Eszközök és vállalati adatok felügyelete iOS rendszeren

Áttekintés

A vállalkozások a világ minden táján iPhone és iPad készülékekkel segítik az alkalmazottak munkáját.

Tartalom

A sikeres mobilstratégia kialakításának fő eleme az informatikai felügyelet és a felhasználói mozgástér egyensúlyának megtalálása. Az iOS-eszközök saját alkalmazásokkal és tartalmakkal való testre szabása révén a felhasználók nagyobb mértékben magukénak érzik a készülékeket, nagyobb felelősséget vállalnak érte, így nő az elkötelezettség és a termelékenység szintje. Mindezt az Apple felügyeleti keretrendszere teszi lehetővé, amely intelligens lehetőségeket kínál a vállalati adatok és alkalmazások elkülönített kezelésére, így zökkenőmentesen különválasztja a munkahelyi és a személyes adatokat. A felhasználók ezenkívül ismerik az eszközök felügyeletének módját, és biztosak lehetnek az adataik védelmében.

Ez a dokumentum arról nyújt útmutatást, hogy miként alakítható ki az alapvető informatikai felügyelet, miközben a felhasználóknak is adottak a munkájukhoz szükséges legjobb eszközök. A dokumentum az iOS üzembe helyezési útmutatót egészíti ki, amely az iOS-eszközök vállalati környezetben történő üzembe helyezését és felügyeletét ismertető, átfogó online műszaki referenciaanyag.

Az iOS üzembe helyezési útmutató a következő címen tekinthető meg: help.apple.com/deployment/ios.

Felügyeleti alapismeretek

iOS rendszeren számos olyan beépített megoldással leegyszerűsíthető az iPhone és az iPad üzembe helyezése, amelyek egyszerűbb fiókbeállítást, házirend-konfigurálást, alkalmazásterjesztést, illetve az eszközkorlátozások távoli alkalmazását teszik lehetővé.

A felügyelet jellege

Az Apple felügyeleti keretrendszere jelenti a mobileszközök felügyeletének alapját. Ez a keretrendszer az iOS részét képezi, így a cégek a szolgáltatások zárolása vagy a funkciók letiltása helyett saját maguk felügyelhetik a szükséges tartalmakat, méghozzá nagyon egyszerűen. Mindennek eredményeként az Apple felügyeleti keretrendszere részletes lehetőségeket kínál az eszközök, alkalmazások és adatok külső fejlesztésű mobileszköz-felügyeleti (Mobile Device Management-, MDM-) megoldásokkal történő szabályozására. A legfontosabb dolog pedig az, hogy a szükséges felügyelet változatlan felhasználói élmény és adatvédelem mellett biztosítható.

A piacon elérhető más eszközfelügyeleti módszerek néha másképp nevezik az MDM-funkciókat, ilyen például az Enterprise Mobility Management (EMM) vagy a Mobile Application Management (MAM). Ezek a megoldások ugyanazt a célt szolgálják: nevezetesen a cég eszközeinek és a

vállalati adatok vezeték nélküli kapcsolaton biztosított felügyeletét. Mivel az Apple felügyeleti keretrendszere az iOS beépített részét képezi, nincs szükség külön ügynökalkalmazás beszerzésére az MDM-megoldás szolgáltatójától.

A munkahelyi és a személyes adatok elkülönítése

Függetlenül attól, hogy a cég a felhasználói vagy a vállalati tulajdonban lévő eszközök használatát támogatja, egyszerre teljesítheti az informatikai felügyeleti célokat és biztosíthatja a felhasználók maximális termelékenységét. A munkahelyi és a személyes adatok kezelése külön történik, de ez a felhasználói élményre nincs hatással. Ez azt jelenti, hogy a legjobb irodai alkalmazások és a vállalat saját alkalmazásai egymás mellett futhatnak az eszközökön, így a felhasználók szabadabban dolgozhatnak. Az iOS mindezt külső féltől származó, a felhasználókat és a felhasználói élményt zavaró megoldások, például tárolók használata nélkül éri el.

A különböző felügyeleti modellek ismertetése

Más platformokon gyakran tárolókkal hárítják el a problémákat – de ezek az akadályok az iOS-en nem jelentkeznek. Egyes tárolók „kettős személyiség" stratégiát használnak, amely ugyanazon az eszközön két környezetet hoz létre. Mások arra helyezik a hangsúlyt, hogy magukat az alkalmazásokat helyezzék tárolóba kódalapú integrációval vagy alkalmazáscsomagoló megoldásokkal. Minden ilyen módszer termelékenységi problémákat okoz a felhasználóknak, legyen az a több munkaterületbe való be- és kijelentkezés, vagy az olyan, saját fejlesztésű kódtól való függés, amely alkalmazáskompatibilitási problémákat okoz az operációs rendszer frissítésekor.

Azok a cégek, amelyek már nem használnak tárolókat, azt tapasztalhatják, hogy az iOS natív felügyeleti vezérlői optimális felhasználói élményt és nagyobb termelékenységet eredményeznek. Ahelyett, hogy megnehezítené a felhasználóknak, hogy munkára és személyes célokra is használják az eszközeiket, olyan házirendeket biztosít, amelyek az adatáramlás zökkenőmentes, háttérben zajló kezelésére szolgálnak.

Vállalati adatok kezelése

Az iOS használatával nem szükséges zárolnia az eszközeit. A kulcsfontosságú technológiák szabályozzák a vállalati adatok alkalmazások közötti áramlását, és megelőzik a felhasználó személyes alkalmazásaiba vagy felhőszolgáltatásokba történő kiszivárgásukat.

Felügyelt tartalmak

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

- **Felügyelt alkalmazások.** Az MDM használatával telepített alkalmazásokat felügyelt alkalmazásoknak hívják. Ezek lehetnek ingyenes vagy fizetős App Store-alkalmazások, vagy egyéni vállalati alkalmazások, amelyek mindegyike MDM használatával vezeték nélkül telepíthető. A felügyelt alkalmazások gyakran tartalmaznak bizalmas adatokat, és nagyobb mértékű szabályozást biztosítanak, mint a felhasználó által letöltött alkalmazások. Az MDM-szerver igény szerint eltávolíthatja a felügyelt alkalmazásokat és a hozzájuk kapcsolódó adatokat, illetve megadhatja, hogy egy alkalmazást a rendszer eltávolítson-e az MDM-profil törlésekor. Az MDM-szerver továbbá megakadályozhatja a felügyelt alkalmazások adatainak biztonsági mentését az iTunesba és az iCloudba.

- **Felügyelt fiókok.** Az MDM segítségével a felhasználók automatikusan beállíthatják a 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 az aláíráshoz tartozó tanúsítványazonosítókkal. Az MDM a következő fióktípusok konfigurálására használható: IMAP/POP, CalDAV, feliratkozott Naptárak, CardDAV, Exchange ActiveSync és LDAP.
- **Felügyelt könyvek.** Az MDM használatával a könyvek, az ePub-könyvek és a PDF-dokumentumok automatikusan továbbíthatók a felhasználók eszközeire, hogy a szükséges fájlok mindig az alkalmazottak rendelkezésére álljanak. A felügyelt könyvek csak más felügyelt alkalmazásokkal oszthatók meg, illetve csak felügyelt fiókokból küldhetők el. Ha pedig többé nincsen szükség a segédanyagokra, távolról is törölhetők.
- **Felügyelt tartományok.** A Safariból letöltött dokumentumok akkor minősülnek felügyelt dokumentumnak, ha felügyelt tartományról származnak. Adott URL-címek és altartományok is felügyelhetők. Ha például a felhasználó egy PDF-fájlt tölt le egy felügyelt tartományról, a tartomány megköveteli, hogy a PDF-fájl megfeleljen a felügyelt dokumentumokra vonatkozó összes beállításnak. A tartományt követő elérési utak felügyelete alapértelmezés szerint engedélyezve van.

Felügyelt terjesztés

A felügyelt terjesztés révén a mennyiségi vásárlási programból (VPP-ből) beszerzett alkalmazások és könyvek az MDM-megoldással vagy az Apple Configurator 2-vel is felügyelhetők. A felügyelt terjesztés engedélyezéséhez először egy biztonságos token segítségével össze kell kapcsolnia az MDM-megoldást a VPP-fiókjával. Miután az MDM-szerver csatlakozott a VPP-hez, az alkalmazások közvetlenül – a felhasználó Apple ID-jának megadása nélkül – az adott eszközökhöz rendelhetők. A rendszer értesíti a felhasználót, amikor az alkalmazások készen állnak az eszközön való telepítésre. Felügyelt eszközök esetén az alkalmazások a felhasználó értesítése nélkül, „csendben” továbbítódnak az adott eszközre.

Az alkalmazások MDM-megoldással való teljes körű vezérléséhez az alkalmazásokat közvetlenül rendelje az eszközökhöz.

Felügyelt alkalmazások konfigurálása

A felügyelt alkalmazások konfigurálása során az MDM az iOS natív felügyeleti keretrendszerével konfigurálja az alkalmazásokat az üzembe helyezés alatt vagy után. A fejlesztők ezzel a keretrendszerrel azonosítani tudják az alkalmazandó konfigurációs beállításokat, ha az

alkalmazásuk felügyelt alkalmazásként van telepítve. Az így konfigurált alkalmazásokat az alkalmazottak azonnal, egyéni beállítások nélkül is használatba vehetik. Az informatikai szakemberek biztosak lehetnek abban, hogy a vállalati adatok alkalmazáson belüli kezelése biztonságosan történik, saját fejlesztésű SDK-k vagy alkalmazáscsomagolási megoldások nélkül.

Az alkalmazásfejlesztők a felügyelt alkalmazások konfigurálásával olyan képességeket vehetnek igénybe, mint például az alkalmazáskonfigurálás, az alkalmazások biztonsági mentésének letiltása, a képernyőfelvétel készítésének letiltása és az alkalmazások távoli törlésének lehetősége.

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

További információk az AppConfig-közösségről: www.appconfig.org.

Felügyelt adatfolyam

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.

  Így megakadályozható például, hogy a cég által felügyelt postafiókban lévő, bizalmas e-mail-mellékletet bármely felhasználó a személyes alkalmazásaiban nyisson 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.

A vállalati adatok védelme érdekében ez a munkadokumentum kizárólag MDM-mel telepített és felügyelt alkalmazásokkal nyitható meg.

- **Felügyelt bővítmények.** Az alkalmazásbővítményekkel a külső fejlesztők funkciókat biztosíthatnak más alkalmazásoknak, vagy akár az iOS-be beépített olyan kulcsfontosságú rendszereknek is, mint például az Értesítési központ, így új üzleti munkafolyamatok hozhatók létre az alkalmazások között. A felügyelt megnyitási engedélyek használatával megakadályozható, hogy a nem felügyelt bővítményfunkciók a felügyelt alkalmazásokkal kommunikáljanak. Az alábbi példákban különböző bővítménytípusokat mutatunk be:
  - A **dokumentumszolgáltatói bővítmények** lehetővé teszik az irodai alkalmazásoknak a számos felhőszolgáltatásból származó dokumentumok megnyitását, így nem kell másolatokat készítenie.
  - A **műveleti bővítmények** segítségével a felhasználók más alkalmazásokban is szerkeszthetnek vagy megtekinthetnek bizonyos tartalmakat. A felhasználók például egy adott művelettel közvetlenül a Safariban fordíthatnak le szövegeket egy másik nyelvre.
  - Az **egyéni billentyűzetbővítmények** az iOS beépített billentyűzetein kívül további billentyűzetek használatát teszik lehetővé. A felügyelt megnyitási engedélyekkel megakadályozható, hogy nem engedélyezett billentyűzetek jelenjenek meg a saját vállalati alkalmazásokban.
  - A **„Ma”-bővítmények** (más néven widgetek) az Értesítési központ Ma nézetében jelenítenek meg könnyen áttekinthető információkat. A felhasználók így azonnali, naprakész adatokhoz jutnak az alkalmazásokból, és további információkért egyszerű műveletekkel elindíthatják a teljes alkalmazást.
  - A **megosztási bővítmények** segítségével a felhasználók kényelmesen megoszthatják tartalmaikat másokkal, például közösségi oldalak vagy fájlfeltöltési szolgáltatások használatával. Ha például az adott alkalmazás egy Megosztás gombot tartalmaz, a felhasználók kiválaszthatják egy közösségi webhely megosztási bővítményét, majd ezzel tehetnek közzé hozzászólásokat vagy egyéb tartalmakat.

Rugalmas felügyeleti lehetőségek

Az Apple felügyeleti keretrendszere rugalmas és kiegyensúlyozott megoldást kínál a felhasználói és a vállalati tulajdonban lévő eszközök cégen belüli kezelésére. Ha külső féltől származó MDM-megoldásokat használ iOS rendszeren, az eszközfelügyeleti beállítások tartománya a nagymértékben nyitott módszerektől a szükséges mértékig részletezett megoldásokig terjed.

Tulajdoni modellek

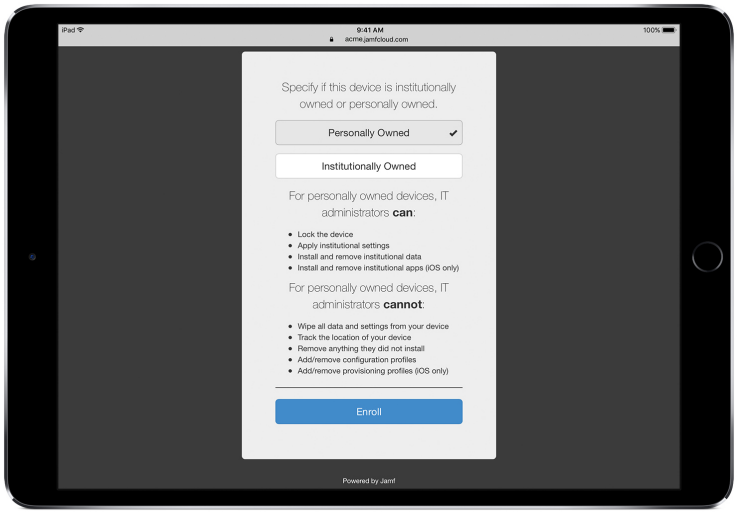
Az adott cég eszköztulajdon-modelljétől (vagy modelljeitől) függően a különböző eszközök és alkalmazások felügyelete eltérő módon történik. A vállalatok által gyakran használt két tulajdoni modell az iOS-ben a vállalati és a felhasználói tulajdonú modell.

Felhasználói tulajdonban lévő eszközök

A felhasználói tulajdonban lévő eszközök üzembe helyezésekor az iOS minden felhasználónak személyre szabott beállítást kínál, átláthatóvá teszi az eszközök konfigurálását, valamint biztosítja, hogy a cég nem fog tudni hozzáférni a felhasználók személyes adataihoz.

- **Kérelmezés- és leiratkozásalapú regisztráció.** Ha az eszközök beszerzését és beállítását a felhasználók végzik – ezt gyakran BYOD-nek nevezik –, Ön továbbra is hozzáférést biztosíthat az olyan vállalati

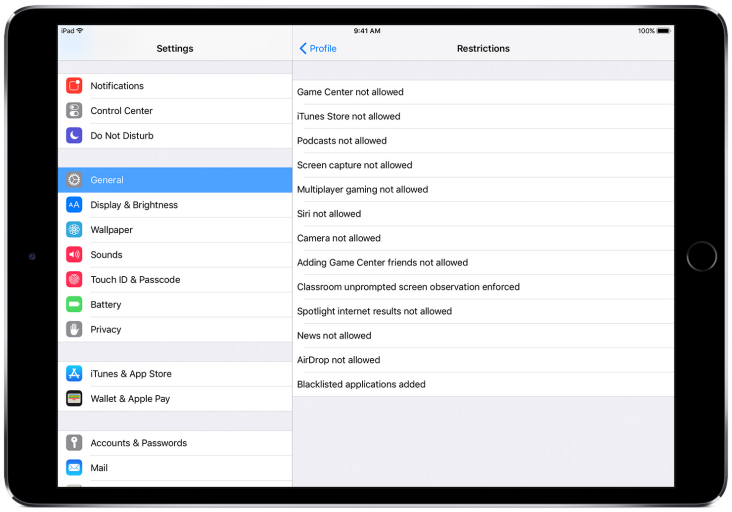
szolgáltatásokhoz, mint például a Wi-Fi, a levelezés és a naptár. A felhasználóknak csak kérelmezniük kell a céges MDM-megoldásra való regisztrációt. Amikor a felhasználók először regisztrálnak az MDM-be egy iOS-eszközön, a rendszer tájékoztatja őket, hogy az MDM-szerver milyen adatokhoz férhet hozzá az eszközükön, és milyen szolgáltatásokat fog konfigurálni. Mindez átláthatóvá teszi a felhasználók számára a felügyelt tartalmakat, és bizalmat épít ki a vállalat és a felhasználók között. A felhasználóknak fontos tudniuk, hogy ha bármikor problémájuk támad a felügyeleti megoldással, visszavonhatják a regisztrációjukat, ha eltávolítják az eszközről a felügyeleti profilt. Ezzel az MDM által telepített összes vállalati fiókot és alkalmazást eltávolítják.



A külső féltől származó MDM-megoldások jellemzően felhasználóbarát felületet biztosítanak az alkalmazottaknak, akik így kényelmesen feliratkozhatnak a regisztráció során.*

*A képernyőfelvétel felhasználása a Jamf engedélyével történt.

- **Nagyobb mértékű átláthatóság.** Ha a felhasználók regisztráltak az MDM-re, a Beállításokban az alkalmazottak egyszerűen megtekinthetik a felügyelt alkalmazásokat, könyveket és fiókokat, illetve az alkalmazott korlátozásokat. Az iOS az MDM által telepített összes vállalati beállítást, fiókot és tartalmat„felügyeltként” jelöli meg.



A Beállításokban, a konfigurációs profilok felhasználói felületén a felhasználók pontosan láthatják az eszközük beállításait.

- **Felhasználói adatok védelme.** Bár az MDM-szerver engedélyezi az iOS-eszközökkel történő kommunikációt, nem minden beállítás és fiókadat jelenik meg. Felügyelheti az MDM-mel létrehozott vállalati fiókokat, beállításokat és adatokat, de a felhasználó személyes fiókjaihoz nem férhet hozzá. Tulajdonképpen ugyanazok a szolgáltatások akadályozzák meg, hogy a felhasználó személyes tartalmai a vállalati adatfolyammal keveredjenek, amelyek a vállalat által felügyelt alkalmazásokban az adatvédelemért felelnek.

  Az alábbi példák azt mutatják be, hogy egy külső féltől származó MDM-szerver számára milyen adatok láthatók és nem láthatók egy személyes iOS-eszközön:

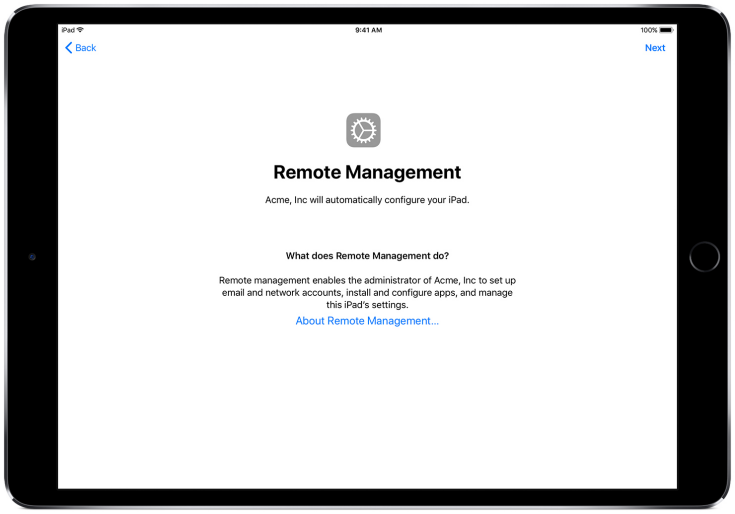
Az MDM számára láthatók a következők:	**Az MDM számára nem láthatók például a következő személyes adatok:**
Eszköz neve	Személyes vagy munkahelyi levelezés, naptárak, névjegyek
Telefonszám	
Sorozatszám	SMS- vagy iMessage-üzenetek
A modell neve és száma	A Safari böngészési előzményei
Tárhelykapacitás és a szabad hely mennyisége	FaceTime- és telefonhívás-naplók
iOS-verziószám	Személyes emlékeztetők és jegyzetek
Telepített alkalmazások	Az alkalmazások használatának gyakorisága
	Az eszköz helye

- **Eszközök személyre szabása.** A vállalkozások felismerték, hogy ha engedélyezik a felhasználóknak az eszközeik testreszabását a saját Apple ID azonosítóikkal, akkor a felhasználók nagyobb mértékben magukénak érzik a készülékeket, nagyobb felelősséget vállalnak érte, így nő az elkötelezettség és a termelékenység szintje.

Céges tulajdonban lévő eszközök

Céges tulajdonban lévő eszközök üzembe helyezése esetén minden felhasználónak biztosíthat egy eszközt – ezt személyre szabott központi telepítésnek nevezik –, vagy pedig a felhasználók cserélgethetik az eszközöket – ez a nem személyre szabott központi telepítés. Az olyan iOS-szolgáltatások, mint például az automatikus regisztráció, a zárolható MDM-beállítások, az eszközfelügyelet vagy a mindig működő VPN biztosítják, hogy az eszközök a cég konkrét követelményei szerint legyenek konfigurálva. Mindez nagyobb mértékű szabályozást biztosít a vállalati adatok védelme mellett.

- **Automatikus regisztráció.** A Készülékregisztrációs program (DEP) segítségével a céges tulajdonban lévő iPhone-ok, iPadek és Mac gépek üzembe helyezésekor automatizálható az MDM-regisztráció. A regisztráció kötelezővé és nem visszavonhatóvá is tehető. A regisztráció során az eszközöket felügyelt üzemmódba is helyezheti, így a felhasználók egyes alapszintű beállítási lépéseket kihagyhatnak.



A DEP használata esetén az MDM-megoldás automatikusan konfigurálja az iOS-eszközöket a Beállítási asszisztens használatakor.

- **Felügyelt eszközök.** Felügyelt üzemmódban további felügyeleti lehetőségek állnak rendelkezésre a céges tulajdonban lévő iOS-eszközökhöz. Ezek közé tartozik a webes szűrők engedélyezése egy globális proxyn keresztül, így többek között biztosítható, hogy a felhasználói internetes adatforgalom megfeleljen a cég irányelveinek, illetve megakadályozható, hogy a felhasználók alaphelyzetbe állítsák az eszközöket. Alapértelmezés szerint az összes iOS-eszköz nem felügyeltként van beállítva. A felügyelt üzemmód nemcsak a DEP használatával, hanem manuálisan is engedélyezhető az Apple Configurator 2-vel.

Még ha jelenleg nem is tervezi csak felügyelt szolgáltatások használatát, akkor is fontolja meg az eszközök üzembe helyezésekor a felügyelet beállítását, mivel így a jövőben kihasználhatja az ilyen szolgáltatások előnyeit. Ellenkező esetben törölnie kell majd a már üzembe helyezett eszközöket. A felügyelet nem az eszközök zárolását jelenti, sőt a felügyeleti képességek kiterjesztésével a vállalati tulajdonban lévő eszközök még hatékonyabban használhatók. Hosszabb távon az eszközök felügyelete további lehetőségeket nyit meg a vállalata számára.

A felügyelt beállítások teljes listáját lásd az iOS üzembe helyezési útmutatóban.

Korlátozások

Az iOS az alábbi korlátozási kategóriákat támogatja, amelyeket vezeték nélkül konfigurálhat a céges igényeknek megfelelően, a felhasználói élményre gyakorolt hatás nélkül:

- AirPrint
- Alkalmazások telepítése
- Alkalmazáshasználat
- Osztályterem alkalmazás
- Eszköz
- iCloud
- A profilkezelő felhasználóira és felhasználói csoportjaira érvényes korlátozások
- Safari
- Biztonsági és adatvédelmi beállítások
- Siri

Az alábbi kategóriáknak szintén vannak olyan beállítási lehetőségei, amelyek az MDM-megoldással konfigurálhatók:

- Automatikus MDM-regisztrációs beállítások
- A Beállítási asszisztens képernyői

További felügyeleti képességek

Eszközök lekérdezése

Az eszközök beállításának lehetőségén túl az MDM-szerver különféle információkat is le tud kérdezni az eszközökről, például az eszközök, a hálózat, az alkalmazások, illetve a megfelelőségi és biztonsági adatok részleteit. Ezekkel az információkkal biztosítható, hogy az eszközök továbbra is megfeleljenek az előírt házirendeknek. Az MDM-szerver határozza meg az információgyűjtés gyakoriságát.

Példák az iOS-eszközökről lekérdezhető információkra:

- Eszközadatok (név)
- Modellszám, iOS-verzió, sorozatszám
- Hálózati információk
- Barangolási állapot, MAC-címek
- Telepített alkalmazások
- Alkalmazás neve, verziószáma, mérete
- Megfelelőségi és biztonsági adatok
- Telepített beállítások, házirendek, tanúsítványok
- Titkosítási állapot

Felügyeleti feladatok

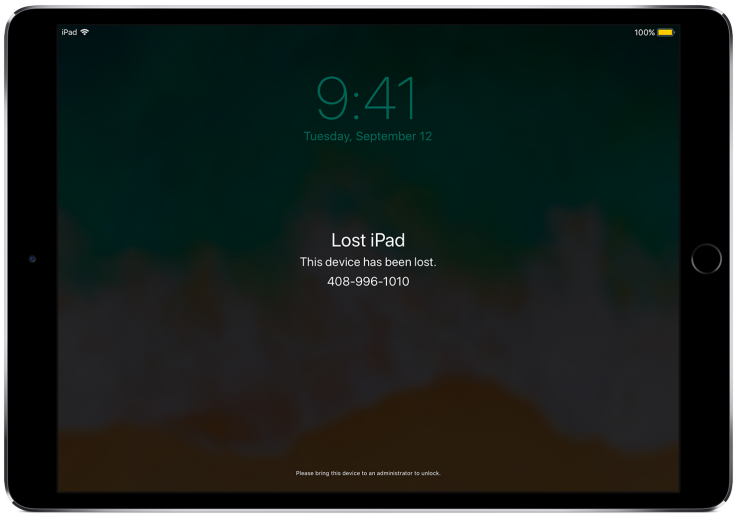
A felügyelt eszközökön az MDM-szerver az adminisztratív feladatok széles skáláját tudja végrehajtani, beleértve a konfigurációs beállítások automatikus módosítását felhasználói közreműködés nélkül, az iOS frissítését jelszóval zárolt eszközökön, az eszközök távoli zárolását vagy törlését, illetve a jelszavas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

Elveszett üzemmód

Az iOS 9.3-as vagy újabb verzióiban az MDM-megoldással távolról Elveszett üzemmódba is helyezheti a felügyelt eszközöket. Ez a művelet zárolja az eszközt, és lehetővé teszi egy telefonszám és egy üzenet megjelenítését a zárolási képernyőn.

Elveszett üzemmódban meghatározható az elveszett vagy ellopott felügyelt eszközök helye, mivel az MDM távolról le tudja kérdezni azt a helyet, ahol az adott eszköz legutóbb csatlakoztatott állapotban volt. Az Elveszett üzemmód aktiválásához nem szükséges engedélyezni az iPhone keresése szolgáltatást.

Ha az MDM távolról letiltja az Elveszett üzemmódot, az eszköz zárolása feloldódik, és a rendszer begyűjti a helyadatait. Az átláthatóság fenntartása érdekében a rendszer értesíti a felhasználót, hogy az Elveszett üzemmód ki van kapcsolva.



Amikor az MDM Elveszett üzemmódba helyez egy elveszett eszközt, akkor zárolja a készüléket, lehetővé teszi üzenetek megjelenítését a képernyőjén, valamint azonosítja a helyét.

Aktivációs zár

Az iOS 7.1-es és újabb verzióiban az aktivációs zár engedélyezhető az MDM-mel, ha a felhasználó bekapcsolja az iPhone keresése szolgáltatást egy felügyelt eszközön. Így a cég élhet az aktivációs zár „lopásgátló” funkciójának előnyeivel, ugyanakkor Ön továbbra is megkerülheti a szolgáltatást, ha például egy felhasználó a cégből való kilépés előtt nem távolította el az aktivációs zárat a saját Apple ID-jával.

Az MDM-megoldással a következőképpen lehívható a megkerülési kód, és engedélyezhető a felhasználónak az aktivációs zár használatának engedélyezése:

- Ha az iPhone keresése szolgáltatás be van kapcsolva, miközben az MDM-megoldásban engedélyezve van az aktivációs zár, akkor az aktivációs zár működésbe lép.
- Ha az iPhone keresése szolgáltatás ki van kapcsolva, miközben az MDM-megoldásban engedélyezve van az aktivációs zár, az aktivációs zár akkor lép működésbe, amikor a felhasználó legközelebb bekapcsolja az iPhone keresése szolgáltatást.

Összefoglalás

Az iOS felügyeleti keretrendszere a legjobb funkciókat ötvözi: az informatikai részleg konfigurálhatja, felügyelheti és megvédheti az eszközöket, valamint szabályozhatja a rajtuk áthaladó vállalati adatokat, ugyanakkor a felhasználóknak továbbra is lehetőségük nyílik a kedvenc eszközeik hatékony munkavégzéshez történő használatára.