option, or command, the iOS device receives notification of the action via the Apple Push Notification service (APNs). With a network connection, devices can receive APNs commands anywhere in the world.

Supervised devices

To enable additional configuration options and restrictions, you may choose to supervise iOS devices owned by your organization. For example, supervision gives you the ability to disallow modification of account settings, or lets you filter web connections via Global Proxy to make sure users' web traffic stays within the corporate network.

By default, all iOS devices are non-supervised. You can combine supervision with remote management via MDM to manage additional settings and restrictions. To enable supervision of your organization's devices, use Apple's Device Enrollment Program or Apple Configurator.

Device Enrollment Program

The Device Enrollment Program (DEP) enables organizations that have purchased iOS devices directly from Apple to easily set up, configure, and supervise devices wirelessly. With the Device Enrollment Program, all of your devices can be properly configured without the need for staging services that prep devices before users get them.

The process is simple: After enrolling in the program, administrators log into the program website, link the program to their MDM server, and "claim" the iOS devices purchased through Apple. The devices can then be assigned to users via MDM. Once a user has been assigned, any MDM-specified configurations, restrictions, or controls are automatically installed.

Learn more about the Device Enrollment Program at
www.apple.com/ipad/business/it/management.html

Apple Configurator

Apple Configurator is a free application for OS X available from the Mac App Store. It enables administrators to set up and configure multiple iOS devices at a time via USB before they are provided to users. With this tool, your enterprise can quickly configure and update multiple devices to the latest version of iOS, configure device settings and restrictions, and install apps and content.

Apple Configurator is ideal for scenarios where users share iOS devices that need to be quickly refreshed and kept up to date with the correct settings, policies, apps, and

data. Apple Configurator can also be used to supervise a device prior to using MDM to manage settings, policies and apps.

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

Deploy Apps and Content

There are a number of ways of deploying apps to iOS devices throughout your enterprise. You can purchase and assign apps with MDM through the Volume Purchase Program (VPP), or create and deploy your own in-house apps by joining the iOS Developer Enterprise Program. Additionally, if you are in a shared-device deployment scenario you can install apps and content locally with Apple Configurator.

Volume Purchase Program

The Volume Purchase Program (VPP) allows businesses to purchase iOS apps and books in volume and distribute them to employees. You can also get custom B2B apps for iOS that are built uniquely for you by third-party developers and procured privately through the VPP store.

MDM solutions integrate with VPP and can be used to assign apps and books to users. When apps are no longer needed, MDM can be used to revoke and reassign them to a different user. Each app is automatically available for download on all the user's devices, with no additional effort or cost to you.

Redemption codes can also be purchased through VPP for use with Apple Configurator, or in situations where MDM is not applicable.

Learn more about the Volume Purchase Program at
www.apple.com/business/vpp

Enterprise in-house apps

Develop iOS apps for use by your company using the iOS Developer Enterprise Program. This program offers a complete and integrated process for developing, testing, and distributing your iOS apps to employees within your organization.

Distributing in-house apps can be done either by hosting your app on a simple web-server you create internally, or by using a third-party MDM or app management solution. The benefits of managing in–house apps with MDM include the ability to configure apps remotely, manage versions, configure single sign on, set policies for network access such as per app VPN, and control which apps can export documents. Your specific requirements, infrastructure and level of app management will dictate which solution makes the most sense for you.

Installing apps with Apple Configurator

In addition to basic setup and configuration capabilities, Apple Configurator can be used to install apps and content. This is most likely when Apple Configurator is being used to supervise a device and therefore will not be personalized by the user. When you configure devices with Apple Configurator, you can install free apps, paid apps using Volume Purchase Program (VPP) codes, enterprise apps, and documents. You can also retrieve documents from assigned iOS devices. Retrieving and updating documents uses the same process as sharing documents by importing from and exporting to iTunes.

Plan for Support

Apple provides a variety of programs and support options for iOS users. Before deploying devices, find out what's available for your institution and plan for any support you will need.

AppleCare OS Support

AppleCare OS Support includes AppleCare Help Desk Support in addition to incident support. This includes support for system components, network configuration, and administration; integration into heterogeneous environments; professional software applications, web applications, and services; and technical issues requiring the use of command-line tools for resolution.

AppleCare Help Desk Support

AppleCare Help Desk Support provides priority access to Apple's senior technical support staff by telephone. It also includes a suite of tools to diagnose and troubleshoot Apple hardware, which can help large organizations manage their 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 iOS devices.

AppleCare for iOS device users

Every iOS device comes with a one-year limited warranty and complimentary telephone technical support for 90 days after the purchase date. This service coverage can be extended to two years from the original purchase date with AppleCare+ for iPhone, AppleCare+ for iPad, or the AppleCare Protection Plan (APP) for iPod touch. You can call Apple's technical support experts as often as you like with questions. Apple also provides convenient service options when devices need to be repaired. In addition, AppleCare+ for iPhone and AppleCare+ for iPad offer up to two incidents of accidental damage coverage, each subject to a service fee.

iOS Direct Service Program

As a benefit of AppleCare+ and the AppleCare Protection Plan, the iOS Direct Service Program enables your help desk to screen devices for issues without calling AppleCare or visiting an Apple Store. If necessary, your organization can directly order a replacement iPhone, iPad, iPod touch, or in-box accessories.

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

Summary

Whether your company deploys iOS devices to a group of users or across the organization, there are many options to easily deploy and manage these devices. Choosing the right strategies for your organization can help your employees be more productive and accomplish their work in entirely new ways.

Learn more about integrating iOS into enterprise IT environments at
www.apple.com/ipad/business/it

For more detailed technical information about deploying iOS, download the iOS Deployment Technical Reference at
www.apple.com/ipad/business/it/deployment.html