Gestire dispositivi e dati aziendali in iOS

Panoramica

Aziende di tutto il mondo stanno offrendo ai propri dipendenti la possibilità di lavorare al meglio con iPhone e iPad.

Indice

Il segreto di una strategia mobile di successo è trovare il giusto equilibro tra il livello di controllo da parte del reparto IT e la libertà di azione degli utenti sui dispositivi. Personalizzando i dispositivi iOS con le proprie app e i propri contenuti, gli utenti hanno maggior controllo e responsabilità, e di conseguenza sono più coinvolti e produttivi. Il merito va al framework di gestione di Apple, che fornisce modi intelligenti di gestire i dati e le app aziendali con discrezione, separando i dati corporate da quelli personali. In più, gli utenti comprendono come vengono gestiti i propri dispositivi e possono essere certi che la loro privacy sia al sicuro.

Questo documento illustra come garantire il controllo necessario da parte del reparto IT, offrendo allo stesso tempo agli utenti gli strumenti migliori per lavorare. È parte integrante della Guida di riferimento per la distribuzione di iOS, una risorsa tecnica online completa per la gestione e la distribuzione dei dispositivi iOS in azienda.

La Guida di riferimento per la distribuzione di iOS è disponibile su help.apple.com/deployment/ios.

Le basi della gestione

Per snellire le distribuzioni di iPhone e iPad, iOS offre varie soluzioni integrate che semplificano l'impostazione di account, la configurazione di criteri aziendali, la distribuzione di app e l'applicazione di restrizioni da remoto.

Il nostro approccio alla gestione

Il framework di gestione di Apple rappresenta il punto di partenza per gestire i dispositivi iOS. Integrato in iOS, permette alle organizzazioni di gestire solo ciò che è necessario, in modo discreto e non semplicemente bloccando o disabilitando alcune funzioni dei dispositivi. In questo modo, dispositivi, app e dati possono essere controllati nel dettaglio mediante una soluzione MDM di altre aziende, senza compromettere l'esperienza utente o la privacy dei dipendenti.

Alcune soluzioni di gestione dei dispositivi disponibili sul mercato potrebbero usare termini diversi per descrivere le proprie funzionalità, per esempio Enterprise Mobility Management (EMM) o Mobile Application Management (MAM). Tutte queste soluzioni hanno comunque lo stesso obiettivo: gestire over-the-air i dispositivi e i dati di un'azienda. E dato che il framework di gestione di Apple è integrato in iOS, non è necessario usare un'ulteriore applicazione agente del fornitore MDM.

Separare dati aziendali e dati personali

Indipendentemente dalla strategia di distribuzione scelta (con dispositivi di proprietà dell'azienda o degli utenti), è possibile raggiungere gli obiettivi prefissati in materia di gestione consentendo al contempo agli utenti di svolgere al meglio tutte le loro attività. Dati aziendali e dati personali vengono gestiti separatamente, senza compromettere l'esperienza utente. Significa che le migliori app per la produttività possono coesistere con quelle aziendali, permettendo ai dipendenti di lavorare liberamente. Con iOS, questo risultato può essere ottenuto senza usare soluzioni di altri fornitori come i contenitori, che risultano frustranti per gli utenti e compromettono la loro esperienza d'uso.

Comprendere i diversi modelli di gestione

Spesso i contenitori vengono creati per risolvere problemi di altre piattaforme, che non si verificano con iOS. Alcuni contenitori utilizzano una strategia con doppio utente, creando due ambienti separati sullo stesso dispositivo. Altri si concentrano sulla containerizzazione delle app mediante integrazione basata su codice o soluzioni di app wrapping. Molte di queste metodologie presentano degli ostacoli per la produttività degli utenti, come doversi connettere e disconnettere da più spazi di lavoro o dover aggiungere una dependency nel codice proprietario che spesso crea un'incompatibilità delle app con gli aggiornamenti dei sistemi operativi.

Le aziende che hanno smesso di usare i contenitori si stanno accorgendo che i controlli di gestione nativi in iOS garantiscono un'esperienza ottimale per gli utenti e li aiutano a essere più produttivi. Invece di complicare l'uso dei dispositivi a livello sia personale sia lavorativo, è possibile utilizzare i criteri per gestire facilmente il flusso di dati dietro le quinte.

Gestire i dati aziendali

Con iOS, non c'è bisogno di bloccare i dispositivi. Tecnologie chiave controllano il flusso dei dati aziendali tra le app ed evitano che possano raggiungere le app personali dell'utente o i servizi cloud.

Contenuti gestiti

La gestione dei contenuti include l'installazione, la configurazione, la gestione e la rimozione di app in-house personalizzate o dell'App Store, di account, libri e domini.

- **App gestite.** Le app installate via MDM sono dette "app gestite". Possono essere app gratuite o a pagamento dell'App Store o app in-house personalizzate, e si possono installare over-the-air con una soluzione MDM. Le app gestite spesso contengono informazioni sensibili e offrono un maggiore controllo rispetto alle app scaricate dall'utente. Il server MDM può rimuovere su richiesta le app gestite e i relativi dati, o specificare se le app devono essere eliminate contestualmente alla rimozione del profilo MDM. Inoltre, il server MDM può impedire che i dati delle app gestite vengano inclusi nei backup di iTunes e iCloud.
- **Account gestiti.** La gestione dei dispositivi mobili può aiutare gli utenti a impostare rapidamente e in automatico account di posta e altro. A seconda della soluzione MDM e dell'integrazione con i sistemi interni, i payload degli account possono essere precompilati con un nome utente, un indirizzo email e, se necessario, delle identità di certificati per l'autenticazione e la firma. È possibile configurare via MDM i seguenti tipi di account: IMAP/POP, CalDAV, calendari sottoscritti, CardDAV, Exchange ActiveSync e LDAP.
- **Libri gestiti.** Con la soluzione MDM si possono inviare in automatico libri, ePub e documenti PDF ai dispositivi degli utenti, che avranno sempre a disposizione tutto ciò di cui hanno bisogno. I libri gestiti possono essere condivisi solo con altre app gestite o inviati tramite email usando account gestiti. E quando i file non servono più, si possono rimuovere a distanza.

- **Domini gestiti.** I download da Safari sono considerati documenti gestiti se provengono da un dominio gestito. Si possono gestire URL e sottodomini specifici. Per esempio, se un utente scarica un PDF da un dominio gestito, il dominio richiede che il PDF sia conforme a tutte le impostazioni dei documenti gestiti. I percorsi che seguono il dominio sono gestiti per impostazione predefinita.

Distribuzione gestita

Con la distribuzione gestita, l'azienda può usare la propria soluzione MDM o Apple Configurator 2 per gestire le app e i libri acquistati tramite il Volume Purchase Program (VPP). La prima cosa da fare per abilitare la distribuzione gestita è collegare la soluzione MDM aziendale all'account VPP utilizzando un token di sicurezza. Una volta collegata la soluzione MDM al VPP, le app possono essere assegnate direttamente ai dispositivi, senza che gli utenti debbano avere un proprio ID Apple. Quando le app sono pronte per essere installate sul dispositivo, l'utente riceve una richiesta di autorizzazione. Se il dispositivo è supervisionato, le app vengono installate senza l'intervento dell'utente.

Configurazione delle app gestite

Con la configurazione delle app gestite, la soluzione MDM usa il framework di gestione nativo di iOS per configurare le app durante o dopo la distribuzione. Grazie a questo framework, gli sviluppatori possono identificare le impostazioni di configurazione che dovrebbero essere implementate quando la loro app viene installata come app gestita. I dipendenti possono iniziare a usare fin da subito le app che sono state configurate in questo modo, senza bisogno di un setup personalizzato. Il reparto IT ha la certezza che i dati aziendali all'interno delle app saranno gestiti in modo sicuro, senza dover usare soluzioni di app wrapping o SDK proprietari.

Per mantenere il pieno controllo delle app con una soluzione MDM, bisogna assegnare le app direttamente ai dispositivi.

Con la configurazione delle app gestite, gli sviluppatori possono attivare diverse funzioni; per esempio, possono configurare le app, impedirne i backup, cancellarle a distanza e disattivare l'acquisizione delle schermate.

L'AppConfig Community ha l'obiettivo di fornire strumenti e best practice sulle funzioni native dei sistemi operativi mobili. I principali fornitori di soluzioni MDM che fanno parte di questa community hanno definito uno schema standard che tutti gli sviluppatori possono usare per la configurazione delle app gestite. Rendendo la configurazione e la sicurezza delle app mobili più coerenti, aperte e semplici, la community incentiva l'adozione delle tecnologie mobili nelle aziende.

Per saperne di più sull'AppConfig Community: www.appconfig.org.

Flusso di dati gestito

Le soluzioni MDM offrono funzioni specifiche che permettono di gestire a livello granulare i dati aziendali per evitare che raggiungano le app personali dell'utente o i servizi cloud.

- **Funzione "Apri in" gestita.** Questa funzione utilizza una serie di restrizioni che impediscono agli utenti di aprire in destinazioni non gestite i documenti o gli allegati provenienti da fonti gestite, e viceversa.

  Per esempio, si può impedire che gli allegati email riservati negli account di posta gestiti dell'azienda vengano aperti nelle app personali dell'utente. Solo le app installate e gestite dalla soluzione MDM potranno aprire questi documenti di lavoro. Le app non gestite dell'utente non compariranno nemmeno nell'elenco delle app disponibili per aprire gli allegati. Le restrizioni della funzione "Apri in" gestita vengono rispettate non solo dalle app, gli account, i libri e i domini gestiti, ma anche da diverse estensioni.

Per proteggere i dati aziendali, solo le app installate e gestite via MDM possono aprire questo documento di lavoro.

- **Estensioni gestite.** Con le estensioni delle app, gli sviluppatori esterni possono fornire funzioni ad altre app o persino a sistemi chiave integrati in iOS, come Centro Notifiche, creando nuovi flussi di lavoro tra le app che prima non erano possibili. La funzione "Apri in" gestita impedisce l'uso di estensioni non gestite nelle app gestite. Ecco alcuni esempi dei vari tipi di estensioni.
  - **Estensioni per i fornitori di documenti.** Grazie a queste estensioni, le app per la produttività possono aprire documenti da svariati servizi cloud, senza dover creare inutili copie.
  - **Estensioni per le azioni.** Permettono agli utenti di visualizzare o modificare i contenuti di un'altra app. Per esempio, gli utenti possono usare un'azione per tradurre un testo in un'altra lingua direttamente in Safari.
  - **Estensioni per le tastiere personalizzate.** Forniscono tastiere diverse da quelle incluse in iOS. Con la funzione "Apri in" gestita è possibile impedire che tastiere non autorizzate appaiano nelle app aziendali.
  - **Estensioni per la vista Oggi.** Note anche come widget, sono usate per fornire informazioni consultabili a colpo d'occhio nella vista Oggi in Centro Notifiche. In questo modo gli utenti possono accedere all'istante alle informazioni aggiornate di un'app, e aprire l'app con semplici interazioni nel caso in cui vogliano saperne di più.

– **Estensioni per la condivisione.** Offrono agli utenti un modo comodo per condividere contenuti su altre destinazioni, come i social network o i servizi di upload. Per esempio, nelle app che includono un pulsante di condivisione, gli utenti possono scegliere un'estensione per la condivisione che rappresenta un social network e utilizzarla per postare un commento o altri contenuti.

Opzioni di gestione flessibili

Il framework di Apple è flessibile e offre un approccio equilibrato per la gestione dei dispositivi sia degli utenti sia di proprietà dell'azienda. Quando si usa una soluzione MDM di altri fornitori con iOS, sono disponibili diverse opzioni di gestione: in base alle esigenze dell'azienda, è possibile scegliere un approccio flessibile o un controllo rigoroso.

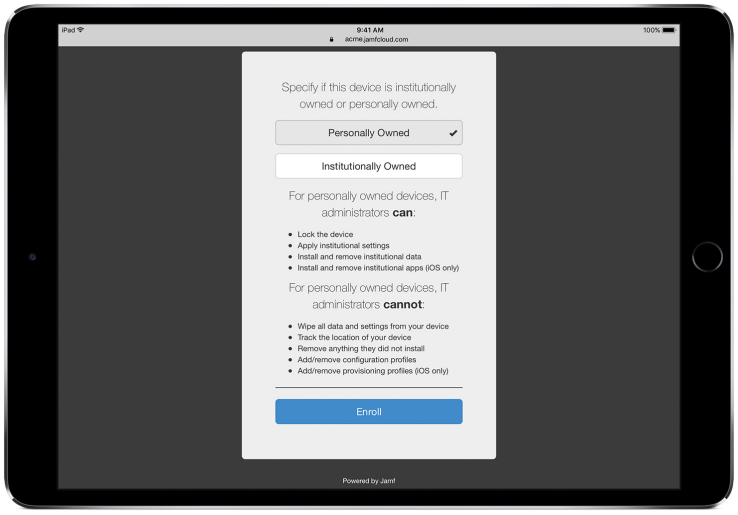
Modelli di proprietà

La gestione dei dispositivi e delle app di un'organizzazione cambia in base al modello o ai modelli di proprietà scelti. Nelle grandi aziende si usano prevalentemente due modelli di proprietà per i dispositivi iOS: dell'azienda o dell'utente.

Dispositivi di proprietà dell'utente

Nelle distribuzioni con dispositivi personali, iOS offre agli utenti la possibilità di personalizzare il setup e la massima trasparenza sul modo in cui i dispositivi vengono configurati. Inoltre, l'azienda non può in alcun modo accedere ai dati personali.

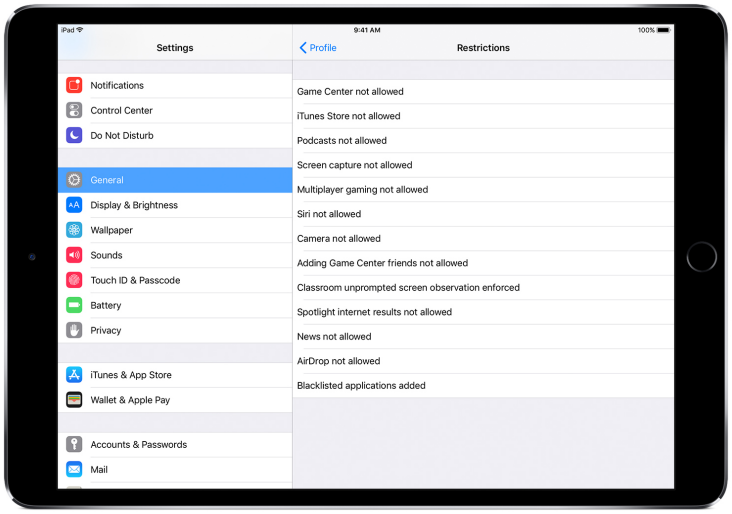
- **Possibilità di eseguire la registrazione o rinunciarvi.** Quando i dispositivi sono acquistati e configurati dall'utente (in quella che viene comunemente detta distribuzione BYOD), è comunque possibile garantire l'accesso ai servizi aziendali come Wi-Fi, posta elettronica e calendari. Gli utenti devono semplicemente registrare il dispositivo nella soluzione MDM dell'organizzazione. La prima volta che si registrano nella soluzione MDM su un dispositivo iOS, vengono informati sugli elementi a cui il server MDM può accedere e sulle funzioni che configurerà. In questo modo sanno esattamente cosa viene gestito e si stabilisce un rapporto di fiducia con l'azienda. È importante che gli utenti sappiano che, se non sono a proprio agio con questo tipo di gestione, possono rinunciarvi in qualsiasi momento rimuovendo il profilo di gestione dal dispositivo. Se lo faranno, tutti gli account e le app aziendali installati via MDM saranno rimossi.



Le soluzioni MDM di altre aziende presentano in genere un'interfaccia utente intuitiva, quindi per i dipendenti sarà semplice effettuare la registrazione.*

*Screenshot fornito da Jamf.

- **Maggiore trasparenza.** Dopo essersi registrati nella soluzione MDM, i dipendenti possono facilmente vedere in Impostazioni quali app, libri e account sono gestiti e le restrizioni che sono state impostate. Qualsiasi impostazione, account e contenuto installato dalla soluzione MDM è contrassegnato da iOS come "gestito".



L'interfaccia utente per i profili di configurazione in Impostazioni mostra con esattezza cosa è stato configurato sul dispositivo.

- **Privacy degli utenti.** Sebbene il reparto IT possa interagire con i dispositivi iOS attraverso il server MDM, non può visualizzare tutte le impostazioni e le informazioni sugli account. Può intervenire solo su account, impostazioni e informazioni aziendali fornite mediante MDM, perché le funzioni che proteggono i dati delle app aziendali gestite impediscono anche che i contenuti personali dell'utente entrino nel flusso di dati corporate.

  Gli esempi di seguito mostrano quello che un server MDM di altre aziende può e non può vedere su un dispositivo iOS personale.

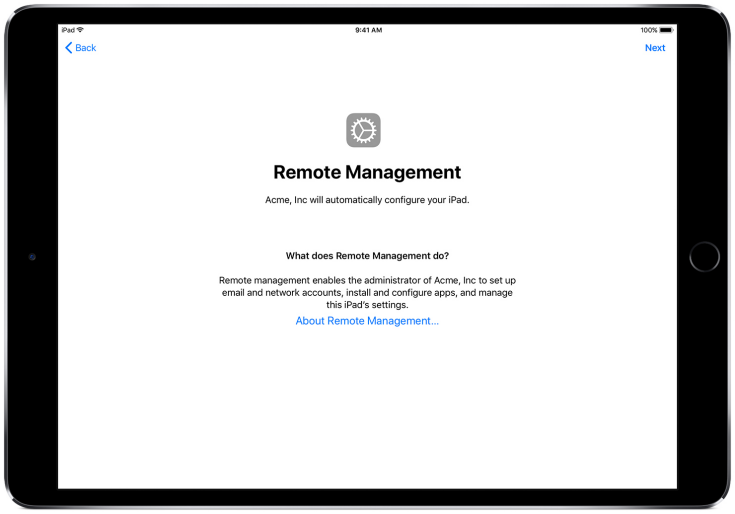
Il server MDM può vedere:	**Il server MDM non può vedere dati personali come:**
Nome del dispositivo	Email, calendari e contatti personali o aziendali
Numero di telefono	SMS o iMessage
Numero di serie	Cronologia di Safari
Nome e numero modello	Registri delle chiamate FaceTime o telefoniche
Capacità e spazio disponibile	Promemoria e note personali
Versione di iOS	Frequenza di utilizzo delle app
App installate	Posizione del dispositivo

- **Personalizzazione dei dispositivi.** Le aziende si sono rese conto che consentendo agli utenti di personalizzare il dispositivo con il proprio ID Apple offrono loro maggiore controllo e responsabilità. Non solo: la produttività dei dipendenti migliora, perché possono scegliere autonomamente le app e i contenuti di cui hanno bisogno per lavorare al meglio.

Dispositivi di proprietà dell'azienda

In uno scenario di distribuzione con dispositivi di proprietà dell'azienda, si può scegliere di dare un dispositivo a ogni dipendente, adottando il metodo definito come distribuzione individuale, o di far ruotare i dispositivi tra i dipendenti, adottando il metodo definito come distribuzione non individuale. Le funzioni di iOS, come la registrazione automatica, le impostazioni MDM bloccabili, la supervisione del dispositivo e il VPN sempre attivo assicurano che i dispositivi vengano configurati in base ai requisiti specifici dell'organizzazione, offrendo il massimo controllo e proteggendo al contempo i dati aziendali.

- **Registrazione automatizzata.** Il Device Enrollment Program (DEP) offre la possibilità di automatizzare la registrazione MDM durante il setup iniziale degli iPhone, iPad e Mac di proprietà dell'azienda. La registrazione può essere resa obbligatoria e irrevocabile. Si può anche scegliere di abilitare la modalità di supervisione dei dispositivi durante la registrazione ed evitare che gli utenti eseguano alcuni passaggi del setup di base.



Con il DEP, la soluzione MDM configurerà automaticamente i dispositivi iOS durante l'impostazione assistita.

- **Dispositivi supervisionati.** La supervisione fornisce un maggior controllo sui dispositivi di proprietà dell'organizzazione, permettendo per esempio di attivare un filtro web mediante proxy globale per garantire che il traffico web degli utenti rispetti le linee guida dell'azienda, impedire che gli utenti ripristinino i dispositivi alle impostazioni di fabbrica e molto altro. Per impostazione predefinita, i dispositivi iOS non sono supervisionati. La supervisione può essere attivata automaticamente con il DEP, oppure manualmente usando Apple Configurator 2.

Anche se non si prevede di usare subito le funzioni disponibili solo per i dispositivi supervisionati, consigliamo di attivare la supervisione al momento della configurazione, in modo da poter eventualmente utilizzare queste funzioni in futuro. Altrimenti, sarà necessario inizializzare i dispositivi che sono già stati distribuiti. Supervisionare i dispositivi non significa impostare dei blocchi; con la supervisione si possono migliorare i dispositivi di proprietà dell'azienda estendendo le funzioni di gestione. A lungo termine, la supervisione offre ancora più opzioni per le grandi aziende.

Per un elenco completo delle impostazioni supervisionate, consultare la Guida di riferimento per la distribuzione di iOS.

Restrizioni

iOS supporta le categorie di restrizioni elencate di seguito, che possono essere configurate over the air in base alle esigenze dell'azienda senza compromettere l'esperienza utente.

- AirPrint
- Installazione di app
- Uso delle app
- App Classroom
- Dispositivo
- iCloud
- Restrizioni per gli utenti e i gruppi di utenti in Gestore profilo

- Safari
- Impostazioni di sicurezza e privacy
- Siri

Per le seguenti categorie sono anche disponibili delle opzioni configurabili tramite la soluzione MDM.

- Impostazioni della registrazione MDM automatizzata
- Schermate di Impostazione Assistita

Funzioni di gestione aggiuntive

Interrogazione dei dispositivi

Oltre a configurare i dispositivi, il server MDM è in grado di interrogarli per ottenere una serie di informazioni, come dettagli sul dispositivo, sulla rete, sulle applicazioni e dati relativi a conformità e sicurezza, utili per garantire il rispetto dei criteri richiesti. Il server MDM determina la frequenza con cui raccogliere le informazioni.

Di seguito sono indicati alcuni esempi delle informazioni che si possono ottenere interrogando un dispositivo iOS.

- Dettagli sul dispositivo (nome)
- Modello, versione di iOS, numero di serie
- Informazioni di rete
- Stato del roaming, indirizzi MAC
- App installate
- Nomi, versione e dimensioni delle app
- Dati su conformità e sicurezza
- Impostazioni, criteri e certificati installati
- Stato della crittografia

Attività di gestione

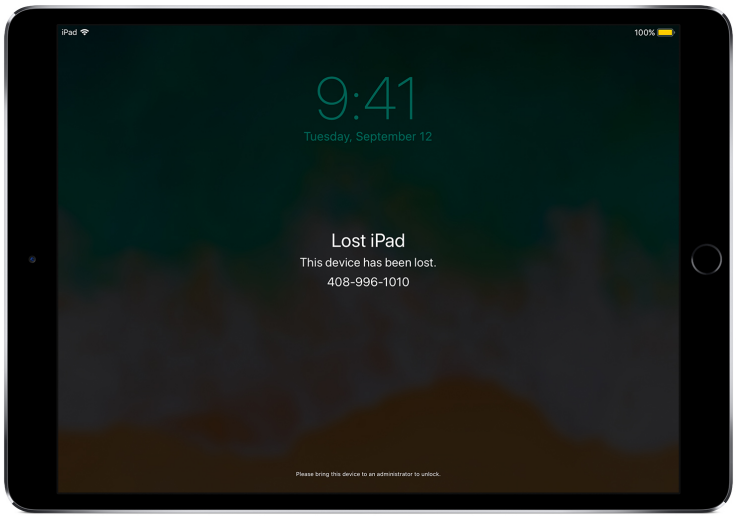
Se i dispositivi sono gestiti, il server MDM può eseguire svariate attività di amministrazione, per esempio modificare le impostazioni di configurazione in automatico senza l'intervento dell'utente, aggiornare iOS sui dispositivi protetti da codice d'accesso, bloccare o inizializzare un dispositivo da remoto, oppure rimuovere un codice di blocco per permettere all'utente di reimpostare la password. Il server MDM può anche richiedere a un dispositivo iOS di avviare la duplicazione AirPlay su una specifica destinazione o di terminare la sessione AirPlay in corso.

Modalità Smarrito

Con iOS 9.3 o versioni successive, la soluzione MDM può impostare un dispositivo supervisionato in modalità Smarrito da remoto. Questa azione blocca il dispositivo e permette di mostrare un messaggio con un numero di telefono sulla schermata di blocco.

Con la modalità Smarrito, i dispositivi supervisionati che sono stati rubati o persi possono essere localizzati dalla soluzione MDM, che li interroga da remoto per conoscere la posizione in cui si trovavano l'ultima volta che erano online. La modalità Smarrito non richiede l'attivazione di "Trova il mio iPhone".

Se la soluzione MDM disattiva da remoto la modalità Smarrito, il dispositivo viene sbloccato e ne viene rilevata la posizione. Per garantire trasparenza, l'utente riceve una notifica quando la modalità Smarrito viene disattivata.



Quando si attiva la modalità Smarrito per un dispositivo, la soluzione MDM lo blocca, ne determina la posizione e consente di mostrare dei messaggi sullo schermo.

Blocco di attivazione

Con iOS 7.1 o versioni successive, è possibile usare una soluzione MDM per abilitare il blocco di attivazione quando un utente attiva "Trova il mio iPhone" su un dispositivo supervisionato. In questo modo l'azienda può sfruttare la funzione antifurto del blocco di attivazione, permettendo comunque di eluderla se, per esempio, un utente lascia l'organizzazione senza aver prima rimosso il blocco di attivazione con il proprio ID Apple.

La soluzione MDM può recuperare un codice di elusione e permettere all'utente di abilitare il blocco di attivazione sul dispositivo, conformemente ai seguenti scenari:

- Se "Trova il mio iPhone" viene attivato quando la soluzione MDM consente di abilitare il blocco di attivazione, anche quest'ultimo viene attivato.
- Se "Trova il mio iPhone" viene disattivato quando la soluzione MDM consente di abilitare il blocco di attivazione, quest'ultimo verrà attivato quando l'utente riattiverà "Trova il mio iPhone".

Riepilogo

Con il framework di gestione di iOS il rovescio della medaglia non esiste: da una parte, il reparto IT può configurare e gestire i dispositivi, garantirne la sicurezza e controllare il flusso dei dati aziendali, dall'altra, gli utenti possono lavorare al meglio con i dispositivi che amano di più.