Verwalteten Apple IDs für Unternehmen

Es ist wichtig, dass Sie bei der Verwendung von Apple Produkten in Ihrem Unternehmen verstehen, wie verwaltete Apple IDs die Dienste unterstützen, die Ihre Mitarbeiter möglicherweise benötigen. Verwaltete Apple IDs sind Benutzerkonten, die speziell dafür gedacht sind, Unternehmen die Nutzung wichtiger Apple Services zu ermöglichen.

Unternehmen können Apple Business Manager nutzen, um automatisch verwaltete Apple IDs anzulegen, damit die Mitarbeiter die Möglichkeit haben, mit Apps und Diensten von Apple zusammenzuarbeiten und auf Unternehmensdaten in verwalteten Apps zuzugreifen, die iCloud Drive verwenden. Mit der Verbundauthentifizierung nutzen diese Benutzerkonten die gleichen Zugangsdaten wie in vorhandener Infrastruktur des jeweiligen Unternehmens.

Was sind verwaltete Apple IDs?

Wie alle Apple IDs werden verwaltete Apple IDs verwendet, um Geräte zu personalisieren. Sie werden auch verwendet, um auf Apple Apps und Services zuzugreifen, und sie erlauben IT-Teams, auf Apple Business Manager zuzugreifen. Im Unterschied zu Apple IDs gehören verwaltete Apple IDs dem Unternehmen und werden auch von diesem verwaltet, inklusive dem Zurücksetzen von Passwörtern und der Rollenverwaltung.

Mit Apple Business Manager lassen sich ganz einfach einzigartige verwaltete Apple IDs für jeden Mitarbeiter im Unternehmen erstellen. Dank der Integration von Microsoft Azure Active Director können Unternehmen ihren Mitarbeitern verwaltete Apple IDs über bereits vorhandene Unternehmensanmeldedaten bereitstellen.

Verwaltete Apple IDs können auf Geräten, die den Mitarbeitern gehören, auch zusammen mit persönlichen Apple IDs verwendet werden, falls das Unternehmen die Benutzerregistrierung in iOS, iPadOS und macOS Catalina nutzt. Alternativ können verwaltete Apple IDs auf Geräten auch als primäre – und einzige – Apple ID genutzt werden. Verwaltete Apple IDs ermöglichen nach der erstmaligen Anmeldung auf einem Apple Gerät auch den Zugriff auf iCloud via Internet.

Der Einsatz von Geräten mit einer Apple ID ist aus technischer Hinsicht nicht erforderlich. Apple Geräte können auch ohne Apple ID verwaltet werden – auch Apps lassen sich ohne Apple ID verteilen. Überprüfen Sie die Services, die Ihr Unternehmen zu verwenden plant, und bestimmen Sie so den bestmöglichen Übergang zu verwalteten Apple IDs. Da verwaltete Apple IDs nur für geschäftliche Zwecke gedacht sind, sind bestimmte Funktionen deaktiviert, um Unternehmen zu schützen.

Features für Unternehmen

- **Zugang zu Apple Services.** Mitarbeiter können Apple Services nutzen, dazu gehören auch iCloud und die Zusammenarbeit mit iWork und der Notizen App. E-Mail ist deaktiviert und Facebook und iMessage sind nur verfügbar, wenn die verwaltete Apple ID die einzige Apple ID auf einem Gerät ist.
- **Suche nach Benutzerkonten.** Dürfen Mitarbeiter in einem Unternehmen mit Apple Business Manager nach den Kontaktdaten anderer Nutzer suchen, vereinfacht dies die Zusammenarbeit über alle Apps hinweg.
- **Optimierte Kontoeröffnung.** Mit Apple Business Manager werden Benutzerkonten automatisch erstellt, wenn die Mitarbeiter sich zum ersten Mal auf einem Apple Gerät anmelden.
- **Verbundauthentifizierung.** Administratoren können Apple Business Manager mit Microsoft Azure Active Directory verbinden, wodurch die Mitarbeiter automatisch mit vorhandenen Unternehmensanmeldedaten eingerichtet werden.
- **Rollen und Berechtigungen.** Administratoren können Rollen und Rechte erstellen und IT-Teams zuweisen, damit sie unterschiedliche Funktionen von Apple Business Manager nutzen können.
- **Integrierte Funktionen für Datenschutz und Sicherheit.** Verwaltete Apple IDs nutzen die gleiche Datenverschlüsselung wie normale Apple IDs und lassen auf der Werbeplattform von Apple keine zielgerichtete Werbung zu. Einkäufe sind deaktiviert, ebenso Services wie Apple Pay und Wallet. Die „Wo ist?“ Funktion ist deaktiviert, da Unternehmen dafür den „Verloren“-Modus ihrer MDM-Lösung nutzen können.

Verbundauthentifizierung

Mit der Verbundauthentifizierung kann Apple Business Manager mit Microsoft Azure Active Directory (Azure AD) verbunden werden, was es Mitarbeitern ermöglicht, ihre vorhandenen Benutzernamen und Passwörter als verwaltete Apple IDs zu verwenden.

Microsoft Azure AD ist der Identitätsanbieter (Identity Provider, IdP) mit den Benutzernamen und Passwörtern für die Accounts, die Sie mit Apple Business Manager verwenden wollen.

Durch die Integration mit Microsoft Azure AD folgen verwaltete Apple IDs den gleichen Passwortrichtlinien, da sie über die gleichen Anmeldedaten verbunden sind.

Verwaltete Apple IDs werden automatisch erstellt, wenn sich die Benutzer auf Apple Geräten anmelden, sodass sich IT-Administratoren im Vorfeld nicht extra Zeit dafür nehmen müssen.

Mitarbeiter können ihre vorhandenen Azure AD Anmeldedaten nutzen, um auf Apple Services zuzugreifen (inklusive iCloud Drive, Notizen, Erinnerungen und Zusammenarbeit).

Da das Unternehmen die Identität bereits verwaltet, werden alle Passwortrichtlinien und Wiederherstellungen vom Unternehmen oder dem Benutzer in Microsoft Azure AD durchgeführt.

Voraussetzung für die Verbundauthentifizierung

- **Microsoft Azure Active Directory.** Legen Sie mit der Verbundauthentifizierung los, wenn Sie dies bereits eingerichtet haben.
- **Active Directory vor Ort vorhanden.** Für die Synchronisation mit Azure AD sind weitere Schritte nötig. Microsoft bietet die Dokumentation und ein Tool für die Synchronisierung (Link unten).

Einrichtung der Verbundauthentifizierung

1. **Domain von Apple verifizieren lassen**. Melden Sie sich als Administrator oder Personenmanager an und fügen Sie die gewünschten Domains für die Verbundauthentifizierung hinzu.
2. **Verbinden Sie sich mit Microsoft Active Directory und gewähren Sie Apple Business Manager Zugriff.** Verwenden Sie das Benutzerkonto eines Global Administrators oder eines Application Administrators, um sich bei Azure AD anzumelden und Apple Business Manager die Genehmigung zu erteilen, Benutzerprofile zu lesen.
3. **Verifizieren Sie die Domain-Inhaberschaft mit Microsoft Azure Active Directory.** Sind die nötige Schritte durchgeführt worden, setzen Sie die Verifizierung der Domain(s) fort. Melden Sie sich aus Apple Business Manager bei Microsoft Azure AD mit einem Account an, der mit Ihrer Domain für die Verbundauthentifizierung endet. Dieser Schritt verifiziert die Einrichtung der Domain und bestätigt, dass Sie sich in ihrem Besitz befindet.
4. **Prüfen, ob Domain-Konflikte vorliegen.** Apple Business Manager sucht dabei nach potenziellen Konflikten mit bestehenden Apple IDs in Ihren Domains. Dabei kann es sich um persönliche Apple IDs oder um verwaltete Apple IDs anderer Unternehmen handeln, die die gleiche Domain verwenden.
5. **Domain-Konflikte lösen**. Entdeckt Apple Business Manager eine persönliche Apple ID in den Domains, die Sie für die Verbundauthentifizierung nutzen wollen, werden die Benutzer benachrichtigt und müssen die E-Mail-Adresse für ihre Apple ID ändern. Alle Einkäufe und Daten der privaten Apple IDs dieser Benutzer bleiben dabei erhalten.
6. **Vorhandene Konten migrieren.** Wenn Sie bereits verwaltete Apple IDs eingerichtet haben, können Sie diese zur Verbundauthentifizierung migrieren, indem Sie die zugehörigen Angaben in den Domain- und Benutzernamen für die Verbundauthentifizierung ändern.

Ressourcen

- Einführungshandbuch zu Apple Business Manager
- Apple Business Manager – Benutzerhandbuch
- Mehr zur Erstellung verwalteter Apple IDs in Apple Business Manager
- Einführung in die verknüpfte Authentifizierung mit Apple Business Manager
- Mehr zu Konflikten mit bestehenden Apple IDs
- Integrieren von lokalen Active-Directory-Domänen in Azure Active Directory