

# 可能安裝在FireSIGHT系統上的更新檔案的型別

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[更新型別](#)

[Web介面上的更新頁面](#)

[產品更新](#)

[規則更新](#)

[GeoDB更新](#)

[安全情報更新](#)

[URL過濾更新](#)

## 簡介

本文檔概述了FireSIGHT系統為保持系統最新而安裝的各種型別的更新檔案。有些檔案會更新FireSIGHT系統的軟體和作業系統，而有些檔案會增強安全性。

## 必要條件

### 需求

本文件沒有特定需求。

### 採用元件

本檔案中的資訊是根據以下硬體和軟體版本：

- Sourcefire FirePOWER 7000系列裝置、8000系列裝置和NGIPS虛擬裝置
- Sourcefire軟體版本5.0或更新版本

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。

## 更新型別

在FireSIGHT系統上，可以安裝以下型別的更新：

	說明	範例
升級	<ul style="list-style-type: none"><li>• 介紹新功能和元件。</li><li>• 包括錯誤修正。</li></ul>	Sourcefire_3 5.4.0-763.sh
補丁	<ul style="list-style-type: none"><li>• 解決已知問題。</li><li>• 包括先前修補程式中提供的解析度。</li></ul>	Sourcefire_3 59.sh
Sourcefire規則更新(SRU)	<ul style="list-style-type: none"><li>• 可以安裝在5.0或更高版本的軟體上。</li><li>• 更新Snort規則和共用對象規則。</li></ul>	Sourcefire_R
漏洞資料庫(VDB)	<ul style="list-style-type: none"><li>• 更新應用程式和作業系統的指紋、檢測器和漏洞資訊。</li></ul>	Sourcefire_V 241.sh
SourceFire GeoLocation資料庫更新(GeoDB)	<ul style="list-style-type: none"><li>• 更新與可路由IP地址關聯的地理資料。</li></ul>	Sourcefire_G
安全情報源 URL過濾資料	<ul style="list-style-type: none"><li>• 更新用於將IP地址列入黑名單的IP地址清單。</li><li>• 更新訪問控制規則中用於URL過濾的資料。</li></ul>	FireSIGHT管理中 FireSIGHT管理中

## Web介面上的更新頁面

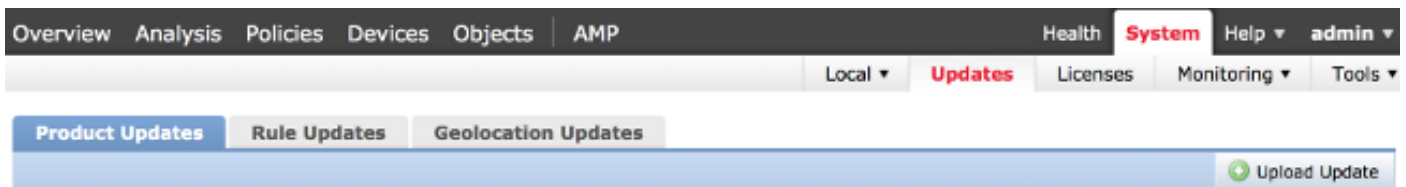
要更新FireSIGHT管理中心，您可能必須導航到Web介面的各個頁面。這取決於要下載的更新型別。本節提供了指向各種更新頁面的導航。

### 產品更新

若要上傳或安裝這些元件，請選擇**System > Updates**，然後選擇**Product Updates**頁籤：

- 升級
- 補丁
- VDB

如果要直接從思科支援網站下載升級、修補程式或VDB檔案，請按一下「**Download Updates**」。此按鈕在頁面底部可用。或者，如果您手動從[思科支援網站](#)下載檔案，並希望將其上傳到FireSIGHT系統，請按一下「**Upload Update**」。



### 規則更新

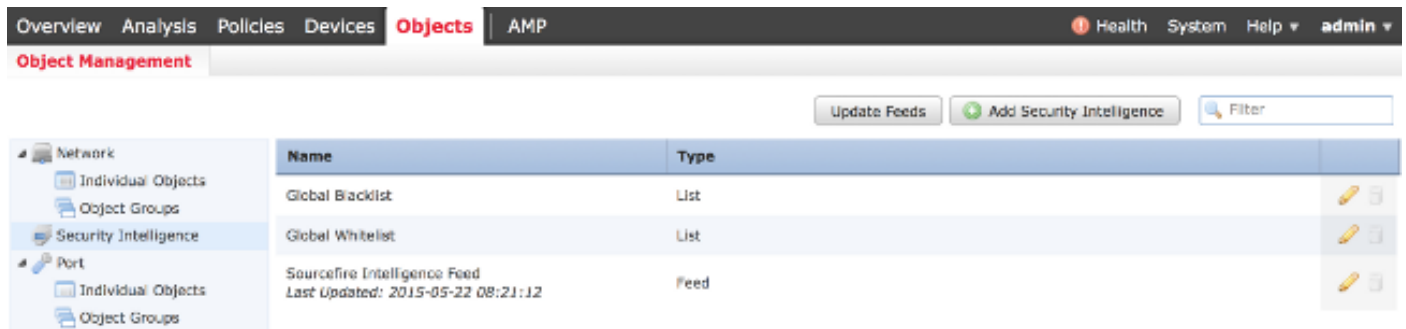
要更新SRU，請選擇**System > Updates**，然後選擇**Rule Updates**頁籤。

### GeoDB更新







要更新GeoDB，請選擇**System > Updates**，然後選擇**Geolocation Updates**頁籤。

## 安全情報更新

要更新安全情報源，請選擇**對象>對象管理**。從左側面板中選擇**Security Intelligence**選項，然後按一下**Update Feeds**。如果要更新自定義源，或者要建立自定義清單，請按一下**Add Security Intelligence**。

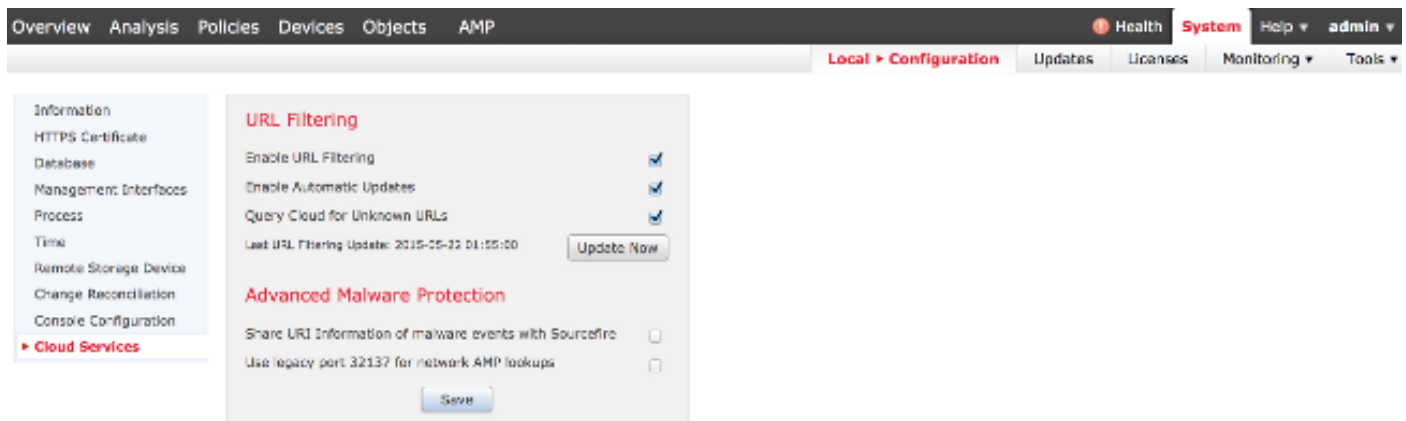


The screenshot shows the AMP Object Management interface. The top navigation bar includes Overview, Analysis, Policies, Devices, **Objects**, and AMP. The left sidebar shows a tree view with Network, Security Intelligence, and Port categories. The main content area displays a table of security intelligence feeds.

Name	Type	
Global Blacklist	List	 
Global Whitelist	List	 
Sourcefire Intelligence Feed Last Updated: 2015-05-22 08:21:12	Feed	 

## URL過濾更新

要更新URL過濾資料庫，請選擇**System > Local > Configuration**。選擇**Cloud Services**，然後按一下**Update Now**。



The screenshot shows the AMP System Configuration interface. The top navigation bar includes Overview, Analysis, Policies, Devices, Objects, AMP, Health, **System**, Help, and admin. The left sidebar shows a tree view with Information, Database, Management Interfaces, Process, Time, Remote Storage Device, Change Reconciliation, Console Configuration, and **Cloud Services**. The main content area displays the URL Filtering configuration page.

**URL Filtering**

- Enable URL Filtering
- Enable Automatic Updates
- Query Cloud for Unknown URLs
- Last URL Filtering Update: 2015-05-22 04:05:00

**Advanced Malware Protection**

- Share URI Information of malware events with Sourcefire
- Use legacy port 32137 for network AMP lookups