Administrere enheter og bedriftsdata i iOS

Innhold

Oversikt

Bedrifter over hele verden utruster sine ansatte med iPhone og iPad.

Nøkkelen til en vellykket mobilstrategi er å finne balansen mellom IT-kontroll og brukermuligheter. Når brukerne kan tilpasse iOS-enhetene med egne apper og eget innhold, tar de større eierskap og ansvar, og både engasjementet og produktiviteten øker. Dette støttes av Apples rammeverk for administrering. Bedriftsdata og apper kan administreres smart og diskret, og bedriftsdata holdes atskilt fra personlige data på en smidig måte. Dessuten forstår brukerne hvordan enhetene deres administreres, og de kan derfor føle seg trygge på at personlige data beskyttes.

Dette dokumentet forklarer hvordan viktig IT-kontroll kan opprettholdes samtidig som brukerne utstyres med de beste verktøyene for jobben. Det utfyller iOS – Håndbok for utrulling, som er en omfattende nettbasert teknisk håndbok om utrulling og administrasjon av iOS-enheter i bedriften.

iOS – Håndbok for utrulling: help.apple.com/deployment/ios.

Grunnleggende om administrering

Med iOS kan du effektivisere utrullingen av iPhone og iPad med en rekke innebygde løsninger for enkelt kontooppsett, og du kan konfigurere retningslinjer, distribuere apper og angi enhetsrestriksjoner trådløst.

Vår administreringsløsning

Apples rammeverk for administrering danner grunnlaget for å administrere mobile enheter. Rammeverket er bygd inn i iOS, slik at organisasjoner kan administrere det de må – med enkle grep – uten at de må slå av funksjoner eller deaktivere funksjonalitet. Apples rammeverk for administrering og en MDM-løsning fra en tredjepart gir dermed detaljert og presis kontroll over enheter, apper og data. Og det viktigste av alt er at du får den kontrollen du trenger, uten at det går ut over brukerens opplevelse eller personlige data.

Andre administreringsmetoder på markedet kan bruke andre betegnelser for MDM-funksjonalitet – som EMM (Enterprise Mobility Management) eller MAM (Mobile Application Management). Formålet er det samme – å administrere organisasjonens enheter og bedriftens data trådløst. Og siden Apples rammeverk for administrering er innebygd i iOS, trenger du ikke et eget agentprogram fra MDM-leverandøren.

Skille mellom bedriftens data og personlige data

Enten det er brukeren eller bedriften som eier enhetene, kan kravene til IT-administrering oppfylles samtidig som brukerne kan jobbe mest mulig produktivt. Bedriftens data og personlige data administreres hver for seg, uten at det går ut over brukeropplevelsen. Brukeren kan ha den nyeste og beste produktivitetsappen rett ved siden av bedriftsappene på enheten sin og står fritt til å jobbe slik hun eller han vil. Med iOS er dette mulig uten bruk av tredjepartsløsninger som avgrensede arbeidsområder, som kan gi en dårligere brukeropplevelse og skape frustrasjon.

Forstå ulike administreringsmodeller

Avgrensede arbeidsområder er utviklet for å løse problemer på andre plattformer – problemer som ikke finnes i iOS. Noen avgrensede arbeidsområder er basert på doble identiteter, hvor to separate miljøer kjøres på samme enhet. I andre isoleres appene eller plasseres i egne områder ved hjelp av kodebasert integrering. Alle disse metodene går ut over produktiviteten – enten brukerne må logge seg av og på flere arbeidsområder eller bruke kode som fører til at appen ofte ikke er kompatibel med oppdateringer av operativsystemet.

Organisasjoner som har sluttet å bruke avgrensede arbeidsområder, ser at de spesialutviklede administreringskontrollene i iOS gir en bedre brukeropplevelse og økt produktivitet. I stedet for å gjøre det vanskelig for brukerne å benytte samme enhet på jobben og privat, kan du angi regler som styrer datastrømmen sømløst og umerkelig.

Administrere bedriftsdata

Med iOS trenger du ikke å deaktivere funksjonalitet på enhetene. Nøkkelteknologier styrer strømmen av bedriftens data mellom apper og forhindrer at dataene lekker ut til brukerens personlige apper eller nettskytjenester.

Administrert innhold

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

- **Administrerte apper.** Apper som er installert med MDM, kalles administrerte apper. Dette kan enten være apper som lastes ned gratis eller kjøpes fra App Store, eller det kan være tilpassede interne apper, og de kan alle installeres trådløst med MDM. Administrerte apper inneholder ofte sensitive opplysninger og gir bedre kontroll enn apper som brukeren laster ned selv. MDM-tjeneren kan fjerne administrerte apper og tilknyttede data ved behov eller angi om appene skal fjernes når MDM-profilen fjernes. MDM-tjeneren kan hindre at administrerte apper sikkerhetskopieres til iTunes og iCloud.
- **Administrerte kontoer.** MDM kan hjelpe brukerne med å komme raskt i gang ved at e-post og andre kontoer klargjøres automatisk. Avhengig av MDM-leverandøren og integreringen med de interne systemene kan konfigurasjoner også forhåndsutfylles med brukernavn, e-postadresse og eventuelt sertifikatidentiteter for autentisering og signering. MDM kan konfigurere følgende kontotyper: IMAP/POP, CalDAV, kalenderabonnementer, CardDAV, Exchange ActiveSync og LDAP.
- **Administrerte bøker.** Ved hjelp av MDM kan bøker, ePub-bøker og PDF-dokumenter sendes automatisk til brukernes enheter via push, slik at de ansatte alltid har det de trenger. Administrerte bøker kan bare deles med andre administrerte apper eller sendes med e-post fra administrerte kontoer. Innholdet kan fjernslettes når det ikke lenger er behov for det.

- **Administrerte domener.** Dokumenter som lastes ned fra Safari, regnes som administrerte hvis de kommer fra et administrert domene. Spesifikke URL-er og underdomener kan administreres. Hvis en bruker for eksempel laster ned en PDF fra et administrert domene, krever domenet at PDF-en samsvarer med alle innstillingene for administrerte dokumenter. Baner som følger domenet, administreres som standard.

Administrert distribusjon

Administrert distribusjon gjør at du kan bruke MDM-løsningen eller Apple Configurator 2 til å administrere apper og bøker du har kjøpt via voluminnkjøpsprogrammet (VPP). Hvis du vil aktivere administrert distribusjon, må du først koble MDM-løsningen til VPP-kontoen med et sikkerhetskjennetegn. Når MDM-tjeneren er tilkoblet VPP, kan du tilordne apper direkte til en enhet uten at brukeren må ha en Apple ID. Brukeren blir varslet når apper er klare til å installeres på enheten. Hvis en enhet er under tilsyn, overføres apper til enheten via push uten at brukeren varsles.

Vil du ha full kontroll over apper i en MDM-løsning, tilordner du apper direkte til en enhet.

Administrert appkonfigurasjon

Med administrert appkonfigurasjon bruker MDM det spesialutviklede iOS-rammeverket for administrering til å konfigurere apper under eller etter utrulling. Med dette rammeverket kan utviklerne se hvilke konfigurasjonsinnstillinger som bør implementeres når appen installeres som en administrert app. Når apper er konfigurert på denne måten, kan de ansatte begynne å bruke dem med en gang uten å måtte sette opp noe selv. IT-administratoren er trygg på at bedriftens data håndteres på en sikker måte, og det er ikke behov for å bruke egne SDK-er eller å pakke inn apper.

Funksjoner som er tilgjengelige for apputviklere, kan aktiveres – for eksempel for å konfigurere apper, hindre sikkerhetskopiering av apper, deaktivere skjermbilder og fjernslette apper.

AppConfig Community jobber for å utarbeide verktøy og mønsterpraksiser for funksjoner som er spesialutviklet for mobilplattformer. Her har ledende leverandører av MDM-løsninger laget en standardplan som alle apputviklere kan bruke for å støtte konfigurasjon av administrerte apper. Ved å tilby en enklere, åpnere og mer enhetlig måte å konfigurere og sikre mobilapper på bidrar organisasjonen til å fremme bruken av mobile løsninger i bedrifter.

Du finner mer informasjon om AppConfig Community på www.appconfig.org.

Administrert dataflyt

MDM-løsninger inneholder spesifikke funksjoner for administrering av bedriftsdata på detaljnivå, slik at dataene ikke lekker ut til brukernes personlige apper eller skytjenester.

- **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.

For å beskytte bedriftens data vil kun apper som er installert og administrert av MDM, kunne åpne dette jobbdokumentet.

- **Administrerte tillegg.** Tredjepartsutviklere kan bruke apptillegg til å bygge inn funksjonalitet i andre apper – og til og med i sentrale iOS-systemer som Varslingssenter. Det åpner for nye arbeidsflyter mellom apper. Managed Open In sørger for at funksjonalitet i uadministrerte tillegg ikke kan kommunisere med administrerte apper. Følgende eksempler viser ulike typer tillegg:
  - **Tillegg for dokumentutveksling** gjør det mulig for produktivitetsapper å åpne dokumenter fra en rekke forskjellige nettskytjenester uten å opprette unødvendige kopier.
  - **Handlingstillegg** gjør det mulig for brukere å manipulere eller vise innhold i en annen app. Brukerne kan for eksempel benytte en handling til å oversette tekst på et annet språk direkte i Safari.
  - **Tillegg for tilpassede tastaturer** gir støtte for andre tastaturer enn dem som allerede er innebygd i iOS. Managed Open In kan hindre at uautoriserte tastaturer vises i bedriftsappene.
  - **I dag-tillegg**, som også kalles widgeter, brukes til å levere oversiktlig informasjon til I dag-visningen i Varslingssenter. Det gir brukerne en glimrende måte å få umiddelbar og oppdatert informasjon fra en app på, med forenklet kommunikasjon som går inn i appen for mer informasjon.
  - **Tillegg for deling** gir brukerne en praktisk måte å dele innhold på, som på sosiale nettsteder eller via opplastingstjenester. I en app med en delingsknapp kan brukerne for eksempel velge et tillegg for deling på et sosialt nettsted, og deretter bruke dette til å legge ut kommentarer eller annet innhold på nettstedet.

Fleksible administreringsvalg

Apples rammeverk for administrering er fleksibelt og skaper en god balanse i administreringen av brukereide så vel som bedriftseide enheter. Kombinasjonen av iOS og en MDM-løsning fra en tredjepart gjør at du kan velge mellom alt fra svært åpne metoder til detaljert styring.

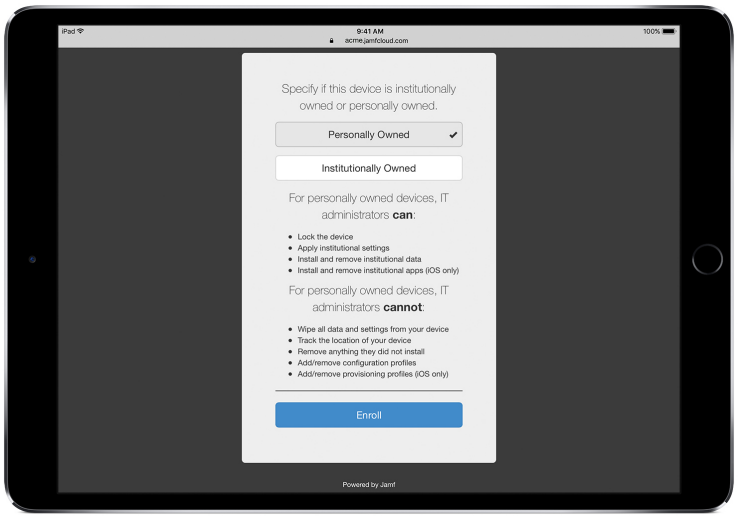
Eierskapsmodeller

Enheter og apper administreres på forskjellige måter avhengig av eierskapsmodellen – eller -modellene – i organisasjonen. De to eierskapsmodellene som bedrifter vanligvis bruker for iOS-enheter, er bedriftseid og brukereid.

Brukereide enheter

Ved utrulling av brukereide enheter med iOS kan brukerne ha personlige oppsett på enhetene, de kan se hvordan enhetene konfigureres, og de kan være trygge på at bedriften ikke har tilgang til personlige data.

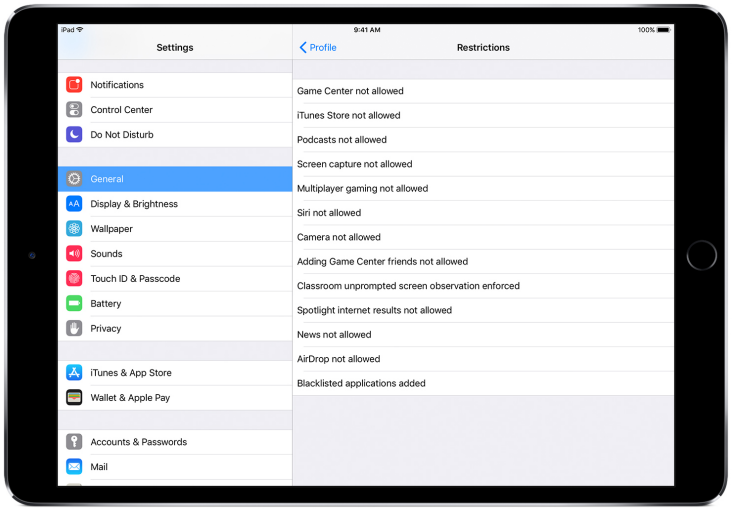
- **Valgfri registrering.** Når enheter kjøpes og klargjøres av brukeren – en modell kalt BYOD («bring your own device») – kan du likevel gi tilgang til bedriftstjenester som Wi-Fi, e-post og kalender. Brukerne kan ganske enkelt velge å registrere seg i organisasjonens MDM-løsning. Første gang brukerne registrerer seg i MDM på en iOS-enhet, får de informasjon om hva MDM-tjeneren har tilgang til på enheten deres, og hvilke funksjoner som blir konfigurert. Slik vet alle hva som administreres, og det skaper tillit mellom deg og brukerne. Det er viktig å fortelle brukerne at de når som helst kan fjerne administreringsprofilen fra enheten sin dersom de ikke ønsker å være registrert. Når de gjør det, fjernes alle bedriftskontoer og apper som er installert med MDM.



MDM-løsninger fra tredjeparter har gjerne et brukervennlig grensesnitt som gjør det enkelt for ansatte å registrere seg.*

*Skjermbilde fra Jamf.

- **Større åpenhet.** Når brukerne er registrert i MDM, kan de enkelt gå til Innstillinger for å se hvilke apper, bøker og kontoer som administreres, og hvilke restriksjoner som er implementert. Alle bedriftsinnstillinger, -kontoer og -apper som er installert via MDM, flagges som «administrert» i iOS.



I brukergrensesnittet for konfigurasjonsprofiler i Innstillinger kan brukerne se nøyaktig hva som er konfigurert på enheten deres.

- **Personvern.** Selv om du kan administrere iOS-enheter med en MDM-tjener, er det ikke alle innstillinger eller all kontoinformasjon som er tilgjengelig. Du kan administrere bedriftskontoer, bedriftsinnstillinger og informasjon som er lagt til via MDM, men du har ikke tilgang til brukerens personlige kontoer. De samme funksjonene som holder dataene sikre i bedriftsadministrerte apper, sørger for å holde brukerens personlige innhold utenfor bedriftens datastrøm.

  Følgende eksempler viser hva MDM-tjeneren fra en tredjepart kan og ikke kan se på en privat iOS-enhet:

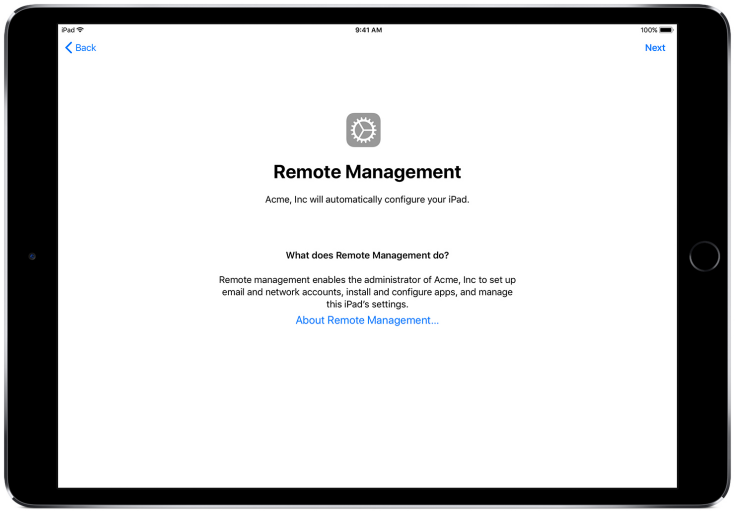
MDM ser:	**MDM ser ikke personlig data, som:**
enhetsnavn	personlige eller jobbrelaterte e-poster, kalendere og kontakter
telefonnummer	SMS-er eller iMessage-meldinger
serienummer	historikk fra Safari
modellnavn og -nummer	logger fra FaceTime eller samtaler
kapasitet og ledig plass	personlige påminnelser og notater
iOS-versjonsnummer	hvor ofte appene brukes
installerte apper	enhets- plassering

- **Tilpasse enheter.** Bedrifter har oppdaget at når brukerne kan tilpasse enheten med sin egen Apple ID, føler de større eierskap til enheten og tar større ansvar for den. Dessuten øker produktiviteten fordi de selv kan velge hvilke apper og hvilket innhold de vil arbeide med.

Bedriftseide enheter

I en utrulling av bedriftseide enheter kan du enten gi hver bruker en enhet som kun benyttes av den enkelte, eller du kan gi de ansatte tilgang til ikke-personlige enheter som de veksler på å bruke. iOS-funksjoner som automatisk registrering, låsbare MDM-innstillinger, tilsyn av enheter og Always-on VPN sikrer at enheter konfigureres i henhold til organisasjonens retningslinjer. Det gir økt kontroll og bidrar til å beskytte bedriftens data.

- **Automatisk registrering.** Med programmet for enhetsregistrering (DEP) kan du automatisere MDM-registrering i den første klargjøringen av iPhoner, iPader og Macer som organisasjonen eier. Du kan gjøre registreringen obligatorisk og ikke-slettbar. Du kan også sette enheter i tilsynsmodus under registreringen, og du kan dessuten la brukerne hoppe over enkelte trinn i oppsettsprosessen.



Med DEP vil MDM-løsningen konfigurere iOS-enhetene i oppsettassistenten automatisk.

- **Enheter under tilsyn.** Tilsyn gir organisasjonen flere muligheter til å administrere bedriftseide iOS-enheter. Bedriften kan for eksempel aktivere et nettfilter via en global proxy for å sikre at brukernes nettrafikk samsvarer med organisasjonens retningslinjer, hindre brukerne i å tilbakestille enheten til fabrikkinnstillingene og mye annet. Tilsynsmodus er ikke aktivert på iOS-enheter som standard. Du kan bruke DEP til å aktivere tilsynsmodus, eller du kan aktivere tilsyn manuelt ved hjelp av Apple Configurator 2.

Selv om du ikke har planer om å bruke noen tilsynsfunksjoner nå, bør du vurdere å aktivere tilsynsmodus i oppsettet, slik at du kan benytte funksjonene senere. Ellers vil du måtte slette enheter som allerede er rullet ut. Tilsyn handler ikke om å blokkere funksjoner på en enhet – det handler mer om å forbedre bedriftseide enheter ved å utvide administreringsfunksjonene. På sikt gir tilsyn bedriften flere valgmuligheter.

Du finner en fullstendig oversikt over tilsynsinnstillinger på iOS – Håndbok for utrulling.

Begrensninger

iOS støtter følgende typer restriksjoner som du kan konfigurere trådløst i henhold til organisasjonens behov – uten at det går ut over brukeropplevelsen:

- AirPrint
- Appinstallering
- Bruk av apper
- Klasserom-appen
- Enhet
- iCloud
- Restriksjoner for brukere og brukergrupper i Profile Manager

- Safari
- Sikkerhets- og personverninnstillinger
- Siri

De to følgende kategoriene har også funksjoner som kan konfigureres av MDM-løsningen:

- Automatiserte innstillinger for MDM-registrering
- Oppsettassistent

Flere administreringsfunksjoner

Sende spørringer til enheter

I tillegg til å konfigurere enheter kan en MDM-tjener innhente informasjon fra enheter, blant annet opplysninger om enheten, nettverket, apper, samsvar og sikkerhet. Denne informasjonen bidrar til å sikre at enhetene fortsatt tilfredsstiller nødvendige regler. MDM-tjeneren bestemmer hvor ofte den samler inn informasjon.

Følgende er informasjon som kan innhentes fra en iOS-enhet:

- Opplysninger om enheten (navn)
- Modell, iOS-versjon, serienummer
- Nettverksinformasjon
- Roaming-status, MAC-adresser
- Installerte apper
- App-navn, versjon, størrelse
- Informasjon om samsvar og sikkerhet
- Installerte innstillinger, retningslinjer og sertifikater
- Krypteringsstatus

Administreringsoppgaver

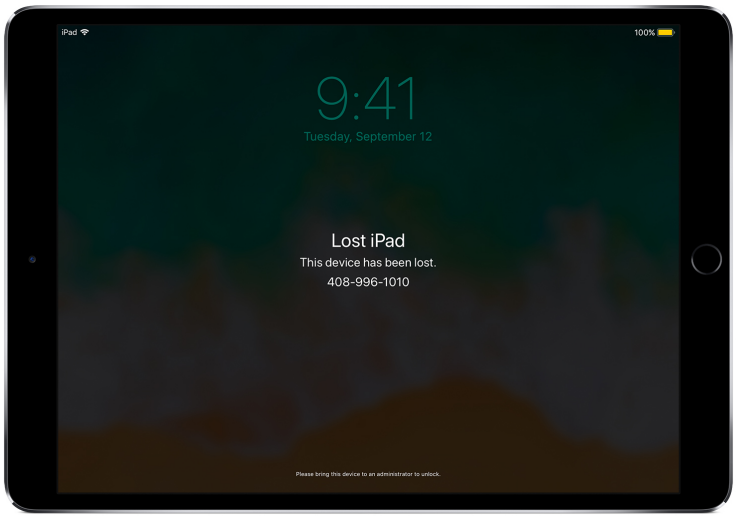
Når en enhet administreres, kan en MDM-tjener utføre en rekke ulike administrative oppgaver, for eksempel endre konfigurasjonsinnstillingene automatisk uten brukermedvirkning, utføre iOS-oppdatering på kodelåste enheter, låse eller slette en enhet eksternt, eller fjerne kodelåsen slik at brukerne kan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

Mistet-modus

I iOS 9.3 eller nyere kan enheter der tilsyn er aktivert, fjernplasseres i Mistet-modus via MDM-løsningen. 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 MDM-tjenere og enhetens stedsplassering forrige gang de var på nettet. Mistet-modus krever ikke at Finn iPhone er aktivert.

Hvis MDM deaktiverer Mistet-modus eksternt, låses enheten opp, og det innhentes informasjon om plasseringen. Brukeren blir varslet når Mistet-modus slås av.



Hvis en enhet er kommet på avveier og MDM setter den i Mistet-modus, låses enheten, slik at meldinger kan vises på skjermen og enheten kan lokaliseres.

Aktiveringslås

I iOS 7.1 og nyere kan du bruke MDM til å aktivere aktiveringslåsen når en bruker slår på Finn iPhone på en enhet under tilsyn. Slik kan organisasjonen dra fordel av tyverisikringen som aktiveringslåsen gir, samtidig som det er mulig å overstyre funksjonen dersom en ansatt for eksempel slutter i jobben uten først å fjerne aktiveringslåsen med Apple ID-en sin.

MDM-løsningen kan hente en overstyringskode og tillate at brukeren aktiverer aktiveringslåsen på enheten på følgende premisser:

- Hvis Finn iPhone slås på når MDM-løsningen tillater aktiveringslås, vil aktiveringslåsen deaktiveres.
- Hvis Finn iPhone slås av når MDM-løsningen tillater aktiveringslås, vil aktiveringslåsen aktiveres neste gang brukeren aktiverer Finn iPhone.

Oppsummering

iOS-rammeverket for administrering gir deg det beste fra to verdener: IT-administratoren kan konfigurere, administrere og sikre enheter – og kontrollere bedriftsdataene på enhetene – samtidig som brukerne utrustes til å gjøre en god jobb med enheter de liker å bruke.