Overzicht beheerde Apple ID's voor bedrijven

Wanneer uw organisatie Apple producten gebruikt, is het belangrijk te weten hoe beheerde Apple ID's de voorzieningen ondersteunen die uw werknemers nodig hebben. Beheerde Apple ID's zijn accounts voor bedrijven die toegang bieden tot essentiële Apple voorzieningen.

Organisaties kunnen Apple Business Manager gebruiken om automatisch beheerde Apple ID's te maken voor werknemers die samenwerken via apps en voorzieningen van Apple en die gegevens benaderen in beheerde apps die gebruikmaken van iCloud Drive. Met gebundelde authenticatie gebruiken deze accounts dezelfde referenties als de bestaande infrastructuur in eigendom en beheer van de organisatie.

Wat zijn beheerde Apple ID's?

Net als andere Apple ID's worden beheerde Apple ID's gebruikt om een device te personaliseren. Ze worden ook gebruikt voor toegang tot apps en voorzieningen van Apple, en om IT-teams de mogelijkheid te bieden Apple Business Manager te gebruiken. Anders dan gewone Apple ID's zijn beheerde Apple ID's eigendom van de organisatie en worden ze door de organisatie beheerd – inclusief wachtwoordherstel en beheer op basis van rollen.

Met Apple Business Manager maakt u voor elke werknemer moeiteloos een beheerde Apple ID. Dankzij de integratie met Microsoft Azure Active Directory kunnen organisaties werknemers voorzien van beheerde Apple ID's op basis van bestaande bedrijfsreferenties.

Als organisaties gebruikmaken van gebruikersinschrijving op iOS, iPadOS en macOS Catalina, kunnen beheerde Apple ID's naast een persoonlijke Apple ID worden gebruikt op eigen devices van werknemers. Beheerde Apple ID's kunnen ook op elk device worden gebruikt als primaire (en enige) Apple ID. Beheerde Apple ID's hebben ook toegang tot iCloud op het web, na de eerste aanmelding op een Apple device.

Er zijn geen technische redenen om devices met een Apple ID te implementeren. Ook zonder Apple ID kunnen Apple devices worden beheerd en kunnen apps worden gedistribueerd. Bedenk welke voorzieningen uw organisatie wil gebruiken en bepaal op grond daarvan het beste traject voor de overstap op beheerde Apple ID's. Beheerde Apple ID's zijn bedoeld voor zakelijk gebruik, dus bepaalde features zijn uitgeschakeld om organisaties te beschermen.

Features voor organisaties

- **Toegang tot Apple voorzieningen.** Werknemers kunnen Apple voorzieningen gebruiken, zoals iCloud en samenwerken met iWork en Notities. E-mail is uitgeschakeld en FaceTime of iMessage zijn alleen beschikbaar wanneer een beheerde Apple ID de enige Apple ID op een device is.
- **Gebruikersaccounts opzoeken.** Bied werknemers de mogelijkheid naar contactgegevens van andere gebruikers in uw Apple Business Manager-organisatie te zoeken. Zo maakt u samenwerking in verschillende apps gemakkelijker.
- **Gestroomlijnd accounts aanmaken.** Met Apple Business Manager worden er automatisch accounts aangemaakt wanneer werknemers zich voor de eerste keer aanmelden bij een Apple device.
- **Gebundelde authenticatie.** Beheerders kunnen Apple Business Manager koppelen aan Microsoft Azure AD zodat werknemers automatisch worden geconfigureerd met bestaande bedrijfsreferenties.
- **Rollen en rechten.** Beheerders kunnen rollen en rechten voor IT-teams instellen voor het gebruik van verschillende functies in Apple Business Manager.
- **Ingebouwde privacy en beveiliging.** Beheerde Apple ID's gebruiken dezelfde encryptiebeveiliging als gewone Apple ID's en worden afgeschermd tegen gerichte reclame op het reclameplatform van Apple. Online kopen is uitgeschakeld, net als voorzieningen als Apple Pay en Wallet. 'Zoek mijn' is uitgeschakeld, aangezien organisaties de Verloren-modus kunnen gebruiken met MDM.

Gebundelde authenticatie

Met gebundelde authenticatie kunt u Apple Business Manager koppelen met Microsoft Azure AD, zodat werknemers hun bestaande gebruikersnaam en wachtwoord kunnen gebruiken als beheerde Apple ID.

Microsoft Azure AD fungeert als identiteitsprovider (IdP) en bevat alle gebruikersnamen en wachtwoorden van de accounts die u wilt gebruiken met Apple Business Manager.

Door de integratie met Microsoft Azure AD volgen beheerde Apple ID's dezelfde regels voor wachtwoordbeleid, aangezien ze gebundeld zijn met bestaande inloggegevens.

Beheerde Apple ID's worden automatisch aangemaakt zodra een gebruiker zich aanmeldt bij zijn Apple device, dus IT-beheerders zijn geen tijd kwijt aan het vooraf aanmaken van deze ID's.

De werknemers kunnen vervolgens hun bestaande Azure AD-referenties gebruiken voor toegang tot Apple voorzieningen zoals iCloud Drive, Notities, Herinneringen en samenwerking.

Aangezien de organisatie de identiteit al beheert, worden wachtwoordbeleid en wachtwoordherstel door de organisatie of gebruiker geregeld in Microsoft Azure AD.

Vereisten gebundelde authenticatie

- **Microsoft Azure Active Directory.** Als u hier al gebruik van maakt, kunt u aan de slag met gebundelde authenticatie.
- **Lokale Active Directory.** Er zijn extra configuratiestappen die met Azure AD gesynchroniseerd moeten worden. Microsoft heeft documentatie en een hulpprogramma voor synchronisatie. U vindt de betreffende links hieronder.

Gebundelde authenticatie instellen

1. **Domein verifiëren bij Apple**. Meld u aan als beheerder of personenmanager bij Apple Business Manager en voeg een of meerdere domeinen toe die u wilt bundelen.
2. **Verbinding maken met Microsoft Azure AD en toegang verlenen aan Apple Business Manager.** Gebruik de account van een globale beheerder of een toepassingsbeheerder om u aan te melden bij Azure AD en accepteer de machtigingen zodat wordt toegestaan dat Apple Business Manager gebruikersprofielen leest.
3. **Het domeineigendom bevestigen bij Microsoft Azure AD.** Als de vertrouwensrelatie tot stand is gebracht, kunt u verder met het bevestigen van het domein of de domeinen. Meld u vanuit Apple Business Manager aan bij Microsoft Azure AD met een account die eindigt met het domein dat u wilt bundelen. Met deze stap wordt de domeininstallatie bevestigd en het eigendom bewezen.
4. **Controleren op domeinconflicten.** Apple Business Manager controleert of er conflicten zijn met bestaande Apple ID's in uw domein(en). Het kan hier gaan om persoonlijke Apple ID's of beheerde Apple ID's die met hetzelfde domein zijn ingesteld door een andere organisatie.
5. **Oplossing van domeinconflict starten**. Als Apple Business Manager een persoonlijke Apple ID aantreft in een domein dat gebundeld moet worden, worden deze gebruikers op de hoogte gesteld en moeten zij het e-mailadres voor hun Apple ID veranderen. Alle aankopen en gegevens blijven gekoppeld aan de persoonlijke Apple ID van de gebruiker.
6. **Bestaande accounts migreren.** U kunt bestaande beheerde Apple ID's overzetten naar gebundelde authenticatie door de gegevens ervan zo te wijzigen dat ze overeenkomen met het gebundelde domein en de bijbehorende gebruikersnaam.

Informatiebronnen

- Basishandleiding Apple Business Manager
- Gebruikershandleiding Apple Business Manager
- Meer informatie over het aanmaken van beheerde Apple ID's in Apple Business Manager
- Inleiding tot gebundelde authenticatie met Apple Business Manager
- Meer informatie over conflicten met bestaande Apple ID's
- Meer informatie over integratie van on-premises AD met Azure AD