# 使用ASDM（機箱內管理）配置系統/流量事件的Firepower模組日誌記錄

## 目錄



## 簡介

本檔案介紹Firepower模組的系統/流量事件以及將這些事件傳送到外部日誌記錄伺服器的各種方法。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- ASA（自適應安全裝置）防火牆、ASDM（自適應安全裝置管理器）知識。
- Firepower裝置知識。
- 系統日誌、SNMP協定知識。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本5.4.1及更高版本的ASA Firepower模組(ASA 5506X/5506H-X/5506W-X、ASA 5508-X、ASA 5516-X).
- 運行軟體版本6.0.0及更高版本的ASA Firepower模組(ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X)。
- ASDM 7.5(1)及更高版本。

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。

# 背景資訊

### 事件型別

Firepower模組事件可以分為兩種型別：-

1. 流量事件（連線事件/入侵事件/安全情報事件/SSL事件/惡意軟體/檔案事件）。
2. 系統事件(Firepower作業系統(OS)事件)。

# 設定

## 配置輸出目標

### 步驟1.系統日誌伺服器配置

要為通訊事件配置系統日誌伺服器，請導航到**Configuration > ASA Firepower Configuration > Policies > Actions Alerts**，然後點選**Create Alert**下拉選單並選擇**Create Syslog Alert選項。**輸入系統日誌伺服器的值。

**名稱:** 指定唯一標識系統日誌伺服器的名稱。

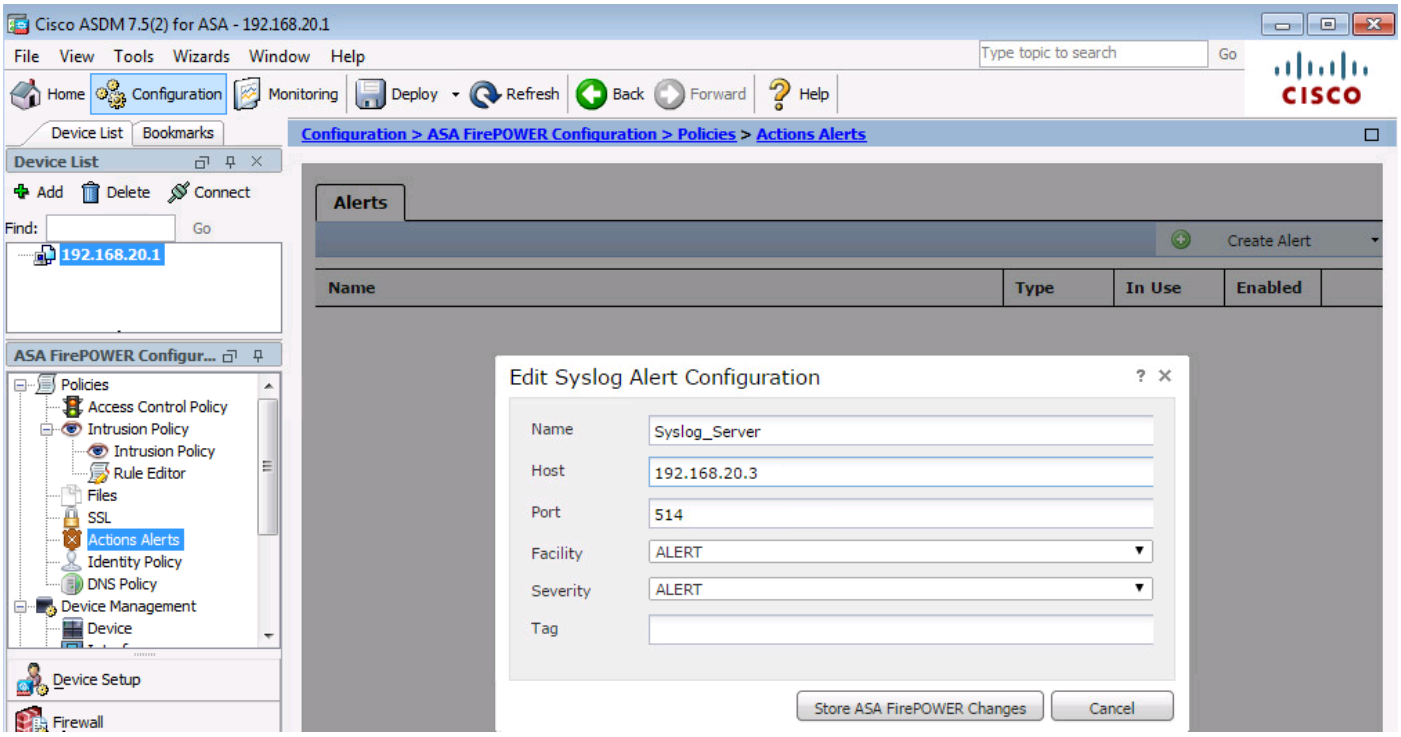
**主機：**指定Syslog伺服器的IP地址/主機名。

**連接埠:** 指定系統日誌伺服器的埠號。

**設施：** 選擇系統日志伺服器上配置的任何設施。

**嚴重性:** 選擇系統日誌伺服器上配置的任意嚴重性。

**標籤：** 指定要與系統日誌消息一起顯示的標籤名稱。




**步驟2.SNMP伺服器配置**

要為流量事件配置SNMP陷阱伺服器，請導航到**ASDM Configuration > ASA Firepower Configuration > Policies > Actions Alerts**，然後點選**Create Alert**下拉選單並選擇**Create SNMP Alert選項。**

**名稱:** 指定唯一標識SNMP陷阱伺服器的名稱。

**陷阱伺服器：** 指定SNMP陷阱伺服器的IP地址/主機名。

**版本:** Firepower模組支援SNMP v1/v2/v3。從下拉選單中選擇SNMP版本。

**社群字串： 如果您選擇**v1或**v2 in Version**選項，請指定SNMP社群名稱。

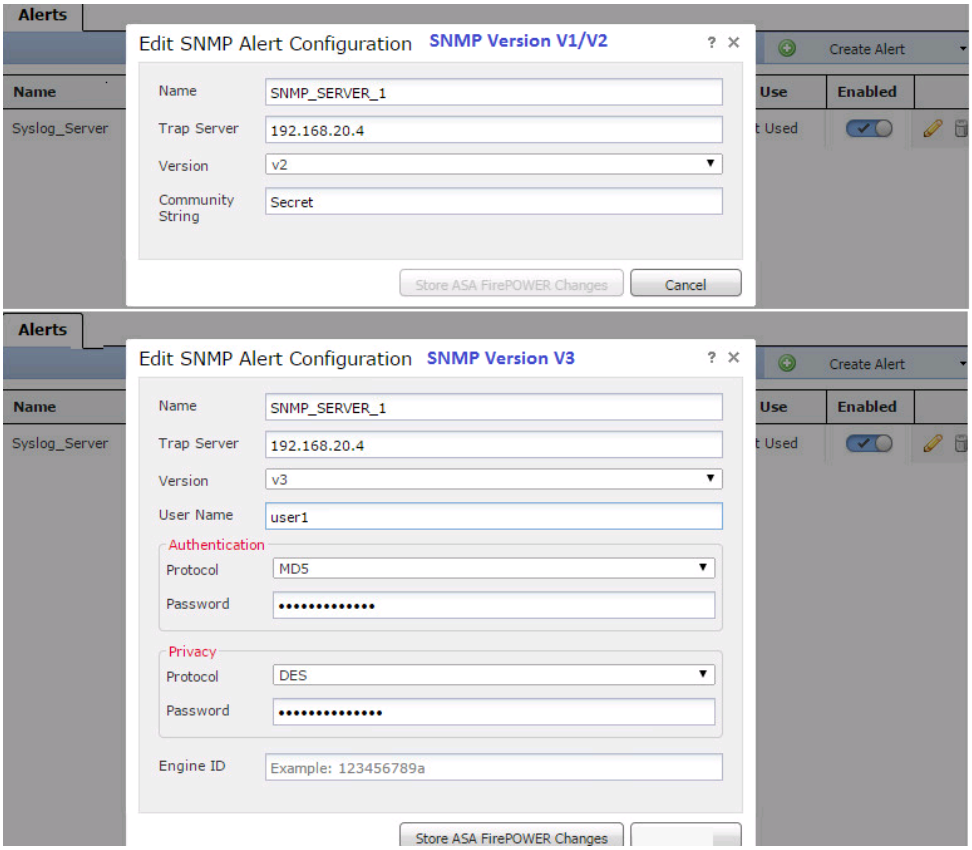
**使用者名稱:** 如果在**Version**選項中選擇v3，系統將提示**User Name**欄位。指定使用者名稱。

**驗證:** 此選項是SNMP v3配置的一部分。它提供基於雜湊的身份驗證

演算法使用MD5或SHA演算法。在**Protocol**下拉選單中，選擇雜湊演算法並輸入

**Password** 選項中的密碼。如果不希望使用此功能，請選擇**None**選項。

**隱私**:此選項是SNMP v3配置的一部分。它使用DES演算法提供加密。在**Protocol**下拉選單中，選擇選項作為**DES**，並在**Password**欄位中輸入密碼。如果您不想使用資料加密功能，請選擇**None**選項。




## 用於傳送流量事件的配置

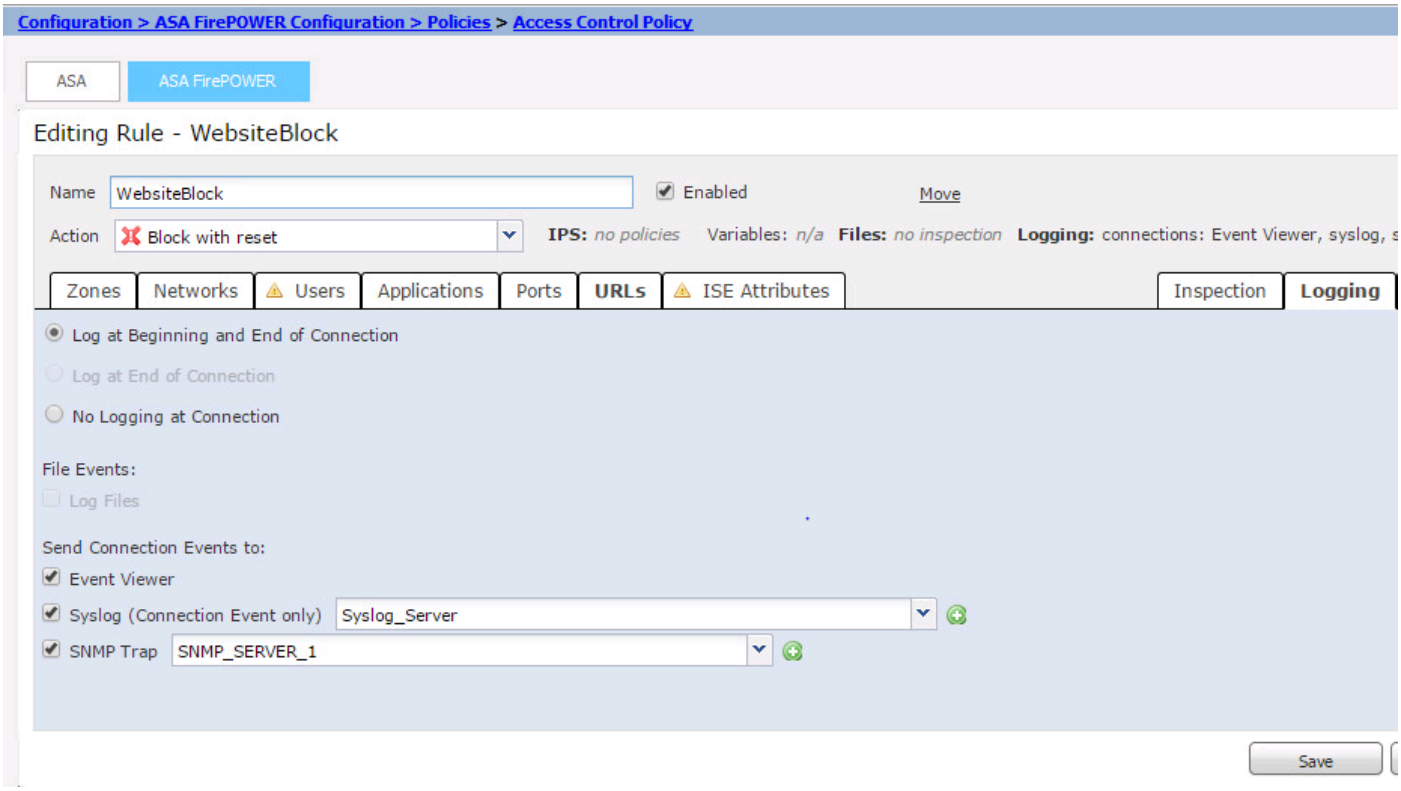
### 為連線事件啟用外部日誌記錄

當流量到達已啟用日誌記錄的訪問規則時，會生成連線事件。要為連線事件啟用外部日誌記錄，請導航到(ASDM Configuration > ASA Firepower Configuration > Policies > Access Control Policy)編輯訪問規則，然後導航到logging選項。

選擇日誌記錄選項：**在連線的開始和結束處**記錄，**或在連線結束時記錄**。導航到**將連線事件傳送到**選項，並指定將事件傳送到何處。

若要將事件傳送到外部Syslog伺服器，請選擇**Syslog**，然後從下拉選單中選擇Syslog警報響應。或者，您可以通過按一下add **icon**新增Syslog警報響應。

要將連線事件傳送到SNMP陷阱伺服器，請選擇**SNMP Trap**，然後從下拉選單中選擇SNMP警報響應。或者，您可以通過按一下新增**圖示**來新增SNMP警報響應。




**為入侵事件啟用外部日誌記錄**

當簽名（snort規則）與某些惡意流量匹配時，就會生成入侵事件。要啟用入侵事件的外部日誌記錄，請導航到**ASDM Configuration > ASA Firepower Configuration > Policies> Intrusion Policy > Intrusion Policy。**建立新的入侵策略或編輯現有入侵策略。導覽至**Advanced Setting > External Responses。**

若要將入侵事件傳送到外部SNMP伺服器，請在**SNMP警報**中選擇**Enabled**選項，然後按一下**Edit**選項。

陷阱型別：陷阱型別用於警報中顯示的IP地址。如果網路管理系統正確呈現INET_IPV4地址型別，則可以選擇為Binary。否則，選擇為字串。

**SNMP版本：** 選擇其中一個 **版本2** 或 **版本3** 單選按鈕。

**SNMP v2選項**

**陷阱伺服器：**指定SNMP陷阱伺服器的IP地址/主機名，如下圖所示。

**社群字串**:指定團體名稱。

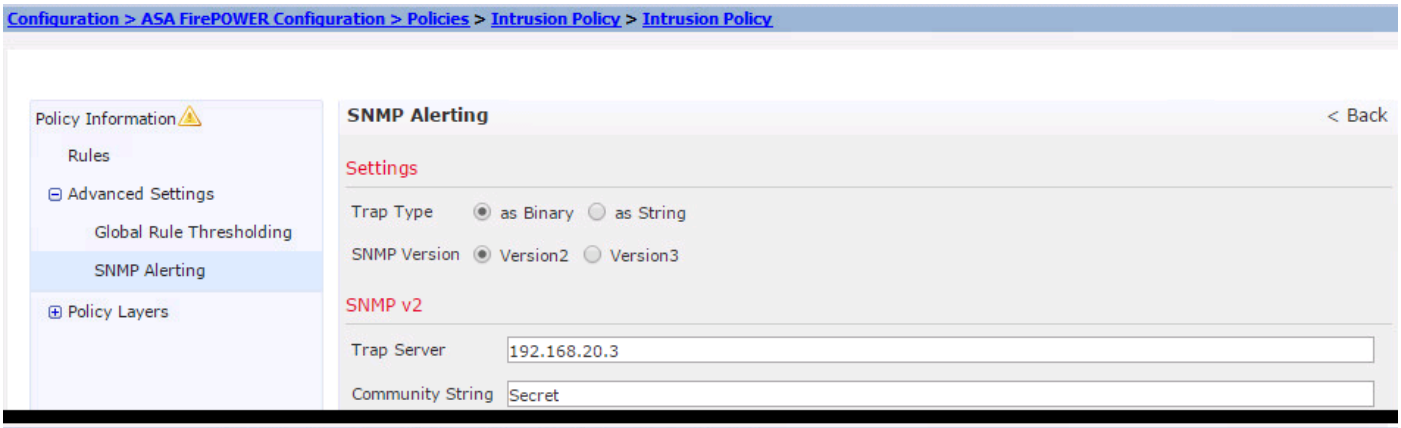
**SNMP v3選項**

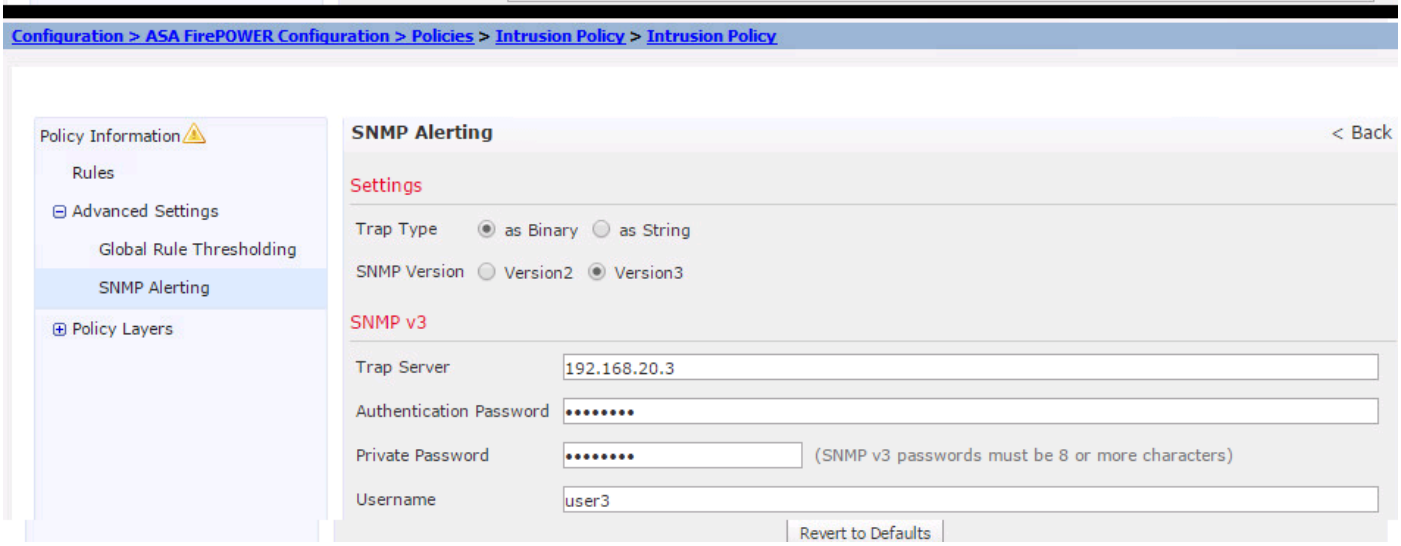
**陷阱伺服器：**指定SNMP陷阱伺服器的IP地址/主機名，如下圖所示。

**身份驗證密碼：**指定身份驗證所需的密碼。SNMP v3使用雜湊函式對密碼進行身份驗證。

**專用密碼：**指定加密的密碼。SNMP v3使用資料加密標準(DES)分組密碼加密此密碼。

**使用者名稱：**指定使用者名稱。




要將入侵事件傳送到外部系統日誌伺服器，請選擇選項 **已啟用** 在**Syslog中 警報** 然後按一下 **編輯** 選項，如下圖所示。

**日誌記錄主機：**指定Syslog伺服器的IP地址/主機名。

**設施：** 選擇任何合作室 配置的系統日誌伺服器。

**嚴重性:**選擇系統日誌伺服器上配置的任意嚴重性。

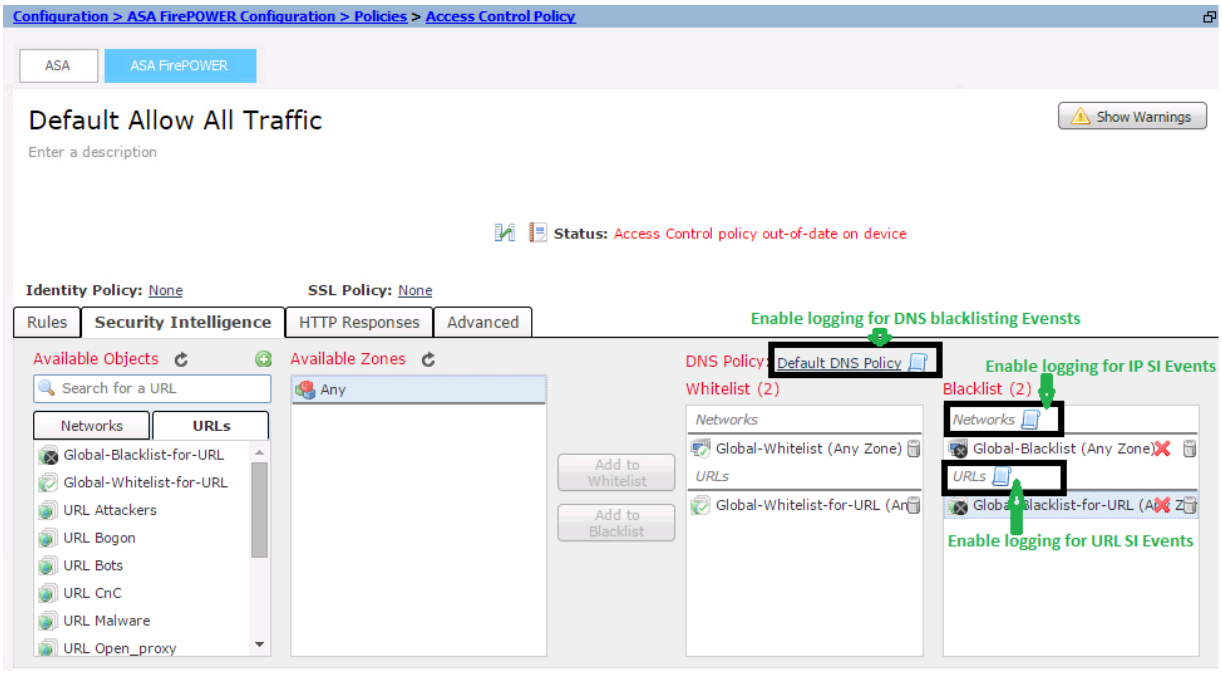

**為IP安全情報/DNS安全情報/URL安全情報啟用外部日誌記錄**

**當流量與任何IP地址/域名/URL安全情報資料庫**匹配時，會生成IP安全情報/DNS安全情報/URL安全情報事件。要啟用IP/URL/DNS安全情報事件的外部日誌記錄，請導航到(**ASDM Configuration > ASA Firepower Configuration > Policies > Access Control Policy > Security Intelligence**),

按圖中所示的**圖示**可啟用IP/DNS/URL安全情報的日誌記錄。按一下該圖示將提示一個對話方塊以啟用日誌記錄，並提示一個選項以將事件傳送到外部伺服器。

若要將事件傳送到外部Syslog伺服器，請選擇**Syslog**，然後從下拉選單中選擇Syslog警報響應。或者，您可以通過按一下新增圖示來新增系統日誌警報響應。

若要將連線事件傳送到SNMP陷阱伺服器，請選擇**SNMP Trap**，然後從下拉選單中選擇SNMP警報響應。或者，您可以通過按一下新增圖示來新增SNMP警報響應。



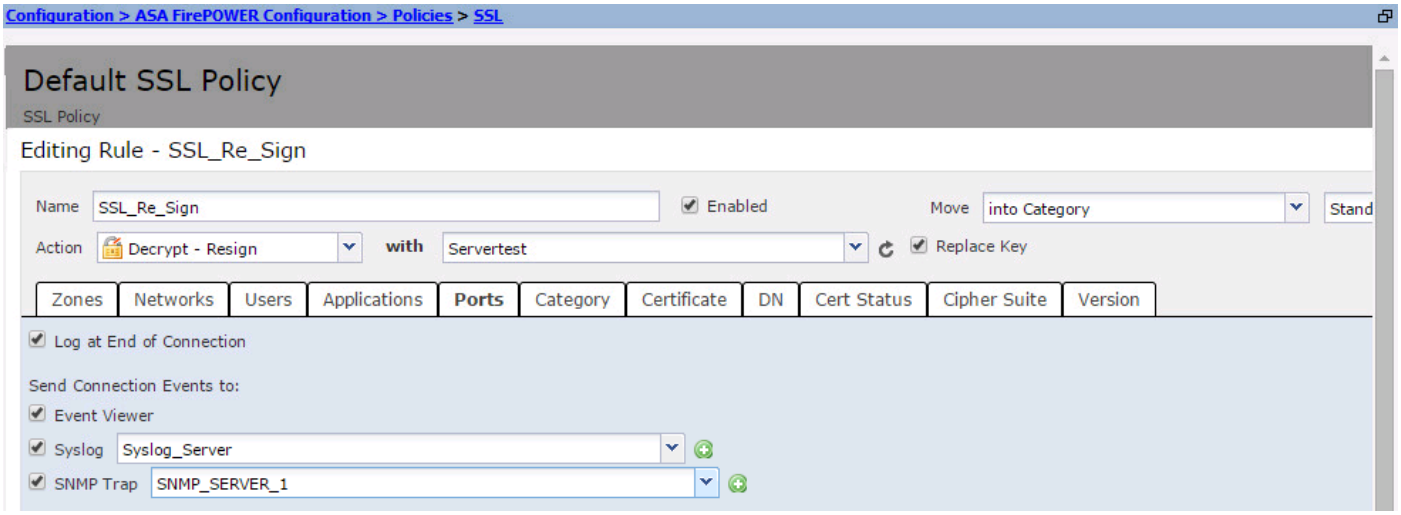

## 為SSL事件啟用外部日誌記錄

**當流量與**啟用了日誌記錄的SSL策略中的任何規則匹配時，會生成SSL事件。若要為SSL流量啟用外部日誌記錄，請導航到**ASDM配置> ASA Firepower配置> 策略> SSL。編輯現有規則或建立新規則，然後導航到**logging 選項。選擇**End of Connection** 選項**log。**

然後導航到**將連線事件傳送到**，並指定將事件傳送到何處。

要將事件傳送到外部Syslog伺服器，請選擇**Syslog**，然後從下拉選單中選擇一個Syslog警報響應。或者，您可以通過按一下新增圖示來新增系統日誌警報響應。

要將連線事件傳送到SNMP陷阱伺服器，請選擇**SNMP Trap**，然後從下拉選單中選擇SNMP警報響應。或者，您可以通過按一下新增圖示來新增SNMP警報響應。




## 用於傳送系統事件的配置

### 為系統事件啟用外部日誌記錄

系統事件顯示Firepower作業系統的狀態。SNMP管理器可用於輪詢這些系統事件。

要配置SNMP伺服器以便從Firepower模組輪詢系統事件，需要配置系統策略，使資訊在firepower MIB（管理資訊庫）中可用，SNMP伺服器可以輪詢該資訊。

導航到**ASDM Configuration > ASA Firepower Configuration > Local > System Policy**，然後按一下**SNMP**。

**SNMP版本：** Firepower模組支援SNMP v1/v2/v3。請指定SNMP版本。

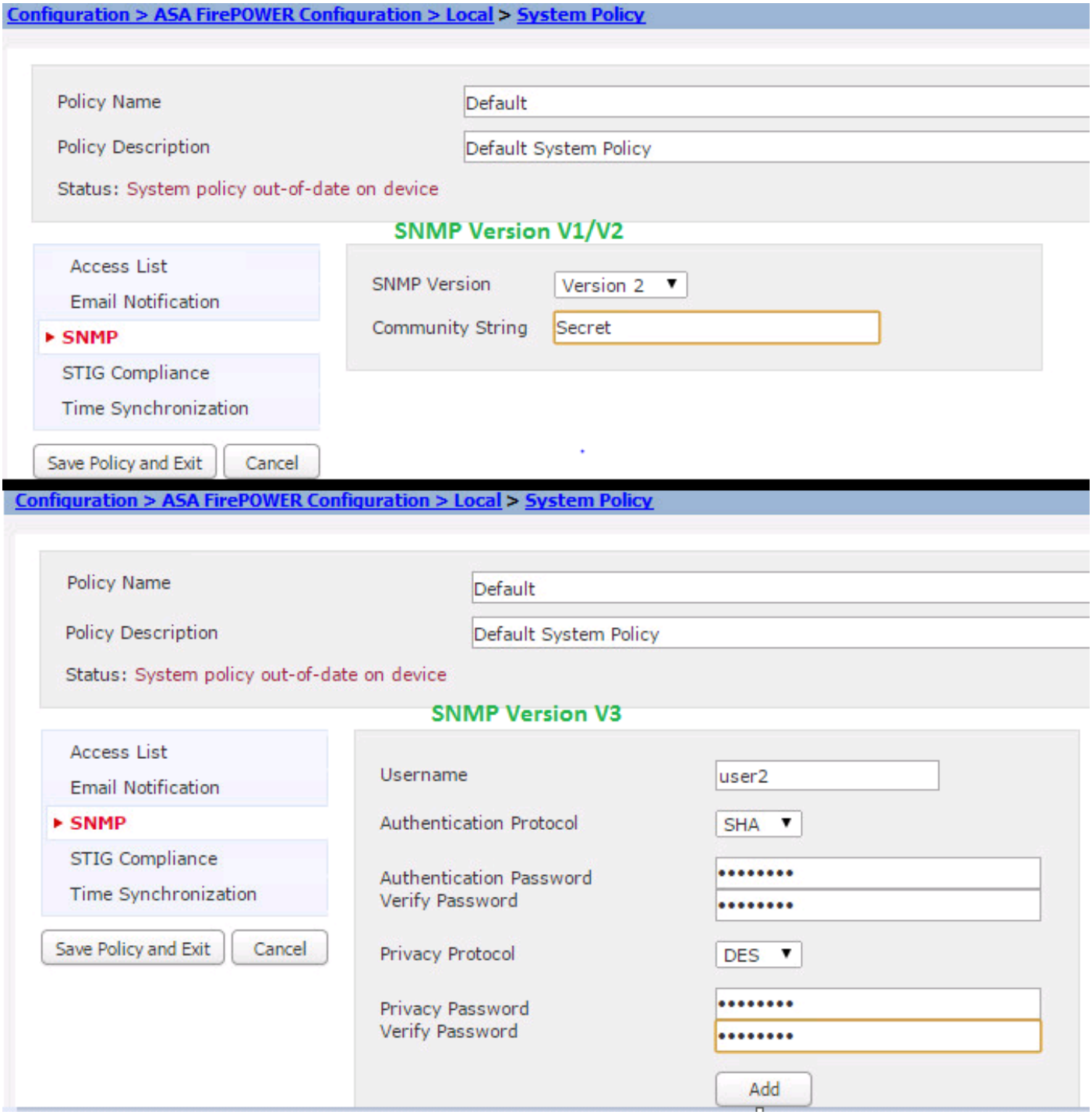
**社群字串：** 如果您在**SNMP版本選項中選擇**v1/ v2，請在Community String欄位中鍵入SNMP社群名稱。

**使用者名稱: 如果您選擇v3**選項in version選項。按一下**Add User**按鈕，並在使用者名稱欄位中指定**Username**。

**驗證:** 此選項是SNMP v3配置的一部分。它使用MD5或SHA演算法提供基於雜湊消息身份驗證代碼的身份驗證。選擇**Protocol** for hash algorithm，然後輸入密碼

在**Password**欄位中。如果不希望使用身份驗證功能，請選擇**None**選項。

**隱私**: 此選項是SNMP v3配置的一部分。它使用DES/AES演算法提供加密。選擇加密的協定，並在**Password(密碼)欄位中輸入**密碼。如果您不需要資料加密功能，請選擇**None**選項。




:(MIB)FirepowerMIB(DCEALERT.MIB)(/etc/sf/DCEALERT.MIB)

## 驗證

目前沒有適用於此組態的驗證程序。

## 疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

# 相關資訊

- 技術支援與文件 - Cisco Systems