Sandblast Mobile 整合 MobileIron

客戶需求:

客戶希望能夠透過 Sandblast Mobile 整合 MobileIron 之後,能夠強化手持裝置或手機的 APT 攻擊防禦,並且利用 MDM 功能達到進一步防堵受感染或觸發資安事件的裝置擴大影響。

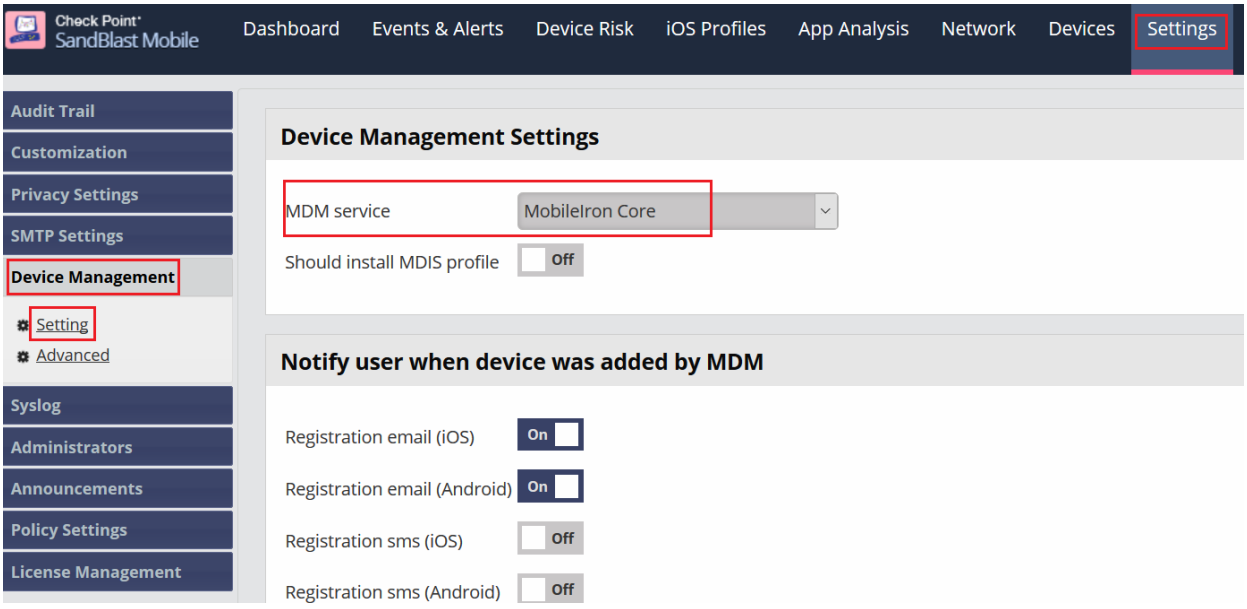
另外本文不討論 MobileIron 設定(雖然客戶的 MobileIron Policy 我也有調整)。

客戶環境:

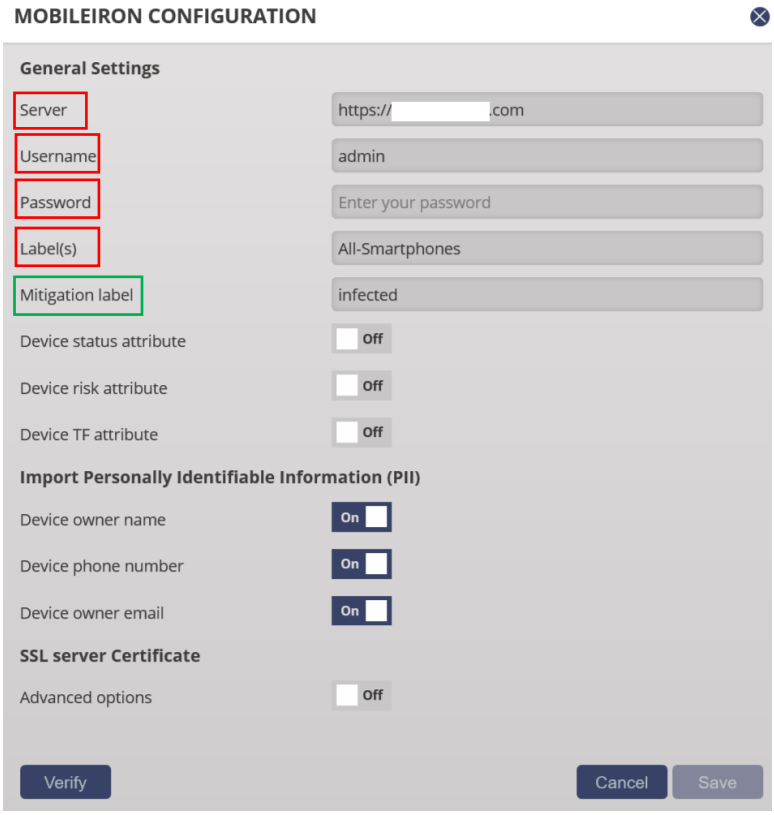
- Sandblast Mobile 500U(用戶陸續上線中)
- MobileIron 一套

設定:

最重要的,要拿到 MobileIron 設定,MobileIron 分成 Core 和 Sentry 兩部份,Sentry 和終端裝置有關,主要設定在 Core 上面,拿到設定後就可以在 SBM 的 Portal→Settings→Device Management→Setting 把設定填入,如下圖:



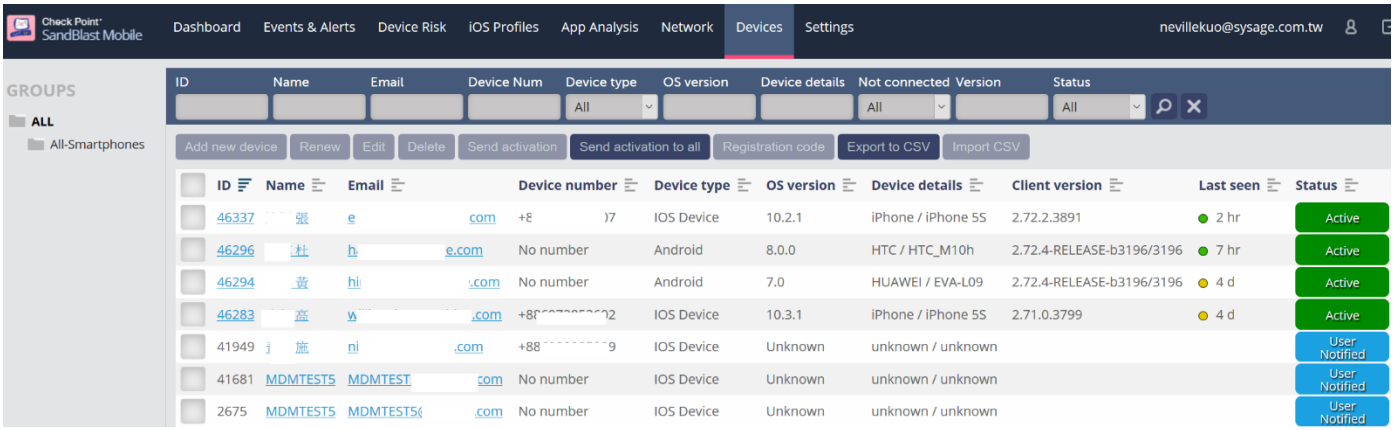
準備好你的 MobileIron 設定,填好它,請注意 MobileIron 需要公開憑證,如果您的環境沒有,SBM Portal 就會錯誤,下圖的客戶是正式環境所以沒有問題:



這張圖裡有幾個欄位要注意,必填的有:
Server:客戶的 MobileIron Core 對外的 FQDN
Username/Password:不用我說了吧
Label(s):SBM 和 MobileIron 建立連線之後,會同步 MobileIron 裝置到 SBM Portal 裡的資料庫,至於要同步哪些裝置,看得就是這個 Label 名稱,不要填錯。

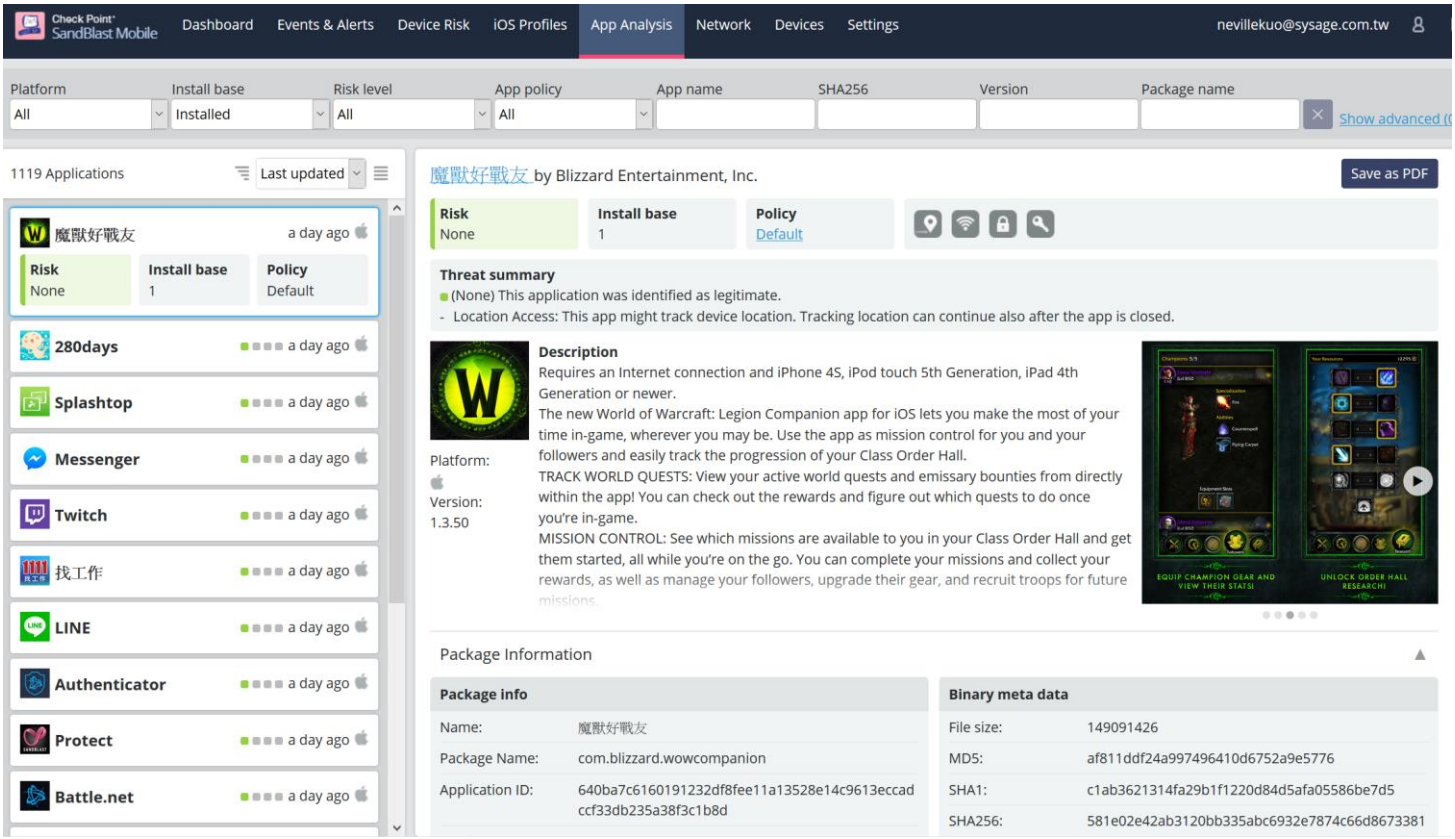
非必要欄位:
Mitigation Label:當 SBM 發現裝置觸發資安事件時,會幫裝置貼標籤,這個客戶是用 infected,可自定,這個設定一開始非必要,但如果需要 MDM 做到感染裝置自動隔離或其它動作時,就需要這個標籤。

上述設定填完之後 SBM 會每十分鐘和 MobileIron 同步一次,把裝置撈到 Device 清單裡,如下圖:

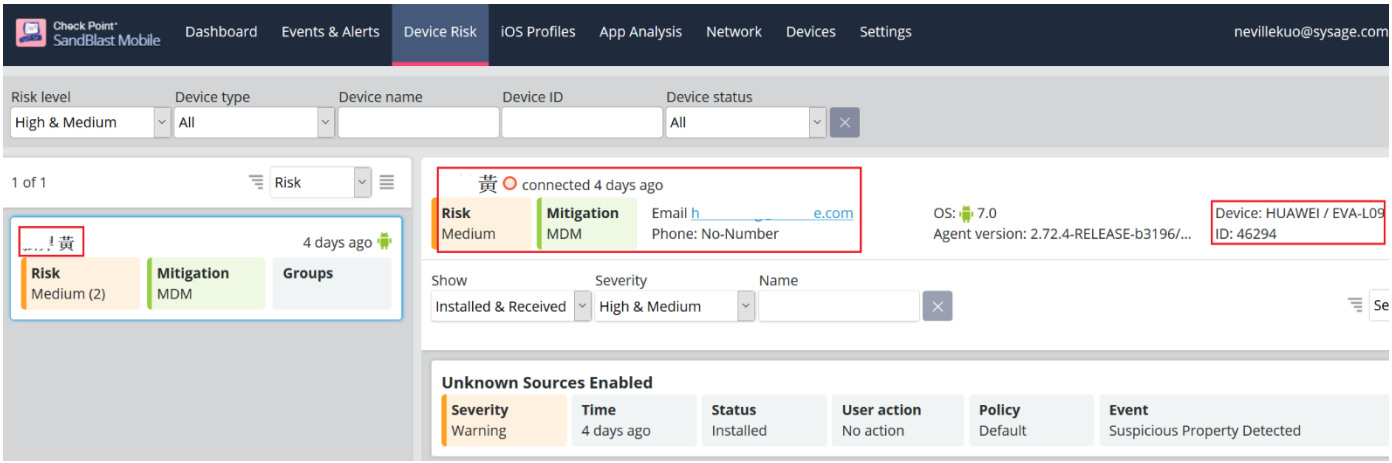


因為已經和 MDM 產品整合,所以圖中某些功能都會反灰不能使用,如 Add new device,基本上看到這個,代表初始工作已經完成,可以針對要納管的裝置做啟動(Activation)了。

SBM 除非觸發資安事件,否則不會告訴管理員某某用戶安裝了什麼 APP,所以是保有隱私的:



下圖則是實際觸發事件的用戶裝置:



最後,因為 SBM 畢竟也是雲端產品,隨時都有可能改版,所以介面有可能會變或新增,這也是要注意的地方。