paloalto
TECHDOCS

Strata Cloud Manager 入門

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

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2023-2025 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

February 4, 2025

Table of Contents

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

Strata Cloud Manager 簡介

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目 • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

Palo Alto Networks Strata Cloud Manager 可讓您對整個網路安全部署執行採用 AI 計數的統一管理和操作。透過 Strata Cloud Manager，您可以從簡化的單一使用者介面輕鬆管理整個 Palo Alto Networks 網路安全性基礎架構（NGFW 和 SASE 環境）。全方位檢視所有網路安全強制執行點的使用者、分支站台、應用程式和威脅；為您提供可操作的洞察、提升安全性，並且讓您輕鬆地排解和解決問題。

- ❑ 預測和防止網路中斷

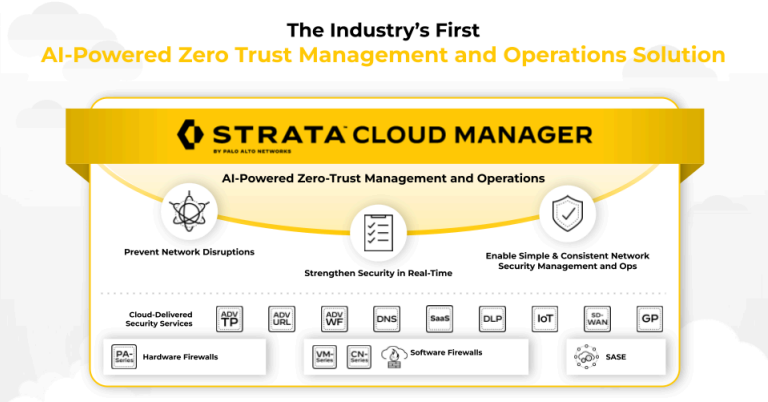
  Strata Cloud Manager 可預測和防止網路中斷，並快速修復問題，讓您和使用者能夠繼續日常業務並保持工作效率。

- ❑ 透過即時最佳做法加強安全性

  Strata Cloud Manager 可識別重要且未充分利用的安全功能，並引導您根據符合自身需求的最佳做法加以啟用。透過採用 AIOPS 技術的內建最佳做法和內嵌修復功能，來加強您的安全性狀態。

- ❑ 簡單而一致的網路安全性管理和操作

  Strata Cloud Manager 整合了您的安全工具，藉此改善操作和洞察力，讓您能夠為整個網路安全性堆疊採用簡單而一致的管理體驗。



 ©2025 Palo Alto Networks, Inc.

Strata Cloud Manager 如何加強安全性

盡可能利用安全功能

- 查看您所使用的安全功能，並識別您可以利用的安全功能在採用方面的漏洞。→ 功能採用
- 查看安全服務訂閱的採用率。→ CDSS 採用
- 瞭解您的安全功能是否遵循最佳做法，或您可以在哪些方面進行改進以加強安全性狀態。→ 內建最佳做法

加強和最佳化現有設定

根據使用量資料和自動產生的建議，清理和簡化您的安全性政策。

- 清理政策中未參考的物件以及沒有任何流量的規則；這些物件和規則可能會影響效能，並使政策管理複雜化。→ 設定清理
- 過於通泛的規則會引發安全漏洞，因為這類規則會允許您的網路中未使用的應用程式。政策最佳化工具可讓您將這些過於寬鬆的規則轉換為更具體、更有針對性的規則，而僅允許您實際使用的應用程式。→ 政策最佳化工具

安全設定的即時指引

- 最佳做法資料護欄可讓您即時驗證安全性策略規則是否符合最佳做法。→ 即時、內嵌最佳做法設定檢查

©2025 Palo Alto Networks, Inc.

Strata Cloud Manager 如何預測和防止網路中斷

全方位的可觀察性

- 瞭解安全基礎架構如何確保您的網路安全。→ 控管中心
- 瞭解使用者、分支站台、應用程式和 IT 基礎架構的健康情況和效能單一儀表板。→SASE 健康情況儀表板
- 從單一儀表板瞭解裝置的健康情況和效能。→ 裝置健康情況儀表板

預測健康情況並修復中斷

自動預測可防止潛在的中斷；在偵測到問題時，可操作的洞察可加快解決問題。

- 機器輔助預測即將發生的中斷，並提供修復步驟的建議。→ 預測和異常偵測
- 縮短可能成因分析的解析時間。→ 檢視可能成因

妥善規劃以因應不斷變化的安全需求

- 主動識別潛在容量以提高穩定性。→ 容量分析器

©2025 Palo Alto Networks, Inc.

Strata Cloud Manager 如何隨處一致運作

一致的設定

透過簡化的程序在所有強制執行點套用一致的政策，而無須再對 NGFW 和 SASE 部署進行個別變更。

- 設定及上線 NGFW 和 Prisma Access 行動使用者與遠端網路，並規劃 NGFW 的軟體升級。→ Strata Cloud Manager 中的工作流程
- 設定在 NGFW 與 Prisma Access 間共用的安全性政策。→ NGFW 和 Prisma Access 的共用管理

靈活的設定組織

透過簡單的資料夾和裝置管理工作流程，大規模簡化設定管理。

- 在整個環境中全域套用組態設定並強制執行政策，或將設定和政策的目標定為組織的某些部分。→ 設定範圍
- 對您的防火牆或部署類型進行邏輯分組（Prisma Access 行動使用者、遠端網路或服務連線），以簡化設定管理。→ 資料夾管理
- 對設定進行分組，讓您能夠將其快速推送至防火牆或部署。→ 片段
- 您可以靈活因應裝置或部署特有的設定值。→ 變數

實現威脅的統一可見性

- 全方位檢視您的網路流量、訂閱、使用者、應用程式、網路、威脅等等。→ 監控
- 以互動方式檢視網路中執行的應用程式、ION 裝置、威脅、使用者和安全性訂閱。儀表板可讓您檢視部署中發生的健康情況、安全性狀態和活動，協助您防止或解決網路中的效能問題和安全漏洞。→ 儀表板
- 取得網路流量模式、頻寬使用率、安全性訂閱資料等項目的報告。報告針對您的網路提供可操作的洞察，讓您用於規劃和監控用途。→ 報告

©2025 Palo Alto Networks, Inc.

Strata Cloud Manager 支援的產品

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目 • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

Strata Cloud Manager 為您的 NGFW 和 SASE 網路提供了採用 AI 技術的統一管理和操作，以及可供您使用的 Strata Cloud Manager 功能（具體取決於您的授權）。以下是使 Strata Cloud Manager 能夠管理 NGFW 和 SASE，並可解鎖 Strata Cloud Manager 網路安全功能的授權。→ 以下說明如何驗證您的授權

表 **1:**

Strata Cloud Manager Essentials	Strata Cloud Manager Essentials 提供管理和安全功能，連同下列功能免費供您使用： • 新世代防火牆 (NGFW) • Prisma Access Strata 記錄服務是 Strata Cloud Manager Essentials 的選用附加元件。 *Strata Cloud Manager Essentials* 和 *Strata Cloud Manager Pro* 可在沒有以下功能的客戶支援入口網站 *(CSP)* 帳戶中啟動：搭配合適儲存空間的 *Strata* 記錄服務、*AIOps for NGFW Free* 或 *Premium*，或是 *Prisma Access*。
Strata Cloud Manager Pro	Strata Cloud Manager Pro 是付費層，包含 Strata Cloud Manager Essentials 的所有功能，以及可增強運作健康情況、防止網路中斷、加強即時安全性狀態的進階功能，和用來監控使用者體驗效能的自發數位體驗管理 (ADEM)。Strata Cloud Manager Pro 包含 Strata 記錄服務，具有一年的日誌保留和無

 ©2025 Palo Alto Networks, Inc.

	限儲存空間，可讓您在集中位置記錄和順暢地擷取整個部署中的資料。購買 Strata Cloud Manager Pro 可以取得下列功能： • 新世代防火牆 (NGFW) • 由軟體 NGFW 積分資助的 VM 系列 • Prisma Access
NGFW Premium 的 AIOps	對於具有 AIOps for NGFW Premium 授權的 NGFW，Strata Cloud Manager 可讓您完整檢視 NGFW 的健康情況和安全性，並且可強制執行主動檢查以消弭安全漏洞。 • **NGFW (Managed by PAN-OS or Panorama)** → 對於具有 AIOps for NGFW Premium 授權的 PAN-OS 和 Panorama 管理的 NGFW，請使用 Strata Cloud Manager 來監控您的部署健康情況和安全性狀態。 • **NGFW (Managed by Strata Cloud Manager)** → 透過 AIOps for NGFW 授權，您也可以將 Strata Cloud Manager 用於 **NGFW** 的雲端管理。 • 請聯絡您的客戶團隊，以使用 *Strata Cloud Manager* 啟用 NGFW 的雲端管理。 • *Strata Cloud Manager* 僅針對使用 *AIOps for NGFW Premium* 授權的 *NGFW* 提供統一管理和操作。繼續使用 AIOps for NGFW Free 應用程式，將 *NGFW* 上線至 *AIOps for NGFW Free*。
軟體 **NGFW** 積分	對於由軟體 NGFW 積分資助的 VM-Series，Strata Cloud Manager 支援 AIOps for NGFW Premium 功能，包括 NGFW 的雲端管理。
Prisma Access	有兩種方式可以管理 Prisma Access：您可以使用 Strata Cloud Manager 或 Panorama。Strata Cloud Manager 提供 Prisma Access 可見性功能，無論您使用什麼管理介面，都支援這些功能。這表示，如果您使用 Panorama 來管理 Prisma Access，您仍可使用 Strata Cloud Manager 全面監控 Prisma Access 環境。 **Prisma Access (Managed by Strata Cloud Manager)** 使用 Strata Cloud Manager 對您的 Prisma Access 環境進行完整的上線、管理和監控。 其中包括使用 Strata Cloud Manager 管理和監控 Prisma Access 中包含的雲端交付安全服務。 Strata Cloud Manager 可讓您在 Prisma Access 環境中進行全方位的監控、警示和檢視：

 ©2025 Palo Alto Networks, Inc.

	• 採用 AI 技術的自發 DEM • 在 Strata Cloud Manager 中監控 Prisma Access • Strata Cloud Manager 儀表板 • Strata Cloud Manager 監控 • Strata Cloud Manager 報告 **Prisma Access (Managed by Panorama)** 如果您使用 Panorama 來管理 Prisma Access，則必須繼續使用 Panorama 管理您的環境。不過，您可以使用 Strata Cloud Manager 在 Prisma Access 環境中進行全方位的監控、警示和檢視： • 採用 AI 技術的自發 DEM • 在 Strata Cloud Manager 中監控 Prisma Access • Strata Cloud Manager 儀表板 • Strata Cloud Manager 監控 • Strata Cloud Manager 報告
採用 **AI** 技術的 **ADEM**	採用 AI 技術的 ADEM 是一個 Prisma Access 附加元件授權，可自動執行複雜的 IT 操作，以提高生產力並縮短解決問題所需的時間。Strata Cloud Manager 對所有的 Prisma Access 使用者（包括 Panorama 管理的 Prisma Access 和 Prisma Access 雲端管理）均支援採用 AI 技術的 ADEM。 如果您使用 *Panorama* 來管理 *Prisma Access*，則必須繼續使用 *Panorama* 管理您的環境，且可以使用 *Strata Cloud Manager* 進行 *ADEM* 監控。
Prisma SD-WAN	將 Strata Cloud Manager 用於 Prisma SD-WAN。Prisma SD-WAN 是一項雲端交付服務，可實作應用程式定義的自發 SD-WAN，協助您保護和連接分公司、資料中心和大型校園站台，而不會增加成本和複雜性。AppFabric 透過應用程式感知安全地連接您的站台，並且讓您自由使用任何 WAN、任何雲端來執行精簡型分支（來自雲端的安全性）解決方案。
雲端交付安全服務 **(CDSS)**： • 進階威脅防護 • **Advanced URL Filtering** 進階 **URL** 篩選 • 進階 **WildFire** • **DNS** 安全性 • 企業 **DLP** • **IoT Security**	如果您有 Prisma Access 或 AIOps for NGFW Premium 授權，則可以使用 Strata Cloud Manager 來管理和監控您的安全性訂閱。Strata Cloud Manager 提供您的安全性訂閱在整個企業流量中穩定提供的保護。 基於安全性訂閱提供給您的 Strata Cloud Manager 功能取決於您的授權，可包含： • Strata Cloud Manager 的安全性訂閱儀表板和報告 • Strata Cloud Manager 的安全性訂閱統一管理。如果您使用 Strata Cloud Manager 在 NGFW 和/或 Prisma Access 間強制

 ©2025 Palo Alto Networks, Inc.

• SaaS 安全性	執行共用安全性政策，您可以對安全性訂閱使用單一而集中的設定。

 ©2025 Palo Alto Networks, Inc.

Strata Cloud Manager 初始概覽

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目 • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

以下是 Strata Cloud Manager 的初始概覽。Strata Cloud Manager 使用者介面可讓您全方位檢視自己的網路，並提供統一的工作流程來管理 NGFW 和 SASE。透過簡化且一致的全新導覽與您所有的網路資料互動，獲得為您自動呈現的可操作洞察，並共同管理及監控 Prisma Access、NGFW 和雲端交付安全服務。

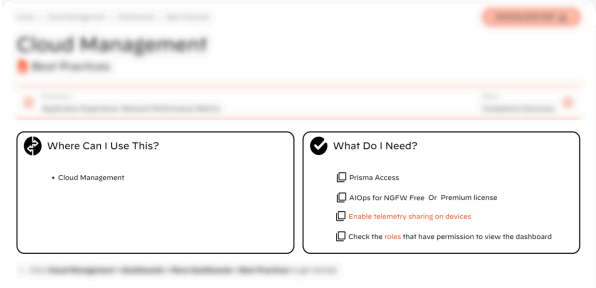
探索左側導覽列上的每個功能表 - 這些路徑現在是與 Strata Cloud Manager 搭配使用的任何 Palo Alto Networks 產品或訂閱的標準。這讓您得以輕鬆地：

- 採用新的功能和訂閱
- 上線新的使用者、裝置、站台或位置

因為它們將直接融入您現有的管理設定中。

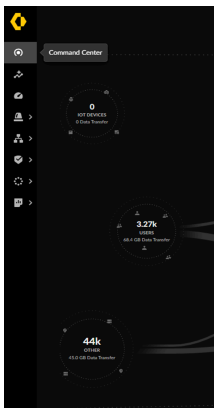
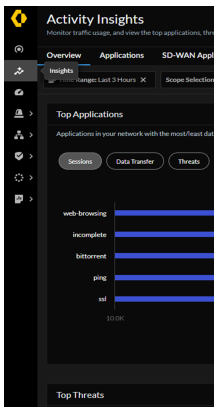
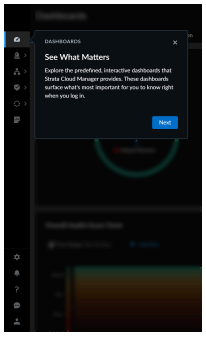
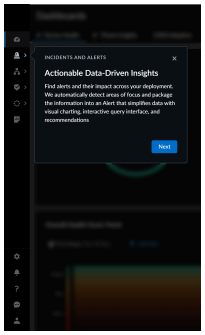
重要

您可以在 *Strata Cloud Manager* 中使用的功能取決於您的訂閱。您可以檢閱 *Strata Cloud Manager* 文件，以查看 *Strata Cloud Manager* 功能的任何授權需求。

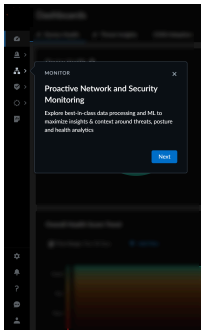
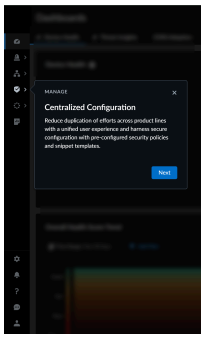
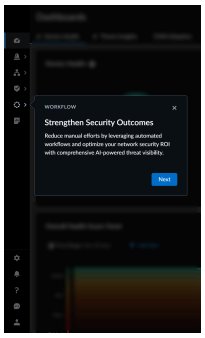


 ©2025 Palo Alto Networks, Inc.

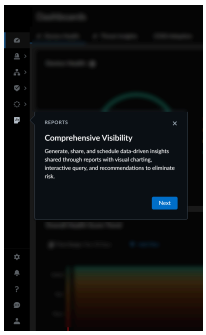
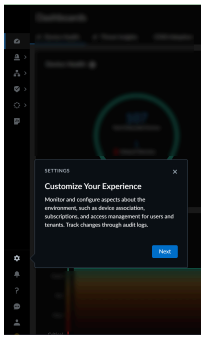
表 **2:**

控管中心	您評估網路的健康情況、安全性和效率的第一站 控管中心是您的網路和安全性基礎架構的視覺化概要。其中提供四種不同的檢視，分別有其本身的追蹤資料、指標和可操作洞察，可供檢查和互動。 • 控管中心：Strata Cloud Manager	
活動洞察	統一的網路資料，全部集中在一處 活動洞察可讓您深入檢視 Prisma Access 與 NGFW 部署間的網路活動。活動洞察將網路流量、應用程式使用情況、威脅和使用者活動等網路資料統整到同一處。 • 洞察：活動洞察	
儀表板	立即查看重要事項 當您登入時，儀表板會隨即顯示您需要瞭解的重要內容。每個儀表板都會突顯您可以採取行動以改善安全性狀態或網路健康情況的領域。 探索所有預先定義的隨附互動式儀表板，您可以釘選「我的最愛」。 • 儀表板：Strata Cloud Manager	
事件和警示	可操作的資料驅動洞察 Strata Cloud Manager 提供統一的事件和警示架構。在同一處檢視、調查和解決網路上的警示與事件，以及跳至日誌查看相關聯的活動。 • 事件和警示：Strata Cloud Manager	

 ©2025 Palo Alto Networks, Inc.

監控	主動網路和安全性監控 監控網路上所有項目的健康情況和安全性，並使用 IoC 搜尋來調查網路上構件的歷程記錄，並檢閱全域分析結果。根據您所使用的訂閱和產品，您可以監控： • NGFW 裝置 • Prisma Access • 應用程式 • 使用者 • 分支站台 • 資料中心 • 網路服務（例如 GlobalProtect 和 DNS） • 您的 Palo Alto Networks 訂閱 • 您的 Prisma Access 位置 • Prisma SD-WAN • 資產	
管理	集中設定 管理網路安全性產品和訂閱的共用政策；第一天，您可以根據預先定義的最佳做法政策和設定以及內嵌最佳做法檢查，進行安全性設定。 • 管理：NGFW 和 Prisma Access • 管理：IoT 政策建議 • 管理：企業 DLP • 管理：SaaS 安全性	
工作流程	強化安全成果 當您首次導覽至工作流程時，**Discovery**（探索）儀表板會在有關鍵和建議的動作可供您執行以改善安全性狀態或最佳化設定管理時，立即加以顯示。繼續在此處設定及上線 NGFW 和 Prisma Access 行動使用者與遠端網路，並規劃 NGFW 的軟體升級。 • 設定 Prisma Access	

 ©2025 Palo Alto Networks, Inc.

	• 設定 NGFW • 軟體升級規劃工具 (AIOps for NGFW)	
報告	全面的可見性 產生、共用和排程透過具有視覺化圖表、互動式查詢和建議的報告共用的資料驅動洞察，用以消除風險。 • 報告：Strata Cloud Manager	
設定	上線和啟動設定 當您新增使用者、授權或管理員時，甚至當您自己開始使用 Strata Cloud Manager 時，您就會回到這些設定： • 訂閱 • 租用戶 • 裝置關聯 • 識別與存取 • 稽核日誌	

 ©2025 Palo Alto Networks, Inc.

啟動 Strata Cloud Manager

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目 • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

Strata Cloud Manager 應用程式可從 Palo Alto Networks 中樞取得，您也可以直接透過 stratacloudmanager.paloaltonetworks.com 加以存取。

Prisma Access 授權、AIOps for NGFW Premium 授權或 Prisma SD-WAN 授權是 Strata Cloud Manager 統一管理和操作的基本需求。如果您至少擁有其中一個授權，即可存取 Strata Cloud Manager 以瞭解或管理您的產品。

如果您擁有以上多個授權，Strata Cloud Manager 會為您提供可與這些產品互動的單一介面，以及其他授權或附加元件訂閱（例如，您的 Palo Alto Networks 安全性訂閱）。→ 查看有哪些產品和授權支援 *Strata Cloud Manager* 統一管理和操作

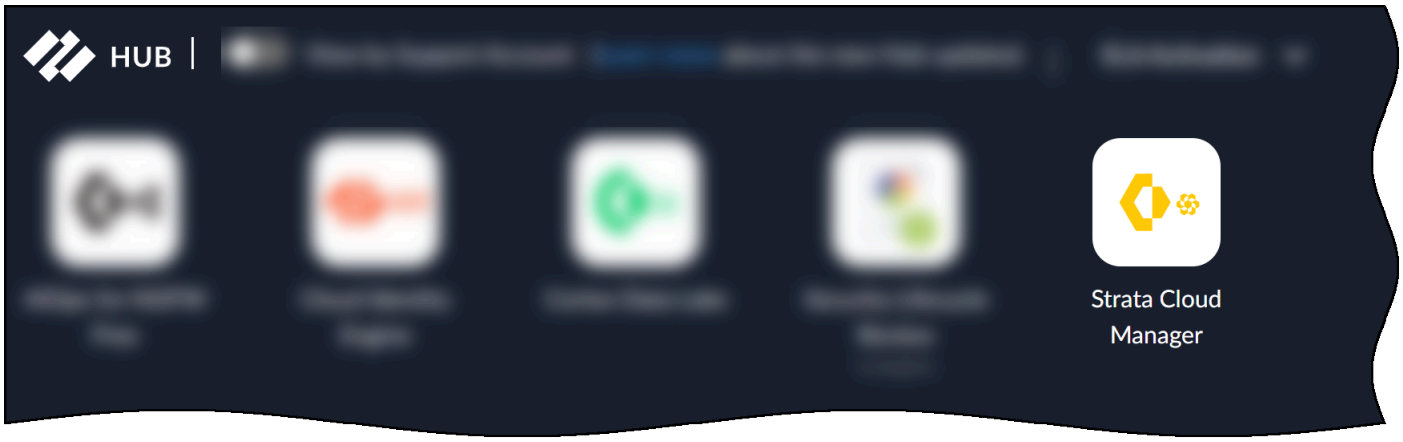
若要啟動或存取 **Strata Cloud Manager**：

- 如果您是在 2023 年 10 月或之後首次接觸 Prisma Access、AIOps for NGFW Premium 或 Prisma SD-WAN，此處說明如何 首次啟動 Strata Cloud Manager
- 如果您先前曾使用中樞上個別的獨立應用程式來管理產品，此處詳細說明如何 從專用產品應用程式移轉至 Strata Cloud Manager

首次啟動 Strata Cloud Manager

啟動 Prisma Access、AIOps for NGFW Premium 或 Prisma SD-WAN 授權後，您將可在 Palo Alto Networks 中樞取得 Strata Cloud Manager 應用程式，或者，您可以直接經由 stratacloudmanager.paloaltonetworks.com 加以存取。

©2025 Palo Alto Networks, Inc.



啟動應用程式並 Strata Cloud Manager 初始概覽。接著，將您的產品上線：

- 開始使用 AIOps for NGFW Premium，包括 NGFW 的雲端管理
- 開始使用 Prisma Access
- 開始使用 Prisma SD-WAN

從專用產品應用程式移轉至 Strata Cloud Manager

重要

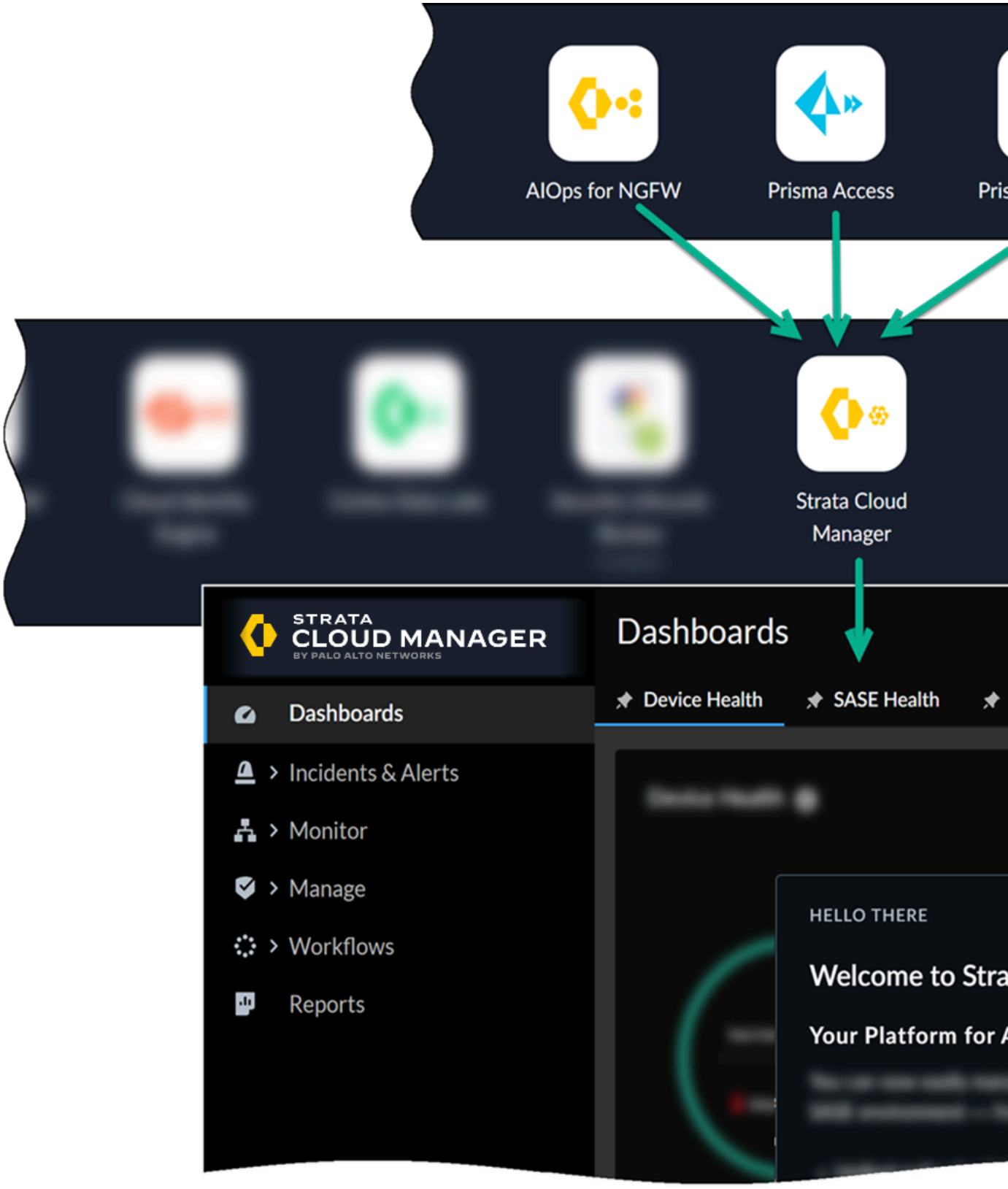
只有在您先前使用獨立應用程式來管理產品或與其互動時，才適用這些資訊：*Prisma Access* 應用程式、*AIOps for NGFW Premium* 應用程式或 *Prisma SD-WAN* 應用程式。這些應用程式已更新（或即將更新），為您提供 *Strata Cloud Manager* 統一管理和操作的功能。

從專用產品應用程式移轉至 **Strata Cloud Manager** 時會發生什麼情況：

- Strata Cloud Manager 會根據授權支援提供統一管理和操作 - 以下是您可以使用 Strata Cloud Manager 監控或管理的產品。
- 產品內通知將提前讓您知道有更新即將推出，為您提供 Strata Cloud Manager。
- 更新會無縫進行，不影響您的資料、警示或資產。

©2025 Palo Alto Networks, Inc.

- 更新完成後，您將登入中樞上的 Strata Cloud Manager 應用程式；您將不再使用中樞上 Prisma Access、AIOps for NGFW Premium 或 Prisma SD-WAN 的個別應用程式。



 ©2025 Palo Alto Networks, Inc.

- 您的產品應用程式會自動將您重新導向至 stratacloudmanager.paloaltonetworks.com。這是 Strata Cloud Manager URL。

  如果您先前使用多個為 *Strata Cloud Manager* 更新的產品應用程式，則更新後的產品應用程式將全部重新導向至相同的 *Strata Cloud Manager* 執行個體。
- Strata Cloud Manager 會為您提供跨網路安全性產品通用的全新導覽。搶先看看 Strata Cloud Manager，並探索新的導覽體驗和功能。
- 在新的統一管理介面中尋找您的產品功能：
  - AIOps for NGFW：功能在 Strata Cloud Manager 中位於何處？
  - Prisma SD-WAN：功能在 Strata Cloud Manager 中位於何處？
  - Prisma Access 洞察：功能在 Strata Cloud Manager 中位於何處？
  - Prisma Access：功能在 Strata Cloud Manager 中位於何處？

©2025 Palo Alto Networks, Inc.

開始使用 Strata Cloud Manager

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目 • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

Strata Cloud Manager 可讓您對 NGFW 和 SASE 網路進行採用 AI 技術的統一管理和操作。以下是首次使用 Strata Cloud Manager 的備忘錄。

如果您打算使用 Strata Cloud Manager 上線並管理 Prisma Access 和（或）NGFW（需要 AIOps for NGFW Premium），這項資源包含您開始使用 Prisma Access 和 NGFW 的共用管理 時所需的知識

❑ （在中樞）啟動您的授權

購買授權後，您會收到一則包含啟動連結的電子郵件。此連結會在中樞啟動引導式工作流程；請依照您要啟動的每個授權的啟動工作流程操作：

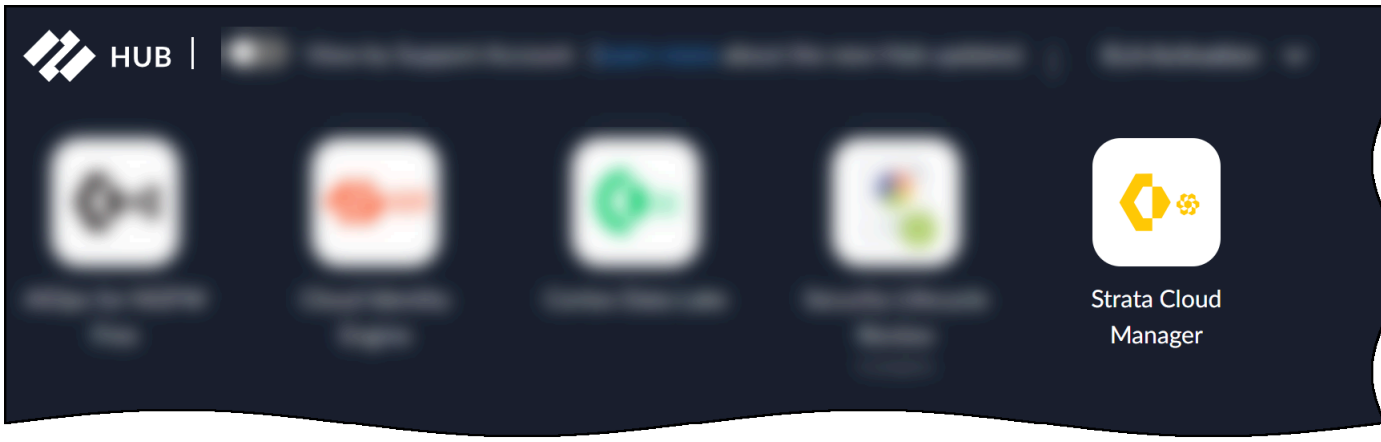
- AIOps for NGFW Premium 授權
- 啟動 Prisma Access 授權
- Prisma SD-WAN

啟動其中任一授權均可啟用 Strata Cloud Manager。啟動至少其中一個授權後，請繼續啟動任何其他授權或附加元件訂閱。

©2025 Palo Alto Networks, Inc.

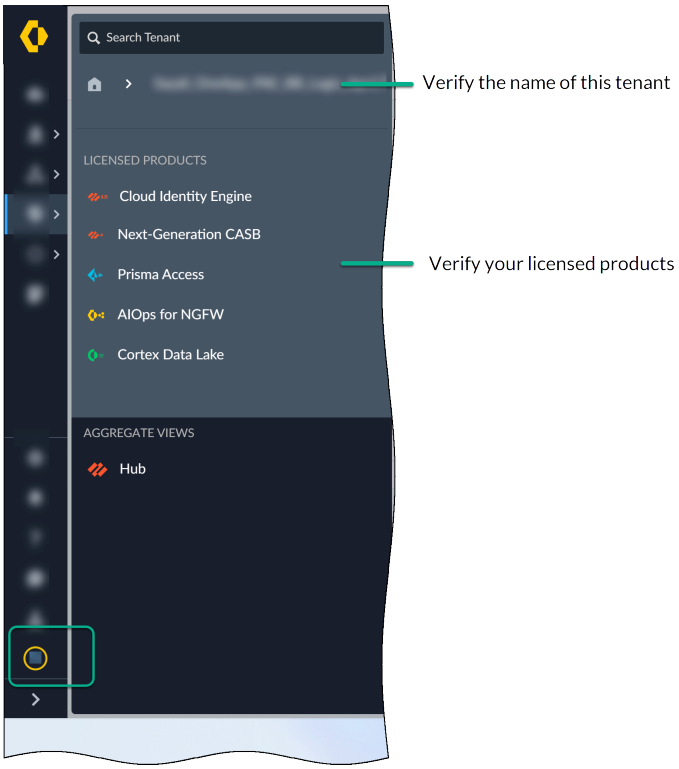
- 啟動 **Strata Cloud Manager**

  啟動 Prisma Access、AIOps for NGFW Premium 或 Prisma SD-WAN 授權後，您將可在 Palo Alto Networks 中樞取得 Strata Cloud Manager 應用程式，或者，您可以直接經由 stratacloudmanager.paloaltonetworks.com 加以存取。



 ©2025 Palo Alto Networks, Inc.

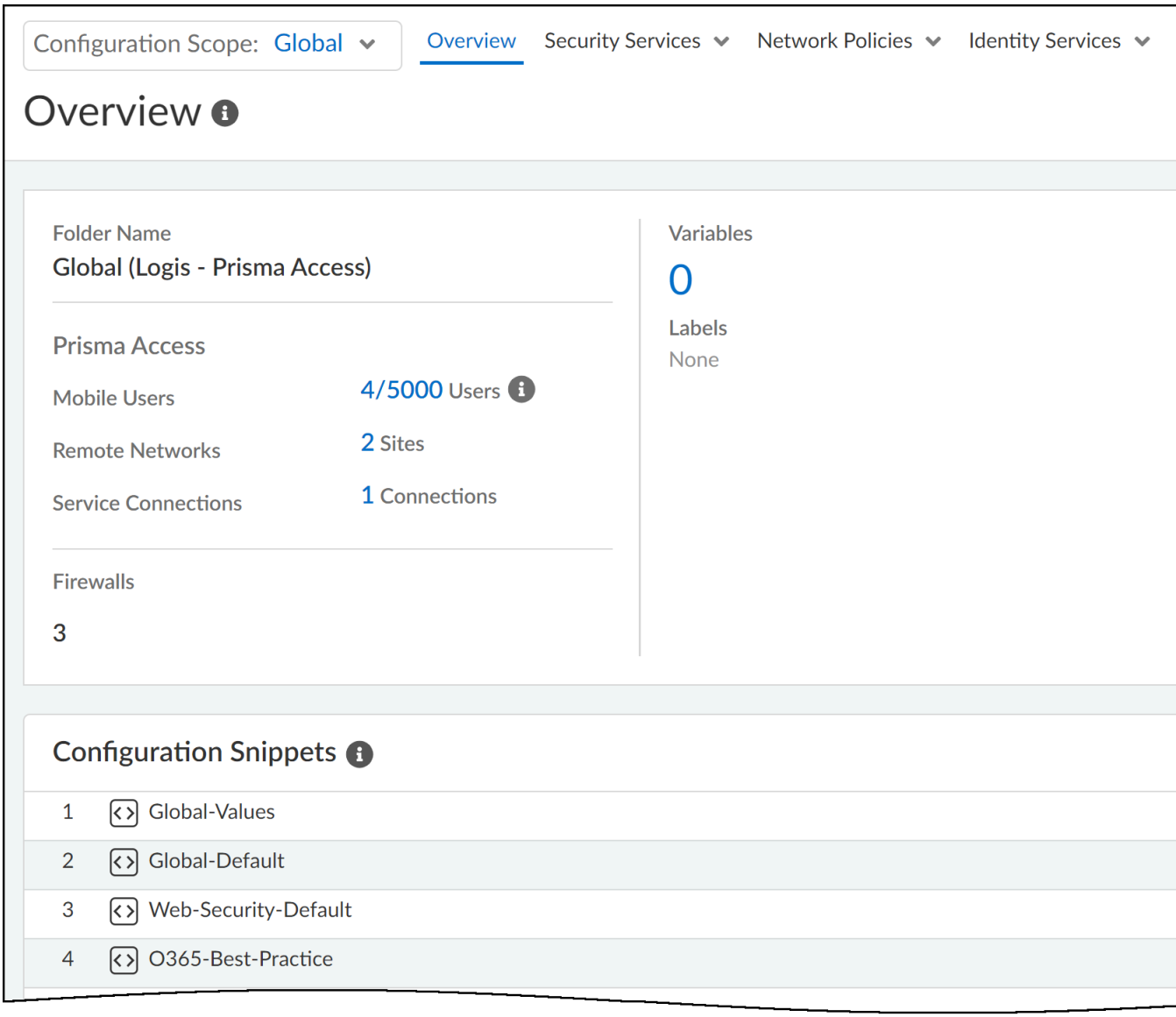
- 驗證您的授權
  - 在導覽功能表底部，選取您的租用戶詳細資料，並驗證您所使用的租用戶名稱，以及您的授權產品。以下是關於租用戶和訂閱管理的詳細資訊。



  - 移至**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**）檢查您的 Prisma Access 授權狀態和詳細資料，並查看是否有其他可用的詳細資料。

    如果您尚未將 *NGFW* 上線，或您的 *Prisma Access* 環境仍在佈建中，您可能在此處看不到太多資料。若是如此，請在完成此處的其餘步驟後儘快回來查看。

©2025 Palo Alto Networks, Inc.



- **Strata Cloud Manager** 的監控和可見性
  - 使用控管中心探索網路和安全性基礎架構的視覺化呈現。
  - 在活動洞察中檢閱重要的網路資料。
  - 探索您可以使用的 Strata Cloud Manager 儀表板。許多儀表板也支援可由您排程或與利害關係人共用的報告。
  - 監控您的 Prisma Access 環境、Prisma SD-WAN 和 NGFW。
  - 檢閱 Prisma Access、NGFW 和 Prisma SD-WAN 間的事件和警示。
- 內嵌最佳做法建議和工作流程

  進一步瞭解直接內建於 Strata Cloud Manager 的最佳做法指引和自動化。

©2025 Palo Alto Networks, Inc.

- **Strata Cloud Manager** 上線設定

  Strata Cloud Manager 會將常用服務彙整在 **Settings**（設定）功能表中。移至 **Settings**（設定）以管理：

  - 角色和權限 – 進一步瞭解 Strata Cloud Manager 上的可用角色和相關聯的權限。
  - 裝置關聯 – 將支援的雲端應用程式與您的裝置產生關聯。
  - 租用戶管理 – 建立及管理業務組織和單位的階層（由租用戶代表）。

Prisma Access 和 NGFW 的共用管理

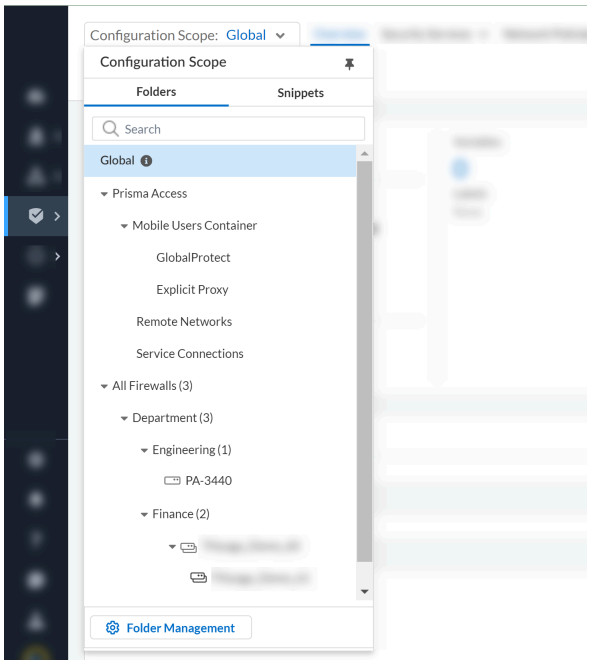
對於 Prisma Access 和 NGFW， Strata Cloud Manager 提供共用管理；將 NGFW 和 Prisma Access 使用者、遠端網路和服務連線上線至 Strata Cloud Manager， 並強制執行通用的安全性政策。

- 將 **NGFW** 和 **Prisma Access** 上線至 **Strata Cloud Manager**
  - 設定 Prisma Access， 並上線行動使用者、遠端網路和服務連線：
    - 設定 Prisma Access 服務基礎架構
    - 設定 Prisma Access 行動使用者， 包括 GlobalProtect 和明確 Proxy 連線
    - 設定 Prisma Access 遠端網路
    - 設定 Prisma Access 服務連線
  - 上線並設定 NGFW：
    - NGFW 雲端管理的上線和設定

 ©2025 Palo Alto Networks, Inc.

組織您的設定

在處理 Strata Cloud Manager 組態設定時，目前的 管理：設定範圍 一律會顯示，且您可以切換檢視以管理更廣泛或更精細的設定。設定範圍可讓您全域套用政策，或為特定 NGFW 或 Prisma Access 部署提供針對性的強制執行。



以下進一步說明如何開始組織您的 Strata Cloud Manager 設定：

- 工作流程：資料夾管理

  使用資料夾對 NGFW 進行邏輯分組，以簡化設定管理。Prisma Access 資料夾會根據部署類型預先定義。您也可以在資料夾層級啟用 Web 安全性（以簡化管理員對網際網路和 SaaS 應用程式存取進行管理的體驗）。

- 管理：片段

  使用片段對設定進行分組，讓您能夠將其快速推送至 NGFW 或 Prisma Access 部署。

- 管理：變數

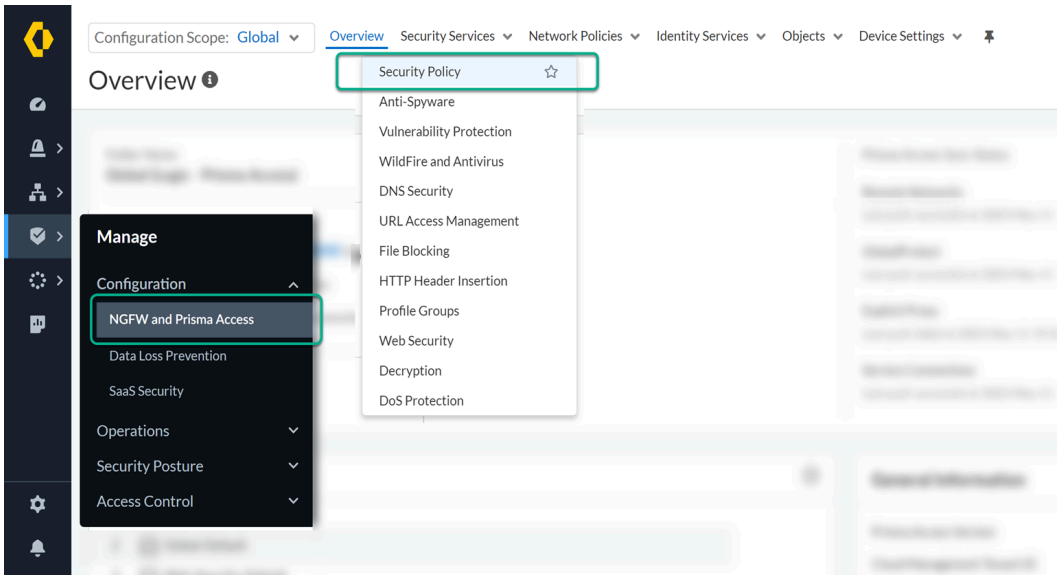
  在設定中使用變數，以因應裝置或部署的特定設定物件。

©2025 Palo Alto Networks, Inc.

- **NGFW** 和 **Prisma Access** 的共用安全性政策

  Strata Cloud Manager 為您提供 Prisma Access 和 NGFW 的統一管理。你的 Strata Cloud Managervsecurity 政策是共用的，您可將其全域套用至 Prisma Access 和 NGFW，或將特定設定的目標定為 Prisma Access 部署或特定防火牆群組。

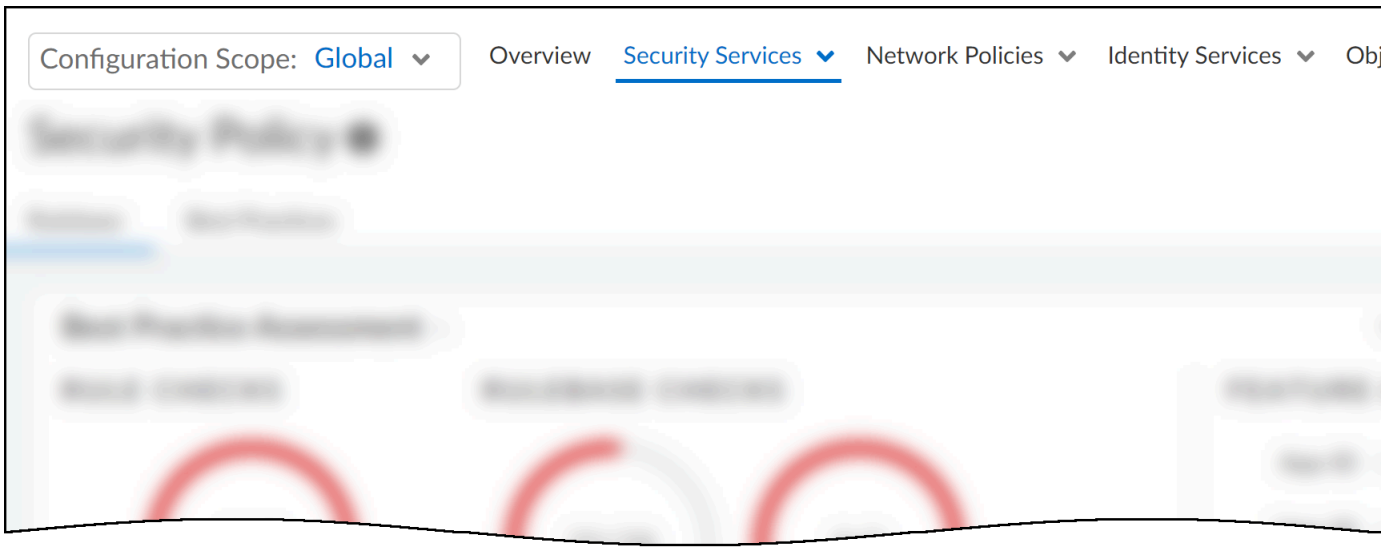
  首先，移至**Manage**（管理）**> Configuration**（設定）**> NGFW and Prisma Access**（**NGFW 和 Prisma Access**）。



 ©2025 Palo Alto Networks, Inc.

- 將設定變更推送至 **NGFW** 和 **Prisma Access**

  在管理你的 Strata Cloud Manager 設定時，選取 **Push Config**（推送設定），將設定變更推送至 NGFW 和 Prisma Access：



  系統會提示您根據資料夾設定「設定推送」的範圍。以下進一步說明如何：

  - 推送您的設定變更
  - 檢閱設定推送的狀態
  - 查看如何清除您的設定

©2025 Palo Alto Networks, Inc.

Strata Cloud Manager 中的內建最佳做法

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目 • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

Palo Alto Networks 最佳做法旨在協助您簡化網路基礎架構的合規性檢查程序，藉以獲得最安全的網路。我們直接在 Strata Cloud Manager 中建置了最佳做法檢查，以便您可以即時評估設定。請遵循最佳做法以加強安全性狀態。您可以利用 Strata Cloud Manager，根據最佳做法評估您的 Panorama、NGFW 和 Panorama 管理的 Prisma Access 安全性設定，並修復失敗的最佳做法檢查。

最佳做法指引旨在協助您增強安全性狀態，同時協助您有效管理環境，並盡可能提高使用者工作效率。根據這些內嵌檢查持續評估您的設定，並且在發現有機會可提高安全性時立即採取行動。

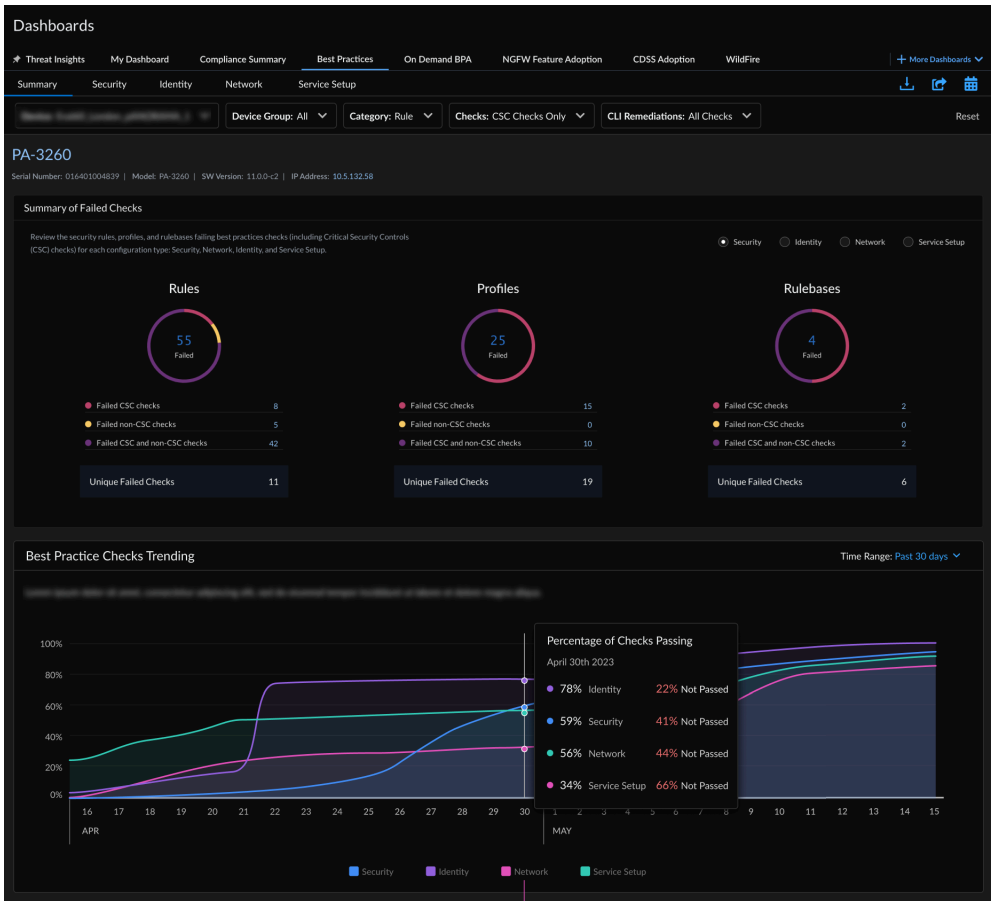
檢視最佳做法的採用和合規性

首先，您可以透過檢查以下安全性狀態儀表板，以快速評估整體安全性狀態。

瞭解您大致上的表現，並指出您可以從哪些領域開始著手。

©2025 Palo Alto Networks, Inc.

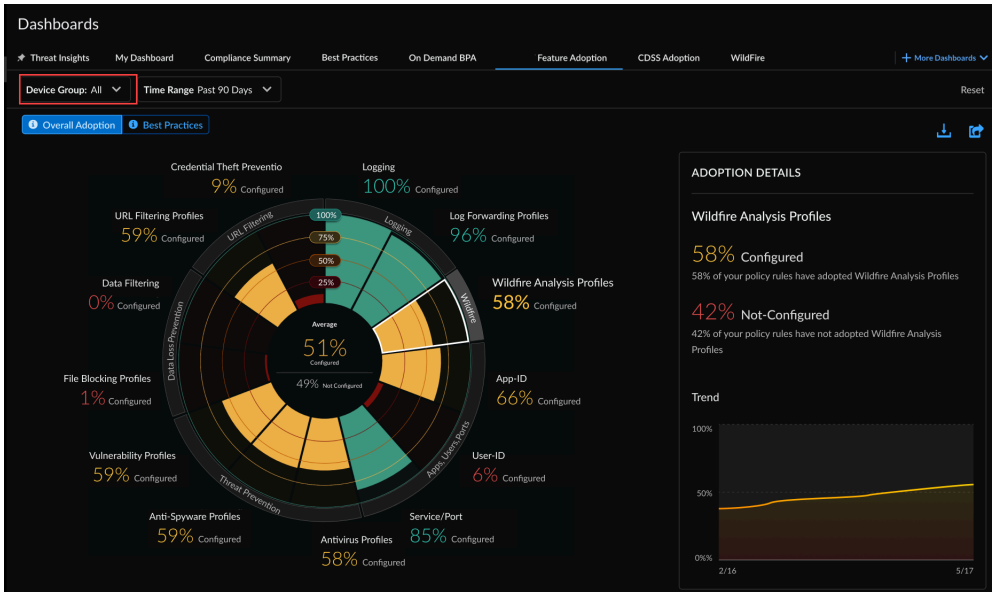
- 在 儀表板：最佳做法 儀表板中查看每日最佳做法報告，及其與 Center for Internet Security 的重大安全性控制 (CSC) 檢查的對應，以利確認哪些領域可進行變更以提高最佳做法合規性。以 PDF 格式共用最佳做法報告，並將其排程為定期發送到您的收件匣。



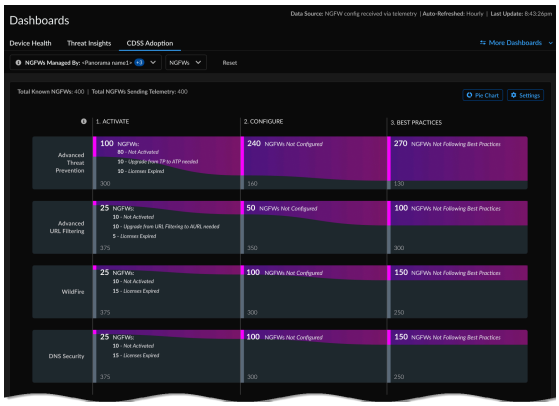
- 檢查合規性摘要儀表板，檢視安全性檢查在過去 12 個月內進行變更的歷程記錄；Center for Internet Security (CIS) 和美國國家標準技術研究所 (NIST) 架構會將這些內容分門別類。

 ©2025 Palo Alto Networks, Inc.

- 監控 儀表板：功能採用 並隨時瞭解您在部署中使用的安全功能，以及覆蓋範圍中的潛在差距。



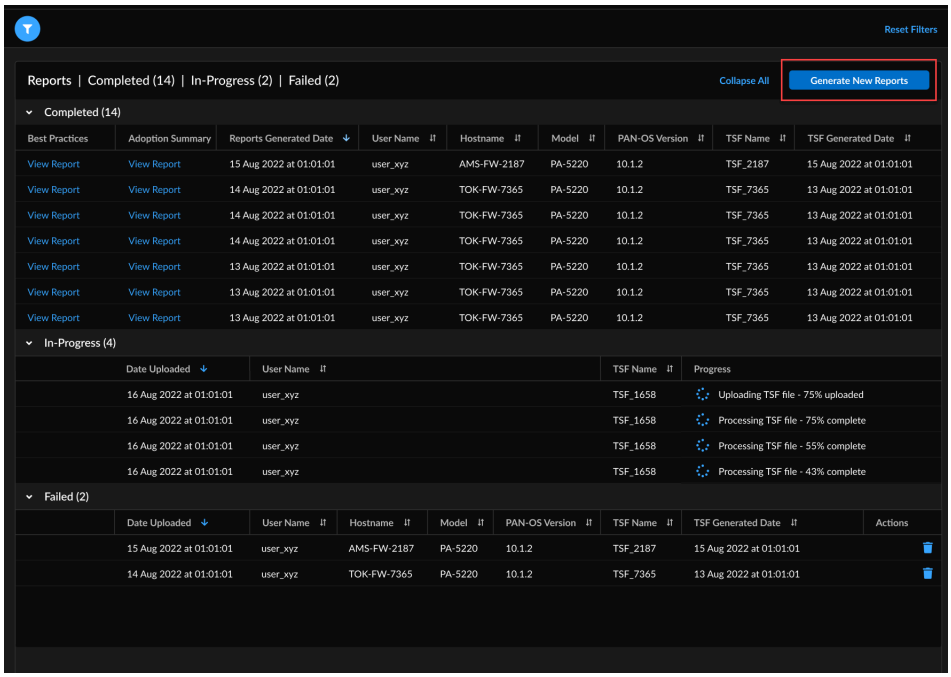
- 監控 儀表板：CDSS 採用 - 檢視裝置中的安全服務或功能訂閱及其授權使用情況，以識別安全漏洞並強化企業的安全性狀態。



- 透過 儀表板：安全性狀態洞察，根據已上線 NGFW 裝置的安全性狀態深入瞭解部署的安全性狀態和趨勢，並且在事件發生時或安全性設定可能需要仔細檢查時收到警示。

 ©2025 Palo Alto Networks, Inc.

- 為執行版本 9.1 及更高版本的（非遙測）PAN-OS 裝置產生 BPA 報告（現在包括功能採用指標）。



加強安全性狀態的最佳做法工具

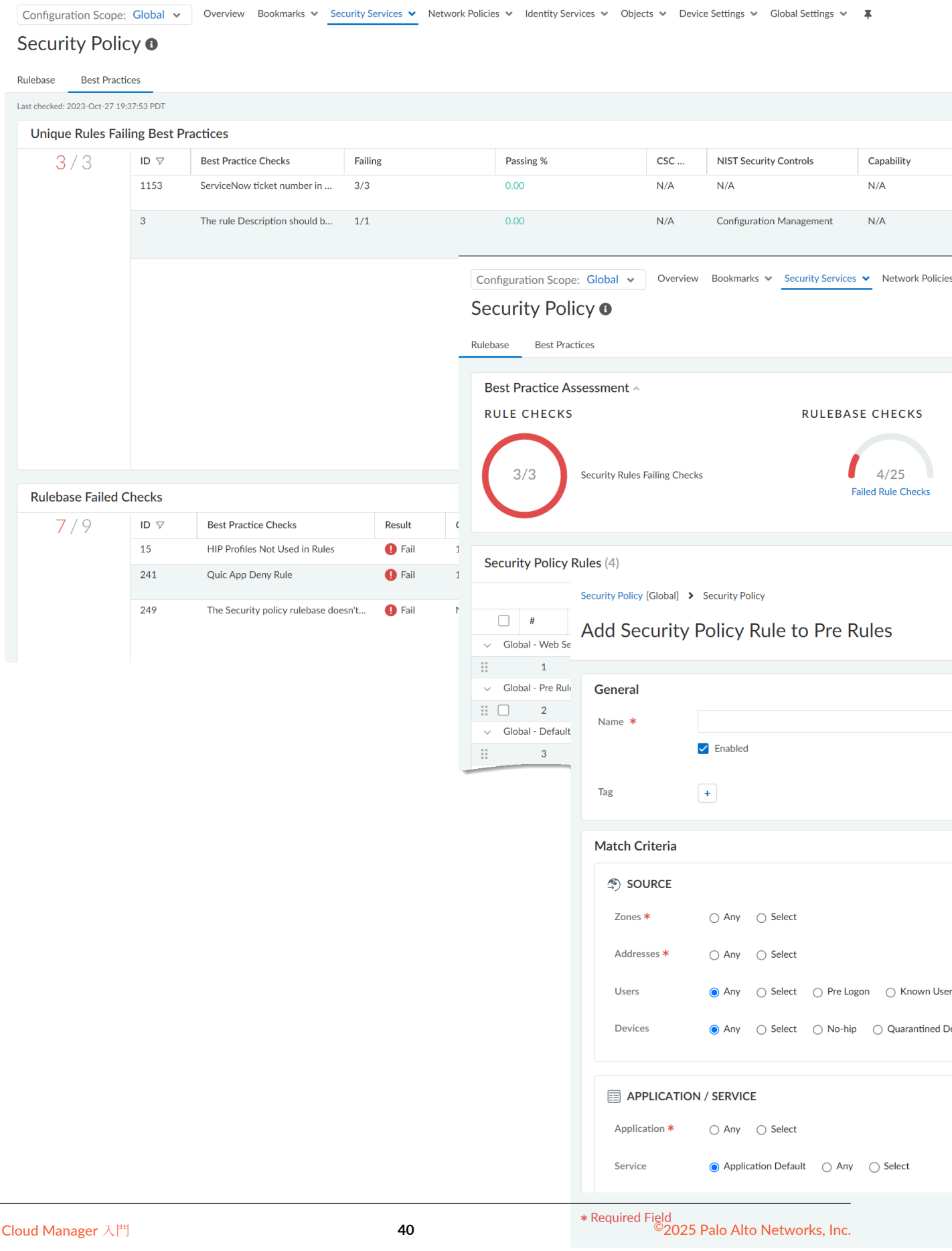
尋找可協助您改善安全性狀態的工具集合。

- 為您的部署自訂安全性狀態檢查，以盡可能在 管理：安全性狀態設定 中提供相關建議
- 使用設定清理來識別及移除未使用的設定物件和政策規則。
- 設定政策最佳化工具設定，以完善和最佳化過於寬鬆的安全性規則，使其僅允許在您的網路中實際使用的應用程式。
- 建立您自己的合規性檢查 – 自訂現有的最佳做法檢查，並建立及管理特殊豁免，以妥善因應組織的業務需求。
- 使用政策分析器可快速確保您對安全性政策規則所做的更新會符合您的需求，並且不會產生錯誤或設定有誤（例如導致規則重複或衝突的變更）。

即時的內嵌最佳做法設定檢查

最佳做法指引旨在協助您增強安全性狀態，同時協助您有效管理環境，並盡可能提高使用者工作效率。根據這些內嵌檢查持續評估您的設定，並且在發現有機會可提高安全性時立即採取行動。

 ©2025 Palo Alto Networks, Inc.



©2025 Palo Alto Networks, Inc.

- 最佳做法分數

  最佳做法分數會顯示在功能儀表板上（例如安全性政策、解密或 URL 存取控制）。這些分數可以讓您快速檢視最佳做法進度。您可以迅速識別需要進一步調查的領域，或您想要採取措施以改善安全性狀態的部分。

- 最佳做法實地檢查

  實地檢查可確切指出您的設定與最佳做法不符之處。最佳做法指引是內嵌提供的，因此您可以立即採取行動。

- 最佳做法評估

  在此，您可以全方位檢視您的功能實作是否符合最佳做法。檢查失敗的檢查，以瞭解可改進之處（您也可以檢閱通過的檢查）。規則庫檢查可突顯您可以在個別規則外進行的設定變更，例如，對跨數個規則使用的政策物件進行的變更。

最佳做法檢查適用於：

- 安全性政策規則庫

  規則庫檢查會查看安全性政策的組織和管理方式，包括套用於多個規則的組態設定。

- 安全性規則
- 安全性設定檔
  - 反間諜軟體
  - 漏洞保護
  - WildFire 和 Antivirus
  - URL 存取管理
  - DNS 安全性
- 驗證
- 解密
- **GlobalProtect**

想進一步瞭解 ***Palo Alto Networks*** 最佳做法嗎？

這是最佳做法首頁，此處提供可協助您轉移至最佳做法並予以實作的資源。

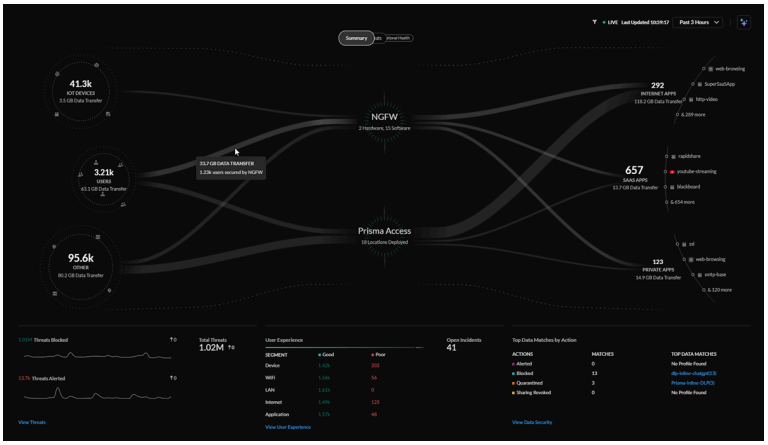
©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

控管中心：Strata Cloud Manager

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目 • Prisma SD-WAN	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro ❑ Strata Cloud Manager Essentials ❑ Prisma SD-WAN 存取控管中心所需的其他授權和先決條件： ❑ Strata Logging Service ❑ 在控管中心用來檢視特定指標的特定授權（如下所述） ❑ 有權檢視控管中心的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

Strata Cloud Manager 控管中心是您的新 NetSec 首頁；這是一個互動式視覺摘要，可協助您評估網路的健康情況、安全性和效率。控管中心提供 NetSec 平台的整合檢視，讓您可在單一位置全方位檢視您的來源、應用程式、Prisma Access 部署、NGFW 和安全服務。



控管中心可讓您與資料互動並視覺化網路上各事件之間的關係，以便您立即採取行動以增強安全性。

控管中心可與新的活動洞察儀表板 **(Insights**（洞察） **> Activity Insights**（活動洞察）**)**整合，且會透過可操作的洞察醒目提示已上線的授權和訂閱所偵測到的異常，並提供修復這些異常的路徑。

在新的首頁中，您可以：

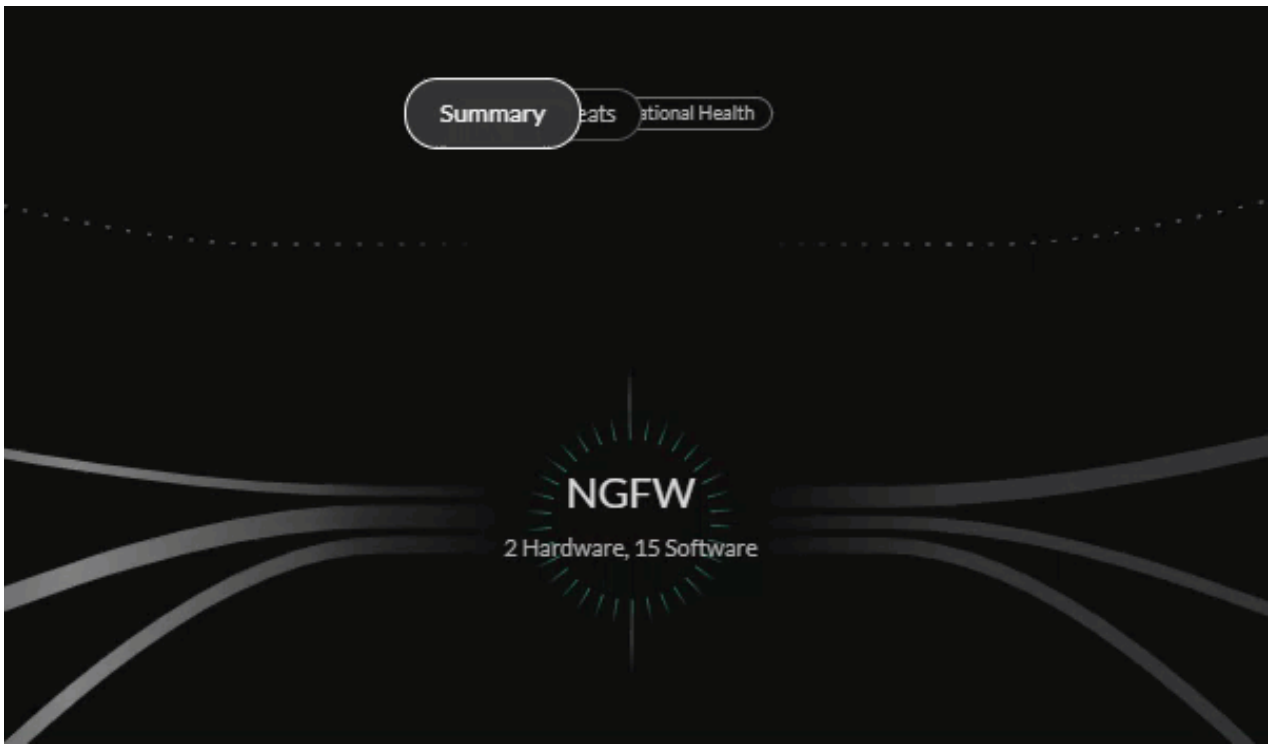
- 全方位檢視您的網路上從來源（使用者、IoT、外部主機）流向應用程式（網際網路、SaaS、私人）的所有流量。
- 瞭解存取和保護使用者、裝置和應用程式等資產的方式。
- 導覽至具有內容的特定儀表板，以深入地瞭解對網路造成影響的問題。
- 使用者在工作時遇到的威脅類型。

首先，啟動 Strata Cloud Manager 並按一下 **Command Center**（控管中心）（ ）。

 ©2025 Palo Alto Networks, Inc.

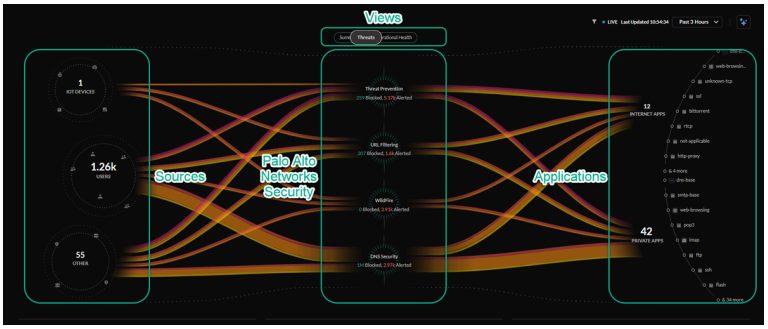
如何與 Strata Cloud Manager 控管中心互動

控管中心的各個檢視會將您評估網路健康情況和安全性所需的所有資訊分門別類。



控管中心的資料每 5 分鐘會重新整理一次，且依預設會顯示最近 24 小時的資料。您也可以按過去 1 小時、3 小時、7 天或 30 天篩選這項資料。

每個控管中心檢視分別顯示不同類型的視覺化資料，這些資料從來源流經 Prisma Access 和 NGFW 或部署在網路上的安全性訂閱，最終前往網路上的各種應用程式。



來源泡泡（混合式工作者、辦公室使用者、IoT 裝置等等）位於左側，應用程式泡泡（透過網際網路、SaaS 存取，並託管於內部部署或雲端中）位於右側。應用程式泡泡會顯示每個類別中最常用的三個應用程式。

來源包括：

- **IoT** 裝置 – 由作用中 IoT Security 授權探索到並啟用的裝置。
- 使用者 – 遠端和分支使用者。

 ©2025 Palo Alto Networks, Inc.

- 其他 – 透過網際網路存取資源的內部和外部主機。

應用程式包括：

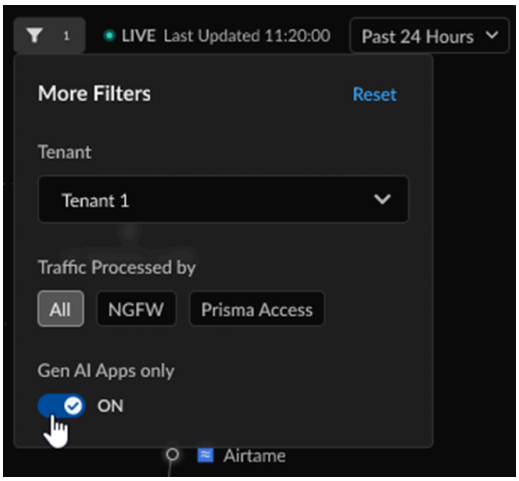
- 網際網路應用程式 – 使用網頁瀏覽器存取的應用程式。
- **SaaS** 應用程式 – 由應用程式服務提供者擁有和管理的雲端應用程式。
- 私人應用程式 – 託管於資料中心的應用程式。

按一下來源、部署或應用程式的泡泡，可篩選中央檢視中的資料。這將可讓您深入檢視與所選泡泡相關的追蹤資料。

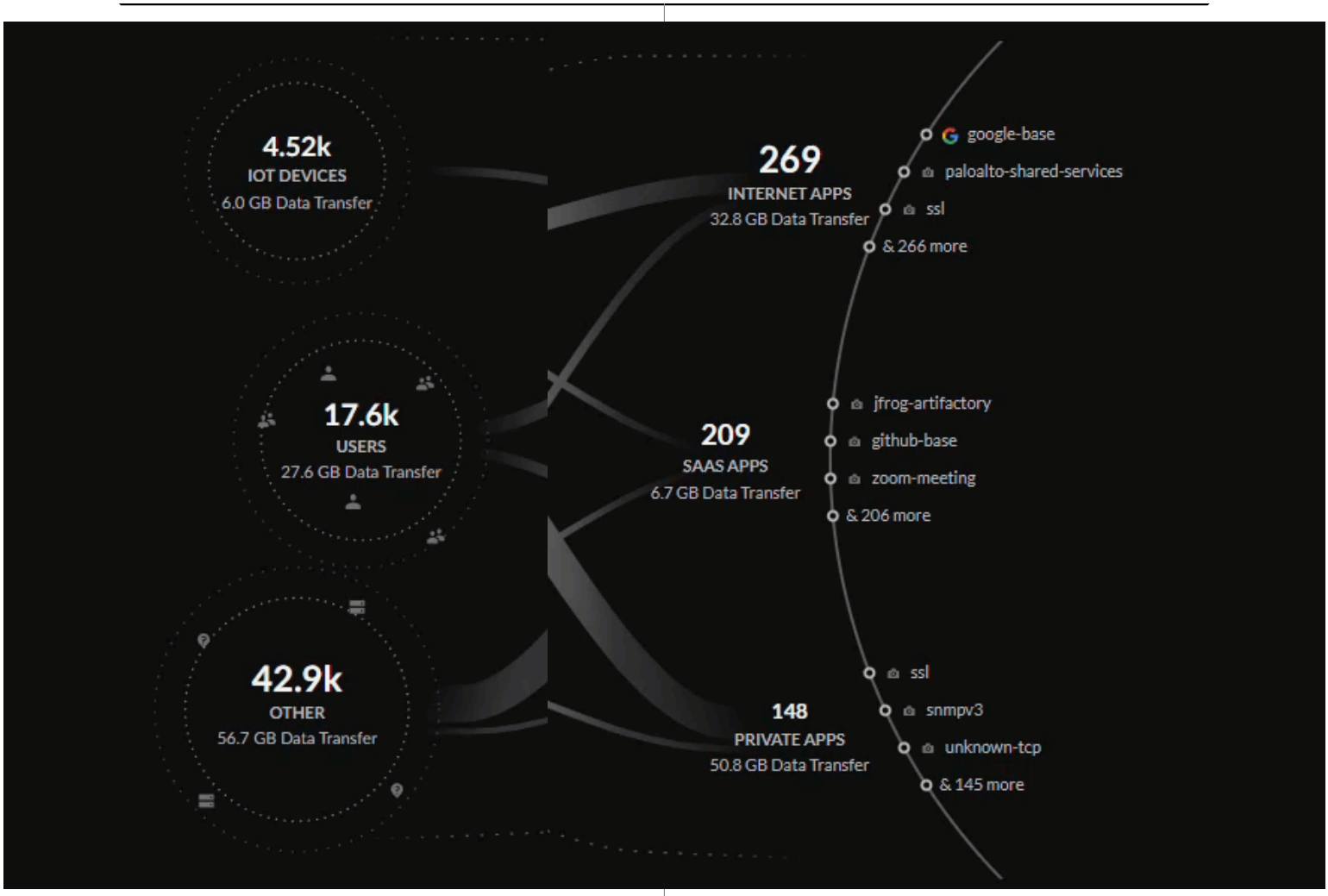
藉由選取篩選器 ( )，您可以按 **Tenant**（租用戶）或 **NGFW** 或 **Prisma Access** 特定資料來篩選控管中心檢視中的資料。

透過 AI Access 授權，您可以用 **GenAI Apps only**（僅限 **GenAI** 應用程式）來篩選所有控管中心檢視中的流量，以妥善評估使用者在您的網路上使用的 GenAI 應用程式對資料安全性可能有何影響。

如需 *AI* 存取安全性和 *AI* 存取安全性授權的詳細資訊，請按一下這裡。

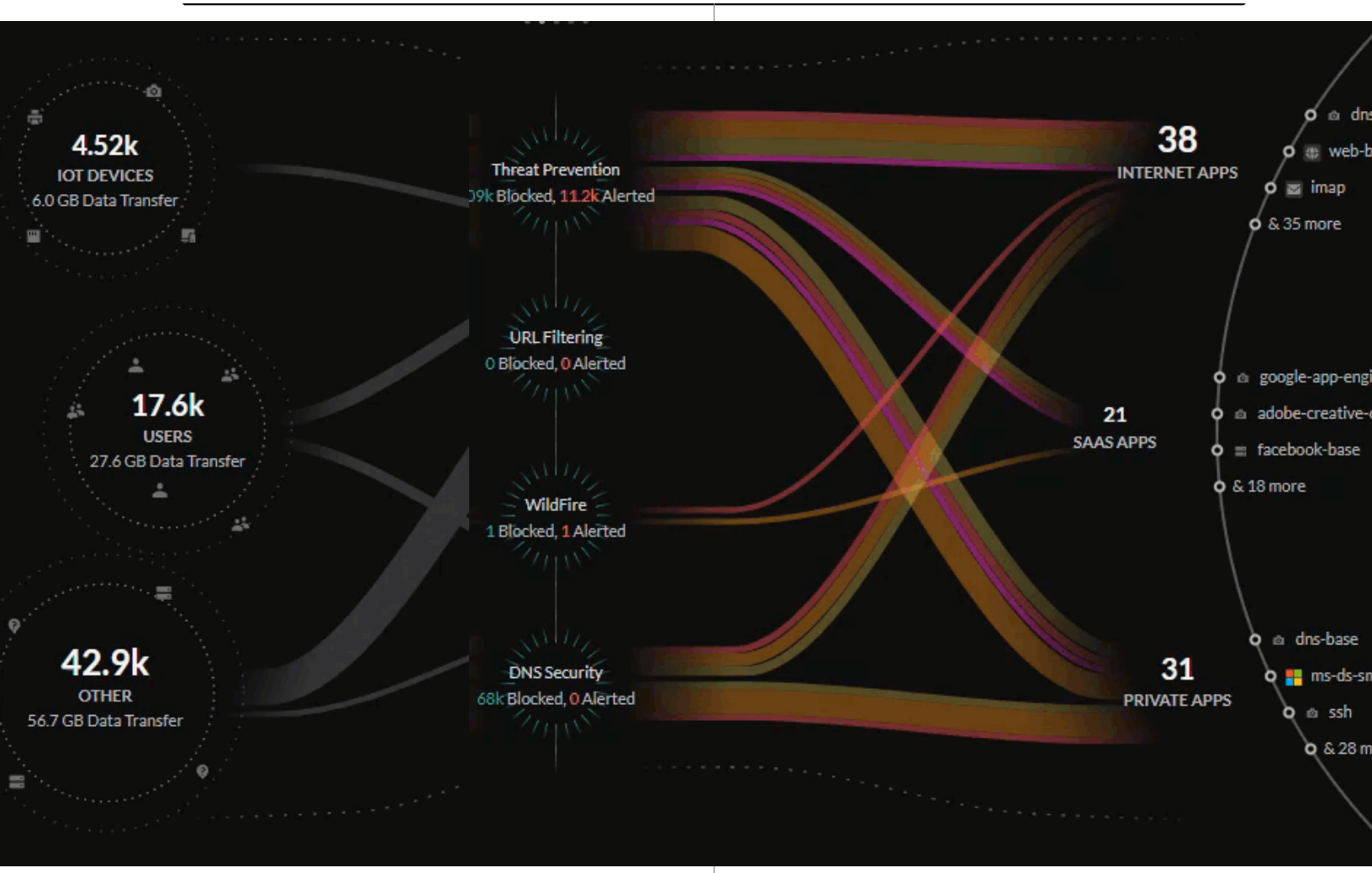


 ©2025 Palo Alto Networks, Inc.

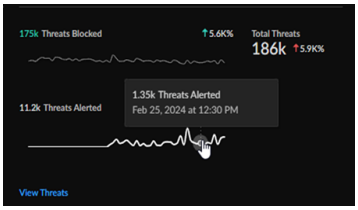


查看其中一個檢視時，您可以將滑鼠暫留在線條上方，以獲取關於網路的詳細資訊，例如網路上的流量或是封鎖或允許的威脅。

©2025 Palo Alto Networks, Inc.



中央視覺摘要下方是您啟動的訂閱所追蹤的數個關鍵指標，會針對您的網路提供可操作的洞察。透過這些關鍵指標，您可以導覽至數個詳細內容頁面之一，以進一步瞭解顯示的指標，並深入探索可能的解決方案。



 ©2025 Palo Alto Networks, Inc.

Strata Cloud Manager 控管中心檢視

控管中心提供四個不同的檢視，各有其本身的追蹤資料和指標可供檢查及互動。

- Summary
- 威脅
- 運作健康情況
- 資料安全性

©2025 Palo Alto Networks, Inc.

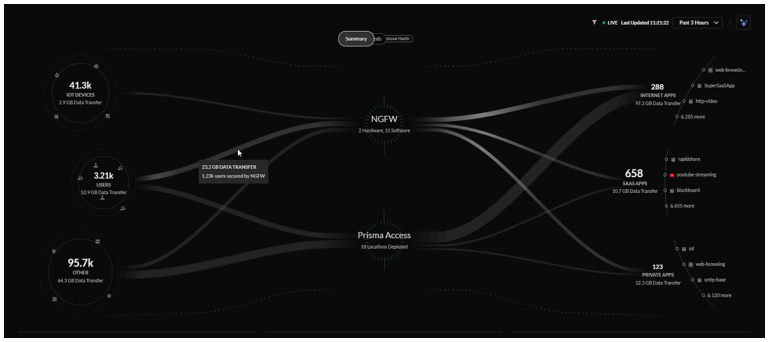
控管中心（摘要）

Summary（摘要）檢視可讓您概略查看來自使用者、外部主機、IoT 裝置和應用程式的所有流量，以及預覽其他檢視突顯的某些網路問題和異常。您可以使用此檢視初步查看每天的網路健康情況。

摘要授權	• 至少要有 Strata Logging Service 隨附的下列其中一個授權，才能使用 Strata 控管中心：
	  ❑ Prisma Access 授權
	  ❑ AIOps for NGFW Premium 授權
	• 或 AIOps for NGFW 免費版授權以及 Strata Logging Service 授權
	• [Summary（摘要）] 檢視中的其他指標所需的授權：
	  ❑ 雲端交付安全服務 (CDSS) 訂閱
	  ❑ 資料安全性訂閱
	  ❑ ADEM 授權
	  ❑ AI Access 授權

中央摘要檢視

中央 [Summary（摘要）] 檢視可讓您查看網路上的 IoT 裝置、使用者、從網際網路存取資源的外部主機、網際網路應用程式、SaaS 應用程式和私人應用程式之間傳輸的資料。



中央 [Summary（摘要）] 檢視中的線條代表網路上的資料傳輸和流量，線條的粗細代表從來源和應用程式傳輸的資料量。

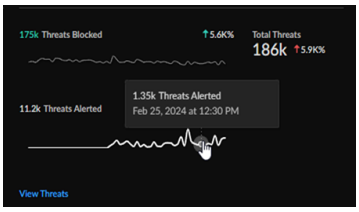
您可以查看網路基礎架構如何保護這些來源：

- Prisma Access 部署
- Strata Logging Service 詳細目錄中的新世代防火牆

 ©2025 Palo Alto Networks, Inc.

威脅總數

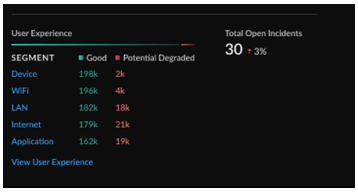
Total Threats Count（威脅總數）Widget 可讓您快速檢視在網路中偵測到的威脅總數、已封鎖的威脅數量、已引發警示的威脅數量，以及威脅在選定時間範圍內的變化。



點進 Activities Insights（活動洞察）（**Insights**（洞察） **> Activities Insights**（活動洞察） **> Threats**（威脅）） 畫面，瞭解關於網路威脅的詳細資訊。

未決事件和使用者體驗

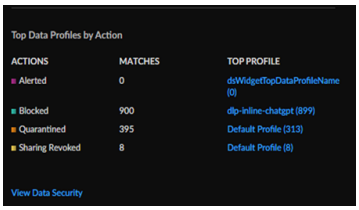
Open Incidents and User Experience（未決事件和使用者體驗） Widget 可讓您檢視未決事件總數、從使用者裝置到應用程式的服務交付鏈中個別區段的良好和可能下降的使用者體驗詳細資訊，以及未決事件在選定時間範圍內的變化。



點進 [Application Experience（應用程式體驗）] 儀表板 **(Dashboards**（儀表板） **> Application Experience**（應用程式體驗）**)**，以瞭解網路整體健康情況與使用者體驗和效能指標更詳細的資訊。

按動作顯示的最高排名資料設定檔

Top Data Profiles（最高排名的資料設定檔）Widget 可讓您檢視最高排名的預先定義資料篩選設定檔、在網路流量中找到的相符項數目，以及基於這些資料設定檔對敏感資料採取的動作。



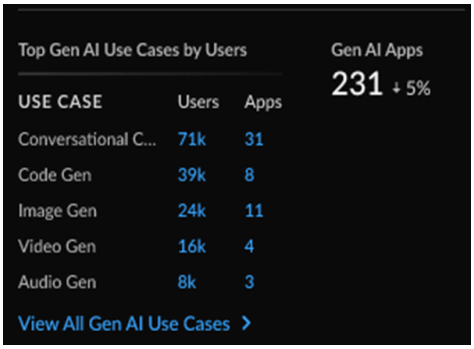
按一下 Data Security（資料安全性）檢視**(Command Center**（控管中心） **> Data Security**（資料安全性）**)**，以瞭解網路上敏感資料的詳細資訊。

按使用者和 GenAI 應用程式顯示的最高排名 GenAI 使用案例

Top GenAI Use Cases by User（按使用者顯示的最高排名 **GenAI** 使用案例）Widget 可讓您檢視使用者最常在您的網路上使用的 GenAI 應用程式使用案例、每個使用案例的使用者數量，以及屬於每個使用案例的 GenAI 應用程式數量。

©2025 Palo Alto Networks, Inc.

您也可以查看網路上的 GenAI 應用程式總數，以及基於時間篩選器的應用程式百分比變化。



點進活動洞察中的 AI 存取安全性 **(Insights**（洞察） **> AI Access**（**AI** 存取）**)**儀表板，深入瞭解您的網路上採用 GenAI 應用程式的情形，以及如何更妥善保護資料的建議。

若要進一步瞭解 *AI* 存取安全性，以及組織如何安全地採用 *GenAI* 應用程式，同時降低資料安全性的風險，請從這裡開始。

©2025 Palo Alto Networks, Inc.

威脅

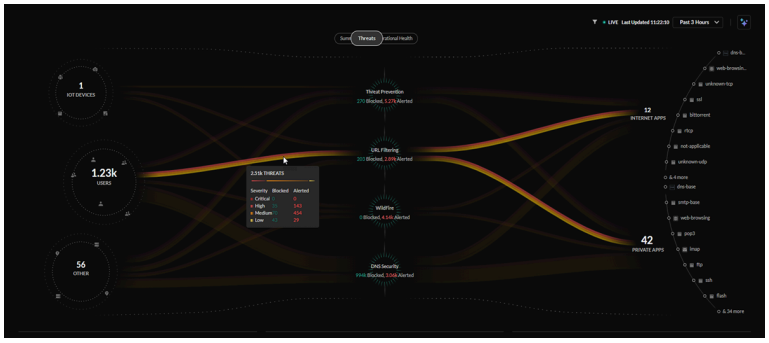
Threats（威脅）檢視會顯示在您的網路上檢查的流量，以及您的 CDSS 訂閱偵測到的威脅。您可以使用此檢視來監控您的網路上已封鎖和引發警示的威脅，或調查有哪些網路區域需要更新政策以適當封鎖任何引發了警示的威脅。

威脅授權	• 威脅授權，包括： ❑ 威脅防護授權 ❑ URL 篩選授權 ❑ WildFire 授權 ❑ DNS 安全性授權

中央威脅檢視

中央 [Threats（威脅）] 檢視可讓您查看網路上已由您的作用中雲端交付安全服務訂閱識別出的所有威脅。

[Threats（威脅）] 檢視會監控您的網路上潛在的威脅，以顯示 Palo Alto Networks CDSS 訂閱為您保護流量的情形。控管中心可讓您深入瞭解為 IoT 裝置、使用者和應用程式檢查的流量百分比，以及允許或引發警示的威脅總數。



中央[Threats（威脅）] 檢視中的線條代表安全性訂閱所監控的流量，粗細代表偵測到的威脅數量，色採代表威脅的嚴重性為重大、高、中或低。

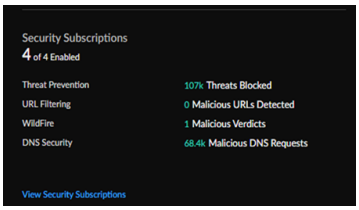
安全性訂閱

Security Subscriptions（安全性訂閱）Widget 可讓您檢視雲端交付安全性訂閱、哪些是作用中訂閱，及其如何保護網路的快照。

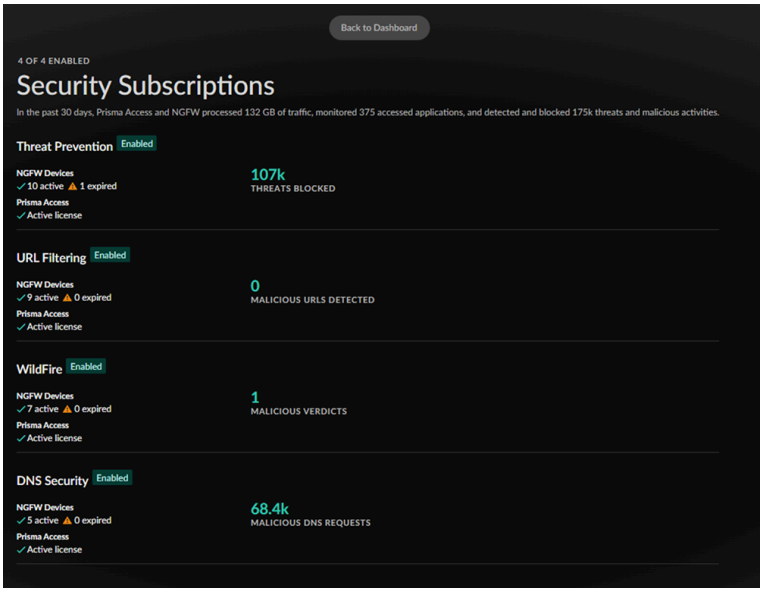
訂閱	說明
威脅防護	威脅防護可保護您的網路免受商品威脅（普遍但不精細），以及由有組織的網路攻擊者延續的針對性進階威脅。

©2025 Palo Alto Networks, Inc.

訂閱	說明
URL 篩選	進階 URL 篩選是我們全方位的 URL 篩選解決方案，可保護您的網路和使用者免受 Web 式威脅。
WildFire	雲端交付的 WildFire 惡意軟體分析服務會使用業界最大的全球社群提供的資料與威脅情報，並利用進階分析自動識別未知威脅及阻止攻擊者。
DNS 安全性	使用 Palo Alto Networks DNS 安全服務自動保護您的 DNS 流量。



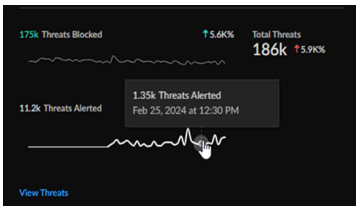
按一下 **Security Subscriptions**（安全性訂閱）Widget**(Command Center**（控管中心）**> View Security Subscriptions**（檢視安全性訂閱）**)**，可詳細報告與您的 NGFW 和 Prisma Access 部署相關的訂閱狀態。按一下 **Back to the Dashboard**（返回儀表板），返回 **Threats**（威脅）檢視。



威脅總數

Total Threats Count（威脅總數）Widget 可讓您快速檢視在網路中偵測到的威脅總數、已封鎖的威脅數量、已引發警示的威脅數量，以及威脅在選定時間範圍內的變化。

 ©2025 Palo Alto Networks, Inc.



點進 Activities Insights（活動洞察）（**Insights**（洞察） **> Activities Insights**（活動洞察） **> Threats**（威脅）），瞭解關於網路威脅的詳細資訊。

已封鎖和引發警示的威脅

Blocked and Alerted Threats（已封鎖和警示的威脅）Widget 會提供在您的網路中偵測到的威脅由上至下的檢視，並且按類別、威脅層級（重大、高、中和低）以及威脅是否遭到封鎖或引發警示進行組織。

點進所有對您的網路造成影響之威脅的詳細表格 **(Insights**（洞察） **> Activity Insights**（活動洞察） **> Threats**（威脅）**)**。

 ©2025 Palo Alto Networks, Inc.

運作健康情況

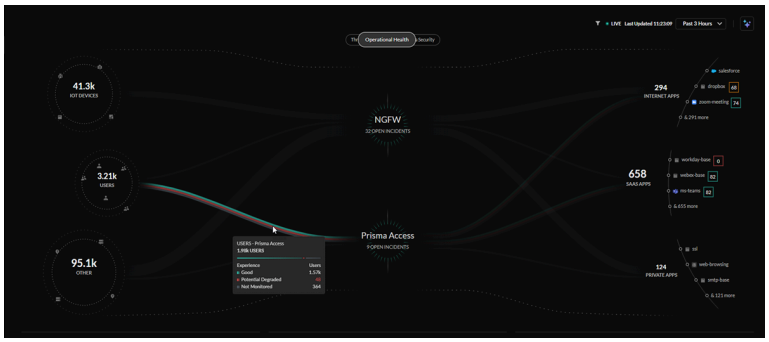
Operational Health（運作健康情況）檢視會顯示網路上基礎架構的健康情況和使用者體驗。您可以使用此檢視來監控 NGFW 和 Prisma Access 部署的健康情況，以及網路上的使用者體驗，並檢閱每個區域中未決事件的嚴重性。

運作健康情況授權	• 監控訂閱，包括： ❑ ADEM 可觀察性 ❑ 採用 AI 技術的 ADEM ❑ AIOps for NGFW Premium

中央運作健康情況檢視

中央 Operational Health（運作健康情況）檢視可讓您查看基礎架構的健康情況，以及網路上的使用者體驗。使用者若有自主數位體驗管理 (ADEM) 授權，則會在此檢視中看到增強的資料。

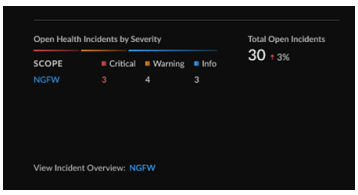
[Operational Health（運作健康情況）] 檢視會顯示您的 Palo Alto Networks ADEM 訂閱如何監控您的 SASE 環境中所有使用者和應用程式的數位體驗。



中央 [Operational Health（運作健康情況）] 檢視中的線條代表網路上的所有使用者。使用者會按使用者體驗分數進行組織，線條的色彩代表良好、不佳或未監控等評等。

未決事件總數和按嚴重性顯示的事件

Open Health Incidents by Severity（按嚴重性顯示的未決健康情況事件）Widget 可讓您檢視網路上的所有未決事件，並按範圍（NGFW、Prisma Access 和 Prisma SD-WAN）、嚴重性和事件數量進行細分。



此 Widget 會根據選定時段追蹤未決事件的百分比變化。

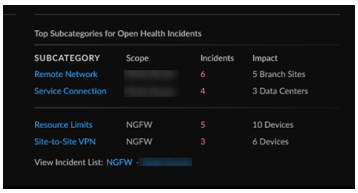
©2025 Palo Alto Networks, Inc.

點進每個可用範圍的 **Incidents and Alerts**（事件和警示）儀表板 **(Incidents and Alerts**（事件和警示） **> Prisma Access / NGFW > All Incidents**（所有事件）**)**。

未決健康情況事件的最高排名子類別

Top Subcategories for Open Health Incidents（未決健康情況事件的最高排名子類別）Widget 可讓您檢視網路上未決健康情況事件的最高排名子類別，並且按範圍、子類別、事件數量以及受影響的項目（資料中心、站台、裝置等等）進行組織。

此 Widget 會顯示單一範圍的前五個子類別，或多個範圍（如果適用）的前兩個子類別。



點進 **Incidents and Alerts**（事件和警示）儀表板 **(Incidents and Alerts**（事件和警示） **> Prisma Access / NGFW / Prisma SD-WAN)**，以瞭解事件的詳細資料。

受監控的使用者和使用者體驗

Open Incidents and User Experience（未決事件和使用者體驗） Widget 可讓您檢視未決事件總數、從使用者裝置到應用程式的服務交付鏈中個別區段的良好和可能下降的使用者體驗詳細資訊，以及未決事件在選定時間範圍內的變化。

點進 **Application Experience**（應用程式體驗）儀表板 **(Dashboards**（儀表板） **> Application Experience**（應用程式體驗）**)**，以瞭解網路整體體驗和效能指標更詳細的資訊。

 ©2025 Palo Alto Networks, Inc.

最佳做法

©2025 Palo Alto Networks, Inc.

資料安全性

Data Security（資料安全性）檢視會顯示在您的網路和各種連線的 SaaS 應用程式中偵測到的所有敏感資料。您可以將其用來監控及識別組織中的高風險敏感資料流程。

資料安全性授權	• 資料安全性授權，包括： ❑ SaaS 安全性授權 ❑ 資料安全性授權 ❑ 企業 DLP 授權

中央資料安全性檢視

中央 [Data Security（資料安全性）] 檢視提供您的網路和連線的 SaaS 應用程式中的敏感與高風險資料圖。控管中心可讓您深入瞭解組織中的敏感資料使用者、偵測到敏感資料活動（資產上傳、下載或資產公開）的特定已認可、未認可、容許或未標記的應用程式，以及已允許、封鎖、隔離、撤銷共用或公開的資產數目。

中央 [Data Security（資料安全性）] 檢視中的線條代表透過靜態資料和動態資料安全性解決方案偵測到的敏感資料，線條的粗細代表資料數量，色彩代表資料是否加上旗標或分類為重大、高、中或低風險。

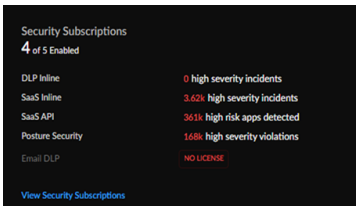
安全性訂閱

透過 **Security Subscriptions**（安全性訂閱）Widget，您可以檢視資料安全性訂閱、哪些是作用中訂閱，及其如何保護網路的快照。

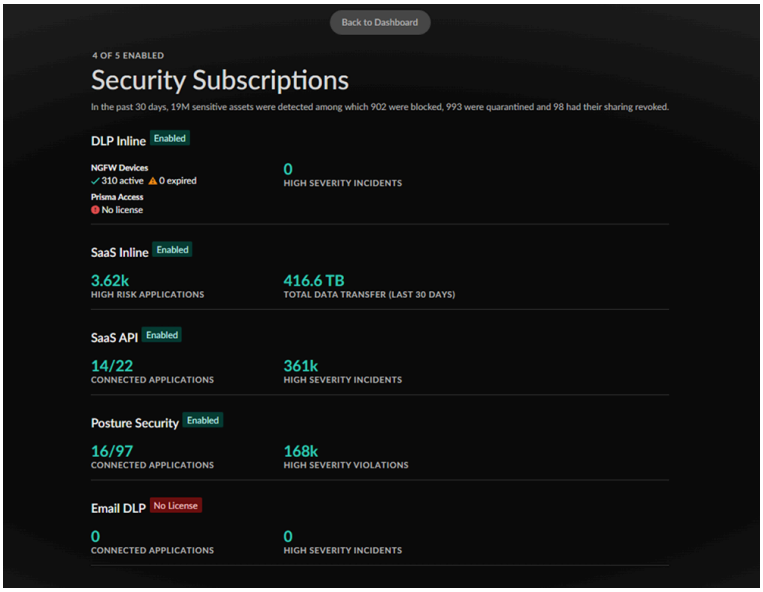
訂閱	說明
DLP 內嵌	企業 DLP 是一項雲端式服務，會使用受監督的機器學習演算法對敏感文件進行分類，以防止公開、資料遺失和資料外洩。
SaaS 內嵌	SaaS 內嵌解決方案可與 Strata Logging Service 搭配運作，以探索正在您的網路上使用的所有 SaaS 應用程式。

©2025 Palo Alto Networks, Inc.

訂閱	說明
SaaS API	SaaS API 是一項雲端式服務，您可以使用雲端應用程式的 API 直接將其連線至已認可的 SaaS 應用程式，並在應用程式內提供資料分類、共用或權限可見性以及威脅偵測。
安全性狀態	SaaS 安全性狀態管理 (SSPM) 會透過持續監控，協助您偵測並修復已認可的 SaaS 應用程式中設定不當的設定。
電子郵件 **DLP**	電子郵件 DLP 是企業 DLP 的附加元件，可透過採用 AI/ML 技術的資料偵測防止包含敏感資訊的電子郵件外洩。



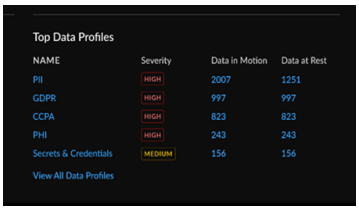
按一下 **Security Subscriptions**（安全性訂閱） Widget **(Command Center**（控管中心） **> View Security Subscriptions**（檢視安全性訂閱）**)**，可詳細報告與您的 NGFW 和 Prisma Access 部署相關的訂閱狀態。按一下 **Back to Table View**（返回表格檢視），返回 **Data Security**（資料安全性）檢視。



最高排名的資料設定檔

Top Data Profiles（最高排名的資料設定檔）Widget 會顯示在所有檢查的敏感資料中最常偵測到的資料設定檔、資料設定檔的嚴重性，以及在動態資料與靜態資料中偵測到的資產相符項數目。

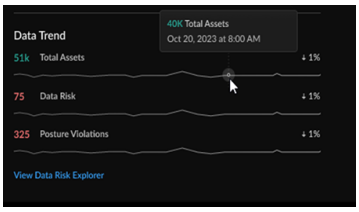
 ©2025 Palo Alto Networks, Inc.



按一下 **Data Loss Prevention**（資料遺失防護）儀表板 **(Manage**（管理） **> Configuration**（設定） **> Data Loss Prevention**（資料遺失防護）**)**，以檢閱所有預先定義的資料設定檔並新增自訂資料設定檔。

資料趨勢

Data Trend（資料趨勢）Widget 會顯示由資料安全性訂閱監控之敏感資料的趨勢，並且按總資產、資料風險和狀態違規的百分比變化進行組織。



按一下 **Data Risk**（資料風險）儀表板 **(Manage**（管理） **> Configuration**（設定） **> Data Loss Prevention**（資料遺失防護） **> Data Risk**（資料風險）**)**，瞭解您的整體資料風險分數並檢視可操作的建議，以改善組織的資料安全性狀態。

 ©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

洞察：活動洞察

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目 • Prisma SD-WAN	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 存取特定活動洞察檢視所需的其他授權和先決條件包括： ❑ Strata Logging Service ❑ 雲端交付安全服務 (CDSS) ❑ ADEM 可觀察性 ❑ WAN Clarity 報告 ❑ 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

活動洞察可讓您深入檢視 Prisma Access 與 NGFW 部署間的網路活動。此檢視將網路流量、應用程式使用情況、威脅和使用者活動等網路資料統整到同一處。活動洞察提供視覺化、監控和報告功能，讓您輕鬆執行工作。透過 Strata Cloud Manager 控管中心找出需要關注的領域後，請使用內容連結導覽至活動洞察或 其他儀表板，以進行進一步分析。

活動洞察具有進階篩選器，可協助您專注於部署不可或缺的安全層面。活動洞察中的進階報告功能可讓您從 [Overview（概要）] 頁籤中的資料下載、共用和排程報告。此報告分別顯示儀表板中所套用的每個篩選器的資料。或者，您可以從**Strata Cloud Manager > Reports**（報告）功能表排程活動洞察和儀表板的報告。

啟動 Strata Cloud Manager，然後按一下 **Insights**（洞察）( ) 開始使用。

活動洞察會顯示哪些內容？

活動洞察會按照部署在 Prisma Access 和 NGFW 環境中的 Strata Logging Service 租用戶顯示彙總資料。您可以篩選特定部署的資料。活動洞察有不同的頁籤。每個頁籤都提供與應用程式、使用者、威脅、URL 和網路使用相關的網路資料統合檢視。

- 概要 - 顯示應用程式、威脅、使用者、URL 和工作階段的資料，以及選定時間範圍內涉及的最大活動數目。瀏覽此檢視可快速識別網路中的任何異常，然後深入探究是否有需要調查的活動。
- 應用程式 - 網路中所有應用程式使用的概要，包括資料傳輸、應用程式風險，以及用來監控應用程式體驗的 ADEM 功能。
- **SD-WAN** 應用程式 - 檢視 Prisma SD-WAN 應用程式的效能，包括特定時間範圍內的健康情況分數、交易統計資料和頻寬使用率指標的詳細資料。
- 威脅 - 可讓您整體檢視 Palo Alto Networks 安全服務在您的網路中偵測到並封鎖的所有威脅。
- 使用者 - 提供對使用者流量和活動的深入洞察，包括 ADEM 監控使用者體驗的功能。
- **URL** - 顯示在您的網路中存取的 URL、其中有多少是惡意的、存取 URL 的使用者和應用程式、允許網路中的 URL 的規則，以及安全服務的強制執行。
- 規則 - 可讓您深入瞭解允許使用者和應用程式所產生之流量的安全性政策規則、在流量工作階段中偵測到的威脅，以及影響規則的 URL。
- 區域 - 顯示與應用程式、使用者、威脅和 URL 相關的網路流量詳細資料。

如何使用儀表板中的資料？

此處可協助你 -

- 識別您想要監控的應用程式、改善低分應用程式的使用者體驗，以及控制未經認可且有風險的應用程式。
- 檢視與您的部署最相關的威脅，並獲取威脅的背景資訊以進行調查。
- 根據您在日誌中的發現修訂安全性政策規則和流量規則，以彌補安全漏洞。
- 監控使用者活動以偵測並阻止潛在威脅，以及防止敏感資訊遭到不當使用。

©2025 Palo Alto Networks, Inc.

活動洞察：概要

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目 • Prisma SD-WAN	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 存取特定活動洞察檢視所需的其他授權和先決條件包括： ❑ Strata Logging Service ❑ 雲端交付安全服務 (CDSS) ❑ ADEM 可觀察性 ❑ WAN Clarity 報告 ❑ 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

檢視選定時段內在您的網路中最常見的應用程式、威脅、使用者、URL 和規則的摘要。瀏覽此檢視可快速識別網路中的任何異常，然後深入探究是否有需要調查的活動。[Overview（概要）] 檢視包含：

- 您的網路中具有最大活動量的前 5 個應用程式和應用程式類別，評量層面包括工作階段數目、資料傳輸、偵測到的威脅、存取的 URL，以及存取應用程式的使用者。按一下 **View all Applications**（檢視所有應用程式），以查看應用程式詳細資料。

- 對工作階段、使用者和應用程式影響最大的前 5 個威脅和威脅類別。分別在日誌檢視器、使用者和應用程式頁籤中檢視工作階段、使用者和應用程式的詳細資料。

- 封鎖、允許和警示工作階段的網路流量趨勢、傳輸的資料量，以及產生最多流量的使用者。

- 具有最多流量工作階段、傳輸的資料、在流量中發現的威脅、存取的 URL，以及受監控應用程式的使用者體驗評分最高的前 5 個使用者。

©2025 Palo Alto Networks, Inc.

- 最常存取的 URL，以及關於存取 URL 的工作階段、使用者和應用程式的詳細資料。

- 在設定您的部署中最受影響的前 5 個安全性政策規則，附有篩選器可瞭解符合規則的流量中涉及的工作階段、使用者、URL、威脅、傳輸的資料和應用程式。

您可以使用篩選器來檢視您想要關注、且與您的部署相關的資料點。這些篩選器在儀表板的所有頁籤中均可使用。

篩選器

活動洞察具有進階篩選器，可協助您專注於部署不可或缺的安全層面。可用的篩選器包括：

- 時間範圍 - 檢視指定時段的資料
- 範圍選取 - 部署的特定資料：Prisma Access、NGFW
- 子租用戶 - 顯示資料的 Prisma Access 執行個體
- 使用者名稱 - 檢視涉及個別使用者的活動
- 應用程式 - 關於特定應用程式的網路事件
- 應用程式類型 - 應用程式類型；SaaS、網際網路、私人
- 威脅類別 - 特定威脅類別的資料
- 威脅動作 - 允許或封鎖威脅的特定檢視
- **URL** 風險層級 - 與具有特定風險層級的 URL 相關的資料；高、中或低
- **URL** 類別 - 根據 URL 類別篩選資料
- 來源位置 - 檢視源自特定位置的活動
- 目的地位置 - 檢視以特定區域為目標的活動
- **URL** - 與存取的特定 URL 相關的活動。
- **SaaS** 應用程式- 關於特定 SaaS 應用程式的資料
- 認可的應用程式 - 僅檢視已認可或未經認可應用程式的資料
- 連接埠類型 - 對來自應用程式、通過標準或非標準連接埠的流量進行排序。
- 通訊協定 - 查看使用特定 TCP、UDP 或 HTTP 連接埠的流量
- 來源類型 - 檢視從特定裝置、使用者或其他來源產生的活動。

報告

按一下 **Overview**（概要）頁籤中的一個圖示  ，從根據 **Overview**（概要）頁籤中 的資料下載、共用和排程報告。您也可以從**Strata Cloud Manager** > **Reports**（報告）功能表中排程報告；按一下 圖示，然後從 **Type**（類型）下拉式清單中選取 [Activity Insights- Summary（活動洞察 - 摘要）]。

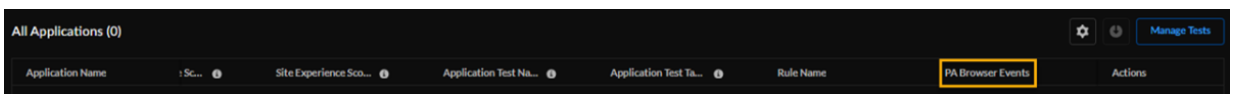
 ©2025 Palo Alto Networks, Inc.

活動洞察：應用程式

這可在何處使用？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	至少要有下列其中一個授權，才能使用活動洞察： ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) 或 AIOps for NGFW Premium license (use the Strata Cloud Manager app) 檢視 [Activity Insights:Applications（活動洞察：應用程式）] 頁籤所需的其他授權為： ❑ Strata Logging Service ❑ ADEM Observability 可解鎖其他 Prisma Access 功能

監控 Prisma Access 和 NGFW 設定中的應用程式、使用應用程式的使用者、風險分數、每個應用程式的使用者體驗，並瞭解有風險的應用程式所造成的安全性影響。應用程式使用情況的結果可協助您修訂安全性政策，以控制未經認可且有風險的應用程式。按一下 **Activity Insights**（活動洞察）**>Applications**（應用程式），以檢視下列資訊：

- 按風險分數顯示的應用程式 - 在您的組織中執行的應用程式總數，以及執行效能「良好」、「尚可」和「不良」的應用程式數目。這些應用程式會根據其應用程式體驗分數分類為「良好」、「尚可」和「不良」。
- 應用程式資料傳輸 - 選定時間範圍內，在 NGFW 與 Prisma Access 防火牆間下載和上傳的資料總計。您可以進行篩選，以檢視源自應用程式類別，並從裝置（資料中心或防火牆）流經目的地的資料傳輸。
- 所有應用程式 - 使用此 Widget 查看哪些 Prisma Access 應用程式受到監控並且執行綜合測試，以及在您的 NGFW 環境上執行的應用程式。表格中也顯示其體驗分數，這可以讓您得知每個應用程式的健康情況。如果您已有 Prisma Access 瀏覽器訂閱，就會看到 **PA Browser Events**（**PA** 瀏覽器事件）的欄。選取事件數目，這會將您重新導向至 Prisma Access 瀏覽器管理頁面。

  您可以用 csv 格式下載表格中的資料（僅限 Prisma Access 應用程式）。按一下 **Manage Tests**（管理測試）按鈕，以檢視為您在應用程式測試表格中的所有 Prisma Access 應用程式設定的所有綜合測試。如果要建立測試以監控應用程式，請按一下 User Experience（使用者體驗）欄底下的 **Monitor App to view Health**（監控應用程式以檢視健康情況）。

©2025 Palo Alto Networks, Inc.

- 應用程式詳細資料 - 檢視應用程式的一般詳細資料，以及關於應用程式活動和應用程式體驗的詳細資料。
  - **Activity**（活動）頁籤會顯示應用程式中出現的威脅總數、存取應用程式的使用者總數、透過應用程式傳輸的資料、PA 瀏覽器資料事件，以及 PA 瀏覽器存取事件。

    下圖顯示關於 **PA Browser Data Events**（PA 瀏覽器資料事件）和 **PA Browser Access Events**（PA 瀏覽器存取事件）的應用程式詳細資料。預設檢視會顯示所有事件和封鎖事件的 **Aggregate**（彙總），或者，您可以選擇按 **Event Type**（事件類型）和 **Count**（計數）檢視 **Breakdown**（詳細資訊）。

  - **Experience**（體驗）頁籤會顯示應用程式體驗分數、選定時間範圍內的分數趨勢，以及網路效能指標。

如果應用程式是容器應用程式，則顯示的統計資料會彙總容器中的所有應用程式。例如，*Gmail* 是一個容器應用程式（*Gmail* 沒有 *App-ID*）。它會將應用程式分組，例如 *gmail-posting*、*gmail-downloading*、*gmail-uploading* 等等。為此容器應用程式設定的風險分數，是針對包含的應用程式找到的最高風險分數。加總針對包含的應用程式找到的最高風險分數，即可算出所有其他指標。

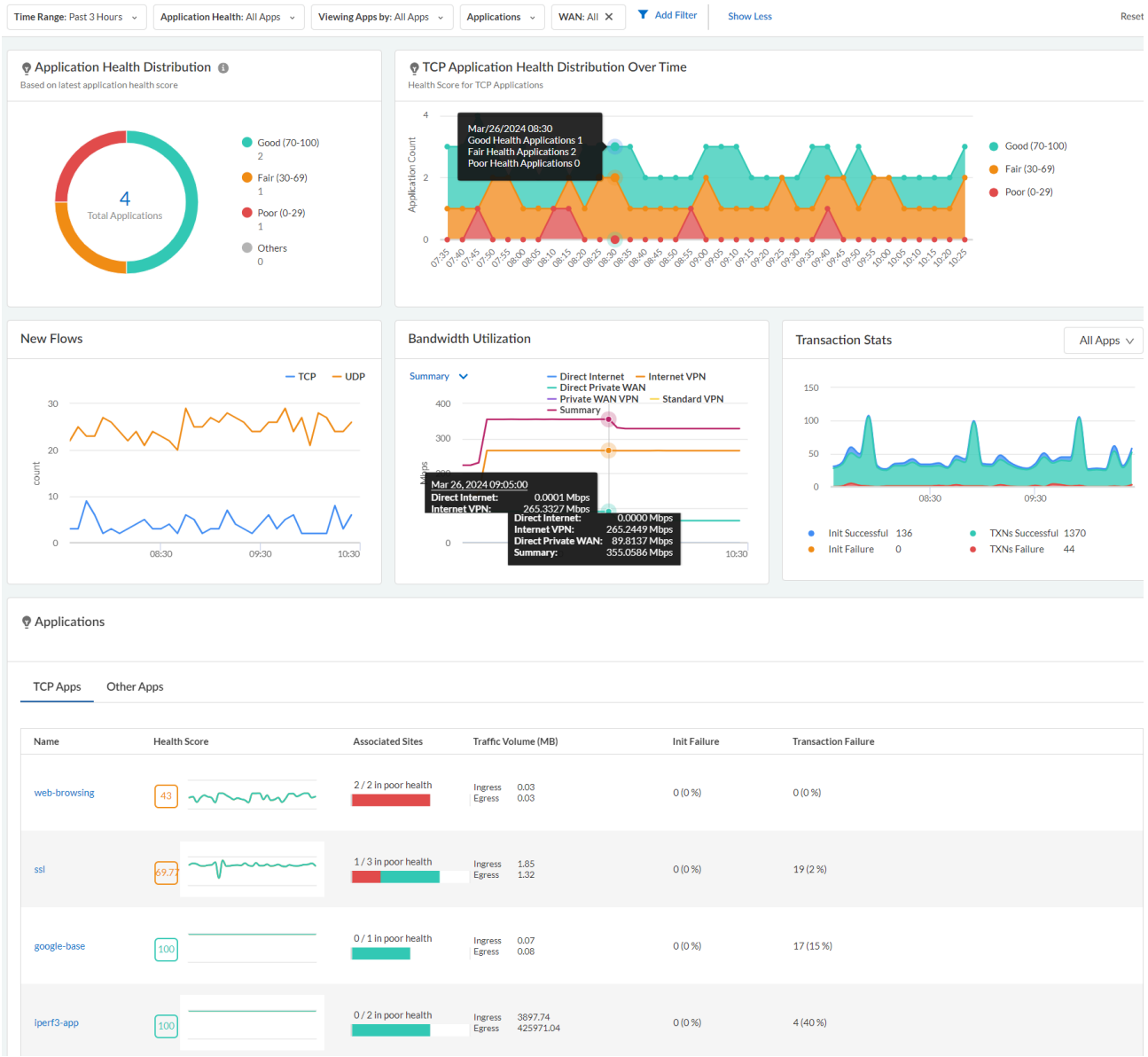
報告 - 您無法產生涵蓋此檢視中所含資料的報告。但是，您可以使用 **Application Usage**（應用程式使用情況）報告來檢視網路中的應用程式使用資料。若要排程報告，請從**Strata Cloud Manager** > **Reports**（報告）功能表中按一下 圖示，然後從 **Type**（類型）下拉式清單中選取 [Application Usage（應用程式使用情況）]。

 ©2025 Palo Alto Networks, Inc.

活動洞察：SD-WAN 應用程式

這可在何處使用？	我需要哪些內容？
• Prisma SD-WAN	❑ Prisma SD-WAN 授權 ❑ WAN Clarity Reporting 授權（用以檢視特定 Widget）

檢視在 Prisma SD-WAN 中效能最差的幾個應用程式。查看所有不良應用程式已確定的健康情況分數、租用戶的不良應用程式清單（以健康情況分數為基礎），以及不良應用程式在過去 3 小時（以 5 分鐘為間隔）的平均健康情況分數。



©2025 Palo Alto Networks, Inc.

- 應用程式健康情況分佈（需要 WAN Clarity 授權）：給定租用戶的「良好」、「尚可」和「不良」應用程式的分佈。
- 一段時間的 **TCP** 應用程式健康情況分佈（需要 WAN Clarity 授權）：「良好」、「尚可」和「不良」TCP 應用程式健康情況在一段時間內的分佈。時間序列圖應根據選取的持續時間計算和重新整理。例如，支援的持續時間為 1 小時、3 小時、1 天、7 天、30 天和 90 天，間隔為 1 分鐘、5 分鐘、1 小時和 1 天。
- 新流量：顯示給定期間的一個應用程式、一組特定應用程式或所有應用程式的新 TCP 和 UDP 流量。TCP 流量在遇到第一個 SYN 封包後，就會被視為新流量。UDP 流量在遇到任一方向的第一個 UDP 封包後，就會被視為新流量。流量是由來源和目的地 IP、來源和目的地連接埠以及通訊協定識別的雙向封包序列。
- 頻寬使用率：頻寬使用率圖表會顯示網路中的某個軌跡所使用的頻寬量。使用此圖表可識別網路中可能影響應用程式效能的 WAN 擁塞。此圖會呈現頻寬尖峰、特定站台耗用的總頻寬，以及應用程式；無論上傳是進入還是輸出方向。將游標移至 Bandwidth Utilization（頻寬使用率）圖表中，可更詳細地檢視應用程式或時間戳記的頻寬使用率。應用程式通常會按其頻寬使用率的順序列出。
- 交易統計資料：提供 TCP 流量的交易統計資料，包括特定應用程式或所有應用程式、特定路徑或所有路徑，以及所有健康情況事件的起始/交易成功和失敗。
- 應用程式：列出所有應用程式詳細資料，例如名稱、應用程式設定檔、健康情況分數、受影響的站台、流量、起始/失敗和交易/失敗。按一下應用程式名稱，可以在新頁面上查看個別的應用程式詳細資料。

 ©2025 Palo Alto Networks, Inc.

活動洞察：威脅

這可在何處使用？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	至少要有下列其中一個授權，才能使用活動洞察： ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) 或 AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 檢視 [Activity Insights:Threats（活動洞察：威脅）] 頁籤所需的其他授權為： ❑ Strata Logging Service ❑ CDSS 授權 ❑ ADEM Observability 可解鎖其他 Prisma Access 功能

全方位檢視在您的網路中發現的威脅活動和各種類型的威脅。此頁籤顯示在 Prisma Access 和 NGFW 部署中發現的威脅工作階段總數，以及選定時段內以威脅類別和威脅嚴重性為基礎的數目明細。您可以依據與威脅相關聯的安全構件進行搜尋，例如檔案雜湊、URL、網域或 IP 位址（IPv4 或 IPv6），以瞭解 Palo Alto Networks 威脅情報分析和第三方分析結果。

檢閱您的網路中特有威脅的下列詳細資料：

- 威脅名稱 - 威脅特徵碼名稱。使用此項目可尋找關於威脅的最新威脅資料庫資訊，包括某個時間範圍內的所有威脅工作階段。
- 威脅 **ID** - 唯一的威脅特徵碼 ID。使用威脅 ID 查閱 Palo Alto Networks 威脅資料庫中有關此特徵碼的最新資訊。
- 威脅類別和子類別 - 以威脅特徵碼（防毒、間諜軟體 (C2) 和弱點）為基礎的威脅類型。
- 授權 - 偵測到威脅的 Palo Alto Networks 安全服務。

©2025 Palo Alto Networks, Inc.

- 嚴重性 - 威脅嚴重性取決於入侵弱點的難易程度、對弱點的影響、易受攻擊的產品是否普遍、弱點產生的影響等等。嚴重性分類為：
  - 嚴重 - 當弱點對廣泛部署的軟體造成預設安裝上的影響，並且入侵可能導致 root 受損時。入侵程式碼（關於如何入侵系統程式碼、方法、概念證明（POC）的資訊）四處散佈，且易於利用。攻擊者不需要任何特殊的驗證認證，或對於個別受害者的相關瞭解。
  - 高 - 可能變成嚴重等級，但具有可減輕攻擊之因素的威脅；例如，難以入侵、不會導致權限提升，或沒有大型受害集區。
  - 中 - 帶來輕微影響的次要威脅，例如不會影響目標的 DoS 攻擊或需要攻擊者與受害者位於相同 LAN 的入侵行為，只會影響非標準設定或不重要的應用程式，或提供極其有限的存取權。
  - 低 - 對組織基礎結構影響極小的警告層級威脅。這些威脅通常需要本機或實體系統存取權，且可能經常導致隱私受損或 DoS 問題和資訊洩漏。
  - 參考性 - 未產生立即威脅的可疑事件，但會報告以讓您注意可能存在的深入問題。
- 工作階段總數 - 偵測到威脅的工作階段數目。按一下威脅名稱，可檢視指定時間範圍內所有相關的威脅工作階段。威脅工作階段表格會提供關於威脅的內容，例如 Palo Alto Networks 安全服務偵測到威脅的時間、受威脅影響的使用者、規則、應用程式、裝置，以及對威脅採取的動作（允許或封鎖）。
- 使用者總數 - 暴露於威脅下的使用者數目。
- 允許的威脅和封鎖的威脅 - 檢閱對威脅強制執行的動作，以確保這些動作不會在您的網路上觸發誤報。
- 動作 - 在日誌檢視器中調查威脅的日誌歷程記錄。

報告 - 您無法產生涵蓋此檢視中所含資料的報告。

 ©2025 Palo Alto Networks, Inc.

活動洞察：使用者

這可在何處使用？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	至少要有下列其中一個授權，才能使用活動洞察： ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) 或 AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 檢視 [Activity Insights:Users（活動洞察：使用者）] 頁籤所需的其他授權為： ❑ Strata Logging Service ❑ Advanced URL Filtering 授權 ❑ Cloud Identity Engine 授權 ❑ Advanced Threat Prevention 授權 ❑ ADEM Observability 可解鎖其他 Prisma Access 功能

監控 Prisma Access 和 NGFW 環境中的使用者活動。您可以透過其裝置上的 GlobalProtect 應用程式，或透過裝置上的 Web 瀏覽器使用明確 Proxy，來檢視連線至 Prisma Access 和 NGFW 安全服務的使用者資料。監控使用者活動有助於偵測並阻止潛在威脅、防止敏感資訊遭到不當使用，以及調整安全性政策規則以彌補安全漏洞。

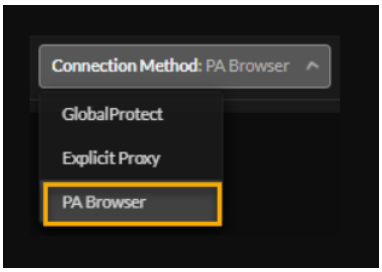
您可以根據以下條件篩選使用者資料：

- 部署；Prisma Access、NGFW
- 連線方法和版本；GlobalProtect、明確 Proxy、Prisma Access 瀏覽器
- 使用者名稱
- 裝置名稱
- 流量來源位置和 Prisma Access 位置
- 使用者存取的應用程式和使用者體驗分數篩選器

在此處檢視下列詳細資料：

 ©2025 Palo Alto Networks, Inc.

- 連線/作用中使用者 - 監控關於您目前連線的 GlobalProtect、明確 Proxy 行動使用者和 Prisma Access 瀏覽器的彙總資料。



  檢視在擷取資料時連線至網路的使用者數目，或時間戳記所示的數目。您可以按使用者或使用者裝置來檢視趨勢。選取數字可查看 **Connected Users | Connected User Devices**（已連線的使用者 **|** 已連線的使用者裝置）表格，以取得關於所有連線使用者及其所有裝置的詳細資料。

  檢視 **View Trend by Users**（按使用者檢視趨勢）中的動態權限存取資料，或按 **User Devices**（使用者裝置）、**Connected Users | Connected User Devices**（已連線的使用者）**|**（連線的使用者裝置）以及 **Project Distribution by Theater**（按場域顯示的專案分佈）檢視。

- 受監控的使用者 - 檢視受 ADEM 監控的使用者或使用者裝置總數，及其平均使用者體驗，這是 ADEM 上監控的所有使用者彙總而來的體驗分數。按一下數值，可檢視與使用者體驗相關的使用者活動詳細資料。
- 有風險的使用者 - 檢視受威脅影響的使用者數目。向上或向下箭頭可將此時間範圍與之前的時間範圍進行比較，以確認連線裝置數目的差異（以百分比為單位）。針對 [GlobalProtect Versions（GlobalProtect 版本）] 或 [IP Pool Utilization（IP 集區使用率）] 選取 [View More Details（更多詳細資料）]，以查看與環境中有風險的使用者有關的詳細資料。
- **GlobalProtect** 版本詳細資料會顯示您的裝置上安裝的 GlobalProtect 版本。您可以查看每個版本的連線使用者數目。使用這項資料，可要求必須符合最新的 GlobalProtect 應用程式版本。將游標暫留在 [Distribution Trend（發佈趨勢）] 行上，以查看當時連線使用者的 IP 位址。
- 根據當時的連線使用者數目，按不同的 IP 集區配置場域查看 **IP** 集區使用率。圖上的 IP 集區使用率百分比是在所有子網路上可用的所有 IP 集區區塊中，已使用的 IP 集區區塊數目。當您看到 IP 集區列接近任何區域的最大容量時，可藉由新增子網路來採取主動動作。

 ©2025 Palo Alto Networks, Inc.

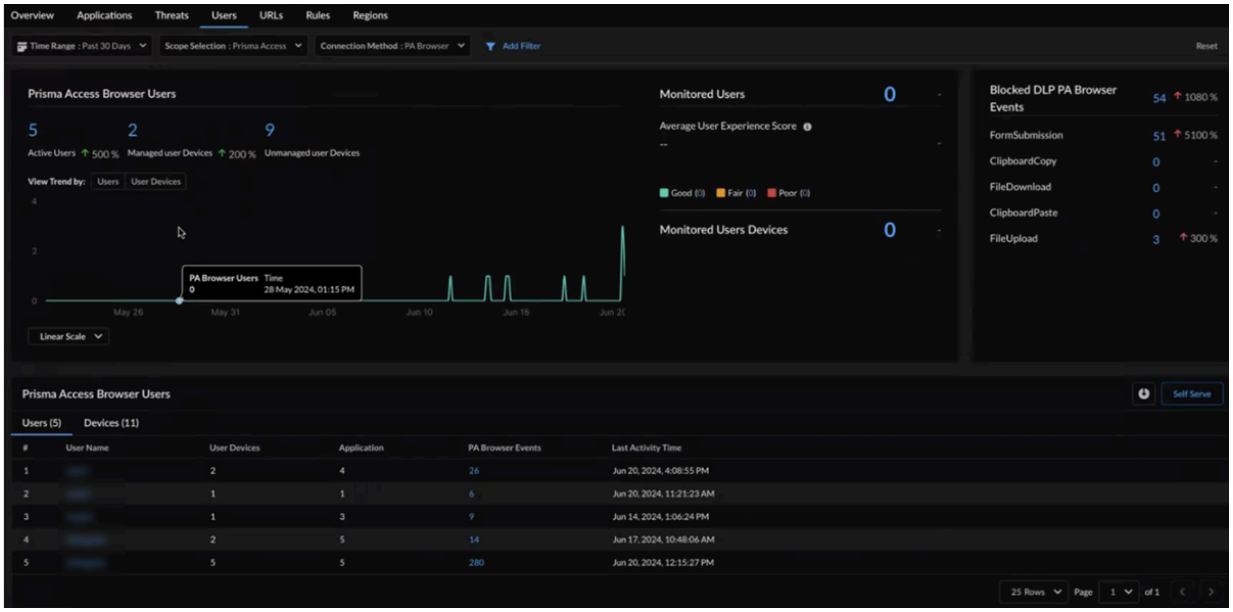
- **Users**（使用者）表格會顯示在時間範圍內登入之使用者的相關資訊。按一下使用者名稱，可查看個別使用者的瀏覽模式：他們最常造訪的站台、他們傳輸資料的站台，以及存取高風險站台的嘗試。
  - 威脅
    - 瀏覽摘要 - 查看使用者進行最多資料傳輸的站台類型數值，以及使用者的站台造訪次數。
    - 最多人造訪的前 **10** 個 **URL** 類別 - 根據資料傳輸檢視使用者的最高排名 URL 類別。您也可以查看屬於各個 URL 類別的唯一 URL 造訪次數。
    - **URL** 瀏覽摘要 - 在使用者造訪的唯一 URL 之中，請留意對惡意和高風險 URL 的造訪 — 這些站台可能會使您的網路暴露於威脅、資料遺失和違規的風險下。如果您看到這些站台的造訪次數超過預期，請調整安全性政策規則以彌補漏洞。
    - 前 **10** 個 **URL** - 檢閱使用者最常造訪之站台的風險層級。高風險 URL 可能會使您的網路暴露於威脅下，因此必須受到監控。
    - 按風險顯示的封鎖 **URL** - 這些是使用者最常嘗試存取的封鎖 URL。檢閱 URL 篩選日誌，並確認是否需要調整安全性政策規則以變更動作。
    - 嚴重威脅 - 檢視為使用者偵測到的威脅總數，和以威脅嚴重性為基礎的數目。將數目與其他使用者進行比較。如果數目異常偏高，請調整安全性政策規則。
    - 最嚴重的威脅 - 這些是對使用者最常偵測到的威脅。
  - 連線性 - 顯示使用者登入的裝置在特定時段內的趨勢，以及每個使用者登入和登出事件的裝置連線詳細資料。
  - 體驗 - 提供裝置的使用者體驗資料、每個受監控應用程式的體驗分數和趨勢，以及個別裝置受監控的使用者和應用程式的效能指標。
- Prisma Access 瀏覽器 -選取 **Prisma Access Browser Connection Method**（**Prisma Access** 瀏覽器連線方法），以檢視 Prisma Access 瀏覽器使用者的相關資訊。

  Prisma Access Browser Users（**Prisma Access** 瀏覽器使用者）活動趨勢圖會顯示在選定時間範圍篩選器中的某個時間點處於作用中狀態的使用者數目。此圖詳細列出安裝了 Prisma Access 連

 ©2025 Palo Alto Networks, Inc.

線代理程式的作用中使用者裝置（受管理的裝置），以及沒有任何代理程式（非受管理）使用者的裝置。

Prisma Access 瀏覽器可讓您清晰檢視瀏覽器使用者的動作，並指出企業的 DLP 政策是否允許或封鎖使用者在其裝置上對企業的資料資產執行的行動。**Blocked DLP PA Browser Events**（封鎖的 **DLP PA** 瀏覽器事件）Widget 會顯示使用者在瀏覽器上執行的動作遭到政策封鎖的事件。

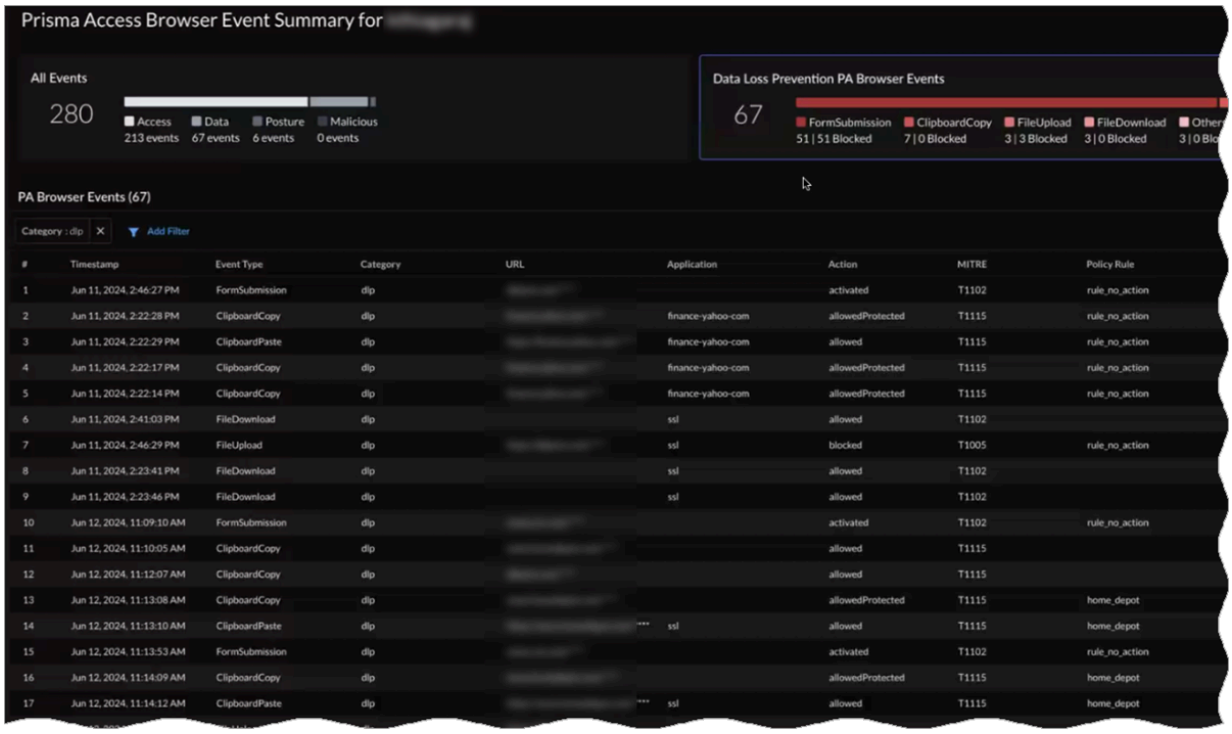


Prisma Access Browser Users（**Prisma Access** 瀏覽器使用者）表格會顯示透過 Prisma Access 瀏覽器存取應用程式的作用中使用者清單。按一下任何 **User Name**（使用者名稱），即可在**User Details**（使用者詳細資料） > **Activity**（活動）頁面中查看此使用者的 **Activity**（活動）。

Prisma Access Browser Event Summary（**Prisma Access** 瀏覽器事件摘要）頁面會列出使用者在選取的時間間隔內透過瀏覽器執行的所有瀏覽器動作。**PA Browser Events**（**PA** 瀏覽器事件）表格的預設檢視會顯示所有 DLP **Browser Events**（瀏覽器事件）的清單，無論政策允許還是封鎖。您可以選取適當的事件類別，將檢視切換為其他事件類別，例如 **Access Events**（存取事件）、**Posture Events**（狀態事件）或 **Malicious Events**（惡意事件）。在每個 **Event**（事

©2025 Palo Alto Networks, Inc.

件）類別中，您可以檢視事件類型的明細，以及顯示瀏覽器事件於何時執行的時間戳記、已存取應用程式 URL 的相關資訊、應用程式名稱，以及任何相關聯的 MITRE 攻擊備註。



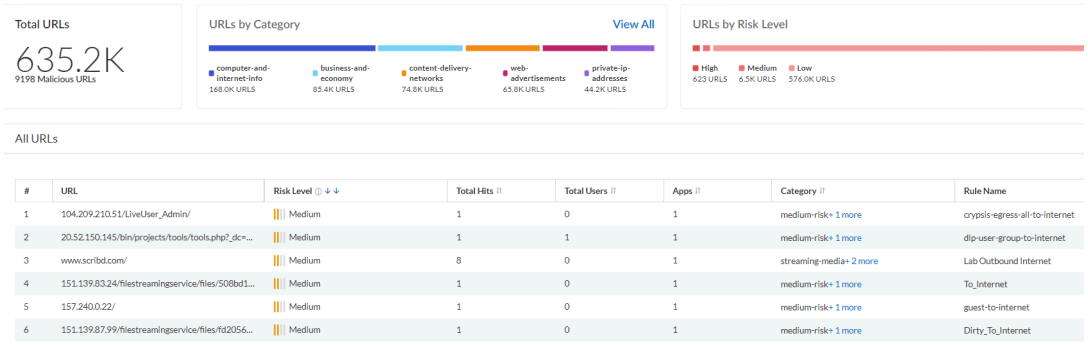
報告 - 您無法產生涵蓋此檢視中所含資料的報告。不過，您可以使用「使用者活動」報告來檢視網路中的使用者特定的活動。若要從**Strata Cloud Manager** > **Reports**（報告）功能表排程報告，請按一下 圖示，然後從 **Type**（類型）下拉式清單中選取使用者。

 ©2025 Palo Alto Networks, Inc.

活動洞察：URL

這可在何處使用？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	至少要有下列其中一個授權，才能使用活動洞察： ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) 或 AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 檢視 [Activity Insights:URLs（活動洞察：URL）] 頁籤所需的其他授權為： ❑ Strata Logging Service ❑ Advanced URL Filtering 授權

此檢視會彙總進階 URL 篩選服務在 Prisma Access 和 NGFW 部署中偵測到的 URL 活動。您可以檢視指定時段內在您的網路中偵測到的 URL 總數，以及這些 URL 按 URL 類別與風險層級顯示的明細。使用篩選選項，可篩選儀表板中的檢視。



使用此處的資料：

- 識別最常存取的 URL 類別、具有 URL 類別的唯一 URL、網路中的 URL 歷程記錄，以及全域分析結果。根據 URL 篩選服務所篩選的惡意 URL，這些 URL 類別很可能會使您的網路暴露於惡意和攻擊性的內容下。最佳做法是封鎖這些 URL 類別。
- 檢閱高風險 URL，及其對使用者、應用程式和規則的影響。高風險 URL 站台不一定是惡意的；但仍可能會使您的網路暴露於威脅下（舉例來說，不是惡意、但由 Bulletproof ISP 託管的站台，就是高風險站台）。請考慮將目標定為具有嚴格解密和安全性政策規則的站台。

報告 - 您無法產生涵蓋此檢視中所含資料的報告。

©2025 Palo Alto Networks, Inc.

活動洞察：規則

這可在何處使用？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	至少要有下列其中一個授權，才能使用活動洞察： ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) 或 AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 檢視 [Activity Insights:Rules（活動洞察：規則）] 頁籤所需的其他授權為： ❑ Strata Logging Service

檢視與網路中的所有流量比對的安全性政策規則。安全性政策規則會根據流量屬性判斷是否要封鎖或允許工作階段，例如來源和目的地 IP 位址、應用程式、使用者和服務。所有通過網路的流量都會與工作階段進行比對，而各工作階段也將與安全性政策規則進行比對。有相符的工作階段時，就會套用安全性政策規則。

All Rules

#	Rule Name	Sessions	Upload Data	Download Data	Threats	Users	URLs	Apps
1	prod-to-db-access	46635	210.2 MB	2.4 GB	3,788,442	16,466	950	14
2	corp-to-ad-services-dns	904365	960.6 MB	249.4 GB	2,008,112	2,269	0	1
3	dns-outbound	127994	19.5 MB	17.2 GB	862,523	4	0	1
4	inet-access	9950	14.7 MB	55.8 GB	483,769	0	77	3
5	lab-to-lab-services	32857	7.0 MB	10.7 GB	349,630	0	0	1
6	gcs-outbound-transit	2378	2.0 MB	17.2 GB	215,461	0	1	1
7	server-to-pki-prod-ocsp-web-nstd	22237	21.0 MB	151.6 MB	109,061	0	52	1
8	users-to-internet-business-low	22169	342.4 MB	1.9 GB	86,646	1,632	86,247	15
9	corp-user-to-lab-smb	252	464.0 kB	259.9 kB	85,002	101	0	1

儀表板顯示與安全性政策規則相符之網路事件的下列詳細資料：

流量工作階段、傳輸的資料、在工作階段中偵測到的威脅、受影響的使用者、瀏覽的 URL，以及存取的應用程式。檢閱最符合流量工作階段的規則，分析這些工作階段以瞭解規則是否過於寬鬆，並視需要最佳化規則。

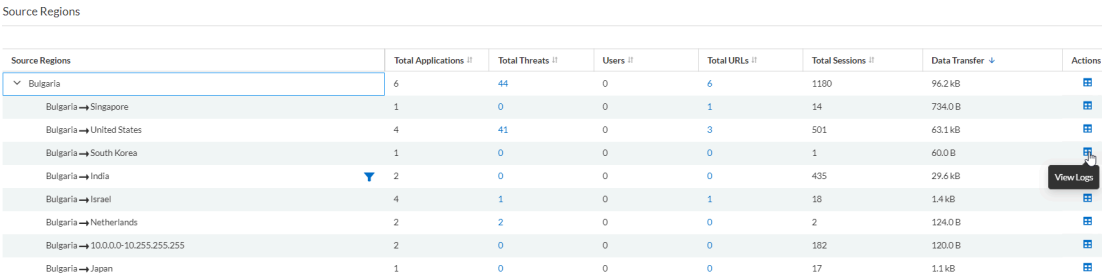
報告 - 您無法產生涵蓋此檢視中所含資料的報告。

©2025 Palo Alto Networks, Inc.

活動洞察：地區

這可在何處使用？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	至少要有下列其中一個授權，才能使用活動洞察： ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) 或 AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 檢視 [Activity Insights:Regions（活動洞察：區域）] 頁籤所需的其他授權為： ❑ Strata Logging Service

以下是您的網路中流量的來源區域。此檢視提供關於源自這些位置的威脅、使用者、URL、網路工作階段和資料傳輸的資訊。您也可以深入瞭解流量的目標位置。按一下 [Actions（動作）] 可檢視工作階段的流量日誌。您可以使用這些資料來識別試圖滲透網路的威脅所鎖定的目標區域，並縮小其範圍。最佳化適用於目標區域的規則。



有一些篩選選項可以縮小進出於特定來源和目的地區域的流量範圍。其他篩選選項包括：

- 在特定部署（Prisma Access、NGFW）中出現的流量
- 進出於已認可或未經認可應用程式的流量
- 使用特定連接埠和通訊協定的流量
- 涉及特定威脅類型、威脅類別、URL 和 URL 類別的流量

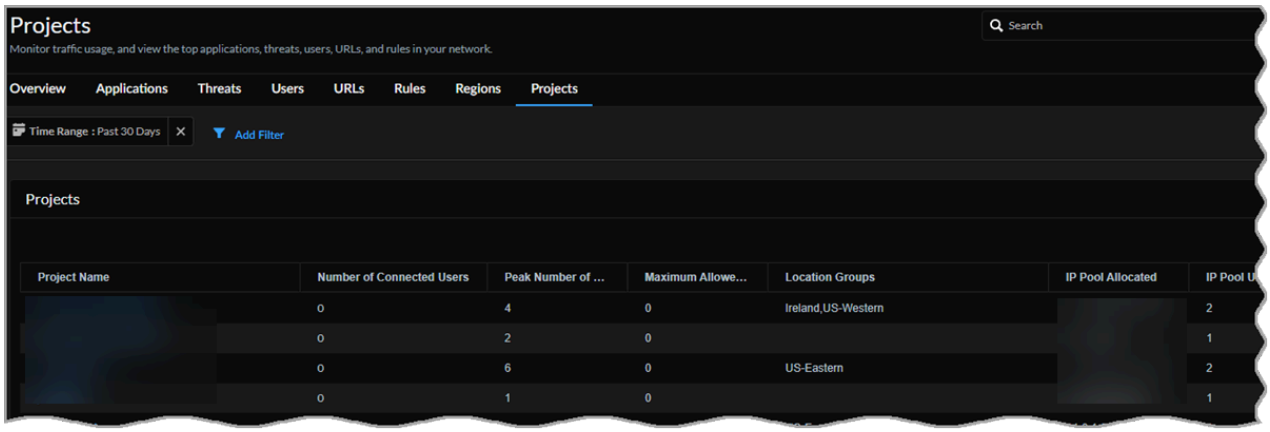
報告 - 您無法產生涵蓋此檢視中所含資料的報告。但是，您可以利用網路使用情況報告來瞭解關於網路流量的詳細資料。若要排程報告，請從**Strata Cloud Manager > Reports**（報告）功能表中按一下 圖示，然後從 **Type**（類型）下拉式清單中選取 [Network Usage（網路使用情況）]。

©2025 Palo Alto Networks, Inc.

活動洞察：專案

這可在何處使用？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	至少要有下列其中一個授權，才能使用活動洞察： ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) 或 AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

使用 Strata Cloud Manager 監控您的動態權限存取專案活動，以瞭解您的 Prisma Access 代理程式部署。



- **Projects**（專案）表格會概略說明動態權限存取使用者使用 Prisma Access 存取的專案。選取任何專案的名稱以檢視其詳細資料頁面。
- 專案的詳細資料頁面會顯示：
  - 概要 — 檢視為此專案選取的時間範圍內允許的最大使用者數目和尖峰使用者數目。
  - **IP** 集區使用率 — 檢視使用中的 IP 數目，以及此專案中的集區仍可用的 IP 數目。
  - 已連線的使用者 — 檢視選定時間範圍內連線使用者的圖表。
  - 按位置群組顯示的連線使用者 — 按使用者所在的 Prisma Access 位置群組查看使用者數目。

©2025 Palo Alto Networks, Inc.

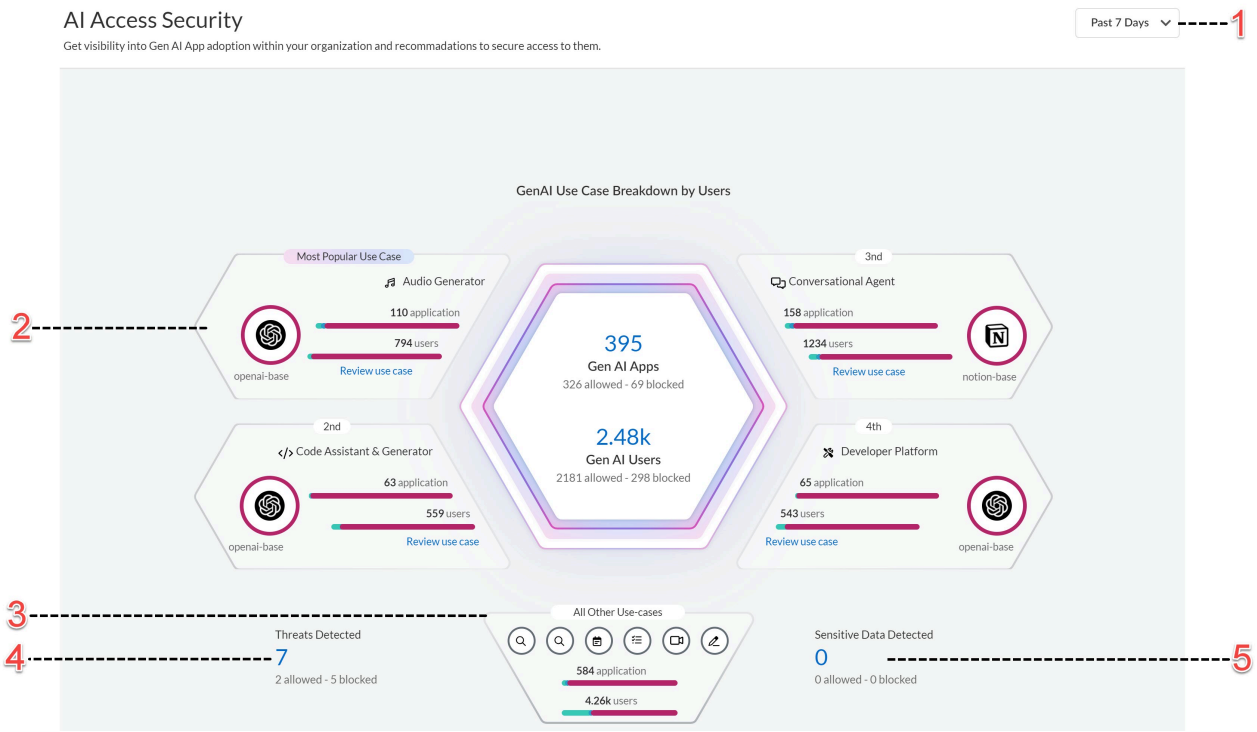
洞察：AI Access

這可在何處使用？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	下列其中一個授權： ❑ AI Access Security 授權 ❑ CASB-PA 授權 ❑ CASB-X 授權 若要進一步瞭解支援 AI 存取安全性的授權，請按一下這裡。

生成式人工智慧 (GenAI) 應用程式是能夠產生文字、影像、影片和其他形式的資料以回應使用者提示，並根據使用者資料輸入不斷學習的 AI 應用程式。其運用正以驚人的速度激增，並且為企業帶來了無限的商機。然而，GenAI 應用程式本質上會以爭議性的方式演進，為企業和安全管理員帶來了新的危機 - 如何確保員工不會將敏感或專屬資料公開給 GenAI 應用程式？

Palo Alto Networks 導入了 AI 存取安全性，以確保您能夠在整個組織中安全地採用 GenAI 應用程式。

使用 AI 存取安全性洞察儀表板，篩選網路上的 GenAI 應用程式使用情況。[AI Access Security Insights（AI 存取安全性洞察）] 儀表板提供了深入的詳細資料，可協助您瞭解哪些 GenAI 應用程式正在使用，以及由誰使用。



©2025 Palo Alto Networks, Inc.

若要進一步瞭解如何保護敏感資料不受 *GenAI* 應用程式誤用，請按一下這裡。

 ©2025 Palo Alto Networks, Inc.

洞察：AI 執行階段安全性

這可在何處使用？	我需要哪些內容？
• Prisma Access（使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW（使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ 啟動您的 AI 執行階段安全性授權 ❑ AI 執行階段安全性設定先決條件 ❑ 在 SCM 中上線和啟動雲端帳戶

Palo Alto Networks AI 執行階段安全性是專用的集中式安全性解決方案，可透過採用 AI 技術的即時安全性，保護組織的雲端網路架構免受 AI 特定和傳統網路攻擊侵害。它可以保護您的新世代 AI 模型、AI 應用程式和 AI 資料集免受網路威脅，例如提示插入、敏感資料外洩、不安全的輸出（例如惡意軟體和 URL）以及模型 DoS 攻擊。

使用 AI Runtime Security Insights（AI 執行階段安全性洞察）儀表板，瞭解您的雲網路攻擊面，並保護雲端資產免受惡意威脅侵害。

要進一步瞭解如何保護 *AI* 和非 *AI* 網路流量免受潛在攻擊，請按一下這裡。

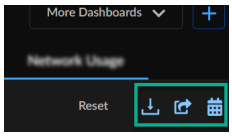
©2025 Palo Alto Networks, Inc.

儀表板：Strata Cloud Manager

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目 • Prisma SD-WAN	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN 存取特定儀表板所需的其他授權和先決條件包括： ❑ 雲端交付安全服務 (CDSS) ❑ ADEM 可觀察性 ❑ 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

Strata Cloud Manager 提供一組互動式儀表板，可讓您全方位檢視在您的網路中運作的應用程式、ION 裝置、威脅、使用者和安全性訂閱。儀表板可讓您檢視部署中發生的健康情況、安全性狀態和活動，協助您防止或解決網路中的效能問題和安全漏洞。儀表板支援涵蓋雲端管理支援的 Palo Alto Networks 產品和訂閱，也來自其他來源，包括 Traps、Cortex XDR、Prisma SaaS 和 Proofpoint。您可看到的資料通常取決於您的訂閱。您可以檢閱每個儀表板主題，以瞭解該儀表板的授權需求、角色權限是否會影響可見的資料，以及瞭解每個訂閱解鎖的不同資料類型。

您可以從左側導覽窗格的 **Dashboards**（儀表板）功能表存取儀表板。根據預設，SASE 健康情況儀表板會釘選至登陸頁面。按一下 **More Dashboards**（更多儀表板），然後選取或清除儀表板名稱旁的核取方塊，以將儀表板固定至儀表板登陸頁面，或取消固定。您也可以使用 **Build My Dashboard**（建置我的儀表板）選項來建立自己的儀表板。某些儀表板還也有選項可供您下載及共用可以離線共用和排程定期更新的報告。若要查看儀表板是否支援報告，請查看下列圖示：



與雲端識別引擎整合

建議您設定雲端識別引擎（目錄同步），以充分利用儀表板。雲端識別引擎是一個免費的 Palo Alto Networks 應用程式，可讓其他應用程式對您的 Active Directory 資訊進行唯讀存取，並且讓您：

- 取得使用者活動資料 - 雲端識別引擎可讓您指定要為其執行報告的使用者。
- 在設定雲端識別引擎後，輕鬆而安全地與組織的其他成員共用報告，即可將收件者新增至已排程的報告。您的報告收件者會受到雲端識別引擎的檢查，如果找不到相符，就會執行額外的驗證步驟，方法是根據與支援帳戶相關聯的電子郵件地址網域檢查電子郵件地址網域。這些檢查可確保報告不會傳送至組織外部。

整合的應用程式必須部署在相同區域中。您可以隨時移至中樞，將雲端識別引擎與 Prisma Access 或目錄同步整合。 # 整合 Palo Alto Networks 應用程式

©2025 Palo Alto Networks, Inc.

儀表板的支援

產品中的某些儀表板支援正在等待移轉至 *Strata Cloud Manager*。

功能	支援的系統				授權和其他需求	彙總資料的範圍
	Prisma Access（雲端管理）	**Prisma Access**（Par管理）*	**AIOps for N(**	**Prisma SASE** 多租用戶平台		
	• Prisma Access (Managed by Strata Cloud Manager) 和 Prisma Access (Managed by Panorama) 的文件		• AIOps for NGFW 的文件	• Prisma SASE 多租用戶平台的文件		
SASE 健康情況	是	是	是		• ADEM 可觀察性 • 採用 AI 技術的 ADEM	
最佳做法	是	否。	PAN-OS 版本：10.0 或更新版本	是	[僅適用於 AIOps for NGFW] 在裝置中啟用遙測共用	• Prisma Access (Manage 每個租用戶 • AIOps for NGFW：每個與 AIOps for NGFW 執行個體相關聯的 NGFW/Panorama
合規性摘要	否。	否。	是	否。	[僅適用於 AIOps for NGFW] 在裝置中啟用遙測共用	AIOps for NGFW：每個與 AIOps for NGFW 執行個體相關聯的 NGFW/Panorama
隨選 BPA	否。	否。	是	否。	TSF	AIOps for NGFW：每個與 AIOps

©2025 Palo Alto Networks, Inc.

功能	支援的系統				授權和其他需求	彙總資料的範圍
	Prisma Access（雲端管理）	Prisma Access（Par 管理）*	AIOps for N(	Prisma SASE 多租用戶平台		
						for NGFW 執行個體相關聯的 NGFW/ Panorama
執行摘要	是	是	是	是	• Strata Logging Service 授權 • 威脅防護授權 • URL 篩選授權 • WildFire 授權 • 企業 DLP 授權	每個 Strata Logging Service 租用戶
WildFire	是	否。	是	是**	WildFire 授權	每個租用戶服務群組 (TSG)
DNS 安全性	是	是	是	是**	DNS 安全性授權	每個租用戶服務群組 (TSG)
日誌檢視器	是	是	是	是	Strata Logging Service 授權	每個 Strata Logging Service 租用戶
IOC 搜尋	是	否。	是	是**	在搜尋中檢視趨勢圖的需求： • DNS 授權 • WildFire 授權 • Strata Logging	

©2025 Palo Alto Networks, Inc.

功能	支援的系統				授權和其他需求	彙總資料的範圍
	Prisma Access（雲端管理）	Prisma Access（Par 管理）*	AIOps for N(	Prisma SASE 多租用戶平台		
					Service 授權 • URL 篩選	
下載#共用#排程	是	是	是	是		請參閱此表格中各自的功能欄
SaaS 安全性	是	否。	否。	否。	• SaaS 安全性授權 • Strata Logging Service	每個 Prisma Access 租用戶
DLP 事件	是	否。	否。	否。	企業 DLP 授權	每個 Prisma Access 租用戶
裝置健康情況	否。	否。	是	否。	• [僅適用於 AIOps for NGFW] 在裝置中啟用遙測共用	AIOps for NGFW：每個與 AIOps for NGFW 執行個體相關聯的 NGFW/ Panorama
安全性狀態洞察	否。	否。	是	否。		AIOps for NGFW：每個與 AIOps for NGFW 執行個體相關聯的 NGFW/ Panorama
進階威脅防護	否。	否。	是	否。	• 威脅防護或進階威脅防護授權 • Strata Logging Service	每個 Strata Logging Service 租用戶

©2025 Palo Alto Networks, Inc.

功能	支援的系統				授權和其他需求	彙總資料的範圍
	Prisma Access（雲端管理）	Prisma Access（Pan 管理）*	AIOps for N(	Prisma SASE 多租用戶平台		
IoT Security	是	是	是	否。	IoT Security 授權	每個 IoT Security 租用戶
Prisma SD-WAN	否。	否。	否。	是	Prisma SD-WAN 授權	每個 Prisma SD-WAN 租用戶
PAN-OS CVE	否。	是	是		[僅適用於 AIOps for NGFW] 在裝置中啟用遙測共用	• AIOps for NGFW：每個與 AIOps for NGFW 執行個體相關聯的 NGFW/ Panorama • 使用 API 存取之 CVE 的 PSIRT 資料庫
CDSS 採用	是	是	是		[僅適用於 AIOps for NGFW] 在裝置中啟用遙測共用	AIOps for NGFW：每個與 AIOps for NGFW 執行個體相關聯的 NGFW/ Panorama
功能採用	否。	是	是		[僅適用於 AIOps for NGFW] 在裝置中啟用遙測共用	AIOps for NGFW：每個與 AIOps for NGFW 執行個體相關聯的 NGFW/ Panorama

Prisma Access（Panorama 管理）* -

©2025 Palo Alto Networks, Inc.

- 對於在非美洲區域託管 Strata Logging Service 的 Prisma Access（Panorama 管理）使用者，您必須表示同意，才能允許 Prisma Access 讀取和處理非美洲區域中來自 Strata Logging Service 的資料。檢閱並接受儀表板首頁上的隱私權聲明以表示同意，並檢視更多儀表板和日誌。只有應用程式、執行個體和帳戶管理員可以查看並接受隱私權聲明。
- Prisma Access（Panorama 管理）多租用戶環境中不支援儀表板。

是* - 「是」表示所有版本的 Prisma Access 和 PAN-OS 都受到支援。

是** - 在多租用戶平台中，租用戶會識別為租用戶服務群組 (TSG)，並且獲派 TSG ID。每個客戶支援入口網站 (CSP) 可以與一或多個租用戶相關聯。儀表板中顯示的資料取決於下列情況：

- 您從中存取儀表板的應用程式必須受 TSG 支援，並透過 SASE 平台或中樞上的租用戶檢視來存取。
- 您已使用中樞的通用服務將裝置與租用戶產生關聯。
- 確認您的租用戶與 CSP 之間有一對一或多對一的對應。
  - 如果您的租用戶與 CSP 之間有一對一的對應，您可以檢視所有來源的儀表板資料（例如，在 WildFire 儀表板中，會顯示來自 Palo Alto Networks 防火牆、Prisma Access、Traps、Cortex XDR、Prisma SaaS、Proofpoint 和手動上傳的範例資料）。
  - 如果每個 CSP 有多個相關聯的租用戶，則儀表板只會顯示來自 Prisma Access、Palo Alto Networks 防火牆以及與特定租用戶相關聯的 Panorama 設備（而非其他來源）的資料。

AIOps for NGFW* - AIOps for NGFW 中可用的儀表板取決於您擁有的是免費還是進階 授權層。

 ©2025 Palo Alto Networks, Inc.

儀表板：建置自訂儀表板

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目 • Prisma SD-WAN	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN 可見性所需的其他授權和先決條件包括： ❑ 在儀表板中解鎖特定 Widget 的授權 ❑ 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

除了預設儀表板之外，您也可以建立自訂儀表板，以使用 Widget 深入瞭解您感興趣的網路區域。Widget 是用來建立儀表板的元件。Widget 會分類並儲存在 Widget 程式庫中。按一下**Dashboards**（儀表板） > **+**，然後從下拉式清單中選取類別以檢視 Widget。Widget 程式庫中可用的 Widget 取決於您的安全服務訂閱。例如，如果你有 AIOps for NGFW Premium 和 Advanced WildFire 授權，您可以檢視和使用 WildFire 類別下的所有 Widget，以建立儀表板。

這些是可用來建立儀表板的 Widget 類別。請參閱下方的連結，查看存取這些類別下的 Widget 所需的授權，並加以瞭解。

- 儀表板：進階威脅防護
- 儀表板：DNS 安全性
- 儀表板：WildFire

建立儀表板

您可以在自訂儀表板中新增最多 10 個 Widget，並為每個使用者建立 10 個自訂儀表板。儀表板和 Widget 可以隨時自訂。您可以自訂 Widget 圖格、說明、顯示或隱藏篩選器、儀表板設定（如版面配置、儀表板名稱和說明），也可以在儀表板中包含篩選器。

STEP 1 | 按一下**Dashboards**（儀表板） > **+**。

STEP 2 | 輸入儀表板的名稱。

©2025 Palo Alto Networks, Inc.

STEP 3 | 從 [Widget Library（Widget 程式庫）] 下拉式清單中選取 Widget 類別。

STEP 4 | 將 Widget 新增至儀表板 - 將滑鼠暫留在 Widget 上方，可以瞭解 Widget。將 Widget 拖放到儀表板畫布上。

您可以將其他 Widget 類別的相同或不同類型的更多 Widget 新增至儀表板畫布。

STEP 5 | 在範例資料與實際資料檢視之間切換，以瞭解儀表板 Widget 的外觀。範例資料可協助您視覺化儀表板的外觀，以及您可以看到的資訊類型。使用實際資料選項，檢視部署的實際資料。

STEP 6 | （選用）您可以在編輯器檢視中自訂儀表板：

- 在儀表板中重新排列 Widget - 選取 Widget，並拖放到畫布中所需的位置。
- 編輯 Widget - 使用每個 Widget 右上角的編輯圖示，來編輯 Widget 設定。可用的設定取決於 Widget，且並非所有 Widget 都相同。例如，您可以編輯 Widget 名稱、說明和選項，以篩選及排序 Widget 中的資料，例如裁定、動作。

您可以在編輯器檢視中編輯 *Widget* 設定，或是儲存儀表板後編輯。

STEP 7 | 儲存儀表板，然後按一下 **Go to see dashboard**（前去查看儀表板）以開啟儀表板。

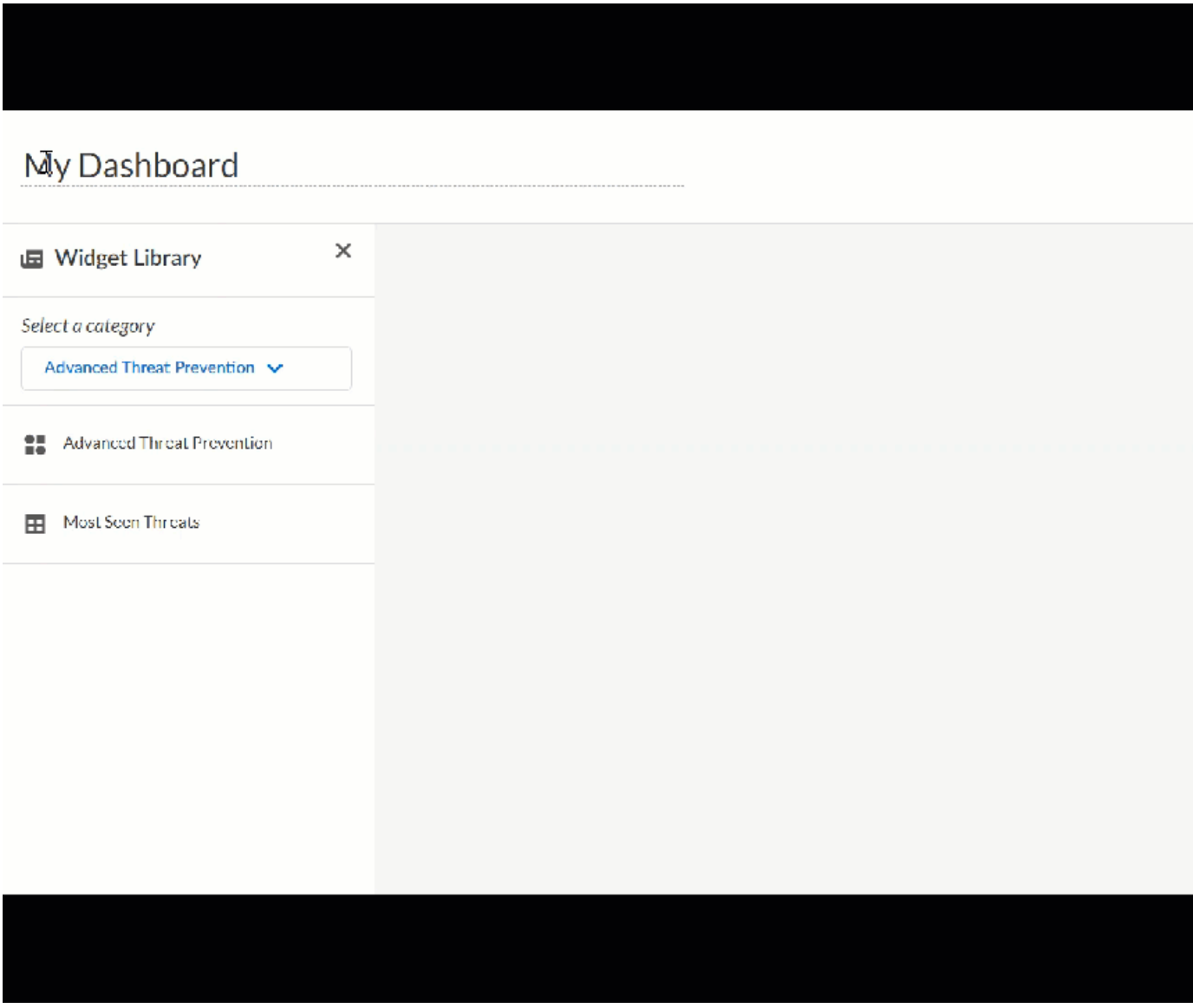
 ©2025 Palo Alto Networks, Inc.

STEP 8 | （選用）儲存儀表板後，您可以：

- 變更要檢視儀表板資料的時間範圍。

  只有在儲存儀表板後，才能變更時間。在編輯器檢視中，時間範圍預設為 24 小時。

- 使用編輯或刪除圖示來修改或刪除自訂儀表板。



©2025 Palo Alto Networks, Inc.

儀表板：裝置健康情況

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 首先，按一下**Dashboards**（儀表板） > **Device Health**（裝置健康情況）。

此儀表板顯示哪些內容？

此儀表板會顯示所有在您的租用戶上線並傳送遙測資料之防火牆的彙總資料。

裝置健康情況儀表板會根據已上線 NGFW 的健康情況分數，顯示部署的累計健康情況狀態和效能。裝置健康情況取決於健康情況分數 (0-100) 的嚴重程度，及其對應的健康情況等級（良好、尚可、不良、嚴重）。健康情況分數會根據開放警示的優先順序、數量、類型和狀態來計算。

如何使用儀表板中的資料？

此儀表板可協助您：

- 查看歷史健康情況分數資料，瞭解您在一段時間內進行的部署改進。
- 減少部署時需要注意的裝置，並優先處理問題加以解決。

©2025 Palo Alto Networks, Inc.

此儀表板不支援報告功能（下載、共用和排程報告）。

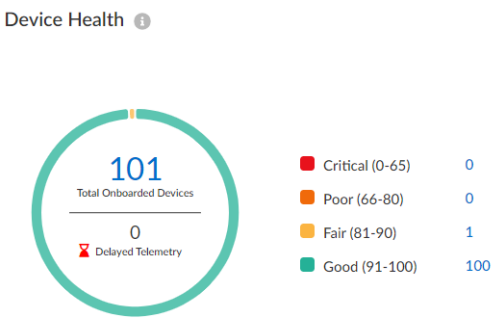
裝置健康情況儀表板：裝置健康情況分數

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 按一下**Dashboards**（儀表板） > **Device Health**（裝置健康情況），以檢視儀表板。

儀表板 Widget 會顯示：

- 已上線的 NGFW 總數。
- 超過 12 小時未傳送遙測資料的裝置數量。
- 部署中已上線裝置的健康情況分數的嚴重性。按一下數字連結，可瞭解裝置詳細資料、裝置健康情況統計資料，以及裝置上需要注意的警示。



裝置健康情況儀表板：裝置統計資料

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 按一下**Dashboards**（儀表板） > **Device Health**（裝置健康情況），以檢視儀表板。

 ©2025 Palo Alto Networks, Inc.

Top Unhealthy | Top Improving | Top Worsening

Health Score	Host Name	Model	SW Version	# Alerts	30 Day Score Change
100 (Good)	Eval60_Atlanta_220_10	PA-220	10.1.4	1	▲ 3
100 (Good)	Eval60_Beijing_220_2	PA-220	10.1.4	0	0
100 (Good)	Eval60_Beijing_220_1	PA-220	10.1.4	1	▲ 49
100 (Good)	Eval60_Boston_220_0	PA-220	10.1.4	0	0
100 (Good)	Eval60_Boston_220_1	PA-220	10.1.4	0	0
100 (Good)	Eval60_Boston_220_10	PA-220	10.1.4	0	0
100 (Good)	Eval60_Boston_220_11	PA-220	10.1.4	0	0
100 (Good)	Eval60_Boston_220_2	PA-220	10.1.4	0	0
100 (Good)	Eval60_Boston_220_3	PA-220	10.1.4	0	0
100 (Good)	Eval60_Boston_220_4	PA-220	10.1.4	0	0

狀況最差

這些是您的部署中健康情況和效能問題最多的裝置。您也可以深入檢視裝置詳細資料和裝置上的警示。修正重大警示，以改善健康情況分數和部署健康情況。

改進程度最大

檢視在 30 天的時段內健康情況分數較裝置目前的健康情況分數有所改善的前 10 個裝置。

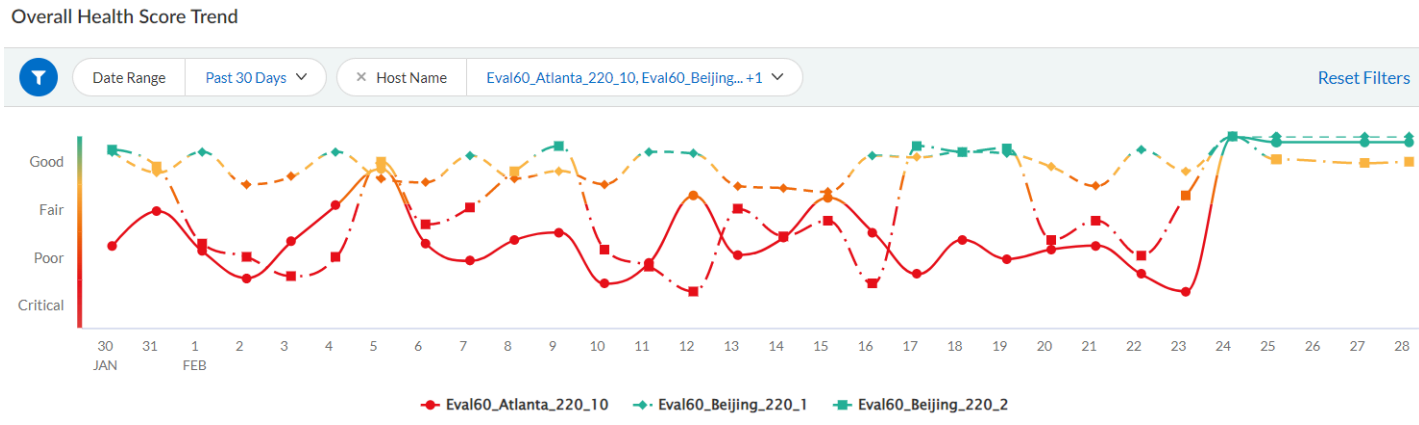
惡化程度最大

檢閱 30 天時間範圍內的裝置健康情況。這些是與裝置目前的健康情況分數相比健康情況分數有所下降的前 10 個裝置。

裝置健康情況儀表板：分數趨勢

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 按一下**Dashboards**（儀表板） > **Device Health**（裝置健康情況），以檢視儀表板。



©2025 Palo Alto Networks, Inc.

圖表中顯示所選時段內部署的健康情況趨勢。將滑鼠暫留在觸發點上方，可瞭解助長健康情況分數嚴重性的裝置。您可以檢視按主機名稱、型號或軟體版本篩選的一或多個裝置的趨勢。

 ©2025 Palo Alto Networks, Inc.

儀表板：執行摘要

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目 • Prisma SD-WAN	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN 可見性所需的其他授權和先決條件包括： ❑ 在儀表板中解鎖特定 Widget 的授權 ❑ 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 首先，按一下**Strata Cloud Manager** > **Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **Executive Summary**（執行摘要）。

此儀表板顯示哪些內容？

此儀表板顯示每個 *Strata Logging Service* 租用戶的彙總資料。

[Executive Summary（執行摘要）] 儀表板會顯示 Palo Alto Networks 安全性訂閱如何為您提供保護。此報告會詳細分析這些訂閱在您的網路中偵測到的惡意活動：**WildFire**、進階威脅防護、進階 **URL** 篩選和企業 **DLP**。此儀表板會顯示其中每項服務的資料，並提供安全服務儀表板的連結，讓您更深入地進一步調查。

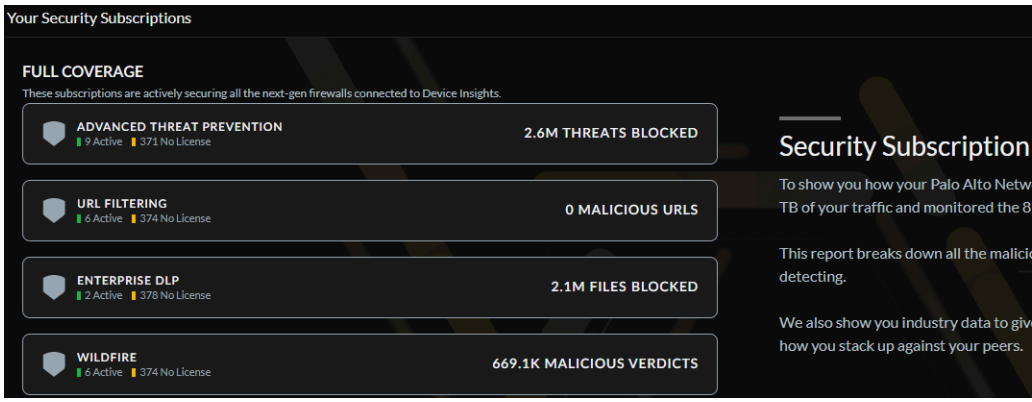
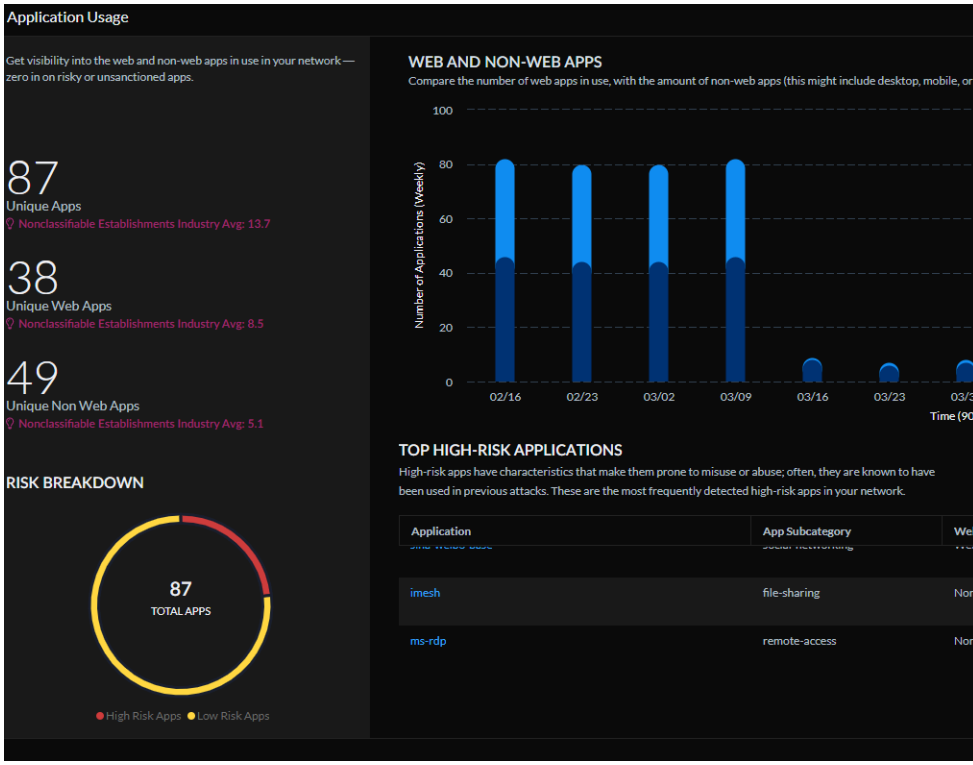
此儀表板支援報告。儀表板右上方若有圖示  ，表示此儀表板支援報告。您可以共用、下載及排程涵蓋此儀表板顯示之資料的報告。

儀表板中的資料可以如何使用？

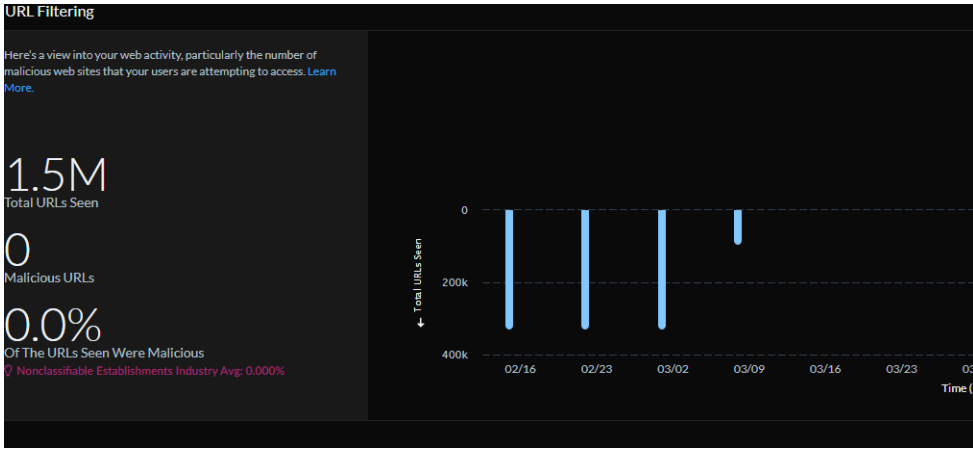
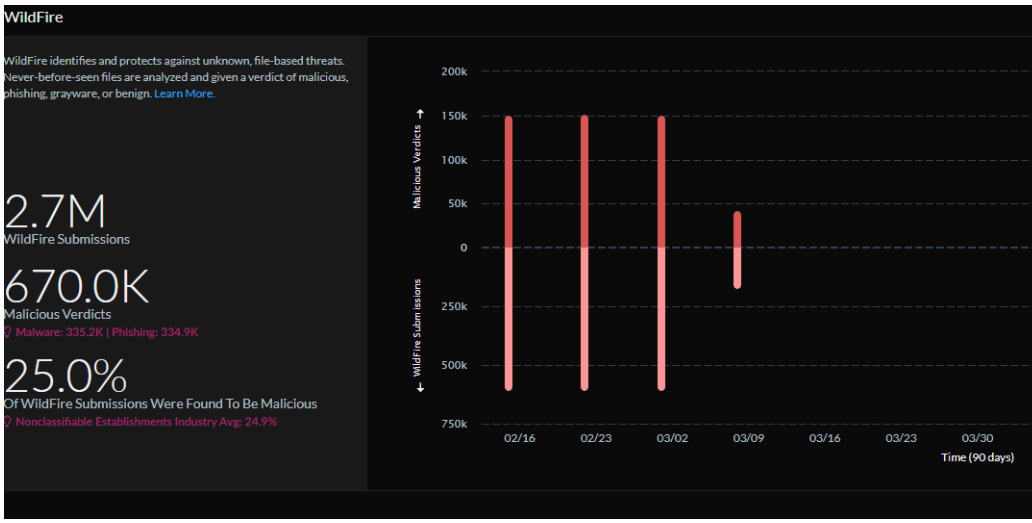
- 檢閱作用中 Palo Alto Networks 訂閱偵測到的所有惡意活動。確認您是否需要修訂訂閱設定或安全性規則設定，以彌補任何安全漏洞。
- 向您顯示產業資料，讓您瞭解目前面臨的威脅態勢，以及您與同業的競爭情況。

此儀表板提供下列資料。

©2025 Palo Alto Networks, Inc.

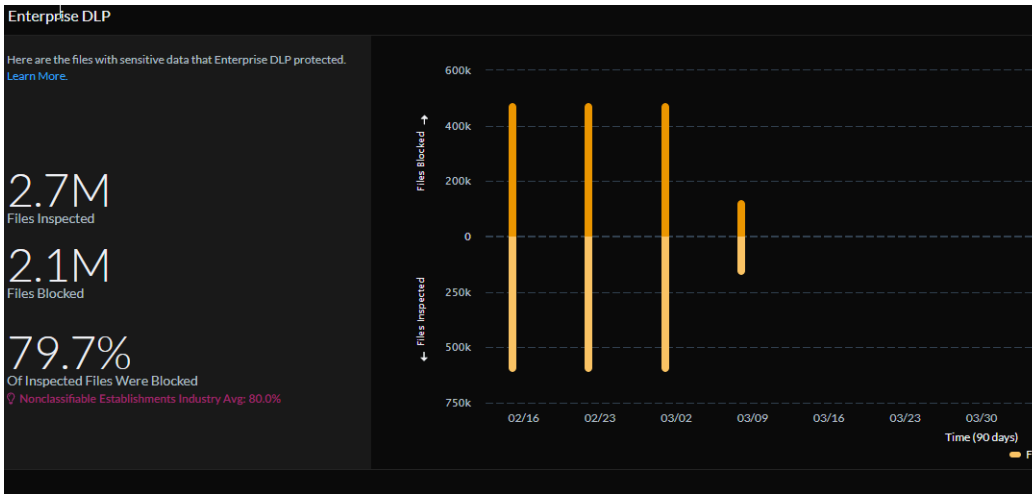
執行摘要儀表板：您的安全性訂閱	此報告會提供您的訂閱所偵測和防止的惡意活動數量： • 高風險應用程式 • 嚴重威脅（入侵、惡意軟體和 C2） • 惡意 Web 活動 • 檔案型威脅（包括前所未見的威脅） • 資料遺失 
執行摘要儀表板：應用程式使用方式	檢閱高風險應用程式的流量日誌，並瞭解如何加強安全性狀態。 
執行摘要儀表板：進階威脅防護	檢查允許最多威脅的安全性政策規則。檢閱這些規則，瞭解可以在何處啟用更嚴格的威脅強制執行。進一步瞭解。

 ©2025 Palo Alto Networks, Inc.

需要進階威脅防護授權。	
執行摘要儀表板：**URL** 篩選 需要進階 *URL* 篩選授權。	檢閱網路中的惡意 Web 活動，尤其是使用者嘗試存取的惡意網站數目。 
執行摘要儀表板：**WildFire** 需要進階 *WildFire* 授權。	此儀表板中的同業資料可讓您瞭解產業的威脅態勢，以及您的安全覆蓋範圍與類似組織的比較。對於您未使用的訂閱也會顯示這項產業資料；這有助於您瞭解是否有任何位置可讓您增加覆蓋範圍，以彌補安全漏洞。 這裡會詳述此儀表板提供的資料類型 - 在此處，您可以看到 WildFire 為了保護您的網路和產業所做的工作。進一步瞭解。# 
執行摘要儀表板：企業 **DLP** 需要企業 *DLP* 授權。	瞭解 Palo Alto Networks 企業 DLP 服務如何藉由強制執行資料安全標準來保護您的資料。此儀表板可讓您深入瞭解 DLP 阻止了最多上傳的應用程式，以及 DLP 在您網路中封鎖的檔案總數。您也可以使用此資料與同業比較，並對您的安全性狀態標準進行基準測試。

 ©2025 Palo Alto Networks, Inc.

檢閱應用程式和來源使用者名稱，以進一步瞭解 DLP 事件的起源並加以管理。



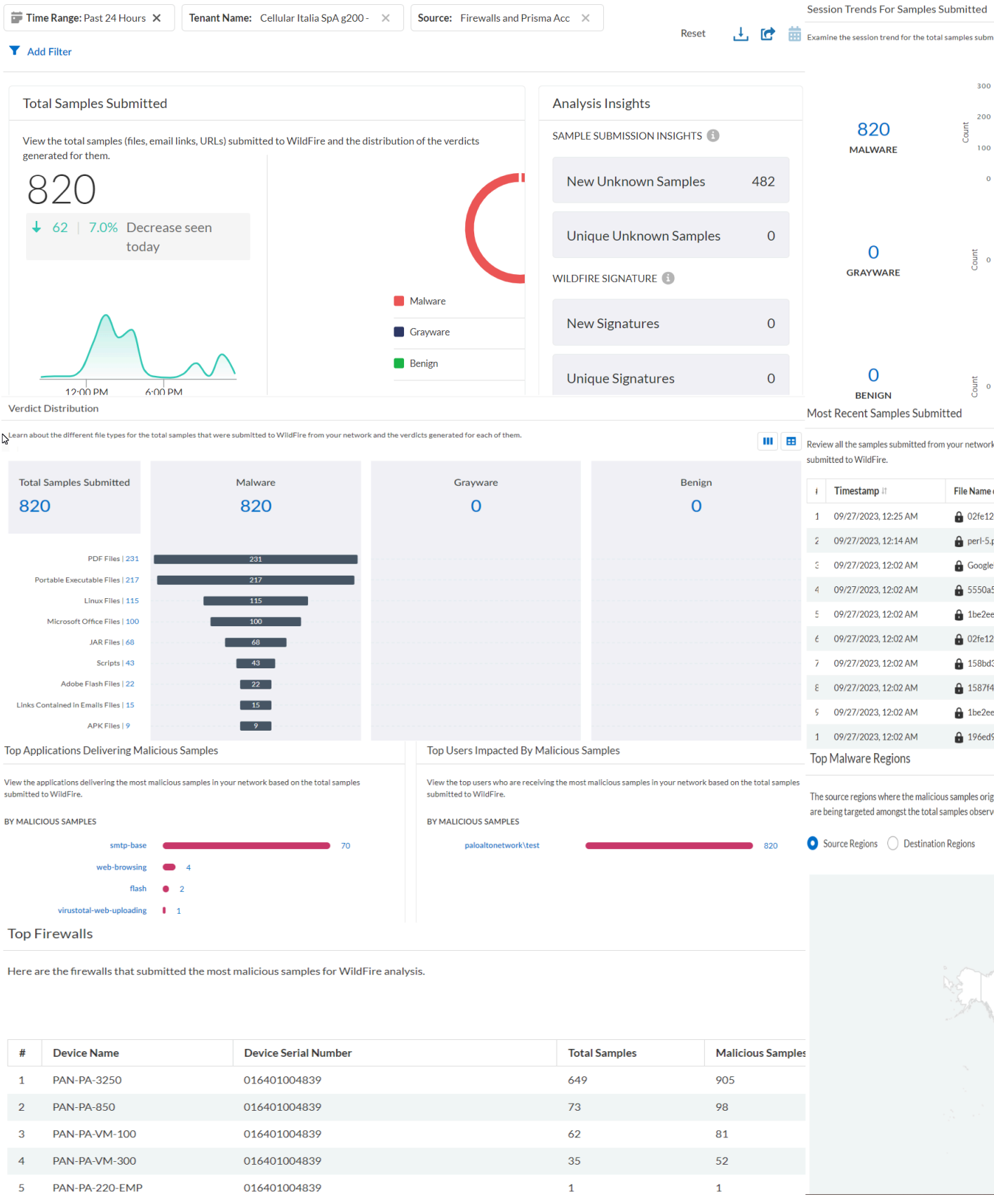
 ©2025 Palo Alto Networks, Inc.

儀表板：WildFire

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 可見性所需的其他授權和先決條件包括： ❑ 有權檢視儀表板的角色 ❑ 進階 WildFire → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 首先，按一下**Strata Cloud Manager** > **Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **WildFire**。

©2025 Palo Alto Networks, Inc.



#	Device Name	Device Serial Number	Total Samples	Malicious Samples
1	PAN-PA-3250	016401004839	649	905
2	PAN-PA-850	016401004839	73	98
3	PAN-PA-VM-100	016401004839	62	81
4	PAN-PA-VM-300	016401004839	35	52
5	PAN-PA-220-EMP	016401004839	1	1

©2025 Palo Alto Networks, Inc.

此儀表板顯示哪些內容？

此儀表板會顯示每個租用戶服務群組 *(TSG)* 的彙總資料。儀表板會顯示與您的租用戶相關聯的 *Prisma Access*、*Palo Alto Networks* 防火牆和 *Panorama* 設備中的資料，前提是您的租用戶與客戶支援入口網站帳戶具有一對一的對應。如果每個客戶支援入口網站有多個相關聯的租用戶，則儀表板不會顯示其他來源的資料。

WildFire 儀表板會顯示 WildFire 如何保護您免受隱藏在檔案和執行檔中的新興網路惡意軟體侵害。此儀表板支援報告。儀表板右上方若有圖示  ，表示此儀表板支援報告。您可以共用、下載及排程涵蓋此儀表板顯示之資料的報告。

儀表板中的資料可以如何使用？

使用此儀表板可以-

- （需要 AIOps for NGFW Premium 授權）監控 WildFire 提交，以及詳細瞭解提交到 WildFire 雲端進行分析的 WildFire 範例。
- 詳盡檢視目標使用者、傳遞檔案的應用程式、提交範例進行分析的防火牆，以及檔案的命令和控制活動中涉及的所有 URL。
- （需要 AIOps for NGFW Premium 授權）檢視 WildFire 日誌和分析報告，並根據報告修訂部署的 WildFire 設定。

WildFire 儀表板：篩選器

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 可見性所需的其他授權和先決條件包括： ❑ 有權檢視儀表板的角色 ❑ 進階 WildFire → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

WildFire 儀表板提供了下列篩選選項，縮小儀表板中特定資料的範圍。

- 時間範圍 - 從 過去 **24** 小時、過去 **7** 天、過去 **30** 天或自訂時間範圍中選取，以顯示特定時間範圍內的資料。

©2025 Palo Alto Networks, Inc.

- 租用戶名稱 - 顯示了儀表板資料的租用戶。
- 來源 - 儀表板資料的範圍來自 Prisma Access 和 Palo Alto Networks 防火牆。
- 範例 - 從公用或私人選項中選取，以檢視從 Wildfire 公共雲端或私人雲端環境提交的資料。
- 裁定 - 檢視在 WildFire 分析中識別為良性、惡意軟體或灰色軟體的範例。
- 動作 - 從允許或封鎖選項中選取，以顯示您的政策規則允許或封鎖的 WildFire 範例。
- 檔案類型 - 根據 WildFire 所分析之範例的檔案類型檢視資料。瞭解 WildFire 分析支援的檔案類型。
- 檔案雜湊 - 檢視 WildFire 所分析之檔案雜湊的資料。以下列出 WildFire 針對每個已分析檔案產生的雜湊版本：
  - **SHA-1**—顯示檔案的 SHA-1 值。
  - **SHA-256**—顯示檔案的 SHA-256 值。
  - **MD5**—顯示檔案的 MD5 資訊。
- 應用程式名稱 - 根據應用程式傳遞的範例篩選資料。
- 來源區域 - 篩選以檢視從特定位置傳送的範例。
- 目標區域 - 篩選以檢視在特定位置接收到的範例。
- 使用者名稱- 輸入使用者名稱以篩選要在您的網路中傳遞範例之使用者的資料。
- 裝置序號 - 篩選提交範例以進行 WildFire 分析之裝置的資料。

WildFire 儀表板：已提交的範例總數

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 可見性所需的其他授權和先決條件包括： ❑ 有權檢視儀表板的角色 ❑ 進階 WildFire → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 首先，按一下**Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **WildFire**，以檢視儀表板。

 ©2025 Palo Alto Networks, Inc.

在選取的時段內提交以進行 WildFire 分析的範例總數。此 Widget 會顯示從每個來源提交的範例數目，以及為範例產生的裁定。此 Widget 也會顯示提交以進行 WildFire 分析的範例數尖峰。調查惡意軟體範例數的尖峰，並採取行動以減輕威脅對網路的影響。

WildFire 儀表板：分析洞察

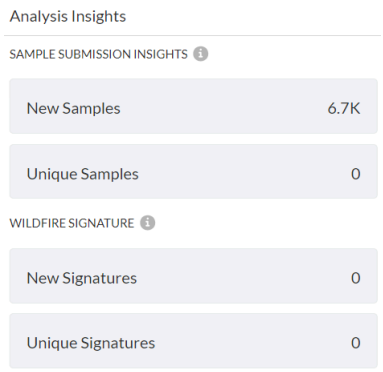
這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 可見性所需的其他授權和先決條件包括： ❑ 有權檢視儀表板的角色 ❑ 進階 WildFire → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 首先，按一下**Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **WildFire**，以檢視儀表板。

深入瞭解從您的網路提交的唯一 WildFire 範例，和產生的特徵碼。使用這些資料，瞭解在選取的時間範圍內僅在您的網路中觀察到的新威脅，以及您的網路受到產生的特徵碼保護的次數。

- 唯一的未知範例 - 從您的網路提交至 WildFire、且僅在您的網路中發現、WildFire 先前未知、在其他公用或私人來源中無法使用的範例數目。
- 新的未知範例 - 從您的網路提交至 WildFire、且 WildFire 先前未知（具有不同的 sha256）的新範例數目。
- 唯一特徵碼 - 從範例產生而在您的環境中具獨特性的特徵碼數目。
- 新特徵碼 - WildFire 根據您上傳的所有範例建立的新特徵碼數目。

 ©2025 Palo Alto Networks, Inc.



WildFire 儀表板：已提交範例的工作階段趨勢

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 可見性所需的其他授權和先決條件包括： ❑ 有權檢視儀表板的角色 ❑ 進階 WildFire → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 首先，按一下**Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **WildFire**，以檢視儀表板。

查看從您的網路提交到 WildFire 的所有範例有何趨勢，以及這些範例的裁定。您可以對這些範例執行 IOC 搜尋，以瞭解範例在您網路中的歷程記錄，以及範例的全域分析結果。

 ©2025 Palo Alto Networks, Inc.

WildFire 儀表板：裁定分佈

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 可見性所需的其他授權和先決條件包括： ❑ 有權檢視儀表板的角色 ❑ 進階 WildFire → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 首先，按一下**Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **WildFire**，以檢視儀表板。

進一步瞭解 WildFire 在您的網路中第一次偵測到的全新範例的裁定。專注於最常隱藏惡意軟體的範例類型。按一下連結以進一步瞭解範例。

 ©2025 Palo Alto Networks, Inc.

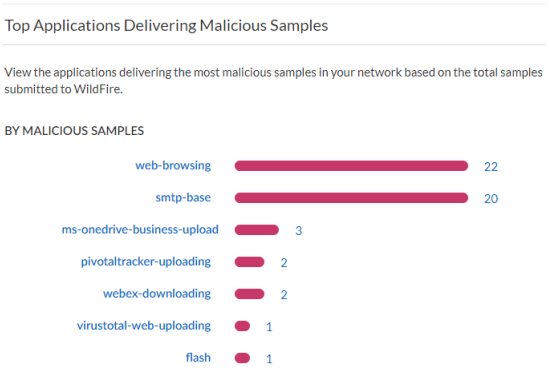
WildFire 儀表板：傳遞惡意範例的最高排名應用程式

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 可見性所需的其他授權和先決條件包括： ❑ 有權檢視儀表板的角色 ❑ 進階 WildFire → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 首先，按一下**Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **WildFire**，以檢視儀表板。

檢閱在您的網路中傳遞最多惡意範例的應用程式的詳細資料。按一下惡意範例計數，可瞭解更多關於範例的資訊。

 ©2025 Palo Alto Networks, Inc.

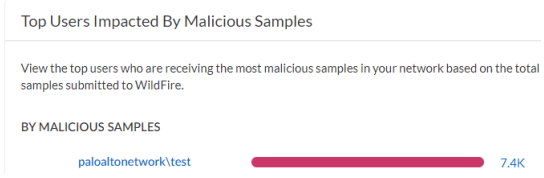


WildFire 儀表板：受惡意範例影響最大的使用者

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 可見性所需的其他授權和先決條件包括： ❑ 有權檢視儀表板的角色 ❑ 進階 WildFire → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 首先，按一下**Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **WildFire**，以檢視儀表板。

這會顯示您的網路中最常用來傳遞惡意範例的使用者帳戶。按一下使用者名稱，可調查使用者活動模式。



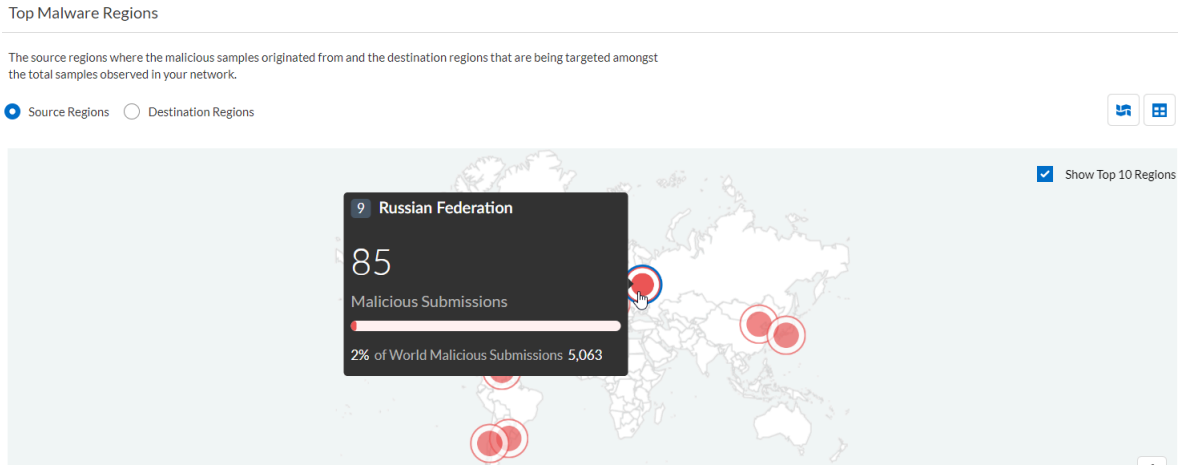
 ©2025 Palo Alto Networks, Inc.

WildFire 儀表板：最高排名的惡意軟體區域

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 可見性所需的其他授權和先決條件包括： ❑ 有權檢視儀表板的角色 ❑ 進階 WildFire → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 首先，按一下**Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **WildFire**，以檢視儀表板。

檢閱您的網路上成為惡意範例的來源或目的地的位置。您可以用地圖或表格格式檢視來源和目標區域的範例計數。使用此功能，惡意軟體的目標區域和惡意軟體攻擊的類型都可縮小範圍。



WildFire 儀表板：最高排名的防火牆

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權：

©2025 Palo Alto Networks, Inc.

這可在何處使用？	我需要哪些內容？
	❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 可見性所需的其他授權和先決條件包括： ❑ 有權檢視儀表板的角色 ❑ 進階 WildFire → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 首先，按一下**Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **WildFire**，以檢視儀表板。

檢視提交最多惡意範例進行 WildFire 分析的防火牆。檢閱這些防火牆以追蹤受影響的端點，並重新設定政策規則以減輕威脅，並從來源遏制惡意檔案。

Top Firewalls

Here are the firewalls that submitted the most malicious samples for WildFire analysis.

#	Device Name	Device Serial Number	Total Samples	Malicious Samples
1	PAN-PA-3250	016401004839	4866	6947
2	PAN-PA-5220-AC	016401004839	1168	1715
3	PAN-PA-VM-300	016401004839	619	1054
4	PAN-PA-VM-100	016401004839	673	1017
5	PAN-PA-850	016401004839	39	56
6	PAN-PA-VM-500-E60	016401004839	5	6
7	PAN-PA-220-EMP	016401004839	3	5
8	PAN-PA-5260-AC	016401004839	1	1

©2025 Palo Alto Networks, Inc.

儀表板：DNS 安全性

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 可見性所需的其他授權和先決條件包括： ❑ 有權檢視儀表板的角色 ❑ DNS 安全性或進階 DNS 安全性 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 首先，按一下**Strata Cloud Manager** > **Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **DNS Security**（**DNS** 安全性）。

此儀表板顯示哪些內容？

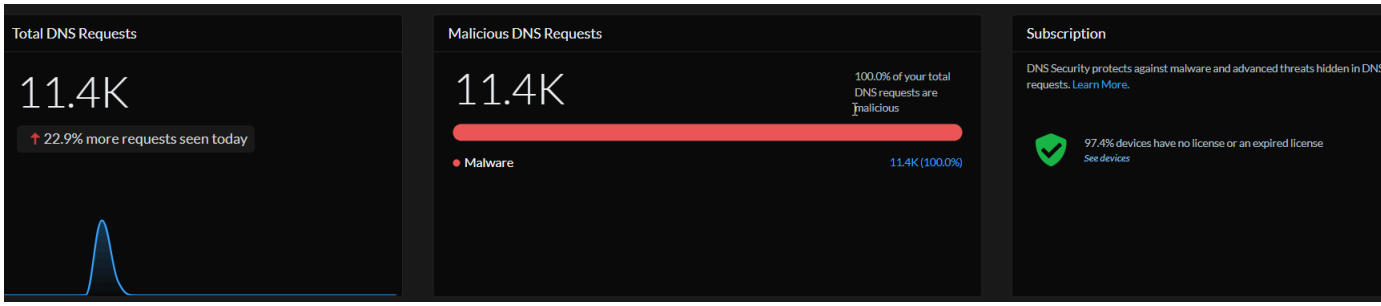
此儀表板會顯示每個租用戶服務群組 *(TSG)* 的彙總資料。此儀表板會顯示與您的租用戶相關聯的 *Prisma Access*、*Palo Alto Networks* 防火牆和 *Panorama* 設備的資料。

新的 DNS Security（DNS 安全性）儀表板會顯示您的 DNS 安全性訂閱如何保護您免受使用 DNS 的進階威脅和惡意軟體侵害。您也可以按時間範圍、採取的動作、網域、解析程式 IP 和 DNS 類別，篩選儀表板上顯示的資訊。有資料顯示在儀表板上的來源和租用戶名稱，會顯示在「租用戶名稱」和「來源」篩選器中。您可以檢視：DNS 要求統計資料和趨勢

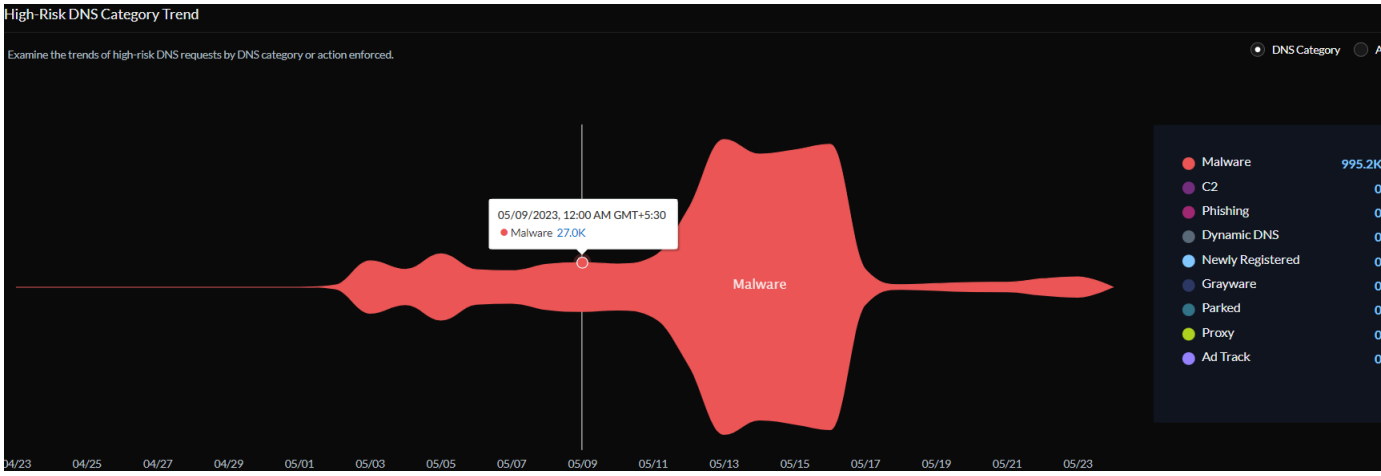
- **DNS** 要求總數 - 顯示 DNS 安全性所處理的 DNS 要求總數。此折線圖會根據使用者定義的時間範圍繪製 DNS 要求數量。指定自訂時間範圍會相應地更新折線圖。
- 惡意 **DNS** 要求 - 顯示堆疊長條圖，內含歸類為惡意的 DNS 要求。按一下數字連結，可檢視 DNS 要求的詳細資料。

©2025 Palo Alto Networks, Inc.

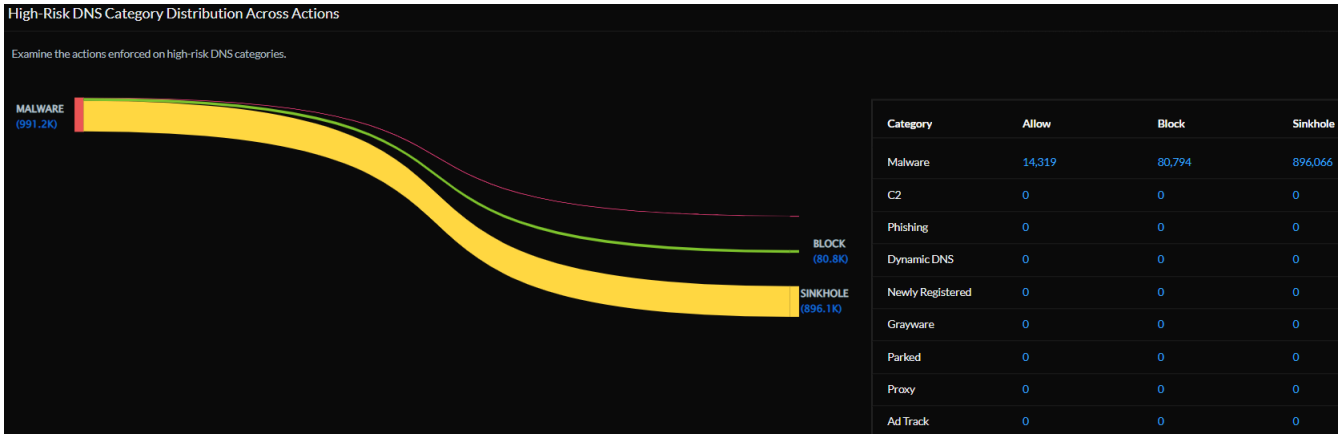
- 訂閱 - 顯示網路中具備作用中 DNS 安全性訂閱的裝置數量。此外也顯示未配備 DNS 安全性或訂閱已過期的裝置百分比，以及完整清單的連結。



- 高風險 **DNS** 類別趨勢 - 根據 DNS 類別或對其採取的動作，檢查高風險 DNS 要求的趨勢。將滑鼠暫留在特定流程上方可開啟快顯視窗，顯示要求的數目或強制執行的動作類型。

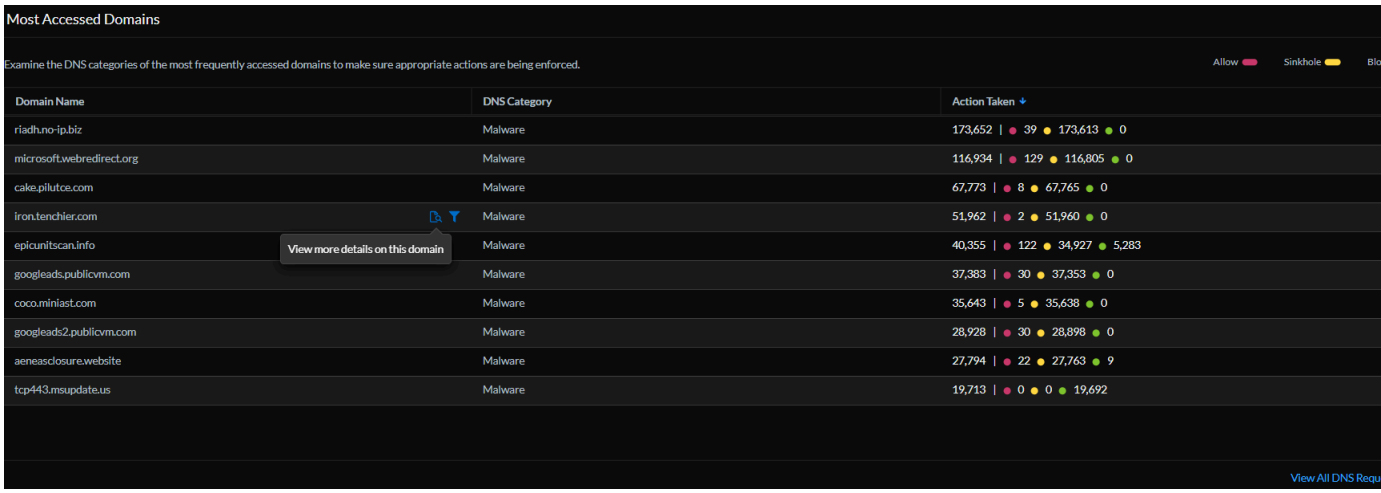


- 各動作間的高風險 **DNS** 類別分佈 - 檢查防火牆對特定高風險 DNS 類別採取的動作。

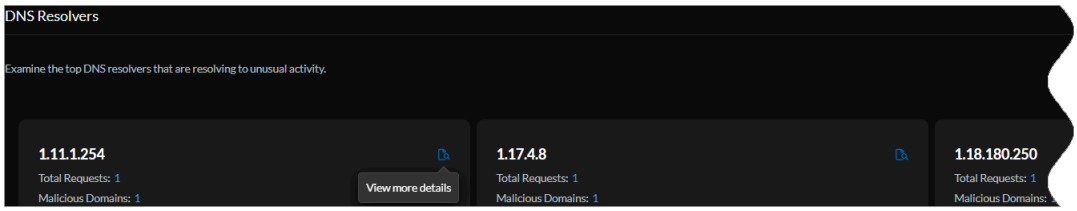


 ©2025 Palo Alto Networks, Inc.

- 最常存取的網域 - 列出您的網路中前 10 個最常要求的網域，以及 DNS 類別和採取的動作。您可以對網域檢視更多詳細資料和相關日誌。選取 **View All DNS Requests**（檢視所有 **DNS** 要求），以取得已存取之網域的完整清單。



- **DNS** 解析程式 - 監控網路中惡意和可疑的 DNS 解析活動。檢視最常解析為惡意網域的 DNS 解析程式，以及解析異常低量 DNS 要求的解析程式。按一下搜尋圖示，可針對構件（IP 位址）檢視更多詳細資料。您可以檢視網路中構件的歷程記錄，以及全域分析結果。



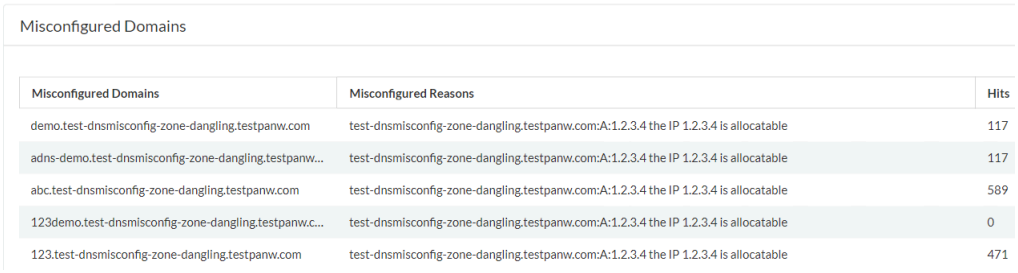
- 造訪惡意網域的使用者 - 檢查您的網路上試圖解析惡意 URL 的主機名稱或網域的主機。
- （需要進階 **DNS** 安全授權）被劫持的網域- 列出由進階 DNS 安全性判定的被劫持網域。對於每個項目，都有一個分類原因和基於來源 IP 的流量命中計數。

Hijacked Domains

Hijacked	Hits
xyz.test-ipv4-wildcard.hijacking.testpanw.com	117
www.test-ipv4-wildcard.hijacking.testpanw.com	118
www.test-cname-rrname-sub-wc.hijacking.testpanw.com	353
test.test-ipv4-wildcard.hijacking.testpanw.com	118
test-ipv6.hijacking.testpanw.com	469
test-ipv4.hijacking.testpanw.com	472
test-cname-rrname.hijacking.testpanw.com	234
test-cname-rrname-wc.hijacking.testpanw.com	117
qpwc.test-ipv4-wildcard.hijacking.testpanw.com	118

 ©2025 Palo Alto Networks, Inc.

- （需要進階 **DNS** 安全性授權）設定錯誤的網域- 列出與使用者指定的面向公眾父系網域相關聯的不可解析網域。對於每個項目，都有一個設定錯誤原因和基於來源 **IP** 的流量命中計數。


Misconfigured Domains

Misconfigured Domains	Misconfigured Reasons	Hits
demo.test-dnsmisconfig-zone-dangling.testpanw.com	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	117
adns-demo.test-dnsmisconfig-zone-dangling.testpanw...	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	117
abc.test-dnsmisconfig-zone-dangling.testpanw.com	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	589
123demo.test-dnsmisconfig-zone-dangling.testpanw.c...	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	0
123.test-dnsmisconfig-zone-dangling.testpanw.com	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	471

此儀表板支援報告。儀表板右上方若有圖示  ，表示此儀表板支援報告。您可以共用、下載及排程涵蓋此儀表板顯示之資料的報告。

儀表板中的資料可以如何使用？

此儀表板可協助您：

- 檢查 DNS 要求的處理和分類方式
- 深入瞭解 DNS 型威脅
- 透過進階 DNS 安全性偵測來自被劫持和錯誤設定之網域的 DNS 要求

©2025 Palo Alto Networks, Inc.

儀表板：AI 執行階段安全性

Strata Cloud Manager (SCM) 控管中心儀表板提供部署在叢集和 VM 中的雲端工作負載的合併檢視，例如 Pod、模型、應用程式、VM 和命名空間。

這可在何處使用？	我需要哪些內容？
• AI 執行階段安全性	❑ 啟動您的 AI 執行階段安全性授權 ❑ AI 執行階段安全性設定先決條件 ❑ 在 SCM 中上線並啟動雲端帳戶

探索雲端資源

在 SCM 中將您的雲端帳戶成功上線並啟動您的服務帳戶後，SCM 儀表板提供您的雲端工作負載的統合即時資產探索。

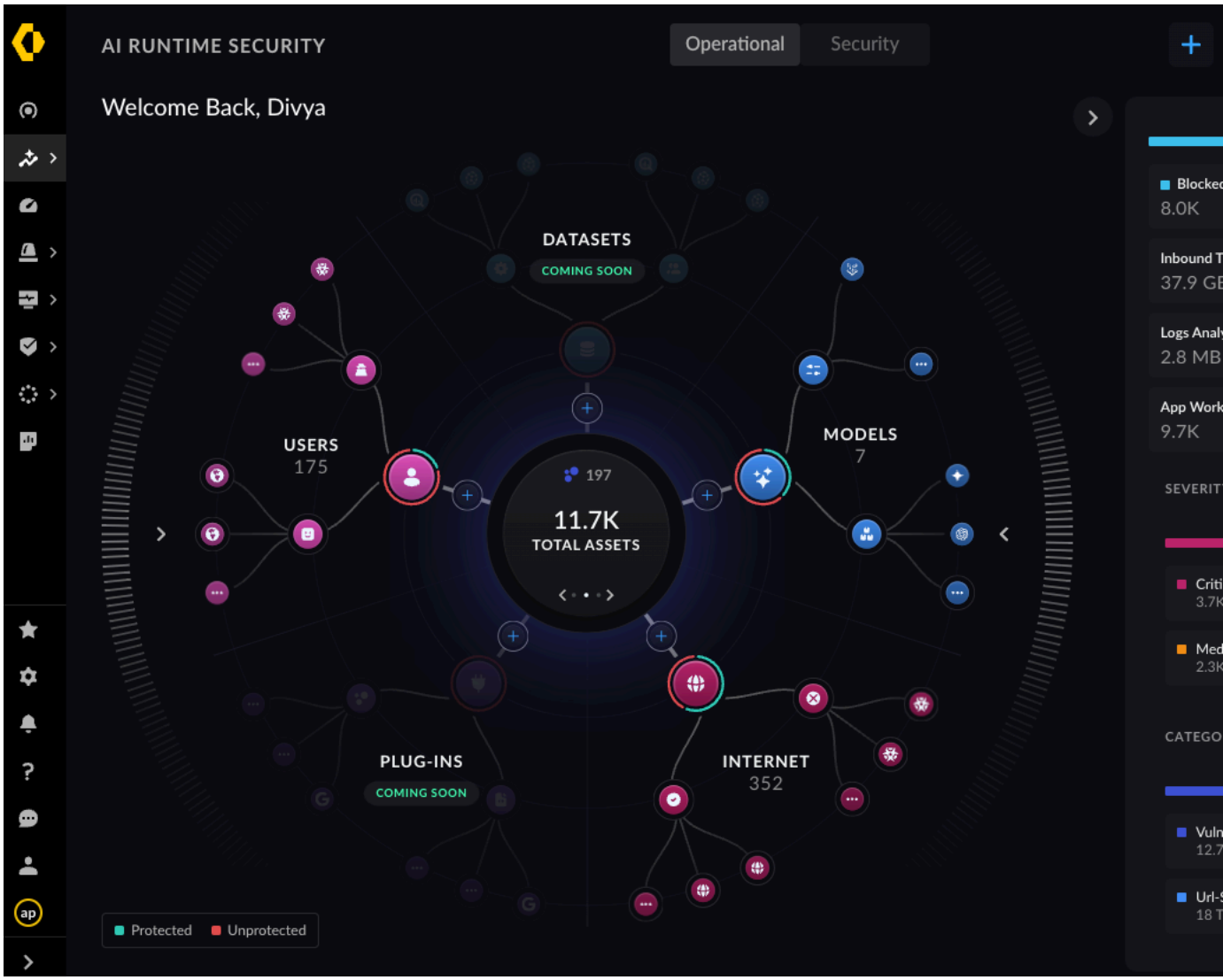
SCM 中的雲端應用程式控管中心會在 **Insights**（洞察） → **AI Runtime Security**（執行階段安全性）底下提供了可操作的洞察，以供探索您已上線的雲端帳戶中所有的雲端資產。

SCM 儀表板上的資產探索分類為操作檢視和安全性檢視。

探索會根據威脅急迫性和風險類別（例如弱點偵測、URL 安全性和提示插入）顯示威脅明細。

©2025 Palo Alto Networks, Inc.

1. 操作檢視是以下內容的彙總檢視：
    1. 在已上線的雲端環境中探索到的資產總數和明細
    2. 流量 - 受 AI 執行階段安全執行個體保護和未保護
    3. 應用程式工作負載（容器、無伺服器函數和 VM）
    4. 正在查詢的 AI 模型
    5. 存取網際網路目的地的使用者應用程式
    6. 從外部應用程式存取的應用程式使用者應用程式
    7. 輸入和輸出流量統計資料



 ©2025 Palo Alto Networks, Inc.

2. 在安全性檢視中：
   1. 您可以新增（"+" 圖示）AI 執行階段安全性執行個體，以保護在操作檢視中識別為未受保護的網路流量。
   2. 如果已有 AI 執行階段安全性執行個體保護存在，則可透過可用的 AI 執行階段安全性執行個體重新導向未受保護的流量。

接下來，偵測使用者應用程式、AI 模型與網際網路之間有風險的網路流量路徑。請參閱 AI 流量網路風險分析和部署 AI 執行階段安全性執行個體，以監控及保護您的雲端網路架構。

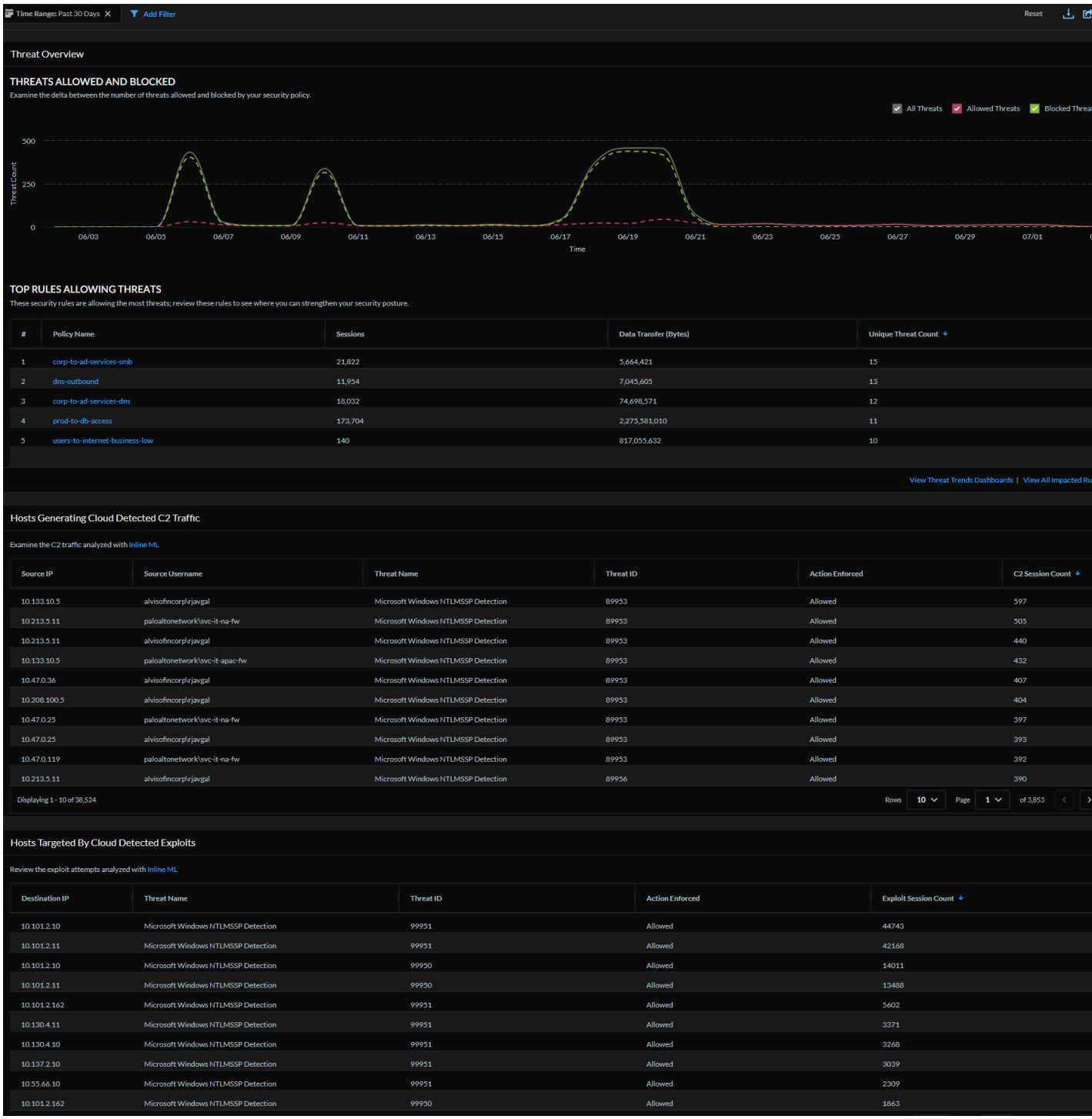
 ©2025 Palo Alto Networks, Inc.

儀表板：進階威脅防護

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 可見性所需的其他授權和先決條件包括： ❑ 有權檢視儀表板的角色 ❑ 威脅防護或進階威脅防護 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 首先，按一下 **Strata Cloud Manager** > **Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **Advanced Threat Prevention**（進階威脅防護）。

©2025 Palo Alto Networks, Inc.



此儀表板顯示哪些內容？

此儀表板顯示每個 *Strata Logging Service* 租用戶的彙總資料。

進階威脅防護儀表板可讓您深入瞭解在網路中偵測到的威脅，並找出強化安全性狀態的機會。偵測威脅時，會使用從各種 Palo Alto Networks 服務收集到的惡意流量資料所產生的內嵌雲端分析模

 ©2025 Palo Alto Networks, Inc.

型和威脅特徵碼。此儀表板會針對允許和封鎖的威脅提供時間軸檢視，並列出產生雲端偵測 C2 流量的主機，以及雲端偵測入侵所鎖定的主機。

此儀表板支援報告。儀表板右上方若有圖示  ，表示此儀表板支援報告。您可以共用、下載及排程涵蓋此儀表板顯示之資料的報告。

如何使用儀表板中的資料？

使用此儀表板：

- 檢視網路流量中的威脅
- 分析威脅工作階段以提升政策規則的準確性
- 深入瞭解內嵌雲端分析所偵測到的即時威脅
- 從日誌和雲端報告中獲取關於威脅的內容，並使用這項資料改善您的事件回應程序。

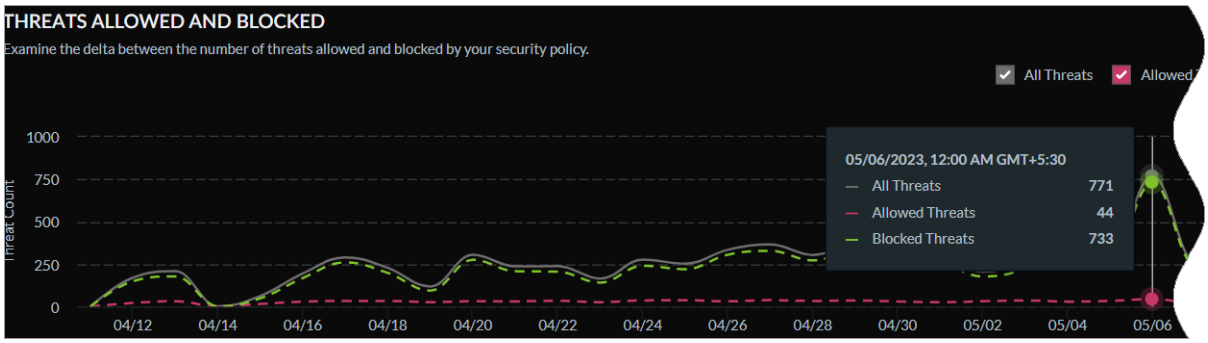
進階威脅防護儀表板：威脅概要

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 可見性所需的其他授權和先決條件包括： ❑ 有權檢視儀表板的角色 ❑ 威脅防護或進階威脅防護 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 按一下**Strata Cloud Manager** > **Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **Advanced Threat Prevention**（進階威脅防護），以檢視儀表板。

比較安全性規則允許和封鎖的威脅有何差異。

 ©2025 Palo Alto Networks, Inc.

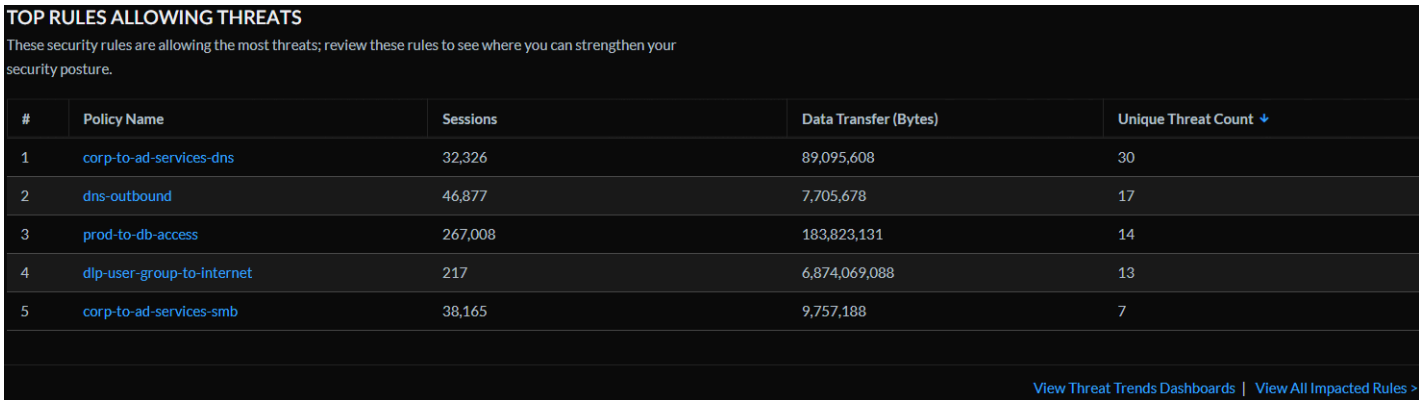


進階威脅防護儀表板：最常允許威脅的規則

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 可見性所需的其他授權和先決條件包括： ❑ 有權檢視儀表板的角色 ❑ 威脅防護或進階威脅防護 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 按一下**Strata Cloud Manager** > **Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **Advanced Threat Prevention**（進階威脅防護），以檢視儀表板。

檢查符合安全性政策規則的威脅工作階段，並確認是否需要修改政策規則以強化安全性狀態。您可以在 Activity Insights（活動洞察）中進一步分析威脅和比對規則。



 ©2025 Palo Alto Networks, Inc.

欄	說明
政策名稱	允許對應威脅的安全性政策規則。
工作階段	符合安全性政策規則的威脅工作階段數目。
資料傳輸 (位元組)	透過符合安全性政策規則的工作階段流動的資料量。
獨特威脅計數	符合安全性政策規則的威脅數目。

進階威脅防護儀表板：產生雲端偵測 C2 流量的主機

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 可見性所需的其他授權和先決條件包括： ❑ 有權檢視儀表板的角色 ❑ 威脅防護或進階威脅防護 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 按一下**Strata Cloud Manager** > **Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **Advanced Threat Prevention**（進階威脅防護），以檢視儀表板。

檢查負責產生命令和控制 (C2) 流量的來源 IP 與使用者。進階威脅防護會使用雲端式引擎和內嵌雲端分析來偵測及分析流量中的未知 C2 和弱點。按一下來源 IP 旁的搜尋圖示，檢閱與來源 IP 相關的使用模式。日誌檢視器的內容相關式連結有助於分析威脅工作階段，下載封包擷取和雲端報告以獲取更多內容，並利用 Palo Alto Networks 威脅分析資料，改進您的事件回應程序。

進階威脅防護儀表板：遭到雲端偵測的入侵鎖定的主機

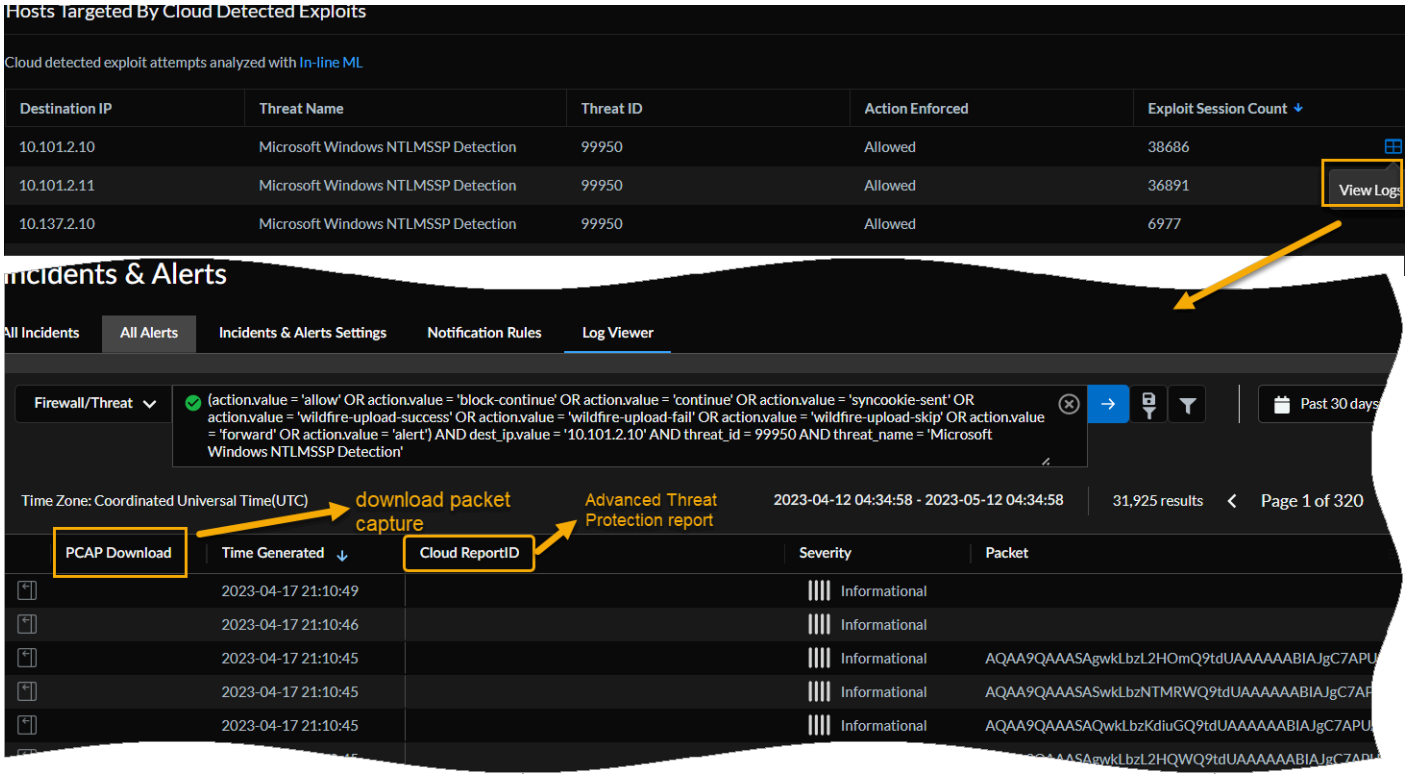
這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access

©2025 Palo Alto Networks, Inc.

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 可見性所需的其他授權和先決條件包括： ❑ 有權檢視儀表板的角色 ❑ 威脅防護或進階威脅防護 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 按一下**Strata Cloud Manager** > **Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **Advanced Threat Prevention**（進階威脅防護），以檢視儀表板。

這些是遭到弱點入侵鎖定的 IP。進階威脅防護會使用雲端式引擎和內嵌雲端分析來偵測及分析此流量。將游標暫留在目的地 IP 位址上方，然後按一下搜尋圖示，以檢閱與目的地 IP 相關的使用模式。檢視日誌以取得威脅的內容。從日誌下載雲端報告和封包擷取以取得額外的內容，並使用 Palo Alto Networks 威脅分析資料和威脅情報來改善事件回應程序。

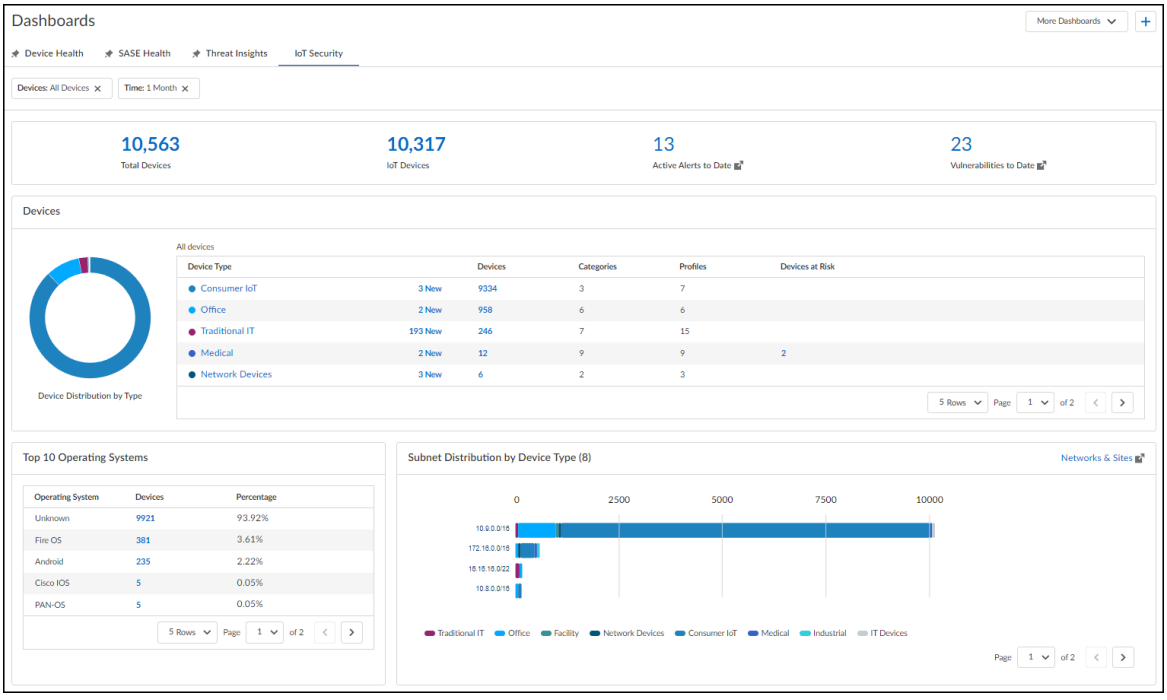


 ©2025 Palo Alto Networks, Inc.

儀表板：IoT Security

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 可見性所需的其他授權和先決條件包括： ❑ 有權檢視儀表板的角色 ❑ IoT Security → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

首先，選取**Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **IoT Security**。



此儀表板顯示哪些內容？

IoT Security 儀表板提供網路上的裝置、其裝置設定檔和作業系統，及其如何按裝置類型分佈於子網路間的相關資訊。對於進階 IoT Security 產品（Enterprise IoT Security Plus、Industrial IoT

©2025 Palo Alto Networks, Inc.

Security 或 Medical IoT Security），IoT Security 儀表板還會顯示迄今為止的作用中警示總數和迄今為止的弱點數。

藍色格式的文字具互動性。點選時會有以下行為：

- 摘要（位於頂端）– **Total Devices**（裝置總數）和 **IoT Devices**（IoT 裝置）的連結，可前往**Monitor**（監控） > **Assets**（資產）頁面，該處套用了篩選以顯示所有裝置或所有 IoT 裝置的詳細目錄。「迄今為止的作用中警示」和「迄今為止的作用中弱點」的藍色文字會在您的 IoT Security 入口網站中開啟對應的頁面。（沒有警示或弱點時，數字會顯示為 0，且沒有連結。）
- 裝置 – 按一下圖表中的部分或 [Device Type（裝置類型）] 欄中的項目，可放大查看所選類型中的裝置類別，並從該處查看所選類別中的裝置設定檔。按一下圖表內的 **back**（返回），或按一下表格上方的階層連結，重新縮小較更廣泛的裝置分類層級。

  [Devices（裝置）] 和 [Devices at Risk（有風險的裝置）] 欄中的數字會連結至**Monitor**（監控） > **Assets**（資產）頁面。Strata Cloud Manager 會自動套用篩選器以顯示符合所選欄和列的裝置，可以是裝置類型、類別名稱或設定檔名稱，具體取決於目前顯示的層級。

  有時您會看到 *IoT Security* 在網路上偵測到新裝置數量。這些數字會出現在 *[Devices*（裝置）*]* 欄中的數字左側。*IoT Security* 如果在儀表板頂端設定的時間篩選器內首次在網路上偵測到裝置，就會將裝置視為「新」裝置。
- 最高排名的 10 個作業系統 – [Devices（裝置）] 欄中的數字會連結至**Monitor**（監控） > **Assets**（資產）頁面，並套用篩選器而僅顯示具有所選作業系統的裝置。
- 按裝置類型顯示的子網路分佈 - 將游標暫留在子網路列上方，可查看子網路中按裝置類型分組的裝置數目。這些資訊可協助您確定是否在相同子網路中混合了太多不相關的裝置類型。例如，如果您在一個子網路中看到設施、工業和消費性 IoT 裝置，您可能會想要將各類型的裝置劃分到各自的個別子網路中。按一下 **Networks & Sites**（網路與站台）會啟動新的瀏覽器視窗，並在 IoT Security 入口網站中開啟**Networks**（網路） > **Networks and Sites**（網路與站台） > **Networks**（網路）。

此儀表板中的資料可以如何使用？

使用此儀表板中的資料，瞭解網路上的裝置：

篩選器（位於頁面頂端）

- 按裝置類型和時段（過去的年、月、週、日或小時）篩選儀表板中顯示的資料，以查看相關裝置的資料。

摘要（位於儀表板頂端）

- 查看網路上處於作用中狀態的裝置總數（由裝置類型和時間篩選器決定）。
- 在作用中裝置總數中，確認有多少個是 IoT 裝置。
- 藉由查看迄今為止偵測到的作用中警示和弱點數目，瞭解裝置運作的安全性態勢。

裝置

- 瞭解各種裝置類型的裝置數量，並深入瞭解各種裝置類別、乃至於各種裝置設定檔中的裝置數量。藉由各種日益精細的裝置分類層級，瞭解有重大風險的裝置數量，及所屬的裝置類型。

10 大作業系統

 ©2025 Palo Alto Networks, Inc.

- 從作業系統被 IoT Security 偵測到的所有裝置中，查看最常見的 10 個作業系統、使用各種作業系統的裝置數量，及其百分比為何。

按裝置類型顯示的子網路分佈

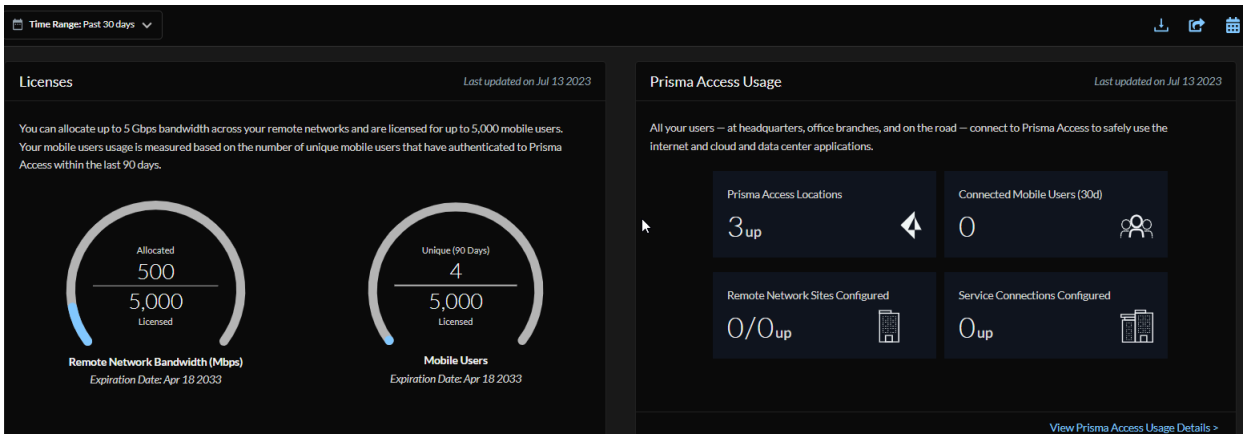
- 查看不同的裝置類型如何分佈在整個網路的子網路中。如果您發現相同子網路中混合了多種裝置類型，請考慮將其劃分到各自的個別子網路中。

 ©2025 Palo Alto Networks, Inc.

儀表板：Prisma Access

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	其中一個： ❑ Prisma Access 授權 ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 首先，按一下**Strata Cloud Manager** > **Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **Prisma Access**。



此儀表板顯示哪些內容？

瞭解如何利用授權提供的功能，並從高層級檢視 Prisma Access 環境的健康情況和效能。

Prisma Access 使用情況資料包括：

- Prisma Access 使用情況概要 — 您的授權、Prisma Access 位置，以及行動使用者容量和/或頻寬使用率
- 行動使用者和遠端網路的最高排名 Prisma Access 位置
- 遠端網路和服務連線站台的整體頻寬消耗，以及耗用量最高的遠端網路和服務連線站台
- 通道中斷連線趨勢，包括受影響最大的通道

此儀表板會顯示每個 *Prisma Access* 租用戶的彙總資料。

此儀表板支援報告。儀表板右上方若有圖示  ，表示此儀表板支援報告。您可以共用、下載及排程涵蓋此儀表板顯示之資料的報告。

 ©2025 Palo Alto Networks, Inc.

儀表板中的資料可以如何使用？

此儀表板有助於您瞭解網路中的 Prisma Access 使用情況，並可根據儀表板資料調整組態設定。

©2025 Palo Alto Networks, Inc.

儀表板：應用程式體驗

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ Prisma Access 授權 ❑ ADEM Observability 檢視，用以檢視受監控應用程式的資料 ❑ 遠端網路授權 （查看遠端站台體驗資料的必要授權）

- 首先，按一下 **Strata Cloud Manager** > **Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **Application Experience**（應用程式體驗）。

此儀表板顯示哪些內容？

此儀表板中顯示的資料會隨著您選取的卡片而不同 - 行動使用者體驗或遠端站台體驗。如果您才剛開始使用 AI-Powered ADEM，您可以先調查整個組織正在使用的應用程式，並利用這項資訊識別您要為哪些應用程式建立應用程式測試。此外，如果有使用者或遠端站台報告了應用程式問題，此儀表板將是隔離問題的絕佳起點。應用程式使用資料是從通過 Prisma Access 的實際使用者流量中提取的。這包括來自行動使用者和遠端站台的流量。

您可以新增篩選器以縮小結果範圍，僅顯示特定應用程式、部署類型、體驗分數、行動使用者、群組或 Prisma Access 位置的資料。檢視應用程式的個別體驗分數，以及受任何現有效能問題影響的使用者和遠端站台數目。

如何使用儀表板中的資料？

在調查了執行於網路上的應用程式，並決定您要監控的應用程式之後，您可以建立應用程式測試。建立應用程式測試時請留意，雖然您可以建立以多個使用者或站台為目標的應用程式測試，但測試數目取決於每個使用者或 ION 裝置所執行的應用程式測試數目（例如，如果您有 Slack 的應用程式測試，並將其目標定為 1000 個使用者，這將會在您的授權中計為 1000 次測試）。

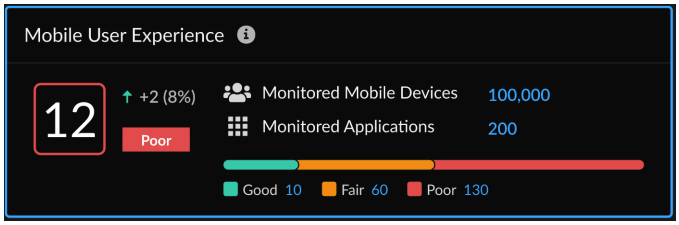
應用程式體驗儀表板：行動使用者體驗卡片

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ Prisma Access 授權 ❑ ADEM Observability 檢視，用以檢視受監控應用程式的資料

此 Widget 會顯示所有受監控應用程式的所有行動使用者的應用程式區段分數平均值。此外也會按使用者裝置數目顯示良好、尚可和不良體驗的詳細資訊。您可以深入瞭解效能體驗尚可或不良的使用者，以開始進行調查。此卡片中的體驗分數可指出使用者的整體數位體驗。對於每個行動使用

 ©2025 Palo Alto Networks, Inc.

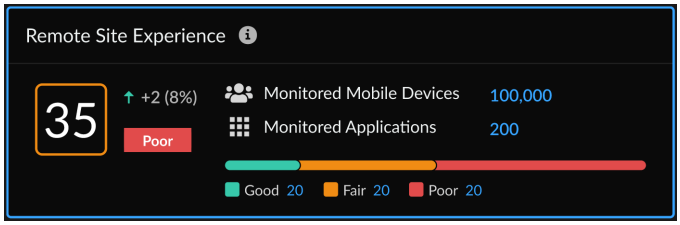
者受監控的每個應用程式，ADEM 會根據 5 個關鍵指標計算分數 - 應用程式可用性、DNS 解析時間、TCP 連線時間、SSL 連線時間和 HTTP 延遲。如果應用程式未通過可用性測試（應用程式無法使用），則體驗分數為 0。如果應用程式是可連線的，就只會計算其餘四個指標。上述每個指標（應用程式連線性除外）各有不同的權重和基準下限/上限閾值，且總權重等於 100。這些個別指標分數的總和會決定使用者的應用程式體驗分數。每個應用程式的所有測試範例結果的平均值，會決定使用者的體驗分數。



應用程式體驗儀表板：遠端站台體驗卡片

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ Prisma Access 授權 ❑ ADEM Observability 檢視，用以檢視受監控應用程式的資料 ❑ 遠端網路授權

遠端站台體驗分數是所有作用中 WAN 路徑上的所有受監控應用程式的平均分數。這是從針對該遠端站台監控的個別應用程式收集的所有測試範例結果的平均值。這是遠端站台或分支的整體體驗分數（包含在以顏色區分的方形內），從針對該站台監控的所有應用程式的作用中路徑上收集所有測試範例，並平均計算其體驗分數，即可得出。儘管每個備份路徑的體驗分數將個別計算，並可用於每個遠端站台和應用程式，但在計算遠端站台的體驗分數時，並不會考量備份路徑的體驗分數。您可以按一下 Fair（尚可）或 Poor（不良）旁的數字，深入瞭解效能尚可或不良的站台。

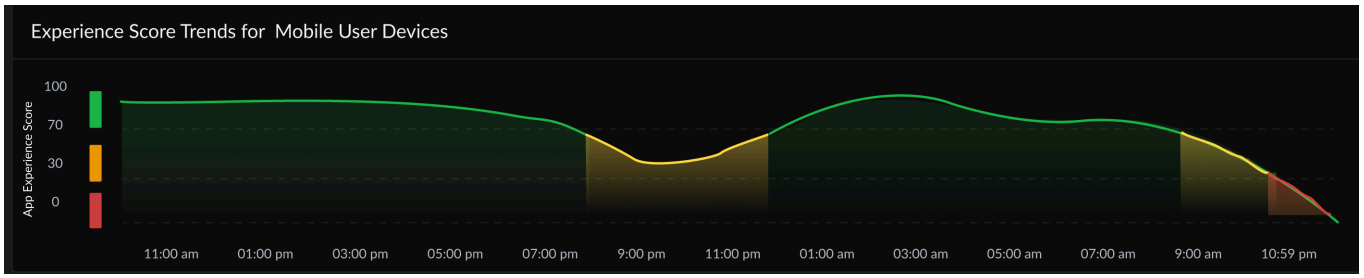


應用程式體驗儀表板：體驗分數趨勢

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ Prisma Access 授權 ❑ ADEM Observability 檢視，用以檢視受監控應用程式的資料

 ©2025 Palo Alto Networks, Inc.

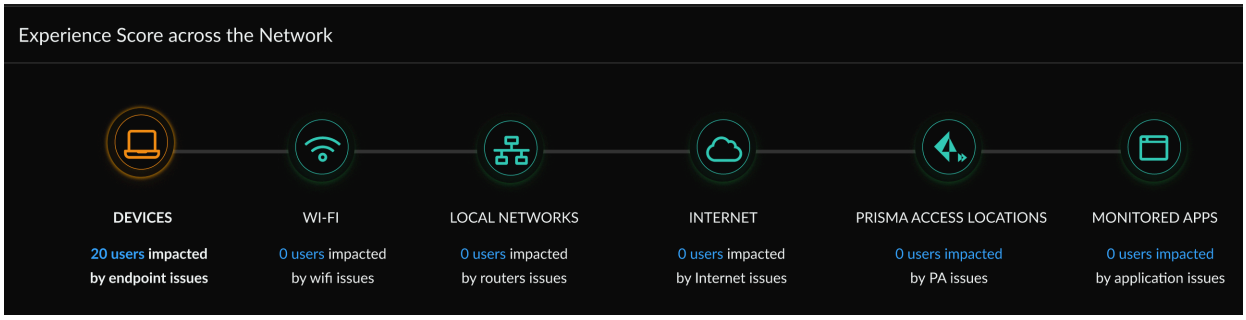
此 Widget 會顯示所有行動使用者的平均行動使用者體驗的時間序列圖。體驗分數會在選取的時間範圍內按設定的時間間隔計算及顯示。y 軸會根據分數範圍以顏色區分，以顯示體驗分數的品質（紅色 = 不良、黃色 = 尚可、綠色 = 良好）。將滑鼠游標暫留在趨勢線上方，可查看您放置游標時的體驗分數。



應用程式體驗儀表板：整個網路的體驗分數

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ Prisma Access 授權 ❑ ADEM Observability 檢視，用以檢視受監控應用程式的資料

識別可能導致組織內部發生問題的網路區段；從端點（針對行動使用者）或分支（遠端站台）一直到應用程式，都有可能。您可以從端點和 Prisma SD-WAN 遠端站台一路查看到應用程式，確認組織內的哪個網路區段可能導致問題。您可以查看哪個區段（例如 ISP 或計算位置中斷或 SaaS 應用程式中斷）正在影響組織內的數位體驗，以及受其影響的使用者或站台的確切數目。圖示會以顏色區分，並且以所有行動使用者的區段健康情況分數平均值為準。綠色圖示代表「良好」（分數 >= 70），黃色代表「尚可」（分數為 30-70），紅色代表「不良」（分數 < 30）。



裝置 - 裝置健康情況指標（CPU/記憶體/磁碟空間/磁碟佇列/電池）

Wi-Fi- WIFI 指標（訊號品質、Tx、Rx、SSID、BSSID、頻道）

區域網路 - 網路效能指標（延遲/遺失/抖動）

網際網路 - 網路效能指標（延遲/遺失/抖動）如果裝置未連線至 GlobalProtect（網際網路區段），網路效能指標就會與對應用程式區段執行的 TCP PING 測試相同。

Prisma Access 位置 - 網路效能指標（延遲/遺失/抖動）如果裝置未連線至 GlobalProtect，就不會執行此區段的測試。

 ©2025 Palo Alto Networks, Inc.

受監控的應用程式 - 網路效能指標（延遲/遺失/抖動）應用程式效能指標（可用性、DNS 查閱、TCP 連線、SSL 連線、HTTP 延遲、到第一位元組的時間、到最後一個位元組的時間、資料傳輸）

應用程式體驗儀表板：應用程式體驗分數的全域分佈

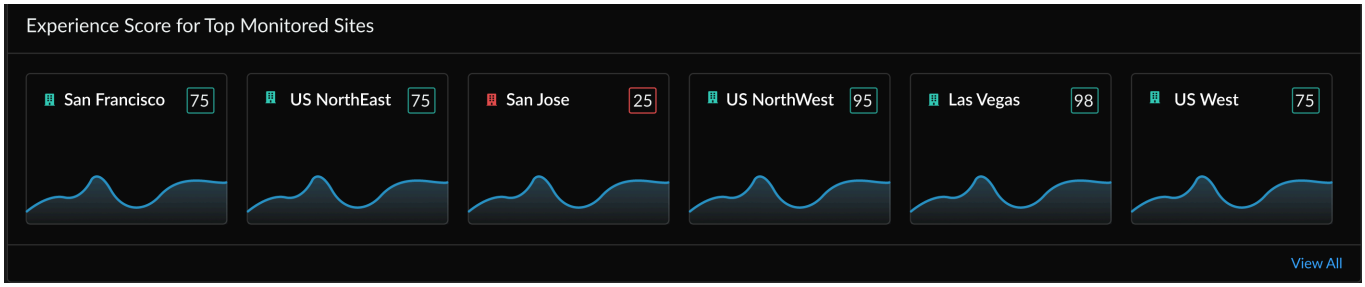
我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ Prisma Access 授權 ❑ ADEM Observability 檢視，用以檢視受監控應用程式的資料

根據您選取的卡片，此 Widget 中的地圖檢視會根據監控的行動使用者和應用程式總數，或特定 Prisma Access 位置上監控的遠端站台和應用程式總數，向您顯示 Prisma Access 位置的體驗。Prisma Access 位置標有以顏色區分的圓圈，表示連線至該特定 Prisma Access 位置（該圓圈所在之處）的所有受監控行動使用者和遠端站台的應用程式區段分數的狀態。將滑鼠游標暫留在圓圈上方，可查看該位置的體驗分數，以及受監控的行動使用者裝置或遠端站台的總數，以及該位置受監控的應用程式總數。地理位置非常接近的多個位置會以一個圓圈表示，且圓圈中會有一個數字。該數字表示分組在該區域中的位置數。若要確切查看哪些位置分組在一起，請放大地圖。

應用程式體驗儀表板：最高排名的受監控站台的體驗分數

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ Prisma Access 授權 ❑ ADEM Observability 檢視，用以檢視受監控應用程式的資料

此 Widget 會為每個應用程式顯示一張卡片，並顯示分數最高的站台。此 Widget 會顯示選定時間範圍內的遠端站台體驗分數趨勢。將滑鼠游標暫留在趨勢線上方，可查看該時間點的體驗分數。



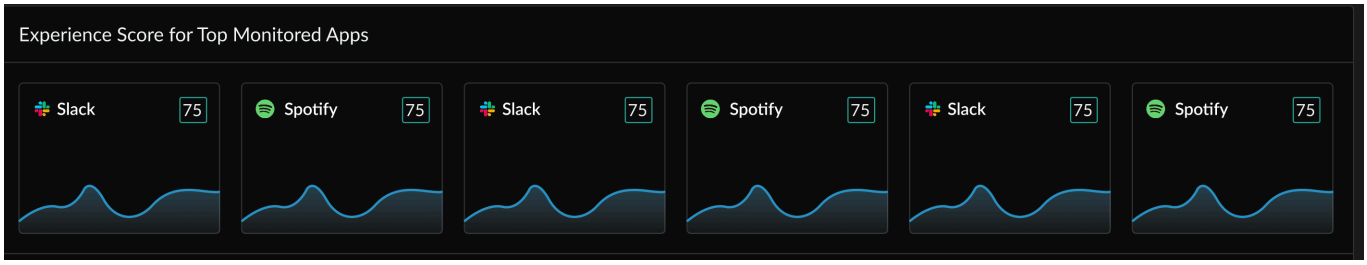
 ©2025 Palo Alto Networks, Inc.

應用程式體驗儀表板：最高排名的受監控應用程式的體驗分數

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ Prisma Access 授權 ❑ ADEM Observability 檢視，用以檢視受監控應用程式的資料

每個應用程式卡片都會顯示遠端站台上的特定應用程式所有的受監控行動使用者的平均應用程式區段分數（方框內的數字）。體驗分數是從所有受監控應用程式的應用程式體驗分數的平均值計算出來的。體驗分數可說明應用程式作用中路徑的端對端體驗。這是僅針對該應用程式在其作用中路徑上收集到的所有測試樣本的平均值。趨勢線顯示選定時間範圍內的所有 5 分鐘 APM 資料樣本的平均值。

您可以查看正在監控的應用程式數目，以及監控的作用中和備份路徑數目。每個應用程式卡片都會顯示受影響的路徑數目。按一下應用程式卡片，可查看該應用程式的指標。



應用程式體驗儀表板：應用程式效能指標

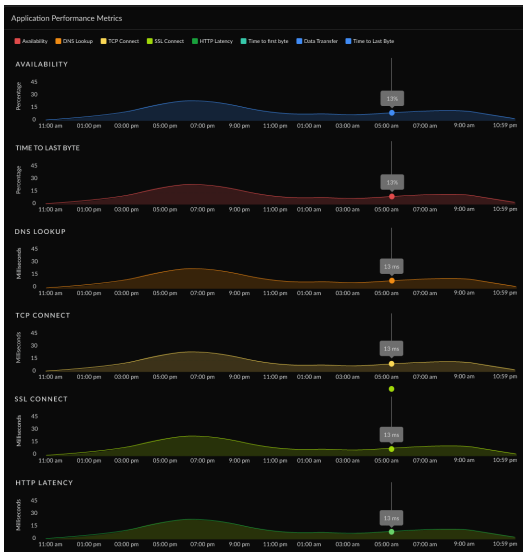
我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ Prisma Access 授權 ❑ ADEM Observability 檢視，用以檢視受監控應用程式的資料

自動 DEM 會使用 TCP ping（偵測）和 Curl 來判斷端對端應用程式效能。

指標	說明
可用性	時間範圍內的應用程式可用性（百分比）。
DNS 查閱	DNS 解析時間。
TCP 連線	建立 TCP 連線所花費的時間。
SSL 連線	建立 SSL 連線所花費的時間。

©2025 Palo Alto Networks, Inc.

指標	說明
HTTP 延遲	建立 HTTP 連線所花費的時間。
到第一個位元組的時間	DNS 查詢、TCP 連線、SSL 連線和 HTTP 延遲時間的總計，會產生「到第一個位元組的時間」。
資料傳輸	要傳輸的整體資料所耗費的時間總計。
到最後一個位元組的時間	到第一個位元組的時間 + 資料傳輸時間。



應用程式體驗儀表板：網路效能指標

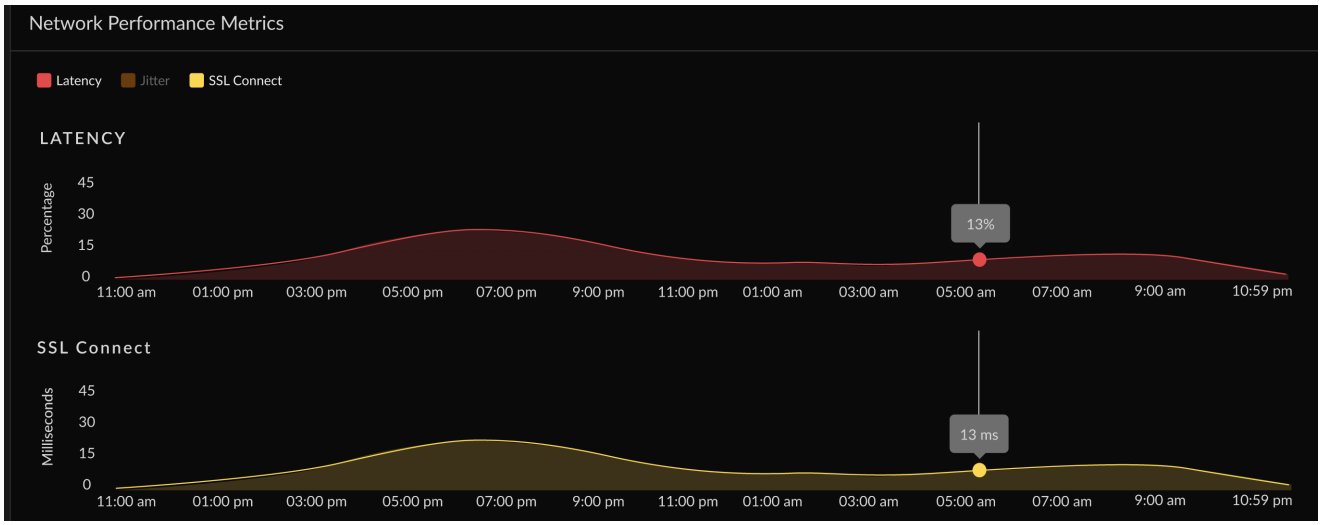
我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ Prisma Access 授權 ❑ ADEM Observability 檢視，用以檢視受監控應用程式的資料

ADEM 會使用 ICMP ping（偵測）來決定每個區段的網路效能。

指標	說明
可用性	**Time Range**（時間範圍）內的網路可用性指標。
網路延遲	透過網路傳輸資料所花費的時間。
封包遺失	在資料傳輸過程中遺失封包。

©2025 Palo Alto Networks, Inc.

指標	說明
抖動	**Time Range**（時間範圍）內的延遲變化。

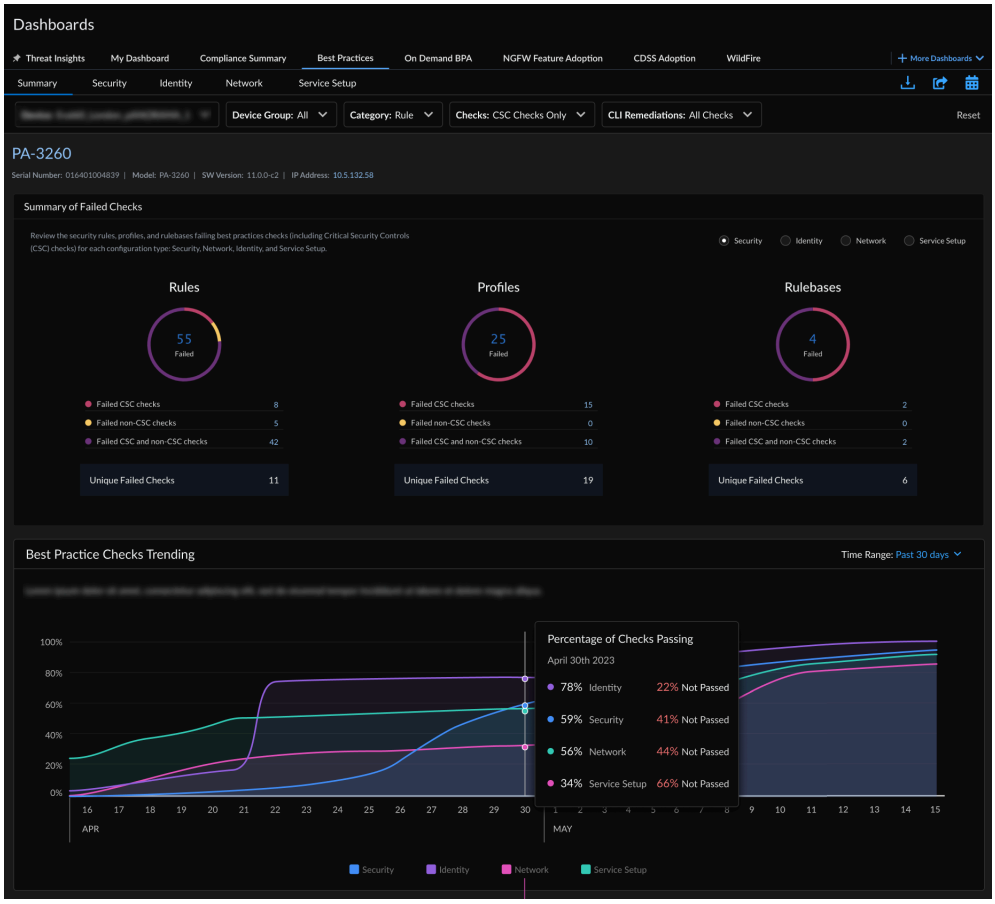


 ©2025 Palo Alto Networks, Inc.

儀表板：最佳做法

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 首先，按一下**Strata Cloud Manager** > **Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **Best Practices**（最佳做法）。



 ©2025 Palo Alto Networks, Inc.

此儀表板顯示哪些內容？

儀表板會根據與您的租用戶相關聯的 *Prisma Access* 和 *NGFW/Panorama*，顯示彙總資料。

最佳做法儀表板會根據 Palo Alto Networks 的最佳做法指引，衡量您的安全性狀態。重要的是，最佳做法評估包括對 Center for Internet Security 的重大安全性控制 (CSC) 進行檢查。CSC 檢查會與其他最佳做法檢查分開，因此您可以輕鬆選擇更新，並優先挑選可讓您符合 CSC 的更新。

最佳做法儀表板分成五個部分：

- **Summary**

  讓您全面檢視不同設定類型（安全性、網路、識別和服務設定）上裝置的所有失敗檢查、以及檢視 BPA 檢查的歷史趨勢圖和評估重要功能領域的最佳做法採用率。

- **security**

  針對所選裝置和位置，顯示未通過最佳做法和 CSC 檢查的規則、規則庫或設定檔。CLI 補救功能在適用時，可讓您解決政策規則的問題。CLI 補救功能是使用您在產生隨選 BPA 時上傳的 TSF 資料產生的。

  - 規則庫

    檢視政策的組織方式，以及適用於許多規則的組態設定是否符合最佳做法（包括 CSC 檢查）。

  - 規則

    顯示未通過最佳做法和 CSC 檢查的規則。查看您可以在何處採取快速行動，來修正失敗的檢查。規則會根據工作階段計數排序，因此您可以先檢閱和更新影響最大流量的規則。

  - 設定檔

    顯示您的設定檔為何違反最佳做法（包括 CSC 檢查）。設定檔會針對與安全性或解密規則相符的流量，執行進階檢查。

- 識別

  顯示裝置的驗證強制執行設定（驗證規則、驗證設定檔和驗證入口網站）是否符合最佳做法，並且與 CSC 檢查相符。

- 網路

  檢查應用程式覆寫規則和網路設定是否符合最佳做法和 CSC 檢查。

- 服務設定

  瞭解您在裝置上啟用的訂閱如何符合最佳做法和 CSC 檢查。您可以在此處檢閱 WildFire 設定、GlobalProtect 入口網站和 GlobalProtect 閘道設定，並修正失敗的檢查。

此儀表板支援報告。儀表板右上方若有圖示  ，表示此儀表板支援報告。您可以共用、下載及排程涵蓋此儀表板顯示之資料的報告。

如何使用儀表板中的資料？

雖然最佳做法指南旨在協助您加強安全性狀態，但本報告中的結果也可以協助您識別可以進行變更的領域，以便更有效地管理環境。

 ©2025 Palo Alto Networks, Inc.

儀表板：合規性摘要

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	☐ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

您可以檢視安全性檢查在過去 12 個月內進行變更的歷程記錄；Center for Internet Security (CIS) 和美國國家標準技術研究所 (NIST) 架構會將這些內容分門別類。對於每個架構，您都會看到一個控制清單，以及目前和平均合規率的百分比、最佳做法檢查的總數，以及每個控制的失敗檢查數目。

與圖表和清單互動，以查看控制與其歷史統計資料之間的關係。檢視個別控制及其相關檢查的詳細資料，並選取最佳做法檢查，以檢視未通過檢查的防火牆設定。

CIS 重大安全性控制架構是一組優先的建議動作和最佳做法，有助於保護組織及其資料免受已知網路攻擊媒介的侵害。您可以檢視 11 個基本和基礎 CIS 控制（共 16 個）的檢查摘要：

- CSC 3：持續的弱點管理
- CSC 4：控制管理權限的使用
- CSC 6：稽核日誌的維護、監控和分析
- CSC 7：電子郵件和網頁瀏覽器保護
- CSC 8：惡意軟體防禦
- CSC 9：限制和控制網路連接埠、通訊協定和服務
- CSC 11：網路裝置（如防火牆、路由器和交換器）的安全設定
- CSC 12：邊界防禦
- CSC 13：資料保護
- CSC 14：根據須知事項控制存取
- CSC 16：帳戶監控和控制

NIST Cybersecurity Framework SP 800-53 控制架構提供了聯邦政府機構和其他組織為其資訊系統實作及維護安全與隱私控制的相關指引。您可以檢視 8 個 NIST 控制系列的檢查摘要：

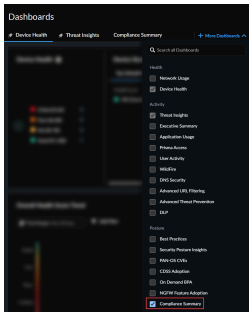
- SC：存取控制
- AU：稽核和責任
- CM：設定管理
- CP：應變規劃
- IA：識別和驗證
- RA：風險評估
- SC：系統和通訊保護

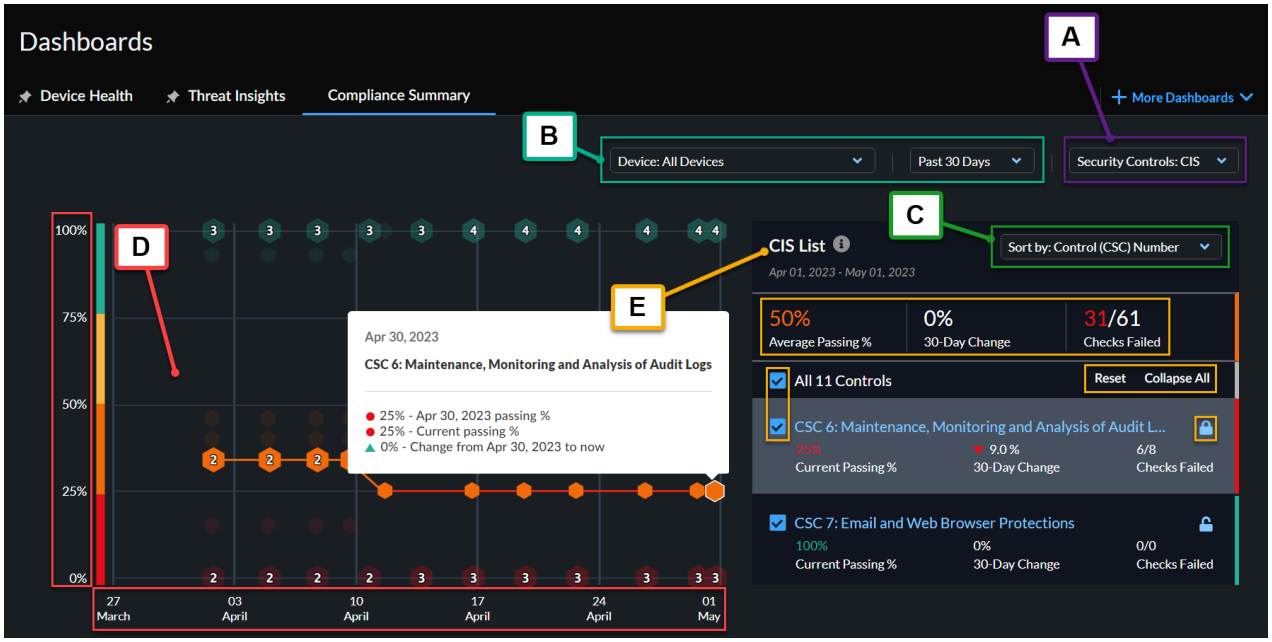
©2025 Palo Alto Networks, Inc.

- SI：系統和資訊完整性

若要存取合規性摘要儀表板，請移至 **Dashboards**（儀表板），然後選取 **Compliance Summary**（合規性摘要）頁籤。

如果您在頁籤選項中未看到 ***Compliance Summary***（合規性摘要），請選取 ***More Dashboards***（更多儀表板），然後在 ***Posture***（狀態）底下選取 ***Compliance Summary***（合規性摘要）。





A) 安全控制選取器	選取 CIS 或 NIST 控制
B) 篩選依據	• 裝置

©2025 Palo Alto Networks, Inc.

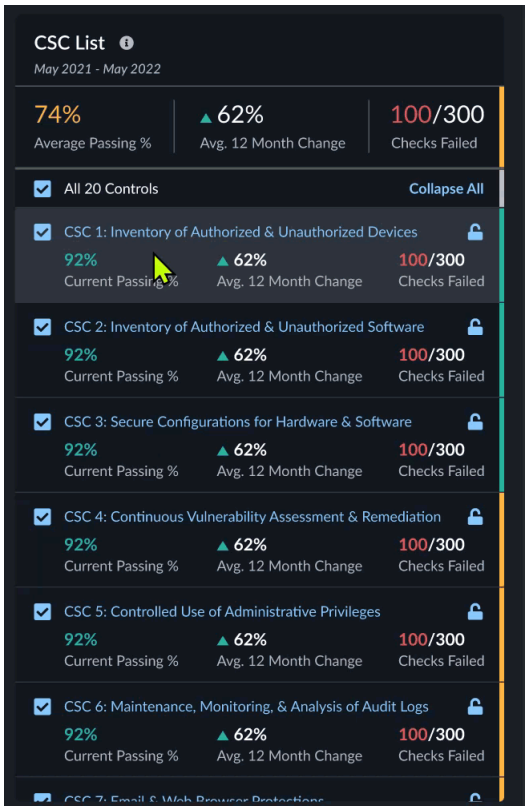
	• 時間範圍
	  • 過去 7 天
	  • 過去 30 天
	  • 過去 90 天
	  • 過去 6 個月
	  • 過去 12 個月

C) 排序方式	• 控制 CSC 號碼 • 目前的通過百分比 • 百分比變化 • 失敗檢查數目
D) 折線圖	• 通過百分比 - 顯示給定檢查類型的通過百分比。 • 時間軸 - 顯示為給定的檢查類型測量百分比的時間。

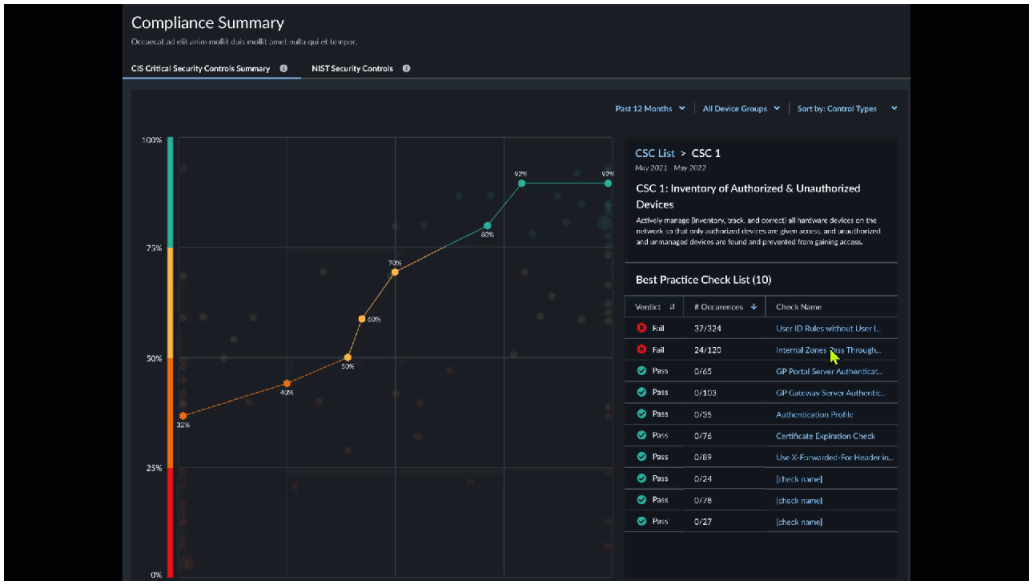
E) 檢查清單	• 統計資料
	  • 平均通過百分比 - 顯示通過檢查的平均百分比。
	  • 12 個月的變化 - 顯示 12 個月期間內的變化。
	  • 檢查失敗 - 顯示失敗的檢查數目。
	• 選取的控制 - 核取記號會將控制顯示在折線圖上。
	• 重設 - 移除所有鎖定。
	• 全部摺疊/全部展開 - 顯示/隱藏清單中的統計資料。
	• 鎖定折線圖 - 在折線圖上保留檢視中鎖定的檢查。

 ©2025 Palo Alto Networks, Inc.

- 選取清單中的控制，查看其中包含的最佳做法檢查。



- 選取最佳做法檢查，以檢視未通過檢查的防火牆設定。

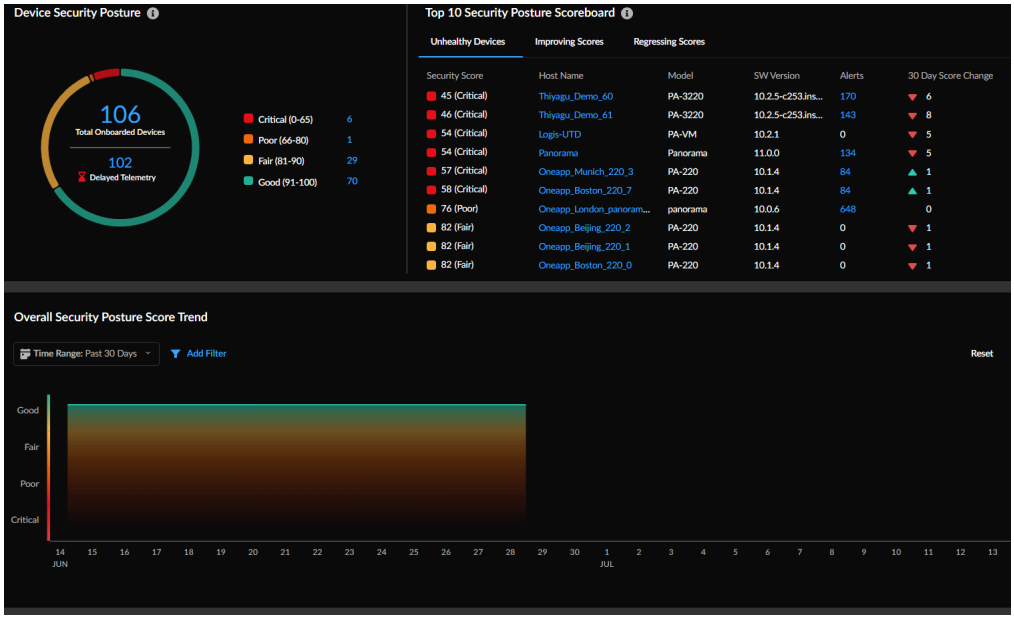


 ©2025 Palo Alto Networks, Inc.

儀表板：安全性狀態洞察

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 首先，按一下**Strata Cloud Manager** > **Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **Security Posture Insights**（安全性狀態洞察）。



此儀表板顯示哪些內容？

此儀表板會顯示所有與您的租用戶相關聯且會傳送遙測資料之防火牆的彙總資料。

根據載入 NGFW 裝置的安全性狀態，了解部署的安全狀態和趨勢。安全分數 (0-100) 的嚴重性及其相應的安全等級（良好、尚可、不良、嚴重）決定了裝置的安全態勢。安全分數是根據開放警示的優先順序、數量、類型和狀態來計算。

儀表板中的資料可以如何使用？

使用此儀表板執行下列作業：

- 瞭解影響部署安全性狀態的問題趨勢。

 ©2025 Palo Alto Networks, Inc.

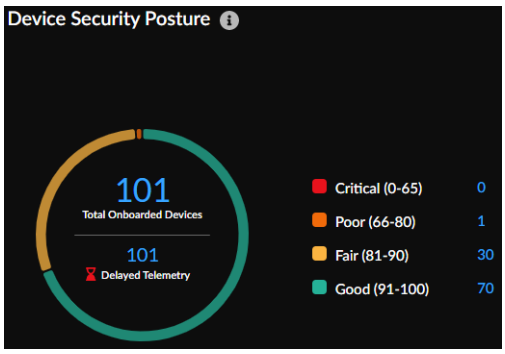
- 查看歷史安全分數資料，瞭解您在部署中所做的安全性改進。
- 縮小有機會改善安全性狀態的裝置範圍，並優先處理問題加以解決。

此儀表板不支援報告功能（下載、共用和排程報告）。

安全性狀態洞察儀表板：裝置安全性狀態

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 按一下**Strata Cloud Manager** > **Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **Security Posture Insights**（安全性狀態洞察），以檢視儀表板。



此儀表板 Widget 會顯示：

- 已上線的 NGFW 總數。
- 超過 12 小時未傳送遙測資料的裝置數量。
- 部署中載入裝置的安全分數優先順序。按一下數字連結即可瞭解裝置詳細資料和安全統計資料。

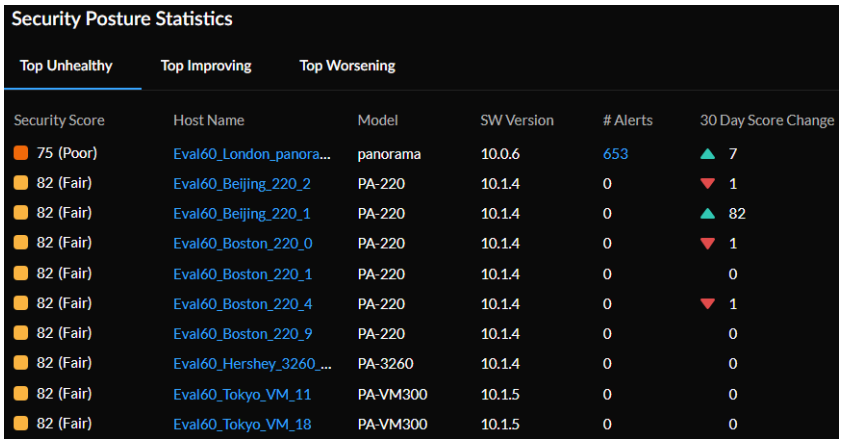
安全性狀態洞察儀表板：安全性狀態統計資料

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium或Strata Cloud Manager Pro

©2025 Palo Alto Networks, Inc.

這可在何處使用？	我需要哪些內容？
	→ 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 按一下**Strata Cloud Manager** > **Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **Security Posture Insights**（安全性狀態洞察），以檢視儀表板。



狀況最差

這些是對部署的安全性狀態影響最大的 10 個裝置。深入檢視裝置詳細資料和裝置上的警示。針對裝置上的重大警示執行修復步驟，以改善安全性狀態。

改進程度最大

與裝置目前的安全分數相比，檢視在 30 天內安全性狀態分數有所改善的前 10 個裝置。

惡化程度最大

這些是與裝置目前的安全分數相比安全性狀態分數有所下降的裝置。檢閱這些裝置上的警示，並優先加以修正。

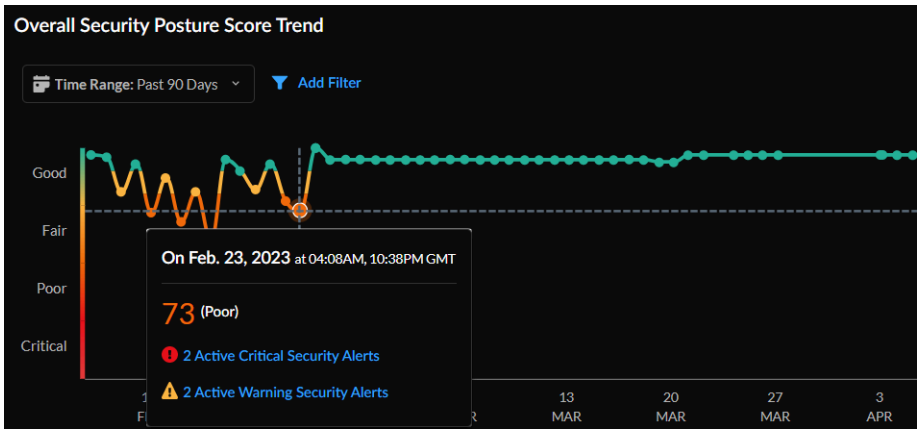
安全性狀態洞察儀表板：分數趨勢

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 按一下**Strata Cloud Manager** > **Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **Security Posture Insights**（安全性狀態洞察），以檢視儀表板。

圖表中顯示所選時段內部署的安全態勢趨勢。將滑鼠暫留在觸發點上方，可瞭解有助於安全性狀態趨勢的裝置和活動警示。您可以檢視按主機名稱、型號或軟體版本篩選的一或多個裝置的趨勢。

 ©2025 Palo Alto Networks, Inc.

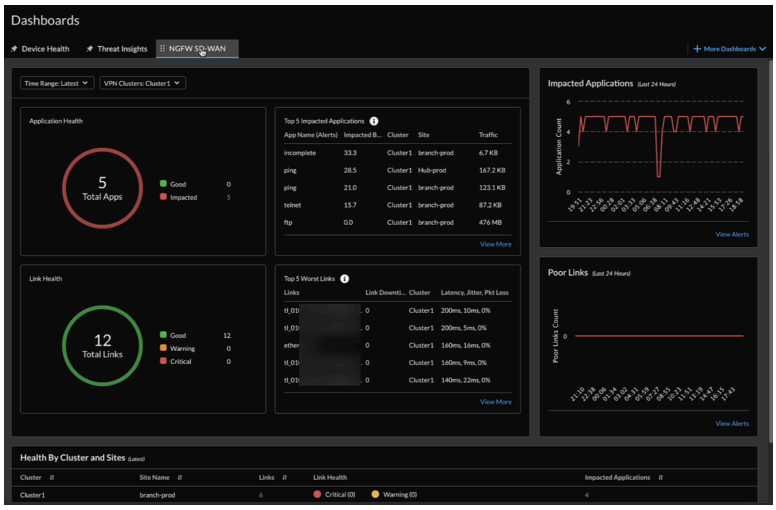


 ©2025 Palo Alto Networks, Inc.

儀表板：NGFW SD-WAN

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 首先，按一下 **Dashboards**（儀表板）**> More Dashboards**（更多儀表板）**> NGFW SD-WAN**。



若要使用此儀表板，您可以在 Strata Cloud Manager 上為 Palo Alto Networks 新世代防火牆設定軟體定義的廣域網路 (SD-WAN)。

此儀表板顯示哪些內容？

NGFW SD-WAN 儀表板會針對具有 SD-WAN 的雲端管理防火牆，顯示連結和應用程式流量的效能指標。

儀表板中的資料可以如何使用？

此儀表板可協助您：

- 藉由檢視所有 VPN 叢集的摘要資訊，瞭解 VPN 叢集中的應用程式和連結效能指標，以對問題進行疑難排解。
- 深入檢視以找出受影響的站台、應用程式和連結的問題。
- 引發可操作的警示，以調查並修復不良的連結和應用程式。藉助於採用 ML 技術的異常偵測、正常範圍和預測功能，可操作的警示是以資料驅動的閾值為基礎，您將獲得關於趨勢的洞察。

這段影片說明如何監控 NGFW SD-WAN 儀表板。

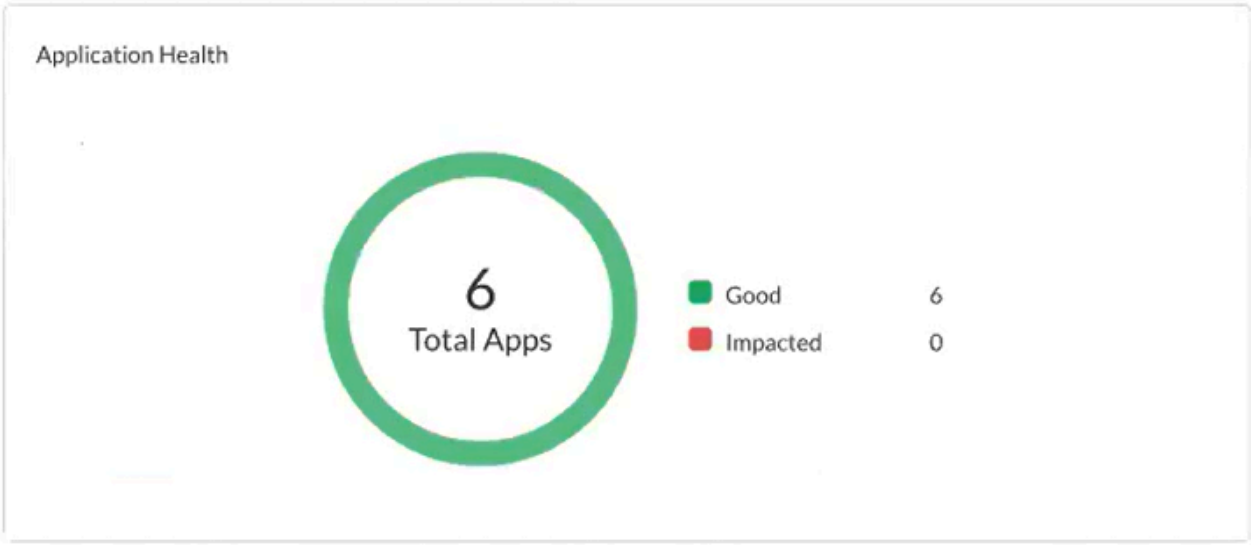
 ©2025 Palo Alto Networks, Inc.

NGFW SD-WAN 儀表板：應用程式健康情況

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	☐ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

儀表板顯示：

- VPN 叢集在選定持續時間內的應用程式總數。
- 受影響的應用程式數目，這是指 VPN 叢集中一或多個如下的應用程式：任何路徑的抖動、延遲或封包遺失效能均未達到可供防火牆選擇的路徑清單中的路徑品質設定檔所指定的閾值。
- 健康情況良好的應用程式數量，即 VPN 叢集中未經歷抖動、延遲或封包遺失效能問題的應用程式數量。

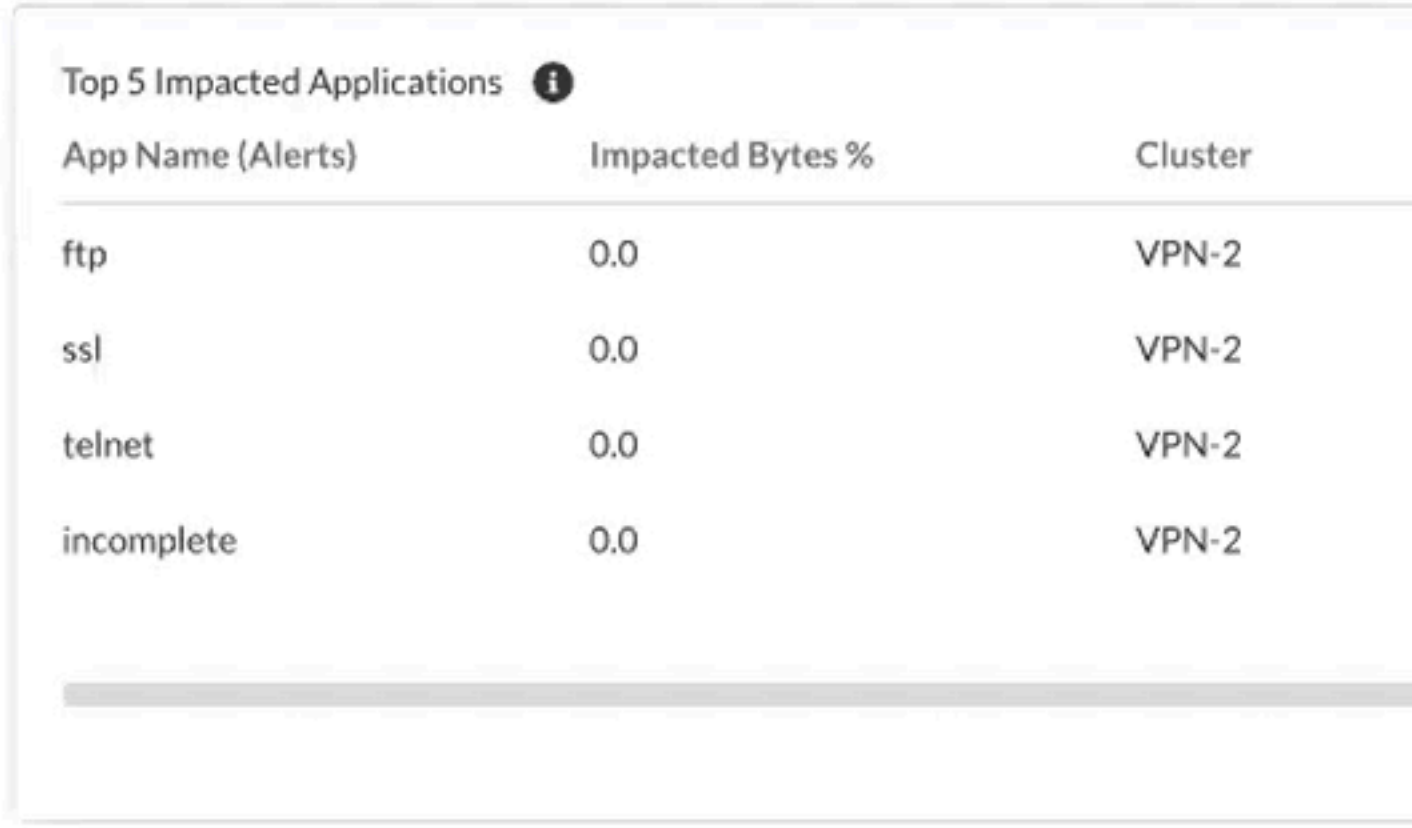


 ©2025 Palo Alto Networks, Inc.

NGFW SD-WAN 儀表板：最高排名的受影響應用程式

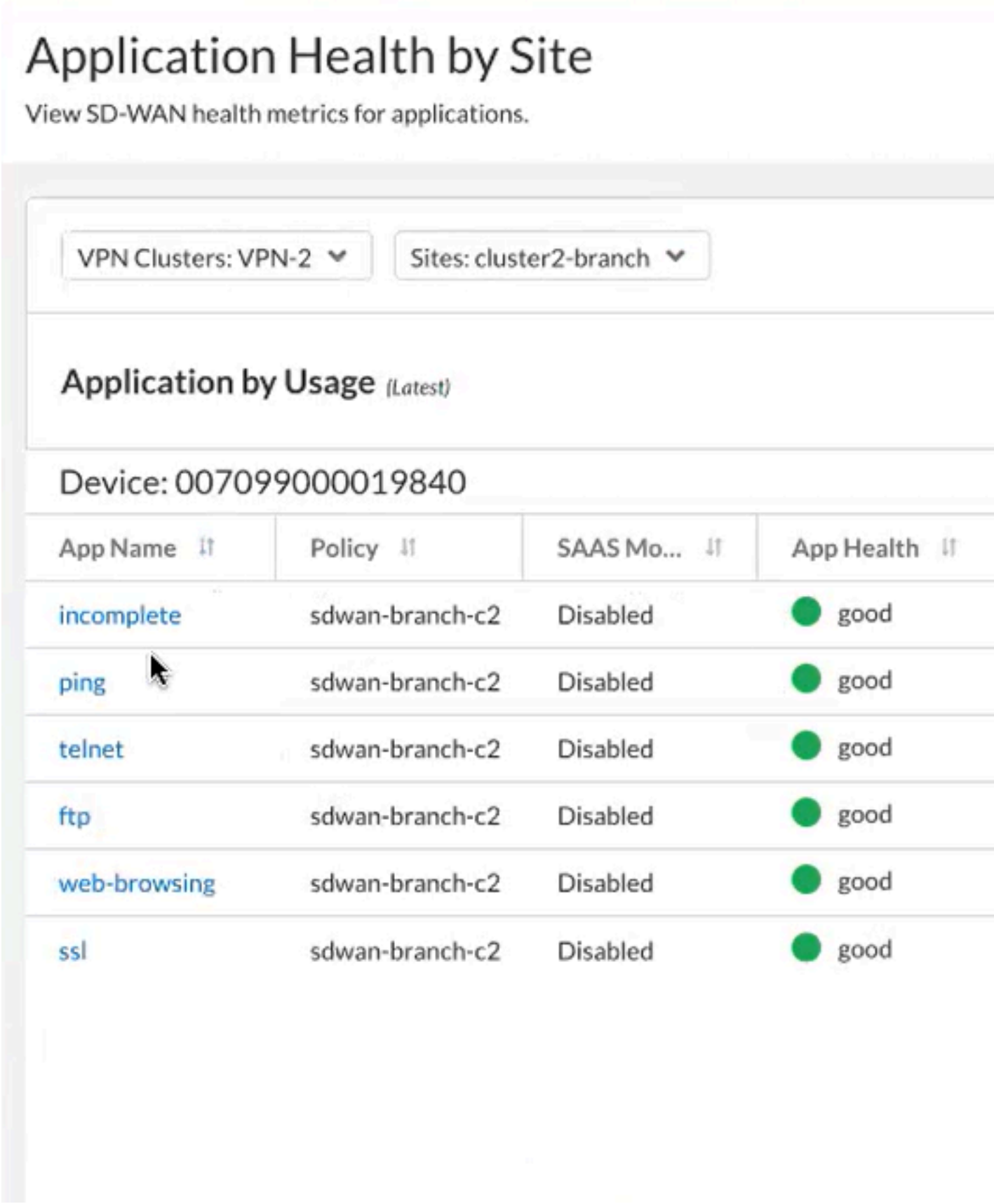
這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

對於選取的持續時間和 VPN 叢集，Strata Cloud Manager 會根據受影響的流量佔總位元組數的計算百分比，顯示最高排名的 5 個受影響應用程式。計算出的百分比越高，表示對應用程式的影響越大。



按一下 **View More**（檢視更多），以查看所有受影響的應用程式。

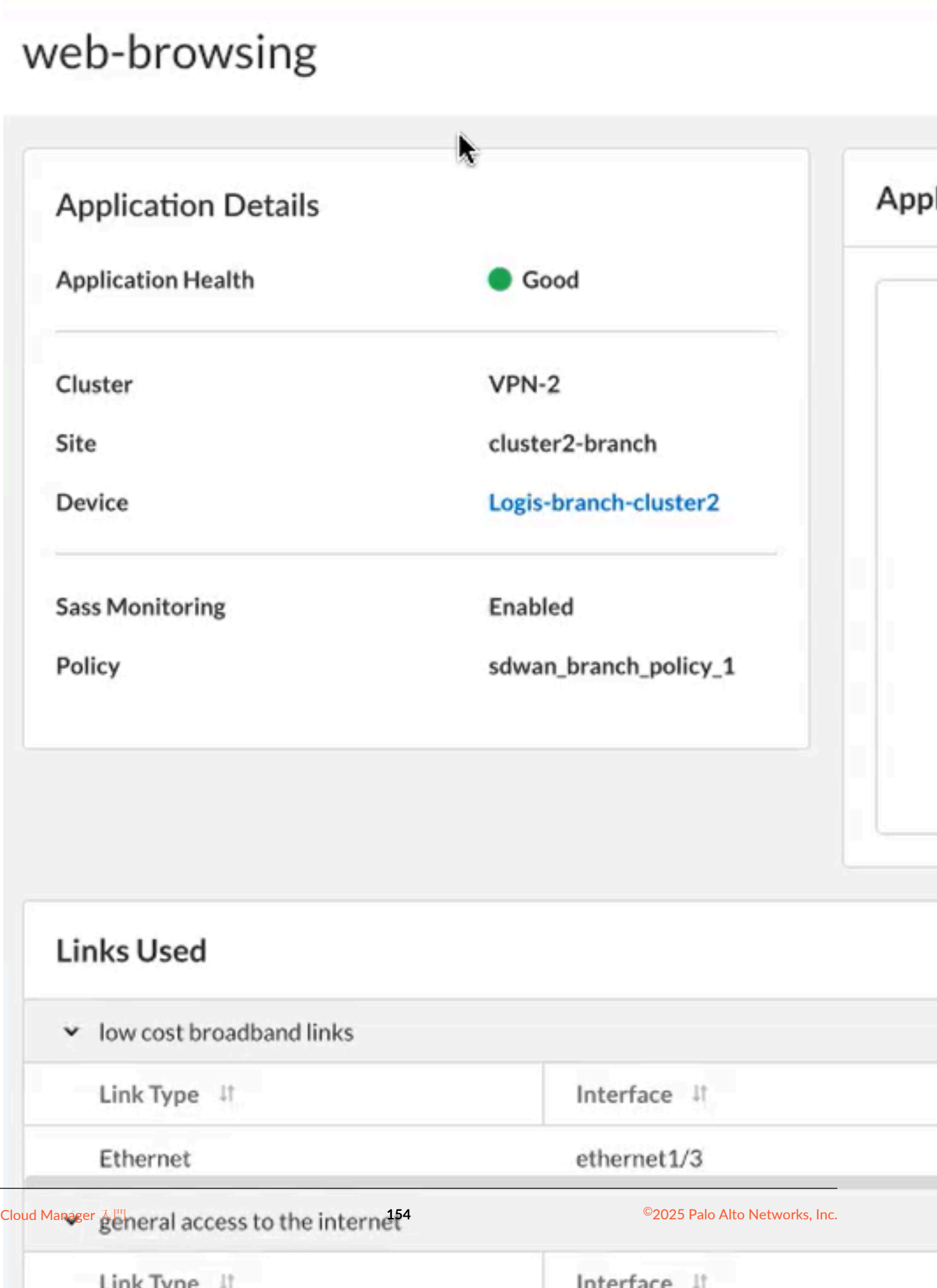
 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

此外，按一下應用程式可檢視其詳細資料，包括流量和使用的連結。您也可以按一下已使用的連結，以檢視其詳細資料。

 ©2025 Palo Alto Networks, Inc.



©2025 Palo Alto Networks, Inc.

NGFW SD-WAN 儀表板：受影響的應用程式

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

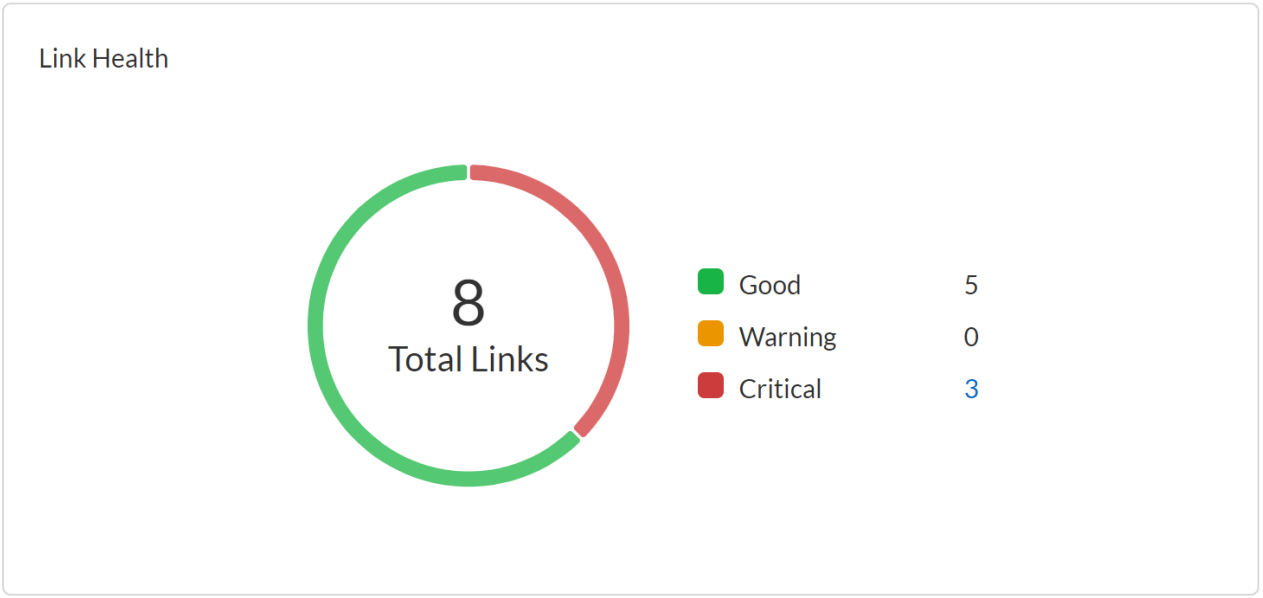
- 圖表中顯示受影響的應用程式在過去 24 小時內的趨勢。將游標停留在趨勢線上方，可檢視在特定時間點受影響的應用程式。
- 按一下 **View Alerts**（檢視警示），以檢視因受影響的應用程式而引發的相關警示。

NGFW SD-WAN 儀表板：連結健康情況

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- VPN 叢集在選定持續時間內的連結總數。
- 分類為「重大」、「警告」和「良好」的連結數目。
- 按一下**Critical**（重大）的數字連結，以檢視因 SD-WAN 連結效能而引發的警示。

©2025 Palo Alto Networks, Inc.

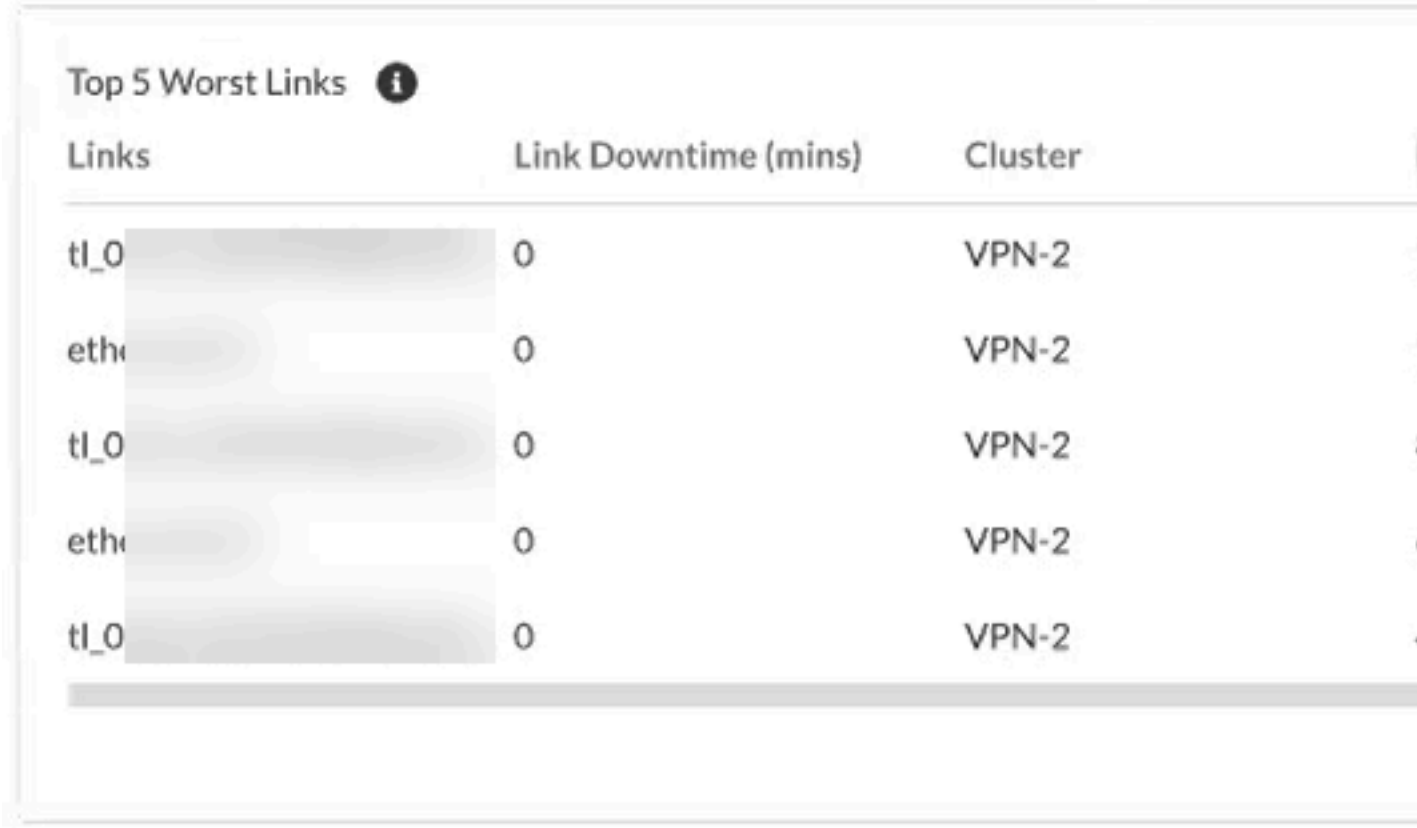


©2025 Palo Alto Networks, Inc.

NGFW SD-WAN 儀表板：最差的連結

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

對於選取的持續時間和 VPN 叢集，Strata Cloud Manager 會根據介面指標的計算平均值 (通道停機時間、延遲、抖動和封包遺失) 顯示前 5 個最差的連結。這些連結會根據通道停機時間、延遲、封包遺失和抖動的優先順序排名。計算出的平均值越高，表示連結品質越差。

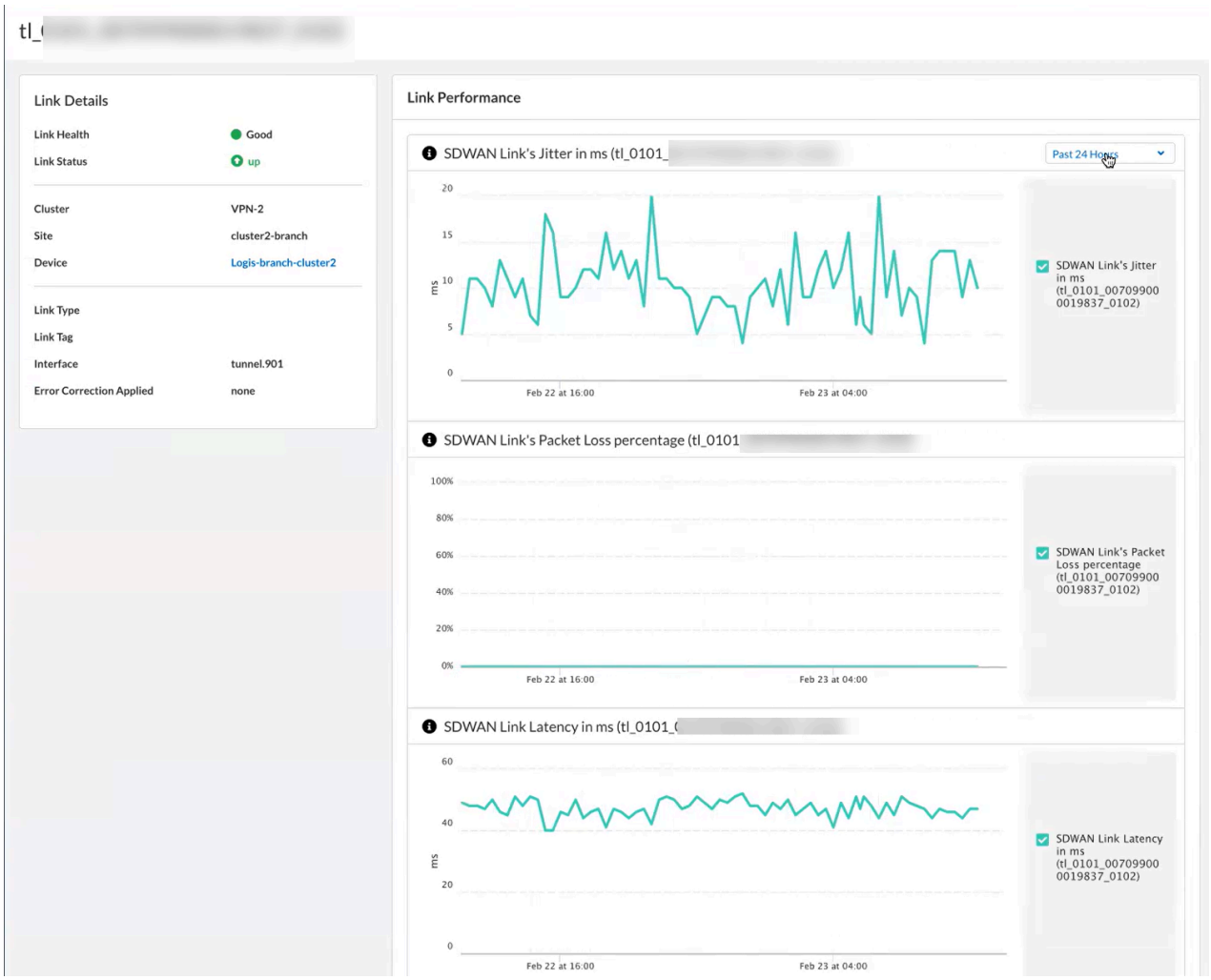


您可以按一下 **View More**（檢視更多），以查看所有受影響的連結。

©2025 Palo Alto Networks, Inc.

此外，按一下連結可檢視其詳細資料，包括以連結效能為基礎的圖表。

 ©2025 Palo Alto Networks, Inc.

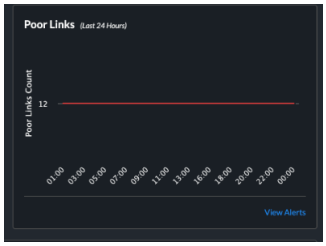


 ©2025 Palo Alto Networks, Inc.

NGFW SD-WAN 儀表板：不良連結

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 圖表中顯示過去 24 小時內偵測到的不良連結呈現的趨勢。將游標暫留在趨勢線上方，可檢視特定時間點的不良連結。
- 按一下 **View Alerts**（檢視警示），以檢視因連結不良而引發的相關警示。

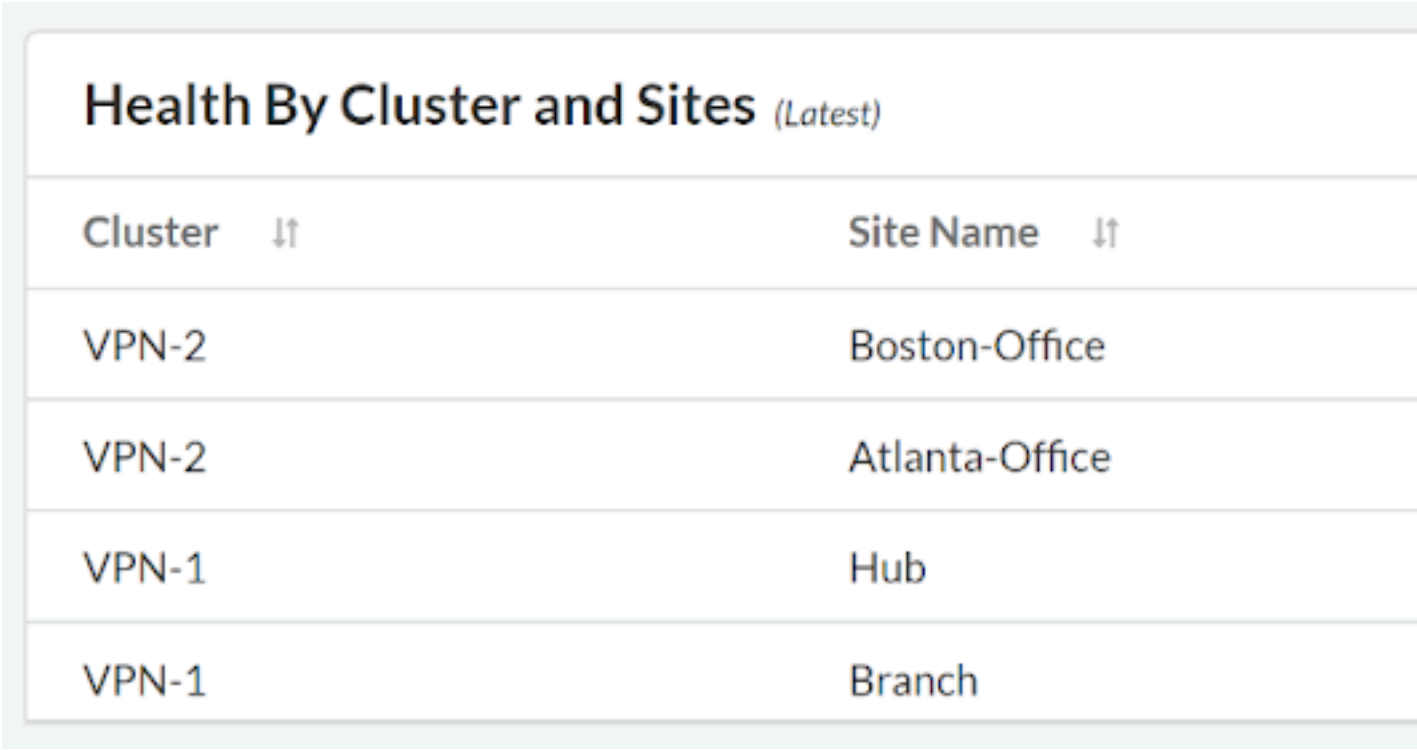


NGFW SD-WAN 儀表板：按叢集和站台顯示的健康情況

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

檢視每個站台的連結數目、其健康情況，以及受影響的應用程式。

©2025 Palo Alto Networks, Inc.



按一下這些欄底下的數字連結，以檢視其相關詳細資料。

 ©2025 Palo Alto Networks, Inc.

儀表板：Prisma SD-WAN

這可在何處使用？	我需要哪些內容？
• Prisma SD-WAN	❑ Prisma SD-WAN 授權 可見性所需的其他授權和先決條件包括： ❑ 在儀表板中解鎖特定 Widget 的授權 ❑ WAN Clarity（用於預測分析） ❑ 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

此儀表板顯示哪些內容？

此儀表板會顯示 Prisma SD-WAN 的網路、裝置和應用程式指標的高階圖形檢視。此外也會顯示：

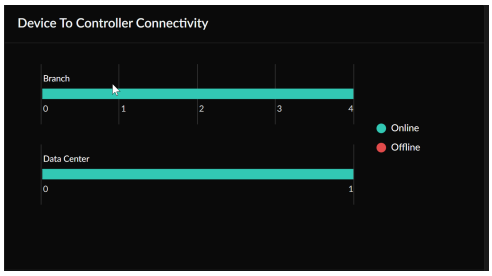
- 分支和資料中心裝置與控制器的連線狀態。
- 進入和輸出流量的應用程式使用率資料。
- 過去一週租用戶中所有分支站台的基本網路洞察和報告。
- 最高排名的分支和資料中心站台的相關資訊（按產生的事件數目顯示）。
- 各站台的連結品質指標，例如 MOS 分數、封包遺失、抖動和延遲。
- 站台層級的預測容量使用率（以過去三到六個月的資訊為基礎）。

Prisma SD-WAN 儀表板：裝置到控制器的連線

這可在何處使用？	我需要哪些內容？
• Prisma SD-WAN	❑ Prisma SD-WAN 授權 可見性所需的其他授權和先決條件包括： ❑ 在儀表板中解鎖特定 Widget 的授權 ❑ WAN Clarity（用於預測分析） ❑ 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

裝置到控制器的連線 Widget 會說明連線至分支和資料中心的 Prisma SD-WAN 控制器的線上和離線 ION 裝置數量。使用此互動式圖表，您可以檢視對應分支和資料中心的已宣告裝置的線上或離線狀態。

©2025 Palo Alto Networks, Inc.

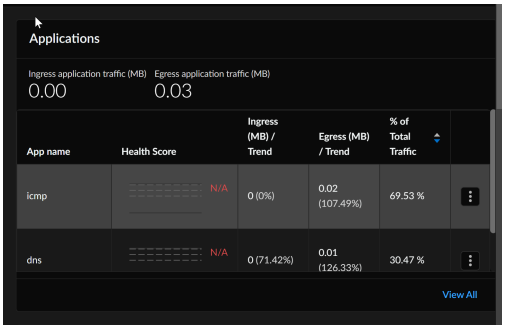


按一下互動式圖表上的 **Branch**（分支）或 **Data Center**（資料中心）後，您可以檢視已宣告和未宣告的裝置名稱、狀態、已安裝的軟體版本、上次活動，以及裝置的備援狀態。

Prisma SD-WAN 儀表板：應用程式

這可在何處使用？	我需要哪些內容？
• Prisma SD-WAN	❑ Prisma SD-WAN 授權 可見性所需的其他授權和先決條件包括： ❑ 在儀表板中解鎖特定 Widget 的授權 ❑ WAN Clarity（用於預測分析） ❑ 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

應用程式 Widget 會顯示關於站台在選定時間範圍內的應用程式使用率資訊。顯示時間範圍內的應用程式進入和輸出流量總計。按流量排名的前 10 個的應用程式會與其他流量一起顯示。按一下 **View All**（檢視全部），以檢視選定時間範圍內的應用程式健康情況分佈、一段時間的 TCP 應用程式健康情況分佈、新流量、頻寬使用率、交易統計資料，以及最高排名的應用程式。您可以在儀表板中深入檢視每個站台的應用程式在選定時間範圍內的效能和指標。



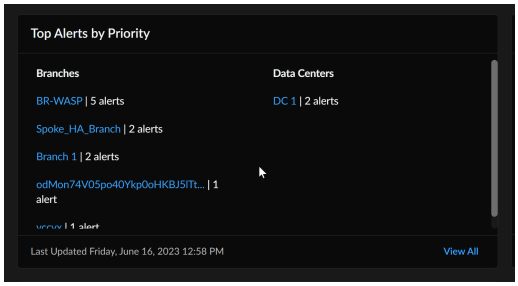
最初會顯示所有 TCP 應用程式的指標，但您可以選取前 10 個 TCP 應用程式中的任何一個，更集中地關注特定的高排名應用程式。

 ©2025 Palo Alto Networks, Inc.

Prisma SD-WAN 儀表板：按優先順序顯示的最高排名警示

這可在何處使用？	我需要哪些內容？
• Prisma SD-WAN	❑ Prisma SD-WAN 授權 可見性所需的其他授權和先決條件包括： ❑ 在儀表板中解鎖特定 Widget 的授權 ❑ WAN Clarity（用於預測分析） ❑ 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

Top Alerts by Priority（按優先順序顯示的最高排名警示）Widget 會按優先順序顯示前 5 個警示。您可以根據選定時間範圍內產生的警示數目，查看最高排名的分支和資料中心站台的資訊。您可以深入檢視每個站台在選定時間範圍內的警示資訊。



按一下 **View All**（檢視全部），以檢視警示的下列資訊：

- 警示建立的時間。
- 事件的名稱。
- 主要的受影響物件。
- 警示的嚴重性。
- 警示的優先順序。

按一下省略符號，對警示進行疑難排解。

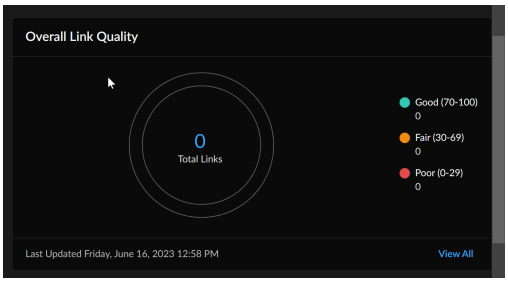
Prisma SD-WAN 儀表板：整體連結品質

這可在何處使用？	我需要哪些內容？
• Prisma SD-WAN	❑ Prisma SD-WAN 授權 可見性所需的其他授權和先決條件包括： ❑ 在儀表板中解鎖特定 Widget 的授權 ❑ WAN Clarity（用於預測分析）

 ©2025 Palo Alto Networks, Inc.

這可在何處使用？	我需要哪些內容？
	❑ 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

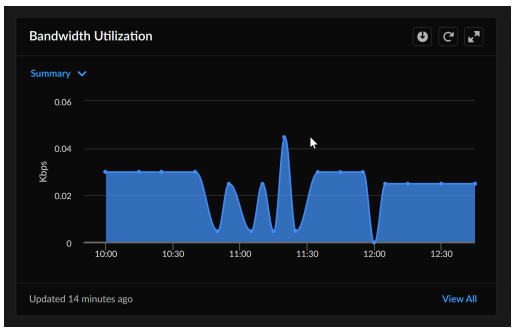
整體連結品質 Widget 會提供您所有的站台在選定時間範圍內的目前連結狀態的整體快照。您可以深入檢視連結效能、連結封包遺失、連結抖動和連結延遲，而得以分析您要在 Link Quality Metrics（連結品質指標）儀表板中更詳細檢視的資訊。



Prisma SD-WAN 儀表板：頻寬使用率

這可在何處使用？	我需要哪些內容？
• Prisma SD-WAN	❑ Prisma SD-WAN 授權 可見性所需的其他授權和先決條件包括： ❑ 在儀表板中解鎖特定 Widget 的授權 ❑ WAN Clarity（用於預測分析） ❑ 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

頻寬使用率 Widget 會顯示網路中使用的頻寬量。此圖會呈現頻寬尖峰、特定站台耗用的總頻寬，以及應用程式；無論上傳是進入還是輸出方向（或兩者）。



將游標移至 **Bandwidth Utilization**（頻寬使用率）圖表中，可更詳細地檢視應用程式或時間戳記的頻寬使用率。應用程式通常會按其頻寬使用率的順序列出。圖表中顯示一段時間內消耗的頻

 ©2025 Palo Alto Networks, Inc.

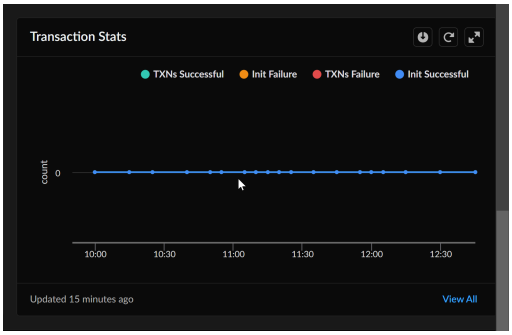
寬。1H 檢視提供每分鐘精細度的資料，1D 圖片顯示每 5 分鐘的資料。每個範例的 1D 圖表資料的平均值超過 5 分鐘。如果使用率持續超過 5 分鐘，您可以在兩個圖表中查看對應的峰值使用率。

您可以使用 Widget 中的下載選項，下載 PDF、CSV、XLS 或 PNG 格式的頻寬使用率圖表。

Prisma SD-WAN 儀表板：交易統計資料

這可在何處使用？	我需要哪些內容？
• Prisma SD-WAN	❑ Prisma SD-WAN 授權 可見性所需的其他授權和先決條件包括： ❑ 在儀表板中解鎖特定 Widget 的授權 ❑ WAN Clarity（用於預測分析） ❑ 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

交易統計資料 Widget 會提供 TCP 流量的交易統計資料，包括特定應用程式或所有應用程式、特定路徑或所有路徑，以及所有健康情況事件的起始/交易成功和失敗。它測量網路路徑上執行的網路和應用程式的效能和可用性。對於給定路徑上的每個要求，Prisma SD-WAN 會即時監控起始和資料傳輸交易的交易錯誤率。



從交易統計圖表中，按頻寬使用率或按路徑檢視應用程式清單。您可以篩選掉成功交易，以取得交易失敗統計資料的詳細檢視。圖表中顯示下列類別的成功或失敗交易計數：

- 初始化成功：成功完成三向交握。
- **TXN** 成功：在完成三向交握後成功傳輸資料。
- 初始化失敗：無法完成三向交握。失敗的原因可能包括防火牆設定錯誤、應用程式伺服器問題、網路存取控制清單設定錯誤，或 WAN 網路提供者問題。
- **TXN** 失敗：完成三向交握後的資料傳輸不成功。失敗的原因可能包括防火牆設定錯誤、應用程式伺服器問題、網路存取控制清單設定錯誤，或 WAN 網路提供者問題。

您可以使用 Widget 中的下載選項，下載 PDF、CSV、XLS 或 PNG 格式的頻寬使用率圖表。

 ©2025 Palo Alto Networks, Inc.

Prisma SD-WAN 儀表板：預測分析

這可在何處使用？	我需要哪些內容？
• Prisma SD-WAN	❑ Prisma SD-WAN 授權 可見性所需的其他授權和先決條件包括： ❑ 在儀表板中解鎖特定 Widget 的授權 ❑ WAN Clarity（用於預測分析） ❑ 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

預測分析 Widget 可讓您深入瞭解站台和應用程式的健康情況，並進行主動監控，以識別重大問題並快速進行疑難排解，從而提高服務水準。它可識別重要站台、連結和應用程式，並根據 AI/ML 健康情況分數在租用戶層級將其分類為 **Good**（良好）、**Fair**（尚可）和 **Poor**（不良）。此 Widget 會根據過去三到六個月的資訊，預測分支站台層級的容量使用率。

檢視指標的預設時間範圍為三小時；但您可以根據所需的資訊範圍將其調整為更短或更長的時間。深入瞭解過去 28 天頻寬使用率增加的前 10 個站台；當 28 天的預測無法使用時，您可以檢視 7 天的預測，並預測未來的分支容量使用率。

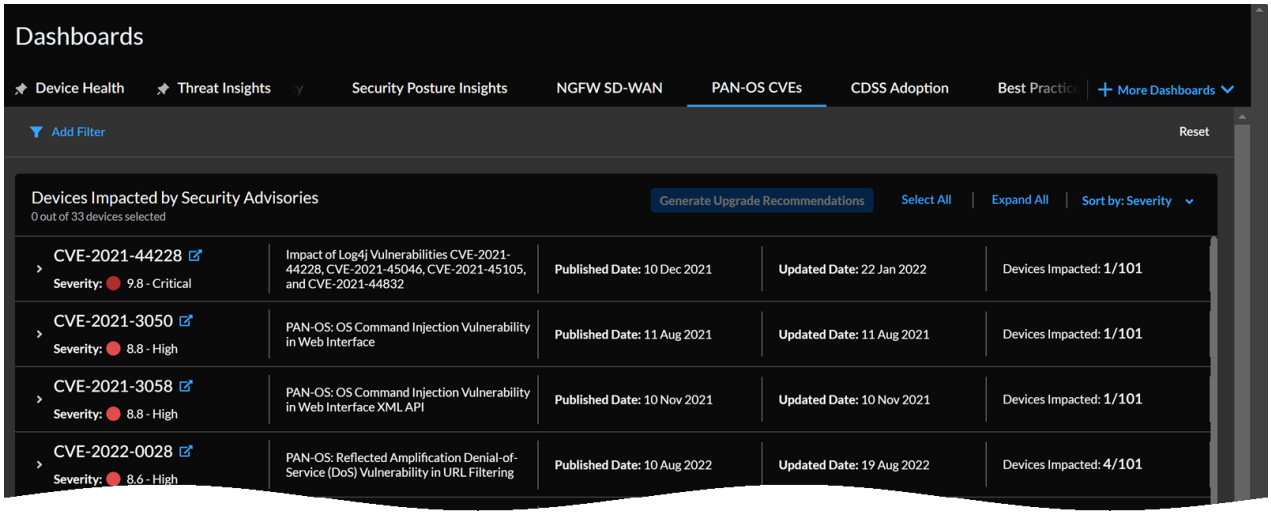
按一下 **View All**（檢視全部），以深入瞭解分支站台、應用程式、連結、網路洞察、過去 30 天內流量成長最多的站台，以及站台容量預測和異常。

©2025 Palo Alto Networks, Inc.

儀表板：PAN-OS CVE

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 首先，按一下 **Dashboards**（儀表板）**> More Dashboards**（更多儀表板）**> PAN-OS CVE**。



此儀表板顯示哪些內容？

此儀表板會顯示所有在您的租用戶上線並傳送遙測資料之防火牆和 *Panorama* 的彙總資料。此外也會顯示來自 *CVE* 的 *NGFW PSIRT* 資料庫的遙測資料。

PAN-OS CVEs 儀表板會根據裝置啟用的功能，顯示受特定弱點影響的裝置數目。Strata Cloud Manager 會分析已啟用的功能，以確認受 CVE 影響的裝置。

瞭解受影響的裝置有何弱點後，您可以使用「升級建議」功能規劃修補措施。展開 CVE，選取要升級以修復弱點的防火牆，然後按一下 **Generate Upgrade Recommendations**（產生升級建議）。您將重新導向至 NGFW - 升級建議，以檢視產生的報告。

以下說明如何評估影響裝置的弱點，並產生升級建議以修正這些弱點。

儀表板中的資料可以如何使用？

此儀表板可協助您：

- 決定要升級哪些裝置以緩解弱點。

 ©2025 Palo Alto Networks, Inc.

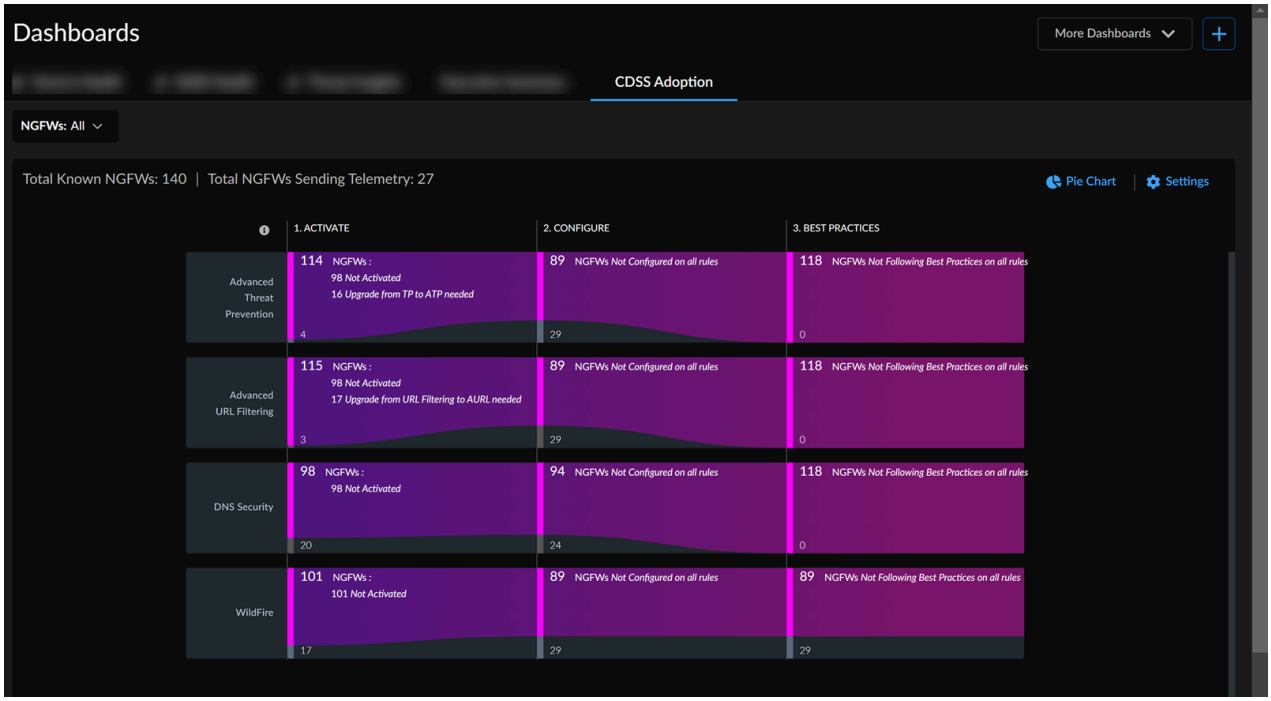
- 透過擴展 CVE，檢視關於受影響裝置的詳細資料，例如主機名稱、型號、序號、軟體版本，以及前次遙測更新。
- 篩選 CVE，並按 **Severity**（嚴重性）或 **Devices Impacted**（受影響的裝置）進一步加以排序。
- 按一下 CVE 以檢視其相關聯的諮詢。

 ©2025 Palo Alto Networks, Inc.

儀表板：CDSS 採用

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 首先，按一下**Dashboards**（儀表板） > **Posture**（狀態） > **CDSS Adoption**（**CDSS** 採用）。



此儀表板顯示哪些內容？

- 此儀表板會顯示所有在您的租用戶上線並傳送遙測資料之防火牆的彙總資料。
- 目前，此儀表板僅支援四個安全性訂閱：進階威脅防護、進階 *URL* 篩選、*DNS* 安全性和 *Wildfire*。

CDSS Adoption（**CDSS** 採用）儀表板會顯示建議的雲端交付安全服務 (CDSS) 訂閱，及其在您裝置中的使用情況。這有助於識別安全漏洞，並強化企業的安全性狀態。瀏覽至此頁面後，您會看到一個快顯視窗，要求您確認或更新 NGFW 中的區域角色，以取得正確的安全服務建議。您可以進入此快顯視窗中的連結，將區域對應至角色。

以下影片說明如何使用 **CDSS Adoption**（**CDSS** 採用）儀表板監控安全性訂閱：

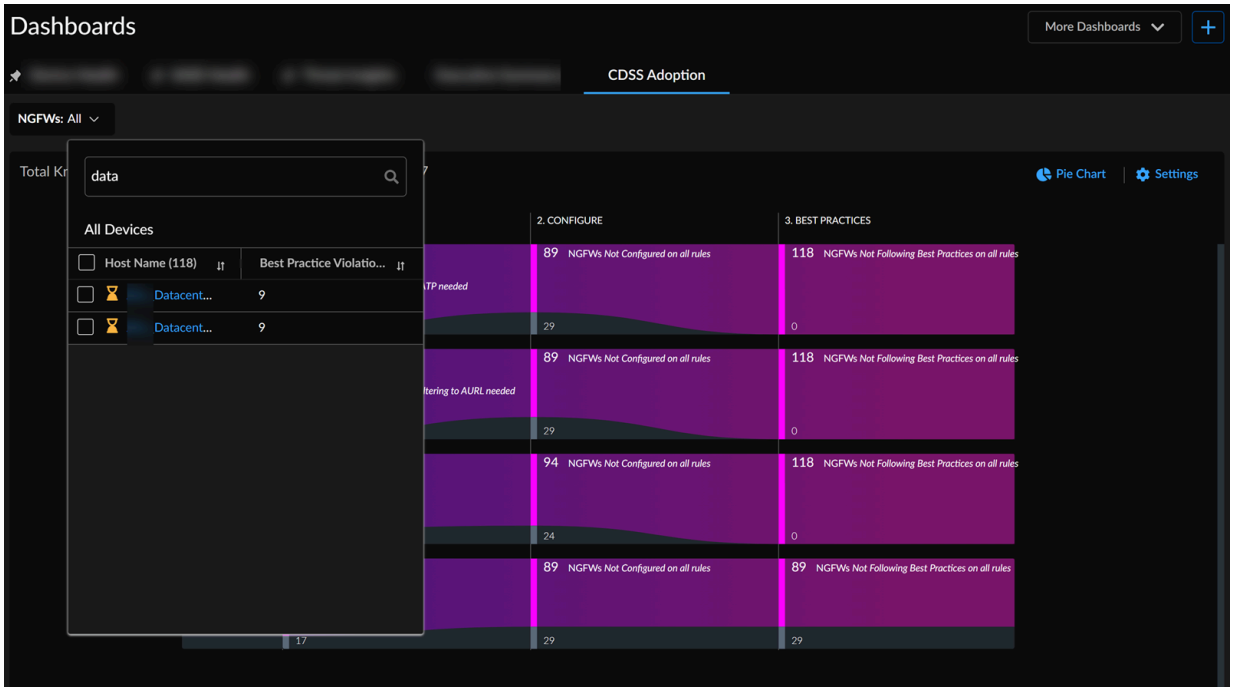
©2025 Palo Alto Networks, Inc.

如何使用儀表板中的資料？

此儀表板可協助您進行下列事項：

- 在 [Overview（概要）] 頁面頂端，您可以檢視已知 NGFW 的總數，以及在您的 AIOps for NGFW 執行個體中傳送遙測的 NGFW 數目。採用 CDSS 時需進行啟動、設定，且須遵守最佳做法。要追蹤每個訂閱的進度，只需按一下圖表中的數字，即可檢視在此過程中需要更新的裝置清單。若要在裝置中使用安全性訂閱授權，您必須啟動該授權，並據以設定服務或功能。

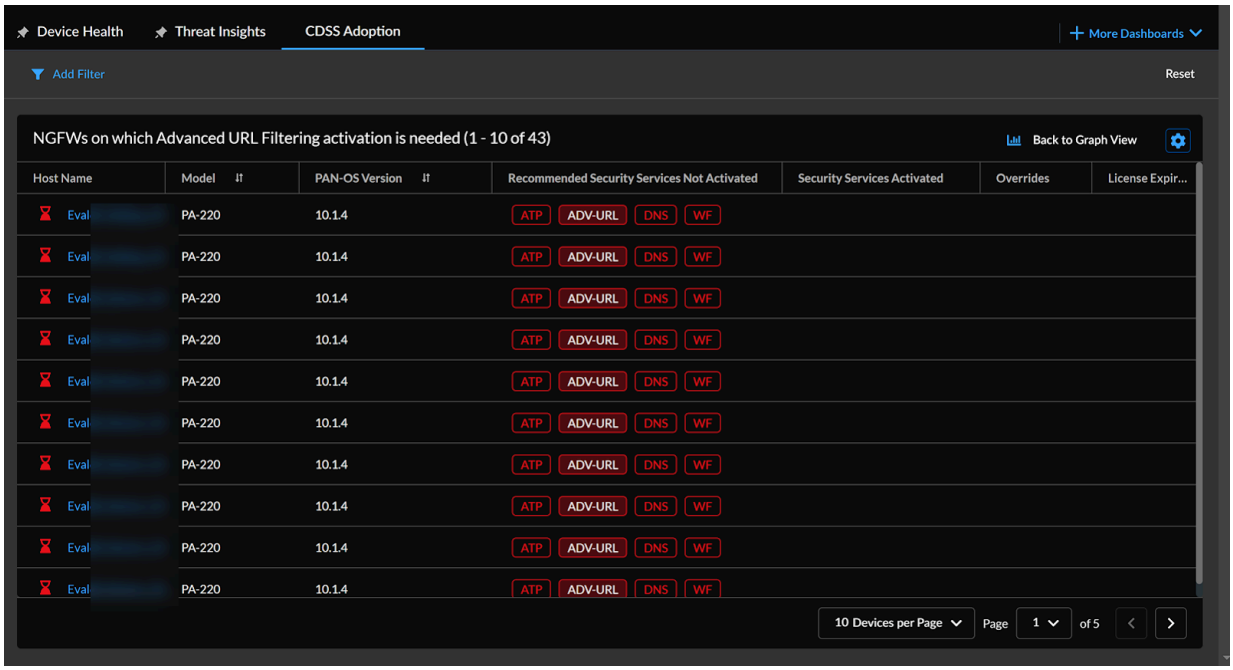
  若要專注於特定 NGFW 的安全服務資料，請據以篩選圖表。您也可以在此下拉式清單中檢視裝置的最佳做法違規。



 ©2025 Palo Alto Networks, Inc.

- 您可以按一下 **ACTIVATE**（啟動）、**CONFIGURE**（設定）或 **BEST PRACTICES**（最佳做法）底下的其中一個值，檢視表格格式的詳細資料。

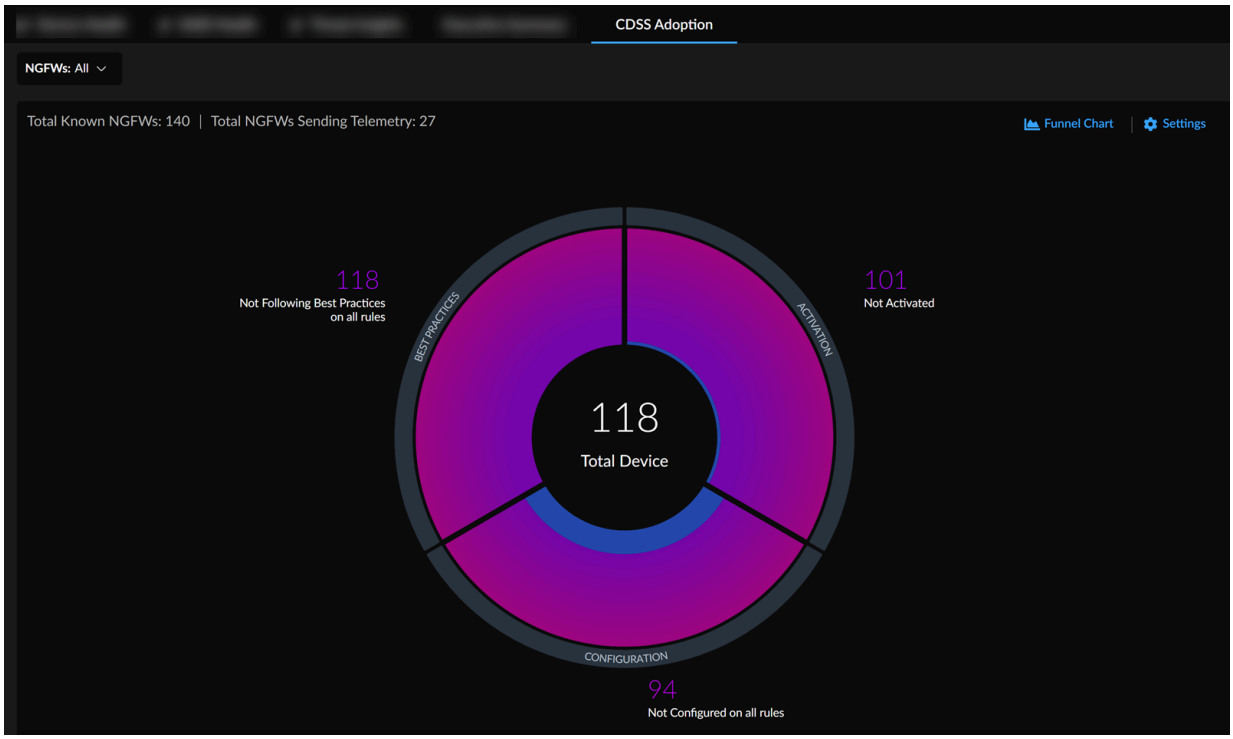
 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

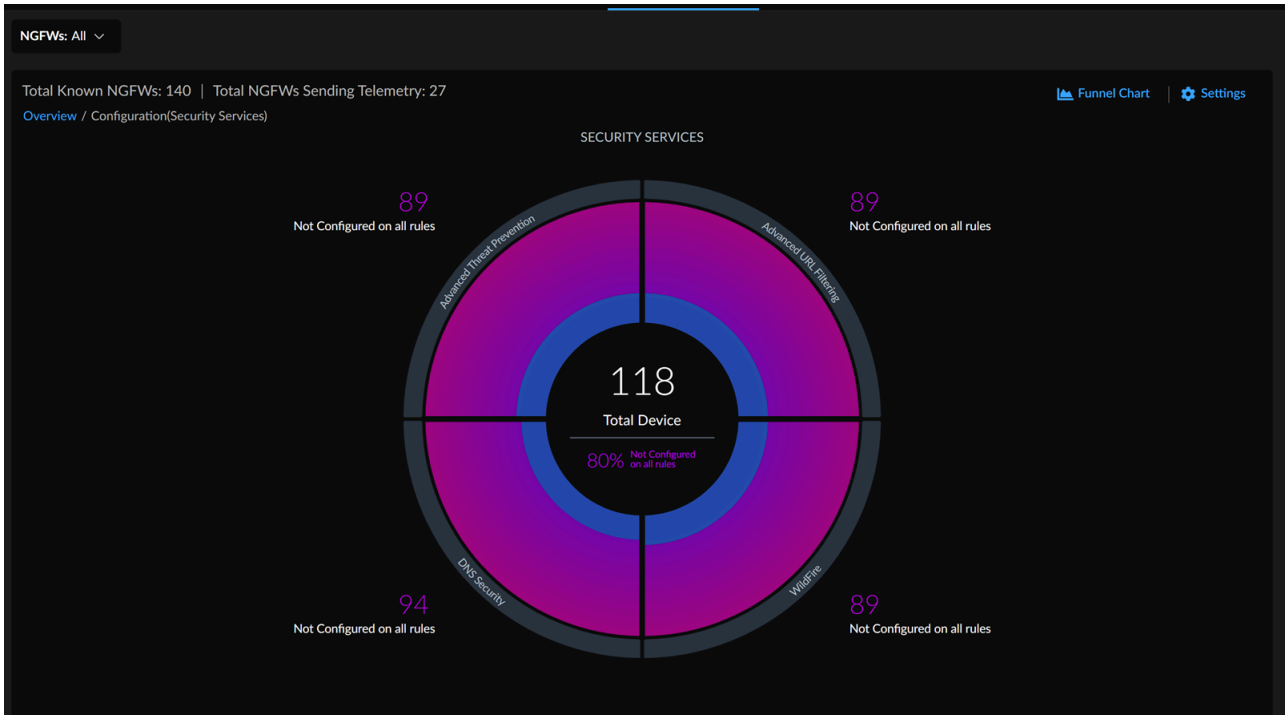
在此範例中，AIOps for NGFW 建議為 NGFW 啟動進階 URL 篩選 (ADV-URL) 以及進階威脅防護 (ATP)、網域名稱系統 (DNS) 和 WildFire (WF) 安全服務。您可以按一下 **Back to Graph View**（返回圖形檢視），以導覽至 [Overview（概要）] 頁面。

- 您也可以用圓形圖格式檢視相同的安全性狀態資料。按一下圓形圖圖示，以圓形圖格式檢視建議安全服務的相關資訊。



 ©2025 Palo Alto Networks, Inc.

- 您可以按一下圓形圖的區段，以檢視個別安全服務的相關資訊。

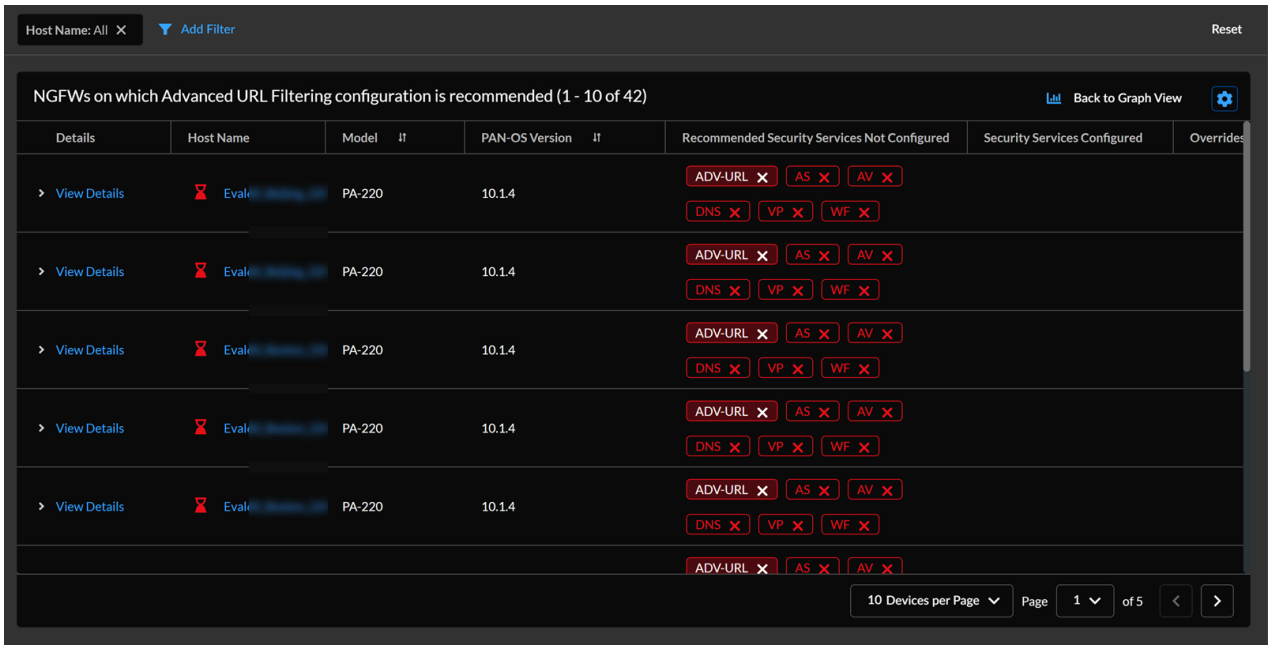


在此範例中，若要檢視未設定 DNS 安全性的 NGFW，您可以按一下圓形圖 **DNS** 安全性區段上方的值，或按一下圓形圖的 **DNS** 安全性區段。

覆寫建議的安全服務

當您基於任何原因不需要建議的安全服務時，即可加以覆寫。按一下 **CONFIGURE**（設定）底下的值可檢視表格格式的詳細資料，您可以覆寫建議的安全服務。

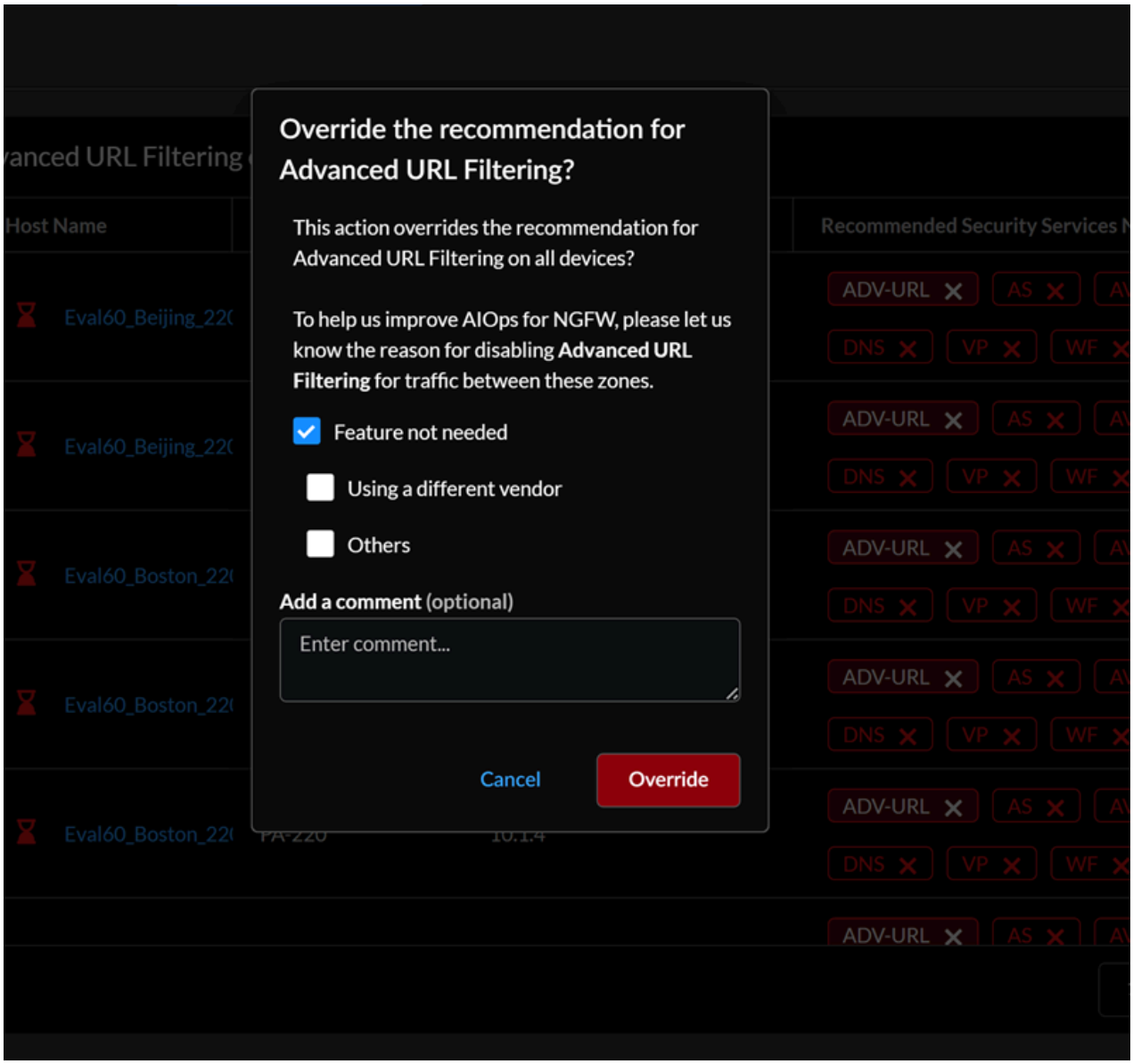
©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

在此範例中，AIOps for NGFW 建議為裝置設定進階 URL 篩選 (ADV-URL) 以及其他安全服務。您可以取消 NGFW 裝置及其下所有區域的 ADV-URL 安全服務。

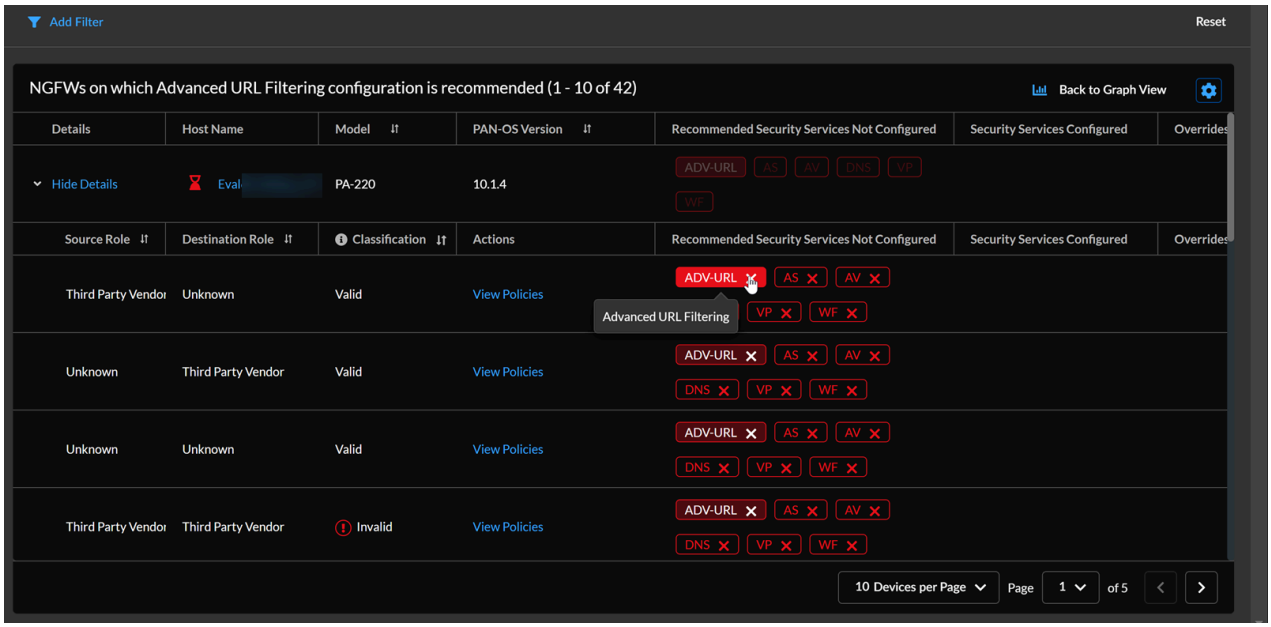
 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

您也可以在區域層級覆寫建議的安全服務。對 NGFW 檢視詳細資料，以檢視來源和目的地角色、政策以及其建議的安全服務。

 ©2025 Palo Alto Networks, Inc.

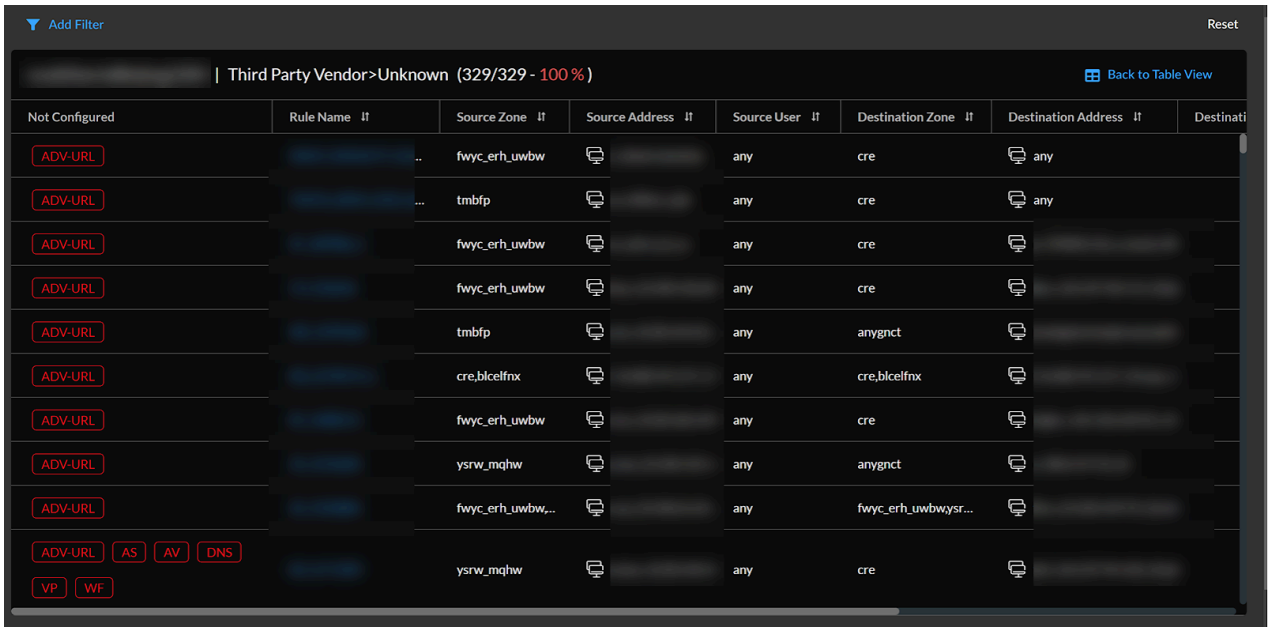


 ©2025 Palo Alto Networks, Inc.

在此範例中，您可以將來源角色的 **ADV-URL** 安全服務覆寫為 **Third Party Vendor**（第三方廠商），並將目的地角色覆寫為 **Unknown**（未知）。您也可以按一下 **Overrides**（覆寫）欄底下的安全服務，還原覆寫的建議。

您可以檢視與角色相關聯的政策。選取規則即可檢視其詳細資料，而無須離開應用程式。

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

按一下 **Back to Table View**（返回表格檢視），檢視表格格式的安全服務。

 ©2025 Palo Alto Networks, Inc.

儀表板：功能採用

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

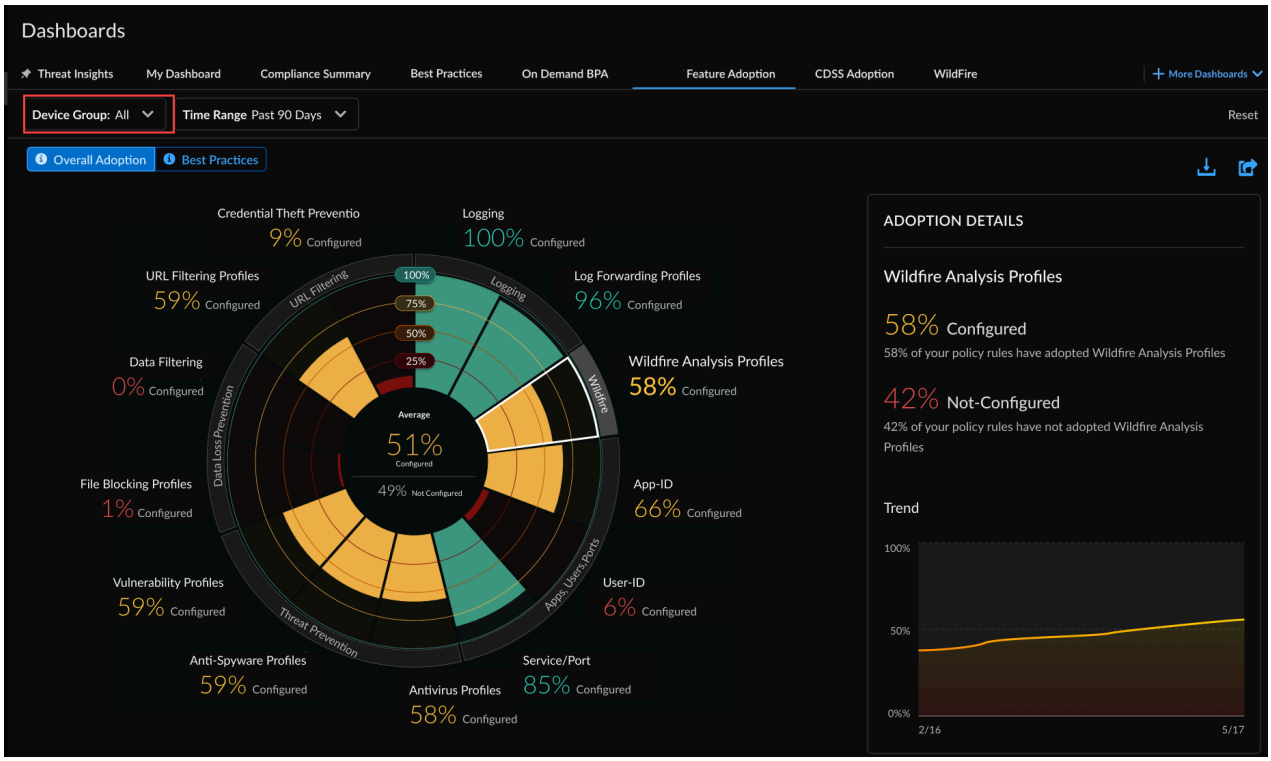
- 首先，按一下**Dashboards**（儀表板） > **Feature Adoption**（功能採用）。

此儀表板顯示哪些內容？

此儀表板會顯示所有在您的租用戶上線並傳送遙測資料之防火牆的彙總資料。

Feature Adoption（功能採用）儀表板會顯示您在部署中使用的安全功能，您可以將其用來識別採用漏洞。這有助於您確保能充分利用 Palo Alto Networks 安全訂閱和防火牆的功能。

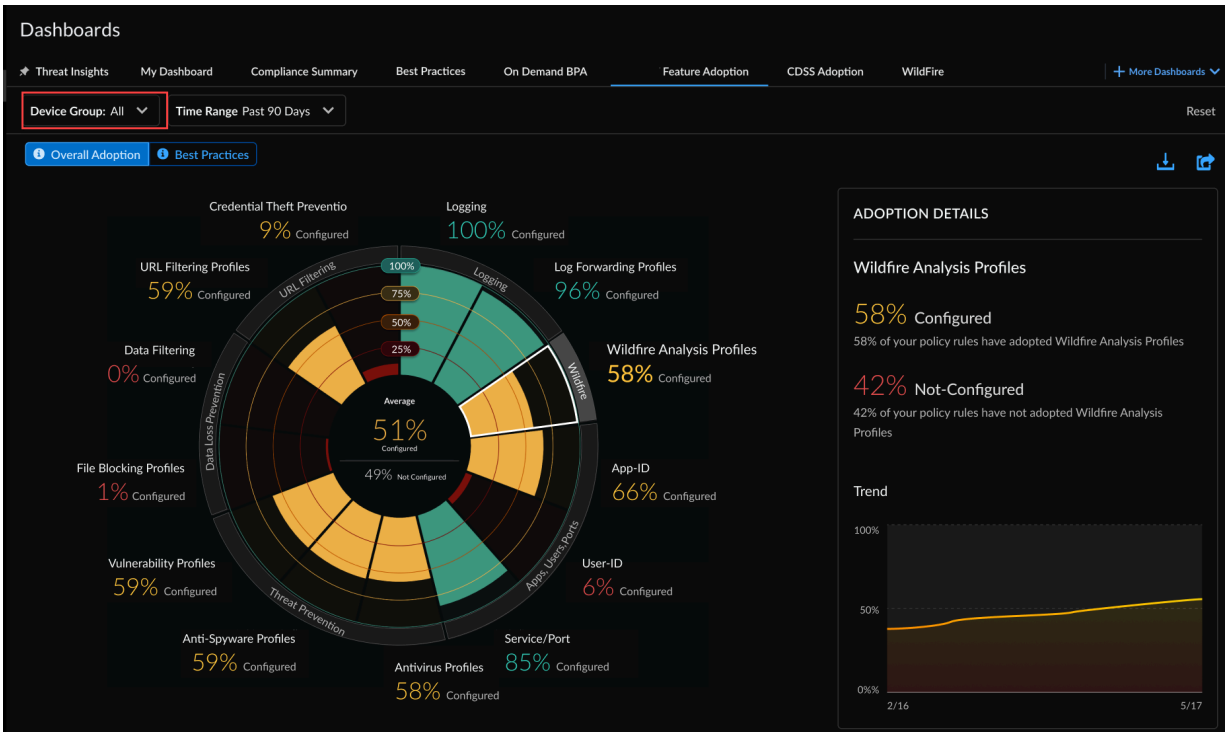
©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

如何使用此儀表板

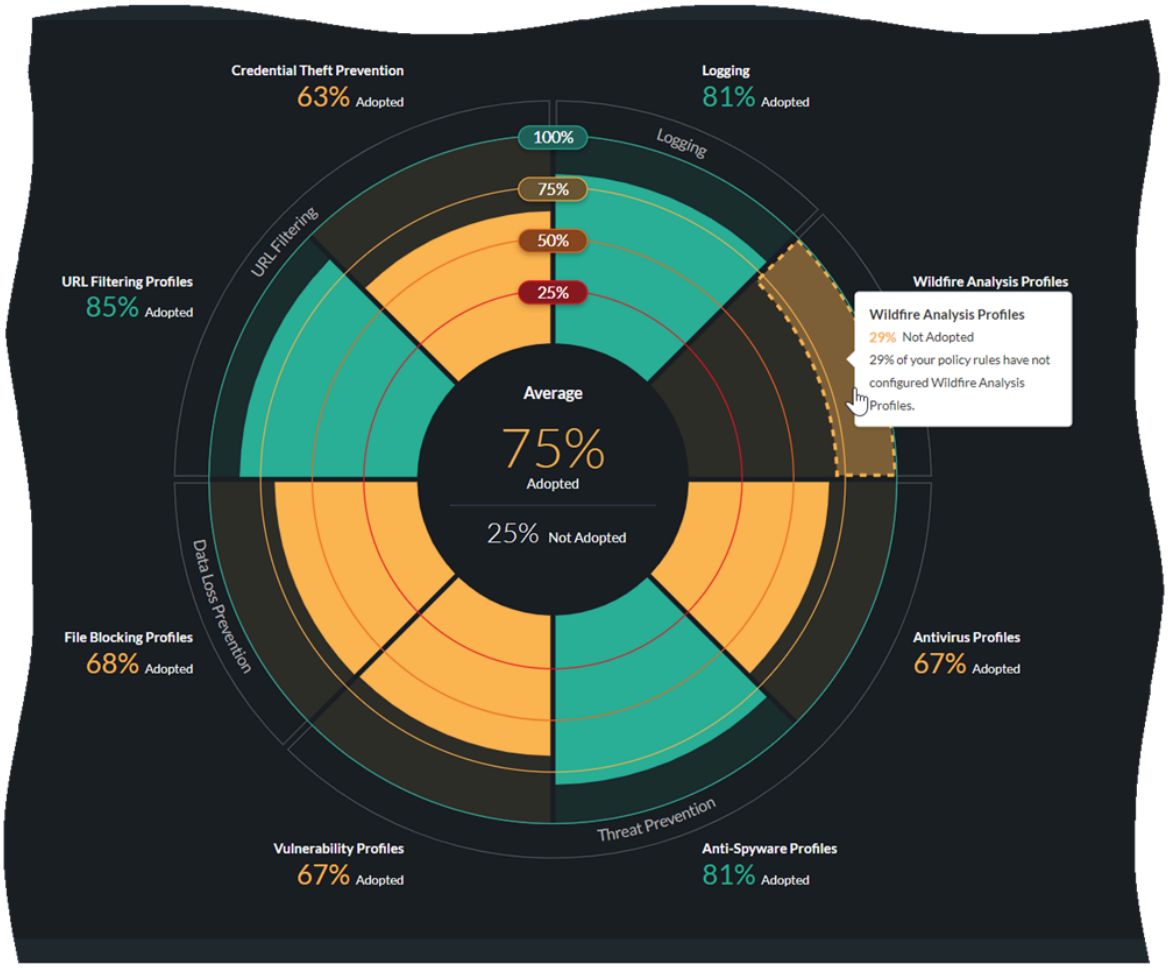
若要專注於一組特定防火牆的功能採用，您可以根據裝置群組來篩選圖表，包括 Panorama 管理的裝置。您也可以查看歷史採用趨勢圖。



 ©2025 Palo Alto Networks, Inc.

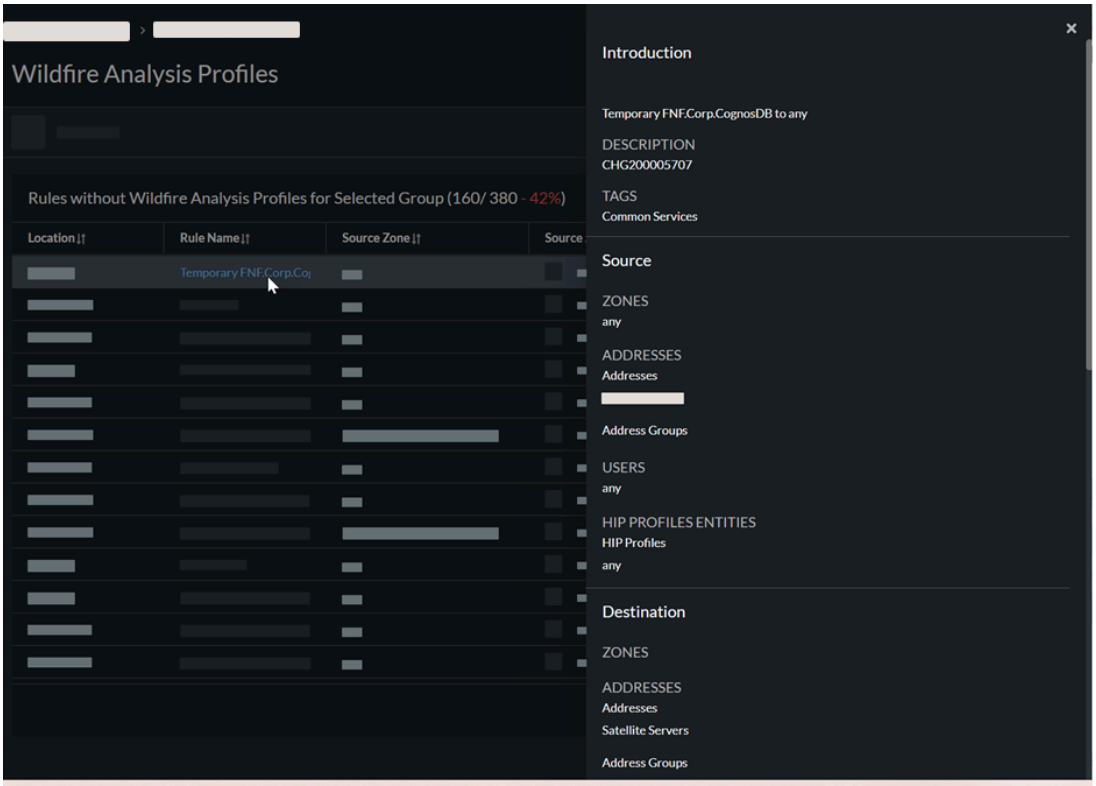
- 當您使用 *TSF* 產生隨選 *BPA* 報告時，來自 *TSF* 的採用資訊會反映在 *[Feature Adoption*（功能採用）*]* 儀表板上。（*PAN-OS 9.1* 和更新版本 *TSF*）
- 您可以匯出 *.csv* 格式的採用資料，以便在 *Microsoft Excel* 等第三方應用程式中使用

選取圖表上某個功能的區段，以檢視哪些政策規則缺少該功能。



 ©2025 Palo Alto Networks, Inc.

選取規則即可檢視其詳細資料，而無須離開應用程式。



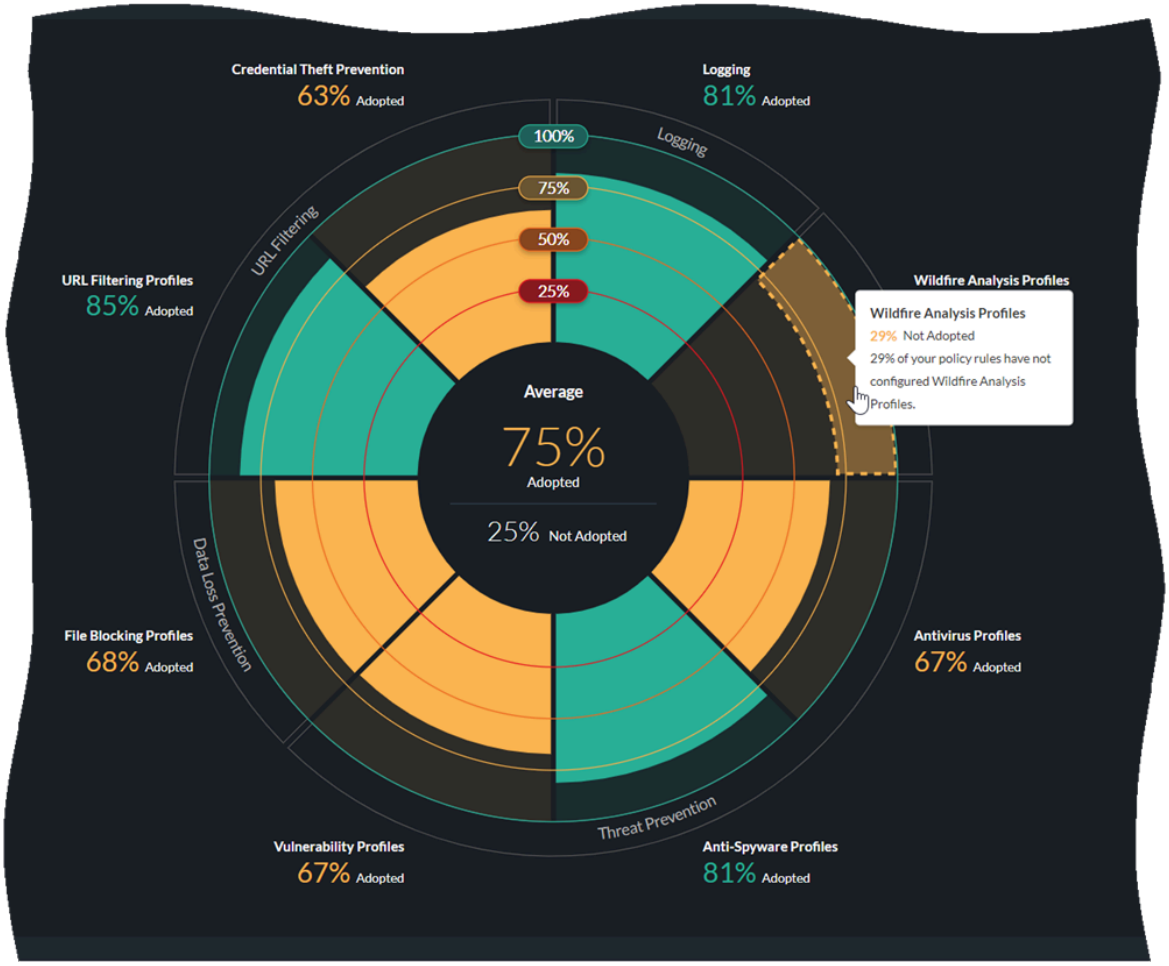
識別採用漏洞

此儀表板顯示安全政策強大的地方，以及您可以專注於改進的功能採用漏洞。若要看到最多流量以及獲得最大程度的攻擊保護，請設定安全性功能採用的目標，並使用下列建議作為最佳做法基準線。根據基準線來評估目前狀態，以識別安全性政策功能採用漏洞。

[Adoption Summary（採用摘要）] 有助於識別可改善安全性政策功能採用的裝置、區域和領域。您可以依裝置群組、序號和 Vsys、區域、架構區域、標籤、規則詳細資料和區域對應來檢閱採用資訊。在裝置群組上進行篩選，以縮小範圍並識別漏洞。

在**Dashboard**（儀表板） > **Feature Adoption**（功能採用）中選取 **Overall Adoption**（整體採用），以檢查下列功能的採用率。選取 **Best Practices**（最佳做法），查看符合 Palo Alto Networks 最佳做法之功能的採用率。使用這項資訊作為漏洞識別準則；如果實際採用率與建議不符，則請計劃縮小漏洞：

©2025 Palo Alto Networks, Inc.



- 將 WildFire 分析、防毒、反間諜軟體、弱點和檔案封鎖設定檔套用至所有允許流量的規則，且目標為 100% 或幾乎 100% 採用。如果您未將設定檔套用至允許規則，則請確定有不套用設定檔的良好業務原因。

  在所有允許規則上設定安全性設定檔，可讓防火牆檢查解密流量中是否有威脅，不論為應用程式或服務/連接埠。更新設定之後，您可以為非遙測裝置執行 BPA，以測量進度以及捕捉未連結安全性設定檔的新規則。

  您可以在沒有 *WildFire* 授權的情況下將 *WildFire* 設定檔套用至規則。覆蓋範圍限制為 *PE* 檔案，但這仍為未知的惡意檔案提供有用的可見度。

- 在反間諜軟體設定檔中，將 DNS Sinkhole 套用至所有規則，防止受危害的內部主機傳送惡意和自訂網域的 DNS 查詢、識別和追蹤可能受危害的主機，以及避免 DNS 檢查漏洞。啟用 DNS Sinkhole 可保護網路而不影響可用性，因此您可以且應該立即啟用它。
- 將 URL 篩選和認證竊取（網路釣魚）保護套用至所有輸出網際網路流量。

在 [Adoption Summary（採用摘要）] 的 [Apps, Users, Ports（應用程式、使用者、連接埠）] 摘要中，檢查下列功能的採用率。使用建議作為漏洞識別準則；如果實際採用率與建議不符，則請計劃縮小漏洞：

- 將 App-ID 套用至盡可能接近 100% 的規則。將 User-ID 套用至來源區域或位址範圍內存在使用者的所有規則（部分區域可能沒有使用者來源；例如，資源中心區域中的來源應該是伺服器，

 ©2025 Palo Alto Networks, Inc.

而非使用者）。利用 App-ID 和 User-ID 來建立政策，以允許適當的使用者認可（和容忍）應用程式。明確封鎖惡意和不需要的應用程式。

- 目標設為 100% 或接近 100% 服務/連接埠採用，不允許非標準連接埠上的應用程式，除非它有適當的業務原因。

在 [Adoption Summary（採用摘要）] 的 [Logging（記錄）] 摘要中，檢查下列功能的採用率。使用建議作為漏洞識別準則；如果實際採用率與建議不符，則請計劃縮小漏洞：

- 目標是等於或接近記錄和日誌轉送的 100% 採用。
- 設定所有區域上的區域保護設定檔。

總結：

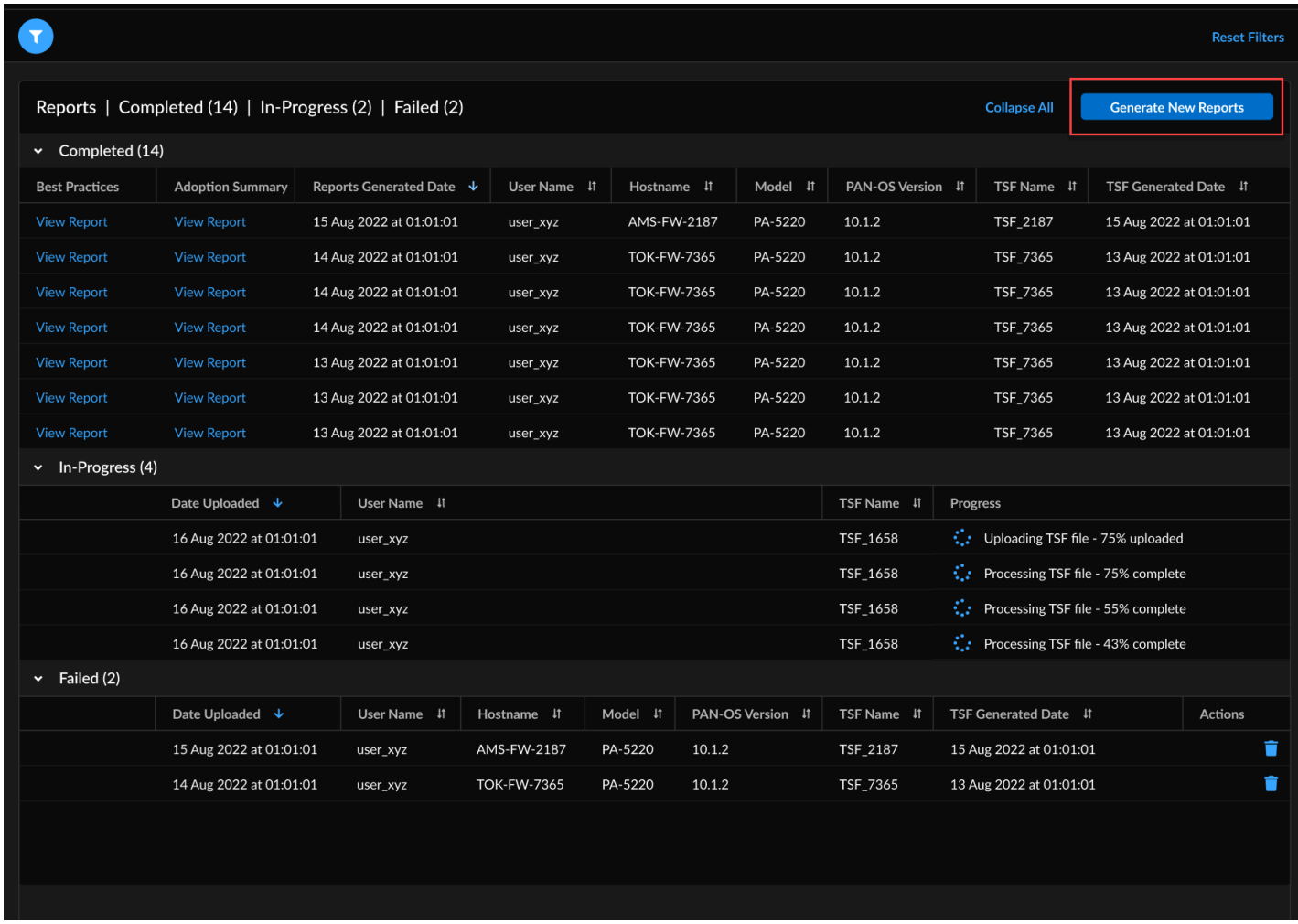
功能	採用目標
WildFire	盡可能接近 100% 的安全性政策規則
防毒軟體	盡可能接近 100% 的安全性政策規則
反間諜軟體	盡可能接近 100% 的安全性政策規則
漏洞	盡可能接近 100% 的安全性政策規則
檔案封鎖	盡可能接近 100% 的安全性政策規則
URL 篩選和認證竊取	所有輸出網際網路流量
App-ID	盡可能接近 100% 的安全性政策規則
使用者-ID	來源區域或位址範圍內存在使用者的所有規則
服務/連接埠	盡可能接近 100% 的安全性政策規則
記錄	盡可能接近 100% 的安全性政策規則
日誌轉送	盡可能接近 100% 的安全性政策規則
區域保護	所有區域

 ©2025 Palo Alto Networks, Inc.

儀表板：隨選 BPA

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

- 首先，按一下**Dashboards**（儀表板） > **On Demand BPA**（隨選 **BPA**）。



此儀表板顯示哪些內容？

此儀表板會根據裝置上傳的 *TSF* 檔案顯示最佳做法評估 *(BPA)* 報告。

©2025 Palo Alto Networks, Inc.

現在您可以直接從 Strata Cloud Manager 執行最佳做法評估 (BPA) 和功能採用摘要。只需上傳技術支援檔案 (TSF) 即可。您可以為不傳送遙測資料或未載入 AIOps for NGFW 的裝置產生隨選 BPA 報告。

儀表板中的資料可以如何使用？

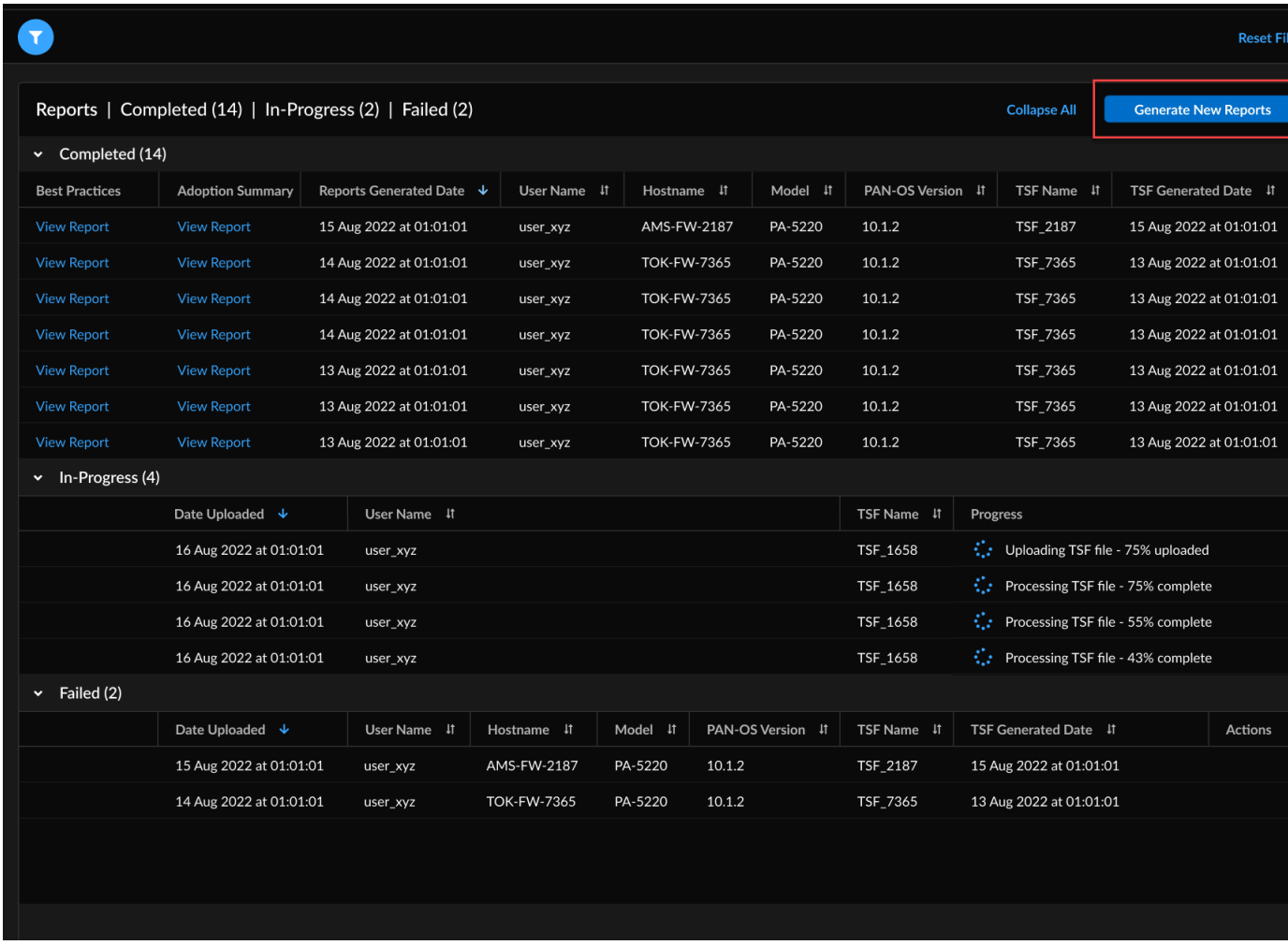
BPA 會根據 Palo Alto Networks 最佳做法評估您的安全性狀態，並優先進行裝置的改進。安全性最佳做法可防止已知和未知威脅、減少攻擊面，以及查看流量，因此您可以知道和控制網路上的應用程式、使用者和內容。此外，最佳做法包括對 Center for Internet Security 的重大安全性控制 (CSC) 進行檢查。請參閱最佳做法指南，以加強安全性狀態並實施改善。

產生隨選 BPA 報告

請依照下列步驟隨需產生 BPA 報告。

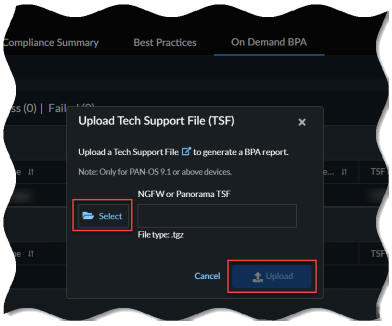
STEP 1 | 移至**Dashboards**（儀表板） > **On Demand BPA**（隨選 **BPA**）。

STEP 2 | 產生新的 **BPA** 報告。



 ©2025 Palo Alto Networks, Inc.

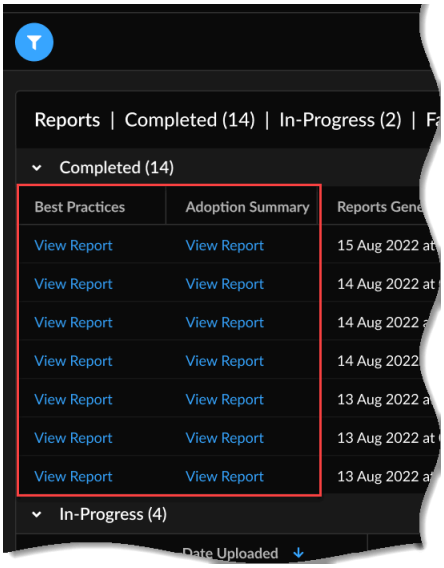
STEP 3 | 選取 **TSF** 並上傳 **TSF** 檔案。



上傳時間取決於 .tgz 檔案的大小和您的網路速度。對於較大的檔案，上傳檔案可能需要幾分鐘的時間。展開 **In-Progress**（進行中）以檢視 TSF 檔案的狀態。

- 隨選 *BPA* 僅支援 *.tgz* 檔案格式的技術支援檔案 *(TSF)*。
- 隨選 *BPA* 支援來自 *PAN-OS* 版本 *9.1* 或更高版本裝置的 *TSF*，用於產生報告。
- 如需 *Palo Alto Networks* 的資料擷取、處理和遙測儲存的相關資訊，請參閱信任中心的 AIOps for NGFW 隱私權。

STEP 4 | 檢視 **Completed**（已完成）下的報告，以檢視結果。



 ©2025 Palo Alto Networks, Inc.

儀表板：SASE 健康情況

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	• 其中一個： ❑ Prisma Access 和 ADEM 可觀察性 ❑ Strata Cloud Manager Pro • 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

此儀表板顯示哪些內容？

此儀表板會顯示目前連線至 Prisma Access 的行動使用者、遠端站台和應用程式的整體健康情況（如果您已購買 AI-Powered ADEM 授權）。圓圈中的數字代表目前從其所在的 Prisma Access 位置連線的使用者或站台數目。一個點代表一個使用者或站台。地圖上具有藍色背景的區域，表示該區域中顯示的數值是預測的。

使用下列一或多個篩選器來篩選此儀表板中顯示的資料

- 時間範圍
- Prisma Access 位置
- 來源位置

儀表板中的資料可以如何使用？

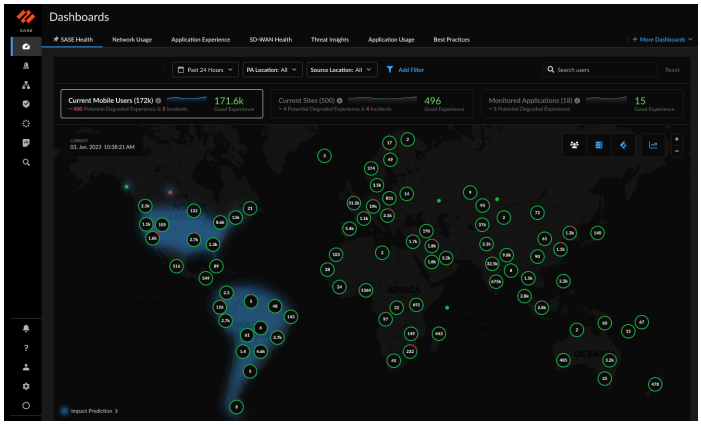
使用儀表板大致瞭解有多少行動使用者和遠端站台連線至 Prisma Access，及其整體健康情況（按其在地圖上的位置分類）。您也可以在此儀表板中檢視其整體健康情況。

SASE 健康情況儀表板：目前的行動使用者 - 地圖檢視

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	• 其中一個： ❑ Prisma Access 和 ADEM 可觀察性 ❑ Strata Cloud Manager Pro • 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

©2025 Palo Alto Networks, Inc.

SASE Health（**SASE** 健康情況）儀表板中的 **Current Mobile Users**（目前行動使用者）頁籤會概述行動使用者體驗在所有位置的詳細資訊。圓圈中的數字對應於目前使用 GlobalProtect 連線至 Prisma Access 的行動使用者數目。一個點代表一個行動使用者。綠色圓圈或點表示使用者體驗分數為「良好」。紅色圓圈則表示體驗分數下降。下級的體驗分數包括「尚可」和「不良」分數的組合。**Current Mobile Users**（目前行動使用者）右側的折線圖顯示所有的目前行動使用者在選定時間範圍內的平均體驗分數趨勢。



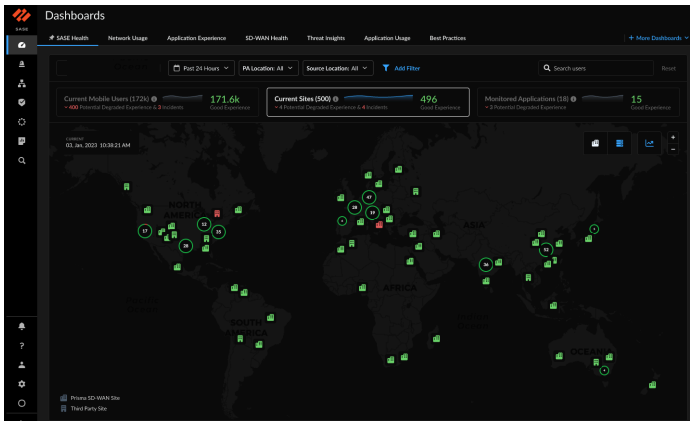
按一下 **Potential Degraded Experience**（潛在降級的體驗）或 **Incidents**（事件）旁的數字（代表體驗可能下降的使用者計數），在左側開啟的窗格中查看降級使用者體驗的詳細資料。

SASE 健康情況儀表板：目前站台 - 地圖檢視

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	• 其中一個： ❑ Prisma Access 和 ADEM 可觀察性 ❑ Strata Cloud Manager Pro • 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

此儀表板會顯示連線至全球 Prisma Access 位置的已設定站台數目。括號中的數字是已連線的站台總數，卡片右側的數字則是獲得「良好」體驗分數的站台數目。在計算連線站台數目時，不會排除基於任何原因無法獲得體驗分數的站台。藍線折線圖表示所有站台在一段時間內的平均體驗分數趨勢。在 [Current Sites（目前站台）] 底下，您可以看到體驗分數降低（不良）的站台數目，以及所有站台的事件數目。事件可能屬於以下一或多個類別：基礎架構、網路服務、資料中心和第三方站台（資料中心已關閉）。

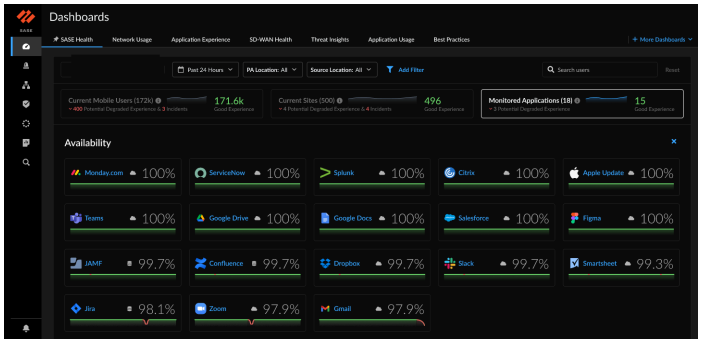
 ©2025 Palo Alto Networks, Inc.



SASE 健康情況儀表板：受監控的應用程式

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	• 其中一個： ❑ Prisma Access 和 ADEM 可觀察性 ❑ Strata Cloud Manager Pro • 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

在 **SASE Health**（**SASE** 健康情況）儀表板的 （受監控應用程式）頁籤中，查看應用程式可用性指標。此儀表板會顯示有多少應用程式透過 ADEM 受到監控，以及其中有多少個分數下降的應用程式。該數字同時將行動使用者和遠端站台的應用程式體驗納入考量。應用程式體驗分數為「不良」或「尚可」的應用程式，會被視為體驗下降。您也可以查看在您使用篩選器選取的時間範圍內，應用程式的可用性如何。



應用程式名稱右側的數字表示應用程式在時間範圍內處於可用狀態的時間百分比。

 ©2025 Palo Alto Networks, Inc.

監控：Strata Cloud Manager

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目 • Prisma SD-WAN	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN 可見性所需的其他授權和先決條件包括： ❑ ADEM 可觀察性 ❑ 遠端網路的自發 DEM ❑ 採用 AI 技術的 ADEM ❑ WAN Clarity 報告 ❑ 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

全方位檢視您的網路流量，以及您透過 Strata Cloud Manager 管理的產品和訂閱。您可以在 Prisma Access 中保護性地監控遠端網路、應用程式、NGFW 裝置和行動使用者的健康情況與連線狀態。Strata Cloud Manager 也有相關功能可監控常見網路服務的效能、訂閱授權耗用量的詳細資料，以及管理用來分析連線問題的工具。Prisma SD-WAN 使用者也可在單一位置監控 Prisma SD-WAN 應用程式、ION 裝置、資料中心的健康情況與連線狀態。

監控：IOC 搜尋

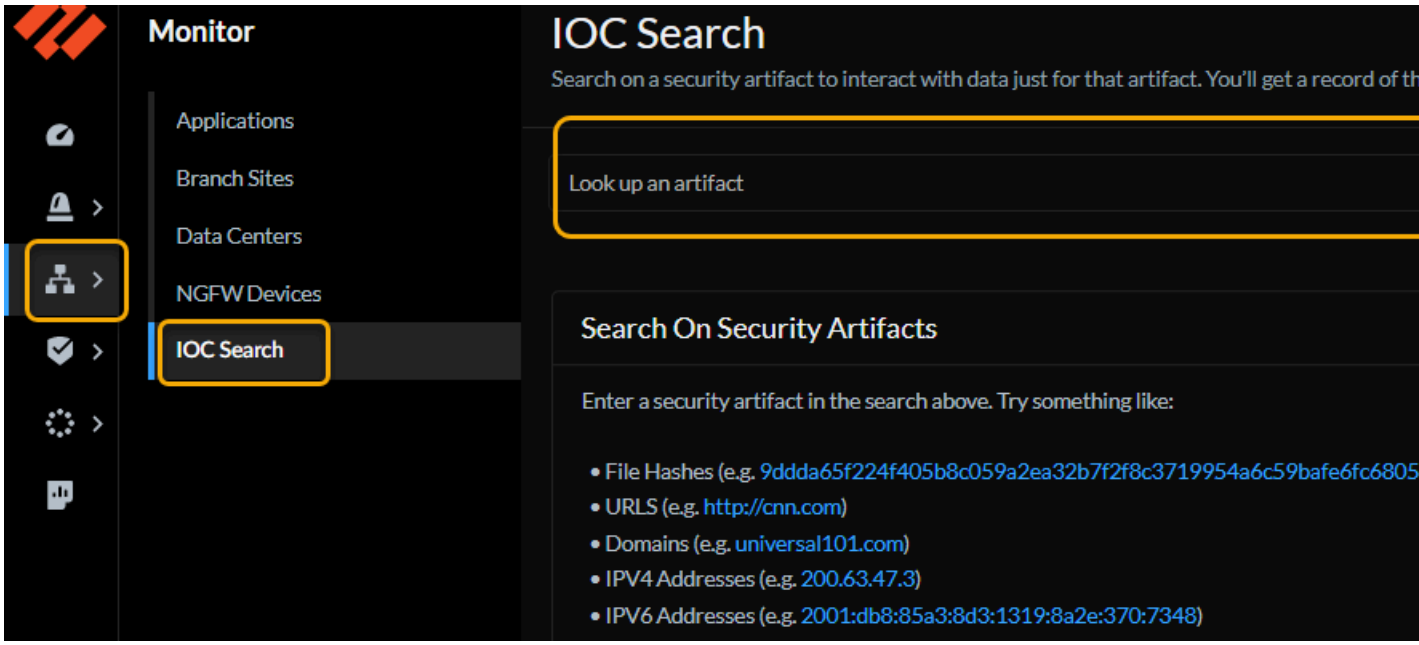
這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目 • Prisma SD-WAN	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN 可見性所需的其他授權和先決條件包括： ❑ ADEM 可觀察性 ❑ 遠端網路的自發 DEM ❑ 採用 AI 技術的 ADEM ❑ WAN Clarity 報告 ❑ 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

您可以搜尋安全性構件，而僅與該構件的資料進行互動。搜尋結果包括：

- 構件在您的網路中的歷程記錄和活動。評估該構件在您的網路中的普及性，並將其與同業進行比較。
- 關於構件的 Palo Alto Networks 威脅情報（基於對 Palo Alto Networks 處理和分析的所有流量進行的分析）。
- 構件的整合式第三方分析結果。

首先，按一下**Monitor**（監控） > **IOC Search**（**IOC** 搜尋）。

 ©2025 Palo Alto Networks, Inc.



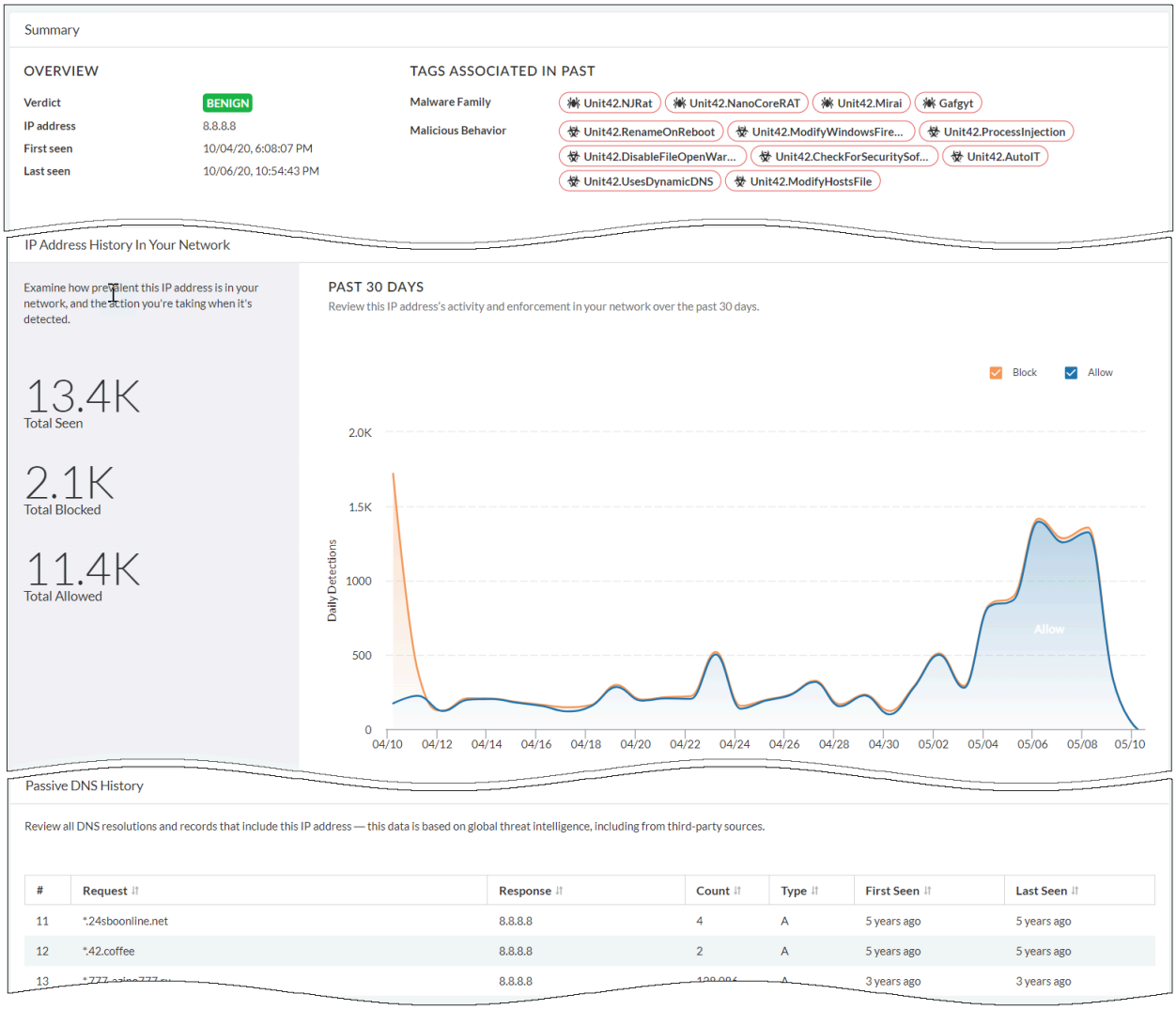
首先，請搜尋下列其中一個類型的構件：檔案雜湊、**URL**、網域或 **IP** 位址（IPv4 或 IPv6）。

IP 位址

您可以尋找 IP 位址，以分析與網路中的 IP 位址活動相關的威脅資訊。搜尋結果中會顯示下列資料：

- 過去 30 天內在您的網路中偵測到 IP 位址的總次數。
- 對 IP 位址採取的動作（允許或封鎖）的圖形呈現。
- 包含 IP 位址的 DNS 要求清單（基於 Palo Alto Networks 威脅情報和第三方來源）。

 ©2025 Palo Alto Networks, Inc.

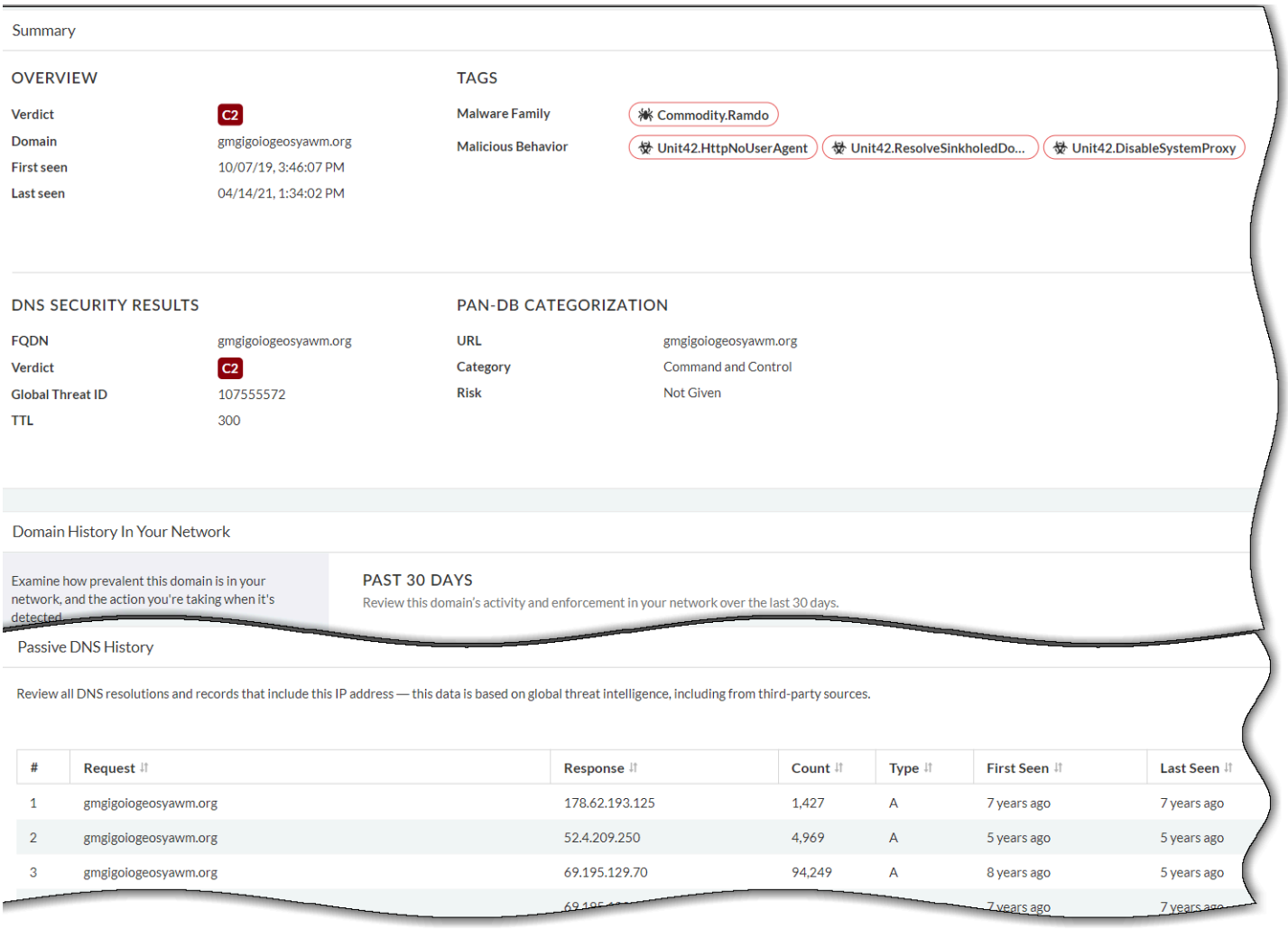


網域

檢視與網路中的網域相關聯的活動摘要。搜尋結果包括：

- 網路中的網域分類（基於 WildFire 範例分析）。
- 過去 30 天內與網域相關聯的活動總數。
- 以圖形格式對每個活動套用的強制執行。
- WildFire 分析中支援將資料用來為網域指派裁定的資訊。
- 從包含此網域執行個體的所有 WildFire 提交中收集的 DNS 活動。

 ©2025 Palo Alto Networks, Inc.

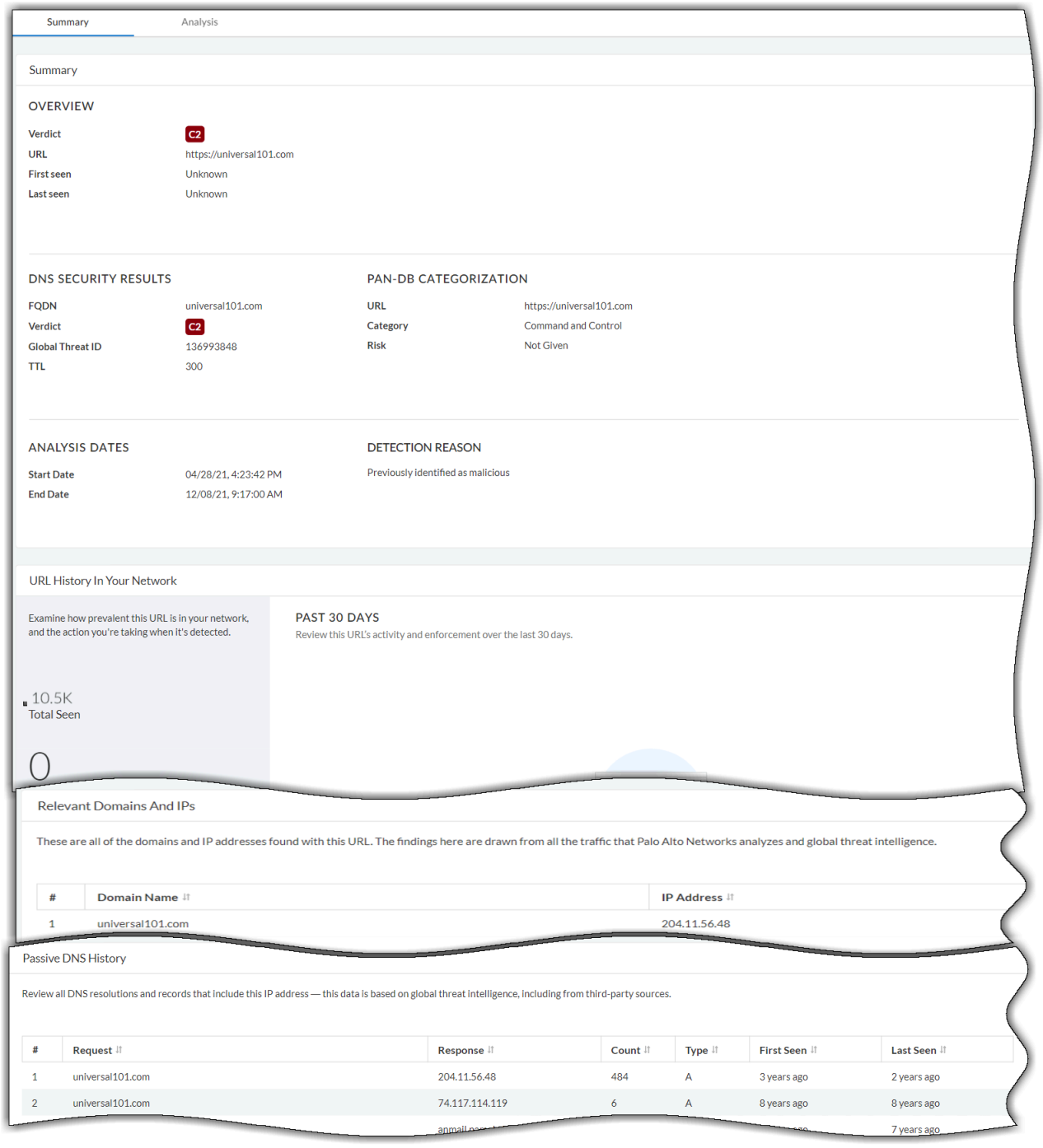


URL

瞭解 Palo Alto Networks 所分析的所有流量中的 URL 活動。搜尋結果包括：

摘要 - 檢閱網路中的 URL 活動摘要。資料包括：URL 和 PAN-DB 分類的 DNS 安全性結果。

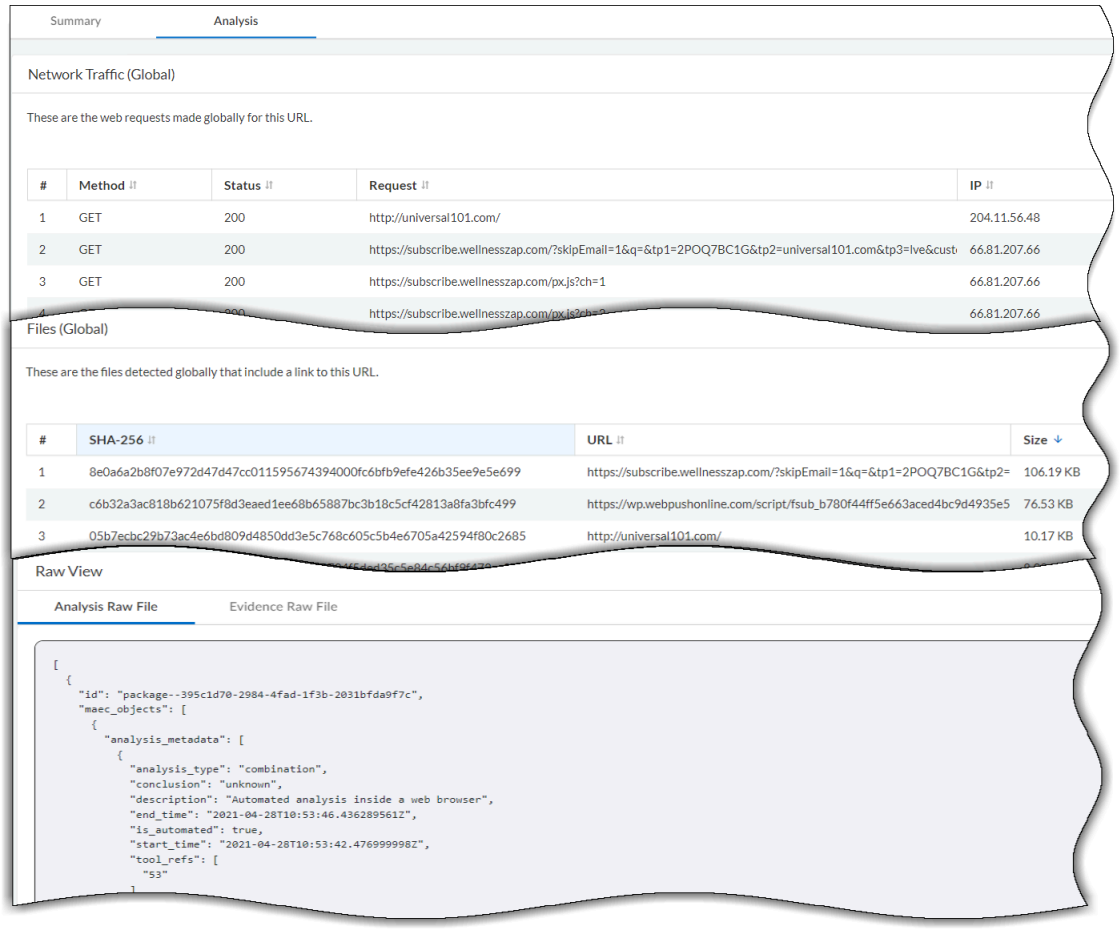
 ©2025 Palo Alto Networks, Inc.



螢幕擷取畫面 - 顯示您搜尋 URL 構件時的站台快照。

分析 - 查看檔案分析資料，其中包含為此 URL 全域發出的要求，以及使用此 URL 偵測到的檔案。您可以使用檔案雜湊值或檔案檢視來瞭解詳情。

 ©2025 Palo Alto Networks, Inc.

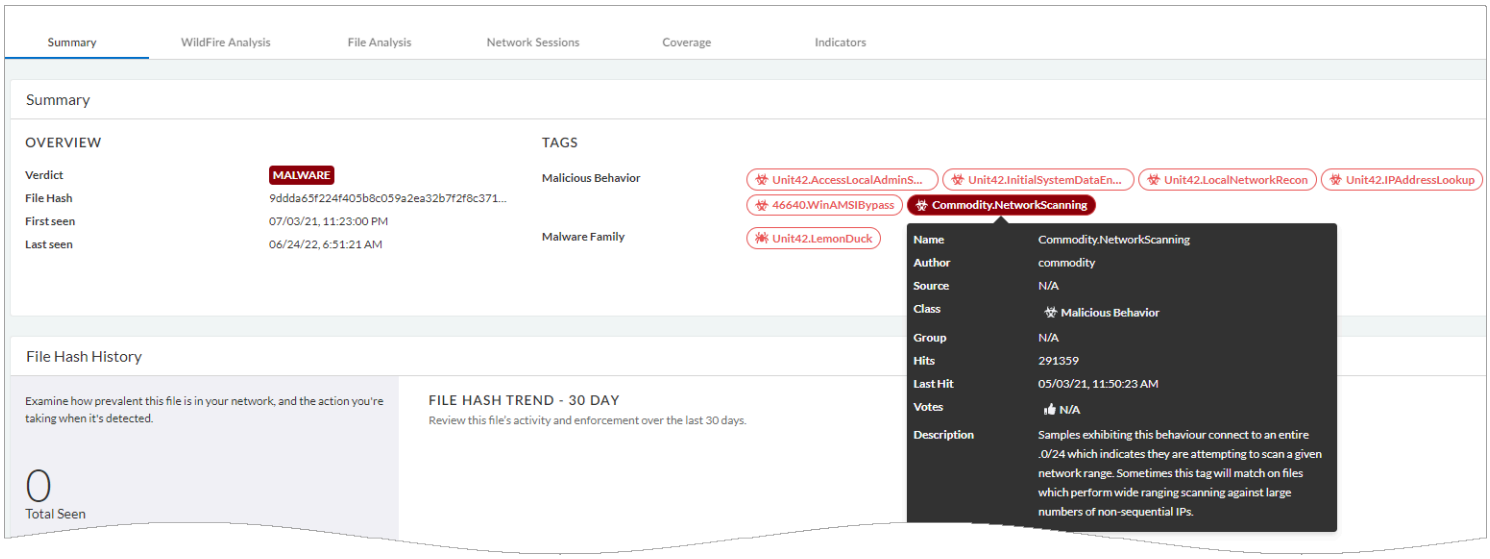


檔案雜湊

檔案雜湊搜尋會彙總檔案的活動、檔案屬性的分析，以及 WildFire 範例分析的詳細資料。您可以深入檢視搜尋結果，以檢閱下列資料：

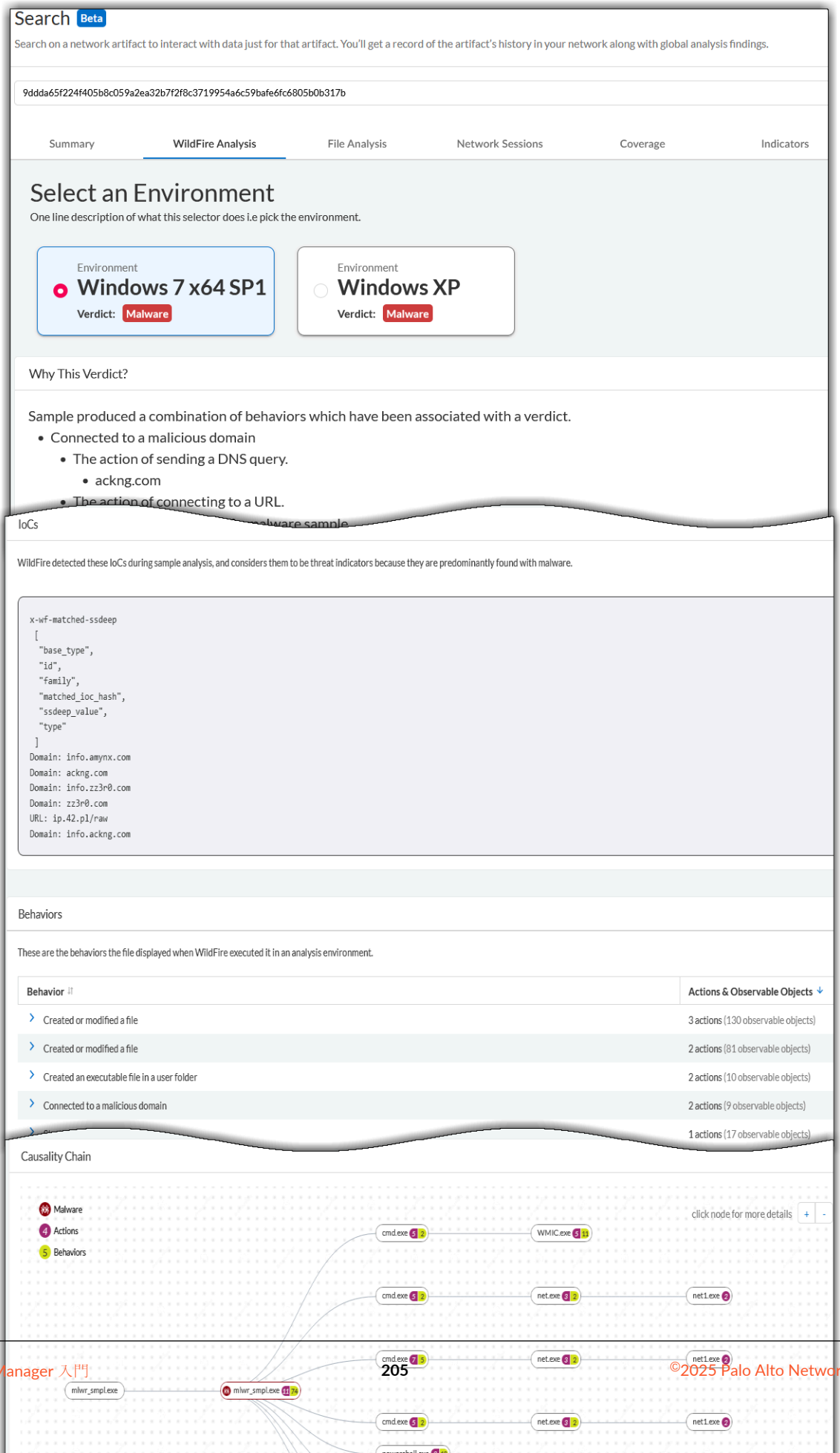
摘要 - 檢視檔案雜湊裁定，以及網路中的檔案活動歷程記錄。按一下標籤名稱，檢視該標籤的詳細資料。標籤可協助您瞭解檔案是否為任何威脅系列、活動或行為者的一部分。

 ©2025 Palo Alto Networks, Inc.



WildFire 分析 - 評估範例（檔案）在 WildFire 分析期間的行為。您可以檢視下列項目的相關資訊：範例裁定、在範例分析期間偵測到的威脅指標，以及在分析環境中處理範例時的行為。您也可以檢視在 WildFire 範例分析期間擷取的不同程序里程碑的螢幕擷取畫面。

 ©2025 Palo Alto Networks, Inc.

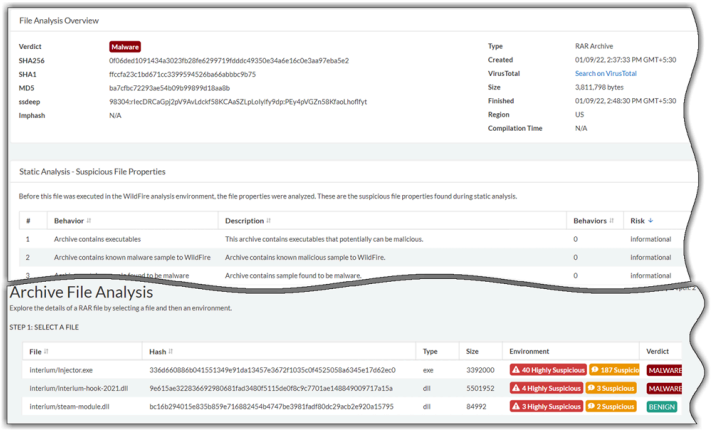


 ©2025 Palo Alto Networks, Inc.

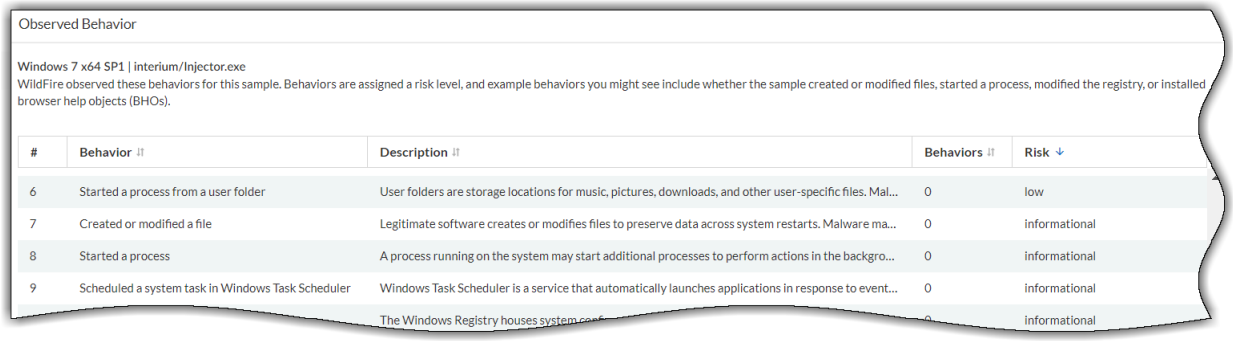
檔案分析 - 比較在 WildFire 分析環境中執行範例（檔案）之前和之後的分析。

概要 - 在此處檢查範例的裁定。如果裁定分類錯誤，請要求變更裁定。Palo Alto Networks 威脅團隊會對範例進行深入調查，若發現錯誤則更新裁定。

靜態分析 - 靜態分析會審視在 WildFire 分析環境中執行特定檔案之前的檔案內容。搜尋也會顯示在靜態分析期間發現的可疑檔案屬性。搜尋結果會隨著檔案類型而不同。此處的螢幕擷取畫面顯示封存檔的靜態分析。

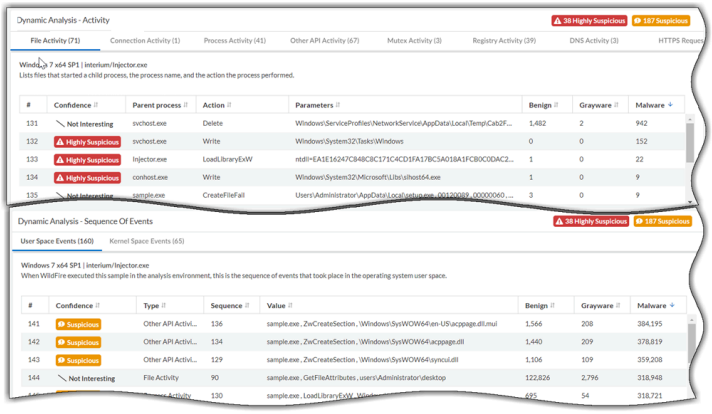


觀察到的行為 - 檢閱特定環境中樣本的 WildFire 行為分析。

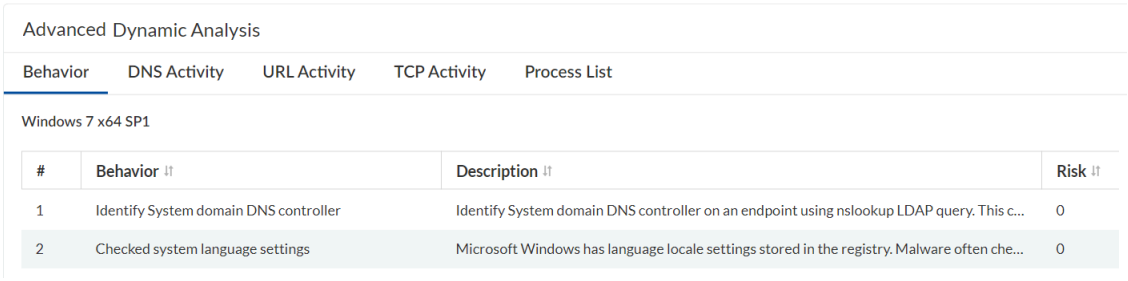


動態分析 - 詳細檢查檔案，擷取遭入侵網路的附加資訊和指標。您可以檢查涉及的程序活動，以及執行檔案時系統中的事件發生順序。

 ©2025 Palo Alto Networks, Inc.

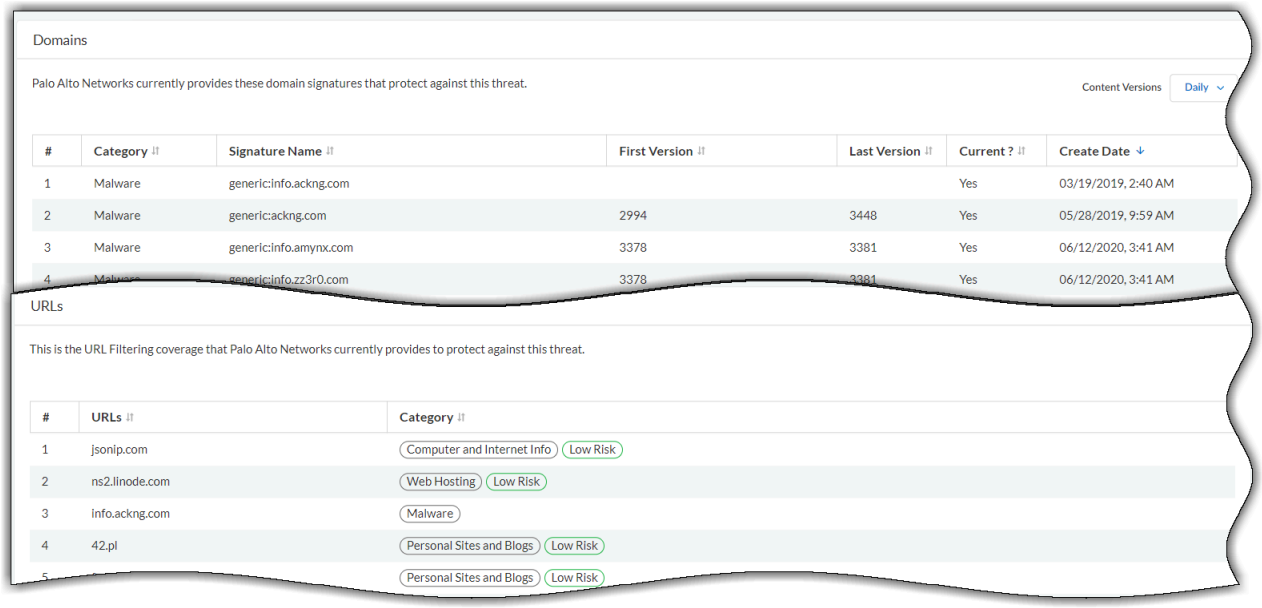


進階動態分析 - 檢視由進階 WildFire 技術（智慧型執行階段記憶體分析、管理程式動態分析、依賴模擬等）分析的範例有何分析結果，這是一種雲端式引擎，可偵測和防止具高度規避能力的惡意軟體威脅。您可以檢視觀察到的行為，並使用這項資訊進行執行後的分析。



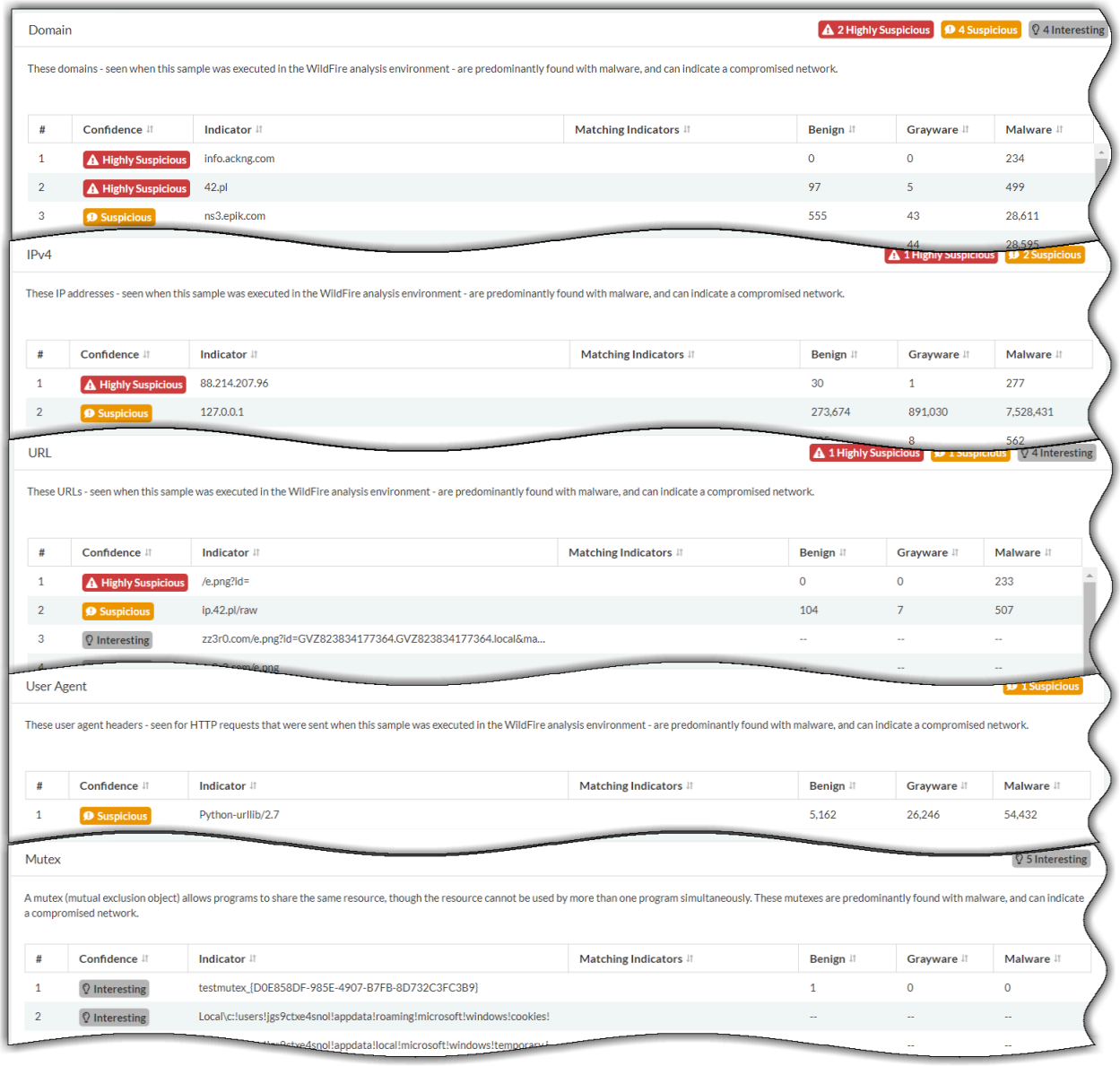
網路工作階段 - 瞭解範例的網路工作階段。使用這項資料可以深入瞭解威脅的內容、受影響的主機和用戶端，以及用來傳播惡意軟體的應用程式。

覆蓋範圍 - 檢查範例的特徵碼覆蓋範圍，以評估對威脅的防護層級。您可以檢視標記到下載範例之網域的特徵碼，以及範例所存取的 URL。



 ©2025 Palo Alto Networks, Inc.

指標 - 檢視作為網路組成指標的構件。指標會根據構件類型進行分類；網域、IP 位址、URL、使用者代理程式標頭，以及互斥物件。高風險構件被標示為「可疑」或「高度可疑」。



 ©2025 Palo Alto Networks, Inc.

監控：分支站台

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目 • Prisma SD-WAN	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN 可見性所需的其他授權和先決條件包括： ❑ ADEM 可觀察性 ❑ 遠端網路的自發 DEM ❑ 採用 AI 技術的 ADEM ❑ WAN Clarity 報告 ❑ 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

分支站台：**Prisma Access**

選取**Monitor**（監控） > **Branch Sites**（分支站台） > **Prisma Access**，以檢視遠端網路的健康情況與連線，以及部署在不同 Prisma Access 位置的所有遠端網路的使用情況。其中顯示即時連線狀態和頻寬消耗詳細資料，以及其他部署詳細資料。行動使用者、分公司和零售地點連線至遠端網路。您也可以檢視在「遠端網路」和「行動使用者」中設定之通道的健康情況。

除了與 Prisma Access 授權一起顯示的 Widget 以外，此儀表板只會在您擁有 ADEM Observability 或 AI-Powered ADEM 授權時，才會顯示站台體驗分數和 Prisma SD-WAN 分支站台詳細資料頁面。

分支站台：**Prisma SD-WAN**

選取**Monitor**（監控） > **Branch Sites**（分支站台） > **Prisma SD-WAN**，以在 Prisma SD-WAN 中設定分支站台。分支站台包含您在 Prisma SD-WAN 的廣域網路中擁有的分公司。您可以在 ION 裝置到達給定站台之前或之後設定分支站台。Prisma SD-WAN 中的分支站台提供下列檢視：

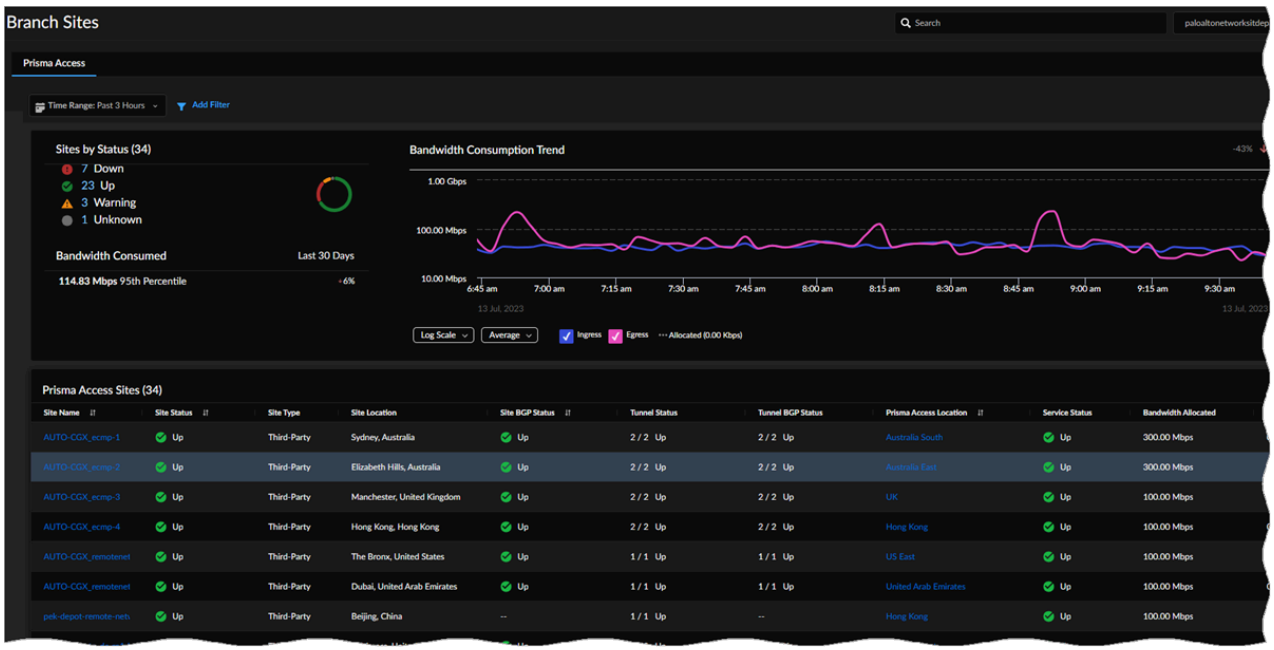
- 分支站台的 **Map**（地圖）檢視提供分支站台裝置與控制器的連線狀態，以及站台的警報狀態。
- **List**（清單）檢視會顯示在選取的 **Time Range**（時間範圍）內有多少個站台處於作用中狀態，以及分支站台的整體健康情況指標。
- **Activity**（活動）檢視會顯示重要應用程式分析、最新的站台健康情況分數，以及一段時間內的站台健康情況分佈。

 ©2025 Palo Alto Networks, Inc.

- Prisma Access
- Prisma SD-WAN

分支站台 (Prisma Access)

選取**Branch Sites**（分支站台） > **Prisma Access**，以檢視遠端網路的健康情況與連線，以及部署在不同 Prisma Access 位置的所有遠端網路的使用情況。



其中顯示即時連線狀態和頻寬消耗詳細資料，以及其他部署詳細資料。行動使用者、分公司和零售地點連線至遠端網路。您也可以檢視在「遠端網路」和「行動使用者」中設定之通道的健康情況。如需這些 Widget 的詳細說明，請參閱檢視和監控分支站台。

您可以：

- 按狀態查看您的遠端網站。
- 檢視遠端網路頻寬消耗的趨勢。
- 檢視您的 Prisma Access 站台，然後選取任何站台以檢視更多詳細資料。
- 開啟 **IPSec Termination Node Utilization Details**（**IPSec** 終止節點使用率詳細資料），以檢視站台中每個 SPN 的頻寬消耗詳細資料。
- 檢視站台的通道資料和通道趨勢。
- 檢視站台狀態、健康情況、連線性和耗用量資訊。

分支站台 (Prisma SD-WAN)

您可以在 ION 裝置到達給定站台之前或之後設定分支站台。Prisma SD-WAN 中的分支站台提供下列檢視：

 ©2025 Palo Alto Networks, Inc.

- 分支站台的 **Map**（地圖）檢視提供分支站台裝置與控制器的連線狀態，以及站台的警報狀態。選取分支站台時，會顯示下列資訊：
  - 站台摘要：用於分析和疑難排解。
  - 設定：用於站台和裝置設定。
  - 覆疊連線：用來檢視所有 VPN 覆疊連線的狀態。
- **List**（清單）檢視會顯示在選取的 **Time Range**（時間範圍）內有多少個站台處於作用中狀態，以及分支站台的整體健康情況指標。不良站台的平均分數，是所有被認定為不良的不良站台範例的平均值。時間序列圖會根據選取的持續時間計算和重新整理。例如，支援的持續時間分別是一小時、三小時、24 小時、七天、30 天和 90 天，間隔分別是一分鐘、五分鐘、一小時和一天。
  - 站台連線健康情況分佈：給定的租用戶基於最新站台連線健康情況分佈的「良好」、「尚可」和「不良」站台分佈圖。
  - 一段時間的站台連線健康情況分佈：執行裝置軟體 5.6.1 或更高版本的健康情況分數的時間序列圖。
  - 站台應用程式體驗分數：站台應用體驗分數。
  - **Prisma SD-WAN** 分支站台：檢視分支站台的站台健康情況、站台連線健康情況、線路健康情況、安全網狀架構健康情況，以及接近容量閾值。您可以按站台預測、警報狀態和 ADEM 狀態進一步檢視及篩選分支站台。
- **Activity**（活動）檢視會顯示重要應用程式分析、最新的站台健康情況分數，以及一段時間內的站台健康情況分佈。其中包括：
  - 站台健康情況分佈：根據最新的站台健康情況分數，顯示給定租用戶的「良好」、「尚可」和「不良」站台分佈圖。
  - 一段時間內的站台健康情況分佈：根據分支站台的健康情況分數，顯示給定租用戶在一段時間內的站台健康情況分佈的時間序列圖表。
  - 頻寬使用率：顯示站台和 WAN 路徑上每個應用程式的頻寬使用率，並顯示網路中消耗最多頻寬的十大應用程式的資料。
  - 交易統計資料：顯示 TCP 流量的交易統計資料，包括特定應用程式或所有應用程式、特定路徑或所有路徑，以及所有健康情況事件的起始/交易成功和失敗。
  - 新流量：顯示給定期間的一個應用程式、一組特定應用程式或所有應用程式的新 TCP 和 UDP 流量。
  - 並行流量：協助您瞭解網路上有多少作用中的連線（按應用程式）。

 ©2025 Palo Alto Networks, Inc.

監控：資料中心

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目 • Prisma SD-WAN	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN 可見性所需的其他授權和先決條件包括： ❑ ADEM 可觀察性 ❑ 遠端網路的自發 DEM ❑ 採用 AI 技術的 ADEM ❑ WAN Clarity 報告 ❑ 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

監控服務連線、ZTNA 連接器和站台連線在 Prisma SD-WAN 資料中心的運作情形。選取**Monitor**（監控） > **Prisma Access** > **Data Centers**（資料中心） > **Service Connections**（服務連線）或 **ZTNA Connectors**（**ZTNA** 連接器）頁籤，在 Prisma Access 中檢視服務連線和 ZTNA 連接器的健康情況和狀態。

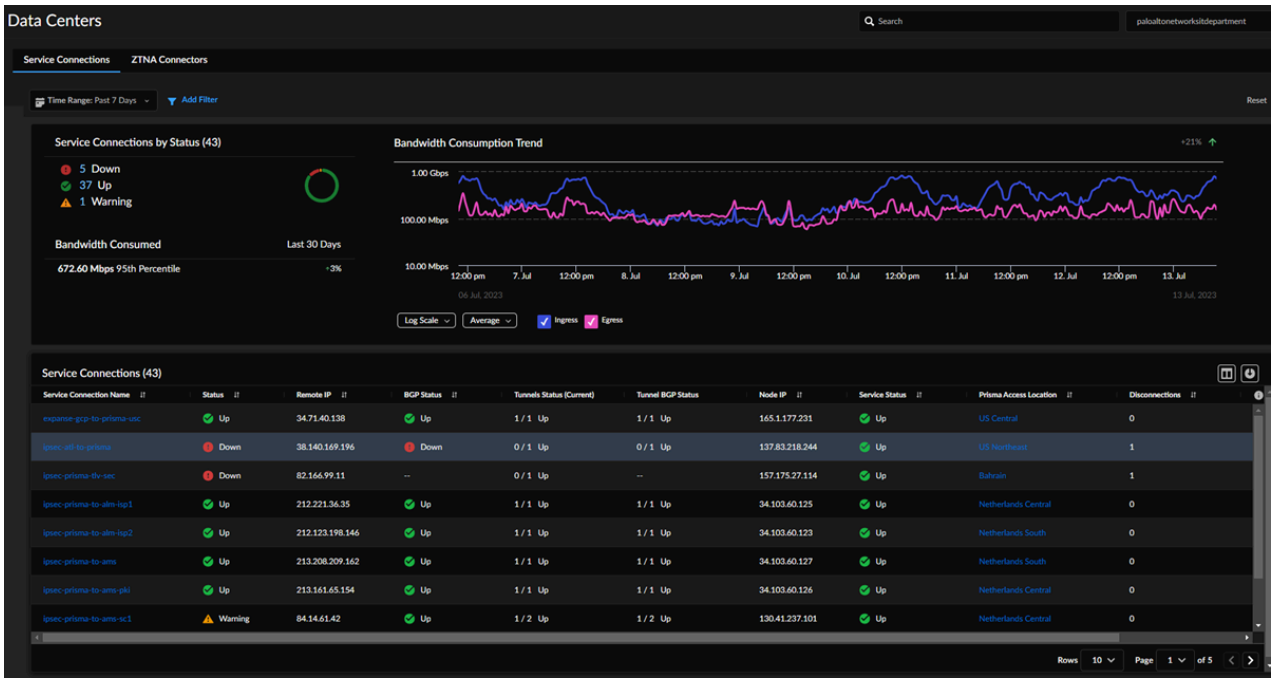
針對每個 Prisma SD-WAN 資料中心，選取**Monitor**（監控） > **Data Centers**（資料中心） > **Prisma SD-WAN**，以檢視站台連線資訊和 VPN 覆疊連線的狀態。

- 服務連線
- ZTNA 連接器
- Prisma SD-WAN

服務連線

首先，選取 **Monitor**（監控） > **Data Centers**（資料中心） > **Service Connections**（服務連線）。

©2025 Palo Alto Networks, Inc.



檢視彙總的服務連線資料，以及個別服務連線的相關資訊。服務連線支援行動使用者和遠端網路。除了提供對公司資源的存取，服務連線也允許您的行動使用者連線到分支位置。如需這些 Widget 的詳細說明，請參閱 *Prisma Access* 管理指南中的檢視和監控資料中心。

- 選取時間範圍，以按狀態及其頻寬消耗趨勢檢視服務連線。
- 檢視所有服務連線的健康狀態。
- 檢視您所有服務連線的頻寬消耗趨勢。
- 檢視服務連線的相關資料，例如狀態、遠端 IP 位址、BGP 狀態、目前通道狀態和其他資料。選取任何服務連線以檢視其詳細資料。

ZTNA 連接器

首先，選取**Monitor**（監控） > **Data Centers**（資料中心） > **ZTNA Connectors**（**ZTNA** 連接器）。

零信任網路存取 (ZTNA) 連接器可簡化所有應用程式的私人應用程式存取。您環境中的 ZTNA 連接器 VM 會自動在您的私人應用程式與 Prisma Access 之間形成通道。檢視所有已設定的 ZTNA 連接器的摘要，包括與連接器相關聯的 **Application Targets**（應用程式目標）、其平均頻寬和中位數頻寬，以及 **Status**（狀態）（開啟、部分開啟、關閉）。如需這些 Widget 的詳細說明，請參閱 *Prisma Access* 管理指南中的檢視和監控資料中心。

您可以：

- 檢視 ZTNA 連接器群組的健康情況和狀態。
- 檢視個別 ZTNA 連接器的健康情況和狀態。

 ©2025 Palo Alto Networks, Inc.

資料中心 (Prisma SD-WAN)

Prisma SD-WAN 站台包含您希望在廣域網路中擁有的資料中心。您可以在資料中心託管企業應用程式和服務。在建立資料中心的過程中，您可以選取預設網域和政策集、設定 WAN 網路、線路類別、線路標籤和線路規格。Prisma SD-WAN 資料中心畫面會顯示資料中心清單，包括資料中心名稱、ION 裝置，以及站台任何開啟的警報。

對於資料中心，您會看到：

- **Configuration**（設定）頁籤，會顯示站台連線資訊、部署模式、WAN 多點傳送對等群組設定檔、網際網路和私人 WAN 線路，以及 IP 前置詞。您也可以設定使用者代理程式，並檢視資料中心的叢集設定詳細資料。
- **Overlay Connections**（覆疊連線）頁籤會顯示所有 VPN 覆疊連線的狀態。每個站台的連線都是根據其 VPN 覆疊連線的狀態計算的。

 ©2025 Palo Alto Networks, Inc.

監控：網路服務

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目 • Prisma SD-WAN	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN 可見性所需的其他授權和先決條件包括： ❑ ADEM 可觀察性 ❑ 遠端網路的自發 DEM ❑ 採用 AI 技術的 ADEM ❑ WAN Clarity 報告 ❑ 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

在**Monitor**（監控） > **Network Services**（網路服務）頁面中，您可以檢視對存取應用程式的使用者體驗造成影響的常用網路服務的效能。選取 **GlobalProtect Authentication**（**GlobalProtect** 驗證）頁籤，以檢視 GlobalProtect 在不同位置的驗證成功或失敗計數。選取 **Network Services: DNS**（網路服務：**DNS**），查看在租用戶間接收到、與 Prisma Access DNS Proxy 有關的 DNS Proxy 要求和回應。

- GlobalProtect 驗證
- DNS

GlobalProtect 驗證

首先，選取**Monitor**（監控） > **Network Services**（網路服務） > **GlobalProtect Authentication**（**GlobalProtect** 驗證）。

 ©2025 Palo Alto Networks, Inc.

在 [Insights（洞察）] 中，您可以檢視對存取應用程式的使用者體驗造成影響的常用網路服務的效能。網路服務包括報告 GlobalProtect 驗證成功和失敗的次數，作為行動使用者能夠連線至 Prisma Access 的衡量標準。您可以檢視：

- GlobalProtect 在不同位置的驗證成功計數具體資料。
- GlobalProtect 在不同位置的驗證失敗計數。
- GlobalProtect 在不同位置的驗證逾時失敗。

如需這些 Widget 的詳細說明，請參閱檢視和監控網路服務。

DNS

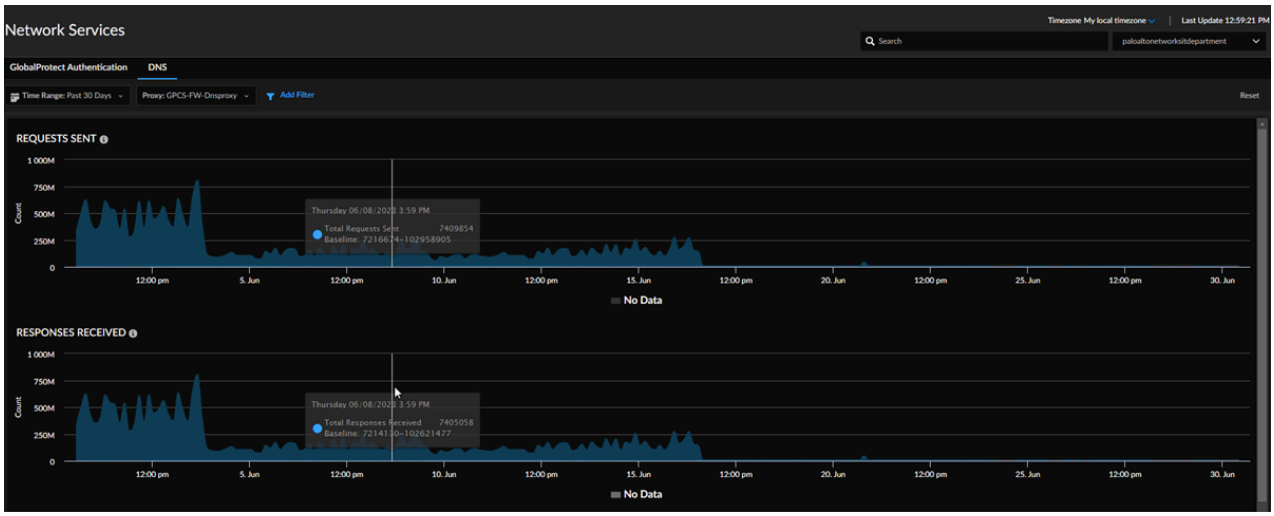
首先，選取**Monitor**（監控） > **Network Services**（網路服務） > **DNS**。

網路服務：**DNS** 會顯示 DNS Proxy 要求和回應。您可以使用下列篩選器：

- 時間範圍
- **DNS Proxy** 名稱

DNS Proxy 篩選器值與最近 30 天有關，且會在您載入時自動選取（也就是說，如果沒有明確 Proxy 資料，則沒有明確 Proxy 篩選器）。如需詳細資訊，請參閱檢視和監控網路服務。

 ©2025 Palo Alto Networks, Inc.

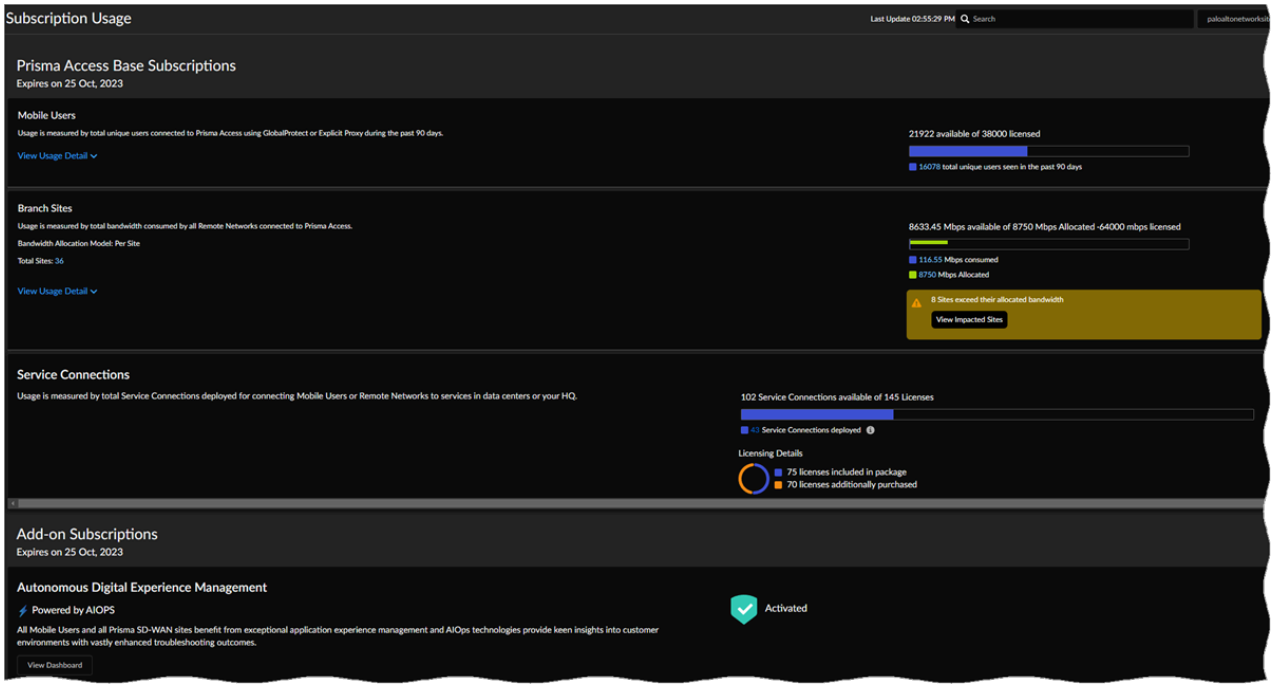


 ©2025 Palo Alto Networks, Inc.

監控：訂閱使用情況

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ Prisma Access 授權 ❑ AI-Powered ADEM 可解鎖特定功能。

選取**Monitor**（監控） > **Subscription Usage**（訂閱使用情況）檢視 **Prisma Access Base** 訂閱使用情況的詳細資料，包括已連線的唯一使用者總數、遠端網路使用者消耗的頻寬、已部署的服務連線總數，以及關於任何附加元件訂閱的詳細資料。



- 行動使用者：檢視您到目前為止已使用多少個唯一的行動使用者授權。此 Widget 會顯示連線至 Prisma Access 的唯一行動使用者在過去 90 天內耗用的授權總數，因為授權是以過去 90 天的 Prisma Access 登入資料為準的。過去 90 天內至少曾登入 Prisma Access 一次的使用者，會消耗一個行動使用者授權。
- 分支站台：查看所有連線至 Prisma Access 的遠端網路所耗用的總頻寬使用量。檢視您配置了多少頻寬，以及耗用了多少頻寬（以 Mbps 為單位）。您可以按所有連線至 Prisma Access 的遠端網路所耗用的總頻寬，來查看使用量。
- 訂閱使用情況：查看您到目前為止已耗用多少個服務連線授權。

請參閱此頁面上的 **Add-on Subscriptions**（附加元件訂閱）區段，瞭解您已購買的附加元件授權，例如行動使用者和遠端網路的 **Autonomous Digital Experience Management**（自主數位體驗管理）授權。您可以查看已購買的授權總數，以及迄今為止未使用的授權數量。檢視 **Application Tests for Mobile User Monitoring**（用於行動使用者監控的應用程式測試） - 您可以為行動使用者

 ©2025 Palo Alto Networks, Inc.

建立的剩餘應用程式測試數目。應用程式測試取決於受監控的行動使用者數目，每個行動使用者最多允許 10 個應用程式測試。

如需詳細資訊，請參閱檢視和監控訂閱使用情況。

 ©2025 Palo Alto Networks, Inc.

監控：ION 裝置

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma SD-WAN	❑ Prisma SD-WAN 授權

Prisma SD-WAN 中的 ION 裝置可讓您將不同的 WAN 網路（例如 MPLS、LTE 和網際網路連結）結合為單一、高效的混合式廣域網路 (WAN)。

Device List（裝置清單）畫面提供關於 Prisma SD-WAN 裝置清單的資訊，包括 ION 裝置的軟體版本和狀態，您可以在其中升級裝置的軟體版本或設定裝置。

實體	說明
裝置名稱	顯示為 ION 裝置設定的名稱。
裝置資訊	顯示 ION 裝置的類型和序號。
軟體	顯示裝置目前的軟體版本。按一下 **Upgrade**（升級），變更裝置軟體版本。
上次活動	顯示關於 ION 裝置上次於何時設定和升級的資訊。
狀態	顯示 ION 裝置目前的狀態。
備援	顯示 ION 裝置是否屬於高可用性 (HA) 設定的一部分。
動作	您可以從省略符號功能表中選擇，以設定 ION 裝置。

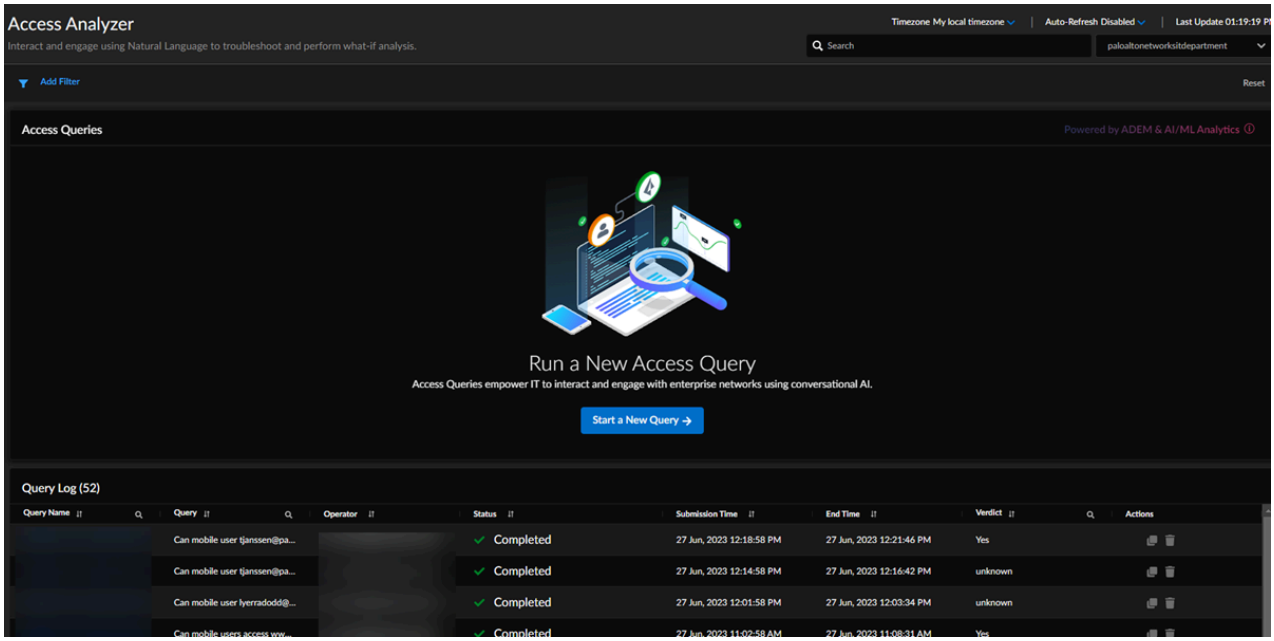
Device Activity（裝置活動）畫面會顯示站台在過去 24 小時內的各種裝置活動報告。

 ©2025 Palo Alto Networks, Inc.

監控：存取分析器

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ Prisma Access 授權 ❑ AI-Powered ADEM 授權

選取**Monitor**（監控） > **Access Analyzer**（存取分析器），以啟動新的存取分析器查詢，並檢視現有查詢的表格。



存取分析器提供了對 SASE 環境的自動監控功能。它提供了一個用於內容疑難排解和假設性分析的對話式 AI 工具，供您分析 SASE 環境中的存取和連線問題。

您可以：

- 瞭解如何在存取分析器中建立自然語言查詢。
- 啟動新的存取分析器查詢。
- 檢視現有查詢的清單，並從表格中選取任何查詢以檢視更多詳細資料。

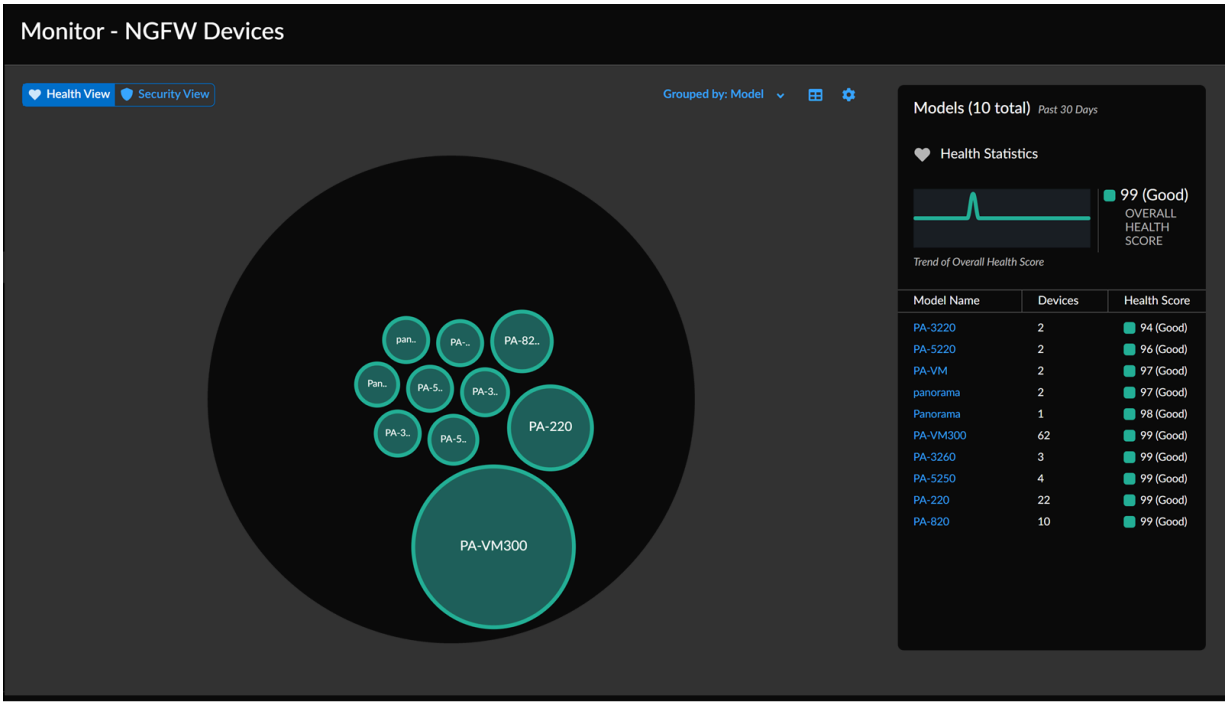
©2025 Palo Alto Networks, Inc.

監控：NGFW 裝置

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ AIOps for NGFW Free (use the AIOps for NGFW Free ap ❑ 軟體 NGFW 積分 （適用於 *VM-Series* 軟體 *NGFW*）

在**Monitor**（監控） > **NGFW Devices**（**NGFW** 裝置）中，您會看到部署中的裝置以彩色的互動方式呈現，以便您輕鬆直觀地進行管理和調查。

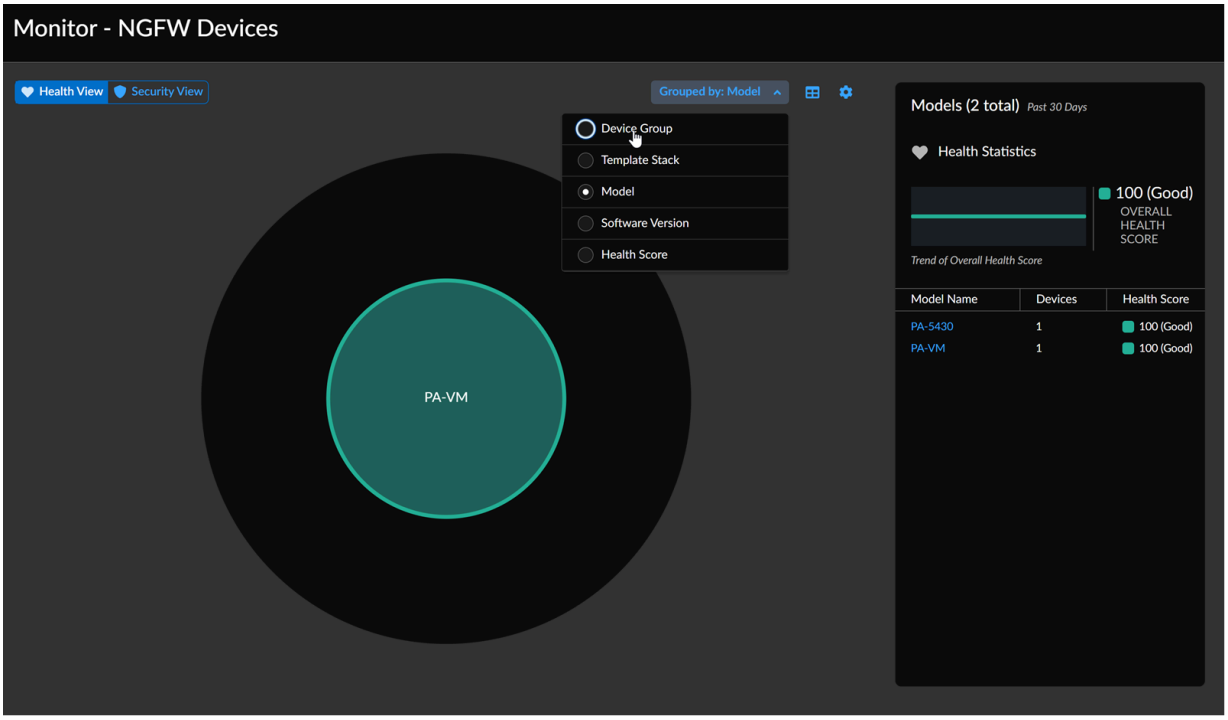
STEP 1 | 選取**Monitor**（監控） > **NGFW Devices**（**NGFW** 裝置）。



STEP 2 | 選取 **Health**（健康情況）或 **Security**（安全性）。

©2025 Palo Alto Networks, Inc.

STEP 3 | 選取您要以哪個屬性作為視覺效果的分組依據。



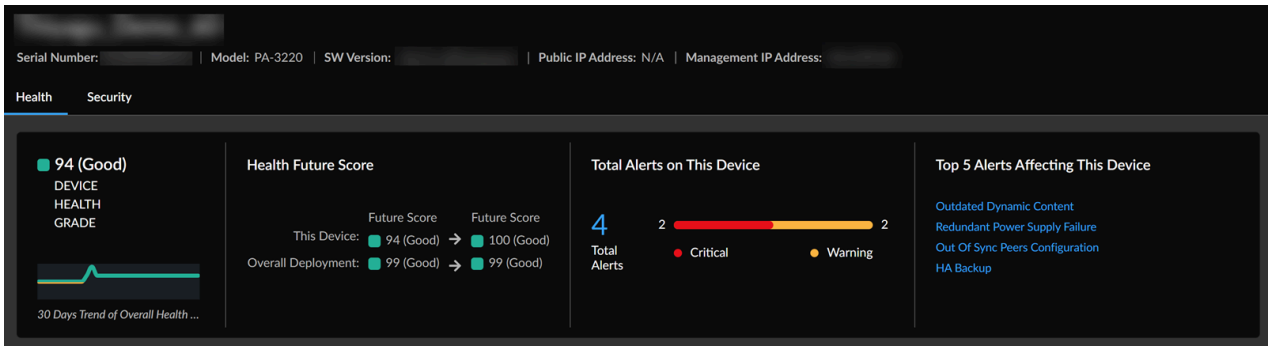
Device Group（裝置群組）和 ***Template Stack***（範本堆疊）群組選項僅適用於由 *Panorama* 管理、且 *Panorama* 會傳送裝置遙測的部署中。

STEP 4 | 選取群組以檢視其中的裝置，然後選取裝置以檢視其相關的一般資訊。

如果您想進一步瞭解裝置，請選取該裝置。

檢視裝置詳細資料

從 **NGFW Devices**（**NGFW** 裝置）視覺效果中選取裝置，或經由應用程式其他位置的連結進行選取，即可檢視關於防火牆或 Panorama 設備的特定詳細資料，例如健康情況等級、指標、連線等等。



裝置健康情況等級

裝置目前的健康情況等級，圖表會顯示其過去 30<x> 天的歷程記錄。可能的健康情況等級為「良好」、「尚可」、「不良」和「嚴重」。

 ©2025 Palo Alto Networks, Inc.

修復後的健康情況等級

您解決開放警示後的裝置健康情況等級。此圖格也會顯示關閉警示後整體部署的健康情況。

警示總計

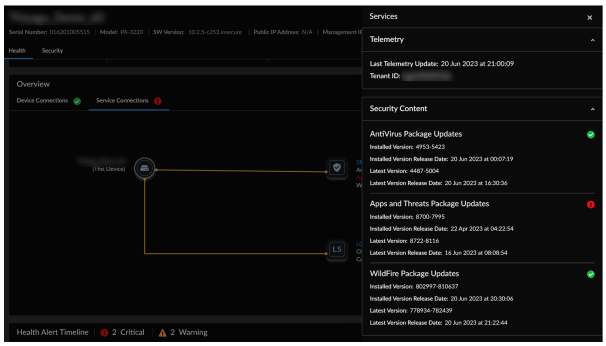
裝置上的開放警示總數。

最高排名的 **5** 個警示

此裝置上過去 30 天最常見的五個警示。

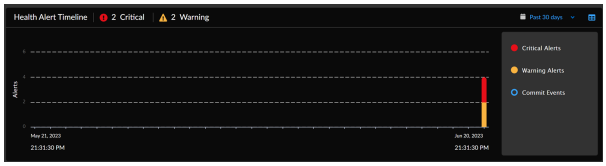
概要 > 裝置連線 連線至您目前正在檢視之裝置的其他裝置。選取裝置以檢視其詳細資料。	
概要 > 服務連線 概述與裝置整合的所有安全性和記錄服務。選取服務以檢視其詳細資料。	

 ©2025 Palo Alto Networks, Inc.



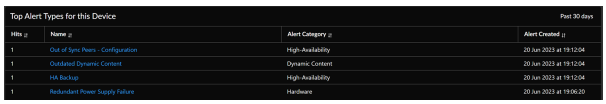
警示時間軸

裝置警示和認可事件的時間軸。警示分類為「重大」、「警告」或「認可」事件。切換為以表格格式檢視警示資料。



此裝置的最高排名警示類型

過去 30 天最常見的警示。選取警示以檢視其警示詳細資料。



最高排名的 **10** 個應用程式使用方式

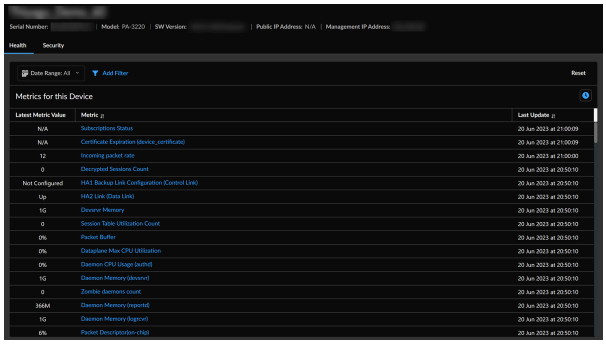
使用防火牆上最多資料的十個應用程式。

 ©2025 Palo Alto Networks, Inc.

此裝置的指標

列出所有為了對裝置執行的安全性檢查而收集的健康情況指標，包括 HA 連結資料。

選取指標以檢視其詳細資料。



 ©2025 Palo Alto Networks, Inc.

監控：容量分析器

這可在何處使用？	我需要哪些內容？
• NGFW	❑ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

容量分析器可讓您根據裝置的型號類型追踪其指標使用情況，藉以分析及監控裝置的資源容量。容量分析器提供下列優點：

- 全面瞭解現有的指標使用率和最大限制內的未使用指標容量。
- 熱圖視覺化，可以在單一檢視中顯示與硬體平台相關的指標使用情況，並且有助於深入探索詳細資料。
- 能夠根據您的特定需求規劃升級至更高容量的防火牆。

VM 系列防火牆不支援 ***Capacity Analyzer***（容量分析器）功能。

以下影片說明如何使用容量分析器功能：

容量分析器已增強，可支援警示功能，協助您預測資源耗用量是否接近最大容量，並及時觸發通知。容量分析器警示會提前 3 個月產生，以識別潛在的容量瓶頸。這有助於您規劃設定清理，或是在 NGFW 容量達到最大使用率前加以擴大，並維持系統穩定性。如需支援的容量警示清單，請參閱進階健康情況警示。

容量分析器會根據下列類型將指標分組：

- 設定資源指標，例如 NAT 政策和位址物件。
- 系統操作資源指標，例如 CPU、記憶體、磁碟和日誌。
- 流量資源指標，例如解密使用情況和工作階段表格使用率。

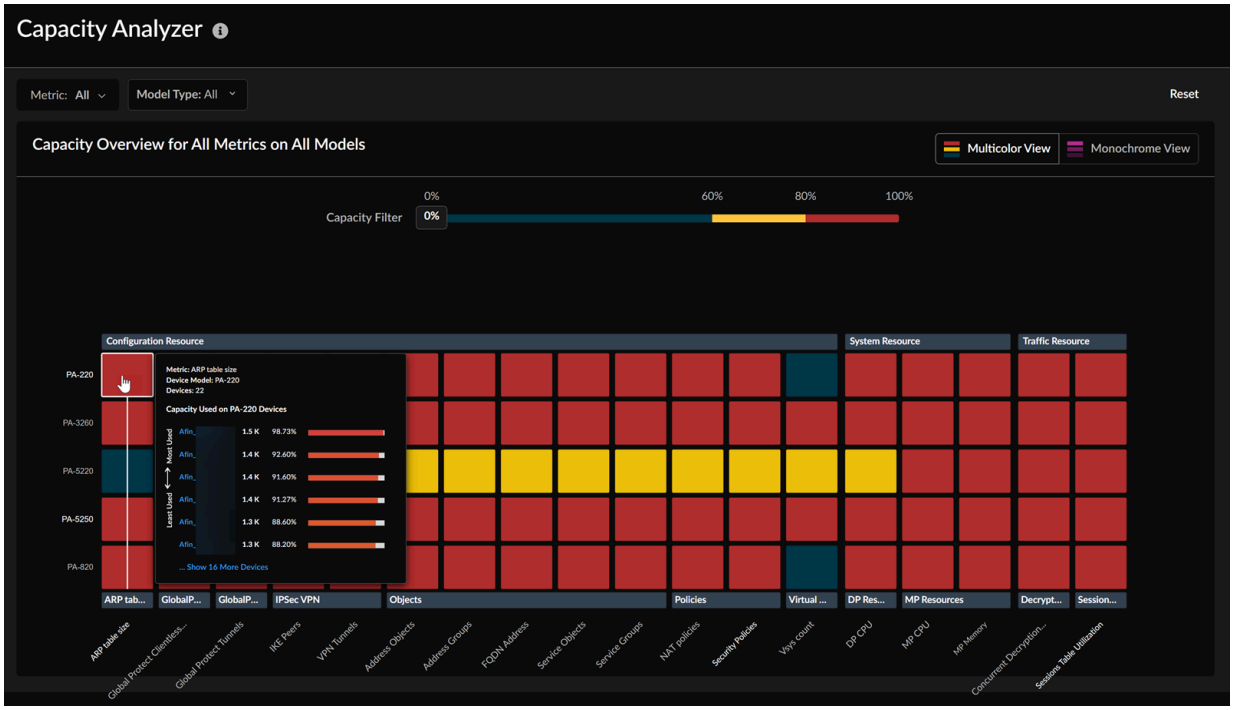
 ©2025 Palo Alto Networks, Inc.

熱圖會顯示每個裝置的指標使用情況。顏色越深表示使用率越高，淺色則表示低使用率。依預設會選取 **Multicolor View**（彩色檢視）。您也可以切換至 **Monochrome View**（單色檢視）。

以下是可以使用容量分析器熱圖來取得指標使用情況相關資訊的不同方式：

 ©2025 Palo Alto Networks, Inc.

- 將游標暫留在裝置的指標區塊上方，可檢視提供下列詳細資料的工具提示：
  - 指標的名稱
  - 裝置型號和裝置清單
  - 裝置容量範圍



- 使用下列屬性篩選資料：
  - 指標 - 選取要使用指標名稱檢視或搜尋的一或多個指標。
  - 型號 - 選取一或多個裝置型號，或使用型號名稱搜尋。
  - 容量 - 在 **Capacity Filter**（容量篩選器）刻度上選取容量。

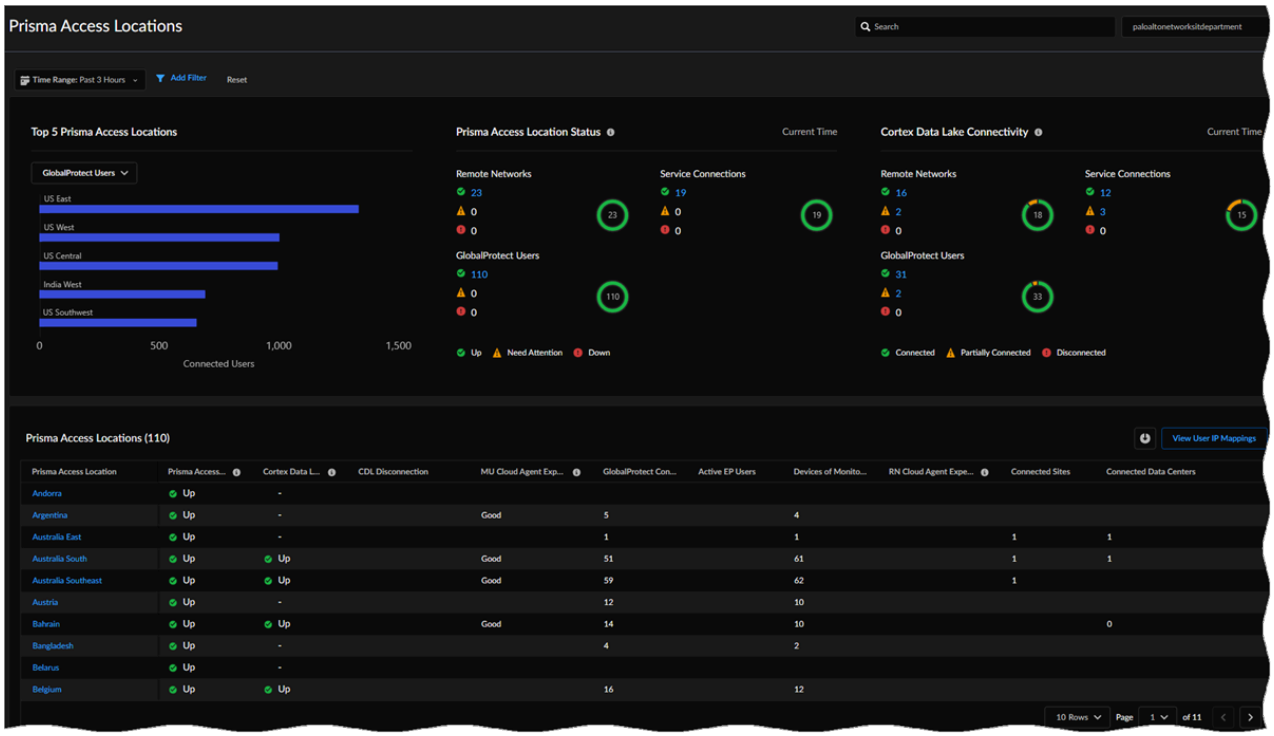
若要進一步瞭解如何使用容量分析器熱圖，請參閱分析指標容量。

 ©2025 Palo Alto Networks, Inc.

監控：Prisma Access 位置

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ Prisma Access 授權 這是 Prisma Access 洞察功能。

首先，選取**Monitor**（監控） > **Prisma Access Locations**（**Prisma Access** 位置）。在此處，您可以檢視遠端網路和行動使用者的所有 Prisma Access 位置的健康情況。如需這些 Widget 的詳細說明，請參閱 *Prisma Access* 管理指南中的檢視和監控 Prisma Access 位置。



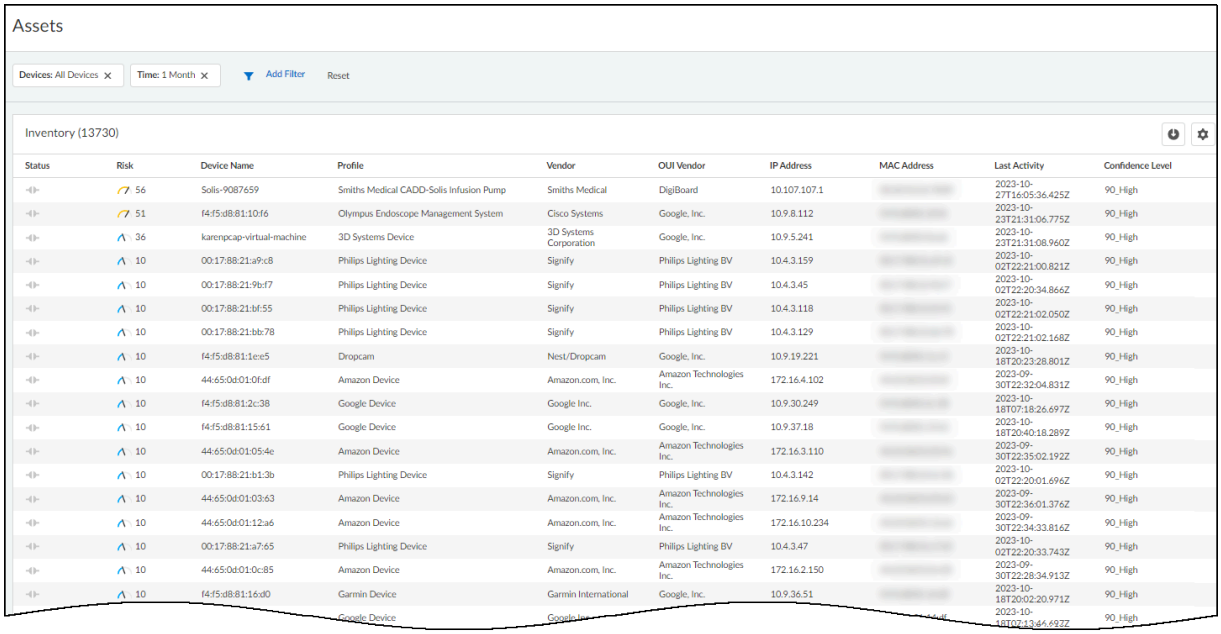
- 根據消耗的總頻寬，查看遠端網路、服務連線、GlobalProtect 行動使用者或明確 Proxy 行動使用者的前 5 個 Prisma Access 位置。
- 檢視 Prisma Access 位置的狀態。
- 檢視 Strata Logging Service 連線。
- 檢視 Prisma Access 位置表格（其中列出了所有 Prisma Access 位置），並按名稱選取個別 Prisma Access 位置以檢視其詳細資料。

 ©2025 Palo Alto Networks, Inc.

監控：資產

這可在何處使用？	我需要哪些內容？
• NGFW （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ IoT Security 訂閱 ❑ 軟體 NGFW 積分 （適用於 *VM-Series* 軟體 *NGFW*）

首先，選取 **Monitor**（監控）**> Assets**（資產）。在這裡，您可以看到網路上的 IoT、OT 和 IT 裝置動態維護的詳細目錄，且各自都有許多屬性，例如 IP 和 MAC 位址、設定檔、廠商、型號和作業系統，以及（進階 IoT Security 產品的）裝置層級風險分數。



使用此詳細目錄中的資料來瞭解網路上的資產：

- 針對在您的網路上偵測到的裝置（包括 IoT、OT 和 IT 裝置），檢視動態產生的最新詳細目錄。
- IoT 儀表板會概列出您擁有的裝置類型，而資產詳細目錄則可讓您探索各個裝置以查看更多詳細資料，並評估其安全性狀態。
- 按站台、裝置類型、時段和一或多個裝置屬性篩選儀表板中顯示的資料，以查看相關裝置的資料。
- 顯示和隱藏欄，以檢視對您具重要性的裝置屬性。有超過 100 個屬性欄可供選擇。
- 將目前作用中的頁面上顯示的資料下載為 CSV 格式的檔案，以包含在報告中或供日後參考。檔案中包含下載時顯示的裝置和裝置屬性。

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

事件和警示：Strata Cloud Manager

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目 • Prisma SD-WAN	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro 可見性所需的其他授權和先決條件包括： ❑ 有權檢視儀表板的角色 → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

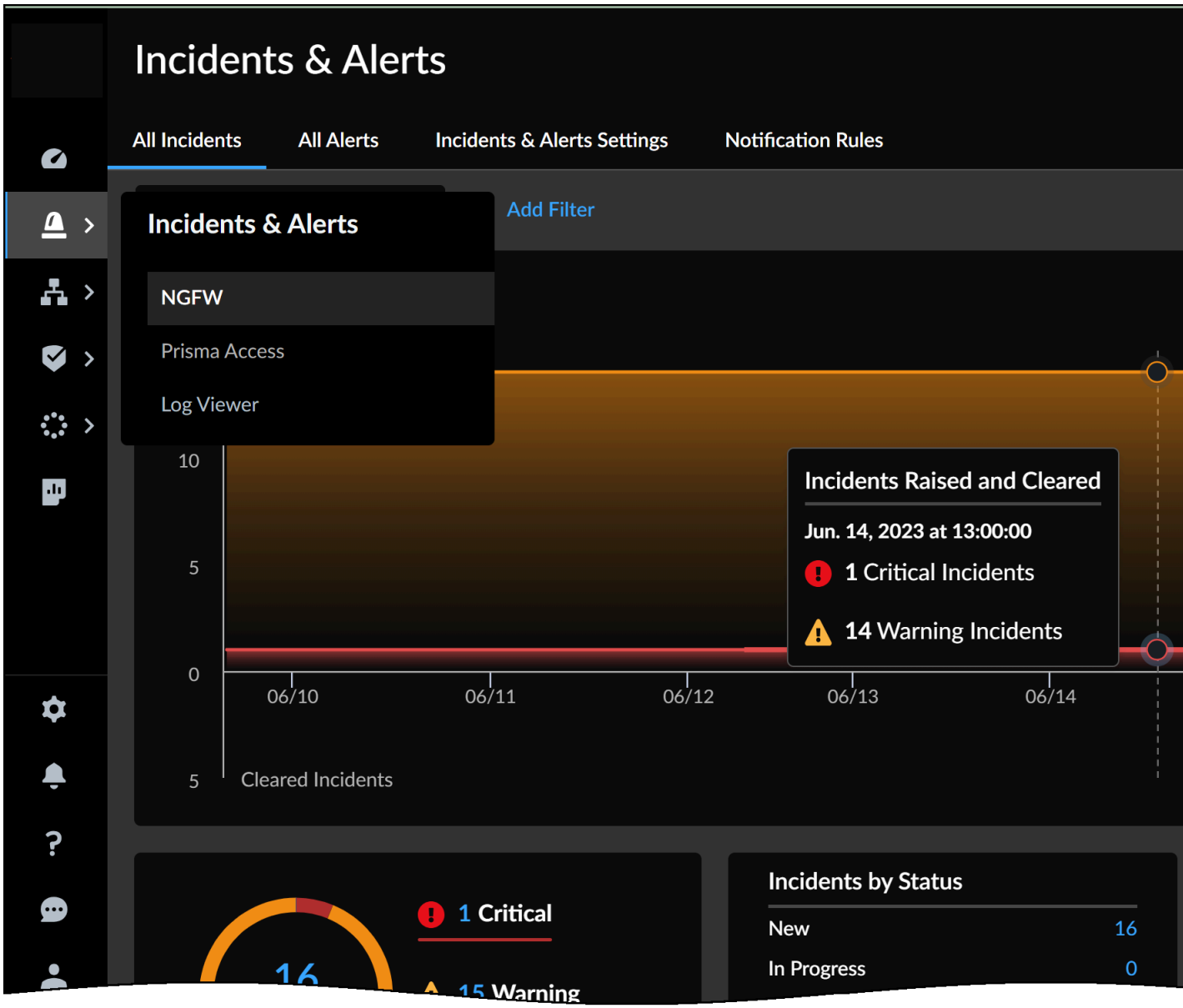
Strata Cloud Manager 為您提供一個通用架構，用來操作及調查 Palo Alto Networks 產品和訂閱在您的企業中偵測到的事件和警示：

- 事件和警示：NGFW
- 事件和警示：Prisma Access
- 事件和警示：Prisma SD-WAN

為了協助您的裝置和部署持續正常運作，並避免業務中斷，請瀏覽每個事件和警示頁面，以執行下列作業：

- 檢視網路上的事件和警示，並深入檢視以進行調查。
- 建立及檢閱觸發事件和警示通知的規則。

您可以在事件和警示與 事件和警示：日誌檢視器 之間移動，以調查網路上觸發事件和警示或與其相關聯的活動。



 ©2025 Palo Alto Networks, Inc.

事件和警示：NGFW

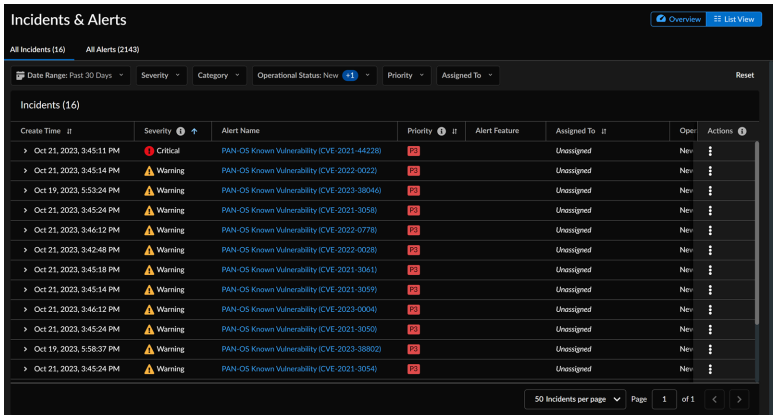
我可以在哪裡使用這個？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ 下列其中一個授權： ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) 或 AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

為了協助您讓裝置持續正常運作，並避免造成業務中斷的事件，您的應用程式會根據防火牆部署所偵測到的一或多個問題產生事件和警示。透過**Incidents & Alerts**（事件和警示） > **NGFW**，您可以在單一位置檢視 NGFW 間的事件和警示。

以下是如何啟動並執行 **NGFW** 事件與警示的方法：

- 事件可讓您獲得有關弱點的通知。您可以詳加調查，並且在必要時採取預防措施。

  導覽至**Incidents & Alerts**（事件與警示） > **NGFW** > **All Incidents**（所有事件），以檢視網路中的事件並與其互動。



 ©2025 Palo Alto Networks, Inc.

- 警示可指出需要解決的特定問題（防火牆功能下降或損失）。也可以根據多個事件之間的關聯或整合來產生警示。將事件整合為單一警示有助於分類、簡化團隊之間的警示傳遞、集中關鍵資訊並減少通知疲勞。

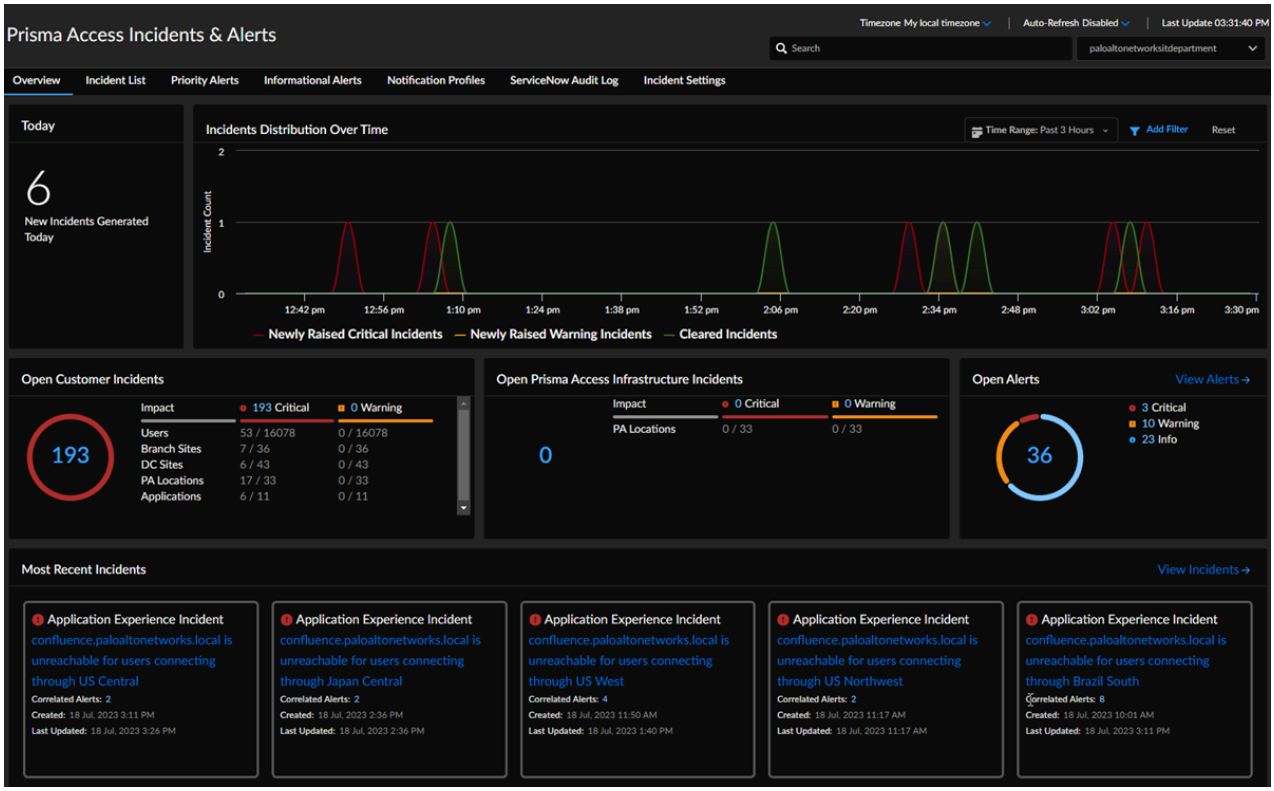
  導覽至**Incidents & Alerts**（事件與警示） > **NGFW** > **All Alerts**（所有警示），以檢視網路中的警示並與其互動。

 ©2025 Palo Alto Networks, Inc.

事件和警示：Prisma Access

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ AI-Powered ADEM 授權 ❑ ADEM Observability 授權 ❑ Prisma Access 授權

首先，選取**Incidents & Alerts**（事件與警示） > **Prisma Access Incidents & Alerts**（**Prisma Access** 事件與警示）。您的環境中可用的事件和警示取決於您的授權。



取得概要

請參閱與 Prisma Access 環境相關的事件和警示資訊的 Overview（概要）。您的環境中可用的事件和警示取決於您的授權。

查看所有事件

檢視事件清單，其中顯示您的環境中所有的事件。使用 **Add Filter**（新增篩選器）下拉式清單，按表格中的欄選取事件（可以有多個篩選依據）。從表格中選取任何 **Incident**（事件），以檢視其詳細資訊。

©2025 Palo Alto Networks, Inc.

檢視優先順序警示

請參閱優先順序警示，此處說明您的 Prisma Access 環境的狀態。

檢視資訊警示

檢視資訊警示，這會通知您即將進行的軟體升級以及進行中或已完成升級的狀態。

通知設定檔

在通知設定檔中，您可以檢視 **Notification Subscriptions**（通知訂閱）的相關資訊，並建立新的或修改現有的 **Notification Profile**（通知設定檔）。

ServiceNow 稽核日誌

如果您使用 ServiceNow，您可以檢閱 ServiceNow 稽核日誌，其中會顯示每個 ServiceNow 事件 **ID**。此外也會顯示對每個事件執行的 ServiceNow 操作，例如建立、更新和刪除。

事件設定

在事件設定中，您可以按事件類別和事件代碼自訂接收到的事件。

按代碼顯示的事件和警示

按代碼 ID 檢視事件和警示，瞭解其說明的問題，並找出加以修復的方法。事件和警示按授權分類：

- 採用 AI 技術的 ADEM 事件
- ADEM 事件
- Prisma Access 事件
- 優先順序警示
- 資訊警示

如需事件和警示的相關資訊，請參閱事件和警示參考指南。

如需 ServiceNow 整合的相關資訊，請參閱整合指南中的整合 ServiceNow 與 Prisma Access。

 ©2025 Palo Alto Networks, Inc.

事件和警示：Prisma SD-WAN

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma SD-WAN	❑ Prisma SD-WAN 授權

當系統達到系統定義或客戶定義的閾值，或系統故障時，Prisma SD-WAN 會產生事件和警示。使用這些事件和警示可對系統進行疑難排解。

選取**Incidents and Alerts**（事件和警示） > **Prisma SD-WAN**，以檢視 Strata Cloud Manager 中的事件和警示。

使用以下頁籤，導覽 Prisma SD-WAN 中的事件和警示。

- 概要
- 事件
- 警示
- 設定

概要

在 Prisma SD-WAN 中檢視事件和警示及其類別。**Overview**（概要）頁籤是您的預設檢視。

檢視最常顯示下列資訊的前幾個事件和警示。

事件類型	顯示事件的類別。
說明	顯示事件的說明。
severity	顯示事件的嚴重性。
優先順序	顯示事件的優先順序。
相關警示	顯示此事件中彙總的事件數目。
STATUS (狀態)	顯示事件的狀態。
已建立	顯示系統引發事件的時間。
上次更新	顯示系統上次更新事件的時間。

事件

出現事件時，表示系統發生錯誤。事件的引發、清除和變化，會以嚴重性為準：

- 重大 — 整個或部分網路已關閉，需要立即採取措施。
- 警告 — 對網路造成影響，需要立即關注。

 ©2025 Palo Alto Networks, Inc.

- 資訊 — 網路效能下降，需要盡快關注。

警示

出現警示時，不一定表示網路發生錯誤。當系統達到系統定義或客戶定義的閾值時，就會引發警示。

設定

使用 **Settings**（設定）頁籤建立事件政策，以根據設定的指定分類和動作屬性來管理事件代碼抑制。您可以使用事件政策規則來抑制或升級在排程時段內引發的事件。此外，您也可以對系統產生的事件進行預設優先順序的變更，使其優先順序層級更符合您的業務需求。

 ©2025 Palo Alto Networks, Inc.

事件和警示：日誌檢視器

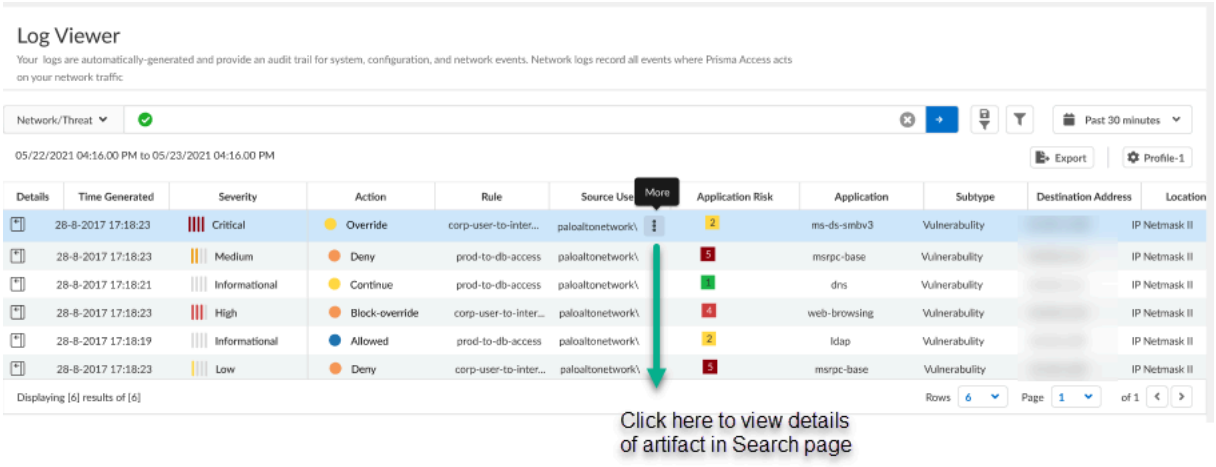
我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW，包括由軟體 NGFW 積分資助的項目	❑ 以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)或AIOps for NGFW Free (use the AIOps for NGFW Free app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ 有權檢視儀表板的角色

Log Viewer（日誌檢視器）提供探索功能 - 您可以在此處檢視儲存在 Strata Logging Service 中的日誌，並與其互動。

Log Viewer（日誌檢視器）提供系統、設定和網路事件的稽核追蹤。從儀表板跳到日誌，以獲取詳細資料並調查結果。查詢欄位和時間範圍偏好設定有助於縮小您感興趣的特定日誌。

- 進一步瞭解如何建置查詢
- 在 Strata Logging Service版本資訊中探索新的日誌檢視器功能。

Log Viewer（日誌檢視器）會醒目提示日誌的動作和嚴重性，以協助您瞭解工作階段的強制執行情形。您也可以在搜尋頁面中檢視日誌的安全構件詳細資料。



* 您可以在 [Search（搜尋）] 中檢視下列日誌類型和日誌欄位的詳細資料：

©2025 Palo Alto Networks, Inc.

日誌類型	欄名稱
流量、威脅、URL、檔案	• 來源位址 • 目的地位址 • NAT 來源 • NAT 目的地
威脅、檔案	檔案雜湊
URL	• URL • URL 網域
DNS 安全性	• 來源位址 • 目的地位址 • 網域 • FQDN

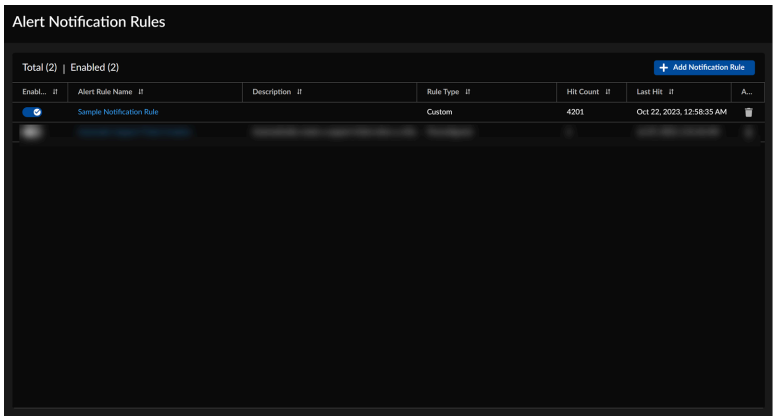
 ©2025 Palo Alto Networks, Inc.

事件和警示設定

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ AIOps for NGFW Free (use the AIOps for NGFW Free app)或AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

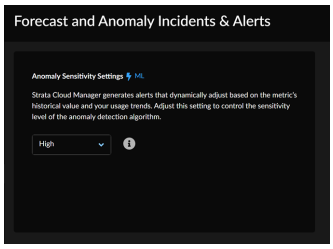
- 若要定義通知偏好設定，例如哪些警示觸發通知、接收通知的方式以及接收通知的頻率，請建立通知規則。

  導覽至**Incidents & Alerts**（事件與警示） > **Incident & Alert Settings**（事件與警示設定） > **Notification Rules**（通知規則），以檢視和新增觸發通知的規則。



- Strata Cloud Manager 會產生根據指標的歷史值和您的使用趨勢動態調整的警示和事件。您可以調整此設定來控制異常偵測演算法的敏感度層級。

  導覽至**Incidents & Alerts**（事件與警示） > **Incident & Alert Settings**（事件與警示設定） > **Anomaly Sensitivity**（異常敏感度），以設定異常偵測演算法的敏感度層級。



 ©2025 Palo Alto Networks, Inc.

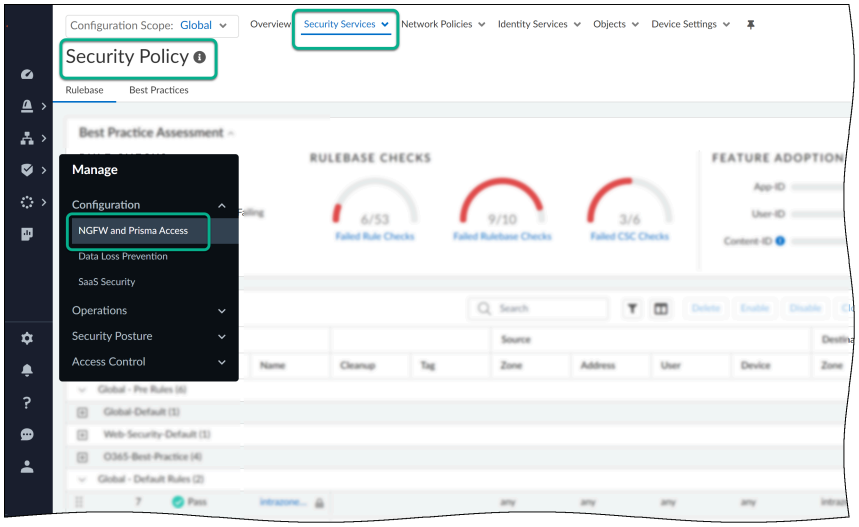
 ©2025 Palo Alto Networks, Inc.

管理：NGFW 和 Prisma Access

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

Strata Cloud Manager 可讓您設定在 NGFW 與 Prisma Access 間共用的安全性政策。首先，請您：

- ❑ 使用 Strata Cloud Manager 設定 Prisma Access 和（或）NGFW
- ❑ 設定資料夾，以對需要類似設定的 NGFW 進行分組。Prisma Access 資料夾是預先定義的，可讓您根據部署類型找出設定目標：行動使用者、遠端網路、服務連線。
- ❑ 設定你的工作所需的 管理：設定範圍。您可以設定將在 NGFW 和 Prisma Access 環境中全域套用的設定，也可以根據資料夾將設定目標定為特定的 NGFW 或 Prisma Access 部署。
- ❑ 使用 管理：片段，為一組 NGFW 或部署標準化通用基礎設定。片段可讓您以已知的良好設定快速上線新裝置、使用者或位置，並縮短新裝置上線所需的時間。
- ❑ 移至**Manage**（管理）> **Configuration**（設定）> **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**）開始建立安全性政策，並使用上述管理功能在 NGFW 和 Prisma Access 之間共用政策。



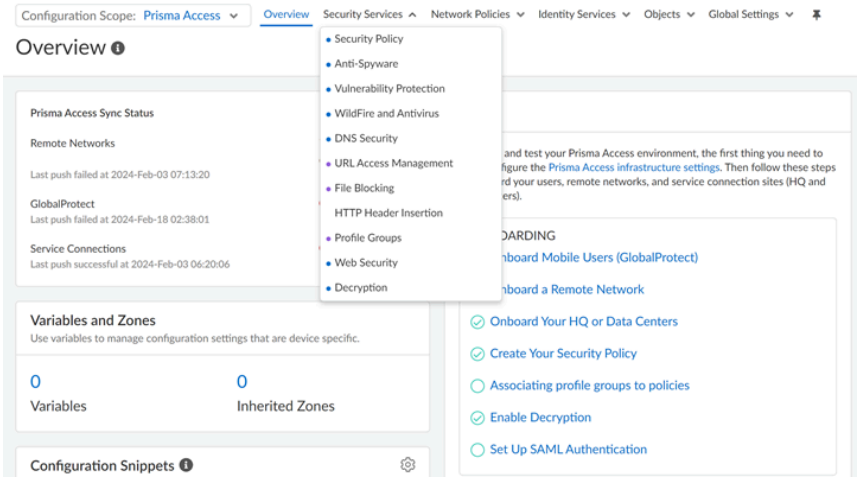
管理：設定範圍

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

透過 Strata Cloud Manager，您可以在整個環境中全域套用組態設定並強制執行政策，或將設定和政策的目標定為組織的某些部分。當你使用 Strata Cloud Manager 設定管理時，目前的 **Configuration Scope**（設定範圍）一律會顯示，且您可以切換檢視以管理更廣泛或更精細的設定。

您可以清楚瞭解適用於特定設定範圍的設定元素，及其是從通用設定範圍繼承的，還是由系統產生的。以顏色區分的設定指標可協助您瞭解設定繼承自何處，並且可目視區分物件類型以便進行掃描。

- 灰色點表示繼承的設定
- 紫色點表示預先定義的設定
- 藍色點表示物件存在於目前的設定範圍內



全域組態設定可協助您輕鬆管理及強制執行您的所有網路流量適用的政策需求。或者，您可以將政策和組態設定的目標定為適合這些設定的部署類型。

 ©2025 Palo Alto Networks, Inc.

- **Prisma Access**
  - 行動使用者容器 – 設定會套用至所有行動使用者連線類型：GlobalProtect 和明確 Proxy，或個別套用至每個連線類型。
  - 遠端網路 – 設定會套用至遠端網站（分公司、零售地點等等）。
  - 服務連線 – 設定會套用至服務連線站台（總部和資料中心）。
- 所有防火牆 – 設定會套用至所有 NGFW，或套用至將需要共用或特定組態設定或政策強制執行的 NGFW 分組在一起的特定資料夾。

進一步瞭解：

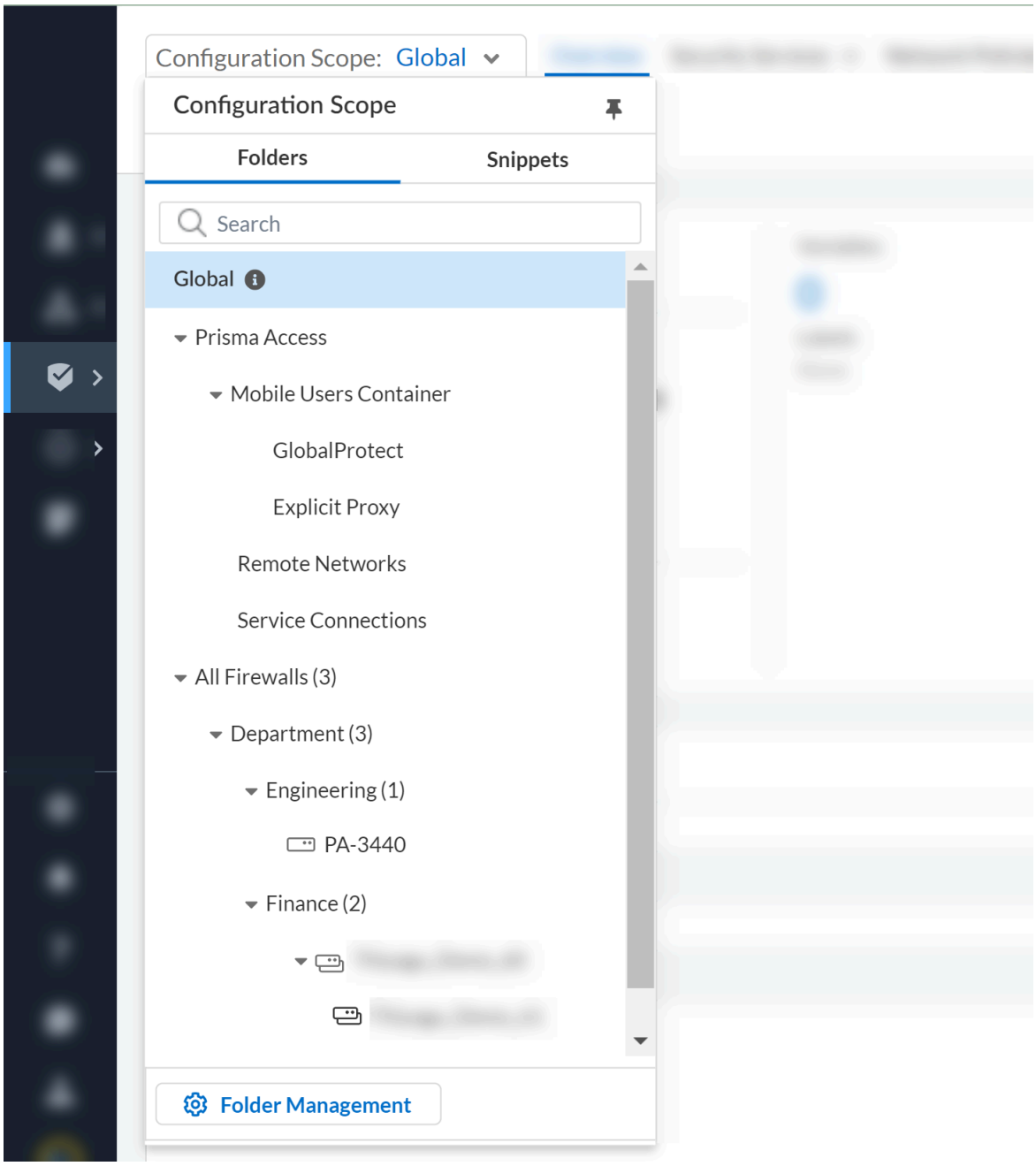
- 工作流程：資料夾管理

  使用資料夾對裝置和部署類型進行邏輯分組，以簡化設定管理。
- 管理：片段

  使用片段對設定進行分組，讓您能夠將其快速推送至防火牆或部署。
- 管理：變數

  在設定中使用變數，以因應裝置或部署的特定設定物件。

 ©2025 Palo Alto Networks, Inc.



管理：片段

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials

 ©2025 Palo Alto Networks, Inc.

這可在何處使用？	我需要哪些內容？
	❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

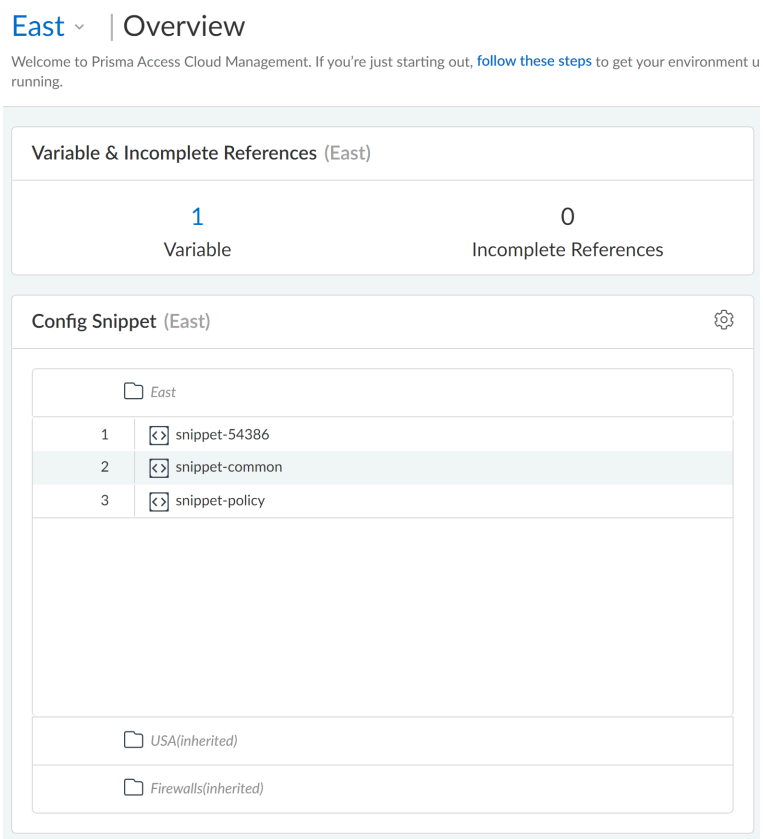
使用片段對設定進行分組，讓您能夠將其快速推送至防火牆或部署。

片段是一個設定物件，無法貼合於可以與資料夾、部署或裝置相關聯的階層（或設定物件的群組）中。片段可用來標準化一組防火牆或部署的通用基礎設定，使您能夠使用已知良好的設定快速上線新裝置，並縮短上線新裝置所需的時間。例如，您可以在遠端分公司上線新的防火牆。您可以將一組包含所有必要網路和政策規則設定的片段，與新防火牆所屬的資料夾產生關聯。這樣可以縮短設定防火牆以保護遠端分公司所需的時間。

若物件值發生衝突，片段關聯會採由上至下的優先順序。不允許使用重複名稱的規則，且若在任何資料夾中建立具有相同名稱的片段，或者在產生片段與資料夾的關聯時，已有同名的片段相關聯，驗證將會失敗。

這表示，如果同一物件的第一個和最後一個相關聯的片段具有不同的值，則裝置或部署會繼承第一個片段的值。此外，從片段繼承的所有設定，都可以在子資料夾、部署或裝置層級覆寫。

在資料夾階層內，片段在任何資料夾階層內只能關聯一次。這表示片段不能同時與資料夾及其下內嵌的資料夾相關聯。不過，您可以將相同片段與不同的資料夾或內嵌在不同資料夾下的資料夾產生關聯。已與資料夾階層中的某個資料夾相關聯的片段會顯示為灰色，因此在適用情況下不可多次使用。



 ©2025 Palo Alto Networks, Inc.

片段中的跨範圍設定參考性

此功能可讓您參考連結至全域範圍的任何通用設定或物件，並將其推送至 Prisma Access 和 NGFW 防火牆。這些位於全域範圍內的共用物件和設定，可供所有片段使用。與全域範圍相關聯的片段，會被視為全域片段。定義於這些片段內並連結至全域範圍的物件，可供設定中的任何片段參考。

例如，您可以建立名為「全域變數」的片段以合併變數，並將其連結至全域範圍。如此，設定中的所有其他片段在參考和使用上都會很容易。同樣地，您可以對存取政策規則、威脅防護設定檔、區域、位址，以及其他代表標準網路區段的物件有效管理其自訂 URL 類別。

建立片段

建立片段並將其與資料夾、部署或裝置產生關聯，以將通用基礎設定套用至裝置群組。您可以視需要將任意數量的片段與資料夾、部署或裝置產生關聯。

片段建立後可以隨時修改，以及與任何資料夾、部署或裝置重新產生關聯。

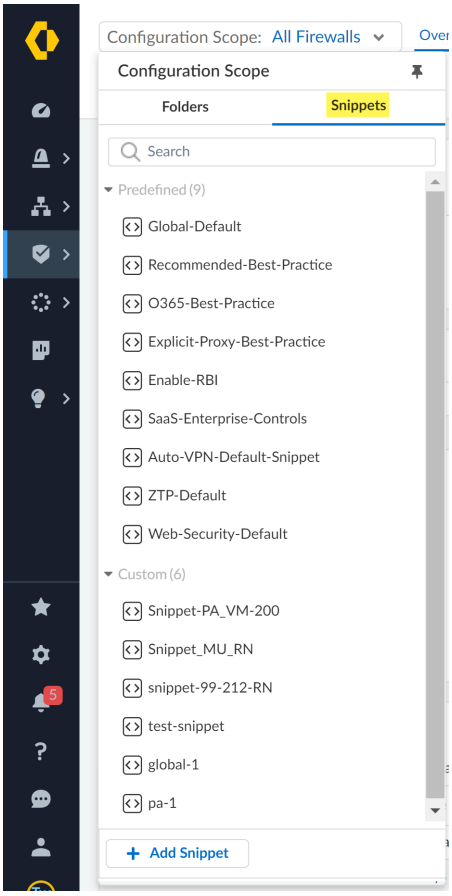
不再使用的自訂片段可以刪除。

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概要），並展開 [Configuration Scope（設定範圍）] 以檢視 **Snippets**（片段）。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | 新增片段。



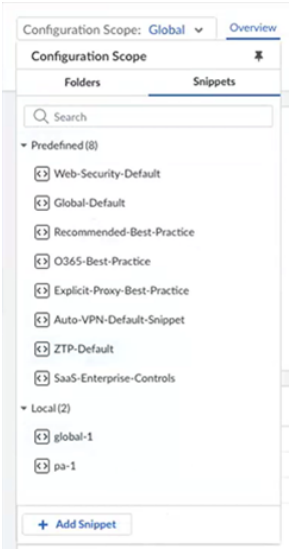
 ©2025 Palo Alto Networks, Inc.

STEP 4 | 建立片段。

1. 為片段指定一個描述性名稱。
2. （選用）輸入片段的說明。
3. （選用）指派一或多個標籤。

   您可以選取現有標籤，或鍵入您要建立的標籤來建立新標籤。
4. **Create**（建立）。

   新建立的片段會在 **Local**（本機）片段下分類列出。片段發佈後，會移至「已發佈的」片段下。



STEP 5 | 建立您的片段設定。

您現在位於片段的設定範圍內。您在片段範圍內建立的所有設定，都僅適用於片段。

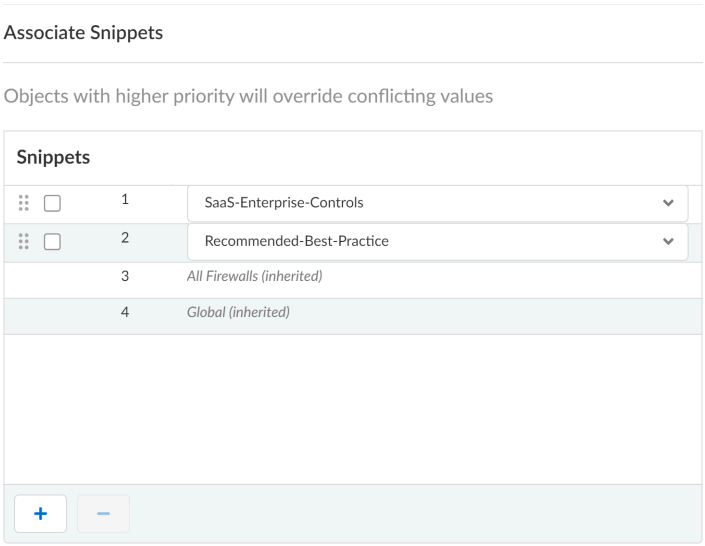
在片段範圍內，您可以檢閱片段 **Overview**（概要），以查看關於片段的詳細資料。其中包括變數數量的資訊、關於片段的建立和上次更新時間的資訊，以及與片段相關聯的所有資料夾、部署和裝置的清單。

 ©2025 Palo Alto Networks, Inc.

STEP 6 | 為片段產生關聯。

1. 選取**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**）**s** > **Overview**（概要），並展開 [Configuration Scope（設定範圍）] 以檢視 **Config Tree**（設定樹狀結構）。
2. 選取要與片段產生關聯的資料夾、部署或裝置。
3. 編輯 **Config Snippet**（設定片段）。
4. 新增您想要關聯的片段，並視需要為其排序。

   如果您將片段關聯至全域範圍，它將可被設定中的所有其他片段參考和使用。所有片段都能夠參考在片段中連結至全域資料夾的物件。
5. 關閉。



STEP 7 | 推送設定，將您的設定變更推送至您的網路。

修改片段

修改您的片段設定、詳細資料和關聯。

不再與資料夾、部署或裝置相關聯的自訂片段可以刪除。

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概要），並展開 [Configuration Scope（設定範圍）] 以檢視 **Snippets**（片段）。

STEP 3 | 選取您要修改的片段。

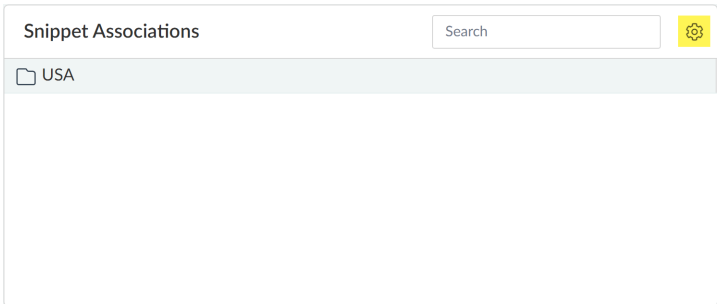
選取片段後，您會被重新導向至片段 **Overview**（概要）。

STEP 4 | （選用）編輯片段以修改名稱、說明，或變更或指派其他標籤。啟用或停用 **Pause Update**（暫停更新），以查看設定差異並決定接受變更。

 ©2025 Palo Alto Networks, Inc.

STEP 5 | 編輯 **Snippet Associations**（片段關聯），將片段與不同的資料夾、部署或裝置重新產生關聯，或將片段與額外的資料夾、部署或裝置產生關聯。

退出片段重新關聯畫面，以套用變更。



STEP 6 | 視需要對片段設定進行任何變更。

STEP 7 | **Push Config**（推送設定）。

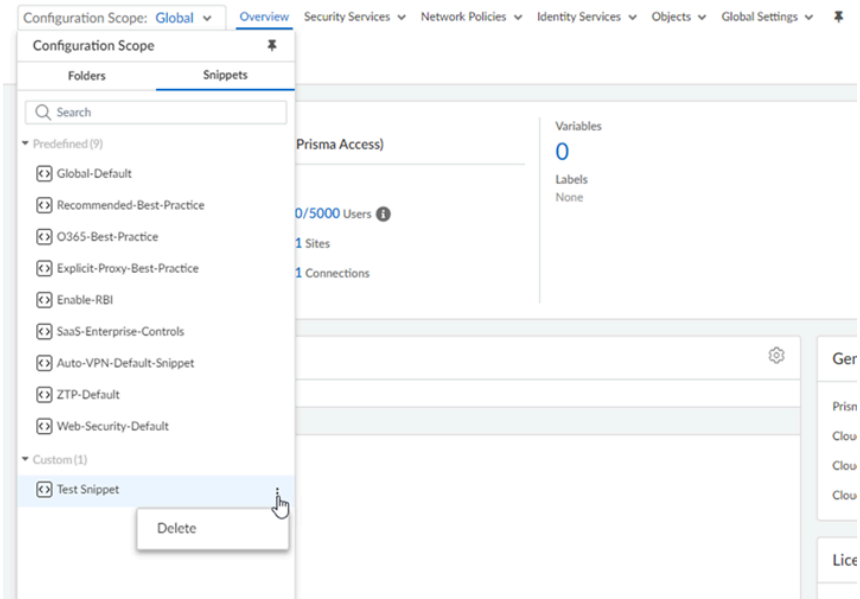
刪除片段

刪除自訂片段以維持設定的簡潔。片段必須先與任何防火牆、資料夾或部署解除關聯，才能刪除。不支援刪除預先定義的片段。

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概要），並展開 **Configuration Scope**（設定範圍） 以檢視 [Snippets（片段）]。

STEP 3 | 按一下要刪除的自訂片段的三個垂直點。



 ©2025 Palo Alto Networks, Inc.

STEP 4 | 刪除片段。

> 目前與資料夾、部署或裝置相關聯的片段無法刪除。請先編輯 ***Snippet Associations***（片段關聯）以移除所有現有的關聯，片段才能移除。

複製片段

如果您想使用現有片段作為新片段的範本，您可以輕鬆複製，這樣即無須設定新物件。

複製的片段不會與任何裝置、資料夾或部署相關聯，因此您可以隨意自訂，而無須在開始設定之前解除關聯。

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概要），並展開 **Configuration Scope**（設定範圍） 以檢視 [Snippets（片段）]。

STEP 3 | 按一下要複製的自訂片段的三個垂直點。

STEP 4 | 複製片段。

1. （選用）為複製的片段指定新名稱。

共用片段設定

此功能提供了獨特且靈活的方法，可在任何租用戶間共用通用設定，包括在多租用戶環境中。您可以將各種設定儲存為片段並加以管理，並且在客戶帳戶下的租用戶間輕鬆共用。此功能讓您能夠相當靈活地在不同的租用戶環境間管理共用設定，並掌握全局。

此外，此功能支援對租用戶之間的常見案例進行集中設定管理，以及監督多業務單位設定中的全域設定。

在此架構中，發佈者租用戶與訂閱者租用戶共用片段，而訂閱者租用戶會接收來自發佈者租用戶的片段。

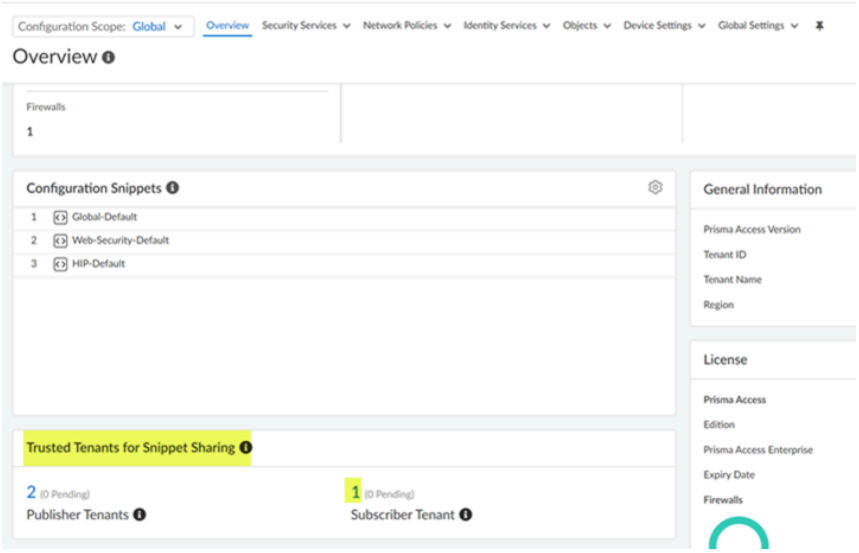
STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 在發佈者租用戶上，選取**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概要），然後選取 **Global**（全域）設定範圍。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | 建立租用戶之間的信任：建立訂閱者和發佈者租用戶之間的連線，以實現片段共用。

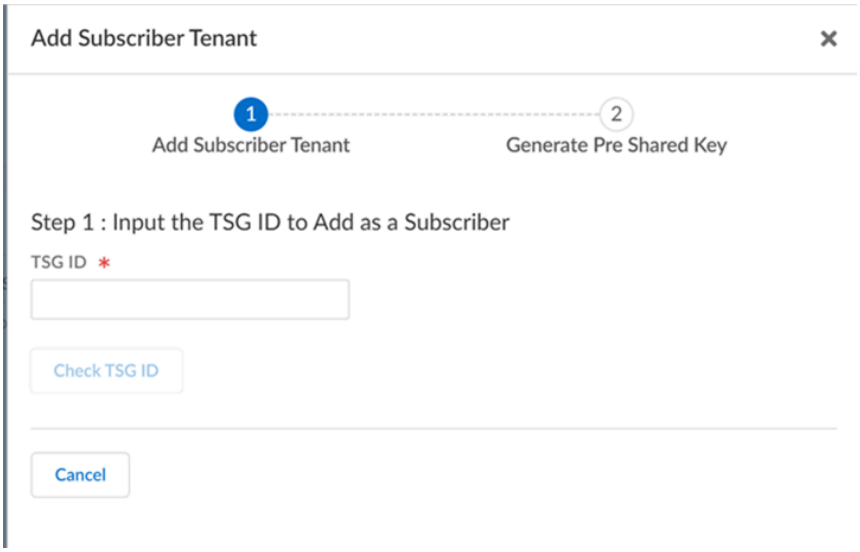
1. 按一下 **Trusted Tenants for Snippet Sharing**（片段共用的受信任租用戶）底下的 **Subscriber Tenant**（訂閱者租用戶）。



2. 新增訂閱者租用戶。

3. 輸入要新增為訂戶租用戶的 **TSG ID**，然後輸入 **Check TSG ID**（檢查 **TSG ID**）。這樣可以有效防止隨機產生的 TSG 或序列化的 TSG 型攻擊。

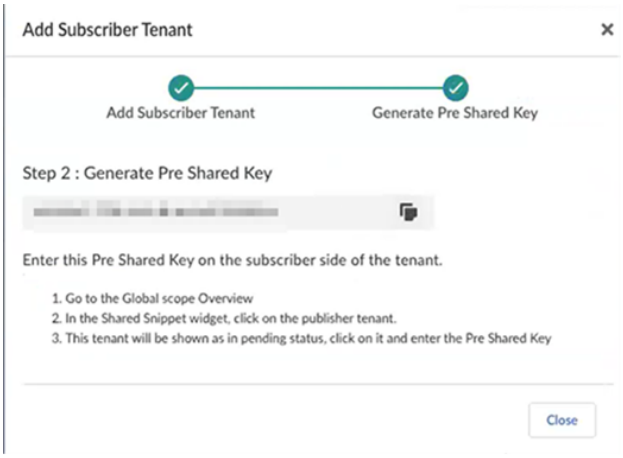
   驗證成功後會出現確認訊息，指出 TSD ID 已通過驗證。



4. 下一步：產生預先共用金鑰。

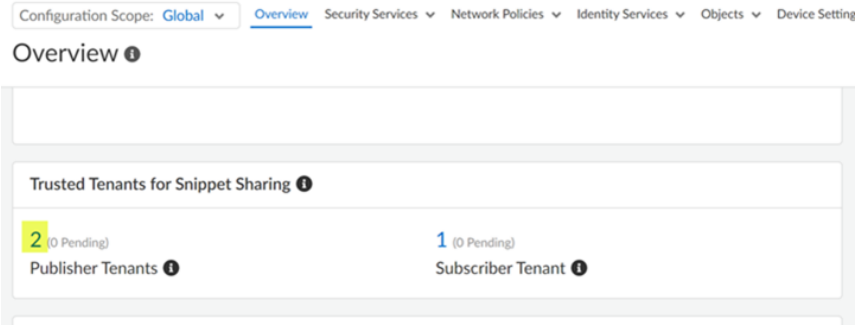
   複製產生的 PSK。您在步驟 4 中驗證發佈者租用戶時將輸入此 PSK。

 ©2025 Palo Alto Networks, Inc.



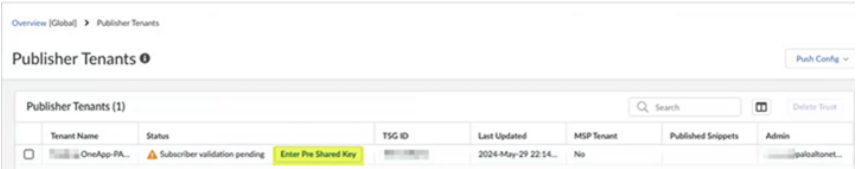
STEP 4 | 移至訂閱者租用戶，選取**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概要），然後將設定範圍設為 **Global**（全域）。

1. **Trusted Tenants for Snippet Sharing**（片段共用的受信任租用戶）下的 **Publisher Tenants**（發佈者租用戶）狀態會顯示為 **Pending**（擱置中）。



2. 按一下 **Publisher Tenants**（發佈者租用戶），並輸入在先前的步驟中產生的預先共用金鑰，然後驗證訂閱者租用戶。

   驗證成功後會出現一則訊息，確認租用戶是可信任的，從而在訂閱者和發佈者租用戶之間建立信任。



 ©2025 Palo Alto Networks, Inc.

STEP 5 | 將片段發佈至訂閱者租用戶。

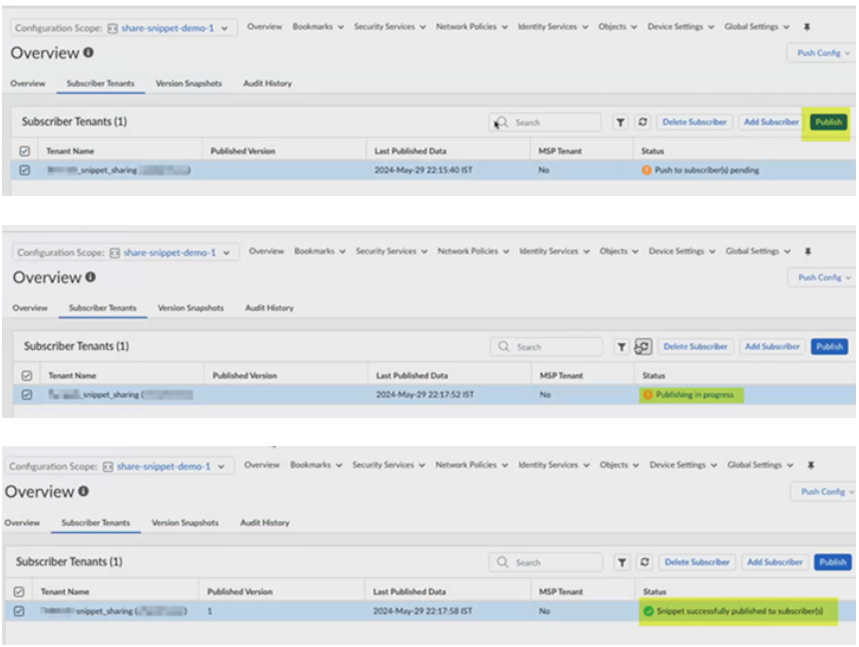
1. 建立片段並將其與資料夾產生關聯。

   新建立的片段可在 **Local**（本機）片段下找到。

   - **Overview**（概要）頁籤會顯示片段詳細資料，例如名稱、說明、建立時間（片段在訂閱者端載入的時間）、上次更新時間，和標籤詳細資料。
   - **Subscriber Tenants**（訂閱者租用戶）頁籤會顯示租用戶名稱、租用戶上的發佈版本、上次發佈日期和發佈狀態。
     - 按一下 **Published Version**（已發佈的版本），以檢閱設定變更。
     - 將片段發佈至租用戶之前，請新增訂閱者並加以儲存。
   - **Version Snapshots**（版本快照）會提供了片段設定的歷程記錄。在此畫面中，您可以比較設定快照與候選設定，然後儲存版本快照或載入先前的設定快照作為候選設定。按一下版本號碼，以檢視設定差異。
   - **Audit History**（稽核歷程記錄）會提供管理員起始之所有動作的稽核追蹤。其中會記錄詳細資料，例如已發佈的版本號碼、所做的變更、變更的擁有者、變更的日期和時間，以及變更的細節。

2. 在 **Subscriber Tenant**（訂閱者租用戶）頁籤上，選取租用戶名稱，然後選取 **Publish**（發佈）。

   這會將發佈要求傳送至訂閱者租用戶。**Status**（狀態）欄指出片段已成功發佈給訂閱者，且該片段會提供在「已發佈的片段」下。



STEP 6 | 驗證訂閱者租用戶。

1. 移至**Overview**（概要） > **Configuration Scope**（設定範圍） > **Snippets**（片段），然後選取 **Subscribed**（已訂閱）片段下的片段。

   您會被重新導向至片段 **Overview**（概要），其中會顯示多項詳細資料，例如發佈者租用戶的名稱、說明、TSG ID、片段建立時間、上次更新時間、標籤和暫停更新詳細資料等等。

 ©2025 Palo Alto Networks, Inc.

STEP 7 | 刪除信任。

與資料夾或防火牆相關聯的已訂閱片段只能複製，而無法刪除。

1. 移至訂閱者或發佈者租用戶。
2. 按一下 **Trusted Tenants for Snippet Sharing**（片段共用的受信任租用戶）底下的 **Subscriber Tenant**（訂閱者租用戶）。
3. 選取 **Tenant Name**（租用戶名稱），然後選取 **Delete Trust**（刪除信任）。

刪除信任後，片段將不再與防火牆或資料夾相關聯，而會成為本機片段。

片段分類

- 預先定義：所有 Strata Cloud Manager 使用者都可以存取這些片段，以使用最佳做法設定快速設定新的防火牆和部署。
- 本機：這些可編輯片段是在租用戶內建立的，無法與其他訂閱者租用戶共用。
- 已發佈：受信任的訂閱者租用戶可以存取這些共用片段，但無法複製或編輯。
- 已訂閱：這些片段由發佈者租用戶共用，可由使用者複製，但無法編輯。

 ©2025 Palo Alto Networks, Inc.

管理：變數

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

在設定中使用變數，以因應裝置或部署的特定設定物件。

變數是一項進階工具，可讓您將設定標準化，同時能靈活因應裝置或部署特定的唯一設定值。變數可讓您減少需要管理的片段數量，同時可讓您視需要保留任何防火牆或部署特定的設定值。

例如，您有一個設定的片段要與多個巢狀資料夾相關聯，而其中的每個巢狀資料夾都包含一組專屬於某個地理位置的防火牆。在片段中，您已設定政策規則，限制只有特定 IP 範圍可存取業務關鍵系統。在此案例中，您可以為每個巢狀資料夾特定的每個 IP 範圍建立一個變數，並在繼承的片段設定中使用該變數。這可讓您管理和推送設定變更，同時使用較少的片段來容納裝置或部署特定的設定值。

變數可在資料夾、部署或防火牆層級建立。當您為資料夾建立變數時，內嵌在該資料夾下的所有資料夾都會繼承該變數。如果資料夾設定範圍中出現衝突的變數，防火牆或部署將會從包含巢狀資料夾的資料夾繼承變數值。不過，您可以在巢狀資料夾、部署或防火牆層級覆寫繼承的變數。

支援的變數類型如下：

變數類型	說明
AS 編號	要在 BGP 設定中使用的自發系統編號。
計數	要觸發動作所需發生的事件數目。
裝置 **ID**	用來在主動-主動高可用性 (HA) 設定中指派裝置優先順序評估器的裝置 ID。
裝置優先順序	裝置優先順序可指出防火牆在主動/被動高可用性 (HA) 設定中應扮演主動角色的偏好設定。
輸出最大	要在服務品質 (QoS) 設定檔設定中使用的輸出最大值。
FQDN	完整網域名稱。
群組 **ID**	高可用性群組 ID。

 ©2025 Palo Alto Networks, Inc.

變數類型	說明
IP 網路遮罩	靜態 IP 或網路位址。
IP 範圍	IP 範圍。例如 **192.168.1.10-192.168.1.20**。
IP 萬用字元	IP 萬用字元遮罩可允許或拒絕類似的 IP 位址。例如 10.0.0.5/255.255.0.255。
連結標籤	要在 SD-WAN 設定中使用的連結標籤。
百分比	百分比介於 **0** 到 **99** 之間。
連接埠	來源或目的地連接埠。
QoS 設定檔	用於 QoS 設定中的 QoS 設定檔。
比率	比率可指定觸發動作的閾值。例如，DoS 保護設定檔的警報率。
路由器 **ID**	您為邏輯路由器設定邊界閘道通訊協定 (BGP) 時的路由器 ID。
計時器	以秒為單位的計時器，用以設定觸發動作的閾值。
區	安全性區域。

建立變數

您也可以在支援變數之處建立內嵌變數。

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概要），然後您要在其中建立變數的設定範圍。

在 **Folders**（資料夾）中，選取您要為其建立變數的資料夾或裝置。

在 **Snippets**（片段）中，選取您要為其建立變數的特定片段。

STEP 3 | 在 [Variables（變數）] 區段中，按一下顯示的變數計數。

STEP 4 | 新增變數。

 ©2025 Palo Alto Networks, Inc.

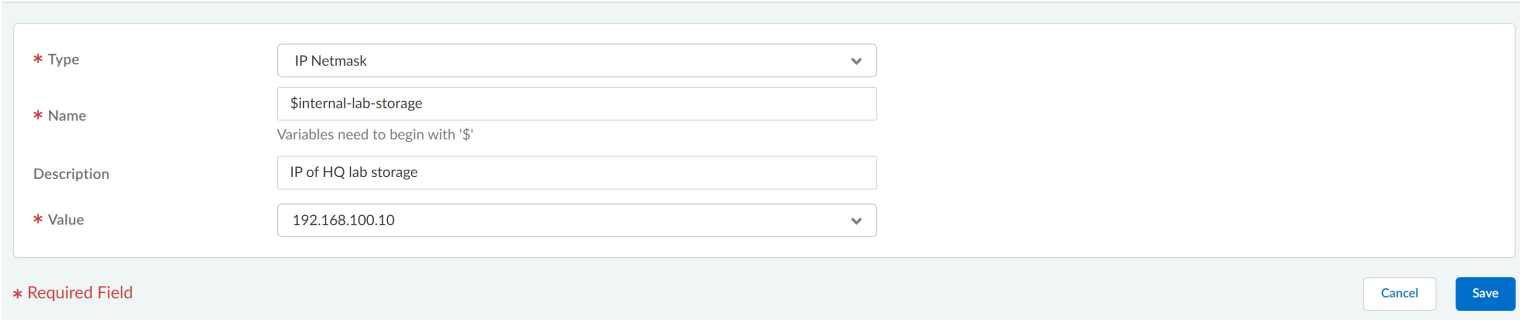
STEP 5 | 建立變數。

在此範例中，建立 **IP** 網路遮罩變數，作為重要內部資源的位址物件。

1. 選取變數類型。
2. 為變數指定描述性名稱。

   所有變數名稱都必須以 **$** 開頭。
3. （選用）輸入變數的說明。
4. 輸入變數值。
5. **Save**（儲存）。

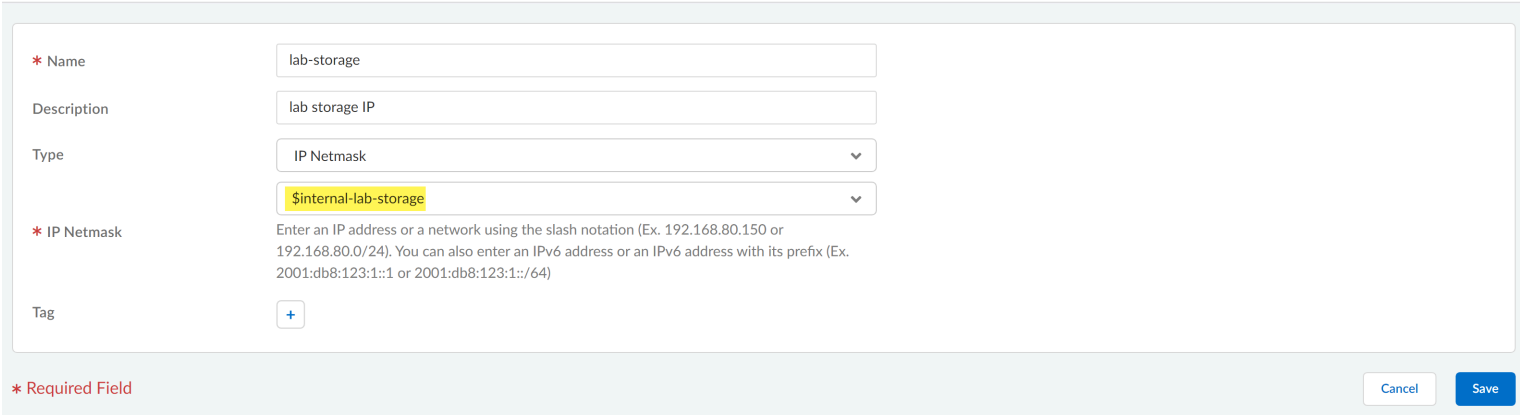
Variables



STEP 6 | 將變數新增至您的設定。

在此範例中，在先前的步驟中建立的 **$internal-lab-storage** 變數會新增至位址物件設定。

Addresses



STEP 7 | 推送設定。

匯入變數

我可以在哪裡使用這個？	我需要哪些內容？
• Strata Cloud Manager	❑ AIOps for NGFW Premium 授權

 ©2025 Palo Alto Networks, Inc.

我可以在哪裡使用這個？	我需要哪些內容？
	❑ Prisma Access 授權

使用 CSV 檔案將變數匯入至 Strata Cloud Manager。變數匯入的用意，是要將防火牆從資料夾階層中繼承的多個變數，或已在防火牆設定範圍中設定的多個變數，覆寫為新防火牆的特定值。

變數必須已從資料夾階層中繼承，或已在防火牆設定範圍中設定，才能使用變數匯入來覆寫。不支援藉由匯入變數來建立全新的變數。

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概要）。

STEP 3 | 在 [Variables（變數）] 區段中，按一下顯示的變數計數。

STEP 4 | 選取 **CSV Export/Import**（**CSV** 匯出/匯入） > **Export**（匯出），以匯出您要覆寫的變數。

Palo Alto Networks 建議您先匯出要覆寫的變數。這樣可以確保您上傳至 Strata Cloud Manager 的 CSV 檔案會正確格式化。此外也可確保目標資料夾和防火牆變數會正確歸因，以加速匯入程序。

 ©2025 Palo Alto Networks, Inc.

STEP 5 | 修改已匯出 CSV 檔案中的變數。

修改 CSV 檔案以進行匯入時，請考量下列事項。

- 僅支援使用簡單的文字編輯器 (例如記事本) 來修改匯出的 CSV 檔案。
- **#** 表示變數建立於資料夾階層中，並且由防火牆繼承。

  移除 **#** 可將繼承的變數值覆寫為防火牆特定值。

  匯入時 Strata Cloud Manager 會忽略附加 **#** 的變數值，因為僅支援在防火牆設定範圍上覆寫變數值。
- `-NA-` 表示變數不存在於防火牆設定中。這表示變數建立在防火牆所屬的資料夾階層外。

  不支援將變數值變更為 `-NA-`。Strata Cloud Manager 會忽略任何修改為 `-NA-` 的變數值。

  不支援將防火牆特定值指定給值為 `-NA-` 的變數，因為該變數不存在於防火牆設定範圍中。防火牆必須從資料夾階層中繼承變數，或設定在防火牆設定範圍中，才能使用變數匯入加以覆寫。
- 變數值若為無**#** 或無，表示變數建立時的值設為無。

  您可以將任何變數值修改為無，以移除該值，但不刪除變數。
- 對於在防火牆設定範圍中建立的變數，刪除變數值並保留為空白，將會刪除變數。

  若是在資料夾階層中建立、並且由防火牆繼承的變數，刪除變數值並保留為空白，會將變數值還原為從資料夾階層繼承的值。

1. 找出您匯出的 CSV 檔案，並加以開啟。匯出的 CSV 檔案名稱格式為：

   ```
   <cloud-management-tenant-name> - Prisma Access_<export-date>_variables
   ```
2. 視需要修改變數。

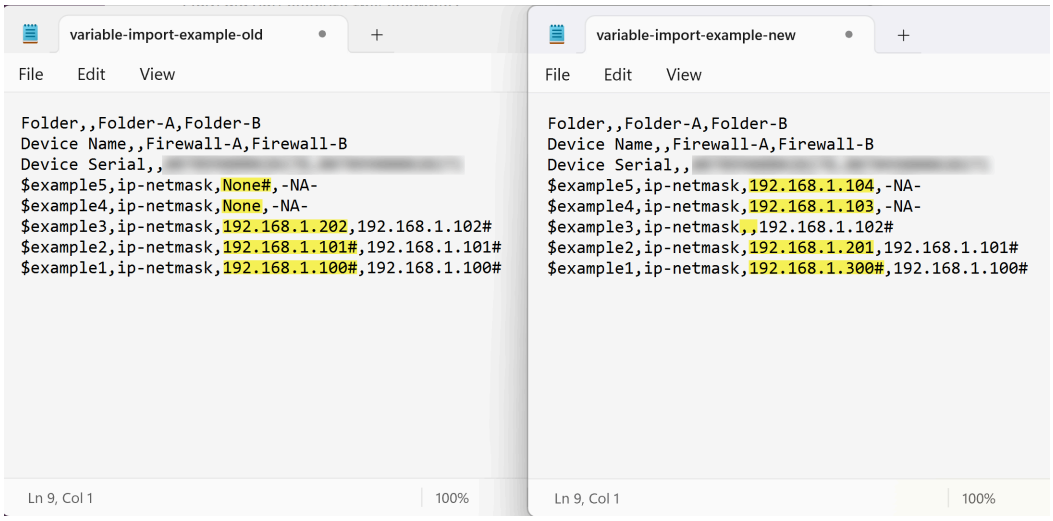
   Palo Alto Networks 不建議修改資料夾名稱、裝置名稱或裝置序號。這可能會導致匯入失敗。

   在下方的範例中，已對 `Firewall-A` 設定範圍中的變數值進行下列變更，以說明如何使用變數匯入一次修改多個變數。

   - `$example1`—將繼承的無**#** 值覆寫為防火牆特定值。
   - `$example2`—將防火牆特定的無值覆寫為防火牆特定值。
   - `$example3`—如果變數是在防火牆設定範圍中建立的，則空值會刪除該變數。

     如果變數是從資料夾階層繼承的，並且已在防火牆設定範圍中被覆寫，則空值會還原從資料夾階層繼承的變數值。
   - `$example4`—將繼承的 `192.168.1.101` 值覆寫為防火牆特定值。
   - `$example5`— Strata Cloud Manager 因 **#** 仍附加而忽略變數變更的範例。

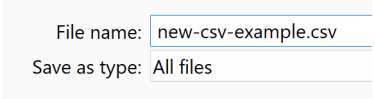
 ©2025 Palo Alto Networks, Inc.



STEP 6 | 儲存變更。

選取**File**（檔案） > **Save**（儲存），以儲存您對 CSV 檔案所做的變更。

或者，選取**File**（檔案） > **Save As**（另存新檔），將變更儲存在新的 CSV 檔案中。若要建立新的 CSV 檔案，您必須在副檔名中包含 **.csv**。



STEP 7 | 將 CSV 檔案匯入至 Strata Cloud Manager。

1. 選取**Manage**（管理） > **Configuration**（設定） > **Overview**（概要）。
2. 在 [Variables（變數）] 區段中，按一下顯示的變數計數。
3. 選取**CSV Export/Import**（**CSV** 匯出/匯入） > **Import**（匯入）。
4. 選擇檔案，然後選取您修改的變數所在的 CSV 檔案。
5. 匯入。

匯出變數

將您的資料夾和防火牆設定變數以 CSV 格式匯出至本機裝置。在多個防火牆間覆寫大量變數時，匯出變數將有其效用。

不支援匯出您在資料夾層級設定介面時建立的介面變數。

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取**Manage**（管理） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Configuration**（設定） > **Overview**（概要）。

STEP 3 | 在 [Variables（變數）] 區段中，按一下顯示的變數計數。

STEP 4 | 選取**CSV Export/Import**（**CSV** 匯出/匯入） > **Export**（匯出）。

 ©2025 Palo Alto Networks, Inc.

STEP 5 | 選取要匯出的變數所在資料夾和防火牆，然後按 **Next**（下一步）。

如果要匯出在 *Strata Cloud Manager* 上建立的所有變數，請選取 ***All Firewalls***（所有防火牆）。

STEP 6 | 選取一或多個要匯出的變數。

STEP 7 | (選用) 預覽選取的變數，以檢視其他詳細資料。

在變數預覽中，您可以檢視多項資訊，例如變數名稱、建立變數的設定範圍，以及變數值。

按一下 **Cancel**（取消），然後繼續進行下一步，或將 **CSV** 下載至本機裝置。

STEP 8 | 以 CSV 格式匯出選取的變數。

CSV 會匯出並下載到您的本機裝置。匯出的 CSV 檔案名稱格式為：

```
<cloud-management-tenant-name> - Prisma Access_<export-
date>_variables
```

 ©2025 Palo Alto Networks, Inc.

管理：概要

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

將 [Overview（概要）] 頁面視為 NGFW 和 Prisma Access 的起始點，無論是首次設定還是日常設定管理（**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概要））。

- 全域
- Prisma Access
- Strata Cloud Manager

全域

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma Access 授權

如果選取 **Global**（全域）設定範圍，則可以檢視下列詳細資料：

- 您建立的全域資料夾及其變數
- 有設定衝突的防火牆
- 防火牆同步狀態與防火牆連線狀態
- 一般資訊
- 設定片段

 ©2025 Palo Alto Networks, Inc.

- 授權
- 片段共用的受信任租用戶
- 設定版本快照

設定概要 (Prisma Access)

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 授權

如果您是剛開始使用 Prisma Access：

- **Basics**（基本）檢查清單會顯示如何啟動並執行 Prisma Access；完成此處的工作和逐步解說即可開始進行基本設定；然後測試您的環境，並建置部署。
- 以下是政策和設定資料夾的運作方式。
- 以下說明如何將設定變更推送至 Prisma Access。

如需 **Prisma Access** 環境的詳細資料：

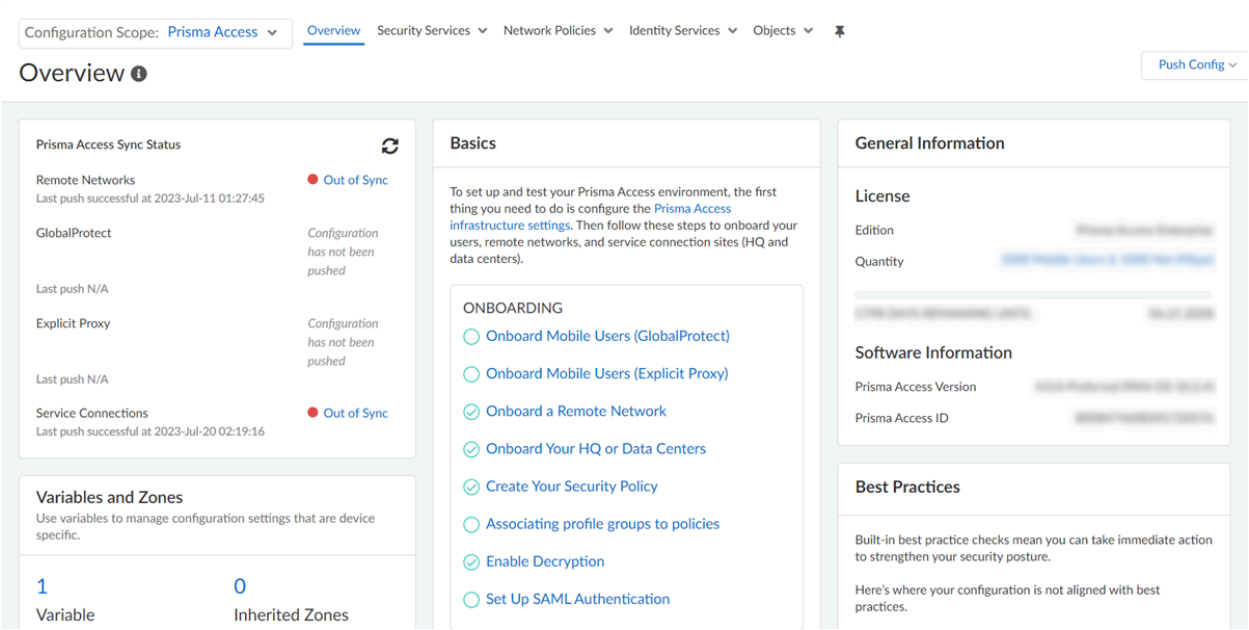
- 檢閱 **License**（授權）詳細資料，以檢視 Prisma Access 訂閱包含的內容。
- **About**（關於）面板會顯示 Prisma Access 環境的軟體和租用戶資訊。

對於日常設定管理：

- 設定狀態一目了然
- 使用設定片段將一組 Prisma Access 部署的通用基礎設定標準化
- 尋找設定快照 — 比較設定版本並還原 (或載入) 舊版，以從對流量或安全性造成非預期影響的設定推送還原
- 清除未使用的物件和規則，並藉由允許您未使用的應用程式來緊縮導致安全漏洞的規則，將您的設定最佳化
- 指出您可以在哪些區域進行設定變更以強化安全性狀態

 ©2025 Palo Alto Networks, Inc.

- 您也可以找到關於 Prisma Access 授權及其所含內容的詳細資料



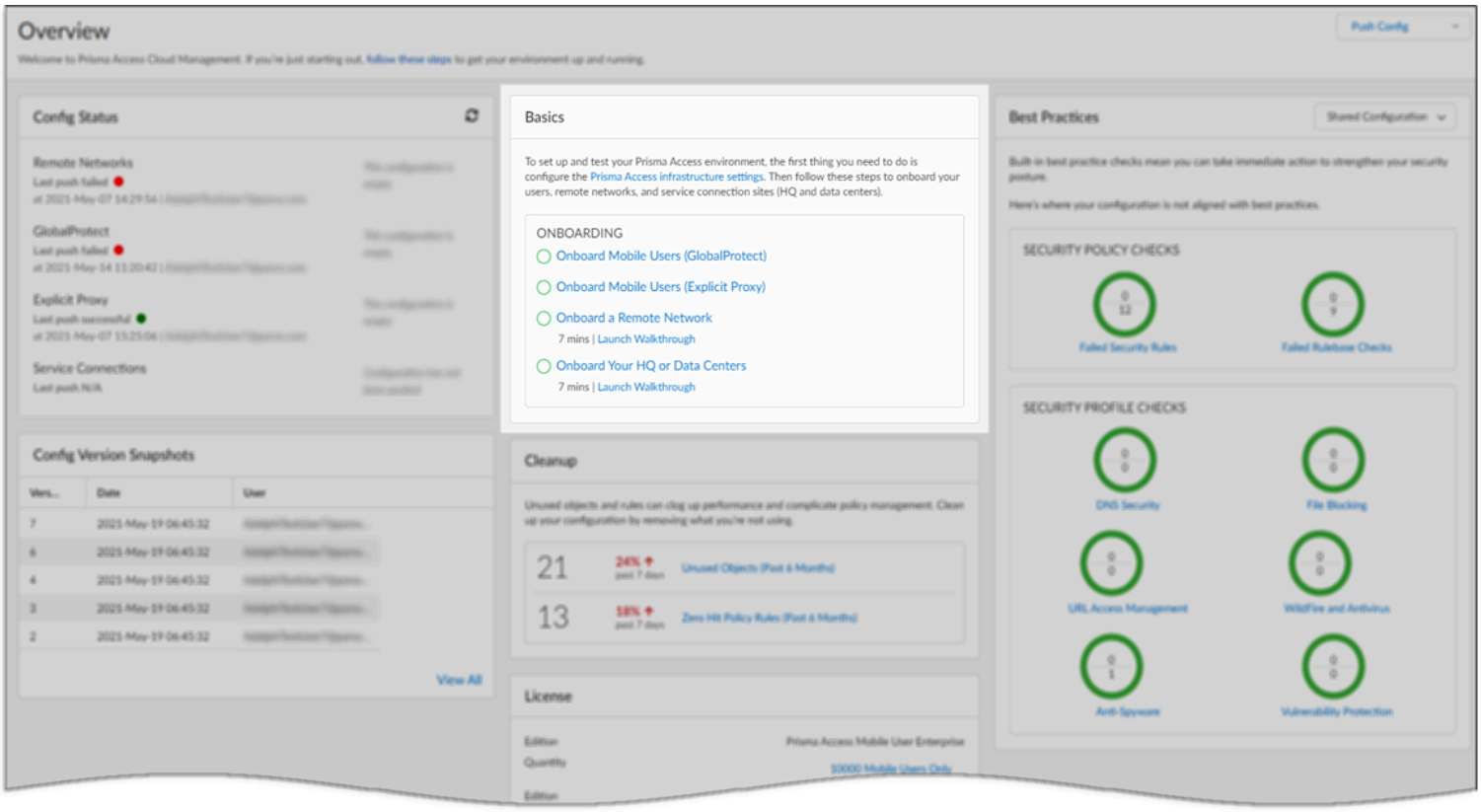
完成基本設定後，您即可開始測試環境並建立部署。

基本

Prisma Access 設定的 **Basics**（基本）可引導您啟動並執行 Prisma Access。完成此處的工作，以開始進行基本設定，以便後續用來測試環境及建置部署。

每個工作會將您連結至可以設定相關設定的頁面；完成後，此清單中的工作會顯示為已完成。因此，您可以輕鬆追踪進度，這在上線階段將特別有幫助。

 ©2025 Palo Alto Networks, Inc.

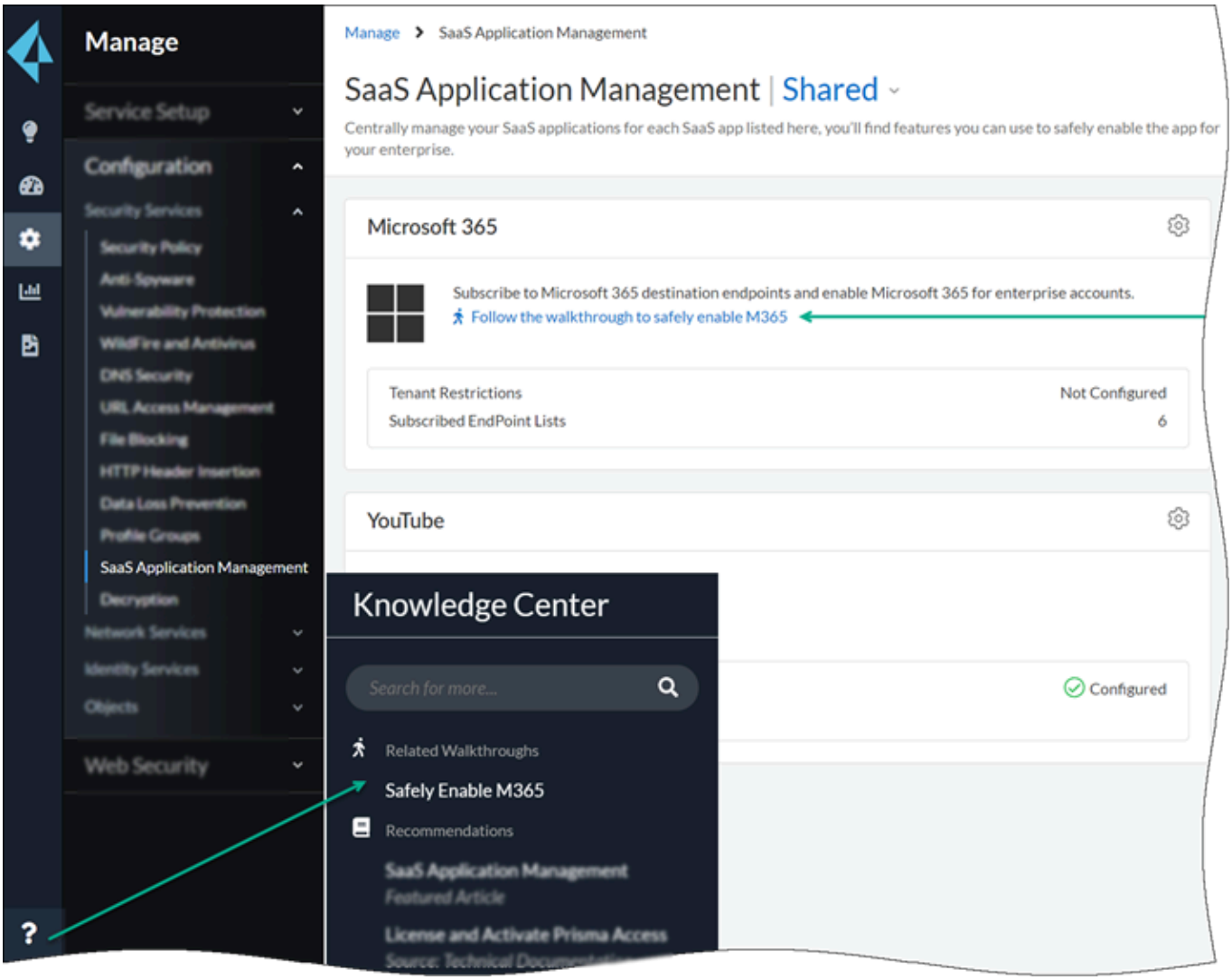


逐步解說

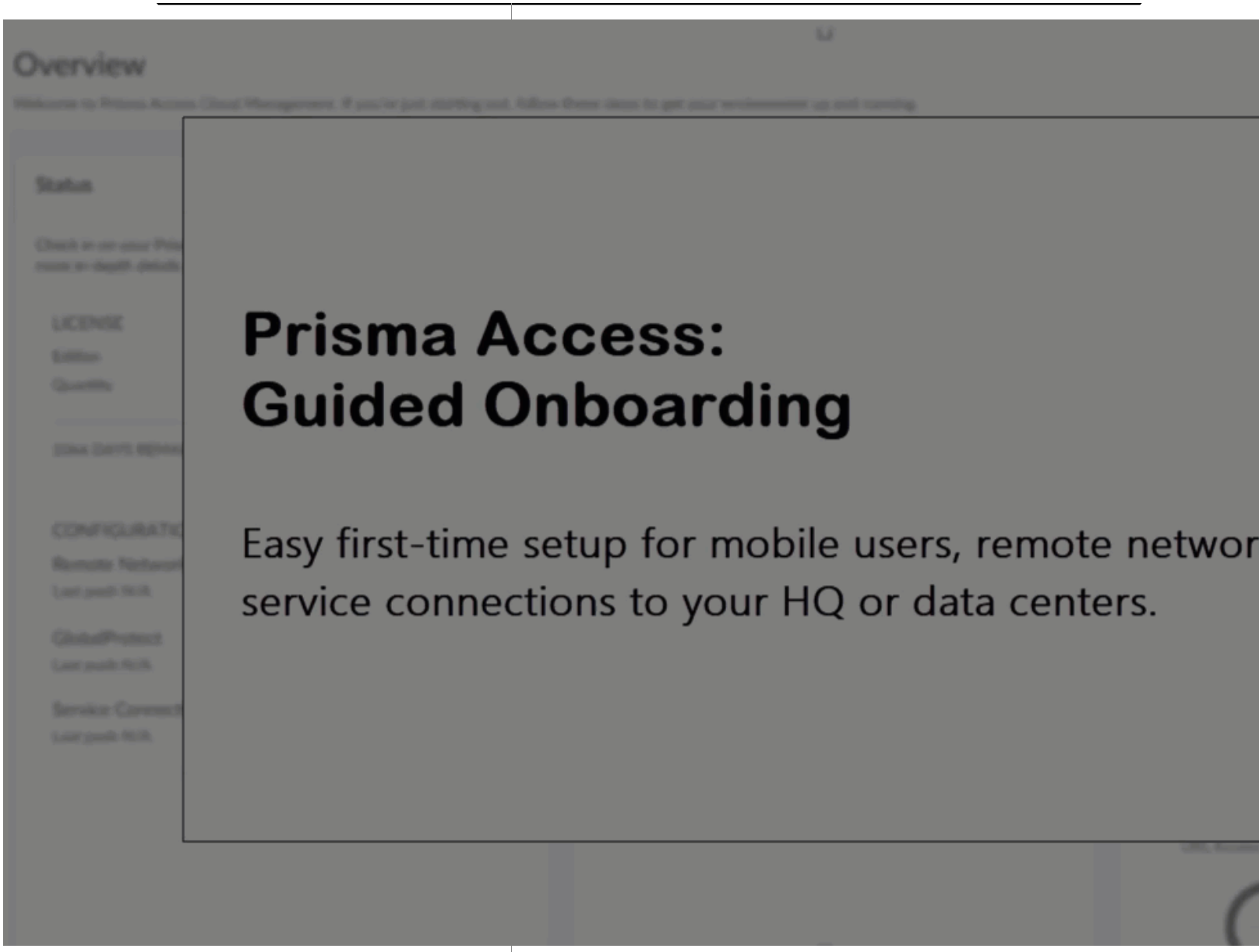
待辦事項還包括依照逐步解說完成啟動並執行環境所需的基本步驟。

您可以在 **Overview**（概要）儀表板上找到上線逐步解說。您可以按一下說明，查看您所在的頁面是否有可用的逐步解說，並留意是否有可直接在頁面上啟動的逐步解說：

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.



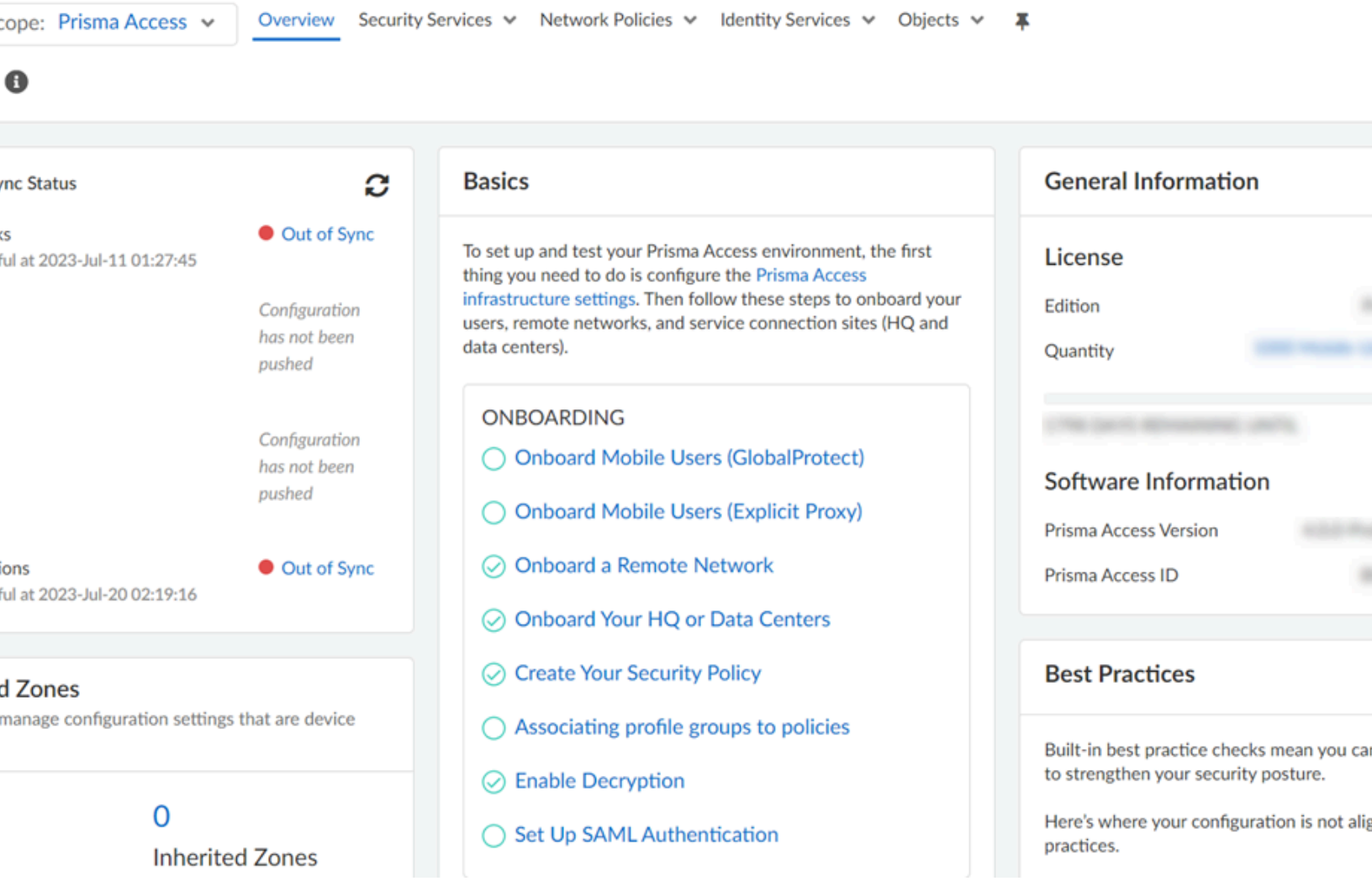
Prisma Access 同步狀態

在 **Overview**（概要）頁面上，您可以快速查看 Prisma Access 設定的狀態。如果您發現意外狀況，請深入檢視以識別受影響的設定。以下是您可能看到的狀態：

- 設定尚未推送 — 目前為止沒有任何設定推送至 Prisma Access。
- 此設定是空的 — 使用者將空的設定推送至 Prisma Access。在此情況下，由於先前已有設定，因此對 Prisma Access 的推送可能會移除設定。移至**Push Config**（推送設定） > **Jobs**（工作）以檢視最近的變更。
- 不同步 — 使用者已將設定推送至 Prisma Access，但沒有與推送相關的錯誤或警告。這可能是設定問題，或是推送至 Prisma Access 的相關問題。
- 同步 — 最新的設定已成功推送至 Prisma Access，且未出現錯誤。

 ©2025 Palo Alto Networks, Inc.

如果出現非預期的狀況，請按一下狀態以開啟地圖檢視，顯示有行動使用者（GlobalProtect 或明確 Proxy 連線）、遠端網路或服務連線的位置。然後，您即可找出需要檢閱的設定或可能需要更新的部分。

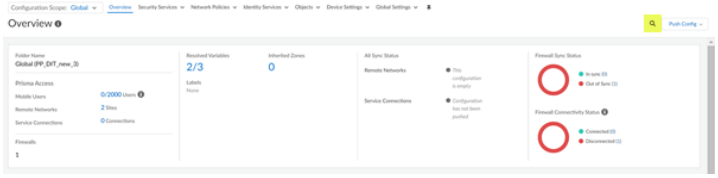


使用設定搜尋的全域搜尋

「設定搜尋」可讓您在特定的設定物件和設定中尋找特定字串，例如 IP 位址、物件名稱、參考的物件、重複物件、政策名稱、政策規則、特定 CVE 涵蓋的政策、規則 UUID、預先定義的片段或應用程式名稱，並取得所有使用物件之參考的清單。

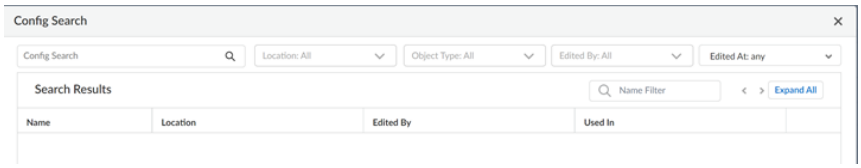
1. 若要啟動 **Config Search**（設定搜尋），請按一下網頁介面右上方的 **Push Config**（推送設定）旁的

   圖示。所有頁面的 **Manage**（管理）底下均提供 **Config Search**（設定搜尋）。



 ©2025 Palo Alto Networks, Inc.

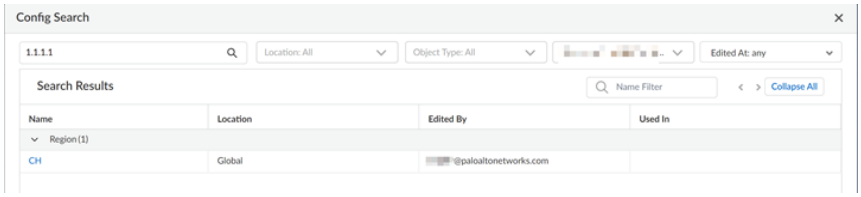
2. 在 **Config Search**（設定搜尋）畫面中，您可以使用 **Config String**（設定字串）、**Location**（位置）、**Object Type**（物件類型）、**Edited By**（編輯者）或 **Edited At**（編輯位置）等欄位進行搜尋。



搜尋提示：

- 若要尋找完全相同的片語，請用引號括住片語。
- 搜尋字詞中的空格會以 AND 運算來處理。例如，如果您搜尋 corp policy，則搜尋結果會包含設定中存在 corp 與 policy 的執行個體。
- 若要重新執行先前的搜尋，請按一下 **Config Search**（設定搜尋）圖示，該圖示會顯示最近的 50 次搜尋。按一下清單中的任何項目，即可重新執行該搜尋。每個管理員帳戶都有唯一的搜尋歷程記錄清單。
- 「設定搜尋」適用於每個可搜尋的欄位。例如，您可以在下列物件類型中搜尋安全性政策：標籤、區域、位址、使用者、HIP 設定檔、應用程式、UUID 和服務。
- 位置會按資料夾和片段分組。您可以選取多個要搜尋的位置。若未選取任何位置，依預設會選取 **All**（全部）的位置。
- 若未選取物件類型，則會選取 **All**（全部）。

3. 搜尋結果會進行分類，並提供 Strata Cloud Manager 中的設定位置連結，讓您輕鬆找到搜尋字串的所有相符項目和參考。



設定概要（Strata Cloud Manager）

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)

如果您是剛開始使用 NGFW 的雲端管理：

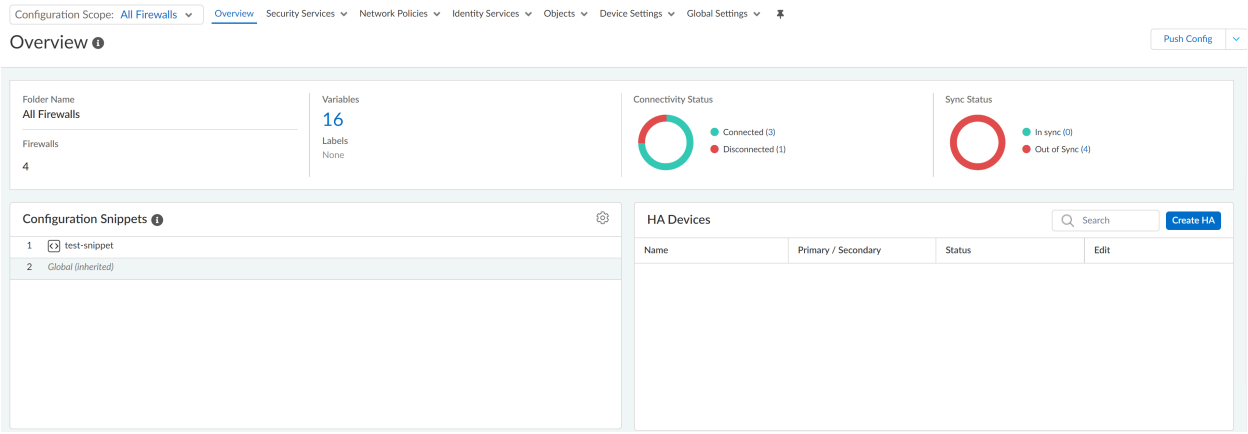
- 以下是政策和設定資料夾的運作方式。

 ©2025 Palo Alto Networks, Inc.

- 以下說明如何將設定變更推送至防火牆。

對於日常設定管理：

- 概覽目前資料夾名稱、新增至資料夾的防火牆數目、為資料夾建立的變數數目的摘要。
- 取得對本機防火牆設定的可見性和控制，而無須在中央管理與個別防火牆之間切換以管理本機設定。
  - **Firewalls with config conflicts**（有設定衝突的防火牆）會顯示有衝突的防火牆數目。按一下數字，可檢視防火牆的衝突及其位置。按一下任何防火牆，即可查看裝置層級的衝突。
  - **Objects with config conflict**（有設定衝突的物件）會顯示每個防火牆的衝突數目。按一下數字，可檢視特定防火牆的衝突物件及其類型。按一下物件可提供關於衝突的詳細資料。
- 使用設定片段將一組受管理防火牆的通用基礎設定標準化。
- 在高可用性 (HA) 設定中設定受管理的防火牆，以提供備援性並確保業務連續性。
- 檢閱受管理防火牆對 Strata Cloud Manager 的連線狀態。
- 檢閱 Strata Cloud Manager 與受管理防火牆上目前執行中的設定之間的設定同步狀態。

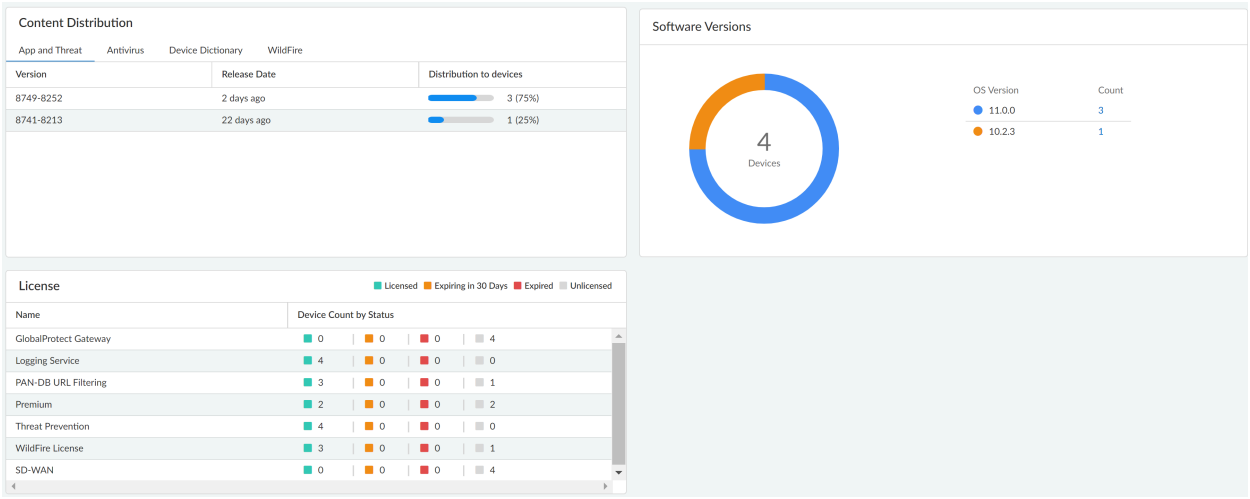


關於受管理防火牆的詳細資料：

- 檢閱內容散佈和軟體版本詳細資料，以瞭解哪些動態內容更新和 PAN-OS 軟體版本正在您受管理的防火牆上執行。

 ©2025 Palo Alto Networks, Inc.

- 檢閱 **License**（授權）詳細資料，以查看您受管理的防火牆上啟動了哪些授權。

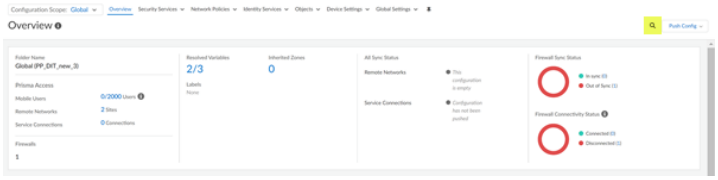


使用設定搜尋的全域搜尋

「設定搜尋」可讓您在設定物件和設定中搜尋特定字串，例如 IP 位址、物件名稱、參考的物件、重複物件、政策名稱、政策規則、特定 CVE 涵蓋的政策、規則 UUID、預先定義的片段或應用程式名稱，並取得所有使用物件之參考的清單。

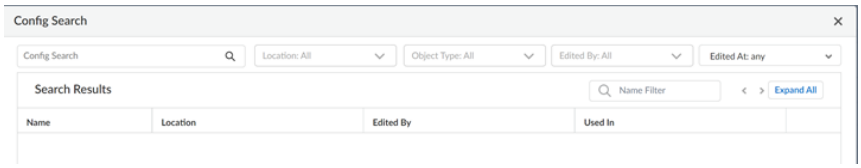
1. 若要啟動 **Config Search**（設定搜尋），請按一下網頁介面右上方的 **Push Config**（推送設定）旁的

   圖示。所有頁面的 **Manage**（管理）底下均提供 **Config Search**（設定搜尋）。



 ©2025 Palo Alto Networks, Inc.

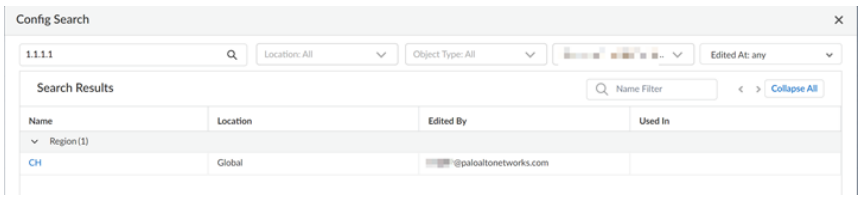
2. 在 **Config Search**（設定搜尋）畫面中，您可以使用 **Config String**（設定字串）、**Location**（位置）、**Object Type**（物件類型）、**Edited By**（編輯者）或 **Edited At**（編輯位置）等欄位進行搜尋。



搜尋提示：

- 若要尋找完全相同的片語，請用引號括住片語。
- 搜尋字詞中的空格會以 AND 運算來處理。例如，如果您搜尋 corp policy，則搜尋結果會包含設定中存在 corp 與 policy 的執行個體。
- 若要重新執行先前的搜尋，請按一下 [Config Search（設定搜尋）] 圖示，該圖示會顯示最近的 50 次搜尋。按一下清單中的任何項目，即可重新執行該搜尋。每個管理員帳戶都有唯一的搜尋歷程記錄清單。
- 「設定搜尋」適用於每個可搜尋的欄位。例如，您可以在下列物件類型中搜尋安全性政策：標籤、區域、位址、使用者、HIP 設定檔、應用程式、UUID 和服務。
- 位置會按資料夾和片段分組。您可以選取多個要搜尋的位置。若未選取任何位置，依預設會選取 **All**（全部）的位置。
- 若未選取物件類型，則會選取 **All**（全部）。

3. 搜尋結果會進行分類，並提供 Strata Cloud Manager 中的設定位置連結，讓您輕鬆找到搜尋字串的所有相符項目和參考。



 ©2025 Palo Alto Networks, Inc.

管理：安全服務

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

管理您的安全服務，並保護網路、系統和使用者。

移至**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服務）。

透過安全服務，您可以：

- 透過 管理：安全性原則 定義要強制執行 Prisma Access 流量的方式。
- 透過 管理：解密 阻止隱藏在加密流量中的威脅。

管理：安全性原則

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

安全性政策是您定義要如何在 Prisma Access 和 NGFW 部署中強制執行流量的位置。通過 Strata Cloud Manager 環境的所有流量都會根據您的安全性政策進行評估，並從上到下套用規則。

若要設定安全性政策，請**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）。

 ©2025 Palo Alto Networks, Inc.

開始使用安全性政策

現在您可以執行以下一些操作，讓安全性政策為您所用。

- 建立安全性政策規則 – 安全性政策可讓您強制執行規則並採取行動，並且視需要作為一般或特定政策。
- 追蹤規則庫中的規則 - 規則庫中的每個規則都會自動編號；當您移動或重新排序規則時，編號將根據新的順序而變更。
- 強制執行政策規則最佳做法 – 建立或修改規則時，可以要求提供規則說明、標籤和稽核註解，以確保原則規則庫正確組織和分組，並保留重要的規則歷程記錄以用於稽核目的。
- 測試政策規則 – 使用政策分析器檢查政策規則。
- 啟動安全性設定檔 – 安全性政策允許應用程式或類別後，會套用安全性設定檔以掃描流量。
- 建立安全性設定檔群組 – 安全性設定檔群組是一組安全性設定檔，您可以將這一組設定檔視為一個單元，輕鬆地將此單元新增至安全性政策。
- 設定檔案封鎖 – 識別要封鎖或監控的特定檔案類型。
- 建立資料篩選設定檔 – 防止敏感資訊離開您的網路。
- 管理 Web 安全性 – 控制對網際網路和 SaaS 應用程式的存取（一般瀏覽）。

管理：解密

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

啟用解密以阻止隱藏在加密流量中的威脅。您只需要匯入解密憑證即可開始使用。至於其他一切，我們建立了最佳做法設定，供您用於啟動並執行。

在這裡進一步瞭解流量的解密。

移至**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服務） > **Decryption**（解密）。

解密概要介紹

Secure Sockets Layer（安全通訊端層，SSL）與 Secure Shell（安全殼層，SSH）加密通訊協定用於保護兩個實體（例如 Web 伺服器與用戶端）之間的流量。SSL 與 SSH 會將流量封裝並加密資料，讓資料只對擁有憑證與金鑰的用戶端與伺服器有意義，憑證用於確認裝置之間值得信任，金鑰則用於將資料解碼。解密 SSL 和 SSH 流量可：

 ©2025 Palo Alto Networks, Inc.

- 防止隱藏為加密流量的惡意軟體滲入您的網路。例如，攻擊者會入侵使用 SSL 解密的網站。員工造訪該網站並在不知情的情況下下載漏洞或惡意軟體。惡意軟體隨後使用受感染的員工端點在網路中橫向傳播，並危及其他系統。
- 防止敏感資訊移到網路之外。
- 確保適當的應用程式在安全的網路上執行。
- 選取性地解密流量；例如，建立解密政策和設定檔，使金融或醫療保健站台的流量免於解密。

Strata Cloud Manager 中不支援 *SSH Proxy* 解密。

解密政策

Strata Cloud Manager 提供兩種類型的解密政策規則：控制輸出 SSL 流量的 SSL 正向 Proxy，以及控制輸入 SSL 流量的 SSL 輸入檢查。

SSL 正向 **Proxy**

當您設定防火牆解密通往外部站台的 SSL 流量時，防火牆會用作 SSL 正向 Proxy。使用 Ssl 正向 Proxy 解密原則將從內部使用者流到 Web 的 SSL/TLS 流量進行解密與檢查。SSL 正向 Proxy 解密可防止隱藏為 SSL 加密流量的惡意軟體透過解密流量滲入公司網路，以便防火牆可以將解密設定檔和安全性原則及設定檔套用於流量。

SSL 輸入檢查

使用 SSL 輸入檢查可對從用戶端流向目標網路伺服器（任何您有其憑證並能將憑證匯入到防火牆上的伺服器）的輸入 SSL/TLS 流量進行解密與檢查，並封鎖可疑工作階段。例如，假設惡意行為者想要利用 Web 伺服器中的已知漏洞。輸入 SSL/TLS 解密提供對流量的可見度，從而允許防火牆主動回應威脅。

解密設定檔

您可將解密設定檔附加到原則規則以將精確存取設定套用於流量，比如檢查伺服器憑證、不受支援的模式以及失敗。

SSL 正向 **Proxy** 設定檔

對於連結了設定檔的正向 Proxy 解密政策中定義的輸出 SSL/TLS 流量，SSL 正向 Proxy 解密設定檔可控制伺服器驗證、工作階段模式檢查與失敗檢查。

SSL 輸入檢查設定檔

對於連結了設定檔的輸入檢查解密政策中定義的輸入 SSL/TLS 流量，SSL 輸入檢查解密設定檔可控制工作階段模式檢查與失敗檢查。

「不解密」的設定檔

「不解密」設定檔會為您選擇不解密的流量執行伺服器驗證檢查。將「不解密」設定檔連結至「不解密」解密政策，定義要從解密中排除的流量。（請勿使用原則排除無法解密的流量，因為網站會因釘選憑證或相互驗證之類的技術原因而中斷解密。而是將主機名稱新增至解密排除清單。）

 ©2025 Palo Alto Networks, Inc.

解密提示

- 使用最佳做法政策規則作為建置解密政策的起點

  這些規則（一個將流量解密的規則，和一個將敏感內容排除於解密外的規則）是根據 URL 類別建置的。

- 將敏感內容排除於解密外

  基於商業、法律或法規原因，將敏感內容排除於解密外。

  - 預先定義的解密排除 — Palo Alto Networks 會維護此排除清單，並定期更新。此清單會全域套用，且依預設會套用至您指定要解密的所有流量。如果符合您的業務需求，您可以停用清單項目。
  - 自訂排除 — 將全域的站台或應用程式排除於解密外。
  - 政策型排除 — 使用 URL 類別和外部動態清單，建立針對性的政策型解密規則。將解密政策規則動作設定為不解密，將相符的流量排除於解密外。

  請務必將解密排除設置於政策規則之上，使其優先套用。

- 請考量您可以全域套用部分解密設定，其他設定則以特定位置為目標

  - 您的 Strata Cloud Manager 解密政策將全域套用至所有 NGFW 和 Prisma Access 位置。

    管理 > 組態設定 > **NGFW** 和 **Prisma Access** > 安全服務 > 解密

  - 瀏覽至各種類型的解密政策，以建立以特定防火牆、行動使用者位置、遠端網站或服務連線為目標的政策規則

    管理 > 組態設定 > **NGFW** 和 **Prisma Access** > 設定範圍 > 全域/防火牆/行動使用者/遠端網路/服務連線

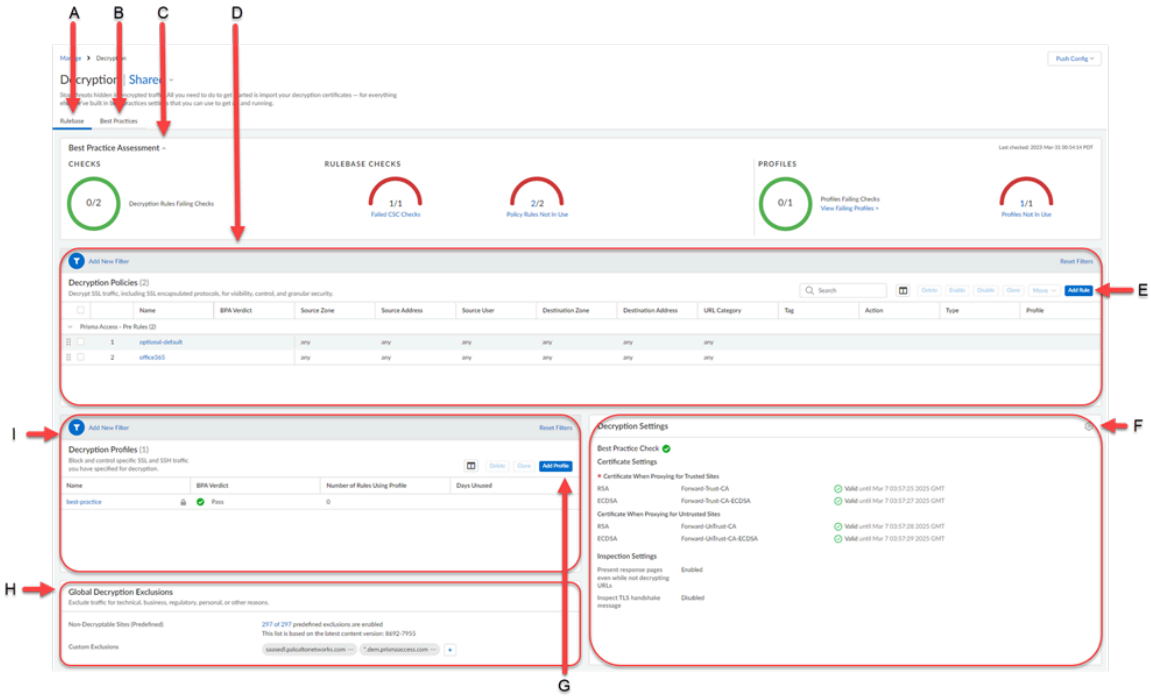
- 規則順序有其重要性

  解密政策規則會由上至下套用。請將您要先強制執行的規則設置於解密政策規則清單的頂端。全域規則（預先規則）會先套用，且一律列在行動使用者、遠端網路和服務連線的特定規則前面。

解密概覽

[Decryption（解密）] 畫面是供您設定解密政策和設定檔以及檢視最佳做法評估的位置。

 ©2025 Palo Alto Networks, Inc.



A) 規則庫 — 規則庫檢查會查看如何安全性政策的組織和管理方式，包括適用於許多規則的組態設定。

B) 最佳做法 — 在此，您可以全方位檢視您的功能實作是否符合最佳做法。檢查失敗的檢查，以瞭解可改進之處（您也可以檢閱通過的檢查）。

C) 最佳做法評估 — 最佳做法分數顯示在解密儀表板上。這些分數可以讓您快速檢視最佳做法進度。您可以迅速識別需要進一步調查的領域，或您想要採取措施以改善安全性狀態的部分。

D) 解密政策 — 已上線的解密政策清單。檢閱政策設定、政策類型（*SSL* 正向 *Proxy*、、*SSL* 輸入檢查或 *SSH Proxy*）、政策動作（解密或不解密），以及 BPA 裁定。

E) 新增規則 — 新增和設定新的解密政策。

F) 解密設定 — 存取憑證和解密設定。匯出和匯入憑證。

G) 新增設定檔 — 新增和設定新的解密設定檔。

H) 全域解密排除 — 排除於解密外的應用程式。

I) 解密設定檔 — 已上線的解密設定檔清單。檢閱設定檔設定、使用設定檔的政策，以及 BPA 裁定。

 ©2025 Palo Alto Networks, Inc.

管理：網路政策

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

您可以建立各種類型的網路政策，來保護網路免受威脅和中斷。它可協助您最佳化網路資源配置及管理網路政策，以排定流量的優先順序並設定應用程式分類。

規則是由上至下評估的，且在流量與定義的規則準則比對時，將不會評估後續規則。您應將較具體的政策規則排序在較通泛的政策規則之上，以盡可能執行最佳比對準則。為規則啟用記錄時，會為符合政策規則的流量產生日誌。每個規則的記錄選項都是可設定的。

最佳做法政策規則適用於大部分的政策類型，可協助您快速且安全地開始使用。雖然這些規則無法編輯以確保您始終能擁有最低層級的安全性，但如果您想將其用作自訂政策的基礎，可加以複製。

移至**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Network Policies**（網路政策）。

透過網路政策，您可以：

- 透過 管理：QoS 優先考量對您的操作最重要的流量。
- 透過 管理：應用程式覆寫 管理 Prisma Access 對您的應用程式進行分類的方式。

管理：QoS

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	其中一個： ❑ Prisma Access 授權 ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

透過服務品質 (QoS)，您可以優先考量需要低延遲的業務關鍵流量和應用程式（例如 VoIP 和視訊應用程式）。若要新增或編輯 QoS 政策規則，請移至**Manage**（管理） > **Configuration**（設

©2025 Palo Alto Networks, Inc.

定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Network Policies**（網路政策） > **QoS**。

QoS 政策規則

服務品質 (QoS) 政策規則可識別需要優先處理或頻寬限制的流量。QoS 規則可讓您在有限的網路容量下可靠地執行高優先順序的應用程式和流量。您可以使用區分服務代碼點 (DSCP) 來設定流量 QoS 處理。這些代碼點是封包標頭值，可用於要求流量的高優先順序或盡力傳遞等。Prisma Access 會對傳入流量強制執行 DSCP 值，也會在工作階段流量離開防火牆時使用 DSCP 值標記工作階段。這意味著工作階段的所有輸入和輸出流量都會受到連續的 QoS 處理。您可以使用下列代碼點來設定流量 QoS 處理：

- 加速轉送 **(EF)**—用來要求流量的低損失、低延遲和保證頻寬。

  具有 EF 代碼點值的封包通常保證以最高優先順序傳遞。
- 保證式轉送 **(AF)**—用來提供可靠的應用程式傳遞。

  具有 AF 代碼點的封包，表示要求流量接受比服務最佳效能還要高的優先處理。具有 EF 代碼點的封包優先於具有 AF 代碼點的封包。
- 類別選取器 **(CS)** — 用來提供使用 IP 優先順序欄位以標記優先順序流量的網路 IP 位址所需的回溯相容性。
- **IP** 優先順序 **(ToS)**— 供舊版網路 IP 位址用來標記優先順序流量。
- 自訂代碼點- 輸入代碼點名稱和二進位值，藉以建立用來比對流量的自訂代碼點。

  例如，您可以建立 QoS 政策規則以優先考量語音通訊，例如 voice over IP (VOIP)，以確保封包傳輸的一致性。這樣可以確保語音通訊的一致性。

管理：應用程式覆寫

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

建立應用程式覆寫政策，指定要使用快速路徑第四層檢查來處理應用程式，而不是使用 App-ID 進行第七層檢查。這會強制安全性強制執行節點將工作階段視為定期具狀態檢查進行處理，並節省應用程式處理時間。若您不想要對已知 IP 位址之間的自訂應用程式進行流量檢查，您可以建立應用程式覆寫政策規則。例如，如果您在非標準連接埠上有一個自訂應用程式，且您知道存取該應用程式的使用者都受到認可，而且兩者都位於「信任」區域中，您可以對存取自訂應用程式的受信任使用者覆寫應用程式檢查需求。

 ©2025 Palo Alto Networks, Inc.

若要變更 Prisma Access 應用程式的分類方式，請移至**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Network Policies**（網路政策） > **Application Override**（應用程式覆寫），然後建立應用程式覆寫政策規則。

應用程式覆寫提示

設想您在建立應用程式覆寫政策規則時，您將 App-ID 限定為無法分類部署的流量，並根據該應用程式識別執行威脅檢查。為了支援內部專屬應用程式，可以考慮建立包含應用程式簽章的自訂應用程式 (而非應用程式覆寫規則)，以便 Strata Cloud Manager 執行第七層檢查，並掃描應用程式流量中是否包含威脅。若要建立自訂應用程式，請移至**Manage** > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（物件） > **Applications**（應用程式）。

應用程式覆寫政策

使用下列區段來設定應用程式覆寫規則：

- 來源
  - 區域—**Add** 來源區域。
  - 位址—新增來源位址、位址群組或區域並指定設定。
- 目的地
  - 區域—新增以選擇目的地區域。
  - 位址—新增來源位址、位址群組或區域並指定設定。
- 應用程式
  - 應用程式 — 為符合以上規則準則的流量選取覆寫應用程式。覆蓋自訂應用程式時，不會進行任何威脅檢驗。您覆寫預先定義的應用程式支援威脅檢驗時則為例外。

    若要定義新應用程式，請移至**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（物件） > **Applications**（應用程式）。
- 通訊協定
  - 通訊協定 — 選取要允許應用程式覆寫的通訊協定（**TCP** 或 **UDP**）。
  - 連接埠—輸入指定目的地位址的連接埠號碼（0 至 65535）或連接埠號碼範圍（連接埠 1 - 連接埠 2）。多個連接埠或範圍必須以逗號隔開。

管理：基於原則的轉送

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ☐ Prisma Access ☐ AIOps for NGFW Premium ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro

 ©2025 Palo Alto Networks, Inc.

這可在何處使用？	我需要哪些內容？
	→ 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

政策型轉送規則允許流量從路由表中指定的下一躍點取得替代路徑，基於安全或效能考量，PBF 規則一般用於指定輸出介面。

移至**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Network Policies**（網路政策） > **Policy Based Forwarding**（政策型轉送）。

使用政策型轉送規則，將流量導向至特定的輸出介面，並覆寫流量的預設路徑。建立政策型轉送規則之前，請務必先瞭解 IPv4 位址集會被視為 IPv6 位址集的子集。

請使用下列區段來設定政策型轉送規則：

- 來源
  - 區域—新增來源區域。
  - 介面—新增來源介面。
  - 位址—新增來源位址、位址群組或區域並指定設定。
  - 使用者—新增套用政策的使用者和使用者群組。
- 目的地
  - 位址—新增來源位址、位址群組或區域，並指定設定。
- 應用程式和服務
  - 應用程式實體 — 選取要透過替代路徑路由的應用程式

    。

    政策型轉送規則可在防火牆有足夠的資訊可判斷應用程式前套用。因此不建議將應用程式特定的規則與政策型轉送搭配使用。盡可能使用服務物件。

    您無法在政策型轉送規則中設定自訂應用程式、應用程式篩選器或應用程式群組。
  - 服務實體 — 選取您要透過替代路徑路由的服務和服務群組。

 ©2025 Palo Alto Networks, Inc.

- 轉送
  - 動作—您可以選擇下列選項，藉以設定在比對封包時所要採取的動作：
    - 轉送—將封包導向至指定的 **Egress Interface**（輸出介面）。
    - 捨棄—捨棄封包。
    - 非 **PBF**—排除符合在規則中所定義來源、目的地、應用程式或服務準則的封包。相符的封包會使用路由表，而不是 PBF。
  - 輸出介面 — 選取您要將符合政策型轉送規則的流量轉送至何處的網路資訊。
  - 下一個躍點
    - **IP** 位址 — 輸入 IP 位址，或選取 IP 網路遮罩類型的位址物件，以將相符的封包轉送至該處。
    - **FQDN** — 輸入 FQDN（或選取或建立類型為 FQDN 的位址物件），防火牆會將相符封包轉送到該物件。
    - 無—無下一個躍點意味著封包的目的地 IP 位址會作為下一個躍點。如果目的地 IP 位址與輸出介面未在同一個子網路上，轉送將失敗。
  - 監控—若未指定 IP 位址，則啟用監控功能以確認對目標 IP 位址或下一個躍點 IP 位址的連線。

管理：NAT

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

您可使用 NAT 將非可路由的私人 IPv4 位址轉譯為一或多個可全域路由的 IPv4 位址，因此能保留組織的可路由 IP 位址。使用 NAT，也可在不洩露主機的真實 IP 位址的情況下讓主機存取公用位址，並透過執行連接埠轉送來管理流量。您可使用 NAT 來解決網路設計挑戰，並讓網路具有可彼此通訊的相同 IP 子網路。

您至少可以設定 NAT 政策規則來比對封包的來源區域與目的地區域。除了區域外，您還可以根據封包的目的地介面、來源與目的地位址，以及服務來設定比對準則。您可以設定多個 NAT 規則。

移至**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Network Services**（網路服務） > **NAT**。

 ©2025 Palo Alto Networks, Inc.

排解連線問題 - 取得路由和通道狀態的彙總檢視，並深入瞭解具體情況，找出異常和有問題的設定。

管理：SD-WAN

我可以在哪裡使用這個？	我需要哪些內容？
• SD-WAN	❑ SD-WAN 授權

SD-WAN 原則規則指定應用程式和/或服務以及流量散佈設定檔，以確定防火牆如何為不屬於現有工作階段且與滿足所有其他條件（如來源和目的地區域、來源和目的地 IP 位址以及來源使用者）的傳入封包選取偏好路徑。SD-WAN 政策規則也會指定一個路徑品質設定檔，其中包含延遲、抖動和封包遺失的閾值。當超出其中一個閾值時，防火牆會為應用程式和/或服務選取新路徑。

若要設定 SD-WAN 政策，請選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Network Policies**（網路政策） > **SD-WAN**。

規則

您可在共用內容中，將預先規則和後續規則定義為所有受管理防火牆的共用政策，或定義於某個裝置群組內容中，使其成為某個裝置群組的特定規則：

- 預先規則—新增至規則順序的頂端，並且將優先評估的規則。您可以使用預先規則強制執行組織的可接受使用原則。例如，您可以封鎖存取特定 URL 類別或允許所有使用者的 DNS 流量。
- 後續規則—新增至規則順序的底部，並且在預先規則和防火牆本機上定義的規則之後才會評估的規則。後續規則通常包含會根據 **App-ID™**、**User-ID™** 或服務拒絕他人存取流量的規則。

設定檔

建立設定檔以套用至 SD-WAN 政策規則中指定的應用程式和服務集。

路徑品質

SD-WAN 可讓您為具有獨特網路品質要求的每組應用程式、應用程式篩選器、應用程式群組、服務、服務物件和服務群組物件建立一個路徑品質設定檔，然後在 SD-WAN 政策規則中參考該設定檔。在該設定檔中，設定三個參數的最大閾值：延遲、抖動和封包遺失。當 SD-WAN 連結超出任何一個閾值時，防火牆會為符合套用此設定檔之 SD-WAN 規則的封包選取新的最佳路徑。

SaaS 品質

SD-WAN 允許您建立軟體即服務 (SaaS) 品質設定檔，以測量中樞或分支防火牆與伺服器端 SaaS 應用程式之間的路徑健康情況品質，從而準確地監控 SaaS 應用程式的可靠性，以及在路徑健康情況品質下降時交換路徑。這讓防火牆能夠準確地確定，何時容錯移轉至不同的直接網際網路存取 (DIA) 連結。

SaaS 品質設定檔允許您使用監控應用程式活動的自適應學習演算法，來指定要監控的 SaaS 應用程式，或者使用應用程式 IP 位址、FQDN 或 URL 來指定 SaaS 應用程式。

流量分佈

 ©2025 Palo Alto Networks, Inc.

對於此流量散佈設定檔，選取防火牆用於散佈工作階段並在路徑品質惡化時容錯移轉到更好的路徑的方法。新增連結標籤，防火牆在確定用於轉送 SD-WAN 流量的連結時需要考慮這些標籤。將流量散佈設定檔套用至您建立的每個 SD-WAN 政策規則。

Error Correction 錯誤更正

如果您的 SD-WAN 流量包含對封包遺失或損毀敏感的應用程式（例如音訊、VoIP 或視訊會議），則可套用正向錯誤更正 (FEC) 或封包複製作為錯誤更正方法。使用 FEC，接收防火牆（解碼器）可透過使用編碼器嵌入應用程式流中的同位檢查位元，來復原遺失或損毀的封包。封包複製是錯誤更正的另一種方法，其中應用程式工作階段從一個通道複製到第二個通道。若要採用這些方法之一，請建立一個錯誤更正設定檔，並在特定應用程式的 SD-WAN 政策規則中引用。

（您還必須透過在 SD-WAN 介面設定檔中指示介面 Eligible for Error Correction Profile interface selection（符合錯誤更正設定檔介面選取資格），來指定防火牆可用於選取哪些介面進行錯誤更正。）

SD-WAN 介面

建立一個 SD-WAN 介面設定檔以定義 ISP 連線的特征，並指定連結的速度以及防火牆監控連結的頻率，然後為連結指定一個連結標籤。當您在多個連結上指定相同連結標籤時，便可將這些實體連結分組（組合）到一個連結組合或粗管。必須先設定一個 SD-WAN 介面設定檔，將其指定給一個已啟用 SD-WAN的乙太網路介面，然後才可儲存該乙太網路介面。

連結標籤

建立一個連結標籤，以標識您希望應用程式和服務在 SD-WAN 流量散佈和容錯移轉保護期間以特定順序使用的一個或多個實體連結。將多個實體連結分組在一起，可在實體連結健康情況惡化時最大化應用程式和服務品質。

當計劃如何對連結分組時，請考慮連結的用途或目的並進行相應的分組。例如，如果您正在設定計劃用於低成本或非業務關鍵流量的連結，請建立一個連結標籤，並將這些介面分組在一起，以確保預期流量主要在這些連結上流動，而不是在可能影響業務關鍵應用程式或服務的昂貴連結上流動。

 ©2025 Palo Alto Networks, Inc.

管理：識別服務

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

瞭解如何管理您的識別服務，並確認只有特定使用者可在您的網路上存取正確的資料。

移至**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Identity Services**（識別服務）。

透過識別服務，您可以：

- 僅允許合法使用者存取您的網路，方法是將 Prisma Access 連線至您的識別提供者 (IdP)，並在管理：驗證 中選擇您要使用的識別驗證方法。
- 透過 管理：雲端識別引擎 為 Prisma Access 提供對您的 Active Directory 資訊的唯讀存取權。
- 一致地強制執行安全性政策，並透過 管理：識別重新散佈 與遠端網站或服務連線站台（HQ 和資料中心）的內部部署裝置共用識別資料。

管理：驗證

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

為了確保只有合法使用者才能存取您最受保護的資源，Prisma Access 支援數種驗證類型，包括對 SAML、TACACS+、RADIUS、LDAP、Kerberos、MFA、本機資料庫驗證和 SSO 的支援。

 ©2025 Palo Alto Networks, Inc.

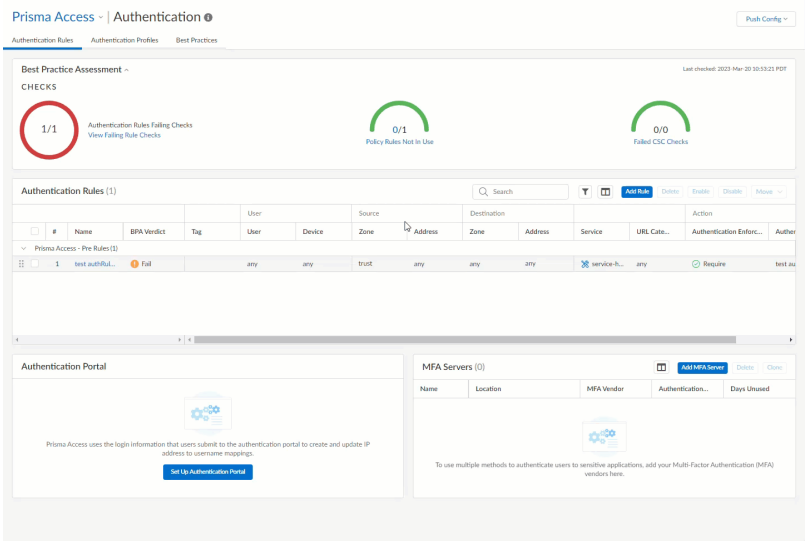
若要設定驗證政策，請移至**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Identity Services**（識別服務） > **Authentication**（驗證）。

以下是與 Prisma Access 整合用以提供驗證的服務，以及您在規劃驗證設定時所應考量的功能：

驗證支援

SAML	如果使用者存取您的網路外部的服務和應用程式，您可以使用 SAML 將 Prisma Access 與識別提供者 (IdP) 整合，以控制對外部和內部服務與應用程式的存取。SAML 單一登入 (SSO) 可讓您在登入一次後存取多個應用程式；若在您的環境中，每個使用者存取許多應用程式，每個應用程式逐一進行驗證將影響使用者的工作效率，SSO 將有所幫助。在此情況下，SAML 單一登入 (SSO) 可讓您在登入一次後存取多個應用程式。同樣地，SAML 單一登出 (SLO) 將允許使用者登出一個工作階段即可結束多個應用程式的工作階段。SSO 適用於透過 GlobalProtect 應用程式存取應用程式的行動使用者，或在遠端網路上透過驗證入口網站存取應用程式的使用者。SLO 可供 GlobalProtect 應用程式使用者使用。 您無法在驗證順序中使用 *SAML* 驗證設定檔。
TACACS+	終端存取控制器存取控制系統 + (TACACS+) 是一個通訊協定家族，允許透過集中伺服器進行驗證和授權。TACACS+ 會加密使用者名稱和密碼，因此比 RADIUS 更安全，因為後者僅加密密碼。TACACS+ 更加可靠，因為它使用了 TCP，則 RADIUS 則使用 UDP。
RADIUS	遠端驗證撥號使用者服務 (RADIUS) 是一種受到普遍支援的網路通訊協定，提供集中驗證和授權。您也可以將 RADIUS 伺服器新增至 Prisma Access，以實作多因素驗證。
LDAP	輕量型目錄存取通訊協定 (LDAP) 是用於存取資訊目錄的標準通訊協定。您可以使用 LDAP 對透過驗證入口網站存取應用程式或服務的使用者進行驗證。
Kerberos	Kerberos 是一種驗證通訊協定，可讓您使用唯一金鑰（稱為票證）在各方之間安全地交換資訊，以識別各方。透過 Kerberos，您可以對透過驗證入口網站存取應用程式的使用者進行驗證。啟用 Kerberos SSO 後，使用者僅需要在首次存取網路時登入（例如登入 Microsoft Windows）。在首次登入之後，使用者便可存取網路中任何以瀏覽器為基礎的服務，而不必再次登入，直到 SSO 工作階段到期為止。 若要使用 Kerberos，首先必須要有 Prisma Access 的 Kerberos 帳戶，以對使用者進行驗證。必須有帳戶才能建立 Kerberos

 ©2025 Palo Alto Networks, Inc.

	金鑰標籤，即包含防火牆或 Panorama 主體名稱與雜湊密碼的檔案。SSO 程序需要金鑰標籤。 Kerberos SSO 僅適用於 Kerberos 環境內部的服務和應用程式。若要為外部服務和應用程式啟用 SSO，請使用 SAML。
雲端識別引擎	雲端識別引擎 (CIE) 可為 Prisma Access — 明確 Proxy 部署中的行動使用者提供使用者識別和使用者驗證。雲端識別引擎可與明確 Proxy 驗證快取服務 (ACS) 整合，並使用 SAML 識別提供者 (IdP) 提供明確 Proxy 行動使用者的驗證。
MFA	多因素驗證 (MFA) 可讓您實作不同類型（稱為因素）的多重驗證挑戰，以保護您最敏感的服務和應用程式。例如，您可能希望對重要財務文件實作比搜尋引擎更強的驗證措施。 Prisma Access 具有支援的 MFA 廠商內建清單，且清單會隨著廠商的新增而自動更新： 
本機資料庫驗證	建立在 Prisma Access 本機執行、且包含使用者帳戶（使用者名稱和密碼或雜湊密碼）的資料庫。這種驗證方法適用於當您僅知道雜湊密碼而不知道純文字密碼時，重複使用現有 Unix 帳戶憑證建立使用者帳戶。對於使用純文字密碼的帳戶，您還可以定義密碼複雜性和過期設定。此驗證方法適用於透過驗證入口網站或 GlobalProtect 應用程式存取服務和應用程式的使用者。

驗證功能重點

SSO	如果您使用 SAML 或 Kerberos，則可以實作單一登入 (SSO)，讓使用者只需進行一次驗證即可存取多項服務和應用程式。SAML 和 Kerberos 支援 SSO。

 ©2025 Palo Alto Networks, Inc.

驗證入口網站	將符合驗證規則的 Web 要求重新導向至會顯示驗證提示的 Prisma Access 登入頁面。Prisma Access 會使用使用者提交至此驗證入口網站的資訊，建立或更新使用者名稱對應的 IP 位址。 這對於遠端網路特別有用，您可以繼續根據使用者（或群組）來監控及強制執行流量。當使用者起始符合驗證規則的 Web 流量（HTTP 或 HTTPS）時，Prisma Access 會提示使用者透過驗證入口網站進行驗證。Prisma Access 會根據使用者提交至入口網站的資訊來建立或更新 IP 位址與使用者名稱的對應。這可以確保您能確切得知誰正在遠端網站上存取最敏感的應用程式和資料。
驗證順序	如果您基於不同目的使用多種類型的驗證，您可以設定驗證順序對設定檔進行排名。Prisma Access 會根據您的排名檢查每個設定檔，直到成功驗證使用者為止。

驗證的運作方式

將組織的驗證服務新增至 Prisma Access 後（具體方法如下），Prisma Access 會在多個時間點驗證使用者：

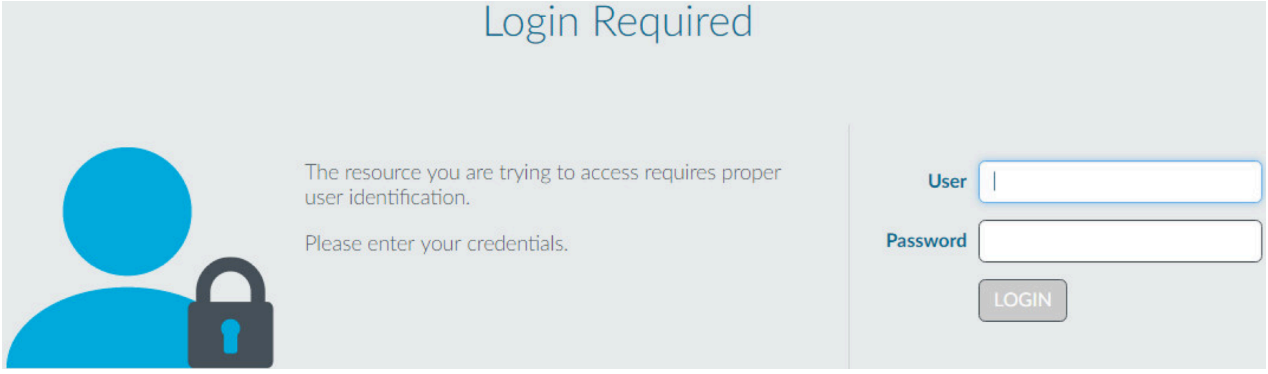
- 當他們連線至 **Prisma Access** 時

  以下說明如何定義您希望行動使用者對 Prisma Access 進行驗證的方法。您無須為遠端網路的使用者定義驗證設定即可連線至 Prisma Access，因為遠端網路流量是透過安全 VPN 通道進行路由的。

- 當使用者流量符合您額外驗證的需求時

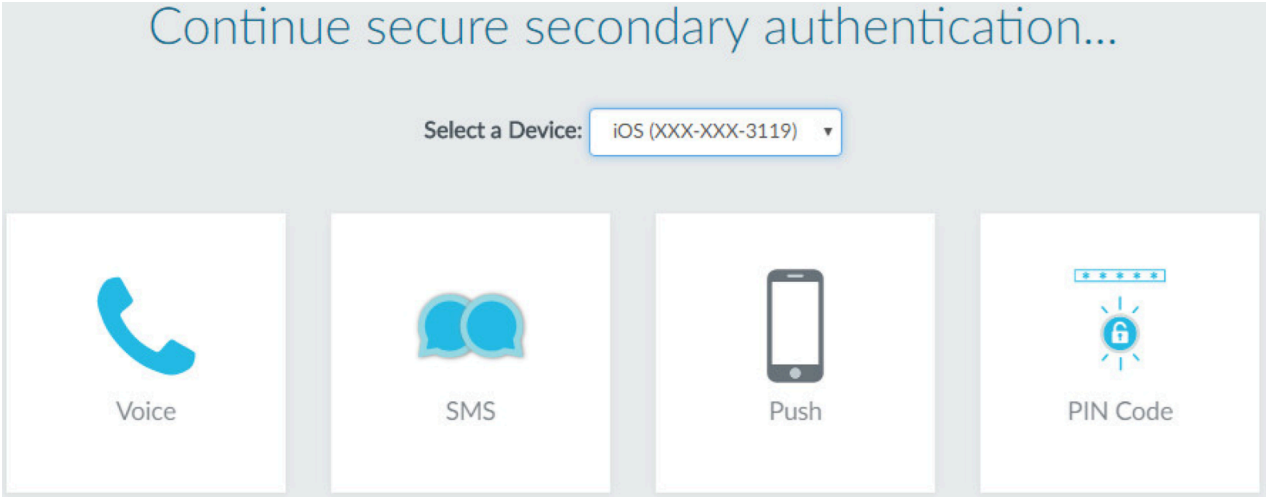
  以下說明如何要求使用者進行驗證（使用一或多種方法）以存取企業應用程式和受保護的網路資源。

當使用者產生與您的驗證需求相符的 Web 流量時，Prisma Access 會提示使用者使用一或多種方法（因素）進行驗證，以檢查使用者是否合法；這些因素包括登入名稱和密碼、語音、SMS、推播或一次性密碼 (OTP) 驗證（Prisma Access 所使用的因素完全取決於驗證服務和您在驗證設定檔中指定的設定）。對於第一個因素（登入名稱和密碼），使用者必須透過驗證入口網站進行驗證。



對於其他因素，使用者隨後應透過多因素驗證登入頁面進行驗證。

 ©2025 Palo Alto Networks, Inc.



驗證使用者之後，Prisma Access 會評估您的安全性規則，以確認是否要允許存取應用程式。Prisma Access 會記錄使用者嘗試存取您指定用於安全存取的應用程式、服務或資源的所有活動。

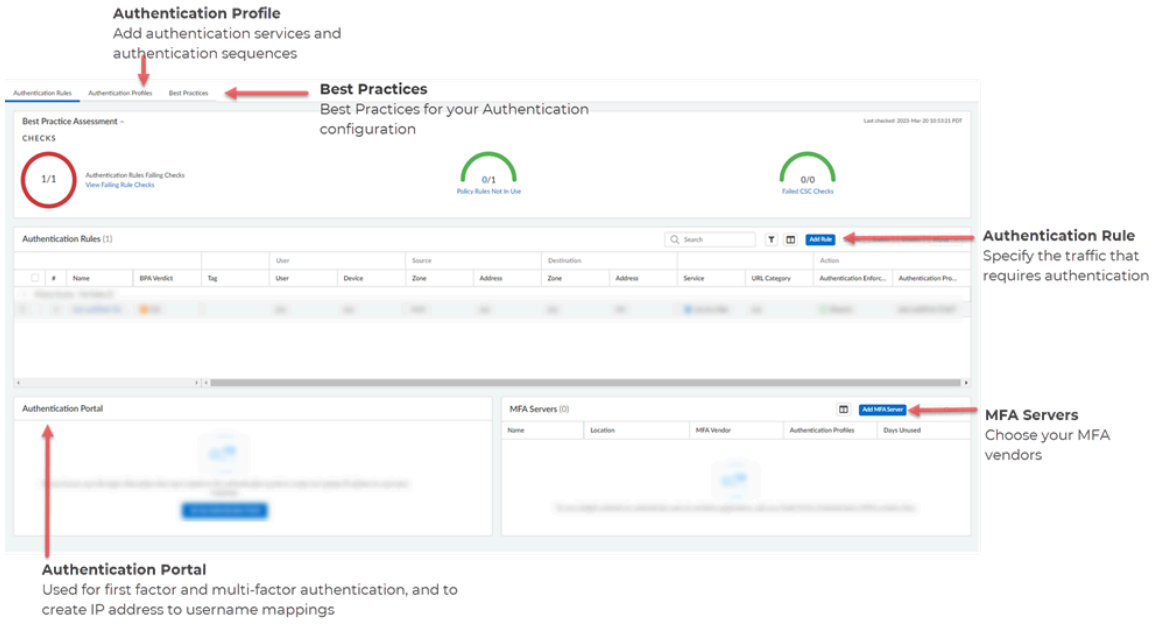
管理：驗證設定

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	其中一個： ❑ Prisma Access 授權 ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

若要在 Strata Cloud Manager 中設定 Prisma Access 的驗證，請先將您的驗證服務新增至 Prisma Access。然後，指定您認為需要驗證的流量。根據這些設定新增更多驗證功能，例如 MFA、驗證順序，或讓 Prisma Access 建立和更新 IP 位址與使用者名稱的對應。

以下說明如何開始使用 — 啟用 Prisma Access 驗證所需的所有設定都位於同一個位置：**Manage**（管理） > **Identity Services**（識別服務） > **Authentication**（驗證）。

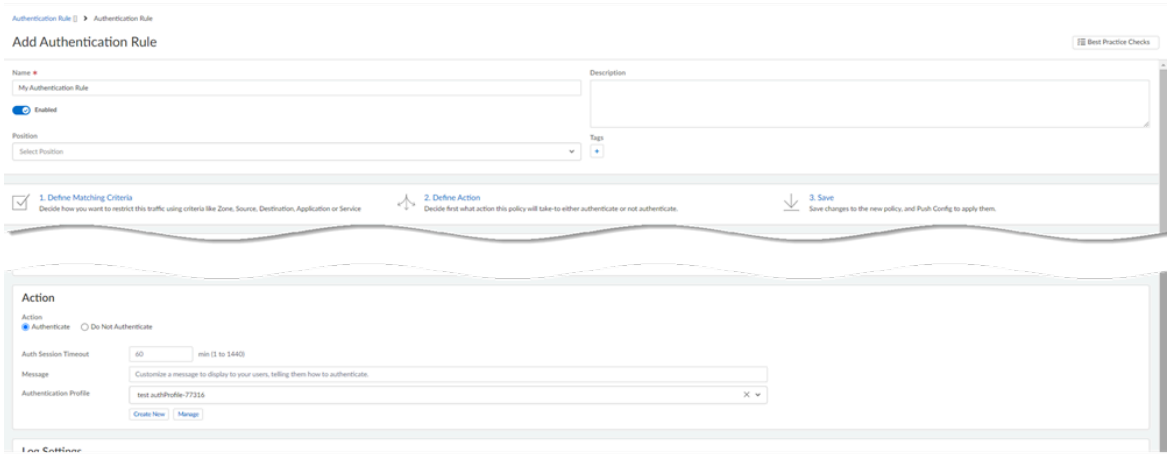
 ©2025 Palo Alto Networks, Inc.



驗證規則 您可以在此處指定需要驗證的流量

設定驗證規則的一部分，包括將驗證設定檔新增至規則。Prisma Access 在偵測到符合驗證規則的流量時，即會將定義於驗證設定檔中的驗證方法和設定套用至相符的流量。設定檔定義了使用者需要進行驗證的方式。

1. 移至**Manage**（管理） > **Identity and Access Services**（識別與存取服務） > **Authentication**（驗證） > **Authentication Rule**（驗證規則）和 **Add Authentication Rule**（新增驗證規則）。
2. 定義需要驗證的使用者、服務和 URL 類別。
3. 將規則動作設定為 **Authenticate**（驗證），然後選擇 **Profile**（設定檔）以定義符合此規則的流量所要使用的驗證方法。



 ©2025 Palo Alto Networks, Inc.

驗證設定檔 在此處新增您的驗證服務，並定義驗證設定

將 Prisma Access 連線至您要用來驗證使用者的服務（SAML、TACACS+、RADIUS、LDAP 或 Kerberos），並定義驗證設定（例如，設定失敗登入嘗試的限制）。

如果您使用內部部署驗證服務，則必須先建立服務連線，以將內部部署驗證服務連線至 *Prisma Access*。然後，返回此處設定您的驗證設定檔。

移至**Manage**（管理） > **Identity and Access Services**（識別與存取服務） > **Authentication**（驗證） > **Authentication Profile**（驗證設定檔） > **Add Profile**（新增設定檔），然後先設定設定檔 **Auth Type**（驗證類型）：

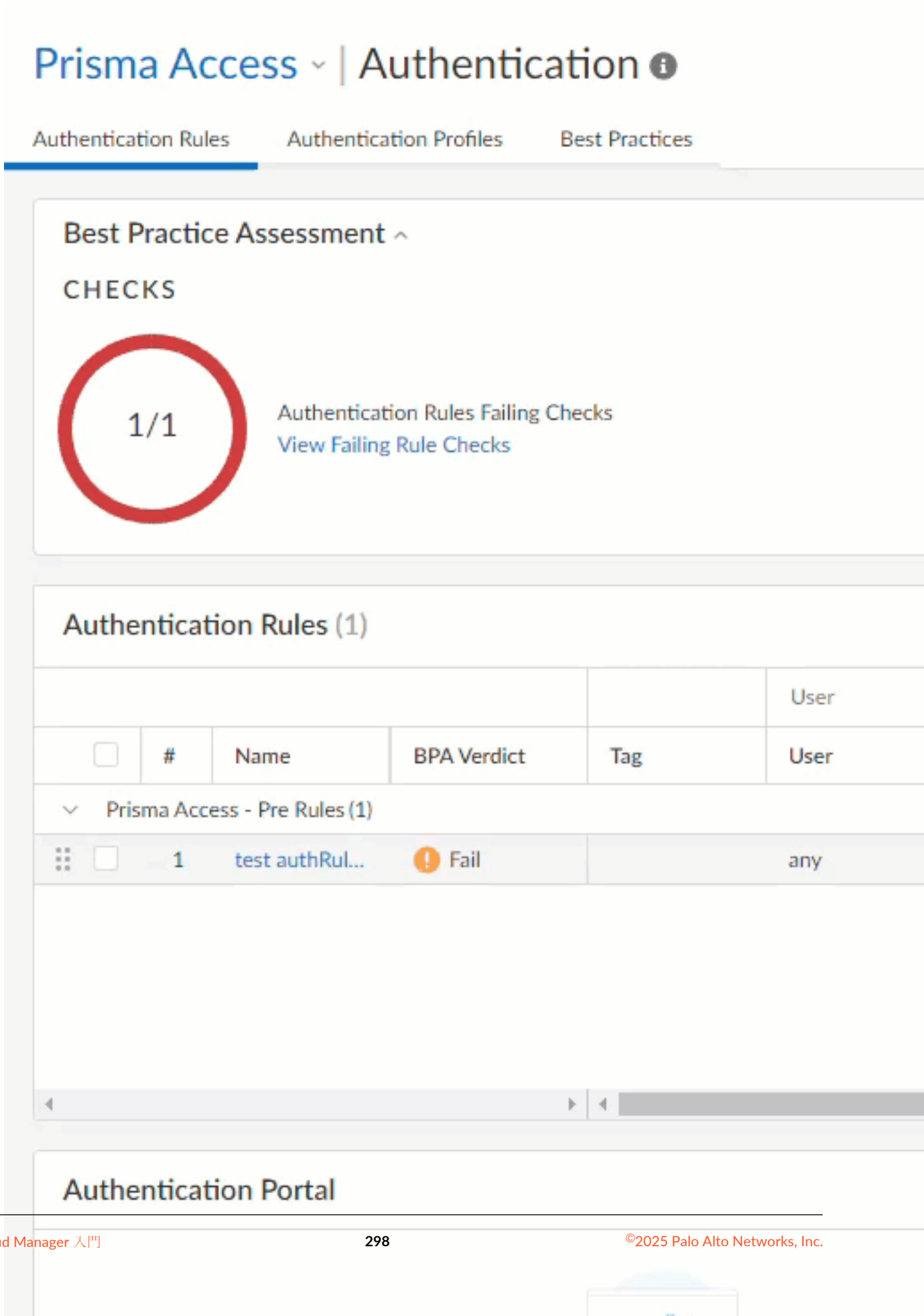
系統會提示您新增與您選擇的驗證服務有關的詳細資料，使 Prisma Access 能夠連線至該服務，以及讀取使用者認證和角色權限。設定檔中提供了用來自訂驗證的其他設定，具體可能會隨著您設定的驗證類型而有所不同。

 ©2025 Palo Alto Networks, Inc.

MFA 伺服器 指定您所使用的 MFA 廠商

若要使用多種方法對敏感的應用程式進行使用者驗證，請先新增您要使用的 MFA 廠商（**Add MFA Server**（新增 **MFA** 伺服器））。Prisma Access 有 MFA 廠商清單可供您選擇。

 ©2025 Palo Alto Networks, Inc.



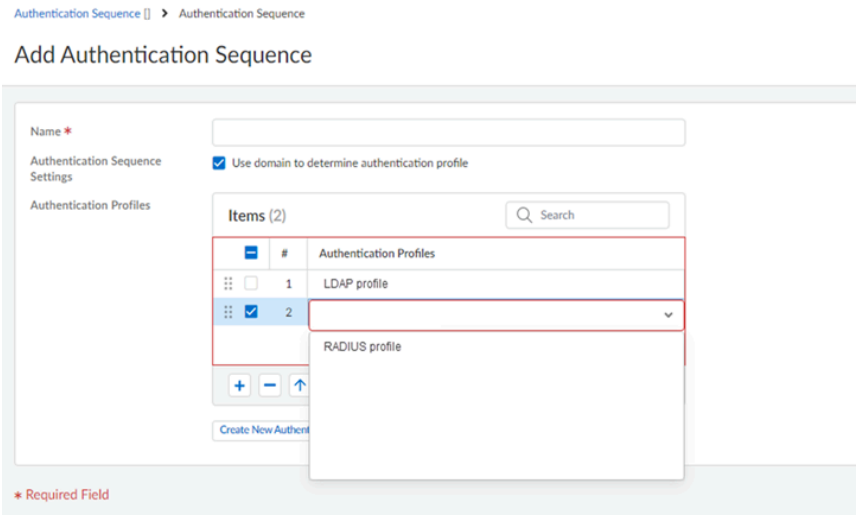
 ©2025 Palo Alto Networks, Inc.

驗證入口網站 為遠端網站的使用者設定驗證入口網站（也稱為被控制的入口網站），並且讓 Prisma Access 建立 IP 位址與使用者名稱的對應

對於第一因素驗證（登入名稱和密碼），遠端網站的使用者必須透過驗證入口網站進行驗證。如果驗證成功，Prisma Access 會針對所需的每個附加驗證因素顯示 MFA 登入頁面。Prisma Access 會使用使用者提交的認證來建立和更新 IP 位址與使用者名稱的對應。這意味著您隨時都知道誰正在遠端網站上存取 Web 內容和企業應用程式。

驗證順序 依照您希望 Prisma Access 嘗試的順序對驗證設定檔進行排名

選取**Manage**（管理） > **Identity and Access Services**（識別與存取服務） > **Authentication**（驗證） > **Authentication Profile**（驗證設定檔）和 **Add Authentication Sequence**（驗證順序），對驗證設定檔進行排名。Prisma Access 會依序檢查各項，直到成功驗證使用者為止。



管理：驗證設定檔

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	其中一個： ❑ Prisma Access 授權 ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

驗證設定檔定義了用於驗證以下管理員和使用者登入認證的驗證服務：存取防火牆 Web 介面的管理員和透過網頁認證或 GlobalProtect 存取應用程式的使用者。驗證設定檔也會定義選項，例如單一登入 (SSO)。

- Kerberos

 ©2025 Palo Alto Networks, Inc.

- 雲端識別引擎

雲端識別引擎

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 授權

雲端識別引擎 (CIE) 可為 Prisma Access — 明確 Proxy 部署中的行動使用者提供使用者識別和使用者驗證。雲端識別引擎可與明確 Proxy 驗證快取服務 (ACS) 整合，並使用 SAML 識別提供者 (IdP) 提供明確 Proxy 行動使用者的驗證。

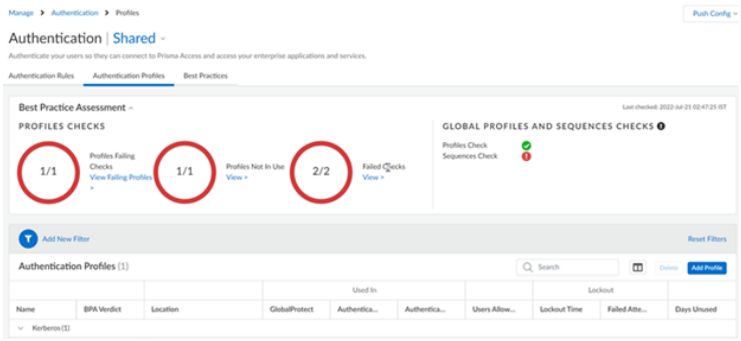
設定驗證設定檔，以使用雲端識別引擎對使用者進行驗證。

只有在雲端驗證服務 (CAS) 啟用時，才會顯示 SAML/CIE 驗證方法。如果您的 Prisma Access 租用戶不支援 CIE 驗證或 CAS，就只會顯示 SAML 驗證方法。

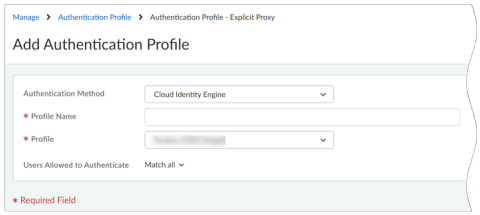
開始之前：

- 檢閱明確 Proxy 指導方針。
- 在雲端識別引擎中設定驗證設定檔。

STEP 1 | 移至**Manage**（管理） > **Configuration**（設定） > **Identity Services**（識別服務） > **Authentication**（驗證），在 **Authentication Profiles**（驗證設定檔）底下將設定範圍設為 **Explicit Proxy**（明確 **Proxy**）和 **Add Profile**（新增設定檔）。



STEP 2 | 選取 **Authentication Method**（驗證方法）：雲端識別引擎。



STEP 3 | 輸入唯一的 **Profile Name**（設定檔名稱）。

STEP 4 | 選取您在雲端識別引擎中設定的雲端識別引擎驗證設定檔。

STEP 5 | **Save**（儲存）變更。

 ©2025 Palo Alto Networks, Inc.

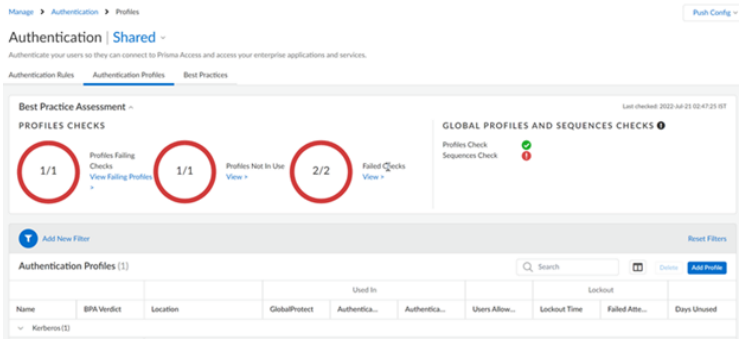
Kerberos

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 授權

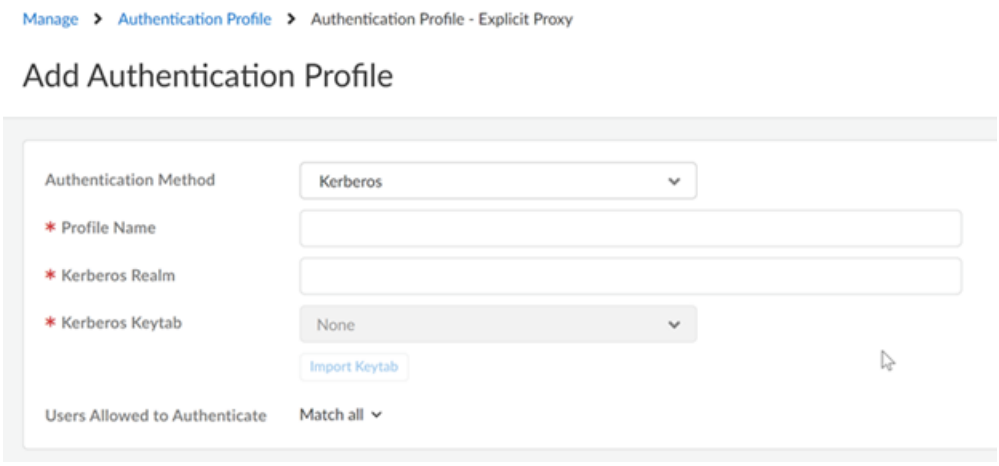
Erberos 是一電腦網路驗證通訊協定，可以使用票證允許節點透過非安全性網路通訊以安全的方式向彼此證明其識別。

驗證設定檔指定入口網站或閘道在驗證使用者時使用的伺服器設定檔。依照以下步驟，為明確 Proxy 行動使用者設定 Kerberos 驗證設定檔，以連線至 Prisma Access。

STEP 1 | 移至**Manage**（管理） > **Configuration**（設定） > **Identity Services**（識別服務） > **Authentication**（驗證） > **Authentication Profiles**（驗證設定檔）和 **Add Profile**（新增設定檔）。



STEP 2 | 選取 **Authentication Method**（驗證方法）：**Kerberos**。



STEP 3 | 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱）。驗證設定檔指定入口網站或閘道在驗證使用者時使用的伺服器設定檔。

STEP 4 | 輸入 **Kerberos Realm**（**Kerberos** 領域）（最多 127 個字元）以指定使用者登入名稱的主機名稱部分。例如，使用者帳戶名稱 user@EXAMPLE.LOCAL 具有領域 EXAMPLE.LOCAL。

 ©2025 Palo Alto Networks, Inc.

STEP 5 | 匯入包含 Kerberos 帳戶資訊的 **Kerberos** 金鑰標籤檔案。出現提示時，請瀏覽金鑰標籤檔案，然後按一下 **Save**（儲存）。驗證期間，端點首先會嘗試使用金鑰標籤建立 SSO。

STEP 6 | 選擇 **Kerberos Keytab**（**Kerberos** 金鑰標籤）。

STEP 7 | 按一下 **Save**（儲存）。

管理：雲端識別引擎

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

雲端識別引擎（目錄同步）為 Prisma Access 提供對 Active Directory 資訊的唯讀存取權，讓您能夠輕鬆設定及管理使用者和群組的安全性與解密政策。

雲端識別引擎可與內部部署 Active Directory 和 Azure Active Directory 搭配運作。

若要使用 Prisma Access 設定雲端識別引擎，請先移至中樞啟動雲端識別引擎，並將其新增至 Prisma Access。然後，移至 Prisma Access，驗證 Prisma Access 能夠存取目錄資料。

STEP 1 | 啟動雲端識別引擎

雲端識別引擎可以與中樞上任何支援的應用程式共用 Active Directory 資訊。它是免費的，且無需授權碼即可開始使用。雲端識別引擎設定包括在中樞啟動雲端識別引擎應用程式、設定雲端識別引擎代理程式以收集 Active Directory 對應，並設定雲端識別與代理程式之間的相互驗證。

請確實將雲端識別引擎執行個體部署在先前部署 Prisma Access 和 Strata Logging Service 的相同區域中。

STEP 2 | 為 Prisma Access 啟用雲端識別引擎。

您可以在首次啟動 Prisma Access 時或後續的任何時間，將 Prisma Access 與雲端識別引擎產生關聯：

- 當您啟動 **Prisma Access** 時：首次啟動 Cloud Managed Prisma Access 時，您可以選擇一個雲端識別引擎執行個體供 Prisma Access 使用。請確實選取與 Prisma Access 部署在相同區域中的執行個體。
- 在您啟動 **Prisma Access** 後：若要為現有的 Prisma Access 執行個體啟用雲端識別引擎，請登入中樞。從中樞設定下拉式清單（請參閱頂端功能表列上的齒輪）中，選取 **Manage**

 ©2025 Palo Alto Networks, Inc.

Apps（管理應用程式）。找出您要更新的 Prisma Access 執行個體，然後選取要讓 Prisma Access 使用的雲端識別引擎執行個體。

STEP 3 | 確認 Prisma Access 已連線至雲端識別引擎，且雲端識別引擎正在與 Prisma Access 共用目錄資訊。

- 檢查您是否可在 Prisma Access 中查看您的目錄。

  移至**Manage**（管理） > **Configuration**（設定） > **Identity Services**（識別服務） > **Cloud Identity Engine**（雲端識別引擎）：

- 驗證您可將使用者和群組新增至政策規則。

  選取 **Manage**（管理） > **Security Services**（安全服務） > **Security**（安全性）或 **Decryption**（解密）。在安全性或解密政策規則中，確認 **Users**（使用者）下拉式清單顯示了您的 Active Directory 使用者和群組項目。現在，您可以開始將這些使用者和群組新增至安全性和解密政策規則。

  對未按預期強制執行的流量進行疑難排解 - 檢查特定防火牆的狀態，以瞭解預期的政策（按設定）與強制執行的政策之間是否不相符。

管理：識別重新散佈

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

使用 Strata Cloud Manager 設定及管理 NGFW 和 Prisma Access 的識別重新散佈。

- Prisma Access
- NGFW

識別重新散佈 (Prisma Access)

為了讓您能夠一致地強制執行安全性政策，Prisma Access 會共用 GlobalProtect 在您整個 Prisma Access 環境中本機探索的識別資料。Prisma Access 也可以與遠端網站或服務連線站台（HQ 和資料中心）的內部部署裝置共用識別資料。

對於 Prisma Access 雲端管理，我們預設啟用了某種程度的識別資料重新散佈，對其餘部分，我們則經由設定簡化了重新散佈的流程（只需選取核取方塊來選取要共用的資料即可）。

 ©2025 Palo Alto Networks, Inc.

在 [Identity Distribution（識別散佈）] 儀表板中，您可以查看識別資料的共用方式，以及管理資料重新散佈：**Manage**（管理） > **Configuration**（設定） > **Identity Services**（識別服務） > **Identity Redistribution**（識別重新散佈）。

您可以重新散佈的識別資料包括：

- HIP 資料
- IP 位址到標籤的對應
- IP 位址到使用者的對應
- 使用者到標籤的對應
- 隔離裝置

開始進行識別重新散佈

識別重新散佈的運作方式

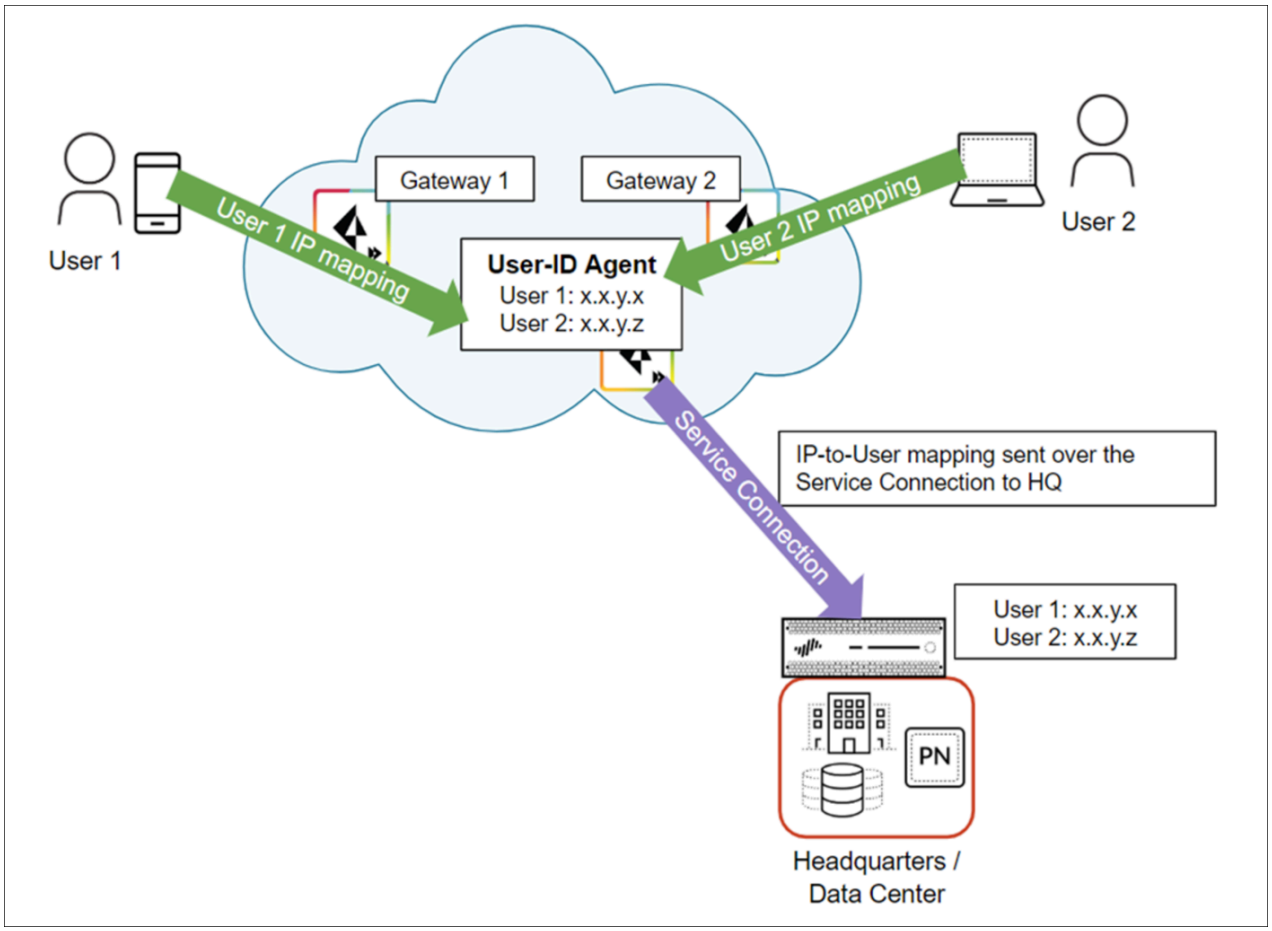
若要讓行動使用者存取遠端網路位置或 HQ/資料中心上的資源，而這些位置受到裝置的使用者行政策保護，這時您就必須將 Prisma Access 行動使用者和遠端網路使用者的識別資料重新散佈至該內部部署裝置。

當使用者連線至 Prisma Access 時，Prisma Access 會收集使用者的識別資料並加以儲存。

下列範例說明在 Prisma Access 中具有現有「IP 位址到使用者名稱」對應的兩個行動使用者。Prisma Access 隨後會讓服務連線至保護 HQ/資料中心的內部部署裝置，藉以重新散佈此對應。

Prisma Access 雲端管理會自動啟用服務連線，作為識別重新散佈代理程式（也稱為 User-ID 代理程式）。

 ©2025 Palo Alto Networks, Inc.



設定識別重新散佈

確認您的服務連線設定

如果您尚未為 HQ 或資料中心設定服務連線，請先設定服務連線。必須要有服務連線，Prisma Access 才能在您的環境中共用識別資料；Prisma Access 會自動啟用服務連線，作為重新散佈代理程式。當您看到新建立的服務連線站台已被指派 User-ID 代理程式位址時，該站台即可作為重新散佈代理程式（Prisma Access 會自動執行此動作，且只需要幾分鐘）。移至**Manage**（管理） > **Configuration**（設定） > **Identity Services**（識別服務） > **Identity Redistribution**（識別重新散佈），並將設定範圍設定為 **Service Connections**（服務連線），以驗證服務連線 User-ID 代理程式詳細資料。

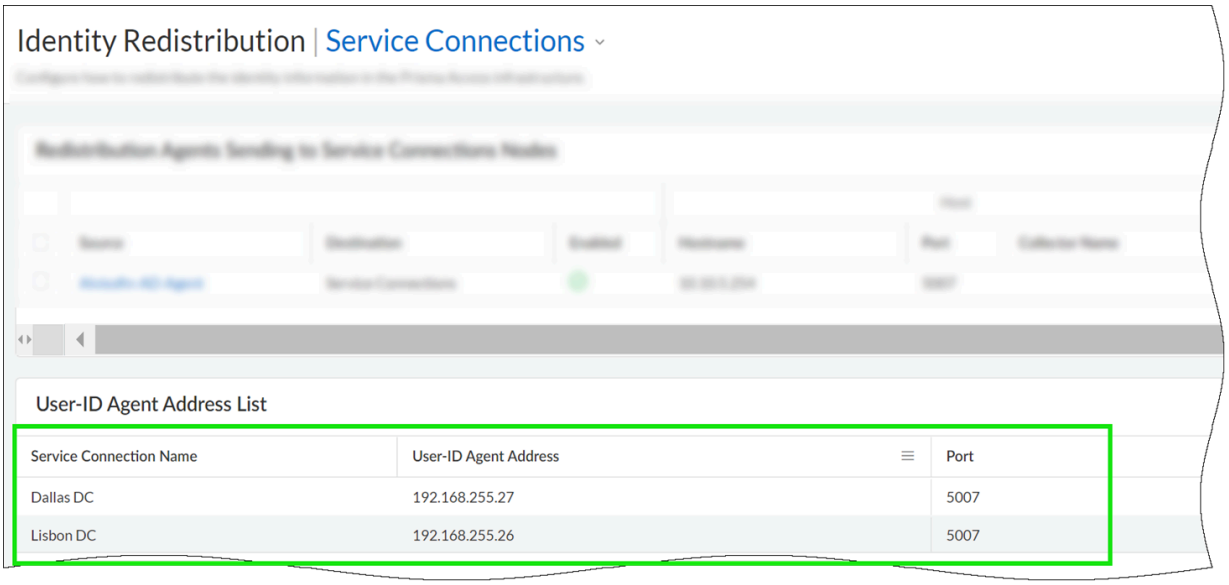
 ©2025 Palo Alto Networks, Inc.

將識別資料從 Prisma Access 傳送至內部部署裝置

您只需設定服務連線的 User-ID 代理程式資訊，即可將 Prisma Access 設定為將識別資料散佈至內部部署裝置。

移至**Manage**（管理） > **Configuration**（設定） > **Identity Services**（識別服務） > **Identity Redistribution**（識別重新散佈），並將設定範圍設定為 **Service Connections**（服務連線），以取得服務連線 User-ID 代理程式詳細資料。

使用這些詳細資料，將 Prisma Access 設定為 Panorama 或新世代防火牆上的資料重新散佈代理程式。



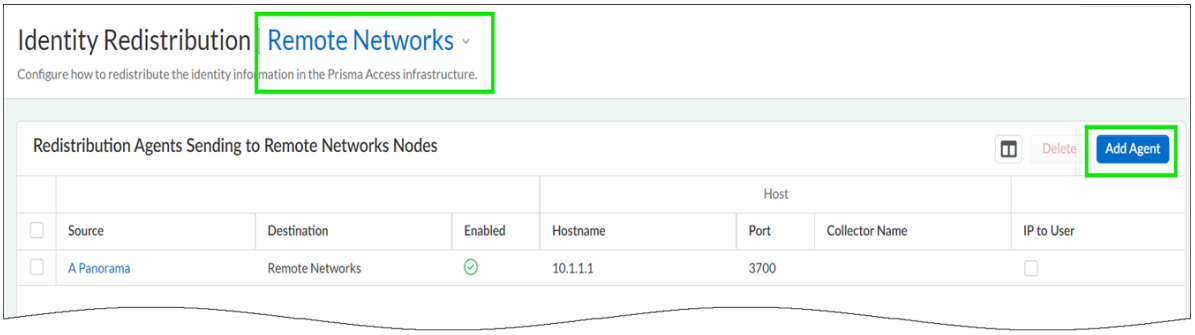
 ©2025 Palo Alto Networks, Inc.

將識別資料從內部部署裝置傳送至 Prisma Access

將內部部署裝置新增至 Prisma Access 作為重新散佈代理程式；您新增的裝置將能夠將識別資料散佈至 Prisma Access。

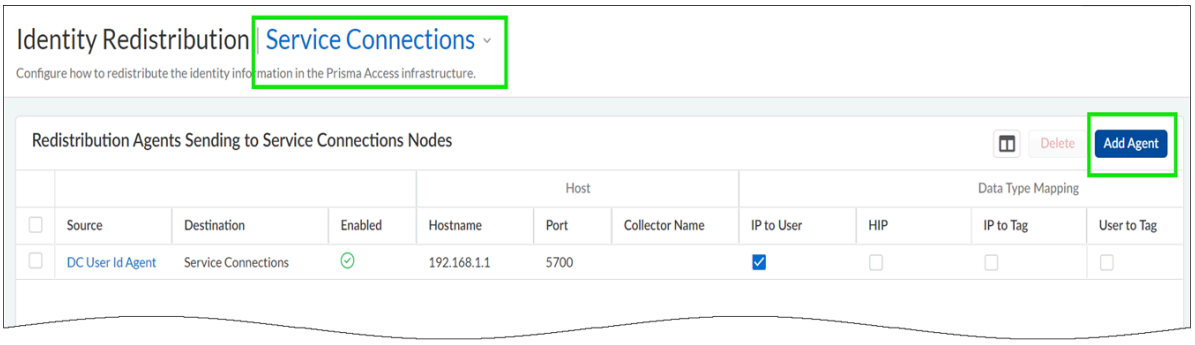
- 從遠端網站上的裝置：

  移至 **Identity Redistribution**（識別重新散佈）儀表板，將設定範圍設定為 **Remote Networks**（遠端網路），然後新增代理程式。除了指定主機詳細資料以外，也請選取裝置與 Prisma Access 共用的資料類型。選用設定包括裝置的名稱和預先共用金鑰。



- 從服務連線站台上的裝置：

  移至 **Identity Redistribution**（識別重新散佈）儀表板，將設定範圍設定為 **Service Connections**（服務連線），然後新增代理程式。除了指定主機詳細資料以外，也請選取裝置與 Prisma Access 共用的資料類型。選用設定包括裝置的名稱和預先共用金鑰。



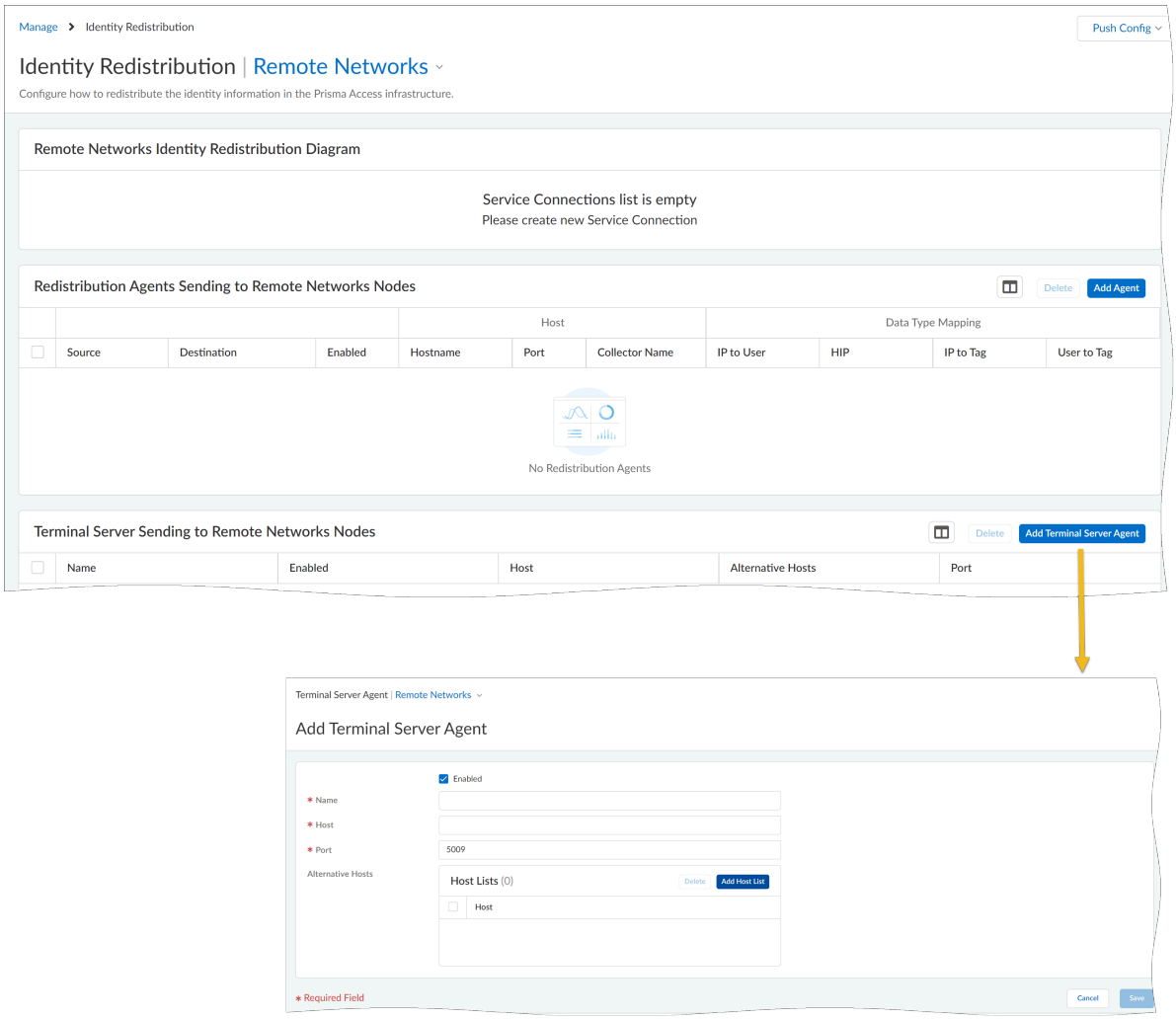
 ©2025 Palo Alto Networks, Inc.

為使用者對應設定終端伺服器代理程式

終端伺服器 (TS) 代理程式會為每個使用者指派一個連接埠範圍，以識別 Windows 型終端伺服器上的特定使用者。TS 代理程式會向 Prisma Access 指出已配置的連接埠範圍，讓 Prisma Access 能夠根據使用者和使用者群組強制執行政策。

在 **Identity Redistribution**（識別重新散佈）儀表板上，將設定範圍設定為 **Remote Networks**（遠端網路），並在 **Terminal Server Sending to Remote Networks Nodes**（傳送至遠端網路節點的終端伺服器）底下新增終端伺服器代理程式。

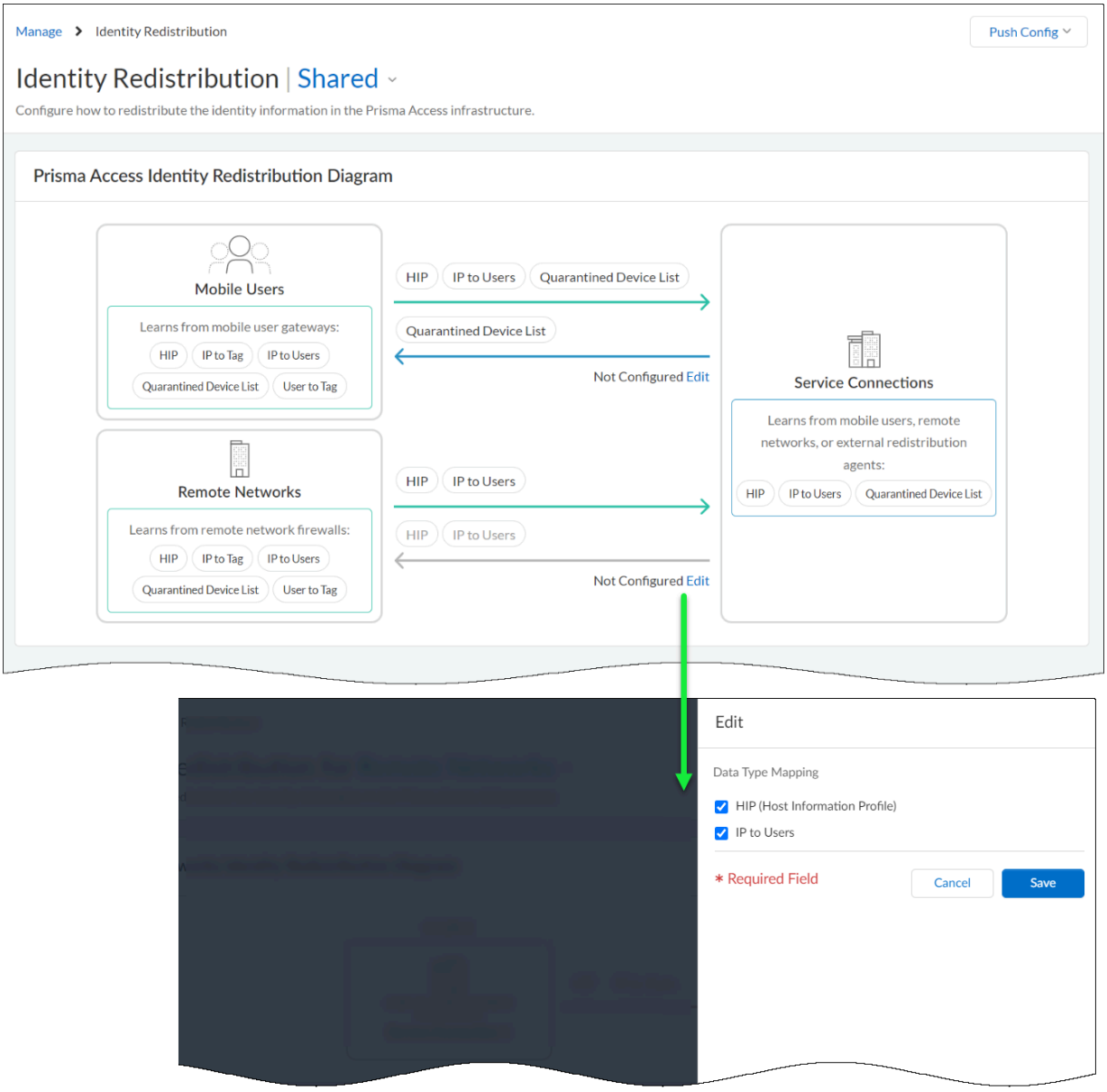
- 依預設會啟用該設定。
- 輸入 TS 代理程式的名稱。
- 輸入安裝 TS 代理程式之 Windows 主機的 IP 位址。
- 輸入代理程式用來接聽使用者識別要求的連接埠號碼。此連接埠預設為 5009。
- **Save**（儲存）變更。



 ©2025 Palo Alto Networks, Inc.

在 Prisma Access 環境中散佈識別資料

在 **Identity Redistribution**（識別重新散佈）儀表板上，編輯圖表以指定您要從每個來源收集，並在 Prisma Access 中共用的識別資料。



若要啟動您的變更，請將設定推送至 Prisma Access。

識別重新散佈 (NGFW)

在大型網路中，您可以設定部分防火牆透過重新散佈來收集對應資訊，藉以簡化資源使用，而不必設定所有防火牆直接查詢對應資訊來源。資料重新散佈還會提供細微性，允許您僅將指定的資訊類型重新散佈給選取的裝置。您還可以使用子網路和範圍篩選 IP 使用者對應或 IP 標籤對應，以確保防火牆僅收集強制執行政策規則所需的對應。

要重新散佈資料，可以使用以下架構類型：

 ©2025 Palo Alto Networks, Inc.

- 用於單個區域的中樞和支點架構：

  要在防火牆之間重新散佈資料，最佳做法是使用中樞和支點架構。在此設定中，中樞防火牆從 Windows User-ID 代理程式、syslog 伺服器、網域控制站或其他防火牆等來源收集資料。設定重新散佈用戶端防火牆以從中樞防火牆收集資料。

- 用於多個區域的多中樞和支點架構：

  如果您在多個區域部署了防火牆，且希望將資料散佈到所有這些區域的防火牆，以便無論使用者在哪裡登入，都可以一致地強制執行政策規則，則可以對多個區域使用多中樞和支點架構。

- 階層式架構：

  要重新散佈資料，您還可以使用階層式架構。例如，要重新散佈 User-ID 資訊之類的資料，可以分層組織重新散佈順序，其中每層具有一個或多個防火牆。在底層中，整合了 PAN-OS 的 User-ID 代理程式在防火牆上執行，基於 Windows 的 User-ID 代理程式將在對應 IP 位址到使用者名稱的 Windows 伺服器上執行。每個較高層都有防火牆從下方一層中最多 100 個 從新分配點接收對應資訊和驗證時間戳記。頂層防火牆將彙總來自於所有層的對應資訊和時間戳記。此部署提供了相關選項，為所有使用者（在頂層的防火牆中）設定政策規則，並為對應網域（有較低層防火牆提供伺服）中的使用者子集設定區域或功能特定的政策規則。

當流量的強制執行不符合預期時，請使用疑難排解來檢查特定防火牆的資料平面狀態，以瞭解預期的政策（按設定）與強制執行的政策之間是否不相符。

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 確定您的 Strata Cloud Manager 部署符合設定識別重新散佈的需求。

1. 為您的 Strata Cloud Manager 租用戶設定並啟動雲端識別引擎 (CIE)。

   這是使用識別重新散佈的必要條件。

   1. 啟動雲端識別引擎。
   2. 設定雲端識別引擎。

2. 選取**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（物件） > **Address Groups**（位址群組），並新增具有必要「IP 位址-標籤」對應的動態位址群組。

   針對位址群組類型，選取 **Dynamic**（動態）。視需要設定動態位址群組並儲存。

3. 選取**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（物件） > **Dynamic User Groups**（動態使用者群組），並新增具有必要「使用者名稱-標籤」對應的動態位址群組。

   視需要設定動態使用者群組並儲存。

STEP 3 | 選取**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Identity Services**（識別服務） > **Identity Redistribution**（識別重新散佈），然後選取要設定識別重新散佈的設定範圍。

您可以從 **Folders**（資料夾）中選取資料夾或防火牆，或選取 **Snippets**（片段）以在片段中設定識別重新散佈。

STEP 4 | 新增代理程式。

 ©2025 Palo Alto Networks, Inc.

STEP 5 | 輸入代理程式的描述性名稱。

STEP 6 | 輸入主機 IP 位址。

STEP 7 | 輸入 **Port**（連接埠）（範圍為 1-65535）。

STEP 8 | 選取 **Data Type Mapping**（資料類型對應）。

- **IP** 到使用者 — User-ID 的 IP 位址至使用者名稱對應。
- 主機資訊設定檔 **(HIP)** — 動態位址群組的 IP 位址到標籤對應。
- **IP** 到標籤 — 動態使用者群組的使用者名稱到標籤對應。
- 使用者到標籤 — 來自 GlobalProtect 的 HIP 資料，其中包括 HIP 物件和設定檔。
- 隔離裝置清單 — GlobalProtect 識別為隔離的裝置。

STEP 9 | **Save**（儲存）。

STEP 10 | （僅限 NGFW 的雲端管理）為防火牆啟用識別重新散佈。

1. 選取**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Device Settings**（裝置設定） > **Device Setup**（裝置設定） > **Management**（管理），然後選取 **Customize**（自訂），以設定 **uid-agent** 服務的服務路由。

   選取您要在其中建立服務路由的設定範圍。您可以從 **Folders**（資料夾）中選取資料夾或防火牆，或選取 **Snippets**（片段）以在片段中設定服務路由。
2. 允許防火牆在其他防火牆查詢要重新散佈的資料時回應。
   1. 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Device Settings**（裝置設定） > **Device Setup**（裝置設定） > **Management**（管理），然後啟用 **User-ID** 網路服務。
   2. 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Device Settings**（裝置設定） > **Interfaces**（介面），以建立或選取第三層介面。

      展開 **Advanced Settings**（進階設定）。在 **Other**（其他）中建立或編輯管理設定檔，以啟用 **User-ID**。

      - 選取

STEP 11 | Push Config（推送設定）。

管理：本機使用者和群組

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW，包括由軟體 NGFW 積分資助的項目	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium

 ©2025 Palo Alto Networks, Inc.

這可在何處使用？	我需要哪些內容？
	❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

將管理員和一般使用者的驗證資訊儲存在本機。您可以儲存使用 GlobalProtect 或驗證入口網站進行驗證的管理員和一般使用者的驗證資訊。

若要設定本機資料庫驗證，您可以建立在防火牆本機執行，並且包含使用者帳戶（使用者名稱和密碼或雜湊密碼）的資料庫。您可以設定屬於防火牆本機的使用者資料庫，驗證存取防火牆 Web 介面的管理員以及驗證透過驗證入口網站或 GlobalProtect 存取應用程式的一般使用者。

本機資料庫驗證可以與驗證設定檔相關聯，因此能夠因應不同組的使用者需要不同驗證設定的部署，例如 Kerberos 單一登入 (SSO) 或多因素驗證 (MFA)。對於使用驗證設定檔的管理員帳戶，不會套用密碼複雜性和到期設定。此驗證方法適用於存取防火牆的管理員，以及透過驗證入口網站或 GlobalProtect 存取服務和應用程式的一般使用者。

移至**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Identity Services**（識別服務） > **Local Users & Groups**（本機使用者與群組），開始收集驗證資料。。

建立本機使用者

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Identity Services**（識別服務） > **Local Users & Groups**（本機使用者與群組） > **Local Users**（本機使用者），然後選取要建立本機使用者的設定範圍。

您可以從 **Folders**（資料夾）中選取資料夾或防火牆，或選取 **Snippets**（片段）以在片段中設定本機使用者。

STEP 3 | 新增本機使用者。

STEP 4 | 輸入使用者名稱。

STEP 5 | 確認本機使用者已啟用。

您可以藉由取消勾選（停用）讓使用者不再啟用驗證，而不是從驗證的本機防火牆資料庫中刪除本機使用者。

STEP 6 | 輸入 **Password**（密碼）和 **Confirm Password**（確認密碼）。

STEP 7 | **Save**（儲存）。

STEP 8 | 推送設定。

 ©2025 Palo Alto Networks, Inc.

建立本機使用者群組

將多個本機使用者分組為單一本機群組，以將群組資訊新增至本機防火牆資料庫。您可以建立本機使用者群組，以管理多個具有相同驗證需求的本機使用者。

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Identity Services**（識別服務） > **Local Users & Groups**（本機使用者與群組） > **Local User Groups**（本機使用者群組），然後選取要建立本機使用者群組的設定範圍。

您可以從 **Folders**（資料夾）中選取資料夾或防火牆，或選取 **Snippets**（片段）以在片段中設定本機使用者群組。

STEP 3 | 新增本機使用者群組。

STEP 4 | 輸入本機使用者群組名稱。

STEP 5 | 新增您在先前的步驟中建立的本機使用者。

STEP 6 | **Save**（儲存）。

STEP 7 | 推送設定。

 ©2025 Palo Alto Networks, Inc.

管理：裝置設定

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium或Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

在 **Device Settings**（裝置設定）中，您可以為雲端管理的防火牆設定下列設定：

setting	說明
介面	設定介面，讓您的防火牆可同時在多個部署中運作。 在 **Ethernet**（乙太網路）頁籤上，使用 **Show local device configs**（顯示本機裝置設定）來檢視本機防火牆和 Strata Cloud Manager 上顯示的各種設定。
路由	為您的防火牆設定路由設定檔、邏輯路由器和靜態路由。
IPSec 通道	設定 IPsec 通道，以在 IP 封包經過通道時加以驗證和加密。
DHCP	設定 DHCP 以提供 TCP/IP 與連結層設定參數，並提供網路位址以便在 TCP/IP 網路上動態設定主機。
地區	設定區域，將您的網路分成功能和組織區域，以縮小攻擊面。
DNS Proxy	設定 DNS Proxy，將防火牆設定為 DNS 用戶端與伺服器之間的中介。
裝置設定	設定裝置，以針對防火牆的管理和輔助介面設定服務路由、連線設定、允許的服務，以及管理存取設定。
Proxy	設定 Web Proxy，以將 Proxy 和防火牆功能整合到單一裝置中。 *Strata Cloud Manager* 的 *Web Proxy* 需要傳統路由器堆疊。如果您希望啟用此功能，請聯繫您的帳戶團隊。

©2025 Palo Alto Networks, Inc.

setting	說明
Virtual Wire	設定虛擬介接，將防火牆介面整合到拓撲中，使防火牆上的兩個連線的介面無須執行任何切換或路由。
GlobalProtect	啟用雲端管理的 NGFW 作為 GlobalProtect 閘道和入口網站，以便為各地的使用者提供彈性、安全的遠端存取。

©2025 Palo Alto Networks, Inc.

管理：全域設定

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	其中一個： ❑ Prisma Access 授權 ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

在 Strata Cloud Manager 中檢閱和設定全域設定 **(Manage**（管理） **> Configuration**（設定） **> NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） **> Global Settings**（全域設定）**)**

object	說明
SaaS 應用程式管理	集中管理您的每個 SaaS 應用程式。SaaS 應用程式管理可讓您找到適當功能，用來安全地為您的企業啟用應用程式。
使用者輔導通知範本	集中管理一般使用者通知範本，以在使用者產生 Enterprise Data Loss Prevention (E-DLP) 事件（系統檢查到包含敏感資料的流量並加以封鎖）時，透過 AI-Powered ADEM 對使用者發出警示。
自動 VPN	手動設定網路裝置和建立 VPN 通道是繁瑣的過程，且容易發生設定錯誤。自動 VPN 可自動在網路裝置之間建立 VPN 通道。自動 VPN 可讓您建立 VPN 叢集以連接多個區域網路 (LAN)。SD-WAN 與自動 VPN 搭配運作，可讓您輕鬆部署及管理 SD-WAN 部署。

使用者輔導通知範本

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager)	❑ GlobalProtect app 6.3 版或更新版本 ❑ Enterprise Data Loss Prevention (E-DLP) 授權 ❑ Prisma Access 行動使用者授權 ❑ Prisma Access 授權

 ©2025 Palo Alto Networks, Inc.

這可在何處使用？	我需要哪些內容？
	或下列任何包含 Enterprise DLP 授權的授權 ❑ Prisma Access CASB 授權 ❑ Next-Generation CASB for Prisma Access and NGFW (CASB-X) 授權

一般使用者輔導通知範本可讓您設定在使用者產生 Enterprise Data Loss Prevention (E-DLP) 事件時會在存取體驗使用者介面 (UI) 中對使用者顯示的通知。當下載或上傳的檔案包含敏感資料時，或包含敏感資料的非檔案型流量發布於 Web 表單時，就會產生 Enterprise DLP 事件。

若要確認哪些資料會被視為敏感資料，請新增一或多個內嵌 **DLP** 規則。DLP 規則包含的流量比對準則會定義哪種資料會被視為敏感資料。DLP 規則是從相同名稱的 Enterprise DLP 資料設定檔衍生出來的。此外，您可以設定在檔案型或非檔案型 Enterprise DLP 事件產生時的自訂訊息。Enterprise DLP 事件產生後，產生事件的使用者可以檢視資料安全性通知，以進一步瞭解上傳、下載或發佈的敏感資料。

無論使用者產生相同事件的次數為何，每個事件在 30 秒內只會顯示一則通知。例如，假設某使用者嘗試將包含敏感資料的檔案上傳至 Box Web 應用程式，而 Enterprise Data Loss Prevention (E-DLP) 封鎖了上傳。使用者隨即又嘗試上傳同一個檔案 5 次，但每次都遭到封鎖。在此案例中，即便使用者在將包含敏感資料的檔案上傳至 Box Web 應用程式時遭到封鎖共 6 次，也只會產生一個「存取體驗」警示。

STEP 1 | 聯絡您的 Palo Alto Networks 代表，在租用戶上啟用一般使用者輔導。

STEP 2 | 在 Windows 或 macOS 上安裝 GlobalProtect app 6.3 版或更新版本。

STEP 3 | 登入 Strata Cloud Manager。

STEP 4 | 啟用 Autonomous DEM。

在 Strata Cloud Manager 上，選取**Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **GlobalProtect** > **GlobalProtect App**（**GlobalProtect** 應用程式）和 **Add App Settings**（新增應用程式設定）。您必須設定這些必要設定，才能在使用者產生 DLP 事件時透過「存取體驗 UI」對使用者顯示通知。

- 啟用自發 **DEM** 和 **GlobalProtect** 日誌收集進行以疑難排解
- **DEM for Prisma Access**（僅限 **Windows** 和 **Mac**） - 選取 **Install and User Cannot Enable or Disable DEM**（安裝後使用者無法啟用或停用 **DEM**）
- **DEM for Prisma Access 6.3** 版及更高版本（僅限 **Windows** 和 **Mac**） - 選取 **Install the Agent**（安裝代理程式）

STEP 5 | （僅限 macOS）在「存取體驗 UI」中，選取**Settings**（設定） > **Notifications**（通知），然後啟用 **Allow notifications**（允許通知）。

此設定必須在「存取體驗 UI」中為每個使用者啟用，且必須在使用者桌面上顯示通知。視需要設定其他「存取體驗」通知設定。

 ©2025 Palo Alto Networks, Inc.

STEP 6 | 設定 Enterprise DLP。

1. 建立解密設定檔和政策規則。

   這是 Enterprise DLP 解密和檢查流量中的敏感資料所需的條件。

2. 建立自訂資料模式，以定義您的比對準則。

   或者，您可以使用預先定義的資料模式，而不要建立自訂資料模式。

3. 建立資料設定檔並新增您的資料模式。

   僅支援自訂資料設定檔。根據預設，所有預先定義 DLP 規則的 **Action**（動作）都會設定為 **Alert**（警示）。如果您必須複製預先定義的資料設定檔，請編輯 DLP 規則動作。

4. 修改 DLP 規則。

   - 修改 DLP 規則時，您必須將 **Action**（動作）設定為 **Block**（封鎖）。必須在「存取體驗 UI」中產生警示。如果 **Action**（動作）設定為 **Alert**（警示），則不會顯示警示。
   - 將 DLP 規則新增至設定檔群組，並將設定檔群組連結至安全性政策規則。若要讓 Enterprise DLP 產生 DLP 事件，繼而在「存取體驗 UI」中產生通知，則需執行此動作。

STEP 7 | 選取**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Global Settings**（全域設定） > **User Coaching Notification Template**（使用者輔導通知範本）和 **Add Notification Template**（新增通知範本）。

 ©2025 Palo Alto Networks, Inc.

STEP 8 | 設定 **General Information**（一般資訊）。

1. 確認 **Product Name**（產品名稱）是內嵌 **DLP**。

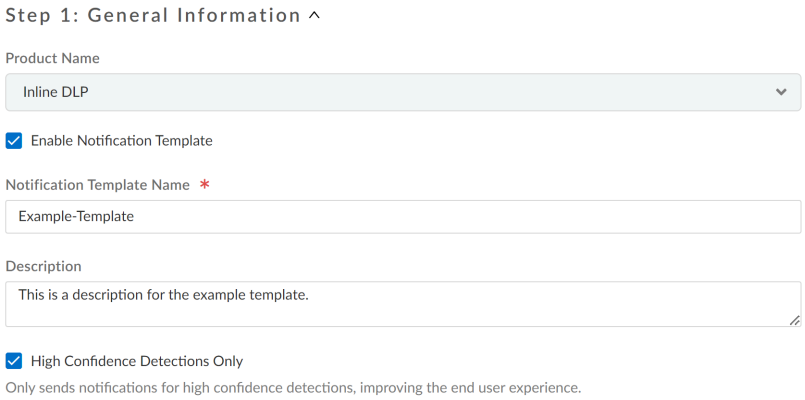
   這是預設設定，無法變更

2. 選取 **Enable Notification Template**（啟用通知範本），以在您儲存後啟用範本。

   此設定預設為啟用。

3. 輸入描述性的 **Notification Template Name**（通知範本名稱）。
4. (選用) 輸入通知範本的說明。
5. (選用) 選取 **High Confidence Detections Only**（僅限高信賴度偵測），僅針對高信賴度流量比對產生存取體驗警示。

   高信賴度比對會反映 Enterprise DLP 在偵測相符流量時的信賴度。對於規則運算式 (regex) 模式，其基準為與設定的鄰近關鍵字間隔的字元距離。對於機器學習 (ML) 模式，此信賴等級由 ML 模型所計算。



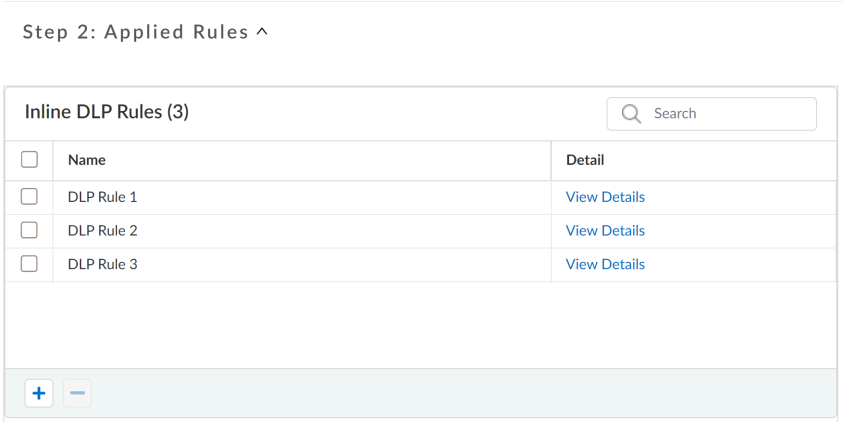
STEP 9 | 將一或多個 **Applied Rules**（套用的規則）新增至通知範本。

DLP 規則必須將 **Action**（動作）規則設定為 **Block**（封鎖），並新增到連結至安全性政策規則的設定檔群組，才能產生存取體驗通知。必須將 DLP 規則新增至設定檔群組，且該群組必須與

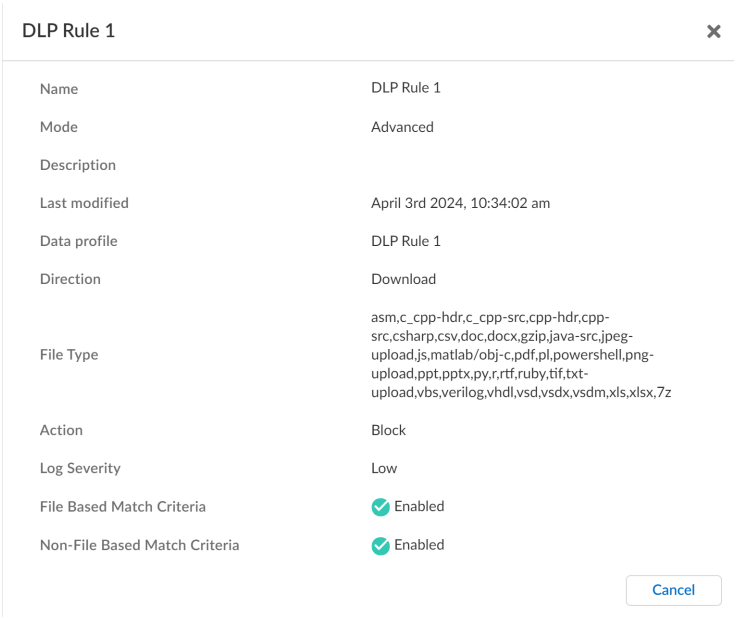
 ©2025 Palo Alto Networks, Inc.

安全性政策規則相關聯。若要讓 Enterprise DLP 產生 DLP 事件，繼而在「存取體驗 UI」中產生通知，則需執行此動作。一個 DLP 規則可新增至多個使用者輔導通知範本。

當 Enterprise DLP 封鎖與 DLP 規則的相關資料設定檔相符的敏感資料時，所有新增至通知範本的 DLP 規則將會產生相同的通知訊息。



您可以對您新增的每個 DLP 規則檢視詳細資料，以檢閱特定的檢查詳細資料。這包括流量檢查方向、適用的檔案類型、動作，以及 DLP 規則是檢查檔案型比對準則還是非檔案型比對準則，或兩者都檢查。



 ©2025 Palo Alto Networks, Inc.

STEP 10 | 定義使用者在 Enterprise DLP 封鎖與 DLP 規則的相關資料設定檔相符的敏感資料時所收到的通知訊息。

訊息範本是使用者在 Enterprise DLP 封鎖敏感資料時所收到的「存取體驗」快顯通知。您可以在訊息範本中使用下列變數。每個變數都必須加上括號。

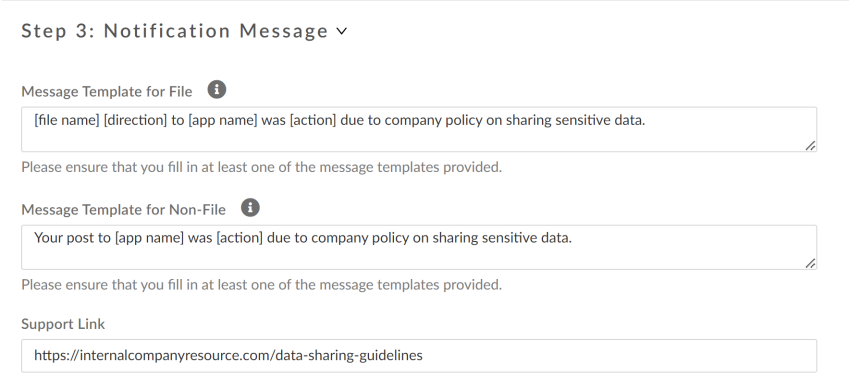
- **[**檔案名稱**]** — 包含敏感資料遭到 Enterprise DLP 封鎖的檔案名稱和副檔名
- （僅限檔案型）**[**方向]— 指定 Enterprise DLP 封鎖的是檔案上傳還是下載。
- **[**應用程式名稱**]** - 使用者嘗試對其上傳、下載或發布檔案型內容的應用程式。
- **[**動作] - Enterprise DLP 在偵測到敏感資料時採取的動作。此值一律會為 `Blocked`（封鎖）。

1. 定義檔案型偵測的訊息範本。

   若未設定檔案型偵測的 DLP 規則，請跳過此步驟。
2. 定義非檔案型偵測的訊息範本。

   若未設定非檔案型偵測的 DLP 規則，請跳過此步驟。
3. 新增 **Support Link**（支援連結）。

   您可以直接在「存取體驗」快顯通知中新增連結，以說明您的公司在共用或下載敏感資料方面的政策。



STEP 11 | **Save**（儲存）。

STEP 12 | 產生 Enterprise DLP 事件的使用者可以檢視資料安全性通知，以查看已上傳、下載或發布的敏感資料片段。

 ©2025 Palo Alto Networks, Inc.

管理：操作人員

這可在何處使用？	我需要哪些內容？
• NGFW (Managed by Panorama or Strata Cloud Manager) • 包括 VM-Series	❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

疑難排解

從 Strata Cloud Manager 對 NGFW 進行疑難排解，且無需在各種防火牆介面之間移動。

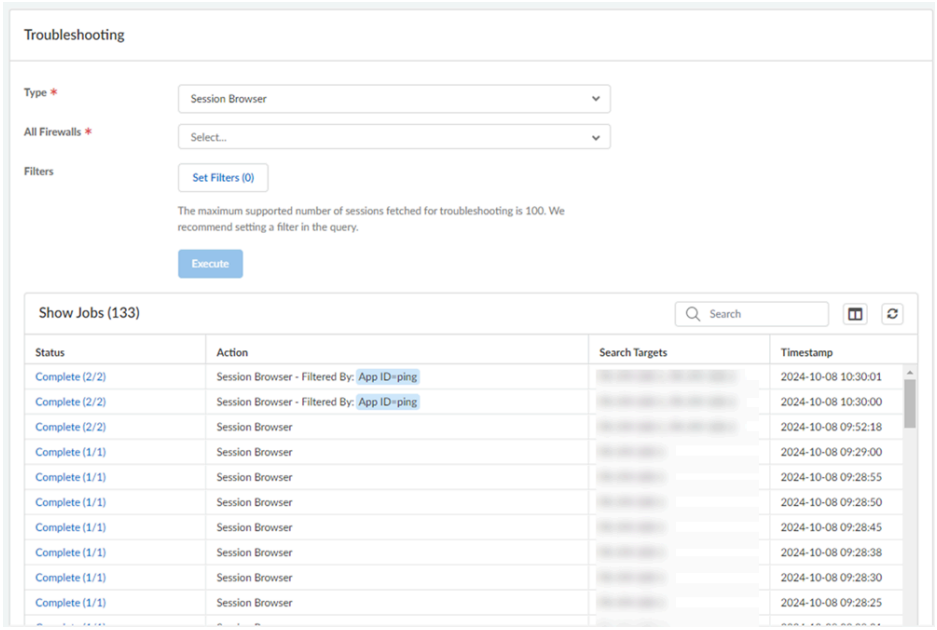
如需疑難排解的詳細資訊，請按一下這裡。

疑難排解儀表板可讓您對 Strata Cloud Managed NGFW 的網路、識別和政策問題進行疑難排解。使用疑難排解儀表板，可以找出下列領域的異常和有問題的設定：

- ❑ DNS Proxy
- ❑ NAT
- ❑ 使用者群組
- ❑ 動態位址群組
- ❑ 動態使用者群組
- ❑ 使用者 ID
- ❑ 工作階段瀏覽器

首先，移至**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW 和 Prisma Access**） > **Operations**（操作） > > **Troubleshooting**（疑難排解） > **Session Browser**（工作階段瀏覽器）。

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

管理：IoT 政策建議

這可在何處使用？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ 至少要有下列其中一個授權，才能使用 Strata Cloud Manager 管理您的設定；若要統一管理 NGFW 和 Prisma Access，您將同時需要： ❑ Prisma Access 授權 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ 進階 IoT Security 產品（Enterprise IoT Security Plus、Industrial IoT Security 或 Medical IoT Security）的 IoT Security 訂閱

IoT Security 會為 Strata Cloud Manager 提供自動產生的安全性政策規則建議（按裝置設定檔組織）。每個設定檔中的每個應用程式各有一個建議。選取設定檔、選取您要使用的規則建議，然後選取要強制執行這些建議的新世代防火牆或 Prisma Access 部署類型。

開始

選取安全性政策規則建議，並將其套用至新世代防火牆或 Prisma Access。

STEP 1 | 建立新世代防火牆的資料夾或片段。

如果您想要使用預先定義的資料夾或先前建立的資料夾或片段，請跳過此步驟。*Prisma Access* 資料夾是預先定義的。

資料夾基本上是包含各種規則、安全性設定和物件的容器。為了匯入 IoT Security 所產生的政策規則建議，資料夾會保存新世代防火牆或 Prisma Access 部署。

片段也是可與多個資料夾相關聯的容器類型。透過資料夾和片段，您可以將政策規則匯入您所需的任何防火牆或部署群組中。

例如，您可以建立名為 California 的資料夾，並在其中放置 60 個防火牆，然後建立名為 Hawaii 的另一個資料夾，並在其中放置 15 個防火牆。然後，您可以建立名為 CA-HI 的片段，並將其套用至 California 和 Hawaii 資料夾。若您只想將規則建議匯入至加州的防火牆，請將範圍設定為 **Folder**（資料夾），然後選取 California 資料夾。如果您要將規則建議同時匯入至 California 和 Hawaii，請將範圍設定為 **Snippet**（片段），然後選取 CA-HI 片段。

根據資料夾結構的階層，在 California 和 Hawaii 之上可能會有像是 US-West 的父資料夾。然後，如果您在匯入規則建議時將範圍設定為 **Folder**（資料夾）並選取了 **US-West**（美國西部），則 California 和 Hawaii 兩個子資料夾都會繼承匯入的規則。但是，如果您只想將規則匯入 California 和 Hawaii，而它們在 US-West 資料夾下有 Oregon、Alaska、Washington 和 Arizona 等資料夾，就不是如此了。然後，你必須使用 CA-HI 片段。

STEP 2 | 建立安全性原則規則。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **IoT Policy Recommendation**（**IoT** 政策建議）。
2. 選取設定檔名稱。

   IoT Security 會使用機器學習，根據相同裝置設定檔中的 IoT 裝置正常、可接受的網路行為，自動產生安全性政策規則建議。Strata Cloud Manager 會顯示按應用程式組織的建議清單。對於每個行為，您可以看到下列項目：

行為元件	解釋
應用程式風險	這是應用程式中固有的風險層級，取決於多項因素，採用從風險 1 到 5 遞增的刻度。
已建立安全性政策	當此處出現一或多個資料夾或片段名稱時，表示先前已針對此行為建立了安全性政策規則。按一下其中之一可開啟側面板，其中包含設定檔、應用程式、資料夾或片段的名稱，以及政策規則動作。此處顯示 **No**（否）時，表示規則尚未建立。

 ©2025 Palo Alto Networks, Inc.

行為元件	解釋
探索的位置	**Internal**（內部）表示目的地位於本機網路上。**External**（外部）表示目的地位於本機網路以外。
本機觀察	**Yes**（是）表示是您的 IoT Security 租用戶環境中觀察到行為的。**No**（否）表示是在多個 IoT Security 租用戶環境中觀察到的，但在您的環境中未觀察到。
應用程式使用情況	**Common**（常見）表示已在多個 IoT Security 租用戶環境中偵測到應用程式。**Unique**（唯一）表示已在您的環境中觀察到，但在相同設定檔中也有裝置的其他租用戶環境中則未觀察到。
目的地位址與 FQDN	這是建議政策規則的目的地。可以是 [Any（任何）]、[IP address（IP 位址）] 或 [FQDN]。
Destination Profile 目的地設定檔	若目的地為內部，且已識別出目的地的裝置設定，就會顯示設定檔。
上次看見	就本機觀察到的行為而言，這是上次觀察到時的時間戳記。對於未在本機觀察到的常見行為，則會顯示虛線。

3. 選取一或多個行為，然後選取 **Create Security Policy**（建立安全性政策）。
4. 檢閱將建立的安全性政策規則，然後為將套用規則的 Strata Cloud Manager 選取設定範圍。

   若要將規則套用至資料夾中的一或多個新世代防火牆或 Prisma Access 部署，請選取 **Folders**（資料夾），然後從 [Scope Selection（範圍選取）] 中選取資料夾。

   若要將規則套用至片段中的一或多個新世代防火牆或 Prisma Access 部署，請選取 **Snippets**（片段），然後從 [Scope Selection（範圍選取）] 中選取片段。
5. 建立安全性政策。

©2025 Palo Alto Networks, Inc.

STEP 3 | 將設定推送至新世代防火牆和 Prisma Access 部署。

1. 選取**Manage**（管理） > **Operations**（操作） > **Push Config**（推送設定）。
2. 選取具有設定變更的資料夾，然後依序選取 **Push Config**（推送設定）、**Push**（推送）和 **Push**（推送）。

   Strata Cloud Manager 會在所選資料夾的 [Job ID（工作 ID）] 欄中顯示 ID 號碼，並在 [Push Status（推送狀態）] 欄中顯示設定推送的狀態。

   當 [Push Status（推送狀態）] 從 **Pending**（擱置中）變更為 **Success**（成功）時，您即得知推送的設定已開始執行。
3. 若要查看推送工作的狀態，請選取**Manage**（管理） > **Operations**（操作） > **Push Status**（推送狀態）。您可以在這裡查看父工作的狀態以及子工作的狀態，每個防火牆或部署各有一個。

 ©2025 Palo Alto Networks, Inc.

管理：企業 DLP

這可在何處使用？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	• Enterprise Data Loss Prevention (E-DLP) 授權 • **NGFW (Managed by Panorama)** — 支援和 Panorama 裝置管理授權 • **Prisma Access (Managed by Strata Cloud Manager)**—Prisma Access 授權 • **SaaS Security**—SaaS Security 授權 • **NGFW (Managed by Strata Cloud Manager)** — 支援和 AIOps for NGFW Premium 授權 或下列任何包含 Enterprise DLP 授權的授權 • Prisma Access CASB 授權 • Next-Generation CASB for Prisma Access and NGFW (CASB-X) 授權 • Data Security 授權

Enterprise Data Loss Prevention (E-DLP) 會保護敏感資訊不受未經授權的存取、濫用、擷取或共用。Strata Cloud Manager 上的 Enterprise DLP 可讓您強制執行組織的資料安全性標準，並防止 NGFW 以及 Prisma Access 行動使用者和遠端網路中的敏感資料遺失。

功能重點

- 企業資料遺失防護 **(E-DLP)** 儀表板

  移至 **Manage**（管理） > **Configuration**（設定） > **Data Loss Prevention**（資料遺失防護），以設定及管理 Enterprise DLP。

  你的 Enterprise DLP 設定會在使用 Enterprise DLP 的產品之間共用。因此，您可能會在此處看到他處設定的設定，且您可在此處設定的某些設定，也可以在其他產品中使用。

- 預先定義 **+** 自訂 **Enterprise DLP** 設定

  Enterprise DLP 包含可讓您快速開始保護最敏感內容的內建設定：

  - 預先定義的 regex 和 ML 型資料模式會指定您可能想要掃描和保護的常見敏感資訊類型（例如信用卡和社會安全號碼）
  - 預先定義的資料設定檔會將通常需要相同強制執行類型的資料模式分組在一起

  您也可以直接在 Strata Cloud Manager 上建立自訂資料模式和設定檔。

- **DLP** 事件的調查

  當流量符合與 Strata Cloud Manager 上的安全性政策規則連結的 DLP 資料設定檔時，就會產生 DLP 事件。在 DLP 事件儀表板上，您可以檢視觸發事件之流量的詳細資料，例如相符的資料模式、流量的來源和目的地、檔案和檔案類型。

- 掃描支援檔案格式的影像

  透過光學字元辨識 (OCR)加強您的安全性狀態，進一步防止意外的資料誤用、遺失或遭竊。OCR 允許 DLP 雲端服務掃描影像中有敏感資訊符合 Enterprise DLP 篩選設定檔的支援檔案類型。

- 精確資料比對 **(EDM)**

  EDM 是一項進階偵測工具，用以監控及保護敏感資料免於外洩。使用 EDM 可偵測結構化資料來源（例如資料庫、目錄伺服器）或結構化資料檔案（CSV 和TSV）中的敏感資料與個人識別資訊 (PII)，例如社會安全號碼、病歷號碼、銀行帳號和信用卡號碼，且具有高精確度。

- 自訂文件類型

  將包含智慧財產權或敏感資訊的自訂文件上傳至 Enterprise Data Loss Prevention (E-DLP)，以建立自訂文件類型。您的自訂檔案類型可在進階資料設定檔中作為比對準則，用以偵測和防止外洩。

- 電子郵件 **DLP**

  電子郵件 DLP 可透過採用 AI/ML 技術的資料偵測防止包含敏感資訊的電子郵件外洩。例如，企業 DLP 可防止敏感資料透過輸出電子郵件外洩，例如，從組織內部銷售人員傳送給其個人電子郵件。

- **Enterprise DLP** 的角色型存取

  您可以在 Strata Cloud Manager 中啟用對 Enterprise DLP 的角色型存取控制。如此，您即可控制哪些使用者對 Enterprise DLP 的不同部分具有讀取和寫入存取權限。

 ©2025 Palo Alto Networks, Inc.

開始

STEP 1 | 在 Strata Cloud Manager 上啟用 Enterprise DLP。

若要設定 Enterprise DLP，必須建立解密設定檔以允許 DLP 雲端服務檢查流量。選取**Manage**（管理） > **Configuration**（設定） > **Security Services**（安全服務） > **Decryption**（解密），然後：

1. 選取**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服務） > **Decryption**（解密），並新增規則。

   預先定義的解密設定檔設定會允許 Enterprise DLP 檢查流量。除非您需要啟用 **Strip ALPN**（除去 **ALPN**）（**Advanced Settings**（進階設定） > **SSL Forward Proxy**（**SSL** 正向 **Proxy**）），否則不需要修改預先定義的解密設定檔設定。

2. 將解密設定檔新增至 **SSL Forward Proxy**（**SSL** 正向 **Proxy**）解密規則。

- 以下說明如何啟用企業 DLP

STEP 2 | （選用）選取**Manage**（管理） > **Configuration**（設定） > **Data Loss Prevention**（資料遺失防護） > **Detection Methods**（偵測方法），並建立資料模式

您可以建立自訂 Enterprise DLP 資料模式，指定哪些是敏感的且需要保護的內容 — 這就是您應篩選的內容。您可以建立以規則運算式為基礎的自訂資料模式或以檔案屬性為基礎的資料模式。

- 以下說明如何建立資料模式

STEP 3 | 建立資料設定檔

將應以相同方式強制執行的資料模式分組到資料設定檔中。您也可以使用資料設定檔來指定其他比對準則和比對信賴等級。

- 以下說明如何建立資料設定檔

STEP 4 | 建立 DLP 規則

指定要由 Enterprise DLP 保護的流量和檔案類型。設定 Enterprise DLP 在偵測到 DLP 事件時所要採取的動作。

- 以下說明如何建立 DLP 規則

 ©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

管理：SaaS 安全性

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ Prisma Access 授權

使用 SaaS 安全性內嵌，識別已認可和未認可的應用程式中的雲端式威脅和有風險的使用者活動。

SaaS 安全性內嵌內建於 Cloud Managed Prisma Access 中，可讓您集中檢視網路和 CASB 安全性。其中提供 SaaS 可見性（包括進階分析和報告），讓您的組織能夠深入瞭解網路上已認可和未認可的 SaaS 應用程式在使用上的資料安全性風險。

雲端存取安全性代理程式 (CASB) 套件組合包含 Saas 安全性內嵌、企業資料遺失防護 (DLP) 內嵌、SaaS 安全性 API、資料遺失防護 (DLP) API 和 SaaS 安全性狀態管理 (SSPM)。

新世代雲端存取安全性代理程式 (CASB-X) 授權包含所有的 CASB 元件，例如 SaaS 安全性內嵌、SaaS 安全性 API、SaaS 安全性狀態管理 (SSPM) 和企業 DLP。它可套用於單一租用戶環境中的 Cloud Managed Prisma Access、Panorama 管理的 Prisma Access，以及 Panorama 管理的新世代防火牆 (NGFW) 裝置。

以下是在 ***Strata Cloud Manager*** 上使用 **SaaS** 安全性的所有須知事項。

開始

以下說明如何在 Prisma Access 雲端管理上啟動並執行 SaaS 安全性內嵌：

確認您的 Prisma Access 訂閱隨附 SaaS 安全性附加元件授權。

移至 **Manage**（管理） > **Configuration**（設定） > **Overview**（概要），以檢查您的授權可用的功能。

如果尚未啟動，請在中樞啟動 SaaS 安全性內嵌應用程式。

啟動後，SaaS 安全性內嵌會自動探索所有 SaaS 應用程式和使用者，並從儲存在 Strata Logging Service 中的 Prisma Access 日誌中分析使用者的 SaaS 活動和使用資料。

檢閱及管理管理員角色和存取權。

在 Prisma Access 雲端管理中移至**Settings**（設定） > **Identity and Access**（識別與存取），以提供對 SaaS 安全性的角色型存取控制。

若要全面管理 *SaaS* 安全性，使用者也必須是 *SaaS* 安全性內嵌應用程式的管理員。直接從 *Prisma Access* 雲端管理儀表板跳到 ***SaaS*** 安全控制台，以新增 *SaaS* 安全性內嵌管理員。

探索 Prisma Access 雲端管理中的 **SaaS Security**（**SaaS** 安全性）儀表板。

移至**Manage**（管理） > **Configuration**（設定） > **Security Services**（安全服務） > **SaaS Security**（**SaaS** 安全性）。

Prisma Access 雲端管理中直接支援所有儀表板檢視。檢查這些檢視，以識別有風險的 SaaS 應用程式和使用者，以及 SaaS 安全性狀態管理。SaaS 安全性狀態管理 (SSPM) 會透過持續監控，協助您偵測並修復已認可的 SaaS 應用程式中設定不當的設定。

檢閱和共用 SaaS 安全性報告。

SaaS 安全性內嵌包含 SaaS 安全性報告，提供應用程式使用情況的快照，以及進階的彙總資料和檢視。此報告可作為 SaaS 安全團隊與高階管理層之間的溝通工具。您可以與 SaaS 安全團隊共用此隨選 PDF 報告以進行定期檢查，或透過電子郵件將報告傳送給主管，以突顯組織使用中的 SaaS 應用程式，及其伴隨的安全性風險。

- 以下將詳細說明 SaaS 安全性報告
- 以下說明如何在 SaaS 安全性內嵌應用程式中產生 SaaS 安全性報告

瞭解 SaaS 安全性和 Prisma Access 雲端管理還有哪些功用。

©2025 Palo Alto Networks, Inc.

SaaS 政策建議

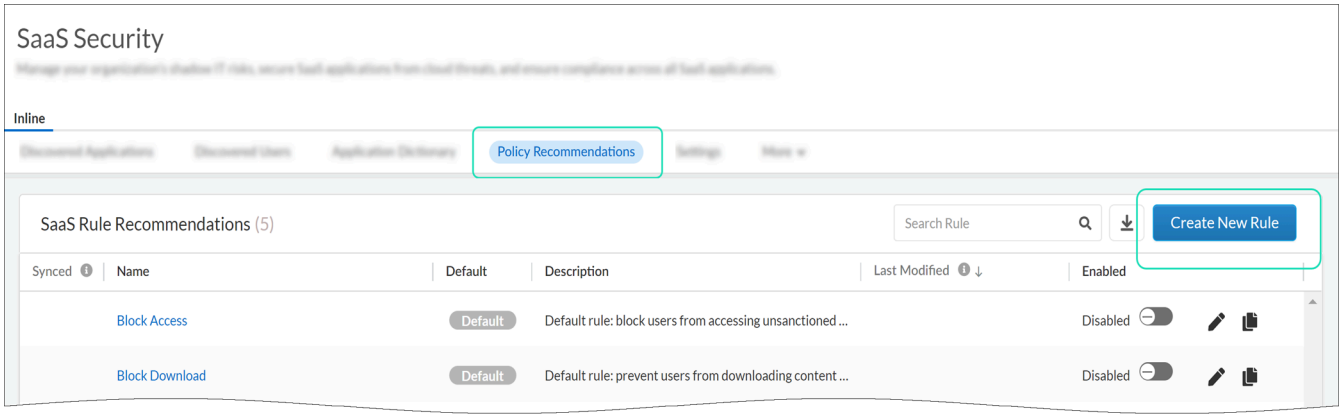
為了獲得對 SaaS 應用程式的可見性和控制，SaaS 安全性管理員會使用 App-ID 雲端引擎 (ACE) 提供的特定 SaaS App-ID 建立 SaaS 規則建議。

在 Prisma Access 雲端管理中，現在您可以檢閱並選擇接受 SaaS 安全性管理員建議的規則。SaaS 規則建議會新增至 Web 存取政策 - 必須啟用 Web 安全性，才能使用 SaaS 規則建議。

以下說明如何著手 — 在此處檢閱工作流程，以檢閱並接受 **SaaS** 政策建議：

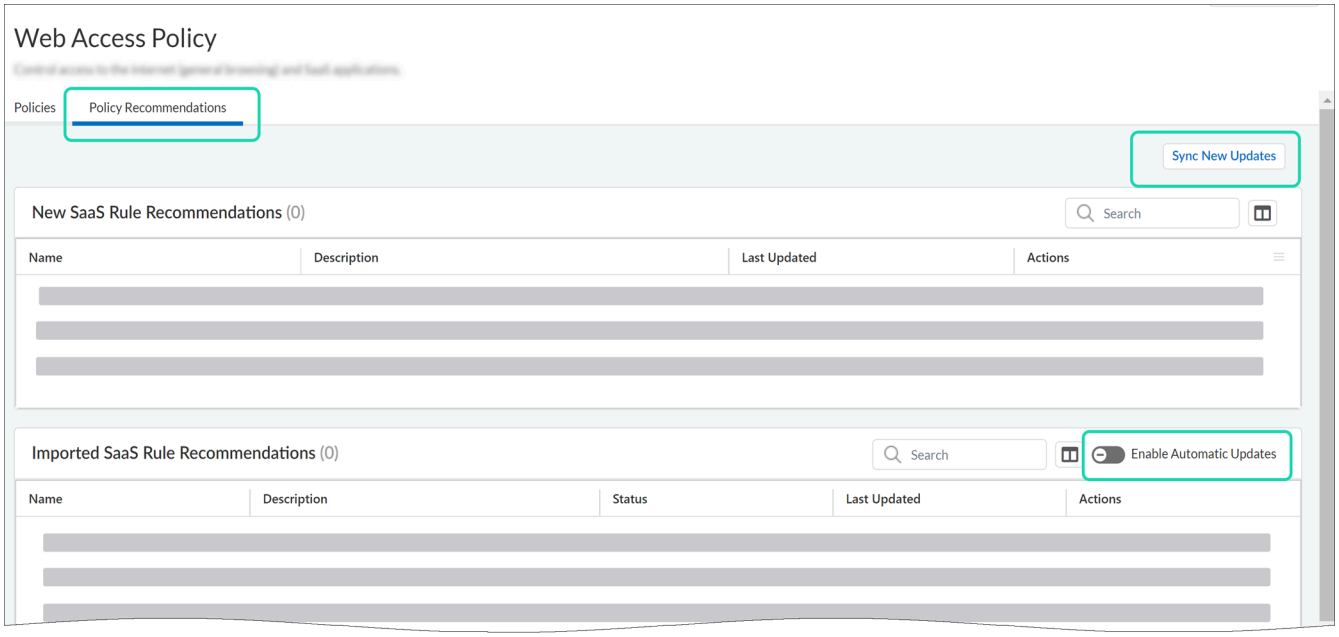
1. SaaS 安全性管理員可在 SaaS 安全性內嵌應用程式中建立 SaaS 規則建議，或直接在 Prisma Access 雲端管理中建立。

   # 在 Prisma Access 雲端管理中，移至**Manage**（管理） > **Configuration**（設定） > **Security Services**（安全服務） > **SaaS Security**（**SaaS** 安全性）



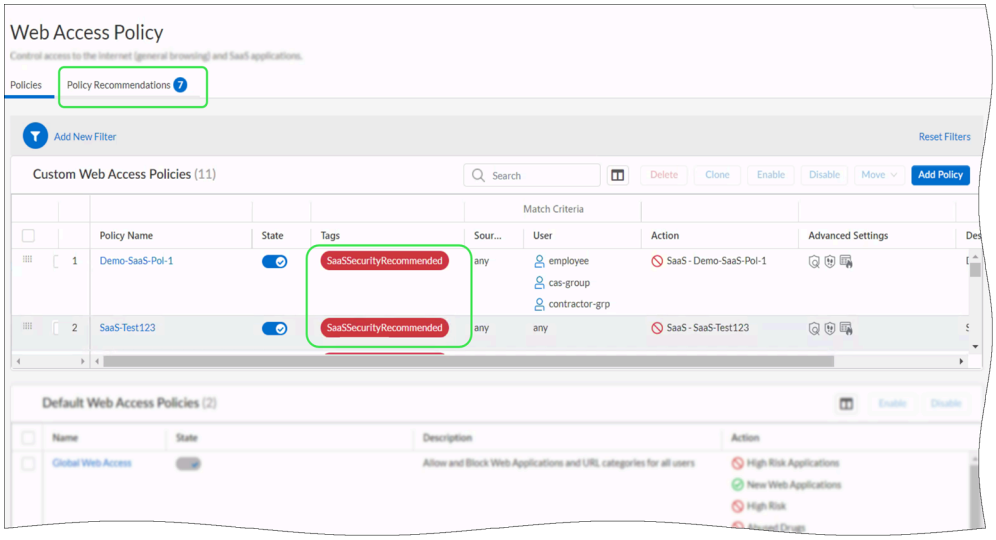
2. 您可以檢閱及匯入 SaaS 規則建議。

   # 移至**Manage**（管理） > **Web Security**（**Web** 安全性） > **Web Access Policy**（**Web** 存取政策）



©2025 Palo Alto Networks, Inc.

3. 您匯入的 SaaS 規則建議帶有標籤，以便您輕鬆識別。



 ©2025 Palo Alto Networks, Inc.

管理：Prisma SD-WAN

這可在何處使用？	我需要什麼？
• Prisma SD-WAN	❑ Prisma SD-WAN 授權

Prisma SD-WAN 提供了軟體定義的廣域網路 (SD-WAN) 解決方案，將舊版廣域網路 (WAN) 轉換為極其簡化、安全的應用程式網狀架構 (AppFabric)，將異質基礎傳輸虛擬化為統一的混合 WAN。系統的核心是應用程式效能引擎。

您可以檢視精細的應用程式驅動分析、建置妥善的政策，以及 WAN 的效能型流量管理。透過 Instant-On Network (ION) 裝置，Prisma SD-WAN 簡化了 WAN 的設計、建置和管理方式，將資料中心級安全性穩健延伸至網路邊緣。

Prisma SD-WAN 支援用於流量轉送操作的堆疊政策。使用集中定義的政策，每個 ION 裝置均執行自動路徑選取、流量塑形或連結之間的主動-主動負載平衡等動作，而 Prisma SD-WAN 控制器則完整呈現所有 WAN 連結的應用程式效能和回應時間。

Prisma SD-WAN 會根據應用程式效能服務等級協定 (SLA) 和業務優先順序控制網路應用程式效能。您可以使用 Strata Cloud Manager 為 Prisma SD-WAN 設定政策、資源、CloudBlade 和系統設定。

選取**Manage**（管理） > **Prisma SD-WAN**以管理下列項目的設定：

- 政策
- 資源
- CloudBlade
- 系統

管理：適用於 Prisma SD-WAN 的政策

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma SD-WAN	❑ Prisma SD-WAN 授權

Prisma SD-WAN 支援堆疊和原始政策。使用集中定義的政策時，每個 ION 裝置會執行諸如自動路徑選取、流量塑形或連結之間的主動-主動負載平衡的動作，而 Prisma SD-WAN 控制器則可讓您完整檢視所有 WAN 連結的應用程式效能和回應時間。

使用 Strata Cloud Manager 在 Prisma SD-WAN 中設定政策。

STEP 1 | 選取**Manage**（管理） > **Prisma SD-WAN** > **Policies**（政策）。

您可以在 Prisma SD-WAN 中設定下列類型的政策：

- 路徑

  設定流程轉送和流量塑形操作的堆疊路徑政策。

- 效能

  設定效能政策，以測量應用程式效能和應用程式 SLA。

- QoS

  設定堆疊 QoS 政策，以指定業務優先順序。

- 安全性

  設定堆疊安全性政策，以定義相關規則來決定分支內的應用程式存取權。

- NAT

  設定堆疊 NAT 政策，以確保連線至公用或私人網路的內部網路保有隱私。

- 安全性（原始）

  這些是舊版安全性政策。如果您是從 ION 裝置軟體 6.0.1 版開始的新使用者，就只能設定堆疊安全性政策。如果您已設定原始或舊版政策，您必須將這些舊版政策轉換為堆疊政策，才能將裝置升級至 6.0.1 版。

- 網路（原始）

  這些是舊版網路政策。如果您是從 ION 裝置軟體 6.0.1 版開始的新使用者，就只能設定堆疊網路政策。如果您已設定原始或舊版政策，您必須將這些舊版政策轉換為堆疊政策，才能將裝置升級至 6.0.1 版。

STEP 2 | 選取 **Bindings**（繫結），將政策堆疊繫結至站台。

為了讓路徑、QoS、安全性和 NAT 堆疊中的政策規則生效，您必須將政策堆疊繫結至站台。一次只能將一個路徑、QoS、安全性和 NAT 堆疊繫結至一個站台。

 ©2025 Palo Alto Networks, Inc.

管理：Prisma SD-WAN 的資源類型

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma SD-WAN	❑ Prisma SD-WAN 授權

您可以在 Prisma SD-WAN 中管理不同類型的資源。

使用 Strata Cloud Manager 在 Prisma SD-WAN 中管理資源。

選取**Manage**（管理） > **Prisma SD-WAN** > **Resources**（資源）。

您可以在 Prisma SD-WAN 中管理下列類型的資源：

- 應用程式

  應用程式是 Prisma SD-WAN 解決方案的核心。部署在網路中的 ION 裝置會主動分析每個應用程式流量，以確保會維護效能、合規性和安全性的政策，並且對每個流量使用最佳網路連線。ION 裝置會將應用程式定義和指紋技術用於路徑選取、QoS 和防火牆政策。

  系統應用程式會預設為可用，但您可以根據企業需求設定自訂應用程式。

- 線路類別

  線路類別是對網路中可能存在的各種線路和連線所做的邏輯分組。這種分組讓整個網路的網路政策規則得以簡化，並且可重複使用。例如，網際網路有線寬頻、計量網際網路 LTE 連結、衛星網際網路連結、網際網路 DSL，或專用 MPLS。

- 網路內容

  網路內容可以劃分網路流量，以便為相同的應用程式套用不同的網路政策規則。具有網路內容的規則一律會優先於沒有網路內容的規則。您可以建立一或多個網路內容，但一個 LAN 網路只能屬於一個網路內容。必須將網路內容連結至適當的 LAN 區段，才能生效。

- 服務與 DC 群組

  使用服務與 DC 群組可將第三方端點對應至群組，以便能靈活地建立網路政策規則，實現站台之間的唯一性。目的是無論站台位置為何，政策規則都保持不變。

- 安全區域

  安全區域會指定流量受到檢查和篩選的強制執行邊界。每個安全區域分別對應於連結至裝置的實體介面、邏輯介面或子介面的網路。這些區域層級介面可作為實體線路和虛擬線路的 Proxy，例如 VLAN、第三層 VPN 和第二層 VPN 線路。

- 站台範本

  站台設定範本可協助您建立客製化站台範本以因應部署需求，讓您能夠輕鬆且有效率地大規模部署分支和資料中心。使用此範本，您可以部署多個站台。您可以使用現有範本、編輯現有範本或建立新範本，以部署多個站台。

- 前置詞篩選器

  前置詞是由一或多個單獨的 IP 位址或 IP 位址子網路組成的群組。前置詞可用於路徑集政策和優先順序政策。其範圍可以是全域，也可以是區域。

 ©2025 Palo Alto Networks, Inc.

- 組態設定檔

  使用組態設定檔可設定不同資源類型的設定。

  - IPsec

    建立 IPsec 設定檔，以設定分支裝置與雲端安全服務端點之間的 IPsec VPN 連線。
  - IPFIX

    IPFIX 設定檔是一個全域的 IPFIX 設定物件，可識別收集器設定、篩選器設定、匯出流量資訊元素的範本，以及流量取樣工具設定。
  - APN

    建立存取點名稱 (APN) 設定檔，以定義行動網路資料連線的網路路徑。連線至行動網路時需要 APN 資訊。
  - DNS

    設定網域名稱系統 (DNS) 設定檔，以指定 DNS 服務的設定參數。常設定的參數包括 DNS 伺服器、網域到位址的對應、快取設定，以及 DNSSEC 設定。DNS 服務設定檔建立後，會繫結至裝置。
  - NTP 範本

    使用網路時間通訊協定 (NTP) 設定範本新增或編輯 NTP 伺服器。
  - 多點傳送

    建立 WAN 多點傳送組態設定檔，並將其與分支站台產生關聯，以便為分支站台啟用多點傳送 WAN 多點傳送路由。
  - VRF

    建立全域（預設）虛擬路由和轉送表格 (VRF) 設定檔，並產生其關聯，然後將其指派給所有分支和資料中心站台。
  - IoT 探索

    使用 IoT 裝置可見性，識別網路中的裝置。Prisma SD-WAN 分支 ION 裝置會檢查封包、擷取資訊，和產生要以特定格式傳送至 Strata Logging Service 的訊息。

 ©2025 Palo Alto Networks, Inc.

管理：適用於 Prisma SD-WAN 的 CloudBlade

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma SD-WAN	❑ Prisma SD-WAN 授權 ❑ 對應 CloudBlade 的 CloudBlade 授權

使用 Prisma SD-WAN CloudBlade 平台可安全地存取 ION 裝置，透過自訂範本自動執行 Web 介面工作流程，以降低操作複雜性。

使用 Strata Cloud Manager 在 Prisma SD-WAN 中設定 CloudBlade。

選取**Manage**（管理） > **Prisma SD-WAN** > **CloudBlades**。

您將可在 Prisma SD-WAN 中檢視您已訂閱的 CloudBlade。依照相關 CloudBlade 整合指南中的步驟設定您的 CloudBlade。

©2025 Palo Alto Networks, Inc.

管理：Prisma SD-WAN 的系統資源

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma SD-WAN	❑ Prisma SD-WAN 授權

在 Prisma SD-WAN 中，使用 **System**（系統）頁籤下的可用資源管理及監控使用者和權限。

選取**Manage**（管理） > **Prisma SD-WAN** > **System**（系統）。

您可以在 Prisma SD-WAN 中設定下列類型的系統資源：

- 授權管理

  使用「授權管理」，為虛擬 ION 產生授權權杖。這提供了一組控制，防止未經授權者在環境中新增虛擬裝置。

- 稽核日誌

  使用稽核日誌，檢視系統中的設定變更記錄。您可以將這些日誌用於合規性和疑難排解用途。稽核日誌提供多種資訊，例如所做的變更、變更的擁有者、變更的時間，以及站台、系統或站台子集上的變更範圍。

- 企業前置詞

  使用企業前置詞，可讓 Prisma SD-WAN 資料中心站台輕易地通告分支站台的路由和連線性。

 ©2025 Palo Alto Networks, Inc.

- 存取管理
  - 使用者存取
    - 使用者管理

      根據您企業的需求新增具有系統角色的新使用者。系統角色是為每個角色預先定義的一組權限。這些角色包含由一或多個系統權限組成的集合。可用的系統角色包括根、超級管理員、IAM 管理員、網路管理員、安全性管理員，以及僅限檢視使用者。
    - 自訂角色

      您可以用不同方式結合現有的系統角色與權限，藉以建置自訂角色。您可以藉由組合一組系統權限，或是新增或移除系統角色的權限，來加以建立。
    - 密碼需求

      設定密碼的字元和安全需求。您也可以設定重複使用舊密碼和重新整理密碼的頻率。
  - 裝置存取
    - 裝置工具套件使用者存取
    - 裝置離線存取政策
  - 租用戶存取
    - 驗證權杖

      設定存取 Prisma SD-WAN API 的驗證權杖。為使用者產生權杖後，將可將其用來進行重複的 API 呼叫，而無須再登入以存取 API。

      有權存取驗證權杖的使用者，可以存取指派給該權杖的所有權限。

      選取**Manage**（管理） > **System**（系統） > **Tenant Access**（租用戶存取） > **Auth Tokens**（驗證權杖） > **Create Auth Token**（建立驗證權杖），以建立驗證權杖。
  - 識別管理
    - 雲端識別引擎

 ©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

管理：Prisma Access 瀏覽器

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 授權

從 Strata Cloud Manager 中選取**Manage**（管理） > **Configuration**（設定） > **Prisma Access Browser**（**Prisma Access** 瀏覽器）。

Prisma Access Secure Enterprise Browser (Prisma Access Browser) 是唯一可同時保護受管理和未受管理裝置的解決方案，其工具為原生整合、可將保護延伸至未受管理裝置的企業瀏覽器。請參閱什麼是 Prisma Access 瀏覽器？

首頁

首頁是您從 Strata Cloud Manager 存取 Prisma Access Browser 時的登陸頁面。在首頁中，您可以使用 Prisma Access 瀏覽器儀表板，從使用者行為和瀏覽資料的分析中衍生出有意義的洞察。對於您可能想要監控的特定使用案例，有多種儀表板可供使用，例如使用者行為、資料洩漏保護、Web 安全性和政策。每個儀表板都包含一系列的 Widget，且部分 Widget 會顯示在多個儀表板中。

©2025 Palo Alto Networks, Inc.

分析

Prisma Access Browser 的 [Events（事件）] 畫面是您調查企業瀏覽器部署中的每個活動時關鍵的可見性工具，可確認政策和規則均正常運作。這是您調查 Prisma Access 瀏覽器事件的位置。

©2025 Palo Alto Networks, Inc.

目錄

- 使用者目錄可作為中央位置，顯示關於使用者及其與 Prisma Access 瀏覽器連線的裝置、使用者群組中的成員資格，以及相關政策規則的資訊。管理 Prisma Access 瀏覽器使用者
- 裝置目錄會提供 Prisma Access 瀏覽器裝置和裝置群組的清單。管理 Prisma Access 瀏覽器裝置
- Prisma Access 瀏覽器配備了既有的已驗證應用程式清單。已驗證的應用程式清單會參考 Palo Alto Networks App-ID™ 應用程式目錄，並定期與雲端資料庫同步。您也可以建立自訂和私人應用程式。管理 Prisma Access 瀏覽器應用程式
- Prisma Access 瀏覽器有一個 Extension 目錄，其中包含一般使用者在瀏覽器上安裝的延伸。這項資訊可讓您保有適當的公司政策管理，管理可見性和風險分析。管理 Prisma Access 瀏覽器延伸

©2025 Palo Alto Networks, Inc.

原則

- 您可以使用規則來指定將受到各種政策影響的使用者、使用者群組和裝置群組。這些規則可控管對 Web 應用程式、安全性政策和自訂選項的存取。利用規則，您可以精確控制使用者對組織工具和元件的存取。管理 Prisma Access 瀏覽器政策規則
- Prisma Access Browser 規則的控制可設定於個別規則的內文中。當您想要儲存可重複使用的（舊版）設定檔，且後續要將其新增至規則時，即可使用設定檔（外部控制）。管理 Prisma Access 瀏覽器政策設定檔
- 使用登入規則來決定哪些使用者和裝置有權存取 Prisma Access Browser。管理 Prisma Access 瀏覽器登入規則
- 當您在政策規則中定義略過條件之後，若使用者嘗試執行的動作或造訪的站台受到對應規則封鎖，他們可以提交略過要求。若要設定略過條件，請設定啟用權限要求的提示動作。管理 Prisma Access 瀏覽器要求以略過政策規則。

©2025 Palo Alto Networks, Inc.

管理

使用下列途徑管理其他功能的整合：

- Microsoft 365
- Microsoft Information Protection
- Google Workspace
- Votiro
- CrowdStrike Falcon Intelligence
- OPSWAT MetaDefender
- YazamTech SelectorIT
- Symantec DLP

©2025 Palo Alto Networks, Inc.

管理：操作人員

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW，包括由軟體 NGFW 積分資助的項目	❑ 至少要有下列其中一個授權，才能使用 Strata Cloud Manager 管理您的設定；若要統一管理 NGFW 和 Prisma Access，您將同時需要： ❑ Prisma Access 授權 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能取決於您所使用的授權。

使用 Strata Cloud Manager 操作推送設定變更、檢閱過去的設定推送，以及管理設定版本快照以將其載入或還原到先前的設定版本。

- 推送您的設定變更
- 檢閱設定推送的狀態
- 查看如何清理您的設定

管理：推送設定

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW，包括由軟體 NGFW 積分資助的項目	❑ 至少要有下列其中一個授權，才能使用 Strata Cloud Manager 管理您的設定；若要統一管理 NGFW 和 Prisma Access，您將同時需要： ❑ Prisma Access 授權 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能取決於您所使用的授權。

進行設定變更並準備好加以啟動後，您必須將變更推送至防火牆。您可以選擇推送所有設定變更，或選取要包含在推送中的特定管理員。首次進行設定推送時，必須從所有管理員推送變更。您可以選擇要將哪些設定變更推送至 Prisma Access：

- **Web** 安全性

  將 Web 安全性更新推送至 Prisma Access。
- 行動使用者 — **GlobalProtect**

  將 GlobalProtect 更新推送至 Prisma Access。
- 行動使用者 — 明確 **Proxy**

  將明確 Proxy 更新推送至 Prisma Access。
- 遠端網路

  將 遠端網路更新推送至 Prisma Access。
- 服務連線

  將 服務連線更新推送至 Prisma Access。

您可以在進行另一個設定推送時推送設定。Prisma Access 會依照您提交設定變更的順序加以套用。

如果設定推送時發生錯誤，或變更導致網路或安全機制中斷，您可以將 Prisma Access 設定還原為最近執行的 Prisma Access 設定。這可讓您將 Prisma Access 設定還原為已知可運作且不會損害網路安全性的可行設定。您無法選取特定的可行設定。Prisma Access 會自動選取最新的已知可行設定，並還原為該設定。

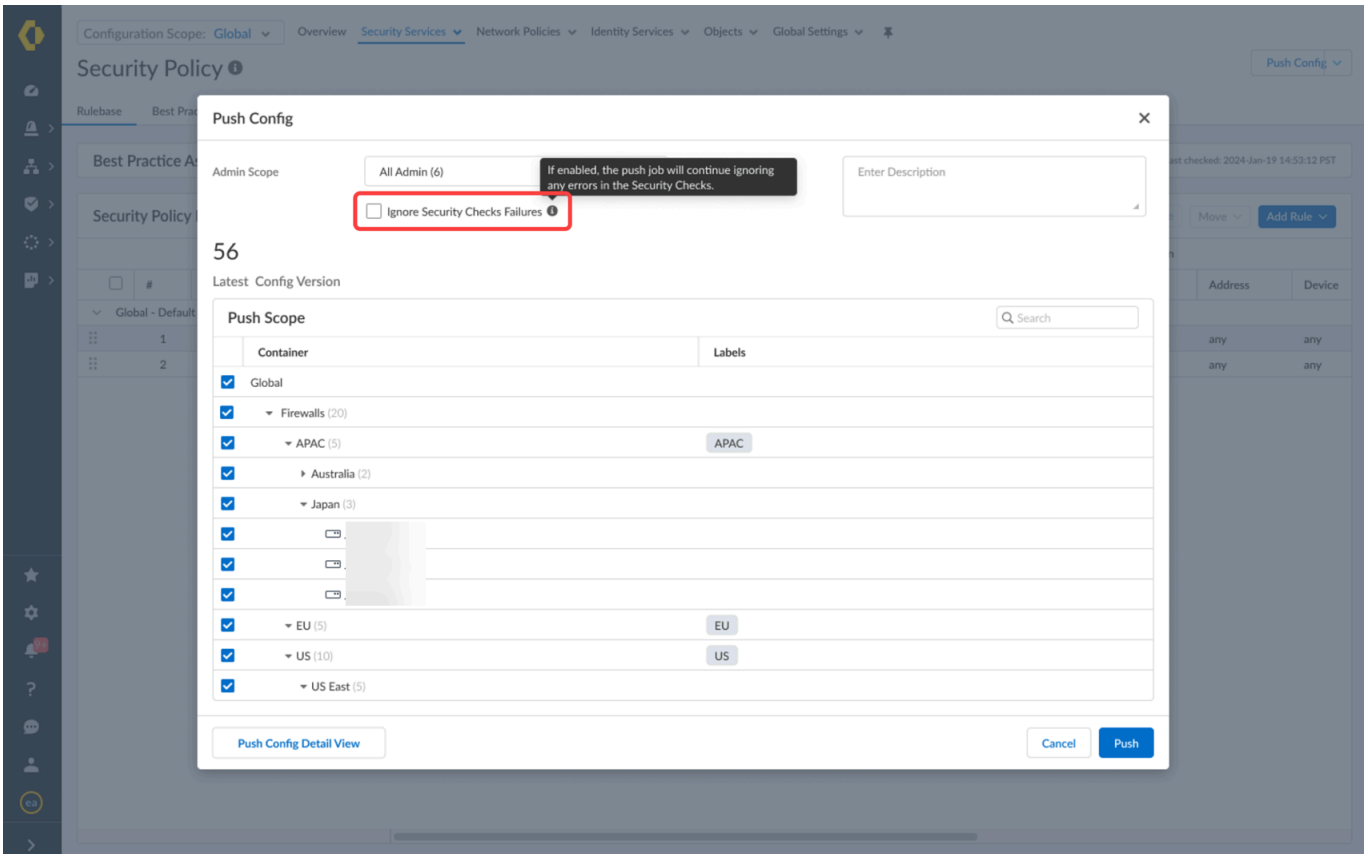
STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 視需要進行設定變更。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | 推送設定並推送您的設定變更。

或者，您可以選取***Manage***（管理）**>** ***Operations***（操作）**>** ***Push Config To Devices***（將設定推送至裝置）。



在 **Push Config**（推送設定）對話方塊中，您可以忽略安全性檢查失敗。此功能可讓您繼續推送操作，即使某些檢查會阻止該過程。若未選取該核取方塊（預設設定），且使用「封鎖」動作的最佳做法檢查失敗，Strata Cloud Manager 將會停止推送。

STEP 4 | （選用）新增篩選器。

您可以藉由套用篩選器，來篩選推送範圍中顯示的裝置。應用程式篩選器只會影響推送範圍中會顯示哪些防火牆或 Prisma Access 部署，而不影響您要推送到的裝置。

 ©2025 Palo Alto Networks, Inc.

STEP 5 | 編輯推送範圍。

編輯推送範圍可讓您將目標設定變更推送至部分或全部的防火牆或 Prisma Access 部署。

不支援執行部分設定推送，如果您符合下列情況，就必須推送整個 *Strata Cloud Manager* 設定：

- 設定新的租用戶，且這是您的第一個設定推送。
- 將防火牆上線至 *Strata Cloud Manager*。
- 將 *Prisma Access* 行動使用者和遠端使用者上線。
- 重新命名或移動資料夾，使其內嵌於不同的資料夾下。
- 將防火牆移至不同的資料夾。
- 將片段重新命名、產生關聯或取消關聯。
- 載入設定。
- 將設定還原為上次推送的設定或先前的設定版本快照。

- 管理範圍 — 選取要包含在推送中的管理員設定變更。根據預設，管理範圍選取目前的使用者，且該使用者所做的變更會推送至選取的防火牆或 Prisma Access 部署。選取 **Changes from all admins**（來自所有管理員的變更），會包含所有管理員所做的所有設定變更。

  編輯管理範圍以選取特定管理員時，會包含選取的管理員所做的所有設定變更。執行第一次設定推送時無法使用此選項。不支援選取特定設定變更以包含在推送中。

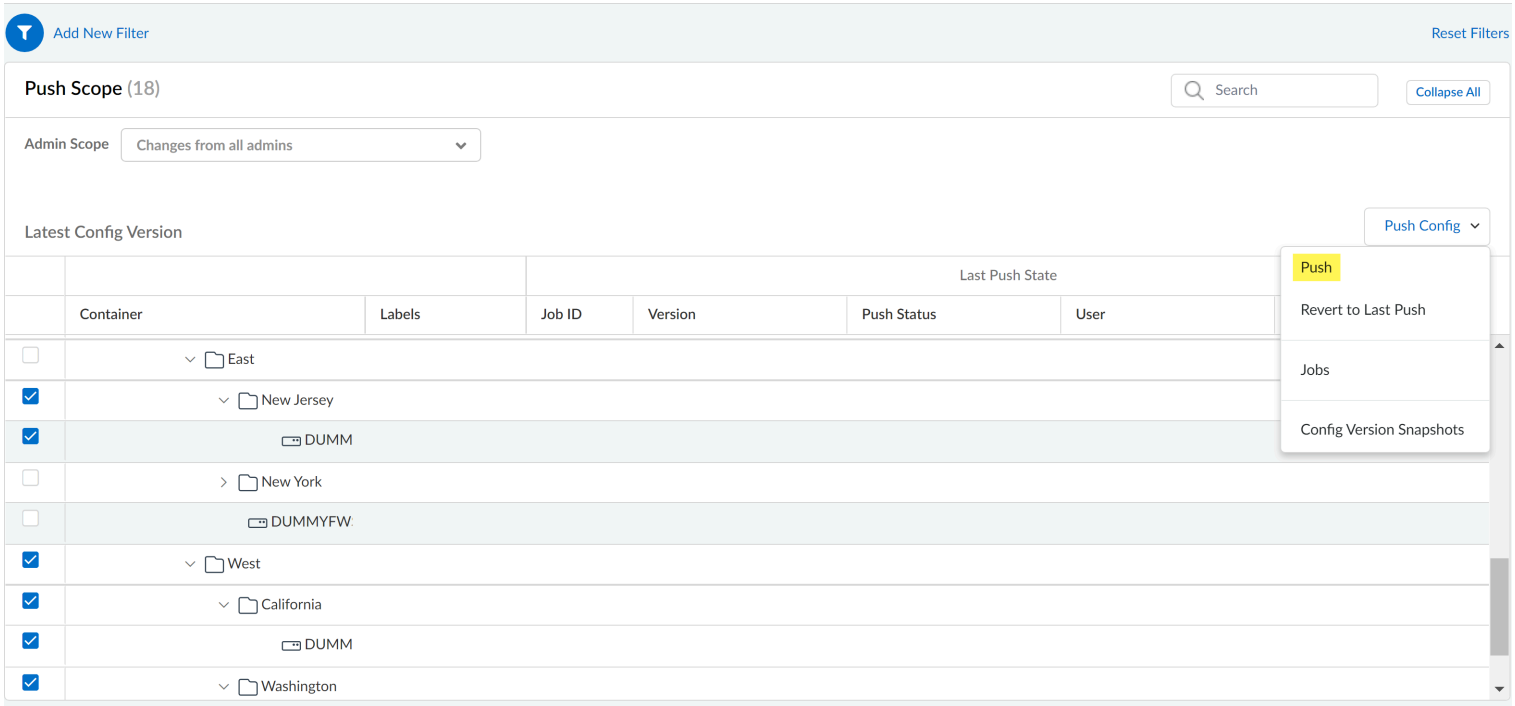
- 推送範圍 — 選取要推送到的部署類型或資料夾。當您選取部署或資料夾時，設定變更會推送至所有防火牆或部署。

  當您選取包含子資料夾的資料夾時，所有子資料夾以及相關聯的防火牆或 Prisma Access 部署都會包含在推送中。選取特定防火牆或 Prisma Access 部署時，會自動選取與其相關聯的資料夾。

 ©2025 Palo Alto Networks, Inc.

STEP 6 | 推送設定和推送。

檢閱推送目標和推送。



STEP 7 | 檢閱設定推送狀態。

如果設定推送時發生錯誤，或變更導致網路或安全機制中斷，您可以還原 Prisma Access 設定。

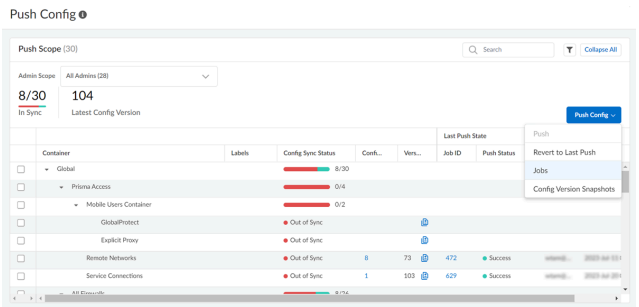
還原、載入和比較設定版本

檢視 Prisma Access 工作

您可以在 Prisma Access 上檢視工作歷程記錄，以顯示關於管理員起始的操作以及自動內容和授權更新的詳細資料。其中包括任何設定認可、推送和還原。您可以使用 [Jobs（工作）] 檢視對失敗的操作進行疑難排解，調查與已完成的提交相關的警告，或取消擱置中的提交。

STEP 1 | 啟動 Prisma Access。

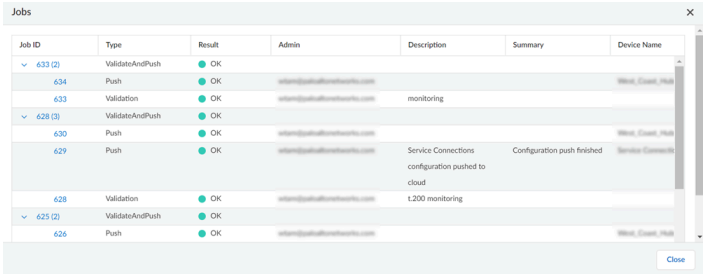
STEP 2 | 在頂端功能表列上，選取 **Push Config**（推送設定），然後檢視 Prisma Access 作業。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | 執行下列任何工作：

- 調查警告或失敗 — 閱讀 [Summary（摘要）] 欄中的項目，取得警告或失敗詳細資訊。
- 檢視認可說明 - 如果管理員輸入了認可說明，您可以參考 [Description（說明）] 欄以瞭解認可的目的。
- 檢查操作在佇列中的位置 - 檢視操作位置和狀態，以確認操作的位置。



 ©2025 Palo Alto Networks, Inc.

管理：推送狀態

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW，包括由軟體 NGFW 積分資助的項目	❑ 至少要有下列其中一個授權，才能使用 Strata Cloud Manager 管理您的設定；若要統一管理 NGFW 和 Prisma Access，您將同時需要： ❑ Prisma Access 授權 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能取決於您所使用的授權。

檢閱過去的設定推送至防火牆的推送狀態，以檢閱推送操作結果、起始推送的管理員和目標防火牆等詳細資料。

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 推送您的設定變更。

STEP 3 | 選取**Manage**（管理） > **Operation**（操作） > **Push Status**（推送狀態），並找出您要檢閱的設定推送操作。

STEP 4 | 展開您要檢視支設定推送的 工作 `ID`。

設定驗證工作一律會在任何設定推送發生之前執行。當您推送到多個防火牆時，每個設定推送都有一個唯一的工作 `ID` 和推送詳細資料。

STEP 5 | 檢閱關於設定推送狀態的詳細資料。

例如，檢閱推送結果、起始設定推送的管理員、設定推送摘要，以及設定推送的結束時間和開始時間。

如果推送成功，則設定推送結果將是成功，如果設定推送失敗，結果將是失敗。

STEP 6 | 按一下將設定推送至防火牆的唯一工作 `ID`，以檢閱工作詳細資料。

[Job Details（工作詳細資料）] 會提供關於在執行設定推送時遇到的警告和錯誤的詳細資訊。例如，如果推送至防火牆的作業失敗，您可以檢閱工作詳細資料，以瞭解導致設定推送失敗的原因。

©2025 Palo Alto Networks, Inc.

管理：設定版本快照

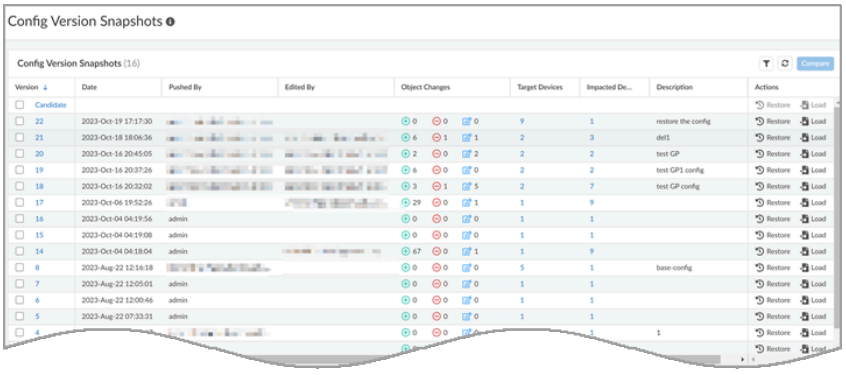
這可在何處使用？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW，包括由軟體 NGFW 積分資助的項目	❑ 至少要有下列其中一個授權，才能使用 Strata Cloud Manager 管理您的設定；若要統一管理 NGFW 和 Prisma Access，您將同時需要： ❑ Prisma Access 授權 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能取決於您所使用的授權。

設定快照可讓您檢視 Strata Cloud Manager 設定歷程記錄。當設定推送產生意外的安全隱患或對流量產生意外影響時，可以藉由還原至早期版本來復原。您也可以比較設定，以查看各個版本的變更。

設定快照概要

[Config Snapshot Version（設定快照版本）] 畫面可用來檢閱已推送的設定、將設定快照與候選設定進行比較，以及載入或還原較舊的設定。

選取**Manage**（管理） > **Operations**（操作） > **Config Version Snapshots**（設定版本快照），以尋找設定快照並還原、載入或比較版本。



1. 新增篩選器 — 選擇篩選器，按欄對設定版本進行排序和篩選。

 ©2025 Palo Alto Networks, Inc.

2. 版本 — 已推送設定的版本號碼。

   Candidate（候選）可讓您比較 Strata Cloud Manager 目前擱置中的設定變更與先前的設定版本。

   設定版本號碼會遞增。例如，如果您有 *10* 個版本，而您還原了設定版本 *2*，則設定版本會從 *10* 變更為 *11*（不會顯示為 *2*）。
3. 日期 — 推送設定的日期和時間。
4. 推送者 — 推送變更的管理員。
5. 編輯者 — 在設定推送之前加以變更的管理員。
6. 物件變更 — 查看在推送設定時新增、移除或修改了多少物件。
7. 目標裝置 — 定位於設定推送快照範圍內的裝置。

   執行還原動作時，您可以選擇要對哪些裝置執行。
8. 受影響的裝置 — 自上次設定推送後有所修改的裝置。與先前的設定推送快照不同時，裝置才會被視為受到影響。

   受影響的裝置和目標裝置

   如果您有兩個裝置 *A* 和 *B*，且僅推送至裝置 *A*，則 *A* 會成為目標裝置和受影響的裝置。

   如果您隨後再推送至裝置 *A* 和 *B*，則 *A* 和 *B* 都會成為目標裝置，但只有 *B* 是受影響的裝置。

   執行載入動作時，列出的裝置將受到影響。
9. 說明 — 檢閱在推送設定時提供的任何資訊。
10. 重新整理 — 更新快照表格中的資訊。
11. 重設篩選器 — 清除所有篩選器以顯示所有設定版本。
12. 比較 — 查看不同版本有何變更。

    一次只能比較兩個版本。

 ©2025 Palo Alto Networks, Inc.

13.動作 — 您可以還原或載入設定版本。

- 還原 – 還原較早的設定版本。

  還原設定版本會直接更新原始推送範圍內的部署上正在執行的設定，您不需要推送設定。

  還原設定推送原始範圍內的所有裝置或部署，或選取要還原的特定裝置或部署。您無法擴展設定以納入原始範圍外的裝置或部署。

  還原設定版本並不會刪除或修改候選設定。正在進行的設定將被儲存。還原設定只會更新執行中的設定版本。使用還原動作時，部署可能會出現不同步的狀況。
- 載入 – 載入舊版本作為 Strata Cloud Manager 中的候選設定。載入較舊的設定時，您目前的候選設定將會遺失。

  對新的候選設定進行更新，或將設定套用至原始設定快照以外的新裝置和部署，並且準備就緒後推送設定。
- 儲存 – 將候選設定儲存為具名快照，以作為已知設定。有了已知設定，您即可輕鬆地使部署進入已知且可行的狀態。您可以在 **Named Snapshots**（具名快照）與 **Version Snapshots**（版本快照）中自動記錄的設定推送之間來回切換。

Strata Cloud Manager 最多可儲存 *6* 個月的快照，或 *200* 個快照。

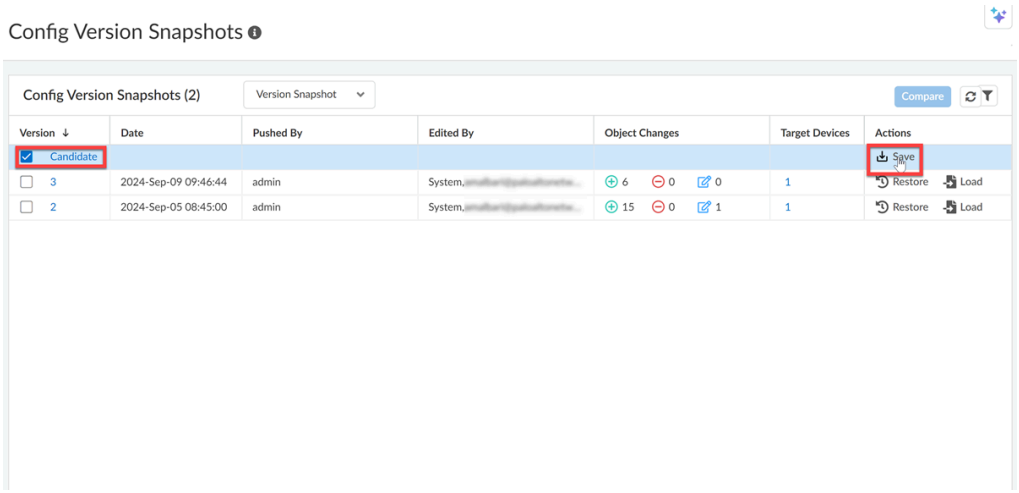
儲存具名快照

將目前的候選設定儲存為具名快照。您無法將部分設定儲存為具名快照。儲存具名快照可讓您載入已知的設定狀態，而無須追蹤最終將從設定版本快照表格循環的各個快照。

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取**Manage**（管理） > **Operations**（操作） > **Config Version Snapshots**（設定版本快照）。

STEP 3 | 選取 **Candidate**（候選項目）。

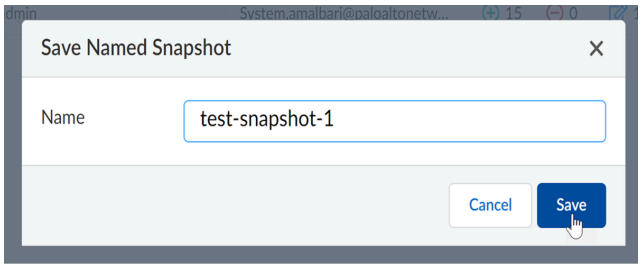


STEP 4 | 按一下 **Save**（儲存）。

 ©2025 Palo Alto Networks, Inc.

STEP 5 | 輸入最多 64 個字元的名稱。

快照的名稱將預設為 **config_year-month-day-timestamp**。

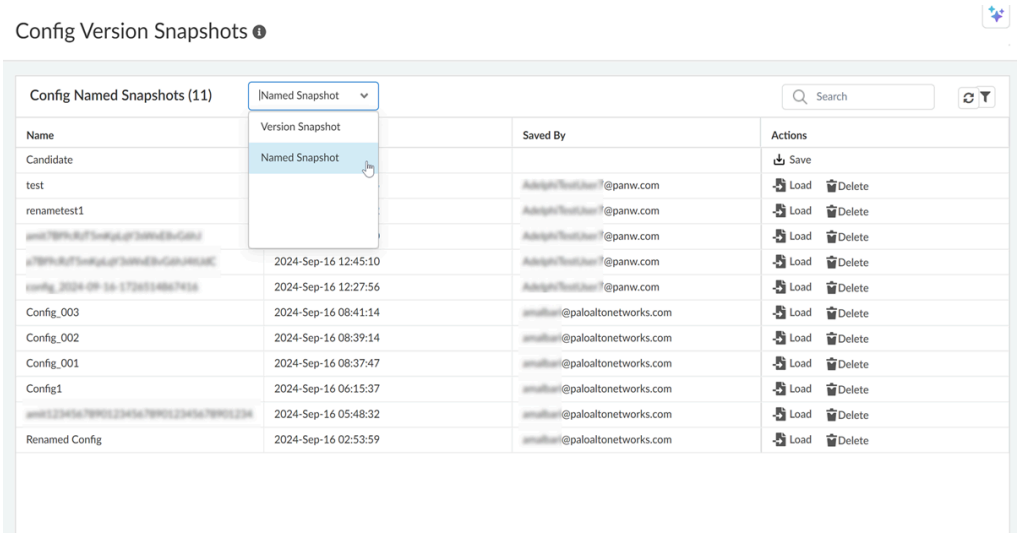


STEP 6 | 儲存您的快照。

STEP 7 | （選用）導覽至 [Config Snapshot Version（設定快照版本）] 表格中的 **Named Snapshots**（具名快照），確認您的快照已儲存。

管理具名快照

管理員可以刪除自己的具名快照。超級使用者可以刪除所有具名快照。



還原快照

還原先前推送的設定。還原較舊的設定，將會更新在部署和裝置上執行的設定。這些變更不會反映在 Strata Cloud Manager 中，因此部署和裝置可能會出現不同步的狀況。

只有在原始設定推送範圍內的已設定裝置，才能還原至選取的版本。

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取**Manage**（管理） > **Operations**（操作） > **Config Version Snapshots**（設定版本快照）。

STEP 3 | 選取您要還原的設定版本。

1. （選用）選取版本號碼以檢視設定快照所做的變更。

 ©2025 Palo Alto Networks, Inc.

STEP 4 | 還原版本。

1. （選用）選取您要對其執行還原動作的裝置。
2. 還原。

STEP 5 | （選用）選取 **Manage**（管理） > **Configuration**（設定） > **Operations**（操作） > **Push Config**（推送設定），以驗證設定已還原。

載入快照

載入較早的設定快照以作為候選設定。

設定載入後，您可以在推送之前對其進行修改。

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取**Manage**（管理） > **Operations**（操作） > **Config Version Snapshots**（設定版本快照）。

STEP 3 | 選取您要載入的設定版本。

1. （選用）選取版本號碼以檢視設定快照所做的變更。

STEP 4 | 載入版本。

STEP 5 | （選用）視需要修改已載入的候選設定。

STEP 6 | **Push Config**（推送設定）。

 ©2025 Palo Alto Networks, Inc.

管理：安全性狀態

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW，包括由軟體 NGFW 積分資助的項目	❑ 至少要有下列其中一個授權，才能使用 Strata Cloud Manager 管理您的設定；若要統一管理 NGFW 和 Prisma Access，您將同時需要： ❑ Prisma Access 授權 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能取決於您所使用的授權。

使用這些工具改善您的安全性狀態，並依照安全性政策最佳做法驗證您是否具備威脅防護。

- 為您的部署自訂安全性狀態檢查，以盡可能在 管理：安全性狀態設定 中提供相關建議
- 使用設定清理來識別及移除未使用的設定物件和政策規則。
- 設定合規性檢查，以完善和最佳化過於寬鬆的安全性規則，使其僅允許在您的網路中實際使用的應用程式。
- 建立您自己的 管理：安全性狀態設定 – 自訂現有的最佳做法檢查，並建立及管理特殊豁免，以妥善因應組織的業務需求。
- 使用政策分析器可快速確保您對安全性政策規則所做的更新會符合您的需求，並且不會產生錯誤或設定有誤（例如導致規則重複或衝突的變更）。

管理：政策分析器

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW（Panorama 管理） • VM-Series, funded with Software NGFW Credits（Panorama 管理） • Prisma Access (Managed by Panorama)	❑ 至少需要下列其中一個授權： ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro ❑ 用於 Panorama 管理部署的 Panorama CloudConnector 外掛程式

安全性政策規則的更新通常具有時效，需要您快速採取行動。但是，您需要確保對安全性政策規則庫所做的任何更新都符合您的需求，並且不會產生錯誤或設定有誤（例如導致規則重複或衝突的變更）。

為達此目的，Strata Cloud Manager 中的政策分析器可讓您在實施變更要求時，最佳化時間和資源。政策分析器不僅會分析並提供可能的合併或移除特定規則的建議，以滿足您的意圖，還會檢查規則庫中的異常情況，例如陰影、冗餘、一般化、相關性和合併。

使用政策分析器，來新增或最佳化您的安全性政策規則庫。

- 新增規則之前 - 請檢查是否需要新增規則。政策分析器會建議如何最好地變更現有的安全性政策規則，以滿足您的要求，且無需新增其他規則（如果可行的話）。
- 簡化和最佳化現有的規則庫 - 查看您可以在哪裡更新規則，以盡可能減少內容膨脹和消除衝突，並確保流量強制執行符合安全性政策規則庫的意圖。

在提交變更之前和之後，分析您的安全性政策規則。

- 變更前的政策分析 - 使您能夠評估新規則的影響，並根據現有規則分析新規則的意圖，以建議如何最適切地符合意圖。
- 變更後的政策分析- 使您能夠透過識別隨時間累積的影子、冗餘和其他異常，來清理現有的規則庫。

請參閱政策分析器以瞭解更多資訊。

©2025 Palo Alto Networks, Inc.

管理：原則最佳化工具

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW，包括由軟體 NGFW 積分資助的項目	❑ 至少要有下列其中一個授權，才能使用 Strata Cloud Manager 管理您的設定；若要統一管理 NGFW 和 Prisma Access，您將同時需要： ❑ Prisma Access 授權 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能取決於您所使用的授權。

趁著政策最佳化工具可供搶先存取時試用一下。如果您有興趣在搶先存取期間結束後繼續使用此功能，請與您的客戶團隊聯繫。

過於通泛的規則會引發安全漏洞，因為這類規則會允許您的網路中未使用的應用程式。政策最佳化工具可讓您將這些過於寬鬆的規則轉換為更具體、更有針對性的規則，而僅允許您實際使用的應用程式。

政策最佳化只會考量在過去 90 天以前建立的規則。

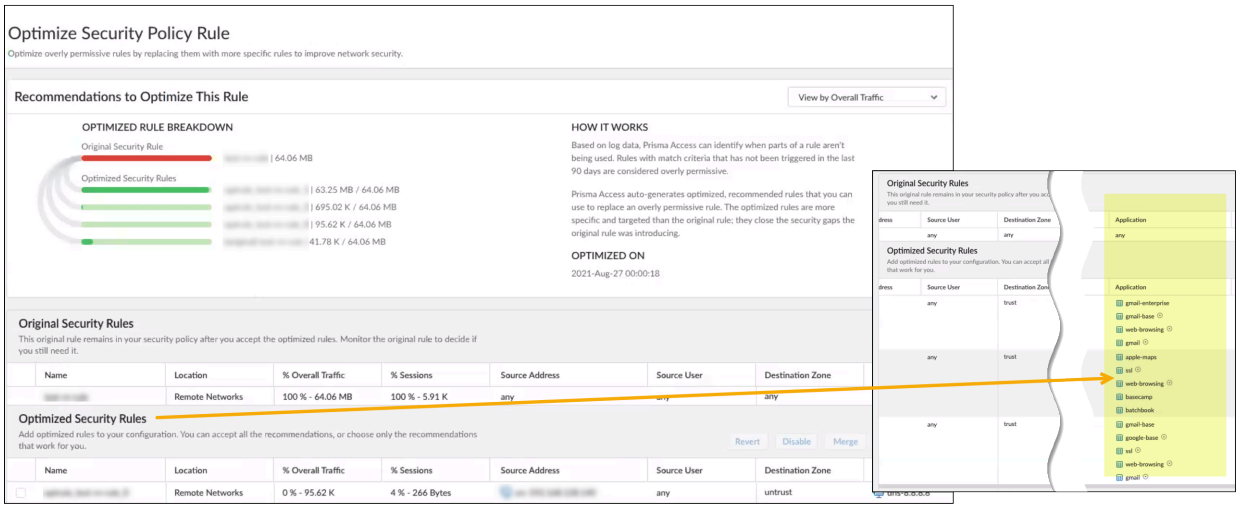
其運作方式為何

Strata Cloud Manager 會分析日誌資料，並在允許任何應用程式流量時將規則歸類為過於寬鬆，且規則必須至少已存在 90 天。如果這些規則允許對於企業使用而言不需要的流量，則可能會引發安全漏洞。

對於被認定為過於寬鬆的規則，Strata Cloud Manager 會自動產生可供您採用以最佳化規則的建議。新的建議規則比原有規則更具體且具針對性；會明確地僅允許過去 90 天內在您的網路中偵測到的應用程式。

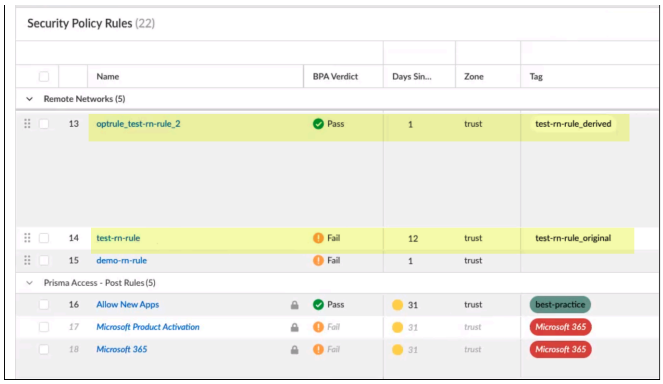
選取過於寬鬆的規則來檢閱、調整和接受最佳化建議。將這些規則取代為更具體的建議規則，以加強您的安全性狀態。

©2025 Palo Alto Networks, Inc.



接受最佳化規則的建議，並不會移除原始規則。原始規則仍會列在安全性政策中的新規則下方；這樣您就可以監控規則，並在您確信不需要時將其移除。

原始規則和最佳化規則都會標記，以便您可以在安全性政策中輕鬆加以識別：



最佳化規則

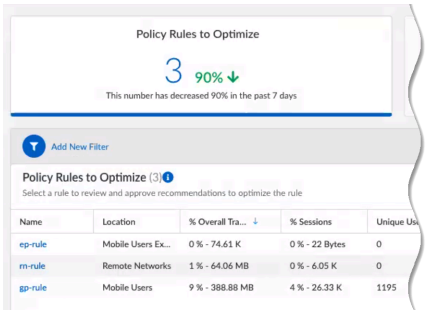
STEP 1 | 存取 **Config Cleanup**（設定清理），以查看是否有可以最佳化的規則。

移至**Manage**（管理） > **Security Posture**（安全性狀態） > **Policy Optimizer**（政策最佳化工具）。

 ©2025 Palo Alto Networks, Inc.

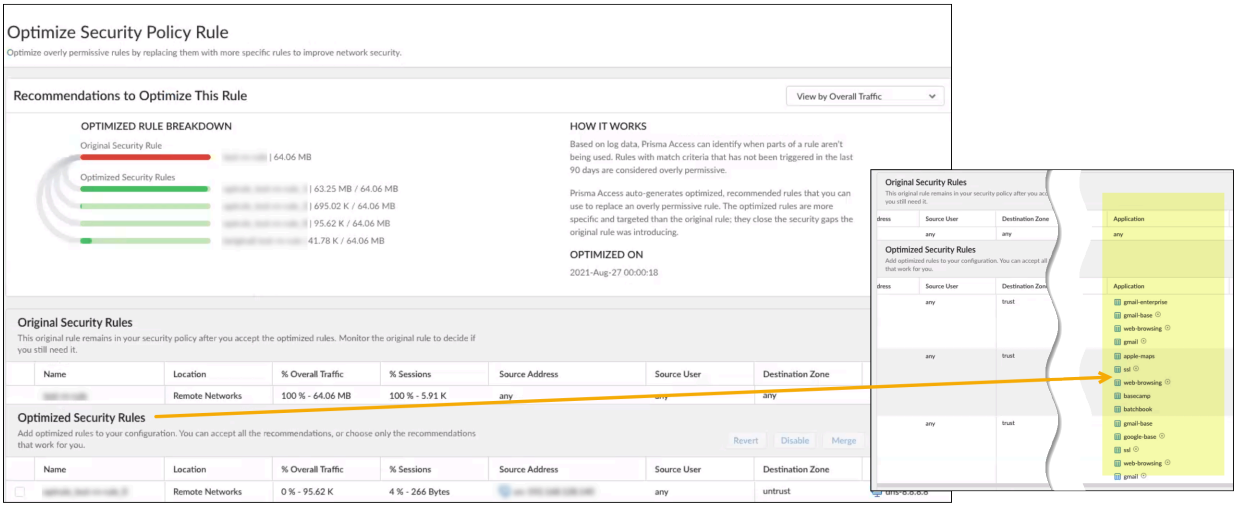
STEP 2 | 檢閱過於寬鬆的規則，並選擇一個規則以檢閱最佳化建議。

如果有多個過於寬鬆的規則，請著重於最佳化對流量影響最大的規則；這將使您對安全性狀態的強化帶來最顯著的好處。



STEP 3 | 檢閱建議的最佳化規則。

您可以查看每個新規則將覆蓋多少原始規則的流量。請注意每個新規則強制執行的特定應用程式。



STEP 4 | 接受部分或所有規則建議。

接受新的最佳化規則，會將規則新增到您的規則庫中。它們此時還不會作用；要等到您在下一個步驟中推送設定到 Prisma Access 時，才會開始作用。

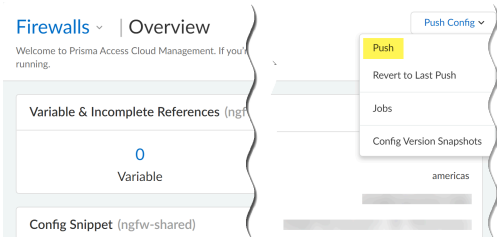
Accept All（全部接受）會按原狀接受建議的規則。您也可以在接受最佳化規則之前進行變更：

- 從最佳化中移除規則。將此規則新增至要排除於最佳化外的規則清單（這次和以後）。
- 停用最佳化規則。這意味著您不接受此規則，規則不會新增至規則庫。
- 還原您所做的任何變更。這會復原您所做的任何編輯，並將規則還原為建議。
- 合併規則。如果您發現任何相似的建議規則，就可能會決定將其合併。

接受最佳化規則後，系統會提示您更新規則庫。當您同意後，最佳化的規則會新增至您的安全性政策中。不過，此時還不會強制執行流量。

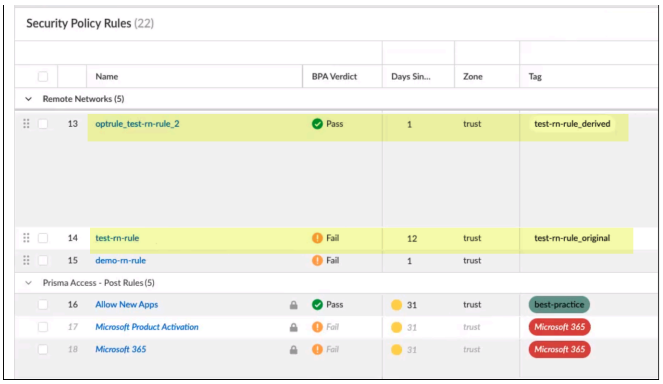
 ©2025 Palo Alto Networks, Inc.

STEP 5 | 推送設定以將設定更新傳送至 Prisma Access，並開始強制執行最佳化規則。



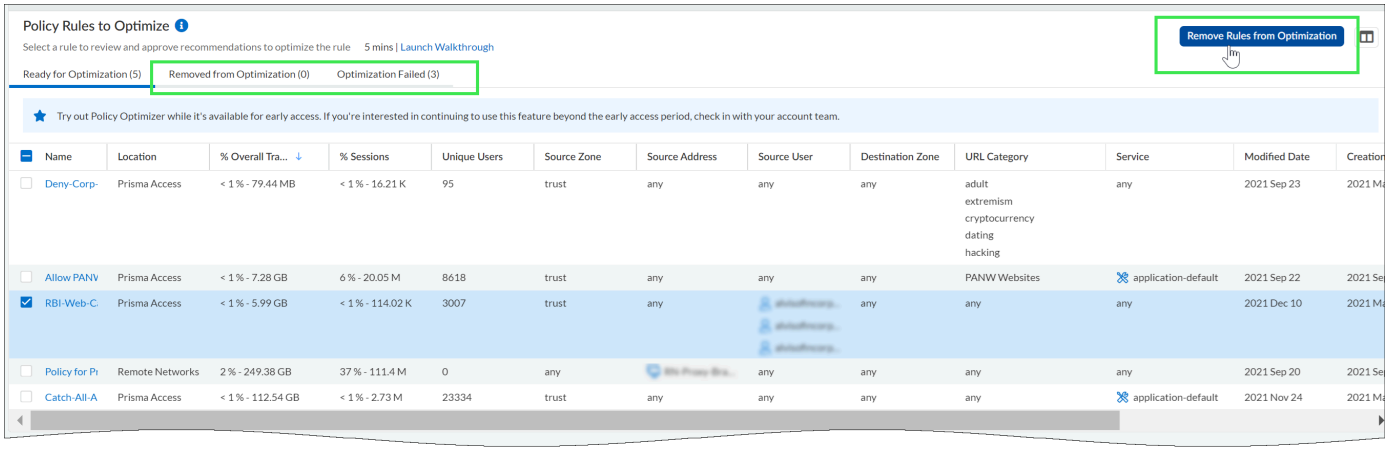
STEP 6 | 監控原始規則，直到您確信不需要該規則為止。

原有過於寬鬆的規則仍會保留在安全性政策中；它會列在規則庫中的最佳化規則下方，並帶有標籤，以便您輕鬆識別。標籤名稱將 _original 附加到規則名稱（例如 security-rule-name_original）。



將規則排除於最佳化外

將規則移至 **Excluded from Optimization**（排除於最佳化外）清單，Prisma Access 就不會對其進行最佳化。規則設定會保持原狀。



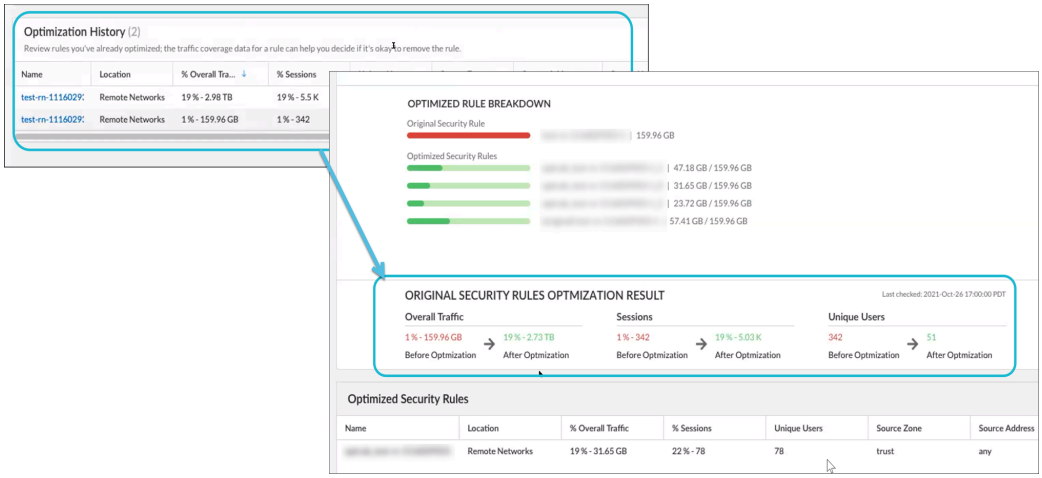
將規則移至排除清單後請務必推送設定；推送設定後，規則可能需要 24 小時才會顯示在清單中。後續您可以隨時選擇將規則新增回最佳化清單。

 ©2025 Palo Alto Networks, Inc.

追蹤最佳化結果

政策最佳化工具會顯示您已最佳化之安全性規則的歷程記錄。歷程資料包括最佳化結果：將原始規則的流量覆蓋範圍與最佳化規則進行比較。

您看到的 **Policy Optimizer History**（政策最佳化工具歷程記錄）資料是過去 30 天的資料。如果原始規則（您最佳化的規則）在六個月內未命中，則會從政策最佳化工具歷程記錄中移除，並且歸類為零命中政策規則。



 ©2025 Palo Alto Networks, Inc.

管理：設定清理

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW，包括由軟體 NGFW 積分資助的項目	❑ 至少要有下列其中一個授權，才能使用 Strata Cloud Manager 管理您的設定；若要統一管理 NGFW 和 Prisma Access，您將同時需要： ❑ Prisma Access 授權 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能取決於您所使用的授權。

使用設定清理，從您的 Strata Cloud Manager 設定中識別並移除未使用的設定物件和政策規則。移除未使用的設定物件可以避免混亂並且僅保留強制執行安全性所需的設定物件，從而簡化防火牆管理。

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取**Manage**（管理） > **Security Posture**（安全性狀態） > **Config Cleanup**（設定清理）。

STEP 3 | 選取您的整個 Strata Cloud Manager 設定中在過去 6 個月內未使用的物件和政策規則。

- 要最佳化的政策規則 — 按一下以檢閱過於寬鬆的政策規則，將這些規則轉換為更具體、更有針對性的規則，而僅允許您實際使用的應用程式。
- 未使用的物件（過去 **6** 個月） — 過去 6 個月內未在任何設定或政策規則中使用的所有設定物件。
- 零叫用物件（過去 **6** 個月） — 政策規則中收到零叫用的設定物件。

  此處僅列出在其相關聯的政策規則中收到零叫用的設定物件。使用這些物件，可能會在其使用所在的其他政策規則中收到叫用。
- 零叫用規則（過去 **6** 個月） — 在過去 6 個月沒有任何相符流量的所有政策規則。

©2025 Palo Alto Networks, Inc.

STEP 4 | 套用其他篩選器，將特定的未使用物件和政策規則定為目標。

未使用的物件（過去 **6** 個月）和零叫用政策規則（過去 **6** 個月）支援 **Add New Filter**（新增篩選器）。

- 未使用的物件（過去 **6** 個月） — 您可以根據下列條件來篩選及刪除未使用的物件：
  - 名稱 — 搜尋並選取特定的設定物件名稱。
  - 位置 — 建立設定物件名稱所在的設定範圍。
  - 物件類型 — 設定物件類型。
  - 未使用天數 — 設定物件未使用的天數。
    - **< 50** — 未使用的時間少於 50 天。
    - **>= 50, <=100** — 50 到 100 天未使用。
    - **> 50** — 超過 100 天未使用。
- 零叫用政策規則（過去 **6** 個月） — 您可以根據 **Name**（名稱）、**Days with Zero Hits**（零叫用天數）或任何來源和目的地資料來篩選及啟用、停用或刪除零叫用政策規則。

 ©2025 Palo Alto Networks, Inc.

管理：安全性狀態設定

這可在何處使用？	我需要哪些內容？
• NGFW，包括由軟體 NGFW 積分資助的項目 • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能，取決於您所使用的授權。

Strata Cloud Manager 會使用一組預先定義的最佳做法檢查，這些檢查符合產業特定的標準網路安全控制，例如 CIS (Center for Internet Security) 和 NIST（美國國家標準技術研究所），也符合您根據組織特定需求建立的自訂檢查。這些檢查評估雲端基礎架構內的組態和設定，識別與最佳做法或合規需求的偏差。

Strata Cloud Manager 中的安全性狀態檢查涵蓋一系列的安全領域，包括網路安全性、資料保護，以及識別與存取管理。這些檢查會評估防火牆規則、加密、驗證機制，以及設定的整體完整性。

當您的設定偵測到偏差時，Strata Cloud Manager 會提供可操作的洞察和修復建議，甚至可以自動執行某些部分的錯誤設定和不合規設定的更正程序，以協助您以最少的手動操作，維護安全且合規的雲端環境。

安全性狀態設定匯集了 AIOps 和 Strata Cloud Manager 安全性檢查設定頁面的功能。

選取**Manage**（管理） > **Security Posture**（安全性狀態） > **Settings**（設定），以檢視、管理和自訂部署的安全性狀態檢查，以盡可能提供相關建議。

©2025 Palo Alto Networks, Inc.

- 安全性檢查 – 用來評估設定的最佳做法檢查清單。

  您的設定將與這些檢查進行比較，以評估裝置的安全性狀態，並產生安全警示。您可以根據自己的環境執行下列動作，來管理這些檢查：

  1. 設定自訂檢查的嚴重性等級，以識別對您的部署而言最重要的檢查。

     您可以變更自訂檢查的嚴重性等級，但 *Palo Alto Networks* 最佳做法檢查的嚴重性等級是固定的，無法變更。

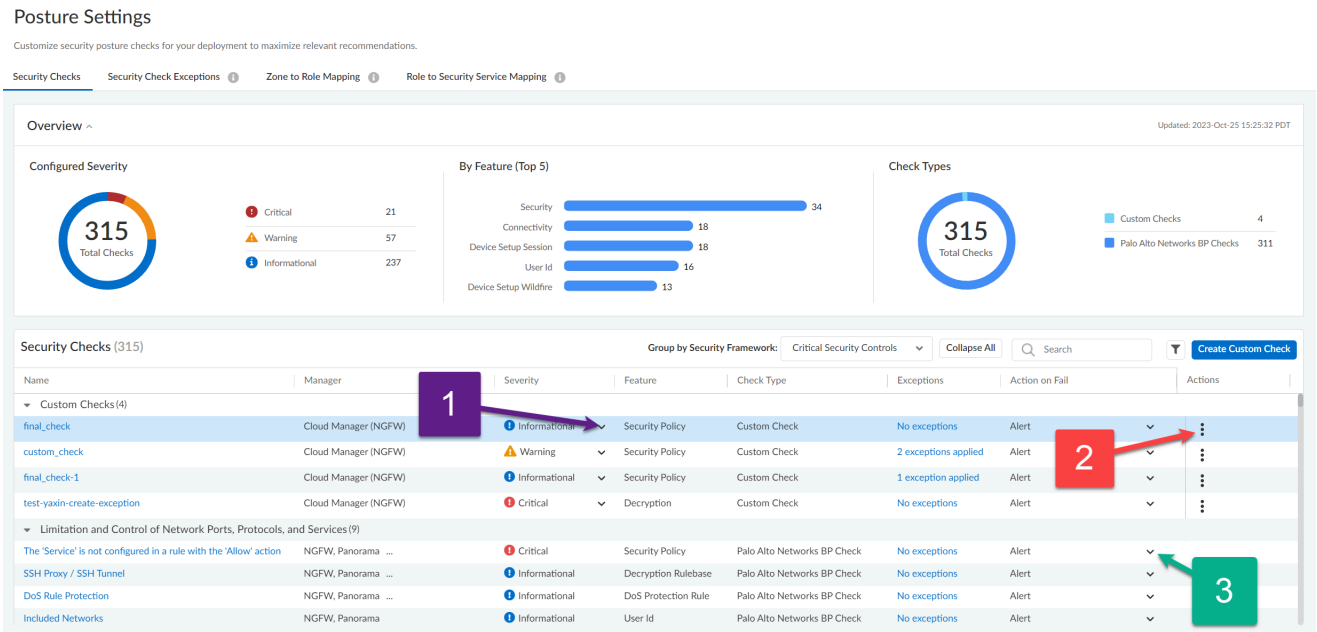
  2. 建立和刪除您自己的自訂檢查，複製和編輯現有檢查以建立新檢查，並針對您不希望套用至部分部署的檢查設定特殊例外。

     初始部署這些檢查的過程中，您可以複製自訂檢查架構中的檢查。

  3. 設定檢查失敗時的回應。
     - 警示（預設值）— 針對失敗的檢查引發警示。
     - 封鎖— 在潛在的錯誤設定進入您的部署之前加以阻止。封鎖可能意味著以下任何一種情況，具體取決於您的管理方式：
       - **Strata Cloud Manager** 上的內嵌檢查 - 阻止您認可或推送不合規的設定，但不會阻止您在本機上儲存設定。
       - **Strata Cloud Manager** 上的即時*內嵌檢查— 進一步阻止您儲存不合規的設定。
       - **Panorama** 管理**— 阻止您將不合規的設定認可到 Panorama，但不會阻止您將其儲存到 Panorama 候選設定。
       - PAN-OS 網頁介面、API 或 CLI 管理 - 設定若未受到雲端管理或 Panorama 管理，封鎖將沒有強制執行效果。

     - *由於邏輯較為複雜，某些內嵌檢查按固定排程非同步執行，而不是即時執行。如果設定中的即時檢查失敗，您將無法儲存該設定，連在本機都不行。
     - **需要 Panorama CloudConnector 外掛程式，才能在 *Panorama* 上強制執行封鎖認可動作。

 ©2025 Palo Alto Networks, Inc.



- 安全性檢查例外

  為您指定的裝置或裝置群組關閉個別檢查。
- 區域到角色的對應

  將 NGFW 中的區域對應到角色，以獲得自訂建議。
- 角色到安全服務的對應

  管理所有 NGFW 中，區域和角色之間的流量所需的安全服務。

建立自訂檢查

從現有的檢查建立您自己的自訂檢查。或者，跳到步驟 #4 從頭開始建立自訂檢查。

STEP 1 | 選取 **Manage**（管理） > **Security Posture**（安全性態勢） > **Settings**（設定）。

STEP 2 | 識別您要複製的檢查，然後進行複製。

STEP 3 | 編輯您所複製的檢查，然後跳到步驟 #5 進行變更。

STEP 4 | 移至**Manage**（管理） > **Security Posture**（安全性狀態） > **Settings**（設定），然後選取 **Create Custom Check**（建立自訂檢查）。

STEP 5 | 為您的檢查指定一般資訊。您的自訂檢查必須具有名稱和說明，但您也應為檢查新增建議和理由，以協助其他人瞭解自訂檢查的意圖和最佳做法。

STEP 6 | 選用 選取物件類型– 您要為其建立檢查的設定部分，可確認您在建立檢查時可以選擇哪些要比對的規則屬性。

 ©2025 Palo Alto Networks, Inc.

STEP 7 | 對您的自訂檢查使用邏輯建立器。

1. 新增運算式– 說明設定比對準則的單行邏輯。

要比對的規則屬性	比對運算子	特定準則
• 一般 — 名稱、說明、位置和排程 • 來源 — 區域、位址、使用者 • 目的地 – 區域和位址 • 應用程式、服務和 URL • 動作和進階檢查	• 是 • 不是 • 為空 • 不為空 • 開頭為 • 結尾為 • 包含 • 大於 • In • 等於或大於 • 等於或小於 • 少於 • 等於 • 不等於 • 不包含 • 所有的 • 部分 • 沒有任何	[文字欄位]

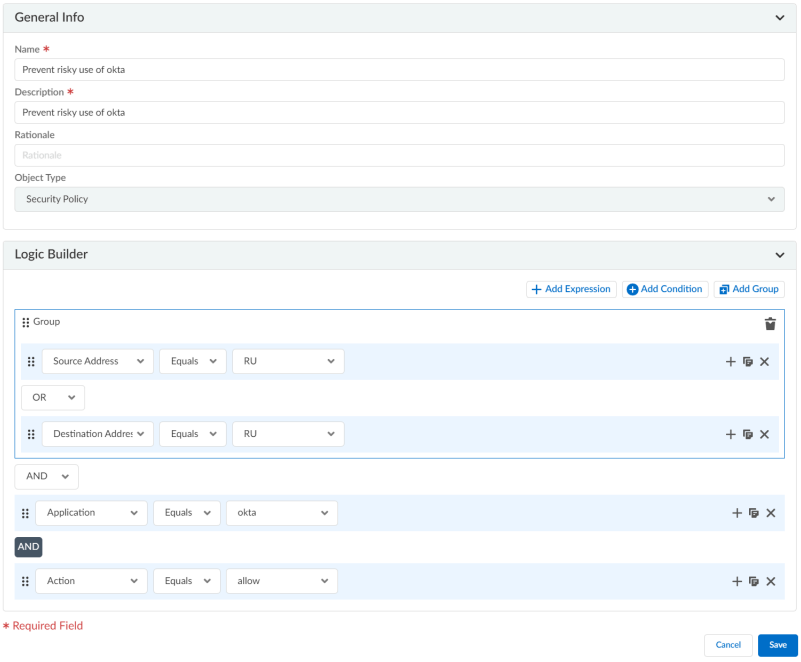
2. 新增條件– 使用邏輯運算子（例如 AND、OR、IF、THEN、ELSE 和 ELSE IF）連接或結合運算式、附加條件和群組。

 ©2025 Palo Alto Networks, Inc.

3. 新增群組– 建立一組運算式和（或）條件。搭配此群組，可產生 True 或 False 條件。

   - 新增運算式或條件
   - 複製運算式或條件
   - 移除運算式或條件

   此範例中的運算式在發現有政策規則允許 Okta 流量進出 Russian IP 位址時，會發出警告。此範例旨在說明邏輯建立器的運作方式，並不提供建議。



STEP 8 | 儲存您的檢查。

管理您的檢查

您可以對安全性檢查執行下列任何動作：

- 複製* – 建立檢查的複本。
- 編輯** – 對現有的自訂檢查進行變更。
- 移除** – 移除您建立的自訂檢查。

選取您要對其執行動作的檢查，並選取適當的動作。

- *您一次只能複製一個檢查。
- **您只能編輯或刪除自訂檢查。
- 您可能需要獲得管理員的許可，才能編輯自訂檢查。

建立檢查的例外

如有需要，您可以限制在部署中套用檢查的位置。

 ©2025 Palo Alto Networks, Inc.

STEP 1 | 選取 **Manage**（管理） > **Security Posture**（安全性狀態） > **Settings**（設定） > **Security Check Exceptions**（安全性檢查例外）和 **Create Security Check Exception**（建立安全性檢查例外）。

或者，選取**Manage**（管理） > **Security Posture**（安全性狀態） > **Settings**（設定），然後識別要排除的檢查並加以選取（**Exceptions**（例外）欄）。

STEP 2 | 指定為您的檢查建立例外規則所需的資訊。提供例外的名稱、原因和條件。

Security Check Exception（安全性檢查例外）功能目前僅適用於警示，以及 ***Best Practices***（最佳做法）和 ***Security Posture Insights***（安全性狀態洞察）儀表板。

STEP 3 | 選用 為您的例外新增票證號碼或說明，以協助其他人瞭解您的例外背後的意圖和歷程記錄。

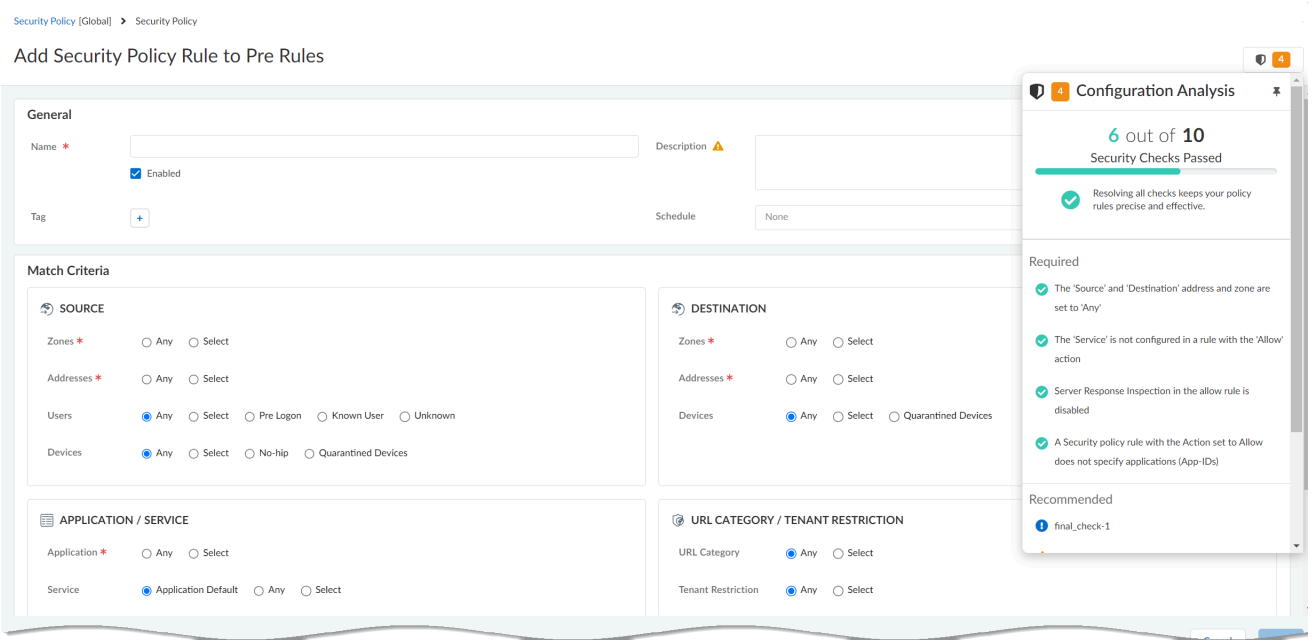
STEP 4 | 儲存您的例外。

您的有效檢查

實地檢查可指出您的設定與最佳做法或自訂檢查的不符之處。檢查會提供內嵌的最佳做法指引，以便您能夠立即採取行動。

您也可以就地檢視和管理安全性檢查。

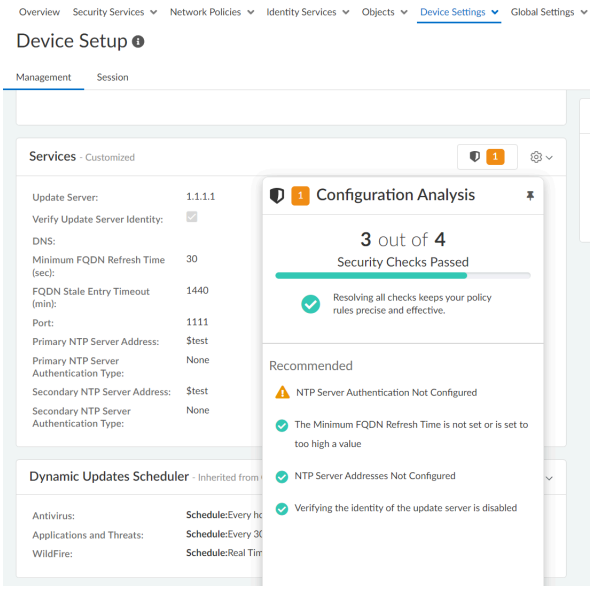
- 建立和管理您的政策規則– 安全性政策規則可讓您強制執行規則並採取行動，並且可視需要設為一般或具體。(**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服務） > **Security Policy**（安全性政策）)



- Setup Devices（設定裝置）– 針對防火牆的管理和輔助介面設定服務路由、連線設定、允許的服務，以及管理存取設定。(**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma**

 ©2025 Palo Alto Networks, Inc.

Access（**NGFW** 和 **Prisma Access**） > **Device Settings**（裝置設定） > **Device Setup**（裝置設定）)



如果您嘗試儲存的設定未通過您的準則，您可以選擇修復問題，或覆寫* 警告並儲存您的變更。

- *覆寫權限由角色型存取控制 (RBAC) 控管，且必須為您的角色啟用，此選項才會顯示。與覆寫、自訂檢查和異常相關的動作，都會記錄在稽核日誌中：***Incidents and Alerts**（事件和警示）**Log Viewer**（日誌檢視器）稽核 (日誌類型)。
- 您對自訂檢查、覆寫和例外所做的所有操作，都會記錄在稽核中：***Incidents and Alerts***（事件和警示） > ***Log Viewer***（日誌檢視器） > 稽核 (日誌類型)。

©2025 Palo Alto Networks, Inc.

管理：存取控制

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW，包括由軟體 NGFW 積分資助的項目	❑ 至少要有下列其中一個授權，才能使用 Strata Cloud Manager 管理您的設定；若要統一管理 NGFW 和 Prisma Access，您將同時需要： ❑ Prisma Access 授權 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro ❑ 軟體 NGFW 積分 （適用於 *VM-Series* 軟體 *NGFW*） → 您可以在 Strata Cloud Manager 中使用的特性和功能取決於您所使用的授權。

以角色為基礎的存取控制 (RBAC) 可讓您定義每位管理使用者（管理員）應有的權限與責任。每個管理員都必須有指定角色和驗證方法的使用者帳戶。Prisma Access 雲端管理可實作自訂 RBAC，使您能夠管理角色或特定權限，以及將存取權限指派給管理使用者。使用 RBAC，您可以在雲端管理內管理使用者及其對各種資源的存取。

SaaS 安全性內嵌和行為威脅不支援 *RBAC*。所有使用者都可以看到 ***Discovered Apps***（探索到的應用程式）和 ***Behavior Threats***（行為威脅）底下的所有頁籤，無論其指派的角色為何。

更多 ***RBAC*** 資源

- 誰可以使用常見服務：識別與存取：雲端管理 Prisma Access
- 常見服務的一般流程為何：識別與存取
- 關於透過常見服務的角色和權限

管理員角色

Prisma Access 的使用者是指被指派了管理權限的人，而角色會定義管理員對服務具備的存取類型。在指派角色時，您會指定管理員可管理的權限群組和帳戶群組。針對使用 Prisma Access 的管理員，中樞提供了下列內建權限群組。

- 應用程式管理員 - 具有對給定應用程式的完整存取權，包括未來新增至應用程式的所有執行個體。應用程式管理員可為應用程式執行個體指派角色，也可以啟動該應用程式特定的應用程式執行個體。
- 執行個體管理員 — 具有指派此角色的應用程式執行個體的完整存取權。「執行個體管理員」也可以將其他使用者設為應用程式執行個體的「執行個體管理員」。如果應用程式具有預先定義或自訂角色，則執行個體管理員可以將這些角色指派給其他使用者。
- 超級讀者 — 可以檢視所有設定元素、日誌和設定。超級讀者無法變更其他設定。
- 稽核管理員 — 只能檢視及管理日誌和日誌設定。稽核管理員無法變更其他設定。
- 加密管理員 — 可以檢視日誌及管理加密設定，例如 IKE、IPSec、主要金鑰管理和憑證設定。加密管理員無法檢視或變更其他設定。
- 安全性管理員 — 可以檢視日誌，以及管理除加密管理員角色可用的加密設定以外的所有設定。
- **Web** 安全性管理員 — 只能檢視與 Web 安全性相關的設定元素。
- 資料遺失防護管理員 — 可以存取企業 DLP 設定，但無法將設定變更推送至 Prisma Access。
- 資料安全性管理員 — 可以存取企業 DLP 和 SaaS 安全性控制，但無法將設定變更推送至 Prisma Access。
- **SaaS** 管理員 — 可以存取 SaaS 安全性設定，但無法將設定變更推送至 Prisma Access。

©2025 Palo Alto Networks, Inc.

自訂角色型存取控制 — 設定

以下說明如何使用預先定義角色或建立自訂角色、將角色指派給使用者，以及在存取 Prisma Access 應用程式時管理使用者範圍。

STEP 1 | 透過常見服務新增自訂角色

如果您需要的存取控制比預先定義的角色提供的更精細，您可以新增自訂角色，以定義要為使用者強制執行哪些權限。與預先定義的角色類似，自訂角色是一組權限和權限集。不同於預先定義的角色，每個自訂角色只能指派給階層中該角色定義所在的租用戶服務群組 (TSG) 下的使用者。這樣可以避免不同客戶定義的自訂角色因命名類似而發生名稱衝突。

如果您在階層的最上層（父系）新增自訂角色，該角色將會指派給內嵌於下方的租用戶，讓父租用戶可以管理子租用戶。

STEP 2 | 透過常見服務新增使用者存取權

常見服務：存取與識別可讓您新增對平台以及您所建立的租用戶的使用者存取權。

STEP 3 | 透過常見服務將預先定義的角色指派給租用戶使用者或服務帳戶

如果您已新增使用者，並想要新增其他角色，您也可以指派一批預先定義的角色。檢視關於角色和權限的其他資訊。

STEP 4 | 在 Prisma Access 雲端管理 UI 中建立新範圍

Prisma Access 雲端管理可讓您（以管理員身分）將管理範圍指派給雲端管理使用者（非管理員），以根據資料夾和程式碼片段等範圍產生權限的關聯。

權限是系統中允許的動作。權限代表一組您用來讀取、寫入和刪除系統內物件的特定應用程式開發介面 (API) 呼叫。所有權限都會按角色分組。

©2025 Palo Alto Networks, Inc.

管理：範圍管理

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW，包括由軟體 NGFW 積分資助的項目	❑ 至少要有下列其中一個授權，才能使用 Strata Cloud Manager 管理您的設定；若要統一管理 NGFW 和 Prisma Access，您將同時需要： ❑ Prisma Access 授權 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能取決於您所使用的授權。

設定範圍管理以強制執行自訂角色型存取控制。這允許您指定哪個 Strata Cloud Manager 管理員可以存取和修改特定資料夾、防火牆、Prisma Access 部署與片段設定。為雲端管理員定義範圍管理，可確保他們不會過度佈建，並且可定義選取的資料夾、防火牆、Prisma Access 部署和片段設定。常用服務多平台和企業角色可用來定義 Strata Cloud Manager 管理員的讀寫和寫入存取權限。

範圍管理設定會定義於整個 Strata Cloud Manager 租用戶。您無法為特定資料夾 Prisma Access 或防火牆設定範圍定義範圍管理。

只有「雲端管理」管理員或超級使用者才能建立範圍物件。範圍管理 *Widget* 不適用於具有其他角色的使用者。

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取 **Manage**（管理） > **Access Control**（存取控制） > **Scope Management**（範圍管理）。

STEP 3 | 建立新範圍。

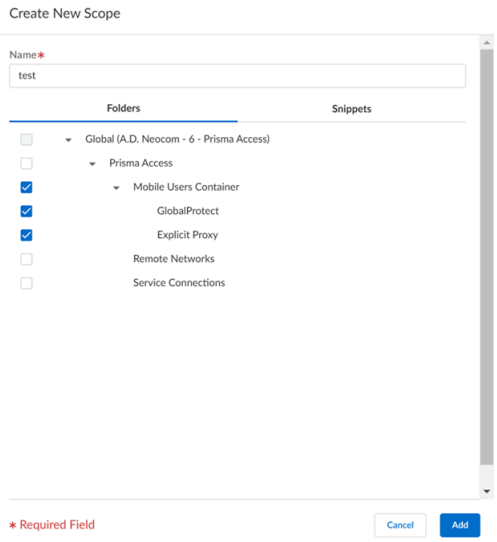
©2025 Palo Alto Networks, Inc.

STEP 4 | 定義範圍管理設定。

範圍管理設定會標記為範圍物件。

1. 輸入描述性的 **Name**（名稱）。
2. 選取 **Folders**（資料夾），然後勾選（啟用）要包含在範圍內的資料夾、防火牆和 Prisma Access 部署。

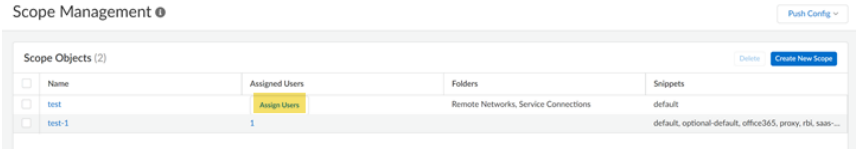
   選取防火牆時，也包含範圍管理設定中與所選防火牆相關聯的資料夾。只會包含直接關聯的資料夾，不會包含父資料夾。
3. 選取 **Snippets**（片段），然後勾選（啟用）您要包含的片段。
4. 新增範圍物件。



 ©2025 Palo Alto Networks, Inc.

STEP 5 | 將範圍管理設定套用至 Strata Cloud Manager 管理員。

1. 指派使用者給您在先前的步驟中建立的範圍物件。



2. 選取 Strata Cloud Manager 管理員的角色。例如，您可以為需要存取所有租用戶的所有功能的使用者選取 MSP 超級使用者。

   預設值為 None（無）。如需與每個可用角色的讀取和寫入存取權限有關的詳細資訊，請參閱常用服務多平台和企業角色。

   選取特定的 *Strata Cloud Manager* 管理員和 ***Clear Role***（清除角色），以移除目前指派的常見服務角色。這會將預設的無角色套用至管理員。

3. 若要修改現有範圍以編輯名稱，以及新增或移除資料夾，請選取範圍物件、視需要修改範圍，然後更新範圍。
4. 若要修改已指派的使用者，以新增更多使用者或變更使用者，請按一下 **Assigned Users**（已指派的使用者）並視需要進行修改，然後關閉視窗。

©2025 Palo Alto Networks, Inc.

管理：IP 限制

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW，包括由軟體 NGFW 積分資助的項目	❑ 至少要有下列其中一個授權，才能使用 Strata Cloud Manager 管理您的設定；若要統一管理 NGFW 和 Prisma Access，您將同時需要： ❑ Prisma Access 授權 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro → 您可以在 Strata Cloud Manager 中使用的特性和功能取決於您所使用的授權。

指定 Prisma Access 雲端管理管理員的可信任 IP 位址。只有從這些來源 IP 位址登入（並且成功通過驗證）的管理員，才能存取 Prisma Access 雲端管理。

IP 位址必須是公用位址。依預設不會強制執行任何受信任的位址（清單設定為 **any**（任何））。

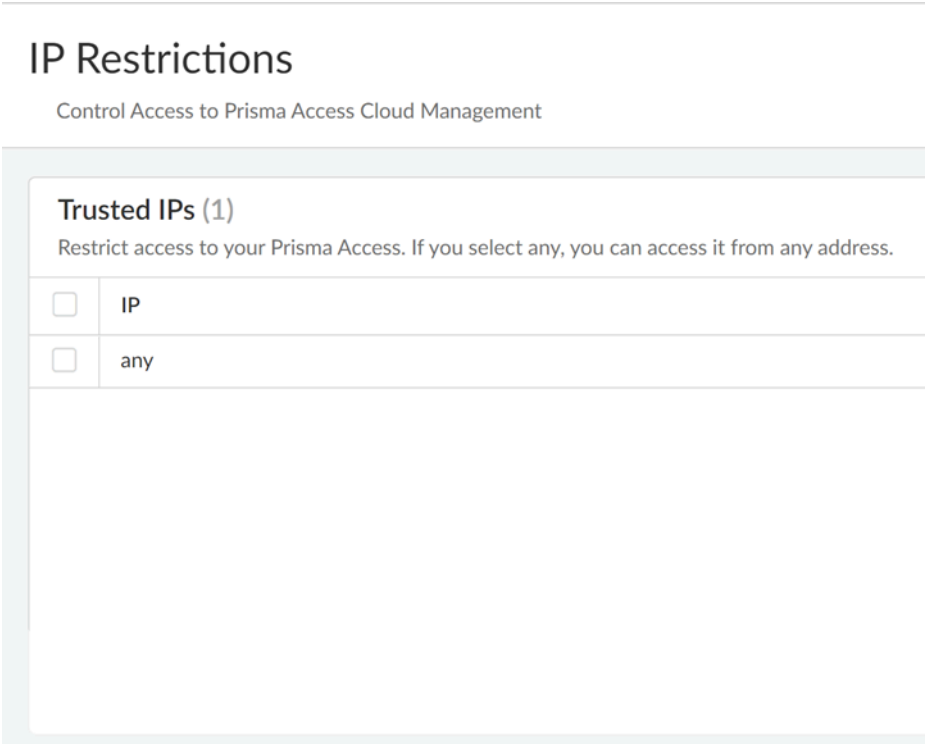
首先，請移至 **Manage**（管理） > **Access Control**（存取控制） > **IP Restrictions**（**IP** 限制）。

對於 IP 限制，不支援子網路位址。僅支援 IP 位址和 IP 位址範圍。請勿指定與下列 IP 位址和子網路重疊的任何子網路，因為 Prisma Access 會保留這些 IP 位址和子網路供內部使用：

- 169.254.169.253 和 169.254.169.254
- 100.64.0.0/10
- 169.254.201.0/24
- 169.254.202.0/24

建議使用符合 RFC 1918 和 RFC 6598 的 IP 位址集區。雖然使用不符合 RFC 1918 和 RFC 6598 的（公用）IP 位址是可行的，但我們不建議這麼做，因為可能會與網際網路公用 IP 位址空間發生衝突。

©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

工作流程：Strata Cloud Manager

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager) • Prisma SD-WAN	以下一或多個授權，具體取決於工作流程： ❑ AIOps for NGFW Premium 授權 ❑ 記錄需要 Strata Logging Service 授權 ❑ Prisma Access 授權 ❑ Prisma SD-WAN ❑ 遠端瀏覽器隔離授權

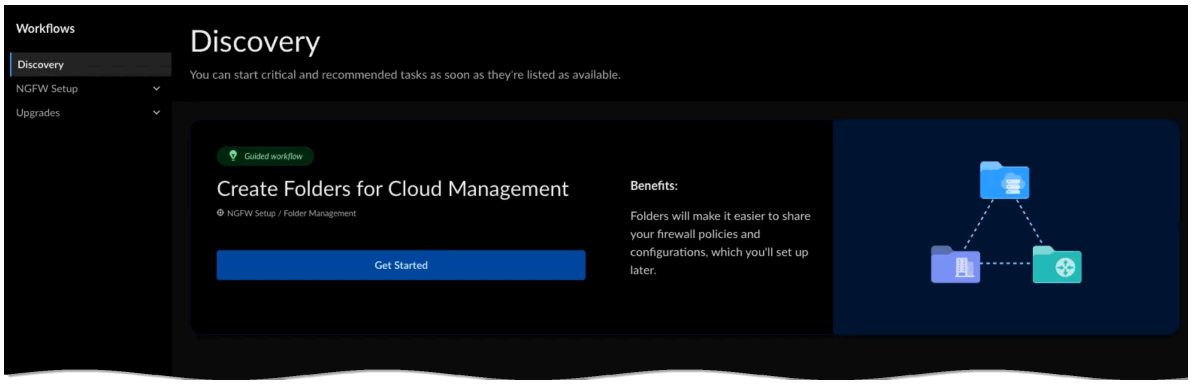
當您首次導覽至工作流程時，**Discovery**（探索）儀表板會在有關鍵和建議的動作可供您執行以改善安全性狀態或最佳化設定管理時，立即加以顯示。繼續在此處設定及上線 NGFW 和 Prisma Access 行動使用者與遠端網路，並規劃 NGFW 的軟體升級。

- 探索上線工作
- 設定 Prisma Access
- 設定 NGFW
- 設定 Prisma SD-WAN
- 軟體升級 (NGFW)
- 軟體升級 (Prisma Access)

工作流程：探索

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager) • Prisma SD-WAN	❑ AIOps for NGFW Premium 授權或 Prisma Access 授權

「探索」是您在重要和建議工作可用時可隨即加以啟動的位置。可能有一些引導式工作流程或工作是您可以自行完成的。在此主題中，我們將說明如何使用引導式工作流程建立資料夾結構並為其指派裝置，既輕鬆又直觀。



依照下列步驟為您的防火牆建立資料夾：

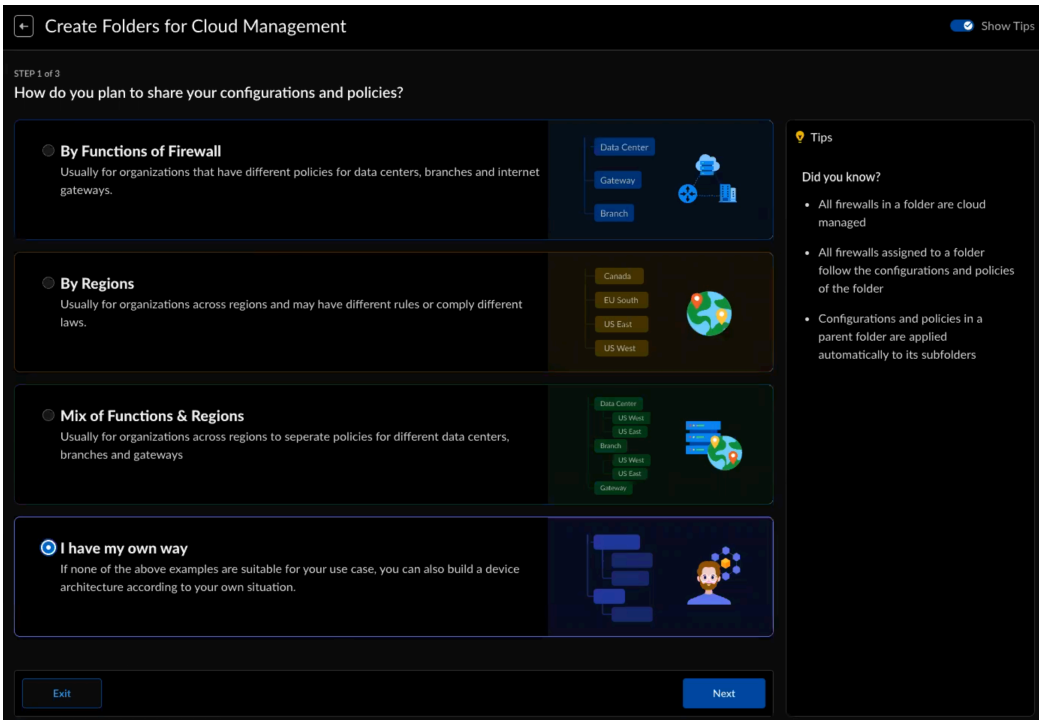
STEP 1 | 移至**Workflows**（工作流程） > **Discovery**（探索），然後選取 **Get Started**（開始使用）。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 選擇您要共用政策規則和設定的方式。

- 按防火牆的功能 – 您的組織是否對資料中心、分支和網際網路閘道使用不同的政策？這可能是適合您的選項。
- 按區域 – 您的組織是否跨越具有不同規則或遵守不同法律的區域？請考慮使用此選項。
- 功能與區域的混合 – 您的跨區域組織是否希望對不同的資料中心、分支和網際網路閘道使用不同的政策？您可以試試此選項。
- 我有自己的方式 – 如果以上範例都不符合您的使用案例，您也可以根據自己的情況建置裝置架構。

在此範例中，我們將選擇 **I have my own way**（我有自己的方式）選項。



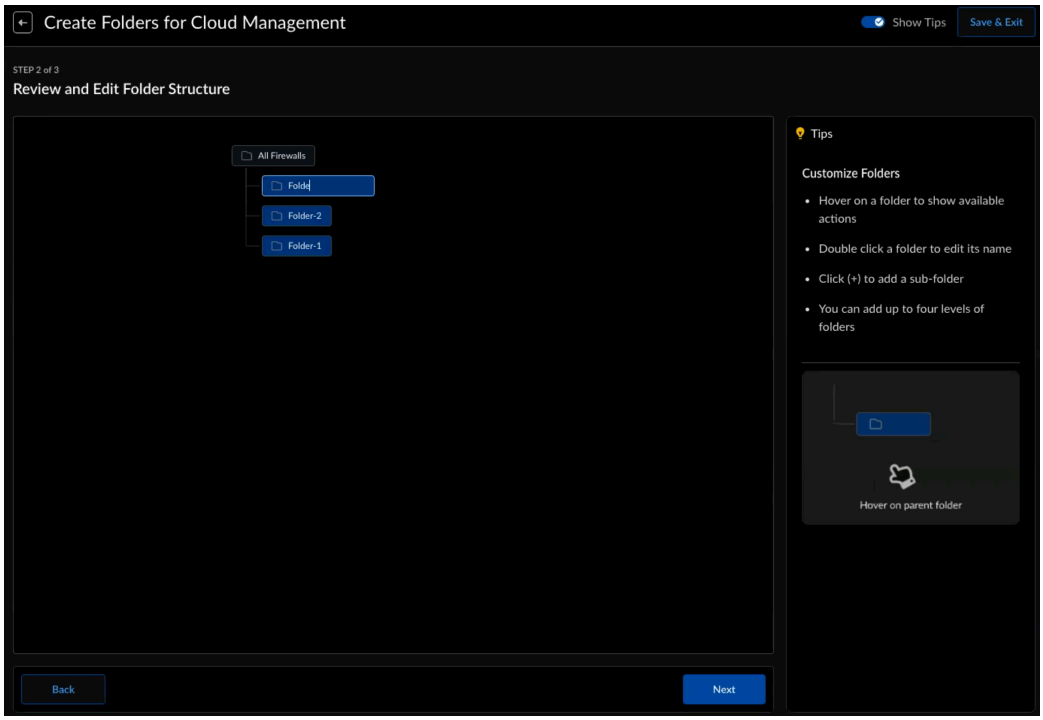
開啟 ***Show Tips***（顯示提示），查看可協助您做出明智決策的提示。

STEP 3 | 選取 **Next**（下一步）以建置資料夾結構。

 ©2025 Palo Alto Networks, Inc.

STEP 4 | 使用下列動作，根據您在步驟 1 中選取的範本建置資料夾結構。您可以：

- 新增新資料夾 – 將游標暫留在資料夾上方，顯示新增資料夾的選項。按一下 ，然後為您的新資料夾命名。
- 刪除資料夾 – 將游標暫留在資料夾上方，顯示刪除資料夾的選項。選取 以刪除資料夾。
- 重新命名資料夾 – 按兩下資料夾，為該資料夾鍵入新名稱。按 **Enter** 鍵或按一下文字欄位外部，使新名稱生效。
- 展開或摺疊具有子系的資料夾節點。



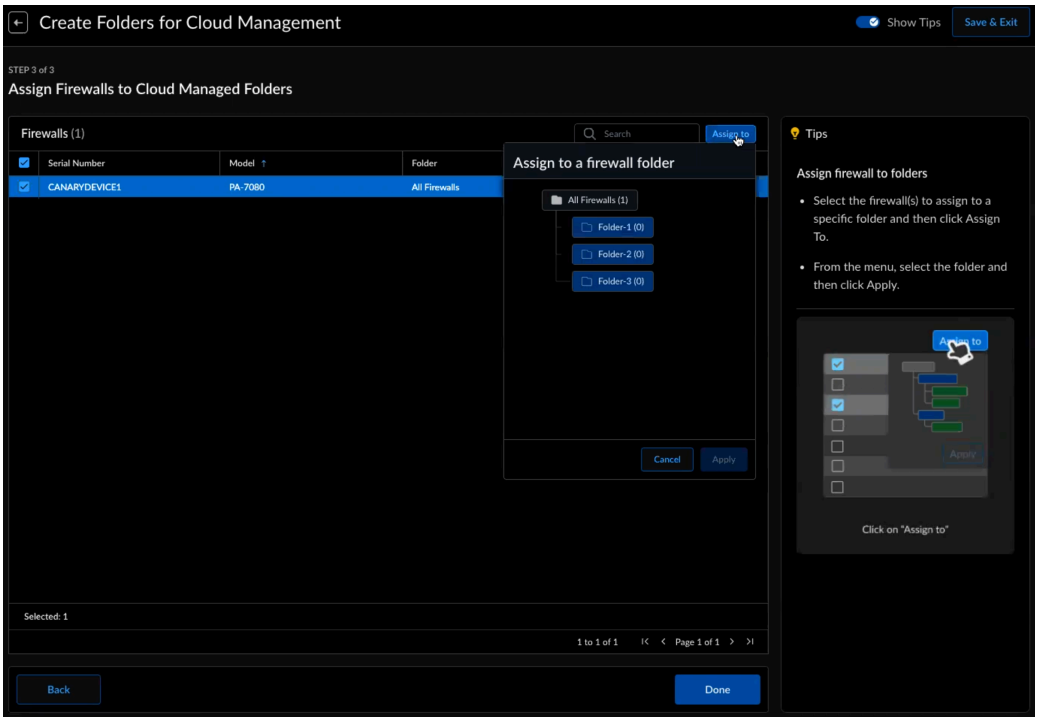
- 資料夾樹狀結構最多可以有四個層級。
- 最上層資料夾無法刪除或重新命名。
- 查看 *[Tips*（提示）*]*，以獲取關於特定資料夾動作的提示。
- 我們將儲存您的工作，您可以隨時退出，稍後再回來。

STEP 5 | 選取 **Next**（下一步），將防火牆指派給資料夾。

STEP 6 | 在此清單中選取一或多個防火牆。

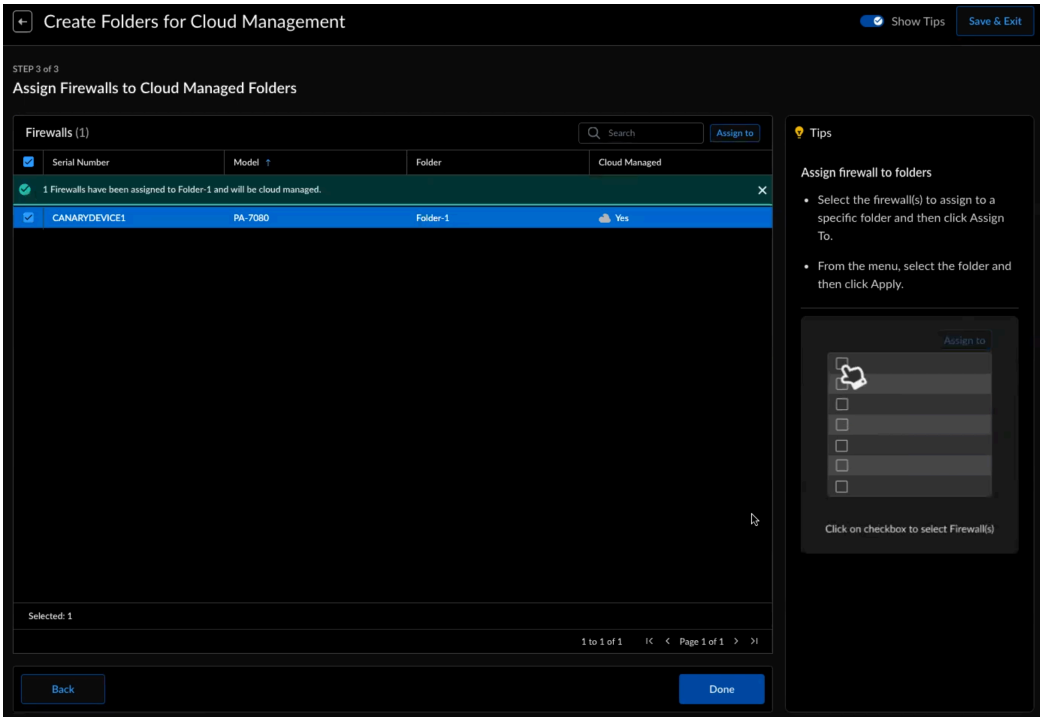
 ©2025 Palo Alto Networks, Inc.

STEP 7 | 選取 **Assign To**（指派給），選擇防火牆要指派到的資料夾，然後選取 **Apply**（套用）。您指派給 **Cloud Managed**（雲端管理）資料夾的防火牆，會啟用雲端管理。

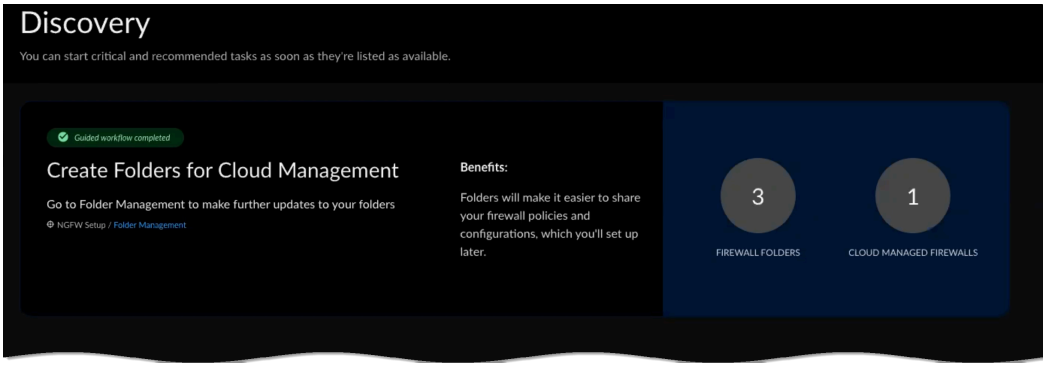


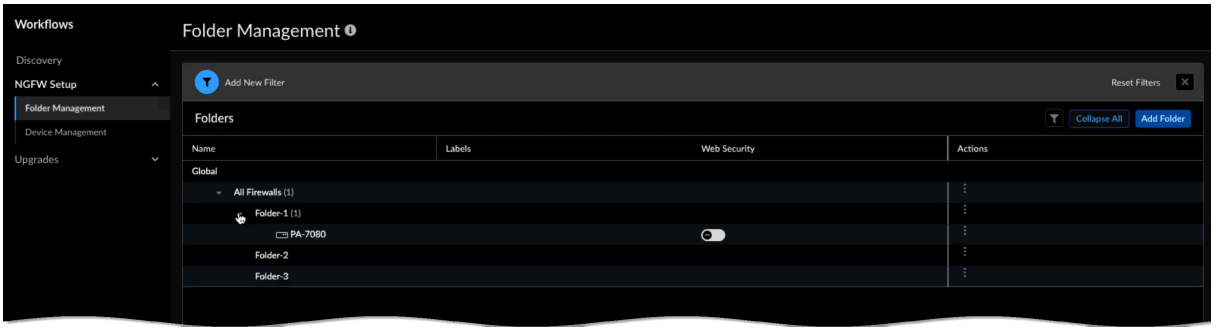
 ©2025 Palo Alto Networks, Inc.

STEP 8 | 確認您的指派並選取 **Done**（完成）。



您會在主要 **Discovery**（探索）頁面上以及**NGFW Setup**（**NGWF** 設定） **> Folder Management**（資料夾管理）頁籤底下看到您建立的資料夾和您指派的防火牆。





 ©2025 Palo Alto Networks, Inc.

工作流程：NGFW 設定

這可在何處使用？	我需要哪些內容？
• NGFW (Managed by Strata Cloud Manager)	❑ NGFW 的雲端管理需要 AIOps for NGFW Premium 授權 ❑ 記錄需要 Strata Logging Service 授權 ❑ 如果您擁有 Prisma Access 授權，則可以使用 **Folder Management**（資料夾管理）來檢視預先定義的資料夾，並為資料夾啟用 Web 安全性

為雲端管理設定 NGFW 的過程中，您必須將 將新世代防火牆上線至 Strata Cloud Manager。上線作業包括設定資料夾以對需要類似設定的防火牆進行分組。進一步瞭解 工作流程：資料夾管理，然後使用 **Device Management**（裝置管理）頁面檢視資料夾階層中所有裝置的詳細資料。

STEP 1 | 啟動 Strata Logging Service 和 AIOps for NGFW Premium 授權。

記錄需要 Strata Logging Service 授權，NGFW 的雲端管理需要 AIOps for NGFW Premium 授權。

STEP 2 | 建立一或多個資料夾。

資料夾可用來對防火牆或部署類型進行邏輯分組，以簡化設定管理。

STEP 3 | 將防火牆上線至 Strata Cloud Manager。

若要將防火牆上線至 Strata Cloud Manager，您必須在防火牆上設定本機 Panorama 設定，並將防火牆與您的 Strata Cloud Manager 租用戶產生關聯。上線之後，您可以繼續設定防火牆的一般和工作階段設定。

STEP 4 | （僅限 HA）如有需要，請在高可用性 (HA) 設定中設定受管理的防火牆。

STEP 5 | 建立一或多個片段。

片段可用來對套用於資料夾、部署或個別防火牆的設定物件進行分組。這可讓您標準化可快速應用和推送的通用基礎設定，從而簡化並加速上線程序。

STEP 6 | 建立您的設定物件。

設定物件是您的網路和政策規則設定的建置組塊。

STEP 7 | 建立並設定網路和政策規則設定。

STEP 8 | 將設定變更從 Strata Cloud Manager 推送至受管理的防火牆。

©2025 Palo Alto Networks, Inc.

工作流程：裝置管理

這可在何處使用？	我需要什麼？
• NGFW (Managed by Strata Cloud Manager)	❑ AIOps for NGFW Premium

由 Strata Cloud Manager 管理的 Palo Alto Networks NGFW 稱為雲端管理裝置。Strata Cloud Manager 可管理執行 PAN-OS 10.2.3 或更新版本的防火牆。

如需 Strata Cloud Manager 先決條件的詳細資訊，請按一下這裡。

透過 **Device Management**（裝置管理）儀表板（**Workflows**（工作流程） **> NGFW Setup**（**NGFW** 設定） **> Device Management**（裝置管理）），您可以檢閱與您所有受管理的裝置有關的重要裝置和版本詳細資料，並選取要移至雲端管理的裝置。

查看所有雲端管理的 NGFW 詳細資料

Cloud Managed Devices（雲端管理的裝置）頁籤（**Workflows**（工作流程） **> NGFW Setup**（**NGFW** 設定） **> Device Management**（裝置管理） **> Cloud Managed Devices**（雲端管理的裝置））會顯示所有 SCM 上線防火牆、它們被指派到的資料夾，及其相關的重要詳細資料。

裝置資訊	說明
名稱	NGFW 的名稱及其所在的資料夾。
標籤	任何連結至 NGFW 的標籤。
設定同步狀態	NGFW 的同步狀態： • 同步 • 不同步
HA 狀態	已上線 NGFW 的 HA 狀態： • **Active**（主動）—正常流量處理操作狀態。 • **Passive**（被動）—正常備份狀態。 • **Initiating**（啟動中）—開機後，防火牆處於此狀態會持續最多 60 秒。 • **Non-functional**（非作用中）—錯誤狀態。 • **Suspended**（已暫停）—管理員已停用防火牆。 • **Tentative**（暫訂）—針對於主動/主動組態中的連結或路徑監控事件。
序號	已上線 NGFW 的序號。
Model	已上線 NGFW 的型號。

 ©2025 Palo Alto Networks, Inc.

裝置資訊	說明
類型	已上線 NGFW 的類型： • VM • PA
位址	已上線 NGFW 的 IP 位址。
授權	已上線 NGFW 的授權資訊 • 相符 • 不相符
軟體版本 | 應用程式和威脅 | 防毒 | URL 篩選	顯示目前在防火牆上安裝的軟體和內容版本。如需詳細資訊，請參閱防火牆軟體和內容更新。
裝置字典	供防火牆匯入的檔案。字典檔案為 Strata Cloud Manager 和防火牆管理員提供了在匯入建議的安全性政策規則時可選取的裝置屬性清單。
動作	已上線防火牆的動作： • 擷取授權資訊 • 重新啟動 • 變更路由模式 • 本機設定管理 • 強制啟動

從雲端管理的裝置中移除 NGFW

Available Devices（可用的裝置）頁籤會顯示所有已可上線至 SCM 的 NGFW，以及已由 Strata Cloud Manager 管理的 NGFW。

如需 *Strata Cloud Manager* 上線程序的詳細資訊，請按一下這裡。

您可以使用可用的裝置頁籤將裝置移入和移出 Strata Cloud Manager。

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取**Workflows**（工作流程） > **NGFW Setup**（**NGFW** 設定） > **Device Management**（裝置管理） > **Available Devices**（可用的裝置）。

1. 選取 **Back to Available Devices**（返回可用的裝置），將防火牆移出 Strata Cloud Manager。

 ©2025 Palo Alto Networks, Inc.

在防火牆上還原本機設定版本快照

您可以還原任何版本，以及下載 XML 格式的設定詳細資料。

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取**Workflows**（工作流程） > **NGFW Setup**（**NGFW** 設定） > **Device Management**（裝置管理），然後從 **Actions**（動作）中選取 **Local Configuration Management**（本機設定管理）。

STEP 3 | 載入版本以還原本機設定。

STEP 4 | 按一下 **Yes**（是），將防火牆上的本機設定取代為設定版本。建立新的認可工作。

您可以使用 **Jobs**（工作）檢視對失敗的操作進行疑難排解，調查與已完成的認可相關的警告，或取消擱置中的認可。

STEP 5 | 下載以檢視所選版本的設定詳細資料。

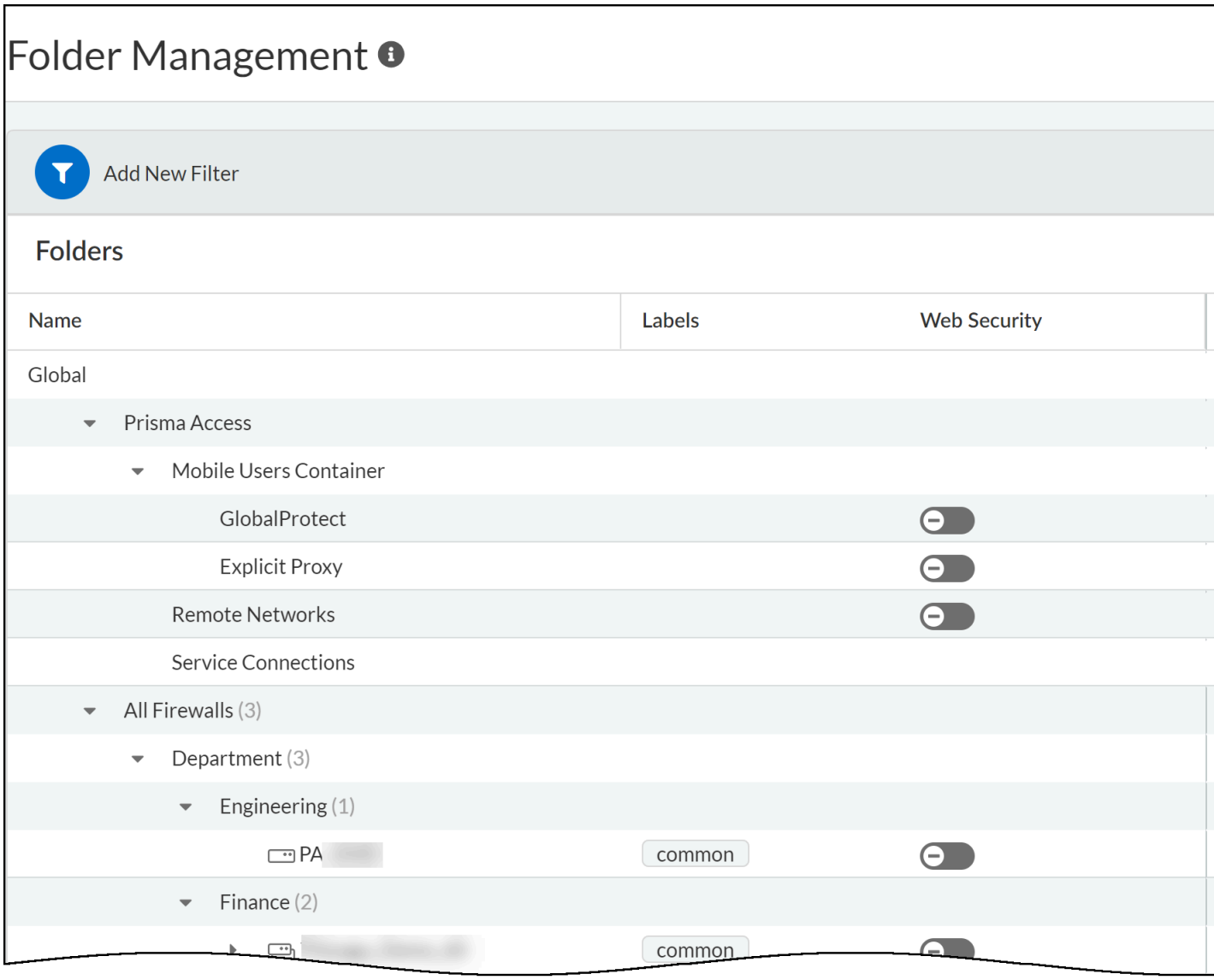
工作流程：資料夾管理

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager)	❑ AIOps for NGFW Premium 授權 ❑ Prisma Access 授權

資料夾可用來對您的防火牆或部署類型進行邏輯分組（Prisma Access 行動使用者、遠端網路或服務連線），以簡化設定管理。您可以建立一個包含多個內嵌資料夾的資料夾，以對需要類似設定的防火牆和部署進行分組。已內嵌的資料夾也可以有多個內嵌資料夾。

Prisma Access 和 NGFW 的資料夾是獨立的；您無法將 NGFW 與 Prisma Access 部署分組到一個資料夾中。但是，您可以在所有資料夾輕鬆地全域套用共用設定，或使用 管理：片段 輕鬆地跨多個資料夾套用標準設定和政策需求。

©2025 Palo Alto Networks, Inc.



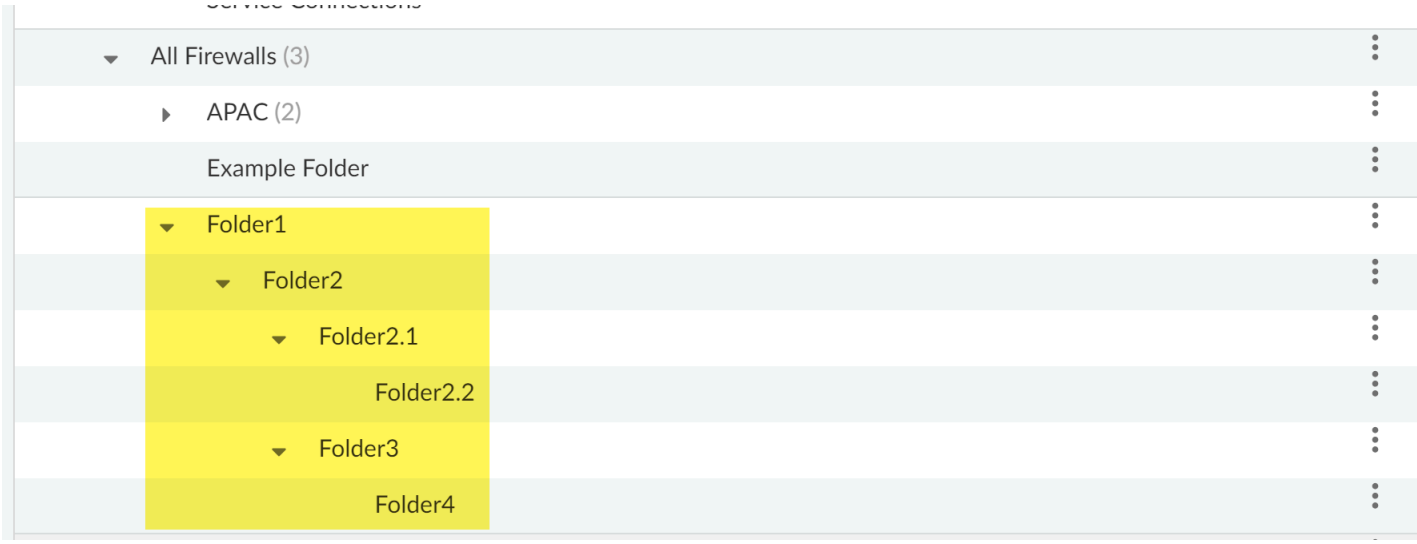
- NGFW
- Prisma Access

資料夾管理 (NGFW)

為協助管理資料夾和防火牆，您可以套用標籤來篩選和鎖定特定防火牆群組，以進行設定變更。此外，每個資料夾也都會顯示防火牆的目前安裝的軟體版本、動態內容發行版本，以及與資料夾相關聯的 GlobalProtect 應用程式版防火牆。

對於防火牆資料夾，Strata Cloud Manager 在任何給定的資料夾階層內最多支援四個內嵌資料夾，且預設的 `All Firewalls` 資料夾始終是任何資料夾階層的最上層。例如，在設計資料夾階層時，請考量下列事項。在下方的範例中，`Folder1`、`Folder2`、`Folder3` 和 `Folder4` 內嵌於 `All Firewalls` 資料夾下，且您無法將任何其他資料夾內嵌至此資料夾階層中。此外 `Folder2.1` 和 `Folder2.2` 內嵌在 `Folder2` 下，且你也無法新增或內嵌任何其他資料夾。

 ©2025 Palo Alto Networks, Inc.



建立資料夾

建立資料夾對防火牆進行邏輯分組，以簡化設定管理。您可以在預設的 `Firewalls` 資料夾下或另一個現有資料夾下建立資料夾。

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 選取 **Workflows**（工作流程） > **NGFW Setup**（**NGFW** 設定） > **Folder Management**（資料夾管理） 和 **Add Folder**（新增資料夾）。

STEP 3 | 為資料夾提供描述性名稱。

STEP 4 | (選用）輸入資料夾的說明。

STEP 5 | (選用）指派一或多個標籤。

您可以選取現有標籤，或鍵入您要建立的標籤來建立新標籤。

STEP 6 | 指定建立資料夾的位置。

選取 **All FirewallsN**（所有防火牆），或選取現有的資料夾以將資料夾內嵌於其下。

 ©2025 Palo Alto Networks, Inc.

STEP 7 | 建立資料夾。

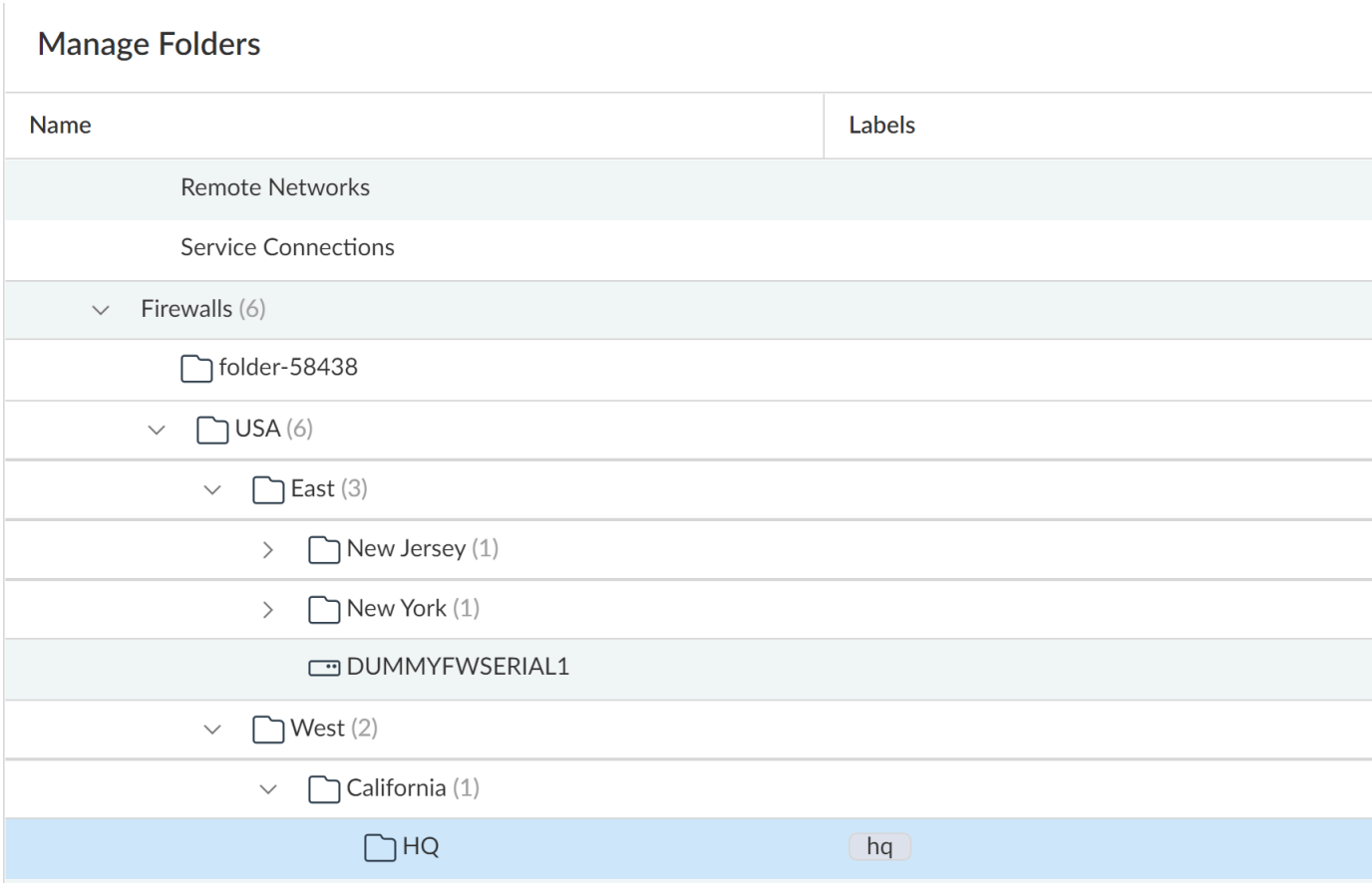
修改資料夾

修改現有資料夾以編輯名稱、說明，以及新增或變更標籤。此外，您可以視需要移動或刪除資料夾。

STEP 1 | 登入 Strata Cloud Manager。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 選取**Workflows**（工作流程） > **NGFW Setup**（**NGFW** 設定） > **Folder Management**（資料夾管理），並展開 [Actions（動作）] 功能表。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | 視需要修改資料夾。

- 編輯資料夾
  1. 編輯資料夾名稱。
  2. (選用）編輯資料夾說明。
  3. 選取或建立 **Labels**（標籤）。

     您可以為資料夾指派完全不同的標籤，或新增其他標籤。
  4. **Save**（儲存）。
- 移動資料夾並選取 **Destination**（目的地）。

您可以透過下列方式移動資料夾。

- 您可以移動資料夾，以將其內嵌在其他資料夾下。
- 您可以移動防火牆資料夾下的內嵌資料夾。
- 您可以將一個資料夾的內嵌資料夾移至另一個資料夾。

在選取資料夾目標後移動資料夾。

- 刪除資料夾，然後按一下 **OK**（確定）加以確認。

您只能刪除沒有相關防火牆、且其下沒有內嵌資料夾的資料夾。

資料夾管理 (Prisma Access)

Prisma Access 資料夾是預先定義的；您可以將其用來指定設定範圍，並確保 Prisma Access 部署類型（行動使用者、遠端網路和服務連線）會接收所有全域設定，然後接收每個類型所需或特有的設定。

定義於資料夾下的設定，會由內嵌在該資料夾階層下的所有資料夾繼承。例如，您可以在 **Prisma Access** 資料夾下設定在 GlobalProtect、明確 Proxy、遠端網路和服務連線間通用的設定。同理，您可以在行動使用者容器下設定在 GlobalProtect 與明確 Proxy 間通用的設定。

您無法編輯 Prisma Access 的資料夾階層。

在資料夾層級上，您也可以為 Prisma Access 行動使用者、遠端網路或服務連線部署啟用 Web 安全性。

 ©2025 Palo Alto Networks, Inc.

工作流程：Prisma SD-WAN 設定

這可在何處使用？	我需要哪些內容？
• Prisma SD-WAN	❑ Prisma SD-WAN 授權

您可以使用 Strata Cloud Manager 在 Prisma SD-WAN 中設定分支站台、資料中心站台和 ION 裝置。

選取**Workflows**（工作流程） > **Prisma SD-WAN Setup**（設定）。

您可以設定下列項目的工作流程：

- 分支站台

  使用 **Branch Sites**（分支站台）頁籤在您的網路中設定分支站台。一個企業可在一個網路內擁有一或多個分支。建立分支時，您可以選取預設網域和政策規則集，並設定 WAN 網路、線路類別、線路標籤和線路規格。

- 資料中心

  使用 **Data Centers**（資料中心）頁籤在您的網路中設定資料中心站台。資料中心站台會連線至分支站台，而您可以在資料中心託管企業應用程式和服務。

- 裝置

  使用 **Devices**（裝置）頁籤在您的網路中設定 ION 裝置。ION 裝置可部署在分支站台或資料中心站台上。這些裝置提供了硬體和軟體兩種規格，可滿足任何位置和任何部署案例的需求。您必須為分支和資料中心站台連接、宣告、指派和設定 ION 裝置。

 ©2025 Palo Alto Networks, Inc.

工作流程：Prisma Access 設定

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager)	Prisma Access 授權

選取**Workflows**（工作流程） > **Prisma Access Setup**（設定），開始設定您的 Prisma Access。

- 設定服務基礎架構，用來聯繫您的遠端網路位置、行動使用者，以及您計劃透過服務連線連接到 Prisma Access 的 HQ 或資料中心。服務連線提供對資料中心的連線。
- 將行動使用者上線，並確認如何將其連線至 Prisma Access。
- 將遠端網路上線以保護遠端網路位置（例如分支），以及這些分支中的使用者。遠端站台上必須要有新世代防火牆或符合 IPSec 規範的第三方裝置，包括可對服務建立 IPSec 通道的 SD-WAN。
- 新增服務連線，讓行動使用者和分支網路上的使用者都能存取總部 (HQ) 或資料中心 (DC) 的資源。除了提供對公司資源的存取，服務連線也允許您的行動使用者連線到分支位置。

工作流程：Prisma Access

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager)	Prisma Access 授權

您必須先設定基礎架構子網路，才能使用 Prisma Access 保護您的遠端網路和行動使用者。

Prisma Access 會使用子網路建立網路主幹，用來聯繫分支網路、行動使用者與 Prisma Access 安全性基礎架構，以及您計劃要透過服務連線連接到 Prisma Access 的 HQ 和資料中心網路。如果您對遠端網路或服務連線使用動態路由，則也必須設定符合 RFC 6696 規範的 BGP 私人 AS 編號。

在為 Prisma Access 新增基礎架構子網路時，請遵循下列建議和需求。

- 使用符合 RFC 1918 規範的子網路。而 Prisma Access 支援使用不符合 RFC 1918 規範的（公用）IP 位址，但不建議這樣做，因為可能會與網際網路公用 IP 位址空間發生衝突。
- 請勿指定任何與 169.254.169.253、169.254.169.254 和 100.64.0.0/10 子網路範圍重疊的子網路，因為 Prisma Access 會保留這些 IP 位址和子網路供內部使用。此子網路是現有網路的延伸，因此不可與您在公司網路中使用的任何 IP 子網路重疊，或是與您為使用者適用的 Prisma Access 或網路適用的 Prisma Access 指派的 IP 位址集區重疊。由於服務基礎架構需要大量 IP 位址，因此您必須指定 /24 子網路（例如，172.16.55.0/24）。
- 輸入適當的基礎架構子網路，此子網路必須可讓 Prisma Access 用來聯繫您的遠端網路位置、行動使用者，以及您計劃透過服務連線連接到 Prisma Access 的 HQ 或資料中心。將符合 RFC 1918 規範的子網路用於基礎架構子網路。

如需詳細資訊，請參閱 Prisma Access 設定。

 ©2025 Palo Alto Networks, Inc.

為基礎架構設定 DNS

Prisma Access 可讓您指定網域名稱系統 (DNS) 伺服器來解析組織內部的網域和外部網域。Prisma Access 會根據您 DNS 伺服器的設定，對 DNS 要求進行 Proxy 處理。

設定基礎架構 DNS 後，會提供對公司網路上的服務（如 LDAP 和 DNS 伺服器）的存取，尤其是您計劃要設定服務連線，用來存取 HQ 或資料中心這些類型的資源時。對內部網域清單所含網域的 DNS 查詢會傳送至您的本機 DNS 伺服器，以確保資源可供 Prisma Access 遠端網路使用者和行動使用者使用。

這將設定適用於所有流量的內部網域清單。如果您要的話，可以檢視管理員指南，以瞭解如何建立僅適用於特定行動使用者部署或遠端網站的內部網域清單。

為基礎架構設定 DNS 的好處包括：

- 讓 Prisma Access 能夠解析您的內部網域
- 設定 DNS 以解析內部和外部網域
- 在網域清單中的網域前面使用萬用字元 (*)，例如 *.acme.local 或 *.acme.com

如需詳細資訊，請參閱 的 DNS。

工作流程：行動使用者

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 授權 ❑ Strata Logging Service 授權

設定行動使用者之前，請確定您擁有所需的授權（行動使用者的 Prisma Access 授權，和有適當防火牆儲存空間的 Strata Logging Service 授權）。如果行動使用者要連線至其他連線網路，您將需要零信任網路存取 (ZTNA) 或 Enterprise Edition Prisma Access 授權，以提供連線所需的企業存取節點 (CAN)。

您會先選擇連線類型，或可同時使用 GlobalProtect 和明確 Proxy。對於這兩種連線類型，您只需在最初完成一些必要的設定，即可讓 Prisma Access 佈建您的行動使用者環境。

1. 連線至 Prisma Access。

   確定您所設定之位置中的行動使用者應如何連線至 Prisma Access。您可以將行動使用者授權劃分為 GlobalProtect 和明明確 Proxy 連線；有些使用者可透過 GlobalProtect 連線，其他則透過明確 Proxy 連線。

   安裝在行動使用者裝置上的 GlobalProtect 應用程式會將流量傳送至 Prisma Access。
2. 設定基礎架構。

   設定基本基礎架構設定，然後設定您的連線類型（GlobalProtect 或明確 Proxy）特定的基礎架構設定。

   行動使用者裝置上的 Proxy 自動設定 (PAC) 檔案會將瀏覽器流量重新導向至 Prisma Access。

 ©2025 Palo Alto Networks, Inc.

3. 選擇 Prisma Access 位置。

   地圖會顯示您可以為使用者部署 Prisma Access 的全球區域：北美洲、南美洲、歐洲、非洲、中東、亞洲、日本和 ANZ（澳大利亞和紐西蘭）。此外，Prisma Access 在每個區域內提供多個位置，以確保您的使用者可以連線至依據其區域設定提供客製化使用者體驗的位置。為了獲得最佳效能，請全選。或者，在每個選定的區域內選取您的使用者需要存取的特定位置。將部署限定於單一區域，可以對您部署的區域進行更精細的控制，並排除政策或產業法規要求的區域。

4. 新增 Prisma Access 位置。

   配置設定以新增要支援使用者的 Prisma Access 位置。

5. 驗證行動使用者。

   設定使用者驗證，僅允許合法使用者存取您的服務和應用程式。要測試您的設定，您可以新增 Prisma Access 在本機驗證的使用者，或者，您可以直接設定企業層級的驗證。

將您的初始設定推送至 Prisma Access 後，Prisma Access 就會開始佈建您的行動使用者環境。這最多可能需要 15 分鐘。您的行動使用者位置啟動並執行時，您可以在 [Mobile Users setup（行動使用者設定）] 頁面、[Summary Overview（摘要概要）] 頁面以及 Prisma Access 洞察內加以驗證。

如需詳細資訊，請參閱 Prisma Access 行動使用者。

工作流程：遠端網路

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager)	Prisma Access 授權

在準備將遠端網路連線至 Prisma Access 時，您必須知道有多少個站台要上線。這項資訊可協助您確認連線需求，例如如何透過 Prisma Access 路由流量。在規劃遠端網路部署時，您必須知道哪些應用程式會通過 Prisma Access，以便正確設定最佳安全性政策規則。同樣重要的是，建立您的威脅設定檔設定。此外，您也應考慮將一致的威脅、URL 和 WildFire 掃描套用至所有規則，以實現一致的威脅緩解策略。

如需詳細資訊，請參閱 Prisma Access 遠端網路。

工作流程：服務連線

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager)	Prisma Access 授權

服務連線可讓行動使用者和分支網路上的使用者都能存取總部 (HQ) 或資料中心 (DC) 的資源。除了提供對公司資源的存取，服務連線也允許您的行動使用者連線到分支位置。

選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Service Connections**（服務連線），以新增服務連線。

 ©2025 Palo Alto Networks, Inc.

您建立的第一個通道是服務連線的主要通道。請重複此工作流程，選擇性地設定次要通道。當兩條通道都已啟動時，主要通道的優先順序會高於次要通道。如果主要服務連線通道發生故障，連線將會回復到次要通道，直到主要通道恢復正常。根據您用來建立通道的 IPSec 裝置，Prisma Access 會提供內建的建議 IKE 和 IPSec 安全性設定。一開始您可以使用建議設定，或根據您的環境需求自訂設定。

如需詳細資訊，請參閱 Prisma Access 服務連線。

工作流程：遠端瀏覽器隔離

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.0 Innovation ❑ 具有行動使用者或遠端網路授權訂閱的 Prisma Access 授權 ❑ 遠端瀏覽器隔離授權

Palo Alto Networks 的遠端瀏覽器隔離 (RBI) 是一個解決方案，可將所有瀏覽活動隔離，並從使用者受管理的裝置和公司網路傳輸至外部實體（例如 Prisma Access），以保護並隔離其平台內潛在的惡意程式碼與內容。

RBI 可與 Prisma Access 原生整合，讓您能夠輕鬆地將隔離設定檔套用至現有的安全性政策。所有隔離的流量都會經歷雲端交付安全服務 (CDSS) 提供的分析和威脅防護，例如進階威脅防護、進階 WildFire、進階 URL 篩選、DNS 安全性，和 SaaS 安全性。

當您準備將使用者上線至 RBI 時，請考量您要為使用者的隔離瀏覽啟用哪些 URL 類別。請想一下您希望禁止使用者執行哪些瀏覽器動作，例如複製和貼上功能、鍵盤輸入，以及上傳、下載和列印檔案等共用選項。

如需詳細資訊，請參閱遠端瀏覽器隔離。

©2025 Palo Alto Networks, Inc.

工作流程：軟體升級

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager)	• 至少要有下列其中一個授權，才能使用 Strata Cloud Manager 管理您的設定；若要統一管理 NGFW 和 Prisma Access，您將同時需要 NGFW 和 Prisma Access 授權： ❑ Prisma Access 授權 ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro

使用 Strata Cloud Manager 來規劃及管理 NGFW 和 Prisma Access 的軟體升級。以下是您可以執行的工作流程：

- 升級建議：建立升級建議，以確認您可升級的裝置適合的最佳軟體版本。軟體升級建議會分析防火牆上啟用的功能，並提供客製化建議。
- Prisma Access 升級儀表板：為特定 Prisma Access 升級選擇慣用時間視窗。
- NGFW - 排程器：排程 PAN-OS 軟體更新，以在您選擇的日期和時間將防火牆升級或降級至目標 PAN-OS 版本。
- NGFW
- Prisma Access

軟體升級 (NGFW)

選取**Workflows**（工作流程） > **Software Upgrades**（軟體升級） > **Upgrade Recommendations**（升級建議），藉由分析裝置並建立升級建議來規劃裝置的升級。

升級建議

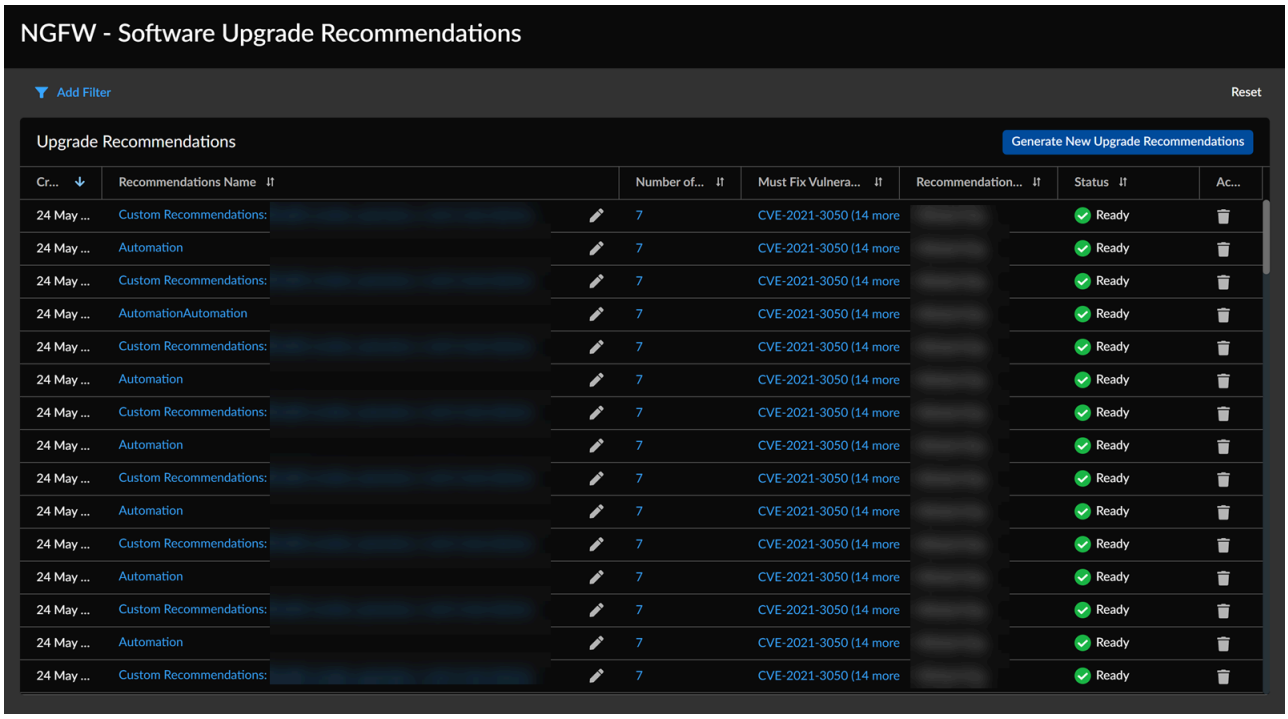
在**Workflows**（工作流程） > **Software Upgrades**（軟體升級） > **Upgrade Recommendations**（升級建議）中，您可以建立建議，以確認可升級的裝置適合的最佳軟體版本。軟體升級建議會分析防火牆上啟用的功能，並提供客製化建議，包括：

- 您可以升級的裝置適合的最佳軟體版本。
- 每個建議軟體版本中的新功能、行為變更、弱點和軟體問題的相關資訊。

升級建議類型如下：

- 系統產生的建議，會每週產生，並且包含建議的升級選項。
- 使用者產生的自訂建議（根據安全性諮詢摘要中特定 CVE 的選定裝置而產生）。
- 使用者產生的建議（根據防火牆的技術支援檔案 (TSF) 上傳而產生）。

©2025 Palo Alto Networks, Inc.



對於升級建議中的每個計劃，您可以：

- 檢視需要升級的裝置數目，以及必須修正的弱點。
- 編輯建議報告的名稱以區分自訂報告。
- 按「建立日期」、「計劃名稱」和「建議產生者」來篩選建議報告。
- 刪除失敗或不再需要的升級建議。

按一下建議報告以檢視詳細報告，其中包含裝置的升級選項。選取升級選項以進一步檢視關於 **New Features**（新功能)、**PAN-OS Known Vulnerabilities**（**PAN-OS** 已知弱點）、**Changes of Behavior**（行為變更）和 **PAN-OS Known Issues**（**PAN-OS** 已知問題）的詳細資料對於 **PAN-OS Known Issues**（**PAN-OS** 已知問題）下的已知問題，**Associated Case Count**（相關聯的案例計數）下的值可由報告此問題的客戶數量得出。

按一下 **Export**（匯出）以 CSV 格式下載此報告。

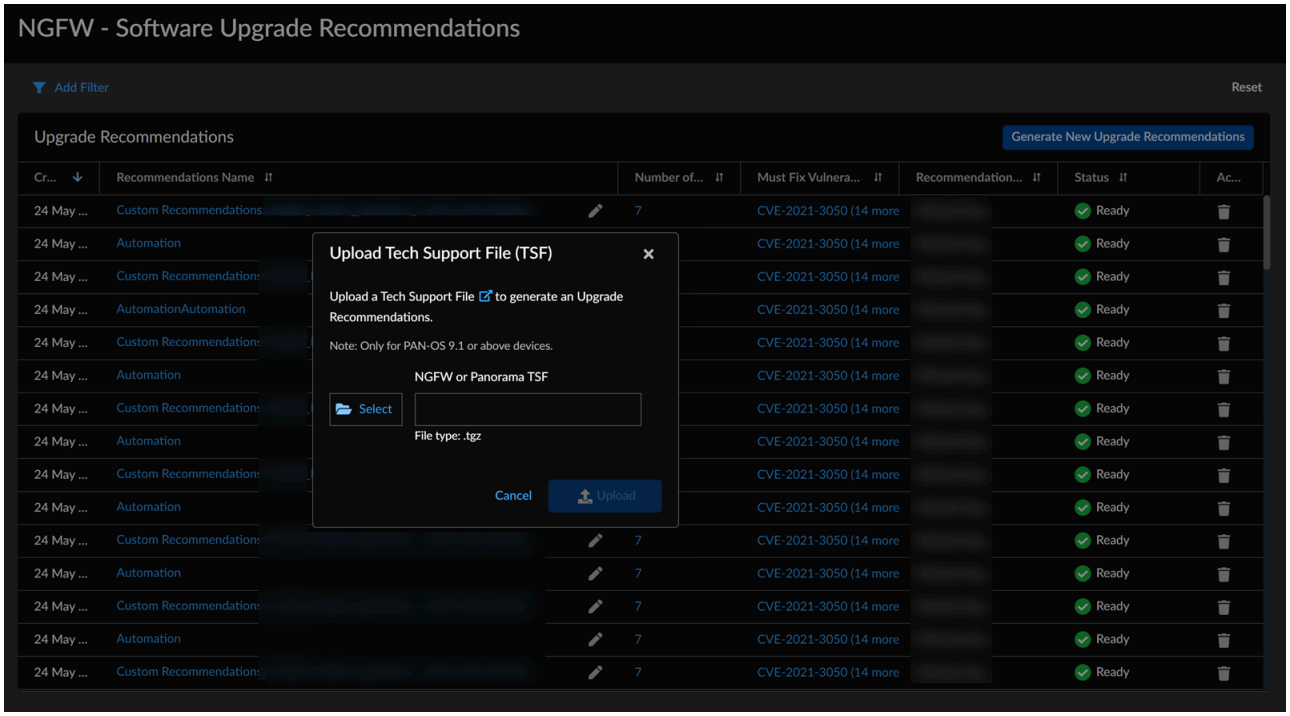
產生隨選軟體升級建議

1. 導覽至 **Workflows**（工作流程）> **Software Upgrades**（軟體升級）> **Upgrade Recommendations**（升級建議）。
2. 產生新的升級建議。

 ©2025 Palo Alto Networks, Inc.

3. 選取技術支援檔案 (TSF)，然後選取 **Upload**（上傳）。

   - 您一次只能上傳一個裝置的 *TSF*，且必須是 *.tgz* 檔案格式的 *TSF*。
   - 軟體升級建議支援來自 *PAN-OS 9.1* 版或更高版本裝置的 *TSF*，用以產生報告。



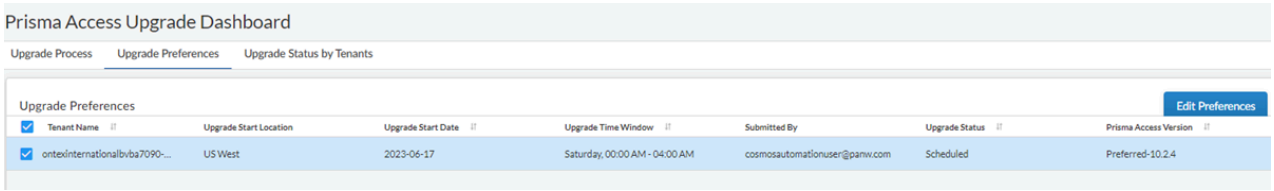
4. 在狀態顯示為 **Ready**（就緒）後檢視軟體升級建議。您也可以檢查 **Status**（狀態）欄，以確認是否有與 TSF 檔案的上傳、檔案格式或處理相關的錯誤。

軟體升級 (Prisma Access)

選取 **Workflows**（工作流程） > **Software Upgrades**（軟體升級） > **Prisma Access**，以檢視 Prisma Access 資料平面升級程序的相關資訊。

您可以：

- 瞭解 Prisma Access 資料平面升級程序。
- 選擇您的升級偏好設定：



選取租用戶名稱以選擇您的升級偏好設定。如需詳細資訊，請參閱為特定 Prisma Access 升級選擇慣用視窗。

 ©2025 Palo Alto Networks, Inc.

工作流程：Prisma Access 瀏覽器

這可在何處使用？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 具有 Prisma Access Browser 套件授權 ❑ 超級使用者或 Prisma Access Browser 角色

選取**Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Prisma Access Browser**，開始將 Prisma Access Browser 上線。

Prisma Access Secure Enterprise Browser (Prisma Access Browser) 是唯一可同時保護受管理和未受管理裝置的解決方案，其工具為原生整合、可將保護延伸至未受管理裝置的企業瀏覽器。請參閱什麼是 Prisma Access 瀏覽器？

上線是一系列的步驟，其間您會設定下列項目：

- 使用者驗證和群組
- Prisma Access 整合
- 路由
- 強制執行 SSO 應用程式
- 下載和散佈
- 瀏覽器政策

在 Strata Cloud Manager 上線 Prisma Access 瀏覽器。

 ©2025 Palo Alto Networks, Inc.

報告：Strata Cloud Manager

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • Prisma SD-WAN	❑ 以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN ❑ 軟體 NGFW 積分 （適用於 *VM-Series* 軟體 *NGFW*） ❑ WAN Clarity 報告授權 ❑ 有權下載、共用和排程報告的角色。

在 Strata Cloud Manager 中取得網路流量模式、頻寬使用率、安全性訂閱資料的報告。報告針對您的網路提供可操作的洞察，讓您用於規劃和監控用途。特定 Prisma Access 和 NGFW 儀表板、活動洞察概要和 Prisma SD-WAN 支援報告。有完全存取權可使用儀表板的 Prisma Access 和 NGFW 使用者，可以將儀表板資料下載為 PDF、在其組織內共用報告，以及將報告排程為定期傳遞至其電子郵件收件匣。報告是 Prisma SD-WAN 中的授權訂閱服務。您可以從 Prisma SD-WAN 中的控制器、跨站台和線路下載及檢視報告。

在 Strata Cloud Manager 中檢視這些報告：

- Prisma Access 和 NGFW - 您可以從 Prisma Access 和 NGFW 儀表板與活動洞察產生報告。儀表板右上方若有圖示  ，表示此儀表板支援報告。您也可以直接從 **Reports**（報告）功能表中產生、下載、共用和排程報告。
- Prisma SD-WAN - 檢視下列 WAN Clarity 報告：
  - WAN Clarity 分支報告
  - WAN Clarity 資料中心報告
  - 彙總頻寬使用量報告
- Prisma Access 和 NGFW
- Prisma SD-WAN

報告（Prisma Access 和 NGFW）

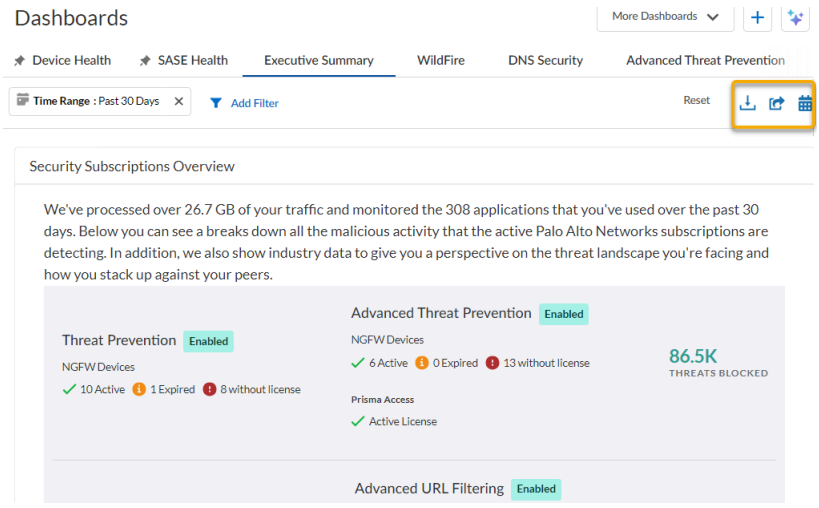
儀表板和活動洞察摘要可在您的組織內以 PDF 報告的形式共用，您也可以將報告排程為定期（每天、每週或每月）傳遞至您的電子郵件收件匣（和同事的收件匣）。

如此，您即可輕鬆地與組織成員共用報告，為此應用程式設定雲端識別引擎（目錄同步）。雲端識別引擎可為應用程式提供對 Active Directory 資訊的唯讀存取權。設定雲端識別引擎後，您即可輕鬆地將收件者新增至排程報告中。您的報告收件者會受到雲端識別引擎的檢查，如果找不到相符，就會執行額外的驗證步驟，方法是根據與支援帳戶相關聯的電子郵件地址網域檢查電子郵件地址網域。這些檢查可確保報告不會傳送至組織外部。

您可以直接從 **Reports**（報告）功能表或從個別 **Dashboard**（儀表板）頁面和 **Insights**（洞察）> > **Activity Insights**（活動洞察） > **Overview**（概要）頁面下載、共用或排程報告。報告會以 PDF 格式共用和下載。

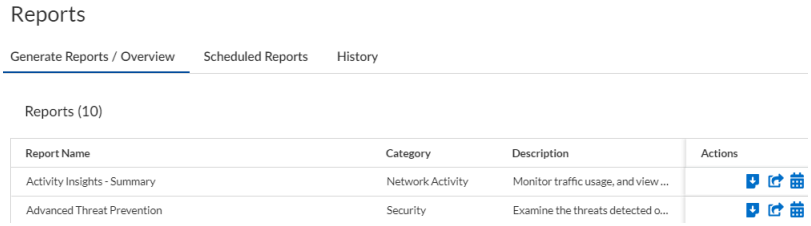
若要下載、共用或排程報告：

STEP 1 | 在 **Dashboard**（儀表板）頁面上，或**Insights**（洞察）> > **Activity Insights**（活動洞察） > **Overview**（概要）頁面上，按一下 中的任何圖示。



或

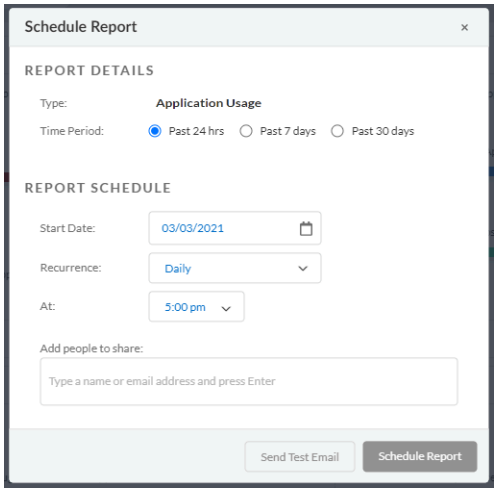
按一下**Strata Cloud Manager** > **Reports**（報告） > **Generate Reports/Overview**（產生報告/概要），並從報告格式清單中選取以下任一圖示 。預設情況下，根據您要為其產生報告的儀表板類型，使用過去 24 小時或 30 天的資料產生報告。在排程報告時，您可以自訂要在報告中收集資料的時段。



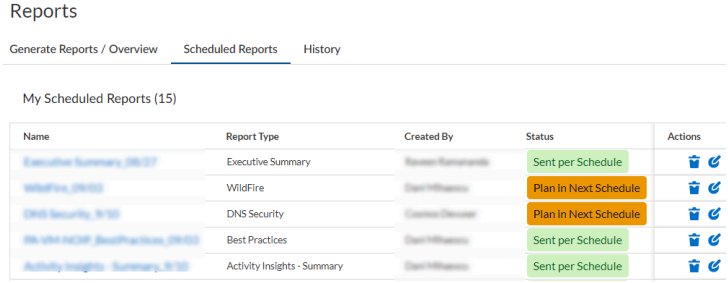
 ©2025 Palo Alto Networks, Inc.

STEP 2 | 如果您要排程報告，則必須繼續定義報告參數，包括：

- 要收集資料的 **Time Period**（時段）
- **Recurrence**（週期性），這是您的報告據以傳遞的頻率（每天、每週或每月）



您可以檢視、編輯或刪除**Strata Cloud Manager** > **Reports**（報告） > **Scheduled Reports**（排程報告）頁籤。



History（歷程記錄）會顯示過去 30 天內下載的所有報告。

 ©2025 Palo Alto Networks, Inc.

報告 (Prisma SD-WAN)

Prisma SD-WAN WAN Clarity 報告會提供您網路中的流量散佈和頻寬使用率的彙總檢視。您可以從 Prisma SD-WAN 控制器下載整個報告套件或檢視報告，以便進行逐週的趨勢比較，以及跨站台和線路的比較。

報告可立即作為授權的訂閱服務使用。請聯絡 Prisma SD-WAN 銷售團隊以啟用訂閱。

Prisma SD-WANWAN Clarity 報告包含：

- WAN Clarity 分支報告
- WAN Clarity 資料中心報告
- 彙總頻寬使用量報告

若要檢視報告：

STEP 1 | 選取**Reports**（報告） > **Prisma SD-WAN**。

STEP 2 | 按一下 **WAN Clarity Reports**（**WAN Clarity** 報告）上的 **View Reports**（檢視報告）。

STEP 3 | 選取 **Time Range**（時間範圍），然後在 **Report for**（報告標的）欄位中選取下列任一項。

- 分支
- 資料中心
- 彙總頻寬使用量

 ©2025 Palo Alto Networks, Inc.

我的最愛：Strata Cloud Manager

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ 以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ 任何租用戶或租用戶服務群組 (TSG) 支援的應用程式 ❑ 取決於您的需求的角色

「我的最愛」功能可讓您儲存感興趣的項目，然後在需要時從 Strata Cloud Manager 中的任何位置快速加以存取。您可以藉由組織、編輯和刪除清單中的內容，在自己的私人清單中個人化您偏好的功能表項目名稱。

依照下列方式管理我的最愛：

- 新增我的最愛
- 檢視我的最愛
- 編輯我的最愛
- 刪除我的最愛

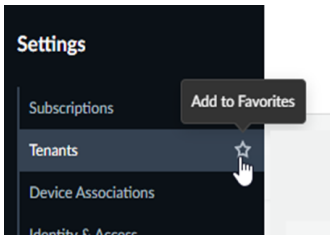
新增我的最愛

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ 以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ 任何 租用戶或租用戶服務群組 (TSG) 支援的應用程式 ❑ 取決於您的需求的角色

如果您在 Strata Cloud Manager 中有需要反覆存取的功能表項目或頁面，但您不想要重複加以搜尋或導覽，您可以將這些項目儲存到我的最愛清單中。

STEP 1 | 導覽至要儲存的功能表項目或頁面。

STEP 2 | 將滑鼠暫留在項目上方，可檢視星形圖示。



STEP 3 | 選取星形可將此項目新增至 **Favorites**（我的最愛）。

最上層的功能表項目無法新增為我的最愛。只有子功能表才可新增為我的最愛。

©2025 Palo Alto Networks, Inc.

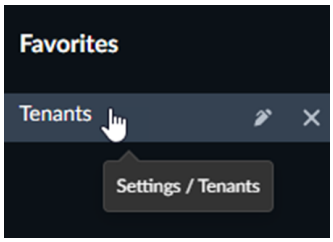
檢視我的最愛

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ 以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ 任何租用戶或租用戶服務群組 (TSG) 支援的應用程式 ❑ 取決於您的需求的角色

在新增我的最愛之後，您可以檢視「我的最愛」及其原始位置。

STEP 1 | 選取 **Favorites**（我的最愛）。

STEP 2 | 將滑鼠暫留在項目上方，檢視位置圖示。



STEP 3 | 顯示實際位置的路徑和功能表名稱。

按一下我的最愛清單中的項目，前往其原始位置。

©2025 Palo Alto Networks, Inc.

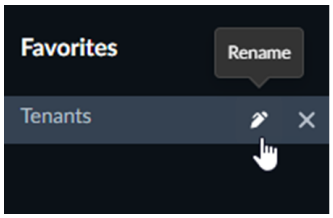
編輯我的最愛

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ 以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ 任何租用戶或租用戶服務群組 (TSG) 支援的應用程式 ❑ 取決於您的需求的角色

新增我的最愛之後，您可以編輯我的最愛加以個人化。

STEP 1 | 選取 **Favorites**（我的最愛）。

STEP 2 | 將滑鼠暫留在項目上方，檢視編輯圖示。



STEP 3 | 將項目重新命名。

將我的最愛清單中的項目重新命名，並不會重新命名原始位置中的原始項目。

©2025 Palo Alto Networks, Inc.

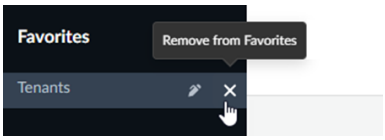
刪除我的最愛

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理） • NGFW （使用 *Strata Cloud Manager* 或 *Panorama* 設定管理）	❑ 以下各授權都包含對 Strata Cloud Manager 的存取權： ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ 任何租用戶或租用戶服務群組 (TSG) 支援的應用程式 ❑ 取決於您的需求的角色

新增我的最愛之後，您可以從清單中刪除我的最愛。

STEP 1 | 選取 **Favorites**（我的最愛）。

STEP 2 | 將滑鼠暫留在項目上方，檢視刪除圖示。



STEP 3 | 按一下圖示，可從清單中刪除我的最愛。

刪除我的最愛清單中的項目，並不會從原始位置移除原始項目。

©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

設定：Strata Cloud Manager

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager)	❑ 任何租用戶或租用戶服務群組 (TSG) 支援的應用程式 ❑ 取決於您的需求的角色 ❑ Strata Logging Service 用以管理日誌

在 **Settings**（設定）中，您可以管理與 Strata Cloud Manager 中提供的所有服務有關的程序。這些程序包括：

訂閱

檢視已核准的產品訂閱。

管理訂閱。

Device Associations

Device Associations 多半用於裝置和應用程式上線，可讓您：

- 將新裝置與租用戶產生關聯
- 將應用程式與您的裝置產生關聯
- 管理裝置和應用程式關聯

開始使用裝置關聯。

產品

如果您有單一租用戶環境，請檢視、啟動和管理您的產品：

- 取得產品資訊
- 重新命名執行個體
- 管理共用
- 新增租用戶

開始使用產品管理。

租用戶

如果您是受管理的安全服務提供者 (MSSP) 或分散式企業，則可以建立和管理業務組織和單位的階層（由租用戶代表）。在 **Tenants**（租用戶）中，您可以：

- 新增租用戶
- 編輯租用戶
- 管理租用戶授權

- 刪除租用戶
- 從單一租用戶轉換至多租用戶部署

開始使用租用戶管理。

識別與存取

控制使用者角色的驗證和授權，以及所有應用程式和 API 型存取的權限。透過識別與存取，您可以管理：

- 使用者存取
- 服務帳戶
- 角色
- 第三方識別提供者整合

開始使用識別與存取。

稽核日誌

檢視由 Strata Cloud Manager 的使用者起始之所有動作的記錄

檢視稽核日誌。

ION 授權管理

為虛擬 ION 裝置產生授權權杖。這提供了一組控制，防止未經授權者在環境中新增虛擬裝置。

管理 ION 授權。

使用者偏好設定

自訂您的偏好設定以滿足自身需求。例如，選擇您的顯示模式。

設定使用者偏好設定。

可信任 **IP** 清單

就個別租用戶指定允許的 IP 位址，使用可信任 IP 清單來限制對應用程式的存取。

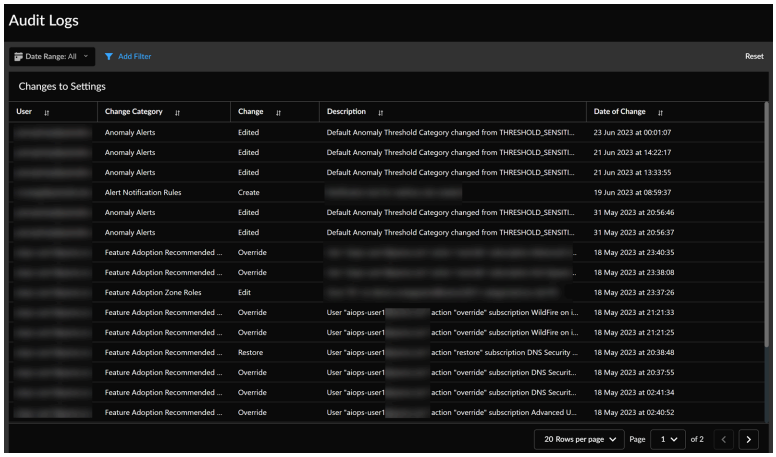
設定可信任 IP 清單。

 ©2025 Palo Alto Networks, Inc.

設定：稽核日誌

我可以在哪裡使用這個？	我需要哪些內容？
• Strata Cloud Manager	❑ 下列其中之一： • AIOps for NGFW Free 應用程式 • AIOps for NGFW Premium (使用 Strata Cloud Manager 應用程式) • Strata Cloud Manager Essentials • Strata Cloud Manager Pro ❑ 下列任何預先定義的角色：稽核員、業務管理員、資料安全性管理員、部署管理員、IAM 管理員、多租用戶 IAM 管理員、多租用戶管理使用者、多租用戶監控使用者、多租用戶超級使用者、網路管理員、安全性管理員、SOC 分析師、超級使用者、第 1 層支援、第 2 層支援、僅限檢視管理員

在 **Settings**（設定）**> Audit Logs**（稽核日誌）底下，您可以看到由 Strata Cloud Manager 的使用者起始起的動作清單。其中提供關於所做變更的日誌、變更的擁有者、變更的日期和時間，以及變更的說明。您可以將這些日誌用於合規性和疑難排解用途。您可以按日期範圍與功能來篩選稽核日誌，或按使用者、類別和變更類型篩選。



 ©2025 Palo Alto Networks, Inc.

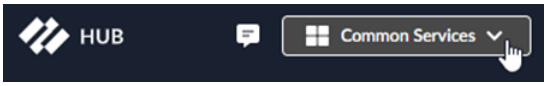
設定：可信任 IP 清單

我可以在哪裡使用這個？	我需要哪些內容？
• Strata Cloud Manager	❑ 超級使用者、多租用戶超級使用者、多租用戶 IAM 管理員的 IAM 角色，或任何設定了「可信任 IP 清單」權限的自訂角色

雲端交付的應用程式可讓您從世界各地便利地存取。然而，這也會帶來風險，例如使用遭竊的憑證、字典攻擊和其他形式的暴力攻擊進行存取，以獲取對應用程式的存取權。

識別與存取管理可以降低部分風險，而您也可以使用可信任 IP 清單，藉由指定每個租用戶允許的 IP 位址，進一步限制對應用程式的存取。

根據預設，在建立新租用戶期間允許從任何 IP 位址存取網頁介面和 API。可信任 IP 清單是可存取租用戶的可信任 IP 位址清單。您可以使用可信任 IP 清單來限制對單一租用戶的存取，也可以使用它來限制對多租用戶階層中的父租用戶及其子租用戶的存取。在多租用戶階層中，您在父租用戶上新增可信任 IP 清單後，清單將會從父租用戶繼承到子租用戶上，並且由上至下強制執行。

如何從 **Strata Cloud Manager** 管理可信任 IP 清單	如何從 **hub** 管理可信任 IP 清單
若要從 Strata Cloud Manager 管理可信任 IP 清單，請選取**Settings**（設定） > **Trusted IP List**（可信任 **IP** 清單）。  您可以從 Strata Cloud Manager 和 Strata Cloud Manager 網頁介面管理可信任 IP 清單，API 將僅允許存取這些可信任 IP。	若要從 hub 管理可信任 IP 清單，請選取中樞的租用戶檢視 > **Common Services**（常用服務） > **Trusted IP List**（可信任 **IP** 清單）。  您可以從 hub 管理可信任 IP 清單，但 hub 不受可信任 IP 強制執行的約束，因此您對 hub 的存取不受可信任 IP 限制。如果您的 IP 位址被 Strata Cloud Manager 上的租用戶封鎖，但您應該有其存取權，您可以前往 hub 解鎖您的存取權（如果您擁有此處所列的權限）。

新增可信任 IP

刪除可信任 IP

解鎖存取權

 ©2025 Palo Alto Networks, Inc.

新增可信任 IP

我可以在哪裡使用這個？	我需要哪些內容？
• Strata Cloud Manager	❑ 超級使用者、多租用戶超級使用者、多租用戶 IAM 管理員的 IAM 角色，或任何設定了「可信任 IP 清單」權限的自訂角色

在您針對 Strata Cloud Manager 啟動授權、建立租用戶並管理使用者存取後，您可以藉由將可信任 IP 位址新增至可信任 IP 清單，進一步限制對租用戶的存取。依預設會允許任何 IP 位址存取。

使用 Strata Cloud Manager 新增可信任 IP。

STEP 1 | 選取 **Settings**（設定） > **Trusted IP List**（可信任 **IP** 清單）。

STEP 2 | 搜尋或捲動以尋找並選取您的租用戶。

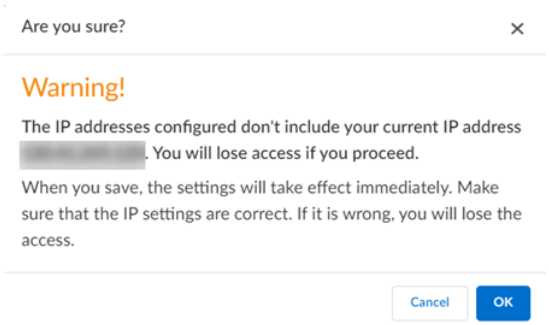
STEP 3 | 選取 **Add New**（新增）。

STEP 4 | 輸入可存取此租用戶的 **IP Address**（**IP** 位址）。

- 此欄位支援 CIDR 標記法。僅允許使用 IPv4 位址。
- 您可以使用單一 IP 位址，或者，可以使用具有子網路遮罩（例如 12.12.12.1/30）的範圍。
- IP 和範圍經過驗證，因此不受支援的項目會產生錯誤。
- **Added By**（新增者）欄位會自動填入。

STEP 5 | **Save**（儲存）。

變更會立即生效，因此請確定您的 *IP* 位址正確無誤，否則您可能會失去對租用戶的存取權。



 ©2025 Palo Alto Networks, Inc.

STEP 6 | 在父租用戶上新增可信任 IP 清單後，清單將會從父租用戶繼承到子租用戶上，並且由上至下強制執行。子租用戶也可以新增本身的可信任 IP 清單。

刪除可信任 IP

我可以在哪裡使用這個？	我需要哪些內容？
• Strata Cloud Manager	❑ 超級使用者、多租用戶超級使用者、多租用戶 IAM 管理員的 IAM 角色，或任何設定了「可信任 IP 清單」權限的自訂角色

新增可信任 IP 至租用戶的可信任 IP 清單後，您可以藉由刪除可信任 IP 位址，回復為不受限制的存取。

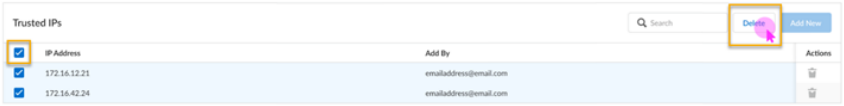
使用 Strata Cloud Manager 刪除可信任 IP。

STEP 1 | 選取 **Settings**（設定） > **Trusted IP List**（可信任 **IP** 清單）。

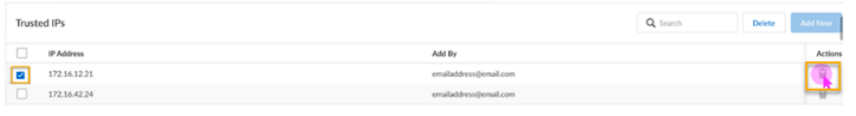
STEP 2 | 搜尋或捲動以尋找並選取您的租用戶。

STEP 3 | 使用下列其中一個選項：

- 刪除多個 IP — 選取 **IP Address**（**IP** 位址）核取方塊以同時反白顯示所有 IP 位址，然後選取 **Delete**（刪除）按鈕。



- 刪除單一 IP — 選取該 IP 的個別核取方塊，然後從**Actions**（動作） > **Delete**（刪除）中刪除。



如果您從父租用戶繼承了可信任 *IP* 清單，您將無法從子租用戶將其刪除，因為這些清單是繼承的。如果您是直接在子層級新增可信任 *IP* 清單的，就只能從子租用戶將其刪除。

STEP 4 | 在出現提示時選取 **OK**（確定）。

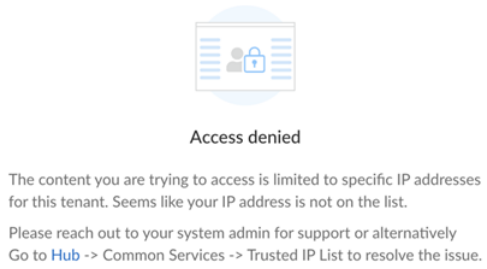
變更會立即生效。如果您刪除了所有可信任 IP，則 IP 存取將回復為 **Any**（任何）。

 ©2025 Palo Alto Networks, Inc.

解鎖存取權

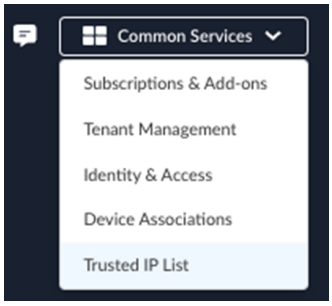
我可以在哪裡使用這個？	我需要哪些內容？
• Strata Cloud Manager	❑ 超級使用者、多租用戶超級使用者、多租用戶 IAM 管理員的 IAM 角色，或任何設定了「可信任 IP 清單」權限的自訂角色

將可信任 IP 新增至租用戶的可信任 IP 清單後，Strata Cloud Manager 就會強制執行該存取。如果您的 IP 位址不在租用戶的可信任 IP 清單中，當您嘗試加以存取時，將會看到拒絕存取訊息。

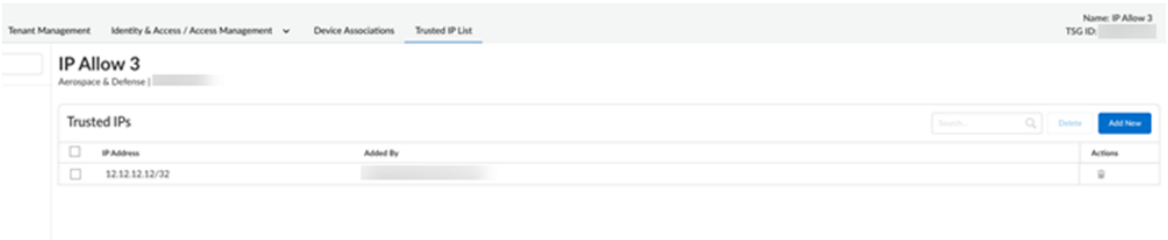


如果您的 IP 位址租用戶封鎖，但您應該有其存取權，您可以前往 hub 自行解鎖（如果您擁有此處所列的權限）。

STEP 1 | 從 hub 選取中樞的租用戶檢視 > **Common Services**（常用服務） > **Trusted IP List**（可信任 IP 清單）。



STEP 2 | 將您的 IP 位址新增至可信任 IP 位址清單。



 ©2025 Palo Alto Networks, Inc.

設定：使用者偏好設定

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Strata Cloud Manager	其中一個： ❑ AIOps for NGFW Free 或 AIOps for NGFW Premium 授權 ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

在 **Settings**（設定）**> User Preferences**（使用者偏好設定）中，您可以自訂 Strata Cloud Manager，藉由修改使用者偏好設定來滿足您的特定需求。這些設定包括：

- 淺色/深色/系統模式 - 選擇深色和淺色顯示模式，或選擇使用您自己的系統設定。

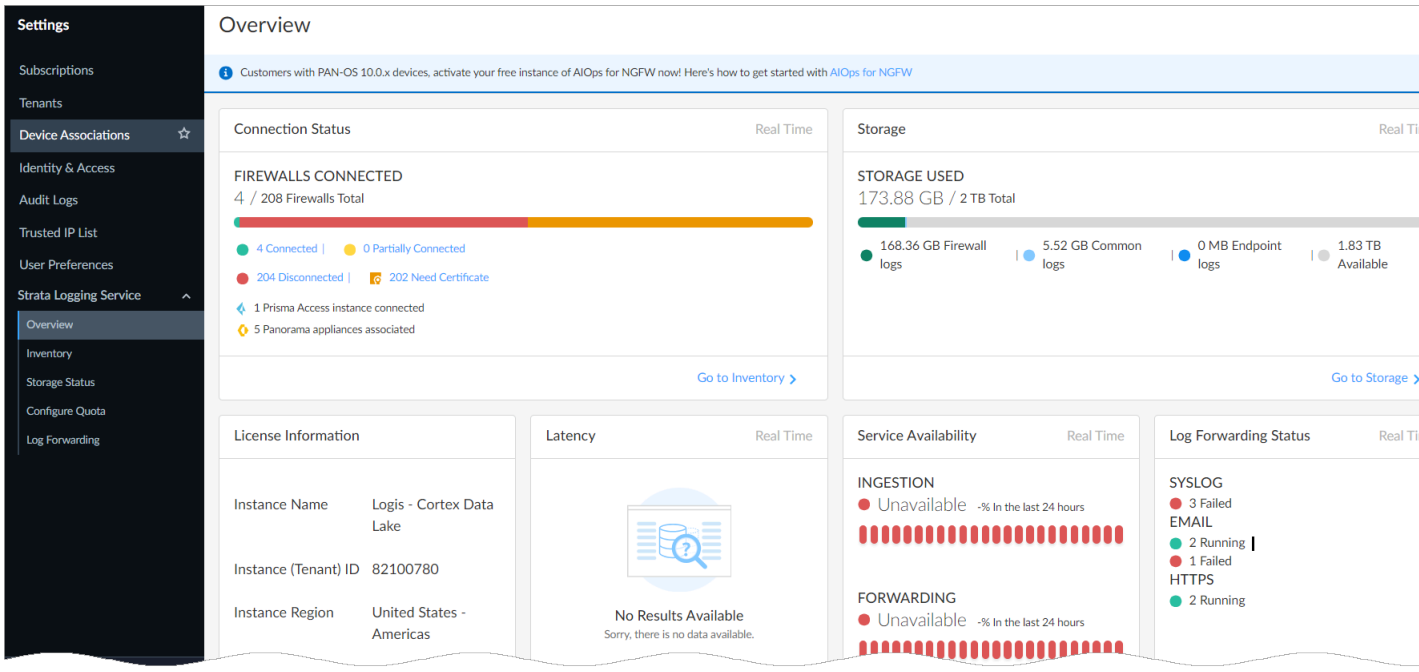
 ©2025 Palo Alto Networks, Inc.

設定：Strata Logging Service

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 PAN-OS or Panorama) • NGFW (Managed by Strata Cloud Manager)	❑ Strata Logging Service

Strata Logging Service（前身為 Cortex Data Lake）是一個雲端式記錄系統，用來儲存由我們的安全產品（包括 NGFW、Prisma Access 和 Cloud NGFW for AWS）產生的豐富內容增強型網路日誌。透過 Strata Logging Service，您可以收集數量不斷擴大的資料，而無須規劃本機計算和儲存，並且從一開始就可以進行規模調整。瞭解如何在你的產品中啟動和部署 Strata Logging Service。

此外，您也可以使用中樞提供的 *Strata Logging Service* 應用程式來存取及管理日誌。*Strata Logging Service* 應用程式和 *Strata Cloud Manager* 兩者的日誌資料是相同的，但在網路介面方面有所差異。



使用 Strata Logging Service 來：

- 檢查 Strata Logging Service 執行個體的狀態 - 按一下 **Strata Logging Service** > **Overview**（概要）

©2025 Palo Alto Networks, Inc.

- 檢視和上線防火牆、Cloud NGFW、Prisma Access 或 Panorama 設備 - 按一下**Strata Logging Service** > **Inventory**（詳細目錄）
- 根據您的傳入日誌速率檢視已配置的日誌儲存配額、可用儲存空間，以及日誌保留天數 - 按一下**Strata Logging Service** > **Storage Status**（儲存狀態）
- 設定日誌儲存配額- 按一下 **Strata Logging Service** > **Configure Quota**（設定配額）
- 搜尋、篩選和匯出日誌資料- 按一下 **Incidents & Alerts**（事件與警示） > **Log Viewer**（日誌檢視器）。日誌檢視器的功能與 Strata Logging Service 應用程式中的「探索」相同。
- 將日誌資料轉送至外部伺服器以進行長期儲存、SOC 或內部稽核 - 按一下**Strata Logging Service** > **Log Forwarding**（日誌轉送）

©2025 Palo Alto Networks, Inc.

應用程式體驗

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager)	下列授權之一： ❑ Prisma Access 授權 ❑ ADEM Observability 授權或 AI-Powered ADEM 授權

您可以使用 **Application Experience**（應用程式體驗）頁面，管理您的自發 DEM 使用者和遠端站台。檢視稽核日誌，以查看哪些管理員已在選取的時間範圍內對 Prisma Access 進行驗證。

請參閱管理自發 DEM 代理程式升級，以瞭解升級選項。

端點代理程式管理

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager)	下列授權之一： ❑ Prisma Access 授權 ❑ ADEM Observability 授權或 AI-Powered ADEM 授權

使用此頁籤可取得關於所有已註冊 ADEM 使用者的詳細資料，例如使用者是在線上（使用者裝置向 ADEM 服務傳送保持活動訊息）還是離線（ADEM 服務在過去十分鐘內未接收到來自使用者裝置的保持活動訊息）、最後一次看到使用者裝置的時間、ADEM 使用者的使用者名稱、裝置類型和主機名稱，及其所執行的 ADEM 代理程式版本。

在此頁籤中，表格中的每一列各代表個別列中的唯一使用者。每個使用者/裝置組合都被視為唯一的使用者。例如，如果有 2 個使用者分別登入 3 個裝置，則唯一使用者數目將是 6 個。因此，多個列的使用者名稱可能會重複，具體取決於使用者登入的裝置數目。

在此 Widget 的表格標題中，**Total Endpoint Agents**（端點代理程式總數）表示受監控的裝置總數。使用者的數目是使用者總數，與使用者登入的裝置數目無關。這是因為授權耗用量是以使用者總數為準，與每個使用者登入的裝置數量無關。

使用 **Last logged in User**（上次登入的使用者）左側的核取方塊，藉由選取端點的列來進行批次設定。藉由從端點代理程式管理表格中選取項目加以刪除，可釋出授權項目。

欄名稱	說明
上次登入的使用者	一個裝置可以有多個登入的使用者。此欄會列出最近使用此裝置登入 GlobalProtect 的使用者 ID。

©2025 Palo Alto Networks, Inc.

欄名稱	說明
裝置	此裝置上執行的作業系統。
主機名稱	裝置的主機名稱。
上次看見	從裝置傳送至 DEM 伺服器的最後一則訊息。
第一次看見	DEM 伺服器從此裝置接收到的第一則訊息。
使用者狀態	目前使用者的連線狀態。
監控狀態	應用程式測試是否正在裝置上執行。
端點代理程式版本	裝置上安裝的 ADEM 代理程式版本。

遠端站台代理程式管理

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager)	下列授權之一： ❑ Prisma Access 授權 ❑ ADEM Observability 授權或 AI-Powered ADEM 授權

此頁籤提供關於為數位體驗管理啟用的分支 Prisma SD-WAN ION 裝置的詳細資料。使用此頁籤可取得您所有已註冊的 ADEM 遠端站台的相關詳細資料，例如裝置型號、主機名稱、站台狀態、監控狀態（是否為站台啟用監控）、高可用性伺服器的主機名稱（如果有的話），以及遠端站台代理程式版本。

欄名稱	說明
遠端站台名稱	Pisma SD-WAN 分支站台。
裝置型號	Prisma SD-WAN ION 裝置型號。
主機名稱	ION 裝置的主機名稱。
HA 對等主機名稱	該站台是否設定了高可用性待命 ION 裝置。
上次看見	從 ION 裝置傳送至 DEM 伺服器的最後一則訊息。
第一次看見	DEM 伺服器從 ION 裝置接收到的第一則訊息。

 ©2025 Palo Alto Networks, Inc.

欄名稱	說明
站台狀態	站台 ION 裝置與 DEM 代理程式的連線狀態。
監控狀態	站台是否設定為執行應用程式測試。
遠端站台代理程式版本	ION 裝置上安裝的 ADEM 代理程式版本。

健康情況分數設定檔

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager)	下列授權之一： ❑ Prisma Access 授權 ❑ ADEM Observability 授權或 AI-Powered ADEM 授權

在此頁籤中檢視網域健康情況分數詳細資料。

欄名稱	說明
網域健康情況分數指標名稱	列出計算健康情況分數指標的網域。按一下此欄中的網域名稱可檢視其指標（如閾值下限和上限），及其在數值超過閾值時對總分的影響（體驗總分的百分比）。這些指標目前是唯讀的，如管理員所設定。這些項目無法修改。
類型	網域類型
相關聯的使用案例	顯示計算體驗分數的儀表板或 Widget。

ADEM 稽核日誌

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager)	下列授權之一： ❑ Prisma Access 授權 ❑ ADEM Observability 授權或 AI-Powered ADEM 授權

檢視所有因 API 呼叫而觸發之事件的稽核日誌。

©2025 Palo Alto Networks, Inc.

欄名稱	說明
事件時間	觸發事件導致日誌建立的時間。
電郵	建立日誌時收到通知之人員的電子郵件地址。
說明	導致事件觸發從而建立日誌的 API 呼叫。

©2025 Palo Alto Networks, Inc.