Mobile Device Management

101

iPad und iPhone in Unternehmen optimal nutzen

Inhalt

Mobilität: Einführung

Die Evolution der Mobilität

Die Mobilität begann in den 1990er Jahren mit der Handschrifterkennungs -Technologie von Apple Newton und Palm Pilot und mit der Möglichkeit der Netzanbindung über ein Modem.

Mitte der 2000er kamen dann neue Anbieter auf den Smartphone-Markt. In Europa war Symbian das beliebteste Betriebssystem, in den USA war es Palm OS. Auf dem Markt drängten sich fünf mobile Betriebssysteme, ohne dass eines davon zum klaren Marktführer wurde.

2007 kam das iPhone auf den Markt, das erste Android Smartphone folgte dann 2008. Kurz nach der Einführung des iPhone bot der Apple App Store Entwicklern die Möglichkeit, native Apps für iOS zu entwickeln. Dies eröffnete eine ganz neue Welt der mobilen Produktivität und ermöglichte eine Optimierung der Geschäftsabläufe.

Ab 2007 gingen die Nutzungszahlen von BlackBerry und Windows Mobile rapide zurück; Palm, Symbian und SideKick sind ganz vom Markt verschwunden.

Die frühen Smartphones wurden von BlackBerry und Windows Mobile dominiert. Sie öffneten die Türen der mobilen Kommunikation.

iPhone

Android

Windows Phone

17

Heute dominieren drei große Betriebssystemanbieter den Mobilgerätemarkt. Die Smartphones haben sich weiterentwickelt und sind viel mehr als nur einfache Kommunikationsgeräte. Apps sind die Tools, die den Wandel der Mobilität und der Unternehmen ermöglichen.

Gründe für iOS

Von den drei vorherrschenden mobilen Betriebssystemen ist iOS die einzige Plattform, die für den Endverbraucher entwickelt wurde und in Unternehmen Fuß gefasst hat. Mit seiner intuitiven Benutzeroberfläche, seinem sicheren Ökosystem von Apps, die sich für den sofortigen Einsatz in Unternehmen eignen, und den integrierten Tools, die eine beispiellose Produktivität ermöglichen, überzeugt iOS auf ganzer Linie.

Schnellste und effizienteste mobile Hardware

Läuft auf iPhone und iPad mit unterschiedlichen Bildschirmgrößen

Native hardwarebasierte Verschlüsselung zum Schutz der Date

Gesundes Entwicklerökosystem mit 1,5 Millionen Apps im App Store und 40 Mrd. US-Dollar für Entwickler

Touch ID für biometrische Sicherheit

Über 70 % der Benutzer verwenden die neueste Version des Betriebssystems, die einmal im Jahr erscheint

Produktivitäts-Apps zum Erstellen von Dokumenten, Tabellen und Präsentationen, einschließlich Microsoft Office für iOS

Multitasking dank der Funktion zum Teilen des Bildschirms für iPad

Integrierte Unterstützung für moderne und sichere Drahtlosnetzwerke wie VPN und Single-Sign-On

Integrierte Microsoft Exchange-Unterstützung für E-Mail, Kalender und Kontakte

Gründe für eine geschäftliche Nutzung von iOS

Laut einer Studie von Harris Poll[1] fließt 2016 ein Großteil der IT-Investitionen in die Unternehmensmobilität. Aus der Studie geht hervor, dass mehr als 90% der IT Entscheidungsträger die Unternehmensmobilität als entscheidenden Faktor für die Kundenbindung, Wettbewerbsfähigkeit und betriebliche Produktivität 2016 sehen.

Unternehmen statten ihre Belegschaft nicht mit irgendeiner mobilen Technologie aus. Sie entscheiden sich immer öfter für iOS, weil es bei den Benutzern beliebt, leicht zu verwalten und dazu noch sicher ist. Durch die Wahl von iPad und iPhone für ihre Mitarbeiter ebnen Unternehmen jeglicher Form und Größe den Weg für ein stärkeres Engagement, verbesserte Geschäftspraktiken und mehr kreative und innovative Arbeit.

Wie viele Unternehmen entscheiden sich für iOS?

In der Jamf-Umfrage „Managing Apple Devices in the Enterprise Survey“[1] aus dem Jahr 2017 sagen fast alle IT-Fachkräfte in den Unternehmen, dass die Nutzung von iPad und iPhone in ihrem Zuständigkeitsbereich im Jahresvergleich um 76 % zunahm. Zudem waren 93 % der Umfrageteilnehmer der Meinung, dass die Implementierung von iPhone und iPad im Vergleich zu allen anderen Plattformen einfacher ist.

76%

der Unternehmen meldeten einen Zuwachs bei der Nutzung von iPhone und iPad in ihrem Umfeld

93%

der Umfrageteilnehmer sind der Meinung, dass die Implementierung von iPhone und iPad im Vergleich zu anderen Plattformen einfacher ist

Source 1 - Jamf
https://resources.jamf.com/documents/books/managing-apple-devices-in-the-enterprise.pdf

Mit iOS Geschäftsprozesse optimieren

Laut einer Theorie des amerikanischen Psychologen Abraham Maslow haben alle Menschen dieselben Grundbedürfnisse. Zunächst müssen die grundlegenden Bedürfnisse (Essen, Kleidung und Unterkunft) befriedigt werden, bevor sich der Mensch der nächsten Stufe wie Liebe und Selbstachtung widmet. Mit anderen Worten: Eine stetige Verbesserung ist nur möglich, wenn bestimmte Bedürfnisse befriedigt wurden.

Die Bedürfnishierarchie von Maslow lässt sich auch auf die Möglichkeiten von iOS in Unternehmen anwenden. Die Bereitstellung der Geräte und die Kommunikation sind die Grundbedürfnisse eines jeden Unternehmens. Doch iOS bietet noch viel mehr. Es ist das Tor zum unternehmerischen Wandel. Alle Unternehmen streben nach maximaler Produktivität und Kundenzufriedenheit. Vor diesem Hintergrund sind iOS-Apps ein Instrument zur Vereinfachung der Kommunikation, Verbesserung von Transaktionen und Optimierung von Geschäftsprozess.

Prozess

Um über die Grenzen des Möglichen hinauszugehen, investieren die innovativsten Unternehmen nicht nur in Hardware, sondern auch in benutzerdefinierte Apps, mit denen sie ihre Geschäftsprozesse optimieren können. Neben dem MobileFirst- Programm von IBM eignen sich hierzu auch B2B-Apps oder ternehmenseigene Apps.

Transaktionen

Der riesige App Store mit seinen Millionen von Apps eröffnet eine Vielzahl an Möglichkeiten für eine einfachere Abwicklung mobiler Transaktionen. Beispiele sind Square und Salesforce1 zur Verarbeitung von Kreditkartentransaktionen oder zur Übermittlung von Aufträgen für einen Geschäftsabschluss. Die Bereitstellung der App Store-App ist entscheidend, um das Potenzial von iOS-Geräten voll ausschöpfen zu können.

Kommunikation

Sobald sich die Geräte in den Händen der Benutzer befinden, müssen grundlegende Kommunikationsmöglichkeiten gegeben sein. Dazu gehören der Zugriff auf geschäftliche E-Mails, WLAN und VPN-Einstellungen – natürlich ohne das System unnötig aufzublähen.

Bereitstellung

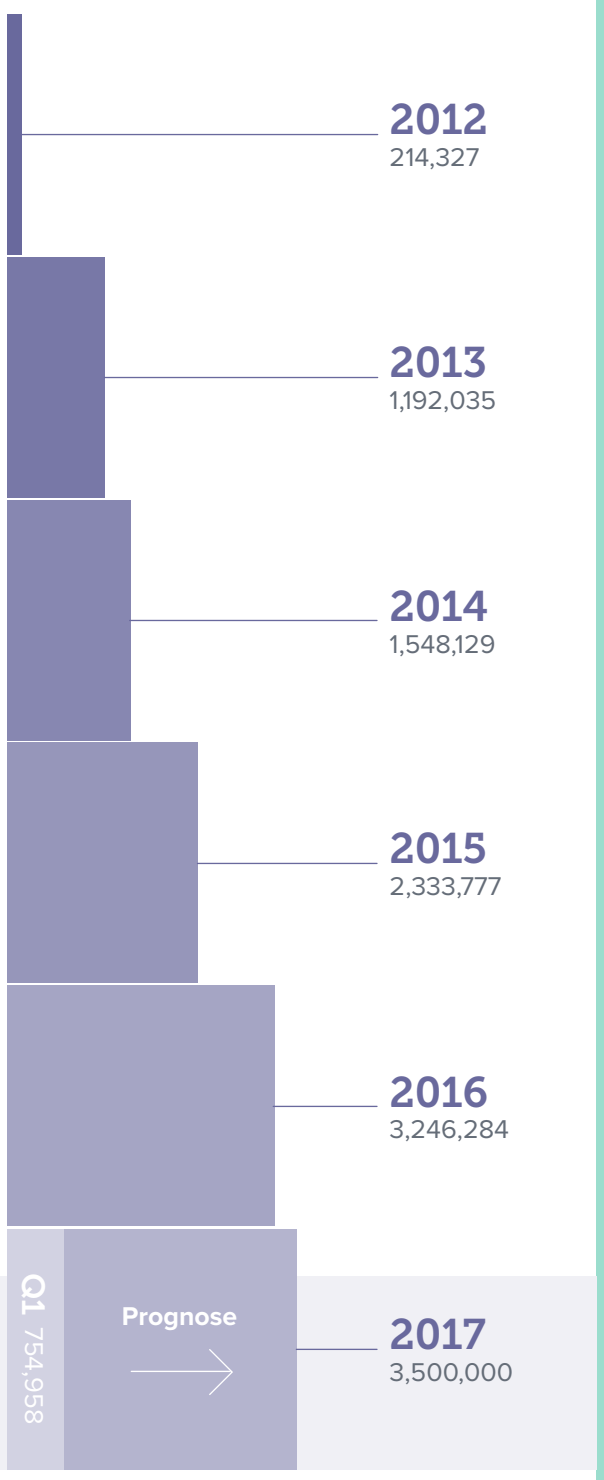
Unternehmen müssen sich dem Problem der Bereitstellung, Gerätekonfiguration und Bestandsverwaltung stellen. Das ist die unterste Ebene der Pyramide und die Grundlage für jedes Unternehmen, das eine Vielzahl von iOS-Geräten zu verwalten hat.

Was ist mit Android?

Das Betriebssystem von Google wird aufgrund seiner Vielzahl an Formfaktoren, den umfassenden Anpassungsmöglichkeiten und den meist günstigeren Geräten immer beliebter. Für Verbraucher oder BYOD-Programme kann sich Android als gute Wahl erweisen, weil die Benutzer auf andere Dinge Wert legen. Für Unternehmen hingegen ist es aufgrund von Fragmentierungs- und Sicherheitsproblemen schwierig, Android zu standardisieren und zu unterstützen.

Nutzungsquote

Beispiele für neue Android-Malware



Source 2 - Google: http://developer.android.com/about/dashboards/index.html
Source 1 - Apple: https://developer.apple.com/support/app-store/

Source 3 - G Data: https://public.gdatasoftware.com/Presse/Publikationen/Malware_Reports/G_DATA_MobileMWR_Q3_2015_EN.pdf

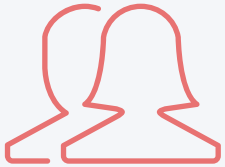
Mobile Device Management: Überblick

Was is MDM?

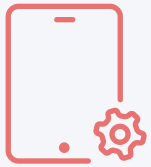
Mobile Device Management (MDM) ist das Framework von Apple zur Verwaltung von iOS. Um iOS-Geräte effizient verwalten und ihr gesamtes Potenzial ausschöpfen zu können, benötigen Unternehmen eine ebenso leistungsstarke MDM-Lösung. MDM bietet eine umfassende Palette an Tools, um umfangreiche Bereitstellungen zu bewältigen und die Sicherheit der Geräte zu gewährleisten – von der Bereitstellung neuer Geräte und der Bestandsaufnahme über die Konfiguration von Einstellungen und die Verwaltung von Apps bis hin zum Löschen von Daten.

Bereitstellung

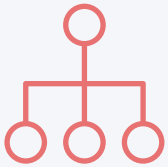
Inventar



Konfigurations-Profile



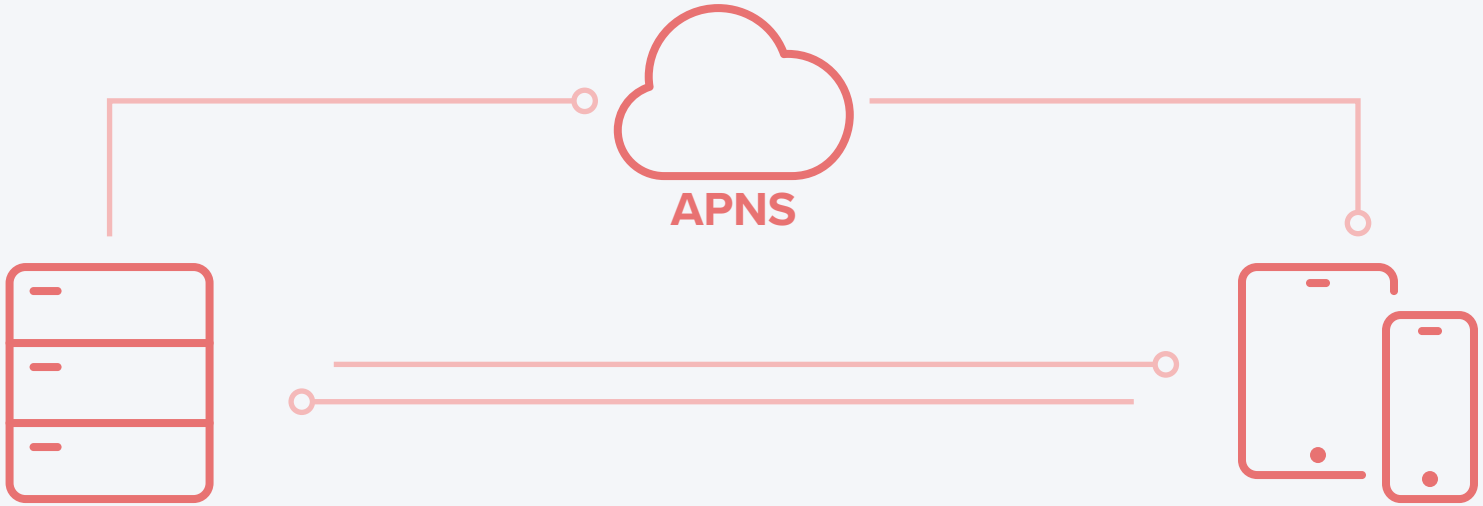
MDM-Befehle



App Bereitstellung

Sicherheit und Datenschutz

Architektur für MDM



Apple-Server für Push-Benachrichtigungen

Beim Senden von Befehlen an Apple-Geräte kommuniziert Ihr MDM-Server mit dem Server für Push- Benachrichtigungen von Apple (APNS). Der Apple-Server ist ständig mit den Geräten verbunden, sodass Sie sich darum nicht kümmern müssen. Die Geräte senden eine Antwort an den MDM-Server und erhalten die von Ihnen gesendeten Befehle, Konfigurationsprofile oder Apps.

Bereitstellungsmethoden

Bevor Sie MDM zur Verwaltung Ihrer iOS-Geräte nutzen können, müssen Sie die Geräte zunächst registrieren. Im Falle von iPad oder iPhone geht das ganz einfach mithilfe eines MDM-Tools. Darüber hinaus können Apps und Inhalte einheitlich verteilt und Sicherheitsund Zugriffsprofile eingerichtet werden. Es gibt mehrere Möglichkeiten zur Registrierung eines Apple-Mobilgeräts, etwa über den Apple Configurator, eine URL oder das Programm zur Geräteregistrierung (DEP) von Apple.

Bereitstellung

	Beschreibung	Benutzererfahrung	Betreuung	Am besten geeignet für
Programm zur Geräteregistrierung (DEP)	Automatische drahtlose Registrierung	Benutzer erhält verpacktes Gerät, das beim Einschalten automatisch konfiguriert wird	Ja – drahtlos	Verschicken der Geräte an Endbenutzer
Apple Configurator	Registrierung über eine Mac-App, die via USB eine Verbindung zu den Geräten herstellt	Entfällt – dieser Prozess wird von der IT übernommen, die Geräte dann an die Benutzer ausgibt	Ja – über Kabel	Modelle für gemeinsame Nutzung und Wagen
User Initiated via URL	Manuelle drahtlose Registrierung	Benutzer ruft eine bestimmte URL auf, um das Gerät automatisch zu konfigurieren	Nein	Geräte im Außendienst, die registriert werden müssen

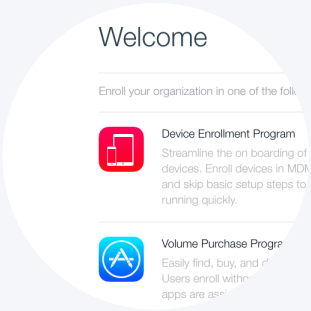
Betreuung

Mit dem Betreuungsmodus von iOS ist eine detailliertere Verwaltung durch einen MDM-Server möglich. Immer mehr Konfigurationen sind nur verfügbar, wenn das Gerät betreut wird. Es wird empfohlen, den Betreuungsmodus für unternehmenseigene Geräte zu aktivieren.

Beispiele für Befehle, die nur im Betreuungsmodus möglich sind:

- Kamera deaktivieren
- App Store deaktivieren
- Safari deaktivieren
- Deaktivieren das Ändern des Hintergrunds
- Option zum Hinzufügen von E-Mail-Konten deaktivieren
- und vieles mehr....

Bewährte Vorgehensweise: Vollautomatische Einrichtung mit dem Programm zur Geräteregistrierung (DEP)

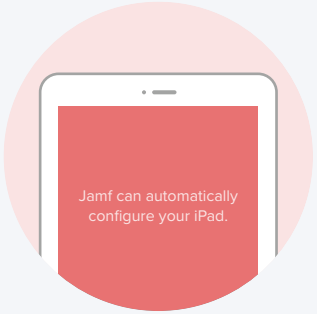


1

Registrieren Sie sich über die Apple-Website für DEP und fügen Sie dem DEP-Portal Ihren MDM-Server hinzu.

2

Kaufen Sie Geräte und verknüpfen Sie mit Ihrem DEP-Account. Lassen Sie direkt an die Benutzer liefern.



3

Wenn die Benutzer ihre iOS-Geräte zum ersten Mal einschalten, wird das Gerät automatisch registriert – sie müssen nichts weiter tun.

4

Das Gerät wird am MDM-Server registriert. Bereiten Sie eventuelle Konfigurationsprofile und Apps vor, die auf den Geräte installiert werden sollen.

5

Das Gerät empfängt die vorgesehenen Konfigurationen und Apps und der Benutzer wird zum Startbildschirm weitergeleitet. Das Gerät wird nun verwaltet und die Konfiguration ist abgeschlossen – ohne dass einer der IT-Mitarbeiter es in die Hand nehmen musste!

Inventar

MDM kann ein iOS-Gerät abfragen, um eine große Menge an Inventardaten zu erfassen. So wird sichergestellt, dass die Geräteinformationen immer auf dem neuesten Stand sind und Sie fundierte Verwaltungsentscheidungen treffen können. Das Inventar eines Geräts kann in verschiedenen Intervallen abgefragt werden und enthält Informationen wie Seriennummer, iOS-Version, installierte Apps und vieles mehr.

Datenerfassung mit MDM

Hardwaredetails

- Gerätetyp
- Gerätemodel
- Gerätename
- Seriennummer
- UDID
- Akkustatus

Softwaredetails

- iOS-Version
- Liste der installierte Apps
- Speicherkapazität
- Verfügbarer Speicherplatz
- Status des iTunes Store

Details zur Verwaltung

- Verwaltungsstatus
- Überwachungsstatus
- IP-Addresse
- Registrierungsmethoded
- Sicherheitsstatus

Weitere Details

- Installierte Profile
- Installierte Zertifikate
- Status der Aktivierungssperre
- Informationen zu Einkäufen
- Letzte Bestandsaktualisierung

Warum ist der Inventar so wichtig?

Sie können nicht verwalten, was Sie nicht erfassen können. Die von MDM erfassten Inventardaten lassen sich vielseitig verwenden und liefern Ihnen Antworten auf häufige Fragen wie: Sind meine Geräte sicher? Wie viele Apps wurden bereitgestellt? Welche iOSVersion wurde bereitgestellt?

Konfigurationsprofile

Anhand von Profilen können Sie die Verhaltensweise Ihrer Geräte steuern. Während Sie früher die Geräte manuell konfigurieren mussten, lässt sich dank der MDM-Technologie die Konfiguration von Code-Einstellungen, WLAN-Passwörtern oder VPN automatisieren. Außerdem haben Sie die Möglichkeit, die Nutzung bestimmter Elemente wie Kamera oder Safari-Webbrowser zu beschränken oder sogar das Gerät umzubenennen.

Verfügbare MDM Profil-Payloads

Die Grundlagen

- Passcode
- Restrictions
- Wi-Fi
- VPN
- Home Screen Layout
- Single App Mode
- LDAP
- Web Clips

E-mail-Accounts

- Mail
- Exchange ActiveSync
- Google Account
- VPN
- Calendar
- Contacts
- Subscribed Calendars
- macOS Server Account

Interneteinstellungen

- Global HTTP Proxy
- Content Filter
- Domains
- Cellular
- Network Usage Rules
- Certificates

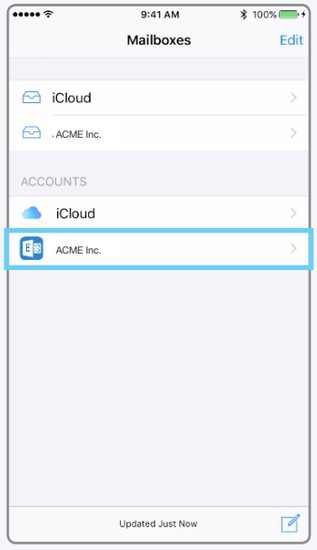
Sonstige Einstellungen

- AirPlay
- AirPlay Security
- Conference Room Display
- AirPrint
- Fonts
- SCEP
- Lock Screen Message
- Notifications
- Single Sign-on
- Access Point Name

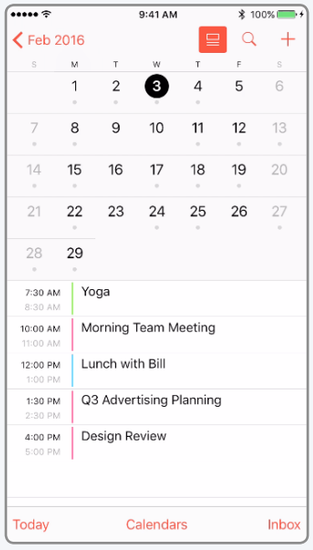
Bewährte Vorgehensweise: Container für iOS-Verwaltung meiden Management

In der Welt von MDM ist ein Container eine zusätzliche App, die als sicherer Ort für Geschäftsdaten wie E-Mails, Kalender, Kontakte und sogar für das Surfen im Internet verwendet wird. Dieses Konzept findet in Unternehmen zwar häufig Anwendung, geht jedoch auf Kosten einer guten Benutzererfahrung. Container wurden in einigen MDM-Lösungen populär, um Sicherheitslücken unter Android zu beseitigen.

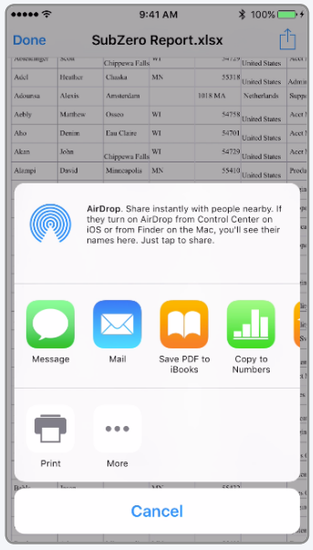
Die Wahrheit ist: iOS-eigene Apps wie Mail, Kalender, Kontakte und Safari sind bereits sicher. Man braucht keinen „sicheren“ E-Mail-Container. Nutzen Sie stattdessen Konfigurationsprofile. So gewährleisten Sie eine erstklassige Erfahrung für Ihre Benutzer. Mit einem Profil können Sie iOS einen Exchange-Accounthinzufügen, der dann Zugriff auf geschäftliche E-Mails und Kalender ermöglicht.



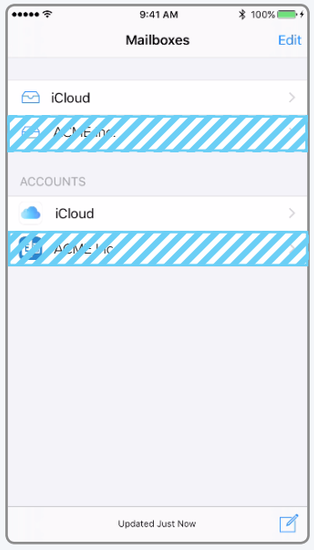
Ein Konfigurationsprofil fügt der nativen Mail-App einen Exchange-Account hinzu, und zwar direkt neben dem persönlichen E-Mail-Account des Benutzers.



Damit befinden sich die geschäftlichen Daten gleich neben den persönlichen Daten in den nativen Apps, was für die gewohnte Benutzererfahrung und Sicherheit sorgt.



Die IT kann darüber hinaus den Datenfluss kontrollieren, indem Apps das Öffnen von Anhängen im geschäftlichen E-Mail-Account untersagt wird.



Und zuletzt kann die IT, wenn ein Mitarbeiter das Unternehmen verlässt, einfach das Konfigurationsprofil entfernen, um den geschäftlichen E-Mail Account einschließlich sämtlicher Daten zu löschen. Persönliche Accounts werden dabei nicht gelöscht.

Bewährte Vorgehensweise: iPad standardisieren

Tragen Sie zur Steigerung der Produktivität ihrer Mitarbeiter bei, indem Sie auf allen unternehmenseigenen Geräten eine einheitliche Benutzerführung anbieten. Die Standardisierung von Apple Geräten für Ihre Mitarbeiter erfolgt mithilfe eines optimierten Einrichtungsverfahrens, welches den Benutzern ermöglicht, schnell auf die erforderlichen Apps zuzugreifen - und zwar zur richtigen Zeit und am richtigen Ort. Die Zeitersparnis beim Suchen nach Apps steigert die Produktivität der Benutzer.

Für die Standardisierung von iPad und iPhone in Ihrem Unternehmen gibt es drei Möglichkeiten:

Hintergrundbild für den Homescreen festlegen

Sorgen Sie durch die Anzeige des Hintergrundbilds mit Unternehmenslogo für eine einheitliche Markendarstellung.

Layout des Homescreens gestalten

Platzieren Sie Apps und Ordner sowie Weblinks auf dem Homescreen. Positionieren Sie hierbei die wichtigsten Apps auf der ersten Seite, weniger wichtige Apps auf anderen Seiten.

Apps anzeigen/verbergen

Zeigen Sie nur die Apps an, die Ihre Mitarbeiter benötigen. Verbergen Sie Apps, die für deren Arbeit nicht notwendig sind.

MDM-Befehle

MDM-Befehle sind spezifische Aktionen, die sich auf individuelle Geräte anwenden lassen, um die Sicherheit von Unternehmensdaten zu gewährleisten. Damit können Sie zum Beispiel auf den Verlust oder Diebstahl von Geräten reagieren, indem Sie das Gerät sperren oder sämtliche Daten löschen. Über weitere Befehle lassen sich Push-Benachrichtigungen senden, Geräte auf die neueste iOS-Version aktualisieren und Gerätenamen ändern, sodass die IT ihren Gerätebestand einfacher verwalten kann.

Verfügbare Befehle für MDM


INTERNETE-INSTELLUNGEN


GERÄT SPERREN


CODE LÖSCHEN


BESCHRÄNKUNGEN LÖSCHEN


VERWALTUNG DES GERÄTS AUFHEBEN


GERÄT LÖSCHEN


LEERE PUSH-BENACHRICHTIGUNG SENDEN


HINTERGRUND FESTLEGEN


BENACHRICHTIGUNG SENDEN


IOS AKTUALISIEREN


NAMEN ÄNDERN


GERÄT AUSSCHALTEN

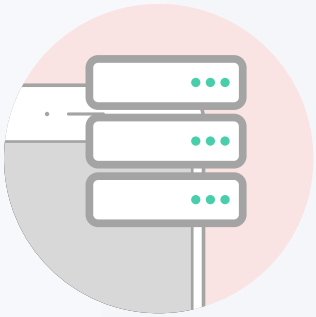

GERÄT NEU STARTEN


VERLOREN-MODUS UND TON

Bewährte Vorgehensweise: Aktivierungssperre mit MDM verwaltenwith

Die Aktivierungssperre soll den Diebstahl von iPhones und iPads verhindern. Durch die Abfrage von Apple ID und Kennwort des Besitzers kann das Gerät nicht von jedem x-Beliebigen entsperrt werden. Diese Funktion ist für die Benutzer wichtig, kann jedoch für IT-Administratoren zum Problem werden, wenn Geräte neu zugewiesen werden müssen. Ohne eine MDM-Lösung ist die Aktivierungssperre ein wahrer Verwaltungsalbtraum und hat in vielen Unternehmen dazu geführt, dass die Benutzer gar keine Apple IDs mehr verwenden dürfen.
Solange ein Gerät bei einem MDM-Server registriert ist und überwacht wird, können Sie einen Code zur Umgehung der Aktivierungssperre generieren, falls ein Gerät mit der Apple ID des vorherigen Benutzers gesperrt ist. Geben Sie im Systemassistenten den Code in das Kennwortfeld ein und schon ist das Gerät entsperrt.

1



Das Gerät ist bereits bei einem MDM-Server registriert und wird überwacht. Ein Code zur Umgehung der Aktivierungssperre wird auf dem MDM-Server generiert und gespeichert.

2

Das gesperrte Gerät wird der IT-Abteilung übergeben, die dann den auf dem MDM-Server gespeicherten Umgehungscode abruft.

3

Der IT-Mitarbeiter startet das Gerät im Systemassistenten neu und wird auf dem ersten Bildschirm nach der Apple ID und dem Kennwort des vorherigen Benutzers gefragt. Um die Aktivierungssperre zu umgehen, gibt der ITMitarbeiter den Code in das Kennwortfeld ein. Das Feld für die Apple ID bleibt leer. Das Gerät ist nun entsperrt.

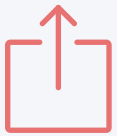
App-Bereitstellung

Ein iOS-Gerät ist schon beim Auspacken ein tolles Kommunikationstool, die umfassende App-Bibliothek für Freizeit und Beruf im iOS App Store kann die Produktivität der Benutzer jedoch noch steigern und Ihren Mitarbeitern helfen, über sich hinauszuwachsen. Außerdem können Sie mit den Apps im iOS App Store ein iPad in einer Kasse verwandeln, Reisekostenabrechnungen unterwegs erstellen und senden und sogar Geschäftsprozesse wie die Verwaltung von Verkaufszyklen oder das Unterschreiben von Verträgen optimieren. Mit einer App-Strategie und MDM zur Verwaltung Ihrer App-Bereitstellungen sorgen Sie dafür, dass die Benutzer immer Zugriff auf die nötigen Apps haben – konfiguriert und sicher für Ihre Umgebung.

Strategien zur App-Verwaltung

Was ist eine verwaltete App?

Verwaltete Apps wurden in iOS 5 eingeführt. Im Gegensatz zu Standard-Apps sind sie als Eigentum eines Unternehmens gekennzeichnet. Das bedeutet, dass verwaltete Apps via MDMTechnologie verteilt werden und so konfiguriert werden können, dass eine Sicherung der App-Daten nicht möglich ist und sie im Falle einer Entfernung des MDM-Profils gelöscht werden.



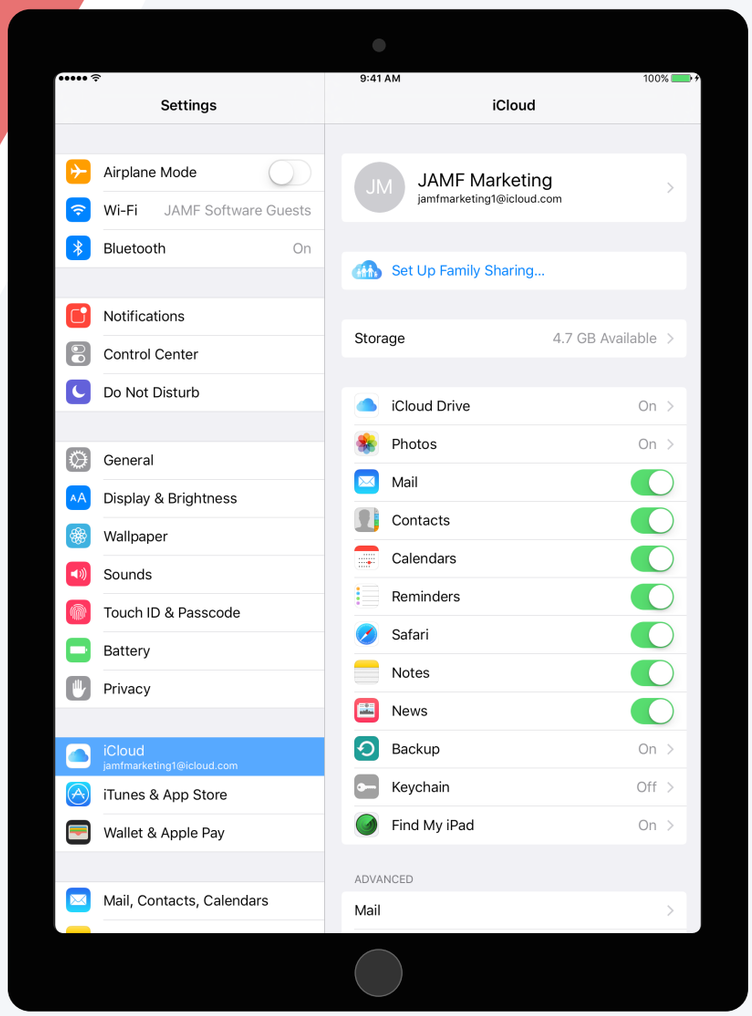
Managed Open In

„Managed Open In“ führt das Konzept der verwalteten Apps weiter, indem der Datenfluss zwischen den Apps kontrolliert wird. Unternehmen können so festlegen, welche Apps im iOS Share Sheet zum Öffnen von Dokumenten angezeigt werden. Zum Beispiel könnten Sie Regeln definieren, sodass E-Mail-Anhänge aus geschäftlichen Accounts nur in der Box-App und nicht in einem persönlichen Dropbox-Account geöffnet werden können. Dies ermöglicht eine wahrhaft native Datenverwaltung ganz ohne Container.

App-Konfigurationen

In manchen Fällen ist es mit der Bereitstellung einer App nicht getan und Sie möchten einige Einstellungen vorab anpassen. Hier kommt die App-Konfiguration ins Spiel. Die App-Entwickler können festlegen, welche Einstellungen sich von einem MDM-Server für ihre App vorkonfigurieren lassen. Zum Beispiel könnten Sie die Box-App mit bereits vorausgefüllter Server-URL bereitstellen, sodass die Benutzer lediglich ihren Benutzernamen und ihr Kennwort eingeben müssen, um die App nutzen zu können.

Bewährte Vorgehensweise: individuelle Apple IDs für Benutzer



Persönliche Apple IDs tragen zu einer gesteigerten Nutzung von iOS bei und unterstützen Ihre Benutzer bei der Suche nach spezifischen Lösungen für Geschäftsprobleme.

Was ist eine Apple ID?

Eine Apple ID ist ein persönlicher Account für Benutzer, über den sie auf Apple-Dienste wie den App Store, iTunes, iCloud, iMessage, FaceTime und vieles mehr zugreifen können. Eine Apple ID besteht aus einer E-Mail-Adresse und einem Kennwort. Außerdem sind Kontakt-, Zahlungs- und Sicherheitsdetails hinterlegt.

Warum sind Apple IDs für Benutzer wichtig?

Mit einer Apple ID können Benutzer alle Vorteile von iOS und App Store nutzen. Zum Beispiel haben sie damit Zugriff auf kostenlose Kommunikationsdienste von Apple wie FaceTime und iMessage oder andere Dienste wie „Mein iPhone suchen“ und iCloud.

Wie sieht es mit unternehmenseigenen Apps aus?

Da über den VPP-Store nun auch eine Lizenzierung von Apps anhand der Methode „verwaltete Verteilung“ möglich ist, können Sie Apps ganz einfach dem Gerät oder der Apple ID eines Benutzers zuweisen, ohne die Eigentumsrechte dauerhaft an den Benutzer zu übertragen. So muss die IT-Abteilung keine Zeit damit verschwenden, gerätespezifische Apple IDs zu erstellen.

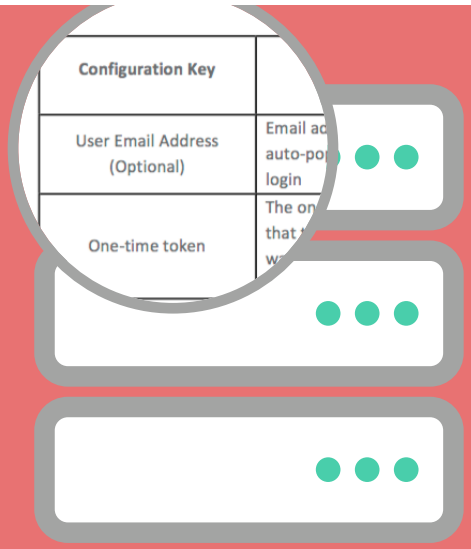
Welche Sicherheitsrisiken gibt es?

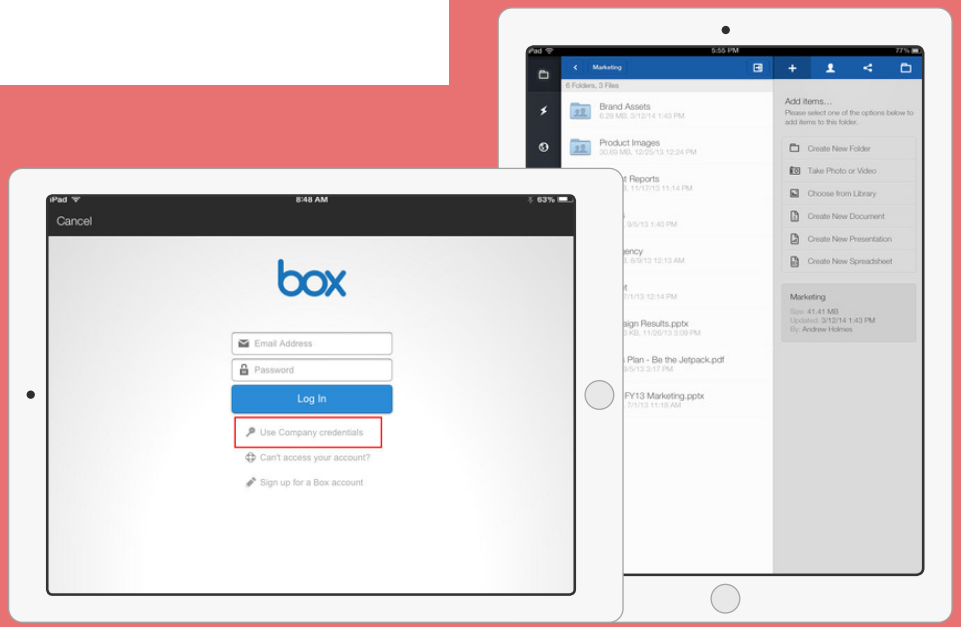
Durch die Verwendung von MDM-Funktionen wie „Managed Open In“ und die Beschränkungen in einem Konfigurationsprofil kann die IT die Sicherheitsrisiken besser eindämmen, sodass ein generelles Verbot von Apple IDs nicht notwendig ist. Die Apple-Dienste sind für ihre Sicherheit bekannt und das Hinzufügen einer persönlichen Apple ID zu einem Firmengerät stellt kein Sicherheitsrisiko dar. In einigen Fällen kann damit sogar die Sicherheit erhöht werden, weil Apple IDs die zweistufige Authentifizierung unterstützen.

Bewährte Vorgehensweise: Bereitstellungsbeispiel für verwaltete App-Konfiguration

Mit der Box-App für iPhone und iPad können Sie Ihre Arbeit auch unterwegs erledigen. Es ist schnell, sicher und benutzerfreundlich, damit Sie überall produktiv sein können. Darum wird es von mehr als 25.000 Millionen Menschen und 225.000 Unternehmen genutzt.

Stellen Sie Box über VPP mit vorkonfigurierten Optionen bereit, damit Ihre Benutzer auch davon Gebrauch machen.

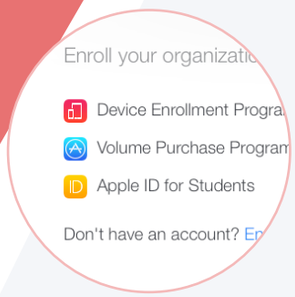




Box bietet eine Reihe von Konfigurationsschlüsseln, die Elemente wie URL, E-Mail-Adresse des Benutzers, Einmaltoken und vieles mehr vorgeben. Diese Konfigurationsschlüssel können Ihrem MDMServer hinzugefügt werden, um die Ersteinrichtung von Box zu automatisieren.

Sobald die App über Ihren MDM-Server bereitgestellt wurde, übernehmen die Konfigurationsschlüssel den Rest. Wenn Sie zum Beispiel die URL vorkonfiguriert haben, werden die Benutzer beim ersten Start von Box anstatt zum Standardbildschirm automatisch zum Anmeldebildschirm des Unternehmens weitergeleitet.

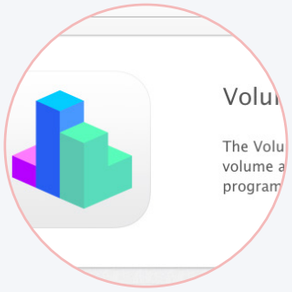
Bewährte Vorgehensweise: Apps über das Programm für Volumenlizenzen (VPP) bereitstellen



1

Registrieren Sie sich über die Apple- Website für VPP und verknüpfen Sie Ihren VPP-Account mit Ihrem MDM-Server.

2



Suchen Sie sich die gewünschten App-Lizenzen aus dem VPP Webstore aus. Auch kostenlose Apps müssen „gekauft“ werden.

3

Fügen Sie Ihrem MDM-Server die App-Lizenzen hinzu, einschließlich kostenloser apps.

?

Sie können die Apps entweder direkt einem Gerät oder der Apple ID eines Benutzers zuweisen.

4

Informieren Sie die Benutzer per E-Mail oder Push-Benachrichtigung über Ihre VPP-Bereitstellung.

4

Die Apps werden direkt auf dem Gerät bereitgestellt. Ganz ohne Interaktion oder Apple ID.

5

Apps, die mit der Apple ID eines Benutzers verknüpft sind, finden Sie auf dem Tab für Einkäufe im App Store.

Sicherheit und Datenschutz

Das Thema Sicherheit und Datenschutz spielt für Unternehmen eine wichtige Rolle. iOS verfügt daher über eine Reihe integrierter Sicherheitsfunktionen. Zusammen mit MDM können Sie dafür sorgen, dass nicht nur Ihre Geräte sicher sind, sondern auch Ihre Apps und Ihr Netzwerk.

Native Apple Security Features

VPN pro App

Virtual Private Networks (VPN) werden in Unternehmen seit Langem zur Verschlüsselung von Internetdatenverkehr verwendet. Bei traditionellen Desktopgeräten lässt sich der gesamte Datenverkehr über VPN leiten. Bei Mobilgeräten hingegen ist das nicht so einfach.Die Lösung von Apple: Unternehmen und App-Entwickler können auf App-Ebene definieren, welche Daten über VPN geleitet werden. Das spart Bandbreite und steigert die Netzwerkgeschwindigkeit.

Touch ID

Die meisten neuen iOS-Geräte verfügen über einen Fingerabdrucksensor, sodass das Betriebssystem zusätzlich biometrisch gesichert ist. Mit der Touch ID können Sie Geräte entsperren oder sich in bestimmten Apps anmelden. Die Fingerabdruckdaten werden lokal auf dem Gerät gespeichert und nicht an Apple weitergegeben.

Verschlüsselung

iOS verfügt über eine integrierte 256-Bit-Verschlüsselung, die bei eingestelltem Code automatisch aktiviert ist. Das bedeutet, dass die Daten auf Ihren Geräten auch ohne zusätzliche Software, die das Betriebssystem nur unnötig aufbläht, sicher sind. Da Apple sowohl die Hardware als auch die Software entwickelt, ist die Verschlüsselung so schnell, dass der Benutzer davon überhaupt nichts merkt.

Bewährte Vorgehensweise: MDM-Lösung zur Schadensverhütung einsetzen

Die Möglichkeit, ein betreutes Gerät mithilfe von MDM in den verwalteten Verloren-Modus zu schalten, ist eine entscheidende Sicherheitsoptimierung, die ab iOS 9.3 zur Verfügung steht. Mithilfe dieser Einstellung kann das Gerät geortet werden, was für das Auffinden verloren gegangener oder gestohlener Geräte unerlässlich ist. Zudem kann der Benutzer das Gerät erst dann entsperren, wenn der Verloren-Modus deaktiviert wurde. Zu diesem Zeitpunkt wird der Benutzer über sämtliche Standortdaten informiert, auf die zugegriffen wurde.

Der verwaltete Verloren-Modus wird vom Administrator gesteuert und muss von diesem deaktiviert werden, bevor das Gerät wieder einsatzbereit gemacht werden kann. Wie bei der Funktion „Mein iPhone suchen“ kann der Administrator Nachrichten an das Gerät senden, während dieses im verwalteten Verloren-Modus ist.

Szenarien

Einzelhändler müssen bei der Wahl der richtigen Technologie eine Vielzahl von Aspekten bedenken, auch im Hinblick auf ein reibungsloses Einkaufserlebnis. Dabei sind neben den Kassensystemen auch Treueprogramme, Dienstpläne, Buchhaltung und vieles mehr zu berücksichtigen. Ein iPad oder iPhone in Kombination mit leistungsstarken Apps stellt für Start-up-Unternehmen eine schnelle und bezahlbare Lösung dar. Bei Tausenden von Einzelhandels-Apps im App Store kann es jedoch schwierig sein, das Richtige zu finden. Im Folgenden haben wir eine Auswahl zusammengestellt.

Kassensystem

Kassensysteme waren früher groß, unhandlich, benutzerunfreundlich und nicht mobil. Dank iPad und iPhone, die heute so leistungsstark wie traditionelle Kassencomputer sind, ist Mobilität kein Problem mehr – und das, ohne alles umkrempeln zu müssen. Mit Apps wie Square, Vend und Revel, die individuell angepasst werden können, lässt sich Hardware wie Kassenschublade, Kreditkartenleser oder Scanner ganz einfach verbinden. Square unterstützt sogar Apple Pay, die einfachste Möglichkeit für iPhone-Benutzer, an der Kasse zu bezahlen.

Buchhaltung

Die Buchhaltung kann viel Zeit in Anspruch nehmen, aber zumindest können Sie sie jetzt dank einiger toller Apps von FreshBooks und Xero auch unterwegs erledigen. Beide Lösungen bieten cloudbasierte Buchhaltungssysteme, auf die über mobile Apps zugegriffen werden kann. Mit diesen Systemen haben Sie Ihre Ausgaben und Einnahmen jederzeit im Blick.

Zeiterfassung

Aufgaben wie Dienstpläne, Zeiterfassung und Mitarbeiterkommunikation machen viel Arbeit und werden oft mit Stift und Papier erledigt. Mit Deputy und Replicon können Sie Ihre manuellen Systeme in die Cloud verlegen und Ihre Mobilgeräte als Schnittstelle nutzen. Beide Lösungen bieten Möglichkeiten zur Erstellung von Dienstplänen und zur Zeiterfassung sowie eine Plattform für die Mitarbeiterkommunikation.

Treueprogramm

Mit Treueprogrammen können Sie Ihre Kunden dauerhaft an sich binden. Die Implementierung eines eigenen Systems kann sich jedoch als äußerst schwierig erweisen. Hier kommt Belly ins Spiel. Belly ist ein Treuebonusprogramm, das von über 12.000 Unternehmen und sechs Millionen Kunden genutzt wird. Einfach anmelden und loslegen!

Beispiele aus der Praxis

Gesundheitsdienstleister suchen nach neuen Möglichkeiten, um ihren Patienten eine schnellere und persönlichere Versorgung bieten zu können und gleichzeitig die Kommunikation zwischen Ärzten und Pflegepersonal zu verbessern. Hierzu werden Krankenakten an einem sicheren zentralen Speicherort abgelegt, auf den Ärzte und Pfleger über ein Mobilgerät zugreifen können. In Kombination mit Drittanbieter-Apps und -Hardware für die Gesundheitsüberwachung zu Hause revolutionieren Apple und die nachfolgenden Unternehmen die Gesundheitspflege.

Kommunikation

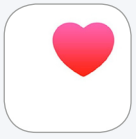
Kommunikation ist eine wesentliche Komponente für eine rechtzeitige Patientenversorgung. iOS bietet eine Plattform für attraktive Kommunikations-Apps mit umfassenden Funktionen. Voalte, Vocera und Praxify sind drei führende Unternehmen, die Gesundheitseinrichtungen leistungsstarke Kommunikationstools auf der Basis von Apple-Technologie an die Hand geben.

Klinische Versorgung

Ein modernes System für elektronische Patientenakten sollte für Ärzte und Pflegepersonal überall zugänglich sein – ob zu Hause, im Krankenhaus oder unterwegs. Die Lösungen von Emis und Epic wurden beide für iOS entwickelt. Mit den mobilen Apps sind Ärzte und Pflegepersonal jederzeit über den Gesundheitszustand ihrer Patienten informiert. Sie brauchen lediglich ein iPhone, iPad oder eine Apple Watch.

Patientenversorgung

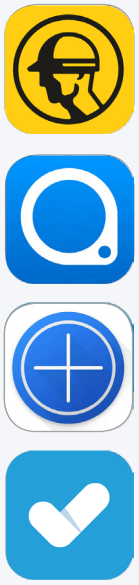
Die klinische Versorgung hat ihre Grenzen. Insbesondere bei chronischen Erkrankungen wird häufig eine häusliche Überwachung empfohlen. Dank iPad und iPhone, in Kombination mit Drittanbieter-Hardware, lässt sich der Gesundheitszustand von Patienten mittels Verbraucherprodukten überwachen. Focus Cura, Physitrack und Withings sind Pioniere in diesem Bereich und geben Benutzern die Möglichkeit, ihren Gesundheitszustand auf ihren persönlichen Mobilgeräten zu überwachen.



Apple und Gesundheit

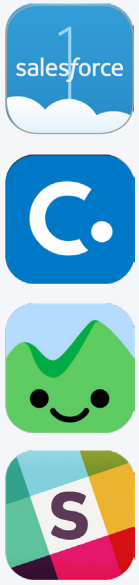
Apple gibt seinen Benutzern leistungsstarke Geräte in die Hand, mit denen sie ihren Gesundheitszustand überwachen und Gesundheitsdaten erfassen können – integriert in iPhone und Apple Watch. Mit der Health App können Benutzer ihre Gesundheitsdaten in einer einzigen App erfassen, ohne sich um die Sicherheit der Daten sorgen zu müssen.

Unternehmen mit Außendienstmitarbeitern müssen dafür sorgen, dass diese Zugriff auf die richtigen Mittel und Informationen haben – jederzeit und überall. Die richtige App- Strategie ist dabei für den Erfolg und die Produktivität von entscheidender Bedeutung. Unten finden Sie einige Beispiele für die Möglichkeiten von iOS in der Baubranche sowie für Außendienstmitarbeiter im Allgemeinen.



Baugewerbe

Im Baugewerbe gehört iOS mittlerweile zur festen Ausstattung – dank Produkten, mit denen sich Entwürfe und CAD-Pläne auf dem iPad einsehen lassen. Mit den Apps von Fieldwire, PlanGrid und FinalCAD können Bauteams auf Entwurfsdateien zugreifen – riesige Ausdrucke gehören damit der Vergangenheit an. Und mit SafetyCulture und der zugehörigen iAuditor-App wird sogar die Prüfung einfacher.



Außendienst

Kundenpflege, Projekt- und Teamverwaltung sowie Spesenabrechnung sind wesentliche Geschäftsaufgaben, mit denen die meisten Vertriebsorganisationen täglich zu tun haben. Mit Lösungen von Unternehmen wie Salesforce1, Concur, Basecamp und Slack können Sie dafür sorgen, dass Ihre Außendienstmitarbeiter unterwegs alles Nötige zur Hand haben einfach und bequem.

Geschäftsprozesse mit benutzerdefinierten Apps optimieren

Unternehmen, die iOS bereitstellen, können die grundlegende Kommunikation mit integrierten Apps wie Mail, Notes und Kalender sicherstellen. Doch iOS bietet noch viel mehr. Dank des Zugriffs auf eine leistungsstarke Plattform für benutzerdefinierte Apps können Sie Ihre Geschäftsprozesse und sogar die gesamte Branche revolutionieren.

Zum Beispiel arbeitet Apple mit IBM an der Entwicklung branchenspezifischer Apps, um die Produktivität und Effizienz zu steigern. Bis dato haben Apple und IBM über 100 Apps für branchenspezifische Aufgaben entwickelt: vom Finanzsektor und der Hightechbranche über Regierungseinrichtungen, das Gesundheitswesen und die Versicherungsbranche bis hin zum Einzelhandel und Verkehrswesen.

Bei über 1,5 Millionen Apps im App Store sind die Chancen groß, dass Sie eine App finden, die Ihre Anforderungen zu 90 % erfüllt. Hier kommt der B2B App Store ins Spiel. Dabei fungiert Apple als Schnittstelle zwischen Unternehmen und Entwicklern, um eine individuell angepasste Version einer App bereitzustellen. Ob einfaches Branding oder individuelle Anpassung vorhandener Apps – Unternehmen haben die freie Wahl.

Die innovativsten Unternehmen entwickeln nicht nur Hardware, sondern auch Software. Erst wenn Sie in Ressourcen zur Entwicklung firmeneigener Apps investieren, erkennen Sie, welche Möglichkeiten sich Ihnen auf einer mobilen Plattform eröffnen.
Mit Swift verfügt Apple über eine der besten Entwicklungsplattformen für mobile Inhalte auf dem Markt Swift ist eine leistungsstarke und intuitive Programmiersprache für alle Betriebssysteme von Apple. Und dank Open-Source-Lizenz erhalten Sie Zugriff auf kostenlose Ressourcen der Apple Community und können sofort loslegen!

Den Wandel im Unternehmen gestalten

Das Unternehmen mit Apple TV voranbringen

Die Anforderungen an die Nutzung mobiler Geräte am Arbeitsplatz nehmen ständig zu. Damit muss Ihre Technologie Schritt halten können. Mit der aktuellsten Version von tvOS ist die IT-Abteilung jetzt in der Lage, mithilfe des verwalteten Apple TV für die private Nutzung konzipierte Apple TV-Geräte als verwaltete Arbeitstools einzusetzen.

Drahtloser Konferenzraum

Richten Sie für einen modernen Konferenzraum einen Adapter und ein drahtloses Display ein. Aktivieren Sie dann den Modus "Konferenzraum-Display und erstellen Sie eine eigene Begrüßungsbotschaft mit zusätzlichen Anweisungen bzw. Informationen, die speziell für den betreffenden Raum gelten.

Digitale Werbung

Digitale Werbung mit Apple TV ist kostengünstig, besser zugänglich, leichter skalierbar und leichter zu handhaben. Mit MDM-Software können Unternehmen auf einfache Weise steuern, was an einem einzelnen Standort oder an mehreren Standorten angezeigt wird.

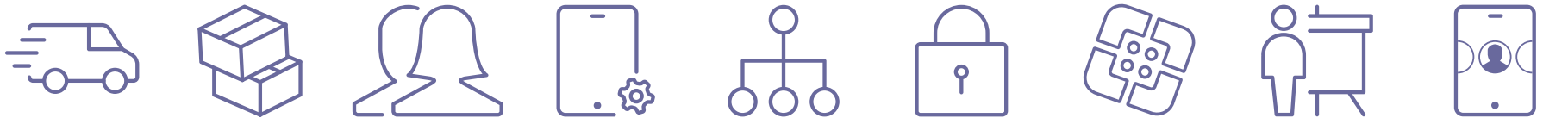
Spontane Zusammenarbeit

Mit verwaltetem Apple TV und Airplay ist es einfacher denn je, die Displays von Mobilgeräten auf einem gemeinsam genutzten Bildschirm anzuzeigen. Damit wird eine ideale Konfiguration für die Zusammenarbeit am Arbeitsplatz geschaffen.

jamf | PRO

MDM für iOS

Jamf Pro ist das branchenführende Lösung zur Verwaltung von Mobilgeräten für iOS. Damit haben Benutzer alle Mittel zur Hand, um die alltäglichen Supportaufgaben zu bewältigen. So können Sie sich auf die strategischen Aspekte konzentrieren und sparen ganz nebenbei auch noch Zeit und Geld.



Bereitstellung | Inventar | Konfigurations-Profile | MDM-Befehle | App Bereitstellung | Sicherheit & Datenschutz | Self Service | Apple School Manager | Classroom Management

iOS jetzt mit kostenloser Testversion verwalten

Profil-Payload und Liste der MDM-Befehle

Nur verwaltet

Payload Code

- Einfache Werte erlauben
- Alphanumerische Werte voraussetzen
- Mindestlänge für Codes (0-16)
- Mindestanzahl komplexer Zeichen (0-4)
- Maximale Codelaufzeit (0-730 Tage)
- Maximale Zeit für Automatische Sperre
- Codeverlauf (0-50 Codes)
- Maximale Zeitgrenze für Gerätesperrung
- Maximale Anzahl von Fehlversuchen

Payload für Einschränkungen

- Verwendung der Kamera erlauben
- Bildschirmfotos und -aufzeichnung erlauben
- Sprachwahl erlauben, während Gerät gesperrt ist
- Siri erlauben
- Siri erlauben, während das Gerät gesperrt ist
- Installieren von Apps über Apple Configurator und iTunes erlauben
- In-App-Käufe erlauben
- iTunes-Store-Kennwort für alle Einkäufe erforderlich
- iCloud-Backup erlauben
- iCloud-Schlüsselbund erlauben
- Verwalteten Apps das Sichern von Daten in iCloud erlauben
- Backup von Büchern des Unternehmens erlauben
- Synchronisieren von Notizen und Hervorhebungen in Büchern des Unternehmens erlauben
- iCloud Fotofreigabe erlauben
- iCloud Fotomediathek erlauben
- Mein Fotostream erlauben
- Automatische Synchronisierung beim Roaming erlauben
- Verschlüsselte Backups erzwingen
- Beschränktes Ad-Tracking erzwingen
- Benutzer dürfen nicht vertrauenswürdige TLS-Zertifikate annehmen
- Automatische Updates für die Einstellungen vertrauenswürdiger Zertifikate
- Vertrauen neuer Autoren von Unternehmens-Apps erlauben
- Dokumente aus verwalteten Quellen in unverwalteten Zielen erlauben
- Dokumente aus nicht verwalteten Quellen in verwalteten Zielen erlauben
- AirDrop als unverwaltetes Ziel behandeln
- Handoff erlauben
- Senden von Diagnose- und Nutzungsdaten an Apple erlauben
- Touch ID zum Entsperren des Geräts erlauben
- Apple Watch Handgelenkerkennung durchsetzen
- Code-Eingabe bei erster AirPlay-Verbindung anfordern
- Wallet-Mitteilungen im Sperrbildschirm erlauben
- Kontrollzentrum im Sperrbildschirm anzeigen
- Mitteilungszentrale im Sperrbildschirm anzeigen
- „Ansicht heute“ im Sperrbildschirm anzeigen
- Bereich für Altersfreigabe festlegen
- Bewertungen für zulässige Inhalte von Filmen, Fernsehsendungen und Apps einstellen
- Anstößige sexuelle Inhalte im iBooks Store erlauben

Andere Payloads

- WLAN-Payload
- VPN-Payload
- Mail-Payload
- Exchange-ActiveSync-Payload
- Google Account Payload
- LDAP-Payload
- Kalender-Payload
- Kontakte-Payload
- Payload Abonnierte Kalender
- Webclips-Payload
- Payload für macOS Server-Accounts
- Domänen-Payload
- Zertifikate-Payload
- SCEP-Payload
- APN-Payload
- Mobilfunk-Payload
- Payload für Single-Sign-On
- Schriftarten-Payload
- AirPrint-Payload
- Payload für Netzwerknutzungsregeln

MDM-Befehle

- Fernsperren
- Fernlöschen
- Code löschen
- Verwaltung des Geräts aufheben
- Bestand aktualisieren
- Leere Push-Benachrichtigung senden

Verwaltet + Betreut

Registrierung (nur DEP)

- Gerät betreuen
- MDM-Profil obligatorisch machen
- Koppeln mit Mac Computern sperren
- Benutzern verbieten, das MDM-Profil zu entfernen
- Geteiltes iPad ermöglichen
- Anmeldedaten für Registrierung verlangen
- Systemassistentenoptionen auslassen
- Benennungsmethode für Geräte definieren

Payload für Einschränkungen (nur betreute Geräte)

- FaceTime erlauben
- Bildschirmbeobachtung per Classroom App erlauben
- Ändern der Berechtigung für AirPlay und Displayanzeige für verwaltete Klassen erlauben
- AirDrop erlauben
- iMessage erlauben
- Siri-Obszönitätenfilter aktivieren
- Benutzergenerierten Inhalt in Siri erlauben
- iBooks Store erlauben
- Installation von Apps aus dem App Store erlauben
- Automatische App-Downloads erlauben
- Entfernen von Apps erlauben
- Apple Music erlauben
- Radio erlauben
- iCloud Dokumente und Daten erlauben
- Alle Inhalte und Einstellungen löschen erlauben
- Installation von Konfigurationsprofilen erlauben
- Ändern von Account-Einstellungen erlauben
- Ändern von Bluetooth-Einstellungen erlauben
- Änderung der App-Einstellungen für mobile Daten erlauben
- Ändern des Gerätenamens erlauben
- Ändern der Einstellungen für „Freunde suchen“ erlauben
- Ändern von Benachrichtigungseinstellungen erlauben
- Ändern des Codes erlauben
- Ändern der Touch ID Fingerabdrücke erlauben
- Ändern von Einschränkungen erlauben
- Ändern des Hintergrundbilds erlauben
- Verbindung mit Hosts ohne Configurator Installation erlauben
- Ändern von Diagnoseeinstellungen erlauben
- Koppeln mit Apple Watch erlauben
- Verbindung zu nicht verwalteten WLAN-Netzen erlauben
- Textvorschläge erlauben
- Tastaturkurzbefehle erlauben
- Automatische Korrektur erlauben
- Rechtschreibprüfung erlauben
- Definieren erlauben
- Diktierfunktion erlauben
- Nutzung von iTunes Store erlauben
- Nutzung von Nachrichten erlauben
- Nutzung von Podcasts erlauben
- Verwendung von Game Center erlauben
- Verwendung von Safari erlauben
- Automatisches Ausfüllen aktivieren
- Betrugswarnung erzwingen
- JavaScript aktivieren
- Pop-Ups unterdrücken
- Cookies blockieren
- Wiedergabe anstößiger Musik, Podcasts und iTunes U-Medien erlauben
- Autonomer Einzel-App-Modus
- Apps anzeigen/ausblenden
- AirPlay-Ziele beschränken

Sonstige Payloads (nur betreute Geräte)

- Payload für Layout des Home-Bildschirms
- Einzel-App-Modus
- Payload für Globalen HTTP-Proxy
- Payload für Inhaltsfilter
- Payload für Sperrbildschirm-Nachricht
- Payload für Mitteilungen

MDM-Befehle (nur betreute Geräte)

- SHintergrundbild einstellen
- Aktivierungssperre umgehen
- Verloren-Modus mit Ton
- iOS aktualisieren (nur mit DEP-Registrierung)
- Einschränkungen löschen
- Gerät umbenennen
- Gerät neu starten
- Gerät ausschalten
- Benutzer löschen (nur geteiltes iPad)
- Benutzer abmelden (nur geteiltes iPad)