

The Palo Alto Networks logo, featuring a stylized orange and red icon to the left of the word "paloalto" in a lowercase, sans-serif font.

TECHDOCS

Strata Cloud Manager 啟動與裝載

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

© 2024-2026 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

April 17, 2026

Table of Contents

啟動您的 Strata Cloud Manager 授權.....	5
啟動 Strata Cloud Manager Essentials.....	6
啟動 Strata Cloud Manager Pro.....	9
從 Panorama 移轉至 Strata Cloud Manager.....	21
從 Panorama 移至 Strata Cloud Manager 時設定管理的變更方式.....	22
準備將 NGFW 移轉至 Strata Cloud Manager.....	23
將您的 Panorama 受管理 NGFW 移轉至 Strata Cloud Manager.....	23
準備移轉至 Prisma Access (Managed by Strata Cloud Manager).....	34
將您的 Prisma Access (Managed by Panorama) 部署移轉至 Strata Cloud Manager.....	35
Strata Cloud Manager 中的裝置關聯.....	47
裝置型號相容性.....	52
防火牆和授權類型相容性.....	57

啟動您的 **Strata Cloud Manager** 授權

若要開始使用 **Strata Cloud Manager**，您需要啟動適當的授權層級：**Essentials** 或 **Pro**。

- **啟動 [Strata Cloud Manager Essentials](#)**：免費層級提供設定管理、網路安全性生命周期管理，並且如果您擁有 [Strata 記錄服務](#) 的付費版授權，則還可以提供可視性。
- **啟動 [Strata Cloud Manager Pro](#)**：此層級提供進階功能以及所有 **Strata Cloud Manager Essentials** 功能。當您啟動 **Strata Cloud Manager Pro** 時，其中也包括 **Strata 記錄服務** 的存取權，該服務提供一年的日誌保留和無限儲存空間。



如果您在引入這些新授權層級之前使用 **Strata Cloud Manager**，則您現有的 **Prisma Access** 和 **AIOps for NGFW Premium** 授權仍會繼續受到支援。您可以繼續修改、延長或續約這些授權。此外，如果您使用 **AIOps for NGFW Free**，您可以選擇升級到 **AIOps for NGFW Premium**。

- [啟動 AIOps for NGFW Premium](#)
- [啟動 AIOps for NGFW Premium 的 ELA](#)
- [啟動軟體 NGFW 積分授權合約](#)
- [啟動您的 Prisma Access 授權](#)
- [ADEM 授權](#)

啟動 Strata Cloud Manager Essentials

Strata Cloud Manager Essentials 是免費層，提供設定和網路安全性生命週期管理功能，可簡化作業並提供基礎的安全性。如需裝置型號支援的詳細資訊，請參閱[裝置型號相容性](#)。

您可以使用 Strata Cloud Manager Essentials 授權層來[啟動由軟體 NGFW 積分資助的 VM-Series](#)。如果您選取的[雲端訂閱不在部署設定檔中](#)，Strata Cloud Manager Essentials 會自動啟動。

STEP 1 | 登入中樞。

STEP 2 | 前往 Strata Cloud Manager Essentials 啟動 URL: <https://apps.paloaltonetworks.com/activation/scm-essentials>。

STEP 3 | 選取客戶支援帳戶。

STEP 4 | **Create New**（新建）[租用戶](#)以便在其中啟動 Strata Cloud Manager。

STEP 5 | 選取您要部署 Strata Cloud Manager 的 **Region**（地區）。請參閱 [Strata Cloud Manager 的支援地區](#)。

地區支援會因您要管理 NGFW、Prisma Access 或同時管理兩者而異。若要同時管理這兩者，您必須選取同時支援 NGFW 和 Prisma Access 的地區。

STEP 6 | 選取[雲端識別引擎](#)或建立新的 CIE 執行個體來識別和驗證基礎結構中的所有使用者。您也可以透過選取 **None**（無）將其略過。

paloalto
Activate Product
Strata Cloud Manager

Select Customer Support Account
This account is used for the registration and support of the products and add-ons that are bundled with this subscription. [Learn more](#)

Customer Support Account: [Edit](#)

Recipient: [Edit](#)

Region: United States - Americas [Edit](#)

Cloud Identity Engine [Done](#)

Create New [v](#)
CIE instance for this tenant

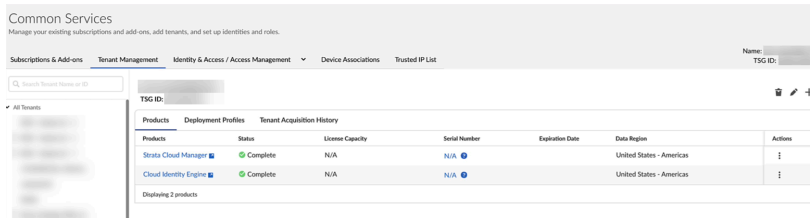
Device Onboarding Steps
You can view the list of devices in the customer support portal. To get the most of the product, follow the onboarding steps below. You can complete these onboarding steps after you finish product activation.

- 1 If you have firewalls: Associate Devices with Tenant**
Go to Settings > Devices Associations to associate devices with the tenant. [Learn more](#)
- 2 If you want to manage configuration in the cloud: Move Devices to Cloud Management**
Move devices to the cloud by following these [steps](#)
- 3 If you want to manage configuration in Panorama**
Please follow the Panorama documentation to configure the devices in Panorama [steps](#)
- 4 Enable Telemetry**
Device telemetry collects data about your device and shares it with Palo Alto Networks by uploading the data to Strata Logging Service. Enable telemetry on the device by following these [steps](#)


STEP 7 | 同意 **Terms and Conditions**（條款和條件），然後 **Activate**（啟動）。

STEP 8 | 等待 Strata Cloud Manager 初始化，並等待 [Status (狀態)] 顯示 [Complete (完成)]。

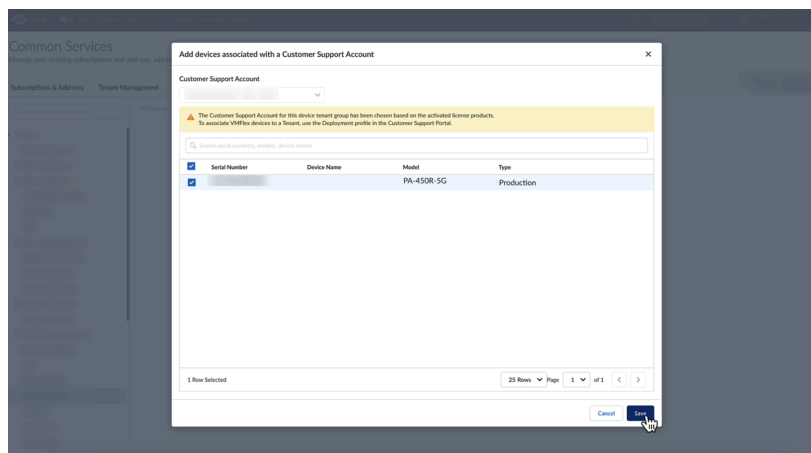
如果您已建立新的雲端識別引擎執行個體，請等待其 [Status (狀態)] 顯示 [Complete (完成)]。



STEP 9 | 將 NGFW、Panorama 或兩者關聯至包含您 Strata Cloud Manager 的租用戶。

 請務必將 *Panorama* 管理的所有防火牆與租用戶個別建立關聯。

1. 導覽至 **Common Services** (常見服務) > **Device Associations** (裝置關聯)。
2. 新增裝置。

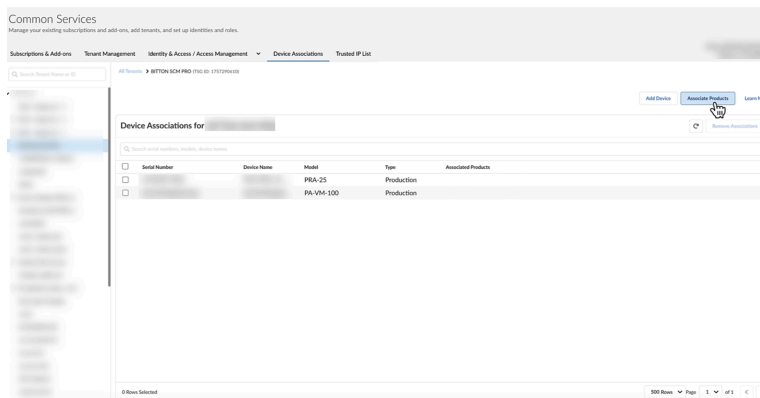


3. 選取一或多個防火牆或 Panorama 設備，然後 **Save** (儲存)。

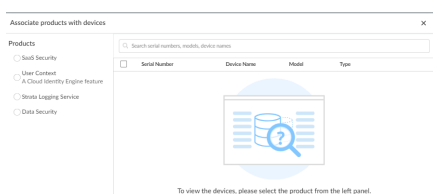
STEP 10 | 如果您有 **Strata 記錄服務**，則可以將其關聯至裝置。否則可以跳過。

啟動 **Strata Cloud Manager Essentials** 後，您可以指定要與 **Strata 記錄服務** 搭配使用的防火牆或 **Panorama** 設備。

1. 選取 **Common Services**（常見服務） > **Device Associations**（裝置關聯）。
2. 關聯產品。




3. 在 [Products（產品）] 選取欄中，選取 **Strata Logging Service**（**Strata 記錄服務**）。



4. 選取裝置並儲存。

STEP 11 | 在裝置上啟用遙測。Strata Cloud Manager 會分析您的 PAN-OS 裝置傳送到 **Strata 記錄服務** 的遙測資料，藉此評估您部署中裝置的健康狀況。若要傳送此資料，您必須在裝置上啟用裝置遙測。

 自 **PAN-OS 12.1.2、11.1.11、11.2.8、10.2.17** 及後續版本開始，**遙測自動啟用功能** 會預設啟用您裝置上的遙測。在載入新裝置（**Panorama** 或防火牆）時，由 **Strata Cloud Manager** 或中樞集中控制的設定會自動啟用遙測。

STEP 12 | 按一下中樞內的圖標以登入 **Strata Cloud Manager**。

啟動 Strata Cloud Manager Pro

Strata Cloud Manager Pro 提供超越 Essentials 授權的進階功能。不同於 Essentials 版本，該版本包括 Strata 日誌服務，並提供一年的日誌保留。如需裝置型號支援的詳細資訊，請參閱[裝置型號相容性](#)。

當您的 Strata Cloud Manager Pro 授權到期時，Strata Cloud Manager 執行個體將還原為 Strata Cloud Manager Essentials 授權層級。其他訂閱的授權到期後，一部份將繼續以有限的容量運行，而另一些將完全停止運作。請參閱[每個訂閱到期時的狀況](#)。

- [NGFW](#)
- [Prisma Access](#)
- 採用軟體 NGFW 積分的 VM-Series
- [ELA](#)
- [ESA Pro](#)

啟動 Strata Cloud Manager Pro for NGFW

此工作顯示如何啟動 Strata Cloud Manager Pro for NGFW。如需裝置型號支援的詳細資訊，請參閱[裝置型號相容性](#)。

NGFW 的先決條件如下：

- [雲端管理裝載先決條件](#) - 在將 NGFW 裝載到 Strata Cloud Manager 之前，請驗證是否已滿足設備就緒的所有條件。這包括網路設定、軟體相容性和授權要求。完成這些步驟可確保您的防火牆可以成功使用 Strata Cloud Manager 進行管理。
- [雲端管理的 TCP 端口和 FQDN](#) - 為了實現 NGFW 和 Strata Cloud Manager 之間的無縫通訊，請設定特定的 TCP 端口和完全合格網域名稱 (FQDN)。

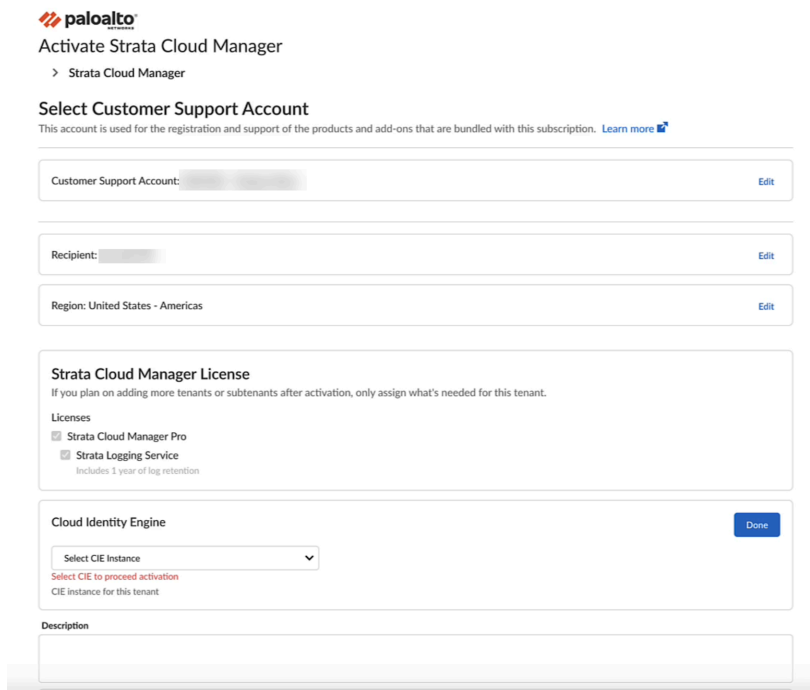
STEP 1 | 當您收到 Palo Alto Networks 的電子郵件，指明您正在啟動的 Strata Cloud Manager Pro 授權時，請按一下電子郵件連結以開始啟動程序。

STEP 2 | 選擇您要使用的客戶支援帳戶。

STEP 3 | **Select Tenant**（選取租用戶），您將在此啟動 Strata Cloud Manager Pro。如果您沒有現有租用戶，請 **Create New**（新建）。

STEP 4 | 選取您要部署 Strata Cloud Manager 的 **Region**（地區）。請參閱 [Strata Cloud Manager 的支援地區](#)。

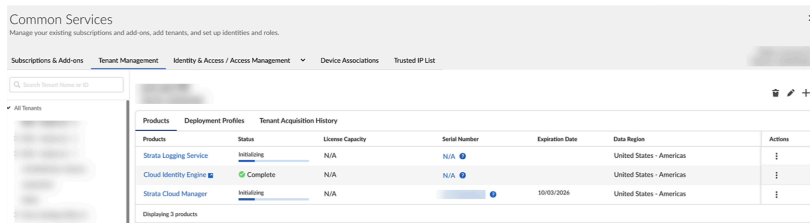
Strata Cloud Manager Pro 包含 [Strata 記錄服務](#)，並提供一年的日誌保留。



STEP 5 | 選取雲端識別引擎或建立新的 CIE 執行個體來識別和驗證基礎結構中的所有使用者。

STEP 6 | 同意 **Terms and Conditions**（條款和條件），然後 **Activate**（啟動）。

STEP 7 | 等待 Strata Cloud Manager、雲端識別引擎和 Strata 記錄日誌服務初始化，並等待 [Status（狀態）] 顯示 [Complete（完成）]。



STEP 8 | 將 NGFW、Panorama 或兩者關聯至包含您 Strata Cloud Manager 的租用戶。

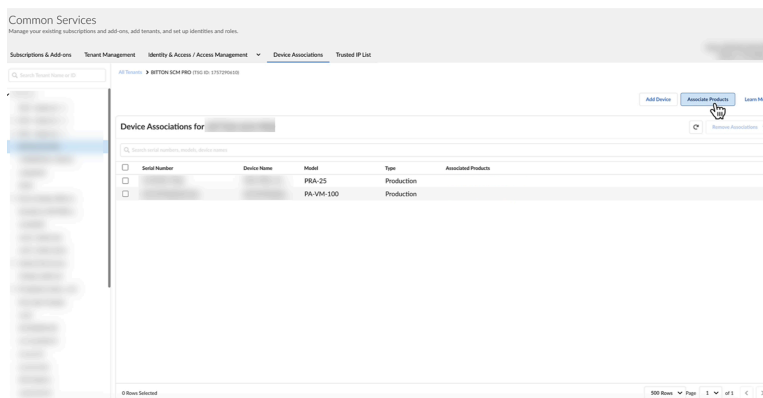


請務必將 *Panorama* 管理的所有防火牆與租用戶個別建立關聯。

1. 導覽至 **Common Services**（常見服務）> **Device Associations**（裝置關聯）。
2. 新增裝置。
3. 選取一或多個防火牆或 Panorama 設備，然後 **Save**（儲存）。


STEP 9 | 將產品關聯至裝置。啟用 Strata Cloud Manager Pro 後，您需要指定要搭配使用的防火牆或 Panorama 設備。

1. 導覽至 **Common Services**（常見服務） > **Device Associations**（裝置關聯）。
2. 關聯產品。



3. 在 [Products（產品）] 選取欄中，選取 **Strata Cloud Manager**。
4. 選取裝置並儲存。

STEP 10 | 在裝置上啟用遙測。Strata Cloud Manager 會分析您的 PAN-OS 裝置傳送到 Strata 記錄服務的遙測資料，藉此評估您部署中裝置的健康狀況。若要傳送此資料，您必須在裝置上啟用裝置遙測。

 自 PAN-OS 12.1.2、11.1.11、11.2.8、10.2.17 及後續版本開始，**遙測自動啟用功能**會預設啟用您裝置上的遙測。在載入新裝置（**Panorama** 或防火牆）時，由 **Strata Cloud Manager** 或中樞集中控制的設定會自動啟用遙測。

STEP 11 | 按一下中樞內的圖標以登入 Strata Cloud Manager。

啟動 Strata Cloud Manager Pro for Prisma Access

所有 **Prisma Access 授權類型**都包括存取 Strata Cloud Manager，所有 Prisma Access 部署都可利用 Strata Cloud Manager 的可視性功能（例如指揮中心和活動洞察）以及**自主 DEM** 監控。

此外，您可以選擇使用 Strata Cloud Manager 進行 **Prisma Access 設定管理**；另一個選擇是使用 Panorama 進行設定管理。在這兩種情況下，Prisma Access 授權啟動期間，系統都會引導您啟動 Strata Cloud Manager Pro：

- 啟動 **Prisma Access**（使用 **Strata Cloud Manager 設定管理**）
- 啟動 **Prisma Access**（使用 **Panorama 設定管理**）

為採用軟體 NGFW 積分的 VM-Series 啟動 Strata Cloud Manager Pro

您可以使用 Strata Cloud Manager 管理由 Software NGFW Credits 資助的 VM-Series 防火牆，透過啟動 Strata Cloud Manager Pro 以無縫存取進階管理和監控功能。

Strata Cloud Manager 支援管理獨立的 VM-Series 防火牆和 Panorama 管理的 VM-Series 部署，提供監控多個環境的全方位解決方案：

- 為 [VM-Series](#) 啟動 [Strata Cloud Manager Pro](#)
- 為 [Panorama](#) 管理的 [VM-Series](#) 啟動 [Strata Cloud Manager Pro](#)

使用企業授權協議啟動 Strata Cloud Manager Pro

此工作顯示如何為 Strata Cloud Manager 啟動企業授權協議 (ELA)。ELA 的附加元件是一種耗用模型，供大型企業將訂閱大量指派至從 Palo Alto Networks 購買的資產。

NGFW 的先決條件如下：

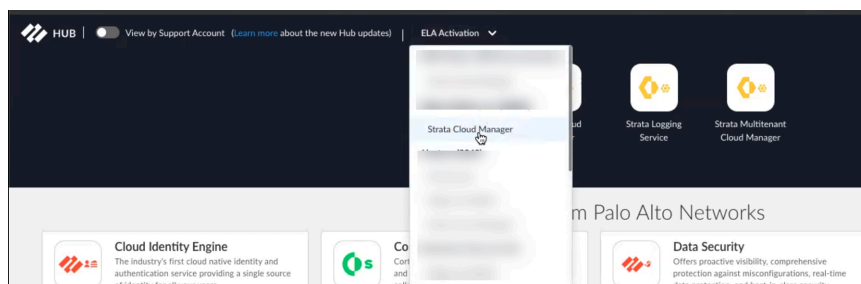
- [雲端管理裝載先決條件](#) - 在將 NGFW 裝載到 Strata Cloud Manager 之前，請驗證是否已滿足設備就緒的所有條件。這包括網路設定、軟體相容性和授權要求。完成這些步驟可確保您的防火牆可以成功使用 Strata Cloud Manager 進行管理。
- [雲端管理的 TCP 端口和 FQDN](#) - 為了實現 NGFW 和 Strata Cloud Manager 之間的無縫通訊，請設定特定的 TCP 端口和完全合格網域名稱 (FQDN)。



針對屬於相同支援帳戶的裝置，您可以使用相同的授權啟動多個 [Strata Cloud Manager Pro](#) 租用戶。若要這麼做，請導覽至 [[Tenant Management](#) (租用戶管理)] 以 [建立新租用戶](#)。接著前往 [Subscriptions & Add-ons](#) (訂閱和附加元件)、搜尋您的訂閱，按一下 [Activate Cloud Tenant](#) (啟動雲端租用戶)，系統會將您重新導向至啟動頁面。在啟動頁面上選擇您最初使用的同一 [TSG](#)。

STEP 1 | 使用下列其中一種啟動方法。

- 登入 [中樞](#)，並選取 [ELA Activation](#) (ELA 啟動) > [Strata Cloud Manager](#)。



- 登入客戶支援入口網站，並從 [License Management](#) (授權管理) > [Licenses](#) (授權) 啟動，然後按一下 [ELA-Ngfw Activation](#) (ELA-Ngfw 啟動)。

STEP 2 | 選擇您要使用的客戶支援帳戶。

STEP 3 | [Select Tenant](#) (選取租用戶)，您將在此啟動 Strata Cloud Manager Pro。如果您沒有現有租用戶，請 [Create New](#) (新建)。

STEP 4 | 選取您要部署 Strata Cloud Manager 的 **Region**（地區）。請參閱 [Strata Cloud Manager 的支援地區](#)。


Strata Cloud Manager Pro 包含 [Strata 記錄服務](#)，並提供一年的日誌保留。

STEP 5 | 選取 [雲端識別引擎](#) 或建立新的 CIE 執行個體來識別和驗證基礎結構中的所有使用者。

STEP 6 | 同意 **Terms and Conditions**（條款和條件），然後 **Activate**（啟動）。

STEP 7 | 等待 Strata Cloud Manager 和 Strata 記錄服務初始化，並確保兩者的 [Activation Status（啟動狀態）] 顯示為 [Complete（完成）]。

STEP 8 | 將 [NGFW](#)、[Panorama](#) 或兩者關聯至包含您 Strata Cloud Manager 的租用戶。


 請務必將 *Panorama* 管理的所有防火牆與租用戶個別建立關聯。

1. 導覽至 **Common Services**（常見服務）> **Device Associations**（裝置關聯）。
2. 新增裝置。
3. 選取一或多個防火牆或 Panorama 設備，然後 **Save**（儲存）。

STEP 9 | 將 [產品關聯](#) 至裝置。啟用 Strata Cloud Manager Pro 後，您需要指定要搭配使用的防火牆或 Panorama 設備。

1. 登入中樞並選取 **Common Services**（共用服務）> **Device Associations**（裝置關聯）。
2. 關聯產品。
3. 在 [Licensed Products（授權產品選取）] 欄中選取 **Strata Cloud Manager**。
4. 選取裝置並儲存。

STEP 10 | 在裝置上啟用遙測。Strata Cloud Manager 會分析您的 PAN-OS 裝置傳送到 Strata 記錄服務的遙測資料，藉此評估您部署中裝置的健康狀況。若要傳送此資料，您必須在裝置上啟用裝置遙測。

 自 PAN-OS 12.1.2、11.1.11、11.2.8、10.2.17 及後續版本開始，遙測自動啟用功能會預設啟用您裝置上的遙測。在載入新裝置（Panorama 或防火牆）時，由 Strata Cloud Manager 或中樞集中控制的設定會自動啟用遙測。

STEP 11 | 按一下中樞內的圖標以登入 Strata Cloud Manager。

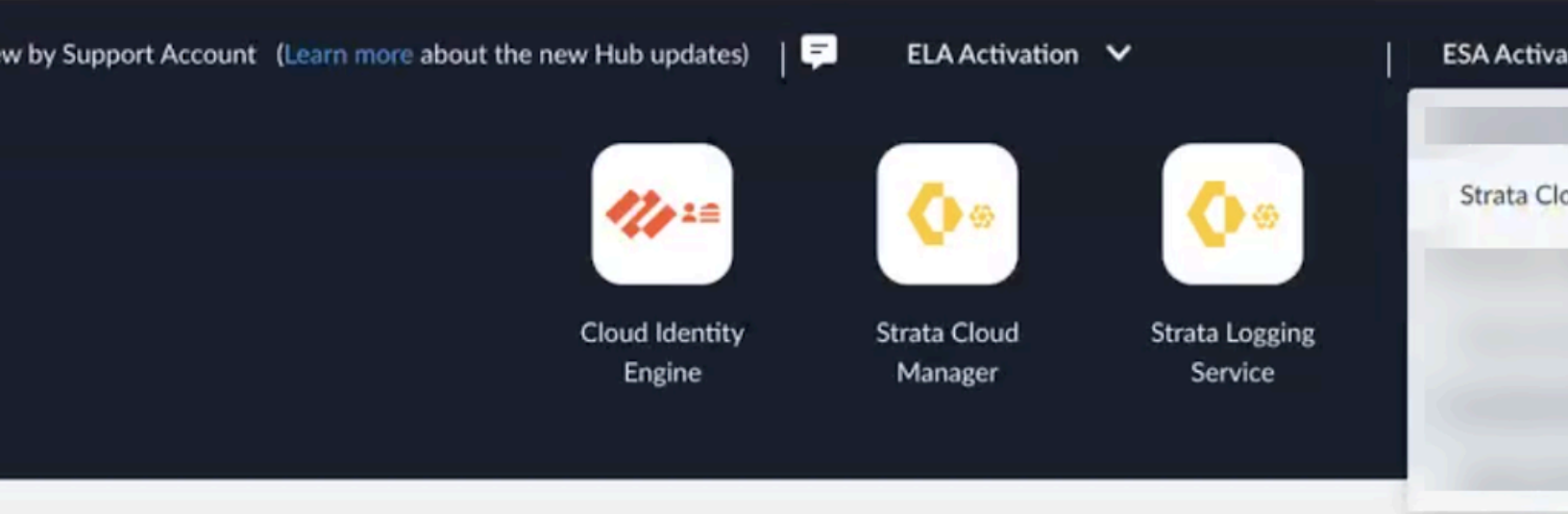
使用企業支援協議啟動 Strata Cloud Manager Pro

Palo Alto Networks 企業支援協議 (ESA) Pro 包括 Strata Cloud Manager Pro for NGFW。ESA Pro 提供一個簡化的解決方案，為您現有的資產和計劃中的購買提供一致的支援體驗。這個企業方案可讓組織在擴大規模時將節省和利益最大化，這對於擁有大型防火牆部署且正在擴展的客戶來說是一個理想的選擇。

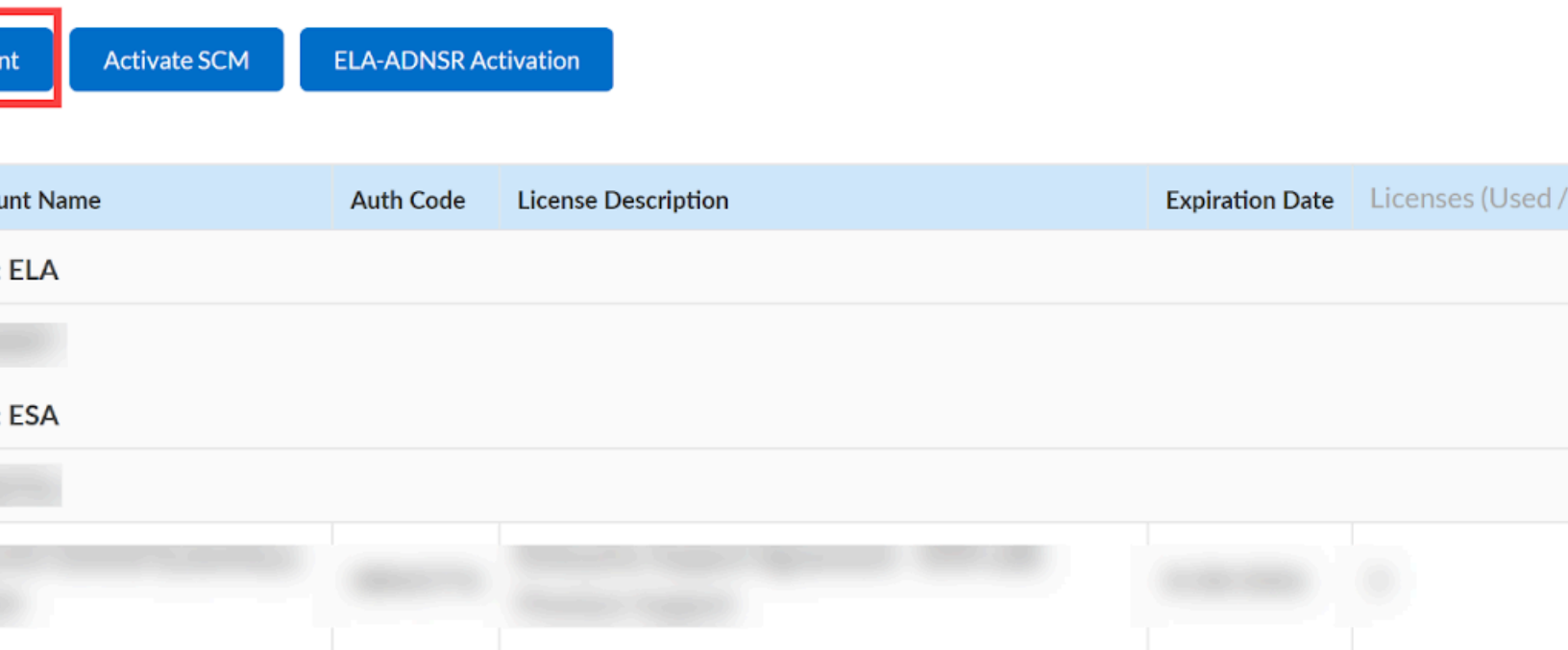
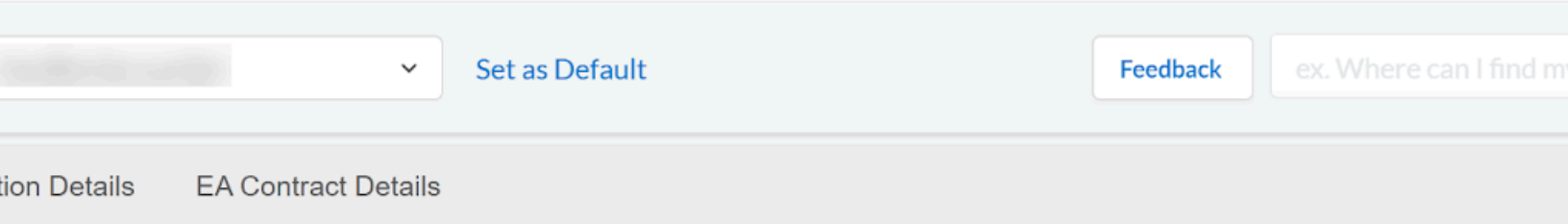
此工作顯示如何為 Strata Cloud Manager 啟動 ESA Pro。您可以按照下列說明，從中樞或客戶支援入口網站開始 ESA Pro 啟動程序。

STEP 1 | 使用以下其中一種啟動方法：

- 登入中樞，並選取 **ESA Activation**（ESA 啟動） > **Strata Cloud Manager**。



- 登入客戶支援入口網站。在左側面板中，轉到 授權管理，然後在 授權 下，選取 啟動企業協議。



STEP 2 | 選擇您要使用的客戶支援帳戶。

STEP 3 | 建立一個 **New**（新）租用戶，您將在其中啟動 Strata Cloud Manager 執行個體。

Strata Cloud Manager

Manager

Manager Pro for NGFW

Account 

Support Account 

Recipient 

where the product will be activated. [Learn more about tenants](#)





STEP 4 | 選取您要部署 Strata Cloud Manager 的 **Region**（地區）。請參閱 [Strata Cloud Manager 的支援地區](#)。

Strata Cloud Manager Pro 授權包括 [Strata 記錄服務](#)，並提供一年的日誌保留。

Manager License

For more tenants or subtenants after activation, only assign what's needed for this tenant.

Manager Pro

ing Service

of log retention

STEP 5 | 選取 [雲端識別引擎](#) 或建立新的 CIE 執行個體來識別和驗證基礎結構中的所有使用者。

STEP 6 | **Agree**（同意）**Terms and Conditions**（條款和條件），然後 **Activate**（啟動）。

STEP 7 | 等待 Strata Cloud Manager 和 Strata 記錄服務初始化，並確保兩者的 [Activation Status（啟動狀態）] 顯示為 [Complete（完成）]。

STEP 8 | 將 [NGFW](#)、[Panorama](#) 或兩者關聯至包含您 Strata Cloud Manager 的租用戶。




請務必將 *Panorama* 管理的所有防火牆與租用戶個別建立關聯。

1. 導覽至 **Common Services**（常見服務）> **Device Associations**（裝置關聯）。
2. 新增裝置。
3. 選取一或多個防火牆或 Panorama 設備，然後 **Save**（儲存）。

STEP 9 | 將產品關聯至裝置。啟用 Strata Cloud Manager Pro 後，您需要指定要搭配使用的防火牆或 Panorama 設備。

1. 登入中樞並選取 **Common Services**（共用服務）> **Device Associations**（裝置關聯）。
2. 關聯產品。
3. 在 [Licensed Products（授權產品選取）] 欄中選取 **Strata Cloud Manager**。
4. 選取裝置並儲存。

STEP 10 | 在裝置上啟用遙測。Strata Cloud Manager 會分析您的 PAN-OS 裝置傳送到 Strata 記錄服務的遙測資料，藉此評估您部署中裝置的健康狀況。若要傳送此資料，您必須在裝置上啟用裝置遙測。

 自 PAN-OS 12.1.2、11.1.11、11.2.8、10.2.17 及後續版本開始，遙測自動啟用功能會預設啟用您裝置上的遙測。在載入新裝置（*Panorama* 或防火牆）時，由 Strata Cloud Manager 或中樞集中控制的設定會自動啟用遙測。

STEP 11 | 按一下中樞內的圖標以登入 Strata Cloud Manager。

從 Panorama 移轉至 Strata Cloud Manager

我可以在哪裡使用這個？	我需要哪些內容？
<ul style="list-style-type: none"> • NGFW (Managed by Panorama) • Prisma Access (Managed by Panorama) 	<p>移轉 NGFW:</p> <ul style="list-style-type: none"> □ Strata Cloud Manager Essentials 或 Pro 授權 □ 確保 NGFW 符合雲端管理的先決條件 <p>移轉 Prisma Access:</p> <ul style="list-style-type: none"> □ Prisma Access 授權 □ 若要開始從 Prisma Access (由 Panorama 管理) 移轉至 Prisma Access (由 Strata Cloud Manager 管理) 移轉，請聯繫 Palo Alto Networks 客戶團隊

Prisma Access 和 NGFW 部署現在都可從 Panorama 移轉至 Strata Cloud Manager，讓您在雲端環境中享有雲端管理和共用設定管理的優勢。這項移轉程序可解決設定保留和政策連續性等考量事項。

對於 NGFW 部署，即使您尚未準備好移轉，您也可以遵循此工作流程來檢閱設定相容性。您可以決定修剪或接受 Strata Cloud Manager 設定管理不支援或部分支援的任何功能。在移轉期間，Strata Cloud Manger 會將 Panorama 裝置群組階層轉換為對應的 Strata Cloud Manager 資料夾結構，並將 Panorama 範本和範本堆疊轉換為可重複使用的片段。

對於 Prisma Access 部署，移轉著重於保留遠端存取基礎結構、行動使用者設定和站台對站台連線，同時將管理監督作業移交給 Strata Cloud Manager。

- [新世代防火牆移轉](#)
- [Prisma Access 移轉](#)

從 Panorama 移轉至 Strata Cloud Manager (NGFW)

您可以將現有 NGFW 設定從 Panorama 移轉到 Strata Cloud Manager 以進行雲端型設定管理。

在移轉期間，Strata Cloud Manager 將會：

- 複製並轉譯支援的安全性政策、網路設定和物件。
- 維護現有的網路拓撲和 NGFW 部署。
- 反白顯示部分支援或不支援的區域。

請聯絡您的 *Palo Alto Networks* 客戶團隊以啟用移轉工作流程。

使用 [Strata Cloud Manager](#) 取代 [Panorama](#) 來管理您的 NGFW 具有多項優點，例如 [Prisma Access](#) 和 NGFW 的統一管理、網路的雲端原生擴充性，以及增強的資訊可視性。

Strata Cloud Manager 會透過以下關鍵步驟引導您移轉設定：

- 上傳現有設定 - 匯入您目前的 [Panorama](#) 設定。
- 執行相容性評估 - 識別需要注意的不支援功能或設定。
- 執行驗證並準備部署 - 在移轉前完成最終檢查。
- 移轉控制 - 可以分階段移轉裝置和裝置群組，讓您可以移轉非關鍵裝置或逐站移轉。

在完成移轉之前，請檢閱每個步驟的結果、進行必要調整，並確認您的設定與 [Strata Cloud Manager](#) 完全相容。

從 Panorama 移至 Strata Cloud Manager 時設定管理的變更方式

[Panorama](#) 設定管理的構成要素為：

- 裝置群組 - 將防火牆組織為安全性政策管理的階層群組（安全性規則、NAT 政策、應用程式篩選器）。
- 範本和範本堆疊 - 定義網路和裝置設定（介面、區域、路由、系統設定）。
- 繼承 - 裝置群組會繼承父系群組的政策；範本堆疊會將多個範本分層，並具有取代功能。

[Strata Cloud Manager](#) 設定管理的構成要素為：

- 資料夾 - 包含安全性政策以及網路設定的階層式容器。
- 片段 - 可重複使用的設定區塊，可附加至任何層級的資料夾。
- 容器 - 針對唯一防火牆需求，存放裝置特定設定的區域。

在移轉期間，[Strata Cloud Manager](#) 會轉換 [Panorama](#) 型設定，並將其建置為資料夾和片段：

Panorama	Strata Cloud Manager
裝置群組	資料夾
範本與範本堆疊	片段
共用 DG	所有防火牆資料夾

Panorama	Strata Cloud Manager
共用物件	全域資料夾作為附加的片段
裝置群組中的政策	對應資料夾下的政策
物件（位址、EDL 等）	對應資料夾下的物件

Panorama 與 Strata Cloud Manager 之間需注意的主要差異：

- **Strata Cloud Manager** 資料夾同時包含網路和安全性設定，而 **Panorama** 則會將這些設定分散於範本和裝置群組
- 相較於 **Panorama** 所提供的較低層級群組取代，**Strata Cloud Manager** 資料夾可透過片段型取代提供更彈性的繼承
- 相較於 **Panorama** 的範本和範本堆疊，**Strata Cloud Manager** 片段提供更立即可用的設定方法。

移轉之後，您可透過資料夾和片段模型來管理設定。片段附件順序會決定設定的優先順序，可精確控制多個設定來源的合併方式。針對在資料夾繼承模型以外需要唯一設定的 NGFW，您可以為其建立裝置特定的容器。



額外資源

進一步瞭解 [裝置群組](#) 和 [範本](#)。

進一步瞭解 [片段](#) 和 [資料夾](#)

準備將 NGFW 移轉至 Strata Cloud Manager

開始移轉之前，請確保您已準備好下列項目：

- 最低軟體需求：PAN-OS 10.2.3 或更新版本
- [匯出 Panorama 設定檔案](#)：從來源 Panorama 執行個體匯出 XML 格式的完整執行設定
- [Panorama 主要金鑰](#)：取得 Panorama 設定中用於加密的主要金鑰（如果未使用預設金鑰）
- [Strata Cloud Manager 租用戶](#)：確認您的 Strata Cloud Manager 租用戶已部署、正確授權且可運作
- [NGFW 設定](#)：從您計劃在移轉後驗證的 NGFW 收集上次推送的設定檔案（技術支援檔案）
- [網路拓撲](#)：檢閱目前裝置群組階層、範本關係和 NGFW 指派
- [設定備份](#)：建立目前 Panorama 和 NGFW 設定的完整備份作為安全措施
- [管理存取權](#)：確保您在 Panorama 和 Strata Cloud Manager 中都具備超級使用者角色存取權。
- 移轉規劃：識別您在初始階段中要移轉的裝置群組、範本和 NGFW
- [相容性矩陣](#)：瞭解 Strata Cloud Manager 中可能不支援的功能，並規劃任何必要的設定調整

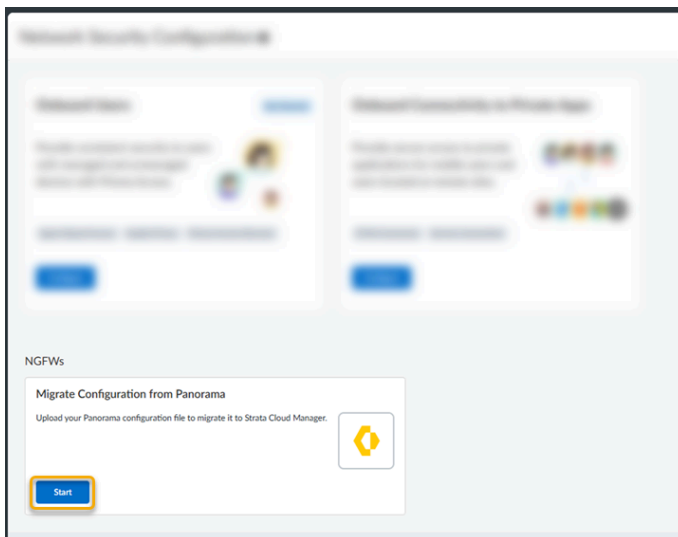
將您的 Panorama 受管理 NGFW 移轉至 Strata Cloud Manager

將 NGFW 設定從 Panorama 移轉至 Strata Cloud Manager：

STEP 1 | 準備您的 Panorama 進行移轉。

1. 使用獲指派**超級使用者**角色的管理帳戶登入管理 NGFW 的 Panorama。
2. **(選用)** 如果您已為 Panorama 設定自訂主要金鑰，請將其記下。
如果您的部署使用預設主要金鑰，則不需要此步驟。
3. 確保您目前的 Panorama 設定是最新狀態，並且您已提交目前的所有變更，並將其推送到 Panorama，方法是前往 **Commit** (提交) > **Commit & Push** (提交並推送)，並 **Preview Changes** (預覽變更)。
4. **(選用)** 檢查執行中設定與候選設定之間的差異，並確定您是否要推送這些變更。若要提交並推送變更，請 **Edit Selections** (編輯選取項目)，並在 **Push Scope** (推送範圍) 中選取您想要推送的 NGFW。
5. **(選用)** **Commit and Push** (提交並推送) 您的變更。
6. 前往 **Panorama > Setup** (設定) > **Operations** (操作)，並 **Export** (匯出) 具名 Panorama 設定快照。
在移轉過程中，需要透過 .xml 檔案上傳到 Strata Cloud Manager。請勿上傳技術支援檔案或 .xml 設定檔案以外的任何其他檔案。
7. 選取 **running-config.xml** 設定檔案，然後按一下 **OK** (確定)。

STEP 2 | 以具有超級使用者角色的管理員身分登入 Strata Cloud Manager，然後前往 **Configuration** (設定) > **Onboarding** (裝載)。



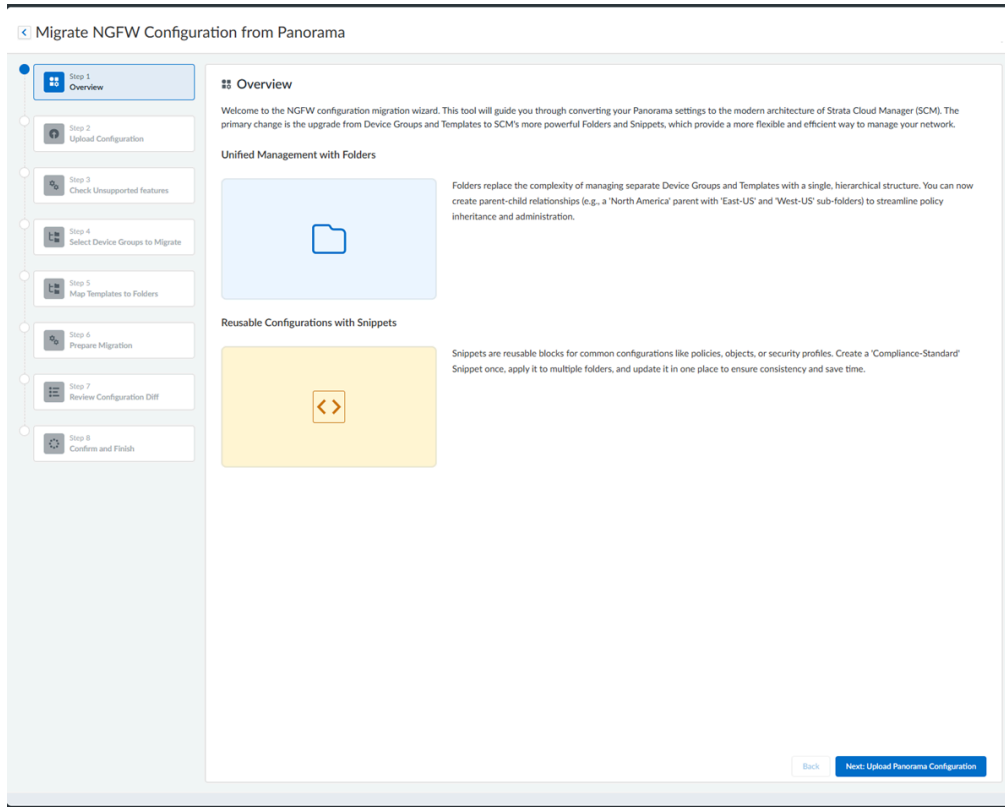
移轉程式偵測到您有 Panorama 受管理部署。

1. 確認租用戶正確無誤。
2. **(選用)** 針對需要回復的狀況，請為執行中的設定 [建立具名快照](#)。



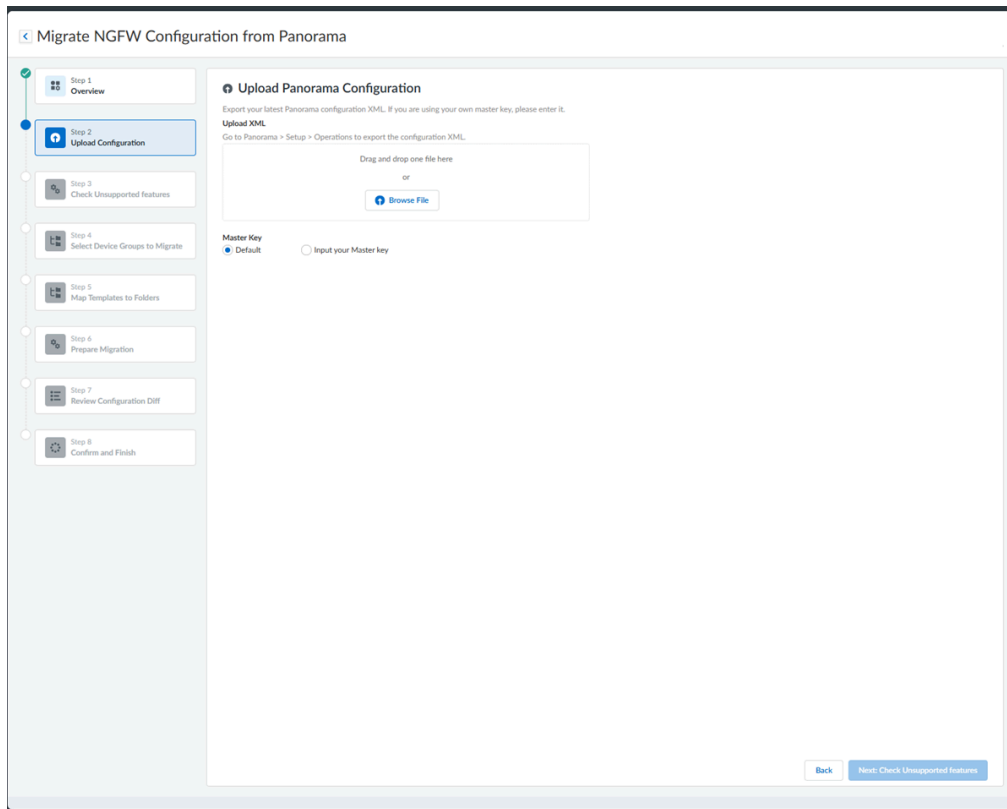
不應在 *Strata Cloud Manager* 升級時段嘗試移轉。請檢查您的升級排程，以確認是否有即將進行的升級。

STEP 3 | 閱讀移轉 Overview (概要)。



1. 檢閱 Strata Cloud Manager 的管理建置區塊：**Folders** (資料夾) 和 **Snippets** (片段)。
2. 按一下 **Next** (下一步)：**Upload Panorama Configuration** (上傳 Panorama 設定)。

STEP 4 | 上傳 Panorama 設定。



1. 從檔案總管拖放或是選取 **Choose File**（選擇檔案），藉此選取您在先前步驟中下載的 Panorama 設定 *.xml* 檔案。
2. （選用）輸入您的 **Master Key**（主要密鑰），或者如果您沒有建立自訂主要密鑰，則會使用 **Default**（預設值）的主要金鑰。

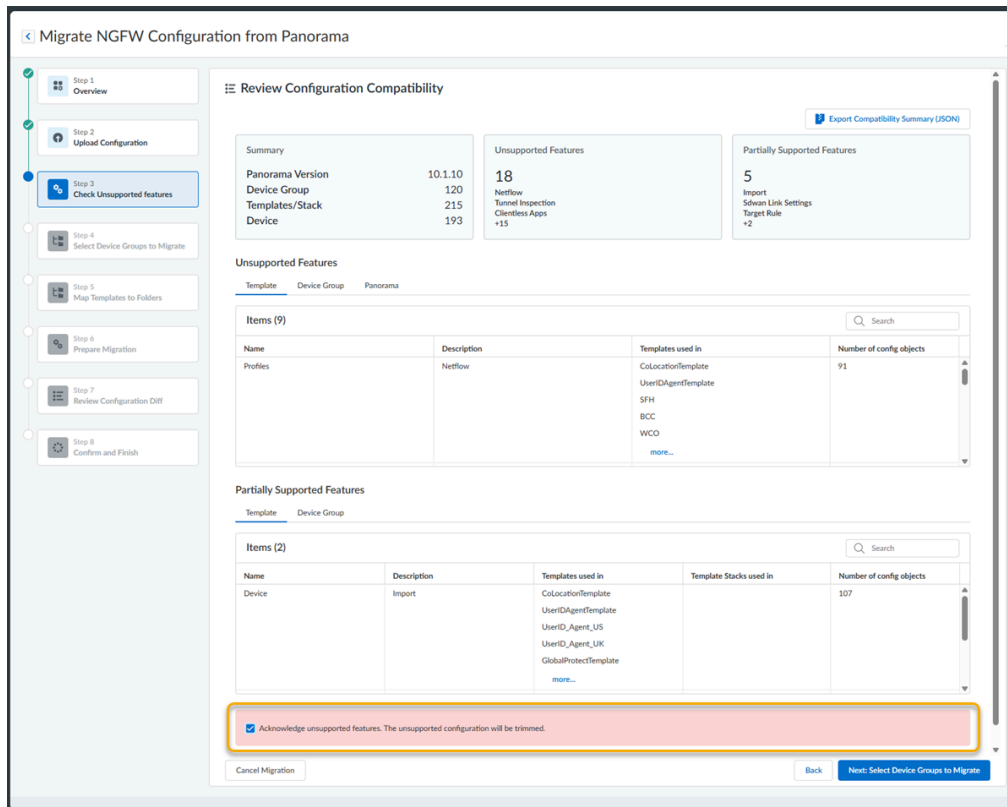
Master Key

Default Input your Master key

Master Key *

3. 按一下 **Next**（下一步）：**Review Migration Compatibility**（檢閱移轉相容性）。

STEP 5 | 檢閱設定相容性。

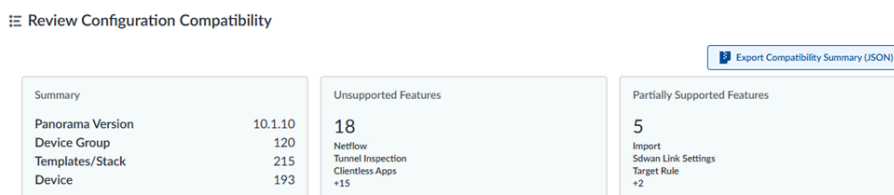


1. (選用) 繼續之前，請先 **Export Compatibility Summary** (匯出相容性摘要) 並檢閱您組織的設定相容性，並允許 **Strata Cloud Manager** 修剪任何不受支援或部分支援的設定。

修剪不受支援和部分支援的功能可避免無法在 **Strata Cloud Manager** 中妥善或安全部署的功能受到移轉。

此程序只會影響 **Strata Cloud Manager** 的分階段設定。Panorama 中的設定將維持不受影響。

對於每個標記的區域，您應該計劃重新建立、取代或暫緩這些設定。



2. 檢閱您設定中將在移轉期間修剪的 **Unsupported Features** (不受支援功能)。
系統將從您的設定中修剪掉這些功能，不會在設定移轉程序中準備匯入 **Strata Cloud Manager** 中。
3. 檢閱 **Partially Supported Features** (部分支援的功能) 並確定解決路徑。
確定設定中將缺少的內容。

您可以接受部分支援的功能，並建立移轉後的修復計劃，或返回 Panorama 設定並清除這些區域，然後再重新開始移轉程序。

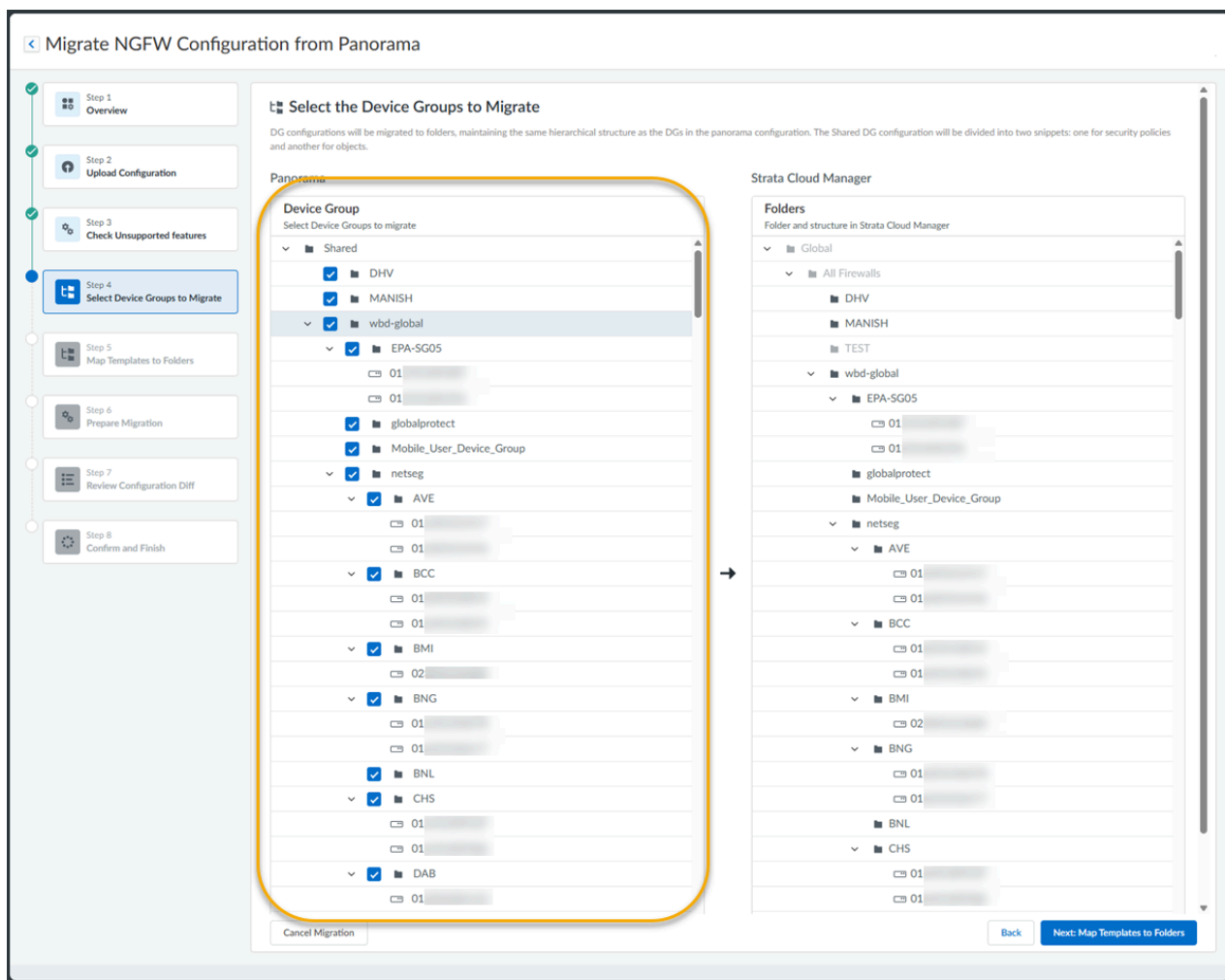
4. **Acknowledge**（確認）不受支援和部分支援的功能。
5. 按一下 **Next**（下一步）：**Select Device Groups to Migrate**（選取要移轉的裝置群組）。



如果只是想比較支援的設定，或者判斷是否需要更多規劃，您可以在這裡結束移轉程序。

STEP 6 | 選取您要移轉的 **Devices**（裝置）或 **Device Groups**（裝置群組）。

 如果您是第一次從 *Panorama* 移轉 NGFW，建議您先僅移轉非關鍵裝置或裝置群組，以測試您的設定將如何移轉到 *Strata Cloud Manager*。



在移轉期間：

- 物件會匯入至片段，並附加至全域資料夾。
- 政策會匯入工作流程所移轉的資料夾下。
- 共用裝置群組會自動對應至所有防火牆資料夾。

1. 按一下 **Next**（下一步）：**Map Templates to Folders**（將範本對應至資料夾）。

STEP 7 | 將 **Templates**（範本）對應至新設定的 **Folders**（資料夾）。

Migrate NGFW Configuration from Panorama

Step 1 Overview

Step 2 Upload Configuration

Step 3 Review Configuration Compatibility

Step 4 Select Device Groups to Migrate

Step 5 Map Templates to Folders

Step 6 Prepare Migration

Step 7 Review Configuration Diff

Step 8 Confirm and Finish

Map Templates to Folders

Auto Template Mapping
This option automatically associates the template and template stack configuration, after being migrated to snippets, to the respective folders.

Manual Template Mapping
This option enables administrators to manually associate template and template stack configurations with folders after migration to snippets.

Rule: You must assign every Template and Template Stack to a folder. They will be imported into SCM as Snippets.
Recommendation: We recommend assigning commonly used configurations to a shared folder (like "All Firewalls") for more efficient management later.


Shared

- US
 - 11111
 - 22222
- US-West
 - 33333
- California
 - 44444**

Templates/Template Stacks used in 44444

Name	SHARED		SCOPED (44444)	
	Referenced Template Stack / Total	Referenced NGFW / Total	Referenced Template Stack / Total	Referenced NGFW / Total
Template Stacks (1)				
ts4	N/A	1/4	N/A	1/1
Templates (3)				
tpl-Common	4/4	4/4	1/1	1/1
tpl-US-West	2/4	2/4	1/1	1/1
tpl-VM	2/4	2/4	1/1	1/1

在移轉過程中，**Templates**（範本）會設定為對等的 **Snippets**（片段）。

 如果兩個以上的裝置群組重複使用相同範本，請將其提升至較高層的資料夾。如果只有一個網站需要該群組，請將其保持在網站層級。

1. 選取 **Device Group**（裝置群組）以顯示該裝置群組使用的 **Templates/Template Stacks**（範本/範本堆疊）。

Strata Cloud Manager 啟動與裝載

30

©2026 Palo Alto Networks, Inc.

AVE-STACK

Associate the migrated snippets to either the folder or the device, depending how they are applied within the Panorama configuration.

Name	Attached Snippets
▼ All Firewalls	0
▼ <input checked="" type="checkbox"/> wbd-global	1
▼ <input type="checkbox"/> netseg	0
▼ <input type="checkbox"/> AVE	0
<input type="checkbox"/> 01 [redacted]	0
<input type="checkbox"/> 01 [redacted]	0
▼ <input type="checkbox"/> BCC	0
<input type="checkbox"/> 01 [redacted]	0
<input type="checkbox"/> 01 [redacted]	0
▼ <input type="checkbox"/> BMI	0
<input type="checkbox"/> 02 [redacted]	0

Referenced Template Stack Referenced NGFW

Referenced NGFWs (2)

Name
01 [redacted]
01 [redacted]

* Required Field

2. **Edit**（編輯）對應以將每個 **Template/Template Stack**（範本/範本堆疊）指派給 **Folder**（資料夾）。
3. 將有多個位置參考的範本提升至較高的資料夾。
 例如，如果您有全域範本設定，將其對應至所有防火牆資料夾會將這些設定建立為所有 NGFW 的來源。
4. 將多個片段指派給資料夾後，請調整順序。
5. **Move Up**（上移）或 **Move Down**（下移）以完成訂單。
6. **Update**（更新）順序。
7. **Save**（儲存）新順序。

在繼續進行下一步之前，請確保以下事項：

- 沒有剩餘未指派的範本或範本堆疊。
 - 任何由多個裝置群組參考的範本都已提升至適當的資料夾。
8. 按一下 **Next**（下一步）：**Prepare Migration**（準備移轉）。

移轉程序隨即開始。

等待所有步驟完成。



如果移轉發生任何問題，請返回先前的步驟進行評估和變更。如果問題仍然存在，請聯絡 *Palo Alto Networks* 支援。

STEP 8 | 準備移轉。

1. **Load Configuration to Strata Cloud Manager**（將組態載入至 **Strata Cloud Manager**）以準備移轉。

1. 移轉工作流程：

- 使用您定義的對應和片段順序，將裝置和裝置群組以及範本和範本堆疊轉譯為資料夾和片段。
 - 建立 **Strata Cloud Manager** 快照以啟用暫存變更的回復。
 - 檢查現有 **Strata Cloud Manager** 設定中的衝突（名稱衝突、缺少參考、31 個字元限制、RBAC 範圍）。
 - 建置載入後將位於 **Strata Cloud Manager** 中的暫存設定。
2. **Load Results**（載入結果）並檢閱已建立、更新或跳過的物件、政策或片段。
 3. 檢閱 **Validation Results**（驗證結果）中是否有任何移轉後的錯誤、警告和資訊訊息。
 4. 按一下 **Next**（下一步）：**Review Config Diffs**（檢閱組態差異）。
這會將新產生的設定提交到 **Strata Cloud Manager**。

STEP 9 | 檢閱設定差異。

1. 在左側資料夾樹狀結構中，展開至 [Folder (資料夾)]，然後選取要驗證的 NGFW 序號
2. **Browse File** (瀏覽檔案) 並選擇所選序號的 TSF。

上傳所選 NGFW 的 TSF 可讓您正確驗證所有支援、部分支援和不支援的設定。

請務必找出已建立、修改或刪除的任何內容。如果設定遭到修剪，這是正常情況。



由於 *Strata Cloud Manager* 中的命名慣例，某些長名稱將視需要壓縮。

3. 檢閱設定差異窗格。
 1. 綠色窗格：已建立或新增。這些設定存在於 *Strata Cloud Manager* 中，但不在原始裝置上。
 2. 紅色窗格：已刪除或修剪。位於裝置上，但 *Strata Cloud Manager* 中可能不支援。
 3. 黃色窗格：已修改



差異檢視可能很廣泛，限制為一次一個 NGFW，並根據 TSF 上次推送的 XML 計算。

4. 請確認每種模式或網站類型代表性裝置的差異。
5. (選用) 匯出差異結果。
6. (選用) 如果進行了任何更正，請 **Regenerate Diff**s (重新產生差異)。
7. 按一下 **Next** (下一步)： **Confirm and Finish** (確認並完成)。


STEP 10 | **Confirm** (確認) 並完成將 NGFW 移轉至 *Strata Cloud Manager*。

移轉完成後，請檢閱 *Strata Cloud Manager* 的可用 [說明文件](#)。

1. 請確保已接受步驟 8 和 9 中的結果。
2. **Confirm** (確認) 移轉。
這會正式將移轉標記為完成。
3. (選用) 若在任何時間點想將設定還原為其移轉前狀態，請選取 **Revert** (還原)。這會啟動回復工作流程，將 *Strata Cloud Manager* 還原至移轉載入前儲存的快照。
4. (選用) 若在任何時間點想取消移轉，請選取 **Cancel Migration** (取消移轉)。這會中止移轉程序，並清除任何暫時變更。

從 Panorama 移轉至 Strata Cloud Manager (Prisma Access)

如果您有其設定由 Panorama 管理的現有 Prisma Access 部署，並想要將其移轉至 Strata Cloud Manager 進行設定管理，Palo Alto Networks 提供了產品內工作流程，讓您可將現有的 Prisma Access 設定移轉至 Strata Cloud Manager。

 若要啟用移轉工作流程，您必須聯繫您的 *Palo Alto Networks* 帳戶團隊。

使用 Strata Cloud Manager 而不是 Panorama 管理您的 Prisma Access 設定，可以為您提供以下好處：

- 持續[最佳做法評估](#)
- 安全預設設定
- 機器學習 (ML) 型設定最佳化
- 簡化了 Web 安全性工作流程
- 互動式視覺摘要（[控管中心](#)）可協助您評估網路的健康情況、安全性和效率
- 適用於複雜工作的直覺[工作流程](#)
- 簡單、安全的[管理 API](#)
- 雲端原生架構提供可擴展性、彈性和全球影響力
- 沒有要管理的硬體或要維護的軟體

準備移轉至 Prisma Access (Managed by Strata Cloud Manager)

在開始移轉之前，您應該了解最低軟體需求，以及您可以移轉的 Prisma Access (Managed by Panorama) 部署類型。

- 何時移轉—請勿在資料平面或基礎結構升級期間執行升級。檢查您的[升級偏好設定](#)，以查看是否有即將進行的資料平面升級。
- 從 **Panorama** 單向移轉至 **Prisma Access (Managed by Strata Cloud Manager)**—您只能從 Prisma Access (Managed by Panorama) 移轉至 Prisma Access (Managed by Strata Cloud Manager) 部署。在移轉至 Strata Cloud Manager 之後，您無法返回使用 Panorama 管理您的 Prisma Access 部署。
- 最低 **Panorama** 版本—最低必要 Panorama 版本為 10.0。
- 必要管理員角色—您必須以 Strata Cloud Manager 中的超級使用者身分登入，才能開始移轉。
- 授權需求#需要有效的 Prisma Access 授權。
- 雲端識別引擎—移轉前您必須已[整合雲端識別引擎的目錄同步元件](#)與目前的 Prisma Access (Managed by Panorama) 租用戶。

- 不受支援的功能—移轉程序不支援以下 Prisma Access 功能：
 - 資料篩選（或者，使用企業 DLP 替代）
 - FedRAMP 部署
 - IoT 安全性
 - 多租用戶 <https://docs.paloaltonetworks.com/prisma-access/administration/manage-multiple-tenants-in-prisma-access> 部署
 - SSH Proxy
 - GlobalProtect 入口網站和閘道的單獨驗證
- Prisma SD-WAN 和 Prisma Access 移轉—如果您移轉 Prisma Access 和 Prisma SD-WAN 部署，Prisma Access 和 Prisma SD-WAN 必須共用相同的租用戶服務群組 ID (TSG ID)。
- Config Diff Issues（設定差異問題）—當您在移轉期間執行設定差異時，請忽略顯示下列物件名稱的任何差異，因為這不會影響您的設定：
 - Clientless-vpn crypto-settings
 - Hip-profiles rename
 - Mobile-user-redundancy
 - Exclude-video-traffic

將您的 Prisma Access (Managed by Panorama) 部署移轉至 Strata Cloud Manager

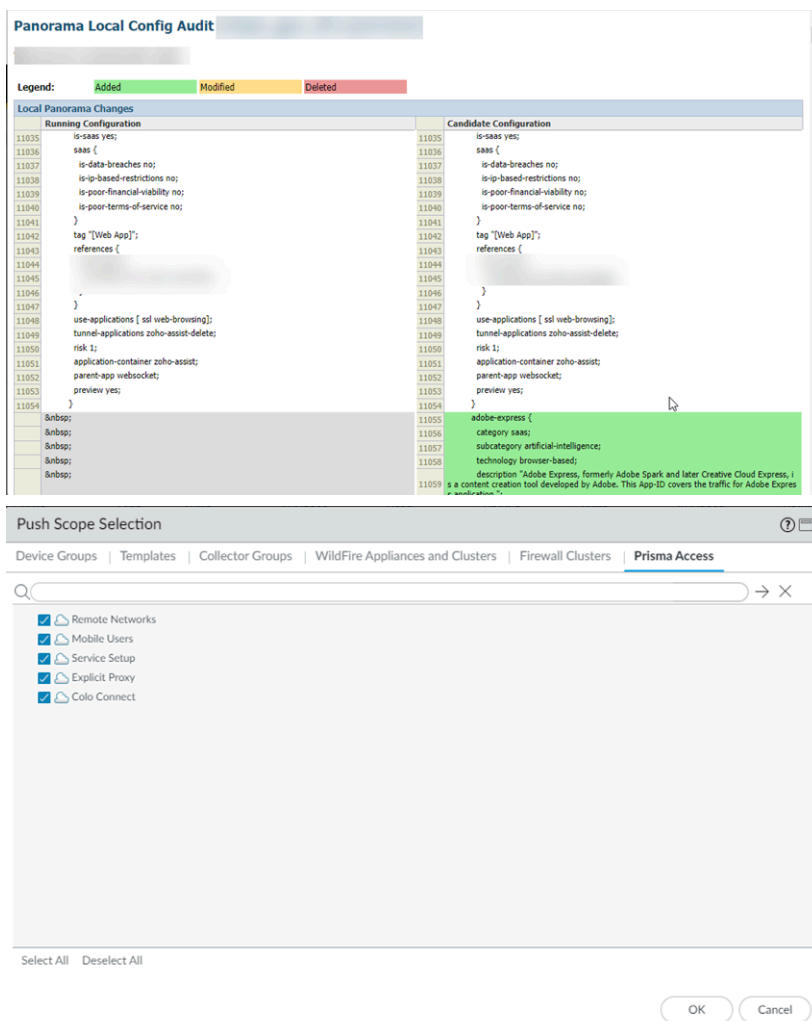
若要將您的 Prisma Access (Managed by Panorama) 移轉至 Prisma Access (Managed by Strata Cloud Manager) 部署，請完成以下步驟。

在較高的層級上，您：

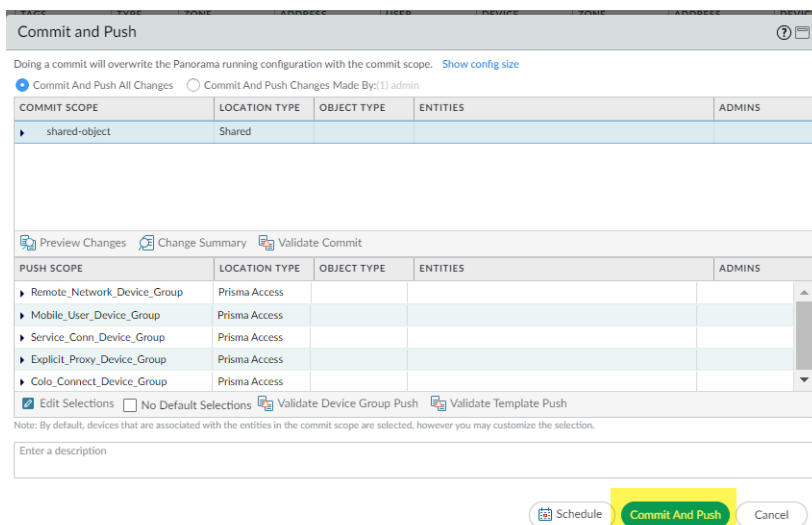
1. 確保您已成功將最新設定推送到 Prisma Access、已儲存最新設定，並已從管理 Prisma Access 的 Panorama 匯出 .xml 設定檔案。
2. 從 Strata Cloud Manager 啟動移轉程式。
3. 檢查 Panorama 設定與移轉後 Strata Cloud Manager 設定之間的設定差異。
4. 解決差異並完成移轉。

STEP 1 | 準備您的 Panorama 進行移轉。

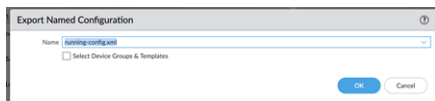
1. 使用指派給超級使用者角色的管理帳戶登入管理 Prisma Access 的 Panorama。
2. **(選用)** 如果您已為 Panorama 以及為 Prisma Access 設定了自訂**主要金鑰**，請記下它。如果您的部署使用預設主要金鑰，則不需要此步驟。
3. 確保您目前的 Panorama 設定是最新的，並且您已提交所有變更並將其推送到 Panorama 和 Prisma Access，方法是前往 **Commit (提交) > Commit & Push (提交並推送)**，並 **Preview Changes (預覽變更)**。
4. **(選用)** 檢查執行中設定與候選設定之間的差異，並確定您是否要推送這些變更。如果您想要提交並推送變更，請 **Edit Selections (編輯選取項目)**，並在 **Push Scope (推送範圍)** 中選取您想要推送的 Prisma Access 元件。



5. **(選用)** **Commit and Push (提交並推送)** 您的變更。



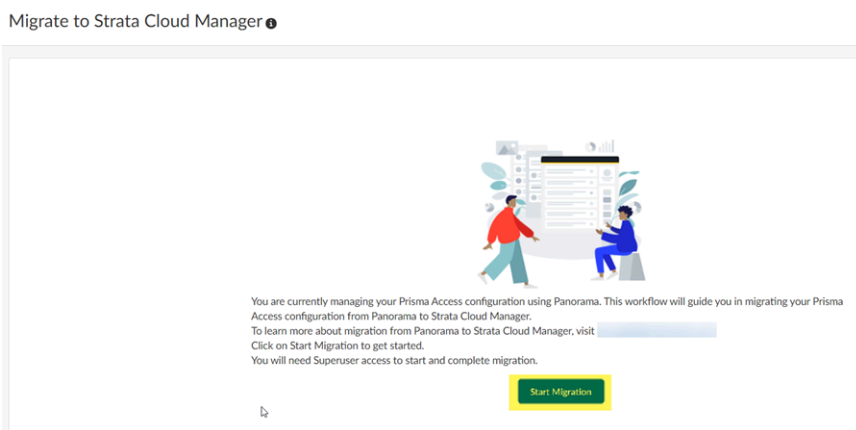
6. 前往 **Panorama > Setup (設定) > Operations (操作)**，並 **Export named Panorama configuration snapshot (匯出具有名 Panorama 設定快照)**。
- 在移轉過程中，此 .xml 檔案需要上傳至 Strata Cloud Manager。請勿上傳技術支援檔案或 .xml 設定檔案以外的任何其他檔案。
7. 選取 **running-config.xml** 設定檔案並選取 **OK (確定)**。



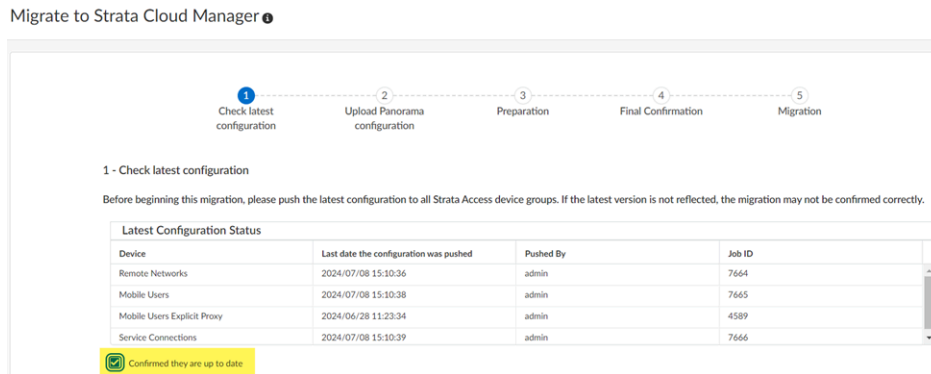
STEP 2 | 以具有 **超級使用者角色** 的管理員身分登入 Strata Cloud Manager，並前往 **Manage (管理) > Configuration (設定) > NGFW and Prisma Access (NGFW 和 Prisma Access) Configuration (設定) > NGFW and Prisma Access (NGFW 和 Prisma Access)**。

移轉程式偵測到您有 Panorama 受管理部署。

STEP 3 | 開始移轉。



STEP 4 | 移轉程式要求您確保您的設定是最新的，並顯示上次更新它的使用者。在驗證了此設定具有最新變更之後，請選取 **Confirmed they are up to date**（已確認它們是最新的），然後按一下 **Next**（下一步）。



STEP 5 | 透過拖放方式選取您在先前步驟中下載的 Panorama 設定 .xml 檔案，或 **Choose File**（選擇檔案）。

STEP 6 | 輸入您的 **Master Key**（主要密鑰），或者如果您沒有建立自訂**主要密鑰**，請要求 Strata Cloud Manager 使用 **Default**（預設）主要金鑰並按一下 **Next**（下一步）。

The screenshot shows the '2 - Upload Panorama Configuration' step of a migration wizard. At the top, a progress bar indicates five steps: 1. Check latest configuration (completed), 2. Upload Panorama configuration (current step), 3. Preparation, 4. Final Confirmation, and 5. Migration. The main content area is titled '2 - Upload Panorama Configuration' and includes the instruction: 'Export your latest Panorama configuration XML. If you are using your own master key, please enter it.' Below this, there is a section for 'Upload Panorama configuration XML' with a file upload area containing a 'Browse' button and a file named '2153.xml' (160 KB) with a progress bar. At the bottom, there is a 'Master Key' section with two radio buttons: 'Default' (selected) and 'Input your Master key'. At the bottom right of the form, there are 'Cancel Migration' and 'Next' buttons.

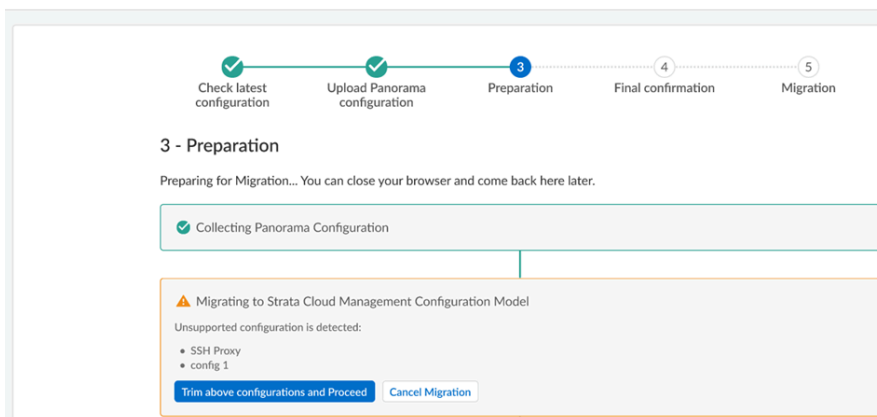
移轉計劃開始。

The screenshot shows the '3 - Preparation' step of the migration wizard. The progress bar at the top shows steps 1 and 2 completed, step 3 as the current step, and steps 4 and 5 as future steps. The main content area is titled '3 - Preparation' and includes the instruction: 'Preparing for Migration... You can close your browser and come back here later.' Below this, there is a vertical list of five tasks: 'Collecting Panorama Configuration' (completed), 'Migrating to Strata Cloud Management Configuration Model' (completed), 'Onboarding Strata Cloud Manager Configuration Service (Takes up to 5 minutes)' (in progress), 'Loading and Validating Migrated Configuration (Takes up to 5 minutes)' (pending), and 'Generate Push Configuration Changes for Preview' (pending). At the bottom right of the form, there are 'Cancel Migration' and 'Next' buttons.

等待所有步驟完成。

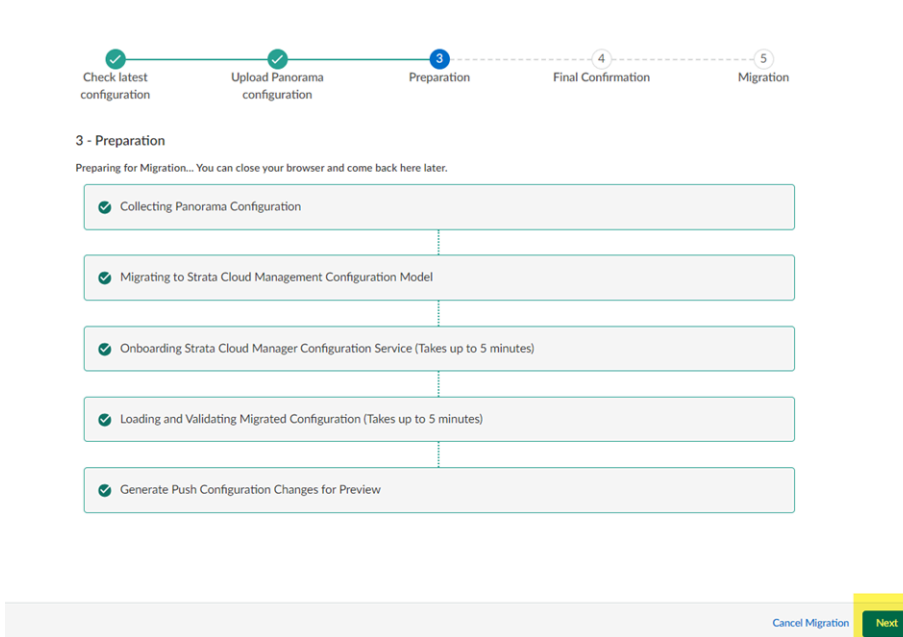
STEP 7 | 如果在移轉過程中程式指出遇到不受支援的設定，您可以 **Trim the above configurations and proceed**（修剪上述設定並繼續）或 **Cancel migration**（取消移轉）。

Migrate to Strata Cloud Manager



某些不受支援的設定（例如多租用戶設定）會取消移轉，且移轉程式無法解決問題；在此情況下，請 **Cancel migration**（取消移轉）。

STEP 8 | 移轉完成後，請按一下 **Next**（下一步）。



STEP 9 | 如果移轉程式進行了變更，請在最終確認畫面中檢閱它們。

移轉程式可能會對您的設定進行變更，以說明 Panorama 和 Strata Cloud Manager 設定中的差異，或修復不支援的功能。如果需要變更，移轉程式會在差異檢視中顯示這些變更，其中新增行以綠色顯示，已刪除行以紅色顯示。



忽略顯示以下物件名稱的任何差異；它們不會影響您的設定：

- *Clientless-vpn crypto-settings*
- *Hip-profiles rename*
- *Mobile-user-redundancy*
- *Exclude-video-traffic*

4 - Final Confirmation

There are differences in the configurations. If everything is OK, click the Complete Migration button.

Cloud Service Plugin Policies and Objects

Prisma Access Mobile Users Mobile Users Explicit Proxy Remote Networks Service Connections

Items (3)

Object Name	Config Diff Type	Object Type	Acknowledge
Backbone Routing	Modified	backbone-routing	<input type="checkbox"/>
Traffic Steering	Deleted	traffic-steering	<input type="checkbox"/>
Cloud_services	Deleted	cloud_services	<input type="checkbox"/>

Backbone Routing	
1 {	1 {
2 - "backbone-routing": "no-asymmetric-routing"	2 + "backbone-routing": "asymmetric-routing-only"
3 }	3 }

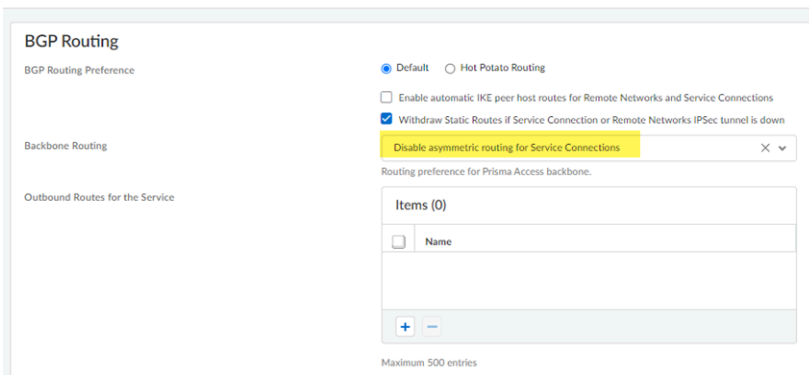
STEP 10 | (選用) 對差異進行變更。

在完成移轉並將您的變更推送到 Strata Cloud Manager 之前，您所做的任何變更都不會提交到您的設定。

1. 導覽至 Prisma Access 設定中的區域，您在其中找到差異並對設定進行變更。
對於上一個步驟中的範例，移轉程式對骨幹路由進行了變更（從 **no-asym-routing** 變更為 **asymmetry-routing-only**）。若要將此設定變更回您的原始設定，請前往 **Workflows** (工作流程) > **Prisma Access Setup** (Prisma Access 設定) > **Service Connections** (服務連線) > **Advanced Settings** (進階設定) **Configuration** (設定) > **NGFW and Prisma Access** (NGFW 和 Prisma Access) > **Configuration Scope** (設定範圍) > **Prisma Access** > **Service Connections** (服務連線) > **Advanced Settings** (進階設

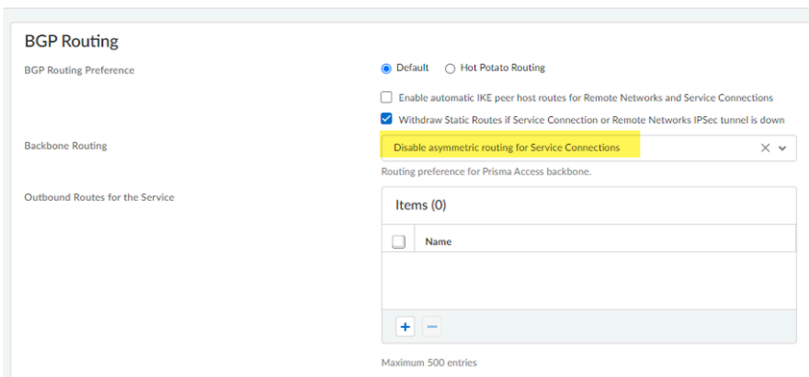
定），並將 **Backbone Routing**（骨幹路由）設定變更為 **Disable Asymmetric Routing for Service Connections**（停用服務連線的非對稱路由）。

Advanced Settings



2. （用選）若要追蹤您的變更，請在完成變更時 **Acknowledge**（確認）它們。雖然不是必要的，但在進行每個變更時確認這些變更可能很有用，以便您可以追蹤它們。

Advanced Settings



3. 繼續檢閱變更，然後進行變更並確認它們。

STEP 11 | (選用) 如果您已對設定進行任何變更，請**Regenerate Diffs** (重新產生差異) 以查看更新的差異。

The screenshot shows the 'Service Connections' tab in the Strata Cloud Manager. It displays a table with two items:

Object Name	Config Diff Type	Object Type	Acknowledge
Onboarding	Deleted	onboarding	<input type="checkbox"/>
Remote Networks	Deleted	remote-networks	<input type="checkbox"/>

Below the table, the configuration for 'Onboarding' is shown in a code editor:

```

1 - {
2 -   "entry": {
3 -     "@name": "VPN_Sivesa_Nogales",
4 -     "ecmp-load-balancing": "disabled",
5 -     "ipsec-tunnel": "VPN_Sivesa_Nogales",
6 -     "license-type": "FWAAS-5Mbps",
7 -     "protocol": {
8 -       "bgp": {
9 -         "enable": "yes",
10 -        "local-ip-address": "192.168.196.189",
11 -        "peer-as": "65010",
12 -        "peer-ip-address": "192.168.15.21"
13 -      }
14 -    },
15 -    "region": "mexico-central",
16 -    "secondary-man-enabled": "no",
17 -    "subnets": {
18 -      "member": "192.72.208.0/20"
19 -    }
20 -  }
21 - }
    
```

At the bottom, there are three buttons: 'Cancel Migration', 'Regenerate Diffs' (highlighted in yellow), and 'Complete Migration'.

STEP 12 | Complete Migration (完成移轉)。

雖然不需要這樣做，但您也可以 **Acknowledge** (確認) 您的變更。

Complete Migration (完成移轉) 後，您無法返回 **Panorama** 受管理部署，並且您的部署會永久將 **Strata Cloud Manager** 用於其管理。

4 - Final Confirmation

There are differences in the configurations. If everything is OK, click the Complete Migration button.

Cloud Service Plugin Policies and Objects

The screenshot shows the 'Service Connections' tab in the Strata Cloud Manager. It displays a table with three items:

Object Name	Config Diff Type	Object Type	Acknowledge
Internal Dns List	Deleted	internal-dns-list	<input checked="" type="checkbox"/>
Onboarding	Deleted	onboarding	<input checked="" type="checkbox"/>
Service Connection	Created	service-connection	<input checked="" type="checkbox"/>

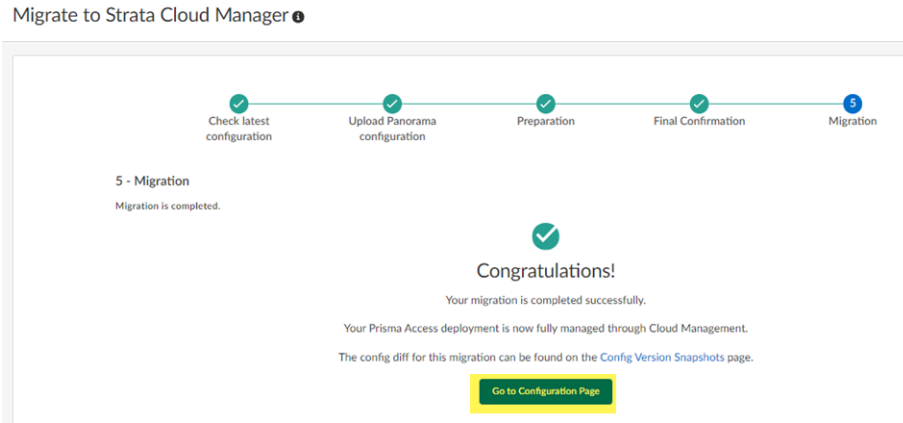
Below the table, the configuration for 'Service Connection' is shown in a code editor:

```

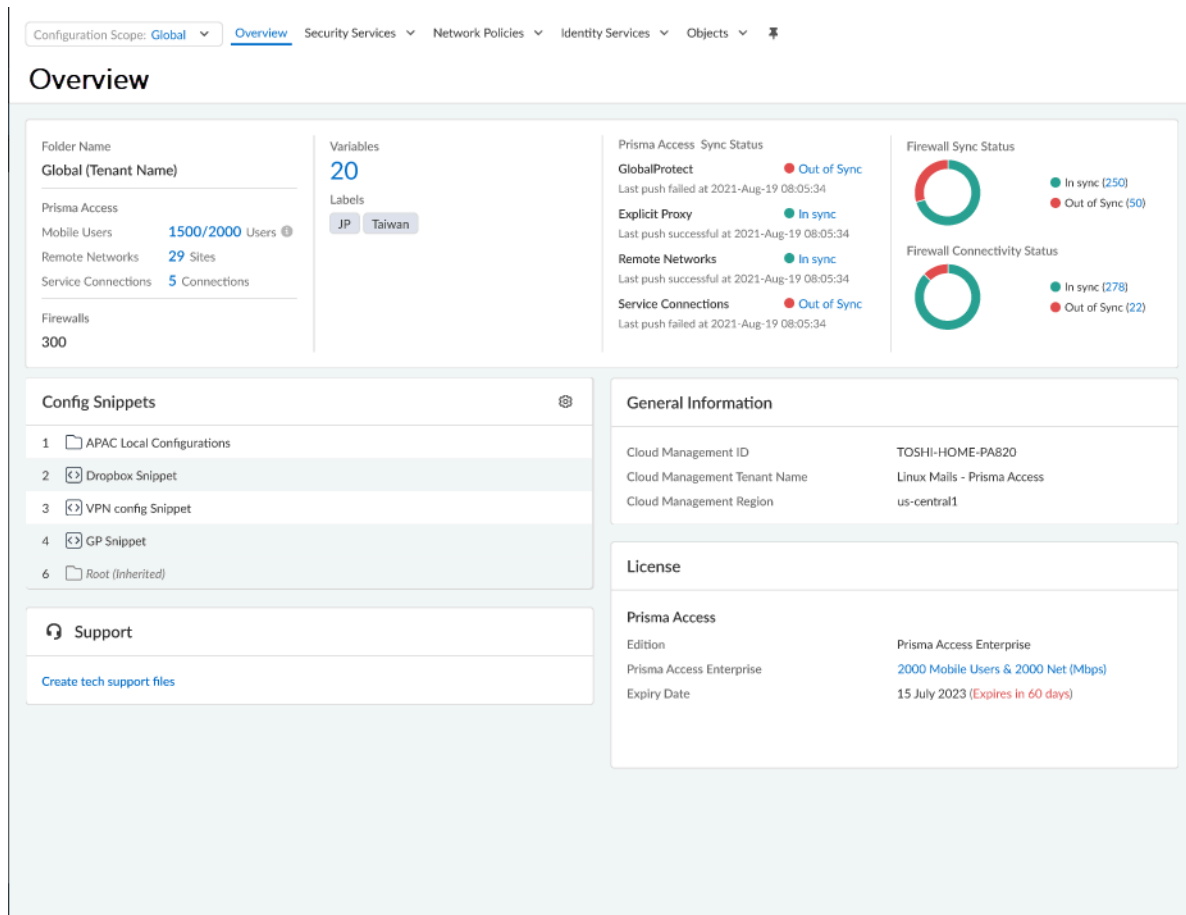
1 + {
2 +   "app-blocks-bgp-advertise": "no",
3 +   "connector-application-blocks": {
4 +     "member": "10.1.0.0/16"
5 +   }
6 + }
    
```

At the bottom, there are three buttons: 'Cancel Migration', 'Regenerate Diffs', and 'Complete Migration' (highlighted in yellow).

STEP 13 | (選用) Go to Configuration Page (前往設定頁面) 以查看您移轉的設定。

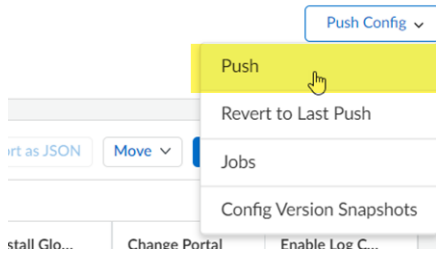


您移轉的部署即會顯示。



STEP 14 | Push Config（推送設定） > **Push**（推送）以套用您移轉的設定變更。

此推送操作可確保您的移轉已成功完成，並且 Prisma Access 已將所有變更套用到您移轉的設定。



STEP 15 | 注意您在推送操作期間收到的任何訊息，如果您看到任何問題，請視需要變更您的設定。

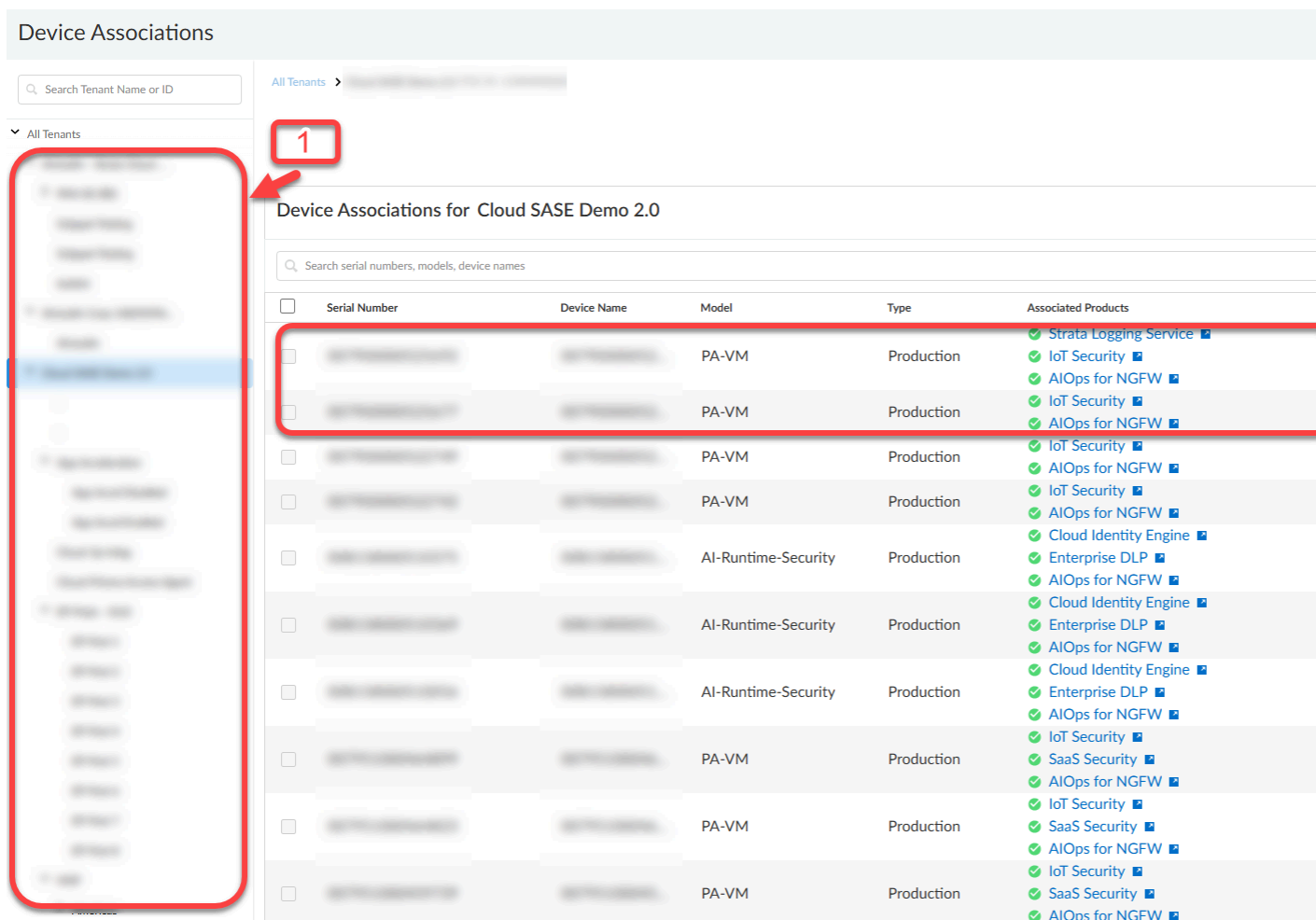
Strata Cloud Manager 中的裝置關聯

我可以在哪裡使用這個？	我需要哪些內容？
<ul style="list-style-type: none"> • NGFW，包括由軟體 NGFW 積分資助的項目 	<p>其中一個：</p> <ul style="list-style-type: none"> ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro <p>如果您在這些授權層級推出之前就開始使用 Strata Cloud Manager，那麼您的授權仍會受到支援。</p>

作為 Strata Cloud Manager 和公共服務的一部分，**Device Associations** 會提供您部署中所有裝置的集中管理檢視。您可透過此功能將裝置整理為[租用戶服務群組 \(TSG\)](#)（用於整理裝置的邏輯容器），並輕鬆地將支援的產品關聯至您的裝置。

您可以將 Device Associations 搭配以下產品使用：

- ❑ [Strata Cloud Manager](#)
- ❑ [AIOps for NGFW](#)
- ❑ [IoT Security](#)（企業授權協議）
- ❑ [Next-Generation CASB for Prisma Access and NGFW \(CASB-X\)](#)
- ❑ [SaaS Security Inline](#)
- ❑ [Strata Logging Service](#)



1. 在 **Device Associations**（裝置關聯）中（**Settings**（設定）> **Device Associations**（裝置關聯））中，您可以查看與您的客戶支援帳戶相關的所有**租用戶服務群組（TSG）**的清單。
 2. 選取一個 **TSG** 以查看與其相關的任何防火牆或 **Panorama** 設備。如果您沒有看到任何項目，可以從客戶支援帳戶 **Add Devices**（新增裝置）。
 3. 每當您需要將新裝置關聯至 **TSG** 時，請 **Add Devices**（新增裝置）。
 4. 在您新增防火牆或 **Panorama** 裝置後，您可以 **Associate Products**（關聯產品）以開始使用包含已啟動產品的裝置。應用程式必須與您裝置的硬體型號相容，否則在應用程式關聯期間，將不會顯示該裝置。
- [關聯裝置](#)
 - [關聯產品](#)
 - [移除關聯](#)

裝置關聯（將裝置關聯至租用戶）

若要開始使用包含您已啟動授權產品的防火牆或 Panorama 設備，您必須先將其關聯至包含已啟用 [相容產品](#) 的租用戶。

STEP 1 | 使用中樞或 Strata Cloud Manager 導覽至 **Device Associations**。

1. **（選用）** 使用您的 Palo Alto Networks CSP 憑證登入 [中樞](#)，然後選取 **Common Services**（常見服務）> **Device Associations**（裝置關聯）。
2. **（選用）** 登入 Strata Cloud Manager 並選取 **Settings**（設定）> **Device Associations**（裝置關聯）。

STEP 2 | 將防火牆或 Panorama 設備新增至您的租用戶。

1. 選取 **Add Device**（新增裝置）。
系統會根據您所在租用戶的已啟動產品自動選取 **Customer Support Account**（客戶支援帳戶）。如果您尚未啟動任何 [支援 Device Associations](#) 的產品，**Add Device**（新增裝置）將顯示為灰色。
2. 選取一或多個防火牆或 Panorama 設備。
您可以使用序號來搜尋特定裝置。
3. **Save**（儲存）。

STEP 3 | 繼續將產品關聯至裝置。

裝置關聯（將裝置關聯至產品）

在為支援的產品啟動授權後，您可以使用 **Device Associations**（裝置關聯）來指定您希望與該產品一起使用的防火牆或 Panorama 裝置。

STEP 1 | 啟動您的產品授權。

執行方法取決於您正在啟動的授權。請參閱特定產品說明文件以取得更多詳細資料。您還可以在此查看授權與 Strata Cloud Manager 的相容性。

STEP 2 | 使用中樞或 Strata Cloud Manager 導覽至 **Device Associations**。

1. **（選用）** 使用您的 Palo Alto Networks CSP 憑證登入中樞，然後選取 **Common Services**（常見服務） > **Device Associations**（裝置關聯）。
2. **（選用）** 登入 Strata Cloud Manager 並選取 **Settings**（設定） > **Device Associations**（裝置關聯）。

STEP 3 | 將產品關聯至防火牆或 Panorama 設備。

1. 選取 **Associate Products**（關聯產品）。
2. 在 [Products（產品）] 選取欄中，選取您想要關聯的產品。
3. 如適用，可選取授權類型。
某些產品的授權適用特定有效性條款和裝置型號。只有與您選取的授權類型相容的裝置才會顯示以供關聯。
4. 選取裝置。
5. **Save**（儲存）或 **Apply Licenses**（套用授權）。

STEP 4 | 驗證關聯是否成功。

如果關聯失敗，請複製錯誤 ID 並遵循 [步驟以開啟支援案例](#)。在開啟支援案例時，請務必包括錯誤 ID、裝置序號、TSG ID 和關聯失敗的產品名稱。

STEP 5 | 返回到您所關聯產品的說明文件，以取得進一步的裝載步驟。

裝置關聯（移除裝置關聯）

如果您要淘汰或歸還防火牆或 Panorama 裝置，或者想要將其關聯至另一個租用戶服務群組 (TSG)，可能需要移除裝置關聯。

如果您正在嘗試將試用授權轉換為生產，請轉換授權，而不是解除關聯。

STEP 1 | 使用中樞或 Strata Cloud Manager 導覽至 **Device Associations**。

1. **（選用）** 使用您的 Palo Alto Networks CSP 憑證登入中樞，然後選取 **Common Services**（常見服務） > **Device Associations**（裝置關聯）。
2. **（選用）** 登入 Strata Cloud Manager 並選取 **Settings**（設定） > **Device Associations**（裝置關聯）。

STEP 2 | 移除產品關聯。

如果您想要從 TSG 中移除防火牆或 Panorama 設備，您必須先移除任何關聯的產品。

1. 選取您想要解除關聯的防火牆或 Panorama 設備。
2. 選取 **Remove Associations**（移除關聯） > **Remove product association**（移除產品關聯）。
3. 選取您想要移除的產品，然後 **Remove Associations**（移除關聯）。

STEP 3 | 移除租用戶關聯。



您只能從沒有應用程式關聯的裝置中移除租用戶關聯。如果裝置已關聯至應用程式，請先移除應用程式關聯再繼續。

1. 選取您想要從租用戶中移除的防火牆或 Panorama 設備。
2. 選取 **Remove Associations**（移除關聯） > **Remove tenant association**（移除租用戶關聯）。
3. 確認您要繼續並 **Remove**（移除）。

STEP 4 | 如果您要移除防火牆或 Panorama 設備以將其新增到新的 TSG，將其關聯至新的 TSG。

裝置型號相容性

您可以關聯至不同應用程式的裝置型號如下。

- [AIOps for NGFW或Strata Cloud Manager](#)
- [CASB-X](#)
- [IoT Security](#)
- [SaaS Security](#)

AIOps for NGFW或Strata Cloud Manager

系列	型號
Panorama 虛擬設備	<ul style="list-style-type: none"> • PRA-25 • PRA-100 • PRA-1000
VM-Series	<ul style="list-style-type: none"> • VM-200 • VM-300 • VM-500 • VM-600 • VM-700
200	<ul style="list-style-type: none"> • 220
400	<ul style="list-style-type: none"> • 410 • 410R • 440 • 445 • 450 • 450R • 460
800	<ul style="list-style-type: none"> • 820 • 850
3000	<ul style="list-style-type: none"> • 3220 • 3250 • 3260 • 3410

系列	型號
	<ul style="list-style-type: none"> • 3420 • 3430 • 3440
5000	<ul style="list-style-type: none"> • 5220 • 5250 • 5260 • 5280 • 5410 • 5420 • 5430 • 5445 • 5450
7000	<ul style="list-style-type: none"> • 7050 • 7080

CASB-X

系列	型號
200	<ul style="list-style-type: none"> • 220
400	<ul style="list-style-type: none"> • 400 • 410 • 415 • 440 • 445 • 450 • 450R • 460
800	<ul style="list-style-type: none"> • 820 • 850
1000	<ul style="list-style-type: none"> • 1410 • 1420

系列	型號
3000	<ul style="list-style-type: none"> • 3200 • 3220 • 3250 • 3260 • 3410 • 3420 • 3430 • 3440
5000	<ul style="list-style-type: none"> • 5220 • 5250 • 5260 • 5280 • 5400 • 5420 • 5430 • 5440 • 5445 • 5450
7000	<ul style="list-style-type: none"> • 7050 • 7080

IoT Security

此表格僅包含您可在 **Device Associations** 中關聯至 **IoT Security** 的裝置型號。此表格不包含有關 **IoT Security** 功能適用的不同裝置型號和 **PAN-OS** 版本組合資訊。

系列	型號
VM-Series	<ul style="list-style-type: none"> • VM-100 • VM-300 • VM-500 • VM-700
200	<ul style="list-style-type: none"> • 200 • 220

系列	型號
	<ul style="list-style-type: none"> • 220R
400	<ul style="list-style-type: none"> • 410 • 410R • 440 • 450 • 450R • 460
500	<ul style="list-style-type: none"> • 500
800	<ul style="list-style-type: none"> • 820 • 850
3000	<ul style="list-style-type: none"> • 3020 • 3050 • 3060 • 3220 • 3250 • 3260 • 3410 • 3420 • 3430 • 3440
7000	<ul style="list-style-type: none"> • 7050 • 7080

SaaS Security

此表格僅包含您可在 **Device Associations** 中關聯至 **SaaS Security** 的裝置型號。此表格不包含有關 **SaaS Security** 功能適用的不同裝置型號和 **PAN-OS** 版本組合資訊。

系列	型號
200	<ul style="list-style-type: none"> • 220 • 220R
400	<ul style="list-style-type: none"> • 410

系列	型號
	<ul style="list-style-type: none">• 410R• 440• 440R• 450• 450R• 460• 460R
800	<ul style="list-style-type: none">• 820• 850
3000	<ul style="list-style-type: none">• 3220• 3250• 3260• 3410• 3420• 3430• 3440
5000	<ul style="list-style-type: none">• 5220• 5250• 5260• 5280• 5410• 5420• 5430• 5450
7000	<ul style="list-style-type: none">• 7050• 7080

防火牆和授權類型相容性

某些產品訂閱具有不同的授權類型，使其僅相容於特定類型的防火牆和設備。當您將產品關聯至裝置，並選取您的產品授權時，系統只會顯示與授權類型相對應的裝置。然而，某些授權類型，例如評估、試用和企業授權協議（ELA）與所有防火牆型號都相容。

防火牆類型是由防火牆 SKU 定義。若要查看防火牆的 SKU，請登入您的客戶支援入口網站帳戶，然後選取 **Assets**（資產） > **Devices**（裝置），並檢查 [Model Name（模型名稱）] 欄中防火牆的序號項目。這便是 SKU，以下列格式表示防火牆類型：

- 產品 SKU 的結尾是防火牆型號名稱，例如 PAN-PA-410
- 評估 SKU 結尾為 -E60，代表評估 + 60 天，例如，PAN-PA-410-E60
- 實驗室 SKU 的結尾為 -LAB，例如，PAN-PA-410-LAB

您應用程式支援的防火牆和授權類型組合請參閱下方。

- [#unique_38](#)
- [AIOps for NGFW](#)
- [IoT Security](#)
- [SaaS Security Inline](#)

AIOps for NGFW

AIOps for NGFW 授權類型	防火牆類型			
	NFR	LAB	PROD	Eval
TRIAL	否	是	是	是
Eval	否	是	是	是
NFR	是	否。	否。	否
LAB	否	是	否。	否
PROD	否	否。	是	否

IoT Security

IoT Security 授權 類型	防火牆類型			
	NFR	LAB	PROD	Eval
TRIAL	否	是	是	是
Eval	否	是	是	是

IoT Security 授權 類型	防火牆類型			
	NFR	LAB	PROD	EVAL
NFR	是	否。	否。	否
LAB	否	是	否。	否
PROD	否	否。	是	否

SaaS Security Inline

SaaS Security Inline 授權類型	防火牆類型			
	NFR	LAB	PROD	EVAL
TRIAL	否	是	是	是
EVAL	否	是	是	是
NFR	是	否。	否。	否
LAB	否	是	否。	否
PROD	否	否。	是	否