Översikt av hanterade Apple-ID:n för företag

Det är viktigt att förstå hur hanterade Apple-ID:n fungerar med de tjänster som medarbetarna kan tänkas behöva när man börjar använda Apple-produkter i en organisation. Hanterade Apple-ID:n är konton särskilt utformade för företag som ger åtkomst till viktiga Apple-tjänster.

Med Apple Business Manager kan organisationer automatiskt skapa hanterade Apple-ID:n åt medarbetare så att de kan samarbeta med Apples appar och tjänster och skaffa åtkomst till företagsdata i hanterade appar som använder iCloud Drive. Tack vare federerad autentisering kan de här kontona användas med samma inloggningsuppgifter som för den befintliga infrastrukturen, som ägs och hanteras av respektive organisation.

Vad är hanterade Apple-ID:n?

Precis som andra Apple-ID:n används hanterade Apple-ID:n till att anpassa enheter. De ger även åtkomst till Apples appar och tjänster och de ger it-medarbetare åtkomst till Apple Business Manager. Till skillnad från vanliga Apple-ID:n ägs och hanteras dessa Apple-ID:n av respektive organisation. Detsamma gäller återställning av lösenord och rollbaserad administration.

Med Apple Business Manager är det enkelt att skapa unika hanterade Apple-ID:n åt alla medarbetare i en organisation. Tack vare integreringen med Microsoft Azure Active Directory kan organisationer använda medarbetarnas befintliga inloggningsuppgifter till att skapa hanterade Apple-ID:n.

Hanterade Apple-ID:n kan användas parallellt med personliga Apple-ID:n på medarbetarnas egna enheter om organisationen använder användarregistrering i iOS, iPadOS eller macOS Catalina. Oavsett vilken typ av enhet som används kan man även välja att ha ett hanterat Apple-ID som primärt och enda Apple-ID. Medarbetaren kan även använda sitt hanterade Apple-ID för att skaffa åtkomst till iCloud på webben efter att ha loggat in på en Apple-enhet första gången.

Det finns inget tekniskt krav på att enheter ska driftsättas med Apple-ID. Det går bra att hantera Apple-enheter och distribuera appar även utan ett Apple-ID. Se över vilka tjänster som organisationen tänker använda och bedöm hur ni kan övergå till att använda hanterade Apple-ID:n på bästa sätt. Eftersom hanterade Apple-ID:n endast är avsedda för yrkesmässig användning inaktiveras vissa funktioner för att skydda organisationen.

Funktioner för organisationer

- **Åtkomst till Apple-tjänster.** Medarbetarna kan använda iCloud och andra Apple-tjänster och samarbeta i iWork och Anteckningar. E-post är inaktiverat och FaceTime och iMessage kan bara användas om det hanterade Apple-ID:t är det enda Apple-ID:t på enheten.
- **Söka efter användarkonton.** Medarbetare kan söka efter kontaktuppgifter om andra användare i organisationens Apple Business Manager, vilket gör det enklare för dem att samarbeta med varandra i olika appar.
- **Konton skapas automatiskt.** Ett konto skapas automatiskt i Apple Business Manager första gången en medarbetare loggar in på sin Apple-enhet.
- **Federerad autentisering.** Administratörer kan ansluta Apple Business Manager till Microsoft Azure Active Directory och registrera medarbetare med deras befintliga inloggningsuppgifter.
- **Roller och behörigheter.** Administratörer kan skapa och tilldela roller och behörigheter så att it-personalen kan använda olika funktioner i Apple Business Manager.
- **Inbyggda integritets- och säkerhetsfunktioner.** Hanterade Apple-ID:n skyddas med samma data-kryptering som vanliga Apple-ID:n och riktad reklam blockeras via Apples annonsplattform. Inköp är inaktiverade och detsamma gäller Apple Pay, Wallet och andra liknande tjänster. Hitta min är inaktiverat eftersom organisationer kan använda Förlorat läge via MDM.

Federerad autentisering

Med federerad autentisering kan du ansluta Apple Business Manager till Microsoft Azure Active Directory (Azure AD) och på så sätt låta medarbetarna använda sina befintliga användarnamn och lösenord som hanterade Apple-ID:n.

Microsoft Azure AD är identitetsleverantören som innehåller användarnamnen och lösenorden för de konton som du vill använda med Apple Business Manager.

Integreringen med Microsoft Azure AD gör att hanterade Apple-ID:n följer exakt samma lösenordspolicyer, eftersom de federeras med befintliga inloggningsuppgifter.

Hanterade Apple-ID:n skapas automatiskt när användarna loggar in på sina Apple-enheter, så it-administratören behöver inte lägga tid på att skapa allt i förväg.

Medarbetare kan använda sina befintliga Azure AD-inloggningsuppgifter för att skaffa åtkomst till iCloud Drive, Anteckningar, Påminnelser, samarbetsfunktioner och andra Apple-tjänster.

Eftersom organisationen redan hanterar identiteten sköts alla lösenordspolicyer och lösenordsåterställningar av organisationen eller användaren i Microsoft Azure AD.

Krav för federerad autentisering

- **Microsoft Azure Active Directory.** Du kan komma igång med federerad autentisering direkt om ni redan använder Azure AD.
- **Lokal Active Directory.** Du måste göra ytterligare några inställningar för att synkronisera med Azure AD. Längre ner finns länkar till dokumentation och ett synkroniseringsverktyg från Microsoft.

Konfigurera federerad autentisering

1. **Verifiera domän hos Apple**. Logga in i Apple Business Manager som administratör eller personansvarig och lägg till den eller de domäner som du vill federera.
2. **Anslut till Microsoft Azure Active Directory och bevilja åtkomst för Apple Business Manager.** Logga in i Azure AD med ett konto för Global Administrator eller Application Administrator och ge Apple Business Manager behörighet att läsa användarprofiler.
3. **Verifiera vem som äger domänen i Microsoft Azure Active Directory.** Gå vidare med processen för att verifiera domänerna när du har upprättat en betrodd relation. Logga in i Microsoft Azure AD från Apple Business Manager med ett konto som slutar med den domän som du vill federera. Genom att göra det verifierar du domänen och bekräftar att du äger den.
4. **Kontrollera om det finns domänkonflikter.** Apple Business Manager kontrollerar om det finns några konflikter med befintliga Apple ID:n i din domän. Det kan till exempel vara personliga eller hanterade Apple-ID:n som har skapats av en annan organisation som använder samma domän.
5. **Börja lösa domänkonflikterna**. Användarna meddelas om Apple Business Manager upptäcker att det finns personliga Apple-ID:n i den domän som du vill federera. Användarna måste sedan ändra e-postadresserna i sina Apple-ID:n. Alla köp och data finns kvar i en användares personliga Apple-ID.
6. **Migrera befintliga konton.** Om det finns befintliga hanterade Apple-ID:n kan ni migrera dem till federerad autentisering genom att ändra uppgifterna så att de matchar den federerade domänen och användarnamnet.

Resurser

- Komma igång med Apple Business Manager
- Användarhandbok för Apple Business Manager
- Skapa hanterade Apple-ID:n i Apple Business Manager
- Intro till federerad autentisering med Apple Business Manager
- Läs mer om konflikter med befintliga Apple-ID:n
- Integrera lokala Active Directory-domäner med Azure Active Directory