paloalto TECHDOCS

進階 WildFire 管理

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

April 8, 2025

Table of Contents

進階 WildFire 概要介紹

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

進階 WildFire™ 同時使用動態和靜態分析，以及智慧執行階段記憶體分析，以偵測高規避性威脅並建立防護，封鎖惡意程式，進而偵測並防範零時差惡意軟體的攻擊。

進階 WildFire 分析環境可識別之前未知的惡意軟體，並產生特徵碼，供 Palo Alto Networks NGFW 用於檢測和封鎖惡意軟體。當 Palo Alto Networks 防火牆檢測到未知範例時，防火牆會從任何應用程式自動轉送所有支援的檔案類型到 WildFire 公共雲端服務，以進行進階 WildFire 分析。根據範例在沙箱中分析和執行時顯示的屬性、行為和活動，進階 WildFire 會判定範例為良性、灰色軟體、網路釣魚或惡意軟體，並產生特徵碼以識別新發現的惡意軟體，讓最新的特徵碼可供全域即時搜尋。然後，所有 Palo Alto Networks 防火牆都可以比較傳入的範例與這些特徵碼，以自動封鎖單一防火牆先檢測到的惡意軟體。

如需詳細瞭解進階 WildFire 或立即上手進階 WildFire，請參閱下列主題：

- 請參閱進階 WildFire 概念，深入瞭解可提交進行 WildFire 分析、WildFire 裁定和擷取 WildFire 特徵碼的範例類型。
- 深入瞭解您可透過防火牆設定的進階 WildFire 部署。您可以將想要分析的樣本提交至 Palo Alto Networks 託管的 WildFire 雲端（本機託管的 WildFire 私人雲端），或使用混合型雲端，使防火牆提交特定樣本至公共雲端，並提交另一些特定樣本至私人雲端。
- 開始使用進階 WildFire 以定義您想要提交進行分析的樣本，並開始向 WildFire 雲端提交樣本。
- 若要部署 WildFire 設備，請參閱 WildFire 設備管理。

訂閱選項

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

基本 WildFire 服務為 Palo Alto Networks 次世代防火牆的一部分已被納入，無需進階 WildFire 訂閱。透過基本 WildFire 服務，防火牆可以轉送可攜式執行檔 (PE) 以進行分析，並可擷取僅具防毒和/或威脅防護更新的進階 WildFire 特徵碼，該特徵碼每 24-48 小時可用。

Palo Alto Networks 提供多種訂閱選項：

- **WildFire**—WildFire 訂閱可將範例轉送至進階 WildFire 雲端來提供惡意軟體防護，其中使用一系列分析環境來偵測並防止未知的惡意軟體威脅，藉此產生防護，以封鎖威脅的進一步執行個體。根據訂閱，您可以存取定期進階 WildFire 特徵碼更新、進階檔案類型轉送，並使用 WildFire API 上傳檔案。若您正在使用需要內部部署解決方案的環境，WildFire 訂閱可用於將檔案轉送至本機 WildFire 設備。
- 進階 **WildFire**—（PAN-OS 10.0 及更高版本）進階 WildFire 訂閱方案包含標準 WildFire 訂閱的所有功能，並透過先進的雲端檢測器提供範例分析，讓功能更強大。先進的檢測系統使用智慧即時執行階段記憶體分析、執行階段 DLL 模擬、自動解壓縮、家族分類、隱形觀察和其他技術來分析範例，以鎖定高規避性惡意軟體。
- 獨立 **WildFire API**—使用 SOAR 工具、自訂安全應用程式和其他威脅評估軟體的 Palo Alto Networks 客戶可以透過提供 API 專屬存取權的獨立訂閱方案，存取 WildFire 雲端的進階檔案分析功能。如此一來，您便能利用基於 WildFire 的分析，而無需依賴 Palo Alto Networks 防火牆做為轉送機制。WildFire 獨立 API 訂閱可讓您直接查詢 WildFire 雲端威脅資料庫，以取得潛在惡意內容的相關資訊，並根據貴組織的特定需求使用 WildFire 的進階威脅分析，提交檔案進行分析。訂閱方案的增強存取限制讓各規模的組織皆能根據使用情況自訂存取限制，其中包括可調式授權，即可執行特定數量的檔案/報表查詢、範例提交（用於進階 WildFire 分析）或同時執行兩者。如需更多詳細資訊，請參閱 WildFire API 參考。

標準 WildFire 訂閱包含以下功能：

- 即時更新—（PAN-OS 10.0 及更高版本）一旦進階 WildFire 公共雲端可以產生特徵碼，防火牆就可為新發現的惡意軟體擷取進階 WildFire 特徵碼。在樣本檢查期間下載的特徵碼將儲存在防火牆快取中，並且可用於快速（本機）尋找。此外，為了最大化覆蓋範圍，啟用即時特徵碼後，防火牆還會定期自動下載特徵碼套件。這些補充特徵碼將會新增至防火牆快取中，在其變

得過時並經過重新整理，或被新特徵碼覆寫之前一直可用。建議您使用即時進階 WildFire 更新設定。

選取 **Device**（裝置） > **Dynamic Updates**（動態更新），然後啟用防火牆以即時取得最新的進階 WildFire 特徵碼。

- 五分鐘更新—（所有 PAN-OS 版本）進階 WildFire 公共雲端可以每五分鐘為新發現的惡意軟體產生和散佈 WildFire 特徵碼，您可以設定防火牆每分鐘擷取並安裝這些特徵碼，讓防火牆在特徵碼可用一分鐘內即獲得最新的特徵碼。

  若您使用 *PAN-OS 10.0* 或更高版本，最佳做法是使用即時進階 *WildFire* 更新，而非排程週期性更新。

  選取 **Device**（裝置） > **Dynamic Updates**（動態更新）即可讓防火牆獲得最新的進階 WildFire 特徵碼。根據您的進階 WildFire 部署，您可以設定以下一或兩項特徵碼套件更新：

  - **WildFire**—從 WildFire 公共雲端獲得最新的特徵碼。
  - **WF-私人**—從為本機產生特徵碼和 URL 類別的 WildFire 設備獲得最新特徵碼。
- 進階 **WildFire** 內嵌 **ML**—（PAN-OS 10.0 和更高版本）透過防火牆資料平面上的機器學習 (ML)，即時防止可攜可執行檔、可執行連結格式 (ELF) 檔案和 PowerShell 指令碼的惡意變體進入網路。利用防火牆上的進階 WildFire 雲端分析技術，進階 WildFire 內嵌 ML 會評估各種檔案詳細資料（包括解碼器欄位和模式）來動態偵測指定類型的惡意檔案，以制訂高可能性的檔案分類。此保護擴展到威脅的當前未知變體及未來變體，這些威脅與 Palo Alto Networks 已確定為惡意的特徵相符。進階 WildFire 內嵌 ML 對現有防毒設定檔保護設定進行了補充。此外，您可以指定檔案雜湊例外狀況，以排除遇到的所有誤判，這使您能夠在設定檔中建立更細微的規則來滿足特定的安全需求。
- 檔案類型支援—除 PE 外，進階 WildFire 分析的轉送進階檔案類型，包括 APK、Flash 檔案、PDF、Microsoft Office 檔案、Java Applet、Java 檔案 (.jar 及 .class) 和 HTTP/HTTPS 電子郵件連結的進階檔案類型轉送包含在 SMTP 和 POP3 電子郵件訊息中。（WildFire 私人雲端分析不支援 APK、Mac OS X、Linux (ELF) 、歸檔 (RAR/7-Zip) 以及指令碼（JS、BAT、VBS、Shell 指令碼、PS1 及 HTA）檔案）。
- 進階 **WildFire API**—存取 WildFire API，可直接以程式設計方式存取進階 WildFire 公共雲端或 WildFire 私人雲端。使用 API 提交檔案進行分析，以及擷取後續進階 WildFire 分析報告。根據進階 WildFire 或 WildFire 訂閱，您每天可以提交最多 150 個範例和 1,050 個範例查詢。這些每日樣本提交限制可以根據組織的特定需求進行延伸。如需詳細資訊，請聯絡您的 Palo Alto Networks 業務代表。
- **WildFire** 私有和混合型雲端支援 —轉送檔案進行進階 WildFire 分析。WildFire 私人雲端和 WildFire 混合型雲端部署都要求防火牆可以提交樣本至 WildFire 設備。啟用 WildFire 設備僅需要支援授權。

如果您已購買進階 WildFire 訂閱，請務必啟動授權，然後便可充分利用訂閱專屬的 WildFire 功能。

進階 WildFire 訂閱包含以下功能：

- 智慧執行階段記憶體分析—智慧執行階段記憶體分析是雲端型的進階分析引擎，可與靜態和動態分析引擎相結合，以偵測並防止逃避惡意軟體威脅。進階威脅所使用的規避技術包括但不限於使用偽裝策略、顯示定制設計 / 暫時行為的跡象，使用複雜工具建立，並具快速傳播特性的惡意軟體。透過雲端式偵測基礎架構，內向分析偵測器可操作多種偵測機制，這些機制會自動更新和部署，而不需使用者下載內容更新套件或執行資源密集型、以設備為基礎的分析儀。雲端式偵測引擎會根據用於分析進階 WildFire 範例的 ML 型資料集持續監控和更新，並取得 Palo Alto Networks 威脅研究人員的額外支援。這些研究人員透過人工干預達到準確度高的偵測增強功能。

  智慧執行階段記憶體分析仰賴現有 WildFire 分析設定檔設定，而不需任何其他設定；但您必須具作用中的進階 WildFire 授權。顯示規避和/或進階惡意軟體品質的範例會自動轉送至適當的分析環境。

進階 WildFire 概念

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

- 範例
- 防火牆轉送
- 工作階段資訊共享
- 分析環境
- 進階 WildFire 內嵌雲端分析
- 進階 WildFire 內嵌 ML
- 裁定
- 檔案分析
- 電子郵件連結分析
- URL 分析
- 壓縮和編碼檔案分析
- 進階 WildFire 特徵碼
- 進階 WildFire 範例

範例

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

我可以在哪裡使用這個？	我需要哪些內容？
• VM-Series • CN-Series	

範例為防火牆和公共 API 提交進行進階 WildFire 分析的所有檔案類型和電子郵件連結。請參閱 檔案分析 和 電子郵件連結分析 深入瞭解防火牆可提交進行進階 WildFire 分析的檔案類型和連結。

防火牆轉送

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

防火牆可轉送未知範例以及與防毒特徵碼相符的封鎖檔案，以根據設定的 WildFire 分析設定檔設定進行 WildFire 分析（**Objects**（物件） > **Security Profiles**（安全性設定檔） > **WildFire Analysis**（**WildFire** 分析））。除了檢測電子郵件中的連結、電子郵件中隨附的檔案和基於瀏覽器的檔案下載以外，防火牆還利用 App-ID 檢測應用程式內的檔案傳輸。對於防火牆偵測到的樣本，防火牆會分析其結構和內容，並將其與現有特徵碼對比。如果樣本與特徵碼相符，防火牆將應用為特徵碼定義的預設動作（允許、警示或封鎖）。如果範例與防毒特徵碼相符或與進階 WildFire 特徵碼對比後為未知範例，防火牆會轉送該範例進行進階 WildFire 分析。

預設情況下，防火牆也會轉送在其中偵測到未知樣本的工作階段相關資訊。若要管理防火牆轉送的工作階段資訊，請選取 **Device**（裝置） > **Setup**（設定） > **WildFire** 並編輯工作階段資訊設定。

工作階段資訊共享

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

我可以在哪裡使用這個？	我需要哪些內容？
• VM-Series • CN-Series	

除轉送未知和封鎖的樣本進行分析外，防火牆還會轉送關於樣本網路工作階段的資訊。Palo Alto Networks 使用工作階段資訊瞭解有關可疑網路事件內容、與惡意軟體相關的入侵指標、受影響的主機與用戶端，以及用於傳遞惡意軟體的更多資訊。

根據預設，系統會啟用工作階段資訊轉送功能；但您可以調整預設設定，選擇防火牆向 WildFire 雲端選項轉送的工作階段資訊類型。

- Strata Cloud Manager
- PAN-OS 和 Panorama

工作階段資訊共用 (Cloud Management)

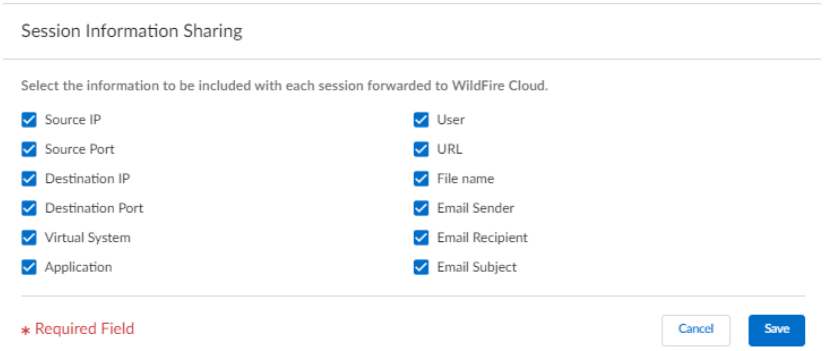
如果您使用 ***Panorama*** 管理 ***Prisma Access***：

請切換到 ***PAN-OS*** 頁籤並按照指示進行操作。

如果您使用 ***Prisma Access*** 雲端管理，請從此處繼續。

STEP 1 | 使用與您的 Palo Alto Networks 支援帳戶相關聯的認證，並登入中樞上的 Strata Cloud Manager 應用程式。

STEP 2 | 選取 **Manage**（管理）> **Configuration**（設定）> **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**）> **Security Services**（安全服務）> **WildFire and Antivirus**（**WildFire** 和防毒），然後設定您的 **Session Information Settings**（工作階段資訊設定）選項。



- **Source IP**（來源 **IP**）— 轉送傳送未知檔案的來源 IP 地址。
- **Source Port**（來源連接埠）— 轉送傳送未知檔案的來源連接埠。
- **Destination IP**（目的地 **IP**）— 轉送未知檔案的目的地 IP 地址。
- **Destination Port**（目的地連接埠）— 轉送未知檔案的目的地連接埠。
- **Virtual System**（虛擬系統）— 轉送偵測到未知檔案的虛擬系統。
- **Application**（應用程式）— 轉送傳輸未知檔案的使用者應用程式。

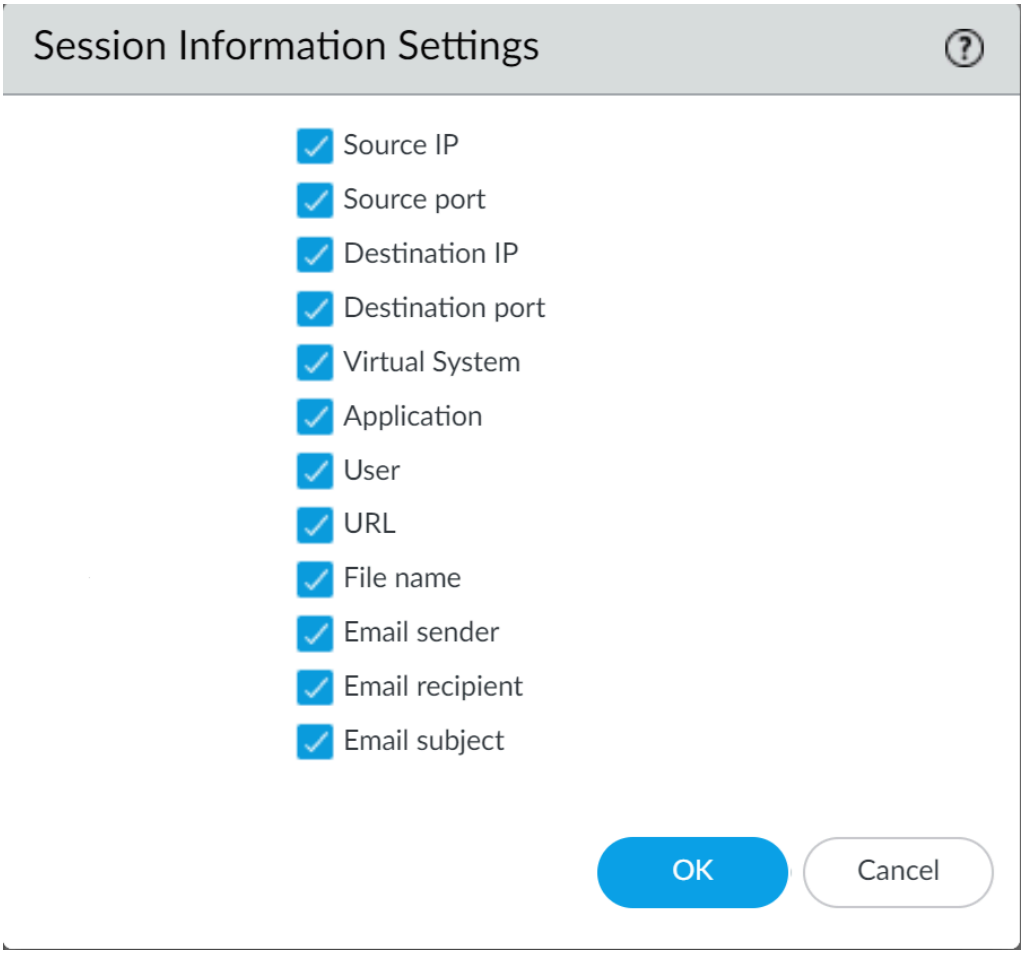
- **User**（使用者）— 轉送目標使用者。
- **URL**— 轉送與未知檔案相關的 URL。
- **Filename**（檔案名稱）— 轉送未知檔案的名稱。
- **Email sender**（電子郵件寄件者）— 轉送未知電子郵件連結的寄件者（該電子郵件寄件者的名字也會出現在 WildFire 日誌和報告中）。
- **Email recipient**（電子郵件收件者）— 轉送未知電子郵件連結的收件者（該電子郵件收件者的名字也會出現在 WildFire 日誌和報告中）。
- **Email subject**（電子郵件主旨）— 轉送未知電子郵件連結的主旨（該電子郵件主旨會出現在 WildFire 日誌和報告中）。

STEP 3 | **Save**（儲存）變更。

工作階段資訊共用（**PAN-OS** 和 **Panorama**）

STEP 1 | 登入 PAN-OS 網頁介面。

STEP 2 | 選擇 **Device**（裝置） > **Setup**（設定） > **WildFire** 然後選擇或清除下列 **Session Information Settings**（工作階段資訊設定）選項。



- **Source IP**（來源 **IP**）— 轉送傳送未知檔案的來源 IP 地址。
- **Source Port**（來源連接埠）— 轉送傳送未知檔案的來源連接埠。
- **Destination IP**（目的地 **IP**）— 轉送未知檔案的目的地 IP 地址。
- **Destination Port**（目的地連接埠）— 轉送未知檔案的目的地連接埠。
- **Virtual System**（虛擬系統）— 轉送偵測到未知檔案的虛擬系統。
- **Application**（應用程式）— 轉送傳輸未知檔案的使用者應用程式。
- **User**（使用者）— 轉送目標使用者。
- **URL**— 轉送與未知檔案相關的 URL。
- **Filename**（檔案名稱）— 轉送未知檔案的名稱。
- **Email sender**（電子郵件寄件者）— 轉送未知電子郵件連結的寄件者（該電子郵件寄件者的名字也會出現在 WildFire 日誌和報告中）。
- **Email recipient**（電子郵件收件者）— 轉送未知電子郵件連結的收件者（該電子郵件收件者的名字也會出現在 WildFire 日誌和報告中）。

- **Email subject**（電子郵件主旨）— 轉送未知電子郵件連結的主旨（該電子郵件主旨會出現在 WildFire 日誌和報告中）。

STEP 3 | 按一下 **OK**（確定）儲存您的變更。

分析環境

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

進階 WildFire 重新產生了各種分析環境（包括作業系統），以識別範例內的惡意行為。視乎樣本的特徵與功能而定，可能會使用多種分析環境來判斷檔案的性質。進階 WildFire 使用靜態分析與機器學習來初步判定已知範例的變體是否為惡意軟體。根據對提交內容的初步裁定，進階 WildFire 將傳送未知範例至分析環境，透過從動態分析擷取額外資訊與指標來更詳細地檢查檔案。若檔案已透過自訂或開放來源方法混淆，使用靜態分析前，進階 WildFire 雲端會在動態分析環境內壓縮並解密記憶體檔案。在動態分析過程中，進階 WildFire 會觀察檔案在用戶端系統執行時的行為，並尋找惡意活動的各種徵兆，例如變更瀏覽器安全性設定、將指令碼插入其他程序、修改作業系統資料夾的檔案，或範例嘗試存取惡意網域。此外，在進階 WildFire 雲端動態分析期間產生的 PCAP 會進行深度檢測並用於建立網路活動設定檔。網路流量設定檔可以偵測已知的惡意軟體和之前使用一對多 profile match 的未知惡意軟體。

進階 WildFire 會根據範例特性，使用下列方法分析檔案：

- **Static Analysis**（靜態分析）—透過在執行前分析樣本的特徵，偵測已知威脅。
- **Machine Learning**（機器學習）—透過將惡意軟體特性集與動態更新的分類系統進行對比，識別已知威脅的變體。
- **Dynamic Unpacking (WildFire Cloud analysis only)**（動態解壓縮（僅限 **WildFire** 雲端分析））—識別並解壓縮以自訂/開放來源方法加密的檔案，並準備進行靜態分析。
- **Dynamic Analysis**（動態分析）—自訂建立、防規避的虛擬環境，可在該環境中觸發之前未知的提交，以確定實際效果及行為。
- **Intelligent Run-time Memory Analysis (Advanced WildFire License | Advanced WildFire global cloud only — requires PAN-OS 10.0 and later on NGFWs)**（智慧執行階段記憶體分析（進階 **WildFire** 授權 **|** 僅限進階 **WildFire** 全球雲端 — 需要 **PAN-OS 10.0** 及更高版本的 **NGFW**））— 這是一個基於雲端的分析環境，會以進階偵測器分析使用多種規避技術的現代威脅。

進階 WildFire 會執行複製下列作業系統的分析環境：

- **Microsoft Windows XP 32** 位元（僅以 **WildFire** 私有雲端的選項受支援）
- **Microsoft Windows 7 64** 位元
- **Microsoft Windows 7 32** 位元（僅以 **WildFire** 私有雲端的選項受支援）
- **Microsoft Windows 10 64** 位元（僅以進階 **WildFire** 公共雲端和執行 **PAN-OS 10.0** 或更高版本的 **WildFire** 私有雲端的選項受支援）
- **Mac OS X**（僅限進階 **WildFire** 公共雲端）
- **Android**（僅限進階 **WildFire** 公共雲端）
- **Linux**（僅限進階 **WildFire** 公共雲端）

進階 WildFire 公共雲端還會使用多個版本的軟體來分析檔案，以準確識別針對特定版本的用戶端應用程式的惡意軟體。WildFire 私人雲端不支援多版本分析，也不分析多個版本中的應用程式特定檔案。

進階 WildFire 內嵌雲端分析

這可在何處使用？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權

進階 WildFire 雲端使用一系列以內嵌雲端 ML 為基礎的偵測引擎，藉此分析穿過您網路的 PE（可攜式執行檔）樣本，以即時偵測並防止未知惡意軟體。這可讓進階 WildFire 雲端服務偵測前所未見的惡意軟體（不具有現有 WildFire 特徵碼，或可透過本機進階 WildFire 內嵌雲端 ML 偵測器進行偵測）並將其封鎖以免感染用戶端。這些狀況包括先前從未被其他人發現且未被進階 WildFire 內嵌 ML 攔截的某些惡意軟體類型，這些惡意軟體可以不受干擾繼續執行，因為最近發現該檔案的次數不足，導致特徵碼逾時或達特徵碼資料庫上限，而沒有傳達給防火牆。新定義的惡意檔案將在後續碰到時遭防火牆封鎖，因為特徵碼已納入當前的特徵碼集，然而，這得在 WildFire 雲端分析惡意檔案之後才會發生。

進階 WildFire 內嵌雲端可以阻止檔案下載（並可能在您的網路中傳播），同時在雲端中分析這些可疑檔案是否存在惡意軟體，並進行即時資訊交換。與 WildFire 分析的其他惡意內容一樣，進階 WildFire 內嵌雲端偵測到的任何威脅都會產生威脅特徵碼，Palo Alto Networks 將透過特徵碼更新套件以向客戶提供該特徵碼，藉此為所有 Palo Alto Networks 客戶提前建立防禦。

進階 WildFire 內嵌雲端在防火牆上使用輕量級轉送機制，以將任何本機效能影響降至最低；為了瞭解威脅形勢的最新變化，雲端內嵌 ML 偵測模型將透過雲端流暢地新增或更新，而無需內容更新或功能發佈支援。

進階 WildFire 內嵌雲端分析之啟用與設定將透過 WildFire 分析設定檔進行，並且需要具有作用中進階 WildFire 授權的 PAN-OS 11.1 或更新版本。

進階 WildFire 內嵌 ML

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

防毒設定檔中的進階 WildFire 內嵌 ML 選項使防火牆資料平面能即時將機器學習套用至 PE（可攜式執行檔）、ELF（可執行連結格式）、MS Office 檔案、OOXML、Mach-O 以及 PowerShell 及 Shell 指令碼。這層防毒保護為基於進階 WildFire 的特徵碼提供了補充，進而將防護範圍覆蓋到尚不存在特徵碼的檔案。每個內嵌 ML 模型都透過評估檔案詳細資料（包括解碼器欄位和模式）來動態偵測指定類型的惡意檔案，以制訂高可能性的檔案分類。此保護擴展到威脅的當前未知變體及未來變體，這些威脅與 Palo Alto Networks 已確定為惡意的特徵相符。為了瞭解威脅形勢的最新變化，內嵌 ML 模型透過內容發佈而新增或更新。在能夠啟用進階 WildFire 內嵌 ML 前，您必須先擁有作用中的進階 WildFire 或標準WildFire 訂閱。

還可啟用基於內嵌 ML 的保護作為 URL 篩選設定的一部分，以即時偵測惡意 URL。

進階 *WildFire* 內嵌 *ML* 在 *VM-50* 或 *VM50L* 虛擬設備上不受支援。

裁定

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

當進階 WildFire 在 Palo Alto Networks 託管的進階 WildFire 公共雲端或本機託管的 WildFire 私人雲端分析之前未知的範例時，系統會產生裁定，將範例判別為惡意、不良（灰色軟體會造成干擾但非惡意）、網路釣魚或良性：

- 良性—樣本安全無虞，並未出現任何惡意行為。
- 灰色—樣本不並未構成直接安全威脅，但可能顯示其他干擾行為。灰色軟體通常包括廣告軟體、間諜軟體及瀏覽器協助程式物件 (BHO)。
- 網路釣魚—連結將使用使用者導向至網路釣魚網站，並構成安全威脅。被攻擊者偽裝成合法網站的網路釣魚網站用於竊取使用者資訊，特別是解鎖網路存取權的公司密碼。WildFire 設備不支援網路釣魚裁定，仍將這類連結歸類為惡意。
- 惡意—樣本為惡意且構成安全威脅。惡意軟體包含病毒、蠕蟲、木馬程式、遠端存取工具 (RAT)、Rootkit 和 Botnet。針對判別為惡意軟體的檔案，系統將產生並散佈特徵碼以防範未來威脅的攻擊。

不論全域（美國）或區域，每個進階 WildFire 雲端和 WildFire 私人雲端皆獨立於其他 WildFire 雲端選項來分析範例並產生 WildFire 裁定。除 WildFire 私人雲端裁定之外，裁定可在全球共享，讓進階 WildFire 使用者可存取威脅資料的全球資料庫。

您懷疑誤判或漏報的裁定可提交至 *Palo Alto Networks* 威脅團隊以進行額外分析。您還可手動變更已提交至 *WildFire* 設備的樣本裁定。

檔案分析

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

透過 WildFire 分析設定檔設定的 Palo Alto Networks 防火牆可以根據檔案類型（包括電子郵件連結）轉送範例進行進階 WildFire 分析。此外，防火牆可解碼編碼或壓縮最多四次的檔案（如 ZIP 格式的檔案）；如果解碼檔案符合進階 WildFire 分析設定檔條件，防火牆會轉送解碼檔案進行分析。

您也可以在防火牆上啟用進階 WildFire 分析功能，以提供內嵌防毒保護。防毒設定檔的進階 WildFire 內嵌 ML 選項使防火牆資料平面能即時對 PE 和 ELF 檔案以及 PowerShell 指令碼套用機器學習分析。每個內嵌 ML 模型都透過評估檔案詳細資料（包括解碼器欄位和模式）來動態偵測指定類型的惡意檔案，以制訂高可能性的檔案分類。此保護擴展到威脅的當前未知變體及未來變體，這

些威脅與 Palo Alto Networks 已確定為惡意的特徵相符。為了瞭解威脅形勢的最新變化，內嵌 ML 模型透過內容發佈而新增或更新。如需詳細資訊，請參閱 進階 WildFire 內嵌 ML。

進階 WildFire 雲端也能分析用作次要承載，為多階段 PE、APK 及 ELF 惡意軟體套件部分的一些檔案類型。分析次要承載可提供額外覆蓋範圍，以中斷進階威脅所精心策劃的攻擊。這些進階威脅藉由執行程式碼來啟動額外惡意承載，包括經設計以輔助規避安全性措施以及促進主要承載擴散。進階 WildFire 會在靜態或動態分析環境中處理多階段威脅，藉此進行分析。在分析期間會獨立處理多階段惡意軟體所參考的檔案；因此，只要完成每個檔案分析，即可實現裁定及保護。多階段檔案的整體裁定係基於在所有經分析攻擊階段中發現的惡意內容威脅評估而判定。分析多階段檔案期間所發現的惡意內容會立即標記為惡意。

擁有惡意內容安全處理程序的組織可以透過 API 或 WildFire 入口網站，以 RAR 格式手動提交受密碼保護的樣本。若進階 WildFire 雲端接收的範例已使用密碼 *infected* 或 *virus* 進行加密，則進階 WildFire 雲端會解密並分析封存檔案。您可以按照接收檔案（此範例為封存檔）的格式檢視檔案的裁定及分析結果。

雖然防火牆可轉送下列所有檔案類型，但進階 WildFire 分析支援會根據您提交範例的進階 WildFire 雲端而有所不同。如需更多詳細資訊，請參閱進階 WildFire 檔案類型支援。

支援 **WildFire** 轉送的檔案類型	說明
`apk`	Android 應用程式套件 (APK) 檔案。 包含在 *APK* 檔案內的 *DEX* 檔案被分析視為 *APK* 檔案分析的一部分。
`flash`	網頁中內嵌的 Adobe Flash applet 和 Flash 內容。
`jar`	Java Applet（JAR/Class 檔案類型）。
`ms-office`	Microsoft Office 使用的檔案，包括文件（DOC、DOCX、RTF）、活頁簿（XLS、XLSX）、PowerPoint（PPT、PPTX）簡報及 Office Open XML (OOXML) 2007+ 文件。內容版本 8462 支援網際網路查詢 (IQY) 和符號連結 (SLK) 檔案。
`pe`	可攜式執行檔 (PE) 檔案。PE 包括可執行檔檔案、物件碼、DLL、FON（字型）及 LNK 檔案。內容版本 8462 支援 MSI 檔案。不需要使用授權即可轉送 PE 檔案進行 WildFire 分析，但需要使用授權才可分析其他所有支援的檔案類型。
`pdf`	可攜式文件格式 (PDF) 檔案。
`MacOSX`	macOS 平台使用的各種檔案類型。DMG、PKG 和 ZBundle 檔案的靜態分析僅在 Advanced WildFire Global（美國）

支援 **WildFire** 轉送的檔案類型	說明
	和歐洲雲端區域中可用，然而，所有區域雲端都支援其他 Mac OS X 檔案（fat 和 macho）的靜態分析。僅 Advanced WildFire Global（美國）和歐洲雲端區域支援針對所有 MacOSX 檔案進行動態分析。如需詳細資訊，請參閱文件類型支援。
電子郵件-連結	SMTP 和 POP3 電子郵件訊息包含的 HTTP/HTTPS 連結。參閱電子郵件連結分析。
`archive`	Roshal Archive (RAR) 和 7-Zip (7z) 歸檔檔案。如果多磁碟區封存檔分割成若干個小檔案，則無法提交進行分析。 進階 WildFire 雲端僅解密及分析使用密碼 *infected* 或 *virus* 加密的 RAR 檔案。 雖然防火牆能夠在解碼之後轉送 *ZIP* 封存檔中包含的支援檔案，但無法以編碼狀態轉送完整的 *ZIP* 檔案。如果想要提交完整的 *ZIP* 檔案，您可以使用 *WildFire* 入口網站或透過 *WildFire API* 手動上傳 *ZIP* 檔案。
`linux`	可執行和可連結格式 (ELF) 檔案。
指令碼	各種指令碼檔案。 • 內容版本 8101 支援 Jscript (JS)、VBScript (VBS) 和 PowerShell 指令碼 (PS1)。 • 內容版本 8168 支援批次 (BAT) 檔案。 • 內容版本 8229 支援 HTML 應用程式 (HTA) 檔案。

電子郵件連結分析

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

我可以在哪裡使用這個？	我需要哪些內容？
• CN-Series	

Palo Alto Networks 防火牆可擷取 SMTP 及 POP3 電子郵件訊息中所載的 HTTP/HTTPS 連結，並將連結轉送至 WildFire 進行分析。防火牆只會從電子郵件訊息中擷取連結和相關的工作階段資訊（寄件者、收件者和主旨），它不會接收、儲存、轉送或檢視電子郵件訊息。

WildFire 會造訪提交的連結來判斷是否有對應的網頁主導任何入侵行為或顯示網路釣魚活動。WildFire 認定為惡意或網路釣魚的連結是：

- 作為 WildFire 提交日誌項目記錄在防火牆上。詳細記錄該連結行為和活動的 WildFire 分析報告適用於每個 WildFire 提交日誌項目。日誌項目還包含電子郵件標頭資訊—電子郵件寄件者、收件者及主旨—以便您識別訊息並將它從郵件伺服器上刪除，或在已傳送電子郵件或開啟的情況下移轉威脅。
- 新增至 PAN-DB 並且 URL 被分類為惡意軟體。

防火牆會以每批 100 個電子郵件連結轉送或每 2 分鐘轉送電子郵件連結一次（取決於達到限制的順序）。WildFire 的每批上傳視為特定防火牆每分鐘上傳容量中的一次上傳 依型號的防火牆檔案轉送容量。如果電子郵件中包含的連結對應檔案下載而非 URL，則當啟用對應檔案類型進行 WildFire 分析時，防火牆將轉送檔案。

若要讓防火牆轉送電子郵件中包含的連結進行 WildFire 分析，請參閱 轉送檔案進行進階 WildFire 分析。藉助進階 URL 篩選授權，您也可防止使用者存取惡意和釣魚網站。

URL 分析

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

進階 WildFire 全域雲端（美國）和地區雲端可分析 URL 以及電子郵件連結，以透過 WildFire API 提供標準化的裁定與報告。透過彙總來自所有 Palo Alto Networks 服務（包括 PAN-DB）的威脅分析詳細資料，進階 WildFire 能夠產生更準確的裁定，並提供一致的 URL 分析資料。

在進階 WildFire 全域雲端執行的 URL 分析器會處理 URL 摘要、相關的 URL 來源（例如電子郵件連結）、NRD（新註冊的網域）清單、PAN-DB 內容和手動上傳的 URL，為所有進階 WildFire 雲端提供改良功能，而不影響 GDPR 合規性。處理完 URL 後，您可以擷取 URL 分析報告，其中

包括裁定、附有證據的偵測原因、螢幕截圖以及針對網路請求產生的分析資料。您還可以擷取在 URL 分析期間看到的網頁構件（下載的檔案與螢幕擷取畫面），以進一步調查異常活動。

此功能無需額外設定，不過，若您想自動提交電子郵件連結以進行分析（現已透過此服務進行分析），您必須 轉送檔案進行進階 WildFire 分析。

您懷疑為誤判或漏報的裁定可提交至 Palo Alto Networks 威脅團隊以進行額外分析。

壓縮和編碼檔案分析

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

預設情況下，防火牆解碼編碼或最多壓縮四次的檔案，包括使用 ZIP 格式壓縮的檔案。之後，防火牆檢查並在解碼檔案上執行原則；如果檔案未知，防火牆會轉送解碼檔案進行 WildFire 分析。雖然防火牆無法轉送完整的 ZIP 封存檔案以進行進階 WildFire 分析，但您可以使用 WildFire 入口網站或 WildFire API 將檔案直接提交到進階 WildFire 公共雲端。

防火牆不會對 *RAR* 和 *7-Zip* 歸檔檔案進行解碼。對這些檔案進行的所有處理均發生在進階 *WildFire* 公共雲端中。

進階 WildFire 特徵碼

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

進階 WildFire 能夠找出網路流量 (HTTP/HTTPS)、電子郵件通訊協定（SMTP、IMAP 和 POP）和 FTP 流量中的零時差惡意軟體，並快速產生特徵碼，以針對所有偵測到的惡意軟體進行識別和防範後續感染。進階 WildFire 將根據範例的惡意軟體裝載自動產生特徵碼，並測試特徵碼的準確性與安全性。

每個進階 WildFire 雲端都會獨立於其他進階 WildFire 雲端來分析範例並產生惡意軟體特徵碼。除 WildFire 私人雲端特徵碼之外，進階 WildFire 特徵碼可在全球共享，讓全球使用者受益於惡意軟體涵蓋範圍資訊，無論惡意軟體最先偵測到的位置在哪裡都可以。由於惡意軟體進化速度相當快，進階 WildFire 產生的特徵碼也會因應惡意軟體的眾多變體。

具作用中進階 WildFire 授權的防火牆可在最新的進階 WildFire 特徵碼可用時對其進行即時擷取。若您沒有進階 WildFire 訂閱，做為防毒更新的其一步驟，24 到 48 小時內系統將針對具主動威脅防範使用授權的防火牆提供特徵碼。

在防火牆下載並安裝新的特徵碼後，防火牆將封鎖任何包含該惡意軟體（或其變體）的檔案。惡意軟體特徵碼不會偵測惡意和網路釣魚連結；若要執行這些連結，您必須具有 PAN-DB URL 篩選授權。然後您可阻止使用者存取惡意和釣魚網站。

進階 WildFire 部署

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

您可以設定 Palo Alto Networks 防火牆提交未知的範例至一個 Palo Alto Networks 託管的進階 WildFire 公共雲端、美國政府雲端、本機託管的 WildFire 私人雲端，或者您可以啟用防火牆將特定範例轉送至一個進階 WildFire 公共雲端選項，另將特定範例轉送至 WildFire 私人雲端：

- 進階 WildFire 公共雲端
- WildFire 私人雲端
- WildFire 混合型雲端
- WildFire：美國政府雲端

進階 WildFire 公共雲端

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

Palo Alto Networks 防火牆可以轉送未知檔案和電子郵件連結至進階 WildFire 全域雲端（美國）或 Palo Alto Networks 擁有並維護的進階 WildFire 區域雲端。選擇進階 WildFire 公共雲端，根據您的位置和組織需要向其提交範例進行分析：

- 進階 **WildFire** 全域雲端（美國）

  進階 WildFire 全域雲端（美國）是一個在美國託管的公共雲端環境。

  請使用下列 URL 提交檔案至進階 WildFire 全域雲端（美國）進行分析並存取進階 WildFire 全域雲端（美國）入口網站：wildfire.paloaltonetworks.com。

- 進階 **WildFire** 歐洲雲端

  WildFire 歐洲雲端是一個在荷蘭託管的區域公共雲端環境。它被設計為遵守歐盟 (EU) 資料隱私權法規，且提交至 WildFire 歐洲雲端的樣本應留在 EU 境內。

  使用下列 URL 提交檔案至 WildFire 歐洲雲端進行分析並存取進階 WildFire 歐洲入口網站：eu.wildfire.paloaltonetworks.com。

- 進階 **WildFire** 日本雲端

  進階 WildFire 日本雲端是一個在日本託管的區域公共雲端環境。

  使用下列 URL 提交檔案至進階 WildFire 日本雲端進行分析並存取進階 WildFire 日本入口網站：jp.wildfire.paloaltonetworks.com。

- 進階 **WildFire** 新加坡雲端

  進階 WildFire 新加坡雲端是一個在新加坡託管的區域公共雲端環境。

  使用下列 URL 提交檔案至進階 WildFire 新加坡雲端進行分析並存取進階 WildFire 新加坡入口網站：sg.wildfire.paloaltonetworks.com。

- 進階 **WildFire** 英國雲端

  進階 WildFire 英國雲端是一個在英國託管的區域公共雲端環境。

  使用下列 URL 提交檔案至進階 WildFire 英國雲端進行分析並存取進階 WildFire 英國雲端入口網站：uk.wildfire.paloaltonetworks.com。

- 進階 **WildFire** 加拿大雲端

  WildFire 加拿大雲端是一個在加拿大託管的區域公共雲端環境。

  使用下列 URL 提交檔案至進階 WildFire 加拿大雲端進行分析並存取進階 WildFire 加拿大雲端入口網站：ca.wildfire.paloaltonetworks.com。

- 進階 **WildFire** 澳洲雲端

  WildFire 澳洲雲端是一個在加拿大託管的區域公共雲端環境。

  使用下列 URL 提交檔案至進階 WildFire 澳洲雲端進行分析並存取進階 WildFire 澳洲雲端入口網站：au.wildfire.paloaltonetworks.com。

- 進階 **WildFire** 德國雲端

  進階 WildFire 德國雲端是一個在德國託管的區域公共雲端環境。

  使用下列 URL 提交檔案至進階 WildFire 德國雲端進行分析並存取進階 WildFire 德國雲端入口網站：de.wildfire.paloaltonetworks.com。

- 進階 **WildFire** 印度雲端

  進階 WildFire 印度雲端是一個在印度託管的區域公共雲端環境。

  使用下列 URL 提交檔案至進階 WildFire 印度雲端進行分析並存取進階 WildFire 印度雲端入口網站：au.wildfire.paloaltonetworks.com。

- 進階 **WildFire** 瑞士雲端

  進階 WildFire 瑞士雲端是一個在瑞士託管的區域公共雲端環境。

  使用下列 URL 提交檔案至進階 WildFire 瑞士雲端進行分析並存取進階 WildFire 瑞士雲端入口網站：ch.wildfire.paloaltonetworks.com。

- 進階 **WildFire** 波蘭雲端

  進階 WildFire 波蘭雲端是一個在波蘭託管的區域公共雲端環境。

  使用下列 URL 提交檔案至進階 WildFire 波蘭雲端進行分析並存取進階 WildFire 波蘭雲端入口網站：pl.wildfire.paloaltonetworks.com。

- 進階 **WildFire** 印尼雲端

  進階 WildFire 印尼雲端是一個在印尼託管的區域公共雲端環境。

  使用下列 URL 提交檔案至進階 WildFire 印尼雲端進行分析並存取進階 WildFire 印尼雲端入口網站：id.wildfire.paloaltonetworks.com。

- 進階 **WildFire** 台灣雲端

  進階 WildFire 台灣雲端是一個在台灣託管的區域公共雲端環境。

  使用下列 URL 提交檔案至進階 WildFire 台灣雲端進行分析並存取進階 WildFire 台灣雲端入口網站：tw.wildfire.paloaltonetworks.com。

- 進階 **WildFire** 法國雲端

  進階 WildFire 法國雲端是一個在法國託管的區域公共雲端環境。

  使用下列 URL 提交檔案至進階 WildFire 法國雲端進行分析並存取進階 WildFire 法國雲端入口網站：fr.wildfire.paloaltonetworks.com。

- 進階 **WildFire** 卡達雲端

  進階 WildFire 卡達雲端是一個在卡達託管的區域公共雲端環境。

  使用下列 URL 提交檔案至進階 WildFire 卡達雲端進行分析並存取進階 WildFire 卡達雲端入口網站：qatar.wildfire.paloaltonetworks.com。

- 進階 **WildFire** 韓國雲端

  Advanced WildFire 韓國雲端是一個在韓國託管的區域公共雲端環境。

  使用下列 URL 提交檔案至進階 WildFire 韓國雲端進行分析並存取進階 WildFire 韓國雲端入口網站：kr.wildfire.paloaltonetworks.com。

- 進階 **WildFire** 以色列雲端

  進階 WildFire 以色列雲端是一個在以色列託管的區域公共雲端環境。

  使用下列 URL 提交檔案至進階 WildFire 以色列雲端進行分析並存取進階 WildFire 以色列雲端入口網站：il.wildfire.paloaltonetworks.com。

- 進階 **WildFire** 沙烏地阿拉伯雲端

  Advanced WildFire 沙烏地阿拉伯雲端是一個在沙烏地阿拉伯託管的區域公共雲端環境。

  使用下列 URL 提交檔案至進階 WildFire 沙烏地阿拉伯雲端進行分析並存取進階 WildFire 沙烏地阿拉伯雲端入口網站：sa.wildfire.paloaltonetworks.com。

- 進階 **WildFire** 西班牙雲端

  進階 WildFire 西班牙雲端是一個在西班牙託管的區域公共雲端環境。

  使用下列 URL 提交檔案至進階 WildFire 西班牙雲端進行分析並存取進階 WildFire 西班牙入口網站：es.wildfire.paloaltonetworks.com。

每個進階 WildFire 雲端不論全域（美國）或區域，皆會獨立於其他 WildFire 雲端來分析範例並產生惡意軟體特徵碼和裁定。然後進階 WildFire 特徵碼和裁定可在全球共享，讓全球 WildFire 使用者受益於惡意軟體涵蓋範圍資訊，而無論惡意軟體最先偵測到的位置在哪裡都可以。請參閱進階 WildFire 檔案類型支援，深入瞭解每個雲端分析的檔案類型。

如果您有 WildFire 設備，您可以啟用 WildFire 混合型雲端部署，以便防火牆轉送某些檔案至 WildFire 公共雲端，並轉送其他檔案至 WildFire 私人雲端進行本機分析。還可以設定 WildFire 設備以透過在執行分析前查詢公共雲端來快速收集已知樣本的裁定。這使 WildFire 設備可以向私人網路和全球 WildFire 社群均未知的樣本分配分析資源。

WildFire 私人雲端

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 或 WildFire 授權

在 Palo Alto Networks 私人雲端部署中，Palo Alto Networks 防火牆將檔案轉送至用於託管私人雲端分析位置的公司網路上的 WildFire 設備。

如需詳細瞭解混合型雲端轉送，請參閱 WildFire 設備管理員指南。

WildFire 混合型雲端

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 或 WildFire 授權

在 WildFire 混合型雲端部署中，防火牆可將某些樣本轉送至 Palo Alto Networks 託管的一個 WildFire 公共雲端，以及將其他樣本轉送至由 WildFire 設備託管的 WildFire 私人雲端。

如需詳細瞭解混合型雲端轉送，請參閱 WildFire 設備管理員指南。

WildFire FedRAMP 授權雲端平台

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。 ❑ 進階 WildFire FedRAMP 附加元件

除了 WildFire 全域雲端、 私人雲端和 混合雲端部署選項之外，Palo Alto Networks 還為需要遵守安全雲端操作標準的組織提供數個高安全性、FedRAMP 授權的雲端環境存取權。FedRAMP 授權的雲端有兩個影響等級可用：高階和中階，中階均可在兩種雲端設定中使用。進階 WildFire 政府雲端符合 FedRAMP 高階認證標準，而進階 WildFire 政府雲端和 WildFire 美國政府雲端均符合 FedRAMP 中階認證標準。

WildFire 美國政府雲端（符合 *FedRAMP* 中階認證標準）已準備終止服務。對於所有新客戶，*Palo Alto Networks* 建議使用進階 *WildFire* 公共部門雲端，該雲端具有增強的功能集並支援進階 *WildFire* 雲端。

FedRAMP 中階雲端（進階 WildFire 政府雲端和 WildFire 美國政府雲端）通常可供 Palo Alto Networks 客戶使用，然而，符合 FedRAMP 高階認證標準的進階 WildFire 政府雲端僅可供聯邦政府、國防部或經核准的國防工業基地 (DIB) 客戶使用。

由於這些服務的敏感性，FedRAMP 雲端具有與其他服務不同的特定客戶引導流程。如需更多資訊，請參閱特定的 FedRAMP 雲端類型：

- 進階 WildFire 政府雲端
- 進階 WildFire 公共部門雲端
- WildFire：美國政府雲端

上方列出的 FedRAMP 雲端無法在同一裝置上混合搭配，也不能與進階 WildFire 全域或區域雲端同時使用。然而，任何 FedRAMP 雲端都可以與其他以雲端為基礎的安全服務（例如進階威脅防護、DLP 等）搭配使用。如果您需要在單一裝置上整合多個 FedRAMP 安全層級，則必須使用單獨的帳戶 ID。客戶引導完成後，您可以依循與任何其他進階 WildFire 雲端相同的方式，在防毒安全設定檔和 API 中引用 FedRAMP 雲端 URL。

進階 **WildFire** 政府雲端

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。 ❑ 進階 WildFire 政府雲端附加元件

Palo Alto Networks 為聯邦政府、國防部或經核准的國防工業基地 (DIB) 客戶提供進階 WildFire 政府雲端，這是一個符合 FedRAMP（聯邦政府風險與授權管理計畫）高階認證標準的高安全性惡意軟體分析平台。

進階 WildFire 公共部門雲端作為獨立且有別於商業或政府雲端區域的實體運作 - 任何傳送用於分析的樣本中，可能存在的任何隱私資訊（例如電子郵件地址、IP 位址和被動 DNS）都不會與任何其他 WildFire 雲端執行個體共用。然而，其仍然能夠利用進階 WildFire 公共雲端所產生的威脅資料，以發揮最大涵蓋能力，以及保護透過檔案分析所產生的特徵碼及防毒。

若需有關 *Palo Alto Networks* 進階 *WildFire FedRAMP* 授權的詳細資訊，請造訪：FedRAMP.gov

若需有關 Palo Alto Network 之 WildFire FedRAMP 授權的詳細資計，請造訪：Palo Alto Networks Government Cloud Services - WildFire

進階 WildFire 政府雲端與標準商業進階 WildFire 公共雲端有數個功能差異。連線至進階 WildFire 政府雲端的客戶無法使用下列功能：

- 進階 WildFire 美國政府雲端區域不支援裸機分析
- 進階 WildFire 政府雲端無法透過 WildFire 入口網站存取。
- 如果沒有服務要求，則不提供刪除功能的權利。

開始使用進階 **WilFire** 政府雲端

請遵循任何內部程序措施，以判斷您的網路否適合使用進階 WildFire 美國政府雲端，例如但不限於進行風險分析、評估 CSP 提交套件，以及授權核准。請聯絡您的 Palo Alto Networks 業務代表 / 進階 WildFire:美國政府雲端聯絡窗口，以討論任何其他的操作詳細資訊。

存取及進階 WildFire 美國政府雲端前，請先確定您符合操作 FedRAMP 授權服務的適當組織要求。

聯絡 Palo Alto Networks 客戶團隊以開始就任流程。完成進階 WildFire 啟用後，請重新設定防火牆以使用 gov-cloud.wildfire.paloaltonetworks.com 轉送未知檔案及電子郵件連結以供分析。如需詳細資訊，請參閱「轉送檔案供 WildFire 分析」。如果需要其他協助，請聯絡 Palo Alto Networks 客戶支援。

進階 **WildFire** 公共部門雲端

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。 ❑ 進階 WildFire 公共部門附加元件

Palo Alto Networks 為客戶提供進階 WildFire 公共部門雲端，這是一個符合 FedRAMP（聯邦政府風險與授權管理計畫）中階認證標準的高安全性惡意軟體分析平台。進階 WildFire 公共部門雲端將取代 WildFire 美國政府雲端。

進階 WildFire 公共部門雲端作為獨立且有別於商業或政府雲端區域的實體運作 - 任何傳送用於分析的樣本中，可能存在的任何隱私資訊（例如電子郵件地址、IP 位址和被動 DNS）都不會與任何其他 WildFire 雲端執行個體共用。然而，其仍然能夠利用進階 WildFire 公共雲端所產生的威脅資料，以發揮最大涵蓋能力，以及保護透過檔案分析所產生的特徵碼及防毒。

若需有關 *Palo Alto Networks* 進階 *WildFire FedRAMP* 授權的詳細資訊，請造訪：FedRAMP.gov

進階 WildFire 公共部門雲端與標準商業進階 WildFire 公共雲端有少數功能差異。連線至進階 WildFire 公共部門雲端的客戶無法使用下列功能：

- 進階 WildFire 美國政府雲端區域不支援裸機分析
- 進階 WildFire 美國公共部門雲端無法透過 WildFire 入口網站存取。
- 如果沒有服務要求，則不提供刪除功能的權利。

開始使用進階 **WilFire** 公共部門雲端

請遵循任何內部程序措施，以判斷您的網路否適合使用進階 WildFire 公共部門雲端，例如但不限於進行風險分析、評估 CSP 提交套件，以及授權核准。請聯絡您的 Palo Alto Networks 業務代表 / 進階 WildFire:美國公共部門雲端聯絡窗口，以討論任何其他的操作詳細資訊。

存取進階 WildFire 公共部門雲端前，請先確定您符合操作 FedRAMP 授權服務的適當組織要求。

聯絡 Palo Alto Networks 客戶團隊以開始就任流程。完成進階 WildFire 啟用後，請重新設定防火牆以使用 pubsec-cloud.wildfire.paloaltonetworks.com 轉送未知檔案及電子郵件連結以供分析。

如需詳細資訊，請參閱「轉送檔案供 WildFire 分析」。如果需要其他協助，請聯絡 Palo Alto Networks 客戶支援。

WildFire：美國政府雲端

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。 ❑ WildFire U.S.政府客戶引導

截至 *2024* 年 *7* 月 *15* 日，*Palo Alto Networks WildFire* 美國政府雲端已被 進階 WildFire 政府雲端 和 進階 WildFire 公共部門雲端 取代，此兩項服務提供高安全性的進階 *WildFire* 雲端環境，用於操作較新且具有增強功能集的程式碼庫。因此，*Palo Alto Networks* 將不會再將新客戶引導至 *WildFire* 美國政府雲端。現有客戶可以繼續存取 *WildFire* 美國政府雲端直至 *2024* 年 *11* 月 *30* 日終止服務日期為止，此時現有的 *URI* 將重新導向至進階 *WildFire* 公共部門雲端。

如需有關新雲端產品的詳細資訊，請聯絡您的 *Palo Alto Networks* 業務代表聯絡窗口，以便討論任何其他操作詳細資訊。

經授權的 Palo Alto Networks WildFire 美國政府雲端是高度安全的惡意軟體分析平台 FedRAMP（聯邦風險及授權管理計畫，英文全名 Federal Risk and Authorization Management Program）。此 WildFire 雲端意欲僅供美國聯邦機構使用，要求標準化安全性評估、授權及持續監控雲端產品與服務的方法。WildFire：美國政府雲端作為另一且相異的實體運作，所傳送要進行分析的樣本中可能存在任何私人資料，例如，電子郵件地址、IP 位址及被動 DNS，這些私人資料不得與任何其他 WildFire 雲端實例共用。然後，仍然能夠利用 WildFire 公共雲端所產生的威脅資料，以發揮最大涵蓋能力，以及保護透過檔案分析所產生的特徵碼及防毒。

若需有關 Palo Alto Network 之 WildFire FedRAMP 授權的詳細資計，請造訪：Palo Alto Networks Government Cloud Services - WildFire

WildFire 公共雲端（全域及區域雲端）及 WildFire 美國政府雲端有數項功能不同於公共雲端。連線至 WildFire 的客戶不可使用下列功能：美國政府雲端：

- 美國政府雲端不支援Government Cloud（WildFire 美國政府雲端）。
- 目前不支援指令碼檔案（Bat、JS、BVS、PS1、Shell 指令碼及 HTA）分析。
- WildFire：美國政府雲端無法透過 WildFire 入口網站存取。
- WildFire：美國政府雲端無法與其他雲端式服務整合。
- 不提供刪除功能的權利。
- WildFire：美國政府雲端目前不支援進階 WildFire 分析。

開始使用 **WildFire**：美國政府雲端

為了連線至 WildFire：美國政府雲端，您必須申請存取權。請遵循任何內部程序措施，以判定在您的網路內使用 WildFire:美國政府雲端的合適性，例如但不限於進行風險分析、評估 CSP 提交套件，以及授權核准。請聯絡您的 Palo Alto Networks 業務代表 / WildFire:美國政府雲端聯絡窗口，以討論任何其他的操作詳細資訊。

申請存取 WildFire 美國政府雲端前，請先確定您符合操作 FedRAMP 授權服務的適當組織要求。有兩種實體類別可存取 WildFire 美國政府雲端：美國政府承包商及美國聯邦機構（以及其他獲核准的政府部門）。這兩類實體皆須符合特定要求才能存取 WildFire 美國政府雲端：

1. 美國聯邦機構

   美國聯邦機構、部門及局處皆必須收到指定許可機構（Designated Approving Authority，DAA）核發的操作授權證明（Authority to Operate，ATO），在授予存取權之前，由指定許可機構授權操作在機構維運內的 WildFire 美國政府雲端。

   1. 向 the Palo Alto Networks 聯絡窗口 (fedramp@paloaltonetworks.com) 通知意欲使用 WildFire 美國政府雲端。
   2. 傳送申請至 info@fedramp.gov。
   3. 填寫 FedRAMP 套件存取申請表單並且提交填妥的表單至 info@fedramp.gov。

      FedRAMP Program Management Office (PMO) 審查表單，並通常會暫時核發 *30* 天存取 *WildFire FedRAMP* 套件的權限。
   4. 檢閱 FedRAMP 安全性套件，適用於 WildFire 美國政府雲端。完成必要的內部流程以部署 WildFire 美國政府雲端至您的組織。
   5. 簽發 ATO。
   6. 傳送申請至 FedRAMP PMO，以取得 WildFire 美國政府雲端的永久存取權。

2. 美國政府承包商

   美國政府承包商如使用或存取 Wildfire 美國政府雲端，則必須符合下列要求。

   1. 必須是美國公民。
   2. 持有與美國聯邦政府機構的有效合約（或轉包），並且職業確實需要使用網際網路進行資訊交換，例如電子郵件通信、共用文件及其他形式的網際網路通訊。
   3. 承包商聘雇終止後，使用者必須停止使用或存取 WildFire 美國政府雲端。
   4. 遵守 Palo Alto Networks EULA 內含的保密條款。

您的組織發佈操作授權證明 (ATO) 或適用的美國政府承包商符合所有使用規定後時，才可聯絡 Palo Alto Networks 客戶團隊，申請存取 WildFire 美國政府雲端。

1. 請聯絡您的 FedRAMP Program Management Office (PMO) 以判定依據您的安全性需求使用美國政府雲端的可行性。
2. 聯絡 FedRAMP Marketplace 中指定的 Palo Alto Networks 聯絡窗口。聯絡窗口會提供其他關於服務的資訊，以及關於您專屬 WildFire 部署的任何其他操作詳細資訊。
3. 聯絡 Palo Alto Networks 客戶團隊以開始就任流程。客戶團隊會要求下列關於客戶詳細資料的訊及部署詳細規格。
   - 聯絡資訊。
   - 移轉至 WildFire 美國政府雲端的簡短說明Government Cloud（WildFire 美國政府雲端）。
   - 聲明組織遵守 Palo Alto Networks EULA 內載列的保密條款。
   - 所有防火牆閘道（包括管理平面）以及所有 Panorama 實例的外送 IP 位址。
4. WildFire Program Management 核准使用 WildFire 美國政府雲端（通常一至三天營業日）後，Palo Alto Networks Development Operations 會套用適當的控制。
5. 授予 WildFire 美國政府雲端的存取權後，請重新設定防火牆以使用 wildfire.gov.paloaltonetworks.com 轉送未知檔案及電子郵件連結以供分析。如需詳細資訊，請參閱「轉送檔案供 WildFire 分析」。如果需要其他協助，請聯絡 Palo Alto Networks 客戶支援。

文件類型支援

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

下表列出了 WildFire 雲端環境中支援進行分析的檔案類型。

如需 *WildFire* 所支援特定檔案類型的完整列表，請參閱 支援的檔案類型（完整列表）。

支援進行分析的檔案類型	進階 **WildFire** 公共雲端（所有區域）	**WildFire U.S.**政府雲端	進階 **WildFire** 入口網站	**API**（直接上傳；所有區域）
電子郵件包含的連結	✓	✓	✓
Android 應用程式套件 (APK) 檔案	✓	✓	✓
Adobe Flash 檔案	✓	✓	✓
Java 歸檔 (JAR) 檔案	✓	✓	✓
Microsoft Office 檔案（包括 SLK 和 IQY 檔案）	✓	✓	✓
可攜可執行檔（包括 MSI 檔案）	✓	✓	✓

支援進行分析的檔案類型	進階 **WildFire** 公共雲端（所有區域）	**WildFire U.S.**政府雲端	進階 **WildFire** 入口網站	**API**（直接上傳；所有區域）
可攜式文件格式 (PDF) 檔案	✓	✓	✓	
Mac OS X* 檔案	✓	✓	✓	
Linux（ELF 檔案和 Shell 指令碼）檔案	✓	✓	✓	
封存檔（RAR、7-Zip 和 ZIP**）檔案	✓	✓	✓	
指令碼（BAT、JS、VBS、PS1 和 HTA）檔案	✓	✗	✓	
Python 指令碼	✓	✓	✓	
Perl 指令碼	✗	✗	✓	
封存檔（ZIP [直接上傳] 和 ISO）檔案	✗	✗	✓	
圖片（JPG 和 PNG）檔案	✗	✗	✓	

* DMG、PKG 和 ZBundle 檔案的靜態分析僅在 Advanced WildFire Global（美國）和歐洲雲端區域中可用，然而，所有區域雲端都支援其他 Mac OS X 檔案（fat 和 macho）的靜態分析。僅 Advanced WildFire Global（美國）和歐洲雲端區域支援針對所有 Mac OS X 檔案進行動態分析。

** ZIP 檔案不會直接轉送到進階 Wildfire 雲端進行分析。而是首先由防火牆解碼，與 WildFire 分析設定檔條件相符的檔案將單獨轉送以進行分析。

想知道更多？

- 如需每一進階 *WildFire* 雲端部署的詳細資訊，請參閱 進階 WildFire 部署。
- 如需有關支援進行 *WildFire* 分析的每個檔案類型的詳細資訊，請參閱檔案分析。

支援的檔案類型（完整列表）

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

下表列出 WildFire 分析所支援的檔案類型。對於在「轉送支援」欄中標記為「是」的文件，這包括在網頁流量 (HTTP/HTTPS) 和電子郵件協定 (SMTP、IMAP、POP) 中已採用 MIME 編碼的檔案。

受支援的內容類型	擴充範例	轉送支援
7zip 封存檔	7z	是
Adobe Flash 文件	swf	是
Android APK	apk	是
Android DEX	dex	是
批次	批次	是
bzip2 封存檔	bz	是
逗號分隔值	csv	否。
DLL、DLL64	dll	是
ELF	elf	是
Gzip 封存檔	gz	否。
HTML 應用程式	hta	是
ISO	iso	否。

受支援的內容類型	擴充範例	轉送支援
JAVA 類別	class	是
JAVA JAR	jar	是
Javascript/JScript	js、jse、wsf	是（僅限 JS）
聯合攝影專家團隊	jpg	否。
連結	elink	是
Mach-O	macho	是
macOS 應用程式安裝程式	pkg	是
ZIP 封存檔中的 macOS 應用程式套件	zbundle	否。
macOS 通用二進位檔案	fat	否。
macOS 磁碟映像	dmg	是
Microsoft Excel 97 - 2003 文件	xls	是
Microsoft Excel 文件	xlsx	是
Microsoft One Note 文件	one	是
Microsoft PowerPoint 97 - 2003 文件	ppt	是
Microsoft PowerPoint 文件	pptx	是
Microsoft 符號連結檔案	slk	是
Microsoft 網頁查詢檔案	iqy	是
Microsoft Word 97 - 2003 文件	doc	是
Microsoft Word 文件	docx	是
OpenDocument 試算表文件	ods	否。

受支援的內容類型	擴充範例	轉送支援
OpenDocument 文字文件	odt	否。
PDF	pdf	是
PE、PE64	exe	是
Perl 指令碼	pl	否。
可攜式網路圖形檔案	png	否。
PowerShell	ps1	是
Python 指令碼	py	是
RAR 封存檔	rar	是
RTF	rtf	是
Shell 指令碼	sh	是
Tar 封存檔	tar	否。
VBScript	vbs、vbe	是（僅限 VBS）
Windows 安裝程式套件	msi	是
Windows 連結檔案	lnk	是
Windows 指令碼	wsf	否。
Zip 封存檔	zip	否。
作用中的伺服器頁面	asp	否。
擴充作用中的伺服器頁面	aspx	否。
可擴充的標記語言	xml	否。
超文字標記語言	html	否。

進階 WildFire 範例

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

下列示範案例說明整個進階 WildFire™ 生命週期。在此範例中，Palo Alto Networks 的銷售代表下載由銷售合作夥伴上載到 Dropbox 的新軟體銷售工具。銷售合作夥伴在不知情的情況下上載受感染的銷售工具安裝檔案，然後銷售代表下載這個受感染的檔案。

此範例將說明 Palo Alto Networks 防火牆搭配進階 WildFire 如何在即使流量經過 SSL 加密的情況下，找出使用者下載的零時差惡意軟體。在進階 WildFire 判別惡意軟體後，日誌將傳送至防火牆，而防火牆會警示管理員，讓管理員聯絡使用者以清除惡意軟體。然後，進階 WildFire 會為惡意軟體產生新的特徵碼，之後防火牆會自動下載該特徵碼以防止將來暴露。雖然某些檔案共享網站有防毒功能可在上載檔案時檢查檔案，不過充其量只能防範已知的惡意軟體。

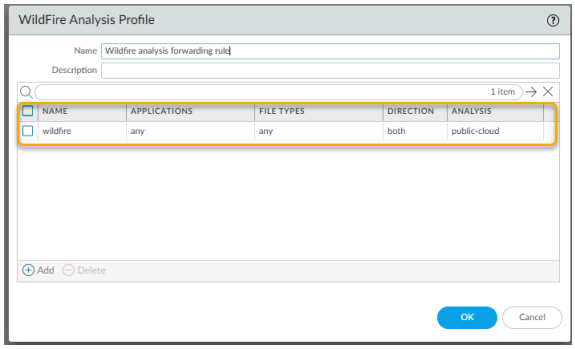
此範例以使用 *SSL* 加密的網站為例。在此情況下，防火牆啟用解密，包括轉送解密內容以供分析的選項。

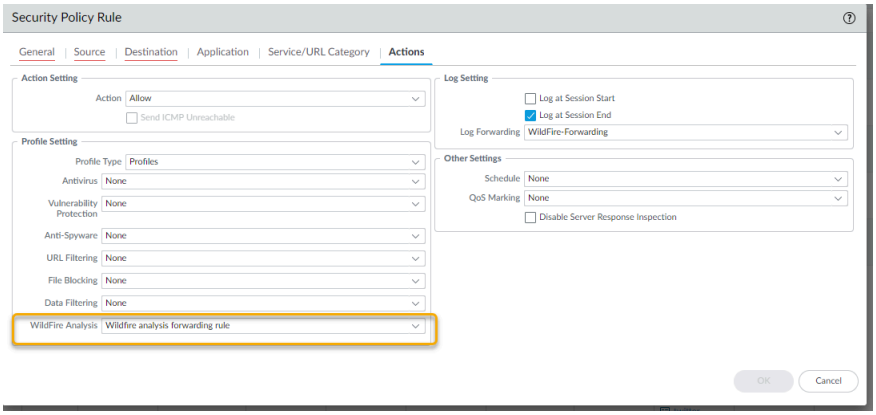
STEP 1 | 來自合作夥伴公司的銷售人員將名稱為 sales-tool.exe 的銷售工具檔案上載到自己的 Dropbox 帳戶，然後將有該檔案連結的電子郵件傳送給 Palo Alto Networks 銷售人員。

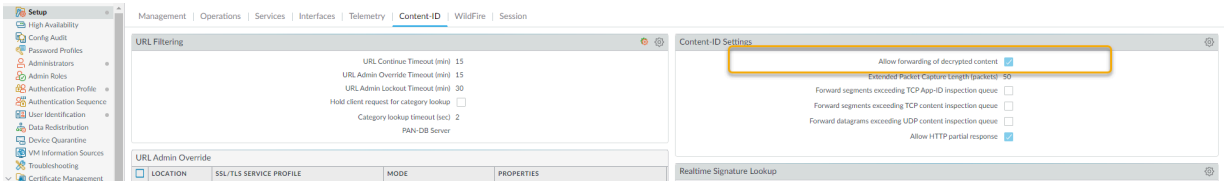
STEP 2 | Palo Alto Networks銷售人員收到銷售合作夥伴寄送的電子郵件後，按一下下載連結前往 Dropbox 網站，接著按一下 **Download**（下載），將檔案儲存到桌面。

STEP 3 | 保護 Palo Alto 銷售代表的防火牆有一個附加在安全性原則的 WildFire 分析設定檔規則，能夠搜尋任何用來下載或上載任何支援檔案類型的應用程式中存在的檔案。防火牆也可設定為轉送電子郵件連結類型檔案，這可讓防火牆擷取 SMTP 和 POP3 電子郵件訊息所包含的 HTTP/HTTPS 連結。一旦銷售代表按一下下載，防火牆便會將 sales-toole.exe 檔案轉送到進階 WildFire，在此會分析該檔案是否有零時差惡意軟體。雖然銷售代表使用 SSL 加密的 Dropbox，不過防火牆仍設定為將流量解密，因此所有流量都會受到檢查。下列螢幕擷取畫面

顯示 WildFire 分析設定檔規則、以附加的 WildFire 分析設定檔規則設定的安全性原則，以及允許啟用解密內容轉送的選項。

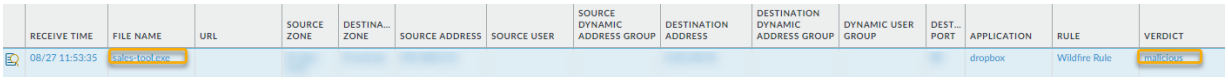






STEP 4 | 此時，進階 WildFire 已收到檔案，並且正在分析比對 200 多種不同的惡意行為。

STEP 5 | 進階 WildFire 完成檔案分析後，會將載明分析結果的進階 WildFire 日誌傳送回防火牆。在此範例中，日誌顯示檔案是惡意檔案。



STEP 6 | 防火牆已透過日誌轉送設定檔進行設定，該設定檔會在發現惡意軟體時，傳送警示給安全性管理員。

NAME	LOCATION	DESCRIPTION	LOG TYPE	FILTER	PANORAMA	SNMP	EMAIL	SYSLOG	HTTP	QUARANTINE	BUILT-IN ACTIONS
WildFire-Forwarding			threat	(severity eq critical)			WildFire-Forwarding				
			wildfire	(category eq benign)	☐						
			wildfire	(category neq benign) and (category neq malicious)			WildFire-Forwarding				
			wildfire	(category eq malicious)	☐		WildFire-Forwarding				

STEP 7 | 安全性管理員可透過名稱識別使用者 (若已設定 User-ID)，也可透過 IP 位址識別未設定使用者 ID 的使用者。此時，管理員可關閉銷售代表使用的網路或 VPN 連線，接著將連絡桌面支援群組協助使用者檢查並清理系統。

使用進階 WildFire 詳細分析報告後，桌面支援人員即可檢查進階 WildFire 分析報告中詳述的檔案、程序和登錄資訊，來判斷使用者系統是否感染到惡意軟體。如果使用者執行惡意軟體，支援人員可嘗試手動清理系統，也可重新製作系統映像。

FILE INFORMATION

File Type	PE
File Signer	
SHA-256	721b79505757ec7831844795afc4e88c23ce57cd4590118895cbfb86bcd34a77
SHA-1	2e8a6dd285f8fa829918aae60cb1b6172d918437
MD5	c67fdb7887368e41469a1a2556ac30df
File Size	55296 bytes
First Seen Timestamp	2016-12-13 18:39:45 UTC
Sample File	Download File
Verdict	Malware

SESSION INFORMATION

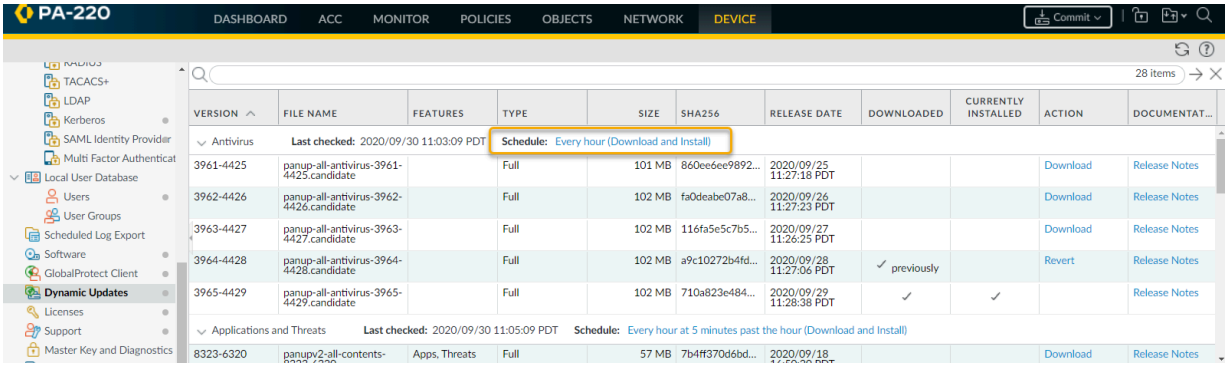
File Source	
File Destination	
User-ID	
Timestamp	2016-12-13 18:39:45 UTC
Serial Number	Manual
Firewall Hostname/IP	
Virtual System	
Application	
URL	
File Name	wildfire-test-pe-file (3).exe
Status	

COVERAGE STATUS

For endpoint antivirus coverage information for this sample, visit VirusTotal

STEP 8 | 目前管理員已發現惡意軟體，而且正在檢查使用者的系統時，如何防範日後暴露？答案：在此範例中，管理員排定在防火牆每隔 15 分鐘下載安裝進階 WildFire 特徵碼一次，並每天下

載安裝防毒更新一次。在銷售代表下載受感染的檔案後不到一個半小時內，進階 WildFire 會辨識出零時差惡意軟體並產生特徵碼，然後將特徵碼新增到 Palo Alto Networks 提供的進階 WildFire 更新特徵碼資料庫，防火牆隨後下載並安裝新的特徵碼。為下載進階 WildFire 與防毒特徵碼而設的防火牆和任何其他 Palo Alto Networks 防火牆現在即受到保護，不受這個新發現的惡意軟體侵害。下列螢幕擷取畫面顯示進階 WildFire 更新排程：



這些都是在大多數防毒軟體廠商察覺這個零時差惡意軟體前完成的。在此範例中，在極短的時間內，惡意軟體不再屬於零時差惡意軟體，因為 Palo Alto Networks 已發現惡意軟體，而且已經為客戶提供防護以防範日後暴露。

開始使用進階 WildFire

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

以下步驟說明在防火牆上開始使用進階 WildFire™ 的快速工作流程。如果您想在開始使用前瞭解關於進階 WildFire 的更多資訊，請參閱 進階 WildFire 概要介紹 並檢閱 進階 WildFire 最佳做法。

如需詳細瞭解如何使用 WildFire 私人雲端或混合型雲端，請參閱 WildFire 設備管理。

如果您在 Prisma Access 上使用進階 WildFire，請先熟悉產品，再設定您的 WildFire 分析安全性設定檔以轉送檔案進行進階 WildFire 分析。

STEP 1 | 取得進階 WildFire 或 WildFire 訂閱。即便您尚未訂閱，您仍可以轉送 PE 進行 WildFire 分析。

STEP 2 | 決定哪個 進階 WildFire 部署 適合您：

- 進階 WildFire 公共雲端—轉送範例至 Palo Alto Networks 託管的進階 WildFire 公共雲端。
- WildFire U.S.政府雲端—轉送樣本至 Palo Alto Networks 託管的 WildFire U.S.Government Cloud（WildFire 美國政府雲端）。

如果您要部署 *WildFire* 私人雲端或混合型雲端，請參閱 *WildFire* 設備管理。

STEP 3 | 請確認防火牆上的授權為作用中。

1. 登入防火牆。
2. 選取 **Device**（裝置） > **Licenses**（授權） 並確認 WildFire 授權為主動。

   如果 WildFire 授權不顯示，請選擇其中一個 License Management（授權管理）選項來啟動授權。

STEP 4 | 將防火牆連線至 WildFire 並設定 WildFire 設定。

1. 選取 **Device**（裝置） > **Setup**（設定） > **WildFire**，然後編輯 General Settings（一般設定）。
2. 請使用 **WildFire Public Cloud**（**WildFire** 公共雲端）欄位將範例轉送到進階 WildFire 公共雲端。
3. 定義防火牆轉送的檔案大小限制並設定 WildFire 日誌和報告設定。

   建議進階 WildFire 最佳做法將 *PE* 的 ***File Size***（檔案大小）設定為大小上限 *10 MB*，並將其他檔案類型的 ***File Size***（檔案大小）設定為預設值。
4. 按一下 **OK**（確定）來儲存 WildFire General Setting（一般設定）。

STEP 5 | 啟用防火牆以轉送解密 SSL 流量進行進階 WildFire 分析。

這是建議的進階 WildFire 最佳做法。

STEP 6 | 開始提交範例進行分析。

1. 定義要轉送進行 WildFire 分析的流量。（選擇 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **WildFire Analysis**（**WildFire** 分析）並進行修改，或 **Add**（新增）WildFire 分析設定檔）。

   做為最佳做法，使用 *WildFire* 分析預設設定檔可確保全面涵蓋防火牆允許的流量範圍。如果您仍決定建立自訂 *WildFire* 分析設定檔，設定該設定檔以轉送 ***Any***（任何）檔案類型—這會使防火牆自動開始轉送新支援的檔案類型進行分析。
2. 針對每項設定檔規則，請將 **public-cloud**（公共雲端）設為 **Destination**（目的地），以轉送範例至進階 WildFire 雲端進行分析。
3. 將 WildFire 分析設定檔附加至安全性政策規則。將轉送符合安全性原則規則的流量進行 WildFire 分析（**Policies**（原則） > **Security**（安全性） 並 **Add**（新增） 或修改安全性原則規則）。

STEP 7 | 啟用防火牆以取得最新的進階 WildFire 特徵碼。

即時擷取新的進階 WildFire 特徵碼，以偵測與識別惡意軟體。若運作的是 PAN OS 9.1 或更早版本，則每五分鐘可收到新的特徵碼。

- PAN-OS 9.1 和更早版本
  1. 選取 **Device**（裝置） > **Dynamic Updates**（動態更新）：
     - 請檢查系統是否顯示 **WildFire** 更新。
     - 選取 **Check Now**（立即檢查）以擷取最新特徵碼更新包。
  2. 請設定**Schedule**（排程）以下載和安裝最新的進階 WildFire 特徵碼。
  3. 使用 **Recurrence**（週期性）欄位將防火牆檢查更新的頻率設定為 **Every Minute**（每分鐘）。

     每五分鐘即可產生新的 *WildFire* 特徵碼，此設定可確保防火牆在有特徵碼可用的一分鐘內擷取這些特徵碼。
  4. 啟用防火牆，使之隨擷取 **Download and Install**（下載並安裝）這些更新。
  5. 按一下 **OK**（確定）。
- PAN-OS 10.0 和更高版本
  1. 選取 **Device**（裝置） > **Dynamic Updates**（動態更新）：
  2. 檢查是否顯示了 **WildFire** 更新。
  3. 選取 Schedule（排程）以設定更新頻率，然後使用 **Recurrence**（週期性）欄位設定防火牆以 **Real-time**（即時）擷取 WildFire 特徵碼。
  4. 按一下 **OK**（確定）。

STEP 8 | 開始掃描流量以偵測威脅，包括進階 WildFire 識別的惡意軟體。

附加 **default**（預設） 防毒設定檔至安全性原則規則以根據防毒特徵碼掃描規則允許的流量（選取 **Policies**（原則） > **Security**（安全性）並新增或修改為規則定義的 **Actions**（動作））。

STEP 9 | 對於已被進階 WildFire 識別為惡意或網路釣魚的連結，控制對相關網站的存取權。

此選項需要 *PAN-DB URL* 篩選授權。深入瞭解 *URL* 篩選，及其如何協助您根據 *URL* 類別控制網站存取權和企業認證提交（用於防止網路釣魚）。

若要設定 URL 篩選：

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **URL Filtering**（**URL** 篩選），然後 **Add**（新增）URL 篩選設定檔。
2. 選取 **Categories**（類別） 並定義網路釣魚和惡意 URL 類別的 **Site Access**（網站存取）。
3. **Block**（封鎖）使用者存取這些類別的網站，或允許存取，但在使用者存取這些類別的網站時產生 **Alert**（警示），以確保您具有這類事件的可見性。
4. 請啟用認證網路釣魚防範，防止使用者向不可信的網站提交認證，而無需封鎖使用者對這些網站的存取權。
5. 套用新的或已更新的 URL 篩選設定檔，並將其附加至安全性原則規則以將這些設定檔設定套用至允許的流量：
   1. 選取 **Policies**（原則） > **Security**（安全性），然後 **Add**（新增） 或修改安全性原則規則。
   2. 選取 **Actions**（動作）並在設定檔設定區段，將 **Profile Type**（設定檔類型） 設定為設定檔。
   3. 將新的或已更新的 **URL Filtering**（**URL** 篩選）設定檔附加至安全性原則規則。
   4. 按一下 **OK**（確定）來儲存安全性原則規則。

STEP 10 | 確認防火牆以成功轉送樣本。

- 若您已啟用良性檔案日誌，請選取 **Monitor**（監控） > **WildFire Submissions**（**WildFire** 提交），然後確認項目已做為良性檔案記錄並提交進行分析。（若您希望在確認防火牆連接至 WIldFire 雲端後停用良性檔案日誌，請選取 **Device**（裝置） > **Setup**（設定） > **WildFire** 然後清除 **Report Benign Files**（回報良性檔案））。
- 其他選項允許您確認防火牆以轉送特定樣本，根據檔案類型檢視防火牆轉送的樣本，以及檢視防火牆轉送的總樣本數。
- 測試樣本惡意軟體檔案 測試您完整的 WildFire 設定。

STEP 11 | 研究分析結果。

- 取得分析結果：
  - 透過防火牆監控惡意軟體並檢視 WildFire 分析報告範例。
  - 在進階 WildFire 入口網站上，檢視提交至進階 WildFire 公共雲端（包括您手動提交至 WildFire 公共雲端）的所有範本報告。
  - 使用進階 WildFire API 擷取來自 WildFire 設備的範例裁定和報告。

STEP 12 | 接下來的步驟：

檢閱並實作 進階 WildFire 最佳做法。

進階 WildFire 部署最佳做法

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

下列主題說明部署和設定 Palo Alto Networks 建議當您使用 WildFire® 硬體或服務做為網路威脅偵測與預防解決方案的一部分。

- 進階 WildFire 最佳做法

進階 WildFire 最佳做法

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

Prisma Access 使用者—請參閱 Prisma Access 文件，瞭解使用者介面相關產品特定資訊。

- ❑ 遵循最佳做法，使您的網路不受第 4 層和第 7 層攻擊影響，從而確保內容識別和分析的穩定。尤其要確保實作 TCP 設定（**Device**（裝置） > **Setup**（設定） > **Session**（工作階段） > **TCP Settings**（**TCP** 設定））及 Content-ID™ 設定（**Device**（裝置） > **Setup**（設定） > **Content-ID**（內容 **ID**） > **Content-ID Settings**（內容 **ID** 設定））的最佳做法。
- ❑ 也確保您同時具有主動威脅防護訂閱。進階 WildFire® 和威脅防護結合在一起可實現全面的威脅偵測和防範。
- ❑ 每日下載並安裝內容更新以接收最新的產品更新和 Palo Alto Networks 產生的威脅保護功能。請參閱安裝內容和軟體更新說明，深入瞭解更新套件所含內容。
- ❑ 若您執行 PAN-OS 10.0 或更高版本，請設定防火牆以即時擷取進階 WildFire 特徵碼。一旦進階 WildFire 公共雲端可以產生新發現的惡意軟體特徵碼後，即可對其進行存取，以盡可能減少暴露於惡意活動的時間，防止攻擊得逞。
- ❑ 如果防火牆設定為解密 SSL 流量，請啟用防火牆以轉送解密 SSL 流量進行 WildFire 分析。只有超級使用者能夠啟用此選項。
- ❑ 使用預設 WildFire 分析設定檔，定義防火牆應轉送進行分析的流量（**Objects**（物件） > **Security Profiles**（安全性設定檔） > **WildFire Analysis**（**WildFire** 分析））。預設 WildFire 分

析設定檔可確保所有流量全面涵蓋安全性政策允許的範圍，該設定檔會指定所有應用程式上支援轉送進行進階 WildFire 分析的檔案類型，而無論這些檔案是否已上傳或下載。

如果您選擇建立自訂 WildFire 分析設定檔，最佳做法是仍然將設定檔設定為轉送 **any**（任何）檔案類型。這讓防火牆能夠在檔案支援分析時自動開始轉送檔案。

如需詳細瞭解如何套用 WildFire 分析設定檔至防火牆流量，請參閱如何 轉送檔案進行進階 WildFire 分析。

如果流量產生的進階 *WildFire* 特徵碼引發重設或丟棄動作，防毒設定檔中的 *WildFire* 動作設定可能會影響流量。因為進階 *WildFire* 可能會將自訂程式判定為惡意程式並為其產生特徵碼，您可以排除內部流量（例如軟體散佈應用程式）以部署自訂程式，安全地轉換到最佳做法。請檢查 ***Monitor***（監控） > ***Logs***（日誌） > ***WildFire Submissions***（***WildFire*** 提交），以查看是否有任何內部自訂程式觸發了進階 *WildFire* 特徵碼。

- 當您將防火牆設定為轉送檔案進行進階 WildFire 分析，請參閱所有支援檔案類型的檔案 **Size Limit**（大小限制）。將所有檔案類型的 **Size Limit**（大小上限） 設定為預設上限。（選取 **Device**（裝置） > **Setup**（設定） > **WildFire** 並編輯一般設定以根據檔案類型調整檔案大小上限。您可以檢視說明資訊以找到每個檔案類型的預設大小上限）。

  關於 **WildFire** 轉送的預設檔案大小上限

  防火牆上的預設檔案大小上限旨在於 WildFire 中包含大多數惡意軟體（小於預設大小上限），並排除不太可能是惡意軟體但會影響 WildFire 檔案轉送能力的大型檔案。由於防火牆保留用於轉送檔案進行進階 WildFire 分析的容量有限，轉送大量大型檔案可能會使防火牆略過部分檔案之轉送。為高速周遊防火牆的檔案類型設定檔案大小上限時，會發生此情況。在這種情況下，

可能不會轉送潛在的惡意檔案進行進階 WildFire 分析。如果您要增加檔案（超過預設大小上限的 PE 除外）大小上限，考慮這種可能的情形。

下表根據 Palo Alto Networks 威脅研究團隊的觀察結果制定，展示了惡意軟體檔案大小的典型散佈。防火牆預設檔案大小設定可以增加至檔案大小上限設定，從而使每種檔案類型的惡意軟體擷取率獲得相對較小的增加。

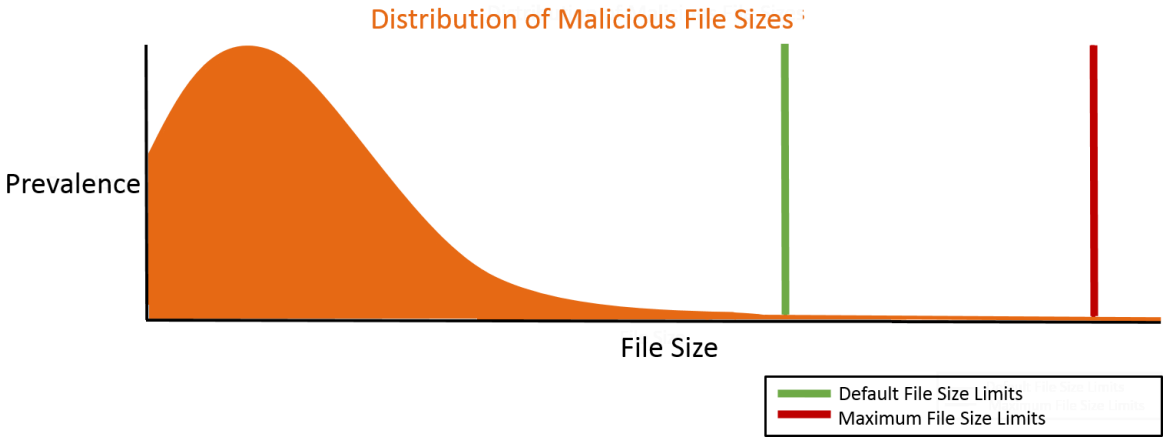


圖 **1:** 建議檔案大小上限以擷取非常大的惡意檔案

如果您特別擔心非常大的惡意檔案造成損壞，可將檔案大小上限增加到超過預設設定。在這種情況下，建議採用下列設定，以擷取罕見的大型惡意檔案。

選取 **Device**（裝置）> **Setup**（設定）> **WildFire**，並編輯一般設定以調整每個檔案類型的 **Size Limit**（大小上限）：

檔案類型	**PAN-OS 9.0** 及更高版本檔案轉送最大大小建議	**PAN-OS 8.1** 檔案轉送最大大小建議
pe	16MB	10MB
apk	10MB	10MB
pdf	3,072KB	1,000KB
ms-office	16,384KB	2,000KB
jar	5MB	5MB
flash	5MB	5MB
MacOSX	10MB	1MB
archive	50MB	10MB
linux	50MB	10MB

檔案類型	**PAN-OS 9.0** 及更高版本檔案轉送最大大小建議	**PAN-OS 8.1** 檔案轉送最大大小建議
指令碼	20KB	20KB

設定進階 WildFire 分析

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

以下主題說明如何在網路部署中啟用進階 WildFire™ 分析。您可以將 Palo Alto Networks 防火牆設定為自動轉送未知檔案至進階 WildFire 公共雲端或 WildFire 私人雲端，您也可以使用進階 WildFire 入口網站手動提交檔案進行分析。提交進行分析的範例將收到良性、灰色軟體、惡意或網路釣魚裁定，且針對每個範例產生詳細的分析報告。

- 轉送檔案進行進階 WildFire 分析
- 轉送解密 SSL 流量進行進階 WildFire 分析
- 啟用進階 WildFire 內嵌 ML
- 啟用進階 WildFire 內嵌雲端分析
- 啟用即時特徵碼查閱的保留模式
- 確認 WildFire 提交
- 手動上載檔案至 WildFire 入口網站
- 依型號的防火牆檔案轉送容量

轉送檔案進行進階 WildFire 分析

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

設定 Palo Alto Networks 防火牆，轉送未知檔案或電子郵件連結及與現有防毒特徵碼相符的封鎖檔案，以進行分析。使用 **WildFire Analysis**（**WildFire** 分析）設定檔來定義轉送至進階 WildFire 公共雲端選項之一的檔案，然後附加設定檔至安全性規則，以觸發零時差惡意軟體檢查。

根據使用中的應用程式、偵測到的檔案類型、電子郵件訊息中包含的連結或樣本的傳輸方向（上載、下載或兩者）指定轉送進行分析的流量。例如，您可以將防火牆設定為轉送可攜式可執行檔 (PE) 或使用者瀏覽網頁時嘗試下載的任何檔案。除未知樣本外，防火牆還會轉送與現有防毒特徵碼相符的封鎖檔案。如此一來便可根據特徵碼成功阻止但先前未遇過的惡意軟體變體，為 Palo Alto Networks 提供可貴的威脅情報來源。

如果您使用 WildFire 設備託管 WildFire 私人雲端，您可將防火牆設定為繼續轉送機敏檔案至您的 WildFire 私人雲端進行本機分析，即可將 WildFire 分析資源延伸至WildFire 混合型雲端，而將不太機敏或不受支援的檔案類型轉送至 WildFire 公共雲端。如需詳細瞭解如何使用和設定 WildFire 設備，請參閱 WildFire 設備管理。

開始之前：

- 檔案分析支援在進階 WildFire 雲端區域之間可能會有輕微差異。如需詳細資訊，請參閱文件類型支援。
- 若負責轉送檔案的防火牆與進階 WildFire 雲端之間有其他防火牆，請確認該防火牆允許下列連接埠：

連接埠	使用方式
443	註冊、PCAP 下載、範例下載、報告搜尋、文件提交、PDF 報告下載
10443	動態更新

- Strata Cloud Manager

- PAN-OS 和 Panorama

轉送檔案進行進階 WildFire 分析（Cloud Management）

如果您使用 ***Panorama*** 管理 ***Prisma Access***：

請切換到 ***PAN-OS*** 頁籤並按照指示進行操作。

如果您使用 ***Prisma Access*** 雲端管理，請從此處繼續。

STEP 1 | 指定要接收範例的進階 WildFire 雲端。

選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服務） > **WildFire and Antivirus**（**WildFire** 和防毒） > **General Settings**（一般設定），然後根據您的 WildFire 雲端部署（公共、政府、私人或混合）編輯一般設定。

WildFire U.S.Government Cloud（*WildFire* 美國政府雲端）僅供美國聯邦機構作為選用分析環境使用。

新增雲端環境的 **WildFire Cloud**（**WildFire** 雲端）URL，以轉送範例進行分析。

進階 **WildFire** 公共雲端選項：

1. 輸入 **WildFire Public Cloud**（**WildFire** 公共雲端） URL：
   - 美國：**wildfire.paloaltonetworks.com**
   - 歐洲：**eu.wildfire.paloaltonetworks.com**
   - 日本：**jp.wildfire.paloaltonetworks.com**
   - 新加坡：**sg.wildfire.paloaltonetworks.com**
   - 英國：**uk.wildfire.paloaltonetworks.com**
   - 加拿大：**ca.wildfire.paloaltonetworks.com**
   - 澳洲：**au.wildfire.paloaltonetworks.com**
   - 德國：**de.wildfire.paloaltonetworks.com**
   - 印度：**in.wildfire.paloaltonetworks.com**
   - 瑞士：**ch.wildfire.paloaltonetworks.com**
   - 波蘭：**pl.wildfire.paloaltonetworks.com**
   - 印尼：**id.wildfire.paloaltonetworks.com**
   - 台灣：**tw.wildfire.paloaltonetworks.com**
   - 法國：**fr.wildfire.paloaltonetworks.com**
   - 卡達：**qatar.wildfire.paloaltonetworks.com**
   - 韓國：**kr.wildfire.paloaltonetworks.com**

- 以色列：**il.wildfire.paloaltonetworks.com**
- 沙烏地阿拉伯：**sa.wildfire.paloaltonetworks.com**
- 西班牙：**es.wildfire.paloaltonetworks.com**

2. 確保 **WildFire Private Cloud**（**WildFire** 私人雲端）欄位為空。

WildFire FedRAMP 雲端選項：

1. 輸入 **WildFire FedRAMP Cloud**（**WildFire FedRAMP** 雲端）URL：
   - 美國政府雲端：**wildfire.gov.paloaltonetworks.com**
   - 進階 WildFire 政府雲端：gov-cloud.wildfire.paloaltonetworks.com
   - 進階 WildFire 公共部門雲端：pubsec-cloud.wildfire.paloaltonetworks.com
2. 確保 **WildFire Private Cloud**（**WildFire** 私人雲端）欄位為空。

STEP 2 | 選取 **Allow Forwarding of Decrypted Content**（允許轉送解密內容），啟用 Prisma Access 來轉送解密的 SSL 流量以進行進階 WildFire 分析。根據安全性政策規則評估的解密流量；若其與附加至安全性規則的 WildFire 分析設定檔相符，解密流量將在重新加密前轉送進行分析。

轉送解密 *SSL* 流量進行分析是進階 *WildFire* 的最佳做法。

STEP 3 | 定義 Prisma Access 轉送進行分析的範例大小上限。

將檔案轉送值設為預設設定是進階 WildFire 最佳做法。

STEP 4 | 設定提交日誌設定。

1. 選取 **Report Benign Files**（回報良性檔案），允許日誌收到良性裁定的檔案。
2. 選取 **Report Grayware Files**（回報灰色軟體檔案），允許日誌收到灰色軟體裁定的檔案。

STEP 5 | 完成後，請 **Save**（儲存）您的變更。

STEP 6 | 定義要轉送進行分析的流量。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服務） > **WildFire and Antivirus**（**WildFire** 和防毒），然後 **Add Profile**（新增設定檔）。提供設定檔的 **Name**（名稱）和 **Description**（說明）。
2. **Add Rule**（新增規則）以定義要轉送進行分析的流量，並為規則提供描述性**Name**（名稱），例如 local-PDF-analysis。
3. 定義設定檔規則以符合未知流量，並根據下列項目轉送範例進行分析：
   - **Direction of Traffic**（流量方向）—根據檔案的傳輸方向（**Upload**（上傳）、**Download**（下載）或 **Upload and Download**（上傳和下載））轉送檔案以進行

分析。例如，選擇 **Upload and Download**（上傳和下載）無論傳輸方向為何，轉送所有未知 PDF 進行分析。

- **Applications**（應用程式）—根據使用中的應用程式轉送檔案進行分析。
- **File Types**（檔案類型）—根據檔案類型，包括電子郵件訊息中包含的連結，轉送檔案進行分析。例如，選取 **PDF** 轉送防火牆偵測到的未知 PDF 進行分析。
- 選取流量要轉送進行分析的目的地。
  - 選取 **Public Cloud**（公共雲端），讓所有符合規則的流量轉送至進階 WildFire 公共雲端以進行分析。
  - 選取 **Private Cloud**（私人雲端），讓所有符合規則的流量轉送至 WildFire 設備以進行分析。
  - 完成後請**Save**（儲存） WildFire 分析轉送規則。

4. 請 **Save**（儲存） WildFire 和防毒安全設定檔。

STEP 7 | 啟用 WildFire 和防毒安全設定檔。

根據附加的 WildFire 分析設定檔評估安全性政策規則允許的流量；Prisma Access 會轉送符合設定檔的流量進行 WildFire 分析。

STEP 8 | 推送設定變更。

STEP 9 | （選用） 啟用進階 WildFire 內嵌 ML

STEP 10 | 選擇下一步操作...

- 驗證 WildFire 提交，以確認防火牆已成功轉送檔案進行分析。
- 監控 WildFire 活動以評估警示及報告惡意軟體的詳細資訊。

轉送檔案進行進階 WildFire 分析（PAN-OS 和 Panorama）

STEP 1 | （僅限 PA-7000 系列防火牆）若要啟用 PA-7000 系列防火牆來轉送範例進行分析，您首先必須在 NPC 上將資料連接埠設為日誌卡介面。如果您的 PA-7000 系列設備配備了 LFC（記錄轉送卡），則必須設定 LFC 使用的連接埠。設定後，當轉送範例時，日誌卡連接埠或 LFC 介面將優先於管理連接埠。

STEP 2 | 指定 進階 WildFire 部署 您的範例轉送目的地。

選取 **Device**（裝置） > **Setup**（設定） > **WildFire** 並根據您的 WildFire 雲端部署（公共、私人或混合型）編輯一般設定。

WildFire U.S.Government Cloud（*WildFire* 美國政府雲端）僅供美國聯邦機構作為選用分析環境使用。

進階 **WildFire** 公共雲端：

1. 輸入 **WildFire Public Cloud**（**WildFire** 公共雲端） URL：
   - 美國：**wildfire.paloaltonetworks.com**
   - 歐洲：**eu.wildfire.paloaltonetworks.com**
   - 日本：**jp.wildfire.paloaltonetworks.com**
   - 新加坡：**sg.wildfire.paloaltonetworks.com**
   - 英國：**uk.wildfire.paloaltonetworks.com**
   - 加拿大：**ca.wildfire.paloaltonetworks.com**
   - 澳洲：**au.wildfire.paloaltonetworks.com**
   - 德國：**de.wildfire.paloaltonetworks.com**
   - 印度：**in.wildfire.paloaltonetworks.com**
   - 瑞士：**ch.wildfire.paloaltonetworks.com**
   - 波蘭：**pl.wildfire.paloaltonetworks.com**
   - 印尼：**id.wildfire.paloaltonetworks.com**
   - 台灣：**tw.wildfire.paloaltonetworks.com**
   - 法國：**fr.wildfire.paloaltonetworks.com**
   - 卡達：**qatar.wildfire.paloaltonetworks.com**
   - 韓國：**kr.wildfire.paloaltonetworks.com**
   - 以色列：**il.wildfire.paloaltonetworks.com**
   - 沙烏地阿拉伯：**sa.wildfire.paloaltonetworks.com**
   - 西班牙：**es.wildfire.paloaltonetworks.com**
2. 確保 **WildFire Private Cloud**（**WildFire** 私人雲端）欄位為空。

WildFire FedRAMP 雲端選項：

1. 輸入 **WildFire FedRAMP Cloud**（**WildFire FedRAMP** 雲端）URL：
   - 美國政府雲端：**wildfire.gov.paloaltonetworks.com**
   - 進階 WildFire 政府雲端：gov-cloud.wildfire.paloaltonetworks.com
   - 進階 WildFire 公共部門雲端：pubsec-cloud.wildfire.paloaltonetworks.com

2. 確保 **WildFire Private Cloud**（**WildFire** 私人雲端）欄位為空。

STEP 3 | 定義防火牆轉送的檔案大小限制並設定日誌和報告設定。

繼續編輯一般設定（**Device**（裝置） > **Setup**（設定） > **WildFire**）。

- 請參閱從防火牆轉送的 **File Size Limits**（檔案大小限制）。

  建議進階 WildFire 最佳做法將 *PE* 的 ***File Size***（檔案大小）上限設為 *10 MB*，其他檔案類型的 ***File Size***（檔案大小）則保留預設值。

- 選取 **Report Benign Files**（回報良性檔案），允許日誌收到良性裁定的檔案。
- 選取 **Report Grayware Files**（回報灰色軟體檔案），允許日誌收到灰色軟體裁定的檔案。
- 透過編輯工作階段資訊設定，定義 WildFire 分析報告中記錄的工作階段資訊。依預設，WildFire 分析報告中顯示所有工作階段資訊。取消選取核取方塊，從 WildFire 分析報告中移除相應欄位，然後按一下 **OK**（確定）儲存設定。

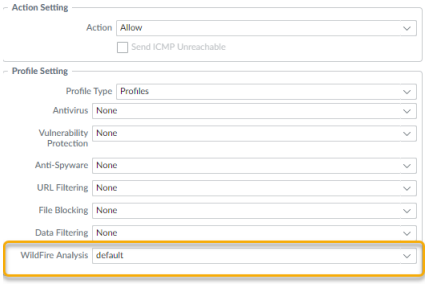
STEP 4 | 定義要轉送進行分析的流量。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **WildFire Analysis**（**WildFire** 分析），**Add**（新增） 新的 WildFire 分析檔案，以及為設定檔提供描述性 **Name**（名稱）。
2. **Add**（新增）設定檔規則以定義要轉送進行分析的流量，並為規則提供描述性**Name**（名稱），例如 local-PDF-analysis。
3. 定義設定檔規則以符合未知流量，並根據下列項目轉送範例進行分析：
   - **Applications**（應用程式）—根據使用中的應用程式轉送檔案進行分析。
   - **File Types**（檔案類型）—根據檔案類型，包括電子郵件訊息中包含的連結，轉送檔案進行分析。例如，選取 **PDF** 轉送防火牆偵測到的未知 PDF 進行分析。
   - **Direction**（方向）—根據檔案的傳輸方向（上載、下載或兩者）轉送檔案進行分析。例如選取**both**（兩者）以轉送所有未知 PDF 進行分析，無論傳輸方向為何。
4. 按一下 **OK**（確定）來儲存 WildFire 分析設定檔。

STEP 5 | 將 WildFire 分析設定檔附加至安全性原則規則。

根據附加的 WildFire 分析設定檔評估安全性原則規則允許的流量；防火牆轉送符合設定檔的流量進行 WildFire 分析。

1. 選取 **Policies**（原則） > **Security**（安全性），然後 **Add**（新增） 或修改原則規則。
2. 按一下原則規則內部的 **Actions**（動作）頁籤。
3. 在設定檔設定部分，選取做為 **Profile Type**（設定檔類型）的 **Profiles**（設定檔），然後選取附加至原則規則的 **WildFire Analysis**（**WildFire** 分析）設定檔



STEP 6 | 請確保啟用防火牆以轉送解密 SSL 流量進行進階 WildFire 分析。

這是 建議的最佳做法。

STEP 7 | （選用） 啟用進階 WildFire 內嵌 ML

STEP 8 | （選用） 啟用即時特徵碼查閱的保留模式

STEP 9 | 檢閱並實作 進階 WildFire 最佳做法。

STEP 10 | 按一下 **Commit**（提交）以套用更新後的設定。

STEP 11 | （選用）安裝裝置憑證以更新至最新憑證版本，讓防火牆可用以和 Palo Alto Networks 雲端服務進行通訊。

STEP 12 | （選用） 設定 Content Cloud FQDN 設定。

STEP 13 | 選擇下一步操作...

- 驗證 WildFire 提交，以確認防火牆已成功轉送檔案進行分析。
- 監控 WildFire 活動以評估警示及報告惡意軟體的詳細資訊。

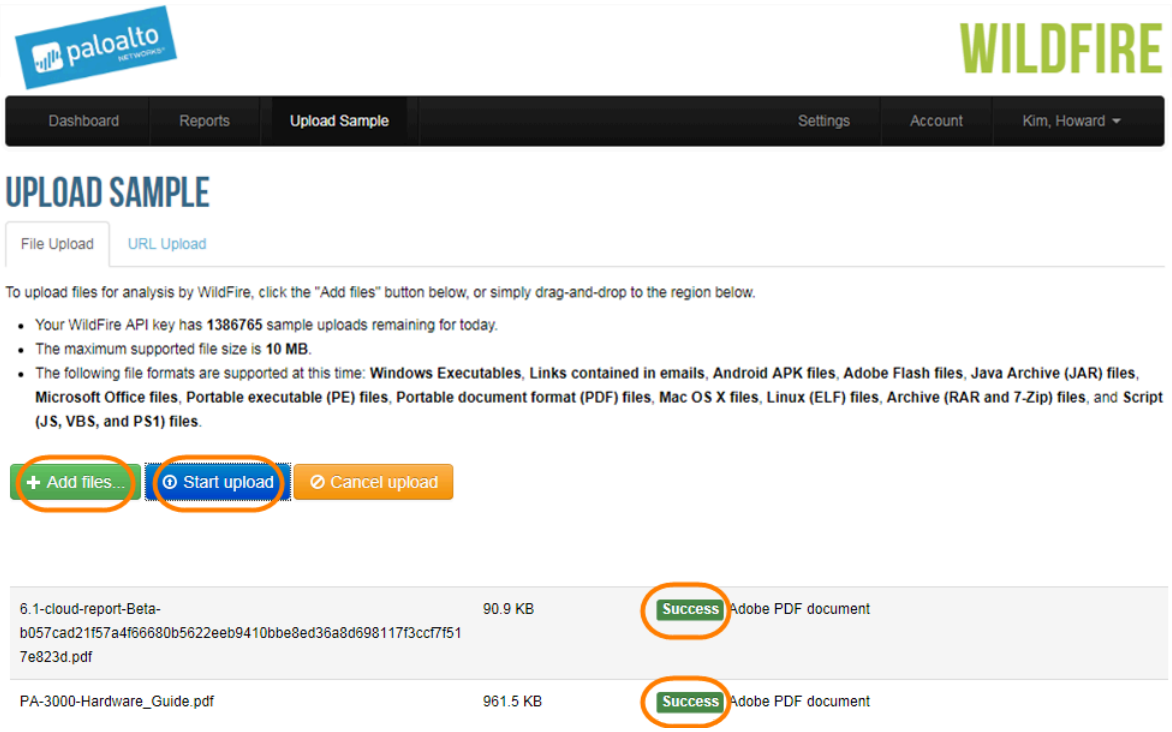
手動上載檔案至 WildFire 入口網站

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

所有擁有支援帳戶的 Palo Alto Networks 客戶皆可使用 Palo Alto Networks WildFire 入口網站，一天最多提交五份範例進行分析。如果您擁有進階 WildFire 或 WildFire 訂閱，您可以手動提交範例至入口網站，其計入每日 1000 份範例上傳限制；但請留意，每日 1000 份範例上傳限制也包括 WildFire API 提交項目。

STEP 1 | 手動上載檔案或 URL 至 WildFire 入口網站進行分析。

1. 登入 WildFire 入口網站。
2. 在功能表列上按一下**Upload Sample**（上載樣本）。
   - 若要提交檔案進行分析，請選取 **File Upload**（檔案上傳）並 **Open**（開啟）您想要提交進行分析的檔案。按一下 **Start**（開始），即可開始對單一檔案進行分析，或按一下 **Start Upload**（開始上傳），提交您已新增進行分析的所有檔案。
   - 若要提交 URL 進行分析，請按一下 **URL Upload**（**URL** 上傳）、輸入 URL，並 **Submit**（提交）進行分析。



3. 關閉 **Uploaded File Information**（已上載檔案資訊）快顯視窗。

STEP 2 | 檢視檔案的裁定和分析結果。

請至少等待五分鐘，讓進階 WildFire 分析範例。

由於手動上載並未與特定防火牆產生關聯，因此手動上載不會在報告中顯示工作階段資訊。

1. 返回 WildFire 入口網站儀表板。
2. 在 Previous 1 Hour（之前 1 小時）區段中，選擇來源欄下的 **Manual**（手動）以檢視最新手動提交樣本的分析資訊。
3. 找出已上載的檔案或 URL，並按一下接收時間左邊的詳細資料圖示。

轉送解密 SSL 流量進行進階 WildFire 分析

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

啟用防火牆以轉送解密 SSL 流量進行進階 WildFire 分析。根據安全性政策規則評估防火牆解密的流量；若其與附加至安全性規則的 WildFire 分析設定檔相符，解密流量將在防火牆重新加密前轉送進行分析。只有超級使用者能夠啟用此選項。

轉送解密的 *SSL* 流量進行分析是 進階 WildFire 最佳做法。

在未啟用多個虛擬系統的防火牆上：

1. 請務必啟用防火牆以執行 解密 和 轉送檔案進行進階 WildFire 分析。
2. 選取 **Device**（裝置） > **Setup**（設定） > **Content - ID**（內容-ID）。
3. 編輯內容 ID 設定，並 **Allow Forwarding of Decrypted Content**（允許轉寄解密的內容）。
4. 按一下 **OK**（確認）以儲存變更。

在啟用虛擬系統的防火牆上：

1. 請務必啟用 解密 和 轉送檔案進行進階 WildFire 分析。
2. 選取 **Device**（裝置） > **Virtual Systems**（虛擬系統），按一下您要修改的虛擬系統，並 **Allow Forwarding of Decrypted Content**（允許轉寄解密的內容）。

針對 Prisma Access，此為 **WildFire and Antivirus**（**WildFire** 和防毒）安全設定檔設定的一部分。如需詳細資訊，請參閱適用於 Prisma Access 的轉送檔案進行進階 WildFire 分析。

啟用進階 WildFire 內嵌雲端分析

這可在何處使用？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權

Palo Alto Networks 進階 WildFire 使用一系列以雲端為基礎的 ML 偵測引擎，藉此真對穿過您網路的 PE（可攜式執行檔）檔案提供內嵌分析，以即時偵測並防止進階惡意軟體。與 WildFire 偵測到的其他惡意內容一樣，進階 WildFire 內嵌雲端偵測到的威脅都會產生特徵碼，然後將透過特徵碼更新套件以向客戶提供該特徵碼，藉此為所有 Palo Alto Networks 客戶提前建立防禦。

以雲端為基礎的引擎能夠偵測到前所未見的惡意軟體（例如，Palo Alto Networks 零日 - 先前從未被其他人或 Palo Alto Networks 發現的惡意軟體）並封鎖其進入您的環境。進階 WildFire 內嵌雲端分析在防火牆上使用輕量級轉送機制，以將任何效能影響降至最低。以雲端為基礎的機器學習模型將流暢地更新，以應對瞬息萬變的威脅形勢，而無需內容更新或功能發佈支援。

進階 WildFire 內嵌雲端分析之啟用與設定將透過 WildFire 分析設定檔進行，並且需要具有作用中進階 WildFire 授權的 PAN-OS 11.1 或更新版本。

STEP 1 | 安裝用於向進階 WildFire 雲端分析服務進行驗證更新的防火牆裝置憑證。對為內嵌雲端分析啟用的所有防火牆重複上述步驟。

如果您已在防火牆上安裝了目前版本的裝置憑證，則無需執行此步驟。

STEP 2 | 登入 PAN-OS 網頁介面。

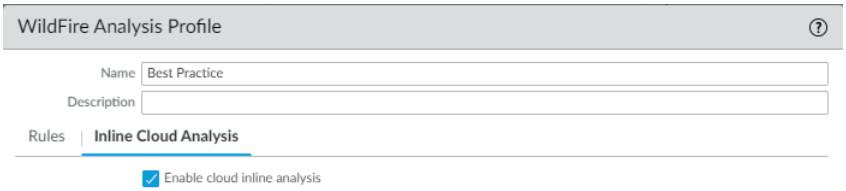
STEP 3 | 若要啟用進階 WildFire 內嵌雲端分析，您必須具有作用中的進階 WildFire 訂閱。如需詳細資訊，請參閱：授權、註冊和啟動。

若要確認當前哪些訂閱具有作用中的授權，請選取 **Device**（裝置） > **Licenses**（授權），並確認有適當的授權可用並且該授權沒有過期。

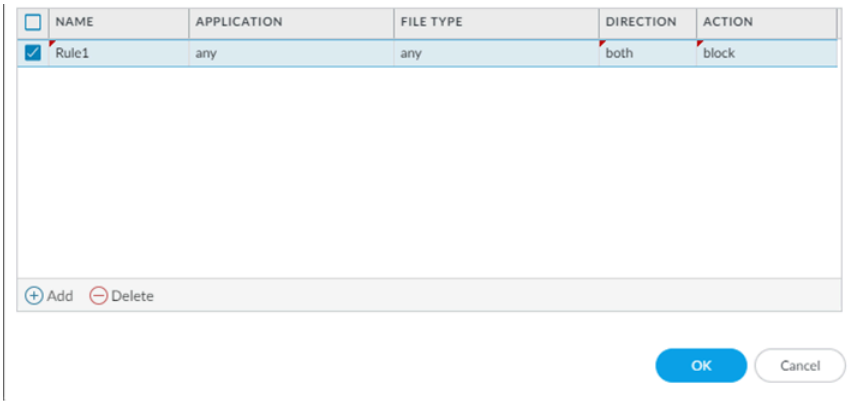
如果您目前的 *WildFire* 授權已過期並且您正在安裝進階 *WildFire* 授權，則必須先從 *NGFW* 中移除 *WildFire* 授權，才能安裝進階 *WildFire* 授權。

STEP 4 | 更新或建立新的 WildFire 分析安全性設定檔以啟用進階 WildFire 內嵌雲端分析。

1. 選擇現有 **WildFire Analysis Profile**（**WildFire** 分析設定檔），或 **Add**（新增）新的設定檔（**Objects**（物件） > **Security Profiles**（安全性設定檔） > **WildFire Analysis**（**WildFire** 分析））。
2. 選取您的 WildFire 分析設定檔，然後移至 **Inline Cloud Analysis**（內嵌雲端分析）並 **Enable cloud inline analysis**（啟用雲端內嵌分析）。



3. 指定規則定義進階 WildFire 內嵌雲端分析偵測到進階惡意軟體時要採取的動作。



- 名稱—針對您新增至設定檔的任何規則輸入描述名稱（最多 31 個字元）。
- 應用程式—新增應用程式流量以符合定義控管內嵌雲端 ML 動作的規則。
- 檔案類型—選取要在已為規則定義的分析目的地進行分析的檔案類型。

  目前僅支援 *PE*（可攜式執行檔）。

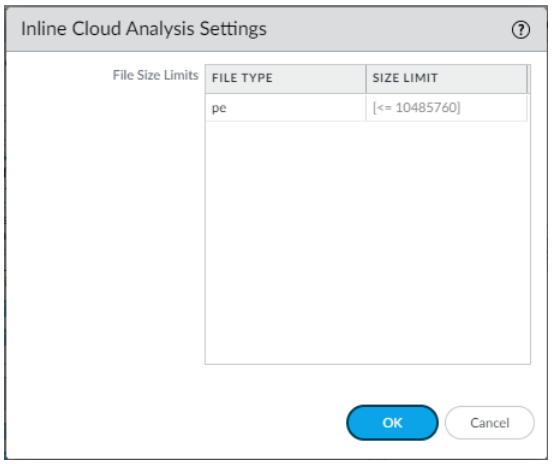
- 方向—取決於傳輸方向，將規則套用至流量。您可以套用該規則來 **download**（下載）流量。
- 動作—設定使用進階 WildFire 內嵌雲端分析偵測到威脅時要採取的動作。您可以 **allow**（允許）應用程式流量繼續前往目的地，或 **block**（封鎖）來自來源或來源目的地的流量。

  Palo Alto Networks 建議將動作設定為封鎖以獲得最佳安全性。

4. 按一下 **OK**（確定）以退出 WildFire 分析設定檔設定對話方塊。

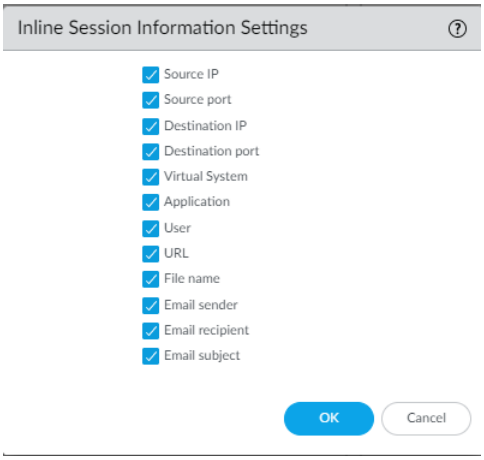
STEP 5 | 檢閱可使用進階 WildFire 內嵌雲端分析轉送以進行分析的檔案大小上限。

進階 *WildFire* 內嵌雲端分析可提供快速的 *WildFire* 裁定，然而，只有在樣本經過完整的動態分析（最多可能需要 *30* 分鐘）後，才能取得惡意樣本的完整報告。



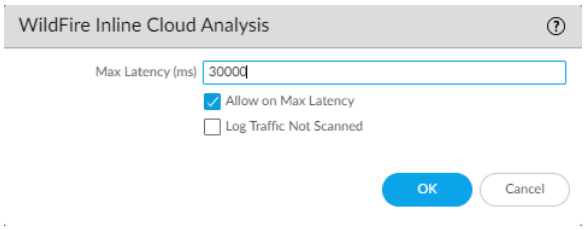
1. 選取 **Device**（裝置） > **Setup**（設定） > **WildFire** > **Inline Cloud Analysis Settings**（內嵌雲端分析設定） 並檢閱檔案大小上限。
2. 按一下 **OK**（確定）確認您的變更。

STEP 6 | 指定防火牆針對相關指定樣本轉送的網路工作階段資訊。Palo Alto Networks 使用工作階段資訊瞭解有關可疑網路事件內容、與惡意軟體相關的入侵指標、受影響的主機與用戶端，以及用於傳遞惡意軟體的更多資訊。根據預設，這些選項均會啟用。



1. 選取 **Device**（裝置） > **Setup**（設定） > **WildFire** > **Inline Session Information Settings**（內嵌工作階段資訊設定），並視需求選取或清除下列選項。
   - **Source IP**（來源 **IP**）— 轉送傳送未知檔案的來源 IP 地址。
   - **Source Port**（來源連接埠）— 轉送傳送未知檔案的來源連接埠。
   - **Destination IP**（目的地 **IP**）— 轉送未知檔案的目的地 IP 地址。
   - **Destination Port**（目的地連接埠）— 轉送未知檔案的目的地連接埠。
   - **Virtual System**（虛擬系統）— 轉送偵測到未知檔案的虛擬系統。
   - **Application**（應用程式）— 轉送傳輸未知檔案的使用者應用程式。
   - **User**（使用者）— 轉送目標使用者。
   - **URL**— 轉送與未知檔案相關的 URL。
   - **Filename**（檔案名稱）— 轉送未知檔案的名稱。
   - **Email sender**（電子郵件寄件者）— 轉送未知電子郵件連結的寄件者（該電子郵件寄件者的名字也會出現在 WildFire 日誌和報告中）。
   - **Email recipient**（電子郵件收件者）— 轉送未知電子郵件連結的收件者（該電子郵件收件者的名字也會出現在 WildFire 日誌和報告中）。
   - **Email subject**（電子郵件主旨）— 轉送未知電子郵件連結的主旨（該電子郵件主旨會出現在 WildFire 日誌和報告中）。
2. 按一下 **OK**（確定）確認您的變更。

STEP 7 | 請設定要求超過最大延遲時，要採取的逾時延遲和動作。

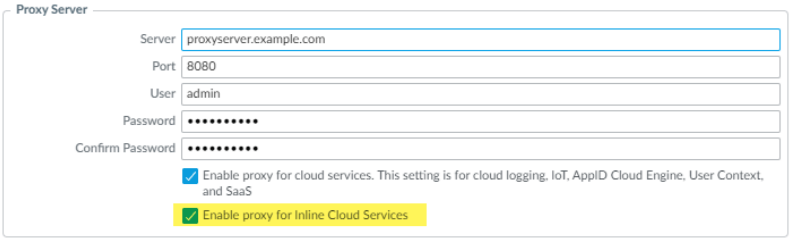


1. 指定進階 WildFire 內嵌雲端分析要求達到延遲上限時要採取的動作：
   - 最大延遲（毫秒）—指定進階 WildFire 內嵌雲端分析回傳結果的最大可接受處理時間（以秒為單位）。
   - 達到最大延遲時允許—使防火牆能夠在達到最大延遲時執行允許動作。取消選取此選項可將防火牆動作設定為封鎖。
   - 未掃描日誌流量—使防火牆能記錄展現存在進階惡意軟體，但尚未受到進階 WildFire 雲端分析處理的要求。
2. 按一下 **OK**（確定）確認您的變更。

STEP 8 | （使用明確 Proxy 伺服器部署防火牆時為必要項目）設定代理伺服器，以用於存取有助於所有已設定內嵌雲端分析功能所產生要求的伺服器。可以指定單一 Proxu 伺服器並將其套用至所有 Palo Alto Networks 更新服務，包括所有已設定的內嵌雲端和記錄日誌服務。

1. （PAN-OS 11.2.3 及更新版本）透過 PAN-OS 設定 Proxy 伺服器。
   1. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務），並編輯 **Services**（服務）詳細資料。
   2. 指定 **Proxy Server**（**Proxy** 伺服器）設定並 **Enable proxy for Inline Cloud Services**（啟用內嵌運端服務的 **Proxy** 存取）。您可以在 **Server**（伺服器）欄位中提供 IP 位址或 FQDN。

      Proxy 伺服器密碼必須包含至少六個字元。

   3. 按一下 **OK**（確定）。
2. （PAN-OS 11.1.5 及更新版本）透過防火牆 CLI 設定 Proxy 伺服器。
   1. 存取防火牆 CLI。
   2. 使用下列 CLI 命令設定基本 Proxy 伺服器設定：

      ```
      set deviceconfig system secure-proxy-server <FQDN_or_IP>
       set deviceconfig system secure-proxy-port <1-65535>
      ```

```
set deviceconfig system secure-proxy-user <value> set
deviceconfig system secure-proxy-password <value>
```

Proxy 伺服器密碼必須包含至少六個字元。

3. 使用下列 CLI 命令啟用 Proxy 伺服器，以向內嵌雲端服務伺服器傳送請求：

```
debug dataplane mica set inline-cloud-proxy enable
```

4. 使用下列 CLI 命令檢視內嵌雲端服務 Proxy 支援的目前運作狀態：

```
debug dataplane mica show inline-cloud-proxy
```

例如：

```
debug dataplane mica show inline-cloud-proxy 適用於已停用進階服務的 Proxy
```

STEP 9 | （建議）設定防火牆以停用用戶端擷取部分檔案內容，並在防火牆因偵測到惡意活動而終止原始工作階段後，停用啟動新工作階段以擷取檔案的剩餘內容。當網頁瀏覽器實作 HTTP Range 選項時，就會發生這種情況。雖然啟用 **Allow HTTP partial response**（允許 **HTTP** 進行部分回應）可提供最大可用性，但這也可能會增加網路攻擊成功的風險。Palo Alto Networks 建議停用 **Allow HTTP partial response**（允許 **HTTP** 進行部分回應）以享有最高安全性。

Allow HTTP partial response（允許 ***HTTP*** 進行部分回應）是全域設定，並且會影響使用 *RANGE* 標頭以 *HTTP* 為基礎的資料傳輸，進而可能導致某些應用程式的服務異常。停用 ***Allow HTTP partial response***（允許 ***HTTP*** 進行部分回應）後，請驗證業務關鍵型應用程式的運作情況。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Content-ID**（內容 **ID**） > **Content-ID Settings**（內容 **ID** 設定）。
2. 取消選取 **Allow HTTP partial response**（允許 **HTTP** 進行部分回應）並按一下 **OK**（確定）。

STEP 10 | **Commit**（提交）您的變更。

STEP 11 | （選用） 設定 Content Cloud FQDN 設定。

啟用進階 WildFire 內嵌 ML

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

您可以使用防火牆資料平面上的機器學習 (ML) 型分析，即時防止可攜式執行檔和 PowerShell 指令碼的惡意變體進入網路。利用安全性平台上的 WildFire® 雲端分析技術，進階 WildFire 內嵌 ML 會評估各種檔案詳細資料（包括解碼器欄位和模式），動態偵測指定類型的惡意檔案，以制訂高可能性的檔案分類。此保護擴展到威脅的當前未知變體及未來變體，這些威脅與 Palo Alto Networks 已確定為惡意的特徵相符。進階 WildFire 內嵌 ML 對現有防毒設定檔保護設定進行了補充。此外，您可以指定檔案雜湊例外狀況，以排除遇到的所有誤判，這使您能夠在設定檔中建立更細微的規則來滿足特定的安全需求。

若要啟用進階 WildFire 內嵌 ML，您必須具作用中的進階 WildFire 或 WildFire 訂閱，請建立（或修改）防毒（或用於 Prisma Access 的 WildFire 和防毒）安全性設定檔，以設定和啟用該服務，然後將防病毒設定檔附加到安全性政策規則。

進階 *WildFire* 內嵌 *ML* 目前在 *VM-50* 或 *VM50L* 虛擬設備上不受支援。

- Strata Cloud Manager
- PAN-OS 和 Panorama

啟用進階 WildFire 內嵌 ML（PAN-OS 和 Panorama）

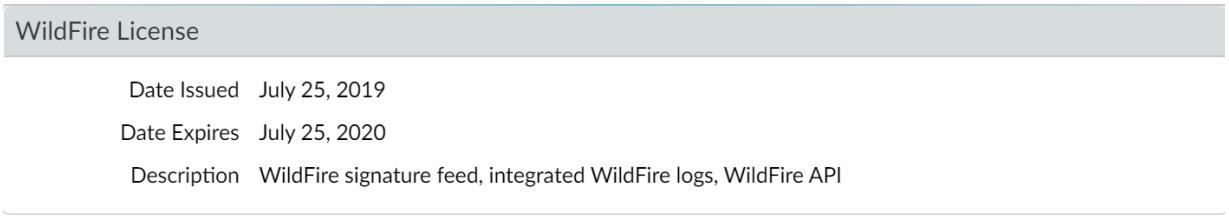
若要啟用 WildFire 內嵌 ML 設定，請將使用內嵌 ML 設定的防毒設定檔附加到安全性政策規則。

若要繞過進階 WildFire 內嵌 ML，您必須針對每個模型將 **Action Setting**（動作設定）設為 **disable**（停用，此項適用於所有協定），或使用部分雜湊建立 WildFire 內嵌 ML 檔案的例外狀況。請勿使用以 WildFire 內嵌 ML 威脅 ID 為基礎的特徵碼例外狀況設定您的防毒設定檔。這將導致防火牆封鎖從您網路到該 IP 位址的所有流量。

WildFire 內嵌 *ML* 目前在 *VM-50* 或 *VM50L* 虛擬設備上不受支援。

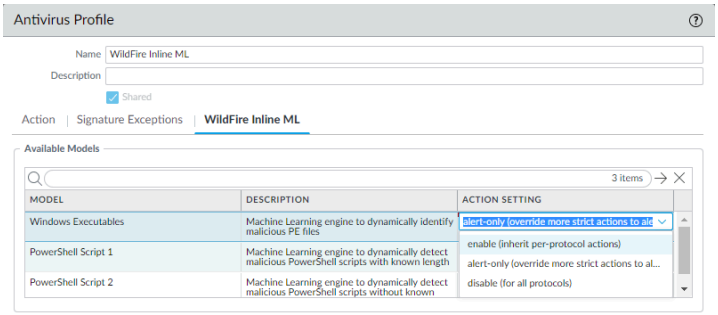
STEP 1 | 要利用 WildFire 內嵌 ML，您必須具有作用中的 WildFire 訂閱以分析 Windows 可執行檔。

確認您擁有 WildFire 訂閱。要確認當前哪些訂閱具有授權，請選取 **Device**（裝置） > **Licenses**（授權），並確認顯示了適當的授權且該授權沒有過期。



STEP 2 | 建立新的防毒安全設定檔或更新現有設定檔以使用即時 WildFire 內嵌 ML 模式。

1. 選取現有 **Antivirus Profile**（防毒設定檔）或建立一個新的（選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Antivirus**（防毒），然後 **Add**（新增）一個新的設定檔）。
2. 設定您的防毒設定檔。
3. 選取 **WildFire Inline ML**（**WildFire** 內嵌 **ML**）頁簽，並為每個 WildFire 內嵌 ML 模式套用 **Action Setting**（動作設定）。這會基於每個模式強制執行為每個通訊協定設定的 WildFire 內嵌 ML 動作設定。下列分類引擎可用：
   - Windows 可執行檔
   - PowerShell 指令碼 1
   - PowerShell 指令碼 2
   - 可執行檔連結格式（在安裝 PAN-OS 內容版本 8367 和更新版本時可用）
   - MSOffice（在安裝 PAN-OS 內容版本 8434 和更新版本時可用）
   - Shell 指令碼（在安裝 PAN-OS 內容版本 8543 和更新版本時可用）
   - OOXML（在安裝 PAN-OS 內容版本 11.1.3 和更新版本，以及 PAN-OS 內容版本 8825 和更新版本時可用）
   - Mach-O（在安裝 PAN-OS 內容版本 11.1.3 和更新版本，以及 PAN-OS 內容版本 8885-8930 和更新版本時可用）



可使用下列動作設定：

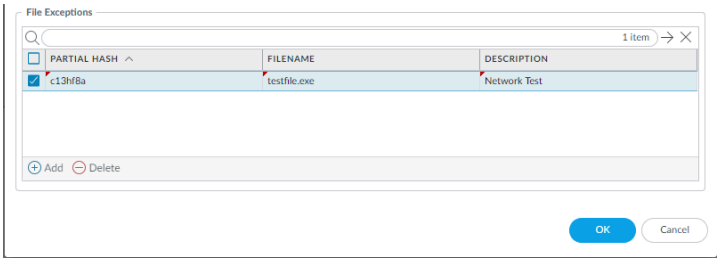
- 啟用（繼承每個通訊協定的動作）—WildFire 根據您在 **Action**（動作）頁簽的「解碼器」區段的「 WildFire 內嵌 ML 動作」欄中的選擇檢查流量。
- 僅警示（覆寫更嚴格的動作來發出警示）—WildFire 根據您在 **Action**（動作）頁簽的「解碼器」區段的「 WildFire 內嵌 ML 動作」欄中的選擇檢查流量，並覆寫嚴重性層級高於警示（丟棄、重設用戶端、重設伺服器、重設二者）警示的任何動作，允許流量通過，同時仍會產生警示並儲存在威脅日誌中。
- 停用（對於所有通訊協定）—WildFire 允許流量通過，而不採取任何原則動作。

4. 按一下 **OK**（確定）以退出防毒設定檔設定視窗並 **Commit**（提交）您的新設定。

STEP 3 | （選用）如果您遇到誤判，新增檔案例外狀況到您的防毒安全性設定檔。通常會為未將檔案轉送至 WildFire 進行分析的使用者執行此操作。您可以將檔案例外狀況詳細資料直接新增到例外狀況清單，或透過從威脅日誌指定檔案來新增。

如果您的 *WildFire* 分析安全性設定檔設定為轉送使用 *WildFire* 內嵌 *ML* 分析的檔案類型，誤判會在收到時自動更正。如果對於已被 *WildFire* 分析歸類為良性的檔案，仍然出現 *ml-virus* 警示，請聯絡 *Palo Alto Networks* 支援部門。

- 將檔案例外狀況直接新增到例外狀況清單。
  1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Antivirus**（防毒）。
  2. 選取您想要為其排除特定檔案的防毒設定檔，然後選取 **WildFire Inline ML**（**WildFire** 內嵌 **ML**）。
  3. 新增您想要從強制執行中排除的檔案的雜湊、檔案名稱和說明。



  4. 按一下 **OK**（確定）以儲存防毒設定檔，然後 **Commit**（提交）您的更新。
- 從威脅日誌項目新增檔案例外狀況。
  1. 選取 **Monitor**（監控） > **Logs**（日誌） > **Threat**（威脅），然後篩選 **ml-virus** 威脅類型的日誌。為您想要為其建立檔案例外狀況的檔案選取威脅日誌。
  2. 轉至 **Detailed Log View**（詳細日誌檢視）並向下捲動到 **Details**（詳細資料）面板，然後選取 **Create Exception**（建立例外狀況）。

  3. 新增 **Description**（說明），然後按一下 **OK**（確定）以新增檔案例外狀況。
  4. 新檔案例外狀況可在 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Antivirus**（防毒） > **WildFire Inline ML**（**WildFire** 內嵌 **ML**）下的 **File Exceptions**（檔案例外狀況）清單中找到。

STEP 4 | （選用）驗證防火牆到內嵌 ML 雲端服務的連線狀態。

在防火牆上使用以下 CLI 命令檢視連線狀態。

```
show mlav cloud-status
```

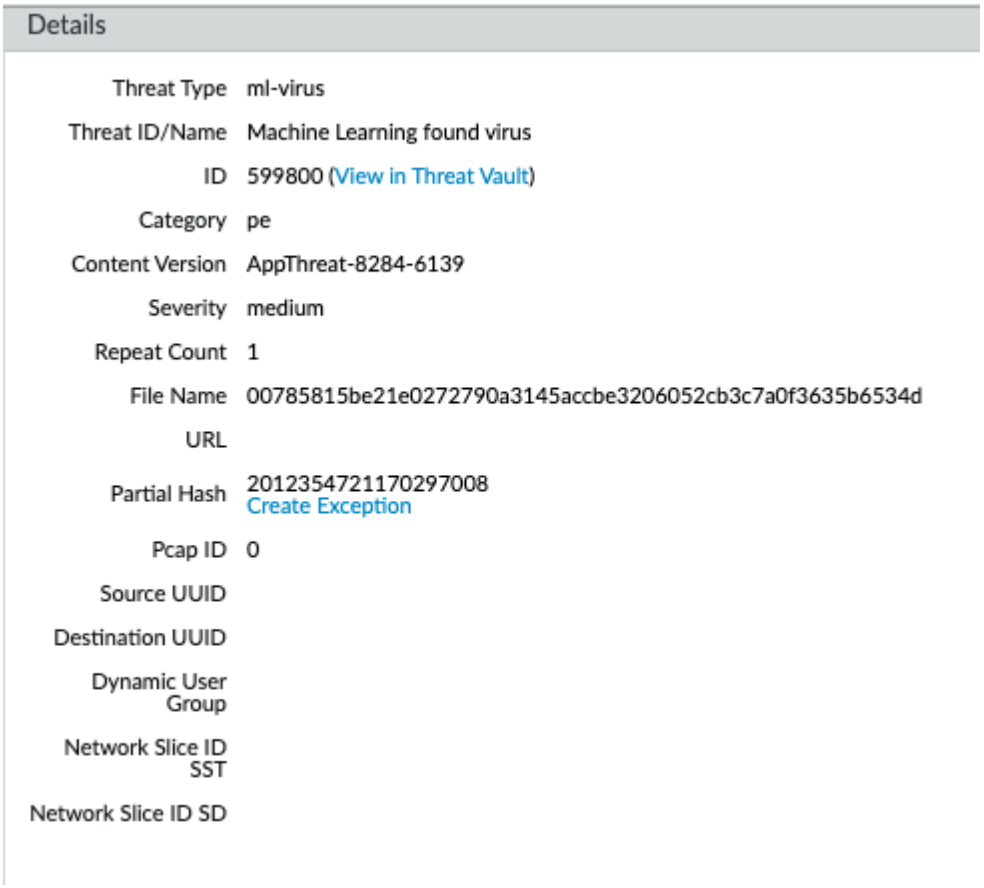
例如：

```
show mlav cloud-status MLAV cloud Current cloud server:
 ml.service.paloaltonetworks.com Cloud connection: connected
```

如果您無法連線至內嵌 ML 雲端服務，請確認以下網域未被封鎖：ml.service.paloaltonetworks.com。

STEP 5 | （選用） 設定 Content Cloud FQDN 設定。

要檢視有關使用 WildFire 內嵌 ML 偵測到的檔案的資訊，請檢查威脅日誌（**Monitor**（監控） > **Logs**（日誌） > **Threat**（威脅），然後從清單中選取日誌類型）。已使用 WildFire 內嵌 ML 分析的檔案標記有威脅類型 **ml-virus**：



啟用進階 WildFire 內嵌 ML (Cloud Management)

如果您使用 ***Panorama*** 管理 ***Prisma Access***：

請切換到 ***PAN-OS*** 頁籤並按照指示進行操作。

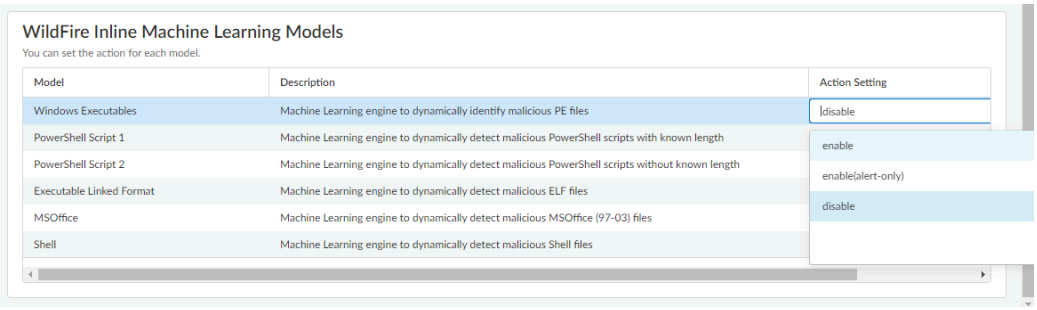
如果您使用 ***Prisma Access*** 雲端管理，請從此處繼續。

STEP 1 | 若要充分利用 WildFire 內嵌 ML，您的 Prisma Access 訂閱必須包含作用中的 WildFire 訂閱。

驗證您是否具有效且未過期的 WildFire 訂閱。

STEP 2 | 建立新的 **WildFire and Antivirus**（**WildFire** 和防毒）安全設定檔或更新現有設定檔，以使用即時 WildFire 內嵌 ML 模式。

1. 選擇現有 **WildFire and Antivirus**（**WildFire** 和防毒）安全設定檔或建立新的安全設定檔（選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全性服務） > **WildFire and Antivirus**（**WildFire** 和防毒）並 **Add Profile**（新增設定檔）。
2. 設定您的 WildFire 和防毒設定檔 以轉送範例進行分析。
3. 選擇 **WildFire Inline Machine Learning Models**（**WildFire** 內嵌機器學習模型） 並為每個 WildFire 內嵌 ML 模型套用 **Action Setting**（動作設定）。這會基於每個模式強制執行為每個通訊協定設定的 WildFire 內嵌 ML 動作設定。



下列分類引擎可用：

- Windows 可執行檔
- PowerShell 指令碼 1
- PowerShell 指令碼 2
- 可執行連結格式
- MSOffice
- Shell 指令碼
- 啟用—WildFire 會根據您在 **Action**（動作）頁籤「解碼器」區段的「WildFire 內嵌 ML 動作」欄中的選擇檢查流量。
- 啟用（僅警示）—WildFire 會根據您在 **Action**（動作）頁籤「解碼器」區段的「WildFire 內嵌 ML 動作」欄中的選擇檢查流量，並覆寫嚴重性層級高於警示（丟棄、重設用戶

端、重設伺服器、重設二者）警示的任何動作，如此一來才能允許流量通過，同時仍產生警示並將其儲存在威脅日誌中。

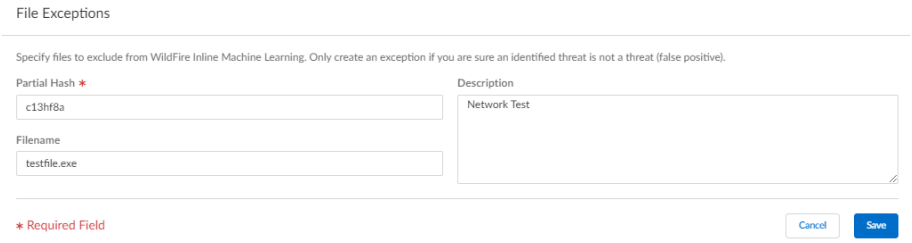
- 停用—WildFire 允許流量通過，無需任何政策動作。

STEP 3 | （選用）若您遇到誤判，請新增檔案例外狀況至 WildFire 和防毒安全設定檔。通常會為未將檔案轉送至 WildFire 進行分析的使用者執行此操作。您可以將檔案例外狀況詳細資料直接新增到例外狀況清單，或透過從威脅日誌指定檔案來新增。

如果您的 *WildFire* 分析安全性設定檔設定為轉送使用 *WildFire* 內嵌 *ML* 分析的檔案類型，誤判會在收到時自動更正。如果對於已被 *WildFire* 分析歸類為良性的檔案，仍然出現 *ml-virus* 警示，請聯絡 *Palo Alto Networks* 支援部門。

- 將檔案例外狀況直接新增到例外狀況清單。

1. 在 **File Exceptions**（檔案例外狀況）窗格中選擇 **Advanced Settings**（進階設定）和 **Add Exception**（新增例外狀況）。
2. 新增您想要從強制執行中排除的檔案的雜湊、檔案名稱和說明。



3. 完成後請 **Save**（儲存）您的檔案例外狀況。

STEP 4 | **Save**（儲存）您的 WildFire 和防毒設定檔設定並 推送設定變更。

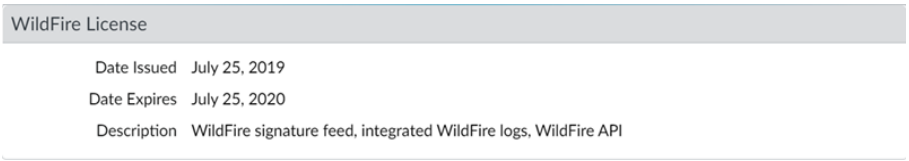
啟用即時特徵碼查閱的保留模式

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權

您可以設定 NGFW，在即時特徵碼雲端執行特徵碼查閱時保留範例傳輸。查閱完成後，系統會根據貴組織針對特定 WildFire 裁定的安全性政策，將檔案發佈（或封鎖）到要求的用戶端，進而防止已知惡意軟體進行初始傳輸。您可以針對每個防毒設定檔設定保留模式，並對特徵碼查閱逾時和相關動作套用全域設定。

所有具作用中 WildFire 或進階 WildFire 授權且執行 PAN-OS 11.0.2 或更新版本的使用者都可以使用此功能。

STEP 1 | 若要啟用 WildFire 即時特徵碼查閱的保留模式，您必須具 WildFire 或進階 WildFire 訂閱服務授權。請務必確認已於防火牆啟用授權。若要確認當前哪些訂閱具作用中的授權，請選取 **Device**（裝置） > **Licenses**（授權），並確認系統顯示正確授權且該授權未過期。以下範例為標準 WildFire 授權的說明。



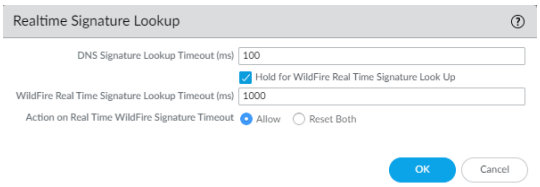
STEP 2 | 設定防火牆即時擷取 WildFire 特徵碼的排程。

即使防火牆已設定使用即時特徵碼，防火牆仍會定期安裝補充特徵碼套件。這可在您遇到連線問題時提供最新的特徵碼來源，並且可從本機提供特徵碼，從而提高速度。

1. 請選取 **Device**（裝置） > **Dynamic Updates**（動態更新）。
2. 針對 WildFire 更新請選取 **Schedule**（排程）。
3. 針對 **Real-time**（即時）更新設定 **Recurrence**（週期性）（防火牆檢查 Palo Alto Networks 更新伺服器是否有新特徵碼的頻率）。
4. 按一下 **OK**（確定）以儲存 WildFire 更新排程，然後 **Commit**（提交）您的變更。

STEP 3 | 若請求超過逾時時間，請設定逾時設定和動作。

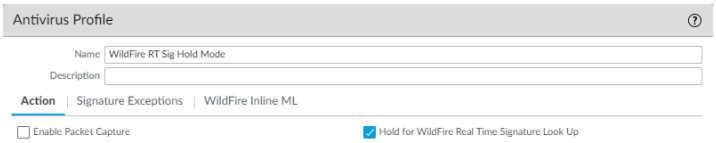
若要根據每個防毒設定檔啟用 *WildFire* 即時特徵碼查閱的保留模式，您必須先全域啟用保留模式。



1. 選擇 **Device Setup**（裝置設定） > **ContentID**（內容 **ID**） > **Realtime Signature Lookup**（即時特徵碼查閱）
2. 啟用 **Hold for WildFire Real Time Signature Look Up**（**WildFire** 即時特徵碼查閱保留模式）。
3. 以毫秒為單位，指定 **WildFire Real Time Signature Lookup Timeout (ms)**（**WildFire** 即時特徵碼查閱逾時 **(ms)**）（預設值為 1000）。

   除非您在測試過程多次逾時，否則 *Palo Alto Networks* 建議您使用預設值 *1000ms*。
4. 指定 **Action On Real Time WildFire Signature Timeout**（即時 **WildFire** 特徵碼逾時的動作）。預設為 **Allow**（允許），但 Palo Alto Networks 建議您在啟用保留模式時將其設為 **Reset-Both**（重設兩者）。選項包括以下內容：
   - 允許—當達到保留逾時閾值時，NGFW 允許封包通過。
   - 重設兩者#當達到保留逾時閾值時，NGFW 會重設用戶端和伺服器端的連線。
5. 完成後請選擇 **OK**（確定）。

STEP 4 | 請更新或建立新的防毒安全設定檔，以啟用 WildFire 即時特徵碼查閱的保留模式。



1. 選擇現有防毒安全設定檔，或 **Add**（新增）新的安全設定檔（**Objects**（物件） > **Security Profiles**（安全性設定檔） > **Antivirus**（防毒））。
2. 選擇您的防毒安全設定檔，然後前往 **Action**（動作）。
3. 選擇 **Hold for WildFire Real Time Signature Look Up**（保留 **WildFire** 即時特徵碼查閱）。
4. 若要為所有防毒設定檔啟用 WildFire 即時特徵碼查閱的保留模式，請重複 4.1-4.3 的步驟。

STEP 5 | **Commit**（提交）您的變更。

STEP 6 | （選用）您可以在防毒摘要檢視頁面上檢視防毒安全設定檔設定摘要，其中包括保留模式啟用。

2 items

					Decoders				WildFire Inline ML			
NAME	LOCATION	HOLD MODE	PACKET CAPTURE	PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION	MODEL	ACTION SETTING	SIGNATURE EXCEPTIONS	WILDFIRE INLINE ML EXCEPTIONS
default	Predefined			http	default (reset-both)	default (reset-both)	default (reset-both)	Windows Executables	enable (inherit per-protocol actions)	0	0
				http2	default (reset-both)	default (reset-both)	default (reset-both)	PowerShell Script 1	enable (inherit per-protocol actions)		
				smtp	default (alert)	default (alert)	default (alert)	PowerShell Script 2	enable (inherit per-protocol actions)		
				imap	default (alert)	default (alert)	default (alert)	Executable Linked Format	enable (inherit per-protocol actions)		
				pop3	default (alert)	default (alert)	default (alert)	MSOffice	enable (inherit per-protocol actions)		
				ftp	default (reset-both)	default (reset-both)	default (reset-both)	Shell	enable (inherit per-protocol actions)		
				smb	default (reset-both)	default (reset-both)	default (reset-both)				
WildFire Profile		✓		http	default (reset-both)	default (reset-both)	default (reset-both)	Windows Executables	disable (for all protocols)	0	0
				http2	default (reset-both)	default (reset-both)	default (reset-both)	PowerShell Script 1	disable (for all protocols)		
				smtp	default (alert)	default (alert)	default (alert)	PowerShell Script 2	disable (for all protocols)		
				imap	default (alert)	default (alert)	default (alert)	Executable Linked Format	disable (for all protocols)		
				pop3	default (alert)	default (alert)	default (alert)	MSOffice	disable (for all protocols)		
				ftp	default (reset-both)	default (reset-both)	default (reset-both)	Shell	disable		
				smb	default (reset-both)	default (reset-both)	default (reset-both)				

設定 Content Cloud FQDN 設定

這可在何處使用？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權

您可以指定 NGFW 使用的雲端內容完全合格網域名稱 (FQDN)，用於處理進階 WildFire 服務要求。預設 FQDN 連接至 hawkeye.services-edge.paloaltonetworks.com，然後解析為最近的雲端服務伺服器。您可以透過指定最能滿足資料落地和效能需求的區域雲端內容伺服器來取代自動伺服器選取。請謹記，雲端內容 FQDN 是全球使用的資源，會影響依賴於此連線的其他服務傳送流量有效負載的方式。

在某些情況下，雲端內容 *FQDN* 可能無法完全支援某些區域中的特定 *Palo Alto Networks* 產品功能。在變更雲端內容 *FQDN* 之前，請先驗證產品是否完全受到支援。

根據您所使用的服務，雲端內容 FQDN 有助於分析服務要求（包括流量負載），從而將資料傳送到所選區域中的伺服器。如果您指定了所在區域之外的內容雲端 FQDN（例如，如果您位於歐盟區域，但指定了亞太地區的 FQDN），則可能會違反貴組織的隱私權和法律規定。請參閱具體產品文件，以瞭解有關 Palo Alto Networks 產品如何使用雲端內容 FQDN 的資訊。

如果您遇到服務連線問題，請先驗證設定的雲端內容 *FQDN* 是否受到封鎖。

STEP 1 | 登入 PAN-OS 網頁介面。

STEP 2 | 選取（**Device**（裝置） > **Setup**（設定） > **Content-ID**（內容 **ID**） > **Content Cloud Settings**（內容雲端設定））並根據需求變更 FQDN：

- 預設—**hawkeye.services-edge.paloaltonetworks.com**
- 美國中部（美國愛荷華州）—**us.hawkeye.services-edge.paloaltonetworks.com**
- 歐洲（德國法蘭克福）—**eu.hawkeye.services-edge.paloaltonetworks.com**
- 亞太地區（新加坡）—**apac.hawkeye.services-edge.paloaltonetworks.com**
- 印度（孟買）—**in.hawkeye.services-edge.paloaltonetworks.com**
- 英國（英國倫敦）—**uk.hawkeye.services-edge.paloaltonetworks.com**
- 法國（法國巴黎）—**fr.hawkeye.services-edge.paloaltonetworks.com**
- 日本（日本東京）—**jp.hawkeye.services-edge.paloaltonetworks.com**
- 澳洲（澳洲雪梨）—**au.hawkeye.services-edge.paloaltonetworks.com**
- 加拿大（加拿大蒙特婁）—**ca.hawkeye.services-edge.paloaltonetworks.com**
- 瑞士—**ch.hawkeye.services-edge.paloaltonetworks.com**
- 荷蘭—**nl.hawkeye.services-edge.paloaltonetworks.com**
- 印尼—**id.hawkeye.services-edge.paloaltonetworks.com**
- 卡達—**qa.hawkeye.services-edge.paloaltonetworks.com**
- 臺灣—**tw.hawkeye.services-edge.paloaltonetworks.com**
- 波蘭—**pl.hawkeye.services-edge.paloaltonetworks.com**
- 韓國（韓國首爾）—**kr.hawkeye.services-edge.paloaltonetworks.com**
- 沙烏地阿拉伯—**sa.hawkeye.services-edge.paloaltonetworks.com**
- 義大利—**it.hawkeye.services-edge.paloaltonetworks.com**

STEP 3 | 按一下 **OK**（確定）。

驗證範例提交

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權

使用惡意軟體測試範例來測試部署，並確認防火牆已正確轉送檔案進行 WildFire 分析。

- 測試樣本惡意軟體檔案
- 確認檔案轉送

測試樣本惡意軟體檔案

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 或 WildFire 授權

Palo Alto Networks 提供惡意軟體檔案範例，可讓您用來測試進階 WildFire 設定。請採取下列步驟下載惡意軟體範例檔案，確認檔案已轉送進行進階 WildFire 分析，並參閱分析結果。

STEP 1 | 下載其中一個惡意軟體測試檔案。您可以選取 PE、APK、MacOSX 和 ELF。

> 下載加密 *WildFire* 樣本惡意軟體檔案之前，您必須在裝置 > 憑證管理 > ***SSL*** 解密排除頁面上暫時停用 **.wildfire.paloaltonetworks.com* 項目，以從解密清單中排除，否則無法正確下載樣本。進行確認測試後，務必重新啟用 *[SSL* 解密排除*]* 頁面上的 **.wildfire.paloaltonetworks.com* 項目。

- 如果您已在防火牆上啟用 SSL 解密，請使用下列其中一個 URL：
  - PE—https://wildfire.paloaltonetworks.com/publicapi/test/pe
  - APK—https://wildfire.paloaltonetworks.com/publicapi/test/apk
  - MacOSX—https://wildfire.paloaltonetworks.com/publicapi/test/macos
  - ELF—wildfire.paloaltonetworks.com/publicapi/test/elf
- 如果您沒有在防火牆上啟用 SSL 加密，請改為使用下列其中一個 URL：
  - PE—http://wildfire.paloaltonetworks.com/publicapi/test/pe
  - APK—http://wildfire.paloaltonetworks.com/publicapi/test/apk
  - MacOSX—http://wildfire.paloaltonetworks.com/publicapi/test/macos
  - ELF—wildfire.paloaltonetworks.com/publicapi/test/elf

測試檔案名稱為 wildfire-test-*file_type*-file.exe 且每個測試檔案擁有唯一的 SHA-256 雜湊值。

> 您也可以使用 *WildFire API* 擷取惡意軟體測試檔案。參閱 WildFire API 參考獲取詳細資訊。

STEP 2 | 在防火牆 Web 介面，選取 **Monitor**（監控） > **WildFire Submissions**（**WildFire** 提交） 以確認檔案已轉送進行分析。

請至少等待五分鐘，檔案的分析結果才會顯示在 **WildFire Submissions**（**WildFire** 提交）頁面上。測試檔案的裁定始終顯示為惡意軟體。

確認檔案轉送

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 或 WildFire 授權

將設定防火牆設為 轉送檔案進行進階 WildFire 分析 之後，請使用下列選項確認防火牆與進階 WildFire 公共 或 WildFire 私人雲端間的連線，並監控檔案轉送。

> 確認防火牆正在轉送範例進行分析的數個選項為 *CLI* 命令；如需深入瞭解 *CLI* 的入門及使用指南，請參閱 PAN-OS CLI 快速入門指南。

請確認連接至進階 WildFire 公共和/或私人雲端的防火牆連線狀態，包括由防火牆轉送進行分析的檔案總數。

使用 **`show wildfire status`** 命令：

- 請檢查防火牆連接的進階 WildFire 公共和/或 WildFire 私人雲端狀態。狀態 閒置 表示進階 WildFire 雲端（不論公共或私人）已就緒，可接收檔案進行分析。
- 確認防火牆轉送檔案的設定大小限制（**Device**（裝置） > **Setup**（設定） > **WildFire**）。
- 請監控檔案轉送，包括防火牆如何轉送全部檔案進行分析。如果防火牆處於 WildFire 混合型部署中，還會顯示轉送至 WildFire 公共雲端及 WildFire 私人雲端的檔案數目。

下列範例顯示防火牆在 WildFire 私人雲端部署中的 `show wildfire status` 輸出：

```
admin@VM-FW> show wildfire status

Connection info:
  Signature verification:            enable
  Server selection:                  enable
  File cache:                        enable
WildFire Public Cloud:
  Server address:                    wildfire.paloaltonetworks.com
  Status:                            Disabled due to configuration
  Best server:
  Device registered:                 no
  Through a proxy:                   no
  Valid wildfire license:            yes
  Service route IP address:          X.X.X.X
WildFire Private Cloud:
  Server address:                    X.X.X.X
  Status:                            Idle
  Best server:                       X.X.X.X:XXXXX
  Device registered:                 yes
  Through a proxy:                   no
  Valid wildfire license:            yes
  Service route IP address:          X.X.X.X
File size limit info:
  pe                                  9 MB
  apk                                 49 MB
  pdf                                 1000 KB
  ms-office                           9500 KB
  jar                                 9 MB
  flash                               10 MB
  MacOSX                              1 MB
Forwarding info:
  file idle time out (second):       90
  total concurrent files:            0
  Public Cloud:
    total file forwarded:            0
    file forwarded in last minute:   0
    concurrent files:                0
  Private Cloud:
    total file forwarded:            0
    file forwarded in last minute:   0
    concurrent files:                0
```

若只要檢視進階 WildFire 公共雲端或 WildFire 私人雲端的轉送資訊，請使用下列命令：

- **`show wildfire status channel public`**
- **`show wildfire status channel private`**

檢視防火牆根據檔案類型（包括電子郵件連結）轉送的範例。

使用此選項確認電子郵件連結已轉送進行分析，即使已啟用良性及灰色軟體範例日誌記錄，此後僅接收惡意或網路釣魚裁定的電子郵件連結會記錄為防火牆上的 ***WildFire Submissions***（***WildFire*** 提交）項目。這是為了針對良性電子郵件連結記錄 *WildFire* 提交項目的數量。

使用 **`show wildfire statistics`** 命令，確認轉送至進階 WildFire 公共或 WildFire 私人雲端的檔案類型：

- 該命令會顯示執行中防火牆的輸出，以及防火牆轉送進行分析的各檔案類型計數器。如果計數器欄位顯示 0，防火牆則不會轉送該檔案類型。
- 透過檢查下列計數器未顯示零，來確認電子郵件連結已轉送進行分析：
- `FWD_CNT_APPENDED_BATCH`—表示已新增至批次，並等待上傳至進階 WildFire 公共雲端或 WildFire 私人雲端的電子郵件連結數。
- `FWD_CNT_LOCAL_FILE`—表示已上傳至進階 WildFire 公共或 WildFire 私人雲端的電子郵件連結總數。

確認防火牆已轉送特定樣本，並檢查該樣本的狀態。

進行疑難排解時，此選項很有幫助，便於：

- 確認尚未接收裁定的範例已由防火牆正確轉送。由於 **WildFire Submissions**（**WildFire** 提交）只在分析完成且範例收到裁定時才會在防火牆上記錄，因此使用此選項可確認防火牆轉送的範例目前正在進行分析。
- 追蹤安全性政策允許，且符合 WildFire 分析設定檔，並轉送進行分析的單一檔案或電子郵件連結的狀態。
- 請確認混合型雲端部署的防火牆正在轉送正確的檔案類型及電子郵件連結至進階 WildFire 公共雲端或 WildFire 私人雲端。

在防火牆上執行下列 CLI 命令，檢視防火牆轉送進行分析的範例：

- 使用 CLI 命令 **debug wildfire upload-log** 檢視防火牆轉送的所有樣本。
- 使用 CLI 命令 **debug wildfire upload-log channel public**，僅檢視轉送至進階 WildFire 公共雲端的範例。
- 使用 CLI 命令 **debug wildfire upload-log channel private** 僅檢視 WildFire 私人雲端轉送的樣本。

下列範本顯示進階 WildFire 公共雲端部署中，在防火牆發出上述三項命令的輸出：

```
user@firewall> debug wildfire upload-log
+ channel   WildFire channel (Public/Private)
  |         Pipe through a command
  <Enter>   Finish input

user@firewall> debug wildfire upload-log channel private

Private Cloud upload logs:


user@firewall> debug wildfire upload-log channel public

Public Cloud upload logs:

    log: 0, filename: support-login.swf
    processed 353590 seconds ago, action: skipped - remote benign dup
    vsys_id:  1, session_id: 169651, transaction_id: 261
    file_len:  91536, flag: 0x81c, file type: flash
    threat id: 52145, user_id: 1238, app_id: 872
    from XX.XX.XX.XX/XXXX to XX.XXX.XXX.XXX/XXX
    SHA256: 6b2f1a23407ab2db9a17ccdf686bacc6dad7d2489c65ba90dbdf02508b3d4efd

    log: 1, filename: G2M_D_because_12.03.2014_300x250.swf
    processed 611505 seconds ago, action: skipped - remote benign dup
    vsys_id:  1, session_id: 259049, transaction_id: 260
    file_len:  39206, flag: 0x81c, file type: flash
    threat id: 52145, user_id: 20583, app_id: 872
    from XX.XX.XX.XX/XXXXX to XXX.XX.XXX.XXX/XX
    SHA256: cd52d1b7a7521a14237c1531edb109627fee084806a300d907b57322b1efd6e7
```

監控順利提交進行分析的範例。

使用防火牆 Web 介面，選取 **Monitor**（監控） > **Logs**（日誌） > **WildFire Submissions**（**WildFire** 提交）。防火牆轉送至進階 WildFire 公共或 WildFire 私人雲端進行分析的所有檔案將記錄在 WildFire 提交頁面。

- 檢查裁定範例：

  根據預設，僅接收惡意或網路釣魚裁定的範例會顯示為 **WildFire Submissions**（**WildFire** 提交）項目。若要為良性和/或灰色軟體樣本啟用日誌記錄，請選取 **Device**（裝置） > **Setup**（設定） > **WildFire** > **Report Benign Files/Report Grayware Files**（報告良性檔案/報告灰色軟體檔案）。

  啟用良性檔案的日誌記錄作為快速的疑難排解步驟，以確認防火牆正在轉送檔案。檢查 ***WildFire Submissions***（***WildFire*** 提交）日誌，確認系統正在轉送檔案進行分析並接收裁定（在此情況下為良性裁定）。

- 確認範例的分析位置：

  WildFire Cloud（**WildFire** 雲端）欄顯示轉送及分析檔案的位置。這在部署混合型雲端時很有用。

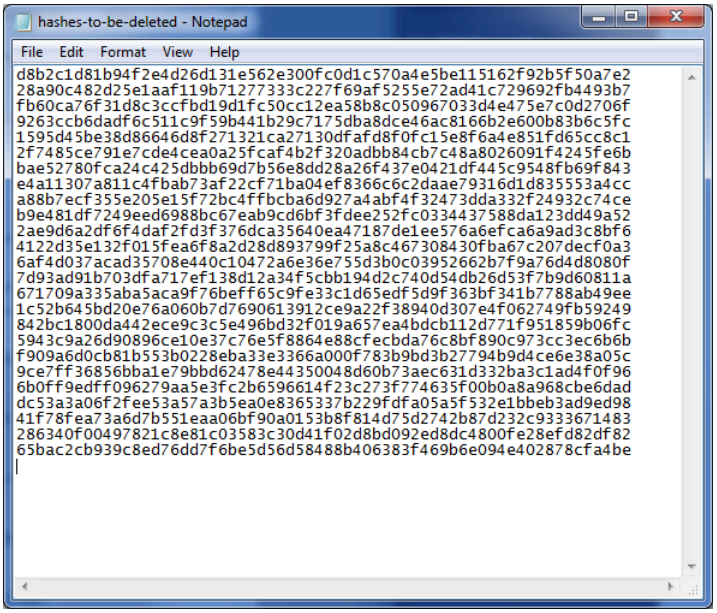
樣本移除請求

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

傳送至進階 WildFire 雲端進行分析的特殊範例可由使用者決定予以刪除。這讓遵守資料保護政策的使用者，包括必須遵守 GDPR 根據組織的保留原則永久清除樣本資料的那些使用者。樣本資料包括估作階段 / 上傳資料以及樣本檔案本身。

STEP 1 | 建立有被刪除的樣本 SHA256 或 MD5 雜湊表的文字檔。每個雜湊必須是在檔案中個別列可以包含最多 100 個樣本。

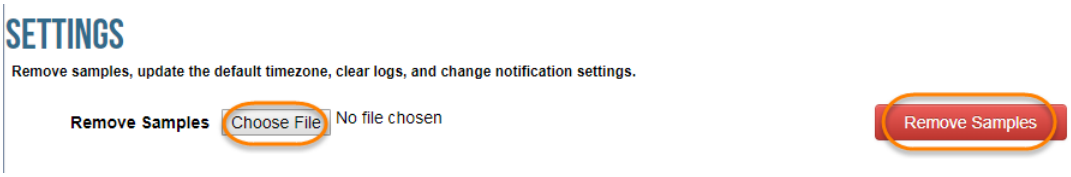
僅對於您的環境是特殊的檔案才可以被刪除。如果檔案被發現適用於其他公開或私人提供，僅指定帳戶的工作階段和上傳資料可以被移除。



STEP 2 | 請使用您的 Palo Alto Networks 支援憑證或 WildFire 帳戶登入 WildFire 入口網站。

STEP 3 | 在功能表列上選取 **Settings**（設定）。

STEP 4 | 點擊 選擇檔案並選擇您在步驟 1 建立的雜奏表文字檔，然後移除樣本。您將收到檔案上傳成功的確認。



STEP 5 | 從 WildFire 雲端移除樣本後，您將收到一封內容有要求細節的確認電子郵件。這包括被要求刪除的樣本清單和每個清單的移除狀態。程序可能需要 7 分鐘才會完成。

```
Dear WildFire customer,
your request for removal of samples from WildFire cloud has been completed. In total 1 samples were removed from WildFire,
the following table shows removal status for each individual sample hash

+------------------------------------------------------------------+---------+-------------------+
| Hash                                                             | Status  |      Information  |
+------------------------------------------------------------------+---------+-------------------+
|6d2ef9f79b5b81429cb1ffeebd6b2919a9a84ec0cc0e5023cbf45a68967c6e1c  | Deleted ||                   |
+------------------------------------------------------------------+---------+-------------------+
```

不存在或對您的環境而言不是特殊的樣本將返回到未發現的狀態並分別被退回。

依型號的防火牆檔案轉送容量

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series	❑ 進階 WildFire 授權

檔案轉送容量是指各 Palo Alto Networks 防火牆模型可提交檔案至進階 WildFire® 雲端或以進行分析的每分鐘速率上限。如果防火牆達到每分鐘上限，則對任何剩餘樣本排佇列。

下表的保留磁碟空間表示針對佇列檔案保留的防火牆磁碟空間。如果防火牆達到磁碟空間上限，則會取消轉送新檔案至 WildFire，直到佇列中有更多空間時。

防火牆可轉送檔案至進階 *WildFire* 雲端的速度也取決於來自防火牆的上傳連結頻寬。

平台	每分鐘檔案數上限	保留磁碟空間
VM-50	5	100MB
VM-100	10	100MB
VM-200	15	200MB
VM-300	25	200MB
VM-500	30	250MB
VM-700	40	250MB
PA-220	20	100MB
PA-400	20	100MB
PA-820	75	300MB
PA-850	75	300MB
PA-1400 系列	20	100MB
PA-3220	100	200MB
PA-3250/3260	100	500MB

平台	每分鐘檔案數上限	保留磁碟空間
PA-3400 Series	100	500MB
PA-5200 系列	250	1500MB
PA-5400 系列	250	1500MB
PA-7000 系列	300	1GB

監視活動

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

視您的 WildFire™ 部署（公共、私有或混合型雲端）而定，透過存取提交樣本的防火牆（或者如果集中管理多個防火牆，則為 Panorama），或使用 WildFire API，您可使用 WildFire 入口網站檢視提交至 WildFire 的樣本及每個樣本的分析結果。

WildFire 已分析一個樣本並傳遞其為惡意軟體、網路釣魚、灰色或良性的裁定，並已產生該樣本的詳細分析報告。在提交樣本的防火牆上檢視的 WildFire 分析報告還包括偵測樣本期間的工作階段詳細資訊。對於識別為惡意軟體的樣本，WildFire 分析報告包括關於現有 WildFire 特徵碼（可能與新識別的惡意軟體相關）的詳細資訊，以及表明樣本為惡意軟體的檔案屬性、行為及活動的相關資訊。

您也可以檢視進階 WildFire 如何與其他 Palo Alto Networks 應用程式和安全服務整合來保護貴組織免受威脅，並同時透過 Strata Cloud Manager 控管中心取得高階檢視以掌握您部署的整體運作健康情況。控管中心可作為您的 NetSec 首頁，並透過具有多個資料面向的互動式視覺化儀表板提供網路運作健康情況、安全性及效率的全面摘要，以便您輕鬆快速地進行評估。

根據產品平台，您可以存取高階儀表板，這些儀表板提供進階 WildFire 惡意軟體偵測統計資料和使用趨勢，其中包括以分析洞察等形式提供的網路活動脈絡。

Palo Alto Networks 提供多種方法監控進階 WildFire 活動：

- Strata Cloud Manager 控管中心
- 進階 WildFire 儀表板
- 關於 WildFire 日誌記錄與報告
- 設定 WildFire 提交日誌設定
- 使用 WildFire 入口網站監控惡意軟體
- WildFire 分析報告—消除
- 設定對於惡意軟體所發出的警示

關於 WildFire 日誌記錄與報告

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

您可以監視活動在防火牆、WildFire 入口網站、Strata Cloud Manager 或 WildFire API 上。

對於每個樣本 WildFire 分析，WildFire 在 WildFire 分析報告中，將樣本分類為惡意軟體、網路釣魚、灰色軟體或良性的 WildFire 分析報告，以及詳細說明樣本資訊及行為。在提交樣本的防火牆及分析樣本的 WildFire 雲端（公共或私人）上可找到 WildFire 分析報告，或者可通過 WildFire API 擷取：

- 在防火牆上—所有防火牆提交進行 WildFire 分析的樣本均記錄為 WildFire 提交項目。WildFire 提交日誌中的 Action（動作）欄表示防火牆是否允許或封鎖檔案。對於每個 WildFire 提交項目，您可以開啟詳細日誌檢視，檢視樣本的 WildFire 分析報告或下載 PDF 格式的報告。
- 在 WildFire 入口網站上—監控 WildFire 活動，包括每個樣本的 WildFire 分析報告，也可下載 PDF 格式的報告。在 WildFire 私人部署中，WildFire 入口網站提供手動上載至入口網站的樣本詳細資訊以及由啟用雲端智慧的 WildFire 設備提交的樣本。

  在入口網站上檢視 *WildFire* 分析報告的選項，僅支援啟用了雲端智慧功能的 *WildFire* 設備。

- 在 Strata Cloud Manager 上，所有由 Prisma Access 針對 WildFire 分析 提交的樣本均會記錄為 WildFire 日誌，並且可以透過 Strata Cloud Manager 日誌檢視器詳閱。您可以檢視流量詳細資訊、脈絡和其他相關詳細資訊，其中包括樣本如何透過您的網路進行的資訊。
- 帶 WildFire API—從 WildFire 設備或 WildFire 公共雲端擷取 WildFire 分析報告。

進階 WildFire 分析報告—關閉

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series	❑ 進階 WildFire 授權

我可以在哪裡使用這個？	我需要哪些內容？
• CN-Series	

在防火牆、WildFire 入口網站及 WildFire API 上存取進階 WildFire 分析報告。

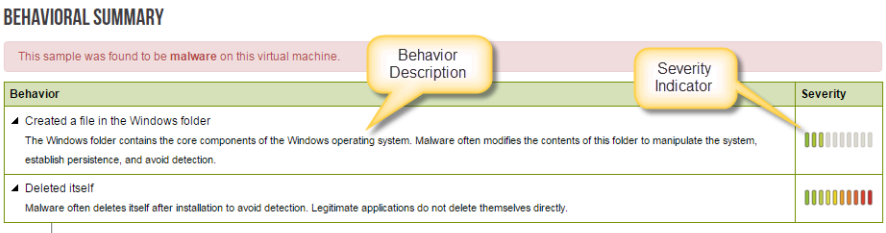
進階 WildFire 分析報告顯示詳細的範例資訊、目標使用者、電子郵件標頭資訊（若啟用）、傳遞檔案的應用程式，以及用於檔案命令和控制活動的所有 URL。根據負責轉送檔案的防火牆上所設工作階段資訊，以及觀測到的檔案行為，進階 WildFire 報告會包含下列表格所述的部分或全部資訊。

檢視檔案（不論手動或透過 *WildFire API* 上傳到 *WildFire* 入口網站）的進階 *WildFire* 報告時，由於流量不會周遊防火牆，報告不會顯示工作階段資訊。例如，報告不會顯示攻擊者/來源和受害者/目的地。

報告標題	說明

檔案資訊	• **File Type**（檔案類型）—Flash、PE、PDF、APK、JAR/Class、歸檔、Linux、指令碼或 MS Office。此欄位針對 HTTP/HTTPS 電子郵件連結報告命名為 URL，且會顯示所分析的 URL 名稱。
	• **File Signer**（檔案簽署者）—為了驗證而簽署檔案的實體。
	• **Hash Value**（雜湊值）—檔案雜湊相當於識別檔案的指紋，能夠確保檔案未經過任何形式的修改。以下列出 WildFire 針對每個已分析檔案產生的雜湊版本：
	  • **SHA-1**—顯示檔案的 SHA-1 值。
	  • **SHA-256**—顯示檔案的 SHA-256 值。
	  • **MD5**—顯示檔案的 MD5 資訊。
	• **File Size**（檔案大小）—WildFire 所分析檔案的大小（位元組）。
	• **First Seen Timestamp**（首次檢視時間戳記）—如果 WildFire 系統先前已分析過該檔案，則這是第一次觀察該檔案的日期/時間。
	• **Verdict**（裁定）—顯示分析裁定。
	• **Sample File**（樣本檔案）—按一下 **Download File**（下載檔案）連結將樣本檔案下載至您的本機系統。請注意，您僅可下載具惡意軟體裁定而非良性裁定的檔案。

報告標題	說明
涵蓋狀態	按一下**Virus Total (**總病毒數**)**連結檢視其他廠商已識別樣本的端點防毒涵蓋資訊。如果任何列出的廠商先前不曾發現該檔案，將顯示找不到檔案。 此外，當報告在防火牆上呈現時，特徵碼的最新資訊以及 Palo Alto Networks 目前為防護威脅所提供的 URL 過濾涵蓋情況也會一併在此區段中顯示。由於資訊以動態方式擷取，因此將不會顯示在 PDF 報告中。 下列涵蓋資訊針對使用中的特徵碼所提供： • **Coverage Type**（涵蓋類型）—Palo Alto Networks 提供的防護類型（病毒、DNS、WildFire 或惡意軟體 URL）。 • **Signature ID**（特徵碼 **ID**）—指派給 Palo Alto Networks 提供的每個特徵碼的唯一 ID。 • **Detail**（詳細資料）—病毒的已知名稱。 • **Date Released**（發行日期）—Palo Alto Networks 發行涵蓋範圍以防護惡意軟體的日期。 • **Latest Content Version**（內容版本）—提供惡意軟體防護所發行內容的版本號碼。
工作階段資訊	在流量周遊轉送樣本的防火牆時，包含以流量為基礎的工作階段資訊。若要定義 WildFire 將在報告中包含的工作階段資訊，請選取 **Device**（裝置）> **Setup**（設定）> **WildFire** > **Session Information Settings**（工作階段資訊設定）。 以下為可用選項： • 來源 IP • 來源連接埠 • 目的地 Ip • 目的地連接埠 • 虛擬系統（如果在防火牆上設定 multi-vsys） • 應用程式 • 使用者（如果在防火牆上設定 User-ID） • URL • FileName • 電子郵件寄件者

報告標題	說明
	• 電子郵件收件者 • 電子郵件主旨 預設情況下，工作階段資訊包含欄位狀態，其表示防火牆是否已允許或封鎖樣本。
動態分析	如果檔案的風險較低，且能夠經 WildFire 輕鬆判定為安全檔案，則僅在檔案上執行靜態分析，而非動態分析。 執行動態分析時，該區段包含各種標籤，顯示執行範例的每種環境類型的分析結果。例如，虛擬機器 4 標籤可能會顯示操作 Windows 7、Adobe Reader 11、Flash 11 和 Office 2010 的分析環境。 在 *WildFire* 設備上，僅會使用一部虛擬電腦來進行分析，該虛擬電腦根據最適合本機環境的分析環境屬性所選取。例如，如果大多數的使用者使用的是 *Windows 7 32* 位元，則會選取該類虛擬電腦。
行為摘要	每個 [Virtual Machine（虛擬電腦）] 頁籤會摘要顯示樣本檔案在特定環境中的行為。例如是否建立或修改樣本、開始程序、產生大量新程序、修改登錄或安裝瀏覽器協助程式物件。 嚴重性欄表示每個行為的嚴重性。嚴重性量表會顯示一列來表示低嚴重性，嚴重性等級提高則會顯示額外的列。此資訊也會新增至動態及靜態分析區段。  以下說明各種分析行為： • **Network Activity**（網路活動）—顯示樣本所執行的網路活動，例如存取網路上的其他主機、DNS 查詢，以及回撥活動。在此會提供可下載封包擷取的連結。 • **Host Activity (by process)**（主機活動（依照流程））—列出在主機上執行的活動，例如設定、修改或刪除的登錄機碼。

報告標題	說明
	• **Process Activity**（程序活動）—列出開始上層程序的檔案、程序名稱和程序執行的動作。 • **File**（檔案）—列出開始子程序的檔案、程序名稱和程序執行的動作。 • **Mutex**—如果樣本檔案產生其他程式執行緒，則將在此欄位中記錄 mutexname 與上層程序。 • **Activity Timeline**（活動時間軸）—逐一列出該樣本所有已記錄的活動。這有助於瞭解分析期間所發生事件的順序。 活動時間軸僅以 *PDF* 版的 *WildFire* 匯出報告形式提供。
提交惡意軟體	使用此選項來手動提交樣本至 Palo Alto Networks。若 WildFire Cloud 判斷樣本為惡意檔案，將重新分析樣本並產生特徵碼。在缺少產生特徵碼或未啟用雲端智慧的 WildFire 設備上，這相當實用；雲端智慧的用途為從設備將惡意軟體轉送至 WildFire 雲端。
報告不正確裁定	如果您認為裁定為誤判或漏報，可按一下此連結將樣本提交至 Palo Alto Networks 威脅團隊。威脅團隊會對該樣本執行進一步分析，判定樣本是否應重新分類。如果將惡意軟體樣本判定為安全，則在近期的防毒特徵碼更新中將停用該檔案的特徵碼，如果將良性檔案判定為惡意，則會產生新的特徵碼。調查完成後，您將收到說明已採取動作的電子郵件。

設定 WildFire 提交日誌設定

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權

WildFire 提交日誌是一個自動產生並附有時間戳記的檔案，當 Palo Alto Networks 網路安全平台根據 WildFire 分析設定檔設定 （物件 > 安全性設定檔 > WildFire 分析）將範例（檔案和電子郵件連結）轉送到 WildFire 雲端進行分析時，此檔案即會提供稽核線索來追蹤事件。每一轉送至 WildFire 雲端，且完成靜態和/或動態分析的範例皆有 WildFire 提交日誌項目。WildFire 提交日誌項目包括對範例採取的動作（允許或封鎖）、透過 WildFire 分析的裁定、範例的嚴重性等級和其他詳細資訊。

根據預設，系統會為良性和惡意範例建立 WildFire 提交日誌；而灰色軟體和良性範例則不產生日誌。您可以變更 WildFire 提交日誌設定，納入灰色軟體和良性範例，以及電子郵件連結所包含的其他工作階段資訊。

啟用 **WildFire Submissions**（**WildFire** 提交）日誌的下列選項

- 啟用良性及灰色樣本的日誌記錄
- 在 WildFire 日誌及報告中包含電子郵件標頭資訊

啟用良性及灰色樣本的日誌記錄

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權

良性及灰色樣本的日誌記錄預設為停用。不記錄接收良性或灰色裁定的電子郵件連結。

STEP 1 | 選取 **Device**（裝置） > **Setup**（設定） > **WildFire**，編輯 **General Settings**（一般設定）。

STEP 2 | 選取 **Report Benign Files**（報告良性檔案）及/或 **Report Grayware Files**（報告灰色檔案），然後按一下 **OK**（確定）以儲存設定。

在 WildFire 日誌及報告中包含電子郵件標頭資訊

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權

使用下列步驟在 WildFire 日誌及報告中包含電子郵件標頭資訊：電子郵件寄件者、電子郵件收件者及主旨。

工作階段資訊以及樣本將轉送至 WildFire 雲端，且用於產生 WildFire 分析報告。防火牆及 WildFire 雲端皆不接收、儲存或檢視實際電子郵件內容。

工作階段資訊可幫助您快速追蹤並修復在電子郵件附件或連結中偵測到的威脅，包括如何識別已下載或存取惡意內容的收件者。

STEP 1 | 選取 **Device**（裝置） > **Setup**（設定） > **WildFire**。

STEP 2 | 編輯 Session Information Settings（工作階段資訊設定）區段並啟用一或多個選項 (**Email sender**（電子郵件寄件者）、**Email recipient**（電子郵件收件者）和 **Email subject**（電子郵件主旨）)。

STEP 3 | 按一下 **OK**（確定）儲存。

設定對於惡意軟體所發出的警示

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權

您可以設定 Palo Alto Networks 防火牆在 WildFire 識別惡意或網路釣魚樣本後傳送警示。您也可以針對良性及灰色檔案設定警示，但無法針對良性及灰色電子郵件連結設定。此範例說明如何設定電子郵件警示；不過，您也可以將日誌轉送設為將警示做為系統日誌訊息、SNMP 陷阱或 Panorama 警示來傳遞。

STEP 1 | 設定電子郵件伺服器設定檔。

1. 選取 **Device**（裝置） > **Server Profiles**（伺服器設定檔） > **Email**（電子郵件）。
2. 按一下 **Add**（新增），然後輸入設定檔的 **Name**（名稱）。例如，WildFire-Email-Profile。
3. （選用）從 **Location**（位置）下拉式清單選取套用此設定檔的虛擬系統。
4. 按一下**Add**（新增） 新增電子郵件伺服器項目，並輸入連接簡易郵件傳輸通訊協定（SMTP）伺服器的必要資訊，然後傳送電子郵件（最多可在設定檔中新增四個電子郵件伺服器）：
   - **Server**（伺服器）—用來識別郵件伺服器的名稱（1-31 個字元）。此欄位只是頁籤，無須成為現有 SMTP 伺服器的主機名稱。
   - **Display Name**（顯示名稱）—顯示在電子郵件 [寄件者] 欄位的名稱。
   - **From**（寄件者）—傳送通知電子郵件的電子郵件地址。
   - **To**（收件者）—傳送通知電子郵件的目標電子郵件地址。
   - 其他收件者—輸入將通知傳送給第二位收件人的電子郵件地址。
   - **Gateway**（閘道）—用來傳送電子郵件的 SMTP 閘道 IP 位址或主機名稱。
5. 按一下 **OK**（確定）來儲存伺服器設定檔。
6. 按一下 **Commit**（交付），將變更儲存至執行中的設定。

STEP 2 | 測試電子郵件伺服器設定檔。

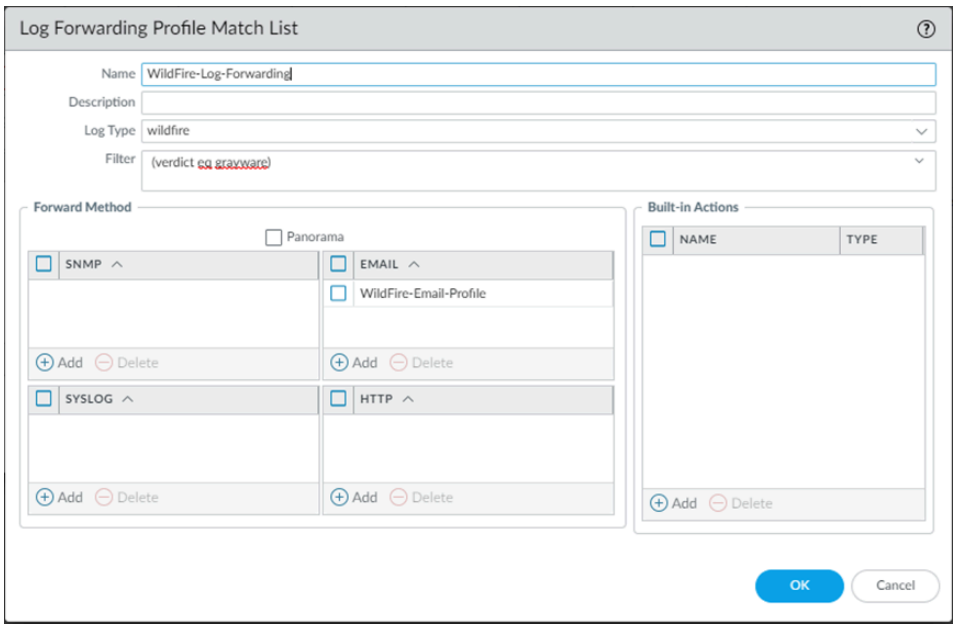
1. 選取 **Monitor**（監控） > **PDF Reports**（**PDF** 報告） > **Email Scheduler**（電子郵件排程器）。
2. 按一下 **Add**（新增），並且從 **Email Profile**（電子郵件設定檔）下拉式清單中選取新的電子郵件設定檔。
3. 按一下 **Send test email**（傳送測試電子郵件）按鈕，應該會有測試電子郵件傳送到電子郵件設定檔中定義的收件人。

STEP 3 | 設定日誌轉送設定檔以將 WildFire 日誌轉送至 Panorama、電子郵件帳戶、SNMP、syslog 伺服器以及作為 HTTP 要求轉送。

在此範例中，您將在樣本被判定為惡意軟體時設定電子郵件日誌。您也可以轉送良性及灰色日誌，這會在您測試時產生更多活動。

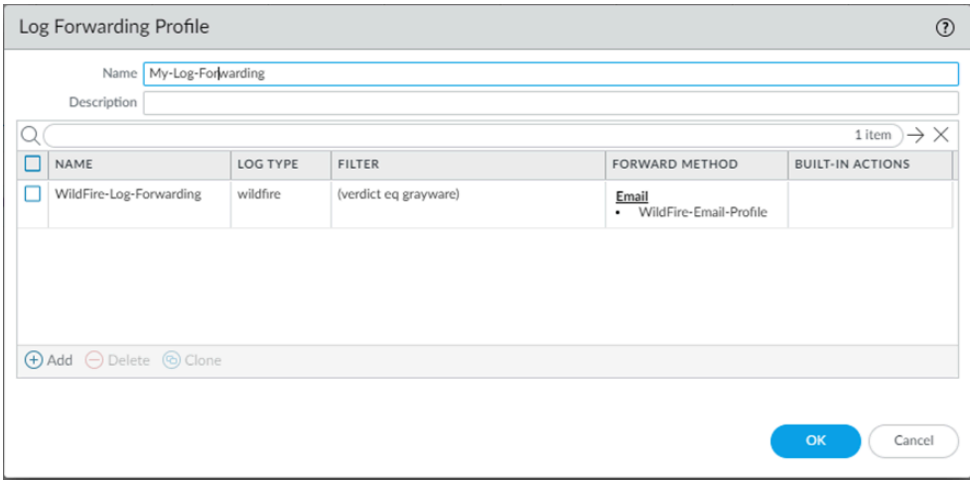
防火牆不會轉送封鎖檔案的 *WildFire* 日誌到電子郵件帳戶。

1. 選取 **Objects**（物件） > **Log Forwarding**（日誌轉送）。
2. **Add**（新增）設定檔並為其命名，例如 WildFire-Log-Forwarding。您也可以新增日誌轉送設定檔的 **Description**（說明）。
3. **Add**（新增）以設定轉送方法。



1. 提供 **Log Fowarding Profile Match List**（日誌轉送設定檔比對清單）的名稱。
2. 選取 **Wildfire** 日誌類型。
3. 使用 **(verdict eq malicious)** 查詢 **Filter**（篩選）日誌。
4. 在 **Forward Method**（轉送方法）選項下，選擇步驟 1 中建立的電子郵件設定檔（在此範例中為 WildFire-Email-Profile），然後按一下 **OK**（確定）以儲存比對清單更新。

4. 再按一下 **OK**（確定）以儲存日誌轉送設定檔更新。



STEP 4 | 將日誌轉送設定檔新增至用於 WildFire 轉送（附加 WildFire 分析設定檔）的安全性原則。

WildFire 分析設定檔會定義防火牆轉送進行進階 WildFire 分析的流量。若要設定 WildFire 分析設定檔並將其附加到安全性政策規則，請參閱 轉送檔案進行進階 WildFire 分析。

1. 選取 **Policies**（原則） > **Security**（安全性），並按一下用於 WildFire 轉送的原則。
2. 在 **Log Setting**（日誌設定）部分的 **Actions**（動作）頁籤中，選取您設定的 **Log Forwarding**（日誌轉送）設定檔。
3. 按一下 **OK**（確定）儲存變更，然後 **Commit**（交付）設定。

檢視 WildFire 日誌和分析報告

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

WildFire 日誌包含上傳到 WildFire 雲端進行分析的範例（檔案和電子郵件連結）的資訊。其中包括構件，也就是與日誌事件相關的屬性、活動或行為，例如攻擊者的應用程式類型或 IP 位址。除此之外也有 Wildfire 特定的品質，例如高層分析結果，包括將範例判別為惡意軟體、網路釣魚、灰色軟體或良性軟體，並詳述範例資訊。透過檢閱 WildFire 提交日誌，您也可瞭解您網路中的使用者是否下載可疑檔案。WildFire 分析報告會顯示詳細的範例資訊、目標使用者、電子郵件標頭資訊（若啟用）、傳遞檔案的應用程式，以及用於檔案命令和控制活動的所有 URL。它會通知您檔案是否有惡意、它是否修改登錄機碼、讀取/寫入至檔案、已建立新檔案、已開啟網路通訊通道、已導致應用程式損毀、已產生大量程序、已下載檔案，或已出現其他惡意行為。

WildFire 日誌會在 NGFW 防火牆上顯示為 WildFire 提交日誌，而在雲端管理平台上，您必須先設定日誌轉送，將相關日誌上傳至 Strata Logging Service，然後將 WildFire 日誌顯示為威脅日誌（類型 WildFire）。

- Strata Cloud Manager
- PAN-OS 和 Panorama

檢視 WildFire 日誌和分析報告（PAN-OS 和 Panorama）

防火牆提交進行 WildFire 分析的樣本做為項目顯示於防火牆 Web 介面上的 **WildFire Submissions (WildFire 提交)**日誌中。對於每個 WildFire 項目，您可以開啟顯示日誌詳細資訊的展開日誌檢視以及該樣本的 WildFire 分析報告。

Mozilla Firefox 使用者：*WildFire* 分析報告僅在 *Firefox v54* 及更早版本中正確顯示。如果您在檢視報告時遇到問題，請考慮使用其他網頁瀏覽器，例如 *Google Chrome* 瀏覽器。或者，您可以下載並開啟 *PDF* 版本或透過 *WildFire* 入口網站檢視報告。

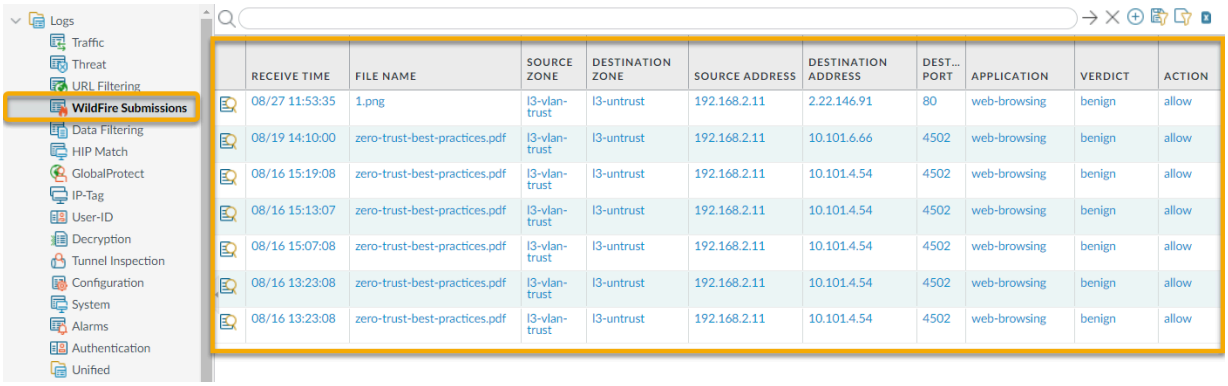
STEP 1 | 轉送檔案進行進階 WildFire 分析.

STEP 2 | 設定 WildFire 提交日誌設定。

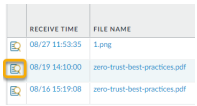
STEP 3 | 若要檢視透過防火牆提交至 WildFire 公共、私有或混合型雲端的樣本，請選取 **Monitor**（監控）> **Logs**（日誌）> **WildFire Submissions**（**WildFire** 提交）。WildFire 完成樣本分析後，結果將傳回提交該樣本防火牆，且可在 WildFire 提交日誌中存取。提交日誌包含指定樣本的詳細資料，包括下列資訊：

- 裁定列指明樣本為良性、惡意、網路釣魚或灰色。
- 動作列表示防火牆允許還是封鎖樣本。
- 「嚴重性」欄透過下列值表示樣本對組織的影響程度：重大、高、中、低及資訊。

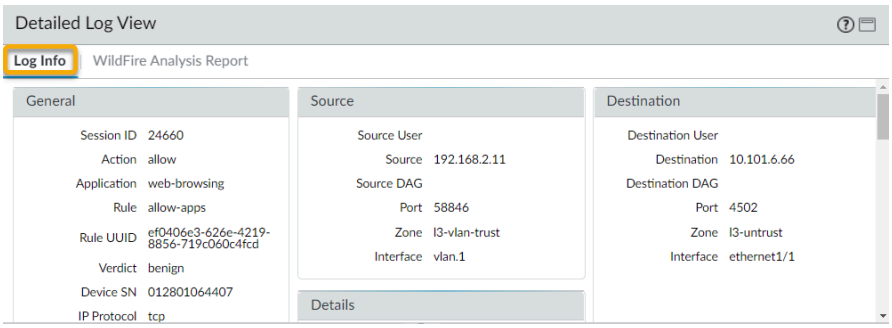
  下列嚴重性值由裁定值和動作值共同確定。
  - 低 - 動作設定為允許的灰色樣本。
  - 高 - 動作設定為允許的惡意樣本。
  - 資訊：
    - 動作設定為允許的良性樣本。
    - 動作設定為封鎖的任何裁定樣本。



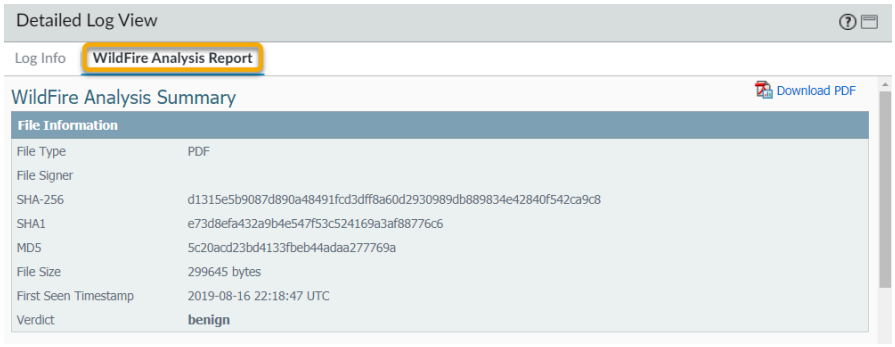
STEP 4 | 對於任何項目，選取 Log Details（日誌詳細資訊）圖示，即可開啟每個項目的詳細日誌檢視：



詳細日誌檢視顯示每個項目的 Log Info（日誌資訊）及 WildFire Analysis Report（WildFire 分析報告）。如果防火牆啟用了封包擷取 (PCAP)，亦會顯示樣本 PCAP。



對於所有樣本，WildFire 分析報告將顯示檔案及工作階段詳細資訊。對於惡意軟體樣本，WildFire 分析報告將會展開，包含表明檔案為惡意的檔案屬性及行為詳細資訊。



STEP 5 | （選用）**Download PDF**（下載 **PDF**） 版本的 WildFire 分析報告。

檢視 WildFire 日誌和分析報告 (Cloud Management)

若您使用 ***Panorama*** 來管理 ***Prisma Access***，您可以按照以下程序存取 *Prisma Access* 的內容，或切換到 ***PAN-OS*** 頁籤，按照其中指示進行操作。

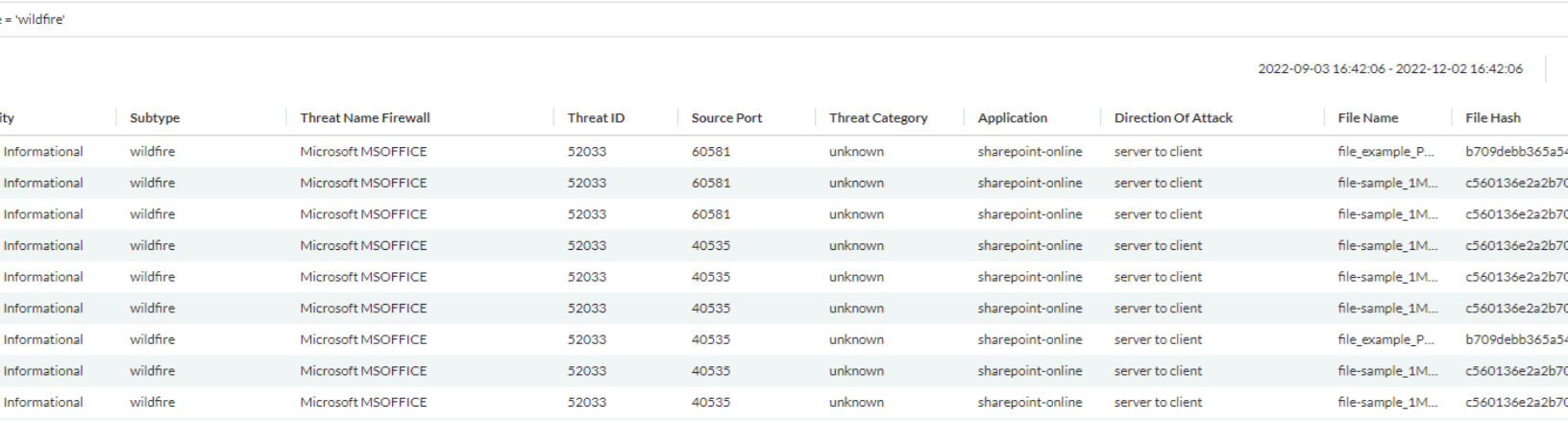
STEP 1 | 使用與您的 Palo Alto Networks 支援帳戶相關聯的認證，並登入中樞上的 Strata Cloud Manager 應用程式。

如需詳細瞭解如何使用 活動，請參閱 日誌檢視器。

STEP 2 | 篩選威脅日誌，在 Prisma Access 中顯示您的 WildFire 範例提交。

1. 選取 **Incidents and Alerts**（事件和警示）> **Log Viewer**（日誌檢視器）。
2. 將要搜尋的日誌類型變更為 **Threat**（威脅）。
3. 透過用於顯示使用查詢建立器的 WildFire 範例提交的 WildFire 子類型，來建立搜尋篩選器。例如，您可以使用 `sub_type.value = 'wildfire'` 來檢視 WildFire 日誌。根據需要調整搜尋條件，包括其他查詢參數（例如嚴重性級別和動作）以及日期範圍。

   若要檢視 *WildFire* 分析報告，您必須先登入 *WildFire* 入口網站並使用雜湊值或檔名來擷取報告檔案。如需詳細資訊，請參閱在 WildFire 入口網站上檢視報告。

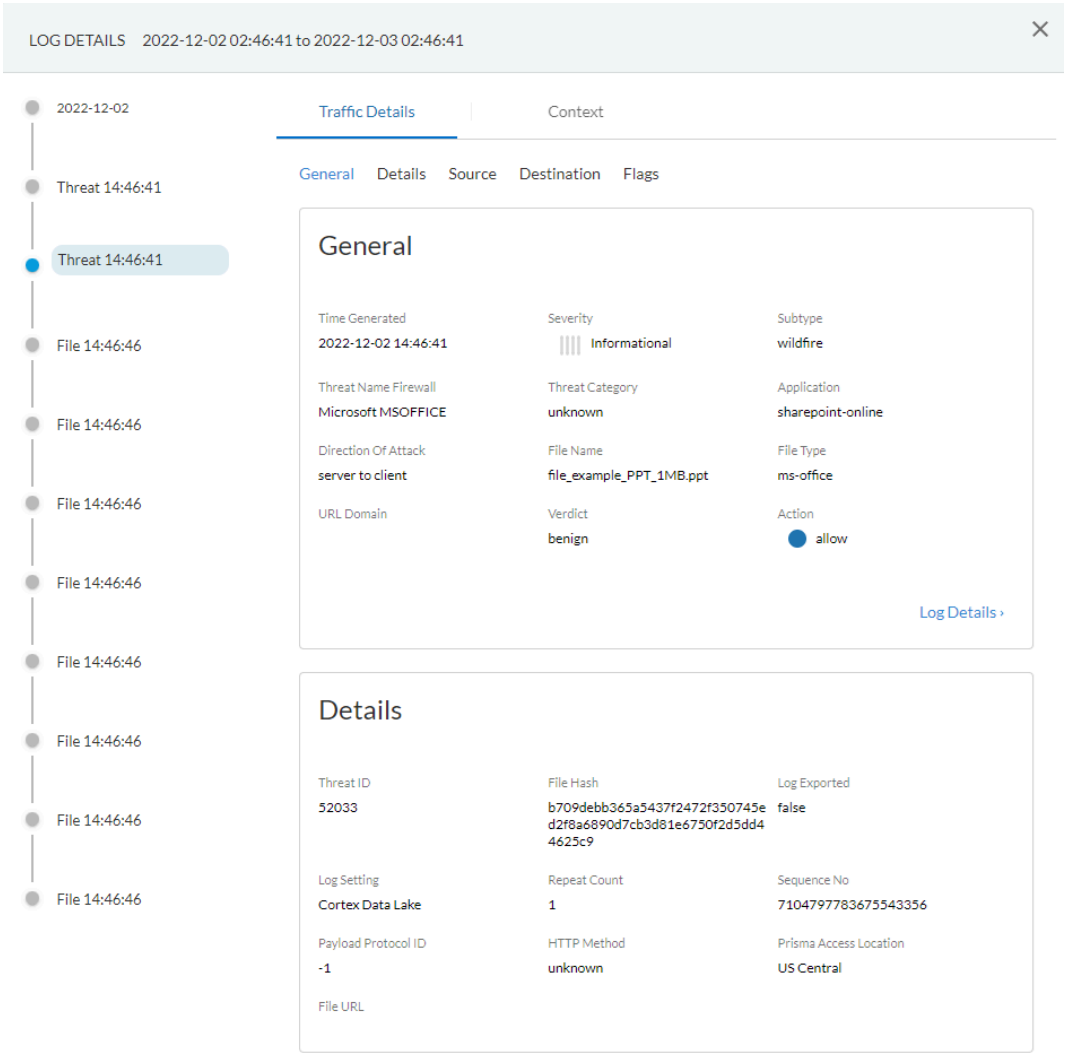


= 'wildfire'

2022-09-03 16:42:06 - 2022-12-02 16:42:06

ity	Subtype	Threat Name Firewall	Threat ID	Source Port	Threat Category	Application	Direction Of Attack	File Name	File Hash
Informational	wildfire	Microsoft MSOFFICE	52033	60581	unknown	sharepoint-online	server to client	file_example_P...	b709debb365a5
Informational	wildfire	Microsoft MSOFFICE	52033	60581	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	60581	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file_example_P...	b709debb365a5
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70

4. 篩選器設定完成後執行查詢。
5. 從結果選擇一個日誌項目，查看日誌詳細資訊。
6. 威脅日誌 **Subtype**（子類型）會與範例其他相關資訊一起顯示在 **General**（一般）窗格。威脅的其他相關詳細資訊會顯示在相應視窗。



使用 WildFire 入口網站監控惡意軟體

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

使用您的 Palo Alto Networks 支援認證或 WildFire 帳戶登入 Palo Alto Networks WildFire 入口網站。入口網站會開啟並顯示儀表板，列出所有防火牆的摘要報告資訊，這些防火牆與特定 WildFire 使用授權或支援帳戶相關。入口網站將針對每個列出的設備顯示偵測到的惡意軟體樣本數、已分析的良性樣本數和等待分析的擱置檔案數這三項統計資料。您的 WildFire 入口網站帳戶顯示由連接至 WildFire 公共雲端的網路上的防火牆提交的所有樣本的資料，以及手動提交至入口網站的樣本資料。此外，如果您已啟用 WildFire 設備來轉送惡意軟體至 WildFire 公共雲端以產生及散佈特徵碼，則也可以在入口網站上存取這些惡意軟體樣本的報告。

請參閱下列章節，瞭解如何使用 WildFire 入口網站監控 WildFire 項目的詳細資訊：

- 設定 WildFire 入口網站設定
- 新增 WildFire 入口網站使用者
- 在 WildFire 入口網站上檢視報告

設定 WildFire 入口網站設定

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

本節說明可針對 WildFire 雲端帳戶自訂的設定，例如連接至帳戶的各個防火牆的時區及電子郵件通知。您也可以刪除儲存於雲端中的防火牆日誌。

STEP 1 | 存取入口網站設定。

1. 登入 WildFire 入口網站。
2. 在功能表列上選取 **Settings**（設定）。

STEP 2 | 設定 WildFire 雲端帳戶的時區。

從 **Set Time Zone**（設定時區）下拉式清單中選取時區，然後選取 **Update Time Zone**（更新時區）儲存變更。

在 *WildFire* 分析報告上出現的時間戳記基於為 *WildFire* 雲端帳戶設定時區。

STEP 3 | （選用）刪除在雲端託管的特定防火牆的 WildFire 日誌。

1. 在 **Delete WildFire Reports**（刪除 **WildFire** 報告）下拉式清單中，選取防火牆（按照序號）及 **Delete Reports**（刪除報告），從 WildFire 入口網站移除該防火牆的日誌。此動作不會刪除儲存於防火牆上的日誌。
2. 按一下 **OK**（確定）繼續刪除。

STEP 4 | （選用）根據 WildFire 分析裁定設定電子郵件通知。

WildFire 入口網站不會傳送針對防火牆已轉送進行 *WildFire* 分析的封鎖檔案之警示。

1. 在 Configure Alerts（設定警示）部分，選取 **Malware**（惡意）、**Phishing**（網路釣魚）、**Grayware**（灰色）及/或 **Benign**（良性）核取方塊，根據這些裁定接收電子郵件通知：
   - 在 **All**（全部）列中選取裁定核取方塊，以接收上載至 WildFire 雲端的所有樣本的裁定通知。
   - 在 **Manual**（手動）列中選取裁定核取方塊，以接收使用 WildFire 入口網站手動上載至 WildFire 公共雲端的所有樣本的裁定通知。
   - 選取一個或若干防火牆序號的裁定核取方塊，以接收這些防火牆提交的樣本的裁定通知。
2. 選取 **Update Notification**（更新通知），將裁定通知寄送至與您的支援帳戶關聯的電子郵件地址。

新增 WildFire 入口網站使用者

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

WildFire 入口網站帳戶是由超級使用者（Palo Alto Networks 設備的註冊擁有者）所建立，能夠讓使用者登入 WildFire 雲端，並檢視超級使用者授權存取的設備資料。WildFire 使用者可以是與現有 Palo Alto Networks 帳戶關聯的使用者，或是不與 Palo Alto Networks 支援帳戶關聯的使用者，您可以允許其只存取 WildFire 公共雲端及特定防火牆資料集。

STEP 1 | 選取您要新增可存取 WildFire 入口網站的使用者的帳戶。

WildFire 入口網站使用者可檢視與支援帳戶關聯的所有防火牆的資料。

1. 登入 Palo Alto Networks Support 入口網站。
2. 在 **Manage Account**（管理帳戶）下，按一下 **Users and Accounts**（使用者和帳戶）。
3. 選取現有的帳戶或子帳戶。

STEP 2 | 新增 WildFire 使用者。

1. 按一下 **Add WildFire User**（新增 **WildFire** 使用者）。
2. 輸入要新增的使用者所用的電子郵件地址。

   新增使用者時唯一的限制是不可使用免費的 *Web* 式電子郵件帳戶（*Gmail*、*Hotmail*、*Yahoo* 等）做為電子郵件地址。如果對於不支援的網域輸入電子郵件地址，將顯示快顯警告。

STEP 3 | 將防火牆指派給新的使用者帳戶，並存取 WildFire 雲端。

按照序號選取要授予存取權的防火牆，並填寫選擇性的帳戶詳細資訊。

擁有現有支援帳戶的使用者將收到列出防火牆清單的電子郵件，這些防火牆可供 WildFire 報告檢視之用。如果使用者沒有支援帳戶，入口網站將傳送說明如何存取入口網站和如何設定新密碼的電子郵件。

新使用者此時即可登入 WildFire 雲端檢視已取得存取權的防火牆相關的 WildFire 報告。使用者也可以設定這些設備的自訂電子郵件警示，以便收到所分析的檔案相關的警示。使用者可選擇接收惡意及/或良性檔案的報告。

在 WildFire 入口網站上檢視報告

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 WildFire 授權 對於 *Prisma Access*，這通常已包含在您的 *Prisma Access* 授權中。

Wildfire 入口網站顯示從防火牆提交，手動上載或使用 WildFire API 上載的樣本報告。選取 **Reports**（報告）以顯示 WildFire 雲端分析的樣本報告。對於列示的每個樣本，報告項目顯示雲端接收的樣本日期及時間、提交檔案的防火牆序號、檔案名稱或 URL 以及 WildFire 傳遞的裁定（良性、灰色、惡意或網路釣魚）。

使用搜尋選項，根據檔案名稱或樣本雜湊值來搜尋報告。您還可以透過只檢視由特定 **Source**（來源）（只檢視手動或由特定防火牆提交的結果）提交的樣本結果或收到特定 WildFire **Verdict**（裁定）（任何、惡意、灰色、網路釣魚或擱置）的樣本結果。

若要從入口網站檢視個別的報告，請按一下報告名稱左側的 **Reports**（報告）圖示。若要儲存詳細的報告，請按一下頁面右上角的 **Download as PDF**（下載為 **PDF**）按鈕。如需有關 WildFire 分析報告的詳細資訊，請參閱 WWildFire 分析報告—消除。

以下顯示特定防火牆所提交的樣本檔案清單：