



Přehled spravovaných Apple ID pro firmy

Při používání produktů Apple ve vaší organizaci je důležité rozumět tomu, jak spravovaná Apple ID podporují služby, které vaši zaměstnanci potřebují. Spravovaná Apple ID jsou účty určené speciálně pro firmy. Umožňují přístup ke klíčovým službám Apple.

Organizace může pomocí Apple Business Manageru vytvářet zaměstnancům spravovaná Apple ID, která jim umožní spolupracovat v aplikacích a službách Apple a přistupovat k firemním datům ve spravovaných aplikacích, které používají iCloud Drive. A když si nastavíte federované ověřování, budou tyto účty používat stejné přihlašovací údaje jako vaše existující infrastruktura, kterou už vlastníte a spravujete.

Co jsou spravovaná Apple ID?

Stejně jako každé Apple ID, i spravovaná Apple ID slouží k personalizaci zařízení. Poskytují přístup k aplikacím a službám Apple a IT týmům umožňují přihlašovat se k Apple Business Manageru. Na rozdíl od klasických Apple ID jsou spravovaná Apple ID vlastněná a spravovaná organizací, která může mimo jiné obnovovat hesla nebo je spravovat na základě rolí.

V Apple Business Manageru můžete jednoduše vytvořit samostatné spravované Apple ID každému zaměstnanci vaší organizace. Díky integraci se službou Microsoft Azure Active Directory může organizace vytvořit zaměstnancům spravovaná Apple ID, která budou používat jejich stávající firemní přihlašovací údaje.

Když organizace používá v iOS, iPadOS nebo macOS Catalina registraci uživatelů, je možné používat na zařízeních patřících zaměstnancům spravované Apple ID zároveň s osobními Apple ID. Anebo můžete na kterémkoli zařízení používat spravované Apple ID jako primární —a jediné— Apple ID. Po prvním přihlášení na zařízení Apple se uživatelé pomocí spravovaných Apple ID dostanou i k iCloudu na webu.

Neexistují žádné technické požadavky, které by vyžadovaly nasazení zařízení s Apple ID. Zařízení Apple se dají spravovat i bez Apple ID a pořád do nich můžete distribuovat aplikace. Zamyslete se nad tím, jaké služby plánuje vaše organizace používat, a vyhodnoťte nejlepší způsob přechodu na spravovaná Apple ID. Jelikož spravovaná Apple ID slouží jen k firemním účelům, některé funkce jsou u nich v zájmu ochrany organizace vypnuté.

Funkce pro organizace

- **Přístup k službám Apple.** Zaměstnanci se dostanou k službám Apple včetně iCloudu a mohou spolupracovat v aplikacích iWork a Poznámkách. Pokud je spravované Apple ID jediným Apple ID na zařízení, bude mít vypnutý e-mail a zakázané používání FaceTimu a iMessage.
- **Vyhledávání uživatelských účtů.** Zaměstnanci mohou v rámci vaší organizace v Apple Business Manageru vyhledávat kontaktní údaje ostatních uživatelů, což jim usnadňuje spolupráci v různých aplikacích.
- **Efektivní vytváření účtů.** Apple Business Manager vytváří účty automaticky, když se uživatel poprvé přihlásí k zařízení Apple.
- **Federované ověřování.** Administrátoři mohou Apple Business Manager propojit se službou Microsoft Azure Active Directory. Potom se uživatelům automaticky nastaví účty používající jejich stávající přihlašovací údaje.
- **Role a oprávnění.** Administrátoři mohou v Apple Business Manageru vytvářet role s různými funkcemi a přiřazovat je IT týmům.
- **Vestavěné zabezpečení a ochrana soukromí.** Spravovaná Apple ID využívají stejné ochrany a šifrování dat jako standardní Apple ID a v rámci reklamní platformy Apple je u nich zablokované zobrazování cílených reklam. Mají vypnuté komerční funkce a přístup k službám jako Apple Pay nebo Wallet. Aplikace Najít je vypnutá, protože organizace může ztracené zařízení najít pomocí MDM.

Federované ověřování

Federované ověřování vám umožňuje propojit Apple Business Manager se službou Microsoft Azure Active Directory (Azure AD), aby uživatelé mohli jako svá spravovaná Apple ID používat svá existující uživatelská jména a hesla.

Poskytovatelem identity (IdP) je v takovém případě Microsoft Azure AD – obsahuje uživatelská jména a hesla všech účtů, které chcete s Apple Business Managerem používat.

Při integraci s Microsoft Azure AD používají spravovaná Apple ID stejná pravidla hesel, protože se federují s existujícími přihlašovacími údaji.

Spravovaná Apple ID se vytvoří automaticky, jakmile se uživatel přihlásí k zařízení Apple, takže správci IT nemusí ztrácet čas ručním nastavováním.

Zaměstnanci se pomocí svých existujících přihlašovacích údajů k Azure AD dostanou k službám Apple včetně iCloud Drivu, Poznámek, Připomínek a spolupráce.

Jelikož identitu už z dřívějška spravuje organizace, stará se o veškerá pravidla nebo obnovování hesel sama organizace nebo uživatel v Microsoft Azure AD.

Požadavky federovaného ověřování

- **Microsoft Azure Active Directory.** Pokud už tuhle službu používáte, můžete s federovaným ověřováním rovnou začít.
- **Místní systém Active Directory.** Pro synchronizaci s Azure AD je potřeba provést pár dodatečných kroků. Na odkazu dole najdete dokumentaci a synchronizační nástroj od společnosti Microsoft.

Zdroje

- [Příručka Začínáme s Apple Business Managerem](#)
- [Uživatelská příručka pro Apple Business Manager](#)
- [Další informace o vytváření spravovaných Apple ID v Apple Business Manageru](#)
- [Úvod do federovaného ověřování s Apple Business Managerem](#)
- [Další informace o konfliktech s existujícími Apple ID](#)
- [Další informace o integraci místního AD s Azure AD](#)

© 2019 Apple Inc. Všechna práva vyhrazena. Apple, logo Apple, Apple Music, Apple Pay, FaceTime, iPad, iTunes, iTunes U, iWork a Safari jsou ochranné známky společnosti Apple Inc., registrované v USA a dalších zemích. App Store, iCloud a iCloud Drive jsou značky služeb společnosti Apple Inc., registrované v USA a dalších zemích. Názvy dalších produktů a společností zmíněné v textu mohou být ochrannými známkami příslušných společností.

Nastavení federovaného ověřování

1. **Ověřte doménu u společnosti Apple.** Přihlaste se k Apple Business Manageru jako administrátor nebo správce osob a přidejte domény, které chcete federovat.
2. **Připojte se k Microsoft Azure Active Directory a udělte Apple Business Manageru přístup.** Účtem globálního správce nebo správce aplikací se přihlaste k Azure AD a přístup potvrďte. Tím Apple Business Manageru umožníte číst uživatelské profily.
3. **Ověřte v Microsoft Azure Active Directory, že domény patří vám.** Až tímhle způsobem zřídíte důvěru, pokračujte ověřením domén. V Apple Business Manageru se přihlaste k Microsoft Azure AD účtem končícím na doménu, kterou chcete federovat. Tím potvrdíte nastavení domény a prokážete, že vám patří.
4. **Zkontrolujte případné konflikty domén.** Apple Business Manager zkontroluje, jestli vaše doména nekoliduje s některými existujícími Apple ID. Může jít o osobní Apple ID nebo o spravovaná Apple ID vytvořená jinou organizací a používající stejnou doménu.
5. **Vyřešte konflikty domén.** Když Apple Business Manager najde nějaká Apple ID kolidující s doménou, kterou chcete federovat, pošle jejich uživatelům upozornění a požádá je, aby změnil e-mailovou adresu svého Apple ID. Všechny nákupy a data zůstanou přidružená k uživatelovu osobnímu Apple ID.
6. **Převeďte existující účty.** Pokud už máte nějaká spravovaná Apple ID, můžete je převést na federované ověřování změnou jejich údajů tak, aby odpovídaly federované doméně a uživatelskému jménu.