

LINEE GUIDA MDM - AIRWATCH INTERCENT

Proprietario: Digitare il proprietario

Data emissione: 00-00-0000

Codice doc.: Codice

Destinatari: Digitare i destinatari o un codice di rif. alla lista

1 INTRODUZIONE	4
2 OBIETTIVI E REQUISITI	4
3 REGISTRAZIONE MODIFICHE DOCUMENTO	4
4 ARCHITETTURA HIGH LEVEL.....	4
4.1 INTRODUZIONE	4
4.2 MULTILAYER.....	5
4.3 DB RECOVERY	6
4.4 TENANTS E MULTITENANCY	7
4.5 BACKUP E RESTORE	7
5 MODELLO FUNZIONALE E GESTIONALE.....	7
6 MODELLO CONFIGURATIVO DI AIRWATCH.....	8
7 ENROLLMENT TERMINALI CLIENTE.....	10
7.1 ORGANIZATION GROUP (TENANT).....	10
7.1.1 Creazione account	11
7.1.2 Configurazione Tenant	12
7.1.3 Privacy Settings	14
7.2 INSTALLAZIONE APNS (APPLE PUSH NOTIFICATION SERVICE) CERTIFICATE.....	14
7.3 SERVIZIO ANDROID PUSH	15
7.4 ENROLLMENT DEI TERMINALI	16
7.4.1 Android	17
7.4.2 Apple.....	17
7.4.3 Win Phone 8.....	18
7.4.4 Black Barry.....	19
7.4.5 Migrazione terminali	19
8 FUNZIONALITÀ	19
8.1 PACKAGE E FILE DISTRIBUTION	19
8.1.1 Android	20
8.1.1.1 Market	20
8.1.1.2 Internal	20
8.1.2 Apple.....	21
8.1.2.1 Market	21
8.1.2.2 Internal	21
8.2 SECURITY 22	
8.2.1 Android	22
8.2.1.1 Gestione Device password	22
8.2.1.2 Gestione blocco device.....	23
8.2.1.3 Utilizzo di Black/White list : Samsung,	24
8.2.1.4 Restrictions all'uso del device : Samsung	24
8.2.1.5 Disabilitazione camera :	24

8.2.1.6 Encryption dati :	24
8.2.1.7 Firewall	24
8.2.2 iOS	24
8.2.2.1 Gestione del JailBreak	25
8.2.2.2 Gestione blocco device.....	25
8.2.2.3 Gestione Device password	25
8.2.2.4 Restrizioni all'uso del device	26
8.2.2.1 Encryption dati :	26
8.2.2.1 Firewall	26
8.3 INVENTORY	26
8.4 DEVICE CONFIGURATION.	27
8.4.1 Android	27
8.4.1.1 Connessioni.....	27
8.4.1.2 Posta elettronica	27
8.4.2 Apple,	28
8.4.2.1 Connessioni.....	28
8.4.2.2 Posta elettronica	28
8.5 AMMINISTRAZIONE.....	28

1 INTRODUZIONE

Il seguente documento definisce la linea guida del servizio MDM (Mobile Device Management) basato sul software AirWatch erogato in modalità SAAS. Definisce il contenuto tecnico e di processo del servizio realizzato su una piattaforma tecnologica costituita da hardware, software dedicata all'erogazione di un servizio MDM (Mobile Device Management) in Nuvola Italiana.

2 OBIETTIVI E REQUISITI

Il documento di linea guida si prefigge l'obiettivo di essere un supporto, ausilio alla progettazione del servizio e alla divulgazione della conoscenza delle modalità tecnico/funzionali di erogazione del servizio.

3 REGISTRAZIONE MODIFICHE DOCUMENTO

La tabella seguente riporta la registrazione delle modifiche apportate al documento.

DESCRIZIONE MODIFICA	REVISIONE	DATA
Prima emissione	1.0	23-01-2014

4 Architettura High Level

4.1 Introduzione

La piattaforma di Mobile Device Management oggetto della presente linea guida è AirWatch. Si tratta di un prodotto che consente di rendere efficiente la gestione di dispositivi mobili, sovrintendendo a tutte le funzionalità di gestione dei dispositivi e delle applicazioni in uso all'utente mobile, oltre che consentendo la gestione e la diagnostica dei terminali che permette di evidenziare eventuali anomalie hardware e software in maniera immediata.

Le attività di Device Management possono essere eseguite in modo "silente" e trasparente all'utente, in modo tale che non possa avere impatti sulle attività di business dell'utente. E' inoltre possibile schedare tali attività con cadenza periodica o innescarle a fronte di eventi particolari. La piattaforma di Mobile Device Management AirWatch è in grado di lavorare sia sotto copertura LAN/WiFi, tipicamente per contesti indoor, sia sul territorio in condizioni di mobilità, con connessione

GPRS/UMTS. AirWatch è inoltre in grado di ottimizzare l'uso della banda disponibile. Nell'ambito delle diverse soluzioni di Mobile Device Management che offre il mercato, alcune caratteristiche peculiari di AirWatch ne fanno una soluzione di eccellenza. Tra queste, vale la pena citare:

- Supporto multiplatforma ,multivendor e multitenant
- Gestione ottimizzata della banda
- Scalabilità ed alta affidabilità
- Referenze in ambiti progettuali complessi

La soluzione permette di gestire dispositivi mobili eterogenei; da iOS, Android, Windows Phone 8,...

In relazione al sistema operativo del dispositivo mobile esistono particolarità nell'uso delle funzionalità implementabili.

Le principali caratteristiche saranno trattate nel corso del documento.

4.2 Multiplayer

L'architettura che eroga il servizio AirWatch è composta da 13 server installati sulla piattaforma virtuale VMware multiplayer area mercato di Pomezia (Nuvola Italiana) protetta da FW per ogni layer ed esposta su Internet per l'erogazione dei servizi e dell'amministrazione.

Prevede:

Front End : proxy server. Vedono Internet ed inoltrano/ricevono le sessioni ai server applicativi nell'application layer da parte dei client AirWatch. Sul livello di FE sono installati 2 server. Il reverse proxy per le comunicazioni https con la console amministrativa e/o verso i siti remoti di Apple, google; mentre i proxy supportano le connessioni dei device che utilizzano il client AirWatch. Infatti la comunicazione viene sempre instaurata dal client per accedere ai servizi di piattaforma MDM. Il servizio invece stimola in modo silente il client per farlo attivare senza il coinvolgimento dell'utente ad utilizzare le nuove configurazioni impostate dall'amministratore del servizio. Ci sono occasioni invece che l'amministratore comanda direttamente azioni sul device (es: wipe e lock in caso di furto,...)

Application layer : riceve ed inoltra verso il front end le sessioni aperte dai client AirWatch installati c/o i device mobili o pc degli utenti. Accede al DB per la scrittura e lettura dei dati applicativi. A questo livello sono presenti 6 server. Due di questi sono nominati AdminConsole e permettono di centralizzare le configurazioni della farm. I restanti 4 server sono i device server che gestiscono le connessioni con i device, così come l'hosting del self service portal; mentre le api server sono utilizzati per esporre le interfacce funzionali per permettere ad applicazioni esterne di interagire con le funzionalità mdm.

DB Layer : l'accesso ai dati da parte dell'application layer avviene su un DB posizionato nel terzo livello di infrastruttura. Il DB è un SQL Server 2008 R2 Standard Edition ed è stato progettato per garantire una replica dei suoi dati su un server equivalente per l'HA. Gli schemi dei dati sono configurati dall'applicazione AirWatch durante la fase di installazione dei server applicativi. Il primo server applicativo installato marca sul db il suo ed unico ruolo di master.

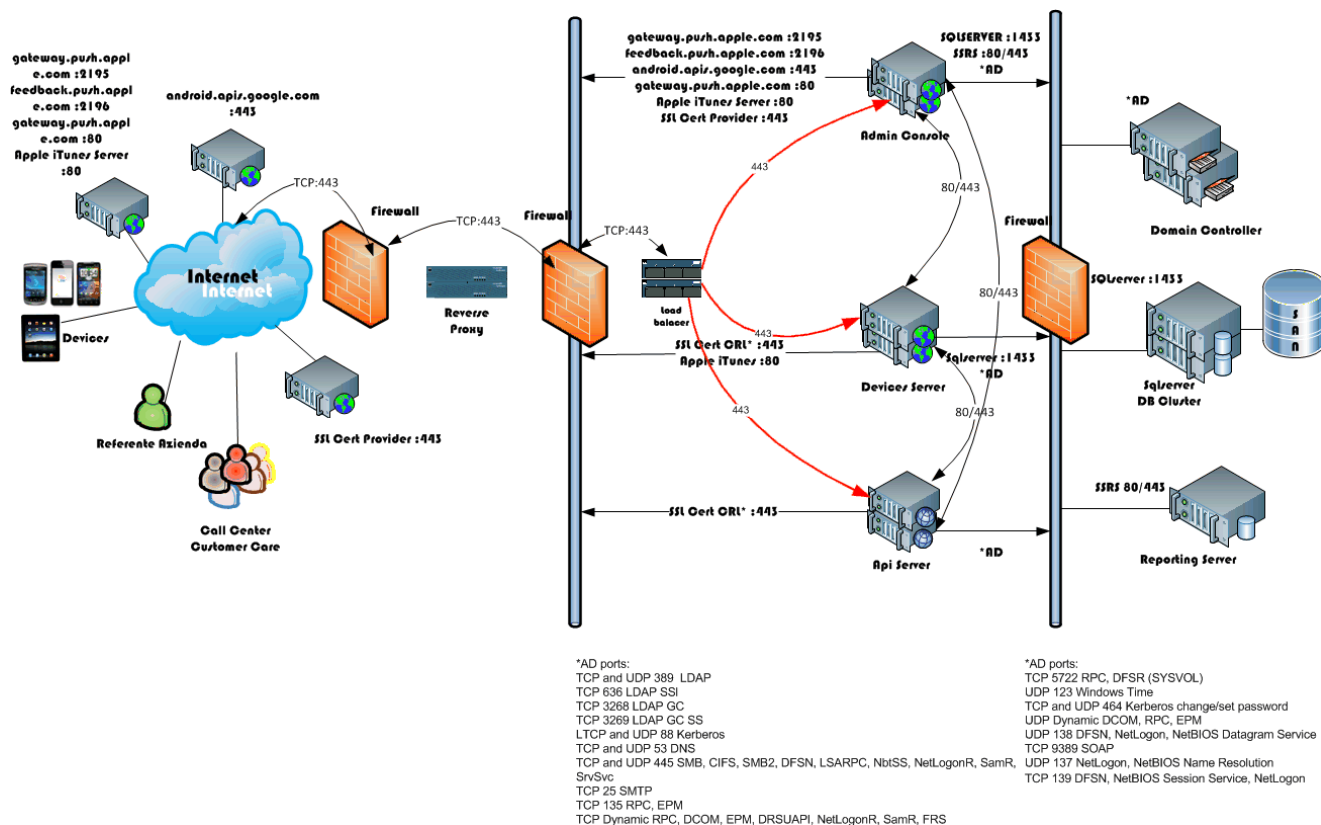


Figura 4-1

Tra i diversi layer di piattaforma e verso i device clienti la comunicazione avviene attraverso protocolli standard e sicuri. Citiamo tra i più usati : https, scep (simple certificate enrollment protocol), sql (1433), etc

Le comunicazioni tra device e piattaforma sono effettuate tramite client AirWatch installato su terminale mobile. Le connessioni e profiling tra client e server sono effettuate su rete dati mobile (APN).

4.3 DB Recovery

Il DB server è realizzato con MS Windows Server 2008 SE R2 64 bit con il *db SQL Server 2008 R2 Standard Edition*.

Il sistema prevede una replica dei dati su un secondo server db. Questo garantisce in caso di fault del db il ripristino del servizio (in pochi minuti) senza perdita di dati.

Va ricordato che tra i meccanismi di recovery ci sono quelli propri dell'infrastruttura virtuale (Nuvola Italiana) con cui sono stati configurati i 13 server della piattaforma.

4.4 Tenants e Multitenancy

La piattaforma di T.I. è di tipo “multitenant”, per cui ogni azienda cliente (tenant) può accedere in modalità Software as a Service (SaaS) alla piattaforma stessa ospitata presso la Nuvola Italiana di TI.

La soluzione multitenant permette di istanziare per ogni azienda un suo “contenitore sw”, anche detto tenant, dove vengono salvati i dati dei device aziendali (no DDT, sensibili o giudiziari), le configurazioni delle policy amministrative create,...

E' possibile accederci attraverso una console amministrativa utilizzando uno qualunque dei browser di mercato disponibili (vedere capitolo amministrazione) ed un account dedicato.

Dunque, su un'unica infrastruttura fisica sono istanziabili centinaia di tenant (clienti) fino a saturare il numero massimo di device supportati da una installazione AirWatch (100.000) e comunque scalabile.

4.5 Backup e restore

La piattaforma AirWatch è gestita con backup giornalieri incrementali e full settimanali dei dati presenti sia di tipo sistemistico, applicativo e di db.

In caso di fault è previsto il restore sui sistemi danneggiati.

5 Modello funzionale e gestionale

Il modello funzionale si basa sulla necessità di servizio espressa dai clienti TI di gestire il lifecycle della flotta di dispositivi mobili dei cliente. Pertanto il servizio di Device Management su AirWatch nasce sulla base delle esigenze espresse dai clienti di poter gestire il parco di dispositivi mobili di cui è dotata la propria azienda e sui quali potranno, per esempio, essere installate le applicazioni a supporto delle attività aziendali, predisponendo una infrastruttura in SaaS, basata su AirWatch, in Nuvola Italiana.

La piattaforma è stata dimensionata per garantire il servizio fino ad almeno 100.000 device, multitenant.

Il servizio è installato in Nuvola Italiana presso il Datacenter TI di Pomezia.

AirWatch fornisce strumenti di nuova generazione per la gestione, il monitoring e l'amministrazione di dispositivi mobili quali smartphone e tablet ed eroga tutte le funzionalità necessarie alla distribuzione di applicazioni, alla configurazione dei dispositivi, alla gestione dell'inventario hardware e software, alla messa in sicurezza dei dati e dei dispositivi (configurazione delle policy di sicurezza aziendali, identificazione degli utenti in rete, lock dei dispositivi, distruzione dei dati sui dispositivi rubati).

Le attività di Device Management possono essere eseguite in modo "silente" e trasparente all'utente, in modo tale che non possa avere impatti sulle attività di business dell'utente. E' inoltre possibile schedulare tali attività con cadenza periodica o innescarle a fronte di eventi particolari.

La struttura IT dei clienti hanno accesso alla console web di amministrazione di AirWatch attraverso il link <https://mdm-aw.nuvolaitaliana.it/>

6 Modello configurativo di AirWatch

Prima di addentrarci nella descrizione delle funzionalità erogate dal servizio MDM con AirWatch , è utile avere un overview sul modello di gestione del terminale.

Fondamentalmente dobbiamo considerare il processo di gestione di un terminale suddiviso in due fasi principali.

La prima fase è quella che indichiamo come Enrollment del device ovvero Registrazione in piattaforma del device utente.

Per poter rendere operativa questa fase , come si vedrà nel capitolo 7, si devono seguire i primi tre passi come pre requisiti alla fase successiva di registrazione:

1. Configurazione dell'organization group(tenant)
2. Definizione degli account amministrativi ed utenti
3. Definizione degli users group (se integrato con LDAP aziendale) o child organization group
4. Configurazione dei profili, settings di enrollment e del gruppo
5. installazione del client AW sul device

La seconda fase , una volta registrato il device in piattaforma nel tenant del cliente, è quella di impostare e rendere operative le varie policy di tipo configurativo ed applicativo per poter modificare

il settings del device, assicurare restrizione all'uso o protezioni all'accesso o ai dati, gestire sw distribution (Apps android e iOS),..

La prima volta che l'utente admin entra nel proprio tenant gli verrà proposto l'accettazione dei termini d'uso e il setting del suo profilo con la configurazione di un PIN di sicurezza che sarà poi utilizzato per accedere a profili e dati di configurazione sensibili al funzionamento del sistema.

7 Enrollment terminali cliente

7.1 Organization Group (Tenant)

Il tenant o organization group rappresenta l'istanza applicativa con cui Airwatch definisce il perimetro all'interno del quale vengono salvati i dati, i parametri, le configurazioni dei device che l'amministratore della company decide di registrare, delle policy create, dei log raccolti,

Ad un livello superiore è definito il system_tenant o root organization, il quale contiene tutti i tenant e le relative configurazioni (vedi Figura 7-1) create.

Ovvero il system_tenant può accedere a tutti i tenant mentre il singolo tenant vede solo le sue configurazioni.

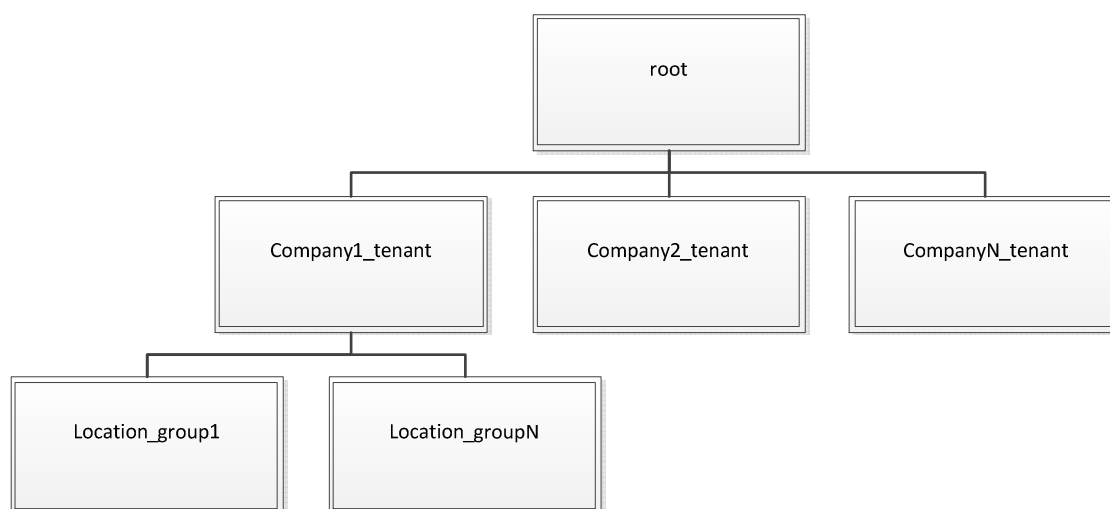


Figura 7-1

L'organization group (tenant) verrà configurato come “customer” in Configuration ► Organization Groups.

Un esempio di organization group può essere

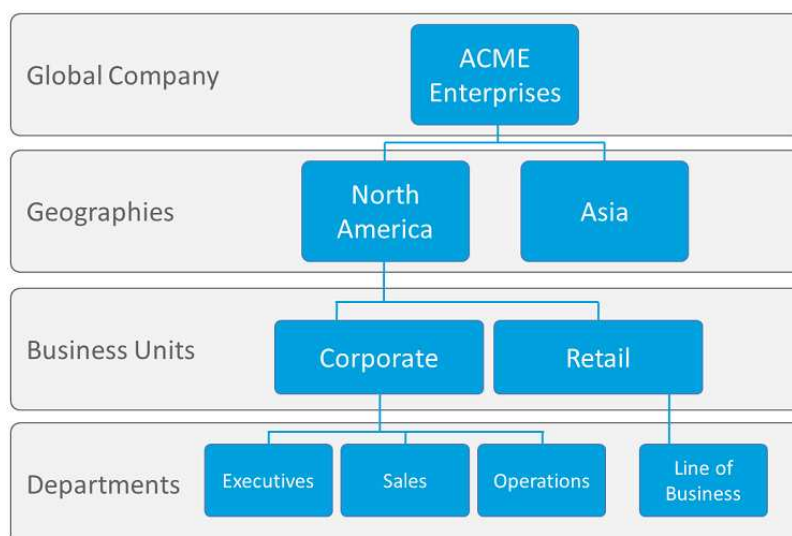


Figura 7-2

L'admin del tenant può creare anche dei child organization group a cui assegna nella configurazione una user e pwd di accesso con un profilo a scelta in base alle esigenze di accesso dell'utente a cui sarà delegato l'amministrazione del sotto gruppo.

7.1.1 Creazione account

In Airwatch il metodo di autenticazione utilizzato dal prodotto è di tipo applicativo.

Dunque verrà configurato uno username/password associato al tenant che servirà al cliente per accedere in console web alle configurazioni delle loro policy.

Ci sono dei profili base predefiniti che si possono utilizzare quando si sta creando un utente amministratore. Questi sono:

- **System Administrator :** profile utilizzato per la gestione della piattaforma. Ha accesso ha tutti le configurazioni e funzionalità. Viene assegnato al superadmin di esercizio
- **AirWatch Administrator :** viene utilizzato per configurare utenti admin di tenant.
- **Read Only :** definisce utenti che possono accedere alla console amministrativa ma in sola lettura
- **Report Viewer :** mette a disposizione solo funzionalità di reporting

Come abbiamo anticipato ci sono , oltre ad account amministrativi, anche quelli per i singoli utenti utilizzabili poi per esempio nella fase di enrollment di un dispositivo.

Dunque una volta definito l'organization group con le sue impostazioni, i relativi utenti amministrativi vediamo come definire un end-user che sarà associato nella fase di enrollment ai propri device

In questo caso sono definibili utenti associati ai diversi livelli dell'organization gruppo con proprie user/pwd che ereditano le configurazioni imposte a quel livello di gerarchia da Accounts ► Users ► List View ► Add

Se si vuole ottimizzare le configurazioni, profili,...definiti per più utenti allora si possono creare degli users group da : Accounts ► Users ► User Groups ► Add (Solo nel caso si è integrati con un AD/LDAP service) se no Accounts ► Users ► Users ► Add

La password in generale dovrà essere configurata secondo questo standard

1. Devono essere composte almeno da 8 caratteri
2. Devono contenere caratteri appartenenti a tre delle quattro categorie seguenti:
3. Lettere maiuscole (da A a Z)
4. Lettere minuscole (da a a z)
5. I primi 10 numeri di base (da 0 a 9)
6. Caratteri non alfabetici (ad esempio, !, \$, #, %)

7.1.2 Configurazione Tenant

Dunque quando è acquisito un nuovo cliente gli viene configurato un nuovo tenant, un Organization Group di tipo Customer, con uno o più account. Per effettuare la configurazione del tenant si deve inizialmente considerare:

1. I child organization groups: definiscono la gerarchia aziendale organizzativa in cui collocare profili e device, la cui root è rappresentata dall'organization group
2. Le admin accounts : sono le credenziali degli amministratori del tenant
3. Le user accounts: sono le credenziali dei singoli utenti dei device sotto mdm

Ogni tenant è acceduto attraverso una web console ed un account dedicato.

Quando l'amministratore vorrà accedere al sito utilizzerà un browser di mercato , un link (<https://mdm-aw.nuvolaitaliana.it/>) e gli account sopradetti.

Al primo login alla console di amministrazione Airwatch, si deve definire un PIN a quattro cifre. Una volta definito questo PIN si potrà proseguire con le successive operazioni di configurazione. Il PIN

rappresenta un secondo livello di sicurezza che protegge in diversi ambiti come per esempio ad evitare wipe o delete accidentali, ...

Le funzionalità sulle quali il PIN può essere attivato sono in :

Configuration ► System Configuration ► System ► Security ► Restricted Actions.

- | Admin Account Delete
- | APNS Certificate Clear
- | Application
- | Delete/Deactivate/Retire
- | Content Delete/Deactivate
- | Data Encryption Toggle
- | Device Delete
- | Device Wipe
- | Enterprise Wipe
- | Organization Group Delete
- | Profile Delete/Deactivate
- | Provisioning Product Delete
- | Revoke Certificate
- | User Account Delete

Successivamente è necessario definire il restante setting del tenant (device enrollment/authentication, term of use, branding, apns certificate,...)

Possiamo pensare che dopo le configurazioni descritte si abbia un ambiente così generalmente schematizzabile:

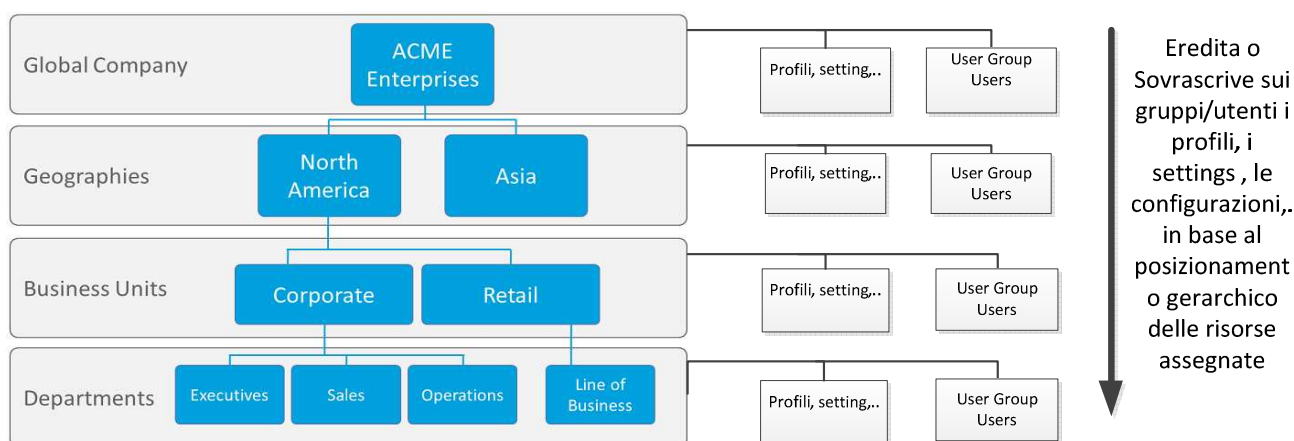


Figura 7-3

La particolarità di Airwatch è la sua impostazione a mo' di directory service dove all'interno della gerarchia definita si assegnano delle risorse: gruppi, utenti, profili, device,...vige il meccanismo della ereditarietà o della sovrascrittura verso le parti terminali della gerarchia.

7.1.3 Privacy Settings

In questa sezione Configuration ► **System Configuration** ► **System** ► Telecom ► **General** ► **Privacy** configuriamo la possibilità o meno di abilitare il collezionamento dei dati TEM e GPS

7.2 Installazione APNS (Apple Push Notification Service) certificate

Le operazioni sui device Apple (iOS) sono stimulate da parte dell'amministrazione del servizio attraverso dei push sul device eseguiti dalla web console di piattaforma. Per esempio per poter applicare una nuova policy. Il push non è diretto sul device ma viene intermediato dal Apple Push Notification Service.

La piattaforma per poter usufruire di questo servizio Apple, unico modo per prendere contatti dalla piattaforma con il device attraverso il client AirWatch installato a bordo del device, deve aver installato un certificato APNS generato su Apple.

La generazione del certificato prevede l'uso di un wizard di navigazione attivabile da Configuration ► System Configuration ► Device&Users ► Apple ► APNs for MDM

Si deve avere come pre requisito:

1. Web browser : Safari o Mozilla Firefox
2. Un Apple ID

La procedura di generazione del certificato è:

Se usi il Getting Started Wizard :in System Configuration ► System ► Getting Started (il wizard si attiva solo con un organization group di tipo Customer)

Seleziona Yes del radio button nella sezione Apple MDM. Scegli l'opzione nuovo certificate apns

1. Download the linked Certificate Request file (MDM_APNsRequest.plist).
2. Vai al portale di Apple Push Certificates Portal , accedi con il tuo Apple ID and password
3. Seleziona un **Create a Certificate e accetta** Apple's EULA.

4. Seleziona **Choose File sotto** Create a New Push Certificate e seleziona il file CSR generato nel precedente Step. Una volta il CSR è uploaded, avrai un nuovo APNs Certificate. Seleziona **Download per salvare sul tuo pc il signed certificate**. Il signed certificate deve essere salvato come **.pem** file.
5. Rinvia alla pagina Airwatch e upload the signed certificate (.pem file) che hai scaricato dal Apple website.
6. Inserisci l'Apple ID usato per la generazione del certificate. Servirà per i futuri rinnovi del APNs certificate.
7. Click **Next e salva** the updated APNs settings. Ora si può procedere con la gestione dei device ios

L'APNs Certificate scade dopo un anno e deve essere rinnovato se non fallisce la comunicazione tra Airwatch e i device Apple con la conseguenza di dover eseguire un nuovo enrollment.

Per rinnovarlo esegui la stessa procedura partendo da

Device & Users ► Apple ► APNs for MDM.

Seleziona **Renew** option ed esegui il download del file .plist

7.3 Servizio Android Push

Airwatch gestisce per i device Android diversi metodi di push. Ha una sua funzionalità specifica, AirWatch Cloud Messaging (AWCM), di notifica verso i device che si sostituisce al GCM. Questo consente di abilitare un numero maggiore di funzionalità legati alle notifiche push.

Quando si gestiscono i device Android è possibile, in alternativa al SMS, utilizzare il servizio push per la notifica degli aggiornamenti al device da parte dell'amministratore aziendale del servizio.

Il servizio funziona con una connessione di rete IP che può essere su rete mobile (GSM, UMTS,...) o rete locale Wi-Fi

Il concetto è uguale a quello di Apple. Per prendere contatti con il device la piattaforma deve eseguire un push su AWCM dove è registrato il device al servizio.

7.4 Enrollment dei terminali

Con enrollment dei terminali intendiamo la fase di registrazione di un client Airwatch precedentemente installato su uno dei device supportati.

I sistemi operativi supportati sono : iOS, Android, Windows Mobile (fino alla 6.5), Windows, Blackberry, Windowsphone 8,...

E' possibile definire diverse modalità di enrollment in funzione delle proprie esigenze di servizio e di sicurezza.

Prima di procedere con l'enrollment è necessario creare dei gruppi di utenti e gli account all'interno della organizzazione definita ed eventualmente dei profili , delle policy configurativa o applicative. Inoltre si consiglia di definire al meglio il setting dell'agent in piattaforma. Per esempio in Android vai in Configuration ► System Configuration ► Devices & Users ► Android ► Agent Settings

L'utente riceve nella notifica di enrollment un link (<https://www.awagent.com/Home/Welcome>), in uno processo di enrollment standard, con il quale accede al sito AWAgent.com. Questo sito esegue una verifica del sistema operativo del device e se l'agent AW è già installato. infine ridirige la chiamata http sullo store pubblico appropriato al sistema operativo . Sempre nella mail di notifica riceve il Gruppo ID lo user e password. Successivamente viene trasmessa una seconda mail di approvazione al servizio.

Di seguito le principali modalità di enrollment (al momento non è operativa la prima modalità in auto-discover):

1. **Auto-discover** : in questo caso l'utente inserirà il suo indirizzo email che è stato precedentemente configurato in piattaforma dall'amministratore insieme al dominio di posta e validato dall'utente attraverso la ricezione di un link di conferma. Per quanto riguarda la modalità di auto-discovery si deve accedere a Configuration ► System Configuration ► Devices & Users ► General ► Enrollment and select Add Email Domain ed aggiungere il proprio/i domini di posta e l'indirizzo email
2. **Notification-Prompt Enrollment** – L'utente riceve una seconda notifica via email con una URL di Enrollment, il Group ID , dove sono definite le policy assegnate all'utente, e le credenziali di autenticazione. Come l'utente, inserisce i dati richiesti ed accetta le condizioni d'uso automaticamente il device si collega alla piattaforma , si autentica e scarica il setting , le app, ...che l'amministratore ha precedentemente configurato.

3. **Single-Click Enrollment** – L'amministratore invia una notifica con una URL di enrollment a cui è associato un token. L'utente utilizzerà questo link per collegare il device, autenticarlo ed eseguire le fasi di enrollment previste. Questo token è reso più sicuro impostando un expiration times
 - a. Abilita il token : in Configuration ► System Configuration ► Devices & Users ► General ► Enrollment in Autanthication e seleziona *Registered Device Only* e *Require Registration Token*
 - b. Crea il messaggio email : in Configuration ► System Configuration ► Devices & Users ► General ► Message Templates
 - c. Invia il messaggio con il link di enrollment :
4. **Dual-Factor Authentication** – L'amministratore invia una notifica con una URL di enrollment a cui è associato un token e le credenziali di login dell'utente. In questo modo si rende più sicuro l'accesso alla piattaforma per eseguire l'enrollment del device utente.
 - a. Si esegue la stessa procedura del punto precedente tenendo presente che al punto a si deve settare l'opzione Token Enrollment Type a two-factor

Nei paragrafi successivi si descriverà la policy di enrollment per singolo sistema operativo compatibile con Airwatch

7.4.1 Android

La registrazione dei device Android si realizza secondo quanto definito nel par. 7.4

Nel caso di device samsung che supportano le funzionalità SAFE la procedura di enrollment dell'agent, precedentemente installato, prevede l'installazione anche di una componente software aggiuntiva. Questa verrà richiesta in automatico durante l'enrollment , dopo la conclusione dell'installazione dell'agent.

Alcune raccomandazioni. Sul device prima di iniziare l'enrollment assicurarsi che sul device:

1. sia stato già eseguito l'accesso con l'account google per abilitare il download dell'agent dal play store
2. configurare in on il flag Allow Non-Market Applications
3. attivare le proprietà di device administrator quando richiesto

Nel caso si vuole gestire un device Knox è necessario abilitare in Configuration ► System Configuration ► Devices & Users ► Android ► Agent Settings il parametro *Enable Containers*

7.4.2 Apple

La registrazione dei device iOS si realizza secondo quanto definito nel par. 7.4.

Si ricorda che la gestione della comunicazione tra la piattaforma ed i device avviene tramite il sistema di push notification APNS. Per abilitare questa comunicazione è necessario generare un certificato APNS da installare nel tenant della azienda. (vedi par. 7.2) . Per fare ciò il cliente deve dotarsi di un proprio Apple ID e password.

Durante la fase di enrollment , si dovrà accedere all'apple store, per scaricare ed installare l'agent. Per tale motivo ogni utente deve dotarsi di un suo apple id e pwd che utilizzerà nel momento del setup del device, se non c'è l'ha gli viene chiesto dal s.o. apple.

7.4.3 Win Phone 8

La registrazione di device wp8 prevede alcuni pre requisiti che devono essere soddisfatti per poter poi procedere con l'enrollment se si vuole fruire a pieno di tutte le funzionalità mdm.

Questi sono :

1. Il cliente deve acquistare un windows account id. E' una licenza che abilita l'azienda ad utilizzare il Windows Phone Development Center e pertanto a distribuire app sui propri device
2. Symantec Certificate : con la licenza viene fornito da MS questo certificato che verrà utilizzato per due scopi:
 - a. Serve per firmare il client mdm airwatch (.xap)
 - b. Serve per generare l'application enterprise token AET (.aetx) che verrà utilizzato per essere caricato nel tenant aziendale airwatch e così abilitare la sw distribution via mdm in
Configuration ► System Configuration ► Devices & Users ► Windows ► Windows Phone 8
► Agent Settings ed abilitare Enterprise App Management caricando il token
3. Scaricare l'agent airwatch .xap
4. Le credenziali di accesso alla web console amministrativa
5. La url di accesso al tenant
6. Il Gruppo ID

La procedura di enrollment prevede in generale due possibilità:

1. Senza agent airwatch : si utilizza solo app company wp8 dove vengono configurati i campi email, dominio, user e pwd con il server airwatch. In questo caso si hanno solo le funzionalità base (wipe, security settings e email)
2. Con agent aw : in questo caso sul device va configurato anche il campo Install company app or Hub. Una volta attivato l'account si deve procedere ad installare l'agent opportunamente firmato con il certificato windows. Solo a questo punto il device è pienamente sotto mdm. Se l'installazione viene fatta entro i 10 min dell'attivazione dell'account non vengono richieste le credenziali di accesso

7.4.4 Black Barry

Per procedere con l'enrollment di un BB 10 si devono avere :

1. AirWatch v6.5 richiede un agent con versione minima 1.2.
2. | AirWatch Admin Console Credentials – Le credenziali di accesso alla web console
3. | BlackBerry ID – La username e pwd per accedere al BB AppWorld per installare l'agent AW.
4. | Enrollment URL – Questa URL è quella definita per il tuo tenant in AirWatch Admin Console.
5. | Group ID – Dove sono associati i device, regole, profili della company definiti nella AirWatch Admin Console.

Dopo di che si possono seguire due procedure di enrollment . La prima è quella con l'auto-discovery usando il dominio di mail ed una mail di conferma con la quale l'utente sottoscrive ed accetta il processo di registrazione.

La seconda prevede l'installazione dell'agent AW dal sito BB AppWorld , lanciando il client utilizzando le opzioni di enroll device : enrollment url e group id. Successivamente si deve inserire la user e pwd di admin console e seleziona il tipo di device. In conclusione bisogna settare l'accettazione d'uso del sw e così si conclude la fase di enrollment

7.4.5 Migrazione terminali

Se abbiamo una installazione di un cliente su una versione antecedente all'ultima supportata è possibile eseguire l'upgrade sw di prodotto senza dover effettuare una nuova registrazione del device.

Nel caso invece che dobbiamo procedere ad un cambio di piattaforma o il device non è stato correttamente registrato è necessario provvedere ad una nuova fase di registrazione del device. Si procederà dunque a creare una nuova policy di enrollment o ad utilizzare la precedente policy rieseguendo dal client il processo di registrazione.

8 Funzionalità

8.1 Package e file distribution

Nella distribuzione delle app in AW è necessario pubblicare l'Enterprise App Catalog andando in Configuration ► System Configuration ► Apps ► Catalog ► General. AW infatti organizza tutte le tue app in un *app catalog* utilizzato dall'agent sul device per permettere all'utente finale di vedere , installare, le app che gli sono state sottomesse dall'admin mdm.

Con AW la configurazione di profili per la distribuzione di app pubbliche richiede l'uso della funzionalità di *search* per trovare le app nei diversi store pubblici.

Nel caso di play store di Google è necessario eseguire un'integrazione per attivare il *search* andando in Configuration ► System Configuration ► Device & Users ► Android ► Google Play Integration. Qui si deve configurare : un account google (username e pwd) ed un Android ID che si estrae dal proprio device utilizzando una apposita app presente nel play store.

Si possono definire degli *smart group*, appartenenti a specifici child organization group, dove inserire solo un insieme selezionato di users verso cui distribuire le app andando in Catalog ► Applications ► Configuration ► Smart Groups.

8.1.1 Android

8.1.1.1 Market

Il device deve avere un account con Google Play

Con la piattaforma AW è possibile pubblicare un'app presente sul Market pubblico utilizzando la funzionalità di *search*. In questo modo si abilita oltre la pubblicazione anche il push da web console, la distribuzione attraverso l'agent AW,... Come detto prima è necessario effettuare la configurazione del search app per google store.

Una volta selezionata l'app si verrà ridiretti nella pagina *add application*. La maggior parte dei campi sono pre popolati dalle informazioni contenute nell'app. Altre si possono inserire direttamente come : commento, rating, categoria. Successivamente sempre nel tab *add application* bisogna configurare il gruppo di appartenenza, la modalità di installazione (automatico o manuale), se rimuovere l'app dopo un unenrollment, si può disabilitare il backup verso gli iCloud. In conclusione cliccare su *save*.

8.1.1.2 Internal

Con la piattaforma AW è possibile pubblicare App Enterprise nella sezione del client.

I device devono permettere l'installazione da unknown sources

Una volta che si ha l'app internal .apk sul proprio pc eseguire l'upload in piattaforma nel proprio organization group o tenant.

Perciò vai in Catalog ► Application ► Internal ed esegui *add application*

In questo tab si definiscono tutta una serie di informazioni necessarie al deploy applicativo come : version, rating, name, application id, una descrizione, un immagine come icona dell'app, ...
Altri andranno configurati come : l'assegnazione dell'app ad un gruppo (smart group), la modalità di installazione (automatico o manuale)...Dopo di che fai *save*.

8.1.2 Apple

Con Apple si può impostare anche una distribuzione delle app seguendo un Apple Volume Purchase Program (VPP). Utilizzando il relativo redemption codes si gestisce il proprio parco licenze nella fase di distribuzione di app pubbliche o private

8.1.2.1 Market

Lo user deve avere un account con Apple id configurato

Con la piattaforma AW è possibile pubblicare un'app presente sul Market pubblico utilizzando la funzionalità di *search*. In questo modo si abilita oltre la pubblicazione anche il push da web console, la distribuzione attraverso l'agent AW,...

Una volta selezionata l'app si verrà ridiretti nella pagina *add application*. La maggior parte dei campi sono pre popolati dalle informazioni contenute nell'app. Altre si possono inserire direttamente come : commento, rating, categoria. Successivamente sempre nel tab *add application* bisogna configurare il gruppo di appartenenza, la modalità di installazione (automatico o manuale), se rimuovere l'app dopo un unenrollment, si può disabilitare il backup verso l' iCloud. In conclusione cliccare su *save*.

8.1.2.2 Internal

L'utente ha compilato la propria app (.ipa) firmata con il suo certificato developer acquistato da Apple e deve generare il relativo provisioning file. La durata del certificato al massimo è di tre anni. Ogni anno però il provisioning file scade e deve essere rinnovato. Via AW non è necessario prevedere una nuova installazione ma solo l'aggiornamento del nuovo provisioning file.

Per caricare sul proprio tenant l'app andare in Catalog ► Applications ► Internal ► Add Application

In questo tab si definiscono tutta una serie di informazioni necessarie al deploy applicativo come : version, rating, name, application id, una descrizione, un immagine come icona dell'app, ...
Altri andranno configurati come : l'assegnazione dell'app ad un gruppo (smart group), la modalità di installazione (automatico o manuale)...Dopo di che fai *save*.

8.2 Security

In questo capitolo analizziamo le funzionalità di sicurezza sulla protezione dei dati, delle comunicazioni, dell'accesso autenticato,... dal punto di vista del device utente.

Gli approfondimenti saranno attuati focalizzando le specificità per singolo sistema operativo dei device supportati da Airwatch

8.2.1 Android

8.2.1.1 Gestione Device password

Sui device Android è possibile abilitare via profile) la richiesta di password per accedere alle funzionalità del device.

Si possono definire una vasta gamma di proprietà della password in modo da poterla rendere conforme alle proprie policy aziendali.

Per esempio è possibile definirne il formato (alfabetico, numerico o alfanumerico), lunghezza minima, il numero di volte che si può digitarla prima di avere il lock, abilitare un history password , una expiration data,...

General

Passcode

Restrictions

Wi-Fi

VPN

Email

Exchange ActiveSync

LDAP

CalDAV

Subscribed Calendars

CardDAV

Web Clips

Credentials

SCEP

Global HTTP Proxy

Single App Mode

Advanced

Custom Settings

Passcode

Require passcode on device

Allow simple value

This field cannot contain spaces or special characters. A single alphanumeric string is required.

Minimum passcode length

6

Minimum number of complex characters

2

Maximum passcode age (days)

30

Auto-Lock (min)

5

Passcode history

3

Grace period for device lock (min)

5 Minutes

Maximum Number of Failed Attempts

11

Save

Save & Publish

Cancel

8.2.1.2 Gestione blocco device

L'amministratore del servizio per esigenze di sicurezza dovute a furto, perdita,...del device può, per assicurare il suo controllo e la protezione del device contro terzi non autorizzati, eseguire delle operazioni di lock, wipe data e wipe enterprise , clear password, dalla sua amministrazione web.

La notifica operativa inviata è silente per l'utente ed attiva il client via AirWatch Cloud Messaging (AWCM)..

Quando si decide per il wipe data si esegue sul device remoto il reset alle condizioni di fabbrica incluso la cancellazione del client Airwatch.

Mentre con il wipe enterprise si intende la cancellazione di dati applicativi airwatch.

Con il lock il device rimane inaccessibile fino a quando non viene inserita la password corretta. Un'azione di reset o cambio batteria non rimuove il lock impostato.

8.2.1.3 Utilizzo di Black/White list : Samsung,

Sui dispositivi Samsung la creazione di blacklist e whitelist di applicazioni è possibile sia per le App pubbliche (Google Play,) che enterprise: .apk (file di installazione diretto),.

Nel caso di blacklist le app che sono riportate nell'elenco non sono installabili viceversa con le whitelist vengono installate solo quelle indicate. E' possibile definire anche le app che vogliamo disinstallare

8.2.1.4 Restrictions all'uso del device : Samsung

Sui device Samsung è possibile impostare delle configurazioni di restrizione e/o abilitazioni di alcune funzionalità.

Le principali sono : l'uso del market place Google Play, della foto camera, dell'interfaccia Bluetooth, WI-FI, della copia dei contatti su un sito web sicuro, del cambio dei settings del device,...

8.2.1.5 Disabilitazione camera :

Da Android 4.x ed oltre è possibile richiedere via policy di Configuration la disabilitazione della camera digitale.

8.2.1.6 Encryption dati :

E' possibile richiedere l'encryption dei dati sulla device memory interna come su quella esterna SD

8.2.1.7 Firewall

Con Airwatch è possibile predisporre l'installazione di un web browser AW con il quale si gestisce, in combinazione eventualmente di un profilo di blocco del browser installato, delle policy restrittive relative all'uso del web. Per esempio si possono così impostare delle white/blacklist di url di navigazione, un proxy con cui accedere ad internet,

8.2.2 iOS

8.2.2.1 Gestione del JailBreak

Come sappiamo i device ios sono sottoposti da Apple a stringenti policy di sicurezza.

Le apps sono organizzate all'interno di "contenitori" (sandbox) entro i quali l'app può agire nel suo normale funzionamento. Inoltre per poter pubblicare una propria app sull'apple store bisogna passare una rigorosa verifica del sw da parte di Apple

Nell'ambito di queste restrizioni sono nati diversi tool che permettono di effettuare JailBreak del device, in genere individuando la pwd di root del device, per poter così accedere a tutte le risorse senza nessun confinamento.

MDM AW con l'uso dei suoi client permette di attivare una serie di controlli per individuare se il device è stato jailbroken.

8.2.2.2 Gestione blocco device

L'amministratore del servizio per esigenze di sicurezza dovute a furto, perdita,...del device può, per assicurare il suo controllo e la protezione del device contro terzi non autorizzati, eseguire delle operazioni di wipe, lock dalla sua amministrazione web.

La notifica silente per l'utente attiva il client via APNS.

Quando si decide per il device wipe si esegue il reset del device remoto anche dal management di AW. Per ristabilire le funzionalità è necessario rieseguire un nuovo enrollment ad. Invece se si utilizza il wipe enterprise verranno cancellate tutte le configurazioni AW.

Col il lock il device rimane inaccessibile fino a quando non viene inserita la password corretta. E' possibile impostare anche un unlock e clear della passcode e rimuovere così centralmente la necessità di sbloccare il device con la password. Se la password è stata impostata attraverso delle policy di AW verrà richiesta una nuova password.

8.2.2.3 Gestione Device password

Sui device iOS è possibile abilitare via profile (Configuration) la richiesta di password per accedere alle funzionalità del device.

Si possono definire una vasta gamma di proprietà della password in modo da poterla rendere conforme alle proprie policy aziendali.

Per esempio è possibile definirne il formato (alfabetico, numerico o alfanumerico), lunghezza minima, il numero di volte che si può digitarla prima di avere il lock, history passcode (fino a 50 passcode), ...

8.2.2.4 Restrizioni all'uso del device

E' possibile, sempre via una policy configuration, abilitare o disabilitare una serie di funzionalità del device. Le principali sono: installare le apps, uso della fotocamera, il sync automatico quando si è in roaming, acquisto di app, multiplayer game,...

Ma si può estendere questi settings anche a livello applicativo o di backup iCloud

Per esempio sul livello applicativo si può: permettere o no l'uso di Youtube, iTunes store, Safari. Si può impedire l'accesso al iCloud per eseguire backup, sync, photo stream

Come abilita il controllo per rating di contenuti TV, Apps, Video

8.2.2.1 Encryption dati :

Con il setting della passcode si fornisce anche un encryption hw del device. In più si può abilitare l'encryption dei dati

8.2.2.1 Firewall

Con Airwatch è possibile predisporre l'installazione di un web browser AW con il quale si gestisce, in combinazione eventualmente di un profilo di blocco del browser installato, delle policy restrittive relative all'uso del web. Per esempio si possono così impostare delle white/blacklist di url di navigazione, un proxy con cui accedere ad internet,

In più, se si ha un Supervised iOS 7 devices (questo si attiva attraverso l'uso dell'Apple configurator) , in alternativa possiamo usare Safari configurando un Web Content Filter payload con delle black/white list di url che riteniamo bloccare od abilitare sul browser Safari.

8.3 Inventory

Per accedere alle informazioni di inventory dei propri device registrati si può procedere così:

HUB ► Device ► Android e cliccando sul device di interesse si apre una vista sulle informazioni hw, sw ,... del terminale selezionato

Possiamo arrivare alla stessa vista passando per Accounts ► Users ► User di interesse ► Device di interesse. In questa vista possiamo accedere anche a comandi di gestione del device come il wipe, lock,...

Invece se accediamo via Dashboard vedremo il nostro device con una veste grafica diversa che riporta in altro ordine le informazioni di inventory e comandi di gestione

Quando si registra un device viene memorizzato una serie di dati del device come model, OS, serial number, UDID e asset number. Questo consiste nel avere censito a livello amministrativo AW informazioni di tipo HW (processore, scheda di memoria,...) , SW (sw installato,..) del device registrato.

Si possono poi vedere queste informazioni nella pagina amministrativa dedicata ai device registrati nel tenant utente.

C'è da osservare che per motivi legati alle singole particolarità costruttive dei device, le informazioni HW che si possono prelevare non sono standardizzabili.
Per esempio, non tutti i device Android rilasciano il numero seriale (in qual caso verrebbe sostituito da AirWatch con l'IMEI (International Mobile Equipment Identity) o con il MEID (Mobile Equipment Identifier).

Così vale per il numero telefonico, le caratteristiche e lo stato del WI-FI o del Bluetooth.

8.4 Device Configuration.

Oltre alle già citate possibilità di configurazione dei device applicate per ragioni di sicurezza , applicative e di collazionamento dei dati hw e sw, è possibile estendere la gestione del settings del device anche su specifiche funzionalità. Tra queste le più importanti sono senz'altro quelle di connessione, posta elettronica e contatti.

8.4.1 Android

8.4.1.1 Connessioni

Su Android è possibile abilitare o meno la disponibilità di connessioni *Bluetooth*, *WI-FI*.

Sono configurabili i parametri di connessione del WI-FI come il SSID o di sicurezza della comunicazione (WEP, WPA,...)

8.4.1.2 Posta elettronica

Ci sono diverse modalità di configurazione del servizio di posta elettronica anche in funzione del particolare device.

Sul sistema operativo Android è configurabile un client che utilizza come server Exchange (Activesync).

Per altri device come il Samsung si può configurare un normale client con protocollo pop/imap e il server SMTP.

8.4.2 Apple,

Su iOS c'è una maggiore estensione nella possibilità di configurazione del device.

E' possibile oltre le particolari policy di sicurezza , applicative ed inventory si può settare i parametri di configurazione di posta elettronica, contatti e calendario..

8.4.2.1 Connessioni

E' possibile abilitare connessioni WI-FI con i relativi parametri di sicurezza (WEP, WPA) , VPN.

Si può settare il roaming voce e dati

8.4.2.2 Posta elettronica

Per la posta elettronica è possibile configurare sia l'uso di client pop/imap che sessioni con Exchange (Activesync)

8.5 Amministrazione

L'amministrazione del servizio viene gestito da parte del cliente attraverso una console di amministrazione performante e compatibile con tutti i principali browser presenti sul mercato che riportiamo di seguito:

- Internet Explorer 8+ |
- Google Chrome 11+
- | Firefox 3.x+

! Safari 5.x L'home page del portale Nuvola It Airwatch è raggiungibile dal sito

<https://mdm-aw.nuvolaitaliana.it/>

La home page è così strutturata:

In testa al menù si può accedere alle seguenti funzionalità:

! **Global Search** – Ricerca su tutti gli aspetti del tuo ambiente AirWatch (devices, users, content, applications, configuration settings ed altro)

! **Getting Started** – Sono dei wizard per avviare in forma guidata il setup del proprio ambiente MDM

! **Add** – Accedi alla pagina di configurazione di un nuovo admin, device, user, compliance policy, content, profile, internal application or public application.

! **Saved** – Accedi alle tue funzionalità più utilizzate con AirWatch Admin Console.

! **Account** – Vedi le tue informazioni di account. Puoi modificare le impostazioni che hai assegnato (roles) al tuo ambiente mdm. Includendo contact information, AirWatch Admin Console settings and preferences and login history. Puoi eseguire il Log out da AirWatch Admin Console

! **Help** – help online alla documentazione.

! **Home** – Ritorna alla home page

! **Save** – Salva le modifiche eseguite nella pagina corrente

In più a sinistra della home page puoi accedere ad un menu per un accesso veloce alle seguenti funzionalità:

Hub – Vedi e configure le informazioni di interesse sull'uso del servizio MDM come :le principali blacklist apps che hanno violato le regole di compliance, tutti i devices c he sono fuori compliance, etc. Alerts, reports and events related to devices, the AirWatch Admin Console and the Syslog.

Devices – Accedi alla Device Dashboard per una dettagliata descrizione dei tuoi device registrati.

Accounts – Gestisci Users and Administrators del tuo tenant MDM.

Apps & Books – Accedi e gestisci il tuo catalogo applicativo e il Volume Purchase Program (VPP) orders. Anche puoi vedere le statistiche ed i logs ed ancora le configurazioni applicative delle tue apps.

Content – Gestisci e carica il contenuto relative agli utenti e device del tenant

Email – Accedi all'Email Dashboard



Telecom – Visualizza e gestisce, se attivo le funzionalità di tracking dei dati telecom (call, SMS, etc)

Groups & Settings – Gestisce : Organization Groups, Smart Groups, App Groups, User Groups and Admin Groups. Configura system settings o access settings relative alle opzioni del menu principale.

Cliccando sul bottone a freccia di sinistra si attiva o disattiva questo