FireSIGHT系統的初始配置步驟

目錄

簡介

重新映像FireSIGHT管理中心或FirePOWER裝置後，需要完成幾個步驟以使系統完全正常運行並為入侵事件生成警報；例如安裝許可證、註冊裝置、應用健康策略、系統策略、訪問控制策略、入侵策略等。本檔案是《FireSIGHT系統安裝指南》的補充。

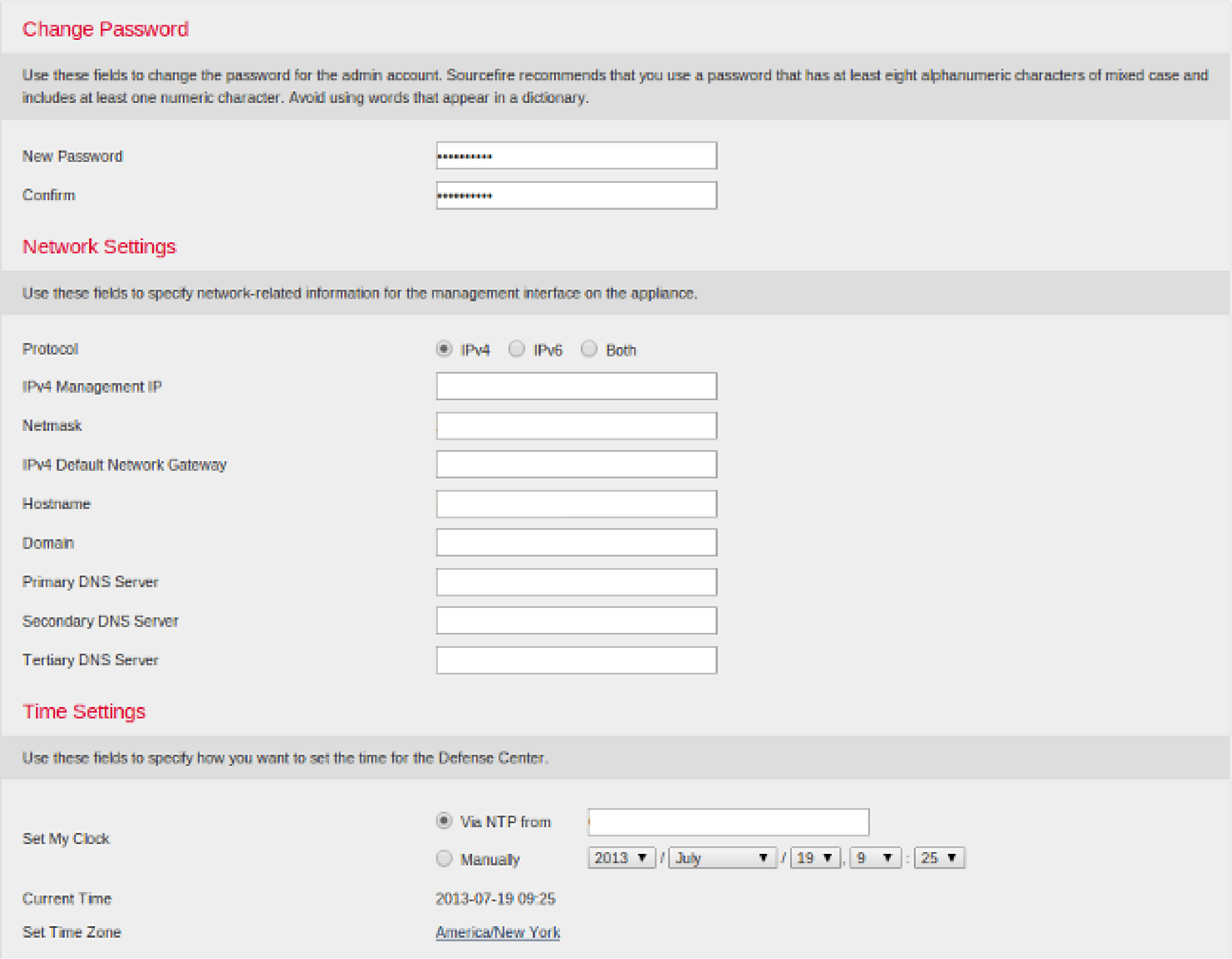
必備條件

本指南假定您仔細閱讀了《FireSIGHT系統安裝指南》。

組態

第1步：初始設定

在FireSIGHT管理中心上，您必須通過登入到Web介面並在設定頁面上指定初始配置選項來完成設定過程，如下所述。在此頁面上，必須更改管理員密碼，還可以指定網路設定（如域和DNS伺服器）以及時間配置。



Change Password

Use these fields to change the password for the admin account. Sourcefire recommends that you use a password that has at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

New Password	••••••••••
Confirm	••••••••••

Network Settings

Use these fields to specify network-related information for the management interface on the appliance.

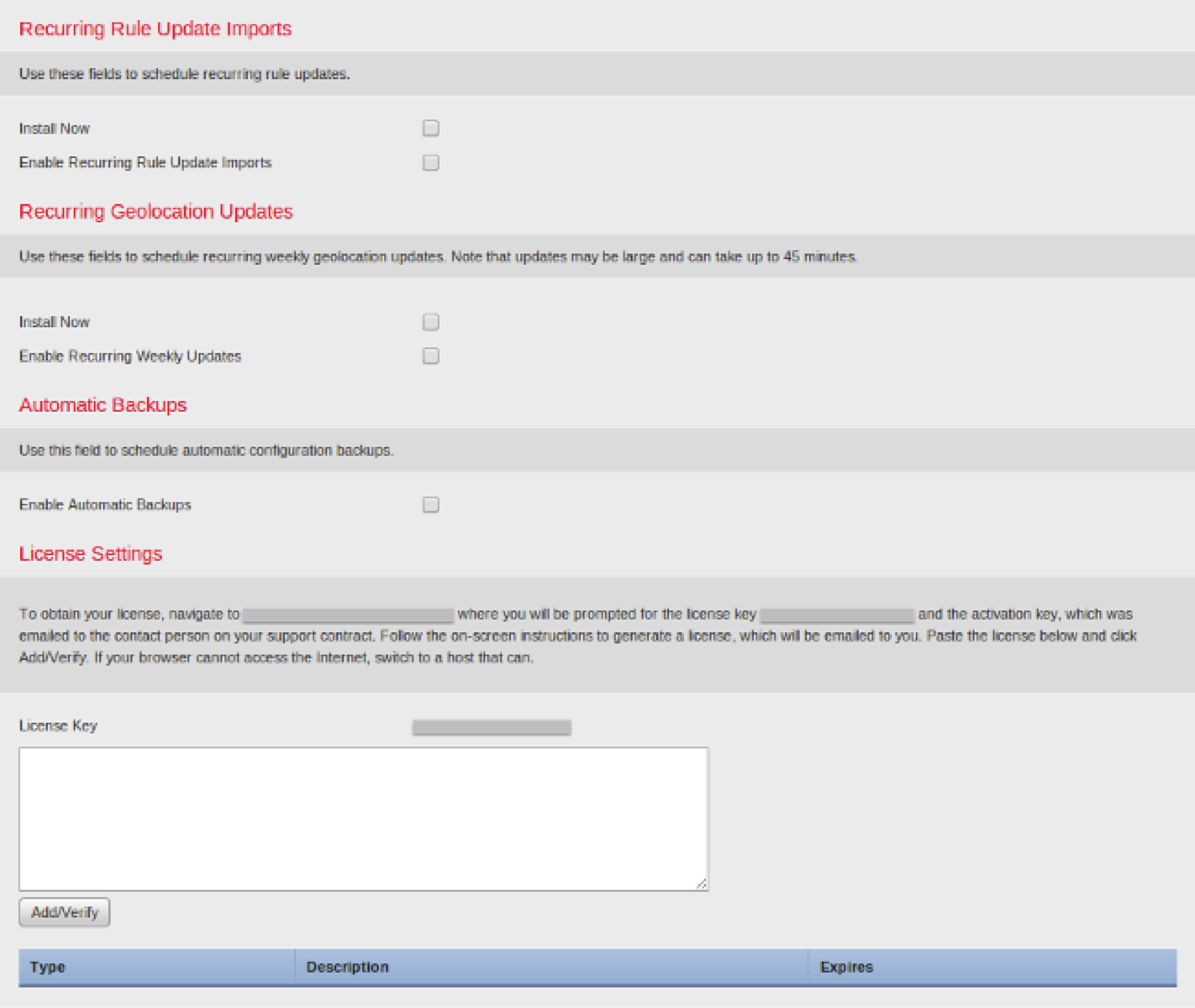
Protocol	● IPv4 ○ IPv6 ○ Both
IPv4 Management IP	
Netmask	
IPv4 Default Network Gateway	
Hostname	
Domain	
Primary DNS Server	
Secondary DNS Server	
Tertiary DNS Server	

Time Settings

Use these fields to specify how you want to set the time for the Defense Center.

Set My Clock	● Via NTP from ○ Manually 2013 ▼ / July ▼ / 19 ▼ , 9 ▼ : 25 ▼
Current Time	2013-07-19 09:25
Set Time Zone	America/New York

您可以選擇配置循環規則和地理位置更新以及自動備份。此時還可以安裝任何功能許可證。



Recurring Rule Update Imports

Use these fields to schedule recurring rule updates.

Install Now ☐

Enable Recurring Rule Update Imports ☐

Recurring Geolocation Updates

Use these fields to schedule recurring weekly geolocation updates. Note that updates may be large and can take up to 45 minutes.

Install Now ☐

Enable Recurring Weekly Updates ☐

Automatic Backups

Use this field to schedule automatic configuration backups.

Enable Automatic Backups ☐

License Settings

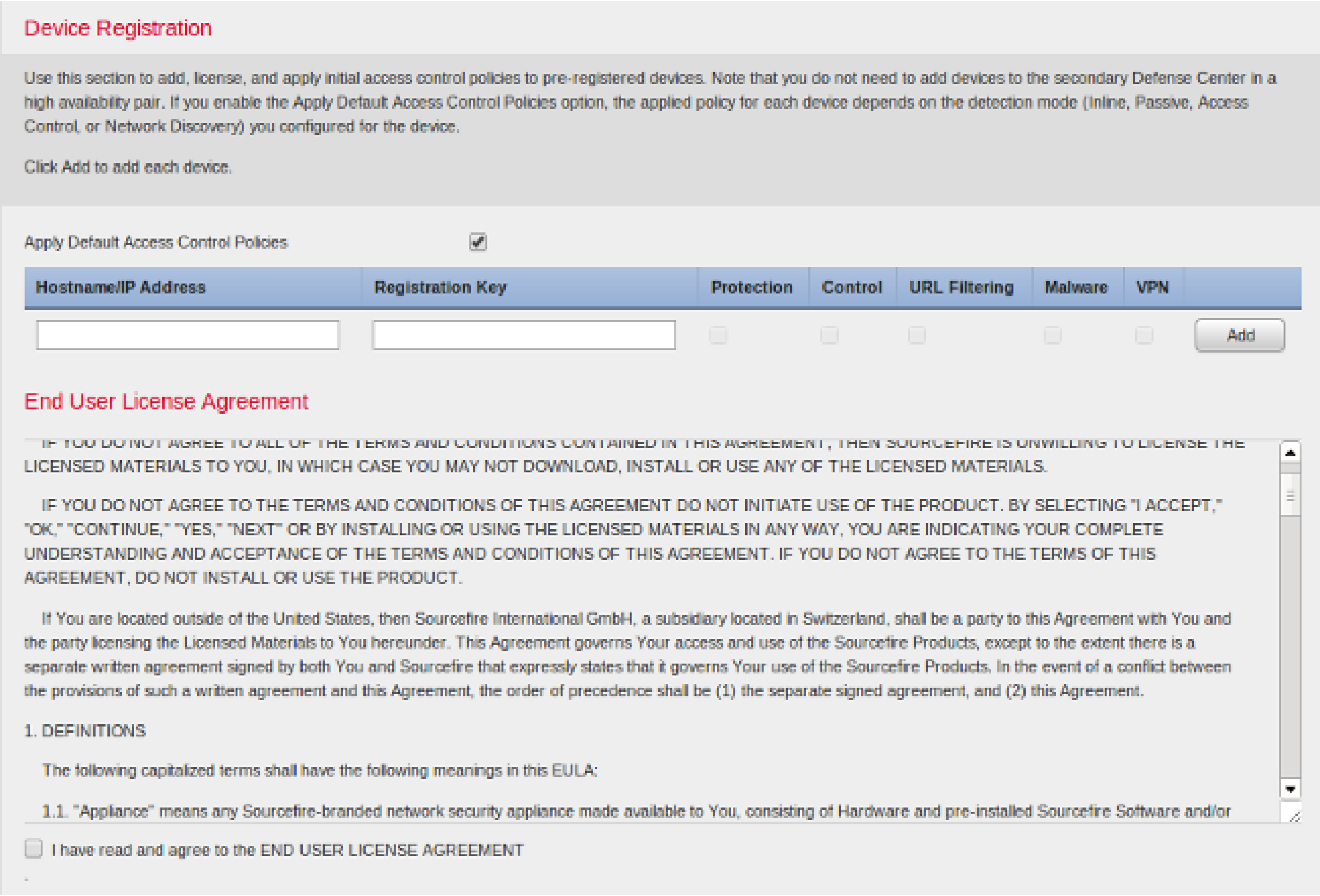
To obtain your license, navigate to [redacted] where you will be prompted for the license key [redacted] and the activation key, which was emailed to the contact person on your support contract. Follow the on-screen instructions to generate a license, which will be emailed to you. Paste the license below and click Add/Verify. If your browser cannot access the Internet, switch to a host that can.

License Key [redacted]

Add/Verify

Type	Description	Expires

在此頁面上，您還可以向FireSIGHT管理中心註冊裝置並指定檢測模式。在註冊過程中選擇的檢測模式和其他選項決定了系統建立的預設介面、內聯集和區域以及最初應用於受管裝置的策略。



Device Registration

Use this section to add, license, and apply initial access control policies to pre-registered devices. Note that you do not need to add devices to the secondary Defense Center in a high availability pair. If you enable the Apply Default Access Control Policies option, the applied policy for each device depends on the detection mode (Inline, Passive, Access Control, or Network Discovery) you configured for the device.

Click Add to add each device.

Apply Default Access Control Policies ☑

Hostname/IP Address	Registration Key	Protection	Control	URL Filtering	Malware	VPN	
		□	□	□	□	□	Add

End User License Agreement

IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT, THEN SOURCEFIRE IS UNWILLING TO LICENSE THE LICENSED MATERIALS TO YOU, IN WHICH CASE YOU MAY NOT DOWNLOAD, INSTALL OR USE ANY OF THE LICENSED MATERIALS.

IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT DO NOT INITIATE USE OF THE PRODUCT. BY SELECTING "I ACCEPT," "OK," "CONTINUE," "YES," "NEXT" OR BY INSTALLING OR USING THE LICENSED MATERIALS IN ANY WAY, YOU ARE INDICATING YOUR COMPLETE UNDERSTANDING AND ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL OR USE THE PRODUCT.

If You are located outside of the United States, then Sourcefire International GmbH, a subsidiary located in Switzerland, shall be a party to this Agreement with You and the party licensing the Licensed Materials to You hereunder. This Agreement governs Your access and use of the Sourcefire Products, except to the extent there is a separate written agreement signed by both You and Sourcefire that expressly states that it governs Your use of the Sourcefire Products. In the event of a conflict between the provisions of such a written agreement and this Agreement, the order of precedence shall be (1) the separate signed agreement, and (2) this Agreement.

1. DEFINITIONS

The following capitalized terms shall have the following meanings in this EULA:

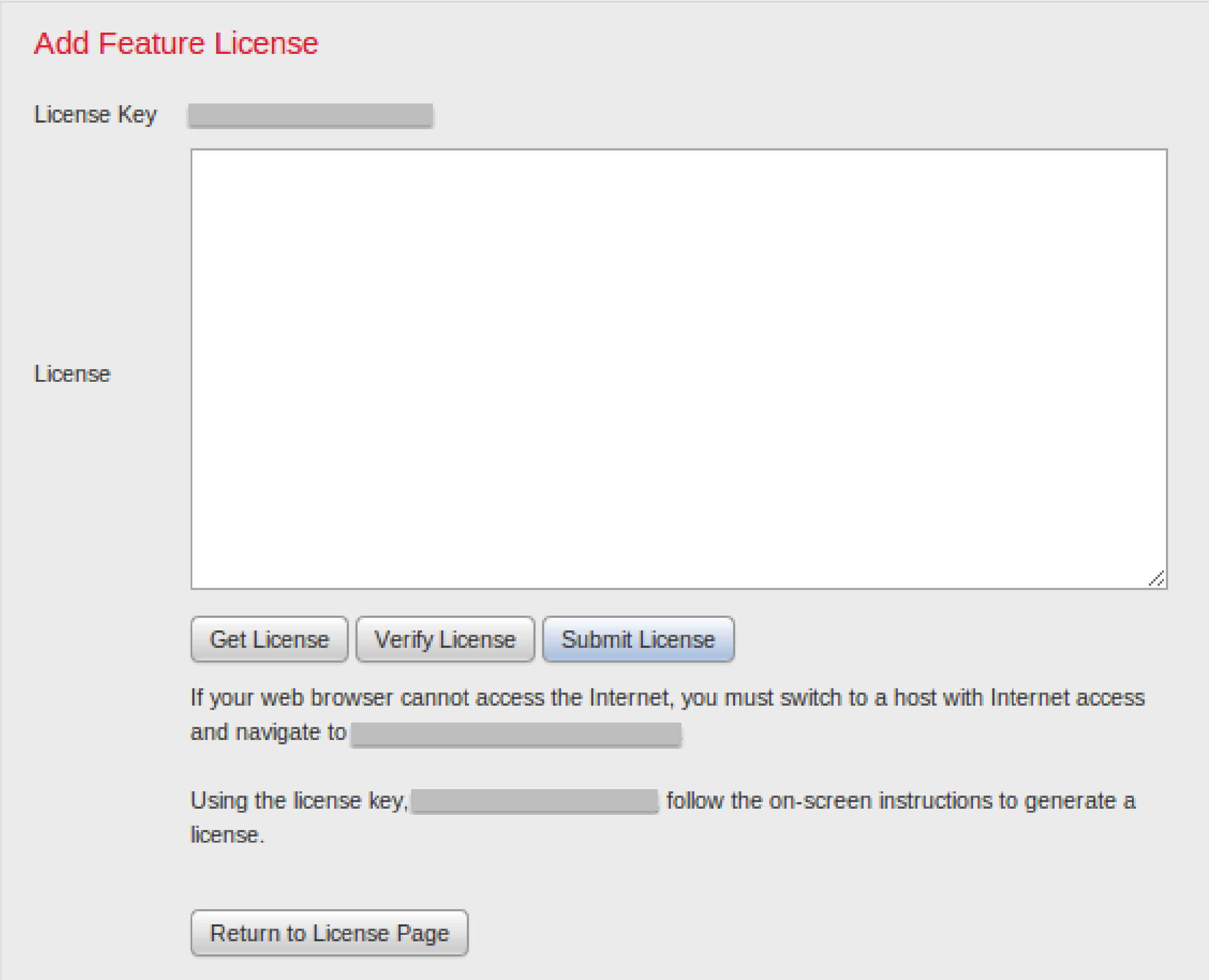
1.1. "Appliance" means any Sourcefire-branded network security appliance made available to You, consisting of Hardware and pre-installed Sourcefire Software and/or

□ I have read and agree to the END USER LICENSE AGREEMENT

第2步：安裝許可證

如果在初始設定頁面期間未安裝許可證，可以通過以下步驟完成任務：

- 導航到以下頁面：**System > Licenses**。
- 按一下**Add New License**。



Add Feature License

License Key [redacted]

License

If your web browser cannot access the Internet, you must switch to a host with Internet access and navigate to [redacted]

Using the license key, [redacted] follow the on-screen instructions to generate a license.

如果您沒有獲得許可證，請聯絡您帳戶的銷售代表。

步驟3:應用系統策略

系統策略指定FireSIGHT管理中心和受管裝置之間的身份驗證配置檔案和時間同步的配置。 要配置或應用系統策略，請導航到**System > Local > System Policy**。 提供了預設系統策略，但需要應用於任何受管裝置。

第4步：應用運行狀況策略

運行狀況策略用於配置受管裝置如何向FireSIGHT管理中心報告其運行狀況狀態。 要配置或應用運行狀況策略，請導航到**Health > Health Policy**。 提供了預設運行狀況策略，但需要應用到任何受管裝置。

第5步：註冊受管裝置

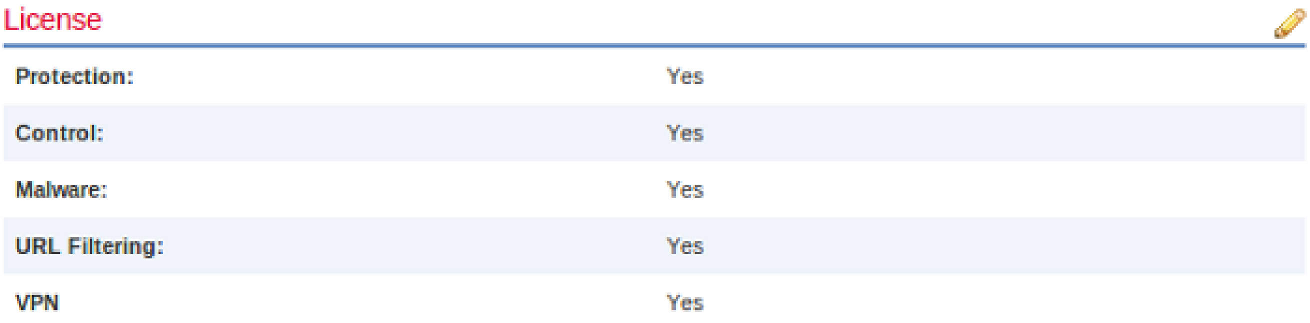
如果在初始設定頁面期間未註冊裝置，請閱讀本文檔，瞭解有關如何向FireSIGHT管理中心註冊裝

置的說明。

第6步：啟用已安裝的許可證

在裝置上使用任何功能許可證之前，您需要為每個受管裝置啟用該許可證。

1. 導航到以下頁面：**Devices > Device Management**。
2. 點選要為其啟用許可證的裝置，並輸入Device頁籤。
3. 點選License旁邊的**Edit**(*鉛筆圖示*)。

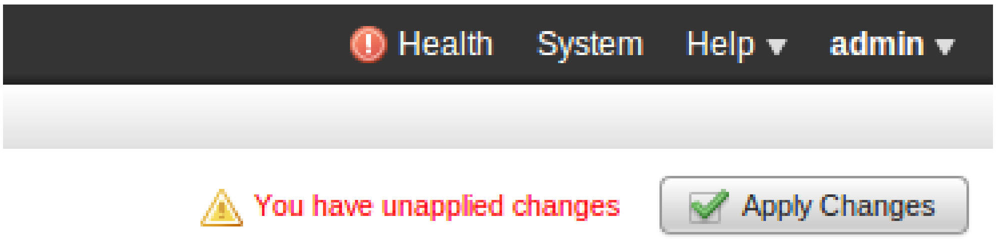


License

Protection:	Yes
Control:	Yes
Malware:	Yes
URL Filtering:	Yes
VPN	Yes

為此裝置啟用所需的許可證，然後按一下**儲存**。

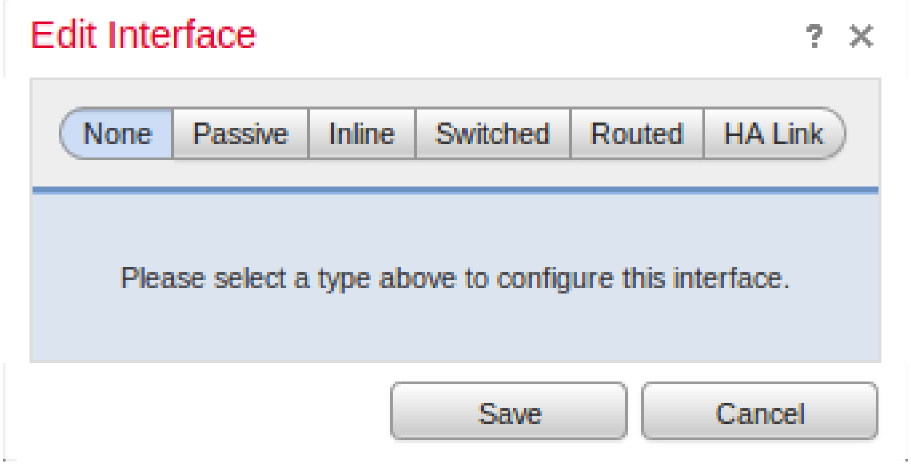
請注意右上角*出現*「*You have unapplied changes*（您有未應用的更改）」資訊。即使您導航離開裝置管理頁面，直到按一下**Apply Changes**按鈕，此警告仍保持活動狀態。



You have unapplied changes

第7步：配置感應介面

1. 導航到以下頁面**Devices > Device Management**。
2. 按一下所選感測器的**編輯**（鉛筆）圖示。
3. 在**Interfaces**頁籤下，按一下所選介面的**Edit**圖示。

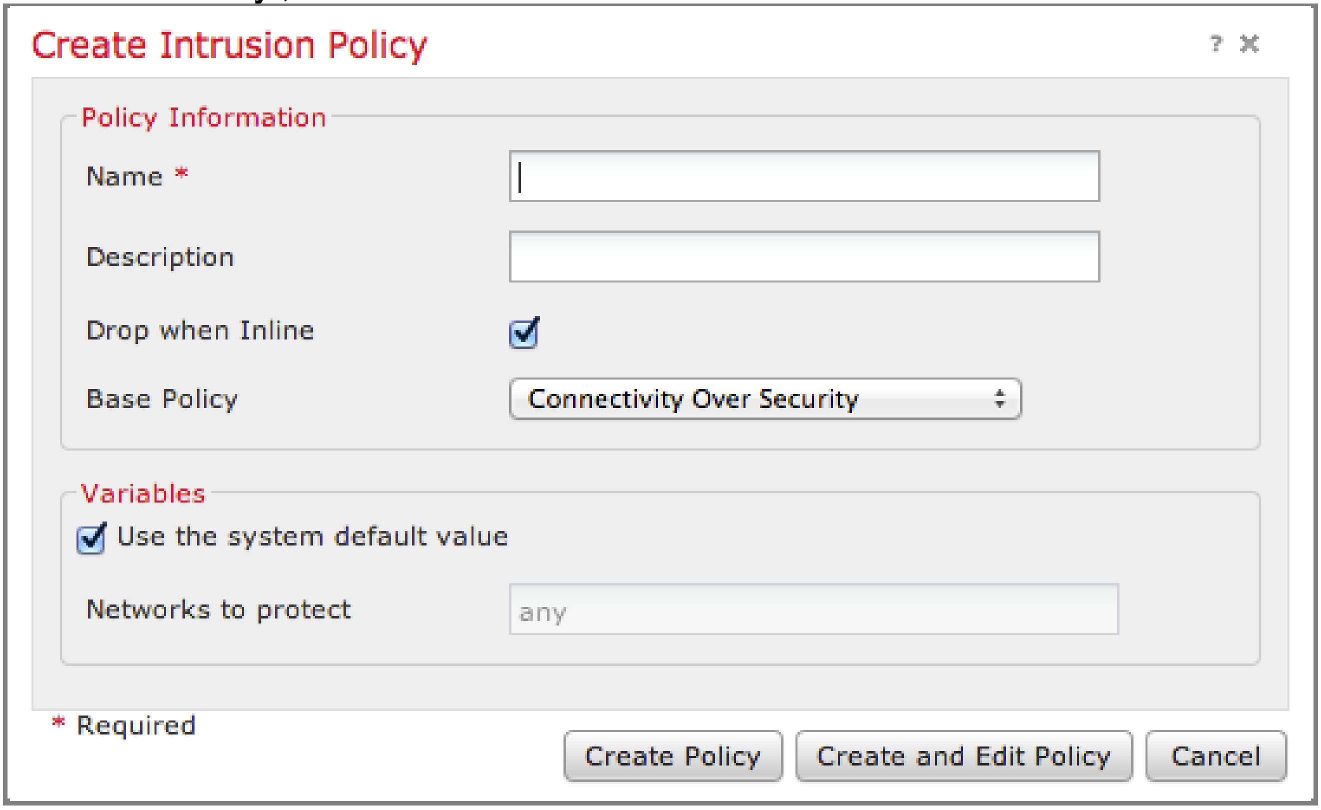

Edit Interface

Please select a type above to configure this interface.

選擇被動介面配置或內聯介面配置。交換介面和路由介面不在本文的討論範圍之內。

第8步：配置入侵策略

- 導航到以下頁面：**Policies > Intrusion > Intrusion Policy。**
- 按一下**Create Policy**，將顯示以下對話方塊：


Create Intrusion Policy

Policy Information

Name *	
Description	
Drop when Inline	☑
Base Policy	Connectivity Over Security

Variables

☑ Use the system default value

Networks to protect: any

* Required

必須分配名稱並定義要使用的基本策略。根據您的部署，您可以選擇啟用內聯**時丟棄**選項。定義要保護的網路，以減少誤報並提高系統效能。

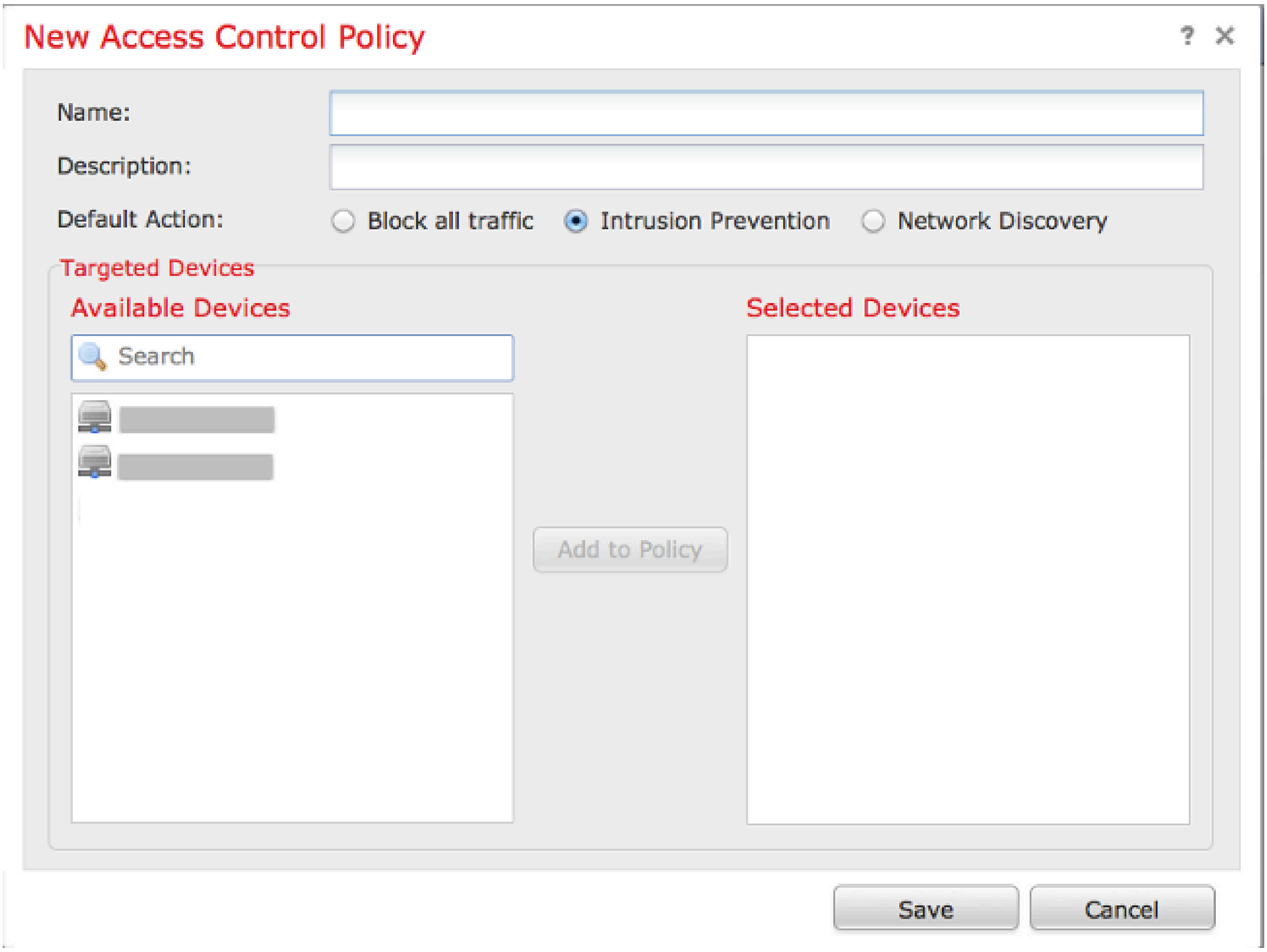
按一下**Create Policy**將儲存設定並建立IPS策略。如果要對入侵策略進行任何修改，可以選擇**Create and Edit Policy**。

> **附註**：入侵策略作為訪問控制策略的一部分應用。 應用入侵策略後，通過按一下**Reapply**按鈕，可以應用所有修改而無需重新應用整個訪問控制策略。

第9步：配置並應用訪問控制策略

1.定位至**策略>訪問控制**。

2.按一下**New Policy**。



New Access Control Policy

Name:

Description:

Default Action: ○ Block all traffic ● Intrusion Prevention ○ Network Discovery

Targeted Devices

Available Devices

[redacted]

[redacted]

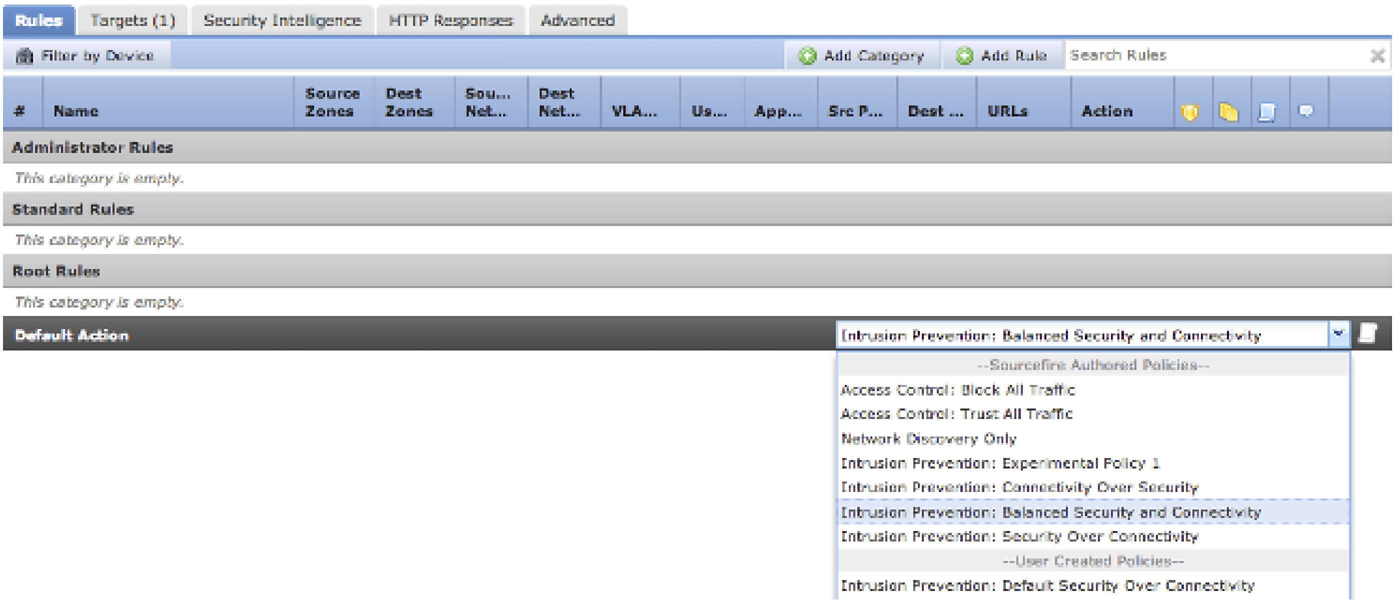
Selected Devices

3.提供策**略的**名稱和**說明**。

4.選擇**Intrusion Prevention**作為**訪問控制策略的Default Action**。

5.最後選擇要應用訪問控制策略的**目標裝置**，然後按一下**儲存**。

6.為預設操作選擇入侵策略。



Rules | Targets (1) | Security Intelligence | HTTP Responses | Advanced

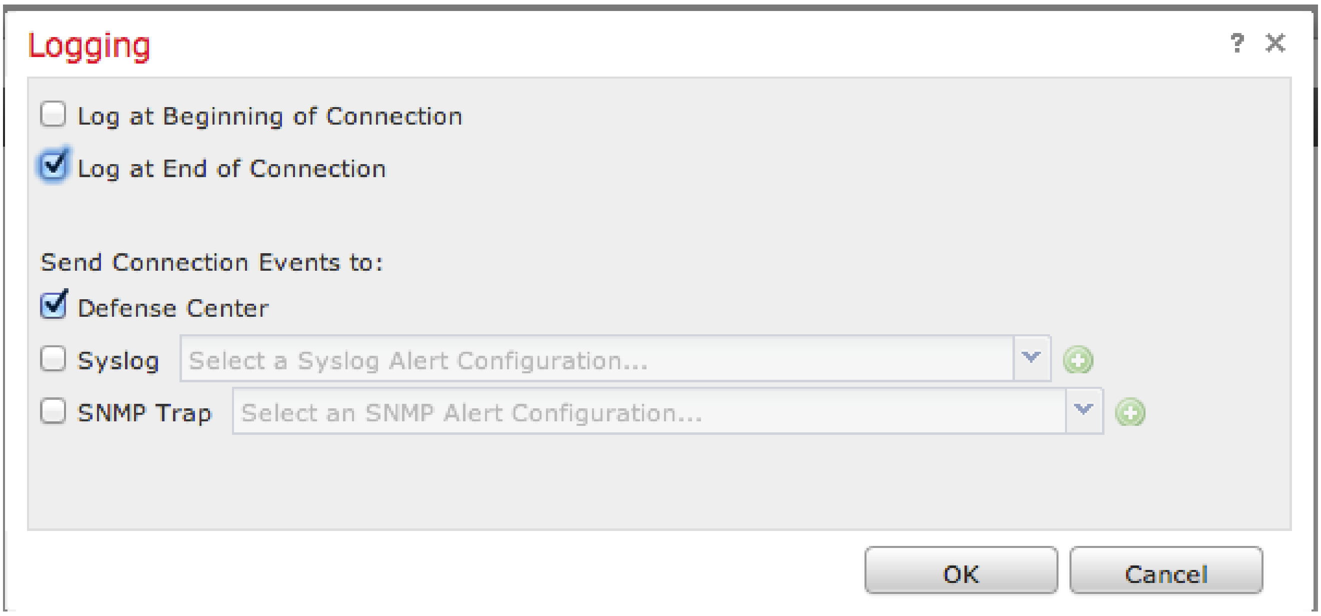
Filter by Device | Add Category | Add Rule | Search Rules

#	Name	Source Zones	Dest Zones	Sou... Net...	Dest Net...	VLA...	Us...	App...	Src P...	Dest ...	URLs	Action
Administrator Rules												
This category is empty.												
Standard Rules												
This category is empty.												
Root Rules												
This category is empty.												

Default Action: Intrusion Prevention: Balanced Security and Connectivity

--Sourcefire Authored Policies--
Access Control: Block All Traffic
Access Control: Trust All Traffic
Network Discovery Only
Intrusion Prevention: Experimental Policy 1
Intrusion Prevention: Connectivity Over Security
Intrusion Prevention: Balanced Security and Connectivity
Intrusion Prevention: Security Over Connectivity
--User Created Policies--
Intrusion Prevention: Default Security Over Connectivity

7.必須啟用連線日誌記錄才能生成連線事件。按一下**Default Action**右側的下拉選單。



Logging

□ Log at Beginning of Connection
☑ Log at End of Connection

Send Connection Events to:
☑ Defense Center
□ Syslog — Select a Syslog Alert Configuration...
□ SNMP Trap — Select an SNMP Alert Configuration...

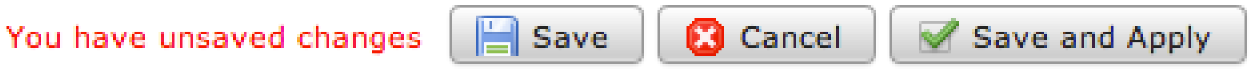
8.選擇在連線的開始或結束處記錄連線。可在FireSIGHT管理中心、系統日誌位置或通過SNMP記錄事件。

> **附註**：建議不要在連線的兩端進行登入，因為每個連線（被阻止的連線除外）將記錄兩次。在開頭記錄對將被阻止的連線很有用，在結尾記錄對所有其它連線都很有用。

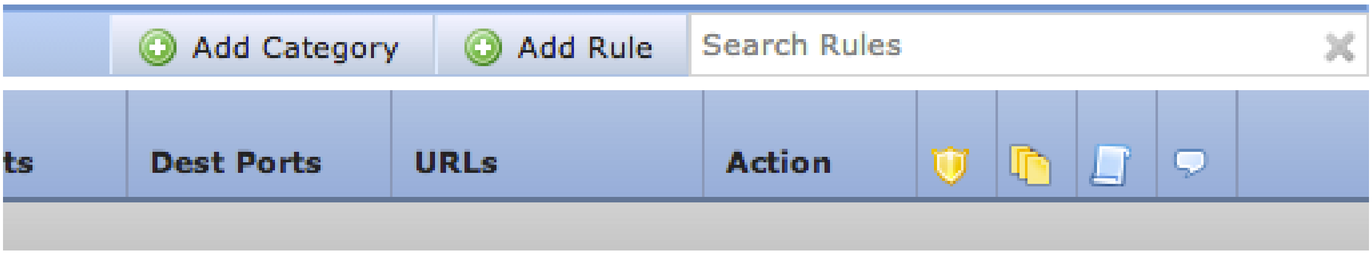
9.按一下**確定**。請注意，日誌圖示的顏色已更改。

10.此時可以新增**訪問控制**規則。您可以使用的選項取決於已安裝的許可證型別。

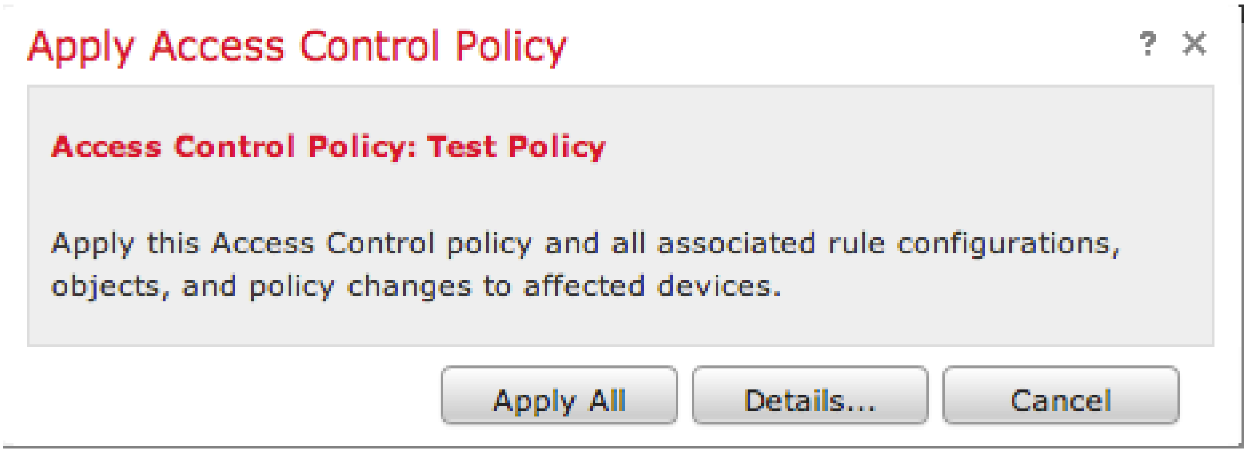
11.完成更改後。按一下**Save and Apply**按鈕。 在按一下按鈕之前，您會看到一條消息，指出您的策略在右上角有未儲存的更改。



You have unsaved changes



您可以選擇僅使用**儲存**更改，或按一下**儲存並應用**。如果您選擇後者，則會出現以下視窗。



Apply Access Control Policy

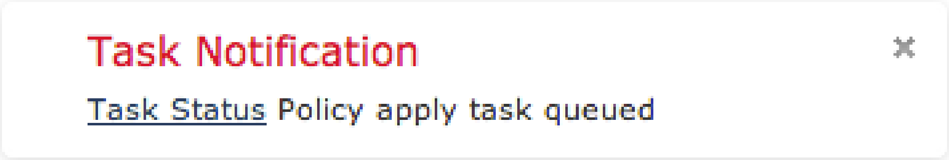
Access Control Policy: Test Policy

Apply this Access Control policy and all associated rule configurations, objects, and policy changes to affected devices.

12. **Apply All**會將訪問控制策略和任何關聯的入侵策略應用到目標裝置。

附註：如果首次應用入侵策略，則無法取消選擇它。

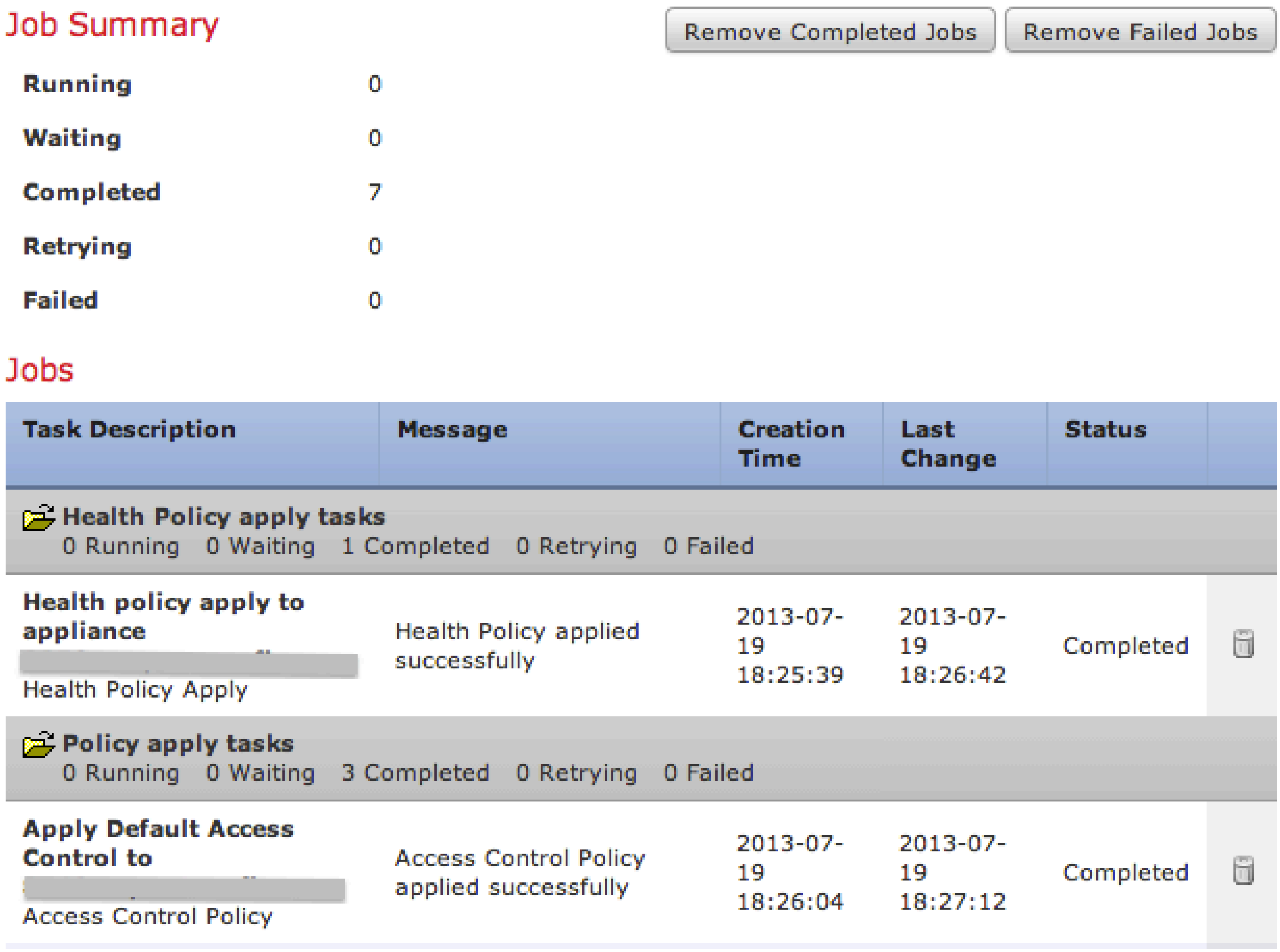
13.您可以按一下頁面頂部顯示的通知上的**任務狀態**連結，或通過導航至以下各項來監控任務的狀態：**System > Monitoring > Task Status**



Task Notification

Task Status Policy apply task queued

14.按一下「任務狀態」連結以監視應用訪問控制策略的進度。



Job Summary

Running	0
Waiting	0
Completed	7
Retrying	0
Failed	0

Jobs

Task Description	Message	Creation Time	Last Change	Status
Health Policy apply tasks 0 Running 0 Waiting 1 Completed 0 Retrying 0 Failed				
Health policy apply to appliance [redacted] Health Policy Apply	Health Policy applied successfully	2013-07-19 18:25:39	2013-07-19 18:26:42	Completed
Policy apply tasks 0 Running 0 Waiting 3 Completed 0 Retrying 0 Failed				
Apply Default Access Control to [redacted] Access Control Policy	Access Control Policy applied successfully	2013-07-19 18:26:04	2013-07-19 18:27:12	Completed

步驟10:驗證FireSIGHT管理中心是否收到事件

訪問控制策略應用完成後，您應該開始檢視連線事件，具體取決於流量入侵事件。

其他建議

您還可以在系統上配置以下其他功能。有關實施的詳細資訊，請參閱《使用手冊》。

- 定時備份
- 自動軟體更新、SRU、VDB和GeoLocation下載/安裝。
- 通過LDAP或RADIUS的外部身份驗證