TECHN 38

Periodieke publicatie van Smals

April 2014

Mobile Device Management

Tools voor het beheer van smartphones en tablets

Bert Vanhalst is licentiaat Informatica. Sinds november 2001 is hij werkzaam als consultant bij de sectie Onderzoek van Smals. Hij werkte mee aan de invoering van webservices en service-georiënteerde architectuur en is momenteel gespecialiseerd in mobiele toepassingen, in het bijzonder de beheers- en veiligheidsaspecten.

Contact: 02 787 48 02

bert.vanhalst@smals.be

1. Inleiding

Mobiele toestellen zijn al enkele jaren bezig aan een stevige opmars, zowel smartphones als tablets zijn razend populair geworden. Dat biedt uiteraard opportuniteiten om die toestellen ook te gebruiken in een bedrijfscontext, om op een meer flexibele manier toegang te krijgen tot bedrijfstoepassingen en informatie.

Uiteraard willen we als organisatie niet dat de sluizen hiermee breed opengezet worden en bedrijfsgegevens te grabbel worden gegooid. We willen mobiele gebruikers wel toegang geven tot bepaalde gegevens, maar dan op een veilige, gecontroleerde manier.

Enerzijds kan een organisatie zelf mobiele toestellen ter beschikking stellen van de werknemers. Anderzijds hebben veel medewerkers al een degelijke, recente smartphone of tablet en willen ze die ook gebruiken in de context van de organisatie. Men spreekt dan van Bring Your Own Device (BYOD[1]).

In beide gevallen is er nood aan een oplossing voor het definiëren en afdwingen van een aantal regels om die toegang op een veilige manier te laten verlopen. Men kan gerust de vergelijking maken met de veiligheidsmaatregelen die men al neemt voor PC's en laptops. Maar de tools die daarvoor gebruikt kunnen worden, zijn niet geschikt voor het beheer van mobiele toestellen. Er is dan ook een specifieke categorie van tools ontstaan, namelijk de Mobile Device Management (MDM) oplossingen.

De MDM-markt bevat een aantal pure-play spelers zoals Airwatch, MobileIron en Zenprise. Er is duidelijk interesse in dergelijke technologie, want grotere spelers vullen hun productgamma aan met zo'n MDM-oplossing. Zo is Airwatch overgenomen door VMware en Zenprise door Citrix.

Daarnaast breiden de leveranciers van beveiligingssoftware (waaronder Symantec en McAfee) de functionaliteit van hun producten ook meer en meer uit met MDM-functionaliteit.

In deze techno bespreken we allereerst de technische architectuur van een MDM-oplossing, gevolgd door een toelichting van de functionaliteiten die we ervan kunnen verwachten. Daarna lichten we de procedure toe om een nieuwe gebruiker en nieuw toestel te registreren in een MDM-systeem. Tenslotte vermelden we de oplossing die Smals biedt in dit kader.

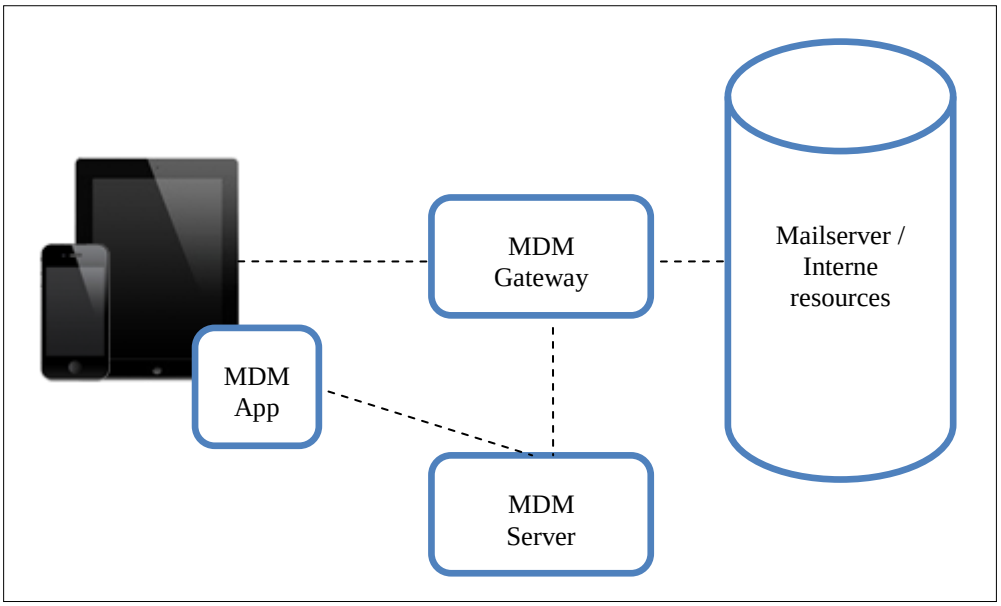
[1] *Zie slides infosessie, beschikbaar op de website van Smals Research: http://www.smalsresearch.be/publications/document?docid=24*

2. Architectuur

Vooraleer we in de details duiken in verband met de functionaliteiten, is het goed om eerst eens te zien hoe de technische architectuur van een MDM-oplossing eruit ziet en welke opties er bestaan op vlak van deployment.

Een MDM-oplossing bestaat doorgaans uit 3 componenten:

1. Een client app
2. Een policy-server
3. Een policy-gateway



Figuur 1: Een typische MDM-architectuur

De security-policies worden opgesteld en beheerd in de policy- en administratie-server (MDM Server in de figuur). De policies worden gecommuniceerd naar de mobiele toestellen via een MDM app. Via die weg worden de toestellen gemonitord. De toegang tot interne resources (bijvoorbeeld de mailserver) wordt gecontroleerd door een gateway die de gedefinieerde toegangsregels afdwingt (policy enforcement).

Globaal zijn er twee opties voor de deployment van een MDM-oplossing:

1. In SaaS-modus: de MDM-oplossing wordt gehost bij de MDM-leverancier zelf. De administratie en configuratie kan door eigen medewerkers uitgevoerd worden, maar de gegevens bevinden zich in een extern datacenter. Bemerk dat er bij deze manier van werken toch nog een lokale gateway-component nodig is voor de integratie met de interne resources (mailserver) en er ook een integratie moet voorzien worden met een user directory.
2. On-premise: de volledige MDM-oplossing wordt geïnstalleerd binnen het bedrijfsnetwerk. Deze vorm biedt het voordeel van vertrouwelijkheid van gegevens. De server-software kan geleverd worden onder de vorm van een virtuele machine of eventueel als een hardware appliance.

3. Functionaliteiten

In dit hoofdstuk worden de verschillende functionaliteiten besproken die we doorgaans terugvinden in een Mobile Device Management oplossing.

Eén van de kerneigenschappen van MDM-oplossingen is dat ze cross-platform werken: verschillende mobiele besturingssystemen worden ondersteund. Doorgaans zijn dat Android, iOS, Windows Phone en in beperkte mate ook BlackBerry. Bepaalde MDM-oplossingen beginnen ook de klassieke desktop-besturingssystemen te ondersteunen, maar dat staat nog in zijn kinderschoenen. Vandaag is er dus geen unieke oplossing voor het beheer van alle types toestellen.

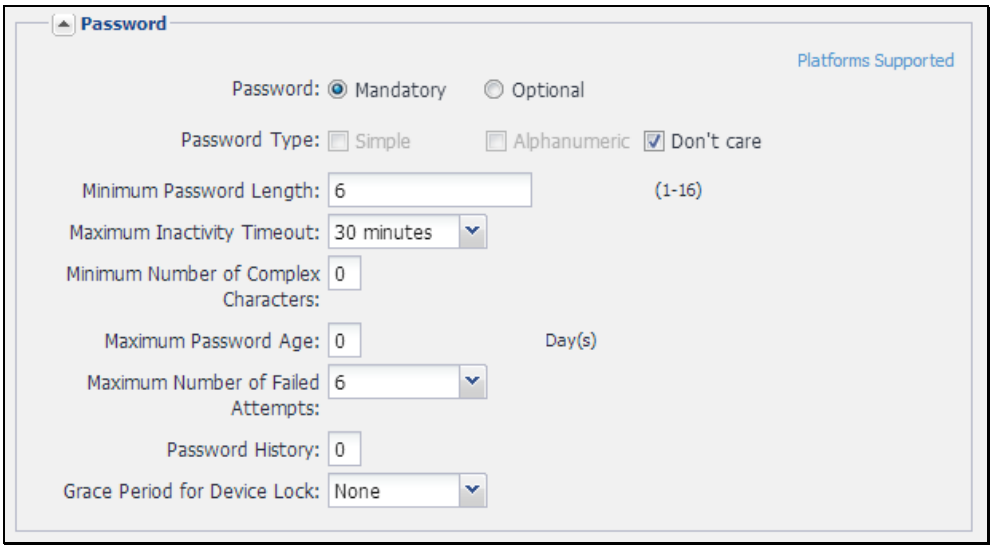
Het feit dat MDM-oplossingen meerdere platformen ondersteunen, betekent echter niet dat alle functionaliteiten op elk platform beschikbaar zijn. Typisch is er in de documentatie van elk product een compatibiliteitsmatrix opgenomen die aangeeft welke functionaliteit op elk platform ondersteund wordt. Hieronder geven we in grote lijnen weer welke functionaliteit doorgaans geleverd wordt in een MDM-oplossing.

3.1. Security policies

Eén van de kerntaken van een MDM-oplossing is om security policies af te dwingen. Afhankelijk van het platform kunnen er policies opgesteld worden op vlak van:

- **Device paswoord** Er kan gevraagd worden om een paswoord in te stellen om het toestel te ontgrendelen. Er kunnen een aantal regels ingesteld worden zoals het maximale aantal ongeldige pogingen en de minimumlengte en complexiteit van het paswoord.
- **Encryptie** Encryptie van de gegevens op het toestel en eventueel encryptie van de SD-kaart.
- **Jailbreak / rooted devices** Detectie van gecompromitteerde toestellen.
- **Minimale OS-versie** Indien er veiligheidsproblemen bekend zijn met oudere versies van het besturingssysteem kunnen die oudere versies uitgesloten worden.
- **Apps** Bepaalde apps kunnen verboden worden (bijvoorbeeld gekende malware) of net verplicht worden (bijvoorbeeld een anti-malware app).

Hieronder is een voorbeeld gegeven van de configuratie van een paswoord-policy. Bemerk dat in dit voorbeeld niet gevraagd wordt aan de gebruiker om het device-paswoord geregeld te vernieuwen ("Maximum Password Age" is niet ingesteld). De gebruiker heeft echter maximaal 6 pogingen om het correcte paswoord in te geven. Daarna kan het toestel volledig gewist worden om ongeoorloofde toegang tegen te gaan. Er kan ook gekozen worden voor een systeem waarbij de gebruiker gedurende een bepaalde tijdsspanne (bijvoorbeeld 30 seconden) geen nieuwe poging kan ondernemen. Die tijdsspanne wordt verlengd bij elke nieuwe foutieve poging.



Figuur 2: Voorbeeld van een paswoord-policy

3.2. Inventaris en monitoring

In de administratieve console is er een overzicht beschikbaar van alle geregistreerde toestellen. Van elk toestel zijn er een aantal detailgegevens beschikbaar, waaronder de naam van de gebruiker, het type toestel, OS-versie, enzovoort. Daarnaast kan de *compliance* status opgevolgd worden ten opzichte van de gedefiniëerde policies.

Figuur 3: Inventaris van de geregistreerde toestellen

In onderstaande figuur is een voorbeeld weergegeven van de status van een toestel ten opzichte van een paswoord-policy. We zien dat voor elk van de instellingen op het toestel de overeenkomstige regel nageleefd wordt. De reden waarom "SD Card Encryption" niet ondersteund is, is omdat het toestel in kwestie eenvoudigweg geen extern SD-cardslot heeft.

Name	Setting Value	Device Value	Status
Password	Mandatory	Mandatory	✓
Password Type	Don't Care	Don't Care	✓
Maximum Inactivity Timeout	5 minutes	5 minutes	✓
Minimum Password Length	4	4	✓
Maximum Passcode Age	0 day	0 day	✓
Maximum number of Failed Attempts	6	6	✓
SD Card Encryption	Disabled	Unsupported	⚠
Device Encryption	Enabled	Enabled	✓

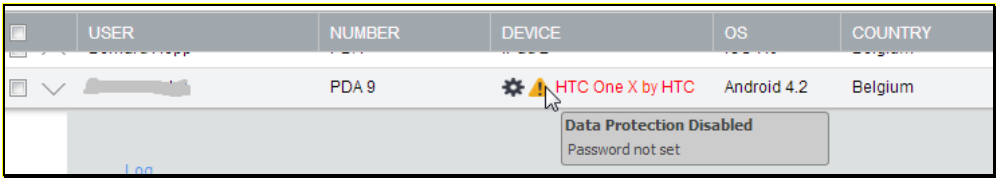
Figuur 4: Voorbeeld van de compliance-status van een toestel

3.3. Beveiligde toegang tot bedrijfsresources

Het wordt pas echt interessant voor een gebruiker van een smartphone of tablet als hij toegang kan krijgen tot bedrijfsresources zoals email, kalender, contacten en bedrijfsdocumenten.

In dit kader biedt een MDM-oplossing een gateway-functie: toestellen die voldoen aan de vooropgestelde regels kunnen toegang krijgen tot die bedrijfsresources. Omgekeerd, als een toestel niet voldoet aan de regels, dan wordt de toegang geblokkeerd en kan dit aan de gebruiker gesignaleerd worden. De gebruiker wordt dan gevraagd het nodige te doen om terug in regel te zijn om opnieuw toegang te kunnen krijgen.

Hieronder is een voorbeeld gegeven van een toestel dat niet compliant is. Er is met name geen device-paswoord ingesteld. De gebruiker kan nu verwittigd worden en gevraagd worden dit aan te passen. Alerts kunnen verstuurd worden via SMS, email of push notification.



Figuur 5: Aanduiding van een incompliant toestel

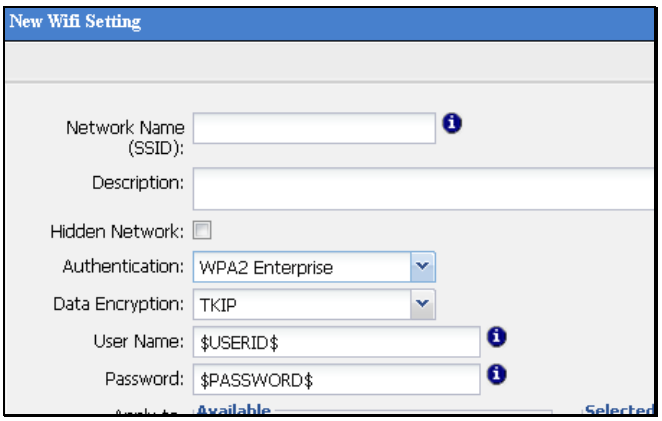
In eerste instantie is die gateway-functie gericht op ActiveSync-communicatie voor het synchroniseren van email, kalender en contacten: compliant toestellen worden toegelaten om te communiceren met een Microsoft Exchange Server of Notes server (via Notes Traveler).

Meer en meer breiden MDM-leveranciers de functie van de gateway uit. Zo kan er bijvoorbeeld ook een beveiligde verbinding opgezet worden tussen specifieke apps en back-end servers. Zo kan een app voor het synchroniseren van bestanden (file sync en sharing) een beveiligde verbinding maken met een interne document repository.

3.4. Instellingen

Het leven van gebruikers kan een stuk gemakkelijker gemaakt worden door het automatisch configureren van bepaalde instellingen. Instellingen kunnen door een administrator op de server ingesteld worden en automatisch gepusht worden naar een toestel. Afhankelijk van het platform kunnen onder andere volgende zaken ingesteld worden:

- E-mail instellingen (server-adres, synchronisatie-instellingen, etc.);
- Toegang tot een wifi-netwerk (SSID, etc.);
- VPN-instellingen (type, server-adres, etc.);



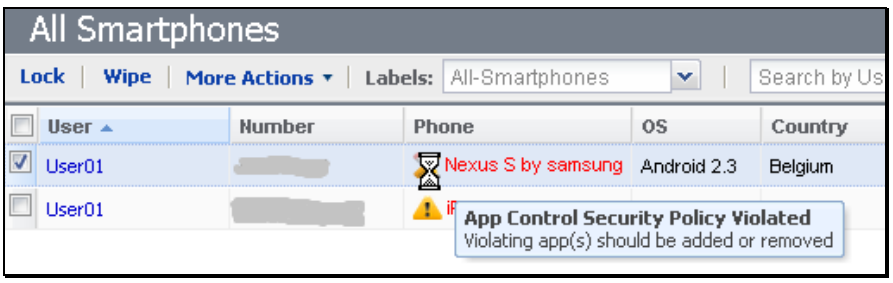
Figuur 6: Voorbeeld van een wifi-configuratie

3.5. Beheer van apps

Policies

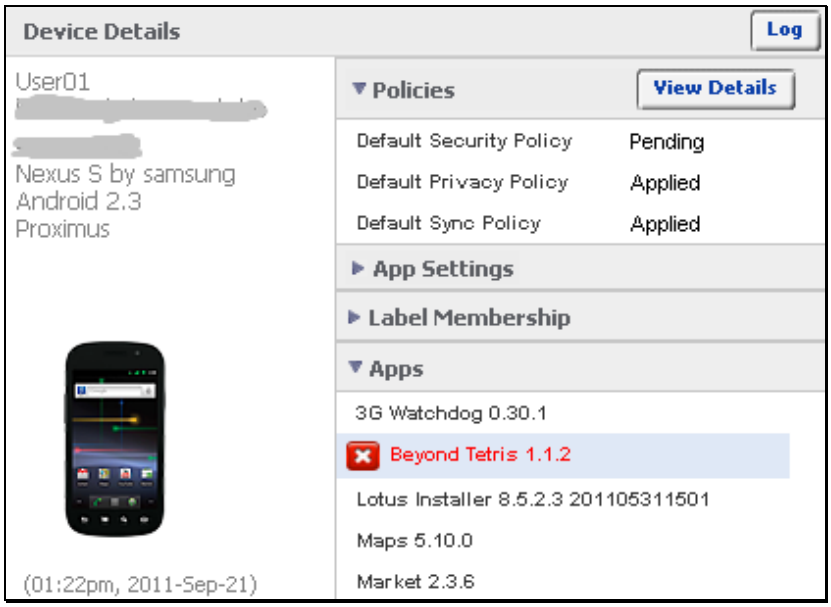
Er kan enige controle uitgevoerd worden over welke apps geïnstalleerd worden op een toestel. Zo kan er bepaald worden welke apps toegelaten, verboden of verplicht zijn. Die regels kunnen via een policy afgedwongen worden. Vervolgens kunnen er consequenties gekoppeld worden aan het niet naleven van de policy. Typisch kan de toegang geweigerd worden tot bedrijfsresources (email, etc.) zolang een verboden app geïnstalleerd is of een verplichte app niet geïnstalleerd is op het toestel.

Bij wijze van voorbeeld is hieronder te zien hoe een niet-toegelaten app op een toestel gedetecteerd is.



Figuur 7: Detectie van het niet naleven van een app-policy

In het detailoverzicht van het toestel is te zien over welke toepassing het gaat (Beyond Tetris 1.1.2). De gebruiker kan nadien gevraagd worden om de betreffende app te verwijderen.



Figuur 8: Detectie van een niet-toegelaten app

Inventaris

Voor de administrator is er een overzicht beschikbaar van alle apps die momenteel geïnstalleerd zijn op de beheerde toestellen. Zo kan er opgevolgd worden welke apps er gebruikt worden en welke het meest populair zijn. Bij gekende malware kan een administrator nagaan of de malware-app geïnstalleerd is op een toestel. Als dat het geval is, dan kan de gebruiker verwittigd worden en gevraagd worden de app te verwijderen. Er kan eventueel gebruik gemaakt worden van een App Reputation dienst zoals Appthority[2] voor het inschatten van de betrouwbaarheid van een app. Op basis van een rating geeft zo'n dienst aan in welke mate een app te vertrouwen is.

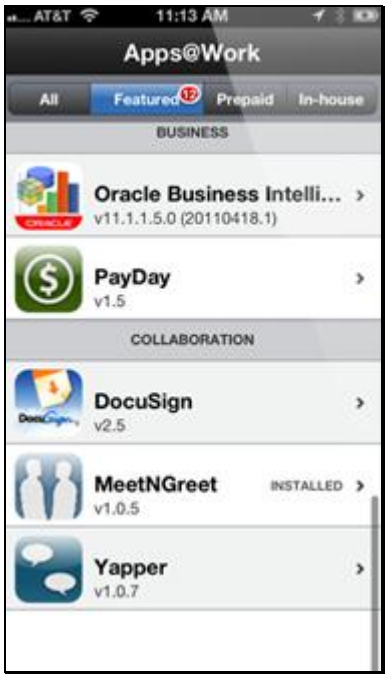
Distributie

Apps kunnen gedistribueerd worden via een eigen *enterprise app store*.

- Apps die publiek beschikbaar zijn in een officiële app store zoals Google Play of de Apple App Store kunnen aanbevolen worden via een eigen enterprise app store. Als een gebruiker zo'n app selecteert, dan wordt die gedownload vanaf de officiële app stores.
- Eigen interne (in-house) apps kunnen ook via de eigen enterprise app store gedistribueerd worden. De download gebeurt dan rechtstreeks op de MDM-server.

In de figuur hieronder is een voorbeeld gegeven van een lijst van aanbevolen apps in een enterprise app store.

[2] www.appthority.com



Figuur 9: Voorbeeld van aanbevolen apps in een enterprise app store

3.6. Blokkeren, wissen en lokaliseren

Een MDM-oplossing biedt doorgaans een aantal maatregelen in het kader van verlies of diefstal van een toestel, namelijk het blokkeren *(block)*, wissen *(wipe)* en lokaliseren *(locate)* van een toestel.

Blokkeren

Allereerst bestaat er de mogelijkheid om het scherm van een toestel van op afstand te blokkeren. De gebruiker moet dan zijn device paswoord terug ingeven. Het nut van een dergelijke *lock* is beperkt omdat de kans klein is dat een malafide persoon een toestel in handen krijgt terwijl het scherm niet geblokkeerd is. In de praktijk lijkt dit dus enkel nuttig indien iemand een toestel met geweld ontfutselt terwijl het scherm actief is (niet geblokkeerd).

Wissen

Naast het blokkeren kan een toestel ook van op afstand gewist worden. Een radicale oplossing is om het toestel volledig te wissen, dan wordt er een zogenaamde *factory reset* uitgevoerd waarbij de configuratie van het toestel herleid wordt naar de fabrieksinstellingen.

Een toestel kan echter ook gedeeltelijk gewist worden. Daarbij worden enkel de bedrijfsgegevens van het toestel verwijderd, met name alle gegevens, instellingen en apps die onder de controle vallen van de MDM-oplossing. Dit is veel interessanter voor de gebruikers: als men een toestel toch terugvindt, dan is men tenminste niet alle persoonlijke gegevens zoals foto's en muziek kwijt.

Lokaliseren

Een laatste maatregel in de context van diefstal en verlies van toestellen is het lokaliseren van een toestel. De laatst gekende locatie van een toestel kan opgevraagd worden via de administratie-console. Indien dit zo ingesteld is door de administrator kan een gebruiker dit ook zelf doen via een self-service portal.

De locatiegegevens worden op geregelde tijdstippen gesynchroniseerd tussen de MDM-client op het toestel en de MDM-server. De lokalisatie kan bij benadering gebeuren op basis van de GSM-masten of nauwkeuriger op basis van GPS.

Figuur 10: Lokalisatie van een toestel

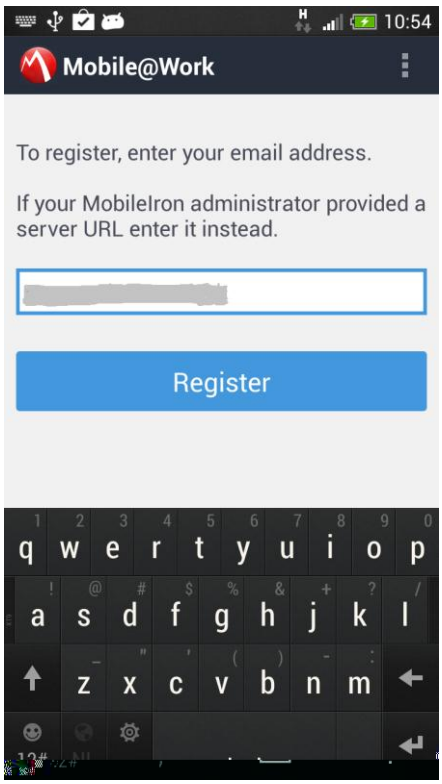
3.7. Self-service portal

Soms wordt ook de mogelijkheid gegeven aan gebruikers om zelf gedeeltelijk hun toestel te beheren via een self-service portal. Afhankelijk van de ingestelde rechten kan een gebruiker dan bijvoorbeeld een toestel lokaliseren, blokkeren, wissen, of een nieuw toestel registreren.

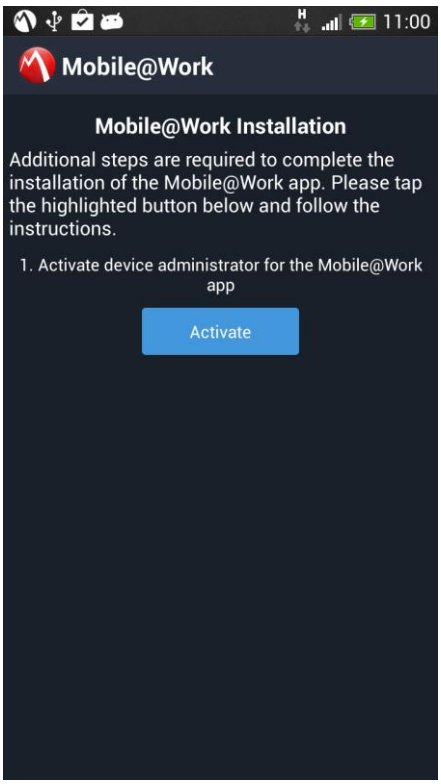
4. Registratieproces

Om een beeld te geven van hoe de registratie van een toestel in een MDM-oplossing typisch verloopt, lichten we hier in grote lijnen de stappen toe die een administrator en eindgebruiker dienen uit te voeren. Wie welke taken uitvoert is afhankelijk van welke ondersteuning de helpdesk levert: volledige configuratie van het toestel of enkel configuratie op niveau van de server. Bemerk dat deze procedure verschillend kan zijn van platform tot platform. Bij wijze van voorbeeld lichten we hier de procedure toe voor een Android-toestel, geïllustreerd met een aantal screenshots.

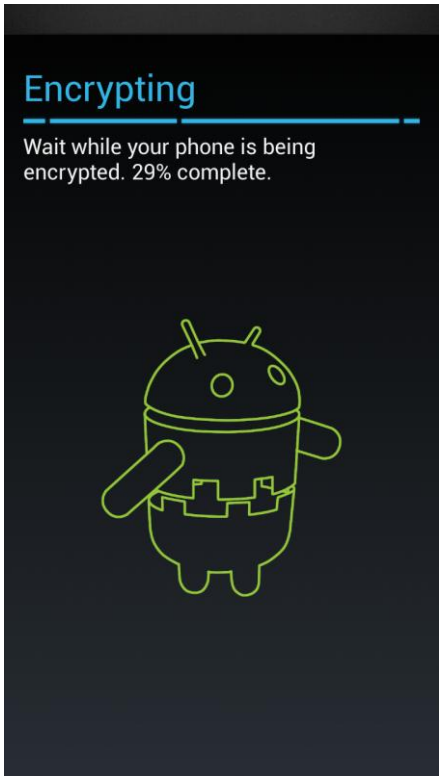
1. Aanmaken van een gebruiker in de MDM-oplossing, eventueel gelinkt met een enterprise directory (LDAP);
2. Configuratie van de mailserver: toegangsrechten geven voor de gebruiker;
3. Installatie van de MDM-app op het toestel via de officiële app stores. De installatie vereist het activeren van *device administrator* voor de MDM-app; Dat betekent dat de MDM-app uitgebreidere rechten krijgt om de taken uit te voeren waarvoor de app bedoeld is;
4. Configuratie van de MDM-app: ingeven server-adres en credentials van de gebruiker;
5. Configuratie van het toestel om de policy-regels te volgen, waaronder bijvoorbeeld het instellen van een device-paswoord en encryptie van het toestel;
6. Configuratie van bedrijfsemail: er kan gebruik gemaakt worden van een beveiligde container op het toestel, zoals Nitrodesk Touchdown of een andere emailclient. De configuratie hiervan kan automatisch gebeuren, de gebruiker hoeft enkel zijn email-paswoord in te geven.



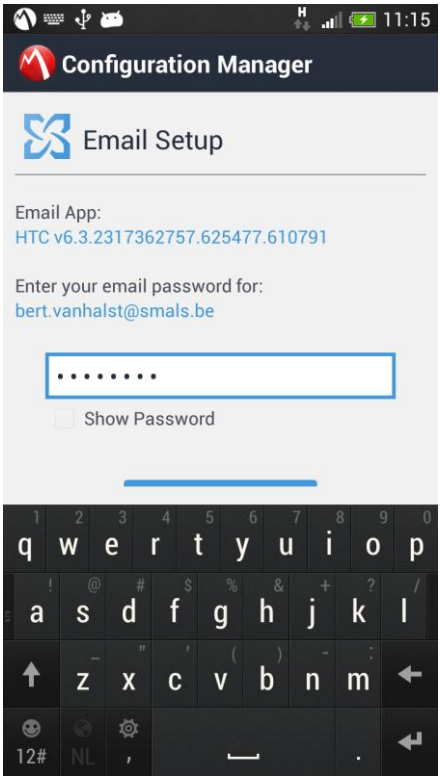
Configuratie van de MDM-app



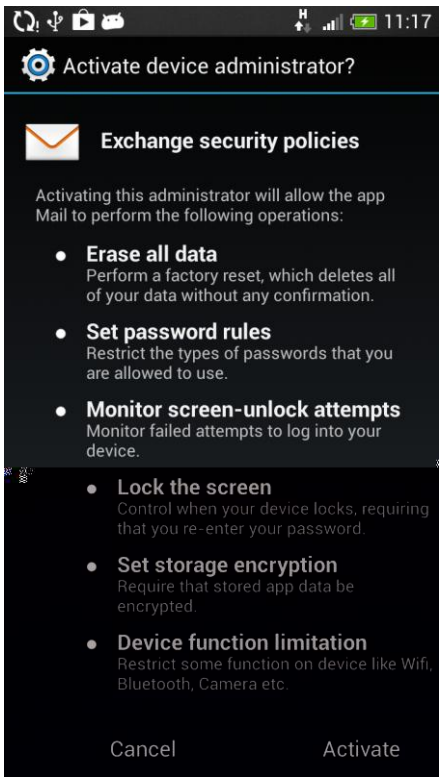
Activeren van *device adminisrator*



Encryptie van het toestel



Configuratie van email



Configuratie van email security policies

5. Smals oplossing

Smals biedt een oplossing aan voor het beheer van smartphones en tablets en beveiligde toegang tot e-mail, kalender en contacten via een Exchange of Notes server.

Omwille van de vertrouwelijkheid van gegevens wordt de oplossing gehost door Smals zelf en niet bij een externe cloud provider.

De oplossing is gebaseerd op technologie van MobileIron en biedt een complete waaier aan features voor het beheer van mobiele toestellen, zoals een inventaris van geregistreerde toestellen, security policies (device paswoord, encryptie van de gegevens op het toestel) en het van op afstand blokkeren, wissen en lokaliseren van een toestel. De security policies zijn daarbij in overeenstemming met die van het Extranet van de Sociale Zekerheid.

6. Conclusie

Een Mobile Device Management (MDM) oplossing laat ons toe om veiligheidsregels af te dwingen op smartphones en tablets en om een beveiligde toegang te bieden tot bedrijfsgegevens zoals email, kalender en contacten.

Een MDM-oplossing kan niet alleen ingezet worden voor toestellen die eigendom zijn van de organisatie, maar ook voor privé-toestellen van medewerkers in een BYOD-context (Bring Your Own Device).

Meer en meer breiden leveranciers van MDM-oplossingen hun aanbod uit. Naast het pure beheer van de toestellen leveren ze nu ook functionaliteit voor het beheer van applicaties en gegevens. Daarbij gaat er aandacht uit naar het distribueren van apps en het extra beveiligen van gegevens die via bepaalde apps te consulteren of manipuleren zijn. Men spreekt dan van Mobile Application Management (MAM) en Mobile Content Management (MCM).

Deze technologie is dus nog volop in beweging en het is dan ook de moeite waard om deze van nabij op te volgen!