Utrulling av Mac – en oversikt

Introduksjon

Innhold

Introduksjon
Kom i gang
Utrullingstrinn
Supportalternativer
Oppsummering

Vi i Apple mener at de ansatte leverer det beste resultatet når de har tilgang til de beste verktøyene og den beste teknologien. Alle produktene våre er utviklet for å hjelpe de ansatte med å bli mer kreative og produktive, og med å jobbe på nye måter – både på kontoret og på farten. Det er også slik arbeidstakere i dagens samfunn ønsker å jobbe – med bedre tilgang til informasjon, sømløst samarbeid, enkel deling og friheten til å kunne koble seg til og jobbe uansett hvor de er.

Det har aldri vært enklere å sette opp og rulle ut Mac i bedrifter. Ved hjelp av sentrale tjenester fra Apple og en MDM-løsning fra en tredjepart kan organisasjonen din enkelt rulle ut og støtte Macer i stor skala. Hvis organisasjonen din allerede har implementert iOS- og iPadOS-enheter internt, er sannsynligvis mesteparten av det nødvendige arbeidet med infrastrukturen for å implementere macOS, allerede er utført.

Vi har nylig forbedret sikkerhets-, administrerings- og utrullingsfunksjonene for Mac. Organisasjoner kan nå gå fra ensartede systemdiskkopier og vanlig katalogbinding til en sømløs leveringsmodell og utrullingsprosess som fokuserer på den enkelte bruker, og som nesten utelukkende bruker verktøy som er bygget inn i macOS.

Denne veiledningen tar opp alt du trenger å vite for å rulle ut Mac i stor skala – fra forståelse av organisasjonens gjeldende infrastruktur til enhetsadministrering og effektiv distribusjon. Emnene som dekkes i dette dokumentet beskriver i mer detalj i Deployment Reference for Mac: support.apple.com/guide/deployment-reference-macos

Kom i gang

Det er viktig å starte utrullingsprosessen med å utvikle en utrullingsstrategi og evaluere de ansattes nåværende macOS-bruk. Påse at de nødvendige teamene involveres tidlig i prosessen og at de deler de fastsatte visjonene og målene. Noen team starter med et lite konseptbevis for å avdekke problemer som er unike for organisasjonen. Det er helt avgjørende å kommunisere med aktive brukere i et større testprosjekt for å få et klart bilde av hvordan enheter brukes i organisasjonen, og kartlegge eventuelle problemer som teamet må informeres om.

Informasjonen som innhentes i denne fasen, kan klargjøre hvilke roller og funksjoner som vil ha størst nytte av Mac. IT-avdelingen kan deretter vurdere om macOS bør tilbys som standard i hele organisasjonen eller bare i enkelte stillinger.

Denne fasen vil som regel også avdekke en rekke interne apper og verktøy som må være kompatible før Mac kan rulles bredt ut. Fokuser mest på de viktigste appene for produktivitet, samarbeid og kommunikasjon som omfatter de fleste brukerne. Sentrale interne tjenester, som bedriftsintranett, kataloger og programvare for utleggsrapportering, er også viktige for at store deler av organisasjonen kan være produktiv.

Dokumenter og informer om fremgangsmåter eller alternativer for andre interne verktøy samtidig som du oppfordrer den enkelte appeier om å oppdatere ved behov. Vær åpen med brukerne om alle de ulike bedriftsappene de vil kunne bruke når de velger Mac, og la brukerbehov styre moderniseringen. Ved behov kan du utarbeide en plan sammen med appeiere for å se nærmere på hvordan de kan oppdatere appene sine med macOS-SDK-en og Swift. Ta også inn innspill fra alle bedriftspartnere som eventuelt kan hjelpe med utviklingen.

Alle Macer i en organisasjon er som regel bedriftseide enheter. Noen bedrifter lar de ansatte bruke Mac på jobben gjennom BYOD-programmer (Bring Your Own Device). Uansett hva slags eierskapsmodell organisasjonen har valgt, kan det være en fordel for hele organisasjonen å gi de ansatte valget mellom ulike Apple-produkter. Det gir mer produktive, kreative, engasjerte og fornøyde ansatte samt lavere kostnader med tanke på restverdi og support. Organisasjoner kan dessuten ta i bruk ulike leasingavtaler og finansieringsmuligheter for å redusere kostnadene i forkant. De kan også kompensere for kostnader ved å la de ansatte betale en egenandel for oppgradering, som trekkes fra lønnen, eller ved å gi de ansatte muligheten til å kjøpe utstyret når en leasingavtale løper ut, eller ved slutten av enhetens livssyklus.

Bedrifters retningslinjer, i tillegg til utrullings-, administrerings- og supportprosessene beskrevet i dette dokumentet, kan variere avhengig av informasjonen teamene henter inn i testperioden. Alle brukerne trenger for eksempel ikke nøyaktig de samme reglene, innstillingene og appene. Det kan være store variasjoner i behovene til ulike grupper og team i organisasjonen.

Utrullingstrinn

Utrulling av macOS kan deles inn i fire faser: forberedelse av miljøet, oppsett av MDM, utrulling av enheter til ansatte og fullføring av pågående administreringsoppgaver.

1. Forbered

Det første trinnet i alle utrullinger består av en evaluering av det eksisterende miljøet. Denne fasen består av innhenting av kunnskap om organisasjonens nettverk og sentrale infrastruktur og oppsett av de systemene som er nødvendige for å kunne gjennomføre en vellykket utrulling.

Evaluer infrastrukturen

Selv om Mac kan integreres sømløst i de fleste vanlige IT-miljøer i bedrifter, er det viktig å gjøre en vurdering av den eksisterende infrastrukturen for å være trygg på at organisasjonen kan dra full nytte av alle fordelene ved macOS. Hvis organisasjonen trenger hjelp til dette, kan du kontakte Apple Professional Services eller tekniske team hos samarbeidspartnere og forhandlere.

Wi-Fi og nettverk
Kontinuerlig og pålitelig tilgang til et trådløst nettverk er avgjørende når du skal sette opp og konfigurere iOS-enheter. Kontroller at Wi-Fi-nettverket er utformet riktig, inkludert plasseringen av og styrken til tilgangspunkter, slik at det sørger for effektiv roaming og dekker kapasitetsbehovene.

Det kan hende du også må justere konfigurasjonen for nettproxyen eller brannmurportene hvis enhetene ikke har tilgang til Apples tjenere, Apples pushvarslingstjeneste (APNs), iCloud eller iTunes Store. Som med iPad og iPhone krever deler av Mac-utrullingen – spesielt med nyere Mac-maskinvare – konstant tilgang til disse tjenestene for å kunne gjøre ting som å oppdatere firmware under installasjonen.

Apple og Cisco har optimalisert hvordan Mac kommuniserer med trådløse Cisco-nettverk, med støtte for avanserte nettverksfunksjoner i macOS, for eksempel Quality of Service (QoS). Hvis du har utstyr som bruker et Cisco-nettverk, bør du samarbeide med organisasjonens interne team for å påse at Macene har kapasiteten til å optimalisere viktig trafikk.

Bedriftene må også vurdere VPN-infrastrukturen for å påse at brukerne har sikker fjerntilgang til bedriftens ressurser. Vurder å bruke VPN On Demand i macOS, slik at det kun opprettes VPN-tilkobling ved behov. Hvis du har tenkt å bruke Per App VPN, bør du kontrollere at VPN-portalene støtter disse funksjonene, og at du kjøper nok lisenser til å dekke alle brukerne og tilkoblingene.

Påse at nettverksinfrastrukturen er klargjort slik at den fungerer riktig med Bonjour, som er Apples standardbaserte nettverksprotokoll uten konfigurering. Bonjour gjør at enheter automatisk kan finne tjenester på et nettverk. macOS bruker Bonjour til å koble til AirPrint-kompatible skrivere og AirPlay-kompatible enheter, for eksempel Apple TV. Noen apper og integrerte macOS-funksjoner bruker også Bonjour til å finne andre enheter for samarbeid og deling.

Mer om Wi-Fi-nettverksdesign:
support.apple.com/guide/deployment-reference-macos

Mer om å konfigurere nettverket for MDM:
support.apple.com/HT210060

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

Administrering av ID-er
macOS kan bruke katalogtjenester for å administrere ID-er og andre brukerdata, inkludert Active Directory, Open Directory og LDAP. Noen MDM-forhandlere har også verktøy som gjør det lettere å integrere administreringsløsningene deres med Active Directory og LDAP-kataloger. Ytterligere verktøy, som Kerberos Single Sign-on-utvidelsen i macOS Catalina, muliggjør integrering med regler og funksjoner i Active Directory uten vanlig binding eller mobil konto. Ulike sertifikater fra både interne og eksterne sertifiseringsmyndigheter (CA) kan også administreres fra MDM-løsningen, slik at identitetene godkjennes automatisk.

Mer om den nye Kerberos Single Sign-on-utvidelsen:
support.apple.com/guide/deployment-reference-macos

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

Viktige tjenester for de ansatte
Kontroller at Microsoft Exchange-tjenesten er oppdatert og konfigurert, slik at den støtter alle brukerne på nettverket. Hvis du ikke bruker Exchange, fungerer macOS også med standardbaserte tjenere som IMAP, POP, SMTP, CalDAV, CardDAV og LDAP. Test enkel arbeidsflyt for e-post, kontakter og kalendere samt annen produktivitets- og samarbeidsprogramvare som omfatter den høyeste prosentandelen av viktig daglig arbeidsflyt for brukerne.

Mer om å konfigurere Microsoft Exchange:
support.apple.com/guide/deployment-reference-macos

Mer om standardbaserte tjenester:
support.apple.com/guide/deployment-reference-macos

Innholdsbufring
Innholdsbufring er en integrert funksjon i macOS. Den lagrer lokale kopier av innhold som ofte etterspørres fra Apples tjenere, noe som gjør at det brukes mindre båndbredde på å laste ned innhold til nettverket. Du kan bruke bufring til å gi raskere nedlasting og levering av programvare fra Mac App Store. Denne funksjonen kan også bufre programvareoppdateringer for raskere nedlasting til organisasjonens enheter, enten det gjelder macOS, iOS eller iPadOS. Ytterligere innhold kan også bufres med tredjepartsløsninger fra Cisco og Akamai.

Mer om innholdsbufring:
support.apple.com/guide/deployment-reference-macos

Velg en administreringsløsning

Med MDM kan organisasjonen registrere Mac i bedriftsmiljøet på en trygg måte, konfigurere og oppdatere innstillinger trådløst, rulle ut apper, kontrollere at bedriftens regler overholdes, sende spørringer til enheter og fjernslette eller fjernlåse enheter. Det er enkelt for IT-avdelingen å opprette profiler for å administrere brukerkontoer, konfigurere systeminnstillinger, implementere restriksjoner og angi passordregler – og det fra den samme MDM-løsningen som de bruker i dag for iPhone og iPad.

I bakgrunnen bruker alle Apple-plattformene et vanlig administreringsrammeverk fra Apple, som gjør det mulig for kunder å jobbe med ulike MDM-løsninger fra tredjeparter. En rekke tredjeparter har løsninger for enhetsadministrering, for eksempel Jamf, VMware og MobileIron. Selv om macOS, iOS og iPadOS deler mange av de samme rammeverkene for enhetsadministrering, er disse løsningene noe ulike med tanke på administreringsfunksjonalitet, support for operativsystemet, priser og vertsmodeller. De kan også hende at de ikke tilbyr de samme tjenestene for integrering, opplæring og support. Før organisasjonen velger en løsning, må den vurdere hvilke funksjoner som er mest relevante for dem.

Når MDM-løsningen er valgt, må du gå til Apple Push Certificates Portal og logge på for å opprette et nytt MDM-pushsertifikat.

Mer om å rulle ut MDM:
support.apple.com/guide/deployment-reference-macos

Gå til Apple Push Certificates Portal:
identity.apple.com/pushcert/

Registrer deg i Apple Business Manager

Apple Business Manager er en nettbasert portal der IT-administratorer kan rulle ut iPhone, iPad, iPod touch, Apple TV og Mac fra ett og samme sted. Apple Business Manager fungerer sømløst med løsningen du allerede bruker for administrering av mobilenheter (MDM), og gjør det enkelt å automatisere utrullingen av enheter, kjøpe apper og distribuere innhold samt opprette administrerte Apple ID-er for ansatte.

Enhetsregistreringsprogrammet (DEP) og Voluminnkjøpsprogrammet (VPP) er nå fullstendig integrert i Apple Business Manager, slik at organisasjonene har alt de trenger for utrulling av Apple-enheter, på ett og samme sted. Disse programmene vil ikke lenger være tilgjengelige etter 1. desember 2019.

Enheter

Apple Business Manager muliggjør automatisk enhetsregistrering. Dermed får organisasjonene en rask og sømløs måte å rulle ut bedriftseide Apple-enheter og registrere dem i MDM på, uten å måtte håndtere dem fysisk eller klargjøre én og én enhet.

- Forenkle konfigurasjonsprosessen ved å harmonisere fremgangsmåten i Oppsettassistent, slik at de ansatte får enhetene korrekt konfigurert ved oppstart. IT-teamene kan nå tilpasse denne opplevelsen ytterligere ved å legge inn samtykketekst, bedriftslogoer og -design samt moderne autentisering.

- Få et høyere nivå av kontroll med bedriftseide enheter ved å bruke enheter under tilsyn, som gir deg ekstra kontroller for enhetsadministrering som ikke er tilgjengelige med andre utrullingsmodeller, for eksempel MDM som ikke kan fjernes.
- Du kan enkelt administrere standard MDM-tjenere ved å angi en standardtjener for hver enhetstype. Og du kan nå registrere iPhone, iPad og Apple TV manuelt i DEP ved hjelp av Apple Configurator 2, uansett hvordan du kjøpte dem.

Innhold

Apple Business Manager gjør det enkelt for organisasjoner å kjøpe innhold i store kvanta. Uansett om de ansatte bruker iPhone, iPad eller Mac, kan du gi dem kvalitetsinnhold som er klart til bruk, med fleksible og sikre alternativer for distribusjon.

- Kjøp apper, bøker og tilpassede apper i store kvanta – også egenutviklede apper. Overfør applisenser mellom avdelinger og del lisenser mellom kjøpere i samme avdeling. Og se en fullstendig kjøpshistorikk, inkludert hvor mange lisenser som for øyeblikket er i bruk via MDM.
- Distribuer apper og bøker direkte til administrerte enheter eller autoriserte brukere. Det er enkelt å holde oversikt over innholdet som er tilordnet de ulike brukerne eller enhetene. Med administrert distribusjon kontrollerer du hele distribusjonsprosessen og beholder fullt eierskap til alle appene. Og når en enhet eller bruker ikke lenger trenger en bestemt app, kan den kalles tilbake og tilordnes på nytt i organisasjonen.
- Velg mellom flere betalingsmetoder, inkludert kredittkort og innkjøpsordrer. Organisasjoner kan kjøpe volumkreditt (der det er tilgjengelig) for bestemte beløp fra Apple eller fra en Apple-autorisert forhandler til et spesifikt beløp i lokal valuta, som leveres elektronisk til kontoinnehaveren i form av en butikkredit.
- Du kan distribuere en app til enheter eller brukere i et hvilket som helst land der appen er tilgjengelig, noe som muliggjør multinasjonal distribusjon. Utviklere kan gjøre appene sine tilgjengelige i flere land ved å følge den vanlige publiseringsprosessen for App Store.

Merk: Bokkjøp i Apple Business Manager er ikke tilgjengelig i enkelte land eller områder. På support.apple.com/HT207305 finner du en oversikt over hvilke funksjoner og betalingsmetoder som er tilgjengelige i de ulike landene.

Personer

Apple Business Manager gir organisasjonene mulighet til å opprette og administrerte kontoer for ansatte, integrere kontoene med eksisterende infrastruktur og få tilgang til Apple-apper og -tjenester samt Apple Business Manager.

- Opprett administrerte Apple ID-er som ansatte kan bruke til å jobbe sammen via Apple-apper og -tjenester samt få tilgang til jobbdata i administrerte apper som bruker iCloud Drive. Disse kontoene eies og kontrolleres av den enkelte organisasjonen.
- Dra nytte av funksjonaliteten for forent autentisering ved å knytte Apple Business Manager til Microsoft Azure Active Directory.

Administrerte Apple ID-er opprettes automatisk når den ansatte logger på første gang med eksisterende påloggingsinformasjon på en kompatibel Apple-enhet.

- Bruk administrerte Apple ID-er sammen med private Apple ID-er på enheter de ansatte selv eier, med den nye Brukerregistrering-funksjonen på iOS 13, iPadOS og macOS Catalina. Eventuelt kan administrerte Apple ID-er brukes som den primære (og eneste) Apple ID-en på en hvilken som helst enhet Administrerte Apple ID-er kan også få tilgang til iCloud på nettet etter første gangs innlogging på en Apple-enhet.
- Tilordne andre roller til IT-teamene i organisasjonen din for å administrere enheter, apper og kontoer effektivt i Apple Business Manager. Bruk Administrator-rollen til å samtykke i vilkår for bruk der dette er aktuelt, og overfør enkelt ansvar dersom noen forlater organisasjonen.

Merk: Brukerregistrering har for tiden ikke støtte for iCloud Drive. iCloud Drive kan brukes med en administrert Apple ID dersom det er den eneste Apple ID-en på enheten.

Mer om Apple Business Manager: apple.com/no/business/it

Registrer deg i Apple Developer Enterprise Program

Apples Developer Enterprise Program tilbyr et komplett sett med verktøy for utvikling, testing og distribuering av apper til brukere. Du kan distribuere appene enten med en MDM-løsning eller ved å plassere dem på en nettjener. Mac-apper og -installerere kan signeres og godkjennes med utvikler-ID-en din for Gatekeeper, som bidrar til å beskytte macOS mot skadelig programvare.

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

2. Sett opp

Oppsett før en utrulling innebærer å fastsette bedriftens regler og gjøre MDM-løsningen klar til å konfigurere de ansattes Macer.

Forstå sikkerhetsfunksjonene i macOS

Det legges stor vekt på sikkerhet og personvern ved utviklingen av Apple-maskinvare, -programvare og -tjenester. Vi ivaretar kundenes personvern med sterk kryptering, og vi har strenge retningslinjer for hvordan vi behandler alle data. En sikker dataplattform for Apple-enheter inkluderer:

- metoder som forhindrer uautorisert tilgang til enheter
- beskyttelse av arkiverte data, selv hvis en enhet blir borte eller stjålet
- nettverksprotokoller og kryptering av data som overføres
- sikker kjøring av apper uten at det går på bekostning av plattformintegriteten

Alle Apple-enheter har flere sikkerhetslag, slik at viktige data beskyttes og enhetene får sikker tilgang til nettverkstjenester. macOS, iOS og iPadOS styrker også sikkerheten med koder og passord, som kan leveres og overholdes med MDM. En bruker eller administrator kan fjernslette all privat informasjon hvis en enhet kommer på avveier.

IT-avdelingen kan bruke MDM til å rulle ut en rekke regler for å bidra til å sikre enhetene. Eksempler er bruk av FileVault og deponering av gjenopprettingsnøkkel via MDM, krav til en bestemt passordregel eller skjermsparerlås, og aktivering av den innebygde brannmuren.

Mer om Apple Platform Security: apple.com/security/

Fastsett bedriftens regler

Start med å fastsette generelle regler som dekker flesteparten av bedriftens Mac-brukere. Med MDM-løsningen kan du definere brukerspesifikke tilpasninger, som kontoer eller tilgang til bestemte apper. Du kan også angi spesifikke regler for organisasjoner eller andre mindre undergrupper av brukere, for eksempel utrulling av programvare eller innstillinger for én bestemt avdeling.

Samarbeid med bedriftens interne team om å oppdatere de eksisterende reglene for å innlemme bruken av Mac. Noen grunnleggende regler forblir de samme på alle plattformene, slik som kompleksitetsnivå for passord og hvor ofte det må endres, tidsavbrudd for skjermsparer og akseptabel bruk.

Hvis bedriftens regler krever en bestemt teknologi som brukes på en annen plattform, er det nødvendig å forstå det underliggende problemet og jobbe med å endre reglene, slik at de også støtter teknologi som er innebygd i macOS. I stedet for å kreve at alle datamaskiner bruker en bestemt løsning fra en tredjepart til å kryptere en hel disk, bør du vurdere å lage en regel som slår fast at bedriftsdata må krypteres ved arkivering, og at det må gjøres med FileVault. Hvis regelen krever en bestemt programvare for å beskytte mot skadelig programvare, må du informere teamene om innebygde funksjoner som Gatekeeper og deretter oppdatere regelen slik at det tillates.

Konfigurer innstillinger i MDM

Hver Mac registreres på en sikker måte med bedriftens MDM-løsning for å muliggjøre administrering av bedriftens regler og sikre at de ansatte har tilgang til de nødvendige ressursene. MDM-løsninger tar deretter i bruk regler og innstillinger ved hjelp av konfigurasjonsprofiler. Konfigurasjonsprofiler er XML-filer som MDM-løsningen har opprettet, og som muliggjør distribusjon av innstillinger til enheter. Disse profilene automatiserer konfigureringen av innstillinger, kontoer, regler, restriksjoner og påloggingsinformasjon. De kan signeres og krypteres for å bidra til økt sikkerhet for systemene.

Når en enhet er registrert i MDM, kan en administrator aktivere MDM-regler, -spørringer eller -kommandoer. Når enheten er koblet til et nettverk, mottar den så en varsling via Apples pushvarslingstjeneste (APNs), som gir den instrukser om å kommunisere direkte med MDM-løsningen over en sikker tilkobling for å behandle administratorens handling. APNs overfører ikke konfidensiell eller merkevarebeskyttet informasjon ettersom kommunikasjonen kun er mellom MDM-løsningen og enheten. Hvis en enhet fjernes fra administrering, vil innstillingene og reglene som kontrolleres av den konfigurasjonsprofilen, bli fjernet. Bedriften kan også fjernslette en enhet om nødvendig.

Mange organisasjoner legger MDM-løsningen til de eksisterende katalogtjenestene. Oppsettassistenten i macOS kan be brukerne om å logge på med påloggingsinformasjonen for katalogtjenesten under automatisk enhetsregistrering.

Med macOS Catalina gjør nye tilpassingsvalg for registrering det mulig for oppsettsassistenten å vise autentisering fra skyidentitetsleverandører. Når enheten tilordnes en bestemt bruker, kan MDM tilpasse konfigurasjoner og kontoer som er spesifikke for enkeltbrukere eller en gruppe. En brukers individuelle Microsoft Exchange-konto kan for eksempel sendes automatisk under registrering. Det er også mulig å bruke sertifikatidentiteter for teknologier som 802.1x, VPN og annet.

Ettersom disse systemene gir gode kontrollmuligheter, gir bedrifter ofte brukeren administratorrettigheter på Macen sin. Brukeren kan da tilpasse innstillinger, installere apper og feilsøke problemer samtidig som vedkommende holdes innenfor bedriftens regler via MDM. Denne modellen følger typen rettigheter og kontroll som brukere har over iPhonen eller iPaden sin når den administreres.

Mer om konfigurasjonsprofiler:
support.apple.com/guide/deployment-reference-macos

Forbered automatisk enhetsregistrering

Du kan enkelt registrere en enhet i MDM under prosessen med oppsettassistenten med automatisk enhetsregistrering i Apple School Manager. Det gjør registrering mulig uten assistanse fra IT-avdelingen. Enkelte av trinnene i oppsettassistenten kan også utelates for å gjøre prosessen raskere for brukerne.

Hvis du vil konfigurere den automatiske enhetsregistreringen, må du koble MDM-løsningen til Apple School Manager-kontoen din ved hjelp av et sikkert kjennetegn. MDM-løsningen blir autorisert på en sikker måte ved hjelp av totrinnsverifisering. MDM-leverandøren kan gi deg dokumentasjon med detaljert informasjon om implementering.

Hvis enhetene allerede brukes av de ansatte eller eies av enkeltbrukere, kan én enkelt konfigurasjonsprofil åpnes av brukeren og kontrolleres i Systemvalg for å fullføre registreringen. Dette er kjent som brukergodkjent MDM-registrering. For å kunne administrere visse sikkerhetssensitive innstillinger, som regler for kjernetillegg og Privacy Preferences Policy Control, må registreringen gjennomføres enten gjennom enhetsregistrering eller via brukergodkjent MDM-registrering.

Mer om lasting av kjerneutvidelser:
support.apple.com/guide/deployment-reference-macos

Mer om Privacy Preferences Policy Control:
support.apple.com/guide/mdm

Klargjør for distribuering av apper og bøker

Apple tilbyr omfattende programmer som gjør det enklere for organisasjonen å dra nytte av appene og innholdet som er tilgjengelig for macOS. Med disse mulighetene kan du distribuere apper og bøker som er kjøpt gjennom Apple Business Manager eller utviklet internt, til brukere, slik at de har alt de trenger for å arbeide effektivt. MDM kan også distribuere apper og installere pakker for programvare som ikke er tilgjengelig på Mac App Store.

MDM-løsningen din kan bruke administrert distribusjon til å distribuere apper og bøker som er kjøpt i Apple Business Manager i land der appen er tilgjengelig. Hvis du vil aktivere administrert distribusjon, kobler du først sammen

MDM-løsningen med Apple Business Manager-kontoen ved hjelp av et sikkert kjennetegn. Når du er tilkoblet MDM-løsningen, kan du tilordne apper og bøker til brukerne selv om App Store er deaktivert på enheten. Du kan også tilordne apper direkte til enhetene, som gjør utrullingen betydelig enklere ettersom alle brukere på den enheten vil ha tilgang til alle appene.

Mer om å kjøpe innhold i Apple Business Manager:
support.apple.com/guide/apple-business-manager

Mer om å distribuere apper og bøker:
support.apple.com/guide/apple-business-manager

Forbered ytterligere innhold

MDM-løsningen kan være til hjelp ved distribuering av ytterligere pakker med innhold som ikke er fra Mac App Store. Dette er en vanlig fremgangsmåte for mange programvarepakker for bedrifter, som spesialutviklede interne apper eller apper som Chrome eller Firefox. Påkrevd programvare kan distribueres med denne metoden og installeres automatisk etter fullført registrering. Fonter, prosedyrer og andre elementer kan også installeres og utføres via pakker. Påse at disse pakkene signeres på riktig måte med utvikler-ID-en fra Developer Enterprise Program.

Mer om å installere ytterligere innhold:
support.apple.com/guide/deployment-reference-macos

3. Rull ut

Med macOS er det lett å rulle ut enheter til ansatte, tilpasse dem etter behov og gjøre alt klart uten assistanse fra IT-avdelingen.

Bruk oppsettassistenten

Ved oppstart kan de ansatte bruke oppsettassistenten i macOS til å angi innstillinger for språk og område og koble til et nettverk. Når brukerne kobler til internett, viser oppsettassistenten en rekke vinduer som leder dem gjennom de grunnleggende trinnene i oppsettet av den nye Macen. Enheter som er registrert i Apple Business Manager, kan automatisk registreres i MDM under denne prosessen. Enhetsregistrerte Mac-systemer kan også konfigureres til å utelate visse trinn, for eksempel vilkår og betingelser, pålogging med Apple ID, stedstjenester og annet.

MDM kan deretter brukes etter oppsettassistenten til å rulle ut en rekke innstillinger ved første konfigurering, inkludert definering av hvorvidt en bruker får fulle administratorrettigheter på datamaskinen. På samme måte som med iPhone og iPad beholder de kontroll over enheten, samtidig som de forholder seg til bedriftens regler og innstillinger som administreres gjennom MDM.
For å sikre at brukerne umiddelbart kan begynne å jobbe etter at oppsettassistenten er fullført, bør bare de viktigste appene og pakkene starte nedlasting og installering i bakgrunnen. Dermed forhindres ikke brukerne fra å jobbe. Større apper kan settes til nedlasting og installering i bakgrunnen eller på et senere tidspunkt av brukeren i MDM-løsningens selvbetjente verktøy.

Konfigurer bedriftskontoer

MDM kan sette opp e-post og andre brukerkontoer automatisk. Avhengig av MDM-løsningen og integreringen med de interne systemene kan nyttelaster for kontoer også forhåndsutfylles med brukernavn, e-postadresse og sertifikatidentiteter for autentisering og signering.

Tillat personlig tilpassing

Det kan bidra til høyere produktivitet å la brukerne tilpasse enhetene, siden de velger hvilke apper og hva slags innhold som best kan hjelpe dem med å gjennomføre oppgaver og nå mål. Og med administrerte Apple ID-er og Brukerregistrering i macOS Catalina får organisasjonene nye måter å gi brukere tilgang til Apple-tjenester fra en organisasjonseid Apple ID eller sammen med en personlig Apple ID.

Apple ID og administrert Apple ID

Når ansatte bruker en Apple ID til å logge på Apple-tjenester som FaceTime, iMessage, App Store og iCloud, får de tilgang til et stort utvalg av innhold for effektivisering av bedriftsoppgaver, produktivitetsøkning og samarbeidsstøtte. I likhet med vanlige Apple ID-er kan administrerte Apple ID-er også brukes til å logge på personlige enheter. De kan også brukes til å få tilgang til Apple-tjenester – som iCloud og samarbeid med iWork og Notater – og Apple Business Manager. I motsetning til Apple ID-er er Administrerte Apple ID-er eid og administrert av den enkelte organisasjonen. Dette gjelder også tilbakestilling av passord og rollebasert administrasjon. Administrerte Apple ID-er har enkelte begrensede innstillinger.

Enheter som er registrert via Brukerregistrering, krever en administrert Apple ID. Brukerregistrering støtter en alternativ personlig Apple ID: andre registreringsalternativer støtter enten en personlig Apple ID eller en administrert Apple ID. Det er kun Brukerregistrering som støtter flere Apple ID-er.

For å få mest mulig ut av disse tjenestene, bør brukerne bruke sine egne Apple ID-er eller administrerte Apple ID-er som er opprettet for dem. Brukere som ikke har en Apple ID, kan lage en allerede før de får enheten. De ansatte kan også bruke Oppsettassistent til å opprette en personlig Apple ID hvis de ikke allerede har en. Brukerne trenger ikke betalingskort for å opprette en Apple ID.

Mer om administrerte Apple ID-er:
support.apple.com/guide/deployment-reference-macos

iCloud

Med iCloud kan brukerne automatisk synkronisere dokumenter og personlig innhold – for eksempel kontakter, kalendere, dokumenter og bilder – og holde dem oppdatert på flere enheter. Med Finn kan brukerne finne en mistet eller stjålet Mac, iPhone, iPad eller iPod touch. Bestemte deler av iCloud, som iCloud-nøkkelring og iCloud Drive, kan deaktiveres gjennom restriksjoner som angis enten manuelt på enheten eller via MDM. Dette gir organisasjonene mer kontroll over hva slags data som arkiveres på hvilken konto.

Mer om å administrere iCloud:
support.apple.com/guide/deployment-reference-macos

4. Administrer

Når brukerne har tatt i bruk enhetene, er det en rekke administrative funksjoner som kan benyttes til administrering og vedlikehold av enheter og innhold over tid.

Administrer enheter

MDM-løsningene kan administrere en administrert enhet gjennom et sett med bestemte oppgaver. Disse oppgavene går blant annet ut på å spørre enhetene om informasjon og å starte oppgaver som kan brukes til å administrere enheter som bryter regler eller er mistet eller stjålet.

Spørringer

En MDM-løsning kan spørre enheter om ulik informasjon for å sikre at brukerne har de nødvendige appene og innstillingene. Spørringene kan gjelde maskinvare, for eksempel serienummer eller enhetsmodell, eller programvare, for eksempel macOS-versjon eller en liste over over installerte apper. I tillegg kan MDM spørre om status for viktige sikkerhetsfunksjoner, for eksempel FileVault eller den innebygde brannmuren.

Administreringsoppgaver

Når en enhet administreres, kan en MDM-løsning utføre en rekke administrative oppgaver, for eksempel å endre konfigureringsinnstillingene automatisk uten brukermedvirkning, utføre en macOS-oppdatering, fjernlåse eller fjernslette en enhet eller administrere passord.

Mer om administreringsoppgaver:
support.apple.com/guide/deployment-reference-macos

Administrer programvareoppdateringer

IT-avdelingen kan gi brukerne mulighet til å velge å oppgradere til det nyeste operativsystemet når det blir gjort tilgjengelig. Ved å teste en førlanseringsversjon av macOS kan IT-avdelingen forsikre seg om at eventuelle kompatibilitetsproblemer for applikasjoner oppdages tidlig og løses sammen med utviklerne før den endelige versjonen lanseres. IT-avdelingen kan også bidra med å teste hver versjon gjennom Apples program for betaprogramvare eller AppleSeed for IT. Legg stor vekt på oppdatering av Macene for å beskytte brukerne og dataene deres. Oppdater ofte, så snart du har sjekket at arbeidsflyten er kompatibel med en ny hovedversjon av macOS.

MDM kan automatisk distribuere macOS-oppdateringer til en enhetsregistrert Mac. En enhetsregistert Mac kan også konfigureres til å utsette oppdateringer og varslinger om oppdateringer i opptil 90 dager hvis viktige systemer ikke er klare. Brukerne vil ikke kunne gjennomføre oppdateringer manuelt før regelen fjernes eller MDM sender en installeringskommando.

Apple anbefaler ikke og støtter ikke ensartede systemdiskkopier for macOS-oppgraderinger. Som med iPhone og iPad er Mac ofte avhengig av modellspesifikke firmwareoppdateringer. Oppdateringer av Macens operativsystem krever også at disse firmwareoppdateringene installeres direkte fra Apple. Den mest pålitelige strategien er å bruke macOS-installereren eller MDM-kommandoer for å oppdatere.

Administrer ytterligere programvare

Organisasjonene har ofte behov for å distribuere flere apper til brukerne etter at de første appene er installert. Dette kan gjøres automatisk med MDM for viktige apper og oppdateringer eller ved behov ved å la de ansatte be om apper gjennom en selvbetjent portal fra MDM-løsningen. Disse portalene kan gjøre alt fra å installere programvare kjøpt på App Store gjennom Apple Business Manager til å installere apper, prosedyrer og andre verktøy som ikke er fra App Store.

Det meste av programvare kan installeres automatisk, men noen installeringer krever brukermedvirkning. For ekstra sikkerhet må brukerne nå godkjenne innlasting av innhold for apper som krever kjerneutvidelser. Dette heter brukergodkjent innlasting av kjerneutvidelser og kan administreres gjennom MDM.

Opprettholde sikkerheten på enheten

I tillegg til de første sikkerhetsretningslinjene som ble etablert før utrullingen av enhetene, må teamet ditt holde tilsyn med maskinene og sjekke at regler overholdes, og de må eksportere så mange rapporter som mulig gjennom bedriftens MDM-løsning. Dette inkluderer kontroll av sikkerhetstilstanden til hver enhet og innhenting av informasjon om installering av programvarefeilrettinger. De fleste organisasjoner synes det er greit å bruke de innebygde verktøyene til å kryptere og beskytte Macene, men noen bruker også filsynkronisering og -deling eller verktøy som verner mot datatap, for å forhindre lekkasje av bedriftsdata og utarbeide detaljerte rapporter om sensitive data.

Finn Mac-funksjonen i iCloud kan brukes til fjernsletting, som innebærer at alle data slettes og at Macen deaktiveres hvis den blir stjålet eller kommer på avveier. IT-avdelingen kan også fjernslette data med MDM.

Distribuer enheter på nytt

Når en ansatt slutter, er det enkelt å distribuere Macen til en annen bruker. Det gjøres med den lokale gjenopprettingspartisjonen eller med Internett-gjenoppretting. Alt innholdet på Macen kan slettes, og den nyeste versjonen av operativsystemet kan installeres. En Mac som er tilordnet en bestemt MDM i Apple Business Manager, vil automatisk registrere seg på nytt i MDM med oppstartsassistenten, konfigurere innstillinger for den nye brukeren, iverksette eventuelle regler for bedriften og rulle ut all nødvendig programvare. Macer som ikke er enhetsregistrerte, kan fjernslettes, og de kan distribueres til en annen bruker på samme måte og deretter registreres på nytt manuelt.

Supportalternativer

Mange organisasjoner gjør den erfaringen at Mac-brukere trenger minimalt med support fra IT-avdelingen. For å oppfordre til egensupport, samt for å øke kvaliteten på supporten, utvikler de fleste IT-avdelingene verktøy for egensupport. Eksempler på dette kan være en omfattende nettside for Mac-support, selvhjelpsforumer og et sted der brukerne kan få teknisk hjelp. Ved hjelp av MDM-løsninger kan også brukerne utføre supportoppgaver, som installering eller oppdatering av programvare fra en selvbetjent portal.

Som mønsterpraksis burde ikke bedrifter tvinge brukerne sine til å være hundre prosent selvgående med tanke på support. Legg heller opp til samarbeid ved problemløsning, og fokuser på å la brukerne gjennomføre feilsøking på egen hånd før de kontakter IT-avdelingen for hjelp. Oppfordre brukerne til å engasjere seg i prosessen, og få dem til å undersøke problemet selv før de ber om hjelp.

Når supportansvaret deles, reduseres nedetiden for de ansatte, og de totale utgiftene til support og bemanning reduseres. For de organisasjonene som trenger mer, tilbyr AppleCare en rekke programmer og tjenester som fungerer side om side med den interne supportstrukturen.

AppleCare for Enterprise

Bedrifter som vil ha komplett dekning, kan bruke AppleCare for Enterprise til å redusere belastningen på de interne supportmedarbeiderne ved å gi teknisk support til ansatte på telefon døgnet rundt, med én times svartid for høyt prioriterte problemer. Programmet legger opp til integreringsscenarioer gjennom IT-avdelingen, inkludert med MDM og Active Directory.

AppleCare OS Support

Med AppleCare OS Support får IT-avdelingen telefon- eller e-postbasert support på bedriftsnivå for iOS-, iPadOS-, macOS- og macOS Server-utrullinger. De har tilgang til support opptil 24 timer i døgnet, syv dager i uken, og en egen teknisk kontaktperson, avhengig av nivået på kundestøtten du kjøper. AppleCare OS Support gir IT-medarbeiderne i organisasjonen direkte tilgang til teknikere som kan svare på spørsmål om integrering, migrering og avansert tjenerbruk, slik at de kan rulle ut og administrere enheter og løse problemer mer effektivt.

AppleCare Help Desk Support

AppleCare Help Desk Support tilbyr prioritert tilgang til Apples erfarne teknikere. Det inkluderer også en verktøypakke for diagnostisering og feilsøking av Apple-maskinvare, slik at store organisasjoner kan administrere ressurser mer effektivt, forbedre responstiden og redusere opplæringskostnadene. AppleCare Help Desk Support dekker et ubegrenset antall supporthenvendelser for maskinvare- og programvarediagnose samt feilsøking og problemisolering for iOS- og iPadOS-enheter.

AppleCare og AppleCare+ for Mac

Alle Macer leveres med en begrenset garanti på ett år og gratis teknisk telefonsupport i 90 dager etter kjøpet. Servicedekningen kan utvides til tre år fra kjøpsdato med AppleCare+ eller AppleCare Protection Plan. De ansatte kan ringe Apple Support med spørsmål om maskinvare og programvare fra Apple. Apple tilbyr også praktiske serviceløsninger når enhetene må repareres. I tillegg tilbyr AppleCare+ for Mac dekning for enkelte tilfeller av skade som følge av uhell, mot et servicetillegg for hvert tilfelle.

Mer om ulike former for AppleCare-support:
apple.com/no/support/professional/

Oppsummering

Enten bedriften skal rulle ut Macer til en gruppe brukere eller hele organisasjonen, har du mange alternativer for enkel utrulling og administrasjon av enheter. Velger du riktig strategi for din bedrift, kan det bidra til at de ansatte blir mer produktive og kan utføre arbeidet på helt nye måter.

Mer om utrullings-, administrerings- og sikkerhetsfunksjoner i macOS:
support.apple.com/guide/deployment-reference-macos

Mer om MDM-innstillinger for IT:
support.apple.com/guide/mdm

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

Mer om administrerte Apple ID-er for bedrifter:
apple.com/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

Mer om Apple at Work:
www.apple.com/no/business/

Mer om IT-funksjoner:
www.apple.com/no/business/it/

Mer om Apple Platform Security:
www.apple.com/security/

Tilgjengelige AppleCare-programmer:
www.apple.com/no/support/professional/

Apple Training and Certification:
training.apple.com

Kontakt Apple Professional Services:
consultingservices@apple.com