



# iOS Deployment Overview for Enterprise

## Contents

What's new in iOS 9  
Ownership models  
Deployment steps  
Support options

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, whether in the office or on the go. Embracing this new way of working leads to benefits across 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 are viewed as shaping the business strategy and solving real-world problems, rather than fixing technology and cost-cutting. Ultimately everyone benefits, with a reinvigorated workforce and new business opportunities everywhere.

Setting up and deploying iPad and iPhone throughout your business has never been easier. With a complete set of tools from Apple and a third-party mobile device management solution, your organization can easily deploy iOS devices and content at scale.

- Mobile device management (MDM) allows you to configure and manage your devices and wirelessly distribute and manage your content.
- The Device Enrollment Program (DEP) automates enrollment of Apple devices into your MDM solution to streamline deployment.
- The Volume Purchase Program (VPP) lets you purchase apps and books in bulk and distribute them to users.

This document offers guidance on deploying iOS devices in your organization and helps you create a deployment plan that best suits your environment.

## What's new in iOS 9

iOS 9 is better than ever for business. It provides new ways to deploy apps and even better ways to manage devices and data, along with streamlined systems integration and powerful productivity features.

### Enhanced app distribution

iOS 9 introduces a more efficient, scalable way to deploy apps across your organization. Businesses can now use VPP and MDM in addition to a user's Apple ID to assign and distribute apps directly to a device. And now, apps purchased through VPP can be assigned to users or devices in any country where the app is available.

### Better device and data management

iOS 9 also provides enhancements to MDM capabilities. For any device enrolled in DEP, you can send an MDM command that prompts the device to perform a separate download and installation of scheduled software updates. With iOS 9, you can also install and update managed apps while restricting general access to the App Store. And unmanaged apps can now be managed after installation, without reinstalling the app or experiencing any loss of user data.

### Deeper integration with enterprise systems

iOS 9 integrates with the latest enterprise systems and services. Support for Exchange ActiveSync v16, Mail, and Calendar are even more seamlessly integrated with your enterprise environment. And per-app VPN can now be configured to work with the built-in VPN client in iOS.

### Powerful productivity features

With the productivity features introduced in iOS 9, users can be even more productive. iOS 9 provides new ways to multitask on iPad, better intelligence through Search and Siri, and new built-in apps such as Notes and News.

Learn more about the new iOS 9 features for business: [www.apple.com/ipad/business/ios/](http://www.apple.com/ipad/business/ios/)

## Ownership models

Evaluating ownership 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. Start by identifying what's best for your organization.

Two ownership models for iOS devices are commonly used in the enterprise:

- Organization owned
- User owned

While most organizations have a preferred model, you might encounter multiple models in your environment. For example, a corporate office might deploy a user-owned 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, the corporation's retail stores might deploy an organization-owned strategy that allows several employees to share iOS devices to process customer transactions.

Exploring these deployment methods will help you identify the best choices for your unique environment. Once you've identified the right deployment for your organization, your team can explore Apple's deployment and management capabilities in detail. These programs and tools are covered at an overview level in the "Deployment steps" section of this guide, and in greater detail in the online iOS Deployment Reference.

iOS Deployment Reference: [help.apple.com/deployment/ios](http://help.apple.com/deployment/ios)

### Organization-owned devices

With an organization-owned deployment, you can purchase devices from Apple or a participating Apple Authorized Reseller or carrier. In this case, you can provide a device to each user, referred to in this document as a *personally enabled* deployment, or you can rotate devices among users, referred to in this document as a *non-personalized* deployment. Using a combination of these deployments, a complete set of tools from Apple and an MDM solution can fully automate device setup and configuration.

**Personally enabled.** When using a personally enabled strategy, you can configure devices with basic settings before giving them to users, or (as with user-owned devices) provide instructions or configuration profiles for users to apply themselves. Alternatively, you can have users enroll their devices with an MDM solution that provides organizational settings and apps over the air. For devices purchased directly from Apple or participating Apple Authorized Resellers or carriers, you can also take advantage of DEP to automatically enroll new devices into your MDM solution. Once configured, users can personalize their devices with their own apps and data in addition to any corporate account or apps provided by your organization.

**Non-personalized.** When devices are shared by several people or used for a single purpose (for example, in a restaurant or a 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.

The following chart illustrates the actions required by both the administrator and the user during each step of a non-personalized deployment.

	Administrator	User
<b>Prepare</b>	Evaluate your infrastructure Select an MDM solution Enroll in Apple Deployment Programs	No user action necessary
<b>Set up</b>	Configure devices Distribute apps and books	No user action necessary
<b>Deploy</b>	Distribute devices <hr/> <b>Personally enabled only</b> Allow users to personalize	<b>Personally enabled only</b> Download and install apps and books Accept invitation to VPP (optional) Use Apple, iTunes Store, and iCloud accounts, if applicable
<b>Manage</b>	Administer devices Deploy and manage additional content	<b>Personally enabled only</b> Discover additional apps to use <hr/> <b>Non-personalized only</b> No user action necessary

## User-owned devices

When devices are purchased and set up by the user—in what’s commonly referred to as a *BYOD*, or *bring-your-own-device* deployment—you can still provide access to corporate services such as Wi-Fi, mail, and calendars with MDM. Users must opt in to enroll in your organization’s MDM solution.

**BYOD.** A BYOD deployment allows users to set up and configure their own devices. To gain access to corporate resources, users can configure settings manually, install a configuration profile, or more commonly, enroll their devices with an 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 chart illustrates the actions required by both the administrator and the user during each step of a BYOD deployment.

	Administrator	User
<b>Prepare</b>	Evaluate your infrastructure Select an MDM solution Enroll in Apple Deployment Programs	No user action necessary
<b>Set up</b>	Configure devices Distribute apps and books	Opt in to company's MDM Download and install apps and books Accept invitation to VPP (optional)
<b>Deploy</b>	Allow users to personalize	Use Apple ID, iTunes Store, and iCloud accounts, if applicable
<b>Manage</b>	Administer devices Deploy and manage additional content	Discover additional apps to use

## Deployment steps

This section provides a more detailed look at each of the four steps for deploying devices and content: preparing the environment, setting up devices, deploying them, and managing them. Again, the steps you use will depend on whether the organization or the user owns the devices.

### 1. Prepare

After identifying the right deployment for your organization, follow these steps to lay the groundwork for deployment; you can take these actions even before you have your devices in hand.

#### Evaluate your infrastructure

iPhone and iPad integrate seamlessly into most standard enterprise IT environments. It's important to assess 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 might 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 Reference: [help.apple.com/deployment/ios](https://help.apple.com/deployment/ios)

Learn more about Bonjour: [www.apple.com/support/bonjour](https://www.apple.com/support/bonjour)

### **Mail, contacts, and 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.

### **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, the Mac App Store, the iTunes Store, and the 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](http://www.apple.com/osx/server/features/#caching-server)

### **iTunes support**

iTunes isn't required for devices using iOS 5 or later, but you might 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](http://help.apple.com/iosdeployment/itunes)

### **Select an 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. iOS provides a built-in set of management features that are enabled by third-party MDM solutions.

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 resource listed below to evaluate which management features are most relevant to your organization. In addition to third-party MDM solutions, a solution from Apple is available called Profile Manager, a feature of OS X Server.

Learn more about MDM: [www.apple.com/ipad/business/it/management.html](http://www.apple.com/ipad/business/it/management.html)

Learn more about Profile Manager: [www.apple.com/osx/server/features/#profile-manager](http://www.apple.com/osx/server/features/#profile-manager)

### **Enroll in Apple Deployment Programs**

Apple Deployment Programs are a suite of programs that make it easy to manage your devices and content.

The program agent is the highest-level administrator for these programs and has full administrative control of the Apple Deployment Programs portal for your organization. If you are new to Apple Deployment Programs, the account created during enrollment will be your program agent account. The same program agent account can be used to enroll in each program.

### Device Enrollment Program

DEP provides a fast, streamlined way to deploy organization-owned iOS and OS X devices that are purchased directly from Apple or participating Apple Authorized Resellers or carriers. You can simplify initial setup by automating MDM enrollment and supervision of devices without having to physically touch or prepare them before users get them. And you can further simplify the setup process for users by removing specific steps in Setup Assistant, so users are up and running quickly. You can also control whether or not the user may remove the MDM profile from the device. To learn more about supervision, visit the “Supervised devices” section of this guide.

After enrolling in the program, administrators log in to the DEP website, link the program to their MDM servers, and assign devices to users. Once assigned, users can go through the Setup Assistant on their devices; any MDM-specified configurations, restrictions, or controls are automatically installed.

Learn more about the Device Enrollment Program: [www.apple.com/business/dep](http://www.apple.com/business/dep)

### Volume Purchase Program

VPP allows businesses to purchase iOS apps and books in volume and distribute them to employees. You can pay with a corporate credit card or with VPP Credit that you’ve procured using a purchase order (PO).

You can also get custom B2B apps for iOS that are built only for you by third-party developers and procured privately through the VPP store. Developers registered in the Apple Developer 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 distribute apps and books to devices and users in any country where the app is available. When apps are no longer needed by a particular device or user, you can use MDM to revoke and reassign them to a different device or user. Redemption codes purchased through VPP can also be used to distribute apps and books, transferring content ownership to the user who redeems the code.

Learn more about VPP: [www.apple.com/business/vpp](http://www.apple.com/business/vpp)

### Apple Developer Enterprise Program

Develop in-house iOS apps for use by your company using the Apple 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.

Learn more about the Apple Developer Enterprise Program: [developer.apple.com/programs/ios/enterprise](http://developer.apple.com/programs/ios/enterprise)

## 2. Set up

In this step, you can leverage Apple Deployment Programs, an MDM solution, or optionally Apple Configurator 2 to configure your devices and distribute your content. You can approach your setup in several ways, depending on who owns the devices and your preferred type of deployment.

### Configure your devices

Multiple options are available for configuring user access to corporate services. IT can set up devices by distributing configuration profiles. Additional configuration options are available for supervised devices.

## Configuring devices with MDM

To enable management, your devices can be securely enrolled with an MDM server using a configuration profile. 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; they can be delivered through MDM if you need to configure many devices and prefer a low-touch, over-the-air deployment. Profiles can also be sent as an email attachment, downloaded from a web page, or installed on devices through Apple Configurator 2.

- **Organization-owned devices.** Use DEP to enable automatic MDM enrollment of your users' devices upon activation.
- **User-owned devices.** Employees can decide whether or not to enroll their device in MDM. They can also disassociate from MDM at any time by removing the configuration profile from their device. You should consider incentives for users to remain managed. For example, you might require users to enroll in MDM in order to get Wi-Fi network access by using your MDM solution to automatically provide the wireless credentials.

Once a device is enrolled, an administrator can initiate an MDM policy, option, or command. Then the iOS device receives notification of the administrator's action via the Apple Push Notification service (APNs) so it can communicate directly with its MDM server over a secure connection. With a network connection, devices can receive APNs commands anywhere in the world. However, no confidential or proprietary information is transmitted via APNs.

## Configuring devices with Apple Configurator 2 (optional)

Accelerate your initial deployments with the completely redesigned Apple Configurator 2. With this free OS X application, you can update iOS devices to the latest version of iOS, configure device settings and restrictions, and install apps and other content. After initial setup, you can continue to manage everything over the air using MDM.

Apple Configurator 2 has an entirely new user interface focused on your devices and the discrete tasks you want to perform on them. The application integrates seamlessly with DEP, enabling devices to automatically enroll in MDM using DEP settings. Custom workflows can be created within Apple Configurator 2 using Blueprints to combine discrete tasks. And it now stores information in an iCloud account, making it easy to have multiple Mac computers use the same information and Blueprints.

Learn more about Apple Configurator 2: [help.apple.com/configurator/mac/](https://help.apple.com/configurator/mac/)

## Supervised devices

Supervision provides a higher level of device management for organization-owned devices, allowing additional restrictions. For example, supervision lets you turn off iMessage, disallow AirDrop, prevent users from modifying account settings, filter web connections via Global Proxy, and more. By default, all iOS devices are unsupervised. To enable supervision, use DEP or Apple Configurator 2. And you can combine supervision with remote management using MDM to manage additional settings and restrictions.

## 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 distribute apps and books purchased through VPP or apps you've developed in house to devices and users, so your users have everything they need to be productive. At the time of purchase, you'll need to determine your distribution method: managed distribution or redeemable codes.

### Managed distribution

With managed distribution, you can use your MDM solution or Apple Configurator 2 to manage apps and books purchased from the VPP store. To enable managed distribution, you must first link your MDM solution to your VPP account using a secure token. Once you're connected to your MDM server, you can assign VPP apps and books, even if the App Store is disabled.

- **Assign VPP apps to devices.** With iOS 9, you can now assign apps directly to devices using your MDM solution or Apple Configurator 2. This method saves several steps in the initial rollout, making your deployment significantly easier and faster, while giving you full control over managed devices and content. After an app is assigned to a device, the app is pushed to that device via MDM and no invitation is required. Anyone using that device has access to that app.
- **Assign VPP apps and books to users.** Use your MDM solution to invite users through email or a push notification message. To accept the invitation, users sign in on their devices with a personal Apple ID. The Apple ID is registered with the VPP service, but remains completely private and not visible to the administrator. Once users agree to the invitation, they're connected to your MDM server so they can start receiving assigned apps and books. Apps are automatically available for download on all the user's devices, with no additional effort or cost to you.

When apps you've assigned are no longer needed by a device or a user, they can be revoked and reassigned to different devices and users so your organization retains full ownership and control of purchased apps. However, once distributed, books remain the property of the recipient and cannot be revoked or reassigned.

### Redeemable codes

You can also distribute content using redeemable codes. This method permanently transfers an app or a book to the user who redeems the code. Redeemable codes are delivered in a spreadsheet format. A unique code is provided for each app or book in the quantity purchased. Each time a code is redeemed, the spreadsheet is updated in the VPP store, allowing you to view the number of redeemed codes at any time. You can distribute codes using MDM, Apple Configurator 2, email, or an internal website.

### Installing apps and content with Apple Configurator 2 (optional)

In addition to using Apple Configurator 2 for basic setup and configuration, you can also use it to install apps and content. For personally enabled deployments, you can preinstall all your apps, saving time and network bandwidth. And for non-personalized deployments, you can fully set up your devices all the way to the Home screen. When you configure devices with Apple Configurator 2, you can install free apps, in-house apps, and documents. Paid App Store apps require VPP. Documents are available for apps that support iTunes file sharing. You can review or retrieve documents from iOS devices by connecting them to a Mac running Apple Configurator 2.

## 3. Deploy

iOS makes it simple for employees to start using their devices right out of the box, without requiring help from IT.

### Distribute your devices

The devices are now ready to distribute. For personally enabled deployments, give devices to users who can use the streamlined Setup Assistant for further personalization and finalize setup. For non-personalized deployments, distribute devices to your shift employees or kiosks designed to charge and secure the devices.

### 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 choosing basic settings, users can also customize their personal preferences, such as language, location, Siri, iCloud, and Find My iPhone. Devices that are enrolled in DEP can be automatically enrolled in MDM right within the Setup Assistant.



### **Allow users to personalize**

For personally enabled and BYOD deployments, allowing users to personalize their devices with their own Apple IDs increases productivity because users choose which apps and content will allow them to best accomplish their tasks and goals.

### **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, the App Store, the 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. Users who don't have an Apple ID can create one even before they receive a device. Setup Assistant also enables users to create a personal Apple ID if they don't have one. Users do not need a credit card to create an Apple ID.

Learn how to create an Apple ID without a credit card: [support.apple.com/en-us/HT204034](https://support.apple.com/en-us/HT204034)

Learn how to sign up for an Apple ID: [appleid.apple.com](https://appleid.apple.com)

### **iCloud**

iCloud allow 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 capability 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](https://www.apple.com/icloud)

## **4. Manage**

Once your users are up and running, a wide range of administrative capabilities is available for managing and maintaining your devices and content over time.

### **Administer your devices**

A managed device can be administered by the MDM server through a set of specific tasks. This set of tasks includes querying devices for information, as well as initiating security commands that allow you to manage devices that are out of policy, lost, or stolen.

#### **Queries**

An MDM server can query devices for a variety of information, including hardware information, such as serial number, device UDID, or Wi-Fi MAC address; as well as software information, such as the iOS version and a detailed list of all apps installed on the device. This information helps to 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.

## Deploy and manage additional content

Organizations often need to distribute apps so their users are productive. At the same time, organizations need to control how apps connect to internal resources or how data security is handled when a user transitions out of the organization, all while coexisting alongside the user's personal apps and data.

### Internal app portals

You have the option of creating an internal app portal for your employees where they can easily find apps for their iOS devices. In-house apps, App Store app URLs or VPP codes, or custom B2B VPP codes can be linked from this portal, making it a single destination for users. You can manage and secure this site centrally. In addition, you can easily build a portal internally or explore third-party MDM solutions to manage app distribution.

### Managed apps

In iOS, managed apps allow an organization to distribute free, paid, and enterprise apps over the air using MDM, while also providing the right balance of protecting corporate data and respecting user privacy.

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 if a user redeemed an app code using a personal Apple ID, the app can be downloaded again from the App Store, but it 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.
- **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.** This setting helps the user stay focused on a task while using an iOS device by limiting the 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 is later reinstalled by the user.

## Support options

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

### AppleCare for Enterprise

For companies looking for complete coverage, AppleCare for Enterprise can help reduce the load on your internal help desk by providing technical support for employees over the phone, 24/7, with one-hour response times for top-priority issues. The program provides IT department-level support for all Apple hardware and software, as well as support for complex deployment and integration scenarios, including MDM and Active Directory.

## 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. It offers up to 24/7 support and an assigned technical account manager, depending on the level of support you purchase. 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, as well as 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 accessory.

Learn more about AppleCare programs: [www.apple.com/support/professional](http://www.apple.com/support/professional)

## Summary

Whether your company deploys iOS devices to a group of users or across the entire organization, you have many options for easily deploying and managing 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](http://www.apple.com/ipad/business/it)

For more detailed technical information about deploying iOS, see the iOS Deployment Reference: [help.apple.com/deployment/ios](http://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.

© 2015 Apple Inc. All rights reserved. Apple, the Apple logo, AirPlay, Apple TV, Bonjour, FaceTime, iBooks, iMessage, iPad, iPhone, iPod touch, iTunes, iTunes U, Keychain, Mac, the Mac logo, OS X, and Siri are trademarks of Apple Inc., registered in the U.S. and other countries. AirPrint is a trademark of Apple Inc. Apple Store, AppleCare, iCloud, and iTunes Store are service marks of Apple Inc., registered in the U.S. and other countries. App Store and iBooks Store are service marks of Apple Inc. Some products or promotions are not available outside the U.S. Product specifications are subject to change. Some features and applications are not available in all areas. Application availability and pricing are subject to change. Other product and company names mentioned herein may be trademarks of their respective companies. September 2015