paloalto
TECHDOCS

進階 URL 篩選管理

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 21, 2023

Table of Contents

URL 篩選基礎

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

URL 篩選技術透過對使用者存取以及與網路內容的互動提供詳盡控制，保護使用者免受基於 Web 的威脅。您可以製定 URL 篩選政策，根據 URL 類別、使用者和群組來限制對網站的存取。例如，您可以封鎖對已知包含惡意軟體的網站的存取，並封鎖一般使用者向某些類別的網站輸入公司憑證。

為了詳盡控制使用者對類別的存取，您可以建立 URL 篩選設定檔並定義預先定義和自訂 URL 類別的網站存取權；然後，將設定檔套用到安全性政策規則。您也可以使用 URL 類別作為安全性政策規則中的比對規則。如需詳細瞭解進階 URL 篩選訂閱可以符合組織的 Web 安全需求的方法，請參閱 URL 篩選使用案例。

- Palo Alto Networks URL 篩選解決方案
- URL 篩選支援
- 本機內嵌分類
- 進階 URL 篩選的工作原理
- URL 篩選原則
- URL 類別
- URL 篩選使用案例

Palo Alto Networks URL 篩選解決方案

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

進階 URL 篩選（之前稱為 URL 篩選）是一項訂閱服務，可保護您的網路及其使用者免受已知和未知惡意和具有規避性的 Web 型威脅。此訂閱提供與 URL 篩選相同的功能，即詳盡的 URL 篩選控制、使用者 Web 活動洞察、安全搜尋強制措施和憑證網路釣魚防護，此外此訂閱也使用基於機器學習的內嵌 Web 安全引擎完整檢查 Web 內容。內嵌 Web 安全引擎可以對 PAN-DB（Palo Alto Networks 基於雲端的 URL 資料庫）中不存在的 URL 進行即時分析和分類。然後，該引擎會決定防火牆該採取的動作。

進階 URL 篩選可防止未經 PAN-DB 分析並將其新增至資料庫的已更新或引入的惡意 URL。啟用進階 URL 篩選後，會針對 URL 要求執行以下動作：

- 使用基於雲端的進階 URL 篩選偵測模組進行即時分析。這彌補了與 PAN-DB 中項目進行比較的 URL。由 ML 驅動的 Web 防護引擎會偵測並封鎖 PAN-DB 無法偵測和封鎖的惡意網站。
- 這種基於防火牆的分析解決方案使用本機內嵌分類，檢查以發現網路釣魚和惡意 JavaScript，可以即時封鎖未知的惡意網頁。

執行 PAN-OS 9.1 及更新版本的新世代防火牆支援進階 URL 篩選授權。您可以在 PAN-OS 和 Panorama 網頁介面、Prisma Access 和 Cloud NGFW 平台上管理 URL 篩選功能。但是，部分 URL 篩選功能並非在每個平台上都可使用。

如果企業中的網路安全性要求禁止防火牆直接存取網際網路，Palo Alto Networks 可透過 PAN-DB 私人雲端提供離線 URL 篩選解決方案。您可以在一或多個 M-600 設備上部署 PAN-DB 私人雲端，這些設備在網路中作為 PAN-DB 伺服器；但是，私人雲端不支援進階 URL 篩選解決方案中的任何基於雲端的 URL 分析功能。

舊版 URL 篩選訂閱

URL 篩選對儲存在本機快取或 PAN-DB 中的網站強制實施政策規則。當使用者要求某個網站時，防火牆會檢查本機快取中的 URL 類別。如果該網站不在快取中，防火牆會查詢 PAN-DB 來決定要套用哪個操作。因此，攻擊者能使用不存在雲端資料庫的 URL 來更順利地發動精準攻擊活動。

舊版訂閱持有者可以繼續使用其 *URL* 篩選部署，直到許可期限結束。

URL 篩選支援

（虛擬和內部部署）新世代防火牆、Prisma Access (Managed by Strata Cloud Manager)、Prisma Access (Managed by Panorama)、AWS 的 Cloud NGFW 和 Azure 的 Cloud NGFW 皆有進階 URL 篩選功能。但是，新世代防火牆和 Azure 的 Cloud NGFW 需要進階 URL 篩選訂閱，而所有 Prisma Access 和 AWS 的 Cloud NGFW 授權皆包括進階 URL 篩選功能。

功能支援取決於平台和 *URL* 篩選授權的類型。僅透過進階 *URL* 篩選授權可用的功能會有進階 *URL* 篩選標籤表明。

下表顯示進階 URL 篩選功能和支援 URL 篩選的 Palo Alto Networks 平台的相容性。

功能	支援的系統						附註
	NGFW (Managed by Strata Cloud Manager)	**NGFW (Managed by PAN-OS or Panorama)**	**Prisma Access (Managed by Strata Cloud Manager)**	**Prisma Access (Managed by Panorama)**	**AWS 的 Cloud NGFW**	**Azure 的 Cloud NGFW**	
內嵌分類 • 本機內嵌分類（在 PAN-OS 10.2 之前的版本中稱為內嵌 ML） • （進階 URL 篩選）雲端內嵌分類	是	是	是	是	是	是	VM-50 或 VM50L 設備皆不支援
自訂 URL 類別	是	是	是	是	是	是	
使用者認證偵測	是	是	是	是	是	是	

功能	支援的系統						附註
	NGFW (Managed by Strata Cloud Manager)	NGFW (Managed by PAN-OS or Panorama)	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)	AWS 的 Cloud NGFW	Azure 的 Cloud NGFW	
自訂 URL 篩選回應頁面	是	是	是	是	是	是	
安全搜尋強制 • 嚴格安全搜尋關閉時封鎖搜尋結果 • 強制執行嚴格安全搜尋	是	是	是	是	是	是	
URL 管理員取代	是	是	是	是	是	是	
SSL/TLS 交握檢查	是	是	是	是	是	是	
與遠端瀏覽器隔離 (RBI) 整合	否。	否。	是	是	否。	否。	
僅記錄容器頁面（僅記錄使用者造訪的頁面）	否。	是	是	是	是	是	

本機內嵌分類

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權 註：Prisma Access 授權包括 *Advanced URL Filtering* 功能。

本機內嵌分類（以前稱為內嵌 ML）讓防火牆資料平面能夠在網頁上套用機器學習 (ML)，以在偵測到網路釣魚變體時向使用者發出警示，同時防止 JavaScript 入侵的惡意變體進入您的網路。本機內嵌分類透過使用一系列 ML 模型對各種網頁詳細資料進行評估，來動態分析和偵測惡意內容。每個 ML 模型都透過評估檔案詳細資料（包括解碼器欄位和模式）來偵測惡意內容，以制訂高可能性的分類和決策，然後將其用作較大的 Web 安全性政策的一部分。分類為惡意的 URL 會轉送到 PAN-DB 進行額外分析和驗證。您可以指定 URL 例外狀況，以排除可能遇到的任何誤判。這允許您為設定檔建立更精細的規則，以支援您的特定安全需求。為了保持瞭解威脅形勢的最新變化，內嵌 ML 模型會定期更新並透過內容發佈而新增。需要作用中的進階 URL 篩選訂閱才能設定內嵌分類。

您也可以啟用基於內嵌 ML 的保護作為防毒設定檔設定的一部分，以即時偵測惡意 Portable Executable (可攜可執行的 - PE)、ELF 和 MS Office 檔案以及 PowerShell 和 Shell 指令碼。如需詳細資訊，請參閱：進階 WildFire 內嵌 ML。

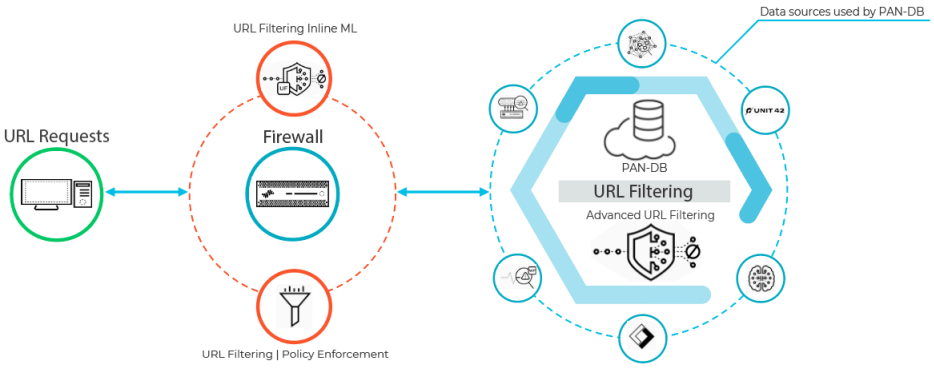
本機內嵌分類在 *VM-50* 或 *VM50L* 虛擬設備上不受支援。

進階 URL 篩選的工作原理

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

進階 URL 篩選根據網站內容、功能和安全對網站進行分類。一個 URL 最多可擁有四個 URL 類別，用於指示網站將使您面臨威脅的可能性。當 PAN-DB（進階 URL 篩選資料庫）對網站進行分類時，啟用進階 URL 篩選功能的防火牆可利用這些資訊來強制執行貴組織的安全性政策。除了 PAN-DB 提供的保護之外，進階 URL 篩選還使用機器學習 (ML) 提供即時分析，以防禦新的和未知的威脅。在 URL 篩選資料庫有機會分析和新增內容之前更新或引入的惡意 URL 為攻擊者提供了一個開放的時間段，他們可以在此期間發起精確攻擊活動，而進階 URL 篩選能夠防範此類惡意 URL。進階 URL 篩選透過基於要求提供即時 URL 分析來彌補資料庫解決方案固有的保障缺口。進階 URL 篩選使用的基於 ML 的模型已經過培訓且會持續更新，以偵測各種惡意 URL、網路釣魚網頁和命令和控制 (C2)。

指示存在某些進階威脅的網站透過基於雲端的內嵌深度學習系統進行額外處理，使用偵測器和分析器來補充進階 URL 篩選使用的 ML 模型。深度學習偵測器可以處理更大的資料集，並可以透過多層神經網路更好地識別複雜的惡意模式和行為。當進階 URL 篩選在收到可疑 Web 要求時從防火牆接收到 HTTP 回應資料，資料將透過深度學習偵測器得到進一步分析，並提供內嵌保護，防止規避零時差 Web 攻擊。這包括隱匿的網站（其中網頁內容是從未知網站秘密擷取的）—這可能包括 URL 資料庫無法解釋的惡意內容、多步驟攻擊、CAPTCHA 挑戰以及以前看不見的一次性 URL。由於規避性惡意網站處於不斷變化的狀態，用於對網站進行分類的偵測器和分析器會在 Palo Alto Networks 威脅研究人員改進偵測邏輯時自動更新和部署，所有這些都不需要管理員下載更新套件。



當使用者要求網頁時，防火牆會查詢使用者新增的例外狀況和 PAN-DB，以瞭解網站的風險類別。PAN-DB 使用來自 Unit 42、WildFire、被動 DNS、Palo Alto Networks 遙測資料、Cyber

Threat Alliance 之資料的 URL 資訊，並套用各種分析器來確定類別。如果 URL 顯示有風險或惡意特性，則還會將 web 有效負載資料提交至雲端中的進階 URL 篩選以進行即時分析，並產生更多的分析資料。然後防火牆會擷取得出的風險類別，並用來基於您的原則設定強制執行 Web 存取規則。此外，防火牆會快取新項目的網站分類資訊，以便快速擷取後續要求，同時移除使用者最近未存取的 URL，以便精確反映您網路中的流量。此外，內建於 PAN-DB 雲端查詢中的檢查可確保防火牆接收最新的 URL 分類資訊。如果您沒有網際網路連線或作用中的 URL 篩選授權，則不會對 PAN-DB 發出任何查詢。

防火牆會按優先順序，將網站的 URL 類別與 1) 自訂 URL 類別、2) 外部動態清單 (EDL) 和 3) 預先定義的 URL 類別中的項目進行比較，以確定網站的 URL 類別。

設定為使用資料平面上的機器學習即時分析 URL 的防火牆可提供額外的安全層，以防止網路釣魚網站和 JavaScript 攻擊。本機內嵌分類使用的 ML 模型可識別當前未知的和將來的基於 URL 的威脅變體，這些變體與 Palo Alto Networks 已確定為惡意的特性相符。為了瞭解威脅形勢的最新變化，本機內嵌分類 ML 模型透過內容發行版本而新增或更新。

當防火牆檢查 PAN-DB 中的 URL 時，其還會尋找重要的更新，例如之前被定為良性但現在是惡意的 URL。

如果您認為 PAN-DB 錯誤分類網站，您可以透過 Test A Site 或直接從防火牆日誌在瀏覽器中提交變更要求。

你知道嗎？

技術上，防火牆會在管理平面和資料平面上快取 *URL*。

- *PAN-OS 9.0* 和更高版本不能下載 *PAN-DB* 種子資料庫。相反，在激活 *URL* 篩選後，防火牆將在進行 *URL* 查詢時填入快取。
- 管理平面持有更多 *URL*，並會直接與 *PAN-DB* 通訊。當防火牆在快取中找不到 *URL* 的類別並在 *PAN-DB* 中執行查閱時，防火牆將在管理平面中快取擷取的類別資訊。管理平面將該資訊傳遞到資料平面，該資料平面也將其快取，並用以強制執行原則。
- 資料平面持有較少的 *URL* 並收取來自管理平面的資訊。在防火牆檢查 URL 類別例外清單（自訂 *URL* 類別和外部動態清單）尋找某一 *URL* 後，防火牆會查看資料平面。如果防火牆在資料平面中找不到該 *URL*，防火牆才會檢查管理平面，如果該類別資訊不存在，則檢查 *PAN-DB*。

URL 篩選原則

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

URL 篩選設定檔定義防火牆如何處理流向特定 URL 類別的流量。URL 篩選設定檔是 URL 篩選控制項的集合，您可以將這些控制項套用到各個允許存取網路的安全性政策規則上。您可以設定 URL 類別的網站存取、允許或禁止使用者憑證提交、啟用安全搜尋強制執行以及各種其他設定。若要強制執行 URL 篩選設定檔中定義的操作，請將設定檔套用至安全性政策規則。防火牆對與安全性政策規則相符的流量強制執行設定檔動作（如需詳細資料，請參閱設定 URL 篩選）。

防火牆的預設設定檔會封鎖潛存威脅的類別，如惡意軟體、網路釣魚及成人內容等。您可以在安全性政策規則中使用預設設定檔、複製設定檔以將其用作新 URL 篩選設定檔的起點，或新增 URL 篩選設定檔。您可以自訂新增的 URL 篩選設定檔，並新增要永遠封鎖或允許的特定網站清單。例如，您可以封鎖「社群媒體」類別，但允許存取該類別的特定網站。根據預設，當您建立新 URL 篩選設定檔時，所有 URL 類別的網站存取均被設定為允許。這表示使用者將能自由地瀏覽所有的網站，且不會記錄流量。

建立最佳做法 URL 篩選設定檔，以確保針對被觀測到裝載惡意軟體或攻擊性內容的 *URL* 提供保護。

URL 篩選設定檔政策動作

在 URL 篩選設定檔中，您可以定義 URL 類別的 **Site Access**（網站存取），允許或禁止基於 URL 類別的**User Credential Submissions**（使用者憑證提交）（例如，您可以封鎖向中等風險和高風險網站提交使用者憑證），並啟用安全搜尋強制執行。

動作	說明
網站存取	
警示	允許網站，並在 URL 篩選日誌中產生日誌項目。 將 ***alert***（警示）設定為您未封鎖之流量類別的 *Action*（動作），從而可記錄並檢視流量。

動作	說明
允許	允許網站，不產生日誌項目。 請勿將 ***allow***（允許）設定為您未封鎖之流量類別的 *Action*（動作），因為您將無法查看未記錄的流量。而是將 ***alert***（警示）設定為您未封鎖之流量類別的 *Action*（動作），從而可記錄並檢視流量。
封鎖	封鎖網站，使用者能看見回應頁面，但無法繼續存取網站。在 URL 篩選日誌中會產生日誌項目。 封鎖某個 URL 類別的 Web 存取也會將該 URL 類別的使用者認證提交設定為封鎖。
繼續	系統會提示使用者回應頁面，表示站台已因公司原則而封鎖，但會提示使用者繼續存取網站的選項。**continue**（繼續）動作通常用於認為是良性的類別，並用於改善使用者體驗，做法是在使用者覺得網站分類錯誤時提供繼續進行的選項。回應頁面訊息可自訂，以包含您公司特有的詳細資訊。在 URL 篩選日誌中會產生日誌項目。 在在設定使用 *Proxy* 伺服器的用戶端系統上，*Continue*（繼續）頁面無法正常顯示。
覆寫	使用者會看見一個回應頁面表示需要密碼才能存取指定類別中的網站。安全性管理員或服務台人員可透過此選項提供密碼，此密碼允許暫時存取指定類別中的所有網站。在 URL 篩選日誌中會產生日誌項目。請參閱 允許使用密碼存取特定網站。 在較早版本中，URL 篩選類別覆寫的執行順序優先於自訂 URL 類別。作為 PAN-OS 9.0 升級的一部分，URL 類別覆寫會轉換為自訂 URL 類別，且執行順序不再優先於其他自訂 URL 類別。與以前版本中為類別覆寫定義的動作不同，新的自訂 URL 類別由具有最嚴格的 URL 篩選設定檔動作之安全性政策規則執行。可能的 URL 篩選設定檔動作包括（嚴格性從強到弱）：封鎖、覆寫、繼續、警示和允許。 這表示，如果您使用允許的動作覆寫 URL 類別，當覆寫內容在 PAN-OS 9.0 中轉換為自訂 URL 類別後，有可能會被封鎖。 在在設定使用 *Proxy* 伺服器的用戶端系統上，*Override*（覆寫）頁面無法正常顯示。

動作	說明
無	無動作僅適用於自訂 URL 類別。選取 **none**（無）可確保當存在多個 URL 設定檔時，自訂類別不會對其他設定檔有任何影響。例如，如果您有兩個 URL 設定檔，並在其中一個設定檔中將自訂 URL 類別設為 **block**（封鎖），如果您不想向另一個設定檔套用封鎖動作，則必須將此動作設為 **none**（無）。 此外若要刪除自訂的 URL 類別，則請在任何使用該類別的設定檔中將該類別設為 **none**（無）。
使用者認證權限 這些設定需要您先設定認證網路釣魚防禦。	
警示	允許使用者向此 URL 類別中的網站提交公司認證，但每次都會產生 URL 篩選警示日誌。
允許（預設）	允許使用者向此 URL 類別中的網站提交公司認證。
封鎖	阻止使用者向此 URL 類別中的網站提交公司認證。當使用者存取禁止提交公司認證的網站時，會向使用者顯示防網路釣魚回應頁面。您可以自訂要顯示的封鎖頁面。
繼續	對使用者顯示回應頁面，提示他們選取 Continue （繼續）才能存取該網站。依預設，當使用者存取不建議提交公司認證的網站時，會向使用者顯示防網路釣魚繼續頁面。例如，您可以自訂回應頁面，以警告使用者防止網路釣魚嘗試或在其他網站上重複使用其憑證。

URL 類別

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

Palo Alto Networks 根據網站的內容、功能和安全性對網站進行分類。每個 URL 類別對應一組可建立政策規則的特徵。您網路上的使用者所造訪的 URL 會新增至 Palo Alto Networks URL 篩選資料庫 PAN-DB。PAN-DB 會為這些網站歸類最多四個 URL 類別，包括風險類別（高、中和低）。

URL 類別啟用以類別為基礎的 Web 流量篩選，以及詳盡的站台政策控制。您可以設定 URL 篩選設定檔來定義 URL 類別的網站存取權限，並將設定檔套用到允許流向網路的流量的安全性政策規則。您也可以使用 URL 類別作為安全性政策規則中的比對規則，以確保這些規則僅適用於指定類別中的網站。例如，您可以設定解密政策規則，防止解密金融服務類別的流量。

若要檢查特定 URL 的類別，請將該 URL 輸入到我們的 URL 查閱引擎 Test A Site。如果您認為 URL 分類錯誤，請提交類別變更要求。

自訂 URL 類別

您可以建立自訂 URL 類別，以從根據類別的強制執行中排除特定網站。您可以根據特定 URL（URL 清單）或其他類別（類別比對）自訂 URL 類別。URL 清單類型的自訂 URL 類別會用作封鎖清單和允許清單。自訂類別比對類型的 URL 類別，可以針對與定義為自訂類別一部分的所有類別相符的網站進行強制執行。

預先定義的 URL 類別

下表列出了 PAN-DB 用於篩選 URL 的預先定義 URL 類別。有些項目說明了從該類別中排除的網站。專注於安全性的 URL 類別 則說明風險類別；這些風險類別並未指派給所有 URL。

URL 類別	說明
墮胎	網站內容包括：支持或反對墮胎的相關資訊或團體、墮胎程序的相關詳細資訊、支持或反對墮胎的協助或支持論壇，或尋求（不）墮胎的後果或影響的相關資訊。

URL 類別	說明
藥物濫用	網站內容包括：宣傳濫用合法或非法藥物、銷售和使用吸毒相關用具，或製造或銷售毒品。
成人內容	網站內容包括：任何露骨內容、媒體（包括語言、遊戲或漫畫）、藝術或產品、具露骨性質的線上群組或論壇，或宣傳成人服務（例如以影片或電話會議形式、陪護服務）和脫衣舞俱樂部。
菸酒	網站內容包括：銷售、製造或使用菸酒產品以及相關用具的相關資訊。也包括與電子煙相關的網站。
人工智慧	使用機器學習和深度學習模型（包括大型語言模型）來提供通常需要人類智慧的服務的網站。提供的服務包括但不限於聊天機器人、生產、摘要器、轉錄器、無代碼以及音訊或視訊編輯相關服務。重點是託管實際人工智慧服務的網站，而非資訊人工智慧內容。
拍賣	促進個人之間商品銷售的網站。 以捐贈為目的的拍賣被歸類為社會類別。
商業與經濟	包含與行銷、管理、經濟、創業或經營業務相關的內容的網站，包括： • 廣告和行銷公司的網站 • 運輸服務網站，例如 fedex.com • 電話、有線傳輸系統和網際網路服務供應商的網站 • 調查或民調網站 • 商會網站 • 會議網站* • 企業網站可能根據其技術而非此類別進行分類。 • *與會議相關的網站應根據內容進行分類。如果該網站無具體內容，則將其分類為商業和經濟。
命令和控制	惡意軟體或受感染系統使用命令與控制 (C2) URL 和網域，秘密地與攻擊者的遠端伺服器進行通訊，以接收惡意命令或竊取資料。

URL 類別	說明
電腦和網路資訊	提供有關電腦和網路的一般資訊的網站，提供的內容包括： • 電腦科學 • 工程 • 硬體和電腦零件 • 軟體 • security • 程式設計 程式設計可能與「文獻與研究」類別有些重疊，但其主要類別應為「電腦和網路資訊」。
內容傳遞網路	主要向第三方提供內容（例如廣告、媒體、文件和圖像伺服器）的網站。
侵害著作權	具有非法內容的網域，例如允許非法下載軟體或其他智慧財產權的內容，這些內容會帶來潛在的責任風險。 提供對等式檔案交換服務或一般串流媒體的網站屬於各自的類別。
加密貨幣	推廣加密貨幣、加密貨幣挖礦（但不包括嵌入式加密貨幣礦工）網站、加密貨幣交易所和供應商，或管理加密貨幣錢包和分類帳的網站。 引用加密貨幣的網站或與加密貨幣相關的惡意網站會另外分類。例如，解釋加密貨幣和區塊鏈技術運作方式的網站屬於「電腦和網路資訊」。
約會	提供線上約會服務、建議或其他個人廣告的網站。 提供性愛聊天室的約會網站屬於成人類別。
動態 DNS	提供或利用動態 DNS 服務，將網域名稱與動態 IP 位址建立關聯的網站。

URL 類別	說明
	攻擊者經常將動態 *DNS* 用於命令和控制通訊以及其他惡意目的。
教育機構	學校、學院、大學、學區、線上課程和其他學術機構的官方網站。其中也包括家教網站。 此類別是指較大型且成熟的教育機構，例如小學、高中和大學。
加密的 DNS	DNS 解析器供應商的網站，其使用透過 HTTPS 的 DNS 等協定加密 DNS 要求和回應，為一般使用者提供安全和隱私。
娛樂與藝術	電影、電視、廣播、影片、節目指南或工具、漫畫、表演藝術、博物館、藝廊或圖書館的網站。其中包括： • 娛樂 • 名人和娛樂新聞 • 小說 • 舞蹈班 • 活動場地 • 紋身藝術
極端內容	網站宣揚恐怖主義、種族主義、法西斯主義或歧視不同種族背景、宗教或其他信仰的其他主義者的觀點。在某些地區，法律和法規可能會禁止存取極端主義網站，因為允許存取可能會帶來責任風險。 討論爭議性政治或宗教觀點的網站分別屬於「哲學和政治倡議」和「宗教」類別。
金融服務	與個人財務或建議相關的網站，例如網路銀行、貸款、抵押貸款、債務管理、信用卡公司、外幣兌換 (FOREX) 和保險公司。但不包括與健康保險、股票市場、經紀或交易服務相關的網站。
賭博	透過樂透或賭博促成真實或虛擬貨幣交換的網站。包括提供賭博資訊、教學或建議（例如如何投注賠率和彩池）的相關網站。

URL 類別	說明
	不推廣賭博的飯店或賭場公司的網站屬於「旅遊」類別。
遊戲	提供線上或下載電玩或電腦遊戲、遊戲評論、提示、秘技或相關出版物和媒體的網站。包括提供非電子遊戲說明、促進棋盤遊戲銷售或交易或支持或舉辦線上抽獎和贈品的網站。
政府	地方、州和國家政府以及相關機構、服務或法律的官方網站。 公共圖書館和軍事機構的網站分別屬於「文獻與研究」以及「軍事」類別。
Grayware	網站內容不會構成直接安全威脅，但會顯示其他侵入行為並誘使一般使用者授予遠端存取權限或執行其他未經授權的操作。 灰色軟體包括： • 被駭客入侵的網站 • 對不表現出惡意行為且不屬於目標網域所有的網域進行網域仿冒 • 含有流氓軟體、廣告軟體或其他未經要求的應用程式的網站，例如嵌入式加密貨幣挖礦程式、點擊劫持或更改 Web 瀏覽器元素的劫持者 • 含有非法或犯罪活動內容的網站
駭客攻擊	與非法或可疑存取或使用通訊設備或軟體相關的網站，包括此類程式的開發和分發、操作建議或可能導致網路和系統受到損害的提示。包括有助於繞過授權和數位版權系統的網站。
健康與醫學	包含一般健康、問題以及傳統和非傳統技巧、療法和治療相關資訊的網站。包括各種醫學專業、實踐、設施（例如健身房和健身俱樂部）和專業人員的網站。與醫療保險和整容手術相關的網站也包括在內。
居家與園藝	提供與家庭維修和保養、建築、設計、施工、裝飾和園藝相關的資訊、產品和服務的網站。
狩獵與釣魚	提供狩獵和釣魚技巧或說明或推廣相關設備和用具銷售的網站。

URL 類別	說明
	主要銷售槍支（即使用於狩獵）的網站屬於「武器」類別。
內容不足	提供測試頁面、未提供任何內容、提供並非用於一般使用者顯示的 API 存取，或要求驗證卻又不顯示任何其他符合其他類別內容的網站和服務。
網際網路通訊及通話	支援或提供視訊聊天、即時訊息或其他通話功能服務的網站。
網路入口網站	通常整合廣泛的內容和主題來作為使用者瀏覽起點的網站。
求職	為雇主和求職者提供職缺列表、雇主評論、面試建議和技巧或相關服務的網站。
法律	提供有關法律、法律服務、律師事務所或其他法律相關問題的資訊、分析或建議的網站。
惡意軟體	包含或已知託管惡意內容、可執行檔、指令碼、病毒、木馬和程式碼的網站。
大麻	討論、鼓勵、推廣、提供、銷售、供應或以其他方式提倡使用、種植、製造或分銷大麻及其各種別名的網站（無論出於娛樂或醫療目的）。包括含大麻相關用具內容的網站。
軍事	提供有關軍事部門、招募、當前或過去的行動或任何相關用具的資訊或評論的網站。包括軍隊和退伍軍人協會的網站。
機動車輛	包含汽車、摩托車、船舶、卡車和休旅車 (RV) 的評論、銷售、交易、改裝、零件和其他相關討論資訊的網站。
音樂	與音樂銷售、發行或資訊相關的網站。包括音樂藝術家、團體、唱片公司、活動、歌詞以及音樂業務其他相關資訊的網站。不包括音樂串流網站。
新註冊的網域	過去 32 天內註冊的網站。新註冊網域通常是有目的或使用網域產生演算法產生的，可能用於惡意活動。
新聞	線上出版品、新聞專線服務和其他整合時事、天氣或其他當代議題的網站。包括以下內容： • 報紙

URL 類別	說明
	• 廣播電台 • 雜誌 • Podcasts • 專門報導新聞的電視節目 • 社交書籤網站，例如 reddit.com 如果雜誌或新聞網站聚焦於運動、旅遊、時尚等特定主題，則會根據網站上的主要內容進行分類。
未解析	此類別表示本地 URL 篩選資料庫中未找到該網站，防火牆無法連線到雲端資料庫查閱該類別。
裸露	包含裸體或半裸人體描繪的網站（無論創作背景或意圖為何，包括藝術品）。包括有參與者圖像的裸體主義網站。
線上儲存與備份	免費或作為服務提供線上檔案儲存的網站。包括照片分享網站。
寄放	託管限制內容或點擊廣告的 URL，其中可能會為託管實體帶來收入，但通常不包含對一般使用者有用的內容。包括待售網域。 含有成人內容的寄放網站屬於「成人」類別。
點對點	提供存取或用戶端以點對點分享種子、下載程式、媒體檔案或其他軟體應用程式的網站。主要適用於具 BitTorrent 下載功能的網站。不包括共享軟體或免費軟體網站。
個人網站和部落格	個人或團體的個人網站和部落格。如果此類網站的主要內容與另一個類別相關，則會被歸類為兩個類別。
哲學和政治倡議	包含哲學或政治觀點相關的資訊、觀點或活動的網站。
網路釣魚	試圖利用社交工程技術，自願或非自願地暗中從受害者獲取資訊，例如登入憑證、信用卡資訊、帳號、PIN 和其他個人識別資訊 (PII) 的 Web 內容。包括技術支援詐騙和恐嚇軟體。

URL 類別	說明
私人 IP 位址	此類別包括 RFC 1918「私人內部網路的位址分配」中定義的 IP 位址，如下所示： • 10.0.0.0 - 10.255.255.255（10/8 前置詞） • 172.16.0.0 - 172.31.255.255（172.16/12 前置詞） • 192.168.0.0 - 192.168.255.255（192.168/16 前置詞） 包括未在公共 DNS 系統中註冊的網域（例如 *.local 和 *.onion）。
代理程式規避與匿名者	代理伺服器和其他繞過 URL 篩選或監控的方法。 企業級使用的 *VPN* 屬於「網際網路通訊和通話」類別。
可疑	包含針對特定個人或人群的低俗笑料或攻擊性內容的網站。
勒索軟體	已知託管勒索軟體或參與勒索軟體活動的惡意流量的網站，其通常威脅（通常透過加密方式）發布私人資料或封鎖對特定資料或系統的存取，除非支付所需的贖金。包括提供可能攜帶勒索軟體有效負載的相關竊取程式、擦除程式和載入程式的 URL。
房地產	提供有關房產租賃、銷售以及相關提示或資訊的網站，包括以下網站： • 房地產公司和代理商 • 租賃服務 • 刊登（和整合） • 物業改善 • 屋主協會 • 物業管理團體或個人 抵押貸款和貸款服務商的網站屬於「金融服務」類別。
即時偵測（僅進階 URL 篩選）	作為進階 URL 篩選的一部分，已透過即時內嵌分析進行分析和偵測的 URL。
休閒娛樂	包含與娛樂活動和興趣相關的資訊、論壇、協會、團體或出版品的網站。

URL 類別	說明
	銷售與娛樂活動或興趣相關的產品的網站（例如 *REI.com*）屬於「購物」類別。
文獻與研究	提供個人、專業人士或學術參考入口網站、資料或服務的網站，包括線上字典、地圖、年鑑、人口普查資訊、圖書館、家譜和科學資訊。包括以下網站或與之相關的網站： • 黃頁 • 日曆 • 公共圖書館 • 研究機構 • 燈光和車輛追蹤服務 • 與房地產、交通等相關的文件和記錄（包括政府資料）
宗教	提供各種宗教、相關活動或事件相關資訊的網站。包括宗教組織、宗教人士、禮拜場所、算命、占星、星座和宗教用具的網站。 附屬於宗教組織的私立小學或中學（例如天主教學校）的網站，其課程教授一般宗教教育和世俗科目，屬於「教育機構」類別。
掃描活動（僅進階 URL 篩選）	競爭者進行的活動可能有漏洞，或試圖進行針對性的攻擊或探測現有漏洞。這些通常是競爭者進行的偵察活動的一部分。
搜尋引擎	使用關鍵字、短語或其他參數提供搜尋介面的網站，這些網站可能會傳回資訊、網站、圖像或其他檔案作為結果。
性教育	提供有關生殖、性發育、安全性行為、性傳染病、節育、性行為技巧以及任何相關產品或用具資訊的網站。包括相關團體、論壇或組織的網站。
共享軟體和免費軟體	免費或捐贈提供軟體、螢幕保護程式、圖示、桌布、實用程式、鈴聲、主題或小工具的網站。包括開放來源項目。
購物	促進購買商品和服務的網站。包括線上商家、百貨公司網站、零售店、目錄以及價格整合或監控工具。此

URL 類別	說明
	類別的網站應是銷售各種商品（或其主要目的是線上銷售）的線上商家。 若一間化妝品公司的網站恰好允許線上購買，該網站則屬於「化妝品」類別。
社群網路	使用者社群或網站，使用者可以在其中互動、發布訊息、圖片以及以其他方式與人群交流。 個人網站、部落格或論壇屬於「個人網站和部落格」類別。
社會	內容與一般大眾或影響大眾（例如時尚、美容、慈善團體、社團或兒童）的議題相關的網站。包括餐廳網站。 與食品相關的企業網站（例如漢堡王）屬於「商業和經濟」類別。
運動	提供有關體育賽事、運動員、教練、官員、團隊或組織、比分、賽程表、相關新聞或體育用品資訊的網站。包括夢幻體育和虛擬體育聯盟的網站。 主要目的是銷售體育用品的網站則屬於「購物」類別。
股票建議和工具	提供有關股票市場、股票或選擇權交易、投資組合管理、投資策略、報價或相關新聞資訊的網站。
串流媒體	免費或購買串流音訊或視訊內容的網站，包括線上廣播電台、串流音樂服務和播客 (podcasts) 檔案。
泳衣和貼身衣物	包含有關泳裝、貼身衣物或其他暗示性服裝的資訊或圖像的網站。
培訓和工具	提供線上教育、培訓和相關資料的網站。包括駕駛或交通學校、工作場所培訓、遊戲、應用程式、教育工具和家教機構。 特定技能課程則根據其主題進行分類。例如，音樂課程的網站屬於「音樂」類別。

URL 類別	說明
翻譯	提供翻譯服務的網站，包括使用者輸入和 URL 翻譯。這些網站也可以讓使用者規避篩選，因為目標頁面的內容呈現在譯者 URL 的上下文當中。
旅遊	提供有關旅遊的資訊（例如建議、優惠、定價、目的地資訊、觀光）和相關服務（例如預訂或價格工具）的網站。包括以下網站： • 當地景點 • 飯店 • 航空公司 • 郵輪公司 • 賭場（如果網站不允許線上賭博） • 旅行社 • 車輛租賃 • 停車設施
未知	Palo Alto Networks 尚未識別的網站。  如果此網站的可用性對您的業務至關重要，且您必須允許該流量，請對未知網站發出警示、對流量套用最佳實務安全性設定檔文件，並檢查警示。  *PAN-DB* 即時更新會在第一次嘗試造訪未知網站後探索這些網站，因此未知 *URL* 會被快速識別，並成為防火牆可以根據實際 *URL* 類別進行處理的已知 *URL*。
武器	處理銷售或提供有關武器、盔甲、防彈背心及其使用的評論、描述或說明的網站。 與紅土射擊、射擊場和射箭相關的網站主要類別為「武器」，次要類別為「體育」。
網路廣告	包含廣告、媒體、內容和橫幅的網站。包括訂閱和取消訂閱電子報或廣告的頁面。
Web 式電子郵件	任何提供對電子郵件收件匣的存取，以及傳送和接收電子郵件的網站。重點是提供免費或付費公共存取此類服務的網站。

URL 類別	說明
Web 託管	提供免費或付費網頁託管服務的網站。包括提供有關網路開發、出版、促銷和其他增加流量的方法的資訊的網站。

專注於安全性的 URL 類別

PAN-DB 會自動評估至少在至少 30 天內僅顯示良性活動，尚未或不再分類為惡意 URL，並將其分配風險類別（高風險、中等風險和低風險）。每個風險類別都有特定的標準，URL 必須符合這些標準才能取得給定的類別。隨著網站內容變化，風險類別和政策執行會動態調整。

如果 *PAN-DB* 判定 *URL* 屬於惡意 URL 類別，則不會為該網站指派風險類別。反之，防火牆會自動封鎖該網站，因為它會對多數環境造成不可接受的風險。

私人 *IP* 位址（和主機）對於主機環境是唯一的，並且對 *PAN-DB* 不可見。因此，*Palo Alto Networks* 不會為此類別中的網站指派風險評等。

專注於安全性的 URL 類別有助於針對性解密和政策實施，進而協助減少攻擊面。例如，您可以封鎖使用者存取高風險和中等風險網站以及新註冊的網域，或解密這些類別的流量（如果您允許此操作）。

下表列出每個風險類別的說明以及預設和建議的政策動作。

您無法針對專注於安全性的 *URL* 類別提交變更要求。

URL 類別	說明
高風險	• 其網域被 ML 模型判定為具先前連結到已知惡意網域的屬性或具較低 Web 信譽訊號的網站。 • 之前確認為惡意軟體、網路釣魚或命令和控制 (C2) 網站的網站。 • 與已確認的惡意活動相關的網站或與已知惡意網站共用網域的網站。 • 防彈 ISP 代管網站。 • 由於存在作用中動態 DNS 設定而被分類為 DDNS 的網域。 • 代管於已知允許惡意內容之 ASN 中 IP 的網站。 • 網站分類為未知。 在 *PAN-DB* 完成網站分析和分類之前，這些網站仍屬於高風險網站。 • 網站將保留在此類別中至少 30 天。 預設和建議的政策動作：警示

URL 類別	說明
中等風險	• 先前被確認為惡意軟體、網路釣魚的網站，或僅顯示良性活動至少 30 天的 C2 網站。 • 所有雲端儲存網站（網站分類為類別為線上儲存與備份）。 • IP 位址分類為未知。 在 *PAN-DB* 完成網站分析和分類之前，這些 *IP* 位址仍為中等風險網站。 • 這些網站將在此類別中額外保留 60 天。 預設和建議的政策動作：警示
低風險	不屬於中等風險或高風險的網站均被視為低風險網站。這些網站在至少 90 天內都顯示為良性活動。 預設和建議的政策動作：允許
新註冊的網域	識別過去 32 天內註冊的網站。新網域經常被用作惡意活動中的工具。 新註冊網域通常是有目的或使用網域產生演算法產生的，用於惡意活動。最佳做法是封鎖此 *URL* 類別。 預設的政策動作：警示 建議的政策動作：封鎖

惡意 URL 類別

我們強烈建議您封鎖標識惡意或入侵內容和行為的以下 URL 類別。

- 命令和控制
- 侵害著作權
- 動態 **DNS**
- 極端內容
- 灰色軟體
- 惡意軟體
- 新註冊的網域
- 寄放
- 網路釣魚
- 代理程式規避與匿名者

- 可疑
- 勒索軟體
- 掃描活動
- 未知

對於要發出警示（而不是封鎖）的類別，您可以嚴格地控制使用者與網站內容的互動方式。例如，讓使用者存取所需資源（如用於研究目的的開發人員部落格或雲端儲存服務），但須採取以下預防措施來減少來自 Web 威脅的攻擊：

- 遵循反間諜軟體、漏洞保護和檔案封鎖最佳做法。有效的保護措施需要能夠封鎖下載危險的檔案類型和您對其發出警示之網站的混淆 JavaScript。
- 根據 URL 進行目標解密。開始最好解密高風險和中等風險網站。
- 當使用者造訪高風險和中等風險網站時，向其顯示回應頁面。警示他們，他們嘗試存取的網站可能包含惡意內容，如果他們決定繼續造訪此網站，則建議他們如何採取預防措施。
- 透過封鎖使用者向網站（包括高風險和中等風險網站）提交公司認證，防止認證網路釣魚。

下表列出 PAN-DB 視為惡意且預設會封鎖的類別，私人 IP 位址除外。私人 IP 位址（和主機）對於主機環境是唯一的，並且對 PAN-DB 不可見。因此，Palo Alto Networks 不會為此類別中的網站指派風險評等。

類別	預設動作
命令和控制	封鎖
Grayware	
惡意軟體	
網路釣魚	
勒索軟體	
掃描活動	
私人 **IP** 位址	允許（不是預設動作）

URL 篩選使用案例

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

除了僅封鎖和允許某些網站之外，還有許多執行網頁存取權的方法。例如，您可以對每個 URL 使用多個類別，以允許使用者存取網站，但須封鎖特定功能，如提交公司認證或下載文件。您還可以使用 URL 類別以強制執行不同的原則類型，例如驗證、解密、QoS 和安全性。

請繼續閱讀，以獲取有關您可以部署 URL 篩選的不同方法的更多資訊。

基於 **URL** 類別控制 **Web** 存取

您可以建立 URL 篩選設定檔來為 URL 類別指定動作，並將設定檔附加至安全性政策規則。防火牆基於設定檔中的設定強制執行針對流量的原則。例如，若要封鎖所有遊戲網站，您可以在 URL 篩選設定檔中設定遊戲類別的封鎖動作。之後，您可以將該設定檔附加到允許 Web 存取的安全性政策規則。

多類別 **URL** 篩選

每個 URL 最多可擁有四個類別，包括風險類別，用於顯示網站將使您面臨威脅的可能性。您能夠透過更詳盡的 URL 分類超越基本的「封鎖或允許」Web 存取方法。反之，您可以控制使用者與線上內容的互動方式，雖然這是業務當中的必要一環，但更可能是防禦網路攻擊的一部分手段。

例如，您可能認為某些 URL 類別對您的組織存在風險，但由於還會提供有價值的資源或服務（例如雲端儲存服務或部落格），因此會猶豫將該等類別徹底封鎖。現在，您可允許使用者造訪這些類型的類別，同時您透過解密和檢查流量並對內容執行唯讀存取。

您也可以選取 **Category Match**（類別比對）並指定兩個或多個 PAN-DB 類別，以定義自訂 URL 類別，新類別將包含這些類別。透過從多個類別建立自訂類別，可讓您針對符合自訂 URL 類別物件中指定之所有類別的網站或頁面進行執行作業。

基於 **URL** 類別封鎖或允許公司認證提交

透過啟用防火牆偵測提交至網站的公司認證防止認證網路釣魚，然後基於 URL 類別控制這些提交。阻止使用者向惡意網站和非受信任網站提交認證，警告使用者不要在未知網站上輸入公司認證，或警告使用者不要在非公司網站上重複使用公司認證，並明確允許使用者向公司網站和認可網站提交認證。

強制執行安全搜尋設定

許多搜尋引擎都有安全搜尋設定，可將來自搜尋結果中的成人影像與視訊篩選掉。針對未使用最嚴格安全搜尋設定的使用者，您可以讓防火牆封鎖搜尋結果或透明地啟用安全搜尋。防火牆支援針對下列搜尋提供者強制執行安全搜尋：Google、Yahoo、Bing、Yandex 及 YouTube。查看如何開始使用 安全搜尋強制。

強制執行使用密碼存取特定網站

您可以封鎖用於大多數使用者的網站的存取，同時允許某些使用者存取該網站。請檢視如何允許使用密碼存取特定網站。

封鎖從某些 URL 類別下載高風險檔案

您可以透過建立附加有檔案封鎖設定檔的安全性政策規則以封鎖下載來自特定 URL 類別的高風險檔案。

基於 URL 類別強制執行安全性、解密、驗證和 QoS 原則

您可以基於 URL 類別強制執行不同類型的防火牆原則。例如，假設您啟用了解密，但是想排除某些個人資訊不被解密。在這種情況下，您可以建立一個解密政策規則，以將與 URL 類別 *financial-services*（金融服務）和 *health-and-medicine*（健康保健）相符的網站從解密中排除。另一範例是在 QoS 原則中使用 URL 類別 *streaming-media*（流媒體），將頻寬控制套用到歸為此類別的網站。

下表說明接受 URL 類別作為比對準則的原則：

原則類型	說明
解密	您還可以使用 URL 類別逐步解密，並將可能包括敏感或個人資訊的 URL 類別從解密中排除。（如金融服務和健康保健）。 計劃先解密風險最高的流量（最有可能存在賭博或高風險這類惡意流量的 URL 類別），然後隨著經驗積累解密更多流量。或者，先解密不會影響業務的 URL 類別（即使出現問題，也不會影響業務），例如新聞資訊來源。在這兩種狀況下，解密一些 URL 類別、聽取使用者意見反應、執行報告以確保解密如預期運作，然後逐步解密更多 URL 類別等等。若因技術原因而無法解密網站，或者您選擇不對其進行解密，請根據解密排除項將這些網站排除在解密之外。 基於 *URL* 類別解密流量是 *URL* 篩選和 Decryption（解密）的最佳做法。
驗證	若要確定會先驗證使用者再允許其存取特定類別，您可以附加 URL 類別作為驗證原則規則的比對準則。

原則類型	說明
QoS	使用 URL 類別配置特定網站類別的輸送量層級。例如，您想要允許串流媒體類別，但透過將 URL 類別新增至 QoS 原則規則中限制輸送量。

security	您可以將 URL 類別用作比對規則或建立 URL 篩選設定檔來為每個類別指定動作，並將其附加至安全性政策規則。
	
	將 ***URL*** 類別用作比對規則 ***vs.*** 將 ***URL*** 篩選設定檔套用至安全性政策規則
	• 請在下列情況下使用 *URL* 類別作為比對規則：
	  • 若要建立 URL 類別強制執行的例外情況
	  • 若要將特定動作指派給自訂或預先定義的 *URL* 類別。例如，您可以建立安全性政策規則，允許存取個人網站和部落格類別中的網站。
	• 請在以下情況下使用 *URL* 篩選設定檔：
	  • 若要在 *URL* 篩選日誌中記錄流向 *URL* 類別的流量
	  • 若要針對流向特定類別的流量指定更明確的動作（例如警示）
	  • 若要設定使用者存取被封鎖或被封鎖繼續的網站時所顯示的回應頁面。
	
	在 *URL* 篩選設定檔中，為每個 *URL* 類別指定的動作僅適用於傳送至安全性政策規則中指定類別的流量。您也可以將特定設定檔套用到多個規則。

原則類型	說明
	例如，如果您公司中的 IT 安全性群組必須能存取入侵類別，但要拒絕其他所有使用者存取該類別，您必須建立下列規則： • 允許 IT 安全性群組存取歸類為入侵之內容的安全性原則規則。此安全性原則規則參考 **Services/URL Category**（服務/**URL** 類別）頁籤中的入侵類別，以及 **Users**（使用者）頁籤中的 IT 安全性群組。 • 允許所有使用者具有一般 Web 存取權的其他安全性原則規則。您可將封鎖入侵類別的 URL 篩選設定檔附加至此規則。 您必須將允許存取入侵站台的原則列在封鎖入侵站台的原則之前。這是因為防火牆會由上而下評估安全性原則規則，所以當屬於安全性群組的使用者嘗試存取入侵網站時，防火牆會對允許存取的原則規則先進行評估，然後授與使用者存取權。防火牆會針對封鎖對入侵站台之存取的一般 web 存取規則，來評估來自其他所有群組的使用者。

設定 URL 篩選

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

熟悉 URL 篩選基礎的概念之後，您就可以開始使用 URL 篩選。從啟動 Advanced URL Filtering 授權（如適用）到測試您的設定，本章涵蓋了有效部署 URL 篩選所需的內容。若要充分利用部署，請遵循 URL 篩選最佳實務。

- 啟動進階 URL 篩選授權
- 開始使用 URL 篩選
- 設定 URL 篩選
- 設定內嵌分類
- URL 類別例外
- URL 篩選最佳做法
- 測試 URL 篩選設定

啟動 Advanced URL Filtering 授權

這可在何處使用？	我需要什麼？
• 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)	❑ Advanced URL Filtering 授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

Advanced URL Filtering 訂閱提供即時 URL 分析和惡意軟體防護。除了 PAN-DB 存取權（Palo Alto Networks 開發的 URL 篩選資料庫，可進行高效能的 URL 查閱）之外，還提供對惡意 URL 和 IP 位址的涵蓋範圍。

（虛擬和內部部署）新世代防火牆、Strata Cloud Manager、Prisma Access (Managed by Panorama)、AWS 的 Cloud NGFW 和 Azure 的 Cloud NGFW 皆有 Advanced URL Filtering 功能。但是，新世代防火牆和 Azure 的 Cloud NGFW 需要 Advanced URL Filtering 訂閱，而所有 Prisma Access 和 AWS 的 Cloud NGFW 授權皆包括 Advanced URL Filtering 功能。

若要檢查 Advanced URL Filtering 功能和每個支援 URL 篩選的 Palo Alto Networks 平台的相容性，請查看 URL 篩選支援。

- Strata Cloud Manager
- PAN-OS 和 Panorama

啟動進階 URL 篩選授權 (Strata Cloud Manager)

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

請切換到 **PAN-OS & Panorama** 頁籤並按照指示啟動授權。

如果您使用 **Strata Cloud Manager:**

❑ 驗證您的進階 URL 篩選授權。

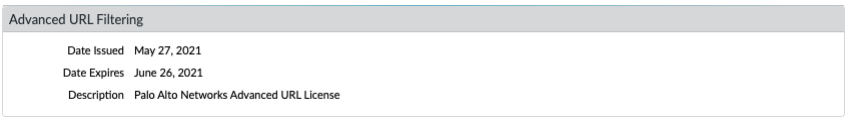
❑ 開始使用進階 URL 篩選。

啟動進階 URL 篩選授權 (PAN-OS & Panorama)

STEP 1 | 取得並安裝 Advanced URL Filtering 授權。

Advanced URL Filtering 授權包括對 *PAN-DB* 的存取權限；如果授權到期，防火牆會停止執行所有 *URL* 篩選功能、*URL* 類別執行以及 *URL* 雲端查閱。此外，在您安裝有效的授權之前，所有其他雲端更新將不會運作。

1. 選取 **Device**（裝置） > **Licenses**（授權），並在授權管理區段中，選取授權安裝方法：
   - 從授權伺服器擷取授權金鑰
   - 使用驗證碼啟動功能
2. 確認 Advanced URL Filtering 區段、**Date Expires**（到期日期）欄位顯示有效日期。



當您啟動 *Advanced URL Filtering* 授權時，*PAN-DB* 和 *Advanced URL Filtering* 的授權權利可能不會在防火牆上正確顯示—這是顯示異常，而非授權問題，且不會影響對服務的存取。您可以使用下列 *CLI* 命令更新防火牆上的授權以修正顯示問題：***request license fetch***。

STEP 2 | 下載並安裝最新的 PAN-OS 內容版本。PAN-OS 應用程式和威脅內容版本 8390-6607 及更高版本允許執行 PAN-OS 9.x 及更高版本的防火牆識別已使用 Advanced URL Filtering 中即時偵測類別分類的 URL。如需有關更新的詳細資訊，請參閱「應用程式和威脅內容版本資訊」。您也可以在 Palo Alto Networks 支援入口網站上檢閱應用程式和威脅的內容版本說明，或直接在防火牆網頁介面上檢閱：選取 **Device**（裝置） > **Dynamic Updates**（動態更新），然後開啟特定內容發行版本的版本說明。

更新至最新內容發行版本時，請遵循應用程式和威脅內容更新的最佳做法。

STEP 3 | 排程防火牆以下載應用程式與威脅的動態更新。

必須有威脅防護授權才能收到內容更新，其中涵蓋「防毒」與「應用程式與威脅」。

1. 請選取 **Device**（裝置） > **Dynamic Updates**（動態更新）。（裝置 > 動態更新）.
2. 在應用程式與威脅區段的排程欄位中，按一下 **None**（無）連結以排程定期更新。

   如果防火牆有直接網際網路存取權，您可以只排程動態更新。如果已在區段中排程更新，則連結文字會顯示排程設定。

   應用程式與威脅更新有時候會包含與 安全搜尋強制 相關的 URL 篩選更新。

接下來的步驟：

1. 設定 URL 篩選設定檔，以定義貴組織的 Web 使用政策。
2. 測試您的 URL 篩選設定。

開始使用 URL 篩選

這可在何處使用？	我需要什麼？
• 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)	❑ Advanced URL Filtering 授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

開始使用 URL 篩選的第一步是瞭解您網路上使用者的 Web 活動模式。

為了安全地觀察這些模式，我們的建議如下：

- ❑ 查看 Palo Alto Networks 預先定義的 URL 類別。
- ❑ 將 URL 輸入到我們的 Test A Site 引擎，檢視 PAN-DB 如何分類這些 URL。
- ❑ （大多數情況下）建立一個被動 URL 篩選設定檔，以針對大部分類別發出警示。當您選擇 URL 類別的警示設定時，防火牆會將流量記錄到該類別。接著，您可以查看使用者正在造訪的網站，並針對 URL 類別和特定網站決定適當的網站存取權限。

  對所有 *Web* 活動發出警示的話可能會建立大量日誌檔案。因此，您可能只想將其當作初始部署的一部分。此時，您也可以啟用 *URL* 設定檔中的 ***Log container page only***（僅限日誌容器頁面）選項來減少 *URL* 篩選設定檔，如此一來只會記錄符合類別的主要頁面，不會記錄後續在容器頁面內載入的頁面或類別。
- ❑ 封鎖已知的不良 URL 類別：惡意軟體、命令和控制和網路釣魚。

- Strata Cloud Manager
- PAN-OS 和 Panorama

開始使用 Advanced URL Filtering (Strata Cloud Manager)

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

請切換到 ***PAN-OS & Panorama*** 頁籤並按照指示進行操作。

如果您使用 ***Strata Cloud Manager***，則請繼續此處操作。

STEP 1 | 使用 Test A Site 檢查 PAN-DB 如何對特定網站進行分類。

您也可以使用該平台針對您認為分類錯誤的任何網站要求變更類別。

STEP 2 | 建立一個會針對所有類別發出警示的被動 URL 存取管理設定檔。

防火牆會為 URL 類別中的網站產生一個 URL 篩選日誌項目，該項目的動作不是允許。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **Security Services**（安全服務） > **URL Access Management**（URL 存取管理）。
2. 在 URL 存取管理設定檔下，選取最佳實務設定檔旁的核取方框，然後 **Clone**（複製）該設定檔。

   複製的設定檔會顯示在名為 `best-practices-1` 的設定檔下。
3. 選取 **best-practices-1** 設定檔並將它重新命名。例如，將它重新命名為 `url-monitoring`。

STEP 3 | 針對所有類別發出 **alert**（警示），但惡意軟體、命令和控制、網路釣魚除外，這些類別應保持為封鎖。

1. 在 **Access Control**（存取控制）下，選取所有類別，然後排除惡意軟體、命令和控制和網路釣魚。
2. 在醒目顯示類別時，按一下 **Set Access**（設定存取）並選擇 **Alert**（警示）。
3. **Block**（封鎖）存取惡意軟體、命令和控制和網路釣魚。其他已知的危險 URL 類別：
   - 網路釣魚
   - 動態 DNS
   - 未知
   - 極端內容
   - 侵害著作權
   - 代理程式規避與匿名者
   - 新註冊的網域
   - 灰色軟體
   - 寄放
4. **Save**（儲存）設定檔。

STEP 4 | 將 URL 存取管理設定檔套用至允許信任區域中的用戶端流量流向網路的安全性政策規則。

僅當 URL 存取管理設定檔包含在安全性政策規則所參考的設定檔群組中，該設定檔才會處於啟用狀態。

依照步驟啟用 URL 存取管理設定檔（和任何安全性設定檔)。

確認您套用 *URL* 存取管理設定檔的安全性政策規則中的來源區域設為受保護的內部網路。

STEP 5 | **Push Config**（推送設定）以提交設定。

STEP 6 | 檢查 URL 日誌以瞭解您的使用者正在造訪哪些網站類別。遭封鎖的網站也會記錄。

關於檢視日誌及產生報告的資訊，請參閱監控 Web 活動。

選取 **Activity**（活動） > **Log Viewer**（日誌檢視器） > **URL**。URL 篩選報告讓您可以在 24 小時期間內檢視 Web 活動。

STEP 7 | 接下來的步驟：

- 對於您沒有允許或封鎖的所有內容，您可基於網站安全性使用風險類別編寫簡單政策。PAN-DB 依風險層級（高、中、低）分類每個 URL。雖然高風險和中等風險網站並未被確認為惡意網站，但其與惡意網站密切相關。例如，其可能與惡意網站處於同一網域，或不久之前裝載過惡意內容。

  您可以採取預防措施限制使用者與高風險網站交互，因為在某些情況下，您希望授予使用者存取權限的網站也可能帶來安全隱患（例如，您可能想允許開發人員使用開發人員部落格進行研究，但部落格是已知常用主機惡意軟體的類別）。
- 將 User-ID 與 URL 篩選配對，以根據組織或部門控制 Web 存取，並防止將公司認證提交到未經批准的網站：
  - URL 篩選會透過基於網站類別偵測公司提交到網站的認證來防止認證竊取。封鎖使用者向惡意網站和非受信任網站提交認證，警告使用者不要在未知網站上輸入公司認證，或在非公司網站上重複使用公司認證，並明確允許使用者向公司網站提交認證。
  - 使用被動 URL 存取管理設定檔來新增或更新安全性政策規則，以將其套用至部門使用者群組，例如行銷或工程部門。監控部門活動，然後獲取部門成員的意見反應，以瞭解對成員工作必不可少的 Web 資源。
- 考慮利用 URL 篩選來減少攻擊面的所有方法。例如，學校可以使用 URL 篩選來對學生實施嚴格的安全搜尋。或者，如果您有一個安全性操作中心，則您可僅為威脅分析人員提供對受危害或危險網站的密碼權限存取以進行研究。
- 遵循 URL 篩選最佳實務。

開始使用 Advanced URL Filtering (PAN-OS & Panorama)

STEP 1 | 使用 Test A Site 檢查 PAN-DB 如何對特定網站進行分類。

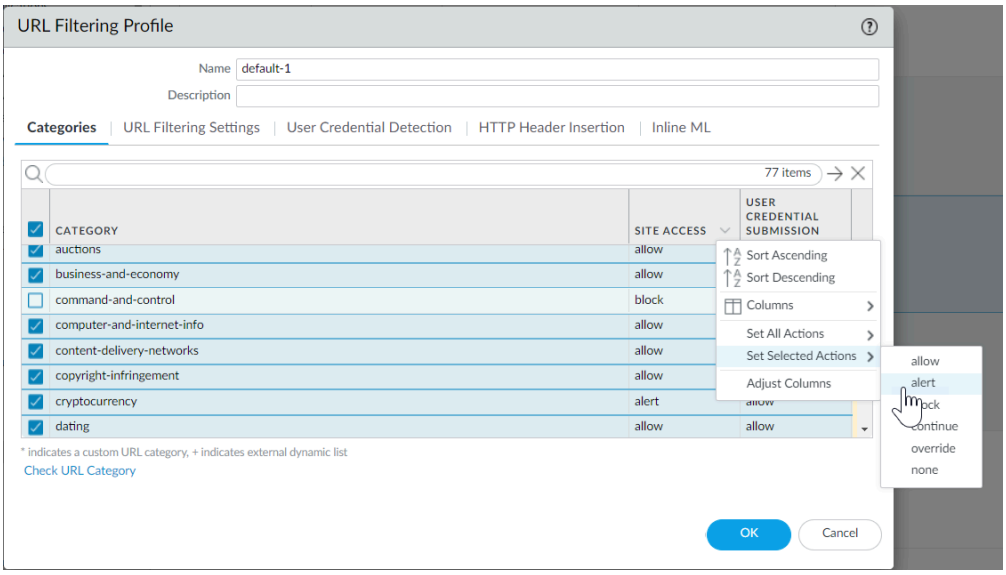
您也可以使用該平台針對您認為分類錯誤的任何網站要求變更類別。

STEP 2 | 建立一個會針對所有類別發出警示的被動 URL 篩選設定檔。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **URL Filtering**（**URL** 篩選）。
2. 選取預設設定檔，然後按一下 **Clone**（複製）。新設定檔將命名為 **default-1**。
3. 選取 **default-1** 設定檔並將它重新命名。例如，將它重新命名為 URL 監控。

STEP 3 | 將所有類別的動作設為 **alert**（警示），但惡意軟體、命令和控制、網路釣魚除外，這些類別應保持為封鎖。

1. 在列出全部 URL 類別的區段中，選取全部類別，然後取消選取惡意軟體、命令和控制以及網路釣魚。
2. 將滑鼠停留在*Action*（動作）欄標題右側，選取下拉式清單，然後選取 **Set Selected Actions**（設定所選動作），再選擇 **alert**（警示）。



3. **Block**（封鎖）存取已知危險 URL 類別。

   阻止對惡意軟體、網路釣魚、動態 *DNS*、未知、命令和控制、極端主義、侵犯著作權、*Proxy* 規避與匿名者網站、新註冊網域、灰色軟體和寄放 *URL* 類別的存取。
4. 按一下 **OK**（確定）來儲存設定檔。

STEP 4 | 將 URL 篩選設定檔套用至允許信任區域中的用戶端流量流向網路的安全性政策規則。

確認您新增 *URL* 存取管理設定檔的安全性政策規則中的來源區域設為受保護的內部網路。

1. 選取 **Policies**（政策） > **Security**（安全性）。然後，選擇要修改的安全性政策規則。
2. 在 **Actions**（動作）頁籤中，編輯設定檔設定。
3. 針對 **Profile Type**（設定檔類型）選取 **Profiles**（設定檔）。接著畫面將顯示設定檔清單。
4. 針對 **URL Filtering**（**URL** 篩選）設定檔，選取您剛建立的設定檔。
5. 按一下 **OK**（確定）儲存您的變更。

STEP 5 | **Commit**（提交）組態。

STEP 6 | 檢視 URL 篩選日誌以查看使用者存取的所有網站類別。也會記錄您設為封鎖的類別。

關於檢視日誌及產生報告的資訊，請參閱監控 Web 活動。

選取 **Monitor**（監控） > **Logs**（日誌） > **URL Filtering**（**URL** 篩選）。系統將為 URL 過濾資料庫內位於動作不是設為 **allow**（允許）之類別中的任何網站建立日誌項目。URL 篩選報告給您可以在 24 小時期間內檢視 web 活動。（**Monitor**（監控） > **Reports**（報告））。

STEP 7 | 接下來的步驟：

- PAN-DB 將每個 URL 分為最多四個類別，且每個 URL 都具備一種風險類別（高、中等和低）。雖然高風險和中等風險網站並未被確認為惡意網站，但其與惡意網站密切相關。例如，其可能與惡意網站處於同一網域，或不久之前裝載過惡意內容。對於您沒有允許或封鎖的所有內容，您可基於網站安全性使用風險類別編寫簡單政策規則。

  您可以採取預防措施限制使用者與高風險網站交互，因為在某些情況下，您希望授予使用者存取權限的網站也可能帶來安全隱患（例如，您可能想允許開發人員使用開發人員部落格進行研究，但部落格是已知常用主機惡意軟體的類別）。
- 將 User-ID 與 URL 篩選配對，以根據組織或部門控制 Web 存取，並防止將公司認證提交到未經批准的網站：
  - URL 篩選會透過基於網站類別偵測公司提交到網站的認證來防止認證竊取。封鎖使用者向惡意網站和非受信任網站提交認證，警告使用者不要在未知網站上輸入公司認證，或在非公司網站上重複使用公司認證，並明確允許使用者向公司網站提交認證。
  - 使用被動 URL 篩選設定檔新增或更新安全性政策規則，以便套用於部門使用者群組，例如，行銷或工程部門（**Policies**（政策） > **Security**（安全性） > **User**（使用者））。監控部門活動，然後獲取部門成員的意見反應，以瞭解對成員工作必不可少的 web 資源。
- 考慮利用 URL 篩選來減少攻擊面的所有方法。例如，學校可以使用 URL 篩選來對學生實施嚴格的安全搜尋。或者，如果您有一個安全性操作中心，則您可僅為威脅分析人員提供對受危害或危險網站的密碼權限存取以進行研究。
- 遵循 URL 篩選最佳實務。

設定 URL 篩選

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

規劃 URL 篩選部署之後，您應該對您的使用者所存取的網站類型有基本瞭解。使用此資訊來建立 URL 篩選設定檔，定義防火牆如何處理流向特定 URL 類別的流量。您也可以限制使用者可以提交公司認證的網站，或強制執行嚴格的安全搜尋。若要啟用這些設定，請將 URL 篩選設定檔套用至允許網頁存取的安全性政策規則。

- Strata Cloud Manager
- PAN-OS 和 Panorama

設定 URL 篩選 (Strata Cloud Manager)

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

請切換到 ***PAN-OS & Panorama*** 頁籤並按照指示進行操作。

如果您使用 ***Strata Cloud Manager***，則請繼續此處操作。

URL 篩選在 Strata Cloud Manager 中稱為 *URL* 存取管理

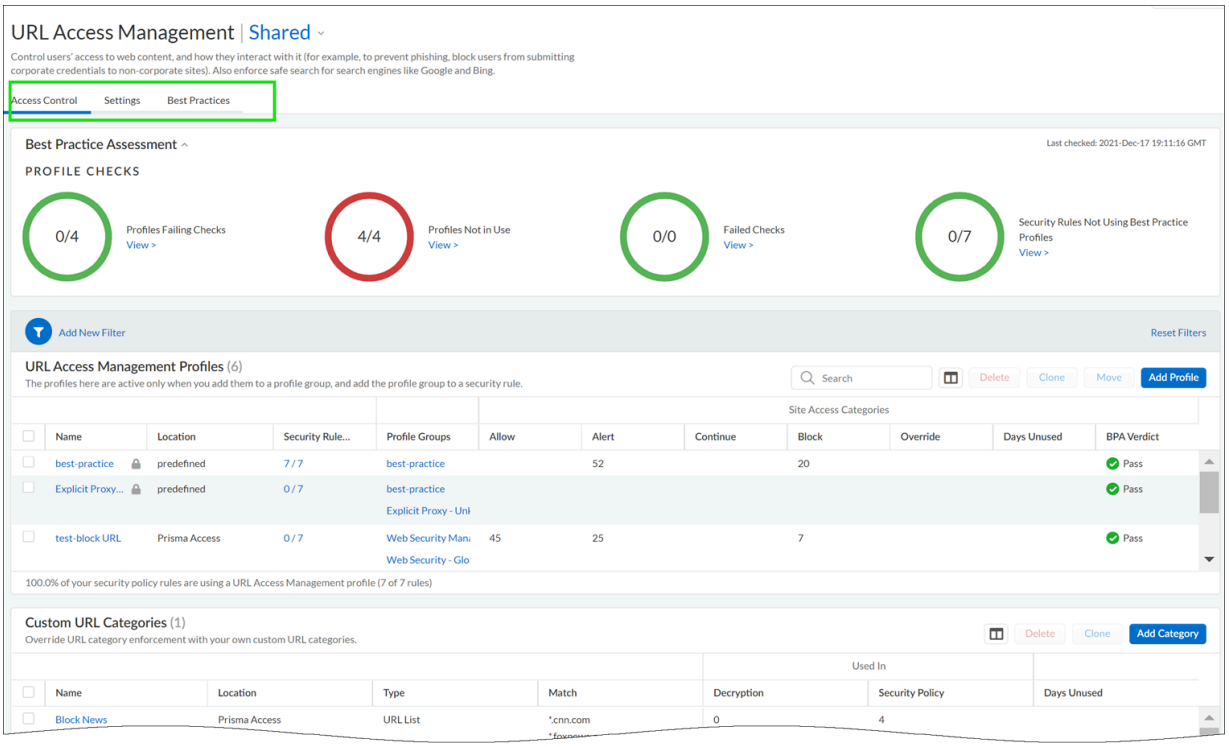
STEP 1 | 檢查您的 Prisma Access 訂閱包括進階 URL 篩選。

- 前往管理 > 服務設定 > 概要 > 授權以確認您的訂閱內容。

STEP 2 | 探索 URL 存取管理儀表板。

前往 **Manage**（管理） > **Configuration**（設定） > **Security Services**（安全服務） > **URL Access Management**（**URL** 存取管理）。

參考 **Access Control**（存取控制）、**Settings**（設定）和 **Best Practices**（最佳實務） 等頁籤內容，探索可用的 URL 篩選功能。



STEP 3 | 查看並自訂一般 URL 篩選設定。

在儀表板上，前往 **Settings**（設定）以查看套用於您 Prisma Access 環境的預設 URL 篩選設定，其中包括：

- URL 篩選逾時和查閱設定
- 部分管理員的 URL 篩選取代
- URL 篩選回應頁面
- 遠端瀏覽器隔離 (RBI) 設定

自動將結束權杖附加到自訂 ***URL*** 類別或外部動態清單中的 ***URL***

（*PAN-OS 10.1* 及更早版本）如果您將 *URL* 新增至自訂 *URL* 類別或 *URL* 清單類型的外部動態清單 *(EDL)* 且未附加尾端斜線 *(/)*，您可能會封鎖或允許比預期更多的 *URL*。例如，您輸入 ***example.com*** 而非 ***example.com/*** 的話，會將符合條件的 *URL* 範圍延伸至 *example.com.website.info* 或 *example.com.br*。*Prisma Access* 可以自動將尾端斜線附加到自訂 *URL* 類別或 *EDL* 中的 *URL*，如此一來，如果您輸入 ***example.com***，*Prisma Access* 會將它視為 ***example.com/***，且僅納入該網域及其子目錄的相符項目。前往 ***Settings***（設定）***> General Settings***（一般設定）並啟用 ***Append End Token to Entries***（將結束權杖附加至項目）選項。

（*PAN-OS 10.2* 及更高版本）*Prisma Access* 會自動在網域項目新增尾端斜線。

您可以為每個部署類型（行動使用者、遠端網路或服務連線）自訂這些設定。

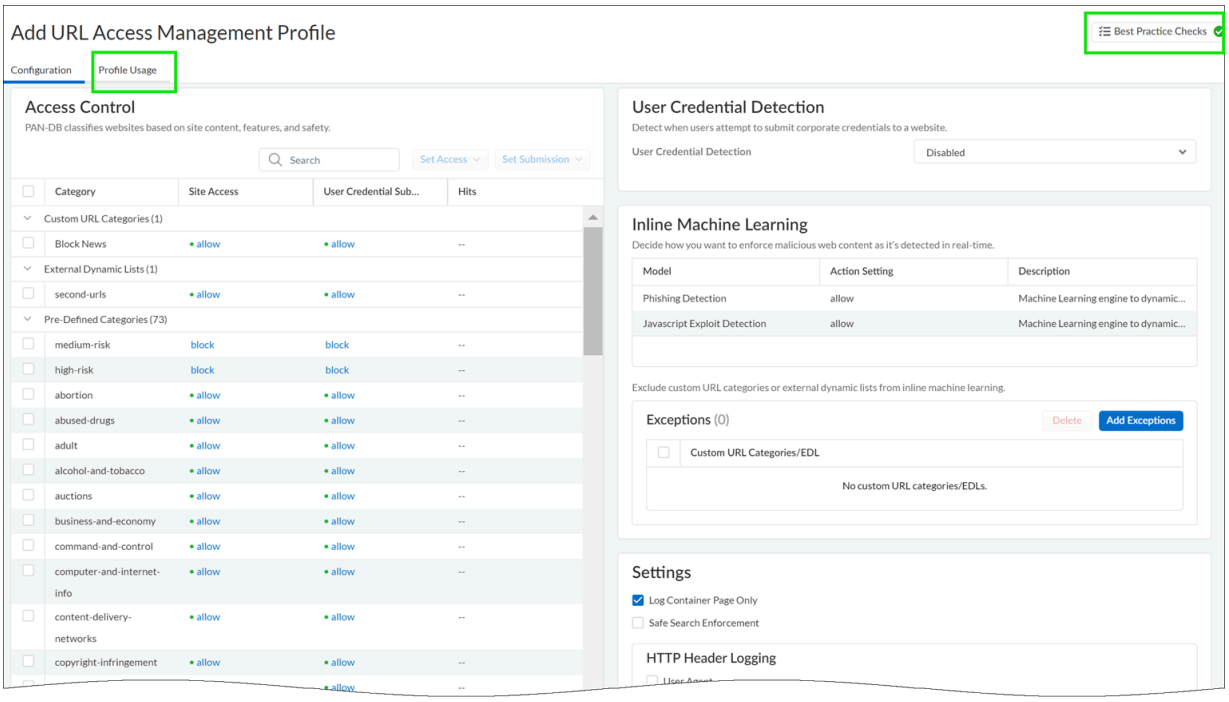
STEP 4 | 建立 URL 存取管理設定檔。

在 URL 存取管理儀表板上 **Add Profile**（新增設定檔）並繼續進行 Web 存取設定：

- **Access Control**（存取控制）顯示您可以為其定義網路存取與使用政策的 URL 類別與清單。依預設，所有類別的 **Site Access**（網站存取）和 **User Credential Submission**（使用者認證提交）權限設定為 **Allow**（允許）。
- 針對每個 URL 類別，設定 **User Credential Detection**（使用者認證偵測），讓使用者只能向指定 URL 類別中的網站提交認證。
- 啟用 **Safe Search Enforcement**（安全搜尋強制）以強制執行嚴格的安全搜尋篩選。
- 啟用 **Log Container Page Only**（僅記錄容器頁面），僅記錄符合指定內容類型的 URL。
- 啟用 **HTTP Header Logging**（**HTTP** 標頭記錄），即可深入檢視傳送至伺服器的 HTTP 要求的屬性。
- 使用 **Advanced URL Inline Categorization**（進階 **URL** 內嵌分類），以啟用和設定即時網頁分析並管理 URL 例外狀況。
  - **Enable local Inline Categorization**（啟用本機內嵌分類）—使用機器學習模型對 URL 流量進行即時分析，以偵測並防止惡意網路釣魚變體和 JavaScript 漏洞進入您的網路。
  - **Enable cloud Inline Categorization**（啟用雲端內嵌分類）—使用基於機器學習的偵測器補充本機內嵌 ML 使用的分析引擎，透過將可疑網頁內容轉送到雲端進行補充分析，進而達成對 URL 的即時分析。
  - 您可以定義 URL **Exceptions**（例外狀況），以從內嵌機器學習動作中指定排除特定網站。

請留意：

- 設定檔有內建最佳實踐檢查，以便您即時評估設定。
- 啟用設定檔之後，您可以檢查設定檔的使用情況，看看是否有任何安全性政策規則參考該設定檔。



STEP 5 | 將 URL 存取管理設定檔套用至安全性政策規則。

僅當 URL 存取管理設定檔包含在安全性政策規則所參考的設定檔群組中，該設定檔才會處於啟用狀態。

依照步驟啟用 URL 存取管理設定檔（和任何安全性設定檔)。請務必記得 **Push Config**（推送設定）

設定 URL 篩選 (PAN-OS & Panorama)

STEP 1 | 建立 URL 篩選設定檔。

如果您尚未安裝，則設定最佳做法 URL 篩選設定檔，以確保針對惡意軟體或攻擊性內容的 *URL* 提供保護。

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。

STEP 2 | 為每個 URL 類別定義網站存取。

選取 **Categories**（類別），然後為每個 URL 類別定義網站存取：

- **allow**（允許）前往該 URL 類別的流量；將不會記錄允許的流量。
- 選取 **alert**（警示），以便能夠查看使用者存取的網站。允許該類別相符的流量但會產生 URL 篩選日誌，以記錄使用者存取該類別中某個網站的時間。
- 選取 **block**（封鎖）可拒絕存取符合該類別的流量，並允許記錄遭封鎖的流量。
- 選取 **continue**（繼續）以向使用者顯示警告頁面，要求他們按一下 **Continue**（繼續）以繼續前往該類別中的網站。
- 若要在使用者提供設定的密碼時僅允許存取權，請選取取代。有關更多詳細資料，請參閱允許使用密碼存取特定網站。

STEP 3 | 設定 URL 篩選設定檔，以偵測向屬於被允許 URL 類別的網站提交公司認證的活動。

為以確保最佳效能和低誤報率，對於從未曾觀測到載有惡意軟體或網路釣魚內容的網站關聯的任何 *App-ID*™—即使您在相應類別中啟用了檢查，防火牆也將自動跳過檢查認證提交。防火牆跳過認證檢查的網站的清單會透過應用程式與威脅內容更新自動更新。

1. 選取 **User Credential Detection**（使用者認證偵測）。
2. 從 **User Credential Detection**（使用者認證偵測）下拉式清單中選取一種檢查公司認證提交（向網頁提交）的方法：
   - 使用 **IP** 使用者對應—檢查有效的企業使用者名稱提交，並驗證使用者名稱是否與登入至工作階段來源 IP 位址的使用者相符。防火牆會針對 IP 位址到使用者名稱的對應表比對使用者所提交的使用者名稱。您可使用將 IP 位址對應至使用者中所述的任何使用者對應方法。
   - **Use Domain Credential Filter**（使用網域認證篩選器）—檢查有效的公司使用者名稱和密碼提交，並確認使用者名稱已對應到已登入使用者的 IP 位址。關於如何設定 User-ID 以啟用此方法的說明，請參閱使用基於 Windows 的 User-ID 代理程式設定認證偵測。
   - **Use Group Mapping**（使用群組對應）—根據您在設定防火牆對應使用者到群組時填入的使用者到群組對應表格，檢查有效的使用者名稱提交。

     對於群組對應，您可以將認證偵測套用至目錄的 **any**（任何）部分或一特定群組，例如有權存取最敏感應用程式的 IT 群組。

     在沒有唯一結構化的使用者名稱的環境中，此方法容易產生誤報，因此，您應僅使用此方法來保護您的高價值使用者帳戶。
3. 設定防火牆用於記錄公司認證提交偵測的 **Valid Username Detected Log Severity**（有效使用者名稱偵測日誌嚴重性）（預設值為中等）。

STEP 4 | 設定 URL 篩選設定檔，以使用本機內嵌分類即時偵測網路釣魚和惡意 JavaScript。

STEP 5 | 根據 URL 類別允許或封鎖使用者提交公司認證到網站，以封鎖認證網路釣魚。

對於從未曾觀測到載有惡意軟體或網路釣魚內容的網站關聯的 *App-ID*，即使您在相應類別中啟用了檢查，防火牆也將自動跳過檢查認證提交，以確保最佳效能和低誤報率。防火牆跳過認證檢查的網站的清單會透過應用程式與威脅內容更新自動更新。

1. 對於您允許 **Site Access**（網站存取）的每個 URL 類別，選取您希望如何處理 **User Credential Submissions**（使用者認證提交）：
   - **alert**（警示）—允許使用者將認證提交至網站，但在每次使用者將認證提交至此 URL 類別中的網站時產生 URL 篩選警示日誌。
   - 允許（預設值）—允許使用者將認證提交至網站。
   - **block**（封鎖）—顯示防網路釣魚封鎖頁面，以阻止使用者向網站提交認證。
   - **continue**（繼續）—顯示防網路釣魚繼續頁面，要求使用者按一下**Continue**（繼續）才能存取網站。
2. 設定 URL 篩選設定檔，以偵測向屬於被允許 URL 類別的網站提交公司認證的活動。

STEP 6 | 定義 URL 類別例外清單，指定無論 URL 類別為何都應封鎖或允許的網站。

例如，要減少 URL 篩選日誌，您可能希望將您的公司網站新增到允許清單中，這樣就不會為這些網站產生日誌，或如果某網站被過度使用且與工作無關，則您可以將該網站新增到封鎖清單。

針對自訂 URL 類別設定的原則動作，其執行優先級高於外部動態清單中的相符 URL。

封鎖清單中的網站流量一律封鎖，無論相關聯類別的動作為何，允許清單中的 URL 流量則一律允許。

關於正確格式與萬用字元使用的詳細資訊，請參閱 URL 類別例外指南。

STEP 7 | 啟用安全搜尋強制。

STEP 8 | 僅記錄使用者造訪的 URL 篩選事件頁面。

1. 選取 **URL Filtering Settings**（**URL** 篩選設定）並啟用 **Log container page only**（僅記錄容器頁面）（預設值），因此防火牆只會記錄符合類別的主要頁面，不會記錄容器頁面內後續載入的頁面或類別。
2. 若要啟用記錄所有的頁面和類別，請停用 **Log container page only**（僅限日誌容器頁面）選項。

STEP 9 | 為一或多個支援的 HTTP 標頭欄位啟用HTTP 標頭記錄。

選取 **URL Filtering Settings**（**URL** 篩選設定），然後選取一或多個下列欄位進行記錄：

- 使用者代理程式
- 參照位址
- **X-Forwarded-For**

STEP 10 | 儲存 URL 篩選設定檔。

按一下 **OK**（確定）。

STEP 11 | 將 URL 篩選設定檔套用至允許信任區域中的用戶端流量流向網路的安全性政策規則。

確認您新增 *URL* 篩選設定檔的安全性政策規則中的來源區域設為受保護的內部網路。

1. 選取 **Policies**（政策） > **Security**（安全性）。然後，選擇要修改的安全性政策規則。
2. 在 **Actions**（動作）頁籤中，編輯設定檔設定。
3. 針對 **Profile Type**（設定檔類型）選取 **Profiles**（設定檔）。接著畫面將顯示設定檔清單。
4. 針對 **URL Filtering**（**URL** 篩選）設定檔，選取您剛建立的設定檔。
5. 按一下 **OK**（確定）儲存您的變更。

STEP 12 | **Commit**（提交）組態。

STEP 13 | 測試您的 URL 篩選設定。

STEP 14 | （最佳實務）在防火牆執行 URL 類別查閱時，啟用 **Hold client request for category lookup**（對類別查閱保留用戶端要求）以封鎖用戶端要求。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Content - ID**（內容-**ID**）。
2. 選取 **Hold client request for category lookup**（對類別查閱保留用戶端要求）。
3. **Commit**（提交）您的變更。

STEP 15 | 設定 URL 類別查閱逾時之前的時間（秒）。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Content - ID**（內容-**ID**） > 齒輪圖示。
2. 在 **Category lookup timeout (sec)**（類別查閱逾時（秒））中輸入一個數字。
3. 按一下 **OK**（確定）。
4. **Commit**（提交）您的變更。

設定內嵌分類

這可在何處使用？	我需要什麼？
• 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)	❑ Advanced URL Filtering 授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

若要啟用內嵌分類，請將有內嵌分類設定的 URL 篩選設定檔附加到安全性政策規則（請參閱設定基本安全性政策）。

URL 篩選本機內嵌分類目前在 *VM-50* 或 *VM50L* 虛擬設備上不受支援。

- Strata Cloud Manager
- PAN-OS 和 Panorama

設定內嵌分類 (Strata Cloud Manager)

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

請切換到 ***PAN-OS & Panorama*** 頁籤並按照指示進行操作。

如果您使用 ***Strata Cloud Manager***，則請繼續此處操作。

STEP 1 | 更新或建立 URL 存取管理設定檔。

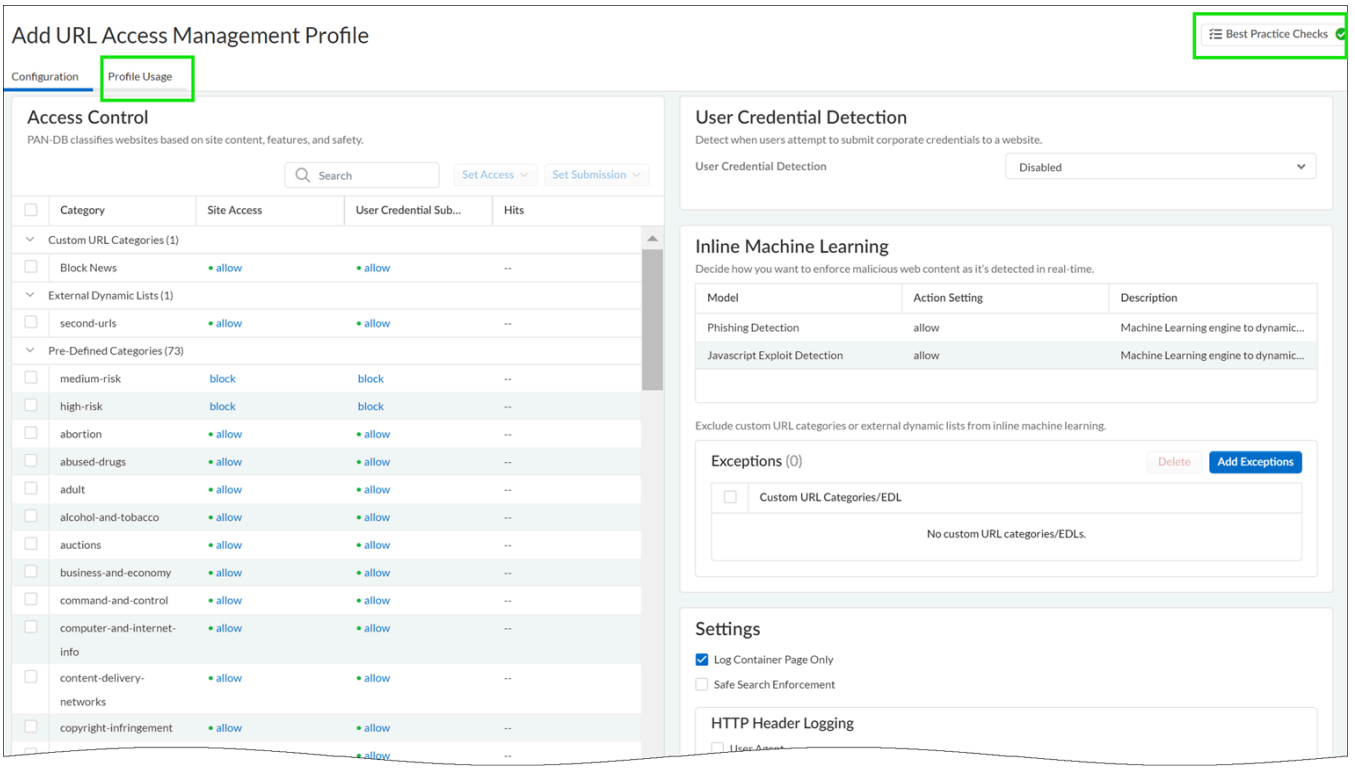
1. 前往 **Manage**（管理） > **Configuration**（設定） > **Security Services**（安全服務） > **URL Access Management**（URL 存取管理）。
2. 在 URL 存取管理儀表板上，選取 URL 存取管理設定檔或 **Add Profile**（新增設定檔）。

   如果您建立了新的設定檔，請在設定檔中進行設定，例如 URL 類別的網站存取（**Access Control**（存取控制））。設定 URL 篩選（雲端管理）說明可用的設定。
3. 在 **Advanced URL Inline Categorization**（進階 **URL** 內嵌分類下，選擇內嵌分類類型。

   兩種選項皆會啟用即時網頁分析並管理 URL 例外狀況。

   - **Enable cloud Inline Categorization**（啟用雲端內嵌分類）—使用基於機器學習的偵測器補充本機內嵌 ML 使用的分析引擎，透過將可疑網頁內容轉送到雲端進行補充分析，進而達成對 URL 的即時分析。
   - **Enable local Inline Categorization**（啟用本機內嵌分類）—使用機器學習模型對 URL 流量進行即時分析，以偵測並防止惡意網路釣魚變體和 JavaScript 漏洞進入您的網路。

- 您也可以定義 URL **Exceptions**（例外狀況），以從內嵌機器學習動作中排除特定網站。



4. **Save**（儲存）設定檔。

STEP 2 | 將 URL 存取管理設定檔套用至安全性政策規則。

若要啟用 URL 存取管理設定檔（以及任何安全性設定檔），請將其新增至設定檔群組，並在安全性政策規則中參照該設定檔群組。

設定內嵌分類 (PAN-OS & Panorama)

在 *PAN-OS 10.2* 中，「*URL* 篩選內嵌 *ML*」功能已重新命名為「內嵌分類」。因此，*PAN-OS 10.1* 的工作使用「*URL* 篩選內嵌 *ML*」，而 *PAN-OS 10.2* 及更高版本的工作使用「內嵌分類」。如需更多詳細資訊，請參閱 PAN-OS 10.2 升級/降級考量事項。

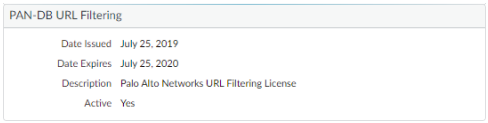
- PAN-OS 10.1
- PAN-OS 10.2 及更新版本

設定內嵌分類 (PAN-OS 10.1)

STEP 1 | 登入 PAN-OS 網頁介面。

STEP 2 | 確認您有啟用進階 URL 篩選或舊版 URL 篩選授權。

選取 **Device**（裝置） > **Licenses**（授權），然後確認 URL 篩選授權可用且未過期。

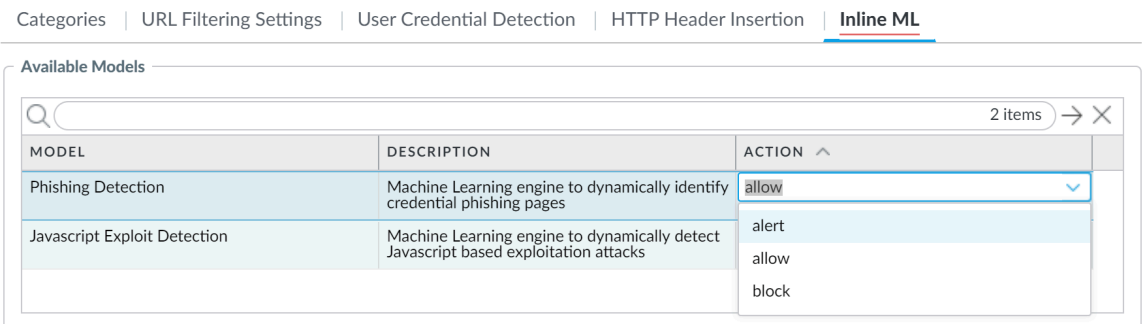


STEP 3 | 在 URL 篩選設定檔中設定 URL 篩選內嵌 ML 設定。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **URL Filtering**（URL 篩選），然後 **Add**（新增）或選取 URL 篩選設定檔。
2. 選取 **Inline ML**（內嵌 **ML**），然後為每個內嵌 ML 模型定義一個 **Action**（動作）。

   每種惡意網頁內容類型都有兩個分類引擎：**Phishing**（網路釣魚）和 **JavaScript Exploit**（**JavaScript** 漏洞）。

   - **Block**（封鎖）—當防火牆偵測到有網路釣魚內容的網站時，防火牆會產生一個 URL 篩選日誌項目。
   - **Alert**（警示）—防火牆允許存取網站，且會產生一個 URL 篩選日誌項目。
   - **Allow**（允許）—防火牆允許存取網站，但不會產生 URL 篩選日誌項目。



3. 按一下 **OK**（確定）儲存您的變更。
4. **Commit**（提交）您的變更。

STEP 4 | （選用）如果您遇到誤判，請新增 URL 例外狀況到您的 URL 篩選設定檔。

您可以從 URL 篩選設定檔指定一個外部動態清單，或從 URL 篩選日誌新增一個網頁項目到自訂 URL 類別，來新增例外狀況。

1. 選取 **Objects**（物件）**> Security Profiles**（安全性設定檔）**> URL Filtering**（**URL** 篩選）。
2. 選取您想要為其排除特定 URL 的 URL 篩選設定檔，然後選取 **Inline ML**（內嵌 **ML**）。
3. **Add**（新增）已存在的 URL 類型的外部動態清單。如果沒有可用清單，則建立一個新的外部動態清單。
4. 按一下 **OK**（確定）儲存您的變更。
5. **Commit**（提交）您的變更。

從 URL 篩選日誌項目新增檔案例外狀況。

1. 選取 **Monitor**（監控） **> Logs**（日誌） **> URL Filtering**（**URL** 篩選），然後篩選日誌以找出內嵌 ML 裁定為 **malicious-javascript** 或 **phishing** 的 URL 項目。為您想要為其建立例外狀況的 URL 選取 URL 篩選日誌。
2. 轉至 **Detailed Log View**（詳細日誌檢視）並向下滾動到 **Details**（詳細資料）面板，然後選取 **Inline ML Verdict**（內嵌 **ML** 裁定）旁邊的 **Create Exception**（建立例外狀況）。

3. 為 URL 例外狀況選取一個自訂類別，然後按一下 **OK**（確定）。

   新的 URL 例外狀況可在其新增到的清單中找到，在 **Objects**（物件） **> Custom Objects**（自訂物件） **> URL Category**（**URL** 類別）下。

STEP 5 | （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
```

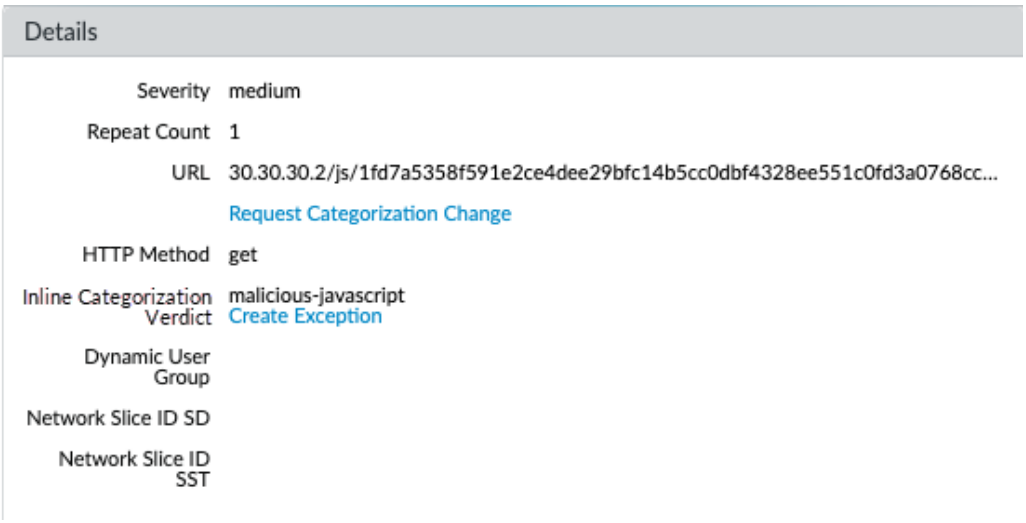
例如：

```
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 ML 網域 ml.service.paloaltonetworks.com 未遭封鎖。

STEP 6 | 測試您的 URL 篩選部署。

若要檢視有關已使用 URL 篩選內嵌 ML 處理之網頁的資訊，請基於 **Inline ML Verdict**（內嵌 **ML** 裁定）篩選日誌（**Monitor > Logs > URL Filtering**（監控 **>** 日誌 **>** URL 篩選））。確定為包含威脅的網頁按 **phishing** 或 **malicious-javascript** 的裁定進行分類。例如：



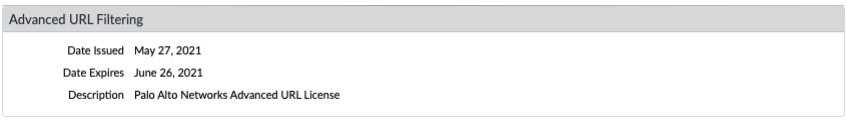
設定內嵌分類 (PAN-OS 10.2 和更新版本)

STEP 1 | 登入 PAN-OS 網頁介面。

STEP 2 | 若要利用內嵌分類，您必須具有作用中的進階 URL 篩選訂閱。

如果您是舊版 *URL* 篩選訂閱的現有持有者，則可以啟用本機內嵌分類。

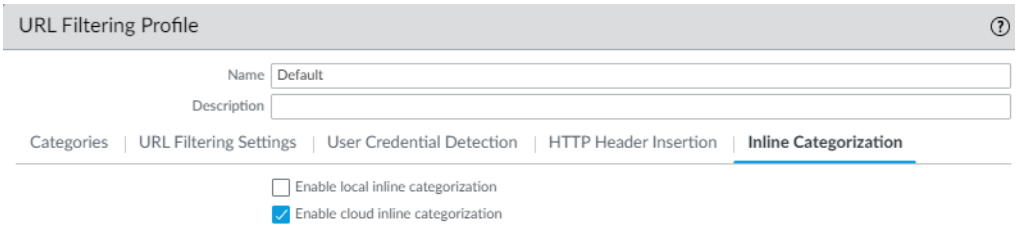
確認您具有進階 URL 篩選訂閱。若要確認當前哪些訂閱具有作用中的授權，請選取 **Device**（裝置） > **Licenses**（授權），並確認有適當的授權可供使用並且該授權沒有過期。



STEP 3 | 更新或建立新的 URL 篩選設定檔以啟用雲端內嵌分類。

本機和雲端內嵌分類使用的政策動作取決於 ***Categories***（類別）頁籤下進行的設定。

1. 選取一個現有 **URL Filtering Profile**（**URL** 篩選設定檔）或 **Add**（新增）一個新的設定檔（**Objects**（物件） > **Security Profiles**（安全性設定檔） > **URL Filtering**（**URL** 篩選））。
2. 選取您的 URL 篩選設定檔，然後移至**Inline Categorization**（內嵌分類）並啟用您要部署的內嵌分類方法。
   - **Enable cloud inline categorization**（啟用雲端內嵌分類）—一種基於雲端的內嵌深度學習引擎，可即時分析可疑網頁內容，以保護使用者免受零時差網路攻擊（包括有針對性的網路釣魚攻擊）和其他使用進階規避技術的基於網路的攻擊。
   - **Enable local inline categorization**（啟用本機內嵌分類）—基於防火牆的偵測引擎，使用機器學習技術來防止網頁中嵌入的 JavaScript 漏洞和網路釣魚攻擊的惡意變體。



3. 按一下 **OK**（確定）並 **Commit**（交付）變更。

STEP 4 | （選用）如果您遇到誤判，請新增 URL 例外狀況到您的 URL 篩選設定檔。您可以透過在 URL 篩選設定檔中指定外部動態清單或自訂 URL 類別清單來新增例外。指定的例外套用於雲端和本機內嵌分類。

透過將項目新增到自訂 *URL* 類別（***Objects***（物件） > ***Custom Objects***（自訂物件） > ***URL Category***（***URL*** 類別））的其他機制建立的 *URL* 例外

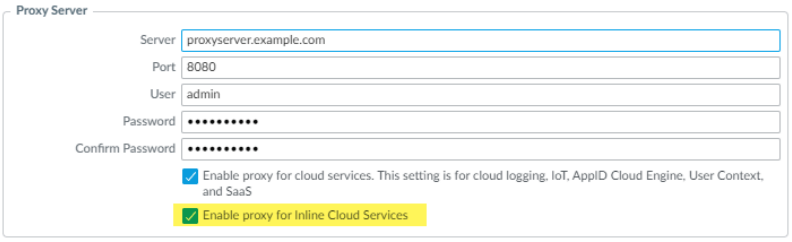
也可以用作內嵌分類的例外。

1. 選取 **Objects**（物件）> **Security Profiles**（安全性設定檔）> **URL Filtering**（**URL** 篩選）。
2. 選取您想要為其排除特定 URL 的 URL 篩選設定檔，然後選取 **Inline Categorization**（內嵌分類）。
3. 按一下 **Add**（新增）以選取一個基於 URL 的現存外部動態清單或自訂 URL 類別。如果這兩者都沒有，則分別建立一個新的外部動態列表或自訂 URL 類別。
4. 按一下 **OK**（確定）儲存 URL 篩選設定檔並 **Commit**（提交）您的變更。

STEP 5 | （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. （僅適用於以下版本：（PAN-OS 10.2.11 及更新版本，以及 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 6 | （選用）設定防火牆用於處理內嵌分類服務要求的雲端內容完全合格網域名稱 (FQDN)。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。

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。

確認防火牆使用適用於您所在區域的正確內容雲端 FQDN（**Device**（裝置） > **Setup**（設定） > **Content-ID**（內容 **ID**） > **Content Cloud Setting**（內容雲端設定）），並視需要變更 FQDN：

- 美國—**us.hawkeye.services-edge.paloaltonetworks.com**
- 歐盟—**eu.hawkeye.services-edge.paloaltonetworks.com**
- 英國—**uk.hawkeye.services-edge.paloaltonetworks.com**

  基於英國的雲端內容 *FQDN* 透過連接至位於歐盟 *(eu.hawkeye.services-edge.paloaltonetworks.com)* 的後端服務，提供進階 *URL* 篩選內嵌分類服務支援。
- 亞太地區—**apac.hawkeye.services-edge.paloaltonetworks.com**

STEP 7 | （選用）驗證防火牆到內嵌分類伺服器的連線狀態。

1. ml.service.paloaltonetworks.com 伺服器為與雲端和本機內嵌分類操作相關的基於防火牆的元件提供定期更新。

   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。

2. 雲端內嵌分類使用 hawkeye.services-edge.paloaltonetworks.com 伺服器來處理服務要求。

   在防火牆上使用以下 CLI 命令檢視連線狀態。

   ```
   show ctd-agent status security-client
   ```

   例如：

   ```
   show ctd-agent status security-client ...Security Client
    AceMlc2(1) Current cloud server: hawkeye.services-
   edge.paloaltonetworks.com Cloud connection: connected ...
   ```

   為簡潔起見，縮短了 *CLI* 輸出。

   如果無法連接至進階 URL 篩選雲端服務，請驗證以下網域是否未被封鎖：hawkeye.services-edge.paloaltonetworks.com。

STEP 8 | 安裝用於向進階 URL 篩選雲端服務進行驗證的更新防火牆裝置憑證。對為雲端內嵌分類啟用的所有防火牆重複此動作。

STEP 9 | 測試您的 URL 篩選部署。

URL 類別例外

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

您可在 URL 類別執行中排除特定網站，確保這些網站得以封鎖或允許，而不受與其 URL 類別相關聯之原則動作的影響。例如，您可以封鎖社交網路 URL 類別，但允許存取 LinkedIn。若要對 URL 類別政策執行建立例外狀況：

- 將您要封鎖或允許的網站 IP 位址或 URL 新增到類型為 **URL List**（**URL** 清單）的自訂 URL 類別。然後，在 URL 篩選設定檔中定義類別的網站存取權。最後，將此設定檔附加至安全性原則規則。

  您也可以使用自訂 *URL* 類別作為安全性政策規則中的比對準則。請務必將例外規則放在封鎖或允許 *URL* 例外所屬類別的任何規則之上。
- 將要封鎖或允許的網站的 URL 新增到類型為 **URL List**（**URL** 清單）的外部動態清單。然後，在 URL 篩選設定檔中使用外部動態清單或作為安全性政策規則中的比對規則。使用外部動態清單的好處是您無需在防火牆上執行設定變更或提交即可更新清單。

不應將類型為 ***URL List***（***URL*** 清單）的外部動態清單與類型為網域清單外部動態清單或 IP 位址類型混淆。*URL* 的外部動態清單允許網域和 *IP* 位址，但反之則不然，並會導致項目無效。

- URL 類別例外指南
- 建立一個自訂 URL 類別
- 在 URL 篩選設定檔中使用外部動態清單

URL 類別例外指南

這可在何處使用？	我需要什麼？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager)	❑ 進階 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。

這可在何處使用？	我需要什麼？
• NGFW (Managed by PAN-OS or Panorama)	• Prisma Access 授權包括 *Advanced URL Filtering* 功能。

以下指引說明如何填入 URL 類別例外清單（自訂 URL 類別或 URL 的外部動態清單）：我們提供範例說明如何使用萬用字元和特定項目。

URL 類別例外清單的基本方針

在將項目新增到 URL 類別例外清單之前，請考慮該項目可能具有的潛在相符項。以下指引指定如何建立封鎖或允許所需網站和頁面的項目。

依預設，防火牆會自動將尾端斜線 (/) 附加到不以尾端斜線 (/) 或星號 (*) 結尾的網域項目。新增尾端斜線會變更防火牆認為是相符項並對其強制實施政策的 URL。在不含萬用字元的網域項目中，尾端斜線將相符項限制為給定網域及其子目錄。例如，**example.com**（處理后 **example.com/**）與自身以及 **example.com/search** 相符。

在萬用字元網域項目（帶有星號或插入號的項目）中，尾端斜線將相符項限制為符合指定模式的 URL。例如，要比對項目 ***.example.com**，URL 必須至少包含一個子網域並以根網域結尾 **example.com**。模式為：**<subdomain>example.com**；*news.example.com* 是相符項，但 **example.com** 不是，因為它缺少子網域。

我們建議手動新增尾端斜線，以便為檢查項目的任何人闡明項目的預期相符行為。尾端斜線如果是由防火牆新增的，則不可見。

執行 PAN-OS® 10.2 的 Panorama™ 管理伺服器只能為同一軟體版本的防火牆啟用此功能。若要為執行 PAN-OS 10.1 或更早版本的防火牆啟用此功能，請在每個防火牆上使用以下 CLI 命令：

```
admin@PA-850> debug device-server append-end-token on
```

```
admin@PA-850> configure
```

```
admin@PA-850# commit
```

若要停用此功能，請選取 **Device**（裝置） > **Setup**（設定） > **Content-ID**（內容 **ID**） > **URL Filtering**（**URL** 篩選）。然後，取消選取 **Append Ending Token**（附加結束語彙基元）。但是，如果停用此功能，您可以封鎖或允許存取比預期更多的 URL。對於不以 / 或 * 結尾的網域項目，防火牆會將隱式星號新增至這些網域項目的末尾。例如，如果您將 **example.com** 新增到允許網站的 URL 清單中，防火牆會將該項目解釋為 **example.com.***。因此，防火牆允許存取 **example.com.domain.xyz** 等網站。URL 類別例外（PAN-OS 10.1 及更早版本）介紹了停用此功能時防火牆的行為。

- 清單項目不區分大小寫。
- 省略 URL 項目中的 `http` 與 `https`。
- 每個 URL 項目長度最多為 255 個字元。

- 輸入要封鎖或允許的 IP 位址或 URL 的精確相符項，或使用萬用字元建立模式匹配。

  不同的項目會導致不同的精確相符項。如果輸入特定網頁的 *URL* (***example.com/contact***)，則防火牆會將相符項限制為僅該網頁。網域的精確比對將相符項限制為網域本身及其子目錄。
- 如果原始項目可以從多個 URL 存取，請考慮將最常用於存取網站或頁面的 URL 新增到例外清單（例如，**blog.paloaltonetworks.com** 和 **paloaltonetworks.com/blog**）。
- 項目 **example.com** 與 **www.example.com** 不同。網域名稱相同，但第二個項目包含 *www* 子網域。

Palo Alto Networks 不支援在自訂 *URL* 類別或外部動態清單項目中使用規則運算式。您必須知道特定的 *URL*，或者使用萬用字元和以下字元構造要比對的 *URL* 模式：*. / ? & = ; +*。

URL 類別例外清單的萬用字元方針

您可以在 URL 類別例外清單中使用星號 (*) 和插入號 (^)，以將單個項目設定為比對多個子網域、網域、頂級網域 (TLD) 或頁面，而無需指定精準的 URL。

如何使用星號 (*) 和插入號 (^) 萬用字元

以下字元是語彙基元分隔符：**. / ? & = ; +**。每一個由此類字元中的一個或兩個字元分隔的字串為一個語彙基元。使用萬用字元作為語彙基元預留位置，表明特定語彙基元可包含任何值。在項目 **docs.paloaltonetworks.com** 中，語彙基元是“docs”、“paloaltonetworks”和“com”。

下表介紹了星號和插入號的工作方式，並提供了範例。

*	^
指示一個或多個可變子網域、網域、TLD 或子目錄。 可以在尾端斜線後面使用星號，例如，**example.com/***。 範例：***.domain.com** 與 **docs.domain.com** 和 **abc.xyz.domain.com** 相符。	指示一個可變子網域、根網域或 TLD。 尾端斜線後面不能使用插入號。以下項目無效：**example.com/^**。 範例：**^.domain.com** 與 **docs.domain.com** 和 **blog.domain.com** 相符。
要點：與插入號相比，星號符合的 URL 範圍更大。星號對應於任意數量的連續語彙基元，而插入號正好對應於一個語彙基元。 像 **xyz.*.com** 這樣的項目符合的網站數量比 **xyz.^.^.com** 多；**xyz.*.com** 符合字串之間含有任意數量的語彙基元的網站，而 **xyz.^.^.com** 符合正好含有兩個語彙基元的網站。	

- 萬用字元必須是語彙基元中的唯一字元。例如，**example*.com** 是一個無效項目，因為 **example** 和 ***** 位於同一個語彙基元中。但是，一個項目可以在多個語彙基元中包含萬用字元。
- 您可以在同一項目中使用星號和插入號（例如，***.example.^**）。

不要以連續星號 (*) 或九個以上的連續插入號 (^) 來建立項目—這些項目可能會影響防火牆效能。

例如，請勿新增像 ***mail.*.*.com*** 這樣的項目。視乎您要控制其存取的網站範圍而定，輸入 ***mail.*.com*** 或 ***mail.^.^.com***。

URL 類別例外清單—範例

下表顯示了範例 URL 清單項目、相符網站以及防火牆自動附加尾端斜線時相符行為的說明。

此表中的項目不包含尾端斜線，以反映防火牆在背景將斜線附加到適用項目。此外，例外清單可能包含在尾端斜線指引之前新增的項目。URL 類別例外清單—範例 *(PAN-OS 10.1)* 顯示依預設防火牆不附加尾端斜線時的相符行為。

我們建議手動新增尾端斜線，以便為檢查項目的任何人闡明項目的預期相符行為。如果由防火牆新增，則尾端斜線不可見。

URL 例外清單項目	相符網站	解釋
範例集 **1**		
paloaltonetworks.com	paloaltonetworks.com paloaltonetworks.com/network-security/security-subscriptions	防火牆將尾端斜線附加到項目，將相符項限制為精確的網域及其子目錄。
paloaltonetworks.com/example	paloaltonetworks.com/example	防火牆不會將尾端斜線附加到此項目，因為子目錄 **example** 跟在網域後面。當您輸入特定網頁的 URL 時，防火牆會將例外動作套用於指定的網頁。
範例集 **2**—星號		
*.example.com	www.example.com docs.example.com support.tools.example.com	星號將相符項擴展到所有 **example.com** 子網域。 防火牆會將尾端斜線附加到項目，但不包括根網域 **example.com** 右側的相符項。
mail.example.*	mail.example.com mail.example.co.uk	星號將相符項擴展到遵循 **mail.example.<*TLD*>** 模式的任何 URL。

URL 例外清單項目	相符網站	解釋
在啟用或不啟用尾端斜線功能的情況下，此項目產生相同的相符項。	mail.example.com/#inbox	
example.*.com	example.yoursite.com example.es.domain.com example.abc.xyz.com	星號將相符項擴展到最左側的子網域是 **example** 且頂級網域是 **com** 的 URL。尾端斜線會排除 TLD 右側的相符項。
example.com/*	example.com/photos example.com/blog/latest 任何 example.com 子目錄	網域後跟一個 / 和一個星號，表示子目錄必須存在。星號用作任何 **example.com** 子目錄的語彙基元預留位置。 防火牆不會附加尾端斜線，因為該項目以星號結尾。
範例集 **3**—插入號		
google.^ *example.co.^* 等模式通常用於比對特定於國家/地區的網域（如 ***example.co.jp***）。但是，通用頂級網域 (*gTLD*) 會產生諸如以下模式：*example.co.^* 與 *example.co.info* 或 *example.co.amzn* 相符，這些網域可能不屬於同一組織。	google.com google.info google.com/search?q=paloaltonetworks	插入號將相符項擴展到以 **google** 開頭並以單個 TLD 結尾的 URL。尾端斜線會排除最後一個語彙基元右側的相符項。
^.google.com	www.google.com news.google.com	插入號將相符項擴展到 **google.com** 的單一層級子網域。防火牆會將尾端斜線附加到項目，但根網域右側的相符項除外。

URL 例外清單項目	相符網站	解釋
^.^.google.com	www.maps.google.com support.tools.google.com	這兩個插入號將相符項擴展到在 **google.com** 前面包含兩個連續子網域的 URL。防火牆會將尾端斜線新增到項目，但根網域右側的相符項除外。
google.^.com	google.example.com google.company.com	插入號將相符項擴展到 URL，其中 **google** 是最左側的子網域，後跟一個語彙基元和 **.com**。 防火牆會將尾端斜線新增到項目，但 TLD 右側的相符項除外。

建立一個自訂 URL 類別

這可在何處使用？	我需要什麼？
• 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)	❑ Advanced URL Filtering 授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

您可以建立自訂 URL 類別來定義 URL 類別強制執行的例外情況，或從多個類別中定義新的 URL 類別。

定義 **URL** 類別強制執行的例外情況（**URL** 清單）

指定您希望獨立於其預先定義的 URL 類別之外，強制執行的 URL 清單（在單一自訂類別下分組）。您可以在套用於安全性政策規則的 URL 篩選設定檔中控制對此類別的存取，或使用該類別作為安全性政策規則中的比對規則。例如，您可以封鎖社群媒體類別，但允許存取 LinkedIn。

根據多個 **PAN-DB** 類別定義自訂 **URL** 類別（類別比對）

建立一個新類別，以針對與定義為自訂類別一部分的*所有*類別相符的網站或頁面進行強制執行。例如，PAN-DB 可能會將工程師用於研究的開發人員部落格歸類為 `personal-sites-and-blogs`、`computer-and-internet-info` 和 `high-risk`。為了讓工程師能夠存取部落格和類似網站*並*取得這些網站的可見度，您可以根據這三個類別建立自訂 URL 類別，並為該類別設定網站存取權，以便在 URL 篩選設定檔中提醒。

PAN-DB 會在外部動態清單和預先定義的 *URL* 類別之前先根據自訂 *URL* 類別來評估 *URL*。因此，防火牆會對自訂 *URL* 清單中的 *URL* 強制執行安全性政策規則，而不是與其所在的各個 *URL* 類別相關的政策規則。

如果多個安全性政策規則皆包含自訂 *URL* 類別，則防火牆會針對相符流量強制使用最嚴格的 *URL* 篩選設定檔動作的安全性政策規則。

- Strata Cloud Manager
- PAN-OS 和 Panorama

建立一個自訂 URL 類別 (Strata Cloud Manager)

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

請切換到 ***PAN-OS & Panorama*** 頁籤並按照指示進行操作。

如果您使用 ***Strata Cloud Manager***，則請繼續此處操作。

STEP 1 | 選取 **Manage**（管理） > **Configuration**（設定） > **Security Services**（安全服務） > **URL Access Management**（**URL** 存取管理） > **Access Control**（存取管理）。

STEP 2 | 在 [Custom URL Categories（自訂 URL 類別）] 下，選取 **Add Category**（新增類別）。

輸入類別的描述性 **Name**（名稱）。

STEP 3 | 將自訂 URL 類別 **Type**（類型）設為 **URL List**（**URL** 清單）或 **Category Match**（類別比對）。

- **URL List**（**URL** 清單）—使用此清單類型來新增要使用不同方式強制執行的 URL（與其所屬的 URL 類別不同），或將 URL 清單定義為屬於自訂類別。建立 URL 清單項目時請參閱 URL 類別例外指南。
- **Category Match**（類別比對）—為與一組類別相符的網站提供針對性執行方法。網站或網頁必須與自訂類別中定義的所有類別相符。

STEP 4 | 在 **Items**（項目）下 **Add**（新增）URL 或現有類別。

STEP 5 | **Save**（儲存）自訂 URL 類別。

STEP 6 | 定義自訂 URL 類別的網站存取和使用者認證提交設定。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **Security Services**（安全服務） > **URL Access Management**（**URL** 存取管理） > **URL Access Management Profiles**（**URL** 存取管理設定檔）。
2. 選取要修改的現有設定檔，或按一下 **Add Profile**（新增設定檔）。
3. 在 [Access Control（存取控制）] 下，選擇您先前建立的自訂 URL 類別。該類別位於自訂 URL 類別和預先定義的類別之間。
4. 設定該類別的 **Site Access**（網站存取）。
5. 設定該類別的 **User Credential Submissions**（使用者認證提交）。
6. **Save**（儲存）設定檔。

STEP 7 | 將 URL 存取管理設定檔套用至安全性政策規則。

僅當 URL 存取管理設定檔包含在安全性政策規則所參考的設定檔群組中，該設定檔才會處於啟用狀態。

依照步驟啟用 URL 存取管理設定檔（和任何安全性設定檔)。請務必記得 **Push Config**（推送設定）。

您也可使用自訂 *URL* 類別作為安全性政策比對規則。在這種情況下，您不會在 *URL* 篩選設定檔中定義 *URL* 類別的網站存取權。反之，在建立自訂 *URL* 類別後，請選取要新增自訂 *URL* 類別的安全性政策規則（***Manage***（管理） > ***Configuration***（設定） > ***Security Services***（安全服務） > ***Security Policy***（安全性政策））。在 ***Applications, Services and URLs***（應用程式、服務和 ***URL***）和 *URL* 類別項目下，按一下 ***Add URL Categories***（新增 ***URL*** 類別）。選取您建立的自訂 *URL* 類別，然後 ***Save***（儲存）安全性政策規則。

建立自訂 URL 類別 (PAN-OS & Panorama)

STEP 1 | 選取 **Objects**（物件） > **Custom Objects**（自訂物件） > **URL Category**（**URL** 類別）。

STEP 2 | **Add**（新增）或修改自訂 URL 類別，並為類別提供一個描述性 **Name**（名稱）。

STEP 3 | 將類別 **Type**（類型）設為 **Category Match**（類別比對）或 **URL List**（**URL** 清單）：

- **URL List**（**URL** 清單）—新增您希望以不同於其所屬 URL 類別之方式執行的 URL。使用此清單類型定義 URL 類別執行的例外，或定義屬於自訂類別的 URL 清單。如需建立 URL 清單項目的指導方針，請參閱 URL 類別例外。

  根據預設，防火牆會自動將尾端斜線 *(/)* 附加到不以尾端斜線或星號 *(*)* 結尾的網域項目 *(**example.com**)*。尾端斜線可防止防火牆在網域右側顯示隱式星號。在不含萬用字元的網域項目中，尾端斜線將相符項限制為給定網域及其子目錄。例如，***example.com***（處理後 ***example.com/***）與自身以及 ***example.com/search*** 相符。

  在萬用字元網域項目（使用星號或插入號的項目）中，尾端斜線將相符項限制為符合指定模式的 *URL*。例如，若要比對 ****.example.com*** 項目，*URL* 必須嚴格以一或多個子網域開頭，並以根網域 ***example.com*** 結尾；***news.example.com*** 是相符項，但 ***example.com*** 不是，因為它缺少子網域。

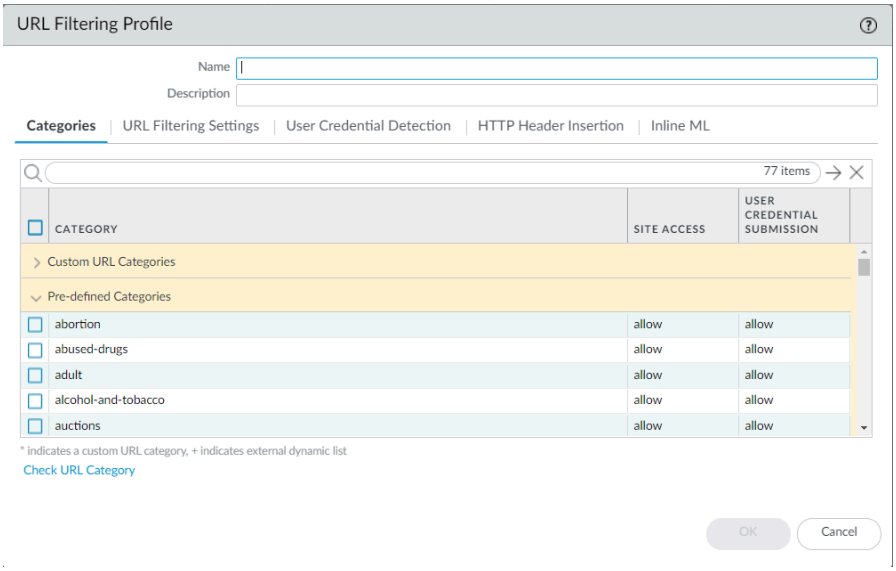
  我們建議手動新增尾端斜線，以便為檢查 *URL* 清單的任何人闡明項目的預期相符行為。如果由防火牆新增，則尾端斜線不可見。URL 類別例外進一步詳細討論尾端斜線和相符行為。

  若要停用此功能，請前往 ***Device***（裝置）***> Setup***（設定）***> Content-ID***（內容 *ID*）***> URL Filtering***（***URL*** 篩選）。然後，取消選取 ***Append Ending Token***（附加結束語彙基元）。如果停用此功能，您可能會封鎖或允許存取超出預期數目的 *URL*。URL 類別例外（*PAN-OS 10.1* 及更早版本）介紹了停用此功能時防火牆的行為。
- **Category Match**（類別比對）—為與一組類別相符的網站提供針對性執行方法。網站或網頁必須與自訂類別中定義的所有類別相符。

STEP 4 | 按一下 **OK**（確定）儲存自訂的 URL 類別。

STEP 5 | 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **URL Filtering**（**URL** 篩選），然後 **Add**（新增）或修改 URL 篩選設定檔。

新的自訂類別會顯示在 **Custom URL Categories**（自訂 **URL** 類別）下方：



STEP 6 | 決定要如何對自訂 URL 執行 **Site Access**（網站存取）和 **User Credential Submissions**（使用者認證提交）。（若要控制使用者可以向其提交公司認證的網站，請參閱防止憑證網路釣魚）。

STEP 7 | 將 URL 篩選設定檔附加至安全性政策規則，以強制執行與該規則相符的流量。

選取 **Policies**（政策） > **Security**（安全性） > **Actions**（動作），並指定安全性政策規則以根據剛才更新的 URL 篩選設定檔強制執行流量。確保 **Commit**（提交）變更。

您還可使用自訂 *URL* 類別作為安全性政策比對規則。在這種情況下，您不會在 *URL* 篩選設定檔中定義 *URL* 類別的網站存取權。建立自訂類別後，前往要新增自訂 *URL* 類別的安全性政策規則（***Policies***（政策） > ***Security***（安全性））。然後，選取 ***Service/URL Category***（服務/*URL* 類別）以使用自訂 *URL* 類別作為規則的比對規則。

在 URL 篩選設定檔中使用外部動態清單

這可在何處使用？	我需要什麼？
• 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)	❑ Advanced URL Filtering 授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

外部動態清單是代管於外部網頁伺服器上的一個文字檔。您可以使用此清單來匯入 URL 並針對這些 URL 強制執行原則。防火牆會動態地以所設間隔匯入清單，並為清單中的 URL（IP 位址或網域會被忽略）強制執行原則。當在 Web 伺服器上更新清單時，防火牆會擷取變更並將原則套用至修改的清單，而不需在防火牆上提交。

為了保護您的網路免受新發現的威脅和惡意軟體的侵害，可以在 URL 篩選設定檔中使用外部動態清單。如需 URL 格式設定方針，請參閱URL 類別例外指南。

- Strata Cloud Manager
- PAN-OS 和 Panorama

在 URL 篩選設定檔中使用外部動態清單 (Strata Cloud Manager)

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

請切換到 ***PAN-OS & Panorama*** 頁籤並按照指示進行操作。

如果您使用 ***Strata Cloud Manager***，則請繼續此處操作。

STEP 1 | 啟用 Prisma Access 以參照外部動態清單。

外部動態清單讓您可以定義匯入的 IP 位址、URL 或網域名稱清單，您可用於政策規則中來封鎖或允許流量。

若要設定外部動態清單，請前往 **Manage**（管理） > **Configuration**（設定） > **Objects**（物件） > **External Dynamic Lists**（外部動態清單）：

- 確保該清單不包括 IP 位址或網域名稱；防火牆會跳過非 URL 項目。
- 使用自訂 URL 清單指導方針來確認清單的格式設定。
- 將 **List Type**（清單類型）指定為 **URL List**（**URL** 清單）。

STEP 2 | 在 URL 篩選中使用外部動態清單。

前往 **Manage**（管理） > **Configuration**（設定） > **Security Services**（安全服務） > **URL Access Management**（**URL** 存取管理）。

- 指定外部動態清單中 URL 的 **Site Access**（網站存取）。
- 從進階內嵌分類中排除外部動態清單的 URL。

您也可以使用外部動態清單建立自訂 *URL* 類別（返回 *URL* 存取管理儀表板執行此操作）。

如果外部動態清單中包括的 *URL* 也被包括在自訂 *URL* 類別或封鎖和允許清單中，則自訂類別中指定的動作將優先於外部動態清單。

STEP 3 | 測試已強制執行該原則動作。

1. 查看外部動態清單項目（**Manage**（管理） > **Configuration**（設定） > **Objects**（物件） > **External Dynamic Lists**（外部動態清單））並嘗試從清單存取 URL。
2. 確認是否在瀏覽器中強制執行您定義的動作。

在 URL 篩選設定檔中使用外部動態清單 (PAN-OS & Panorama)

STEP 1 | 設定防火牆存取外部動態清單。

- 確保該清單不包括 IP 位址或網域名稱；防火牆會跳過非 URL 項目。
- 使用自訂 URL 清單指導方針來確認清單的格式設定。
- 從 Type（類型）下拉式清單中選取 **URL List**（**URL** 清單）。

STEP 2 | 在 URL 篩選設定檔中使用外部動態清單。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **URL Filtering**（**URL** 篩選）。
2. **Add**（新增）或修改既有 URL 篩選設定檔。
3. 為設定檔輸入 **Name**（名稱），然後在 **Categories**（類別）頁籤上，從類別清單中選取外部動態清單。
4. 按一下 Action（動作），為外部動態清單中的 URL 選取更準確的動作。

   如果外部動態清單中包括的 *URL* 也被包括在自訂 *URL* 類別或封鎖和允許清單中，則自訂類別中指定的動作將優先於外部動態清單。
5. 按一下 **OK**（確定）。
6. 將 URL 篩選設定檔附加於安全性原則規則。
   1. 選取 **Policies**（原則） > **Security**（安全性）。
   2. 選取 **Actions**（動作）頁籤，然後在設定檔設定區段，在 **URL Filtering**（**URL** 篩選）下拉式清單中選取新設定檔。
   3. 按一下 **OK**（確定）並 **Commit**（交付）變更。

STEP 3 | 測試已強制執行該原則動作。

1. 檢視外部動態清單項目，並嘗試從清單存取 URL。
2. 確認是否在瀏覽器中強制執行您定義的動作。
3. 若要監控防火牆上的活動：
   1. 選取 **ACC** 並新增 URL 網域作為全域篩選器，以檢視您存取的 URL 的網路活動和封鎖活動。
   2. 選取 **Monitor**（監控） > **Logs**（日誌） > **URL Filtering**（**URL** 篩選）以存取詳細日誌檢視。

STEP 4 | 確認是否忽略或跳過外部動態清單中的項目。

在 URL 類型的清單中，防火牆會跳過非 URL 的項目並忽略超出防火牆型號的最大限值的項目。

若要檢查是否已達到外部動態清單類型的限值，可選取 ***Objects***（物件） > ***External Dynamic Lists***（外部動態清單），然後按一下 ***List Capacities***（清單容量）。

在防火牆上使用以下 CLI 命令以檢閱清單詳情。

```
request system external-list show type url name <list_name>
```

例如：

```
request system external-list show type url name My_URL_List
 vsys5/My_URL_List:Next update at:Tue Jan 3 14:00:00 2017 Source:
 http://example.com/My_URL_List.txt Referenced:Yes Valid:Yes Auth-
Valid:Yes Total valid entries:3 Total invalid entries:0 Valid urls:
 www.URL1.com www.URL2.com www.URL3.com
```


URL 篩選最佳做法

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

Palo Alto Networks URL 篩選解決方案保護您免受基於 Web 的威脅，並為您提供一種監控和控制 Web 活動的簡單方法。為了最大程度地利用 URL 篩選部署，您應該先為開展業務所仰賴的應用程式建立允許規則。然後，檢閱對惡意和入侵內容進行分類的 URL 類別—我們建議您完全封鎖該等類別。然後，對於其他所有方面，這些最佳做法可為您指導減少對基於 Web 的威脅接觸的方法，而不會限制使用者對其所需的 Web 內容的存取。

- 在開始之前，在建置最佳做法網際網路閘道安全性政策時，識別想要允許的應用程式，並建立應用程式允許規則。

  允許的應用程式不僅包括您出於企業與基礎架構用途而佈建和管理的應用程式，還包括使用者需要完成其工作的應用程式，以及您可能想要用於個人用途的應用程式。

  識別了該等經認可的應用程式之後，您可以使用 URL 篩選來控制和保護所有不在允許清單上的 Web 活動。
- 深入瞭解使用者的 Web 活動，以便為您的組織計劃最有效的 URL 篩選政策。此包括：
  - 使用 Test A Site 查看 PAN-DB（Palo Alto Networks URL 篩選雲端資料庫）如何對特定 URL 進行分類，並瞭解所有可能的 URL 類別。
  - （大多數情況下）從被動 URL 篩選設定檔開始，可針對 URL 類別發出警示。這讓您能夠深入瞭解使用者正在存取的網站，從而確定想要允許、限制和封鎖的內容。
  - 監控 Web 活動以評估您的使用者正在存取的網站，並瞭解它們如何與您的業務需求保持一致。
- 封鎖對惡意和攻擊性 Web 內容進行分類的 URL 類別。儘管我們知道該等類別非常危險，但是請始終記住，您決定封鎖的 URL 類別可能取決於您的業務需求。
- 使用 URL 類別逐步解密，並將敏感或個人資訊（如金融服務和健康保健）從解密中排除。

  計劃先解密風險最高的流量（最有可能存在賭博或高風險這類惡意流量的 URL 類別），然後隨著經驗積累解密更多流量。或者，先解密不會影響業務的 URL 類別（即使出現問題，也不會影響業務），例如新聞資訊來源。在這兩種狀況下，解密一些 URL 類別、聽取使用者意見反應、

執行報告以確保解密如預期運作，然後逐步解密更多 URL 類別等等。若因技術原因而無法解密網站，或者您選擇不對其進行解密，請將這些網站排除在解密之外。

基於 *URL* 類別尋找解密目標也是解密的最佳做法。

- 透過啟用防火牆偵測提交至網站的公司認證防止認證被竊取，然後基於 URL 類別控制這些提交。阻止使用者向惡意網站和非受信任網站提交認證，警告使用者不要在未知網站上輸入公司認證，或警告使用者不要在非公司網站上重複使用公司認證，並明確允許使用者向公司網站和認可網站提交認證。
- 即時封鎖 JavaScript 漏洞和網路釣魚攻擊的惡意變體。啟用本機內嵌分類允許您在防火牆上使用機器學習動態分析網頁。
- 設定內嵌分類以啟用內嵌深度學習、基於 ML 的偵測引擎來分析可疑網頁內容並保護使用者免受零時差 Web 攻擊。雲端內嵌分類能夠偵測並防止進階及鎖定目標的網路釣魚攻擊，以及其他使用進階規避技術（如偽裝、多步驟攻擊、CAPTCHA 挑戰及以前未曾見過的一次性 URL）的 Web 攻擊。
- 解密、檢查並嚴格限制使用者與高風險和中等風險內容互動的方式（如果出於業務原因決定不封鎖任何惡意 URL 類別，則應嚴格限制使用者與這些類別進行互動的方式）。

  您批准的 Web 內容和您完全封鎖的惡意 URL 類別只是您整體 Web 流量的一部分。使用者正在存取的其餘內容是良性（低風險）和風險內容（高風險和中等風險）的組合。高風險和中等風險內容並未被確認為惡意內容，但與惡意內容密切相關。例如，高風險 URL 可能與惡意網站位於同一網域中，或者過去可能代管了惡意內容。

  但是，許多對您的組織構成風險的網站也為您的使用者提供了寶貴的資源和服務（雲端儲存服務就是很好的示例）。儘管這些資源和服務對於企業來說屬必要資源和服務，但其也更有可能被用作網路攻擊的一部分。以下為控制使用者如何與此類可能存在危險的內容進行互動，並仍為其提供良好使用者體驗的方法：

  - 在 URL 篩選設定檔中，將高風險和中等風險類別設定為繼續，以顯示回應頁面，該頁面警告使用者正在存取潛在危險的網站。如果決定繼續前往該網站，請告知他們如何採取預防措施。如果您不想在回應頁面上提示使用者，則請在高風險和中等風險類別上發出警示。
  - 解密高風險和中等風險網站。
  - 對於高風險和中風險網站，遵循反間諜軟體、漏洞保護和檔案封鎖最佳做法。有效的保護措施需要能夠封鎖下載危險的檔案類型，並封鎖經過混淆處理的 JavaScript。
  - 透過封鎖使用者向高風險和中等風險網站提交公司認證，阻止認證竊取。
- 學院或教育機構應使用安全的搜尋強制措施，以確保搜尋引擎從搜尋結果中篩選掉成人影像與視訊。
- 在 URL 類別查閱期間保留初始 Web 要求。

  當使用者造訪網站時，Advanced URL Filtering 會檢查快取的 URL 類別以分類網站。如果未在快取中找到 URL 的類別，則其將在 PAN-DB、Palo Alto Networks URL 資料庫中執行查閱。根據預設，此雲端查閱期間系統會允許使用者的 Web 要求。

  但是，當您選擇保留 Web 要求時，您可以封鎖該要求，直到 Advanced URL Filtering 找到 URL 類別或逾時為止。如果查詢逾時，防火牆會認為 URL 類別未解析。在您的 URL 篩選設定中找到此功能，**Hold client request for category lookup**（對類別查閱保留用戶端要求）。

測試 URL 篩選設定

這可在何處使用？	我需要什麼？
• 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)	❑ Advanced URL Filtering 授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

若要測試您的 URL 篩選政策和，請使用 Palo Alto Networks URL 篩選測試頁面。建立這些頁面是為了安全測試所有預先定義的 URL 類別和 Advanced URL Filtering 即時偵測類別。

測試頁面可透過 *HTTP* 和 *HTTPS* 連線存取。但您必須啟用 *SSL* 解密才能透過 *HTTPS* 檢視測試頁面。

您可以使用 *Palo Alto Networks URL* 類別查閱工具 Test A Site 來檢查特定網站的分類。

按照對應於 URL 篩選訂閱的程序操作。

驗證 URL 篩選

如果您有舊版 URL 篩選訂閱，請測試並驗證防火牆是否正確分類、強制執行和記錄一般使用者所存取類別中的 URL。

STEP 1 | 存取感興趣的 URL 類別中的網站。

考慮測試封鎖 URL 類別中的網站。您可以使用測試頁面 (urlfiltering.paloaltonetworks.com/test-*<url-category>*) 以避免直接存取網站。例如，若要測試對惡意軟體的封鎖原則，請造訪 https://urlfiltering.paloaltonetworks.com/test-malware。

STEP 2 | 檢視流量和 URL 篩選日誌以驗證防火牆是否正確處理網站。

例如，如果您設定當有人存取違反組織原則的網站時顯示一個封鎖頁面，請檢查當造訪測試頁面時是否會出現此類頁面。

驗證 Advanced URL Filtering

如果您有 Advanced URL Filtering 訂閱，請測試並驗證提交到 Advanced URL Filtering 的 URL 是否皆獲得正確分析。

Palo Alto Networks 建議設定即時偵測（雲端內嵌類別）動作設定，以 ***alert***（警示）您的作用中 *URL* 篩選設定檔。這可提供對即時分析的 *URL* 的可視性，並會根據針對特定 *Web* 威脅設定的類別設定進行封鎖（或允許，視乎您的原則設定而定）。

對於為給定 *URL* 偵測到的 *URL* 類別，防火牆會強制執行設定的動作中最嚴厲的動作。例如，假設 *example.com* 被分類為 *real-time-detection*、*command-and-control* 和 *shopping* 類別，並分別設定了「警示」、「封鎖」和「允許」動作。防火牆會封鎖該 *URL*，因為「封鎖」是偵測到的類別中最嚴厲的動作。

STEP 1 | 造訪以下每個測試 URL，以驗證 Advanced URL Filtering 服務是否正確分類 URL：

- **Malware**（惡意軟體）—http://urlfiltering.paloaltonetworks.com/test-inline-url-analysis-malware
- **Phishing**（網路釣魚）—http://urlfiltering.paloaltonetworks.com/test-inline-url-analysis-phishing
- **C2**—http://urlfiltering.paloaltonetworks.com/test-inline-url-analysis-command-and-control
- **Grayware**（灰色軟體）—http://urlfiltering.paloaltonetworks.com/test-inline-url-analysis-grayware

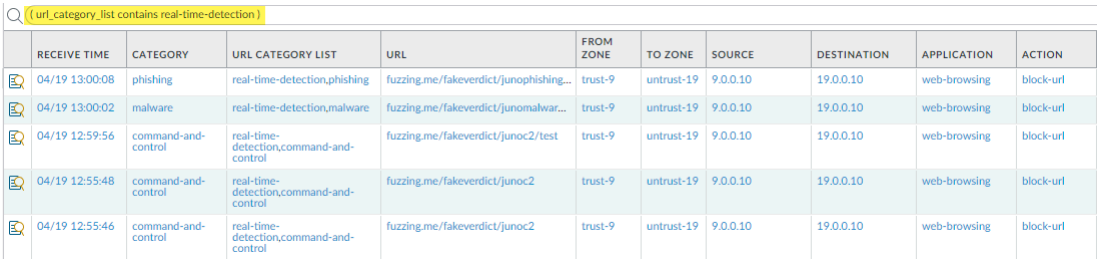
如果啟用雲端內嵌分類，請使用以下 URL 來測試該功能是否正常運作：

- **Malware**（惡意軟體）—http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-malware
- **Phishing**（網路釣魚）—http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-phishing
- **Grayware**（灰色軟體）—http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-grayware
- **Parked**（寄放）—http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-parked
- **Adult**（成人內容）—http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-adult

STEP 2 | 監控 Web 活動以確認 Advanced URL Filtering 是否正確分類測試 URL:

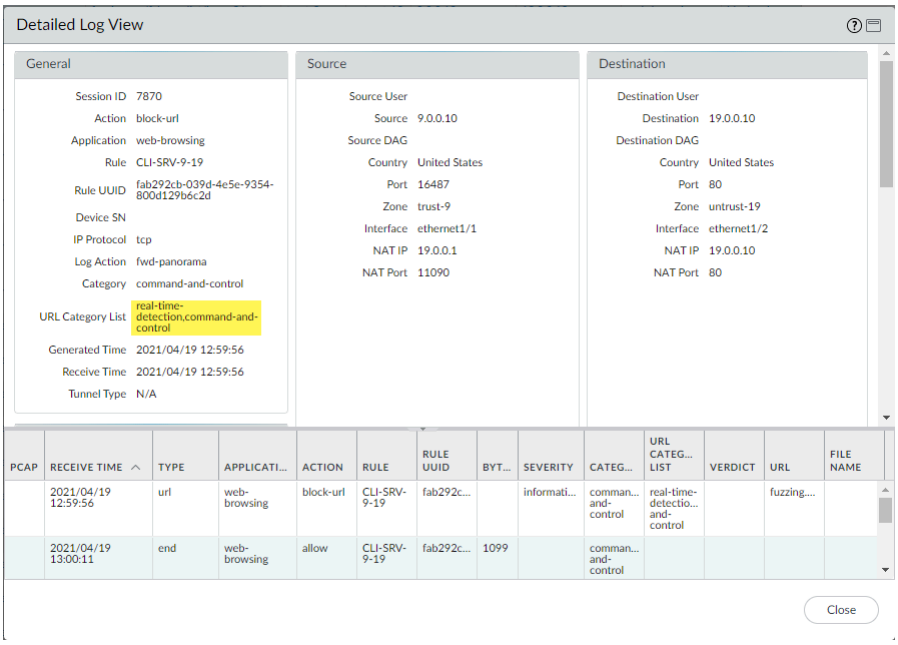
1. 請使用以下篩選您的 URL 篩選日誌：`(url_category_list contains real-time-detection)`。

   還會顯示其他網頁類別相符項，並對應 PAN-DB 定義的類別。



2. 詳細查看日誌，以驗證每種類型的 Web 威脅是否正確進行了分析和分類。

   在下面的範例中，URL 被分類為已即時分析，還具有將其定義為 command-and-control (C2) 的特性。由於 C2 類別的相關動作比 real-time-detection（封鎖而不是警示）更嚴重，URL 被歸類為 command-and-control 且已被封鎖。



URL 篩選功能

這可在何處使用？	我需要什麼？
• 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)	❑ Advanced URL Filtering 授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

設定 URL 篩選部署的基本元件之後，請考慮設定下列功能：

- 內嵌分類
- SSL/TLS 交握檢查
- URL 管理員取代
- 認證網路釣魚防禦
- URL 篩選回應頁面
- 安全搜尋強制
- （僅 Prisma Access）遠端瀏覽器隔離 (RBI) 整合

檢查 SSL/TLS 交握

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

檢查 SSL/TLS 交握可提高網路安全性並改善舊版和進階 URL 篩選訂閱。當您啟用 SSL/TLS 交握檢查時，進階 URL 篩選會使用交握中的資料來識別流量並儘早強制執行適用的安全性政策規則。

這是其運作方式

首先會掃描 Client Hello 訊息中的 伺服器名稱指示 *(SNI)*欄位，這是 SSL/TLS 通訊協定的延伸，其中包含所要求網站的主機名稱。接著可以從主機名稱獲得流量的 URL 類別和伺服器目的地。接下來，根據其 URL 類別強制執行流量。如果偵測到威脅，例如 SNI 欄位中的惡意 Web 伺服器，或安全性政策規則封鎖網站，交握將會終止，Web 工作階段也會立即結束。如果未偵測到威脅且每個政策皆允許該流量，則 SSL/TLS 交握完成，並透過安全連線交換應用程式資料。

SSL/TLS 交握檢查期間遭封鎖的網站不會顯示 *URL* 篩選回應頁面，因為防火牆會重置 *HTTPS* 連線。連線重置會結束 *SSL/TLS* 交握並防止回應頁面通知使用者。瀏覽器會顯示標準連線錯誤訊息。

您可以在流量和解密日誌中瞭解成功 *SSL/TLS* 交握和工作階段的詳細資料。失敗的工作階段的詳細資訊會顯示在 *URL* 篩選日誌；*SSL/TLS* 交握期間不會產生封鎖的 *Web* 工作階段的解密日誌。

- Strata Cloud Manager
- PAN-OS 和 Panorama

檢查 SSL/TLS 交握 (Strata Cloud Manager)

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

請切換到 ***PAN-OS & Panorama*** 頁籤並按照指示進行操作。

如果您使用 ***Strata Cloud Manager***，則請繼續此處操作。

檢查 SSL 交握的必要條件是透過 SSL 正向 Proxy 或 SSL 正向 Proxy 解密 SSL/TLS 流量。

STEP 1 | 請確認您的 Prisma Access 授權包括進階 URL 篩選訂閱。

1. 選取 **Manage**（管理） > **Service Setup**（服務設定） > **Overview**（概要），然後點選數量值的超連結。畫面會顯示包括安全服務在內等資訊。

2. 在安全服務之下，請確認 URL 篩選旁有核取記號。

STEP 2 | 確認您是透過 SSL Forward Proxy（SSL 正向 Proxy）還是 SSL Inbound Inspection（SSL 輸入檢查）解密 SSL/TLS 流量。

STEP 3 | 啟用由 CTD 檢查 SSL/TLS 交握。此選項預設為停用。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **Security Services**（安全服務） > **Decryption**（解密）。
2. 透過解密設定選取設定圖示。接著選取 **Inspect TLS Handshake Messages**（檢查 **TLS** 交握訊息）。

   或者，您可以使用 **`set deviceconfig setting ssl-decrypt scan-handshake <yes|no>`** CLI 命令。
3. **Save**（儲存）變更。在解密設定下，檢查 TLS 交握訊息設定應顯示為已啟用。

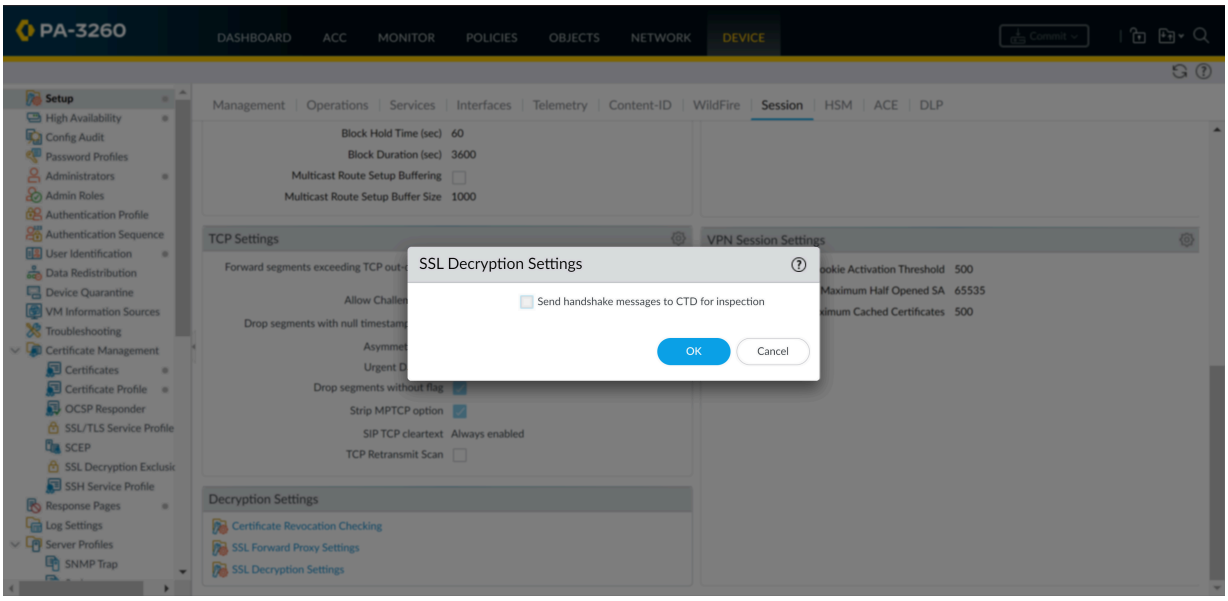
STEP 4 | 選取 **Push Config**（推送設定）以儲存並提交您的變更。

檢查 SSL/TLS 交握 (PAN-OS & Panorama)

STEP 1 | 選取 **Device**（裝置） > **Licenses**（授權）以確認您擁有作用中的進階 URL 篩選授權或舊版 URL 篩選授權。

STEP 2 | 確認您是透過 SSL Forward Proxy（SSL 正向 Proxy）還是 SSL Inbound Inspection（SSL 輸入檢查）解密 SSL/TLS 流量。

STEP 3 | 啟用由 CTD 檢查 SSL/TLS 交握。該選項預設停用。



1. 選取 **Device**（裝置） > **Setup**（設定） > **Session**（工作階段） > **Decryption Settings**（解密設定） > **SSL Decryption Settings**（**SSL** 解密設定）。
2. 選取 **Send handshake messages to CTD for inspection**（向 **CTD** 傳送交握訊息以供檢查）。

   或者，您可以使用 **`set deviceconfig setting ssl-decrypt scan-handshake <yes|no>`** CCLI 命令。
3. 按一下 **OK**（確定）。

STEP 4 | **Commit**（提交）組態變更。

允許使用密碼存取特定網站

這可在何處使用？	我需要什麼？
• 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)	❑ Advanced URL Filtering 授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

在部分情況下，使用者可能需要密碼才能存取部分類別的網站。例如，貴公司可能會封鎖威脅員工安全和福祉的 URL 類別。但是，部分員工可能需要存取這些類別，以進行研究或將其用於其他正當目的。為了在安全和業務需求之間取得平衡，URL 管理員取代可能是有效的解決方案。

若要建立 URL 管理員取代，請將類別動作設為 **override**（取代）。然後建立一組密碼，使用者必須輸入該密碼才能存取此類別的網站。當使用者嘗試造訪您已取代的類別的網站時，畫面會顯示「繼續並取代」的回應頁面。此頁面讓使用者知道某個網站已遭封鎖，且他們需輸入密碼才能繼續存取該網站。

- Strata Cloud Manager
- PAN-OS 和 Panorama

允許使用密碼存取特定網站 (Strata Cloud Manager)

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

請切換到 ***PAN-OS & Panorama*** 頁籤並按照指示進行操作。

如果您使用 ***Strata Cloud Manager***，則請繼續此處操作。

STEP 1 | 前往 URL 存取管理儀表板。

選取 **Manage**（管理） > **Configuration**（設定） > **Security Services**（安全服務） > **URL Access Management**（**URL** 存取管理）。

STEP 2 | 選取 **Settings**（設定）。

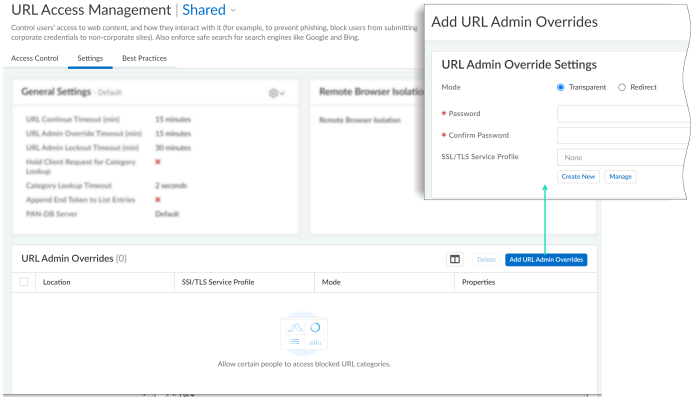
STEP 3 | 建立 URL 管理員取代密碼。

1. 前往 [URL Admin Overrides（URL 管理員取代）]，然後 **Add URL Admin Overrides**（新增 **URL** 管理員取代）。
2. （選用）選取提醒使用者輸入密碼的 **Mode**（模式）：
   - **Transparent**（透明）—密碼提示似乎源自於原始目標 URL。對於目的地是設為取代之 URL 類別中網站的瀏覽器流量，防火牆會攔截該流量，並發出 HTTP 302 以提示輸入密碼，該密碼適用於每個 vsys 層級。

- **Redirect**（重新導向）—密碼提示似乎來自您指定的 **Address**（位址）（IP 位址或 DNS 主機名稱）。防火牆會攔截流向設為取代之 URL 類別的 HTTP 或 HTTPS 流量，並使用 HTTP 302 重新導向，將要求傳送至防火牆上的 Layer 3 介面。

3. 輸入 **Password**（密碼），然後再次輸入以 **Confirm Password**（確認密碼）。
4. （選用）選取 **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）。

   您可以分別點選 **Create New**（新建）和 **Manage**（管理）來建立和管理 SSL/TLS 服務設定檔。
5. **Save**（儲存）變更。



STEP 4 | （選用）設定取代存取和密碼鎖定的持續時間。

根據預設，使用者有 15 分鐘的時間可以存取已成功輸入取代密碼的類別中的網站。超過預設或自訂時間之後，使用者必須重新輸入密碼。

根據預設，三次密碼輸入失敗後，使用者將被封鎖 30 分鐘。超過預設或自訂的使用者封鎖時間之後，使用者可以嘗試再次存取網站。

1. 自訂一般設定。
2. 針對 **URL Admin Override Timeout**（**URL** 管理員取代逾時），請輸入 1 到 86,400 之間的任意值（以分鐘為單位）。
3. 針對 **URL Admin Lockout Timeout**（**URL** 管理員鎖定逾時），請輸入 1 到 86,400 之間的任意值（以分鐘為單位）。
4. **Save**（儲存）變更。

STEP 5 | 指定需要密碼才能存取的 URL 類別。

1. URL 存取管理儀表板的 **Access Control**（存取控制）頁籤下，前往 [URL Access Management Profiles（URL 存取管理設定檔）] 並修改或 **Add Profile**（新增設定檔）。
2. 在存取控制下，選取需要密碼才能存取的類別。
3. 選取所有類別後，按一下 **Set Access**（設定存取），然後選取 **Override**（取代）。

   您應該會看到醒目顯示的類別的網站存取顯示為取代。
4. **Save**（儲存）變更。

STEP 6 | 將 URL 存取管理設定檔套用至安全性政策規則。

僅當 URL 存取管理設定檔包含在安全性政策規則所參考的設定檔群組中，該設定檔才會處於啟用狀態。

依照步驟啟用 URL 存取管理設定檔（和任何安全性設定檔)。完成後請務必 **Push Config**（推送設定）。

允許使用密碼存取特定網站 (PAN-OS & Panorama)

STEP 1 | 設定 URL 管理員取代密碼。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Content - ID**（內容 **ID**）。
2. 在 **URL Admin Override**（**URL** 管理員覆寫）區段中，按一下 **Add**（新增）。
3. 在 **Location**（位置）欄位中，選取要套用此密碼的虛擬系統。
4. 輸入 **Password**（密碼），然後再次輸入以 **Confirm Password**（確認密碼）。
5. 選取 **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔）。

   如果含覆寫的網站是 HTTPS 站台，SSL/TLS 服務設定檔會指定防火牆呈現給使用者的憑證。
6. 選取提醒使用者輸入密碼的 **Mode**（模式）：
   - **Transparent**（透明）—密碼提示似乎源自於原始目標 URL。對於目的地是設為取代之 URL 類別中網站的瀏覽器流量，防火牆會攔截該流量，並發出 HTTP 302 以提示輸入密碼，該密碼適用於每個 vsys 層級。

     如果用戶端瀏覽器不信任憑證，將會顯示憑證錯誤。
   - **Redirect**（重新導向）—密碼提示似乎來自您指定的 **Address**（位址）（IP 位址或 DNS 主機名稱）。防火牆會攔截流向設為取代之 URL 類別的 HTTP 或 HTTPS 流量，並使用 HTTP 302 重新導向，將要求傳送至防火牆上的 Layer 3 介面。
7. 按一下 **OK**（確定）。

STEP 2 | （選用）設定取代存取和密碼鎖定的持續時間。

根據預設，使用者有 15 分鐘的時間可以存取已成功輸入取代密碼的類別中的網站。超過預設或自訂時間之後，使用者必須重新輸入密碼。

根據預設，三次密碼輸入失敗後，使用者將被封鎖 30 分鐘。超過預設或自訂的使用者封鎖時間之後，使用者可以嘗試再次存取網站。

1. 編輯 URL 篩選區段。
2. 針對 **URL Admin Override Timeout**（**URL** 管理員取代逾時），請輸入 1 到 86,400 之間的任意值（以分鐘為單位）。依預設，使用者可存取該類別內的網站達 15 分鐘，無須重新輸入密碼。
3. 針對 **URL Admin Lockout Timeout**（**URL** 管理員鎖定逾時），請輸入 1 到 86,400 之間的任意值（以分鐘為單位）。
4. 按一下 **OK**（確定）。

STEP 3 | （僅限重新導向模式） 建立 Layer 3 介面，讓流向設為取代之類別中網站的網頁要求會重新導向至此介面。

1. 建立管理設定檔，讓介面顯示 URL 篩選繼續與取代頁面回應頁面：
   1. 選取 **Network**（網路） > **Interface Mgmt**（介面管理），然後按一下 **Add**（新增）。
   2. 輸入設定檔的 **Name**（名稱），選取 **Response Pages**（回應頁面），然後按一下 **OK**（確定）。
2. 建立 Layer 3 介面。確定附加您剛剛建立的管理設定檔（在 Ethernet Interface（乙太網路介面）對話方塊的 **Advanced**（進階） > **Other Info**（其他資訊）頁籤上）。

STEP 4 | （僅限重新導向模式）若要在不顯示憑證錯誤的情況下以透明方式重新導向使用者，請安裝符合介面 IP 位址的憑證，您會將前往已設為取代之 URL 類別中網站的網頁要求重新導向至該介面。您可以產生自我簽署或匯入由外部 CA 簽署的憑證。

若要使用自我簽署的憑證，您必須先建立根 CA 憑證，然後使用該 CA 簽署您將用於 URL 管理員覆寫的憑證，說明如下：

1. 若要建立根 CA 憑證，請選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證），然後按一下 **Generate**（產生）。輸入憑證名稱,, 例如 RootCA。請勿在 **Signed By**（簽署者）欄位中選取數值（表示此為自我簽署）。請確定您已選取 **Certificate Authority**（憑證授權單位）核取方塊，然後按一下 **Generate**（產生）以產生憑證。
2. 若要建立用於 URL 管理員覆寫的憑證，請按一下 **Generate**（產生）。輸入 **Certificate Name**（憑證名稱），然後輸入介面的 DNS 主機名稱或 IP 位址作為 **Common Name**（通用名稱）。在簽署者欄位中，選取在先前步驟中建立的 CA。新增 IP 屬性及指定 Layer 3 介面的 IP 位址，您會將前往採用覆寫動作之 URL 類別的網頁要求重新導向至該介面。
3. 產生憑證。
4. 若要設定用戶端信任憑證，請選取 裝置憑證（**Device Certificates**）頁籤上的 CA 憑證，然後按一下 **Export**（匯出）。之後您必須將憑證當成信任的 CA 匯入至所有用戶端瀏覽器，可透過手動設定瀏覽器或新增憑證至 Active Directory 群組原則物件 (GPO) 中的信任根。

STEP 5 | 指定哪些 URL 類別需要覆寫密碼才能存取。

1. 選取 **Objects**（物件） > **URL Filtering**（**URL** 篩選），然後選取現有的 URL 篩選設定檔或 **Add**（新增） 設定檔。
2. 在 **Categories**（類別）頁籤，將每個需要密碼之類別的動作設為 **override**（覆寫）。
3. 完成 URL 篩選設定檔上剩餘的區段，然後按一下 **OK**（確定）儲存設定檔。

STEP 6 | 將 URL 篩選設定檔套用至安全性原則規則，這些規則允許存取需要取代密碼才能進行存取的網站。

1. 選取 **Policies**（原則） > **Security**（安全性），然後選取適當的安全性原則以進行修改。
2. 選取 **Actions**（動作）頁籤，然後在 **Profile Setting**（設定檔組態）區段中，按一下 **URL Filtering**（**URL** 篩選）下拉式清單，然後選取設定檔。
3. 按一下 **OK**（確定）儲存。

STEP 7 | **Commit**（提交）組態。

認證網路釣魚防禦

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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

被攻擊者偽裝成合法網站的網路釣魚網站意圖竊取使用者資訊，特別是提供網路存取權的認證。當網路釣魚電子郵件進入網路時，只要有一個使用者按一下連結並輸入認證，就能成功入侵。您可以根據網站 URL 類別控制使用者可提供公司認證的網站，以偵測並防禦進行中的網路釣魚攻擊，從而阻止認證竊取。這可以讓您封鎖使用者向非受信任網站提交認證，同時允許向公司網站和認可網站提交認證。

認證網路釣魚防禦機制的原理是，掃描向網站提交使用者名稱和密碼的活動，並將這些提交與有效公司認證進行比較。您可以根據網站 URL 類別選擇要允許或阻止公司認證提交的網站。當使用者嘗試向受限制類別的網站提交認證時，封鎖回應頁面（阻止使用者提交認證）或「繼續」頁面會警告使用者不要向特定 URL 類別中的網站提交認證，但仍允許使用者繼續提交認證。您可以自訂回應頁面，以教導使用者不要重複使用公司認證，即使是在合法的非網路釣魚網站上。

下列主題介紹了您可用於偵測認證提交的方法，並提供了關於設定認證網路釣魚保護的說明。

- 公司認證提交的檢查方法
- 使用基於 Windows 的 User-ID 代理程式設定認證偵測
- 啟用認證網路釣魚防禦

公司認證提交的檢查方法

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

在您啟用認證網路釣魚防禦之前，先確定您希望使用什麼方法來檢查是否向網頁提交了有效的公司認證。

所提交認證的檢查方法	User-ID 組態要求	這種方法將如何偵測使用者向網站提交的公司使用者名稱和/或密碼？
群組對應	防火牆上的群組對應	防火牆會進行檢查，以確定使用者提交到受限制網站的使用者名稱是否符合任何有效的公司使用者名稱。 要進行此操作，防火牆會將提交的使用者名稱與使用者到群組對應表中的使用者名稱清單進行比對，以便偵測使用者何時將公司使用者名稱提交到屬於受限制類別的網站中。 此方法僅會根據 LDAP 群組成員資格檢查公司使用者名稱提交，這使得該方法易於設定，但較易有誤判。
IP 使用者對應	透過使用者對應、GlobalProtect 或驗證政策和驗證入口網站識別的 IP 位址到使用者對應。	防火牆會進行檢查，以確定使用者提交到受限制網站的使用者名稱是否與所登入使用者名稱的 IP 位址對應。 為此，防火牆會將所登入使用者名稱的 IP 位址及提交到網站的使用者名稱與 IP 位址到使用者對應表進行比對，以便偵測使用者何時將公司使用者名稱提交到屬於受限制類別的網站。 由於這種方法會對照 IP 位址到使用者名稱對應表比對工作階段所關聯之已登入使用者的 IP 位址，因此是一種偵測公司使用者名稱提交的有效方法，但這種方法並不會偵測公司密碼提交。如果您要偵測公司用戶名稱和密碼提交，則必須使用網域認證篩選方法。
網域憑證篩選	為 Windows 的 User-ID 代理程式設定 User-ID 認證服務附加元件 - 以及 - 透過使用者對應、GlobalProtect 或驗證政策和驗證入口網站識別的 IP 位址到使用者對應。	防火牆會進行檢查，以確定使用者提交的使用者名稱和密碼是否符合相同使用者的公司使用者名稱和密碼。 要進行此操作，防火牆必須能夠將認證提交與有效的公司使用者名稱和密碼比對，並按照下列方式驗證使用者所提交的使用者名稱對應至已登入使用者名稱的 IP 位址： • 偵測公司使用者名稱和密碼—防火牆從裝有 User-ID 認證服務附加元件的 Windows 的 User-ID 代理程式擷取安全位元遮罩（*Bloom* 篩選器）。此附加元件服務將在目錄中掃描使用者名稱及密碼雜湊，並將其解構成安全位元遮罩（Bloom 篩選器），然後將其傳送至 Windows User-ID 代理程式。防火牆會定期從 Windows User-ID 代理程式中擷取 Bloom 篩選器。當防火牆偵測到使用者向受限制類別網站提交認證時，將解構 Bloom 篩選器，尋找相符的使用者名稱和密碼雜湊。防火牆只能連線至一個執行 User-

所提交認證的檢查方法	User-ID 組態要求	這種方法將如何偵測使用者向網站提交的公司使用者名稱和/或密碼？
		ID 認證服務附加元件的 Windows User-ID 代理程式。 • 驗證認證是否屬於已登入使用者名稱—防火牆將檢查已登入使用者名稱的 IP 位址和在 IP 位址到使用者名稱對應表中偵測到的名稱是否對應。 若要深入瞭解網域憑證方法，請參閱使用基於 Windows 的使用者 ID 代理程式設定認證偵測。

使用 Windows 的 User-ID 代理程式設定認證偵測

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

網域認證篩選偵測功能讓防火牆能夠偵測提交到網頁的密碼。這種認證偵測方法需要在唯讀網域控制站 *(RODC)* 上安裝 Windows 的 User-ID 代理程式和 User-ID 認證服務（User-ID 代理程式的附加元件）。

僅 *Windows* 的 *User-ID* 代理程式支援網域認證篩選偵測方法。您無法使用整合了 *PAN-OS* 的 *User-ID* 代理程式設定此認證偵測方法。

RODC 是一種 Microsoft Windows 伺服器，其中裝有網域控制站所裝載之 Active Directory 資料庫的唯讀複本。例如，若網域控制站位於公司總部，可以將 RODC 部署在遠端網路站點，以提供本機驗證服務。由於以下幾個原因，在 RODC 上安裝 User-ID 代理程式可能會非常有用：不需要存取網域控制站目錄即可啟用認證偵測，而且您可以針對限定或特定的使用者組支援認證偵測。由於 RODC 主機的目錄唯讀，網域控制站上的目錄內容將很安全。

由於您必須在 *RODC* 上安裝 *Windows* 的 *User-ID* 代理程式以執行認證偵測，為此，作為最佳做法，請部署單獨的代理程式。請勿使用 *RODC* 上安裝的 *User-ID* 代理程式來將 *IP* 位址對應至使用者。

在 RODC 上安裝 User-ID 代理程式之後，User-ID 認證服務將在背景中執行，並將掃描目錄，尋找 RODC 密碼複製原則 (PRP) 中（您可以定義該清單中的使用者）所列群組成員的使用者名稱和密碼雜湊。User-ID 認證服務隨後將擷取所收集的使用者名稱和密碼雜湊，並將資料解構成一種被稱作 *Bloom* 篩選器的位元遮罩。Bloom 篩選器是壓縮資料結構，提供了一種安全的方法來檢

查元素（使用者名稱或密碼雜湊）是否為元素集合（您已認可複製到 RODC 的認證集合）的成員。User-ID 認證服務會將 Bloom 篩選器轉送至 Windows 的 User-ID 代理程式；防火牆定期從 User-ID 代理程式擷取最新的 Bloom 篩選器，並用其偵測使用者名稱和密碼雜湊提交。視乎您的設定，防火牆將封鎖、警示或允許有效的密碼提交（提交到網頁），或者向使用者顯示回應頁面，警告他們存在網路釣魚的危險，但仍允許他們繼續提交。

在此過程中，User-ID 代理程式不會儲存或披露任何密碼雜湊，也不會將密碼雜湊轉送至防火牆。當密碼雜湊被解構成 Bloom 篩選器之後，將無法再復原。

STEP 1 | 使用 Windows User-ID 代理程式設定使用者對應。

> 您必須在 *RODC* 安裝 *Windows User-ID* 代理程式以啟用認證偵測。有關受支援伺服器的清單，請參閱Compatibility Matrix（相容性矩陣）。為此，安裝單獨的 *User-ID* 代理程式。

設定 User-ID 以啟用網域認證篩選偵測時的重要注意事項：

- 憑證網路釣魚偵測的有效性取決於您的 RODC 設定。請務必參閱 RODC 管理的最佳實務和建議。
- 下載 User-ID 軟體更新：
  - User-ID 代理程式 Windows 安裝程式—UaInstall-x.x.x-x.msi。
  - User-ID 代理程式認證服務 Windows 安裝程式—UaCredInstall64-x.x.x-x.msi。
- 使用具有透過 LDAP 讀取 Active Directory 權限（User-ID 代理程式也需要此權限）的帳戶在 RODC 上安裝 User-ID 代理程式和 User-ID 代理程式認證服務。
  - User-ID 代理程式認證服務需要權限才能登入本機系統帳戶。如需詳細資訊，請參閱為 User-ID 代理程式建立專用服務帳戶。
  - 服務帳戶必須為 RODC 上本機管理員群組成員。

STEP 2 | 啟用 User-ID 代理程式和 User-ID 代理程式認證服務（其將在背景中執行，以掃描允許的認證），以分享資訊。

1. 在 RODC 伺服器上，啟動 User-ID 代理程式。
2. 選取 **Setup**（設定）然後編輯 Setup（設定）區段。
3. 選取 **Credentials**（認證）頁籤。此頁籤會顯示您是否已安裝 User-ID 代理程式認證服務。
4. 選取 **Import from User-ID Credential Agent**（從 **User-ID** 認證代理程式匯入）。這將允許 User-ID 代理程式匯入 User-ID 認證代理程式為表示使用者和相應密碼雜湊而建立的 Bloom 篩選器。
5. 按一下 **OK**（確定），**Save**（儲存）您的設定，然後 **Commit**（提交）。

STEP 3 | 在 RODC 目錄中，定義您要支援認證提交偵測的使用者群組。

- 確認應接收強制提交認證的群組已新增至 Allowed RODC Password Replication Group（允許的 RODC 密碼複製群組）。
- 檢查以確保允許的 RODC 密碼複製群組中沒有任何群組同時在預設的 Denied RODC Password Replication Group（拒絕的 RODC 密碼複製群組）內。這兩者中所列的群組將不接受強制反認證網路釣魚。

STEP 4 | 繼續下一項工作。

在防火牆上設定認證網路釣魚防禦。

設定認證網路釣魚防禦

這可在何處使用？	我需要什麼？
• 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)	❑ Advanced URL Filtering 授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

決定要設定哪種使用者認證偵測方法後，請依照下列步驟，防止認證網路釣魚攻擊。

啟用認證網路釣魚防禦之前，請確認您在防火牆上設定的主要使用者名稱使用 *sAMAccountName* 屬性。認證網路釣魚防禦不支援替代屬性。

- Strata Cloud Manager
- PAN-OS 和 Panorama

設定認證網路釣魚防禦 (Strata Cloud Manager)

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

請切換到 ***PAN-OS & Panorama*** 頁籤並按照指示進行操作。

如果您使用 ***Strata Cloud Manager***，則請繼續此處操作。

STEP 1 | 設定您要使用的使用者認證偵測方法。

查看檢查公司認證提交的方法，以瞭解每種方法的詳細資訊。

- 針對 IP 使用者對應，請設定本機使用者和群組、識別重新散佈或使用 Prisma Access 進行驗證。
- 若要使用網域憑證篩選，請設定識別重新散佈以及本機使用者和群組或驗證。
- 若要使用群組對應，請設定本機使用者和群組或驗證。

STEP 2 | 建立解密政策規則，以解密您要監控的使用者認證提交的流量。

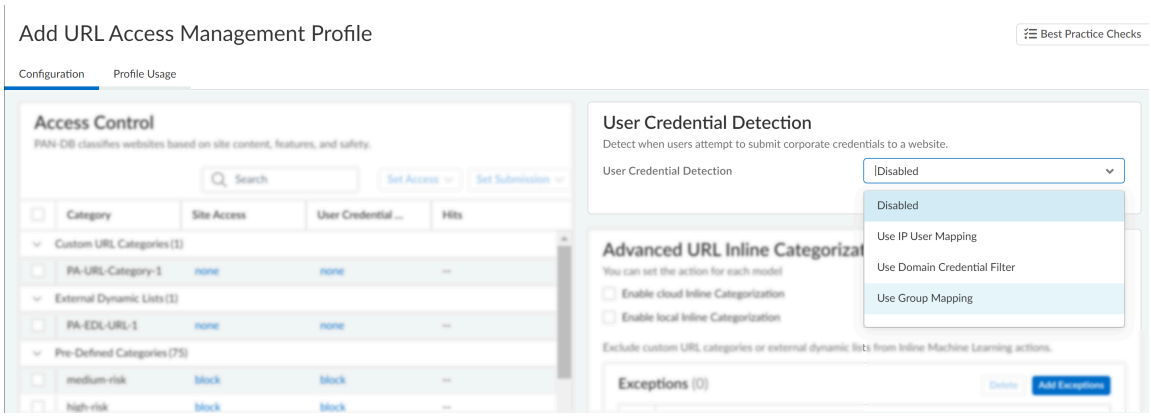
STEP 3 | 建立或修改 URL 存取管理設定檔。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（NGFW 和 **Prisma Access**） > **Security Services**（安全服務） > **URL Access Management**（URL 存取管理）。
2. 在 URL 存取管理設定檔下，點選 **Add Profile**（新增設定檔）或選取現有設定檔。

STEP 4 | 設定使用者認證偵測設定。

1. 在使用者認證偵測下，選擇 **User Credential Detection**（使用者認證偵測）方法。
   - **Use IP User Mapping**（使用 **IP** 使用者對應）—檢查有效的公司使用者名稱提交，並驗證登入使用者名稱是否與工作階段來源 IP 位址對應。為此，Prisma Access 需對照 IP 位址到使用者名稱的對應表，將所提交的使用者名稱與工作階段來源 IP 位址進行比對。
   - **Use Domain Credential Filter**（使用網域認證篩選器）—檢查有效的公司使用者名稱和密碼提交，並驗證使用者名稱是否對應到已登入使用者的 IP 位址。
   - **Use Group Mapping**（使用群組對應）—根據您對應使用者到群組時填入的使用者到群組對應表格，檢查有效的使用者名稱提交。您可以將認證偵測套用至目錄的任何部分或有權存取最敏感應用程式（例如 IT）的特定群組。

     這種方法在未採用唯一結構使用者名稱的環境中容易產生誤報。因此，您只應使用此方法保護高價值使用者帳戶。



2. 針對 **Valid Username Detected Log Severity**（偵測到有效使用者名稱的日誌安全性），請選取防火牆在偵測到公司認證提交時在日誌中記錄的嚴重性層級：
   - 高
   - （預設）中等
   - 低

STEP 5 | 設定防火牆偵測到公司認證提交時要採取的操作。

1. 在存取控制下，為每個 URL 類別選取 **User Credential Submission**（使用者認證提交）操作，並將其 **Site Access**（網站存取）設定為允許或警示。

   您可以從下列動作中選取：

   - （建議）**alert**（警示）—讓使用者向特定 URL 類別中的網站提交認證，但每次提交時都會產生 URL 篩選日誌。
   - （預設）**allow**（允許）—允許使用者向網站提交認證。
   - （建議）**block**（封鎖）—阻止使用者向特定 URL 類別中的網站提交認證。當使用者嘗試提交認證時，防火牆會顯示防網路釣魚封鎖頁面。
   - **continue**（繼續）—當使用者嘗試提交認證時，向使用者顯示防網路釣魚繼續頁面。使用者必須在回應頁面上選取 [Continue（繼續）] 才能前往網頁。

2. **Save**（儲存）設定檔。

STEP 6 | 將 URL 存取管理設定檔套用到您的安全政策規則。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服務） > **Security Policy**（安全性政策）。
2. 在安全性政策規則下，建立或選取安全性政策規則。
3. 選取 **Actions**（動作） > **Profile Group**（設定檔群組），然後選取 URL 存取管理設定檔群組。
4. **Save**（儲存）規則。

STEP 7 | 按一下 **Push Config**（推送設定）。

設定認證網路釣魚防禦 (PAN-OS & Panorama)

STEP 1 | 啟用 User-ID。

每一種公司認證提交檢查方法都需要不同的 User-ID 設定：

- 群組對應—偵測使用者是否提交有效的公司使用者名稱，並要求您將使用者對應至群組。
- IP 使用者對應—偵測使用者是否提交有效的公司使用者名稱以及該使用者名稱是否符合登入使用者名稱—要求您將 IP 位址對應至使用者。
- 網域認證篩選—偵測使用者是否提交有效的使用者名稱和密碼，以及這些認證是否屬於已登入使用者—要求您使用基於 Windows 的 User-ID 代理程式設定認證偵測並將 IP 位址對應至使用者。

STEP 2 | 設定最佳做法 URL 篩選設定檔，以確保針對被觀測到裝載惡意軟體或攻擊性內容的 URL 提供保護。

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. 封鎖對所有已知危險 URL 類別的存取：惡意軟體、網路釣魚、動態 DNS、未知、命令和控制、極端主義、侵犯著作權、Proxy 規避與匿名者網站、新註冊網域、灰色軟體和寄放。

STEP 3 | 建立解密政策規則以解密想要監控的使用者認證提交的流量。

STEP 4 | 偵測向屬於被允許 URL 類別的網站提交公司認證的活動。

為了提供最佳效能，防火牆不會檢查受信任網站的認證提交（即使啟用了對該等網站的 *URL* 類別的檢查）。受信任網站為 *Palo Alto Networks* 尚未觀測到任何惡意或網路網路釣魚攻擊的網站。此受信任網站的更新乃透過應用程式和威脅內容更新傳遞。

1. 選取一個 URL 篩選設定檔（**Objects**（物件） > **Security Profiles**（安全性設定檔） > **URL Filtering**（URL 篩選）），以進行修改。
2. 選取 **User Credential Detection**（使用者認證偵測）並選取一種使用者認證偵測方法。

   確認主要使用者名稱的格式與 *User-ID* 來源提供的使用者名稱相同。

   - **Use IP User Mapping**（使用 IP 使用者對應）—檢查有效的公司使用者名稱提交，並驗證登入使用者名稱是否與工作階段來源 IP 位址對應。為此，防火牆需對照 IP 位址到使用者名稱的對應表，將所提交的使用者名稱與工作階段來源 IP 位址進行比對。若要使用此方法，請設定列在將 IP 位址對應至使用者中的任何使用者對應方法。
   - **Use Domain Credential Filter**（使用網域認證篩選器）—檢查有效的公司使用者名稱和密碼提交，並確認使用者名稱已對應到已登入使用者的 IP 位址。如需瞭解如何設定此方法，請參閱使用基於 Windows 的 User-ID 代理程式設定認證偵測。
   - **Use Group Mapping**（使用群組對應）—根據您在設定防火牆對應使用者到群組時填入的使用者到群組對應表格，檢查有效的使用者名稱提交。

     對於群組對應，您可以將認證偵測套用至目錄的任何部分，或有權存取您最敏感應用程式的特定群組，例如 IT 群組。

     這種方法在未採用唯一結構用戶名的環境中易於產生誤報。因此，您只應使用此方法保護高價值使用者帳戶。
3. 設定防火牆用於記錄公司認證提交偵測的 **Valid Username Detected Log Severity**（有效使用者名稱偵測日誌嚴重性）。依預設，防火牆將記錄中等嚴重性的事件。

STEP 5 | 封鎖（或警示）向允許的網站提交認證的動作。

1. 選取 **Categories**（類別）。
2. 對於允許 **Site Access**（網站存取）的每個 類別，選取您希望如何處理 **User Credential Submissions**（使用者認證提交）：
   - 警示—允許使用者將認證提交至網站，但在每次使用者將認證提交至此 URL 類別中的網站時產生 URL 篩選日誌。
   - 允許（預設值）—允許使用者將認證提交至網站。
   - 封鎖—封鎖使用者將認證提交至網站。當使用者嘗試提交認證時，防火牆會顯示防網路釣魚封鎖頁面，阻止認證提交。
   - **continue**（繼續）—當使用者嘗試提交認證時，向使用者顯示防網路釣魚繼續頁面。使用者必須在回應頁面上選取 Continue（繼續）才能繼續提交。
3. 選取 **OK**（確定）來儲存 URL 篩選設定檔。

STEP 6 | 將具有認證偵測設定的 URL 篩選設定檔套用至安全性原則規則。

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. 在 **Actions**（動作）頁籤中，將 **Profile Type**（設定檔類型）設定為 **Profiles**（設定檔）。
3. 選取新的或已更新的 **URL Filtering**（**URL** 篩選）設定檔，將其附加至安全性原則規則。
4. 選取 **OK**（確定）來儲存安全性原則規則。

STEP 7 | **Commit**（提交）組態。

STEP 8 | 監控防火牆偵測到的認證提交。

選取 ***ACC*** > ***Hosts Visiting Malicious URLs***（造訪惡意 ***URL*** 的主機），以瞭解瀏覽過惡意軟體和網路釣魚網站的使用者數目。

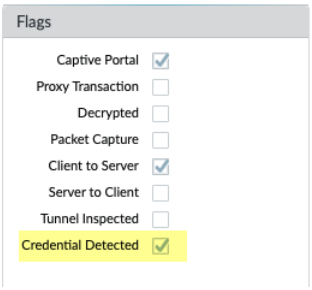
選取 **Monitor**（監控） > **Logs**（日誌） > **URL Filtering**（**URL** 篩選）。

新的 **Credential Detected**（已偵測認證）欄指示防火牆偵測到包含有效認證的 HTTP post 要求的事件：

	CATEGORY	APPLICATION	ACTION	CREDENTIAL DETECTED
	streaming-media		block-url	yes
	streaming-media		block-url	yes
	streaming-media		block-url	yes
	streaming-media		block-url	yes
	streaming-media		block-url	yes

若要顯示此欄，可將滑鼠暫留在任何欄標頭上，然後按一下箭頭以選取您要顯示的欄。

日誌項目詳細資料也指示了認證提交：



STEP 9 | 驗證認證提交偵測，並進行疑難排解。

- 使用下列 CLI 名稱檢視認證偵測統計資料：

```
> show user credential-filter statistics
```

此命令的輸出因防火牆設定用於偵測認證提交之方法而異。例如，若在任何 URL 篩選設定檔中設定了網域認證篩選方法，將顯示已向防火牆轉送 Bloom 篩選器的 User-ID 代理程式清單，以及 Bloom 篩選器中包含的認證數目。

- （僅適用於群組對應方法）使用下列 CLI 命令，檢閱群組對應資訊，包括啟用了群組對應認證偵測的 URL 篩選設定檔數目，以及嘗試過向受限制網站提交認證的群組成員的使用者名稱。

  ```
  > show user group-mapping statistics
  ```

- （僅適用於網域認證篩選方法）使用下列 CLI 命令，查看所有向防火牆傳送對應的基於 Windows 的 User-ID 代理程式：

  ```
  > show user user-id-agent state all
  ```

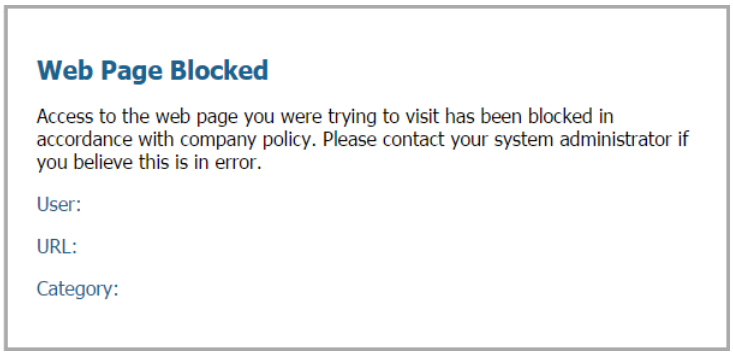
  命令輸出此時會顯示 Bloom 篩選器計數，其中包括防火牆從每個代理程式接收的 Bloom 篩選器更新數目，是否有任何 Bloom 篩選器更新處理失敗，以及上一次 Bloom 篩選器更新後已經過去了多少秒。

- （僅限網域認證篩選方法）基於 Windows 的 User-ID 代理程式將顯示參考 BF（Bloom 篩選器）向防火牆推送的日誌訊息。在 User-ID 代理程式介面中，選取 **Monitoring**（監控） > **Logs**（日誌）。

URL 篩選回應頁面

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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

針對所要求的 URL 存取受限時，URL 篩選回應頁面會通知使用者。如果網站所屬類別設有封鎖、繼續或取代動作，或已封鎖向網站或類別提交憑證，則該存取動作可能受限。如果使用者沒有為搜尋引擎設定最嚴格的安全搜尋設定，且安全政策規則強制執行安全搜尋，則該存取動作也會受限。有預先定義回應頁面的五個原因。有些回應頁面完全封鎖存取，而其他回應頁面則允許部分存取。例如，如果出現 URL 篩選繼續和取代頁面或防網路釣魚繼續頁面，使用者可以按一下 [Continue（繼續）] 進入網站（除非啟用 URL 管理員取代）。



通常，回應頁面會說明無法存取頁面的原因，並列出使用者、URL 和 URL 類別。但是，您可以自訂回應頁面的內容和外觀。例如，您可以變更通知訊息、加上企業名稱，或加上您的可接受使用政策的連結。

您可能會發現不同 *PAN-OS* 軟體版本的回應頁面外觀有所不同。但所有功能皆保持不變。

請留意，您可以自訂回應頁面以符合您的個別需求。

如果啟用 SSL/TLS 交握檢查，瀏覽器就不會顯示回應頁面。

- 預先定義 URL 篩選回應頁面
- URL 篩選回應頁面物件
- 自訂 URL 篩選回應頁面

預先定義 URL 篩選回應頁面

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

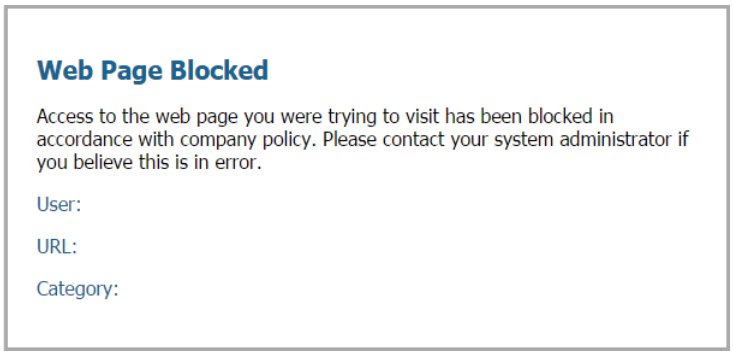
針對所要求的 URL 存取受限時，Web 瀏覽器會顯示 URL 篩選回應頁面。每個回應頁面都會解釋該頁面無法存取的原因，多數頁面會列出使用者、所要求的 URL 以及觸發封鎖動作的 URL 類別的相關資訊。

您可能會發現不同 *PAN-OS* 軟體版本的回應頁面外觀有所不同。但所有功能皆保持不變。

請留意，您可以自訂回應頁面以符合您的個別需求。

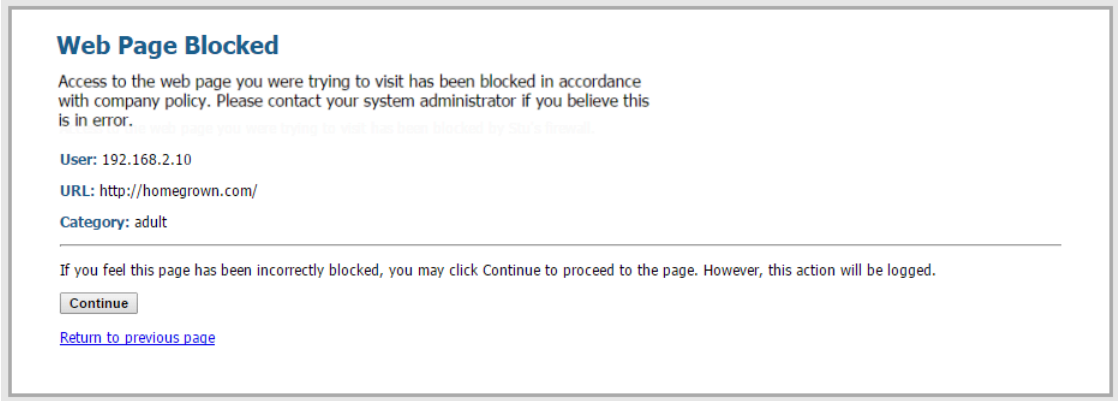
- **URL** 篩選與類別比對封鎖頁面

  存取被 URL 篩選設定檔封鎖，或因為 URL 類別被安全性原則規則封鎖。



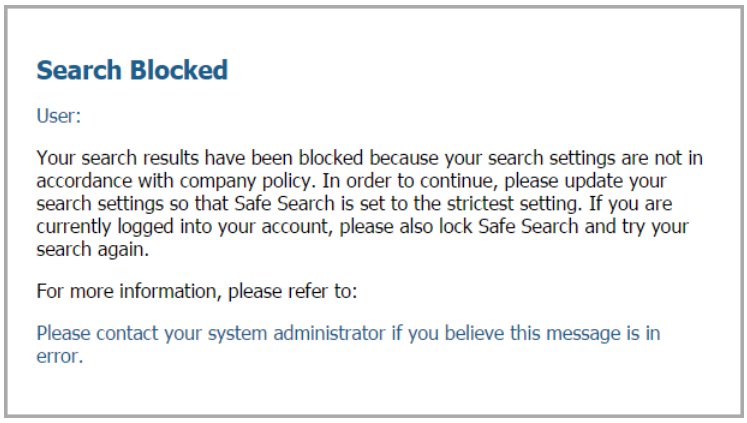
- **URL** 篩選繼續與取代頁面

  可透過按一下 **Continue**（繼續）讓使用者避開封鎖的頁面與初始封鎖原則。啟用 URL 管理員覆寫時，（允許使用密碼存取特定網站），當按一下 **Continue**（繼續）後，使用者必須提供密碼才能覆寫封鎖此 URL 的原則。



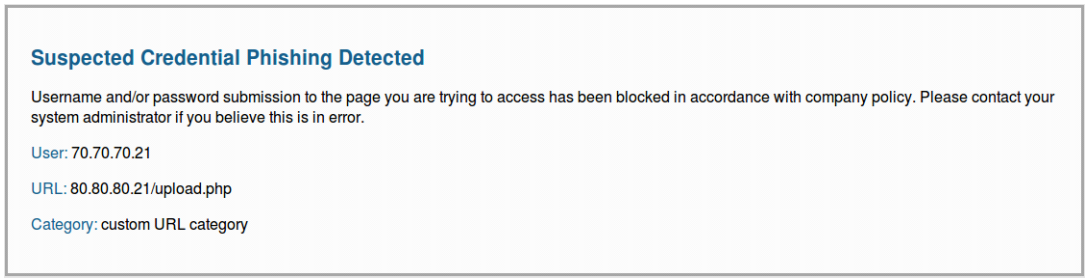
- **URL** 篩選安全搜尋封鎖頁面

  遭到啟用安全搜尋強制執行選項的 URL 篩選設定檔的安全性政策規則封鎖存取（請參閱 安全搜尋強制）。若是使用 Google、Bing、Yahoo 或 Yandex 執行搜尋，且其瀏覽器或搜尋引擎帳戶設定未將安全搜尋設為嚴格，使用者將看到此頁面。



- 防網路釣魚封鎖頁面

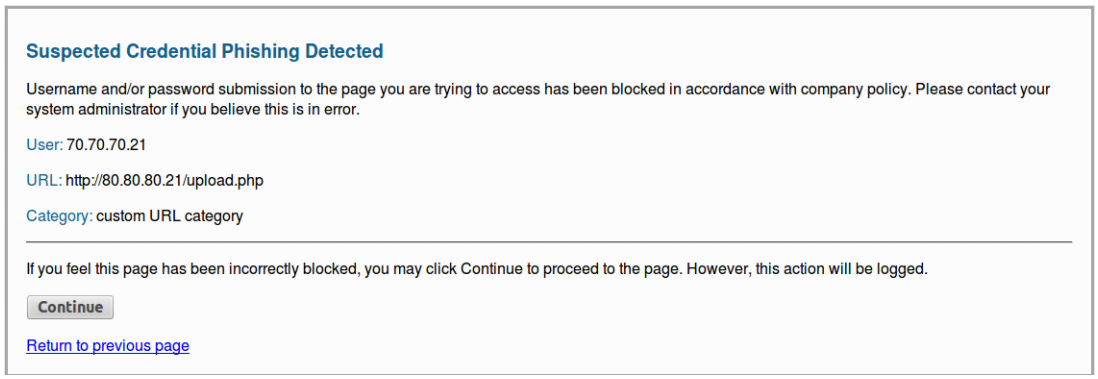
  當使用者嘗試在封鎖認證提交之類別中的網頁上輸入有效的公司認證（使用者名稱或密碼）時，會向使用者顯示此頁面。使用者可以繼續存取網站，但仍無法提交有效的公司認證給任何相關聯的網頁表單。若要控制使用者可以向哪些網站提交公司認證，您必須設定 User-ID 並根據 URL 類別啟用認證網路釣魚防禦。



- 防網路釣魚繼續頁面

  此頁面會在使用者向網站提交認證（使用者名稱和密碼）時發出警告。針對提交認證向使用者發出警告，有助於防止他們重複使用公司認證，並教育他們可能發生的釣魚嘗試。他們必須選

擇 Continue（繼續）才能繼續在網站上輸入認證。若要控制使用者可以向哪些網站提交公司認證，您必須設定 User-ID 並根據 URL 類別啟用認證網路釣魚防禦。



URL 篩選回應頁面物件

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

使用以下區段說明的變數和參照來自訂 URL 篩選回應頁面。回應頁面變數會顯示 URL 要求的不同相關資訊。例如，針對所要求 URL 類別的回應頁面，防火牆會在 HTML 碼中取代 `<category/>` 變數。您可以透過回應頁面參照新增外部映像、聲音、樣式表和連結。

回應頁面變數

下表列出回應頁面變數以及系統在封鎖事件期間替換每個變數的資訊或物件。根據預設，每個 URL 篩選回應頁面都使用以下變數：「使用者」、「URL」和「類別」。但是，您可以自訂回應頁面。例如，您可以修改變數的順序或為特定 URL 類別新增不同的資訊。

變數	使用方式
<user/>	顯示回應頁面時，防火牆會將此變數取代為使用者名稱 (若透過 User-ID 提供時) 或使用者的 IP 位址。
<url/>	顯示回應頁面時，防火牆會將此變數取代為要求的 URL。
<category/>	防火牆會將變數取代為封鎖要求的 URL 篩選類別。

變數	使用方式
<pan_form/>	用於在 URL 篩選繼續與覆寫頁面上顯示 **Continue**（繼續）按鈕的 HTML 指令碼。

您也可以新增可觸發防火牆的指令碼，以根據使用者正嘗試存取的 URL 類別來顯示不同的訊息。例如，回應頁面的下列指令碼片段可指定如果 URL 類別為賭博，則顯示訊息 1，如果是旅遊，則顯示訊息 2，如果是兒童，則顯示訊息 3：

```
var cat = "<category/>"; switch(cat) { case 'games':
 document.getElementById("warningText").innerHTML = "Message 1";
 break; case 'travel':
 document.getElementById("warningText").innerHTML = "Message 2";
 break; case 'kids': document.getElementById("warningText").innerHTML
 = "Message 3"; break; }
```

回應頁面參照

系統會針對每一類型的封鎖頁面，只將單一 *HTML* 頁面載入到每一個虛擬系統。然而，當瀏覽器中顯示回應頁面時，系統會從其他伺服器載入如影像、聲音與階層樣式表（*CSS* 檔案）等其他資源。所有參照皆須包含完全合格的 *URL*。

參照類型	範例 **HTML** 指令碼
影像	`<img src="http://virginiadot.org/images/Stop-Sign-gif.gif">`
聲音	`<embed src="http://simplythebest.net/sounds/WAV/WAV_files/ movie_WAV_files/ do_not_go.wav" volume="100" hidden="true" autostart="true">`
樣式表	`<link href="http://example.com/style.css" rel="stylesheet" type="text/css" />`
超連結	`<a href="http://en.wikipedia.org/wiki/Acceptable_use_policy">檢視公司政策</a>`

自訂 URL 篩選回應頁面

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

根據預設，URL 篩選回應頁面會說明為何無法存取所要求的 URL，並顯示使用者的 IP 位址、要求的 URL 和 URL 類別。您可以自訂回應頁面，以符合貴企業的需求。例如，您可以變更顯示給使用者的訊息、加上企業名稱，或加上可接受的使用政策的連結。

若要自訂頁面，請從平台匯出頁面，然後在文字編輯器中進行修改。您可以使用所提供的回應頁面變數和參考來進行更新。回應頁面變數對應至遭封鎖的特定使用者、URL 和類別。回應頁面參照允許使用映像、聲音、樣式表和連結。

Panorama™ 網頁介面不支援匯出回應頁面。

大於支援大小上限的自訂回應頁面不會被解密或顯示給使用者。在 *PAN-OS 8.1.2* 與較舊版本 *PAN-OS 8.1* 中，解密網站上的自訂回應頁面不能超過 *8,191* 個位元組；在 *PAN-OS 8.1.3* 及更新版本中，大小上限為 *17,999* 個位元組。

- Strata Cloud Manager
- PAN-OS 和 Panorama

自訂 URL 篩選回應頁面 (Strata Cloud Manager)

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 ***Strata Cloud Manager***，則請繼續此處操作。

STEP 1 | 匯出您要自訂的預設回應頁面。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服務） > **URL Access Management**（**URL** 存取管理） > **Settings**（設定）。
2. 在 [Response Pages（回應頁面）] 窗格中，針對您要編輯的每個回應頁面按一下 **Export HTML Template**（匯出 **HTML** 範本）。
3. 將檔案儲存到您的系統。

STEP 2 | 編輯匯出的回應頁面。

1. 使用您所選擇的 HTML 文字編輯器來編輯頁面：
   - 如果要顯示特定使用者、URL 或已封鎖類別的相關自訂資訊，請新增一個或多個回應頁面變數。
   - 若要納入自訂映像、聲音、樣式表或連結，請納入一個或多個回應頁面參照。
2. 以新檔案名稱儲存編輯的頁面。

   請確保該頁面保留其 *UTF-8* 編碼。例如，在記事本中，您從 *[Save As*（另存新檔）*]* 對話框的 ***Encoding***（編碼）下拉式清單中選取 ***UTF-8***。

STEP 3 | 匯入自訂的回應頁面。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服務） > **URL Access Management**（**URL** 存取管理） > **Settings**（設定）。
2. 在 [Response Pages（回應頁面）] 窗格中，按一下您自訂的回應頁面類型。畫面將顯示檔案選擇對話框。

   例如，如果您自訂 URL 存取管理封鎖頁面，則請按一下 **URL Access Management Block Page**（**URL** 存取管理封鎖頁面）。
3. 按一下 **Choose File**（選擇檔案），然後選取您自訂的檔案。
4. 按一下 **Save**（儲存）。

STEP 4 | 按一下 **Push Config**（推送設定）。

STEP 5 | 確定顯示自訂的回應頁面。

在 Web 瀏覽器中前往將觸發回應頁面的 URL。例如，若要確認自訂的 URL 存取管理封鎖頁面，請前往被安全性政策規則封鎖的 URL。

防火牆使用以下連接埠來顯示 URL 存取管理回應頁面：

- **HTTP**—6080
- 具有防火牆憑證的預設 **TLS**—6081
- 自訂 **SSL/TLS** 設定檔—6082

自訂 URL 篩選回應頁面 (PAN-OS & Panorama)

STEP 1 | 匯出您要自訂的預先定義回應頁面。

> *Panorama* 網頁介面不支援匯出回應頁面。您可以直接從特定防火牆的網頁介面匯出回應頁面，也可以使用 *Panorama* 網頁介面上的內容下拉式清單，快速切換到受管理防火牆的網頁介面。

1. 選取 **Device**（裝置） > **Response Pages**（回應頁面）。
2. 選擇您要編輯的回應頁面 **Type**（類型）。畫面會顯示特定回應頁面的對話框。
3. 選取 **Predefined**（預先定義），然後選取 **Export**（匯出）。
4. **Close**（關閉）對話框。

   (選用）針對其他回應頁面重複步驟 2 到 4。
5. 將檔案儲存到您的系統。

STEP 2 | 自訂匯出的 HTML 回應頁面。

1. 在您慣用的文字編輯器中開啟檔案。
   - 若要顯示特定使用者、要求的 URL 或封鎖的 URL 類別的相關自訂資訊，請使用回應頁面變數。
   - 若要整合自訂映像、聲音、樣式表或連結，請使用回應頁面參照。
2. 以新名稱儲存編輯後的檔案。

> 請確保該頁面保留其 *UTF-8* 編碼。例如，在記事本中，您從（另存新檔）對話方塊的 ***Encoding***（編碼）下拉式清單中選取 ***UTF-8***。

STEP 3 | 匯入自訂的回應頁面。

1. 選取 **Device**（裝置） > **Response Pages**（回應頁面）。
2. 選擇您已編輯的回應頁面 **Type**（類型）。畫面會顯示特定回應頁面的對話框。
3. 選取 **Predefined**（預先定義），然後選取 **Import**（匯入）。畫面將顯示匯入檔案對話框。

   針對 **Import File**（匯入檔案），請 **Browse**（瀏覽）已編輯的回應頁面。
4. (選用）針對 **Destination**（目的地），選取將使用該回應頁面的虛擬系統，或選取 **shared**（共用）使該回應頁面可用於所有虛擬系統。
5. 按一下 **OK**（確定），然後 **Close**（關閉）對話框。

STEP 4 | **Commit**（提交）您的變更。

STEP 5 | 測試自訂回應頁面。

從 Web 瀏覽器前往觸發特定回應頁面的 URL。例如，若要驗證 URL 篩選和類別符合回應頁面，請前往在安全性政策規則中封鎖的 URL。確認畫面是否顯示您的變更。

防火牆使用以下連接埠來顯示 URL 篩選回應頁面：

- **HTTP**—6080
- 具有防火牆憑證的預設 **TLS**—6081
- 自訂 **SSL/TLS** 設定檔—6082

安全搜尋強制

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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。 • 透明安全搜尋需要執行至少版本 4.1 的 Prisma Access 授權。

許多搜尋引擎皆提供安全的搜尋設定，可讓您從搜尋結果中過濾成人內容。篩選設定通常包括中度、嚴格和關閉。您可以使用中度設定，僅篩選成人影像和影片，或使用嚴格設定額外篩選掉不雅文字。教育機構、工作場所、兒童和成人皆受益於此安全搜尋功能。但是，如果讓您網路中的使用者進行安全搜尋設定，不一定會獲得您所需的保護。

為了保護您的網路免受成人內容侵害，您都可以對所有最終使用者強制執行最嚴格的安全搜尋設定（無論其目前的個別設定為何）。最嚴格的安全搜尋設定提供最安全的瀏覽體驗。首先，選取 URL 篩選設定檔的**Safe Search Enforcement**（安全搜尋強制）選項。然後，將設定檔套用至允許信任區域中的用戶端流量流向網路的任何安全性政策規則。

搜尋引擎提供商或 *Palo Alto Networks* 都無法保證完整且準確地過濾不雅內容。搜尋引擎會將網站分類為安全或不安全。因此，分類為安全的網站可能包含不雅內容。*Palo Alto Networks* 僅根據搜尋引擎的篩選機制執行篩選。

若使用者透過 Bing、Yahoo、Yandex 或 YouTube 進行搜尋，且尚未將這些引擎的安全搜尋設定設為最嚴格的層級，防火牆可強制執行下列動作：

- 關閉嚴格安全搜尋時封鎖搜尋結果（預設）—防火牆會防止一般使用者看到搜尋結果，除非他們將安全搜尋設定設為最嚴格的可用選項。在此情況下，瀏覽器會顯示 URL 篩選安全搜尋封鎖頁面。此回應頁面會讓一般使用者知道其搜尋結果遭封鎖的原因，並提供連結前往執行該搜尋的搜尋引擎的搜尋設定。

  由於 *Google* 安全搜尋措施有所變更，*Palo Alto Networks* 無法再偵測 *Google* 安全搜尋是否啟用。因此，上述封鎖方式不適用於 *Google* 搜尋。反之，您可以使用 搜尋提供者的安全搜尋設定 中所述方式設定 *Google* 安全搜尋。

- 強制執行嚴格安全搜尋（僅支援 Yahoo 和 Bing 搜尋引擎）—防火牆會自動清楚地執行最嚴格的安全搜尋設定。具體而言，防火牆會將搜尋查詢重新導向至返回經嚴格篩選搜尋結果的 URL，並變更所使用搜尋引擎的安全搜尋偏好設定。若要啟用此功能，請將 URL 篩選安全搜尋

封鎖頁面文字取代為程序中指定的文字。替換文字包含 JavaScript 程式碼，該程式碼會使用用於搜尋引擎的嚴格安全搜尋參數來重新寫入搜尋查詢 URL。

當您使用此方法時，瀏覽器不會顯示 *URL* 篩選安全搜尋封鎖頁面。

- 透明安全搜尋（僅限 Prisma Access 部署）—如果無法解密流量（例如在提供客人網路存取的商店），且您希望防止具未受管裝置（包括顯示裝置）的使用者搜尋遭限制、不當或冒犯性的資料，您可以在 Prisma Access 中使用透明安全搜尋，透過執行 FQDN 至 IP 對應來解析行動裝置使用者到引擎安全搜尋入口網站的搜尋查詢。

檢視每個受支援搜尋引擎的安全搜尋設定，開始執行安全搜尋。然後決定哪種方法最符合您的需求。

- 搜尋提供者的安全搜尋設定
- 嚴格安全搜尋關閉時封鎖搜尋結果
- 強制執行嚴格安全搜尋
- 在 Prisma Access 中使用透明的安全搜尋

搜尋提供者的安全搜尋設定

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

各搜尋提供者的安全搜尋設定各不相同，請檢閱下列設定以瞭解更多。

搜尋供應商	安全搜尋設定說明
Google/YouTube	透過 Google 的安全搜尋虛擬 IP 位址在個別電腦或整個網路上提供安全搜尋： 個別電腦上 **Google** 搜尋的安全搜尋強制執行 在 Google 搜尋設定中，**Filter explicit results** (篩選器明確結果) 設定會啟用安全搜尋功能。啟用時，每一次使用者執行 Google 搜尋時，系統會將該設定儲存在瀏覽器 Cookie 中成為 FF=，並傳遞到伺服器。 將 **`safe=active`** 附加到 Google 搜尋查詢 URL，也會啟用最嚴格的安全搜尋設定。

搜尋供應商	安全搜尋設定說明
	使用虛擬 **IP** 位址強制讓 **Google** 與 **YouTube** 搜尋執行安全搜尋 Google 提供給伺服器在每一個 Google 與 YouTube 搜尋中會有的 Lock SafeSearch (forcesafesearch.google.com) 設定。**`www.google.com`** 與 **`www.youtube.com`**（及另一個相關的 Google 與 YouTube 國家子網域）的 DNS 項目中包含指向 **`forcesafesearch.google.com`** 的 CNAME 記錄，透過將此項目新增至 DNS 伺服器設定，您可以確定您網路上的所有使用者每次執行 Google 或 YouTube 搜尋時都會使用嚴格安全搜尋設定。但請記住，此解決方案與防火牆中的（安全搜尋強制）不相容。因此，如果您要使用此選項來對 Google 執行強制安全搜尋，最佳作法是建立自訂 URL 類別並將其新增至 URL 篩選設定檔中的封鎖清單，來封鎖對防火牆中其他搜尋引擎的存取。 • *PAN-OS* 支援透過 *HTTP* 標頭插入強制讓 *YouTube* 執行安全搜尋。*HTTP/2* 當前不支援 *HTTP* 標頭插入。若要對 *YouTube* 強制執行安全搜尋，App-ID 和 HTTP/2 檢查請使用適當解密設定檔中的 ***Strip ALPN***（除去 ***ALPN***）功能將 *HTTP/2* 連線降級為 *HTTP/1.1*。 • 如果您打算使用 *Google Lock SafeSearch* 解決方案，請考慮設定 *DNS Proxy*（***Network***（網路）> ***DNS Proxy***），然後將繼承來源設為 *Layer 3* 介面，防火牆會在此介面上透過 *DHCP* 接收來自服務供應商的 *DNS* 設定。您可以針對 *www.google.com* 與 *www.youtube.com* 設定含 ***Static Entries***（靜態項目）的 *DNS Proxy*，針對 *forcesafesearch.google.com* 伺服器使用本機 *IP* 位址。
Yahoo	只在個別電腦上提供安全搜尋。Yahoo 搜尋偏好設定包含三種 SafeSearch 設定：**Strict**（嚴

搜尋供應商	安全搜尋設定說明
	格）、**Moderate**（適中）或**Off**（關閉）。啟用時，每一次使用者執行 Yahoo 搜尋時，系統會將該設定儲存在瀏覽器 Cookie 中成為 `vm=`，並傳遞到伺服器。 將 `vm=r` 附加到 Yahoo 搜尋查詢 URL，也會啟用最嚴格的安全搜尋設定。 當您登入 *Yahoo* 帳戶後若要在日本 *Yahoo* (***yahoo.co.jp***) 上執行搜尋，一般使用者必須也啟用 ***SafeSearch Lock***（鎖定）選項。
Bing	在個別電腦上提供安全搜尋。Bing 設定包括三個 SafeSearch 設定：**Strict**（嚴格）、**Moderate**（適中）或**Off**（關閉）。啟用後，當每一次使用者執行 Bing 搜尋時，系統會將該設定作為 `adtl=` 儲存在瀏覽器 Cookie 中並傳遞到伺服器。 將 **`adlt=strict`** 附加到 Bing 搜尋查詢 URL，也會啟用最嚴格的安全搜尋設定。 Bing SSL 搜尋引擎不強制執行安全搜尋 URL 參數，因此您應考慮封鎖經由 SSL 的 Bing，以強制執行完整的安全搜尋。

嚴格安全搜尋關閉時封鎖搜尋結果

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

如果啟用安全搜尋強制，防火牆的預設行為是封鎖一般使用者在 Bing、Yahoo、Yandex 或 Youtube 搜尋引擎上的搜尋結果，除非使用者將安全搜尋設定設為最嚴格的可用選項。根據預設，瀏覽器會顯示 URL 篩選安全搜尋封鎖頁面。預先定義的封鎖頁面會提供所用搜尋引擎的搜尋設定連結，以讓使用者能調整安全搜尋設定。您可以自訂安全搜尋封鎖頁面以滿足組織的特定需求。

如果您打算使用此方法強制執行安全搜尋，請在實作政策前先向使用者傳達政策內容。如果您希望自動將一般使用者的搜尋查詢 URL 重新導向至嚴格安全搜尋版本，請啟用透明的嚴格安全搜尋。

由於 *Google* 安全搜尋有變更，*Palo Alto Networks* 無法再偵測 *Google* 安全搜尋是否開啟。因此，防火牆無法使用此方法強制執行安全搜尋。您仍然可以透明地執行安全搜尋。但是，我們無法保證 *Google* 會篩選掉不雅的圖片和內容。

- Strata Cloud Manager
- PAN-OS 和 Panorama

嚴格安全搜尋關閉時封鎖搜尋結果 (Strata Cloud Manager)

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 ***Strata Cloud Manager***，則請繼續此處操作。

STEP 1 | 啟用 URL 存取管理設定檔中的安全搜尋強制。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **Security Services**（安全服務） > **URL Access Management**（**URL** 存取管理）。
2. 在 URL 存取管理設定檔下，點選現有設定檔或 **Add Profile**（新增設定檔）以建立新的設定檔。畫面會顯示設定選項。
3. 在 **Settings**（設定）下，選取 **Safe Search Enforcement**（安全搜尋強制）。
4. **Save**（儲存）設定檔。

STEP 2 | (選用）限制一般使用者可以存取的搜尋引擎。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **Security Services**（安全服務） > **URL Access Management**（**URL** 存取管理）。
2. 在 **Access Control**（存取控制）下，**Search**（搜尋）( ) **search-engines**（搜尋引擎）類別。
3. 將 **search-engines**（搜尋引擎）類別的網站存取設為 **block**（封鎖）。

   在稍後步驟中，您將建立一個自訂 URL 類別（URL 清單類型），其中包括您要允許的搜尋引擎。
4. **Save**（儲存）設定檔。

STEP 3 | 將 URL 存取管理設定檔套用至允許信任區域中的用戶端流量流向網路的安全性政策規則。

若要啟用 URL 存取管理設定檔（以及任何安全性設定檔），請將其新增至設定檔群組，並在安全性政策規則中參照該設定檔群組。

STEP 4 | 針對支援的搜尋引擎建立自訂 URL 類別。

在下一個步驟中，您將設定防火牆以解密流向此自訂類別的流量。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **Security Services**（安全服務） > **URL Access Management**（**URL** 存取管理）。
2. 在 **Access Control**（存取控制）下，針對自訂 URL 類別 **Add Category**（新增類別）。
3. 針對類別輸入 **Name**（名稱），例如 **`SearchEngineDecryption`**。
4. 針對自訂 URL 類別的 **Type**（類型），選取 **URL List**（**URL** 清單）。

5. 在 **Items**（項目）下，將以下項目 **Add**（新增）至 URL 清單：
   - **`www.bing.*`**
   - **`search.yahoo.*`**
   - **`yandex.com.*`**
6. **Save**（儲存）自訂類別。
7. 為新的自訂 URL 類別設定網站存取。
   1. 在 URL 存取管理設定檔下，選取您先前設定的設定檔。
   2. 在存取控制下，選取新的自訂 URL 類別。它會顯示在 自訂 URL 類別部分的（外部動態 URL 清單和預先定義的類別上方）。
   3. 將 **Site Access**（網站存取）設為 **allow**（允許）。
   4. **Save**（儲存）變更。

STEP 5 | 設定 SSL 正向 Proxy 解密。

因為大多數的搜尋引擎會將其搜尋結果加密，所以您也必須啟用 Ssl 正向 Proxy 解密，讓防火牆能夠檢查搜尋流量，並偵測安全搜尋設定。

在解密政策規則的 **Services and URLs**（服務和 **URL**）區段下，按一下 **Add URL Categories**（新增 **URL** 類別）。然後，選擇您先前建立的自訂 URL 類別。新的自訂類別會位於清單頂部。

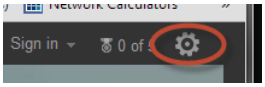
Save（儲存）解密政策規則。

STEP 6 | 點選 **Push Config**（推送設定）以啟動您的變更。

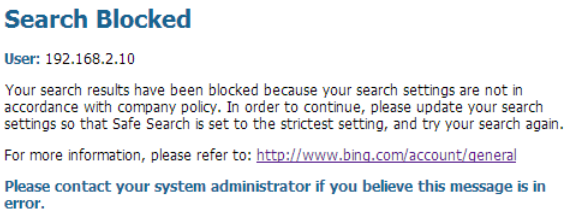
STEP 7 | 驗證安全搜尋強制設定。

此驗證步驟僅適用於您使用封鎖頁面強制執行安全搜尋時。如果您啟用透明安全搜尋，則還有另一種驗證步驟。

1. 從防火牆後方的電腦來停用受支援搜尋供應商的嚴格搜尋設定。例如在 bing.com 上，按一下 Bing 工作表列上的 **Preferences**（偏好設定）圖示。



2. 將 **SafeSearch**（安全搜尋）選項設為 **Moderate**（適中）或 **Off**（關閉），然後按一下 **Save**（儲存）。
3. 執行 Bing 搜尋（或透過其他供應商進行搜尋），並檢視是否顯示 URL 存取管理安全搜尋封鎖頁面，而非顯示搜尋結果：



4. 透過封鎖頁面上的連結將安全搜尋設定設為最嚴格的等級（Bing 的 **Strict**（嚴格）），然後按一下 **Save**（儲存）。
5. 從 Bing 再次執行搜尋，並確認會顯示篩選後的搜尋結果，而非顯示封鎖頁面。

嚴格安全搜尋關閉時封鎖搜尋結果 (PAN-OS & Panorama)

STEP 1 | 啟用 URL 篩選設定檔中的安全搜尋強制。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **URL Filtering**（URL 篩選）。
2. 選取現有設定檔進行修改，或複製預設設定檔以建立新的設定檔。
3. 在 **URL Filtering Setting**（URL 篩選設定）頁籤上，選取 **Safe Search Enforcement**（安全搜尋強制）。

STEP 2 | (選用）限制一般使用者可以在同一個 URL 篩選設定檔中存取的搜尋引擎。

1. 在 **Categories**（類別）頁籤上，**Search**（搜尋）( ) **search-engines**（搜尋引擎）類別。
2. 將 **search-engines**（搜尋引擎）類別的網站存取設為 **block**（封鎖）。

   在稍後步驟中，您將建立一個自訂 URL 類別（URL 清單類型），其中包括您要允許的搜尋引擎。
3. 按一下 **OK**（確定）來儲存設定檔。

STEP 3 | 將 URL 篩選設定檔套用至允許信任區域中的用戶端流量流向網路的安全性政策規則。

1. 選取 **Policies**（政策） > **Security**（安全性）。然後，點選要套用 URL 篩選設定檔的規則。
2. 在 **Actions**（動作）頁籤中，找到設定檔設定。針對 **Profile Type**（設定檔類型）選取 **Profiles**（設定檔）。接著畫面將顯示設定檔清單。
3. 針對 **URL Filtering**（**URL** 篩選）設定檔，選取您先前建立的設定檔。
4. 按一下 **OK**（確定）來儲存安全性原則規則。

STEP 4 | 針對支援的搜尋引擎建立自訂 URL 類別。

在以下步驟中，您將指定要解密的自訂類別中網站的流量。

1. 選取 **Objects**（物件） > **Custom Objects**（自訂物件） > **URL Category**（**URL** 類別），然後 **Add**（新增） 自訂類別。
2. 針對類別輸入 **Name**（名稱），例如 **`SearchEngineDecryption`**。
3. 將下列項目 **Add**（新增）至 **Sites**（網站）清單：
   - **`www.bing.*`**
   - **`search.yahoo.*`**
   - **`yandex.com.*`**
4. 按一下 **OK**（確定）以儲存自訂類別。
5. 為新的自訂 URL 類別設定網站存取。
   1. 前往 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **URL Filtering**（**URL** 篩選），並選取您先前設定的 URL 篩選設定檔。
   2. 在 **Category**（類別）頁籤中，選取新的自訂 URL 類別。它會顯示在 自訂 URL 類別部分的（外部動態 URL 清單和預先定義的類別上方）。
   3. 將 **Site Access**（網站存取）設為 **allow**（允許）。
   4. 按一下 **OK**（確定）儲存您的變更。

STEP 5 | 設定 SSL 正向 Proxy 解密。

因為大多數的搜尋引擎會將其搜尋結果加密，所以您也必須啟用 Ssl 正向 Proxy 解密，讓防火牆能夠檢查搜尋流量，並偵測安全搜尋設定。

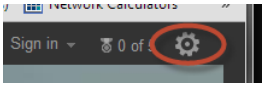
在解密政策規則的 **Service/URL Category**（服務/**URL** 類別）頁籤中，**Add**（新增）您先前建立的自訂 URL 類別。然後按一下 **OK**（確定）。

STEP 6 | **Commit**（提交）您的變更。

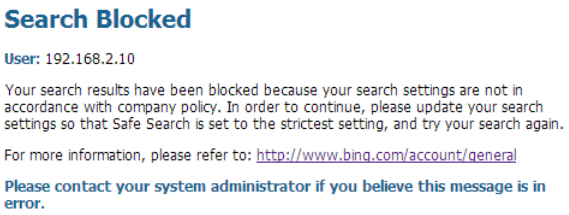
STEP 7 | 驗證安全搜尋強制設定。

此驗證步驟僅適用於您使用封鎖頁面強制執行安全搜尋時。如果您啟用透明安全搜尋，則還有另一種驗證步驟。

1. 從防火牆後方的電腦來停用受支援搜尋供應商的嚴格搜尋設定。例如在 bing.com 上，按一下 Bing 工作表列上的 **Preferences**（偏好設定）圖示。



2. 將 **SafeSearch**（安全搜尋）選項設為 **Moderate**（適中）或 **Off**（關閉），然後按一下 **Save**（儲存）。
3. 執行 Bing 搜尋（或透過其他供應商進行搜尋），並檢視是否顯示 URL 篩選安全搜尋封鎖頁面，而非顯示搜尋結果：



4. 透過封鎖頁面上的連結將安全搜尋設定設為最嚴格的等級（Bing 的 **Strict**（嚴格）），然後按一下 **Save**（儲存）。
5. 從 Bing 再次執行搜尋，並確認會顯示篩選後的搜尋結果，而非顯示封鎖頁面。

強制執行嚴格安全搜尋

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

您可以透明地啟用嚴格的安全搜尋，為 Bing 和 Yahoo 一般使用者提供安全且順暢的搜尋體驗。當一般使用者在未啟用嚴格安全搜尋的情況下進行搜尋時，防火牆不會封鎖搜尋結果，而是自動開啟嚴格安全搜尋並僅傳回嚴格篩選後的搜尋結果。例如，學校和圖書館可以受益於此自動執行功能，確保使用者獲得一致的學習經驗。

若要啟動透明的安全搜尋強制，您需要在 URL 篩選設定檔中啟用安全搜尋強制，並將 URL 篩選安全搜尋封鎖頁面檔案中的文字改為下列步驟中的文字。取代文字包含 JavaScript，該 JavaScript 為用於搜尋的搜尋引擎附加帶有嚴格安全搜尋參數的搜尋查詢 URL。

瀏覽器不會顯示 *URL* 篩選安全搜尋封鎖頁面。

完成這些步驟後，只要一般使用者進行搜尋，防火牆就會執行 JavaScript。例如，假設學生的搜尋內容可能產生不當結果，他們的 Bing 安全搜尋偏好設定會設為關閉。防火牆偵測到安全搜尋偏好設定之後，會將 `&adlt=strict` 附加到搜尋查詢 URL。然後，搜尋引擎會顯示適當結果，且安全搜尋偏好設定會變更為嚴格。

- Strata Cloud Manager
- PAN-OS 和 Panorama

強制執行嚴格安全搜尋 (Strata Cloud Manager)

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

請切換到 ***PAN-OS & Panorama*** 頁籤並按照指示進行操作。

如果您使用 ***Strata Cloud Manager***，則請繼續此處操作。

STEP 1 | 啟用 URL 存取管理設定檔中的安全搜尋強制。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **Security Services**（安全服務） > **URL Access Management**（**URL** 存取管理）。
2. 在 URL 存取管理設定檔下，點選現有設定檔或 **Add Profile**（新增設定檔）以建立新的設定檔。畫面會顯示設定選項。
3. 在 **Settings**（設定）下，選取 **Safe Search Enforcement**（安全搜尋強制）。
4. **Save**（儲存）設定檔。

STEP 2 | (選用）限制一般使用者可以存取的搜尋引擎。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **Security Services**（安全服務） > **URL Access Management**（**URL** 存取管理）。
2. 在 **Access Control**（存取控制）下，**Search**（搜尋）( ) **search-engines**（搜尋引擎）類別。
3. 將 **search-engines**（搜尋引擎）類別的網站存取設為 **block**（封鎖）。

   在稍後步驟中，您將建立一個自訂 URL 類別（URL 清單類型），其中包括您要允許的搜尋引擎。
4. **Save**（儲存）設定檔。

STEP 3 | 將 URL 存取管理設定檔套用至允許信任區域中的用戶端流量流向網路的安全性政策規則。

若要啟用 URL 存取管理設定檔（以及任何安全性設定檔），請將其新增至設定檔群組，並在安全性政策規則中參照該設定檔群組。

STEP 4 | 編輯 URL 存取管理安全搜尋封鎖頁面，將現有的指令碼取代為 JavaScript 以重新寫入搜尋查詢 URL。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **Security Services**（安全服務） > **URL Access Management**（**URL** 存取管理） > **Response Pages**（回應頁面）。
2. **Export HTML Template**（匯出 **URL** 存取管理封鎖頁面的 **HTML** 範本）。

3. 使用 HTML 編輯器，並將所有現有的封鎖頁面文字取代成下列文字。然後儲存檔案。

```
<html> <head> <title>搜尋已遭到封鎖</title> <meta http-
equiv="Content-Type" content="text/html; charset=utf-8">
 <meta http-equiv="pragma" content="no-cache"> <meta
 name="viewport" content="initial-scale=1.0"> <style> #content
 { border:3px solid#aaa; background-color:#fff; margin:1.5em;
 padding:1.5em; font-family:Tahoma,Helvetica,Arial,sans-serif;
 font-size:1em; } h1 { font-size:1.3em; font-weight:bold;
 color:#196390; } b { font-weight:normal; color:#196390; }
 </style> </head> <body bgcolor="#e7e8e9"> <div id="content">
 <h1>搜尋已遭到封鎖</h1> <p> <b>使用者：</b><user/> </p> <p>您的搜
尋結果已遭到封鎖，因為您的搜尋設定不符合公司政策。若要繼續，請更新您的搜尋
設定，以便將 Safe Search（安全搜尋）設定為最嚴格的設定。如果您目前已登
入帳戶，請同時鎖定 Safe Search（安全搜尋）並再次嘗試搜尋。</p><p> 如
需詳細資訊，請參閱：<a href="<ssurl/>"> <ssurl/> </a> </p> <p
 id="java_off"> 請在您的瀏覽器中啟用 JavaScript。<br></p><p><b>如
果您認為此訊息有誤，請聯絡您的系統管理員。</b> </p> </div> </body>
 <script> // Grab the URL that's in the browser. var s_u =
 location.href; //bing // Matches the forward slashes in the
 beginning, anything, then ".bing." then anything followed
 by a non greedy slash.Hopefully the first forward slash.
 var b_a = /^.*\/\/(.+\.bing\..+?)\//.exec(s_u); if (b_a)
 { s_u = s_u + "&adlt=strict"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML =
 'You are being redirected to a safer search!'; } //
yahoo // Matches the forward slashes in the beginning,
 anything, then ".yahoo."" then anything followed by
 a non greedy slash.Hopefully the first forward slash.
 var y_a = /^.*\/\/(.+\.yahoo\..+?)\//.exec(s_u);
 if (y_a) { s_u = s_u.replace(/&vm=p/ig,""); s_u
 = s_u + "&vm=r"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML =
 'You are being redirected to a safer search!'; }
 document.getElementById("java_off").innerHTML = ' '; </
script> </html>
```

STEP 5 | 在防火牆上匯入已編輯的 URL 存取管理安全搜尋封鎖頁面。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **Security Services**（安全服務） > **URL Access Management**（URL 存取管理） > **Response Pages**（回應頁面）。
2. 按一下 [URL Access Management Safe Search Block Page（URL 存取管理安全搜尋封鎖頁面）]。畫面會出現一個對話框，其中有 **Choose File**（選擇檔案）選項。
3. 選取您先前編輯的安全搜尋封鎖頁面檔案，然後按一下 **Save**（儲存）。

STEP 6 | 針對支援的搜尋引擎建立自訂 URL 類別。

在下一個步驟中，您將設定防火牆以解密流向此自訂類別的流量。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **Security Services**（安全服務） > **URL Access Management**（**URL** 存取管理）。
2. 在 **Access Control**（存取控制）下，針對自訂 URL 類別 **Add Category**（新增類別）。
3. 針對類別輸入 **Name**（名稱），例如 **`SearchEngineDecryption`**。
4. 針對自訂 URL 類別的 **Type**（類型），選取 **URL List**（**URL** 清單）。
5. 在 **Items**（項目）下，將以下項目 **Add**（新增）至 URL 清單：
   - **`www.bing.*`**
   - **`search.yahoo.*`**
   - **`yandex.com.*`**
6. **Save**（儲存）自訂類別。
7. 為新的自訂 URL 類別設定網站存取。
   1. 在 URL 存取管理設定檔下，選取您先前設定的設定檔。
   2. 在存取控制下，選取新的自訂 URL 類別。它會顯示在 自訂 URL 類別部分的（外部動態 URL 清單和預先定義的類別上方）。
   3. 將 **Site Access**（網站存取）設為 **allow**（允許）。
   4. **Save**（儲存）變更。

STEP 7 | 設定 SSL 正向 Proxy 解密。

因為大多數的搜尋引擎會將其搜尋結果加密，所以您也必須啟用 Ssl 正向 Proxy 解密，讓防火牆能夠檢查搜尋流量，並偵測安全搜尋設定。

在解密政策規則的 **Services and URLs**（服務和 **URL**）區段下，按一下 **Add URL Categories**（新增 **URL** 類別）。然後，選擇您先前建立的自訂 URL 類別。新的自訂類別會位於清單頂部。

Save（儲存）解密政策規則。

STEP 8 | 點選 **Push Config**（推送設定）以啟動您的變更。

STEP 9 | 驗證安全搜尋強制設定。

在防火牆後方的電腦上開啟瀏覽器並使用 Bing、Yahoo 或 Yandex 執行搜尋。然後，使用以下任一方法確認您的設定：

- 檢查 URL 的查詢字串以取得安全搜尋參數。搜尋供應商的安全搜尋設定列出了附加到每個搜尋查詢 URL 的安全搜尋參數。
- 前往受支援搜尋引擎的安全搜尋設定，並確認所選安全搜尋偏好設定是否是最嚴格的等級（多數為 **Strict**（嚴格）等級）。

強制執行嚴格安全搜尋 (PAN-OS & Panorama)

STEP 1 | 確定防火牆執行的是內容發行版本 475 或更新版本。

1. 請選取 **Device**（裝置） > **Dynamic Updates**（動態更新）。（裝置 > 動態更新）.
2. 檢查 **Applications and Threats**（應用程式與威脅）區段，以判斷目前正在執行的是何種更新。
3. 如果防火牆未執行必要或更新版的更新，請按一下 **Check Now**（立即檢查）來擷取可用更新清單。
4. 找到所需的更新，然後按一下 **Download**（下載）。
5. 完成下載後，按一下 **Install**（安裝）。

STEP 2 | 啟用 URL 篩選設定檔中的安全搜尋強制。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **URL Filtering**（**URL** 篩選）。
2. 選取現有設定檔進行修改，或複製預設設定檔以建立新的設定檔。
3. 在 **URL Filtering Setting**（**URL** 篩選設定）頁籤上，選取 **Safe Search Enforcement**（安全搜尋強制）。

STEP 3 | (選用）限制一般使用者可以在同一個 URL 篩選設定檔中存取的搜尋引擎。

1. 在 **Categories**（類別）頁籤上，**Search**（搜尋）( ) **search-engines**（搜尋引擎）類別。
2. 將 **search-engines**（搜尋引擎）類別的網站存取設為 **block**（封鎖）。

   在稍後步驟中，您將建立一個自訂 URL 類別（URL 清單類型），其中包括您要允許的搜尋引擎。
3. 按一下 **OK**（確定）來儲存設定檔。

STEP 4 | 將 URL 篩選設定檔套用至允許信任區域中的用戶端流量流向網路的安全性政策規則。

1. 選取 **Policies**（政策） > **Security**（安全性）。然後，點選要套用 URL 篩選設定檔的規則。
2. 在 **Actions**（動作）頁籤中，找到設定檔設定。針對 **Profile Type**（設定檔類型）選取 **Profiles**（設定檔）。接著畫面將顯示設定檔清單。
3. 針對 **URL Filtering**（**URL** 篩選）設定檔，選取您先前建立的設定檔。
4. 按一下 **OK**（確定）來儲存安全性原則規則。

STEP 5 | 編輯 URL 篩選安全搜尋封鎖頁面，將現有的指令碼取代為 JavaScript 以重新寫入搜尋查詢 URL。

1. 選取 **Device**（裝置） > **Response Pages**（回應頁面） > **URL Filtering Safe Search Block Page**（**URL** 篩選安全搜尋封鎖頁面）。
2. 選取 **Predefined**（預先定義），然後按一下 **Export**（匯出）將檔案儲存在本機。
3. 使用 HTML 編輯器，並將所有現有的封鎖頁面文字取代成下列文字。然後儲存檔案。

```
<html> <head> <title>搜尋已遭到封鎖</title> <meta http-
equiv="Content-Type" content="text/html; charset=utf-8">
 <meta http-equiv="pragma" content="no-cache"> <meta
```



```
 name="viewport" content="initial-scale=1.0"> <style> #content
 { border:3px solid#aaa; background-color:#fff; margin:1.5em;
 padding:1.5em; font-family:Tahoma,Helvetica,Arial,sans-serif;
 font-size:1em; } h1 { font-size:1.3em; font-weight:bold;
 color:#196390; } b { font-weight:normal; color:#196390; }
 </style> </head> <body bgcolor="#e7e8e9"> <div id="content">
 <h1>搜尋已遭到封鎖</h1> <p> <b>使用者：</b><user/> </p> <p>您的搜
尋結果已遭到封鎖，因為您的搜尋設定不符合公司政策。若要繼續，請更新您的搜尋
設定，以便將 Safe Search（安全搜尋）設定為最嚴格的設定。如果您目前已登
入帳戶，請同時鎖定 Safe Search（安全搜尋）並再次嘗試搜尋。</p><p> 如
需詳細資訊，請參閱：<a href="<ssurl/>"> <ssurl/> </a> </p> <p
 id="java_off"> 請在您的瀏覽器中啟用 JavaScript。<br></p><p><b>如
果您認為此訊息有誤，請聯絡您的系統管理員。</b> </p> </div> </body>
 <script> // Grab the URL that's in the browser. var s_u =
 location.href; //bing // Matches the forward slashes in the
 beginning, anything, then ".bing." then anything followed
 by a non greedy slash.Hopefully the first forward slash.
 var b_a = /^.*\/\/(.+\.bing\..+?)\//.exec(s_u); if (b_a)
 { s_u = s_u + "&adlt=strict"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML =
 'You are being redirected to a safer search!'; } //
yahoo // Matches the forward slashes in the beginning,
 anything, then ".yahoo."" then anything followed by
 a non greedy slash.Hopefully the first forward slash.
 var y_a = /^.*\/\/(.+\.yahoo\..+?)\//.exec(s_u);
 if (y_a) { s_u = s_u.replace(/&vm=p/ig,""); s_u
 = s_u + "&vm=r"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML =
 'You are being redirected to a safer search!'; }
 document.getElementById("java_off").innerHTML = ' '; </
script> </html>
```

STEP 6 | 在防火牆上匯入已編輯的 URL 篩選安全搜尋封鎖頁面。

1. 選取 **Device**（裝置） > **Response Pages**（回應頁面） > **URL Filtering Safe Search Block Page**（URL 篩選安全搜尋封鎖頁面）。
2. 按一下 **Import**（匯入）。然後 **Browse**（瀏覽）封鎖網頁檔案，或在 **Import File**（匯入檔案）欄位中輸入路徑與檔案名稱。
3. （選用）針對 **Destination**（目的地），選取要使用該登入頁面的虛擬系統，或選取 **shared**（共用）以使該登入頁面可用於所有虛擬系統。
4. 按一下 **OK**（確定）匯入檔案。

STEP 7 | 針對支援的搜尋引擎建立自訂 URL 類別。

在下一個步驟中，您將設定防火牆以解密流向此自訂類別的流量。

1. 選取 **Objects**（物件） > **Custom Objects**（自訂物件） > **URL Category**（**URL** 類別），然後 **Add**（新增） 自訂類別。
2. 針對類別輸入 **Name**（名稱），例如 **`SearchEngineDecryption`**。
3. 將下列項目 **Add**（新增）至 **Sites**（網站）清單：
   - **`www.bing.*`**
   - **`search.yahoo.*`**
   - **`yandex.com.*`**
4. 按一下 **OK**（確定）儲存自訂的 URL 類別。

STEP 8 | 設定 SSL 正向 Proxy 解密。

因為大多數的搜尋引擎會將其搜尋結果加密，所以您也必須啟用 Ssl 正向 Proxy 解密，讓防火牆能夠檢查搜尋流量，並偵測安全搜尋設定。

在解密政策規則的 **Service/URL Category**（服務/**URL** 類別）頁籤中，**Add**（新增）您先前建立的自訂 URL 類別。然後按一下 **OK**（確定）。

STEP 9 | **Commit**（提交）您的變更。

STEP 10 | 驗證安全搜尋強制設定。

在防火牆後方的電腦上開啟瀏覽器並使用 Bing 或 Yahoo 執行搜尋。然後，使用以下任一方法確認您的設定是否按照預期運作：

- 檢查 URL 的查詢字串以取得安全搜尋參數。搜尋供應商的安全搜尋設定列出了附加到每個搜尋查詢 URL 的安全搜尋參數。
- 前往搜尋引擎的安全搜尋設定，並確認所選安全搜尋偏好設定是否是最嚴格的等級（Bing 的**Strict**（嚴格）等級）。

在 Prisma Access 中使用透明的安全搜尋

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) 如果您想在 Prisma Access 環境中使用此功能，請與您的帳戶團隊聯繫以瞭解更多資訊。	❑ 執行最低版本 4.1 的 Prisma Access 部署 ❑ Prisma Access 授權

Prisma Access 可讓您執行 FQDN 到 IP 對應，將行動使用者搜尋引擎查詢解析至引擎的安全搜尋入口網站。當無法解密流量（例如在提供訪客網路存取的商店），且您想要防止使用未受管裝置（包括顯示裝置）的使用者搜尋受限制、不當或侵犯性的資料時，請使用透明的安全搜尋來替代嚴格的安全搜尋。

- Strata Cloud Manager
- Panorama

在 Prisma Access 中使用透明的安全搜尋 (Strata Cloud Manager)

若要設定 Strata Cloud Manager 中的 Prisma Access 透明安全搜尋支援，請完成以下步驟。您可以為遠端網路或 GlobalProtect 行動使用者設定透明的安全搜尋。

STEP 1 | 選擇要為其設定安全搜尋的部署類型（行動使用者或遠端網路）。

- 針對行動使用者—GlobalProtect 部署，請前往 **Manage**（管理） > **Service Setup**（服務設定） > **Mobile Users**（行動使用者），然後選取 **GlobalProtect Setup**（**GlobalProtect** 設定） > **Infrastructure Settings**（基礎架構設定）。

  如果您使用的是 Strata Cloud Manager，請前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Mobile Users**（行動使用者），然後選取 **GlobalProtect Setup**（**GlobalProtect** 設定） > **Infrastructure Settings**（基礎架構設定）。
- 針對遠端網路部署，請前往 **Manage**（管理） > **Service Setup**（服務設定） > **Remote Networks**（遠端網路）。

  如果您使用的是 Strata Cloud Manager，請前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Remote Networks**（遠端網路）。

STEP 2 | 選取 **Advanced Settings**（進階設定）。

STEP 3 | 使用 **Static Entries**（靜態項目）將 FQDN 解析為特定 IP 位址。

STEP 4 | 輸入靜態條目規則的唯一 **Name**（名稱）、搜尋引擎的 **FQDN** 以及應將 FQDN 要求重新導向到的搜尋引擎安全搜尋 IP **Address**（位址）。

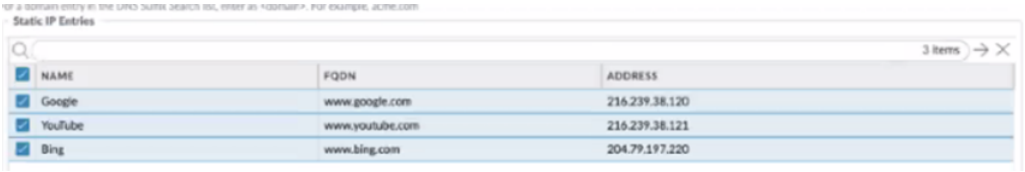
在 Prisma Access 中使用透明的安全搜尋 (Panorama)

若要設定 Panorama 中的 Prisma Access 透明安全搜尋支援，請完成以下步驟。您可以為遠端網路或 GlobalProtect 行動使用者設定透明的安全搜尋。

STEP 1 | 選擇要為其設定安全搜尋的部署類型（行動使用者或遠端網路）。

- 針對行動使用者 - GlobalProtect 部署，請前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users—GlobalProtect**（行動使用者 - **GlobalProtect**），在 **Onboarding**（裝載） 區段中選取 **Configure**（設定），然後選取 **Network Services**（網路服務）。
- 針對遠端網路部署，請前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路），按一下齒輪以編輯 **Settings**（設定），然後選取 **DNS Proxy**。

STEP 2 | 輸入靜態條目規則的唯一 **Name**（名稱）、搜尋引擎的 **FQDN** 以及應將 FQDN 要求重新導向到的搜尋引擎安全搜尋 IP **Address**（位址）來輸入 **Static IP Entries**（靜態 **IP** 項目）。



與第三方遠端瀏覽器隔離供應商整合

這可在何處使用？	我需要什麼？
• Prisma Access (Managed by Strata Cloud Manager)	❑ 進階 URL 篩選授權 註：Prisma Access 授權包括 *Advanced URL Filtering* 功能。

雖然這是最安全的方式，但封鎖未知和具風險的網站可能會減損使用者的體驗和生產力。遠端瀏覽器隔離 (RBI) 會將使用者從未知或具風險的網站重新導向至由 RBI 供應商託管的隔離環境。該網站專為使用者設計，讓使用者可以查看所需資源，而不需從其端點直接存取未知或具風險的網站。

Prisma Access 可以輕易與 RBI 供應商整合，以達成此瀏覽器重新導向功能。您只需一、兩步驟即可選擇欲整合的 RBI 供應商，並選擇要將使用者重新導向至 RBI 供應商託管環境的 URL 類別。

除了第三方 *RBI* 供應商之外，*Palo Alto Networks* 的遠端瀏覽器隔離 (RBI) 也可以與 *Prisma Access* 原生整合。與其他隔離解決方案不同的是，*RBI* 使用新世代隔離技術，在不影響安全性的前提之下，為造訪網站的使用者提供近乎原生的體驗。

以下是與 Prisma Access 整合的 RBI 供應商—部分供應商可能會要求您將 RBI 環境詳細資訊（例如虛名 URL 或租用戶 ID）新增至 Strata Cloud Manager 以設定整合操作：

- ❑ **Palo Alto Networks 的 RBI**

  若要與 *Palo Alto Networks* 的 *RBI* 進行整合，您需要設定遠端瀏覽器隔離。
- ❑ **Authentic8**

  若要與 *Authentic8* 進行整合，請先準備 *Authentic8 RBI* 環境的虛名 *URL*。
- ❑ **Proofpoint**

  若要與 *Proofpoint* 進行整合，請為 *RBI* 選擇使用 *Proofpoint* 生產或 *PoC* 環境。
- ❑ **Ericom**

  若要與 *Ericom* 進行整合，請先準備 *Ericom RBI* 環境的租用戶 *ID*。
- ❑ **Menlo Security**

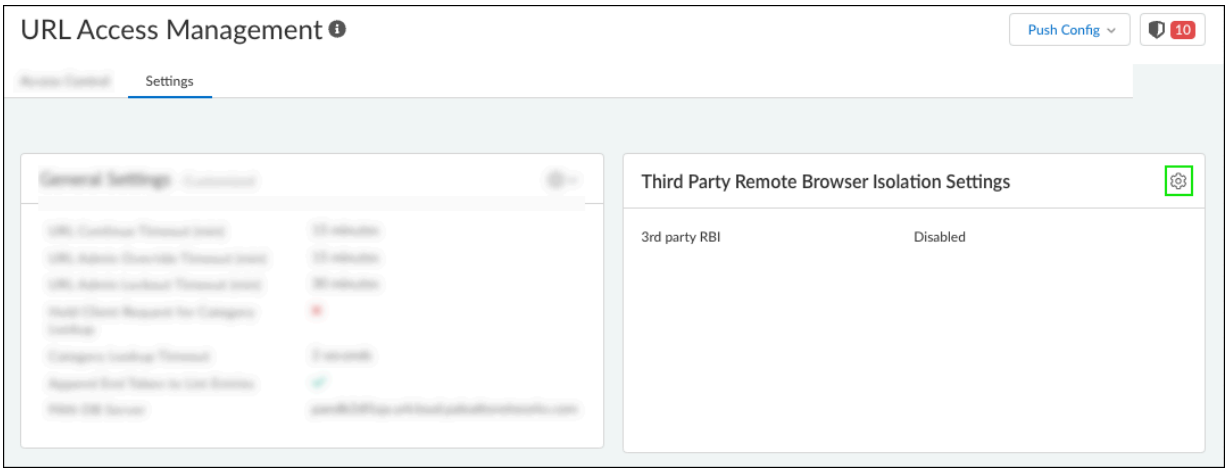
  您無需為 *Menlo Security RBI* 環境進行任何設定；您只需要啟用整合即可。

以下說明如何將您的第三方 RBI 供應商新增至 Strata Cloud Manager，並指定將使用者重新導向至 RBI 環境的 URL 類別。

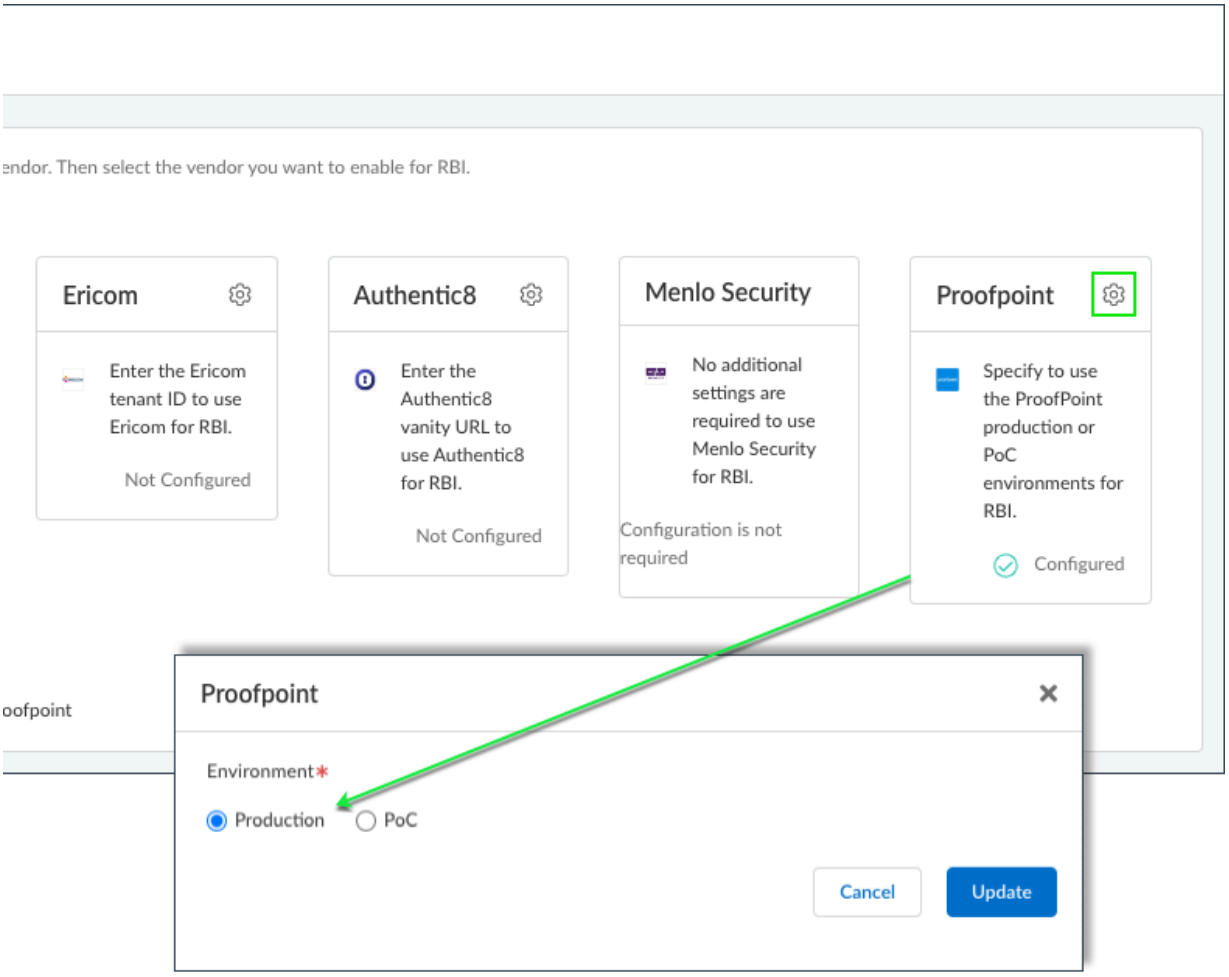
STEP 1 | 設定遠端瀏覽器隔離 (RBI)。

- 前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服務） > **URL Access Management**（**URL** 存取管理） > **Settings**（設定），然後開啟 **Third Party Remote Browser Isolation Settings**（第三方遠端瀏覽器隔離設定）。
- **IF YOU'RE A WEB SECURITY ADMIN**（如果您是 **Web** 安全性管理員）：前往 **Manage**（管理） > **Configuration**（設定） > **Web Security**（**Web** 安全性） > **Threat**

Management（威脅管理），然後開啟 **Third Party Remote Browser Isolation Settings**（第三方遠端瀏覽器隔離設定）。

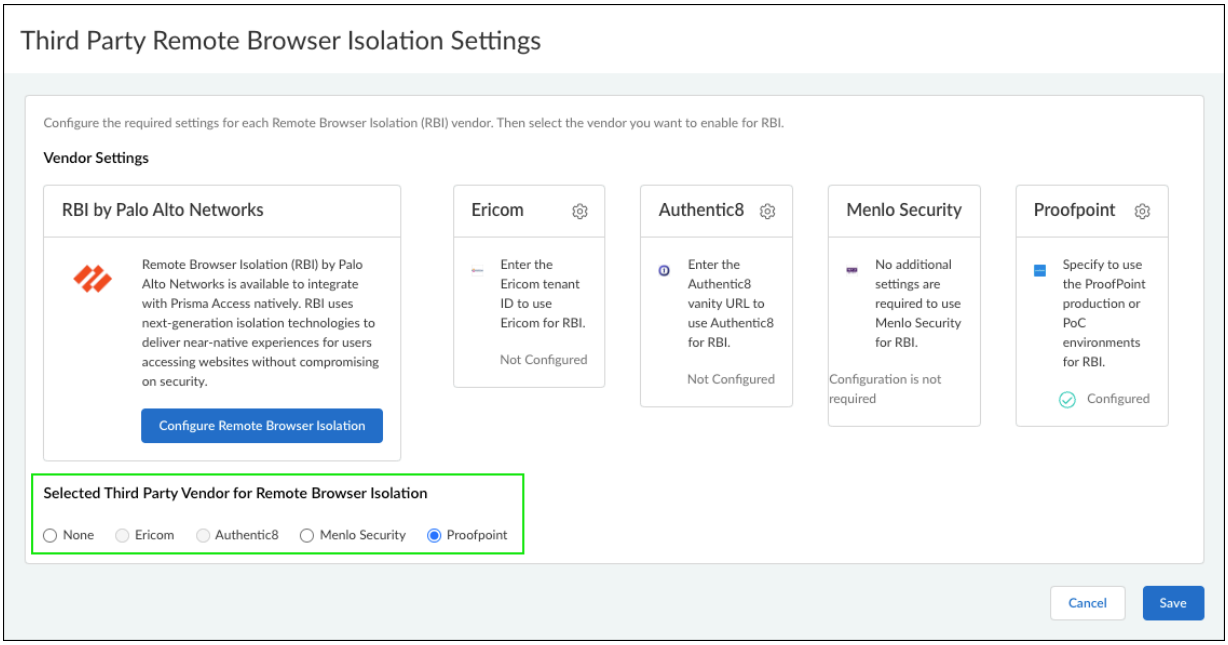


STEP 2 | 檢查 RBI 是否要求您指定您要使用的 RBI 環境；如果是的話，請輸入所需設定。



STEP 3 | 接著選取您要啟用的第三方 RBI 供應商並 **Save**（儲存）。完成了#當您下次 **Push Config**（推送設定）時，您的 RBI 供應商將與 Prisma Access 整合。

如果您已購買並啟動 Palo Alto Networks 的 RBI 授權，您也可以 ***Configure Remote Browser Isolation***（設定遠端瀏覽器隔離）。但是，您不能同時使用 *Palo Alto Networks* 的 *RBI* 和第三方 *RBI* 供應商進行隔離。如果您選擇使用 *Palo Alto Networks* 的 *RBI*，請選取 ***None***（無），否則請從 ***Selected Third Party Vendor for Remote Browser Isolation***（所選遠端瀏覽器隔離第三方供應商）中選取第三方 *RBI* 供應商。

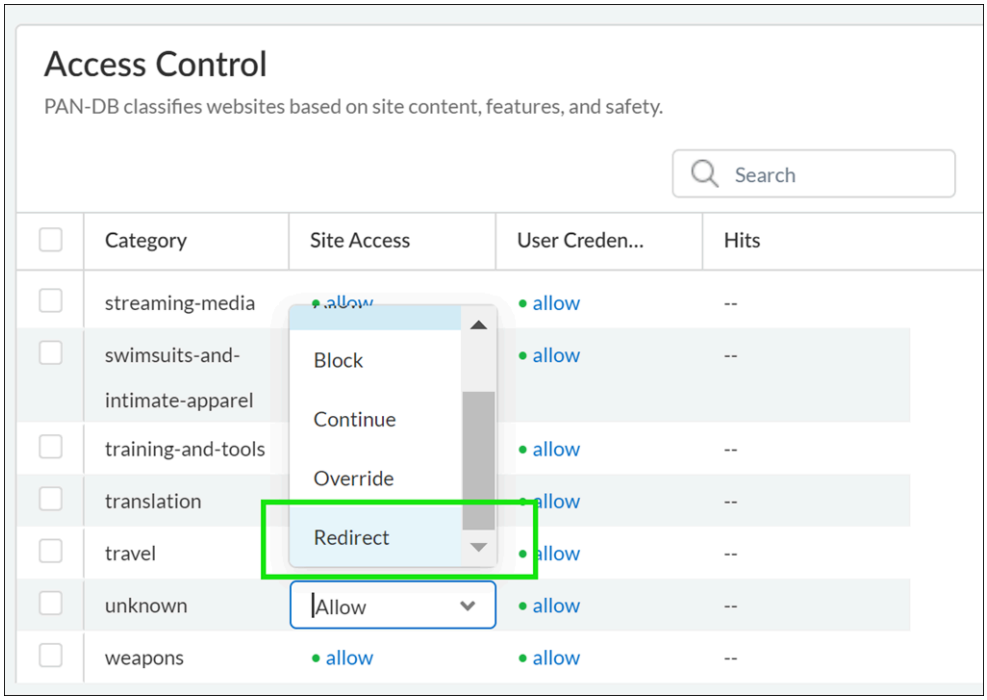


STEP 4 | 接著，請指定將使用者重新導向至 RBI 環境的 URL 類別。

前往 **URL Access Management > Access Control**（**URL** 存取管理 **>** 存取控制）並新增或編輯 **URL Access Management Profile**（**URL** 存取管理設定檔）。

在 **Access Control**（存取控制）設定中，將 **Site Access**（網站存取）更新為 **Redirect**（重新導向）。

新的 **Redirect**（重新導向）操作會將使用者重新導向至 RBI 環境，而非向使用者顯示封鎖頁面。



監控

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

網路上的 Web 活動監控至關重要，攸關於您的組織防護並確保 URL 篩選政策的有效性。Palo Alto Networks 平台會產生詳細日誌，作為儀表板和報告的來源。您可以自訂日誌、儀表板和報告，以符合您的特定監控和報告需求。如有必要，您可以從 URL 篩選日誌要求變更 URL 類別。使用我們的監控工具所提供的洞察來微調 Web 存取政策規則，並對任何可疑活動進行分析並採取相應行動。

HTTP 標頭記錄和僅記錄容器頁面功能提供針對日誌詳細資訊和磁碟區的控制。HTTP 標頭記錄會提升日誌的詳盡程度。僅記錄使用者造訪的主頁可減少產生的日誌數量。

探索以下主題，深入瞭解 Web 活動監控工具和功能。

- 監控 Web 活動
- 僅記錄使用者造訪的頁面
- HTTP 標頭記錄
- 要求變更 URL 類別

監控 Web 活動

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

您可以檢視各種儀表板、報告和日誌，以查看和分析網路上的 Web 活動。例如，在 PAN-OS 新世代防火牆上，應用程式控管中心 (ACC)、URL 篩選日誌與報告會針對設為 **alert**（警示）、**block**（封鎖）、**continue**（繼續）或 **override**（覆寫）的 URL 類別顯示其所有的使用者 Web 活動。藉由以下工具監控使用者活動，您可以更加瞭解使用者群體的 Web 活動並制定適當的 Web 存取政策規則。

平台	檢視使用者 **Web** 活動的方法
PAN-OS 和 Panorama	• 應用程式控管中心 (ACC) • 網路活動 Widget • URL 篩選日誌 • URL 篩選報告
Prisma Access	• 日誌 • 洞察 • 自發 DEM • 活動

- Strata Cloud Manager
- PAN-OS 和 Panorama

監控 Web 活動 (Strata Cloud Manager)

無論您使用哪個介面來管理 Prisma Access（Panorama 或 Strata Cloud Manager），Strata Cloud Manager 中的「活動」窗格皆提供全面的網路活動視圖。「活動」窗格由多個儀表板組成，位於 Strata Cloud Manager 和裝置洞察應用程式中。您也可以與組織中的其他使用者共享活動資料。

以下互動式儀表板可協助您監控和分析網路上的 Web 活動：

- **Threat Insights**（威脅洞察）—全面瞭解進階 URL 篩選和其他 Palo Alto Networks 安全服務在您的網路中偵測並封鎖的所有威脅。您可以檢視威脅趨勢、受影響的應用程式、使用者以及允許或封鎖威脅的安全性政策規則。
- **Log Viewer**（日誌檢視器）—您的日誌提供系統、設定和網路事件的稽核追蹤紀錄。從「活動」儀表板前往日誌以取得詳細資訊與調查結果。
- **Application Usage**（應用程式使用情況）—查看網路上應用程式的概要說明，包括其風險、認可狀態、消耗的頻寬以及這些應用程式的主要使用者。
- **Executive Summary**（執行摘要）（**URL** 篩選）—查看哪些 URL 類別占網路中 Web 活動比例最多、10 大惡意 URL 以及 10 大高風險 URL。
- **User Activity**（使用者活動）—查看個別使用者的瀏覽模式：最常造訪的網站、傳輸資料的網站以及嘗試造訪的高風險網站。來自 URL 篩選日誌和雲端識別引擎的資料可提供這些資訊。
  - 為了輕鬆且安全地存取使用者活動資料並共享報告，建議您啟用並設定雲端識別引擎。

其他資訊和監控方法：

- 「報告」窗格包含排程報告傳遞或隨時下載和共享報告以供離線檢視的選項。
- 您也可以搜尋安全性構件（IP 位址、網域、URL 或檔案雜湊），使用從您的網路和全球威脅情報洞察中擷取的構件資料。

開啟「活動」儀表板。

- 選取 **Activity**（活動） > **Threat Insights | Application Usage | User Activity | Executive Summary**（威脅洞察 | 應用程式使用情況 | 使用者活動 | 執行摘要）。

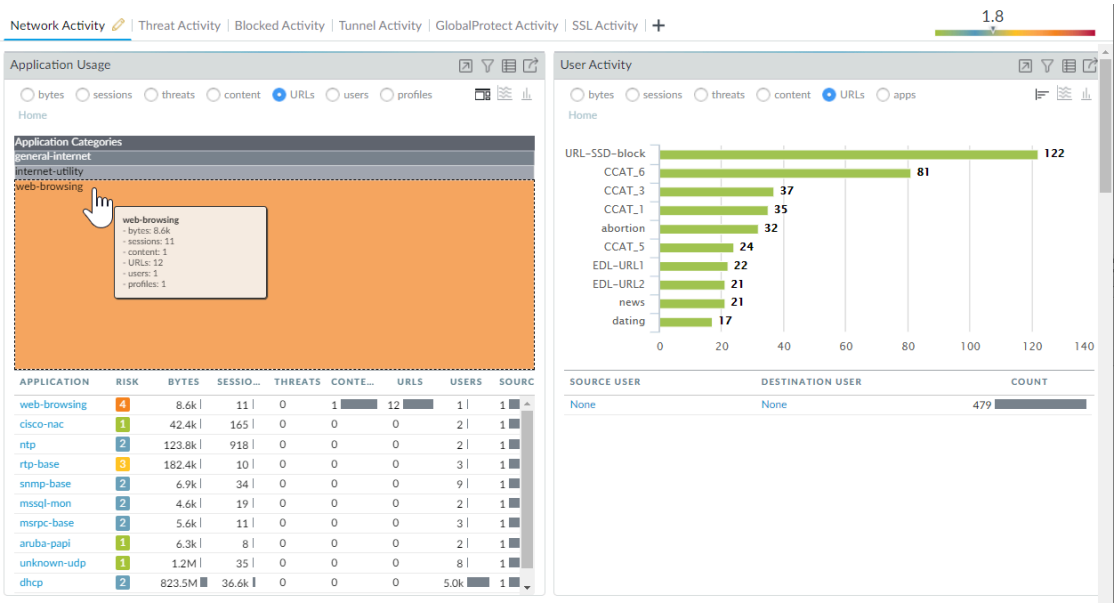
  若要檢視 URL 篩選的執行摘要，您需要在登入儀表板時點選「URL 篩選」頁籤。
- 若要存取日誌檢視器，請選取 **Activity**（活動） > **Logs**（日誌） > **Log Viewer**（日誌檢視器）。

下載、分享和排程「活動」報告。

監控 Web 活動 (PAN-OS & Panorama)

如需快速檢視您環境中使用者最常存取的類別，請核取 **ACC** Widget。大多數 **Network Activity**（網路活動）Widget 均可讓您按照 URL 進行排序。例如，在應用程式使用情況

Widget 中，您可以看到，網路類別是最常存取的類別，隨後是加密通道與 ssl。您也可以檢視按照 URL 排序的 **Threat Activity**（威脅活動）與 **Blocked Activity**（封鎖的活動）的清單。



檢視日誌並設定日誌選項：

您可以直接從 ACC 跳至日誌 () 或選取 **Monitor**（監控） > **Logs**（日誌） > **URL Filtering**（**URL** 篩選）。

每個項目的日誌動作視乎於您為相應類別定義的 Site Access（網站存取）設定：

- 警示日誌—在此範例中，computer-and-internet-info（電腦和網際網路資訊）類別設定為「警示」。

RECEIVE TIME	CATEGORY	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	APPLICATION	ACTION
2020/04/16 14:10:53	computer-and-internet-info	outlook.office36...	pm wifi	UNTRUST				outlook-web-online	alert

- 封鎖日誌—在此範例中，insufficient-content（缺少內容）類別設定為「繼續」。如果該類別已設定為封鎖，則日誌動作將為 block-url（封鎖 URL）。

RECEIVE TIME	CATEGORY	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	APPLICATION	ACTION
2020/04/08 18:47:49	insufficient-content	munchkin.mark...	pm wifi	UNTRUST				ssl	block-continue

- 加密網站上的警示日誌—在此範例中，類別為 private-ip-addresses（私人 IP 位址），應用程式為 web-browsing（Web 瀏覽）。此日誌還指示防火牆已解密該流量。

RECEIVE TIME	CATEGORY	URL	DECRYPTED	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	APPLICATION	ACTION
2020/04/09 14:11:29	private-ip-addresses	/Updates/Updat...	yes	TRUST	UNTRUST	192.168.58.3			web-browsing	alert

[本機] 內嵌 ML 裁定 (PAN-OS 10.0/10.1) 和 [本機和雲端] 內嵌分類裁定（PAN-OS 10.2 及更新版本）會顯示由基於 ML 的內嵌分析器裁定的結果。

- 內嵌 ML 裁定適用於在 PAN-OS 10.0/10.1 上使用本機操作的 URL 篩選內嵌 ML 進行分類的 URL。

	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	INLINE ML VERDICT	ACTION	URL
	10/11 17:32:10	malware	malware	phishing	block	hisperfectlight.com/downloads/etipa/login.php?cmd=login_submit&id=2cf35df3...
	10/11 14:15:14	malware	malware	phishing	block	hisperfectlight.com/downloads/etipa/login.php?cmd=login_submit&id=2cf35df3...
	04/30 15:19:30	medium-risk	medium-risk,unknown	malicious-javascript	block	130.127.24.16/0x39814f84/448d21c8e396e8f4e0eb75de69d6473e033422b...

可能出現以下裁定結果：

- **Phishing**（網路釣魚）—本機內嵌 ML 偵測到的網路釣魚攻擊內容。
- **Malicious-javascript**（惡意 **javascript**）本機內嵌 ML 偵測到的惡意 javascript 內容。
- **Unknown**（未知）—對 URL 進行分類並確定內容無害。

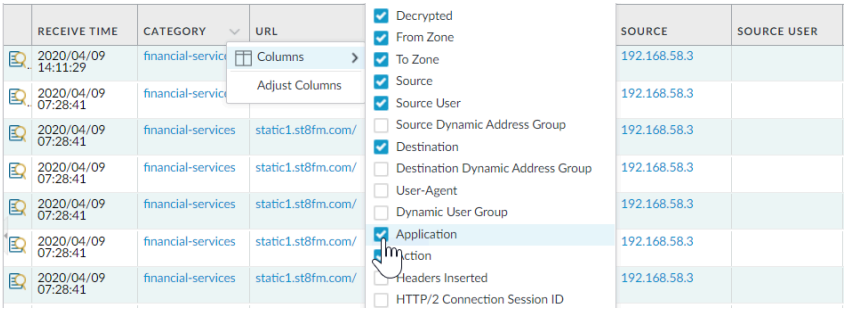
- 內嵌分類裁定適用於使用本機操作的 URL 篩選內嵌 ML（在 PAN-OS 10.2 中已重命名為本地內聯分類）以及在進階 URL 篩選雲端中執行的雲端內嵌分類進行分類的 URL。日誌的類別欄位中會具體說明攻擊類型。

	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	INLINE CATEGORIZATI... VERDICT	ACTION	URL
	08/16 15:16:58	computer-and-internet-info	computer-and-internet-info,high-risk	N/A	alert	mlav.testpanw.com/js.html
	08/16 15:16:58	phishing	computer-and-internet-info,high-risk	local	block	mlav.testpanw.com/phishing.html
	08/16 15:14:58	phishing	phishing,real-time-detection	cloud	block-url	urlfiltering.paloaltonetworks.com/test-inline-content-analysis-phishing
	08/16 15:14:58	phishing	phishing,real-time-detection	cloud	block-url	urlfiltering.paloaltonetworks.com:80/test-inline-content-analysis-phishing

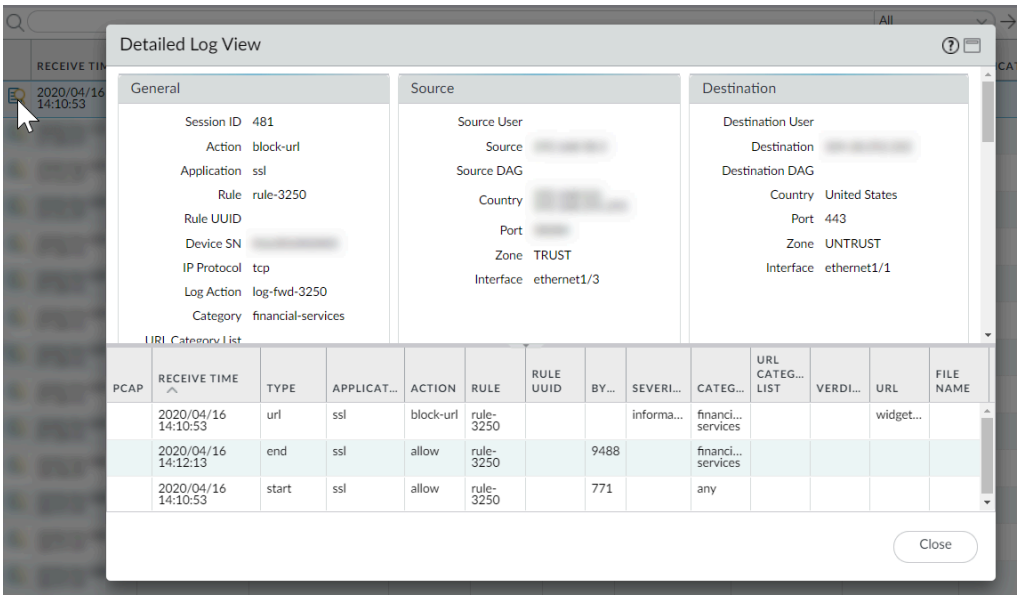
可能出現以下裁定結果：

- **Local**（本機）—使用本機內嵌分類偵測到的惡意內容。
- **Cloud**（雲端）—使用位於進階 URL 篩選雲端中的雲端內嵌分類引擎偵測到的惡意內容。
- **N/A**（不適用）—本機或雲端內嵌分類引擎未分析該 URL。

您也可以將其他數欄新增至您的 URL 篩選日誌檢視，例如目的地區與來源區域、內容類型，以及是否執行封包擷取。若要修改要顯示哪些欄，請按一下任何欄中的向下箭頭，並選取要顯示的屬性。

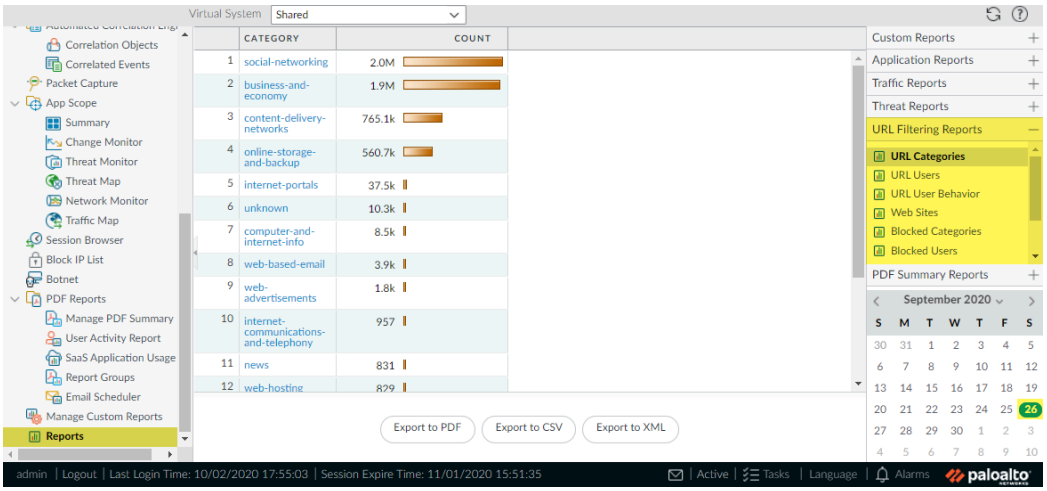


若要檢視完整的日誌詳細資訊和/或要求變更已存取所指定 URL 的類別，請按一下日誌第一欄的日誌詳細資訊圖示。



按 URL 類別、URL 使用者、存取的網站、封鎖的類別等產生預先定義的 URL 篩選報告。

選取 **Monitor**（監控） > **Reports**（報告），然後在 **URL Filtering Reports**（**URL** 篩選報告）區段中，選取一個報告。報告中涵蓋了您在行事歷上所選日期的 24 小時期間。您也可以將報告匯出為 PDF、CSV 或 XML 報告。



檢視使用者活動報告

這可在何處使用？	我需要什麼？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ 進階 URL 篩選授權（或舊版 URL 篩選授權） 附註：

這可在何處使用？	我需要什麼？
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	• 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

此報告可讓您快速檢視使用者或群組活動，也提供檢視瀏覽時間活動的選項。

- Strata Cloud Manager
- PAN-OS 和 Panorama

檢視使用者活動報告 (Strata Cloud Manager)

無論您使用 Panorama 或 Strata Cloud Manager 管理 Prisma Access，您都可以前往 Strata Cloud Manager 應用程式以產生使用者活動報告。在應用程式中，前往 **Activity**（活動）查找 **User Activity Report**（使用者活動報告）儀表板。必須具有效的雲端識別引擎租用戶才能存取使用者活動資料。

STEP 1 | 啟動雲端識別引擎。

STEP 2 | 設定雲端識別引擎。

STEP 3 | 設定使用者活動報告。

1. 選取 **Activity**（活動） > **User Activity**（使用者活動）。
2. **Enter Username**（輸入使用者名稱）以產生個人報告。
3. 選取報告 **Type**（類型）：
   - 若要為某個人產生報告，選取 **User**（使用者）。
   - 若要為使用者群組產生報告，則選取 **Group**（群組）。

   您必須啟用 User-ID，才能選取使用者或群組名稱。如果未設定 *User-ID*，您可以選取 ***User***（使用者）類型，然後輸入使用者電腦的 *IP* 位址。
4. 輸入使用者報告的 **Username/IP Address**（使用者名稱/**IP** 位址），或輸入使用者群組報告的群組名稱。
5. 選取時段。您可以選取現有的時段，或選取 **Custom**（自訂）。
6. 選取 **Include Detailed Browsing**（包含詳細瀏覽）核取方塊，讓報告中包含瀏覽資訊。

STEP 4 | 執行報告。

1. 按一下 **Run Now**（立即執行）。
2. 當防火牆完成產生報告後，按一下以下其中一個連結以下載報告：
   - 按一下 **Download User Activity Report**（下載使用者活動報告），可下載 PDF 版的報告。
   - 按一下 **Download URL Logs**（下在 **URL** 日誌），可下載相應日誌項目的 CSV 檔案。
3. 下載報告後，按一下 **Cancel**（取消）。
4. 若要儲存使用者活動報告設定，便於以後執行相同報告，可按一下 **OK**（確定），否則按一下 **Cancel**（取消）。

STEP 5 | 開啟所下載的檔案，以檢視使用者活動報告。PDF 版本的報告將顯示報告所基於的使用者或群組、報告時間範圍以及目錄：

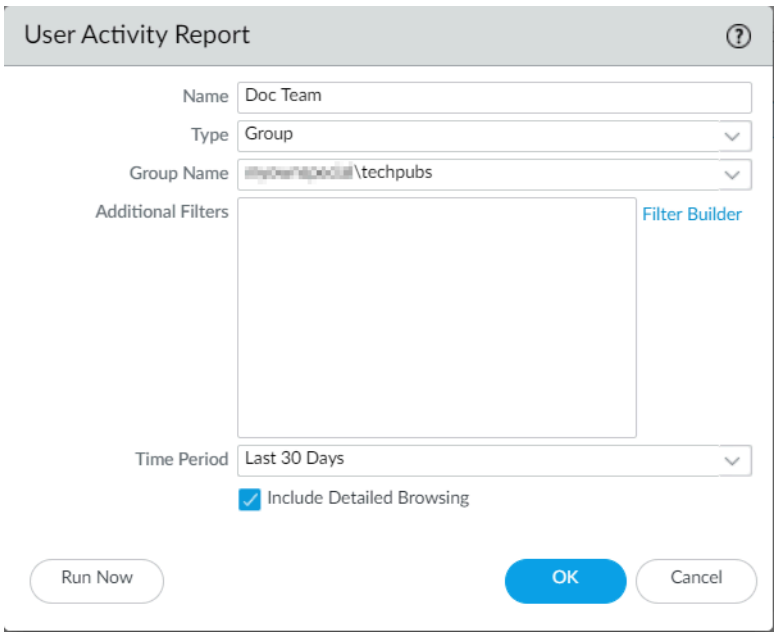
STEP 6 | 按一下目錄中的項目可檢視報告的詳細資訊。例如，按一下 **Traffic Summary by URL Category**（**URL** 類別的流量摘要）以檢視所選使用者或群組的統計資料。

檢視使用者活動報告 (PAN-OS & Panorama)

STEP 1 | 設定使用者活動報告。

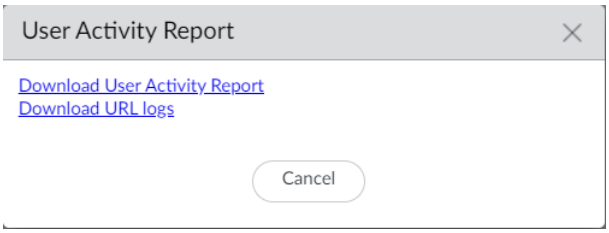
1. 選取 **Monitor**（監控） > **PDF Reports**（**PDF** 報告） > **User Activity Report**（使用者活動報告）。
2. **Add**（新增）報告，然後輸入其 **Name**（名稱）。
3. 選取報告 **Type**（類型）：
   - 若要為某個人產生報告，選取 **User**（使用者）。
   - 若要為使用者群組產生報告，則選取 **Group**（群組）。

   您必須啟用 User-ID，才能選取使用者或群組名稱。如果未設定 *User-ID*，您可以選取 ***User***（使用者）類型，然後輸入使用者電腦的 *IP* 位址。
4. 輸入使用者報告的 **Username/IP Address**（使用者名稱/**IP** 位址），或輸入使用者群組報告的群組名稱。
5. 選取時段。您可以選取現有的時段，或選取 **Custom**（自訂）。
6. 選取 **Include Detailed Browsing**（包含詳細瀏覽）核取方塊，讓報告中包含瀏覽資訊。



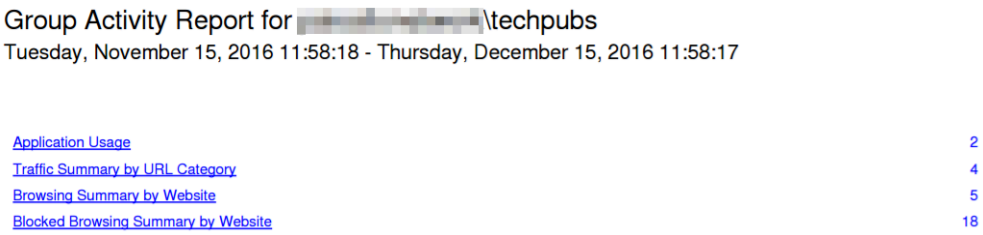
STEP 2 | 執行報告。

1. 按一下 **Run Now**（立即執行）。
2. 當防火牆完成產生報告後，按一下以下其中一個連結以下載報告：
   - 按一下 **Download User Activity Report**（下載使用者活動報告），可下載 PDF 版的報告。
   - 按一下 **Download URL Logs**（下在 **URL** 日誌），可下載相應日誌項目的 CSV 檔案。

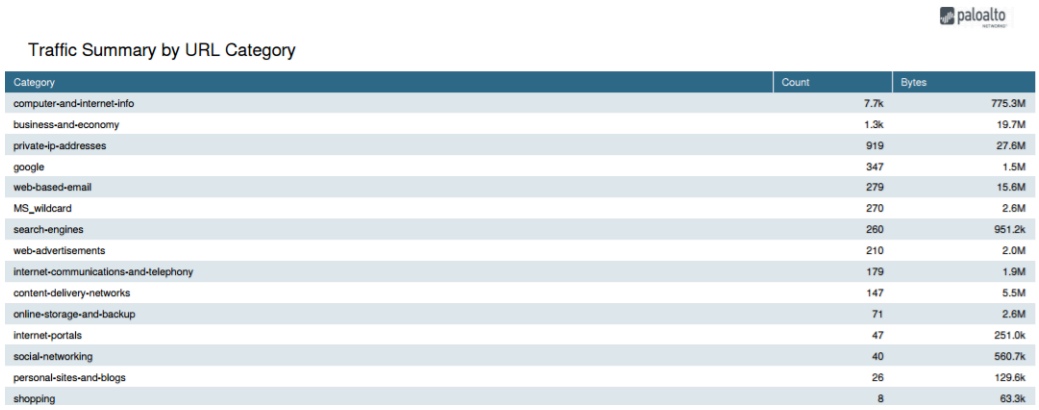


3. 下載報告後，按一下 **Cancel**（取消）。
4. 若要儲存使用者活動報告設定，以便日後執行相同報告，可按一下 **OK**（確定），否則請按 **Cancel**（取消）。

STEP 3 | 開啟所下載的檔案，以檢視使用者活動報告。PDF 版本的報告將顯示報告所基於的使用者或群組、報告時間範圍以及目錄：



STEP 4 | 按一下目錄中的項目可檢視報告的詳細資訊。例如，按一下 **Traffic Summary by URL Category**（**URL** 類別的流量摘要）以檢視所選使用者或群組的統計資料。



Traffic Summary by URL Category

Category	Count	Bytes
computer-and-internet-info	7.7k	775.3M
business-and-economy	1.3k	19.7M
private-ip-addresses	919	27.6M
google	347	1.5M
web-based-email	279	15.6M
MS_wildcard	270	2.6M
search-engines	260	951.2k
web-advertisements	210	2.0M
internet-communications-and-telephony	179	1.9M
content-delivery-networks	147	5.5M
online-storage-and-backup	71	2.6M
internet-portals	47	251.0k
social-networking	40	560.7k
personal-sites-and-blogs	26	129.6k
shopping	8	63.3k

排程和分享 URL 篩選報告

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

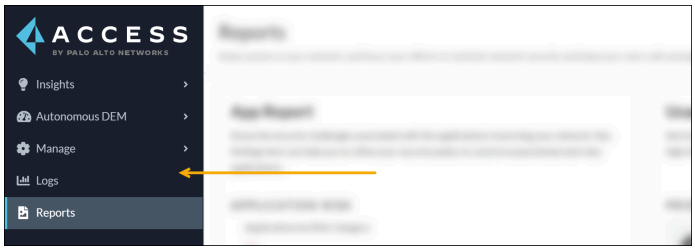
您可以排程、產生和分享與 URL 篩選和 Web 活動相關的各種報告。

- Strata Cloud Manager
- PAN-OS 和 Panorama

排程與分享 URL 篩選報告 (Strata Cloud Manager)

無論您使用 Panorama 或 Strata Cloud Manager 管理 Prisma Access，您都可以將 Strata Cloud Manager 用於 URL 篩選報告。在 Strata Cloud Manager 中，前往「活動」以取得互動式 URL 篩選資料和報告。您可以在組織內分享「活動」報告，並排定定期更新。以下是使用且與 URL 篩選最相關的 Prisma Access 儀表板和工具：

- **Executive Summary**（執行摘要）—查看哪些 URL 類別占網路中 Web 活動比例最多、10 大惡意 URL 以及 10 大高風險 URL。
- **User Activity**（使用者活動）—查看個別使用者的瀏覽模式：最常造訪的網站、傳輸資料的網站以及嘗試造訪的高風險網站。來自 URL 篩選日誌和雲端識別引擎的資料可提供這些資訊。
- 搜尋安全性構件（IP 位址、網域、URL 或檔案雜湊），使用從您的網路和全球威脅情報洞察中擷取的構件資料。



為了輕鬆且安全地存取使用者活動資料並共享報告，建議您啟用並設定雲端識別引擎。

STEP 1 | 下載、分享和排程「活動」報告。

STEP 2 | 存取 URL 篩選執行摘要。

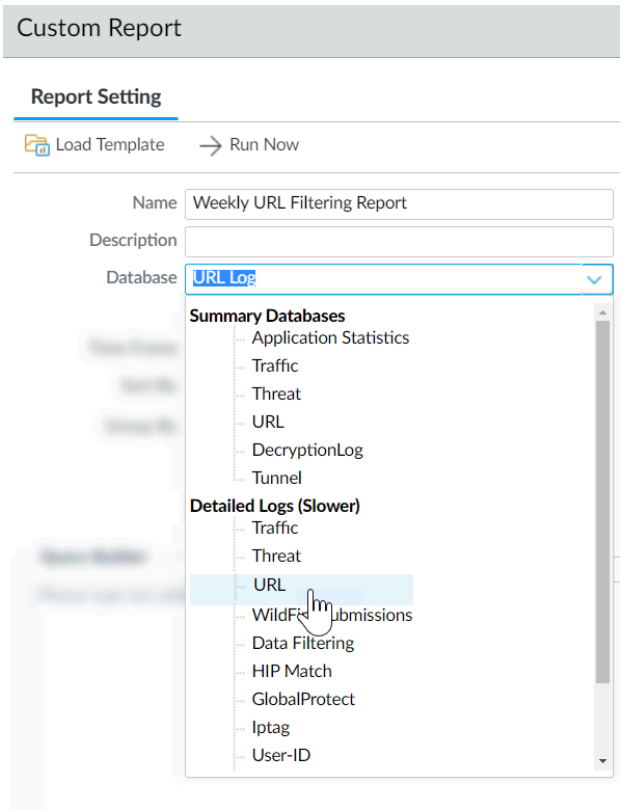
選取 **Activity**（活動） > **Executive Summary**（執行摘要）並點選 [URL Filtering（URL 篩選）] 頁籤。

STEP 3 | 搜尋安全性構件。

排程與分享 URL 篩選報告 (PAN-OS & Panorama)

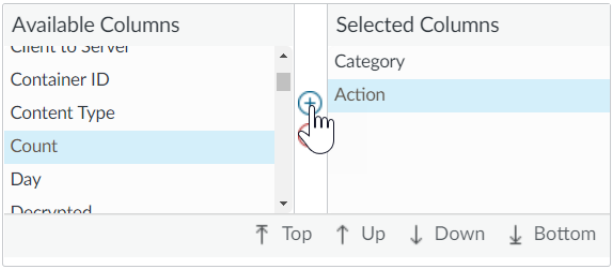
STEP 1 | 新增新的自訂報告。

1. 選取 **Monitor**（監控） > **Manage Custom Reports**（管理自訂報告），然後 **Add**（新增） 報告。
2. 為報告提供唯一 **Name**（名稱），選擇性地輸入 **Description**（描述）。
3. 選取您要用於產生報告的 **Database**（資料庫）。若要產生詳細的 URL 篩選報告，需從 Detailed Logs（詳細日誌）區段選取 **URL**：

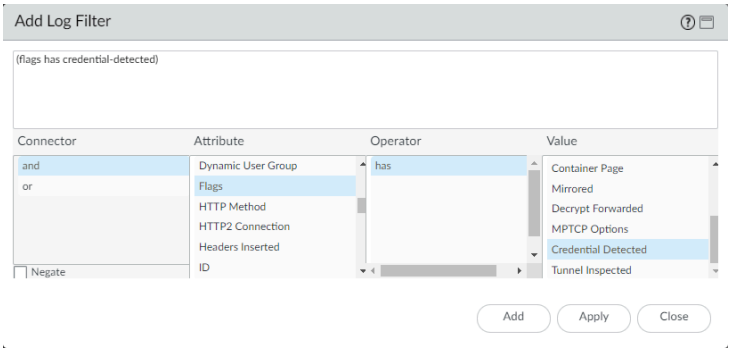


STEP 2 | 設定報告選項。

1. 選取預定義的 **Time Frame**（時間範圍），或者選取 **Custom**（自訂）。
2. 從 Available Columns（可用欄）清單中選取報告中要包含的日誌欄，然後將其新增 ( ) 至 Selected Columns（選定欄）。例如，您可以為 URL 篩選報告選取：
   - 動作
   - 應用程式類別
   - 類別
   - 目的地國家
   - 來源使用者
   - URL

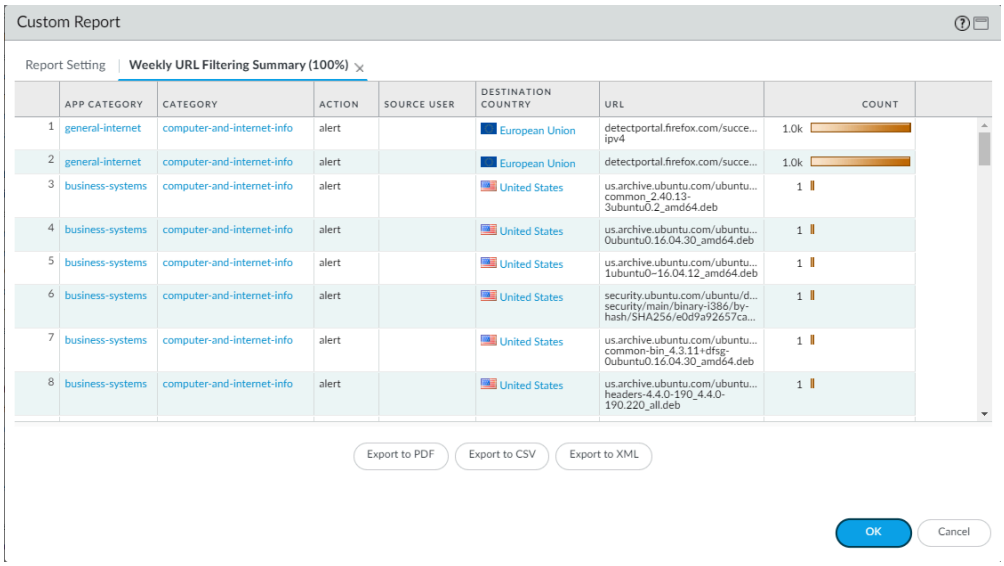


3. 如果啟用了防火牆以防禦認證網路釣魚，則選取屬性 **Flags**（標幟）、運算子 **has** 和值 **Credential Detected**（認證已偵測），以在報告中包含使用者向網站提交有效公司認證時記錄的事件。



4. （選用）選取 **Sort By**（排序方式）選項，以設定用於彙總報告詳細資料的屬性。如果您未選取作為排序方式的屬性，報告會傳回前 N 個結果，不進行任何的彙總。選取 **Group By**（分組方式）屬性，以用作分組資料的錨點。以下範例顯示了一項將 **Group By**（分組

方式）設定為 **App Category**（應用程式類別）、**Sort By**（排序方式）設定為 **Count**（排名前 **5**）**Top 5**（排名前 **5**）的報告。



STEP 3 | 執行報告。

1. 按一下 **Run Now**（立即執行）圖示，立即產生報告（將在新頁籤上開啟）。
2. 檢閱完報告後，返回 **Report Setting**（報告設定）頁籤，調整設定並再次執行報告，或者繼續進行排程報告的下一步驟。
3. 選中 **Schedule**（排程）核取方塊，每天執行一次報告。這會每天產生報告，詳細記錄過去 24 小時的 Web 活動。

STEP 4 | **Commit**（提交）組態。

STEP 5 | 檢視自訂報告。

1. 選取 **Monitor**（監控） > **Reports**（報告）。
2. 展開右欄中的 **Custom Reports**（自訂報告）窗格，選取您要檢視的報告。會自動顯示最新的報告。
3. 若要檢視之前日期的報告，可從行事曆中選取相應日期。您也可以將報告匯出為 PDF、CSV 或 XML 報告。

僅記錄使用者造訪的頁面

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

容器頁面是一種主要頁面，當使用者造訪網站時會存取此頁面，但其他頁面也可與主要頁面一起載入。如果 URL 篩選設定檔（Prisma Access 的 URL 存取管理設定檔）的 **Log Container page only**（僅限日誌容器頁面）選項已啟用，則只會記錄主要容器頁面，不會記錄後續在容器頁面內載入的頁面。因為 URL 篩選可能會產生許多的日誌項目，所以您可能會想要開啟此選項，讓日誌項目只包含那些要求頁面檔案名稱符合特定 mime 類型的 URI。預設設定包含下列 mime 類型：

- application/pdf
- application/soap+xml
- application/xhtml+xml
- text/html
- text/plain
- text/xml

如果您啟用 ***Log container page only***（僅限日誌容器頁面）選項，則不一定會有由防毒或漏洞保護所偵測到威脅的關聯 *URL* 日誌項目。

- Strata Cloud Manager
- PAN-OS 和 Panorama

僅記錄使用者造訪的頁面 (Strata Cloud Manager)

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

請切換到 ***PAN-OS & Panorama*** 頁籤並按照指示進行操作。

如果您使用 ***Strata Cloud Manager***，則請繼續此處操作。

STEP 1 | 在 URL 存取管理設定檔中，選取 **Log Container Page Only**（僅限日誌容器頁面）。

STEP 2 | 將 URL 存取管理設定檔套用至安全性政策規則。

僅當 URL 存取管理設定檔包含在安全性政策規則所參考的設定檔群組中，該設定檔才會處於啟用狀態。

依照步驟啟用 URL 存取管理設定檔（和任何安全性設定檔)。請務必記得 **Push Config**（推送設定）。

僅記錄使用者造訪的頁面 (PAN-OS & Panorama)

STEP 1 | 建立或選取要修改的 URL 篩選設定檔。

選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **URL Filtering**（URL 篩選）。

STEP 2 | 啟用 **Log container page only**（僅限日誌容器頁面）。

STEP 3 | 按一下 **OK**（確定）來儲存設定檔。

STEP 4 | **Commit**（提交）您的變更。

HTTP 標頭記錄

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

URL 篩選可讓您檢視及控制網路上的網頁流量。若要改善對 Web 內容的可見度，您可以設定 URL 篩選設定檔來記錄包含在 Web 要求中的 HTTP 標頭屬性。用戶端要求網頁時，HTTP 標頭中會包含 user agent、referer 與 x-forwarded-for 欄位作為屬性值配對，並將這些欄位轉送到網頁伺服器。啟用記錄 HTTP 標頭時，防火牆會將下列屬性值配對記錄在 URL 篩選記錄中。

您還可以使用 *HTTP* 標頭來管理對 *SaaS* 應用程式的存取。您不需要 *URL* 篩選授權即可執行此操作，但是必須使用 *URL* 篩選設定檔才能啟用此功能。

屬性	說明
使用者代理程式	使用者用來存取 URL 的網頁瀏覽器，例如 Internet Explorer。此資訊是在 HTTP 要求中傳送給伺服器。 HTTP 標頭不包含使用者代理程式的完整字串。包含標頭端的封包之前的封包記錄的最大位元組數為 36 個位元組。
參照位址	網頁的 URL，可將使用者連結至其他網頁；它是將使用者重新導向 (轉介) 至正在要求之網頁的來源。
X-Forwarded-For (XFF)	HTTP 要求標頭欄位中的選項，用來保留要求網頁之使用者的 IP 位址。如果您在網路上具有 Proxy 伺服器，XFF 可讓您識別要求內容之使用者的 IP 位址，而不是僅將 Proxy 伺服器的 IP 位址記錄為要求網頁的來源 IP 位址。
插入的標頭	防火牆會插入的標頭類型和標頭文本。

要求變更 URL 類別

這可在何處使用？	我需要什麼？
• 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 URL 篩選授權（或舊版 URL 篩選授權） 附註： • 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。 • Prisma Access 授權包括 *Advanced URL Filtering* 功能。

如果您認為某個網域或 URL 分類錯誤，您可以透過防火牆或 Test A Site（我們的 URL 類別查閱工具）提交重新分類的要求。您也可以透過 Test A Site 提交大量重新分類的要求。這兩種方法都會要求您為要審核的 URL 提議至少一個新類別。

您無法要求變更 *URL* 會收到的風險類別，也不能要求變更分類為不足的內容或新註冊網域的 *URL*。

在防火牆上，您可以從 URL 篩選日誌條目的詳細日誌檢視中要求變更 URL 類別。在 Test A Site 上，您必須輸入您要重新分類的網站才能查看其 PAN-DB 分類。要求表單連結位於搜尋結果後方。同樣，Strata Cloud Manager 會顯示 Test A Site 表單的連結，其中包含編輯 URL 存取管理設定檔時可用的內部 Test A Site 工具查詢結果。若要存取大量變更要求表單，您需要先登入 Test A Site。登入後，網頁會顯示大量要求表單的連結。

一旦有使用者提交變更要求之後，自動爬蟲會立即分析 URL。一旦爬蟲程式確認您的類別建議，Palo Alto Networks 會核准您的要求並立即使用新類別更新 PAN-DB。若未確認，Palo Alto Networks 威脅研究和資料科學團隊的編輯會手動審核您的要求。他們可能決定保留原本的類別、同意您建議的類別或變更類別（如果他們不同意原本的類別和建議類別）。

提交變更要求之後，您將收到一封確認電子郵件。調查完成後，您將收到第二封說明調查結果的電子郵件。

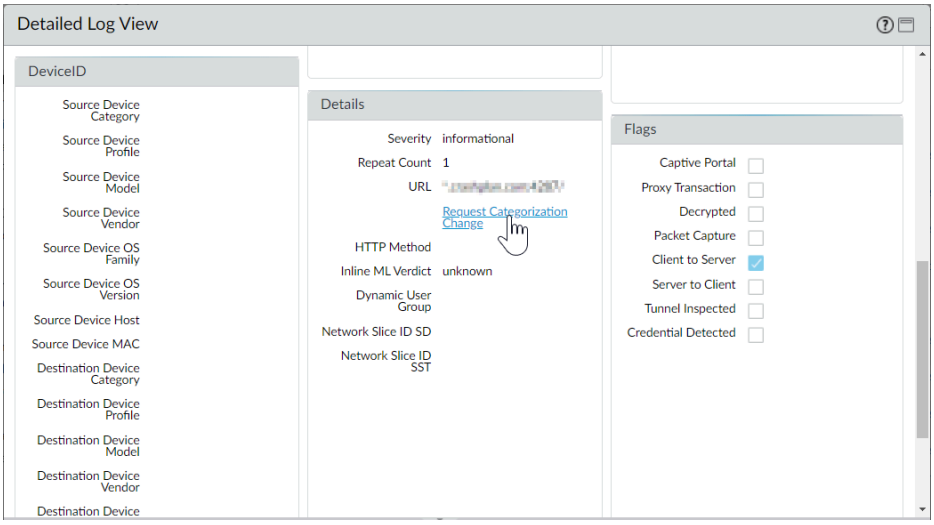
- PAN-OS 和 Panorama
- Test A Site

要求變更 URL 類別 (PAN-OS & Panorama)

STEP 1 | 存取 URL 篩選日誌（**Monitor**（監控） > 日誌 > **URL** 篩選）。

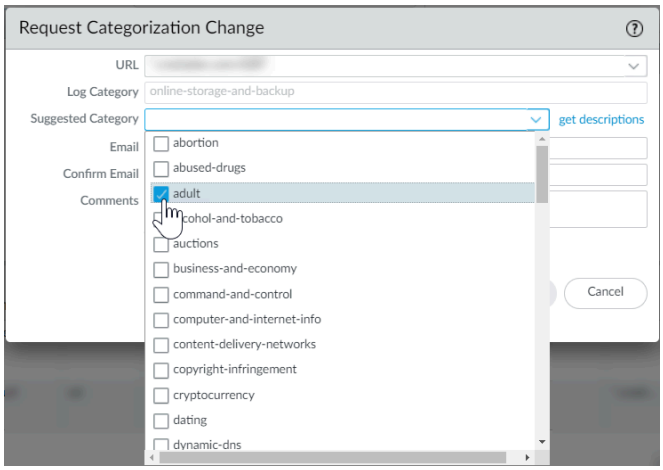
STEP 2 | 開啟詳細日誌檢視，以取得您要變更的 URL 分類的 URL 篩選日誌條目。

1. 點選相應日誌條目的望遠鏡 ( )。畫面將顯示詳細日誌檢視。



STEP 3 | 在詳細資訊下，點選 **Request Categorization Change**（要求類別變更）。

STEP 4 | 填寫申請表並提交。



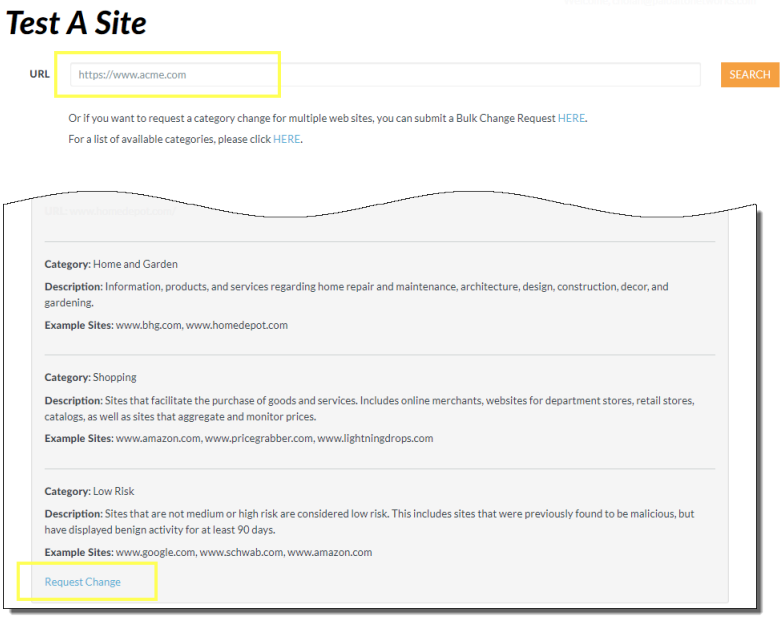
要求變更 URL 類別 (Test A Site)

STEP 1 | 前往 Test A Site。

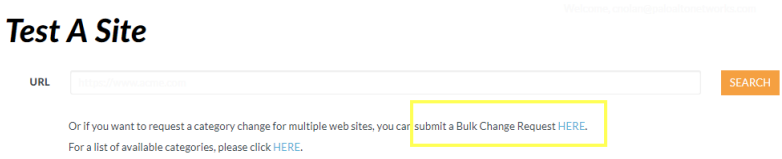
Log in（登入）以避免完成 *CAPTCHA* 測試和在變更要求表單上輸入您的電子郵件。請留意，您必須登入才能存取大量變更要求表單。

STEP 2 | 選取要完成的變更要求表單。

- **Change Request for a Single URL**（單一 **URL** 的變更要求）—輸入您想重新分類的 **URL**，然後點選 **Search**（搜尋）。在 URL 類別結果下，點選 **Request Change**（要求變更）。



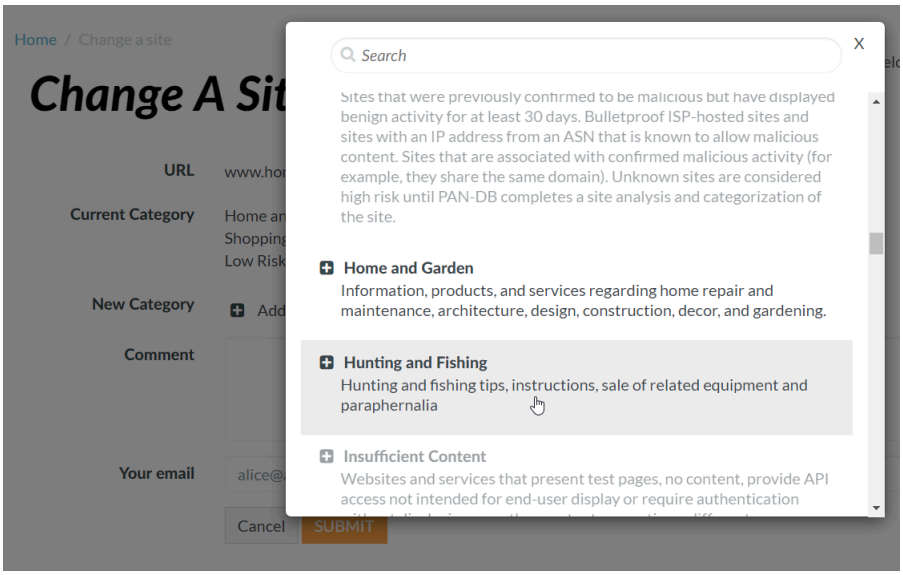
- **Bulk Change Request**（大量變更要求）—**Log-in**（登入）Test A Site。然後 **HERE**（在此）點選 [submit a Bulk Change Request（提交大量變更要求）]。



STEP 3 | 填寫變更要求表單。

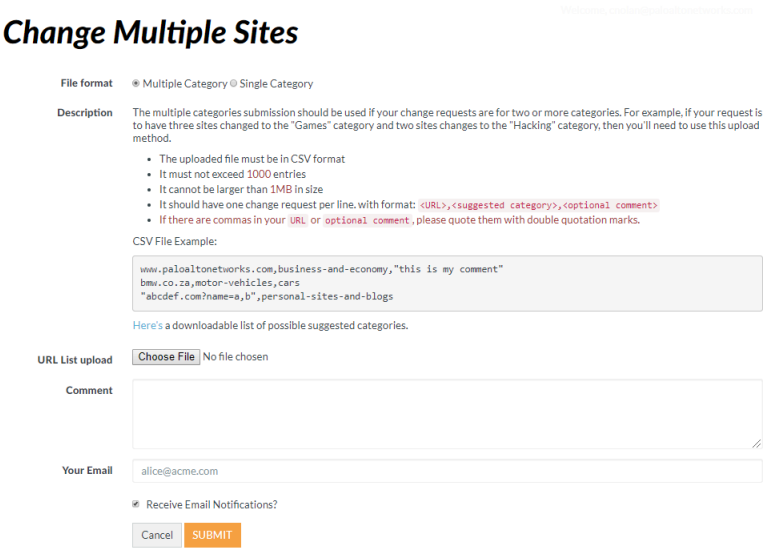
- **Change Request for a Single URL**（單一 **URL** 的變更要求）—建議最多兩個 URL 新類別。點選 **Select category (from a list)**（選取類別（從清單）），然後一次選取一個類別。或者

您也可以針對您的要求留下 **Comment**（評論）。例如，您可以解釋為什麼您的建議較合適。



- **Bulk Change Request**（大量變更要求）—選擇一個 **File Format**（檔案格式）。如果您的變更要求包含兩個或多個類別，請選擇 [Multiple Category（多個類別）]。例如，如果要將清單中的一半 URL 重新分類為商業與經濟，另一半分類為個人網站和部落格。

  然後，按一下 **Choose File**（選擇檔案）並選取要上傳的 CSV 檔。檔案每行應有一個變更要求，格式如下：`<URL>,<first suggested category>,<second suggested category>,<(optional) comment>`。檔案不能超過 1000 個條目或大於 1MB。或者您也可以針對您的要求留下 **Comment**（評論）。



STEP 4 | **Submit**（提交）表單。

疑難排解

這可在何處使用？	我需要什麼？
• NGFW (Managed by PAN-OS or Panorama)	☐ 進階 URL 篩選授權（或舊版 URL 篩選授權） 註： 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。

本章分享如何診斷和解決 Palo Alto Networks 新世代防火牆的常見 URL 篩選問題。針對這些問題聯絡 Palo Alto Networks 支援團隊之前，請先完成相關步驟。如果您仍需聯絡支援團隊，請務必提供您從執行疑難排解工作中獲得的所有資訊。

疑難排解和監控 *Web* 活動通常是並進的。請經常善用監控和日誌記錄工具來找出並解決本章未明確討論的問題。請深入瞭解監控章節中提到的監控工具和工作。

- 啟動進階 URL 篩選時發生問題
- PAN-DB 雲端連線問題
- 分類為未解析的 URL
- 錯誤分類
- 疑難排解網站存取問題
- 疑難排解 URL 篩選回應頁面顯示問題

啟動進階 URL 篩選時發生問題

這可在何處使用？	我需要什麼？
• NGFW (Managed by PAN-OS or Panorama)	❑ 進階 URL 篩選授權（或舊版 URL 篩選授權） 註： 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。

使用下列工作流程疑難排解進階 URL 篩選啟動問題。

STEP 1 | 存取 PAN-OS CLI。

STEP 2 | 執行下列命令，驗證是否已啟動進階 URL 篩選：

```
show system setting url-database
```

如果回應是 `paloaltonetworks`，則 Palo Alto Networks URL 篩選資料庫 PAN-DB 是作用中的廠商。

STEP 3 | 驗證防火牆具備有效的進階 URL 篩選授權。

執行要求授權資訊 CLI 命令。

您應該會看見授權項目`Feature：Advanced URL Filtering`如果授權未安裝，您必須取得及安裝授權。請參閱 設定 URL 篩選。

STEP 4 | 檢查PAN-DB 雲端連線狀態。

PAN-DB 雲端連線問題

這可在何處使用？	我需要什麼？
• NGFW (Managed by PAN-OS or Panorama)	❑ 進階 URL 篩選授權（或舊版 URL 篩選授權） 註：舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。

為協助確保 *PAN-DB* 雲端的連線能力，請建立專用的安全性政策規則，以允許所有 *Palo Alto* 管理服務流量。這將避免管理流量被歸類為 *not-resolved*，並防止流量在透過資料平面路由時遭到封鎖。

若要檢查防火牆與 PAN-DB 雲端之間的連線：

```
show url-cloud status
```

如果雲端可存取，則預期的回應如下所示：

```
show url-cloud status PAN-DB URL Filtering License : valid Current
 cloud server : serverlist.urlcloud.paloaltonetworks.com Cloud
 connection : connected Cloud mode : public URL database version -
 device :20200624.20296 URL database version - cloud :20200624.20296
 ( last update time 2020/06/24 12:39:19 ) URL database status : good
 URL protocol version - device : pan/2.0.0 URL protocol version -
 cloud : pan/2.0.0 Protocol compatibility status : compatible
```

如果雲端不可存取，則預期的回應如下所示：

```
show url-cloud status PAN-DB URL Filtering License : valid
 Cloud connection : not connected URL database version -
 device :0000.00.00.000 URL protocol version - device : pan/0.0.2
```

使用下列檢查清單識別並解決連線問題：

- ❑ PAN-DB URL 篩選授權欄位是否顯示無效？取得並安裝有效的 PAN-DB 授權。
- ❑ URL 通訊協定版本是否不相容？將 PAN-OS 升級至最新版本。

- 是否可以從防火牆偵測 PAN-DB 雲端伺服器？執行下列命令以進行檢查：

```
ping source <ip-address> host
 serverlist.urlcloud.paloaltonetworks.com <
```

例如，如果您的管理介面 IP 位址是 10.1.1.5，請執行下列命令：

```
ping source 10.1.1.5 host serverlist.urlcloud.paloaltonetworks.com
```

- 防火牆是否在 HA 組態中？驗證防火牆的 HA 狀態是否為主動、主動-主要、或主動-次要。如果防火牆處於其他狀態，則將被阻止存取 PAN-DB 雲端。在配對中的每個防火牆上執行下列命令，以查看狀態：

```
show high-availability state
```

如果防火牆和 PAN-DB 雲端之間的連線仍有問題，則請聯絡 Palo Alto Networks 支援部門。

分類為未解析的 URL

這可在何處使用？	我需要什麼？
• NGFW (Managed by PAN-OS or Panorama)	❑ 進階 URL 篩選授權（或舊版 URL 篩選授權） 註： 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。

如果您的防火牆無法連線到 PAN-DB URL 篩選雲端服務來執行查閱，或 PAN-DB 回應 URL 查詢的時間過長，則 URL 會被分類為未解析。雲端連線狀態和 URL 分類不適用於過期的訂閱授權或未授權使用者。有關 URL 分類過程的詳細說明，請參閱 URL 篩選的運作原理。

使用下列工作流程，解決 PAN-DB 所識別之部分或全部 URL 被分類為「未解決」的問題：

STEP 1 | 執行 **`show url-cloud status`** CLI 命令來檢查 PAN-DB 雲端連線。

雲端連線：欄位應顯示已連線。如果您看到的不是已連線，則任何在管理背板快取中沒有的 URL 將會分類為未解析。要解決此問題，請參閱 PAN-DB 雲端連線問題。

STEP 2 | 如果雲端連線狀態顯示已連線，請檢查防火牆的目前使用情況。

如果防火牆使用率突然增加，則 URL 要求可能遭到丟棄（未到達管理背板），並將歸類為未解析。

若要查看系統資源，請執行 **`show system resources`** CLI 命令。然後查看 %CPU 和 %MEM 欄。

您也可以在 Web 介面 **Dashboard**（儀表板） 中的 System Resources（系統資源）Widget 上檢視系統資源。

STEP 3 | 考慮增加 **Category lookup timeout (sec)**（類別查閱逾時（秒））值。

增加類別查閱逾時值可提高解析 URL 類別的機率，並降低日誌中出現未解析 URL 的頻率。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Content-ID**，然後編輯 URL 篩選設定。
2. 按一下 **OK**（確定）並 **Commit**（交付）變更。

   您也可以使用 **`set deviceconfig setting ctd url-wait-timeout`** CLI 命令來更新該值。

STEP 4 | 如果問題仍然存在，請聯絡 Palo Alto Networks 支援部門。

錯誤分類

這可在何處使用？	我需要什麼？
• NGFW (Managed by PAN-OS or Panorama)	❑ 進階 URL 篩選授權（或舊版 URL 篩選授權） 註： 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。

有時，您可能會遇到您認為分類錯誤的 URL。使用下列工作流程，以確定網站的 URL 分類並在必要時要求類別變更。

STEP 1 | 執行下列命令確認資料面板中的類別：

```
show running url <URL>
```

例如，若要檢視 Palo Alto Networks 網站的類別，請執行下列命令：

```
show running url paloaltonetworks.com
```

如果存放在資料背面快取中的 URL 有正確的類別 (在此範例中為 computer-and-internet-info)，則分類正確，不需要採取進一步的動作。如果類別不正確，請繼續下一個步驟。

STEP 2 | 請執行下列命令確認該類別在管理背板中：

```
test url-info-host <URL>
```

例如：

```
test url-info-host paloaltonetworks.com
```

如果存放在管理背板中的 URL 有正確的類別，請執行下列命令將 URL 自資料平面快取中移除：

```
clear url-cache url <URL>
```

下次防火牆要求此 URL 的類別時，系統會將要求轉送至管理背板。這會解決此問題，不需要採取進一步的動作。如果這無法解決問題，請執行下一個步驟檢查雲端系統上的 URL 類別。

STEP 3 | 執行下列命令確認雲端中的類別：

```
test url-info-cloud <URL>
```


STEP 4 | 如果存放在雲端的 URL 有正確的類別，請將 URL 自資料平面與管理背板快取中移除。

執行下列命令將 URL 自資料平面快取中刪除：

```
clear url-cache url <URL>
```

執行下列命令將 URL 自管理背板快取中刪除：

```
delete url-database url <URL>
```

下次防火牆查詢所指定 URL 的類別時，系統會將要求轉送至管理背板，然後轉送至雲端。這會解決類別查閱問題。如果問題仍然存在，請使用下一個步驟提交分類變更要求。

STEP 5 | 若要從 Web 介面提交變更要求，請移至 URL 日誌以從 Web 介面提交變更要求，然後選取您想要變更 URL 的日誌項目。

STEP 6 | 按一下 **Request Categorization**（要求分類）變更連結，並依照指示進行。您也可以搜尋 URL，再按一下 **Request Change**（要求變更）圖示，向 Palo Alto Networks Test A Site 網站要求變更類別。若要查看每個類別的說明，請參閱預先定義的 URL 類別。

如果核准了您的變更要求，您將會收到電子郵件通知。接著您會有兩個選擇可確定防火牆上的 URL 分類已更新：

- 一直等待到快取中的 URL 過期為止，下一次使用者存取 URL 時，新的分類更新便會放在快取中。
- 執行下列命令強制執行快取中的更新：

```
request url-filtering update url <URL>
```


疑難排解網站存取問題

這可在何處使用？	我需要什麼？
• NGFW (Managed by PAN-OS or Panorama)	❑ 進階 URL 篩選授權（或舊版 URL 篩選授權） 註： 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。

一般使用者可能因為各種原因遇到網站存取問題，包括遺失 URL 篩選授權、政策規則設定錯誤、PAN-DB 連線問題或網站分類錯誤。請透過下列步驟來診斷並解決網站存取問題。

這個問題可能與 *URL* 篩選無關。此工作中步驟後的「下一步該做什麼」區段列出了疑難排解的其他重點領域。

STEP 1 | 確認您有啟用進階 URL 篩選或舊版 URL 篩選授權。

新世代防火牆需要有效的 *URL* 篩選授權，才能準確地分類網站和應用程式。如果您沒有 *URL* 篩選授權，則網站存取問題就與 *URL* 篩選無關。

選取 **Device**（裝置） > **Licenses**（授權），然後尋找進階 URL 篩選（或 PAN-DB URL 篩選）授權。啟用中的授權會顯示超過目前日期的到期日期。

或者，您也可以使用要求授權資訊 CLI 命令。如果授權處於啟用狀態，介面會顯示包括到期狀態等授權資訊：已到期？無。

STEP 2 | 確認 CLI 上的 PAN-DB 雲端連線狀態。

雲端連線：欄位應顯示已連線。否則，不存在管理平面 (MP) 快取中的任何 URL 都將被分類為未解析，且可能被安全性政策規則中的 URL 篩選設定檔設定封鎖。

STEP 3 | 清除特定 URL 的 MP 和資料平面 (DP) 快取。

清除快取可能需要耗費許多資源。您可以考慮在維護時段清除快取。

1. 若要清除 MP 快取，請使用 **`delete url-database url <affected url>`** CLI 命令。
2. 若要清除 DP 快取，請使用清除 **`clear url-cache url <affected url>`** CLI 命令。

STEP 4 | 檢視 URL 篩選日誌，以確認該網站所屬的 URL 類別是否已被封鎖。

1. 選取 **Monitor**（監控） > **URL Filtering**（**URL** 篩選）。
2. 搜尋受影響的 URL，然後選取最近的日誌項目。
3. 檢視「類別」和「動作」欄。

   URL 是否有正確分類？使用 Palo Alto Networks 的 URL 類別查閱工具 Test A Site 來驗證其類別。如果您仍認為分類錯誤，請提交變更要求。

   如果「動作」欄顯示 `block-url`，請記下與日誌項目相關的安全性政策規則的名稱。

STEP 5 | 檢視安全性政策規則，並視需要進行更新。

1. 選取 **Policies**（政策） > **Security**（安全性），然後選取您在上一步驟中記下的政策規則。
2. 確認安全性政策規則是否允許存取要求的 URL 或其 URL 類別。

   尋找兩種設定之一：

   - **URL Category as Match Criteria:**（作為比對準則的 **URL** 類別：）在 **Service/URL Category**（服務/**URL** 類別）下，其中一個指定類別會包含要求的 URL。在 **Actions**（動作）下，「動作設定」設為 **Allow**（允許）。
   - **URL Filtering Profile:**（**URL** 篩選設定檔：）在 **Actions**（動作）下，「設定檔設定」設為允許存取所要求 URL 的 URL 篩選設定檔。

STEP 6 | 測試您的安全性政策規則。

如果上述步驟未醒目顯示或解決問題，則可能需要額外的疑難排解以進一步隔離問題。重點領域應包括：

- 基本 IP 位址連線
- 路由設定
- DNS 解析
- Proxy 設定
- 封包路徑中的上游防火牆或檢查裝置

如出現間歇性或複雜問題，請聯繫 Palo Alto Networks 支援團隊以獲得進一步協助。

疑難排解 URL 篩選回應頁面顯示問題

這可在何處使用？	我需要什麼？
• NGFW (Managed by PAN-OS or Panorama)	❑ 進階 URL 篩選授權（或舊版 URL 篩選授權） 註： 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。

URL 篩選回應頁面可能因各種原因而無法顯示，包括：

- 啟用 SSL/TLS 交握檢查。
- 該網站在 SSL/TLS 交握檢查期間被封鎖。在此情況下，畫面不會顯示 URL 篩選回應頁面，因為防火牆重設了 HTTPS 連線。
- 該網站使用 HTTPS 協定或包含透過 HTTPS 提供的內容（例如廣告），但該網站或 URL 類別未解密。
- 自訂回應頁面超過所支援的大小上限。

請透過下列步驟開始疑難排解無法顯示的 URL 篩選回應頁面。如果問題仍然存在，請聯絡 Palo Alto Networks 支援部門。

STEP 1 | 確定問題範圍。

該問題是否只發生於特定網站或網頁子集？檢查造訪網站上的其他頁面時是否顯示回應頁面。

STEP 2 | 識別網站的協定（HTTP 或 HTTPS）。

這個區別有助於進一步隔離和診斷問題。

STEP 3 | （HTTPS 網站或包含 HTTPS 內容的 HTTP 網站）驗證 SSL/TLS 解密政策規則是否對網站或 URL 類別的流量進行解密。

一般來說，防火牆無法在 *HTTPS* 網站上提供回應頁面，除非它可以解密該網站。

部分網站可能透過 *HTTP* 提供其主頁，但透過 *HTTPS* 提供廣告或其他內容。這些網站也應該解密以確保顯示回應頁面。

1. 登入網頁介面。
2. 選取 **Policies**（政策） > **Decryption**（解密），並驗證相關規則是否解密到特定網站或 URL 類別的流量。

   如果情況非如此，請更新解密政策規則以解密網站或 URL 類別。

- 如果啟用 SSL/TLS 解密但回應頁面仍未顯示，則請啟用 SSL/TLS 交握檢查。
- 若要透過 HTTPS 工作階段提供 URL 篩選回應頁面而不啟用 SSL/TLS 解密，請依照下列步驟操作。

STEP 4 | 確認該網站所屬的 URL 類別是否已被封鎖。

如果該類別已被套用於安全性政策規則的 URL 篩選設定檔中，或被以特定 URL 類別作為符合條件的安全性政策規則封鎖，則給定項目的「動作」欄會顯示 `block-url`。

1. 選取 **Monitor**（監控） > **URL Filtering**（**URL** 篩選）。
2. 搜尋受影響的網站，然後選取最近的日誌項目。
3. 檢查「類別」和「動作」欄。

   指派給網站的類別是否正確？使用 Palo Alto Networks 的 URL 類別查閱工具 Test A Site 來驗證其類別。如果您仍認為網站分類錯誤，請提交變更要求。

   「動作」值是 `block-url` 嗎？若非，請更新 URL 篩選設定檔或安全性政策規則。
4. 請記下與此日誌條目相關的規則，以供日後參考。

STEP 5 | 確定自訂回應頁面是否是導致此問題的原因。

1. 選取 **Device**（裝置） > **Response Pages**（回應頁面）。
2. 確認僅選取 **Predefined**（預先定義）。

   如果在以下任一位置列出 **shared**（共用）（除了 **Predefined**（預先定義）之外），則表示自訂回應頁面處於啟用狀態：

   - **Device**（裝置） > **Response Pages**（回應頁面）：在對應於給定回應頁面的「位置」欄下。
   - **Device**（裝置） > **Response Pages**（回應頁面） > ***Type***（類型）：在「位置」下。
3. （如果列出 **Shared**（共用））將自訂頁面恢復為其預設狀態，以確認自訂回應頁面是問題根本原因。

   1. **Delete**（刪除）自訂頁面。
   2. **Commit**（提交）您的變更。
   3. 前往受影響的網站以查看是否顯示預設回應頁面。

   如果問題仍未解決，請致電支援團隊進行進一步調查。

如果上述步驟無法解決問題，請聯絡 Palo Alto Networks 支援團隊。可能需要進行其他疑難排解才能找出問題。例如，如果回應頁面無法在部分網頁正常運作但可以在其他網頁正常運作，則透過封包擷取 (pcap) 工具和支援來分析流量可能會有所幫助。

PAN-DB 私人雲端

這可在何處使用？	我需要什麼？
• NGFW (Managed by PAN-OS or Panorama)	☐ 進階 URL 篩選授權（或舊版 URL 篩選授權） 註： 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。

PAN-DB 私人雲端提供內部部署解決方案，適用於限制使用公共雲端服務的組織。但請注意，防火牆在 URL 查閱期間會查詢 PAN-DB 私人雲端伺服器，而非 PAN-DB 公共雲端伺服器。若要採取此解決方案，您需要在網路或資料中心內部署一或多個 M-600 或 M-700 設備作為 PAN-DB 伺服器。只有執行 PAN-OS 9.1 或更新版本的防火牆能與 PAN-DB 私人雲端進行通訊。 後新增 xref 至「部署」

PAN-DB 私人雲端部署不支援 *Advanced URL Filtering* 訂閱的基於雲端的 *URL* 分析功能。

下表說明 PAN-DB 公共雲端和 PAN-DB 私人雲端之間的差異。

表 **1: PAN-DB** 公共雲端與 **PAN-DB** 私人雲端之間的差異

差異	PAN-DB 公共雲端	PAN-DB 私人雲端
內容與資料庫更新	內容（定期與重要）更新與完整 URL 資料庫更新一天發佈多次。PAN-DB 公共雲端每五分鐘會更新一次惡意軟體和網路釣魚 URL 類別。防火牆也會在其為了查閱 URL 而查詢雲端伺服器時，檢查重要更新。	內容更新與完整 URL 資料庫更新在工作週中，一天只能用一次。
URL 分類要求	您可以透過以下方式要求變更 URL 類別： • Palo Alto Networks Test A Site 網站。 • URL 篩選設定檔。 • URL 篩選日誌。	您可以透過 Palo Alto Networks Test A Site 網站要求變更 URL 類別。
未解析的 **URL** 查詢	如果防火牆無法解析 URL 查詢，會將要求傳送至公共雲端中的伺服器。	如果防火牆無法解析查詢，會將要求傳送至 PAN-DB 私人雲端中的設備。如果沒有符合的 URL 項目，PAN-DB 私人雲端會將未知類別的回應傳送至防火牆；不會將要求傳送至公共雲

差異	PAN-DB 公共雲端	PAN-DB 私人雲端
		端，除非您已設定設備來存取 PAN-DB 公共雲端。 如果 PAN-DB 私人雲端中的設備完全離線執行，防火牆不會向公共雲端傳送任何資料或分析。

- PAN-DB 私人雲端的運作方式
- PAN-DB 私人雲端設備
- 設定 PAN-DB 私人雲端

PAN-DB 私人雲端的運作方式

這可在何處使用？	我需要什麼？
• NGFW (Managed by PAN-OS or Panorama)	❑ 進階 URL 篩選授權（或舊版 URL 篩選授權） 註： 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。

當您設定 PAN-DB 私人雲端時，可以將 M-600 或 M-700 設備設為擁有直接網路存取權或保持離線。設備需要資料庫和內容更新才能執行 URL 查閱。如果設備沒有使用中的網際網路連線，您必須將更新手動下載至網路中的伺服器，並使用 SCP 將更新匯入 PAN-DB 私人雲端的每個 M-600 或 M-700 設備。此外，裝置必須能夠取得種子資料庫，以及它所提供之防火牆的其他任何定期或重要的內容更新。

私人雲端和公共雲端部署中的防火牆 URL 查閱程序相同。但是，在私人雲端部署中，防火牆會查詢 PAN-DB 私人雲端中的伺服器。您需要指定每個 M-600 或 M-700 伺服器可查詢的 IP 位址或 FQDN，以授予防火牆對私人雲端伺服器的存取權限。

M-600 和 M-700 設備使用預先包裝的伺服器憑證來驗證連線到 PAN-DB 私人雲端的防火牆。您無法匯入或使用其他伺服器憑證來進行驗證。如果您變更設備中的主機名稱，設備會自動產生一組新的憑證來驗證防火牆。

PAN-DB 私人雲端設備

這可在何處使用？	我需要什麼？
• NGFW (Managed by PAN-OS or Panorama)	❑ 進階 URL 篩選授權（或舊版 URL 篩選授權） 註： 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。

若要部署 PAN-DB 私人雲端，您需要一或多個 M-600 或 M-700 設備。兩種設備均處於 Panorama 模式，但將作為 PAN-DB 私人雲端部署，因此您必須對其進行設定才能在 PAN-URL-DB 模式下操作。在 PAN-URL-DB 模式下，裝置會為不想使用 PAN-DB 私人雲端的企業提供 URL 分類服務。

在作為 PAN-DB 私人雲端部署時，M-600 和 M-700 設備可使用 MGT (Eth0) 與 Eth1 兩個連接埠；Eth2 無法使用。管理連接埠用於獲得對裝置的管理存取權，以及從 PAN-DB 公共雲端或從您網路中的伺服器取得最新內容更新。為了讓 PAN-DB 私人雲端與您網路中的防火牆通訊，您可以使用 MGT 連接埠或 Eth1。

M-200 設備無法作為 *PAN-DB* 私人雲端部署。

PAN-URL-DB 模式中的 M-600 和 M-700 設備：

- 沒有網頁介面，僅支援命令列介面 (CLI)。
- 無法由 Panorama 管理。
- 無法在高可用性配對中部署。
- 不需要 URL 篩選授權。防火牆必須有有效的 PAN-DB URL 篩選授權才能與 PAN-DB 私人雲端連線，並對其進行查詢。
- 隨附一組預設伺服器憑證，用來驗證連線至 PAN-DB 私人雲端的防火牆。您無法匯入或使用其他伺服器憑證來驗證防火牆。如果您變更任一設備中的主機名稱，設備會自動產生一組新的憑證來驗證它所提供的防火牆。
- 只能重設為 Panorama 模式。如果您想將設備部署為專用日誌收集器，請切換至 Panorama 模式，然後在日誌收集器模式下對其進行設定。

設定 PAN-DB 私人雲端

這可在何處使用？	我需要什麼？
• NGFW (Managed by PAN-OS or Panorama)	❑ 進階 URL 篩選授權（或舊版 URL 篩選授權） 註： 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。

若要將一或多個 M-600 或 M-700 設備作為 PAN-DB 私人雲端部署在網路或資料中心內，您必須完成下列工作：

- 設定 PAN-DB 私人雲端
- 設定防火牆以存取 PAN-DB 私人雲端
- 在 PAN-DB 私人雲端上設定採用自訂憑證的驗證

設定 PAN-DB 私人雲端

這可在何處使用？	我需要什麼？
• NGFW (Managed by PAN-OS or Panorama)	❑ 進階 URL 篩選授權（或舊版 URL 篩選授權） 註： 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。

STEP 1 | 在機架中安裝 M-600 或 M-700 設備。

請參閱相關硬體參考指南取得機架安裝說明。

STEP 2 | 註冊 M-600 設備。

STEP 3 | 執行設備的初始設定。

PAN-DB 模式中的 *M-600* 和 *M-700* 設備使用 *MGT (Eth0)* 與 *Eth1* 兩個連接埠；不會在 *PAN-DB* 模式中使用 *Eth2*。管理連接埠用於獲得對裝置的管理存取權，以及從 *PAN-DB* 公共雲端取得最新內容更新。為了讓裝置 *(PAN-DB* 伺服器*)* 與網路中的防火牆通訊，您可以使用 *MGT* 連接埠或 *Eth1*。

1. 以下列其中一種方式連線至設備：
   - 從電腦中將序列纜線連線至設備上的主控台連接埠，然後使用終端機模擬軟體連線 (9600-8-N-1)。
   - 將 RJ-45 乙太網路纜線從電腦連線至設備的 MGT 連接埠。在瀏覽器中前往 https://192.168.1.1。若要允許存取此 URL，可能需要將電腦上的 IP 位址變更為 192.168.1.0 網路中的位址（例如 192.168.1.2）。
2. 出現提示時，登入裝置。使用預設使用者名稱與密碼 (admin/admin) 登入。裝置將開始初始化。
3. 設定 MGT 介面的網路存取設定（包括 IP 位址）：

   請使用以下 CLI 命令：**set deviceconfig system ip-address *<server-IP>* netmask *<netmask>* default-gateway *<gateway-IP>* dns-setting servers primary *<DNS-IP>***。

   變數說明：
   - *<server-IP>* 是您要指派給伺服器的管理介面的 IP 位址
   - *<netmask>* 是子網路遮罩
   - *<gateway-IP>* 是網路閘道的 IP 位址，*<DNS-IP>* 則是主要 DNS 伺服器的 IP 位址
   - *<DNS-IP>* 是 DNS 伺服器的 IP 位址
4. 設定 Eth1 介面的網路存取設定（包括 IP 位址）。

   請使用以下命令：**set deviceconfig system eth1 ip-address *<server-IP>* netmask *<netmask>* default-gateway *<gateway-IP>* dns-setting servers primary *<DNS-IP>***。
5. 將您的變更儲存至 PAN-DB 伺服器。

   使用提交命令。

STEP 4 | 切換至 PAN-DB 私人雲端模式。

您可以在 *Panorama* 模式與 *PAN-DB* 模式之間來回切換；也可以在 Panorama 模式與日誌收集器模式之間來回切換。不支援 *PAN-DB* 模式與日誌收集器模式之間的直接來回切換。切換操作模式時會觸發資料重設。除了管理存取設定以外，所有現有設定與日誌都會在重新啟動時遭到刪除。

1. 若要切換至 PAN-DB 模式，請使用 **request system system-mode pan-url-db** 命令。
2. 若要驗證模式切換，請使用 **show system info** 命令。

   如果您已成功切換至 PAN-DB 私人雲端模式，系統模式欄位會顯示 PAN-URL-DB。

```
admin@M-600> show system info  hostname:M-600 ip-
address:1.2.3.4 public-ip-address: netmask:255.255.255.0
 default-gateway:1.2.3.1 ipv6-address: unknown ipv6-
link-local-address: fe80:00/64 ipv6-default-gateway:
 mac-address:00:56:90:e7:f6:8e time:Mon Apr 27 13:43:59
 2015 uptime:10 days, 1:51:28 family: m model:M-600
 serial:0073010000xxx sw-version:7.0.0 app-version:492-2638
 app-release-date:2015/03/19 20:05:33 av-version:0 av-release-
date: unknown wf-private-version:0 wf-private-release-date:
 unknown wildfire-version:0 wildfire-release-date: logdb-
version:7.0.9 platform-family: m pan-url-db:20150417-220
 system-mode:Pan-URL-DB operational-mode: normal licensed-
device-capacity:0 device-certificate-status:None
```

3. 若要檢查設備上雲端資料庫的版本，請使用 **show pan-url-cloud-status** 命令。

   系統資訊顯示的 *pan-url-db* 欄位會有相同的資訊。

STEP 5 | 安裝內容及資料庫更新。

設備僅儲存內容的目前執行版本以及一個舊版本。

請選擇下列任一安裝方法：

- 如果 PAN-DB 伺服器擁有直接的網際網路存取權，請使用下列命令：
  - 若要檢查是否發佈新版本：**request pan-url-db upgrade check**
  - 若要檢查目前安裝在您伺服器上的版本：**request pan-url-db upgrade info**。
  - 若要下載最新版本：**request pan-url-db upgrade download latest**。

    若要安裝最新版本：**request pan-url-db upgrade install <*version latest | file*>**。
  - 若要安排設備自動檢查更新：**set deviceconfig system update-schedule pan-url-db recurring weekly action download-and-install day-of-week <*day of week*> at <*hr:min*>**。
- 若 PAN-DB 伺服器離線，請存取 Palo Alto Networks 客戶支援入口網站，以將內容更新下載並儲存至您網路中的 SCP 伺服器。然後，您可以使用下列命令匯入並安裝更新：
  - **scp import pan-url-db remote-port <*port-number*> from username@host:path**
  - **request pan-url-db upgrade install file <*filename*>**

STEP 6 | 設定 PAN-DB 私人雲端的管理存取權。

裝置擁有預設 *admin* 帳戶。您建立的其他任何管理使用者可以是超級使用者（擁有完整存取權），也可以是擁有唯讀存取權的超級使用者。

PAN-DB 私人雲端不支援 *RADIUS VSA* 的使用。如果將在防火牆或 *Panorama* 上使用的 *VSA* 用於啟用對 *PAN-DB* 私人雲端的存取，會發生驗證失敗。

- 若要在 PAN-DB 伺服器上設定本機管理使用者，請使用下列命令：
  1. **configure**
  2. **set mgt-config users <*username*> permissions role-based <superreader | superuser> yes**
  3. **set mgt-config users <*username*> password**
  4. 輸入密碼：**xxxxx**
  5. Confirm password:**xxxxx**
  6. 提交
- 若要使用 RADIUS 驗證設定管理使用者，請使用下列命令：
  1. 若要建立 RADIUS 伺服器設定檔：**set shared server-profile radius <*server_profile_name*> server <*server_name*> ip-address <*ip_address*> port <*port_no*> secret <*shared_password*>**。
  2. 若要建立驗證設定檔：**set shared authentication-profile <*auth_profile_name*> user-domain <*domain_name_for_authentication*> allow-list <all> method radius server-profile <*server_profile_name*>**。
  3. 若要將驗證設定檔附加至使用者：**set mgt-config users <*username*> authentication-profile <*auth_profile_name*>**。
  4. 若要提交您的變更：**commit**。
- 若要檢視使用者清單，請使用 **show mgt-config users** 命令。

STEP 7 | 設定防火牆以存取 PAN-DB 私人雲端。

設定防火牆以存取 PAN-DB 私人雲端

這可在何處使用？	我需要什麼？
• NGFW (Managed by PAN-OS or Panorama)	☐ 進階 URL 篩選授權（或舊版 URL 篩選授權） 註：舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。

使用 PAN-DB 公共雲端時，每個防火牆都可以存取 AWS 雲端中的 PAN-DB 伺服器，來下載其可連線以進行 URL 查閱之合格伺服器的清單。在使用 PAN-DB 私人雲端的情況下，您必須使用將用

於 URL 查閱之 PAN-DB 私人雲端伺服器的（靜態）清單來設定防火牆。該清單最多可包含 20 個項目；支援 IPv4 位址、IPv6 位址與 FQDN。清單中的每個項目—IP 位址或 FQDN—必須指定給 PAN-DB 伺服器的管理連接埠或 eth1。

STEP 1 | 從 PAN-OS CLI，新增用於 URL 查閱的靜態 PAN-DB 私人雲端伺服器清單。

- 使用下列 CLI 命令新增私人 PAN-DB 伺服器的 IP 位址：

```
> configure
```

```
# set deviceconfig setting pan-url-db cloud-static-list <IP addresses>
```

或者，在每個防火牆的 Web 介面上，選取 **Device**（裝置） > **Setup**（設定） > **Content-ID**（內容 **ID**），編輯 [URL Filtering（URL 篩選）] 區段，然後輸入 PAN-DB 伺服器的 IP 位址或 FQDN。清單必須以逗號分隔。

- 若要刪除私人 PAN-DB 伺服器的項目，請使用下列 CLI 命令：

```
# delete deviceconfig setting pan-url-db cloud-static-list <IP addresses>
```

刪除私人 PAN-DB 伺服器清單會在防火牆上觸發重新選取程序。防火牆會先檢查 PAN-DB 私人雲端伺服器的清單，當它找不到時，防火牆會存取 AWS 雲端中的 PAN-DB 伺服器，來下載其可連線之合格伺服器的清單。

STEP 2 | 輸入 **# commit** 以儲存變更。

STEP 3 | 若要確認變更是否有效，請在防火牆上使用下列 CLI 命令：

```
> show url-cloud status Cloud status:Up URL database version:20150417-220
```

在 PAN-DB 私人雲端上設定採用自訂憑證的驗證

這可在何處使用？	我需要什麼？
• NGFW (Managed by PAN-OS or Panorama)	☐ 進階 URL 篩選授權（或舊版 URL 篩選授權） 註： 舊版 *URL* 篩選授權已終止，但仍支援有效的舊版授權。

根據預設，PAN-DB 伺服器會使用預先定義的憑證相互驗證，以建立 SSL 連線來用於管理存取和裝置間通訊。不過，您可以設定改用自訂憑證進行驗證。自訂憑證可讓您建立唯一的信任鏈，以確保 PAN-DB 伺服器與防火牆之間的相互驗證。對於 PAN-DB 私人雲端而言，防火牆充當用戶端，而 PAN-DB 伺服器則充當伺服器。

STEP 1 | 為 PAN-DB 伺服器與防火牆獲取金鑰配對以及憑證授權單位 (CA) 憑證。

STEP 2 | 匯入 CA 憑證以在防火牆上驗證憑證。

1. 登入 PAN-DB 伺服器上的 CLI 並進入組態模式。

```
admin@M-600> configure
```

2. 使用 TFTP 或 SCP 匯入 CA 憑證。

```
admin@M-600# {tftp | scp} import certificate from <value>
 file <value> remote-port <1-65535> source-ip <ip/netmask>
 certificate-name <value> passphrase <value> format {pkcs12 |
 pem}
```

STEP 3 | 使用 TFTP 或 SCP 匯入包含私人雲端設備的伺服器憑證與私密金鑰的金鑰配對。

```
admin@M-600# {tftp | scp} import keypair from <value> file <value>
 remote-port <1-65535> source-ip <ip/netmask> certificate-
name <value> passphrase <value> format {pkcs12 | pem}
```

STEP 4 | 設定包含 root CA 和中繼 CA 的憑證設定檔。此憑證設定檔定義 PAN-DB 伺服器與防火牆之間的裝置驗證。

1. 在 PAN-DB 伺服器的 CLI 中，進入組態模式。

```
admin@M-600> configure
```

2. 為憑證設定檔命名。

```
admin@M-600# set shared certificate-profile <name>
```

3. （選用）設定使用者網域。

```
admin@M-600# set shared certificate-profile <name>
 domain <value>
```

4. 設定 CA。

Default-ocsp-url 與 ***ocsp-verify-cert*** 為選用參數。

admin@M-600# **set shared certificate-profile <name> CA <name>**

```
admin@M-600# set shared certificate-profile <name> CA <name>
 [default-ocsp-url <value>]
```

```
admin@M-600# set shared certificate-profile <name> CA <name>
 [ocsp-verify-cert <value>]
```


STEP 5 | 設定設備的 SSL/TLS 服務設定檔。此設定檔定義 PAN-DB 及用戶端裝置為 SSL/TLS 服務所使用的憑證與通訊協定範圍。

1. 識別 SSL/TLS 服務設定檔。

```
admin@M-600# set shared ssl-tls-service-profile <name>
```

2. 選取憑證。

```
admin@M-600# set shared ssl-tls-service-profile <name>
 certificate <value>
```

3. 定義 SSL/TLS 範圍。

PAN-OS 8.0 和更新版本僅支援 *TLSv1.2* 和更新 *TLS* 版本。必須將最高版本設定為 ***TLS 1.2*** 或 ***max***（最高）。

```
admin@M-600# set shared ssl-tls-service-profile <name>
 protocol-settings min-version {tls1-0 | tls1-1 | tls1-2
```

```
admin@M-600# set shared ssl-tls-service-profile <name>
 protocol-settings max-version {tls1-0 | tls1-1 | tls1-2 | max
```

STEP 6 | 在 PAN-DB 上設定安全伺服器通訊。

1. 設定 SSL/TLS 服務設定檔。此設定檔套用至 PAN-DB 與防火牆之間的所有 SSL 連線。

```
admin@M-600# set deviceconfig setting management secure-conn-
server ssl-tls-service-profile <ssltls-profile>
```

2. 設定憑證設定檔。

```
admin@M-600# set deviceconfig setting management secure-conn-
server certificate-profile <certificate-profile>
```

3. 設定中斷連線等候時間。這是 PAN-DB 在中斷連線並與防火牆重新建立連線之前等候的時間（範圍為 0 至 44,640）。

```
admin@M-600# set deviceconfig setting management secure-conn-
server disconnect-wait-time <0-44640
```

STEP 7 | 匯入 CA 憑證以驗證設備憑證。

1. 登入防火牆 Web 介面。
2. 匯入 CA 憑證。

STEP 8 | 為防火牆設定本機憑證或 SCEP 憑證。

1. 若您為 設定本機憑證，請匯入防火牆金鑰配對。
2. 若您為 設定 SCEP 憑證，請設定 SCEP 設定檔。

STEP 9 | 為防火牆設定憑證設定檔。您可以在每個防火牆上個別設定這一項，也可以作為範本的一部分將此組態從 Panorama 推送至防火牆。

1. 對於防火牆，請選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificate Profile**（憑證設定檔），或者對於 Panorama，則選取 **Panorama** > **Certificate Management**（憑證管理） > **Certificate Profile**（憑證設定檔）。
2. 設定憑證設定檔。

STEP 10 | 在每個防火牆上部署自訂憑證。可透過 Panorama 集中部署憑證，或者在每個防火牆上手動設定憑證。

1. 登入防火牆 Web 介面。
2. 針對防火牆請選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），或針對 Panorama 請選取 **Panorama** > **Setup**（設定） > **Management**（管理），並 **Edit**（編輯）安全通訊 設定。
3. 從各自的下拉式清單中選取 **Certificate Type**（憑證類型）、**Certificate**（憑證）以及 **Certificate Profile**（憑證設定檔）。
4. 在 Customize Communication（自訂通訊）設定中，選取 **PAN-DB Communication**（**PAN-DB** 通訊）。
5. 按一下 **OK**（確定）。
6. **Commit**（提交）您的變更。

   提交變更後，防火牆不會終止目前與 PAN-DB 伺服器之間建立的工作階段，直到 **Disconnect Wait Time**（中斷連線等候時間）過後。在下一步中執行自訂憑證的使用後，中斷連線等候時間會開始倒計時。

STEP 11 | 強制執行自訂憑證驗證。

1. 登入 PAN-DB 伺服器上的 CLI 並進入組態模式。

```
admin@M-600> configure
```

2. 執行自訂憑證的使用。

```
admin@M-600# set deviceconfig setting management secure-conn-
server disable-pre-defined-cert yes
```

提交此變更後，中斷連線等候時間會開始倒計時（若您已在 PAN-DB 上設定此 設定）。等候時間結束後，PAN-DB 及其防火牆僅使用設定的憑證進行連線。

STEP 12 | 將新防火牆或 Panorama 新增至您的 PAN-DB 私人雲端部署時，有兩個選擇可用。

- 如果您未啟用 **Custom Certificates Only**（僅限自訂憑證），則您可將新防火牆新增至 PAN-DB 私人雲端，然後部署自訂憑證。
- 如果您已在 PAN-DB 私人雲端上啟用 **Custom Certificates Only**（僅限自訂憑證），則您必須先在防火牆上部署自訂憑證，才能將其連線至 PAN-DB 私人雲端。

