Utrulling av iOS og iPadOS – en oversikt

Introduksjon

Innhold

iPhone og iPad kan endre bedriften og måten de ansatte jobber på. De kan gi produktiviteten et kraftig løft og gi de ansatte frihet og fleksibilitet til å jobbe på nye måter, enten på kontoret eller når de er på farten. Satsing på disse moderne arbeidsmetodene vil gagne hele organisasjonen. Brukerne har bedre tilgang til informasjon, slik at de har verktøyene de trenger, og kan løse problemer på en kreativ måte.

Ved å støtte iOS og iPadOS kan IT-avdelingene bli sett på som de som former forretningsstrategien og løser praktiske problemer, i stedet for bare å være de som ordner med teknologi og kutter kostnader. Dette er positivt for alle parter, siden det gir de ansatte ny giv og åpner for nye forretningsmuligheter.

Det har aldri vært enklere å sette opp og rulle ut iPhone og iPad i hele bedriften. Med Apple Business Manager og en MDM-løsning (Mobile Device Management) fra en tredjepart kan organisasjonen din enkelt rulle ut iOS- og iPadOS-enheter og -apper i stor skala.

- MDM-løsninger brukes til å konfigurere og administrere enheter samt distribuere og administrere apper trådløst.
- Apple Business Manager automatiserer registrering av Apple-enheter i MDM-løsningen for mer effektive utrullinger med berøringsfri konfigurering for IT-avdelingen.
- I Apple Business Manager kan du kjøpe apper og bøker i store kvanta og distribuere dem trådløst til brukerne.
- Med Apple Business Manager kan du også opprette administrerte Apple ID-er for ansatte ved hjelp av forent autentisering med Microsoft Azure AD.

Dette dokumentet gir veiledning i utrulling av iOS- og iPadOS-enheter i organisasjonen og hjelper deg med å lage en utrullingsplan som er best mulig tilpasset miljøet ditt. Du finner mer utfyllende informasjon on disse emnene i Håndbok for utrulling for iPhone og iPad på nett: support.apple.com/guide/deployment-reference-ios

Eierskapsmodeller

Det viktige første trinnet i utrullingen er å evaluere forskjellige eierskapsmodeller og finne den som er riktig for organisasjonen. Utrulling kan utføres forskjellige måter, avhengig av hvem som eier enhetene. Du begynner med å finne ut hva som passer best for organisasjonen.

Det er to eierskapsmodeller for iOS- og iPadOS-enheter som vanligvis brukes i bedrifter:

- Organisasjonseid
- Brukereid

De fleste organisasjoner har en foretrukket modell, men det kan hende at du kommer over flere modeller i miljøet ditt. Hovedkontoret kan for eksempel ha en utrullingsstrategi med brukereide enheter, der de ansatte kan sette opp en brukereid iPad, samtidig som bedriftens ressurser beskyttes og administreres uten innvirkning på brukernes egne data og apper. Selskapets butikker kan imidlertid velge en strategi med bedriftseide enheter der flere ansatte kan dele iOS- og iPadOS-enheter for å behandle kundetransaksjoner.

Gå gjennom disse modellene, og finn ut hvilke som passer best for akkurat ditt miljø. Når du har bestemt hvilken modell organisasjonen skal bruke, kan du og kollegene dine se nærmere på Apples løsninger for utrulling og administrering.

Organisasjonseide enheter

Med organisasjonseide enheter kan du supplere enheter til de ansatte til daglig bruk, dele enheter blant de ansatte til fellesarbeid eller konfigurere enheter til spesifikt bruk som er låst til en enkelt app. Enheter som gis til en enkelt bruker, kan tilpasses av sluttbrukeren. Enheter som er låst til en enkelt app eller deles blant flere brukere, er typisk ikke tilpasset av sluttbrukeren. Ved å bruke en kombinasjon av disse modellene, viktige teknologier fra Apple og en MDM-løsning kan oppsett og konfigurering av enheter utføres helt automatisk.

Med personlig tilpassing. Hvis du velger en strategi med personlig tilpassing av enhetene, kan du få hver bruker til å velge sin egen enhet og registrere den i en MDM-løsning der organisasjonsinnstillinger og apper overføres trådløst. For enheter kjøpt direkte fra Apple eller deltakende Apple-autoriserte forhandlere eller leverandører kan du også bruke Apple Business Manager til automatisk registrering av nye enheter i MDM-løsningen, også kjent som automatisert enhetsregistrering. Når enhetene er konfigurert, kan de tilpasses av brukeren med egne apper og data, i tillegg til eventuelle bedriftskontoer eller -apper som leveres av organisasjonen.

Uten personlig tilpassing. Når enhetene deles av flere eller brukes utelukkende til ett bestemt formål (for eksempel på en restaurant eller et hotell), konfigurerer og administrerer vanligvis IT-administratorer enhetene sentralt i stedet for å la hver enkelt bruker gjøre dette. Ved utrulling som ikke kan tilpasses personlig, har brukerne vanligvis ikke tilgang til å installere apper eller arkivere personlige data på enhetene. Automatisert enhetsregistrering via Apple Business Manager kan også hjelpe med å automatisere oppsettet av ikke-tilpassede enheter. Diagrammet nedenfor viser hvilke handlinger som må utføres av administratoren og brukeren i de enkelte trinnene i en organisasjonseid strategi. Med mindre annet er angitt, gjelder de utrulling av både enheter *med personlig tilpassing* og enheter *uten personlig* tilpassing.

	Administrator	Bruker
Forberedelse	• Evaluer infrastrukturen • Velg en MDM-løsning • Registrer deg i Apple Business Manager	• Ingen brukerhandlinger er nødvendig
Sett opp	• Konfigurer enheter • Distribuer apper og bøker	• Ingen brukerhandlinger er nødvendig
Rull ut	• Distribuer enheter **Kun med personlig tilpassing** • Tillat at brukerne tilpasser enhetene	**Med personlig tilpassing** • Last ned og installer apper og bøker • Bruk eventuelt Apple ID og App Store- og iCloud-kontoer **Kun uten personlig tilpassing** • Ingen brukerhandlinger nødvendig
Administrer	• Administrer enheter • Rull ut og administrer ekstra innhold	**Med personlig tilpassing** • Finn flere apper som kan brukes **Kun uten personlig tilpassing** • Ingen brukerhandlinger er nødvendig

Brukereide enheter

Når enheter kjøpes og settes opp av brukeren i det som vanligvis kalles utrullinger av brukereide enheter, eller BYOD-utrullinger (Bring Your Own Device), kan du fortsatt gi tilgang til bedriftstjenester som Wi-Fi, e-post og kalendere med MDM gjennom det nye valget for Brukerregistrering i iOS 13 og iPadOS.

En utrulling av brukereide enheter åpner for at brukerne kan sette opp og konfigurere sine egne enheter. Brukerne kan enten registrere enhetene i organisasjonens MDM-løsning for å få tilgang til bedriftsressurser, konfigurere innstillinger manuelt, installere en konfigurasjonsprofil eller installere bedriftsapper. Brukerne kan velge å registrere seg i organisasjonens MDM-løsning.

Brukerregistrering for personlige enheter tillater at en bedrifts ressurser og data kan håndteres sikkert, og på samme tid ivareta brukerens personvern, private opplysninger og apper. IT-administratorer kan kun iverksette spesifikke innstillinger, kontrollere at bedriftens regelverk følges, og kun fjerne bedriftens data og apper fra enheter uten å fjerne brukerens personlige data og apper.

Brukerregistrering inkluderer følgende:

- **Administrert Apple ID.** Brukerregistrering er integrert i administrert Apple-ID for å etablere en brukers identitet på enheten og gi tilgang til Apple-tjenester. Den administrerte Apple-ID-en kan brukes sammen med en personlig Apple ID som brukeren har logget på med. Administrerte Apple ID-er opprettes i Apple Business Manager og deles ut via forent autentisering til Microsoft Azure Active Directory.
- **Atskilte data.** Brukerregistrering oppretter et separat APFS-volum for administrerte kontoer, apper og data på enheten. Dette administrerte volumet er kryptografisk atskilt fra resten av enheten.
- **Kuratert håndtering for BYOD.** Brukerregistrering ble designet for brukereide enheter, slik at IT kan håndtere et undersett av konfigurasjoner og poliser og samtidig begrense enkelte håndteringsoppgaver, som å fjernslette enheten eller samle inn personlig informasjon.

Diagrammet nedenfor viser hvilke handlinger som må utføres av administratoren og brukeren i de enkelte trinnene i en utrulling av brukereide enheter.

	Administrator	Bruker
Forberedelse	• Evaluer infrastrukturen • Velg en MDM-løsning • Registrer deg I Apple Business Manager	• Bruk eventuelt personlig Apple ID og administrert Apple ID, App Store og iCloud-kontoer
Sett opp	• Angi enhetsinnstillinger • Distribuer apper og bøker	• Velg selskapets MDM-løsning • Last ned og installer apper og bøker
Rull ut	• Ingen administratorhandlinger er nødvendig	• Ingen brukerhandlinger er nødvendig
Administrer	• Administrer enheter • Rull ut og administrer ekstra innhold	• Finn flere apper som kan brukes

Finn ut mer om Brukerregistrering i MDM:
support.apple.com/guide/mdm

Finn ut mer om forent autentisering:
support.apple.com/guide/apple-business-manager

Utrullingstrinn

Denne delen gir en mer detaljert oversikt over de fire trinnene for utrulling av enheter og innhold: forberedelse av miljøet, oppsett, utrulling og administrasjon av enheter. Disse trinnene vil avhenge av hvorvidt organisasjonen eller brukeren eier enhetene.

1. Forbered

Når du har funnet riktig utrullingsmodell for organisasjonen, følger du disse trinnene for å legge fundamentet for utrullingen. Du kan gjennomføre disse tiltakene selv om du ikke har mottatt enhetene.

Evaluer infrastrukturen

iPhone og iPad kan integreres sømløst i de fleste standard IT-miljøer hos bedrifter. Det er viktig at du går gjennom den eksisterende infrastrukturen for å forsikre deg om at organisasjonen drar nytte av alle fordelene i iOS og iPadOS.

Wi-Fi og nettverk

Kontinuerlig og pålitelig tilgang til et trådløst nettverk er avgjørende når du skal sette opp og konfigurere iOS- og iPadOS-enheter. Kontroller at bedriftens Wi-Fi-nettverk kan støtte flere enheter som kobles til samtidig av alle brukerne. Du må kanskje konfigurere nettproxyen eller brannmurportene hvis enhetene ikke har tilgang til Apples aktiveringstjenere, iCloud eller App Store. Apple og Cisco har også optimalisert måten iPhone og iPad kommuniserer med et trådløst Cisco-nettverk på, og med det banet veien for andre avanserte nettverksfunksjoner, som rask roaming og Quality of Service (QoS) for apper.

Evaluer VPN-infrastrukturen for å forsikre deg om at brukerne kan få tilgang til lærestedets på en sikker måte fra en ekstern plassering via iOS- og iPadOS-enhetene. Vurder å bruke VPN On Demand eller Per App VPN i iOS og iPadOS, slik at det kun opprettes VPN-tilkobling ved behov. Hvis du har tenkt å bruke VPN per app, bør du kontrollere at VPN-portalene støtter disse funksjonene, og at du kjøper nok lisenser til å dekke alle brukerne og tilkoblingene.

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

Finn ut mer om Wi-Fi og nettverk:
support.apple.com/guide/deployment-reference-ios

Finn ut mer om Bonjour:
developer.apple.com/library

E-post, kontakter og kalendere

Hvis du bruker Microsoft Exchange, bør du kontrollere at ActiveSync-tjenesten er oppdatert og konfigurert slik at den støtter alle brukerne på nettverket. Hvis du bruker nettskybasert Office 365, bør du kontrollere at du har nok lisenser til alle iOS- og iPadOS-enhetene som skal kobles til. iOS og iPadOS har også støtte for den moderne autentiseringsteknologien i Office 365, som bruker OAuth 2.0 og flerfaktorautentisering. Hvis du ikke bruker Exchange, fungerer iPadOS og iOS også med standardbaserte tjenere som IMAP, POP, SMTP, CalDAV, CardDAV og LDAP.

Innholdsbufring

Innholdsbufring er en integrert funksjon i macOS High Sierra og nyere. Den lagrer en lokal kopi av innhold som etterspørres ofte fra Apples tjenere, noe som gjør at det brukes mindre båndbredde på å laste ned innhold til nettverket. Innholdsbufring gir raskere nedlasting og levering av programvare fra App Store, Mac App Store og Apple Books.

Denne funksjonen kan også bufre programvareoppdateringer for raskere nedlasting til iOS- og iPadOS-enheter. Innholdsbufring inkluderer også bufring med direkte tilkobling, som gjør at Mac kan dele en internettilkobling med flere iOS- og iPadOS-enheter via USB.

Finn ut mer om Innholdsbufring:
support.apple.com/guide/deployment-reference-macos

Mer om bufring med direkte tilkobling:
support.apple.com/HT207523

Velg en MDM-løsning

Apples administreringsrammeverk for iOS og iPadOS gjør at bedrifter kan registrere enheter på en trygg måte i bedriftsmiljøet, konfigurere og oppdatere innstillinger trådløst, overvåke samsvar med bedriftens regler, rulle ut apper og bøker samt utføre fjernsletting eller fjernlåsing av administrerte enheter. Disse administreringsfunksjonene aktiveres av MDM-løsninger fra tredjeparter.

Det finnes også en rekke tredjeparts MDM-løsninger som støtter ulike tjenerplattformer. Hver løsning har ulike administreringskonsoller, funksjoner og priser. Før du velger en løsning, bør du gå gjennom ressursene nedenfor for å evaluere hvilke administreringsfunksjoner som er mest relevante for organisasjonen. I tillegg til MDM-løsninger fra tredjeparter finnes det en Apple-løsning kalt Profile Manager, som er en funksjon i macOS Server.

Finn ut mer om håndtering av enheter og bedriftsdata:
apple.com/no/business/docs/resources/Managing_Devices_and_Corporate_Data_on_iOS.pdf

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: www.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 notariseres med din utvikler-ID for Gatekeeper, som hjelper med å beskytte macOS fra skadelig programvare.

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

2. Sett opp

I dette trinnet konfigurerer du enheter og distribuerer innholdet gjennom Apple Business Manager, en MDM-løsning eller eventuelt Apple Configurator 2. Oppsettet kan skje på flere måter, avhengig av hvem som eier enhetene, og hvilken utrullingstype du foretrekker.

Konfigurer enhetene

Det finnes flere tilgjengelige alternativer for konfigurering av brukertilgang til bedriftstjenester. IT-avdelingen kan sette opp enheter ved å distribuere konfigurasjonsprofiler. Det finnes flere konfigureringsvalg for enheter under tilsyn.

Konfigurering av enheter med MDM

Når enhetene er trygt registrert på en MDM-tjener, kan de administreres ved hjelp av konfigurasjonsprofiler – en XML-fil med konfigurasjonsinformasjon som sendes til en iOS- og iPadOS-enhet. Disse profilene automatiserer konfigureringen av innstillinger, kontoer, restriksjoner og påloggingsinformasjon. De kan også leveres trådløst fra MDM-løsningen din, noe som er ideelt for tilnærmet kontaktløs konfigurering av flere enheter samtidig. Profiler kan også sendes som e-postvedlegg, lastes ned fra en nettside eller installeres på enheter via Apple Configurator 2.

- **Organisasjonseide enheter.** Apple Business Manager åpner for automatisk registrering av brukernes enheter i MDM når enhetene aktiveres. Alle iOS- og iPadOS-enheter som er lagt til i Apple Business Manager, er kontinuerlig under tilsyn med obligatorisk MDM-registrering.
- **Brukereide enheter.** Ansatte kan selv velge om de vil registrere enhetene sine i MDM. Og hvis de vil melde enheten ut av MDM, fjerner de ganske enkelt konfigurasjonsprofilen fra enheten. Da blir også bedriftsdata og -innstillinger fjernet. Du bør imidlertid vurdere å ta i bruk insentiver, slik at brukere forblir administrert. Du kan for eksempel kreve at brukerne registrerer seg i MDM for å få tilgang til Wi-Fi-nettverket, ved å bruke MDM-løsningen til å levere påloggingsinformasjonen automatisk.

Når en enhet er registrert, kan en administrator starte MDM-regler, -valg eller -kommandoer. Håndteringsvalgene som er tilgjengelige for enhetene vil variere avhengig av tilsyns- og registreringsmetoden. Da mottar iOS- eller iPadOS-enheten en varsling om administratorens handling via Apples pushvarslingstjeneste (APNs), slik at den kan kommunisere direkte med MDM-tjeneren via en sikker tilkobling. Enheter med nettverkstilkobling kan motta APNs-kommandoer hvor som helst i verden. Det blir imidlertid ikke overført konfidensiell eller proprietær informasjon via Apples pushvarslingstjeneste.

Konfigurering av enheter med Apple Configurator 2 (valgfritt)

Organisasjoner kan bruke Apple Configurator 2 til lokale utrullinger av flere nye enheter. Med denne gratisappen for macOS kan du koble iOS- og iPadOS-enheter til en Mac via USB og oppdatere dem til siste versjon av iOS og iPadOS, angi innstillinger og restriksjoner på enhetene og installere apper og annet innhold. Når det første oppsettet er klart, kan du fortsette å administrere alt trådløst ved hjelp av MDM.

Brukergrensesnittet i Apple Configurator 2 fokuserer på enhetene dine og hver oppgave du vil utføre på dem. Appen integreres med Apple Business Manager, som gjør det mulig for enhetene å registreres automatisk i MDM ved å bruke organisasjonens innstillinger. Det er mulig å opprette tilpassede arbeidsflyter i Apple Configurator 2 ved hjelp av Blueprints for å kombinere atskilte oppgaver.

Mer om Apple Configurator 2:
support.apple.com/no-no/apple-configurator

Enheter under tilsyn
Med tilsyn får du flere administreringsmuligheter for iOS- og iPadOS-enheter som eies av organisasjonen, og kan angi restriksjoner som deaktivering av AirDrop eller låse enheten til én app. Det gir også muligheten til å aktivere et nettfilter via en global proxy for ting som å sikre at brukernes nettrafikk følger organisasjonens retningslinjer, for å forhindre at brukerne tilbakestiller enhetene til fabrikkinnstillingene, og mye mer. iOS- og iPadOS-enheter er som standard ikke under tilsyn. Du kan bruke Apple Business Manager til å aktivere tilsyn, eller du kan aktivere tilsyn manuelt ved hjelp av Apple Configurator 2.

Selv om du ikke har planer om å bruke noen av funksjonene som kun gjelder for enheter under tilsyn, bør du vurdere å sette enhetene under tilsyn når du setter dem opp, slik at du i fremtiden kan benytte deg av funksjoner som kun er for enheter under tilsyn. Ellers må du slette enheter som er rullet ut. Tilsyn handler ikke om å stenge en enhet, snarere tvert imot. Det forbedrer bedriftseide enheter ved at administreringsmulighetene utvides. På sikt gir tilsyn bedriften flere valgmuligheter.

Finn ut mer om begrensninger for enheter under tilsyn:
support.apple.com/guide/mdm

Distribuer apper og bøker

Apple tilbyr omfattende programmer som gjør det enklere for organisasjonen å dra nytte av appene og innholdet som er tilgjengelig for iOS og iPadOS. Med disse mulighetene kan du distribuere apper og bøker som er kjøpt gjennom Apple Business Manager eller utviklet internt, til enheter og brukere, slik at brukerne har alt de trenger for å arbeide effektivt. Når du gjør et kjøp, må du velge distribusjonsmetode: administrert distribusjon eller innløsingskoder.

Administrert distribusjon

Med administrert distribusjon bruker du MDM-løsningen eller Apple Configurator 2 til å administrere apper og bøker som er kjøpt i Apple Business Manager i landene der appen er tilgjengelig. Hvis du vil aktivere administrert distribusjon, kobler du først sammen MDM-løsningen med VPP-kontoen ved hjelp av et sikkert kjennetegn. Når du er tilkoblet MDM-tjeneren, kan du tilordne apper og bøker i Apple Business Manager selv om App Store er deaktivert på enheten.

- **Tilordne apper til enhetene.** Bruk MDM-løsningen eller Apple Configurator 2 til å tilordne apper direkte til enheter. Denne metoden sparer flere trinn i den første utrullingen, slik at utrullingen blir betydelig enklere og raskere. Du får full kontroll over administrerte enheter og innhold. Når en app har blitt tilordnet til en enhet, blir appen sendt til enheten via MDM, og det kreves ingen invitasjon. Alle som bruker enheten, har tilgang til appen.
- **Tilordne apper og bøker til brukere.** En alternativ metode er å bruke MDM-løsningen til å sende brukerne en e-post eller pushvarsling med invitasjon om å laste ned apper og bøker. Brukerne godkjenner invitasjonen ved å logge på med en personlig Apple ID på sine egne enheter. Apple ID-en registreres i Apple Business Manager-tjenesten, men forblir privat og er ikke synlig for administratoren. Når brukere godtar invitasjonen, kobles de til MDM-tjeneren, slik at de kan begynne å motta apper og bøker. Apper er automatisk tilgjengelige for nedlasting på alle brukerens enheter, uten ekstra arbeid eller kostnad.

Når en bruker eller enhet ikke lenger har behov for en tilordnet app, kan du tilbakekalle appen og gjøre den tilgjengelig for en annen bruker eller enhet. Organisasjonen beholder altså fullt eierskap til appene. Distribuerte bøker er mottakerens eiendel og kan ikke kalles tilbake eller tilordnes på nytt.

Innløsingskoder

Du kan også distribuere innhold med innløsingskoder. Dette er nyttig når organisasjonen din ikke kan bruke MDM på sluttbrukerens enhet, for eksempel i en franchise-bedrift. Med denne metoden overføres en app eller bok permanent til brukeren som innløser koden. Innløsingskoder leveres i regnearkformat. Alle apper og bøker du kjøper, har en unik kode. Hver gang en kode løses inn, oppdateres regnearket i Apple Business Manager-butikken, slik at du alltid kan se hvor mange koder som er løst inn. Distribuer kodene med MDM, Apple Configurator 2, e-post eller et internt nettsted.

Installering av apper og innhold med Apple Configurator 2 (valgfritt)
I tillegg til grunnleggende oppsett og konfigurering kan Apple Configurator 2 også brukes til å installere apper og innhold for enheter du vil sette opp på vegne av brukeren. Ved utrulling av enheter som kan tilpasses personlig, kan du installere apper på forhånd og spare både tid og båndbredde. Når du skal rulle ut enheter som ikke kan tilpasses personlig, kan du sette opp alt på enhetene – selv Hjem-skjermen. Når du konfigurerer enheter med Apple Configurator 2, kan du installere App Store-apper, interne apper og dokumenter. App Store-apper krever Apple Business Manager. Dokumenter er tilgjengelige for apper som støtter fildeling. Når du vil gå gjennom eller hente dokumenter fra iOS- og iPadOS-enheter, kobler du dem til en Mac som har Apple Configurator 2.

3. Rull ut

iPhone og iPad gjør det enkelt for ansatte å klargjøre enhetene straks de pakker dem ut, uten at de trenger hjelp fra IT-avdelingen.

Distribuer enhetene

Når klargjøringen og oppsettet av enhetene i de to første trinnene er utført, er enhetene klare til å distribueres. Hvis utrullingen tillater personlig tilpassing, kan brukerne selv tilpasse enhetene og fullføre oppsettet ved hjelp av den effektive oppsettassistenten. Hvis utrullingen ikke tillater personlig tilpassing, distribuerer du enheter til de skiftansatte eller plasserer enheter i kiosker som laget for å lade og sikre dem.

Oppsettassistent
Med Oppsettassistent kan brukerne aktivere enhetene, konfigurere grunnleggende innstillinger og begynne å jobbe straks de har pakket enhetene ut av esken. Etter det første oppsettet kan brukeren også angi personlige innstillinger for elementer som språk, sted, Siri, iCloud og Finn iPhone. Enheter som er registrert i Apple Business Manager, registreres automatisk i MDM i selve oppsettassistenten.

Tillat at brukerne tilpasser enhetene
Ved utrullinger med mulighet for personlig tilpassing og BYOD-utrullinger økes produktiviteten når brukerne kan tilpasse enhetene med sin egen Apple ID, fordi brukerne velger appene og innholdet som gjør dem best i stand til å utføre arbeidet og nå målene.

Apple ID og administrert Apple ID
Når ansatte bruker en Apple ID til å logge seg på Apple-tjenester som FaceTime, iMessage, App Store og iCloud, har de tilgang til et stort innholdsutvalg for å effektivisere bedriftsoppgaver, øke produktiviteten og fremme samarbeid.

I likhet med vanlige Apple ID-er brukes administrerte Apple ID-er også til å logge på en personlig enhet: De brukes også til å få tilgang til Apple-tjenester – inkludert 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 organisasjonen din. Dette gjelder for ting som 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 valgfri, personlig Apple ID; andre registreringsvalg støtter enten en personlig Apple ID eller en administrert Apple ID. Det er kun Brukerregistrering som støtter flere Apple ID-er.

For å få størst mulig utbytte av disse tjenestene, bør brukere bruke sin egne Apple ID-er eller administrerte Apple ID-er som lages 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/apple-business-manager

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 Hvor er? 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 organisasjoner mer kontroll over hvilke data som arkiveres på hvilke kontoer.

Finn ut mer om administrering av iCloud:
support.apple.com/guide/deployment-reference-ios

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 enhetene

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

Spørringer

En MDM-tjener kan innhente forskjellig informasjon fra enheter, inkludert maskinvareinformasjon som serienummer, enhets-UDID eller Wi-Fi MAC-adresse, samt programvareinformasjon, for eksempel iOS- eller iPadOS-versjon og en detaljert liste over alle appene som er installert på enheten. Denne informasjonen kan brukes av MDM-løsningen til å holde informasjon om enhetsbeholdningen oppdatert, ta informerte administrasjonsavgjørelser og automatisere administrasjonsoppgaver, for eksempel å sørge for at brukerne oppdaterer appene sine.

Administreringsoppgaver

Når en enhet administreres, kan en MDM-tjener utføre en rekke ulike administrative oppgaver, for eksempel endre konfigurasjonsinnstillingene automatisk uten brukermedvirkning, utføre en programvareoppdatering på kodelåste enheter, fjernlåse eller fjernslette en enhet, eller fjerne kodelåsen, slik at brukerne kan tilbakestille passord de har glemt. En MDM-tjener kan be en iPhone eller iPad om å opprette Skjermbilde over AirPlay med en bestemt destinasjon, eller om å avslutte en pågående AirPlay-økt.

Administrerte programvareoppdateringer

Du kan forhindre trådløs, manuell oppdatering av enheter under tilsyn for en bestemt periode. Når du angir en slik restriksjon, er standardvarigheten for slike utsettelser 30 dager, og den utløses når Apple lanserer en iOS- eller iPadOS-oppdatering. Du kan imidlertid velge hvor mange dager du vil forhindre oppdateringer, fra én til 90 dager. Det er også mulig å forhåndsprogrammere programvareoppdateringer på enheter under tilsyn ved hjelp av MDM-løsningen.

Mistet-modus

MDM-løsningen kan eksternt sette en enhet som er under tilsyn, i Mistet-modus. Handlingen låser enheten og viser en melding med et telefonnummer på låst skjerm. I Mistet-modus kan enheter under tilsyn som mistes eller blir stjålet, lokaliseres ved hjelp av forrige registrerte posisjon på MDM-tjeneren. Mistet-modus krever ikke at Finn iPhone er aktivert.

Aktiveringslås

I iOS 7.1 og nyere kan du bruke MDM til å aktivere Aktiveringslås når en bruker slår på Hvor er? på en enhet under tilsyn. Da kan organisasjonen dra nytte av tyverisikringsfunksjonaliteten til Aktiveringslås, samtidig som det er mulig å overstyre funksjonen hvis en bruker ikke kan logge på med Apple ID-en sin.

Rull ut og administrer ekstra innhold

Organisasjoner må ofte distribuere apper for at brukerne skal kunne jobbe produktivt. Samtidig må organisasjonene kontrollere hvordan apper kobles til interne ressurser, og hvordan datasikkerheten håndteres når en bruker forlater organisasjonen. Og alt skal fungere side om side med brukerens personlige apper og data.

Intern portal for apper

De fleste MDM-tjenere tilbyr portaler for interne apper som en del av løsningen. Du kan skape din egen portal for interne apper for de ansatte, hvor de enkelt kan finne apper til iPhone eller iPad. Interne apper, apper fra App Store URL-er, Apple Business Manager-koder eller tilpassede apper kan knyttes til denne portalen, slik at brukerne finner alt på ett sted. Du kan administrere og sikre dette stedet sentralt. Med en portal for interne apper kan de ansatte enkelt finne godkjente ressurser uten at de må kontakte IT-avdelingen.

Administrert innhold

Administrert innhold omfatter installering, konfigurering, administrering og fjerning av App Store-apper og tilpassede interne apper, kontoer, bøker og dokumenter.

- **Administrerte apper.** I iOS og iPadOS kan en organisasjon bruke administrerte apper til å rulle ut gratis-, betalings- og bedriftsapper trådløst via MDM, med riktig balanse mellom beskyttelse av bedriftsdata og respekt for brukerens personvern. Administrerte apper kan fjernes eksternt av en MDM-tjener eller når brukeren fjerner enheten fra MDM. Når en app blir fjernet, fjernes også dataene som er tilknyttet appen. Hvis en app fortsatt er tilordnet en bruker gjennom Apple Business Manager, eller hvis en bruker har løst inn en appkode med en personlig Apple ID, kan appen lastes ned på nytt fra App Store, men den vil ikke lenger være administrert av MDM.
- **Administrerte kontoer.** MDM kan hjelpe brukerne med å komme raskt i gang ved å sette opp e-post og andre kontoer automatisk. Avhengig av MDM-leverandøren og integreringen med de interne systemene kan nyttelaster for kontoer også forhåndsutfylles med brukernavn, e-postadresse og eventuelt sertifikatidentiteter for autentisering og signering.
- **Administrerte bøker og dokumenter.** MDM-verktøy, bøker, ePub-bøker og PDF-dokumenter kan sendes automatisk til brukernes enheter, slik at de ansatte alltid har det de trenger. Samtidig kan administrerte bøker kun deles med andre administrerte apper eller sendes med e-post ved hjelp av administrerte kontoer. Materialet kan slettes eksternt når det ikke er behov for det lenger. Bøker som kjøpes gjennom Apple Business Manager, kan distribueres gjennom administrert bokdistribusjon, men de kan ikke tilbakekalles og tilordnes på nytt. En bok som brukeren allerede har kjøpt, kan ikke administreres med mindre boken uttrykkelig er tilordnet brukeren gjennom Apple Business Manager.

Administrert appkonfigurasjon

Apputviklere kan angi innstillinger og funksjonalitet som kan aktiveres når appen installeres som en administrert app. Installer disse konfigurasjonsinnstillingene før eller etter installering av den administrerte appen. IT-administratorer kan for eksempel etablere et sett med standardpreferanser for en SharePoint-app, slik at brukerne slipper å konfigurere tjenerinnstillingene manuelt.

Ledende leverandører av MDM-løsninger har opprettet forumet AppConfig Community og laget et standardoppsett som alle apputviklere kan bruke, som en støtte til administrert appkonfigurasjon. AppConfig Community jobber for å utarbeide verktøy og mønsterpraksiser for funksjoner som er spesialutviklet for mobiloperativsystemer. Forumet bidrar til en mer ensartet, åpen og enkel måte å konfigurere og sikre mobilapper på, for at flere bedrifter skal ta i bruk mobilløsninger.

Mer om AppConfig-samfunnet:
appconfig.org

Administrert dataflyt

MDM-løsninger inneholder spesifikke funksjoner som gjør det mulig å administrere bedriftsdata på detaljnivå og forhindre at informasjon lekker ut til brukerens personlige apper eller nettskytjenester.

- **Managed Open In.** Managed Open In bruker restriksjoner som hindrer at vedlegg eller dokumenter fra administrerte kilder kan åpnes på uadministrerte plasseringer og omvendt. Du kan for eksempel hindre at et konfidensielt e-postvedlegg i organisasjonens administrerte e-postkonto åpnes i en av brukerens personlige apper. Jobbdokumentet kan kun åpnes i apper som er installert og administrert av MDM. Brukerens uadministrerte, personlige apper vises ikke i listen over apper som vedlegget kan åpnes i. I tillegg til administrerte apper, kontoer, bøker og domener gjelder Managed Open In-restriksjoner også for mange tillegg.
- **Lås enheten til én app.** Denne innstillingen begrenser iOS- eller iPadOS-enheten til én enkelt app og er ideell for kiosker eller enheter som brukes til kun ett formål, for eksempel en enhet som brukes til betaling i butikk eller innsjekking ved et sykehus. Utviklere kan også aktivere denne funksjonaliteten i appene, slik at appene uavhengig av hverandre kan gå inn i og ut av modusen som låser enheten til én app.
- **Forhindre sikkerhetskopiering.** Restriksjonen forhindrer sikkerhetskopiering av administrerte apper til iCloud eller en datamaskin. Når sikkerhetskopiering ikke tillates, kan heller ikke dataene i en administrert app gjenopprettes hvis appen fjernes via MDM, men brukeren installerer den på nytt.

Supportalternativer

Apple tilbyr en rekke programmer og supportalternativer for iOS- og iPadOS-brukere og IT-administratorer.

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 over telefon døgnet rundt, med én times svartid for høyt prioriterte problemer. Programmet yter support på linje med IT-avdelingen for all Apple-maskinvare og -programvare, i tillegg til støtte for avanserte utrullings- og integreringsscenarioer, inkludert MDM og Active Directory.

AppleCare OS Support

Med AppleCare OS Support får IT-avdelingen telefon- eller e-postbasert support på bedriftsnivå for iOS- og iPadOS-, macOS- og macOS Server-utrullinger. Det har support tilgjengelig opptil 24 timer i døgnet, 7 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 bedrifter 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 for brukere med iOS- og iPadOS-enheter

Alle iOS- og iPadOS-enheter leveres med en begrenset garanti på ett år og kostnadsfri teknisk telefonsupport i 90 dager etter kjøpet. Servicedekningen kan utvides til to år fra kjøpsdato med AppleCare+ for iPhone, AppleCare+ for iPad eller AppleCare+ for iPod touch. Hvis du har spørsmål, kan du ringe Apples tekniske support så ofte du vil. Apple tilbyr også praktiske serviceløsninger når enhetene må repareres. I tillegg tilbyr programmene dekning for opptil to tilfeller av skade som følge av uhell, mot et servicetillegg for hvert tilfelle.

iOS Direct Service Program

En fordel ved AppleCare+ er iOS Direct Service Program (programmet for direkte iOS-service), som gjør at din interne supportavdeling kan kontrollere enheter for feil uten å måtte kontakte AppleCare eller oppsøke en Apple Store. Ved behov kan bedriften bestille erstatningsenheter av iPhone, iPad, iPod touch eller tilbehør direkte.

Finn ut mer om AppleCare-programmene:
apple.com/no/support/professional

Oppsummering

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

Mer om utrulling, administrering og sikkerhetsfunksjoner i OS og iPadOS:
support.apple.com/guide/deployment-reference-ios

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-plattformsikkerhet:
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