Přehled nasazování Maců

Úvod

Obsah

Ve společnosti Apple jsme přesvědčeni, že když mají zaměstnanci přístup k těm nejlepším nástrojům a technologiím, můžou odvádět vynikající práci. Všechny naše produkty jsou navržené tak, aby zaměstnanci byli kreativnější a produktivnější a mohli pracovat novými způsoby – v kanceláři i v terénu. Odpovídá to moderním požadavkům zaměstnanců, kteří potřebují mít při práci lepší přístup k informacím a chtějí bezproblémově spolupracovat a sdílet nebo zůstat ve spojení s ostatními a pracovat odkudkoli.

Nastavování a nasazování Maců v současném firemním prostředí nebylo nikdy jednodušší. Pomocí hlavních služeb od společnosti Apple a řešení pro správu mobilních zařízení (MDM) od dalších výrobců může vaše organizace snadno nasazovat Mac v libovolném rozsahu. Pokud už jsou ve vaší organizaci interně nasazená iOS a iPadOS zařízení, většina práce na infrastruktuře potřebné k implementaci macOS je už pravděpodobně hotová.

Nedávná vylepšení zabezpečení, správy a nasazování Macu umožňují organizacím přejít od vytváření neflexibilních bitových obrazů a tradičních vazeb mezi adresáři na bezproblémové procesy přidělování a nasazování zařízení, které se zaměřují na jednotlivé uživatele a které se téměř výhradně spoléhají na nástroje zabudované do macOS.

Tento dokument obsahuje veškeré pokyny potřebné při rozsáhlém nasazování Macu, od základního rozboru stávající infrastruktury přes správu zařízení až po efektivní přidělování zařízení. Témata probíraná v tomto dokumentu jsou podrobněji popsána v online referenčních materiálech k nasazování Macu: support.apple.com/guide/deployment-reference-macos

Začátky

Důležitým počátečním krokem v procesu nasazování je formulování strategie nasazování a plánu spuštění a taky vyhodnocení toho, jakým způsobem už zaměstnanci macOS používají. Je třeba co nejdřív zapojit nezbytné týmy a zajistit, aby postupovaly v souladu s vizí a cíli vašeho programu. Některé týmy začínají malým pilotním programem, v rámci kterého se zjišťuje, jaké výzvy jsou typické pro dané prostředí. Důležité je komunikovat se stávajícími uživateli, od kterých se dovíte, jak se zařízení ve vaší organizaci reálně využívají a jestli neexistují nějaké problémy, o kterých by váš tým měl vědět.

Informace získané v této fázi pomůžou určit, pro jaké role a činnosti zaměstnanců bude využívání Maců nejpřínosnější. IT oddělení potom může vyhodnotit, jestli se macOS má standardně nabízet v celé organizaci, nebo jestli se bude přidělovat jenom na konkrétní pracovní činnosti.

V této fázi se taky zjistí kompletní seznam interních aplikací a nástrojů, u kterých je před plošným nasazením Maců potřeba zajistit kompatibilitu. V první řadě se zaměřte na hlavní kancelářské a komunikační aplikace a aplikace pro spolupráci, které se týkají největšího počtu uživatelů. Nezapomeňte taky na důležité interní služby, jako je podnikový intranet, adresářové služby a software pro evidenci nákladů, které umožňují produktivní práci značné části organizace.

Zjistěte a zdokumentujte veškeré alternativy k ostatním interním nástrojům a v případě potřeby vyzvěte vlastníky jednotlivých aplikací k jejich modernizaci. Uživatele důsledně seznamte se všemi firemními aplikacemi, které budou moct používat, když si vyberou Mac, a podle poptávky uživatelů určete priority pro modernizaci. Pokud je to nutné, vytvořte ve spolupráci s majiteli aplikací plán, podle kterého můžou aplikace aktualizovat (s využitím SDK macOS a Swiftu), a zapojte všechny možné firemní partnery, kteří by s vývojem mohli pomoci.

Macy se běžně používají jako zařízení vlastněná organizací. Některé firmy můžou v rámci programu používání vlastního zařízení (Bring Your Own Device – BYOD) zaměstnancům povolit používat jejich vlastní Mac. Když zaměstnancům dáte možnost vlastního výběru produktů Apple, může z toho – bez ohledu na zvolený model vlastnictví – mít přínos celá organizace. Povede to k větší produktivitě, kreativitě, angažovanosti a pracovní spokojenosti zaměstnanců a taky k nižším nákladům díky vyšší zbytkové hodnotě zařízení a efektivnější podpoře. Organizace taky můžou využít různé možnosti leasingu a financování, které jim sníží počáteční pořizovací náklady. Organizace můžou náklady kompenzovat srážkami ze mzdy, když zaměstnanci dostanou novější produkt, nebo zaměstnancům umožnit odkup zařízení po skončení jeho životního cyklu nebo leasingu.

Podnikové zásady, spolu s nasazením, správou a procesy podpory popisovanými v tomto dokumentu, se v závislosti na některých informacích, které váš tým shromáždí při pilotním programu, můžou lišit. Ne všichni uživatelé musí používat úplně stejné zásady, nastavení a aplikace – požadavky se můžou výrazně lišit mezi různými skupinami nebo týmy v rámci společnosti.

Postup nasazení

Nasazení macOS probíhá ve čtyřech hlavních krocích: příprava prostředí, nastavení řešení MDM, nasazení zařízení zaměstnancům a nakonec průběžná správa.

1. Příprava

Prvním krokem jakékoli implementace je vzít v úvahu existující prostředí. Tato fáze zahrnuje důkladné seznámení s vaší sítí a klíčovou infrastrukturou a taky nastavení systémů potřebných k úspěšnému nasazení.

Vyhodnocení infrastruktury

I když jde Mac bezproblémově integrovat do většiny standardních podnikových IT prostředí, je pořád důležité vyhodnotit vaši stávající infrastrukturu, aby vaše organizace mohla plně využívat všechno, co macOS nabízí. Pokud vaše organizace potřebuje v tomto ohledu pomoct, můžete se obrátit na Profesionální služby Apple nebo na technické týmy vašeho dodavatele nebo partnera.

Wi-Fi a sítě

Pro nastavení a konfiguraci macOS zařízení je rozhodující konzistentní a spolehlivý přístup k bezdrátové síti. Zkontrolujte, jestli má vaše společnost správně navrženou Wi-Fi síť, včetně pečlivého zvážení umístění a napájení přístupových bodů, aby byly splněny požadavky na nepřetržité připojení při pohybu v celém firemním areálu a na potřebnou kapacitu.

Pokud se zařízení nemůžou připojit k serverům Apple, službě Apple Push Notification (APNs), iCloudu nebo iTunes Storu, možná je potřeba upravit konfigurace webových proxy serverů nebo portů firewallu. Stejně jako v případě iPadu a iPhonu platí, že některé části procesu nasazování Macu (hlavně u novějšího hardwaru Mac) vyžadují přístup k těmto službám, aby bylo možné během instalace aktualizovat firmware a provádět další činnosti.

Společnosti Apple a Cisco taky optimalizovaly způsob, jakým Macy komunikují s bezdrátovými sítěmi Cisco, a přidali do macOS podporu vyspělých síťových funkcí, jako je Quality of Service (QoS). Pokud máte síťová zařízení Cisco, pak ve spolupráci se svými interními týmy zajistěte, aby Mac dokázal optimalizovat důležité datové přenosy.

Firmy by taky měly vyhodnotit svoji VPN infrastrukturu a ujistit se, že uživatelé můžou bezpečně na dálku přistupovat k firemním zdrojům. Zvažte použití funkce VPN na vyžádání, která je součástí macOS, aby se VPN připojení navazovalo jenom v případě potřeby. Pokud máte v plánu používat VPN na úrovni aplikací, ujistěte se, že VPN brány tyto funkce podporují a že máte zakoupený dostatečný počet licencí k pokrytí odpovídajícího počtu uživatelů a připojení.

Vaše síťová infrastruktura musí být správně nastavená, aby podporovala Bonjour, síťový protokol vytvořený společností Apple, který je založený na standardech a vyžaduje nulovou konfiguraci. Bonjour umožňuje zařízením automaticky vyhledávat služby v síti. Zařízení s macOS používají Bonjour pro připojování k tiskárnám podporujícím AirPrint a k zařízením podporujícím AirPlay, například

Apple TV. Některé aplikace a vestavěné funkce macOS taky Bonjour používají ke zjišťování dalších zařízení pro účely spolupráce a sdílení.

Další informace o návrhu Wi-Fi sítí:
support.apple.com/guide/deployment-reference-macos

Přečtěte si, jak vaši síť nakonfigurovat pro MDM:
support.apple.com/HT210060

Další informace o Bonjour:
support.apple.com/guide/deployment-reference-macos

Správa identit
macOS má přístup k adresářovým službám pro správu identit a dalších uživatelských dat, jako například Active Directory, Open Directory a LDAP. Někteří dodavatelé řešení MDM automaticky poskytují i nástroje na integraci jejich administračního řešení se službou Active Directory a adresáři LDAP. Další nástroje, jako rozšíření Kerberos pro jednotné přihlašování v macOS Catalina, umožňují integraci se zásadami a funkcemi služby Active Directory, aniž by vyžadovaly tradiční propojení a mobilní účet. Vaše řešení MDM taky může spravovat různé typy certifikátů od interních i externích certifikačních autorit, takže dochází k automatickému nastavení důvěryhodnosti identit.

Další informace o novém rozšíření Kerberos pro jednotné přihlašování:
support.apple.com/guide/deployment-reference-macos

Další informace o integraci adresářových služeb:
support.apple.com/guide/deployment-reference-macos

Základní služby pro zaměstnance
Ověřte, jestli je vaše služba Microsoft Exchange aktualizovaná a nakonfigurovaná na podporu všech uživatelů v síti. Pokud nepoužíváte Exchange, macOS spolupracuje i s jinými servery založenými na standardech jako IMAP, POP, SMTP, CalDAV, CardDAV a LDAP. Otestujte základní pracovní postupy pro e-maily, kontakty, kalendáře a ostatní podnikový kancelářský software a software pro spolupráci, který zajišťuje většinu každodenních pracovních aktivit.

Další informace o konfiguraci Microsoft Exchange:
support.apple.com/guide/deployment-reference-macos

Další informace o službách používajících standardy:
support.apple.com/guide/deployment-reference-macos

Ukládání obsahu do mezipaměti
Služba ukládání do mezipaměti zabudovaná do macOS ukládá místní kopii často požadovaného obsahu ze serverů Apple, čímž pomáhá šetřit síťovou kapacitu potřebnou ke stahování obsahu ve vaší síti. Ukládání obsahu do mezipaměti urychluje stahování softwaru z Mac App Storu. Může taky ukládat aktualizace softwaru a urychlit tak jejich stahování do firemních zařízení s macOS, iOS i iPadOS. Pomocí řešení od společností Cisco a Akami se dá do mezipaměti ukládat i obsah od jiných výrobců.

Další informace o ukládání obsahu do mezipaměti:
support.apple.com/guide/deployment-reference-macos

Zavedení řešení správy

Řešení MDM organizacím umožňuje bezpečnou registraci Maců v podnikovém prostředí, bezdrátovou konfiguraci a aktualizaci nastavení, nasazování aplikací, monitorování souladu se zásadami, dotazování zařízení a vzdálené mazání nebo zamykání spravovaných zařízení. IT oddělení může snadno vytvářet profily pro správu uživatelských účtů, konfigurovat nastavení systému, vynucovat omezení a nastavovat zásady hesel – stačí k tomu stejné řešení správy mobilních zařízení, jaké se v současnosti používá pro iPhone a iPad.

Všechny platformy Apple na pozadí používají společný framework Apple pro správu, který zákazníkům umožňuje pracovat s různými řešeními MDM od jiných výrobců. Existuje široká řada řešení správy zařízení od společností jako Jamf, VMware a MobileIron. macOS sice sdílí spoustu stejných frameworků pro správu zařízení s iOS a iPadOS, ale řešení správy MDM od jiných dodavatelů se mírně liší z hlediska administrátorských funkcí, podpory operačního systému, cenové strategie nebo modelu hostování. Můžou taky nabízet různé úrovně služeb pro integraci, školení a podporu. Před volbou řešení vyhodnoťte, které funkce jsou pro vaši organizaci nejdůležitější.

Až si vyberete řešení MDM, budete muset navštívit portál Apple Push Certificates, přihlásit se a vytvořit si nový push certifikát pro MDM.

Další informace o nasazení MDM:
support.apple.com/guide/deployment-reference-macos

Navštivte portál Apple Push Certificates Portal:
identity.apple.com/pushcert/

Registrace do Apple Business Manageru

Apple Business Manager je webový portál pro správce IT, který jim umožňuje nasazovat iPhony, iPady, iPody touch, Apple TV a Macy z jednoho místa. Apple Business Manager hladce spolupracuje s vaším řešením správy mobilních zařízení (MDM) a usnadňuje automatické nasazování zařízení, kupování aplikací, distribuování obsahu a vytváření spravovaných Apple ID pro zaměstnance.

Program registrace zařízení (DEP) a Program hromadných nákupů (VPP) jsou teď kompletně integrované do Apple Business Manageru, takže organizace mají na jednom místě všechno, co potřebují k nasazování zařízení Apple. Tyto programu nebudou od 1. prosince 2019 dále dostupné.

Zařízení

Apple Business Manager umožňuje automatickou registraci zařízení, což dává organizacím rychlý a optimalizovaný způsob, jak nasazovat zařízení Apple vlastněná firmou a registrovat je do MDM bez toho, aby bylo nutné s nimi fyzicky manipulovat nebo připravovat každé zvlášť.

- Uživatelům můžete zjednodušit proces nastavení tím, že optimalizujete kroky Průvodce nastavením a zajistíte, aby uživatelé hned po aktivaci měli správnou

konfiguraci. IT týmy teď můžou proces nastavení dál přizpůsobit vlastním textem o vyjádření souhlasu, logem firmy nebo moderními způsoby ověřování.

- Zařízení vlastněná firmou můžete mít pod kontrolou pomocí funkce dozorování, která zpřístupňuje další možnosti správy zařízení, které v jiných modelech nasazení nejsou dostupné, včetně nemožnosti odebrat MDM.
- Můžete snadno spravovat výchozí MDM servery nastavením výchozího serveru podle typu zařízení. iPhone, iPad a Apple TV teď můžete ručně zaregistrovat pomocí Apple Configuratoru 2 a vůbec nezáleží na tom, jak jste si je pořídili.

Obsah

Apple Business Manager umožňuje organizacím jednoduše kupovat obsah ve velkém množství. Ať už vaši pracovníci používají iPhony, iPady, nebo Macy, můžete jim nabízet skvělý obsah okamžitě připravený k práci, který se dá flexibilně a bezpečně distribuovat.

- Kupujte hromadně aplikace, knihy a vlastní aplikace – anebo nasazujte aplikace vyvinuté interně. Licence k aplikacím se dají snadno přenášet mezi různými místy nebo sdílet různými kupujícími na stejném místě. A k dispozici je taky přehledný výpis historie nákupů včetně aktuálního počtu licencí používaných v rámci MDM.
- Distribuujte aplikace a knihy přímo do spravovaných zařízení nebo oprávněným uživatelům a jednoduše sledujte, jaký obsah je přidělený konkrétním uživatelům nebo zařízením. Díky správě distribuce máte celý postup pod kontrolou a aplikace zůstanou ve vašem vlastnictví. Aplikace, které už zařízení nebo uživatel nepotřebují, můžete odebrat a přidělit je někomu jinému z organizace.
- Platťte různými způsoby včetně platebních karet nebo nákupních objednávek. Organizace si můžou koupit kredit na hromadné nákupy (pokud je k dispozici) přímo od společnosti Apple nebo od autorizovaného prodejce Apple. Kredit obchodu v přesné hodnotě v místní měně pak přijde elektronicky majiteli účtu.
- Distribuujte aplikace do zařízení nebo uživatelům v libovolné zemi, kde je aplikace dostupná, čímž ve své organizaci umožníte mezinárodní distribuci. Vývojáři můžou svoje aplikace zpřístupnit v různých zemích tím, že je standardně publikují v App Storu.

Poznámka: Nakupování knih v Apple Business Manageru není k dispozici ve všech zemích a oblastech. Informace o dostupnosti funkcí a způsobů platby najdete na stránce support.apple.com/HT207305.

Lidé

Apple Business Manager dává organizacím nástroje na vytváření a správu zaměstnaneckých účtů, které jsou integrované s existující infrastrukturou a umožňují přístup k aplikacím a službám Apple a taky k Apple Business Manageru.

- Zaměstnancům můžete vytvářet spravovaná Apple ID, která jim umožní spolupracovat v aplikacích a službách Apple a přistupovat k firemním datům ve spravovaných aplikacích, které používají iCloud Drive. Tyto účty vlastní a spravuje přímo vaše organizace.

- Po propojení Apple Business Manageru s Microsoft Azure Active Directory můžete používat federované ověřování. Každému zaměstnanci se automaticky vytvoří spravované Apple ID, když se na kompatibilním zařízení Apple poprvé přihlásí svými stávajícími přihlašovacími údaji.
- Nové funkce registrace uživatelů v iOS 13, iPadOS a macOS Catalina umožňují používat na zařízeních patřících zaměstnancům spravovaná Apple ID zároveň s osobními Apple ID. Anebo můžete na kterémkoli zařízení používat spravované Apple ID jako primární (a jediné) Apple ID. Po prvním přihlášení na zařízení Apple se uživatelé pomocí spravovaných Apple ID dostanou i k iCloudu na webu.
- Různým IT týmům ve vaší organizaci můžete přiřadit různé role, což vám v Apple Business Manageru usnadní správu zařízení, aplikací a účtů. Pomocí role administrátora můžete podle potřeby přijmout smluvní podmínky nebo snadno přenést zodpovědnost, když z vaší organizace někdo odejde.

Poznámka: Registrace uživatelů momentálně nepodporuje iCloud Drive. iCloud Drive se dá se spravovanými Apple ID používat, jen pokud na zařízení není žádné jiné Apple ID.

Další informace o Apple Business Manageru: apple.com/cz/business/it

Registrace do programu Apple pro podnikové vývojáře

Apple Developer Enterprise Program nabízí kompletní sadu nástrojů pro vývoj, testování a distribuci aplikací uživatelům. Aplikace můžete distribuovat buď jejich hostováním na webovém serveru, nebo pomocí řešení MDM. Aplikace a instalátory pro Mac můžete podepsat a notarizovat svým ID vývojáře v Gatekeeperu, což pomáhá chránit macOS před malwarem.

Další informace o Developer Enterprise Programu:
developer.apple.com/programs/enterprise

2. Nastavení

Příprava nasazení obnáší i nadefinování podnikových zásad a nastavení řešení správy mobilních zařízení (MDM) na konfiguraci Maců vašich zaměstnanců.

Jak funguje zabezpečení macOS

Na soukromí a zabezpečení klade Apple při vývoji veškerého svého hardwaru, softwaru i služeb maximální důraz. Soukromí našich zákazníků chráníme prostřednictvím silného šifrování a striktních zásad, které řídí způsob zacházení s daty. Bezpečnost výpočetní platformy pro zařízení Apple je založená na následujících věcech:

- Metody bránící neautorizovanému používání zařízení
- Ochrana uložených dat, i v případě ztráty nebo zcizení zařízení
- Síťové protokoly a šifrování dat při přenosech
- Možnost bezpečného spouštění aplikací bez ohrožení integrity platformy

Všechna zařízení Apple obsahují několik vrstev zabezpečení, aby mohla bezpečně přistupovat k síťovým službám a chránit důležitá data. macOS, iOS a iPadOS zajišťují zabezpečení taky pomocí zásad přístupových kódů a hesel,

které můžete nastavit a vynutit přes MDM. Když se zařízení dostane do nesprávných rukou, může z něj uživatel nebo administrátor pomocí vzdálených příkazů vymazat veškeré osobní informace.

IT oddělení může přes MDM nasadit spoustu bezpečnostních zásad, které zařízení ochrání. Sem patří například vynucení FileVaultu a úschovy klíčů obnovení, vynucení konkrétní zásady hesla nebo zámku spořiče obrazovky a povolení zabudované brány firewall.

Další informace o zabezpečení platformy Apple: apple.com/security/

Definování podnikových zásad

Při určování podnikových zásad začněte stanovením všeobecných zásad, které se týkají většiny uživatelů Maců ve vaší společnosti. Řešení MDM vám umožní zadefinovat přizpůsobení specifická pro konkrétní uživatele, třeba nastavení účtů nebo přístupu k různým aplikacím. Můžete taky nastavit konkrétní zásady pro organizace nebo jiné menší podmnožiny uživatelů, například nasazovat software a nastavení jenom konkrétním oddělením.

Ve spolupráci se svými interními týmy aktualizujte existující podnikové zásady tak, aby zohledňovaly používání Maců. Některé základní zásady jsou ve všech platformách pořád stejné – například požadavky na složitost a obměňování hesel, časy spuštění spořiče obrazovky a přípustné používání.

Pokud vaše podnikové zásady vyžadují specifickou technologii používanou na jiné platformě, seznamte se se základním problémem a zásadu nadefinujte znova, aby se týkala technologií zabudovaných do macOS. Místo požadavku, aby všechny počítače k šifrování celého disku používaly konkrétní řešení jiného výrobce, zvažte vytvoření zásady, která vyžaduje šifrování podnikových dat pomocí FileVaultu. Pokud zásady vyžadují konkrétní software na ochranu proti malwaru, seznamte týmy se zabudovanými funkcemi, jako je Gatekeeper, a zásady upravte tak, aby ho povolovaly.

Konfigurace nastavení v řešení MDM

Aby bylo možné zapnout správu podnikových zásad a zajistit přístup zaměstnanců k nezbytným zdrojům, musí být všechny Macy bezpečně zaregistrované do řešení MDM. Řešení MDM potom můžou aplikovat zásady a nastavení pomocí konfiguračních profilů. Konfigurační profily jsou XML soubory vytvořené řešením MDM, které umožňují distribuovat nastavení do zařízení. Profily automatizují konfiguraci nastavení, účtů, zásad, omezení a přihlašovacích údajů. Pro vyšší zabezpečení vašich systémů se dají i podepsat a zašifrovat.

Jakmile je zařízení zaregistrováno do řešení MDM, může administrátor začít uplatňovat zásady, možnosti nebo příkazy MDM. Když se zařízení připojí k síti, dostane přes službu Apple Push Notification (APN) pokyn, aby prostřednictvím zabezpečeného spojení začalo komunikovat přímo s řešením MDM a zpracovalo akci zadanou správcem. Komunikace probíhá jenom mezi řešením MDM a zařízením, takže služba APN nebude přenášet žádné důvěrné ani chráněné informace. Když zařízení odeberete ze správy, odstraní se i nastavení a zásady řízené jeho konfiguračním profilem. Společnost taky v případě potřeby může zařízení na dálku vymazat.

Spousta organizací připojuje svoje řešení MDM ke stávajícím adresářovým službám. Průvodce nastavením v macOS může uživatele při automatizované registraci zařízení vyzvat, aby se přihlásili pomocí svých přihlašovacích údajů k adresářové službě. Nové možnosti přizpůsobení v macOS Catalina umožňují uzpůsobit Průvodce nastavením tak, aby zobrazoval ověřování přes cloudové poskytovatele identit. Jakmile bude zařízení přiděleno konkrétnímu uživateli, můžete přes řešení MDM upravit konfigurace a účty specifické pro jednotlivce nebo skupinu. Například můžete uživateli během registrace automaticky vytvořit zřídit Microsoft Exchange. Je taky možné použít certifikační identity pro technologie jako 802.1x, VPN a další.

Díky kontrole, kterou tyto systémy poskytují, společnosti často bez problémů udělují uživatelům plný správcovský přístup k jejich Macu, umožňují jim plně personalizovat nastavení, instalovat aplikace a řešit problémy, a přitom mají prostřednictvím řešení MDM pořád plnou kontrolu nad podnikovými zásadami. Tento model se řídí oprávněními a možnostmi ovládání, které uživatelé mají nad svým spravovaným iPhonem nebo iPadem.

Další informace o konfiguračních profilech:
support.apple.com/guide/deployment-reference-macos

Příprava na automatizovanou registraci zařízení

Nejjednodušší způsob, jak zařízení zaregistrovat do MDM, je v Průvodci nastavením pomocí funkcí automatizované registrace zařízení, které jsou součástí Apple Business Manageru. Není přitom potřeba obracet se na IT oddělení a některé obrazovky Průvodce nastavením se dají zjednodušit tak, aby uživatel zvládl celý postup rychleji.

Automatizovanou registraci zařízení nakonfigurujete tak, že své řešení MDM propojíte pomocí zabezpečeného tokenu se svým účtem Apple Business Manageru. Řešení MDM se potom bezpečně autorizuje pomocí dvoufázového ověření. Dodavatel MDM může poskytnout dokumentaci se specifickými informacemi pro konkrétní implementaci.

Pokud už zaměstnanci zařízení používají nebo pokud zařízení vlastní jednotlivci, může uživatel dokončit registraci otevřením jednoho konfiguračního profilu a jeho ověřením v Předvolbách systému. Tento proces se nazývá uživatelem schválená registrace v řešení MDM. Aby bylo možné spravovat určitá nastavení, která jsou z hlediska zabezpečení citlivá (například zásady rozšíření jádra nebo datovou část Privacy Preferences Policy Control), musí registrace proběhnout buď zaregistrováním zařízení, nebo prostřednictvím uživatelem schválené registrace do MDM.

Další informace o načítání rozšíření jádra:
support.apple.com/guide/deployment-reference-macos

Další informace o datové části Privacy Preferences Policy Control:
support.apple.com/guide/mdm

Příprava na distribuci aplikací a knih

Apple nabízí rozsáhlé programy, které vaší organizaci pomůžou využívat skvělé aplikace a obsah pro macOS. Díky těmto možnostem můžete zaměstnancům

distribuovat aplikace a knihy zakoupené v Apple Business Manageru nebo vlastní interní aplikace, aby měli vše, co potřebují k práci. Řešení MDM taky může distribuovat aplikace a instalovat softwarové balíčky, které nejsou dostupné v Mac App Storu.

Řešení MDM podporuje spravovanou distribuci aplikací a knih zakoupených v Apple Business Manageru ve všech zemích, kde je tato aplikace dostupná. Pokud si chcete zapnout spravovanou distribuci, musíte nejdřív propojit své řešení MDM pomocí bezpečného tokenu se svým účtem Apple Business Manageru. Po připojení k řešení MDM můžete uživatelům přidělovat aplikace a knihy i v případě, že je na zařízení vypnutý App Store. Aplikace taky můžete přidělovat přímo k zařízením, čímž se vaše nasazení výrazně usnadní, protože všichni uživatelé daného zařízení budou mít přístup ke všem aplikacím.

Další informace o nakupování obsahu přes Apple Business Manager:
support.apple.com/guide/apple-business-manager

Další informace o distribuci aplikací a knih:
support.apple.com/guide/apple-business-manager

Příprava dalšího obsahu

Řešení MDM vám může pomoct distribuovat další balíčky s obsahem, který nepochází z Mac App Storu. Jde o běžný postup u spousty balíčků podnikového softwaru, například u vlastních interních aplikací nebo aplikací jako Chrome a Firefox. Touto metodou můžete po dokončení registrace automaticky rozdistribuovat a nainstalovat požadovaný software. Prostřednictvím balíčků je možné taky instalovat písma, spouštět skripty a zpracovávat další položky. Balíčky musí být řádně podepsané vaším ID vývojáře z Developer Enterprise Programu.

Další informace o instalaci dodatečného obsahu:
support.apple.com/guide/deployment-reference-macos

3. Nasazení

macOS umožňuje snadné nasazení zařízení zaměstnancům, provedení potřebné personalizace a zahájení práce bez nutnosti zásahu IT oddělení.

Pomocí Průvodce nastavením

Zaměstnanci můžou při spuštění pomocí Průvodce nastavením v macOS nastavit předvolby jazyka a oblasti a připojit se k síti. Po připojení k internetu se uživatelům zobrazí řada oken Průvodce nastavením se základními kroky nastavení nového Macu. Při tomto procesu se zařízení zaregistrovaná do Apple Business Manageru dají automaticky zaregistrovat do MDM. Macy registrované pomocí registrace zařízení se taky dají nakonfigurovat tak, aby přeskočily určité obrazovky, třeba smluvní podmínky, přihlášení pomocí Apple ID, nastavení polohových služeb a další.

Po dokončení úvodního nastavení v Průvodci nastavením můžete pomocí MDM provést podrobnější nastavení, například definovat, jestli bude mít uživatel na svém počítači úplná administrátorská práva. Stejně jako v případě iPhonu

a iPadu tím uživatel získá kontrolu nad svým zařízením, a přitom bude pořád vyhovovat podnikovým zásadám a nastavením spravovaným přes MDM. Aby uživatelé po dokončení Průvodce nastavením mohli okamžitě začít pracovat, měly by se na pozadí začít stahovat a instalovat jenom nejdůležitější aplikace. Stahování a instalaci větších aplikací jde v samoobslužném nástroji řešení MDM naplánovat tak, aby tento proces probíhal na pozadí nebo aby ho uživatel mohl spustit sám později.

Konfigurace podnikových účtů

Řešení MDM může automaticky nastavovat poštu a další uživatelské účty. Podle toho, jaké řešení MDM používáte a jak je integrované do vašich interních systémů, můžou mít datové části vašich účtů předem vyplněné jméno, e-mailovou adresu uživatele a certifikační identity pro ověřování a podepisování.

Povolení uživatelské personalizace

Když svým uživatelům umožníte personalizaci zařízení, můžete zvýšit jejich produktivitu, protože uživatelé si sami zvolí, které aplikace a obsah potřebují ke splnění svých úkolů a cílů. macOS Catalina teď podporuje spravovaná Apple ID a registraci uživatelů, což dává organizacím nové možnosti, jak uživatelům zajistit přístup k službám Apple pomocí Apple ID vlastněných organizací. Uživatel přitom může na zařízení používat i své osobní Apple ID.

Apple ID a spravované Apple ID

Když se zaměstnanci pomocí Apple ID poprvé přihlásí k službám Apple, jako jsou FaceTime, iMessage, App Store nebo iCloud, získají přístup k širokému výběru obsahu, který jim usnadní práci, zvýší jejich produktivitu a podpoří spolupráci. Stejně jako běžná Apple ID, i spravovaná Apple ID slouží k přihlašování k osobním zařízením. Navíc umožňují přístup k službám Apple – včetně iCloudu nebo spolupráce v Poznámkách a aplikacích iWork – a k Apple Business Manageru. Na rozdíl od klasických Apple ID jsou spravovaná Apple ID vlastněná a spravovaná organizací, která může mimo jiné obnovovat hesla nebo je spravovat na základě rolí. Spravovaná Apple ID mají omezená některá nastavení.

Zařízení zaregistrovaná přes registraci uživatelů vyžadují Apple ID. Registrace uživatelů podporuje volitelně i osobní Apple ID. Další možnosti registrace podporují buď osobní Apple ID, nebo spravované Apple ID. Používání více Apple ID souběžně podporuje jenom registrace uživatelů.

Aby uživatelé z těchto služeb vytěžili maximum, měli by používat svá vlastní Apple ID nebo spravovaná Apple ID, která jim vytvoříte. Uživatelé, kteří Apple ID nemají, si ho můžou vytvořit ještě předtím, než dostanou zařízení. Další příležitost k vytvoření osobního Apple ID dostanou v Průvodci nastavením. K vytvoření Apple ID nepotřebují platební kartu.

Další informace o spravovaných Apple ID:
support.apple.com/guide/deployment-reference-macos

iCloud

iCloud uživatelům umožňuje automaticky synchronizovat dokumenty a osobní obsah, jako jsou kontakty, kalendáře, dokumenty a fotky, aby byly vždy aktuální na všech zařízeních. Služba Najít uživatelům umožňuje vyhledat ztracený nebo ukradený Mac, iPhone, iPad nebo iPod touch. Určité části iCloudu, jako Klíčenka

na iCloudu a iCloud Drive, jde zakázat pomocí omezení zadaných ručně na zařízení nebo nastavených prostřednictvím řešení MDM. Organizace díky tomu mají kontrolu nad tím, jaká data se budou ukládat na jakém účtu.

Další informace o správě iCloudu:
support.apple.com/guide/deployment-reference-macos

4. Správa

Jakmile mají uživatelé všechno nastavené a funkční, je k dispozici široká škála možností umožňující správu zařízení a obsahu.

Správa zařízení

Ke správě zařízení slouží v řešení MDM sada konkrétních akcí. K těm patří vyžádání informací ze zařízení nebo vyvolání počátečních kroků, které umožňují správu zařízení, pokud nevyhovují zásadám, jsou ztracená nebo odcizená.

Dotazy

Řešení MDM se zařízení může dotazovat na různé informace a zajistit tak, aby uživatelé používali správné aplikace a nastavení. Dotazy se můžou týkat hardwaru, třeba sériového čísla a modelu zařízení, nebo softwaru, například verze macOS nebo seznamu nainstalovaných aplikací. MDM se navíc může dotazovat na stav hlavních bezpečnostních funkcí, jako je FileVault nebo zabudovaný firewall.

Správcovské akce

Na spravovaném zařízení může řešení MDM provádět celou řadu správcovských akcí, včetně automatických změn konfiguračních nastavení bez zásahu uživatele, provedení aktualizace macOS, vzdáleného zablokování a vymazání zařízení nebo správy hesel.

Další informace o správcovských akcích:
support.apple.com/guide/deployment-reference-macos

Správa aktualizací softwaru

IT oddělení může uživatelům umožnit upgrade na nejnovější verzi operačního systému, která právě vyšla. Testováním předběžných verzí macOS může IT oddělení včas zjistit problémy s kompatibilitou aplikací a vyřešit je s vývojáři před vydáním konečné verze. IT oddělení může otestovat všechny verze v rámci Apple Beta Software Programu nebo AppleSeed pro IT. Macy aktualizujte pečlivě, ať ochráníte uživatele a jejich data. Na nové verze přecházejte hned, jak si ověříte, že vaše pracovní postupy jsou s novou verzí macOS kompatibilní.

Do Maců zaregistrovaných pomocí registrace zařízení může MDM přenášet aktualizace macOS automaticky. Mac zaregistrovaný pomocí registrace zařízení se taky dá nakonfigurovat tak, aby aktualizace a upozornění na aktualizace odložil až o 90 dní, pokud vaše důležité systémy nejsou na aktualizaci připravené. Dokud tahle zásada platí nebo řešení MDM nepošle příkaz k instalaci, nemůžou uživatelé zahájit aktualizaci ručně.

Apple pro upgrady nedoporučuje ani nepodporuje monolitické bitové obrazy systému. Macy, stejně jako iPhony a iPady, často vyžadují aktualizace firmwaru

specifické pro jejich model. Navíc aktualizace operačního systému Macu vyžadují, aby aktualizace firmwaru pocházela přímo od společnosti Apple. Nejspolehlivější je použít k aktualizaci instalátor macOS nebo příkazy MDM.

Správa dalšího softwaru

Organizace svým uživatelům často potřebují distribuovat aplikace, které nejsou součástí základní sady. U důležitých aplikací a aktualizací se to dá provádět automaticky řešením MDM anebo na vyžádání, kdy zaměstnancům umožníte požadovat aplikace prostřednictvím samoobslužného portálu poskytovaného vaším řešením MDM. Tyto portály můžou provádět cokoli od instalace softwaru zakoupeného v App Storu prostřednictvím Apple Business Manageru až po instalaci aplikací, skriptů a dalších nástrojů, které nepochází z App Storu.

Většinu softwaru je sice možné instalovat automaticky, některé aplikace ale můžou vyžadovat zásah uživatele. V zájmu vyšší bezpečnosti teď aplikace, které vyžadují rozšíření jádra, potřebují souhlas uživatele k načtení. Říká se tomu uživatelem schválené načítání rozšíření jádra a je možné ho spravovat přes MDM.

Udržování bezpečnosti zařízení

Navíc k počáteční sadě bezpečnostních zásad, které byly zavedeny před nasazením zařízení, bude váš tým chtít prostřednictvím řešení MDM sledovat dodržování zásad jednotlivými počítači a získávat co nejvíc zpráv a hlášení. Sem může patřit sledování bezpečnostní situace jednotlivých zařízení nebo shromažďování informací o instalaci softwarových patchů. Většina organizací sice k šifrování a ochraně Maců bez problémů využívá nativní nástroje, ale některé organizace můžou vyžadovat používání dalších služeb sdílení a synchronizace souborů nebo nástroje na ochranu před ztrátou dat, aby se chránily před únikem podnikových dat a aby mohly zajistit detailní hlášení týkající se citlivých dat.

Funkce iCloudu zvaná Najít můj Mac může v případě ztráty nebo krádeže Macu vyvolat jeho vzdálené vymazání, čímž se odstraní veškerá data a Mac se zablokuje. IT oddělení taky může přes MDM provést vzdálené vymazání.

Opětovné přidělení zařízení

Když nějaký zaměstnanec opustí organizaci, jde Mac pomocí zotavení z internetu a místního zotavovacího oddílu znova snadno přidělit dalšímu uživateli. Tento proces umožňuje vymazat obsah Macu a nainstalovat nejnovější verzi operačního systému. Mac přiřazený v Apple Business Manageru ke konkrétnímu programu MDM se v průběhu Průvodce nastavením automaticky znova zaregistruje do programu MDM, nakonfigurují se na něm nastavení pro nového uživatele, použijí se firemní zásady a nasadí se veškerý příslušný software. Nezaregistrovaný Mac se stejným způsobem dá vymazat, znovu přidělit a potom zaregistrovat ručně.

Možnosti podpory

Spousta organizací zjišťuje, že uživatelé Maců potřebují jen minimální podporu IT oddělení. Většina IT týmů vyvíjí nástroje, které umožňují podporu svépomocí a zvyšují celkovou kvalitu podpory. Proto vznikl třeba rozsáhlý web podpory pro Macy, kde se dají najít online fóra věnovaná podpoře svépomocí a poskytování technické podpory přímo na místě. Díky řešením MDM si uživatelé některé činnosti podpory, jako je instalace nebo aktualizace softwaru ze samoobslužného portálu, zařídí sami.

Doporučujeme ale, aby společnosti nenutily uživatele k tomu, aby byli při podpoře odkázáni jenom sami na sebe. Místo toho problémy řešte spoluprací a soustřeďte se na to, aby uživatelé před zavoláním technické podpory měli možnost problém vyřešit sami. Povzbuzujte uživatele, aby se aktivně zapojili a problémy zkoumali sami, než zavolají pomoc.

Sdílená zodpovědnost za řešení problémů snižuje prostoje zaměstnanců a celkové náklady na podporu a zaměstnance podpory. Náročnějším organizacím nabízí AppleCare celou řadu programů a služeb, které doplňují vaše interní struktury pro podporu zaměstnanců IT.

AppleCare for Enterprise

Pokud společnost potřebuje nepřetržitou podporu, může podnikový program AppleCare ulevit internímu helpdesku tím, že zaměstnancům poskytuje nepřetržitou podporu po telefonu. Na urgentní problémy navíc reaguje do jedné hodiny. Program pomáhá IT oddělení s integrací, například s MDM a službou Active Directory.

Podpora AppleCare pro operační systémy

Podpora AppleCare pro operační systémy pomůže vašemu IT oddělení s nasazováním iOS, iPadOS, macOS a macOS Serveru na úrovni celé instituce. V závislosti na tom, jakou úroveň podpory si objednáte, vám bude k dispozici nepřetržitá podpora a přiřazený správce účtu. Podpora AppleCare pro operační systémy vám umožní přímé spojení s techniky, kteří vám poradí s integrací, migrací a složitějšími problémy se serverem, takže vaši IT pracovníci budou moct efektivněji nasazovat a spravovat zařízení nebo řešit problémy.

Podpora AppleCare přes helpdesk

Helpdesk AppleCare vás po telefonu přímo propojí se zkušenými technickými poradci Apple. Podpora navíc zahrnuje i spoustu nástrojů na diagnostiku a řešení problémů s hardwarem Apple, což velkým organizacím pomáhá efektivněji využívat zdroje, zkracuje reakční dobu a snižuje náklady na školení. Helpdesk AppleCare pokrývá neomezený počet událostí podpory, které se týkají diagnostiky hardwaru a softwaru, zjišťování příčin potíží s iOS a iPadOS zařízeními a řešení problémů.

AppleCare a AppleCare+ pro Mac

Každý Mac se dodává s jednoletou omezenou zárukou a bezplatnou technickou podporou po telefonu po dobu 90 dní od data nákupu. Toto servisní krytí je možné rozšířit až na dobu tří let od původního data nákupu zakoupením programu AppleCare+ nebo AppleCare Protection Plan. Zaměstnanci pak můžou volat na podporu Apple s otázkami ohledně hardwaru nebo softwaru Apple. Apple navíc nabízí i praktické možnosti servisu, když potřebujete zařízení opravit. Navíc AppleCare+ pro Mac kryje až dva incidenty neúmyslného poškození (každý podléhá servisnímu poplatku).

Další informace o možnostech podpory AppleCare:
apple.com/support/professional/

Shrnutí

Ať už vaše firma nasazuje Macy ve skupině uživatelů, nebo v celé organizaci, máte řadu možností, jak nasazení i správu zařízení snadno provést. Výběrem vhodné strategie pro vaši organizaci pomůžete zaměstnancům zvýšit výkonnost a přistupovat k práci zcela novými způsoby.

Další informace o nasazování, správě a bezpečnostních funkcích macOS:
support.apple.com/guide/deployment-reference-macos

Další informace o nastaveních správy mobilních zařízení pro IT:
support.apple.com/guide/mdm

Další informace o Apple Business Manageru:
support.apple.com/guide/apple-business-manager

Další informace o spravovaných Apple ID pro firmy:
apple.com/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

Další informace o produktech Apple v práci:
www.apple.com/cz/business/

Další informace o funkcích pro IT:
www.apple.com/cz/business/it/

Další informace o zabezpečení platformy Apple:
www.apple.com/security/

Projděte si dostupné programy AppleCare:
www.apple.com/support/professional/

Seznamte se se školeními a certifikacemi Apple:
training.apple.com

Kontaktujte Profesionální služby Apple:
consultingservices@apple.com