Panoramica sulla distribuzione del Mac

Introduzione

Apple crede fermamente che il personale delle aziende possa lavorare al meglio quando ha a disposizione gli strumenti e le tecnologie migliori. Tutti i nostri prodotti sono progettati per permettere ai dipendenti di essere più creativi, produttivi e lavorare in modi nuovi, dentro e fuori dall'ufficio. Perché è così che vogliono lavorare oggi: con un migliore accesso alle informazioni, la possibilità di collaborare e condividere dati in modo semplice, e la libertà di restare in contatto e lavorare ovunque.

Configurare e distribuire il Mac in ambito aziendale non è mai stato più facile. Grazie a servizi specifici offerti da Apple e a una soluzione per la gestione dei dispositivi mobili (Mobile Device Management, MDM) di fornitori esterni, le aziende possono distribuire e gestire i dispositivi macOS in modo semplice e su larga scala. Se la tua organizzazione ha già distribuito internamente dispositivi iOS e iPadOS, è probabile che la maggior parte degli interventi sull'infrastruttura necessari per implementare macOS sia già stata eseguita.

Con i recenti miglioramenti in fatto di sicurezza, gestione e distribuzione dei Mac, le organizzazioni possono passare dalla creazione di immagini monolitiche e dal tradizionale binding delle directory a un semplice modello di provisioning con un processo di distribuzione incentrato sui singoli utenti, basato quasi esclusivamente su strumenti già inclusi in macOS.

Questo documento fornisce indicazioni su tutto ciò che serve per distribuire il Mac su larga scala, dalla valutazione dell'infrastruttura esistente alla gestione dei dispositivi, fino alle procedure di provisioning semplificate. Gli argomenti descritti qui sono trattati più ampiamente nella guida "Deployment Reference for Mac" disponibile online:
support.apple.com/guide/deployment-reference-macos

Per cominciare

Nelle fasi iniziali della distribuzione è importante sviluppare una strategia e un piano di implementazione, e valutare il modo in cui macOS viene attualmente usato dai dipendenti. Assicurati che i team necessari siano coinvolti sin dall'inizio e che condividano la vision e gli obiettivi del programma. Alcuni iniziano con un piccolo gruppo di prova per individuare le difficoltà specifiche del proprio ambiente. È fondamentale coinvolgere gli utenti esistenti in un progetto pilota più ampio, per comprendere come vengono usati i dispositivi all'interno dell'organizzazione e se il tuo team deve essere informato di eventuali problematiche.

Le informazioni raccolte in questa fase possono aiutarti a determinare i ruoli e le mansioni dei dipendenti che trarrebbero più vantaggio dall'uso dei computer Mac. Il reparto IT potrà quindi valutare se macOS deve essere offerto come piattaforma standard nell'intera organizzazione o come possibile scelta per specifiche mansioni.

Spesso in questa fase si definisce anche un elenco completo di app e strumenti interni che devono essere compatibili prima di poter distribuire il Mac su larga scala. Concentrati sulle principali app per la produttività, la collaborazione e la comunicazione che saranno usate dalla maggior parte degli utenti. Tieni conto che l'operatività dell'azienda dipende anche da servizi in-house fondamentali come l'intranet, la directory e il software di gestione delle spese.

Documenta e comunica possibili soluzioni o alternative per altri strumenti interni incoraggiando allo stesso tempo i responsabili delle app a modernizzarle secondo necessità. Fai sapere agli utenti quali app aziendali potranno usare se scelgono un Mac, e fai in modo che le loro richieste definiscano le priorità degli interventi di modernizzazione. Se necessario, definisci con i responsabili delle app un piano di aggiornamento utilizzando sia il kit SDK per macOS sia Swift, e coinvolgi i vari partner enterprise che potrebbero fornire assistenza nel processo di sviluppo.

I computer Mac vengono solitamente distribuiti come dispositivi di proprietà dell'azienda. Alcune organizzazioni potrebbero consentire ai dipendenti di acquistare personalmente il Mac da usare al lavoro, nell'ambito di un programma BYOD (Bring Your Own Device). Indipendentemente dal modello di proprietà scelto, permettere al personale di scegliere i prodotti Apple può portare vantaggi all'intera organizzazione: livelli più alti di produttività, creatività, coinvolgimento e soddisfazione professionale, e costi più bassi in considerazione del maggiore valore residuo e del minore ricorso all'assistenza. Le organizzazioni possono anche usufruire di vari piani di leasing e finanziamento per ridurre i costi iniziali, che si possono inoltre compensare permettendo ai dipendenti di contribuire con trattenute sulla busta paga durante un aggiornamento, o di acquistare il computer al termine di un leasing o del suo ciclo di vita.

I criteri aziendali e i processi di distribuzione, gestione e assistenza descritti in questo documento potrebbero variare a seconda delle informazioni raccolte dal tuo team durante il progetto pilota. Non tutti gli utenti hanno bisogno degli stessi criteri e delle stesse impostazioni e app, dato che i requisiti dei diversi gruppi o team all'interno di un'azienda spesso variano sensibilmente.

Fasi della distribuzione

La distribuzione di macOS si articola in quattro fasi principali: la preparazione dell'ambiente, la configurazione della soluzione MDM, la distribuzione dei dispositivi ai dipendenti e lo svolgimento di attività di gestione continuativa.

1. Preparazione

Il primo passo da compiere in ogni distribuzione è valutare l'ambiente esistente, ovvero conoscere meglio la rete e l'infrastruttura, e configurare i sistemi necessari per la riuscita della distribuzione.

Valutare l'infrastruttura

Sebbene il Mac si integri senza problemi nella maggior parte degli ambienti IT aziendali standard, è comunque importante valutare l'infrastruttura esistente per assicurarsi di sfruttare appieno tutto quello che macOS ha da offrire. Se la tua organizzazione necessita di assistenza per questo aspetto, puoi rivolgerti a Apple Professional Services o al team tecnico del tuo rivenditore o partner di canale.

Wi-Fi e connessione in rete

Per impostare e configurare i dispositivi macOS è essenziale poter contare su un accesso costante e affidabile a una rete wireless. Verifica che la rete Wi-Fi della tua azienda sia progettata in modo corretto e valuta attentamente il posizionamento e l'alimentazione dei punti di accesso per assicurarti che rispondano alle esigenze di roaming e capacità.

Se i dispositivi non riescono ad accedere ai server Apple, al servizio di notifiche push di Apple (APNs), ad iCloud e all'iTunes Store, potrebbe anche essere necessario modificare le configurazioni dei web proxy o delle porte del firewall. Come per iPad e iPhone, alcuni passaggi del processo di distribuzione del Mac, soprattutto per l'hardware più recente, richiedono l'accesso a questi servizi per operazioni quali l'aggiornamento del firmware durante l'installazione.

Apple e Cisco hanno ottimizzato il modo in cui i computer Mac comunicano con le reti wireless Cisco grazie al supporto di funzioni di rete evolute in macOS, come la QoS (Quality of Service). Se hai apparecchiature di rete Cisco, lavora con i tuoi team interni per fare in modo che i Mac siano in grado di dare priorità al traffico più importante.

Le aziende devono anche esaminare l'infrastruttura VPN per assicurarsi che gli utenti possano accedere alle risorse interne da remoto tramite una connessione sicura. Considera l'utilizzo della funzione "VPN su richiesta" di macOS per connettersi alla VPN solo quando necessario. Se pensi di usare la funzione "VPN per app", verifica che i tuoi gateway VPN la supportino e acquista un numero di licenze sufficiente per tutti gli utenti e le connessioni.

Assicurati di impostare correttamente la tua infrastruttura di rete affinché funzioni con Bonjour, il protocollo di rete Apple basato su standard che non richiede alcuna configurazione e che consente ai dispositivi di rilevare automaticamente i servizi su una rete. macOS usa Bonjour per collegarsi alle stampanti compatibili con AirPrint e ai dispositivi compatibili con AirPlay, per esempio Apple TV. Anche alcune app e funzioni incluse in macOS utilizzano Bonjour per rilevare altri dispositivi per la collaborazione e la condivisione.

Per saperne di più sulla progettazione della rete Wi-Fi:
support.apple.com/guide/deployment-reference-macos

Per saperne di più sulla configurazione della rete per la soluzione MDM:
support.apple.com/HT210060

Per saperne di più su Bonjour:
support.apple.com/guide/deployment-reference-macos

Gestire le identità
Per gestire le identità e altri dati sugli utenti, macOS può accedere ai servizi di directory, fra cui Active Directory, Open Directory e LDAP. Alcuni fornitori MDM offrono strumenti per integrare fin da subito le loro soluzioni di gestione con Active Directory e le directory LDAP. Altri strumenti, come l'estensione per il Single Sign-on con Kerberos in macOS Catalina, permettono l'integrazione con i criteri e le funzioni di Active Directory senza richiedere il tradizionale binding e un account mobile. La soluzione MDM può anche gestire vari tipi di certificati provenienti da autorità di certificazione (CA) interne o esterne in modo che le identità vengano considerate automaticamente attendibili.

Per saperne di più sulla nuova estensione per il Single Sign-on con Kerberos:
support.apple.com/guide/deployment-reference-macos

Per saperne di più sull'integrazione di directory:
support.apple.com/guide/deployment-reference-macos

Servizi essenziali per i dipendenti
Verifica che il servizio Microsoft Exchange sia aggiornato e configurato per supportare tutti gli utenti sulla rete. Se non utilizzi Exchange, macOS funziona anche con i server basati su standard, fra cui IMAP, POP, SMTP, CalDAV, CardDAV e LDAP. Testa i flussi di lavoro base per le email, i contatti e i calendari, e gli altri software aziendali per la produttività e la collaborazione che saranno usati nella maggior parte dei quotidiani flussi di lavoro degli utenti.

Per saperne di più sulla configurazione di Microsoft Exchange:
support.apple.com/guide/deployment-reference-macos

Per saperne di più sui servizi basati su standard:
support.apple.com/guide/deployment-reference-macos

Cache dei contenuti
La cache dei contenuti è un servizio integrato in macOS che archivia in locale una copia dei contenuti più richiesti dai server Apple, riducendo la larghezza di banda utilizzata per scaricarli sulla rete. Puoi usare la cache dei contenuti per velocizzare il download e la distribuzione di software tramite Mac App Store. Inoltre, questo servizio può conservare nella cache anche gli aggiornamenti software, per un download più rapido sui dispositivi macOS, iOS o iPadOS. Per memorizzare nella cache altri contenuti è possibile utilizzare anche soluzioni Cisco e Akamai.

Per saperne di più sulla cache dei contenuti:
support.apple.com/guide/deployment-reference-macos

Scegliere una soluzione di gestione

Le soluzioni MDM permettono alle organizzazioni di registrare i Mac in modo sicuro nell'ambiente aziendale, configurare e aggiornare le impostazioni in wireless, distribuire app, monitorare la conformità con i criteri imposti, interrogare i dispositivi e perfino inizializzare o bloccare a distanza i dispositivi gestiti. I reparti IT possono creare facilmente profili per gestire gli account utente, configurare le impostazioni di sistema, imporre restrizioni e applicare criteri per le password, tutto dalla stessa soluzione di gestione dei dispositivi mobili che usano già per iPhone e iPad.

Dietro le quinte, tutte le piattaforme Apple usano lo stesso framework di gestione creato da Apple, che permette ai clienti di lavorare con varie soluzioni MDM di altre aziende. Esistono numerose soluzioni per la gestione dei dispositivi offerte da altre aziende, come Jamf, VMware e MobileIron. Benché macOS, iOS e iPadOS condividano molti dei framework per la gestione dei dispositivi, le soluzioni MDM di altre aziende sono leggermente diverse in termini di funzioni amministrative, supporto dei sistemi operativi, fasce di prezzo e modello di hosting. Potrebbero anche offrire diversi livelli di servizi per l'integrazione, la formazione e l'assistenza. Prima di scegliere, valuta quali funzioni di gestione sono più appropriate per la tua organizzazione.

Dopo aver scelto la soluzione MDM, dovrai accedere all'Apple Push Certificates Portal per creare un nuovo certificato push MDM.

Per saperne di più sull'implementazione di una soluzione MDM:
support.apple.com/guide/deployment-reference-macos

Per accedere all'Apple Push Certificates Portal:
identity.apple.com/pushcert/

Iscriversi a Apple Business Manager

Apple Business Manager è un portale web che consente agli amministratori IT di distribuire iPhone, iPad, iPod touch, Apple TV e Mac da un unico posto. Apple Business Manager si integra con la tua soluzione MDM semplificando la distribuzione automatica dei dispositivi, l'acquisto di app, la distribuzione dei contenuti e la creazione di ID Apple gestiti per i dipendenti.

Il Programma di registrazione dei dispositivi (Device Enrollment Program, DEP) e il Volume Purchase Program (VPP) sono stati integrati in Apple Business Manager per offrire in un unico strumento tutto ciò che serve per distribuire i dispositivi Apple. A partire dal 1° dicembre 2019 questi programmi non saranno più disponibili.

Dispositivi

Apple Business Manager consente la registrazione automatica dei dispositivi e offre alle organizzazioni un modo semplice e veloce per distribuire dispositivi Apple di proprietà dell'azienda e registrarli con una soluzione MDM senza doverli preparare fisicamente.

- Semplifica la procedura di setup per gli utenti eliminando alcuni passaggi di Impostazione Assistita, così i dipendenti riceveranno le configurazioni corrette già al momento dell'attivazione. I reparti IT ora possono personalizzare ulteriormente questa esperienza includendo un branding personalizzato, testi sul consenso informato o un moderno metodo di autenticazione.
- Aumenta il livello di controllo sui dispositivi di proprietà dell'azienda attivando la supervisione, che offre ulteriori opzioni di gestione non disponibili per altri modelli di distribuzione, per esempio l'MDM non rimovibile.

- Gestisci più facilmente i server MDM predefiniti impostando un server di default in base al tipo di dispositivo. E adesso puoi registrare manualmente iPhone, iPad e Apple TV usando Apple Configurator 2, indipendentemente da come sono stati acquistati.

Contenuti

Apple Business Manager permette di acquistare contenuti in grandi quantità in modo ancora più semplice. Indipendentemente dal dispositivo utilizzato, iPhone, iPad o Mac, è possibile fornire ai dipendenti straordinari contenuti pronti all'uso, con opzioni di distribuzione sicure e flessibili.

- Acquista app, libri e app personalizzate in grandi quantità, incluse le app sviluppate internamente. Puoi trasferire le licenze delle app da una sede all'altra e condividerle tra acquirenti di una stessa sede. Vedrai una cronologia unificata degli acquisti, con anche l'indicazione del numero di licenze attualmente in uso tramite MDM.
- Distribuisci app e libri direttamente ai dispositivi gestiti o agli utenti autorizzati, tenendo traccia dei contenuti assegnati a ciascuno. Con la distribuzione gestita puoi controllare l'intero processo di distribuzione mantenendo la piena proprietà delle app. E quando un dispositivo o un utente non ha più bisogno di un'app, puoi revocarla e riassegnarla all'interno dell'organizzazione.
- Scegli fra diverse opzioni di pagamento, fra cui carta di credito e ordine d'acquisto. Le organizzazioni possono acquistare un credito a volume (laddove disponibile) direttamente da Apple o da un Rivenditore Autorizzato Apple per importi specifici in valuta locale: verrà inviato elettronicamente al titolare dell'account come credito dello Store.
- Assegna le app a utenti o dispositivi in qualsiasi Paese in cui sono disponibili, per una distribuzione su scala internazionale. Gli sviluppatori possono rendere disponibili le proprie app in diversi Paesi tramite il processo di pubblicazione standard dell'App Store.

N.B. In alcuni Paesi o territori non è possibile acquistare libri tramite Apple Business Manager. Per conoscere la disponibilità delle funzioni e dei metodi di acquisto, vai su support.apple.com/HT207305.

Persone

Apple Business Manager offre alle aziende la possibilità di creare e gestire account per i dipendenti che si integrano con l'infrastruttura esistente e facilitano l'accesso a app e servizi Apple, incluso Apple Business Manager.

- Crea ID Apple gestiti per consentire ai dipendenti di collaborare usando le app e i servizi Apple, e di accedere ai dati di lavoro nelle app gestite che usano iCloud Drive. Questi account sono di proprietà e sotto il controllo dell'organizzazione.
- Sfrutta l'autenticazione federata collegando Apple Business Manager con Microsoft Azure Active Directory. Gli ID Apple gestiti verranno creati automaticamente quando i dipendenti accedono per la prima volta a un dispositivo Apple compatibile usando le credenziali che hanno già.

- Grazie alle nuove funzioni per la registrazione degli utenti in iOS 13, iPadOS e macOS Catalina, i dispositivi di proprietà dell'utente possono ospitare contemporaneamente un ID Apple gestito e uno personale. In alternativa, gli ID Apple gestiti possono essere utilizzati su qualsiasi dispositivo come ID Apple principale (e unico). Dopo il primo accesso, sarà possibile usare gli ID Apple gestiti anche per iCloud.
- Per gestire dispositivi, app e account in modo efficiente con Apple Business Manager, definisci altri ruoli per i team IT della tua organizzazione. Usa il ruolo Amministratore per accettare termini e condizioni (se necessario) e trasferire facilmente la responsabilità se qualcuno lascia l'organizzazione.

N.B. Al momento iCloud Drive non è compatibile con la registrazione degli utenti. Se l'ID Apple gestito è l'unico ID Apple presente sul dispositivo, potrà essere usato per accedere ad iCloud Drive.

Per saperne di più su Apple Business Manager: apple.com/it/business/it

Iscriversi all'Apple Developer Enterprise Program

L'Apple Developer Enterprise Program offre una serie completa di strumenti per sviluppare, testare e distribuire app agli utenti. Puoi distribuire le app ospitandole su un server web oppure usando una soluzione MDM. Le app e gli installer per Mac devono essere firmati e autenticati con il tuo ID sviluppatore per Gatekeeper, che protegge macOS dal malware.

Per saperne di più sul Developer Enterprise Program: developer.apple.com/programs/enterprise

2. Configurazione

In questa fase devi definire i criteri aziendali e preparare la soluzione per la gestione dei dispositivi mobili in modo da poter configurare i Mac per i dipendenti.

Comprendere la sicurezza di macOS

Sicurezza e privacy sono alla base della progettazione di tutti gli hardware, i software e i servizi Apple. Proteggiamo la privacy dei nostri clienti con una codifica forte e politiche rigorose che governano il modo in cui i dati sono gestiti. La creazione di una piattaforma sicura per i dispositivi Apple prevede:

- metodi che impediscono l'uso non autorizzato dei dispositivi;
- protezione dei dati archiviati, anche quando un dispositivo viene smarrito o rubato;
- protocolli di rete e crittografia dei dati in transito;
- tecnologie che consentono di eseguire le app in modo sicuro senza il rischio di compromettere l'integrità della piattaforma.

Tutti i dispositivi Apple integrano vari livelli di sicurezza, in modo che possano accedere senza rischi ai servizi di rete e proteggere i dati importanti. In macOS, iOS e iPadOS, la sicurezza è garantita anche da criteri per codici e password che si possono distribuire e applicare via MDM. Se un dispositivo finisce nelle mani sbagliate, l'utente o l'amministratore può cancellare da remoto tutte le informazioni riservate.

Il reparto IT può usare la soluzione MDM per distribuire una serie di criteri che proteggano i dispositivi: per esempio, può imporre l'uso di FileVault e l'escrow di una chiave di recupero, applicare un criterio specifico per le password o un blocco per il salvaschermo e attivare il firewall integrato.

Per saperne di più sulla sicurezza delle piattaforme Apple: apple.com/security/

Definire i criteri aziendali

Per impostare i criteri aziendali, inizia definendo criteri generali che vadano bene per la maggior parte degli utenti Mac dell'azienda. Con la soluzione MDM potrai impostare configurazioni su misura specifiche per i singoli utenti, come gli account o l'accesso a determinate app. Potrai anche impostare criteri precisi per le organizzazioni o altri sottogruppi di utenti, per esempio distribuendo software o impostazioni specifiche per i reparti.

Lavora con i tuoi team interni per aggiornare i criteri aziendali esistenti in modo da integrare l'uso dei computer Mac. Alcuni criteri chiave, come i requisiti di complessità e rotazione delle password, i timeout dei salvaschermo e l'uso accettabile, rimangono invariati per tutte le piattaforme.

Se un criterio aziendale impone l'uso di una particolare tecnologia utilizzata su un'altra piattaforma, esamina la problematica e riformulalo in modo che includa le tecnologie integrate in macOS. Anziché imporre che tutti i computer usino una determinata soluzione di un altro fornitore per crittografare un intero disco, valuta se creare un criterio che specifichi che i dati aziendali archiviati debbano essere crittografati e mettilo in atto utilizzando FileVault. Se il criterio richiede un software particolare per la protezione dai malware, istruisci i team su funzioni integrate come Gatekeeper e quindi aggiorna il criterio per consentirne l'uso.

Configurare le impostazioni nella soluzione MDM

Per abilitare la gestione dei criteri aziendali e garantire ai dipendenti l'accesso alle risorse necessarie, ogni Mac verrà registrato in modo sicuro nella soluzione MDM, che applicherà poi i criteri e le impostazioni usando i profili di configurazione. I profili di configurazione sono file XML creati dalla soluzione MDM che consentono di distribuire le impostazioni ai dispositivi. Questi profili automatizzano la configurazione di impostazioni, account, criteri, restrizioni e credenziali, e possono essere firmati e crittografati per aumentare la sicurezza dei sistemi.

Una volta registrato il dispositivo nella soluzione MDM, un amministratore può avviare un criterio, un'interrogazione o un comando MDM. Se il dispositivo è connesso a una rete, riceverà una notifica attraverso il servizio di notifiche push di Apple (APNs) con l'istruzione di comunicare direttamente con la soluzione MDM tramite una connessione sicura per elaborare l'azione dell'amministratore. Poiché la comunicazione avviene solo tra la soluzione MDM e il dispositivo, il servizio APNs non trasmetterà informazioni riservate né proprietarie. Se il dispositivo viene rimosso dal sistema di gestione, le impostazioni e i criteri controllati da tale profilo di configurazione saranno rimossi. Se necessario, le aziende possono anche inizializzare i dispositivi da remoto.

Molte organizzazioni collegano la soluzione MDM ai servizi di directory esistenti. Durante la registrazione automatica dei dispositivi, Impostazione Assistita di macOS può richiedere che gli utenti eseguano il login con le credenziali del servizio di directory. In macOS Catalina, le nuove opzioni di personalizzazione della registrazione permettono a Impostazione Assistita di mostrare l'autenticazione dei fornitori di identità cloud . Una volta assegnato il dispositivo a un utente specifico, la soluzione MDM può personalizzare le configurazioni e gli account in base ai singoli utenti o gruppi. Per esempio, un account Microsoft Exchange personale può essere fornito automaticamente all'utente durante la registrazione. È anche possibile usare identità di certificati per tecnologie come 802.1x, VPN e tante altre.

Considerato l'elevato livello di controllo offerto da questi sistemi, spesso le aziende forniscono tranquillamente agli utenti l'accesso di amministratore al proprio Mac, permettendo loro di personalizzare tutte le impostazioni, installare app e risolvere problemi pur rimanendo sotto il controllo dei criteri aziendali via MDM. Questo modello è in linea con il tipo di privilegi e controlli che gli utenti hanno sul proprio iPhone o iPad quando è inserito nel sistema di gestione.

Per saperne di più sui profili di configurazione:
support.apple.com/guide/deployment-reference-macos

Preparare tutto per la registrazione automatica dei dispositivi

Il metodo più semplice per registrare un dispositivo nella soluzione MDM è farlo durante la procedura di impostazione assistita con le funzioni di registrazione automatica dei dispositivi di Apple Business Manager. Questo approccio consente di completare la registrazione senza l'intervento del reparto IT e di semplificare alcune schermate di Impostazione Assistita per velocizzare la procedura per gli utenti.

Per configurare la registrazione automatica dei dispositivi, dovrai collegare la soluzione MDM all'account Apple Business Manager utilizzando un token di sicurezza. Una procedura di verifica in due passaggi permette di autorizzare la soluzione MDM in modo sicuro. Il tuo fornitore MDM può farti avere la documentazione con i dettagli specifici per la sua soluzione.

Se i dispositivi sono già in uso tra i dipendenti o sono di proprietà degli utenti, questi ultimi possono aprire i singoli profili di configurazione e verificarli in Preferenze di Sistema per completare la registrazione. Questa procedura è nota come registrazione MDM approvata dall'utente. Per gestire alcune impostazioni sensibili sotto il profilo della sicurezza (come i criteri per le estensioni del kernel o il payload "Controllo politiche preferenze privacy"), la registrazione deve essere effettuata tramite la registrazione dei dispositivi o la procedura di registrazione MDM approvata dall'utente.

Per saperne di più sul caricamento delle estensioni del kernel:
support.apple.com/guide/deployment-reference-macos

Per saperne di più sul payload "Controllo politiche preferenze privacy":
support.apple.com/guide/mdm

Prepararsi a distribuire app e libri

Apple ha creato programmi ad hoc per aiutare le organizzazioni come la tua a sfruttare al meglio le app e i contenuti disponibili per macOS. Con queste funzioni puoi distribuire ai dipendenti le applicazioni sviluppate in-house e le app e i libri acquistati tramite Apple Business Manager, così avranno tutto il necessario per essere ancora più produttivi. Con una soluzione MDM puoi anche distribuire app e installare pacchetti software non disponibili sul Mac App Store.

Acquistando app e libri attraverso Apple Business Manager, la soluzione MDM può usare la distribuzione gestita per distribuirli in qualsiasi Paese in cui siano disponibili. La prima cosa da fare per abilitare la distribuzione gestita è collegare la soluzione MDM al tuo account Apple Business Manager utilizzando un token di sicurezza. Una volta stabilita la connessione alla soluzione MDM, potrai assegnare app e libri agli utenti anche se l'accesso all'App Store è disabilitato sul dispositivo. Potrai anche assegnare le app direttamente ai dispositivi, semplificando notevolmente la distribuzione poiché qualsiasi utente su tali dispositivi avrà accesso a ogni app.

Per saperne di più sull'acquisto di contenuti con Apple Business Manager:
support.apple.com/guide/apple-business-manager

Per saperne di più sulla distribuzione di app e libri:
support.apple.com/guide/apple-business-manager

Preparare altri contenuti

La soluzione MDM può aiutarti a distribuire anche altri pacchetti con contenuti che non provengono dal Mac App Store. È un approccio comune per molti software aziendali, per esempio le applicazioni interne personalizzate o le app come Chrome o Firefox. Il software necessario può essere distribuito con questo metodo e installato in automatico dopo il completamento della registrazione. Anche i font, gli script e altri elementi si possono installare ed eseguire tramite pacchetti. Assicurati che i pacchetti siano correttamente firmati con il tuo ID sviluppatore del Developer Enterprise Program.

Per saperne di più sull'installazione di altri contenuti:
support.apple.com/guide/deployment-reference-macos

3. Distribuzione

Con macOS è facile distribuire i dispositivi ai dipendenti, personalizzarli secondo necessità e iniziare subito a lavorare senza l'intervento del reparto IT.

Usare Impostazione Assistita

All'avvio, i dipendenti possono usare l'utility Impostazione Assistita in macOS per definire le preferenze relative alla lingua e alla zona geografica e per collegarsi a una rete. Una volta collegati a internet, gli utenti visualizzeranno una serie di finestre di Impostazione Assistita con i passaggi di base per configurare un nuovo Mac. In questa fase i dispositivi presenti in Apple Business Manager possono essere registrati automaticamente nella soluzione MDM. I Mac registrati mediante la funzione di registrazione dei dispositivi possono anche essere configurati per saltare determinate schermate, tra cui i termini e le condizioni, l'accesso con l'ID Apple e l'impostazione dei servizi di localizzazione.

Dopo Impostazione Assistita, la soluzione MDM può intervenire per applicare svariate impostazioni durante la configurazione iniziale, per esempio stabilendo se un utente avrà privilegi amministrativi completi sul proprio computer. Come per iPhone e iPad, questo permette agli utenti di avere il controllo sul loro Mac pur continuando a rispettare le impostazioni e i criteri aziendali gestiti via MDM. Per fare in modo che i dipendenti possano iniziare a lavorare subito dopo il completamento di Impostazione Assistita, bisogna avviare il download e l'installazione in background solo delle applicazioni e dei pacchetti più importanti. Per le applicazioni più voluminose, è possibile programmare il download e l'installazione in background oppure lasciare che vengano eseguiti in un secondo momento dall'utente con lo strumento self-service della soluzione MDM.

Configurare gli account aziendali

La soluzione MDM permette di configurare in automatico l'email e altri account utente. In base alla soluzione MDM utilizzata e alla sua integrazione con i sistemi interni in uso, i payload degli account possono essere precompilati con nome utente, indirizzo email e identità di certificati per l'autenticazione e la firma.

Consentire la personalizzazione da parte dell'utente

Consentendo agli utenti di personalizzare i dispositivi, si aumenta la produttività: sono loro stessi, infatti, a scegliere le app e i contenuti migliori per portare a termine le mansioni assegnate e raggiungere gli obiettivi. Ora che in macOS Catalina sono disponibili gli ID Apple gestiti e la registrazione utente, le organizzazioni hanno nuove opzioni per fornire accesso ai servizi Apple tramite un ID Apple di loro proprietà o personale.

ID Apple e ID Apple gestito

Quando i dipendenti usano gli ID Apple per servizi Apple come FaceTime, iMessage, l'App Store e iCloud, hanno accesso a una vasta gamma di contenuti che semplificano le attività lavorative, aumentano la produttività e favoriscono la collaborazione. Come tutti gli ID Apple, anche quelli gestiti sono usati per accedere a dispositivi personali. Sono usati anche per accedere ai servizi Apple, tra cui iCloud e le funzioni di collaborazione di iWork e Note, e a Apple Business Manager. A differenza degli ID Apple, gli ID Apple gestiti restano di proprietà e sotto il controllo dell'organizzazione e sono usati, fra le altre cose, per il ripristino delle password e l'amministrazione basata sui ruoli. Gli ID Apple gestiti hanno alcune impostazioni limitate.

I dispositivi registrati tramite la registrazione utente richiedono un ID Apple gestito. La registrazione utente supporta l'uso opzionale di un ID Apple personale; altre opzioni di registrazione supportano un ID Apple personale o un ID Apple gestito. Solo la registrazione utente supporta l'uso di più ID Apple.

Per poter sfruttare al massimo questi servizi, gli utenti dovrebbero usare il proprio ID Apple o l'ID Apple gestito creato per loro. Se gli utenti non hanno un ID Apple, possono crearne uno prima di ricevere il dispositivo oppure durante l'impostazione assistita (non è necessaria una carta di credito).

Per saperne di più sugli ID Apple gestiti:
support.apple.com/guide/deployment-reference-macos

iCloud

Con iCloud gli utenti possono sincronizzare automaticamente documenti e altri contenuti personali come contatti, calendari e foto, e tenerli aggiornati su più dispositivi. La funzione "Dov'è" permette di localizzare un Mac, iPhone, iPad o iPod touch smarrito o rubato. Componenti specifiche di iCloud, come il portachiavi iCloud e iCloud Drive, si possono disattivare impostando restrizioni sul dispositivo, manualmente o tramite MDM. In questo modo le organizzazioni possono controllare meglio quali dati vengono archiviati e su quale account.

Per saperne di più sulla gestione di iCloud:
support.apple.com/guide/deployment-reference-macos

4. Gestione

Una volta che gli utenti sono operativi, i dispositivi e i contenuti possono essere gestiti e aggiornati attraverso un'ampia gamma di funzioni di amministrazione.

Amministrare i dispositivi

Per amministrare i dispositivi gestiti, le soluzioni MDM possono usare una serie di operazioni specifiche, tra cui l'interrogazione per ottenere informazioni e l'avvio di attività per la gestione dei dispositivi non conformi, smarriti o rubati.

Query
La soluzione MDM può interrogare i dispositivi per ottenere una serie di informazioni utili a garantire che gli utenti mantengano il set di applicazioni e impostazioni appropriato. Le interrogazioni possono riguardare l'hardware, come il numero di serie o il modello di dispositivo, o il software, come la versione di macOS o un elenco delle applicazioni installate. Inoltre, la soluzione MDM può inviare una query per conoscere lo stato delle principali funzioni di sicurezza, come FileVault o il firewall integrato.

Attività di gestione
Se i dispositivi sono gestiti, la soluzione MDM può eseguire svariate attività di amministrazione, per esempio modificare in automatico le impostazioni di configurazione senza l'intervento dell'utente, aggiornare macOS, bloccare o inizializzare un dispositivo da remoto, oppure gestire le password.

Per saperne di più sulle attività di gestione:
support.apple.com/guide/deployment-reference-macos

Gestire gli aggiornamenti software

Il reparto IT può lasciare che siano gli utenti a scegliere se effettuare l'aggiornamento al sistema operativo più recente quando viene reso disponibile. Testando una versione pre-release di macOS, il personale IT può assicurarsi che i problemi di compatibilità delle applicazioni siano identificati preventivamente e risolti dagli sviluppatori prima della release finale. Il reparto IT può partecipare alla fase di testing di ogni release tramite l'Apple Beta Software Program o il programma AppleSeed for IT. Adotta una strategia che ti consenta di mantenere sempre aggiornati i computer Mac per proteggere i tuoi utenti e i loro dati. Esegui gli aggiornamenti regolarmente, subito dopo aver accertato la compatibilità del tuo flusso di lavoro con la nuova versione di macOS.

La soluzione MDM può inviare automaticamente gli aggiornamenti di macOS in push ai Mac registrati. I Mac registrati possono anche essere configurati in modo da differire gli aggiornamenti e le relative notifiche fino a 90 giorni se i sistemi critici non sono pronti. Gli utenti non potranno avviare gli aggiornamenti manualmente finché il criterio non viene rimosso o la soluzione MDM non invia un comando di installazione.

Apple non consiglia né supporta la creazione di immagini di sistema monolitiche per gli aggiornamenti di macOS. Come iPhone e iPad, i Mac spesso si basano su aggiornamenti del firmware specifici per il proprio modello. Allo stesso modo, gli aggiornamenti del sistema operativo del Mac impongono che questi aggiornamenti del firmware siano installati direttamente da Apple. La strategia più affidabile consiste nell'eseguire l'aggiornamento con l'Installer di macOS o con i comandi MDM.

Gestire altri software

Spesso le organizzazioni hanno bisogno di distribuire ai propri utenti altre app oltre a quelle iniziali. Questa distribuzione può essere gestita in automatico via MDM per le applicazioni e gli aggiornamenti critici, oppure on demand consentendo ai dipendenti di richiedere le applicazioni attraverso un portale self-service fornito dalla soluzione MDM. Questi portali permettono di installare software acquistato sull'App Store tramite Apple Business Manager, ma anche app, script e altre utility che non provengono dall'App Store.

Anche se la maggior parte del software si può installare in automatico, alcune installazioni possono richiedere l'intervento dell'utente. Per una maggiore sicurezza, ora le app che richiedono estensioni del kernel hanno bisogno dell'autorizzazione dell'utente per caricarsi. Questo processo è noto come caricamento delle estensioni del kernel approvate dall'utente e può essere gestito tramite MDM.

Mantenere al sicuro i dispositivi

Oltre alla serie iniziale di criteri di sicurezza definiti prima della distribuzione dei dispositivi, il tuo team dovrebbe monitorare i computer per verificarne la conformità e ottenere più report possibili tramite la soluzione MDM. Questo può includere il monitoraggio del livello di sicurezza di ogni dispositivo o la raccolta di informazioni sull'installazione delle patch. Anche se molte organizzazioni si sentono a proprio agio nell'usare strumenti nativi per crittografare e proteggere i Mac, alcune potrebbero imporre l'uso di altri servizi di condivisione e sincronizzazione dei file o strumenti di prevenzione delle perdite di dati per impedire la fuga di informazioni aziendali e fornire report dettagliati sui dati sensibili.

La funzione "Trova il mio Mac" di iCloud può avviare un'inizializzazione a distanza per rimuovere tutti i dati e disattivare un Mac smarrito o rubato. Anche i team IT possono eseguire un'inizializzazione remota tramite la soluzione MDM.

Riassegnare i dispositivi

Quando un dipendente lascia l'azienda, il suo Mac può essere facilmente riassegnato a un altro utente con Internet Recovery e la partizione di recupero locale. In questo modo è possibile cancellare i contenuti del Mac e installare l'ultima versione del sistema operativo. Un Mac assegnato a una specifica soluzione MDM in Apple Business Manager si registrerà di nuovo automaticamente nella soluzione MDM durante Impostazione Assistita, configurerà le impostazioni per il nuovo utente, applicherà i criteri aziendali e installerà il software appropriato. I Mac che non sono registrati possono essere inizializzati e riassegnati con la stessa procedura e poi registrati di nuovo manualmente.

Opzioni di assistenza

Molte organizzazioni hanno notato che gli utenti Mac richiedono un'assistenza minima da parte del reparto IT. Per favorire l'autonomia e migliorare la qualità del supporto, molti reparti IT sviluppano strumenti self-service come per esempio un'esaustiva pagina web di assistenza per Mac, forum con soluzioni fai-da-te e help desk tecnici in loco. Le soluzioni MDM possono anche consentire agli utenti di eseguire da un portale self-service attività di supporto come l'installazione o l'aggiornamento di software.

Come best practice, le aziende non dovrebbero costringere gli utenti a contare esclusivamente su sé stessi per risolvere gli eventuali problemi. È preferibile invece adottare un approccio collaborativo al problem-solving e dare agli utenti la possibilità di cercare una soluzione da soli prima di rivolgersi all'help desk. Incoraggia la collaborazione da parte degli utenti ed esortali a esaminare i problemi in autonomia prima di chiedere aiuto.

Condividere la responsabilità permette di ridurre i tempi di inattività dei dipendenti, nonché l'impatto totale sui costi e sul personale di assistenza. Per le aziende che necessitano di ulteriore assistenza, AppleCare offre diversi programmi e servizi che completano gli strumenti di supporto interni per i dipendenti e il reparto IT.

AppleCare for Enterprise

Pensato per le aziende che cercano un servizio di assistenza completo, AppleCare for Enterprise consente di ridurre il carico di lavoro dell'help desk interno offrendo ai dipendenti supporto tecnico telefonico 24/7, con risposte entro un'ora per i problemi più urgenti. Il programma offre ai reparti IT assistenza per scenari di integrazione complessi, per esempio con le soluzioni MDM e Active Directory.

AppleCare OS Support

AppleCare OS Support fornisce ai reparti IT un servizio di assistenza telefonica e via email di livello enterprise per la distribuzione di iOS, iPadOS, macOS e macOS Server. A seconda del tipo di contratto, potrai ricevere assistenza fino a 24 ore su 24 e 7 giorni su 7, e contare su un account manager tecnico dedicato per la tua organizzazione. Con AppleCare OS Support, i reparti IT possono contattare direttamente gli esperti Apple in caso di problematiche legate all'integrazione, alla migrazione e al funzionamento dei server, così da poter distribuire e gestire i dispositivi in modo più efficiente e risolvere tempestivamente gli eventuali problemi.

AppleCare Help Desk Support

AppleCare Help Desk Support garantisce un accesso telefonico prioritario ai migliori esperti Apple. Include anche una serie di strumenti per la diagnosi e la risoluzione dei problemi dell'hardware Apple, con cui le grandi organizzazioni possono gestire le proprie risorse in modo più efficiente, migliorare i tempi di risposta e ridurre i costi di formazione. AppleCare Help Desk Support copre un numero illimitato di interventi di assistenza per la diagnosi e la risoluzione di problemi hardware e software e l'isolamento di problemi per i dispositivi iOS e iPadOS.

AppleCare e AppleCare+ per Mac

Ogni Mac include una garanzia limitata di un anno e 90 giorni di assistenza telefonica gratuita dalla data di acquisto. Con AppleCare+ o AppleCare Protection Plan si può estendere la copertura a tre anni dalla data di acquisto originale. I dipendenti possono rivolgersi al Supporto Apple per domande relative all'hardware e al software Apple. Apple offre anche vantaggiose opzioni di assistenza per la riparazione dei dispositivi. Inoltre AppleCare+ per Mac copre una serie interventi per danni accidentali, ciascuno soggetto a un costo addizionale.

Per saperne di più sulle opzioni di assistenza di AppleCare:
apple.com/it/support/professional/

Riepilogo

Esistono varie opzioni per distribuire e gestire facilmente i computer Mac, che siano destinati a un numero limitato di utenti o a tutti i dipendenti dell'azienda. Scegliere le strategie più adatte alla tua organizzazione può aiutare i dipendenti a lavorare meglio e a svolgere le proprie mansioni in modi completamente nuovi.

Per saperne di più sulle funzioni di sicurezza, gestione e distribuzione di macOS:
support.apple.com/guide/deployment-reference-macos

Per saperne di più sulle impostazioni IT per la gestione dei dispositivi mobili:
support.apple.com/guide/mdm

Per saperne di più su Apple Business Manager:
support.apple.com/guide/apple-business-manager

Per saperne di più sugli ID Apple gestiti per le aziende:
apple.com/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

Per saperne di più su Apple at Work:
www.apple.com/it/business/

Per saperne di più sulle funzioni IT:
www.apple.com/it/business/it/

Per saperne di più sulla sicurezza delle piattaforme Apple:
www.apple.com/security/

Esplora i programmi AppleCare disponibili:
www.apple.com/it/support/professional/

Scopri i programmi di formazione e certificazione Apple:
training.apple.com

Contatta Apple Professional Services:
consultingservices@apple.com