Administration af enheder og virksomhedsdata i iOS

Indhold

Oversigt

Grundlæggende om administration

Adskillelse af arbejdsdata og personlige data

Fleksible muligheder for administration

Opsummering

Oversigt

Virksomheder over hele verden styrker deres medarbejdere med iPhone og iPad.

Nøglen til en vellykket mobilstrategi er at skabe balance mellem IT-styringen og de muligheder, brugerne har adgang til. Når de gør iOS-enhederne mere personlige med egne apps og eget indhold, føler brugerne større ejerskab og ansvar – og det fører til større engagement og øget produktivitet. Det kan lade sig gøre gennem administrationsplatformen fra Apple, som tilbyder intelligente metoder til separat administration af virksomhedens data og apps, der effektivt holder arbejdsrelaterede og personlige data adskilt. Desuden forstår brugerne, hvordan deres enheder administreres, og de har tiltro til, at deres anonymitet og privatliv beskyttes.

Dette dokument indeholder vejledning i, hvordan man kan opnå den nødvendige IT-styring og samtidig sikre, at brugerne udstyres med de bedste værktøjer til deres arbejde. Det er et supplement til Håndbog om iOS-implementering, som er en omfattende teknisk online-håndbog om implementering og administration af iOS-enheder i virksomheden.

Se Håndbog om iOS-implementering på help.apple.com/deployment/ios.

Grundlæggende om administration

Med iOS kan I strømline implementeringer af iPhone og iPad ved hjælp af en række indbyggede teknikker, som giver jer mulighed for at forenkle kontoindstilling, konfigurere politikker, distribuere apps og anvende enhedsbegrænsninger eksternt.

Vores tilgang til administration

Administrationsplatformen fra Apple er grundlaget for administration af mobile enheder. Denne platform er indbygget i iOS og gør det muligt for virksomheder at administrere lige præcis det, de behøver, på en enkel måde – og ikke kun ved at låse funktioner eller deaktivere dem. Det betyder, at I med administrationsplatformen fra Apple kan få detaljeret kontrol over jeres enheder, apps og data via MDM-løsninger fra tredjepartsleverandører (MDM = administration af mobile enheder). Og vigtigst af alt får I den nødvendige kontrol, uden at det går ud over brugeroplevelsen eller medarbejdernes privatliv.

Blandt andre metoder til enhedsadministration bruger man måske andre navne til at beskrive MDM-funktionalitet, f.eks. EMM (Enterprise Mobility Management) eller MAM (Mobile Application Management). Disse løsninger har det samme formål: at administrere jeres virksomheds enheder og data trådløst. Og fordi administrationsplatformen fra Apple er indbygget i iOS, har I ikke brug for et separat administratorprogram fra udbyderen af jeres MDM-løsning.

Adskillelse af arbejdsdata og personlige data

Uanset om jeres virksomhed understøtter enheder, der ejes af brugerne eller virksomheden, kan I leve op til jeres mål for IT-administration og samtidig sikre, at brugerne får optimal produktivitet i alle deres arbejdsopgaver. Arbejdsrelaterede og personlige data administreres separat, uden at brugeroplevelsen bliver segmenteret. Dermed kan den mest populære produktivitetsapp placeres side om side med jeres virksomhedsapps på brugerens enhed – så medarbejderne får større frihed under arbejdet. iOS muliggør dette uden brug af løsninger fra tredjepartsleverandører, f.eks. datacontainere, der påvirker brugeroplevelsen og ofte gør brugerne frustrerede.

Overblik over forskellige administrationsmodeller

Der laves ofte datacontainere for at løse problemer på andre platforme – problemer, som ikke findes med iOS. Nogle datacontainere bruger en strategi med dobbelte konti, hvor to separate miljøer kører på den samme enhed. Andre fokuserer på at placere de forskellige apps i datacontainere ved hjælp af kodebaseret integration eller løsninger til "app wrapping". Alle disse metoder forhindrer brugerne i at være produktive – både, når de skal logge ind og ud af forskellige arbejdsområder, og når de er afhængige af proprietær kode, som ofte gør de enkelte apps inkompatible med opdateringer af styresystemet.

Virksomheder, der ikke længere bruger datacontainere, oplever i stedet, at de indbyggede iOS-funktioner til administrationsstyring er med til at give en optimal personlig brugeroplevelse og øget produktivitet. I stedet for at gøre det svært for brugerne at anvende deres enheder til både arbejde og fritid kan I bruge funktioner til politikkontrol, der administrerer datastrømmen helt problemfrit i baggrunden.

Administration af virksomhedsdata

Med iOS er det ikke nødvendigt at låse jeres enheder. Nøgleteknologier styrer strømmen af virksomhedens data mellem apps og forhindrer, at de finder vej ind i brugerens personlige apps eller cloud-tjenester.

Administreret indhold

Administreret indhold dækker installation, konfiguration, administration og fjernelse af apps fra App Store og specialudviklede interne apps, konti, bøger og domæner.

- **Administrerede apps.** Apps, som er installeret via MDM, kaldes for administrerede apps. De kan være gratis eller betalte apps fra App Store eller specialudviklede interne apps, og de kan alle installeres trådløst via MDM. Administrerede apps indeholder ofte følsomme oplysninger og giver større kontrol end apps, der downloades af brugeren. MDM-serveren kan fjerne administrerede apps og tilhørende data efter anmodning eller angive, om disse apps bør fjernes, når MDM-profilen fjernes. Desuden kan MDM-serveren forhindre, at data fra administrerede apps bliver sikkerhedskopieret til iTunes og iCloud.
- **Administrerede konti.** MDM kan hjælpe jeres brugere hurtigt i gang ved at indstille deres mail og andre konti helt automatisk. Afhængigt af MDM-løsningens udbyder og integrationen med jeres interne systemer kan kontodata også udfyldes automatisk med brugerens navn, mailadresse og eventuelle certifikat-ID'er til godkendelse og signering. MDM kan konfigurere følgende typer konti: IMAP/POP, CalDAV, kalendere i abonnement, CardDAV, Exchange ActiveSync og LDAP.
- **Administrerede bøger.** Ved hjælp af MDM kan bøger, ePub-bøger og PDF-dokumenter automatisk overføres til brugernes enheder, så medarbejderne altid har det materiale, de har

brug for. Administrerede bøger kan kun deles med andre administrerede apps eller sendes via mail ved hjælp af administrerede konti. Når de ikke længere skal bruges, kan materialerne fjernes eksternt.

- **Administrerede domæner.** Downloads fra Safari betragtes som administrerede dokumenter, hvis de stammer fra et administreret domæne. Det er muligt at administrere specifikke URL-adresser og underdomæner. Hvis en bruger f.eks. downloader en PDF-fil fra et administreret domæne, kræver domænet, at PDF-filen overholder alle indstillinger for administrerede dokumenter. Stier, der følger domænet, administreressom standard.

Administreret distribution

Med administreret distribution kan I bruge jeres MDM-løsning eller Apple Configurator 2 til at administrere de apps og bøger, der er købt gennem Apples mængdekøbsordning (VPP). For at aktivere administreret distribution skal I først oprette forbindelse mellem jeres MDM-løsning og jeres konto til mængdekøbsordningen ved hjælp af et sikkert token. Når MDM-serveren har forbindelse til mængdekøbsordningen, kan der tildeles apps direkte til en enhed, uden at brugeren behøver at have et Apple-id. Brugeren får besked, når apps er klar til at blive installeret på enheden. Hvis en enhed er overvåget, bliver der overført apps til den pågældende enhed i baggrunden, uden at brugeren får besked.

For at bevare den fulde kontrol over apps via en MDM-løsning skal der tildeles apps direkte til en enhed.

Administreret konfiguration af apps

Med administreret konfiguration af apps bruger MDM den administrationsplatform, der er indbygget i iOS, til at konfigurere apps under eller efter implementeringen. Denne platform gør det muligt for udviklerne at identificere de konfigurationsindstillinger, der bør implementeres, når deres app installeres som en administreret app. Medarbejderne kan gå i gang med at bruge apps, der er konfigureret på denne måde, med det samme – uden at det kræver specialtilpasset indstilling. IT-afdelingen kan være sikker på, at alle virksomhedsdata i apps bliver håndteret fortroligt, og der er hverken brug for proprietære SDK'er eller app wrapping.

App-udviklere kan få adgang til visse funktioner, som kan aktiveres ved hjælp af administreret konfiguration af apps, så udviklerne f.eks. kan konfigurere apps, forhindre sikkerhedskopiering af apps, slette apps eksternt og deaktivere muligheden for at tage skærmbilleder.

AppConfig Community fokuserer på at levere værktøjer og eksempler på bedste praksis i forbindelse med indbyggede funktioner i styresystemer til mobile enheder. Førende udbydere af MDM-løsninger fra dette fællesskab har etableret et standardskema, som alle app-udviklere kan bruge som hjælp til administreret konfiguration af apps. Idet de skaber muligheder for en mere ensartet, åben og enkel måde at konfigurere og sikre mobile apps på, er dette fællesskab med til at øge indførelsen af mobil teknologi i virksomheder.

Læs mere om AppConfig Community på www.appconfig.org.

Administrerede datastrømme

MDM-løsninger omfatter særlige funktioner, der gør det muligt at administrere virksomhedsdata på et detaljeret niveau, så de ikke finder vej til brugernes personlige apps eller cloud-tjenester.

- **Administreret åbning.** Administreret åbning anvender en række begrænsninger, der forhindrer, at vedhæftede bilag eller dokumenter fra administrerede kilder bliver åbnet på ikke-administrerede destinationer og omvendt.

  I kan f.eks. forhindre, at et fortroligt bilag, der hører til en mail på jeres virksomheds administrerede mailkonto, bliver åbnet i nogen af brugernes personlige apps. Det er kun de apps, der er installeret og administreret via MDM, som kan åbne dette arbejdsdokument. Brugerens ikke-administrerede personlige apps vises ikke på listen over apps, der kan åbne det vedhæftede bilag. Ud over administrerede apps, konti, bøger og domæner findes der adskillige udvidelser, som overholder begrænsningerne for administreret åbning.

For at beskytte virksomhedsdata er det kun de apps, der er installeret og administreret via MDM, som kan åbne dette arbejdsdokument.

- **Administrerede udvidelser.** App-udvidelser giver tredjepartsudviklere en ny måde at levere funktionalitet til andre apps på – og endda til vigtige indbyggede systemer i iOS såsom Meddelelsescenter – så jeres virksomhed kan bruge nye arbejdsprocesser mellem de forskellige apps. Når man bruger administreret åbning, kan ikke-administrerede udvidelsesfunktioner ikke interagere med administrerede apps. Her er nogle eksempler på forskellige typer udvidelser:
  - **Document Provider-udvidelser** gør det muligt for produktivitetsapps at åbne dokumenter fra en række forskellige cloud-tjenester, uden at der skal laves unødvendige kopier.
  - **Handlingsudvidelser** giver brugerne mulighed for at håndtere eller se indhold inden for rammerne af en anden app.

For eksempel kan brugerne anvende en handling til at oversætte tekst fra et andet sprog direkte i Safari.

- **Specielle tastaturudvidelser** giver adgang til andre tastaturer end dem, der allerede er indbygget i iOS. Administreret åbning kan forhindre, at uautoriserede tastaturer bliver vist i jeres virksomhedsapps.
- **"I dag"-udvidelser**, også kaldet widgets, bruges til at sende overskuelige oplysninger til oversigten "I dag" i Meddelelsescenter. Det giver brugerne en fantastisk mulighed for at få øjeblikkelig, opdateret information fra en app, og en enklere måde at åbne hele appen på, hvis de vil vide mere.
- **Deleudvidelser** gør det nemt for brugerne at dele indhold med andre medier, f.eks. sociale netværk eller tjenester til upload. Brugerne i en app, der indeholder en Del-knap, kan f.eks. vælge en deleudvidelse, der repræsenterer et socialt netværk, og derefter bruge den til at lægge en kommentar eller andet indhold op.

Fleksible muligheder for administration

Administrationsplatformen fra Apple er fleksibel og tilbyder en afbalanceret tilgang til jeres administration af enheder, der ejes af brugerne eller virksomheden. Når I bruger en MDM-løsning fra en tredjepartsleverandør sammen med iOS, kan I vælge mellem mange forskellige muligheder for enhedsadministration, lige fra meget åbne metoder til detaljeret kontrol helt efter jeres behov.

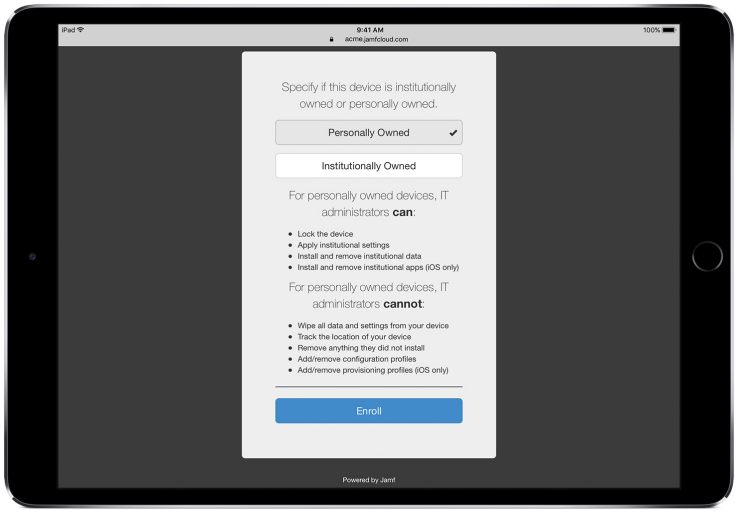
Ejerskabsmodeller

Den ejerskabsmodel – eller de ejerskabsmodeller – I følger for enheder i jeres virksomhed, er afgørende for, hvordan I administrerer enheder og apps. De to ejerskabsmodeller for iOS-enheder, der ofte anvendes i virksomheder, er brugerejede og virksomhedsejede.

Brugerejede enheder

Ved en implementering, hvor brugerne ejer enhederne, tilbyder iOS personlig indstilling udført af brugerne selv samt gennemsigtighed omkring, hvordan enhederne er konfigureret, og ikke mindst forvisning om, at virksomheden ikke har adgang til brugernes private data.

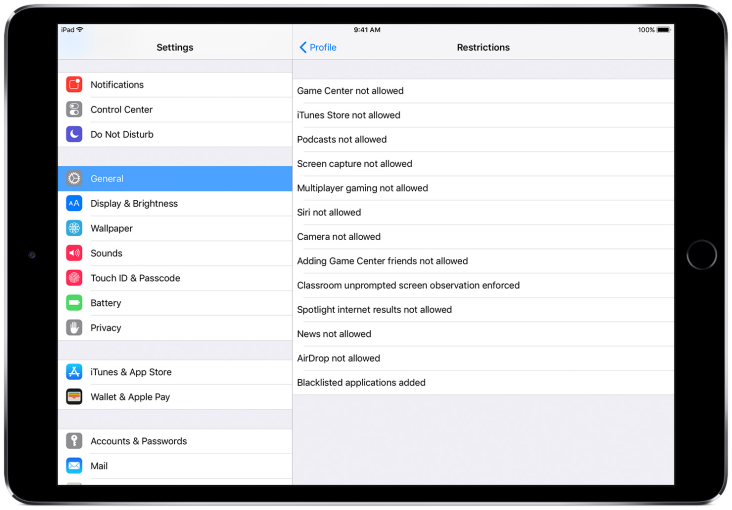
- **Tilmelding og framelding.** Når enheder købes og indstilles af brugerne – normalt kaldet BYOD (Bring Your Own Device) – kan I stadig give adgang til virksomhedstjenester som Wi-Fi, mail og kalender. Brugerne skal bare vælge at tilmelde sig jeres virksomheds MDM-løsning. Når brugerne tilmelder sig MDM for første gang på en iOS-enhed, får de oplysninger om, hvad MDM-serveren har adgang til på deres enhed, samt hvilke funktioner den vil konfigurere. Det giver gennemsigtighed for brugerne med hensyn til, hvad der administreres, og det skaber tillid mellem jer og brugerne. Det er vigtigt at gøre brugerne opmærksomme på, at de til enhver tid kan framelde sig denne type administration ved at fjerne administrationsprofilen på deres enhed, hvis de ikke føler sig trygge ved den. Når de gør det, slettes alle de virksomhedskonti og -apps, der er installeret via MDM.



MDM-løsninger fra tredjepartsleverandører har normalt en brugervenlig grænseflade, så medarbejderne føler sig trygge ved at tilmelde sig.*

*Skærmbillede stillet til rådighed af Jamf.

- **Større gennemsigtighed.** Når brugerne er tilmeldt MDM, kan medarbejderne nemt gå ind under Indstillinger for at se, hvilke apps, bøger og konti der administreres, og hvilke begrænsninger der er implementeret. Alle de virksomhedsindstillinger og -konti og alt det indhold fra virksomheden, som er installeret via MDM, markeres af iOS som administrerede.



I brugergrænsefladen til konfigurationsbeskrivels er under Indstillinger kan brugerne se helt præcist, hvad der er konfigureret på deres enhed.

- **Brugernes anonymitet.** Selvom en MDM-server giver jer mulighed for at interagere med iOS-enheder, betyder det ikke, at alle indstillinger og kontooplysninger bliver synlige. I kan administrere virksomhedens konti, indstillinger og oplysninger leveret via MDM, men der er ikke adgang til brugernes personlige konti. Faktisk sørger de samme funktioner, som sikrer data i virksomhedsadministrerede apps, også for at beskytte brugernes personlige indhold, så det ikke kan indgå i virksomhedens datastrøm.

  Følgende eksempler viser, hvad en MDM-server fra en tredjepartsleverandør kan se – og hvad den ikke kan se – på en personlig iOS-enhed:

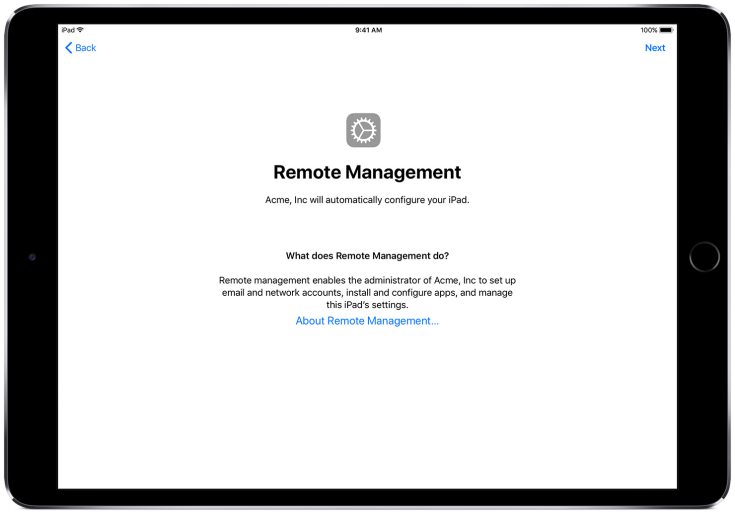
MDM kan se:	MDM kan ikke se personlige data som f.eks.:
Enhedens navn	Personlige eller arbejdsrelaterede mails, kalendere og kontakter
Telefonnummer	SMS eller iMessages
Serienummer	Safari-browserhistorik
Modelnavn og -nummer	Logfiler fra FaceTime- eller telefonopkald
Kapacitet og ledig plads	Personlige påmindelser og noter
iOS-versionsnummer	Hyppigheden af brug af apps
Installerede apps	Enhedens placering

- **Gør enhederne personlige.** Virksomheder har fundet ud af, at når brugerne får mulighed for at gøre en enhed personlig med deres eget Apple-id, fører det til større ejerskabs- og ansvarsfølelse blandt brugerne, og samtidig øges deres produktivitet, fordi de nu selv kan vælge de apps og det indhold, de skal bruge for at gøre deres arbejde bedst muligt.

Virksomhedsejede enheder

Ved en implementering, hvor virksomheden ejer enhederne, kan I give en enhed til hver bruger – dette kaldes implementering med personlig tilpasning. En anden mulighed er at lade enhederne gå på skift mellem brugerne, og det kaldes ikke-individualiseret implementering. iOS-funktioner såsom automatisk tilmelding, låsbare MDM-indstillinger, enhedsovervågning og Altid til-VPN sikrer, at enhederne bliver konfigureret i overensstemmelse med virksomhedens specifikke krav. Dermed får I større kontrol samtidig med, at jeres virksomhedsdata bliver beskyttet.

- **Automatisk tilmelding.** Apples tilmeldingsordning for enheder (DEP) giver jer mulighed for at automatisere tilmelding til MDM under den første indstilling af de iPhone- og iPad-enheder og Mac-systemer, jeres virksomhed ejer. Tilmeldingen kan gøres obligatorisk og permanent. I kan også aktivere overvåget tilstand på jeres enheder under tilmeldingsprocessen og lade brugerne springe nogle af de grundlæggende indstillingstrin over.



Med tilmeldingsordningen for enheder vil jeres MDM-løsning automatisk konfigurere jeres iOS-enheder via indstillingsassistenten.

- **Overvågede enheder.** Overvågning giver adgang til yderligere administrationsfunktioner for iOS-enheder, der ejes af jeres virksomhed. Det er f.eks. muligt at aktivere et webfilter gennem en global proxy for at sikre, at brugernes internettrafik holder sig inden for virksomhedens retningslinjer, forhindre brugerne i at gendanne enhedens fabriksindstillinger m.m. Som standard

er iOS-enheder ikke overvågede. Brug tilmeldingsordningen for enheder til at aktivere overvågningstilstand automatisk eller Apple Configurator 2 til at aktivere overvågning manuelt.

Selvom I måske ikke lige nu har planer om at bruge funktioner, der kun er tilgængelige i overvågningstilstand, bør I overveje at vælge overvågning af jeres enheder, når I indstiller dem. Det sikrer, at I senere hen kan udnytte funktioner, der kun er tilgængelige på overvågede enheder. Ellers vil I være nødt til at slette de enheder, der allerede er taget i brug. Overvågning drejer sig ikke om at låse en enhed – det er i stedet et spørgsmål om at gøre virksomhedsejede enheder bedre ved at udvide administrationsfunktionerne. På længere sigt vil overvågning give jeres virksomhed endnu flere muligheder.

Se hele listen over overvågede indstillinger i Håndbog om iOS-implementering.

Begrænsninger

iOS understøtter følgende kategorier af begrænsninger, som I kan konfigurere trådløst for at opfylde virksomhedens behov, uden at det går ud over brugerne:

- AirPrint
- Installation af apps
- Brug af apps
- Klasseværelse-appen
- Enhed
- iCloud
- Profile Manager-begrænsninger for brugere og brugergrupper
- Safari
- Indstillinger for sikkerhed og anonymitet
- Siri

I følgende kategorier findes der også valgmuligheder, som kan konfigureres via jeres MDM-løsning:

- Indstillinger for automatiseret MDM-tilmelding
- Trin i indstillingsassistenten

Yderligere administrationsfunktioner

Forespørgsler til enheder

Ud over at konfigurere enheder kan en MDM-server sende forespørgsler til enhederne for at få forskellige oplysninger, f.eks. information om de enkelte enheder, netværk, apps, data om overholdelse af virksomhedspolitikker og sikkerhedsdata. Disse oplysninger er med til at sikre, at enhederne bliver ved med at overholde de påkrævede politikker. MDM-serveren afgør, hvor tit den indhenter oplysninger.

Følgende er eksempler på oplysninger, der kan sendes forespørgsler om til en iOS-enhed:

- Enhedsoplysninger (navn)
- Model, iOS-version og serienummer
- Netværksoplysninger

- Roaming-status, MAC-adresser
- Installerede apps
- Appens navn, version og størrelse
- Data om overholdelse af politikker og sikkerhedsdata
- Installerede indstillinger, retningslinjer og certifikater
- Krypteringsstatus

Administrationsopgaver

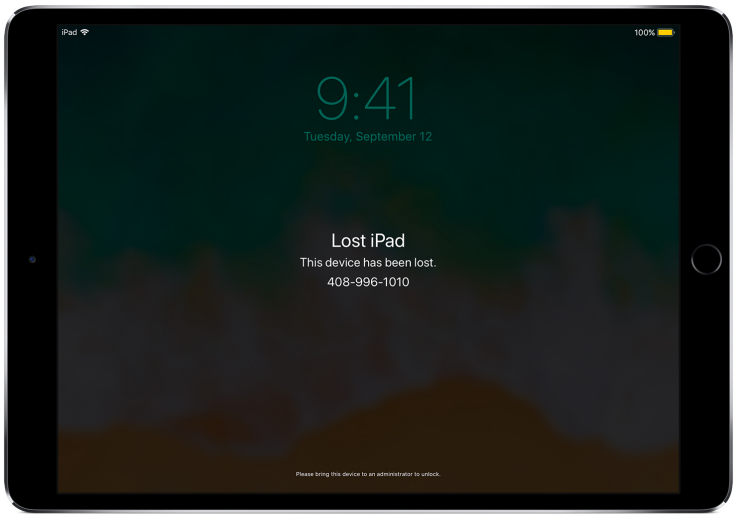
Når en enhed bliver administreret, kan en MDM-server udføre mange forskellige administrationsopgaver. Det kan f.eks. være automatisk ændring af konfigurationsindstillingerne uden brugerinteraktion, iOS-opdatering på enheder låst med adgangskode, ekstern låsning eller sletning af en enhed eller fjernelse af en adgangskodelås, så brugere kan nulstille glemte adgangskoder. Det er også muligt for en MDM-server at anmode en iOS-enhed om at starte AirPlay-skærmdublering til en bestemt destination eller afslutte en aktuel AirPlay-session.

Funktionen Mistet

Med iOS 9.3 eller nyere kan jeres MDM-løsning eksternt slå funktionen Mistet til på en overvåget enhed. Denne handling låser enheden og giver tilladelse til, at der vises en besked med et telefonnummer på låseskærmen.

Ved hjælp af funktionen Mistet kan man finde overvågede enheder, der er blevet væk eller stjålet, fordi MDM sender eksterne forespørgsler om deres placering, sidst de var online. Funktionen Mistet kræver ikke, at Find min iPhone er aktiveret.

Hvis MDM slår funktionen Mistet fra eksternt, bliver enheden låst op, og der indhentes oplysninger om dens placering. For at bevare gennemsigtigheden får brugeren besked om, at funktionen Mistet er slået fra.



Når MDM slår funktionen Mistet til på en enhed, betyder det også, at den låser enheden, giver tilladelse til, at der vises beskeder på skærmen, og fastslår dens placering.

Aktiveringslås

Med iOS 7.1 eller nyere kan MDM bruges til at slå Aktiveringslås til, når en bruger slår Find min iPhone til på en overvåget enhed. Dermed kan jeres virksomhed få gavn af tyverisikringen i Aktiveringslås, mens I fortsat kan omgå funktionen – f.eks. hvis en bruger forlader virksomheden uden først at fjerne Aktiveringslås ved hjælp af deres Apple-id.

Jeres MDM-løsning kan hente en kode til at omgå funktionen og tillade, at brugeren slår Aktiveringslås til på enheden, på følgende præmisser:

- Hvis Find min iPhone er slået til, når jeres MDM-løsning tillader Aktiveringslås, bliver Aktiveringslås slået til på dette tidspunkt.
- Hvis Find min iPhone er slået fra, når jeres MDM-løsning tillader Aktiveringslås, bliver Aktiveringslås slået til, næste gang brugeren slår Find min iPhone til.

Opsummering

Administrationsplatformen i iOS giver jer det bedste fra begge verdener: IT-medarbejderne kan konfigurere, administrere og sikre enhederne samt styre de virksomhedsdata, der strømmer gennem dem, og samtidig udrustes brugerne til at gøre et fantastisk stykke arbejde med de enheder, de elsker at bruge.