Przegląd zarządzanych kont Apple ID dla firm

W kontekście użytkowania produktów Apple w organizacji ważna jest znajomość funkcji, z jakich pracownicy mogą korzystać dzięki zarządzanym kontom Apple ID. Zarządzane konta Apple ID to konta opracowane specjalnie dla firm, umożliwiające dostęp do najważniejszych usług Apple.

Organizacje mogą używać usługi Apple Business Manager do automatycznego tworzenia zarządzanych kont Apple ID, które służą im do zespołowej pracy z wykorzystaniem aplikacji i usług Apple, a także dają dostęp do danych w aplikacjach zarządzanych korzystających z iCloud Drive. Dzięki uwierzytelnianiu federacyjnemu konta te korzystają z tych samych danych uwierzytelniających, co dotychczasowa infrastruktura posiadana i zarządzana przez organizację.

Co to są zarządzane konta Apple ID?

Tak jak wszystkie konta Apple ID, zarządzane konta Apple ID służą do personalizacji urządzeń. Są również przepustką do aplikacji i usług Apple, a zespołom IT umożliwiają dostęp do usługi Apple Business Manager. W odróżnieniu od zwykłych kont Apple ID, zarządzane konta Apple ID są własnością poszczególnych organizacji i są przez nie zarządzane — dotyczy to m.in. resetowania haseł i administrowania na podstawie ról.

Apple Business Manager umożliwia łatwe założenie niepowtarzalnego zarządzanego konta Apple ID dla każdego pracownika organizacji. Dzięki integracji z usługą Microsoft Azure Active Directory organizacje mogą udostępniać pracownikom zarządzane konta Apple ID powiązane z ich dotychczasowymi firmowymi danymi uwierzytelniającymi.

Gdy organizacja korzysta z modelu rejestracji użytkowników w systemach iOS, iPadOS i macOS Catalina, zarządzane konta Apple ID mogą być używane równolegle z prywatnymi kontami Apple ID na urządzeniach należących do pracowników. Alternatywnym modelem jest używanie zarządzanych kont Apple ID na dowolnym urządzeniu jako głównych (i jedynych) kont Apple ID. Zarządzane konta Apple ID dają także dostęp do iCloud w sieci WWW po pierwszym zalogowaniu na urządzeniu Apple.

Konto Apple ID nie jest technicznie konieczne do wdrożenia urządzenia. Możliwe jest zarządzanie urządzeniami Apple i dystrybucja aplikacji do urządzeń bez konta Apple ID. Zalecamy dokonanie przeglądu usług, z których organizacja planuje korzystać, i wybranie na tej podstawie optymalnej drogi do wdrożenia zarządzanych kont Apple ID. Ponieważ zarządzane konta Apple ID są przeznaczone tylko do celów biznesowych, niektóre ich funkcje są wyłączone, aby chronić organizację.

Funkcje dla organizacji

- **Dostęp do usług Apple.** Pracownicy mogą używać usług Apple, w tym iCloud oraz aplikacji iWork i Notatki do pracy zespołowej. Poczta e-mail jest wyłączona, a z usług FaceTime lub iMessage można korzystać tylko wtedy, gdy zarządzane konto Apple ID jest jedynym kontem Apple ID na urządzeniu.
- **Wyszukiwanie kont użytkowników.** Użytkownicy mogą wyszukiwać dane kontaktowe innych użytkowników w organizacji korzystającej z usługi Apple Business Manager. Ułatwia to współpracę między użytkownikami przy użyciu aplikacji.
- **Usprawnienie zakładania kont.** Dzięki usłudze Apple Business Manager konto zakładane jest automatycznie, gdy dany użytkownik po raz pierwszy loguje się na urządzeniu Apple.
- **Uwierzytelnianie federacyjne.** Administratorzy mogą połączyć usługę Apple Business Manager z usługą Microsoft Azure Active Directory, aby pracownicy automatycznie mogli używać dotychczasowych firmowych danych uwierzytelniających.
- **Role i uprawnienia.** Administratorzy mogą tworzyć i przydzielać role i uprawnienia umożliwiające zespołom IT korzystanie z różnych funkcji w ramach usługi Apple Business Manager.
- **Wbudowana ochrona prywatności i zabezpieczenia** Zarządzane konta Apple ID są tak samo chronione kryptograficznie, jak standardowe konta Apple ID, a ponadto są wykluczone z targetowanych reklam na platformie reklamowej Apple. Funkcje handlowe są wyłączone, podobnie jak dostęp do takich usług, jak Apple Pay czy Wallet. Funkcja Znajdź mój jest wyłączona, ponieważ organizacje mogą korzystać z trybu Utracony w powiązaniu z systemem MDM.

Uwierzytelnianie federacyjne

Uwierzytelnianie federacyjne umożliwia połączenie usługi Apple Business Manager z usługą Microsoft Azure Active Directory (Azure AD), tak by pracownicy mogli używać swoich dotychczasowych nazw użytkowników i haseł jako identyfikatorów zarządzanych kont Apple ID.

Microsoft Azure AD to dostawca tożsamości przechowujący nazwy użytkowników i hasła do kont, które mają być używane z portalem Apple Business Manager.

W wyniku integracji z usługą Microsoft Azure AD zarządzane konta Apple ID podlegają dokładnie tym samym zasadom dotyczącym haseł, co dotychczasowe dane uwierzytelniające, ponieważ są z nimi sfederowane.

Zarządzane konta Apple ID tworzone są automatycznie, gdy użytkownicy logują się na swoich urządzeniach Apple, zatem administratorzy IT nie muszą poświęcać czasu na przygotowywanie tych kont.

Pracownicy mogą używać swoich dotychczasowych danych uwierzytelniających z usługi Azure AD, by uzyskiwać dostęp do usług Apple, w tym iCloud Drive, Notatki, Przypomnienia i aplikacje do pracy zespołowej.

Ponieważ organizacja ma już działający system zarządzania tożsamością, wszystkie zasady dotyczące haseł i operacje resetowania haseł są obsługiwane przez organizację lub samego użytkownika w usłudze Microsoft Azure AD.

Wymagania uwierzytelniania federacyjnego

- **Microsoft Azure Active Directory.** Aby zacząć korzystać z uwierzytelniania federacyjnego, organizacja musi mieć już wdrożone następujące komponenty.
- **Lokalna usługa Active Directory.** Istnieją dodatkowe etapy konfiguracji związane z synchronizacją z Azure AD. Microsoft oferuje dokumentację i narzędzie do synchronizacji na stronach wskazanych poniżej.

Jak skonfigurować uwierzytelnianie federacyjne

1. **Weryfikacja domeny w Apple**. Zaloguj się w portalu Apple Business Manager jako Administrator lub Menedżer użytkowników i dodaj domenę(-y), którą(-e) chcesz sfederować.
2. **Nawiązanie połączenia z Microsoft Azure Active Directory i nadanie uprawnień dostępu usłudze Apple Business Manager.** Skorzystaj z konta Administratora globalnego lub Administratora aplikacji, by zalogować się do usługi Azure AD i zaakceptować uprawnienia zezwalające usłudze Apple Business Manager na odczyt profili użytkowników.
3. **Weryfikacja własności domeny w usłudze Microsoft Azure Active Directory.** Po ustanowieniu relacji zaufania przejdź do weryfikacji domen(y). Z portalu Apple Business Manager zaloguj się w usłudze Microsoft Azure AD za pomocą konta, którego identyfikator kończy się domeną przeznaczoną do sfederowania. Ta operacja weryfikuje konfigurację domen i potwierdza ich własność.
4. **Sprawdzenie, czy występują konflikty domen.** Apple Business Manager sprawdzi, czy występują kolizję z istniejącymi identyfikatorami Apple ID w domenie przeznaczonej do sfederowania. Mogą to być identyfikatory prywatnych kont Apple ID lub zarządzanych kont Apple ID założonych przez inną organizację korzystającą z tej samej domeny.
5. **Zainicjowanie rozwiązania konfliktów domen**. Jeśli Apple Business Manager wykryje prywatne konto Apple ID w domenie(-ach) przeznaczonej(-ych) do sfederowania, użytkownicy tych kont zostaną powiadomieni i będą musieli zmienić adresy e-mail przypisane do swoich kont Apple ID. Wszystkie zakupy i dane pozostaną powiązane z prywatnym kontem Apple ID użytkownika.
6. **Migracja istniejących wcześniej kont.** Istniejące zarządzane konta Apple ID można przenieść do uwierzytelniania federacyjnego, zmieniając ich dane tak, by zgadzały się z federacyjną domeną i nazwą użytkownika.

Materiały

- Apple Business Manager — pierwsze kroki
- Podręcznik użytkownika usługi Apple Business Manager
- Więcej informacji o tworzeniu zarządzanych kont Apple ID w usłudze Apple Business Manager
- Wprowadzenie do uwierzytelniania federacyjnego w usłudze Apple Business Manager
- Więcej informacji o kolizjach z istniejącymi identyfikatorami Apple ID
- Więcej informacji o integracji lokalnej usługi AD z usługą Azure AD