Guida di riferimento per la distribuzione di iOS

T019-00124/2015-04

Contenuto

Guida di riferimento per la distribuzione di iOS 1

Introduzione

Questa guida di riferimento si rivolge agli amministratori IT che vogliono gestire i dispositivi iOS sulle proprie reti. Contiene informazioni sulla distribuzione e la gestione di iPad, iPhone e iPod touch in organizzazioni aziendali o didattiche di grandi dimensioni. Viene spiegato come vengono fornite le seguenti funzionalità:

- Integrazione con l'infrastruttura esistente
- Sicurezza a livello globale
- Strumenti avanzati per la distribuzione
- Metodi di distribuzione di app e libri a dipendenti e studenti

Nota: Anche se la presente guida di riferimento ha come oggetto esclusivo la distribuzione di dispositivi iOS, alcuni paragrafi sono validi anche per computer desktop Apple e computer portatili. In questi casi, verrà utilizzato il termine *dispositivi Apple* per indicare iPhone, iPad, iPod touch, computer desktop Mac e computer portatili. La distribuzione di Apple TV è descritta nel capitolo AirPlay di questa guida di riferimento.

La guida è suddivisa nei seguenti capitoli:

Modelli di distribuzione
I metodi possibili per distribuire i dispositivi iOS all'interno di un'organizzazione sono molteplici. A prescindere dal modello di distribuzione scelto, è utile prendere in considerazione i passi da compiere per garantire uno svolgimento il più possibile privo di difficoltà. Questa guida copre tutti gli aspetti di una distribuzione di dispositivi iOS, ma le aziende e gli istituti didattici potrebbero aver bisogno di procedere in maniera differente le une dagli altri.

Configurazione Wi-Fi
I dispositivi Apple possono connettersi in sicurezza a reti Wi-Fi aziendali o per ospiti fin da subito, permettendo agli utenti di accedere in maniera semplice e veloce ai network wireless sia quando sono in sede sia quando sono in viaggio. In questo capitolo vengono descritti i protocolli Wi-Fi standard per la trasmissione e la codifica dei dati.

Infrastruttura e integrazione
I dispositivi iOS supportano da subito un'ampia gamma di infrastrutture di rete. Questa sezione spiega quali sono le tecnologie usate da iOS e alcune linee guida per l'integrazione con Microsoft Exchange, VPN e altri servizi standard.

Servizi Internet
Apple ha realizzato un solido set di servizi per aiutare gli utenti a trarre il massimo vantaggio dai propri dispositivi Apple. Questi servizi includono iMessage, FaceTime, Continuity, iCloud, Portachiavi iCloud e la procedura di configurazione e gestione degli ID Apple utilizzati per accedere a tali servizi.

Considerazioni sulla sicurezza

iOS è progettato per accedere in modo sicuro ai servizi aziendali e proteggere i dati importanti. iOS fornisce una solida codifica per i dati in trasmissione, metodi di autenticazione collaudati per accedere ai servizi aziendali e codifica hardware per tutti i dati archiviati sui dispositivi iOS. Leggi questa sezione per una panoramica sulle funzioni di sicurezza di iOS.

Configurazione e gestione

I dispositivi Apple supportano tecnologie e strumenti evoluti che ti permettono di impostarli facilmente, di configurarli secondo le tue esigenze e di gestirli agevolmente in un'ambiente di grandi dimensioni. Questa sezione descrive gli strumenti disponibili per la distribuzione, inclusa una panoramica sulla gestione dei dispositivi mobili (MDM) e sul Device Enrollment Program.

Distribuzione di app e libri

Esistono vari modi per distribuire app e contenuti nella tua organizzazione. I programmi ideati da Apple, come il Volume Purchase Program e l'iOS Developer Enterprise Program, consentono alla tua organizzazione di acquistare, sviluppare e distribuire app e libri per i tuoi utenti. Leggi questa sezione per scoprire i dettagli di questi programmi e come distribuire le app e i libri acquistati o sviluppati per l'uso interno.

Pianificare l'assistenza

Apple offre una vasta gamma di programmi e di opzioni per l'assistenza agli utenti Apple. Prima di iniziare la distribuzione dei dispositivi Apple, scopri le opzioni più adatte alla tua organizzazione e pianifica eventuali esigenze in fatto di assistenza.

Le seguenti appendici contengono ulteriori dettagli tecnici e requisiti:

Restrizioni MDM

Informazioni sulle restrizioni che puoi utilizzare per configurare i dispositivi iOS in base alle tue esigenze in fatto di sicurezza, codici di accesso e altro.

Installare app in-house in modalità wireless

Informazioni su come distribuire app in-house usando il tuo portale web.

Risorse aggiuntive

- www.apple.com/it/education/it
- www.apple.com/ipad/business/it
- www.apple.com/iphone/business/it

Nota: Puoi trovare una versione web di questa guida di riferimento all'indirizzo https://help.apple.com/deployment/ios.

Nota: Se iBooks Store è disponibile nel tuo paese o nella tua area, puoi scaricare questa guida di riferimento in formato ePub. Cerca *Guida di riferimento per la distribuzione di iOS*.

Modelli di distribuzione 2

Panoramica

Per distribuire e configurare i dispositivi iOS, sono disponibili varie opzioni possibili, dalla pre-configurazione alla configurazione self-service da parte degli studenti o dei dipendenti. Esplora le varie possibilità prima di iniziare. Il modello di distribuzione determinerà anche gli strumenti e i processi utilizzati per la stessa.

- In ambito didattico, i modelli di distribuzione per i dispositivi iOS sono tipicamente tre: Modello one-to-one di proprietà dell'istituzione, modello di proprietà dello studente e modello condiviso. Sebbene gran parte degli istituti abbiano un modello di preferenza, nel tuo istituto potresti avere più modelli.
- Nelle aziende, i metodi possibili per distribuire i dispositivi iOS all'interno dell'organizzazione sono molteplici. Sia che scegliate di distribuire dispositivi iOS di proprietà dell'azienda, di condividere i dispositivi iOS tra i dipendenti o di consentire ai dipendenti di utilizzare i propri dispositivi personali, è utile prendere in considerazione tutti i passi necessari, così da garantire una distribuzione priva di difficoltà.

Una volta identificati i modelli di distribuzione, il tuo team può esplorare nel dettaglio le capacità di distribuzione e gestione offerte da Apple. Tali strumenti e programmi vengono trattati in maniera approfondita in questa guida di riferimento, che dovrebbe essere consultata insieme alle principali parti interessate della tua organizzazione.

Modelli di distribuzione in ambito didattico

Panoramica

iPad porta nelle aule una serie di strumenti straordinari. La scelta delle strategie e degli strumenti giusti può aiutare a trasformare l'esperienza didattica per gli insegnanti, gli studenti e altri utenti.

Sia che il tuo istituto distribuisca i dispositivi iOS in una singola aula o che lo faccia per tutte le classi, le opzioni per una facile distribuzione e gestione di dispositivi iOS e contenuti sono molteplici.

Modelli di distribuzione

Negli istituti didattici, i più comuni modelli di distribuzione per i dispositivi iOS sono tre:

- Modello one-to-one di proprietà dell'istituzione
- Modello di proprietà dello studente
- Modello condiviso

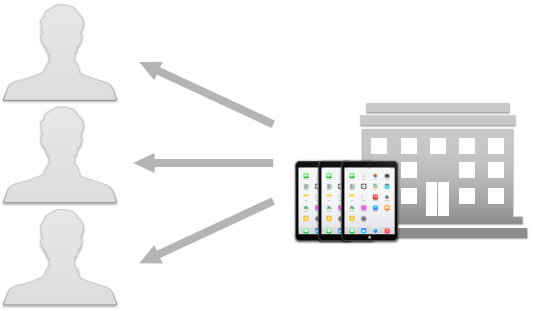
Sebbene gran parte degli istituti abbiano un modello di preferenza, nel tuo istituto potresti averne più di uno.

Di seguito vengono presentati alcuni esempi di come tali modelli verrebbero applicati in un tipico istituto didattico.

- Una scuola media può pianificare e distribuire un modello one-to-one di proprietà dell'istituto per tutte le classi.
- Un grande distretto scolastico può inizialmente distribuire un modello one-to-one di proprietà dell'istituto in una singola scuola superiore, quindi lanciare gli stessi modelli in tutto il distretto.
- Un istituto comprensivo può distribuire sia un modello one-to-one di proprietà dell'istituto per le scuole medie e uno condiviso per la scuola materna e per le elementari.
- In ambito universitario, è comune trovare il modello per studenti sia a livello di polo che interpolo.

L'esplorazione dettagliata di questi modelli di distribuzione sarà di aiuto per identificare quello più adatto al tuo ambito specifico.

Modello one-to-one di proprietà dell'istituzione



Un modello di distribuzione one-to-one di proprietà dell'istituto fornisce più opportunità ai dispositivi iOS di influire positivamente sul processo di apprendimento.

In una tipica distribuzione one-to-one di proprietà dell'istituto, l'istituto acquista dispositivi iOS per tutti gli studenti e gli insegnanti idonei. Questo potrebbe voler dire per una classe in particolare, per un dipartimento o per un intero distretto, facoltà o ateneo.

Con questo modello, a ogni utente viene assegnato un dispositivo iOS configurato e gestito dall'istituto. Una soluzione MDM di gestione dei dispositivi mobili può aiutare a semplificare e automatizzare il processo. Se i dispositivi iOS vengono acquistati direttamente da Apple o da un rivenditore o un gestore autorizzati da Apple che partecipano al programma, l'istituto può utilizzare il programma di registrazione di dispositivi (DEP) per automatizzare la registrazione alla MDM e distribuire i dispositivi iOS direttamente agli utenti.

Una volta che i dispositivi iOS sono stati distribuiti, gli utenti seguono una configurazione guidata ottimizzata, vengono automaticamente registrati nella MDM e possono ulteriormente personalizzare i dispositivi iOS e scaricare i propri contenuti. Gli utenti possono inoltre ricevere un invito a scaricare contenuti didattici specifici, come app e libri acquistati tramite il VPP (Volume Purchase Program) o corsi di iTunes U. Se gli studenti hanno un'età inferiore ai 13 anni, l'istituto può avviare la creazione di un ID Apple a loro nome tramite l'apposito programma ID Apple per studenti, in modo da poter inviare loro app e libri. L'istituto può distribuire o aggiornare tali risorse via etere in qualsiasi momento durante l'anno scolastico e con un server cache gran parte di questi download può provenire dalla rete locale dell'istituto stesso. Se i dispositivi iOS sono supervisionati, le app vengono installate automaticamente.

La seguente tabella illustra le responsabilità dell'amministratore e dell'utente di una distribuzione one-to-one di proprietà dell'istituto:

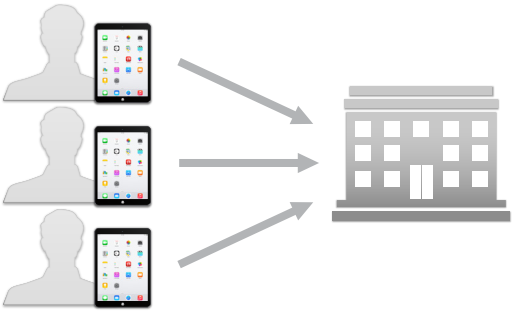
Preparazione	
Amministratore: • Ricercare, ottenere e distribuire una soluzione MDM. • Registrarsi ai programmi DEP, VPP e ID Apple per studenti. • Rimuovere il dispositivo iOS dalla confezione e (facoltativamente) etichettarlo. • Iniziare a creare ID Apple per studenti minori di 13 anni (se applicabile).	**Utenti:** • Creare ID Apple e account iTunes Store e iCloud.
Configurazione e gestione	
Amministratore: • Assegnare i dispositivi iOS al DEP per la supervisione e la registrazione ottimizzata alla MDM. • Utilizzare Apple Configurator anziché DEP e MDM per configurare e supervisionare i dispositivi iOS. • Configurare e installare account, impostazioni e restrizioni in modalità wireless con la MDM.	**Utenti:** • All'utente viene fornito un dispositivo iOS. • Inserire le credenziali dell'istituto nella configurazione guidata per il DEP (facoltativo). • Personalizzare il dispositivo iOS tramite "Impostazione assistita" e inserire un ID Apple personale. • Le impostazioni e le configurazioni del dispositivo iOS vengono ricevute automaticamente dalla MDM.
Distribuzione di dispositivi e contenuti	
Amministratore: • Acquistare app e libri tramite il VPP e assegnarli agli utenti tramite la MDM. • Inviare inviti del VPP agli utenti. • Installare il server cache per velocizzare la distribuzione dei contenuti sulla rete locale.	**Utenti:** • Accettare l'invito al VPP. • Scaricare e installare app e libri assegnati dall'istituto. • Se il dispositivo iOS è supervisionato, le app possono essere inviate al dispositivo senza notifiche all'utente.
Gestione in itinere	
Amministratore: • Revocare e riassegnare app ad altri utenti a seconda delle necessità tramite la MDM. • Con la MDM, un amministratore può controllare i dispositivi iOS gestiti per verificarne la conformità o visualizzare degli avvisi se gli utenti aggiungono app o contenuti non approvati. • La MDM può anche bloccare i dispositivi iOS o cancellare da remoto gli account o i dati gestiti oppure cancellare completamente il dispositivo iOS. • Distribuire Apple TV per supportare AirPlay.	**Utenti:** • Eseguire il backup del dispositivo iOS su iTunes o iCloud, per salvare i documenti e altri contenuti personali. • Se il dispositivo iOS viene smarrito o rubato, l'utente lo può localizzare con "Trova il mio iPhone".

Risorse aggiuntive

- VPP Panoramica
- MDM Panoramica
- DEP (Device Enrollment Program)
- ID Apple per studenti
- ID Apple

- Caching Server
- AirPlay
- Apple Configurator

Modello con dispositivi di proprietà dello studente



In ambito universitario,comunemente gli studenti sono in possesso di dispositivi iOS propri. Anche se non è un'abitudine diffusa, in alcuni istituti comprensivi gli studenti portano in aula i propri dispositivi iOS.

In questo modello, i dispositivi iOS vengono configurati dallo studente o da un genitore. Affinché possano utilizzare i servizi d'istituto come Wi-Fi, e-mail e calendari o essere configurati secondo i requisiti di un particolare corso, i dispositivi iOS di proprietà dello studente vengono di norma registrati in una soluzione MDM fornito dall'istituto. Negli ambienti didattici, una tecnologia come la MDM può avere un ruolo fondamentale nella gestione dei dispositivi iOS di proprietà dello studente. L'accesso ai servizi di un'istituto funge da incentivo per gli utenti a registrare i propri dispositivi iOS alla soluzione MDM dell'organizzazione.

Ciò garantisce che tutte le impostazioni di configurazione, i criteri, le restrizioni, le app, i libri e i contenuti vengano distribuiti in maniera automatica e non intrusiva, rimanendo sempre sotto il controllo dell'istituto. La registrazione alla MDM è un processo su autorizzazione, quindi gli studenti, una volta che avranno completato il corso, si saranno laureati o abbandoneranno l'istituto, possono rimuovere tale registrazione. La rimozione di questo tipo di gestione comporta la rimozione anche dei contenuti o dei servizi forniti dall'istituto stesso.

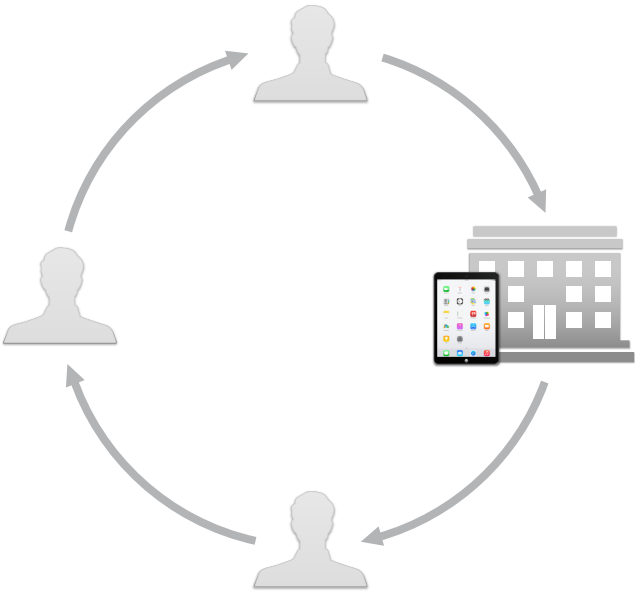
La seguente tabella illustra le responsabilità dell'amministratore e dell'utente di una distribuzione di proprietà dello studente:

Preparazione	
Amministratore: • Ricercare, ottenere e distribuire una soluzione MDM. • Registrarsi al programma VPP.	**Utenti:** • Rimuovere il dispositivo iOS dalla confezione e attivarlo. • Creare ID Apple e account iTunes Store e iCloud, se applicabile.
Configurazione e gestione	
Amministratore: • Nessuna azione necessaria in questa fase.	**Utenti:** • Registrare i dispositivi iOS in maniera autonoma e configurare account, impostazioni e restrizioni in modalità wireless via MDM in base ai criteri utente e di gruppo stabiliti dall'istituto. • Personalizzare i dispositivi iOS tramite "Impostazione assistita" e (facoltativamente) inserire un ID Apple personale. • Registrarsi alla MDM.
Distribuzione di app e libri	
Amministratore: • Acquistare app e libri tramite il VPP e assegnarli agli utenti tramite la MDM. • Inviare inviti del VPP agli utenti. • Installare il server cache per velocizzare la distribuzione dei contenuti sulla rete locale.	**Utenti:** • Accettare l'invito al VPP. • Scaricare e installare app e libri assegnati dall'istituto. • Aggiornare iOS e le app sul dispositivo iOS.
Gestione in itinere	
Amministratore: • Revocare e riassegnare app ad altri utenti a seconda delle necessità tramite la MDM. • Con la MDM, un amministratore può controllare i dispositivi iOS gestiti per verificarne la conformità o visualizzare degli avvisi se gli utenti aggiungono app o contenuti non approvati. • La MDM può anche bloccare i dispositivi iOS o cancellare da remoto gli account o i dati gestiti oppure cancellare completamente il dispositivo iOS.	**Utenti:** • Eseguire il backup del dispositivo su iTunes o iCloud, per salvare i documenti e altri contenuti personali. • Se il dispositivo iOS viene smarrito o rubato, l'utente lo può localizzare con "Trova il mio iPhone". • Una volta che la relazione MDM viene rimossa, gli account e i dati gestiti vengono rimossi, ma le app, i libri, i dati e i contenuti personali dell'utente vengono mantenuti. ***Nota:*** I libri VPP vengono assegnati in modo permanente e non possono essere revocati.

Risorse aggiuntive

- VPP Panoramica
- MDM Panoramica
- ID Apple
- Caching Server

Modello condiviso



In un modello condiviso, i dispositivi iOS vengono acquistati per l'utilizzo in un'aula o laboratorio e durante la giornata possono essere condivisi tra gli studenti. Tali dispositivi hanno possibilità di personalizzazione limitate, quindi non possono sfruttare al massimo un ambiente di apprendimento personalizzato per ciascuno studente. Oltre a offrire la possibilità di far girare i dispositivi con un modello per l'uso condiviso, questo approccio può anche essere utilizzato per una distribuzione uno a uno in un contesto altamente controllato, come nella scuola primaria o secondaria. In questo caso i dispositivi hanno una personalizzazione minima.

Le distribuzioni per uso condiviso sono caratterizzate da una gestione più rigida rispetto a quelle personalizzate, dal momento che la configurazione e la gestione sono eseguite dal personale dell'istituto. In una distribuzione per uso condiviso è l'istituto a prendersi la responsabilità dell'installazione delle app, dei libri e degli altri contenuti necessari all'apprendimento.

La seguente tabella illustra le responsabilità dell'amministratore e dell'utente di una distribuzione per uso condiviso:

Preparazione	
Amministratore: • Ricercare, ottenere e distribuire una soluzione MDM. • Registrarsi al programma VPP. • Rimuovere il dispositivo iOS dalla confezione e (facoltativamente) etichettarlo. • Creare ID Apple istituzionali per ogni istanza di Apple Configurator.	**Utenti:** • Nessuna azione necessaria in questa fase.

Configurazione e gestione	
Amministratore: • Utilizzare Apple Configurator per configurare e supervisionare i dispositivi. • Utilizzare Apple Configurator per registrare i dispositivi alla MDM (facoltativo). • Utilizzare Apple Configurator o la MDM per installare account, impostazioni e restrizioni.	**Utenti:** • Nessuna azione necessaria in questa fase.

Distribuzione di app	
Amministratore: • Acquistare app tramite il VPP e distribuirle utilizzando codici di riscatto per l'installazione e la gestione con Apple Configurator.	**Utenti:** • Nessuna azione necessaria in questa fase.

Gestione in itinere	
Amministratore: • Aggiornare iOS sul dispositivo con Apple Configurator. • Aggiornare, configurare e installare account, impostazioni e restrizioni in modalità wireless con Apple Configurator o la MDM. • Ripristinare periodicamente i dispositivi alla configurazione standard con Apple Configurator. • Installare e aggiornare app sul dispositivo iOS con Apple Configurator. • Con la MDM, puoi controllare i dispositivi iOS gestiti per verificarne la conformità o visualizzare degli avvisi se gli utenti aggiungono app o contenuti non approvati. • La MDM può anche bloccare i dispositivi iOS o cancellare da remoto gli account o i dati gestiti oppure cancellare completamente il dispositivo iOS. • È necessario eseguire regolarmente un backup del Mac su cui è in esecuzione Apple Configurator, perché gli acquisti VPP vengono gestiti localmente.	**Utenti:** • Nessuna azione necessaria in questa fase.

Risorse aggiuntive

- VPP Panoramica
- MDM Panoramica
- ID Apple
- Apple Configurator

Modelli di distribuzione in ambito aziendale

Panoramica

I dispositivi iOS sono in grado di dare un sostanziale impulso alla tua azienda. Essi sono in grado di potenziare la produttività e dare ai tuoi dipendenti la libertà e la flessibilità di lavorare in maniera nuova, sia in ufficio sia in viaggio.

Adottare questo nuovo modo di lavorare porta vantaggi all'intera organizzazione. Gli utenti hanno un migliore accesso alle informazioni, tanto da sentire di avere il controllo della situazione ed essere in grado di risolvere i problemi in maniera creativa. Essendo di supporto a iOS, i dipartimenti informatici vengono visti come parte integrante della strategia aziendale e, piuttosto che occuparsi di riparare guasti informatici e di tagliare i costi, si trovano a risolvere problemi reali. Essenzialmente i vantaggi si estendono a tutti, con dipendenti rinvigoriti e nuove opportunità di affari ovunque.

Sia che la tua organizzazione sia grande o piccola, i modi per distribuire e gestire in maniera semplice i dispositivi iOS e i contenuti sono molteplici.

Inizia con l'identificazione del modello di distribuzione che più si adatta alla tua organizzazione. In base al modello scelto, Apple fornisce diversi strumenti di distribuzione e di gestione.

Modelli di distribuzione

Nelle aziende, i più comuni modelli di distribuzione per i dispositivi iOS sono tre:

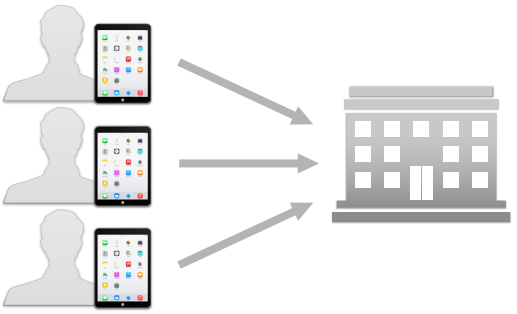
- Dispositivo personalizzato (di proprietà dell'utente)
- Dispositivo personalizzato (di proprietà dell'azienda)
- Non personalizzato (dispositivo condiviso)

Sebbene gran parte delle organizzazioni abbiano un modello di preferenza, nella tua organizzazione potresti averne più di uno.

Ad esempio, un'organizzazione commerciale potrebbe adottare una strategia con dispositivi personalizzati di proprietà dell'utente, permettendo ai dipendenti di configurare i propri iPad personali, ma mantenendo comunque separate le risorse aziendali dai dati e dalle app personali dell'utente. Tuttavia, i punti vendita dell'azienda potrebbero anche adottare una strategia con dispositivi non personalizzati, come iPod touch da condividere tra i vari dipendenti per permettere loro di elaborare le transazioni con i clienti.

L'esplorazione dettagliata di questi modelli di distribuzione sarà di aiuto per identificare quello più adatto al tuo ambito specifico.

Dispositivo personalizzato (di proprietà dell'utente)



Con una distribuzione basata sui dispositivi di proprietà dell'utente, gli utenti configurano i propri dispositivi iOS personali utilizzando il proprio ID Apple. Per poter accedere alla risorse aziendali, gli utenti possono configurare le impostazioni manualmente, installare un profilo di configurazione o più comunemente, registrare il dispositivo iOS con la soluzione MDM dell'organizzazione.

Un vantaggio dell'utilizzo della MDM per registrare i dispositivi iOS personali è la possibilità di mantenere le risorse aziendali separate dai dati e dalle app personali dell'utente. È possibile forzare impostazioni, monitorare la conformità con i requisiti dell'azienda e rimuovere dati e app aziendali, lasciando al tempo stesso inalterati i dati e le app sul dispositivo iOS di ciascun utente.

La seguente tabella illustra le responsabilità dell'amministratore e dell'utente di una distribuzione con dispositivi personalizzati (di proprietà dell'utente):

Preparazione	
Amministratore:	**Utenti:**
• Valutare l'infrastruttura esistente, tra cui Wi-Fi, VPN e server di posta e di calendario. • Ricercare, ottenere e distribuire una soluzione MDM. • Registrarsi al programma VPP.	• Rimuovere il dispositivo iOS dalla confezione e attivarlo. • Creare ID Apple e account iTunes Store e iCloud, se applicabile.

Configurazione e gestione	
Amministratore:	**Utenti:**
• Le organizzazioni possono fornire agli utenti impostazioni per gli account individuali e i criteri possono essere inviati tramite Exchange o installati tramite un profilo di configurazione.	• Registrare i dispositivi iOS in maniera autonoma e configurare account, impostazioni e restrizioni in modalità wireless via MDM in base ai criteri utente e di gruppo stabiliti dall'organizzazione. • Le impostazioni e le configurazioni del dispositivo iOS vengono ricevute automaticamente dalla MDM. • In alternativa, gli utenti possono installare profili di configurazione manualmente o configurare le impostazioni fornite da te.

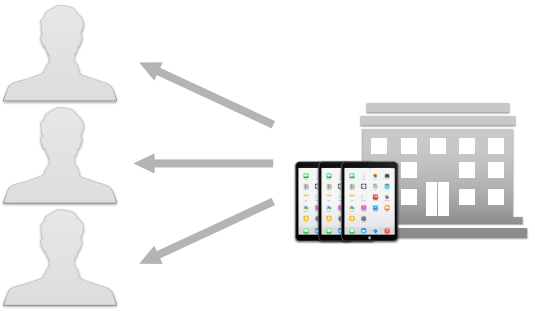
Distribuzione di app e libri	
Amministratore:	**Utenti:**
• Acquistare app e libri tramite il VPP e assegnarli agli utenti tramite la MDM. • Inviare inviti del VPP agli utenti. • Distribuire app interne da iOS Developer Enterprise Program e libri in-house caricandoli su un server web o sulla soluzione MDM. • Installare il server cache per velocizzare la distribuzione dei contenuti sulla rete locale.	• Accettare l'invito al VPP. • Scaricare e installare app e libri assegnati dall'organizzazione.

Gestione in itinere	
Amministratore:	**Utenti:**
• Revocare e riassegnare app ad altri utenti a seconda delle necessità tramite la MDM. • Con la MDM, puoi controllare i dispositivi iOS gestiti per verificarne la conformità o visualizzare degli avvisi se gli utenti aggiungono app o contenuti non approvati. • La MDM può anche bloccare i dispositivi iOS o cancellare da remoto gli account o i dati gestiti oppure cancellare completamente il dispositivo iOS.	• Eseguire il backup del dispositivo iOS su iTunes o iCloud, per salvare i documenti e altri contenuti personali. • Se il dispositivo viene smarrito o rubato, l'utente lo può localizzare con "Trova il mio iPhone". • Una volta che la relazione MDM viene rimossa, gli account e i dati gestiti vengono rimossi, ma le app, i libri, i dati e i contenuti personali dell'utente vengono mantenuti.

Risorse aggiuntive

- VPP Panoramica
- MDM Panoramica
- ID Apple
- Caching Server

Dispositivo personalizzato (di proprietà dell'azienda)



Puoi utilizzare il modello basato sui dispositivi personalizzati per distribuire i dispositivi iOS di proprietà della tua organizzazione. Puoi configurare i dispositivi iOS con impostazioni di base prima di consegnarli agli utenti oppure (come per quelli di proprietà dell'utente), fornire istruzioni o profili di configurazione affinché gli utenti le applichino autonomamente.

In alternativa, puoi chiedere agli utenti di registrare i dispositivi iOS con una soluzione MDM che fornirà loro impostazioni e app via etere. Gli utenti potranno in seguito personalizzare i dispositivi iOS con le proprie app e i propri dati, che resteranno separati da quelli gestiti dall'organizzazione. Se i dispositivi vengono acquistati direttamente da Apple o da un rivenditore o un gestore autorizzati da Apple che partecipano al programma, l'organizzazione può utilizzare il programma di registrazione di dispositivi (DEP) per automatizzare la registrazione alla MDM e distribuire i dispositivi iOS direttamente agli utenti oppure spedirli agli utenti e attivarli da remoto.

La seguente tabella illustra le responsabilità dell'amministratore e dell'utente di una distribuzione con dispositivi personalizzati (di proprietà dell'azienda):

Preparazione

Amministratore:

- Valutare l'infrastruttura esistente, tra cui Wi-Fi, VPN e server di posta e di calendario.
- Ricercare, ottenere e distribuire una soluzione MDM.
- Registrarsi al DEP e al VPP.

Utenti:

- Creare ID Apple e account iTunes Store e iCloud, se applicabile.

Configurazione e gestione

Amministratore:

- Dal sito del DEP, collegare il server virtuale alla soluzione MDM.
- Ottimizzare la registrazione attraverso il DEP assegnando i dispositivi iOS ai server MDM virtuali per numero di ordine o numero di serie.
- Assegnare i dispositivi iOS al DEP per la supervisione e la registrazione ottimizzata alla MDM.
- Utilizzare Apple Configurator per configurare e supervisionare il dispositivo iOS (alternativa alla precedente).
- Configurare e installare account, impostazioni e restrizioni in modalità wireless con la MDM o tramite USB con Apple Configurator.

Utenti:

- All'utente viene fornito un dispositivo iOS. Se il dispositivo è stato configurato tramite Apple Configurator, l'utente non deve effettuare ulteriori configurazioni.
- Inserire le credenziali dell'organizzazione nella configurazione guidata per il DEP (facoltativo).
- Personalizzare il dispositivo iOS tramite "Impostazione assistita" e inserire un ID Apple personale.
- Registrarsi alla MDM.
- Le impostazioni e le configurazioni del dispositivo iOS vengono ricevute automaticamente dalla MDM.

Distribuzione di app e libri

Amministratore:

- Scaricare il token dallo store VPP e collegarlo alla soluzione MDM.
- Acquistare app e libri tramite il VPP e assegnarli agli utenti tramite la MDM.
- Inviare inviti del VPP agli utenti.
- Distribuire app interne da iOS Developer Enterprise Program e libri in-house caricandoli su un server web o sulla soluzione MDM.
- Installare il server cache per velocizzare la distribuzione dei contenuti sulla rete locale.

Utenti:

- Accettare l'invito al VPP.
- Scaricare e installare app e libri assegnati dall'organizzazione.
- Se il dispositivo iOS è supervisionato, le app possono essere inviate al dispositivo senza notifiche all'utente.

Gestione in itinere

Amministratore:

- Revocare e riassegnare app ad altri utenti a seconda delle necessità tramite la MDM.
- Con la MDM, puoi controllare i dispositivi iOS gestiti per verificarne la conformità o visualizzare degli avvisi se gli utenti aggiungono app o contenuti non approvati.
- La MDM può anche bloccare i dispositivi iOS o cancellare da remoto gli account o i dati gestiti oppure cancellare completamente il dispositivo iOS.

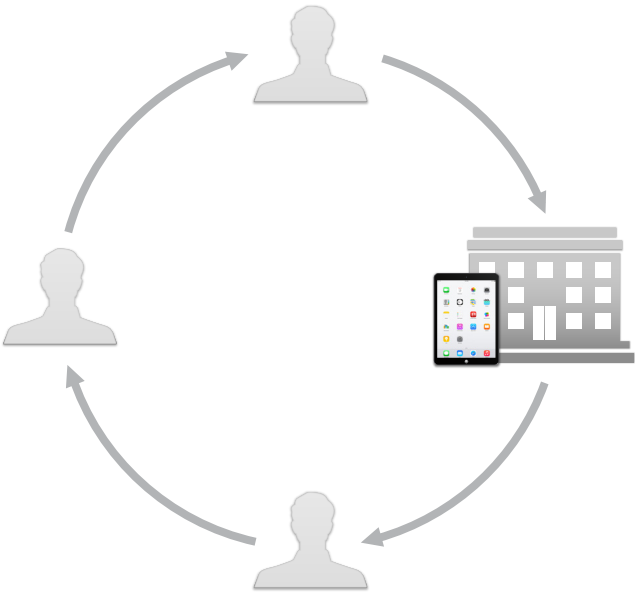
Utenti:

- Eseguire il backup del dispositivo iOS su iTunes o iCloud, per salvare i documenti e altri contenuti personali.
- Se il dispositivo viene smarrito o rubato, l'utente lo può localizzare con "Trova il mio iPhone".

Risorse aggiuntive

- VPP Panoramica
- MDM Panoramica
- DEP (Device Enrollment Program)
- ID Apple
- Caching Server
- Apple Configurator

Dispositivo non personalizzato (condiviso)



Se i dispositivi iOS sono condivisi tra più persone o utilizzati per un singolo scopo (come in un ristorante o in un albergo), normalmente vengono configurati e gestiti dall'amministratore piuttosto che da un utente individuale. Con una distribuzione basata su dispositivi non personalizzati, di norma gli utenti non archiviano dati personali né hanno la possibilità di installare app.

I dispositivi non personalizzati sono solitamente supervisionati tramite Apple Configurator e registrati con una soluzione MDM. In questo modo se i contenuti sul dispositivo vengono modificati dall'utente, essi possono essere aggiornati o ripristinati.

La seguente tabella illustra le responsabilità dell'amministratore e dell'utente di una distribuzione con dispositivi non personalizzati (condivisi):

Preparazione	
Amministratore: • Valutare l'infrastruttura esistente, tra cui Wi-Fi, VPN e server di posta e di calendario. • Ricercare, ottenere e distribuire una soluzione MDM. • Registrarsi al VPP.	**Utenti:** • Nessuna azione necessaria in questa fase.

Configurazione e gestione

Amministratore:

- Rimuovere il dispositivo iOS dalla confezione e (facoltativamente) etichettarlo.
- Utilizzare Apple Configurator per configurare e supervisionare i dispositivi.
- Utilizzare Apple Configurator per registrare i dispositivi alla MDM (facoltativo).
- Utilizzare Apple Configurator o la MDM per installare account, impostazioni e restrizioni.

Utenti:

- Nessuna azione necessaria in questa fase.

Distribuzione di app

Amministratore:

- Acquistare app tramite il VPP e distribuirle con Apple Configurator.
- Distribuire app in-house da iOS Developer Enterprise Program tramite Apple Configurator.
- Distribuire libri in-house caricandoli su un server web o sulla soluzione MDM.

Utenti:

- Nessuna azione necessaria in questa fase.

Gestione in itinere

Amministratore:

- Aggiornare iOS sul dispositivo con Apple Configurator.
- Aggiornare, configurare e installare account, impostazioni e restrizioni in modalità wireless con Apple Configurator o la MDM.
- Ripristinare periodicamente i dispositivi alla configurazione standard con Apple Configurator.
- Installare e aggiornare app sul dispositivo con Apple Configurator.
- Con la MDM, puoi controllare i dispositivi iOS gestiti per verificarne la conformità o visualizzare degli avvisi se gli utenti aggiungono app o contenuti non approvati.
- La MDM può anche bloccare i dispositivi iOS o cancellare da remoto gli account o i dati gestiti oppure cancellare completamente il dispositivo iOS.

Utenti:

- Nessuna azione necessaria in questa fase.

Risorse aggiuntive

- VPP Panoramica
- MDM Panoramica
- ID Apple
- Apple Configurator

Wi-Fi 3

Panoramica

Quando si prepara l'infrastruttura Wi-Fi per la distribuzione di dispositivi Apple, occorre considerare vari fattori:

- Throughput Wi-Fi
- Soglia di attivazione Wi-Fi
- Area da coprire
- Numero e densità dei dispositivi che si collegheranno alla rete Wi-Fi
- Tipo di dispositivi Apple e loro specifiche Wi-Fi
- Tipo e quantità di dati da trasferire
- Esigenze relative alla sicurezza nell'accesso alla rete wireless
- Esigenze relative alla codifica

L'elenco non è completo, ma include alcuni dei principali fattori da considerare nella predisposizione di una rete Wi-Fi.

Nota: Questa sezione si concentra sulle reti Wi-Fi così come vengono predisposte in Nord America. I tipi di predisposizione potrebbero essere differenti in altri paesi.

Throughput Wi-Fi

Nel pianificare la distribuzione dei dispositivi iOS all'interno della tua organizzazione, assicurati che la rete Wi-Fi e le infrastrutture di supporto siano solide e aggiornate. Un accesso continuo e affidabile a una rete potente è fondamentale per la configurazione dei dispositivi iOS. Inoltre, la capacità di supportare più dispositivi iOS con connessioni simultanee da parte di tutti i dipendenti, studenti o insegnanti è importante per il successo de programma.

Importante: Gli utenti e i loro dispositivi iOS devono avere accesso alla rete wireless e ai servizi Internet per effettuare la configurazione. Se tali dispositivi non riescono ad accedere ai server di attivazione di Apple, a iCloud o a iTunes Store, potresti aver bisogno di configurare il proxy web o le porte del firewall in modo da autorizzare tutto il traffico di rete dai dispositivi Apple alla rete Apple (17.0.0.0/8). Per un elenco delle porte utilizzate dai dispositivi Apple, consulta l'articolo del supporto Apple Porte TCP e UDP utilizzate dai prodotti software Apple.

Accesso Wi-Fi

Gli utenti possono impostare i dispositivi Apple affinché si connettano automaticamente alle reti Wi-Fi disponibili. Nel caso siano richieste credenziali di accesso o altre informazioni, è possibile connettersi direttamente dalle impostazioni Wi-Fi o da app come Mail, senza aprire una sessione separata del browser. Inoltre la connettività Wi-Fi persistente e a bassa potenza consente alle app di utilizzare le reti wireless per inviare notifiche push. Puoi configurare le impostazioni per le reti wireless, la sicurezza, i proxy e l'autenticazione utilizzando i profili di configurazione o la gestione dei dispositivi mobili.

Per ulteriori informazioni su come iOS sceglie la rete wireless a cui accedere automaticamente, consulta l'articolo del supporto Apple In che modo iOS decide a quale rete wireless accedere automaticamente.

WPA2 Enterprise

I dispositivi Apple supportano i protocolli di rete wireless standard di settore, tra cui WPA2 Enterprise, grazie ai quali è possibile accedere in modo sicuro alle reti Wi-Fi aziendali. WPA2 Enterprise utilizza la codifica a 128 bit AES, che garantisce agli utenti la protezione dei loro dati.

Con il supporto per 802.1X, i dispositivi iOS possono essere integrati in un'ampia gamma di ambienti di autenticazione RADIUS. I protocolli di autenticazione wireless 802.1X supportati da iOS comprendono: EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, IKEv2, PEAPv0, PEAPv1 e LEAP.ara.

Roaming

Per consentire il roaming all'interno delle reti Wi-Fi aziendali di grandi dimensioni, iOS è compatibile con i protocolli 802.11k e 802.11r.

La soglia di attivazione è rappresentata dal livello di segnale minimo richiesto da un client per mantenere la connessione attuale.

I dispositivi iOS controllano e mantengono la connessione al BSSID attuale finché il valore RSSI non supera la soglia di -70 dBm. Una volta superato tale valore, iOS avvia una scansione alla ricerca di possibili BSSID per effettuare il roaming pre l'ESSID attuale.

Questa è un'informazione è importante da valutare durante la definizione delle celle wireless e della relativa sovrapposizione di segnale prevista. Ad esempio, se le celle da 5 GHz vengono definite in base a una sovrapposizione pari a -67 dBm:

- iOS utilizza -70 dBm come soglia di attivazione e pertanto si manterrà connesso al BSSID attuale più a lungo del previsto.
- Rivedi la modalità di misurazione della sovrapposizione delle celle. Le antenne di un computer portatile sono più grandi e potenti rispetto a quelle di uno smartphone o un tablet. I dispositivi iOS rilevano pertanto limiti di cella diversi dal previsto. È sempre buona norma eseguire delle misurazioni utilizzando il dispositivo di destinazione.

802.11k consente al dispositivo iOS di rilevare rapidamente i punti di accesso più vicini disponibili per il roaming. Quando l'intensità del segnare del punto di accesso attuale si riduce e il dispositivo deve passare a un nuovo punto di accesso, esso conoscerà già il punto di accesso migliore a cui connettersi.

802.11r semplifica il processo di autenticazione utilizzando una funzionalità definita Fast Basic Service Set Transition (FT) o Fast BSS transition (FT) quando il dispositivo iOS passa da un punto di accesso a un altro sulla stessa rete. FT consente ai dispositivi iOS di associarsi ai punti di accesso più rapidamente. A seconda del fornitore dell'hardware Wi-Fi, FT può funzionare sia con il metodo di autenticazione basato sulle chiavi precondivise (PSK) che con il metodo 802.1X.

Nota: Non tutti i fornitori di hardware per reti Wi-Fi supportano 802.11k e 802.11r. Contatta il produttore dell'hardware Wi-Fi (controller e punti di accesso) per verificare se tali configurazioni sono supportate. Dopo aver verificato il supporto per entrambi gli standard, devi abilitare 802.11k e la funzionalità FT. I metodi di configurazione possono variare. Consulta la documentazione di configurazione più aggiornata relativa all'hardware Wi-Fi in uso per ulteriori informazioni.

Nella tabella riportata di seguito sono elencati quali dispositivi iOS supportano gli standard 802.11k e 802.11r con iOS. Anche se un dispositivo iOS non supporta lo standard 802.11r, in iOS 5.1 è stato aggiunto il supporto per il caching PMKID (Pairwise Master Key Identifier), che può essere utilizzato con alcuni dispositivi Cisco per ottimizzare il roaming tra punti di accesso. Potrebbero essere necessari altri SSID per supportare sia dispositivi iOS con FT sia dispositivi iOS con caching PMKID.

Dispositivo iOS	Supporto per 802.11k/r	Metodi supportati da iOS 6 e versioni successive	Metodi supportati da iOS di versioni precedenti alla 6
iPad Air 2, iPad mini 3, iPhone 6, iPhone 6 Plus, iPhone 5s. iPhone 5c, iPad Air, iPad mini con display Retina, iPad (4a generazione), iPad mini, iPhone 5, iPod touch (5a generazione)	Sì	FT, caching PMKID	Non applicabile
iPad (3a generazione), iPhone 4s	Sì	FT, caching PMKID	Caching PMKID
iPad (2a generazione) e versioni precedenti, iPhone 4 e versioni precedenti, iPod touch (4ta generazione) e versioni precedenti	No	Caching PMKID	Caching PMKID

- Prima di iOS 5.1, in iOS non esistevano metodi di ottimizzazione del roaming dei punti di accesso.
- La funzionalità SKC (Sticky Key Caching) è una forma di caching PMKID. SKC non è equivalente a né compatibile con la funzionalità OKC (Opportunistic Key Caching).

Per visualizzare la documentazione di riferimento relativa al roaming wireless di Apple, consulta l'articolo del supporto Apple iOS 8: guida di riferimento sul roaming wireless per clienti aziendali. Per ulteriori informazioni sul roaming con gli standard 802.11k e 802.11r, consulta l'articolo del supporto AppleiOS: roaming su reti Wi-Fi con gli standard 802.11k e 802.11r.

Pianificare in base a copertura e capacità

Per l'uso dei dispositivi Apple è fondamentale garantire una copertura Wi-Fi, ma è altrettanto importante progettare la rete in base alla densità di dispositivi che verranno utilizzati in una data area per garantire la capacità adeguata.

La maggior parte degli odierni punti di accesso di classe aziendale può gestire fino a più di 50 client Wi-Fi, ma l'esperienza utente non è delle migliori se un numero così alto di dispositivi utilizza effettivamente un singolo punto di accesso 802.11n. La fruibilità da parte di ciascun utente dipende dalla disponibilità di banda sul canale utilizzato dal dispositivo e dal numero di dispositivi che condividono tale banda. Più dispositivi utilizzano lo stesso canale, più la relativa velocità di rete diminuisce. Nel predisporre la propria rete Wi-Fi, quindi, bisogna tenere in considerazione quanti dispositivi Apple la useranno.

Importante: Evita l'utilizzo di SSID (Service Set Identifier) nascosti, perché i dispositivi Wi-Fi devono ricercarli in maniera attiva. Ciò porta a ritardi nel ristabilire la connessione al SSID, con potenziali effetti negativi sul flusso dei dati e sulle comunicazioni. Inoltre, nascondere il SSID non porta alcun vantaggio a livello di sicurezza. Gli utenti tendono a cambiare frequentemente posizione e dispositivi Apple, quindi i SSID nascosti spesso provocano ritardi nell'associazione alla rete e riducono le prestazioni del roaming. Questa pratica può far utilizzare più energia rispetto a un SSID visibile e pertanto ridurre la durata della batteria del dispositivo.

Scegliere tra 2,4 GHz e 5 GHz

In Nord America, le reti Wi-Fi che operano a 2,4 GHz offrono 11 canali. Tuttavia, dovendo considerare anche eventuali interferenze tra i canali, dovrebbero essere usati solo i canali 1, 6 e 11.

I segnali a 5 GHz non hanno la stessa capacità di quelli a 2,4 GHz di oltrepassare i muri o altre barriere, e questo riduce la copertura della rete. Pertanto, utilizza reti a 5 GHz se prevedi un'alta densità di dispositivi in spazi chiusi come aule o grandi sale riunioni. Il numero di canali disponibili sulla banda a 5 GHz varia in base al produttore e al Paese, ma saranno sempre disponibili almeno otto canali.

I canali a 5 GHz non si sovrappongono e offrono un significativo vantaggio rispetto ai tre canali non sovrapponibili disponibili sulla banda a 2,4 GHz. Quando si progetta una rete Wi-Fi a elevata densità di dispositivi Apple, i canali aggiuntivi offerti dalle reti a 5 GHz diventano un'importante considerazione strategica.

Importante: La copertura wireless dovrebbe estendersi a tutte le aree del luogo di lavoro. Se vengono utilizzati dispositivi obsoleti, nella progettazione occorre tenere in considerazione entrambe le bande Wi-Fi, sia quella da 2,4 GHz 802.11b/g/n sia quella da 5 GHz 802.11a/n/ac.

Considerazioni sulla progettazione

Durante la fase di progettazione delle reti Wi-Fi, devi tenere presente tre considerazioni fondamentali.

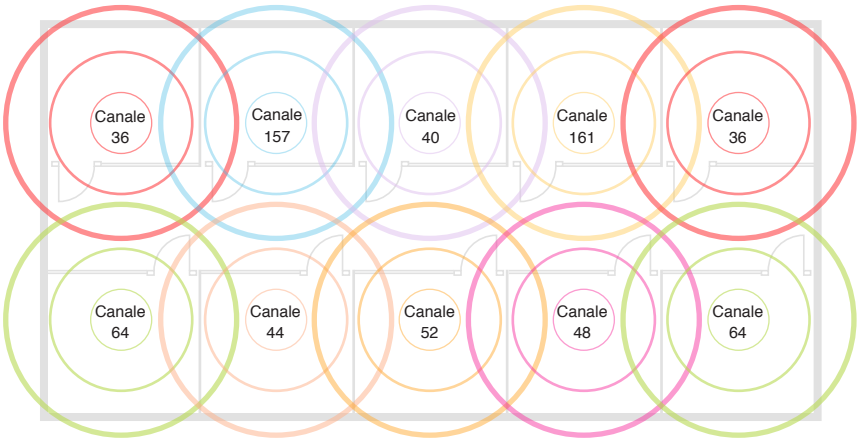
Progettazione finalizzata alla copertura

La disposizione dell'edificio può influire sulla progettazione della rete Wi-Fi. Ad esempio, nel contesto di una piccola impresa, gli utenti potrebbero incontrare i colleghi nelle sale conferenze o nei rispettivi uffici, per poi spostarsi all'interno dell'edificio nell'arco della giornata. In questo scenario, la maggior parte degli accessi alla rete è dato da attività che richiedono poca banda, come controllare le e-mail e i calendari e navigare in Internet, quindi la *copertura* Wi-Fi ha una priorità maggiore. La progettazione della rete Wi-Fi potrebbe includere un piccolo numero di punti di acceso su ogni piano per fornire la copertura agli uffici. Potrebbero poi essere presi in considerazione altri punti di accesso per aree che ospitano un alto numero di dipendenti, come una grande sala riunioni.

Progettazione finalizzata alla capacità

Confronta lo scenario appena descritto con quello di un liceo che ha 1000 studenti e 30 professori all'interno di un edificio di due piani. A ogni studente viene fornito un iPad e a ogni insegnante viene fornito sia un MacBook Air sia un iPad. Ogni aula ospita circa 35 studenti e le aule sono una accanto all'altra. Durante tutta la giornata, gli studenti effettuano ricerche su Internet, guardano video didattici e copiano file da e verso un file server sulla LAN.

Predisporre una rete Wi-Fi in questo scenario è un'operazione più complessa, per via della maggiore densità di dispositivi mobili. A causa dell'alto numero di dispositivi in ogni aula, potrebbe essere necessario un punto di accesso in ciascuna di esse. Per le aree comuni, dovrebbe essere presa in considerazione l'installazione di più punti di accesso, così da fornire una *copertura* e una *capacità* adeguate. Il numero di punti di accesso per le aree comuni può variare a seconda del numero di dispositivi Wi-Fi in tali spazi.



Importante: Per stabilire l'esatto numero di punti di accesso necessari e l'ubicazione di ciascuno di essi, è opportuno eseguire sempre un sopralluogo prima dell'installazione. Il sopralluogo è anche utile a determinare le giuste impostazioni per la potenza di ciascun radiotrasmettitore. Una volta completata l'installazione della rete Wi-Fi, è opportuno eseguire un ulteriore sopralluogo per confermare la corretta predisposizione. Ad esempio, in caso di progettazione di una rete per supportare un numero elevato di utenti in un edificio, è buona norma convalidare e verificare il progetto quando nell'edificio sono presenti delle persone. Oppure se le porte delle aule rimarranno chiuse durante il periodo di utilizzo della rete, le porte dovranno rimanere chiuse anche durante la fase di convalida del progetto.

A volte può essere utile creare più SSID per scopi diversi. Ad esempio, potrebbe essere necessaria una rete per gli ospiti. Occorre comunque fare attenzione a non creare troppi SSID, perché ciò comporterebbe un utilizzo di banda aggiuntivo.

Progettazione finalizzata alle app
I prodotti Apple utilizzano il networking multicast per servizi come AirPlay e AirPrint. Quindi nella progettazione deve essere tenuto in considerazione il supporto per il multicast. Per informazioni su come predisporre la rete per Bonjour, consulta Bonjour.

Standard Wi-Fi nei prodotti iOS

Le specifiche Wi-Fi dei dispositivi iOS Apple vengono descritte in dettaglio nel seguente elenco, che comprende queste informazioni:

- *Compatibilità 802.11:* 802.11ac, 802.11n, 802.11a, 802.11b/g
- *Banda di frequenza:* 2,4 GHz o 5 GHz
- *Velocità di trasmissione massima:* si tratta della velocità massima in base alla quale un client può trasmettere dati via Wi-Fi.
- *Stream spaziali:* ogni radiotrasmettitore può inviare contemporaneamente più stream di dati indipendenti, ognuno contenente dati diversi, aumentando così il throughput generale. Il numero di questi stream di dati indipendenti è definito come il numero di stream spaziali.
- *Indice MCS:* l'indice MCS (Modulation and Coding Scheme) definisce la velocità di trasmissione massima a cui i dispositivi 802.11ac/n possono comunicare. 802.11ac utilizza lo standard VHT (Very High Throughput) , mentre 802.11n utilizza lo standard HT (High Throughput).
- *Ampiezza canale:* ampiezza massima del canale. A partire da 802.11n, i canali possono essere combinati per creare un canale più ampio che consenta la trasmissione di una maggiore quantità di dati durante una singola trasmissione. Con 802.11n, è possibile combinare due canali da 20 MHz per creare un canale da 40 MHz. Con 802.11ac, è possibile combinare quattro canali da 20 MHz per creare un canale da 80 MHz.
- *Intervallo di guardia:* lo spazio (tempo) tra i simboli trasmessi da un dispositivo all'altro. Lo standard 802.11n definisce l'opzione per un intervallo di guardia breve di 400 ns che permette di ottenere throughput complessivi più veloci, ma i dispositivi possono usare un intervallo di guardia lungo di 800 ns.

Modello	Compatibilità 802.11 e frequenza di banda	Velocità di trasmissione massima	Stream spaziali	Indice MCS	Ampiezza canale	Intervallo di guardia
iPad Air 2	802.11ac/n/a a 5 GHz 802.11 n/g/b a 2,4 GHz	866 Mbps	2	9 (VHT) 15 (HT)	80 MHz	400 ns
iPad mini 3	802.11n a 2,4 GHz e 5 GHz 802.11a/b/g	300 Mbps	2	15 (HT)	40 MHz	400 ns
iPhone 6 Plus iPhone 6	802.11ac/n/a a 5 GHz 802.11 n/g/b a 2,4 GHz	433 Mbps	1	9 (VHT) 7 (HT)	80 MHz	400 ns
iPhone 5s iPhone 5c iPhone 5	802.11n a 2,4 GHz e 5GHz 802.11a/b/g	150 Mbps	1	7 (HT)	40 MHz	400 ns
iPhone 4s iPhone 4	802.11n a 2,4GHz 802.11b/g	65 Mbps	1	7 (HT)	20 MHz	800 ns
iPad Air iPad mini con display Retina	802.11n a 2,4GHz e 5GHz 802.11a/b/g	300 Mbps	2	15 (HT)	40 MHz	400 ns
iPad (4a generazione) iPad mini	802.11n a 2,4GHz e 5GHz 802.11a/b/g	150 Mbps	1	7 (HT)	40 MHz	400 ns
iPad (1a, 2a e 3a generazione)	802.11n a 2,4GHz e 5GHz 802.11a/b/g	65 Mbps	1	7 (HT)	20 MHz	800 ns
iPod touch (5a generazione)	802.11n a 2,4GHz e 5GHz 802.11a/b/g	150 Mbps	1	7 (HT)	40 MHz	400 ns
iPod touch (4a generazione)	802.11n a 2,4GHz 802.11b/g	65 Mbps	1	7 (HT)	20 MHz	800 ns

Infrastruttura e integrazione 4

Panoramica

iOS supporta un'ampia gamma di infrastrutture di rete, tra cui le seguenti:

- Reti locali che utilizzano Bonjour.
- Connessioni senza cavo verso Apple TV tramite AirPlay.
- Certificati digitali per autenticare l'accesso degli utenti e proteggere le comunicazioni.
- Single Sign-On per semplificare l'autenticazione alle app e ai servizi sulla rete.
- E-mail, directory, calendari e altri sistemi basati su standard.
- Principali sistemi di terze parti, come ad esempio Microsoft Exchange
- Reti VPN, inclusa la funzione "VPN per app" e "VPN sempre attivo".

Il supporto è integrato in iOS, quindi il reparto IT dovrà configurare solo alcune impostazioni per integrare i dispositivi nell'infrastruttura esistente. Continua a leggere per scoprire le tecnologie supportate da iOS e alcune linee guide per le aziende e gli istituti didattici.

Microsoft Exchange

iOS comunica direttamente con il tuo server Microsoft Exchange tramite Microsoft Exchange ActiveSync (EAS), per avere e-mail, risposte per fuori sede, calendari, contatti e attività con tecnologia push. Inoltre Exchange ActiveSync permette agli utenti di accedere alla Global Address List (GAL), e agli amministratori di controllare i criteri di accesso e le azioni di cancellazione a distanza. iOS supporta sia l'autenticazione di base sia quella via certificato per Exchange ActiveSync.

Se la tua organizzazione utilizza Exchange ActiveSync, disponi già dei servizi necessari per supportare iOS e non occorre un'ulteriore configurazione.

Requisiti

iOS 8 o versione successiva supporta le seguenti versioni di Microsoft Exchange:

- Office 365 (con utilizzo di EAS 14.1)
- Exchange Server 2013 (con utilizzo di EAS 14.1)
- Exchange Server 2010 SP 2 (con utilizzo di EAS 14.1)
- Exchange Server 2010 SP 1 (EAS 14.1)
- Exchange Server 2010 (EAS 14.0)
- Exchange Server 2007 SP 3 (EAS 12.1)
- Exchange Server 2007 SP 2 (EAS 12.1)
- Exchange Server 2007 SP 1 (EAS 12.1)
- Exchange Server 2007 (con utilizzo di EAS 2.5)

Microsoft Exchange Autodiscovery

iOS e OS X supportano il servizio Autodiscover di Microsoft Exchange Server 2007 o versione successiva. Durante la configurazione manuale del dispositivo Apple, il servizio utilizza tuo indirizzo e-mail e la tua password per determinare le corrette informazioni sul server Exchange.

Per ulteriori informazioni, consulta Servizio di identificazione automatica sul sito web di Microsoft.

Microsoft Direct Push

Se è disponibile una connessione dati Wi-Fi o cellulare, Exchange Server invia automaticamente e-mail, attività, contatti ed eventi di calendario ai dispositivi iOS.

Elenco indirizzi globale di Microsoft Exchange

I dispositivi Apple recuperano i contatti dalla directory aziendale del server Exchange della tua organizzazione. Puoi accedere alla directory mentre esegui una ricerca nei contatti. L'accesso avviene automaticamente per consentire il completamento degli indirizzi e-mail durante la loro immissione.

Nota: iOS 6 o versione successiva supporta le foto dell'elenco indirizzi globale (è richiesto Exchange Server 2010 SP 1 o versione successiva).

Impostare messaggi di risposta per fuori sede

iOS 8 supporta l'utilizzo di messaggi di risposta automatici da utilizzare quando l'utente non è disponibile. L'utente può anche selezionare una data di fine per le risposte.

Calendario

iOS 8 o versione successiva e OS X Mavericks o versione successiva supportano le seguenti funzionalità di Microsoft Exchange:

- Creare e accettare inviti di calendario in modalità wireless.
- Visualizzare le informazioni di calendario sulla disponibilità di un invitato.
- Creare eventi di calendario privati.
- Configurare eventi ripetitivi personalizzati.
- Visualizzare i numeri di settimana in Calendario.
- Ricevere aggiornamenti di calendario.
- Sincronizzare le attività con l'app Promemoria.

Visualizzare l'identificatore di Exchange

iOS 8 consente all'utente di visualizzare l'identificatore unico del dispositivo che viene visto dal server Exchange, definito ID dispositivo di Exchange. Ciò e utile quando il server Exchange al quale l'utente si connette richiede che i dispositivi vengano inseriti nella whitelist prima che l'accesso sia consentito. Tale identificatore ti può essere fornito in anticipo. L'ID dispositivo di Exchange cambia solo se il dispositivo viene ripristinato alle impostazioni di fabbrica. Non cambia con l'aggiornamento da iOS 7 a iOS 8. Per visualizzare l'ID dispositivo di Exchange su un dispositivo iOS, tocca Impostazioni > Mail, Contatti, Calendari > Aggiungi account, quindi tocca Exchange.

Identificare le versioni di iOS tramite Exchange

Quando si connette a un server Exchange, il dispositivo segnala la propria versione iOS. Il numero di versione viene inviato nel campo "Agente utente" dell'intestazione della richiesta ed è simile a Apple-iPhone2C1/705.018. Il numero dopo il delimitatore (/) è il numero di build iOS che è unico per ogni release iOS.

Per visualizzare il numero di build su un dispositivo, apri Impostazioni > Generali > Info. Vedrai il numero di versione e il numero di build, ad esempio 4.1 (8B117A). Il numero tra parentesi è il numero di build e identifica la release in esecuzione sul dispositivo.

Quando il numero di build viene inviato al server Exchange, viene convertito dal formato *NANNNA* (dove *N* è un carattere numerico e *A* è un carattere alfabetico) al formato Exchange *NNN.NNN*. I valori numerici vengono mantenuti, mentre le lettere vengono convertite nel valore corrispondente alla posizione occupata nell'alfabeto. Ad esempio, "F" diventerà "06" perché è la sesta lettera dell'alfabeto. Se necessario, tra i numeri vengono inseriti degli zeri per adattarli al formato di Exchange. In questo esempio, il numero di build 7E18 è stato convertito in "705.018".

Il primo numero, 7, rimane "7." Il carattere E è la quinta lettera dell'alfabeto, per cui diventa "05". Nella versione convertita viene inserito un punto (.) come richiesto dal formato. Al numero successivo, 18, viene anteposto uno zero per convertirlo in "018".

Se il numero di build termina con una lettera, adesempio 5H11A, il numero viene convertito come descritto sopra e il valore numerico dell'ultimo carattere viene aggiunto in fondo alla stringa, separato da 3 zeri: 5H11A diventa quindi "508.01100001".

Cancellazione a distanza
Exchange offre funzioni che ti consentono di cancellare a distanza i contenuti di un dispositivo iOS. La cancellazione rimuove tutti i dati e le informazioni di configurazione presenti sul dispositivo, che viene inizializzato e riportato alle impostazioni di fabbrica originali. La cancellazione rimuove la chiave di codifica dei dati (codificati con AES a 256 bit); questo processo è immediato e rende tutti i dati irrecuperabili.

Con Microsoft Exchange Server 2007 o successivo, puoi avviare una cancellazione a distanza da Exchange Management Console, Outlook Web Access o Exchange ActiveSync Mobile Administration Web Tool. Con Microsoft Exchange Server 2003, puoi farlo usando Microsoft Exchange ActiveSync Mobile Administration Web Tool.

In alternativa, gli utenti possono cancellare il proprio dispositivo andando in Impostazioni > Generali > Ripristina e scegliendo "Cancella contenuto e impostazioni". Inoltre puoi configurare i dispositivi perché vengano automaticamente inizializzati dopo un determinato numero di tentativi falliti di inserimento del codice.

Bonjour

Bonjour è il protocollo di rete standardizzato e senza necessità di configurazione sviluppato da Apple che consente ai dispositivi di trovare servizi su una rete. I dispositivi iOS utilizzano Bonjour per individuare stampanti compatibili con AirPrint, mentre i dispositivi iOS e i computer Mac utilizzano Bonjour per individuare dispositivi compatibili con AirPlay come Apple TV. Alcune app utilizzano Bonjour anche per la collaborazione peer-to-peer e per la condivisione.

Bonjour utilizza il traffico multicast per rendere visibile la disponibilità dei servizi. Il traffico multicast solitamente non è instradato, quindi assicurati che Apple TV o le stampanti AirPrint si trovino sulla stessa sottorete IP dei dispositivi iOS che devono utilizzarli. Se la rete è più grande e utilizza più sottoreti IP, potrebbe essere consigliabile utilizzare un gateway Bonjour come quelli offerti da vari produttori di infrastrutture Wi-Fi.

Per ulteriori informazioni su Bonjour, consulta il sito web di Apple Bonjour e la documentazione per gli sviluppatori di Apple su Bonjour.

AirPlay

iOS 8 e OS X Yosemite supportano la possibilità di inviare contenuti in streaming da un dispositivo Apple a Apple TV anche se i dispositivi si trovano su reti diverse o non ci sono reti disponibili. Il dispositivo Apple utilizza la tecnologia BTLE (Bluetooth® Low Energy) per avviare il processo di individuazione dei dispositivi Apple TV disponibili, quindi stabilisce una connessione diretta con Apple TV tramite Wi-Fi. L'individuazione BTLE è un sottoinsieme distinto di AirPlay peer-to-peer.

In iOS 8 e OS X Yosemite, AirPlay peer-to-peer consente agli utenti di utilizzare AirPlay direttamente da un dispositivo iOS o Mac supportato verso Apple TV senza connettersi alla rete dell'organizzazione. AirPlay peer-to-peer elimina il bisogno di accedere alla rete giusta o fornire password Wi-Fi, evita problemi di raggiungibilità su ambienti di rete complessi e ottimizza le prestazioni fornendo un percorso diretto dal mittente AirPlay al destinatario AirPlay. AirPlay peer-to-peer è abilitato di default su iOS 8 e OS X Yosemite e non richiede alcuna configurazione.

AirPlay peer-to-peer richiede:

- Apple TV (3a generazione rev A Modello A1469 o successiva) con software Apple TV 7.0 o versione successiva
- Dispositivi iOS (fine 2012 o successiva) con iOS 8 o versione successiva
- Computer Mac (2012 o successiva) con OS X Yosemite o versione successiva

Per trovare il numero di modello di Apple TV, consulta l'articolo del supporto Apple Identificazione dei modelli di Apple TV.

L'individuazione peer-to-peer viene avviata utilizzando BTLE quando un utente seleziona AirPlay su un dispositivo con iOS 8 o un Mac con OS X Yosemite. Successivamente, il dispositivo e Apple TV utilizzano il canale Wi-Fi 149,1 nella banda dei 5 GHz e il canale Wi-Fi 6 nella banda dei 2,4 GHz per continuare il processo di individuazione. Una volta che l'utente ha selezionato Apple TV e AirPlay viene avviato, i trasmettitori Wi-Fi condividono il canale 149,1 e qualsiasi canale dell'infrastruttura attualmente utilizzato da ciascun dispositivo. Se possibile, il mittente AirPlay viene instradato sullo stesso canale dell'infrastruttura utilizzato da Apple TV. Se nessuno dei due dispositivi sta attualmente utilizzando una rete di infrastruttura, i dispositivi utilizzeranno *solo* il canale Wi-Fi 149 per AirPlay. AirPlay peer-to-peer aderisce agli standard 802.11 sulla condivisione della banda con altri dispositivi Wi-Fi.

Quando distribuisci dispositivi Apple TV su una grande rete Wi-Fi aziendale, tieni in considerazione le seguenti linee guida:

- Collega il dispositivi Apple TV via Ethernet quando possibile.
- Se possibile, non utilizzare i canali Wi-Fi 149 o 153 per la rete di infrastruttura.
- Non posizionare o fissare Apple TV dietro oggetti che potrebbero disturbare i segnali BTLE e Wi-Fi.
- Durante il montaggio di un dispositivo Apple TV su una parete o un'altra superficie, accertati di montarlo con il lato inferiore appoggiato alla superficie.
- Se AirPlay peer-to-peer non è supportato né sul mittente AirPlay né sul ricevitore AirPlay, viene utilizzata automaticamente la connessione all'infrastruttura.

Individuazione AirPlay

I dispositivi iOS continueranno a utilizzare gli stessi metodi di individuazione disponibili oggi per trovare i ricevitori AirPlay. I ricevitori AirPlay possono rendersi visibili utilizzando Bonjour o Bluetooth. L'individuazione tramite Bluetooth richiede iOS 7.1 o versione successiva sui seguenti dispositivi:

- iPad Air

- Apple TV (3a generazione o versione successiva) con software 6.1 o versione successiva
- iPhone 4s o versione successiva
- iPad 3a generazione o versione successiva
- iPad mini 1a generazione o versione successiva
- iPod touch 5a generazione o versione successiva

I ricevitori AirPlay individuati vengono visualizzati nel menu AirPlay.

I servizi Bonjour *_airplay._tcp* e *_raop._tcp* devono essere visibili sui prodotti gateway Bonjour. Contatta il fornitore del gateway per assicurarti che questi servizi siano visibili.

Connettività
L'infrastruttura e il peer-to-peer sono le due modalità di connettività AirPlay supportate. Se sia il ricevitore che il mittente AirPlay supportano AirPlay peer-to-peer, questo sarà il percorso dati preferito, a prescindere della disponibilità o meno dell'infrastruttura. AirPlay peer-to-peer coesiste con la connessione all'infrastruttura, quindi il client AirPlay o il mittente AirPlay possono mantenere la connettività a Internet contemporaneamente a quella peer-to-peer. La banda a 5 GHz è la migliore per la connessione peer-to-peer, perché fornisce una connessione rapida e diretta tra il mittente AirPlay e il ricevitore AirPlay.

Sicurezza
AirPlay utilizza la codifica AES per assicurare che i contenuti rimangano protetti durante la duplicazione o lo streaming da un dispositivo iOS o un Mac a Apple TV.

L'accesso tramite AirPlay a Apple TV può essere limitato impostando un codice su schermo o una password. Solo gli utenti che inseriscono il codice su schermo (per tentativo AirPlay) o la password sul dispositivo iOS o Mac possono inviare contenuti AirPlay a Apple TV.

L'abilitazione della richiesta di verifica del dispositivo (richiede un dispositivo iOS con iOS 7.1 o versione successiva o un Mac con OS X Mavericks 10.9.2 o versione successiva) richiede l'autenticazione del dispositivo iOS o Mac alla prima connessione AirPlay. La richiesta di verifica del dispositivo è utile quando Apple TV viene distribuito su una rete Wi-Fi aperta. Per garantire che i dispositivi iOS e i computer Mac siano abbinati in maniera sicura, all'utente viene richiesto di inserire un codice, da utilizzare una sola volta, che viene visualizzato sullo schermo. Le connessioni successive non richiedono un codice, a meno che non siano abilitate le opzioni "Codice su schermo". Il ripristino delle impostazioni di fabbrica di un dispositivo Apple TV o di un client precedentemente abbinato reimposta le condizioni di connessione iniziali.

AirPlay peer-to-peer è sempre protetto dalla richiesta di autenticazione del dispositivo. Questa impostazione non è configurabile dall'utente e impedisce a eventuali utenti non autorizzati di accedere a Apple TV.

Nota: Per i dispositivi che non si trovano su una rete di infrastruttura, la visibilità Bonjour dei dispositivi Apple TV supportati (A1469 o versione successiva) è avviata da Bluetooth.

Servizi basati su standard

Con il supporto del protocollo di posta IMAP, dei servizi di directory LDAP, dei calendari CalDAV e dei contatti CardDAV, iOS e OS X possono integrarsi con praticamente qualsiasi ambiente basato su standard. Se il tuo ambiente di rete è configurato per richiedere l'autenticazione dell'utente e SSL, iOS e OS X forniscono un approccio molto sicuro per accedere a e-mail, calendari, attività e contatti dell'azienda. Con SSL, iOS e OS X supportano la codifica a 128 bit e i certificati root X.509 generati dalle principali autorità di certificazione.

In una distribuzione standard, i dispositivi Apple stabiliscono un accesso diretto ai server di posta IMAP e SMTP per l'invio e la ricezione di messaggi di posta via etere o, in caso di computer Mac, via etere o Ethernet. Impostano quindi lo stato VIP nei relativi thread di messaggi e possono anche sincronizzare in modalità wireless le note con i server basati su IMAP. I dispositivi Apple possono connettersi alle directory aziendali LDAPv3 della tua organizzazione, consentendo così agli utenti di accedere ai contatti aziendali dalle app Mail, Contatti e Messaggi. Grazie al supporto CardDAV, è possibile mantenere un gruppo di contatti sincronizzato con il tuo server CardDAV usando il formato vCard. La sincronizzazione con il server CalDAV, consente agli utenti di:

- Creare e accettare inviti di calendario in modalità wireless
- Visualizzare le informazioni di calendario sulla disponibilità di un invitato.
- Creare eventi di calendario privati.
- Configurare eventi ripetitivi personalizzati.
- Visualizzare i numeri di settimana in Calendario.
- Ricevere aggiornamenti di calendario.
- Sincronizzare le attività con l'app Promemoria.

Tutti i servizi e server di rete possono trovarsi all'interno di una sottorete demilitarizzata (DMZ), dietro un firewall aziendale o in entrambe le posizioni.

Certificati digitali

I dispositivi Apple supportano i certificati e le identità digitali e offrono così alla tua organizzazione un accesso semplice e sicuro ai servizi aziendali. I certificati si possono utilizzare in vari modi. Ad esempio, il browser Safari è in grado di verificare la validità del certificato digitale X.509 e di impostare una sessione sicura con codifica AES fino a 256 bit. Ciò verifica che l'identità del sito sia legittima e che la comunicazione sia protetta, per impedire l'intercettazione di dati riservati o personali. I certificati possono anche essere utilizzati per autenticare l'identità dell'autore o del "firmatario" e per codificare la posta, i profili di configurazione e le comunicazioni di rete in modo da proteggere ulteriormente le informazioni confidenziali o riservate.

Utilizzare i certificati con i dispositivi Apple

I dispositivi Apple appena acquistati includono una serie di certificati root preinstallati di varie autorità di certificazione, la cui affidabilità viene convalidata da iOS. Se iOS non riesce a convalidare la catena di trust dell'autorità di certificazione firmataria, il servizio restituirà un errore. Ad esempio, di default un certificato autofirmato non può essere verificato in iOS. Per visualizzare l'elenco corrente di certificati root attendibili in iOS, consulta l'articolo del supporto Apple iOS 8: Elenco dei certificati root attendibili disponibili.

Se un certificato root preinstallato viene compromesso, i dispositivi iOS possono aggiornarlo in modalità wireless. Per disattivare questa funzione, esiste una restrizione MDM che impedisce gli aggiornamenti dei certificati via etere.

Questi certificati digitali possono essere utilizzati per identificare in modo sicuro un client o un server e per codificare le comunicazioni tra client e server utilizzando una coppia di chiavi private e pubbliche. Un certificato contiene una chiave pubblica e le informazioni sul client (o sul server) ed è firmato (verificato) da un'autorità di certificazione.

Un certificato e la relativa chiave privata associata sono anche definiti *identità*. I certificati possono essere distribuiti liberamente, ma le identità devono essere conservate in un luogo sicuro. Il certificato distribuito e soprattutto la relativa chiave pubblica vengono utilizzati per la codifica, che potrà essere decodificata solo tramite la corrispondente chiave privata. Per proteggere la chiave privata di un'identità, essa viene memorizzata in un file PKCS12 e codificata con un'altra chiave protetta da una frase chiave. Un'identità può essere utilizzata per l'autenticazione (ad esempio 802.1x EAP-TLS), la firma o la codifica (ad esempio S/MIME).

L'elenco dei formati di certificato e identità supportati sui dispositivi Apple è:

- Certificati X.509 con chiavi RSA
- *Certificati:* .cer, .crt, .der
- *Identità:* .pfx, .p12

Distribuisci i certificati per definire l'attendibilità delle autorità di certificazione che non sono considerate attendibili di default, ad esempio un'autorità di certificazione emittente-organizzativa.

Distribuire e installare i certificati
Distribuire manualmente certificati ai dispositivi iOS è semplice. Ogni volta che si riceve un certificato, basta un tocco per esaminarne i contenuti e un altro per aggiungerlo al dispositivo. Quando si installa un certificato di identità, all'utente viene chiesto di inserire la password che lo protegge. Se è impossibile verificare l'autenticità di un certificato, verrà indicato come non attendibile e l'utente potrà decidere se aggiungerlo o meno al dispositivo.

Installare i certificati tramite i profili di configurazione
Se utilizzi profili di configurazione per distribuire le impostazioni di servizi aziendali come posta S/MIME, VPN o Wi-Fi, puoi aggiungere i certificati al profilo per ottimizzarne la distribuzione. I certificati si possono distribuire anche via MDM.

Installare i certificati via Mail o Safari
Se un certificato viene inviato in un messaggio e-mail, verrà visualizzato come allegato. È anche possibile usare Safari per scaricare i certificati da una pagina web. Puoi ospitare il certificato su un sito web protetto e fornire agli utenti l'URL da cui scaricarlo sui loro dispositivi Apple.

Rimozione e revoca dei certificati
Per rimuovere manualmente un certificato installato, scegli Impostazioni > Generali > Gestione dispositivo, seleziona un profilo, scegli "Più dettagli" e scegli il certificato che desideri rimuovere. Se un utente rimuove un certificato che è necessario per accedere a un account o a una rete, il dispositivo iOS non potrà più collegarsi a tali servizi.

Un server MDM è in grado di visualizzare tutti i certificati presenti sul dispositivo e di rimuovere quelli che ha installato.

Inoltre sono supportati i protocolli OCSP (Online Certificate Status Protocol) e CRL (Certificate Revocation List) per controllare lo stato dei certificati. Quando si utilizza un certificato abilitato per OCSP o CRL, iOS e OS X lo convalidano periodicamente per verificare che non sia stato revocato.

Single Sign-On (SSO)

Il Single Sign-On (SSO) è un processo durante il quale un utente può fornire le informazioni di autenticazione una sola volta, ricevere un ticket e utilizzare tale ticket per accedere alle risorse per tutta la durata di validità del ticket. Questo metodo consente di proteggere l'accesso alle risorse senza che il sistema richieda all'utente di immettere le proprie credenziali a ogni richiesta di accesso. Migliora anche la sicurezza dell'utilizzo quotidiano delle app impedendo che le password vengano trasmesse tramite rete.

Con iOS 7, le app possono sfruttare l'infrastruttura Single Sign-On in-house già esistente tramite Kerberos. Il sistema di autenticazione Kerberos usato da iOS 7 o versione successiva è la tecnologia Single Sign-On più diffusa nel mondo. Se utilizzi Active Directory, eDirectory o Open Directory, è probabile che tu disponga già di un sistema Kerberos utilizzabile da iOS 7 o versione successiva. Per l'autenticazione degli utenti, i dispositivi iOS devono essere in grado di contattare il servizio Kerberos tramite una connessione di rete. In iOS 8, i certificati possono essere utilizzati per rinnovare senza notifiche un ticket Kerberos e consentire agli utenti di mantenere connessioni a determinati servizi che sfruttano Kerberos per l'autenticazione.

App supportate

iOS offre un supporto flessibile per il Single Sign-On (SSO) con Kerberos per tutte le app che utilizzano la classe NSURLConnection o NSURLSession per gestire le connessioni di rete e l'autenticazione. Apple mette a disposizione di tutti gli sviluppatori queste strutture di alto livello per consentire di integrare perfettamente le connessioni di rete nelle loro app. Inoltre, Safari è un ottimo esempio di utilizzo nativo dei siti web abilitati per il Single Sign-On.

Configurare il Single Sign-on

Il Single Sign-On si configura attraverso profili di configurazione installati manualmente o gestiti via MDM. Il payload Single Sign-On permette una configurazione flessibile. Il Single Sign-On può essere aperto a tutte le app o limitato dall'identificatore dell'app, l'URL del servizio o entrambi.

Viene utilizzato un pattern di corrispondenza semplice e gli URL devono cominciare con http:// o https://. L'intero URL deve corrispondere, quindi assicurati che siano perfettamente uguali. Ad esempio, un valore URLPrefixMatches di https://www.example.com/ non risulterà corrispondente a https://www.example.com:443/. Puoi specificare http:// o https:// per limitare l'uso del SSO ai servizi HTTP protetti o normali. Ad esempio, utilizzando un valore URLPrefixMatches https:// si consente l'uso dell'account Single Sign-On solo con servizi HTTPS protetti. Se il pattern di corrispondenza di un URL non finisce con uno slash (/), ne viene aggiunto uno.

L'array AppIdentifierMatches deve contenere stringhe che corrispondano agli ID bundle dell'app. Queste stringhe devono essere match perfetti (com.miaazienda.miaapp, ad esempio) oppure possono specificare un match del prefisso sull'ID bundle utilizzando il carattere jolly (*). Il carattere jolly deve essere preceduto da un punto (.) e comparire alla fine della stringa (ad esempio, com.miaazienda.*). Quando c'è un carattere jolly, tutte le app il cui ID bundle inizia con il prefisso possono accedere all'account.

VPN (Virtual Private Network)

Panoramica

I protocolli VPN standard di settore consentono l'accesso sicuro alle reti aziendali da iOS e OS X. Nella loro configurazione iniziale, iOS e OS X supportano i protocolli Cisco IPSec, L2TP over IPSec e PPTP. iOS supporta anche il protocollo IKEv2. Se la tua organizzazione supporta uno di questi protocolli, per collegare i dispositivi Apple alla VPN non servono altre configurazioni di rete o app aggiuntive di terze parti.

iOS e OS X supportano le VPN SSL dei principali provider VPN. Come altri protocolli VPN supportati da iOS e OS X, anche VPN SSL può essere configurato sul dispositivo Apple manualmente, tramite un profilo di configurazione o via MDM.

iOS e OS X supportano anche le tecnologie standard di settore come IPv6, i server proxy e lo split tunneling, garantendo la disponibilità di tutte le funzioni VPN durante il collegamento alle reti aziendali. Inoltre iOS e OS X sono compatibili con un'ampia gamma di metodi di autenticazione, tra cui password, token a due fattori, certificati digitali e, per OS X, Kerberos. Per semplificare la connessione in ambienti in cui viene utilizzata l'autenticazione basata su certificati, iOS e OS X utilizzano la funzionalità "VPN su richiesta", che, se necessario, avvia una sessione VPN per stabilire la connessione ai domini specificati.

iOS 7 o versione successiva e OS X Yosemite o versione successiva consentono di configurare singole app affinché utilizzino una connessione VPN diversa da quella delle altre app. In questo modo si è certi che i dati aziendali viaggino sempre sulla connessione VPN, e che questa non venga utilizzata per altri dati, come le app personali che il dipendente ha scaricato da App Store. Per maggiori dettagli, consulta VPN per app.

Con "VPN sempre attivo" di iOS, un dispositivo iOS deve connettersi a una VPN conosciuta e approvata prima di potersi connettere a qualsiasi altro servizio della rete. È possibile configurare "VPN sempre attivo" sia per la configurazione Wi-Fi sia per quella cellulare. Ad esempio, utilizzando "VPN sempre attivo", un dispositivo iOS deve connettersi a una VPN conosciuta e approvata prima di potersi connettere a qualsiasi altro servizio della rete come e-mail, web o messaggi. Questa funzionalità dipende dalla capacità di supportare tale configurazione da parte del provider della VPN ed è disponibile solo per i dispositivi supervisionati. Per ulteriori informazioni, consulta la Panoramica di "VPN sempre attivo".

Protocolli e metodi di autenticazione supportati

I dispositivi iOS e OS X supportano i seguenti protocolli e metodi di autenticazione:

- *L2TP su IPSec:* autenticazione utente tramite password MS-CHAP v2, token a due fattori, certificato, autenticazione automatica mediante segreto condiviso o certificato.
- *VPN SSL:* autenticazione utente tramite password, token a due fattori, certificati mediante un client VPN di terze parti.
- *Cisco IPSec:* autenticazione utente tramite password, token a due fattori, autenticazione automatica mediante segreto condiviso e certificati.
- *IKEv2:* Certificati (solo RSA), EAP-TLS, EAP-MSCHAPv2. (solo iOS)
- *PPTP:* autenticazione utente mediante password MS-CHAP v2, certificato e token a due fattori.

OS X può anche utilizzare l'autenticazione automatica Kerberos tramite un segreto condiviso o un certificato con i protocolli L2TP su IPSec e PPTP.

Client VPN SSL

Diversi fornitori SSL VPN hanno creato app che aiutano a configurare i dispositivi iOS per utilizzarli con le rispettive soluzioni. Per configurare un dispositivo per una soluzione specifica, scarica l'app abbinata da App Store e, se lo desideri, fornisci un profilo di configurazione con le impostazioni necessarie.

Le soluzioni VPN SSL includono:

- *AirWatch SSL VPN:* per ulteriori informazioni, consulta il sito web di AirWatch.
- *Aruba Networks SSL VPN:* iOS supporta Aruba Networks Mobility Controller. Per configurare, installa l'app Aruba Networks VIA, disponibile su App Store.

  Per informazioni di contatto, consulta il sito web di Aruba Networks.
- *Check Point Mobile SSL VPN:* iOS supporta Check Point Security Gateway con un tunnel VPN full Layer-3. Installa l'app Check Point Mobile, disponibile su App Store.
- *Cisco AnyConnect SSL VPN:* iOS supporta Cisco Adaptive Security Appliance (ASA) con in esecuzione la versione software suggerita 8.2.5 o successiva. Installa l'app Cisco AnyConnect, disponibile su App Store.
- *F5 SSL VPN:* iOS supporta le soluzioni VPN SSL F5 BIG-IP Edge Gateway, Access Policy Manager e FirePass. Installa l'app F5 BIG-IP Edge Client, disponibile su App Store.

  Per ulteriori informazioni, consulta la guida tecnica di F5 Accesso sicuro tramite iPhone ad applicazioni web aziendali.
- *Juniper Junos Pulse SSL VPN:* iOS supporta i gateway SSL VPN Juniper Networks SA Series versione 6.4 o successive con pacchetto IVE Juniper Networks versione 7.0 o successive. Installa l'app Junos Pulse, disponibile su App Store.

  Per ulteriori informazioni, consulta la pagina Junos Pulse sul sito web di Juniper Networks.
- *Mobile Iron SSL VPN:* per ulteriori informazioni, consulta il sito web di Mobile Iron.
- *NetMotion SSL VPN:* per ulteriori informazioni, consulta il sito web di NetMotion.
- *OpenVPN SSL VPN:* iOS supporta OpenVPN Access Server, Private Tunnel e OpenVPN Community. Per configurare, installa l'app OpenVPN Connect, disponibile su App Store.
- *VPN SSL Palo Alto Networks GlobalProtect:* iOS supporta il gateway GlobalProtect di Palo Alto Networks. Installa l'app GlobalProtect per iOS, disponibile su App Store.
- *SonicWALL SSL VPN:* iOS supporta le apparecchiature SonicWALL Aventall E-Class Secure Remote Access (SRA) con software 10.5.4 o successivo, SonicWALL SRA con software 5.5 o successivo, e SonicWALL Next-Generation Firewall, tra cui i dispositivi TZ, NSA e E-Class NSA con SonicOS 5.8.1.0 o successivo. Installa l'app SonicWALL Mobile Connect, disponibile su App Store.

  Per ulteriori informazioni, consulta il sito web di SonicWALL.

Linee guida per la configurazione di una VPN

Linee guida per la configurazione di Cisco IPSec

Utilizza queste linee guida per configurare il server Cisco VPN per l'utilizzo con dispositivi iOS. iOS supporta i prodotti Cisco ASA 5500 Security Appliances e PIX Firewall configurati con il software 7.2.x o successivo. È consigliabile utilizzare l'ultima versione rilasciata del software (8.0.x o versione successiva). iOS supporta anche i router Cisco IOS VPN con IOS versione 12.4(15)T o versione successiva. I concentratori serie VPN 3000 non supportano le caratteristiche VPN di iOS.

Configurazione proxy
Per tutte le configurazioni è possibile specificare un proxy VPN:

- Per configurare un solo proxy per tutte le connessioni, utilizza l'impostazione manuale e, se necessario, fornisci i dati relativi a indirizzo, porta e autenticazione.
- Per fornire al dispositivo un file di configurazione proxy automatica tramite PAC o WPAD, utilizza l'impostazione Automatica. Per PAC, specifica l'URL del file PAC o JavaScript. Per WPAD, iOS ottiene le impostazioni necessarie dai server DHCP e DNS.

La configurazione proxy VPN viene utilizzata quando la VPN fornisce:

- *Il resolver di default e il percorso di default:* il proxy VPN viene utilizzato per tutte le richieste web sul sistema.
- *Split tunneling:* Solo le connessioni verso host che corrispondono ai domini di ricerca del DNS della VPN utilizzeranno il proxy VPN.

Metodi di autenticazione
iOS supporta i seguenti metodi di autenticazione:

- Autenticazione IPSec con chiave pre-condivisa con autenticazione utente mediante xauth.
- Certificati client e server per autenticazione IPSec con autenticazione utente facoltativa via xauth.
- Autenticazione ibrida in cui il server fornisce un certificato e il client fornisce una chiave pre-condivisa per l'autenticazione IPSec. L'autenticazione utente è richiesta mediante xauth.
- L'autenticazione utente è effettuata mediante xauth e comprende i seguenti metodi di autenticazione:
  - Nome utente con password
  - SecurID RSA
  - CRYPTOCard

Gruppi di autenticazione
Il protocollo Cisco Unity utilizza gruppi di autenticazione per riunire gli utenti in base a un set comune di parametri. Si consiglia di creare un gruppo di autenticazione per gli utenti di dispositivi iOS. Per l'autenticazione mediante chiave pre-condivisa e ibrida, il nome del gruppo deve essere configurato sul dispositivo con la relativa chiave pre-condivisa definita come password di gruppo.

Se l'autenticazione avviene tramite certificati, non è necessaria alcuna chiave pre-condivisa. Il gruppo dell'utente viene stabilito in base ai campi presenti nel certificato. Puoi usare le impostazioni del server Cisco per mappare i campi di un certificato con i gruppi di utenti.

RSA-Sig deve essere la massima priorità nell'elenco priorità ISAKMP.

Certificati
Per la configurazione e l'installazione dei certificati:

- Il certificato di identità del server deve contenere il nome DNS o l'indirizzo IP nel campo SubjectAltName. Il dispositivo usa queste informazioni per verificare che il certificato appartenga al server. Per una maggiore flessibilità, puoi specificare il valore di SubjectAltName utilizzando i caratteri jolly per la corrispondenza dei vari segmenti, ad esempio vpn.*.miasocieta.com. Se non viene specificato alcun valore in SubjectAltName, è possibile inserire il nome DNS nel campo del nome comune.

- Sul dispositivo deve essere installato il certificato della CA che ha firmato il certificato del server. Se non si tratta di un certificato root, installa la parte rimanente della catena di trust in modo da garantire l'attendibilità del certificato. In caso di utilizzo di certificati client, verifica che sul server VPN sia installato il certificato della CA attendibile che ha firmato il certificato del client. Quando usi l'autenticazione con certificato, assicurati che il server sia configurato in modo da identificare il gruppo dell'utente in base ai campi presenti nel certificato client.

  Importante: I certificati e le autorità di certificazione devono essere validi (ad esempio, non scaduti). L'invio della catena di certificazione da parte del server non è supportato.

Impostazioni e descrizioni di IPSec

IPSec presenta varie impostazioni che puoi utilizzare per stabilirne l'implementazione:

- *Modalità:* modalità Tunnel.
- *Modalità scambio IKE:* modalità Aggressive per l'autenticazione mediante chiave pre-condivisa e ibrida o modalità Main per l'autenticazione mediante certificato.
- *Algoritmi di codifica:* 3DES, AES-128 o AES256.
- *Algoritmi di autenticazione:* HMAC-MD5 o HMAC-SHA1.
- *Gruppi Diffie-Hellman:* per l'autenticazione mediante chiave pre-condivisa e ibrida è necessario il gruppo 2. Gruppo 2 con 3DES e AES-128 per l'autenticazione mediante certificato. Gruppo 2 o 5 con AES-256.
- *PFS (Perfect Forward Secrecy):* IKE fase 2, in caso di utilizzo di PFS il gruppo Diffie Hellman deve essere lo stesso usato per IKE fase 1.
- *Configurazione modalità:* attivata.
- *Rilevamento dead peer:* consigliato.
- *Attraversamento NAT standard:* supportato e attivabile (IPSec su TCP non supportato).
- *Bilanciamento del carico:* supportato e attivabile.
- *Re-key della fase 1:* attualmente non supportato. È consigliabile impostare i tempi di re-key sul server su un'ora.
- *Maschera indirizzo ASA:* verifica che tutte le maschere pool degli indirizzi dei dispositivi siano impostate su 255.255.255.255 oppure non siano impostate. Ad esempio:

  ```
  asa(config-webvpn)# ip local pool vpn_users 10.0.0.1-10.0.0.254 mask
  255.255.255.255.
  ```

  Se utilizzi la maschera indirizzo consigliata, alcuni percorsi adottati dalla configurazione VPN potrebbero venire ignorati. Per evitarlo, assicurati che la tabella di instradamento contenga tutti i percorsi necessari e assicurati che gli indirizzi di sottorete siano accessibili prima procedere alla distribuzione.

  - *Versione app:* la versione del software client viene inviata al server per consentirgli di accettare o respingere le connessioni in base alla versione del software disponibile sul dispositivo.
  - *Banner:* se impostato sul server, il banner viene visualizzato sul dispositivo e l'utente può accettarlo o disconnettersi.
  - *Split tunneling:* supportato.
  - *Split DNS:* supportato.
  - *Dominio predefinito:* supportato.

VPN per app

Con iOS e OS X, è possibile stabilire connessioni VPN in base alle singole app. Ciò fornisce un controllo più approfondito sul tipo di dati che passa tramite la VPN. Con una connessione VPN per l'intero dispositivo, tutti i dati viaggiano sulla rete privata indipendentemente dalla loro origine. La possibilità di separare il traffico a livello di app permette di tenere divisi i dati personali da quelli dell'organizzazione. Nelle aziende si usano sempre più spesso i dispositivi personali, e "VPN per app" offre una connessione in rete protetta per le app interne, salvaguardando la privacy delle attività personali.

La funzione "VPN per app" consente a ogni app gestita via MDM di comunicare con la rete privata attraverso un tunnel sicuro, escludendo tutte le altre app non gestite presenti sui dispositivi Apple. Le app gestite possono essere configurate con connessioni VPN diverse per un'ulteriore protezione dei dati. Ad esempio, un'app per i preventivi può utilizzare un centro dati completamente diverso da quello di un'app per gli acquisti, mentre il traffico web dell'utente viaggia su una connessione Internet pubblica. La possibilità di separare il traffico a livello di app permette di tenere divisi i dati personali da quelli dell'organizzazione.

Per utilizzare la funzione "VPN per app", l'app deve essere gestita via MDM e utilizzare le API di rete standard. Dopo aver abilitato "VPN per app" per qualsiasi connessione VPN, dovrai associare tale connessione alle app che la utilizzeranno per proteggere il relativo traffico di rete. Questa operazione viene eseguita mediante il payload di mappatura di "VPN per app" in un profilo di configurazione. La funzione si imposta con una configurazione MDM che specifica le app e i domini di Safari a cui è consentito l'utilizzo dei parametri.

Per informazioni sul supporto per "VPN per app", contatta i fornitori SSL o VPN di terze parti.

VPN su richiesta

Panoramica

"VPN su richiesta" consente ai dispositivi Apple di stabilire automaticamente una connessione senza alcuna azione da parte dell'utente. La connessione VPN viene avviata quando necessario, in base alle regole definite da un profilo di configurazione. "VPN su richiesta" richiede un'autenticazione tramite certificati.

"VPN su richiesta" si configura usando la chiave OnDemandRules in un payload VPN di un profilo di configurazione. Le regole vengono applicate in due fasi.

- *Fase di rilevamento della rete:* definisce i requisiti VPN applicati quando cambia la connessione di rete primaria del dispositivo.
- *Fase di valutazione della connessione:* definisce i requisiti VPN per le richieste di connessione a nomi dominio, quando necessarie.

Ad esempio, le regole si possono usare per:

- Riconoscere se un dispositivo Apple è connesso a una rete interna e non serve una VPN.
- Riconoscere se si utilizza una rete Wi-Fi sconosciuta e serve una VPN per tutte le attività di rete.
- Richiedere una VPN quando una richiesta DNS per un nome dominio specifico non va a buon fine.

Fasi

"VPN su richiesta" stabilisce la connessione alla rete in due fasi.

Fase di rilevamento della rete

Le regole della funzione "VPN su richiesta" vengono valutate quando cambia l'interfaccia di rete primaria del dispositivo, come quando un dispositivo Apple si connette a una rete Wi-Fi diversa, o dalla rete Wi-Fi passa alla rete cellulare su iOS o a Ethernet su OS X. Se l'interfaccia primaria è virtuale, come un'interfaccia VPN, le regole per la VPN su richieste vengono ignorate.

Le regole di matching di ogni set (dizionario) devono tutte corrispondere affinché l'azione a esse associata venga intrapresa; se una di queste regole non corrisponde, la valutazione passa al dizionario successivo, e così via, finché l'array OnDemandRules è esaurito.

L'ultimo dizionario dovrebbe definire una configurazione di default, cioè non dovrebbe avere alcuna regola di matching, ma solo un'azione che catturerà tutte le connessioni che non corrispondevano alle regole precedenti.

Fase di valutazione della connessione

La VPN può essere attivata quando serve in base alle richieste di connessione ad alcuni domini, invece di collegarsi e scollegarsi alla VPN in base all'interfaccia di rete.

Regole e azioni

Le regole aiutano a stabilire i tipi di rete associati a "VPN su richiesta". Le azioni aiutano a stabilire cosa accade quando vengono trovate regole di matching.

Regole di matching su richiesta

Specifica una o più delle seguenti regole di matching per i client Cisco IPSec:

- *InterfaceTypeMatch:* facoltativo. Un valore di stringa "cellulare (per iOS) o Ethernet (per OS X)" o "Wi-Fi". Se specificata, c'è corrispondenza quando l'interfaccia hardware primaria è del tipo specificato.
- *SSIDMatch:* facoltativo. Un array di SSID da confrontare con la rete attuale. Se la rete non è Wi-Fi o se il suo SSID non appare nell'elenco, non ci sarà alcuna corrispondenza. Per ignorare il SSID, ometti questa chiave e il suo array.
- *DNSDomainMatch:* facoltativo. Un array di domini di ricerca sotto forma di stringhe. Se il dominio di ricerca DNS configurato per la rete primaria attuale è incluso nell'array, ci sarà una corrispondenza. È supportato il prefisso jolly (*), come in *.example.com che corrisponde a qualsiasi.example.com.
- *DNSServerAddressMatch:* facoltativo. Un array di indirizzi di server DNS sotto forma di stringhe. Se l'array contiene tutti gli indirizzi di server DNS configurati al momento per l'interfaccia primaria, ci sarà una corrispondenza. Il carattere jolly (*) è supportato. Ad esempio, 1.2.3.* restituirà un match con qualsiasi server DNS con il prefisso 1.2.3.
- *URLStringProbe:* facoltativo. Un server per sondare la raggiungibilità. Il reindirizzamento non è supportato. L'URL dovrebbe puntare a un server HTTPS affidabile. Il dispositivo invia una richiesta GET per verificare che il server sia raggiungibile.

Action

Questa chiave obbligatoria definisce il comportamento della VPN qualora tutte le regole di matching specificate vengano valutate come vere. e i suoi valori sono:

- *Connect:* avvia la connessione VPN in maniera incondizionata al tentativo successivo di connettersi a una rete.

- *Disconnect:* interrompe la connessione alla VPN e non avvia alcuna nuova connessione su richiesta.
- *Ignore:* mantiene le connessioni alla VPN esistenti, ma non avvia nuove connessioni su richiesta.
- *EvaluateConnection:* valuta gli ActionParameters per ogni tentativo di connessione. Quando si utilizza, per specificare le regole di valutazione è richiesta la chiave ActionParameters descritta di seguito.
- *Allow:* Per i dispositivi con iOS 6 o precedente, consulta Compatibilità retroattiva.

ActionParameters
Si tratta di un array di dizionari contenenti le chiavi descritte di seguito, valutati nell'ordine in cui si presentano. Obbligatoria quando il valore Action è EvaluateConnection.

- *Domains:* obbligatorio. Un array di stringhe che definiscono i domini cui si applica questa valutazione. Sono supportati i prefissi jolly, come in *.example.com.
- *DomainAction:* obbligatorio. Definisce il comportamento della VPN per i domini. Il valori per la chiave DomainAction sono:
  - *ConnectIfNeeded:* attiva la VPN se la risoluzione DNS per il dominio non va a buon fine, ad esempio quando il server DNS indica che non riesce a risolvere il nome dominio, se la risposta DNS viene reindirizzata o se la connessione non riesce o scade.
  - *NeverConnect:* non attiva alcuna VPN per i domini.

Quando DomainAction è ConnectIfNeeded, puoi anche specificare le seguenti chiavi nel dizionario di valutazione della connessione.

- *RequiredDNSServers:* facoltativo. Un array di indirizzi IP di server DNS da usare per risolvere i domini. Non è necessario che questi server facciano parte della configurazione di rete attuale del dispositivo. Se non sono raggiungibili, la VPN non viene attivata. Per ottenere connessioni continuative, configura un server DNS interno o un server DNS esterno affidabile.
- *RequiredURLStringProbe:* facoltativo. Un URL HTTP o HTTPS (preferibile) per il probing tramite richiesta GET. Se la risoluzione DNS per questo server va a buon fine, deve riuscire anche il probing. Se non riesce, viene attivata la VPN.

Compatibilità retroattiva

Prima di iOS 7, le regole di attivazione dei domini venivano configurate tramite array di domini:

- OnDemandMatchDomainAlways
- OnDemandMatchDomainOnRetry
- OnDemandMatchDomainNever

iOS 7 o versione successiva supporta ancora i casi OnRetry e Never, benché siano stati abbandonati a favore dell'azione EvaluateConnection.

Per creare un profilo che funzioni sia con iOS 7 sia con le versioni precedenti, usa le nuove chiavi EvaluateConnection in aggiunta agli array OnDemandMatchDomain. Le versioni precedenti di iOS che non riconoscono EvaluateConnection utilizzano i vecchi array; iOS 7 o versioni successive utilizzano EvaluateConnection.

I vecchi profili di configurazione che specificano l'azione Allow dovrebbero funzionare su iOS 7, a eccezione dei domini OnDemandMatchDomainsAlways.

VPN sempre attivo

Panoramica

"VPN sempre attivo" fornisce alla tua organizzazione un controllo totale sul traffico dei dispositivi attraverso il tunneling di tutto il traffico IP verso l'organizzazione. Il protocollo di tunneling di default, IKEv2, protegge il traffico attraverso la codifica dei dati. La tua organizzazione adesso può monitorare e filtrare il traffico verso e dai dispositivi, proteggere i dati nella rete e limitare l'accesso dei dispositivi a Internet.

Per abilitare "VPN sempre attivo" è necessaria la supervisione del dispositivo. Una volta che il profilo "VPN sempre attivo" sarà installato su un dispositivo, questo si attiverà automaticamente senza alcuna interazione da parte dell'utente. "VPN sempre attivo" rimane abilitato (anche in seguito al riavvio) finché il relativo profilo non viene disinstallato.

Con "VPN sempre attivo" abilitato sul dispositivo, l'attivazione e l'interruzione del tunnel VPN sono legate allo stato dell'interfaccia IP. Quando l'interfaccia ottiene la raggiungibilità sulla rete IP, si ha il tentativo di stabilire il tunneling. Quando lo stato dell'interfaccia IP risulta non attivo, il tunneling viene interrotto. "VPN sempre attivo" supporta anche tunnel specifici per le singole interfacce. Per i dispositivi iOS, sarà presente un tunnel per ogni interfaccia IP attiva (ovvero, un tunnel per l'interfaccia cellulare e un tunnel per l'interfaccia Wi-Fi). Finché il tunnel o i tunnel VPN sono attivi, tutto il traffico IP passerà attraverso di essi. Tutto il traffico include tutto il traffico IP instradato e tutto il traffico IP proveniente da app proprietarie come FaceTime e Messaggi. Se il tunnel o i tunnel non sono attivi, tutto il traffico IP viene bloccato.

Tutto il traffico proveniente da un dispositivo raggiungerà un server VPN. È possibile applicare dei filtri e/o trattamenti di monitoraggio opzionali prima di inoltrare il traffico verso la propria destinazione all'interno della rete dell'organizzazione o verso Internet. Analogamente, il traffico verso il dispositivo verrà instradato verso il server VPN dell'organizzazione, dove possono essere applicati filtri o trattamenti di monitoraggio prima dell'inoltro verso il dispositivo.

Scenari di distribuzione

I dispositivi iOS operano in modalità utente singolo. Non vi è distinzione tra l'identità del dispositivo e l'identità dell'utente. Quando un dispositivo iOS stabilisce un tunnel IKEv2 verso il server IKEv2, il server percepisce il dispositivo iOS come una singola entità di pari livello. Tradizionalmente, esiste un solo tunnel tra una coppia composta da un dispositivo iOS e un server VPN. Dal momento che "VPN sempre attivo" introduce la possibilità di avere tunnel specifici per ogni interfaccia, possono esserci più tunnel simultanei stabiliti tra un singolo dispositivo iOS e il server IKEv2, a seconda del modello di distribuzione.

La configurazione "VPN sempre attivo" supporta i seguenti modelli di distribuzione in grado di soddisfare i requisiti di diverse soluzioni.

Dispositivi solo cellulare

Se la tua organizzazione sceglie di distribuire "VPN sempre attivo" su dispositivi iOS solo cellulare (con interfaccia Wi-Fi rimossa in maniera permanente o disattivata), viene stabilito un tunnel IKEv2 tramite l'interfaccia IP cellulare tra ciascun dispositivo e il server IKEv2. È la stessa configurazione del modello VPN tradizionale. Il dispositivo iOS costituisce un client IKEv2, con un'identità (ovvero, un certificato client o una combinazione utente/password) stabilendo un tunnel IKEv2 con il server IKEv2.

Dispositivi cellulari e Wi-Fi

Se la tua organizzazione sceglie di distribuire "VPN sempre attivo" per dispositivi iOS che presentano sia l'interfaccia cellulare sia quella Wi-Fi, dal dispositivo verranno stabiliti due tunnel IKEv2 simultanei. Esistono due possibili scenari con l'utilizzo di dispositivi cellulari e Wi-Fi:

- Tunnel cellulare e tunnel Wi-Fi diretti su server IKEv2 distinti

  Le chiavi di configurazione del tunneling per interfaccia di "VPN sempre attivo" consentono alla tua organizzazione di configurare i dispositivi affinché stabiliscano un tunnel cellulare verso un server IKEv2 e un tunnel Wi-Fi verso un secondo server IKEv2. Un vantaggio di questo modello è che un dispositivo può usare la stessa identità di client (ovvero certificato client o combinazione utente/password) per entrambi i tunnel, dato che essi sono diretti verso server distinti. Con diversi server, la tua compagnia può inoltre godere di una maggiore flessibilità sulla separazione e sul controllo del tipo di traffico per ciascuna interfaccia (traffico cellulare vs. traffico Wi-Fi). Lo svantaggio è che la tua organizzazione deve disporre di due diversi server IKEv2 con criteri di autenticazione dei client identici.
- Tunnel cellulare e tunnel Wi-Fi diretti sullo stesso server IKEv2

  La configurazione dei tunnel per interfaccia di "VPN sempre attivo" consente anche alla tua organizzazione di configurare un dispositivo affinché stabilisca il tunnel cellulare e il tunnel Wi-Fi verso lo stesso server IKEv2.

  Utilizzo dell'identità del client:

  - *Un'identità di client per dispositivo:* La tua organizzazione può configurare la stessa identità di client (ovvero un certificato client o una combinazione utente/password) sia per il tunnel cellulare sia per quello Wi-Fi, se il server IKEv2 supporta più tunnel per client. Il vantaggio è che è possibile evitare un'identità in più per dispositivo e il carico di configurazioni e risorse in più sul server. Lo svantaggio è che quando un dispositivo entra ed esce della rete, vengono stabiliti nuovi tunnel e quelli vecchi diventano obsoleti. A seconda dell'implementazione del server, questo potrebbe non essere in grado di cancellare in maniera efficiente e accurata i tunnel obsoleti. L'organizzazione dovrà implementare una strategia per la cancellazione dei tunnel obsoleti sul server.
  - *Due identità di client per dispositivo:* La tua organizzazione può configurare due identità di client (ovvero due certificati client o due combinazioni utente/password), una per un tunnel cellulare, una per un tunnel Wi-Fi. Il server IKEv2 rileva due diversi client che stabiliscono ognuno il proprio tunnel. Il vantaggio di questo modello è che funziona con gran parte delle implementazioni di server, dato che molti server differenziano i tunnel a seconda dell'identità dei client e consentono un solo tunnel per ciascuno di essi. Lo svantaggio di questo modello è la gestione della doppia identità del client e la gestione di configurazioni e risorse doppie sul server.

Profilo di configurazione di "VPN sempre attivo"

Un profilo di configurazione di "VPN sempre attivo" può essere composto manualmente, utilizzando uno degli appositi editor di Apple come "Gestore profilo", Apple Configurator oppure di un fornitore MDM di terze parti. Per ulteriori informazioni, consulta Aiuto Gestore Profilo o Aiuto Apple Configurator.

Chiavi per l'interazione dell'utente

Per impedire agli utenti di disattivare la funzione "VPN sempre attivo", disabilita la rimozione del relativo profilo impostando la chiave di profilo di primo livello PayloadRemovalDisallowed su vero.

Per impedire agli utenti di alterare il comportamento della funzione "VPN sempre attivo" installando altri profili di configurazione, disabilita l'installazione del profilo UI impostando la chiave allowUIConfigurationProfileInstallation su falso nel payload com.apple.applicationaccess. La tua organizzazione può implementare restrizioni aggiuntive utilizzando altre chiavi supportate nello stesso payload.

Payload del certificato

- *Certificato della CA del server:* se il metodo di autenticazione del tunnel IKEv2 utilizza i certificati, il server IKEv2 invia il proprio certificato al dispositivo iOS, il quale ne convalida l'identità. Affinché il dispositivo iOS possa convalidare il certificato server, gli occorre il certificato dell'autorità di certificazione (l'ente che ha emesso il certificato) del server. Il certificato della CA del server potrebbe essere già stato installato precedentemente sul dispositivo. Altrimenti la tua organizzazione può includerlo creando un apposito payload di certificato.
- *Certificati della CA del client:* se il metodo di autenticazione del tunnel IKEv2 utilizza i certificati o EAP-TLS, il dispositivo iOS invia i propri certificati client al server IKEv2, il quale ne convalida l'identità. Il client può avere uno o due certificati client, a seconda del modello di distribuzione selezionato. La tua organizzazione dovrà includere i certificati client creando appositi payload di certificato. Al tempo stesso, affinché il server IKEv2 possa convalidare l'identità del client, il server IKEv2 dovrà avere installato il certificato dell'autorità di certificazione (l'ente che ha emesso il certificato) del client.
- *Certificati supportati da "VPN sempre attivo" con IKEv2:* attualmente, "VPN sempre attivo" con IKEv2 supporta solo certificati RSA.

Payload di "VPN sempre attivo"

Le seguenti informazioni riguardano il payload di "VPN sempre attivo".

- Il payload può essere installato sono su dispositivi iOS supervisionati.
- Un profilo di configurazione può contenere un solo payload di "VPN sempre attivo".
- È possibile installare un solo profilo di configurazione di "VPN sempre attivo" alla volta su un dispositivo iOS.

Connessione automatica in iOS

"VPN sempre attivo" mette a disposizione una chiave facoltativa UIToggleEnabled che consente alla tua organizzazione di abilitare un interruttore "Connetti automaticamente" nelle impostazioni VPN. Se la chiave non è specificata o è impostata su 0, "VPN sempre attivo" tenta di stabilire uno o due tunnel VPN. Se la chiave è impostata su 1, sarà presente l'interruttore nel pannello delle impostazioni VPN e l'utente potrà scegliere di attivare o disattivare il tunneling VPN. Se l'utente sceglie di disattivare il tunneling VPN, non viene stabilito alcun tunnel e il dispositivo blocca tutto il traffico IP. Ciò è utile nel caso in cui non vi sia raggiungibilità IP e l'utente voglia comunque effettuare delle telefonate. L'utente può disattivare il tunneling VPN per evitare tentativi superflui di stabilire un tunnel VPN.

Array di configurazione del tunneling per interfaccia

È necessaria la configurazione di almeno un tunnel (ovvero, applicato all'interfaccia cellulare per i dispositivi solo cellulari o applicato sia all'interfaccia cellulare sia a quella Wi-Fi) nell'array TunnelConfigurations. Al massimo possono essere incluse due configurazioni di tunneling (una per le interfacce cellulari, una per le interfacce Wi-Fi).

Eccezioni per il traffico Captive

"VPN sempre attivo" supporta solo reti Captive con AutoLogon (accesso automatico a reti Captive con credenziali preassegnate, come ad esempio credenziali derivate dalla scheda SIM).

"VPN sempre attivo" permette anche il controllo sulla gestione delle reti Captive supportando le seguenti opzioni:

- *AllowCaptiveWebSheet:* una chiave per consentire al traffico dall'app integrata WebSheet di passare al di fuori del tunnel. L'app WebSheet è un browser che gestisce l'accesso alle reti Captive se non sono presenti altre app Captive di terze parti. La tua organizzazione dovrebbe tenere in considerazione il rischio per la sicurezza derivato dall'utilizzo di tale chiave, perché WebSheet è un browser funzionale capace di elaborare qualsiasi contenuto proveniente dai server Captive che gli inviano risposta. Consentire il traffico per WebSheet rende il dispositivo vulnerabile nei confronti di server Captive malevoli o malintenzionati.
- *AllowAllCaptiveNetworkPlugins:* Una chiave per consentire al traffico di tutte le app Captive autorizzate di terze parti di passare a di fuori del tunnel. La chiave ha la precedenza sul dizionario AllowedCaptiveNetworkPlugins.
- *AllowedCaptiveNetworkPlugins:* Un elenco di ID bundle delle app Captive autorizzate di terze parti. Il traffico proveniente da tale elenco di app Captive di terze parti è consentito al di fuori del tunnel. Se è configurata anche la chiave AllowAllCaptiveNetworkPlugins, l'elenco non avrà effetto.

Eccezioni di servizio
Di default, "VPN sempre attivo" effettua il tunneling di tutto il traffico IP. Esso include tutto il traffico locale e il traffico per i servizi dell'operatore cellulare. Dunque il comportamento di default di "VPN sempre attivo" non supporta alcun servizio IP locale né servizio IP dell'operatore. Il supporto per le eccezioni di servizio di "VPN sempre attivo" consente alla tua organizzazione di alterare il trattamento di default del traffico dei servizi affinché passi al di fuori del tunnel o venga bloccato. I servizi attualmente supportati sono VoiceMail e AirPrint e le azioni consentite sono Allow (per consentire il passaggio fuori dal tunnel) o Drop (per bloccarlo a prescindere dal tunnel).

Per ulteriori informazioni sulle chiavi e sugli attributi IKEv2 di "VPN sempre attivo", consulta il materiale di riferimento sulle chiavi dei profili di configurazione sul sito web di iOS Developer Library.

Servizi Internet 5

Panoramica

I servizi Internet di Apple sono stati sviluppati con gli stessi obiettivi di sicurezza che caratterizzano l'intera piattaforma iOS: gestione sicura dei dati archiviati sul dispositivo iOS o in transito su reti wireless, protezione delle informazioni personali dell'utente e protezione contro l'accesso doloso o non autorizzato a informazioni e servizi. Ogni servizio utilizza una propria, potente architettura di sicurezza senza compromettere la facilità d'uso complessiva di iOS.

Questi servizi aiutano gli utenti a comunicare e a creare dati personali con la possibilità di eseguirne il backup, il tutto senza compromettere i dati aziendali.

Essi includono:

- ID Apple
- "Trova il mio iPhone" e "Blocco attivazione"
- Continuity
- iCloud
- Portachiavi iCloud
- iMessage
- FaceTime
- Siri
- ID Apple per studenti

Con una soluzione MDM e le restrizioni iOS, puoi limitare alcuni di questi servizi. Per informazioni, fai riferimento alle restrizioni MDM descritte nella Panoramica.

L'attenzione di Apple nei confronti della sicurezza e della privacy è fondamentale nella fase di progettazione di tutto l'hardware, il software e i servizi. Questo è il motivo per cui la privacy dei clienti Apple viene rispettata ai massimi livelli e viene protetta con un sistema di codifica sofisticato e grazie a criteri molto rigidi alla base della gestione di tutti i tipi di dati. Per ulteriori informazioni, consulta www.apple.com/it/privacy.

ID Apple

L'ID Apple è necessario a chiunque voglia accedere ai servizi di Apple. È importante comprendere gli ID Apple, così da poter spiegare agli utenti come configurarne uno personale.

Un ID Apple è un'identità utilizzata per accedere a vari servizi Apple, come FaceTime, iMessage, iTunes Store, App Store, iBooks Store e iCloud. Tali servizi offrono agli utenti l'accesso a una vasta gamma di contenuti utili a ottimizzare le attività aziendali, aumentare la produttività e incoraggiare la collaborazione.

Per usare al meglio questi servizi, gli utenti dovrebbero utilizzare il proprio ID Apple personale. Se non ne hanno uno, possono crearlo ancora prima di ricevere un dispositivo oppure possono utilizzare "Impostazione assistita". Questo strumento offre loro un metodo semplice per creare un ID Apple direttamente dal dispositivo Apple. Gli ID Apple possono essere creati anche senza che sia necessaria una carta di credito.

Per distribuzioni di dispositivi uno a uno o di proprietà dello studente oppure per distribuzioni di dispositivi personali, ogni utente dovrebbe avere il proprio ID Apple personale. In una distribuzione basata sull'utilizzo condiviso, è possibile utilizzare un ID Apple di proprietà dell'azienda per distribuire contenuti su più dispositivi Apple.

Grazie all'ID Apple, ogni studente o dipendente può installare app, libri e altri contenuti forniti dall'istituzione, annotare i testi in iBooks a cui è possibile accedere sia con dispositivi iOS sia con computer Mac, nonché iscriversi ai corsi di iTunes U. Tutte queste operazioni possono essere svolte senza che un reparto IT debba gestire gli ID Apple sui dispositivi Apple degli utenti.

Per ulteriori informazioni sugli ID Apple, consulta il sito web Il mio ID Apple.

"Trova il mio iPhone" e "Blocco attivazione"

Se un dispositivo iOS viene smarrito o rubato, è importante disattivarlo e cancellare tutti i suoi dati. Grazie alla funzione "Trova il mio iPhone", inclusa nella suite iCloud, gli utenti possono individuare l'ultima posizione rilevata del proprio iPad, iPhone o iPod touch utilizzando "Trova il mio iPhone" su iCloud.com o l'app "Trova il mio iPhone" su un dispositivo iOS. Dopo aver individuato il dispositivo iOS, l'utente potrà riprodurre un suono su di esso, attivare la "Modalità smarrito" oppure cancellare tutti i dati in esso contenuti se il dispositivo è connesso a Internet.

La funzionalità "Modalità smarrito" (iOS 6 o versione successiva) bloccherà il dispositivo iOS con un codice d'accesso, visualizzerà un messaggio personalizzato sullo schermo e terrà traccia della posizione del dispositivo. Per i dispositivi iOS con iOS 5, questa funzionalità si limiterà a bloccare il dispositivo.

Con iOS 7 o versione successiva, quando "Trova il mio iPhone" è attivo, il dispositivo iOS può essere riattivato solo inserendo le credenziali dell'ID Apple del proprietario. È consigliabile supervisionare i dispositivi di proprietà dell'organizzazione e implementare criteri affinché gli utenti disattivino la funzione e "Trova il mio iPhone" non impedisca all'azienda di assegnare il dispositivo a un'altra persona.

Con iOS 7.1 o versione successiva puoi utilizzare una soluzione MDM compatibile per abilitare "Blocco attivazione" sui dispositivi supervisionati quando un utente attiva "Trova il mio iPhone". Gli amministratori della MDM possono gestire il blocco attivazione di "Trova il mio iPhone" supervisionando i dispositivi con Apple Configurator o il DEP (Device Enrollment Program). La soluzione MDM potrà dunque archiviare un codice di elusione quando "Blocco attivazione" è abilitato e utilizzarlo per cancellare il blocco dell'attivazione automaticamente quando ti occorrerà inizializzare il dispositivo e assegnarlo a un nuovo utente. Per maggiori dettagli, consulta la documentazione della tua soluzione MDM.

Importante: Di default, i dispositivi supervisionati non hanno mai un blocco attivazione abilitato, anche se l'utente attiva "Trova il mio iPhone". Tuttavia, un server MDM potrebbe ricevere un codice di elusione e consentire "Blocco attivazione" sul dispositivo. Se "Trova il mio iPhone" viene attivato quando il server MDM abilita il blocco attivazione, quest'ultimo viene abilitato in quel momento. Se "Trova il mio iPhone" viene disattivato quando il server MDM abilitata il blocco attivazione, quest'ultimo viene abilitato la volta successiva che l'utente attiva "Trova il mio iPhone".

Per ulteriori informazioni su "Trova il mio iPhone", "Modalità smarrito" e "Blocco attivazione", consulta gli articoli del supporto Apple Supporto iCloud, iCloud: Utilizzo della Modalità smarrito e Blocco attivazione via MDM e Trova il mio iPhone. Consulta anche Impostazioni di Blocco attivazione nell'Aiuto di "Gestore profilo".

Continuity

Continuity è una serie di funzionalità che consente a un Mac e a iPhone o iPad di comunicare perfettamente tra loro. Continuity richiede iOS 8 o versione successiva e OS X Yosemite o versione successiva e potrebbe richiedere la registrazione dei dispositivi con lo stesso ID Apple.

Nota: Alcune funzionalità potrebbero non essere disponibili in tutti i paesi, regioni o lingue.

Telefonate

iPhone e un Mac possono interagire alla perfezione durante l'invio o la ricezione delle telefonate. Se utilizza il proprio Mac e il proprio iPhone è nelle vicinanze, un utente potrà inviare o ricevere una telefonata utilizzando il Mac e, se lo desidera, continuare la chiamata con iPhone.

SMS

Gli utenti possono comunicare tramite SMS utilizzando il proprio dispositivo iOS con iOS 8.1 o versione successiva o con OS X Yosemite o versione successiva. I messaggi SMS appaiono su tutti i dispositivi dell'utente in modo da consentire di rispondere con il dispositivo desiderato.

Handoff

Un utente può iniziare a scrivere un messaggio in Mail o creare un documento Pages sul proprio Mac e quindi continuare a lavorare su un altro dispositivo iOS con iOS 8 o versione successiva vicino. Apparirà una piccola icona nell'angolo del dispositivo iOS oppure sul Dock del Mac. Per visualizzare il documento, è sufficiente scorrere il dito sul dispositivo iOS desiderato o fare clic sul Mac. Handoff funziona con Calendario, Contatti, Mail, Maps, Messaggi, Pages, Numbers, Keynote, Promemoria e Safari. Gli sviluppatori di app possono inoltre integrare Handoff nelle proprie app.

Instant Hotspot

Instant Hotspot consente a un Mac di utilizzare iPhone o iPad (con connettività cellulare) con iOS 8.1 o versione successiva come connessione Internet quando non è disponibile una rete Wi-Fi. La potenza del segnale e la durata della batteria del dispositivo iOS appaiono sulla barra dei menu del Mac. Non appena l'utente si disconnette dal dispositivo iOS, l'hotspot viene disattivato per salvaguardare la durata della batteria del dispositivo.

Nota: Per la disponibilità del servizio hotspot, consulta il tuo gestore.

AirDrop

AirDrop consente a un Mac con OS X Mavericks o versione successiva e a un dispositivo iOS con iOS 8 o versione successiva nelle vicinanze di condividere file in modalità wireless senza un'effettiva rete wireless. AirDrop è disponibile da qualsiasi menu di condivisione e nella barra laterale del Finder sul Mac.

iCloud

iCloud consente agli utenti di archiviare contenuti personali, come ad esempio contatti, calendari, documenti e foto, e mantenerli costantemente aggiornati nei vari dispositivi iOS e computer Mac. iCloud protegge i contenuti codificandoli durante il processo di invio tramite Internet, quindi li archivia in un formato codificato e utilizza token sicuri per l'autenticazione. I dispositivi iOS utilizzano il backup di iCloud per eseguire il backup giornaliero tramite Wi-Fi di informazioni quali, ad esempio, i dati delle app, le impostazioni dei dispositivi iOS e i messaggi SMS e MMS. Il backup di iCloud funziona solo quando il dispositivo è bloccato, è collegato all'alimentazione e dispone di un accesso Wi-Fi a Internet. iCloud offre anche la possibilità di localizzare i dispositivi iOS e i computer Mac smarriti o rubati tramite "Trova il mio iPhone".

Con una soluzione MDM è anche possibile impedire il backup su iCloud delle app gestite. Ciò offre agli utenti il vantaggio di utilizzare iCloud per i dati personali, impedendo tuttavia alle informazioni aziendali di essere archiviate su iCloud. Per i dati da account aziendali e da app in-house, il backup su iCloud non viene eseguito. Alcuni servizi, come "Foto iCloud", "Portachiavi iCloud" e iCloud Drive, possono essere limitati tramite le restrizioni inserite manualmente sul dispositivo o impostate tramite profili di configurazione.

Per ulteriori informazioni su iCloud, consulta il sito web di iCloud. Per ulteriori informazioni sulla sicurezza e sulla privacy in iCloud, consulta l'articolo del supporto Apple Panoramica sulla sicurezza e sulla privacy in iCloud. Per ulteriori informazioni sui requisiti di sistema per iCloud, consulta l'articolo del supporto Apple Requisiti di sistema per iCloud.

Nota: Alcune funzioni richiedono una connessione Wi-Fi. Alcune funzioni non sono disponibili in tutti i paesi. L'accesso ad alcuni servizi è limitato a 10 dispositivi.

iCloud Drive

Gli utenti possono archiviare in sicurezza i loro documenti in iCloud Drive e accedervi da qualsiasi luogo e in qualsiasi momento da iPhone, iPad, Mac o computer Windows. Le librerie di documenti delle app iOS sono accessibili anche dal Mac. In questo modo, un documento creato su un dispositivo iOS può essere modificato sul Mac.

Gli utenti possono anche condividere documenti di Pages, Numbers e Keynote archiviati in iCloud Drive con altri utenti. Ogni app iOS mostra i documenti compatibili archiviati in iCloud Drive. Su un Mac, iCloud Drive appare sotto forma di cartella in OS X. Gli utenti possono trascinare gli elementi selezionati per aggiungere file, organizzarli in cartelle e tag e persino eseguire ricerche utilizzando Spotlight.

iCloud mantiene aggiornate le informazioni su tutti i dispositivi. Qualsiasi modifica apportata a un file in modalità non in linea viene automaticamente aggiornata non appena il dispositivo torna in linea.

Portachiavi iCloud

La funzionalità "Portachiavi iCloud" mantiene costantemente aggiornate le password dei siti web utilizzati in Safari e le password delle reti Wi-Fi su tutti i dispositivi iOS e i computer Mac configurati per iCloud. Memorizza anche le password per altre app che supportano tale funzionalità, nonché le informazioni relative alla carta di credito salvate in Safari, in modo tale che Safari le compili automaticamente sui dispositivi iOS e computer Mac. Grazie a questa funzionalità potrai anche archiviare le informazioni di accesso agli account Internet e le informazioni di configurazione.

Il portachiavi iCloud è composto da due servizi:

- Aggiornamento costante del portachiavi su tutti i dispositivi
- Recupero del portachiavi

L'aggiornamento del portachiavi sui dispositivi iOS e computer Mac prevede che i dispositivi partecipino a questo servizio solo dopo l'approvazione dell'utente. Ogni elemento del portachiavi idoneo viene scambiato con una codifica specifica per il dispositivo mediante l'archiviazione del valore della chiave iCloud. Si tratta di elementi temporanei che una volta sincronizzati scompaiono da iCloud.

Con il ripristino del portachiavi gli utenti possono affidare il proprio portachiavi a Apple, che non avrà modo di leggere le password e gli altri dati al suo interno. Anche se l'utente ha un solo dispositivo iOS o computer Mac, il ripristino del portachiavi funge da rete di sicurezza contro la perdita dei dati. Ciò è particolarmente importante quando Safari viene utilizzato per generare password complesse casuali per gli account web, perché l'unica traccia di quelle password è nel portachiavi.

Se l'utente crea un codice di sicurezza iCloud, il portachiavi iCloud viene incluso nel backup su iCloud. L'autenticazione secondaria e il servizio di archiviazione sicura sono funzionalità importanti del recupero del portachiavi. Il portachiavi dell'utente viene codificato usando un codice complesso e il servizio di archiviazione fornisce una copia del portachiavi solo se vengono rispettate una serie di condizioni molto rigide.

Importante: Se l'utente non crea un codice di sicurezza iCloud, Apple non potrà fornire alcun servizio di ripristino del portachiavi. Consulta l'articolo del supporto Apple Domande frequenti sul portachiavi di iCloud.

iMessage

iMessage è un servizio di messaggistica per i dispositivi iOS e per i computer Mac che consente di eseguire chat di gruppo o singole. iMessage supporta testo e allegati come foto, contatti e posizioni. I messaggi appaiono su tutti i dispositivi iOS e computer Mac registrati dell'utente, così la conversazione può proseguire su ognuno di essi. iMessage utilizza il servizio di notifiche push di Apple (APNs) e sfrutta la codifica end-to-end con chiavi conosciute solo dai dispositivi iOS e computer Mac mittenti e riceventi. Apple non può decodificare i messaggi e questi non vengono registrati.

Nota: Potrebbero essere applicati i costi previsti dall'operatore per il traffico dati. Quando iMessage non è disponibile, i messaggi potrebbero essere inviati come SMS (alle tariffe previste dall'operatore).

FaceTime

FaceTime è il servizio Apple per le chiamate audio e video. Le chiamate FaceTime si servono del servizio di notifiche push di Apple per stabilire una connessione, dopodiché utilizzano i protocolli ICE (Internet Connectivity Establishment) e SIP (Session Initiation Protocol) per creare uno stream codificato. Gli utenti possono comunicare utilizzando una combinazione qualsiasi di dispositivi iOS e OS X con FaceTime installato.

Nota: Per chiamare con FaceTime, entrambi gli interlocutori devono disporre di un dispositivo con FaceTime e di una connessione Wi-Fi. FaceTime su rete cellulare richiede iPhone 4s e successivi, iPad con display Retina o successivi o iPad mini o successivi con funzione dati cellulare. La disponibilità del servizio su rete cellulare dipende dall'operatore. Potrebbero essere applicati i costi previsti per il traffico dati.

Siri

Basta parlare normalmente per chiedere a Siri di inviare messaggi, organizzare riunioni, telefonare e molto altro. Siri usa il riconoscimento vocale, la sintesi vocale e un modello client-server per rispondere alle richieste più disparate. Le attività supportate da Siri sono progettate per far sì che le informazioni personali vengano utilizzate in misura minima e siano totalmente protette. Le richieste a Siri e le registrazioni vocali non sono identificate in modo personale e, quando possibile, le funzioni di Siri sono eseguite sul dispositivo iOS invece che sul server.

Nota: Siri potrebbe non essere disponibile in tutte le lingue o in tutti i paesi, e le sue funzioni potrebbero variare a seconda dell'area geografica. È richiesto un accesso a Internet. Potrebbero essere applicati i costi previsti per il traffico dati cellulari.

ID Apple per studenti

Il programma ID Apple per studenti è pensato per studenti di età inferiore ai 13 anni. Gli ID Apple vengono richiesti dalla scuola o dal distretto scolastico e creati da Apple dopo aver ricevuto un modulo di autorizzazione sulla privacy e sulla divulgazione firmato da un genitore o da un tutore. Tale modulo è conforme al Children's Online Privacy Protection Act.

Per ulteriori informazioni sull'ID Apple per studenti, consulta:

- Il sito web di ID Apple per studenti
- Aiuto ID Apple per studenti

Nota: Il programma ID Apple per studenti non è disponibile in tutti i paesi o le regioni.

Servizio di notifiche push di Apple (APNs)

Molti servizi si avvalgono del servizio di notifiche push di Apple (APNs). Tale servizio è fondamentale perché consente ai dispositivi Apple di rilevare gli aggiornamenti disponibili, i criteri MDM e i messaggi in entrata. Per consentire ai dispositivi Apple di utilizzare questo tipo di servizi, devi abilitare il traffico di rete dal dispositivo alla rete Apple (17.0.0.0/8) sulla porta 5223, con un'opzione di fallback sulla porta 443.

Questo traffico si basa su un protocollo binario protetto specifico per le notifiche push di Apple (APNs) e non può avvenire mediante un proxy. Eventuali tentativi di analisi o rendirizzamento del traffico faranno sì che il client, il servizio di notifiche push di Apple (APNs) e i server dei provider del servizio push contrassegnino la conversazione come danneggiata e non valida.

Al servizio di notifiche push di Apple (APNs) sono applicati vari livelli di sicurezza in corrispondenza degli endpoint e dei server. Per informazioni tecniche relative alle misure cautelari implementate, consulta la guida di programmazione delle notifiche locali e remote.

Sicurezza 6

Panoramica

iOS e OS X sono progettati per offrire vari livelli di sicurezza. I dispositivi Apple possono quindi accedere in modo sicuro ai servizi di rete e proteggere i dati importanti. iOS e OS X prevedono inoltre una protezione sicura attraverso l'utilizzo di criteri relativi ai codici d'accesso e password che si possono distribuire e imporre via MDM. Inoltre, se un dispositivo Apple finisce nelle mani sbagliate, gli utenti e gli amministratori IT possono avviare operazioni di cancellazione a distanza per eliminare tutte le informazioni private.

Garantire la sicurezza dei dispositivi Apple per uso aziendale comporta i seguenti aspetti:

- Metodi che impediscono l'utilizzo non autorizzato del dispositivo
- Protezione dei dati archiviati, anche quando il dispositivo viene smarrito o rubato
- Protocolli di rete e codifica dei dati che vengono trasmessi
- Esecuzione delle app in sicurezza e senza compromettere l'integrità della piattaforma.

Queste funzioni operano in sinergia per creare una piattaforma mobile estremamente sicura. Per ulteriori informazioni sulla sicurezza con iOS, consulta iOS e il nuovo IT.

Sicurezza dei dispositivi e dei dati

Panoramica

Stabilire criteri sicuri per accedere ai dispositivi Apple è fondamentale per la protezione delle informazioni della tua organizzazione. I codici di accesso sicuri per i dispositivi iOS sono uno strumento potente per proteggere i dispositivi dall'accesso non autorizzato. Tali codici possono essere configurati e applicati via MDM.

I dispositivi iOS utilizzano un codice di accesso univoco stabilito da ogni utente per generare una chiave di codifica sofisticata che aumenta la protezione della posta e dei dati delle applicazioni sul dispositivo. Inoltre iOS offre metodi sicuri per configurare il dispositivo in un ambiente IT che richiede impostazioni, criteri e restrizioni specifici. Questi metodi offrono opzioni flessibili per stabilire un livello di protezione standard per gli utenti autorizzati.

Criteri per codici di accesso

Il codice d'accesso per un dispositivo iOS impedisce agli utenti non autorizzati di accedere al dispositivo. iOS ti consente di scegliere tra un'ampia gamma di requisiti per il codice d'accesso in base alle tue esigenze di sicurezza.

Tali requisisti includono:

- Richiedi l'utilizzo di un codice di accesso su un dispositivo iOS
- Richiedi valore alfanumerico
- Lunghezza minima del codice
- Numero minimo di caratteri complessi

- Tempo massimo di validità del codice
- Intervallo di tempo prima del blocco automatico
- Cronologia dei codici
- Intervallo per il blocco del dispositivo
- Numero massimo di tentativi non riusciti prima che il dispositivo iOS venga cancellato

Imposizione dei criteri

I criteri si possono distribuire come parte di un profilo di configurazione che l'utente deve installare. È anche possibile definire il profilo in modo che possa essere cancellato esclusivamente fornendo una password da amministratore, oppure bloccarlo e impedirne la rimozione senza la parallela cancellazione di tutti i contenuti del dispositivo iOS. Le impostazioni dei criteri d'accesso si possono configurare via MDM trasmettendole direttamente al dispositivo. Questo consente di imporli e aggiornarli senza alcuna operazione da parte dell'utente.

Se un dispositivo è configurato in modo da accedere a un account Microsoft Exchange, i criteri di Exchange ActiveSync vengono inviati in modalità wireless. I criteri disponibili variano in base alla versione di Exchange ActiveSync e Exchange Server. Qualora esista sia un criterio Exchange sia un criterio MDM, verrà applicato quello più rigido.

Configurazione sicura del dispositivo

Un profilo di configurazione è un file XML che contiene criteri di sicurezza e restrizioni, informazioni sulla configurazione VPN, impostazioni Wi-Fi, account e-mail e di calendario e credenziali di autenticazione che consentono ai dispositivi iOS di funzionare con i tuoi sistemi IT. La possibilità di fissare in un profilo di configurazione sia i criteri del codice d'accesso sia le impostazioni del dispositivo garantisce che i dispositivi siano configurati correttamente e secondo gli standard di sicurezza stabiliti dal tuo reparto IT. Poiché i profili di configurazione possono essere codificati e bloccati, le impostazioni non possono essere eliminate, modificate o condivise con altri.

I profili di configurazione possono essere sia firmati sia criptati. Firmando un profilo di configurazione, si garantisce che i parametri imposti non possano essere modificati in alcun modo. La codifica, invece, protegge i contenuti del profilo e consente l'installazione solo sul dispositivo per il quale è stato creato. I profili di configurazione vengono codificati con CMS (Cryptographic Message Syntax, RFC 3852), che supporta 3DES e AES 128.

Per distribuire per la prima volta i profili di configurazione codificati, puoi installarli tramite un collegamento USB con Apple Configurator, in wireless tramite il protocollo di distribuzione e configurazione dei profili over-the-air, oppure via MDM. Successivamente i profili di configurazione codificati possono essere distribuiti allegandoli a un'e-mail, ospitandoli su un sito web accessibile agli utenti o trasferendoli sui dispositivi attraverso soluzioni MDM.

Per ulteriori informazioni, consulta Distribuzione e configurazione dei profili over-the-air.

Protezione dei dati

Dati sensibili come i messaggi e-mail e gli allegati archiviati sul dispositivo possono essere ulteriormente protetti grazie alle funzioni di protezione dei dati integrate in iOS. La protezione dei dati utilizza il codice di accesso univoco dell'utente unitamente alla codifica hardware dei dispositivi iOS per generare una chiave di codifica forte, che impedisce l'accesso ai dati quando il dispositivo è bloccato. In questo modo le informazioni più importanti sono al sicuro anche se il dispositivo viene compromesso.

Per attivare la protezione dei dati è sufficiente definire un codice d'accesso. Poiché l'efficacia di questa funzione dipende dall'efficacia del codice di accesso, è importante richiedere l'utilizzo di codici formati da più di quattro caratteri.

Gli utenti possono verificare se la protezione dei dati è attiva osservando la schermata delle impostazioni del codice d'accesso, mentre le soluzioni MDM possono ottenere questa informazione interrogando l dispositivo.

Vi sono inoltre a disposizione degli sviluppatori della API di protezione dei dati, che possono essere utilizzate per tutelare i dati delle app di App Store o di quelle in-house sviluppate ad hoc. Con iOS 7 o versione successiva, i dati archiviati dalle app si trovano di default nella classe "Protetto fino a prima autenticazione", che è simile alla codifica dell'intero disco sui computer desktop e protegge i dati da attacchi che prevedono un riavvio.

iOS 8 offre la protezione dei dati di Calendario, Contatti, Messaggi, Note, Promemoria e libri e PDF gestiti.

Nota: Se un dispositivo è stato aggiornato da iOS 6, gli archivi di dati esistenti non vengono convertiti alla nuova classe. Per far sì che l'app riceva la nuova classe di protezione, occorre rimuoverla e installarla di nuovo.

Codifica

I dispositivi iOS usano una codifica basata su hardware che adotta lo standard AES a 256 bit per proteggere tutti i dati sul dispositivo. La codifica è sempre attiva e non può essere disabilitata. È inoltre possibile codificare i dati contenuti nei backup di iTunes sul computer dell'utente. Questa funzione può essere attivata dall'utente oppure applicata tramite le impostazioni di restrizione dei profili di configurazione.

I moduli di codifica di iOS 6 o versione successiva sono convalidati per la compatibilità con gli standard statunitensi FIPS (Federal Information Processing Standard) 140-2 Livello 1. In questo modo, viene convalidata l'integrità delle operazioni di codifica nelle app di Apple e nelle app di altri sviluppatori che utilizzano correttamente i servizi di codifica di iOS.

Per ulteriori informazioni, consulta gli articoli del supporto Apple,
Sicurezza dei prodotti iOS: convalida e linee guide e Moduli di codifica Apple 4.0 convalidati FIPS.

S/MIME per messaggio

iOS 8 e OS X Yosemite supportano S/MIME per messaggio, che consente agli utenti di scegliere se firmare e codificare sempre di default oppure firmare e/o codificare in maniera selettiva i singoli messaggi e ottenere quindi un maggiore controllo sulla sicurezza di ciascuna e-mail.

I certificati da utilizzare con S/MIME possono essere distribuiti ai dispositivi Apple tramite un profilo di configurazione, via MDM o SCEP. Ciò offre al reparto IT tutta la flessibilità necessaria per garantire che tutti gli utenti dispongano dei certificati appropriati installati.

Indirizzi e-mail esterni

iOS 8 e OS X Yosemite supportano la creazione di un elenco di domini con specifici suffissi. I messaggi e-mail che non sono indirizzati ai domini nella lista di quelli approvati vengono contrassegnati in rosso. Ad esempio, un utente potrebbe avere sia example.com e gruppo.example.com nel proprio elenco di domini conosciuti. Se un utente nel cui elenco di domini conosciuti sono inclusi example.com e group.example.com immette anyone@acme.com in un messaggio e-mail, tale indirizzo verrà contrassegnato per informare l'utente che il dominio acme.com non è incluso nell'elenco dei domini approvati.

Touch ID

Touch ID è il sistema di rilevamento di impronte digitali integrato in alcuni dispositivi iOS che permette di accedere al dispositivo in tutta sicurezza e in modo semplice e veloce e più protetto. Questa tecnologia legge le impronte digitali da qualsiasi angolazione, e nel tempo impara a conoscerle sempre meglio: il sensore continua ad ampliare la mappa dell'impronta perché a ogni utilizzo vengono individuati nuovi nodi corrispondenti.

Con Touch ID, usare un codice di accesso più lungo e complesso diventa più semplice perché non dovrà essere inserito spesso.

Quando Touch ID è attivo, il dispositivo si blocca non appena si preme il tasto Standby/Riattiva. Quando utilizzano il solo codice di accesso, molti utenti impostano un tempo di sblocco durante il quale potranno usare il dispositivo senza dover inserire ogni volta il codice. Con Touch ID il dispositivo si blocca ogni volta che va in standby, e per riattivarlo serve un'impronta digitale o, facoltativamente, il codice di accesso.

Touch ID funziona con Secure Enclave, un coprocessore inserito nel chip A7 di Apple. Secure Enclave ha una sua memoria protetta e codificata e comunica in modo sicuro con il sensore Touch ID. Quando il dispositivo si blocca, le chiavi Complete per la classe Data Protection sono protette da una chiave conservata nella memoria codificata del Secure Enclave. La chiave viene conservata per un massimo di 48 ore ed eliminata se si riavvia il dispositivo o se si utilizza un'impronta digitale sconosciuta per cinque volte. Se l'impronta viene riconosciuta, il Secure Enclave fornisce la chiave per aprire le chiavi Data Protection e il dispositivo viene sbloccato.

iOS 8 introduce l'utilizzo di Touch ID per accedere ad app di terze parti. Se lo sviluppatore ha integrato tale funzionalità nella propria app, l'utente non avrà bisogno di inserire una password. Qualsiasi elemento del portachiavi specificato dallo sviluppatore può essere sbloccato tramite Touch ID. I dati dell'impronta digitale dell'utente vengono protetti e né iOS né le app vi possono accedere.

Cancellazione a distanza

I dispositivi Apple supportano completamente la cancellazione da remoto. Se un dispositivo Apple viene smarrito o rubato, un amministratore o il proprietario del dispositivo stesso possono eseguire un comando di cancellazione da remoto per rimuovere tutti i dati e disattivare il dispositivo, tramite una soluzione MDM oppure la funzionalità "Trova il mio iPhone" di iCloud. Se il dispositivo è configurato con un account Exchange, si può avviare la cancellazione a distanza da Exchange Management Console (Exchange Server 2007) o Exchange ActiveSync Mobile Administration Web Tool (Exchange Server 2003 o 2007). Gli utenti di Exchange Server 2007 possono inviare il comando di cancellazione a distanza usando direttamente Outlook Web Access.

Cancellazione locale

È possibile configurare i dispositivi affinché avviino automaticamente una cancellazione locale dopo vari tentativi di inserimento del codice non riusciti. È un deterrente fondamentale contro i tentativi di accedere al dispositivo con la forza. Una volta stabilito il codice di accesso, gli utenti possono attivare la cancellazione locale direttamente dalle impostazioni. Di default, iOS cancella automaticamente i dati dopo 10 tentativi di inserimento non riusciti. Il numero massimo di tentativi falliti può essere impostato con un profilo di configurazione, tramite un server MDM oppure imposto via etere tramite i criteri di Microsoft Exchange ActiveSync.

Sicurezza della rete

Gli utenti di dispositivi mobili devono poter accedere a reti aziendali da qualsiasi parte del mondo, tuttavia è importante anche assicurarsi che gli utenti siano autorizzati e che i loro dati siano protetti nel corso della trasmissione. Le tecnologie integrate di sicurezza delle reti in iOS garantiscono questi obiettivi di sicurezza sia per le connessioni Wi-Fi sia per quelle cellulari.

La sicurezza della rete di iOS supporta:

- Protocolli Cisco IPSec, L2TP, IKEv2, PPTP integrati
- SSL VPN tramite le app di App Store
- SSL/TLS con certificati X.509
- WPA/WPA2 Enterprise con 802.1X
- Autenticazione basata su certificati
- RSA SecurID, CRYPTOCard

VPN

Molti ambienti aziendali dispongono di alcune forme di reti private virtuali (VPN, Virtual Private Network). Questi servizi di rete sicuri di solito richiedono impostazioni e configurazioni minime per funzionare con dispositivi Apple, che si integrano con un'ampia gamma di tecnologie VPN tra le più comuni.

Per maggiori dettagli, consulta la Panoramica sulle VPN.

IPSec

iOS e OS X supportano i protocolli e i metodi di autenticazione IPSec. Per maggiori dettagli, consulta Protocolli e metodi di autenticazione supportati.

SSL/TLS

iOS supporta SSL v3 e Transport Layer Security (TLS v1.0, 1.1 e 1.2). Safari, Calendario, Mail e altre applicazioni Internet avviano automaticamente questi meccanismi per instaurare un canale di comunicazione codificato tra iOS e OS X e i servizi aziendali.

WPA/WPA2

iOS e OS X supportano WPA2 Enterprise per fornire un accesso autenticato alla rete wireless della tua azienda. WPA2 Enterprise utilizza la codifica AES a 128 bit, così da proteggere i dati degli utenti durante la comunicazione tramite una connessione di rete Wi-Fi. Grazie al supporto di 802.1X, i dispositivi Apple possono essere integrati in un'ampia gamma di ambienti di autenticazione RADIUS.

iOS e OS X supportano i seguenti protocolli di autenticazione 802.1X:

- EAP-TLS
- EAP-TTLS
- EAP-FAST
- EAP-SIM
- EAP-AKA
- PEAP v0, v1
- LEAP

Per ulteriori informazioni, consulta la Panoramica su Wi-FI.

Codifica di FaceTime e iMessage

Ogni sessione FaceTime e conversazione iMessage viene codificata. iOS e OS X creano un ID univoco per ciascun utente, garantendo che le comunicazioni siano codificate, instradate e connesse adeguatamente.

Sicurezza delle app

Per evitare che le app vengano danneggiate o manomesse, iOS e OS X includono un approccio "sandboxed" per la protezione in fase di runtime e per la firma delle app. iOS e OS X includono inoltre la funzionalità Portachiavi, un framework che semplifica l'archiviazione sicura delle credenziali di app e servizi di rete in una posizione di archiviazione codificata. Inoltre iOS e OS X offrono agli sviluppatori un'architettura Common Crypto per codificare i dati archiviati dalle app.

Protezione runtime

Tutte le app disponibili in App Store sono "sandboxed" per limitare l'accesso ai dati archiviati da altre applicazioni. Inoltre i file, le risorse e il kernel del sistema sono protetti dallo spazio in cui sono attive le app dell'utente. Se un'app richiede l'accesso ai dati di un'altra app, può farlo solo tramite le API e i servizi forniti da iOS e OS X. Viene inoltre impedita la generazione di codice.

Firma obbligatoria del codice

Tutte le app disponibili in App Store devono essere firmate. Le app fornite con il dispositivo Apple sono firmate da Apple, quelle di altri produttori sono firmate dallo sviluppatore tramite un certificato emesso da Apple. Questo garantisce che le app non siano state manomesse o alterate. Per garantire che un'applicazione non sia divenuta inattendibile dall'ultima volta in cui è stata usata, vengono effettuati controlli runtime.

L'uso di app aziendali in-house personalizzate può essere controllato tramite un profilo di fornitura: per avviare l'app, gli utenti devono avere installato tale profilo. I profili di fornitura si possono installare via etere per mezzo di soluzioni MDM. È inoltre possibile limitare l'uso di un'app a dispositivi specifici.

Framework di autenticazione sicuro

iOS e OS X forniscono un portachiavi sicuro e cifrato per l'archiviazione di identità digitali, nomi utenti e password. I dati del portachiavi vengono suddivisi e protetti mediante elenchi di controllo degli accessi, in modo tale che le credenziali archiviate da app di terze parti non possano essere utilizzate da app con identità diverse, a meno che l'utente non le approvi in modo esplicito. Con questo meccanismo si proteggono le credenziali di autenticazione memorizzate sui dispositivi Apple per una gamma di app e servizi all'interno di un'organizzazione.

Architettura Common Crypto

Gli sviluppatori possono utilizzare API di codifica per proteggere i dati delle proprie app. I dati possono essere codificati simmetricamente tramite metodi collaudati come AES, RC4 o 3DES. Inoltre i dispositivi iOS e gli attuali computer Mac con processori Intel forniscono l'accelerazione hardware per la codifica AES e l'hashing SHA1, massimizzando così le prestazioni dell'applicazione.

Protezione dei dati delle app

Le app possono sfruttare anche la codifica hardware integrata dei dispositivi iOS per proteggere ancora di più i dati sensibili. Gli sviluppatori possono definire file specifici da proteggere: quando il dispositivo è bloccato, il sistema cripta i contenuti dei file rendendoli inaccessibili sia all'app sia a potenziali intrusi.

Autorizzazioni delle app

Di default, un dispositivo iOS ha privilegi molto limitati. Gli sviluppatori devono aggiungere esplicitamente le autorizzazioni per utilizzare la maggior parte delle funzioni, come iCloud, elaborazione in background e portachiavi condivisi. In questo modo le app non possono accedere a dati che non le riguardano. Inoltre, le app iOS devono ottenere il permesso esplicito dell'utente anche per usare molte delle funzioni di iOS, come localizzazione GPS, contatti, fotocamera e foto archiviate.

Single Sign-On e Touch ID

Gli sviluppatori possono sfruttare Single Sign-On e Touch ID per fornire un'integrazione sicura e senza interruzioni dell'autenticazione tra diverse app e consentire l'autenticazione tramite Touch ID.

Per ulteriori informazioni, consulta Configurare il Single Sign-on e Touch ID.

Configurazione e gestione 7

Panoramica

Le distribuzioni di dispositivi Apple possono essere ottimizzate adottando alcune tecniche di gestione che semplificano l'impostazione degli account, la configurazione dei criteri istituzionali, la distribuzione delle app e l'applicazione delle restrizioni. Puoi configurare le preferenze di iOS e OS X e gli account manualmente oppure con una soluzione MDM. La funzione "Impostazione assistita", integrata nei dispositivi Apple, permette agli utenti di occuparsi della configurazione iniziale. E una volta configurati e registrati i dispositivi per la gestione MDM, il reparto IT potrà gestirli in modalità wireless.

La MDM fornisce alla tua organizzazione l'abilità di registrare in maniera sicura i dispositivi Apple nell'ambito aziendale e didattico, configurare e aggiornare le impostazioni in modalità wireless, monitorare la conformità con i criteri, distribuire app e cancellare o bloccare da remoto i dispositivi gestiti. Le soluzioni MDM disponibili per le varie piattaforme server sono molteplici. Ogni soluzione offre la propria console di gestione, le proprie funzionalità e le proprie tariffe. Prima di scegliere una soluzione MDM, consulta questo paragrafo per individuare quali funzionalità sono più importanti per la tua organizzazione.

A seconda di chi è il possessore dei dispositivi Apple e dal modo in cui vengono distribuiti, vi sono diversi flussi di lavoro per la configurazione e diverse possibilità. Per ulteriori informazioni, consulta la Panoramica sui modelli di distribuzione.

Questo paragrafo descrive l'insieme completo di strumenti, programmi e servizi disponibili a supporto della distribuzione di dispositivi Apple.

"Impostazione assistita" e attivazione

iOS e OS X offrono "Impostazione assistita" per attivare ogni nuovo dispositivo Apple o un dispositivo Apple inizializzato, per configurare impostazioni di base e personalizzare le preferenze come lingua, servizi di localizzazione, Siri, iCloud e "Trova il mio iPhone". Gli utenti possono utilizzare queste funzionalità per rendere operativo un dispositivo Apple appena tolto dalla confezione oppure queste operazioni di configurazione di base possono essere eseguite dall'organizzazione. Inoltre, se l'utente non ha un ID Apple, "Impostazione assistita" gli consente di crearne uno.

Nei dispositivi Apple registrati nel DEP e gestiti tramite MDM, queste schermate di "Impostazione assistita" possono essere saltate:

- *Ripristino da backup:* non viene eseguito un ripristino da backup.
- *ID Apple:* all'utente non viene richiesto di accedere con un ID Apple.
- *Termini e condizioni:* i termini e le condizioni vengono saltati.
- *Invio informazioni diagnostiche:* le informazioni diagnostiche non vengono inviate automaticamente.
- *Posizione (solo iOS):* i servizi di localizzazione non vengono attivati.

- *Touch ID (solo iOS):* "Touch ID" non viene abilitato.
- *Codice (solo iOS):* l'impostazione del codice di accesso viene saltata.
- *Apple Pay (solo iOS):* Apple Pay non viene abilitato.
- *Siri (solo iOS):* Siri non viene abilitato.
- *Zoom schermo (solo iOS):* "Zoom schermo" non viene abilitato.
- *Registrazione (solo OS X):* non viene consentita la registrazione.
- *FileVault (solo OS X):* FileVault non viene abilitato.

A meno che questi elementi non vengano limitati in modo definitivo utilizzando la soluzione MDM, gli utenti potranno eseguire le suddette operazioni dopo la configurazione del dispositivo Apple.

Per ulteriori informazioni sul DEP, consulta

- DEP (Device Enrollment Program)
- DEP (Device Enrollment Program)
- Aiuto Programmi di Distribuzione Apple

Profili di configurazione

Un profilo di configurazione è un file XML utilizzato per distribuire informazioni di configurazione ai dispositivi Apple. I profili di configurazione automatizzano la configurazione di impostazioni, account, restrizioni e credenziali. Possono essere installati tramite un allegato a un messaggio e-mail, scaricati da una pagina web o installati sui dispositivi iOS tramite Apple Configurator. Se ti occorre configurare un alto numero di dispositivi iOS o preferisci semplicemente un modello di distribuzione via etere, puoi fornire i profili di configurazione tramite la MDM.

I profili di configurazione che contengono payload di certificato e Wi-Fi possono essere installati anche su Apple TV. Per ulteriori informazioni, consulta l'articolo del supporto Apple Come installare un profilo di configurazione su Apple TV.

I profili di configurazione possono essere codificati e firmati; questo ti consente di restringerne l'uso a un dispositivo Apple specifico e impedisce che le impostazioni in essi contenute vengano modificate. Un amministratore MDM può anche contrassegnare un profilo come bloccato, così una volta installato potrà essere rimosso solo cancellando tutti i dati sul dispositivo oppure inserendo una password.

A eccezione dei codici d'accesso, gli utenti non potranno modificare le impostazioni fornite in un profilo di configurazione. Gli account configurati attraverso un profilo, come ad esempio gli account Exchange, possono essere rimossi solo mediante l'eliminazione del profilo.

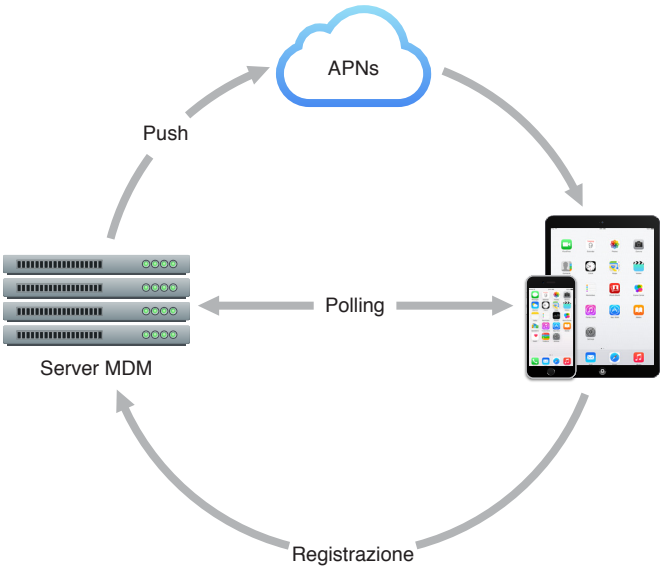
Per ulteriori informazioni, consulta il
materiale di riferimento sulle chiavi dei profili di configurazione.

MDM (Mobile Device Management)

Panoramica

Il supporto di iOS e OS X per la MDM consente al reparto IT di configurare e gestire in modo sicuro le distribuzioni scalate di dispositivi Apple all'interno delle organizzazioni. A tale scopo, iOS e OS X integrano un framework MDM che permette alle soluzioni MDM di terze parti di interagire in modalità wireless con i dispositivi Apple. È una struttura leggera e modulare, progettata appositamente per i dispositivi Apple, ma abbastanza potente da poter configurare e gestire nel modo più completo tutti i dispositivi iOS, OS X e Apple TV di un'organizzazione.

Una soluzione MDM ti permette registrare in maniera sicura i dispositivi Apple in un'organizzazione, di configurare e aggiornare le impostazioni, di monitorarne la conformità con i criteri aziendali e di inizializzare o bloccare a distanza i dispositivi gestiti. La MDM per iOS e OS X offre agli utenti un metodo semplice per accedere ai servizi di rete e contemporaneamente garantisce la corretta configurazione dei dispositivi Apple, indipendentemente da chi ne è il proprietario.



Le soluzioni MDM usano il servizio di notifiche push di Apple (APNs) per mantenere una comunicazione persistente con i dispositivi Apple sulle reti sia pubbliche sia private. MDM richiede vari certificati, tra cui un certificato APNs per comunicare con i client e un certificato SSL per comunicare in modo sicuro. Le soluzioni MDM possono anche firmare i profili con un certificato. Le funzionalità MDM sono integrate nelle tecnologie iOS e OS X esistenti, come ad esempio i profili di configurazione, la registrazione in modalità wireless e le notifiche push di Apple (APNs). Ad esempio, le notifiche push di Apple (APNs) vengono utilizzate per riattivare il dispositivo in modo che possa comunicare direttamente con il relativo server MDM su una connessione protetta.

Importante: Tramite le notifiche push di Apple (APNs) non vengono trasmesse informazioni riservate o sensibili.

La MDM consente al tuo reparto IT di registrare in sicurezza dispositivi Apple di proprietà degli utenti e di proprietà dell'azienda. Una soluzione MDM ti permette di configurare e aggiornare le impostazioni, di monitorarne la conformità con i criteri aziendali e di cancellare o bloccare a distanza i dispositivi Apple gestiti. La MDM permette inoltre di distribuire, gestire e configurare app e libri acquistati tramite il VPP o sviluppati all'interno dell'azienda.

Per ulteriori informazioni sulla MDM, consulta:

- L'informatica in classe - Gestione dei dispositivi
- iOS e nuovo IT per le aziende

Nella maggior parte dei casi i certificati, inclusi quelli APNs, devono essere rinnovati annualmente. Se il certificato è scaduto, il server MDM non può più comunicare con i dispositivi Apple finché il certificato non viene aggiornato, quindi dovrai ricordarti di procedere all'aggiornamento prima della scadenza. Contatta l'autorità di certificazione per ulteriori informazioni sul rinnovo dei tuoi certificati. Per ulteriori informazioni sulle notifiche push di Apple (APNs), consulta il sito web di Apple Push Certificates Portal.

Per abilitare la gestione, i dispositivi Apple vengono registrati con un server MDM tramite un profilo di configurazione per la registrazione. Questa operazione può essere eseguita direttamente dall'utente. Per i dispositivi di proprietà dell'azienda, la registrazione alla MDM può essere automatizzata attraverso il DEP (descritto in questo paragrafo). Quando un amministratore attiva un criterio, un'opzione o un comando tramite la MDM, i dispositivi Apple ricevono una notifica push dell'azione tramite le notifiche push di Apple (APNs). Con una connessione di rete, i dispositivi possono ricevere comandi APNs in qualsiasi parte del mondo.

Registrazione

La registrazione dei dispositivi Apple permette di catalogarli e di gestirli. Il processo di registrazione in genere sfrutta il protocollo SCEP (Simple Certificate Enrollment Protocol), che consente a un dispositivo di creare e registrare certificati d'identità univoci per autenticare l'accesso ai servizi dell'organizzazione.

Nella maggior parte dei casi, gli utenti decidono se registrare o meno il proprio dispositivo Apple per la gestione MDM e possono dissociarlo in qualsiasi momento, ma è buona norma incentivare il mantenimento della gestione. Ad esempio, dovresti richiedere la registrazione per l'accesso alla rete Wi-Fi utilizzando la soluzione MDM per fornire automaticamente le credenziali wireless. Quando un utente lascia la gestione MDM, il relativo dispositivo tenta di inviare una notifica al server MDM.

Per registrare automaticamente i dispositivi Apple di proprietà dell'organizzazione con la soluzione MDM durante la configurazione iniziale può essere usato anche il Device Enrollment Program. Puoi anche supervisionare i dispositivi iOS in modo tale che gli utenti che usano questi dispositivi non possano bypassare la MDM né annullare la registrazione.

Per ulteriori informazioni, consulta DEP (Device Enrollment Program).

Configurazione

Una volta registrato, un dispositivo Apple può essere configurato dinamicamente con impostazioni e criteri tramite il server MDM, che invierà profili di configurazione che verranno installati automaticamente e senza notifiche da parte di iOS o OS X.

I profili di configurazione possono essere firmati, codificati e bloccati per impedire che le impostazioni vengano modificate o condivise, in modo che solo gli utenti e i dispositivi Apple affidabili, configurati secondo le tue specifiche, abbiano accesso alla rete e ai servizi dell'azienda. Se un utente dissocia il dispositivo dalla MDM, tutte le impostazioni installate via MDM saranno rimosse.

In iOS 8, una nuova interfaccia per i profili mostra agli utenti quali elementi sono stati configurati e hanno ricevuto restrizioni tramite la MDM. Adesso è possibile vedere facilmente account, app, libri e restrizioni. In iOS 8, i profili di fornitura non sono più visibili agli utenti e i profili scaduti vengono rimossi automaticamente.

Account

La MDM può aiutare gli utenti a impostare rapidamente e in automatico account di posta e altro. A seconda della soluzione MDM adottata e della sua integrazione con i tuoi sistemi interni, i payload degli account possono essere precompilati con un nome utente, un indirizzo e-mail e, se necessario, identità di certificati per l'autenticazione e la firma.

È possibile configurare via MDM i seguenti tipi di account.

- Calendario
- Contatti
- Exchange ActiveSync
- Identità
- Jabber
- LDAP
- Posta
- Calendari a cui si è iscritti
- VPN
- 802.1X

Gli account di posta e calendario gestiti rispettano le restrizioni di apertura gestita di iOS 7 o versione successiva.

Query

Il server MDM può interrogare i dispositivi Apple per ottenere una serie di informazioni, che comprendono le informazioni sull'hardware, come ad esempio numero di serie, UDID dispositivo, indirizzo MAC Wi-Fi o stato della codifica FileVault (per OS X). Sono inoltre comprese informazioni sul software, come ad esempio versione del dispositivo, restrizioni e un elenco dettagliato di tutte le app installate sul dispositivo. Tali informazioni possono essere utilizzate per assicurarsi che gli utenti dispongano sempre del giusto set di app. iOS e OS X consentono di interrogare i dispositivi per conoscere la data e l'ora dell'ultimo backup su iCloud e l'hash dell'account per l'assegnazione delle app dell'utente collegato.

Con il software per Apple TV 5.4 o successivo, il sistema MDM può interrogare i dispositivi per raccogliere informazioni come lingua, luogo e organizzazione.

Attività di gestione

Quando un dispositivo iOS è gestito, può essere amministrato dal server MDM tramite un insieme di attività specifiche. Di seguito trovi alcune delle attività che si possono gestire.

- *Modificare le impostazioni di configurazione:* È possibile inviare un comando per installare un profilo di configurazione nuovo o aggiornato su un dispositivo Apple. La configurazione viene modificata senza notifiche e senza alcun intervento da parte dell'utente.
- *Bloccare un dispositivo iOS:* se si deve bloccare un dispositivo iOS all'istante, è possibile inviare un comando di blocco con l'attuale codice di accesso.

- *Cancellare a distanza un dispositivo iOS:* se un dispositivo iOS viene smarrito o rubato, è possibile inviare un comando per cancellare tutti i dati al suo interno. Una volta ricevuto, il comando di cancellazione a distanza non può essere annullato.
- *Cancellare un codice di blocco:* se si cancella un codice di blocco, il dispositivo iOS richiede immediatamente all'utente di inserire un nuovo codice d'accesso. Si utilizza quando l'utente dimentica il codice di accesso e vuole che il reparto IT lo ripristini.
- *Cancellare la password delle restrizioni:* supporto per la cancellazione delle restrizioni e della password delle restrizioni impostate sul dispositivo iOS dall'utente. Questa funzionalità è disponibile solo per i dispositivi supervisionati.
- *Richiedere Duplicazione AirPlay* Aggiunge un comando per chiedere a un dispositivo iOS supervisionato di avviare Duplicazione AirPlay verso una specifica destinazione.
- *Interrompere Duplicazione AirPlay* Aggiunge un comando per chiedere a un dispositivo iOS supervisionato di interrompere Duplicazione AirPlay verso una specifica destinazione.

Alcune attività possono essere messe in coda in iOS 8 o versione successiva e in OS X Mavericks o versione successiva se il dispositivo è in "Impostazione assistita". Queste attività sono:

- Invito al VPP
- Installare app
- Installare contenuti multimediali
- Bloccare un dispositivo
- Richiedere Duplicazione AirPlay (solo iOS)

App gestite

La distribuzione di app agli utenti può incentivare la loro produttività al lavoro o in classe. Tuttavia, a seconda dei requisiti dell'organizzazione, potresti aver bisogno di controllare in che modo tali app si collegano alle risorse interne o di gestire la sicurezza dei dati quando un utente lascia l'organizzazione, il tutto senza intaccare i dati e le app personali dell'utente. Le app gestite in iOS 7 o versione successiva e OS X Yosemite o versione successiva consentono alle organizzazioni di distribuire in modalità wireless via MDM app gratuite, a pagamento e aziendali con un server MDM, offrendo nel contempo il giusto equilibrio tra sicurezza istituzionale e personalizzazione dell'utente.

I server MDM possono distribuire le app da App Store e le app sviluppate internamente ai dispositivi Apple in modalità wireless. Inoltre, possono gestire le app gratuite e a pagamento di App Store usando la distribuzione gestita del VPP (Volume Purchase Program). Per ulteriori informazioni sulla distribuzione gestita tramite MDM, consulta la Panoramica di Volume Purchase Program.

L'installazione delle app VPP può avvenire nei seguenti modi:

- La MDM chiede agli utenti con un dispositivo Apple personale di installare l'app da App Store inserendo il proprio ID Apple.
- Se il dispositivo iOS supervisionato è di proprietà dell'organizzazione ed è registrato via MDM, l'installazione delle app avviene senza notifiche.

Le app gestite possono essere rimosse da remoto dal server MDM o quando l'utente scollega il proprio dispositivo Apple dal sistema MDM. Se si rimuove un'app, vengono rimossi anche i dati ad essa associati. Se l'app del VPP è ancora assegnata all'utente o se l'utente ha usato un codice di riscatto con il proprio ID Apple, l'app potrà essere nuovamente scaricata da App Store, ma non sarà gestita. Se viene revocata, un'app continuerà a funzionare per un periodo limitato di tempo. Trascorso tale periodo, l'app viene disabilitata e l'utente riceverà una notifica per informarlo che dovrà acquistare una copia personale se vorrà continuare a utilizzare l'app.

iOS 7 ha aggiunto alle app gestite una serie di restrizioni e funzionalità che aumentano la sicurezza e migliorano l'esperienza utente.

- *Apertura gestita:* Offre due utili opzioni per proteggere i dati delle app delle organizzazioni:
  - *Consenti documenti da sorgenti non gestite in destinazioni gestite.* Applicando questa restrizione, si impedisce che le sorgenti e gli account personali dell'utente aprano documenti nelle destinazioni gestite dell'organizzazione. Ad esempio, questa restrizione può impedire che una copia di Keynote di proprietà dell'utente apra una presentazione in formato PDF in un'app aziendale per la visualizzazione dei PDF. Può anche impedire all'account iCloud dell'utente di aprire un allegato a un'e-mail in una copia di Pages di proprietà dell'organizzazione.
  - *Consenti documenti da sorgenti gestite in destinazioni non gestite.* Applicando questa restrizione, si impedisce che le sorgenti e gli account gestiti dall'organizzazione aprano i documenti nelle destinazioni personali dell'utente. Questa restrizione può impedire che gli allegati e-mail riservati negli account di posta gestiti dall'azienda vengano aperti nelle app personali dell'utente.
- *Configurazione delle app:* Permette agli sviluppatori di identificare i parametri che si possono impostare quando l'app viene installata come gestita. I parametri di configurazione possono essere installati prima o dopo l'installazione dell'app gestita.
- *Feedback dalle app:* Gli sviluppatori hanno la possibilità di identificare le impostazioni delle app gestite che possono essere dal server MDM. Ad esempio, è possibile specificare una chiave DidFinishSetup che il server MDM può richiedere per determinare se l'app è stata avviata e configurata.
- *Impedisci il backup:* Questa restrizione impedisce alle app gestite di includere i propri dati nei backup di iCloud o iTunes. Impedendo il backup si impedisce il ripristino dei dati dell'app gestita quando viene rimossa via MDM e reinstallata dall'utente.

iOS 8 introduce le seguenti funzionalità di gestione:

- *Download di Safari da domini gestiti:* I download da Safari vengono considerati documenti gestiti se sono originati da un dominio gestito. Ad esempio, se un utente scarica un PDF utilizzando Safari da un dominio gestito, a tale PDF vengono applicate tutte le impostazioni dei documenti gestiti.
- *Gestione dei documenti di iCloud:* Questa restrizione impedisce alle app gestite di archiviare dati in iCloud. Ad esempio, i dati creati o utilizzati da un'app gestita non possono essere archiviati in iCloud, ma i dati creati dagli utenti in app non gestite possono essere archiviati in iCloud.

Restrizioni alle tastiere di terze parti

iOS 8 supporta regole di apertura gestita applicabili a estensioni di tastiera di terze parti. Ciò impedisce a tastiere non gestite di essere visualizzate in app gestite.

Libri gestiti

iOS 8 e OS X Mavericks o versione successiva consentono di distribuire e gestire libri, ePub e PDF creati o acquistati via MDM. Ciò garantisce una gestione semplificata e senza interruzioni di materiali didattici e altri documenti aziendali.

I libri, gli ePub e i PDF distribuiti tramite MDM hanno le stesse proprietà degli altri documenti gestiti: possono essere condivisi solo con altre app gestite o inviati via e-mail solo tramite gli account gestiti. I libri acquistati tramite il VPP possono essere distribuiti in maniera gestita, ma non possono essere revocati e riassegnati. Un libro acquistato dall'utente non può essere gestito, a meno che non gli sia stato esplicitamente assegnato tramite il VPP.

Domini gestiti

In iOS 8, puoi gestire URL e sottodomini specifici. Qualsiasi documento proveniente da tali domini verrà considerato gestito e seguirà il comportamento delle restrizioni di apertura gestita esistenti. I percorsi che seguono il dominio vengono gestiti di default. I sottodomini alternativi non vengono inclusi a meno che non venga applicato un carattere jolly. I domini inseriti in Safari con www (ad esempio, www.example.com), vengono trattati come .example.com.

Mostrati in impostazioni	Domini gestiti	Domini non gestiti
example.com	example.com/* www.example.com/*	*.example.com hr.example.com
example.com/docs	example.com/docs/* www.example.com/docs/*	example.com www.example.com hr.example.com/docs
www.example.com	www.example.com/* www.example.com/docs	example.com hr.example.com
*.example.com	*.example.com/*	example.com
*.example.com/docs	*.example.com/docs/*	example.com www.example.com

Gestore profilo

Oltre al supporto per soluzioni MDM di terze parti, Apple offre una soluzione MDM chiamata "Gestore profilo", un servizio di OS X Server. "Gestore profilo" facilita la configurazione dei dispositivi Apple secondo le specifiche della tua organizzazione.

"Gestore profilo" fornisce tre componenti:

- *Configurazione via etere dei dispositivi Apple:* ottimizzare la configurazione dei dispositivi Apple di proprietà dell'organizzazione. Registra i dispositivi nella MDM durante l'attivazione e salta alcuni passi di base durante la configurazione per rendere gli utenti operativi in pochi istanti.
- *Servizio MDM:* "Gestore profilo" offre un servizio MDM che ti consente di gestire da remoto i dispositivi Apple registrati. Una volta che un dispositivo è stato registrato, è possibile aggiornarne la configurazione dalla rete senza che l'utente interagisca o esegua altre operazioni.
- *Distribuzione di app e libri:* "Gestore profilo" può distribuire le app e i libri acquistati tramite il VPP. L'assegnazione di app e libri è supportata sui dispositivi iOS con iOS 7 o versione successiva e sui computer Mac con OS X Mavericks o versione successiva.

Per ulteriori informazioni, consulta Gestione dei dispositivi. Consulta anche Aiuto di "Gestore profilo".

Supervisionare i dispositivi

Per abilitare opzioni e restrizioni di configurazione aggiuntive, devi supervisionare i dispositivi iOS di proprietà dell'organizzazione. Ad esempio, la supervisione ti consente di impedire la modifica delle impostazioni degli account o di filtrare le connessioni web tramite Global Proxy per assicurarti che il traffico web degli utenti rimanga all'interno della rete dell'organizzazione.

Di default, nessun dispositivo iOS è supervisionato. Puoi combinare la supervisione e la gestione remota tramite MDM per avere il controllo su impostazioni e restrizioni aggiuntive. Per abilitare la supervisione dei dispositivi della tua organizzazione, utilizza il programma di registrazione dispositivi DEP o Apple Configurator.

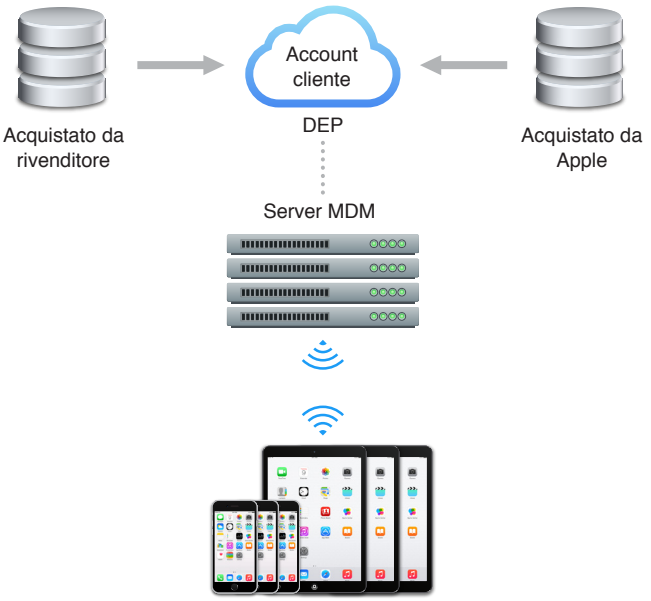
La supervisione fornisce un controllo ancora maggiore sui dispositivi di proprietà dell'organizzazione, consentendo di applicare restrizioni come la disattivazione di iMessage e Game Center. Offre anche configurazioni e funzioni aggiuntive, come i filtri per i contenuti web e la possibilità di installare app senza notifiche. Con il Device Enrollment Program è possibile attivare la supervisione in modalità wireless durante la configurazione oppure manualmente usando Apple Configurator.

Per ulteriori informazioni, consulta Impostazioni supervisionate.

DEP (Device Enrollment Program)

Il DEP (Device Enrollment Program) offre un modo semplice e veloce per distribuire i dispositivi Apple acquistati dalla tua organizzazione direttamente da Apple o da rivenditori o gestori autorizzati da Apple che partecipano al programma. Puoi registrare direttamente i dispositivi Apple sul server MDM prima di consegnarli agli utenti, senza doverli toccare o preparare materialmente. E puoi semplificare ulteriormente il processo per gli utenti eliminando passaggi specifici in "Impostazione assistita", così saranno operativi in pochi istanti. Puoi anche scegliere se consentire o meno all'utente di rimuovere il profilo MDM dal dispositivo. Ad esempio, è possibile ordinare dispositivi Apple da Apple o dai rivenditori o gestori autorizzati da Apple che partecipano al programma, configurare tutte le impostazioni di gestione e farli spedire direttamente a casa degli utenti. Una volta che il dispositivo viene tolto dalla confezione e attivato, viene registrato nella soluzione MDM e tutte le impostazioni di gestione, le app e i libri sono pronti all'uso.

Il procedimento è semplice: Una volta effettuata la registrazione al programma, gli amministratori accedono al sito web DEP, collegano il programma al server o ai server MDM e "reclamano" i dispositivi Apple acquistati da Apple o dai rivenditori o gestori autorizzati da Apple che partecipano al programma. Quindi i dispositivi potranno essere assegnati a un server MDM. Una volta avvenuta la registrazione, tutte le configurazioni, le restrizioni o i controlli specificati dalla MDM vengono installati automaticamente.



Affinché i dispositivi Apple siano idonei all'assegnazione tramite il DEP, devono soddisfare i seguenti criteri:

- I dispositivi devono essere ordinati dal primo marzo 2011 in poi e acquistati presso Apple utilizzando i numeri cliente Apple registrati e verificati.
- I dispositivi devono essere acquistati presso un rivenditore Apple autorizzato che partecipa al programma DEP o un gestore e devono essere associati all'ID di tale rivenditore. La data effettiva di idoneità viene stabilita dal rivenditore Apple autorizzato che partecipa al programma DEP o in base allo storico delle vendite del gestore, ma questa non può essere precedente al primo marzo 2011.

Nota: Il DEP non è disponibile in tutti i paesi o le regioni.

L'elenco dei dispositivi Apple idonei all'assegnazione in base al numero di ordine ai server MDM è disponibile sul sito web dei Programmi di distribuzione Apple. All'interno degli ordini, puoi anche cercare i dispositivi per tipo e numero di serie. Una volta che gli ordini sono stati spediti, li puoi cercare sul sito web del programma e assegnarli automaticamente a un server MDM specifico. Ad esempio, se hai ordinato 5000 iPad, puoi usare il numero d'ordine per assegnare tutti i dispositivi, o solo alcuni di essi, a un server MDM autorizzato già esistente. I dispositivi si possono assegnare a un server MDM specifico anche usando il numero di serie, un'opzione utile quando le unità sono già in tuo possesso.

Gli ordini successivi possono essere assegnati automaticamente a un server MDM autorizzato, evitando così la necessità di gestire manualmente l'assegnazione dei dispositivi Apple.

Una volta assegnato un dispositivo a un server MDM nell'ambito del programma, è possibile applicare altri profili e funzioni usando il server MDM della tua organizzazione. La funzioni includono:

- Abilitare la supervisione
- Configurazione obbligatoria
- Richiesta di autorizzazione al sistema di directory per il completamento della configurazione
- Profilo di registrazione MDM bloccabile
- Saltare passaggi in "Impostazione assistita"

Per ulteriori informazioni, consulta:

- Programmi di Distribuzione Apple
- Aiuto del Device Enrollment Program
- Device Enrollment Program per l'Istruzione

Apple Configurator

Per i dispositivi iOS che gestisci in e che non sono configurati da utenti individuali, puoi utilizzare Apple Configurator, un'app per Mac gratuita disponibile su Mac App Store. Essa ti consente di configurare più dispositivi alla volta via USB, prima di consegnarli agli utenti. Con questo strumento, la tua organizzazione può rapidamente configurare e aggiornare più dispositivi all'ultima versione di iOS, configurare le impostazioni e le restrizioni e installare app e contenuti. Puoi anche ripristinare i dispositivi da backup, in modo da recuperare impostazioni, layout della schermata Home, e installare dati delle app.

Apple Configurator è ideale nelle situazioni in cui gli utenti condividono dispositivi iOS che necessitano di essere rapidamente aggiornati con le impostazioni, i criteri, le app e i dati corretti. Inoltre puoi utilizzare Apple Configurator per supervisionare i dispositivi prima di utilizzare la MDM per gestire le impostazioni, i criteri e le app.

Per ulteriori informazioni, consulta Aiuto Apple Configurator.

Distribuzione di app e libri 8

Panoramica

iOS include una serie di app avanzate integrate che consentono agli utenti all'interno della tua organizzazione di svolgere in modo semplice e rapido le attività di ogni giorno, dalla gestione dei messaggi e-mail e del calendario al controllo di contatti e contenuti web. Le funzioni aggiuntive di cui i dipendenti hanno bisogno per il lavoro vengono fornite dalle centinaia di migliaia di terze parti disponibili su App Store, oppure da app aziendali personalizzate sviluppate da sviluppatori in-house o di terze parti. In ambito didattico, puoi stimolare la produttività e la creatività degli utenti tramite app iOS e contenuti pertinenti.

I modi per distribuire app e libri a dispositivi Apple nella tua organizzazione sono molteplici. Il metodo più flessibile e modulare è rappresentato dall'acquisto di app e libri tramite il Volume Purchase Program (comprese le app B2B) e dalla loro assegnazione agli utenti tramite la MDM. La tua organizzazione può anche creare e distribuire app sviluppate internamente, se è iscritta all'iOS Developer Enterprise Program. Se hai adottato un modello di distribuzione basato su dispositivi condivisi, puoi installare app e contenuti localmente con Apple Configurator.

Durante la distribuzione di app e libri, tieni in considerazione quanto segue:

- VPP (Volume Purchase Program)
- App B2B personalizzate
- App e libri sviluppati in-house
- Distribuzione di app e libri
- Caching Server

VPP (Volume Purchase Program)

Panoramica

Su App Store e su iBooks Store ci sono migliaia di app e di libri che gli utenti possono acquistare, scaricare e installare. Il VPP (Volume Purchase Program) offre alle organizzazioni un metodo semplice per acquistare a volume app e libri e distribuirli a dipendenti, collaboratori, insegnanti e studenti. Puoi scegliere nell'intero catalogo di app e libri disponibili su App Store e su iBooks Store, sia gratis sia a pagamento. Sono disponibili due siti web per il Volume Purchase Program, uno per le aziende e uno per gli istituti didattici.

In ambito aziendale, il VPP per le aziende ti consente di ottenere app B2B personalizzate, realizzate ad hoc per te da sviluppatori di terze parti e scaricabili privatamente attraverso lo store dedicato.

In ambito didattico, il VPP consente agli sviluppatori di app di offrire prezzi speciali per l'acquisto di 20 o più app a istituti didattici idonei, inclusi istituti comprensivi, distretti scolastici o qualsiasi istituto superiore o universitario accreditato. I prezzi speciali non sono disponibili per i libri.

Il VPP può essere integrato con soluzioni MDM, così da consentire alla tua organizzazione di acquistare a volume app e libri a assegnarli a specifici utenti o gruppi. Quando un utente non ha più bisogno di un'app, tramite la MDM è possibile revocarla e assegnarla a un altro utente. E ogni app o libro è disponibile automaticamente per il download sui dispositivi Apple degli utenti. Una volta distribuiti, i libri rimangono di proprietà del mittente e non è possibile revocarli o riassegnarli.

Per ulteriori informazioni, consulta:

- Volume Purchase Program per il settore aziendale
- Volume Purchase Program per il settore didattico
- Aiuto Programmi di Distribuzione Apple

Nota: Il VPP non è disponibile in tutti i paesi o le regioni.

Registrarsi al Volume Purchase Program

Per acquistare app a volume, devi registrarti e creare un account con Apple. Dovrai fornire alcune informazioni sulla tua organizzazione, come il numero D-U-N-S di D&B (se sei un'impresa) e le informazioni di contatto. Inoltre, devi creare un ID Apple che verrà utilizzato solo per amministrare il programma.

Acquista app e libri a volume

L'acquisto di app e libri per la tua azienda o per il tuo istituto didattico avviene tramite il sito web del Volume Purchase Program.

Utilizza l'ID Apple associato al tuo account Volume Purchase Program per accedere al sito. Cerca le app o i libri che desideri acquistare, quindi indica il numero di copie che stai acquistando. Puoi pagare con una carta di credito aziendale o con il credito VPP acquisito tramite un ordine di acquisto (PO). Non c'è limite al numero di copie di app o libri che puoi acquistare. Le app e i libri potranno quindi essere assegnati tramite la tua soluzione MDM, purché sia collegata al tuo account VPP e abbia un token valido.

Distribuzione gestita

Quando acquisti app e libri a volume, puoi distribuirli via MDM tramite la distribuzione gestita per assegnarli a utenti con iOS 7 o versione successiva o OS X Mavericks o versione successiva. E quando una persona non ha più bisogno dell'app o lascia l'azienda, puoi riassegnare l'app a un altro utente. I libri assegnati, invece, non possono essere revocati.

Prima di utilizzare la tua soluzione MDM per assegnare le app agli utenti, devi collegare il server MDM al tuo account VPP usando un token sicuro che puoi scaricare sul server accedendo al riepilogo del tuo account sullo store del VPP. Per ulteriori informazioni, consulta Aiuto Programmi di distribuzione Apple.

Per consentire agli utenti di partecipare alla distribuzione gestita via VPP, devi prima invitarli. Quando l'utente accetta l'invito, il suo ID Apple personale viene collegato alla tua organizzazione. Così facendo, l'utente non dovrà comunicarti il suo ID Apple e tu non dovrai crearne uno per suo conto. Per account in ambito didattico, puoi creare ID Apple per studenti sotto i 13 anni. Per ulteriori informazioni, consulta il sito web di ID Apple per studenti.

È importante registrare e assegnare app e libri agli utenti del VPP prima di inviare l'invito all'utente. In questo modo l'assegnazione avrà più tempo per propagarsi nella cronologia degli acquisti dell'utente quando viene accettato l'invito VPP. La registrazione degli utenti o l'assegnazione delle app può avvenire in qualsiasi momento, anche prima che i dispositivi Apple siano registrati alla MDM.

Le app assegnate via MDM appariranno nella cronologia degli acquisti dell'utente su App Store. È quindi possibile invitare l'utente ad accettare l'installazione dell'app oppure, nel caso dei dispositivi iOS supervisionati, installarla senza notifiche.

Se le app non ancora installate su un dispositivo vengono inviate tramite il comando di invio tramite push delle app VPP, tali app verranno automaticamente rimosse quando un utente disabilita la registrazione alla MDM.

Le app e i libri distribuiti via distribuzione gestita non vengono condivisi con i membri familiari tramite la funzionalità "In famiglia".

App B2B personalizzate

Attraverso il Volume Purchase Program è anche possibile acquistare app create o personalizzate da uno sviluppatore esterno per la tua azienda (app B2B).

Gli sviluppatori iscritti all'iOS Developer Program possono inviare app per la distribuzione B2B tramite iTunes Connect, lo stesso processo utilizzato per pubblicare altre app su App Store. Lo sviluppatore fissa il prezzo per copia e aggiunge l'ID Apple che usi per il Volume Purchase Program al proprio elenco di acquirenti B2B autorizzati. Solo gli acquirenti autorizzati possono vedere o acquistare l'app.

Le app B2B non sono garantite da Apple; lo sviluppatore è responsabile per la sicurezza dei dati di un'app. Apple raccomanda di utilizzare le best practice iOS per la codifica e l'autenticazione in-app.

Dopo la revisione dell'app da parte di Apple, utilizza il sito web del Volume Purchase Program per acquistare le copie, come descritto in Acquista app e libri a volume. Le app B2B personalizzate non vengono elencate su App Store, ma vanno acquistate tramite il sito web del Volume Purchase Program.

App in-house

Sviluppa app iOS per i dipendenti della tua organizzazione tramite iOS Developer Enterprise Program. Il programma offre un procedimento completo e integrato per lo sviluppo, il testing e la distribuzione di app iOS ai dipendenti della tua organizzazione. Puoi distribuire app in-house sia ospitandole su un semplice web server sicuro creato internamente sia utilizzando una soluzione MDM o di gestione di app di terze parti.

I vantaggi della gestione delle app tramite una MDM includono la possibilità di configurare le app da remoto, gestire le versioni, configurare il Single Sign-On, impostare criteri di accesso alla rete e controllare quali app possono esportare documenti. La soluzione più adatta alle tue esigenze verrà dettata dai tuoi requisiti specifici, dall'infrastruttura e dal livello di gestione delle app.

Per distribuire app in-house per dispositivi iOS:

1. Esegui la registrazione al programma iOS Developer Enterprise Program.
2. Prepara l'app per la distribuzione.

3 Crea un profilo di fornitura per la distribuzione aziendale che autorizzi i dispositivi a utilizzare le app che hai firmato.

4 Crea il build dell'app con il profilo di fornitura.

5 Distribuisci l'app agli utenti.

Registrarsi per lo sviluppo di app
Una volta iscritto all'iOS Developer Enterprise Program, puoi richiedere un certificato e un profilo di fornitura da sviluppatore che userai per il build e il testing dell'app. Il profilo di fornitura da sviluppatore consente di eseguire le app firmate con il tuo certificato sui dispositivi iOS registrati. Il profilo ad hoc scade dopo tre mesi e specifica quali dispositivi (in base al loro ID) possono eseguire i build di sviluppo dell'app. Il tuo build firmato e il profilo di fornitura vanno distribuiti al team di sviluppo e ai tester delle app.

Per ulteriori informazioni, consulta il sito web di iOS Developer Enterprise Program.

Preparare le app per la distribuzione
Al termine delle fasi di sviluppo e testing, quando sei pronto a distribuire l'app, firmala utilizzando il tuo certificato di distribuzione e prepara il bundle con un profilo di fornitura. Il Team Agent o l'amministratore designati per la tua partecipazione al programma creano il certificato e il profilo sul sito web di iOS Dev Center.

In iOS 8, i profili di fornitura non sono più visualizzabili dall'utente sul proprio dispositivo.

Fornire app in-house
Il profilo di fornitura per la distribuzione aziendale consente di installare un'app su un numero illimitato di dispositivi iOS. Puoi creare un profilo per un'app specifica o per più app.

Dopo aver installato sul tuo Mac sia il certificato di distribuzione aziendale sia il profilo di fornitura, userai Xcode per firmare e creare il build di una versione production dell'app. Il certificato di distribuzione aziendale è valido per tre anni e potrai avere fino a due certificati validi alla volta. Quando un certificato è in scadenza, dovrai ripetere la firma e il build dell'app utilizzando un certificato rinnovato. Il profilo di fornitura è valido per un anno, quindi dovrai emettere nuovi profili a cadenza annuale. Per ulteriori informazioni, consulta Fornire app aggiornate.

È importante limitare l'accesso al tuo certificato di distribuzione e alla chiave privata. Utilizza Accesso Portachiavi su OS X per esportarli ed eseguirne il backup in formato .p12. Se la chiave privata viene persa non è possibile ripristinarla o scaricarla una seconda volta. È inoltre opportuno limitare l'accesso al personale responsabile dell'accettazione finale dell'app. Firmando un'app con il certificato di distribuzione, la tua organizzazione ne approva il contenuto e il funzionamento e conferma il rispetto dei termini di licenza dell'Enterprise Developer Agreement.

Per ulteriori informazioni sulla distribuzione di app in-house, consulta il manuale di distribuzione di app di Apple.

Libri in-house

iOS 8 e OS X Yosemite sono caratterizzati da notevoli migliorie grazie all'introduzione della distribuzione gestita dei libri. Questa funzionalità ti consente di assegnare libri agli utenti tramite la MDM e di mantenere tali libri sotto il controllo della tua organizzazione. I PDF e gli ePub creati da te possono essere assegnati agli utenti, revocati e riassegnati quando non saranno più necessari, proprio come per le app in-house.

Distribuzione di app e libri

Panoramica

Per distribuire app e libri, puoi utilizzare i metodi descritti di seguito:

- Utilizza un server MDM per dire ai dispositivi Apple gestiti di installare un'app in-house o di App Store, se il server MDM lo supporta.
- Pubblica l'app su un server web sicuro, in maniera tale che gli utenti possano accedervi e installarla in modalità wireless. Per informazioni, consulta Installare app in-house in modalità wireless.
- Puoi installare l'app sui dispositivi iOS usando Apple Configurator localmente.

Installare app e libri tramite MDM

Un server MDM può gestire le app di terze parti disponibili su App Store, oltre a quelle in-house. Le app installate via MDM sono dette *app gestite*. Il server MDM può specificare se le app gestite e i relativi dati devono restare dove sono quando l'utente disabilita la gestione MDM. Il server può impedire che i dati dell'app gestita vengano inclusi nei backup di iTunes e iCloud. Ciò ti consente di gestire le app che potrebbero contenere informazioni aziendali riservate con un controllo maggiore rispetto a quelle scaricate direttamente dall'utente.

Per installare un'app gestita, il server MDM invia al dispositivo Apple un comando di installazione. Se è stata acquistata da App Store, l'app verrà scaricata e installata da Apple. Se invece si tratta di un'app sviluppata in-house, essa verrà installata dalla tua soluzione MDM. Sui dispositivi non supervisionati, le app gestite richiedono l'accettazione da parte dell'utente prima di essere installate.

In iOS 7 o versione successiva e OS X Mavericks o versione successiva, le connessioni VPN possono essere specificate a livello di app, quindi solo il traffico di rete per quella specifica app si troverà nel tunnel VPN protetto. In questo modo si è sicuri che i dati privati rimangano tali e non si mescolino con quelli pubblici.

Le app gestite supportano la funzione di apertura gestita in iOS 7 o versione successiva. Ciò significa che è possibile impedire che trasferiscano dati da o verso le app personali dell'utente; così, l'organizzazione ha la certezza che i dati sensibili rimangano dove devono essere.

Un server MDM può installare libri da iBooks Store che sono stati assegnati all'utente tramite il VPP. Può anche installare PDF, ePub e libri di iBooks Author gestiti, direttamente dai tuoi server, e aggiornarli con nuove versioni quando necessario. Il server può impedire il backup dei libri gestiti. I libri gestiti verranno rimossi una volta che l'utente avrà annullato la registrazione alla MDM.

Installare app con Apple Configurator

Apple Configurator semplifica le operazioni di configurazione di base, ma può essere anche utilizzato per installare app e altri contenuti sui dispositivi iOS. Apple Configurator è particolarmente utile quando viene utilizzato per supervisionare dispositivi che non verranno personalizzati dall'utente, come ad esempio iPad condivisi in un'aula.

Oltre alle app, puoi utilizzare Apple Configurator per installare documenti e renderli disponibili quando gli utenti iniziano a utilizzare i dispositivi. I documenti sono disponibili per le app che supportano la condivisione file di iTunes. Inoltre, puoi anche visualizzare e ricevere documenti dai dispositivi iOS collegandoli a un Mac che ha in esecuzione Apple Configurator.

Caching Server

Con iOS e OS X, accedere e utilizzare contenuti digitali è facilissimo, e alcuni utenti potrebbero richiedere molti gigabyte di dati sotto forma di app, libri e aggiornamenti software quando sono connessi alla rete dell'azienda. La richiesta di tali risorse ha dei picchi: il primo avviene in concomitanza con la distribuzione dei dispositivi Apple, seguito da altri occasionali quando gli utenti scoprono nuovi contenuti o li aggiornano nel tempo. Questi download possono causare bruschi aumenti della richiesta di ampiezza di banda per la connessione a Internet.

Caching Server è un servizio di OS X Server che salva sulla rete locale della tua organizzazione i contenuti che sono già stati richiesti, riducendo l'ampiezza di banda necessaria a scaricarli. Ciò si ottiene riducendo la banda per le connessioni a Internet in uscita sulle reti private (RFC 1918) e archiviando nella cache della LAN copie dei contenuti richiesti.

Caching Server su OS X Server Yosemite archivia nella cache i seguenti tipi di contenuti per i dispositivi con iOS 7 o versione successiva e OS X Mountain Lion v10.8.2 o versione successiva:

- Aggiornamenti software per iOS (iOS 8.1 o versione successiva)
- Aggiornamenti software per OS X
- Immagine di ripristino Internet (OS X Mavericks o versione successiva)
- Aggiornamenti di Java e dei driver di stampa
- App di App Store
- Aggiornamenti di App Store
- Libri acquistati sull'iBooks Store
- Corsi e contenuti di iTunes U
- Contenuti scaricabili di GarageBand
- Voci in alta qualità e dizionari

Per ulteriori informazioni sui contenuti archiviati nella cache dal servizio di cache, consulta l'articolo del supporto Apple OS X Server: Tipi di contenuto supportati dal servizio di cache.

Anche iTunes supporta Caching Server. Di seguito trovi un elenco dei tipi di contenuti supportati da iTunes 11.0.4 o successivo (su computer Mac e Windows):

- App di App Store
- Aggiornamenti di App Store
- Libri acquistati sull'iBooks Store

L'utilizzo di diversi server cache rappresenta un enorme vantaggio per le reti di grandi dimensioni. Per molte distribuzioni, configurare un server cache è molto semplice: basta attivare il servizio. Con Caching Server su OS X Server Yosemite non è più necessario un ambiente NAT per il server e tutti i dispositivi che lo utilizzano. Caching Server ora può essere utilizzato in reti composte da indirizzi IP instradabili a livello pubblico. I dispositivi Apple con iOS 7 o versione successiva e OS X Mountain Lion 10.8.2 o versione successiva contattano il Caching Server più vicino senza la necessità di configurazioni aggiuntive.

Per ulteriori informazioni, cerca Servizio di caching in Supporto OS X Server.

Quella che segue è una spiegazione del flusso di lavoro di un server cache.

1. Quando un dispositivo Apple collegato a una rete con più server cache richiede contenuti dall'iTunes Store o dal server Aggiornamento Software, il dispositivo Apple viene indirizzato a un server cache.
2. Per prima cosa, il server cache verifica se il contenuto richiesto è già presente nella sua cache locale.
   - Se è così, il contenuto verrà immediatamente trasferito al dispositivo.
   - Se il server cache non trova i contenuti richiesti, tenta di scaricarli da un'altra fonte. Caching Server 2 o versione successiva include una funzione di replica peer in grado di utilizzare altri server cache sulla rete, se hanno già scaricato il contenuto richiesto.
3. Non appena il server cache riceve i dati in download, li trasmette immediatamente ai dispositivi che ne hanno fatto richiesta e ne salva una copia sul dispositivo di archiviazione designato.

Pianificare l'assistenza 9

Panoramica

La distribuzione di dispositivi Apple dovrebbe includere un servizio di assistenza. AppleCare offre piani di supporto per le organizzazioni di qualsiasi dimensione, inclusi il supporto alla distribuzione del software e la copertura hardware:

- Computer Mac con OS X, dispositivi iOS con iOS
  - AppleCare Help Desk Support
  - AppleCare OS Support
  - AppleCare for Enterprise
- Solo dispositivi iOS
  - AppleCare per utenti di dispositivi iOS
  - iOS Direct Service Program
- Solo computer Mac
  - AppleCare Protection Plan per Mac o schermi Apple

Puoi scegliere il piano che più si adatta alle esigenze della tua organizzazione. Per ulteriori informazioni, consulta il sito web di AppleCare Professional Support.

AppleCare Help Desk Support

AppleCare Help Desk Support offre accesso telefonico prioritario allo staff di assistenza tecnica più esperto di Apple. Esso include una serie di strumenti di diagnosi e di risoluzione dei problemi per l'hardware Apple che può aiutare le aziende a gestire le risorse in maniera più efficiente, migliorare i tempi di risposta e ridurre i costi per la formazione. AppleCare Help Desk Support copre un numero illimitato di interventi di assistenza per la diagnosi e la risoluzione di problemi hardware o software e l'isolamento di problemi per i dispositivi iOS e OS X. Per ulteriori informazioni, consulta il sito web di AppleCare Help Desk Support.

AppleCare OS Support

AppleCare OS Support include AppleCare Help Desk Support, con l'aggiunta del supporto per gli interventi di assistenza. AppleCare OS Support include l'assistenza per componenti di sistema, configurazione e amministrazione della rete, integrazione in ambienti eterogenei, applicazioni software professionali, applicazioni e servizi web e problemi tecnici la cui risoluzione richiede l'utilizzo di strumenti a riga di comando. Per ulteriori informazioni, consulta il sito web di AppleCare OS Support.

AppleCare for Enterprise

AppleCare for Enterprise offre un supporto globale a livello di hardware e software per aziende e istituti didattici. Il tuo AppleCare Account Manager ti offrirà un supporto avanzato durante le fasi di analisi dell'infrastruttura IT e l'individuazione e la gestione delle problematiche riscontrate, fornendo resoconti mensili sulle attività legate alle chiamate di supporto e alle richieste di interventi di riparazione. Potrai avvalerti di un servizio di supporto altamente professionale sia telefonicamente che tramite e-mail per tutto l'hardware e il software Apple. Avrai a disposizione un supporto per scenari di distribuzione e integrazione complessi, tra cui MDM e Active Directory.

Se hai bisogno di aiuto con IBM MobileFirst per le app iOS, questo tipo di offerta ti consente di analizzare le varie problematiche della soluzione in uso assieme a un AppleCare Account Manager e congiuntamente collaborare con IBM per la risoluzione degli eventuali problemi riscontrati. AppleCare for Enterprise ti consente di ridurre il carico di lavoro dell'help desk interno grazie a un servizio telefonico di supporto tecnico rivolto ai dipendenti disponibile 24 ore al giorno, 7 giorni su 7. Apple fornisce inoltre supporto tecnico per hardware e sistemi operativi Apple, per app Apple quali, ad esempio Keynote, Pages e Numbers, nonché per account e impostazioni personali. Per ulteriori informazioni, consulta il sito web di AppleCare for Enterprise.

AppleCare per utenti di dispositivi iOS

Ogni dispositivo iOS include una garanzia limitata di un anno e assistenza tecnica complementare per 90 giorni a partire dalla data di acquisto. Tale copertura può essere estesa a due anni dalla data di acquisto originale con AppleCare+ per iPhone, AppleCare+ per iPad o AppleCare+ per iPod touch. Gli utenti potranno telefonare agli esperti tecnici di Apple quante volte vorranno e porre domande sull'utilizzo di base. Apple offre anche comode opzioni di assistenza ogni volta che un dispositivo ha bisogno di essere riparato. Tutti e tre i programmi coprono fino a due interventi per danno accidentale, entrambi soggetti a una tariffa di servizio.

iOS Direct Service Program

In aggiunta a AppleCare+ e AppleCare Protection Plan, iOS Direct Service Program consente alla tua assistenza tecnica di monitorare i dispositivi per individuare eventuali problemi senza chiamare AppleCare o visitare Apple Store. Se necessario, la tua organizzazione può ordine direttamente un iPhone, iPad o iPod touch sostitutivi o anche gli accessori inclusi nella confezione. Per ulteriori informazioni, consulta il sito di iOS Direct Service Program.

AppleCare Protection Plan per Mac o schermi Apple

Ogni Mac include una garanzia limitata di un anno e assistenza tecnica complementare per 90 giorni a partire dalla data di acquisto. Tale copertura può essere estesa fino a tre anni dalla data di acquisto originale e può includere interventi di riparazione in loco per i computer desktop. Sono inoltre inclusi servizi di riparazione (con spedizione postale del dispositivo al centro di assistenza) per computer portatili o schermi Apple e servizi di riparazione (con trasporto del dispositivo al centro di assistenza a carico dell'utente) per computer Mac o schermi Apple presso i punti vendita Apple o altri centri di assistenza autorizzati Apple. Puoi telefonare agli esperti tecnici di Apple ogni volta che vorrai per ottenere supporto per hardware Apple, OS X e app Apple, come ad esempio quelle incluse nelle suite iLife e iWork.

Appendici 10

Restrizioni

Panoramica

I dispositivi Apple supportano i criteri e le restrizioni elencati di seguito, che puoi configurare in base alle esigenze della tua organizzazione. A seconda della soluzione MDM adottata, i nomi delle restrizioni possono variare leggermente.

Nota: Non tutte le restrizioni sono disponibili per tutti i dispositivi Apple.

Impostazioni del Device Enrollment Program (DEP)

Le restrizioni elencate di seguito sono valide per i dispositivi Apple assegnati ai server MDM attraverso il DEP.

Opzioni di registrazione

- *Richiedi all'utente di registrare il dispositivo:* quando questa opzione è attivata, il dispositivo richiede all'utente di registrare il dispositivo per la gestione MDM. Di default l'opzione è disattivata.

  Le seguenti impostazioni sono un sottoinsieme dell'opzione precedente.

  - *Non consentire all'utente di ignorare la registrazione:* quando questa opzione è attivata, l'utente deve registrare il dispositivo per la gestione MDM prima di poter configurare il dispositivo. Di default l'opzione è disattivata.
  - *Richiedi le credenziali per la registrazione:* quando questa opzione è disattivata, l'utente non deve eseguire l'autenticazione in un servizio di directory prima di registrare il dispositivo per la gestione MDM. Di default l'opzione è attivata.
  - *Supervisiona il dispositivo (solo iOS):* quando questa opzione è attivata, il dispositivo è sottoposto a supervisione durante la registrazione. L'utente non potrà annullare la registrazione del dispositivo. Di default l'opzione è disattivata.

  Le seguenti impostazioni sono un sottoinsieme dell'opzione precedente.

  - *Consenti abbinamento (solo iOS):* quando questa opzione è disattivata, gli utenti non possono abbinare il proprio dispositivo a un computer. Di default l'opzione è attivata.
  - *Impedisci l'annullamento della registrazione:* quando questa opzione è attivata, l'utente non potrà annullare la registrazione di un dispositivo iOS supervisionato. È possibile annullare la registrazione dei computer Mac solo se l'utente dispone del nome utente e della password dell'amministratore. Di default l'opzione è disattivata.

Opzioni di "Impostazione assistita"

Nei dispositivi Apple registrati nel DEP e gestiti tramite MDM, queste schermate di "Impostazione assistita" possono essere saltate (di default, tutte le opzioni sono attivate):

A meno che questi elementi non vengano limitati in modo definitivo utilizzando la soluzione MDM, gli utenti potranno eseguire le suddette operazioni dopo la configurazione del dispositivo Apple.

- *Configura come nuovo dispositivo o ripristina da backup:* quando questa opzione è disattivata, l'utente non può selezionare tra le due scelte.
- *Consenti all'utente di immettere il proprio ID Apple:* quando questa opzione è disattivata, l'utente non può immettere il proprio ID Apple.
- *Consenti all'utente di visualizzare i termini e le condizioni:* quando questa opzione è disattivata, l'utente non può consultare i termini e le condizioni Apple.
- *Consenti all'utente di scegliere se inviare i dati di diagnostica a Apple e agli sviluppatori:* quando questa opzione è disattivata, l'utente non può scegliere se inviare i dati di diagnostica a Apple e i dati delle app agli sviluppatori.
- *Consenti all'utente di attivare i servizi di localizzazione:* quando questa opzione è disattivata, l'utente non può abilitare i servizi di localizzazione.
- *Consenti all'utente di abilitare Touch ID (solo iOS):* quando questa opzione è disattivata, l'utente non può abilitare Touch ID per sbloccare il dispositivo o autenticare le app utilizzando Touch ID.
- *Consenti all'utente di modificare le impostazioni "Blocco con codice" (solo iOS):* quando questa opzione è disattivata, l'utente non può modificare il codice di accesso nelle impostazioni gestite.
- *Consenti all'utente di abilitare Apple Pay (solo iOS):* quando questa opzione è disattivata, l'utente non può abilitare Apple Pay.
- *Consenti all'utente di abilitare Siri (solo iOS):* quando questa opzione è disattivata, l'utente non può abilitare Siri.
- *Consenti all'utente di modificare "Zoom schermo" (solo iOS):* quando questa opzione è disattivata, l'utente non può modificare le impostazioni standard o con zoom di "Zoom schermo".
- *Consenti all'utente di registrare il Mac con Apple (solo OS X):* quando questa opzione è disattivata, l'utente non può compilare il modulo di registrazione e inviarlo a Apple.
- *Consenti all'utente di abilitare FileVault (solo OS X):* quando questa opzione è disattivata, l'utente non può abilitare FileVault.

Funzionalità del dispositivo

Funzionalità dei dispositivi iOS

Di seguito sono descritte le restrizioni delle funzionalità iOS.

- *Consenti installazione di app:* quando questa opzione è disattivata, App Store viene disabilitato e la relativa icona rimossa dalla schermata Home. Gli utenti non possono installare o aggiornare le app di App Store tramite App Store, iTunes o la MDM. Le app in-house possono ancora essere installate e aggiornate.
- *Consenti Siri:* quando questa opzione è disattivata, non è possibile utilizzare Siri.
- *Consenti Siri con dispositivo bloccato:* quando questa opzione è disattivata, Siri risponde solo quando il dispositivo è sbloccato.
- *Apple Pay:* quando questa opzione è disattivata, Apple Pay è disattivato.
- *Consenti Handoff:* quando questa opzione è disattivata, gli utenti non possono utilizzare Handoff con i dispositivi Apple.
- *Consenti l'uso della fotocamera:* quando questa opzione è disattivata, le fotocamere vengono disabilitate e la relativa icona rimossa dalla schermata Home. Gli utente non possono scattare fotografie, registrare video o utilizzare FaceTime.
- *Consenti FaceTime:* quando questa opzione è disattivata, gli utenti non possono effettuare o ricevere chiamate audio o video FaceTime.
- *Consenti istantanee:* quando questa opzione è disattivata, gli utenti non possono salvare un'istantanea dello schermo.

- *Consenti sincronizzazione automatica in roaming:* quando questa opzione è disattivata, i dispositivi in roaming vengono sincronizzati solo quando l'utente accede all'account.
- *Consenti composizione vocale:* quando questa opzione è disattivata, gli utenti non possono utilizzare i comandi vocali per comporre i numeri telefonici.
- *Consenti acquisti in-app:* quando questa opzione è disattivata, gli utenti non possono effettuare acquisti dall'interno di un'app.
- *Consenti Touch ID per sbloccare il dispositivo:* quando questa opzione è disattivata, gli utenti devono utilizzare un codice per sbloccare il dispositivo.
- *Forza rilevamento polso Apple Watch:* quando questa opzione è attivata, Apple Watch viene bloccato automaticamente quando viene rimosso dal polso dell'utente. Può essere sbloccato con il relativo codice d'accesso o iPhone abbinato. Di default l'opzione è disattivata.
- *Consenti l'accesso a Centro di Controllo da "Blocco schermo":* quando questa opzione è disattivata, gli utenti non possono visualizzare Centro di Controllo facendo scorrere il dito verso l'alto.
- *Consenti l'accesso a Centro Notifiche da "Blocco schermo":* quando questa opzione è disattivata, gli utenti non possono visualizzare Centro Notifiche da "Blocco schermo" facendo scorrere il dito verso il basso.
- *Consenti la vista Oggi da "Blocco schermo":* quando questa opzione è disattivata, gli utenti non possono visualizzare la vista Oggi da "Blocco schermo" facendo scorrere il dito verso il basso.
- *Consenti notifiche Passbook in "Blocco schermo":* quando questa opzione è disattivata, gli utenti devono sbloccare il dispositivo per utilizzare Passbook.
- *Richiedi password di iTunes per tutti gli acquisti:* quando questa opzione è disattivata, per gli acquisti in-app in iTunes e per gli acquisti in iTunes non viene richiesta la password dell'account.
- *Imposta classificazioni consentite per i contenuti:* imposta la regione e le classificazioni per film, programmi TV e app.

Funzionalità Mac

Di seguito sono descritte le restrizioni delle funzionalità Mac.

- *Abilita adozione App Store:* quando questa opzione è disattivata, le app iLife e iWork fornite assieme a OS X non possono essere adottate da App Store.
- *Limita App Store solo agli aggiornamenti software:* quando questa opzione è attivata, App Store può essere utilizzato solo per aggiornare le app. Di default l'opzione è disattivata.
- *Richiedi una password di amministratore per installare o aggiornare le app:* quando questa opzione è attivata, viene richiesta una password di amministratore per aggiornare le app. Di default l'opzione è disattivata.
- *Limita le app autorizzate all'avvio:* quando questa opzione è attivata, è possibile limitare le app che è possibile utilizzare. Di default l'opzione è disattivata.
- *Limita pannelli specifici delle Preferenze di Sistema:* quando questa opzione è attivata, è possibile selezionare gli elementi delle Preferenze di Sistema a cui gli utenti possono accedere. Se un pannello non è riportato nell'elenco, assicurati che sia installato sul Mac in cui è installato "Gestore profilo". Di default l'opzione è disattivata.
- *Blocca immagine della scrivania:* quando questa opzione è attivata, è possibile impedire all'utente di modificare l'immagine della scrivania. Di default l'opzione è disattivata.

Impostazioni supervisionate

Di default, le due restrizioni della funzionalità "Blocco attivazione" sono disattivate per tutti gli utenti e i gruppi di utenti.

- *Invia il comando "Consenti blocco attivazione" dopo la registrazione MDM:* quando questa opzione è attivata, gli utenti possono configurare il proprio dispositivo iOS in modo che possa essere cancellato solo dopo aver immesso il proprio ID Apple.

  Le seguenti impostazioni sono un sottoinsieme dell'opzione precedente.

  - *Invia il comando solo dopo aver recuperato il codice di elusione di "Blocco attivazione":* quando questa opzione è attivata, il server MDM deve ricevere un codice di elusione di "Blocco attivazione" prima che l'utente possa configurare il proprio dispositivo iOS in modo che non possa essere cancellato senza l'immissione del corrispondente ID Apple.
- *Proxy di rete globale per HTTP:* quando questo payload viene aggiunto a un profilo, i dispositivi iOS devono utilizzare il proxy stabilito nel payload per tutto il traffico di rete via HTTP.
- *Consenti iMessage:* quando questa opzione è disattivata per i dispositivi solo Wi-Fi, l'app Messaggi viene nascosta. quando questa opzione è disattivata per dispositivi con Wi-Fi e cellulare, l'app Messaggi rimane disponibile, ma può essere utilizzato solo il servizio SMS/MMS.
- *Consenti Game Center:* quando questa opzione è disattivata, l'app Game Center e la sua icona vengono rimosse.
- *Consenti la rimozione di app:* quando questa opzione è disattivata, gli utenti non possono rimuovere le app installate.
- *Consenti iBooks Store:* quando questa opzione è disattivata, gli utenti non possono acquistare libri in iBooks Store.
- *Consenti Podcast:* quando questa opzione è disattivata, gli utenti non possono scaricare podcast.
- *Consenti tastiera predittiva:* quando questa opzione è disattivata, la tastiera predittiva non sarà visibile agli utenti.
- *Consenti correzione automatica:* quando questa opzione è disattivata, gli utenti non vedranno i suggerimenti per la correzione delle parole.
- *Consenti controllo ortografico:* quando questa opzione è disattivata, gli utenti non vedranno le parole con ortografia potenzialmente errata come testo sottolineato in rosso.
- *Consenti definizione:* quando questa opzione è disattiva, gli utenti non possono toccare due volte per cercare la definizione di una parola.
- *Consenti contenuto generato da utenti in Siri:* quando questa opzione è disattivata, Siri non può ottenere contenuti da fonti che consentono contenuti generati dagli utenti, come ad esempio Wikipedia.
- *Consenti installazione manuale dei file di configurazione:* quando questa opzione è disattivata, gli utenti non possono installare manualmente profili di configurazione.
- *Consenti configurazione delle restrizioni:* quando questa opzione è disattivata, gli utenti non possono impostare le proprie restrizioni sul dispositivo.
- *Consenti abbinamento a computer per sincronizzare i contenuti:* quando questa opzione è disattivata gli utenti non possono abbinare il dispositivo iOS a nessun computer che non sia il Mac nel quale è installato Apple Configurator e con il quale è stato supervisionato la prima volta.
- *Consenti AirDrop:* quando questa opzione è disattivata, gli utenti non possono utilizzare AirDrop con nessuna app.

- *Consenti modifica delle impronte digitali associate a "Touch ID":* quando questa opzione è disattivata, gli utenti non possono aggiungere o rimuovere le informazioni esistenti della funzione "Touch ID".
- *Consenti modifiche dell'account:* quando questa opzione è disattivata, gli utenti non possono creare nuovi account o modificare il nome utente, la password o altre impostazioni associate al loro account.
- *Consenti modifiche delle impostazioni dei dati cellulari:* quando questa opzione è disattivata gli utenti non possono modificare nessuna impostazione su quali app utilizzano i dati cellulari.
- *Consenti la modifica delle impostazioni di "Trova i miei amici":* quando questa opzione è disattivata gli utenti non possono modificare nessuna impostazione nell'app Trova i miei amici.
- *Consenti cancellazione di tutti i contenuti e le impostazioni:* quando questa opzione è disattivata gli utenti non possono cancellare il dispositivo e ripristinarlo ai valori di fabbrica.
- *Consenti URL specifici (payload "Filtro contenuti"):* quando questo payload viene aggiunto a un profilo, gli utenti non possono scegliere i siti web che possono visualizzare sui propri dispositivi iOS.
  - *URL consentiti:* Aggiungi URL all'elenco per consentire l'accesso a determinati siti web, anche se vengono considerati per adulti dal filtro automatico. Se lasci vuoto l'elenco, l'accesso è consentito a tutti i siti web non per adulti, tranne a quelli i cui URL sono bloccati.
  - *URL bloccati:* Aggiungi URL all'elenco per negare l'accesso a determinati siti web. Gli utenti non possono visitare tali siti web, anche se vengono considerati non per adulti dal filtro automatico.
  - *Solo siti web specifici:* L'utente del dispositivo avrà accesso solo ai siti web da te stabiliti. Inserisci l'URL del sito web nell'apposita colonna. Inserisci il nome del segnalibro nella colonna Nome. Per creare un segnalibro in una cartella, inseriscine la posizione nella colonna Segnalibro. Ad esempio, crea un segnalibro nella cartella Preferiti inserendo /Preferiti/.
- *Limita le connessioni AirPlay con whitelist e codici di connessione opzionali:* quando questa opzione è disattivata, non viene richiesto un codice quando un dispositivo viene abbinato per la prima volta per AirPlay.
- *Abilita filtro volgarità di Siri:* quando questa opzione è disattivata, il filtro volgarità di Siri non è abilitato.
- *Modalità app singola:* consente l'utilizzo di un'unica app selezionata.
- *Impostazioni di accessibilità:* consente determinate impostazioni di accessibilità in modalità app singola.

Per ulteriori informazioni sulla supervisione dei dispositivi iOS, consulta Supervisionare i dispositivi.

Impostazioni della sicurezza e della privacy

Impostazioni della sicurezza e della privacy per iOS e OS X

Le restrizioni relative a sicurezza e privacy elencate di seguito sono valide sia per iOS che per OS X:

- *Consenti invio di dati di diagnosi a Apple:* quando questa opzione è disattivata, i dati di diagnosi sul dispositivo non verranno inviati a Apple.

Impostazioni della sicurezza e della privacy per iOS

Le restrizioni relative a sicurezza e privacy elencate di seguito sono valide solo per iOS:

- *Consenti risultati Internet in Spotlight:* quando questa opzione è disattivata, Spotlight non restituirà risultati di ricerca da Internet.

- *Domini (e-mail):* I messaggi e-mail che non sono indirizzati ai domini nella lista di quelli approvati verranno contrassegnati. Ad esempio, un utente potrebbe avere sia example.com e gruppo.example.com nel proprio elenco di domini conosciuti. Se l'utente inserisse qualcuno@foo.com, l'indirizzo verrebbe contrassegnato, in modo che l'utente sappia con certezza che non si trova nell'elenco.
- *Domini (Safari):* I download da Safari verranno considerati documenti gestiti se sono originati da un dominio gestito. Ad esempio, se un utente scarica un PDF utilizzando Safari da un dominio gestito, a tale PDF verranno applicate tutte le impostazioni dei documenti gestiti.
- *Consenti documenti da sorgenti non gestite in destinazioni gestite:* quando questa opzione è disattivata, i documenti creati o scaricati da sorgenti non gestite non possono essere aperti in destinazioni gestite.
- *Consenti documenti da sorgenti gestite in destinazioni non gestite:* quando questa opzione è disattivata, i documenti creati o scaricati da sorgenti gestite non possono essere aperti in destinazioni non gestite.
- *Consenti musica, podcast e iTunes U espliciti:* quando questa opzione è disattivata, i contenuti video o musicali espliciti acquistati da iTunes Store o presenti in iTunes U vengono nascosti. I contenuti espliciti vengono contrassegnati come tali dal fornitore degli stessi, ad esempio dalle case discografiche, quando vengono venduti tramite iTunes Store o distribuiti su iTunes U.
- *Consenti contenuti erotici da iBooks Store:* quando questa opzione è disattivata, i contenuti sessuali espliciti acquistati da iBooks Store vengono nascosti. I contenuti espliciti vengono contrassegnati come tali dal fornitore degli stessi quando vengono venduti tramite iBooks Store. Per iOS 6, questa opzione richiede la supervisione.

  La gestione dell'autorizzazione per contenuti musicali, podcast e contenuti iTunes U espliciti, la classificazione dei contenuti stessi e i contenuti erotici da iBooks Store è disponibile sia in iTunes che in iBooks in OS X.
- *Consenti aggiornamenti automatici alle impostazioni di convalida certificato:* quando questa opzione è disattivata, gli aggiornamenti automatici alle impostazioni di convalida certificato non vengono effettuati.
- *Consenti certificati TLS non attendibili:* quando questa opzione è disattivata, agli utenti non viene chiesto di considerare attendibili i certificati che non possono essere verificati. Questa impostazione si applica a Safari e agli account Mail, Contatti e Calendario. Quando questa opzione è attivata, solo i certificati con certificati di root attendibili vengono accettati senza una richiesta. Per informazioni, sulle CA di root accettate da iOS, consulta l'articolo del supporto Apple Elenco dei certificati di root attendibili disponibili.
- *Richiedi codice al primo abbinamento con AirPlay:* quando questa opzione è disattivata, non viene richiesto un codice quando un dispositivo viene abbinato per la prima volta per AirPlay.
- *Forza limitazione raccolta dati pubblicitari:* quando questa opzione è disattivata, le app possono utilizzare l'ID pubblicitario (un identificatore non permanente del dispositivo) per fornire all'utente pubblicità mirate.
- *Consenti backup dei libri aziendali:* quando questa opzione è disattivata, gli utenti non possono eseguire il backup dei libri distribuiti dalla propria organizzazione su iCloud o iTunes.
- *Forza backup codificati:* quando questa opzione è disattivata, gli utenti possono scegliere se archiviare o meno sul Mac in formato codificato i backup del dispositivo eseguiti in iTunes.

  Se un profilo è codificato e questa opzione è disattivata, iTunes richiede ed effettua la codifica dei backup. I profili installati sul dispositivo da "Gestore profilo" non sono mai codificati.

Sicurezza e privacy per OS X

La restrizione relativa a sicurezza e privacy elencata di seguito è valida solo per iOS:

- *Consenti AirDrop:* quando questa opzione è disattivata, gli utenti non possono utilizzare AirDrop con altri computer Mac.

  Puoi limitare l'utilizzo di AirDrop per i dispositivi iOS, ma prima tali dispositivi devono essere supervisionati.

Utilizzo delle app

Restrizioni delle app valide per iOS e OS X

Le restrizioni relative alle app elencate di seguito sono valide sia per iOS che per OS X:

- Restrizioni dell'app Mail:
  - *Consenti spostamento dei messaggi di Mail da un account a un altro:* quando questa opzione è disattivata, gli utenti non possono spostare un messaggio e-mail da un account all'altro.
  - *Usa solo in Mail:* quando questa opzione è disattivata è possibile utilizzare altre app per inviare e-mail in-app dall'account specificato.
  - *Consenti sincronizzazione indirizzi recenti in Mail:* quando questa opzione è disattivata, gli indirizzi utilizzati recentemente non vengono sincronizzati con altri dispositivi.
- Restrizioni dell'app Safari:
  - *Consenti il completamento automatico di Safari:* quando questa opzione è disattivata, Safari non ricorda gli utenti che hanno utilizzato i moduli web.
- Restrizioni di Game Center:
  - *Consenti giochi multigiocatore:* quando questa opzione è disattivata, gli utenti non possono giocare in modalità multigiocatore in Game Center.
  - *Consenti aggiunta di amici in Game Center:* quando questa opzione è disattivata, gli utenti non possono trovare o aggiungere amici in Game Center.

Restrizioni delle app valide solo per iOS

Le restrizioni relative alle app elencate di seguito sono valide per iOS:

- Restrizioni di iTunes Store:
  - *Consenti utilizzo di iTunes Store:* quando questa opzione è disattivata, iTunes Store viene disabilitato e la relativa icona rimossa dalla schermata Home. Gli utenti non potranno effettuare anteprime, acquisti o download dei contenuti.
- Restrizioni dell'app Safari:
  - *Consenti utilizzo di Safari:* quando questa opzione è disattivata, l'app browser web Safari viene disabilitata e la relativa icona viene rimossa dalla schermata Home. Inoltre, questo impedisce agli utenti di aprire i clip web.
  - *Ricevi avvisi forzati di frode:* quando questa opzione è disattivata, Safari non cercherà di impedire all'utente di visitare siti web identificati come fraudolenti o compromessi.
  - *Abilita JavaScript:* quando questa opzione è disattivata, Safari ignora tutti i JavaScript presenti sui siti web.
  - *Blocco pop-up:* quando questa opzione è disattivata, i pop-up verranno bloccati in Safari.
  - *Modifica delle preferenze dei cookie:* Imposta i criteri relativi ai cookie in Safari. scegli se bloccare sempre tutti i cookie, accettare sempre tutti i cookie, accettare i cookie solo dai siti web attuali oppure dai siti web visitati dall'utente. Di default l'opzione è impostata su Sempre.

Restrizioni delle app valide solo per OS X

Le restrizioni relative alle app elencate di seguito sono valide per OS X:

- Restrizioni dell'app Dashboard:
  - *Consenti esecuzione di widget Dashboard specifici:* quando questa opzione è attivata, è possibile selezionare i widget Dashboard che l'utente può attivare.
- Restrizioni di Game Center:
  - *Consenti Game Center:* quando questa opzione è disattivata, l'app Game Center e la sua icona vengono rimosse.
  - *Consenti modifica dell'account di Game Center:* quando questa opzione è disattivata, gli utenti di Game Center non possono modificare il proprio nome utente e la propria password.

Impostazioni di iCloud

- *Consenti backup:* quando questa opzione è disattivata, il backup del dispositivo può essere eseguito solo in iTunes.
- *Consenti la sincronizzazione di documenti e dati:* quando questa opzione è disattivata, i documenti e i dati non vengono aggiunti a iCloud.
- *Consenti sincronizzazione portachiavi:* quando questa opzione è disattivata, non è possibile utilizzare il portachiavi iCloud.
- *Consenti "Il mio streaming foto":* quando questa opzione è disattivata, le foto in "Il mio streaming foto" vengono cancellate dal dispositivo, le foto in "Rullino foto" non vengono inviate a "Il mio streaming foto" e le foto e i video negli streaming condivisi non possono più essere visualizzati sul dispositivo. Se non ci sono altre copie di queste foto e video, potrebbero andare perduti.
- *Consenti "Condivisione foto di iCloud":* quando questa opzione è disattivata, gli utenti non possono iscriversi a streaming foto condivisi o pubblicarvi foto.
- *Consenti alle app gestite di archiviare dati in iCloud:* quando questa opzione è disattivata, gli utenti non possono archiviare dati da app gestite in iCloud.
- *Consenti sincronizzazione di note ed evidenziazioni dei libri aziendali:* quando questa opzione è disattivata, gli utenti non possono sincronizzare le note o le evidenziazioni sugli altri dispositivi tramite iCloud.

Restrizioni degli utenti e dei gruppi di utenti di "Gestore profilo"

Di default queste impostazioni sono attivate per tutti gli utenti e per il gruppo di utenti *Tutti*. Di default, sono disattivate per il gruppo "*Gruppo di lavoro*" e per qualsiasi gruppo di utenti creato dall'amministratore.

Altre soluzioni MDM possono avere impostazioni simili. Tuttavia, la descrizione dell'impostazione specifica potrebbe essere diversa.

- *Consenti l'accesso al portale "I miei dispositivi":* quando questa opzione è attivata, l'utente può accedere al portale "I miei dispositivi" di "Gestore profilo".

  Le seguenti impostazioni sono un sottoinsieme di questa impostazione.
  - *Consenti download del profilo di configurazione:* quando questa opzione è attivata, gli utenti possono scaricare i profili di configurazione dal portale "I miei dispositivi".
  - *Consenti la registrazione e l'annullamento della registrazione del dispositivo:* quando questa opzione è attivata, gli utenti possono registrare altri dispositivi oppure annullare la registrazione di dispositivi specifici.

- *Consenti la cancellazione del dispositivo:* quando questa opzione è attivata, gli utenti possono cancellare i propri dispositivi.
- *Consenti il blocco del dispositivo (solo iOS):* quando questa opzione è attivata, gli utenti possono bloccare il proprio dispositivo iOS.
- *Consenti la cancellazione del codice d'accesso del dispositivo (solo iOS):* quando questa opzione è attivata, gli utenti possono cancellare il codice d'accesso del proprio dispositivo iOS.

- *Consenti la registrazione durante "Impostazione assistita" per i dispositivi configurati mediante DEP:* quando questa opzione è attivata, i dispositivi Apple nel DEP (Device Enrollment Program) assegnati a questa istanza di "Gestore profilo" possono registrare il proprio dispositivo nel servizio MDM di "Gestore profilo".

  Di default, le seguenti impostazioni sono disattivate per tutti gli utenti e i gruppi di utenti.
- *Consenti la registrazione durante "Impostazione assistita" per i dispositivi configurati mediante Apple Configurator (solo iOS):* quando questa opzione è attivata, i dispositivi iOS configurati con Apple Configurator possono essere registrati nel servizio MDM di "Gestore profilo".
- *Limita la registrazione a dispositivi segnaposto:* quando questa opzione è attivata, solo i dispositivi con un segnaposto con una delle seguenti impostazioni possono registrarsi nel servizio MDM di "Gestore profilo":
  - Numero di serie
  - UDID
  - IMEI
  - MEID
  - ID dispositivo Bonjour (solo Apple TV)

  Nota: La seguente impostazione è un sottoinsieme di questa restrizione.
  - *Limita la registrazione ai dispositivi assegnati:* quando questa opzione è attivata, solo i dispositivi assegnati a un utente possono registrarsi nel servizio MDM di "Gestore profilo":

Installare app in-house in modalità wireless

iOS e OS X supportano l'installazione via etere delle app in-house personalizzate senza utilizzare iTunes o App Store.

Requisiti:

- Un'app iOS in formato .ipa, costruita in versione production con un profilo di fornitura aziendale
- Un file manifest XML, descritto in questa appendice
- Una configurazione di rete che consenta ai dispositivi di accedere a un server iTunes di Apple
- L'utilizzo di HTTPS per iOS 7.1 o versione successiva

Installare l'app è semplice. Gli utenti scaricano il file manifest dal tuo sito web sul loro dispositivo iOS. Il file manifest indica al dispositivo di scaricare e installare le app con riferimenti nel file manifest.

Puoi distribuire l'URL per il download del file manifest via SMS, e-mail o incorporandolo in un'altra app aziendale da te creata.

Dovrai anche prevedere la progettazione e l'hosting del sito web utilizzato per la distribuzione delle app. Assicurati che gli utenti vengano autenticati (mediante autenticazione di base o con directory) e che il sito sia accessibile dalla intranet aziendale o via Internet. Puoi collocare l'app e il file manifest in una directory nascosta o in qualsiasi posizione che possa essere letta via HTTPS.

Se crei un portale self-service, puoi aggiungere un web clip alla schermata Home dell'utente, che in questo modo potrà accedervi facilmente per trovare informazioni, come ad esempio nuovi profili di configurazione e app di App Store consigliate, e per la registrazione con una soluzione MDM.

Preparare un'app in-house per la distribuzione in modalità wireless
Per preparare l'app in-house per la distribuzione wireless, costruisci una versione archiviata (un documento .ipa) e un file manifest che abilita la distribuzione wireless e l'installazione dell'app.

Utilizza Xcode per creare un archivio dell'app. Firma l'app utilizzando il certificato di distribuzione e includi il profilo di fornitura per la distribuzione aziendale nell'archivio. Per ulteriori informazioni sulla costruzione e archiviazione di app, visita iOS Dev Center o consulta il *Manuale Utente di Xcode*, disponibile dal menu Aiuto in Xcode.

Informazioni sul file manifest wireless
Il file manifest è un file plist XML Viene utilizzato dai dispositivi iOS per cercare, scaricare e installare le app dal tuo server web. Il file manifest viene creato da Xcode utilizzando le informazioni da te fornite quando condividi un'app archiviata per la distribuzione aziendale.

I seguenti campi sono obbligatori:

- *URL:* URL HTTPS completo del file dell'app (.ipa).
- *immagine-visualizzata:* immagine PNG di 57x57 pixel visualizzata durante il download e l'installazione. Specifica l'URL completo dell'immagine.
- *Immagine a tutto schermo:* immagine PNG di 512x512 pixel che rappresenta l'app in iTunes.
- *Identificatore bundle:* identificatore bundle dell'app, esattamente come specificato nel progetto Xcode.
- *Versione bundle:* Versione bundle dell'app, come specificato nel progetto Xcode.
- *Titolo:* nome dell'app, visualizzato durante il download e l'installazione.

I seguenti campi sono richiesti solo per le app Edicola:

- *Immagine edicola:* immagine PNG a grandezza piena da visualizzare sullo scaffale di Edicola.
- *UINewsstandBindingEdge e UINewsstandBindingType:* queste chiavi devono coincidere con quelle presenti nel file info.plist dell'app Edicola.
- *UINewsstandApp:* indica che l'app è un'app per Edicola.

Chiavi facoltative utilizzabili come descritto nel file manifest campione. Ad esempio, puoi utilizzare le chiavi MD5 se il documento dell'app è di grandi dimensioni e se desideri garantire l'integrità del download oltre alla verifica degli errori normalmente effettuata per le comunicazioni TCP.

Puoi installare più di un'app con un singolo file manifest specificando altri membri dell'array di elementi.

Alla fine di questa appendice trovi un esempio di file manifest.

Costruire il sito web
Carica questi elementi nell'area del sito web a cui possono accedere gli utenti autenticati:

- Il file dell'app (.ipa)
- Il file manifest (.plist)

Il sito può essere anche solo una pagina web con un collegamento al file manifest. Quando un utente tocca il link web, il file manifest viene scaricato e questo attiva il download e l'installazione delle app che descrive.

Ecco un esempio del link:

```
<a href="itms-services://?action=download-manifest&url=https://exam-
ple.com/manifest.plist">Installa l'app</a>
```

Non aggiungere un link web all'app archiviata (.ipa). Il file .ipa viene scaricato dal dispositivo durante il caricamento del file manifest. Anche se la porzione protocollo dell'URL è itms-services, iTunes Store non viene coinvolto nel processo.

Assicurati inoltre che il file .ipa sia accessibile tramite HTTPS e che il sito sia firmato con un certificato considerato attendibile da iOS. Se un certificato autofirmato non ha un riferimento attendibile e non può essere convalidato dal dispositivo iOS, l'installazione non andrà a buon fine.

Impostare i tipi MIME del server
Devi configurare il server web in modo che il file manifest e il file dell'app vengano trasmessi correttamente.

Per OS X Server, aggiungi i seguenti tipi MIME alle impostazioni dei tipi MIME del servizio web:

application/octet-stream ipa

text/xml plist

Per IIS, utilizza IIS Manager per aggiungere il tipo MIME nella pagina delle proprietà del server:

.ipa application/octet-stream

.plist text/xml

Risoluzione dei problemi relativi alla distribuzione wireless delle app
Se la distribuzione wireless dell'app non riesce e compare un messaggio del tipo "impossibile eseguire il download", controlla quanto segue.

- Verifica che l'app sia firmata correttamente. Prova l'app installandola su un dispositivo tramite Apple Configurator e controllando se si verificano errori.
- Assicurati che il link al file manifest sia corretto e che gli utenti possano accedere al file via web.
- Assicurati che l'URL del file.ipa (nel file manifest) sia corretto e che gli utenti possano accedervi via web via HTTPS.

Requisiti di configurazione network
Se i dispositivi sono connessi a un network interno chiuso, dovresti consentire ai dispositivi iOS l'accesso a quanto segue:

- *ax.init.itunes.apple.com:* Il dispositivo ottiene l'attuale limite delle dimensioni file per il download delle app su rete cellulare. Se il sito web non è raggiungibile, l'installazione potrebbe non riuscire.
- *ocsp.apple.com:* Il dispositivo contatta questo sito web per controllare lo stato del certificato di distribuzione utilizzato per firmare il profilo di fornitura.

Fornire app aggiornate

Le app distribuite direttamente dalla tua azienda non vengono aggiornate automaticamente. Quando è disponibile una nuova versione, informa gli utenti della disponibilità dell'aggiornamento e della necessità di installarlo. Potresti anche configurare l'app in modo che verifichi se sono disponibili aggiornamenti e informi l'utente all'avvio. Se utilizzi la distribuzione wireless delle app, la notifica agli utenti può includere il link al file manifest dell'app aggiornata.

Se vuoi che gli utenti mantengano i dati dell'app archiviati sul loro dispositivo, assicurati che la nuova versione utilizzi lo stesso bundle-identifier della versione da sostituire e chiedi agli utenti di non eliminare la vecchia versione prima di installare quella nuova. La nuova versione sostituirà quella vecchia e manterrà i dati archiviati nel dispositivo, purché il bundle-identifier coincida.

I profili di fornitura per la distribuzione scadono 12 mesi dopo l'emissione. Dopo la scadenza, il profilo viene rimosso e l'app non si aprirà più.

Prima che il profilo di fornitura scada, vai sul sito web di iOS Dev Center per creare un nuovo profilo per l'app. Crea un nuovo archivio dell'app (.ipa) con il nuovo profilo di fornitura per gli utenti che installano l'app per la prima volta.

Se gli utenti hanno già l'app, è consigliabile programmare la versione successiva in modo tale che includa il nuovo profilo di fornitura. Altrimenti, puoi distribuire solo il nuovo file .mobileprovision, così che gli utenti non debbano installare nuovamente l'app. Il nuovo profilo di fornitura sovrascriverà quello già esistente nell'archivio dell'app.

I profili di fornitura possono essere installati e gestiti dalla MDM e quindi scaricati e installati dagli utenti tramite un aggiornamento app o utilizzando la MDM.

Se il certificato di distribuzione scade, l'app non si avvierà più. Il certificato di distribuzione è valido per tre anni dalla data di emissione oppure fino allo scadere della tua iscrizione al programma Enterprise Developer Program, a seconda dell'evento che si verifica prima. Per evitare che il certificato scada, assicurati di rinnovare per tempo l'iscrizione al programma.

Puoi avere contemporaneamente due certificati di distribuzione attivi, l'uno indipendente dall'altro. Il secondo certificato fornisce un periodo di sovrapposizione durante il quale puoi aggiornare le app, prima della scadenza del primo certificato. Quando richiedi il secondo certificato di distribuzione da iOS Dev Center, assicurati di non revocare il primo certificato.

Convalida del certificato

La prima volta che un utente apre un'app, il certificato di distribuzione viene convalidato contattando il server OCSP di Apple. Se il certificato è stato revocato, l'app non si avvierà. L'impossibilità di contattare il server OCSP o di ricevere una risposta non viene considerata una revoca. Per verificare lo stato, il dispositivo deve poter raggiungere ocsp.apple.com. Consulta i requisiti di configurazione della rete.

La risposta OCSP viene archiviata nella cache del dispositivo per un periodo di tempo specificato dal server OCSP; attualmente questo periodo va da tre a sette giorni. La validità del certificato non viene controllata di nuovo fino al riavvio del dispositivo e alla scadenza della risposta archiviata. Se a quel punto si riceve una revoca, l'app non si avvierà.

La revoca di un certificato di distribuzione invaliderà tutte le app firmate con tale certificato. Revoca un certificato solo in ultima istanza, ad esempio se sei sicuro di aver perso la chiave privata o se credi che il certificato sia stato danneggiato.

Esempio di file manifest dell'app

```
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/
     PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <!-- array di download. -->
  <key>items</key>
  <array>
   <dict>
    <!-- array di asset da scaricare -->
     <key>assets</key>
      <array>
       <!-- pacchetto-software: ipa da installare. -->
        <dict>
         <!-- richiesto. il tipo di asset. -->
          <key>kind</key>
          <string>pacchetto-software</string>
          <!-- opzionale. md5 ogni n byte. riavvio chunk se si verifica un errore
     md5. -->
          <key>md5-size</key>
          <integer>10485760</integer>
          <!-- opzionale. array di md5 hash per ciascun chunk di dimensioni "md5-
     size". -->
          <key>md5s</key>
          <array>
            <string>41fa64bb7a7cae5a46bfb45821ac8bba</string>
            <string>51fa64bb7a7cae5a46bfb45821ac8bba</string>
          </array>
          <!-- richiesto. URL del file da scaricare. -->
          <key>url</key>
          <string>https://www.example.com/apps/foo.ipa</string>
        </dict>
        <!-- immagine-visualizzata: icona da visualizzare durante il  download.-->
        <dict>
         <key>kind</key>
         <string>display-image</string>
         <!-- opzionale. indica se l'icona deve presentare un effetto brillante. -->
         <key>needs-shine</key>
         <true/>
         <key>url</key>
         <string>https://www.example.com/image.57x57.png</string>
        </dict>
        <!-- immagine-dimensioni-massime: icona grande da 512 x 512 usata da
     iTunes. -->
        <dict>
         <key>kind</key>
         <string>full-size-image</string>
         <!-- optzionale. hash md5 per l'intero file. -->
```

```
          <key>md5</key>
          <string>61fa64bb7a7cae5a46bfb45821ac8bba</string>
          <key>needs-shine</key>
          <true/>
          <key>url</key><string>https://www.example.com/image.512x512.jpg</string>
         </dict>
       </array><key>metadata</key>
       <dict>
        <!-- richiesto.
        <key>bundle-identifier</key>
        <string>com.esempio.fooapp</string>
        <!-- opzionale (solo software) -->
        <key>bundle-version</key>
        <string>1.0</string>
        <!-- richiesto. tipo di download. -->
        <key>kind</key>
        <string>software</string>
        <!-- opzionale. visualizzato durante il  download; di solito è il nome
     della società  -->
        <key>subtitle</key>
        <string>Apple</string>
        <!-- richiesto. titolo da visualizzare durante il download. -->
        <key>title</key>
        <string>App aziendale di esempio</string>
       </dict>
     </dict>
   </array>
</dict>
</plist>
```

Per ulteriori informazioni sulle chiavi e sugli attributi dei profilo, consulta il materiale di riferimento sulle chiavi dei profili di configurazione.