Überblick über die iOS Implementierung in Unternehmen

Inhalt

Überblick

Mit dem iPad und iPhone können Sie die Arbeitsabläufe in Ihrem Unternehmen und die Arbeit Ihrer Mitarbeiter optimieren. Die Geräte können zu erheblichen 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, iPad und iPhone 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 Inhalte nach Bedarf implementieren.

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

In diesem Dokument erhalten Sie Hinweise zur Implementierung von iOS Geräten in Ihrer Organisation und Hilfe bei der Erstellung eines Implementierungsplans, der am besten zu Ihrer Umgebung passt. Diese Programme und diese Werkzeuge werden in diesem Überblick im Abschnitt „Implementierungsschritte“ beschrieben. Weiterführende Informationen erhalten Sie online in der „iOS-Implementierung: Referenz“.

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

Eigentumsmodelle

Ein wichtiger erster Schritt bei der Implementierung ist die Beurteilung von Eigentumsmodellen und die Wahl des für Ihre Organisation geeigneten Modells. Es gibt verschiedene Implementierungskonzepte, je nachdem, wer Eigentümer des Geräts ist. Beginnen Sie damit, herauszufinden, was für Ihre Organisation am besten ist.

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. Zum Beispiel nutzt eine Firmenzentrale möglicherweise eine

Strategie, bei der die Geräte im Besitz der Benutzer sind. Die Strategie gestattet den Mitarbeitern, ein privates iPad einzurichten, wobei die Unternehmensressourcen ohne Auswirkungen auf persönliche Daten und Apps des Benutzers geschützt und verwaltet werden. In den Einzelhandelsfilialen dieser Firma hingegen wird vielleicht eine Strategie befolgt, bei der die Geräte im Besitz der Organisation sind. Beispielsweise teilen sich mehrere Mitarbeiter iOS Geräte, um mit diesen Geräten Kundentransaktionen durchzuführen.

Wenn Sie diese Implementierungsmethoden genauer erkunden, fällt es Ihnen leichter, die beste Wahl für Ihre ganz spezifische Umgebung zu identifizieren. Nachdem Sie das passende Implementierungsmodell für Ihre Organisation ermittelt haben, kann Ihr Team die Implementierungs- und Verwaltungsfunktionen von Apple im Detail erkunden.

Geräte im Besitz der Organisation

Bei einem Modell mit Geräten im Besitz der Organisation können Sie Geräte bei Apple oder einem teilnehmenden, von Apple Autorisierten Händler bzw. 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 Implementierungsmethoden miteinander kombinieren, können die Einrichtung und Konfiguration der Geräte mithilfe zentraler Technologien von Apple und einer MDM-Lösung vollkommen automatisiert erledigt werden.

Persönlich anpassbares Gerät. Bei einer Strategie mit persönlich anpassbaren Geräten können die Benutzer ihre Geräte bei einer MDM-Lösung registrieren, die Einstellungen und Apps der Organisation drahtlos bereitstellt. Bei Geräten, die direkt bei Apple oder bei teilnehmenden, von Apple Autorisierten Händlern bzw. Mobilfunkanbietern gekauft wurden, können Sie auch die Vorteile des DEP nutzen, um neue Geräte automatisch bei Ihrer MDM-Lösung anzumelden. 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 in der Regel 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 im Falle von Geräten ausführen müssen, die im Besitz des Unternehmenssind. Wenn nicht anders angegeben, beziehen sich diese Aufgaben sowohl auf Implementierungen mit *persönlich anpassbaren* als auch mit *nicht personalisierten* Geräten.

	Administrator	**Benutzer**
Vorbereiten	Infrastruktur auswerten Eine MDM-Lösung wählen Bei Apple Bereitstellungsprogrammen registrieren	Kein Benutzereingriff erforderlich
Einrichten	Geräte konfigurieren Apps verteilen	Kein Benutzereingriff erforderlich
Implementieren	Geräte verteilen **Nur persönlich anpassbares Gerät** Benutzern die Personalisierung erlauben	**Nur persönlich anpassbares Gerät** Apps laden und installieren Einladung zum VPP annehmen (optional) Apple ID, iTunes Store und iCloud Accounts verwenden, falls zutreffend **Nur bei nicht personalisierten Geräten** Kein Benutzereingriff erforderlich

	Administrator	Benutzer
Verwalten	Geräte verwalten Zusätzliche Inhalte bereitstellen und verwalten	**Nur persönlich anpassbares Gerät** Zusätzliche Apps entdecken **Nur bei nicht personalisierten Geräten** Kein Benutzereingriff erforderlich

Benutzereigene Geräte

Wenn Geräte vom Benutzer gekauft und eingerichtet werden, was üblicherweise als *BYOD*- bzw. *Bring-Your-Own-Device*-Implementierung bezeichnet wird, können Sie trotzdem Zugriff auf Unternehmensdienste wie WLAN, Mail und Kalender erteilen, und zwar über MDM. 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 vorgeben, 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 im Falle von Geräten ausführen müssen, die im Besitz des Benutzers sind.

	Administrator	Benutzer
Vorbereiten	Infrastruktur auswerten Eine MDM-Lösung wählen Bei Apple Bereitstellungsprogrammen registrieren	Apple ID, iTunes Store und iCloud Accounts verwenden, falls zutreffend
Einrichten	Geräte konfigurieren Apps verteilen	Bei MDM-Lösung des Unternehmens anmelden Apps laden und installieren
Implementieren	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 implementieren und Geräte verwalten. Wie gesagt, hängen die verwendeten Schritte davon ab, ob die Organisation oder der Benutzer Eigentümer der Geräte ist.

1. Vorbereiten

Nachdem Sie herausgefunden haben, welche Implementierungsmethode für Ihre Organisation die richtige ist, folgen Sie diesen Schritten, um den Grundstein für die Implementierung zu legen. Diese Aktionen können Sie bereits durchführen, bevor die Geräte überhaupt zur Verfügung stehen.

Infrastruktur auswerten

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

WLAN und Netzwerk

Für die Einrichtung und Konfiguration von iOS Geräten ist eine stabile drahtlose Verbindung unverzichtbar. Somit ist zu überprüfen, ob das WLAN des Unternehmens mehrere Geräte mit gleichzeitigen Verbindungen von allen Benutzern unterstützt. Ein Web-Proxy bzw. Firewall-Ports müssen konfiguriert werden, wenn die Geräte nicht auf die Apple Aktivierungsserver, auf iCloud oder den iTunes Store zugreifen können. 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 Quality of Service (QoS).

Bewerten Sie Ihre VPN-Infrastruktur, um sicherzustellen, dass die Benutzer über ihre iOS Geräte per Fernzugriff sicher auf Unternehmensressourcen zugreifen können. Das iOS Feature „VPN On Demand“ ermöglicht es, eine VPN-Verbindung nur dann zu starten, wenn sie benötigt wird. Wenn Sie App-basiertes VPN 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 zum Verbinden mit AirPrint kompatiblen Druckern und AirPlay kompatiblen Geräten wie Apple TV. Manche Apps verwenden Bonjour auch zum Erkennen anderer Geräte für elektronisches Teamwork und Netzwerkfreigaben.

Weitere Informationen zu WLAN und Netzwerkfunktionen für Implementierungen in Unternehmen finden Sie unter „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 iOS Geräten zu unterstützen, die eine Verbindung dazu herstellen werden. Wird Exchange nicht verwendet, kann iOS mit standardbasierten Servern per IMAP, POP, SMTP, CalDAV, CardDAV und LDAP verwendet werden.

Caching Server

Caching Server ist ein integriertes Feature von macOS Server. Er speichert eine lokale Kopie häufig nachgefragter Inhalte von Apple Servern, um so die Bandbreite zu minimieren, die zum Laden von Inhalten in Ihr Netzwerk erforderlich ist. Caching Server beschleunigt das Laden und das Bereitstellen von Software über den App Store, Mac App Store, iTunes Store und iBooks Store. Auch Softwareaktualisierungen können zum schnelleren Laden auf iOS Geräte im Cache zwischengespeichert werden.

Weitere Informationen zum Caching Server finden Sie unter:
www.apple.com/de/macos/server/features/#caching-server

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

iTunes unterstützt mehrere Konfigurationsoptionen, die für Unternehmen geeignet sind, etwa 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 in der Unternehmensumgebung sicher zu registrieren, Einstellungen drahtlos zu konfigurieren und zu aktualisieren, die Einhaltung von Richtlinien zu überwachen sowie Apps zu implementieren. Außerdem können Organisationen die per MDM verwalteten Geräte ferngesteuert löschen bzw. sperren. Diese Verwaltungsfunktionen werden von MDM-Lösungen anderer Anbieter bereitgestellt.

Für die verschiedenen Serverplattformen ist eine Reihe von MDM-Lösungen anderer Anbieter verfügbar. Jede Lösung bietet andere Verwaltungskonsolen und Features zu unterschiedlichen Preisen. Vor der Entscheidung für eine Lösung sollte anhand der unten aufgeführten Ressourcen bewertet werden, welche Verwaltungsfunktionen für die jeweilige Organisation am wichtigsten sind. Neben MDM-Lösungen anderer Anbieter steht eine Lösung von Apple zur Verfügung, der sogenannte Profilmanager, ein Feature von macOS Server.

Weitere Infos zu MDM: www.apple.com/ipad/business/it/management.html

Weitere Informationen über den Profilmanager finden Sie unter:
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.

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. Wenn Apple Bereitstellungsprogramme für Sie Neuland sind, sollten Sie wissen, dass der Account, der während der Registrierung erstellt wird, der Account des Programmvertreters ist. Derselbe Programmvertreter-Account kann zur Registrierung beim jeweiligen Programm genutzt werden.

Programm zur Geräteregistrierung (DEP)
Das DEP bietet eine schnelle, optimierte Möglichkeit, diejenigen iOS und macOS Geräte im Besitz der Organisation zu implementieren, die direkt bei Apple oder bei von Apple Autorisierten Händlern bzw. Mobilfunkanbietern gekauft wurden, welche an diesem Programm teilnehmen. Sie können die erste Einrichtung vereinfachen, indem Sie die MDM-Registrierung und Betreuung der Geräte automatisieren, ohne dass Sie sie manuell einrichten oder vorbereiten müssen, bevor die Benutzer sie erhalten. Darüber hinaus kann der Konfigurationsprozess für Benutzer weiter vereinfacht werden, indem Sie bestimmte Schritte im Systemassistenten entfernen, sodass die Benutzer schnell loslegen können. Sie können auch steuern, ob der Benutzer das MDM-Profil vom Gerät löschen darf. Weitere Informationen über die Betreuung erhalten Sie im Abschnitt „Betreute Geräte“ auf den folgenden Seiten.

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. Sie können mit einer geschäftlichen Kreditkarte oder über das VPP-Guthaben zahlen, das Sie über einen Auftrag erworben haben.

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

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

Apple Developer Enterprise Program
Entwickeln Sie mit Hilfe des Apple Developer Enterprise Program interne iOS Apps zur Verwendung in Ihrem Unternehmen. Dieses Programm stellt einen vollständigen und integrierten Prozess für Entwicklung, Test, Debugging und Verteilung von iOS Apps an Mitarbeiter in Ihrer Organisation bereit. Interne Apps werden nicht beim App Store eingereicht und nicht von Apple geprüft, genehmigt oder gehostet.

Sie können interne Apps verteilen, indem Sie diese 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 Einmalanmeldung konfiguriert und Richtlinien für den Netzwerkzugriff festgelegt (etwa per app-basiertem VPN) 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. Einrichtung

In diesem Schritt konfigurieren Sie die Geräte und verteilen Ihre Inhalte, indem Sie 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 welche Bereitstellungsart 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, melden Sie die Geräte auf sichere Weise mithilfe eines Konfigurationsprofils bei einem MDM-Server an. Dabei handelt es sich um eine XML-Datei, mit deren Hilfe Konfigurationsdaten auf iOS Geräte übertragen werden können. Konfigurationsprofile 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 der Organisation.** Verwenden Sie das DEP, damit die Geräte Ihrer Benutzer bei der Aktivierung automatisch bei MDM registriert werden. Sie können die MDM-Beziehung zu einem Gerät aufheben, indem Sie mit der MDM-Konsole das Konfigurationsprofil entfernen, in welchem die MDM-Serverinformationen enthalten sind.

- **Benutzereigene Geräte** Die Mitarbeiter können sich entscheiden, ob sie ihr Gerät bei MDM registrieren wollen oder nicht. Sie können die Registrierung bei MDM auch jederzeit aufheben, indem sie das Konfigurationsprofil auf ihrem Gerät ganz einfach 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 mit Hilfe des Apple Push-Benachrichtigungsdienstes (APNs) über die Aktion des Administrators benachrichtigt, damit es direkt mit seinem MDM-Server über eine sichere Verbindung 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 auf die neueste Version von iOS aktualisieren, Geräteeinstellungen und -einschränkungen konfigurieren und Apps sowie andere Inhalte installieren. Und nach der ursprünglichen Einrichtung kann alles drahtlos via MDM verwaltet werden.

Apple Configurator 2 hat eine komplett neue Benutzeroberfläche, die auf Ihre Geräte und auf die einzelnen Aufgaben ausgerichtet ist, die Sie darauf ausführen wollen. Diese App ist jetzt nahtlos in das DEP integrierbar, sodass Geräte mithilfe von DEP-Einstellungen automatisch bei MDM registriert werden. Eigene Workflows können in Apple Configurator 2 mit Vorlagen (Blueprints) erstellt werden, um einzelne Aufgaben zusammenzuführen.

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. Sie gestatten Einschränkungen wie etwa AirDrop oder die Aktivierung des Einzel-App-Modus auf dem Gerät. Die Betreuung bietet neben vielen anderen Möglichkeiten auch die Möglichkeit, einen Web-Filter über einen globalen Proxy zu aktivieren, um sicherzustellen, dass der Internetdatenverkehr der Benutzer immer den Richtlinien der Organisation entspricht, um so zu verhindern, dass Benutzer ihr Gerät auf die Werkseinstellungen zurücksetzen. Standardmäßig sind alle iOS Geräte nicht betreut. Die Aktivierung des betreuten Modus kann mit DEP oder auch manuell mithilfe von Apple Configurator 2 erfolgen.

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

Eine ungekürzte Liste betreuter Einstellungen finden Sie unter iOS-Implementierung: Referenz.

Apps verteilen

Apple bietet umfangreiche Programme, mithilfe derer Ihre Organisation von den hervorragenden Apps und Inhalten profitieren kann, die für iOS erhältlich sind. Somit können Sie über das VPP gekaufte Apps 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 dazu nutzen, um die im VPP Store gekauften 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 deaktiviert ist.

- **VPP Apps Geräten zuweisen.** Mit Ihrer MDM-Lösung oder mit Apple Configurator 2 können Sie die Apps den Geräten direkt 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 mit MDM auf das Gerät gepusht, ohne dass eine Einladung erforderlich ist. Jeder Benutzer dieses Geräts hat Zugriff auf die App.

- **VPP Apps Benutzern zuweisen.** Verwenden Sie Ihre MDM-Lösung, um Benutzer per E-Mail oder Push-Benachrichtigung einzuladen. Zum Annehmen der Einladung melden sich die Benutzer auf ihren Geräten mit einer persönlichen Apple ID 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 des Benutzers 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 und behält die Kontrolle über die gekauften Apps.

Einlösecodes

Sie können Inhalte auch mit Einlösecodes verteilen. 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 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 Einlösecodes über MDM, Apple Configurator 2, E-Mail oder eine interne Website verteilen.

Apps und Inhalte mit Apple Configurator 2 installieren (optional)

Apple Configurator 2 kann nicht nur für einfache Einrichtungs- und Konfigurationsaufgaben, sondern auch zur Installation von Apps und Inhalten verwendet werden. Bei Implementierungsmodellen mit persönlich anpassbaren Geräten können Sie alle Apps im Voraus installieren und sparen so Zeit und Netzwerkbandbreite. Bei Implementierungen 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 VPP. Dokumente sind für Apps verfügbar, die die Dateifreigabe mit iTunes unterstützen. Sie können Dokumente auf iOS Geräten anzeigen bzw. abrufen, indem Sie diese mit einem Mac verbinden, auf dem Apple Configurator 2 ausgeführt wird.

3. Implementieren

Mit iOS können Mitarbeiter mit ihren Geräten ganz einfach direkt 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 mit Hilfe 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 von Kiosks, 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, wie zum Beispiel Sprache, Standort, Siri, iCloud und „Mein iPhone suchen“. Geräte, die im DEP registriert sind, können automatisch bei MDM registriert werden, und zwar direkt im Systemassistenten.

Benutzern die Personalisierung erlauben

Bei Implementierungsmodellen mit persönlich anpassbaren Geräten und bei BYOD-Implementierungen wird die Produktivität erhöht, 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 zum Anmelden bei verschiedenen Apple Diensten wie FaceTime, iMessage, iTunes Store, App Store, iBooks Store und iCloud verwendet wird. Diese Dienste bieten den Benutzern Zugriff auf eine Vielzahl von Inhalten zur Optimierung von geschäftlichen Aufgaben, zur Steigerung der Produktivität und Unterstützung der Zusammenarbeit.

Zur optimalen Nutzung dieser Dienste 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

Melden Sie sich an, um eine neue Apple-ID zu erhalten: appleid.apple.com/de

iCloud

Mit iCloud können Benutzer Dokumente und persönliche Inhalte wie Kontakte, Kalender, Dokumente und Fotos automatisch synchronisieren und sie zwischen verschiedenen Geräten aktuell halten.* Die Benutzer können auch automatisch Backups von iOS Geräten erstellen, wenn eine WLAN-Verbindung besteht, und mithilfe von „Mein iPhone suchen“ ein gestohlenes oder verloren gegangenes iPhone bzw. iPad oder einen gestohlenen oder verloren gegangenen iPod touch bzw. Mac lokalisieren.

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 ein Backup verwalteter Apps in iCloud erstellt wird. Die Benutzer haben so den Vorteil, iCloud für ihre persönlichen Daten nutzen zu können, ohne dass dort Unternehmensinformationen gespeichert werden. Es erfolgt auch kein Backup von Daten aus Unternehmens-Accounts wie Exchange oder aus internen Apps des Unternehmens in iCloud.

Hinweis: iCloud ist nicht in allen Ländern verfügbar. Die iCloud Features können je nach Land variieren.

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

4. Verwalten

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

Ihre Geräte verwalten

Ein verwaltetes Gerät kann vom MDM-Server mit Hilfe 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 und Softwareinformationen wie die iOS Version sowie eine detaillierte Liste aller Apps, die auf dem Gerät installiert sind. Mithilfe dieser Informationen kann sichergestellt werden, dass die Benutzer dauerhaft die geeigneten Apps installiert haben.

Verwaltungsaufgaben

Wenn ein Gerät verwaltet wird, kann über einen MDM-Server eine Vielzahl von Verwaltungsaufgaben ausgeführt werden, z. B. das automatische Ändern von Konfigurationseinstellungen ohne Benutzereingriff, das ferngesteuerte Sperren oder Löschen eines Geräts oder das Deaktivieren der Code-Sperre, sodass die Benutzer ihre Passwörter zurücksetzen können, falls sie diese vergessen haben. Über einen MDM-Server kann ein iOS Gerät auch angewiesen werden, mit dem AirPlay Mirroring an ein bestimmtes Ziel zu beginnen oder eine laufende AirPlay Sitzung zu beenden.

Modus „Verloren"

Ihre MDM-Lösung kann unter iOS 9.3 oder neuer ein betreutes Gerät ferngesteuert in den Modus „Verloren" setzen. Mit dieser Maßnahme wird das Gerät gesperrt. Es besteht die Möglichkeit, eine Nachricht mit einer Telefonnummer auf dem Sperrbildschirm des Geräts anzuzeigen. Im Modus „Verloren" können betreute Geräte, die verloren gegangen sind oder gestohlen wurden, geortet werden, da die MDM-Lösung per Fernzugriff deren Standort abfragt. Für den Modus „Verloren" muss „Mein iPhone suchen" nicht aktiviert sein.

Aktivierungssperre

Unter iOS 7.1 oder neuer 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 die Datensicherheit gehandhabt wird, wenn ein Benutzer aus der Organisation ausscheidet – und all das in Koexistenz mit den persönlichen Apps und Daten des Benutzers.

Portale für interne Apps

Sie haben die Möglichkeit, ein internes App-Portal für Ihre Mitarbeiter einzurichten, wo sie Apps für ihre iOS Geräte ganz einfach finden können. Über dieses Portal können interne Apps, URLs für App Store Apps, VPP-Codes 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 Installation, Konfiguration, Verwaltung und Entfernung von Apps, Accounts und Dokumenten aus dem App Store und von eigenen, intern entwickelten Apps und Inhalten kontrolliert.

- **Verwaltete Apps.** In iOS ermöglichen verwaltete Apps einer Organisation 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 oder vom Benutzer entfernt werden, indem er diese selbst auf seinem eigenen Gerät von MDM entfernt. Durch das Entfernen einer App werden auch die der App zugeordneten Daten entfernt. Ist eine App dem Benutzer immer noch über das VPP zugewiesen bzw. hat der Benutzer die App anhand eines Gutscheincodes 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 helfen, einen schnellen Einstieg zu finden, indem ihre E-Mail Accounts und weitere Accounts automatisch eingerichtet werden. Abhängig vom MDM-Lösungsanbieter und dessen 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 versehen werden.

- **Verwaltete Bücher und Dokumente.** Mithilfe von MDM-Tools können Bücher, ePub-Bücher und PDF-Dokumente automatisch auf die Geräte der Benutzer gepusht werden. So steht den Benutzern immer alles zur Verfügung, was sie brauchen. Gleichzeitig können verwaltete Bücher aber nur in anderen verwalteten Apps genutzt oder über verwaltete Accounts per E-Mail versendet werden. Materialien, die nicht mehr benötigt werden, können 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 verwalteter Apps. Zum Beispiel legt die IT-Abteilung eine Reihe von Standardeinstellungen für eine Sharepoint App fest, 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 zur Steigerung der Akzeptanz mobiler Technologien in Unternehmen.

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.** Diese Einschränkung schützt Unternehmensdaten, indem sie steuert, mit welchen Apps und Accounts Dokumente und Anhänge geöffnet werden dürfen. Die IT-Abteilung kann eine Liste der Apps konfigurieren, die im Freigabebildschirm verfügbar sind. So verbleiben Arbeitsdokumente in unternehmenseigenen Apps, und es wird verhindert, dass persönliche Dokumente mit verwalteten Apps geöffnet werden. Diese Richtlinie gilt auch für andere Dokumentanbieter und für Tastatur-Apps anderer Anbieter.

- **Einzel-App-Modus.** Diese Einstellung hilft dem Benutzer dabei, sich auf eine Aufgabe zu konzentrieren, während er ein iOS Gerät nutzt, denn das Gerät wird auf eine einzige App eingeschränkt. Entwickler können diese Funktion auch innerhalb ihrer Apps aktivieren, sodass die Apps den Einzel-App-Modus unabhängig voneinander 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 Benutzern und Administratoren von iOS eine Vielzahl von Programmen und Support-Optionen.

AppleCare for Enterprise

Falls Ihr Unternehmen umfassenden Schutz wünscht, kann AppleCare for Enterprise Sie bei der Entlastung Ihres internen Helpdesks unterstützen. Dies erfolgt durch die Bereitstellung von technischem Support für Mitarbeiter per Telefon, der rund um die Uhr mit Antwortzeiten von einer Stunde bei Problemen mit höchster Priorität erfolgt. 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 unternehmensspezifische Supportangebote per Telefon und E-Mail für Umgebungen unter iOS, macOS und macOS Server. Das Produkt bietet je nach gekaufter Supportstufe Support bis zu rund um die Uhr 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 Trainingskosten reduzieren. AppleCare Help Desk Support bietet unbegrenzt Hilfe bei Fragen zu Hardware- und Softwarediagnose sowie Fehlerbeseitigung und Problemisolierung für iOS Geräte.

AppleCare für Benutzer von iOS Geräten

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

iOS-Direct-Service-Programm

Als Vorteil von AppleCare+ und dem AppleCare Protection Plan ermöglicht das iOS-Direct-Service-Programm Ihrem Helpdesk, Geräte auf Probleme hin zu untersuchen, ohne bei AppleCare anrufen oder einen Apple Store besuchen zu müssen. Ihre Organisation kann bei Bedarf direkt Ersatz für ein iPhone, ein iPad oder einen iPod touch oder zum Lieferumfang gehörende Zubehörprodukte 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 vielfältige Optionen für die einfache Implementierung und Verwaltung der Geräte. Die Entscheidung für die richtigen Strategien kann es den Mitarbeitern Ihrer Organisation ermöglichen, produktiver zu arbeiten und neue Arbeitsformen auszuprobieren.

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

*Einige Features erfordern eine WLAN-Verbindung. Einige Features sind nicht in allen Ländern verfügbar. Bei einigen Diensten ist der Zugriff nur mit iOS 10 Geräten möglich.