Oversikt over administrerte Apple ID-er for bedrifter

Når dere ruller ut Apple-produkter i organisasjonen deres, er det viktig å forstå hvordan administrerte Apple ID-er støtter tjenestene som de ansatte trenger. Administrerte Apple ID-er er kontoer som er spesifikt utformet med tanke på virksomheter, og som gir tilgang til viktige Apple-tjenester.

Organisasjoner kan bruke Apple Business Manager til å opprette administrerte Apple ID-er som ansatte kan bruke til å jobbe sammen via Apple-apper og -tjenester samt få tilgang til jobbdata i administrerte apper som bruker iCloud Drive. Med forent autentisering kan disse kontoene bruke den samme påloggingsinformasjonen som brukes i den eksisterende infrastrukturen som eies og administreres av den enkelte organisasjonen.

Hva er administrerte Apple ID-er?

I likhet med vanlige Apple ID-er brukes administrerte Apple ID-er også til personlig tilpasning av enheter. De brukes også til å få tilgang til Apple-apper og -tjenester, og lar IT-teamene tilgang til Apple Business Manager. I motsetning til Apple ID-er er Administrerte Apple ID-er eid og administrert av den enkelte organisasjonen. Dette gjelder også tilbakestilling av passord og rollebasert administrasjon.

Apple Business Manager gjør det enkelt å opprette en unik administrert Apple ID for hver av de ansatte i organisasjonen. På grunn av integreringen med Microsoft Azure Active Directory kan organisasjoner gi de ansatte administrerte Apple ID-er der de kan bruke den eksisterende jobb-påloggingsinformasjonen sin.

Når organisasjonen benyttet brukerregistrering i iOS, iPadOS og macOS Catalina, kan administrerte Apple ID-er brukes samtidig med private Apple ID-er på ansattes egne enheter. Eventuelt kan administrerte Apple ID-er brukes som den primære (og eneste) Apple ID-en på en hvilken som helst enhet Administrerte Apple ID-er kan også få tilgang til iCloud på nettet etter første gangs innlogging på en Apple-enhet.

Det er ingen tekniske krav for å rulle ut enheter med en Apple ID. Apple-enheter kan administreres og apper kan distribueres til enheter uten bruk av Apple ID. Se gjennom Apple-tjenestene organisasjonen har planer om å bruke, og vurder hvilken metode som er best for å gå over til administrerte Apple ID-er. Ettersom administrerte Apple ID-er kun kan brukes i jobbsammenheng, er det enkelte funksjoner som er deaktivert her for å beskytte arbeidsplassen.

Funksjoner for organisasjoner

- **Tilgang til Apple-tjenester.** De ansatte kan bruke Apple-tjenester som iCloud og samarbeide via iWork og Notater. E-posttilgangen er deaktivert, og bruk av FaceTime eller iMessage er kun mulig dersom en administrert Apple ID er den eneste Apple ID-en på enheten.
- **Slå opp brukerkontoer.** La de ansatte søke etter kontaktinformasjonen til andre brukere i Apple Business Manager-organisasjonen din, slik at det blir enklere for dem å samarbeide med hverandre på tvers av apper.
- **Effektiv kontooppretting.** Med Apple Business Manager opprettes kontoer automatisk når de ansatte logger på en Apple-enhet første gang.
- **Forent autentisering.** Administratorer kan koble Apple Business Manager opp mot Microsoft Azure Active Directory, slik at de ansatte automatisk blir satt opp med den eksisterende jobb-påloggingsinformasjonen sin.
- **Roller og rettigheter.** Administratorer kan opprette og tilordne roller og rettigheter til IT-team som skal bruke ulike funksjoner i Apple Business Manager.
- **Innebygd sikkerhet og personvern.** Administrerte Apple ID-er bruker de samme datakrypterings-beskyttelsene som standard Apple ID-er, og blokkeres for målrettet reklame på Apples annonseplattform. Kjøpsfunksjonene er deaktivert, i likhet med tjenester som Apple Pay og Wallet. Hvor er? er også deaktivert, ettersom organisasjonene kan bruke Mistet-modus via MDM.

Forent autentisering

Med forent autentisering kan du knytte Apple Business Manager opp mot Microsoft Azure Active Directory (Azure AD), slik at de ansatte kan bruke den eksisterende påloggingsinformasjonen sin som administrerte Apple ID-er.

Microsoft Azure AS fungerer som identitetsleverandør (IdP), og inneholder dermed brukernavnene og passordene som brukes med Apple Business Manager.

Ved integrering med Microsoft Azure AD følger de administrerte Apple ID-ene nøyaktig de samme passordretningslinjene som før, ettersom de er forent med den eksisterende påloggingsinformasjonen.

Administrerte Apple ID-er opprettes automatisk når brukerne logger på Apple-enhetene, slik at IT-administratorene ikke trenger å bruke tid på opprette alt på forhånd.

Dermed kan de ansatte bruke den eksisterende påloggingsinformasjonen sin for Azure AD til å bruke Apple-tjenester som iCloud Drive, Notater, Påminnelser og ulike samarbeidsfunksjoner.

Ettersom organisasjonen allerede administrerer identiteten, håndteres alle passordregler og tilbakestilling av passord av organisasjonen eller brukeren i Microsoft Azure AD.

Krav for forent autentisering

- **Microsoft Azure Active Directory.** Kom i gang med forent autentisering hvis du allerede har dette på plass.
- **Lokalt Active Directory.** Det finnes ytterligere konfigurasjonstrinn for synkronisering med Azure AD. Microsoft stiller dokumentasjon om dette og et synkroniseringsverktøy til rådighet via lenken nedenfor.

Slik konfigurerer du forent autentisering

1. **Bekreft domenet deres hos Apple**. Logg på Apple Business Manager som administrator eller personansvarlig, og legg til domenet eller domenene som skal forenes.
2. **Koble til Microsoft Azure Active Directory og gi tilgang til Apple Business Manager.** Bruk en Global Administrator- eller Application Administrator-konto for å logge på Azure AD og godkjenne at Apple Business Manager får lesetilgang til brukerprofiler.
3. **Bekreft eierskap av domenet med Microsoft Azure Active Directory.** Når tilknytningen er godkjent, fortsetter du prosessen med å verifisere domenet eller domenene. Fra Apple Business Manager logger du på Microsoft Azure Active Directory med en konto fra domenet du vil forene. Dette trinnet bekrefter domenekonfigureringen og beviser at du har eierrettigheter til det.
4. **Se etter domenekonflikter.** Apple Business Manager vil se etter potensielle konflikter med eksisterende Apple ID-er i domenet eller domenene deres. Dette kan være personlige Apple ID-er eller Administrerte Apple ID-er konfigurert av en annen organisasjon på det samme domenet.
5. **Start løsing av domenekonflikter**. Dersom Apple Business Manager oppdager en personlig Apple ID i domenet eller domenene du vil forene, blir de aktuelle brukerne varslet om dette og bedt om å endre e-postadressene de bruker for sine personlige Apple ID-er. Alle kjøp og alle data forblir tilknyttet brukerens personlige Apple ID.
6. **Overfør eksisterende kontoer.** Hvis du har eksisterende administrerte Apple ID-er, kan du overføre dem til forent autentisering ved å endre informasjonen for dem slik at den stemmer med det forente domenet og brukernavnet.

Ressurser

- Kom i gang – Apple Business Manager
- Brukerhåndbok for Apple Business Manager
- Få mer informasjon om hvordan du oppretter administrerte Apple ID-er i Apple Business Manager
- Innføring til forent autentisering med Apple Business Manager
- Finn ut mer om konflikter med eksisterende Apple ID-er
- Finn ut mer om integrering av lokal AD med Azure AD