iOS und iPadOS Implementierung: Überblick

Einführung

Inhalt

Mit dem iPhone und iPad können Sie Ihre Geschäftsabläufe und die Arbeitsweise Ihrer Mitarbeiter transformieren. Sie können zu signifikanten Produktivitätssteigerungen führen und Mitarbeitern die Freiheit und Flexibilität geben, neue Arbeitsweisen zu nutzen – sei es im Büro oder auf Reisen. Werden diese modernen Arbeitsweisen gezielt angewandt, profitiert davon die gesamte Organisation. 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 und iPadOS unterstützen, haben in der Wahrnehmung der Benutzer Einfluss auf die Unternehmensstrategie und bringen die IT voran – statt nur defekte Technik zu reparieren und ständig die Kosten drücken zu wollen. Letztlich profitieren alle von einer motivierteren Belegschaft und neuen Geschäftsmöglichkeiten in allen Bereichen.

Noch nie war es so einfach, iPhone und iPad in Ihrem gesamtem Unternehmen einzurichten und zu implementieren. Mit Apple Business Manager und einer Lösung für die mobile Geräteverwaltung (Mobile Device Management, MDM) eines anderen Anbieters kann Ihr Unternehmen iOS und iPadOS Geräte und Apps nach Bedarf implementieren.

- Mit der mobilen Geräteverwaltung können Sie Geräte konfigurieren und verwalten und drahtlos Apps verteilen und verwalten.
- Apple Business Manager registriert Ihre Apple Geräte automatisch bei Ihrer MDM-Lösung, um die Implementierung zu optimieren, ohne dass ein Eingreifen seitens der IT erforderlich ist.
- Mit Apple Business Manager können Sie Apps und Bücher in großen Stückzahlen kaufen und drahtlos an Benutzer verteilen.
- Apple Business Manager erlaubt es Ihnen außerdem, für Mitarbeiter verwaltete Apple IDs für die verknüpfte Authentifizierung mit Microsoft Azure AD zu erstellen.

Dieses Dokument unterstützt Sie bei der Implementierung von iOS und iPadOS Geräten in Ihrer Organisation und hilft Ihnen bei der Erstellung eines Implementierungsplans, der am besten zu Ihrer Umgebung passt. Ausführlichere Infos zu diesen Themen finden Sie online in der Implementierungsreferenz für iPhone und iPad: support.apple.com/guide/deployment-reference-ios

Eigentumsmodelle

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

Die zwei häufigsten Eigentumsmodelle für iOS und iPadOS Geräte in Unternehmen sind:

- Eigentum der Organisation
- Eigentum des Benutzers

Obwohl die meisten Organisationen ein bestimmtes Modell bevorzugen, kommen in Ihrer Umgebung möglicherweise mehrere Modelle zum Einsatz. Eine Unternehmenszentrale könnte z. B. eine Strategie nutzen, bei der sich die Geräte im Besitz der Benutzer befinden. Hierbei könnten Mitarbeiter ein privates iPad einrichten, während die Unternehmensressourcen ohne Auswirkungen auf persönliche Daten und Apps der Mitarbeiter geschützt und verwaltet würden. Dagegen könnten die Einzelhandelsfilialen des Unternehmens eine Strategie mit Geräten im Besitz des Unternehmens nutzen, bei der sich mehrere Mitarbeiter iOS und iPadOS Geräte teilen, um Kundentransaktionen durchzuführen.

Durch die Analyse dieser Modelle können Sie die Strategie ermitteln, die für Ihre spezifische Umgebung am besten geeignet ist. Nachdem Sie das passende Modell für Ihre Organisation identifiziert haben, kann Ihr Team die Implementierungs- und Verwaltungsfunktionen von Apple im Detail erkunden.

Geräte im Besitz der Organisation

Sind die Geräte im Besitz der Organisation, können Mitarbeiter Geräte für den täglichen Einsatz erhalten, sich Geräte für häufige Aufgaben teilen, oder Geräte können für einen speziellen Aufgabenbereich konfiguriert und auf eine einzelne App festlegt werden. Geräte, die einem einzelnen Benutzer zugewiesen werden, können von diesem personalisiert werden. Geräte, die auf eine einzelne App festgelegt oder von mehreren Mitarbeitern geteilt genutzt werden, werden vom Endbenutzer in der Regel nicht personalisiert. Wenn Sie diese Modelle miteinander kombinieren, können die Einrichtung und Konfiguration der Geräte mithilfe zentraler Technologien von Apple und einer MDM-Lösung vollkommen automatisiert werden.

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

Nicht personalisiert. Wenn Geräte von mehreren Personen gemeinsam oder nur für einen bestimmten Zweck verwendet werden (zum Beispiel in einem Restaurant oder Hotel), konfigurieren und verwalten die IT-Administratoren diese in der Regel zentral und überlassen die Einrichtung nicht dem einzelnen Benutzer. Bei der Implementierung nicht personalisierter Geräte ist es den Benutzern normalerweise nicht gestattet, auf dem Gerät Apps zu installieren oder persönliche Daten zu sichern. Die automatische Geräteregistrierung kann Sie auch bei der automatischen Einrichtung von nicht-personalisierten Geräten unterstützen. Die folgende Tabelle fasst alle Aktionen zusammen, die der Administrator und der Benutzer bei den einzelnen Schritten einer Implementierung mit organisationseigenen Geräten ausführen müssen. Wenn nicht anders angegeben, beziehen sich diese Aufgaben sowohl auf Implementierungen mit *persönlich anpassbaren* als auch mit *nicht personalisierten* Geräten.

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

Geräte im Besitz der Benutzer

Wenn Geräte vom Benutzer gekauft und eingerichtet werden, was üblicherweise als BYOD- bzw. Bring-Your-Own-Device-Implementierung bezeichnet wird, können Sie über MDM und die neue Option zur Benutzerregistrierung in iOS 13 und iPadOS dennoch Zugriff auf Unternehmensdienste wie WLAN, Mail und Kalender gewähren.

Bei einer BYOD-Implementierung dürfen Benutzer ihre eigenen Geräte einrichten und konfigurieren. Benutzer können ihre Geräte bei der MDM-Lösung Ihrer Organisation registrieren, um Zugriff auf Unternehmensressourcen zu bekommen, verschiedene Einstellungen zu konfigurieren oder ein Konfigurationsprofil bzw. Unternehmensapps zu installieren. Die Benutzer müssen sich für die Registrierung bei der MDM-Lösung Ihrer Organisation anmelden.

Die Benutzerregistrierung von persönlichen Geräten ermöglicht es, dass Ressourcen und Daten des Unternehmens auf sichere Weise verwaltet werden können und gleichzeitig die Privatsphäre und die privaten Daten und Apps der Benutzer respektiert werden. Die IT-Abteilung kann gezielt bestimmte Einstellungen durchsetzen, die Einhaltung von Unternehmensvorgaben überwachen und Unternehmensdaten und -apps entfernen, während die privaten Daten und Apps auf den Geräten der Benutzer erhalten bleiben.

Die Benutzerregistrierung beinhaltet:

- **Verwaltete Apple ID.** Die Benutzerregistrierung erfolgt mithilfe der verwalteten Apple ID, mit der eine Benutzeridentität auf dem Gerät erstellt und Zugang zu Apple Diensten ermöglicht wird. Die verwaltete Apple ID kann neben der persönlichen Apple ID verwendet werden, mit der sich der Benutzer angemeldet hat. Verwaltete Apple IDs werden in Apple Business Manager erstellt und Microsoft Azure Active Directory über die verknüpfte Authentifizierung zur Verfügung gestellt.
- **Datentrennung.** Bei der Benutzerregistrierung wird ein separates APFS Volume für verwaltete Accounts, Apps und Daten auf dem Gerät erstellt. Dieses verwaltete Volume ist kryptografisch vom Rest des Geräts getrennt.
- **Kuratierte Verwaltung für BYOD** Die Benutzerregistrierung wurde für benutzereigene Geräte entworfen, damit die IT bestimmte Konfigurationen und Richtlinien verwalten, während andere Verwaltungsaufgaben eingeschränkt sind – wie das Löschen des gesamten Geräts per Fernzugriff oder das Sammeln persönlicher Informationen.

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

	Administrator	Benutzer
Vorbereiten	• Ihre Infrastruktur evaluieren • Eine MDM-Lösung wählen • Bei Apple Business Manager anmelden	• Persönliche Apple ID und verwaltete Apple ID, App Store und iCloud Accounts nutzen, falls zutreffend
Einrichten	• Geräteeinstellungen konfigurieren • Apps und Bücher verteilen	• Bei der MDM-Lösung des Unternehmens anmelden • Apps und Bücher laden und installieren
Bereitstellen	• Kein Administratoreingriff erforderlich	• Kein Benutzereingriff erforderlich
Verwalten	• Geräte verwalten • Zusätzliche Inhalte bereitstellen und	• Zusätzliche Apps entdecken

Weitere Infos zur Benutzerregistrierung mit MDM:
support.apple.com/guide/mdm

Weitere Infos zur verknüpften Authentifizierung:
support.apple.com/guide/apple-business-manager

Implementierungsschritte

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

1. Vorbereiten

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

Ihre Infrastruktur evaluieren

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

WLAN und Netzwerk

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

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

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

Weitere Infos zum Thema WLAN und Netzwerke:
support.apple.com/guide/deployment-reference-ios

Weitere Infos zu Bonjour:
developer.apple.com/library

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 die Cloud-basierte Version von Office 365 verwenden, stellen Sie sicher, dass Sie für die Anzahl der voraussichtlich verbundenen iOS und iPadOS Geräte über ausreichend Lizenzen verfügen. iOS und iPadOS unterstützen auch die moderne Authentifizierung in Office 365 und nutzen OAuth 2.0 sowie Multi-Faktor-Authentifizierung. Wird Exchange nicht verwendet, können iOS und iPadOS mit standardbasierten Servern wie IMAP, POP, SMTP, CalDAV, CardDAV und LDAP verwendet werden.

Inhaltscaching

Inhaltscaching ist ein integriertes Feature von macOS High Sierra oder neuer. Es speichert eine lokale Kopie häufig angeforderter Inhalte von Apple Servern, um so die Bandbreite zu minimieren, die zum Laden von Inhalten in Ihrem Netzwerk erforderlich ist. Inhaltscaching beschleunigt das Laden und Bereitstellen von Software über den App Store, Mac App Store und Apple Books.

Auch Softwareaktualisierungen können zum schnelleren Laden auf iOS und iPadOS Geräte im Cache zwischengespeichert werden. Inhaltscaching umfasst den Tethered Caching Dienst, über den der Mac seine Internetverbindung mit vielen per USB angeschlossenen iOS und iPadOS Geräten teilen kann.

Weitere Infos zum Inhaltscaching:
support.apple.com/guide/deployment-reference-macos

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

Eine MDM-Lösung wählen

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

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

Weitere Infos zur Verwaltung von Geräten und Unternehmensdaten:
https://www.apple.com/de/business/docs/resources/Managing_Devices_and_Corporate_Data_on_iOS.pdf

Bei Apple Business Manager anmelden

Apple Business Manager ist ein webbasiertes Portal für IT-Administratoren, mit dem sie iPhone, iPad, iPod touch, Apple TV und Mac von einem zentralen Ort aus bereitstellen können. Apple Business Manager arbeitet nahtlos mit Ihrer Lösung für die mobile Geräteverwaltung (MDM) zusammen und macht es so einfach, die Implementierung von Geräten zu automatisieren, Apps und Inhalte zu kaufen und verwaltete Apple IDs für Mitarbeiter zu erstellen.

Das Programm zur Geräteregistrierung (Device Enrollment Program, DEP) und das Programm für Volumenlizenzen (Volume Purchase Program, VPP) sind jetzt vollständig in Apple Business Manager integriert, sodass Organisationen alles, was sie für die Implementierung von Apple Geräten brauchen, an einem Ort haben. Diese Programme werden ab dem 01. Dezember 2019 nicht mehr verfügbar sein.

Geräte

Apple Business Manager ermöglicht eine automatische Geräteregistrierung und bietet Organisationen so einen schnellen und optimierten Weg, unternehmenseigene Apple Geräte zu implementieren und bei der MDM-Lösung zu registrieren, ohne dass sie dafür einzeln in die Hand genommen oder vorbereitet werden müssen.

- Vereinfachen Sie für Ihre Benutzer den Einrichtungsprozess, indem Sie die Schritte im Systemassistenten optimieren und so sicherstellen, dass Ihre Mitarbeiter sofort nach der Aktivierung die richtigen Einstellungen erhalten. IT-Teams können dieses Erlebnis jetzt noch weiter anpassen, indem sie Zustimmungstexte, Corporate Branding oder moderne Authentifikationsmöglichkeiten für Mitarbeiter verwenden.
- Erhalten Sie zusätzliche Kontrolle über unternehmenseigene Geräte, indem Sie die Gerätebetreuung nutzen, welche ergänzende Geräteverwaltungsfunktionen bietet, die in anderen Implementierungsmodellen nicht verfügbar sind (inkl. nicht-entfernbares MDM).
- Die Verwaltung standardmäßiger MDM-Server wird vereinfacht, indem Sie je nach Gerätetyp unterschiedliche Standardserver festlegen können. Und Sie können iPhone, iPad und Apple TV mit Apple Configurator 2 jetzt auch manuell registrieren – unabhängig davon, auf welchem Weg sie gekauft wurden.

Inhalte

Apple Business Manager macht es für Organisationen einfach, Inhalte in großer Stückzahl zu kaufen. Sie können für Mitarbeiter – ganz gleich ob auf dem iPhone, iPad oder Mac – mithilfe flexibler und sicherer Verteilungsoptionen erstklassige, einsatzbereite Inhalte bereitstellen.

- Kaufen Sie Apps, Bücher und eigene Apps in großen Stückzahlen, einschließlich Apps, die Sie intern entwickelt haben. App-Lizenzen können einfach zwischen Standorten übertragen und zwischen Käufern innerhalb desselben Standorts geteilt werden. Zudem kann eine vereinheitlichte Liste aller getätigten Käufe angezeigt werden, einschließlich der aktuellen Anzahl der über eine MDM-Lösung verteilten Lizenzen.
- Sie können Apps und Bücher direkt an verwaltete Geräte oder autorisierte Benutzer verteilen und einfach nachverfolgen, welche Inhalte welchem Benutzer oder Gerät zugewiesen wurden. Bei der verwalteten Verteilung haben Sie die Kontrolle über den gesamten Verteilungsprozess und behalten gleichzeitig alle Eigentumsrechte an den Apps. Apps, die von einem Gerät oder Benutzer nicht mehr benötigt werden, können zurückgezogen und innerhalb der Organisation neu zugewiesen werden.

- Ihnen stehen verschiedene Zahlungsoptionen zur Auswahl, darunter ein Kauf per Kreditkarte oder auf Rechnung. Organisationen können Guthaben für Volumenlizenzen (wo verfügbar) direkt bei Apple oder bei einem autorisierten Apple Händler in bestimmten Beträgen der lokalen Währung kaufen. Dieses wird dann elektronisch als Store Guthaben an den Accountinhaber übermittelt.
- Sie können Apps an Geräte oder Benutzer in allen Ländern verteilen, in denen die App erhältlich ist, wodurch eine länderübergreifende Verteilung möglich wird. Entwickler können ihre Apps über den Standard-Veröffentlichungsprozess für den App Store in mehreren Ländern bereitstellen.

Hinweis: Der Erwerb von Büchern in Apple Business Manager ist in bestimmten Ländern oder Regionen nicht möglich. Weitere Informationen darüber, welche Funktionen und Kaufoptionen wo verfügbar sind, finden Sie unter support.apple.com/HT207305.

Personen

Apple Business Manager gibt Organisationen die Möglichkeit, Accounts für Mitarbeiter anzulegen und zu verwalten, die sich in die vorhandene Infrastruktur integrieren und Zugriff auf Apple Apps und Services sowie Apple Business Manager bieten.

- Erstellen Sie verwaltete Apple IDs, damit Ihre Mitarbeiter die Möglichkeit haben, mit Apps und Services von Apple zusammenzuarbeiten und auf Unternehmensdaten in verwalteten Apps zuzugreifen, die iCloud Drive verwenden. Diese Benutzeraccounts gehören den jeweiligen Organisationen und werden von diesen verwaltet.
- Nutzen Sie die verknüpfte Authentifizierung, indem Sie Apple Business Manager mit Microsoft Azure Active Directory verbinden. Verwaltete Apple IDs werden automatisch erstellt, wenn sich ein Mitarbeiter das erste Mal mit seinen vorhandenen Benutzerdaten bei einem kompatiblen Apple Gerät anmeldet.
- Mit den neuen Features zur Benutzerregistrierung in iOS 13, iPadOS und macOS Catalina können auf Geräten, die den Mitarbeitern gehören, persönliche Apple IDs zusammen mit verwalteten Apple IDs verwendet werden. Alternativ können verwaltete Apple IDs auf Geräten auch als primäre (und einzige) Apple ID genutzt werden. Verwaltete Apple IDs ermöglichen nach der erstmaligen Anmeldung auf einem Apple Gerät auch den Zugriff auf iCloud via Internet.
- Weisen Sie andere Funktionen für IT-Teams in Ihrer Organisation zu, um Geräte, Apps und Accounts in Apple Business Manager effektiv zu verwalten. Verwenden Sie die Funktion „Administrator“, um bei Bedarf die Geschäftsbedingungen anzunehmen und Befugnisse einfach zu übertragen, wenn jemand die Organisation verlässt.

Hinweis: iCloud Drive wird gegenwärtig nicht mit der Benutzerregistrierung unterstützt. iCloud Drive kann mit einer verwalteten Apple ID verwendet werden, wenn sie die einzige Apple ID auf dem Gerät ist.

Weitere Infos zu Apple Business Manager: www.apple.com/de/business/it

Beim Apple Developer Enterprise Program anmelden

Das Developer Enterprise Program von Apple bietet alle nötigen Tools zum Entwickeln, Testen und Verteilen von Apps an die Benutzer. Sie können Apps verteilen, indem Sie diese auf einem Webserver hosten oder eine MDM-Lösung verwenden. Mac Apps und Installationsprogramme können mit Ihrer Entwickler-ID für Gatekeeper, das macOS vor Schadsoftware schützt, signiert und notarisiert werden.

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

2. Einrichten

In diesem Schritt konfigurieren Sie Ihre Geräte und verteilen Ihre Inhalte mithilfe von Apple Business Manager, einer MDM-Lösung oder optional mit Apple Configurator 2. Es gibt mehrere Strategien für die Einrichtung, je nachdem, wer Eigentümer der Geräte ist und welches Implementierungsmodell Sie bevorzugen.

Ihre Geräte konfigurieren

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

Geräte mit MDM konfigurieren

Sobald Ihre Geräte sicher bei einem MDM-Server registriert sind, lassen sie sich mithilfe von Konfigurationsprofilen – XML-Dateien, die Konfigurationsdaten auf ein iOS oder iPadOS Gerät übertragen – verwalten. Diese Profile automatisieren die Konfiguration von Einstellungen, Accounts, Einschränkungen und Anmeldedaten. Sie können drahtlos über Ihre MDM-Lösung verteilt werden, was ideal ist, wenn Sie mehrere Geräte mit möglichst geringem manuellem Aufwand konfigurieren möchten. 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 Apple Business Manager, damit die Geräte Ihrer Benutzer bei der Aktivierung automatisch bei MDM registriert werden. Alle zu Apple Business Manager hinzugefügten iOS und iPadOS Geräte werden immer betreut und die MDM-Registrierung ist obligatorisch.
- **Geräte im Besitz der Benutzer.** Mitarbeiter können wählen, ob sie ihre Geräte bei MDM registrieren möchten oder nicht. Sie können die Registrierung bei MDM auch jederzeit aufheben, indem sie einfach das Konfigurationsprofil auf ihrem Gerät entfernen. Dadurch werden auch die Daten und Einstellungen Ihres Unternehmens entfernt. 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; welche Verwaltungsaktionen für ein Gerät verfügbar sind, hängt von der Betreuung und der Registrierungsmethode ab. Das iOS oder iPadOS Gerät wird dann mithilfe des Apple Push-Benachrichtigungsdienstes (APNs) über die Aktion des Administrators benachrichtigt, damit es über eine sichere Verbindung direkt mit seinem MDM-Server kommunizieren kann. Über eine Netzwerkverbindung können Geräte Befehle des APNs an jedem Ort der Welt empfangen. Es werden jedoch keine vertraulichen oder geschützten Informationen über den APNs übertragen.

Geräte mit Apple Configurator 2 konfigurieren (optional)

Für lokale Erstimplementierungen mehrerer Geräte können Organisationen Apple Configurator 2 verwenden. Mit dieser kostenlosen macOS App können Sie iOS und iPadOS Geräte über USB mit einem Mac Computer verbinden und sie auf die neueste Version von iOS oder iPadOS aktualisieren, Geräteeinstellungen und -einschränkungen konfigurieren und Apps sowie andere Inhalte installieren. Und nach der Ersteinrichtung können Sie weiterhin alles drahtlos per MDM verwalten.

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

Weitere Infos zu Apple Configurator 2:
support.apple.com/de-de/apple-configurator

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

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

Weitere Infos zu Einschränkungen für betreute Geräte:
support.apple.com/guide/mdm

Apps und Bücher verteilen

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

Verwaltete Verteilung

Mit der verwalteten Verteilung können Sie Ihre MDM-Lösung oder Apple Configurator 2 nutzen, um im Apple Business Manager Store gekaufte Apps und Bücher 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 Apple Business Manager Account verknüpfen. Sobald Sie mit Ihrem MDM-Server verbunden sind, können Sie Apple Business Manager Apps und Bücher zuweisen, selbst wenn der App Store auf dem betreffenden Gerät deaktiviert ist.

- **Apps Geräten zuweisen.** Mit Ihrer MDM-Lösung oder mit Apple Configurator 2 können Sie Apps direkt den Geräten zuweisen. Diese Methode spart mehrere Schritte bei der ersten Bereitstellung und macht sie deutlich einfacher und schneller. Gleichzeitig haben Sie aber die volle Kontrolle über verwaltete Geräte und Inhalte. Nachdem eine App einem Gerät zugewiesen wurde, wird die App per MDM auf das Gerät gepusht, ohne dass eine Einladung erforderlich ist. Jeder Benutzer dieses Geräts kann auf die App zugreifen.
- **Apps und Bücher Benutzern zuweisen.** Alternativ können Sie Ihre MDM-Lösung nutzen, um Benutzer per E-Mail oder Push-Benachrichtigung zum Download von Apps und Büchern einzuladen. Zum Annehmen der Einladung melden sich die Benutzer mit einer persönlichen Apple ID auf ihren Geräten an. Die Apple ID wird bei Apple Business Manager 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 und Bücher empfangen können. Apps sind automatisch auf allen Geräten der Benutzer zum Laden verfügbar, ohne dass Ihnen zusätzlicher Aufwand oder zusätzliche Kosten entstehen.

Wenn ein Benutzer oder ein Gerät die ihm zugewiesenen Apps nicht mehr benötigt, können Sie die Zuweisung widerrufen und die Apps anderen Benutzern oder Geräten zuweisen. Ihre Organisation bleibt so Eigentümer der gekauften Apps und behält die volle Kontrolle darüber. Allerdings bleiben Bücher, wenn sie einmal verteilt wurden, im Besitz des Empfängers und können nicht zurück übertragen oder neu zugewiesen werden.

Einlösecodes

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

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

3. Bereitstellen

iPhone und iPad machen es einfach für Mitarbeiter, ihre Geräte direkt nach dem Auspacken zu nutzen, ohne die Hilfe der IT-Abteilung zu benötigen.

Ihre Geräte verteilen

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

Systemassistent
Ab Werk können die Benutzer ihre Geräte aktivieren, grundlegende Einstellungen konfigurieren und direkt mit dem Systemassistenten loslegen. Nach der Ersteinrichtung können Benutzer auch ihre persönlichen Einstellungen anpassen, z. B. Sprache, Standort, Siri, iCloud und „Mein iPhone suchen“. Geräte, die bei Apple Business Manager registriert sind, werden automatisch bei MDM registriert, und zwar direkt im Systemassistenten.

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

Apple ID und verwaltete Apple ID
Wenn Mitarbeiter sich mit einer Apple ID bei Apple Services wie FaceTime, iMessage, dem App Store und iCloud anmelden, haben sie Zugriff auf eine Fülle von Inhalten, um Geschäftsaufgaben zu optimieren, die Produktivität zu steigern und die Zusammenarbeit zu unterstützen.

Wie alle Apple IDs werden verwaltete Apple IDs verwendet, um sich bei einem persönlichen Gerät anzumelden. Außerdem werden sie verwendet, um sich bei Apple Business Manager und Apple Services anzumelden – inklusive iCloud und der Zusammenarbeit in iWork und der Notizen App. Im Unterschied zu Apple IDs gehören verwaltete Apple IDs der Organisation und werden auch von dieser verwaltet, etwa zum Zurücksetzen von Passwörtern und zur funktionsbasierten Verwaltung. Verwaltete Apple IDs haben bestimmte eingeschränkte Einstellungen.

Geräte, die über die Benutzerregistrierung registriert sind, benötigen eine verwaltete Apple ID. Die Benutzerregistrierung unterstützt eine optionale persönliche Apple ID; andere Registrierungsoptionen unterstützen entweder eine persönliche oder eine verwaltete Apple ID. Nur die Benutzerregistrierung unterstützt mehrere Apple IDs.

Um diese Dienste optimal nutzen zu können, sollten Benutzer ihre eigenen Apple IDs oder verwaltete Apple IDs verwenden, die für sie erstellt wurden. Benutzer, die noch keine Apple ID haben, können eine erstellen, 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.

Weitere Infos zu verwalteten Apple IDs:
support.apple.com/guide/apple-business-manager

iCloud

Mit iCloud können Benutzer automatisch Dokumente und persönliche Inhalte wie Kontakte, Kalender, Dokumente und Fotos synchronisieren und auf mehreren Geräten auf dem neuesten Stand halten. „Wo ist?“ unterstützt Benutzer dabei, verlorene oder gestohlene Mac Computer bzw. iPhone, iPad oder iPod touch Geräte zu orten. Einige Dienste von iCloud – wie der iCloud Schlüsselbund und iCloud Drive – lassen sich anhand von Einschränkungen, die entweder manuell auf dem Gerät eingegeben oder über die MDM-Lösung festgelegt werden, deaktivieren. Das gibt Organisationen mehr Kontrolle darüber, welche Daten in welchen Accounts gespeichert werden.

Weitere Infos zur Verwaltung von iCloud:
support.apple.com/guide/deployment-reference-ios

4. Verwalten

Sobald Ihre Benutzer einsatzbereit sind, steht ein breites Spektrum an administrativen Funktionen zur Verfügung, mit denen Sie Ihre Geräte und Inhalte fortlaufend verwalten und warten können.

Ihre Geräte verwalten

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

Abfragen

Ein MDM-Server kann eine Vielzahl von Geräteinformationen abfragen, darunter Hardwareinformationen wie Seriennummer, Geräte-UDID oder WLAN MAC-Adresse sowie Softwareinformationen wie die iOS oder iPadOS Version und eine detaillierte Liste aller Apps, die auf dem Gerät installiert sind. Mithilfe dieser Informationen kann Ihre MDM-Lösung beispielsweise Bestandsinformationen aktualisieren, informierte Verwaltungsentscheidungen treffen und Verwaltungsaufgaben automatisieren, beispielsweise um sicherzustellen, dass die Benutzer stets die geeigneten Apps installiert haben.

Verwaltungsaufgaben

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

Verwaltete Softwareupdates

Sie können Benutzer für einen festgelegten Zeitraum daran hindern, ein betreutes Gerät manuell drahtlos zu aktualisieren. Wenn Sie diese Einschränkung verwenden, liegt die Standardverzögerung bei 30 Tagen. Sie wird aktiviert, sobald Apple ein iOS oder iPadOS Update veröffentlicht. Sie können die Standarddauer, während der keine Updates installiert werden können, aber auch anpassen – möglich sind Zeiträume von 1 Tag bis 90 Tagen. Außerdem können Sie Softwareupdates auf betreuten Geräten mit Ihrer MDM-Lösung im Voraus planen.

Modus „Verloren“

Mit Ihrer MDM-Lösung können Sie ein betreutes Gerät per Fernzugriff in den Modus „Verloren“ versetzen. Dadurch wird das Gerät gesperrt und es besteht die Möglichkeit, eine Nachricht mit einer Telefonnummer auf dem 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.

Aktivierungssperre

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

Zusätzliche Inhalte bereitstellen und verwalten

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

Interne App-Portale

Die meisten MDM-Server bieten interne App-Portale als Teil Ihrer Lösung. Oder Sie können ein eigenes internes App-Portal für Ihre Mitarbeiter einrichten, wo sie ganz einfach Apps für ihre iPhone oder iPad Geräte finden können. Über dieses Portal können interne Apps, URLs zu App Store Apps sowie Apple Business Manager Codes verlinkt werden, wodurch das Portal zu einer zentralen Plattform für die Benutzer wird. Sie können dieses Portal zentral verwalten und schützen. Über ein internes App-Portal können Mitarbeiter ganz einfach die genehmigten Ressourcen finden, die sie brauchen, ohne dafür die IT-Abteilung kontaktieren zu müssen.

Verwaltete Inhalte

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

- **Verwaltete Apps.** In iOS und iPadOS ermöglichen verwaltete Apps einer Organisation die drahtlose Verteilung von kostenlosen, kostenpflichtigen und Unternehmensapps über MDM und bieten dabei ein ideales Gleichgewicht zwischen dem Schutz von Unternehmensdaten und der Wahrung der Privatsphäre der Benutzer. Verwaltete Apps können per Fernzugriff über einen MDM-Server oder bei der Aufhebung der MDM-Registrierung des Geräts durch den Benutzer entfernt werden. Das Entfernen der App löscht auch alle mit der App verbundenen Daten. Ist eine App dem Benutzer immer noch über Apple Business Manager zugewiesen oder hat der Benutzer die App anhand eines Einlösecodes und einer persönlichen Apple ID geladen, kann er sie erneut aus dem App Store laden. Sie wird dann aber nicht mehr über MDM verwaltet.
- **Verwaltete Accounts.** MDM kann Ihren Benutzern einen schnellen Einstieg ermöglichen, indem ihre E-Mail Accounts und weitere Accounts automatisch eingerichtet werden. Abhängig vom Anbieter der MDM-Lösung und deren Integration in die internen Systeme können Account-Payloads auch mit dem Namen und der E-Mail Adresse eines Benutzers sowie ggf. mit Zertifikatsidentitäten zur Authentifizierung und Signierung vorausgefüllt werden.
- **Verwaltete Bücher und Dokumente.** MDM-Tools, Bücher, ePub Bücher und PDF Dokumente können automatisch auf die Geräte der Benutzer gepusht werden, sodass die Mitarbeiter stets alles Nötige zur Hand haben. Gleichzeitig können verwaltete Bücher aber nur mit anderen verwalteten Apps geteilt oder über verwaltete Accounts per E-Mail versendet werden. Und wenn die Materialien nicht mehr benötigt werden, können sie per Fernzugriff gelöscht werden. Über Apple Business Manager gekaufte Bücher zwar verwaltet verteilt, jedoch nicht zurückgezogen und neu zugewiesen werden. Ein bereits vom Benutzer gekauftes Buch kann nicht verwaltet werden, es sei denn, das Buch wird dem Benutzer explizit per Apple Business Manager zugewiesen.

Verwaltete App-Konfiguration

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

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

Weitere Infos zur AppConfig Community:
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.** „In verwalteter Umgebung öffnen" nutzt eine Reihe von Einschränkungen, die verhindern, dass Anhänge bzw. Dokumente aus verwalteten Quellen an nicht verwalteten Zielorten geöffnet werden können und umgekehrt. Sie können beispielsweise verhindern, dass ein vertraulicher E-Mail Anhang im verwalteten E-Mail Account Ihrer Organisation mit einer der privaten Apps des Benutzers geöffnet wird. Das Arbeitsdokument 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 zum Öffnen des Anhangs verfügbar sind. Neben verwalteten Apps, Accounts, Büchern und Domains gelten die Einschränkungen im Zusammenhang mit dem verwalteten Öffnen auch für eine Reihe von Erweiterungen.
- **Einzel-App-Modus.** Diese Einstellung beschränkt das iOS oder iPadOS Gerät auf eine einzelne App. Sie ist ideal für Kiosks oder Geräte, die nur für einen Zweck genutzt werden, wie an der Kasse im Einzelhandel oder bei der Anmeldung im Krankenhaus. Entwickler können diese Funktion auch innerhalb ihrer Apps aktivieren, sodass die Apps den Einzel-App-Modus eigenständig aktivieren und verlassen können.
- **Backups verhindern.** Diese Einschränkung hindert verwaltete Apps daran, Daten in iCloud oder auf einem Computer zu sichern. Werden Backups verhindert, können Daten aus verwalteten Apps nicht wiederhergestellt werden, falls die App per MDM entfernt und später vom Benutzer erneut installiert wird.

Supportoptionen

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

AppleCare for Enterprise

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

AppleCare OS Support

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

AppleCare Help Desk Support

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

AppleCare für Benutzer von iOS und iPadOS Geräten

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

iOS Direct Service Programm

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

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

Zusammenfassung

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

Weitere Infos zur Implementierung, Verwaltung und zu Sicherheitsfeatures von iOS und iPadOS:
support.apple.com/guide/deployment-reference-ios

Weitere Infos zu MDM-Einstellungen für die IT:
support.apple.com/guide/mdm

Weitere Infos zu Apple Business Manager:
support.apple.com/guide/apple-business-manager

Weitere Infos zu verwalteten Apple IDs für Unternehmen:
apple.com/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

Weitere Infos zu Apple at Work:
www.apple.com/de/business/

Weitere Infos zu IT-Features:
www.apple.com/de/business/it/

Weitere Infos zur Apple Plattformsicherheit:
www.apple.com/security/

Mehr zu den verfügbaren AppleCare Programmen:
www.apple.com/de/support/professional/

Mehr zu Apple Training und Zertifizierung:
training.apple.com

Kontakt zu Apple Professional Services:
consultingservices@apple.com

Einige Apps und Bücher sind je nach Land oder Region bzw. Anmeldung des Entwicklers möglicherweise nicht verfügbar; siehe Verfügbarkeit von Programmen und Inhalten. Einige Funktionen erfordern eine WLAN Verbindung. Einige Funktionen sind nicht in allen Ländern verfügbar. Die empfohlenen und Mindestsystemvoraussetzungen für iCloud finden Sie unter support.apple.com/HT204230.