N-Partner

如何設定 McAfee IntruShield IDS Audit Syslog

V004

2020/01/06

版權聲明

商標

本手冊內所提到的任何的公司產品、名稱及註冊商標，均屬其合法註冊公司所有。

目錄

前言

本文件描述 N-Reporter 使用者如何設定 McAfee IntruShield Syslog。

1. McAfee InstruShield Syslog Forwarding

McAfee IntruShield IDS 可以透過 Fault Notification Syslog Forwarder 送出 Syslog 給 N-Reporter 。

設定步驟如下：

(1) 請使用管理者權限登入 IntruShield IDS

(2) 打開 syslog forwarder 的頁面。

(3) 啟動下列的選項並輸入必要的數值。

Enable Syslog Forwarder: Yes

Forward Alerts: With Severity low and above

Syslog Server: 請輸入 N-Reporter/N-Cloud 設備 IP address

Port: 514

(4) 選擇 Message Preference: [Customized]，然後點選 [Edit] 按鈕，進入編輯客製化 syslog message 的頁面。

(5) 請將下面的文字複製後貼上：

category="$IV_CATEGORY$", sub_category="$IV_SUB_CATEGORY$", attack_name="IV_ATTACK_NAME", attack_severity=$IV_ATTACK_SEVERITY$, interface=$IV_INTERFACE$, source_ip=IV_SOURCE_IP, source_port=IV_SOURCE_PORT,destination_ip=$IV_DESTINATION_IP$,destination_port=$IV_DESTINATION_PORT$, network_protocol=$IV_NETWORK_PROTOCOL$,attack_count=IV_ATTACK_COUNT

※ 注意：上述的格式，沒有任何的換行符號。

(6) 點選 [Save] 按鈕。

(7) 點選 [Apply] 按鈕。

(8) 設定完成。接下來，IntruShield IDS 即會把新產生的 Syslog 送至 N-Reporter/N-Cloud。

2. McAfee Network Security Manager Syslog forwarding

(1) 請使用管理者權限登入

[Network Security Manager] -> [IPS Setting] -> [Alert Notification] -> [Syslog]

(2) 打開 [Syslog forwarder] 的頁面。

(3) 啟動下列的選項並輸入必要的數值：

Enable Syslog Forwarder：Yes

Server Name or IP Address：請輸入 N-Reporter/N-Cloud 設備 IP address

UDP Port：514

Send Notification IF：勾選 [The following notification filter is matched:] 選擇 [Severity Informational and above]

(4) 選擇 Message Preference: [Customized]，然後點選 [Edit] 按鈕，進入編輯客製化 syslog messages 的頁面。

(5) 請將下面的文字複製後貼上：

category="$IV_CATEGORY$", sub_category="$IV_SUB_CATEGORY$", attack_name="IV_ATTACK_NAME", attack_severity=$IV_ATTACK_SEVERITY$, interface=$IV_INTERFACE$, source_ip=IV_SOURCE_IP, source_port=IV_SOURCE_PORT,destination_ip=$IV_DESTINATION_IP$,destination_port=$IV_DESTINATION_PORT$, network_protocol=$IV_NETWORK_PROTOCOL$,attack_count=IV_ATTACK_COUNT

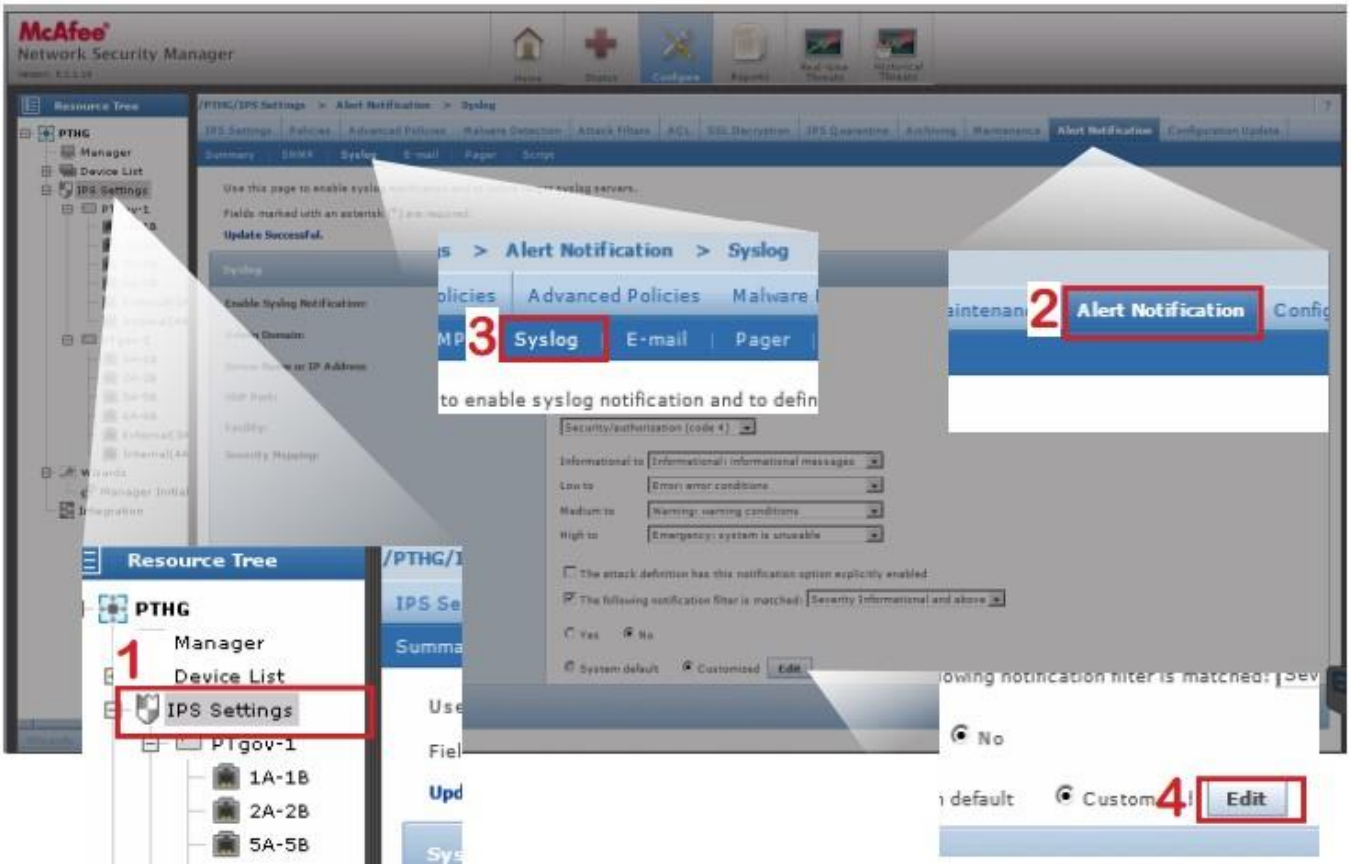
※ 注意：上述的格式，沒有任何的換行符號。

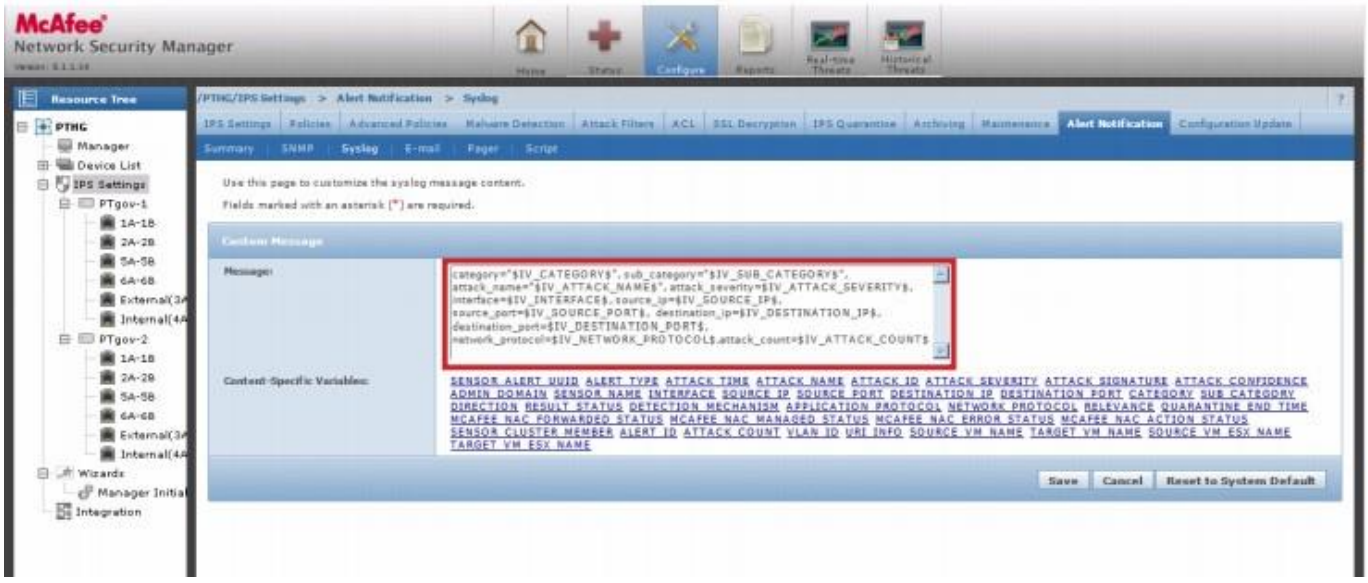
(6) 點選 [Save] 按鈕。

(7) 點選 [Apply] 按鈕。

(8) 設定完成。接下來，IntruShield IDS 即會把新產生的 Syslog 送至 N-Reporter/N-Cloud。

範例如下：

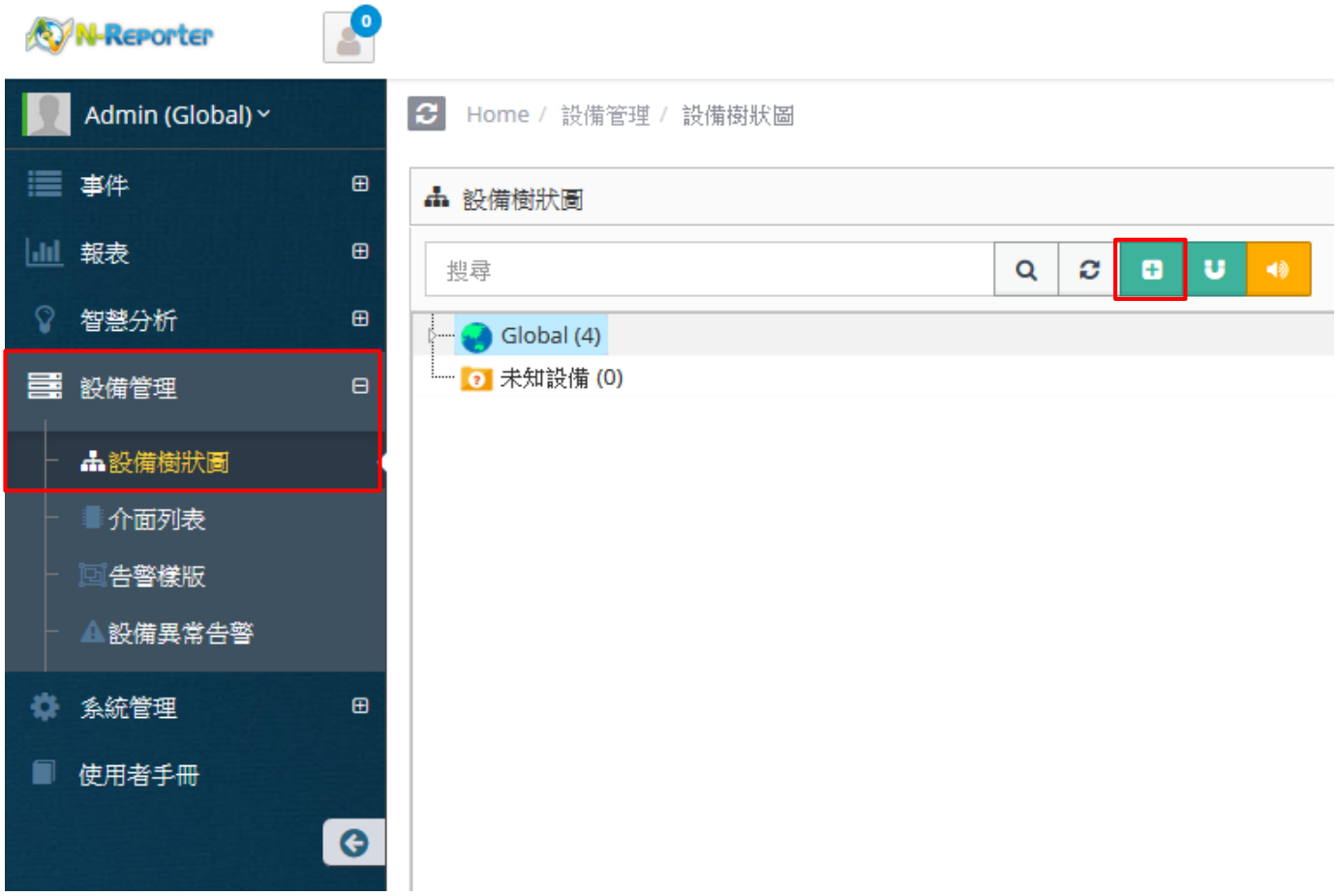




3. N-Reporter

(1) 新增 McAfee NSP 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]



(2) 設定 McAfee NSP 的資料格式

輸入名稱和 IP -> 勾選設備種類: [Syslog] -> 選擇資料格式: [McAfee NSP] 和選擇設備 Icon: [icon-security] -> 點選 接收狀態: [啟用] -> 按下 [確定]

連 絡 資 訊

TEL: +886-4-23752865

FAX: +886-4-23757458

技 術 問 題 請 洽 :

Email: support@npartnertech.com

Skype: support@npartnertech.com

業 務 相 關 請 洽 :

Email: sales@npartnertech.com