Verwaltung von Geräten und Unternehmensdaten unter iOS

Inhalt

Überblick

Unternehmen in aller Welt stellen ihren Mitarbeitern iPhone und iPad zur Verfügung.

Der Schlüssel für eine erfolgreiche mobile Strategie ist ein ausgewogenes Verhältnis zwischen Kontrolle durch die IT und Selbstbestimmung der Benutzer. Indem Benutzer ihre iOS Geräte mit eigenen Apps und Inhalten personalisieren, übernehmen sie mehr Eigenverantwortung, was wiederum zu mehr Engagement und einer höheren Produktivität führt. Ermöglicht wird dies durch die Verwaltungsarchitektur von Apple: Sie bietet intelligente Möglichkeiten, um unternehmenseigene Daten und Apps diskret zu verwalten und berufliche und private Daten nahtlos voneinander zu trennen. Zudem haben die Benutzer auf diese Weise Kenntnis davon, wie ihre Geräte verwaltet werden. Sie können darauf vertrauen, dass ihre Privatsphäre geschützt ist.

Dieses Dokument geht darauf ein, wie eine grundlegende IT-Kontrolle erzielt werden kann und Benutzer dennoch eigenständig die besten Werkzeuge für ihre Arbeit auswählen und nutzen können. Es versteht sich als Ergänzung für „iOS Implementierung: Referenz", ein umfassendes, online verfügbares technisches Referenzdokument zur Bereitstellung und Verwaltung von iOS Geräten in Unternehmen.

Sie finden „iOS-Implementierung: Referenz" unter help.apple.com/deployment/ios.

Grundlagen der Verwaltung

Mit iOS lässt sich die Implementierung von iPhone und iPad durch eine Reihe integrierter Verwaltungstechniken optimieren, die es Ihnen ermöglichen, die Account-Einrichtung zu vereinfachen und per Fernzugriff Richtlinien zu konfigurieren, Apps zu verteilen und Geräteeinschränkungen anzuwenden.

Unser Verwaltungskonzept

Die Verwaltungsarchitektur von Apple ist die Basis für die Verwaltung mobiler Geräte. Die Architektur ist in iOS integriert. Unternehmen sind dadurch in der Lage, die nötigen Aspekte mit möglichst geringen Eingriffen zu verwalten – ohne dass Features gesperrt oder Funktionen deaktiviert werden müssen. Die Verwaltungsarchitektur von Apple ermöglicht eine fein abgestufte Kontrolle über Ihre Geräte, Apps und Daten mithilfe von MDM-Lösungen (Mobile Device Management) anderer Anbieter. Vor allem aber haben Sie die nötige Kontrolle, ohne dass die Benutzerfreundlichkeit oder die Privatsphäre Ihrer Mitarbeiter beeinträchtigt wird.

Andere erhältliche Geräteverwaltungslösungen verwenden möglicherweise unterschiedliche Bezeichnungen für die MDM-Funktionalität, wie etwa Enterprise Mobility Management (EMM) oder Mobile Application Management (MAM). Diese Lösungen verfolgen jedoch dasselbe Ziel: Die drahtlose Fernverwaltung der Geräte und Daten Ihres Unternehmens. Da die Verwaltungsarchitektur von Apple in iOS integriert ist, benötigen Sie keine separaten Hilfsanwendungen Ihres MDM-Lösungsanbieters.

Trennung von beruflichen und privaten Daten

Unabhängig davon, ob in Ihrer Organisation benutzereigene oder unternehmenseigene Geräte genutzt werden, können Sie Ihre Ziele für IT-Management erreichen und gleichzeitig die volle Produktivität der Benutzer bei ihrer Arbeit gewährleisten. Geschäftliche und private Daten werden separat verwaltet, ohne dass die Benutzerfreundlichkeit darunter leidet. Somit können Ihre Benutzer beispielsweise die aktuellsten Produktivitätsapps neben den unternehmenseigenen Apps auf ihren Geräten installieren und nutzen, was ihnen mehr Freiheit bei der Wahl ihrer Arbeitsweise gibt. iOS ermöglicht dies, ohne dass Lösungen anderer Anbieter wie etwa Container benötigt werden, die die Benutzerfreundlichkeit beeinträchtigen und dadurch für Frustrationen bei den Benutzern sorgen würden.

Überblick über unterschiedliche Verwaltungsmodelle

Auf anderen Plattformen wurden häufig Container entwickelt, um Probleme zu lösen. Solche Probleme treten bei iOS gar nicht erst auf. Manche Container setzen auf zwei getrennte Benutzer-Accounts. Dabei werden auf ein und demselben Gerät zwei separate Umgebungen erstellt. Andere Lösungen konzentrieren sich darauf, die Apps selbst durch eine Code-basierte Integration oder durch die Verkapselung der Apps in Containern auszuführen. All diese Methoden führen zu Produktivitätseinschränkungen für die Benutzer – sei es durch die erforderliche An- und Abmeldung bei unterschiedlichen Arbeitsbereichen oder durch zusätzliche Abhängigkeiten von proprietärem Programmcode, die häufig dazu führen, dass Apps mit Aktualisierungen des Betriebssystems nicht mehr kompatibel sind.

Unternehmen, die keine Container mehr verwenden, stellen fest, dass die nativen Kontrollmechanismen für die Verwaltung, die bei iOS zum Einsatz kommen, für optimale Benutzerfreundlichkeit sorgen und die Produktivität der Benutzer steigern. Anstatt den Benutzern die berufliche und private Nutzung ihrer Geräte zu erschweren, können Sie richtlinienbasierte Kontrollmechanismen einsetzen, die den Datenfluss im Hintergrund nahtlos steuern.

Unternehmensdaten verwalten

Mit iOS brauchen Sie Ihre Geräte nicht zu sperren. Schlüsseltechnologien steuern den Unternehmensdatenfluss zwischen Apps und verhindern, dass solche Daten in private Apps oder Cloud-Dienste des Benutzers gelangen.

Verwaltete Inhalte

Bei verwalteten Inhalten werden Installation, Konfiguration, Verwaltung und Entfernung von Apps, Accounts, Büchern und Domains kontrolliert, die aus dem App Store stammen oder selbst intern entwickelt wurden.

- **Verwaltete Apps.** Mit MDM installierte Apps werden als „verwaltete Apps“ bezeichnet. Dabei kann es sich um kostenlose oder kostenpflichtige Apps aus dem App Store oder um eigene, interne Apps handeln. All diese Apps können drahtlos per MDM installiert werden. Verwaltete Apps enthalten häufig vertrauliche Unternehmensinformationen. Sie gestatteten eine strengere

Kontrolle als Apps, die durch Benutzer geladen wurden. Der MDM-Server kann verwaltete Apps und die zugehörigen Daten bei Bedarf entfernen oder angeben, ob die Apps gelöscht werden sollen, wenn das MDM-Profil entfernt wird. Darüber hinaus kann der MDM-Server das Sichern von Daten verwalteter Apps in iTunes und iCloud unterbinden.

- **Verwaltete Accounts.** MDM kann Ihren Benutzern helfen, einen schnellen Einstieg zu finden, indem ihre E-Mail Accounts und weiteren 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. Mit MDM können die folgenden Arten von Accounts konfiguriert werden: IMAP/POP, CalDAV, abonnierte Kalender, CardDAV, Exchange ActiveSync und LDAP.
- **Verwaltete Bücher.** Per MDM 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 mit anderen verwalteten Apps geteilt oder über verwaltete Accounts per E-Mail versendet werden. Materialien, die nicht mehr benötigt werden, können per Fernzugriff gelöscht werden.
- **Verwaltete Domains.** Downloads von Safari gelten als verwaltete Dokumente, wenn sie von verwalteten Domains stammen. Bestimmte URLs und Subdomains können verwaltet werden. Wenn ein Benutzer beispielsweise eine PDF Datei aus einer verwalteten Domain lädt, erfordert die Domain, dass die PDF Datei allen Einstellungen für verwaltete Dokumente entspricht. Pfade, die der Domain folgen, werden standardmäßig verwaltet.

Verwaltete Verteilung

Mit der verwalteten Verteilung können Sie Ihre MDM-Lösung oder Apple Configurator 2 nutzen, um die über das Programm für Volumenlizenzen (VPP) gekauften Apps und Bücher zu verwalten. Zur Aktivierung der verwalteten Verteilung müssen Sie zuerst Ihre MDM-Lösung unter Verwendung eines sicheren Tokens mit Ihrem VPP Account verknüpfen. Sobald Ihr MDM-Server mit VPP verbunden ist, können Sie Apps direkt einem Gerät zuweisen, ohne dass der Benutzer eine Apple ID benötigt. Die Benutzer werden benachrichtigt, wenn Apps zur Installation auf ihren Geräten bereitstehen. Im Fall von betreuten Geräten werden die Apps im Hintergrund gepusht, ohne dass der Benutzer eine Aufforderung erhält.

Um anhand einer MDM-Lösung die volle Kontrolle über Apps zu behalten, sollten Sie Apps direkt einem Gerät zuweisen.

Verwaltete App-Konfiguration

Bei der verwalteten App-Konfiguration nutzt MDM die native iOS Verwaltungsarchitektur, um Apps während oder nach der Implementierung zu konfigurieren. Diese Architektur gestattet es Entwicklern, Konfigurationseinstellungen festzulegen, die angewandt werden sollen, wenn ihre App als verwaltete App installiert wird. Die Mitarbeiter können auf diese Weise konfigurierte Apps sofort nutzen, ohne dass dazu eine benutzerspezifische Einrichtung erforderlich ist. Die IT-Abteilung kann auf diese Weise sicherstellen, dass Unternehmensdaten innerhalb von Apps auf sichere Weise verarbeitet werden, ohne dass dazu proprietäre SDKs oder die Verkapselung der Apps erforderlich sind.

App-Entwicklern stehen Funktionen zur Verfügung, die bei der verwalteten App-Konfiguration aktiviert werden können, z. B. App-Konfiguration, App-Backups verhindern, Bildschirmfotos deaktivieren und Fernlöschen der App.

Die AppConfig Community konzentriert sich auf die Bereitstellung von Tools und Best Practices im Zusammenhang mit den nativen Funktionen mobiler Betriebssysteme. Führende Anbieter von MDM-Lösungen aus dieser Community haben ein Standardschema erstellt, das alle App-Entwickler nutzen können, um die verwaltete App-Konfiguration zu unterstützen. Durch die Bereitstellung einer einheitlicheren, offeneren und einfacheren Methode für die Konfiguration und Sicherung mobiler Apps fördert die Community die Akzeptanz mobiler Technologien in Unternehmen.

Weitere Informationen über die AppConfig Community finden Sie unter www.appconfig.org.

Verwalteter Datenfluss

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

- **In verwalteter Umgebung öffnen.** Für das verwaltete Öffnen werden Einschränkungen angewendet, 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 berufliche Dokument kann 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 für das Öffnen des Anhangs verfügbar sind. Neben verwalteten Apps, Accounts, Büchern und Domains berücksichtigt auch eine Reihe von Erweiterungen die Einschränkungen im Rahmen des verwalteten Öffnens.

Zum Schutz der Unternehmensdaten kann dieses berufliche Dokument nur mit Apps geöffnet werden, die von der MDM-Lösung installiert wurden und verwaltet werden.

- **Verwaltete Erweiterungen.** Mithilfe von App-Erweiterungen können Entwickler Funktionen für andere Apps oder zentrale, in iOS integrierte Systeme wie beispielsweise die Mitteilungszentrale bereitzustellen. Dies ermöglicht neuartige Workflows zwischen verschiedenen Apps. Durch Nutzung der Funktion „In verwalteter Umgebung öffnen" wird verhindert, dass Funktionen nicht verwalteter Erweiterungen mit verwalteten Apps kommunizieren können. Die folgenden Beispiele zeigen verschiedene Arten von Erweiterungen:
  - **Document-Provider-Erweiterungen** gestatten es Produktivitätsapps, Dokumente aus verschiedenen Cloud-Diensten zu öffnen, ohne dass dafür unnötige Kopien erstellt werden müssen.
  - **Aktionserweiterungen** gestatten es Benutzern, Inhalte im Kontext einer anderen App zu bearbeiten oder anzuzeigen. Die Benutzer können mithilfe einer Aktion z. B. fremdsprachige Texte direkt in Safari übersetzen.
  - **Benutzerdefinierte Tastaturerweiterungen** stellen andere Tastaturen bereit als diejenigen, die bereits in iOS integriert sind. Mit „In verwalteter Umgebung öffnen" kann verhindert werden, dass nicht autorisierte Tastaturen in Ihren unternehmenseigenen Apps angezeigt werden.
  - **Heute-Erweiterungen,** die auch als Widgets bekannt sind, liefern Kurzinformationen in der Ansicht „Heute" der Mitteilungszentrale. Dies bietet den Benutzern eine hervorragende Möglichkeit, umgehend aktuelle Informationen aus einer App zu erhalten. Dafür werden vereinfachte Interaktionen in der vollständigen App gestartet, um weitere Informationen anzufordern.
  - **Erweiterungen zum Teilen** bieten Benutzern eine komfortable Möglichkeit, um Inhalte mit sozialen Netzwerken, Upload-Diensten usw. teilen. Dabei wählen sie über die Taste zum Teilen in einer App eine Erweiterung aus, die z. B. auf die Website eines sozialen Netzwerks verweist, wo sie dann Kommentare oder andere Inhalte posten können.

Flexible Verwaltungsoptionen

Die Verwaltungsarchitektur von Apple ist flexibel und bietet ein ausgewogenes Konzept für die Verwaltung benutzereigener sowie unternehmenseigener Geräte in Ihrer Organisation. Wenn Sie eine MDM-Lösung eines anderen Anbieters in Verbindung mit iOS nutzen, stehen Ihnen je nach Bedarf abgestufte Verwaltungsoptionen zur Verfügung, angefangen bei sehr offenen Methoden bis hin zur fein abgestuften Verwaltung.

Eigentumsmodelle

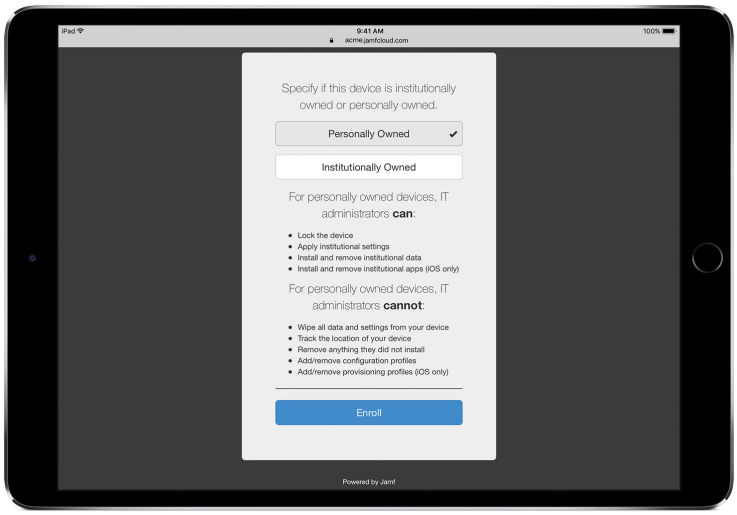
Je nach den in Ihrer Organisation eingesetzten Eigentumsmodellen erfolgt die Verwaltung von Geräten und Apps auf unterschiedliche Art und Weise. Die zwei häufigsten Eigentumsmodelle in Unternehmen sind benutzereigene und unternehmenseigene iOS Geräte.

Benutzereigene Geräte

Bei der Implementierung benutzereigener Geräte ermöglicht iOS eine personalisierte Konfiguration durch die Benutzer, bietet Transparenz im Hinblick auf die Konfiguration der Geräte und gewährleistet, dass Ihre Organisation nicht auf die privaten Daten der Benutzer zugreifen kann.

- **Wahlweise An-/Abmeldung zur Registrierung.** Wenn Geräte von den Benutzern gekauft und eingerichtet werden, was üblicherweise als BYOD-Implementierung bezeichnet wird, können Sie ihnen dennoch Zugriff auf Unternehmensdienste wie WLAN, Mail und Kalender bieten. Die

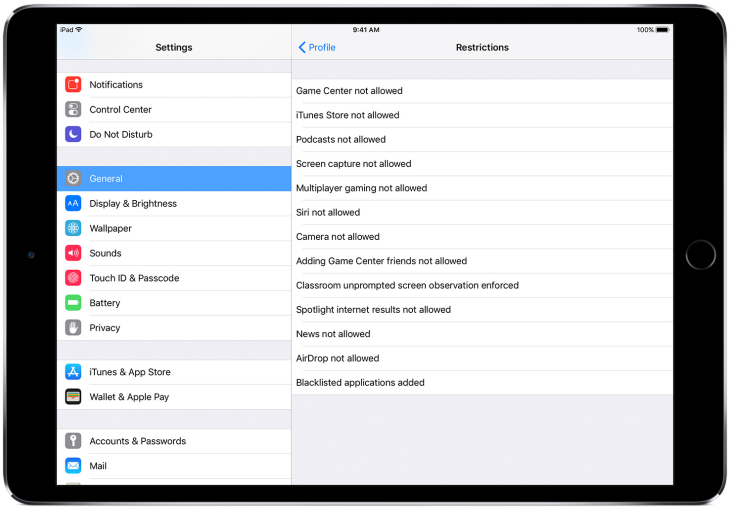
Benutzer müssen sich für die Registrierung bei der MDM-Lösung Ihrer Organisation einfach anmelden. Wenn sich Benutzer auf einem iOS Gerät zum ersten Mal bei MDM registrieren, werden sie darüber informiert, auf welche Inhalte auf ihrem Gerät der MDM-Server zugreifen kann und welche Features er konfigurieren wird. Dies bietet den Benutzern Transparenz im Hinblick auf die Frage, welche Aspekte verwaltet werden, und stärkt das Vertrauen, das die Benutzer Ihnen entgegenbringen. Es ist wichtig, dass Sie den Benutzern mitteilen, dass sie die Registrierung jederzeit rückgängig machen können, indem sie das Verwaltungsprofil vom Gerät entfernen, wenn sie diese Art der Verwaltung nicht wünschen. Dadurch werden alle per MDM installierten Unternehmens-Accounts und -Apps entfernt.



MDM-Lösungen anderer Anbieter bieten in der Regel eine intuitive Benutzeroberfläche die Mitarbeiter, sodass sie der Registrierung bereitwillig zustimmen.*

*Bildschirmabbildung mit freundlicher Genehmigung von Jamf.

- **Größere Transparenz.** Nachdem Benutzer bei MDM angemeldet sind, sehen sie in den Einstellungen auf einen Blick, welche Apps, Bücher und Accounts verwaltet werden und welche Einschränkungen implementiert wurden. Alle mit MDM installierten Einstellungen, Accounts und Inhalte des Unternehmens werden von iOS als „verwaltet" gekennzeichnet.



Die Benutzeroberfläche für Konfigurationsprofile in den Einstellungen zeigt Benutzern genau, was auf ihrem Gerät konfiguriert wurde.

- **Datenschutz für Benutzer.** Sie können zwar über einen MDM-Server mit iOS Geräten kommunizieren. aber dabei werden nicht alle Einstellungen und Accountdaten offengelegt. Sie können unternehmenseigene Accounts, Einstellungen und Daten verwalten, welche per MDM bereitgestellt werden, doch auf die persönlichen Accounts der Benutzer kann nicht zugegriffen werden. Tatsächlich verhindern dieselben Features, die für die Sicherheit von Daten in vom Unternehmen verwalteten Apps sorgen, auch das Einfließen persönlicher Inhalte von Benutzern in den Datenstrom des Unternehmens.

  Die folgenden Beispiele zeigen, welche Daten ein MDM-Server eines anderen Anbieters von einem persönlichen iOS Gerät abrufen kann und welche nicht:

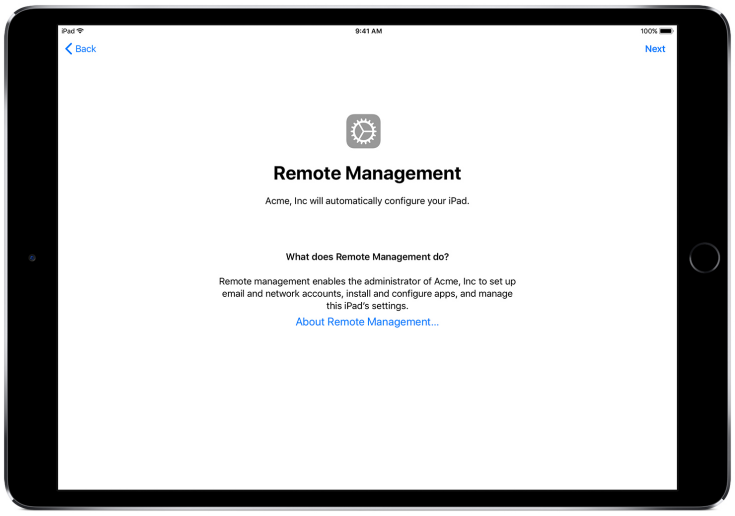
Für MDM sichtbar:	**Private Daten, die für MDM nicht sichtbar sind:**
Gerätename	Private und geschäftliche E-Mails, Kalender, Kontakte
Telefonnummer	SMS oder iMessages
Seriennummer	Safari Browserverlauf
Modellname und -nummer	Protokolle von FaceTime oder Telefongesprächen
Kapazität und freier Speicherplatz	Persönliche Erinnerungen und Notizen
iOS Versionsnummer	Häufigkeit der Nutzung von Apps
Installierte Apps	Standort des Geräts

- **Geräte personalisieren.** In Unternehmen wurden folgende Erfahrungen gemacht: Wenn Benutzern gestattet wird, ihre Geräte mit ihren eigenen Apple IDs zu personalisieren, übernehmen sie mehr Eigenverantwortung. Zudem steigert es die Produktivität, da die Benutzer wählen können, welche Apps und Inhalte sie benötigen, um ihre Arbeit optimal zu erledigen.

Geräte im Besitz der Organisation

Bei der Implementierung von Geräten im Besitz des Unternehmens können Sie jedem Benutzer ein Gerät zur Verfügung stellen, was als Implementierung von persönlich anpassbaren Geräten bezeichnet wird. Alternativ gibt es die Option, dass die Geräte abwechselnd von mehreren Benutzern verwendet werden, was als Implementierung von nicht personalisierten Geräten bezeichnet wird. iOS Features wie die automatische Registrierung, gesperrte MDM-Einstellungen, Gerätebetreuung sowie die Funktion „VPN immer eingeschaltet" gewährleisten, dass die Geräte gemäß den spezifischen Anforderungen Ihrer Organisation konfiguriert werden. Dies bietet mehr Kontrolle und stellt gleichzeitig sicher, dass Unternehmensdaten geschützt sind.

- **Automatische Registrierung.** Das Programm zur Geräteregistrierung ermöglicht es Ihnen, die MDM-Registrierung bei der Ersteinrichtung von iPhone und iPad Geräten sowie von Mac Computern im Besitz Ihrer Organisation zu automatisieren. Sie können die Registrierung verpflichtend und nicht entfernbar machen. Sie können Geräte bei der Registrierung auch in den betreuten Modus versetzen und Benutzern gestatten, einige der grundlegenden Einrichtungsschritte auszulassen.



Mit dem Programm zur Geräteregistrierung (DEP) konfiguriert Ihre MDM-Lösung die iOS Geräte während der Ausführung des Systemassistenten automatisch.

- **Betreute Geräte.** Die Betreuung bietet zusätzliche Verwaltungsfunktionen für iOS Geräte, die im Besitz Ihrer Organisation sind. Dazu zählen etwa die Möglichkeit, einen Web-Filter über einen globalen Proxy zu aktivieren, um sicherzustellen, dass der Internetdatenverkehr der Benutzer immer den Richtlinien der Organisation entspricht. Außerdem können Sie im Rahmen der Betreuung verhindern, dass Benutzer ihr Gerät auf die Werkseinstellungen zurücksetzen, und haben viele weitere Möglichkeiten. Standardmäßig sind alle iOS Geräte unbetreut. Die Aktivierung des betreuten Modus kann automatisch per 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 in Erwägung ziehen, die Betreuung zu aktivieren, um solche Features in Zukunft nutzen zu können. Andernfalls müssten 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 mehr Optionen.

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

Einschränkungen

iOS unterstützt die folgenden Einschränkungskategorien, die drahtlos konfiguriert werden können, um die Anforderungen Ihrer Organisation ohne Beeinträchtigung der Benutzer zu erfüllen:

- AirPrint
- App-Installation
- App-Nutzung
- Classroom App
- Gerät
- iCloud
- Profil-Manager-Einschränkungen für Benutzer und Benutzergruppen
- Safari
- Datenschutz- und Sicherheitseinstellungen
- Siri

Auch die folgenden Kategorien haben Optionen, die mit Ihrer MDM-Lösung konfiguriert werden können:

- Automatische MDM-Registrierungseinstellungen
- Bildschirme des Systemassistenten

Zusätzliche Verwaltungsfunktionen

Geräte abfragen

Zusätzlich zur Konfiguration von Geräten kann ein MDM-Server auch verschiedene Informationen von den Geräten abfragen, z. B. Angaben zum Gerät sowie Daten zum Netzwerk, zu Apps, zur Einhaltung von Richtlinien sowie zur Sicherheit. Mithilfe dieser Informationen können Sie sicherstellen, dass die Geräte die erforderlichen Richtlinien kontinuierlich einhalten. Der MDM-Server legt das Intervall fest, in dem Informationen abgefragt werden.

Hier einige Beispiele für Informationen, die von iOS Geräten abgefragt werden können:

- Detailangaben zum Gerät (Name)
- Modell, iOS Version, Seriennummer
- Netzwerkinformationen
- Roaming-Status, MAC-Adressen
- Installierte Apps
- Name, Version, Größe von Apps
- Daten zu Konformität und Sicherheit
- Installierte Einstellungen, Richtlinien, Zertifikate
- Verschlüsselungsstatus

Verwaltungsaufgaben

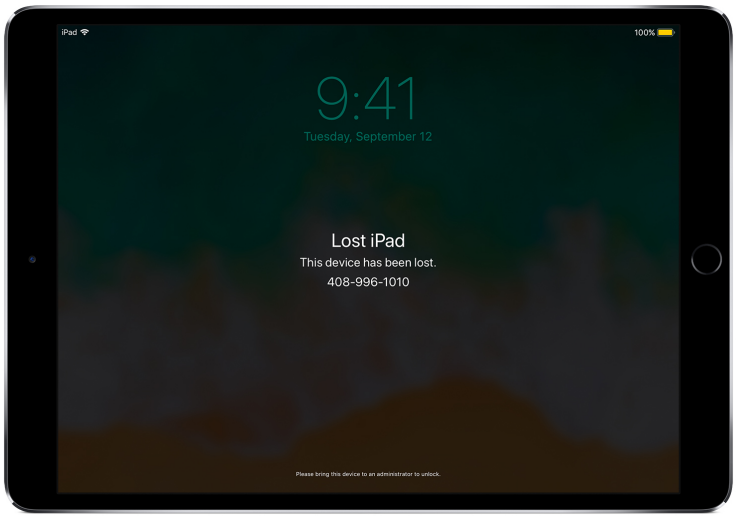
Wenn ein Gerät verwaltet wird, kann eine Vielzahl von Verwaltungsaufgaben über einen MDM-Server ausgeführt werden, z. B. das automatische Ändern von Konfigurationseinstellungen ohne Benutzereingriff, die Durchführung eines iOS Updates auf mit einem Code gesperrten Geräten, das Sperren oder Löschen eines 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 dem AirPlay Mirroring an ein bestimmtes Ziel zu beginnen oder eine laufende AirPlay Sitzung zu beenden.

Modus „Verloren"

Ihre MDM-Lösung kann betreute Geräte mit iOS 9.3 oder neuer per Fernzugriff in den Modus „Verloren" versetzen. Dadurch wird das Gerät gesperrt und es besteht die Möglichkeit, eine Nachricht mit einer Telefonnummer auf seinem Sperrbildschirm 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.

Wenn die MDM-Lösung den Modus „Verloren" per Fernzugriff deaktiviert, wird das Gerät entsperrt und geortet. Zur Aufrechterhaltung der Transparenz wird der Benutzer darüber informiert, dass der Modus „Verloren" ausgeschaltet wurde.



Wenn die MDM-Lösung ein verlorenes Gerät in den Modus „Verloren" versetzt, erfolgt dadurch eine Sperrung des Geräts. Außerdem ist es möglich, Nachrichten auf dem Bildschirm anzuzeigen und den Standort des Geräts zu ermitteln.

Aktivierungssperre

Bei Geräten mit 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 aus Ihrer Organisation ausscheidet, ohne vorher mithilfe seiner Apple ID die Aktivierungssperre zu entfernen.

Ihre MDM-Lösung kann einen Umgehungscode abrufen und dem Benutzer ermöglichen, die Aktivierungssperre auf dem Gerät unter den folgenden Bedingungen zu aktivieren:

- Wenn „Mein iPhone suchen" eingeschaltet ist, wenn die MDM-Lösung die Aktivierungssperre zulässt, wird die Aktivierungssperre zu diesem Zeitpunkt aktiviert.
- Wenn „Mein iPhone suchen" ausgeschaltet ist, wenn die MDM-Lösung die Aktivierungssperre zulässt, wird die Aktivierungssperre aktiviert, sobald der Benutzer „Mein iPhone suchen" aktiviert.

Zusammenfassung

Die iOS Verwaltungsarchitektur vereint das Beste aus beiden Welten: Die IT-Abteilung ist in der Lage, Geräte zu konfigurieren, zu verwalten und zu sichern und die mit diesen Geräten verarbeiteten Unternehmensdaten zu kontrollieren. Gleichzeitig werden die Benutzer in die Lage versetzt, hervorragende Arbeit mit den Geräten zu leisten, die sie begeistern.