



Yleiskatsaus yritysten hallittuihin Apple ID:ihin

Kun Applen tuotteita otetaan käyttöön organisaatiossasi, on tärkeä ymmärtää, millä tavalla hallitut Apple ID:t tukevat työntekijöiden tarvitsemia palveluita. Hallitut Apple ID:t ovat erityisesti yrityksille suunniteltuja tilejä, joiden avulla voidaan käyttää Applen keskeisiä palveluita.

Apple Business Managerin avulla organisaatiot voivat luoda automaattisesti hallittuja Apple ID:itä, joiden avulla työntekijät voivat tehdä yhteistyötä Applen appien ja palveluiden parissa ja päästä käsiksi iCloud Drivea käyttävissä hallituissa apeissa oleviin yritystietoihin. Yhdistetyn todennuksen ansiosta nämä tilit käyttävät samoja tunnuksia kuin muussa organisaation omistamassa ja hallinnoimassa infrastruktuurissa.

Mitä ovat hallitut Apple ID:t?

Muiden Apple ID:iden tapaan myös hallittuja Apple ID:itä käytetään laitteen personointiin. Niitä tarvitaan myös Applen appien ja palveluiden käyttämiseen. Lisäksi IT-tiimit pääsevät niillä käsiksi Apple Business Manageriin. Toisin kuin Apple ID:t, hallitut Apple ID:t ovat organisaation omistamia ja hallinnoimia, salasanojen nollaamiset ja rooleihin perustuva ylläpito mukaan lukien.

Apple Business Managerin avulla yksilöllisen hallitun Apple ID:n luominen jokaiselle organisaation työntekijälle on helppoa. Microsoft Azure Active Directoryn integraation ansiosta organisaatiot voivat tarjota hallittuja Apple ID:itä työntekijöille käyttämällä heidän olemassa olevia yritystunnuksiaan.

Hallittuja Apple ID:itä voidaan käyttää työntekijän omistamalla laitteella yhdessä henkilökohtaisen Apple ID:n kanssa, kun organisaatiot hyödyntävät iOS:n, iPadOS:n ja macOS Catalinan käyttäjän rekisteröintiä. Vaihtoehtoisesti voidaan käyttää hallittuja Apple ID:itä ensisijaisena ja ainoana Apple ID:nä missä tahansa laitteessa. Hallitut Apple ID:t voivat myös käyttää iCloudia verkossa sen jälkeen, kun Applen laitteeseen on kirjaututtu ensimmäistä kertaa.

Laitteiden käyttöönoton tekniset vaatimukset eivät edellytä Apple ID:tä. Applen laitteiden hallinta ja appien jakaminen laitteisiin onnistuu ilman Apple ID:tä. Tarkista, mitä palveluita organisaatiosi aikoo käyttää, ja arvioi paras tapa siirtyä hallittuihin Apple ID:ihin. Hallitut Apple ID:t on tarkoitettu vain yrityskäyttöön, joten niistä on poistettu joitakin ominaisuuksia organisaation tietojen suojaamista varten.

Organisaatioille tarkoitetut ominaisuudet

- **Applen palveluiden käyttö.** Työntekijät voivat käyttää Applen palveluita, kuten iCloudia, ja tehdä yhteistyötä iWorkia ja Muistiinpanoja käyttäen. Sähköposti ei ole käytössä, ja FaceTimen tai iMessage:n käyttö on mahdollista vain, jos hallittu Apple ID on laitteen ainoa Apple ID.
- **Käyttäjätilihaku.** Tarjoa työntekijöille mahdollisuus etsiä muiden käyttäjien yhteystietoja Apple Business Manager -organisaatiossasi helpottaaksesi työntekijöiden välistä yhteistyötä eri apeissa.
- **Sujuvampi tilien luomien.** Apple Business Managerilla tilit luodaan automaattisesti, kun työntekijät kirjautuvat ensimmäistä kertaa Applen laitteeseen.
- **Yhdistetty todennus.** Ylläpitäjät voivat yhdistää Apple Business Managerin Microsoft Azure Active Directoryyn ja määrittää työntekijät automaattisesti heidän olemassa olevilla yritystunnuksillaan.
- **Roolit ja käyttöoikeudet.** Ylläpitäjät voivat luoda ja määrittää IT-tiimeille rooleja ja oikeuksia eri toimintojen käyttöä varten Apple Business Managerissa.
- **Tietosuoja ja tietoturva sisäänrakennettuna.** Hallitut Apple ID:t käyttävät samaa tietojen salausta kuin tavalliset Apple ID:t, ja niihin ei käytetä kohdennettua mainontaa Applen mainosalustalla. Ostosten tekeminen sekä Apple Payn ja Walletin kaltaiset palvelut eivät ole käytössä. Missä on...? on pois käytöstä, sillä organisaatiot voivat käyttää MDM:n Kadonnut-tilaa.

Yhdistetty todennus

Yhdistetyllä todennuksella voit yhdistää Apple Business Managerin Microsoft Azure Active Directoryyn (Azure AD), jolloin työntekijät voivat käyttää olemassa olevia käyttäjätunnuksiaan ja salasanojaan hallittuina Apple ID:nä.

Microsoft Azure AD on tunnistetietojen toimittaja, joka sisältää Apple Business Managerin kanssa käytettävien tilien käyttäjätunnukset ja salasanat.

Integroituessaan Microsoft Azure AD:n kanssa hallitut Apple ID:t käyttävät täsmälleen samoja salasanaikäytäntöjä, koska ne on yhdistetty olemassa oleviin tunnuksiin.

Hallitut Apple ID:t luodaan automaattisesti, kun käyttäjä kirjautuu Apple-laitteeseensa. IT-ylläpitäjien ei siis tarvitse käyttää aikaa tunnuksien luomiseen etukäteen.

Työntekijät voivat käyttää olemassa olevia Azure AD -tunnuksiaan päästäkseen Applen palveluihin, kuten iCloud Driveen, Muistiinpanoihin ja Muistutuksiin sekä tekemään yhteistyötä.

Koska organisaatio hallinnoi jo tunnistetietoja, kaikki salasanaikäytännöt ja palautukset hoidetaan organisaation tai käyttäjän toimesta Microsoft Azure AD:ssä.

Yhdistetyn todennuksen edellytykset

- **Microsoft Azure Active Directory.** Voit aloittaa yhdistetyn todennuksen käytön helposti, jos sinulla on tämä jo käytössä.
- **Paikallinen Active Directory.** Jotta voit synkronoida Azure AD:n kanssa, sinun on suoritettava lisämääritysvaiheita. Microsoft tarjoaa dokumentaation ja synkronointityökalun alla olevan linkin kautta.

Resurssit

- [Apple Business Manager – Aloitusopas](#)
- [Apple Business Managerin käyttöopas](#)
- [Lisätietoja hallittujen Apple ID:iden luomisesta Apple Business Managerissa](#)
- [Johdanto yhdistettyyn todennukseen Apple Business Managerissa](#)
- [Lisätietoja ristiriidoista olemassa olevien Apple ID:iden kanssa](#)
- [Lisätietoja paikallisen AD:n integroinnista Azure AD:n kanssa](#)

© 2019 Apple Inc. Kaikki oikeudet pidätetään. Apple, Apple-logo, Apple Music, Apple Pay, FaceTime, iPad, iTunes, iTunes U, iWork ja Safari ovat Apple Inc:n Yhdysvalloissa ja muissa maissa rekisteröityjä tavaramerkkejä. App Store, iCloud ja iCloud Drive ovat Apple Inc:n Yhdysvalloissa ja muissa maissa rekisteröityjä palvelumerkkejä. Muut mainitut yritys- ja tuotenimet saattavat olla omistajiensa tavaramerkkejä.

Näin otat yhdistetyn todennuksen käyttöön

1. **Vahvista verkkotunnus Applen kanssa.**
Kirjaudu Apple Business Manageriin ylläpitäjänä tai henkilöstövastaavana ja lisää verkkotunnukset, jotka haluat yhdistää.
2. **Muodosta yhteys Microsoft Azure Active Directoryyn ja myönnä käyttöoikeus Apple Business Managerille.**
Käytä Global Administrator- tai Application Administrator -tiliä Azure AD:hen kirjautumiseen ja myönnä Apple Business Managerille oikeus lukea käyttäjäprofileja.
3. **Vahvista verkkotunnuksen omistajuus Microsoft Azure Active Directoryn avulla.** Kun luottamus on määritetty, voit jatkaa prosessia ja vahvistaa verkkotunnuksen tai verkkotunnukset. Kirjaudu Apple Business Managerissa Microsoft Azure AD:hen tiilillä, joka päättyy yhdistettävään verkkotunnukseen. Tämä varmistaa, että verkkotunnus on määritetty ja tarkistaa verkkotunnuksen omistajuuden.
4. **Tarkista verkkotunnusristiriidat.**
Apple Business Manager tarkistaa mahdolliset ristiriidat verkkotunnuksissasi olevien nykyisten Apple ID:iden kanssa. Ne voivat olla henkilökohtaisia Apple ID:itä tai hallittuja Apple ID:itä, jotka toinen samaa verkkotunnusta käyttävä organisaatio on määrittänyt.
5. **Aloita verkkotunnusristiriitojen ratkaiseminen.** Jos Apple Business Manager havaitsee henkilökohtaisia Apple ID:itä yhdistettävissä verkkotunnuksissa, kyseisille käyttäjille ilmoitetaan asiasta ja heidän on vaihdettava Apple ID:nsä sähköpostiosoite. Kaikki ostot ja tiedot pysyvät liitettyinä käyttäjän henkilökohtaiseen Apple ID:hen.
6. **Siirrä olemassa olevia tilejä.** Jos sinulla on olemassa olevia hallittuja Apple ID:itä, voit siirtää ne yhdistettyyn todennukseen muuttamalla niiden tiedot vastaamaan yhdistettävää verkkotunnusta ja käyttäjätunnusta.