

IPS 6.X — 通過IDM啟用/禁用特定事件摘要

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[使用IDM啟用/禁用特定事件的摘要](#)

[IDM配置](#)

[相關資訊](#)

簡介

本文檔介紹如何使用IPS裝置管理器(IDM)在Intrusion Prevention System(IPS)軟體版本6.x中啟用/禁用特定事件的摘要。

註意：必須在IPS裝置中配置訪問清單，以允許從安裝了IDM和IEV(IDS事件檢視器)等管理軟體的主機或網路進行訪問，並正常工作。有關詳細資訊，請參閱[使用命令列介面5.0配置Cisco Intrusion Prevention System感測器的更改訪問清單](#)部分。

必要條件

需求

本文是根據已安裝IPS 6.x且工作正常的假設編寫的。

採用元件

本檔案中的資訊是根據執行軟體版本6.0(2)E1的Cisco 4200系列IPS感應器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

使用IDM啟用/禁用特定事件的摘要

為了清楚瞭解，本節提供啟用/禁用簽名ID摘要的示例：5748。

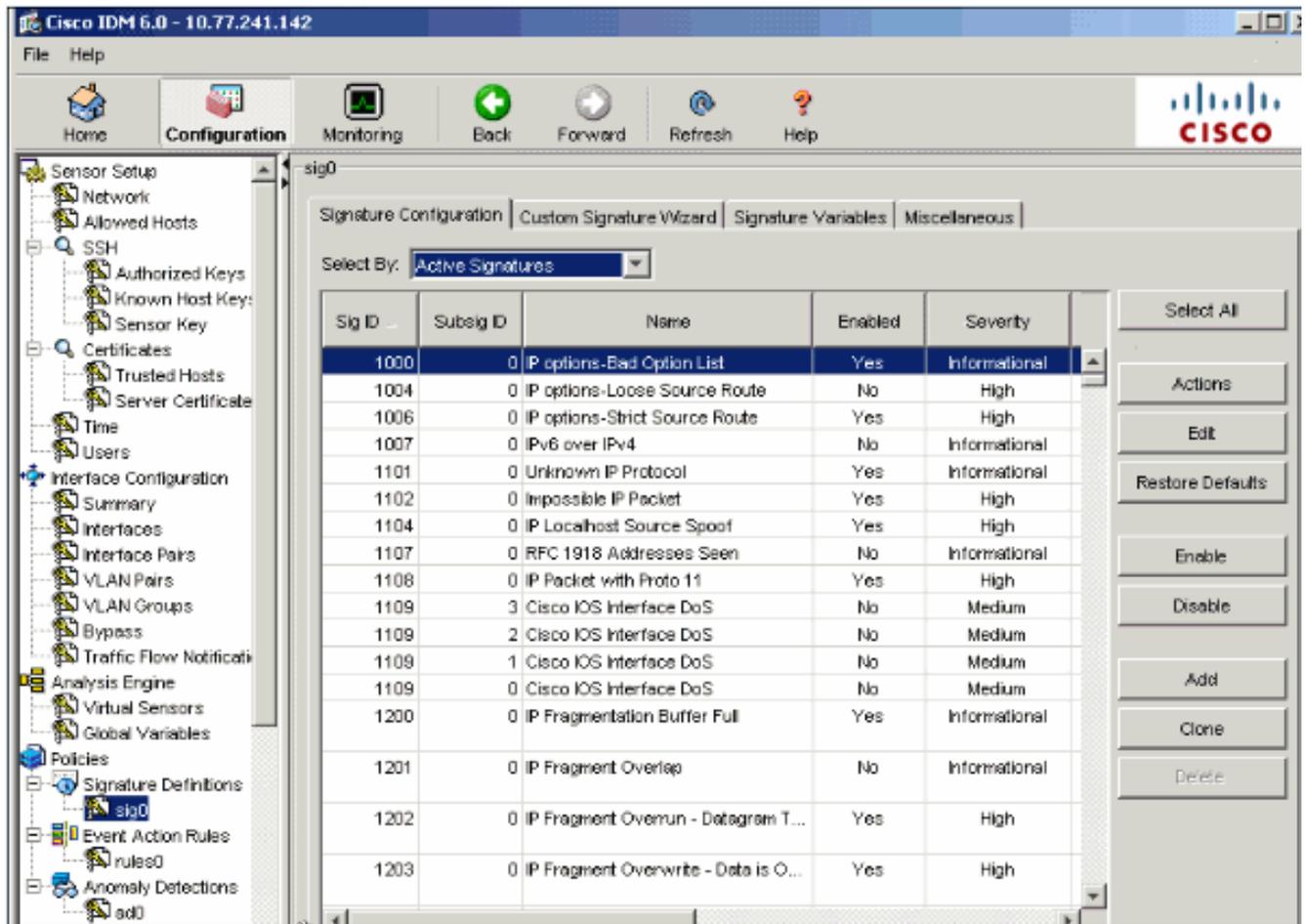
IDM配置

請完成以下步驟。

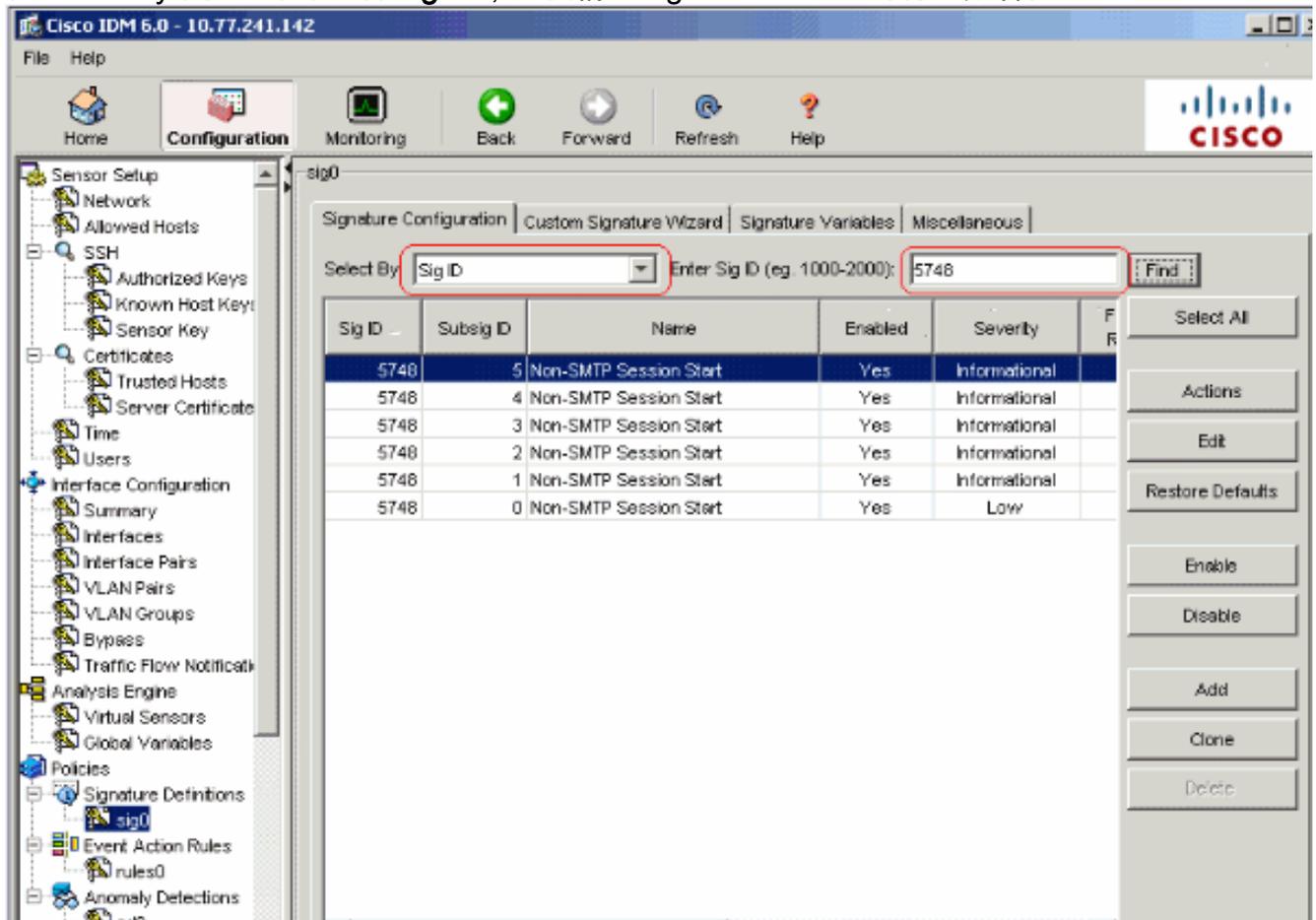
1. 啟動IDM。
2. 按一下Home以檢視IDM的首頁。此頁顯示裝置資訊。



3. 選擇Configuration > Policies > Signature Definitions > sig0 > Signature Configuration > Select By:簽名ID，顯示感測器中的所有可用簽名。



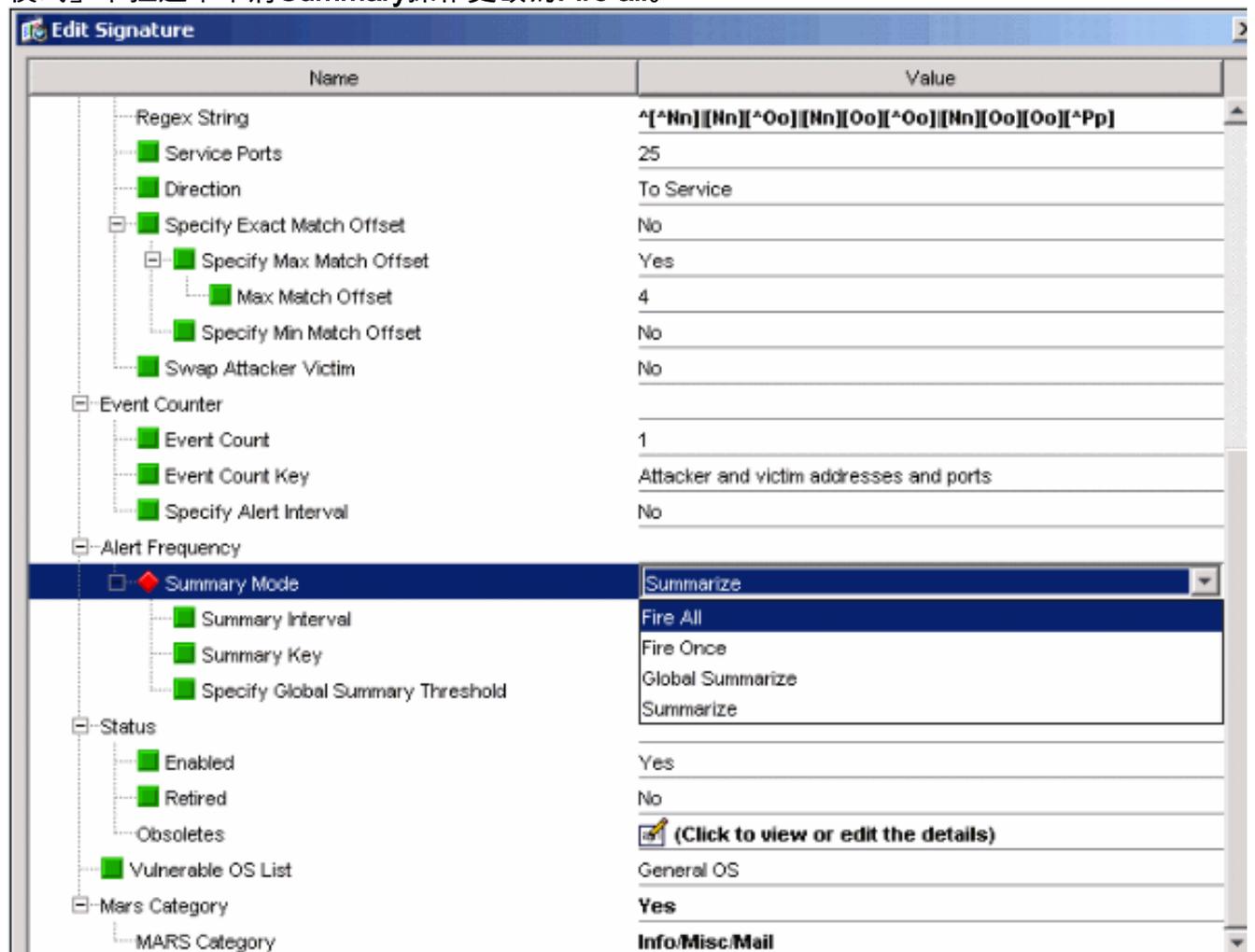
4. 從Select By下拉選單中選擇Sig ID，然後輸入Sig ID 5748以查詢特定簽名。



5. 按一下Edit以編輯簽名。

6. 在「編輯特徵碼」視窗中，選擇「特徵碼定義」>「警報頻率」>「摘要模式」，然後在「摘要

模式」下拉選單中將Summary操作更改為Fire all。



7. 確保「指定全域性摘要閾值」設定為否。

Name	Value
Regex String	*[^\n][\n][^\o][\o][\o][\o][\o][\o][^\p]
Service Ports	25
Direction	To Service
Specify Exact Match Offset	No
Specify Max Match Offset	Yes
Max Match Offset	4
Specify Min Match Offset	No
Swap Attacker Victim	No
Event Counter	
Event Count	1
Event Count Key	Attacker and victim addresses and ports
Specify Alert Interval	No
Alert Frequency	
Summary Mode	Summarize
Summary Interval	15
Summary Key	Attacker address
Specify Global Summary Threshold	No
Status	No
Enabled	Yes
Retired	No
Obsoletes	(Click to view or edit the details)
Vulnerable OS List	General OS
Mars Category	Yes
MARS Category	Info/Misc/Mail

相關資訊

- [思科入侵防禦系統支援頁面](#)
- [Cisco IPS裝置管理員支援頁面](#)
- [IOS IPS入門](#)
- [技術支援與文件 - Cisco Systems](#)