Laitteiden ja yrityksen tietojen hallitseminen iOS:ssä

Yleiskatsaus

Kaikkialla maailmassa yritykset tarjoavat työntekijöilleen vaikutusmahdollisuuksia iPhonen ja iPadin avulla.

Sisältö

IT-hallinnan tasapainottaminen käytettävyyden kanssa on onnistuneen mobiilistrategian avaintekijä. Personoimalla iOS-laitteita omilla apeillaan ja sisällöllään käyttäjät osoittavat suurempaa omistajuutta ja vastuunkantoa. Tämän seurauksena sitoutuminen paranee ja tuottavuus kasvaa. Applen hallintasovelluskehys tarjoaa älykkäitä tapoja hallita yrityksen tietoja ja appeja hienovaraisesti niin, että työtiedot ja henkilökohtaiset tiedot pidetään vaivattomasti erillään. Lisäksi käyttäjät ymmärtävät, miten heidän laitteitaan hallitaan, ja luottavat siihen, että heidän yksityisyytensä on suojattu.

Tämä dokumentti opastaa keskeisen IT-hallinnan saavuttamisessa siten, että käyttäjille voidaan samalla tarjota parhaimmat mahdolliset työkalut. Se täydentää iOS:n käyttöönoton opasta, joka on verkosta löytyvä kattava tekninen opas iOS-laitteiden käyttöönottoon ja hallintaan yrityksessä.

Voit tutustua iOS:n käyttöönoton oppaaseen osoitteessa help.apple.com/deployment/ios.

Hallinnan perusteet

iOS:n avulla voit selkeyttää iPhonen ja iPadin käyttöönottoa monilla sisäänrakennetuilla tekniikoilla, joilla voit yksinkertaistaa tilien käyttöönottoa, määrittää käytäntöjä, jaella appeja ja asettaa laiterajoituksia etänä.

Hallinnan toteutus

Mobiililaitteiden hallinta pohjautuu Applen hallintasovelluskehykseen. Sovelluskehys on iOS:n sisäinen ominaisuus. Sen ansiosta organisaatiot voivat kevyellä kosketuksella hallita sitä, mikä kaipaa hallintaa – muutenkin kuin vain lukitsemalla ominaisuuksia tai poistamalla toimintoja käytöstä. Applen hallintasovelluskehys mahdollistaa laitteiden, appien ja tietojen tarkan hallinnan muun valmistajan mobiililaitteiden hallintaratkaisulla (MDM). Mikä tärkeintä, saat tarvitsemasi hallinnan käyttäjäkokemusta heikentämättä ja työntekijöiden yksityisyydestä tinkimättä.

Muut markkinoilla olevat laitehallinnan tavat voivat kuvata MDM-toimintoja muilla sanoilla, kuten yritysten mobiilihallinta (EMM) tai appien mobiilihallinta (MAM). Kaikilla näillä ratkaisuilla on sama tavoite: organisaation laitteiden ja yrityksen tietojen langaton hallinta. Koska Applen hallintasovelluskehys on iOS:n sisäinen ominaisuus, et tarvitse erillistä agenttia MDM-ratkaisun toimittajalta.

Työtietojen ja omien tietojen pitäminen erillään

Organisaatiossasi voidaan tukea käyttäjän tai yrityksen omistamia laitteita. Kummassakin vaihtoehdossa voit saavuttaa IT-hallinnan tavoitteesi ja samalla pitää työntekijät tuottavina tehtäviensä parissa. Työtietoja ja käyttäjän omia tietoja hallitaan erikseen siten, että käyttökokemus on kuitenkin yhtenäinen. Näin viimeisintä huutoa oleva tuottavuusappi voi olla käyttäjän laitteella yritysappien vieressä, ja työntekijät voivat työskennellä vapaammin. iOS:ssä se onnistuu ilman muun valmistajan ratkaisuja, kuten säiliöitä, jotka vaikuttavat käyttökokemukseen ja saavat käyttäjät turhautumaan.

Erilaiset hallintamallit

Säiliöitä tarvitaan usein ratkaisemaan muiden alustojen ongelmia – joita iOS:ssä ei ole. Joissakin säiliöratkaisuissa käytetään eri käyttäjäprofiileja, jolloin yhdellä laitteella on kaksi eri ympäristöä. Toisissa keskitytään itse appien säiliöintiin koodipohjaisen integraation tai appien paketoinnin avulla. Nämä menetelmät luovat käyttäjille tuottavuusesteitä. Sellaisia voivat olla useisiin työtiloihin sisään- ja uloskirjautuminen tai omisteiseen koodiin pohjautuminen, joka usein aiheuttaa appien yhteensopimattomuutta käyttöjärjestelmän päivitysten kanssa.

Organisaatiossa, joissa säiliöitä ei enää käytetä, huomataan, että iOS:n natiivit hallintasäätimet mahdollistavat käyttäjille optimaalisen yksilöllisen kokemuksen ja kasvattavat heidän tuottavuuttaan. Sen sijaan, että vaikeuttaisit laitteiden käyttämistä sekä työhön että omiin tarkoituksiin, voit hallita tiedonkulkua saumattomasti kulissien takana käytäntöjen valvonnalla.

Yrityksen tietojen hallinta

iOS:ssä laitteita ei tarvitse lukita. Avainteknologiat hallitsevat yrityksen tiedonkulkua appien välillä ja estävät sen vuotamisen käyttäjän henkilökohtaisiin appeihin ja pilvipalveluihin.

Hallittu sisältö

Hallittu sisältö kattaa App Store -appien ja sisäisten appien, tilien, kirjojen ja domainien asennuksen, määrityksen, ylläpidon ja poistamisen.

- **Hallitut apit.** MDM:n avulla asennettuja appeja kutsutaan hallituiksi apeiksi. Ne voivat olla App Storen ilmaisia tai maksullisia appeja tai yrityksen sisäisiä räätälöityjä appeja. Ne kaikki voidaan asentaa langattomasti MDM:llä. Hallitut apit sisältävät usein luottamuksellista tietoa, ja niitä voidaan hallita kattavammin kuin käyttäjän lataamia appeja. MDM-palvelin voi tarvittaessa poistaa hallittuja appeja ja niihin liittyviä tietoja tai määrittää, että apit poistetaan, kun MDM-profiili poistetaan. Lisäksi MDM-palvelin voi estää hallittujen appien tietojen varmuuskopioinnin iTunesiin ja iCloudiin.
- **Hallitut tilit.** MDM voi auttaa käyttäjiä pääsemään alkuun nopeasti ottamalla heidän sähköposti-tilinsä ja muut tilinsä käyttöön automaattisesti. MDM-ratkaisun toimittajasta ja sisäisten järjestelmien integraatiosta riippuen tilien tietosisältöihin voidaan laittaa ennalta myös käyttäjän nimi, sähköpostiosoite ja tarvittaessa varmenteet todentamista ja allekirjoittamista varten. MDM:llä voidaan määrittää seuraavia tilityyppejä: IMAP/POP, CalDAV, tilatut kalenterit, CardDAV, Exchange ActiveSync ja LDAP.
- **Hallitut kirjat.** MDM:llä kirjoja, ePub-kirjoja ja PDF-dokumentteja voidaan automaattisesti siirtää käyttäjien laitteisiin, jotta työntekijöillä on aina kaikki tarvitsemansa. Hallittuja kirjoja voidaan jakaa vain muilla hallituilla apeilla tai lähettää sähköpostitse hallittuja tilejä käyttäen. Kun materiaaleja ei enää tarvita, ne voidaan poistaa etänä.

- **Hallitut domainit.** Safarilla ladattuja tiedostoja käsitellään hallittuina dokumentteina, jos ne ovat peräisin hallitusta domainista. Yksittäisiä verkko-osoitteita ja alidomaineja voidaan hallita. Jos käyttäjä esimerkiksi lataa PDF-tiedoston hallitusta domainista, domain vaatii, että PDF noudattaa kaikkia hallittujen dokumenttien asetuksia. Domainia seuraavat polut ovat oletusarvoisesti hallittuja.

Hallittu jakelu

Hallitussa jakelussa voit käyttää MDM-ratkaisua tai Apple Configurator 2:ta määrälisenssi-ohjelmasta (VPP) hankittujen appien ja kirjojen hallintaan. Jotta voit ottaa hallitun jakelun käyttöön, sinun on ensin yhdistettävä MDM-ratkaisusi VPP-tiliisi suojaustunnuksen avulla. Kun MDM-palvelin on liitetty VPP-ohjelmaan, voit jakaa appeja suoraan laitteille ilman, että käyttäjällä tarvitsee olla Apple ID. Käyttäjää kehotetaan asentamaan apit laitteelleen, kun ne ovat valmiina. Jos laite on valvottu, apit lähetetään laitteelle taustalla ilman, että käyttäjä näkee kehotuksia.

Säilytä appien täysi hallinta MDM-ratkaisussa määrittämällä appeja suoraan laitteille.

Hallittu appien määritys

Hallitussa appien määrityksessä MDM määrittää appeja natiivin iOS-hallintasovelluskehyksen avulla käyttöönoton aikana tai sen jälkeen. Sovelluskehyksen ansiosta kehittäjät tietävät, mitkä määritysasetukset tulee ottaa käyttöön, kun appi asennetaan hallittuna appina. Työntekijät voivat aloittaa tällä tavoin määritettyjen appien käyttämisen heti, ilman erityistä käyttöönottoa. IT-osastolla voidaan luottaa siihen, että apeissa käsitellään yrityksen tietoja suojatusti ja omisteista SDK:ta tai appien paketointia ei tarvita.

Appien kehittäjillä on mahdollisuus käyttää appien hallitun määrityksen ominaisuuksia, kuten appien määritys, appien varmuuskopioinnin esto, näyttökuvien esto ja apin tyhjennys etänä.

AppConfiq-yhteisö tarjoaa työkaluja ja parhaita käytäntöjä mobiilikäyttöjärjestelmien natiivi-ominaisuuksille. Yhteisön johtavat MDM-tarjoajat ovat kehittäneen standardimallin, jota kaikki appien kehittäjät voivat käyttää appien hallitun määrityksen tukemiseen. Yhteisö auttaa edistämään mobiililaitteiden käyttöönottoa yrityksissä mahdollistamalla yhtenäisemmän, avoimen ja selkeän tavan määrittää ja suojata mobiiliappeja.

Lisätietoja AppConfig-yhteisöstä saat osoitteesta www.appconfig.org.

Tiedonkulun hallinta

MDM-ratkaisut tarjoavat ominaisuuksia, joilla yrityksen tietoja voidaan hallita tarkasti siten, että niitä ei vuoda käyttäjän omiin appeihin ja pilvipalveluihin.

- **Hallittu avaaminen.** Avaamisen hallinta käyttää rajoituksia, jotka estävät hallituista lähteistä peräisin olevien liitteiden ja dokumenttien avaamisen ei-hallituissa kohteissa ja päinvastoin.

  Voit esimerkiksi estää sen, että organisaation hallitulla sähköpostitilillä oleva luottamuksellinen sähköpostiliite avattaisiin missään käyttäjän henkilökohtaisista apeista. Vain MDM:llä asennetut ja hallitut apit voivat avata tämän työdokumentin. Käyttäjän ei-hallitut omat apit eivät näy liitteen avaamiseen käytettävissä olevien appien luettelossa. Hallittujen appien, tilien, kirjojen ja domainien lisäksi myös useat laajennukset huomioivat hallitun avaamisen rajoituksen.

Yrityksen tietojen suojaamiseksi vain MDM:llä asennetut ja hallitut apit voivat avata työdokumentin.

- **Hallitut laajennukset.** Appien laajennuksilla muiden valmistajien kehittäjät voivat tarjota toimintoja muille apeille tai jopa keskeisille iOS:n sisäisille järjestelmille kuten Ilmoituskeskukselle, jolloin uudet yritystoiminnan työnkulut appien välillä ovat mahdollisia. Hallitun avaamisen käyttäminen estää ei-hallittuja laajennuksia toimimasta hallittujen appien kanssa. Seuraavissa esimerkeissä esitellään erilaisia laajennuksia:
  - **Dokumenttien tarjoajien laajennuksilla** tuottavuusapit voivat avata dokumentteja eri pilvipalveluista ilman, että niiden tarvitsee luoda tarpeettomia kopioita.
  - **Toimintojen laajennuksilla** käyttäjät voivat käsitellä tai katsella sisältöä toisessa apissa. Käyttäjät voivat esimerkiksi käyttää toimintoa, joka kääntää tekstiä toisesta kielestä suoraan Safarissa.
  - **Muokatut näppäimistölaajennukset** tarjoavat lisänäppäimistöjä, joita iOS:ssä ei ole sisäänrakennettuna. Hallittu avaaminen voi estää luvattomien näppäimistöjen näkymisen yritysapeissa.
  - **Tänään-laajennukset** eli widgetit tuovat yhdellä silmäyksellä nähtävää tietoa Ilmoituskeskuksen Tänään-näkymään. Tällä tavalla käyttäjät saavat välitöntä, ajantasaista tietoa apeista ja he voivat yksinkertaisilla toiminnoilla avata täyden apin katsoakseen lisätietoja.
  - **Jakolaajennuksilla** käyttäjät voivat kätevästi jakaa sisältöä muihin kohteisiin, kuten yhteisö- ja pilvipalveluihin. Esimerkiksi Jaa-painikkeen sisältävässä apissa käyttäjät voivat valita yhteisöpalvelun jakolaajennuksen ja julkaista sillä kommentteja tai muuta sisältöä.

Joustavat hallintavaihtoehdot

Applen hallintasovelluskehys on joustava ja tarjoaa tasapainoisen lähestymistavan sekä käyttäjien että yrityksen omistamien laitteiden hallintaan yrityksessä. Kun muun valmistajan MDM-ratkaisua käytetään iOS:n kanssa, laitteiden hallinnan vaihtoehtoja on useita hyvin avoimista menetelmistä aina tarkkaan hallintaan asti.

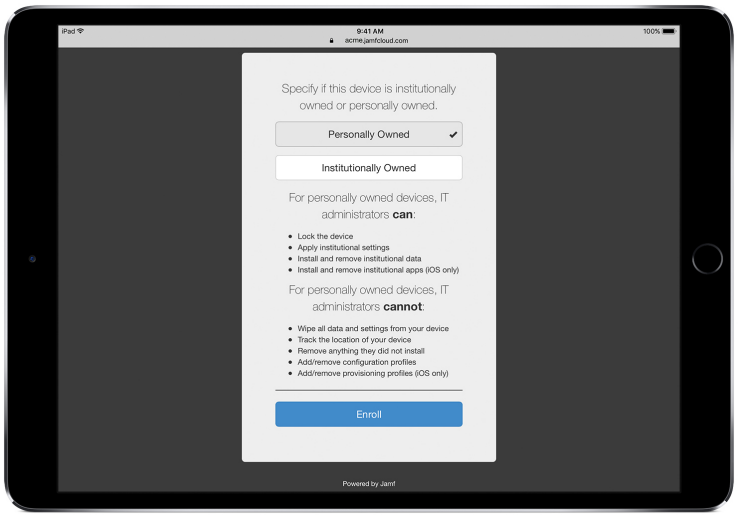
Omistusmallit

Organisaation omistusmallista tai -malleista riippuen laitteita ja appeja hallitaan eri tavoin. Kaksi yrityksissä yleisesti käytössä olevaa iOS-laitteiden omistusmallia ovat käyttäjän omistama ja organisaation omistama.

Käyttäjien omistamat laitteet

Käyttäjien omistamien laitteiden käyttöönotossa iOS tarjoaa käyttäjille yksilöllisen käyttöönoton ja läpinäkyvyyttä laitteiden määrityksessä. Käyttäjät voivat myös luottaa siihen, että yritys ei käytä heidän henkilökohtaisia tietojaan.

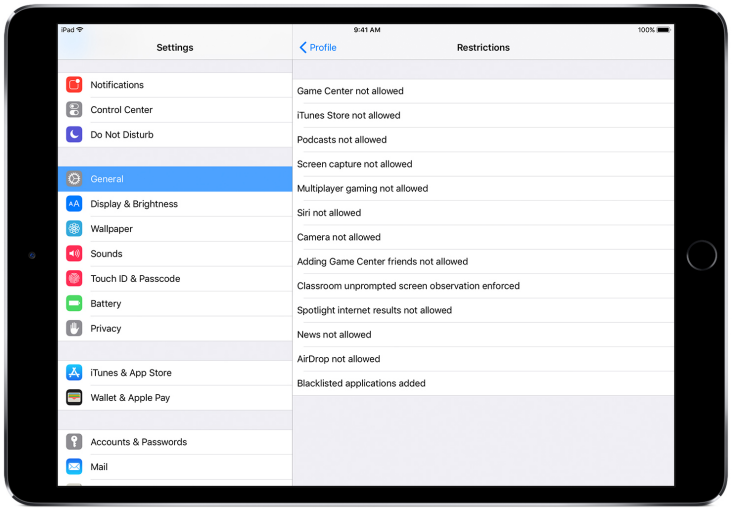
- **Vapaaehtoinen rekisteröityminen.** Vaikka laitteet ovat käyttäjien hankkimia ja määrittämiä (tästä käytetään yleisesti nimitystä BYOD), voidaan silti tarjota pääsy yrityspalveluihin kuten Wi-Fiin, sähköpostiin ja kalenteriin. Käyttäjien tarvitsee vain rekisteröityä yrityksen MDM-ratkaisuun. Kun käyttäjät rekisteröityvät MDM:ään ensimmäistä kertaa iOS-laitteella, heille kerrotaan, mitä MDM-palvelin voi heidän laitteellaan käyttää ja mitä ominaisuuksia se määrittää. Näin käyttäjät tietävät, mitä hallitaan, ja voivat luottaa yritykseen. On tärkeää kertoa käyttäjille, että jos he eivät ole tyytyväisiä hallintaan, he voivat irtautua siitä poistamalla hallintaprofiilin laitteeltaan. Jos he tekevät niin, kaikki MDM:n asentamat yritystilit ja apit poistetaan.



Muiden valmistajien MDM-ratkaisut tarjoavat työntekijöille usein käyttäjäystävällisen käyttöliittymän, jolloin he hyväksyvät sen mielellään rekisteröitymisen yhteydessä.*

*Näyttökuva: Jamf.

- **Enemmän läpinäkyvyyttä.** Kun käyttäjät ovat kirjautuneet MDM:ään, työntekijät voivat helposti katsoa Asetuksista, mitä appeja, kirjoja ja tilejä hallitaan ja mitä rajoituksia on käytössä. iOS merkitsee kaikki MDM:n asentamat yrityksen asetukset, tilit ja sisällöt hallituiksi.



Asetusprofiilien käyttöliittymällä käyttäjät näkevät Asetuksissa tarkasti, mitä heidän laitteelleen on asennettu.

- **Käyttäjien tietoturva.** Vaikka MDM-palvelin sallii yhteyden iOS-laitteisiin, kaikkia asetuksia ja tilitietoja ei paljasteta. Voit hallita MDM:n kautta välitettyjä yrityksen tilejä, asetuksia ja tietoja, mutta et pääse käyttäjän henkilökohtaisille tileille. Itse asiassa samat ominaisuudet, jotka suojaavat tiedot yrityksen hallitsemissa apeissa, estävät myös käyttäjän henkilökohtaista sisältöä joutumasta yrityksen datavirtaan.

  Seuraava esimerkki näyttää, mitä muun valmistajan MDM-palvelin näkee ja ei näe henkilökohtaisella iOS-laitteella:

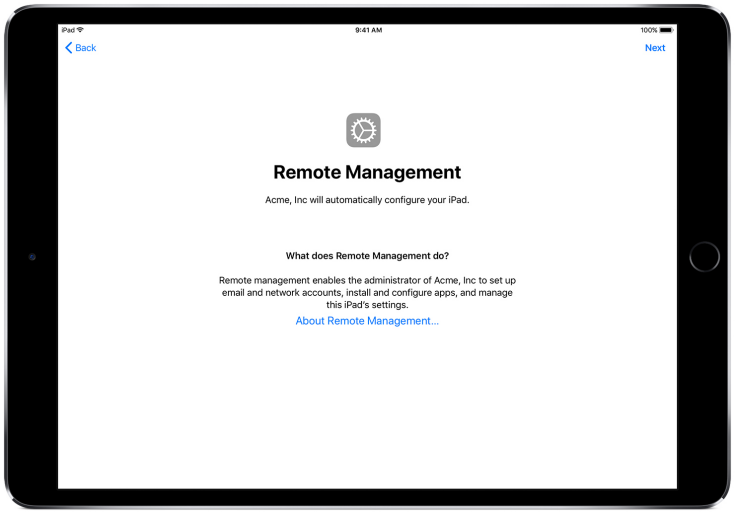
MDM näkee:	**MDM ei näe henkilökohtaisia tietoja, kuten:**
Laitteen nimen	Henkilökohtaisia tai työhön liittyviä sähköposteja, kalentereita, yhteystietoja
Puhelinnumeron	Teksti- tai iMessage-viestejä
Sarjanumeron	Safarin selaushistoriaa
Mallin nimen ja numeron	FaceTime- ja puhelulokeja
Kapasiteetin ja vapaan tilan	Henkilökohtaisia muistutuksia ja muistiinpanoja
iOS-versionumeron	Appien käyttötiheyttä
Asennetut apit	Laitteen sijaintia

- **Laitteiden personointi.** Yrityksissä on huomattu, että jos käyttäjien sallitaan personoida laite omalla Apple ID:llään, he osoittavat suurempaa omistajuutta ja vastuunkantoa. Heidän tuottavuutensa myös kasvaa, koska he voivat valita työhönsä parhaiten sopivat apit ja sisällön.

Organisaation omistamat laitteet

Organisaation omistamien laitteiden käyttöönotossa jokaiselle käyttäjälle voidaan tarjota laite, jolloin sitä kutsutaan personoiduksi käyttöönotoksi. Toinen vaihtoehto on kierrättää laitteita eri käyttäjillä, jolloin kyseessä on personoimaton käyttöönotto. iOS:n ominaisuudet kuten automaattinen rekisteröityminen, lukittavat MDM-asetukset, laitteiden valvonta ja Aina päällä -VPN varmistavat, että laitteet määritetään organisaatiosi vaatimusten mukaisesti. Näin varmistetaan parempi hallinta ja yrityksen tietojen suojaus.

- **Automaattinen rekisteröinti.** Laiterekisteröintiohjelmalla voidaan automatisoida MDM-rekisteröinti organisaation omistamien iPhone- ja iPad-laitteiden sekä Mac-järjestelmien käyttöönotossa. Voit tehdä rekisteröinnistä pakollisen ja pysyvän. Laitteita voidaan myös asettaa valvonnan alaiseksi rekisteröinnin yhteydessä, ja käyttäjien voidaan antaa ohittaa joitakin perusasennuksen vaiheita.



Laiterekisteröintiohjelman avulla MDM-ratkaisu määrittää iOS-laitteet automaattisesti käyttöönottoapurissa.

- **Valvotut laitteet.** Valvonta tarjoaa lisää hallintamahdollisuuksia organisaation omistamille iOS-laitteille. Niihin kuuluu muun muassa mahdollisuus suodattaa verkkoyhteyksiä yleisen välipalvelimen kautta, jotta voidaan varmistaa käyttäjän verkkoliikenteen pysyminen organisaation ohjeiden piirissä, ja mahdollisuus estää käyttäjiä palauttamasta laitetta tehdasasetuksiin. iOS-laitteet ovat oletusarvoisesti valvomattomia. Laitteita voidaan asettaa valvonnan alaiseksi automaattisesti laiterekisteröintiohjelman avulla tai käsin Apple Configurator 2:lla.

Vaikka et aikoisi nyt käyttää valvonnan ominaisuuksia, kannattaa harkita laitteiden asettamista valvonnan alaiseksi, kun niitä otetaan käyttöön. Silloin voit hyödyntää valvonnan ominaisuuksia tulevaisuudessa. Muutoin jo käyttöönotetut laitteet olisi tyhjennettävä. Valvonta ei tarkoita laitteen lukitsemista, vaan sillä voidaan parantaa yrityksen laitteita hallintamahdollisuuksia laajentamalla. Pitkällä tähtäimellä valvonta tarjoaa yrityksellesi enemmän mahdollisuuksia.

Jos haluat nähdä valvottujen ominaisuuksien koko luettelon, katso iOS:n käyttöönoton opas.

Rajoitukset

iOS tukee seuraavia rajoituskategorioita, jotka voit määrittää langattomasti vastaamaan organisaation tarpeita käyttäjien toimintaan vaikuttamatta:

- AirPrint
- Appien asennus
- Appien käyttö
- Oppitunti-appi
- Laite
- iCloud

- Profile Managerin käyttäjä- ja käyttäjäryhmäkohtaiset rajoitukset
- Safari
- Turvallisuus- ja tietosuoja-asetukset
- Siri

Myös seuraavat kategoriat sisältävät asetuksia, jotka voidaan määrittää MDM-ratkaisulla:

- Automaattiset MDM-rekisteröinnin asetukset
- Käyttöönottoapurin valikot

Hallinnan lisäominaisuudet

Laitekyselyt

Laitteiden määrityksen lisäksi MDM-palvelin voi myös kysellä laitteilta tietoja eri asioista kuten laitteistosta, verkosta, apeista sekä vaatimustenmukaisuus- ja suojaustiedoista. Näiden tietojen avulla voidaan varmistaa, että laitteet ovat jatkuvasti vaadittujen käytäntöjen mukaisia. MDM-palvelin määrittää tietojen keräystiheyden.

Seuraavat ovat esimerkkejä tiedoista, joita voidaan kysellä iOS-laitteelta:

- Laitteen tiedot (nimi)
- Malli, iOS-versio, sarjanumero
- Verkon tiedot
- Verkkovierailutila, MAC-osoitteet
- Asennetut apit
- Apin nimi, versio, koko
- Vaatimustenmukaisuus- ja suojaustiedot
- Asennetut asetukset, käytännöt, varmenteet
- Salauksen tila

Hallintatoimet

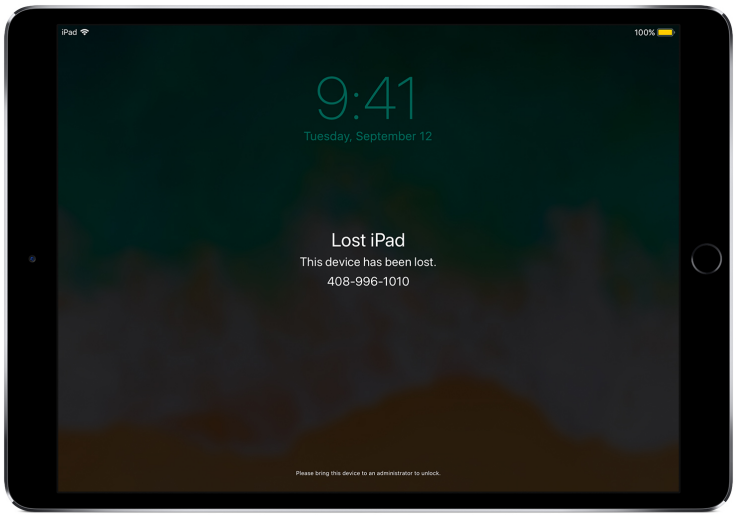
MDM-palvelin voi suorittaa hallitussa laitteessa useita erilaisia ylläpitotoimia, kuten määritysasetusten automaattinen muuttaminen ilman käyttäjän toimenpiteitä, iOS-version päivittäminen pääsykoodilla lukittuihin laitteisiin, laitteen lukitseminen tai tyhjentäminen etänä tai pääsykoodin lukituksen nollaaminen, jolloin käyttäjät voivat vaihtaa unohtuneet salasanat. MDM-palvelin voi myös kehottaa iOS-laitetta aloittamaan AirPlay-peilauksen tiettyyn kohteeseen tai lopettamaan nykyisen AirPlay-istunnon.

Kadonnut-tila

iOS 9.3:ssa tai uudemmassa MDM-ratkaisu voi asettaa valvotun laitteen Kadonnut-tilaan etänä. Se lukitsee laitteen ja sallii puhelinnumeron sisältävän viestin näyttämisen lukitulla näytöllä.

Kadonnut-tilan avulla kadonneet tai varastetut valvotut laitteet voidaan löytää, koska MDM kysyy etänä niiden sijaintia silloin, kun ne olivat viimeksi linjoilla. Kadonnut-tilan käyttämiseen ei tarvita Etsi iPhoneni -ominaisuutta.

Jos MDM laittaa Kadonnut-tilan etänä pois päältä, laitteen lukitus avataan ja sen sijainti tallennetaan. Läpinäkyvyyden säilyttämiseksi käyttäjälle ilmoitetaan, että Kadonnut-tila laitetaan pois päältä.



Kun MDM asettaa kadonneen laitteen Kadonnut-tilaan, se lukitsee laitteen, sallii viestien näyttämisen lukitulla näytöllä ja määrittää laitteen sijainnin.

Aktivointilukitus

iOS 7.1:ssä tai uudemmassa aktivointilukitus voidaan ottaa käyttöön MDM:llä, kun käyttäjä laittaa Etsi iPhoneni -ominaisuuden päälle valvotussa laitteessa. Näin organisaatio voi hyötyä aktivointilukituksen varkauden estämisen toiminnoista mutta silti ohittaa ominaisuuden esimerkiksi silloin, kun käyttäjä lähtee organisaatioista poistamatta aktivointilukitusta Apple ID:llään.

MDM-ratkaisu voi hakea ohituskoodin ja sallia käyttäjän ottaa aktivointilukituksen käyttöön laitteella seuraavasti:

- Jos Etsi iPhoneni on päällä, kun MDM sallii aktivointilukituksen, aktivointilukitus otetaan silloin käyttöön.
- Jos Etsi iPhoneni on pois päältä, kun MDM sallii aktivointilukituksen, aktivointilukitus otetaan käyttöön, kun käyttäjä seuraavan kerran aktivoi Etsi iPhoneni -ominaisuuden.

Yhteenveto

iOS-hallintasovelluskehys tarjoaa parhaat puolet molemmista: IT-osasto voi määrittää, hallita ja suojata laitteita sekä hallita niissä liikkuvia yrityksen tietoja, ja samalla käyttäjät voivat tehdä työnsä hyvin laitteilla, joita he mielellään käyttävät.