Connect2013

IBM

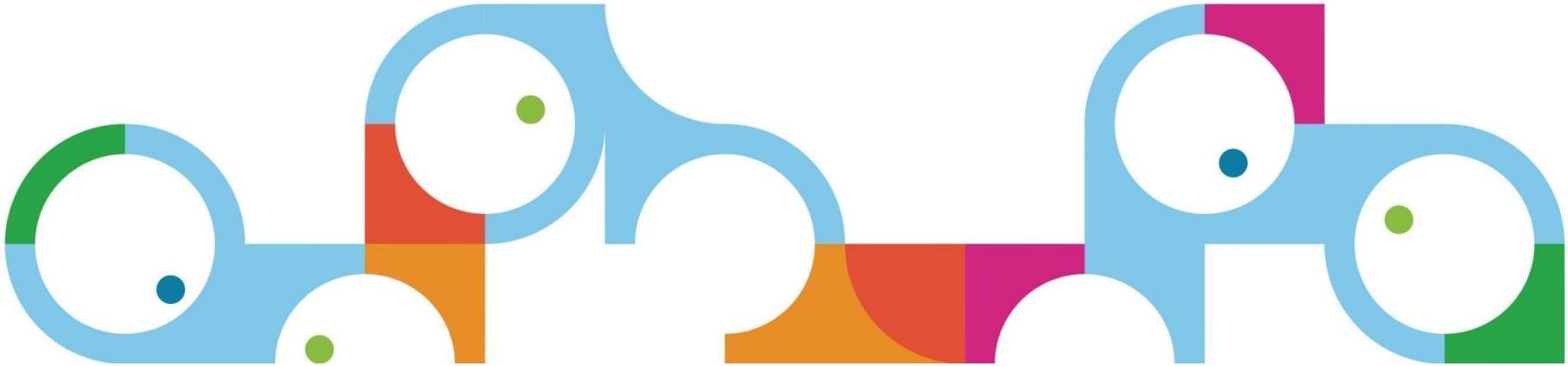
IBM智慧行動協同論壇

打造企業行動力
實踐協同社群力

主辦單位 IBM

媒體協辦 Business Next 數位時代 媒體群 經理人 MANAGER today

Tivoli Endpoint Manager for Mobile Device Management
行動裝置管理



Agenda

- MDM importance in MobileFirst
- Tivoli Endpoint Management for MDM Architecture
- MDM Challenge and Response
- Why TEM Endpoint Manager

行動裝置帶給IT的挑戰

行動裝置的出現帶給企業IT管理很大的挑戰，打破傳統IT管理方式!!

傳統管理模式	行動裝置管理
企業提供所有設備	員工攜帶自己行動裝置設備(BYOD)
Desktop/Laptop種類有限	行動裝置設備種類、品牌甚多
IT緊密控制軟體和安全	User自行控制自己的設備
IT控制軟體使用、升級	設備、OEM方式和User可自行安裝升級app/OS

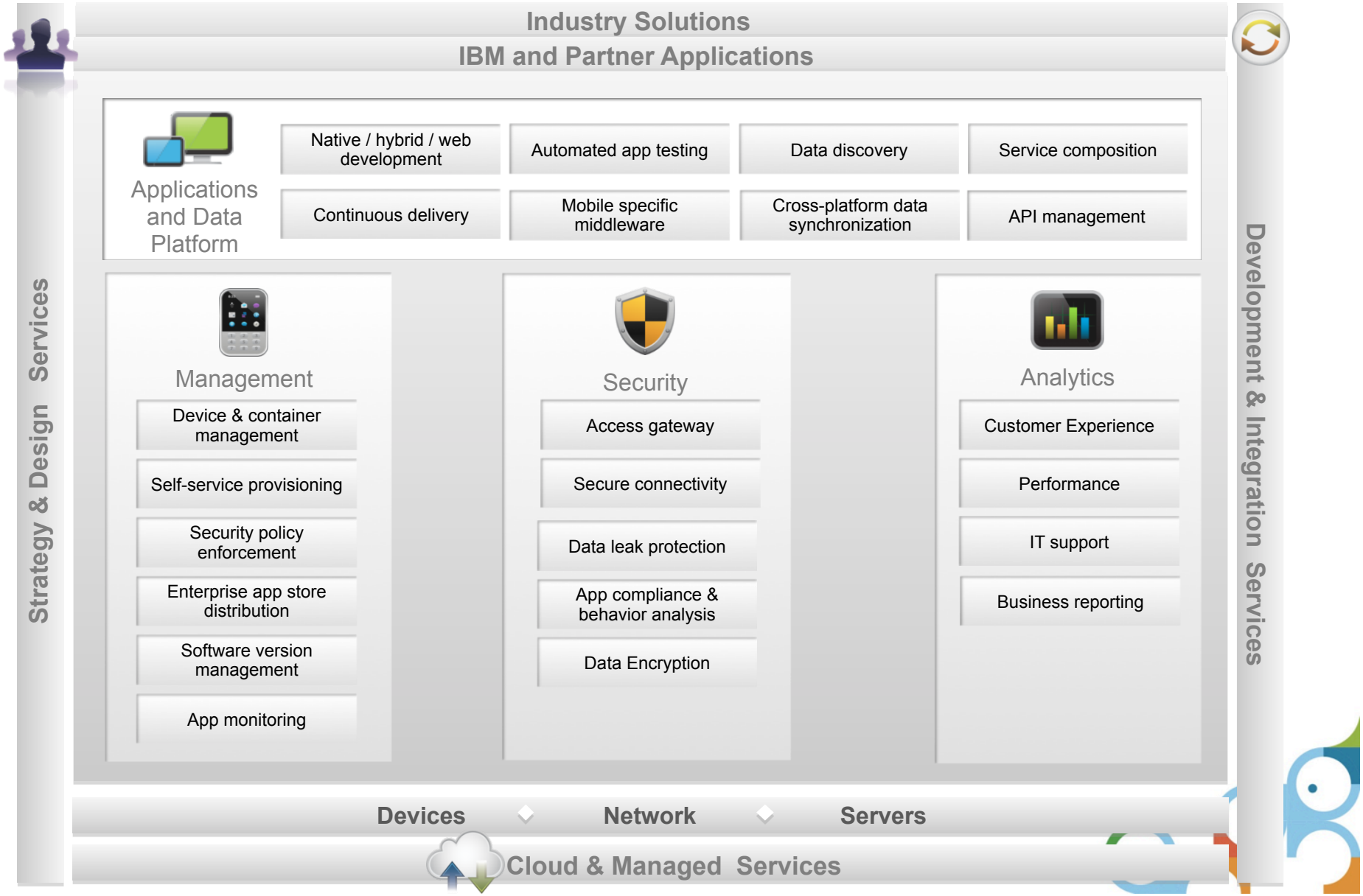
IT部門回應的方向：

- ✗ 不允許行動裝置設備出現在公司，因為太難管理
- ✗ 允許未受管控的行動裝置在公司內部使用
- ✓ 運用工具與服務強化管理行動裝置設備

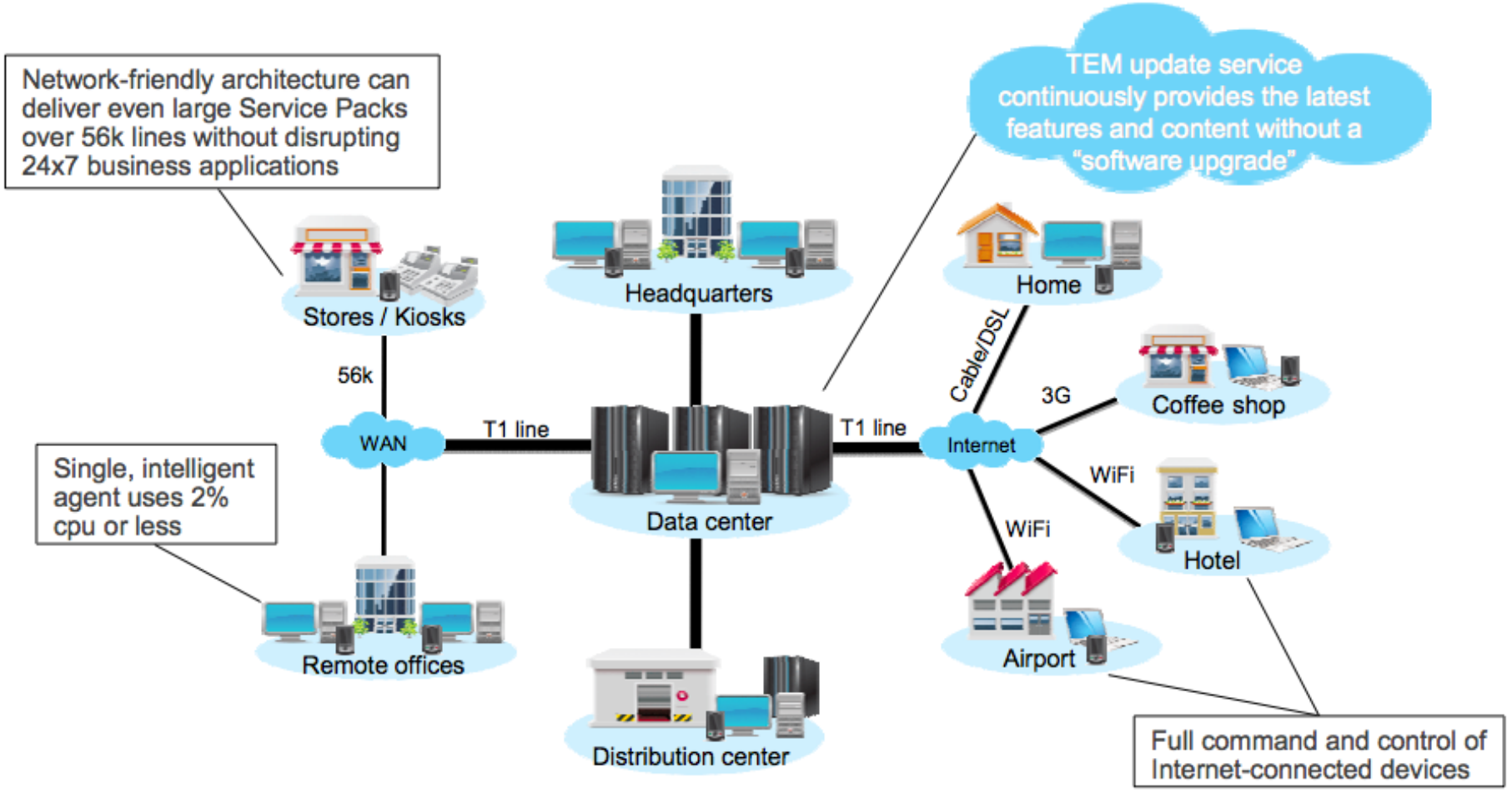
	For Now	3 years later
忽略不管	8%	0%
完全禁止	15%	3%
接受BYOD	30%	60%

Source: Gartner

IBM MobileFirst Portfolio

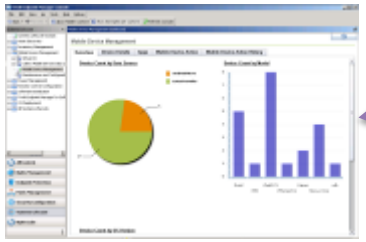


Tivoli Endpoint Manager, built on BigFix technology



Whether it's a Mac connecting from hotel wi-fi, or a Windows laptop at 30K feet, or a Red Hat Linux Server in your data center, Tivoli Endpoint Manager has it covered. In real time, at any scale.

TEM MDM 佈署架構



Console / Web Reports

BigFix Server

DB

Relay(s)

Management Extender for (Exchange or Lotus)

Email Server (Exchange/Lotus)

Apple Push Notification Servers

Mgmt Extender for iOS

Desktops / Laptops

Servers

Phones / Tablets

Android

Android TEM App

w/Email

Apple

Apple TEM App

行動裝置管理挑戰與管理

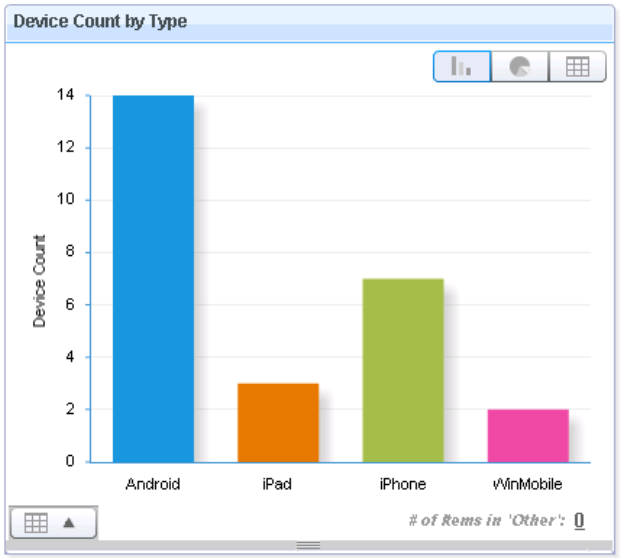
MDM挑戰	TEM for MDM解決方案
BYOD行動裝置怎麼管理	由公司派送WIFI,VPN,MAIL設定 部署軟體 自助服務 偵測並管理越獄裝置
若手機遺失，如何處理?	訊息告知、密碼原則控制(pin length, timeout, wipe after failed login, etc.) 和遠端移除裝置
當員工拿行動裝置離開公司時，如何處理敏感資料外洩可能	離開公司時啟用行動裝置加密、選擇性擦除
面對快速更新的行動裝置 OS/apps ，如何管理行動裝置軟體?	黑名單軟體管理、白名單軟體管理(建議安裝軟體) 、禁止安裝軟體
行動設備數量多，資產如何管理	硬體資產管理 軟體資產管理

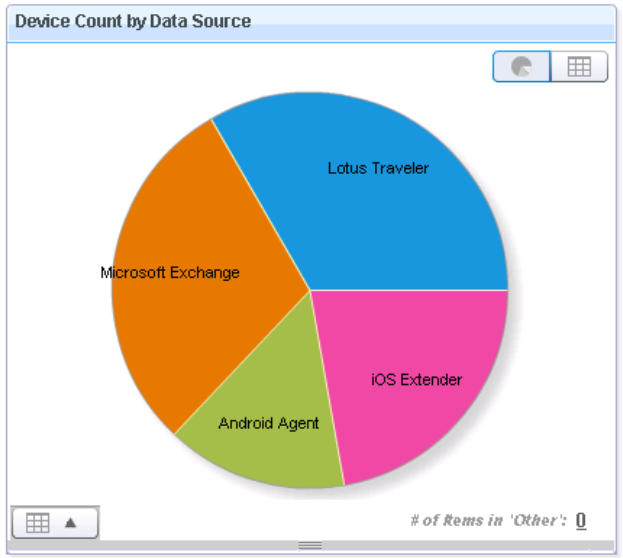
行動裝置管理挑戰與管理

MDM挑戰	TEM for MDM解決方案
BYOD行動裝置怎麼管理	由公司統一佈署WIFI,VPN,MAIL設定 部署軟體 自助服務 偵測並管理越獄裝置
若手機遺失，如何處理?	訊息告知、密碼原則控制(pin length, timeout, wipe after failed login, etc.) 和遠端移除裝置
當員工拿行動裝置離開公司時，如何處理敏感資料外洩可能	離開公司時啟用行動裝置加密、選擇性擦除
面對快速更新的行動裝置 OS/apps ，如何管理行動裝置軟體?	黑名單軟體管理、白名單軟體管理(建議安裝軟體) 、禁止安裝軟體
行動設備數量多，資產如何管理	硬體資產管理 軟體資產管理

Device info

Computer Name	Name	Manufacturer	Model	Carrier	UUID / UDID
000000000000000	n/a	unknown	sdk	generic	3619CE929CAA4AC79B47622F
358224040002945	n/a	Lenovo	ThinkPad Tablet	Lenovo	C85ACE3BC26C448B97594320
7T041BQXA4S	Ben's iPhone4	Apple	iPhone	AT&T	3f50b4cbbaf3386c84c866278b
81938CMX3NP	Estie's iPhone	Apple	iPhone	AT&T	8a8e9890ebca2f6a3d413b268
889393M83NS	Scot's iPhone	Apple	iPhone	Vodafone IT	94d10c4c5012a084c781ce357
99000033060984	n/a	HTC	ADR6400L	verizon_wwe	A605D472C38D4475A42CD03I
99000052220657	n/a	Motorola	Xoom	verizon	68F4409966014DD59183BF30
C8QFR5NYDDPC	soap	Apple	iPhone	Verizon	b5e05236061cb409abe5aecf2
DN6FNBLTDFJ1	Ben's iPad	Apple	iPad	AT&T	cb14a1ad7c616b5b3e5391416
J3050BMSZ38	iPad	Apple	iPad	<error>	bc5fd9984b5085ecb1cf4dad96

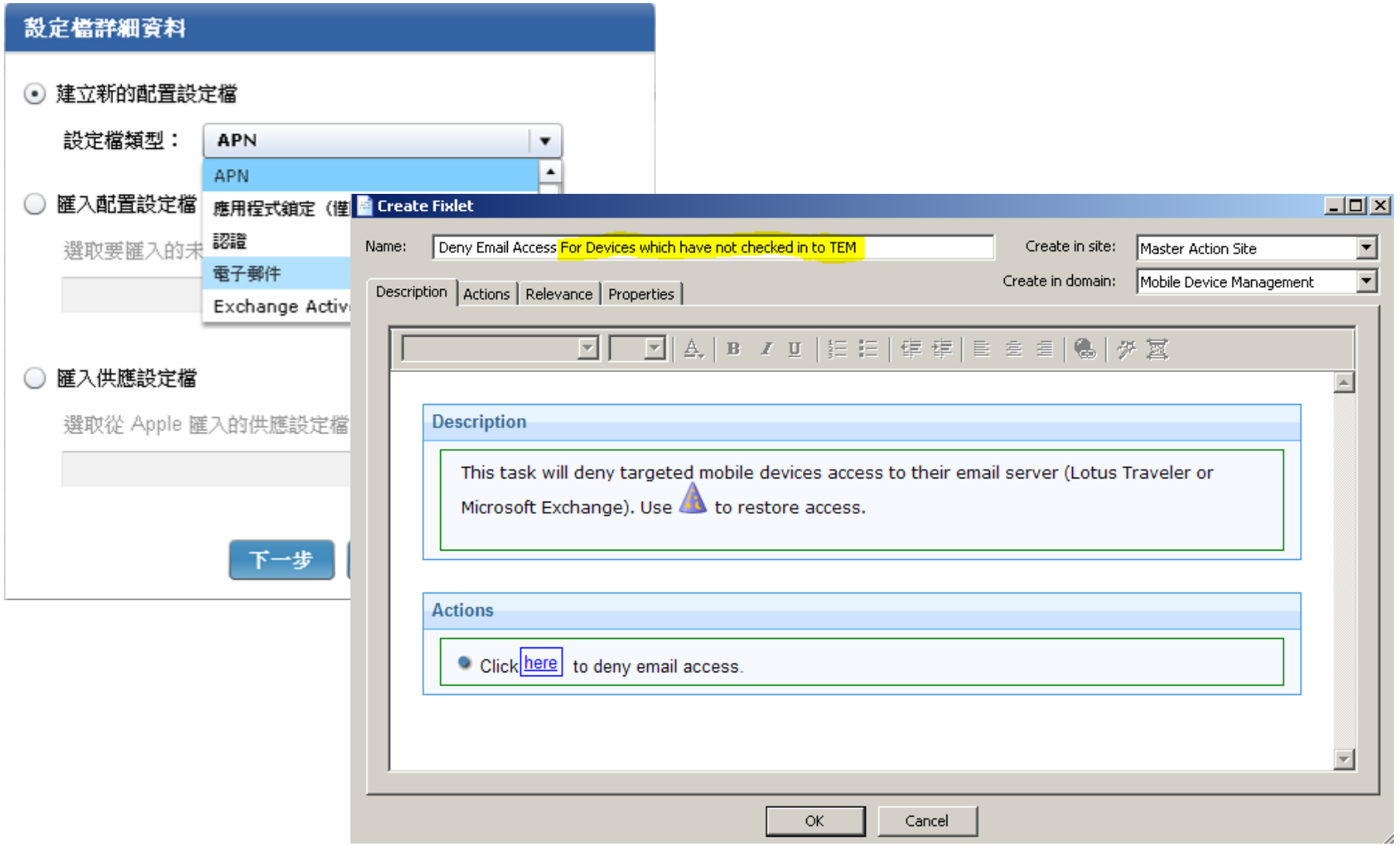




Wi-Fi 派送


WiFi
SSID
要連接的無線網路的識別
自動加入
自動加入目標網路
隱藏的網路
檢查目標網路是否未開啟或播送中
Proxy
此 WiFi 連線的 Proxy 設定
無
安全類型
連接時要使用的無線網路加密
WEP 企業版
企業版設定 - 通訊協定
接受的 EAP 類型
目標網路上支援的鑑別通訊協定
TLS
LEAP
EAP-FAST
TTLS
PEAP
EAP-SIM
EAP-FAST
上一頁
完成
取消

Email 設定

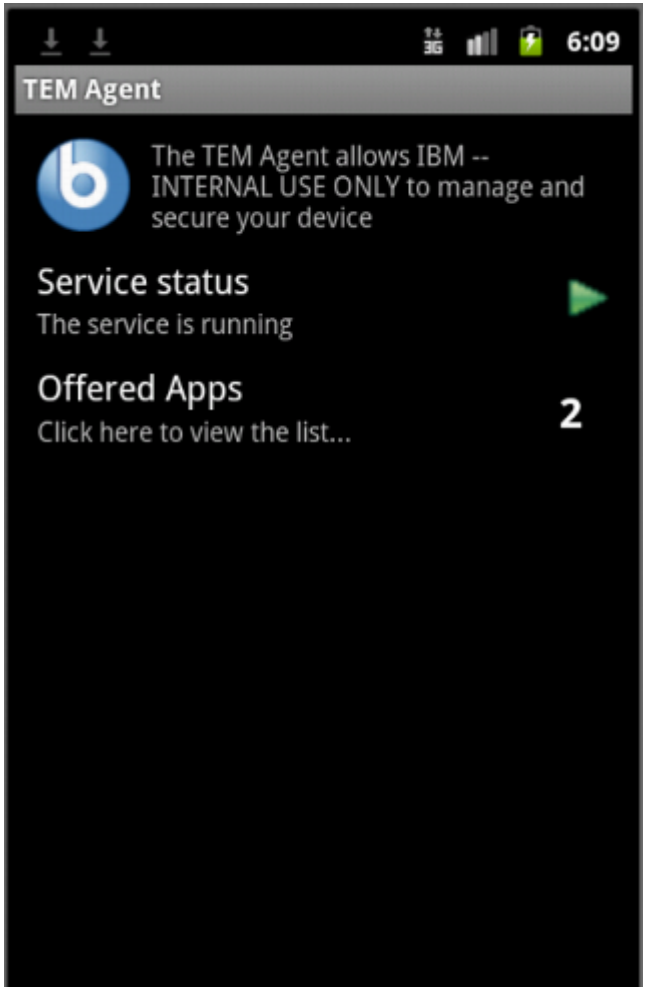

設定檔詳細資料
建立新的配置設定檔
設定檔類型：
APN
APN
應用程式鎖定（僅
認證
電子郵件
Exchange Activ
匯入配置設定檔
選取要匯入的未
匯入供應設定檔
選取從 Apple 匯入的供應設定檔
下一步
Create Fixlet
Name:
Deny Email Access For Devices which have not checked in to TEM
Create in site:
Master Action Site
Create in domain:
Mobile Device Management
Description
Actions
Relevance
Properties
Description
This task will deny targeted mobile devices access to their email server (Lotus Traveler or Microsoft Exchange). Use to restore access.
Actions
Click here to deny email access.
OK
Cancel

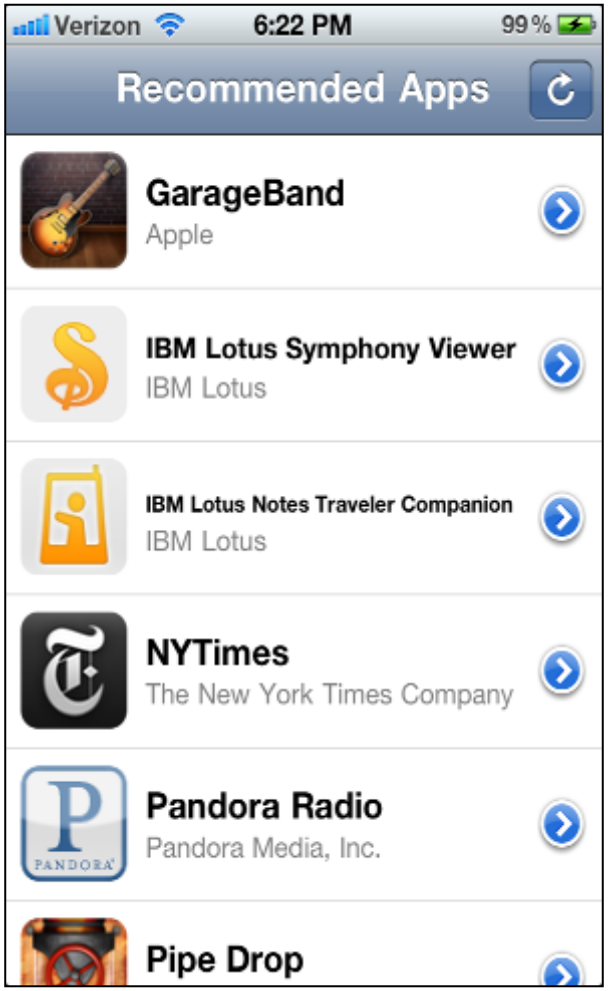
Email 設定

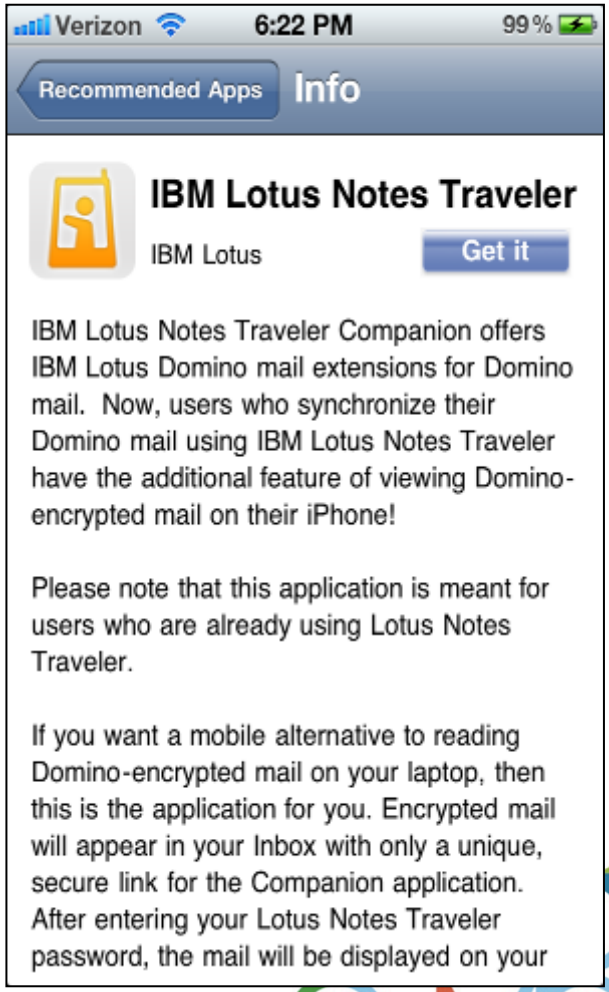

採取行動
名稱:
Profile "com.ib
預設:
Default
目標
執行
使
目標
以下清單中選定的
具有以下樹中所選
以下名單中指定的
適用電腦 (2)
iPad
信箱
收件匣
所有收件匣 88
Gmail 39
alanlai gmail 49
帳號
Gmail 39
alanlai gmail 49
行動裝置管理
預設...
刪除預設...
CPU

Enterprise apps

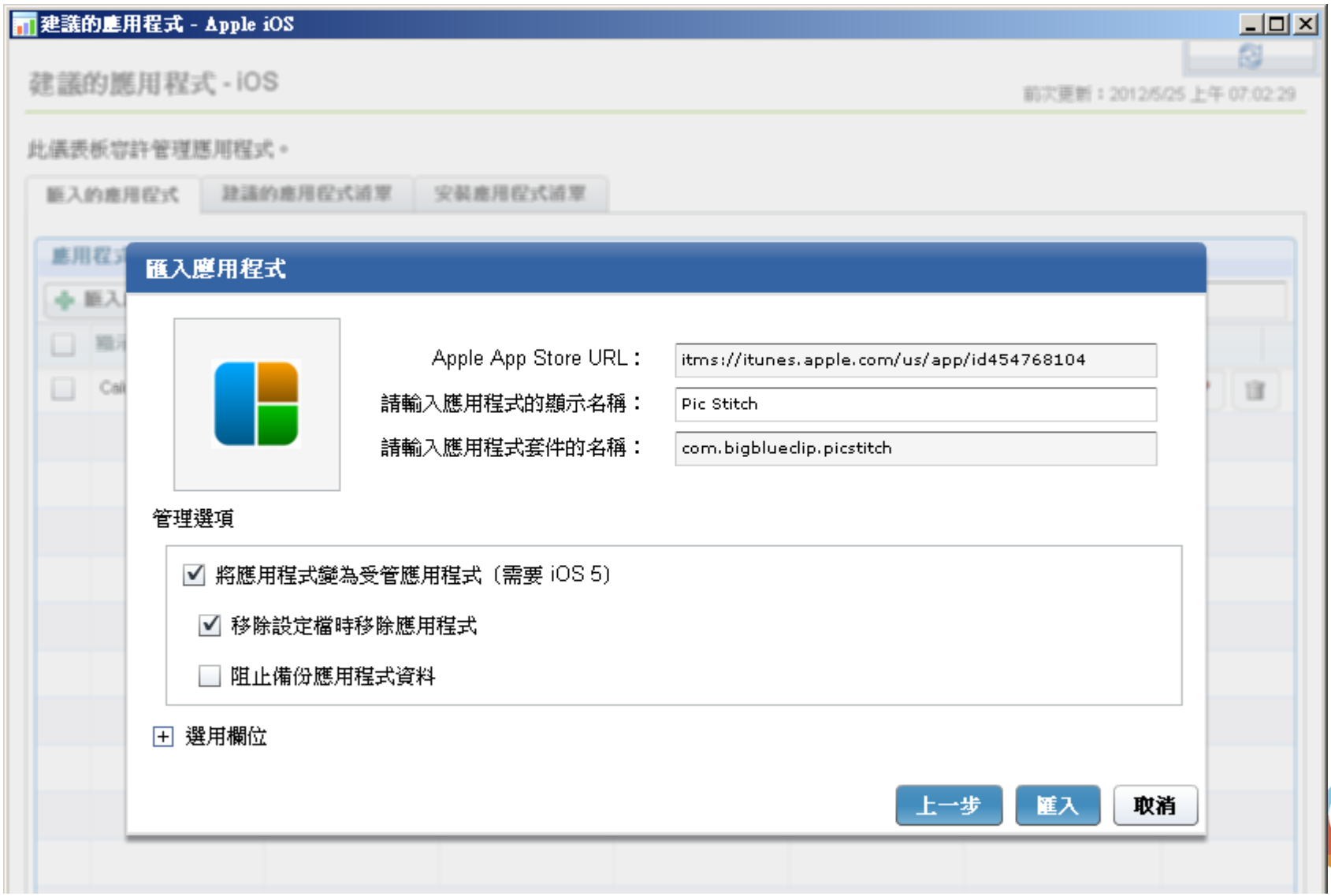
派送APP Store/Market的APP或是APK,IPA檔案





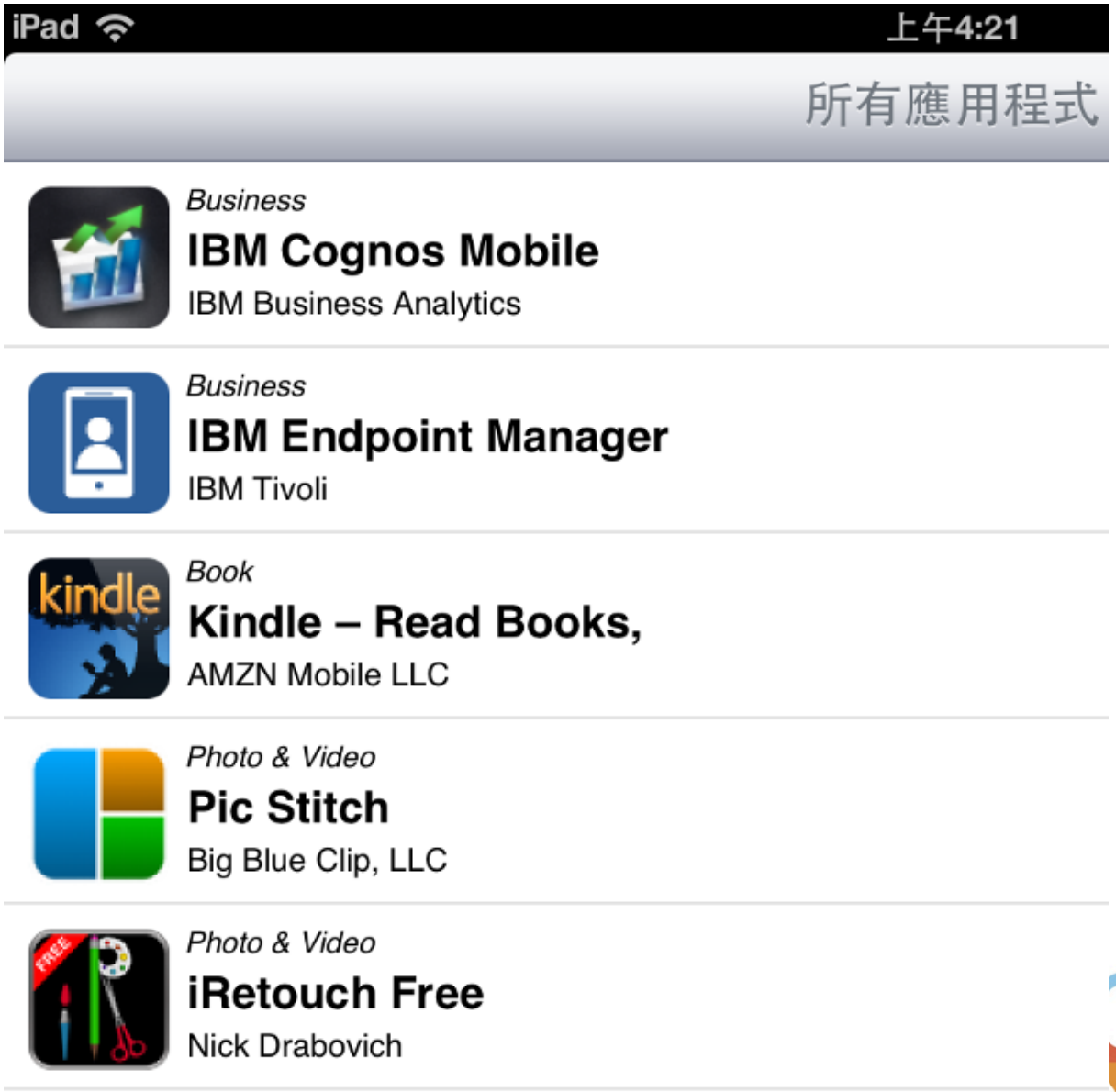


Apps Distribution



Apps Distribution

使用者接獲推送通知
安裝APP



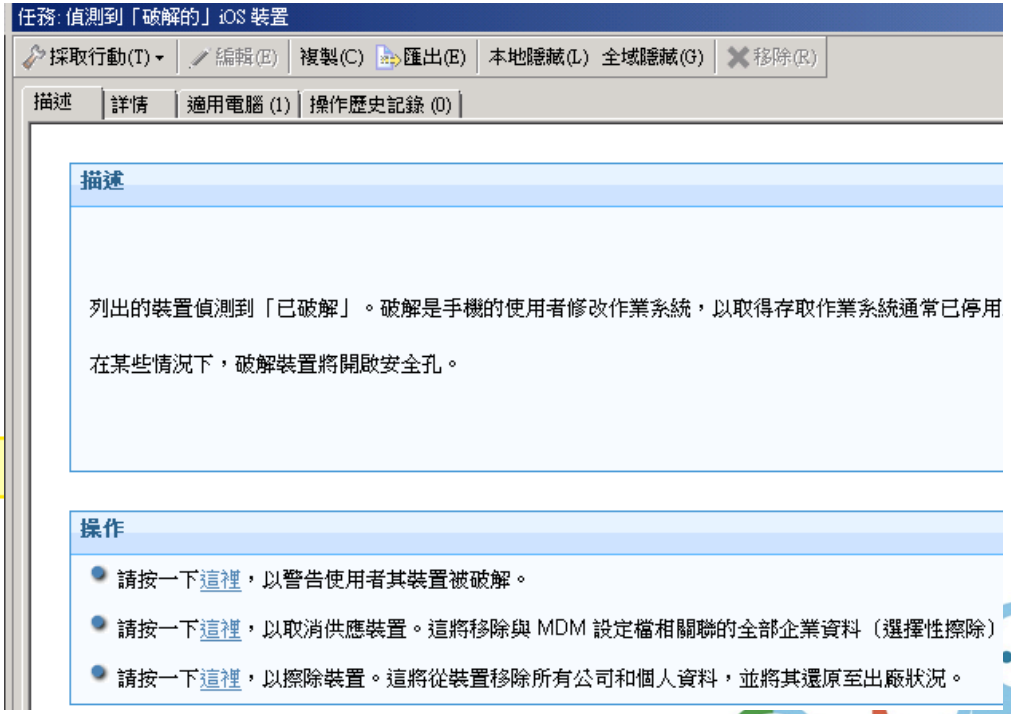
Self-Service Portal

Self-Service Portal

裝置定位
鎖定螢幕
清除密碼
移除裝置
選擇性移除

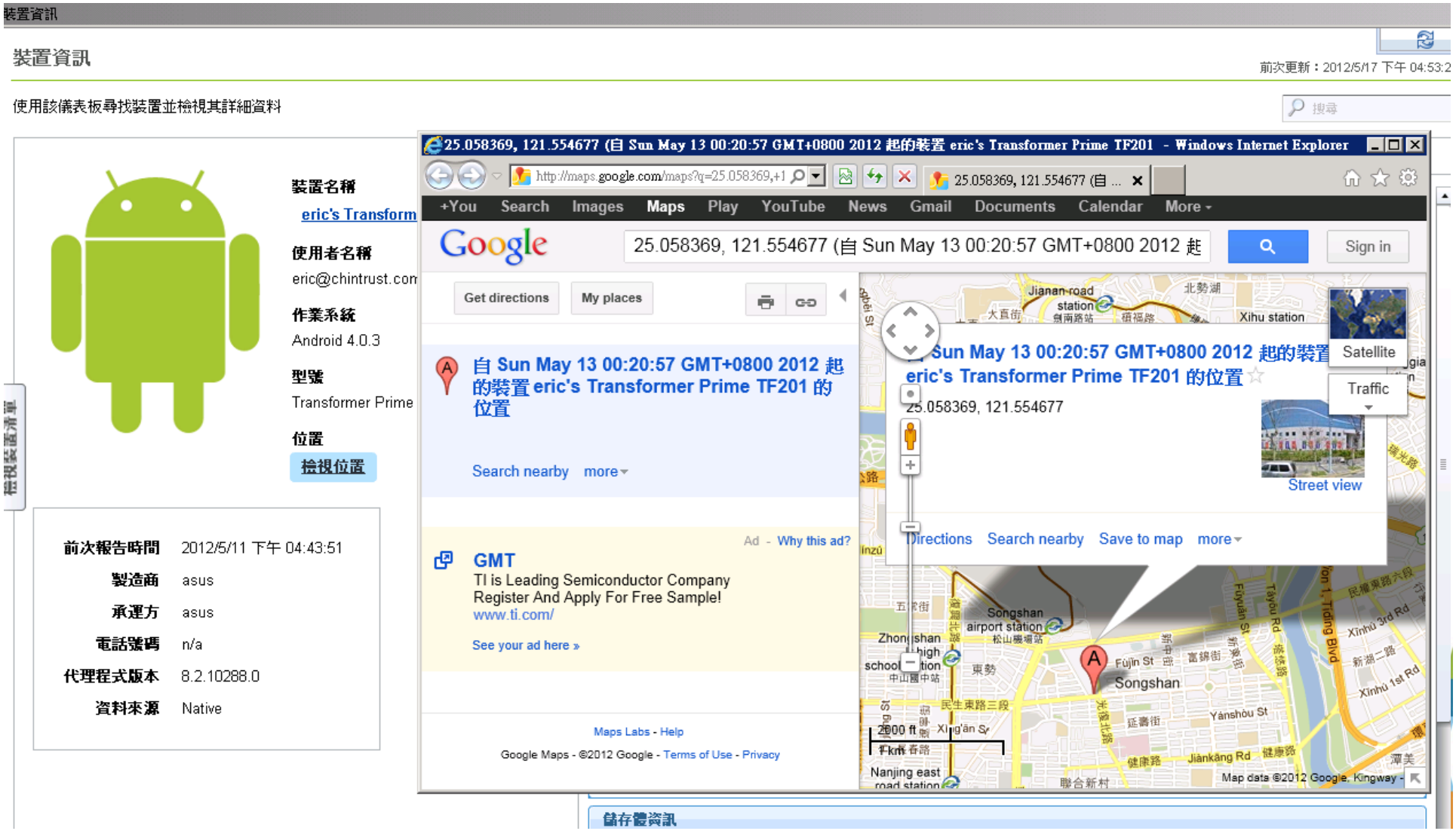
裝置破解偵測(JailBreak/root)

發現JB可傳送訊息警告.



GPS Location

–直接在畫面上點選檢視位置，則可開啟GPS地圖.

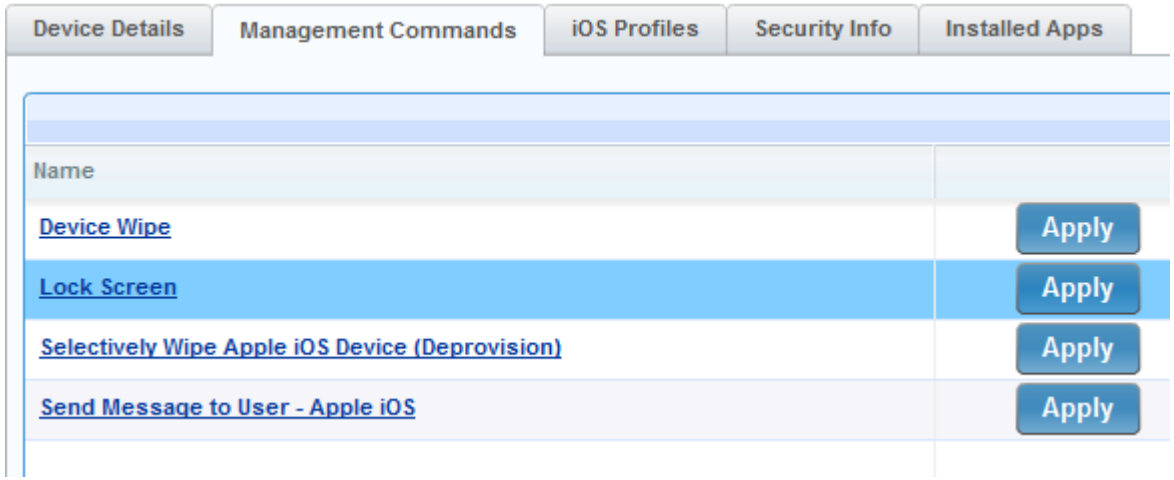


行動裝置管理挑戰與管理

MDM挑戰	TEM for MDM解決方案
BYOD行動裝置怎麼管理	由公司派送WIFI,VPN,MAIL設定 部署軟體 自助服務 偵測並管理越獄裝置
若手機遺失，如何處理?	訊息告知、密碼原則控制(pin length, timeout, wipe after failed login, etc.) 和遠端移除裝置
當員工拿行動裝置離開公司時，如何處理敏感資料外洩可能	離開公司時啟用行動裝置加密、選擇性擦除
面對快速更新的行動裝置 OS/apps ，如何管理行動裝置軟體?	黑名單軟體管理、白名單軟體管理(建議安裝軟體) 、禁止安裝軟體
行動設備數量多，資產如何管理	硬體資產管理 軟體資產管理

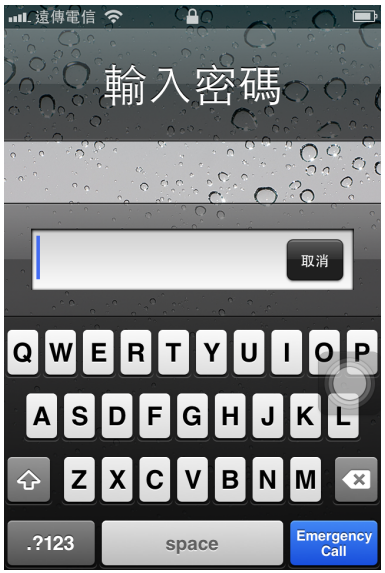
裝置遺失處理

- 發送訊息,請求歸還
- 鎖定裝置
- **SD卡加密**
- 抹除裝置



被告知行動裝置移失時，則請TEM for MDM管理員執行以下方式

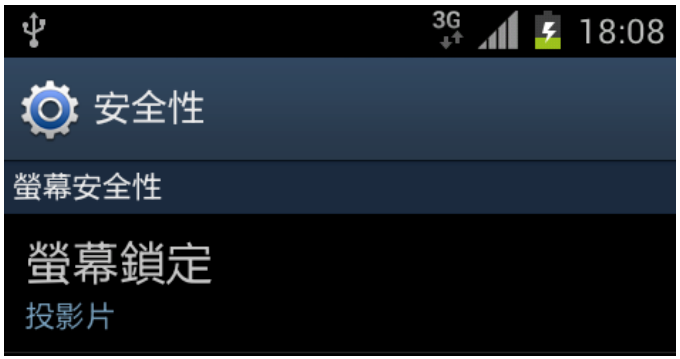
傳送訊息警告拾獲者
立刻歸還裝置

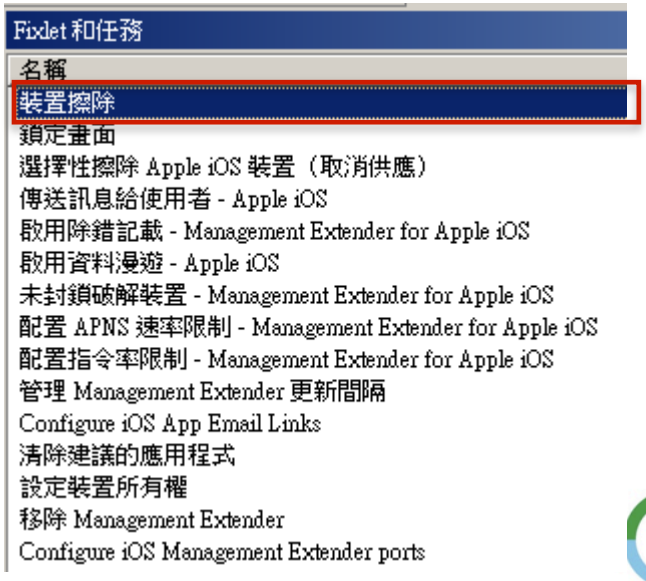


passwd policy設定

- 高強度密碼(包括英文單字和4位元以上)
-10 次失敗即鎖定
- 失敗超過次數移除手機內容

強制鎖定螢幕





失敗超過次數移除手機內容

或手動執行裝置移除內容

Wipe回原廠設定值

儲存體,SD卡強制加密

–可設定儲存體,SD卡加密，並通知用

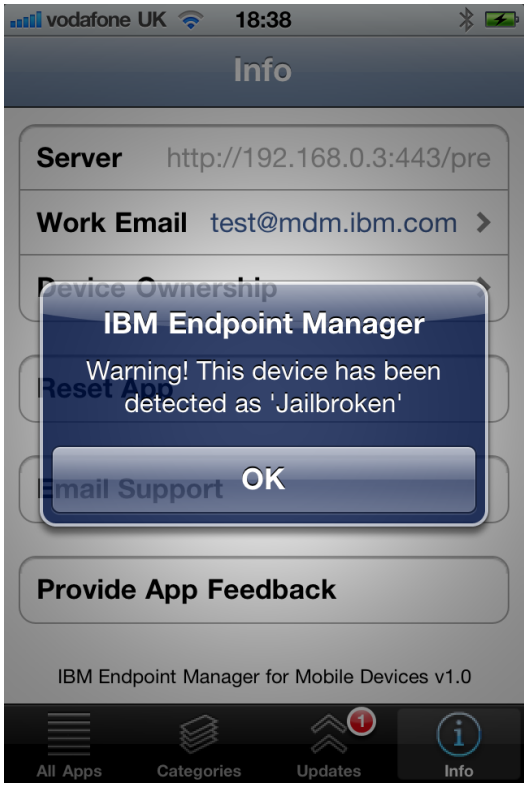
行動裝置管理挑戰與管理

MDM挑戰	TEM for MDM解決方案
BYOD行動裝置怎麼管理	由公司派送WIFI,VPN,MAIL設定 部署軟體 自助服務 偵測並管理越獄裝置
若手機遺失，如何處理?	訊息告知、密碼原則控制(pin length, timeout, wipe after failed login, etc.) 和遠端移除裝置
當員工拿行動裝置離開公司時，如何處理敏感資料外洩可能	離開公司時啟用行動裝置加密、選擇性擦除
面對快速更新的行動裝置 OS/apps ，如何管理行動裝置軟體?	黑名單軟體管理、白名單軟體管理(建議安裝軟體) 、禁止安裝軟體
行動設備數量多，資產如何管理	硬體資產管理 軟體資產管理

避免資料被竊

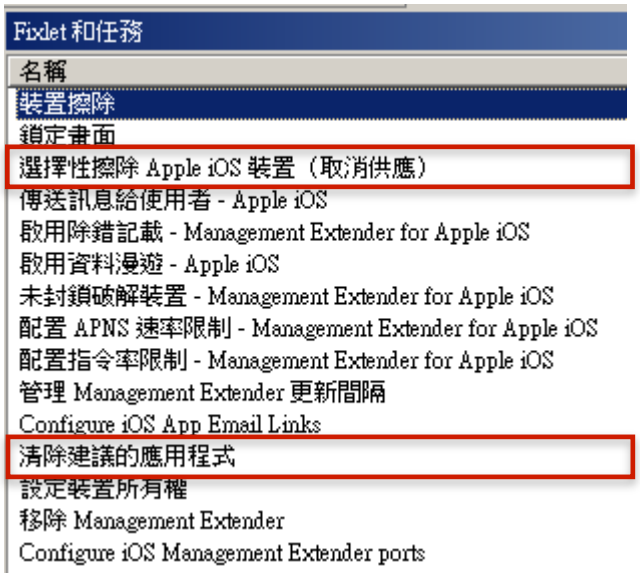
-移除email / 行事曆
-VPN設定 / WIFI設定
-MDM管理的軟體

當資料有遭竊疑慮或被JailBreak(JB)則可使用Selective Wipe選擇性移除，
僅移除企業資料、app和存取企業內網管道.



1

傳送訊息警告持有人JB違反公司規定



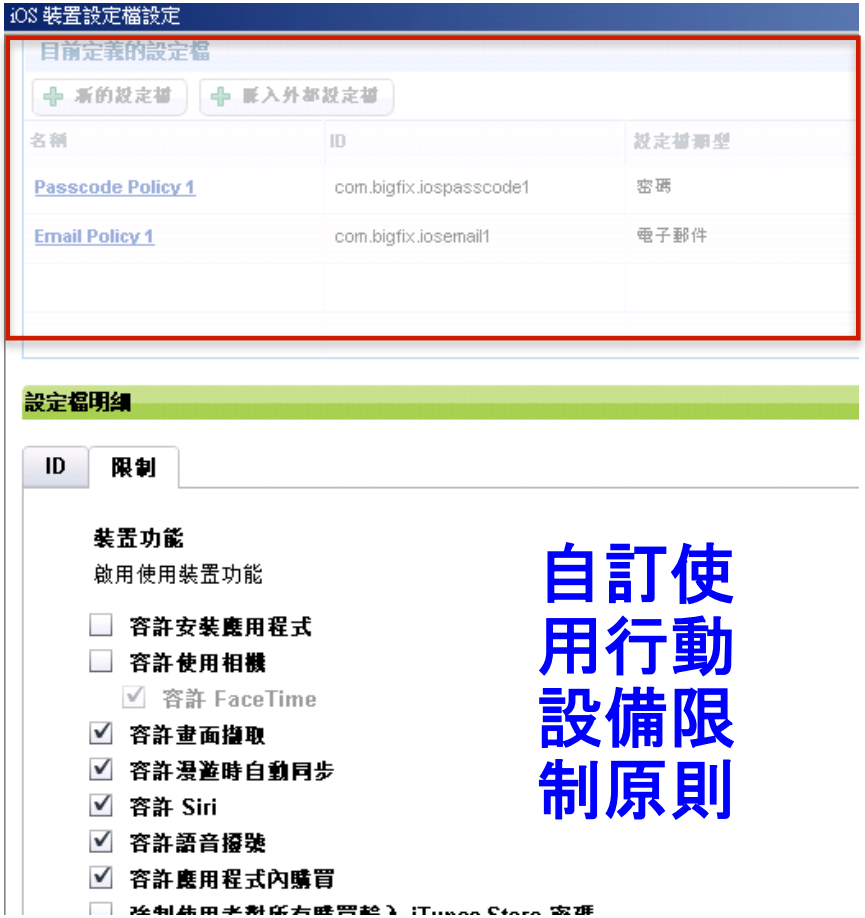
2

選擇性移除

Security Profile

可依照需求自行定義email policy / VPN policy / password policy / Email

Policy Profile設定檔可採加密方式，禁止竄改.



自訂使用行動設備限制原則

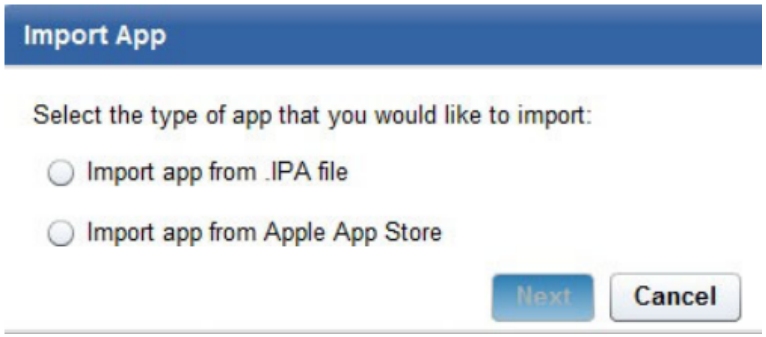
例如passwd policy 原則

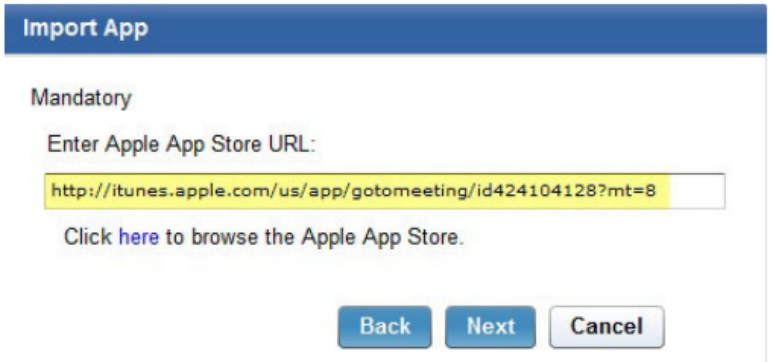
-限制使用高強度密碼，鎖定簡意密碼

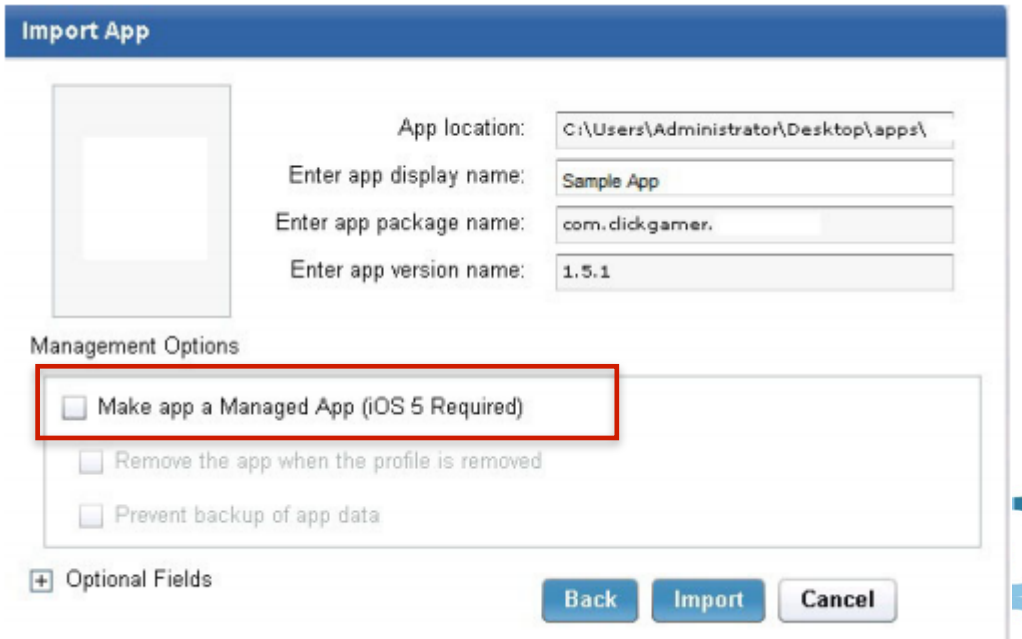
應用程式與資料安全

受管理的應用程式可在TEM上import apps提供給用戶下載使用.

勾選為受管理應用程式(Managed App)則可透過TEM安裝、移除，當mobile client profile被移除時，則此軟體一併自動移除.







Email 設定


電子郵件
用於存取電子郵件帳戶的通訊協定
IMAP
路徑字首：
使用者顯示名稱
使用者的名稱（例如，"John Appleseed"）
[set on device]
電子郵件位址
帳戶的位址（例如，"john@company.com"）
[set on device]
允許移動
允許使用者從此帳戶移動訊息
停用同步化最近的郵件
此帳戶不會進行同步化最近的位址
是否可以由其他Mail轉寄

Email 設定

使用者名稱
用來連接至伺服器取得外寄郵件的使用者名稱

鑑別類型
用於外寄郵件伺服器的鑑別方法
無

密碼
用於外寄郵件伺服器的密碼

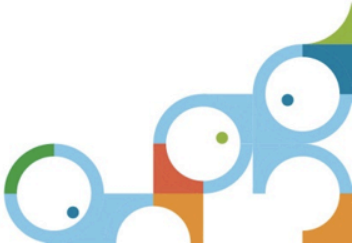
與送入相同的送出密碼
SMTP 鑑別會使用與 POP/IMAP 相同的密碼

僅在郵件中使用
僅在郵件應用程式中從此帳戶傳送外寄郵件

使用 SSL
透過 Secure Sockets Layer 傳送外寄郵件

使用 S/MIME
使用 S/MIME 加密傳送外寄郵件

是否可以由其他APP使用



行動裝置管理挑戰與管理

MDM挑戰	TEM for MDM解決方案
BYOD行動裝置怎麼管理	由公司派送WIFI,VPN,MAIL設定 部署軟體 自助服務 偵測並管理越獄裝置
若手機遺失，如何處理?	訊息告知、密碼原則控制(pin length, timeout, wipe after failed login, etc.) 和遠端移除裝置
當員工拿行動裝置離開公司時，如何處理敏感資料外洩可能	離開公司時啟用行動裝置加密、選擇性擦除
面對快速更新的行動裝置 OS/apps ，如何管理行動裝置軟體?	黑名單軟體管理、白名單軟體管理(建議安裝軟體) 、禁止安裝軟體
行動設備數量多，資產如何管理	硬體資產管理 軟體資產管理

黑名單軟體管理可將用戶行動裝置設備定義黑名單標籤

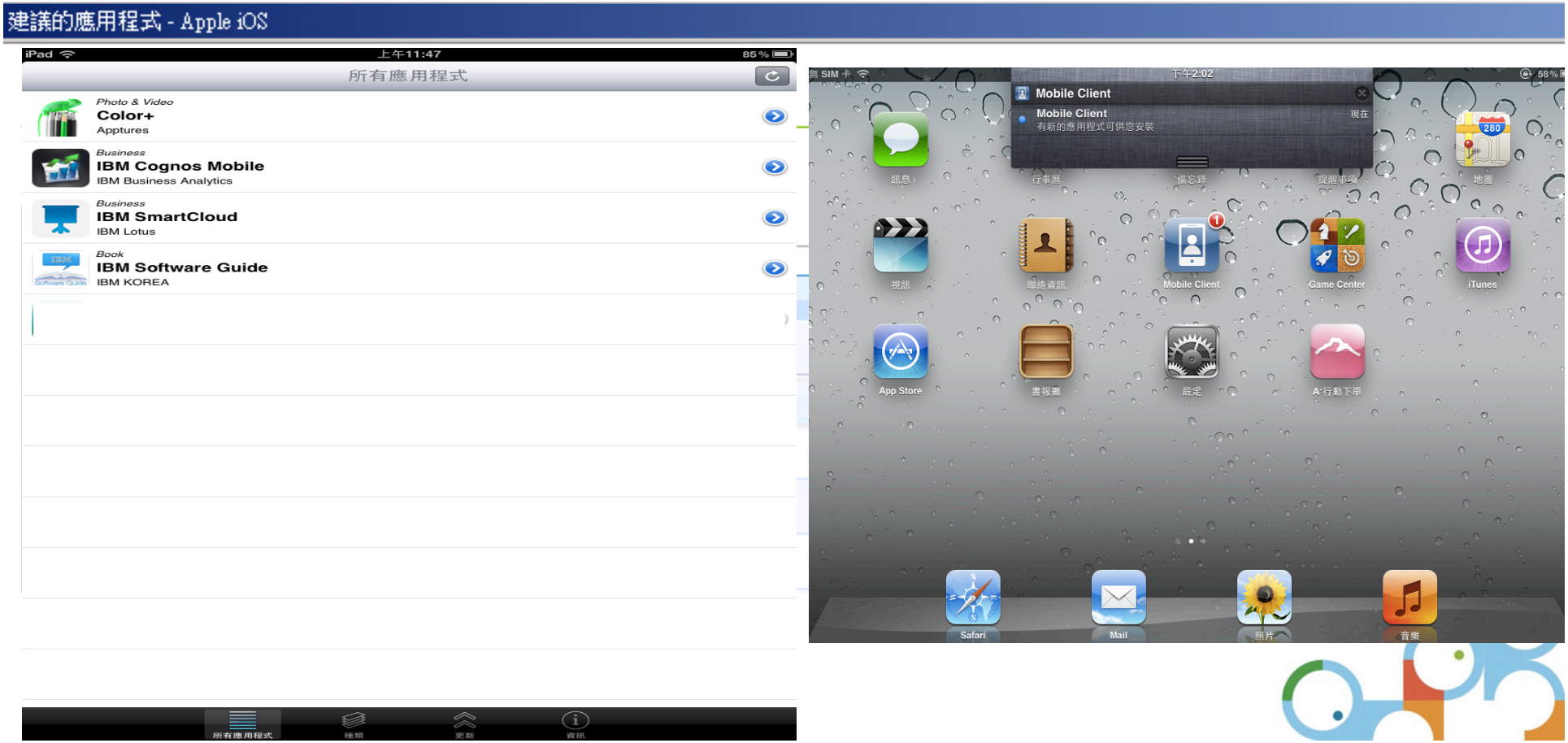
可將特定軟體列為黑名單標籤，方便列管，透過此列管產出報表.
也可依此將其他性軟體分類(例如 私人、企業、...方便報表產出追蹤)

顯示名稱	標籤	套件名稱	說明	版本	電腦計數
Facebook	列入黑名單	com.facebook.Facebook		4110.0	3
台灣明星3缺1	列入黑名單	com.igs.mjstar31		1.0.2	1
AcePlayer		com.ranysoft.aceplayer		1.7	1
Taiwan		com.garmin.onboard.Taiwan		2.2.0	1
GPlayer		com.ginkgo.gplayer		1.0.9	1
BannerFlo		com.fossilsoftware.bannerflo		1.4	1
BookReader		com.readdle.Books		1.2.1	1
玉山銀行		tw.com.ESunbank.mobilebanking.releas		3.0.6417	2
Find Friends		com.apple.mobileme.fmf1		1.1	2
pick		jp.naver.pick		2.4.0	1
TunesMate		com.wizsoft.tunesmate		3.0.1	1
SoundHound		com.melodis.soundhound.free		4.5	2
WhatsApp		net.whatsapp.WhatsApp		2.6.10	2
Newsify		com.synsion.Newsify		34	1
foursquare		com.naveenium.foursquare		4.2.3	1
The Hacker		com.angrybugs.hacker		1.2.0	1
PowerCam?		com.wondershare.PowerCam-TM		1.9.1	2

一旦列為特定標籤，如黑名單，即使app重裝也會自動標示標籤

白名單軟體管理(建議的應用程式)可將企業行動裝置軟體集中提供給使用者下載，白名單軟體僅是清單，當用戶點選應用程式時才開始下載安裝

- **白名單軟體可建立群組，配置不同業務性質用戶不同軟體清單**
- **建議軟體清單更新會主動通知用戶**



app管理

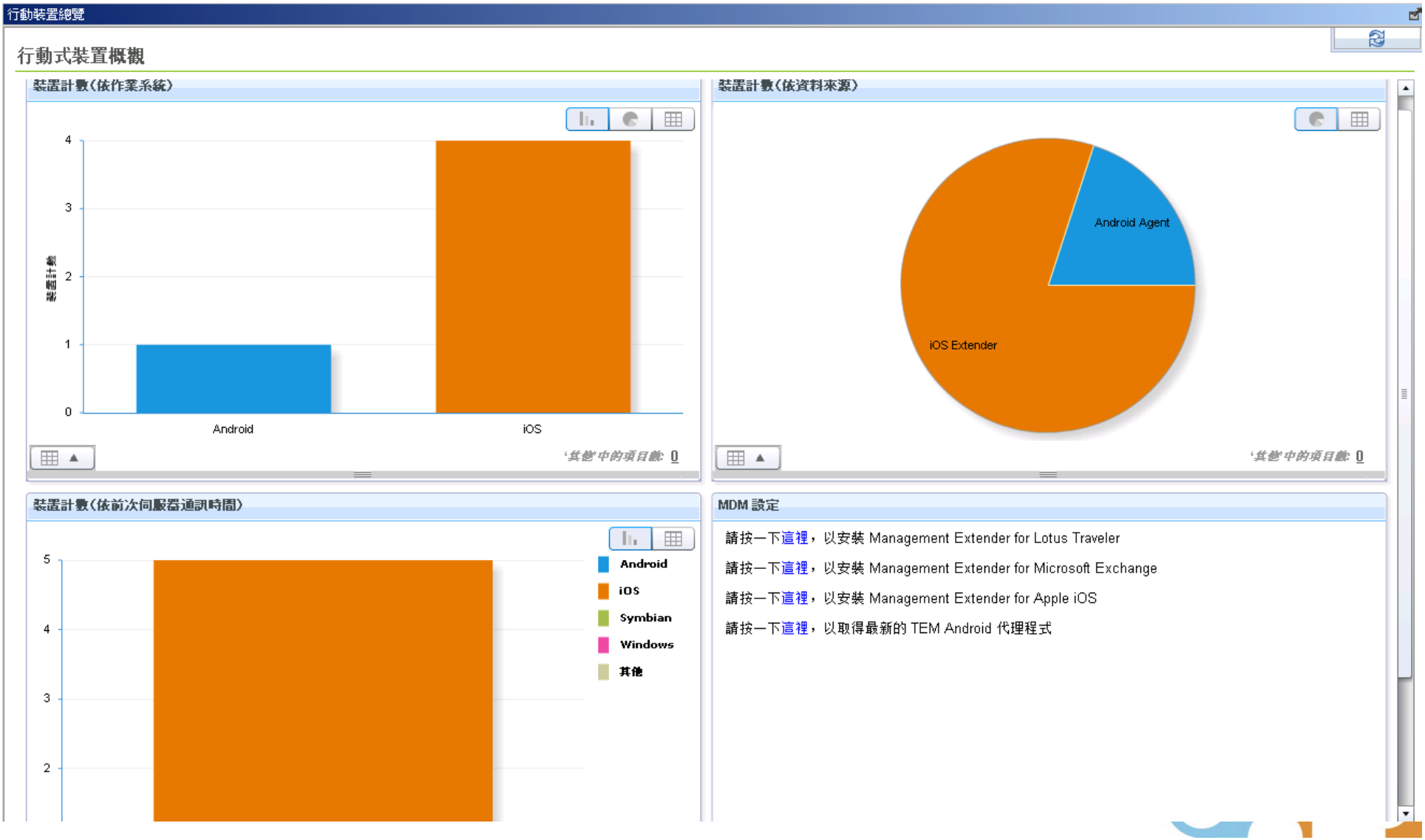
白名單軟體管理可集中push給行動裝置用戶

透過TEM安裝的apps可限制備份到iTune/iCloud，以防資料外洩

行動裝置管理挑戰與管理

MDM挑戰	TEM for MDM解決方案
BYOD行動裝置怎麼管理	由公司派送WIFI,VPN,MAIL設定 部署軟體 自助服務 偵測並管理越獄裝置
若手機遺失，如何處理?	訊息告知、密碼原則控制(pin length, timeout, wipe after failed login, etc.) 和遠端移除裝置
當員工拿行動裝置離開公司時，如何處理敏感資料外洩可能	離開公司時啟用行動裝置加密、選擇性擦除
面對快速更新的行動裝置 OS/apps ，如何管理行動裝置軟體?	黑名單軟體管理、白名單軟體管理(建議安裝軟體) 、禁止安裝軟體
行動設備數量多，資產如何管理	硬體資產管理 軟體資產管理

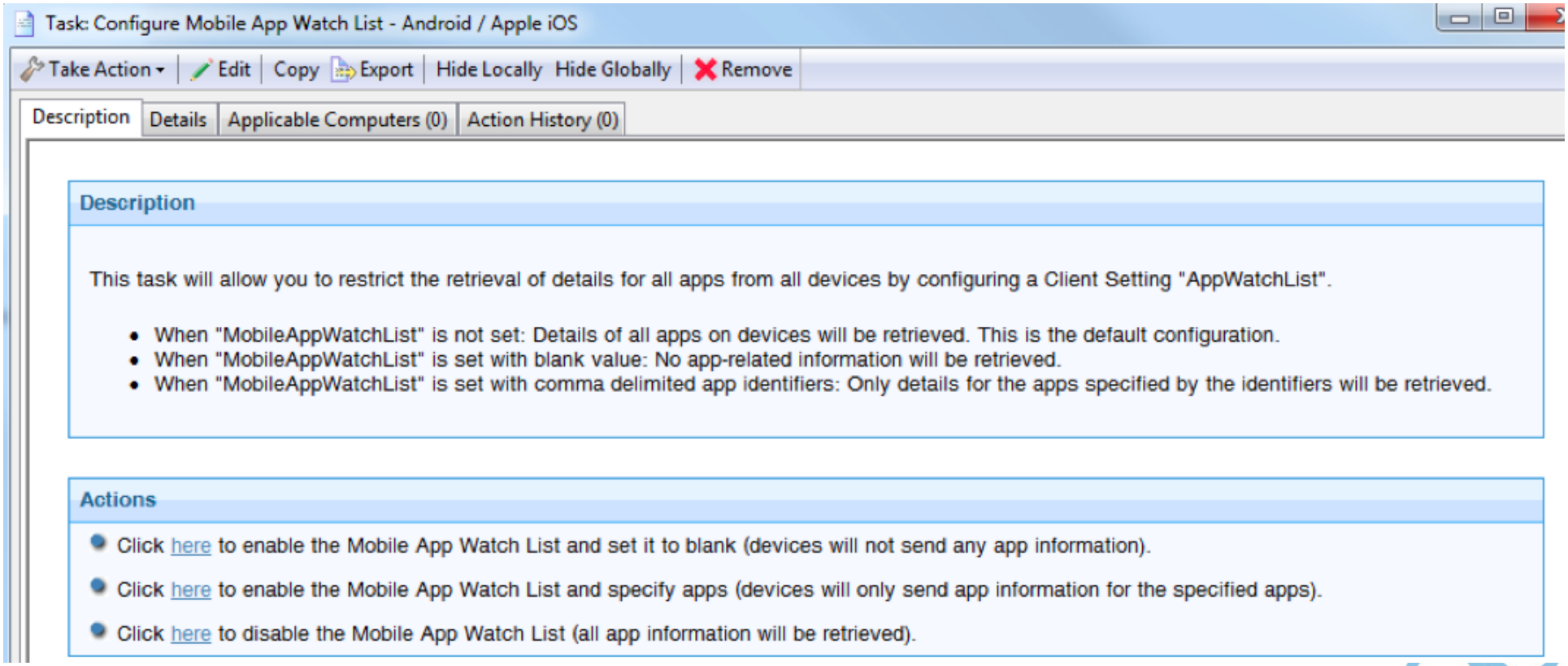
設備基本資訊


行動裝置總覽
行動式裝置概觀
裝置計數(依作業系統)
4
3
2
1
0
裝置計數
Android
iOS
'其他'中的項目數: 0
裝置計數(依資料來源)
Android Agent
iOS Extender
'其他'中的項目數: 0
裝置計數(依前次伺服器通訊時間)
5
4
3
2
Android
iOS
Symbian
Windows
其他
MDM 設定
請按一下這裡，以安裝 Management Extender for Lotus Traveler
請按一下這裡，以安裝 Management Extender for Microsoft Exchange
請按一下這裡，以安裝 Management Extender for Apple iOS
請按一下這裡，以取得最新的 TEM Android 代理程式

立即取得行動裝置資產資訊與軟體資產

行動裝置資產資訊隱私

若行動裝置設備屬於BYOD，員工有資產隱私權，可設定app watch list，僅收集是否有特定黑名單app或是公司付費app資產.



Why TEM-based Approach to MDM

- "Organizations are starting to treat smartphones (and now tablets) the same way they treat PCs"
- "Organizations…would prefer to use the same tools across PCs, tablets and smartphones, because it's increasingly the same people who support those device types"
- "An increasing number of organizations are supporting mobile devices with the desktop group"

– Gartner, PCCLM Magic Quadrant, January 2011

降低管理成本

- "單一管理介面" 管理 mobile devices, laptops, desktops, servers
- 單一TEM 伺服器可管理 250,000+ devices

快速佈署

- 進一步整合事故問題單系統,CMDBs, etc (Integrated Service Management)
- Cloud-based content delivery model 可快速更新系統軟體，不需重新升級或安裝系統軟體

展現管理效率

- 跨平台Fixlet-based 技術，以最少資源和時間佈署apps 和設備安全政策

Tivoli Endpoint Manager 模組與功能— 更快更智能的端點管理

Tivoli Endpoint Manager (Manage and Secure)

生命週期管理	軟體使用分析管理	安全與法規遵循	Patch管理.	病毒與安全防護	行動裝置管理	電源管理

共同的 Single Agent / Platform / Console

Microsoft Windows • Mac OSX • IBM AIX • HP-UX • Solaris • VMWare ESX Server •
7 versions of Linux • iOS • Android • Symbian • Windows Mobile


桌機/筆電/伺服器 端點

行動 端點

特殊用途 端點

Q & A