Správa zařízení a podnikových dat v iOS

Přehled

Firmy z celého světa vybavují své zaměstnance iPhony a iPady.

Obsah

Klíčem k úspěšné mobilní strategii je rovnováha mezi kontrolou zařízení IT odděleními a možnostmi jejich přizpůsobování samotnými uživateli. Když si uživatelé můžou iOS zařízení přizpůsobovat vlastními aplikacemi a obsahem, mají nad nimi větší kontrolu a nesou za ně odpovědnost, což vede k větší angažovanosti a zvýšení produktivity. Toto je umožněno frameworkem pro správu od společnosti Apple, který nabízí inteligentní způsoby samostatné správy podnikových dat a aplikací oddělující pracovní data od osobních. Uživatelé navíc rozumí způsobu, jakým jsou jejich zařízení spravována, a mají jistotu, že je chráněno jejich soukromí.

Tento dokument obsahuje pokyny, jak zajistit nezbytné řízení ze strany IT oddělení a zároveň uživatelům umožnit používání těch nejlepších nástrojů pro jejich práci. Jedná se o doplněk k referenční příručce pro nasazení iOS, což jsou komplexní online technické referenční informace pro nasazování a správu iOS zařízení ve vašem podniku.

Referenční příručku pro nasazení iOS najdete na adrese help.apple.com/deployment/ios.

Základy správy

V iOS můžete zefektivnit nasazování iPhonů a iPadů pomocí řady zabudovaných technik, které umožňují zjednodušit nastavení účtu, konfigurovat zásady, distribuovat aplikace a vzdáleně aplikovat omezení zařízení.

Náš přístup ke správě

Framework pro správu od společnosti Apple je základní stavební kámen správy mobilních zařízení. Tento framework je zabudovaný do iOS a umožňuje organizacím správu nezbytných věcí (s jenom nepatrnou intervencí), a ne jenom prostě blokovat nebo deaktivovat funkce. Framework pro správu od společnosti Apple ve výsledku umožňuje podrobnou kontrolu vašich zařízení, aplikací a dat prostřednictvím řešení správy mobilních zařízení (MDM) třetích stran. Nejdůležitější ovšem je, že získáte podrobnou kontrolu bez snížení uživatelského komfortu nebo narušení soukromí svých zaměstnanců.

Ostatní metody správy zařízení, které jsou na trhu, můžou k popisu funkcí řešení MDM používat jiné názvy, například EMM (Enterprise Mobility Management – Správa podnikové mobility) nebo MAM (Mobile Application Management – Správa mobilních aplikací). Tato řešení se zaměřují na společný cíl – na bezdrátovou správu zařízení a podnikových dat vaší organizace. Protože je framework pro správu od společnosti Apple zabudovaný přímo do iOS, nepotřebujete samostatného agenta od poskytovatele řešení MDM.

Oddělení pracovních a osobních dat

Bez ohledu na to, jestli vaše organizace podporuje zařízení vlastněná uživateli nebo společností, můžete dosahovat svoje cíle správy IT prostředků a zároveň uživatelům umožnit plnou produktivitu při plnění jejich úkolů. Pracovní a osobní data jsou spravována samostatně, takže nedochází k tříštění uživatelského komfortu. Tak může ta nejoblíbenější kancelářská aplikace v zařízení uživatele koexistovat po boku vašich podnikových aplikací, aby zaměstnanci měli při práci větší svobodu. Toho iOS dosahuje bez používání řešení třetích stran, jako jsou kontejnery, která mají nepříznivý vliv na komfort uživatelů a zbytečně jim ztěžují práci.

Princip jednotlivých modelů správy

Kontejnery byly často vytvořeny k tomu, aby řešily problémy na jiných platformách – problémy, které se v iOS nevyskytují. Některé kontejnery využívají strategii duální identity (tzv. dual persona), která v jednom zařízení umožňuje souběžné používání dvou samostatných prostředí. Další výrobci se soustřeďují na běh samotných aplikací ve vlastních kontejnerech, což řeší integrací založenou na kódu nebo zabalováním aplikací. Všechny tyto metodologie představují pro uživatele překážky, ať už se jedná o nutnost přihlašování k různým pracovním prostorům nebo zvyšování závislosti na proprietárním kódu, které často způsobují nekompatibilitu aplikací s aktualizacemi operačního systému.

Organizace, které kontejnery přestaly používat, vidí, že nativní ovládací prvky správy v iOS uživatelům nabízí optimální osobní komfort a zvyšují jejich produktivitu. Namísto toho, abyste uživatelům ztěžovali používání jejich zařízení k pracovním účelům i pro osobní potřeby, můžete používat ovládací prvky zásad, které bezproblémově spravují tok dat na pozadí.

Správa podnikových dat

S iOS není potřeba zařízení blokovat. Klíčové technologie řídí tok podnikových dat mezi aplikacemi a brání jejich pronikání do osobních aplikací nebo cloudových služeb uživatelů.

Spravovaný obsah

Spravovaný obsah pokrývá instalaci, konfiguraci, správu a odstraňování aplikací z App Storu nebo vlastních in-house aplikací, účtů, knih a domén.

- **Správa aplikací.** Aplikace instalované prostřednictvím řešení MDM se nazývají spravované aplikace. Může se jednat o bezplatné nebo placené aplikace z App Storu nebo o vlastní in-house aplikace, a je možné je instalovat bezdrátově přes MDM. Spravované aplikace často obsahují citlivé informace a poskytují větší kontrolu než aplikace stažené uživatelem. Server řešení MDM může odstraňovat spravované aplikace a jejich související data na vyžádání, nebo je možné zadat, jestli se tyto aplikace mají odstranit při odstranění profilu řešení MDM. Server řešení MDM navíc může bránit v zálohování spravovaných dat do iTunes nebo na iCloud.
- **Správa účtů.** Řešení MDM může vašim uživatelům automaticky nastavit poštovní a další účty a umožnit jim tak rychle začít pracovat. V závislosti na poskytovateli řešení MDM a integraci s vašimi interními systémy můžou být datové části účtů taky předem vyplněné jménem a poštovní adresou uživatele, a v případě potřeby taky certifikačními identitami pro ověřování a podepisování. Řešení MDM umožňuje konfigurovat následující typy účtů: IMAP/POP, CalDAV, odebírané kalendáře, CardDAV, Exchange ActiveSync a LDAP.
- **Spravované knihy.** Prostřednictvím MDM, jde do zařízení uživatelů automaticky posílat knihy ePub a PDF dokumenty, takže zaměstnanci mají pořád všechno, co potřebují. Spravované knihy jde sdílet jenom s dalšími spravovanými aplikacemi nebo se dají posílat poštou prostřednictvím spravovaných účtů. Když už materiály nejsou potřeba, je možné je odstranit na dálku.

- **Spravované domény.** Dokumenty stažené prostřednictvím Safari jsou považovány za spravované, když pochází ze spravované domény. Je možné spravovat konkrétní URL adresy a subdomény. Pokud si uživatel například stáhne PDF ze spravované domény, vyžaduje tato doména, aby PDF vyhovovalo všem nastavením spravovaných dokumentů. Cesty za doménou jsou spravovány ve výchozím nastavení.

Spravovaná distribuce

Spravovaná distribuce vám umožňuje používat MDM řešení nebo Apple Configurator 2 ke správě aplikací a knih zakoupených v rámci programu hromadných nákupů (VPP). Pokud chcete povolit spravovanou distribuci, musíte nejdřív svoje řešení MDM pomocí bezpečného tokenu propojit s vaším účtem programu hromadných nákupů. Jakmile je server řešení MDM připojený k programu hromadných nákupů, můžete aplikace přiřazovat přímo k zařízení, aniž by uživatel potřeboval Apple ID. Když jsou aplikace připravené k instalaci do zařízení, uživatel dostane vyrozumění. Pokud je zařízení dozorované, jsou do něj aplikace posílány bezobslužně, bez upozornění uživatele.

Pokud chcete mít s řešením MDM pořád úplnou kontrolu nad aplikacemi, přiřazujte aplikace přímo k zařízením.

Konfigurace spravovaných aplikací

Když je využívána konfigurace spravovaných aplikací, řešení MDM využívá ke konfiguraci aplikací při nebo po nasazení nativní framework pro správu v iOS. Tento framework vývojářům umožňuje identifikovat nastavení konfigurace, která by měla být implementována, když je jejich aplikace instalována jako spravovaná. Zaměstnanci můžou aplikace nakonfigurované tímto způsobem začít používat okamžitě, bez nutnosti vlastního nastavení. IT oddělení má jistotu, že jsou podniková data v aplikacích zpracovávána bezpečně, bez potřeby proprietárních sad SDK nebo zabalování aplikací.

Vývojáři aplikací mají k dispozici různé možnosti, které jde povolit pomocí konfigurace spravovaných aplikací, jako je konfigurace aplikací, zabránění zálohování aplikací, vypnutí funkce pořizování snímků obrazovky a vzdálené mazání aplikací.

Iniciativa AppConfig Community se zaměřuje na poskytování nástrojů a doporučování postupů souvisejících s nativními možnostmi v mobilních operačních systémech. Přední poskytovatelé řešení MDM z této iniciativy vytvořili standardní schéma, které můžou všichni vývojáři aplikací používat k podpoře konfigurace spravovaných aplikací. Umožněním konzistentnějšího, otevřenějšího a jednoduššího způsobu konfigurace a zabezpečení mobilních aplikací tato iniciativa pomáhá zvyšovat penetraci mobilních technologií ve firmách.

Další informace o iniciativě AppConfig Community www.appconfig.org.

Spravovaný tok dat

Řešení MDM poskytují specifické funkce, které umožňují podrobnou správu podnikových dat, takže nemůžou unikat do osobních aplikací a cloudových služeb uživatelů.

- **Spravovaná funkce „Otevřít v".** Správa funkce „Otevřít v" využívá sadu omezení, která brání v otevírání příloh nebo dokumentů ze spravovaných zdrojů v nespravovaných destinacích, a opačně.

  Můžete například zabránit v otevření důvěrné e-mailové přílohy ve spravovaném poštovním účtu vaší organizace libovolnou osobní aplikací uživatele. Tento pracovní dokument můžou otevírat jenom aplikace nainstalované a spravované řešením MDM. Nespravované osobní aplikace uživatele se v seznamu aplikací dostupných k otevření přílohy nezobrazují. Navíc ke spravovaným aplikacím, účtům, knihám a doménám respektují spravovaná omezení funkce „Otevřít v" taky různá rozšíření.

V zájmu ochrany podnikových dat můžou tento pracovní dokument otevírat jenom aplikace nainstalované a spravované řešením MDM.

- **Spravovaná rozšíření.** Rozšíření umožňují vývojářům třetích stran poskytovat funkce ostatním aplikacím nebo dokonce klíčovým systémům zabudovaným do iOS, jako je Oznamovací centrum, čímž umožňují nové pracovní postupy mezi aplikacemi. Používání funkce „Otevřít v" zabraňuje v používání funkcí nespravovaných doplňků k interakci s ostatními aplikacemi. V následujících příkladech jsou ukázány různé typy rozšíření:
  - **Rozšíření Poskytovatel dokumentů** umožňují kancelářským aplikacím otevírat dokumenty z různých cloudových služeb, bez nutnosti vytvářet zbytečné kopie.
  - **Rozšíření Akce** umožňují uživatelům manipulaci nebo prohlížení obsahu v kontextu jiné aplikace. Uživatelé například můžou provést akci, jako je přeložení textu z jiného jazyka přímo v Safari.
  - **Rozšíření Vlastní klávesnice** nabízí klávesnice navíc ke klávesnicím zabudovaným do iOS. Spravovaná funkce „Otevřít v" může bránit v zobrazování neautorizovaných klávesnic v podnikových aplikacích.
  - **Rozšíření Dnes**, taky nazývané widgety, slouží k poskytování stručných informací v zobrazení Dnes v Oznamovacím centru. Toto je skvělý způsob, jakým uživatelé z aplikace získají aktualizované informace, se zjednodušenými interakcemi, které spustí celou aplikaci s dalšími informacemi.
  - **Rozšíření Sdílení** uživatelům poskytují pohodlný způsob sdílení obsahu s dalšími entitami, jako jsou sociální weby na sdílení obsahu nebo služby k nahrávání souborů. Například v aplikaci, která obsahuje tlačítko Sdílet, můžou uživatelé zvolit rozšíření Sdílení, které představuje sociální web na sdílení obsahu, a potom ho použít k publikování komentáře nebo jiného obsahu.

Flexibilní možnosti správy

Framework pro správu od společnosti Apple je flexibilní a nabízí vyvážený přístup ke způsobu, jakým ve svém podniku můžete spravovat zařízení vlastněná uživateli i zařízení vlastněná společností. Když s iOS používáte řešení MDM jiného poskytovatele, vaše možnosti správy zařízení sahají od možnosti použití vysoce otevřené metodologie až po aplikování vysoce podrobných nastavení.

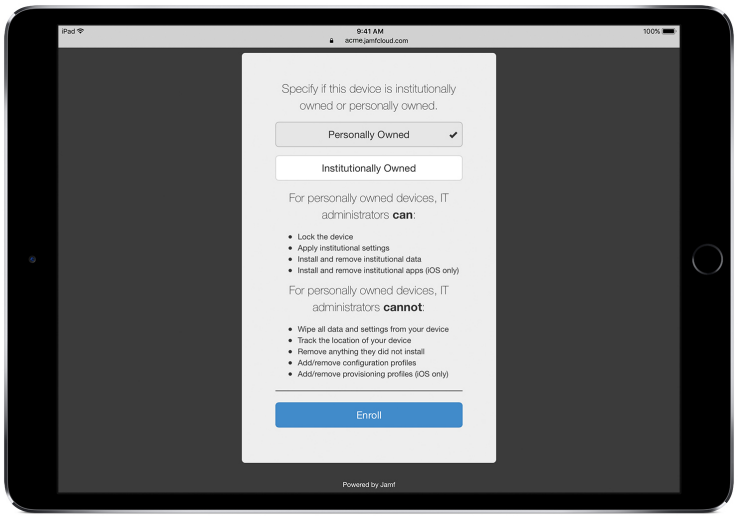
Vlastnické modely

V závislosti na modelu nebo modelech vlastnictví zařízení ve vaší organizaci budete zařízení a aplikace spravovat rozdílným způsobem. Dva vlastnické modely pro iOS zařízení, které se běžně používají v podnikových prostředích, jsou zařízení vlastněná uživateli a zařízení vlastněná organizací.

Zařízení vlastněná uživateli

S nasazením využívajícím model zařízení vlastněných uživateli nabízí iOS personalizované nastavení prováděné uživateli a transparentnost ohledně způsobu konfigurace zařízení, spolu s jistotou, že k jejich osobním datům nebude mít organizace přístup.

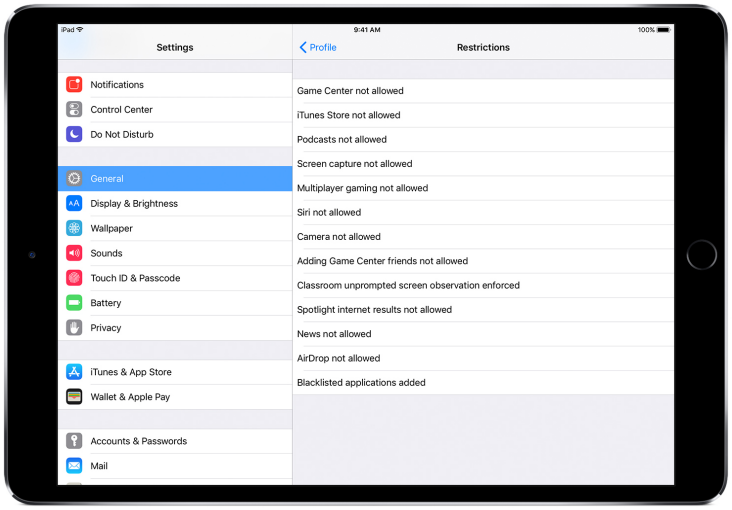
- **Registrace s možností přihlášení a odhlášení.** Když si zařízení kupují a nastavují sami uživatelé, můžete jim pořád poskytnout přístup k podnikovým službám, jako Wi-Fi, pošta a kalendář. Uživatelé se jednoduše přihlásí k registraci do řešení MDM vaší organizace. Když se uživatelé do řešení MDM na iOS zařízení registrují poprvé, jsou jim poskytnuty informace, k jakému serveru řešení MDM můžou se svými zařízeními přistupovat a jaké funkce budou nakonfigurovány. Uživatelé tak mají transparentní informace o tom, co je spravováno, a mezi vámi a uživateli taky bude vytvořen důvěryhodný vztah. Je důležité uživatelům sdělit, že pokud s touto správou někdy nebudou spokojeni, můžou se z registrace odhlásit odstraněním profilu správy ze svého zařízení. V takovém případě budou odstraněny všechny podnikové účty a aplikace nainstalované prostřednictvím řešení MDM.



Řešení MDM třetích stran typicky nabízí uživatelsky přívětivé rozhraní pro zaměstnance, takže se můžou při registraci pohodlně přihlašovat.*

*Snímky obrazovek poskytl Jamf.

- **Větší transparentnost.** Po registraci uživatelů do řešení MDM si zaměstnanci můžou v Nastaveních snadno prohlížet, které aplikace, knihy a účty jsou spravovány, a která omezení jsou implementována. Všechna podniková nastavení, účty a aplikace instalovaná prostřednictvím MDM jsou systémem iOS označená jako „spravovaná"



Uživatelské rozhraní pro konfigurační profily v Nastaveních uživatelům ukazují, co přesně bylo pro jejich zařízení nakonfigurováno.

- **Soukromí uživatelů.** Server řešení MDM vám sice umožní interakci s iOS zařízeními, ale ne všechna nastavení a všechny informace účtu jsou vidět. Můžete spravovat podnikové účty, nastavení a informace zřízené prostřednictvím řešení MDM, ale nebudete mít přístup k osobním účtům uživatele. Ve skutečnosti stejné funkce, které udržují bezpečí dat v aplikacích spravovaných podnikem, taky brání obsahu uživatele před vstupem do streamu podnikových dat.

  Následující příklady ukazují, co server řešení MDM jiného poskytovatele může a nemůže vidět na osobním iOS zařízení:

Řešení MDM vidí:	**Řešení MDM nevidí osobní data jako:**
Název zařízení a kontakty	Osobní nebo pracovní pošta, kalendáře
Telefonní číslo	Obsah zpráv SMS nebo iMessage
Sériové číslo	Historie procházení v Safari
Název a číslo modelu	Protokoly telefonických hovorů a hovorů přes FaceTime
Kapacita a dostupný prostor	Osobní připomínky a poznámky
Číslo verze iOS	Četnost využívání aplikací
Nainstalované aplikace	Poloha zařízení

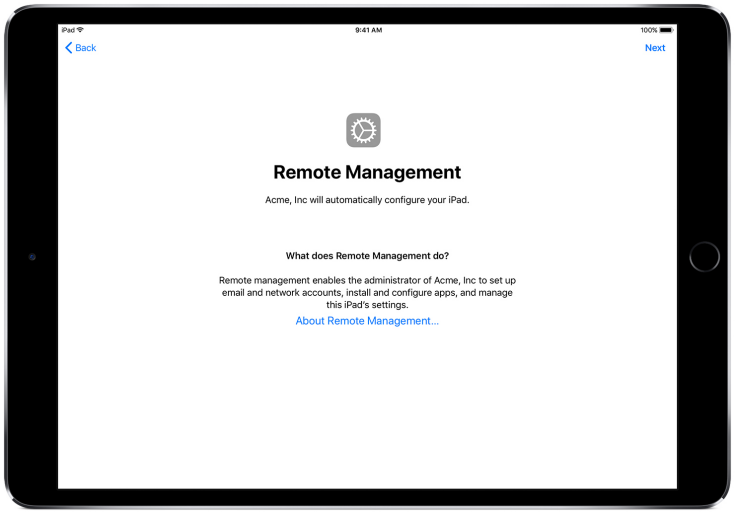
- **Personalizování zařízení.** Společnosti zjistily, že když uživatelům umožní přizpůsobení zařízení pomocí jejich Apple ID, vede to u uživatelů k větší zodpovědnosti a intenzivnějšímu pocitu vlastnictví zařízení, a zvýší se jejich produktivita, protože jsou teď schopni si zvolit aplikace a obsah, které potřebují k co nejlepšímu provádění pracovních úkolů.

Zařízení vlastněná organizací

V případě nasazení zařízení vlastněných společností můžete poskytnout zařízení všem uživatelům (to se nazývá personalizované nasazení) nebo můžou zařízení obíhat mezi uživateli (to se nazývá nepersonalizované nasazení). iOS funkce, jako je automatizovaná registrace, uzamykatelné nastavení řešení MDM, dozor nad zařízením a vždy aktivní VPN, zajišťují, že jsou zařízení

nakonfigurována na základě specifických požadavků vaší organizace, poskytují lepší kontrolu a zaručují ochranu podnikových dat.

- **Automatizovaná registrace.** Program registrace zařízení (DEP) umožňuje automatizovat registraci v řešení MDM při počátečním nastavení iPhonů, iPadů a Maců vlastněných vaší organizací. Registrace může být povinná a neodstranitelná. Zařízení taky můžete během registračního procesu uvést do dozorovaného režimu a umožnit uživatelům přeskočit některé kroky základního nastavení.



S programem DEP řešení MDM automaticky nakonfiguruje vaše iOS zařízení během Průvodce nastavením.

- **Dozorovaná zařízení.** Dozor zajišťuje pro iOS zařízení vlastněná vaší organizací další možnosti správy. Sem patří schopnost povolit webový filtr prostřednictvím globálního proxy, aby webový provoz uživatelů probíhal podle pokynů organizace, schopnost zabránit uživatelům provést obnovení do továrního nastavení a spousta dalších věcí. Všechna iOS zařízení jsou ve výchozím nastavení nedozorovaná. K povolení dozorovaného režimu můžete použít program DEP, nebo ho taky můžete povolit ručně pomocí Apple Configuratoru 2.

I když v tuto chvíli neplánujete používat žádné funkce určené výhradně pro dozorovaná zařízení, zvažte dozorování zařízení při jejich nastavování. Budete tak moct funkce určené výhradně pro dozorovaná zařízení využít v budoucnu. V opačném případě budete muset už nasazená zařízení smazat. Dozorování neznamená zablokování zařízení, místo toho vylepší zařízení vlastněná společností rozšířením možností správy. Z dlouhodobého hlediska dozorování poskytne vašemu podniku další možnosti.

Kompletní seznam dozorovaných nastavení najdete v referenční příručce pro nasazení iOS.

Omezení

iOS podporuje následující kategorie omezení, které můžete konfigurovat bezdrátově, aby splňovaly potřeby vaší organizace bez nepříznivého vlivu na uživatele:

- AirPrint
- Instalace aplikací
- Využití aplikací
- Aplikace Třída
- Zařízení

- iCloud
- Omezení správce profilů pro uživatele a skupiny uživatelů
- Safari
- Nastavení zabezpečení a soukromí
- Siri

Následující informace taky mají možnosti, které jde nakonfigurovat pomocí řešení MDM:

- Nastavení automatizované registrace prostřednictvím řešení MDM
- Obrazovky Průvodce nastavením

Další možnosti správy

Dotazování zařízení

Navíc ke konfigurování zařízení může server řešení MDM do zařízení posílat dotazy na různé informace, jako jsou údaje o zařízeních, sítích a aplikacích, a taky o datech týkajících se zabezpečení a jeho dodržování. Tyto informace pomáhají zajistit, že zařízení pořád vyhovují požadovaným zásadám. Server řešení MDM určuje frekvenci shromažďování informací.

Níže jsou uvedeny příklady informací, na které je možné se dotazovat iOS zařízení:

- Údaje o zařízení (název)
- Model, verze iOS, sériové číslo
- Informace o síti
- Stav roamingu, adresy MAC
- Nainstalované aplikace
- Název, verze a velikost aplikace
- Data týkající se zabezpečení a jeho dodržování
- Nainstalovaná nastavení, zásady, certifikáty
- Stav šifrování

Úlohy správy

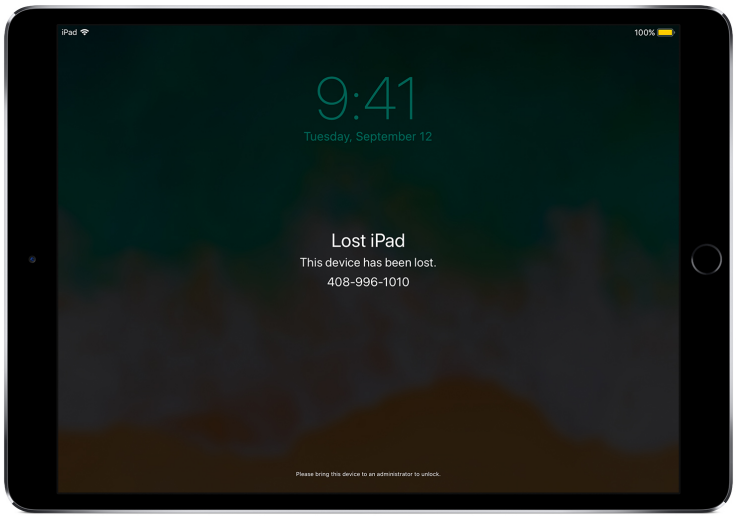
Na spravovaném zařízení může server řešení MDM provádět celou řadu administrativních úloh, včetně automatických změn konfiguračních nastavení bez zásahu uživatele, provedení aktualizace iOS na zařízeních zamčených kódem, vzdáleného zablokování a smazání zařízení nebo zrušení uzamčení kódem, aby uživatelé mohli obnovovat zapomenutá hesla. Server řešení MDM taky může iOS zařízení požádat o započetí zrcadlení AirPlay do konkrétní destinace nebo o ukončení aktuální relace AirPlay.

Režim ztráty

S iOS 9.3 a novějším můžou řešení MDM uvést dozorované zařízení do režimu ztráty na dálku. Tato akce zařízení uzamkne a umožní na zamčené obrazovce zobrazit zprávu s telefonním číslem.

V režimu ztráty jde ztracená nebo odcizená dozorovaná zařízení najít, protože řešení MDM posílá vzdálené dotazy na jejich polohu v době, kdy byla naposledy online. Režim ztráty nevyžaduje aktivní službu Najít iPhone.

Pokud řešení MDM vzdáleně deaktivuje režim ztráty, zařízení se odemkne a načte se jeho poloha. V zájmu zachování transparentnosti je uživatel o vypnutí režimu ztráty informován.



Když řešení MDM uvede zařízení do režimu ztráty, uzamkne ho, povolí zobrazování zpráv na displeji a určí jeho polohu.

Zámek aktivace

S iOS 7.1 a novějším můžete prostřednictvím řešení MDM nastavit v dozorovaném zařízení zapnutí Zámku aktivace, když uživatel zapne službu Najít iPhone. Vaše organizace tak může využívat Zámek aktivace zabraňující krádežím a zároveň vám ho umožňuje obejít, například když uživatel opustí organizaci a Zámek aktivace předtím pomocí svého Apple ID neodstraní.

Vaše řešení MDM může získat kód pro vyřazení a povolit uživateli zapnutí Zámku aktivace při splnění následujících podmínek:

- Když vaše řešení MDM povoluje Zámek aktivace dojde k zapnutí služby Najít iPhone, zapne se v tuto chvíli Zámek aktivace.
- Když vaše řešení MDM povoluje Zámek aktivace a dojde k vypnutí služby Najít iPhone, zapne se Zámek aktivace ve chvíli, kdy uživatel aktivuje službu Najít iPhone.

Shrnutí

Framework pro správu v iOS vám poskytuje to nejlepší z obou světů: IT oddělení může konfigurovat, spravovat a zabezpečovat zařízení a řídit tok podnikových dat, který jimi prochází, a uživatelé zároveň můžou dělat skvělou práci se zařízeními, která rádi používají.