



Overblik over administrerede Apple-id'er til erhverv

Når I bruger Apple-produkter i jeres organisation, er det vigtigt at have en forståelse for, hvordan administrerede Apple-id'er anvendes til de tjenester, som medarbejdere har behov for. Administrerede Apple-id'er er konti, der er beregnet specifikt til virksomheder, som giver adgang til vigtige Apple-tjenester.

Organisationer kan bruge Apple Business Manager til automatisk at oprette administrerede Apple-id'er for medarbejdere, så de kan samarbejde med Apple-apps og -tjenester samt få adgang til virksomhedsdata i administrerede apps, der bruger iCloud Drive. Med godkendelse fra organisationsnetværket bruger disse konti de samme brugeroplysninger som den eksisterende infrastruktur, der ejes og administreres af den enkelte organisation.

Hvad er administrerede Apple-id'er?

Som med ethvert Apple-id bruges administrerede Apple-id'er til at tilpasse en enhed. De bruges også til at få adgang til Apple-apps og -tjenester, og de giver IT-afdelinger adgang til Apple Business Manager. I modsætning til Apple-id'er er administrerede Apple-id'er ejet og administreret af den enkelte organisation. Dette gælder også for nulstilling af adgangskoder og rollebaseret administration.

Apple Business Manager gør det nemt at skabe et unikt administreret Apple-id for hver medarbejder i en organisation. På grund af integration med Microsoft Azure Active Directory kan organisationer forsyne medarbejderne med administrerede Apple-id'er ved hjælp af deres virksomhedsbrugeroplysninger.

Administrerede Apple-id'er kan bruges sammen med et personligt Apple-id på enheder, der ejes af medarbejderne, når organisationer udnytter brugertilmelding i iOS, iPadOS og macOS Catalina. Som alternativ kan administrerede Apple-id'er bruges på hvilken som helst enhed som det primære – og eneste – Apple-id. Administrerede Apple-id'er har også adgang til iCloud på internettet efter at have logget ind på en Apple-enhed for første gang.

Der er ikke noget teknisk krav om at implementere enheder med et Apple-id. Apple-enheder kan administreres, og apps og programmer kan distribueres til enheder uden et Apple-id. Gennemgå de tjenester, som jeres organisation har tænkt sig at benytte, og vurder, hvordan I bedst kan overgå til administrerede Apple-id'er. Da administrerede Apple-id'er kun er til virksomhedsformål, bliver visse funktioner deaktiveret for at beskytte hver organisation.

Funktioner for organisationer

- **Adgang til Apple-tjenester.** Medarbejdere kan bruge Apple-tjenester, herunder iCloud, og samarbejde med iWork og Noter. Mail er deaktiveret, og brugen af FaceTime eller iMessage er kun tilgængelig, når et administreret Apple-id er det eneste Apple-id på en enhed.
- **Søgning efter brugerkonto.** Giver medarbejdere mulighed for at søge efter andre brugeres kontaktoplysninger i jeres Apple Business Manager-organisation, så det er lettere for medarbejdere at samarbejde med hinanden på tværs af apps og programmer.
- **Ensartet kundeoprettelse.** Med Apple Business Manager bliver konti oprettet automatisk, når medarbejdere logger ind på en Apple-enhed for første gang.
- **Godkendelse fra organisationsnetværket.** Administratorer kan forbinde Apple Business Manager med Microsoft Azure Active Directory, så deres medarbejdere opsættes automatisk ved hjælp af deres eksisterende virksomhedsbrugeroplysninger.
- **Roller og rettigheder.** Administratorer kan skabe og tildele roller og rettigheder, så IT-afdelinger kan bruge forskellige funktioner i Apple Business Manager.
- **Indbygget anonymitet og sikkerhed.** Administrerede Apple-id'er bruger de samme datakrypteringsbeskyttelser som almindelige Apple-id'er og blokeres mod målrettede reklamer på Apples reklameplatform. Handel er deaktiveret, og det samme er adgangen til tjenester som Apple Pay og Wallet. Find min er deaktiveret, fordi organisationer kan bruge funktionen Mistet ved hjælp af MDM.

Godkendelse fra organisationsnetværket

Med godkendelse fra organisationsnetværket kan du forbinde Apple Business Manager til Microsoft Azure Active Directory (Azure AD), så medarbejdere kan bruge deres eksisterende brugernavne og adgangskoder som administrerede Apple-id'er.

Microsoft Azure AD er identitetsudbyderen (IdP), som indeholder brugernavnene og adgangskoderne for de konti, du vil bruge med Apple Business Manager.

Når de integreres med Microsoft Azure AD, følger administrerede Apple-id'er de helt samme regler for adgangskoder, fordi de er forenet med eksisterende brugeroplysninger.

Administrerede Apple-id'er oprettes automatisk, når brugerne logger ind på deres Apple-enheder, så IT-administratorerne slipper for at skulle oprette alt på forhånd.

Derefter kan medarbejdere bruge deres eksisterende Azure AD-brugeroplysninger til at få adgang til Apple-tjenester, herunder iCloud Drive, Noter, Påmindelser og samarbejde.

Eftersom organisationen allerede administrerer identiteten, bliver alle regler for adgangskoder og nulstillinger håndteret af organisationen eller brugeren i Microsoft Azure AD.

Krav til Godkendelse fra organisationsnetværket

- **Microsoft Azure Active Directory.** Kom i gang med godkendelse fra organisationsnetværket, hvis du allerede har dette på plads.
- **Active Directory i det lokale miljø.** Der er yderligere opsætningstrin for at synkronisere med Azure AD. Microsoft tilbyder dokumentation om dette og et synkroniseringsværktøj via nedenstående link.

Ressourcer

- [Kom godt i gang – Apple Business Manager](#)
- [Brugervejledning til Apple Business Manager](#)
- [Læs mere om at oprette administrerede Apple-id'er i Apple Business Manager](#)
- [Introduktion til godkendelse fra organisationsnetværket med Apple Business Manager](#)
- [Læs mere om konflikter med eksisterende Apple-id'er](#)
- [Læs mere om at integrere AD i det lokale miljø med Azure AD](#)

Opsætning af godkendelse fra organisationsnetværket

1. **Bekræft domæne med Apple.** Log ind på Apple Business Manager som en Administrator eller Personleadadministrator, og tilføj de(t) domæne(r), du vil forbinde.
2. **Opret forbindelse til Microsoft Azure Active Directory, og tildel adgang til Apple Business Manager.** Brug en konto som Global administrator eller Programadministrator til at logge ind på Azure AD og acceptere tilladelser til at lade Apple Business Manager læse brugerprofiler.
3. **Bekræft domæneejerskab med Microsoft Azure Active Directory.** Fortsæt processen med at bekræfte domæne(r), når tilliden er oprettet. Log ind på Microsoft Azure AD fra Apple Business Manager med en konto, der ender med det domæne, du har til hensigt at forbinde. Dette trin bekræfter domæneopsætning og beviser ejerskab.
4. **Tjek for domænekonflikter.** Apple Business Manager tjekker for potentielle konflikter med eksisterende Apple-id'er i jeres domæne(r). Disse kan være personlige Apple-id'er eller administrerede Apple-id'er, der er opsat af en anden organisation med det samme domæne.
5. **Påbegynd løsning af domænekonflikter.** Hvis Apple Business Manager registrerer et personligt Apple-id i de(t) domæne(r), du har til hensigt at forbinde, vil disse brugere få besked og skal ændre mailadresserne for deres Apple-id'er. Alle køb og data forbliver tilknyttet brugerens personlige Apple-id.
6. **Overfør allerede eksisterende konti.** Hvis du har eksisterende administrerede Apple-id'er, kan du overføre dem til godkendelse fra organisationsnetværket ved at ændre oplysningerne, så de svarer til det forenede domæne og brugernavn.