Beheer van devices en bedrijfsgegevens met iOS

Inhoudsopgave

Overzicht
Vuistregels voor beheer
Scheiding van zakelijke en persoonlijke gegevens
Flexibele beheersopties
Samenvatting

Overzicht

Bedrijven wereldwijd geven hun werknemers de kracht van iPhone en iPad in handen.

De sleutel tot een geslaagde mobiele strategie is een balans tussen beheer door de IT-afdeling en mogelijkheden voor de gebruiker. Door iOS-devices te personaliseren met eigen apps en content, krijgen gebruikers een groter gevoel van eigendom en verantwoordelijkheid, wat tot meer betrokkenheid en een hogere productiviteit leidt. Dit wordt mogelijk gemaakt door het beheerframework van Apple, dat slimme manieren aanreikt om bedrijfsgegevens en -apps afzonderlijk te beheren, zodat bedrijfsgegevens onmerkbaar van persoonlijke gegevens worden gescheiden. Bovendien krijgen gebruikers inzicht in de manier waarop hun device wordt beheerd, en kunnen ze erop vertrouwen dat hun privacy gewaarborgd is.

Dit document bevat informatie over de manier waarop essentieel IT-beheer kan worden gerealiseerd terwijl de gebruikers kunnen blijven profiteren van de beste tools voor hun werk. Het vormt een aanvulling op de online iOS-implementatiehandleiding. Dit is een uitgebreid technische referentiebestand voor het implementeren en beheren van iOS-apparaten in een bedrijf.

De iOS-implementatiehandleiding is te vinden op help.apple.com/deployment/ios.

Vuistregels voor beheer

Met iOS stroomlijnt u de implementatie van iPhone en iPad met een scala aan ingebouwde technologieën waarmee u het instellen van accounts, configureren van beleidsregels, distribueren van apps en toepassen van device-beperkingen sterk vereenvoudigt.

Onze benadering van beheer

Het beheerframework van Apple vormt de basis voor beheer van mobiele devices. Dit framework is in iOS ingebouwd, zodat organisaties kunnen beheren wat ze moeten beheren – op een soepele manier en niet door simpelweg features te blokkeren of functionaliteit uit te schakelen. Hierdoor biedt het beheerframework van Apple mogelijkheden voor fijnmazig beheer met MDM-oplossingen (Mobile Device Management) van andere leveranciers voor uw devices, apps en gegevens. En misschien wel het belangrijkste: u krijgt de controle die u nodig hebt zonder dat de gebruikerservaring – of de privacy van uw werknemers – hieronder te lijden heeft.

Andere methoden voor devicebeheer op de markt gebruiken mogelijk andere benamingen voor de beschrijving van MDM, zoals Enterprise Mobility Management (EMM) of Mobile Application Management (MAM). Met deze oplossingen wordt evenwel hetzelfde beoogd: draadloos beheer van de devices en bedrijfsgegevens van uw organisatie. En aangezien het beheerframework van Apple in iOS is ingebouwd, hebt u geen aparte clientapp van uw MDM-leverancier nodig.

Scheiding van zakelijke en persoonlijke gegevens

Of uw organisatie nu devices in eigendom van de gebruiker of van de organisatie ondersteunt, u kunt uw doelen voor IT-beheer realiseren terwijl de productiviteit van uw medewerkers volledig behouden blijft. Zakelijke en persoonlijke gegevens worden afzonderlijk beheerd, zonder dat de gebruikerservaring daardoor gefragmenteerd wordt. Zo kan de populairste productiviteitsapp direct naast uw bedrijfsapps op een device staan, waardoor werknemers meer vrijheid van werken krijgen. iOS realiseert dit zonder het gebruik van externe oplossingen zoals beveiligingscontainers, die de gebruikservaring schaden en tot frustraties kunnen leiden.

Verschillende beheermodellen

In het verleden zijn vaak beveiligingscontainers ontwikkeld om problemen op te lossen op andere platforms, problemen die iOS helemaal niet kent. Bij sommige containers wordt ervoor gekozen twee afzonderlijke omgevingen op één device te creëren. Bij andere oplossingen ligt de focus op het afschermen van de apps zelf via het vooraf integreren van functionaliteit via de eigen SDK of door de apps "in te pakken". Al deze methoden vormen een productiviteitsobstakel: gebruikers moeten bij meerdere workspaces in- en uitloggen en worden afhankelijk van bedrijfseigen code, waardoor apps na een upgrade van het besturingssysteem vaak niet meer compatibel zijn.

Organisaties die niet langer beveiligingscontainers gebruiken, zien dat de native beheersvoorzieningen in iOS een optimale persoonlijke gebruikservaring bieden en de productiviteit van gebruikers verhogen. U hoeft gebruikers die hun device zowel voor het werk als privé gebruiken niet te beperken. U kunt namelijk ook beleidsvoorzieningen gebruiken die de gegevensstroom onmerkbaar achter de schermen regelen.

Beheer van bedrijfsgegevens

Met iOS hoeft u uw devices niet te begrenzen. Met cruciale technologie wordt de stroom van bedrijfsgegevens tussen verschillende apps beheerd en wordt voorkomen dat bedrijfsgegevens uitlekken naar persoonlijke apps of clouddiensten.

Beheerd materiaal

Het beheer van materiaal bestaat uit het installeren, configureren, beheren en eventueel verwijderen van apps, accounts, boeken en domeinen die afkomstig zijn uit de App Store of die intern zijn ontwikkeld.

- **Beheerde apps.** Apps die zijn geïnstalleerd met behulp van MDM worden "beheerde apps" genoemd. Dit kunnen gratis of betaalde apps uit de App Store zijn of intern ontwikkelde apps op maat, die op afstand via MDM geïnstalleerd kunnen worden. Beheerde apps bevatten vaak vertrouwelijke informatie, en bieden meer controlemogelijkheden dan apps die door de gebruiker gedownload worden. De MDM-server kan op aanvraag beheerde apps en de bijbehorende gegevens verwijderen. Ook kan worden ingesteld of de apps moeten worden verwijderd wanneer het MDM-profiel wordt verwijderd. Bovendien kan de MDM-server voorkomen dat er een reservekopie in iTunes of iCloud wordt gemaakt van gegevens uit beheerde apps.
- **Beheerde accounts.** Met MDM kunnen bijvoorbeeld e-mailaccounts automatisch worden ingesteld, zodat de gebruikers binnen uw organisatie snel aan de slag kunnen. Afhankelijk van de MDM-leverancier en de integratie met uw interne systemen, kunnen de accountgegevens vooraf worden aangevuld met namen, e-mailadressen en eventueel certificaatidentiteiten voor identiteitscontrole en ondertekening. MDM kan de volgende typen accounts beheren: IMAP/POP, CalDAV, agenda's met abonnement, CardDAV, Exchange ActiveSync en LDAP.
- **Beheerde boeken.** Met MDM kunnen boeken, ePub-boeken en pdf-documenten automatisch naar de devices van gebruikers gepusht worden, zodat uw werknemers altijd de benodigde materialen hebben. Beheerde boeken kunnen alleen met andere beheerde apps worden gedeeld

of via beheerde accounts worden gemaild. Als de materialen niet langer nodig zijn, kunnen ze op afstand worden verwijderd.

- **Beheerde domeinen.** Downloads uit Safari worden als beheerde documenten gezien als ze afkomstig zijn uit een beheerd domein. Specifieke URL's en subdomeinen kunnen worden beheerd. Als een gebruiker bijvoorbeeld een pdf-bestand uit een beheerd domein downloadt, vereist het domein dat de pdf aan alle instellingen voor beheerde documenten voldoet. Domeinpaden worden standaard beheerd.

Beheerde distributie

Bij beheerde distributie gebruikt u uw MDM-oplossing of Apple Configurator 2 om apps en boeken te beheren die via het VPP (Volume Purchase Program) zijn gekocht. Om beheerde distributie in te schakelen, moet u uw MDM-oplossing eerst met een veilig token aan uw VPP-account koppelen. Zodra uw MDM-server is gekoppeld aan het VPP, kunt u direct apps aan een device toewijzen. Hiervoor heeft de gebruiker zelfs geen Apple ID nodig. De gebruiker krijgt een melding wanneer er apps op zijn device geïnstalleerd kunnen worden. Als een device onder supervisie staat, worden apps op de achtergrond gepusht zonder dat de gebruiker hier van een melding krijgt.

Voor volledige controle over apps met een MDM-oplossing, wijst u apps direct toe aan een device.

Configuratie van beheerde apps

Bij de configuratie van beheerde apps gebruikt MDM het native iOS-beheerframework om apps te configureren tijdens of na implementatie. Met dit framework kunnen ontwikkelaars de configuratie-instellingen identificeren die geïmplementeerd moeten worden wanneer hun app als beheerde app wordt geïnstalleerd. Werknemers kunnen apps die op deze manier geconfigureerd zijn direct gebruiken, zonder dat daarvoor een speciale configuratie nodig is. De IT-afdeling heeft de zekerheid dat bedrijfsgegevens binnen apps goed beveiligd zijn, zonder gebruik van een bedrijfseigen SDK en zonder inpakken van apps.

App-ontwikkelaars hebben de beschikking over mogelijkheden die via de configuratie van beheerde apps kunnen worden ingeschakeld, zoals het instellen van apps, voorkomen dat er een reservekopie van een app wordt gemaakt, uitschakelen van schermafbeeldingen en wissen van apps op afstand.

De AppConfig Community richt zich op het bieden van tools en beproefde methoden rond native functionaliteit in mobiele besturingssystemen. Gerenommeerde MDM-leveranciers uit deze community hebben een standaardschema opgesteld dat door alle app-ontwikkelaars kan worden gebruikt bij de ondersteuning van de configuratie van beheerde apps. Door een meer consistente,

transparante en eenvoudige manier te bieden om mobiele apps te configureren en beveiligen, draagt de community bij aan de inzet van mobiele apparatuur in het bedrijfsleven.

Meer informatie over de AppConfig Community is te vinden op www.appconfig.org.

Beheerde gegevensstroom

MDM-oplossingen bieden specifieke mogelijkheden waarmee bedrijfsgegevens op detailniveau beheerd kunnen worden zodat deze niet naar de persoonlijke apps en clouddiensten van de gebruiker uitlekken.

- **Open in-functie.** Voor het beheer van de Open in-functie wordt gebruikgemaakt van een reeks beperkingen waarmee voorkomen wordt dat bijlagen en documenten uit beheerde bronnen worden geopend op niet-beheerde bestemmingen, en omgekeerd.

  U kunt bijvoorbeeld voorkomen dat een vertrouwelijke bijlage bij een bedrijfsmail in de beheerde mailaccount van uw organisatie, wordt geopend in een persoonlijke app van een gebruiker. Het bedrijfsdocument kan alleen worden geopend met apps die via MDM zijn geïnstalleerd en worden beheerd. De onbeheerde persoonlijke apps van de gebruiker worden niet eens weergegeven in de lijst met apps waarmee de bijlage kan worden geopend. Naast beheerde apps, accounts, boeken en domeinen maken ook verschillende extensies gebruik van de beperkingen van de beheerde Open in-functie.

Om bedrijfsgegevens te beveiligen, kunnen alleen via MDM geïnstalleerde en beheerde apps dit werkdocument openen.

- **Beheerde extensies.** Met app-extensies kunnen externe ontwikkelaars andere apps of zelfs belangrijke iOS-voorzieningen, zoals het Berichtencentrum, van meer functies voorzien. Zo worden nieuwe zakelijke workflows tussen apps mogelijk. Het gebruik van de beheerde Open in-functie voorkomt dat functies van niet-beheerde extensies de interactie aangaan met beheerde apps. In de volgende voorbeelden ziet u verschillende soorten extensies:
  - Met **extensies voor toegang tot bestanden** kunnen productiviteitsapps documenten openen uit diverse clouddiensten zonder dat daarvoor onnodige kopieën gemaakt hoeven te worden.
  - Met **Actie-extensies** kunnen gebruikers materiaal binnen de context van een andere app bekijken of manipuleren. Zo kunnen gebruikers bijvoorbeeld direct vanuit Safari tekst laten vertalen.
  - **Extensies voor toetsenborden op maat** bieden andere toetsenborden dan die in iOS zijn opgenomen. Met de Open in-functie kan voorkomen worden dat niet-geautoriseerde toetsenborden in uw bedrijfsapps worden gebruikt.

- **Vandaag-extensies** (ook wel widgets genoemd) worden gebruikt om informatie overzichtelijk weer te geven in de Vandaag-weergave van het Berichtencentrum. Op deze manier ontvangen gebruikers snel actuele informatie van een app en kunnen ze de app eenvoudig openen voor meer informatie.
- Met **Deel-extensies** kunnen gebruikers materiaal eenvoudig delen met bijvoorbeeld social media of uploaddiensten. In een app die een Deel-knop heeft, kunnen gebruikers bijvoorbeeld een Deel-extensie kiezen van een site voor social media en vervolgens een opmerking of andere content plaatsen.

Flexibele beheersopties

Het beheerframework van Apple is flexibel en biedt een uitgebalanceerde benadering van de manier waarop u bedrijfsdevices en persoonlijke devices in uw onderneming beheert. Als u een MDM-oplossing van een andere leverancier gebruikt met iOS, variëren uw opties voor devicebeheer van een zeer open benadering tot een uitermate fijnmazig beheerde omgeving, al naar gelang uw behoeften.

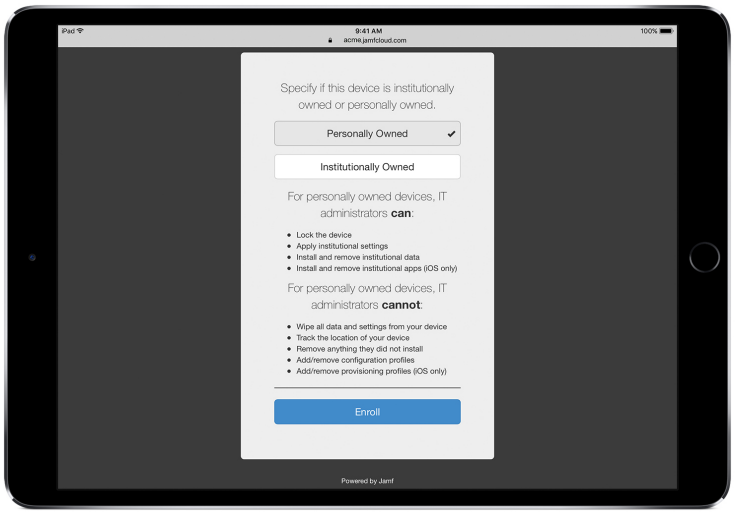
Eigendomsmodellen

Afhankelijk van het eigendomsmodel (of de eigendomsmodellen) in uw organisatie, zult u devices en apps verschillend beheren. De twee eigendomsmodellen voor iOS-devices die het meest worden gebruikt binnen ondernemingen, zijn 'eigendom van bedrijf' en 'eigendom van gebruiker'.

Devices in eigendom van gebruikers

Met een implementatie van devices in eigendom van gebruikers kunnen deze in iOS hun device naar eigen wens configureren, en is het voor hen helder hoe het device is ingesteld. De gebruikers kunnen er bovendien zeker van zijn dat hun persoonlijke gegevens niet voor de organisatie toegankelijk zijn.

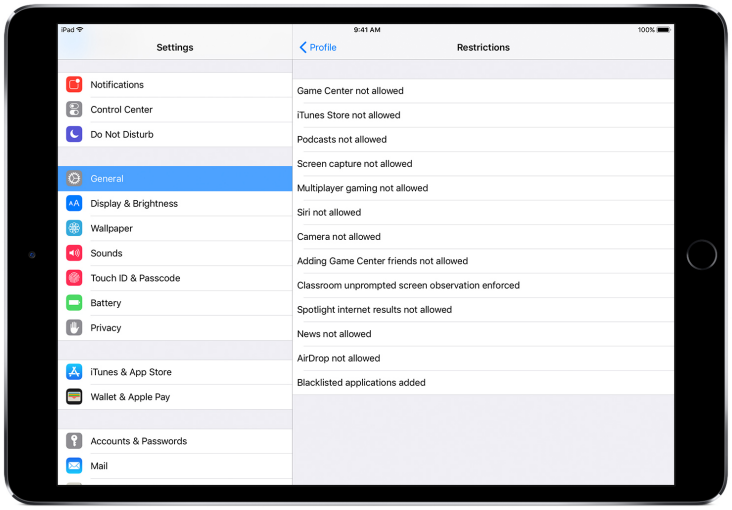
- **Optionele aanmelding** Wanneer de devices door de gebruikers worden gekocht en ingesteld (een zogenaamde BYOD-situatie), kunt u gewoon toegang bieden tot bedrijfsvoorzieningen als wifi, mail en agenda's. Gebruikers melden zich daarvoor aan bij de MDM-oplossing van uw organisatie. Als de gebruikers zich voor de eerste keer aanmelden bij MDM, zien ze waartoe de MDM-server toegang heeft op hun device en welke features de server configureert. Hiermee krijgt de gebruiker inzicht in wat er wordt beheerd en ontstaat er een vertrouwensband tussen u en de gebruikers.Het is belangrijk de gebruikers te laten weten dat wanneer ze niet tevreden zijn over het beheer, ze op elk moment de aanmelding kunnen terugdraaien door het beheerprofiel van hun devices te verwijderen. Als ze dat doen, worden alle via MDM geïnstalleerde accounts en apps verwijderd.



MDM-oplossingen van andere leveranciers hebben vaak een herkenbare interface voor werknemers, zodat ze tijdens de optionele aanmelding met vertrouwen akkoord gaan.*

* Schermafbeelding met dank aan Jamf.

- **Meer transparantie.** Zodra gebruikers bij MDM zijn aangemeld, kunnen ze in Instellingen zien welke apps, boeken en accounts worden beheerd en welke beperkingen er zijn ingesteld. Alle zakelijke instellingen, accounts en content die met MDM worden geïnstalleerd, worden als 'beheerd' gemarkeerd door iOS.



De gebruikersinterface voor configuratieprofielen in Instellingen laat gebruikers precies zien wat er op hun device geconfigureerd is.

- **Privacy.** Bij een MDM-server kunt u met iOS-devices communiceren zonder dat alle instellingen en accountgegevens zichtbaar zijn. U kunt via MDM ingestelde zakelijke accounts, instellingen en informatie beheren, maar de persoonlijke accounts van de gebruiker zijn niet toegankelijk. Dezelfde voorzieningen die de gegevens beveiligen in apps die door het bedrijf worden beheerd, zorgen er ook voor dat de persoonlijke content van de gebruiker niet in de zakelijke gegevensstroom terechtkomt.

  In de volgende voorbeelden ziet u wat een MDM-server van een andere leverancier wel en niet kan inzien op een persoonlijk iOS-device.

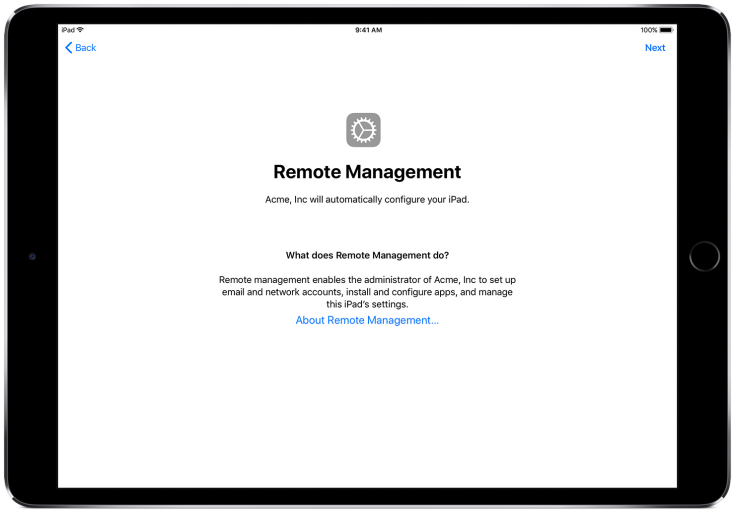
Zichtbaar via MDM:	Persoonlijke gegevens zoals de volgende zijn niet zichtbaar via MDM:
Naam van device	Persoonlijke of zakelijke mail, agenda's, contacten
Telefoonnummer	Sms- of iMessage-berichten
Serienummer	Safari-geschiedenis
Modelnaam en -nummer	Logs van FaceTime- of telefoongesprekken
Capaciteit en vrije ruimte	Persoonlijke herinneringen en notities
iOS-versienummer	Frequentie van appgebruik
Geïnstalleerde apps	Locatie van device

- **Devices personaliseren.** Bedrijven hebben ontdekt dat meer vrijheid voor gebruikers om hun device te personaliseren met hun eigen Apple ID, tot een verhoogd gevoel van eigendom en verantwoordelijkheid leidt. De productiviteit neemt toe doordat de gebruikers nu kunnen kiezen welke apps en welke content ze nodig hebben om hun werk zo goed mogelijk te doen.

Devices in eigendom van de organisatie

Bij een implementatie van devices in eigendom van de organisatie kunt u elke gebruiker van een device voorzien (gepersonaliseerde implementatie) of devices onder gebruikers laten rouleren (niet-gepersonaliseerde implementatie). iOS-features als geautomatiseerde aanmelding, vergrendelbare MDM-instellingen, supervisie van devices en altijd actief VPN zorgen ervoor dat de devices volgens de specifieke vereisten van uw organisatie worden geconfigureerd. Zo ontstaat er meer controle en weet u zeker dat de bedrijfsgegevens beveiligd zijn.

- **Automatische aanmelding.** Met het Device Enrollment Program (DEP) kunt u de MDM-aanmelding tijdens de eerste configuratie voor iPhones, iPads en Macs van uw organisatie automatiseren. U kunt de aanmelding verplicht en niet-verwijderbaar maken.U kunt devices bij aanmelding ook onder supervisie plaatsen, en gebruikers bepaalde basisconfiguratiestappen laten overslaan.



Met DEP configureert uw MDM-oplossing uw iOS-devices automatisch via de configuratie-assistent.

- **Devices onder supervisie.** Supervisie geeft extra beheermogelijkheden voor iOS-devices die eigendom zijn van de organisatie. Zo kunt u een webfilter inschakelen via een globale proxy zodat het webverkeer van gebruikers binnen de richtlijnen van de organisatie blijft, voorkomen dat gebruikers de fabrieksinstellingen van hun device terugzetten, en nog veel meer. iOS-

devices staan standaard niet onder supervisie. U kunt de supervisiemodus automatisch inschakelen met DEP of supervisie handmatig inschakelen met Apple Configurator 2.

Ook als u niet van plan bent mogelijkheden te gebruiken die alleen voor devices onder supervisie beschikbaar zijn, kunt u overwegen supervisie tijdens de configuratie in te schakelen zodat u deze mogelijkheden in de toekomst alsnog kunt benutten. Anders zult u reeds ingezette devices moeten wissen. Bij supervisie gaat het niet om het vergrendelen van een device. Het gaat juist om het verbeteren van devices van de organisatie door de beheermogelijkheden ervan uit te breiden. Op de lange termijn biedt supervisie nog meer opties voor uw onderneming.

Voor een volledig overzicht van de beheerde instellingen raadpleegt u de iOS-implementatiehandleiding.

Beperkingen

iOS ondersteunt de volgende categorieën beperkingen, die u draadloos kunt configureren overeenkomstig de behoeften van uw organisatie, zonder nadelige gevolgen voor de gebruiker:

- AirPrint
- Appgebruik
- Beperkingen voor gebruikers en groepen in Profielbeheer
- Beveiligings- en privacy-instellingen
- Device
- Installatie van apps
- iCloud
- Klaslokaal-app
- Safari
- Siri

De volgende categorieën hebben ook opties die door uw MDM-oplossing kunnen worden geconfigureerd:

- Instellingen geautomatiseerde MDM-aanmelding
- Schermen van de configuratie-assistent

Aanvullende beheermogelijkheden

Gegevens opvragen van devices

Een MDM-server kan niet alleen worden gebruikt voor deviceconfiguratie maar ook voor het benaderen van devices om allerlei informatie op te vragen. U kunt hierbij denken aan informatie over het device zelf, het netwerk, apps, en gegevens over naleving en beveiliging. Met deze informatie kan worden gecontroleerd of devices aan de vereiste beleidsregels blijven voldoen. De MDM-server bepaalt de frequentie waarmee informatie wordt verzameld.

Hieronder ziet u voorbeelden van de informatie die bij een iOS-device kan worden opgevraagd:

- Details van device (naam)
- Model, iOS-versie, serienummer
- Netwerkgegevens

- Roamingstatus, MAC-adressen
- Geïnstalleerde apps
- Naam, versie, grootte van app
- Nalevings- en beveiligingsgegevens
- Geïnstalleerde instellingen, beleidsregels, certificaten
- Encryptiestatus

Beheertaken

Bij beheerde devices kan een MDM-server allerlei taken uitvoeren, zoals het automatisch wijzigen van de configuratie-instellingen zonder tussenkomst van de gebruikers, bijwerken van iOS op met een wachtwoord vergrendelde devices, op afstand vergrendelen of wissen van het device, of verwijderen van het codeslot van de gebruiker zodat deze een nieuw wachtwoord kan instellen. Een MDM-server kan een iOS-device opdracht geven om te beginnen met synchrone AirPlay-weergave naar een specifieke bestemming of om een AirPlay-sessie te beëindigen.

Verloren-modus

Met iOS 9.3 of hoger kan uw MDM-oplossing een device dat onder supervisie staat, op afstand in de Verloren-modus zetten. Met deze handeling wordt het device vergrendeld en kan er een bericht met een telefoonnummer op het toegangsscherm worden geplaatst.

Met de Verloren-modus kunnen devices onder supervisie bij verlies of diefstal worden gelokaliseerd: de MDM-server vraagt de locatie op wanneer ze het laatst online waren. Voor de Verloren-modus hoeft Zoek mijn iPhone niet ingeschakeld te zijn.

Als de MDM-oplossing op afstand de Verloren-modus uitschakelt, wordt het device ontgrendeld en wordt de locatie opgehaald. Om de transparantie te waarborgen, krijgt de gebruiker de melding dat de Verloren-modus is uitgeschakeld.

Als MDM een vermist device in de Verloren-modus zet, wordt het device vergrendeld, kunnen er berichten op het scherm worden geplaatst en kan de locatie van het device worden bepaald.

Activeringsslot

Met iOS 7.1 of hoger kunt u MDM gebruiken om het activeringsslot in te schakelen als een gebruiker Zoek mijn iPhone inschakelt op een device dat onder supervisie staat. Zo kan uw

organisatie profiteren van de antidiefstalfunctionaliteit van het activeringsslot, terwijl deze feature ook kan worden uitgeschakeld wanneer een gebruiker bijvoorbeeld de organisatie verlaat zonder eerst het activeringsslot te verwijderen met de Apple ID.

Uw MDM-oplossing kan een bypass-code opvragen en het de gebruiker toestaan het activeringsslot op het device in te schakelen op basis van het volgende:

- Als Zoek mijn iPhone wordt ingeschakeld wanneer uw MDM-oplossing het activeringsslot toestaat, wordt het activeringsslot op dat moment ingeschakeld.
- Als Zoek mijn iPhone wordt uitgeschakeld wanneer uw MDM-oplossing het activeringsslot toestaat, wordt het activeringsslot ingeschakeld wanneer de gebruiker de volgende keer Zoek mijn iPhone inschakelt.

Samenvatting

Met het iOS-beheerframework kan uw IT-afdeling devices configureren, beheren en beveiligen, en de bedrijfsgegevens op de devices controleren. En tegelijkertijd kunnen uw medewerkers productief aan de slag met de devices waar ze vertrouwd mee zijn.