Az üzleti célra szánt felügyelt Apple ID azonosítók áttekintése

Az Apple-termékeket használó cégekben és szervezetekben fontos megérteni, hogy a felügyelt Apple ID-k hogyan támogatják azoknak a szolgáltatásoknak az igénybe vételét, amelyekre az alkalmazottaknak szüksége lehet. A felügyelt Apple ID azonosítók kimondottan üzleti célra készült fiókok, amelyek hozzáférést biztosítanak az Apple legfontosabb szolgáltatásaihoz.

A cégek és szervezetek az Apple Business Managerrel automatikusan hozhatnak létre felügyelt Apple ID-kat az alkalmazottaiknak, hogy azok közösen dolgozhassanak az Apple-alkalmazásokban és -szolgáltatásokban, és hozzáférhessenek az iCloud Drive-ot használó felügyelt alkalmazásokban található vállalati adatokhoz. Az összevont hitelesítésnek köszönhetően ezek a fiókok ugyanazokat a hitelesítő adatokat használják, mint a szervezet által birtokolt és felügyelt, már kiépített infrastruktúra.

Mik a felügyelt Apple ID-k?

A többi Apple ID azonosítóhoz hasonlóan a felügyelt Apple ID-k is az eszközök testreszabására valók. Emellett az Apple-alkalmazások és -szolgáltatások elérésére is használhatók, illetve arra, hogy az informatikai csapatok hozzáférhessenek az Apple Business Managerhez. Az Apple ID azonosítóktól eltérően a felügyelt Apple ID-kat cégek vagy szervezetek birtokolják és kezelik, beleértve a jelszó-visszaállításokat és a szerepköralapú felügyeletet.

Az Apple Business Managerrel egyedi felügyelt Apple ID-kat lehet létrehozni egy cég vagy szervezet minden alkalmazottjához. Mivel integrálva vannak a Microsoft Azure Active Directoryval, a szervezetek úgy bocsáthatnak felügyelt Apple ID-kat az alkalmazottaik rendelkezésére, hogy azok továbbra is meglévő vállalati hitelesítő adataikat használják.

A felügyelt Apple ID-kat a személyes Apple ID azonosítók mellett lehet beállítani az alkalmazottak saját tulajdonában lévő eszközökön, ha a szervezetek Felhasználói regisztrációt alkalmaznak iOS-en, iPadOS-en vagy macOS Catalinán. 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.

Nincs semmilyen technikai előfeltétele a készülékek Apple ID segítségével történő központi telepítésének. Az Apple-eszközök Apple ID azonosító nélkül is felügyelhetők, és az alkalmazások anélkül is kioszthatók az eszközökre. Gondolja át, hogy a szervezet mely Apple-szolgáltatásokat kívánja majd igénybe venni, és ez alapján határozza meg, hogy melyik a legjobb módja a felügyelt Apple ID-kra való áttérésnek. Mivel a felügyelt Apple ID-k kizárólag üzleti célra szolgálnak, a cégek vagy szervezetek védelme érdekében bizonyos funkciók le vannak tiltva.

Szervezeti funkciók

- **Hozzáférés az Apple szolgáltatásaihoz.** Az alkalmazottak használhatják az Apple szolgáltatásait, például az iCloudot, vagy az iWork és a Jegyzetek együttműködési funkcióit. A levelezés le van tiltva, és a FaceTime és az iMessage csak akkor használható, ha a felügyelt Apple ID az eszköz egyetlen Apple ID-ja.
- **Felhasználói fiók keresése.** Az alkalmazottak kikereshetik az Apple Business Managert használó cég vagy szervezet többi felhasználójának kapcsolati adatait, így könnyebben működhetnek együtt különböző alkalmazásokban.
- **Leegyszerűsített fióklétrehozás.** Az Apple Business Managerben automatikusan létrejön a fiók, amikor az alkalmazottak először jelentkeznek be egy Apple-eszközre.
- **Összevont hitelesítés.** A rendszergazdák összekapcsolhatják az Apple Business Managert a Microsoft Azure Active Directoryval, hogy az alkalmazottak beállítása automatikusan megtörténjen a meglévő vállalati hitelesítő adatokkal.
- **Szerepkörök és jogosultságok.** A rendszergazdák az Apple Business Manager különböző funkcióit magukban foglaló szerepköröket és jogosultságokat hozhatnak létre és rendelhetnek az informatikai csapatokhoz.
- **Beépített adatvédelem és biztonság.** A felügyelt Apple ID-k ugyanolyan adattitkosítási védelmet használnak, mint a szabványos Apple ID azonosítók, és le van tiltva, hogy az Apple hirdetési platformján keresztül célzott hirdetéseket kapjanak. A kereskedelmi jellegű és olyan szolgáltatások hozzáférése is le van tiltva, mint például az Apple Pay vagy a Wallet. Az eszközkeresés sem engedélyezett, mert a szervezetek használhatják az Elveszett módot az MDM-en keresztül.

Összevont hitelesítés

Az összevont hitelesítés lehetővé teszi az Apple Business Manager és a Microsoft Active Directory (Azure AD) összekapcsolását, így az alkalmazottak a meglévő felhasználónevüket és jelszavukat használhatják felügyelt Apple ID azonosítóként.

A Microsoft Azure AD lesz az identitásszolgáltató, amely tartalmazza az Apple Business Managerrel használni kívánt fiókok felhasználónevét és jelszavát.

A Microsoft Azure AD-integráció miatt a felügyelt Apple ID-kra pontosan ugyanazok a jelszószabályzatok vonatkoznak, mert meglévő hitelesítő adatokkal vannak összevonva.

Amikor a felhasználók bejelentkeznek az Apple-eszközre, automatikusan létrejönnek a felügyelt Apple ID-k, így a rendszergazdáknak nem kell időt fordítaniuk az előkészítésre.

Az alkalmazottak meglévő Azure AD hitelesítő adataikat használhatják az Apple-szolgáltatások, például az iCloud Drive, a Jegyzetek, az Emlékeztetők és az együttműködési funkciók használatához.

Mivel már a szervezet kezében van az identitás felügyelete, a szervezet vagy a felhasználó az összes jelszószabályzatot és -visszaállítást a Microsoft Azure AD-ben kezeli.

Mire van szükség az összevont hitelesítés használatához

- **Microsoft Azure Active Directoryra.** Ha már rendelkezik vele, nekivághat az összevont hitelesítésnek.
- **Helyszíni Active Directoryra.** Az Azure AD-vel való szinkronizáláshoz további beállítási lépéseket kell végrehajtani. A Microsoft dokumentációt és szinkronizálási eszközt is biztosít, amelyek hivatkozása alább található.

Az összevont hitelesítés beállítása

1. **Ellenőrizze a tartományt az Apple részéről**. Jelentkezzen be az Apple Business Managerbe rendszergazdaként vagy személykezelőként, és adja meg az összevonni kívánt tartomány(oka)t.
2. **Csatlakozzon a Microsoft Azure Active Directoryhoz, és biztosítson hozzáférést az Apple Business Managernek.** Globális rendszergazdai vagy alkalmazás-rendszergazdai fiókkal jelentkezzen be az Azure AD-be, és engedélyezze, hogy az Apple Business Manager olvashassa a felhasználói profilokat.
3. **Ellenőrizze a tartomány tulajdonjogát a Microsoft Azure Active Directory részéről.** A megbízhatóság ellenőrzése után folytassa a tartomány(ok) ellenőrzésének folyamatát. Az Apple Business Managerből jelentkezzen be a Microsoft Azure AD-be egy olyan fiókkal, amely az összevonni kívánt tartományra végződik. Ez a lépés ellenőrzi a tartomány beállítását, és igazolja a tulajdonjogot.
4. **Ellenőrizze a tartomány(ok) esetleges ütközéseit.** Az Apple Business Manager ellenőrzi, vannak-e ütközések a tartomány(ok) meglévő Apple ID azonosítóival. Az ütköző azonosítók személyes vagy felügyelt Apple ID-k lehetnek, amelyeket egy másik szervezet állított be ugyanazzal a tartománnyal.
5. **Kezdeményezze az ütköző tartományok jelentette probléma feloldását**. Ha az Apple Business Manager személyes Apple ID-kat észlel az összevonni kívánt tartomány(ok)ban, értesíti az érintett felhasználókat, akiknek módosítaniuk kell az Apple ID-hoz tartozó e-mail-címüket. A vásárlások és az adatok továbbra is a felhasználó személyes Apple ID-jához kapcsolódnak majd.
6. **Telepítse át a már létező fiókokat.** Ha vannak meglévő felügyelt Apple ID-k, ezeket áttelepítheti az összevont hitelesítésbe, ha módosítja az adataikat, hogy megegyezzenek az összevont tartománnyal és felhasználónévvel.

Segédletek

- Az Apple Business Manager használatának első lépéseit ismertető útmutató
- Apple Business Manager felhasználói útmutató
- Felügyelt Apple ID-k létrehozása az Apple Business Managerben
- Az összevont hitelesítés Apple Business Managerrel való használatának bemutatása
- További információk a meglévő Apple ID azonosítókkal fennálló ütközésekről
- További információk a helyszíni AD és az Azure AD integrálásáról