Driftsättning av Mac – översikt

Inledning

Innehåll

Vi på Apple är övertygade om att tillgång till de bästa verktygen och den bästa tekniken är avgörande för att prestera på topp. Alla våra produkter är utformade för att stimulera medarbetarnas kreativitet och produktivitet och ge dem möjlighet att arbeta på nya sätt, både på och utanför kontoret. Det här ligger helt i linje med hur dagens anställda vill jobba: med ökad tillgång till information, smidiga metoder för samarbete och delning samt friheten att vara uppkopplad och jobba var som helst.

Att installera och driftsätta Mac-datorer i dagens företagsmiljöer är enklare än någonsin. Med rätt tjänster från Apple och en MDM-lösning från tredje part kan din organisation enkelt driftsätta och ge support för Mac i stor skala. Om din organisation redan har driftsatt iOS- och iPadOS-enheter internt är det mesta av arbetet med infrastrukturen som krävs för en macOS-implementering antagligen redan gjort.

macOS har nyligen uppdaterats för förbättrad säkerhet, hantering och driftsättning. Det innebär att företag nu kan övergå från monolitisk systemavbildning och traditionell katalogkoppling till en smidig process för tillhandahållande och driftsättning som sätter användaren i centrum. Processen kan genomföras nästan uteslutande med de inbyggda verktygen i macOS.

I det här dokumentet hittar du all vägledning du behöver för att driftsätta Mac i stor skala: från kartläggning av företagets infrastruktur till enhetshantering och effektivt tillhandahållande. Mer information om de ämnen som tas upp i det här dokumentet hittar du i referensdokumentet om Mac-driftsättning på support.apple.com/guide/deployment-reference-macos

Komma igång

Två viktiga steg i inledningen av driftsättningsprocessen är att lägga upp en strategi och undersöka hur medarbetarna använder macOS i nuläget. Sätt ihop de team som behövs i god tid och förbered dem så att de är insatta i visionen och målet med programmet. Vissa team börjar med en mindre konceptstudie, där de har chansen att upptäcka utmaningar som är unika för just deras område. Under ett pilotprojekt är det viktigt att kommunicera med de medarbetare som redan använder Mac. På så sätt kan teamen ta reda på hur datorerna används i organisationen och om det finns några problem som de bör vara medvetna om.

Den information som samlas in i det här skedet kan hjälpa till att avgöra vilka yrkesroller och områden som gynnas allra mest av Mac. Utifrån det kan it-teamet bedöma om företaget bör använda macOS som standard eller bara för vissa yrkesroller.

Ofta får man under den här processen också fram en lista över alla de interna appar och verktyg som behöver vara kompatibla för att det ska gå att driftsätta Mac i hela organisationen. Fokusera främst på de mest använda apparna för produktivitet, samarbete och kommunikation. Centrala interna tjänster, som företagets intranät, katalogtjänster och mjukvara för utgiftshantering, är också viktiga för produktiviteten inom stora delar av organisationen.

Dokumentera och informera om eventuella alternativ till andra interna verktyg och uppmana de appansvariga på företaget att göra de uppdateringar som behövs. Ge användarna all tillgänglig information om de olika företagsapparna som de kommer att kunna använda på Mac och låt efterfrågan från användarna avgöra vilka appar som ska prioriteras. Vid behov kan du tillsammans med appansvariga tillsammans lägga upp en uppdateringsplan. Ni kan utnyttja både macOS SDK och Swift och även ta hjälp av företagspartner som arbetar med apputveckling.

Mac-datorer driftsätts ofta som företagsägda enheter. En del företag låter de anställda använda sina egna Mac-datorer på jobbet inom ramen för ett BYOD-program (Bring Your Own Device). Oavsett ägarskapsmodell kan det ge goda resultat inom hela organisationen att låta användarna välja Apple-produkter: högre produktivitet, ökad kreativitet och större engagemang samt nöjdare medarbetare. Dessutom sparar företaget pengar tack vare lägre supportkostnader och högre andrahandsvärde. Det finns även olika leasing- och finansieringsalternativ som kan hålla nere de initiala investeringskostnaderna. Ett annat sätt varpå organisationen kan sprida ut kostnaderna över tid är att låta medarbetarna bidra genom att finansiera uppgraderingar via löneavdrag. Företaget kan också låta användarna köpa loss sina datorer när leasingavtalet löper ut eller produkten inte längre används på företaget.

De företagspolicyer och processer för driftsättning, hantering och support som beskrivs i det här dokumentet kan skilja sig från de du kommer att använda, beroende på vilken information ditt team samlar in under pilotprojektet. Alla användare behöver inte exakt samma policyer, inställningar och program. Behoven kan variera kraftigt mellan olika grupper eller team inom samma företag.

Driftsättningssteg

Driftsättningen av macOS genomförs i fyra steg: förbereda infrastrukturen, ställa in MDM-lösningen, distribuera datorerna till medarbetarna samt hantera löpande administration.

1. Förberedelser

Det första steget i all driftsättning är att kartlägga den befintliga miljön. I det här skedet ska du undersöka och utvärdera nätverket och infrastrukturen samt installera de system som behövs vid driftsättningen.

Utvärdera infrastrukturen

Mac-datorer kan visserligen integreras utan problem i it-miljön på de flesta företag, men för att försäkra dig om att företaget kan utnyttja alla fördelar med macOS är det ändå viktigt att du går igenom och utvärderar den befintliga infrastrukturen. Företaget kan få hjälp av Apple Professional Services liksom återförsäljarens eller en samarbetspartners tekniska team vid behov.

Wifi och nätverk

Kontinuerlig och tillförlitlig åtkomst till ett trådlöst nätverk är avgörande när du ska installera och konfigurera macOS-datorer. Kontrollera att wifi-nätverket är rätt utformat. Det är viktigt att anslutningspunkterna är placerade och strömförsörjda på ett sätt som ger effektiv roaming och uppfyller kapacitetsbehoven.

Du kan även behöva konfigurera företagets webbproxyserver eller brandvägg om enheterna inte kan ansluta till Apples servrar, Apples tjänst för pushnotiser (APNs), iCloud eller iTunes Store. Precis som med iPad och iPhone behövs tillförlitlig och kontinuerlig åtkomst till de här tjänsterna under vissa delar av Mac-driftsättningen, exempelvis vid uppdatering av fast programvara i installationssteget. Detta gäller särskilt nyare Mac-datorer.

Apple och Cisco har optimerat Mac-datorernas sätt att kommunicera med Ciscos trådlösa nätverk genom att lägga till avancerade nätverksfunktioner i macOS, exempelvis QoS (Quality of Service). Du bör tillsammans med företagets interna team arbeta med att optimera viktig nätverkstrafik på Mac-datorerna, om ditt företag har nätverksutrustning från Cisco.

Det är också viktigt att utvärdera VPN-infrastrukturen och kontrollera att användarna har säker fjärråtkomst till företagets resurser. Använd gärna VPN On Demand-funktionen i macOS, så att VPN-anslutningar endast upprättas vid behov. Om du planerar att använda VPN per program måste du kontrollera att VPN-nätverksnoderna stöder den funktionen och att det finns tillräckligt med licenser för alla användare och anslutningar.

Se till att nätverkets infrastruktur fungerar med Bonjour, som är Apples standardbaserade, konfigurationsfria nätverksprotokoll. Med Bonjour kan Apple-enheter automatiskt hitta tjänster i ett nätverk. macOS använder Bonjour för att ansluta till AirPrint-kompatibla skrivare och AirPlay-kompatibla enheter som Apple TV. Vissa program och inbyggda macOS-funktioner använder även Bonjour för att upptäcka andra datorer och enheter för samarbete och delning.

Läs mer om design av wifi-nätverk:
support.apple.com/guide/deployment-reference-macos

Läs mer om att konfigurera ett nätverk för MDM:
support.apple.com/HT210060

Läs mer om Bonjour:
support.apple.com/guide/deployment-reference-macos

Hantera identiteter
macOS kan hantera identiteter och andra användaruppgifter genom att hämta data från katalogservrar som Active Directory, Open Directory och LDAP. Vissa MDM-leverantörer tillhandahåller verktyg för att integrera MDM-lösningen med Active Directory- och LDAP-kataloger. Ytterligare verktyg, som Kerberos tillägg för enkel inloggning (Single Sign-on, SSO) i macOS Catalina, gör det möjligt att integrera med Active Directory-riktlinjer och -funktioner utan att det krävs någon traditionell katalogkoppling eller ett mobilt konto. Olika typer av certifikat från både interna och externa certifikatutfärdare kan också hanteras av MDM-lösningen, vilket automatiskt innebär att identiteterna är tillförlitliga.

Läs mer om Kerberos nya SSO-tillägg:
support.apple.com/guide/deployment-reference-macos

Läs mer om katalogintegrering:
support.apple.com/guide/deployment-reference-macos

Viktiga tjänster för medarbetarna
Kontrollera att Microsoft Exchange-tjänsten är uppdaterad och konfigurerad så att den stöder alla användare i nätverket. Om du inte använder Exchange fungerar macOS även med standardbaserade servrar som stöder IMAP, POP, SMTP, CalDAV, CardDAV och LDAP. Testa de grundläggande arbetsflödena för e-post, kontakter och kalendrar. Testa även övriga appar för produktivitet och samarbete som medarbetarna använder mest för att utföra sina viktigaste arbetsuppgifter.

Läs mer om konfigurering av Microsoft Exchange:
support.apple.com/guide/deployment-reference-macos

Läs mer om standardbaserade tjänster:
support.apple.com/guide/deployment-reference-macos

Innehållscachelagring
Cachelagringstjänsten i macOS sparar en lokal kopia av innehåll som ofta efterfrågas från Apples servrar, så att det tar upp mindre bandbredd att ladda ner innehåll i nätverket. Cachelagring kan användas för att göra det snabbare att ladda ner och distribuera mjukvara från Mac App Store. Tjänsten kan även cachelagra mjukvaruuppdateringar, så att dessa går snabbare att ladda ner till företagets macOS-datorer och iOS- och iPadOS-enheter. Innehåll kan även cachelagras via tredjepartslösningar från Cisco och Akamai.

Läs mer om innehållscachelagring:
support.apple.com/guide/deployment-reference-macos

Välj lösning för enhetshantering

Med MDM kan du driftsätta Mac på ett säkert sätt i företagsmiljön. Via trådlös anslutning kan du konfigurera och uppdatera inställningar, driftsätta appar, övervaka policyefterlevnad, anropa enheter och fjärradera eller fjärrlåsa hanterade datorer. It-personalen kan enkelt skapa profiler för att hantera användarkonton, konfigurera systeminställningar och begränsningar samt ställa in lösenordsriktlinjer. Allt från samma MDM-lösning som de redan använder för iPhone och iPad.

Alla Apples plattformar använder samma hanteringsramverk från Apple, och med det ramverket kan kunderna välja mellan olika MDM-lösningar från tredje part. Det finns ett brett utbud av MDM-lösningar från exempelvis Jamf, VMware och MobileIron. macOS, iOS och iPadOS delar många av funktionerna för enhetshantering. Det finns emellertid vissa skillnader mellan MDM-lösningarna från tredje part i fråga om administratörsfunktioner, stöd för operativsystem, prismodeller och värdtjänster. De kan också ha olika omfattning på sina tjänster för integrering, utbildning och support. Innan du väljer en lösning bör du ta reda på vilka funktioner som är viktigast för ditt företag.

När du har valt en MDM-lösning ska du besöka Apple Push Certificates Portal, där du kan logga in och skapa ett nytt MDM-pushcertifikat.

Läs mer om MDM-driftsättning:
support.apple.com/guide/deployment-reference-macos

Besök Apple Push Certificates Portal:
identity.apple.com/pushcert/

Registrera dig i Apple Business Manager

Apple Business Manager är en webbaserad portal för it-administratörer där de kan driftsätta iPhone, iPad, iPod touch, Apple TV och Mac från ett och samma ställe. Apple Business Manager fungerar smidigt ihop med er MDM-lösning och gör det enkelt att automatisera enhetshantering, driftsätta appar, distribuera innehåll och skapa hanterade Apple-ID:n åt medarbetare.

Nu är programmet för enhetsregistrering (DEP) och programmet för volyminköp (VPP) helt integrerade i Apple Business Manager, så att organisationer har tillgång till allt de behöver för att driftsätta Apple-enheter.
Efter den 1 december 2019 är dessa program inte längre tillgängliga.

Enheter

Apple Business Manager möjliggör automatisk enhetsregistrering, vilket innebär att företag snabbt och smidigt kan driftsätta företagsägda Apple-enheter och registrera dem i MDM utan att behöva hantera de fysiska enheterna eller förbereda dem separat.

- Förenkla inställningsprocessen för användarna genom att effektivisera stegen i inställningsassistenten, så att medarbetarna får rätt konfigurationer direkt när de aktiverar sina enheter. It-team kan nu anpassa processen ytterligare genom att infoga text om samtycke, företagets varumärkesprofil eller modern autentisering.

- Ta större kontroll över företagsägda enheter med hjälp av övervakning, som erbjuder ökad kontroll vid enhetshantering som inte är möjlig med andra driftsättningsmodeller, till exempel permanent MDM.
- Hantera standardservrar för MDM enklare genom att ställa in en standardserver baserad på enhetstyp. Nu kan du även registrera iPhone, iPad och Apple TV med Apple Configurator 2, oavsett hur enheterna är inköpta.

Innehåll

Med Apple Business Manager kan organisationer enkelt göra volyminköp av innehåll. Du kan ge medarbetarna tillgång till suveränt innehåll som är färdigt att använda med flexibla och säkra distributionsalternativ, oavsett om de använder iPhone, iPad eller Mac.

- Gör volyminköp av appar, böcker och anpassade appar, inklusive de som ni utvecklar internt. Överför enkelt licenser för appar mellan olika platser och dela licenser mellan köpare på samma plats. Visa en lista över köphistorik med bland annat antalet licenser som för närvarande används via MDM.
- Distribuera köpta appar och böcker direkt till hanterade enheter eller auktoriserade användare och håll enkelt reda på vilket innehåll som har tilldelats vilken användare eller enhet. Med hanterad distribution kontrollerar du hela distributionsprocessen och behåller fullständig äganderätt till appar. Appar som inte behövs på en enhet eller av en användare kan återkallas och tilldelas till någon annan i organisationen.
- Det finns flera olika betalningsmetoder att välja mellan, till exempel kreditkort och faktura. Organisationer kan köpa volymkredit (där det erbjuds) från Apple eller från en auktoriserad Apple-återförsäljare i specifika belopp i den lokala valutan. Beloppet levereras sedan elektroniskt till kontoinnehavaren, som kan använda krediten i butiken.
- Du kan distribuera appar i flera länder till enheter eller användare i alla länder där appen är tillgänglig. Utvecklare kan göra sina appar tillgängliga i flera länder via den vanliga publiceringsprocessen för App Store.

Obs! Köp av böcker i Apple Business Manager är inte tillgängligt i vissa länder. På support.apple.com/HT207305 finns mer information om vilka funktioner och inköpsmetoder som är tillgängliga.

Personer

Organisationer kan använda Apple Business Manager till att skapa och hantera konton för medarbetare som kan integreras med den befintliga infrastrukturen och som ger åtkomst till Apples appar och tjänster samt till Apple Business Manager.

- Skapa hanterade Apple-ID:n så att medarbetarna kan använda Apples appar och tjänster och komma åt arbetsrelaterade data i hanterade appar som använder iCloud Drive. Dessa konton ägs och kontrolleras av respektive organisation.
- Utnyttja federerad autentisering genom att ansluta Apple Business Manager till Microsoft Azure Active Directory. Hanterade Apple-ID:n skapas automatiskt första gången medarbetarna loggar in med sina befintliga inloggningsuppgifter på kompatibla Apple-enheter.

- Den nya funktionen för användarregistrering i iOS 13, iPadOS och macOS Catalina gör det möjligt att ha ett hanterat Apple-ID såväl som ett privat Apple-ID på en personlig enhet. Oavsett vilken typ av enhet som används kan man även välja att ha ett hanterat Apple-ID som primärt och enda Apple-ID. Medarbetaren kan även använda sitt hanterade Apple-ID för att skaffa åtkomst till iCloud på webben efter att ha loggat in på en Apple-enhet första gången.
- Specificera roller för organisationens it-medarbetare så att de kan hantera enheter, appar och konton i Apple Business Manager på ett effektivt sätt. Använd administratörsrollen för att godkänna eventuella villkor och enkelt överföra ansvaret om någon lämnar organisationen.

Obs! iCloud Drive stöds för närvarande inte vid användarregistrering. iCloud Drive kan användas med ett hanterat Apple-ID under förutsättning att det är det enda Apple-ID som finns på enheten.

Läs mer om Apple Business Manager: www.apple.com/se/business/it

Registrera dig i Apple Developer Enterprise Program

Apple Developer Enterprise Program omfattar kompletta verktyg för att utveckla, testa och distribuera appar till användare. Du kan distribuera program antingen genom att publicera dem på en webbserver eller via en MDM-lösning. Du kan signera och attestera Mac-appar och Mac-installerare med ditt utvecklar-id för Gatekeeper, vilket hjälper dig att skydda macOS mot skadeprogram.

Läs mer om Developer Enterprise Program:
developer.apple.com/programs/enterprise

2. Inställningar

Under driftsättningen kan du utforma företagspolicyer och förbereda MDM-lösningen för att konfigurera medarbetarnas Mac-datorer.

Säkerhetsfunktioner i macOS

Säkerhet och integritetsskydd är A och O för utformningen av Apples hårdvara, mjukvara och tjänster. Vi skyddar användarnas integritet med stark kryptering och strikta regler för datahantering. En säker dataplattform för Apple-enheter upprätthålls genom

- metoder som förhindrar obehörig användning av enheter
- skydd av lagrade data, även om en enhet förloras eller blir stulen
- nätverksprotokoll och kryptering av data under överföring
- säker appanvändning utan att plattformsintegriteten äventyras.

Alla Apple-enheter är utformade med säkerhet i flera lager, som skyddar viktiga data och gör så att enheterna kan ansluta till nätverkstjänster på ett säkert sätt. macOS, iOS och iPadOS skyddas dessutom genom lösenkods- och lösenordspolicyer som kan levereras och tillämpas via MDM. Om en enhet hamnar i fel händer kan användare och it-administratörer utföra en fjärradering som raderar all privat information.

Med MDM kan it-teamet tillämpa olika riktlinjer för att skydda enheter. Exempelvis kan man förse FileVault med en återställningsnyckel, genomdriva en

viss lösenordsriktlinje, kräva lösenord när skärmsläckaren är aktiv eller aktivera den inbyggda brandväggen.

Läs mer om säkerhet på Apple-plattformen: apple.com/security/

Utforma företagspolicyer

Börja med att upprätta allmänna policyer som omfattar majoriteten av alla Mac-användare på företaget. MDM-lösningen gör det möjligt att skapa anpassade riktlinjer för vissa användare, till exempel för konton eller åtkomst till särskilda appar. Du kan också ställa in riktlinjer för avdelningar och andra mindre användargrupper, exempelvis för driftsättning av specifik mjukvara och inställningar.

Ta hjälp av dina interna team med att uppdatera befintliga företagspolicyer så att de innefattar användning av Mac-datorer. En del grundläggande riktlinjer är desamma på alla plattformar, till exempel krav på komplexitet och ändringsintervall för lösenord, tidsgränser för skärmsläckare och tillåten användning.

Om företagspolicyn kräver användning av viss teknik på en annan plattform bör du utreda de bakomliggande orsakerna och omarbeta policyn så att den kan omfatta de inbyggda teknikerna i macOS. Du kan skapa en policy som innebär att företagsdata måste krypteras vid lagring via FileVault, istället för att begära att alla datorer ska använda en särskild tredjepartslösning för att kryptera hela hårddisken. Om policyn kräver att en specifik mjukvara används mot skadeprogram kan du utbilda teamen om Gatekeeper och andra inbyggda funktioner, och sedan uppdatera policyn så att den omfattar dessa.

Konfigurera inställningar i MDM

Varje Mac-dator måste registreras på ett säkert sätt i MDM-lösningen, så att företaget kan hantera policyer och ge alla medarbetare tillgång till nödvändiga resurser. MDM-lösningen ser till att alla riktlinjer och inställningar tillämpas med hjälp av konfigurationsprofiler. Konfigurationsprofiler är XML-filer som skapas av MDM-lösningen och som kan användas för att distribuera inställningar till enheter. Dessa profiler automatiserar konfigureringen av inställningar, konton, riktlinjer, begränsningar och inloggningsuppgifter. De kan signeras och krypteras för ökad säkerhet.

När en Mac-dator har registrerats i MDM kan administratören initiera en riktlinje, ett anrop eller ett kommando via MDM. Om datorn är ansluten till nätverket får den en notis via tjänsten APNs (Apple Push Notification service). Notisen ber datorn utföra administratörens åtgärd genom att kommunicera direkt med MDM-servern via en säker anslutning. Eftersom kommunikationen endast sker direkt mellan MDM-lösningen och datorn överförs ingen konfidentiell eller företagsintern information via APNs. Om en dator tas bort från MDM-systemet raderas också de inställningar och riktlinjer som styrs av den konfigurationsprofilen. Företaget kan även fjärradera Mac-datorer om det behövs.

Många företag integrerar MDM-lösningen med sina befintliga katalogtjänster. Inställningsassistenten i macOS kan uppmana användarna att logga in med sina inloggningsuppgifter till katalogtjänsten vid den automatiska MDM-

registreringen. I macOS Catalina finns nya funktioner för registreringsanpassning så att inställningsassistenten kan visa autentisering från molnbaserade identitetsleverantörer. När en Mac-dator är tilldelad till en specifik användare kan MDM anpassa inställningar och konton efter den användaren eller användargruppen. Till exempel kan en användares individuella Microsoft Exchange-konto tillhandahållas automatiskt vid registreringen. Det går också att använda certifikatidentiteter för bland annat 802.1x och VPN.

Eftersom den här typen av system ger så hög grad av kontroll är många företag beredda att ge varje medarbetare administratörsåtkomst till sin Mac. Användarna kan då själva anpassa inställningar, installera appar och felsöka problem samtidigt som MDM-systemet garanterar att företagets policyer följs. Den här modellen ger samma grad av behörighet och kontroll som användarna har över sina företagshanterade iPhone- eller iPad-enheter.

Läs mer om konfigurationsprofiler:
support.apple.com/guide/deployment-reference-macos

Förbered för automatisk enhetsregistrering

Det enklaste sättet att registrera datorerna i MDM är att använda inställningsassistenten och de automatiska funktionerna för enhetsregistrering i Apple Business Manager. Användarna kan då registrera sig utan hjälp från it-avdelningen. Det går också att ta bort de delar av inställningsassistenten som inte behövs så att processen går snabbare för användarna.

Du konfigurerar automatisk enhetsregistrering genom att koppla MDM-lösningen till ditt Apple Business Manager-konto med hjälp av en säker token. Tvåstegsverifiering används för att auktorisera MDM-servern på ett säkert sätt. MDM-leverantören kan tillhandahålla dokumentation om detaljerna kring implementeringen.

Om det finns Mac-datorer som redan används eller ägs av medarbetare kan de själva utföra registreringen genom att öppna en konfigurationsprofil och verifiera den i Systeminställningar. Detta kallas användargodkänd MDM-registrering. Hantering av vissa inställningar som kräver hög säkerhet, exempelvis policykontroll för kärntillägg och integritetsinställningar, kräver att registreringen sker genom enhetsregistrering eller användargodkänd MDM-registrering.

Läs mer om inläsning av kärntillägg:
support.apple.com/guide/deployment-reference-macos

Läs mer om kontroll av riktlinjer för integritetsinställningar:
support.apple.com/guide/mdm

Förbered för distribution av appar och böcker

Apple erbjuder omfattande program som hjälper din organisation att dra nytta av det stora utbudet av appar och innehåll för macOS. Med dessa funktioner kan du distribuera appar och böcker (köpta via Apple Business Manager eller utvecklade internt) till alla medarbetare, så att de har allt de behöver för att vara produktiva. MDM kan också distribuera och installera mjukvara som inte finns på Mac App Store.

Med hanterad distribution kan MDM-lösningen distribuera appar och böcker köpta från Apple Business Manager i alla länder där de finns tillgängliga. Du kan aktivera hanterad distribution genom att först koppla din MDM-lösning till ditt Apple Business Manager-konto med hjälp av en säker token. När du är ansluten till MDM-servern kan du tilldela appar och böcker även om App Store är inaktiverad på enheten. Du kan också tilldela appar direkt till datorerna, vilket förenklar driftsättningen eftersom alla som använder en dator då har tillgång till alla appar.

Läs mer om inköp av innehåll i Apple Business Manager:
support.apple.com/guide/apple-business-manager

Läs mer om distribution av appar och böcker:
support.apple.com/guide/apple-business-manager

Förbered ytterligare innehåll

MDM-lösningen kan även hjälpa dig att distribuera annat innehåll som inte kommer från Mac App Store. Det är ett vanligt förfarande när det gäller företagsmjukvara, som Chrome och Firefox eller interna appar. Mjukvaran kan då skickas ut med pushteknik och installeras automatiskt när registreringen är klar. Typsnitt, skript och annat kan också installeras och köras i form av paket. Dessa paket måste signeras med ditt utvecklar-ID från Apple Developer Enterprise Program.

Läs mer om installation av övrigt innehåll:
support.apple.com/guide/deployment-reference-macos

3. Driftsättning

Med macOS är det enkelt att driftsätta datorer till medarbetarna, anpassa dem efter behov och börja använda dem utan hjälp från it-teamet.

Inställningsassistenten

Med hjälp av inställningsassistenten i macOS kan medarbetarna efter uppstart ställa in språk och region samt ansluta till ett nätverk. När internetanslutningen har upprättats visas en serie fönster i inställningsassistenten som hjälper användarna att göra alla grundläggande inställningar på Mac. Enheter som är registrerade i Apple Business Manager kan registreras automatiskt i MDM under den här processen. Du kan också välja att låta enhetsregistrerade Mac-datorer hoppa över vissa skärmar, exempelvis villkor, inloggning med Apple-ID och platstjänster.

När inställningsassistenten är klar kan du göra en mängd olika inställningar via MDM. Du kan till exempel bestämma om användaren ska ha fullständiga administratörsbehörigheter på datorn. Det fungerar på samma sätt som på iPhone och iPad: användaren har kontroll över sin egen enhet samtidigt som MDM-systemet styr över vissa inställningar och ser till att företagets policyer följs. Om du vill att användarna ska kunna börja jobba direkt efter att inställningsassistenten är klar bör du endast låta de viktigaste apparna och paketen laddas ner och installeras i bakgrunden, så att det inte stör arbetet. När det gäller större appar kan du schemalägga nedladdning och installation i bakgrunden eller låta användaren installera dem senare via MDM-lösningens självbetjäningsverktyg.

Företagskonton

MDM kan ställa in e-post och andra konton automatiskt. Beroende på leverantör av MDM-lösning och integrering med interna system kan kontons nyttolaster även förkonfigureras med användarens namn, e-postadress och eventuella certifikatidentiteter för autentisering och signering.

Anpassade enheter

Produktiviteten ökar ofta när man låter användarna anpassa datorerna eftersom användarna då kan välja de appar och det innehåll de behöver för att utföra sitt arbete på bästa sätt. Och med hanterade Apple-ID:n och användarregistrering i macOS har organisationer nu fått nya sätt att ge användarna tillgång till Apple-tjänster via såväl ett organisationsägt Apple-ID som ett personligt Apple-ID.

Apple-ID och hanterat Apple-ID

När medarbetarna använder ett Apple-ID för att logga in på FaceTime, iMessage, App Store, iCloud och andra Apple-tjänster, får de tillgång till ett brett utbud av innehåll som hjälper dem att effektivisera arbetsuppgifter, öka produktiviteten och utöka samarbetet. Hanterade Apple-ID:n används till att logga in på en personlig enhet i likhet med andra Apple-ID:n. De ger även åtkomst till iCloud, samarbete via iWork och Anteckningar, Apple Business Manager och andra Apple-tjänster. Till skillnad från vanliga Apple-ID:n ägs och hanteras hanterade Apple-ID:n av din organisation och används till, bland annat återställning av lösenord och rollbaserad administrering. Hanterade Apple-ID:n har en del inställningsbegränsningar.

Enheter som registreras via användarregistrering kräver ett hanterat Apple-ID. Användarregistrering stöder parallell användning av ett personligt Apple-ID, medan andra registreringsalternativ stöder antingen ett personligt Apple-ID eller ett hanterat Apple-ID. Endast användarregistrering har stöd för flera Apple-ID:n.

För att få ut mesta möjliga av de här tjänsterna bör användarna logga in med sina egna Apple-ID:n eller hanterade Apple ID:n som skapas åt dem. Användare kan skapa ett Apple-ID även innan de får en enhet. Med inställningsassistenten kan de också skapa ett personligt Apple-ID om de inte har något. Användarna behöver inte något kreditkort för att skapa ett Apple-ID.

Läs mer om hanterade Apple-ID:n:
support.apple.com/guide/deployment-reference-macos

iCloud

Med iCloud kan användarna automatiskt synka dokument och personligt innehåll, som kontakter, kalendrar, dokument och bilder, och hålla allt uppdaterat på flera enheter. Hitta-funktionen hjälper användaren att leta rätt på en borttappad eller stulen Mac, iPhone, iPad eller iPod touch. Delar av iCloud, som iCloud-nyckelring och iCloud Drive, kan inaktiveras genom begränsningar som ställs in antingen manuellt på enheten eller via MDM. På så vis får organisationen mer kontroll över vilka data som lagras på olika konton.

Läs mer om iCloud-hantering:
support.apple.com/guide/deployment-reference-macos

4. Hantering

När användarna har kommit igång finns många olika administrationsfunktioner för att hantera och underhålla enheterna och innehållet över tid.

Administrera enheter

MDM-lösningar kan administrera hanterade enheter med hjälp av en uppsättning särskilda åtgärder. Dessa åtgärder omfattar anrop som skickas till enheterna samt initiering av åtgärder som gör det möjligt att hantera borttappade eller stulna enheter samt enheter som inte följer institutionens riktlinjer.

Anropa

Genom att anropa datorerna och fråga efter olika typer av information kan MDM-servern kontrollera att användarna har rätt inställningar och mjukvara. Anropen kan gälla hårdvarudata som serienummer och modell eller information om mjukvaran, till exempel macOS-version och installerade appar. Dessutom kan MDM-servern begära statusinformation för viktiga säkerhetsfunktioner, som FileVault och den inbyggda brandväggen.

Hanteringsåtgärder

MDM-lösningen kan utföra en mängd olika administratörsåtgärder på hanterade enheter. Den kan till exempel konfigurera inställningar automatiskt och utan inblandning av användaren uppdatera macOS, fjärrlåsa eller fjärradera enheten och hantera lösenord.

Läs mer om hanteringsåtgärder:
support.apple.com/guide/deployment-reference-macos

Hantera mjukvaruuppdateringar

It-teamet kan låta användarna välja att uppgradera till det senaste operativsystemet så fort det blir tillgängligt. Genom att testa en förhandsversion av macOS kan man upptäcka kompatibilitetsproblem med befintliga appar i ett tidigt skede, så att utvecklare kan lösa problemen före lanseringen. It-teamet kan testa varje ny version med hjälp av Apple Beta Software Program eller AppleSeed for IT. Med ett helhetsgrepp om uppdateringen av företagets Mac-datorer kan användarna och deras data skyddas. Uppdatera ofta och så snart du vet att arbetsflödet är kompatibelt med den senaste versionen av macOS.

MDM kan automatiskt skicka ut macOS-uppdateringar till enhetsregistrerade Mac-datorer. En enhetsregistrerad Mac kan också ställas in så att den skjuter upp uppdateringar och uppdateringsnotiser i upp till 90 dagar om systemet inte är redo för dem. Användaren kan inte sätta igång en uppdatering manuellt förrän riktlinjen har tagits bort eller MDM skickar ut ett installationskommando.

Apple varken rekommenderar eller stöder monolitisk systemavbildning som metod för att uppgradera macOS. Uppdateringar av den fasta programvaran är ofta specifika för en viss modell av Mac-dator, precis som uppdateringar för iPhone och iPad. Vid macOS-uppdatering måste dessa uppdateringar av den fasta programvaran installeras direkt från Apple. Den mest tillförlitliga uppdateringsmetoden är att använda macOS-installeraren eller MDM-kommandon.

Hantera ytterligare mjukvara

Ofta behöver man distribuera ytterligare appar till användarna utöver den ursprungliga uppsättningen. Det kan hanteras automatiskt av MDM-servern när det gäller viktiga appar och uppdateringar. Det kan också skötas manuellt genom att man låter medarbetarna begära appar via en självserviceportal som ingår i MDM-lösningen. Den här typen av portaler kan användas för att installera allt från mjukvara som du har köpt på App Store genom Apple Business Manager till appar, skript och verktyg från andra leverantörer.

De flesta appar kan installeras automatiskt, men vissa installationer kräver åtgärder från användaren. Appar som kräver kärntillägg måste nu av säkerhetsskäl godkännas av användaren innan de kan läsas in. Det kallas användargodkänd inläsning av kärntillägg och kan hanteras av MDM.

Enhetsskydd

De initiala säkerhetsriktlinjer som du och ditt team upprättade före driftsättningen behöver kompletteras med riktlinjer för att övervaka regelefterlevnad och för att få enheterna att rapportera tillbaka så mycket information som möjligt till MDM-servern. Det kan innefatta övervakning av enheternas säkerhetsinställningar eller information om installation av mjukvarufixar. De inbyggda verktygen för kryptering och skydd av Mac-datorer täcker säkerhetsbehoven för de flesta företag, men vissa företag har bestämmelser som kräver användning av ytterligare tjänster för exempelvis filsynkning och delning, skydd mot förlust av data eller detaljerad rapportering om hantering av känsliga data.

iCloud-funktionen Hitta min Mac kan fjärradera alla data på en Mac och inaktivera datorn om den skulle komma i orätta händer. It-teamet kan också utföra fjärraderingar via MDM.

Tilldela en Mac till en annan användare

En Mac kan enkelt tilldelas till en annan användare när en medarbetare lämnar företaget. Det görs med hjälp av internetåterställning och en lokal återställningspartition. På så sätt kan man radera innehållet på datorn och installera den senaste versionen av operativsystemet. En Mac-dator som är tilldelad till en viss MDM i Apple Business Manager kommer automatiskt att registreras i MDM igen via inställningsassistenten, som dessutom gör inställningar för den nya användaren, tillämpar företagspolicyer och driftsätter den mjukvara som behövs. Mac-datorer som inte är registrerade kan raderas och tilldelas till en ny användare på samma sätt och sedan registreras manuellt.

Supportalternativ

Många organisationer upptäcker att Mac-användare behöver minimalt med it-support. De flesta it-team utvecklar verktyg för självbetjäningssupport för att uppmuntra självsupport och höja kvaliteten på supporten. Det kan till exempel handla om att skapa en supportwebbplats för Mac, tillhandahålla webbforum för självsupport och ge teknisk support på plats. MDM-lösningar kan också innehålla en självbetjäningsportal där användarna kan installera och uppdatera mjukvara eller utföra andra supportåtgärder.

Företag bör aldrig sträva efter att lägga ut all support på användarna själva. Däremot kan det vara en bra idé att uppmuntra användarna att själva ta ansvar och delta aktivt genom att felsöka alla problem innan de ringer supporten.

Om alla är med och tar ansvar för support och problemlösning kan man minimera driftstoppen och sänka supportkostnaderna. För organisationer med större behov erbjuder AppleCare en rad program och tjänster som kan användas som komplement till den interna supporten för medarbetare och it-ansvariga.

AppleCare for Enterprise

För företag som önskar heltäckande skydd kan AppleCare for Enterprise hjälpa till att minska belastningen på den interna helpdesken genom att ge teknisk support per telefon dygnet runt, med en timmes svarstid för problem med högsta prioritet. Programmet ger it-teamet support för integreringscenarier med exempelvis MDM och Active Directory.

AppleCare OS Support

Med AppleCare OS Support får it-avdelningen företagssupport per telefon och e-post för driftsättningar med iOS, iPadOS, macOS och macOS Server. Programmet erbjuder support dygnet runt och en särskild Technical Account Manager, beroende på vilken supportnivå du väljer. AppleCare OS Support kan hjälpa it-personalen att effektivisera driftsättning och hantering av enheter samt problemlösning genom att de får direkt tillgång till tekniker för frågor om integrering, migrering och avancerad serverdrift.

AppleCare Help Desk Support

AppleCare Help Desk Support ger förtur till Apples mest erfarna tekniska supportpersonal per telefon. Det innehåller också en uppsättning verktyg för diagnostik och felsökning av Apples hårdvara. Med dem kan stora organisationer administrera sina resurser effektivare, förkorta svarstiderna och minska utbildningskostnaderna. I AppleCare Help Desk Support ingår ett obegränsat antal supporttillfällen för diagnos av mjuk- och hårdvara samt hjälp med att identifiera problem hos iOS-och iPadOS-enheter.

AppleCare och AppleCare+ för Mac

Varje Mac-dator levereras med 90 dagars kostnadsfri teknisk telefonsupport och ett års begränsad garanti. Avtalet kan förlängas till tre år från inköpsdatumet med AppleCare+ eller AppleCare Protection Plan. Användarna kan ringa Apple-supporten och ställa frågor om Apples hårdvara och mjukvara. Apple erbjuder också smidiga servicealternativ för enheter som behöver repareras. AppleCare+ för Mac omfattar också skydd vid ett begränsat antal fall av oavsiktliga skador (för varje fall tillkommer en serviceavgift).

Läs mer om supportalternativ för AppleCare:
www.apple.com/se/support/professional/

Sammanfattning

Det finns många alternativ för enkel driftsättning och hantering, oavsett om ditt företag väljer att driftsätta Mac-datorer i hela organisationen eller endast till en grupp användare. Genom att välja rätt strategier för ditt företag kan du hjälpa medarbetarna att bli mer produktiva och ge dem möjlighet att utföra sitt arbete på helt nya sätt.

Läs mer om driftsättning och hantering av, samt säkerhetsfunktioner i macOS:
support.apple.com/guide/deployment-reference-macos

Läs mer om MDM-inställningar för it-avdelningen:
support.apple.com/guide/mdm

Läs mer om Apple Business Manager:
support.apple.com/guide/apple-business-manager

Läs mer om hanterade Apple-ID:n för företag:
apple.com/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

Läs mer om Apple at Work:
www.apple.com/se/business/

Läs mer om it-funktioner:
www.apple.com/se/business/it/

Läs mer om säkerhet på Apple-plattformen:
www.apple.com/security/

Bläddra bland tillgängliga AppleCare-program:
www.apple.com/se/support/professional/

Upptäck Apple-utbildning och certifiering:
training.apple.com

Kontakta Apple Professional Services:
consultingservices@apple.com