iOS Implementierung: Übersicht für Unternehmen

Inhalt

Überblick

Mit dem iPhone und iPad können Sie Ihre Geschäftsabläufe und die Arbeitsweise Ihrer Mitarbeiter transformieren. Die Geräte können zu signifikanten Produktivitätssteigerungen führen und Mitarbeitern die Freiheit und Flexibilität geben, neue Arbeitsformen auszuprobieren – sei es im Büro oder unterwegs. Werden diese modernen Arbeitsweisen gezielt angewandt, profitiert davon das gesamte Unternehmen. Die Benutzer haben einen besseren Zugang zu Informationen. Dadurch übernehmen sie mehr Verantwortung und sind in der Lage, Probleme kreativ zu lösen. IT-Abteilungen, die iOS unterstützen, haben in der Wahrnehmung der Benutzer Einfluss auf die Unternehmensstrategie und bringen die IT voran, statt nur defekte Technik zu reparieren und ständig die Kosten drücken zu wollen. Letztlich profitieren alle von einer motivierteren Belegschaft und neuen Geschäftsmöglichkeiten in allen Bereichen.

Noch nie war es so einfach, iPhone und iPad in Ihrem Unternehmen einzurichten und zu implementieren. Mit zentralen Apple Programmen und einer MDM-Lösung eines anderen Anbieters kann Ihre Organisation ganz einfach iOS Geräte und Apps nach Bedarf implementieren.

- Mit Mobile Device Management (MDM) können Sie Ihre Geräte konfigurieren und verwalten und drahtlos Ihre Apps verteilen und verwalten.
- Das Programm zur Geräteregistrierung (DEP) registriert Ihre Apple Geräte automatisch bei Ihrer MDM-Lösung, um die Implementierung zu optimieren, ohne dass ein Eingreifen seitens der IT erforderlich ist.
- Mit dem Programm für Volumenlizenzen (VPP) können Sie Apps in großen Stückzahlen kaufen und drahtlos an Benutzer verteilen.

Dieses Dokument unterstützt Sie bei der Implementierung von iOS Geräten in Ihrer Organisation und hilft Ihnen bei der Erstellung eines Implementierungsplans, der am besten zu Ihrer Umgebung passt. Ausführlichere Informationen zu den in dieser Übersicht im Abschnitt „Implementierungsschritte“ beschriebenen Programmen und Werkzeugen finden Sie in der Online-Ressource „iOS Implementierung: Referenz“.

iOS Implementierung: Referenz: help.apple.com/deployment/ios

Eigentumsmodelle

Ein wichtiger erster Schritt bei der Implementierung ist die Evaluierung von Eigentumsmodellen und die Wahl des für Ihre Organisation geeigneten Modells. Es gibt verschiedene Implementierungskonzepte, je nachdem, wer Eigentümer des Geräts ist. Ermitteln Sie als Erstes, was sich für Ihre Organisation am besten eignet.

In Unternehmen werden häufig zwei Eigentumsmodelle für iOS Geräte verwendet:

- Eigentum der Organisation
- Eigentum des Benutzers

Obwohl die meisten Organisationen ein bestimmtes Modell bevorzugen, kommen in Ihrer Umgebung möglicherweise mehrere Modelle zum Einsatz. Eine Firmenzentrale könnte z. B. eine Strategie nutzen, bei der die Geräte im Besitz der Benutzer sind. Hierbei können Mitarbeiter ein privates iPad einrichten, während die Unternehmensressourcen ohne Auswirkungen auf persönliche Daten und Apps des Benutzers geschützt und verwaltet werden. In den Einzelhandelsfilialen dieser Firma hingegen könnte eine Strategie verfolgt werden, bei der die Geräte im Besitz der Organisation sind und sich mehrere Mitarbeiter iOS Geräte teilen, um mit diesen Geräten Kundentransaktionen durchzuführen.

Wenn Sie diese Modelle genauer erkunden, fällt es Ihnen leichter, die beste Strategie für Ihre einzigartige Umgebung zu ermitteln. Nachdem Sie das passende Modell für Ihre Organisation identifiziert haben, kann Ihr Team die Implementierungs- und Verwaltungsfunktionen von Apple im Detail erkunden.

Geräte im Besitz des Unternehmens

Bei einem Modell mit Geräten im Besitz des Unternehmens können Sie Geräte bei Apple oder bei einem teilnehmenden autorisierten Apple Händler oder Mobilfunkanbieter kaufen. In diesem Fall können Sie jedem Benutzer ein Gerät zur Verfügung stellen (Implementierung von *persönlich anpassbaren* Geräten) oder die Geräte abwechselnd von mehreren Benutzern nutzen lassen (Implementierung von *nicht personalisierten* Geräten). Wenn Sie diese Modelle miteinander kombinieren, können die Einrichtung und Konfiguration der Geräte mithilfe zentraler Technologien von Apple und einer MDM-Lösung vollkommen automatisiert werden.

Persönlich anpassbar. Bei einer Strategie mit persönlich anpassbaren Geräten kann jeder Benutzer sein eigenes Gerät wählen und es bei einer MDM-Lösung registrieren, die die Einstellungen und Apps der Organisation drahtlos bereitstellt. Bei Geräten, die direkt bei Apple oder bei teilnehmenden autorisierten Apple Händlern oder Mobilfunkanbietern gekauft wurden, können Sie auch die Vorteile des DEP nutzen, um neue Geräte automatisch bei Ihrer MDM-Lösung zu registrieren. Nach der Konfiguration können die Benutzer ihre Geräte zusätzlich zu den von Ihrer Organisation bereitgestellten Accounts oder Apps mit eigenen Apps und Daten personalisieren.

Nicht personalisiert. Wenn Geräte von mehreren Personen gemeinsam oder nur für einen bestimmten Zweck verwendet werden (zum Beispiel in einem Restaurant oder Hotel), konfigurieren und verwalten die IT-Administratoren diese in der Regel zentral und überlassen die Einrichtung nicht dem einzelnen Benutzer. Bei der Implementierung nicht personalisierter Geräte ist es den Benutzern normalerweise nicht gestattet, auf dem Gerät Apps zu installieren oder persönliche Daten zu speichern.

Die folgende Tabelle fasst alle Aktionen zusammen, die der Administrator und der Benutzer bei den einzelnen Schritten einer Implementierung mit unternehmenseigenen Geräten ausführen müssen. Wenn nicht anders angegeben, beziehen sich diese Aufgaben sowohl auf Implementierungen mit *persönlich anpassbaren* als auch mit *nicht personalisierten* Geräten.

	Administrator	**Benutzer**
Vorbereiten	• Infrastruktur evaluieren • Eine MDM-Lösung wählen • Bei Apple Bereitstellungsprogrammen registrieren	• Kein Benutzereingriff erforderlich
Einrichten	• Geräte konfigurieren • Apps verteilen	• Kein Benutzereingriff erforderlich
Bereitstellen	• Geräte verteilen • **Nur persönlich anpassbare Geräte** Benutzern die Personalisierung erlauben	**Nur persönlich anpassbare Geräte** • Apps laden und installieren • Apple ID, iTunes Store und iCloud Accounts verwenden, falls zutreffend **Nur nicht personalisierte Geräte** • Kein Benutzereingriff erforderlich
Verwalten	• Geräte verwalten • Zusätzliche Inhalte bereitstellen und verwalten	**Nur persönlich anpassbare Geräte** • Zusätzliche Apps entdecken **Nur nicht personalisierte Geräte** • Kein Benutzereingriff erforderlich

Geräte im Besitz der Benutzer

Wenn Geräte vom Benutzer gekauft und eingerichtet werden, was üblicherweise als *BYOD*- bzw. *Bring-Your-Own-Device*-Implementierung bezeichnet wird, können Sie über MDM dennoch Zugriff auf Unternehmensdienste wie WLAN, Mail und Kalender gewähren. Die Benutzer müssen sich für die Registrierung bei der MDM-Lösung Ihrer Organisation anmelden.

BYOD. Bei einer BYOD-Implementierung dürfen Benutzer ihre eigenen Geräte einrichten und konfigurieren. Für den Zugriff auf Unternehmensressourcen können die Benutzer Einstellungen manuell konfigurieren, ein Konfigurationsprofil installieren oder – eine gängige Option – das Gerät bei einer MDM-Lösung registrieren.

Die Nutzung einer MDM-Lösung für die Registrierung privater Geräte hat den Vorteil, dass Unternehmensressourcen und -daten auf sichere Weise verwaltet werden können und gleichzeitig die Privatsphäre und die privaten Daten und Apps der Benutzer respektiert werden. Die IT-Abteilung kann Einstellungen durchsetzen, die Einhaltung von Unternehmensvorgaben überwachen und Unternehmensdaten und -apps entfernen, während die privaten Daten und Apps auf den Geräten der Benutzer erhalten bleiben.

Die folgende Tabelle fasst alle Aktionen zusammen, die der Administrator und der Benutzer bei den einzelnen Schritten einer Implementierung mit benutzereigenen Geräten ausführen müssen.

	Administrator	Benutzer
Vorbereiten	• Infrastruktur evaluieren • Eine MDM-Lösung wählen • Bei Apple Bereitstellungsprogrammen registrieren	• Apple ID, iTunes Store und iCloud Accounts verwenden, falls zutreffend
Einrichten	• Geräte konfigurieren • Apps verteilen	• Bei der MDM-Lösung des Unternehmens anmelden • Apps laden und installieren
Bereitstellen	• Kein Administratoreingriff erforderlich	• Kein Benutzereingriff erforderlich
Verwalten	• Geräte verwalten • Zusätzliche Inhalte bereitstellen und verwalten	• Zusätzliche Apps entdecken

Implementierungsschritte

In diesem Abschnitt erhalten Sie einen detaillierteren Überblick über jeden der vier Schritte für die Implementierung von Geräten und Inhalten: Umgebung vorbereiten, Geräte einrichten, Geräte bereitstellen und Geräte verwalten. Die verwendeten Schritte hängen davon ab, ob die Organisation oder der Benutzer Eigentümer der Geräte ist.

1. Vorbereiten

Nachdem Sie ermittelt haben, welches Modell für Ihre Organisation das richtige ist, befolgen Sie diese Schritte, um den Grundstein für die Implementierung zu legen. Diese Aktionen können Sie bereits durchführen, bevor die Geräte überhaupt zur Verfügung stehen.

Infrastruktur evaluieren

iPhone und iPad lassen sich nahtlos in die meisten standardmäßigen IT-Umgebungen in Unternehmen integrieren. Es ist wichtig, Ihre vorhandene Netzwerkinfrastruktur zu evaluieren, um sicherzustellen, dass Ihre Organisation alle Vorteile von iOS uneingeschränkt nutzen kann.

WLAN und Netzwerk

Für die Einrichtung und Konfiguration von iOS Geräten ist eine stabile WLAN Verbindung unverzichtbar. Vergewissern Sie sich, dass das WLAN Ihres Unternehmens mehrere Geräte mit gleichzeitigen Verbindungen von all Ihren Benutzern unterstützen kann. Falls die Geräte nicht auf die Apple Aktivierungsserver, iCloud oder den iTunes Store zugreifen können, müssen Sie ggf. die Konfiguration Ihres Web-Proxy bzw. Ihrer Firewall anpassen. Außerdem haben Apple und Cisco die Kommunikation von iPhone und iPad mit einem drahtlosen Netzwerk von Cisco optimiert. Dies ebnet den Weg für weitere innovative Netzwerk-Features wie schnelles Roaming und die Optimierung von Apps im Hinblick auf Quality of Service (QoS).

Evaluieren Sie Ihre VPN-Infrastruktur, um sicherzustellen, dass die Benutzer mit ihren iOS Geräten per Fernzugriff sicher auf Unternehmensressourcen zugreifen können. Das iOS Feature „VPN On Demand" bzw. „VPN pro App" ermöglicht es, eine VPN-Verbindung nur dann zu starten, wenn sie benötigt wird. Wenn Sie „VPN pro App" verwenden möchten, stellen Sie sicher, dass Ihre VPN-Gateways diese Funktionen unterstützen und dass Sie genügend Lizenzen erworben haben, um die entsprechende Anzahl an Benutzern und Verbindungen abzudecken.

Sie sollten zudem sicherstellen, dass die Netzwerkinfrastruktur ordnungsgemäß mit Bonjour zusammenarbeitet. Bonjour ist das auf Standards basierende Netzwerkprotokoll von Apple, das ohne Konfiguration auskommt. Es ermöglicht Geräten, Dienste im Netzwerk automatisch zu finden. iOS Geräte verwenden Bonjour, um sich mit AirPrint kompatiblen Druckern und AirPlay kompatiblen Geräten wie Apple TV zu verbinden. Manche Apps verwenden Bonjour auch, um andere Geräte für elektronisches Teamwork und Netzwerkfreigaben zu erkennen.

Weitere Informationen zu WLAN und Netzwerkfunktionen für Implementierungen in Unternehmen finden Sie in der Online-Ressource „iOS Implementierung: Referenz": help.apple.com/deployment/ios

Weitere Infos zu Bonjour: www.apple.com/de/support/bonjour

Mail, Kontakte und Kalender

Überprüfen Sie bei der Verwendung von Microsoft Exchange, ob der ActiveSync Dienst auf dem aktuellen Stand und so konfiguriert ist, dass alle Benutzer im Netzwerk unterstützt werden können. Wenn Sie das Cloud-basierte Office 365 verwenden, sind ausreichend Lizenzen erforderlich, um die vorhergesehene Anzahl von verbundenen iOS Geräten zu unterstützen. iOS unterstützt auch die moderne Authentifizierung in Office 365 und nutzt OAuth 2.0 sowie Multi-Faktor-Authentifizierung. Wird Exchange nicht verwendet, kann iOS mit standardbasierten Servern per IMAP, POP, SMTP, CalDAV, CardDAV und LDAP verwendet werden.

Inhaltscaching

Inhaltscaching ist ein integriertes Feature von macOS High Sierra. Es speichert eine lokale Kopie häufig angeforderter Inhalte von Apple Servern, um so die Bandbreite zu minimieren, die zum Laden von Inhalten in Ihrem Netzwerk erforderlich ist. Inhaltscaching beschleunigt das Laden und Bereitstellen von Software aus dem App Store, Mac App Store, iTunes Store und iBooks Store. Auch Softwareaktualisierungen können zum schnelleren Laden auf iOS Geräte im Cache zwischengespeichert werden. Inhaltscaching umfasst den Tethered Caching Dienst, über den der Mac seine Internetverbindung mit vielen per USB angeschlossenen iOS Geräten teilen kann.

Weitere Infos zu Inhaltscaching: https://support.apple.com/de-de/HT208025

Weitere Infos zu Tethered Caching: https://support.apple.com/de-de/HT207523

iTunes Support

iTunes ist für Geräte ab iOS 5 zwar nicht erforderlich, aber eine Unterstützung ist dennoch sinnvoll, damit die Benutzer Geräte aktivieren, Medien synchronisieren oder Backups ihrer Geräte auf einem Computer erstellen können.

iTunes unterstützt mehrere Konfigurationsoptionen, die für Unternehmen geeignet sind, darunter die Deaktivierung des Zugriffs auf Inhalte für Erwachsene, die Definition der Netzwerkdienste, auf die die Benutzer innerhalb von iTunes zugreifen können, und die Festlegung, ob die Benutzer neue Softwareaktualisierungen installieren dürfen.

Eine MDM-Lösung wählen

Die Verwaltungsarchitektur von Apple für iOS gibt Organisationen die Möglichkeit, Geräte sicher in der Unternehmensumgebung zu registrieren, Einstellungen drahtlos zu konfigurieren und zu aktualisieren, die Einhaltung von Richtlinien zu überwachen, Apps bereitzustellen und verwaltete Geräte per Fernzugriff zu löschen bzw. sperren. Diese Verwaltungsfunktionen werden von MDM-Lösungen anderer Anbieter unterstützt.

Es ist eine Reihe von MDM-Lösungen anderer Anbieter verfügbar, um verschiedene Serverplattformen zu unterstützen. Jede Lösung bietet andere Verwaltungskonsolen und -funktionen zu unterschiedlichen Preisen. Vor der Entscheidung für eine Lösung sollten Sie anhand der unten aufgeführten Ressourcen evaluieren, welche Verwaltungsfunktionen für Ihre Organisation am wichtigsten sind. Neben den MDM-Lösungen anderer Anbieter steht eine Lösung von Apple zur Verfügung, der sogenannte Profilmanager, ein Feature von macOS Server.

Weitere Infos zur Verwaltung von Geräten und Unternehmensdaten unter iOS: https://images.apple.com/business/resources/docs/Managing_Devices_and_Corporate_Data_on_iOS.pdf

Weitere Infos über den Profilmanager: www.apple.com/de/macos/server/features/#profile-manager

Bei Apple Bereitstellungsprogrammen registrieren

Apple Bereitstellungsprogramme sind Programmpakete, mit denen Sie Ihre Geräte und Inhalte einfach verwalten können.

Wenn Apple Bereitstellungsprogramme für Sie Neuland sind, sollten Sie wissen, dass der Account, der während der Registrierung erstellt wird, der Account des Programmvertreters ist. Der Programmvertreter ist der Administrator auf höchster Stufe für diese Programme. Er hat die komplette administrative Kontrolle über das Portal der Apple Bereitstellungsprogramme für Ihre Organisation. Derselbe Programmvertreter-Account kann genutzt werden, um sich bei den einzelnen Programmen anzumelden.

Programm zur Geräteregistrierung (DEP)

Das DEP bietet eine schnelle, optimierte Möglichkeit, iOS und Apple TV Geräte sowie Mac Computer zu implementieren, die Eigentum der Organisation sind und direkt bei Apple oder bei teilnehmenden autorisierten Apple Händlern oder Mobilfunkanbietern gekauft wurden. Sie können die Ersteinrichtung vereinfachen, indem Sie die MDM-Registrierung und Betreuung der Geräte automatisieren, ohne dass Sie sie manuell konfigurieren oder vorbereiten müssen, bevor die Benutzer sie erhalten. Darüber hinaus können Sie den Konfigurationsprozess für Benutzer weiter vereinfachen, indem Sie bestimmte Schritte im Systemassistenten entfernen, sodass die Benutzer schnell loslegen können. Sie können iOS Geräte mit Apple Configurator 2 auch manuell beim DEP registrieren – egal, auf welchem Weg sie gekauft wurden. Mit dem DEP werden die Geräte immer betreut und die MDM-Registrierung ist obligatorisch. Weitere Infos über die Betreuung finden Sie im Abschnitt „Betreute Geräte“.

Weitere Infos über das Programm zur Geräteregistrierung: www.apple.com/business/dep

Programm für Volumenlizenzen (VPP)

Mit dem VPP können Unternehmen iOS Apps in großen Stückzahlen kaufen und an Mitarbeiter verteilen.[1] Sie können mit einer Firmenkreditkarte oder mit dem VPP Guthaben zahlen, das Sie über eine Bestellung auf Rechnung erworben haben.

Sie können auch maßgeschneiderte B2B-Apps für iOS erhalten, die von anderen Entwicklern eigens für Sie erstellt werden und die Sie privat über den VPP Store beziehen. Beim Apple Entwicklerprogramm registrierte Entwickler können Apps für die B2B-Verteilung via iTunes Connect einreichen, also auf dieselbe Weise, wie sie auch andere Apps beim App Store einreichen.

Weitere Infos zum VPP: www.apple.com/business/vpp

Apple Developer Enterprise Program
Entwickeln Sie mithilfe des Apple Developer Enterprise Program interne iOS Apps zur Verwendung in Ihrem Unternehmen. Dieses Programm stellt einen vollständigen und integrierten Prozess bereit, um iOS Apps zu entwickeln, testen und debuggen und an Mitarbeiter in Ihrer Organisation zu verteilen. Interne Apps werden nicht beim App Store eingereicht und nicht von Apple geprüft, genehmigt oder gehostet.

Sie können Ihre internen Apps verteilen, indem Sie sie entweder auf einem einfachen, internen Webserver hosten oder indem Sie eine MDM-Lösung eines anderen Anbieters verwenden. Die Verwaltung interner Apps mit MDM hat den Vorteil, dass Apps per Fernzugriff konfiguriert, Versionen verwaltet, die Gesamtauthentifizierung konfiguriert und Richtlinien für den Netzwerkzugriff (wie VPN pro App) festgelegt werden können und dass gesteuert werden kann, welche Apps Dokumente exportieren dürfen. Die jeweiligen Anforderungen, die jeweilige Infrastruktur und der jeweilige Umfang der App-Verwaltung geben vor, welche Lösung sich am besten für Sie eignet.

Weitere Infos zum Apple Developer Enterprise Program: developer.apple.com/programs/enterprise

2. Einrichten

In diesem Schritt konfigurieren Sie Ihre Geräte und verteilen Ihre Inhalte, indem Sie die Apple Bereitstellungsprogramme, eine MDM-Lösung oder optional Apple Configurator 2 nutzen. Es gibt mehrere Strategien für die Einrichtung, je nachdem, wer Eigentümer der Geräte ist und welches Implementierungsmodell Sie bevorzugen.

Ihre Geräte konfigurieren

Es gibt mehrere Optionen zur Konfiguration des Benutzerzugriffs auf Unternehmensdienste. Die IT-Abteilung kann Geräte einrichten, indem sie Konfigurationsprofile verteilt. Für betreute Geräte sind zusätzliche Konfigurationsoptionen verfügbar.

Geräte mit MDM konfigurieren
Um die Verwaltungsfunktionen nutzen zu können, registrieren Sie Ihre Geräte auf sichere Weise mithilfe eines Konfigurationsprofils bei einem MDM-Server. Ein Konfigurationsprofil ist eine XML-Datei, mit der Sie Konfigurationsdaten auf iOS Geräte übertragen können. Diese Profile automatisieren die Konfiguration von Einstellungen, Accounts, Einschränkungen und Zertifikaten. Sie können über MDM verteilt werden, wenn Sie zahlreiche Geräte konfigurieren müssen und eine drahtlose Implementierung bevorzugen, bei der möglichst wenig manuell erledigt werden muss. Profile können auch als E-Mail Anhang versendet, von einer Webseite geladen oder über Apple Configurator 2 auf Geräten installiert werden.

- **Geräte im Besitz des Unternehmens.** Verwenden Sie das DEP, damit die Geräte Ihrer Benutzer bei der Aktivierung automatisch bei MDM registriert werden. Alle zum DEP hinzugefügten iOS Geräte werden immer betreut und die MDM-Registrierung ist obligatorisch.
- **Geräte im Besitz der Benutzer.** Die Mitarbeiter können entscheiden, ob sie ihr Gerät bei MDM registrieren wollen oder nicht. Sie können die Registrierung bei MDM auch jederzeit aufheben, indem sie einfach das Konfigurationsprofil auf ihrem Gerät entfernen. Sie sollten jedoch Anreize für Benutzer in Betracht ziehen, damit diese ihre Geräte weiterhin verwalten lassen. Beispielsweise könnten Sie die MDM-Registrierung für den Zugriff auf WLAN Netzwerke

vorschreiben und hierzu die MDM-Lösung für die automatische Bereitstellung der WLAN Anmeldedaten verwenden.

Sobald ein Gerät registriert ist, kann ein Administrator eine MDM-Richtlinie, eine MDM-Option oder einen MDM-Befehl anstoßen. Das iOS Gerät wird dann mithilfe des Apple Push-Benachrichtigungsdienstes (APNs) über die Aktion des Administrators benachrichtigt, damit es über eine sichere Verbindung direkt mit seinem MDM-Server kommunizieren kann. Über eine Netzwerkverbindung können Geräte Befehle des APNs an jedem Ort der Welt empfangen. Es werden jedoch keine vertraulichen oder geschützten Informationen über den APNs übertragen.

Geräte mit Apple Configurator 2 konfigurieren (optional)
Beschleunigen Sie Ihre Erstimplementierungen mit dem komplett überarbeiteten Apple Configurator 2. Mit dieser kostenlosen macOS App können Sie iOS Geräte über USB mit einem Mac Computer verbinden und sie auf die neueste Version von iOS aktualisieren, Geräteeinstellungen und -einschränkungen konfigurieren und Apps sowie andere Inhalte installieren. Und nach der Ersteinrichtung können Sie weiterhin alles drahtlos per MDM verwalten.

Die Benutzeroberfläche von Apple Configurator 2 ist auf Ihre Geräte und auf die einzelnen Aufgaben ausgerichtet, die Sie darauf ausführen möchten. Die App ist zudem nahtlos in das DEP integrierbar, sodass Geräte mithilfe von DEP Einstellungen automatisch bei MDM registriert werden können. Mithilfe von Entwürfen, die einzelne Aufgaben zusammenführen, können in Apple Configurator 2 eigene Arbeitsabläufe erstellt werden.

Weitere Infos über Apple Configurator 2: help.apple.com/configurator/mac/2.0/

Betreute Geräte
Die Betreuung bietet zusätzliche Verwaltungsfunktionen für iOS Geräte, die im Besitz Ihrer Organisation sind, und gestattet Einschränkungen wie die Deaktivierung von AirDrop oder die Aktivierung des Einzel-App-Modus auf dem Gerät. Außerdem bietet sie die Möglichkeit, einen Web-Filter über einen globalen Proxy zu aktivieren, um sicherzustellen, dass der Webdatenverkehr der Benutzer immer den Richtlinien der Organisation entspricht. Und mit der Betreuung kann verhindert werden, dass Benutzer ihr Gerät auf die Werkseinstellungen zurücksetzen, und vieles mehr. Standardmäßig sind alle iOS Geräte nicht betreut. Die Aktivierung der Betreuung kann mit dem DEP oder auch manuell mithilfe von Apple Configurator 2 erfolgen.

Auch wenn Sie derzeit nicht vorhaben, Features zu nutzen, die eine Betreuung voraussetzen, sollten Sie beim Einrichten der Geräte deren Betreuung in Erwägung ziehen, sodass Sie in Zukunft solche Features nutzen könnten. Andernfalls müssen Sie bereits implementierte Geräte komplett löschen. Bei der Betreuung geht es nicht darum, Geräte zu sperren. Vielmehr optimiert diese Methode unternehmenseigene Geräte, indem die Verwaltungsfunktionen erweitert werden. Langfristig bietet die Betreuung Ihrem Unternehmen noch weitere Optionen.

Eine ungekürzte Liste betreuter Einstellungen finden Sie in der Online-Ressource iOS Implementierung: Referenz.

Apps verteilen

Apple bietet umfassende Programme, mit denen Ihre Organisation von den großartigen für iOS erhältlichen Apps und Inhalten profitieren kann.[1] Dadurch können Sie über das VPP gekaufte oder intern entwickelte Apps an Geräte und Benutzer verteilen, damit Ihre Benutzer sofort produktiv arbeiten können. Zum Zeitpunkt des Kaufs müssen Sie sich für die gewünschte Verteilungsmethode entscheiden: verwaltete Verteilung oder Einlösecodes.

Verwaltete Verteilung

Mit der verwalteten Verteilung können Sie Ihre MDM-Lösung oder Apple Configurator 2 nutzen, um im VPP Store erworbene Apps in allen Ländern, in denen sie verfügbar sind, zu verwalten. Zur Aktivierung der verwalteten Verteilung müssen Sie zuerst Ihre MDM-Lösung mithilfe eines sicheren Tokens mit Ihrem VPP Account verknüpfen. Sobald Sie mit Ihrem MDM-Server verbunden sind, können Sie VPP Apps zuweisen, selbst wenn der App Store auf dem betreffenden Gerät deaktiviert ist.

- **VPP Apps Geräten zuweisen.** Mit Ihrer MDM-Lösung oder mit Apple Configurator 2 können Sie Apps direkt den Geräten zuweisen. Diese Methode spart mehrere Schritte bei der ersten Bereitstellung und macht sie deutlich einfacher und schneller. Gleichzeitig haben Sie aber die volle Kontrolle über verwaltete Geräte und Inhalte. Nachdem eine App einem Gerät zugewiesen wurde, wird die App per MDM auf das Gerät gepusht, ohne dass eine Einladung erforderlich ist. Jeder Benutzer dieses Geräts hat Zugriff auf die App.
- **VPP Apps Benutzern zuweisen.** Alternativ können Sie Ihre MDM-Lösung nutzen, um Benutzer per E-Mail oder Push-Benachrichtigung zu Ihrer VPP Organisation einzuladen. Zum Annehmen der Einladung melden sich die Benutzer mit einer persönlichen Apple ID auf ihren Geräten an. Die Apple ID wird beim VPP Dienst unter vollständiger Wahrung des Datenschutzes registriert und ist für den Administrator nicht sichtbar. Sobald die Benutzer der Einladung zustimmen, werden sie mit Ihrem MDM-Server verbunden, damit sie zugewiesene Apps empfangen können. Apps sind automatisch auf allen Geräten der Benutzer zum Laden verfügbar, ohne dass Ihnen zusätzlicher Aufwand oder zusätzliche Kosten entstehen.

Wenn ein Benutzer oder ein Gerät die ihm zugewiesenen Apps nicht mehr benötigt, können Sie die Zuweisung widerrufen und die Apps anderen Benutzern oder Geräten zuweisen. Ihre Organisation bleibt so Eigentümer der gekauften Apps und behält die volle Kontrolle darüber.

Einlösecodes

Sie können Inhalte auch mit Einlösecodes verteilen. Dieses Verfahren ist hilfreich, wenn Ihre Organisation auf dem Gerät des Endbenutzers kein MDM verwenden kann. Dies ist zum Beispiel in Franchise-Unternehmen der Fall. Bei dieser Methode wird eine App bzw. ein Buch dauerhaft an den Benutzer übertragen, der den Code einlöst. Einlösecodes werden in Form einer Tabellenkalkulationsdatei bereitgestellt. Zu jeder über das VPP erworbenen App bzw. jedem erworbenen Buch gibt es einen separaten, eindeutigen Code. Jedes Mal, wenn ein Code eingelöst wird, wird die Tabellenkalkulationsdatei im VPP Store aktualisiert, sodass Sie die Anzahl der eingelösten Codes jederzeit einsehen können. Sie können die Einlösecodes über MDM, Apple Configurator 2, E-Mail oder eine interne Website verteilen.

Apps und Inhalte mit Apple Configurator 2 installieren (optional)

Zusätzlich zur grundlegenden Einrichtung und Konfiguration kann Apple Configurator 2 verwendet werden, um Apps und Inhalte auf den Geräten zu installieren, die Sie für den Benutzer einrichten möchten. Bei Implementierungsmodellen mit persönlich anpassbaren Geräten können Sie Apps im Voraus installieren und sparen so Zeit und Netzwerkbandbreite. Bei Implementierungsmodellen mit nicht personalisierten Geräten können Sie die Geräte vollständig einrichten – bis hin zum Homescreen. Wenn Sie mit Apple Configurator 2 Geräte konfigurieren, können Sie Apps aus dem App Store, interne Apps und Dokumente installieren. Apps aus dem App Store erfordern das VPP. Dokumente sind für Apps verfügbar, die die iTunes Dateifreigabe unterstützen. Um Dokumente auf iOS Geräten anzuzeigen bzw. abzurufen, verbinden Sie diese mit einem Mac, auf dem Apple Configurator 2 ausgeführt wird.

3. Bereitstellen

Mit iOS können Mitarbeiter mit ihren Geräten ganz einfach nach dem Auspacken loslegen, ohne die Hilfe der IT-Abteilung zu benötigen.

Ihre Geräte verteilen

Nachdem die Geräte in den ersten beiden Schritten vorbereitet und eingerichtet wurden, sind sie zur Bereitstellung bereit. Bei Implementierungsmodellen mit persönlich anpassbaren Geräten geben Sie die Geräte den Benutzern, die mithilfe des optimierten Systemassistenten weitere Personalisierungen vornehmen und die Einrichtung abschließen können. Bei Implementierungsmodellen mit nicht personalisierten Geräten verteilen Sie die Geräte an die Mitarbeiter einer Schicht oder bewahren die Geräte in Kiosks auf, die für das Laden und Sichern der Geräte eingerichtet wurden.

Systemassistent

Ab Werk können die Benutzer ihre Geräte aktivieren, grundlegende Einstellungen konfigurieren und direkt mit dem Systemassistenten von iOS loslegen. Neben der Wahl der grundlegenden Einstellungen können Benutzer auch ihre persönlichen Einstellungen anpassen, z. B. Sprache, Standort, Siri, iCloud und „Mein iPhone suchen". Geräte, die beim DEP registriert sind, werden automatisch bei MDM registriert, und zwar direkt im Systemassistenten.

Benutzern die Personalisierung erlauben

Bei Implementierungsmodellen mit persönlich anpassbaren Geräten und bei BYOD-Implementierungen können Sie die Produktivität erhöhen, wenn Sie Benutzern erlauben, ihre Geräte mit ihren eigenen Apple IDs zu personalisieren. Die Benutzer wählen dann nämlich selbst, mit welchen Apps und Inhalten sie ihre Aufgaben und Ziele am besten erreichen können.

Apple ID

Die Apple ID ist eine Identität, die verwendet wird, um sich bei verschiedenen Apple Diensten wie FaceTime, iMessage, iTunes Store, App Store, iBooks Store und iCloud anzumelden. Diese Dienste bieten den Benutzern Zugriff auf eine Vielzahl von Inhalten zur Optimierung von geschäftlichen Aufgaben, zur Steigerung der Produktivität und zur Unterstützung der Zusammenarbeit.

Um diese Dienste optimal nutzen zu können, sollten die Benutzer ihre eigene Apple ID verwenden. Benutzer, die noch keine Apple ID haben, können eine erstellen, sogar noch bevor sie ein Gerät erhalten. Der Systemassistent ermöglicht dem Benutzer ebenfalls, eine persönliche Apple ID zu erstellen, falls er noch keine hat. Die Benutzer brauchen keine Kreditkarte, um eine Apple ID zu erstellen.

Erfahren Sie, wie Sie ohne Kreditkarte eine Apple ID erstellen: support.apple.com/de-de/HT204034

Erstellen Sie eine Apple ID: appleid.apple.com

iCloud

Mit iCloud können Benutzer automatisch Dokumente und persönliche Inhalte wie Kontakte, Kalender, Dokumente und Fotos synchronisieren und sie zwischen verschiedenen Geräten aktuell halten.[2] Die Benutzer können auch automatisch Backups von iOS Geräten erstellen, wenn eine WLAN Verbindung besteht, und mithilfe von „Mein iPhone suchen" iPhone, iPad oder iPod touch Geräte bzw. Mac Computer orten, die verloren gingen oder gestohlen wurden.

Einige Dienste, wie Fotostream, iCloud Schlüsselbund, iCloud Drive und iCloud Backup, können anhand von Einschränkungen deaktiviert werden, die entweder manuell auf dem Gerät eingegeben oder über Konfigurationsprofile festgelegt werden. Eine MDM-Lösung kann zudem verhindern, dass verwaltete Apps in iCloud gesichert werden. Die Benutzer haben so den Vorteil, iCloud für ihre persönlichen Daten nutzen zu können, ohne dass dort Unternehmensinformationen gespeichert werden. Daten aus Unternehmens-Accounts wie Exchange oder aus internen Apps des Unternehmens werden nicht in iCloud gesichert.

Weitere Infos über iCloud: www.apple.com/de/icloud

4. Verwalten

Sobald Ihre Benutzer einsatzbereit sind, steht ein breites Spektrum an administrativen Funktionen zur Verfügung, um Ihre Geräte und Inhalte fortlaufend zu verwalten und zu warten.

Ihre Geräte verwalten

Ein verwaltetes Gerät kann vom MDM-Server mithilfe einer Reihe von spezifischen Aufgaben verwaltet werden. Zu diesen Aufgaben zählen das Abfragen von Geräteinformationen sowie das Anstoßen von Verwaltungsaufgaben, mit denen Sie Geräte verwalten können, die gegen eine Richtlinie verstoßen, verloren gehen oder gestohlen werden.

Abfragen

Ein MDM-Server kann eine Vielzahl von Geräteinformationen abfragen, darunter Hardwareinformationen wie Seriennummer, Geräte-UDID oder WLAN MAC-Adresse sowie Softwareinformationen wie die iOS Version und eine detaillierte Liste aller Apps, die auf dem Gerät installiert sind. Mithilfe dieser Informationen kann sichergestellt werden, dass die Benutzer stets die geeigneten Apps installiert haben.

Verwaltungsaufgaben

Wenn ein Gerät verwaltet wird, kann ein MDM-Server eine Vielzahl von Verwaltungsaufgaben ausführen, darunter das automatische Ändern von Konfigurationseinstellungen ohne Benutzereingriff, die Durchführung eines iOS Updates auf gesperrten Geräten, das Sperren oder Löschen eines Geräts per Fernzugriff oder das Deaktivieren der Code-Sperre, sodass Benutzer vergessene Passwörter zurücksetzen können. Ein MDM-Server kann ein iOS Gerät auch anweisen, mit der AirPlay Bildschirmsynchronisation an ein bestimmtes Ziel zu beginnen oder eine laufende AirPlay Sitzung zu beenden.

Modus „Verloren"

Mit Ihrer MDM-Lösung können Sie ein betreutes Gerät per Fernzugriff in den Modus „Verloren" versetzen. Mit dieser Maßnahme wird das Gerät gesperrt. Zudem besteht die Möglichkeit, eine Nachricht mit einer Telefonnummer auf dem Sperrbildschirm des Geräts anzuzeigen. Im Modus „Verloren" können betreute Geräte, die verloren gingen oder gestohlen wurden, geortet werden, da die MDM-Lösung per Fernzugriff den Standort abfragt, an dem sie zuletzt online waren. Für den Modus „Verloren" muss „Mein iPhone suchen" nicht aktiviert sein.

Aktivierungssperre

Ab iOS 7.1 können Sie eine MDM-Lösung verwenden, um die Aktivierungssperre einzuschalten, wenn „Mein iPhone suchen" auf einem betreuten Gerät von einem Benutzer aktiviert wird. Auf diese Weise kann Ihre Organisation von der Diebstahlschutzfunktion der Aktivierungssperre profitieren. Sie können das Feature aber dennoch umgehen, wenn zum Beispiel ein Benutzer nicht in der Lage ist, sich mit seiner Apple ID zu authentifizieren.

Zusätzliche Inhalte bereitstellen und verwalten

Oft müssen Organisationen Apps verteilen, damit ihre Benutzer produktiv arbeiten können. Gleichzeitig müssen Organisationen steuern können, wie diese Apps auf interne Ressourcen zugreifen oder wie Daten sicher gehandhabt werden, wenn ein Benutzer aus der Organisation ausscheidet – und bei all dem müssen sie berücksichtigen, dass sich auf den Geräten auch persönliche Apps und Daten befinden.

Portale für interne Apps

Sie haben die Möglichkeit, ein internes App-Portal für Ihre Mitarbeiter einzurichten, wo sie ganz einfach Apps für ihre iOS Geräte finden können. Über dieses Portal können interne Apps, URLs oder VPP Codes für App Store Apps oder VPP Codes für maßgeschneiderte B2B-Apps verlinkt werden, wodurch das Portal zu einer zentralen Plattform für die Benutzer wird. Sie können dieses Portal zentral verwalten und schützen. Darüber hinaus können Sie auf einfache Weise ein Portal intern erstellen oder MDM-Lösungen anderer Anbieter erkunden, um die App-Verteilung zu verwalten.

Verwaltete Inhalte

Bei verwalteten Inhalten werden die Installation, Konfiguration, Verwaltung und Entfernung von App Store Apps und eigenen, intern entwickelten Apps sowie Accounts und Dokumenten kontrolliert.

- **Verwaltete Apps.** In iOS ermöglichen verwaltete Apps Organisationen die drahtlose Verteilung von kostenlosen, kostenpflichtigen und Unternehmensapps über MDM. Gleichzeitig wird ein ideales Gleichgewicht zwischen dem Schutz von Unternehmensdaten und Respekt für die Privatsphäre der Benutzer erreicht. Verwaltete Apps können per Fernzugriff über einen MDM-Server entfernt werden oder vom Benutzer selbst, wenn er sein Gerät von MDM entfernt. Das Entfernen der App löscht auch alle mit der App verbundenen Daten. Ist eine App dem Benutzer immer noch über das VPP zugewiesen bzw. hat der Benutzer die App anhand eines Einlösecodes und einer persönlichen Apple ID geladen, kann er sie erneut aus dem App Store laden. Sie wird dann aber nicht mehr über MDM verwaltet.
- **Verwaltete Accounts.** MDM kann Ihren Benutzern einen schnellen Einstieg ermöglichen, indem ihre E-Mail Accounts und weitere Accounts automatisch eingerichtet werden. Abhängig vom Anbieter der MDM-Lösung und deren Integration in die internen Systeme können Account-Payloads auch mit dem Namen und der E-Mail Adresse eines Benutzers sowie ggf. mit Zertifikatsidentitäten zur Authentifizierung und Signierung vorausgefüllt werden.
- **Verwaltete Dokumente.** MDM-Tools und PDF Dokumente können automatisch auf die Geräte der Benutzer gepusht werden, sodass die Mitarbeiter stets alles Nötige zur Hand haben. Und wenn die Materialien nicht mehr benötigt werden, können sie per Fernzugriff gelöscht werden.

Konfiguration verwalteter Apps

App-Entwickler können App-Einstellungen und -Funktionen angeben, die aktiviert werden, wenn die jeweilige App als verwaltete App installiert wird. Installieren Sie diese Konfigurationseinstellungen vor oder nach der Installation der verwalteten App. Zum Beispiel könnte die IT-Abteilung eine Reihe von Standardeinstellungen für eine SharePoint App festlegen, sodass der Benutzer die Servereinstellungen nicht manuell konfigurieren muss.

Führende Anbieter von MDM-Lösungen haben die AppConfig Community gegründet und ein Standardschema erstellt, das alle App-Entwickler nutzen können, um die Konfiguration verwalteter Apps zu unterstützten. Die AppConfig Community konzentriert sich auf die Bereitstellung von Tools und Best Practices im Zusammenhang mit den nativen Funktionen mobiler Betriebssysteme. Die Community fördert die Bereitstellung einer einheitlichen, offenen und einfachen Methode für die Konfiguration und Sicherung mobiler Apps, um die Akzeptanz mobiler Technologien in Unternehmen zu steigern.

Weitere Infos zur AppConfig Community: www.appconfig.org

Verwalteter Datenfluss

MDM-Lösungen bieten spezielle Features, mit denen Unternehmensdaten fein abgestimmt verwaltet werden können, damit diese Daten nicht in private Apps oder Cloud-Dienste des Benutzers gelangen können.

- **In verwalteter Umgebung öffnen.** „In verwalteter Umgebung öffnen" nutzt eine Reihe von Einschränkungen, die verhindern, dass Anhänge bzw. Dokumente aus verwalteten Quellen an nicht verwalteten Zielorten geöffnet werden können und umgekehrt. Sie können beispielsweise verhindern, dass ein vertraulicher E-Mail Anhang im verwalteten E-Mail Account Ihres Unternehmens mit einer der privaten Apps des Benutzers geöffnet wird. Das geschäftliche Dokument kann dann nur mit Apps geöffnet werden, die von der MDM-Lösung installiert wurden und verwaltet werden. Die nicht verwalteten Apps des Benutzers werden nicht in der Liste der Apps angezeigt, die zum Öffnen des Anhangs verfügbar sind. Neben verwalteten Apps, Accounts und Domains gelten die Einschränkungen im Zusammenhang mit dem verwalteten Öffnen auch für eine Reihe von Erweiterungen.
- **Einzel-App-Modus.** Diese Einstellung hilft dem Benutzer dabei, sich auf eine Aufgabe zu konzentrieren, indem das iOS Gerät während der Nutzung auf eine einzige App eingeschränkt wird. Entwickler können diese Funktion auch innerhalb ihrer Apps aktivieren, sodass die Apps den Einzel-App-Modus eigenständig aktivieren und verlassen können.
- **Backups verhindern.** Diese Einschränkung hindert verwaltete Apps daran, Daten in iCloud oder iTunes zu sichern. Werden Backups verhindert, können Daten aus verwalteten Apps nicht wiederhergestellt werden, falls die App per MDM entfernt und später vom Benutzer erneut installiert wird.

Supportoptionen

Apple bietet iOS Benutzern und IT-Administratoren eine Vielzahl von Programmen und Supportoptionen.

AppleCare for Enterprise

Falls Ihr Unternehmen umfassenden Schutz wünscht, kann AppleCare for Enterprise Sie bei der Entlastung Ihres internen Helpdesks unterstützen. Dies geschieht durch die Bereitstellung von technischem Support für Mitarbeiter per Telefon, rund um die Uhr mit Antwortzeiten von einer Stunde für Probleme mit höchster Priorität. Das Programm bietet Support auf IT-Abteilungsebene für jegliche Apple Hardware und Software sowie Support für komplexe Implementierungs- und Integrationsszenarien einschließlich MDM und Active Directory.

AppleCare OS Support

AppleCare OS Support bietet Ihrer IT-Abteilung unternehmensspezifischen Support per Telefon und E-Mail für iOS, macOS und macOS Server Implementierungen. Das Produkt bietet je nach gekaufter Supportstufe bis zu Rund-um-die-Uhr-Support und einen zugewiesenen technischen Accountmanager. Durch den direkten Kontakt zum Techniker bei Fragen zu Integration, Migration und Problemen beim erweiterten Serverbetrieb kann AppleCare OS Support die Effizienz Ihres IT-Personals bei der Implementierung und Verwaltung von Geräten und bei der Behebung von Problemen steigern.

AppleCare Help Desk Support

Mit dem AppleCare Help Desk Support erhalten Sie vorrangigen telefonischen Support von erfahrenen Apple Supportmitarbeitern. Er umfasst auch eine Reihe von Werkzeugen für die Diagnose und Behebung bei Problemen mit Apple Hardware. So können große Organisationen ihre Ressourcen effizienter verwalten, die Reaktionszeiten verbessern und Schulungskosten reduzieren. Der AppleCare Help Desk Support bietet unbegrenzten Support für Hardware- und Softwarediagnosen sowie Problembehebung und Problemeingrenzung für iOS Geräte.

AppleCare für Benutzer von iOS Geräten

Für jedes iOS Gerät gilt eine einjährige eingeschränkte Herstellergarantie. Zusätzlich kann innerhalb von 90 Tagen ab Kaufdatum technischer Telefonsupport in Anspruch genommen werden. Der Anspruch auf Service lässt sich mit AppleCare+ für das iPhone, AppleCare+ für das iPad oder dem AppleCare Protection Plan (APP) für den iPod touch auf zwei Jahre ab Kaufdatum verlängern. Benutzer können sich beliebig oft mit Fragen an die Experten des Apple Support Teams wenden. Apple bietet zudem praktische Service-Optionen an, wenn Geräte repariert werden müssen. Außerdem sind im Leistungsumfang von AppleCare+ für das iPhone bzw. für das iPad bis zu zwei Fälle von unabsichtlicher Beschädigung inbegriffen, für die jeweils eine Servicegebühr anfällt.

iOS Direct Service Programm

Als Vorteil von AppleCare+ und des AppleCare Protection Plan ermöglicht das iOS Direct Service Programm Ihrem Helpdesk, Geräte auf Probleme hin zu untersuchen, ohne bei AppleCare anzurufen oder einen Apple Store zu besuchen. Ihre Organisation kann bei Bedarf direkt Ersatz für ein iPhone, ein iPad oder einen iPod touch oder für ein zum Lieferumfang gehörendes Zubehörprodukt bestellen.

Weitere Infos zu AppleCare Programmen: www.apple.com/de/support/professional

Zusammenfassung

Wenn Ihr Unternehmen iOS Geräte für eine Gruppe von Benutzern oder in der gesamten Organisation implementieren möchte, haben Sie viele Optionen für die einfache Implementierung und Verwaltung der Geräte. Die Wahl der richtigen Strategien kann es den Mitarbeitern Ihrer Organisation ermöglichen, produktiver zu arbeiten und ihre Arbeit auf völlig neue Art und Weise zu erledigen.

Weitere Infos zur Integration von iOS in IT-Umgebungen in Unternehmen: www.apple.com/de/business/products-platform/

[1]Nicht alle Dienste und Apps sind in jedem Land verfügbar. Informieren Sie sich bitte vor Ort. Siehe Verfügbarkeit von Programmen und Inhalten.

[2]Einige Funktionen erfordern eine WLAN Verbindung. Einige Funktionen sind nicht in allen Ländern verfügbar. Die empfohlenen und Mindestsystemvoraussetzungen für iCloud finden Sie unter https://support.apple.com/de-de/HT204230.