

Connect2013



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



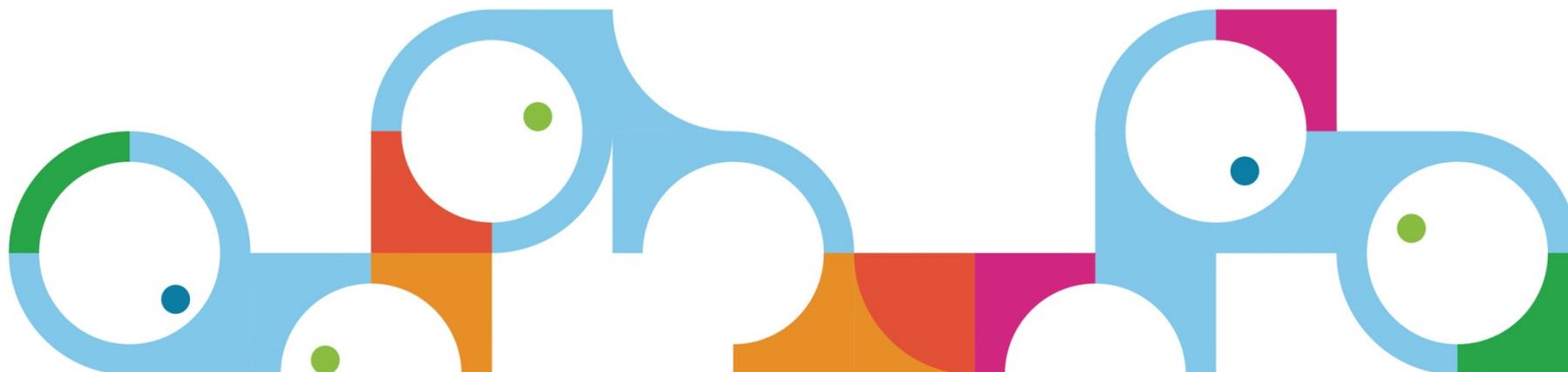
媒體協辦



數位時代 媒體群

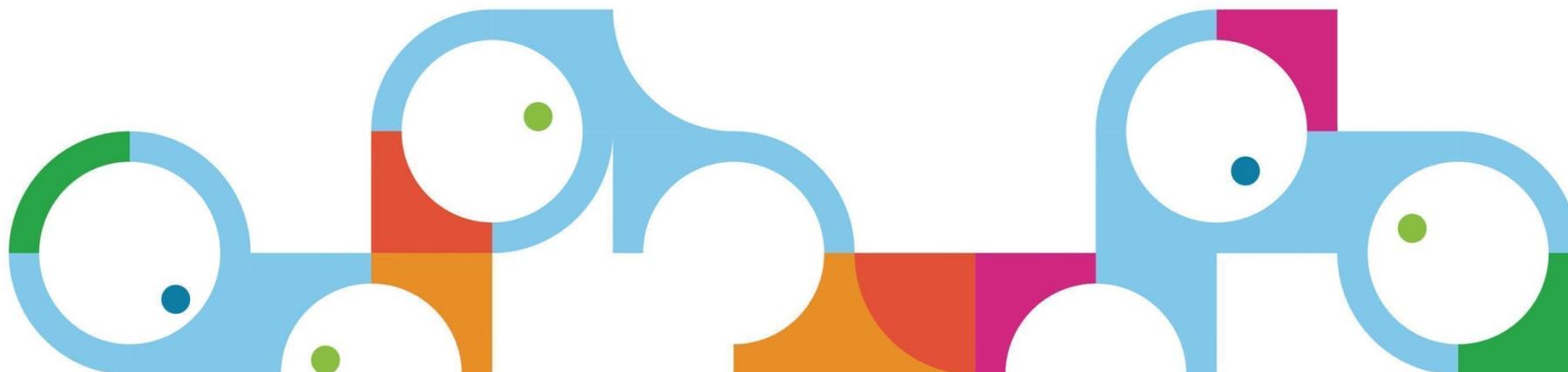
經理人

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!!

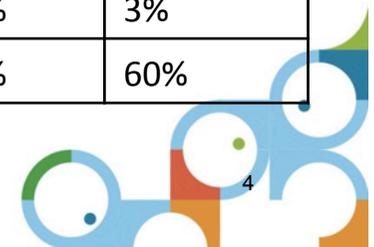
傳統管理模式	行動裝置管理
企業提供所有設備	員工攜帶自己行動裝置設備(BYOD)
Desktop/Laptop種類有限	行動裝置設備種類、品牌甚多
IT緊密控制軟體和安全	User自行控制自己的設備
IT控制軟體使用、升級	設備、OEM方式和User可自行安裝升級app/OS

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%

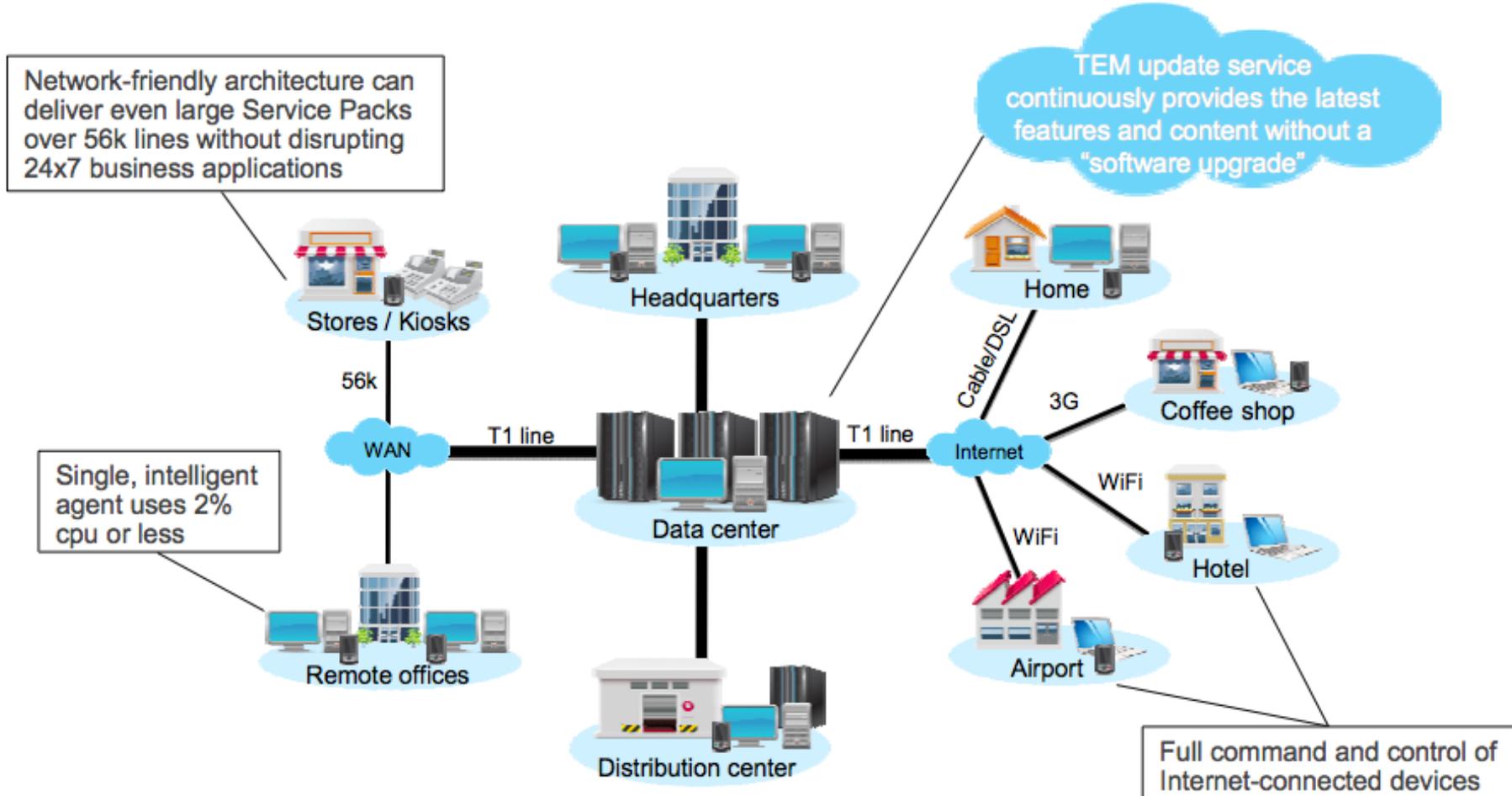
Source: Gartner



IBM MobileFirst Portfolio



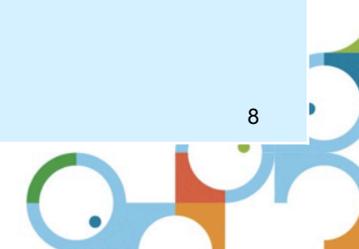
Tivoli Endpoint Manager, built on BigFix technology



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.

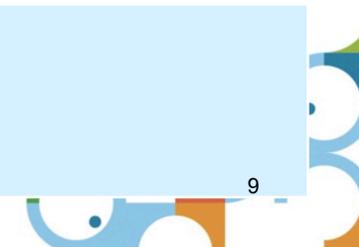
行動裝置管理挑戰與管理

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



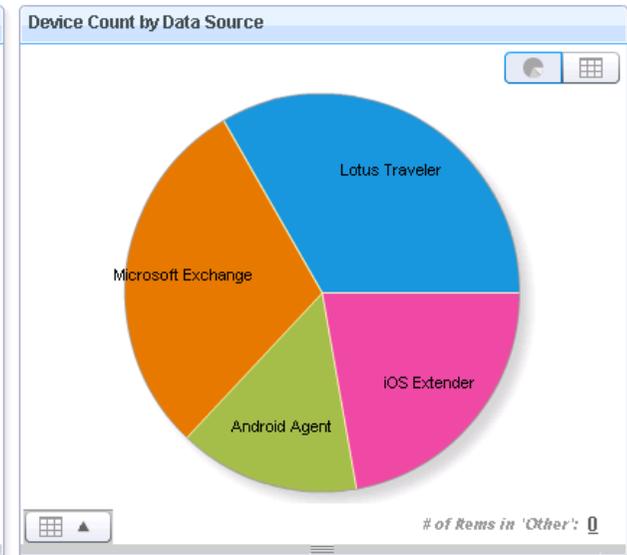
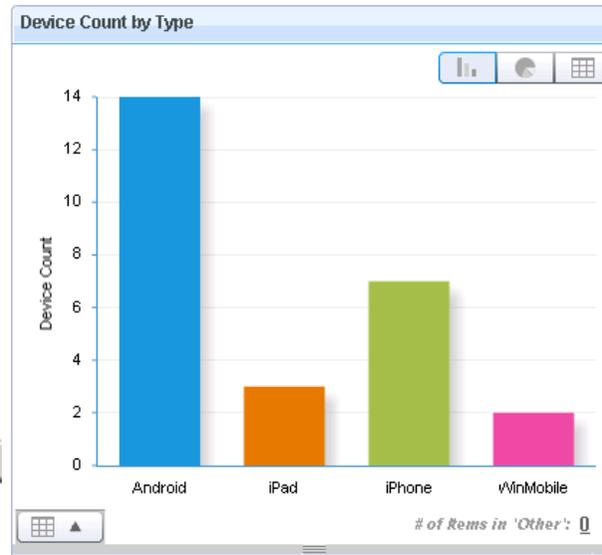
行動裝置管理挑戰與管理

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
0000000000000000	n/a	unknown	sdk	generic	3619CE929CAA4AC79B47622F
358224040002945	n/a	Lenovo	ThinkPad Tablet	Lenovo	C85ACE3BC26C448B97594320
7T041BQXA45	Ben's iPhone4	Apple	iPhone	AT&T	3f50b4cbbaf3386c84c866278b
81938CMX3NP	Estie's iPhone	Apple	iPhone	AT&T	8a8e9890ebca2f6a3d413b268
889393M83N5	Scot's iPhone	Apple	iPhone	Vodafone IT	94d10c4c5012a084c781ce357
99000033060984	n/a	HTC	ADR6400L	verizon_ww	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

前一頁 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：

匯入配置設定檔

選擇要匯入的未認證電子郵件 Exchange Activ

匯入供應設定檔

選擇從 Apple 匯入的供應設定檔

下一步

Create Fixlet

Name: Create in site:

Create in domain:

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

The screenshot shows the Mail app interface on an iPad. The background window displays settings for a profile named "Profile 'com.it...'", with a "預設" (Default) option selected. Under the "目標" (Targets) section, there are three radio button options: "以下清單中選定的" (Selected in the list below), "具有以下樹中所選" (Selected in the tree below), and "以下名單中指定的" (Specified in the list below). The "適用電腦 (2)" (Applicable computers (2)) option is selected, and a red arrow points from it to the foreground window.

The foreground window, titled "信箱" (Inbox), shows a list of mailboxes under the heading "收件匣" (Inboxes):

- 所有收件匣 (All Inboxes) with 88 messages
- Gmail with 39 messages
- alanlai gmail with 49 messages

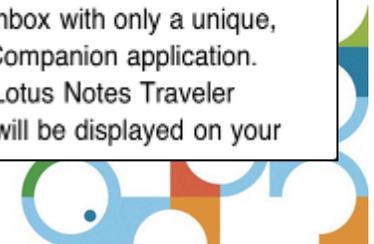
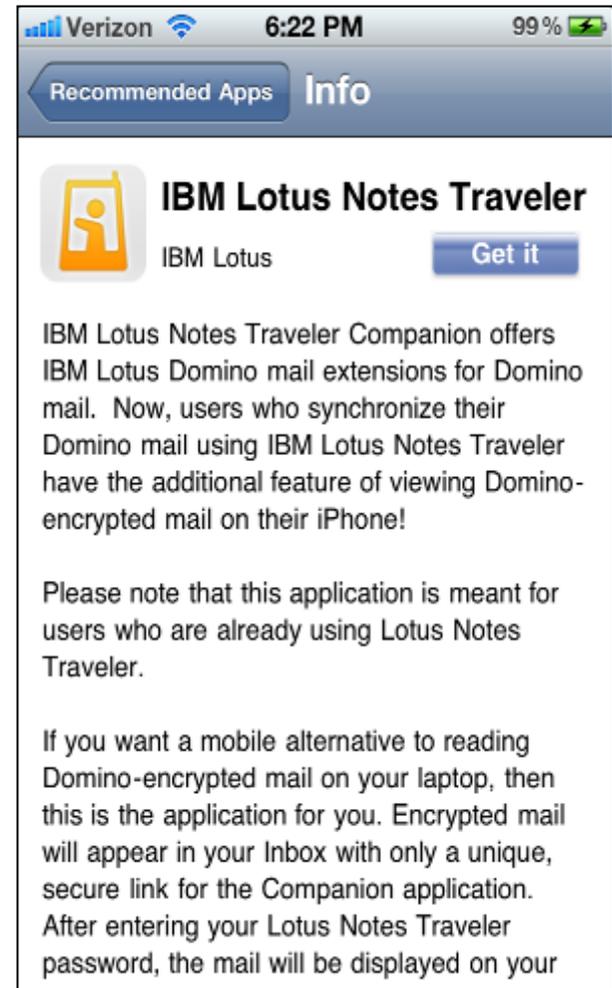
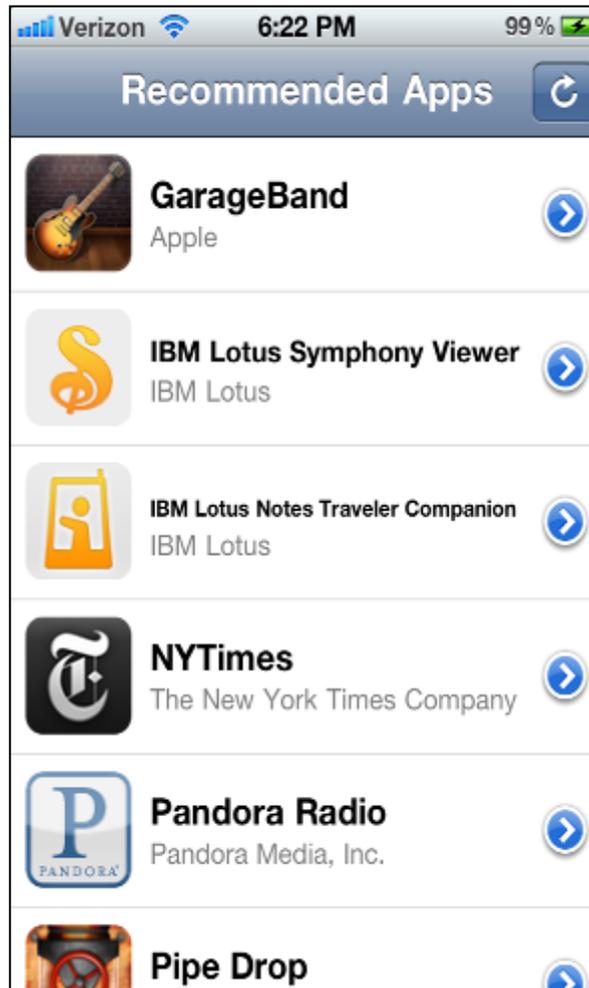
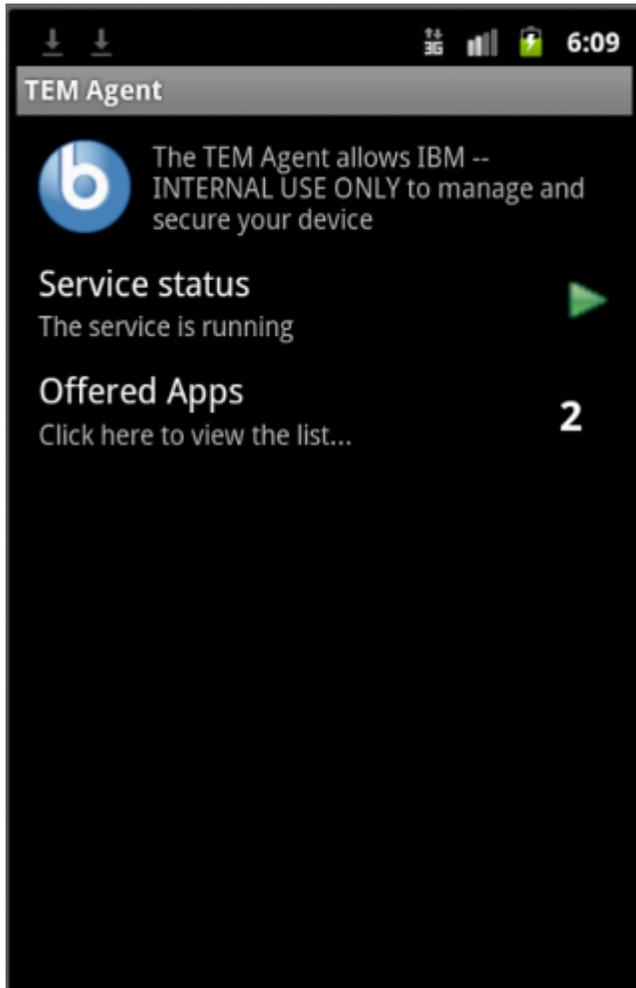
Below the inboxes, under the heading "帳號" (Accounts), there are two accounts listed:

- Gmail with 39 messages
- alanlai gmail with 49 messages



Enterprise apps

派送APP Store/Market的APP或是APK,IPA檔案



Apps Distribution

The screenshot shows a web-based management interface for Apple iOS applications. The main window is titled "建議的應用程式 - Apple iOS" and includes a refresh button and a timestamp "前次更新：2012/5/25 上午 07:02:29". Below the title bar, there are three tabs: "匯入的應用程式", "建議的應用程式清單", and "安裝應用程式清單". The "匯入的應用程式" tab is active, displaying a list of applications with a "+" icon to add new ones. A modal dialog box titled "匯入應用程式" is open, allowing the user to add a new application. The dialog contains the following fields and options:

- Apple App Store URL:**
- 請輸入應用程式的顯示名稱:**
- 請輸入應用程式套件的名稱:**
- 管理選項:**
 - 將應用程式變為受管應用程式 (需要 iOS 5)
 - 移除設定檔時移除應用程式
 - 阻止備份應用程式資料
- 選用欄位:** 選用欄位

At the bottom of the dialog, there are three buttons: "上一步", "匯入", and "取消".



Apps Distribution

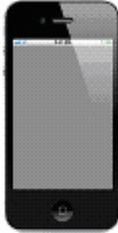
使用者接獲推送通知
安裝APP



Self-Service Portal

 **Select a Device** zak@bigfix.com [Logout](#)

 **Zak's adr6425lvw**
ADR6425LVW
Android 2.3.4

 **Zak's iphone**
iPhone 3G
iOS 4.2.1

 **Zak's kindle fire**
Kindle Fire
Android 2.3.4

 **Zak's sdk**
Android Emulator
Android 4.1.1

 **Zak's adr6425lvw**
ADR6425LVW
Android 2.3.4

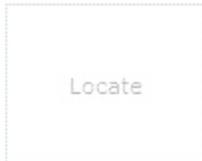


Self-Service Portal

Management

Security

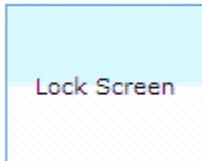
Details



Use this to locate your device on a map.

Location not tracked

裝置定位
鎖定螢幕
清除密碼
移除裝置

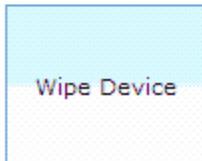


This will lock your device's screen, requiring that you enter a password to access the device again (if a password has been set).

This is usually something you would do if you think you've lost your device, and dont want anyone using it while you look for it.

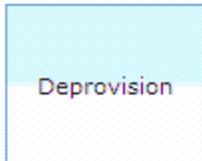
Status: Successfully Sent!

選擇性移除



This will remove all information and apps from your device, and restore it to its factory default settings. This device will have to be re-enrolled once it is wiped.

Do this if your device is lost or stolen. Once a device is wiped, it's old settings and information cannot be recovered.



This will remove your device from management, and selectively wipe any data that required management (such as corporate email and apps). Your personal user Apps and data will not be affected.

Do this if you personally own this device, and no longer want it managed through your MDM provider. Note this usually means you will no longer be able to access restricted information (like corprate email) from this device.



裝置破解偵測(JailBreak/root)

裝置資訊

裝置資訊

使用該儀表板尋找裝置並檢視其詳細資料



裝置名稱

使用者名稱

作業系統
Apple iOS 5.0.1

型號
iPhone 4S

位置
不支援位置

⚠ 此裝置已破解

前次報告時間	2012/5/3 下午 05:00:15
製造商	Apple
承運方	中華電信

操作參數

請輸入使用者的警告文字

Jailbroken devices are not allowed to access corporate data.

發現JB可傳送訊息警告.

任務: 偵測到「破解的」iOS 裝置

採取行動(T) 編輯(E) 複製(C) 匯出(E) 本地隱藏(L) 全域隱藏(G) 移除(R)

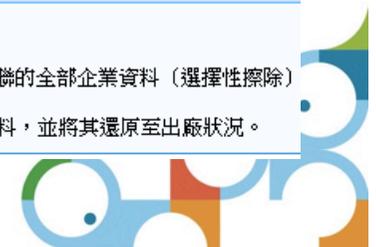
描述 詳情 適用電腦 (1) 操作歷史記錄 (0)

描述

列出的裝置偵測到「已破解」。破解是手機的使用者修改作業系統，以取得存取作業系統通常已停用在某些情況下，破解裝置將開啟安全孔。

操作

- 請按一下[這裡](#)，以警告使用者其裝置被破解。
- 請按一下[這裡](#)，以取消供應裝置。這將移除與 MDM 設定檔相關聯的全部企業資料（選擇性擦除）
- 請按一下[這裡](#)，以擦除裝置。這將從裝置移除所有公司和個人資料，並將其還原至出廠狀況。



GPS Location

– 直接在畫面上點選檢視位置，則可開啟GPS地圖。

裝置資訊

裝置資訊

前次更新：2012/5/17 下午 04:53:2

使用該儀表板尋找裝置並檢視其詳細資料

搜尋



裝置名稱
eric's Transform

使用者名稱
eric@chintrust.com

作業系統
Android 4.0.3

型號
Transformer Prime

位置
[檢視位置](#)

前次報告時間 2012/5/11 下午 04:43:51

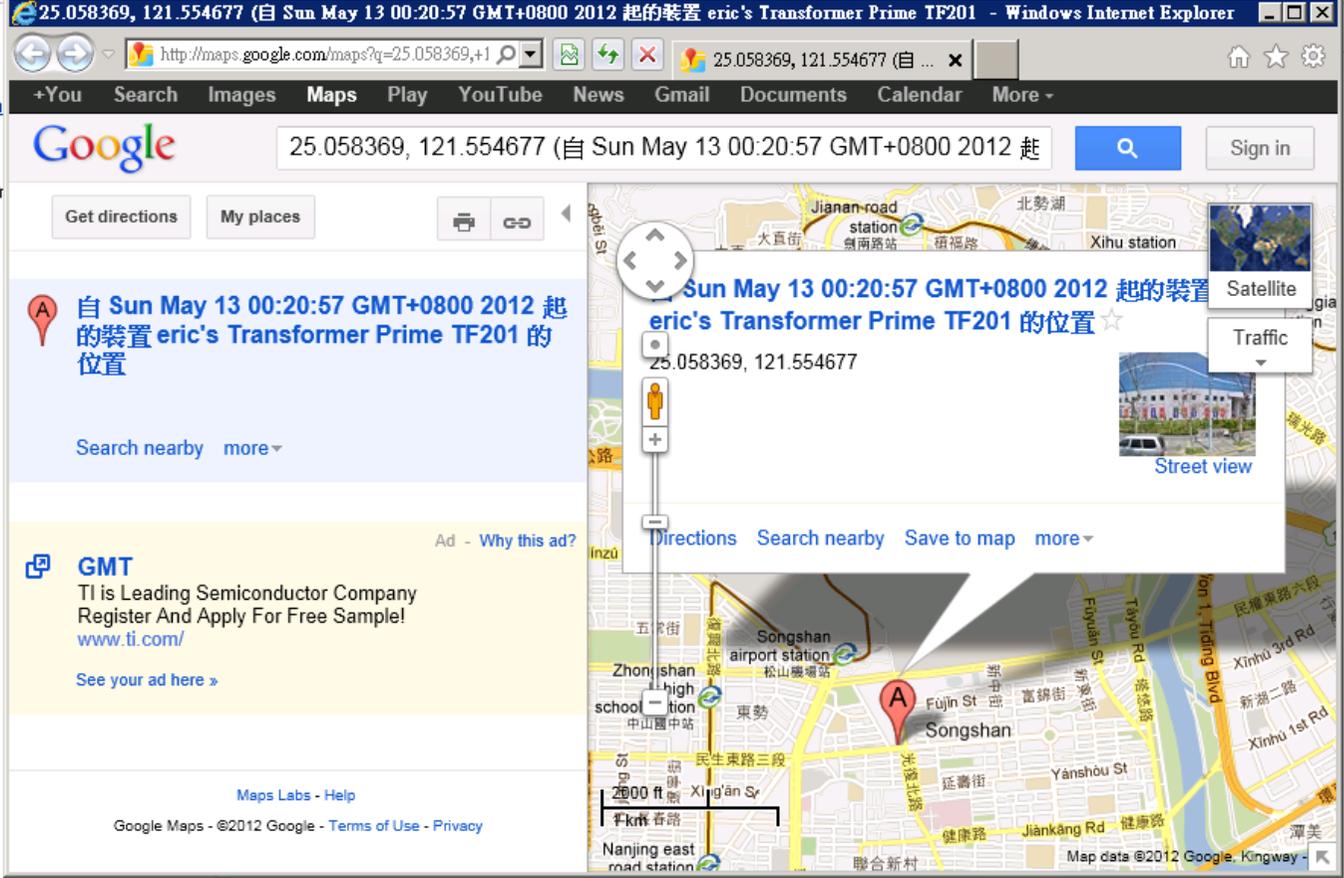
製造商 asus

承運方 asus

電話號碼 n/a

代理程式版本 8.2.10288.0

資料來源 Native



儲存體資訊

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

Device Details	Management Commands	iOS Profiles	Security Info	Installed Apps
Name				
Device Wipe				Apply
Lock Screen				Apply
Selectively Wipe Apple iOS Device (Deprovision)				Apply
Send Message to User - Apple iOS				Apply

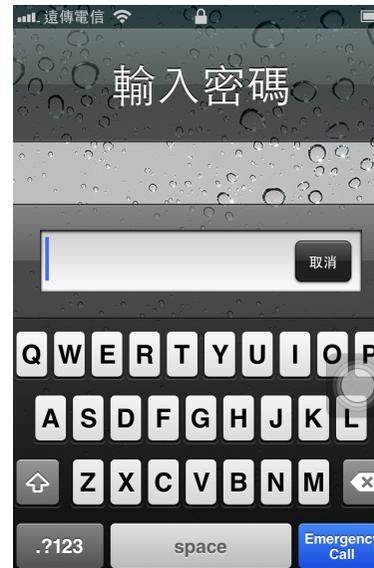


被告知行動裝置移失時，則請TEM for MDM管理員執行以下方式

傳送訊息警告拾獲者
立刻歸還裝置



強制鎖定螢幕



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



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



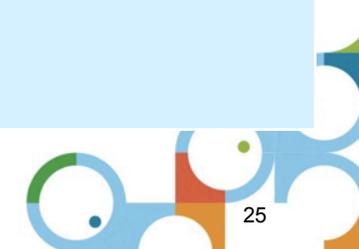
儲存體,SD卡強制加密

–可設定儲存體,SD卡加密，並通知用戶



行動裝置管理挑戰與管理

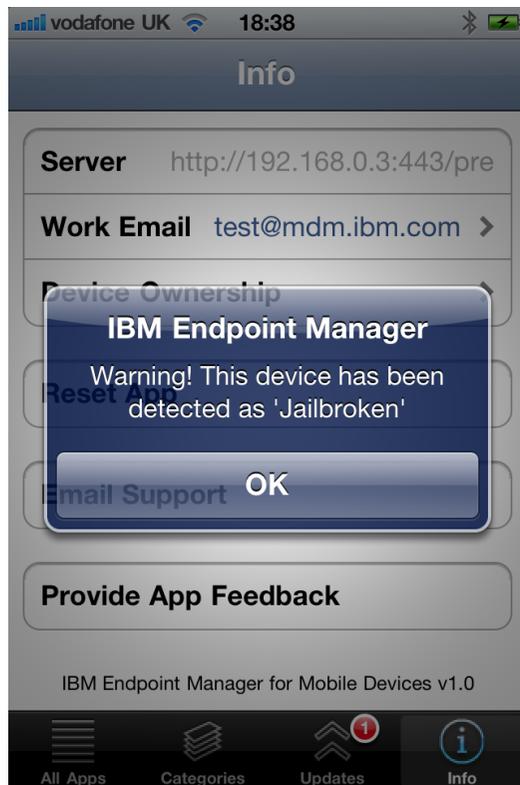
MDM挑戰	TEM for MDM解決方案
BYOD行動裝置怎麼管理	由公司派送WIFI,VPN,MAIL設定 部署軟體 自助服務 偵測並管理越獄裝置
若手機遺失，如何處理？	訊息告知、密碼原則控制(pin length, timeout, wipe after failed login, etc.) 和遠端移除裝置
當員工拿行動裝置離開公司時，如何處理敏感資料外洩可能	離開公司時啟用行動裝置加密、選擇性擦除
面對快速更新的行動裝置 OS/apps，如何管理行動裝置軟體？	黑名單軟體管理、白名單軟體管理(建議安裝軟體)、禁止安裝軟體
行動設備數量多，資產如何管理	硬體資產管理 軟體資產管理



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。

iOS 裝置設定檔設定

目前定義的設定檔

+ 新的設定檔 + 匯入外部設定檔

名稱	ID	設定檔類型
Passcode Policy 1	com.bigfix.iospasscode1	密碼
Email Policy 1	com.bigfix.iosemail1	電子郵件

例如passwd policy 原則

-限制使用高強度密碼，鎖定簡意密碼

設定檔明細

ID	限制
裝置功能	
啟用使用裝置功能	
<input type="checkbox"/>	容許安裝應用程式
<input type="checkbox"/>	容許使用相機
<input checked="" type="checkbox"/>	容許 FaceTime
<input checked="" type="checkbox"/>	容許畫面擷取
<input checked="" type="checkbox"/>	容許漫遊時自動同步
<input checked="" type="checkbox"/>	容許 Siri
<input checked="" type="checkbox"/>	容許語音撥號
<input checked="" type="checkbox"/>	容許應用程式內購買
<input type="checkbox"/>	限制使用者對所有裝置輸入 iTunes Store 密碼

自訂使用行動設備限制原則

描述

此修正將在目標 iOS 裝置上安裝「1」版的密碼設定設定檔如下定義。

- 裝置上需要密碼：是
- 容許簡式值：是
- 需要英數值：是
- 密碼長度下限：4
- 複式字元數下限：無
- 密碼經歷時間上限（天數）：90
- 自動鎖定（分鐘）：無
- 密碼歷程：4
- 裝置鎖定的真限期（分鐘）：無
- 失敗試圖次數上限：10
- 容許移除設定檔：是
- 容許使用密碼移除設定檔：否

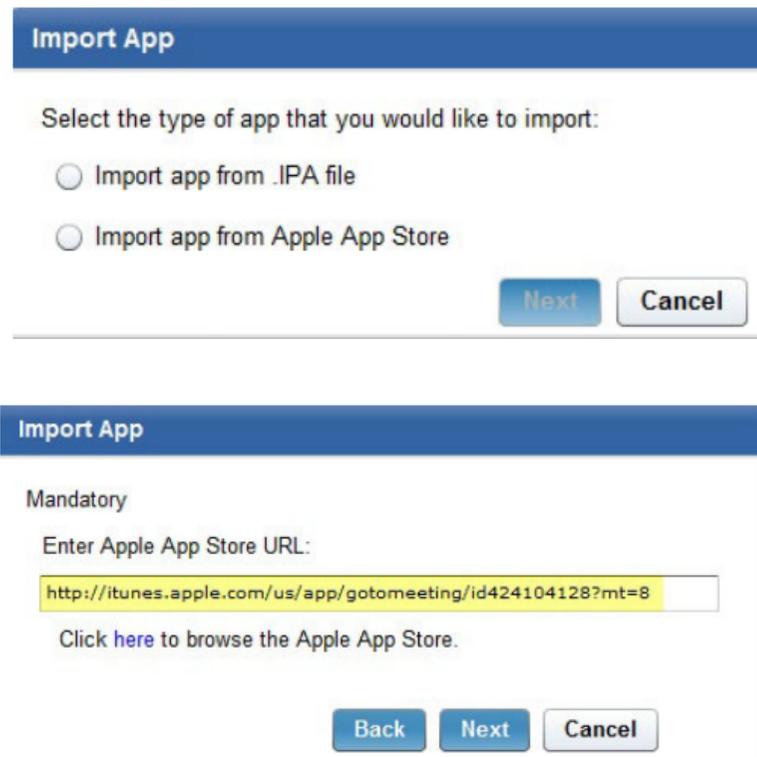
此設定檔於 2012-04-06 19:03:25 建立或修改。



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。



Import App

Select the type of app that you would like to import:

Import app from .IPA file

Import app from Apple App Store

Next **Cancel**

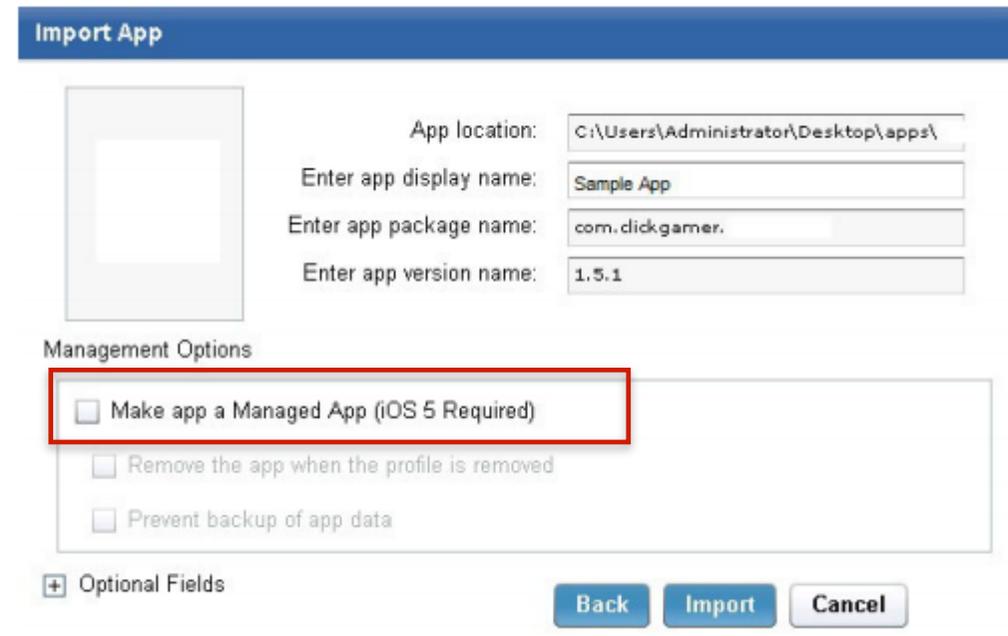
Import App

Mandatory

Enter Apple App Store URL:

Click [here](#) to browse the Apple App Store.

Back **Next** **Cancel**



Import App

App location:

Enter app display name:

Enter app package name:

Enter app version name:

Management Options

Make app a Managed App (iOS 5 Required)

Remove the app when the profile is removed

Prevent backup of app data

+ Optional Fields

Back **Import** **Cancel**

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

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

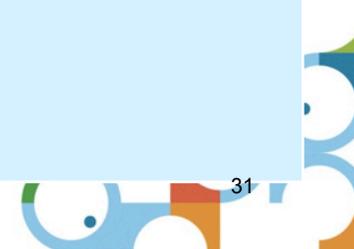
使用 S/MIME 加密傳送外寄郵件

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)

已安裝的應用程式

應用程式管理 - 已安裝的應用程式

此儀表板列出了受管裝置上已安裝的應用程式。

Android 應用程式 | Apple iOS 應用程式

應用程式清單

標籤勾選時間: --- 清除標籤

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

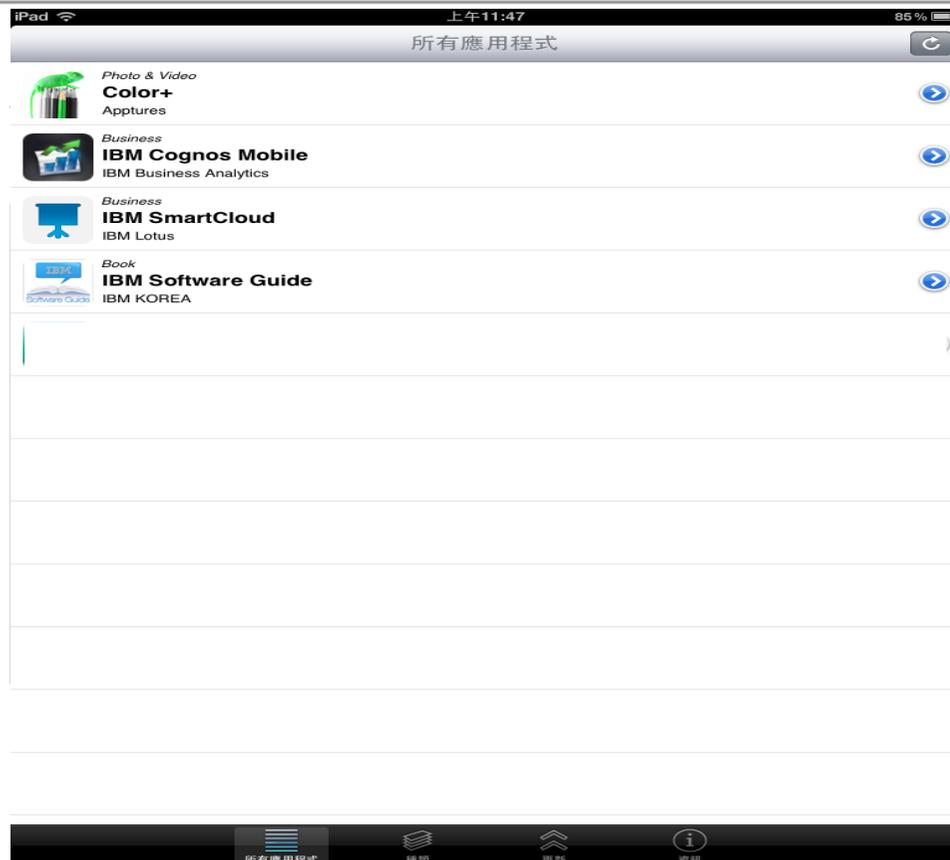
一旦列為特定標籤，如黑名單，即使app重裝也會自動標示標籤



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

建議的應用程式 - Apple iOS



app管理

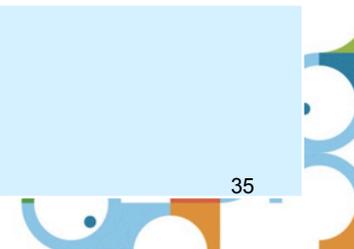
白名單軟體管理可集中push給行動裝置用戶

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)

作業系統	裝置數量
Android	1
iOS	4

'其他'中的項目數: 0

裝置計數(依資料來源)

資料來源	裝置數量
iOS Extender	3
Android Agent	1

'其他'中的項目數: 0

裝置計數(依前次向伺服器通訊時間)

OS	裝置數量
Android	0
iOS	5
Symbian	0
Windows	0
其他	0

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

統計有多少台device裝此軟體，可檢視哪些device

應用程式管理 - 已安裝的應用程式

前次更新: 2012/4/5 下午 01:37:36

此儀表板列出了受管裝置上已安裝的應用程式。

Android 應用程式 | Apple iOS 應用程式

顯示名稱	標籤	套件名稱	說明	版本	電腦計數
<input type="checkbox"/>		轉乘通 Free	com.kingway.Gotch	1.0.0.3	1
<input type="checkbox"/>		群義房屋	com.chyi.iphone	1.5.0	1
<input type="checkbox"/>		Viber	com.viber	2.1.5.270	1
<input type="checkbox"/>		Bakodo	com.bakodo.Bakodo	20	1
<input type="checkbox"/>		PPS影音	com.pps.test	1.2.3	1
<input type="checkbox"/>		AutoV	com.muecsitd.autov	3.3	1
<input type="checkbox"/>		Dove	com.mobile01.dove	13	1
<input type="checkbox"/>		ReaddleDocs	com.readdle.Readdl	3.1.8118	1
<input type="checkbox"/>		GoLook	com.msgup.golook	1.3.0	1
<input type="checkbox"/>		moreBeaute2	com.more-thing.mor	2.1	1
<input type="checkbox"/>		AppSolve	com.baycode.appso	1.1	1
<input type="checkbox"/>		東森房屋	com.etwarm.ethous	1.1	1
<input type="checkbox"/>		Box	net.box.BoxNet	3465	1

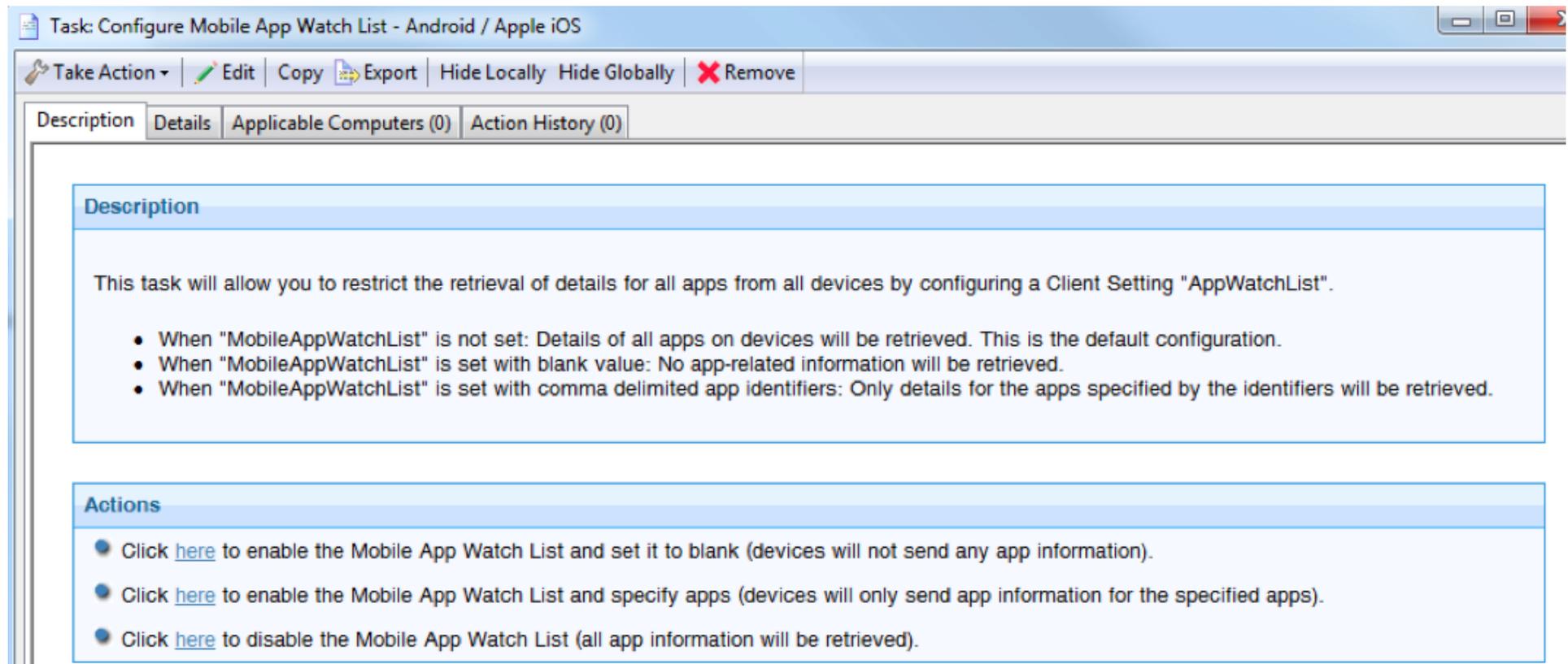
前次報告時間: 2012/5/13 下午
製造商: samsung
承運方: samsung
電話號碼: n/a
代理程式版本: 8.2.10268.0
資料來源: Native

所有內容 | BigFix 管理 | 端點保護 | 行動裝置管理

以使用者 'administrator' 的身分連線到 'BFDEMO.CARESYS.COM.TW'

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。



Task: Configure Mobile App Watch List - Android / Apple iOS

Take Action | Edit | Copy | Export | Hide Locally | Hide Globally | Remove

Description | Details | Applicable Computers (0) | Action History (0)

Description

This task will allow you to restrict the retrieval of details for all apps from all devices by configuring a Client Setting "AppWatchList".

- When "MobileAppWatchList" is not set: Details of all apps on devices will be retrieved. This is the default configuration.
- When "MobileAppWatchList" is set with blank value: No app-related information will be retrieved.
- When "MobileAppWatchList" is set with comma delimited app identifiers: Only details for the apps specified by the identifiers will be retrieved.

Actions

- Click [here](#) to enable the Mobile App Watch List and set it to blank (devices will not send any app information).
- Click [here](#) to enable the Mobile App Watch List and specify apps (devices will only send app information for the specified apps).
- Click [here](#) to disable the Mobile App Watch List (all app information will be retrieved).



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

