



Enterprise Mobility Management

Cosa offrono le soluzioni di gestione oggi?

SOMMARIO

1	Enterprise Mobility Management (EMM)	2
2	Garantire la sicurezza automaticamente	3
2.1	Registrazione	3
2.2	Inventari dei dispositivi	6
2.3	Protezione con password	6
2.4	Blocco e cancellazione a distanza	6
2.5	Rilevamento di manipolazioni	7
2.6	Aggiornamento del firmware	8
2.7	Blocco o abilitazione delle app	9
2.8	Configurazione delle app	9
2.9	Sicurezza tramite certificati, distribuzione del software e Wi-Fi aziendale	10
2.10	Verifica della conformità alle linee guida IT	10
2.11	Capacità self-service	11
2.12	Programma VPP (Volume Purchase Program) di Apple	11
3	Completo, efficiente e semplice	13
3.1	Integrata o standalone: quale soluzione è giusta per voi?	13
3.2	Implementazione e facilità di utilizzo	13
3.3	Le sfide della diversità di piattaforme	13
3.4	Gestione trasparente in tempo reale	15
4	Lista di controllo delle funzionalità importanti	16
5	Conclusione	17

© 2025 baramundi software GmbH

Le dichiarazioni su apparecchiature e funzionalità tecniche non sono vincolanti e devono intendersi unicamente a scopo informativo. Soggetto a modifiche. DocID:WP-EMM-200903

1 Enterprise Mobility Management (EMM)

L'uso di dispositivi mobili è diventato una pratica standard in molte aziende. A molti dipendenti sembra assolutamente normale e si aspettano di poter accedere ai dati aziendali dai propri dispositivi mobili. Questo può avere sicuramente dei vantaggi per le aziende, ma i responsabili IT devono essere consapevoli dei rischi. Prima che computer portatili, tablet e smartphone possano essere integrati in modo sicuro nella routine di lavoro quotidiana, è necessario predisporre delle protezioni efficaci come la gestione dell'inventario IT.

Smartphone e tablet sono ora esposti praticamente allo stesso tipo di minacce dei tradizionali PC. Negli ultimi anni, i sistemi mobili sono stati oggetto di pesanti cyberattacchi mirati e gli esperti hanno segnalato nuove varietà di malware che le aziende devono essere pronte ad affrontare. Per trovare una soluzione adeguata, dovremmo prima porci alcune domande importanti:

- Quanto è facile integrare i dispositivi mobili nella soluzione di gestione?
- È possibile creare un inventario di tutti i dispositivi?
- La soluzione presa in esame permette di eseguirne la configurazione?
- Quali funzionalità di sicurezza dovrebbe offrire la soluzione EMM?
- La soluzione EMM supporta le funzioni specifiche per ciascuna piattaforma, come fanno Apple Business Manager o Android Enterprise?
- Integrata o standalone: quale soluzione è giusta per voi?
- Quanto è facile da utilizzare?

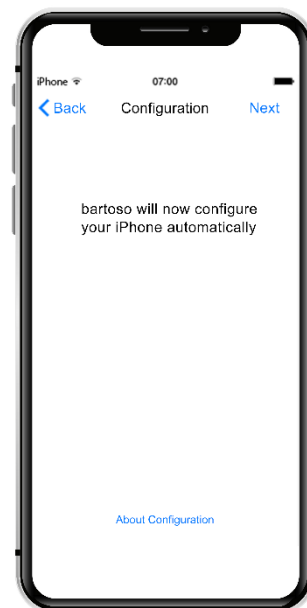
Rispondendo a queste domande è possibile stilare una breve lista dei propri requisiti, che servirà come punto di partenza per valutare vari fornitori in modo più dettagliato ed effettuare una preselezione delle potenziali soluzioni. Gli amministratori dovranno quindi testare le suite EMM e valutarle nella pratica utilizzando questa shortlist personalizzata. Come per i PC, gli obiettivi della gestione dei dispositivi mobili sono: assicurare un funzionamento senza problemi, monitorare lo stato dei dispositivi 24 ore su 24, 7 giorni su 7, e garantire la loro sicurezza. Con l'aiuto di una soluzione di Enterprise Mobility Management, i dispositivi mobili possono essere completamente gestiti e protetti.

2 Garantire la sicurezza automaticamente

2.1 Registrazione

Per la gestione tramite EMM, i dispositivi mobili devono prima essere aggiunti alla soluzione e poi registrati utilizzando il server di gestione. Sono disponibili diverse opzioni:

- registrazione come dispositivo aziendale utilizzabile solo per lavoro (COBO – Company Owned/Business Only)
- registrazione come dispositivo aziendale con abilitazione all'uso personale (COPE – Company Owned/Personally Enabled)
- registrazione come dispositivo personale con accesso ai dati aziendali (BYOD – Bring Your Own Device)
- registrazione come dispositivo dedicato (COSU – Corporate-Owned, Single-Use)



Attivazione di iOS con DEP

2.1.1 Dispositivi aziendali utilizzabili solo per lavoro (COBO)

I dispositivi aziendali utilizzabili solo per finalità lavorative (COBO) non consentono alcun uso personale e non contengono informazioni personali. Questi dispositivi possono essere limitati in base a rigorose linee guida, in modo da prevenire o quantomeno ostacolare un eventuale uso personale "accidentale". Questo fa sì che siano molto sicuri, ma al contempo talmente scomodi che il personale è riluttante ad usarli e finiranno per rimanere nel cassetto dell'ufficio.

2.1.1.1 Programma di registrazione dispositivi Apple (DEP)

Apple fornisce un modo efficiente per integrare rapidamente e senza problemi i dispositivi iOS nel sistema EMM utilizzando il programma DEP (Device Enrollment Program), facente parte di Apple Business Manager.

È possibile ottimizzare questo processo con configurazioni personalizzate, definendo i livelli di autorizzazione degli utenti di ciascun dispositivo durante la relativa fase di attivazione.

I vantaggi chiave del DEP per gli utenti finali risiedono nell'attivazione più rapida e semplice del dispositivo, mentre l'azienda beneficia di una maggiore sicurezza, grazie al costante controllo sui dispositivi aziendali da parte degli amministratori IT.

2.1.1.2 Processo di distribuzione con DEP

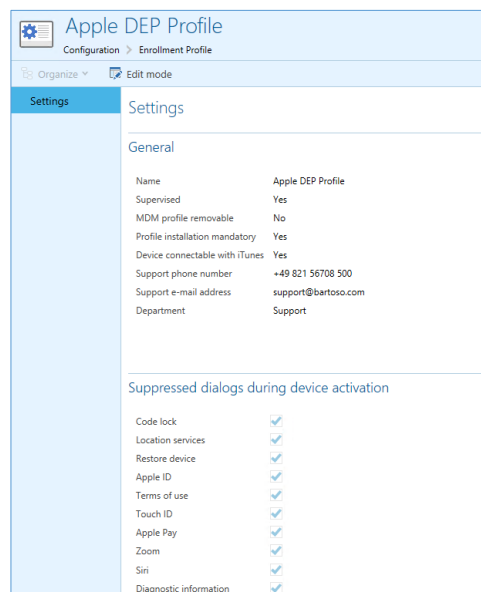
Nell'ambito di una soluzione EMM, il DEP di Apple permette l'esecuzione dei processi di deployment semplificati sotto illustrati, che ne accelerano l'implementazione e offrono una soluzione intelligente di *bulk enrollment*. Gli utenti finali ricevono così i dispositivi nella loro confezione originale con un collegamento immediato al sistema di gestione.

2.1.1.3 DEP dal punto di vista dell'amministratore

L'amministratore non necessita di alcun accesso fisico al dispositivo iOS per integrarlo in modo sicuro nella soluzione di Enterprise Mobility Management.

È possibile preconfigurare un nuovo dispositivo usando EMM per assicurare che sia già conforme alle linee guida aziendali al momento dell'attivazione. In questo modo si può essere certi che tutti i dispositivi sono configurati allo stesso modo e sono sempre monitorati dal sistema di gestione.

Utilizzando un normale profilo, l'amministratore può impostare i livelli di autorizzazione degli utenti finali durante l'attivazione del dispositivo.



Profilo DEP (Device Enrollment Profile) in iOS

2.1.2 Dispositivo aziendale con abilitazione all'uso personale (COPE)

I dispositivi COPE (Company Owned/Personally Enabled) appartengono all'azienda e possono essere usati dall'utente sia per finalità aziendali che personali. Di conseguenza, le linee guida diventano meno rigide e l'uso personale diventa così più attraente per l'utente. Questi dispositivi sono di solito gestiti centralmente dal sistema MDM (Mobile Device Management). In questo scenario, la protezione dei dati assume una rilevanza cruciale. I dati e le app personali devono essere gestiti separatamente da quelli aziendali. Con la configurazione corretta, DEP può essere usato in entrambi gli scenari COBO e COPE.

2.1.3 Dispositivi personali con accesso ai dati aziendali (BYOD)

Il concetto di "Bring Your Own Device" si riferisce alla situazione in cui gli utenti utilizzano i propri dispositivi per scopi aziendali. Analogamente allo scenario COPE, sul dispositivo sono presenti sia i dati personali che quelli aziendali. In questo caso è fondamentale assicurare un'attenta separazione dei dati. Sussiste inoltre il pericolo che i dati di contatto aziendali finiscano nelle app personali come WhatsApp. Allo stesso tempo, l'amministratore IT non deve avere alcun accesso ai dati personali dell'utente del dispositivo. Come tale, il concetto funziona solo quando entrambi i tipi di dati sono accuratamente separati e protetti da entrambe le parti. Una soluzione pratica a questo problema sono le funzioni native per la separazione dei dati in iOS e Android. In questo caso, quando usa Android Work Profile l'amministratore non può vedere le app personali degli utenti. La stessa funzione è possibile anche in iOS con User Enrollment.

2.1.4 Dispositivi dedicati (COSU)

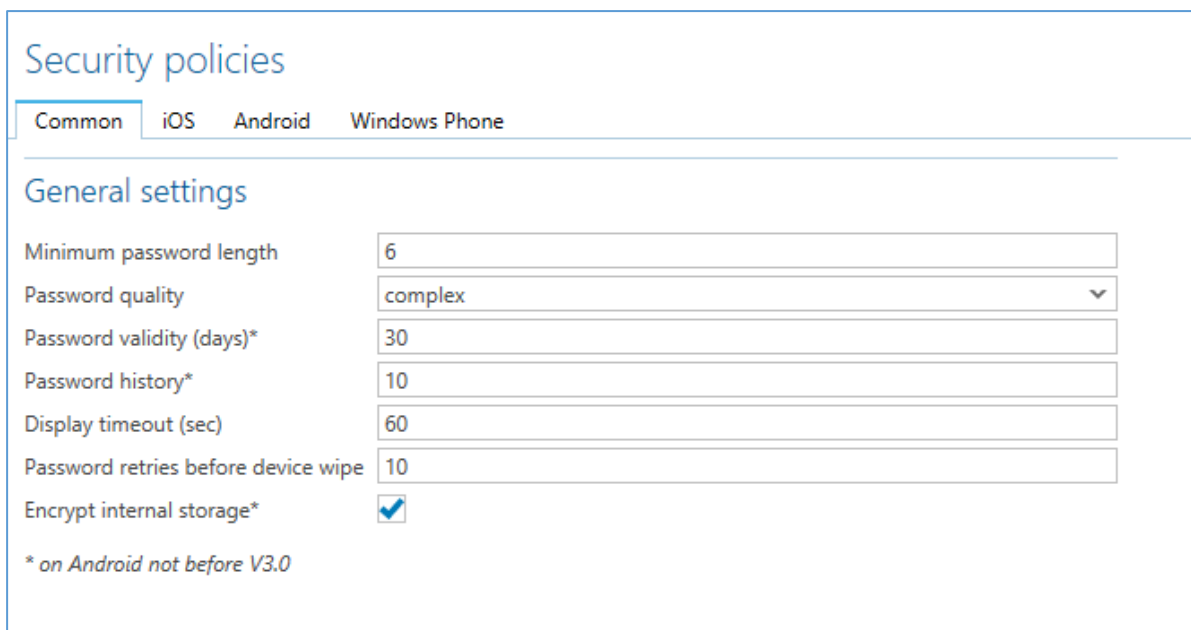
I dispositivi COSU (Corporate Owned, Single-Use) sono configurati esclusivamente per un uso specifico, ad esempio scansione di codici a barre o sistema POS. La funzionalità di questi dispositivi è studiata su misura per uno scopo specifico ed è consentita l'esecuzione di una sola app o di una lista definita di app secondo le specifiche dell'amministratore. Dal momento che questi dispositivi devono essere liberamente condivisi tra diversi utenti dell'azienda nell'uso quotidiano, queste configurazioni non hanno alcun riferimento all'utente e non richiedono l'identificazione di quest'ultimo.

2.2 Inventari dei dispositivi

Quali dispositivi fanno parte della mia rete e cosa è installato su di essi? Un EMM dovrebbe essere in grado di fornire risposte di base a queste domande su tutte le piattaforme più comuni. Per esempio, sui dispositivi mobili iOS e Android, possono essere raccolte informazioni sull'hardware e le impostazioni di sicurezza, così come le app e i certificati installati.

2.3 Protezione con password

Per salvaguardare i preziosi dati aziendali è necessaria una protezione affidabile contro l'accesso non autorizzato attraverso una password. Sui dispositivi mobili ciò può essere applicato tramite EMM. È anche possibile specificare il livello di complessità richiesto per le password. Le politiche di crittografia dei dispositivi possono essere successivamente estese ai dispositivi mobili dove non sono state precedentemente attivate. In questo modo, le politiche di sicurezza possono essere applicate uniformemente in tutta l'organizzazione.



Security policies

Common iOS Android Windows Phone

General settings

Minimum password length	6
Password quality	complex
Password validity (days)*	30
Password history*	10
Display timeout (sec)	60
Password retries before device wipe	10
Encrypt internal storage*	☒

* on Android not before V3.0

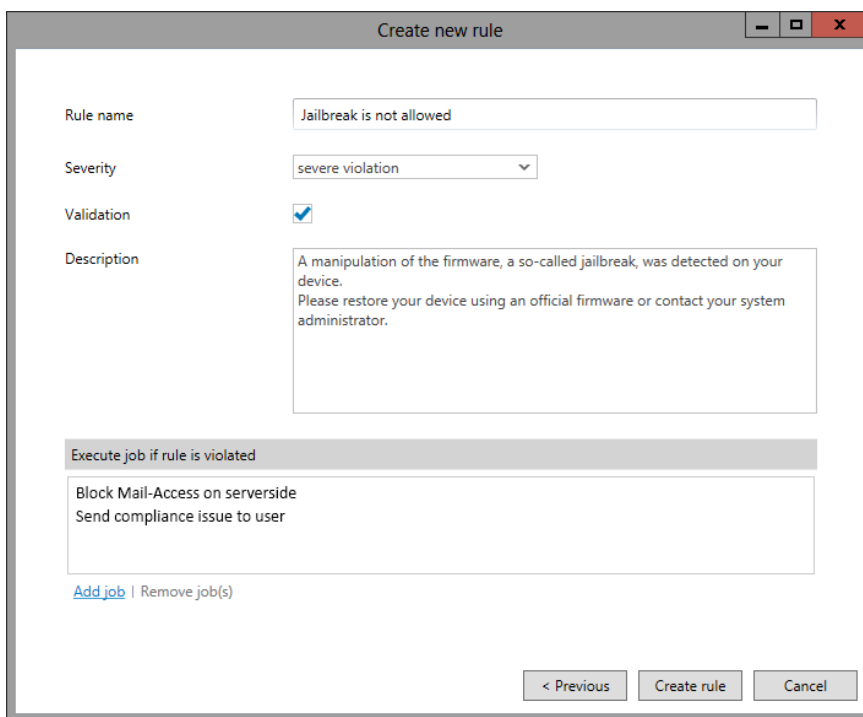
Configurazione del profilo di sicurezza

2.4 Blocco e cancellazione a distanza

In caso di perdita, i dispositivi possono essere bloccati e cancellati a distanza, in base alla rispettiva piattaforma. Se un utente dimentica la propria password, l'amministratore può aiutarlo a sbloccare il dispositivo da remoto. A seconda della piattaforma, il dispositivo può anche essere bloccato, in modo da impedire l'accesso mediante i parametri biometrici e consentirlo solo tramite PIN. Questo "Lost Mode" permette all'amministratore anche di localizzarlo.

2.5 Rilevamento di manipolazioni

Nell'ambito delle modifiche al firmware due termini chiave sono *jailbreak* (su dispositivi iOS) e *root* (su Android). Queste modifiche permettono all'utente di installare app da fonti potenzialmente insicure, compresi App Store alternativi, o di attivare funzioni che non sono state verificate o approvate dal produttore. Le istruzioni per l'installazione di queste modifiche possono essere trovate su Internet. Gli smartphone modificati mediante *jailbreak* o *root* minano le funzionalità di sicurezza del sistema operativo, con un significativo aumento del rischio di installazione di malware. Anche la capacità di gestire un dispositivo modificato tramite EMM è compromessa, poiché le funzionalità di sicurezza del dispositivo possono essere facilmente aggirate. Per prevenire che ciò accada, le aziende dovrebbero vigilare costantemente e controllare l'eventuale presenza di questi tipi di modifiche ai sistemi operativi.



Controllo di jailbreak

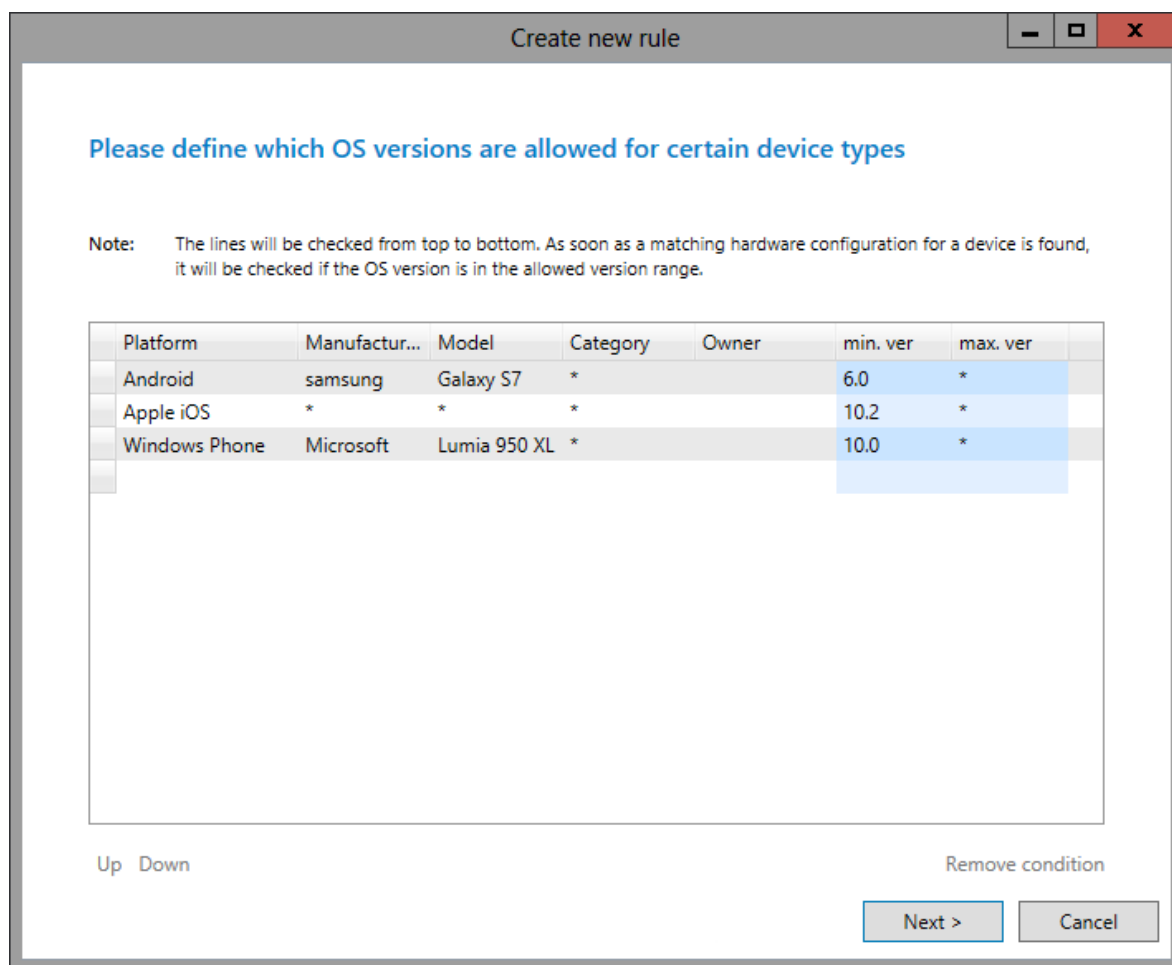
I dispositivi modificati in questo modo dovrebbero essere classificati come rischi estremi per la sicurezza e i sistemi EMM devono essere in grado di riconoscere questo tipo di manipolazioni e auspicabilmente anche di reagire automaticamente a tale evenienza, ad esempio, limitando l'accesso ai dati aziendali da parte dei dispositivi modificati.

2.6 Aggiornamento del firmware

L'aggiornamento tempestivo del firmware è importante quanto la prevenzione delle modifiche. Gli aggiornamenti non vengono eseguiti solo per aggiungere nuove funzionalità, ma anche per eliminare le vulnerabilità.

Una buona soluzione EMM non si limita ad aggiornare il firmware, ma permette anche di posticipare di un determinato intervallo gli aggiornamenti, per consentire agli amministratori di testare prima il nuovo firmware e le sue funzioni, nonché di verificare la sicurezza delle app aziendali sviluppate internamente.

Il monitoraggio della versione del firmware dei dispositivi è possibile su tutte le piattaforme. Gli amministratori possono accedere in remoto a una panoramica della situazione in qualsiasi momento, grazie agli inventari dei dispositivi e ai test delle regole automatizzati.



Create new rule

Please define which OS versions are allowed for certain device types

Note: The lines will be checked from top to bottom. As soon as a matching hardware configuration for a device is found, it will be checked if the OS version is in the allowed version range.

Platform	Manufactur...	Model	Category	Owner	min. ver	max. ver
Android	samsung	Galaxy S7	*		6.0	*
Apple iOS	*	*	*		10.2	*
Windows Phone	Microsoft	Lumia 950 XL	*		10.0	*

Up Down

Remove condition

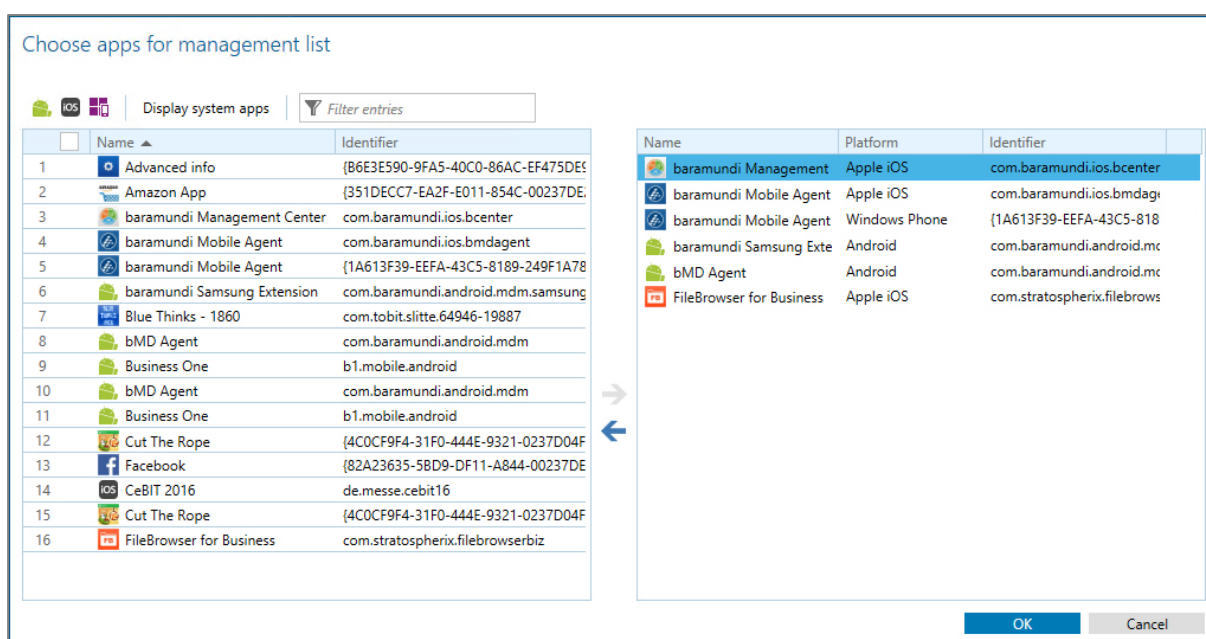
Next > Cancel

Determinazione delle regole per le versioni del sistema operativo

2.7 Blocco o abilitazione delle app

Una soluzione EMM dovrebbe permettere il blocco o l'abilitazione delle app, per impedire l'esecuzione di app pericolose o garantire che solo le app che l'azienda considera affidabili possano essere utilizzate. In questo modo gli amministratori possono impedire l'installazione o l'uso di app indesiderate sui dispositivi mobili gestiti o definire quali app saranno esplicitamente permesse mediante la relativa abilitazione. Tutte le app che non sono approvate dall'azienda non possono essere installate o eseguite.

A seconda del caso, è possibile adottare per un dato dispositivo un approccio basato sull'abilitazione oppure sul blocco delle app. Dopo aver definito l'approccio che si intende utilizzare, si procede a inserire le app consentite in una lista, che viene quindi applicata come profilo al dispositivo mobile.



Selezione delle app per le liste di blocco/abilitazione

Anche con liste create successivamente, con l'EMM l'amministratore può vedere a colpo d'occhio se un'app preinstallata può essere eseguita in sicurezza. Grazie a queste liste è possibile difendersi efficacemente dalle app indesiderate e/o pericolose.

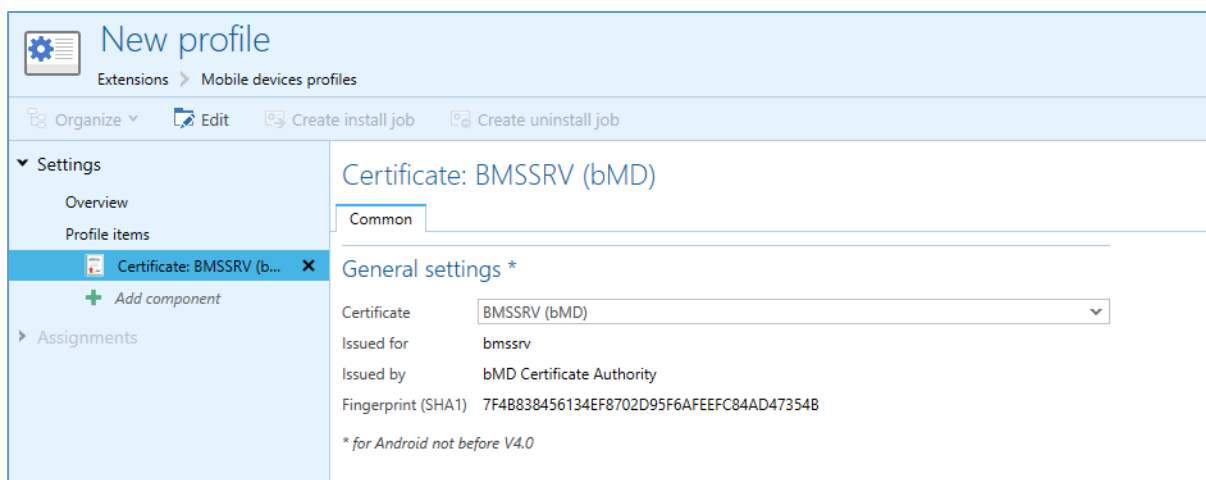
2.8 Configurazione delle app

L'Enterprise Mobility Management comprende diverse sottodiscipline della gestione dei dispositivi mobili. Le tre aree fondamentali sono Mobile Device Management (MDM), Mobile Application Management (MAM) e Mobile Content Management (MCM), quindi la gestione dell'intero dispositivo mobile, delle singole app e infine dei contenuti.

La figura seguente mostra queste connessioni utilizzando meccanismi tipici.

2.9 Sicurezza tramite certificati, distribuzione del software e Wi-Fi aziendale

Una soluzione EMM dovrebbe anche supportare la distribuzione di certificati aziendali client, garantendo così la fiducia necessaria per mantenere la sicurezza dei servizi aziendali.



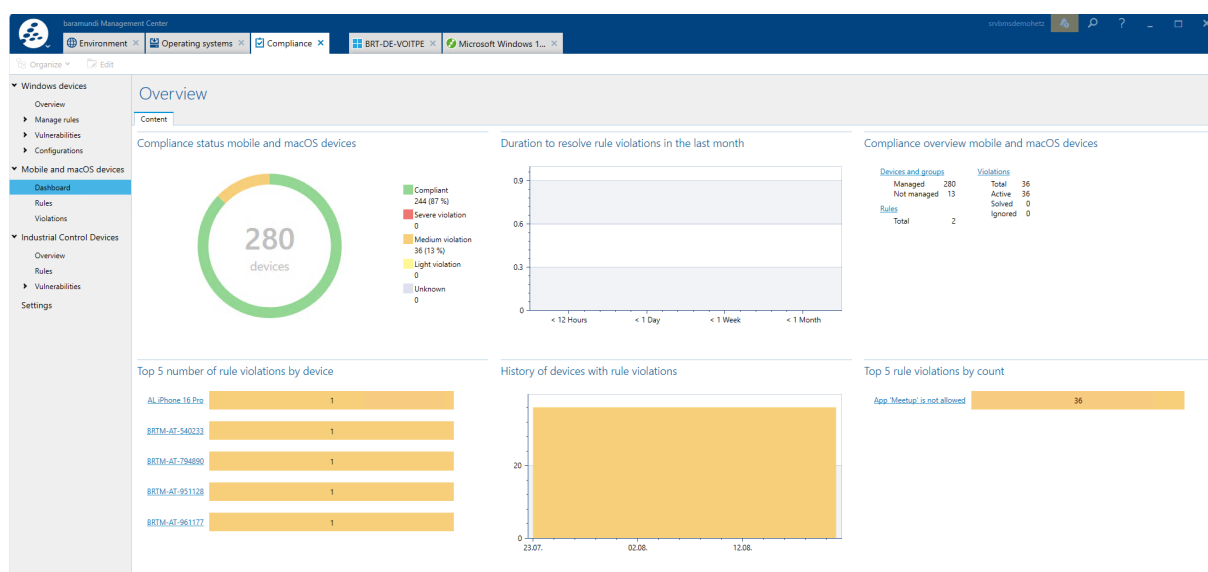
Struttura del profilo per certificati client

Tali certificati possono poi essere utilizzati per proteggere l'accesso tramite Microsoft Exchange o per implementare una rete Wi-Fi aziendale sicura. In entrambi i casi, la sicurezza della connessione dipende dai certificati e non dal login degli utenti.

2.10 Verifica della conformità alle linee guida IT

Garantire la conformità alle regole aziendali è particolarmente importante per i dispositivi mobili. Oltre a stilare le liste delle app bloccate e approvate o rilevare i tentativi di modifica dei dispositivi, gli amministratori possono identificare e installare su ciascun dispositivo eventuali app necessarie non presenti.

Le informazioni sulla conformità alle regole aziendali dovrebbero essere chiaramente visualizzate su un apposito cruscotto e organizzate per tipo di dispositivo e/o livello di gravità. Gli amministratori potranno così identificare con un colpo d'occhio le aree che richiedono un intervento immediato. Si raccomandano soluzioni EMM che supportano risposte automatizzate – dall'invio di e-mail agli utenti alla cancellazione da remoto di un dispositivo in caso di violazioni particolarmente gravi, come un *jailbreak*.



Panoramica sulla conformità alle linee guida IT

2.11 Capacità self-service

Il self-service è una comoda soluzione per fornire supporto immediato all'utente, riducendo al contempo il volume delle richieste di supporto. Attraverso un chiosco è possibile mettere a disposizione app pronte per l'installazione e task senza necessità di intervento da parte dell'amministratore.

2.12 Programma VPP (Volume Purchase Program) di Apple

Apple ha sviluppato per le imprese il programma VPP (Volume Purchase Program) per l'acquisto e la gestione delle licenze delle app con opzioni di utilizzo aggiuntive incluse.

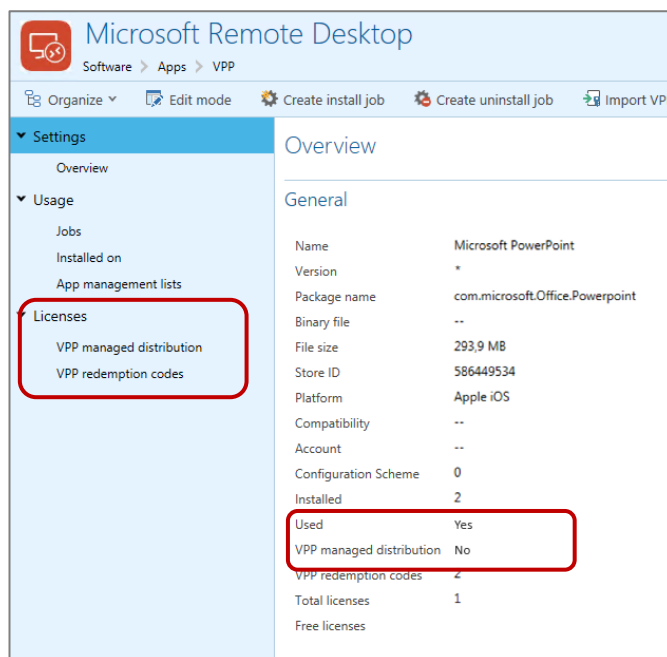
	Codici di attivazione VPP	Managed Distribution User Assignment	Managed Distribution Client Assignment
Collegamento delle licenze	ID Apple*	ID Apple*	Dispositivo
Distribuzione delle app	solo con ID Apple*	solo con ID Apple*	senza ID Apple*
Distribuzione senza interazione dell'utente	n/d	n/d	sì (per dispositivi supervisionati)
Gestione delle licenze/visualizzazione nella suite MDM	elenchi di licenze; inserimento manuale	associazione automatica nella suite MDM	associazione automatica nella suite MDM
Revoca di licenze da admin	n/d	sì	sì
Disponibilità tramite Apple	iOS 5	iOS 7	iOS 9

*) "Apple ID" si riferisce all'ID dell'utente per i prodotti/sistemi Apple

2.12.1 Supporto VPP dal punto di vista dell'amministratore

Il supporto VPP offre una vasta gamma di possibilità per la distribuzione di applicazioni a pagamento o gratuite. Gli amministratori possono scegliere tra l'utilizzo di codici di attivazione (*redemption code*) o la distribuzione gestita per ogni singola app.

Dopo essere stata assegnata a un dispositivo, la licenza può poi essere revocata e trasferita per l'utilizzo su un altro dispositivo.



Supporto VPP in bMD

3 Completo, efficiente e semplice

3.1 Integrata o standalone: quale soluzione è giusta per voi?

Una decisione fondamentale riguarda il modo in cui la soluzione è integrata nell'IT aziendale esistente. È possibile scegliere tra opzioni EMM integrate nell'Unified Endpoint Management (UEM) oppure una soluzione EMM standalone. Le aziende che optano per l'UEM possono gestire in tal modo anche i dispositivi mobili. Il vantaggio in questo caso è ovvio: quando l'EMM è integrato con l'Unified Endpoint Management, tutti i client possono essere gestiti attraverso un'unica interfaccia e l'amministratore ha sempre una panoramica della situazione. Questa soluzione è ideale per le aziende con un numero ridotto di responsabili dell'infrastruttura IT, dove un effetto sinergico potrebbe avere un impatto positivo.

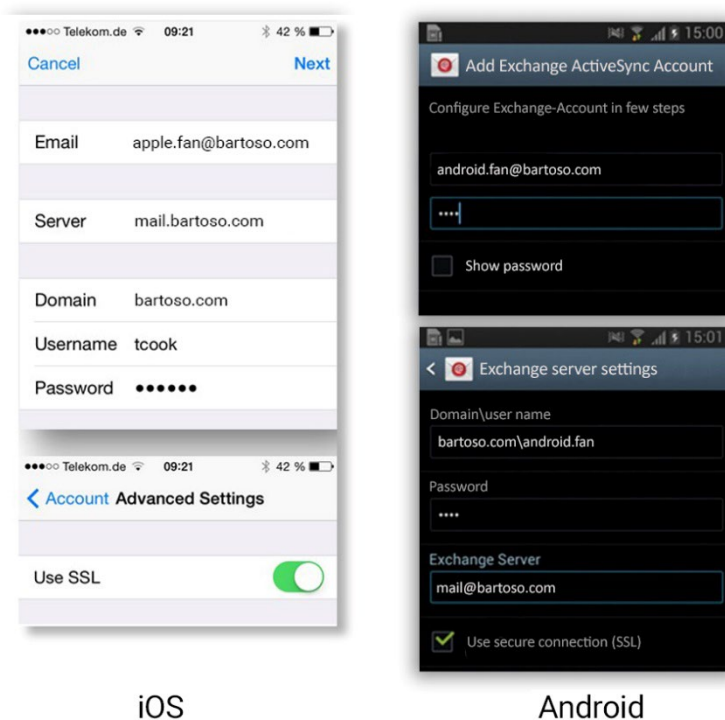
3.2 Implementazione e facilità di utilizzo

Quando si sceglie una soluzione EMM, è necessario considerare gli sforzi richiesti per l'implementazione, la messa in funzione e la formazione. L'integrazione della soluzione nell'infrastruttura IT esistente dovrebbe essere il più semplice possibile. È anche importante che la soluzione presenti un'interfaccia chiara e possa essere usata in modo intuitivo. Questi fattori sono essenziali affinché eventuali nuove risorse IT possano essere subito operative con l'EMM, eliminando così la necessità di una formazione estesa e di costi aggiuntivi. Un aspetto cruciale per le funzioni IT con budget limitati.

3.3 Le sfide della diversità di piattaforme

Gli amministratori sono spesso chiamati a fornire supporto per una grande varietà di piattaforme mobile. Questo implica conoscerle a fondo, saperne eseguire la distribuzione ed essere pronti a offrire assistenza, comprese tutte le impostazioni dettagliate. Un compito alquanto complesso ed anche dispendioso in termini di tempo.

Un tipico esempio è l'inserimento dei dettagli di configurazione di Exchange per il servizio di posta elettronica su due delle piattaforme mobile più diffuse (Android e iOS), dove i parametri di base (cioè nome, indirizzo e-mail, dominio, server, crittografia, ecc.) devono essere specificati in finestre di dialogo completamente diverse.



iOS

Android

Configurazione di Exchange su piattaforme diverse

È ovvio che la soluzione auspicata sia uno strumento che permetta un inserimento dei dati uniforme per tutti i dispositivi da gestire. Con un EMM di questo tipo, gli amministratori possono gestire coerentemente tutti i dispositivi mobili da un'unica interfaccia, accelerando e semplificando le configurazioni di Exchange, indipendentemente dal sistema operativo.

Exchange account: Exchange

Common

iOS

Android

Windows Phone

General settings *

Component name

Exchange

Display name on device

{RegisteredUser.Mail}

E-mail address

{RegisteredUser.Mail}

User name

{RegisteredUser.UserLogonName}

Domain

{RegisteredUser.Domain}

Exchange server (FQDN)

mail.bartoso.com

Encrypted communication

☒

Certificate selection

None

* for Android only supported by devices with Samsung KNOX or HTC Pro

Configurazione multiplatforma di Exchange tramite EMM

3.4 Gestione trasparente in tempo reale

Una buona soluzione EMM fornisce dati tempestivi, aggiornati e rilevanti per tutti i dispositivi mobili gestiti in una vista panoramica. Questo è cruciale, perché gli amministratori possono valutare correttamente la sicurezza dei dispositivi mobili solo se sono pienamente informati e possono accedere rapidamente a tutte le informazioni e ai feedback importanti. Avere un database aggiornato sempre disponibile permette inoltre di creare e redigere rapporti ogni volta che è necessario.

4 Lista di controllo delle funzionalità importanti

Distribuzione e configurazione del software	
☐	Distribuzione Programmazione degli aggiornamenti del firmware
☐	Supporto della separazione nativa dei dati
☐	Installazione di app con senza conferma dell'utente
☐	Disinstallazione delle app con senza conferma dell'utente
☐	Supporto di Volume Purchase Program (VPP) di Apple
☐	Supporto di Device Enrollment Program (DEP) di Apple
☐	Installazione disinstallazione con App Store disattivato
☐	Installazione disinstallazione di applicazioni aziendali sviluppate internamente
☐	App self-service: Chiosco (Kiosk)
☐	Installazione disinstallazione di certificati
☐	Parametrizzazione delle impostazioni tramite variabili
☐	Installazione di collegamenti ipertestuali (iOS: Web Clip)
☐	Disattivazione della telecamera
☐	Configurazione di punti di accesso (APN)
Inventari dei dispositivi	
☐	Informazioni sull'hardware
☐	Limitazioni configurate (blocco iCloud, ecc.)
☐	Profili installati
☐	Certificati installati
☐	Informazioni sulla SIM
☐	Stato del roaming
☐	Impostazioni di sicurezza
☐	Ultimo contatto
☐	Raggruppamento di dispositivi
Sicurezza	
☐	Blocco Sblocco Cancellazione da remoto
☐	Rilevamento richieste e complessità di PIN/password
☐	Rilevamento di manipolazioni del firmware (Jailbreak, Root)
☐	Impostazione delle politiche di crittografia dei dispositivi
☐	Supporto di whitelist blacklist di app
☐	Disattivazione delle app di sistema
☐	Disattivazione della WLAN
☐	Disattivazione del Bluetooth
☐	Cronologia password Reset Impostazione nuova password
☐	Abilitazione / disabilitazione dell'accesso alla scheda SD
☐	Abilitazione / disabilitazione dell'accesso agli App Store
☐	Connessione automatica alla WLAN
Conformità	
☐	Rilevamento di app essenziali mancanti
☐	Rilevamento di app installate indesiderate
☐	Rilevamento di configurazioni errate
☐	Rilevamento di versioni obsolete del sistema operativo
☐	Stato e cronologia di violazioni delle regole

5 Conclusione

Non esiste un'unica soluzione EMM ottimale per tutte le aziende. Per prendere la decisione giusta è importante definire chiaramente il set di funzionalità desiderate e testare le soluzioni candidate. Oltre alle funzionalità offerte, anche la tipologia di impresa e l'uso previsto per il sistema hanno una grande rilevanza. Oltre agli aspetti tecnici, bisogna inoltre considerare anche le esigenze dei colleghi e degli utenti finali. Senza la loro accettazione l'intero progetto per la mobility è destinato a fallire. Per questo motivo, quando si sceglie una soluzione EMM, al momento della decisione occorre cercare un equilibrio tra i seguenti elementi:

- requisiti di sicurezza dell'azienda
- accettazione dei dispositivi mobili da parte del personale e degli utenti finali
- facilità di utilizzo dei servizi di gestione da parte degli amministratori

L'adozione di qualsiasi soluzione EMM potrà avere successo solo prendendo in considerazione tutti e tre questi punti.

Informazioni su baramundi software GmbH

baramundi software sviluppa soluzioni di Unified Endpoint Management per la gestione centralizzata di PC, dispositivi mobili e server. Automatizza la distribuzione dei software, semplifica la gestione delle patch e garantisce la trasparenza nella rete. baramundi contribuisce in modo significativo alla sicurezza IT e libera risorse.

Per maggiori informazioni su baramundi: www.baramundi.com

Pronti a scoprire tutti i dettagli sulla soluzione EMM? Iscrivetevi al live webinar!

Scoprite come gestire smartphone e tablet con la stessa facilità e affidabilità di PC e notebook:
www.baramundi.com/it-training/

**Saremo lieti di
incontrarvi!**

Contattateci!



baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany

 +49 821 5 67 08 - 380
request@baramundi.com
www.baramundi.com

 +44 2071 93 28 77
request@baramundi.com
www.baramundi.com

 +48 735 91 44 54
request@baramundi.com
www.baramundi.com

 +49 821 5 67 08 - 390
request@baramundi.com
www.baramundi.com

 +43 19 28 01 36 00 10
request@baramundi.com
www.baramundi.com

 +39 340 8861886
request@baramundi.com
www.baramundi.com

 +41 77 280 49 79
request@baramundi.com
www.baramundi.com

baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA

 +1 508-861-7561
requestUSA@baramundi.com
www.baramundi.com