iOS Enterprise Deployment Overview

iPad and iPhone can transform your business and how your employees work. They can significantly boost productivity and give your employees the freedom and flexibility to work in new ways. Embracing this new way of working benefits the entire organization. Users have better access to information, so they feel empowered and are able to creatively solve problems. By supporting iOS, IT departments can give users access to the best tools to do their work while also safely protecting corporate data. Ultimately everyone benefits, with a reinvigorated workforce and new business opportunities everywhere.

This document offers guidance on important considerations for getting the most out of your iOS deployment and covers the following topics:

- Deployment models
- Prepare your infrastructure
- Initial setup
- Configure and manage
- Distribute apps and books
- Ongoing management
- Support options

Deployment Models

Evaluating deployment models and choosing the one that's right for your organization is an important first step. You can approach deployment in several ways, depending on who owns the device and your preferred scenario. Start by evaluating and identifying the best deployment models for your organization.

There are three common deployment scenarios for iOS devices in the enterprise:

- Personalized device (BYOD)
- Personalized device (corporate-owned)
- Non-personalized device (shared)

While most organizations have a preferred model, you may encounter multiple models in your own environment. For example, a retail company may deploy a personalized device (BYOD) strategy by allowing employees to set up a personal iPad while keeping corporate resources protected and managed without impacting the user's personal data and apps. However, their retail stores may also deploy a non-personalized device (shared device) strategy allowing iPads to be shared by several employees in order to process transactions for customers.

Exploring these models in more detail will help you identify the best deployment model for your unique environment, following which you can select the appropriate programs and tools in the online iOS Deployment Technical Reference.

iOS Deployment Technical Reference: https://help.apple.com/deployment/ios

Personalized device (BYOD)

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

An advantage of using MDM to enroll personal devices is that it allows corporate resources and data to be managed in a way that is secure, yet also respectful of the user's personal privacy, 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 intact.

The following table illustrates the responsibilities of both the administrator and the user for a personalized device (BYOD) deployment:

Prepare your infrastructure	
Administrator: • Evaluate your existing infrastructure including Wi-Fi, VPN, mail, calendar servers. • Investigate, procure, and deploy an MDM solution, such as Profile Manager. • Sign up for Volume Purchase Program (VPP).	**Users:** • Unbox and activate the device. • Create an Apple ID, which can also be used for your iTunes Store and iCloud accounts, if applicable.
Set up and configure	
Administrator: • Enroll devices using self-service; configure accounts, settings, and restrictions wirelessly using MDM based on user/group policies defined by your institution. • Alternatively, organizations can provide settings for individual accounts to users, and policies can be pushed with Exchange or installed using a configuration profile.	**Users:** • Enroll in MDM. • Device settings and configurations are automatically received from MDM. • Alternatively, users can install configuration profiles manually or configure settings as provided by you.
Distribute apps and books	
Administrator: • Purchase apps and books with VPP and assign them to users with MDM. • Send VPP invitation to users. If you use redeemable codes, distribute using mail or an internal website. • Distribute in-house apps from the iOS Developer Enterprise Program (iDEP) and in-house books by hosting them on a web server or your MDM solution. • Install Caching Server to speed up content delivery over the local network.	**Users:** • Accept invitation to VPP. • Download and install apps and books assigned by the institution.
Ongoing management	
Administrator: • Revoke and reassign apps to other users as needed with MDM. • With MDM, an administrator can query managed devices to monitor compliance, or trigger alerts if users add unapproved apps or content. • MDM can also lock devices or reset device passwords, remotely wipe any managed accounts or data, or wipe a device entirely.	**Users:** • Back up the device to iTunes or iCloud, to save documents and other personal content. • If the device is lost or stolen, the user can locate it with Find My iPhone. • When the MDM relationship is removed, managed accounts and data are removed, but the user's personal apps, books, data, and content are kept.

Personalized device (corporate-owned)

You can also use the personalized device model when deploying iOS devices that are owned by your organization. IT can configure devices with basic settings before giving them to users, or (as with BYOD) provide instructions or configuration profiles for users to apply themselves.

Alternatively, you can have users enroll the device with an MDM solution that provides organizational settings and apps over-the-air. For devices purchased directly from Apple, you can also take advantage of the Device Enrollment Program (DEP) to automatically enroll new devices into your MDM solution. Once configured, users can personalize the device with their own apps and data in addition to any corporate account or apps provided by the organization.

The following table illustrates the responsibilities of both the administrator and the user for a personalized device (corporate-owned) deployment:

Prepare your infrastructure	
Administrator: • Evaluate your existing infrastructure including Wi-Fi, VPN, and mail and calendar servers. • Investigate, procure, and deploy an MDM solution, such as Profile Manager. • Sign up for DEP and VPP.	**Users:** • Create an Apple ID, which can also be used for your iTunes Store and iCloud accounts, if applicable.
Set up and configure	
Administrator: • From the Device Enrollment Program website, link your servers to your MDM solution. • Streamline enrollment through Device Enrollment Program by assigning devices to your MDM servers by order number or by serial number. • Assign devices in DEP for supervision and streamlined enrollment in MDM. • Use Apple Configurator to configure and supervise the device (alternative to the above). • Configure and install accounts, settings, and restrictions wirelessly with MDM or use USB with Apple Configurator.	**Users:** • The user is provided an iOS device. If Apple Configurator was used to setup the device, then no further setup by the user is necessary. • Enter institution credentials in Setup Assistant for DEP (optional). • Personalize the device with Setup Assistant and enter a personal Apple ID. • Enroll in MDM. • Device settings and configurations are automatically received from MDM.
Distribute apps and books	
Administrator: • Purchase apps and books with VPP and assign them to users with MDM. • Download your token from the VPP Store and link it to your MDM solution. • Send VPP invitation to users. If you use redeemable codes, distribute using mail or an internal website. • Distribute in-house apps from the iOS Developer Enterprise Program (iDEP) and in-house books by hosting them on a web server or your MDM solution. • Install Caching Server to speed up content delivery over the local network.	**Users:** • Accept invitation to VPP. • Download and install apps and books assigned by the organization. • Apps can be installed on the user's device automatically.

Ongoing management	
Administrator:	**Users:**
• Revoke and reassign apps to other users as needed with MDM. • With MDM, an administrator can query managed devices to monitor compliance, or trigger alerts if users add unapproved apps or content. • MDM can also lock devices or reset device passwords, remotely wipe any managed accounts or data, or wipe a device entirely.	• Back up the device to iTunes or iCloud, to save documents and other personal content. • If the device is lost or stolen, the user can locate it with Find My iPhone.

Non-personalized device (shared)

When devices are shared by several people or used for a single purpose (for example, in a restaurant or hotel), typically IT administrators configure and manage them centrally rather than relying on an individual user to perform the setup. With a non-personalized device deployment, users generally aren't permitted to install apps or store any personal data on the device.

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

The following table illustrates the responsibilities of both the administrator and the user for a non-personalized device (shared) deployment:

Prepare your infrastructure	
Administrator:	**Users:**
• Evaluate your existing infrastructure including Wi-Fi, VPN, and mail and calendar servers. • Investigate, procure, and deploy an MDM solution, such as Profile Manager. • Sign up for the Volume Purchase Program (VPP).	• No action necessary at this stage.
Set up and configure	
Administrator:	**Users:**
• Unbox and (optionally) asset tag the device. • Use Apple Configurator to configure and supervise the devices. • Use Apple Configurator to enroll devices in MDM (optional). • Use Apple Configurator or MDM to install accounts, settings, and restrictions.	• No action necessary at this stage.
Distribute apps and books	
Administrator:	**Users:**
• Purchase apps and books with VPP and deploy them using redemption codes for installation and management with Apple Configurator. • Distribute in-house apps from the iOS Developer Enterprise Program (iDEP) using Apple Configurator. • Distribute in-house books by hosting them on a web server or your MDM solution. • Add Apple Configurator for book just like apps.	• No action necessary at this stage.

Ongoing management	
Administrator: • Update iOS on the device with Apple Configurator. • Periodically reset devices to standard configuration using Apple Configurator. • With MDM, you can query managed devices to monitor compliance, or trigger alerts if users add unapproved apps or content. • MDM can also lock devices or reset device passwords, remotely wipe any managed accounts or data, or wipe a device entirely. • Regular backup of the Mac running Apple Configurator is necessary, because VPP purchases are managed locally. • MDM can supervise devices using single app mode.	**Users:** • No action necessary at this stage.

Prepare Your Infrastructure

After choosing the right deployment models, review your existing infrastructure to make sure your organization takes full advantage of everything that iOS offers. 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.

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.

Access the iOS Deployment Technical Reference on the web: www.help.apple.com/deployment/ios

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

Mail, contacts, calendars

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 (MDM)

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 books, and remotely wipe or lock managed devices.

A variety of third-party MDM solutions are available to support different server platforms. Each solution offers different management consoles, features, and pricing. Before choosing a solution, review the resources listed below to evaluate which management 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 an MDM server.

Learn more about mobile device management: www.apple.com/ipad/business/it/management.html

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

Caching Server

An integrated feature of OS X Server, Caching Server stores a local copy of frequently requested content from Apple servers, helping to minimize the amount of bandwidth needed to download content on your network. 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: 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: help.apple.com/iosdeployment/itunes

Initial Setup

After preparing your infrastructure, you'll need to deploy iOS devices to your users. You can approach initial device setup in several ways, depending on who owns the device and your preferred deployment model. Explore the possibilities before you get started.

Setup Assistant

Out of the box, users can activate their devices, configure basic settings, and start working right away with Setup Assistant in iOS. Beyond being able to choose basic settings, users can also customize their personal preferences, like language, location, Siri, iCloud, and Find My iPhone. Setup Assistant also enables users to create a personal Apple ID if they don't have one. When devices are enrolled in the Device Enrollment Program (DEP) they can be automatically enrolled in MDM right within the Setup Assistant.

Configuring devices with Apple Configurator

If devices in your organization are centrally managed by IT and not set up by individual users, you can use Apple Configurator to quickly activate devices, define and apply configurations, supervise devices, install apps, and update devices to the latest iOS version. Apple Configurator is a free application for

OS X, available for download from the Mac App Store. Devices need to be connected to a Mac via USB to perform these tasks. You can also restore a backup to devices, which installs app data and applies device settings and Home screen layout.

Apple ID

An Apple ID is an identity that's 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 for streamlining business tasks, increasing productivity, and supporting collaboration.

To get the most out of these services, users should use their own Apple IDs. If they don't have one, they can create one even before they receive a device or use the Setup Assistant built into iOS. This gives users an easy and streamlined way to create an Apple ID right from their iOS devices. Users do not need a credit card to create an Apple ID.

When devices are not personalized by users, as in a shared-device deployment, Apple Configurator can install apps and content on multiple devices using a single administrator's Apple ID.

Learn how to sign up for an Apple ID: 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, iCloud Drive, 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 preventing corporate information from being stored in iCloud. Data from corporate accounts, such as Exchange, or data stored within enterprise in-house apps is also not backed up to iCloud.

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

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

Configure and Manage

Once devices are set up for initial use, there are multiple options for configuring and managing access to corporate services. IT can either distribute configuration profiles or set up devices over the air with MDM. Additional configuration options are available for supervised devices.

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 and configure personally owned and corporate-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 and books 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. Users can enroll themselves directly, or for corporate-owned devices, you can automate MDM enrollment using the Device Enrollment Program. 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

Supervision provides a higher level of device management for devices that your organization owns, allowing additional restrictions, such as turning off iMessage or Game Center or preventing users from modifying account settings. By default, all iOS devices are non-supervised. You can combine supervision with remote management via MDM to manage additional settings and restrictions. Using the Device Enrollment Program, supervision can be wirelessly enabled on the device as part of the setup process, or enabled using Apple Configurator.

Device Enrollment Program

The Device Enrollment Program (DEP) enables organizations that have purchased iOS devices directly from Apple to easily enroll devices in MDM and set up, configure, and supervise devices wirelessly. With the Device Enrollment Program, all your devices can be configured without having to touch each individual device.

The process is simple: after enrolling in the program, administrators log in to the program website, link the program to their MDM server, and assign devices to users. Once users are assigned, they can go through the Setup Assistant on their devices and any MDM-specified configurations, restrictions, or controls are automatically installed.

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

Apple Configurator

Apple Configurator—a free OS X application, available from the Mac App Store—enables administrators to set up and configure multiple iOS devices at once via USB before providing them to users. With this tool, your IT staff 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 in which users share iOS devices that need to be refreshed and kept up to date with the correct settings, policies, apps, and data. Prior to using MDM to manage settings, policies, and apps, you can use Apple Configurator to enable device supervision, which provides additional restrictions and controls.

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

Distribute Apps and Books

Apple offers extensive programs to help your organization take advantage of the great apps and content available for iOS. With these capabilities, you can deliver apps and content directly to employees' devices over the air and provide them with everything they need to be productive.

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. Developers registered in the iOS Developer Enterprise Program can submit apps for B2B distribution using iTunes Connect, the same process used to submit other apps to the App Store.

MDM solutions integrate with VPP and can be used to assign apps and books to users. When apps are no longer needed by a particular user, you can use MDM 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. You can also purchase redemption codes through VPP for use with Apple Configurator or if MDM isn't applicable.

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

iOS Developer Enterprise Program

Develop in-house 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. In-house apps are not submitted to the App Store and are not reviewed, approved, or hosted by Apple.

You can distribute in-house apps either by hosting your app on a simple internal web server 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.

To develop and deploy in-house apps for iOS, learn more about the iOS Developer Enterprise Program: developer.apple.com/programs/ios/enterprise/

Distributing apps and books with managed distribution

MDM servers can deploy both App Store apps and in-house enterprise apps to devices over the air. Both paid and free App Store apps can be managed by an MDM server using VPP managed distribution. See "Volume Purchase Program" above for more information about managed distribution with MDM.

You can install apps purchased through VPP three different ways. Users with a personal device are prompted by MDM to install the app from the App Store using an Apple ID. With a supervised device that's enrolled with MDM, app installation occurs automatically. And if a device is not associated with MDM, users install paid apps via a redemption code; the app then becomes associated with each user's personal Apple ID.

Installing apps and content with Apple Configurator

In addition to basic setup and configuration, you can also use Apple Configurator to install apps and content. This would most likely be in situations where Apple Configurator is supervising a device that won't be personalized by the user. When you configure devices with Apple Configurator, you can install free apps, paid apps using VPP codes, in-house 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.

Ongoing Management

Once your users are up and running there are a wide range of administrative capabilities available to manage devices throughout the life cycle. This includes querying devices for information, initiating security commands, such as a remote wipe, and performing specific tasks related to apps.

Queries

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

Commands

When a device is managed, an MDM server can perform a wide variety of administrative commands, including changing configuration settings automatically without user interaction, locking or wiping a device remotely, or clearing the passcode lock so users can reset forgotten passwords. An MDM server can also request an iOS device to begin AirPlay mirroring to a specific destination or end a current AirPlay session.

Managed apps

Organizations often need to distribute apps so their users are productive at work. At the same time, organizations need to control how those apps connect to internal resources or how data security is handled when a user transitions out of the organization. Managed apps in iOS allows an organization to distribute free, paid, and enterprise apps over the air using MDM, while also providing the right balance between protection of corporate data and protection of the user's personal apps and data.

Managed apps can be removed remotely by an MDM server or when users remove their own devices from MDM. Removing the app also removes the data associated with the app. If an app remains assigned to a user through VPP or the user redeemed an app code using a personal Apple ID, the app can be downloaded again from the App Store, but will not be managed by MDM.

iOS and your MDM solution provide additional capabilities to manage apps, improve security, and deliver a better user experience:

- **Managed open in.** This restriction protects corporate data by controlling which apps and accounts are used to open documents and attachments. IT organizations can configure a list of apps available in the sharing panel to keep work documents in corporate apps and prevent personal documents from being opened in managed apps. This policy also applies to third-party document providers and third-party keyboard apps in iOS 8.
- **App configuration.** App developers can identify app settings that can be enabled when installed as a managed app. These configuration settings can be installed before or after the managed app is installed. For example, IT can establish a set of default preferences for a Sharepoint app so the user doesn't need to manually configure server settings.
- **Single app mode.** Helps the user stay focused on a task while using an iOS device. This setting limits an iOS device to a single app. Developers can also enable this functionality within their apps so that apps can enter and exit single app mode independently.
- **Prevent backup.** This restriction prevents managed apps from backing up data to iCloud or iTunes. Disallowing backup prevents managed app data from being recovered if the app is removed via MDM but later reinstalled by the user.

Support Options

Apple provides a variety of programs and support options for iOS users and IT administrators.

AppleCare OS Support

AppleCare OS Support provides your IT department with enterprise-level phone and email support for iOS, OS X, and OS X Server deployments. With direct access to technicians for questions on integration, migration, and advanced server operation issues, AppleCare OS Support can increase your IT staff's efficiency in deploying and managing devices and resolving issues.

AppleCare Help Desk Support

AppleCare Help Desk Support provides priority telephone access to Apple's senior technical support staff. It also includes a suite of tools to diagnose and troubleshoot Apple hardware, which can help 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: www.apple.com/support/products

Summary

Whether your company deploys iOS devices to a group of users or across the entire organization, there are many options to easily deploy and manage 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: www.apple.com/ipad/business/it

For more detailed technical information about deploying iOS, access the iOS Deployment Technical Reference at https://help.apple.com/deployment/ios

*Some features require a Wi-Fi connection. Some features are not available in all countries. Access to some services is limited to 10 devices.