MobileIron Virtual Smartphone Management Platform

David Rupprechter

Immer mehr Consumer-Endgeräte, besonders jene von Apple, werden zu unerlässlichen Gadgets im beruflichen Umfeld. Zugangsschutz, Remote-Löschung bei Diebstahl und andere Anforderungen lassen sich ohne spezielle Software jedoch nicht umsetzen. Virtual Smartphone Management Platform von MbileIron versucht innovativ diese Anforderungen zu erfüllen.

IN DIESEM ARTIKEL ERFAHREN SIE...

- Funktionen, welche Virtual Smartphone Management Platform von MobileIron bietet um die Verwaltung mobiler Endgeräte zu verbessern und Richtlinien durchzusetzen“

WAS SIE VORHER WISSEN SOLLTEN...

- Grundlegende Erfahrung mit Smartphones oder anderen mobilen Endgeräten.
- Allgemeine VMware ESX- und Netzwerkkenntnisse

Virtual Smartphone Management Platform

Die Firma Mobile Iron wurde 2007 gegründet und hat ihren Sitz in Kalifornien. 33 Techniker bemühen Smartphones Enterprise-Ready zu machen. Hierfür bietet die Firma das Produkt „Virtual Smartphone Management Platform“ (kurz VSP) an. Dieses steht als Appliance oder als ESX-Image zur Verfügung. Der Vorteil der virtualisierten Variante besteht in der Ausfallsicherheit, da in Zusammenspiel mit VMware HA und redundanten ESX-Server so eine Hochverfügbarkeit gewährleistet werden kann. Bei Ausfall einer Appliance wäre bis zum Austausch keine Verbindung der mobilen Endgeräte

Lockdown Policies Support

	iOS	BlackBerry	Windows Mobile 5.x	Windows Mobile 6.x	Symbian	Android	Palm webOS
Camera				✔	✔*	✔**,***	
SD Card				✔	✔*		
Bluetooth (Enable Audio & Data)				✔	✔*	✔**	
Bluetooth (Enable Audio)			✔	✔			
Bluetooth (Disable)				✔	✔*	✔**	
IRDA				✔			
WiFi			✔	✔		✔**	

* Disabled by unmounting.

** Requires Android version 2.3 (and higher) with Samsung Enterprise APIs.

*** Requires Android version 4.0 (and higher).

Abbildung 1. *Lockdown-Policy Unterstützung mobiler Endgeräte*

zum Exchange-Server verfügbar. Die Plattform besteht aus zwei Systemen. Beide Systeme basieren auf Linux und lassen sich nach der kurzen Grundkonfiguration *(Hostname, IP, Gateway,…)* bequem per Webinterface administrieren.

Integration in das Firmennetzwerk

Die Plattform besteht aus einem Sentry-System, welches Exchange-ActiveSync-Inhalte über Port 443 zur Verfügung stellt und dem VSP-System, welches für Registrierung, Konfigurationsmanagement, Apps usw. zuständig ist. Beide Systeme, welche auf Linux basieren, sind in der DMZ zu positionieren. Die Installation erfolgt bei der virtuellen Appliance nach dem Import auf den ESX-Server über die Konsole und dauert nur wenige Minuten.

Die Sentry Appliance erfüllt den Zweck eines Reverse Proxies und stellt Exchange-ActiveSync-Dienste bereit. So erhält man einen eigenen ActiveSync-Pfad für mobile Endgeräte. Der Zugriff auf diesen Kommunikationspfad lässt sich beim Verstoß gegen Firmenrichtlinien deaktivieren oder zum Beispiel nur für bestimmte verwaltete Geräte aktivieren. Dadurch ergibt sich auch die Möglichkeit Outlook Web Access (OWA), falls nur für mobile Endgeräte benötigt, generell zu deaktivieren. Bis dato wurde OWA für einen Großteil der Smartphones (exkl. Blackberry) benötigt um eben jene an Exchange anzubinden.

Nach der Basisinstallation ist eine Konfiguration über das Webinterface vorzunehmen. Im Hauptpunkt „*Settings*“ sind Interfaces, Routen und DNS zu überprüfen und gegebenenfalls anzupassen. Aufgrund der späteren Verwendung von Zertifikaten ist ein NTP-Server ebenfalls zu hinterlegen. Ein weiterer benötigter Schritt ist die Hinterlegung eines Mailservers. Optional können für die Überwachung der Plattform SNMP- oder Syslog-Server definiert werden. Bei Bedarf können die Standard-Ports (Sync-, Helpdesk- und Provisioningports) geändert werden.

In der Registerkarte „*Security*“ können Zertifikate und lokale Benutzer verwaltet werden. Ebenso können hier über Access Control Lists (ACL´s) die Schnittstellen des Systems nur für bestimmte IP-Bereiche/… geöffnet werden.

Andere benötigte Anpassungen und die Verwaltung von Smartphones kann über die Smartphone-Management-Seite durchgeführt werden. Der Wechsel zwischen dem System- und Smartphone-Management erfolgt ein wenig versteckt mit einem Klick auf „Smartphone“ oder „System“ rechts neben dem MobileIron Logo.

Das Smartphone-Management beinhaltet eine „*Settings*“-Seite auf welcher man die LDAP-Anbindung

Sync Policies Support

	iOS*	BlackBerry	Windows Mobile 5.x	Windows Mobile 6.x	Symbian	Android	Palm webOS
Use TLS	✔	✔	✔	✔	✔	✔	
Sync While Roaming		✔	✔	✔	✔	✔	
Sync SD Card Files		✔	✔	✔	✔		
Sync on Low Battery		✔	✔	✔	✔	✔	
Battery Level		✔	✔	✔	✔	✔	
Battery Level for File Upload		✔	✔	✔	✔		
Heartbeat Interval	✔	✔	✔	✔	✔	✔	
Sync Interval	✔	✔	✔	✔	✔	✔	
iOS App Multitasking Sync Interval	✔						
Client is Always Connected	✔		✔	✔	✔	✔	

* Assumes MDM is enabled.

Abbildung 2. *Sync-Policy Unterstützung mobiler Endgeräte*

oder zum Beispiel einen optional bestehenden Blackberry-Enterprise-Server hinterlegen kann. Ebenso werden hier Sicherheitseinstellungen für die Registrierung von iOS/Android-Geräten verwaltet. Die Sentry-Appliance ist unter „*Settings*“ -> „*Sentry*“ zu hinterlegen.

Abbildung 6 zeigt die Positionierung der beiden Appliances im Firmennetzwerk. Die entsprechenden Ports (eingehend, ausgehend) müssen auf der Firewall freigeschaltet werden um einen ordnungsgemäßen Betrieb gewährleisten zu können.

Initialer Rollout von Endgeräten

Für den Rollout wird das jeweilige Gerät über das Webinterface registriert. Daraufhin erhält der Benutzer eine SMS mit Instruktionen um den Registrierungsvorgang abzuschließen. Hierfür ist der MobileIron-Client auf dem Gerät herunterzuladen (zB im Apple AppStore verfügbar). Den Status des jeweiligen Geräts kann man im Webinterface unter „*Smartphones & Users*“ -> „*All Smartphones*“ überprüfen. Für jedes Gerät werden alle relevanten Informationen aufgelistet. Dazu zählen verfügbarer Speicherplatz, installierte Apps, Version des Smartphone-OS usw.

Unterstütze Endgeräte und Policies/App Settings und Labels

Es werden eine große Anzahl von Endgeräten unterstützt (*iOS-Geräte, Blackberry, Windows Mobil 5.x und 6.x, Symbian, Android und Palm webOS*). Zahlreiche

Privacy Policies Support

	iOS*	BlackBerry	Windows Mobile 5.x	Windows Mobile 6.x	Symbian	Android	Palm webOS
Calls		✔	✔	✔	✔		
SMS		✔	✔	✔	✔		
Data Traffic		✔	✔	✔	✔		
Contacts		✔	✔	✔	✔		
Apps	✔	✔	✔	✔	✔	✔	
Documents		✔	✔	✔	✔		
Picture Files		✔	✔	✔	✔		
Video Files		✔	✔	✔	✔		
Music Files		✔	✔	✔	✔		
Store File Types		✔	✔	✔	✔		
iOS App Multitasking	✔						
Location		✔	✔	✔	✔		
Exclude File Directory		✔	✔	✔	✔		

* Assumes MDM is enabled.

Abbildung 3. *Privacy-Policy Unterstützung mobiler Endgeräte*

Backup and Restore Policies Support

	iOS	BlackBerry	Windows Mobile 5.x	Windows Mobile 6.x	Symbian	Android	Palm webOS
Backup		✔	✔	✔	✔		
Restore		✔	✔	✔	✔		

Abbildung 4. *Backup&Restore-Policy Unterstützung mobiler Endgeräte*

Policies können jedoch nur auf die unterstützen Endgeräte angewendet werden.

Es gibt vier verschiedene Arten von Policy-Gruppen:

- Lockdown-Policy *(Kamera, Wifi,…)*
- Sync-Policy *(Batterie, Roaming, TLS,…)*
- Privacy-Policy *(Anrufe, SMS, Apps,…)*
- Backup & Restore Policy

Es sieht so aus als würden iOS-Geräte (Apple-Geräte) kaum eine gute Unterstützung finden. Diese Geräte können jedoch über die iOS App-Settings, zu finden in der Karte „App & Files“ (siehe Abbildung 5), ausgiebig verwaltet werden.

Unter anderem können folgende Device Features für iOS-Geräte deaktiviert/aktiviert werden:

- Installation von Apps
- Benutzung der Kamera
- Benutzung von Youtube
- Benutzung von Safari
- Benutzung von iCloud

Zusätzlich können Exchange- und Mailzugänge, Wifi- und VPN-Verbindungen sowie Bookmarks und Zertifikate innerhalb der App Settings für alle Geräte geregelt werden.

Wie in Auflistung eins bis vier zu sehen werden die jeweiligen Policy-Features nur von bestimmten Geräten unterstützt. Sehr gute Unterstützung finden vor Allem Blackberry (bis auf Lockdown-Policy), Windows Mobile und Symbian-Geräte. Bis auf die Privacy- und Backup-Richtlinien können auf Android-Geräte ebenfalls alle restlichen Policies angewendet werden.

Über die Funktion „App Control“ lassen sich nicht erwünschte/benötigte/erlaubte Apps definieren. Bei einem Verstoß gegen Richtlinien werden je nach Einstellung Warnungen an den Benutzer versendet oder die Exchange-Synchronisation deaktiviert. Zusätzlich können noch weitere Aktionen manuell definiert werden.

Über den Punkt „App Distribution“ lassen sich Apps in eine Favoritenliste hinzufügen um diese den Benutzern auf dem Endgeräten bereitzustellen. Das beziehen dieser Apps erfolgt jedoch mit dem eigenem iTunes/Google/…-Account. Auf iOS-Geräten lassen sich, mit Hilfe des iOS Volume Purchase Program (VPP) Apps im Voraus bezahlen. Hierfür kann die jeweilige VPP-Datei der jeweiligen App in „App Distribution“ hinterlegt werden. Somit entstehen für den Endnutzer keine Kosten mehr.

Alle Policies lassen sich bestimmten Labels zuweisen. Vordefinierte Labels sind zum Beispiel „Employee-Owned“ oder „Company-Owned“. Geräte können mehreren Labels zugeordnet werden. Kommt es hier zu Konflikten kommt das als vorranging definierte Label zum Einsatz.

Wie in den Abbildungen eins bis fünf zu sehen bietet das Produkt viele Möglichkeiten zur Verwaltung mobiler Endgeräte. Eine detaillierte Besprechung aller Optionen würde den Rahmen dieses Artikels sprengen. Einige von Firmen eventuell benötigte Features fehlen jedoch. Ein Beispiel hierfür wäre zum Beispiel die Möglichkeit

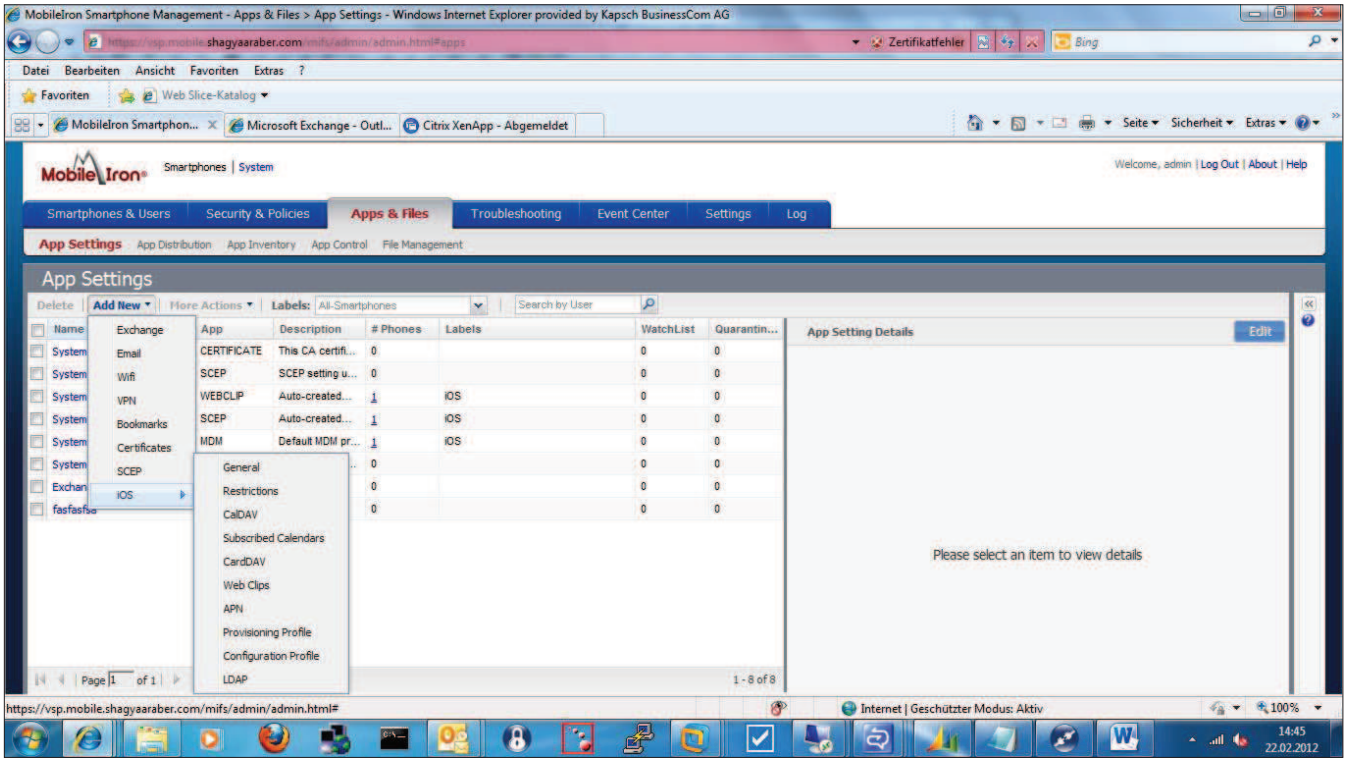

Abbildung 5. *Die iOS-App-Settings und deren Möglichkeiten*

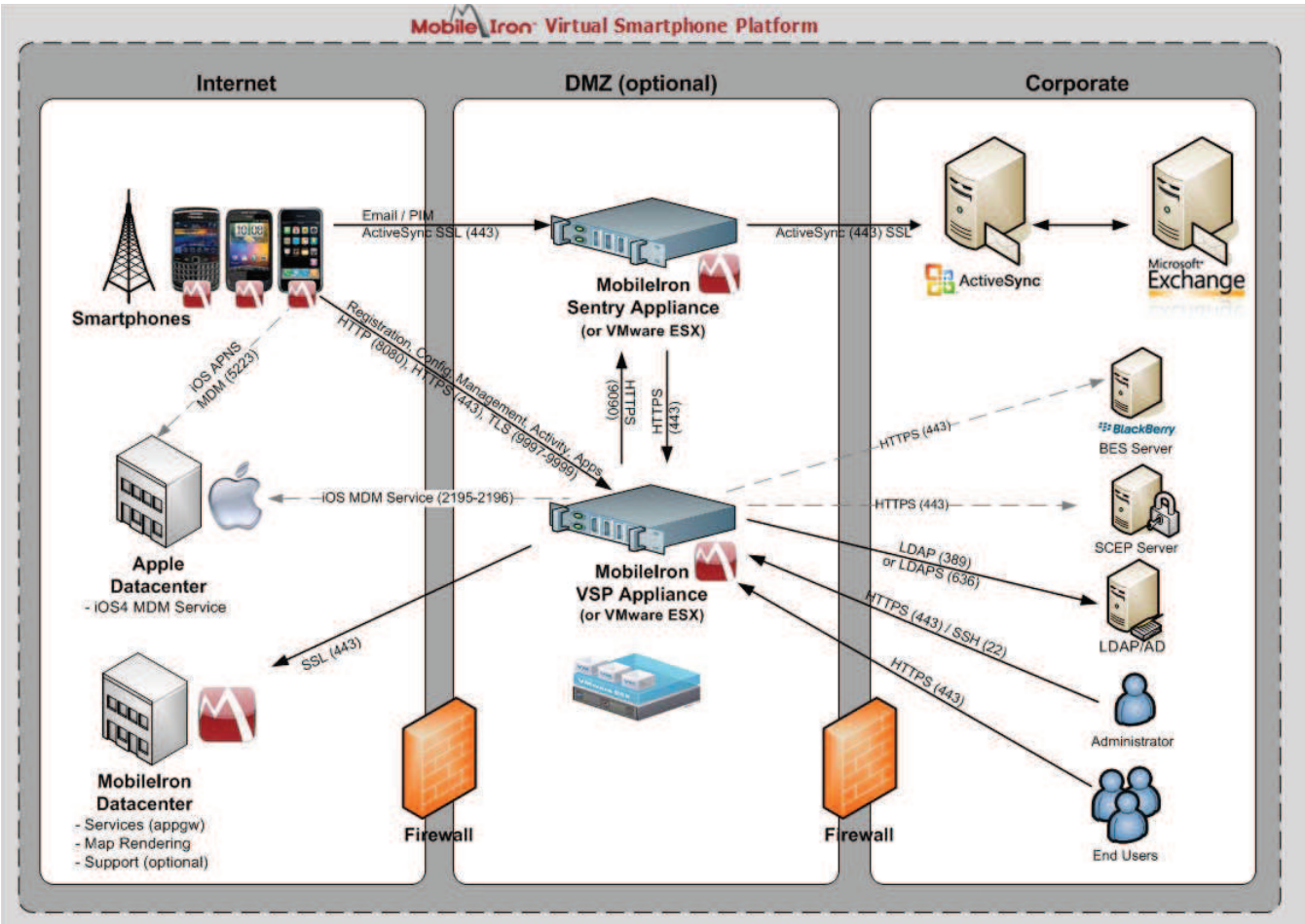

Abbildung 6. *Positionierung von VSP und Sentry im Firmennetzwerk*

die Hinterlegung von zusätzlichen Online-Konten in der App Goodreader (Google-Docs/Dropbox-Anbindung) zu unterbinden. Derartige Einschränkungen sind leider, zumindest in der jetzigen Version, nicht umsetzbar.

Apple MDM Architektur

Um iOS-Geräte per MobileIron VSP verwalten zu können wird Apple MDM (Mobile Device Management) verwendet. Hierbei wird von Apple das „Apple Push Notification Service“ (APNs) verwendet, welches ein von Apple signiertes Zertifikat für die Benutzung benötigt. Über die Registerkarte „Settings“ in der Smartphones-Verwaltung kann man hierfür unter „MDM Preferences“ einen Zertifikatsrequest erstellen und diesen in einem zweiten Schritt über das Apple Push Certificates Portal signieren zu lassen um zuletzt das erhaltene MDM Zertifikat auf das VSP-System zu importieren.

Fazit

Die Virtual Smartphone Platform bietet zahlreiche Möglichkeiten zur Verwaltung von mobilen Endgeräten. Features wie Remote-Wipe, die Verteilung von VPN- und Wifi-Profilen oder das einheitliche Setzen von Smartphone-Einstellungen überzeugen und sparen dem Administrator viel Zeit. Zusätzlich kann die Exchange-Synchronisation auf Basis von Geräten und Einhaltung von Regeln erlaubt/gesperrt werden. Bei Interesse an den Möglichkeiten des Produkts bietet sich eine Beantragung einer Testversion an um zusätzliche Einstellungsmöglichkeiten, welche im Rahmen diesen Artikels nicht erwähnt wurden, zu erforschen.

Im Internet

- *https://mobileiron.zendesk.com/home* - MobileIron Support Portal
- *http://www.youtube.com/user/mobileiron?blend=2&ob=video-mustangbase* – MobileIron Youtube Channel
- *http://cysalesteam.com/mobileiron* - MobileIron University

DAVID RUPPRECHTER

Der Autor beschäftigt sich mit Windows/Linux/Virtualisierung/Sicherheit seit vielen Jahren. Auf der privaten Webseite www.dotlike.net sind Projekte und Artikel von ihm zu finden. Kontakt mit dem Autor: rupprechter@dotlike.net