Panoramica sugli ID Apple gestiti per le aziende

Quando i prodotti Apple vengono distribuiti all'interno di un'organizzazione, è importante capire in che modo gli ID Apple gestiti supportano i servizi di cui il personale potrebbe avere bisogno. Gli ID Apple gestiti sono degli account pensati appositamente per le aziende che forniscono l'accesso ai principali servizi Apple.

Le organizzazioni possono usare Apple Business Manager per creare automaticamente gli ID Apple gestiti per consentire ai dipendenti di collaborare utilizzando le app e i servizi Apple, e di accedere ai dati di lavoro nelle app gestire che usano iCloud Drive. Con l'autenticazione federata, questi account usano le credenziali già in uso per l'infrastruttura esistente di proprietà e sotto il controllo dell'organizzazione.

Cosa sono gli ID Apple gestiti?

Come tutti gli ID Apple, anche quelli gestiti sono usati per personalizzare i dispositivi. Servono inoltre per accedere ad app e servizi Apple, e al reparto IT per accedere a Apple Business Manager. A differenza degli ID Apple, gli ID Apple gestiti restano di proprietà e sotto il controllo dell'organizzazione e sono usati, fra le altre cose, per il ripristino delle password e l'amministrazione basata sui ruoli.

Con Business School Manager, creare ID Apple gestiti univoci per membri del personale di un'organizzazione è facilissimo. Attraverso l'integrazione con Microsoft Azure Active Directory, è possibile fornire ID Apple gestiti ai dipendenti usando le credenziali aziendali già esistenti.

Grazie alla nuova funzione Registrazione utente di iOS, iPadOS e macOS Catalina, i dispositivi di proprietà dell'utente possono ospitare contemporaneamente un ID Apple gestito e uno personale. In alternativa, gli ID Apple gestiti possono essere utilizzati su qualsiasi dispositivo come ID Apple principale (e unico). Dopo il primo accesso, sarà possibile usare gli ID Apple gestiti anche per iCloud.

Distribuire i dispositivi con ID Apple non è un requisito tecnico. È possibile gestire i dispositivi Apple e distribuire le app anche senza un ID Apple. Verifica quali sono i servizi che la tua organizzazione intende utilizzare e valuta il percorso migliore per passare agli ID Apple gestiti. Dato che gli ID Apple gestiti sono destinati esclusivamente all'uso aziendale, alcune funzioni sono disabilitate per proteggere l'organizzazione.

Funzioni per le organizzazioni

- **Accesso ai servizi Apple.** I dipendenti possono usare i servizi Apple, fra cui iCloud e la possibilità di collaborare in iWork e Note. La posta elettronica è disabilitata e l'utilizzo di FaceTime e iMessage è consentito solo se l'ID Apple gestito è l'unico ID Apple presente sul dispositivo.
- **Ricerca di account utente.** I membri del personale possono cercare le informazioni di contatto di altri utenti in Apple Business Manager, così collaborare è più facile anche quando si usano app diverse.
- **Creazione di account semplificata.** Con Apple Business Manager, gli account vengono creati automaticamente quando i dipendenti accedono per la prima volta a un dispositivo Apple.
- **Autenticazione federata.** Gli amministratori possono collegare Apple Business Manager con Microsoft Azure Active Directory e consentire al personale di procedere automaticamente alla configurazione usando le credenziali già in loro possesso.
- **Ruoli e privilegi.** Gli amministratori possono creare e assegnare ruoli e privilegi per consentire al personale IT di utilizzare funzioni diverse in Apple Business Manager.
- **Privacy e sicurezza integrate.** Gli ID Apple gestiti usano la crittografia per proteggere i dati, proprio come gli ID Apple standard, e non possono ricevere inserzioni mirate sulla piattaforma pubblicitaria di Apple. Gli acquisti sono disabilitati come anche l'accesso a servizi come Apple Pay e Wallet. L'app Dov'è è disabilitata perché le organizzazioni possono usare la modalità Smarrito via MDM.

Autenticazione federata

Con l'autenticazione federata, sarà possibile collegare Apple Business Manager a Microsoft Azure Active Directory (Azure AD) e permettere ai membri del personale di utilizzare come ID Apple gestiti i nomi utenti e le password che già possiedono.

Microsoft Azure AD è il provider di identità (IdP) che contiene i nomi utente e le password degli account che si vogliono usare con Apple Business Manager.

Attraverso l'integrazione con Microsoft Azure AD, gli ID Apple gestiti seguono gli stessi criteri delle password perché sono federati con le credenziali esistenti.

Gli ID Apple gestiti vengono creati automaticamente nel momento in cui gli utenti eseguono l'accesso sul proprio dispositivo Apple, e gli amministratori IT non dovranno crearli preventivamente.

Questo significa che potranno usare le credenziali Microsoft Azure AD già esistenti per accedere a servizi Apple come iCloud Drive, Note, Promemoria e alle funzioni di collaborazione.

Visto che è l'organizzazione a gestire l'identità, i criteri delle password e gli eventuali reset sono gestiti dall'organizzazione o dall'utente in Microsoft Azure AD.

Requisiti per l'autenticazione federata

- **Microsoft Azure Active Directory.** Se è già configurato, inizia a utilizzare l'autenticazione federata.
- **Active Directory locale.** È necessario eseguire ulteriori passaggi di configurazione per sincronizzare la directory con Azure AD. Microsoft offre documentazione e uno strumento di sincronizzazione di cui trovi il link qui sotto.

Come configurare l'autenticazione federata

1. **Verificare il dominio con Apple**. Accedi a Apple Business Manager come Amministratore o Responsabile persone e aggiungi uno o più domini per cui desideri utilizzare la federazione.
2. **Collegarsi a Microsoft Azure AD e concedere l'accesso a Apple Business Manager.** Usa un account Amministratore globale o Amministratore applicazione per accedere ad Azure AD e accettare le autorizzazioni per consentire a Apple Business Manager di leggere i profili degli utenti.
3. **Verificare la proprietà del dominio con Microsoft Azure Active Directory.** Una volta stabilita la relazione di trust, continua la procedure per verificare il dominio o i domini. Da Apple Business Manager, accedi a Microsoft Azure AD con un account che termini con il dominio da federare. Questo passaggio verifica la configurazione del dominio e la proprietà.
4. **Controllare la presenza di conflitti tra domini.** Apple Business Manager controllerà la presenza di potenziali conflitti con gli ID Apple esistenti nel dominio; un'altra organizzazione che utilizza lo stesso dominio potrebbe aver configurato degli ID Apple gestiti o personali.
5. **Iniziare la risoluzione dei conflitti tra domini**. Se Apple Business Manager rileva degli ID Apple personali che usano il dominio che hai aggiunto, i relativi utenti riceveranno una notifica e dovranno modificare gli indirizzi email dei propri ID Apple. Tutti gli acquisti e i dati resteranno associati all'ID Apple personale di ogni utente.
6. **Migrare gli account già esistenti.** Se disponi già di ID Apple gestiti, puoi eseguirne la migrazione all'autenticazione federata modificandone i dettagli in modo che corrispondano al dominio federato e al nome utente.

Risorse

- Guida introduttiva a Apple Business Manager
- Manuale utente di Apple Business Manager
- Scopri di più sull'utilizzo degli ID Apple gestiti in Apple Business Manager
- Introduzione all'autenticazione con account associato con Apple Business Manager
- Scopri di più sui conflitti con ID Apple esistenti
- Scopri di più sull'integrazione di AD in locale con Azure AD