Omówienie wdrażania systemów iOS i iPadOS

Wprowadzenie

Spis treści

iPhone i iPad mogą odmienić firmę i sposób wykonywania codziennych obowiązków przez personel. Potrafią znacząco zwiększyć produktywność pracowników, dając im, zarówno w biurze, jak i w podróży, swobodę i elastyczność, tak by innowacyjnie realizowali swoje zadania. Zastosowanie tych nowoczesnych metod pracy przynosi korzyści całej organizacji. Użytkownicy mają lepszy dostęp do informacji, co daje im poczucie sprawczości i pozwala kreatywnie rozwiązywać problemy.

W firmach, które korzystają z systemów iOS i iPadOS, praca działów IT jest postrzegana nie tylko jako eliminowanie przeszkód technicznych i szukanie oszczędności, ale też jako tworzenie strategii biznesowej i rozwiązywanie rzeczywistych problemów. Wzbudzenie w pracownikach zapału do pracy i pojawienie się licznych nowych możliwości biznesowych jest korzystne dla całej organizacji.

Skonfigurowanie i wdrażanie iPhone'a i iPada do zastosowań biznesowych nigdy nie było prostsze. Dzięki usłudze Apple Business Manager i oferowanym przez inne firmy rozwiązaniom do zarządzania urządzeniami mobilnymi (MDM) organizacja może swobodnie wdrażać urządzenia z systemami iOS i iPadOS oraz aplikacje na dużą skalę.

- System zarządzania urządzeniami mobilnymi pozwala skonfigurować urządzenia i zarządzać nimi, a także bezprzewodowo rozpowszechniać i kontrolować aplikacje.
- Usługa Apple Business Manager automatyzuje rejestrację urządzeń Apple w systemie MDM, aby umożliwić ich wdrażanie bez angażowania personelu IT w konfigurację każdego egzemplarza.
- Apple Business Manager umożliwia hurtowy zakup aplikacji i książek oraz bezprzewodowe rozsyłanie ich użytkownikom.
- Apple Business Manager umożliwia również tworzenie zarządzanych kont Apple ID dla pracowników korzystających z uwierzytelniania federacyjnego Microsoft Azure AD.

W tym dokumencie zawarto wskazówki dotyczące wdrażania urządzeń z systemami iOS i iPadOS w organizacji oraz tworzenia planu wdrażania odpowiadającego potrzebom danego środowiska. Zagadnienia te omówiono bardziej szczegółowo w podręczniku wdrażania iPhone'ów i iPadów dostępnym w Internecie pod adresem: support.apple.com/guide/deployment-reference-ios

Modele własności

Analiza modeli własności i wybór rozwiązania odpowiedniego dla organizacji to pierwszy i niezwykle ważny etap wdrażania. Zależnie od tego, kto jest właścicielem urządzenia, wdrożenie można przeprowadzić na kilka sposobów. Proces należy rozpocząć od określenia najlepszego dla organizacji rozwiązania.

W przedsiębiorstwach stosowane są powszechnie dwa modele własności urządzeń z systemami iOS i iPadOS:

- Urządzenie należy do organizacji
- Własność użytkownika

Choć większość organizacji ma preferowany model wdrażania, w środowisku jednej instytucji można zastosować ich kilka. Przykładowo, centrala firmy może wdrożyć strategię, w której urządzenia są własnością użytkowników i pozwolić pracownikom na skonfigurowanie ich własnych iPadów, chroniąc jednocześnie zasoby korporacyjne i zarządzając nimi bez ingerowania w prywatne aplikacje oraz dane użytkowników. W tym samym czasie należący do firmy sklep może wdrożyć strategię, w której to organizacja jest właścicielem urządzeń, i udostępnić pracownikom współdzielone urządzenia z systemem iOS i iPadOS służące tylko do przetwarzania transakcji.

Zapoznanie się z tymi modelami pozwala na wybór rozwiązania najlepszego dla unikalnego środowiska danej instytucji. Po określeniu modelu najlepszego dla organizacji jej zespół może przejść do analizy wszystkich możliwości wdrożenia i zarządzania oferowanych przez Apple.

Urządzenia należące do organizacji

W modelu, w którym urządzenia są własnością organizacji, można udostępnić urządzenia pracownikom indywidualnie, do codziennego użytku; można je udostępnić do wspólnego użytku przy wykonywaniu typowych zadań; wreszcie — można skonfigurować je pod kątem jednego konkretnego zastosowania, tak by działała na nich tylko jedna aplikacja. Użytkownik końcowy, któremu indywidualnie udostępniono urządzenie, może je spersonalizować. Urządzenia, na których może działać tylko jedna aplikacja lub są współużytkowane przez wiele osób zwykle, nie są personalizowane przez użytkowników końcowych. Korzystanie z połączenia tych modeli, najważniejszych technologii Apple i odpowiedniego rozwiązania MDM pozwala w pełni zautomatyzować przygotowanie i konfigurację urządzeń.

Model z możliwością personalizacji. W przypadku strategii dopuszczającej personalizację każdy użytkownik może wybrać urządzenie dla siebie i zarejestrować je w systemie MDM, który będzie bezprzewodowo przekazywał ustawienia i aplikacje używane w organizacji. Jeśli organizacja nabywa urządzenia bezpośrednio od Apple, uczestniczącego w programie autoryzowanego sprzedawcy Apple (Apple Authorized Reseller) lub operatora, może wykorzystać usługę Apple Business Manager do automatycznej rejestracji nowych urządzeń w rozwiązaniu MDM, czyli tak zwanej zautomatyzowanej rejestracji urządzeń. Po skonfigurowaniu urządzenia użytkownik może je spersonalizować, dodając oprócz firmowych aplikacji i konta swoje własne aplikacje i dane.

Model bez możliwości personalizacji. Kiedy urządzenia są współdzielone przez kilkoro pracowników lub pełnią tylko jedną funkcję (np. w restauracji czy hotelu), administratorzy IT zazwyczaj konfigurują je i zarządzają nimi w sposób scentralizowany, bez umożliwiania pojedynczym użytkownikom ich konfiguracji. Zasadniczo w modelu wdrażania bez opcji personalizacji użytkownicy nie są uprawnieni do instalowania na urządzeniu aplikacji ani zapisywania w nim prywatnych danych. Zautomatyzowana rejestracja urządzeń za pośrednictwem usługi Apple Business Manager może także usprawnić konfigurację urządzeń niespersonalizowanych. Umieszczona poniżej tabela przedstawia działania, które powinni podjąć administrator i użytkownik na każdym etapie wdrażania urządzeń będących własnością organizacji. Jeśli nie zaznaczono inaczej, opisane działania mają zastosowanie zarówno w wypadku modelu wdrożenia *z możliwością personalizacji*, jak i *bez takiej możliwości*.

	Administrator	Użytkownik
Przygotowanie	• Ocena istniejącej infrastruktury • Wybór rozwiązania MDM • Rejestracja w usłudze Apple Business Manager	• Nie jest wymagane żadne działanie użytkownika
Konfiguracja	• Skonfigurowanie urządzeń • Dystrybucja aplikacji i książek	• Nie jest wymagane żadne działanie użytkownika
Wdrożenie	• Dystrybucja urządzeń **Tylko dla wdrożenia z możliwością personalizacji** • Umożliwienie użytkownikom personalizacji	**Tylko dla wdrożenia z możliwością personalizacji** • Pobranie i instalacja aplikacji oraz książek • Użycie kont Apple ID, App Store i iCloud tam, gdzie ma to zastosowanie **Tylko dla wdrożenia bez możliwości personalizacji** • Nie jest wymagane działanie użytkownika
Zarządzanie	• Administrowanie urządzeniami • Wdrożenie dodatkowych treści i zarządzanie nimi	**Tylko dla wdrożenia z możliwością personalizacji** • Poszukiwanie dodatkowych aplikacji **Tylko dla wdrożenia bez możliwości personalizacji** • Nie jest wymagane żadne działanie użytkownika

Urządzenia będące własnością użytkowników

Nawet jeśli pracownik sam zakupił i skonfigurował urządzenie — w tzw. modelu wdrażania BYOD (Bring Your Own Device) — organizacja może mu udostępnić usługi firmowe, np. sieć Wi-Fi, pocztę e-mail lub kalendarze, za pomocą systemu MDM, korzystając z nowej opcji Rejestracja użytkownika dostępnej w systemach iOS 13 i iPadOS.

Model wdrożenia BYOD umożliwia użytkownikom przygotowanie i konfigurację ich własnych urządzeń. Użytkownik może zarejestrować swoje urządzenie w systemie MDM, by zyskać dostęp do zasobów firmowych, skonfigurować różne ustawienia bądź zainstalować profil konfiguracyjny lub aplikacje firmowe. Użytkownik musi tylko wyrazić zgodę na rejestrację w należącym do organizacji systemie MDM.

Zastosowanie funkcji Rejestracja użytkownika do urządzeń będących własnością pracowników umożliwia bezpieczne zarządzanie zasobami i danymi firmy z poszanowaniem prywatności użytkownika, jego osobistych danych i aplikacji. Zespół IT może wymuszać określone ustawienia, monitorować przestrzeganie zasad obowiązujących w firmie i usuwać dane i aplikacje należące do firmy, nie naruszając osobistych danych i aplikacji na urządzeniu użytkownika.

Oto najważniejsze cechy funkcji Rejestracja użytkownika:

- **Zarządzane konto Apple ID.** Rejestracja użytkownika jest zintegrowana z zarządzanym kontem Apple ID, aby ustanowić tożsamość użytkownika na urządzeniu i umożliwić dostęp do usług Apple. Zarządzanego konta Apple ID można używać równolegle z osobistym kontem Apple ID, na którym użytkownik jest zalogowany. Zarządzane konta Apple ID są tworzone w usłudze Apple Business Manager i udostępniane za pośrednictwem uwierzytelniania federacyjnego w usłudze Microsoft Azure Active Directory.
- **Separacja danych.** Rejestracja użytkownika tworzy w urządzeniu osobny wolumin APFS na zarządzane konta, aplikacje i dane. Ten zarządzany wolumin jest kryptograficznie odseparowany od reszty urządzenia
- **Selektywne zarządzanie w modelu BYOD.** Rejestracja użytkownika jest rozwiązaniem zaprojektowanym z myślą o urządzeniach będących własnością użytkowników. Dlatego zespół IT może zarządzać podzbiorem ustawień konfiguracyjnych i zasad, ale nie ma możliwości wykonywania niektórych zadań administracyjnych, np. zdalnego wymazania całej zawartości urządzenia lub zbierania danych osobowych.

Umieszczona poniżej tabela przedstawia działania, które powinni podjąć administrator i użytkownik na każdym etapie wdrażania w modelu, w którym urządzenia należą do pracowników.

	Administrator	Użytkownik
Przygotowanie	• Ocena istniejącej infrastruktury • Wybór rozwiązania MDM • Rejestracja w usłudze Apple Business Manager	• Korzystanie z osobistych i zarządzanych kont Apple ID oraz kont w App Store i iCloud tam, gdzie ma to zastosowanie
Konfiguracja	• Konfigurowanie ustawień urządzenia • Dystrybucja aplikacji i książek	• Wyrażenie zgody na włączenie do firmowego systemu MDM • Pobranie i instalacja aplikacji oraz książek
Wdrożenie	• Nie jest wymagane żadne działanie administratora	• Nie jest wymagane żadne działanie użytkownika
Zarządzanie	• Administrowanie urządzeniami • Wdrożenie dodatkowych treści i zarządzanie nimi	• Poszukiwanie dodatkowych aplikacji

Więcej informacji o Rejestracji użytkownika w rozwiązaniu MDM:
support.apple.com/guide/mdm

Więcej informacji o uwierzytelnianiu federacyjnym:
support.apple.com/guide/apple-business-manager

Etapy wdrażania

W tej sekcji zawarto bardziej szczegółowy opis każdego z czterech etapów wdrażania urządzeń i treści: przygotowanie środowiska, konfigurację urządzeń, wdrażanie ich i zarządzanie nimi. Działania, które powinna podjąć organizacja, zależą od przyjętego modelu własności.

1. Przygotowanie

Po określeniu odpowiedniego dla organizacji modelu wdrażania należy podjąć przedstawione poniżej kroki, które odpowiednio przygotują środowisko. Działania te można rozpocząć jeszcze przed otrzymaniem urządzeń.

Ocena istniejącej infrastruktury

iPhone'a i iPada można bezproblemowo zintegrować z większością korporacyjnych środowisk informatycznych. Ocena posiadanej infrastruktury sieciowej jest bardzo ważna dla pełnego wykorzystania potencjału systemów iOS i iPadOS.

Wi-Fi i sieć

Stały, niezawodny dostęp do sieci bezprzewodowej jest niezbędny do konfigurowania urządzeń z systemami iOS i iPadOS. Ponadto firmowa sieć Wi-Fi powinna w razie potrzeby obsłużyć dużą liczbę urządzeń — gdyby wszyscy pracownicy zechcieli łączyć się z nią jednocześnie. Może okazać się, że konieczne jest skonfigurowanie serwera proxy WWW lub portów w zaporze sieciowej, jeśli urządzenia nie mają dostępu do serwerów aktywacji Apple, usług iCloud lub App Store. Ponadto komunikacja iPhone'a i iPada z bezprzewodową siecią Cisco została zoptymalizowana przez Apple i Cisco, by umożliwić korzystanie z innych zaawansowanych funkcji sieciowych, takich jak szybkie przemieszczanie urządzeń między punktami dostępu (roaming) czy optymalizacja jakości usług (QoS — Quality of Service) dla aplikacji.

Ocena infrastruktury VPN pozwala upewnić się, czy użytkownicy mają bezpieczny zdalny dostęp do zasobów firmowych ze swoich urządzeń z systemami iOS i iPadOS. Warto rozważyć użycie funkcji „VPN na żądanie” lub „Izolowana VPN” w systemie iOS i iPadOS, tak aby połączenie VPN było nawiązywane tylko wtedy, gdy jest potrzebne. Jeżeli bramy VPN mają obsługiwać te funkcje, należy je odpowiednio skonfigurować i zakupić tyle licencji, by zaspokoić potrzeby planowanej liczby użytkowników i połączeń.

Powinno się też sprawdzić, czy infrastruktura sieciowa jest odpowiednio skonfigurowana i będzie poprawnie współpracować z Bonjour — protokołem sieciowym Apple, który nie wymaga konfiguracji i bazuje na standardach branżowych. Bonjour umożliwia urządzeniom automatyczne znajdowanie usług w sieci. Urządzenia z systemami iOS i iPadOS używają protokołu Bonjour do nawiązywania połączeń z drukarkami zgodnymi z protokołem AirPrint oraz urządzeniami zgodnymi z protokołem AirPlay, takimi jak Apple TV. Niektóre aplikacje mogą także za pośrednictwem Bonjour odnajdywać inne urządzenia, umożliwiając użytkownikom współpracę i wymianę plików.

Więcej informacji o sieciach Wi-Fi i funkcjach sieciowych:
support.apple.com/guide/deployment-reference-ios

Więcej informacji o protokole Bonjour:
developer.apple.com/library

Poczta, kontakty i kalendarze

W przypadku korzystania z serwera Microsoft Exchange należy sprawdzić, czy usługa ActiveSync jest aktualna i skonfigurowana tak, by mogli z niej korzystać wszyscy użytkownicy sieci. Jeśli organizacja korzysta z usługi Office 365 w chmurze, należy upewnić się, że posiadane licencje wystarczą do obsługi planowanej liczby podłączonych urządzeń z systemami iOS i iPadOS. Systemy iOS i iPadOS obsługują także mechanizmy nowoczesnego uwierzytelniania w aplikacjach Office 365, korzystające z protokołu OAuth 2.0 i uwierzytelniania wieloczynnikowego. Korzystanie z serwera Exchange nie jest konieczne, ponieważ systemy iOS i iPadOS współdziałają także z innymi serwerami obsługującymi standardy branżowe, np. IMAP, POP, SMTP, CalDAV, CardDAV czy LDAP.

Magazyn zawartości

Magazyn zawartości, będący jedną z funkcji systemów od macOS High Sierra wzwyż, lokalnie przechowuje treści często pobierane z serwerów Apple. Rozwiązanie to minimalizuje obciążenie łącza internetowego przez użytkowników pozyskujących te materiały w sieci należącej do instytucji. Magazyn zawartości przyspiesza pobieranie i dostarczanie oprogramowania za pośrednictwem App Store, Mac App Store oraz Apple Books.

Magazyn zawartości może także buforować uaktualnienia oprogramowania, aby urządzenia z systemami iOS i iPadOS pobierały je szybciej. Z magazynem zawartości związana jest usługa Tethered Caching, która umożliwia komputerowi Mac udostępnianie połączenia internetowego — przez interfejs USB — wielu urządzeniom z systemami iOS i iPadOS.

Więcej informacji o magazynie zawartości:
support.apple.com/guide/deployment-reference-macos

Więcej informacji o usłudze Tethered Caching:
support.apple.com/HT207523

Wybór rozwiązania MDM

Architektura zarządzania Apple dla systemów iOS i iPadOS pozwala organizacjom na bezpieczne rejestrowanie urządzeń w środowisku korporacyjnym, bezprzewodowe konfigurowanie i aktualizowanie ustawień, monitorowanie przestrzegania zasad, wdrażanie aplikacji i książek oraz zdalne wymazywanie lub blokowanie zarządzanych urządzeń. Realizację tych funkcji zarządzania umożliwiają rozwiązania MDM innych firm.

Na rynku dostępny jest szereg dostosowanych do różnych platform rozwiązań MDM. Rozwiązania te oferują różne konsole zarządzania, różne funkcje i są dostępne w różnych przedziałach cenowych. Przed wyborem rozwiązania warto zapoznać się z wymienionymi poniżej materiałami, które pomogą wybrać funkcje zarządzania najważniejsze dla organizacji. Oprócz rozwiązań MDM innych firm dostępne jest też narzędzie Profile Manager od Apple, będące składnikiem oprogramowania macOS Server.

Więcej informacji o zarządzaniu urządzeniami i firmowymi danymi:
apple.com/pl/business/docs/resources/Managing_Devices_and_Corporate_Data_on_iOS.pdf

Rejestracja w usłudze Apple Business Manager

Apple Business Manager to portal WWW przeznaczony dla administratorów IT, który umożliwia wdrażanie urządzeń iPhone, iPad, iPod touch, Apple TV i Mac w sposób scentralizowany — z jednego miejsca. Dzięki bezproblemowej współpracy z systemem zarządzania urządzeniami mobilnymi (Mobile Device Management, MDM) używanym w tej samej firmie lub instytucji, Apple Business Manager ułatwia automatyzację wdrażania urządzeń, kupowanie aplikacji, dystrybucję treści i tworzenie zarządzanych kont Apple ID dla pracowników.

Program rejestracji urządzeń (Device Enrollment Program, DEP) i program zakupów grupowych (Volume Purchase Program, VPP) zostały włączone do portalu Apple Business Manager, zatem wszystkie funkcje potrzebne organizacji do wdrażania urządzeń Apple są dostępne w jednym miejscu. Począwszy od 1 grudnia 2019 roku programy te nie będą już dostępne.

Urządzenia

Apple Business Manager umożliwia zautomatyzowaną rejestrację urządzeń, udostępniając szybką, sprawną metodę wdrażania urządzeń Apple należących do firmy oraz rejestracji w systemie MDM bez fizycznej interakcji z urządzeniami i bez konieczności ich przygotowywania.

- Poprzez usprawnienie wykonania odpowiednich kroków w Asystencie ustawień możliwe jest uproszczenie procesu konfiguracji z perspektywy użytkownika, tak by pracownicy dysponowali właściwie skonfigurowanym urządzeniem od razu po aktywacji. Zespoły IT mogą teraz w szerszym zakresie adaptować proces konfiguracji, przez który przechodzą pracownicy, wprowadzając do niego tekst zgody, elementy marki firmy lub nowoczesne mechanizmy uwierzytelniania.
- Nadzór — czyli dodatkowe mechanizmy niedostępne w innych modelach wdrożenia, takie jak niewyłączalne zarządzanie MDM — zapewnia wyższy poziom kontroli nad urządzeniami należącymi do firmy.
- Zarządzanie domyślnymi serwerami MDM jest łatwiejsze, ponieważ można przyporządkować je do określonych rodzajów urządzeń. Za pomocą aplikacji Apple Configurator 2 można także ręcznie rejestrować urządzenia iPhone, iPad i Apple TV niezależnie od tego, w jaki sposób zostały nabyte.

Treści

Apple Business Manager umożliwia organizacjom łatwe hurtowe kupowanie treści. Niezależnie od tego, czy pracownicy używają iPhone'ów, iPadów czy Maców, można w elastyczny i bezpieczny sposób udostępniać im atrakcyjne treści od razu gotowe do wykorzystania.

- Aplikacje, książki i aplikacje niestandardowe — w tym opracowane wewnętrznie przez organizację — można kupować hurtowo. Przenoszenie licencji na aplikacje między lokalizacjami i współużytkowanie licencji przez różnych nabywców z tej samej lokalizacji nie sprawia żadnych trudności. Oprócz tego dostępna jest ogólna lista historii zakupów zawierająca informacje o liczbie licencji aktualnie użytkowanych za pośrednictwem rozwiązania MDM.
- Aplikacje i książki można dystrybuować bezpośrednio do zarządzanych urządzeń lub autoryzowanych użytkowników i bez trudu sprawdzać, jakie treści zostały przydzielone do danego użytkownika lub urządzenia. Dzięki zarządzanej dystrybucji można sprawować kontrolę nad całym procesem udostępniania, zachowując przy tym pełną własność aplikacji. Gdy aplikacja przestanie być potrzebna użytkownikowi lub na urządzeniu, można cofnąć uprawnienia do korzystania z niej i przekazać je innemu użytkownikowi lub przenieść na inne urządzenie w organizacji.
- Zakupu można dokonać za pomocą różnych metod płatności, na przykład przy użyciu karty kredytowej lub na podstawie zamówienia. Organizacje mogą

również kupować środki w programie na zakupy hurtowe (tam, gdzie opcja ta jest oferowana) — bezpośrednio od Apple lub od sprzedawców Apple Authorized Reseller — o określonych kwotach wyrażonych w walucie lokalnej, które są następnie elektronicznie wysyłane właścicielowi konta w formie środków na zakupy.

- Dystrybucję aplikacji można prowadzić w wielu krajach, udostępniając je urządzeniom i użytkownikom we wszystkich państwach, w których te aplikacje są dostępne. Deweloperzy mogą udostępniać swoje aplikacje w wielu krajach w ramach standardowego procesu publikowania w App Store.

Uwaga: W niektórych krajach lub regionach zakup książek w portalu Apple Business Manager nie jest możliwy. Informacje o tym, gdzie poszczególne funkcje i metody zakupu są dostępne, znajdują się na stronie support.apple.com/HT207305.

Użytkownicy

Apple Business Manager umożliwia organizacjom tworzenie dla pracowników kont zintegrowanych z istniejącą już infrastrukturą, które pozwalają na dostęp do aplikacji i usług Apple oraz do samego portalu Apple Business Manager, a także zarządzanie tymi kontami.

- Zarządzane konta Apple ID utworzone dla pracowników służą im do zespołowej pracy z wykorzystaniem aplikacji i usług Apple, a także dają dostęp do danych związanych z pracą w aplikacjach zarządzanych korzystających z iCloud Drive. Każda organizacja jest właścicielem takich kont i sprawuje nad nimi kontrolę.
- Połączenie portalu Apple Business Manager z usługą Microsoft Azure Active Directory otwiera drogę do uwierzytelniania federacyjnego. Zarządzane konto Apple ID dla pracownika tworzone będzie automatycznie, gdy tylko zaloguje się on po raz pierwszy, używając swoich dotychczasowych danych uwierzytelniających, na zgodnym urządzeniu Apple.
- Nowa funkcja Rejestracja użytkownika w systemach iOS 13, iPadOS i macOS Catalina pozwala na korzystanie z zarządzanych kont Apple ID równolegle z prywatnymi kontami Apple ID na prywatnych urządzeniach 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.
- Aby efektywnie zarządzać urządzeniami, aplikacjami i kontami w portalu Apple Business Manager, warto przydzielić członkom zespołów IT odpowiednie inne role. Rola Administratora pozwala na zaakceptowanie, w razie potrzeby, formalnych warunków i zasad oraz łatwe przeniesienie odpowiedzialności w wypadku, gdy ktoś opuści organizację.

Uwaga: Funkcja Rejestracja użytkownika nie obsługuje obecnie iCloud Drive. iCloud Drive można używać z zarządzanym kontem Apple ID tylko wtedy, gdy jest to jedyne konto Apple ID na urządzeniu.

Więcej informacji o usłudze Apple Business Manager: www.apple.com/pl/business/it

Rejestracja w programie Apple Developer Enterprise Program

Program Apple Developer Enterprise Program oferuje kompletny zestaw narzędzi do tworzenia i testowania aplikacji oraz przekazywania ich użytkownikom. Aplikacje mogą być udostępniane na serwerze WWW lub za pomocą rozwiązania MDM. Aplikacje i programy instalacyjne na Maca mogą być podpisywane i poświadczane identyfikatorem dewelopera rozpoznawanym przez funkcję Gatekeeper, która chroni system macOS przed złośliwym oprogramowaniem.

Więcej informacji o programie Developer Enterprise Program: developer.apple.com/programs/enterprise

2. Konfiguracja

Na tym etapie należy skonfigurować urządzenia i rozdystrybuować treści, używając do tego usługi Apple Business Manager, rozwiązania MDM lub opcjonalnie aplikacji Apple Configurator 2. Istnieją różne strategie konfiguracji, a wybór jednej z nich zależeć będzie od modelu własności urządzeń i preferowanego typu wdrożenia.

Konfiguracja urządzeń

Firma ma do wyboru wiele różnych opcji udostępniania pracownikom swoich usług. Dział IT może skonfigurować urządzenia, udostępniając użytkownikom profile konfiguracji. W przypadku urządzeń nadzorowanych dostępne są dodatkowe opcje konfiguracji.

Konfiguracja urządzeń za pośrednictwem MDM

Urządzeniami, które zostały bezpiecznie zarejestrowane na serwerze MDM, można zarządzać przy użyciu profili konfiguracji — plików XML umożliwiających przesyłanie szczegółów konfiguracji do urządzeń z systemami iOS i iPadOS. Profile te automatyzują konfigurowanie ustawień, kont, ograniczeń i poświadczeń. Można je przesyłać zdalnie z rozwiązania MDM, dzięki czemu świetnie nadają się do zautomatyzowanego konfigurowania wielu urządzeń. Profile konfiguracji można przesyłać do urządzeń w formie załączników do wiadomości e-mail, pobierać ze strony WWW lub instalować na urządzeniach za pomocą narzędzia Apple Configurator 2.

- **Urządzenia należące do organizacji.** Apple Business Manager umożliwia automatyczną rejestrację urządzeń użytkowników w systemie MDM w momencie aktywacji. Wszystkie urządzenia z systemami iOS i iPadOS zarejestrowane w usłudze Apple Business Manager są zawsze nadzorowane i obowiązkowo muszą być zarejestrowane w systemie MDM.
- **Urządzenia będące własnością użytkowników.** Pracownik może zadecydować o rejestracji urządzenia w systemie MDM. W każdej chwili może też zakończyć relację urządzenia z serwerem MDM, usuwając z niego profil konfiguracyjny, co powoduje jednoczesne usunięcie firmowych danych i ustawień. Warto jednak zachęcać użytkowników do utrzymywania zgody na obejmowanie ich urządzeń zarządzaniem. Można na przykład uwarunkować dostęp do sieci Wi-Fi zarejestrowaniem urządzenia w systemie MDM. System MDM będzie wówczas automatycznie podawał dane uwierzytelniające do sieci Wi-Fi.

Po rejestracji danego urządzenia administrator może wprowadzić przez system MDM zasady, a także zainicjować zapytanie lub polecenie. To, jakie czynności administracyjne można wykonać w odniesieniu do urządzenia, zależy od metody sprawowania nadzoru i rejestracji. Urządzenie z systemem iOS lub iPadOS odbiera następnie powiadomienie o działaniach administratora wygenerowane za pomocą usługi aktywnych powiadomień Apple (Apple Push Notification service, APNs) i może w bezpieczny sposób komunikować się bezpośrednio ze swoim serwerem MDM. Wystarczy połączenie sieciowe, aby urządzenia otrzymywały polecenia APNs w dowolnym miejscu na świecie. Za pomocą usługi APNs nie są jednak przesyłane żadne poufne lub zastrzeżone informacje.

Konfigurowanie urządzeń za pomocą Apple Configurator 2 (opcjonalnie)

Do przeprowadzenia początkowej fazy wdrożenia wielu urządzeń w środowisku lokalnym organizacja może użyć narzędzia Apple Configurator 2. Ta bezpłatna

aplikacja dla systemu macOS umożliwia podłączenie urządzenia z systemem iOS lub iPadOS do Maca przez interfejs USB i uaktualnienie na nim systemu iOS lub iPadOS do najnowszej wersji, skonfigurowanie jego ustawień i ograniczeń, a także zainstalowanie aplikacji i innych treści. Po wstępnej konfiguracji można nadal zarządzać urządzeniami zdalnie, drogą bezprzewodową, korzystając z systemu MDM.

Interfejs użytkownika aplikacji Apple Configurator 2 ułatwia koncentrację na urządzeniach i wykonywanych wobec nich zadaniach. Aplikacja współdziała z usługą Apple Business Manager, dzięki czemu urządzenia rejestrują się w systemie MDM automatycznie przy użyciu ustawień organizacji. Apple Configurator 2 pozwala także na definiowanie niestandardowych kolejek czynności na podstawie wzorców.

Więcej informacji o narzędziu Apple Configurator 2:
support.apple.com/apple-configurator

Urządzenia nadzorowane

Dzięki nadzorowi organizacja może korzystać z dodatkowych funkcji zarządzania na posiadanych przez siebie urządzeniach z systemami iOS i iPadOS, np. ograniczania dostępu do AirDrop lub przełączania urządzeń w tryb jednej aplikacji (Single App Mode, SAM). Funkcje nadzoru obejmują też filtrowanie połączeń WWW przez globalny serwer proxy, dzięki czemu organizacja może, między innymi, egzekwować korzystanie z Internetu zgodnie z przyjętymi zasadami, a także uniemożliwić użytkownikom przywrócenie ustawień fabrycznych urządzenia. Domyślnie wszystkie urządzenia z systemami iOS i iPadOS są nienadzorowane. Nadzór można włączyć za pomocą usługi Apple Business Manager lub ręcznie, korzystając z aplikacji Apple Configurator 2.

Nawet jeśli nie planuje się korzystania z funkcji dostępnych tylko dla urządzeń nadzorowanych, warto w trakcie konfiguracji rozważyć uruchomienie nadzorowania urządzeń, tak by mieć dostęp do takich funkcji w przyszłości. Bez tego może okazać się, że konieczne będzie wymazanie zawartości z już użytkowanych urządzeń. Nadzorowanie nie polega na ograniczaniu dostępu do funkcji urządzeń, umożliwia natomiast organizacji bardziej zaawansowane zarządzanie posiadanymi przez nią urządzeniami. W dłuższej perspektywie czasowej nadzorowanie może zapewnić firmie dostęp do jeszcze szerszych możliwości.

Więcej informacji o ograniczeniach dotyczących urządzeń nadzorowanych:
support.apple.com/guide/mdm

Dystrybucja aplikacji i książek

Apple oferuje szeroko zakrojone programy wspierające organizacje w skutecznym wykorzystaniu fantastycznych aplikacji oraz treści dostępnych dla systemów iOS i iPadOS. Umożliwiają one udostępnianie urządzeniom i użytkownikom aplikacji i książek zakupionych za pomocą usługi Apple Business Manager, a także aplikacji stworzonych przez samą organizację, by użytkownicy mieli wszystko, czego potrzeba do wydajnej pracy. Podczas dokonywania zakupu należy wybrać metodę rozpowszechniania treści: zarządzaną dystrybucję lub kody dostępu.

Zarządzanie dystrybucją

W ramach zarządzanej dystrybucji można za pomocą rozwiązania MDM lub narzędzia Apple Configurator 2 zarządzać aplikacjami i książkami zakupionymi w sklepie Apple Business Manager w dowolnym kraju, w którym aplikacja jest dostępna. Aby korzystać z dystrybucji zarządzanej, należy najpierw połączyć rozwiązanie MDM z kontem w usłudze Apple Business Manager za pomocą bezpiecznego tokenu. Gdy serwer MDM jest już połączony z usługą Apple Business Manager, zakupione w niej aplikacje i książki można przypisać do urządzenia, nawet jeśli jest na nim zablokowana obsługa App Store.

- **Przydzielanie aplikacji do urządzeń.** Aplikacje można przypisać bezpośrednio do urządzenia za pomocą rozwiązania MDM lub narzędzia Apple Configurator 2. Funkcja ta umożliwia pominięcie kilku kroków podczas wstępnego wdrożenia. Znacznie ułatwia to i przyspiesza cały proces, a jednocześnie pozwala zachować pełną kontrolę nad zarządzanymi urządzeniami i treścią. Po przypisaniu aplikacji do urządzenia zostaje ona do niego aktywnie przesłana za pośrednictwem systemu MDM — nie trzeba nawet wysyłać zaproszeń do użytkowników. Aplikacja jest dostępna dla wszystkich użytkowników danego urządzenia.
- **Przydzielanie aplikacji i książek użytkownikom.** Alternatywna metoda polega na wykorzystaniu rozwiązania MDM do zapraszania użytkowników do pobierania aplikacji i książek za pośrednictwem wiadomości e-mail lub aktywnych powiadomień. Aby zaakceptować zaproszenie, użytkownicy logują się na swoich urządzeniach za pomocą osobistego konta Apple ID. Konto Apple ID jest rejestrowane w usłudze Apple Business Manager, ale pozostaje całkowicie poufne i niewidoczne dla administratora. Z chwilą przyjęcia zaproszenia użytkownik zostaje połączony z serwerem MDM instytucji i może już otrzymywać przypisane mu aplikacje i książki. Aplikacje są automatycznie dostępne do pobrania na wszystkie urządzenia użytkowników bez żadnych dodatkowych czynności ani kosztów po stronie organizacji.

Kiedy przydzielone aplikacje nie są już potrzebne danym użytkownikom lub na danych urządzeniach, można cofnąć uprawnienia do korzystania z tych aplikacji i przekazać je innym urządzeniom lub użytkownikom. W rezultacie organizacja zachowuje pełną kontrolę nad zakupionymi aplikacjami oraz prawo własności do nich. Raz przydzielone książki stają się jednak własnością użytkowników i nie mogą im zostać odebrane ani przekazane komuś innemu.

Kody wykupu

Treści można też rozpowszechniać za pomocą kodów wykupu. Ta metoda jest przydatna, gdy organizacja nie może objąć urządzeń użytkowników zarządzaniem w systemie MDM — na przykład dlatego, że urządzenia te należą do franczyzobiorcy. Aplikacja lub książka zostaje w tym wypadku na stałe przypisana do użytkownika, który zrealizował kod wykupu. Kody wykupu są dostarczane instytucji w formie arkusza kalkulacyjnego. Do każdej aplikacji lub książki — w liczbie zakupionej przez instytucję — przydzielony zostaje unikalny kod wykupu. Po każdym użyciu któregoś z kodów arkusz kalkulacyjny zostaje zaktualizowany w sklepie Apple Business Manager. Dzięki temu można w każdej chwili sprawdzić, ile niewykorzystanych kodów jeszcze zostało. Kody można udostępniać za pośrednictwem rozwiązania MDM, narzędzia Apple Configurator 2, poczty e-mail lub wewnętrznej strony WWW.

Instalacja aplikacji i treści za pomocą narzędzia Apple Configurator 2 (opcjonalnie)
Oprócz definiowania podstawowych ustawień i konfigurowania urządzeń aplikacja Apple Configurator 2 może także służyć do instalowania aplikacji i treści na urządzeniach przygotowywanych w imieniu użytkownika. W przypadku wdrożenia z opcją personalizacji możliwe jest wstępne zainstalowanie aplikacji, co przekłada się na oszczędność czasu i zmniejszenie obciążenia sieci. We wdrożeniach urządzeń bez opcji personalizacji możliwe jest kompleksowe skonfigurowanie urządzenia, do ekranu początkowego włącznie. Konfigurując urządzenia za pomocą narzędzia Apple Configurator 2, można instalować aplikacje z App Store, aplikacje stworzone na specjalne zamówienie oraz dokumenty. Dla aplikacji z App Store wymagana jest usługa Apple Business Manager. Dokumenty są obsługiwane przez aplikacje, które umożliwiają udostępnianie plików. Aby przejrzeć lub pobrać dokument z urządzenia z systemem iOS lub iPadOS, należy podłączyć je do Maca z zainstalowaną aplikacją Apple Configurator 2.

3. Wdrożenie

Pracownik, otrzymując do dyspozycji iPhone'a lub iPada, może bardzo szybko przygotować urządzenie do pracy, i to bez wsparcia działu IT.

Dystrybucja urządzeń

Po przeprowadzeniu dwóch pierwszych etapów wdrażania, czyli przygotowania i konfiguracji, urządzenia można przekazać pracownikom. W wypadku wdrożenia z możliwością personalizacji urządzenia należy przekazać użytkownikom, którzy dzięki usprawnionej konfiguracji w Asystencie ustawień będą mogli ostatecznie dostosować je do swoich potrzeb. W wypadku wdrożenia bez możliwości personalizacji urządzenia należy przekazać użytkownikom pracującym na danej zmianie lub umieścić na stanowiskach służących do ładowania i bezpiecznego przechowywania.

Asystent konfiguracji
Dzięki Asystentowi ustawień użytkownik zaraz po wyjęciu urządzenia z pudełka może je aktywować, skonfigurować jego podstawowe ustawienia i rozpocząć pracę. Po skonfigurowaniu ustawień podstawowych użytkownik może też określić swoje preferencje indywidualne, takie jak język, lokalizacja, Siri, iCloud i Znajdź mój iPhone. Urządzenia zarejestrowane w usłudze Apple Business Manager są automatycznie rejestrowane w systemie MDM bezpośrednio z Asystenta ustawień.

Umożliwienie użytkownikom personalizacji
Wdrożenie z możliwością personalizacji lub w modelu BYOD pozwala użytkownikom na dostosowanie urządzeń do indywidualnych potrzeb, z użyciem ich własnych kont Apple ID. Dzięki temu pracownicy sami decydują o tym, za pomocą których aplikacji i treści realizują swoje zadania i cele, co prowadzi do wzrostu ich produktywności.

Konta Apple ID i zarządzane konta Apple ID
Gdy pracownik loguje się na swoim koncie Apple ID w usługach Apple, takich jak FaceTime, iMessage, App Store czy iCloud, uzyskuje dostęp do szerokiej gamy treści ułatwiających sprawne wykonywanie zadań zawodowych oraz sprzyjających wysokiej wydajności oraz pracy zespołowej.

Tak jak wszystkie konta Apple ID, zarządzane konta Apple ID służą do logowania się na osobistym urządzeniu. Zapewniają także dostęp do usług Apple — w tym iCloud i funkcji pracy zespołowej w aplikacjach iWork i Notatki — oraz do portalu 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. Niektóre ustawienia zarządzanych kont Apple ID podlegają ograniczeniom.

Urządzenia rejestrowane za pomocą funkcji Rejestracja użytkownika wymagają zarządzanych kont Apple ID. Rejestracja użytkownika obsługuje opcjonalne osobiste konta Apple ID; pozostałe opcje rejestracji pozwalają na stosowanie albo osobistego, albo zarządzanego konta Apple ID. Tylko funkcja Rejestracja użytkownika obsługuje więcej niż jedno konto Apple ID.

Aby jak najefektywniej korzystać z tych usług, użytkownicy powinni używać własnych kont Apple ID lub założonych dla nich zarządzanych kont Apple ID. Użytkownik bez konta Apple ID może je utworzyć jeszcze przed otrzymaniem urządzenia. Jeśli użytkownik nie ma jeszcze osobistego konta Apple ID, to może je utworzyć w Asystencie ustawień. Do założenie konta Apple ID nie jest potrzebna karta kredytowa.

Informacje o zarządzanych kontach Apple ID:
support.apple.com/guide/apple-business-manager

iCloud

iCloud automatycznie synchronizuje i uaktualnia dokumenty oraz prywatne treści użytkowników — takie jak kontakty, kalendarze, pliki tekstowe i zdjęcia — na wielu urządzeniach jednocześnie. Funkcja Znajdź mój umożliwia użytkownikowi odszukanie zgubionego lub skradzionego Maca, iPhone'a, iPada lub iPoda touch. Wybrane funkcje iCloud — takie jak Pęk kluczy iCloud i iCloud Drive — można wyłączyć poprzez nałożenie ograniczeń wprowadzonych ręcznie na urządzeniu lub za pośrednictwem rozwiązania MDM. Dzięki temu organizacja ma większy wpływ na to, jakie dane są przechowywane na poszczególnych kontach.

Więcej informacji o zarządzaniu usługami iCloud:
support.apple.com/guide/deployment-reference-ios

4. Zarządzanie

Po przygotowaniu i uruchomieniu urządzeń organizacja ma do dyspozycji wiele funkcji administracyjnych, które umożliwiają ciągłe zarządzanie urządzeniami i treścią, a także ich kontrolę.

Administrowanie urządzeniami

Urządzeniami zarządzanymi można administrować z serwera MDM, realizując szereg zadań. Należy do nich wysyłanie do urządzeń zapytań, a także inicjowanie czynności administracyjnych, dzięki którym można kontrolować urządzenia, które zostały zagubione bądź skradzione lub są wykorzystywane niezgodnie z polityką instytucji.

Zapytania

Serwer MDM może kierować do urządzeń zapytania o różne dane, m.in. o informacje dotyczące sprzętu, takie jak numer seryjny, identyfikator UDID urządzenia lub adres MAC w sieci Wi-Fi, a także informacje dotyczące oprogramowania, np. wersję sytemu iOS lub iPadOS, i o szczegółową listę wszystkich aplikacji zainstalowanych na urządzeniu. Korzystając z tych danych, rozwiązanie MDM może aktualizować informacje inwentaryzacyjne, podejmować decyzje dotyczące zarządzania i automatyzować zadania administracyjne, takie jak dbanie o to, by wszyscy użytkownicy dysponowali odpowiednimi aplikacjami.

Zadania administracyjne

Serwer MDM może wydawać zarządzanym urządzeniom wiele różnych poleceń administracyjnych — na przykład zmienić ustawienia konfiguracyjne bez interakcji z użytkownikiem, uaktualnić oprogramowanie na urządzeniu zabezpieczonym kodem, zdalnie zablokować urządzenie lub wymazać jego zawartość oraz skasować zapomniany przez użytkownika kod, aby umożliwić mu ustawienie nowego. Serwer MDM może także zażądać od iPhone'a lub iPada rozpoczęcia klonowania AirPlay na konkretne urządzenie lub zakończenia bieżącej sesji AirPlay.

Zarządzane uaktualnienia oprogramowania

Użytkownikowi można na pewien czas uniemożliwić ręczne uaktualnienie systemu przez sieć bezprzewodową. Po wprowadzeniu tego ograniczenia domyślny okres blokowania wynosi 30 dni od momentu wydania przez Apple uaktualnionej wersji iOS lub iPadOS. Domyślny okres blokowania uaktualnień można dowolnie zmienić na inny, trwający od 1 do 90 dni. Oprócz tego uaktualnianie oprogramowania na urządzeniach nadzorowanych można zaplanować przy użyciu MDM.

Tryb Utracony

System MDM może zdalnie przełączyć nadzorowane urządzenie w tryb Utracony. Po włączeniu tego trybu urządzenie zostaje zablokowane i pojawia się na nim ekran blokady z komunikatem zawierającym numer telefonu. Zagubione lub skradzione urządzenie nadzorowane, które przełączono w tryb Utracony, można zlokalizować, ponieważ system MDM zdalnie przesyła do niego zapytanie o lokalizację w momencie ostatniego połączenia z siecią. Tryb Utracony nie wymaga do działania włączonej funkcji Znajdź mój iPhone.

Blokada aktywacji

W systemie iOS 7.1 lub jego nowszej wersji rozwiązanie MDM umożliwia włączenie blokady aktywacji, gdy użytkownik uruchomi na urządzeniu nadzorowanym funkcję Znajdź mój Dzięki temu organizacja może korzystać ze zniechęcającej złodziei blokady aktywacji, mając jednak możliwość jej ominięcia, gdy użytkownik nie może przeprowadzić uwierzytelnienia za pomocą konta Apple ID.

Wdrożenie dodatkowych treści i zarządzanie nimi

Organizacje często muszą przesyłać użytkownikom aplikacje, które umożliwiają im produktywną pracę. Jednocześnie ważne jest, by zachować kontrolę nad sposobem, w jaki aplikacje nawiązują połączenie z zasobami wewnętrznymi, a także nad bezpieczeństwem danych, kiedy użytkownik zmienia miejsce pracy — nie ingerując przy tym w jego prywatne aplikacje oraz dane.

Wewnętrzne portale z aplikacjami

Większość serwerów MDM oferuje wewnętrzne portale z aplikacjami. Można też utworzyć własny wewnętrzny portal z aplikacjami dla pracowników, w którym łatwo znajdą aplikacje dla swoich iPhone'ów i iPadów. Taki portal może posłużyć jako centralne miejsce udostępniania zasobów użytkownikom, w którym instytucja umieszcza aplikacje stworzone na jej specjalne zamówienie, adresy URL aplikacji z App Store, kody dla usługi Apple Business Manager lub aplikacje niestandardowe. Zarządzanie taką stroną i jej zabezpieczanie może przebiegać w sposób scentralizowany. Dzięki wewnętrznemu portalowi z aplikacjami pracownicy mogą łatwo znaleźć zatwierdzone do użytku zasoby i nie muszą w tym celu kontaktować się z zespołem IT.

Treść zarządzana

Mechanizmy zarządzania treścią obejmują instalację, konfigurację, obsługę oraz usuwanie aplikacji z App Store i aplikacji opracowanych na zamówienie, kont, książek i dokumentów.

- **Zarządzane aplikacje.** W systemach iOS i iPadOS organizacja używająca funkcji aplikacji zarządzanych może za pomocą systemu MDM zdalnie udostępniać użytkownikom bezpłatne, płatne i korporacyjne aplikacje, korzystając jednocześnie z odpowiedniej ochrony danych firmowych i nie naruszając prywatności użytkowników. Aplikacje zarządzane można usunąć zdalnie za pomocą serwera MDM lub w wyniku usunięcia przez użytkownika jego urządzenia z systemu MDM. Wraz z aplikacją zostają usunięte powiązane z nią dane. Jeżeli aplikacja pozostaje powiązana z użytkownikiem przez usługę Apple Business Manager lub jeśli użytkownik, korzystając z osobistego konta Apple ID, zrealizował przypisany do aplikacji kod, aplikację można nadal pobrać z App Store, ale nie będzie ona już zarządzana przez system MDM.
- **Konta zarządzane.** Rozwiązanie MDM pozwala użytkownikom na szybkie rozpoczęcie pracy, automatycznie konfigurując ich pocztę e-mail i inne konta. Zależnie od dostawcy rozwiązania MDM i integracji z systemami wewnętrznymi, przypisane do konta pakiety mogą już wstępnie zostać uzupełnione o nazwę użytkownika i jego adres e-mail, a tam, gdzie ma to zastosowanie, także o tożsamości certyfikatów do uwierzytelniania i podpisywania.
- **Książki i dokumenty zarządzane.** Dzięki narzędziom MDM książki, publikacje ePub i dokumenty PDF mogą być automatycznie przesyłane do urządzeń użytkowników, tak by pracownicy zawsze mieli dostęp do potrzebnych materiałów. Książki zarządzane mogą być udostępniane tylko między innymi aplikacjami zarządzanymi i przesyłane pocztą e-mail tylko między kontami zarządzanymi. Materiały można usunąć zdalnie, gdy nie będą już potrzebne. Książki zakupione za pośrednictwem usługi Apple Business Manager mogą być objęte zarządzaną dystrybucją, ale nie można odbierać uprawnień do korzystania z nich ani zmieniać przypisania książek do użytkowników. Książki raz zakupionej przez użytkownika nie można objąć zarządzaniem, chyba że zostanie mu jednoznacznie przydzielona w usłudze Apple Business Manager.

Konfiguracja aplikacji zarządzanych

Twórca aplikacji może wskazać ustawienia i funkcje, które mają być włączane w wypadku zainstalowania jej jako aplikacji zarządzanej. Takie ustawienia konfiguracji można wprowadzić przed zainstalowaniem aplikacji zarządzanej lub później. Dział IT może na przykład ustalić dla aplikacji Sharepoint preferencje domyślne, dzięki którym użytkownik nie będzie musiał ręcznie konfigurować serwera.

Czołowi dostawcy rozwiązań MDM zrzeszyli się w społeczności AppConfig Community i opracowali schemat standardów, którego realizacja powinna ułatwiać twórcom aplikacji wyposażanie oprogramowania w obsługę konfiguracji aplikacji zarządzanych. Celem społeczności AppConfig Community jest dzielenie się narzędziami i sprawdzonymi praktykami wykorzystania możliwości natywnych w mobilnych systemach operacyjnych. Społeczność ta ułatwia swoim członkom bardziej spójne, otwarte i prostsze konfigurowanie oraz zabezpieczanie aplikacji mobilnych, przyczyniając się do coraz powszechniejszego wdrażania w firmach urządzeń mobilnych.

Więcej informacji o społeczności AppConfig:
appconfig.org

Zarządzany przepływ danych

Rozwiązania MDM oferują funkcje, które umożliwiają precyzyjne zarządzanie firmowymi danymi, zapobiegając ich wyciekom do prywatnych aplikacji i do usług chmurowych użytkowników.

- **Zarządzanie otwieraniem plików.** Zarządzanie otwieraniem plików polega na wykorzystywaniu zestawu ograniczeń, dzięki którym załączniki i dokumenty ze źródeł zarządzanych nie są otwierane w niezarządzanych miejscach docelowych — i odwrotnie. Przykładowo, możliwe jest zablokowanie otwarcia w prywatnej aplikacji użytkownika poufnego załącznika e-mail z zarządzanego konta e-mail organizacji. Taki dokument roboczy otworzą tylko aplikacje zainstalowane i zarządzane przez rozwiązanie MDM. Niezarządzane, prywatne aplikacje użytkownika nie pojawiają się na liście dostępnych aplikacji, za pomocą których można otworzyć załącznik. Oprócz zarządzanych aplikacji, kont, książek i domen ograniczenia związane z otwieraniem plików są respektowane też przez niektóre rozszerzenia.
- **Tryb jednej aplikacji.** Po włączeniu tego ustawienia na urządzeniu z systemem iOS lub iPadOS można korzystać tylko z jednej aplikacji. Takie rozwiązanie świetnie sprawdza się w wypadku kiosków interaktywnych bądź urządzeń pełniących tylko jedną funkcję, na przykład w punktach sprzedaży lub urządzeniach do rejestracji pacjentów. Oprócz tego deweloper może wyposażyć aplikację w tę funkcję, tak by autonomicznie włączała i wyłączała Tryb jednej aplikacji.
- **Zapobieganie tworzeniu kopii zapasowych.** Ta funkcja zapobiega kopiowaniu przez aplikacje zarządzane danych do iCloud lub na komputer. Zablokowanie archiwizacji uniemożliwia odtworzenie danych z aplikacji zarządzanej wtedy, gdy po usunięciu aplikacji przez system MDM użytkownik zainstaluje ją ponownie.

Opcje wsparcia

Apple oferuje szeroką gamę programów i szereg opcji wsparcia dla użytkowników urządzeń z systemami iOS i iPadOS oraz administratorów IT.

AppleCare for Enterprise

Firmy zainteresowane pełną ochroną mogą przystąpić do planu AppleCare dla przedsiębiorstw, który pozwala im odciążyć wewnętrzne centrum pomocy, zapewniając telefoniczne, całodobowe wsparcie techniczne dla pracowników i jednogodzinny czas reakcji w wypadku najpoważniejszych problemów. Program zapewnia wsparcie na poziomie działu IT dotyczące wszelkiego sprzętu i oprogramowania Apple, a także pomoc związaną z realizacją skomplikowanych scenariuszy wdrażania i integracji, w szczególności obejmujących rozwiązania MDM i Active Directory.

AppleCare OS Support

W ramach usługi AppleCare OS Support działom IT zapewniane jest telefoniczne i elektroniczne wsparcie na poziomie korporacyjnym dotyczące wdrażania systemów iOS, iPadOS, macOS i macOS Server. W zależności od zakresu wykupionej usługi może ona obejmować pomoc 24/7 i wsparcie przypisanego opiekuna technicznego. Oferując możliwość bezpośredniego zadawania pytań o integrację, migrację i problemy z zawansowaną eksploatacją serwerów specjaliście, usługa AppleCare OS Support pozwala zespołom IT efektywniej wdrażać urządzenia i zarządzać nimi, a także sprawniej rozwiązywać problemy.

AppleCare Help Desk Support

Plan AppleCare Help Desk Support umożliwia priorytetowy dostęp telefoniczny do najbardziej doświadczonych pracowników działu wsparcia Apple. Ponadto decydując się na ten plan, organizacja otrzyma pakiet narzędzi wspomagających diagnostykę i rozwiązywanie problemów ze sprzętem Apple, co pozwoli jej efektywniej zarządzać zasobami, skrócić czas reakcji na zgłoszenia i obniżyć koszty przeszkolenia. Plan wsparcia AppleCare Help Desk Support obejmuje nieograniczoną liczbę incydentów związanych z diagnostyką i rozwiązywaniem problemów dotyczących sprzętu i oprogramowania, a także z izolowaniem problemów w urządzeniach z systemami iOS i iPadOS.

AppleCare dla użytkowników urządzeń z systemami iOS i iPadOS

Każde urządzenie z systemem iOS lub iPadOS objęte jest roczną ograniczoną gwarancją oraz 90-dniowym bezpłatnym telefonicznym wsparciem technicznym. Wykupując plan ochrony AppleCare+ dla iPhone'a, AppleCare+ dla iPada lub AppleCare) dla iPoda touch, okres serwisowania można wydłużyć do dwóch lat od pierwotnej daty zakupu urządzenia. Użytkownik ma wówczas także do dyspozycji telefoniczne wsparcie techniczne świadczone przez ekspertów Apple — może dzwonić z pytaniami tak często, jak zechce. Ponadto Apple zapewnia dostęp do wygodnych form obsługi serwisowej, gdy zajdzie konieczność naprawy urządzenia. Oprócz tego plany obejmują maksymalnie dwie naprawy urządzenia w razie jego przypadkowego uszkodzenia w określonych okolicznościach. Za każdą taką naprawę klient jest obciążany opłatą serwisową.

Program iOS Direct Service

Dzięki programowi iOS Direct Service własny dział pomocy technicznej firmy może wykrywać problemy z urządzeniami bez konieczności dzwonienia na infolinię AppleCare czy wizyty w sklepie Apple Store. Jest to jedna z korzyści, jaką przynosi plan AppleCare+. W razie potrzeby organizacja może od razu zamówić na wymianę nowego iPhone'a, iPada lub iPoda touch lub dołączone akcesorium.

Więcej informacji o programach AppleCare:
apple.com/support/professional

Podsumowanie

Niezależnie od tego, czy z iPhone'ów lub Padów ma korzystać wybrana grupa pracowników, czy cała organizacja, firma ma do dyspozycji wiele rozwiązań upraszczających wdrażanie urządzeń i zarządzanie nimi. Wybór najlepszej dla firmy strategii może przyczynić się do wzrostu produktywności pracy i sprawić, że pracownicy zaczną bardziej innowacyjnie podchodzić do realizacji swoich obowiązków.

Informacje o funkcjach systemów iOS i iPadOS związanych z wdrażaniem, zarządzaniem i zabezpieczeniami:
support.apple.com/guide/deployment-reference-ios

Informacje o ustawieniach zarządzania urządzeniami mobilnymi przeznaczonych dla zespołów IT:
support.apple.com/guide/mdm

Informacje o usłudze Apple Business Manager:
support.apple.com/guide/apple-business-manager

Informacje o zarządzanych kontach Apple ID dla firm:
apple.com/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

Informacje o inicjatywie Apple w pracy:
www.apple.com/pl/business/

Informacje o funkcjach przeznaczonych dla zespołów IT:
www.apple.com/pl/business/it/

Informacje o zabezpieczeniach platform Apple:
www.apple.com/security/

Oferta programów AppleCare:
www.apple.com/support/professional/

Szkolenia i certyfikaty Apple:
training.apple.com

Kontakt z działem Apple Professional Services:
consultingservices@apple.com