



Mail and Calendar

Začínáme s firemní správou zařízení Apple

Návod ■ Ivan Malík

Zatímco většina uživatelů zná svůj Apple velmi dobře, mnoho z nich slyší o správě zařízení poprvé, popřípadě netuší, kudy na to. Tento článek je určen pro druhou kategorii a jeho cílem je vytvořit základní představu, s jakými nástroji se pustit do správy zařízení.



Wi-Fi



VPN



Single Sign-On



Nenechme se mýlit – obliba zařízení Apple neroste pouze u koncových uživatelů, ale také u administrátorů. Podle magazínu Forbes roste počet zařízení Apple ve velkých a středních firmách meziročně o 20 %. A podle nedávné studie zahrnující zhruba 1 000 pracovníků v segmentu IT bylo zjištěno, že 77 % z nich považuje Mac za bezpečnější platformu a 79 % se domnívá, že jsou snadnější na údržbu.

Důvod je pochopitelný. Operační systém macOS je stabilní systém postavený na unixových základech a administrátor může jít za určitých podmínek poměrně do hloubky. Nemusí však používat pouze vestavěné nástroje Konzola, Monitor aktivity a Terminál. Pokročilejší nástroje si může stáhnout, ručně zkompileovat či najít v některém z repozitářů Fink, MacPorts nebo Homebrew.

Ani Mac App Store nestojí stranou a lze najít užitečné nástroje, které pomáhají administrátorům zvládnout každodenní úkoly. Ať se již jedná o jednoduché utility typu 1Password, LanScan, Microsoft Remote Desktop nebo ty robustnější typu BBEEdit.

ZÁKLADNÍ ARZENÁL

Spravovaná zařízení, která jsou majetkem organizace, je potřeba mít vždy zaregistrovaná

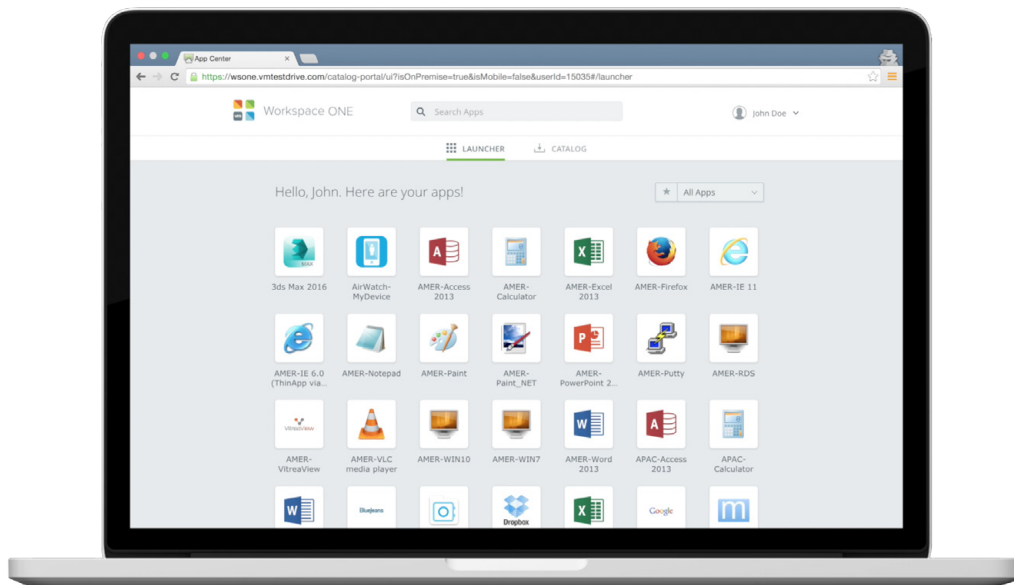
v Apple Business Manageru nebo v Apple School Manageru. Výhody, které bezplatná registrace jednoho z portálů přináší, nebudu zde rozebírat; pouze vyslovím základní tezi – bez registrace je práce výrazně komplikovanější a někdy nelze cíle dosáhnout.

Druhým nástrojem, nutným pro efektivní správu, je server pro hromadnou správu zařízení (označovaný zkratkou MDM). Ten může běžet v cloudu nebo ve firmě – v takovém případě budete potřebovat ještě hardware a někoho, kdo se o něj bude průběžně starat.

Stejný server MDM lze však s úspěchem použít pro více platform současně, takže administrátor nemusí přeskakovat mezi několika nástroji. To představuje neskutečnou úsporu času a výdajů na správu zařízení. Typickým zástupcem takového unifikovaného řešení je například VMware Workspace ONE.

ŽIVOTNÍ CYKLUS SPRÁVY

Při správě je užitečné rozdělit si veškeré úkoly, které má administrátor na starosti, do několika samostatných skupin. Toto rozdělení se označuje jako životní cyklus zařízení. Framework MDM definuje celkem šest klíčových momentů v celém životním cyklu zařízení.



1. DEPLOYMENT

Nejdříve se zaregistrujte do portálu Apple Business Manager (popřípadě Apple School Manager) a přidejte do tohoto portálu svůj server MDM. Máte hotovo? Výborně! Zkontrolujte, že nakoupená zařízení máte uvedena ve svém portálu a fyzicky je předejte uživatelům. Když uživatel zapne své zařízení poprvé, automaticky se zaregistruje do serveru MDM, který pro změnu nakonfiguruje zařízení – to vše bez toho, aby se ho IT zaměstnanec musel dotknout. Tuto variantu označujeme jako Zero-Touch Deployment.

2. KONFIGURACE

Konfigurovat lze jakoukoliv hardwarovou nebo softwarovou část počítače. Můžete spravovat Wi-Fi, VPN, nastavení e-mailu, instalovat vlastní software a tiskárny, spravovat místní uživatelské účty a provádět pokročilá nastavení aplikací. Definice nastavení probíhá díky konfiguračnímu profilu, který generuje server MDM. Tento malý

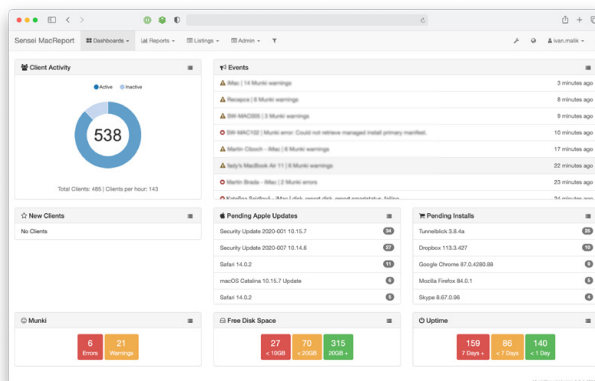
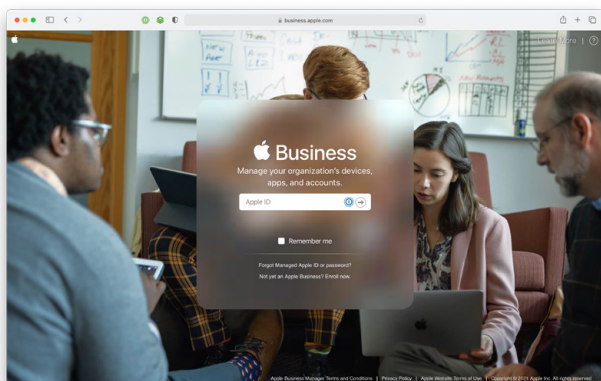


soubor XML se pak rozdistribuuje do spravovaných zařízení.

Popřípadě lze provést spuštění shellových skriptů. Cokoli, co lze v Terminálu spustit pomocí příkazového řádku, lze změnit na skript. Schopnost spouštět skripty poskytuje mnohem větší flexibilitu než standardní konfigurační profily a otevírá tak dveře k nekonečným možnostem správy zařízení.

3. SPRÁVA APLIKACÍ

Jistě znáte velmi podrobně App Store na svém iPhone nebo iPadu. Jde o jediný oficiální způsob, jak



do takového zařízení nainstalovat novou aplikaci. Tato forma distribuce aplikací je pro uživatele výhodná – Apple vždy zkontroluje kód vývojáře a dohlíží tak na bezpečnost a výkon platformy. Pro Mac lze software získat i mimo App Store.

Mezi oblíbené tituly, které nejsou v obchodě Mac App Store, patří například TeamViewer nebo Adobe Creative Suite. Proto je důležité mít po ruce takové nástroje, které umožní software distribuovat na spravované počítače. Některé nástroje mají schopnost vytvářet vlastní balíčky.pkg nebo otisky.dmg a nasadit je na spravované počítače bez toho, aby uživatelé museli být správci.

Mezi oblíbené nástroje patří například open source projekt studia Walt Disney Animation Studios nazvaný Munki. Pokud jej doplníte o další podpůrné nástroje jako například AutoPkg, rázem máte k dispozici kompletní ekosystém potřebný k distribuci aplikací pro Mac získaných mimo App Store.

Stejným způsobem lze nainstalovat například i nové ovladače k tabletu, tiskárně nebo skeneru, popřípadě další komponenty systému. Zajímavostí je, že výše uvedený nástroj Munki přidává VMware k produktu Workspace ONE.

4. INVENTÁŘ

V IT platí pravidlo: „Nelze spravovat to, co nelze změřit.“ Údaje o inventáři hardware a software jsou proto kritické pro další práci administrátora. Umožňují odpovídat na základní otázky, jako: „Jsu všechna moje zařízení zabezpečena?“, nebo: „Kolik a jaké aplikace jsme nasadili?“

Některé nástroje však umožňují shromažďovat další informace o dalších doplňcích hardwaru nebo softwaru. Lze tak snadno zjistit, kdy došlo k poslednímu spuštění zálohy a s jakým výsledkem zálohování skončilo. S úspěchem nabízíme klientům nástroj Sensei MacReport, který je postaven na open

source řešení MunkiReport a je upraven tak, aby vyhovoval jejich podmínkám.

5. BEZPEČNOST

Každoročními aktualizacemi hlavních verzí macOS, iOS, iPadOS a tvOS nastavila společnost Apple poměrně svižné tempo. Kromě nových a skvělých funkcí, které zajímají spíše koncového spotřebitele, přidává bezpečnostní vrstvy a opravuje známé chyby. Aktualizace systému mají proto zásadní význam na bezpečnost zařízení a je důležité, aby byly nainstalovány vždy všechny aktualizace operačního systému.

V případě ztráty zařízení mají administrátoři k dispozici navíc Režim ztraceného zařízení, kdy mohou zařízení vzdáleně smazat nebo zamknout. V tomto režimu odesílá zařízení svou aktuální polohu, je možné jej vysledovat a následně vypnout Režim ztraceného zařízení.

6. POSÍLENÍ SOBĚSTAČNOSTI UŽIVATELŮ

Soběstačnost koncových uživatelů je odrazem pandemie COVID-19, díky které se zaměstnanci přesunuli z kanceláří na home office a chtějí si některé základní úkony řešit sami. Proto by neměl chybět nástroj, který dává uživatelům do rukou možnost doinstalovat si ověřené aplikace, tiskárny, popřípadě získat základní nápovědu – a to vše na jedno kliknutí.

Takový katalog aplikací lze vytvořit opět open source nástrojem Managed Software Center. A pokud jste si jako server MDM zvolili VMware Workspace ONE, máte vyhráno. V takovém případě použijte VMware Intelligent Hub, který kombinuje aplikace zakoupené v App Store v rámci Volume Purchase Programu, aplikace mimo App Store díky Workspace ONE Munki, webové aplikace SaaS a aplikace VDI Windows ve VMware Horizon.

Pro základní nápovědu zaměstnanců, která doplňuje HR oddělení, doporučuji použít nástroj Octory a DEPNotify. Jde o „švýcarské nože“ digitálního onboarding a offboarding.

JAKÉ JSOU DALŠÍ KROKY SPRÁVY?

Žádný operační systém nebo hardware však není dokonalý. Bez ohledu na hardware a nástroje musí administrátoři neustále sledovat vývoj v oblasti správy, testovat dopředu nové verze používaných nástrojů, dbát na zabezpečení klíčových oblastí jako například prevence ztráty, nástroje na ochranu koncových bodů či antivirový software. O těch si ale můžeme povědět v některém z dalších dílů věnovaných správě zařízení. 