



Az iOS és az iPadOS üzembe helyezésének áttekintése

Tartalom

Bevezetés

Birtoklási modellek

Az üzembe helyezés lépései

Támogatási lehetőségek

Összegzés

Bevezetés

Az iPhone és az iPad átformálhatja vállalata működését és az alkalmazottak munkáját. Mindkettő jelentősen növelni tudja a hatékonyságot, illetve szabadságot és rugalmasságot biztosít az alkalmazottaknak, akik így az irodában és azon kívül is új módokon dolgozhatnak. Ez a modern munkamódszer a szervezet minden tagjának előnyös. A felhasználók jobban hozzáférnek az információkhoz, így hatékonyabban dolgozhatnak, és képesek kreatívan megoldani a problémákat.

Az iOS és az iPadOS támogatásának köszönhetően az informatikai részlegek nem csak a technológiai problémák elhárításával és a költségek csökkentésével foglalkoznak, hanem részt vesznek az üzleti stratégia kialakításában, és valós problémákat oldanak meg. Az elkötelezettebb munkaerő és az új üzleti lehetőségek mindenki számára előnyt jelentenek.

Az iPhone és az iPad az egész vállalatra kiterjedő beállítása és üzembe helyezése minden eddiginél egyszerűbbé vált. Az Apple Business Managerrel és egy harmadik féltől származó mobilkészítési-felügyeleti (MDM) megoldással szervezete nagy tételben is egyszerűen helyezheti üzembe az iOS- és az iPadOS-eszközöket és -alkalmazásokat.

- A mobilkészítési-felügyelettel konfigurálhatja és felügyelheti eszközeit, és vezeték nélkül terjesztheti, illetve kezelheti alkalmazásait.
- Az Apple Business Manager automatizálja az Apple-eszközök regisztrációját az MDM-megoldásba, és az üzembe helyezést az informatikai részleg beavatkozását nem igénylő konfigurálási folyamattal egyszerűsíti le.
- Az Apple Business Manager az alkalmazások és könyvek nagy mennyiségű vásárlását és a felhasználóknak való vezeték nélküli kiosztását teszi lehetővé.
- Az Apple Business Manager biztosítja a Felügyelt Apple ID azonosítók létrehozását is a Microsoft Azure AD összevont hitelesítését használó alkalmazottak számára.

Ez a dokumentum útmutatást nyújt az iOS- és iPadOS-eszközök szervezeten belüli üzembe helyezésével kapcsolatban, és segít létrehozni egy olyan üzembehelyezési tervet, amely a környezetének a legjobban megfelel. E témák részletesebb kifejtése az iPhone és az iPad online üzembehelyezési útmutatójában érhető el:

support.apple.com/guide/deployment-reference-ios

Birtoklási modellek

Az üzembe helyezés egyik fontos első lépése a birtoklási modellek kiértékelése és a szervezet számára megfelelő modell kiválasztása. Az üzembe helyezés többféle módon is megközelíthető attól függően, hogy ki az eszköz tulajdonosa. Először állapítsa meg, mi lenne szervezete számára a legjobb.

A vállalatok általában kétféle birtoklási modellt használnak az iOS- és iPadOS-eszközök esetén:

- Szervezeti tulajdonú
- Felhasználói tulajdonú

Bár a legtöbb szervezet egy adott modellt részesít előnyben, előfordulhat, hogy több modellel is találkozik a környezetében. Például egy vállalati iroda bevezethet egy felhasználói tulajdonon alapuló stratégiát, és engedélyezheti az alkalmazottaknak egy személyes iPad beállítását, miközben a vállalati erőforrásokat biztonságban tarthatja és felügyelheti a felhasználók személyes adataira és alkalmazásaira gyakorolt hatás nélkül. A vállalat kiskereskedelmi üzletei ugyanakkor bevezethetnek egy szervezeti tulajdonra épülő stratégiát, amellyel több alkalmazott közösen használja az iOS- és iPadOS-eszközöket az ügyféltranzakciók feldolgozására.

Ezeknek a modelleknek a megismerése segít abban, hogy az egyedi környezetéhez leginkább illeszkedő megoldást válassza ki. Ha már tudja, hogy melyik modell elégíti ki leginkább a szervezet igényeit, csapata részletesen is megismerkedhet az Apple üzembehelyezési és felügyeleti képességeivel.

Szervezeti tulajdonban lévő eszközök

A szervezeti tulajdonban lévő eszközöket ki lehet osztani az alkalmazottaknak a mindennapi feladataik elvégzésének megkönnyítésére, vagy akár osztozhat azokon több alkalmazott is, hogy különböző általános feladatokat hajtsanak végre rajtuk, de speciális használatra, akár egyetlen alkalmazáshoz is konfigurálhatók. Az egyetlen felhasználó által használt eszközök személyre szabhatók a végfelhasználó által. Az egyetlen alkalmazáshoz használt és a több alkalmazott között megosztott eszközök általában nem szabhatók személyre a végfelhasználó által. A modellek kombinációjával, az Apple főbb technológiáival és egy MDM-megoldással teljesen automatizálhatja az eszközök beállítását és konfigurálását.

Személyre szabott. Személyre szabott stratégiát követve mindegyik felhasználó megválaszthatja a saját eszközét, és regisztrálhatja egy MDM-megoldásban, amely vezeték nélküli kapcsolaton keresztül biztosítja a szervezeti beállításokat és alkalmazásokat. A közvetlenül az Apple-től, illetve a részt vevő hivatalos Apple-viszonteladótól vagy -szolgáltatóktól vásárolt eszközöknél kihasználhatja az Apple Business Manager előnyeit, és automatikusan regisztrálhatja az új eszközöket az Automatizált készülékrejestrációként ismert MDM-megoldásba. A konfigurálás után a felhasználók személyre szabhatják ezeket az eszközöket saját alkalmazásaikkal és adataikkal, valamint a szervezet által biztosított bármilyen szervezeti fiókkal vagy alkalmazással.

Nem személyre szabott. Ha egy eszközön többen osztoznak, vagy csak egy bizonyos feladatra használják (például egy étteremben vagy egy szállodában), akkor a rendszergazda általában központilag konfigurálja és kezeli a készüléket, és nem egy alkalmazott végzi el a beállítást. Nem személyre szabott környezetben a felhasználók általában nem telepíthetnek alkalmazásokat vagy menthetnek személyes adatokat az eszközre. Az Apple Business Manager Automatizált készülékre regisztrációja segít a nem személyre szabott eszközök beállításának automatizálásában. A következő ábra bemutatja, hogy milyen intézkedésekre van szükség a rendszergazda és a felhasználó részéről egy szervezeti tulajdonú stratégia egyes lépései során. Hacsak másképp nincs jelölve, az intézkedések a *személyre szabott* és a *nem személyre szabott* környezetekre is vonatkoznak.

	Rendszergazda	Felhasználó
Előkészítés	- Az infrastruktúra kiértékelése - Egy MDM-megoldás kiválasztása - Regisztráció az Apple Business Managerben	Nincs szükség felhasználói beavatkozásra
Beállítás	- Készülékek konfigurálása - Alkalmazások és könyvek terjesztése	Nincs szükség felhasználói beavatkozásra
Üzembe helyezés	- Eszközök kiosztása Csak személyre szabott - Felhasználói személyre szabás engedélyezése	Csak személyre szabott - Alkalmazások és könyvek letöltése és telepítése - Az Apple ID, valamint az App Store- és az iCloud-fiókok igény szerinti használata Csak nem személyre szabott - Nincs szükség felhasználói beavatkozásra
Felügyelet	- Eszközök adminisztrálása - További tartalmak telepítése és kezelése	Csak személyre szabott - További alkalmazások felfedezése Csak nem személyre szabott - Nincs szükség felhasználói beavatkozásra

Felhasználói tulajdonban lévő eszközök

Az MDM-mel az iOS 13 és az iPadOS új Felhasználói regisztrációja akkor is hozzáférést biztosíthat az olyan vállalati szolgáltatásokhoz, mint például a Wi-Fi, a levelezés és a naptárak, ha az eszközöket a felhasználó vásárolta és állította be – az úgynevezett BYOD, vagyis saját eszköz használatára épülő környezetben.

A BYOD (saját eszköz használatára épülő) környezetben a felhasználók saját maguk állíthatják be és konfigurálhatják az eszközeiket. A felhasználók regisztrálhatják az eszközeiket egy vállalati MDM-megoldásban, így hozzáférhetnek a vállalati erőforrásokhoz, konfigurálhatnak különböző beállításokat, telepíthetnek egy konfigurációs profilt vagy vállalati alkalmazásokat. A felhasználóknak regisztrálniuk kell a szervezet MDM-megoldásában.

A személyes eszközök Felhasználói regisztrációjának egyik előnye, hogy a vállalati erőforrások és adatok biztonságosan kezelhetők, emellett pedig tiszteletben tartják a felhasználók személyes adatvédelmét, adatait és alkalmazásait. Az informatikai részleg csak bizonyos beállításokat léptethet érvénybe, felügyelheti a vállalati megfelelőséget, és csak vállalati adatokat és alkalmazásokat távolíthat el, érintetlenül hagyva a felhasználók eszközein található személyes adatokat és alkalmazásokat.

A Felhasználói regisztráció az alábbiakat tartalmazza:

- **Felügyelt Apple ID.** A Felhasználói regisztráció együttműködik a felügyelt Apple ID azonosítóval az eszköz felhasználói identitásának létrehozásához és az Apple-szolgáltatások elérésének biztosításához. A felügyelt Apple ID-kat a felhasználó által a bejelentkezéshez használt személyes Apple ID azonosítók mellett is lehet használni. A felügyelt Apple ID-k az Apple Business Managerben hozhatók létre, és a Microsoft Azure Active Directory összevont hitelesítése által lesznek kiosztva.
- **Az adatok szétválasztása.** A Felhasználói regisztráció egy különálló APFS-kötetet hoz létre a felügyelt fiókok, alkalmazások és adatok számára. Ez a felügyelt kötet titkosított módon különíti el az adatokat a készüléken található többi tartalomtól.
- **A BYOD szelektív felügyelete.** A Felhasználói regisztráció a felhasználói tulajdonban lévő eszközökhöz lett tervezve, hogy az informatikai részleg egy sor beállítást és szabályzatot tudjon felügyelni, azonban bizonyos felügyeleti feladatokhoz, például a teljes eszköz távoli törléséhez vagy a személyes adatok gyűjtéséhez nem fér hozzá.

	Rendszergazda	Felhasználó
Előkészítés	• Az infrastruktúra kiértékelése • Egy MDM-megoldás kiválasztása • Regisztráció az Apple Business Managerben	• A személyes Apple ID és a felügyelt Apple ID azonosító, az App Store, valamint az iCloud-fiókok igény szerinti használata
Beállítás	• Eszközbeállítások konfigurálása • Alkalmazások és könyvek terjesztése	• Regisztráció a vállalati MDM-megoldásra • Alkalmazások és könyvek letöltése és telepítése
Üzembe helyezés	• Nincs szükség rendszergazdai beavatkozásra	• Nincs szükség felhasználói beavatkozásra
Felügyelet	• Eszközök adminisztrálása • További tartalmak telepítése és kezelése	• További alkalmazások felfedezése

A következő táblázat bemutatja, hogy milyen intézkedésekre van szükség a rendszergazda és a felhasználó részéről egy felhasználói tulajdonú eszközökre épülő üzembehelyezési stratégia egyes lépései során.

További információk az MDM-beli Felhasználói regisztrációról:

support.apple.com/guide/mdm

Ismerje meg jobban az összevont hitelesítést:

support.apple.com/guide/apple-business-manager

Az üzembe helyezés lépései

Ez a szakasz részletesebben ismerteti az eszközök és tartalmak üzembe helyezésének mind a négy lépését, amelyek a következők: a környezet előkészítése, illetve az eszközök beállítása, üzembe helyezése és felügyelete. Az egyes végrehajtott lépések attól függenek, hogy az eszközök a szervezet vagy a felhasználók tulajdonában állnak-e.

1. Előkészítés

A szervezetének megfelelő üzembehelyezési modell azonosítása után kövesse a következő lépéseket a telepítés előkészítéséhez. Ezeket az intézkedéseket már azelőtt megteheti, hogy az eszközök a kezében volnának.

Az infrastruktúra kiértékelése

Az iPhone és az iPad gördülékenyen integrálható a legtöbb hagyományos vállalati informatikai környezetbe. Fontos a meglévő hálózati infrastruktúra felmérése, így meggyőződhet arról, hogy vállalata az iOS és az iPadOS összes előnyét ki tudja használni.

Wi-Fi és hálózatkezelés

A folyamatos és megbízható hozzáférés egy vezeték nélküli hálózathoz elengedhetetlen az iOS- és az iPadOS-eszközök beállításához és konfigurálásához. Győződjön meg arról is, hogy vállalatának Wi-Fi-hálózata támogatja több felhasználói eszköz egyidejű csatlakoztatását. Szükség lehet webproxyjának vagy tűzfalportjainak a konfigurálására, ha az eszközök nem férnek hozzá az Apple aktivációs szervereihez, valamint az iCloudhoz vagy az App Store-hoz. Az Apple és a Cisco azt is optimalizálta, ahogyan az iPhone és az iPad kommunikál a Cisco vezeték nélküli hálózataival, így más fejlett hálózati szolgáltatások is elérhetővé váltak, mint például a gyors barangolás és a szolgáltatásminőség (QoS) optimalizálása az alkalmazásokhoz.

Mérje fel a VPN-infrastruktúrát, és győződjön meg róla, hogy a felhasználók iOS- és iPadOS-eszközeikről biztonságosan hozzáférhetnek távolról a vállalati erőforrásokhoz. Fontolja meg az iOS és az iPadOS igény szerinti VPN vagy alkalmazásonkénti VPN funkciójának használatát, hogy csak akkor jöjjön létre VPN-kapcsolat, amikor szükség van rá. Ha külön VPN használatát tervezi alkalmazásonként, ellenőrizze, hogy a VPN-átjárói támogatják-e ezeket a képességeket, illetve hogy elég licencet vásárolt-e a megfelelő számú felhasználó és kapcsolat kiszolgálásához.

Győződjön meg arról is, hogy a hálózati infrastruktúra megfelelően működik a Bonjourral, az Apple szabványalapú, konfigurálást nem igénylő hálózati protokolljával. A Bonjour lehetővé teszi az eszközök számára a szolgáltatások automatikus észlelését a hálózaton. Az iOS- és az iPadOS-eszközök a Bonjour segítségével csatlakoznak az AirPrint-kompatibilis nyomtatókhoz és az olyan AirPlay-kompatibilis eszközökhöz, mint például az Apple TV. Egyes alkalmazások a Bonjour használatával fedezik fel az együttműködéshez vagy megosztáshoz elérhető többi eszközt is.

További információk a Wi-Fi-ről és a hálózatkezelésről:

support.apple.com/guide/deployment-reference-ios

További információ a Bonjourról: developer.apple.com/library

E-mail, kontaktok és naptárak

Ha a Microsoft Exchange-et használja, ellenőrizze, hogy az ActiveSync naprakész-e, és hogy úgy van-e konfigurálva, hogy támogassa a hálózaton lévő összes felhasználó hozzáférését. Ha a felhőalapú Office 365-öt használja, győződjön meg róla, hogy elég licenccel rendelkezik a várhatóan csatlakoztatni kívánt iOS- és iPadOS-eszközök támogatásához. Az iOS és az iPadOS támogatja az Office 365 modern hitelesítését, amely kihasználja az OAuth 2.0 szabvány és a többtényezős hitelesítés előnyeit. Ha nem az Exchange-et használja, az iOS és az iPadOS többek között az IMAP, a POP, az SMTP, a CalDAV, a CardDAV és az LDAP szabványon alapuló szerverekkel is együttműködik.

Tartalmak gyorsítótárazása

A macOS High Sierra és az újabb verziók Tartalom-gyorsítótárazás nevű integrált funkciója tárolja az Apple-szerverekről gyakran lekért tartalmak helyi másolatát, ezáltal minimálisra csökkenti a letöltéshez szükséges sávszélességet a hálózaton. A Tartalom-gyorsítótárazás felgyorsítja az App Store, a Mac App Store és az Apple Books áruházakból származó szoftverek letöltését és közzétételét.

Szoftverfrissítéseket is képes tárolni a gyorsítótárban az iOS- és az iPadOS-eszközökre történő gyorsabb letöltés érdekében. A Tartalom-gyorsítótárazás tartalmazza a vezetékes gyorsítótárazási szolgáltatást, amelynek segítségével a Mac több iOS- és iPadOS-eszközzel is megoszthatja az internet-hozzáférését egy USB-kapcsolaton keresztül.

További információ a Tartalom-gyorsítótárazásról:

support.apple.com/guide/deployment-reference-macos

Információk a vezetékes gyorsítótárazásról:

support.apple.com/HT207523

Egy MDM-megoldás kiválasztása

Az Apple iOS-hez és iPadOS-hez készült felügyeleti keretrendszere lehetővé teszi a szervezeteknek, hogy biztonságosan regisztráljanak készülékeket a vállalati környezetben, vezetékek nélkül konfigurálják és frissítsék a beállításokat, felügyeljék a szabályzatoknak való megfelelést, alkalmazásokat és könyveket telepítsenek, vagy akár távolról töröljenek vagy zároljanak felügyelt eszközöket. Ezek a felügyeleti funkciók harmadik féltől származó MDM-megoldásokon keresztül érhetők el.

Számos külső MDM-megoldás áll rendelkezésre a különböző szerverplatformokhoz. Mindegyik megoldás különböző felügyeleti konzolokat, szolgáltatásokat és árképzést kínál. A végleges megoldás kiválasztása előtt tekintse át az alábbi segédleteket annak felméréséhez, hogy melyik felügyeleti szolgáltatások a legmegfelelőbbek a szervezete számára. A harmadik féltől származó MDM-megoldások mellett Profilkezelő néven az Apple kínálatában is szerepel egy MDM-megoldás, amely a macOS Server egyik szolgáltatása.

Információk az eszközök és vállalati adatok felügyeletéről:

apple.com/business/docs/resources/

[Managing_Devices_and_Corporate_Data_on_iOS.pdf](#)

Regisztráció az Apple Business Managerben

Az Apple Business Manager egy webes portál, amelyen a rendszergazdák egy helyről végezhetik el az iPhone, iPad, iPod touch, Apple TV és Mac üzembe helyezését. Az Apple Business Manager problémamentesen működik együtt a cég mobilkészíték-felügyeleti (MDM-) megoldásával, és megkönnyíti az eszközök automatikus üzembe helyezését, az alkalmazásvásárlást és a tartalmak kiosztását, valamint az alkalmazottak felügyelt Apple ID azonosítóinak létrehozását.

A Készülékregisztrációs program (DEP) és a Mennyiségi vásárlási program (VPP) mostanra már az Apple Business Manager szerves részét képezi, így a szervezeteknek egyetlen helyen áll rendelkezésre minden, amire csak szükségük lehet az Apple-eszközök üzembe helyezéséhez. 2019. december 1-től ezek a programok nem lesznek elérhetők.

Eszközök

Az Apple Business Manager lehetővé teszi az automatizált eszközregisztrációt. Gyors és gördülékeny módot biztosít a vállalati tulajdonban lévő Apple-eszközök üzembe helyezésére és MDM-ben való regisztrációjára, anélkül, hogy a készülékeket kézbe kéne venni vagy elő kéne készíteni.

- Leegyszerűsíti a felhasználók által végrehajtandó beállítási folyamatot azzal, hogy egyes lépéseket gördülékenyebbé tesz a Beállítási asszisztensben, így amikor az alkalmazottak aktiválják a készüléküket, azonnal a megfelelő beállítások lépnek érvénybe. Az informatikai részleg most még inkább testre szabhatja ezt a lehetőséget azáltal, hogy hozzájárulási szöveget, vállalati arculatot vagy modern hitelesítési eljárást biztosít az alkalmazottaknak.
- A felügyelet lehetővé teszi a vállalati tulajdonban lévő eszközök szigorúbb kézben tartását, ami olyan szintű eszközfelügyeletet tesz lehetővé (például a nem eltávolítható MDM-et), amely más üzembehelyezési modelleknél nem érhető el.
- Az eszköztípus alapján beállított alapértelmezett szerverekkel könnyedén beállíthatók alapértelmezett MDM-szerverek. Emellett a beszerzési forrástól függetlenül manuálisan is regisztrálhat iPhone-okat, iPadeket és Apple TV-ket az Apple Configurator 2 használatával.

Tartalmak

Az Apple Business Managerrel a cégek egyszerűen vásárolhatnak tartalmakat nagy tételben. Alkalmazottaik iPhone-jához, iPadjéhez vagy Mac gépéhez nagyszerű, használatra kész tartalmakat biztosíthatnak, amelyeket rugalmasan és biztonságos módon tehetnek közzé.

- Az alkalmazásokat, könyveket és egyéni alkalmazásokat nagy tételben is beszerezheti, a belső fejlesztésű alkalmazásokkal egyetemben. Az alkalmazáslicencek egyszerűen átadhatók a helyszínek között, a licenceken pedig oszthatóknak az egy helyszínen tartózkodó beszerzők. A vásárlási előzmények egységes listája is megtekinthető azzal együtt, hogy éppen mennyi licenc van használatban az MDM-en keresztül.
- Közvetlenül a felügyelt eszközökre vagy a jogosult felhasználóknak oszthatja ki az alkalmazásokat és a könyveket, és egyszerűen nyomon követheti, hogy a tartalmak mely felhasználókhoz vagy készülékekhez lettek hozzárendelve.

A felügyelt terjesztéssel az irányítása alatt tarthatja a terjesztési folyamatot, és az alkalmazások teljes tulajdonjoga is Önnél marad. Az egyes eszközökön vagy felhasználók számára szükségtelenné vált alkalmazások visszavonhatók, és a cégen belül hozzárendelhetők más készülékekhez vagy felhasználókhoz.

- Fizetni többféle módon is lehet, például hitelkártyával vagy beszerzési rendeléssel. A szervezetek VPP-egyenleget vásárolhatnak (ahol az elérhető) az Apple-től vagy egy hivatalos Apple-viszonteladótól a helyi pénznemben megadott összegért, amely áruházi egyenleg formájában elektronikus úton érkezik meg a fióktulajdonoshoz.
- Az alkalmazások minden olyan ország eszközei vagy felhasználói számára elérhetővé tehetők, ahol az adott alkalmazás beszerezhető, így a nemzetközi terjesztés is lehetővé válik. A fejlesztők több országban is elérhetővé tehetik alkalmazásaikat az App Store hagyományos terjesztési módszerével.

Megjegyzés: Az Apple Business Manageren keresztüli könyvvásárlás egyes országokban vagy régiókban nem érhető el. Az egyes funkciók és vásárlási módok elérhetőségéről a következő helyen tájékozódhat: support.apple.com/HT207305.

Személyek

Az Apple Business Manager lehetővé teszi, hogy a szervezetek a meglévő infrastruktúrát integráló alkalmazotti fiókokat hozzanak létre és kezeljenek, amelyek hozzáférést biztosítanak az Apple-alkalmazásokhoz és -szolgáltatásokhoz, valamint az Apple Business Managerhez.

- Létrehozhat felügyelt Apple ID-kat az alkalmazottaknak, hogy közösen dolgozhassanak az Apple-alkalmazásokban és -szolgáltatásokban, és hozzáférhessenek az iCloud Drive-ot használó felügyelt alkalmazásokban található vállalati adatokhoz. Ezek a fiókok a cég vagy szervezet kezelésében és tulajdonában vannak.
- Kihasználhatja az összevont hitelesítés előnyeit az Apple Business Manager és a Microsoft Azure Active Directory összekapcsolásával. A felügyelt Apple ID-k automatikusan létrejönnek, amikor az alkalmazottak először bejelentkeznek már meglévő hitelesítő adataikkal egy kompatibilis Apple-eszközön.
- Az iOS 13, az iPadOS és a macOS Catalina új Felhasználói regisztrációs szolgáltatásainak köszönhetően a felügyelt Apple ID-k a személyes Apple ID-k mellett is beállíthatók az alkalmazottak saját tulajdonában lévő eszközökön. A felügyelt Apple ID-k ugyanakkor az eszköz elsődleges (és egyetlen) Apple ID azonosítójaként is használhatók. A felügyelt Apple ID-kkal az iCloudhoz is hozzá lehet férni az interneten, miután bejelentkeztek velük egy Apple-eszközre.
- Kijelölhet különböző szerepköröket a vállalati informatikai csapatoknak, hogy hatékonyan tudják kezelni az eszközöket, alkalmazásokat és fiókokat az Apple Business Managerben. A rendszergazdai szerepkör lehetővé teszi a használati feltételek elfogadását, ha arra szükség van, és megkönnyíti a feladatok átruházását, ha egy alkalmazott elhagyja a szervezetet.

Megjegyzés: Az iCloud Drive a Felhasználói regisztrációval történő használata egyelőre nem támogatott. Az iCloud Drive csak akkor használható felügyelt Apple ID-val, ha egy eszközön ez az egyetlen Apple ID azonosító.

További információ az Apple Business Managerről: www.apple.com/business/it

Regisztráció az Apple Developer Enterprise Programba

Az Apple vállalati fejlesztői programja (Apple Developer Enterprise Program) teljes körű eszközkészletet kínál az alkalmazások fejlesztéséhez, teszteléséhez és felhasználók közötti terjesztéséhez. Az alkalmazások terjesztése kétféleképpen lehetséges: webszerverről vagy MDM-megoldással. A Mac-alkalmazásokat és a telepítőket az Ön fejlesztői azonosítójával lehet aláírni és hitelesíteni a Gatekeeper számára (amely segít megvédeni a macOS-t a kártevőktől).

További információ a Developer Enterprise Programról:

developer.apple.com/programs/enterprise

2. Beállítás

Ebben a lépésben kerül sor az eszközök konfigurálására és a tartalmak terjesztésére az Apple Business Manager, valamilyen MDM-megoldás vagy az Apple Configurator 2 használatával. A beállításhoz többféle megközelítési mód is választható attól függően, hogy ki az eszközök tulajdonosa, illetve hogy milyen típusú üzembe helyezést részesít előnyben.

Az eszközök konfigurálása

A felhasználók vállalati szolgáltatásokhoz való hozzáférését többféleképpen konfigurálhatja. Az informatikai részleg konfigurációs profilok terjesztésével szabályozhatja az eszközök konfigurálását. A felügyelt eszközökhöz további konfigurációs lehetőségek is elérhetők.

Készülékek beállítása MDM használatával

Miután az eszközök biztonságosan regisztrálva lettek egy MDM-szerveren, a felügyeletüket konfigurációs profilok teszik lehetővé – ezek olyan XML-fájlok, amelyek az iOS- és az iPadOS-eszközök konfigurációs adatait tartalmazzák. Ezek a profilok automatizálják a beállítások, fiókok, korlátozások és hitelesítő adatok konfigurálását. A profilok az MDM-megoldásból vezetékek nélkül továbbíthatók, ami ideális módja több eszköz minimális beavatkozást igénylő konfigurálásának. A profilok elküldhetők e-mail-mellékletként, letölthetők egy weboldaltól, vagy az Apple Configurator 2-vel is telepíthetők az eszközökre.

- **Szervezeti tulajdonban lévő eszközök.** Az Apple Business Manager lehetővé teszi a felhasználók eszközeinek MDM használatával történő automatikus regisztrálását az eszközök aktiválásakor. Az Apple Business Managerbe felvett iOS- és iPadOS-eszközök folyamatos felügyelet alatt állnak, és az MDM-regisztráció kötelező.
- **Felhasználói tulajdonban lévő eszközök.** Az alkalmazottak eldönthetik, hogy szeretnék-e regisztrálni eszközeiket az MDM-ben. Ha szeretnének kilépni az MDM-ből, bármikor eltávolíthatják a konfigurációs profilt az eszközről. Ezzel együtt a vállalati adatokat és beállításokat is eltávolítják. Érdemes elgondolkozni azon, hogyan ösztönözheti a felhasználókat a felügyelet fenntartására. Például a Wi-Fi-hálózathoz való hozzáférés feltétele lehet az MDM-regisztráció, vagyis az MDM-megoldással automatikusan kioszthatja a vezetékek nélküli hitelesítési adatokat.

A készülékek regisztrálása után a rendszergazdák MDM-szabályzatokat és beállításokat alkalmazhatnak, illetve parancsokat adhatnak ki. A műveletek a felügyelet és a regisztrációs mód függvényében változnak. Az iOS- és az iPadOS-eszköz ezután értesítést kap a rendszergazda által végzett műveletről az Apple push-értesítési (APN) szolgáltatáson keresztül, így közvetlenül, egy biztonságos kapcsolaton keresztül kommunikálhat az MDM-szerverrel. A hálózati kapcsolattal rendelkező készülékek világszerte tudják fogadni az APN-parancsokat. Az APN értesítéseiben nincsenek bizalmas adatok vagy védett információk.

Készülékek beállítása az Apple Configurator 2 használatával (opcionális)

Az Apple Configurator 2-vel a vállalatok helyben is elvégezhetik egyszerre több eszköz kezdeti üzembe helyezését. Ezzel az ingyenes macOS-alkalmazással iOS- és iPadOS-eszközöket egy Mac géphez csatlakoztathatja USB-n keresztül,

és az iOS és az iPadOS legfrissebb verziójára frissítheti őket, konfigurálhatja az eszközök beállításait és korlátozásait, valamint alkalmazásokat és egyéb tartalmakat is telepíthet azokra. A kezdeti beállítást követően a készülék vezeték nélkül felügyelhető az MDM-mel.

Az Apple Configurator 2 felhasználói felülete az Ön eszközeire és a rajtuk elvégezni kívánt különálló feladatokra fókuszál. Az alkalmazás integrálható az Apple Business Managerrel, így az eszközök a vállalat beállításával automatikusan regisztrálhatnak az MDM-be. Az Apple Configurator 2-ben sablonok alapján egyéni munkafolyamatok hozhatók létre különálló feladatok kombinálásához.

További információ az Apple Configurator 2-ről:

support.apple.com/apple-configurator

Felügyelt eszközök

Felügyelt üzemmódban további felügyeleti lehetőségek állnak rendelkezésre a szervezeti tulajdonban lévő iOS- és iPadOS-eszközökhöz, például letilthatja az AirDropot, vagy Egyetlen alkalmazás módba helyezheti az eszközt. A felügyelet a webes szűrők globális proxyn keresztül engedélyezésére is lehetőséget nyújt, így gondoskodni lehet többek között arról, hogy a felhasználói internetes adatforgalom megfeleljen a szervezet irányelveinek, vagy meg lehet akadályozni, hogy a felhasználók visszaállítsák a készülékeket a gyári beállításokra. Alapértelmezés szerint az összes iOS- és iPadOS-eszköz nem felügyeltként van beállítva. A felügyelet nemcsak az Apple Business Managerrel, hanem manuálisan is engedélyezhető az Apple Configurator 2-vel.

Még ha jelenleg nem is tervezi csak felügyelt szolgáltatások használatát, akkor is érdemes lehet beállítani a felügyeletet az eszközök üzembe helyezésekor, mivel így a jövőben kihasználhatja az ilyen képességekkel járó előnyöket. Ellenkező esetben törölnie kell az üzembe helyezett eszközök tartalmát. A felügyelet nem az eszközök zárolását jelenti, sőt, a felügyeleti képességek kiterjesztésével a vállalati tulajdonban lévő eszközök hatékonyabban használhatók. Hosszabb távon az eszközök felügyelete további lehetőségeket nyit meg a vállalat számára.

További információk a felügyelt eszközök korlátozásairól:

support.apple.com/guide/mdm

Alkalmazások és könyvek terjesztése

Az Apple a programok széles körét kínálja, amelyekkel a vállalat kihasználhatja az iOS- és iPadOS-hez elérhető kiváló alkalmazásokat és tartalmakat. Ezekkel a képességekkel eljuttathatja az eszközökre és a felhasználóknak az Apple Business Manageren keresztül vásárolt vagy a vállalaton belül fejlesztett alkalmazásokat és könyveket, így minden a felhasználók rendelkezésére áll majd a hatékony munkához. Vásárláskor ki kell választania, hogy melyik terjesztési módszert szeretné használni: a felügyelt terjesztést vagy a beváltható kódokat.

Felügyelt terjesztés

A felügyelt terjesztéssel az Apple Business Manager áruházából beszerzett alkalmazások és könyvek az MDM-megoldással vagy az Apple Configurator 2-vel is felügyelhetők azokban az országokban, ahol az alkalmazás elérhető. A felügyelt terjesztés engedélyezéséhez először egy biztonságos tokennel össze kell kapcsolnia az MDM-megoldást és az Apple Business Manager-fiókot. Miután csatlakozott az MDM-szerverhez, az Apple Business Manager-alkalmazásokat és -könyveket akkor is hozzá tudja rendelni, ha az App Store elérése le van tiltva az adott eszközön.

- **Alkalmazások hozzárendelése az eszközökhöz.** Az MDM-megoldás vagy az Apple Configurator 2 használatával közvetlenül az eszközökhöz is rendelheti az alkalmazásokat. Ez a módszer az alkalmazások bevezetésének több lépését is megtakarítja, így érezhetően egyszerűbbé és gyorsabbá teszi a terjesztést, miközben teljes felügyeletet biztosít az eszközök és tartalmak felett. Az eszközökhöz hozzárendelt alkalmazásokat az MDM továbbítja az eszközre, és nincs szükség a felhasználók meghívására. Az eszközt használó bármely személy hozzáférhet az alkalmazáshoz.
- **Alkalmazások és könyvek hozzárendelése a felhasználókhoz.** Egy másik módszer, ha az MDM-megoldással meghívja a felhasználókat az alkalmazások és könyvek letöltésére egy e-mail-üzenet vagy push-értesítés formájában. A meghívó elfogadásához a felhasználóknak személyes Apple ID azonosítójukkal be kell jelentkezniük az eszközükön. Az Apple ID regisztrálva van az Apple Business Manager szolgáltatásban, de a rendszer bizalmas adatként kezeli, és a rendszergazda számára sem látható. Ha a felhasználó elfogadja a meghívást, akkor csatlakozik az MDM-szerverhez, és fogadhatja a hozzá rendelt alkalmazásokat és könyveket. Az alkalmazások automatikusan letölthetővé válnak a felhasználó összes eszközén, így a kiosztásuk a szervezet részéről semmilyen további teendőt vagy költséget nem igényel.

Ha a hozzárendelt alkalmazások bizonyos eszközökön vagy felhasználók számára szükségtelenné válnak, akkor vissza lehet őket vonni, és hozzá lehet rendelni a vállalaton belül más eszközökhöz vagy felhasználókhöz, így a megvásárolt alkalmazások teljes mértékben a szervezet tulajdonában és ellenőrzése alatt maradnak. A kiosztott könyvek azonban a címzett tulajdonában maradnak, és nem vonhatók vissza vagy rendelhetők át másra.

Beváltható kódok

A tartalmakat beváltható kódok segítségével is kioszthatja. Ez akkor hasznos, ha a szervezetnek nem áll módjában MDM-megoldást használni a végfelhasználó eszközén, például egy franchise-alapú üzleti környezetben. Ilyenkor a kódot beváltó felhasználó véglegesen megkapja az adott alkalmazást vagy könyvet. A beváltható kódokat a vásárló intézmény táblázatos formában kapja meg, amely a megvásárolt példányszámban, minden alkalmazáspéldányhoz vagy könyvhöz egyedi kódot tartalmaz. A kódok beváltásakor a táblázat frissül az Apple Business Manager áruházában, így a beváltott kódok száma bármikor ellenőrizhető. A kódok MDM vagy az Apple Configurator 2 használatával, illetve e-mailben és belső webhelyen keresztül is kioszthatók.

Alkalmazások és tartalmak telepítése az Apple Configurator 2 használatával (opcionális)

Az alapvető beállításon és konfiguráláson túl az Apple Configurator 2-vel alkalmazásokat és tartalmakat is telepíthet a felhasználók helyett beállítani kívánt eszközökre. A személyre szabott üzembe helyezések esetén előre telepítheti az alkalmazásokat, amivel időt és sávszélességet takaríthat meg. A nem személyre szabott üzembe helyezéseknél pedig teljes körűen beállíthatja minden eszközét, egészen a kezdőképernyőig. Az eszközök Apple Configurator 2 használatával történő konfigurálásakor App Store-alkalmazásokat, vállalaton belüli alkalmazásokat és dokumentumokat is telepíthet. Az App Store-alkalmazásokhoz az Apple Business Managert kell használni. A dokumentumok olyan alkalmazásokban érhetők el, amelyek támogatják a fájlmegosztást. Az iOS- és az iPadOS-eszközökön lévő dokumentumok áttekintéséhez vagy lekéréséhez csatlakoztassa az eszközöket egy Apple Configurator 2-t futtató Machez.

3. Üzembe helyezés

Az alkalmazottak egyszerűen, az informatikai részleg segítségével, ráadásul azonnal használatba vehetik az iPhone-okat és az iPadeket.

Készülékek kiosztása

Miután megtörtént az eszközök előkészítése és beállítása az első két lépésben leírtak szerint, a készülékek készen állnak a kiosztásra. Személyre szabott üzembe helyezés esetén adja át az eszközöket a felhasználóknak, akik az egyszerűsített Beállítási asszisztens segítségével véglegesíthetik a telepítést, és személyre szabhatják a készülékeket. Nem személyre szabott üzembe helyezés esetén adja át az eszközöket a műszakban dolgozó alkalmazottaknak, vagy helyezze el őket az eszközök töltésére és biztonságos tárolására tervezett kioszkokban.

Beállítási asszisztens

A Beállítási asszisztens segíti az alkalmazottakat eszközeik aktiválásában, az alapvető beállítások konfigurálásában és a munka azonnali megkezdésében. A kezdeti beállítást követően a felhasználók testre szabhatják személyes beállításait, például a nyelvet, a tartózkodási helyet, Sirit vagy az iCloud és az iPhone keresése használatát. Az Apple Business Managerbe regisztrált készülékek automatikusan regisztrálva lesznek az MDM-be is a Beállítási asszisztenssel.

Felhasználói személyre szabás engedélyezése

A személyre szabott és a saját tulajdonban lévő (BYOD) eszközökön végzett üzembe helyezések hatékonyságát tovább növelheti, ha engedélyezi a felhasználóknak a készülékek Apple ID-val végzett személyre szabását, mivel így a felhasználók maguk választhatják ki a feladataik és céljaik teljesítéséhez legjobban megfelelő alkalmazásokat és tartalmakat.

Apple ID és felügyelt Apple ID

Ha az alkalmazottak Apple ID-val jelentkeznek be az Apple olyan szolgáltatásaiba, mint a FaceTime, az iMessage, az App Store vagy az iCloud, olyan tartalmak széles köréhez férhetnek hozzá, amelyek leegyszerűsítik az üzleti feladatok elvégzését, növelik a hatékonyságot, és megkönnyítik az együttműködést.

A többi Apple ID azonosítóhoz hasonlóan a felügyelt Apple ID-kkal is be lehet jelentkezni a személyes eszközökre. Emellett az Apple-szolgáltatások (például az iCloud, vagy az iWork és a Jegyzetek együttműködési funkciói) és az Apple Business Manager elérésére is használhatók. Az Apple ID azonosítóktól eltérően a felügyelt Apple ID-kat a szervezet birtokolja és kezeli, beleértve a jelszó-visszaállításokat és a szerepköralapú felügyeletet is. A felügyelt Apple ID-k egyes beállításai korlátozva vannak.

A Felhasználói regisztrációval regisztrált eszközöknek rendelkezniük kell felügyelt Apple ID-val. A Felhasználói regisztráció egy opcionális személyes Apple ID használatát is támogatja, míg a többi regisztrációs lehetőség vagy egy személyes, vagy egy felügyelt Apple ID használatát teszi lehetővé. Csak a Felhasználói regisztráció támogatja több Apple ID használatát.

Annak érdekében, hogy ki tudják használni a szolgáltatások előnyeit, az alkalmazottaknak a saját Apple ID-jukat vagy a számukra létrehozott felügyelt Apple ID-t kell használniuk. Az Apple ID-val nem rendelkező felhasználók létrehozhatják saját azonosítójukat, mielőtt megkapnák az általuk használt eszközt. A felhasználók a Beállítási asszisztensben is létrehozhatják személyes Apple ID-jukat. A felhasználóknak nincs szükségük hitelkártyára az Apple ID létrehozásához.

További információ a felügyelt Apple ID azonosítókról:

support.apple.com/guide/apple-business-manager

iCloud

Az iClouddal a felhasználók több eszköz között automatikusan szinkronizálhatják és naprakészen tarthatják a dokumentumokat és személyes tartalmakat, például a névjegyzékeket, naptárakat, dokumentumokat és fényképeket. A felhasználók a Lokátor alkalmazással megkereshetik elveszett vagy ellopt Mac gépüket, illetve iPhone, iPad vagy iPod touch készüléküket. Igény szerint letilthatja az iCloud egyes részeit, például az iCloud-kulcskarikát vagy az iCloud Drive-ot. Ez akár az eszközön manuálisan, akár az MDM-megoldáson keresztül is elvégezhető. A szervezetek így hatékonyabban felügyelhetik, hogy milyen adatokat tárolnak az egyes fiókokban.

További információ az iCloud kezeléséről:

support.apple.com/guide/deployment-reference-ios

4. Felügyelet

Ha a felhasználók készülékei használatra készen állnak, számos különféle adminisztratív képesség érhető el az eszközök és tartalmak folyamatos felügyeletéhez és karbantartásához.

Eszközök adminisztrálása

A felügyelt eszközök az MDM-szerveren keresztül is kezelhetők bizonyos műveletekkel. Ilyen például az információk lekérdezése, valamint olyan felügyeleti feladatok futtatása, amelyekkel felügyelheti a szabályzatoknak nem megfelelő, elvesztett vagy elloptott eszközöket.

Lekérdezések

Az MDM-szerverek számos információt tudnak lekérdezni az eszközökről, beleértve az olyan hardverinformációkat, mint például a sorozatszám, vagy az eszköz UDID azonosítója, a Wi-Fi MAC-címe, illetve olyan szoftverinformációkat, mint az iOS- vagy az iPadOS-verzió és az eszközre telepített összes alkalmazás részletes listája. Az információk alapján az MDM-megoldás naprakészen tartja a készlet adatait, megalapozott felügyeleti döntéseket lehet hozni, valamint automatizálni lehet a felügyeleti feladatokat, például az arról való gondoskodást, hogy a felhasználók mindig a megfelelő alkalmazásokat használják.

Felügyeleti feladatok

A felügyelt eszközökön az MDM-szerver az adminisztratív feladatok széles skáláját tudja végrehajtani, beleértve a konfigurációs beállítások automatikus, felhasználói közreműködés nélküli módosítását, a szoftver frissítését jelszóval zárolt eszközökön, az eszközök távoli zárolását vagy törlését, illetve a jelkódos zárolás törlését, hogy a felhasználók új jelszót hozhassanak létre, ha a régi elfelejtették. Az MDM-szerver kérést is küldhet az iPhone-nak vagy az iPadnek, hogy AirPlay-tükrözést indítsanak egy adott célhelyre, vagy hogy leállítsanak egy folyamatban lévő AirPlay-munkamenetet.

Felügyelt szoftverfrissítések

Egy adott ideig megakadályozható, hogy a felhasználók manuálisan vezetéknélküli eszközfrissítést végezzenek a felügyelt eszközökön. Ha ezt a korlátozást alkalmazzák, a késleltetés alapértelmezett ideje 30 nap. A napok számítása onnantól kezdődik, amikor az Apple kiadja az iOS vagy az iPadOS frissítését. Ezenfelül az alapértelmezett 30-ról legfeljebb 90 napra ki is tolható a napok száma a frissítések késleltetéséhez. A felügyelt eszközökön emellett az MDM-megoldással ütemezhetők is a szoftverfrissítések.

Elvesztett mód

Az MDM-megoldással távolról Elvesztett üzemmódba is helyezheti a felügyelt eszközöket. Ez a művelet zárolja az eszközt, és lehetővé teszi egy telefonszám és egy üzenet megjelenítését a zárolási képernyőn. Elvesztett üzemmódban meghatározható az elvesztett vagy elloptott felügyelt eszközök helye, mivel az MDM távolról le tudja kérdezni azt a helyet, ahol az adott eszköz legutóbb csatlakoztatott állapotban volt. Az Elvesztett üzemmód aktiválásához nem szükséges engedélyezni az iPhone keresését.

Aktiválási zár

Az iOS 7.1-es és újabb verziókban az Aktiválási zár engedélyezhető az MDM-mel, ha a felhasználó bekapcsolja a Lokátort egy felügyelt eszközön. Így a szervezet élhet az Aktiválási zár „lopásgátló” funkciójának előnyeivel, ugyanakkor Ön továbbra is megkerülheti a szolgáltatást, ha egy felhasználó nem tudja végrehajtani a hitelesítést az Apple ID-jával.

További tartalmak telepítése és kezelése

A szervezeteknek gyakran van szükségük alkalmazások terjesztésére, hogy lehetővé tegyék a hatékony munkavégzést. Ugyanakkor azt is ellenőrizniük kell, hogyan kapcsolódnak az alkalmazások a belső erőforrásokhoz, vagy hogyan biztosítható az adatok biztonságos kezelése, amikor egy felhasználó elhagyja a vállalatot, és az eszközén a személyes alkalmazásai és adatai mellett vállalati adatok is voltak.

Belső alkalmazásportálok

A legtöbb MDM-szerver tartalmaz egy belső alkalmazásportált. De létrehozhat egy saját belső alkalmazásportált is az alkalmazottak számára, ahol könnyedén megtalálhatják az alkalmazásokat iPhone-jukhoz vagy iPadjükhöz. A vállalaton belüli alkalmazásokra, az App Store-alkalmazások URL-címeire, az Apple Business Manager-kódokra vagy az egyéni alkalmazásokra mutató hivatkozások elhelyezhetők a portálon, így a felhasználók egyetlen központi helyet használhatnak. A portál felügyeletéről és védelméről központilag lehet gondoskodni. A belső alkalmazásportálokon az alkalmazottak könnyebben megtalálhatják a szükséges jóváhagyott erőforrásokat anélkül, hogy az informatikai részleghez kellene fordulniuk.

Felügyelt tartalmak

A felügyelt tartalmak magukban foglalják az App Store-ból származó és az egyéni vállalati alkalmazások, fiókok, könyvek és dokumentumok telepítését, konfigurálását, felügyeletét és eltávolítását.

- **Felügyelt alkalmazások.** Az iOS-ben és az iPadOS-ben az alkalmazásfelügyelettel a szervezetek ingyenes, fizetős és vállalati alkalmazásokat terjeszthetnek vezeték nélküli kapcsolaton keresztül egy MDM-megoldás használatával, miközben fenntarthatják a megfelelő egyensúlyt a vállalati adatok védelme és a felhasználók személyes adatainak tiszteletben tartása között. A felügyelt alkalmazások távolról is eltávolíthatók egy MDM-szerverrel, vagy ha a felhasználó törli a saját eszközét az MDM-ből. Az alkalmazás törlésével a hozzá kapcsolódó adatok is törölődnek. Ha egy alkalmazás az Apple Business Manageren keresztül hozzárendelve marad egy felhasználóhoz, vagy ha a felhasználó beváltott egy alkalmazáskódot a saját Apple ID-jával, az alkalmazás újból letölthető az App Store-ból, de az MDM többé nem fogja felügyelni.
- **Felügyelt fiókok.** Az MDM segítségével a felhasználók automatikusan beállíthatják levelező- és egyéb fiókjaikat, így gyorsan munkához láthatnak. Az MDM-megoldás szolgáltatójától és a belső rendszerekkel való integrációtól függően a fiókcsomag előzetesen is feltölthető a felhasználónevekkel, e-mail-címekkel, illetve (ha alkalmazható) a hitelesítéshez és aláíráshoz tartozó tanúsítványokkal.
- **Felügyelt könyvek és dokumentumok.** Az MDM-eszközök, a könyvek, az ePub-könyvek és a PDF-dokumentumok automatikusan továbbíthatók a felhasználók eszközeire, hogy a szükséges fájlok mindig az alkalmazottak rendelkezésére álljanak. Ugyanakkor a felügyelt könyvek csak más felügyelt alkalmazásokkal oszthatók meg, illetve csak felügyelt fiókokból küldhetők el. Ha pedig többé nincsen szükség a segédletekre, távolról is eltávolíthatók. Az Apple Business Manageren keresztül vásárolt könyvek terjeszthetők a felügyelt könyvterjesztési csatornán keresztül, de nem vonhatók vissza, és nem rendelhetők hozzá máshoz. A felhasználó által már megvásárolt könyvek nem felügyelhetők, hacsak az adott könyvek nincsenek kifejezetten hozzárendelve a felhasználóhoz az Apple Business Manageren keresztül.

Felügyelt alkalmazások konfigurálása

Az alkalmazásfejlesztők megadhatják, hogy a felügyelt alkalmazásként telepített alkalmazások mely beállításait és képességeit kívánják engedélyezni. Ezek a konfigurációs beállítások a felügyelt alkalmazás telepítése előtt vagy után érvényesíthetők. Az informatikai részleg például meghatározhat egy alapértelmezett beállításkészletet egy SharePoint-alkalmazáshoz, hogy a felhasználónak ne kelljen manuálisan megadnia a szerver beállításait.

Az AppConfig-közösség piacvezető, MDM-megoldásokkal foglalkozó szolgáltatói egy olyan szabványos sémát állítottak elő, amelyet az alkalmazásfejlesztők a felügyelt alkalmazások konfigurálásának támogatására használhatnak. Az AppConfig-közösség célja, hogy a mobil operációs rendszerek natív képességeihez biztosítson eszközöket és bevált módszereket. A közösség a mobilalkalmazások konfigurálásának és biztonságossá tételének egységesebb, nyitottabb és egyszerűbb módjával járul hozzá a mobilmegoldások üzleti elterjedéséhez.

További információ az AppConfig-közösségről:

appconfig.org

Felügyelt adatáramlás

Az MDM-megoldások olyan speciális szolgáltatásokat biztosítanak, amelyek lehetővé teszik a vállalati adatok részletes szabályozását, így az adatok nem „szivárognak ki” a felhasználók személyes alkalmazásaiba és felhőszolgáltatásaiba.

- **Felügyelt megnyitási engedélyek.** A megnyitási engedélyek felügyelete olyan korlátozásokat tartalmaz, amelyek megakadályozzák, hogy a felügyelt forrásokból származó mellékletek vagy dokumentumok felügyelet nélküli célhelyeken nyíljanak meg, és fordítva. Megakadályozható például, hogy a cég által felügyelt postafiókban lévő bizalmas e-mail-mellékletet a felhasználók személyes alkalmazásaikban nyissák meg. Ez a munkadokumentum kizárólag MDM-mel telepített és felügyelt alkalmazásokkal nyitható meg. A felhasználó nem felügyelt személyes alkalmazásai nem jelennek meg a melléklet megnyitására elérhető alkalmazások között. A felügyelt alkalmazásokon, fiókokon, könyveken és tartományokon kívül számos bővítmény támogatja a felügyelt megnyitási korlátozásokat.
- **Egyetlen alkalmazás mód.** Ez a beállítás az iOS- vagy az iPadOS-eszközöket egyetlen alkalmazás használatára korlátozza. Ideális megoldás kioszkok vagy csak bizonyos célra használt eszközök, például kiskereskedelmi értékesítési pontok vagy kórházi betegfelvételi eszközök beállításához. Ezt a funkciót a fejlesztők saját alkalmazásaikon belül is engedélyezhetik, így az alkalmazás magától indíthatja és hagyhatja el az Egyetlen alkalmazás módot.
- **Biztonsági mentés megakadályozása.** Ez a korlátozás megakadályozza, hogy a felügyelt alkalmazások biztonsági mentései az iCloudba vagy a számítógépre kerüljenek. Ha le van tiltva a biztonsági mentés, a felügyelt alkalmazásadatokat nem lehet helyreállítani, ha az alkalmazást az MDM törli, majd a felhasználó később újratelepíti.

Támogatási lehetőségek

Az Apple többféle programot és támogatási lehetőséget biztosít az iOS- és az iPadOS-felhasználók és rendszergazdák számára.

AppleCare for Enterprise

A teljes garanciát igénylő vállalatok számára az AppleCare for Enterprise segíthet csökkenteni a belső ügyfélszolgálat terhelését az alkalmazottak számára elérhető napi 24 órás telefonos műszaki támogatással, amely egyórás válaszütemet garantál a kritikus problémák esetében. A program informatikairészség-szintű támogatást biztosít minden Apple-hardverhez és szoftverhez, valamint támogatja az összetett központi telepítési és az integrációs forgatókönyveket, beleértve az MDM és az Active Directory kezelését.

AppleCare operációsrendszer-támogatás

Az AppleCare operációsrendszer-támogatás vállalati szintű telefonos és e-mailes támogatást biztosít az informatikai részleg számára az iOS-, iPadOS-, macOS- és macOS Server-környezetekhez. A megvásárolt támogatási szinttől függően akár a nap 24 órájában elérhető a támogatás és egy kijelölt műszaki ügyfélkapcsolati munkatárs is rendelkezésre állhat. A szakemberek közvetlenül megkereshetők az integrációval és migrálással kapcsolatos kérdésekkel, valamint a speciális szerverüzemeltetési problémákkal kapcsolatban, így az AppleCare operációsrendszer-támogatás növelheti az informatikai csapat hatékonyságát az eszközök üzembe helyezése és felügyelete, valamint a problémák megoldása során.

AppleCare Help Desk ügyféltámogatási szerződés

Az AppleCare Help Desk ügyféltámogatási szolgáltatással elsőbbségi telefonos segítséget kaphat az Apple vezető műszaki támogatási szakembereitől. A szolgáltatás egy eszközcsomagot is biztosít az Apple-hardvereszközök diagnosztizálásához és hibaelhárításához, amellyel a nagyobb szervezetek hatékonyabban felügyelhetik erőforrásaikat, javíthatják válaszütemüket és csökkenthetik a képzési költségeket. Az AppleCare Help Desk ügyféltámogatási szerződés keretében korlátlan számú támogatási kérést lehet leadni hardverek és szoftverek diagnosztizálásához, valamint az iOS- és az iPadOS-készülékek hibaelhárításához és a problémák körülhatárolásához.

AppleCare az iOS- és az iPadOS-eszközök felhasználói számára

Minden iOS- és iPadOS-készülékhez egyéves korlátozott jótállás és a vásárlás időpontjától számított 90 napig ingyenes telefonos műszaki támogatás jár. Az iPhone-ra, iPadre vagy iPod touchra érvényes AppleCare+ csomaggal a szervizgarancia meghosszabbítható a vásárlás napjától számított két évre. Az Apple műszaki támogatási szakemberei telefonon is bármikor válaszolnak a kérdéseire. Az Apple kényelmes szervizelési lehetőségeket is biztosít, ha javításra szorulnak az eszközök. Emellett a csomag két véletlen károsodás megjavítását is fedezi (további szervizdíjak ellenében).

iOS Direct Service Program

Az AppleCare+ részét képező iOS Direct Service Program lehetővé teszi, hogy a szervezet ügyfélszolgálatának anélkül kiszűrje a problémás készülékeket, hogy hívni kellene az AppleCare-t, vagy el kellene látogatni egy Apple Store-ba. A szervezet szükség esetén közvetlenül rendelhet iPhone-, iPad-, iPod touch-csere-készülékeket vagy eredeti tartozékokat.

Információk az AppleCare-programokról:

apple.com/support/professional

Összegzés

Függetlenül attól, hogy a vállalat egy felhasználói csoport vagy a cég minden tagja számára helyez üzembe iPhone-okat vagy iPadeket, számos lehetőség áll a rendelkezésére az eszközök leegyszerűsített üzembe helyezéséhez és felügyeletéhez. A szervezetnek leginkább megfelelő stratégiák kiválasztásával növelhető az alkalmazottak hatékonysága, és új munkamódszerek vezethetők be.

További információ az iOS és az iPadOS üzembe helyezéséről, felügyeletéről és biztonsági funkcióiról:

support.apple.com/guide/deployment-reference-ios

További információ az informatikai részleg számára elérhető moobileszköz-felügyeleti beállításokról:

support.apple.com/guide/mdm

További információ az Apple Business Managerről:

support.apple.com/guide/apple-business-manager

További információ az üzleti felhasználók számára elérhető felügyelt Apple ID azonosítókról:

apple.com/business/docs/site/

[Overview_of_Managed_Apple_IDs_for_Business.pdf](#)

Információk az Apple at Work programról:

www.apple.com/business/

További információ az informatikai funkciókról:

www.apple.com/business/it/

További információ az Apple-platformok biztonságról:

www.apple.com/security/

Az elérhető AppleCare-programok áttekintése:

www.apple.com/support/professional/

Az Apple képzési és tanúsítási programjainak megismerése:

training.apple.com

Kapcsolatfelvétel az Apple szakmai szolgáltatásait nyújtó csapattal:

consultingservices@apple.com

Lehetséges, hogy egyes alkalmazások vagy könyvek az adott országtól vagy régiótól és fejlesztői regisztrációtól függően nem érhetők el. Tekintse meg [a programok és tartalmak elérhetőségét](#). Egyes funkciók használatához Wi-Fi-kapcsolat szükséges. Egyes szolgáltatások nem minden országban érhetők el. Az iCloud minimális és ajánlott rendszerkövetelményei: <https://support.apple.com/HT204230>.

© 2019 Apple Inc. Minden jog fenntartva. Az Apple, az Apple embléma, az AirDrop, az AirPlay, az AirPrint, az Apple TV, a Bonjour, a FaceTime, az iMessage, az iPad, az iPhone, az iPod touch, az iWork, a Mac, a macOS és a Siri az Apple Inc. Az Amerikai Egyesült Államokban és más országokban bejegyzett védjegye. Az iPadOS az Apple Inc. védjegye. Az App Store, az AppleCare, az Apple Store, az Apple Books, az iCloud, az iCloud Drive és az iCloud Keychain az Apple Inc. Az Amerikai Egyesült Államokban és más országokban bejegyzett szolgáltatási védjegye. Az iOS a Cisco védjegye vagy bejegyzett védjegye az Amerikai Egyesült Államokban és más országokban, és a használata a licenctulajdonos beleegyezésével történt. A dokumentumban szereplő további termék- és vállalatnevek az illető vállalatok védjegyei lehetnek. A termékjellemzők előzetes értesítés nélkül megváltozhatnak. Ez az anyag kizárólag a tájékoztatást szolgálja. Az Apple nem vállal felelősséget a használatával kapcsolatban.