paloalto TECHDOCS

PAN-OS 升級指南

Version 11.1 & later

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

May 22, 2024

Table of Contents

軟體和內容更新

PAN-OS 是執行所有 Palo Alto Networks 下一代防火牆的軟體。Palo Alto Networks 還經常發佈更新，為防火牆配備最新的安全性功能。防火牆可以根據內容更新提供的應用程式和威脅特徵碼等執行原則，無需更新防火牆組態。

在實體防火牆上成功下載並安裝 PAN-OS 軟體更新後，作為軟體安裝程序的一部分，實體防火牆重新啟動後，將對軟體更新進行驗證，以確保 PAN-OS 軟體的完整性。這樣可以確保新執行的軟體更新已知良好，且防火牆不會由於遠端或實體漏洞而受到危害。

PAN-OS 軟體更新

PAN-OS 是執行所有 Palo Alto Networks 下一代防火牆的軟體。防火牆執行的 PAN-OS 軟體版本顯示在防火牆的 **Dashboard**（儀表板）上。

您可直接在防火牆中查看新的 PAN-OS 版本，也可在 Palo Alto Networks 支援入口網站上查看。若要將防火牆升級至最新版本的 PAN-OS：

STEP 1 | 檢閱最新的 PAN-OS 版本資訊以瞭解最新內容。同時查看 升級/降級考量事項，以確保瞭解 PAN-OS 版本可能引入的所有潛在變更。

STEP 2 | 查看新的 PAN-OS 版本：

- **On the support portal**（在支援入口網站上）—移至 support.paloaltonetworks.com，在左側功能表列上，選取 **Updates**（更新） > **Software Updates**（軟體更新）。下載並儲存要用於升級防火牆的版本。
- **On the firewall**（在防火牆上）—選取 **Device**（裝置） > **Software**（軟體） 並 **Check Now**（立即檢查） 防火牆，以查看 Palo Alto Networks 更新伺服器提供的全新 PAN-OS 發行版本。

檢查軟體更新有困難嗎？請參閱本文，瞭解一些常見連線問題的解決方案。

STEP 3 | 在您決定了想要的發行版本之後，按照完整的工作流程來 將防火牆升級到 PAN-OS 11.1。您將採取的步驟可能取決於目前執行的發行版本、是否使用 HA 及是否使用 Panorama 管理防火牆。

動態內容更新

Palo Alto Networks 經常發佈更新，以便防火牆用於執行安全性原則，無需升級 PAN-OS 軟體或變更防火牆組態。這些更新為防火牆配備了最新的安全性功能和威脅情報。

除了應用程式更新和一些防毒軟體更新以外（任何防火牆都可以接收這些更新），可用的動態內容更新可能取決於您的訂閱。您可以為每個動態內容更新設定時間表，以定義防火牆檢查和下載或安裝新更新的頻率（**Device**（裝置） > **Dynamic Updates**（動態更新））。

動態內容更新	此套件包含哪些內容？
防毒軟體	防毒軟體更新每 24 小時發佈一次，包括： • 新發現的惡意軟體的 WildFire 特徵碼。若要每五分鐘（而不是每天）更新一次，您需要進行 WildFire 訂閱。 • （需要威脅防護）自動產生命令和控制 (C2) 特徵碼，用於偵測 C2 流量中的特定模式。這些特徵碼讓防火牆即使在 C2 主機未知或快速變化的情況下，仍可偵測 C2 活動。 • （需要威脅防護）內建外部動態清單的全新和更新清單項目。這些清單包括惡意、高風險和防彈主機提供的 IP 位址，幫助您免受惡意主機攻擊。 • （需要威脅防護）更新至本機 DNS 特徵碼集，以供防火牆用於識別已知惡意網域。如果您設定了 DNS Sinkholing，則防火牆可以識別網路上嘗試連線至這些網域的主機。若要允許防火牆根據完整的 DNS 特徵碼資料庫檢查網域，請設定 DNS 安全性。
應用程式	應用程式更新提供新的以及已修改的應用程式特徵碼，或 App-ID。此更新不需要其他訂閱，但需要有效的維護/支援合約。新的應用程式更新僅於每月第三個週二發佈，以便您有時間提前準備任何必要的原則更新。 在極少數情況下，包含新 *App-ID* 的更新發佈可能會延遲一天或兩天。 App-ID 修改的發佈頻率更高。雖然新的以及已修改的 App-ID 可讓防火牆日益精準地執行安全性原則，但是安全性原則執行導致的變更會影響應用程式可用性。若要充分利用應用程式更新，請遵循我們的管理新的以及已修改的 App-ID 提示。
應用程式與威脅	包括全新及更新的應用程式與威脅特徵碼。如果您已具有威脅防護使用授權（在本例中，您將進行此更新取代應用程式更新），即可進行此更新。新的威脅更新經常發佈，有時一週會發佈幾次，同時還會發佈更新後的 App-ID。新的 App-ID 僅在每月的第三個週二發佈。 在極少數情況下，包含新 *App-ID* 的更新發佈可能會延遲一天或兩天。

動態內容更新	此套件包含哪些內容？
	在最新威脅和應用程式更新變得可用後的短短 30 分鐘內，防火牆即可進行擷取。 有關如何最佳地啟用應用程式和威脅更新，以確保應用程式可用性和最新威脅防護的指導，請查看 應用程式與威脅內容更新的最佳做法。
裝置字典	裝置字典是一個 XML 檔案，供防火牆在基於 Device-ID 的安全性政策規則中使用。其包含各種裝置屬性的項目，會定期完全重新整理並作為新檔案發佈在更新伺服器上。如果字典項目發生任何變更，修訂後的檔案將發佈在更新伺服器上，以便 Panorama 和防火牆在下次檢查更新伺服器時自動下載並安裝，其每兩小時自動下載和安裝一次。
GlobalProtect 資料檔案	包含可用於定義及評估由 GlobalProtect 應用程式傳回之主機資訊設定檔 (HIP) 的廠商特定資料。您必須擁有 GlobalProtect 閘道訂閱才能接收這些更新。此外，您還必須建立這些更新的排程，然後 GlobalProtect 才會正常運作。
GlobalProtect 無用戶端 **VPN**	包含新的和更新的應用程式特徵碼，以支援從 GlobalProtect 入口網站進行通用網頁應用程式的無用戶端 VPN 存取。您必須擁有 GlobalProtect 訂閱才能接收這些更新。此外，您還必須建立這些更新的排程，然後 GlobalProtect 無用戶端 VPN 才會正常運作。建議的最佳做法是，始終為 GlobalProtect 無用戶端 VPN 安裝最新內容更新。
WildFire	即時提供對 WildFire 公共雲端產生的惡意軟體和防毒特徵碼的存取。或者，您還可以選擇設定 PAN OS 來擷取 WildFire 特徵碼更新套件。您可以將防火牆設定為每分鐘一次的頻率檢查新的更新，以確保防火牆可在可取得後的一分鐘內擷取最新的 WildFire 特徵碼。如果沒有 WildFire 訂閱，您必須等待至少 24 小時，特徵碼才會在防毒軟體更新中提供。
WF-私人	提供幾近即時的惡意軟體和防毒特徵碼，這些特徵碼由 WildFire 設備完成的分析所建立。若要從 WildFire 設備接收內容更新，防火牆與設備必須均執行 PAN-OS 6.1 或更新版本，且防火牆必須設定為轉送檔案與電子郵件連結至 WildFire 私人雲端。

安裝內容更新

若要確保您始終可獲得保護而免於最新的威脅（包括尚未發現的威脅），您必須使用 Palo Alto Networks 發佈的最新內容與軟體更新，確保防火牆維持在最新狀態。可用 動態內容更新 取決於您擁有的訂閱。

按照下列步驟安裝內容更新。您也可以設定內容更新排程，定義防火牆擷取並安裝更新的頻率。

應用程式和威脅內容更新的執行方式與其他更新類型略有不同—若要充分利用最新的應用程式知識和威脅防護，請遵循部署應用程式與威脅內容更新指引，而不是以下步驟。

STEP 1 | 確保防火牆可存取更新伺服器。

1. 依預設，防火牆在 **updates.paloaltonetworks.com** 存取 **Update Server**（更新伺服器），以便防火牆從最靠近的伺服器接收內容更新。如果您的防火牆具有有限的網際網路存取，則可能需要設定允許清單，以啟用存取涉及更新下載的伺服器。有關內容更新伺服器的更多資訊，請參閱適用於動態更新的內容傳遞網路基礎結構。如果您需要其他參考資訊，或是遇到了連線與更新下載問題，請參閱 https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000001UtRCAU。

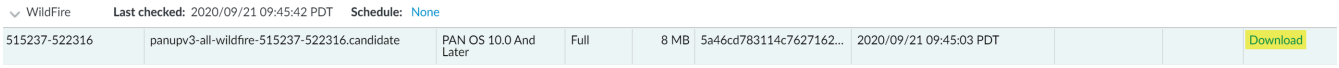
   如果您的裝置位於中國大陸，*Palo Alto Networks* 建議使用 ***updates.paloaltonetworks.cn*** 伺服器來下載更新。

2. （選用）按一下 **Verify Update Server Identity**（驗證更新伺服器身分識別），進行額外層級的驗證，使防火牆檢查由受信任授權單位簽署的伺服器 SSL 憑證。預設會啟用此功能。
3. （選用）如果防火牆需要使用代理程式伺服器才能取得 Palo Alto Networks 更新服務，則在 **Proxy Server**（**Proxy** 伺服器）視窗中輸入：
   - 伺服器—代理程式伺服器的 IP 位址或主機名稱。
   - 連接埠—代理程式伺服器的連接埠。範圍：1-65535。
   - 使用者—用來存取伺服器的使用者名稱。
   - 密碼—使用者用來存取代理程式伺服器的密碼。在 **Confirm Password**（確認密碼）中重新輸入密碼。
4. （選用）設定當發生連線失敗時最多可進行三次重新連線嘗試。使用 **debug set-content-download-retry attempts** 設定連線嘗試次數。預設值為 0。

STEP 2 | 檢查是否有最新的內容更新。

選取 **Device**（裝置） > **Dynamic Updates**（動態更新），然後按一下 **Check Now**（立即檢查）（位於視窗的左下角）以檢查最新更新。**Action**（動作）欄中的連結表示更新是否可用：

- 下載 — 表示可使用新的更新檔案。按一下連結以開始將檔案直接下載到防火牆。成功下載後，**Action**（動作）欄中的連結會從 **Download**（下載）變更為 **Install**（安裝）。



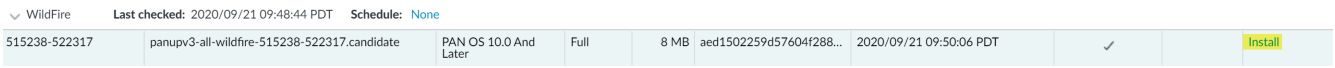
在安裝應用程式與威脅更新前，您無法下載防毒更新。

- 還原—表示有先前安裝的內容版本或軟體版本可用。您可以選擇還原為之前安裝的版本。

STEP 3 | 安裝內容更新。

在 *PA-220* 防火牆上執行安裝最多需要 *10* 分鐘，而在 *PA-5200* 系列、*PA-7000* 系列或 *VM* 系列防火牆上最多僅需要 *2* 分鐘。

按一下 **Action**（動作）欄中的 **Install**（安裝）連結。完成安裝後，**Currently Installed**（目前已安裝）欄會顯示核取標記。



STEP 4 | 排程每個內容更新。

針對每個要排程的更新重複此步驟。

錯開更新排程，因為防火牆一次只能下載一個更新。如果您在相同的時間間隔期間排程下載更新，則只有第一次下載會成功。

1. 按一下 **None**（無）連結以設定每個更新類型的排程。

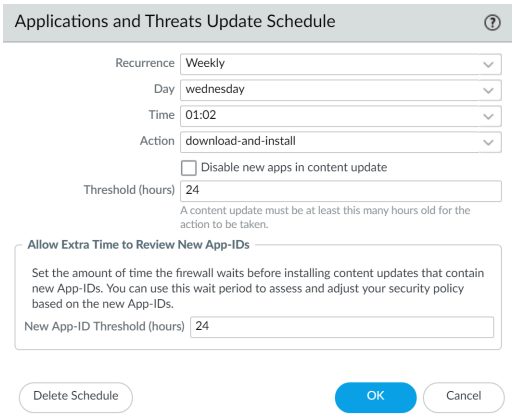
2. 從 **Recurrence**（週期性）下拉式清單選取值，以指定更新的頻率。可用值因內容類型而有所不同（WildFire 更新可排程為 **Real-time**（即時）、**Every Minute**（每分鐘）、**Every 15 Minutes**（每 **15** 分鐘）、**Every 30 minutes**（每 **30** 分鐘）或 **Every Hour**（每小時），而應用程式與威脅更新可排程為 **Weekly**（每週）、**Daily**（每

日）、**Hourly**（每小時）或 **Every 30 Minutes**（每 **30** 分鐘），防毒軟體更新可排程為 **Hourly**（每小時）、**Daily**（每日）或 **Weekly**（每週））。

您還可以為應用程式和威脅或防毒更新選取 **None (Manual)**（無（手動））。這意味著此項目沒有週期性排程，您必須手動安裝更新。若要完全移除排程節點，請選取 **Delete Schedule**（刪除排程）。

3. 指定 **Time**（時間）（或在 WildFire 中為小時之後的分鐘數），並視您選取的 **Recurrence**（週期性）值而定，指定要在每星期幾進行更新（如果適用）。
4. 指定您要系統 **Download Only**（僅下載）更新，或依照最佳做法 **Download And Install**（下載並安裝）更新。
5. 您可透過指定 **Threshold (Hours)**（臨界值（小時）），設定在發行後執行內容更新前的等待時間。在極少數的情況下，可能會在內容更新中找到錯誤。基於此原因，您可能會想要在發行特定小時數前，延遲安裝新的更新。

   如果您有必須 *100%* 可用的任務關鍵性應用程式，則將應用程式或應用程式與威脅更新的臨界值設定為至少 *24* 小時，並遵循應用程式與威脅內容更新的最佳做法。此外，雖然排程內容更新為一次性工作或不常發生的工作，但是在您設定排程後，需繼續管理新的以及已修改的 App-ID（包含在內容發行版本中），因為這些 *App-ID* 會變更安全性原則的執行方式。
6. （選用）輸入 **New App-ID Thresholds**（新 **App-ID** 臨界值）（以小時為單位）以設定防火牆在安裝包含新 App-ID 的內容更新前等待的時間長度。



7. 按一下 **OK**（確定）來儲存排程設定。
8. 按一下 **Commit**（提交），將設定儲存至執行中的組態。

STEP 5 | 更新 PAN-OS。

務必先更新內容再更新 *PAN-OS*。每一個 *PAN-OS* 版本都擁有支援的最低內容發行版本。

1. 檢閱版本資訊。
2. 更新 PAN-OS 軟體。

應用程式與威脅內容更新

應用程式與威脅內容更新向防火牆傳送最新的應用程式與威脅特徵碼。封包的應用程式部分包含新的和已修改的 App-ID，無需授權。完整的應用程式與威脅內容封包同樣包含新的以及已修改的威脅特徵碼，需要威脅防禦授權。由於防火牆可自動擷取與安裝最新的應用程式與威脅特徵碼（根據您的自訂設定），它可依據最新的 App-ID 與威脅防禦開始執行安全性原則，而無需任何額外的設定。

新的和已修改的威脅特徵碼，以及已修改的 App-ID，至少每週發行一次，發行頻率通常更高。新的 App-ID 會在每月第三個週二發佈。

在極少數情況下，包含新 *App-ID* 的更新發行可能會延遲一天或兩天。

由於新的 App-ID 可變更安全性原則對流量執行動作的方式，因此對新的 App-ID 實施更加有限的發行方式，旨在為您提供可預測的時間，以便讓您制訂以及更新安全性原則。此外，內容更新會累計；這意味著最新的內容更新始終包含先前版本中發行的應用程式與威脅特徵碼。

由於應用程式與威脅特徵碼以單一封包傳送—採用相同的解碼器，使應用程式特徵碼識別應用程式，同時使威脅特徵碼檢查流量—您需考慮同時還是分開部署特徵碼。您選擇透過何種方式部署內容更新，取決於組織的網路安全性與應用程式可用性要求。作為起點，將您的組織識別為擁有以下某種狀態（或者可能同時擁有兩種狀態，取決於防火牆位置）：

- 以安全性優先的組織會將使用最新威脅特徵碼的保護機制的優先順序排在應用程式可用性之上。您主要利用防火牆來實現威脅防禦功能。可影響安全性原則對應用程式流量執行何種動作的 App-ID 變更，居次要地位。
- 任務關鍵性網路會將應用程式可用性的優先順序排在使用最新特徵碼的保護機制之上。您的網路將對停機零容忍。以內嵌方式部署防火牆，以執行安全性原則，如果您在安全性原則中使用了 App-ID，任何會影響 App-ID 的內容發行版本變更都可能造成停機。

您可以採用任務關鍵性或安全性優先方式部署內容更新，也可以將這兩種方式結合起來，以滿足業務的需求。檢閱並考慮應用程式與威脅內容更新的最佳做法以確定如何實作應用程式與威脅更新。然後：

- 部署應用程式與威脅內容更新。
- 按照我們的內容更新提示。

雖然排程內容更新為一次性工作或不常發生的工作，但是在您設定排程後，需繼續管理新的以及已修改的 App-ID（包含在內容發行版本中），因為這些 *App-ID* 會變更安全性原則的執行方式。

部署應用程式與威脅內容更新

在採取步驟以設定應用程式與威脅內容更新前，請先瞭解 應用程式與威脅內容更新 的工作原理，並確定您要如何實作 應用程式與威脅內容更新的最佳做法。

此外，透過 Panorama，您可輕鬆、快速向防火牆部署內容更新。如果您使用 Panorama 管理防火牆，請遵循這些步驟來部署內容更新，而非採用以下步驟。

STEP 1 | 若要解鎖完整的應用程式與威脅內容封包，請獲取威脅防禦授權並在防火牆上啟動授權。

1. 選取 **Device**（裝置） > **Licenses**（授權）。
2. 手動上傳授權金鑰，或從 Palo Alto Networks 授權伺服器中擷取授權金鑰。
3. 驗證威脅防禦授權是否在使用中。

STEP 2 | 為防火牆設定排程，以擷取並安裝內容更新。

完成以下步驟後，務必要考慮貴組織是任務關鍵性組織還是安全性優先組織（或者同時結合這兩者），以及您已檢閱應用程式與威脅內容更新的最佳做法。

1. 請選取 **Device**（裝置） > **Dynamic Updates**（動態更新）。（裝置 > 動態更新）.
2. 為應用程式與威脅內容更新選取 **Schedule**（排程）。
3. 設定防火牆與 Palo Alto Networks 更新伺服器核實新應用程式與威脅內容發行版本的頻率（**Recurrence**（週期性）），以及具體 **Day**（日期）與 **Time**（時間）。
4. 設定防火牆發現並擷取新內容發行版本時其要採取的 **Action**（動作）。
5. 為內容發行版本設定安裝 **Threshold**（臨界值）。Palo Alto Networks 更新伺服器必須至少在這一時間點提供內容發行版本，防火牆才能擷取發行版本並執行在上一步中設定的 Action（動作）。
6. 如果您的網路為對應用程式停機零容忍的任務關鍵性網路（應用程式可用性甚至與最新的威脅防禦同等重要），您可設定 **New App-ID Threshold**（新 **App-ID** 臨界值）。只有在包含新 App-ID 的內容更新在此時間可用後，防火牆才會進行擷取。
7. 按一下 **OK**（確定）以儲存應用程式與威脅內容更新排程，並 **Commit**（提交）。

STEP 3 | 組態日誌轉送，以將 Palo Alto Networks 關鍵內容警示傳送至您用於監控網路以及防火牆活動的外部服務。透過這一點，您可確保向對應人員告知關鍵內容事宜，以便他們可按需採取動作。關鍵內容警示作為系統日誌項目予以記錄，包含以下類型與事件：(subtype eq dynamic-updates) 和 (eventid eq palo-alto-networks-message)。

STEP 4 | 雖然排程內容更新為一次性工作或不常發生的工作，但是在您設定排程後，需繼續管理新的以及已修改的 App-ID（包含在內容發行版本中），因為這些 App-ID 會變更安全性原則的執行方式。

內容更新提示

Palo Alto Networks 應用程式與威脅內容發行版本會採取嚴苛的效能與品質保證機制。但是，由於客戶環境中可能出現的變數如此之多，在極其偶然的情況下，內容發行版本可能會對網路造成意外影響。遵循這些提示可緩解或疑難排解與內容版本有關的問題，以便最大程度地降低對網路造成的影響。

- 遵循應用程式和威脅內容更新的最佳做法。

  檢閱並實作應用程式與威脅內容更新的最佳做法。您選擇透過何種方式部署內容更新，取決於網路安全性與應用程式可用性要求。

- 確保執行最新內容。

  若您未設定防火牆自動下載並安裝內容更新，請獲取最新內容更新。

  防火牆會在安裝時驗證下載的內容更新仍然為 Palo Alto Networks 所建議的內容。依預設，防火牆會執行此檢查，對於在安裝前從 Palo Alto Networks 更新伺服器（手動或依排程）下

載內容更新的情況而言，此檢查非常有用。由於在極少數的情況下，Palo Alto Networks 會移除內容更新的可用性，此選項會阻止防火牆安裝 Palo Alto Networks 已移除的內容更新，即使防火牆已下載此內容更新。如果您看到錯誤訊息，表明正在嘗試安裝的內容更新不再有效，請 **Check Now**（立即檢查）以獲取最新內容更新並安裝此版本（**Device**（裝置）> **Dynamic Updates**（動態更新））。

- 開啟威脅情報遙測。

  開啟防火牆向 Palo Alto Networks 傳送的威脅情報遙測。我們使用遙測資料來識別並疑難排解與內容更新相關的問題。

  遙測資料可在整個 Palo Alto Networks 客戶群中，幫助我們快速識別會對防火牆效能或者安全性原則執行造成意外影響的內容更新。我們識別問題的速度越快，就越能夠快速幫助您完全避免問題或緩解對您網路造成的影響。

  若要啟用防火牆收集並與 Palo Alto Networks 共用遙測資料：

  1. 選取 **Device**（裝置）> **Setup**（設定）> **Telemetry**（遙測）。
  2. 編輯 **Telemetry**（遙測）設定並 **Select All**（全選）。
  3. 按一下 **OK**（確定）和 **Commit**（提交），以儲存變更。

- 將 **Palo Alto Networks** 內容更新警示轉送給合適人員。

  為 Palo Alto Networks 關鍵內容警示啟用日誌轉送，以便關於內容發行版本問題的重要訊息會直接傳送至對應的人員。

  如今，Palo Alto Networks 可將內容更新問題相關警示直接簽發至防火牆網頁介面（若已啟用日誌轉送），或者簽發至您用於監控的外部服務。關鍵內容警示會詳細描述問題，以便您可瞭解它會造成的影響，同時還包含按需採取的動作。

  在防火牆網頁介面中，有關內容問題的關鍵警示的顯示方式類似於當日訊息。Palo Alto Networks 簽發有關內容更新的關鍵警示後，依預設，在您登入防火牆網頁介面時，會顯示此警示。如果您已登入防火牆網頁介面，功能表列（位於網頁介面底部）的訊息圖示上方將會顯示驚嘆號，按一下訊息圖示以檢視警示。

  此外，關鍵內容更新警示還作為系統日誌項目予以記錄，類型為 **dynamic-updates**，事件為 **palo-alto-networks-message**。使用以下篩選器檢視這些日誌項目：(subtype eq dynamic-updates) 與 (eventid eq palo-alto-networks-message)。

- 如有需要，請使用 **Panorama** 回復到較舊的內容版本。

  收到有關內容更新問題的通知後，可使用 Panorama 快速將受管理防火牆還原至上一個內容更新版本，而非為各個防火牆手動還原內容版本：從 Panorama 復原內容更新。

應用程式與威脅內容更新的最佳做法

部署內容更新的最佳做法有助於確保順暢執行原則，因為防火牆會不斷引入新的以及已修改的應用程式和威脅特徵碼。雖然透過一個內容更新套件同時傳遞應用程式和威脅特徵碼（詳細閱讀 應用程式與威脅內容更新），但是您可根據網路安全性與可用性要求以不同方式靈活地進行部署：

- 以安全性優先的組織會將使用最新威脅特徵碼的保護機制的優先順序排在應用程式可用性之上。您主要利用防火牆來實現威脅防禦功能。
- 任務關鍵性網路會將應用程式可用性的優先順序排在使用最新特徵碼的保護機制之上。您的網路將對停機零容忍。以內嵌方式部署防火牆，以執行安全性原則，如果您在安全性原則中使用了 App-ID，任何會影響 App-ID 的內容變更都可能造成停機。

您可以採用任務關鍵性或安全性優先方式部署內容更新，也可以將這兩種方式結合起來，以滿足業務的需求。套用以下最佳做法時考慮採用的方式，以最為有效地利用新的以及已修改的威脅與應用程式特徵碼：

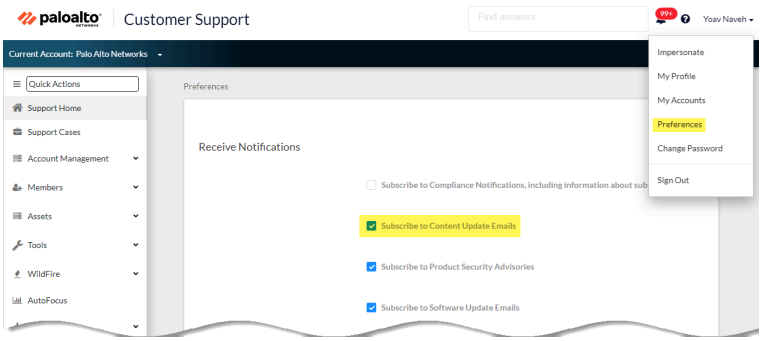
- 任務關鍵性內容更新的最佳做法
- 安全性優先之內容更新的最佳做法

任務關鍵性內容更新的最佳做法

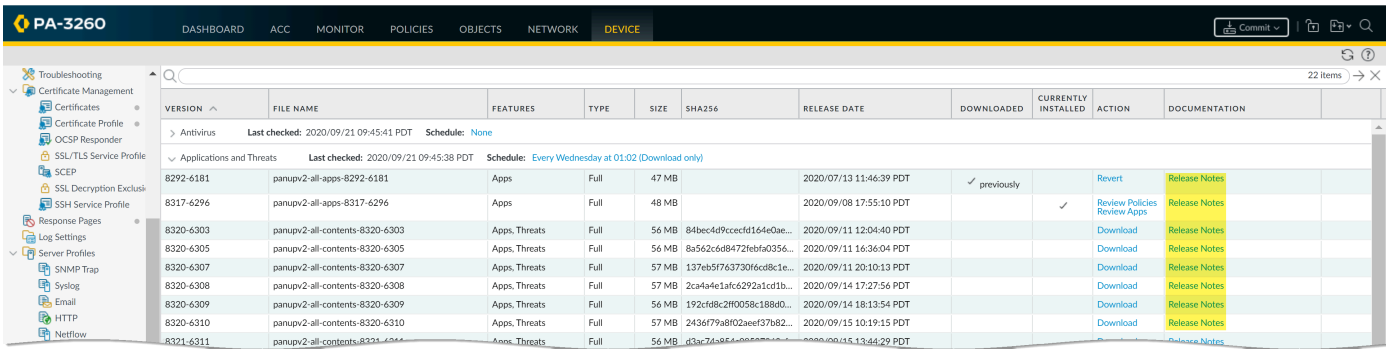
應用程式與威脅內容更新的最佳做法，有助於確保在發行新的應用程式和威脅特徵碼時實現無縫政策執行。遵循這些最佳做法，在對應用程式停機零容忍的任務關鍵性網路中部署內容更新。

- 務必檢閱內容版本資訊，查看內容版本中引入的新識別和修改的應用程式和威脅特徵碼清單。內容版本資訊中還會介紹更新對現有安全性原則的執行有哪些影響，並提供關於如何修改安全性原則以最大程度地利用新內容的建議。

  若要訂閱最新內容更新的通知，請瀏覽客戶支援入口網站，編輯您的 **Preferences**（喜好設定），然後選取 **Subscribe to Content Update Emails**（訂閱內容更新電子郵件）。



  您還可以在 Palo Alto Networks 支援入口網站上檢閱應用程式和威脅的內容版本說明，或直接在防火牆網頁介面上檢閱：選取 **Device**（裝置） > **Dynamic Updates**（動態更新），然後開啟特定內容發行版本的 **Release Note**（版本說明）。

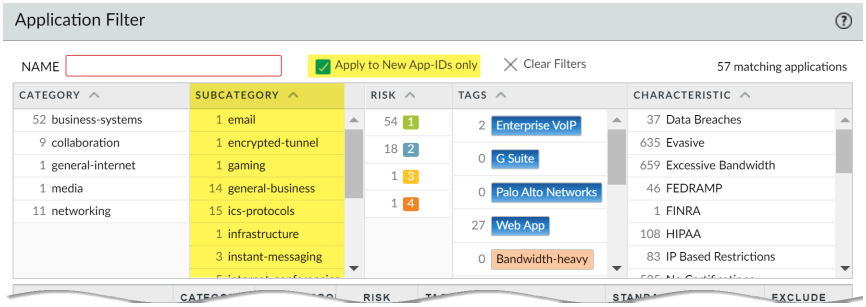


  內容版本說明的說明區段中強調顯示了 *Palo Alto Networks* 已確定可能嚴重影響涵蓋範圍的未來更新：例如新 *App-ID* 或解碼器。檢查這些未來更新，以便在更新發佈之前估計對原則的影響。

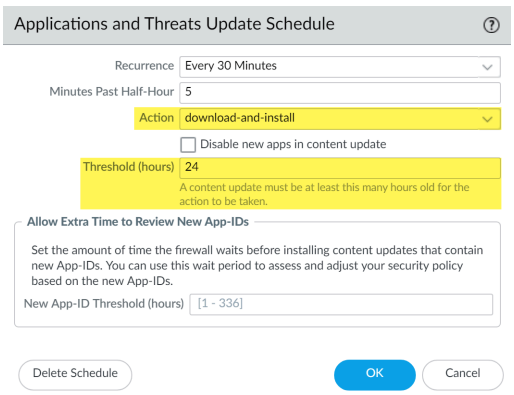
- 建立安全性原則規則，以始終允許特定類別的新 App-ID，例如關鍵業務功能所依賴的驗證或軟體開發應用程式。這意味著若內容版本引入或變更重要業務應用程式的範圍，防火牆會繼續無縫允許應用程式，而不會要求您更新安全性原則。透過這一點，可消除可能會對關鍵類別 App-

ID 可用性產生的影響，並可為您預留三十天時間（新 App-ID 每月發行一次）來調整您的安全性原則，以允許任務關鍵性 App-ID。

為此，請建立用於關鍵類別新 App-ID 的應用程式篩選器（**Objects**（物件） > **Application Filters**（應用程式篩選器）），並將應用程式篩選器新增至安全性原則規則。



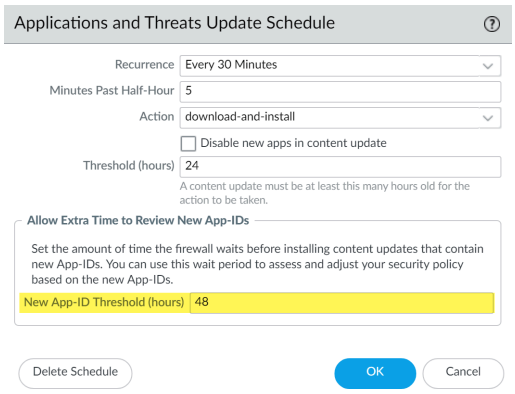
- 為降低對與啟用新應用程式和威脅特徵碼相關之安全性原則執行所產生的影響，請交錯部署新內容。在為商業風險較高的站點（例如有關鍵應用程式的站點）部署新內容之前，先在商業風險較小的站點（使用者較少的衛星辦公室）部署。此外，在全網部署之前，先為某些防火牆部署最新的內容更新，還有助於在發生問題時輕鬆解決。您可使用 Panorama 依據組織或位置向防火牆及裝置群組推送交錯排程以及安裝臨界值（使用 Panorama 將更新部署至防火牆）。
- 排程內容更新，以便其自動 **download-and-install**（下載並安裝）。然後，設定 **Threshold**（臨界值），確定防火牆等待多長時間後再安裝最新內容。在任務關鍵性網路中，排程的臨界值至多為 48 小時。



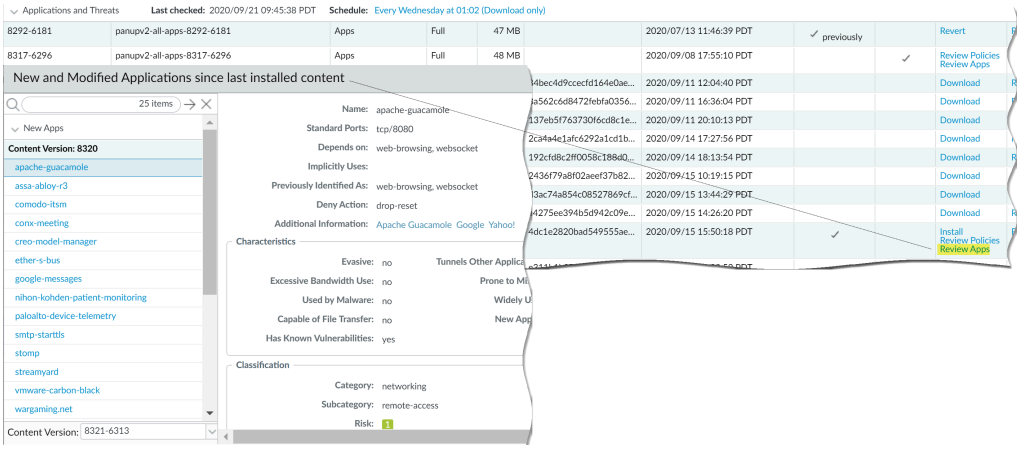
安裝延遲可確保防火牆僅安裝可用內容以及於指定期限內在客戶環境中運作的內容。若要排程內容更新，請選取 **Device**（裝置） > **Dynamic Updates**（動態更新） > **Schedule**（排程）。

- 預留時間，依據新的 App-ID 調整您的安全性原則，然後再安裝這些 App-ID。為此，設定僅套用至包含新 App-ID 之內容更新的安裝臨界值。新 App-ID 的內容更新每月僅發行一次，

僅在此時觸發安裝臨界值。排程內容更新以設定 **New App-ID Threshold**（新 **App-ID** 臨界值）（**Device**（裝置） > **Dynamic Updates**（動態更新） > **Schedule**（排程））。

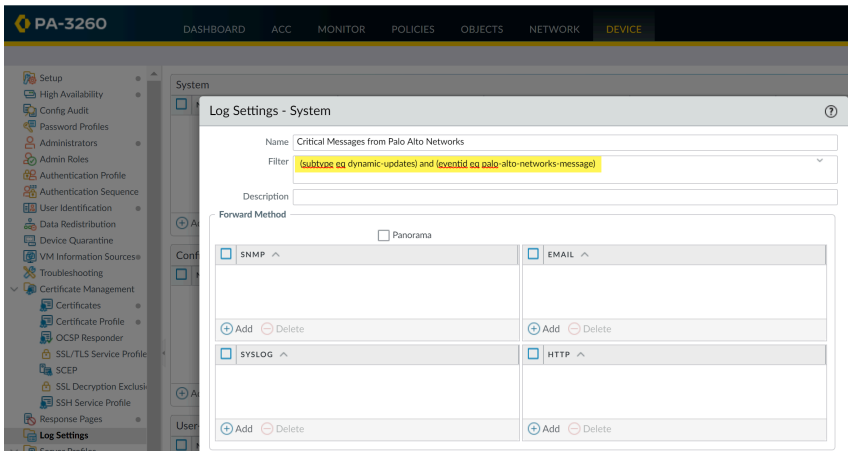


- 務必檢閱內容版本所導入的新的以及已修改的 App-ID，以評估變更會對您的安全性原則產生何種影響。以下主題描述了您可使用哪些選項來在安裝新 App-ID 前後更新您的安全性原則：管理新的以及已修改的 App-ID。



- 組態日誌轉送，以將 Palo Alto Networks 關鍵內容警示傳送至您用於監控網路以及防火牆活動的外部服務。透過這一點，您可確保向對應人員告知關鍵內容事宜，以便他們可按需採

取動作。關鍵內容警示作為系統日誌項目予以記錄，包含以下類型與事件：**(subtype eq dynamic-updates)** 和 **(eventid eq palo-alto-networks-message)**。



PAN-OS 8.1.2 已將關鍵內容警示的日誌類型從 ***general*** 變更為 ***dynamic-updates***。如果您使用的是 *PAN-OS 8.1.0* 或 *PAN-OS 8.1.1*，則關鍵內容將作為具有以下類型和事件的系統日誌項目予以記錄，您應使用以下篩選器為這些警示設定轉送：***(subtype eq general)*** 和 ***(eventid eq palo-alto-networks-message)***。

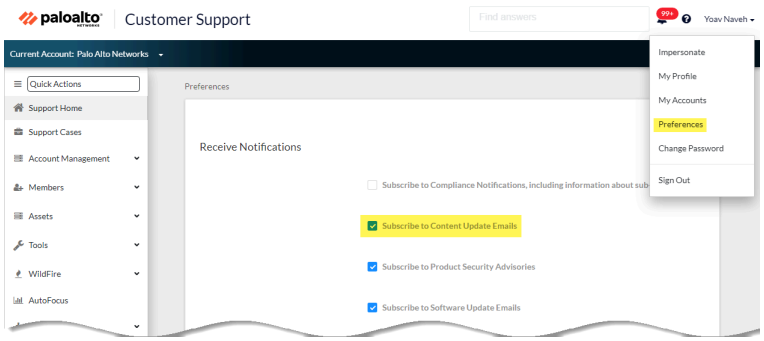
- 在生產環境中啟用新應用程式和威脅內容更新之前，先在專用的模擬環境中進行測試。測試新應用程式和威脅的最簡單方式是使用測試防火牆來接入生產流量。在測試防火牆上安裝最新內容，監控防火牆處理從生產環境複製而來的流量。您還可以使用測試用戶端和測試防火牆或封包擷取 (PCAP) 來模擬生產流量。使用 PCAP 能夠為防火牆安全性原則因站點而異的各種部署模擬流量。

安全性優先之內容更新的最佳做法

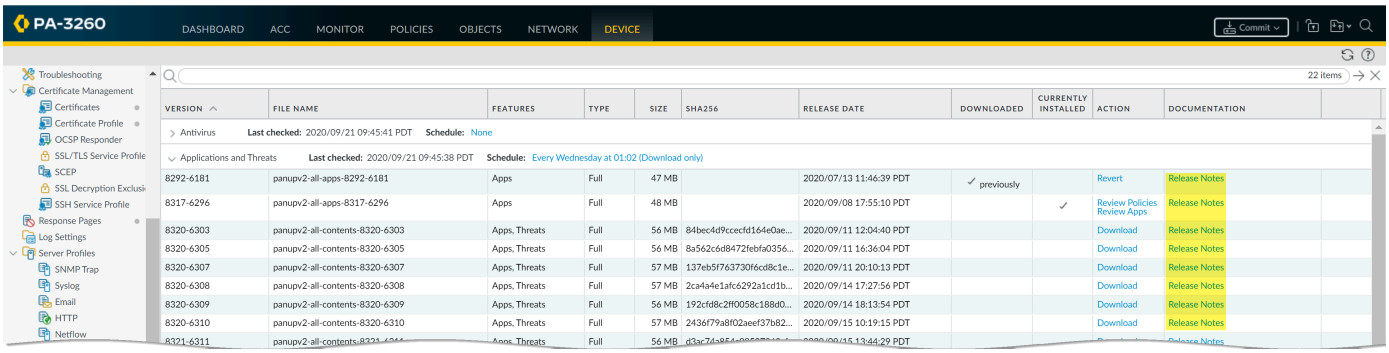
應用程式與威脅內容更新的最佳做法，有助於確保在發行新的應用程式和威脅特徵碼時實現無縫政策執行。遵循這些最佳做法，在安全性優先網路中部署內容更新，在此類網路中，防火牆的主要用途為威脅防禦，您的第一要務為防禦攻擊。

- 務必檢閱內容版本資訊，查看內容版本中引入的新識別和修改的應用程式和威脅特徵碼清單。內容版本資訊中還會介紹更新對現有安全性原則的執行有哪些影響，並提供關於如何修改安全性原則以最大程度地利用新內容的建議。

  若要訂閱最新內容更新的通知，請瀏覽客戶支援入口網站，編輯您的 **Preferences**（喜好設定），然後選取 **Subscribe to Content Update Emails**（訂閱內容更新電子郵件）。



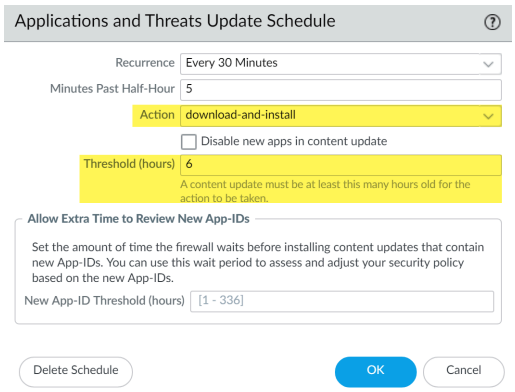
  您還可以在 Palo Alto Networks 支援入口網站上檢閱應用程式和威脅的內容版本說明，或直接在防火牆網頁介面上檢閱：選取 **Device**（裝置） > **Dynamic Updates**（動態更新），然後開啟特定內容發行版本的 **Release Note**（版本說明）。



  內容版本說明的說明區段中強調顯示了 *Palo Alto Networks* 已確定可能嚴重影響涵蓋範圍的未來更新：例如新 *App-ID* 或解碼器。檢查這些未來更新，以便在更新發佈之前估計對原則的影響。

- 為降低對與啟用新應用程式和威脅特徵碼相關之安全性原則執行所產生的影響，請交錯部署新內容。在為商業風險較高的站點（例如有關鍵應用程式的站點）部署新內容之前，先在商業風險較小的站點（使用者較少的衛星辦公室）部署。此外，在全網部署之前，先為某些防火牆部署最新的內容更新，還有助於在發生問題時輕鬆解決。您可使用 Panorama 依據組織或位置向防火牆及裝置群組推送交錯排程以及安裝臨界值（使用 Panorama 將更新部署至防火牆）。

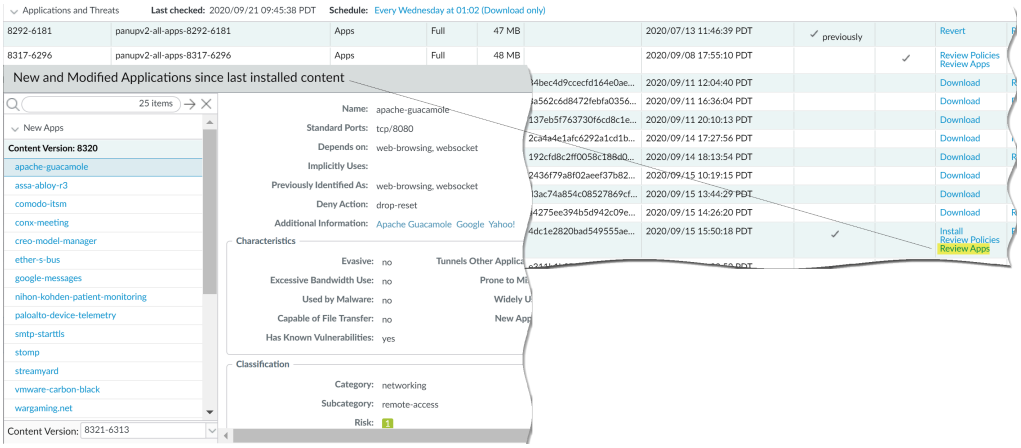
- 排程內容更新，以便其自動 **download-and-install**（下載並安裝）。然後，設定 **Threshold**（臨界值），確定防火牆等待多長時間後再安裝最新內容。在安全性優先網路中，排程的臨界值為六至十二小時。



安裝延遲可確保防火牆僅安裝可用內容以及於指定期限內在客戶環境中運作的內容。若要排程內容更新，請選取 **Device**（裝置） > **Dynamic Updates**（動態更新） > **Schedule**（排程）。

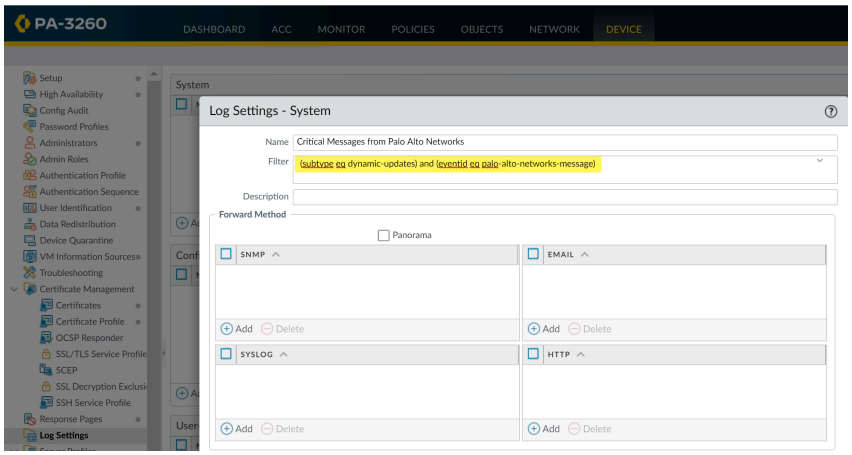
請勿排程 ***New App-ID Threshold***（新 ***App-ID*** 臨界值）。透過此臨界值，任務關鍵性組織可獲得額外時間來依據新 *App-ID* 調整安全性原則執行。但是，由於此臨界值同時會延遲最新威脅防禦更新的傳送，因此不建議安全性優先組織進行採用。

- 檢閱內容版本所導入的新的以及已修改的 App-ID，以評估變更會對您的安全性原則產生何種影響。以下主題描述了您可使用哪些選項來在安裝新 App-ID 前後更新您的安全性原則：管理新的以及已修改的 App-ID。



- 組態日誌轉送，以將 Palo Alto Networks 關鍵內容警示傳送至您用於監控網路以及防火牆活動的外部服務。透過這一點，您可確保向對應人員告知關鍵內容事宜，以便他們可按需採

取動作。關鍵內容警示作為系統日誌項目予以記錄，包含以下類型與事件：(`subtype eq dynamic-updates`) 和 (`eventid eq palo-alto-networks-message`)。



PAN-OS 8.1.2 已將關鍵內容警示的日誌類型從 ***`general`*** 變更為 ***`dynamic-updates`***。如果您使用的是 *PAN-OS 8.1.0* 或 *PAN-OS 8.1.1*，則關鍵內容將作為具有以下類型和事件的系統日誌項目予以記錄，您應使用以下篩選器為這些警示設定轉送：***`(subtype eq general)`*** 和 ***`(eventid eq palo-alto-networks-message)`***。

內容傳送網路基礎結構

Palo Alto Networks 會透過維持內容傳送網路 (CDN) 基礎結構，從而將內容更新傳送至 Palo Alto Networks 防火牆。該防火牆將存取 CDN 中的 Web 資源，以執行各種內容與應用程式識別功能。

下表列出防火牆將針對功能或應用程式而存取的網路資源：

資源	URL	靜態位址 (當靜態伺服器為必要時)
應用程式資料庫 威脅/防毒資料庫	• updates.paloaltonetworks.com（全球，不包括中國大陸） • updates.paloaltonetworks.cn（僅限中國大陸） 如果您的防火牆對網際網路的存取受限，請將以下 URL 新增至您的防火牆允許清單： • downloads.paloaltonetworks.com:443 • proditpdownloads.paloaltonetworks.com:443 作為最佳做法，將更新伺服器設定為 updates.paloaltonetworks.com。這讓 Palo Alto Networks 防火牆可從 CDN 基礎結構中最接近的伺服器接收內容更新。 如果您需要其他參考資訊或遇到連線和更新下載問題，請參閱：https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u0000001UtRCAU Palo Alto Networks ThreatVault 資料庫包含有關漏洞、入侵、病毒和間諜軟體威脅的資訊。防火牆功能（包括 DNS 安全性和防毒設定檔）會使用下列資源來擷取威脅 ID 資訊以建立例外狀況： • data.threatvault.paloaltonetworks.com	us-static.updates.paloaltonetworks.com 將下列 IPv4 或 IPv6 靜態伺服器位址集新增至防火牆允許清單： • **IPv4**—35.186.202.45:443 and 34.120.74.244:443 • **IPv6**—[2600:1901:0:669::]:443 and [2600:1901:0:5162::]:443 為給定通訊協定類型提供的兩個 *IP* 位址必須新增至允許清單，才能正常運作。
PAN-DB URL 篩選 | 進階 URL 篩選	*.urlcloud.paloaltonetworks.com 解析為主要 URL s0000.urlcloud.paloaltonetworks.com，然後重新導向至最接近的區域伺服器： • s0100.urlcloud.paloaltonetworks.com • s0200.urlcloud.paloaltonetworks.com	靜態 IP 位址無法使用。然而，您可以手動將 URL 解析為 IP 位址，並允許存取區域伺服器 IP 位址。

資源	URL	靜態位址 (當靜態伺服器為必要時)
	• s0300.urlcloud.paloaltonetworks.com • s0500.urlcloud.paloaltonetworks.com	
雲端服務	解析為 hawkeye.services-edge.paloaltonetworks.com，然後重新導向至最接近的區域伺服器： • 美國—**us.hawkeye.services-edge.paloaltonetworks.com** • 歐盟—**eu.hawkeye.services-edge.paloaltonetworks.com** • 英國—**uk.hawkeye.services-edge.paloaltonetworks.com** • 亞太地區—**apac.hawkeye.services-edge.paloaltonetworks.com**	靜態 IP 位址無法使用。
DNS 安全性	• 雲端—dns.service.paloaltonetworks.com:443 • 遙測—io.dns.service.paloaltonetworks.com:443 下載允許清單時，dns.service.paloaltonetworks.com 會解析為以下伺服器： • static.dns.service.paloaltonetworks.com:443 • data.threatvault.paloaltonetworks.com（用於建立 DNS 例外狀況）	靜態 IP 位址無法使用。
基於防火牆的內嵌 ML： • URL 篩選內嵌 ML • WildFire 內嵌 ML	• ml.service.paloaltonetworks.com:443	靜態 IP 位址無法使用。
WildFire	• 雲端（報告擷取）—wildfire.paloaltonetworks.com:443 WildFire 雲端區域： • 全球—wildfire.paloaltonetworks.com • 歐盟—eu.wildfire.paloaltonetworks.com • 日本—jp.wildfire.paloaltonetworks.com	靜態 IP 位址無法使用。

資源	URL	靜態位址 (當靜態伺服器為必要時)
	• 新加坡—sg.wildfire.paloaltonetworks.com • 英國—uk.wildfire.paloaltonetworks.com • 加拿大—ca.wildfire.paloaltonetworks.com • 澳洲—au.wildfire.paloaltonetworks.com • 德國—de.wildfire.paloaltonetworks.com • 印度—in.wildfire.paloaltonetworks.com • 瑞士—ch.wildfire.paloaltonetworks.com • 波蘭—pl.wildfire.paloaltonetworks.com • 印尼—id.wildfire.paloaltonetworks.com • 台灣—tw.wildfire.paloaltonetworks.com • 法國—fr.wildfire.paloaltonetworks.com • 卡達—qatar.wildfire.paloaltonetworks.com • 南韓—krv.wildfire.paloaltonetworks.com • 以色列—il.wildfire.paloaltonetworks.com • 沙烏地阿拉伯—sa.wildfire.paloaltonetworks.com • 西班牙—es.wildfire.paloaltonetworks.com	

升級 Panorama

- 安裝 Panorama 的內容更新和軟體升級
- 對您的 Panorama 升級進行疑難排解
- 使用 Panorama 將升級部署至防火牆、日誌收集器和 WildFire 設備

安裝 Panorama 的內容更新和軟體升級

有效的支援使用授權允許存取 Panorama 軟體影像與版本資訊。為了享有最新修正與安全性強化，請升級至轉售商或 Palo Alto Networks 系統工程師針對您的部署所建議的最新軟體與內容更新。安裝軟體與內容更新的程序，視 Panorama 是否直接與網際網路連線和是否有高可用性 (HA) 設定而定。

- 在具有網際網路連線的情況下升級 Panorama
- 在沒有網際網路連線的情況下升級 Panorama
- 為沒有網際網路連線的 Panorama 自動安裝內容更新
- 在 HA 設定中升級 Panorama
- 安裝 PAN-OS 軟體修補程式
- 將 Panorama 日誌移轉為新的日誌格式
- 為增加的設備管理容量升級 Panorama
- 在 FIPS-CC 模式下升級 Panorama 和受管理的裝置
- 從 Panorama 11.1 降級

在具有網際網路連線的情況下升級 Panorama

如果 Panorama™ 直接與網際網路連線，請依需要，執行下列步驟來安裝 Panorama 軟體和內容更新。如果 Panorama 在高可用性 (HA) 設定中執行，請升級每個對等上的 Panorama 軟體（請參閱 在 HA 設定中升級 Panorama）。如果您要在 FIPS-CC 模式下將 Panorama 和受管理的裝置從 PAN-OS 10.2 或更早版本升級至 PAN-OS® 11.1，且在執行 PAN-OS 10.2 版本時已新增至 Panorama 管理，則必須採取其他步驟在 FIPS-CC 模式下重設裝置的安全連線狀態。請參閱 在 FIPS-CC 模式下升級 Panorama 和受管理的裝置，瞭解關於在 FIPS-CC 模式下升級 Panorama 和 FIPS-CC 裝置的更多詳細資訊。

在 Panorama 虛擬設備上升級軟體不會變更系統模式；切換至 Panorama 模式或僅管理模式是手動工作，需要額外的設定，如設定具備本機日誌收集器的 Panorama 虛擬設備所述。

Palo Alto Networks 在升級路徑的不同點引入了新的日誌資料格式，具體取決於您要升級的 *PAN-OS* 版本。

- 從 ***PAN-OS 8.1*** 升級至 ***PAN-OS 9.0***—*PAN-OS 9.0* 為本機和專用日誌收集器引入了新的日誌資料格式。在升級到 *PAN-OS 11.1* 的路徑上，當您從 *PAN-OS 8.1* 升級到 *PAN-OS 9.0* 時，現有日誌資料會自動移轉至新格式。
- 從 ***PAN-OS 10.0*** 升級至 ***PAN-OS 10.1***—*PAN-OS 10.1* 為本機和專用日誌收集器引入了新的日誌格式。在升級到 *PAN-OS 11.1* 的路徑上，在 *PAN-OS 8.1* 或更早版本中產生的日誌不再可用。這包括升級到 *PAN-OS 9.0* 的過程中移轉的日誌。升級到 *PAN-OS 10.1* 後，您可以選擇還原這些日誌並將其移轉至 *PAN-OS 10.1* 日誌格式。

您必須同時在收集器群組內升級所有日誌收集器，以避免丟失日誌資料。如果收集器群組內的日誌收集器並非執行相同的 PAN-OS 版本，則無法進行日誌轉送或日誌收集。此外，除非所有日誌收集器執行相同的 PAN-OS 版本，否則收集器群組內的日誌收集器日誌資料在 **ACC** 或 **Monitor**（監控器）頁籤內不可見。例如，如果您在收集器群組內有三個日誌收集器，且您升級了其中兩個，則不會有日誌被轉送至收集器群組內的任何日誌收集器。

更新 Panorama 之前，請參閱版本資訊，瞭解 PAN-OS® 11.1 所需的最低內容發行版本。

STEP 1 | 確認您計劃安裝的更新適合您的 Panorama 部署。

Palo Alto Networks 高度建議 *Panorama*、日誌收集器和所有受管理的防火牆執行相同的內容發行版本。

- 請參閱版本資訊，瞭解 Panorama 軟體版本所需的最低內容發行版本。如果您要升級日誌收集器和防火牆至特定版本，必須先將 Panorama 升級至該版本（或更新版本）。
- 對於 Hypervisor 上執行的 Panorama 虛擬設備，確保實例符合 設定 Panorama 虛擬設備的先決條件 。

STEP 2 | 確定升級到 PAN-OS 11.1 的路徑.

您無法略過從目前執行的 PAN-OS 版本到 PAN-OS 11.1 的路徑中任何功能發佈版本的安裝。

檢閱 PAN-OS 升級檢查清單，瞭解您在升級路徑中會經過的每個版本的版本資訊和 升級/降級考量事項 中的已知問題和預設行為變更。

STEP 3 | （僅 Panorama Interconnect 外掛程式）同步 Panorama 節點與 Panorama 控制器。

開始升級 Panorama 節點之前，您必須同步 Panorama 控制器和 Panorama 節點設定。您必須這麼做才能在升級之後，成功將常見 Panorama 控制器設定推送到 Panorama 節點。

STEP 4 | 儲存目前 Panorama 組態檔案的備份，如果升級發生問題，此檔案可用來還原設定。

雖然 *Panorama* 會自動建立設定的備份，但最好在升級前建立備份並儲存在外部。

1. 登入 Panorama 網頁介面。
2. 儲存名為 **Panorama** 的設定快照（**Panorama** > **Setup**（設定） > **Operations**（操作）），輸入設定的 **Name**（名稱），然後按一下 **OK**（確定）。
3. **Export named Panorama configuration snapshot**（匯出具名 **Panorama** 組態快照），選取您剛儲存的設定 **Name**（名稱），按一下 **OK**（確定），並將匯出的檔案儲存至 Panorama 外部的位置。

STEP 5 | （最佳做法）如果您正在使用 Cortex Data Lake (CDL)，請安裝 Panorama 裝置憑證。

Panorama 會在升級至 PAN-OS 11.1 時自動切換至使用裝置憑證進行 CDL 擷取和查詢端點的驗證。

如果在升級至 *PAN-OS 11.1* 之前未安裝裝置憑證，*Panorama* 會繼續使用現有日誌記錄服務憑證進行驗證。

STEP 6 | 在網路上啟用以下 TCP 連接埠。

您必須在網路上啟用這些 TCP 連接埠，才能允許日誌收集器之間的通訊。

- TCP/9300
- TCP/9301
- TCP/9302

STEP 7 | 安裝最新內容更新。

如果 *Panorama* 執行的內容版本，不是您要升級到的 *Panorama* 版本所需的最低內容版本，您必須先將內容版本更新至最低（或更新）版本，然後才安裝軟體更新。請參閱版本資訊，瞭解 *Panorama* 版本的最低內容發行版本。

Palo Alto Networks® 高度建議 *Panorama*、日誌收集器和所有受管理的防火牆執行相同的內容發行版本。此外，建議您排定自動的週期性更新，以一律執行最新內容版本（請參考 18）。

1. 選取 **Panorama** > **Dynamic Updates**（動態更新），然後選取 **Check Now**（立即檢查）以獲得最新更新。如果在 Action（動作）欄中的值為 **Download**（下載），則表示可進行該項更新。

   請確定 *Panorama* 執行的內容發行版本，與受管理的防火牆和日誌收集器相同，但並不是更新的版本。

2. （在 Panorama 上更新內容發行版本之前，務必將防火牆從 Panorama 升級至 PAN-OS 11.1和日誌收集器（請參閱當 Panorama 連線至網際網路時升級日誌收集器）至相同（或更新）的內容發行版本。

   如果您此時不需要安裝內容更新，請直接跳至下個步驟。

3. 依需要安裝其餘的內容更新。安裝後，Currently Installed（目前已安裝）欄會顯示核取標記。

   1. **Download**（下載）並 **Install**（安裝） 應用程式和威脅更新。無論您的訂閱如何，Panorama 都只安裝和需要應用程式內容更新，而不是威脅內容。請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。
   2. 依需要、一次一個、以任意順序 **Download**（下載）並 **Install**（安裝）其他更新（防毒、WildFire® 或 URL 篩選）。

STEP 8 | 選取 **Panorama** > **Plugins**（外掛程式） 並為目前 Panorama 上安裝的所有外掛程式 **Download**（下載）PAN-OS 11.1 支援的外掛程式版本。

有關您的目標 PAN-OS 11.1 版本支援的 Panorama 外掛程式版本，請參閱相容性矩陣。

需要執行此步驟以成功地將 Panorama 從 PAN-OS 11.0 升級至 PAN-OS 11.1。如果未下載支援的外掛程式版本，將封鎖升級至 PAN-OS 11.1。

升級到 *PAN-OS 11.1* 所需的已下載外掛程式會在 *Panorama* 成功升級至 *PAN-OS 11.1* 後自動安裝。如果下載的外掛程式沒有自動安裝，您必須在升級至 *PAN-OS 11.1* 後手動安裝受影響的外掛程式

STEP 9 | 沿著您升級到 PAN-OS 11.1 的路徑，將 Panorama 升級至 PAN-OS 版本。

1. 在具有網際網路連線的情況下將 Panorama 升級 到 PAN-OS 9.1。
2. 在具有網際網路連線的情況下將 Panorama 升級到 PAN-OS 10.0。

   （僅限傳統模式下的 *Panorama*）***Download***（下載）*PAN-OS 10.0.0*，然後在繼續升級路徑之前 ***Download***（下載）並 ***Install***（安裝）*PAN-OS 10.0.8* 或更高版本。

   需要執行此步驟以保留儲存在 *NFS* 儲存分割區上的所有日誌。如果安裝 *PAN-OS 10.0.7* 或更早的 *PAN-OS 10.0* 版本，部分在傳統模式下儲存在 *Panorama* 的 *NFS* 儲存分割區上的日誌將被刪除。
3. 在具有網際網路連線的情況下將 Panorama 升級到 PAN-OS 10.1。

   PAN-OS 10.1 引入了新的日誌格式。從 PAN-OS 10.0 升級至 PAN-OS 10.1 時，您可以選擇移轉 PAN-OS 8.1 或更早版本中產生的日誌。否則，這些日誌會在成功升級至 PAN-OS 10.1 時自動被刪除。移轉過程中，日誌資料在 ACC 或 Monitor（監控器）頁籤中不可見。進行移轉時，日誌資料會繼續轉送至適當的日誌收集器，但您可能會遇到一些對效能的影響。

   （僅限傳統模式下的 *Panorama*）***Download***（下載）*PAN-OS 10.1.0*，然後 ***Download***（下載）並 ***Download***（安裝）*PAN-OS 10.1.3* 或更高版本。

   需要執行此步驟以保留儲存在 *NFS* 儲存分割區上的所有日誌。如果安裝 *PAN-OS 10.1.2* 或更早的 *PAN-OS 10.1* 版本，部分在傳統模式下儲存在 *Panorama* 的 *NFS* 儲存分割區上的日誌將被刪除。
4. 在具有網際網路連線的情況下將 Panorama 升級到 PAN-OS 10.2。
5. 在具有網際網路連線的情況下將 Panorama 升級到 PAN-OS 11.0。

STEP 10 | 將 Panorama 升級到 PAN-OS 11.1。

1. **Check Now**（立即檢查）（**Panorama** > **Software**（軟體））有無最新版本。

   （PAN-OS 11.1.3 及更新版本）根據預設，系統會顯示慣用版本和相應的基礎版本。若要僅查看慣用版本，請停用（清除）**Base Releases**（基礎版本）核取方塊。同理，若要僅查看基礎版本，請停用（清除）**Preferred Releases**（管用版本）核取方塊。
2. 找到並 **Download**（下載）PAN-OS 11.1.0 映像。成功下載之後，已下載的映像的 Action（動作）欄會從 **Download**（下載）變更為 **Install**（安裝）。
3. （僅 Panorama 模式）如果您的日誌收集器包含在 PAN-OS 10.0 或更舊版本中生成的日誌，則系統會顯示通知。

   首次嘗試 **Install**（安裝）PAN-OS 11.1.2 或更新版本的 11.1 版本時，系統會顯示此通知，但在通知關閉後就不會再顯示。通知會警告您系統偵測到執行 PAN-OS 10.0 或更舊

版本時，Panorama 或受管理裝置生成的日誌，且這些日誌將在升級時遭刪除。這表示在成功升級之後，您無法再查看或搜尋受影響的日誌。

但您可以在升級之後復原這些受影響的日誌。通知也會為您提供以下資訊：

- 受影響的日誌類型。
- 每種日誌類型的受影響時間範圍。
- 復原每種日誌類型的受影響日誌時需要的每個 `debug logdb migrate-lc` 命令。

  複製所列 `debug logdb migrate-lc` 然後再 **Close**（關閉）通知。

Close（關閉）通知。

4. **Install**（安裝）下載的映像，然後重新啟動。
   1. 安裝映像。
   2. 安裝成功完成後，使用下列其中一種方法重新啟動：
      - 如果提示重新啟動，請按一下 **Yes**（是）。如果您看到 CMS Login（CMS 登入）提示，請按下 Enter，無須鍵入使用者名稱或密碼。當 Panorama 登入提示出現時，請輸入您在初始設定期間指定的使用者名稱與密碼。
      - 如果未提示您重新啟動，請從裝置操作部分 **Reboot Panorama**（重新啟動 **Panorama**）（**Panorama** > **Setup**（設定） > **Operations**（操作））。

   Panorama 成功重新啟動後，請繼續執行下一步。

STEP 11 | （PAN-OS 11.1.2 及更新版本；僅限 Panorama 模式）登入 Panorama CLI，並使用上一步列出的 `debug logdb migrate-lc` 命令復原受影響的日誌。

這些命令必須按照順序執行，不能同時執行。如果您沒有複製通知視窗中的 `debug logdb migrate-lc` 命令，請按一下 **Tasks**（工作）並查看失敗安裝作業詳細資訊。

STEP 12 | 確認您的 Panorama 外掛程式版本是否受 PAN-OS 11.1 支援。

成功升級 Panorama 後，您必須確認並安裝 PAN-OS 11.1 支援的 Panorama 外掛程式版本。有關 PAN-OS 11.1 支援的 Panorama 外掛程式版本的詳細資訊，請參閱相容性矩陣。

1. 登入 Panorama 網頁介面並檢閱 **Dashboard**（儀表板）中的一般資訊 Widget，以驗證是否成功安裝了 PAN-OS 11.1 相容的外掛程式版本。

   您還可以 登入 Panorama CLI 並輸入命令 `show plugins installed` 以檢視目前安裝的外掛程式清單。
2. 選取 **Panorama** > **Plugins**（外掛程式）並搜尋未安裝的外掛程式。
3. **Install**（安裝）PAN-OS 11.1 支援的外掛程式版本。
4. 重複上述步驟，直至 Panorama 上安裝的所有外掛程式都執行 PAN-OS 11.1 支援的版本。

STEP 13 | （如果本機日誌收集器位於收集器群組內）在收集器群組內升級剩餘日誌收集器。

- 當 Panorama 連線至網際網路時升級日誌收集器
- 當 Panorama 未連線至網際網路時升級日誌收集器

STEP 14 | （FIPS-CC 模式下的 Panorama 和受管理的裝置）在 FIPS-CC 模式下升級 Panorama 和受管理的裝置。

如果在執行 PAN-OS 11.1 版本時已新增至 Panorama 管理，則在 FIPS-CC 模式下升級 Panorama 與受管理的裝置時，必須在 FIPS-CC 模式下重設裝置的安全連線狀態。您需要將下列受管理的裝置重新裝載至 Panorama 管理：

- 使用裝置註冊驗證金鑰在 FIPS-CC 模式下新增至 Panorama 的受管理裝置。
- 使用裝置註冊驗證金鑰在正常操作模式下新增至 Panorama 的受管理裝置

。當受管理的裝置執行 PAN-OS 10.0 或更早版本時，您無需重新裝載已新增至 Panorama 管理的受管理裝置。

STEP 15 | 重新產生或重新匯入所有憑證以遵守 OpenSSL 安全性等級 2。

如果您從 PAN-OS 10.1 或更早版本升級至 PAN-OS 11.1，則需要執行此步驟。如果您是從 PAN-OS 10.2 升級並且已經重新產生或重新匯入憑證，請略過此步驟。

要求所有憑證滿足以下最低要求：

- RSA 2048 位元或以上，或 ECDSA 256 位元或以上
- SHA256 或更高版本的摘要

有關重新產生或重新匯入憑證的更多資訊，請參閱 PAN-OS 管理員指南或 Panorama 管理員指南。

STEP 16 | （建議用於 Panorama 模式）將 Panorama 虛擬設備的記憶體增加至 64GB。

在 Panorama 模式下將 Panorama 虛擬設備成功升級至 PAN-OS 11.1 後，Palo Alto Networks 建議將 Panorama 虛擬設備的記憶體增加到 64GB 以滿足增加的系統要求，從而避免發生任何與佈建不足的 Panorama 虛擬設備相關的日誌記錄、管理和運作效能問題。

STEP 17 | 選取 **Commit**（提交） > **Commit and Push**（提交並推送）並 **Commit and Push**（提交並推送）Panorama 受管理設定至所有受管理裝置。

成功將 Panorama 和受管理裝置升級到 PAN-OS 11.1 之後，您需要先完全提交並推送 Panorama 受管理設定，才能將選擇性設定推送到您的受管理裝置，並善用 Panorama 管理的多重 vsys 防火牆的改良共用設定物件管理。

STEP 18 | （最佳作法）排程自動週期性內容更新。

Panorama 不會在 *HA* 端點之間同步內容更新排程。您必須在主動和被動 *Panorama* 上執行此工作。

在每種更新類型的標題列中（**Panorama** > **Dynamic Updates**（動態更新）），**Schedule**（排程）最初設定為 **None**（無）。針對每種更新類型執行下列步驟。

1. 按一下 **None**（無），然後選取更新頻率（**Recurrence**（週期性））。頻率選項取決於更新類型。
2. 選取排程動作：
   - **Download And Install**（下載並安裝）（最佳作法）—Panorama 下載更新後會自動安裝更新。

     Download Only（僅下載）—您必須在 Panorama 下載完成後手動安裝更新。
3. 根據組織的安全性狀態的最佳作法，設定有可用的更新之後到 Panorama 下載更新之前的延遲（**Threshold**（閾值））。
4. 按一下 **OK**（確定）儲存您的變更。
5. 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交） 您的變更。

在沒有網際網路連線的情況下升級 Panorama

如果 Panorama™ 未直接與網際網路連線，請依需要，執行下列步驟來安裝 Panorama 軟體和內容更新。如果 Panorama 部署在高可用性 (HA) 設定中，您必須升級每個對等（請參閱 在 HA 設定中升級 Panorama）。如果您要在 FIPS-CC 模式下將 Panorama 和受管理的裝置從 PAN-OS 10.2 或更早版本升級至 PAN-OS 11.1，且在執行 PAN-OS 10.2 版本時已新增至 Panorama 管理，則必須採取其他步驟在 FIPS-CC 模式下重設裝置的安全連線狀態。請參閱 在 FIPS-CC 模式下升級 Panorama 和受管理的裝置，瞭解關於在 FIPS-CC 模式下升級 Panorama 和 FIPS-CC 裝置的更多詳細資訊。

在 Panorama 虛擬設備上升級軟體不會變更系統模式；切換至 Panorama 模式或僅管理模式是手動工作，需要額外的設定，如設定具備本機日誌收集器的 Panorama 虛擬設備所述。

Palo Alto Networks 在升級路徑的不同點引入了新的日誌資料格式，具體取決於您要升級的 *PAN-OS* 版本。

- 從 ***PAN-OS 8.1*** 升級至 ***PAN-OS 9.0***—*PAN-OS 9.0* 為本機和專用日誌收集器引入了新的日誌資料格式。在升級到 *PAN-OS 11.1* 的路徑上，當您從 *PAN-OS 8.1* 升級到 *PAN-OS 9.0* 時，現有日誌資料會自動移轉至新格式。
- 從 ***PAN-OS 10.0*** 升級至 ***PAN-OS 10.1***—*PAN-OS 10.1* 為本機和專用日誌收集器引入了新的日誌格式。在升級到 *PAN-OS 11.1* 的路徑上，在 *PAN-OS 8.1* 或更早版本中產生的日誌不再可用。這包括升級到 *PAN-OS 9.0* 的過程中移轉的日誌。升級到 *PAN-OS 10.1* 後，您可以選擇還原這些日誌並將其移轉至 *PAN-OS 10.1* 日誌格式。

您必須同時在收集器群組內升級所有日誌收集器，以避免丟失日誌資料。如果收集器群組內的日誌收集器並非執行相同的 PAN-OS 版本，則無法進行日誌轉送或日誌收集。此外，除非所有日誌收集器執行相同的 PAN-OS 版本，否則收集器群組內的日誌收集器日誌資料在 **ACC** 或 **Monitor**（監控器）頁籤內不可見。例如，如果您在收集器群組內有三個日誌收集器，且您升級了其中兩個，則不會有日誌被轉送至收集器群組內的任何日誌收集器。

升級 Panorama 之前，請參閱版本資訊，瞭解 PAN-OS® 11.1 所需的最低內容發行版本。

STEP 1 | 確認您計劃安裝的更新適合您的 Panorama 部署。

Palo Alto Networks 高度建議 *Panorama*、日誌收集器和所有受管理的防火牆執行相同的內容發行版本。

- 參考版本資訊，瞭解您必須為 Panorama 軟體版本安裝的最低內容版本。如果您要升級日誌收集器和防火牆至特定版本，必須先將 Panorama 升級至該版本（或更新版本）。
- 對於 Panorama 虛擬設備，確保實例符合 設定 Panorama 虛擬設備的先決條件 。

STEP 2 | 確定升級到 PAN-OS 11.1 的路徑.

您無法略過從目前執行的 PAN-OS 版本到 PAN-OS 11.1 的路徑中任何功能發佈版本的安裝。

檢閱 PAN-OS 升級檢查清單，瞭解您在升級路徑中會經過的每個版本的版本資訊和 升級/降級考量事項 中的已知問題和預設行為變更。

STEP 3 | （僅 Panorama Interconnect 外掛程式）同步 Panorama 節點與 Panorama 控制器。

開始升級 Panorama 節點之前，您必須同步 Panorama 控制器和 Panorama 節點設定。您必須這麼做才能在升級之後，成功將常見 Panorama 控制器設定推送到 Panorama 節點。

STEP 4 | 儲存目前 Panorama 組態檔案的備份，如果升級發生問題，此檔案可用來還原設定。

雖然 *Panorama* 會自動建立設定的備份，但最好在升級前建立備份並儲存在外部。

1. 登入 Panorama 網頁介面。
2. 儲存名為 **Panorama** 的設定快照（**Panorama** > **Setup**（設定） > **Operations**（操作）），輸入設定的 **Name**（名稱），然後按一下 **OK**（確定）。
3. **Export named Panorama configuration snapshot**（匯出具名 **Panorama** 組態快照），選取您剛儲存的設定 **Name**（名稱），按一下 **OK**（確定），並將匯出的檔案儲存至 Panorama 外部的位置。

STEP 5 | 將最新內容更新下載到可透過 SCP 或 HTTPS 連線至 Panorama 並上傳內容的主機。

如果您此時不需要安裝內容更新，請直接跳至步驟 6。

1. 使用可存取網際網路的主機登入 Palo Alto Networks 客戶支援網站。
2. 依需要下載內容更新：
   1. 在 Resources（資源）區段按一下 **Updates**（更新） > **Dynamic Updates**（動態更新）。
   2. **Download**（下載）適當的內容更新，然後將檔案儲存至主機。針對您需要更新的各內容類型執行此步驟。

STEP 6 | 在網路上啟用以下 TCP 連接埠。

您必須在網路上啟用這些 TCP 連接埠，才能允許日誌收集器之間的通訊。

- TCP/9300
- TCP/9301
- TCP/9302

STEP 7 | 安裝最新內容更新。

您必須在軟體更新前安裝內容更新，且必須在 *Panaroma* 管理伺服器上安裝防火牆和日誌收集器前，先將防火牆從 Panorama 升級至 PAN-OS 11.1 後，再升級日誌收集器。

先安裝「應用程式」或「應用程式和威脅」更新，再一次一個、以任意順序安裝其他任何更新（防毒、WildFire® 和 URL 篩選）。

無論您的訂閱是否同時包含應用程式和威脅內容，*Panorama* 都只需要並且只會安裝應用程式內容。請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。

登入 Panorama 網頁介面，為每個內容類型執行以下步驟：

1. 選取 **Panorama** > **Dynamic Updates**（動態更新）。
2. 按一下 **Upload**（上傳），選取內容 **Type**（類型），**Browse**（瀏覽）至您已將更新下載至主機上的那個位置，選取更新，然後按一下 **OK**（確定）。
3. **Install From File**（從檔案安裝），選取 **Package Type**（套件類型），並按一下 **OK**（確定）。

STEP 8 | 為目前 Panorama 上安裝的所有外掛程式上傳 PAN-OS 11.1 支援的外掛程式版本。

有關您的目標 PAN-OS 11.1 版本支援的 Panorama 外掛程式版本，請參閱相容性矩陣。

需要執行此步驟以成功地將 Panorama 從 PAN-OS 11.0 升級至 PAN-OS 11.1。如果未下載支援的外掛程式版本，將封鎖升級至 PAN-OS 11.1。

升級到 *PAN-OS 11.1* 所需的已下載外掛程式會在 *Panorama* 成功升級至 *PAN-OS 11.1* 後自動安裝。如果下載的外掛程式沒有自動安裝，您必須在升級至 *PAN-OS 11.1* 後手動安裝受影響的外掛程式

1. 下載 PAN-OS 11.1 支援的外掛程式版本。
   1. 登入 Palo Alto Networks Support 入口網站。
   2. 選取 **Updates**（更新） > **Software Updates**（軟體更新）並從下拉式功能表中選取外掛程式。
   3. **Download**（下載）PAN-OS 10.2 支援的外掛程式版本。
   4. 對 Panorama 上目前安裝的所有外掛程式重複此步驟。
2. 登入 Panorama 網頁介面。
3. 選取 **Panorama** > **Plugins**（外掛程式）並 **Upload**（上傳） 您在上一步中下載的外掛程式版本。

   對 Panorama 上目前安裝的所有外掛程式重複此步驟。

STEP 9 | 沿著您升級到 PAN-OS 11.1 的路徑，將 Panorama 升級至 PAN-OS 版本。

1. 在沒有連線至網際網路的情況下將 Panorama 升級到 PAN-OS 9.1。
2. 在沒有連線至網際網路的情況下將 Panorama 升級 到 PAN-OS 10.0。

   （僅限傳統模式下的 *Panorama*）**Download**（下載）*PAN-OS 10.0.0*，然後在繼續升級路徑之前 **Download**（下載）並 **Install**（安裝）*PAN-OS 10.0.8* 或更高版本。

   需要執行此步驟以保留儲存在 *NFS* 儲存分割區上的所有日誌。如果安裝 *PAN-OS 10.0.7* 或更早的 *PAN-OS 10.0* 版本，部分在傳統模式下儲存在 *Panorama* 的 *NFS* 儲存分割區上的日誌將被刪除。
3. 在沒有連線至網際網路的情況下將 Panorama 升級 到 PAN-OS 10.1。

   PAN-OS 10.1 引入了新的日誌格式。從 PAN-OS 10.0 升級至 PAN-OS 10.1 時，您可以選擇移轉 PAN-OS 8.1 或更早版本中產生的日誌。否則，這些日誌會在成功升級至 PAN-OS 10.1 時自動被刪除。移轉過程中，日誌資料在 ACC 或 Monitor（監控器）頁籤中不可見。進行移轉時，日誌資料會繼續轉送至適當的日誌收集器，但您可能會遇到一些對效能的影響。

   （僅限傳統模式下的 *Panorama*）**Download**（下載）*PAN-OS 10.1.0*，然後 **Download**（下載）並 **Download**（安裝）*PAN-OS 10.1.3* 或更高版本。

   需要執行此步驟以保留儲存在 *NFS* 儲存分割區上的所有日誌。如果安裝 *PAN-OS 10.1.2* 或更早的 *PAN-OS 10.1* 版本，部分在傳統模式下儲存在 *Panorama* 的 *NFS* 儲存分割區上的日誌將被刪除。
4. 在沒有連線至網際網路的情況下將 Panorama 升級 到 PAN-OS 10.2。
5. 在沒有連線至網際網路的情況下將 Panorama 升級 到 PAN-OS 11.0。

STEP 10 | 將最新 PAN-OS 11.1 版本映像下載到可透過 SCP 或 HTTPS 連線至 Panorama 並上傳內容的主機。

1. 使用可存取網際網路的主機登入 Palo Alto Networks 客戶支援網站。
2. 下載軟體更新：
   1. 在 Palo Alto Networks 客戶支援網站的主頁面，按一下 **Updates**（更新） > **Software Updates**（軟體更新）。
   2. 為最新的 PAN-OS 11.1 版本找到特定於型號的映像。例如，若要將 M-Series 設備升級至 Panorama 11.1.0，請下載 `Panorama_m-11.1.0` 映像檔；若要將 Panorama 虛擬設備升級至 Panorama 11.1.0，請下載 `Panorama_pc-11.1.0` 映像檔。

      您可以從 **Content By**（內容依據）下拉式清單中，選取 ***Panorama M Images***（*Panorama M* 映像）（*M-Series* 設備）或 ***Panorama Updates***（*Panorama* 更新）（虛擬設備），快速找到 *Panorama* 映像。

      （*PAN-OS 11.1.3* 及更新版本）根據預設，結果會顯示慣用版本。在 ***Release type***（發佈類型）欄位中，按一下 **Other**（其他）以查看其他可用版本。
   3. 按一下檔名，並將檔案儲存至主機。

STEP 11 | 將 Panorama 升級到 PAN-OS 11.1。

1. 登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Software**（軟體），然後 **Upload**（上傳）您在上一步驟中下載的 PAN-OS 11.1 映像。
3. **Browse**（瀏覽）至您已將更新下載至主機上的那個位置，如果 Panorama 在 HA 設定中，請選取 **Sync To Peer**（同步至對等）核取方塊（將軟體映像推送至次要對等），然後按一下 **OK**（確定）。
4. （僅 Panorama 模式）如果您的日誌收集器包含在 PAN-OS 10.0 或更舊版本中生成的日誌，則系統會顯示通知。

   首次嘗試 **Install**（安裝）PAN-OS 11.1.2 或更新版本的 11.1 版本時，系統會顯示此通知，但在通知關閉後就不會再顯示。通知會警告您系統偵測到執行 PAN-OS 10.0 或更舊版本時，Panorama 或受管理裝置生成的日誌，且這些日誌將在升級時遭刪除。這表示在成功升級之後，您無法再查看或搜尋受影響的日誌。

   但您可以在升級之後復原這些受影響的日誌。通知也會為您提供以下資訊：

   - 受影響的日誌類型。
   - 每種日誌類型的受影響時間範圍。
   - 復原每種日誌類型的受影響日誌時需要的每個 `debug logdb migrate-lc` 命令。

     複製所列 `debug logdb migrate-lc` 然後再 **Close**（關閉）通知。

   Close（關閉）通知。
5. 安裝軟體映像並重新啟動。

   對於 HA 設定，在 HA 設定中升級 Panorama；否則：

   1. **Install**（安裝）上傳的映像。
   2. 成功完成安裝後，使用下列其中一種方法重新啟動：

      - 如果提示重新啟動，請按一下 **Yes**（是）。如果您看到 CMS Login（CMS 登入）提示，請按下 Enter，無須鍵入使用者名稱或密碼。當 Panorama 登入提示出現時，請輸入您在初始設定期間指定的使用者名稱與密碼。
      - 如果未提示您重新啟動，請從裝置操作部分 **Reboot Panorama**（重新啟動 **Panorama**）（**Panorama** > **Setup**（設定） > **Operations**（操作））。

   Panorama 成功重新啟動後，請繼續執行下一步。

STEP 12 | （PAN-OS 11.1.2 及更新版本；僅限 Panorama 模式）登入 Panorama CLI，並使用上一步列出的 `debug logdb migrate-lc` 命令復原受影響的日誌。

這些命令必須按照順序執行，不能同時執行。如果您沒有複製通知視窗中的 `debug logdb migrate-lc` 命令，請按一下 **Tasks**（工作）並查看失敗安裝作業詳細資訊。

STEP 13 | 確認您的 Panorama 外掛程式版本是否受 PAN-OS 11.1 支援。

成功升級 Panorama 後，您必須確認並安裝 PAN-OS 11.1 支援的 Panorama 外掛程式版本。有關 PAN-OS 11.1 支援的 Panorama 外掛程式版本的詳細資訊，請參閱相容性矩陣。

1. 登入 Panorama 網頁介面並檢閱 **Dashboard**（儀表板）中的一般資訊 Widget，以驗證是否成功安裝了 PAN-OS 11.1 相容的外掛程式版本。

   您還可以 登入 Panorama CLI 並輸入命令 `show plugins installed` 以檢視目前安裝的外掛程式清單。
2. 選取 **Panorama** > **Plugins**（外掛程式）並搜尋未安裝的外掛程式。
3. **Install**（安裝）PAN-OS 11.1 支援的外掛程式版本。
4. 重複上述步驟，直至 Panorama 上安裝的所有外掛程式都執行 PAN-OS 11.1 支援的版本。

STEP 14 | （如果本機日誌收集器位於收集器群組內）在收集器群組內升級剩餘日誌收集器。

STEP 15 | （建議用於 Panorama 模式）將 Panorama 虛擬設備的記憶體增加至 64GB。

在 Panorama 模式下將 Panorama 虛擬設備成功升級至 PAN-OS 11.1 後，Palo Alto Networks 建議將 Panorama 虛擬設備的記憶體增加到 64GB 以滿足增加的系統要求，從而避免發生任何與佈建不足的 Panorama 虛擬設備相關的日誌記錄、管理和運作效能問題。

STEP 16 | （FIPS-CC 模式下的 Panorama 和受管理的裝置）在 FIPS-CC 模式下升級 Panorama 和受管理的裝置。

如果在執行 PAN-OS 11.1 版本時已新增至 Panorama 管理，則在 FIPS-CC 模式下升級 Panorama 與受管理的裝置時，必須在 FIPS-CC 模式下重設裝置的安全連線狀態。您需要將以下受管理裝置重新載入 Panorama 管理：

- 使用裝置註冊驗證金鑰在 FIPS-CC 模式下新增至 Panorama 的受管理裝置。
- 使用裝置註冊驗證金鑰在正常操作模式下新增至 Panorama 的受管理裝置

。當受管理的裝置執行 PAN-OS 10.0 或更早版本時，您無需重新裝載已新增至 Panorama 管理的受管理裝置。

STEP 17 | （PAN-OS 10.2 及更高版本）重新產生或重新匯入所有憑證以遵守 OpenSSL 安全性等級 2。

如果您從 PAN-OS 10.1 或更早版本升級至 PAN-OS 11.1，則需要執行此步驟。如果您是從 PAN-OS 10.2 升級並且已經重新產生或重新匯入憑證，請略過此步驟。

要求所有憑證滿足以下最低要求：

- RSA 2048 位元或以上，或 ECDSA 256 位元或以上
- SHA256 或更高版本的摘要

有關重新產生或重新匯入憑證的更多資訊，請參閱 PAN-OS 管理員指南或 Panorama 管理員指南。

STEP 18 | 選取 **Commit**（提交） > **Commit and Push**（提交並推送）並 **Commit and Push**（提交並推送）Panorama 受管理設定至所有受管理裝置。

成功將 Panorama 和受管理裝置升級到 PAN-OS 11.1 之後，您需要先完全提交並推送 Panorama 受管理設定，才能將選擇性設定推送到您的受管理裝置，並善用 Panorama 管理的多重 vsys 防火牆的改良共用設定物件管理。

為沒有網際網路連線的 Panorama 自動安裝內容更新

自動下載內容更新到氣隙網路中的防火牆、日誌收集器和 WildFire® 設備，在該網路中，Panorama™ 管理伺服器、受管理防火牆、日誌收集器和 WildFire 設備均未連線至網際網路。要實現這一點，您必須部署一個能夠存取網際網路的額外 Panorama 和一個 SCP 伺服器。在部署能夠存取網際網路的 Panorama 後，請設定連線網際網路的 Panorama 以自動下載內容更新到 SCP 伺服器。氣隙 Panorama 設定為根據內容更新排程從該 SCP 伺服器自動下載並安裝內容更新。當能夠存取網際網路的 Panorama 下載內容更新到 SCP 伺服器或當氣隙 Panorama 從 SCP 伺服器下載並安裝內容更新時，Panorama 會產生系統日誌。

僅支援從具有網際網路連線的 Panorama 到無網際網路連線的 Panorama 的以下內容更新排程：

在將內容更新檔案成功下載到 *SCP* 伺服器後，不要操縱或變更其名稱。*Panorama* 無法下載和安裝檔案名稱已修改的內容更新。此外，為成功完成自動內容更新，您必須確保 *SCP* 伺服器上有足夠的磁碟空間、準備開始下載時 *SCP* 伺服器正在執行，以及兩個 *Panorama* 均已開啟且不在重新啟動的過程中。

本範例顯示如何為應用程式和威脅內容更新設定自動內容更新。

STEP 1 | 部署 SCP 伺服器。

從連線到網際網路的 Panorama 下載受管理防火牆、日誌收集器和 WildFire 設備的內容更新。氣隙 Panorama 從 SCP 伺服器下載內容更新，然後將更新安裝在受管理防火牆、WildFire 設備和日誌收集器上。

為內容更新建立資料夾目錄時，最佳做法是為每種類型的內容更新各建一個資料夾。這是管理大量內容更新的負擔，減少了刪除不應從 *SCP* 伺服器刪除的內容更新的可能性。

STEP 2 | 部署連線到網際網路的 Panorama。

此 Panorama 與 Palo Alto Networks 更新伺服器進行通訊，並將內容更新下載到 SCP 伺服器。

1. 設定 Panorama 管理伺服器。
   - 設定 M-Series 設備
   - 設定 Panorama 虛擬設備
2. 執行初始 Panorama 設定。
   - 執行 M-Series 設備的初始設定
   - 執行 Panorama 虛擬設備的初始設定

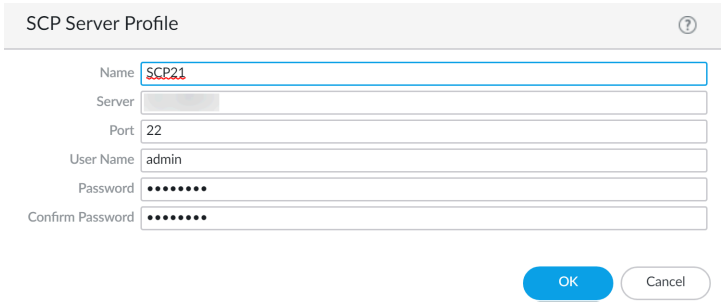
STEP 3 | 部署沒有網際網路連線的 Panorama。

此 Panorama 與 SCP 伺服器進行通訊，以在受管理防火牆、日誌收集器和 WildFire 設備上下載並安裝內容更新。

1. 設定 Panorama 管理伺服器。
   - 設定 M-Series 設備
   - 設定 Panorama 虛擬設備
2. 執行初始 Panorama 設定。
   - 執行 M-Series 設備的初始設定
   - 執行 Panorama 虛擬設備的初始設定
3. 新增受管理防火牆、日誌收集器和 WildFire 設備。
   - 將防火牆新增為受管理的裝置
   - 設定受管理收集器
   - 新增獨立 Wildfire 設備以便使用 Panorama 進行管理

STEP 4 | 設定連線到網際網路的 Panorama 以下載內容更新到 SCP 伺服器。

1. 登入 Panorama 網頁介面。
2. 建立 SCP 伺服器設定檔。
   1. 選取 **Panorama** > **Server Profiles**（伺服器設定檔） > **SCP**，並 **Add**（新增）新的 SCP 伺服器設定檔。
   2. 輸入 SCP 伺服器設定檔的描述性 **Name**（名稱）。
   3. 輸入 SCP **Server**（伺服器）IP 位址。
   4. 輸入 **Port**（連接埠）。
   5. 輸入 SCP 伺服器 **User Name**（使用者名稱）。
   6. 輸入 SCP 伺服器 **Password**（密碼）與 **Confirm Password**（確認密碼）。
   7. 按一下 **OK**（確定）儲存您的變更。

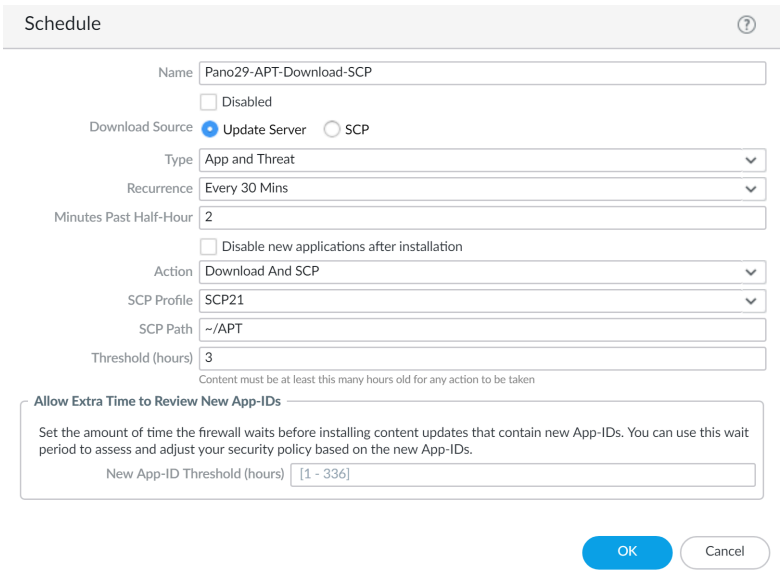


3. 建立內容更新排程以定期將內容更新下載到 SCP 伺服器。

   您必須為打算自動下載並安裝在受管理防火牆、日誌收集器和 WildFire 設備上的每種類型的內容更新建立排程。

   1. 選取 **Panorama** > **Device Deployment**（裝置部署） > **Dynamic Updates**（動態更新），選取 **Schedules**（排程），然後 **Add**（新增）內容更新排程。
   2. 為內容更新排程輸入描述性 **Name**（名稱）。
   3. 對於 **Download Source**（下載來源），選取 **Update Server**（更新伺服器）。
   4. 選取內容更新 **Type**（類型）。
   5. 選取 **Recurrence**（週期性）以設定 Panorama 在 Palo Alto Networks 更新伺服器上查看新內容更新的間隔。

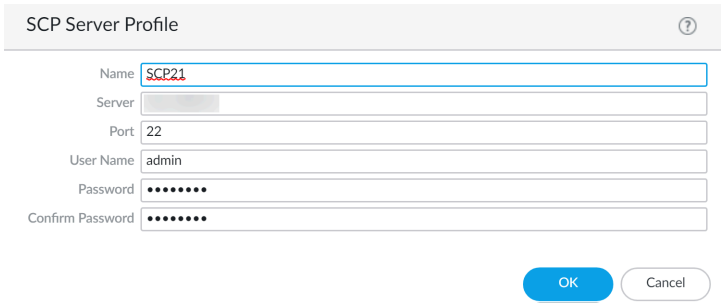
      要設定更精確的週期性排程，請輸入所選週期性間隔之後的分鐘數。如果您排程使用相同的週期性間隔下載多個內容更新，請交錯安排以免 *Panorama* 和 *SCP* 伺服器過載。
   6. 對於 **Action**（動作），選取 **Download And SCP**（下載和 **SCP**）。
   7. 選取您在上一步中設定的 **SCP Profile**（**SCP** 設定檔）。
   8. 輸入內容更新類型的 **SCP Path**（**SCP** 路徑）。
   9. （選用）輸入內容更新的 **Threshold**（閾值）（以小時為單位）。Panorama 僅下載達到此存在小時數（或更久）的內容更新
   10. 按一下 **OK**（確定）儲存您的變更。



4. **Commit**（提交）您的變更。

STEP 5 | 設定氣隙 Panorama 從 SCP 伺服器下載內容更新，然後將更新安裝在受管理防火牆、日誌收集器和 WildFire 設備上。

1. 登入 Panorama 網頁介面。
2. 建立 SCP 伺服器設定檔。
   1. 選取 **Panorama** > **Server Profiles**（伺服器設定檔） > **SCP**，並 **Add**（新增）新的 SCP 伺服器設定檔。
   2. 輸入 SCP 伺服器設定檔的描述性 **Name**（名稱）。
   3. 輸入 SCP **Server**（伺服器）IP 位址。
   4. 輸入 **Port**（連接埠）。
   5. 輸入 SCP 伺服器 **User Name**（使用者名稱）。
   6. 輸入 SCP 伺服器 **Password**（密碼）與 **Confirm Password**（確認密碼）。
   7. 按一下 **OK**（確定）儲存您的變更。



3. 建立內容更新排程，以定期從 SCP 伺服器下載並安裝內容更新。

   您必須為打算自動下載並安裝在受管理防火牆、日誌收集器和 WildFire 設備上的每種類型的內容更新建立排程。

   1. 選取 **Panorama** > **Device Deployment**（裝置部署） > **Dynamic Updates**（動態更新），選取 **Schedules**（排程），然後 **Add**（新增）內容更新排程。
   2. 為內容更新排程輸入描述性 **Name**（名稱）。
   3. 對於 **Download Source**（下載來源），選取 **SCP**。
   4. 選取您在上一步中設定的 **SCP Profile**（**SCP** 設定檔）。
   5. 輸入內容更新類型的 **SCP Path**（**SCP** 路徑）。
   6. 選取內容更新 **Type**（類型）。
   7. 選取 **Recurrence**（週期性）以設定 Panorama 在 Palo Alto Networks 更新伺服器上查看新內容更新的間隔。

      要設定更精確的週期性排程，請輸入所選週期性間隔之後的分鐘數。如果您排程使用相同的週期性間隔下載多個內容更新，請交錯安排以免 *Panorama* 和 *SCP* 伺服器過載。
   8. 對於 **Action**（動作），選取 **Download**（下載）或 **Download And Install**（下載並安裝）。

當 ***Download Source***（下載來源）為 ***SCP*** 時，僅支援 ***Download***（下載）和***Download and Install***（下載並安裝）。

如果您選取 ***Download***（下載），則必須手動在受管理防火牆上開始進行內容更新安裝。

9. 選取要安裝內容更新的 **Devices**（裝置）。
10. （選用）輸入內容更新的 **Threshold**（閾值）（以小時為單位）。Panorama 僅下載達到此存在小時數（或更久）的內容更新
11. 按一下 **OK**（確定）儲存您的變更。

4. **Commit**（提交）您的變更。

在 HA 設定中升級 Panorama

在高可用性 (HA) 設定中更新 Panorama 軟體時，為了確保容錯移轉順暢，主動和被動 Panorama 對等必須執行相同的 Panorama 版本及相同的應用程式資料庫版本。下列範例說明如何升級 HA 配對（主動對等為 Primary_A，被動對等為 Secondary_B）。

如果您要在 FIPS-CC 模式下將 Panorama 和受管理的裝置從 PAN-OS 10.2 或更早版本升級至 PAN-OS 11.1，且在執行 PAN-OS 10.2 版本時已新增至 Panorama 管理，則必須採取其他步驟在 FIPS-CC 模式下重設裝置的安全連線狀態。請參閱 在 FIPS-CC 模式下升級 Panorama 和受管理的裝置，瞭解關於在 FIPS-CC 模式下升級 Panorama 和 FIPS-CC 裝置的更多詳細資訊。

更新 Panorama 之前，請參閱版本資訊，瞭解 PAN-OS 11.0 所需的最低內容發行版本。

STEP 1 | 在 Secondary_B（被動）對等上升級 Panorama 軟體。

在 Secondary_B 對等上執行下列其中一項工作：

- 在具有網際網路連線的情況下升級 Panorama
- 在沒有網際網路連線的情況下升級 Panorama

升級後，此 Panorama 會轉變為非運作狀態，因為對等執行的軟體版本已不相同。

STEP 2 | （僅 Panorama Interconnect 外掛程式）同步 Panorama 節點與 Panorama 控制器。

開始升級 Panorama 節點之前，您必須同步 Panorama 控制器和 Panorama 節點設定。您必須這麼做才能在升級之後，成功將常見 Panorama 控制器設定推送到 Panorama 節點。

STEP 3 | （最佳做法）如果您正在使用 Cortex 資料湖 (CDL)，請在每個 Panorama HA 對等上安裝 Panorama 裝置憑證。

Panorama 會在升級至 PAN-OS 11.0 時自動切換至使用裝置憑證進行 CDL 擷取和查詢端點的驗證。

如果在升級至 *PAN-OS 11.0* 之前未安裝裝置憑證，*Panorama* 會繼續使用現有日誌記錄服務憑證進行驗證。

STEP 4 | 暫停 Primary_A 對等以強制容錯移轉。

在 Primary_A 對等上：

1. 在 **Operational Commands**（操作命令）部分中（**Panorama** > **High Availability**（高可用性）），**Suspend local Panorama**（暫停本機 **Panorama**）。
2. 確認狀態為 `suspended`（暫停）（顯示在網頁介面的右下角）。

   容錯移轉結果應該會使 Secondary_B 對等轉變為 `active`（主動）狀態。

STEP 5 | 在 Primary_A（主動）對等上升級 Panorama 軟體。

在 Primary_A 對等上執行下列其中一項工作：

- 在具有網際網路連線的情況下升級 Panorama
- 在沒有網際網路連線的情況下升級 Panorama

重新啟動後，Primary_A 對等最初仍然為被動狀態。接著，如果啟用先佔（預設值），Primary_A 對等會自動轉變為主動狀態，Secondary_B 對等會還原為被動狀態。

如果您已停用先佔，則手動將主要 Panorama 還原至主動狀態。

STEP 6 | 確認兩個對等現在都執行任何新安裝的內容發行版本，以及新安裝的 Panorama 版本。

在每個 Panorama 對等的 **Dashboard**（儀表板），檢查 Panorama 軟體版本和應用程式版本，並確認這些版本在兩個對等上都相同，且執行中的設定已同步。

STEP 7 | （僅在一個收集器群組內的本機日誌收集器）在收集器群組內升級剩餘日誌收集器。

- 當 Panorama 連線至網際網路時升級日誌收集器
- 當 Panorama 未連線至網際網路時升級日誌收集器

STEP 8 | （建議用於 Panorama 模式）將 Panorama 虛擬設備的記憶體增加至 64GB。

在 Panorama 模式下將 Panorama 虛擬設備成功升級至 PAN-OS 11.1 後，Palo Alto Networks 建議將 Panorama 虛擬設備的記憶體增加到 64GB 以滿足增加的系統要求，從而避免發生任何與佈建不足的 Panorama 虛擬設備相關的日誌記錄、管理和運作效能問題。

STEP 9 | 選取 **Commit**（提交）> **Commit and Push**（提交並推送）並 **Commit and Push**（提交並推送）Panorama 受管理設定至所有受管理裝置。

成功將 Panorama 和受管理裝置升級到 PAN-OS 11.1 之後，您需要先完全提交並推送 Panorama 受管理設定，才能將選擇性設定推送到您的受管理裝置，並善用 Panorama 管理的多重 vsys 防火牆的改良共用設定物件管理。

STEP 10 | （FIPS-CC 模式下的 Panorama 和受管理的裝置）在 FIPS-CC 模式下升級 Panorama 和受管理的裝置。

如果在執行 PAN-OS 11.1 版本時已新增至 Panorama 管理，則在 FIPS-CC 模式下升級 Panorama 與受管理的裝置時，必須在 FIPS-CC 模式下重設裝置的安全連線狀態。您需要將以下受管理裝置重新載入 Panorama 管理：

- 使用裝置註冊驗證金鑰在 FIPS-CC 模式下新增至 Panorama 的受管理裝置。
- 使用裝置註冊驗證金鑰在正常操作模式下新增至 Panorama 的受管理裝置

。當受管理的裝置執行 PAN-OS 10.0 或更早版本時，您無需重新裝載已新增至 Panorama 管理的受管理裝置。

STEP 11 | 重新產生或重新匯入所有憑證以遵守 OpenSSL 安全性等級 2。

如果您從 PAN-OS 10.1 或更早版本升級至 PAN-OS 11.1，則需要執行此步驟。如果您是從 PAN-OS 10.2 升級並且已經重新產生或重新匯入憑證，請略過此步驟。

要求所有憑證滿足以下最低要求：

- RSA 2048 位元或以上，或 ECDSA 256 位元或以上
- SHA256 或更高版本的摘要

有關重新產生或重新匯入憑證的更多資訊，請參閱 PAN-OS 管理員指南或 Panorama 管理員指南。

安裝 PAN-OS 軟體修補程式

這可在何處使用？	我需要哪些內容？
• 執行 PAN-OS 11.1.3 或更新版本的 Panorama	❑ 裝置管理授權 ❑ 支援授權 ❑ PAN-OS 11.1.3 或更新 11.1 版本 ❑ 輸出網際網路存取權

查看 PAN-OS 11.1 版本資訊，然後使用下列程序安裝 PAN-OS 軟體修補程式，以解決目前在 Panorama™ 管理伺服器上執行的 PAN-OS 版本錯誤及常見弱點和暴露 (CVE)。安裝 PAN-OS 軟體

修補程式時會套用錯誤和 CVE 的修正程式，而無需安排長時間進行維護，並可讓您立即強化安全狀態，避免引入任何新的已知問題或變更安裝新 PAN-OS 版本可能產生的預設行為。此外，您也可以復原目前安裝的軟體修補程式，以解除安裝軟體修補程式時套用的錯誤和 CVE 修正程式。

安裝或復原 PAN-OS 軟體修補程式時會產生系統日誌（**Monitor**（監控） > **Logs**（日誌） > **System**（系統））。必須有輸出網際網路連線才能從 Palo Alto Networks 客戶支援入口網站下載 PAN-OS 軟體修補程式。

- 安裝
- 還原

安裝

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Panorama** > **Software**（軟體）和 **Check Now**（立即檢查），從 Palo Alto Networks 更新伺服器檢索最新的 PAN-OS 軟體修補程式。

STEP 3 | 選取（啟用）**Include Patch**（包含修補程式）以顯示所有可用的 PAN-OS 軟體修補程式。

STEP 4 | 尋找目前安裝在 Panorama 上的 PAN-OS 版本的軟體修補程式。

軟體修補程式由 **Version**（版本）名稱旁邊顯示的修補程式標籤表示。

STEP 5 | 查看 **More Info**（更多資訊），以檢視軟體修補程式詳細資訊，例如重要錯誤和 CVE 修正程式，以及是否需要重新啟動新世代防火牆才能套用修正項目。

STEP 6 | **Download**（下載）軟體修補程式。

（僅 HA）選取（啟用）同步至 HA 對等並 **Continue Download**（繼續下載）以下載 PAN-OS 軟體修補程式。

軟體修補程式下載成功後按一下 **Close**（關閉）。

STEP 7 | **Install**（安裝）軟體修補程式。

軟體修補程式安裝成功後，按一下 **Close**（關閉）。

STEP 8 | **Apply**（套用）軟體修補程式。

當系統提示您確認要將已安裝的 PAN-OS 軟體修補程式套用到 Panorama 時，請按 **Apply**（套用）。

系統將顯示狀態欄，顯示 PAN-OS 軟體修補程式應用程式的目前進度。修補程式成功套用後，按一下 **Close**（關閉）。

此時如果需要重新啟動才能將 PAN-OS 軟體修補程式套用到 Panorama，則 Panorama 會自動重新啟動。

STEP 9 | （僅 HA）在 Panorama HA 對等上安裝 PAN-OS 軟體修補程式。

1. 登入 HA 對等的 Panorama 網頁介面。
2. 選取 **Panorama** > **Software**（軟體）**Check Now**（立即檢查）。
3. **Install**（安裝）軟體修補程式。
4. 如果需要，請重新啟動 Panorama。

還原

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Panorama** > **Software**（軟體）並找到您要還原的 PAN-OS 軟體修補程式。

STEP 3 | **Revert**（還原）軟體修補程式。

當系統提示您確認要還原安裝在 Panorama 的 PAN-OS 軟體修補程式時，請按 **Revert**（還原）。

系統將顯示狀態欄，顯示 PAN-OS 軟體修補程式應用程式的目前進度。修補程式成功套用後，按一下 **Close**（關閉）。

此時如果需要重新啟動才能將 PAN-OS 軟體修補程式套用到 Panorama，則防火牆會自動重新啟動。

將 Panorama 日誌移轉為新的日誌格式

升級至 Panorama 8.0（或更新）版本之後，Panorama 日誌收集器會使用新的日誌儲存格式。因為 Panorama 在升級之後無法從 8.0 版以前日誌格式的日誌產生報告或 ACC 資料，當您將 Panorama 及其日誌收集器從 PAN-OS® 7.1 或更舊版本升級至 PAN-OS 8.0 或更新版本時，您必須盡快移轉現有的日誌，而且必須在升級受管理的防火牆之前這樣做。Panorama 在日誌移轉期間會繼續從受管理的裝置收集日誌，但在您升級至 PAN-OS 8.0 或更新版本之後，將會以新的日誌格式儲存傳入的日誌。因此，在 Panorama 完成日誌移轉程序之前，您在 ACC 和報告中只會看到局部資料。

將日誌移轉至新格式是一次性工作，必須在升級至 *PAN-OS 8.0* 或更新版本（或當您升級至 *PAN-OS 8.0* 作為升級路徑的一部分）時執行；在升級至更新的 *PAN-OS* 版本時不需要再一次執行此移轉。

Panorama 完成日誌移轉程序所需的時間，取決於寫入 Panorama 的新日誌數量，以及您要移轉的日誌資料庫大小。因為日誌移轉是很耗用 CPU 的程序，請在日誌記錄速率較低的期間才開始移轉。如果在尖峰期間發現 CPU 使用率很高，您一律可以停止移轉，等到傳入日誌速率較低時再繼續移轉。

在安裝 Panorama 內容和軟體更新 和升級日誌收集器之後，請如下移轉日誌：

檢視進入日誌記錄速率。

最佳作法是在傳入日誌速率較低時開始日誌移轉。若要檢查速率，請從日誌收集器 CLI 執行下列命令：

```
admin@FC-M500-1> debug log-collector log-collection-stats show
 incoming-logs
```

在日誌移轉期間，*CPU* 使用率通常很高（接近 *100%*），操作會繼續正常運作。在資源競用的情況下，日誌移轉會調節以利於傳入日誌和其他程序。

開始將每個日誌收集器上的日誌移轉為新格式。

若要開始移轉，請從每個日誌收集器的 CLI 輸入下列命令：

```
admin@FC-M500-1> request logdb migrate lc serial-number <ser_num>
 start
```

檢視日誌移轉狀態，以估計將所有現有日誌移轉為新格式所需的時間。

```
admin@FC-M500-1> request logdb migrate lc serial-number <ser_num>
 status Slot: all Migration State:In Progress Percent Complete:0.04
 Estimated Time Remaining:451 hour(s) 47 min(s)
```

停止日誌移轉程序。

若要暫時停止日誌移轉程序，請從日誌收集器 CLI 輸入下列命令：

```
admin@FC-M500-1 request logdb migrate lc serial-number <ser_num>
 stop
```

為增加的設備管理容量升級 Panorama

升級至 PAN-OS 9.1 或更高版本，以使用 M-600 設備上現有的裝置管理授權，管理多至 5,000 個防火牆，或使用 Panorama™ 虛擬設備管理多至 2,500 個防火牆。

STEP 1 | 如果 Panorama 虛擬設備已無法滿足所增加裝置管理的最低資源需求，則增加 Panorama 虛擬設備的 CPU 和記憶體。

升級前，請檢閱增加的裝置管理容量需求，以確認您現有的 Panorama 虛擬設備是否滿足最低資源需求。

STEP 2 | 登入 Panorama CLI。

STEP 3 | 變更 Panorama 管理伺服器至 Management Only（僅限管理）模式（如果 Panorama 未處於此模式下）。

- （僅限 M-600 設備）從步驟 5 開始，以在僅管理模式下設定 M-Series 設備。

或

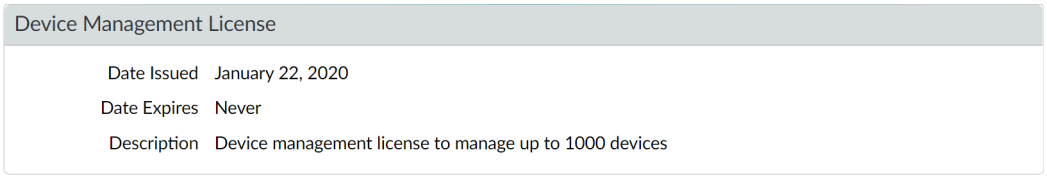
- 在僅管理模式下設定 Panorama 虛擬設備。

STEP 4 | 登入 Panorama 網頁介面。

STEP 5 | 升級 Panorama 管理伺服器。

- 在具有網際網路連線的情況下升級 Panorama。
- 在沒有網際網路連線的情況下升級 Panorama。
- 在 HA 設定中升級 Panorama.

STEP 6 | 選取 **Panorama** > **Licenses**（授權），確認已成功啟動裝置管理授權。



如果您已啟動您的裝置管理授權并接著升級至 *PAN-OS 9.1* 或更高版本，您可以用 *M-600* 設備管理多至 *5,000* 個防火牆，或用 *Panorama* 虛擬設備管理多至 *2,500* 個防火牆，但說明仍然顯示 *`Device management license to manage up to 1000 devices or more`*（裝置管理授權管理多至 *`1000`* 部裝置或更多）。

在 FIPS-CC 模式下升級 Panorama 和受管理的裝置

成功升級到 PAN-OS 11.1 後，FIPS-CC 模式下的所有受管理的裝置以及在裝置執行 PAN-OS 10.0 或更舊版本時新增至 Panorama 的任何受管理的裝置都必須重新裝載至 Panorama 管理。這需要您為 FIPS-CC 模式下的 Panorama 和 FIPS-CC 模式下任何受管理的裝置重設安全連線狀態。重設安全連線狀態後，您必須使用裝置註冊驗證金鑰將新增至 Panorama 的防火牆、日誌收集器和 WildFire 設備新增回 Panorama 管理。在執行 PAN-OS 10.0 或更早版本時，無需進行此過程，也不會影響新增至 Panorama 的受管理的裝置。這對於 FIPS-CC 模式下的所有受支援的 Panorama 型號和新世代防火牆硬體及 VM-Series 型號都是必需的。

STEP 1 | 使用裝置註冊驗證金鑰建立 FIPS-CC 模式下的受管理的裝置及任何新增至添 Panorama 的受管理的裝置清單。這將幫助您稍後在將受管理的裝置重新裝載至 Panorama 管理時集中精力。

STEP 2 | 將 Panorama 和受管理的裝置升級到 PAN-OS 11.1。

- 在具有網際網路連線的情況下升級 Panorama
- 在沒有網際網路連線的情況下升級 Panorama
- 在 HA 設定中升級 Panorama

STEP 3 | 成功升級到 PAN-OS 11.1 後，檢閱 Panorama 上的系統日誌，以確定 FIPS-CC 模式下哪些受管理的裝置無法連線至 Panorama。

STEP 4 | 在 Panorama 上重設安全連線狀態。

此步驟會重設在執行 PAN-OS 11.1 版本時新增至 Panorama 管理的任何受管理的裝置連線，並且無法還原。此步驟對執行 PAN-OS 10.0 或升級到 PAN-OS 11.1 的更早版本時新增的防火牆的連線狀態沒有影響。

1. 登入 Panorama CLI。
2. 重設安全連線狀態。

```
admin> request sc3 reset
```

3. 在 Panorama 上重新啟動管理伺服器。

```
admin> debug software restart process management-server
```

4. （僅限 HA）對高可用性 (HA) 設定中的每個對等重複此步驟。

STEP 5 | 在 FIPS-CC 模式下重設受管理的裝置上的安全連線狀態。

此步驟會重設受管理的裝置連線，且無法還原。

1. 登入受管理裝置 CLI。
   - 登入防火牆 CLI
   - 登入日誌收集器 CLI
   - 登入 WildFire 設備 CLI
2. 重設安全連線狀態。

```
admin> request sc3 reset
```

3. 重新啟動受管理裝置上的管理伺服器。

```
admin> debug software restart process management-server
```

STEP 6 | 將受影響的受管理的裝置新增回 Panorama。

- 將防火牆新增為受管理的裝置
- 設定受管理收集器
- 新增獨立 WildFire 設備給 Panorama 管理

STEP 7 | 重新產生或重新匯入所有憑證以遵守 OpenSSL 安全性等級 2。

在升級到 PAN-OS 11.1 時，要求所有憑證滿足以下最低要求：

- RSA 2048 位元或以上，或 ECDSA 256 位元或以上
- SHA256 或更高版本的摘要

請參閱 PAN-OS 管理員指南或 Panorama 管理員指南，瞭解有關重新產生或重新匯入憑證的更多資訊。

從 Panorama 11.1 降級

PAN-OS® 11.1 引入了進階威脅防護支援，以實現零時差入侵防護，其利用內嵌深度學習，簡化了 Panorama 和受管理裝置的軟體升級與降級，以減少跨多個 PAN-OS 版本升級受管理裝置的運作負擔，使用 AIOps 主動最佳做法評估 (BPA) 可進一步消除安全狀態受損帶來的風險，內部部署 Web Proxy 有助於在不犧牲安全性或效率的情況下移轉至雲端，防火牆支援具狀態 DHCPv6 用戶端取得 IPv6 位址，增強了雲端識別引擎 (CIE) 使用者內容的可視性，對管理存取的 TLSv1.3 支援，以及增強了 IoT 安全性政策規則建議，以便更輕鬆地擴展和管理政策規則建議。使用以下工作流程在降級日誌收集器和執行 Panorama 11.1 版的 Panorama 至更舊的功能版本之前，先降級防火牆。對於管理本機日誌收集器的 Panorama 與管理一個或多個專用日誌收集器的 Panorama，此程序都適用。

若要從 *PAN-OS 11.1* 降級至更早的 *PAN-OS* 版本，您必須下載並安裝慣用的 *PAN-OS 11.0* 或更高的 *PAN-OS 11.0* 版本，然後才能繼續降級至目標 *PAN-OS* 版本。如果您嘗試降級至 *PAN-OS 10.2* 或更早的 *PAN-OS* 版本，則從 *PAN-OS 11.0* 降級會失敗。

檢閱 Palo Alto Networks 相容性矩陣，確認您想要降級的防火牆和設備相容於您想要降級的 *PAN-OS* 發佈版本。對於您可以降級的防火牆和設備，您也應該檢閱 升級/降級考量事項，以確保您瞭解降級之後會不同或無法使用的所有功能和組態設定。

執行 *PAN-OS 11.1* 時產生的日誌不相容於 *PAN-OS 11.0* 和更舊版本，會在降級時遭刪除。若要保留執行 *PAN-OS 11.1.1* 或 *PAN-OS 11.1.0* 時產生的日誌，您必須先升級至 *PAN-OS 11.1.2*，然後才開始降級至目標 *PAN-OS* 版本。如果要在降級後成功復原 *PAN-OS 11.1* 產生的日誌就必須這麼做。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 為 Panorama 和受管理裝置儲存設定檔案備份。

1. **Export Panorama and device configuration snapshot**（匯出 **Panorama** 和裝置組態快照）（**Panorama** > **Setup**（設定） > **Operations**（操作））。
2. 將匯出的 .tgz 檔案儲存至 Panorama、日誌收集器和防火牆外部的位置。如果發生問題而必須重來，您可以使用此備份來還原設定。

STEP 3 | 如果您為專用日誌收集器設定了驗證，且移除了 `admin` 管理員，請設定新的 `admin` 使用者並推送到您的專用日誌收集器。

專用日誌收集器必須設定 `admin` 使用者才可降級至 PAN-OS 9.1 和更早版本。

STEP 4 | 選取 **Panorama** > **Plugins**（外掛程式） 並為目前 Panorama 上安裝的所有外掛程式 **Download**（下載）PAN-OS 11.0 支援的外掛程式版本。

有關 PAN-OS 11.0 和更早版本支援的 Panorama 外掛程式版本，請參閱 Panorama 外掛程式相容性矩陣。

需要執行此步驟以成功地將 Panorama 從 PAN-OS 11.1 降級至 PAN-OS 11.0 和更早版本。下載的外掛程式版本會在降級至 PAN-OS 11.0 期間自動安裝。如果未下載支援的外掛程式版本，將封鎖降級至 PAN-OS 11.0。

（僅限 *ZTP* 外掛程式）若要成功將 *Panorama* 降級至 *PAN-OS 11.0*，您必須在開始降級過程之前解除安裝 ZTP 外掛程式。成功降級至 *PAN-OS 11.0* 後，您必須在 *Panorama* 上重新安裝 *ZTP* 外掛程式。

STEP 5 | 降級每個執行 PAN-OS 11.1 的防火牆。

如果要從 *PAN-OS 11.1* 降級至舊版功能，您必須先降級至慣用的 *PAN-OS 11.0* 版本或更高的 *PAN-OS 11.0* 版本。成功降級至慣用的 *PAN-OS 11.0* 或更高的 *PAN-OS 11.0* 版本後，您可以繼續降級至目標 *PAN-OS* 版本。

如果降級一個以上的防火牆，請先將防火牆特定的每個 *PAN-OS 11.0* 映像下載至 *Panorama* 再開始降級，讓過程順暢進行。例如，若要將 *PA-220* 防火牆降級至 *PAN-OS 11.0*，請下載 *`PanOS_220-11.0.0`* 或 *`PanOS_3000-11.0.0`* 映像。

Panorama 要求所有防火牆必須執行相同或更舊的 PAN-OS 版本。因此，請根據您的環境，使用並重複下列適當的工作，將所有受管理的防火牆降級之後，您才能降級 Panorama：

1. **Check Now**（立即檢查）有無可用的映像（**Panorama** > **Device Deployment**（裝置） > **Software**（軟體））。

   （PAN-OS 11.1.3 及更新版本）根據預設，系統會顯示慣用版本和相應的基礎版本。若要僅查看慣用版本，請停用（清除）**Base Releases**（基礎版本）核取方塊。同理，若要僅查看基礎版本，請停用（清除）**Preferred Releases**（管用版本）核取方塊。
2. 針對您想要降級的每個防火牆型號或系列，尋找 PAN-OS 11.0 映像。如果尚未下載映像，請 **Download**（下載）。

非 **HA** 防火牆

Install（安裝）（動作欄）適當的 PAN-OS 11.0 版本，選取您想要降級的所有防火牆，再選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 **OK**（確定）。

主動/主動 **HA** 防火牆

1. 按一下 **Install**（安裝），停用（清除）**Group HA Peers**（群組 **HA** 對等），選取任一 HA 對等，選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 **OK**（確定）。繼續之前，等候防火牆完成重新開機。
2. 按一下 **Install**（安裝），停用（清除）**Group HA Peers**（群組 **HA** 對等），選取您在上一步未更新的 HA 對等、選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 **OK**（確定）。

主動/被動 **HA** 防火牆

在此範例中，主動防火牆名為 fw1，被動防火牆名為 fw2：

1. **Install**（安裝）（動作欄）適當的更新，停用（清除）**Group HA Peers**（群組 **HA** 對等），選取 fw2，選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 **OK**（確定。
2. 當 fw2 完成重新開機後，向 fw1 確認（**Dashboard**（儀表板） > **High Availability**（高可用性）Widget）仍然是主動對等，且 fw2 仍然是被動對等（Local（本機）防火牆狀態為 `active`（主動），Peer（對等）-fw2 為 `passive`（被動））。
3. 存取 fw1 和 **Suspend local device**（暫停本機裝置）（**Device**（裝置） > **High Availability**（高可用性） > **Operational Commands**（操作命令））。

4. 存取 fw2（**Dashboard**（儀表板） > **High Availability**（高可用性）），確認 Local（本機）防火牆狀態 `active`（主動），Peer（對等）防火牆—fw1—為 `suspended`（暫停）。
5. 存取 Panorama，選取 **Panorama** > **Device Deployment**（裝置部署） > **Software**（軟體） **Install**（安裝）（操作欄）適當更新，停用（清除）**Group HA Peers**（群組 **HA** 對等），選取 fw1，選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 **OK**（確定）。繼續之前，等候 fw1 完成重新開機。
6. 存取 fw1（**Dashboard**（儀表板） > **High Availability**（高可用性）Widget），確認 Local（本機）防火牆狀態為 `passive`（被動），Peer（對等）(fw2) 為 `active`（主動）。

   如果在 *Election*（選取）設定中啟用先佔（***Device***（裝置） > ***High Availability***（高可用性） > ***General***（一般）），*fw1* 在重新開機之後會恢復為主動對等。

STEP 6 | 降級每個執行 Panorama 11.0 的日誌收集器。

如果要從 *PAN-OS 11.1* 降級至舊版功能，您必須先降級至慣用的 *PAN-OS 11.0* 或更高的 *PAN-OS 11.0* 版本。成功降級至慣用的 *PAN-OS 11.0* 或更高的 *PAN-OS 11.0* 版本後，您可以繼續降級至目標 *PAN-OS* 版本。

1. 登入日誌收集器 CLI 並刪除所有 `esdata` 目錄。

   `admin>` **`debug elasticsearch erase`** 資料

   針對您要降級的收集器群組中的所有日誌收集器重複此步驟。
2. **Check Now**（立即檢查）有無可用的映像（**Panorama** > **Device Deployment**（裝置） > **Software**（軟體））。

   （PAN-OS 11.1.3 及更新版本）根據預設，系統會顯示慣用版本和相應的基礎版本。若要僅查看慣用版本，請停用（清除）**Base Releases**（基礎版本）核取方塊。同理，若要僅查看基礎版本，請停用（清除）**Preferred Releases**（管用版本）核取方塊。
3. 尋找 PAN-OS 11.0 映像。如果尚未下載映像，請 **Download**（下載）（Action（動作）欄）。
4. 下載完成之後，將映像 **Install**（安裝）在每個執行 11.1 的日誌收集器上。選取 **Reboot device after install**（安裝後重新啟動裝置），可在升級完成之後自動重新啟動裝置。

STEP 7 | 降級 Panorama。

如果要從 *PAN-OS 11.1* 降級至舊版功能，您必須先降級至慣用的 *PAN-OS 11.0* 或更高的 *PAN-OS 11.0* 版本。成功降級至慣用的 *PAN-OS 11.0* 或更高的 *PAN-OS 11.0* 版本後，您可以繼續降級至目標 *PAN-OS* 版本。

1. （僅 Panorama 模式）登入 Panorama CLI 並刪除所有 `esdata` 目錄。

   `admin>` **`debug elasticsearch erase`** 資料

2. 登入 Panorama 網頁介面，選取 **Panorama** > **Software**（軟體），然後**Check Now**（立即檢查）可用的映像。

   （PAN-OS 11.1.3 及更新版本）根據預設，系統會顯示慣用版本和相應的基礎版本。若要僅查看慣用版本，請停用（清除）**Base Releases**（基礎版本）核取方塊。同理，若要僅查看基礎版本，請停用（清除）**Preferred Releases**（管用版本）核取方塊。

3. 尋找目標 PAN-OS 映像。如果尚未下載映像，請 **Download**（下載）。
4. 下載完成之後，將映像 **Install**（安裝）在 Panorama 上。
5. 按照下列方式重新啟動 Panorama：
   - 如果提示您重新啟動，請按一下**Yes**（是）。如果您看到 **CMS Login**（**CMS** 登入）提示，請按下 Enter，無須鍵入使用者名稱或密碼。當 Panorama 登入提示出現時，請輸入您在初始設定期間設定的使用者名稱與密碼。
   - 如果未提示重新啟動，請選取**Panorama** > **Setup**（設定） > **Operations**（操作），然後按一下 **Reboot Panorama**（重新啟動 **Panorama**）（裝置操作）。

STEP 8 | （僅限 ZTP 外掛程式）重新安裝 ZTP 外掛程式。

1. 登入 Panorama 網頁介面。
2. 安裝 ZTP 外掛程式。
3. 選取 **Panorama** > **Zero Touch Provisioning**（零接觸佈建）並核取（啟用）**ZTP**。

STEP 9 | （僅限企業 DLP） 編輯企業 DLP 資料篩選設定以將 **Max File Size**（最大檔案大小）減小到 20MB 或以下。

從企業 DLP 4.0.1 或更新版本的 Panorama 外掛程式降級時必須這麼做。企業 DLP 4.0.1 及更新版本支援大型檔案大小檢查。

STEP 10 | （僅企業 DLP）同步 Panorama 上的企業 DLP 資料篩選設定檔與 DLP 雲端服務。

您必須這麼做才能將 Panorama 從 PAN-OS 11.0.2 和企業 DLP 外掛程式 4.0.1 降級為 PAN-OS 11.0.1 或更舊的 11.1 版本和企業 DLP 外掛程式 4.0.0。

1. 登入 Panorama CLI。
2. 將企業 DLP 設定從 Panorama 推送到 DLP 雲端服務。

   ```
   admin> 要求外掛程式 DLP push-dlp-config
   ```

3. 重新設定企業 DLP 外掛程式。

   ```
   admin> 要求外掛程式 DLP 重設
   ```

4. 在 Panorama 上提交並使用企業 DLP 推送到受管理防火牆。
   1. 登入 Panorama 網頁介面。
   2. 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**）並 **Commit**（提交）。
   3. 選取 **Commit**（提交） > **Push to Devices**（推送至裝置）並 **Edit Selections**（編輯選擇）。
   4. 選取 **Device Groups**（裝置群組），以及 **Include Device and Network Templates**（包括裝置和網路範本）。
   5. 按一下 **OK**（確定）。
   6. 透過企業 DLP **Push**（推送）您的受管理防火牆設定變更。

STEP 11 | 登入 Panorama CLI 並復原 PAN-OS 11.1 產生的日誌。

```
admin> debug logdb migrate-lc start log-type all
```

若要檢視日誌移轉的狀態：

```
admin> debug logdb migrate-lc status
```


對您的 Panorama 升級進行疑難排解

要對您的 Panorama 升級進行疑難排解，請使用下表來檢閱可能的問題以及如何解決這些問題。

徵兆	解析度
軟體保固授權已過期。	從 CLI 中，刪除過期的授權金鑰： 1. 輸入 **delete license key <software license key>**。 2. 輸入 **delete license key Software_Warranty<expiredate>.key**。
最新的 PAN-OS 軟體版本不可用。	您只能看到先於當前安裝版本一個功能版本的軟體版本。例如，如果您安裝了 8.1 版本，則只有 9.0 版本可供您使用。若要查看 9.1 版本，您必須先升級至 9.0。
（僅適用於舊版模式中的 Panorama 虛擬設備）升級版本未能預先載入軟體管理員。	當沒有足夠的資源可用時，就會發生這個問題。您可以增加虛擬機器容量，也可以從舊版模式移轉至 Panorama 模式。

使用 Panorama 將升級部署至防火牆、日誌收集器和 WildFire 設備

您可以先將軟體和內容更新部署到一部分的防火牆、專用日誌收集器或 WildFire® 裝置和設備叢集，並使用 Panorama™ 來證明這些更新有用，然後才更新安裝在其餘的受管理的設備上。Panorama 需要直接的網際網路連線，您才能為定期的內容更新進行排程。若要依需求（非排程）部署軟體或內容更新，程序會根據 Panorama 是否連線至網際網路而有所不同。如果您在排程更新程序已開始或排程在五分鐘內開始時手動部署內容更新，Panorama 會顯示警告。

部署更新時，Panorama 會向受管理的設備（防火牆、日誌收集器和 WildFire 設備）通知有更新可用，裝置就會從 Panorama 擷取更新套件。依預設，受管理的設備會透過 Panorama 上的管理 (MGT) 介面擷取更新。不過，如果您要讓裝置使用另一個介面擷取更新，以降低 MGT 介面的流量負載，您可以設定 Panorama 來使用多個介面。

您可以使用 Panorama 快速將一個或多個防火牆的內容版本還原為之前安裝的內容版本。在新內容版本安裝於防火牆之後，如果新安裝的內容版本不穩定或甚至干擾了網路運作，您可以還原回之前安裝的版本。

依預設，您最多可將每個類型的兩個軟體或內容更新下載至 *Panorama*。當您開始任何超過該上限的下載時，*Panorama* 會刪除所選類型最舊的更新。若要變更該上限，請參閱 管理 Panorama 儲存軟體與內容更新。

- Panorama 可以將哪些更新推送至其他裝置？
- Panorama、日誌收集器、防火牆和 WildFire 版本相容性
- 使用 Panorama 排程內容更新
- 當 Panorama 連線至網際網路時升級防火牆
- 當 Panorama 未連線至網際網路時升級防火牆
- 當 Panorama 連線至網際網路時升級日誌收集器
- 當 Panorama 未連線至網際網路時升級日誌收集器
- 在有網際網路連線的情況下從 Panorama 升級 WildFire 叢集
- 在沒有網際網路連線的情況下從 Panorama 升級 WildFire 叢集
- 升級 ZTP 防火牆
- 安裝 PAN-OS 軟體修補程式
- 從 Panorama 復原內容更新

Panorama 可以將哪些更新推送至其他裝置？

您可以安裝的軟體與內容更新，根據各防火牆、日誌收集器及 WildFire® 設備和設備叢集上有哪些作用中的訂閱而異：

設備類型	軟體更新	內容更新
日誌收集器	Panorama™	應用程式（日誌收集器不需要威脅簽章） 防毒軟體 WildFire®
防火牆	PAN-OS® GlobalProtect™ 代理程式/應用程式	應用程式 應用程式與威脅 防毒軟體 WildFire
WildFire	PAN-OS VM 映像	WildFire

使用 Panorama 排程內容更新

Panorama™ 需要直接的網際網路連線，才能在防火牆、日誌收集器及 WildFire® 設備和設備叢集上排程支援的更新。如果沒有，您可以只執行依需求更新。（若要排程日誌收集器的防毒、WildFire 或 BrightCloud URL 更新，日誌收集器必須執行 Panorama 7.0.3 或更新版本。）每個接收更新的防火牆、日誌收集器或 WildFire 設備或設備叢集都會產生日誌，以指出安裝成功（設定日誌）或失敗（系統日誌）。若要在 Panorama 管理伺服器上排程更新，請參閱為有網際網路連線的 Panorama 安裝更新。

在部署更新之前，請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性，瞭解關於內容發行版本相容性的重要資訊。參考版本資訊，瞭解您必須為 *Panorama* 版本安裝的最低內容版本。

Panorama 一次只能下載一個相同類型的更新。如果您將同一類型的多個更新排程在「週期性」下的同一時間下載，則只有第一次下載成功。

如果您的防火牆直接連線至 *Palo Alto Networks*® 更新伺服器，您還可以使用 *Panorama* 範本（***Device*** （裝置） **> *Dynamic Updates*** （動態更新））將內容更新排程推送至防火牆。如果您想在更新發佈後延遲一段時間再安裝，您必須使用範本部署排程。在極少數的情況下，內容更新會包含錯誤；指定延遲可讓 *Palo Alto Networks* 更有機會發現這種更新，並從更新伺服器中移除，以免被防火牆安裝。

針對每個您想要排程的更新類型執行下列步驟。

STEP 1 | 選取 **Panorama** > **Device Deployment**（裝置部署） > **Dynamic Updates**（動態更新），按一下 **Schedules**（排程），然後 **Add**（新增） 排程。

STEP 2 | 指定 **Name**（名稱）（用於識別排程）、更新 **Type**（類型），以及更新頻率（**Recurrence**（週期性））。頻率選項取決於更新 **Type**（類型）。

PAN-OS® 使用 *Panorama* 時區來排程更新。

如果您將 **Type**（類型）設定為 **App and Threat**（應用程式與威脅），日誌收集器都只需要並且只會安裝應用程式內容，而不會安裝威脅內容。防火牆則會同時使用應用程式和威脅內容。請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。

STEP 3 | 從以下排程動作中選取一個，然後選取防火牆或日誌收集器：

- **Download And Install**（下載並安裝）（最佳作法）—選取 **Devices**（裝置）（防火牆）、**Log Collectors**（日誌收集器）或 **WildFire Appliances and Clusters**（**WildFire** 設備和叢集）。
- **Download Only**（僅下載）—Panorama 會下載更新，但不安裝。

STEP 4 | 按一下 **OK**（確定）。

STEP 5 | 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。

Panorama、日誌收集器、防火牆和 WildFire 版本相容性

為了得到最佳結果，請遵守下列 Panorama™ 相容性方針：

- 在 Panorama 管理伺服器和專用日誌收集器上安裝相同的 Panorama 版本。
- Panorama 必須執行與其管理的防火牆相同或更新的 PAN-OS 版本。請參閱 Panorama 管理相容性，瞭解詳細資訊。

  在將防火牆升級到 PAN-OS 11.0 前，您必須先升級 Panorama 至 11.0。
- 專用日誌收集器必須執行與受管理防火牆轉送日誌相同或更新版本的 PAN-OS 版本。
- 執行 PAN-OS 11.1 的 Panorama 可以管理執行相同或更舊 PAN-OS 版本的 WildFire® 設備和 WildFire 設備叢集。請參閱 Panorama 管理相容性，瞭解詳細資訊。

  建議 Panorama 管理伺服器、Wildfire 設備和 Wildfire 設備叢集執行相同的 PAN-OS 版本。
- Panorama 管理伺服器上的內容發行版本，與任何專用日誌收集器和受管理防火牆上的內容發行版本相比，必須是相同（或更舊）版本。請參閱 Panorama 管理相容性，瞭解詳細資訊。

Palo Alto Networks® 建議在 *Panorama* 上安裝與專用日誌收集器和防火牆上相同的「應用程式」資料庫版本。

無論您的訂閱包含「應用程式」資料庫還是「應用程式與威脅」資料庫，Panorama 都只會安裝「應用程式」資料庫。Panorama 和專用日誌收集器不會執行原則規則，因此不需要「威脅」資料庫中的威脅特徵碼。「應用程式」資料庫中包含了當您在定義原則規則以推送至受管理防火牆以及在判讀日誌和報告中的威脅資訊時，可以在 Panorama 和專用日誌收集器上使用的威脅中繼資料（例如威脅 ID 和名稱）。不過，防火牆需要完整的「應用程式與威脅」資料庫，才能將日誌中記錄的識別碼，與對應的威脅、URL 或應用程式名稱進行比對。請參閱版本資訊，瞭解 Panorama 版本所需的最低內容發行版本。

當 Panorama 連線至網際網路時升級日誌收集器

如需可在日誌收集器上安裝的軟體和內容更新清單，請參閱 支援的更新 。

如果您是從 *PAN-OS 8.1* 升級，*PAN-OS 9.0* 會為本機和專用日誌收集器引入新的記錄資料格式。在升級到 *PAN-OS 10.1* 的路徑上，當您從 *PAN-OS 8.1* 升級到 *PAN-OS 9.0* 時，現有日誌資料會自動移轉至新的日誌資料格式。

您必須同時在收集器群組內升級所有日誌收集器，以避免丟失日誌資料。如果收集器群組內的日誌收集器並非執行相同的 PAN-OS 版本，則無法進行日誌轉送或日誌收集。此外，除非所有日誌收集器執行相同的 PAN-OS 版本，否則收集器群組內的日誌收集器日誌資料在 **ACC** 或 **Monitor**（監控器）頁籤內不可見。例如，如果您在收集器群組內有三個日誌收集器，且您升級了其中兩個，則不會有日誌被轉送至收集器群組內的任何日誌收集器。

Palo Alto Networks 建議您在維護時段升級日誌收集器。由於日期格式的轉移，整個升級程序需要額外花費數個小時，具體取決於本機和專用日誌收集器上的日誌資料量。

STEP 1 | 升級日誌收集器之前，請確定您在 Panorama 管理伺服器上是執行適當的 Panorama™ 軟體版本。

Palo Alto Networks® 高度建議 *Panorama* 和日誌收集器執行相同的軟體發行版本，而且 *Panorama*、日誌收集器和所有受管理的防火牆也都執行相同的內容發行版本。如需瞭解重要軟體和內容相容性的詳細資訊，請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。

Panorama 執行的軟體版本必須與日誌收集器相同（或更新），但必須具有相同或更新的內容發行版本：

- 軟體發行版本—如果 Panorama 管理伺服器執行的軟體版本，與您想要更新的日誌收集器不是相同或更新的版本，則在更新任何日誌收集器之前，您必須先將相同或更新的 Panorama 版本安裝在 Panorama 上（請參閱 安裝 Panorama 的內容更新和軟體升級）。
- 內容發行版本—在內容發行版本方面，您應該確定所有日誌收集器都執行最新的內容發行版本，或執行的版本至少比 Panorama 上正在執行的版本還要新；否則，請先將防火牆從 Panorama 升級至 PAN-OS 11.1，再更新日誌收集器，然後才在 Panorama 管理伺服器上更新內容發行版本。

檢查軟體和內容版本：

- **Panorama** 管理伺服器—若要查明 Panorama 管理伺服器上執行的軟體和內容版本，請登入 Panorama 網頁介面並移至 General Information（一般資訊）設定（**Dashboard**（儀表板））。
- 日誌收集器 —若要查明日誌收集器上執行的軟體和內容版本，請登入每個日誌收集器的 CLI 並執行 **`show system info`** 命令。

STEP 2 | 在網路上啟用以下 TCP 連接埠。

您必須在網路上啟用這些 TCP 連接埠，才能允許日誌收集器之間的通訊。

- TCP/9300
- TCP/9301
- TCP/9302

STEP 3 | 確定升級到 PAN-OS 11.1 的路徑.

您無法略過路徑中任何功能發佈版本的安裝，從目前執行的 PAN-OS 版本到 PAN-OS 11.1.0 版本皆是如此。

檢閱 PAN-OS 升級檢查清單，瞭解您在升級路徑中會經過的每個版本的版本資訊和 升級/降級考量事項 中的已知問題和預設行為變更。

STEP 4 | 安裝最新內容更新。

請參閱版本資訊，瞭解 *Panorama* 軟體版本所需的最低內容發行版本。

1. 登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Device Deployment**（裝置部署） > **Dynamic Updates**（動態更新） 和 **Check Now**（立即檢查） 以獲得最新更新。如果有可用的更新，Action（動作）欄會顯示 **Download**（下載）連結。
3. 如果尚未安裝，請 **Download**（下載）適當的內容更新。成功下載後，Action（動作）欄中的連結會從 **Download**（下載）變更為 **Install**（安裝）。
4. 在其他任何內容之前 **Install**（安裝）內容更新（「應用程式」和「威脅」更新）。

   如果您的訂閱同時包含「應用程式」和「威脅」內容，請先安裝應用程式內容。這會自動安裝「應用程式」和「威脅」內容。

   無論您的訂閱是否同時包含應用程式和威脅內容，*Panorama* 都只需要並且只會安裝應用程式內容。請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。
5. 根據需要對其他任何更新（防毒、WildFire 或 URL 篩選）重複上述子步驟，一次針對一個更新，可隨意選擇更新順序。

STEP 5 | 沿著您升級到 PAN-OS 11.1 的路徑，將日誌收集器升級為 PAN-OS 版本。

如果是升級多個日誌收集器，在您開始下載映之前，請決定您想升級的所有日誌收集器的升級路徑，讓過程順暢進行。

1. 當 Panorama 連線至網際網路時將日誌收集器升級到 PAN-OS 9.1。
2. 當 Panorama 連線至網際網路時將日誌收集器升級到 PAN-OS 10.0。
3. 當 Panorama 連線至網際網路時將日誌收集器升級到 PAN-OS 10.1。

   PAN-OS 11.1 引入了新的日誌格式。從 PAN-OS 11.1 升級至 PAN-OS 10.1 時，您可以選擇移轉 PAN-OS 8.1 或更早版本中產生的日誌。否則，這些日誌會在成功升級至 PAN-

OS 10.1 時自動被刪除。移轉過程中，日誌資料在 ACC 或 Monitor（監控器）頁籤中不可見。進行移轉時，日誌資料會繼續轉送至適當的日誌收集器，但您可能會遇到一些對效能的影響。

4. 當 Panorama 連線至網際網路時將日誌收集器升級到 PAN-OS 10.2。
5. 當 Panorama 連線至網際網路時將日誌收集器升級到 PAN-OS 11.0。

STEP 6 | 將日誌收集器升級到 PAN-OS 11.1。

1. 在 Panorama 上，**Check Now**（立即檢查）（**Panorama** > **Device Deployment**（裝置部署） > **Software**（軟體））有無最新更新。如果有可用的更新，Action（動作）欄會顯示 **Download**（下載）連結。
2. 為 PAN-OS 11.1 發行版本 **Download**（下載）特定於型號的檔案。例如，若要將 M-Series 設備升級至 Panorama 11.1.0，請下載 `Panorama_m-11.1.0` 映像。

   成功下載之後，該映像的 Action（動作）欄會從 **Download**（下載）變更為 **Install**（安裝）。
3. **Install**（安裝）PAN-OS 11.1 並選取適當的日誌收集器。
4. 如果一個或多個所選日誌收集器包含在 PAN-OS 10.0 或更舊版本中生成的日誌，則系統會顯示通知。

   首次嘗試 **Install**（安裝）PAN-OS 11.1.2 或更新版本的 11.1 版本時，系統會顯示此通知，但在通知關閉後就不會再顯示。通知會警告您系統偵測到執行 PAN-OS 10.0 或更舊版本時，Panorama 或受管理裝置生成的日誌，且這些日誌將在升級時遭刪除。這表示在成功升級之後，您無法再查看或搜尋受影響的日誌。

   但您可以在升級之後復原這些受影響的日誌。通知也會為您提供以下資訊。如果您選擇多個日誌收集器，請按一下 **Tasks**（工作）並查看每個日誌收集器的失敗安裝作業詳細資訊，以檢視和複製必要移轉命令。

   - 受影響的日誌類型。
   - 每種日誌類型的受影響時間範圍。
   - 復原每種日誌類型的受影響日誌時需要的每個 `debug logdb migrate-lc` 命令。

     複製所列 `debug logdb migrate-lc` 然後再 **Close**（關閉）通知。

   Close（關閉）通知。
5. 依據您的需求選取下列其中一項：
   - **Upload only to device (do not install)**（僅上傳至裝置（不要安裝））。
   - **Reboot device after install**（安裝後重新啟動裝置）。
6. 按一下 **OK**（確定） 以啟動上傳或安裝。

   在所選日誌收集器成功重新啟動後，繼續執行下一步。

STEP 7 | 驗證日誌收集器上安裝的軟體和內容更新版本。

輸入 **`show system info`** 操作命令。輸出如下所示：

```
sw-version:11.1.0 app-version：8750-8261 app-release-
date：2023/08/31 03:57:2
```


STEP 8 | （PAN-OS 11.1.2 及更新版本；僅限 Panorama 模式）登入每個受影響日誌收集器的日誌收集器 CLI，並使用上一步列出的 `debug logdb migrate-lc` 命令復原受影響的日誌。

這些命令必須按照順序執行，不能同時執行。如果您沒有複製通知視窗中的 `debug logdb migrate-lc` 命令，請按一下 **Tasks**（工作）並查看特定日誌收集器的失敗安裝作業詳細資訊。

STEP 9 | （僅限 FIPS-CC 模式）在 FIPS-CC 模式下升級 Panorama 和受管理的裝置

如果在專用日誌收集器執行 PAN-OS 11.1 版本時將專用日誌收集器新增至 Panorama 管理中，則在 FIPS-CC 模式下升級專用日誌收集器需要重設安全連線狀態。

當專用日誌收集器執行 PAN-OS 10.0 或更早版本時，您無需重新裝載新增至 Panorama 管理的專用日誌收集器。

STEP 10 | 重新產生或重新匯入所有憑證以遵守 OpenSSL 安全性等級 2。

如果您從 PAN-OS 10.1 或更早版本升級至 PAN-OS 11.0，則需要執行此步驟。如果您是從 PAN-OS 10.2 升級並且已經重新產生或重新匯入憑證，請略過此步驟。

要求所有憑證滿足以下最低要求：

- RSA 2048 位元或以上，或 ECDSA 256 位元或以上
- SHA256 或更高版本的摘要

有關重新產生或重新匯入憑證的更多資訊，請參閱 PAN-OS 管理員指南或 Panorama 管理員指南。

STEP 11 | （建議用於 Panorama 虛擬設備）將 Panorama 虛擬設備的記憶體增加至 64GB。

在日誌收集器模式下將 Panorama 虛擬設備成功升級至 PAN-OS 11.1 後，Palo Alto Networks 建議將 Panorama 虛擬設備的記憶體增加到 64GB 以滿足增加的系統要求，從而避免發生任何與佈建不足的 Panorama 虛擬設備相關的日誌記錄、管理和運作效能問題。

當 Panorama 未連線至網際網路時升級日誌收集器

如需可在日誌收集器上安裝的軟體和內容更新清單，請參閱 支援的更新 。

如果您是從 *PAN-OS 8.1* 升級，*PAN-OS 9.0* 會為本機和專用日誌收集器引入新的記錄資料格式。在升級到 *PAN-OS 10.1* 的路徑上，當您從 *PAN-OS 8.1* 升級到 *PAN-OS 9.0* 時，現有日誌資料會自動移轉至新格式。

您必須同時在收集器群組內升級所有日誌收集器，以避免丟失日誌資料。如果收集器群組內的日誌收集器並非執行相同的 PAN-OS 版本，則無法進行日誌轉送或日誌收集。此外，除非所有日誌收集器執行相同的 PAN-OS 版本，否則收集器群組內的日誌收集器日誌資料在 **ACC** 或 **Monitor**（監控器） 頁籤內不可見。例如，如果您在收集器群組內有三個日誌收集器，且您升級了其中兩個，則不會有日誌被轉送至收集器群組內的任何日誌收集器。

Palo Alto Networks 建議您在維護時段升級日誌收集器。由於日期格式的轉移，整個升級程序需要額外花費數個小時，具體取決於本機和專用日誌收集器上的日誌資料量。

STEP 1 | 升級日誌收集器之前，請確定您在 Panorama 管理伺服器上是執行適當的 Panorama™ 軟體版本。

Palo Alto Networks® 高度建議 *Panorama* 和日誌收集器執行相同的軟體發行版本，而且 *Panorama*、日誌收集器和所有受管理的防火牆也都執行相同的內容發行版本。如需瞭解重要軟體和內容相容性的詳細資訊，請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。

Panorama 執行的軟體版本必須與日誌收集器相同（或更新），但必須具有相同或更新的內容發行版本：

- 軟體發行版本—如果 Panorama 管理伺服器執行的軟體版本，與您想更新的日誌收集器不是相同或更新的版本，則在更新任何日誌收集器之前，您必須先將相同或更新的 Panorama 版本安裝在 Panorama（請參閱安裝 Panorama 的內容與軟體更新）。
- 內容發行版本—在內容發行版本方面，您應該確保所有日誌收集器都執行最新的內容發行版本，或者執行的版本至少高於您將安裝的版本或 Panorama 上正在執行的版本；否則，請先將防火牆從 Panorama 升級至 PAN-OS 11.1，再更新日誌收集器，然後才在 Panorama 管理伺服器上更新內容發行版本（請參閱 安裝 Panorama 的內容更新和軟體升級）。

檢查軟體和內容版本：

- **Panorama** 管理伺服器—若要查明 Panorama 管理伺服器上執行的軟體和內容版本，請登入 Panorama 網頁介面並移至 General Information（一般資訊）設定（**Dashboard**（儀表板））。
- 日誌收集器 —若要查明日誌收集器上執行的軟體和內容版本，請登入每個日誌收集器的 CLI 並執行 **`show system info`** 命令。

STEP 2 | 確定升級到 PAN-OS 11.1 的路徑。

檢閱 PAN-OS 升級檢查清單，瞭解您在升級路徑中會經過的每個版本的版本資訊和 升級/降級考量事項 中的已知問題和預設行為變更。

如果是升級多個日誌收集器，在您開始下載映之前，請決定您想升級的所有日誌收集器的升級路徑，讓過程順暢進行。

STEP 3 | 在網路上啟用以下 TCP 連接埠。

您必須在網路上啟用這些 TCP 連接埠，才能允許日誌收集器之間的通訊。

- TCP/9300
- TCP/9301
- TCP/9302

STEP 4 | 將最新內容和軟體更新下載到可透過 SCP 或 HTTPS 連線至 Panorama 並上傳檔案的主機。

請參閱版本資訊，瞭解 *Panorama* 軟體版本所需的最低內容發行版本。

1. 使用可存取網際網路的主機登入 Palo Alto Networks 客戶支援網站。
2. 下載最新內容更新：
   1. 在 Resources（資源）部分中按一下 **Dynamic Updates**（動態更新）。
   2. **Download**（下載）最新內容更新，然後將檔案儲存至主機。為您要更新的各內容類型執行此步驟。
3. 下載軟體更新：
   1. 返回 Palo Alto Networks 客戶支援網站的主頁面，然後在 Resources（資源）部分中按一下 **Software Updates**（軟體更新）。
   2. 檢閱下載欄以決定您要安裝的版本。M-Series 設備的更新套件檔名以 “Panorama_m” 開頭並緊接著版本號碼。例如，若要將 M-Series 設備升級至 Panorama 11.1.0，請下載 `Panorama_m-11.1.0` 映像。

      您可以從 ***Filter By***（篩選依據）下拉式清單中選取 ***Panorama M Images***（***Panorama M*** 映像）（適用於 *M-Series* 設備），快速找到 *Panorama* 映像。
4. 按一下適當的檔名，並將檔案儲存至主機。

STEP 5 | 安裝最新內容更新。

如果您需要安裝內容更新，則必須在安裝軟體更新之前完成。此外，請先將內容更新安裝在防火牆，再安裝於日誌收集器，然後才在 *Panorama* 上更新內容發行版本。

先安裝「應用程式」或「應用程式和威脅」更新，再依需要、一次一個、以任意順序安裝其他任何更新（防毒、WildFire® 或 URL 篩選）。

無論您的訂閱是否同時包含應用程式和威脅內容，*Panorama* 都只需要並且只會安裝應用程式內容。請參閱 Panorama、日誌收集器、防火牆和 WildFire 版本相容性。

1. 登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Device Deployment**（設備部署） > **Dynamic Updates**（動態更新）。
3. 按一下 **Upload**（上傳），選取更新 **Type**（類型），**Browse**（瀏覽）至主機上適當的內容更新檔案，然後按一下 **OK**（確定）。
4. 按一下 **Install From File**（從檔案安裝），選取更新 **Type**（類型），並選取您剛上傳的更新的 **File Name**（檔案名稱）。
5. 選取日誌收集器。
6. 按一下 **OK**（確定）以啟動安裝。
7. 針對每個內容更新重複這些步驟。

STEP 6 | 沿著您升級到 PAN-OS 11.1 的路徑，將日誌收集器升級為 PAN-OS 版本。

1. 當 Panorama 未連線至網際網路時將日誌收集器升級到 PAN-OS 9.1。
2. 當 Panorama 未連線至網際網路時將日誌收集器升級到 PAN-OS 10.0。
3. 當 Panorama 未連線至網際網路時將日誌收集器升級到 PAN-OS 10.1。

   PAN-OS 10.0 引入了新的日誌格式。從 PAN-OS 10.0 升級至 PAN-OS 10.1 時，您可以選擇移轉 PAN-OS 8.1 或更早版本中產生的日誌。否則，這些日誌會在成功升級至 PAN-OS 10.1 時自動被刪除。移轉過程中，日誌資料在 ACC 或 Monitor（監控器）頁籤中不可見。進行移轉時，日誌資料會繼續轉送至適當的日誌收集器，但您可能會遇到一些對效能的影響。
4. 當 Panorama 未連線至網際網路時將日誌收集器升級到 PAN-OS 10.2。
5. 當 Panorama 未連線至網際網路時將日誌收集器升級到 PAN-OS 11.0。

STEP 7 | 將日誌收集器升級到 PAN-OS 11.1。

1. 選取 **Panorama** > **Device Deployment**（裝置部署） > **Software**（軟體）。
2. 按一下 **Upload**（上傳），**Browse**（瀏覽）至主機上適當的軟體更新檔案，然後按一下 **OK**（確定）。
3. 在您剛上傳的版本的 Action（動作）欄中，按一下 **Install**（安裝）。
4. **Install**（安裝）PAN-OS 11.1 並選取適當的日誌收集器。
5. 如果一個或多個所選日誌收集器包含在 PAN-OS 10.0 或更舊版本中生成的日誌，則系統會顯示通知。

   首次嘗試 **Install**（安裝）PAN-OS 11.1.2 或更新版本的 11.1 版本時，系統會顯示此通知，但在通知關閉後就不會再顯示。通知會警告您系統偵測到執行 PAN-OS 10.0 或更舊版本時，Panorama 或受管理裝置生成的日誌，且這些日誌將在升級時遭刪除。這表示在成功升級之後，您無法再查看或搜尋受影響的日誌。

   但您可以在升級之後復原這些受影響的日誌。通知也會為您提供以下資訊。如果您選擇多個日誌收集器，請按一下 **Tasks**（工作）並查看每個日誌收集器的失敗安裝作業詳細資訊，以檢視和複製必要移轉命令。

   - 受影響的日誌類型。
   - 每種日誌類型的受影響時間範圍。
   - 復原每種日誌類型的受影響日誌時需要的每個 `debug logdb migrate-lc` 命令。

     複製所列 `debug logdb migrate-lc` 然後再 **Close**（關閉）通知。

   Close（關閉）通知。
6. 依據您的需求選取下列其中一項：
   - **Upload only to device (do not install)**（僅上傳至裝置（不要安裝））。
   - **Reboot device after install**（安裝後重新啟動裝置）。
7. 按一下 **OK**（確定） 以啟動上傳或安裝。

   在所選日誌收集器成功重新啟動後，繼續執行下一步。

STEP 8 | 驗證各日誌收集器上安裝的軟體和內容版本。

登入日誌收集器 CLI 並輸入 **show system info**（顯示系統資訊）操作命令。輸出如下所示：

```
sw-version:11.1.0 app-version：8750-8261 app-release-
date：2023/08/31 03:57:2
```

STEP 9 | （PAN-OS 11.1.2 及更新版本；僅限 Panorama 模式）登入每個受影響日誌收集器的日誌收集器 CLI，並使用上一步列出的 **debug logdb migrate-lc** 命令復原受影響的日誌。

這些命令必須按照順序執行，不能同時執行。如果您沒有複製通知視窗中的 **debug logdb migrate-lc** 命令，請按一下 **Tasks**（工作）並查看特定日誌收集器的失敗安裝作業詳細資訊。

STEP 10 | （僅限 FIPS-CC 模式）在 FIPS-CC 模式下升級 Panorama 和受管理的裝置

如果在專用日誌收集器執行 PAN-OS 11.1 版本時將專用日誌收集器新增至 Panorama 管理中，則在 FIPS-CC 模式下升級專用日誌收集器需要重設安全連線狀態。

當專用日誌收集器執行 PAN-OS 10.0 或更早版本時，您無需重新裝載新增至 Panorama 管理的專用日誌收集器。

STEP 11 | （PAN-OS 10.2 及更高版本）重新產生或重新匯入所有憑證以遵守 OpenSSL 安全性等級 2。

如果您從 PAN-OS 10.1 或更早版本升級至 PAN-OS 11.0，則需要執行此步驟。如果您是從 PAN-OS 10.2 升級並且已經重新產生或重新匯入憑證，請略過此步驟。

要求所有憑證滿足以下最低要求：

- RSA 2048 位元或以上，或 ECDSA 256 位元或以上
- SHA256 或更高版本的摘要

有關重新產生或重新匯入憑證的更多資訊，請參閱 PAN-OS 管理員指南或 Panorama 管理員指南。

STEP 12 | （建議用於 Panorama 虛擬設備）將 Panorama 虛擬設備的記憶體增加至 64GB。

在日誌收集器模式下將 Panorama 虛擬設備成功升級至 PAN-OS 11.1 後，Palo Alto Networks 建議將 Panorama 虛擬設備的記憶體增加到 64GB 以滿足增加的系統要求，從而避免發生任何與佈建不足的 Panorama 虛擬設備相關的日誌記錄、管理和運作效能問題。

在有網際網路連線的情況下從 Panorama 升級 WildFire 叢集

如果一個叢集中的 WildFire 設備由 Panorama 管理，其升級可並行。如果 Panorama 直接連線至網際網路，您可直接從 Panorama 查看並下載新版本。

Panorama 可以管理執行相同或更舊 *PAN-OS* 軟體版本的 *WildFire* 設備及設備叢集。

STEP 1 | 將 Panorama 升級至與您想要在 WildFire 叢集上安裝的目標軟體版本相同或更新。

有關升級 Panorama 的詳細資料，請參閱安裝 Panorama 的內容與軟體更新。

STEP 2 | 暫停樣本分析。

1. 使防火牆停止轉送任何新樣本至 WildFire 設備。
   1. 登入防火牆 Web 介面。
   2. 選取 **Device**（設備） **> Setup**（設定） **> WildFire**，然後編輯**General Setting**（一般設定）。
   3. 清除 **WildFire Private Cloud**（**WildFire** 私人雲端）欄位。
   4. 按一下 **OK**（確定）與 **Commit**（提交）。
2. 確認防火牆已提交至設備的樣本分析已完成：
   1. 登入 Panorama 網頁介面。
   2. 選取 **Panorama > Managed WildFire Clusters**（受管理的 **WildFire** 叢集） 並 **View**（檢視）叢集分析環境 **Utilization**（使用率）。
   3. 確認 **Virtual Machine Usage**（虛擬電腦使用率）未顯示任何進行中的樣本分析。

   如果您不想等待 *WildFire* 設備完成分析最近提交的樣本，可以繼續下一步。但是，要假定 *WildFire* 設備之後會從分析佇列捨棄擱置樣本。

STEP 3 | 安裝最新 WildFire 設備內容更新。

這些更新為設備提供了最新的威脅資訊以準確偵測惡意軟體。

您必須先安裝內容更新，再安裝軟體更新。參考版本資訊，瞭解您必須為 *Panorama* 版本安裝的最低內容版本。

1. 下載 WildFire 內容更新：
   1. 選取 **Panorama > Device Deployment > Dynamic Updates. (Panorama >** 設備部署 **>** 動態更新。**).**
   2. 選取 WildFire 內容更新套件版本並按一下 **Download**（下載）。
2. 按一下 **Install (**安裝**)**。
3. 選取您想要升級的 WildFire 叢集或個別設備。
4. 按一下 **OK**（確定）以啟動安裝。

STEP 4 | 下載 PAN-OS 軟體版本至 WildFire 設備。

升級 WildFire 設備時，您不能略過任何主要發行版本。例如，如果您想要從 PAN-OS 9.1 版升級至 PAN-OS 11.0 版，您首先必須下載並安裝 AN-OS 10.0、PAN-OS 10.1 和 PAN-OS 10.2 版。

1. 下載 WildFire 軟體升級：
   1. 選取 **Panorama > Device Deployment**（設備部署） **> Software**（軟體）。
   2. 按一下 **Check Now**（立即檢查）以擷取已更新的版本清單。
   3. 選取要安裝的 WildFire 版本，並按一下 **Download**（下載）。
   4. 按一下 **Close**（關閉）以離開 **Download Software**（下載軟體）視窗
2. 按一下 **Install (安裝)**。
3. 選取您想要升級的 WildFire 叢集。
4. 在安裝後選取 Reboot（重新啟動）裝置：
5. 按一下 **OK**（確定）以啟動安裝。
6. （選用）在 Panorama 上監控安裝程序。

STEP 5 | （選用）在 WildFire 控制器節點上檢視重新啟動工作的狀態。

在 WildFire 叢集控制器上，執行下列命令並尋找 **Install**（安裝） 工作類型及 **FIN**（完成）狀態：

```
admin@WF-500(active-controller)> show cluster task pending
```

STEP 6 | 確認 WildFire 設備已可以繼續進行樣本分析。

1. 確認 sw-version 欄位顯示 11.0.0：

   ```
   admin@WF-500(passive-controller)> show system info | match sw-version
   ```

2. 確認所有程序都在執行：

   ```
   admin@WF-500(passive-controller)> show system software status
   ```

3. 確認自動提交（**AutoCom**（自動提交））工作已完成：

   ```
   admin@WF-500(passive-controller)> show jobs all
   ```

在沒有網際網路連線的情況下從 Panorama 升級 WildFire 叢集

如果一個叢集中的 WildFire 設備由 Panorama 管理，其升級可並行。如果 Panorama 沒有直接連線至網際網路，您必須從 Palo Alto Networks 支援網站下載軟體內容和更新，並將其在內部伺服器託管，然後由 Panorama 散佈。

Panorama 可以管理執行相同或更舊 *PAN-OS* 軟體版本的 *WildFire* 設備及設備叢集。

STEP 1 | 將 Panorama 升級至與您想要在 WildFire 叢集上安裝的目標軟體版本相同或更新。

有關升級 Panorama 的詳細資料，請參閱安裝 Panorama 的內容與軟體更新。

STEP 2 | 暫停樣本分析。

1. 使防火牆停止轉送任何新樣本至 WildFire 設備。
   1. 登入防火牆 Web 介面。
   2. 選取 **Device**（設備） **> Setup**（設定） **> WildFire**，然後編輯**General Setting**（一般設定）。
   3. 清除 **WildFire Private Cloud**（**WildFire** 私人雲端）欄位。
   4. 按一下 **OK**（確定）與 **Commit**（提交）。
2. 確認防火牆已提交至設備的樣本分析已完成：
   1. 登入 Panorama 網頁介面。
   2. 選取 **Panorama > Managed WildFire Clusters**（受管理的 **WildFire** 叢集） 並 **View**（檢視）叢集分析環境 **Utilization**（使用率）。
   3. 確認 **Virtual Machine Usage**（虛擬電腦使用率）未顯示任何進行中的樣本分析。

   如果您不想等待 *WildFire* 設備完成分析最近提交的樣本，可以繼續下一步。但是，要假定 *WildFire* 設備之後會從分析佇列捨棄擱置樣本。

STEP 3 | 將 WildFire 內容與軟體更新下載至有網際網路存取權的主機。Panorama 必須具有主機的存取權。

1. 使用可存取網際網路的主機登入 Palo Alto Networks 客戶支援網站。
2. 下載內容更新：
   1. 在 [工具] 部分中按一下 **Dynamic Updates**（動態更新）。
   2. **Download**（下載）所需內容更新，然後將檔案儲存至主機。為您要更新的各內容類型執行此步驟。
3. 下載軟體更新：
   1. 返回 Palo Alto Networks 客戶支援網站的主頁面，然後在 [工具] 部分中按一下 **Software Updates**（軟體更新）。
   2. 檢閱 Download（下載）欄以決定您要安裝的版本。更新套件的檔案名稱表示升級的型號和版本：WildFire_<release>.
   3. 按一下檔名，並將檔案儲存至主機。

STEP 4 | 安裝最新 WildFire 設備內容更新。

這些更新為設備提供了最新的威脅資訊以準確偵測惡意軟體。

您必須先安裝內容更新，再安裝軟體更新。參考版本資訊，瞭解您必須為 *Panorama* 版本安裝的最低內容版本。

1. 下載 WildFire 內容更新：
   1. 選取 **Panorama > Device Deployment > Dynamic Updates. (Panorama >** 設備部署 **>** 動態更新。**).**
   2. 按一下 **Upload**（上載），選取內容 **Type**（類型），**Browse**（瀏覽）至 WildFire 內容更新檔案，並按一下 **OK**（確定）。
   3. 按一下 **Install From File**（從檔案安裝），選取套件 **Type**（類型）、**File Name**（檔案名稱），以及叢集中您想要升級的 WildFire 設備，然後按一下 **OK**（確定）。
2. 按一下 **OK**（確定）以啟動安裝。

STEP 5 | 下載 PAN-OS 軟體版本至 WildFire 設備。

升級 WildFire 設備時，您不能略過任何主要發行版本。例如，如果您想要從 PAN-OS 9.1 版升級至 PAN-OS 11.0 版，您首先必須下載並安裝 AN-OS 10.0、PAN-OS 10.1 和 PAN-OS 10.2 版。

1. 下載 WildFire 軟體升級：
   1. 選取 **Panorama > Device Deployment**（設備部署） **> Software**（軟體）。
   2. 按一下 **Check Now**（立即檢查）以擷取已更新的版本清單。
   3. 選取要安裝的 WildFire 版本，並按一下 **Download**（下載）。
   4. 按一下 **Close**（關閉）以離開 **Download Software**（下載軟體）視窗
2. 按一下 **Install (**安裝**)**。
3. 選取您想要升級的 WildFire 叢集。
4. 在安裝後選取 Reboot（重新啟動）裝置：
5. 按一下 **OK**（確定）以啟動安裝。
6. （選用）在 Panorama 上監控安裝程序。

STEP 6 | （選用）在 WildFire 控制器節點上檢視重新啟動工作的狀態。

在 WildFire 叢集控制器上，執行下列命令並尋找 **`Install`**（安裝） 工作類型及 **`FIN`**（完成）狀態：

```
admin@WF-500(active-controller)> show cluster task pending
```


STEP 7 | 確認 WildFire 設備已可以繼續進行樣本分析。

1. 確認 sw-version 欄位顯示 11.0.0：

```
admin@WF-500(passive-controller)> show system info | match sw-version
```

2. 確認所有程序都在執行：
   admin@WF-500(passive-controller)> **show system software status**
3. 確認自動提交（**AutoCom**（自動提交））工作已完成：

```
admin@WF-500(passive-controller)> show jobs all
```

當 Panorama 連線至網際網路時升級防火牆

檢閱 PAN-OS 11.1 版本資訊，然後使用以下程序來升級您使用 Panorama 管理的防火牆。此程序應用在獨立的防火牆，以及部署在高可用性（HA）設定中的防火牆。

在跨多個功能 PAN-OS 版本升級 HA 防火牆時，您必須先將每個 HA 對等升級至升級路徑上的相同功能 PAN-OS 版本，然後再繼續。例如，將 HA 對等從 PAN-OS 10.2 升級至 PAN-OS 11.1。您必須先將兩個 HA 對等升級至 PAN-OS 11.0，然後才能繼續升級至目標 PAN-OS 11.1 版本。當 HA 對等相隔兩個或更多個功能版本時，安裝了舊版本的防火牆會進入 `suspended` 狀態，並顯示訊息 `Peer version too old`。

若 *Panorama* 無法直接連線至升級的伺服器，則請遵循當 Panorama 未連線至網際網路時升級防火牆中的程序，以讓您可以手動下載映像至 *Panorama*，然後將映像散佈至防火牆。

當部署從 PAN-OS 11.1 Panorama 設備到 PAN-OS 10.1 或更高版本的防火牆的升級時，新的略過軟體版本升級功能使您能夠略過最多三個版本。

在從 Panorama 升級防火牆之前，您必須：

- 確定 Panorama 正執行您要升級版本相同或更新的 PAN-OS 版本。您必須先升級 Panorama 及其日誌收集器（升級至 11.1），再將受管理的防火牆升級至此版本。此外，將日誌收集器升級至 11.1 時，由於記錄基礎結構有所變更，您必須將所有日誌收集器同時升級。
- 確保防火牆連接可靠的電源。升級過程中的電力損耗會使防火牆無法使用。
- 在升級至 PAN-OS 11.1 時，如果 Panorama 虛擬設備處於舊版模式，則決定是否保留在舊版模式。執行 PAN-OS 9.1 或更新版本的新 Panorama 設備部署不支援舊版模式。如果您將 Panorama 虛擬設備從 PAN-OS 9.0 或更早版本升級至 PAN-OS 11.1，Palo Alto Networks 建議您檢閱設定 Panorama 虛擬設備的先決條件，並根據需要變更為 Panorama 模式或僅管理模式。

  如果您要將 Panorama 虛擬設備保持在舊版模式中，請將配置給 Panorama 虛擬設備的 CPU 和記憶體增加到至少 16 個 CPU 和 32GB 記憶體，以成功升級至 PAN-OS 11.1。如需詳細資訊，請參閱 Panorama 虛擬設備的安裝先決條件。

- （建議用於多重 vsys 受管理防火牆）將多重 vsys 受管理防火牆的所有 vsys 轉換為 Panorama。

  建議您這樣做以避免在多重 vsys 受管理防火牆上提交問題，並讓您能夠利用 Panorama 的最佳化共用物件推送。

  這僅適用於使用略過軟體版本升級，從 PAN-OS 10.1 升級到 PAN-OS 11.1 的多重 vsys 防火牆。

- （多重 vsys 受管理防火牆）刪除或重新命名與 Panorama **Shared**（共用）設定中的物件名稱相同的任何本機設定 **Shared**（共用）物件。否則，升級後從 Panorama 推送的設定會失敗並顯示錯誤 `<object-name>` 已在使用中。

  這僅適用於使用略過軟體版本升級，從 PAN-OS 10.1 升級到 PAN-OS 11.1 的多重 vsys 防火牆。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 已修改您的安全性政策規則，以允許 `ssl` 應用程式流量。

這僅適用於使用略過軟體版本升級，從 *PAN-OS 10.1* 升級到 *PAN-OS 11.1* 的防火牆。

如果使用 *`panorama` App-ID* 來控制 *Panorama* 和受管理裝置之間的流量，則您必須這樣做，才能防止升級到 *PAN-OS 11.1* 後受管理裝置與 *Panorama* 中斷連線。如果升級前不允許使用 *`ssl`* 應用程式，受管理裝置將與 *Panorama* 中斷連線。

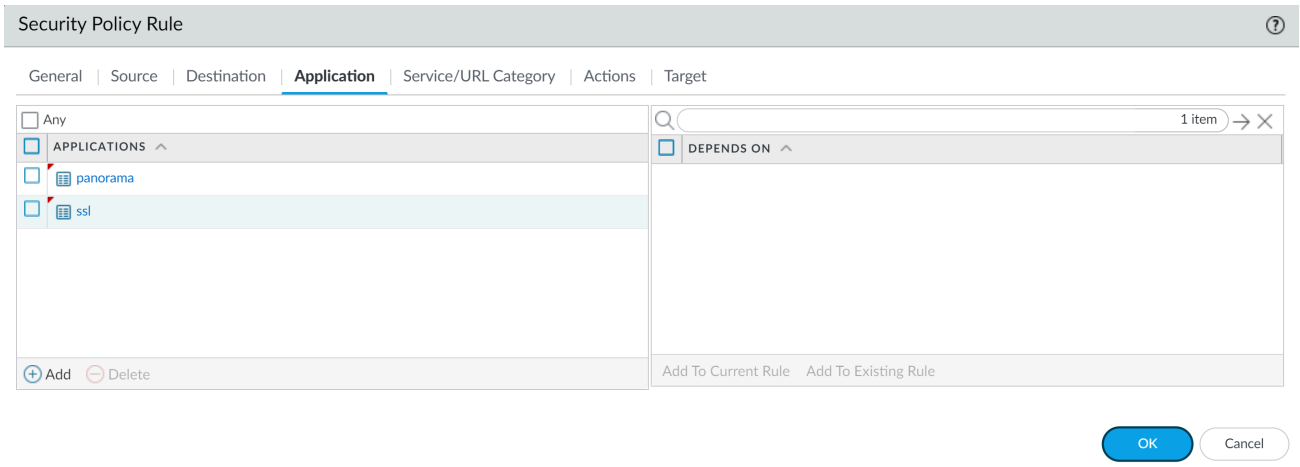
PAN-OS 11.1 會使用 TLS 版本 1.3 來加密 Panorama 與受管理防火牆之間的服務憑證和交握訊息。因此，從受管理防火牆到 Panorama 的流量的 App-ID 會從 `panorama` 重新分類為 `ssl`。

若要繼續 Panorama 和受管理裝置之間的通訊，您必須修改控制 Panorama 和受管理裝置之間流量的安全性政策規則，允許 `ssl` 應用程式。

如果控制 Panorama 和受管理裝置之間流量的安全性政策規則允許 **Any**（任何）應用程式，或者您已修改控制 Panorama 和受管理裝置之間流量的安全性政策規則，則請略過此步驟。

1. 選擇 **Policies**（政策） > **Security**（安全性） > **Pre Rules**（預先規則）。
2. 選擇包含控制 Panorama 和受管理防火牆之間流量的安全性政策規則的 **Device Group**（裝置群組）。
3. 選取安全性政策規則。
4. 選擇 **Application**（應用程式）並 **Add**（新增）`ssl`。

   不要刪除 *`panorama`* 應用程式。否則會導致所有受管理防火牆在您推送變更後與 *Panorama* 中斷連線。

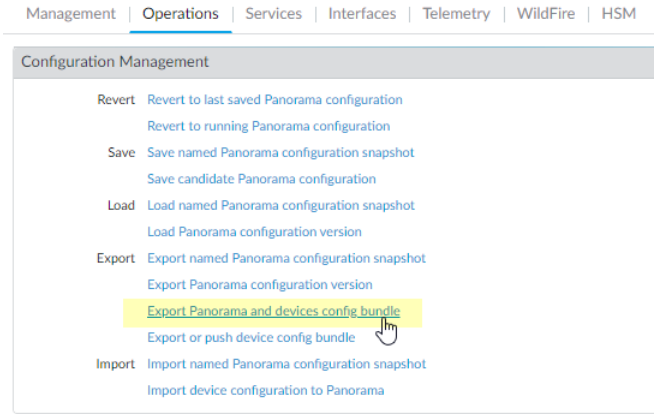


5. 按一下 **OK**（確定）。
6. 選擇 **Commit**（提交） > **Commit and Push**（提交並推送）並 **Commit and Push**（提交並推送）您的設定變更。

STEP 3 | 在您打算升級的每個受管理的防火牆上，儲存目前組態檔案的備份。

雖然防火牆會自動建立設定備份，但最好在升級前建立備份並儲存在外部。

1. 選取 **Panorama** > **Setup**（設定） > **Operations**（操作）並按一下 **Export Panorama and devices config bundle**（匯出 **Panorama** 和裝置設定組合），以產生並匯出 Panorama 和每個受管理設備的最新設定備份。

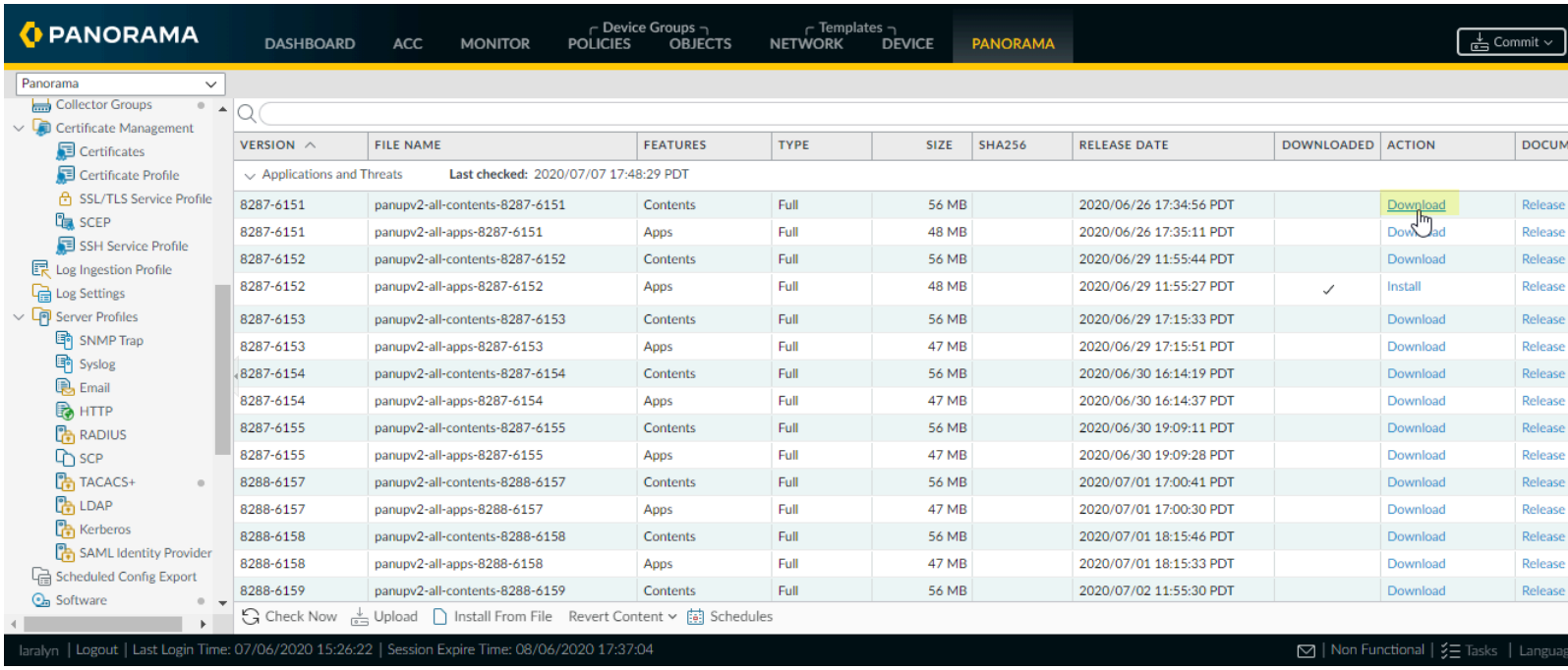


2. 將匯出的檔案儲存至防火牆外部的位置。如果您在升級時發生問題，便可使用此備份還原組態。

STEP 4 | 安裝最新內容更新。

請參閱版本資訊，瞭解 PAN-OS 11.1 所需的最低內容發行版本。在部署內容更新至 Panorama 和受管理防火牆時，請務必遵循 應用程式與威脅內容更新的最佳做法。

1. 選取 **Panorama** > **Device Deployment**（裝置部署） > **Dynamic Updates**（動態更新） 和 **Check Now**（立即檢查）以取得最新更新。如果有可用的更新，Action（動作）欄會顯示 **Download**（下載）連結。



2. 按一下 **Install**（安裝），並選取要安裝更新的防火牆。如果您正在升級 HA 防火牆，則您必須在兩個端點都升級內容。
3. 按一下 **OK**（確定）

STEP 5 | 確定升級到 PAN-OS 11.1 的路徑。

檢閱 PAN-OS 升級檢查清單，對於您在升級路徑中會經過的每個版本，瞭解版本資訊中的已知問題和預設行為變更，以及升級/降級注意事項。

如果是升級多個防火牆，在您開始下載映之前，請決定您想升級的所有防火牆的升級路徑，讓過程順暢進行。

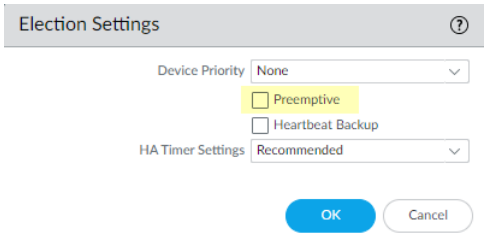
STEP 6 | （最佳做法）如果您正在使用 Cortex 資料湖 (CDL)，請安裝裝置憑證。

防火牆會在升級至 PAN-OS 11.1 時自動切換至使用裝置憑證進行 CDL 擷取和查詢端點的驗證。

如果在升級至 *PAN-OS 11.1* 之前未安裝裝置憑證，防火牆會繼續使用現有的日誌記錄服務憑證進行驗證。

STEP 7 | （僅限 HA 防火牆升級）如果您將升級為 HA 配對一部分的防火牆，請停用先佔。您僅需要在每個 HA 配對中的一個防火牆上停用此設定。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） 並編輯 **Election Settings**（選取設定）。
2. 若啟用，停用（清除）**Preemptive**（先佔）設定，然後按一下 **OK**（確認）。



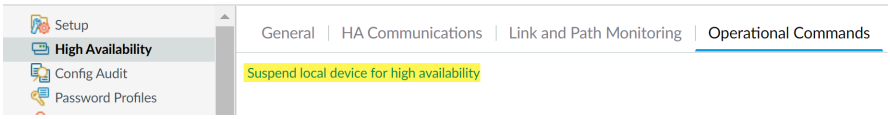
3. **Commit**（提交）您的變更。在您繼續進行更新前，請確認提交成功。

STEP 8 | （僅限 HA 防火牆升級）暫停主要 HA 對等以執行容錯移轉。

（主動/被動防火牆）對於主動/被動 HA 設定中的防火牆，先暫停並升級主動 HA 對等。

（主動/主動防火牆）對於主動/主動 HA 設定中的防火牆，先暫停並升級主動-主要 HA 對等。

1. 登入活動的主要防火牆 HA 對等的防火牆網頁介面。
2. 選取 **Device**（裝置） > **High Availability**（高可用性） > **Operational Commands**（操作命令）和 **Suspend local device for high availability**（暫停本機裝置以取得高可用性）。



3. 在右下角，確認狀態為 `suspended`。

   由此引起的容錯移轉應會導致次要被動 HA 對等轉變為 `active` 狀態。

   由此引起的容錯移轉會在您升級之前確認 *HA* 容錯移轉是否正常執行。

STEP 9 | （選用）將您受管理的防火牆升級至 PAN-OS 10.1。

略過軟體版本升級功能支援執行 PAN-OS 10.1 或更高版本的受管理防火牆。如果您的受管理防火牆執行的是 PAN-OS 10.0 或更早版本，請先升級至 PAN-OS 10.1 或更高版本。

STEP 10 | （選用）將檔案 **Export**（匯出）至已設定的 SCP 伺服器。

在 PAN-OS 11.1 中，在將升級部署到受管理的防火牆時，SCP 伺服器可用作下載來源。在下一步下載軟體和內容映像之前匯出檔案。

STEP 11 | 驗證並下載目標版本所需的軟體和內容版本。

在此步驟中，您可以檢視並下載升級至 PAN-OS 11.1 所需的中間軟體和內容映像。

使用多重映像下載來下載軟體和內容映像為選用。您仍然可以一次下載一個映像。

1. 按一下 **Panorama** > **Device Deployment**（裝置部署） > **Software**（軟體） > **Action**（動作） > **Validate**（驗證）。
2. 檢視您需要下載的中間軟體和內容版本。
3. 選取要升級的防火牆，然後按一下 **Deploy**（部署）。
4. 選取下載來源並按一下 **Download**（下載）。

STEP 12 | 在防火牆上安裝 PAN-OS 11.1.0。

（僅限 *SD-WAN*）要保持 *SD-WAN* 連結的準確狀態，在升級分支防火牆之前，您必須將中樞防火牆升級至 *PAN-OS 11.1*。如果先升級分支防火牆之後才升級中樞防火牆，可能產生錯誤監控資料（***Panorama*** > ***SD-WAN*** > ***Monitoring***（監控）），且 *SD-WAN* 連結會錯誤顯示為關閉。

1. 在對應您想要升級的防火牆型號的動作欄位中按一下 **Install**（安裝）。舉例來說，如果您想要升級 PA-440 防火牆，請按一下 PanOS_440-11.1.0 對應行的 **Install**（安裝）。
2. 在部署軟體檔案對話框中，選取所有您想要升級的防火牆。

   （僅限 HA 防火牆升級）若要減少停機時間，請在每個 HA 配對中只選取一個對等。對於主動/被動配對，請選取主動端點；對立主動/主動配對，請選取主動-次要端點。
3. （僅限 HA 防火牆升級） 確定未選取 **Group HA Peers**（群組 **HA** 配對）。
4. 選取 **Reboot device after install**（安裝後重新啟動裝置）。
5. 若要開始升級，請按一下 **OK**（確認）。
6. 安裝成功完成後，使用下列其中一種方法重新啟動：
   - 如果提示您重新啟動，請按一下**Yes** （是）。
   - 如果未提示您重新啟動，請選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後 **Reboot Device**（重新啟動裝置）。
7. 在防火牆結束重新啟動後，請選取 **Panorama** > **Managed Devices**（受管理的裝置） 並驗證您升級的防火牆軟體版為 11.1.0。還要認證任何您在升級後仍舊為被動的防火牆的 HA 狀態。

STEP 13 | （僅限 HA 防火牆升級）將 HA 功能還原至主要 HA 對等。

1. 登入暫停的主要防火牆 HA 對等的防火牆網頁介面 。
2. 選取 **Device**（裝置） > **High Availability**（高可用性） > **Operational Commands**（操作命令），然後 **Make local device functional for high availability**（讓本機裝置運作以取得高可用性）。
3. 在右下角，確認狀態為 `Passive`。對於主動/主動設定中的防火牆，確認狀態為 `Active`。
4. 等待 HA 對等執行設定同步。

   在 **Dashboard**（儀表板）中，監控「高可用性」Widget 中的「執行設定」狀態。

STEP 14 | （僅限 HA 防火牆升級）暫停次要 HA 對等以執行容錯移轉回主要 HA 對等。

1. 登入活動的次要防火牆 HA 對等的防火牆網頁介面 。
2. 選取 **Device**（裝置） > **High Availability**（高可用性） > **Operational Commands**（操作命令）和 **Suspend local device for high availability**（暫停本機裝置以取得高可用性）。
3. 在右下角，確認狀態為 `suspended`。

   由此引起的容錯移轉應會導致主要被動 HA 對等轉變為 `active` 狀態。

   由此引起的容錯移轉會在您升級之前確認 *HA* 容錯移轉是否正常執行。

STEP 15 | （僅限 HA 防火牆升級）升級每個 HA 配對中的次要 HA 配對。

1. 在 Panorama 網頁介面中，選取 **Panorama** > **Device Deployment**（裝置部署） > **Software**（軟體）。
2. 在對應您正升級 HA 配對的防火牆型號的動作欄位中按一下 **Install**（安裝）。
3. 在部署軟體檔案對話框中，選取所有您想要升級的防火牆。這一次，僅選取您剛升級的 HA 防火牆的端點。
4. 確定未選取 **Group HA Peers**（群組 **HA** 配對）。
5. 選取 **Reboot device after install**（安裝後重新啟動裝置）。
6. 若要開始升級，請按一下 **OK**（確認）。
7. 安裝成功完成後，使用下列其中一種方法重新啟動：
   - 如果提示您重新啟動，請按一下**Yes** （是）。
   - 如果未提示您重新啟動，請選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作） 和 **Reboot Device**（重新啟動裝置）。

STEP 16 | （僅限 HA 防火牆升級）將 HA 功能還原至次要 HA 對等。

1. 登入暫停的次要防火牆 HA 對等的防火牆網頁介面 。
2. 選取 **Device**（裝置） > **High Availability**（高可用性） > **Operational Commands**（操作命令），然後 **Make local device functional for high availability**（讓本機裝置運作以取得高可用性）。
3. 在右下角，確認狀態為 `Passive`。對於主動/主動設定中的防火牆，確認狀態為 `Active`。
4. 等待 HA 對等執行設定同步。

   在 **Dashboard**（儀表板）中，監控「高可用性」Widget 中的「執行設定」狀態。

STEP 17 | （僅限 FIPS-CC 模式）在 FIPS-CC 模式下升級 Panorama 和受管理的裝置

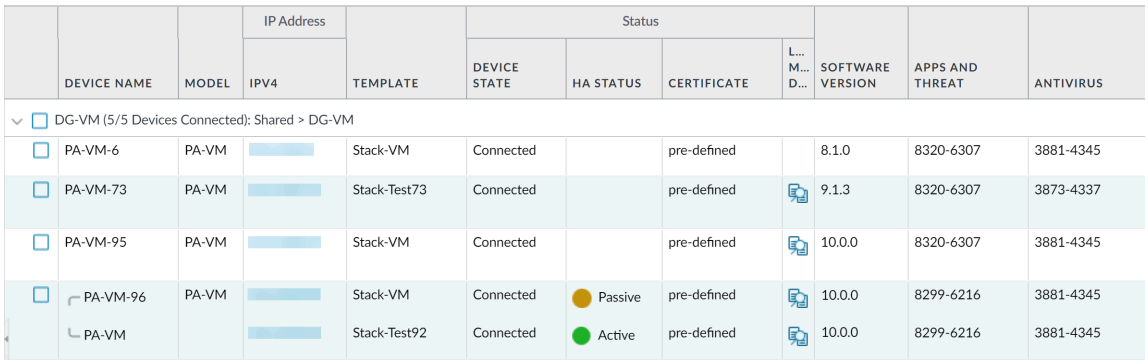
如果在受管理的防火牆執行 PAN-OS 11.1 版本時將專用日誌收集器新增至 Panorama 管理中，則在 FIPS-CC 模式下升級受管理的防火牆需要重設安全連線狀態。

當受管理的防火牆執行 PAN-OS 10.0 或更早版本時，您無需重新裝載新增至 Panorama 管理的受管理防火牆。

STEP 18 | 確認在每個受管理防火牆上執行的軟體與內容發佈版本。

1. 在 Panorama 上，選取 **Panorama** > **Managed Devices**（受管理的裝置）。
2. 在表格內找到防火牆，並檢閱內容和軟體版本。

   對於 HA 防火牆，您也可以驗證每個端點的 HA 狀態是否如預期。



	DEVICE NAME	MODEL	IP Address IPV4	TEMPLATE	Status DEVICE STATE	Status HA STATUS	Status CERTIFICATE	Status L... M... D...	SOFTWARE VERSION	APPS AND THREAT	ANTIVIRUS
DG-VM (5/5 Devices Connected): Shared > DG-VM											
	PA-VM-6	PA-VM		Stack-VM	Connected		pre-defined		8.1.0	8320-6307	3881-4345
	PA-VM-73	PA-VM		Stack-Test73	Connected		pre-defined		9.1.3	8320-6307	3873-4337
	PA-VM-95	PA-VM		Stack-VM	Connected		pre-defined		10.0.0	8320-6307	3881-4345
	PA-VM-96	PA-VM		Stack-VM	Connected	Passive	pre-defined		10.0.0	8299-6216	3881-4345
	PA-VM			Stack-Test92	Connected	Active	pre-defined		10.0.0	8299-6216	3881-4345

STEP 19 | （僅限 HA 防火牆升級）如果您在升級之前在其中一個 HA 防火牆上停用先佔，請編輯 **Election Settings**（選取設定）（**Device**（裝置） > **High Availability**（高可用性）），針對該防火牆重新啟用 **Preemptive**（先佔）設定，然後 **Commit**（提交）。

STEP 20 | 在 Panorama 網頁介面上，將整個 Panorama 受管理設定推送至您的受管理防火牆。

需要執行此步驟以選擇性提交並推送 Panorama 上的裝置群組和範本堆疊設定變更至受管理的防火牆。

需要執行此步驟以在成功由 PAN-OS 10.1 或更早版本升級到 PAN-OS 11.1 後，成功地將設定變更推送至由 Panorama 管理的多重 vsys 防火牆。如需詳細資訊，請參閱由 Panorama 管理的多重 vsys 防火牆的 共用設定物件的預設行為變更。

1. 選取 **Commit**（提交） > **Push to Devices**（推送至裝置）。
2. **Push**（推送）。

STEP 21 | 重新產生或重新匯入所有憑證以遵守 OpenSSL 安全性等級 2。

在升級到 PAN-OS 11.1 或更高版本時，要求所有憑證滿足以下最低要求：如果您是從 PAN-OS 10.2 升級並且已經重新產生或重新匯入憑證，請略過此步驟。

- RSA 2048 位元或以上，或 ECDSA 256 位元或以上
- SHA256 或更高版本的摘要

請參閱 PAN-OS 管理員指南或 Panorama 管理員指南，瞭解有關重新產生或重新匯入憑證的更多資訊。

STEP 22 | 檢視防火牆的軟體升級歷程記錄。

1. 登入 Panorama 介面。
2. 前往 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要）並按一下 **Device History**（裝置歷程記錄）。

當 Panorama 未連線至網際網路時升級防火牆

如需可在防火牆上安裝的軟體和內容更新清單，請參閱支援的更新。

當部署從 PAN-OS 11.1 Panorama 設備到 PAN-OS 10.1 或更高版本的防火牆的升級時，新的略過軟體版本升級功能使您能夠略過最多三個版本。

在從 Panorama 升級防火牆之前，您必須：

- 確定 Panorama 正執行您要升級版本相同或更新的 PAN-OS 版本。您必須先升級 Panorama 及其日誌收集器（升級至 11.1），再將受管理的防火牆升級至此版本。此外，將日誌收集器升級至 11.1 時，由於記錄基礎結構有所變更，您必須將所有日誌收集器同時升級。
- 確保防火牆連接可靠的電源。升級過程中的電力損耗會使防火牆無法使用。
- 在升級至 PAN-OS 11.1 時，如果 Panorama 虛擬設備處於舊版模式，則決定是否保留在舊版模式。執行 PAN-OS 9.1 或更新版本的新 Panorama 設備部署不支援舊版模式。如果您將 Panorama 虛擬設備從 PAN-OS 9.0 或更早版本升級至 PAN-OS 11.1，Palo Alto Networks 建議您檢閱設定 Panorama 虛擬設備的先決條件，並根據需要變更為 Panorama 模式或僅管理模式。

  如果您要將 Panorama 虛擬設備保持在舊版模式中，請將配置給 Panorama 虛擬設備的 CPU 和記憶體增加到至少 16 個 CPU 和 32GB 記憶體，以成功升級至 PAN-OS 11.1。如需詳細資訊，請參閱 Panorama 虛擬設備的安裝先決條件。
- （建議用於多重 vsys 受管理防火牆）將多重 vsys 受管理防火牆的所有 vsys 轉換為 Panorama。

  建議您這樣做以避免在多重 vsys 受管理防火牆上提交問題，並讓您能夠利用 Panorama 的最佳化共用物件推送。

  這僅適用於使用略過軟體版本升級，從 PAN-OS 10.1 升級到 PAN-OS 11.1 的多重 vsys 防火牆。
- （多重 vsys 受管理防火牆）刪除或重新命名與 Panorama **Shared**（共用）設定中的物件名稱相同的任何本機設定 **Shared**（共用）物件。否則，升級後從 Panorama 推送的設定會失敗並顯示錯誤 `<object-name>` 已在使用中。

  這僅適用於使用略過軟體版本升級，從 PAN-OS 10.1 升級到 PAN-OS 11.1 的多重 vsys 防火牆。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 已修改您的安全性政策規則，以允許 `ssl` 應用程式流量。

> 這僅適用於使用略過軟體版本升級，從 *PAN-OS 10.1* 升級到 *PAN-OS 11.1* 的防火牆。
>
> 如果使用 *`panorama` App-ID* 來控制 *Panorama* 和受管理裝置之間的流量，則您必須這樣做，才能防止升級到 *PAN-OS 11.1* 後受管理裝置與 *Panorama* 中斷連線。如果升級前不允許使用 *`ssl`* 應用程式，受管理裝置將與 *Panorama* 中斷連線。

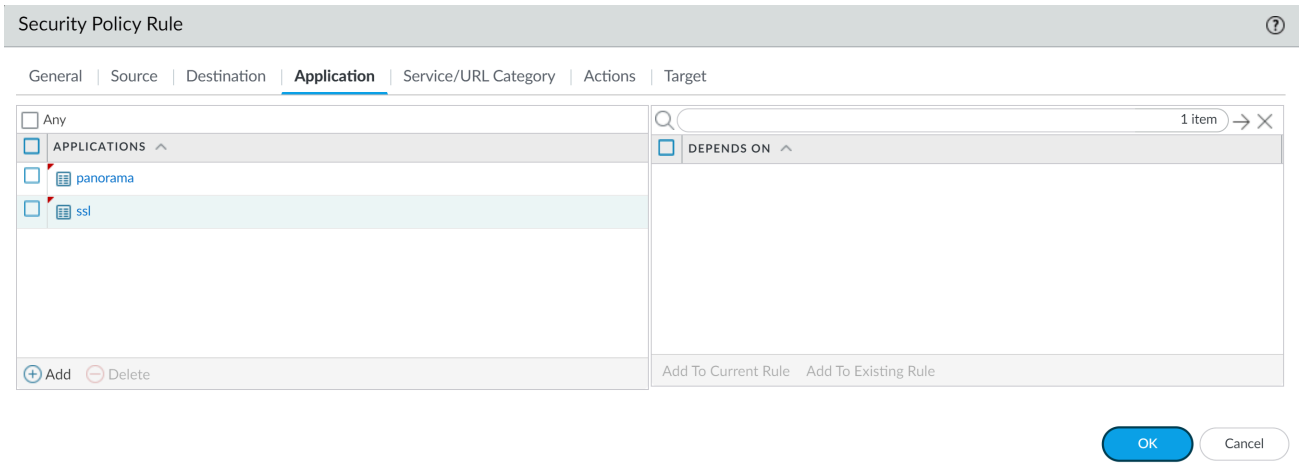
PAN-OS 11.1 會使用 TLS 版本 1.3 來加密 Panorama 與受管理防火牆之間的服務憑證和交握訊息。因此，從受管理防火牆到 Panorama 的流量的 App-ID 會從 `panorama` 重新分類為 `ssl`。

若要繼續 Panorama 和受管理裝置之間的通訊，您必須修改控制 Panorama 和受管理裝置之間流量的安全性政策規則，允許 `ssl` 應用程式。

如果控制 Panorama 和受管理裝置之間流量的安全性政策規則允許 **Any**（任何）應用程式，或者您已修改控制 Panorama 和受管理裝置之間流量的安全性政策規則，則請略過此步驟。

1. 選擇 **Policies**（政策） > **Security**（安全性） > **Pre Rules**（預先規則）。
2. 選擇包含控制 Panorama 和受管理防火牆之間流量的安全性政策規則的 **Device Group**（裝置群組）。
3. 選取安全性政策規則。
4. 選擇 **Application**（應用程式）並 **Add**（新增）`ssl`。

   不要刪除 *`panorama`* 應用程式。否則會導致所有受管理防火牆在您推送變更後與 *Panorama* 中斷連線。



5. 按一下 **OK**（確定）。
6. 選擇 **Commit**（提交） > **Commit and Push**（提交並推送）並 **Commit and Push**（提交並推送）您的設定變更。

STEP 3 | 在您打算升級的每個受管理的防火牆上，儲存目前組態檔案的備份。

雖然防火牆會自動建立設定備份，但最好在升級前建立備份並儲存在外部。

1. **Export Panorama and devices config bundle**（匯出 **Panorama** 和裝置設定組合）（**Panorama** > **Setup**（設定） > **Operations**（操作）），產生並匯出 Panorama 和每個受管理裝置的最新設定備份。
2. 將匯出的檔案儲存至防火牆外部的位置。如果您在升級時發生問題，便可使用此備份還原組態。

STEP 4 | 決定您需要安裝的內容更新。請參閱版本資訊，瞭解您必須為 PAN-OS® 版本安裝的最低內容發行版本。

Palo Alto Networks 高度建議 *Panorama*、日誌收集器和所有受管理的防火牆執行相同的內容發行版本。

針對每個內容更新，決定是否需要更新，並注意您需要下載下列步驟中的哪些內容更新。

請確定 *Panorama* 執行的內容發行版本，與受管理的防火牆和日誌收集器相同，但並不是更新的版本。

STEP 5 | 針對您想要更新至 Panorama 11.1 的防火牆，確定軟體升級路徑。

登入 Panorama，選取 **Panorama** > **Managed Devices**（受管理的裝置），並注意您想升級的防火牆的目前軟體版本。

檢閱 PAN-OS 升級檢查清單，瞭解您在升級路徑中會經過的每個版本的版本資訊和 升級/降級考量事項 中的已知問題和預設行為變更。

STEP 6 | （選用）將您受管理的防火牆升級至 PAN-OS 10.1。

略過軟體版本升級功能支援執行 PAN-OS 10.1 或更高版本的受管理防火牆。如果您的受管理防火牆執行的是 PAN-OS 10.0 或更早版本，請先升級至 PAN-OS 10.1 或更高版本。

STEP 7 | 執行版本的驗證檢查。

在此步驟中，您可以檢視升級至 11.1 所需的中間軟體和內容映像。

1. 選取 **Panorama** > **Device Deployment**（裝置部署） > **Software**（軟體） > **Action**（動作） > **Validate**（驗證）。
2. 檢視您需要下載的中間軟體和內容版本。

STEP 8 | 將內容和軟體更新下載到可透過 SCP 或 HTTPS 連線及上傳檔案至 Panorama 或設定的 SCP 伺服器的主機。

依預設，您可以將每種類型的最多兩個軟體或內容更新上傳至 Panorama 設備，如果您下載相同類型的第三個更新，Panorama 會刪除該類型最舊版本的更新。如果您需要上傳單一類型兩

個以上的軟體更新或內容更新，請使用 **set max-num-images count *<number>*** CLI 命令來增加 Panorama 可儲存的映像數目上限。

1. 使用可存取網際網路的主機登入 Palo Alto Networks 客戶支援網站。
2. 下載內容更新：
   1. 在 Resources（資源）部分中按一下 **Dynamic Updates**（動態更新）。
   2. **Download**（下載）最新的內容發行版本（或至少與您將安裝在 Panorama 管理伺服器上或其正在執行的版本相同或還要新），並將檔案儲存至主機；針對您需要更新的每種內容類型，重複此步驟。
3. 下載軟體更新：
   1. 返回 Palo Alto Networks 客戶支援網站的主頁面，然後在 Resources（資源）部分中按一下 **Software Updates**（軟體更新）。
   2. 檢閱下載欄以決定您需要安裝的版本。更新套件的檔案名稱會指出型號。例如，若要將 PA-440 和 PA-5430 防火牆升級至 PAN-OS 11.1.0，請下載 `Pan0S_440-11.1.0` 和 `Pan0S_5430-11.1.0` 映像。

      您可以從 ***Filter By***（篩選依據）下拉式清單中選取 ***PAN-OS for the PA***（適用於 ***PA*** 的 ***PAN-OS***）*-<series/model>*，快速找到特定的 *PAN-OS* 映像。
4. 按一下適當的檔名，並將檔案儲存至主機。

STEP 9 | 下載中間軟體版本和最新的內容版本。

在 PAN-OS 11.0 上，您可以使用多映像下載功能來下載多個中間版本。

1. 選取要升級的防火牆（**Required Deployments**（所需部署） > **Deploy**（部署））。
2. 選取下載來源並按一下 **Download**（下載）。

STEP 10 | 在受管理的防火牆上安裝內容更新。

您必須先安裝內容更新，再安裝軟體更新。

先安裝「應用程式」或「應用程式和威脅」更新，再依需要、一次一個、以任意順序安裝其他任何更新（防毒、WildFire® 或 URL 篩選）。

1. 選取 **Panorama** > **Device Deployment**（設備部署） > **Dynamic Updates**（動態更新）。
2. 按一下 **Upload**（上傳），選取更新 **Type**（類型），**Browse**（瀏覽）至適當的內容更新檔案，然後按一下 **OK**（確定）。
3. 按一下 **Install From File**（從檔案安裝），選取更新 **Type**（類型），並選取您剛上傳的內容更新的 **File Name**（檔案名稱）。
4. 選取您要安裝更新的防火牆。
5. 按一下 **OK**（確定）以啟動安裝。
6. 針對每個內容更新重複這些步驟。

STEP 11 | （僅限當作 GlobalProtect™ 入口網站的防火牆）將 GlobalProtect 代理程式/應用程式軟體更新上傳至防火牆並啟動。

您可在防火牆上啟動更新，供使用者下載至其端點（用戶端系統）。

1. 使用可存取網際網路的主機登入 Palo Alto Networks 客戶支援網站。
2. 下載適當的 GlobalProtect 代理程式/應用程式軟體更新。
3. 在 Panorama 上，選取 **Panorama** > **Device Deployment**（裝置部署） > **GlobalProtect Client**（**GlobalProtect** 用戶端）。
4. 按一下 **Upload**（上傳），在您已下載檔案的主機上 **Browse**（瀏覽）至適當的 GlobalProtect 代理程式/應用程式軟體更新，然後按一下 **OK**（確定）。
5. 按一下 **Activate From File**（從檔案啟動），選取您剛上傳的 GlobalProtect 代理程式/應用程式更新的 **File Name**（檔案名稱）。

   您一次只能啟動一個版本的代理程式/應用程式軟體。如果您啟動新版本，但某些代理程式需要上一個版本，則您必須再次重新啟動舊版本，讓這些代理程式下載上一個更新。
6. 選取要啟動更新的防火牆。
7. 按一下 **OK**（確定）以啟動。

STEP 12 | 安裝 PAN-OS 11.1。

若要避免在高可用性 *(HA)* 防火牆上更新軟體時的停機時間，每次更新一個 *HA* 端點。

對於主動/主動防火牆，更新端點的順序無關緊要。

對於主動/被動防火牆，您必須先更新被動端點，暫停主動端點（故障復原），更新主動端點，然後將主動端點返回至功能狀態（故障復原）。

（僅限 *SD-WAN*）要保持 *SD-WAN* 連結的準確狀態，在升級分支防火牆之前，您必須將中樞防火牆升級至 *PAN-OS 11.1*。如果先升級分支防火牆之後才升級中樞防火牆，可能產生錯誤監控資料（***Panorama*** > ***SD-WAN*** > ***Monitoring***（監控）），且 *SD-WAN* 連結會錯誤顯示為關閉。

1. 執行適用於您的防火牆組態的步驟，以安裝您剛上傳的 PAN-OS 軟體更新。
   - **Non-HA firewalls**（非 HA 防火牆）——按一下行動欄內的 **Install**（安裝），選取您正在升級的所有防火牆，選取 **Reboot device after install**（安裝後重新開機設備），然後按一下 **OK**（確定）。
   - 主動式/主動式 **HA** 防火牆：
     1. 在您想要升級的第一個對等上，確認先佔設定已停用（**Device**（裝置） > **High Availability**（高可用性） > 選取設定）。如果已啟用，請編輯 **Election Settings**（選取設定），停用（清除） **Preemptive**（先佔）設定，然後

Commit（提交）您的變更。您只需要在每個 HA 配對中的一個防火牆上停用此設定，但要確定提交成功之後再繼續。

2. 按一下 **Install**（安裝），停用（清除）**Group HA Peers**（群組 **HA** 對等），選取任一 HA 對等，選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 **OK**（確定）。繼續之前，等候防火牆完成重新開機。
3. 按一下 **Install**（安裝），停用（清除）**Group HA Peers**（群組 **HA** 對等），選取您在上一步未更新的 HA 對等、選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 **OK**（確定）。

- **Active/passive HA firewalls**（主動式/被動式 **HA** 防火牆）—在此範例中，主動式防火牆名稱為 fw1 而被動式防火牆名稱為 fw2：
  1. 在您想要升級的第一個對等上，確認先佔設定已停用（**Device**（裝置） > **High Availability**（高可用性） > 選取設定）。如果已啟用，請編輯 **Election Settings**（選取設定），停用（清除） **Preemptive**（先佔）設定，然後 **Commit**（提交）您的變更。您只需要在每個 HA 配對中的一個防火牆上停用此設定，但要確定提交成功之後再繼續。
  2. 在適當更新的動作欄中按一下 **Install**（安裝）、停用（清除）**Group HA Peers**（群組 **HA** 對等）、選取 fw2，選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 **OK**（確定）。繼續之前，請等候 fw2 完成重新開機。
  3. fw2 完成重新開機後，在 fw1 上確認（**Dashboard**（儀表板） > 高可用性）fw2 仍然是被動式對等（本機防火牆狀態為主動，而對等—fw2—為被動）。
  4. 存取 fw1 並暫停本機裝置（**Device**（裝置） > **High Availability**（高可用性） > **Operational Commands**（操作命令））。
  5. 存取 fw2（**Dashboard**（儀表板） > 高可用性），確認本機防火牆狀態為主動，對等為暫停。
  6. 存取 Panorama，選取 **Panorama** > **Device Deployment**（裝置部署） > **Software**（軟體），在適當版本的動作欄中按一下 **Install**（安裝）、停用（清除）**Group HA Peers**（群組 **HA** 對等）、選取 fw1、選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 [OK（確定）]。繼續之前，請等候 fw1 完成重新開機。
  7. 存取 fw1（**Device**（裝置） > **High Availability**（高可用性） > **Operational Commands**（操作命令）），按一下 **Make local device functional**（讓本機裝置運作），然後在您繼續之前稍等兩分鐘。
  8. 在 fw1 上（**Dashboard**（儀表板） > 高可用性），確認本機防火牆狀態為被動，對等 (fw2) 為主動。

STEP 13 | （僅限 FIPS-CC 模式）在 FIPS-CC 模式下升級 Panorama 和受管理的裝置

如果在受管理的防火牆執行 PAN-OS 11.1 版本時將專用日誌收集器新增至 Panorama 管理中，則在 FIPS-CC 模式下升級受管理的防火牆需要重設安全連線狀態。

當受管理的防火牆執行 PAN-OS 10.0 或更早版本時，您無需重新裝載新增至 Panorama 管理的受管理防火牆。

STEP 14 | 驗證各受管理的防火牆上安裝的軟體和內容版本。

1. 選取 **Panorama** > **Managed Devices**（受管理的裝置）。
2. 找到防火牆，並檢閱 Software Version（軟體版本）、Apps and Threat（應用程式與威脅）、Antivirus（防毒）、URL Filtering（URL 篩選）及 GlobalProtect Clien（GlobalProtect 用戶端） 欄中的值。

STEP 15 | 如果您在升級之前在其中一個 HA 防火牆上停用先佔，請編輯 **Election Settings**（選取設定）（**Device**（裝置） > **High Availability**（高可用性）），針對該防火牆重新啟用 **Preemptive**（先佔） 設定。

STEP 16 | 在 Panorama 網頁介面上，將整個 Panorama 受管理設定推送至您的受管理防火牆。

需要執行此步驟以選擇性提交並推送 Panorama 上的裝置群組和範本堆疊設定變更至受管理的防火牆。

需要執行此步驟以在成功升級到 PAN-OS 11.1 後，成功地將設定變更推送至由 Panorama 管理的多重 vsys 防火牆。如需詳細資訊，請參閱由 Panorama 管理的多重 vsys 防火牆的 共用設定物件的預設行為變更。

1. 選取 **Commit**（提交） > **Push to Devices**（推送至裝置）。
2. **Push**（推送）。

STEP 17 | 重新產生或重新匯入所有憑證以遵守 OpenSSL 安全性等級 2。

在升級到 PAN-OS 11.1 時，要求所有憑證滿足以下最低要求：

- RSA 2048 位元或以上，或 ECDSA 256 位元或以上
- SHA256 或更高版本的摘要

請參閱 PAN-OS 管理員指南或 Panorama 管理員指南，瞭解有關重新產生或重新匯入憑證的更多資訊。

STEP 18 | 檢視防火牆的軟體升級歷程記錄。

1. 登入 Panorama 介面。
2. 前往 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要）並按一下 **Device History**（裝置歷程記錄）。

升級 ZTP 防火牆

成功新增 ZTP 防火牆至 Panorama™ 管理伺服器後，設定 ZTP 防火牆的目標 PAN-OS 版本。首次成功連線至 Panorama 後，Panorama 會檢查 ZTP 防火牆上安裝的 PAN-OS 版本是否比所設定目標 PAN-OS 版本更新或相同。如果 ZTP 防火牆上安裝的 PAN-OS 版本比目標 PAN-OS 版本更舊，則 ZTP 防火牆進行升級循環，直到安裝目標 PAN-OS 版本。

STEP 1 | 作為管理員使用者登入 Panorama 網頁介面。

STEP 2 | 新增 ZTP 防火牆至 Panorama。

STEP 3 | 選取 **Panorama** > **Device Deployment**（裝置部署） > **Updates**（更新）和 **Check Now**（立即檢查）以獲得最新 PAN-OS 版本。

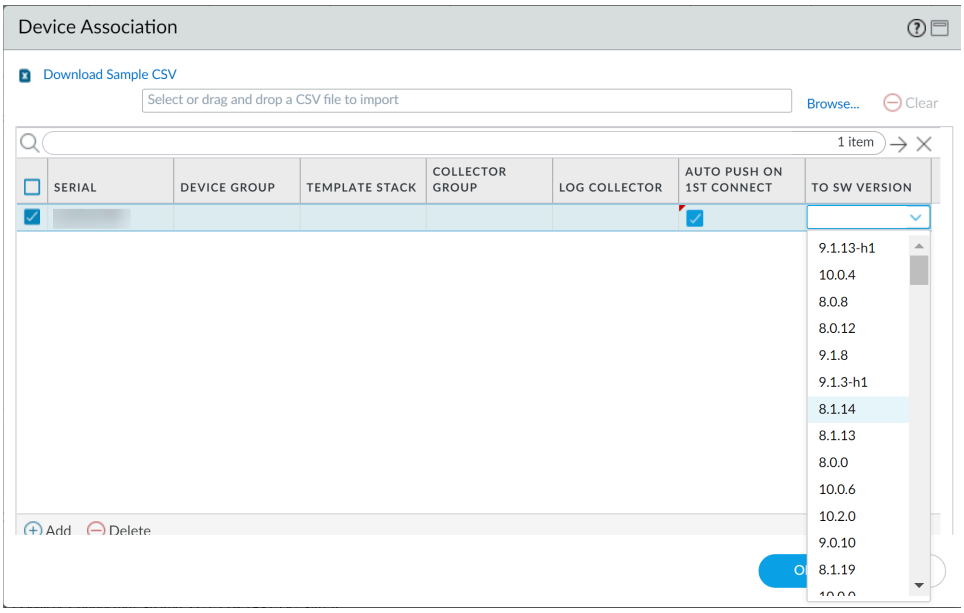
STEP 4 | 選取 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要）並選取一或多個 ZTP 防火牆。

STEP 5 | **Reassociate**（重新關聯）所選取 ZTP 防火牆。

STEP 6 | 核取（啟用） **Auto Push on 1st Connect**（第 **1** 次連線時自動推送）。

STEP 7 | 在 **To SW Version**（至軟體版本）欄中，選取 ZTP 防火牆的目標 PAN-OS 版本。

STEP 8 | 按一下 **OK**（確定）儲存組態變更。



STEP 9 | 按一下 **Commit**（提交） 和 **Commit to Panorama**（提交至 **Panorama**）。

STEP 10 | 開啟 ZTP 防火牆。

當 ZTP 防火牆首次連線至 Panorama 時，會自動升級至您選取的 PAN-OS 版本。

- 執行 **PAN-OS 11.1.0** 的 **Panorama**— 如果您要跨 PAN-OS 主要版本或維護版本升級受管理的防火牆，則在安裝目標 PAN-OS 版本之前，先安裝升級路徑上的中間 PAN-OS 版本。

  例如，您將受管理防火牆的目標 **To SW Version**（至軟體版本）設定為 PAN-OS 11.1.0，並且防火牆正在執行 PAN-OS 10.2。首次連線至 Panorama 時，首先會在受管理的防火牆上安裝 PAN-OS 11.0.0。PAN-OS 11.0.0 成功安裝後，防火牆會自動升級至目標 PAN-OS 11.1.0 版本。

- 執行 **PAN-OS 11.0.1** 及更高版本的 **Panorama**—如果您正在跨 PAN-OS 主要版本或維護版本升級受管理的防火牆，則會先安裝升級路徑上的中間 PAN-OS 主要版本並下載基本 PAN-OS 主要版本，然後才安裝目標 PAN-OS 維護版本。

  例如，您將受管理防火牆的目標 **To SW Version**（至軟體版本）設定為 11.0.1，並且防火牆正在執行 PAN-OS 10.0。首次連線至 Panorama 時，首先會在受管理的防火牆上安裝 PAN-OS 10.1.0 和 PAN-OS 10.2.0。受管理的防火牆重新啟動後，將下載 PAN-OS 11.0.0，然后防火牆會自動安裝到目標 PAN-OS 11.0.1 版本。

STEP 11 | 確認 ZTP 防火牆軟體升級。

1. 登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要）並導覽至 ZTP 防火牆。
3. 確認 **Software Version**（軟體版本）欄中顯示正確的目標 PAN-OS 版本。

STEP 12 | 有關所有未來的 PAN-OS 升級，請參閱 將防火牆從 Panorama 升級至 PAN-OS 11.1。

安裝 PAN-OS 軟體修補程式

這可在何處使用？	我需要哪些內容？
• Panorama 管理的新世代防火牆 不支援 CN-Series 防火牆 • Panorama 管理的 WildFire 設備	❑ 裝置管理授權 ❑ 支援授權 ❑ PAN-OS 11.1.3 或更新 11.1 版本 ❑ 輸出網際網路存取權

查看 PAN-OS 11.1 版本資訊，然後使用下列程序安裝 PAN-OS 軟體修補程式，以解決目前在 Panorama™ 管理伺服器的受管理裝置上執行的 PAN-OS 版本錯誤及常見弱點和暴露 (CVE)。安裝 PAN-OS 軟體修補程式時會套用錯誤和 CVE 的修正程式，而無需安排長時間進行維護，並可讓您立即強化安全狀態，避免引入任何新的已知問題或變更安裝新 PAN-OS 版本可能產生的預設行為。此外，您也可以復原目前安裝的軟體修補程式，以解除安裝軟體修補程式時套用的錯誤和 CVE 修正程式。

安裝或復原 PAN-OS 軟體修補程式時會產生系統日誌（**Monitor**（監控） > **Logs**（日誌） > **System**（系統））。必須有輸出網際網路連線才能從 Palo Alto Networks 客戶支援入口網站下載 PAN-OS 軟體修補程式。如果是氣隙受管理裝置，Panorama 仍必須具有網際網路存取權才能下載 PAN-OS 軟體修補程式，但安裝並將其套用於受管理裝置時，則不需要輸出網際網路連線。

- 安裝
- 還原

安裝

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Panorama** > **Device Deployment**（裝置部署） > **Software**（軟體）和 **Check Now**（立即檢查），從 Palo Alto Networks 更新伺服器檢索最新的 PAN-OS 軟體修補程式。

STEP 3 | 選取（啟用）**Include Patch**（包含修補程式）以顯示所有可用的 PAN-OS 軟體修補程式。

STEP 4 | 尋找目前安裝在受管理裝置上的 PAN-OS 版本的軟體修補程式。

軟體修補程式由 **Version**（版本）名稱旁邊顯示的修補程式標籤表示。

STEP 5 | 查看 **More Info**（更多資訊），以檢視軟體修補程式詳細資訊，例如重要錯誤和 CVE 修正程式，以及是否需要重新啟動受管理裝置才能套用修正項目。

STEP 6 | **Download**（下載）軟體修補程式。

（僅 HA）選取（啟用）同步至 HA 對等並 **Continue Download**（繼續下載）以下載 PAN-OS 軟體修補程式。

軟體修補程式下載成功後按一下 **Close**（關閉）。

STEP 7 | **Install**（安裝）軟體修補程式。

軟體修補程式安裝成功後，按一下 **Close**（關閉）。

STEP 8 | 選擇您要安裝 PAN-OS 軟體修補程式的受管理裝置，然後按一下 **OK**（確定）。

（僅 HA）如果要在高可用性 (HA) 設定中的一對受管理裝置上安裝軟體修補程式，則必須在兩個 HA 對等上選擇並安裝軟體修補程式。

STEP 9 | **Apply**（套用）軟體修補程式。

當系統提示您確認要將已安裝的 PAN-OS 軟體修補程式套用到受管理裝置時，請按 **Apply**（套用）。

系統將顯示狀態欄，顯示 PAN-OS 軟體修補程式應用程式的目前進度。修補程式成功套用後，按一下 **Close**（關閉）。

此時如果需要重新啟動才能將 PAN-OS 軟體修補程式套用到受管理裝置，則防火牆會自動重新啟動。

還原

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Panorama** > **Device Deployment**（裝置部署） > **Software**（軟體）和 **Check Now**（立即檢查），從 Palo Alto Networks 更新伺服器檢索最新的 PAN-OS 軟體修補程式。

STEP 3 | **Revert**（還原）軟體修補程式。

STEP 4 | 選擇您要還原 PAN-OS 軟體修補程式的受管理裝置，然後按一下 **OK**（確定）。

僅顯示符合條件的受管理裝置。

（僅 HA）如果要在高可用性 (HA) 設定中的一對受管理裝置上安裝軟體修補程式，則必須在兩個 HA 對等上選擇並安裝軟體修補程式。

STEP 5 | 當系統提示您確認要從所選受管理裝置還原安裝的 PAN-OS 軟體修補程式時，請按 **Revert**（還原）。

系統將顯示狀態欄，顯示 PAN-OS 軟體修補程式應用程式的目前進度。修補程式成功套用後，按一下 **Close**（關閉）。

此時如果需要重新啟動才能將 PAN-OS 軟體修補程式套用到 Panorama，則防火牆會自動重新啟動。

從 Panorama 復原內容更新

Panorama™ 讓您可以快速復原直接來自 Panorama 的一個或多個防火牆、日誌收集器或 WildFire 設備上的應用程式、應用程式與威脅、防毒、WildFire® 和 WildFire 內容版本。使用 Panorama 復原安裝中受管理的裝置上的內容版本，以利用集中化的工作流程，協助轉移任何與應用程式導入或修改，或內容更新中新威脅特徵碼相關的風險。當您復原內容時，Panorama 會為每個裝置生成一個系統日誌。在將內容更新部署到受管理的裝置時確保使用 應用程式與威脅內容更新的最佳做法。

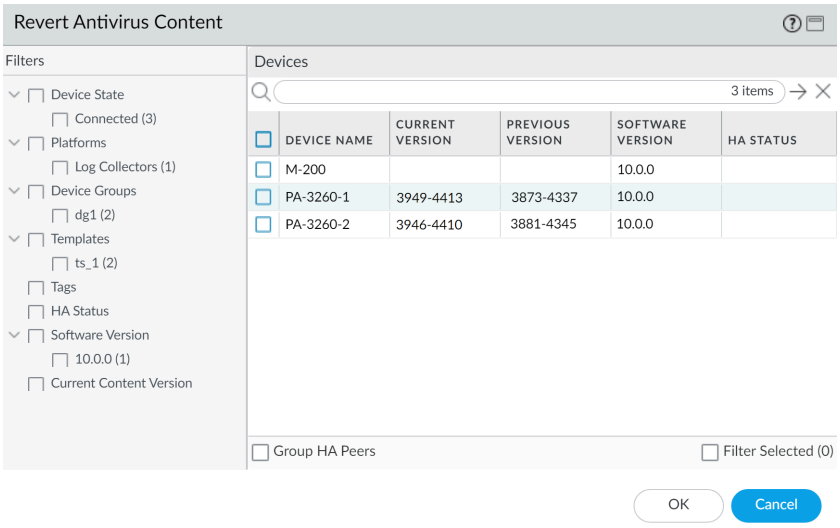
STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 選取 **Panorama** > **Device Deployment**（設備部署） > **Dynamic Updates**（動態更新）和 **Revert Content**（復原內容）。

STEP 3 | 選取您需要復原的內容類型。

Antivirus
Apps
Applications and Threats
WildFire
WildFire-Content

STEP 4 | 選取要復原其上內容的一個或多個防火牆，然後按一下 **OK**（確定）。您復原的內容版本必須早於目前安裝在裝置上的版本。



升級 PAN-OS

PAN-OS 升級檢查清單

規劃 PAN-OS 升級有助於確保 Panorama 或防火牆更順暢地轉換為較新版本的 PAN-OS。

- 確保裝置已註冊且獲得了授權。
- 確認可用的磁碟空間。

  所需的磁碟空間會因 PAN-OS 版本而有所不同。選取 **Device**（裝置） > **Software**（軟體），然後檢視目標 PAN-OS 版本大小以確定所需磁碟空間。

  - 執行 **`show system disk-space`**
- 確認最低內容發行版本。
- 確定慣用的版本。

  - （PAN-OS 11.1.3 及更新版本）

    選取 **Device**（裝置） > **Software**（軟體）。根據預設，「發佈類型」欄位會顯示慣用版本和基礎版本。若要僅查看慣用版本，請停用（清除）**Base Releases**（基礎版本）核取方塊。
  - （PAN-OS 11.1.3 及更新版本）

    執行慣用的要求系統軟體訊息

  如需詳細資訊，請參閱 Palo Alto Networks 支援軟體版本指南和生命週期結束摘要。此外，請檢閱目標 PAN-OS 版本的已知且已解決問題、升級與降級考量事項以及限制，以瞭解 PAN-OS 升級可能會對您造成的影響。
- 決定升級路徑。

  當您從一個 *PAN-OS* 功能發行版本升級至更新的功能版本時，您無法略過前往目標版本的路徑中任何功能發行版本的安裝。
- 檢閱升級路徑中所有版本的升級/降級考量事項。
- （需要 GlobalProtect）確認 GlobalProtect™ 代理程式的最低版本，以防止 GlobalProtect 使用者遺失 VPN 連線。GlobalProtect 可直接升級至最新版本。
- 確認您已安裝的任何外掛程式的目標發行版本的最低外掛程式版本。
- 確認從管理介面到更新伺服器的連線性。

  - 選取 **Device**（裝置） > **Troubleshooting**（疑難排解），測試 **Update Server Connectivity**（更新伺服器連線性）以確認 DNS 能夠解析位址。

    如果無法解析，請將 DNS 變更為 **`8.8.8.8`**（您需要使用公用 DNS 伺服器而非您自己的 DNS 伺服器），然後再次執行 Ping。

    如果這無法解決問題，請將更新伺服器變更為 **`staticupdates.paloaltonetworks.com`**，然後 **Commit**（提交）。
- （僅限 SD-WAN）確定您計劃升級至 PAN-OS 11.1 的中樞和分支防火牆。

  要保持 SD-WAN 連結的準確狀態，在升級分支防火牆之前，您必須先將中樞防火牆升級至 PAN-OS 11.1。在中樞防火牆之前升級分支防火牆可能會產生錯誤的監控資料（**Panorama** > **SD-WAN** > **Monitoring**（監控）），且 SD -WAN 連結會錯誤地顯示為 down（關閉）。

- 如果目前安裝了任何外掛程式，請在升級前為目前 Panorama （**Panorama** > **Plugins**（外掛程式））或防火牆（**Device**（裝置） > **Plugins**（外掛程式））上安裝的所有外掛程式下載 PAN-OS 11.1 支援的外掛程式版本。

  有關 PAN-OS 11.1 支援的 Panorama 外掛程式版本，請參閱 Panorama 外掛程式相容性矩陣。

  需要執行此步驟以成功地將 Panorama 和防火牆升級至 PAN-OS 11.1。下載的外掛程式版本會在升級至 PAN-OS 11.1 期間自動安裝。如果未下載支援的外掛程式版本，將封鎖升級至 PAN-OS 11.1。

升級/降級考量事項

以下表格列出了具有升級或降級影響的新功能。在從 PAN-OS 11.1 版本升級至或降級之前，請確保瞭解全部升級/降級考量事項。如需有關 PAN-OS 11.1 和更新版本的其他資訊，請參閱 PAN-OS 版本資訊。

功能	升級考量事項	降級考量事項
具動態指派 IPv6 位址首碼的 NPTv6	無。	降級到 PAN-OS 11.1.5 之前的版本時，請先在具動態指派 IPv6 位址的介面上停用 NPTv6 或移除設定。（PAN-OS 11.1.5 到 11.1.0 之間不可封鎖降級，因此映像降級成功，但自動提交會失敗。）
重疊 IP 位址支援	無。	啟用重複的 IP 位址支援時，系統會封鎖降級到 PAN-OS 11.1.4 之前的版本的嘗試。降級嘗試一旦出現便會顯示錯誤訊息， 降級失敗。較舊版本不支援重複的 IP 位址。請移除所有重複的 IP 位址設定，停用重複的 IP 位址支援，並在繼續降級之前進行提交。
進階路由引擎 (PAN-OS 11.2.0)	在 PAN-OS 11.2.0 中，啟用進階路由時則不支援 IP 多點傳送。即將推出的新版本將提供此功能的支援。已設定多點傳送或計劃部署多點傳送的客戶不應升級到 11.2.0。 此外，在 PAN-OS 11.2.0 中啟用進階路由後，BGP 抑制設定不會套用於任何對等或對等群組；設定將受保留，但對 BGP 沒有影響。即使客戶已將抑制設定檔套用於特定一組對等，客戶也可以使用 BGP。此問題不會影響任何其他 BGP 功能。	無
使用序號和 IP 位址方法驗證 LSVPN 衛星	PAN-OS 會將設定變更儲存在內部資料庫。因此，當您升級	• 如果您降級到 PAN-OS 10.1 及更高版本，則系統

功能	升級考量事項	降級考量事項
（PAN-OS 11.1.3 和更新版本）	到此功能時，系統會套用最新儲存的設定。 從 PAN-OS 10.0 或更舊版本升級到 PAN-OS 10.1 及更新版本（已啟用使用者名稱/密碼和衛星 Cookie 驗證方法）後，衛星 Cookie 到期將導致登入失敗。 在此情況下，您應該輸入使用者名稱和密碼才能成功驗證。	僅支援使用者名稱/密碼和衛星 Cookie 驗證方法。 • 如果您下載並安裝了外掛程式的次要版本，然後決定降級到同一版本的另一個次要版本，則降級前在次要版本上所做的設定將在同一版本的降級次要版本上生效。 PAN-OS 會將設定變更儲存在內部資料庫。因此，當您從此功能降級時，系統會套用最新儲存的設定。 例如，如果您已使用設定（設定 1）安裝了 SD-WAN 外掛程式 11.1.5，然後決定降級到同一版本的另一個次要版本，即具有不同設定的 11.1.4（設定 2）。此時，次要版本（降級前）的設定（設定 1）將在降級後的次要版本 11.1.4 上生效。
	從 PAN-OS 10.0 或更舊版本/PAN-OS 10.1 及更新版本升級到 PAN-OS 11.1.3 之後，請考慮以下事項： • 如果您停用序號和 IP 位址驗證方法且衛星 Cookie 到期將導致登入失敗。在此情況下，管理員應該輸入使用者名稱和密碼才能成功驗證。 • 如果您已啟用序號和 IP 位址驗證方法且衛星序號已在 GlobalProtect 入口網站中註冊，IP 位址存在於 IP 允許清單中，則能成功登入。 • 如果您已啟用序號和 IP 位址驗證方法但衛星序號尚	• 如果您降級到 10.1 之前的 PAN-OS 版本，則系統僅支援序號驗證方法。 • 如果您降級到 10.1 和 10.2.8 之間的 PAN-OS 版本，則系統支援使用者名稱/密碼和衛星 Cookie 驗證方法。 • 如果您降級到 PAN-OS 10.2.8 和更新 10.2 版本，則系統同時支援「使用者名稱/密碼和衛星 Cookie 驗證」和「序號和 IP 位址驗證」方法。

功能	升級考量事項	降級考量事項
	未在 GlobalProtect 入口網站中註冊，或 IP 位址不存在於 IP 允許清單中，則將導致登入失敗。在此情況下，防火牆不會回復到任何其他驗證方法，且會導致驗證失敗。如果驗證失敗，衛星會等待設定的重試間隔過後再次進行驗證。請確保衛星序號已正確註冊到入口網站且衛星 IP 位址存在於 IP 允許清單中，才能成功進行驗證。	
每個政策的 Persistent DIPP	使用 Panorama 將防火牆從 PAN-OS 11.0.0 升級到 11.1.1 時，一般 DIPP NAT 規則應轉換為 Persistent DIPP NAT 規則，但該轉換作業失敗，規則仍為一般 DIPP NAT 規則。	使用 Panorama 將防火牆從 PAN-OS 11.1.1 降級到 11.0 0 時，每個政策的 Persistent DIPP NAT 規則將轉換為一般 DIPP NAT 規則。
TLSv1.3 支援 GlobalProtect	如果從更舊 PAN-OS 版本升級到 PAN-OS 11.1，且在 SSL/TLS 服務設定檔將 **Max Version**（最高版本）設為 **Max**（最高），則升級後 TLS 版本將替換為 TLSv1.2。 如果從 PAN-OS 11.1 升級到更新 PAN-OS 版本，且在 SSL/TLS 服務設定檔將 **Max Version**（最高版本）設為 **<TLS Version>**，則升級後 TLS 版本將保留為設定的 **<TLS Version>**。由於版本已在 11.1.x 中進行設定，因此無需替換版本。	如果您使用 TLSv1.3 從 PAN-OS 11.1 降級到較舊的 PAN-OS 版本，降級後 TLSv1.3 將替換為 TLSv1.2。如果您在 PAN-OS 11.1 選擇了較舊 PAN-OS 版本不支援的 TLS v1.3 **aes-chacha20-poly1305** 密碼，則降級會成功但自動提交會失敗。您必須為降級版本新增或替換適當的支援密碼，並手動提交變更。
升級 VM-50 和 VM-50L	將 VM-50 或 VM-50L 防火牆升級至 PAN-OS 11.1 之前，您需要先安裝最低外掛程式版本，然後再開始升級： • 從 **PAN-OS 10.2** 升級—所需的最低外掛程式版本為 3.0.6	無。

功能	升級考量事項	降級考量事項
	• 從 **PAN-OS 11.0** 升級—所需的最低外掛程式版本為 4.0.3-h1。	
VM-Series 防火牆	將 VM-Series 防火牆從 PAN-OS 版本 10.1.x 升級到 11.1.x 時，您必須在所有 10.1.x 防火牆上將 VM-Series 外掛程式版本升級到 2.1.6 以上，然後再執行升級，以避免 HA 問題。	無。
收集器群組	升級到 PAN-OS 11.1.1 時，執行 PAN-OS 10.0 或更舊版本時產生的所有日誌都會遭刪除。 若要復原在 PAN-OS 11.0 或更舊版本產生的日誌，您必須升級至 PAN-OS 11.1.2 或更新版本；您可以使用 Palo Alto Networks 提供的 CLI 命令手動復原所有受影響的日誌。	不建議您降級。如果您選擇從 11.1 降級，則 PAN-OS 11.1 產生的所有日誌都將遭刪除且需要手動復原。若要復原 11.1 產生的日誌，您必須： 1. 升級到 PAN-OS 11.1.2 或更新 11.1 版本。 您必須這麼做才能復原受影響的日誌。 2. 登入日誌收集器 CLI 並刪除所有 `esdata` 目錄。 `admin>` **`debug elasticsearch erase`** 資料 3. 降級到您的目標 PAN-OS 版本。 4. 將變更提交並推送至收集器群組和所有受管理的裝置。 5. 登入日誌收集器 CLI 並復原受影響的日誌。 `admin> debug logdb migrate-lc start log-type all`

功能	升級考量事項	降級考量事項
		如果您已從 *PAN-OS 11.1* 降級且 *ElasticSearch* 陷入重啟循環，請聯絡 Palo Alto Networks 支援部門
	收集器群組中的所有日誌收集器必須同時升級。系統不支援升級期間在收集器群組中升級部分（非全部）日誌收集器。	無。
	執行 PAN-OS 11.1 的日誌收集器必須以裝置註冊驗證進行日誌收集器之間的通訊。 在 PAN-OS 11.1 的升級路徑中，執行 PAN-OS 9.1 或更舊版本時新增至 Panorama 管理的日誌收集器必須先升級到 PAN-OS 10.1 或更新版本，並以裝置註冊驗證金鑰重新裝載到 Panorama 管理。 如果系統偵測到日誌收集器在沒有裝置註冊驗證金鑰的情況下裝載到 Panorama 管理，則系統會封鎖到 PAN-OS 11.1 的升級作業。	無。
	如果您使用收集器群組，則必須滿足以下條件才能升級至 11.1.0。 • 升級至 11.1 後，您必須手動推送收集器群組才能升級受管理日誌收集器。 *PAN-OS* 會要求收集器群組內的所有日誌收集器都具備相同版本。	無。

功能	升級考量事項	降級考量事項
	• 您必須以裝置註冊驗證金鑰向 Panorama 註冊日誌收集器。 如果裝置註冊驗證金鑰未正確初始化，則無法與對等節點建立連線。	
	將日誌收集器升級到 PAN-OS 11.1 之後，日誌收集器之間的通訊便需要以下 TCP 連接埠，且必須在網路上開啟。 • TCP/9300 • TCP/9301 • TCP/9302	無。
Pan 服務 Proxy	無。	如果啟用 Pan 服務 Proxy，則從 PAN-OS 11.1 到新世代防火牆的降級作業會失敗。若要成功降級，請在降級之前停用 Pan 服務 Proxy。 新世代防火牆：選取 **Network**（網路） > **Proxy**，按一下 [Proxy Enablement（Proxy 啟用）] 的設定圖示，選取 **None**（無）然後按一下 **OK**（確定）。 Panorama:**Templates**（範本） > **Network**（網路） > **Proxy**，按一下 [Proxy Enablement（Proxy 啟用）] 的設定圖示，選取 **None**（無）然後按一下 **OK**（確定）。
驗證順序	升級至 PAN-OS 11.1.1 時，**domain to determine authentication profile**（使用網域決定驗證設定檔）選項不再控制 **Exit the sequence on**	如果您選取 **Exit the sequence on failed authentication**（驗證失敗時退出序列）選項，就無法從 PAN-OS 11.1.1 降級到更舊版本，除非取消選取

功能	升級考量事項	降級考量事項
	failed authentication（驗證失敗時退出序列）選項。	**Exit the sequence on failed authentication**（驗證失敗時退出序列）選項，或除非同時選取 **Exit the sequence on failed authentication**（驗證失敗時退出序列）和 **Use domain to determine authentication profile**（使用網域決定驗證設定檔）選項。
多重 vsys 防火牆的 Panorama 管理 使用略過軟體版本升級，從 PAN-OS 10.1 升級到 PAN-OS 11.1。	使用略過軟體版本升級將 Panorama 受管理的多重 vsys 防火牆升級到 PAN-OS 11.0 之前： • 刪除或重新命名與 **Panorama Shared**（**Panorama** 共用）設定中的物件名稱相同的任何本機設定防火牆 **Shared**（共用）物件。否則，升級後從 Panorama 推送的設定會失敗並顯示錯誤 `<object-name>` 已在使用中。 • Palo Alto Networks 建議，如果多重 vsys 防火牆由 Panorama 管理，則所有 vsys 設定也應由 Panorama 管理。 這麼一來能避免受管理多重 vsys 防火牆上的提交作業失敗，並讓您能運用 Panorama 的最佳化共用物件推送。	無。
	使用略過軟體版本升級成功將受管理多重 vsys 防火牆升級到 PAN-OS 10.2 之後，防火牆在 Panorama 上會變得不同步，需要完全提交和推送。 在 Panorama 將整個 Panorama 受管理設定 **Commit**（提交）並 **Push to Devices**（推送至裝置）到	

功能	升級考量事項	降級考量事項
	多重 vsys 防火牆，然後再從 Panorama 提交並推送任何設定變更。	
（PAN-OS 11.2）啟動 HSM 與 SSL 輸入檢查整合的 TLSv1.3 支援	無。	當內部伺服器的私密金鑰儲存在 HSM 時，從 PAN-OS 11.2 降級到較舊版本的降級作業中將移除建立和解密 TLSv1.3 工作階段的支援。即使客戶端和伺服器都支援 TLSv1.3，裝置也會建立 TLSv1.2 連線。

將防火牆升級到 PAN-OS 11.1

升級到 PAN-OS 11.1 的方式取決於您是擁有獨立防火牆還是高可用性 (HA) 設定中的防火牆，以及對於任一種情況，您是否使用 Panorama 來管理您的防火牆。檢閱 PAN-OS 11.1 版本資訊，然後遵循特定於部署的程序：

- 確定升級到 PAN-OS 11.1 的路徑
- 將防火牆從 Panorama 升級至 PAN-OS 11.1
- 升級獨立防火牆
- 升級 HA 防火牆配對

當升級使用 *Panorama* 管理的防火牆或設定為轉送內容到 *WildFire* 設備的防火牆時，您必須先升級 Panorama 及其日誌收集器，然後升級 WildFire 設備，之後再升級防火牆。

另外，不建議管理執行維護版本比 *Panorama* 晚的防火牆，因為這可能導致功能未按預期工作。例如，如果 *Panorama* 執行的是 *PAN-OS 10.1.0*，則不建議管理執行 *PAN-OS 10.1.1* 或更高維護版本的防火牆。

確定升級到 PAN-OS 11.1 的路徑

當您從一個 PAN-OS 功能發行版本升級至更新的功能版本時，您無法略過前往目標版本的路徑中任何功能發行版本的安裝。此外，建議的升級路徑包括在下載下一個功能發行版本的基礎映像之前，在每個發行版本中安裝最新的維護版本。若要縮短使用者的停機時間，請在非工作時間執行升級。

對於手動升級，*Palo Alto Networks* 建議在升級路徑上為每個 *PAN-OS* 版本安裝和升級最新的維護版本。請勿為功能版本安裝 *PAN-OS* 基礎映像，除非它是您要升級至的目標版本。

確定升級路徑，如下所示：

STEP 1 | 識別目前安裝的版本。

- 在 Panorama 中，選取 **Panorama** > **Managed Devices**（受管理裝置），並查看您計劃升級的防火牆的軟體版本。
- 在防火牆中，選取 **Device**（裝置） > **Software**（軟體），然後查看哪個版本的「目前已安裝」列中有核取符號。

STEP 2 | （PAN-OS 11.1.3 及更新版本）檢視慣用版本。

- 在 Panorama 中，按一下 **Panorama** > **Software**（軟體），然後停用（清除）**Base Releases**（基礎版本）核取方塊。
- 在防火牆中，按一下 **Device**（裝置） > **Software**（軟體），然後停用（清除）**Base Releases**（基礎版本）核取方塊。

STEP 3 | 識別升級路徑：

在《版本資訊》和 升級/降級考量事項 中檢閱您在升級路徑中會經過的每個版本的已知問題和預設行為變更。

已安裝的 **PAN-OS** 版本	升級至 **PAN-OS 11.1** 的建議路徑
11.0.x	• 如果您已經在執行 PAN-OS 11.0 版本，則可以直接升級至 PAN-OS 11.1。
10.2.x	• 如果您已經在執行 PAN-OS 10.2 版本，則可以直接升級至 PAN-OS 11.1。
10.1.x	在從 PAN-OS 10.1 或更高版本升級裝置時，您現在可以使用略過軟體版本升級功能來略過軟體版本。 • 如果您已經在執行 PAN-OS 10.1 版本，則可以直接升級至 PAN-OS 11.1。
10.0.x	• 下載並安裝最新的偏好 PAN-OS 10.0 維護版本，然後重新啟動。 • 下載 PAN-OS 10.1.0。 • 下載並安裝最新的偏好 PAN-OS 10.1 維護版本，然後重新啟動。 在從 PAN-OS 10.1 或更高版本升級裝置時，您現在可以使用略過軟體版本升級功能來略過軟體版本。 • 繼續前往 將防火牆升級到 PAN-OS 11.1。
9.1.x	• 下載並安裝最新的偏好 PAN-OS 9.1 維護版本，然後重新啟動。 • 下載 PAN-OS 10.0.0。 • 下載並安裝最新的偏好 PAN-OS 10.0 維護版本，然後重新啟動。 • 下載 PAN-OS 10.1.0。 • 下載並安裝最新的偏好 PAN-OS 10.1 維護版本，然後重新啟動。 在從 PAN-OS 10.1 或更高版本升級裝置時，您現在可以使用略過軟體版本升級功能來略過軟體版本。 • 繼續前往 將防火牆升級到 PAN-OS 11.1。

已安裝的 PAN-OS 版本	升級至 PAN-OS 11.1 的建議路徑
9.0.x	• 下載並安裝最新的偏好 PAN-OS 9.0 維護版本，然後重新啟動。 將任何日誌收集器升級至最新的 *PAN-OS 9.0* 維護版本之前，請先檢閱升級/降級考量事項。 • 下載 PAN-OS 9.1.0。 • 下載並安裝最新的偏好 PAN-OS 9.1 維護版本，然後重新啟動。 • 下載 PAN-OS 10.0.0。 • 下載並安裝最新的偏好 PAN-OS 10.0 維護版本，然後重新啟動。 • 下載 PAN-OS 10.1.0。 • 下載並安裝最新的偏好 PAN-OS 10.1 維護版本，然後重新啟動。 在從 PAN-OS 10.1 或更高版本升級裝置時，您現在可以使用略過軟體版本升級功能來略過軟體版本。 • 繼續前往 將防火牆升級到 PAN-OS 11.1。
8.1.x	• 下載並安裝最新的偏好 PAN-OS 8.1 維護版本，然後重新啟動。 • 下載 PAN-OS 9.0.0 • 下載並安裝最新的偏好 PAN-OS 9.0 維護版本，然後重新啟動。 將任何日誌收集器升級至最新的 *PAN-OS 9.0* 維護版本之前，請先檢閱升級/降級考量事項。 • 下載 PAN-OS 9.1.0。 • 下載並安裝最新的偏好 PAN-OS 9.1 維護版本，然後重新啟動。 • 下載 PAN-OS 10.0.0。 • 下載並安裝最新的偏好 PAN-OS 10.0 維護版本，然後重新啟動。 • 下載 PAN-OS 10.1.0。

已安裝的 PAN-OS 版本	升級至 PAN-OS 11.1 的建議路徑
	• 下載並安裝最新的偏好 PAN-OS 10.1 維護版本，然後重新啟動。 在從 PAN-OS 10.1 或更高版本升級裝置時，您現在可以使用略過軟體版本升級功能來略過軟體版本。 • 繼續前往 將防火牆升級到 PAN-OS 11.1。

升級獨立防火牆

檢閱 PAN-OS 11.1 版本資訊，然後使用下列程序將不在 HA 設定中的防火牆升級至 PAN-OS 11.1。

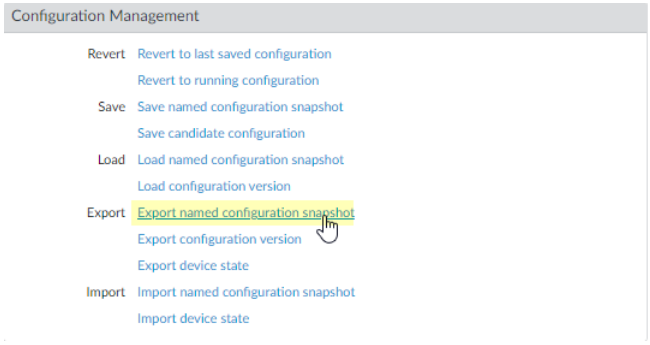
如果您的防火牆設定為將範例轉送至 *WildFire* 設備進行分析，則必須先升級 WildFire 設備，才能升級轉送防火牆。

為了避免影響流量，請將升級規劃在離峰時間進行。確定防火牆連線至可靠的電源。升級過程中的電力損耗會使防火牆無法使用。

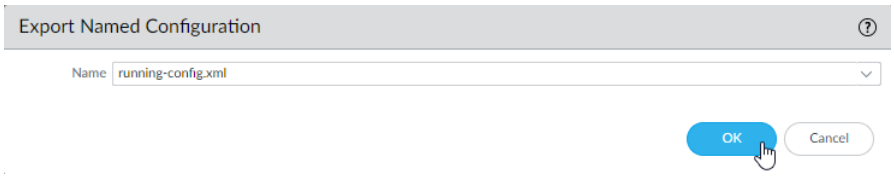
STEP 1 | 儲存目前組態檔案的備份。

雖然防火牆會自動建立設定備份，但最好在升級前建立備份並儲存在外部。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後按一下 **Export named configuration snapshot**（匯出具名設定快照）。



2. 選取包含執行中組態的 XML 檔案（例如 **running-config.xml**），然後按一下 **OK**（確定）匯出組態檔案。



3. 將匯出的檔案儲存至防火牆外部的位置。如果您在升級時發生問題，便可使用此備份還原組態。

STEP 2 | （選用）如果您已啟用 User-ID，在您升級後，防火牆將會清除當前 IP 位址與使用者名稱之間的對應以及群組對應，使其能夠重新填入 User-ID 來源中的屬性。若要測量您的環境重新填入對應所需的時間，請對防火牆執行下列 CLI 命令。

- 針對 IP 位址與使用者名稱的對應：
  - **`show user user-id-agent state all`**
  - **`show user server-monitor state all`**
- 針對群組對應：**`show user group-mapping statistics`**

STEP 3 | 確定防火牆執行最新的內容版本。

請參閱版本資訊，瞭解您必須為 PAN-OS 11.1 版本安裝的最低內容版本。確保遵循 應用程式與威脅內容更新的最佳做法。

1. 選取 **Device**（裝置） > **Dynamic Updates**（動態更新），並查看哪個 **Applications**（應用程式）或 **Applications and Threats**（應用程式與威脅）內容版本是 [Currently Installed（目前安裝的）]。

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOA...	CURRENTLY INSTALLED	ACTION	DOCUMENTAT...
Applications and Threats	**Last checked:** 2020/07/08 01:02:02 PDT	**Schedule:** Every Wednesday at 01:02 (Download only)								
8287-6151	panupv2-all-contents-8287-6151	Apps, Threats	Full	56 MB	36315eff...	2020/06/26 17:34:56 PDT		✓		Release Notes
8287-6152	panupv2-all-contents-8287-6152	Apps, Threats	Full	56 MB	dced5c69...	2020/06/29 11:55:44 PDT	✓ previously		Revert Review Policies Review Apps	Release Notes
8287-6153	panupv2-all-contents-8287-6153	Apps, Threats	Full	56 MB	14af053b...	2020/06/29 17:15:33 PDT			Download	Release Notes
8287-6154	panupv2-all-contents-8287-6154	Apps, Threats	Full	56 MB	c872552f...	2020/06/30 16:14:19 PDT			Download	Release Notes
8287-6155	panupv2-all-contents-8287-6155	Apps, Threats	Full	56 MB	3f0fcb9a6...	2020/06/30 19:09:11 PDT			Download Review Policies Review Apps	Release Notes
8288-6157	panupv2-all-contents-8288-6157	Apps, Threats	Full	56 MB	54f355a1...	2020/07/01 17:00:41 PDT			Download	Release Notes
8288-6158	panupv2-all-contents-8288-6158	Apps, Threats	Full	56 MB	db9e5a8f...	2020/07/01 18:15:46 PDT			Download	Release Notes
8288-6159	panupv2-all-contents-8288-6159	Apps, Threats	Full	56 MB	b6863c96...	2020/07/02 11:55:30 PDT			Download	Release Notes

2. 如果防火牆未執行 PAN-OS 11.1 所需的最低必要內容版本或更新版本，請 **Check Now**（立即檢查）以擷取可用的更新清單。
3. 找出並 **Download**（下載）所需的內容發行版本。

   在您成功下載內容更新檔案後，該內容發行版本的 [Action（動作）] 欄中的連結會從 **Download**（下載）變更為 **Install**（安裝）。
4. **Install**（安裝）更新。

STEP 4 | 確定升級到 PAN-OS 11.1 的路徑

檢閱 PAN-OS 升級檢查清單，瞭解您在升級路徑中會經過的每個版本的版本資訊和 升級/降級考量事項 中的已知問題和預設行為變更。

STEP 5 | （最佳做法）如果您正在使用 Cortex 資料湖 (CDL)，請安裝裝置憑證。

防火牆會在升級至 PAN-OS 11.1 時自動切換至使用裝置憑證進行 CDL 擷取和查詢端點的驗證。

如果在升級至 *PAN-OS 11.1* 之前未安裝裝置憑證，防火牆會繼續使用現有的日誌記錄服務憑證進行驗證。

STEP 6 | 升級到 PAN OS 11.1。

如果防火牆無法從管理連接埠存取網際網路，您可以從 Palo Alto Networks 客戶支援入口網站下載軟體映像，然後再將其手動 ***Upload***（上傳）至防火牆。

1. 選取 **Device**（裝置） > **Software**（軟體），然後按一下 **Check Now**（立即檢查）以顯示最新的 PAN-OS 更新。

   僅顯示下一個可用的 PAN-OS 版本。例如，如果 PAN-OS 11.1 安裝在防火牆上，則僅顯示 PAN-OS 11.1 版本。

   （PAN-OS 11.1.3 及更新版本）根據預設，系統會顯示慣用版本和相應的基礎版本。若要僅查看慣用版本，請停用（清除）**Base Releases**（基礎版本）核取方塊。
2. 選取 **Panorama** > **Device Deployment**（裝置部署） > **Software**（軟體） > **Action**（動作） > **Validate**（驗證）

   Panorama > **Device Deployment**（裝置部署） > **Software**（軟體） > **Action**（動作） > **Validate**（驗證）以檢視升級至 11.1.0 所需的所有中間軟體和內容映像。
3. 下載中間軟體和內容映像。
4. 在您下載映像後（手動升級則是在上傳映像後），請 **Install**（安裝）該映像。
5. 安裝成功完成後，使用下列其中一種方法重新啟動：
   - 如果提示您重新啟動，請按一下**Yes** （是）。
   - 如果未提示您重新啟動，請選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後按一下 **Reboot Device**（重新啟動裝置）。

   此時，防火牆會清除 *User-ID* 對應，然後連線至 *User-ID* 來源以重新填入對應。
6. 如果您已啟用 User-ID，請先使用下列 CLI 命令確認防火牆已重新填入 IP 位址與使用者名稱的對應和群組對應，再允許流量。
   - **`show user ip-user-mapping all`**
   - **`show user group list`**

STEP 7 | 重新產生或重新匯入所有憑證以遵守 OpenSSL 安全性等級 2。

在升級到 PAN-OS 11.1 時，要求所有憑證滿足以下最低要求：

- RSA 2048 位元或以上，或 ECDSA 256 位元或以上
- SHA256 或更高版本的摘要

請參閱 PAN-OS 管理員指南，瞭解有關重新產生或重新匯入憑證的更多資訊。

STEP 8 | 確認防火牆正在傳遞流量。

選取 **Monitor**（監控） > **Session Browser**（工作階段瀏覽器），然後確認您看到新的工作階段。

START TIME	FROM ZONE	TO ZONE	SOURCE	DESTINATI...	FROM PORT	TO PORT	PROTOC...	APPLICATI...	RULE	INGRESS I/F	EGRESS I/F	BYTES	VIRTUAL SYSTEM
07/08 11:29:02	z1	z2			56622	44060	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	558	vsys1
07/08 11:29:00	z1	z2			44823	42573	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	277874	vsys1
07/08 11:29:10	z1	z2			60162	47273	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	580	vsys1
07/08 11:29:10	z1	z2			45751	6013	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	560	vsys1
07/08 11:29:00	z1	z2			52923	42559	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	111119	vsys1
07/08 11:29:12	z1	z2			45772	8348	6	ftp-data	rules6-clone-with-group	ethernet1/3	ethernet1/4	785	vsys1
07/08 11:29:10	z1	z2			39762	61408	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	554	vsys1
07/08 11:29:06	z1	z2			53948	56596	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	792	vsys1
07/08 11:28:11	z1	z2			38185	42186	6	ftp-data	rules6-1	ethernet1/3	ethernet1/4	3243	vsys1

STEP 9 | 檢視防火牆上的軟體升級歷程記錄。

1. 登入防火牆介面。
2. 前往 **Device**（裝置） > **Summary**（摘要） > **Software**（軟體） 並按一下 **Device History**（裝置歷程記錄）。

升級 HA 防火牆配對

檢視 PAN-OS 11.1 版本資訊，然後使用下列程序升級高可用性 (HA) 設定中的一對防火牆。此程序適用於主動/被動和主動/主動設定。

若要避免在高可用性 (HA) 設定中升級防火牆時的停機時間，每次更新一個 HA 對等：對於主動/主動防火牆，先升級哪個對等並沒有差別（但為了方便說明，此程序將說明如何先升級主動-主要對等）。對於主動/被動防火牆，您必須先暫停（容錯移轉）並升級主動（主要）對等。升級主要對等後，您必須取消暫停主要對等以將其還原至正常狀態（被動）。接下來，您必須暫停被動（次要）對等以使主要對等再次處於活動狀態。在主對等處於活動狀態且次要對等被暫停後，您可以繼續升級。若要防止在升級 HA 對等期間發生容錯移轉，您必須先確定已停用先佔，再繼續進行升級。您只需停用配對中一個對等的先佔即可。

在跨多個功能 PAN-OS 版本升級 HA 防火牆時，您必須先將每個 HA 對等升級至升級路徑上的相同功能 PAN-OS 版本，然後再繼續。例如，將 HA 對等從 PAN-OS 10.2 升級至 PAN-OS 11.1。您必須先將兩個 HA 對等升級至 PAN-OS 11.0，然後才能繼續升級至目標 PAN-OS 11.1 版本。當 HA 對等相隔兩個或更多個功能版本時，安裝了舊版本的防火牆會進入 `suspended` 狀態，並顯示訊息 `Peer version too old`。

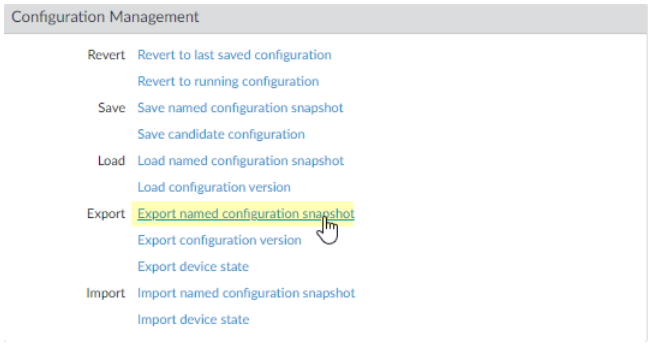
為了避免影響流量，請將升級規劃在離峰時間進行。確保防火牆連線至可靠的電源。升級過程中的電力損耗會使防火牆無法使用。

STEP 1 | 儲存目前組態檔案的備份。

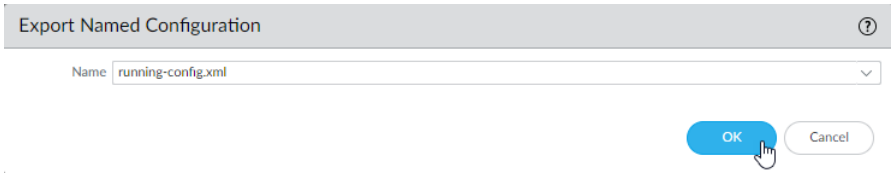
雖然防火牆會自動建立設定備份，但最好是在升級前先建立備份並儲存於外部。

對配對中的每個防火牆執行下列步驟：

1. 選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後按一下 **Export named configuration snapshot**（匯出具名設定快照）。



2. 選取包含執行中組態的 XML 檔案（例如 **running-config.xml**），然後按一下 **OK**（確定）匯出組態檔案。



3. 將匯出的檔案儲存至防火牆外部的位置。如果您在升級時發生問題，便可使用此備份還原組態。

STEP 2 | 選取 **Device**（裝置） > **Support**（支援）並 **Generate Tech Support File**（產生技術支援檔案）。

當提示產生技術支援檔案時按一下 **Yes**（是）。

STEP 3 | 確定 HA 配對中的每個防火牆都執行最新的內容版本。

請參閱版本資訊，瞭解您必須為 PAN-OS 11.1 版本安裝的最低內容版本。確保遵循 應用程式與威脅內容更新的最佳做法。

1. 選取 **Device**（裝置） > **Dynamic Updates**（動態更新），並查看 **Applications**（應用程式）或 **Applications and Threats**（應用程式與威脅），以確認哪個更新是 [Currently Installed（目前安裝的）]。

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOA...	CURRENTLY INSTALLED	ACTION	DOCUMENTAT...
Applications and Threats	**Last checked:** 2020/07/08 01:02:02 PDT	**Schedule:** Every Wednesday at 01:02 (Download only)								
8287-6151	panupv2-all-contents-8287-6151	Apps, Threats	Full	56 MB	36315eff...	2020/06/26 17:34:56 PDT		✓		Release Notes
8287-6152	panupv2-all-contents-8287-6152	Apps, Threats	Full	56 MB	dced5c69...	2020/06/29 11:55:44 PDT	✓ previously		Revert Review Policies Review Apps	Release Notes
8287-6153	panupv2-all-contents-8287-6153	Apps, Threats	Full	56 MB	14af053b...	2020/06/29 17:15:33 PDT			Download	Release Notes
8287-6154	panupv2-all-contents-8287-6154	Apps, Threats	Full	56 MB	c872552f...	2020/06/30 16:14:19 PDT			Download	Release Notes
8287-6155	panupv2-all-contents-8287-6155	Apps, Threats	Full	56 MB	3f0fcb9a6...	2020/06/30 19:09:11 PDT			Download Review Policies Review Apps	Release Notes
8288-6157	panupv2-all-contents-8288-6157	Apps, Threats	Full	56 MB	54f355a1...	2020/07/01 17:00:41 PDT			Download	Release Notes
8288-6158	panupv2-all-contents-8288-6158	Apps, Threats	Full	56 MB	db9e5a8f...	2020/07/01 18:15:46 PDT			Download	Release Notes
8288-6159	panupv2-all-contents-8288-6159	Apps, Threats	Full	56 MB	b6863c96...	2020/07/02 11:55:30 PDT			Download	Release Notes

2. 如果防火牆未執行 PAN-OS 11.1 所需的最低必要內容版本或更新版本，請 **Check Now**（立即檢查）以擷取可用的更新清單。
3. 找出並 **Download**（下載）所需的內容發行版本。
   在您成功下載內容更新檔案後，該內容發行版本的 [Action（動作）] 欄中的連結會從 **Download**（下載）變更為 **Install**（安裝）。
4. **Install**（安裝）更新。您必須在兩個對等上都安裝更新。

STEP 4 | 確定升級到 PAN-OS 11.1 的路徑

您無法略過從目前執行的 PAN-OS 版本到 PAN-OS 11.1 的路徑中任何功能發佈版本的安裝。

檢閱 PAN-OS 升級檢查清單，瞭解您在升級路徑中會經過的每個版本的版本資訊和 升級/降級考量事項 中的已知問題和預設行為變更。

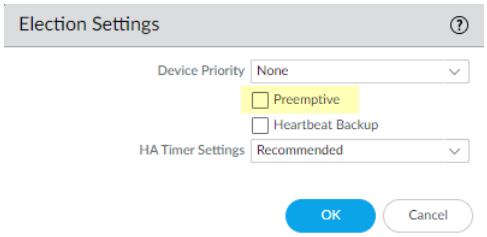
STEP 5 | （最佳做法）如果您正在使用 Cortex 資料湖 (CDL)，請在每個 HA 對等上安裝裝置憑證。

防火牆會在升級至 PAN-OS 11.1 時自動切換至使用裝置憑證進行 CDL 擷取和查詢端點的驗證。

如果在升級至 *PAN-OS 11.1* 之前未安裝裝置憑證，防火牆會繼續使用現有的日誌記錄服務憑證進行驗證。

STEP 6 | 停用每個配對中第一個對等的先佔。您只需要在 HA 配對中的一個防火牆上停用此設定，但務必要在認可成功後再繼續進行升級。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） 並編輯 **Election Settings**（選取設定）。
2. 若啟用，停用（清除）**Preemptive**（先佔）設定，然後按一下 **OK**（確認）。



3. **Commit**（提交）變更。

STEP 7 | 暫停主要 HA 對等以強制容錯移轉。

（主動/被動防火牆）對於主動/被動 HA 設定中的防火牆，先暫停並升級主動 HA 對等。

（主動/主動防火牆）對於主動/主動 HA 設定中的防火牆，先暫停並升級主動-主要 HA 對等。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **Operational Commands**（操作命令）和 **Suspend local device for high availability**（暫停本機裝置以取得高可用性）。
2. 在右下角，確認狀態為 `suspended`。

   由此引起的容錯移轉應會導致次要 HA 對等轉變為 `active` 狀態。

   由此引起的容錯移轉會在您升級之前確認 *HA* 容錯移轉是否正常執行。

STEP 8 | 在暫停的 HA 對等上安裝 PAN-OS 11.1。

1. 在主要 HA 對等上，選取 **Device**（裝置） > **Software**（軟體），然後按一下 **Check Now**（立即檢查）以瞭解最新的更新。

   僅顯示下一個可用的 PAN-OS 版本。例如，如果 PAN-OS 11.1 安裝在防火牆上，則僅顯示 PAN-OS 11.1 版本。

   （PAN-OS 11.1.3 及更新版本）根據預設，系統會顯示慣用版本和相應的基礎版本。若要僅查看慣用版本，請停用（清除）**Base Releases**（基礎版本）核取方塊。

2. 找到並 **Download**（下載）PAN-OS 11.1.0。

   如果防火牆無法從管理連接埠存取網際網路，您可以從 Palo Alto Networks 支援入口網站下載軟體映像，然後再將其手動 ***Upload***（上傳）至防火牆。

   如果您的防火牆確實可以存取網際網路，且遇到檔案下載錯誤，請再次按一下 ***Check Now***（立即檢查）以重新整理 *PAN-OS* 映像清單。

3. 在您下載映像後（手動升級則是在上傳映像後），請 **Install**（安裝）該映像。

VERSION	SIZE	RELEASE DATE	DOWNLOADED	CURRENTLY INSTALLED	ACTION		
10.0.0	1083 MB	2020/06/28 21:36:52			Install		☒
9.1.3	431 MB	2020/06/25 01:17:18			Download	Release Notes	
9.0.9	662 MB	2020/06/24 15:38:06			Download	Release Notes	

4. 安裝成功完成後，使用下列其中一種方法重新啟動：
   - 如果提示您重新啟動，請按一下**Yes**（是）。
   - 如果未提示您重新啟動，請選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作） 和 **Reboot Device**（重新啟動裝置）。
5. 裝置完成重新啟動後，請在 **Dashboard**（儀表板）上檢視「高可用性」Widget，並確認您剛升級的裝置在與對等同步。

STEP 9 | 將 HA 功能還原至主要 HA 對等。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **Operational Commands**（操作命令），然後 **Make local device functional for high availability**（讓本機裝置運作以取得高可用性）。
2. 在右下角，確認狀態為 `Passive`。對於主動/主動設定中的防火牆，確認狀態為 `Active`。
3. 等待 HA 對等執行設定同步。

   在 **Dashboard**（儀表板）中，監控「高可用性」Widget 中的「執行設定」狀態。

STEP 10 | 在次要 HA 對等上，暫停 HA 對等。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **Operational Commands**（操作命令）和 **Suspend local device for high availability**（暫停本機裝置以取得高可用性）。
2. 在右下角，確認狀態為 `suspended`。

   由此引起的容錯移轉應會導致主要 HA 對等轉變為 `Active` 狀態。

STEP 11 | 在次要 HA 對等上安裝 PAN-OS 11.1。

1. 在次要對等上，選取 **Device**（裝置） > **Software**（軟體），然後按一下 **Check Now**（立即檢查）以瞭解最新的更新。
2. 找到並 **Download**（下載）PAN-OS 11.1.0。
3. 下載映像後，請加以 **Install**（安裝）。
4. 安裝成功完成後，使用下列其中一種方法重新啟動：
   - 如果提示您重新啟動，請按一下**Yes** （是）。
   - 如果未提示您重新啟動，請選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作） 和 **Reboot Device**（重新啟動裝置）。

STEP 12 | 將 HA 功能還原至次要 HA 對等。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） > **Operational Commands**（操作命令），然後 **Make local device functional for high availability**（讓本機裝置運作以取得高可用性）。
2. 在右下角，確認狀態為 `Passive`。對於主動/主動設定中的防火牆，確認狀態為 `Active`。
3. 等待 HA 對等執行設定同步。

   在 **Dasbhoard**（儀表板）中，監控「執行設定」狀態高可用性 Widget。

STEP 13 | 重新啟用上一步中在 HA 對等上停用的先佔。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） 並編輯 **Election Settings**（選取設定）。
2. 啟用（核取）**Preemptive**（先佔）設定並按一下 **OK**（確定）。
3. **Commit**（提交）變更。

STEP 14 | 重新產生或重新匯入所有憑證以遵守 OpenSSL 安全性等級 2。

在升級到 PAN-OS 11.1 時，要求所有憑證滿足以下最低要求：

- RSA 2048 位元或以上，或 ECDSA 256 位元或以上
- SHA256 或更高版本的摘要

請參閱 PAN-OS 管理員指南或 Panorama 管理員指南，瞭解有關重新產生或重新匯入憑證的更多資訊。

STEP 15 | 確認兩個對等都如預期傳遞流量。

在主動/被動設定中，只有主動對等應傳遞流量；在主動/主動設定，兩個對等都應傳遞流量。

執行下列 CLI 命令以確認升級成功：

- （僅限主動對等）若要確認主動對等正在傳遞流量，請執行 **show session all** 命令。
- 若要驗證工作階段同步，請執行 **show high-availability interface ha2** 命令，並確定 CPU 表格上的 Hardware Interface（硬體介面）計數器增加如下：
  - 在主動/被動組態中，只有主動對等會顯示傳輸的封包；被動對等將只會顯示接收的封包。

    如果您已啟用 *HA2* 保持活動，被動對等上的硬體介面計數器會同時顯示傳輸與接收封包。這是因為 *HA2* 保持活動是雙向，亦即兩個對等都會傳輸 *HA2* 保持活動封包。
  - 在主動/主動組態中，您會看到兩個對等上接收的封包與傳輸的封包。

將防火牆從 Panorama 升級至 PAN-OS 11.1

從 Panorama™ 管理伺服器為受管理防火牆部署內容更新和升級 PAN-OS。

- 當 Panorama 連線至網際網路時升級防火牆
- 當 Panorama 未連線至網際網路時升級防火牆
- 升級 ZTP 防火牆

當 Panorama 連線至網際網路時升級防火牆

檢閱 PAN-OS 11.1 版本資訊，然後使用以下程序來升級您使用 Panorama 管理的防火牆。此程序應用在獨立的防火牆，以及部署在高可用性（HA）設定中的防火牆。

在跨多個功能 PAN-OS 版本升級 HA 防火牆時，您必須先將每個 HA 對等升級至升級路徑上的相同功能 PAN-OS 版本，然後再繼續。例如，將 HA 對等從 PAN-OS 10.2 升級至 PAN-OS 11.1。您必須先將兩個 HA 對等升級至 PAN-OS 11.0，然後才能繼續升級至目標 PAN-OS 11.1 版本。當 HA 對等相隔兩個或更多個功能版本時，安裝了舊版本的防火牆會進入 `suspended` 狀態，並顯示訊息 `Peer version too old`。

若 *Panorama* 無法直接連線至升級的伺服器，則請遵循當 Panorama 未連線至網際網路時升級防火牆中的程序，以讓您可以手動下載映像至 *Panorama*，然後將映像散佈至防火牆。

當部署從 PAN-OS 11.1 Panorama 設備到 PAN-OS 10.1 或更高版本的防火牆的升級時，新的略過軟體版本升級功能使您能夠略過最多三個版本。

在從 Panorama 升級防火牆之前，您必須：

- 確定 Panorama 正執行您要升級版本相同或更新的 PAN-OS 版本。您必須先升級 Panorama 及其日誌收集器（升級至 11.1），再將受管理的防火牆升級至此版本。此外，將日誌收集器升級至 11.1 時，由於記錄基礎結構有所變更，您必須將所有日誌收集器同時升級。
- 確保防火牆連接可靠的電源。升級過程中的電力損耗會使防火牆無法使用。
- 在升級至 PAN-OS 11.1 時，如果 Panorama 虛擬設備處於舊版模式，則決定是否保留在舊版模式。執行 PAN-OS 9.1 或更新版本的新 Panorama 設備部署不支援舊版模式。如果您將 Panorama 虛擬設備從 PAN-OS 9.0 或更早版本升級至 PAN-OS 11.1，Palo Alto Networks 建議您檢閱設定 Panorama 虛擬設備的先決條件，並根據需要變更為 Panorama 模式或僅管理模式。

  如果您要將 Panorama 虛擬設備保持在舊版模式中，請將配置給 Panorama 虛擬設備的 CPU 和記憶體增加到至少 16 個 CPU 和 32GB 記憶體，以成功升級至 PAN-OS 11.1。如需詳細資訊，請參閱 Panorama 虛擬設備的安裝先決條件。
- （建議用於多重 vsys 受管理防火牆）將多重 vsys 受管理防火牆的所有 vsys 轉換為 Panorama。

  建議您這樣做以避免在多重 vsys 受管理防火牆上提交問題，並讓您能夠利用 Panorama 的最佳化共用物件推送。

  這僅適用於使用略過軟體版本升級，從 PAN-OS 10.1 升級到 PAN-OS 11.1 的多重 vsys 防火牆。

- （多重 vsys 受管理防火牆）刪除或重新命名與 Panorama **Shared**（共用）設定中的物件名稱相同的任何本機設定 **Shared**（共用）物件。否則，升級後從 Panorama 推送的設定會失敗並顯示錯誤 `<object-name>` 已在使用中。

  這僅適用於使用略過軟體版本升級，從 PAN-OS 10.1 升級到 PAN-OS 11.1 的多重 vsys 防火牆。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 已修改您的安全性政策規則，以允許 `ssl` 應用程式流量。

這僅適用於使用略過軟體版本升級，從 *PAN-OS 10.1* 升級到 *PAN-OS 11.1* 的防火牆。

如果使用 *`panorama` App-ID* 來控制 *Panorama* 和受管理裝置之間的流量，則您必須這樣做，才能防止升級到 *PAN-OS 11.1* 後受管理裝置與 *Panorama* 中斷連線。如果升級前不允許使用 *`ssl`* 應用程式，受管理裝置將與 *Panorama* 中斷連線。

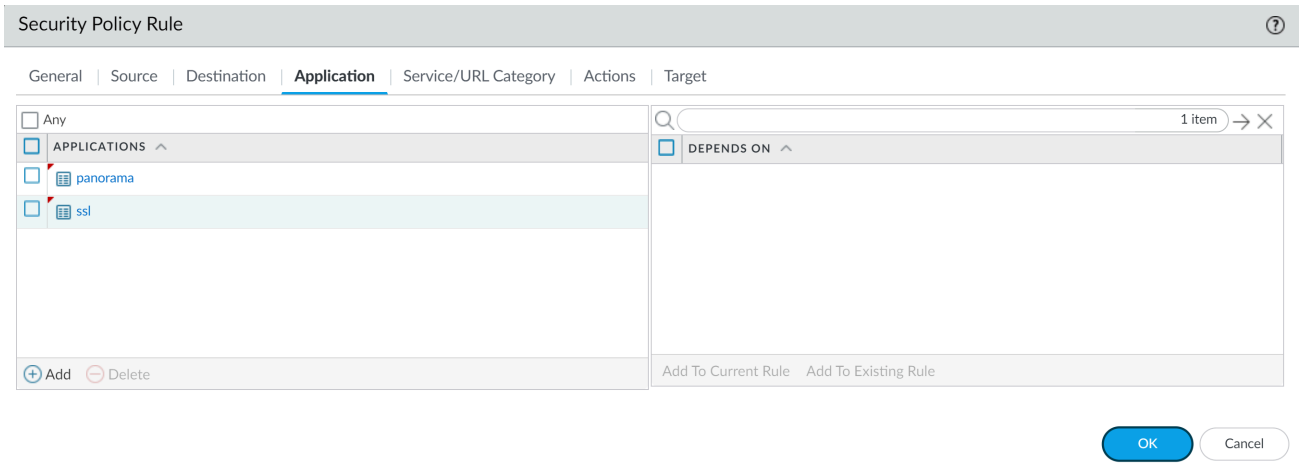
PAN-OS 11.1 會使用 TLS 版本 1.3 來加密 Panorama 與受管理防火牆之間的服務憑證和交握訊息。因此，從受管理防火牆到 Panorama 的流量的 App-ID 會從 `panorama` 重新分類為 `ssl`。

若要繼續 Panorama 和受管理裝置之間的通訊，您必須修改控制 Panorama 和受管理裝置之間流量的安全性政策規則，允許 `ssl` 應用程式。

如果控制 Panorama 和受管理裝置之間流量的安全性政策規則允許 **Any**（任何）應用程式，或者您已修改控制 Panorama 和受管理裝置之間流量的安全性政策規則，則請略過此步驟。

1. 選擇 **Policies**（政策） > **Security**（安全性） > **Pre Rules**（預先規則）。
2. 選擇包含控制 Panorama 和受管理防火牆之間流量的安全性政策規則的 **Device Group**（裝置群組）。
3. 選取安全性政策規則。
4. 選擇 **Application**（應用程式）並 **Add**（新增）`ssl`。

   不要刪除 *`panorama`* 應用程式。否則會導致所有受管理防火牆在您推送變更後與 *Panorama* 中斷連線。

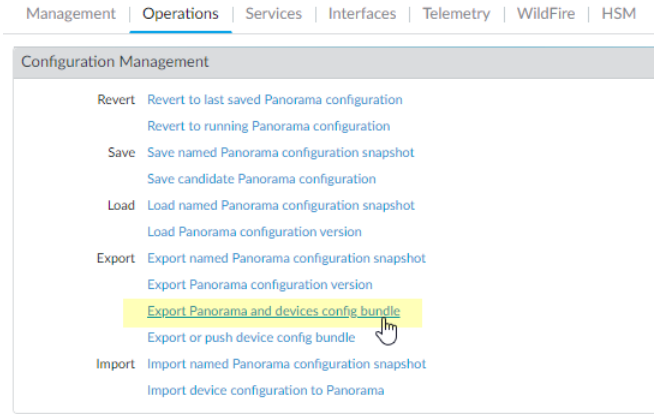


5. 按一下 **OK**（確定）。
6. 選擇 **Commit**（提交） > **Commit and Push**（提交並推送）並 **Commit and Push**（提交並推送）您的設定變更。

STEP 3 | 在您打算升級的每個受管理的防火牆上，儲存目前組態檔案的備份。

雖然防火牆會自動建立設定備份，但最好在升級前建立備份並儲存在外部。

1. 選取 **Panorama > Setup**（設定） **> Operations**（操作）並按一下 **Export Panorama and devices config bundle**（匯出 **Panorama** 和裝置設定組合），以產生並匯出 Panorama 和每個受管理設備的最新設定備份。

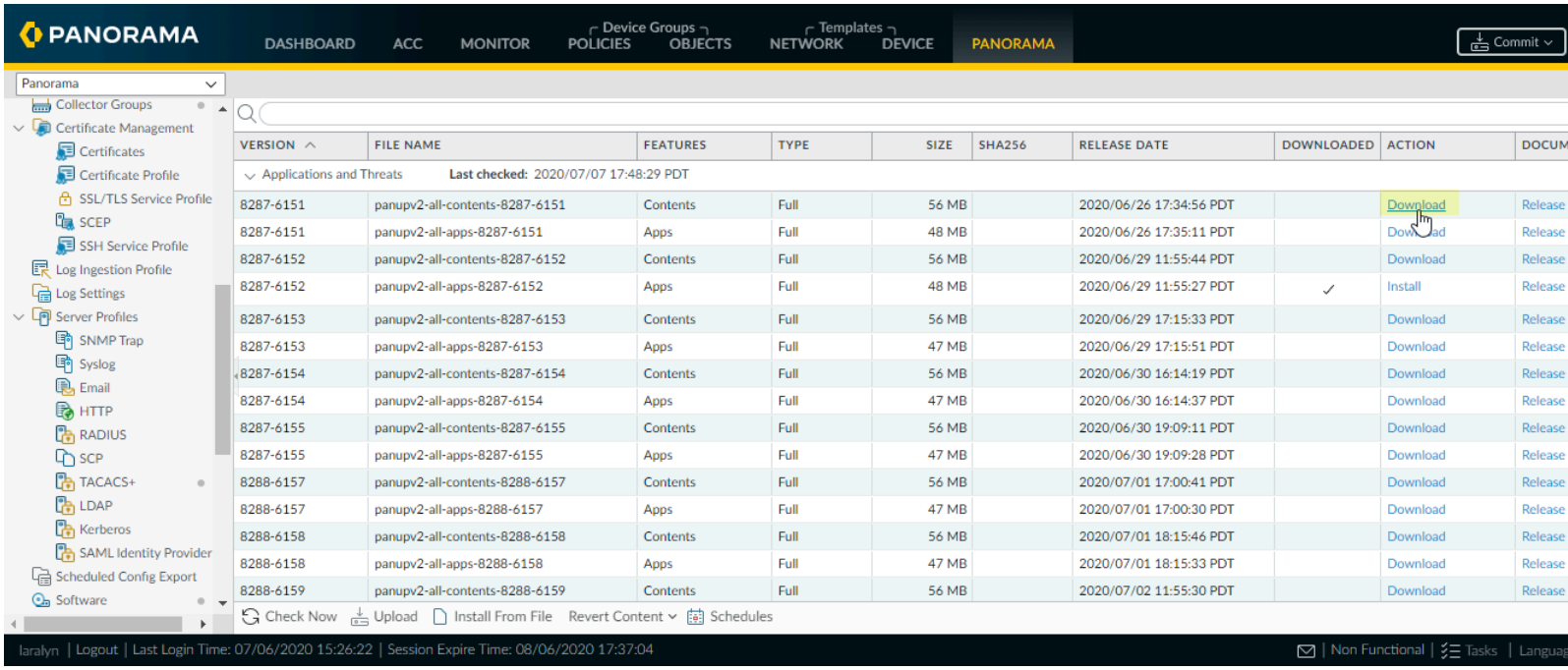


2. 將匯出的檔案儲存至防火牆外部的位置。如果您在升級時發生問題，便可使用此備份還原組態。

STEP 4 | 安裝最新內容更新。

請參閱版本資訊，瞭解 PAN-OS 11.1 所需的最低內容發行版本。在部署內容更新至 Panorama 和受管理防火牆時，請務必遵循 應用程式與威脅內容更新的最佳做法。

1. 選取 **Panorama** > **Device Deployment**（裝置部署） > **Dynamic Updates**（動態更新） 和 **Check Now**（立即檢查）以取得最新更新。如果有可用的更新，Action（動作）欄會顯示 **Download**（下載）連結。



2. 按一下 **Install**（安裝），並選取要安裝更新的防火牆。如果您正在升級 HA 防火牆，則您必須在兩個端點都升級內容。
3. 按一下 **OK**（確定）

STEP 5 | 確定升級到 PAN-OS 11.1 的路徑。

檢閱 PAN-OS 升級檢查清單，對於您在升級路徑中會經過的每個版本，瞭解版本資訊中的已知問題和預設行為變更，以及升級/降級注意事項。

如果是升級多個防火牆，在您開始下載映之前，請決定您想升級的所有防火牆的升級路徑，讓過程順暢進行。

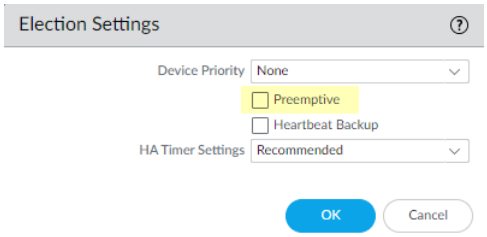
STEP 6 | （最佳做法）如果您正在使用 Cortex 資料湖 (CDL)，請安裝裝置憑證。

防火牆會在升級至 PAN-OS 11.1 時自動切換至使用裝置憑證進行 CDL 擷取和查詢端點的驗證。

如果在升級至 *PAN-OS 11.1* 之前未安裝裝置憑證，防火牆會繼續使用現有的日誌記錄服務憑證進行驗證。

STEP 7 | （僅限 HA 防火牆升級）如果您將升級為 HA 配對一部分的防火牆，請停用先佔。您僅需要在每個 HA 配對中的一個防火牆上停用此設定。

1. 選取 **Device**（裝置） > **High Availability**（高可用性） 並編輯 **Election Settings**（選取設定）。
2. 若啟用，停用（清除）**Preemptive**（先佔）設定，然後按一下 **OK**（確認）。



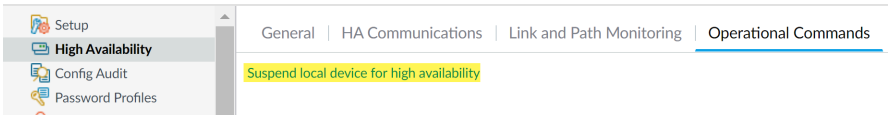
3. **Commit**（提交）您的變更。在您繼續進行更新前，請確認提交成功。

STEP 8 | （僅限 HA 防火牆升級）暫停主要 HA 對等以執行容錯移轉。

（主動/被動防火牆）對於主動/被動 HA 設定中的防火牆，先暫停並升級主動 HA 對等。

（主動/主動防火牆）對於主動/主動 HA 設定中的防火牆，先暫停並升級主動-主要 HA 對等。

1. 登入活動的主要防火牆 HA 對等的防火牆網頁介面。
2. 選取 **Device**（裝置） > **High Availability**（高可用性） > **Operational Commands**（操作命令）和 **Suspend local device for high availability**（暫停本機裝置以取得高可用性）。



3. 在右下角，確認狀態為 `suspended`。

   由此引起的容錯移轉應會導致次要被動 HA 對等轉變為 `active` 狀態。

   由此引起的容錯移轉會在您升級之前確認 *HA* 容錯移轉是否正常執行。

STEP 9 | （選用）將您受管理的防火牆升級至 PAN-OS 10.1。

略過軟體版本升級功能支援執行 PAN-OS 10.1 或更高版本的受管理防火牆。如果您的受管理防火牆執行的是 PAN-OS 10.0 或更早版本，請先升級至 PAN-OS 10.1 或更高版本。

STEP 10 | （選用）將檔案 **Export**（匯出）至已設定的 SCP 伺服器。

在 PAN-OS 11.1 中，在將升級部署到受管理的防火牆時，SCP 伺服器可用作下載來源。在下一步下載軟體和內容映像之前匯出檔案。

STEP 11 | 驗證並下載目標版本所需的軟體和內容版本。

在此步驟中，您可以檢視並下載升級至 PAN-OS 11.1 所需的中間軟體和內容映像。

使用多重映像下載來下載軟體和內容映像為選用。您仍然可以一次下載一個映像。

1. 按一下 **Panorama** > **Device Deployment**（裝置部署） > **Software**（軟體） > **Action**（動作） > **Validate**（驗證）。
2. 檢視您需要下載的中間軟體和內容版本。
3. 選取要升級的防火牆，然後按一下 **Deploy**（部署）。
4. 選取下載來源並按一下 **Download**（下載）。

STEP 12 | 在防火牆上安裝 PAN-OS 11.1.0。

（僅限 *SD-WAN*）要保持 *SD-WAN* 連結的準確狀態，在升級分支防火牆之前，您必須將中樞防火牆升級至 *PAN-OS 11.1*。如果先升級分支防火牆之後才升級中樞防火牆，可能產生錯誤監控資料（***Panorama*** > ***SD-WAN*** > ***Monitoring***（監控）），且 *SD-WAN* 連結會錯誤顯示為關閉。

1. 在對應您想要升級的防火牆型號的動作欄位中按一下 **Install**（安裝）。舉例來說，如果您想要升級 PA-440 防火牆，請按一下 PanOS_440-11.1.0 對應行的 **Install**（安裝）。
2. 在部署軟體檔案對話框中，選取所有您想要升級的防火牆。

   （僅限 HA 防火牆升級）若要減少停機時間，請在每個 HA 配對中只選取一個對等。對於主動/被動配對，請選取主動端點；對立主動/主動配對，請選取主動-次要端點。
3. （僅限 HA 防火牆升級） 確定未選取 **Group HA Peers**（群組 **HA** 配對）。
4. 選取 **Reboot device after install**（安裝後重新啟動裝置）。
5. 若要開始升級，請按一下 **OK**（確認）。
6. 安裝成功完成後，使用下列其中一種方法重新啟動：
   - 如果提示您重新啟動，請按一下**Yes** （是）。
   - 如果未提示您重新啟動，請選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作），然後 **Reboot Device**（重新啟動裝置）。
7. 在防火牆結束重新啟動後，請選取 **Panorama** > **Managed Devices**（受管理的裝置） 並驗證您升級的防火牆軟體版為 11.1.0。還要認證任何您在升級後仍舊為被動的防火牆的 HA 狀態。

STEP 13 | （僅限 HA 防火牆升級）將 HA 功能還原至主要 HA 對等。

1. 登入暫停的主要防火牆 HA 對等的防火牆網頁介面 。
2. 選取 **Device**（裝置） > **High Availability**（高可用性） > **Operational Commands**（操作命令），然後 **Make local device functional for high availability**（讓本機裝置運作以取得高可用性）。
3. 在右下角，確認狀態為 `Passive`。對於主動/主動設定中的防火牆，確認狀態為 `Active`。
4. 等待 HA 對等執行設定同步。

   在 **Dashboard**（儀表板）中，監控「高可用性」Widget 中的「執行設定」狀態。

STEP 14 | （僅限 HA 防火牆升級）暫停次要 HA 對等以執行容錯移轉回主要 HA 對等。

1. 登入活動的次要防火牆 HA 對等的防火牆網頁介面 。
2. 選取 **Device**（裝置） > **High Availability**（高可用性） > **Operational Commands**（操作命令）和 **Suspend local device for high availability**（暫停本機裝置以取得高可用性）。
3. 在右下角，確認狀態為 `suspended`。

   由此引起的容錯移轉應會導致主要被動 HA 對等轉變為 `active` 狀態。

   由此引起的容錯移轉會在您升級之前確認 *HA* 容錯移轉是否正常執行。

STEP 15 | （僅限 HA 防火牆升級）升級每個 HA 配對中的次要 HA 配對。

1. 在 Panorama 網頁介面中，選取 **Panorama** > **Device Deployment**（裝置部署） > **Software**（軟體）。
2. 在對應您正升級 HA 配對的防火牆型號的動作欄位中按一下 **Install**（安裝）。
3. 在部署軟體檔案對話框中，選取所有您想要升級的防火牆。這一次，僅選取您剛升級的 HA 防火牆的端點。
4. 確定未選取 **Group HA Peers**（群組 **HA** 配對）。
5. 選取 **Reboot device after install**（安裝後重新啟動裝置）。
6. 若要開始升級，請按一下 **OK**（確認）。
7. 安裝成功完成後，使用下列其中一種方法重新啟動：
   - 如果提示您重新啟動，請按一下**Yes** （是）。
   - 如果未提示您重新啟動，請選取 **Device**（裝置） > **Setup**（設定） > **Operations**（操作） 和 **Reboot Device**（重新啟動裝置）。

STEP 16 | （僅限 HA 防火牆升級）將 HA 功能還原至次要 HA 對等。

1. 登入暫停的次要防火牆 HA 對等的防火牆網頁介面 。
2. 選取 **Device**（裝置） > **High Availability**（高可用性） > **Operational Commands**（操作命令），然後 **Make local device functional for high availability**（讓本機裝置運作以取得高可用性）。
3. 在右下角，確認狀態為 `Passive`。對於主動/主動設定中的防火牆，確認狀態為 `Active`。
4. 等待 HA 對等執行設定同步。

   在 **Dashboard**（儀表板）中，監控「高可用性」Widget 中的「執行設定」狀態。

STEP 17 | （僅限 FIPS-CC 模式）在 FIPS-CC 模式下升級 Panorama 和受管理的裝置

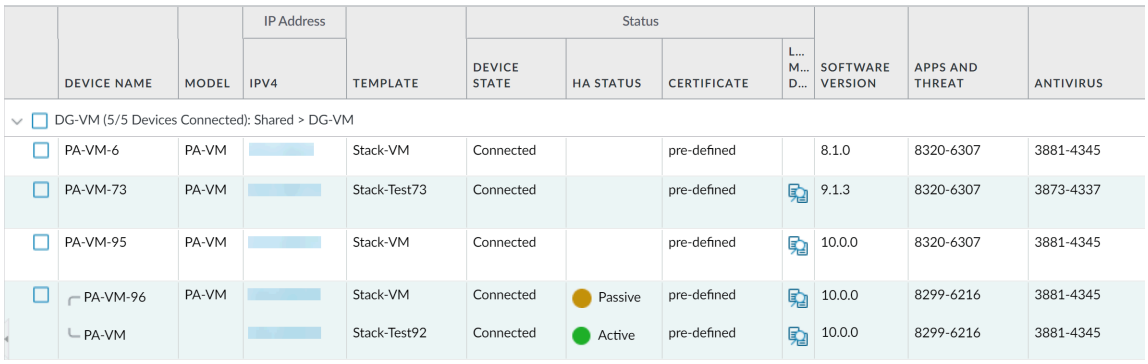
如果在受管理的防火牆執行 PAN-OS 11.1 版本時將專用日誌收集器新增至 Panorama 管理中，則在 FIPS-CC 模式下升級受管理的防火牆需要重設安全連線狀態。

當受管理的防火牆執行 PAN-OS 10.0 或更早版本時，您無需重新裝載新增至 Panorama 管理的受管理防火牆。

STEP 18 | 確認在每個受管理防火牆上執行的軟體與內容發佈版本。

1. 在 Panorama 上，選取 **Panorama** > **Managed Devices**（受管理的裝置）。
2. 在表格內找到防火牆，並檢閱內容和軟體版本。

   對於 HA 防火牆，您也可以驗證每個端點的 HA 狀態是否如預期。



	DEVICE NAME	MODEL	IP Address IPV4	TEMPLATE	Status DEVICE STATE	Status HA STATUS	Status CERTIFICATE	Status L... M... D...	SOFTWARE VERSION	APPS AND THREAT	ANTIVIRUS
DG-VM (5/5 Devices Connected): Shared > DG-VM											
	PA-VM-6	PA-VM		Stack-VM	Connected		pre-defined		8.1.0	8320-6307	3881-4345
	PA-VM-73	PA-VM		Stack-Test73	Connected		pre-defined		9.1.3	8320-6307	3873-4337
	PA-VM-95	PA-VM		Stack-VM	Connected		pre-defined		10.0.0	8320-6307	3881-4345
	PA-VM-96	PA-VM		Stack-VM	Connected	Passive	pre-defined		10.0.0	8299-6216	3881-4345
	PA-VM			Stack-Test92	Connected	Active	pre-defined		10.0.0	8299-6216	3881-4345

STEP 19 | （僅限 HA 防火牆升級）如果您在升級之前在其中一個 HA 防火牆上停用先佔，請編輯 **Election Settings**（選取設定）（**Device**（裝置） > **High Availability**（高可用性）），針對該防火牆重新啟用 **Preemptive**（先佔）設定，然後 **Commit**（提交）。

STEP 20 | 在 Panorama 網頁介面上，將整個 Panorama 受管理設定推送至您的受管理防火牆。

需要執行此步驟以選擇性提交並推送 Panorama 上的裝置群組和範本堆疊設定變更至受管理的防火牆。

需要執行此步驟以在成功由 PAN-OS 10.1 或更早版本升級到 PAN-OS 11.1 後，成功地將設定變更推送至由 Panorama 管理的多重 vsys 防火牆。如需詳細資訊，請參閱由 Panorama 管理的多重 vsys 防火牆的 共用設定物件的預設行為變更。

1. 選取 **Commit**（提交） > **Push to Devices**（推送至裝置）。
2. **Push**（推送）。

STEP 21 | 重新產生或重新匯入所有憑證以遵守 OpenSSL 安全性等級 2。

在升級到 PAN-OS 11.1 或更高版本時，要求所有憑證滿足以下最低要求：如果您是從 PAN-OS 10.2 升級並且已經重新產生或重新匯入憑證，請略過此步驟。

- RSA 2048 位元或以上，或 ECDSA 256 位元或以上
- SHA256 或更高版本的摘要

請參閱 PAN-OS 管理員指南或 Panorama 管理員指南，瞭解有關重新產生或重新匯入憑證的更多資訊。

STEP 22 | 檢視防火牆的軟體升級歷程記錄。

1. 登入 Panorama 介面。
2. 前往 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要）並按一下 **Device History**（裝置歷程記錄）。

當 Panorama 未連線至網際網路時升級防火牆

如需可在防火牆上安裝的軟體和內容更新清單，請參閱支援的更新。

當部署從 PAN-OS 11.1 Panorama 設備到 PAN-OS 10.1 或更高版本的防火牆的升級時，新的略過軟體版本升級功能使您能夠略過最多三個版本。

在從 Panorama 升級防火牆之前，您必須：

- 確定 Panorama 正執行您要升級版本相同或更新的 PAN-OS 版本。您必須先升級 Panorama 及其日誌收集器（升級至 11.1），再將受管理的防火牆升級至此版本。此外，將日誌收集器升級至 11.1 時，由於記錄基礎結構有所變更，您必須將所有日誌收集器同時升級。
- 確保防火牆連接可靠的電源。升級過程中的電力損耗會使防火牆無法使用。
- 在升級至 PAN-OS 11.1 時，如果 Panorama 虛擬設備處於舊版模式，則決定是否保留在舊版模式。執行 PAN-OS 9.1 或更新版本的新 Panorama 設備部署不支援舊版模式。如果您將 Panorama 虛擬設備從 PAN-OS 9.0 或更早版本升級至 PAN-OS 11.1，Palo Alto Networks 建議您檢閱設定 Panorama 虛擬設備的先決條件，並根據需要變更為 Panorama 模式或僅管理模式。

  如果您要將 Panorama 虛擬設備保持在舊版模式中，請將配置給 Panorama 虛擬設備的 CPU 和記憶體增加到至少 16 個 CPU 和 32GB 記憶體，以成功升級至 PAN-OS 11.1。如需詳細資訊，請參閱 Panorama 虛擬設備的安裝先決條件。
- （建議用於多重 vsys 受管理防火牆）將多重 vsys 受管理防火牆的所有 vsys 轉換為 Panorama。

  建議您這樣做以避免在多重 vsys 受管理防火牆上提交問題，並讓您能夠利用 Panorama 的最佳化共用物件推送。

  這僅適用於使用略過軟體版本升級，從 PAN-OS 10.1 升級到 PAN-OS 11.1 的多重 vsys 防火牆。
- （多重 vsys 受管理防火牆）刪除或重新命名與 Panorama **Shared**（共用）設定中的物件名稱相同的任何本機設定 **Shared**（共用）物件。否則，升級後從 Panorama 推送的設定會失敗並顯示錯誤 `<object-name>` 已在使用中。

  這僅適用於使用略過軟體版本升級，從 PAN-OS 10.1 升級到 PAN-OS 11.1 的多重 vsys 防火牆。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 已修改您的安全性政策規則，以允許 `ssl` 應用程式流量。

> 這僅適用於使用略過軟體版本升級，從 *PAN-OS 10.1* 升級到 *PAN-OS 11.1* 的防火牆。
>
> 如果使用 *`panorama` App-ID* 來控制 *Panorama* 和受管理裝置之間的流量，則您必須這樣做，才能防止升級到 *PAN-OS 11.1* 後受管理裝置與 *Panorama* 中斷連線。如果升級前不允許使用 *`ssl`* 應用程式，受管理裝置將與 *Panorama* 中斷連線。

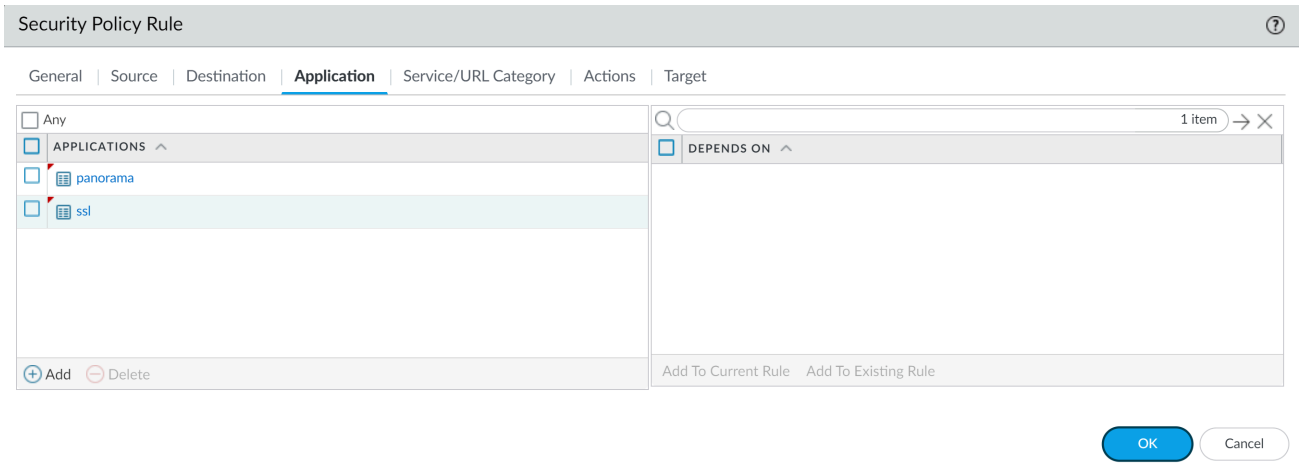
PAN-OS 11.1 會使用 TLS 版本 1.3 來加密 Panorama 與受管理防火牆之間的服務憑證和交握訊息。因此，從受管理防火牆到 Panorama 的流量的 App-ID 會從 `panorama` 重新分類為 `ssl`。

若要繼續 Panorama 和受管理裝置之間的通訊，您必須修改控制 Panorama 和受管理裝置之間流量的安全性政策規則，允許 `ssl` 應用程式。

如果控制 Panorama 和受管理裝置之間流量的安全性政策規則允許 **Any**（任何）應用程式，或者您已修改控制 Panorama 和受管理裝置之間流量的安全性政策規則，則請略過此步驟。

1. 選擇 **Policies**（政策） > **Security**（安全性） > **Pre Rules**（預先規則）。
2. 選擇包含控制 Panorama 和受管理防火牆之間流量的安全性政策規則的 **Device Group**（裝置群組）。
3. 選取安全性政策規則。
4. 選擇 **Application**（應用程式）並 **Add**（新增）`ssl`。

   不要刪除 *`panorama`* 應用程式。否則會導致所有受管理防火牆在您推送變更後與 *Panorama* 中斷連線。



5. 按一下 **OK**（確定）。
6. 選擇 **Commit**（提交） > **Commit and Push**（提交並推送）並 **Commit and Push**（提交並推送）您的設定變更。

STEP 3 | 在您打算升級的每個受管理的防火牆上，儲存目前組態檔案的備份。

雖然防火牆會自動建立設定備份，但最好在升級前建立備份並儲存在外部。

1. **Export Panorama and devices config bundle**（匯出 **Panorama** 和裝置設定組合）（**Panorama** > **Setup**（設定） > **Operations**（操作）），產生並匯出 Panorama 和每個受管理裝置的最新設定備份。
2. 將匯出的檔案儲存至防火牆外部的位置。如果您在升級時發生問題，便可使用此備份還原組態。

STEP 4 | 決定您需要安裝的內容更新。請參閱版本資訊，瞭解您必須為 PAN-OS® 版本安裝的最低內容發行版本。

Palo Alto Networks 高度建議 *Panorama*、日誌收集器和所有受管理的防火牆執行相同的內容發行版本。

針對每個內容更新，決定是否需要更新，並注意您需要下載下列步驟中的哪些內容更新。

請確定 *Panorama* 執行的內容發行版本，與受管理的防火牆和日誌收集器相同，但並不是更新的版本。

STEP 5 | 針對您想要更新至 Panorama 11.1 的防火牆，確定軟體升級路徑。

登入 Panorama，選取 **Panorama** > **Managed Devices**（受管理的裝置），並注意您想升級的防火牆的目前軟體版本。

檢閱 PAN-OS 升級檢查清單，瞭解您在升級路徑中會經過的每個版本的版本資訊和 升級/降級考量事項 中的已知問題和預設行為變更。

STEP 6 | （選用）將您受管理的防火牆升級至 PAN-OS 10.1。

略過軟體版本升級功能支援執行 PAN-OS 10.1 或更高版本的受管理防火牆。如果您的受管理防火牆執行的是 PAN-OS 10.0 或更早版本，請先升級至 PAN-OS 10.1 或更高版本。

STEP 7 | 執行版本的驗證檢查。

在此步驟中，您可以檢視升級至 11.1 所需的中間軟體和內容映像。

1. 選取 **Panorama** > **Device Deployment**（裝置部署） > **Software**（軟體） > **Action**（動作） > **Validate**（驗證）。
2. 檢視您需要下載的中間軟體和內容版本。

STEP 8 | 將內容和軟體更新下載到可透過 SCP 或 HTTPS 連線及上傳檔案至 Panorama 或設定的 SCP 伺服器的主機。

依預設，您可以將每種類型的最多兩個軟體或內容更新上傳至 Panorama 設備，如果您下載相同類型的第三個更新，Panorama 會刪除該類型最舊版本的更新。如果您需要上傳單一類型兩

個以上的軟體更新或內容更新，請使用 **set max-num-images count *<number>*** CLI 命令來增加 Panorama 可儲存的映像數目上限。

1. 使用可存取網際網路的主機登入 Palo Alto Networks 客戶支援網站。
2. 下載內容更新：
   1. 在 Resources（資源）部分中按一下 **Dynamic Updates**（動態更新）。
   2. **Download**（下載）最新的內容發行版本（或至少與您將安裝在 Panorama 管理伺服器上或其正在執行的版本相同或還要新），並將檔案儲存至主機；針對您需要更新的每種內容類型，重複此步驟。
3. 下載軟體更新：
   1. 返回 Palo Alto Networks 客戶支援網站的主頁面，然後在 Resources（資源）部分中按一下 **Software Updates**（軟體更新）。
   2. 檢閱下載欄以決定您需要安裝的版本。更新套件的檔案名稱會指出型號。例如，若要將 PA-440 和 PA-5430 防火牆升級至 PAN-OS 11.1.0，請下載 `Pan0S_440-11.1.0` 和 `Pan0S_5430-11.1.0` 映像。

      您可以從 ***Filter By***（篩選依據）下拉式清單中選取 ***PAN-OS for the PA***（適用於 ***PA*** 的 ***PAN-OS***）*-<series/model>*，快速找到特定的 *PAN-OS* 映像。
4. 按一下適當的檔名，並將檔案儲存至主機。

STEP 9 | 下載中間軟體版本和最新的內容版本。

在 PAN-OS 11.0 上，您可以使用多映像下載功能來下載多個中間版本。

1. 選取要升級的防火牆（**Required Deployments**（所需部署） > **Deploy**（部署））。
2. 選取下載來源並按一下 **Download**（下載）。

STEP 10 | 在受管理的防火牆上安裝內容更新。

您必須先安裝內容更新，再安裝軟體更新。

先安裝「應用程式」或「應用程式和威脅」更新，再依需要、一次一個、以任意順序安裝其他任何更新（防毒、WildFire® 或 URL 篩選）。

1. 選取 **Panorama** > **Device Deployment**（設備部署） > **Dynamic Updates**（動態更新）。
2. 按一下 **Upload**（上傳），選取更新 **Type**（類型），**Browse**（瀏覽）至適當的內容更新檔案，然後按一下 **OK**（確定）。
3. 按一下 **Install From File**（從檔案安裝），選取更新 **Type**（類型），並選取您剛上傳的內容更新的 **File Name**（檔案名稱）。
4. 選取您要安裝更新的防火牆。
5. 按一下 **OK**（確定）以啟動安裝。
6. 針對每個內容更新重複這些步驟。

STEP 11 | （僅限當作 GlobalProtect™ 入口網站的防火牆）將 GlobalProtect 代理程式/應用程式軟體更新上傳至防火牆並啟動。

您可在防火牆上啟動更新，供使用者下載至其端點（用戶端系統）。

1. 使用可存取網際網路的主機登入 Palo Alto Networks 客戶支援網站。
2. 下載適當的 GlobalProtect 代理程式/應用程式軟體更新。
3. 在 Panorama 上，選取 **Panorama** > **Device Deployment**（裝置部署） > **GlobalProtect Client**（**GlobalProtect** 用戶端）。
4. 按一下 **Upload**（上傳），在您已下載檔案的主機上 **Browse**（瀏覽）至適當的 GlobalProtect 代理程式/應用程式軟體更新，然後按一下 **OK**（確定）。
5. 按一下 **Activate From File**（從檔案啟動），選取您剛上傳的 GlobalProtect 代理程式/應用程式更新的 **File Name**（檔案名稱）。

   您一次只能啟動一個版本的代理程式/應用程式軟體。如果您啟動新版本，但某些代理程式需要上一個版本，則您必須再次重新啟動舊版本，讓這些代理程式下載上一個更新。
6. 選取要啟動更新的防火牆。
7. 按一下 **OK**（確定）以啟動。

STEP 12 | 安裝 PAN-OS 11.1。

若要避免在高可用性 *(HA)* 防火牆上更新軟體時的停機時間，每次更新一個 *HA* 端點。

對於主動/主動防火牆，更新端點的順序無關緊要。

對於主動/被動防火牆，您必須先更新被動端點，暫停主動端點（故障復原），更新主動端點，然後將主動端點返回至功能狀態（故障復原）。

（僅限 *SD-WAN*）要保持 *SD-WAN* 連結的準確狀態，在升級分支防火牆之前，您必須將中樞防火牆升級至 *PAN-OS 11.1*。如果先升級分支防火牆之後才升級中樞防火牆，可能產生錯誤監控資料（***Panorama*** > ***SD-WAN*** > ***Monitoring***（監控）），且 *SD-WAN* 連結會錯誤顯示為關閉。

1. 執行適用於您的防火牆組態的步驟，以安裝您剛上傳的 PAN-OS 軟體更新。
   - **Non-HA firewalls**（非 HA 防火牆）——按一下行動欄內的 **Install**（安裝），選取您正在升級的所有防火牆，選取 **Reboot device after install**（安裝後重新開機設備），然後按一下 **OK**（確定）。
   - 主動式/主動式 **HA** 防火牆：
     1. 在您想要升級的第一個對等上，確認先佔設定已停用（**Device**（裝置） > **High Availability**（高可用性） > 選取設定）。如果已啟用，請編輯 **Election Settings**（選取設定），停用（清除） **Preemptive**（先佔）設定，然後

Commit（提交）您的變更。您只需要在每個 HA 配對中的一個防火牆上停用此設定，但要確定提交成功之後再繼續。

2. 按一下 **Install**（安裝），停用（清除）**Group HA Peers**（群組 **HA** 對等），選取任一 HA 對等，選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 **OK**（確定）。繼續之前，等候防火牆完成重新開機。
3. 按一下 **Install**（安裝），停用（清除）**Group HA Peers**（群組 **HA** 對等），選取您在上一步未更新的 HA 對等、選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 **OK**（確定）。

- **Active/passive HA firewalls**（主動式/被動式 **HA** 防火牆）—在此範例中，主動式防火牆名稱為 fw1 而被動式防火牆名稱為 fw2：
  1. 在您想要升級的第一個對等上，確認先佔設定已停用（**Device**（裝置） > **High Availability**（高可用性） > 選取設定）。如果已啟用，請編輯 **Election Settings**（選取設定），停用（清除） **Preemptive**（先佔）設定，然後 **Commit**（提交）您的變更。您只需要在每個 HA 配對中的一個防火牆上停用此設定，但要確定提交成功之後再繼續。
  2. 在適當更新的動作欄中按一下 **Install**（安裝）、停用（清除）**Group HA Peers**（群組 **HA** 對等）、選取 fw2，選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 **OK**（確定）。繼續之前，請等候 fw2 完成重新開機。
  3. fw2 完成重新開機後，在 fw1 上確認（**Dashboard**（儀表板） > 高可用性）fw2 仍然是被動式對等（本機防火牆狀態為主動，而對等—fw2—為被動）。
  4. 存取 fw1 並暫停本機裝置（**Device**（裝置） > **High Availability**（高可用性） > **Operational Commands**（操作命令））。
  5. 存取 fw2（**Dashboard**（儀表板） > 高可用性），確認本機防火牆狀態為主動，對等為暫停。
  6. 存取 Panorama，選取 **Panorama** > **Device Deployment**（裝置部署） > **Software**（軟體），在適當版本的動作欄中按一下 **Install**（安裝）、停用（清除）**Group HA Peers**（群組 **HA** 對等）、選取 fw1、選取 **Reboot device after install**（安裝後重新啟動裝置），然後按一下 [OK（確定）]。繼續之前，請等候 fw1 完成重新開機。
  7. 存取 fw1（**Device**（裝置） > **High Availability**（高可用性） > **Operational Commands**（操作命令）），按一下 **Make local device functional**（讓本機裝置運作），然後在您繼續之前稍等兩分鐘。
  8. 在 fw1 上（**Dashboard**（儀表板） > 高可用性），確認本機防火牆狀態為被動，對等 (fw2) 為主動。

STEP 13 | （僅限 FIPS-CC 模式）在 FIPS-CC 模式下升級 Panorama 和受管理的裝置

如果在受管理的防火牆執行 PAN-OS 11.1 版本時將專用日誌收集器新增至 Panorama 管理中，則在 FIPS-CC 模式下升級受管理的防火牆需要重設安全連線狀態。

當受管理的防火牆執行 PAN-OS 10.0 或更早版本時，您無需重新裝載新增至 Panorama 管理的受管理防火牆。

STEP 14 | 驗證各受管理的防火牆上安裝的軟體和內容版本。

1. 選取 **Panorama** > **Managed Devices**（受管理的裝置）。
2. 找到防火牆，並檢閱 Software Version（軟體版本）、Apps and Threat（應用程式與威脅）、Antivirus（防毒）、URL Filtering（URL 篩選）及 GlobalProtect Clien（GlobalProtect 用戶端） 欄中的值。

STEP 15 | 如果您在升級之前在其中一個 HA 防火牆上停用先佔，請編輯 **Election Settings**（選取設定）（**Device**（裝置） > **High Availability**（高可用性）），針對該防火牆重新啟用 **Preemptive**（先佔） 設定。

STEP 16 | 在 Panorama 網頁介面上，將整個 Panorama 受管理設定推送至您的受管理防火牆。

需要執行此步驟以選擇性提交並推送 Panorama 上的裝置群組和範本堆疊設定變更至受管理的防火牆。

需要執行此步驟以在成功升級到 PAN-OS 11.1 後，成功地將設定變更推送至由 Panorama 管理的多重 vsys 防火牆。如需詳細資訊，請參閱由 Panorama 管理的多重 vsys 防火牆的 共用設定物件的預設行為變更。

1. 選取 **Commit**（提交） > **Push to Devices**（推送至裝置）。
2. **Push**（推送）。

STEP 17 | 重新產生或重新匯入所有憑證以遵守 OpenSSL 安全性等級 2。

在升級到 PAN-OS 11.1 時，要求所有憑證滿足以下最低要求：

- RSA 2048 位元或以上，或 ECDSA 256 位元或以上
- SHA256 或更高版本的摘要

請參閱 PAN-OS 管理員指南或 Panorama 管理員指南，瞭解有關重新產生或重新匯入憑證的更多資訊。

STEP 18 | 檢視防火牆的軟體升級歷程記錄。

1. 登入 Panorama 介面。
2. 前往 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要）並按一下 **Device History**（裝置歷程記錄）。

升級 ZTP 防火牆

成功新增 ZTP 防火牆至 Panorama™ 管理伺服器後，設定 ZTP 防火牆的目標 PAN-OS 版本。首次成功連線至 Panorama 後，Panorama 會檢查 ZTP 防火牆上安裝的 PAN-OS 版本是否比所設定目標 PAN-OS 版本更新或相同。如果 ZTP 防火牆上安裝的 PAN-OS 版本比目標 PAN-OS 版本更舊，則 ZTP 防火牆進行升級循環，直到安裝目標 PAN-OS 版本。

STEP 1 | 作為管理員使用者登入 Panorama 網頁介面。

STEP 2 | 新增 ZTP 防火牆至 Panorama。

STEP 3 | 選取 **Panorama** > **Device Deployment**（裝置部署） > **Updates**（更新）和 **Check Now**（立即檢查）以獲得最新 PAN-OS 版本。

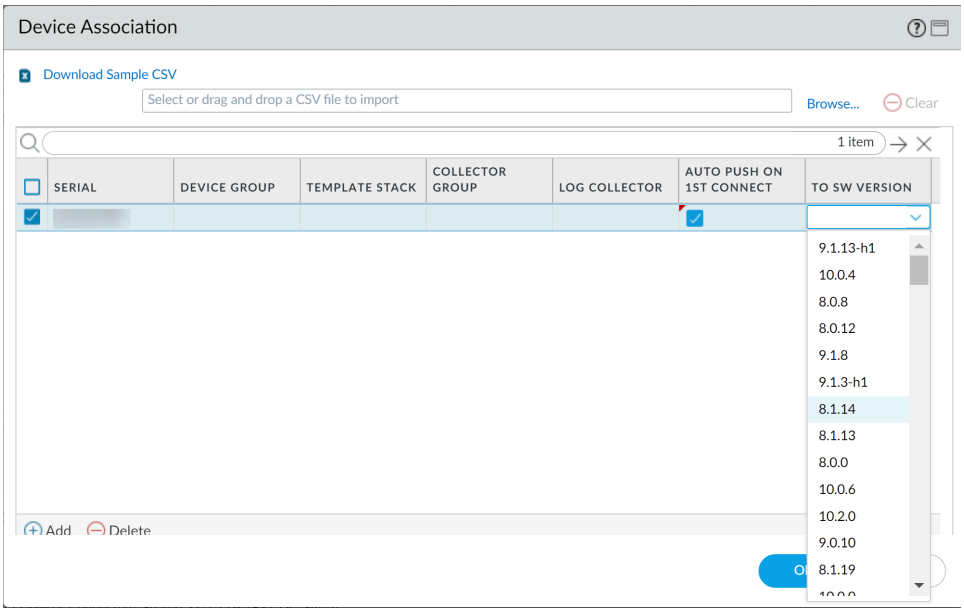
STEP 4 | 選取 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要）並選取一或多個 ZTP 防火牆。

STEP 5 | **Reassociate**（重新關聯）所選取 ZTP 防火牆。

STEP 6 | 核取（啟用） **Auto Push on 1st Connect**（第 **1** 次連線時自動推送）。

STEP 7 | 在 **To SW Version**（至軟體版本）欄中，選取 ZTP 防火牆的目標 PAN-OS 版本。

STEP 8 | 按一下 **OK**（確定）儲存組態變更。



STEP 9 | 按一下 **Commit**（提交） 和 **Commit to Panorama**（提交至 **Panorama**）。

STEP 10 | 開啟 ZTP 防火牆。

當 ZTP 防火牆首次連線至 Panorama 時，會自動升級至您選取的 PAN-OS 版本。

- 執行 **PAN-OS 11.1.0** 的 **Panorama**— 如果您要跨 PAN-OS 主要版本或維護版本升級受管理的防火牆，則在安裝目標 PAN-OS 版本之前，先安裝升級路徑上的中間 PAN-OS 版本。

  例如，您將受管理防火牆的目標 **To SW Version**（至軟體版本）設定為 PAN-OS 11.1.0，並且防火牆正在執行 PAN-OS 10.2。首次連線至 Panorama 時，首先會在受管理的防火牆上安裝 PAN-OS 11.0.0。PAN-OS 11.0.0 成功安裝後，防火牆會自動升級至目標 PAN-OS 11.1.0 版本。

- 執行 **PAN-OS 11.0.1** 及更高版本的 **Panorama**—如果您正在跨 PAN-OS 主要版本或維護版本升級受管理的防火牆，則會先安裝升級路徑上的中間 PAN-OS 主要版本並下載基本 PAN-OS 主要版本，然後才安裝目標 PAN-OS 維護版本。

  例如，您將受管理防火牆的目標 **To SW Version**（至軟體版本）設定為 11.0.1，並且防火牆正在執行 PAN-OS 10.0。首次連線至 Panorama 時，首先會在受管理的防火牆上安裝 PAN-OS 10.1.0 和 PAN-OS 10.2.0。受管理的防火牆重新啟動後，將下載 PAN-OS 11.0.0，然后防火牆會自動安裝到目標 PAN-OS 11.0.1 版本。

STEP 11 | 確認 ZTP 防火牆軟體升級。

1. 登入 Panorama 網頁介面。
2. 選取 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要）並導覽至 ZTP 防火牆。
3. 確認 **Software Version**（軟體版本）欄中顯示正確的目標 PAN-OS 版本。

STEP 12 | 有關所有未來的 PAN-OS 升級，請參閱 將防火牆從 Panorama 升級至 PAN-OS 11.1。

安裝 PAN-OS 軟體修補程式

這可在何處使用？	我需要哪些內容？
• 新世代防火牆	❑ 支援授權 ❑ PAN-OS 11.1.3 或更新 11.1 版本 ❑ 輸出網際網路存取權

查看 PAN-OS 11.1 版本資訊，然後使用下列程序安裝 PAN-OS 軟體修補程式，以解決目前在新世代防火牆上執行的 PAN-OS 版本錯誤及常見弱點和暴露 (CVE)。安裝 PAN-OS 軟體修補程式時會套用錯誤和 CVE 的修正程式，而無需安排長時間進行維護，並可讓您立即強化安全狀態，避免引入任何新的已知問題或變更安裝新 PAN-OS 版本可能產生的預設行為。此外，您也可以復原目前安裝的軟體修補程式，以解除安裝軟體修補程式時套用的錯誤和 CVE 修正程式。

安裝或復原 PAN-OS 軟體修補程式時會產生系統日誌（**Monitor**（監控） > **Logs**（日誌） > **System**（系統））。必須有輸出網際網路連線才能從 Palo Alto Networks 客戶支援入口網站下載 PAN-OS 軟體修補程式。

- 安裝
- 還原

安裝

STEP 1 | 登入防火牆網頁介面。

STEP 2 | 選取 **Device**（裝置） > **Software**（軟體）和 **Check Now**（立即檢查），從 Palo Alto Networks 更新伺服器檢索最新的 PAN-OS 軟體修補程式。

STEP 3 | 選取（啟用）**Include Patch**（包含修補程式）以顯示所有可用的 PAN-OS 軟體修補程式。

STEP 4 | 尋找目前安裝在新世代防火牆上的 PAN-OS 版本的軟體修補程式。

軟體修補程式由 **Version**（版本）名稱旁邊顯示的修補程式標籤表示。

STEP 5 | 查看 **More Info**（更多資訊），以檢視軟體修補程式詳細資訊，例如重要錯誤和 CVE 修正程式，以及是否需要重新啟動新世代防火牆才能套用修正項目。

STEP 6 | **Download**（下載）軟體修補程式。

（僅 HA）選取（啟用）同步至 HA 對等並 **Continue Download**（繼續下載）以下載 PAN-OS 軟體修補程式。

軟體修補程式下載成功後按一下 **Close**（關閉）。

STEP 7 | **Install**（安裝）軟體修補程式。

軟體修補程式安裝成功後，按一下 **Close**（關閉）。

STEP 8 | **Apply**（套用）軟體修補程式。

當系統提示您確認要將已安裝的 PAN-OS 軟體修補程式套用到新世代防火牆時，請按 **Apply**（套用）。

系統將顯示狀態欄，顯示 PAN-OS 軟體修補程式應用程式的目前進度。修補程式成功套用後，按一下 **Close**（關閉）。

此時如果需要重新啟動才能將 PAN-OS 軟體修補程式套用到新世代防火牆，則防火牆會自動重新啟動。

STEP 9 | （僅 HA）在防火牆 HA 對等上安裝 PAN-OS 軟體修補程式。

1. 登入 HA 對等的防火牆網頁介面。
2. 選取 **Device**（裝置） > **Software**（軟體） **Check Now**（立即檢查）。
3. **Install**（安裝）軟體修補程式。
4. 如有需要請重新啟動防火牆。

還原

STEP 1 | 登入防火牆網頁介面。

STEP 2 | 選取 **Device**（裝置） > **Software**（軟體）並找到您要還原的 PAN-OS 軟體修補程式。

STEP 3 | **Revert**（還原）軟體修補程式。

當系統提示您確認要還原安裝在新世代防火牆的 PAN-OS 軟體修補程式時，請按 **Revert**（還原）。

系統將顯示狀態欄，顯示 PAN-OS 軟體修補程式應用程式的目前進度。修補程式成功套用後，按一下 **Close**（關閉）。

此時如果需要重新啟動才能將 PAN-OS 軟體修補程式套用到新世代防火牆，則防火牆會自動重新啟動。

降級 PAN-OS

從 PAN-OS 11.1 降級防火牆的方式取決於您是要降級到舊版功能版本（PAN-OS 版本中的第一個或第二位數字變更，例如，從 9.1.2 降級到 9.0.8，或從 9.0.3 降級到 8.1.14），還是降級到相同功能版本內的維護發行版本（其中發行版本中的第三位數字變更，例如，從 8.1.2 降級到 8.1.0）。當您從一個功能版本降級到舊版功能版本時，您可以從較新版本移轉設定以適應新功能。若要將 PAN-OS 11.1 設定移轉至舊版 PAN-OS 版本，請先還原您要降級的功能版本的設定。當您在相同功能版本中從一個維護版本降級到另一個維護版本時，無需還原設定。

- 將防火牆降級至舊版維護版本
- 將防火牆降級至舊版功能版本
- 降級 Windows 代理程式

始終降級至與軟體版本相匹配的設定。軟體版本和設定不匹配可能會導致降級失敗或強制系統進入維護模式。這僅適用於從一個功能版本降級到另一個功能版本（例如，從 *9.0.0* 降級到 *8.1.3*），而不是降級到同一個功能發行版本中的維護版本（例如，從 *8.1.3* 降級到 *8.1.1*）。

如果降級時出現問題，您可能需要進入維護模式並將裝置重設為原廠預設值，然後從升級前匯出的原始設定檔還原設定。

將防火牆降級至舊版維護版本

因為維護版本不會引入新功能，您可以降級至相同功能版本中的舊版維護版本，而無需還原先前的設定。維護版本是發行版本中第三位數變更的版本，例如，從 10.1.6 降級到 10.1.4 被視為維護版本降級，因為只有發行版本的第三位數字有所不同。

使用下列程序來降級至相同功能版本中的舊版維護版本。

STEP 1 | 儲存目前組態檔案的備份。

雖然防火牆會自動建立設定的備份，但最佳做法是在降級前先建立備份，並將它儲存在外部。

1. **Export named configuration snapshot**（匯出具名設定快照）（**Device**（裝置） > **Setup**（設定） > **Operation**（操作））。
2. 選取包含執行中組態的 XML 檔案（例如 **running-config.xml**），然後按一下 **OK**（確定）匯出組態檔案。
3. 將匯出的檔案儲存至防火牆外部的位置。如果您在降級時發生問題，便可使用此備份還原設定。

STEP 2 | 安裝先前的維護版本映像。

如果您的防火牆無法從管理連接埠存取網際網路，您可以從 Palo Alto Networks 支援入口網站下載軟體更新。然後，您可以手動將它 ***Upload***（上傳）至防火牆。

1. **Check Now**（立即檢查）（**Device**（裝置） > **Software**（軟體））是否有可用的映像。

（PAN-OS 11.1.3 及更新版本）根據預設，系統會顯示慣用版本和相應的基礎版本。若要僅查看慣用版本，請停用（清除）**Base Releases**（基礎版本）核取方塊。

2. 找出您要降級的版本。如果尚未下載映像，請 **Download**（下載）。
3. 下載完成之後，請 **Install**（安裝）映像。
4. 安裝成功完成後，使用下列其中一種方法重新啟動：
   - 如果提示您重新啟動，請按一下**Yes**（是）。
   - 如果系統未提示您重新啟動，請移至「Device Operations（裝置操作）」（**Device**（裝置）> **Setup**（設定）> **Operations**（操作）），並選取 **Reboot Device**（重新啟動裝置）。

將防火牆降級至舊版功能版本

使用下列工作流程可還原在您升級至不同功能版本之前所執行的設定。升級後所做的任何變更都會遺失。因此，請務必備份您目前的設定，以便在恢復為較新的功能版本時還原這些變更。將防火牆降級至舊版功能版本之前，請先檢閱 升級/降級考量事項。

要從 *PAN-OS 11.1* 降級至更早的 *PAN-OS* 版本，您必須下載並安裝 *PAN-OS 10.1.3* 或更高的 *PAN-OS 10.1* 版本，然後才能繼續降級至目標 *PAN-OS* 版本。如果您嘗試降級至 *PAN-OS 10.1.2* 或更早的 *PAN-OS 11.1* 版本，則從 *PAN-OS 11.1* 降級會失敗。

使用下列程序以降級至舊版功能版本。

STEP 1 | 儲存目前組態檔案的備份。

雖然防火牆會自動建立設定的備份，但最佳做法是在升級前先建立備份，並將它儲存在外部。

1. **Export named configuration snapshot**（匯出具名設定快照）（**Device**（裝置）> **Setup**（設定）> **Operation**（操作））。
2. 選取包含執行中組態的 XML 檔案（例如 **running-config.xml**），然後按一下 **OK**（確定）匯出組態檔案。
3. 將匯出的檔案儲存至防火牆外部的位置。如果您在降級時發生問題，便可使用此備份還原設定。

STEP 2 | 安裝先前的功能版本映像。

升級至新版本時，將會建立自動儲存版本。

1. **Check Now**（立即檢查）（**Device**（裝置） > **Software**（軟體））是否有可用的映像。
2. 安裝 PAN-OS 10.1。

   從 PAN-OS 11.1 降級至舊版功能需要您先降級至 PAN-OS 10.1.3 或更高的 PAN-OS 10.1 版本。成功降級至 PAN-OS 10.1.3 或更高的 PAN-OS 10.1 版本後，您可以繼續降級至目標 PAN-OS 版本。

   1. 找到並 **Download**（下載）PAN-OS 11.1 映像。
   2. **Install**（安裝）PAN-OS 11.1 映像。
3. 找到要降級至的目標 PAN-OS 映像。如果尚未下載映像，請 **Download**（下載）。
4. 下載完成之後，請 **Install**（安裝）映像。
5. **Select a Config File for Downgrading**（選取用於降級的組態檔案），防火牆將在您重新啟動裝置後載入該檔案。多數情況下，您應選取在您從目前要降級的版本進行升級時自動儲存的設定。例如，如果您執行的是 PAN-OS 11.1，在降級至 PAN-OS 10.2.2 時，請選取 `autosave-10.2.2`。
6. 安裝成功完成後，使用下列其中一種方法重新啟動：
   - 如果提示您重新啟動，請按一下**Yes**（是）。
   - 如果系統未提示您重新啟動，請移至 [Device Operations（裝置操作）]（**Device**（裝置） > **Setup**（設定） > **Operations**（操作）），並選取 **Reboot Device**（重新啟動裝置）。

降級 Windows 代理程式

解除安裝 PAN-OS 11.1 基於 Windows 的 User-ID 代理程式後，請先執行下列步驟，然後再安裝舊版代理程式版本。

STEP 1 | 開啟 Windows 開始功能表，然後選取 **Administrative Tools**（系統管理工具）。

STEP 2 | 選取 **Computer Management**（電腦管理） > **Services and Applications**（服務和應用程式） > **Services**（服務），然後按兩下 **User-ID Agent**（**User-ID** 代理程式）。

STEP 3 | 選取 **Log On**（登入），再選取 **This account**（此帳戶），然後為 User-ID 代理程式帳戶指定使用者名稱。

STEP 4 | 輸入 **Password**（密碼）與 **Confirm Password**（確認密碼）。

STEP 5 | 按一下 **OK**（確定）儲存您的變更。

對您的 PAN-OS 升級進行疑難排解

要對您的 PAN-OS 升級進行疑難排解，請使用下表來檢閱可能的問題以及如何解決這些問題。

徵兆	解析度
軟體保固授權已過期。	從 CLI 中，刪除過期的授權金鑰： 1. 輸入 **delete license key <software license key>**。 2. 輸入 **delete license key Software_Warranty<expiredate>.key**。
最新的 PAN-OS 軟體版本不可用。	您只能看到先於當前安裝版本一個功能版本的軟體版本。例如，如果您安裝了 9.1 版本，則只有 10.0 版本可供您使用。若要查看 11.1 版本，您必須先升級至 10.1。
檢查動態更新失敗。	由於網路連線錯誤出現此問題。請參閱知識庫文章按下立即檢查按鈕後出現動態更新顯示錯誤。
未找到有效的裝置憑證。	在 PAN-OS 9.1.3 及更高版本中，如果您正在使用 Palo Alto Networks 雲端服務，則必須安裝裝置憑證。若要安裝裝置憑證： 1. 登入客戶支援入口網站。 2. 選取 **Generate OTP**（產生 **OTP**）（**Assets**（資產） > **Device Certificates**（裝置憑證））。 3. 在 **Device Type**（裝置類型）中，選取 **Generate OTP for Next-Gen Firewalls**（為新世代防火牆產生 **OTP**）。 4. 選取您的 PAN OS 裝置序號。 5. **Generate OTP**（產生 **OTP**）並複製一次性密碼。 6. 以管理員使用者的身分登入防火牆。 7. 選取 **Device Certificate**（裝置憑證）（**Device**（裝置） > **Setup**（設定） > **Management**（管理） > **Device**（裝置） > **Certificate**（憑證），然後選取 **Get Certificate**（獲取憑證）。 8. 貼上 OTP，然後按一下 **OK**（確定）。

徵兆	解析度
由於映像驗證錯誤，軟體映像檔案無法載入到軟體管理器中。	要更新軟體映像清單，請按一下 **Check Now**（立即檢查）。這將與更新伺服器建立新連線。
VMware NSX 外掛程式版本與新軟體版本不相容。	升級到 8.0 時，會自動安裝 VMware NSX 外掛程式。如果您不使用外掛程式，您可以解除安裝外掛程式。
升級到 PAN-OS 9.1 後的重新啟動時間比預期得要長。	升級至應用程式和威脅內容版本 8221 或更高版本。請參閱 <xref to 11.1 Associated Software and Content Versions>，瞭解關於最低軟體和內容版本的詳細資訊。
即使授權處於作用中狀態，該裝置也沒有支援。	在 **Device**（裝置） > **Software**（軟體）中，按一下 **Check Now**（立即檢查）。 這將透過建立與更新伺服器的新連線來更新防火牆上的授權資訊。 如果這不起作用，從網頁介面，使用 **`request system software check`**。
防火牆不具有由 DHCP 伺服器指派的 DHCP 位址。	設定安全性原則規則，允許從 ISP DHCP 伺服器到內部網路的流量。
防火牆會不斷啟動進入維護模式。	在 CLI 中，存取維護復原工具 (MRT)。在 MRT 視窗中，選取 **Continue**（繼續） > **Disk Image**（磁碟映像）。選取 **Reinstall**（重新安裝）**<current version>**或 **Revert to**（還原至）**<previous version>**。還原或重新安裝操作完成後，選取 **Reboot**（重新啟動）。
在 HA 設定中，升級對等防火牆時出現防火牆太舊的錯誤後，防火牆會進入暫停狀態。	將一個防火牆升級到多個主要發行版本會導致網路中斷。在升級到下一個主要版本之前，您必須先將兩個防火牆升級一個主要版本。 將對等防火牆降級至暫停執行的防火牆停止時的版本。

升級 VM-Series 防火牆

升級 VM-Series PAN-OS 軟體（獨立）

升級 VM-Series PAN-OS 軟體 （HA 配對）

使用 Panorama 升級 VM-Series PAN-OS 軟體

升級 PAN-OS 軟體版本（NSX 專用 VM-Series）

選取最適合您部署的升級方法。

- 在維護時段升級 NSX 專用 VM-Series — 在維護時段使用此選項升級 VM-Series 防火牆，而不變更服務定義中的 OVF URL。
- 升級 NSX 專用 VM-Series 而不中斷流量 — 使用此選項升級 VM-Series 防火牆，而不中斷對來賓 VM 的服務或變更服務定義中的 OVF URL。

下圖顯示目前支援的 Panorama 與 VMware NSX 專用 Panorama 外掛程式組合，以及成功升級所需遵循的升級路徑。

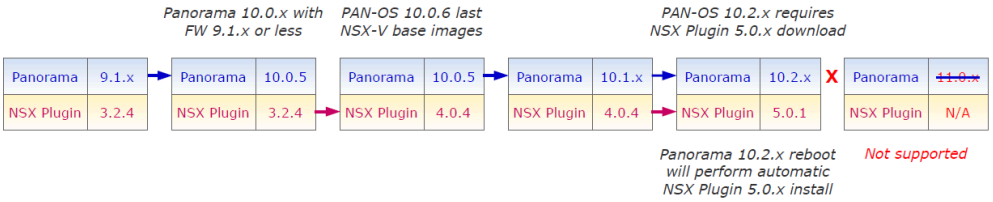
- 以下每個方塊代表一種支援的組合。
- 升級 HA 配對中的 NSX 專用 Panorama 外掛程式或 Panorama 時，請先升級被動 Panorama 對等，之後再升級主動 HA 對等。

升級 VMware NSX 專用 VM-Series 部署之前，請檢閱如下所示的升級路徑，以瞭解哪些升級步驟所達到的外掛程式和 PAN-OS 組合，最適合您的環境。

Panorama and PAN NSX Plugin Upgrade Paths

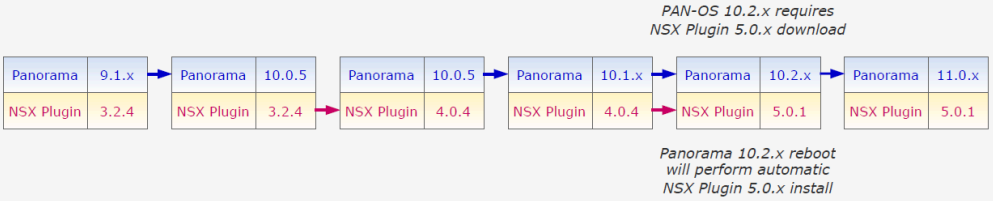
- For Panorama upgrades, first upgrade Panorama HA Passive, then Panorama HA Active
- For NSX Plugin upgrades, first upgrade Panorama HA Passive, then Panorama HA Active
- Best practice is always upgrade one at a time (either Panorama or NSX Plugin)

VM-Series for NSX-V



IMPORTANT! PAN-OS 10.0.6 are the last available base images for VM-Series for NSX-V.

VM-Series for NSX (formerly NSX-T)



IMPORTANT! VMware NSX-T has been renamed to VMware NSX as of version 4.0.x.

在維護時段升級 NSX 專用 VM-Series

在不影響流量的情況下升級 NSX 專用 VM-Series

升級 VM-Series 型號

VM-Series 防火牆的授權程序會使用 UUID 和 CPU ID，為每個 VM-Series 防火牆產生唯一的序號。因此，當您產生授權時，會將授權對應至 VM-Series 防火牆的特定實例且無法修改。

若是下列情況，請依照本節的指示：

- 將評估授權移轉至生產授權。
- 升級型號以增加容量。例如，您想要從 VM-100 升級至 VM-300-型號。

- 升級容量，這將在防火牆上重新啟動一些重要程序。建議使用 *HA* 組態以避免服務中斷；若要在 *HA* 配對升級容量，請參閱升級 HA 配對中的 VM-Series 型號。
- 在私人或公共雲部署中，如果是以 *BYOL* 選項授權您的防火牆，則在變更實例類型或 *VM* 類型之前，必須停用 VM。升級型號或實例會變更 *UUID* 和 *CPU ID*，因此在…時，您必須套用授權。

STEP 1 | 配置額外硬體資源給 VM-Series 防火牆。

在起始容量升級之前，您必須確認有足夠硬體資源可供 VM-Series 防火牆支援新的容量。在每個 Hypervisor 上指派額外硬體資源的程序都不同。

若要查看您的新 VM-Series 型號的硬體需求，請參閱 VM-Series 型號。

雖然容量升級不需要重新啟動 VM-Series 防火牆，但您需要關閉虛擬機器才能變更硬體配置。

STEP 2 | 從客戶支援入口網站擷取授權 API 金鑰。

1. 登入客戶支援入口網站。

   確保您使用的帳戶是您用來註冊初始授權的同一個帳戶。

2. 從左側功能表中，選取 **Assets**（資產） > **API Key Management**（**API** 金鑰管理）。
3. 複製 API 金鑰。

tion Programming Interface (API) key is a unique identifier that authenticates a user or app calling Palo Alto Networks REST APIs. Each
ific Palo Alto Networks service. For example, Licensing API key work only with Licensing APIs, and Threat Vault API keys work only with

PI key Licensing API

ing APIs to manage firewall licenses (e.g., renew licenses, register auth codes, retrieve licenses attached to auth codes, deactivate licens

Licensing API key, click the Enable link below. You can also revoke an API key or regenerate an API key (which revokes the previous API

ate 12/06/2024

Extend Regenerate

STEP 3 | 在防火牆上，使用 CLI 安裝上一步所複製的 API 金鑰。

```
request license api-key set key <key>
```

STEP 4 | （如果您可存取網際網路）在 **Device**（裝置） > **Setup**（設定） > **Service**（服務）上，允許防火牆 **Verify Update Server identity**（驗證更新伺服器識別）。

STEP 5 | **Commit**（提交）您的變更。確定您在防火牆上有本機設定的使用者。如果設定超出未授權的 PA-VM 物件限制，在停用之後，Panorama 推送的使用者可能會無法使用。

STEP 6 | 升級容量。

選取 **Device**（裝置） > **Licenses**（授權） > **Upgrade VM Capacity**（升級 **VM** 容量），然後採用下列其中一種方式啟動授權與訂閱：

- （網際網路）**Retrieve license keys from license server**（從授權伺服器擷取授權金鑰）—如果您已在客戶支援入口網站上啟動您的授權，請使用此選項。
- （網際網路）**Use an authorization code**（使用授權碼） — 使用此選項可利用授權碼暫代先前尚未在支援入口網站上啟動的授權，升級 VM-Series 容量。出現提示時，請輸入 **Authorization Code**（授權碼），然後按一下 **OK**（確定）。
- （無網際網路）手動上傳授權金鑰—如果您的防火牆未經由網際網路連線至客戶支援入口網站，請使用此選項。從可存取網際網路的電腦登入 CSP，下載授權金鑰檔，將金鑰檔傳輸到防火牆所在相同網路中的電腦，然後上傳到防火牆。

STEP 7 | 確認已成功授權防火牆。

在 **Device**（裝置） > **Licenses**（授權）頁面上，確認已成功啟動授權。

升級 HA 配對中的 VM-Series 型號

將 VM-Series 防火牆降級為舊版

升級 **Panorama** 外掛程式

Panorama 外掛程式升級/降級考量事項

以下表格列出了具有升級或降級影響的新功能。在從 PAN-OS 11.1 版本升級至或降級之前，請確保瞭解全部升級/降級考量事項。如需有關 PAN-OS 11.1 版本的其他資訊，請參閱 PAN-OS 11.1 版本資訊。

表 **1: Panorama** 外掛程式升級**/**降級考量事項

功能	升級考量事項	降級考量事項
Panorama 外掛程式 • AWS 外掛程式 • Azure 外掛程式 • Kubernetes 外掛程式 • 軟體防火牆授權外掛程式 • SD-WAN 外掛程式 • IPS 特徵碼轉換器外掛程式 • ZTP 外掛程式 • 企業 DLP 外掛程式 • Openconfig 外掛程式 • GCP 外掛程式 • Cisco ACI 外掛程式 • Nutanix 外掛程式 • VCenter 外掛程式	在升級至 PAN-OS 11.1 之前，您必須為 Panorama 上安裝的所有外掛程式下載 PAN-OS 11.1 支援的 Panorama 外掛程式版本。需要執行此步驟以成功地升級至 PAN-OS 11.1。請參閱相容性矩陣，瞭解詳細資訊 。	若要從 PAN-OS 11.0 降級，您必須下為 Panorama 上安裝的所有外掛程式下載 PAN-OS 10.2 和更早版本支援的 Panorama 外掛程式版本。請參閱 Panorama 外掛程式相容性矩陣，瞭解詳細資訊。
	（企業 DLP）將 Panorama 升級至 PAN-OS 10.2 後，您必須在執行 PAN-OS 11.1 或更早版本的所有受管理防火牆上安裝應用程式和威脅內容版本 8520。需要執行此步驟以利用未升級至 PAN-OS 10.2 的企業 DLP 成功地將設定變更推送到受管理的防火牆。	
	（企業 DLP）載入包含共用企業 DLP 設定的 Panorama 設定備份會刪除掃描非基於檔案的流量所需的共用應用程式排除篩選器。	
	(SD-WAN) PAN-OS 11.0 不支援 SD-WAN 2.2 和更早版本的 Panorama 外掛程式。 在安裝 SD-WAN 2.2 或更早版本的 Panorama 外掛程式時將 Panorama 管理伺服器升級至 PAN-OS 11.1 會導致 SD-WAN 外掛程式隱藏在 Panorama 網頁介面中或導致 SD-WAN 設定被刪除。在這兩種情況下，您都無法安裝新的 SD-WAN 外掛程式	

功能	升級考量事項	降級考量事項
	版本或解除安裝 SD-WAN 外掛程式。	
SD-WAN	成功將 Panorama 升級至 PAN-OS 11.1 並將 Panorama 外掛程式由 SD-WAN 2.0.0 版本升級至 SD-WAN 3.0 版本後，您必須僅為現有 SD-WAN 部署清除 Panorama 上的 SD-WAN 快取。 清除 SD-WAN 快取並不會刪除任何現有的 SD-WAN 設定，但會刪除 SD-WAN 3.0 版本的 Panorama 外掛程式中所引入之新格式的 IP 位址、通道和閘道命名慣例。 對於 SD-WAN 的新部署，如果您在升級至 PAN-OS 11.0 之後，在 Panorama 上安裝了 SD-WAN 3.0 版本的 Panorama 外掛程式，則無需清除 Panorama 上的 SD-WAN 快取。 1. 登入 Panorama CLI。 2. 清除 Panorama 上的 SD-WAN 快取。 ``` admin> debug plugins sd_wan drop-config-cache all ```	無。

升級 Panorama 外掛程式

請遵循以下程序升級 Panorama 管理伺服器上安裝的多數外掛程式版本。升級以下任一種外掛程式時，請遵循連結中的程序。若要升級到最新的 VM-Series 外掛程式，

- 升級企業 DLP 外掛程式
- 升級 Panorama Interconnect 外掛程式
- 升級 VMware NSX 專用 Panorama 外掛程式時，請參閱 VMware NSX 文件專用 VM-Series。

STEP 1 | 請參閱相容性矩陣，瞭解每個 Panorama 外掛程式支援的最低 PAN-OS 版本。

STEP 2 | 查看 Panorama 外掛程式版本資訊以確認您的目標外掛程式版本。

STEP 3 | 檢閱 Panorama 外掛程式升級/降級考量事項。

STEP 4 | 下載外掛程式。

1. 選取 **Panorama** > **Plugins**（外掛程式）。
2. 選取 **Check Now**（立即檢查） 以擷取可用更新清單。
3. 選取 Action（動作）欄中的 **Download**（下載）以下載外掛程式。

STEP 5 | 安裝外掛程式。

選取您在先前步驟下載的外掛程式版本，在 [Action（動作）] 欄中按一下 **Install**（安裝）來安裝外掛程式。安裝完成時，Panorama 會通知您。

第一次在 *Panoramas HA* 配對上安裝外掛程式時，請先將外掛程式安裝於被動對等體，再安裝於主動對等體。在被動端點上安裝外掛程式之後會轉換為非運作狀態。接著，在成功在主動對等體安裝外掛程式後，被動對等體會再轉為運作狀態。

STEP 6 | 選用您可以使用以下 CLI 命令查看外掛程式升級日誌。

```
tail plugins-log ... tail mp-log plugin_install.log
```

升級企業 DLP 外掛程式

升級 Panorama™ 管理伺服器上安裝的企業資料遺失防護 (DLP) 外掛程式版本。

請參閱 Palo Alto Networks Panorama 外掛程式相容性矩陣並檢閱目標企業 DLP 外掛程式版本所需的最低 PAN-OS 版本。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 在 Panorama 上升級企業 DLP 外掛程式版本。

對於採用高可用性 (HA) 設定的 Panorama，在 Panorama HA 對等上重複此步驟。

1. 選取 **Panorama** > **Plugins**（外掛程式）和 **Check Now**（立即檢查），瞭解最新的 **dlp** 外掛程式版本。
2. **Download**（下載）並 **Install**（安裝）最新版本的企業 DLP 外掛程式。
3. 新外掛程式版本成功安裝後，檢視 Panorama **Dashboard**（儀表板）並在「一般資訊」Widget 中確認 `Plugin DLP` 版本顯示了您升級至的企業 DLP 外掛程式。

STEP 3 | （僅限升級至 4.0.0） 編輯企業 DLP 資料篩選設定以將 **Max File Size**（最大檔案大小）減小到 20MB 或以下。

在從企業 DLP 3.0.3 或更高版本的 Panorama 外掛程式升級至企業 DLP 4.0.0 時必須執行此步驟，因為此外掛程式版本不支援大型檔案大小檢查。

升級 Panorama Interconnect 外掛程式

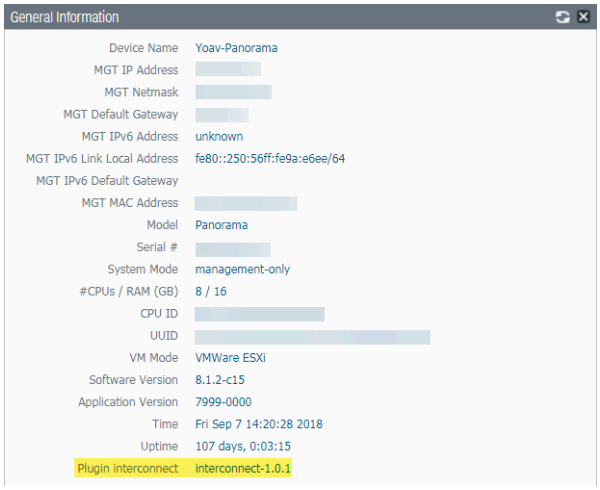
使用下列程序在 Panorama 控制器和 Panorama 節點上升級 Panorama™ Interconnect 外掛程式。升級 Panorama Interconnect 外掛程式時，您必須先升級 Panorama 控制器，再將 Panorama 節點升級至與控制器相同的外掛程式版本。您在 Panorama 節點上下載和安裝的新外掛程式版本必須與在 Panorama 控制器上安裝的版本相同，以確保 Panorama 控制器和選定 Panorama 節點上的外掛程式版本保持同步。

如果這是您第一次安裝外掛程式，請參閱設定 Panorama Interconnect 外掛程式。

STEP 1 | 登入 Panorama 控制器的 Panorama 網頁介面。

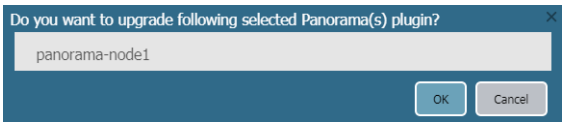
STEP 2 | 在 Panorama 控制器上升級 Panorama Interconnect 外掛程式。

1. 選取 **Panorama** > **Plugins**（外掛程式），然後搜尋 **`Interconnect`**。
2. **Download**（下載）並 **Install**（安裝）新的 Interconnect 外掛程式版本。提示即會顯示，通知您安裝已完成。
3. 確認 **Dashboard**（儀表板）顯示新安裝的 Interconnect 外掛程式版本。

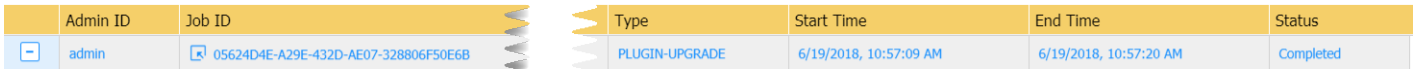


STEP 3 | 在 Panorama 節點上升級 Panorama Interconnect 外掛程式。

1. 選取 **Panorama** > **Interconnect** > **Panorama Nodes**（**Panorama** 節點），選取一個或多個 Panorama 節點，然後 **Upgrade Plugin**（升級外掛程式）。
2. 確認已選取 Panorama 節點，然後按一下 **OK**（確定），開始外掛程式升級。



3. 等待直至外掛程式升級工作 `Completed`（已完成）。按一下**Panorama** > **Interconnect** > **Tasks**（工作），檢視工作進度。



4. 升級成功完成後，選取 **Panorama** > **Interconnect** > **Panorama Nodes**（**Panorama** 節點），確認 **Plugin**（外掛程式）版本適用於選定的 Panorama 節點。

安裝/升級 SD-WAN 外掛程式與相容的 PAN-OS 版本

這可在何處使用？	我需要什麼？
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

請務必確保現有網路架構保持最新狀態且能升級其功能以享有新功能。SD-WAN 升級指南能協助網路管理員升級與 SD-WAN 外掛程式版本相容的 Panorama 管理伺服器和 Palo Alto Networks 防火牆。

在真正開始升級或降級程序之前，請規劃好適當的升級或降級計畫。請參考目前安裝的 SD-WAN 外掛程式版本的可行升級和降級路徑。

在繼續升級程序之前，請確認您滿足以下條件：

- 備份每台裝置上的所有設定。
- 參閱 Panorama 外掛程式相容性矩陣，查看適用於 SD-WAN 的 Panorama 外掛程式每個版本中的功能。
- 您擁有 Palo Alto Networks 裝置的管理員存取權限。

先決條件

升級 Panorama HA 配對之前，請務必儲存設定檔案、建立技術支援檔案並檢查裝置的相容內容發行版本。

備份您的設定檔案

備份目前的設定檔案。建議您備份目前的 Panorama 和防火牆設定：

- 升級裝置前請先備份 Panorama 和防火牆設定。
- 儲存並匯出 Panorama 和防火牆設定以還原該備份。
- 儲存並匯出防火牆設定以還原該備份。

如果升級過程出現問題，您可以在 Panorama 管理伺服器管理的防火牆載入設定備份，使用這些備份來還原設定。

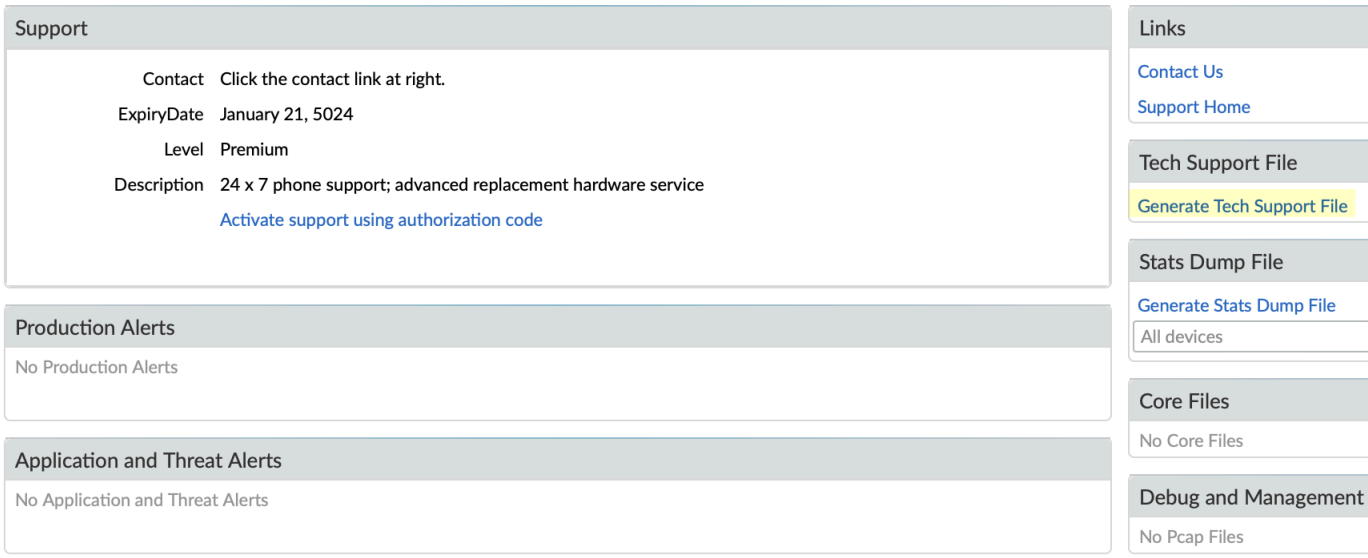
產生技術支援檔案

請務必產生技術支援檔案以進行偵錯。

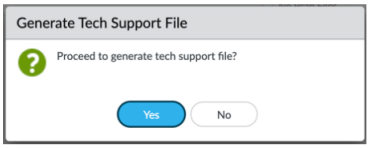
1. 選取 **Device**（裝置） > **Support**（支援）並 **Generate Tech Support File**（產生技術支援檔案）。

   請務必須在兩個 HA 配對上產生技術支援檔案以進行偵錯。

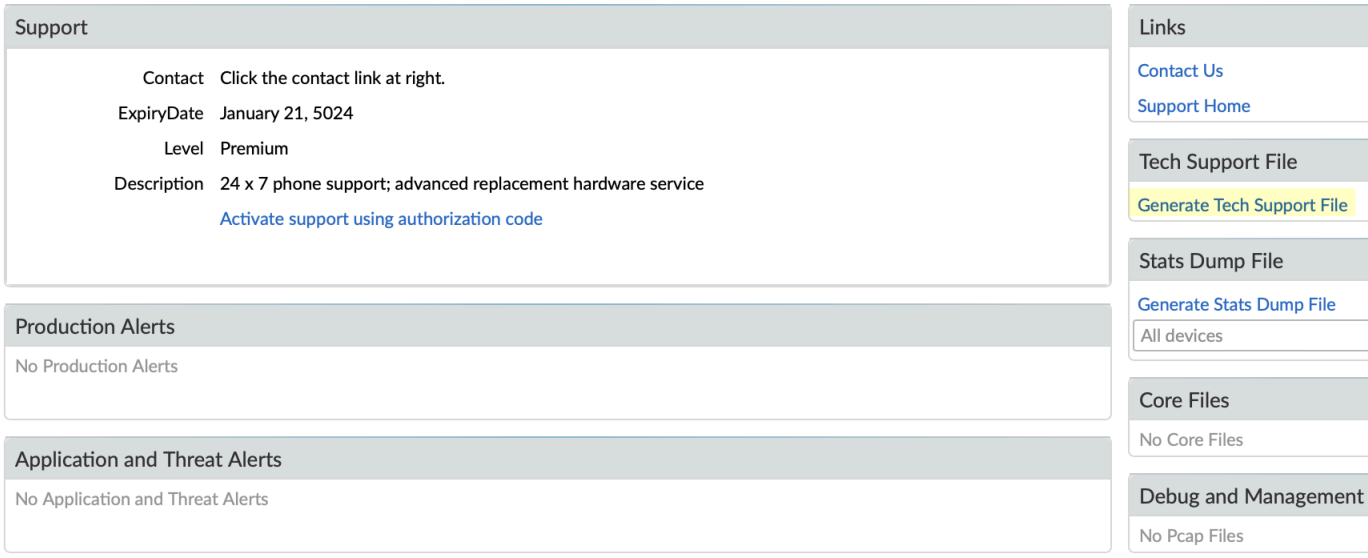
   產生技術支援檔案可能需要幾分鐘的時間。



2. 當提示產生技術支援檔案時按一下 **Yes**（是）。



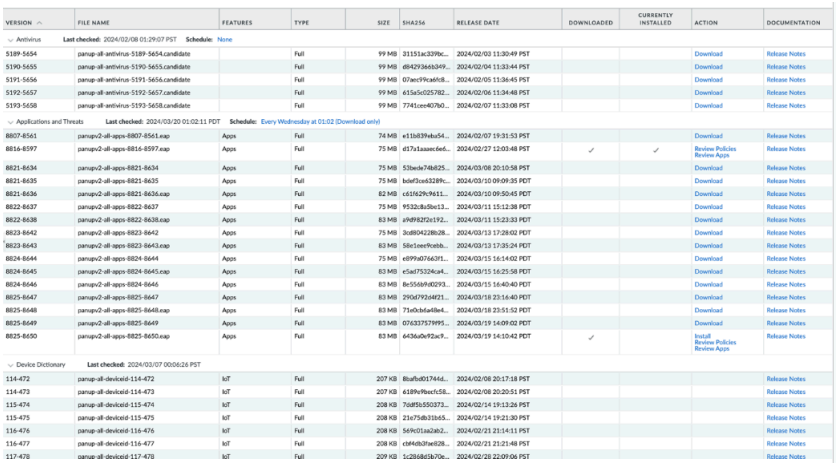
3. 按一下 **Download Tech Support File**（下載技術支援檔案），將其儲存在防火牆或 Panorama。



安裝相容內容發行版本

確定每個防火牆和 Panorama HA 配對都執行最新的內容發行（**Applications and Threats**（應用程式與威脅））版本。

所有防火牆和 *Panorama* 皆必須下載並安裝相同版本的 ***Applications and Threats***（應用程式與威脅）才能成功升級。



請參閱相應的版本資訊，瞭解您必須為相應 PAN-OS 版本安裝的最低內容發行（例如 **Applications and Threats**（應用程式與威脅））版本。請遵循應用程式與威脅內容更新的最佳做法。

您執行特定 PAN-OS 版本的防火牆和 Panorama 必須包含與 PAN-OS 版本相容的最低內容發行（**Applications and Threats**（應用程式與威脅））版本。

請透過以下工作流程下載並安裝與 PAN-OS 版本相容的內容發行版本：

1. 如果是防火牆，請選取 **Device**（裝置） > **Dynamic Updates**（動態更新）；如果是 Panorama，請選取 **Panorama** > **Dynamic Updates**（動態更新）以確認 **Applications and Threats**（應用程式與威脅）的版本資訊。
2. **Check Now**（立即檢查）以擷取可用更新清單。
3. 找出並 **Download**（下載）適當的內容發行版本。在您成功下載內容更新檔案後，該內容發行版本的 [Action（動作）] 欄中的連結會從 **Download**（下載）變更為 **Install**（安裝）。
4. 在 Palo Alto Networks 裝置上 **Install**（安裝）更新。

升級 Panorama 的重要注意事項

以下是在 Panorama 管理伺服器上升級 SD-WAN 外掛程式版本的重要注意事項：

- （僅 HA 部署）主動和被動 Panorama 必須具有相同的 Panorama 軟體和 SD-WAN 外掛程式版本。
- （僅 HA 部署）在升級後和 **commit**（提交）或 **commit all**（全部提交）之前，請確認 Panorama 和 Palo Alto Networks 新世代防火牆維持相同 HA 狀態，才能盡量減少設定變更。
- 請一律讓 Panorama 軟體版本高於 PAN-OS 版本。
- 如需詳細瞭解 SD-WAN 外掛程式版本的 MongoDB 同步狀態，請參閱 涵蓋 SD-WAN 資料庫收集的 MongoDB 同步狀態。

- （僅 *HA* 部署）您必須同時升級主動和被動 *Panorama HA* 配對。
- 完成 *SD-WAN* 外掛程式升級後，您必須透過 *Palo Alto Networks* 裝置上的 *CLI* 命令（在設定模式）執行 *commit force*。如果您執行全部提交而非 *commit force*，您將遺失該裝置上的所有 *SD-WAN* 設定。

升級完成後，請注意升級後的變更項目。

SD-WAN 外掛程式的升級和降級路徑

這可在何處使用？	我需要什麼？
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

在升級或降級 SD-WAN 外掛程式之前，您必須知道哪些適當的外掛程式版本可以從防火牆上目前安裝的 SD-WAN 外掛程式版本進行升級或降級。

升級和降級考量事項

- 如果您需要升級 ***SD-WAN*** 外掛程式，請勿升級到我們在您目前安裝的版本之前發佈的版本。

  例如，我們不支援從 *SD-WAN* 外掛程式版本 *3.0.7* 升級到 *SD-WAN* 外掛程式版本 *3.2.0*，因為我們在 *SD-WAN* 外掛程式 *3.0.7* 之前先發佈了 *SD-WAN* 外掛程式版本 *3.2.0*。

  但是，您可以從任何維護版本升級到相同的主要或次要版本中的另一個維護版本。例如，您可以從任何 *SD-WAN 2.2* 升級到任何其他 *SD-WAN 2.2* 外掛程式版本。
- 如果您需要降級 ***SD-WAN*** 外掛程式，請勿降級到我們在您目前安裝的版本之後發佈的版本。

  例如，我們不支援從 *SD-WAN* 外掛程式版本 *3.2.0* 降級到 *SD-WAN* 外掛程式版本 *3.0.7*，因為我們在 *SD-WAN* 外掛程式 *3.2.0* 之後才發佈 *SD-WAN* 外掛程式版本 *3.0.7*。

因此，在移轉計畫的第一步驟中，請務必先參考目前安裝的 *SD-WAN* 外掛程式版本的可行升級和降級路徑。

SD-WAN 外掛程式的升級路徑

升級表的資訊解釋如下：

- **Upgrade From**（原始版本）—升級前的目前 SD-WAN 外掛程式版本。
- **To SD-WAN Plugin Version**（升級後 **SD-WAN** 外掛程式版本）—您可以從目前 SD-WAN 外掛程式版本進行升級的 SD-WAN 外掛程式版本。
- **To SD-WAN Plugin Version (Recommended)**（升級後 **SD-WAN** 外掛程式版本（建議））—建議您從目前 SD-WAN 外掛程式版本進行升級的目標 SD-WAN 外掛程式版本。

例如，您可以從 SD-WAN 外掛程式版本 2.2.1 升級到 SD-WAN 外掛程式版本 2.2.2、2.2.3、2.2.4、2.2.5、2.2.6 以及更新 2.2 版本。但是，在所有可行的 SD-WAN 外掛程式

版本中（2.2.2、2.2.3、2.2.4、2.2.5、2.2.6 和更新 2.2 版本）中，我們推薦的版本是 2.2.6。請注意，您無法直接從 SD-WAN 2.2.1 升級到 3.0.7。您必須先將 SD-WAN 外掛程式從 2.2.1 升級到 2.2.6（建議版本），然後再升級到 3.0.7。

以下是 SD-WAN 外掛程式版本的升級路徑。執行 SD-WAN 升級時，目標外掛程式版本會執行移轉程序。

原始版本（目前安裝版本）	升級到允許的 **SD-WAN** 外掛程式版本	升級到推薦的 **SD-WAN** 外掛程式版本
SD-WAN 外掛程式 **2.2** 版本		
2.2.1	2.2.2、2.2.3、2.2.4、2.2.5、2.2.6 及更新 2.2 版本	2.2.6
2.2.2	2.2.3、2.2.4、2.2.5、2.2.6 及更新 2.2 版本	2.2.6
2.2.3	2.2.4、2.2.5、2.2.6 及更新 2.2 版本	2.2.6
2.2.4	2.2.5、2.2.6 及更新 2.2 版本	2.2.6
2.2.5	2.2.6 及更新 2.2 版本	2.2.6
2.2.6	• 3.0.7 及更新 3.0 版本 • 3.1.3 及更新 3.1 版本 • 3.2.1 及更新 3.2 版本 • 3.3.0 及更新 3.3 版本	2.2.6
SD-WAN 外掛程式 **3.0** 版本		
3.0.0	3.0.5	—
3.0.1	3.0.5	—
3.0.2	3.0.5	—
3.0.3	3.0.5	—
3.0.4	3.0.5	—
3.0.5	• 3.0.6 • 3.0.7 及更新 3.0 版本 • 3.1.0-hf	3.0.7-h2、3.1.3、3.2.1、3.3.0

原始版本（目前安裝版本）	升級到允許的 **SD-WAN** 外掛程式版本	升級到推薦的 **SD-WAN** 外掛程式版本
	• 3.1.1、3.1.3 及更新 3.1 版本 • 3.2.0 • 3.2.1 及更新 3.2 版本 • 3.3.0 及更新 3.3 版本	
3.0.6	• 3.0.7 及更新 3.0 版本 • 3.1.3 及更新 3.1 版本 • 3.2.0 • 3.2.1 及更新 3.2 版本 • 3.3.0 及更新 3.3 版本	3.0.7-h2、3.1.3、3.2.1、3.3.0
3.0.7	• 3.1.3 及更新 3.1 版本 • 3.2.1 及更新 3.2 版本 • 3.3.0 及更新 3.3 版本	3.1.3、3.2.1、3.3.0
SD-WAN 外掛程式 **3.1** 版本		
3.1.0	• 3.1.1 • 3.1.3 及更新 3.1 版本 • 3.2.0 • 3.2.1 及更新 3.2 版本 • 3.3.0 及更新 3.3 版本	3.1.3、3.2.1、3.3.0
3.1.1	• 3.1.3 及更新 3.1 版本 • 3.2.0 • 3.2.1 及更新 3.2 版本 • 3.3.0 及更新 3.3 版本	3.1.3、3.2.1、3.3.0
3.1.2	• 3.1.3 及更新 3.1 版本 • 3.2.0 • 3.2.1 及更新 3.2 版本 • 3.3.0 及更新 3.3 版本	3.1.3、3.2.1、3.3.0
3.1.3	• 3.2.1 及更新 3.2 版本 • 3.3.0 及更新 3.3 版本	3.2.1 及 3.3.0
SD-WAN 外掛程式 **3.2** 版本		

原始版本（目前安裝版本）	升級到允許的 **SD-WAN** 外掛程式版本	升級到推薦的 **SD-WAN** 外掛程式版本
3.2.0	• 3.2.1 及更新 3.2 版本 • 3.3.0 及更新 3.3 版本	3.2.1 及 3.3.0
3.2.1	3.3.0 及更新 3.3 版本	3.3.0

SD-WAN 外掛程式的降級路徑

降級表的資訊解釋如下：

- **Downgrade From**（原始版本）—降級前的目前 SD-WAN 外掛程式版本。
- **To SD-WAN Plugin Version**（升級後 **SD-WAN** 外掛程式版本）—您可以從目前 SD-WAN 外掛程式版本進行降級的 SD-WAN 外掛程式版本。
- **To SD-WAN Plugin Version (Recommended)**（升級後 **SD-WAN** 外掛程式版本（建議））—建議您從目前 SD-WAN 外掛程式版本進行降級的目標 SD-WAN 外掛程式版本。

以下是 SD-WAN 外掛程式版本的降級路徑。執行 SD-WAN 降級時，目前的外掛程式版本會執行移轉程序。

原始版本（目前安裝版本）	升級到允許的 **SD-WAN** 外掛程式版本
2.2.2、2.2.3、2.2.4、2.2.5 及 2.2.6	2.2.1
2.2.3、2.2.4、2.2.5 及 2.2.6	2.2.2
2.2.4、2.2.5 及 2.2.6	2.2.3
2.2.5 及 2.2.6	2.2.4
2.2.6	2.2.5
3.0.7、3.1.3、3.2.1 及 3.3.0	2.2.6
3.0.5	3.0.0、3.0.1、3.0.2、3.0.3 及 3.0.4
3.0.6、3.0.7、3.1.0-hf、3.1.1、3.1.3、3.2.0、3.2.1 及 3.3.0	3.0.5
3.0.7、3.1.3、3.2.0、3.2.1 及 3.3.0	3.0.6
3.1.3、3.2.1 及 3.3.0	3.0.7
3.1.1、3.1.3、3.2.0、3.2.1 及 3.3.0	3.1.0
3.1.3、3.2.0、3.2.1 及 3.3.0	3.1.1

原始版本（目前安裝版本）	升級到允許的 **SD-WAN** 外掛程式版本
3.1.3、3.2.0、3.2.1 及 3.3.0	3.1.2
3.2.1 及 3.3.0	3.1.3 及 3.2.0

安裝 SD-WAN 外掛程式

在利用 SD-WAN 的 Panorama™ 管理伺服器和防火牆上，安裝 SD-WAN 外掛程式版本。

請參閱 Palo Alto Networks Panorama 外掛程式相容性矩陣並檢閱目標 SD-WAN 外掛程式版本所需的最低 PAN-OS 版本。

STEP 1 | 登入 Panorama 網頁介面。

STEP 2 | 在 Panorama 上，安裝 SD-WAN 外掛程式版本。

對於採用高可用性 (HA) 設定的 Panorama，在 Panorama HA 對等上重複此步驟。

1. 選取 **Panorama** > **Plugins**（外掛程式）和 **Check Now**（立即檢查），瞭解最新的 **sd_wan** 外掛程式版本。
2. **Download**（下載）並 **Install**（安裝） SD-WAN 外掛程式的最新版本。

STEP 3 | 成功安裝新的外掛程式版本之後，請檢視 Panorama **Dashboard**（儀表板），並在「一般資訊」Widget 中確認 `SD-WAN plugin` 顯示您已安裝的 SD-WAN 外掛程式版本。

利用 SD-WAN 外掛程式升級 Panorama 高可用性配對（主動/被動）

這可在何處使用？	我需要什麼？
• PAN-OS • SD-WAN	☐ SD-WAN plugin license

請根據 Panorama 管理伺服器正在執行的 SD-WAN 外掛程式版本遵循升級路徑。

執行 **SD-WAN** 外掛程式版本的 **Panorama**	請遵循以下步驟
1.0.x	Panorama HA 配對：將 SD-WAN 外掛程式 1.0.4 升級至 2.2.6 版本
2.1.x	Panorama HA 配對：將 SD-WAN 外掛程式 2.1.x 升級至 2.2.6 版本
2.2.6	Panorama HA 配對：將 SD-WAN 外掛程式 2.2.6 升級至 3.0.7 版本

Panorama HA 配對：將 SD-WAN 外掛程式 1.0.4 升級至 2.2.6 版本

當您的 Panorama 透過 1.0.x 到 2.2.x 間任何 SD-WAN 外掛程式版本進行安裝時，如果您想升級 SD-WAN 外掛程式版本，則必須先升級到 SD-WAN 外掛程式版本 2.2.6（而非任何中間版本）。因為 SD-WAN 2.2.6 版本包含新功能、錯誤修正、效能改進和增強功能。

建議您一律讓 Panorama 軟體版本高於 PAN-OS 版本。例如，如果您的 Panorama 版本是 10.1.9，則您的 PAN-OS 版本可以是任何比 PAN-OS 10.1.9 更舊的版本。

開始升級程序之前，請先閱讀升級 Panorama 的重要注意事項。

請以相同順序遵循以下工作流程，以 SD-WAN 2.2.6 外掛程式版本升級 Panorama HA 配對。

STEP 1 | 升級 Panorama 管理伺服器版本。

1. 從 Panorama 9.1.x 在主動和被動 Panorama 下載並安裝 Panorama 10.0.7-h3。
2. 從 Panorama 10.0.7-h3 在主動和被動 Panorama 下載並安裝最新 Panorama 10.1 版本。
3. 將 Panorama 升級至最新 10.1 版本後，請檢查主動 Panorama 是否保持主動狀態，而被動 Panorama 則保持被動。如果 HA 狀態沒有變更，則表示升級成功。否則您便需要執行強制切換，以維持升級前的 HA 配對狀態。

   若要執行強制切換，請以同一順序從目前的作用中 HA 對等執行下列 CLI 命令。

   ```
   管理員 > 要求高可用性狀態暫停
   ```

   ```
   管理員 > 要求高可用性狀態功能
   ```

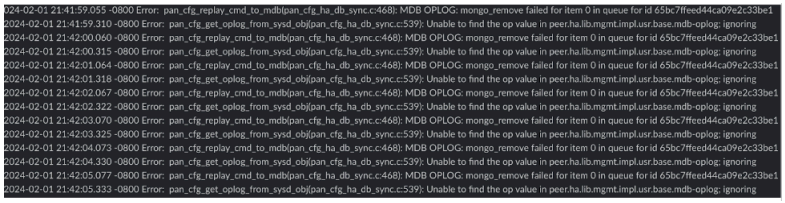
   ```
   admin@sdwan2-panorama-2(secondary-active)> request high-availability state suspend

   Successfully changed HA state to suspended
   admin@sdwan2-panorama-2(secondary-suspended)> request high-availability state functional

   Successfully changed HA state to functional
   admin@sdwan2-panorama-2(secondary-initial)>
   admin@sdwan2-panorama-2(secondary-passive)>
   admin@sdwan2-panorama-2(secondary-passive)>
   admin@sdwan2-panorama-2(secondary-passive)>
   ```

STEP 2 | 監控設定日誌。

（管理員模式下）將 SD-WAN 外掛程式升級至 2.2.6 之前，請開始監控兩個 Panorama HA 配對上的設定日誌。

```
管理員 > tail follow yes mp-log configd.log
```

如果您在執行 **tail follow yes mp-log configd.log** 命令時看到以下錯誤訊息，則表示主動和被動 Panorama 的 Mongo 資料庫已未同步。



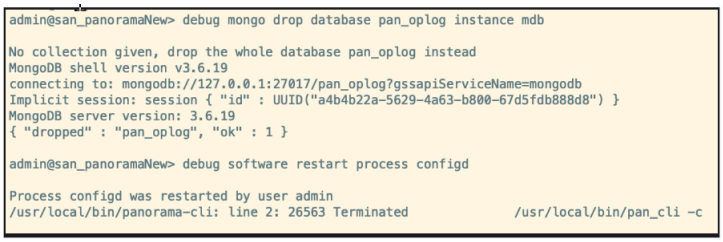
若要解決此問題：

1. （管理員模式下）將整個資料庫 *pan_oplog* 放置在主動和被動 Panorama。

   ```
   管理員 > debug mongo drop database pan_oplog instance mdb
   ```

2. （管理員模式下）在主動和被動 Panorama 重新啟動 *configd*。

   ```
   管理員 > debug software restart process configd
   ```



重新啟動 *configd* 後，請重新整理相應的網頁介面和命令列介面。重新啟動後，您就不會在任何提交程序中看到 *mongo pan_oplog* 錯誤。

建議您在整個升級過程中監控設定日誌。

STEP 3 | 在主動和被動 Panorama 下載並安裝 SD-WAN 外掛程式版本 2.2.6。

STEP 4 | （管理員模式下）將 SD-WAN 集合放置在主動和被動 Panorama。

```
管理員 > debug mongo drop database pl_sd_wan instance mdb
```

```
admin@sdwan-hw-panorama(secondary-passive)> debug mongo drop database pl_sd_wan instance mdb

No collection given, drop the whole database pl_sd_wan instead
MongoDB shell version v3.6.19
connecting to: mongodb://127.0.0.1:27017/pl_sd_wan?gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("c6dcb502-4582-4a0f-90d7-19a0becf8773") }
MongoDB server version: 3.6.19
{ "dropped" : "pl_sd_wan", "ok" : 1 }
```

您必須執行此步驟才能使 SD-WAN Mongo DB 集合保持同步。

STEP 5 | （設定模式下）從主動 Panorama 強制提交變更。

```
Number of failed attempts since last successful login: 0


admin@sdwan2_panorama(primary-active)> configure
Entering configuration mode
[edit]
admin@sdwan2_panorama(primary-active)# commit force


Commit job 5307 is in progress. Use Ctrl+C to return to command prompt
...11%.77%.80%....91%.....100%
sd_wan plugin validation: Config valid
Configuration committed successfully
Disk 'A' on log collector 0007AQA994 in group lc-group1 has a size of zero bytes

[edit]
admin@sdwan2_panorama(primary-active)#
```

完成 SD-WAN 外掛程式升級後，您必須透過 Palo Alto Networks 裝置上的 CLI 命令（在設定模式）執行 commit force。如果您執行全部提交而非 commit force，您將遺失該裝置上的所有 SD-WAN 設定。

STEP 6 | 升級 Panorama HA 之後，請確認以下內容。

1. 首先執行選擇性推送到分支裝置，然後再推送到主動 Panorama 的中樞裝置。
2. 選取 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要），然後確認裝置群組和範本是否同步處於裝置摘要頁面下的主動和被動 Panorama。
3. 確認 SD-WAN 設定（例如通道、BGP、金鑰 ID 和流量）是否符合預期。

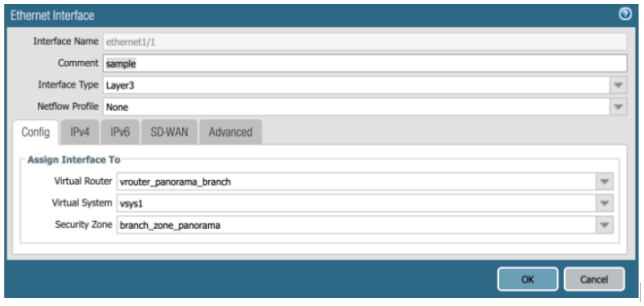
成功升級 *Panorama HA* 配對後，金鑰 *ID*、*PSK*、*IP* 快取、*IPsec* 通道快取和子網路快取將重新整理，這不會影響 *SD-WAN* 的功能。

STEP 7 | （建議）升級已連線的防火牆。

一旦 Panorama HA 配對升級成功，就可以從分支防火牆到中樞防火牆逐一升級連線的中樞和分支裝置（分支和中樞防火牆可以是獨立防火牆或 HA 配對）。

建議您在升級每個防火牆後檢查 *SD-WAN* 設定和功能。

1. 您可以修改或新增範本介面的註解，然後 **Commit**（提交）並 **Push to Devices**（推送至裝置），以在所有範本上進行細微變更。這只是一項驗證方式，以確保設定良好且升級正常運作。



2. 檢查 SD-WAN 設定和功能。
3. 逐一升級分支防火牆，直到所有分支都升級完成。
4. 請先按照以下步驟升級分支防火牆。
   1. 開始將一對分支 HA 或獨立裝置從 Panorama 版本 9.1.x 升級至 10.0.7-h3，然後升級至最新 Panorama 10.1 版本。
   2. 從執行升級的主動 Panorama 的特定防火牆範本中引入介面註解的細微變更，然後 **Commit**（提交）並 **Push to Devices**（推送至裝置）。一旦 **Commit All**（全部提交）之後，請確認 SD-WAN 的設定和功能。這只是一項驗證方式，以確保防火牆升級之後設定良好且升級正常運作。
5. 請按照以下步驟升級中樞防火牆。請務必先完成分支防火牆升級才開始升級中樞防火牆。
   1. 開始將一對中樞 HA 或獨立裝置從 Panorama 版本 9.1.x 升級至 10.0.7-h3，然後升級至最新 Panorama 10.1 版本。
   2. 從執行升級的主動 Panorama 的特定防火牆範本中引入介面註解的細微變更，然後 **Commit**（提交）並 **Push to Devices**（推送至裝置）。一旦 **Commit All**（全部提交）之後，請確認 SD-WAN 的設定和功能。

      這只是一項驗證方式，以確保防火牆升級之後設定良好且升級正常運作。
6. 選取 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要），然後確認裝置群組和範本是否同步處於裝置摘要頁面下的主動和被動 Panorama。
7. 升級完成後，請注意升級後的變更項目。

Panorama HA 配對：將 SD-WAN 外掛程式 2.1.x 升級至 2.2.6 版本

當您的 Panorama 透過 SD-WAN 外掛程式版本 2.1.x 進行安裝時，如果您想升級 SD-WAN 外掛程式版本，則必須先升級到 SD-WAN 外掛程式版本 2.2.6（而非任何中間版本）。因為 SD-WAN 2.2.6 版本包含新功能、錯誤修正、效能改進和增強功能。

建議您一律讓 Panorama 軟體版本高於 PAN-OS 版本。例如，如果您的 Panorama 版本是 10.1.9，則您的 PAN-OS 版本可以是任何比 PAN-OS 10.1.9 更舊的版本。

開始升級程序之前，請先閱讀升級 Panorama 的重要注意事項。

請以相同順序遵循以下工作流程，以 SD-WAN 2.2.6 外掛程式版本升級 Panorama HA 配對。

STEP 1 | 升級 Panorama 管理伺服器版本。

1. 在主動和被動 Panorama 下載並安裝最新 Panorama 10.1 版本。
2. 將 Panorama 升級至最新 10.1 版本後，請檢查主動 Panorama 是否保持主動狀態，而被動 Panorama 則保持被動。如果 HA 狀態沒有變更，則表示升級成功。否則您便需要執行強制切換，以維持升級前的 HA 配對狀態。

   若要執行強制切換，請以同一順序從目前的作用中 HA 對等執行下列 CLI 命令。

   ```
   管理員 > 要求高可用性狀態暫停
   ```

   ```
   管理員 > 要求高可用性狀態功能
   ```

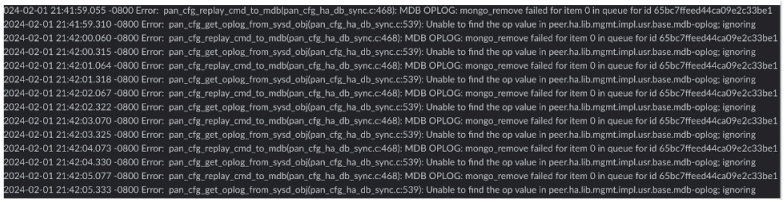
   ```
   admin@sdwan2-panorama-2(secondary-active)> request high-availability state suspend

   Successfully changed HA state to suspended
   admin@sdwan2-panorama-2(secondary-suspended)> request high-availability state functional

   Successfully changed HA state to functional
   admin@sdwan2-panorama-2(secondary-initial)>
   admin@sdwan2-panorama-2(secondary-passive)>
   admin@sdwan2-panorama-2(secondary-passive)>
   admin@sdwan2-panorama-2(secondary-passive)>
   ```


STEP 2 | 監控設定日誌。

（管理員模式下）將 SD-WAN 外掛程式升級至 2.2.6 之前，請開始監控兩個 Panorama HA 配對上的設定日誌。

```
管理員 > tail follow yes mp-log configd.log
```

如果您在執行 `admin > tail follow yes mp-log configd.log` 命令時看到以下錯誤訊息，則表示主動和被動 Panorama 的 mongo 資料庫已未同步。



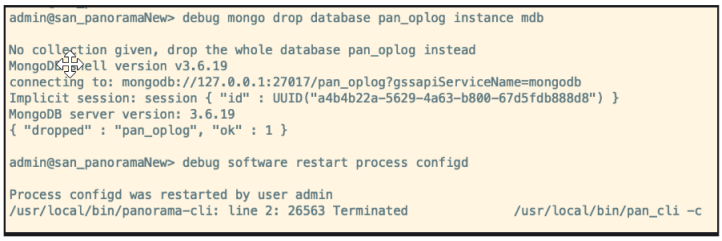
若要解決此問題：

1. （管理員模式下）將整個資料庫 *pan_oplog* 放置在主動和被動 Panorama。

   ```
   管理員 > debug mongo drop database pan_oplog instance mdb
   ```

2. （管理員模式下）在主動和被動 Panorama 重新啟動 *configd*。

   ```
   管理員 > debug software restart process configd
   ```



重新啟動 *configd* 後，請重新整理相應的網頁介面和命令列介面。重新啟動後，您就不會在任何提交程序中看到 *mongo pan_oplog* 錯誤。

建議您在整個升級過程中監控設定日誌。

STEP 3 | 在主動和被動 Panorama 下載並安裝 SD-WAN 外掛程式版本 2.2.6。

STEP 4 | （管理員模式下）將 SD-WAN 集合放置在主動和被動 Panorama。

```
管理員 > debug mongo drop database pl_sd_wan instance mdb
```

```
admin@sdwan-hw-panorama(secondary-passive)> debug mongo drop database pl_sd_wan instance mdb

No collection given, drop the whole database pl_sd_wan instead
MongoDB shell version v3.6.19
connecting to: mongodb://127.0.0.1:27017/pl_sd_wan?gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("c6dcb502-4582-4a0f-90d7-19a0becf8773") }
MongoDB server version: 3.6.19
{ "dropped" : "pl_sd_wan", "ok" : 1 }
```

您必須執行此步驟才能使 SD-WAN Mongo DB 集合保持同步。

STEP 5 | （設定模式下）從主動 Panorama 強制提交變更。

```
Number of failed attempts since last successful login: 0


admin@sdwan2_panorama(primary-active)> configure
Entering configuration mode
[edit]
admin@sdwan2_panorama(primary-active)# commit force


Commit job 5307 is in progress. Use Ctrl+C to return to command prompt
...11%.77%.80%....91%.....100%
sd_wan plugin validation: Config valid
Configuration committed successfully
Disk 'A' on log collector 0007AQA994 in group lc-group1 has a size of zero bytes

[edit]
admin@sdwan2_panorama(primary-active)#
```

完成 SD-WAN 外掛程式升級後，您必須透過 Palo Alto Networks 裝置上的 CLI 命令（在設定模式）執行 commit force。如果您執行全部提交而非 commit force，您將遺失該裝置上的所有 SD-WAN 設定。

STEP 6 | 升級 Panorama HA 之後，請確認以下內容。

1. 首先執行選擇性推送到分支裝置，然後再推送到主動 Panorama 的中樞裝置。
2. 選取 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要），然後確認裝置群組和範本是否同步處於裝置摘要頁面下的主動和被動 Panorama。
3. 確認 SD-WAN 設定（例如通道、BGP、金鑰 ID 和流量）是否符合預期。

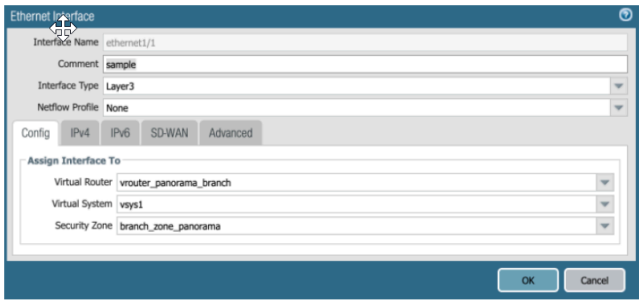
成功升級 *Panorama HA* 配對後，金鑰 *ID*、*PSK*、*IP* 快取、*IPsec* 通道快取和子網路快取將重新整理，這不會影響 *SD-WAN* 的功能。

STEP 7 | （建議）升級已連線的防火牆。

一旦 Panorama HA 配對升級成功，就可以從分支防火牆到中樞防火牆逐一升級連線的中樞和分支裝置（分支和中樞防火牆可以是獨立防火牆或 HA 配對）。

建議您在升級每個防火牆後檢查 *SD-WAN* 設定和功能。

1. 您可以修改或新增範本介面的註解，然後 **Commit**（提交）並 **Push to Devices**（推送至裝置），以在所有範本上進行細微變更。這只是一項驗證方式，以確保設定良好且升級正常運作。



2. 檢查 SD-WAN 設定和功能。
3. 逐一升級分支防火牆，直到所有分支都升級完成。
4. 請先按照以下步驟升級分支防火牆。
   1. 開始將一對分支 HA 或獨立裝置從 Panorama 版本 9.1.x 升級至 10.0.7-h3，然後升級至最新 Panorama 10.1 版本。
   2. 從執行升級的主動 Panorama 的特定防火牆範本中引入介面註解的細微變更，然後 **Commit**（提交）並 **Push to Devices**（推送至裝置）。一旦 **Commit All**（全部提交）之後，請確認 SD-WAN 的設定和功能。這只是一項驗證方式，以確保防火牆升級之後設定良好且升級正常運作。
5. 請按照以下步驟升級中樞防火牆。請務必先完成分支防火牆升級才開始升級中樞防火牆。
   1. 開始將一對中樞 HA 或獨立裝置從 Panorama 版本 9.1.x 升級至 10.0.7-h3，然後升級至最新 Panorama 10.1 版本。
   2. 從執行升級的主動 Panorama 的特定防火牆範本中引入介面註解的細微變更，然後 **Commit**（提交）並 **Push to Devices**（推送至裝置）。一旦 **Commit All**（全部提交）之後，請確認 SD-WAN 的設定和功能。

      這只是一項驗證方式，以確保防火牆升級之後設定良好且升級正常運作。
6. 選取 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要），然後確認裝置群組和範本是否同步處於裝置摘要頁面下的主動和被動 Panorama。
7. 升級完成後，請注意升級後的變更項目。

Panorama HA 配對：將 SD-WAN 外掛程式 2.2.6 升級至 3.0.7 版本

建議您一律讓 Panorama 軟體版本高於 PAN-OS 版本。例如，如果您的 Panorama 版本是 10.1.9，則您的 PAN-OS 版本可以是任何比 PAN-OS 10.1.9 更舊的版本。

開始升級程序之前，請先閱讀升級 Panorama 的重要注意事項。

STEP 1 | 下載 SD-WAN 外掛程式 3.0.7，並刪除兩個 Panorama HA 配對中下載的所有 3.0.x 外掛程式（SD-WAN 外掛程式版本 3.0.7 除外）。

STEP 2 | 將 Panorama 軟體版本從最新的 10.1 版本升級到最新的 10.2 版本。成功升級至最新的 10.2 版本後，SD-WAN 外掛程式 3.0.7 將自動安裝。

若要確認 SD-WAN 外掛程式 3.0.7 版是否已安裝在 Panorama，請檢查 Panorama **Dashboard**（儀表板）的 **General Information**（一般資訊）。

STEP 3 | 升級完成後，請檢查 SD-WAN 設定及其功能是否符合預期。

STEP 4 | 透過 Palo Alto Networks 裝置上的 CLI 命令（在組態模式）執行 commit force。如果您執行全部提交而非 commit force，您將遺失該裝置上的所有 SD-WAN 設定。

STEP 5 | （建議）從分支配對到中樞配對，逐一升級連線裝置。

STEP 6 | 裝置升級後，請檢查 SD-WAN 設定及其功能。

STEP 7 | 升級完成後，請注意升級後的變更項目。

利用 SD-WAN 外掛程式升級獨立 Panorama

這可在何處使用？	我需要什麼？
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

請先滿足先決條件再繼續進行升級。

請根據 Panorama 管理伺服器正在執行的 SD-WAN 外掛程式版本遵循升級路徑。

執行 **SD-WAN** 外掛程式版本的 **Panorama**	請遵循以下步驟
1.0.x	獨立 Panorama：將 SD-WAN 外掛程式 1.0.4 升級至 2.2.6 版本
2.1.x	獨立 Panorama：將 SD-WAN 外掛程式 2.1.x 升級至 2.2.6 版本
2.2.6	獨立 Panorama：將 SD-WAN 外掛程式 2.2.6 升級至 3.0.7 版本

獨立 Panorama：將 SD-WAN 外掛程式 1.0.4 升級至 2.2.6 版本

建議您一律讓 Panorama 軟體版本高於 PAN-OS 版本。例如，如果您的 Panorama 版本是 10.1.9，則您的 PAN-OS 版本可以是任何比 PAN-OS 10.1.9 更舊的版本。

開始升級程序之前，請先閱讀升級 Panorama 的重要注意事項。

STEP 1 | 下載並安裝 Panorama 軟體版本 10.0.7-h3。

STEP 2 | 從 Panorama 10.0.7-h3 下載並安裝最新 Panorama 10.1 版本。

STEP 3 | 在 Panorama 下載並安裝 SD-WAN 外掛程式版本 2.2.6。

STEP 4 | （設定模式下）從主動 Panorama 強制提交變更。

完成 SD-WAN 外掛程式升級後，您必須透過 Palo Alto Networks 裝置上的 CLI（設定模式）執行 commit force。如果您執行全部提交而非 commit force，您將遺失該裝置上的所有 SD-WAN 設定。

```
Number of failed attempts since last successful login: 0


admin@sdwan2_panorama(primary-active)> configure
Entering configuration mode
[edit]
admin@sdwan2_panorama(primary-active)# commit force


Commit job 5307 is in progress. Use Ctrl+C to return to command prompt
...11%.77%.80%....91%.....100%
sd_wan plugin validation: Config valid
Configuration committed successfully
Disk 'A' on log collector 0007AQA994 in group lc-group1 has a size of zero bytes

[edit]
admin@sdwan2_panorama(primary-active)#
```

STEP 5 | 升級獨立 Panorama 後請確認以下內容。

1. 從 Panorama 推送到裝置。
2. 選取 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要），然後確認裝置群組和範本是否同步處於裝置摘要頁面下的主動和被動 Panorama。

3. 確認 SD-WAN 設定（例如通道、BGP、金鑰 ID 和流量）是否符合預期。

成功升級 *Panorama HA* 配對後，金鑰 *ID*、*PSK*、*IP* 快取、*IPsec* 通道快取和子網路快取將重新整理，這不會影響 *SD-WAN* 的功能。

STEP 6 | 一旦 Panorama 升級成功，如有需要，所有連線裝置都可以從分支配對/獨立裝置到中樞配對/獨立裝置開始逐一升級。建議您在每個升級後檢查 SD-WAN 設定和功能。

STEP 7 | 升級完成後，請注意升級後的變更項目。

獨立 Panorama：將 SD-WAN 外掛程式 2.1.x 升級至 2.2.6 版本

建議您一律讓 Panorama 軟體版本高於 PAN-OS 版本。例如，如果您的 Panorama 版本是 10.1.9，則您的 PAN-OS 版本可以是任何比 PAN-OS 10.1.9 更舊的版本。

開始升級程序之前，請先閱讀升級 Panorama 的重要注意事項。

STEP 1 | 下載並安裝最新 Panorama 10.1 版本。

STEP 2 | 在 Panorama 下載並安裝 SD-WAN 外掛程式版本 2.2.6。

STEP 3 | （設定模式下）從主動 Panorama 強制提交變更。

完成 SD-WAN 外掛程式升級後，您必須透過 Palo Alto Networks 裝置上的 CLI（設定模式）執行 commit force。如果您執行全部提交而非 commit force，您將遺失該裝置上的所有 SD-WAN 設定。

```
Number of failed attempts since last successful login: 0


admin@sdwan2_panorama(primary-active)> configure
Entering configuration mode
[edit]
admin@sdwan2_panorama(primary-active)# commit force


Commit job 5307 is in progress. Use Ctrl+C to return to command prompt
...11%.77%.80%....91%.....100%
sd_wan plugin validation: Config valid
Configuration committed successfully
Disk 'A' on log collector 0007AQA994 in group lc-group1 has a size of zero bytes

[edit]
admin@sdwan2_panorama(primary-active)#
```

STEP 4 | 升級獨立 Panorama 後請確認以下內容。

1. 從 Panorama 推送到裝置。
2. 選取 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要），然後確認裝置群組和範本是否同步處於裝置摘要頁面下的主動和被動 Panorama。

3. 確認 SD-WAN 設定（例如通道、BGP、金鑰 ID 和流量）是否符合預期。

成功升級 *Panorama HA* 配對後，金鑰 *ID*、*PSK*、*IP* 快取、*IPsec* 通道快取和子網路快取將重新整理，這不會影響 *SD-WAN* 的功能。

STEP 5 | 一旦 Panorama 升級成功，如有需要，所有連線裝置都可以從分支配對/獨立裝置到中樞配對/獨立裝置開始逐一升級。建議您在每個升級後檢查 SD-WAN 設定和功能。

STEP 6 | 升級完成後，請注意升級後的變更項目。

獨立 Panorama：將 SD-WAN 外掛程式 2.2.6 升級至 3.0.7 版本

建議您一律讓 Panorama 軟體版本高於 PAN-OS 版本。例如，如果您的 Panorama 版本是 10.1.9，則您的 PAN-OS 版本可以是任何比 PAN-OS 10.1.9 更舊的版本。

開始升級程序之前，請先閱讀升級 Panorama 的重要注意事項。

STEP 1 | 下載並安裝最新 Panorama 10.1 版本。

STEP 2 | 在 Panorama 下載並安裝 SD-WAN 外掛程式版本 2.2.6。

STEP 3 | （設定模式下）從主動 Panorama 強制提交變更。

完成 SD-WAN 外掛程式升級後，您必須透過 Palo Alto Networks 裝置上的 CLI（設定模式）執行 commit force。如果您執行全部提交而非 commit force，您將遺失該裝置上的所有 SD-WAN 設定。

```
Number of failed attempts since last successful login: 0


admin@sdwan2_panorama(primary-active)> configure
Entering configuration mode
[edit]
admin@sdwan2_panorama(primary-active)# commit force


Commit job 5307 is in progress. Use Ctrl+C to return to command prompt
...11%.77%.80%....91%.....100%
sd_wan plugin validation: Config valid
Configuration committed successfully
Disk 'A' on log collector 0007AQA994 in group lc-group1 has a size of zero bytes

[edit]
admin@sdwan2_panorama(primary-active)#
```

STEP 4 | 升級獨立 Panorama 後請確認以下內容。

1. 從 Panorama 推送到裝置。
2. 選取 **Panorama** > **Managed Devices**（受管理的裝置） > **Summary**（摘要），然後確認裝置群組和範本是否同步處於裝置摘要頁面下的主動和被動 Panorama。

3. 確認 SD-WAN 設定（例如通道、BGP、金鑰 ID 和流量）是否符合預期。

成功升級 *Panorama HA* 配對後，金鑰 *ID*、*PSK*、*IP* 快取、*IPsec* 通道快取和子網路快取將重新整理，這不會影響 *SD-WAN* 的功能。

STEP 5 | 一旦 Panorama 升級成功，如有需要，所有連線裝置都可以從分支配對/獨立裝置到中樞配對/獨立裝置開始逐一升級。建議您在每個升級後檢查 SD-WAN 設定和功能。

STEP 6 | 升級完成後，請注意升級後的變更項目。

升級後變更事項

這可在何處使用？	我需要什麼？
• PAN-OS • SD-WAN	❑ SD-WAN plugin license

升級後，您必須先進行下列檢查，然後再將變更提交至 *Panorama*：

- 確認 *VPN* 叢集中每個 *SD-WAN* 裝置皆已設定 ***Router Name***（路由名稱）（***Panorama*** > ***SD-WAN*** > ***Devices***（裝置））。*SD-WAN* 外掛程式 *3.1.0* 及更新版本支援 ***Router Name***（路由名稱）設定。
- 確認 *VPN* 叢集中每個 *SD-WAN* 裝置皆已啟用個 ***BGP***（***Panorama*** > ***SD-WAN*** > ***Devices***（裝置））。確定已啟用升級前設定的相同 *BGP* 位址系列（***IPv4 BGP*** 或 ***IPv6 BGP***）。*SD-WAN* 外掛程式 *3.1.1* 及更新版本支援 *IPv6*。因此，只有當您從 *SD-WAN 3.1.1* 或更新版本升級時，升級的外掛程式才會包含 *IPv6* 選項。
- 確認是否已啟用升級前設定的相同 *VPN* 驗證類型（***Pre Shared Key***（預先共用金鑰）或 ***Certificate***（憑證））（***Panorama*** > ***SD-WAN*** > ***Devices***（裝置）> ***VPN Tunnel***（***VPN*** 通道））。*SD-WAN* 外掛程式 *3.2.0* 及更新版本支援 ***Certificate***（憑證）驗證類型。因此，只有當您從 *SD-WAN* 外掛程式 *3.2.0* 或更新版本升級時，升級的外掛程式才會包含 *VPN* 驗證類型（***Pre Shared Key***（預先共用金鑰）或 ***Certificate***（憑證））。

升級後（在 Panorama HA 配對或獨立 Panorama），您可以看到以下變更：

- 您不會在 **Panorama** > **SD-WAN** > **Devices**（裝置）中看到新增的 SD-WAN 裝置的區域頁籤。因此，您必須在現有和預先定義的區域（zone-to-branch、zone-to-hub、zone-internet 和 zone-internal）之間建立安全性政策規則。
- 在完整網狀 VPN 叢集中，序列號較低的分支將作為 IKE 起始者。如果是上游 NAT，NAT 裝置上應該存在輸入和輸出 NAT，如果輸入 NAT 不存在，您將看到 PLUG-15276。

涵蓋 SD-WAN 資料庫收集的 MongoDB 同步狀態

在部分 SD-WAN 外掛程式版本中，MongoDB 中的 SD-WAN 資料庫收集可能沒有進行同步，這是一個已知問題。因此，從任何舊版本升級到 SD-WAN 外掛程式 2.2.6 時，您可能需要在升級程序中執行其他步驟。

下表說明 SD-WAN MongoDB 收集是否與 SD-WAN 外掛程式版本（已經測試）同步。

S.No	相容的 PAN-OS 軟體版本與 SD-WAN 外掛程式版本	SD-WAN 外掛程式版本	Mongo 連接埠	在 Panorama HA 上 Mongo 的 SD-WAN 集合
1	10.1.6	2.1.2	31377	未同步
2	10.1.x	2.1.2	31377	未同步
3	10.1.x	2.2.6	27017	已同步
4	10.2.7-h3	3.0.7	27017	已同步

用於升級的 CLI 命令

- 使用 CLI 命令進行升級工作

使用 CLI 命令進行升級工作

使用下列 CLI 命令來執行升級工作。

如果您想要...	使用...
檢查目前的防火牆版本	
• 檢查防火牆軟體和內容的當前版本。	`show system info`
存取可用的動態更新並升級防火牆的內容版本	
• 直接從 Palo Alto Networks 伺服器檢查動態更新的可用內容版本。	`request content upgrade check`
• 直接從防火牆檢查動態更新的可用內容版本。	`request content upgrade info`
• 將內容版本直接下載到防火牆。	`request content upgrade download <content version>`
• 安裝內容版本。	`request content upgrade install <content version>`

如果您想要...	使用...
存取可用的軟體版本並升級防火牆	
• 檢查可供下載的可用軟體版本。	`request system software info`
• 檢查軟體的慣用版本。 （PAN-OS 11.1.3 和更新版本）	要求慣用系統軟體資訊
• 檢查軟體的基本版本。 （PAN-OS 11.1.3 和更新版本）	要求系統軟體資訊基礎
• 檢查軟體的慣用版本和基礎版本。 （PAN-OS 11.1.3 和更新版本）	要求慣用基礎系統軟體資訊
• 安裝下載的軟體。	`request system software install version 10.1.0`
• 重新啟動防火牆。	`request restart system`

如果您想要...	使用...

存取防火牆的可用軟體修補程式：

修補程式功能目前以預覽模式提供。不提供此功能的完全支援。

如果您想要...	使用...
• 檢查可供下載的可用軟體修補程式。	`request system patch check`
• 檢查目前安裝的防火牆版本的可用修補程式。	`request system patch info`
• 下載特定的修補程式版本。	`request system patch download version <version>`
• 查看特定修補程式版本的更多詳細資訊。	`request system patch info version <version>`
• 安裝已下載的修補程式。	`request system patch install version <version>`

如果您想要...	使用...
• 套用已安裝的修補程式。	`request system patch apply`

用於升級的 API

- 使用 API 進行升級工作

使用 API 進行升級工作

使用下列 CLI 命令來執行升級工作。

如果您想要...	使用...
檢查目前的防火牆版本	
• 檢查防火牆軟體和內容的當前版本。	**https://firewall/api/?type=op&cmd=<request><system><software><chec check></software></system>**
存取可用的動態更新並升級防火牆的內容版本	
• 直接從 Palo Alto Networks 伺服器檢查動態更新的可用內容版本。	**https://firewall/api/?type=op&cmd=<request><content><upgrade><chec check></upgrade></content></request>**
• 直接從防火牆檢查動態更新的可用內容版本。	**https://firewall/api/?type=op&cmd=<request><content><upgrade><info info></upgrade></content></request>**
• 將最新內容版本直接下載到防火牆。	**https://firewall/api/?type=op&cmd=<request><content><upgrade><down latest></download></upgrade></content></request>**
• 將特定內容版本直接下載到防火牆。	**https://firewall/api/?type=op&cmd=<request><content><upgrade><down specific file name here<file></download></upgrade></content></request>**
• 安裝內容版本。	**https://firewall/api/?type=op&cmd=<request><content><upgrade><inst <content version></version></install></upgrade></content></request>**
存取可用的軟體版本並升級防火牆	
• 檢查可供下載的可用軟體版本。	**https://firewall/api/?type=op&cmd=<request><system><software><info**

如果您想要...	使用...
	info></software></system></request>
• 檢查防火牆上載入的可用版本。	**https://firewall/api/?type=op&cmd=<request><system><software><chec check></software></system></request>**
• 下載特定的軟體版本。	**https://firewall/api/?type=op&cmd=request><system><software><downl version></download></software></system></request>**
• 檢查特定下載作業的狀態。	**https://firewall/api/?type=op&cmd=<show><jobs></jobs></show>**
• 安裝下載的軟體。	**https://firewall/api/?type=op&cmd=<request><system><software><inst version></install></software></system></request>**
• 重新啟動防火牆。	**https://firewall/api/?type=op&cmd=<request><restart><system></system></restart></request>**

