Overview

iPhone and iPad 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 modern way of working leads to benefits across the entire organisation. 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 just fixing technology and cutting costs. Ultimately everyone benefits, with an invigorated workforce and new business opportunities everywhere.

Setting up and deploying iPhone and iPad throughout your business has never been easier. With key programmes from Apple and a third-party mobile device management solution, your organisation can easily deploy iOS devices and apps at scale.

- Mobile device management (MDM) allows you to configure and manage your devices, and wirelessly distribute and manage your apps.
- The Device Enrolment Programme (DEP) automates enrolment of Apple devices into your MDM solution to streamline deployment with zero-touch configuration for IT.
- The Volume Purchase Programme (VPP) lets you purchase apps and books in bulk and distribute them to users wirelessly.

This document offers guidance on deploying iOS devices in your organisation, and helps you create a deployment plan that best suits your environment. These programmes and tools, described in the Deployment Steps section of this overview, are covered in greater detail in the online iOS Deployment Reference.

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

Ownership Models

Evaluating ownership models and choosing the one that’s right for your organisation is an important first step to deployment. There are several ways to approach deployment, depending on who owns the device. Start by identifying what’s best for your organisation.

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

- Organisation owned
- User owned
While most organisations 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, and without impacting the user’s personal data and apps. However, the corporation’s retail stores might deploy an organisation-owned strategy that allows several employees to share iOS devices to process customer transactions.

Exploring these models will help you identify the best choices for your unique environment. Once you’ve identified the right model for your organisation, your team can explore Apple’s deployment and management capabilities in detail.

**Organisation-owned devices**

With an organisation-owned model, you can purchase devices from Apple, or a participating Apple Authorised Reseller or carrier. In this case, you can provide a device to each user (a *personally enabled* deployment) or rotate devices between users (a *non-personalised* deployment). By using a combination of these models, key technologies from Apple and an MDM solution, you can fully automate device setup and configuration.

**Personally enabled.** When using a personally enabled strategy, you can have each user choose their own device and enrol it with an MDM solution that provides organisational settings and apps over the air. For devices purchased directly from Apple, or participating Apple Authorised Resellers or carriers, you can also take advantage of DEP to automatically enrol new devices into your MDM solution. Once configured, users can personalise these devices with their own apps and data, in addition to any corporate account or apps provided by your organisation.

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

The following chart illustrates the actions required by both the administrator and the user during each step of an organisation-owned strategy. Unless otherwise indicated, actions serve both *personally enabled* and *non-personalised* deployments.

<table>
<thead>
<tr>
<th></th>
<th>Administrator</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prepare</strong></td>
<td>• Evaluate your infrastructure</td>
<td>• No user action necessary</td>
</tr>
<tr>
<td></td>
<td>• Select an MDM solution</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enrol in Apple Deployment Programmes</td>
<td></td>
</tr>
<tr>
<td><strong>Set up</strong></td>
<td>• Configure devices</td>
<td>• No user action necessary</td>
</tr>
<tr>
<td></td>
<td>• Distribute apps and books</td>
<td></td>
</tr>
<tr>
<td><strong>Deploy</strong></td>
<td>• Distribute devices</td>
<td><strong>Personally enabled only</strong></td>
</tr>
<tr>
<td></td>
<td>• <em>Personally enabled only</em></td>
<td>• Download and install apps and books</td>
</tr>
<tr>
<td></td>
<td>• Allow users to personalise</td>
<td>• Use Apple ID, iTunes Store and iCloud accounts, if applicable</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Non-personalised only</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• No user action necessary</td>
</tr>
<tr>
<td><strong>Manage</strong></td>
<td>• Administer devices</td>
<td><strong>Personally enabled only</strong></td>
</tr>
<tr>
<td></td>
<td>• Deploy and manage additional content</td>
<td>• Discover additional apps to use</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Non-personalised only</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• No user action necessary</td>
</tr>
</tbody>
</table>
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, email and calendars with MDM. Users must opt in to enrol in your organisation’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, enrol their devices with an MDM solution.

An advantage of using MDM to enrol 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 user-owned deployment.

<table>
<thead>
<tr>
<th>Administrator</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prepare</strong></td>
<td></td>
</tr>
<tr>
<td>• Evaluate your infrastructure</td>
<td>• Use Apple ID, iTunes Store and iCloud accounts, if applicable</td>
</tr>
<tr>
<td>• Select an MDM solution</td>
<td></td>
</tr>
<tr>
<td>• Enrol in Apple Deployment Programmes</td>
<td></td>
</tr>
<tr>
<td><strong>Set up</strong></td>
<td></td>
</tr>
<tr>
<td>• Configure devices</td>
<td>• Opt in to company’s MDM solution</td>
</tr>
<tr>
<td>• Distribute apps and books</td>
<td>• Download and install apps and books</td>
</tr>
<tr>
<td><strong>Deploy</strong></td>
<td></td>
</tr>
<tr>
<td>• No administrator action necessary</td>
<td>• No user action necessary</td>
</tr>
<tr>
<td><strong>Manage</strong></td>
<td></td>
</tr>
<tr>
<td>• Administer devices</td>
<td>• Discover additional apps to use</td>
</tr>
<tr>
<td>• Deploy and manage additional content</td>
<td></td>
</tr>
</tbody>
</table>

**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. The steps you use will depend on whether the organisation or the user owns the devices.

1. **Prepare**
After identifying the right deployment model for your organisation, 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 organisation 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. Apple and Cisco have also optimised how iPhone and iPad communicate with a Cisco wireless network, paving the way for other advanced networking features such as fast roaming and Quality of Service (QoS) optimisation for apps.

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

You should also make sure 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/uk/support/bonjour](https://www.apple.com/uk/support/bonjour)

**Email, 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 licences to support the anticipated number of iOS devices that will be connected. iOS also supports Office 365 modern authentication leveraging OAuth 2.0 and multi-factor authentication. If you don’t use Exchange, iOS works with standards-based servers, including IMAP, POP, SMTP, CalDAV, CardDAV and LDAP.

**Content Caching**

An integrated feature of macOS High Sierra, Content Caching stores a local copy of frequently requested content from Apple servers, helping to minimise the amount of bandwidth needed to download content on your network. Content Caching 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. Content Caching includes the tethered caching service, which allows a Mac to share its Internet connection with many iOS devices connected via USB.

Learn more about Content Caching: [https://support.apple.com/en-zA/HT208025](https://support.apple.com/en-zA/HT208025)

Learn more about tethered caching: [https://support.apple.com/en-zA/HT207523](https://support.apple.com/en-zA/HT207523)

**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.

Select an MDM solution
The Apple management framework for iOS gives organisations the ability to securely enrol devices in the corporate environment, wirelessly configure and update settings, monitor policy compliance, deploy apps and books, and remotely wipe or lock managed devices. These management features 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 resources listed below to evaluate which management features are most relevant to your organisation. In addition to third-party MDM solutions, a solution from Apple is available called Profile Manager, a feature of macOS Server.

Learn more about managing devices and corporate data on iOS: https://images.apple.com/business/resources/docs/Managing_Devices_and_Corporate_Data_on_iOS.pdf
Learn more about Profile Manager: www.apple.com/uk/macos/server/features/#profile-manager

Enrol in Apple Deployment Programmes
Apple Deployment Programmes are a suite of programmes that make it easy to manage your devices and content.

If you are new to Apple Deployment Programmes, the account created during enrolment will be your programme agent account. The programme agent is the highest-level administrator for these programmes and has full administrative control of the Apple Deployment Programmes portal for your organisation. The same programme agent account can be used to enrol in each programme.

Device Enrolment Programme
DEP provides a fast, streamlined way to deploy organisation-owned iOS devices, Mac computers and Apple TV devices that are purchased directly from Apple or participating Apple Authorised Resellers or carriers. You can simplify initial setup by automating MDM enrolment and supervising 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 manually enrol iOS devices in the DEP using Apple Configurator 2, regardless of how you purchased them. With DEP, devices are always supervised and MDM enrolment is mandatory. To learn more about supervision, refer to the Supervised devices section.

Learn more about the Device Enrolment Programme: www.apple.com/business/dep

Volume Purchase Programme
VPP allows businesses to purchase iOS apps and books in volume and distribute them to employees.¹

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 Apple Developer Programme can submit apps for B2B distribution using iTunes Connect, the same process used to submit other apps to the App Store.

Learn more about VPP: www.apple.com/business/vpp
Apple Developer Enterprise Programme
Develop in-house iOS apps for use by your company using the Apple Developer Enterprise Programme. This programme offers a complete and integrated process for developing, testing and distributing your iOS apps to employees within your organisation. In-house apps are not submitted to the App Store and are not reviewed, approved or hosted by Apple.

Distribute your in-house apps either by hosting your app on a simple internal web server or by using a third-party MDM 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 Programme: developer.apple.com/programs/enterprise

2. Set up
In this step, configure your devices and distribute your content by leveraging Apple Deployment Programmes, an MDM solution or, optionally, Apple Configurator 2. There are several ways to approach your setup, 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, securely enrol your devices with an MDM server using a configuration profile — an XML file that allows you to distribute configuration information to an iOS device. These 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.

• Organisation-owned devices. Use DEP to enable automatic MDM enrolment of your users’ devices upon activation. All iOS devices added to DEP are always supervised with mandatory MDM enrolment.

• User-owned devices. Employees can decide whether or not to enrol their device in MDM. And to disassociate from MDM at any time, they simply remove the configuration profile from their device. But you should consider incentives for users to remain managed. For example, you might require users to enrol in MDM to get Wi-Fi network access — 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. This free macOS application allows you to connect iOS devices to a Mac computer over USB and 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 a 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 enrol in MDM using DEP settings. Custom workflows can be created within Apple Configurator 2 using Blueprints to combine discrete tasks.

Learn more about Apple Configurator 2: help.apple.com/configurator/mac/2.0/

Supervised devices
Supervision provides additional management capabilities for iOS devices owned by your organisation, allowing restrictions such as disabling AirDrop or placing the device in Single App Mode. It also provides the ability to enable a web filter via a global proxy to ensure the users’ web traffic stays within the organisation’s guidelines, prevent users from resetting their device to factory defaults, and many more. By default, all iOS devices are non-supervised. You can use DEP to enable supervision or you can manually enable supervision using Apple Configurator 2.

Even if you don’t plan to use any supervised-only features now, consider supervising your devices when you set them up, so you can take advantage of supervised-only features in the future. Otherwise, you’ll need to wipe devices that have already been deployed. Supervision isn’t about locking down a device; rather, it enhances company-owned devices by extending management capabilities. In the long run, supervision provides even more options for your enterprise.

For a complete list of supervised settings, see the iOS Deployment Reference.

Distribute apps and books
Apple offers extensive programmes to help your organisation 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 redemption codes.

Managed distribution
With managed distribution, use your MDM solution or Apple Configurator 2 to manage apps and books purchased from the VPP store in any country where the app is available. 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 on the device is disabled.

• Assign VPP apps to devices. Using your MDM solution or Apple Configurator 2, assign apps directly to devices. 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 user invitation is required. Anyone using that device has access to the app.
• **Assign VPP apps and books to users.** An alternative method is to use your MDM solution to invite users to your VPP organisation 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 your 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 organisation retains full ownership and control of purchased apps. However, once distributed, books remain the property of the recipient and cannot be revoked or reassigned.

**Redemption codes**
You can also distribute content using redemption codes. This is helpful when your organisation cannot use MDM on the end-user’s device. For example, in a franchise business scenario. This method permanently transfers an app or a book to the user who redeems the code. Redemption codes are delivered in 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. Distribute the codes using MDM, Apple Configurator 2, email or an internal website.

**Installing apps and content with Apple Configurator 2 (optional)**
In addition to basic setup and configuration, Apple Configurator 2 can be used to install apps and content for devices you want to set up on behalf of the user. For personally enabled deployments, you can pre-install apps, saving time and network bandwidth. And for non-personalised 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 App Store apps, in-house apps and documents. App Store apps require VPP. Documents are available for apps that support iTunes file sharing. To review or retrieve documents from iOS devices, connect them to a Mac running Apple Configurator 2.

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

**Distribute your devices**
Once devices have been prepared and set up in the first two steps, they are ready for distribution. For personally enabled deployments, give devices to users who can use the streamlined Setup Assistant for further personalisation and to finalise setup. For non-personalised deployments, distribute devices to your shift employees or place devices in 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 straightaway with Setup Assistant in iOS. Beyond choosing basic settings, users can also customise their personal preferences, such as language, location, Siri, iCloud and Find My iPhone. Devices that are enrolled in DEP are automatically enrolled in MDM from within the Setup Assistant.
Allow users to personalise

For personally enabled and BYOD deployments, allowing users to personalise 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 already 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-za/HT204034

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 My Photo Stream, iCloud Keychain, iCloud Drive and iCloud Backup — can be disabled through the use of restrictions, either entered manually on the device or set via configuration profiles. In addition, an MDM solution can 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 not backed up to iCloud.

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

4. Manage

Once your users are up and running, a wide range of administrative capabilities are 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. These tasks include querying devices for information, as well as initiating management tasks 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 details such as serial number, device UDID or Wi-Fi MAC address, as well as software details 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.
Management tasks
When a device is managed, an MDM server may perform a wide variety of administrative tasks, including changing configuration settings automatically without user interaction, performing an iOS update on passcode-locked devices, locking or wiping a device remotely, or clearing the passcode lock so users can reset forgotten passwords. An MDM server may also request an iOS device to begin AirPlay mirroring to a specific destination or end a current AirPlay session.

Lost Mode
Your MDM solution can place a supervised device in Lost Mode remotely. This action locks the device and allows a message with a phone number to be displayed on the Lock screen. With Lost Mode, supervised devices that are lost or stolen can be located because MDM remotely queries for their location the last time they were online. Lost Mode doesn't require Find My iPhone to be enabled.

Activation Lock
With iOS 7.1 or later, you can use MDM to enable Activation Lock when a user turns on Find My iPhone on a supervised device. This allows your organisation to benefit from the theft-deterrent functionality of Activation Lock, while still allowing you to bypass the feature if a user is unable to authenticate with their Apple ID.

Deploy and manage additional content
Organisations often need to distribute apps so their users are productive. At the same time, organisations need to control how apps connect to internal resources or how data is securely handled when a user leaves the organisation — 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, it’s easy to build a portal internally or explore third-party MDM solutions to manage app distribution.

Managed content
Managed content involves the installation, configuration, management and removal of App Store and custom in-house apps, accounts, books and documents.

• Managed apps. In iOS, managed apps allow an organisation 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 the 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.

• Managed accounts. MDM can help your users get up and running quickly by setting up their email and other accounts automatically. Depending on the MDM solution provider and integration with your internal systems, account payloads can also be pre-populated with a user’s name, email address and, where applicable, certificate identities for authentication and signing.
• **Managed books and documents.** MDM tools, books, ePub books and PDF documents can be automatically pushed to user devices, so employees always have what they need. At the same time, managed books can be shared only with other managed apps or emailed using managed accounts. When the materials are no longer necessary, they can be removed remotely. Books purchased through VPP can be distributed through managed book distribution, but cannot be revoked and reassigned. A book already purchased by the user cannot be managed unless the book is explicitly assigned to the user by VPP.

**Managed app configuration**

App developers can identify app settings and capabilities that can be enabled when installed as a managed app. Install these configuration settings before or after the managed app is installed. For example, IT could establish a set of default preferences for a SharePoint app, so the user doesn’t need to manually configure server settings.

Leading MDM solution providers have established the AppConfig Community and a standard schema that all app developers can use to support managed app configuration. The AppConfig Community is focused on providing tools and best practices around native capabilities in mobile operating systems. The community helps enable a more consistent, open and simple way to configure and secure mobile apps to increase mobile adoption in business.

Learn more about the AppConfig Community: [www.appconfig.org](http://www.appconfig.org)

**Managed data flow**

MDM solutions provide specific features that enable corporate data to be managed at a granular level so that it does not leak out to users’ personal apps and cloud services.

• **Managed open in.** Managed open in uses a set of restrictions that prevents attachments or documents from managed sources from being opened in unmanaged destinations, and vice versa. For example, you can prevent a confidential email attachment in your organisation’s managed email account from being opened in any user’s personal apps. Only apps installed and managed by MDM can open this work document. The user’s unmanaged personal apps do not appear in the list of apps available to open the attachment. In addition to managed apps, accounts, books and domains, several extensions respect managed open in restrictions.

• **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 to allow apps to enter and exit Single App Mode autonomously.

• **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.
Summary

Whether your company deploys iOS devices to a group of users or across the entire organisation, you have many options for easily deploying and managing devices. Choosing the right strategies for your organisation 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/za/business/products-platform/