如何設定
McAfee IntruShield IDS Audit Syslog

V005

2025/03/17

版權聲明

商標

目錄

前言

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

註：本文件僅做為如何將日誌吐出的設定參考，建議您仍應聯繫設備或是軟體原廠尋求日誌輸出方式之協助。

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 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=$IV_ATTACK_COUNT$
```

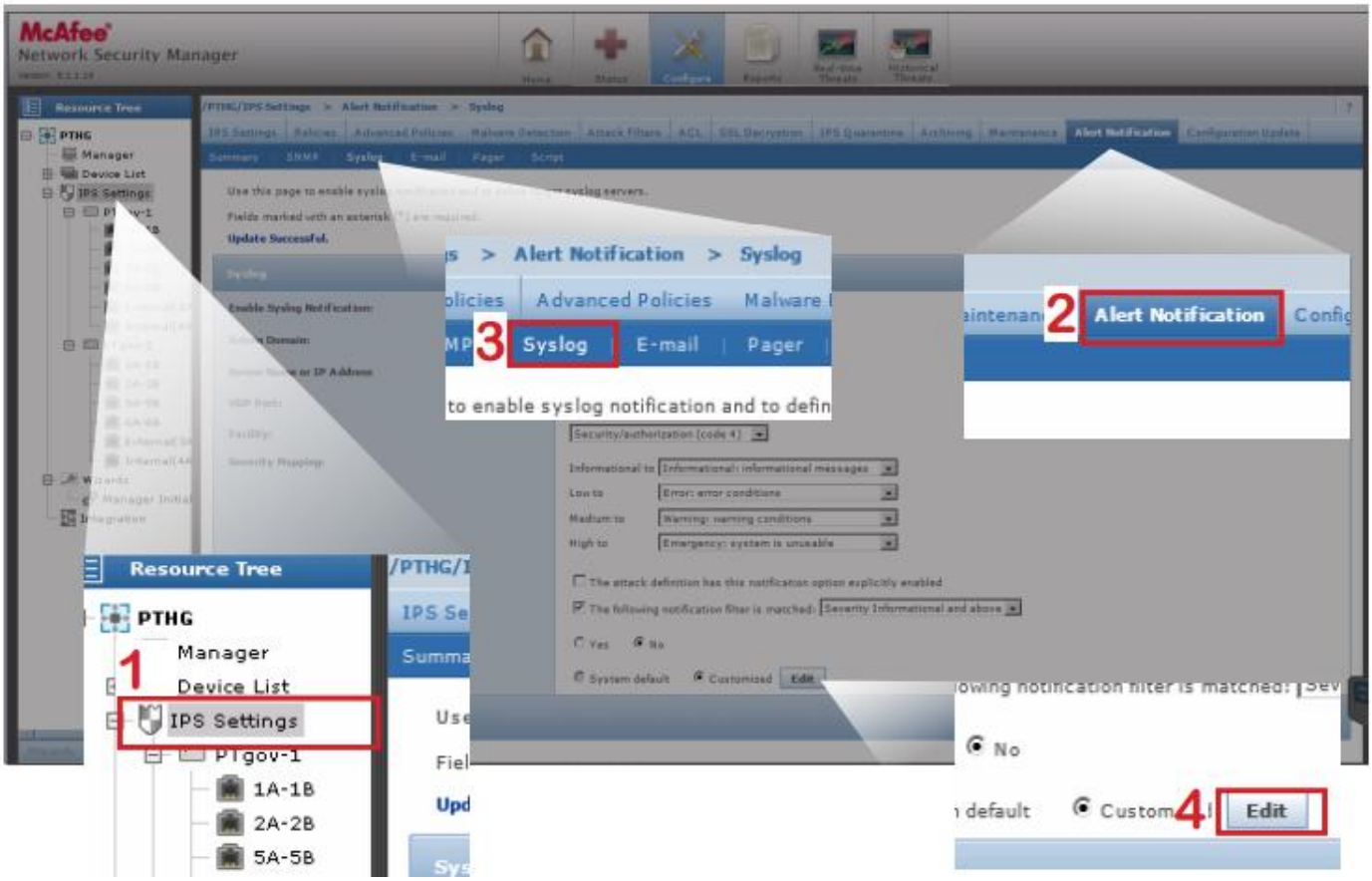
*注意: 上述的格式, 沒有任何的換行符號。

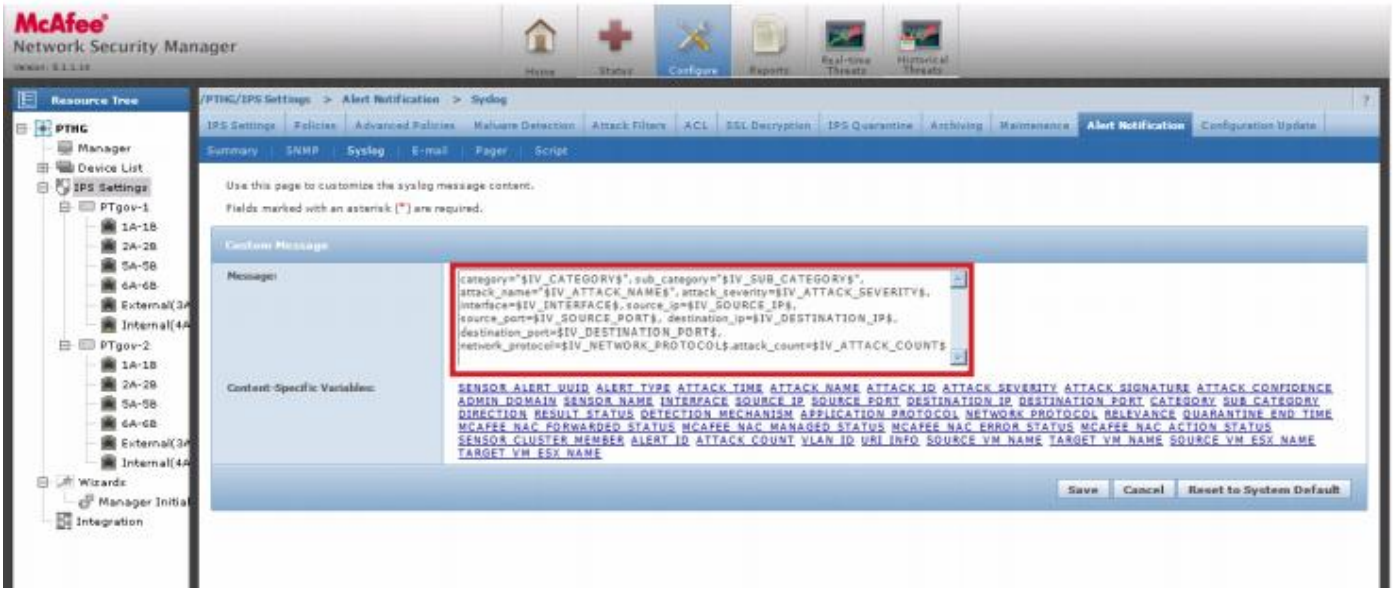
(6) 點選 [Save] 按鈕。

(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。

範例如下:

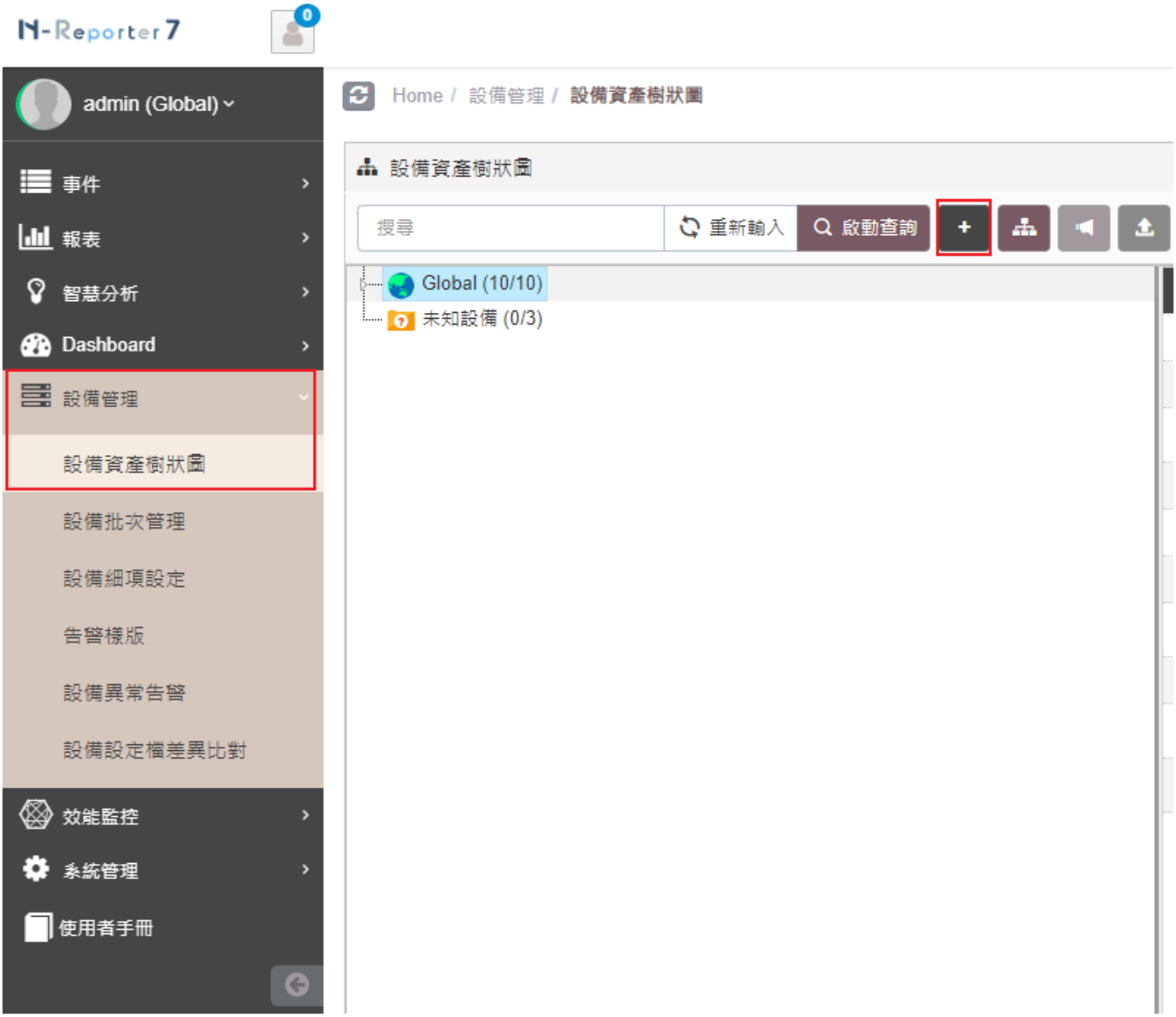




3 N-Reporter

(1) 新增 McAfee NSP 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]



(2) 選擇設備種類

選擇 [Firewall/ IPS/ Load Balancer/ NAC/ UTM/ WAF/ Wireless]-> 點選 [引導模式]

(3) 設備基本設定

輸入設備名稱和IP->Syslog 資料格式選擇 [McAfee NSP]-> 點選 [下一步]

(4) Syslog 相關設定

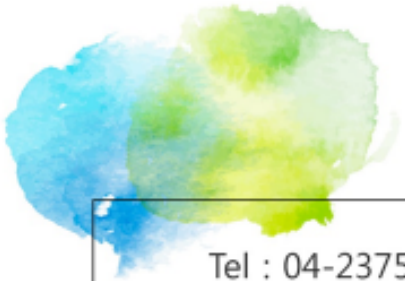
Facility 保持預設-> 點選 [下一步]

(若勾選 [Raw Data 保留]，則 [事件查詢] 顯示 Raw Data 資訊)

(5) 其他

設備 Icon 選擇 [Security]-> 接收狀態選擇 [啟用]-> 點選 [下一步]->[確認]

是否啟用預設報表，將套用置相同廠牌型號設備-> 點擊 [否]



Tel：04-23752865　Fax：04-23757458
業務詢問：sales@npartner.com
技術詢問：support@npartner.com