Zarządzanie urządzeniami i danymi firmowymi w systemie iOS

Wprowadzenie

Spis treści

Firmy na całym świecie, chcąc ułatwić pracownikom wykonywanie obowiązków, udostępniają im iPhone'y i iPady.

Podstawą skutecznej strategii wykorzystania urządzeń mobilnych jest zrównoważenie poziomu swobody użytkowników i nadzoru działu IT. Personalizacja urządzeń iOS za pomocą własnych aplikacji i treści daje użytkownikom większe poczucie własności i odpowiedzialności, prowadząc do wzrostu ich zaangażowania i produktywności. Jest to możliwe dzięki architekturze zarządzania Apple, która wykorzystuje inteligentne sposoby odrębnej obsługi aplikacji i danych firmowych, bezproblemowo oddzielając je od danych prywatnych. Ponadto użytkownicy wiedzą, jak zarządzane są ich urządzenia i mają poczucie, że ich prywatność jest chroniona.

W tym dokumencie opisano jak sprawować podstawowy nadzór informatyczny, jednocześnie umożliwiając użytkownikom korzystanie w pracy z najlepszych narzędzi. Jest on uzupełnieniem publikacji „iOS — Podręcznik wdrażania", referencyjnego dokumentu technicznego dostępnego w sieci, który ułatwia wdrażanie i obsługę urządzeń iOS w firmie.

Publikacja „iOS — Podręcznik wdrażania" jest dostępna pod adresem help.apple.com/deployment/ios.

Podstawy zarządzania

System iOS ułatwia wdrażanie telefonów iPhone i iPadów, korzystając z szerokiej gamy wbudowanych mechanizmów, które upraszczają konfigurację konta i zasad użytkowania oraz umożliwiają dystrybucję aplikacji i zdalne ograniczanie dostępu do pewnych funkcji urządzeń.

Nasza koncepcja zarządzania

Architektura zarządzania Apple jest fundamentem systemu obsługi urządzeń mobilnych. Ponieważ ta architektura stanowi część systemu iOS, organizacje mogą — minimalnym nakładem pracy — zarządzać wszystkimi urządzeniami w pełnym zakresie, nie tylko blokowaniem i ograniczaniem dostępu do funkcji. Dzięki temu architektura zarządzania Apple umożliwia precyzyjne sterowanie urządzeniami, aplikacjami i danymi za pomocą rozwiązań do zarządzania urządzeniami mobilnymi (MDM) innych firm. Co najważniejsze organizacja może sprawować nadzór na pożądanym przez siebie poziomie bez obniżania satysfakcji pracowników i skali ochrony ich prywatności.

W innych dostępnych systemach zarządzania urządzeniami funkcja MDM może nosić różne nazwy, np. zarządzania firmowymi rozwiązaniami mobilnymi (EMM) lub zarządzania aplikacjami mobilnymi (MAM). Wszystkie te rozwiązania są przeznaczone do tego samego — bezprzewodowego zdalnego zarządzania firmowymi urządzeniami i danymi. Ponieważ architektura zarządzania Apple jest częścią systemu iOS, jego użytkownik nie potrzebuje osobnej aplikacji agentowej od dostawcy swojego rozwiązania MDM.

Oddzielanie danych firmowych od prywatnych

Niezależnie od tego, czy organizacja obsługuje prywatne urządzenia pracowników, czy urządzenia firmowe, możliwa jest ich kompleksowa obsługa informatyczna przy jednoczesnym utrzymaniu pełnej produktywności pracowników. Dane prywatne i zawodowe są zarządzane oddzielnie, nie ma jednak różnic w komforcie ich użytkowania. Dzięki temu na urządzeniu mogą znajdować się i aplikacje firmowe, i najnowsze aplikacje biurowe, co daje pracownikom swobodę w wyborze narzędzi pracy. System iOS nie potrzebuje do tego rozwiązań innych firm, np. kontenerów, które utrudniają korzystanie z urządzenia, budząc irytację użytkowników.

Zrozumienie różnych modeli zarządzania

Częstą rolą kontenerów jest rozwiązywanie problemów na innych platformach — problemów nieobecnych w systemie iOS. Niektóre kontenery korzystają ze strategii „dwóch wcieleń", która polega na uruchomieniu na jednym urządzeniu dwóch osobnych środowisk. Inne skupiają się na kontenerowaniu aplikacji za pomocą opartej na kodzie integracji lub rozwiązań do opakowywania aplikacji. Wszystkie te metodologie ograniczają produktywność użytkowników — np. poprzez logowanie i wylogowywanie się z różnych środowisk pracy lub dodawanie zależności do zastrzeżonego kodu, które często powodują niezgodność aplikacji z aktualizacjami systemu operacyjnego.

Organizacje, które zrezygnowały z kontenerów, zauważają, że natywne mechanizmy kontroli zarządzania systemu iOS zapewniają użytkownikom optymalny komfort pracy, zwiększając przy tym ich produktywność. Zamiast utrudniać użytkownikom korzystanie z urządzeń do celów służbowych i prywatnych, można wdrożyć mechanizmy kontroli przestrzegania zasad, które dyskretnie i bezproblemowo zarządzają przepływem danych.

Zarządzanie danymi firmowymi

Z systemem iOS nie trzeba ograniczać funkcjonalności posiadanych urządzeń. Najważniejsze technologie kontrolują przepływ danych firmowych między aplikacjami i chronią przed ich wyciekiem do prywatnych aplikacji użytkownika lub usług chmurowych.

Treść zarządzana

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

- **Aplikacje zarządzane.** Aplikacje zarządzane to aplikacje zainstalowane za pomocą rozwiązania MDM. Mogą być to płatne i bezpłatne aplikacje z App Store lub oprogramowanie zaprojektowane na specjalne zamówienie. Wszystkie można zainstalować zdalnie za pomocą rozwiązania MDM. Aplikacje zarządzane zawierają często informacje poufne i oferują bardziej zaawansowany nadzór niż aplikacje pobierane przez użytkowników. Za pomocą serwera MDM można wymusić usuwanie zarządzanych aplikacji wraz z powiązanymi danymi oraz określić, czy aplikacje zostaną usunięte po usunięciu profilu MDM. Dodatkowo serwer MDM może zablokować tworzenie kopii zapasowych zarządzanych aplikacji w iTunes lub iCloud.
- **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. Rozwiązanie MDM może skonfigurować następujące typy kont: IMAP/POP, CalDAV, kalendarze subskrybowane, CardDAV, Exchange ActiveSync i LDAP.
- **Książki zarządzane.** Dzięki rozwiązaniu MDM książki, książki 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 będą już niepotrzebne.
- **Domeny zarządzane.** Materiały pobierane z Safari są dokumentami zarządzanymi wtedy, gdy pochodzą z domen zarządzanych. Zarządzane mogą być konkretne adresy URL i subdomeny. Przykładowo, gdy użytkownik pobiera plik PDF z domeny zarządzanej, domena wymaga, by plik PDF spełniał kryteria dokumentów zarządzanych. Domyślnie ścieżki w domenie są zarządzane.

Zarządzana dystrybucja aplikacji

Dzięki dystrybucji zarządzanej można zarządzać aplikacjami i książkami zakupionymi w ramach programu Volume Purchase Program (VPP) za pomocą rozwiązania MDM lub narzędzia Apple Configurator 2. Aby korzystać z dystrybucji zarządzanej, należy najpierw połączyć rozwiązanie MDM z kontem VPP za pomocą bezpiecznego tokenu. Gdy serwer MDM jest już połączony z usługą VPP, przypisanie aplikacji bezpośrednio do urządzenia nie wymaga od użytkownika nawet identyfikatora Apple ID. Użytkownik dostaje powiadomienie, gdy aplikacje są gotowe do zainstalowania na urządzeniu. W przypadku urządzeń nadzorowanych przeprowadzana jest cicha instalacja aplikacji bez powiadamiania o niej użytkownika.

Aby za pomocą rozwiązania MDM uzyskać pełną kontrolę nad aplikacjami, należy przypisać je bezpośrednio do urządzenia.

Konfiguracja aplikacji zarządzanych

W przypadku konfiguracji aplikacji zarządzanych rozwiązanie MDM wykorzystuje natywną architekturę zarządzania iOS do konfiguracji aplikacji w trakcie wdrażania lub po wdrożeniu. Ta architektura umożliwia twórcom oprogramowania definiowanie ustawień konfiguracji, które powinny zostać zaimplementowane w trakcie instalowania ich aplikacji jako aplikacji zarządzanej. Pracownicy mogą od razu rozpocząć korzystanie z aplikacji, która została w ten sposób skonfigurowana, nie wprowadzając już żadnych ustawień własnych. Oprócz tego dział IT ma pewność, że firmowe dane są w aplikacjach bezpieczne, a zastrzeżone pakiety SDK i opakowywanie aplikacji są zbędne.

Twórcy aplikacji mogą korzystać z funkcji włączanych przy konfiguracji aplikacji zarządzanych, takich jak funkcja konfiguracji aplikacji, zapobieganie tworzeniu kopii aplikacji czy uniemożliwianie przechwytywania ekranu i zdalnego wymazywania aplikacji.

Celem społeczności AppConfig Community jest dzielenie się narzędziami i sprawdzonymi praktykami wykorzystania możliwości natywnych w mobilnych systemach operacyjnych. Główni dostawcy rozwiązań MDM działający w tej społeczności opracowali schemat standardów, którego realizacja powinna ułatwiać twórcom aplikacji wyposażanie oprogramowania w obsługę konfiguracji aplikacji zarządzanych. Umożliwiając bardziej spójne, otwarte i prostsze konfigurowanie i zabezpieczanie aplikacji mobilnych, społeczność ta przyczynia się do coraz powszechniejszego wdrażania w firmach urządzeń mobilnych.

Dodatkowe informacje o społeczności AppConfig znajdują się na stronie www.appconfig.org.

Zarządzany przepływ danych

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

- **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 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 respektują też niektóre rozszerzenia.

Mechanizmy ochrony danych firmowych uniemożliwiają otwarcie tego dokumentu roboczego za pomocą aplikacji innych niż te zainstalowane i zarządzane przez rozwiązanie MDM.

- **Rozszerzenia zarządzane.** Dzięki rozszerzeniom aplikacji twórcy programów innych firm mogą dodawać funkcje do aplikacji, a nawet do najważniejszych systemów wbudowanych w iOS, takich jak Centrum powiadomień, umożliwiając pojawienie się nowych przepływów informacji biznesowych między aplikacjami. Zarządzanie otwieraniem plików zapobiega interakcjom między aplikacjami zarządzanymi a funkcjami rozszerzeń niezarządzanych. Poniżej przedstawiono różne typy rozszerzeń:
  - **Rozszerzenia typu Document Provider** umożliwiają aplikacjom biurowym otwieranie dokumentów z różnych usług chmurowych bez tworzenia zbędnych kopii.
  - **Rozszerzenia typu Action** pozwalają użytkownikom na modyfikowanie lub wyświetlanie treści w innej aplikacji. Przykładowo, dzięki takiemu rozszerzeniu użytkownik może przetłumaczyć tekst z języka obcego bezpośrednio w przeglądarce Safari.
  - **Rozszerzenia typu Custom Keyboard** sprawiają, że możliwe jest korzystanie z klawiatury innej niż ta wbudowana w iOS. Zarządzanie otwieraniem plików chroni przed korzystaniem w aplikacjach firmowych z nieautoryzowanych klawiatur.
  - **Rozszerzenia typu Today**, zwane też widżetami, służą do wyświetlania krótkich informacji w widoku Dzisiaj w Centrum powiadomień. Dzięki nim użytkownicy błyskawicznie dostają aktualne informacje i w prosty sposób mogą przejść do pełnej aplikacji, by poznać ich szczegóły.
  - **Rozszerzenia typu Share** ułatwiają użytkownikom udostępnianie treści innym podmiotom, np. za pośrednictwem stron społecznościowych lub usług przesyłania danych. Przykładowo, jeśli aplikacja zawiera przycisk Udostępnij, użytkownik może kliknąć rozszerzenie typu Share dla wybranej strony społecznościowej i opublikować swój komentarz lub inny rodzaj treści.

Elastyczne opcje zarządzania

Architektura zarządzania Apple jest elastyczna i umożliwia organizacjom zrównoważone zarządzanie prywatnymi i należącymi do firmy urządzeniami pracowników. Korzystanie z systemu iOS i rozwiązania MDM innej firmy sprawia, że organizacja ma do dyspozycji wiele różnych opcji — od niespotykanie otwartej metodologii po niezwykłą precyzję działań.

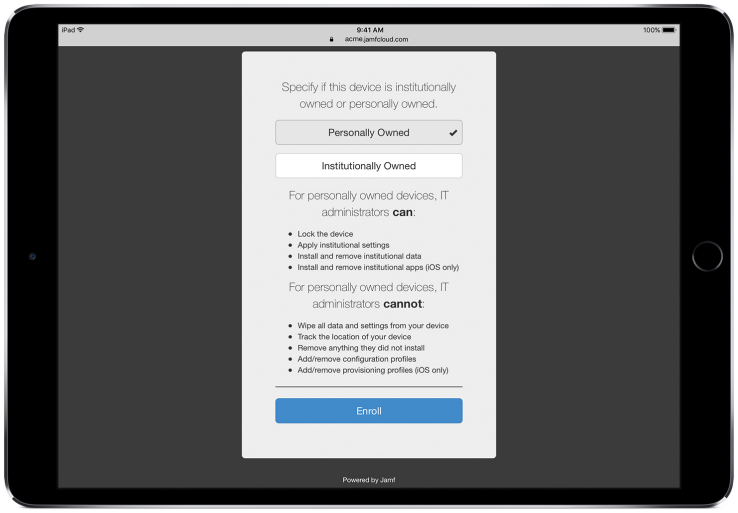
Modele własności

Urządzenia i aplikacje mogą być zarządzane w różny sposób, zależnie od modelu — lub modeli — własności w danej firmie. Firmy powszechnie stosują dwa modele własności urządzeń iOS — sprzęt należy w nich albo do użytkownika, albo do organizacji.

Urządzenia będące własnością użytkowników

W przypadku urządzenia należącego do użytkownika system iOS umożliwia mu przeprowadzenie spersonalizowanej konfiguracji, udostępniając jednocześnie wszystkie informacje dotyczące ustawień urządzenia i gwarantując, że organizacja nie będzie miała dostępu do jego prywatnych danych.

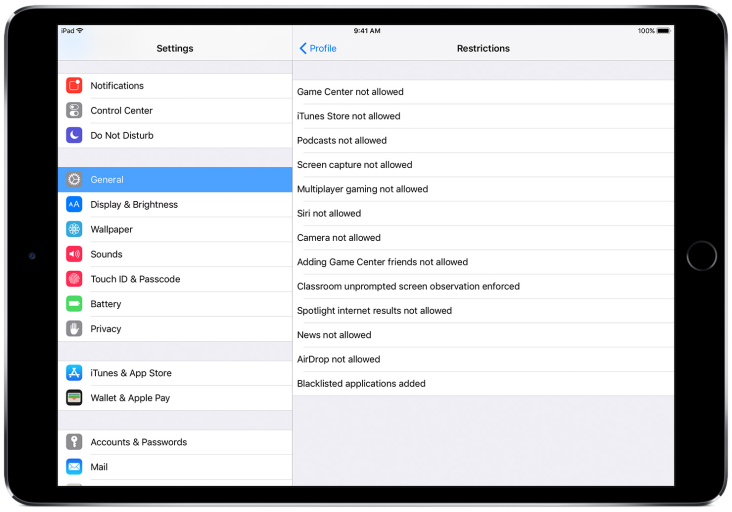
- **Rejestracja w trybie domniemanej zgody lub domniemanego braku zgody.** Nawet jeśli urządzenie zostało zakupione i skonfigurowane przez pracownika — tzw. model BYOD (Bring Your Own Device) — organizacja może mu udostępnić usługi firmowe, np. sieć Wi-Fi, pocztę e-mail czy kalendarz. Użytkownik musi tylko wyrazić zgodę na zarejestrowanie w należącym do firmy rozwiązaniu MDM. Po dokonaniu za pośrednictwem urządzenia iOS pierwszej rejestracji w rozwiązaniu MDM użytkownik otrzymuje informacje o uprawnieniach dostępu serwera MDM na jego urządzeniu oraz o funkcjach, które skonfiguruje serwer. Dzięki temu użytkownik wie, czym zarządza na jego urządzeniu organizacja, a obie strony mają do siebie większe zaufanie. To ważne, by użytkownik wiedział, że jeśli stosowane przez firmę standardy zarządzania będą sprzeczne z jego oczekiwaniami, może cofnąć zgodę na rejestrację, usuwając profil zarządzania ze swojego urządzenia. Wykonanie tej czynności spowoduje usunięcie wszystkich firmowych kont i aplikacji zainstalowanych przez rozwiązanie MDM.



Rozwiązania MDM innych firm zazwyczaj oferują intuicyjny interfejs dla pracowników, dzięki któremu proces wyrażania zgód w czasie rejestracji jest prosty i przyjazny.*

*Zrzut ekranu dzięki uprzejmości Jamf.

- **Większa transparentność.** Po rejestracji w systemie MDM pracownik może łatwo sprawdzić w Ustawieniach, które aplikacje, książki i konta są zarządzane i jakie ograniczenia w dostępie do funkcji zostały nałożone. Wszystkie firmowe ustawienia, konta i treści instalowane przez MDM są oznaczane przez iOS jako „zarządzane”.



Znajdujący się w Ustawieniach interfejs użytkownika z profilami konfiguracji pokazuje dokładnie, co zostało skonfigurowane na danym urządzeniu.

- **Prywatność użytkowników.** Choć serwer MDM pozwala na interakcje z urządzeniami iOS, nie umożliwia dostępu do wszystkich ustawień i informacji o kontach. Organizacja może zarządzać udostępnianymi przez serwer MDM kontami firmowymi, ustawieniami i informacjami, ale nie ma dostępu do prywatnych kont użytkownika. Co więcej, te same funkcje, które zabezpieczają dane w aplikacjach zarządzanych przez firmę, uniemożliwiają również przedostanie się danych prywatnych użytkownika do strumienia danych przedsiębiorstwa.

  Poniżej pokazano, które dane na prywatnym urządzeniu iOS są widoczne dla serwera MDM innej firmy, a które nie:

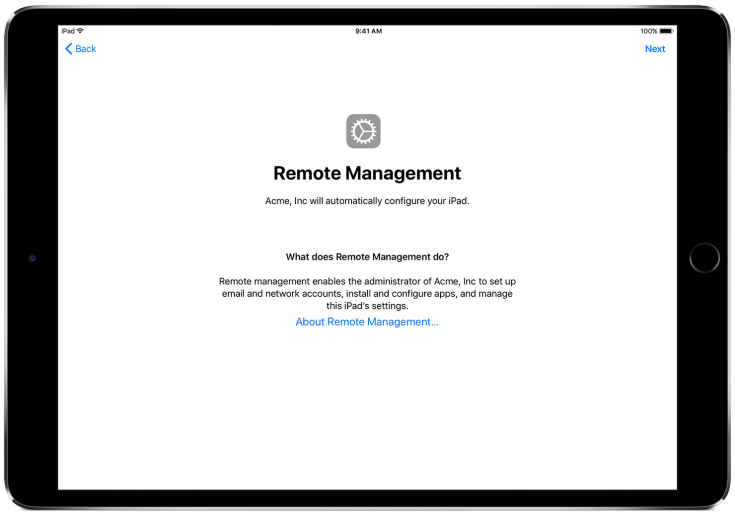
Serwer MDM ma dostęp do następujących danych:	**Serwer MDM nie ma dostępu do prywatnych danych użytkownika takich jak:**
Nazwa urządzenia	Poczta prywatna lub służbowa, kalendarze, kontakty
Numer telefonu	Wiadomości SMS i iMessage
Numer seryjny	Historia przeglądania przy użyciu Safari
Nazwa i numer modelu	Rejestry połączeń telefonicznych lub FaceTime
Pojemność i dostępne miejsce	Osobiste przypomnienia i notatki
Numer wersji iOS	Częstotliwość korzystania z aplikacji
Zainstalowane aplikacje	Lokalizacja urządzenia

- **Personalizowanie urządzeń.** Doświadczenia wielu firm dowodzą, że umożliwienie użytkownikom personalizacji urządzeń z użyciem ich własnych identyfikatorów Apple ID sprzyja poczuciu własności i odpowiedzialności. Oprócz tego powoduje wzrost produktywności pracy, ponieważ użytkownicy sami decydują o tym, których aplikacji i treści używają.

Urządzenia będące własnością organizacji

W przypadku urządzeń należących do organizacji możliwe są dwa modele wdrożenia — w pierwszym (z możliwością personalizacji) każdy użytkownik ma własne urządzenie, które może spersonalizować, w drugim (bez możliwości personalizacji) urządzenie jest rotacyjnie udostępniane różnym pracownikom i nie może zostać spersonalizowane. Funkcje systemu iOS, takie jak zautomatyzowana rejestracja, ustawienia MDM z możliwością blokowania, nadzorowanie urządzeń czy stale aktywne połączenie VPN, gwarantują, że urządzenia są konfigurowane w zgodzie z wymogami organizacji, usprawniając jednocześnie nadzór i ochronę danych firmowych.

- **Zautomatyzowana rejestracja.** Program Device Enrollment Program (DEP) umożliwia zautomatyzowanie rejestracji w systemie MDM w trakcie wstępnej konfiguracji posiadanych telefonów iPhone, iPadów i systemów Mac. Można nakazać, by rejestracja była obowiązkowa i nie można było jej cofnąć. Urządzenie można także przełączyć w tryb nadzorowany, tak by w momencie rejestracji użytkownik mógł pominąć niektóre podstawowe etapy konfiguracji.



Jeśli użytkownik uczestniczy w programie DEP, rozwiązanie MDM automatycznie skonfiguruje jego urządzenia iOS w trakcie pracy Asystenta ustawień.

- **Urządzenia nadzorowane.** Dzięki nadzorowi organizacja może korzystać z dodatkowych funkcji zarządzania na posiadanych przez siebie urządzeniach iOS. Funkcje nadzoru obejmują m.in. filtrowanie połączeń WWW przez globalny serwer proxy, dzięki któremu organizacja może egzekwować korzystanie z Internetu zgodnie z firmowymi zasadami, a także uniemożliwienie użytkownikom przywrócenia ustawień fabrycznych urządzenia. Domyślnie wszystkie urządzenia iOS są nienadzorowane. Tryb nadzoru można włączać automatycznie za pośrednictwem programu DEP albo 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. Inaczej może okazać się, że konieczne będzie wymazanie zawartości z już użytkowanych urządzeń. Nadzorowanie nie polega na ograniczaniu funkcjonalności urządzeń, umożliwia natomiast organizacji bardziej zaawansowane zarządzanie posiadanymi przez nią urządzeniami. W dłuższej perspektywie czasowej nadzorowanie może zapewnić firmie dostęp do jeszcze szerszych możliwości.

Pełna lista ustawień nadzorowanych znajduje się w publikacji iOS — Podręcznik wdrażania.

Ograniczenia dostępu

Ograniczenia dostępu w systemie iOS można skonfigurować zdalnie bez zakłócenia pracy użytkowników, tak by odpowiadały potrzebom organizacji. Mogą one ingerować w:

- AirPrint
- Instalację aplikacji
- Korzystanie z aplikacji
- Aplikację Klasa
- Urządzenie
- iCloud
- Uprawnienia użytkowników lub grup użytkowników aplikacji Profile Manager
- Safari
- Ustawienia zabezpieczeń i prywatności
- Siri

Za pośrednictwem rozwiązania MDM można też konfigurować opcje należące do następujących kategorii:

- Ustawienia zautomatyzowanej rejestracji w systemie MDM
- Ekrany Asystenta ustawień

Dodatkowe funkcje zarządzania

Przesyłanie zapytań do urządzeń

Oprócz konfigurowania urządzeń, serwer MDM może też przesyłać do urządzeń zapytania o różne informacje, np. o szczegóły dotyczące urządzeń, sieci lub aplikacji, a także o dane związane z przestrzeganiem zasad i zabezpieczeniami. Dzięki takim informacjom łatwiej sprawić, by urządzenia były zawsze używane w zgodzie z obowiązującymi zasadami. Serwer MDM określa częstotliwość, z jaką zbierane są informacje.

Informacje, o które serwer może zapytać urządzenie iOS, to m.in.:

- Szczegóły urządzenia (jego nazwa)
- Model, wersja systemu iOS i numer seryjny
- Informacje o sieci
- Status przemieszczania się w sieci, adresy MAC
- Zainstalowane aplikacje
- Nazwa, wersja i rozmiar aplikacji
- Dane związane z przestrzeganiem zasad i zabezpieczeniami
- Wybrane ustawienia, zasady, certyfikaty
- Status szyfrowania

Czynności administracyjne

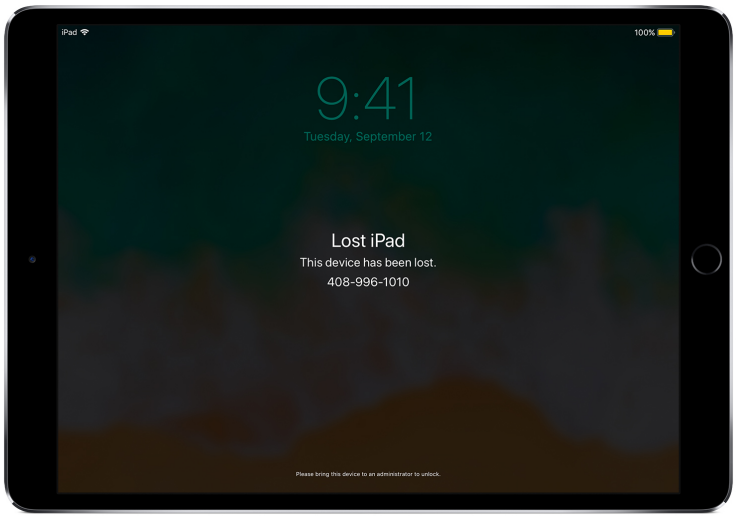
Serwer MDM może wydawać zarządzanym urządzeniom wiele różnych poleceń administracyjnych — na przykład zmienić ustawienia konfiguracyjne bez interakcji z użytkownikiem, uaktualnić system iOS na urządzeniu zabezpieczonym kodem, zdalnie zablokować urządzenie lub wymazać jego zawartość oraz skasować zapomniany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

Tryb Utracony

Jeśli urządzenie działa pod kontrolą systemu iOS 9.3 lub jego nowszej wersji, rozwiązanie MDM może zdalnie przełączyć je 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.

Gdy system MDM wyłącza zdalnie tryb Utracony, urządzenie zostaje odblokowane, pobierana jest też informacja o jego lokalizacji. Aby zachować pełną transparentność, użytkownik jest informowany o tym, że tryb Utracony wyłączono.



Gdy rozwiązanie MDM przełącza urządzenie w tryb Utracony, blokuje je, zezwalając na wyświetlanie wiadomości na ekranie, i określa jego lokalizację.

Blokada aktywacji

W systemie iOS 7.1 lub jego nowszej wersji system MDM umożliwia włączenie blokady aktywacji, gdy użytkownik uruchomi na urządzeniu nadzorowanym aplikację Znajdź mój iPhone. Dzięki temu organizacja może korzystać ze zniechęcającej złodziei blokady aktywacji, mając jednak możliwość jej ominięcia — np. wtedy, gdy użytkownik odejdzie z organizacji bez usuwania blokady aktywacji za pomocą własnego identyfikatora Apple ID.

Rozwiązanie MDM może uzyskać kod obejścia i pozwolić użytkownikowi na włączenie blokady aktywacji urządzenia zgodnie z jednym z następujących scenariuszy:

- Jeśli funkcja Znajdź mój iPhone jest włączona, a rozwiązanie MDM zezwala na blokadę aktywacji, następuje jej włączenie.
- Jeśli funkcja Znajdź mój iPhone jest wyłączona, a rozwiązanie MDM zezwala na blokadę aktywacji, zostaje ona włączona po włączeniu przez użytkownika funkcji Znajdź mój iPhone.

Podsumowanie

Architektura zarządzania iOS zaspokaja pozornie sprzeczne potrzeby organizacji w najlepszy możliwy sposób: z jednej strony umożliwia działom IT konfigurowanie, obsługiwanie i zabezpieczanie urządzeń, a także zarządzanie przepływającymi przez nie danymi firmowymi; z drugiej — stwarza użytkownikom warunki do wydajnej pracy z narzędziami, po które chętnie sięgają.