paloalto TECHDOCS

AI Access Security 啟動和裝載

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

April 17, 2026

Table of Contents

AI Access Security 授權

檢閱可用的 AI Access Security 授權以開始在您的網路上對生成式 AI (GenAI) 應用程式進行安全採用並控制存取。

- **AI Access Security** 授權

  AI Access Security 授權是獨立授權。其中包含下列三種類型的授權:

  - **AI Access Security EVAL**—AI Access Security 的評估授權。如果您已啟動 EVAL 授權,則必須在評估期間結束後將評估授權轉換為生產授權,才能繼續安全控制存取並採用 GenAI 應用程式。
  - **AI Access Security LAB**—實驗室環境特定的 AI Access Security 授權。此授權不適用於生產環境。
  - **AI Access Security**—AI Access Security 的生產授權。
- **CASB-PA** 和 **CASB-X**

  CASB-PA 和 CASB-X 授權預設包含 AI Access Security。不需要其他動作即可啟動 AI Access Security。啟動其中一個授權後,您可以開始使用 AI Access Security 以安全採用 GenAI 應用程式。
- **Prisma Access Browser** 獨立授權

  Prisma Access Browser 獨立授權預設包含 AI Access Security。不需要其他動作即可啟動 AI Access Security。啟動此授權後,您可以開始使用 AI Access Security 以安全採用 GenAI 應用程式。

AI Access Security 授權包含哪些內容？

AI Access Security 包含的內容取決於租用戶上是否已啟動其他授權。

包含的 AI Access Security 功能取決於目前在 NGFW 或 Prisma Access 租用戶上執行的 PAN-OS 或資料平面版本。如需包含功能的詳細資訊,請參閱設定先決條件。

- 僅限 **AI Access Security**

  當僅有 AI Access Security 授權作用中時,這適用於由 Panorama 或 Strata Cloud Manager 管理的 NGFW 或 Prisma Access。

PAN-OS 或資料平面版本	NGFW 和 Prisma Access (由 Panorama 或 Strata Cloud Manager 管理)
11.2.2-h1 與更新版本 Prisma Access 5.1 Innovation 和更新版本	• 透過動態內容更新和 App-ID 雲端引擎 (ACE) 傳遞的超過 2,250 個 GenAI 應用程式可視性。 • 定義政策規則以控制對 GenAI 應用程式和非 GenAI 應用程式的存取。 • Enterprise DLP 檢查和裁定呈現僅適用於支援的 GenAI 應用程式。 針對非 GenAI 應用程式，包含敏感資料的流量相符項目不會轉送到 Enterprise DLP 進行檢查和裁定呈現。 • 存取 Strata Cloud Manager Command Center 以取得 GenAI 可視性。 • 存取 AI Access Security 活動洞察儀表板以檢視詳細 GenAI 應用程式使用資料、使用者和在您網路上常見的 GenAI 使用案例。 • 在 Strata Cloud Manager 上，標記 GenAI 應用程式,以反映應用程式是否已獲得您組織的核准,並適用於基於標籤的政策強制執行。 AI Access Security 不會將 GenAI 應用程式標籤同步到 Panorama。 • 僅針對已發現的 GenAI 應用程式產生報告。 • 在應用程式字典中檢視 GenAI 應用程式,進一步瞭解這些 SaaS 應用程式涉及的特定 GenAI 應用程式、廠商、合規性和風險特性。 • 在 7 個 SaaS Marketplace 應用程式中，檢視作為第三方連線應用程式/外掛程式安裝的 GenAI 應用程式。 • ChatGPT 企業應用程式中靜態資料的可視性和控制。

- **AI Access Security** 和 **Enterprise DLP** 授權

  當 AI Access Security 和 Enterprise DLP 授權同時作用中時,這適用於由 Panorama 或 Strata Cloud Manager 管理的 NGFW 或 Prisma Access。

PAN-OS 或資料平面版本	NGFW 和 Prisma Access (由 Panorama 或 Strata Cloud Manager 管理)
11.2.2-h1 與更新版本 Prisma Access 5.1 Innovation 和更新版本	• 透過動態內容更新和 App-ID 雲端引擎 (ACE) 傳遞的超過 2,250 個 GenAI 應用程式可視性。 • 定義政策規則以控制對 GenAI 應用程式和非 GenAI 應用程式的存取。 • Enterprise DLP 檢查和裁定呈現適用於支援的 GenAI 和非 GenAI 應用程式。 • 存取 Strata Cloud Manager Command Center 以取得 GenAI 可視性。 • 存取 AI Access Security 活動洞察儀表板以檢視詳細 GenAI 應用程式使用資料、使用者和在您網路上常見的 GenAI 使用案例。 • 在 Strata Cloud Manager 上，標記 GenAI 應用程式,以反映應用程式是否已獲得您組織的核准,並適用於基於標籤的政策強制執行。 AI Access Security 不會將 GenAI 應用程式標籤同步到 Panorama。 • 僅針對已發現的 GenAI 應用程式產生報告。 • 在應用程式字典中檢視 GenAI 應用程式,進一步瞭解這些 SaaS 應用程式涉及的特定 GenAI 應用程式、廠商、合規性和風險特性。 • 在 7 個 SaaS Marketplace 應用程式中，檢視作為第三方連線應用程式/外掛程式安裝的 GenAI 應用程式。 • ChatGPT 企業應用程式中靜態資料的可視性和控制。

- **CASB-PA** 和 **CASB-X** 授權

  當 CASB-PA 或 CASB-X 授權作用中時,這適用於由 Strata Cloud Manager 管理的 NGFW 或 Prisma Access。

PAN-OS 或資料平面版本	CASB-PA 和 CASB-X
10.2 11.1 Prisma Access 5.0 Preferred 和 Innovation 及更新版本	• 透過動態內容更新和 App-ID 雲端引擎 (ACE) 傳遞的超過 2,250 個 GenAI 應用程式可視性。 • 定義政策規則以控制對 GenAI 應用程式和非 GenAI 應用程式的存取。 • Enterprise DLP 檢查和裁定呈現適用於支援的 GenAI 和非 GenAI 應用程式。 • 存取 Strata Cloud Manager Command Center 以取得 GenAI 可視性。 • 存取 AI Access Security 活動洞察儀表板以檢視詳細 GenAI 應用程式使用資料、使用者和在您網路上常見的 GenAI 使用案例。

PAN-OS 或資料平面版本	CASB-PA 和 CASB-X

Prisma Access 5.1 Preferred 和更新版本	• 檢視下列包含 GenAI 應用程式的所有 SaaS 內嵌應用程式：
	  • 儀表板
	  • 使用者
	  • 應用程式字典
	  • 應用程式
	  • 報告
	  • 政策建議
	• 檢視包含 GenAI 外掛程式的所有 第三方外掛程式 (SSPM)。
	• 檢視包含 GenAI 應用程式的所有已認可 SaaS 應用程式 (靜態資料) 資產詳細資料。

11.2.2-h1 與更新版本
 	
Prisma Access 5.1 Innovation 和更新版本
	• 透過動態內容更新和 App-ID 雲端引擎 (ACE) 傳遞的超過 2,250 個 GenAI 應用程式可視性。
	• 定義政策規則以控制對 GenAI 應用程式和非 GenAI 應用程式的存取。
	• Enterprise DLP 檢查和裁定呈現適用於支援的 GenAI 和非 GenAI 應用程式。
	• 存取 Strata Cloud Manager Command Center 以取得 GenAI 可視性。
	• 存取 AI Access Security 活動洞察儀表板以檢視詳細 GenAI 應用程式使用資料、使用者和在您網路上常見的 GenAI 使用案例。
	• 在 Strata Cloud Manager 上，標記 GenAI 應用程式,以反映應用程式是否已獲得您組織的核准,並適用於基於標籤的政策強制執行。
	  AI Access Security 不會將 GenAI 應用程式標籤同步到 Panorama。
	• 檢視下列包含 GenAI 應用程式的所有 SaaS 內嵌應用程式：
	  • 儀表板
	  • 使用者
	  • 應用程式字典
	  • 應用程式
	  • 報告
	  • 政策建議
	• 檢視包含 GenAI 外掛程式的所有 第三方外掛程式 (SSPM)。
	• 檢視包含 GenAI 應用程式的所有已認可 SaaS 應用程式 (靜態資料) 資產詳細資料。

AI Access Security 設定先決條件

檢閱使用 AI Access Security 的先決條件。先決條件描述使用 AI Access Security 所需的最低 PAN-OS 和 Prisma Access 資料平面版本及任何其他服務。

檢閱不同的 AI Access Security 授權和 PAN-OS 版本組合，深入瞭解 AI Access Security 支援的功能。

- **NGFW** 和 **Prisma Access (**由 **Panorama** 管理**)**

  當從 Panorama 管理您的 AI Access Security 設定並僅啟動 AI Access Security 授權時，請參閱 **AI Access Security** 授權先決條件。

  當從 Panorama 管理您的 AI Access Security 設定並擁有作用中 CASB-PA 或 CASB-X 授權時，請參閱 **CASB-PA** 和 **CASB-X** 授權先決條件。

先決條件	**AI Access Security** 授權	**CASB-PA** 和 **CASB-X** 授權
PAN-OS 或資料平面	PAN-OS 11.2.2-h1	• PAN-OS 10.2.3 和 Prisma Access 5.0 Preferred 與 Innovation • PAN-OS 11.1.0 和 Prisma Access 5.1 Preferred • PAN-OS 11.2.2-h1 和 Prisma Access 5.1 Innovation 如需最低所需 Prisma Access 版本的詳細資訊，請參閱 Prisma Access 版本資訊。
資料篩選	Enterprise DLP 外掛程式 5.0.4 或更新版本	如需有關 PAN-OS 版本上支援的 Enterprise DLP 外掛程式版本，請參閱相容性矩陣。
	AI Access Security 會在您啟動 AI Access Security、CASB-PA 和 CASB-X 授權 時包含 Enterprise DLP。	
管理	Strata Cloud Manager Essentials或Strata Cloud Manager Pro 進一步瞭解每個授權包含的內容。	無
雲端服務外掛程式	雲端服務外掛程式 5.1	

先決條件	AI Access Security 授權	CASB-PA 和 CASB-X 授權
記錄	Strata Logging Service	

- **NGFW** 和 **Prisma Access (**由 **Strata Cloud Manager** 管理**)**

  當從 Strata Cloud Manager 管理您的 AI Access Security 設定並僅啟動 AI Access Security 授權時，請參閱 **AI Access Security** 授權先決條件。

  當從 Strata Cloud Manager 管理您的 AI Access Security 設定並有已啟動的 CASB-PA 或 CASB-X 授權時，請參閱 **CASB-PA** 和 **CASB-X** 授權先決條件。

先決條件	AI Access Security 授權	CASB-PA 和 CASB-X 授權
PAN-OS 或資料平面	PAN-OS 11.2.2-h1	• PAN-OS 10.2.3 和 Prisma Access 5.0 Preferred 與 Innovation • PAN-OS 11.1.0 和 Prisma Access 5.1 Preferred • PAN-OS 11.2.2-h1 和 Prisma Access 5.1 Innovation 如需最低所需 Prisma Access 版本的詳細資訊，請參閱 Prisma Access 版本資訊。
資料篩選	AI Access Security 會在您啟動 AI Access Security、CASB-PA 和 CASB-X 授權 時包含 Enterprise DLP。	
管理	Strata Cloud Manager Essentials或Strata Cloud Manager Pro 進一步瞭解每個授權包含的內容。	無
記錄	Strata Logging Service	

啟動 AI Access Security 授權

啟動您的 AI Access Security 授權 以使您的組織能夠安全讓員工採用生成式 AI (GenAI) 應用程式。AI Access Security 啟動是使用由 Palo Alto Networks 在購買 AI Access Security 授權後提供的連結來執行。這些程序假設您已具備所有必要的授權驗證碼和啟動所需的連結。

在您購買 AI Access Security 授權後，您必須使用由 Palo Alto Networks 傳送給您的連結啟動該授權。當您啟動 CASB-PA 或 CASB-X 授權時，AI Access Security 會包含在內。在您啟動 CASB-PA 或 CASB-X 授權後，不需要進一步的動作即可啟動 AI Access Security。

- 新部署
- 現有部署

啟動 AI Access Security 授權 (新部署)

STEP 1 | 安裝並執行 NGFW 的初始設定。

這包含啟動所有必要支援授權。

STEP 2 | 為您的 NGFW 或 Prisma Access 租用戶設定管理。

- **NGFW (Managed by Panorama)**
  1. 設定 Panorama。
     - **M-Series** 設備—在 僅管理或 Panorama 模式下設定 M-Series 設備。
     - **Panorama**虛擬設備—在僅管理或 Panorama 模式下，於您慣用的超管理器中安裝 Panorama 虛擬設備
  2. 部署 Strata Logging Service。
  3. 註冊 Panorama。
  4. 啟動 Panorama 支援授權。
  5. 啟動 Panorama 裝置管理授權 (M-Series 設備或 Panorama 虛擬設備)。
  6. 將您的受管理防火牆新增到 Panorama 管理。
  7. 將 Panorama 升級至 AI Access Security 支援的最低 PAN-OS 版本。
  8. 將您的 NGFW 升級至 AI Access Security 支援的最低 PAN-OS 版本。
- **NGFW (Managed by Strata Cloud Manager)**
  1. 部署 Strata Logging Service。

     Strata Cloud Manager 需要 Strata Logging Service，才能進行記錄。
  2. 啟動 Strata Cloud Manager Essentials 或 Strata Cloud Manager Pro 授權。
  3. 將您的 NGFW 裝載至 Strata Cloud Manager。
  4. 安裝最新的動態內容更新，並將您的 NGFW 升級至 AI Access Security 支援的最低 PAN-OS 版本。
- **Prisma Access (Managed by Panorama)**
  1. 設定 Panorama。
     - **M-Series** 設備—在 僅管理或 Panorama 模式下設定 M-Series 設備。
     - **Panorama**虛擬設備—在僅管理或 Panorama 模式下，於您慣用的超管理器中安裝 Panorama 虛擬設備
  2. 部署 Strata Logging Service。
  3. 註冊 Panorama。
  4. 啟動 Panorama 支援授權。
  5. 啟動 Panorama 裝置管理授權 (M-Series 設備或 Panorama 虛擬設備)。
  6. 將 Panorama 升級至 AI Access Security 支援的最低 PAN-OS 版本。
  7. 在 Panorama 上，安裝雲端服務外掛程式。
  8. 設定 Panorama Managed Prisma Access。
- **Prisma Access (Managed by Strata Cloud Manager)**
  1. 部署 Strata Logging Service。

     Strata Cloud Manager 需要 Strata Logging Service，才能進行記錄。
  2. 在 Strata Cloud Manager 上，啟動 Prisma Access 授權。

3. 設定 Prisma Access。

STEP 3 | 設定 Enterprise Data Loss Prevention (E-DLP)。

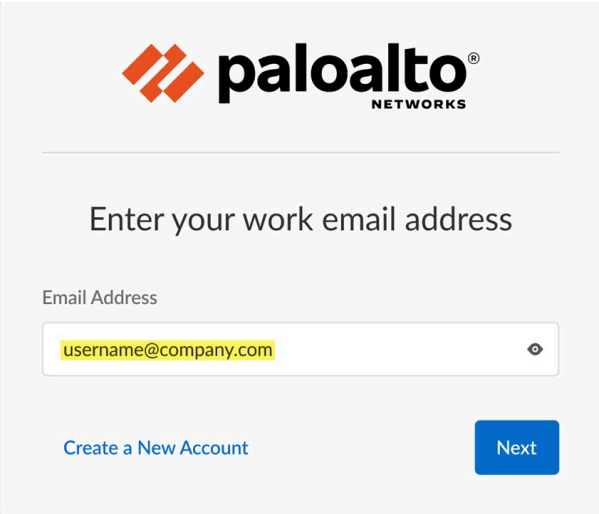
- **NGFW (Managed by Panorama)**
  1. 在 Panorama 上，安裝 Enterprise DLP 外掛程式。
  2. 啟用 NGFW 的 Enterprise DLP。
  3. 視需要編輯 Enterprise DLP 雲端內容、資料篩選，以及片段設定。
- **NGFW (Managed by Strata Cloud Manager)**
  1. 啟用 NGFW 的 Enterprise DLP。
  2. 視需要編輯 Enterprise DLP 資料篩選和片段設定。
- **Prisma Access (Managed by Panorama)**
  1. 在 Panorama 上，安裝 Enterprise DLP 外掛程式。
  2. 啟用 Prisma Access 的 Enterprise DLP。
  3. 視需要編輯 Enterprise DLP 雲端內容、資料篩選，以及片段設定。
- **Prisma Access (Managed by Strata Cloud Manager)**
  1. 啟用 NGFW 的 Enterprise DLP。
  2. 視需要編輯 Enterprise DLP 資料篩選和片段設定。

STEP 4 | 在購買 AI Access Security 訂閱時，請按一下由 Palo Alto Networks 提供的連結。

STEP 5 | 按一下 **Activate Subscription**（啟動訂閱）以開始啟動 AI Access Security。

STEP 6 | 輸入您的 Palo Alto Networks 客戶支援入口網站 (CSP) **Email Address**（電子郵件地址）。此電子郵件地址必須與收到連結的電子郵件相符，才能啟動 AI Access Security。

如果收到 AI Access Security 啟動鏈接的電子郵件地址尚未有有效的 CSP 帳戶，請 **Create a New Account**（建立新帳戶）。新建立的帳戶會自動與您正在啟動 AI Access Security 的相同租用戶相關聯，並獲指派多租用戶超級使用者角色。



STEP 7 | (僅限多租用戶) 在 **Customer Support Account**（客戶支援帳戶）區段中，選擇與您正在啟動 AI Access Security 授權的租用戶相關聯的 Palo Alto Networks 客戶支援帳戶。

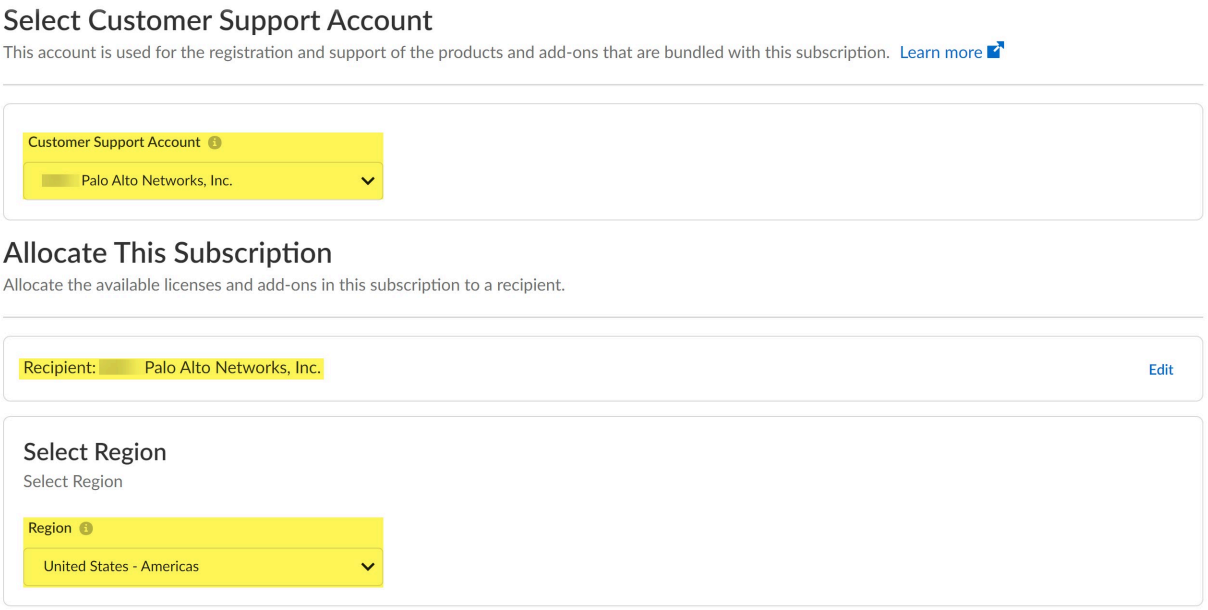
如果您擁有單一租用戶客戶支援入口網站帳戶，請跳過此步驟。依預設，已選取您的客戶支援帳戶。

STEP 8 | (僅限多租用戶) 在 **Allocate This Subscription**（配置此訂閱）區段中，選擇您要啟動 AI Access Security 的租用戶服務群組 (TSG)。您可以選擇父租用戶或子租用戶。

AI Access Security 僅針對所選租用戶啟動。如果您選擇父租用戶，則 AI Access Security 不會針對任何子租用戶啟動。

如果您僅擁有單一租用戶客戶支援入口網站帳戶，請跳過此步驟。依預設，已選取該帳戶。

STEP 9 | 檢閱租用戶 **Region**（地區）。此地區根據已部署的NGFW或Prisma Access 租用戶地區預先填入，且無法變更。

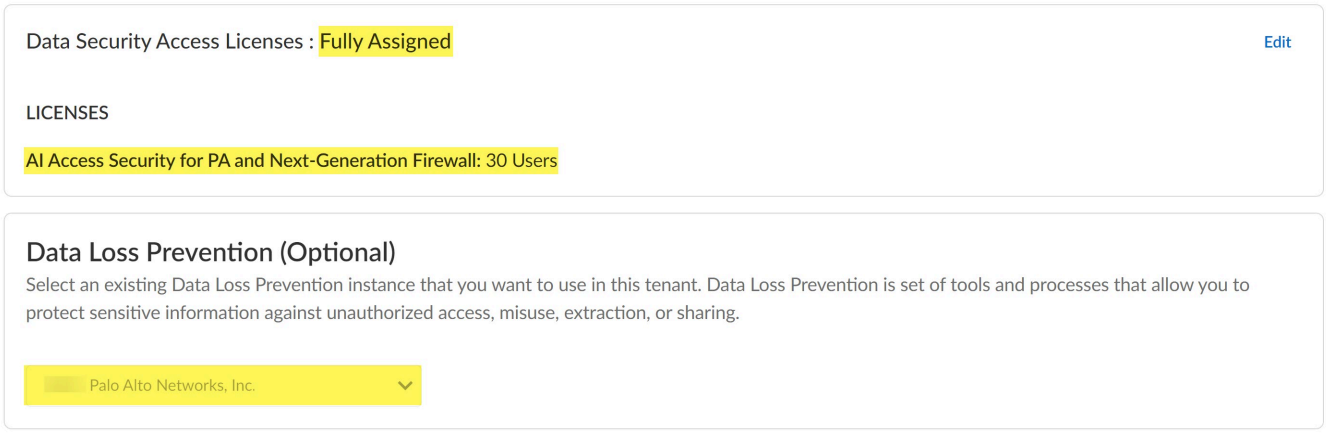


STEP 10 | 在**Assign Licenses**（指派授權）區段中，按一下 **Done**（完成）以指派您所有的 AI Access Security 授權。驗證您的 **AI Access Security License**（**AI** 存取安全性授權）為 `Fully Assigned`。

STEP 11 | 如果您在租用戶上已啟動 Enterprise Data Loss Prevention (E-DLP)，請驗證已選擇您的 **Data Loss Prevention**（資料遺失防護）執行個體。

如果在租用戶上已啟動，則預設會選擇您的 Enterprise DLP 執行個體。

如果您尚未啟動 Enterprise DLP，請跳過此步驟。啟用 AI Access Security 不需要 Enterprise DLP。如果尚未啟動 Enterprise DLP 執行個體，則在授權啟動時會建立一個執行個體。檢閱在您未更新您的 AI Access Security 授權時，Enterprise DLP 將會有何影響。

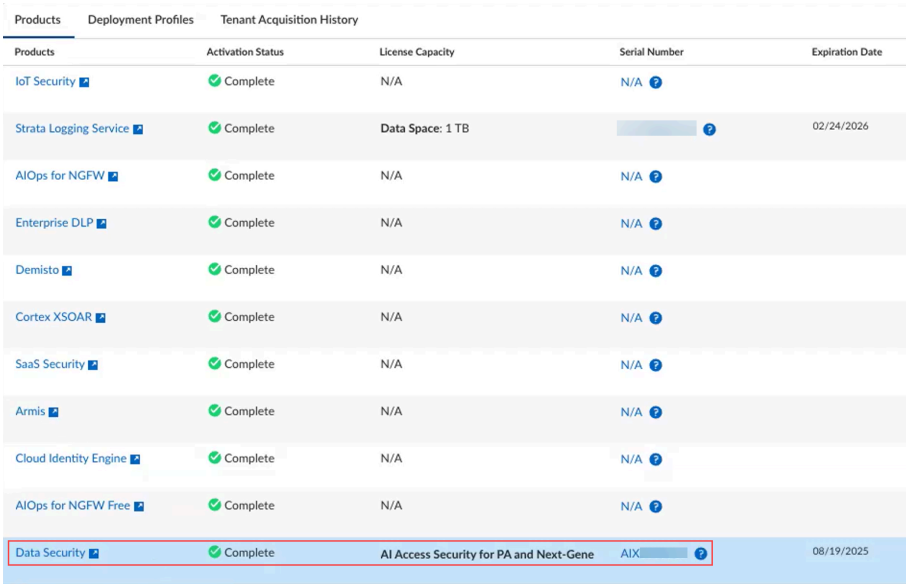


STEP 12 | **Agree to the terms and conditions**（同意條款和條件）。

STEP 13 | **Activate**（啟動）。

系統會將您重新導向至 Tenant Management（租用戶管理）頁面，其中AI Access Security **Activation Status**（啟動狀態）開始初始化。

AI Access Security 授權會顯示為**Data Security**（資料安全性），其序號以 AIX 開頭。在 **Activation Status**（啟動狀態）為 Complete 後，繼續下一步。



STEP 14 | (僅限 NGFW) 將 AI Access Security 授權與您的 NGFW 相關聯。

必須關聯 AI Access Security 授權，才能啟動您的 NGFW 授權。

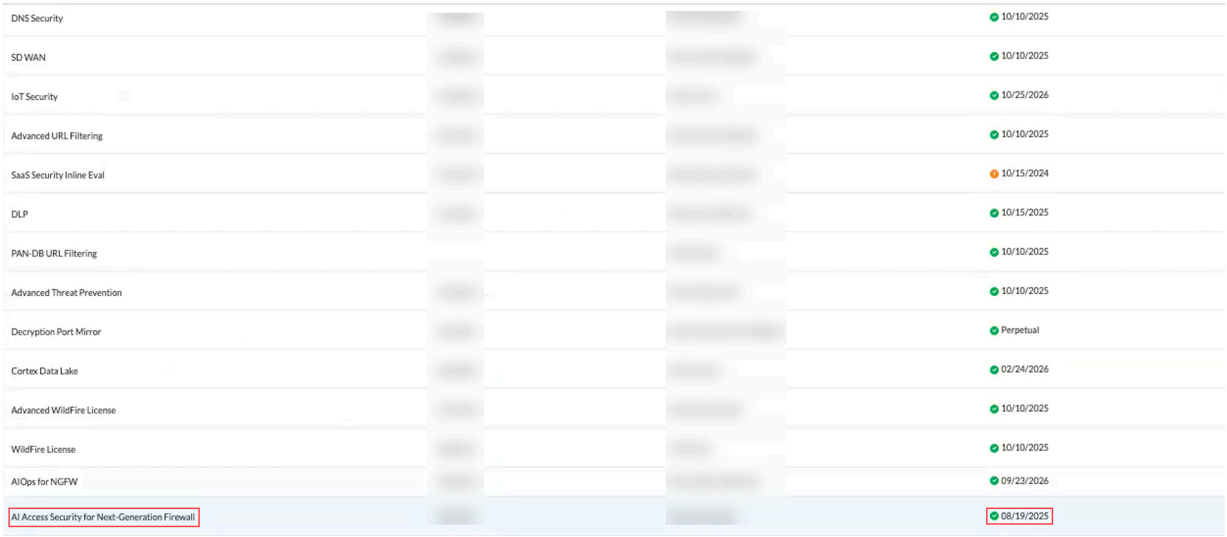
1. 在 Strata Cloud Manager 功能表中，選擇 **Settings**（設定） > **Device Associations**（裝置關聯）。

   Strata Cloud Manager 功能表位於 Strata Cloud Manager 的左下角。
2. 在 Strata Cloud Manager 功能表中，選擇 **System Settings**（系統設定） > **Device Associations**（裝置關聯）。

   Strata Cloud Manager 功能表位於 Strata Cloud Manager 的左下角。
3. **Associate Apps**（關聯應用程式）。
4. 在已授權的產品中，選擇 **Data Security**（資料安全性）。
5. 選擇您要啟動 AI Access Security 的 NGFW。
6. **Save**（儲存）。

STEP 15 | 驗證您已成功啟用 AI Access Security。

1. 登入 Palo Alto Networks 客戶支援入口網站 (CSP)。
2. 選擇 **Products**（產品） > **Assets**（資產）。
3. 根據您啟動 AI Access Security 的強制執行點，選擇 **NGFW** 或 **Prisma Access** 租用戶。
4. 使用篩選器以找到您的 NGFW 或 Prisma Access 租用戶。
5. 展開作用中授權的清單或按一下 **Licenses & Subscriptions**（授權與訂閱）。
6. 驗證 AI Access Security 授權為作用中。



STEP 16 | 開始使用 AI Access Security。

啟動 AI Access Security 授權 (現有部署)

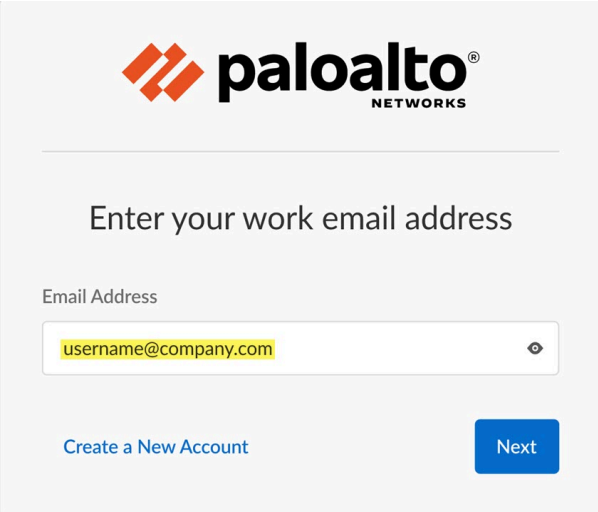
此程序假設您只需要啟動 AI Access Security 授權，且所有先決條件授權都已啟動，並已視需要成功設定您的 NGFW、Prisma Access、Panorama™ management server 和 Strata Cloud Manager。

STEP 1 | 在購買 AI Access Security 訂閱時，請按一下由 Palo Alto Networks 提供的連結。

STEP 2 | 按一下 **Activate Subscription**（啟動訂閱）以開始啟動 AI Access Security。

STEP 3 | 輸入您的 Palo Alto Networks 客戶支援入口網站 (CSP) **Email Address**（電子郵件地址）。此電子郵件地址必須與收到連結的電子郵件相符，才能啟動 AI Access Security。

如果收到 AI Access Security 啟動鏈接的電子郵件地址尚未有有效的 CSP 帳戶，請 **Create a New Account**（建立新帳戶）。新建立的帳戶會自動與您正在啟動 AI Access Security 的相同租用戶相關聯，並獲指派多租用戶超級使用者角色。



STEP 4 | (僅限多租用戶) 在 **Customer Support Account**（客戶支援帳戶）區段中，選擇與您正在啟動 AI Access Security 授權的租用戶相關聯的 Palo Alto Networks 客戶支援帳戶。

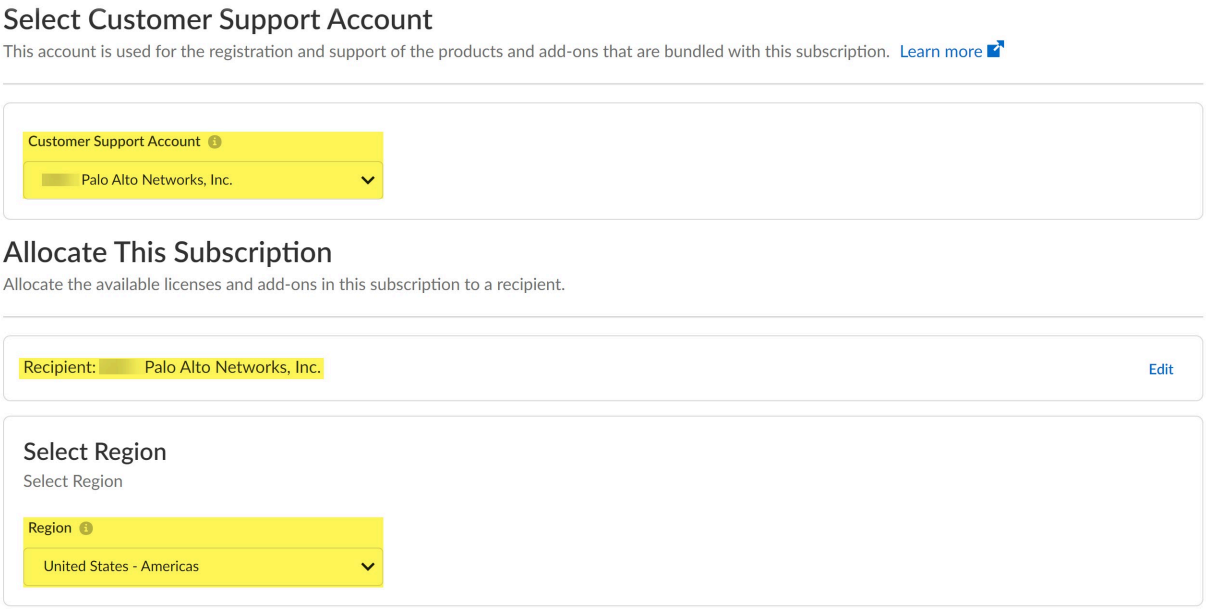
如果您擁有單一租用戶客戶支援入口網站帳戶，請跳過此步驟。依預設，已選取您的客戶支援帳戶。

STEP 5 | (僅限多租用戶) 在 **Allocate This Subscription**（配置此訂閱）區段中，選擇您要啟動 AI Access Security 的租用戶服務群組 (TSG)。您可以選擇父租用戶或子租用戶。

AI Access Security 僅針對所選租用戶啟動。如果您選擇父租用戶，則 AI Access Security 不會針對任何子租用戶啟動。

如果您僅擁有單一租用戶客戶支援入口網站帳戶，請跳過此步驟。依預設，已選取該帳戶。

STEP 6 | 檢閱租用戶 **Region**（地區）。此地區根據已部署的NGFW或Prisma Access 租用戶地區預先填入，且無法變更。

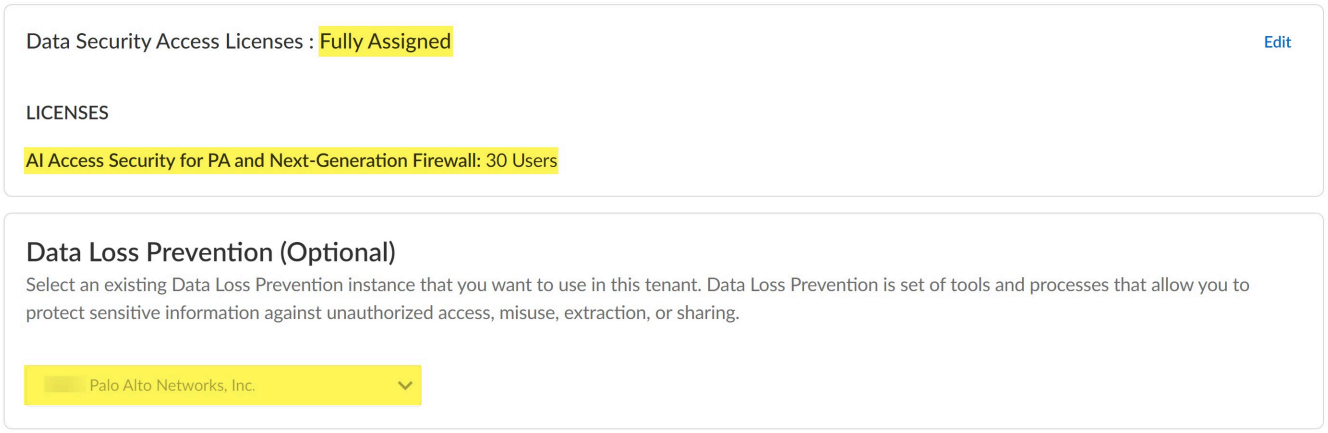


STEP 7 | 在**Assign Licenses**（指派授權）區段中，按一下 **Done**（完成）以指派您所有的 AI Access Security 授權。驗證 **AI Access Security License**（**AI** 存取安全性授權）為 `Fully Assigned`。

STEP 8 | 如果您在租用戶上已啟動 Enterprise Data Loss Prevention (E-DLP)，請驗證已選擇您的 **Data Loss Prevention**（資料遺失防護）執行個體。

如果在租用戶上已啟動，則預設會選擇您的 Enterprise DLP 執行個體。

如果您尚未啟動 Enterprise DLP，請跳過此步驟。啟用 AI Access Security 不需要 Enterprise DLP。如果尚未啟動 Enterprise DLP 執行個體，則在授權啟動時會建立一個執行個體。檢閱在您未更新您的 AI Access Security 授權時，Enterprise DLP 將會有何影響。

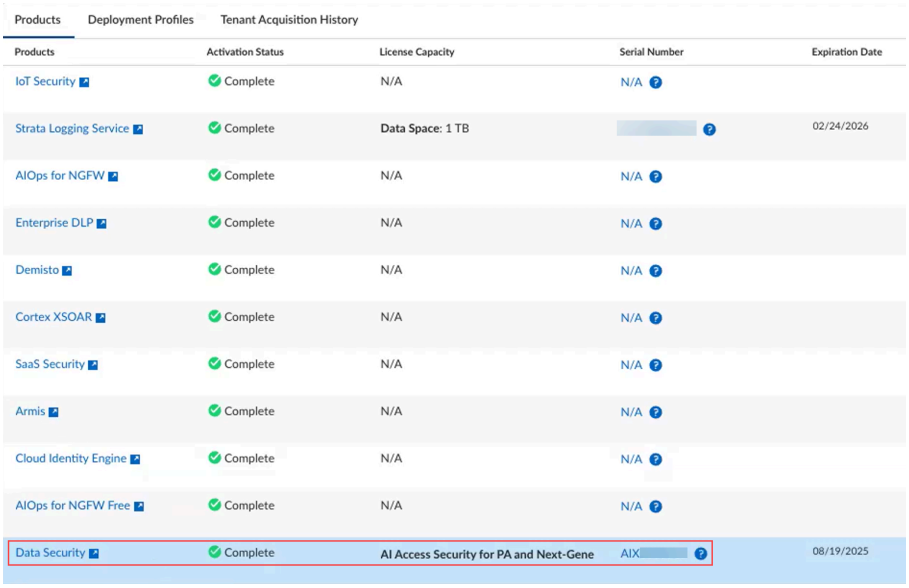


STEP 9 | **Agree to the terms and conditions**（同意條款和條件）。

STEP 10 | Activate（啟動）。

系統會將您重新導向至 Tenant Management（租用戶管理）頁面，其中AI Access Security **Activation Status**（啟動狀態）開始初始化。

AI Access Security 授權會顯示為**Data Security**（資料安全性），其序號以 `AIX` 開頭。在 **Activation Status**（啟動狀態）為 `Complete` 後，繼續下一步。



STEP 11 | (僅限 NGFW) 將 AI Access Security 授權與您的 NGFW 相關聯。

必須關聯 AI Access Security 授權，才能啟動您的 NGFW 授權。

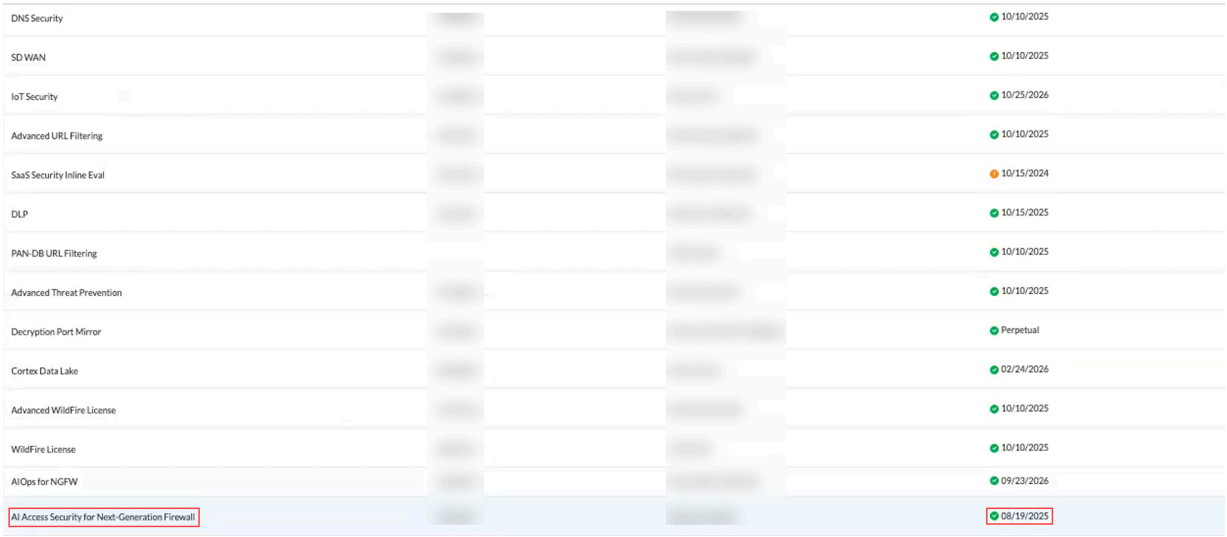
1. 在 Strata Cloud Manager 功能表中，選擇 **Settings**（設定） > **Device Associations**（裝置關聯）。

   Strata Cloud Manager 功能表位於 Strata Cloud Manager 的左下角。
2. 在 Strata Cloud Manager 功能表中，選擇 **System Settings**（系統設定） > **Device Associations**（裝置關聯）。

   Strata Cloud Manager 功能表位於 Strata Cloud Manager 的左下角。
3. **Associate Apps**（關聯應用程式）。
4. 在已授權的產品中，選擇 **Data Security**（資料安全性）。
5. 選擇您要啟動 AI Access Security 的 NGFW。
6. **Save**（儲存）。

STEP 12 | 驗證您已成功啟用 AI Access Security。

1. 登入 Palo Alto Networks 客戶支援入口網站 (CSP)。
2. 選擇 **Products**（產品） > **Assets**（資產）。
3. 根據您啟動 AI Access Security 的強制執行點，選擇 **NGFW** 或 **Prisma Access** 租用戶。
4. 使用篩選器以找到您的 NGFW 或 Prisma Access 租用戶。
5. 展開作用中授權的清單或按一下 **Licenses & Subscriptions**（授權與訂閱）。
6. 驗證 AI Access Security 授權為作用中。



STEP 13 | 開始使用 AI Access Security。

將 AI Access Security 評估授權轉換為生產授權。

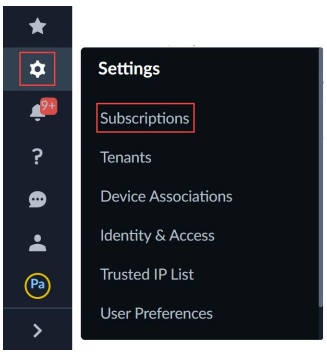
如果您已啟動 AI Access Security EVAL 授權,則必須將評估授權轉換為生產授權，才能在評估期間結束後繼續安全控制存取並採用 GenAI應用程式。如果您未將評估授權轉換為生產授權：

- 包含敏感資料的流量不再轉送到 Enterprise Data Loss Prevention (E-DLP) 進行檢查和裁定呈現。
- Enterprise DLP 不再可存取。
  - **Panorama™ management server**—**Objects**（物件） > **DLP**
  - **Strata Cloud Manager**—**Manage**（管理） > **Configuration**（設定） > **Data Loss Prevention**（資料遺失防護）
- 已保留針對 AI Access Security 建立的 Web 安全性和安全性政策規則。

STEP 1 | 登入 Strata Cloud Manager。

STEP 2 | 在 Strata Cloud Manager 功能表中,選取 **Settings**（設定） > **Subscriptions**（訂閱）。

Strata Cloud Manager 功能表位於 Strata Cloud Manager 的左下角。



STEP 3 | 選取 **System Settings**（系統設定） > **Subscriptions**（訂閱）。

STEP 4 | 尋找 AI Access Security 評估授權,然後選取 **Actions**（動作） > **Eval to Prod Request**（評估轉生產的要求）。

STEP 5 | 為您的租用戶指定您要的生產授權期限。您的 Palo Alto Networks 帳戶代表會檢閱要求以建立報價。

在生產授權要求中指定下列資訊。

- 授權數量—可使用 AI Access Security 的個人數目。
- 期限—AI Access Security 訂閱的時間長度。

STEP 6 | **Send Request**（傳送要求）。

更新 AI Access Security 授權

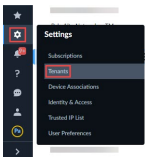
您可以更新即將到期的 AI Access Security 授權以繼續安全採用 GenAI 應用程式。即將到期的 AI Access Security 不會自動更新,需要您手動更新。如果 AI Access Security 到期:

- 包含敏感資料的流量不再轉送到 Enterprise Data Loss Prevention (E-DLP) 進行檢查和裁定呈現。
- Enterprise DLP 不再可存取。
  - **Panorama™ management server**—**Objects**（物件） > **DLP**
  - **Strata Cloud Manager**—**Manage**（管理） > **Configuration**（設定） > **Data Loss Prevention**（資料遺失防護）
- 已保留針對 AI Access Security 建立的 Web 安全性和安全性政策規則。

STEP 1 | 請聯絡您的 Palo Alto Networks 銷售代表，並要求更新您的 AI Access Security 授權。

STEP 2 | 登入 Strata Cloud Manager。

STEP 3 | 從左下角功能表中,選取 **Settings**（設定） > **Tenants**（租用戶）。



STEP 4 | 選取 **System Settings**（系統設定） > **Tenants**（租用戶）。

STEP 5 | 選取您要為其更新 AI Access Security 授權的租用戶。

您可以選擇父租用戶或子租用戶。需要立即採取動作以更新授權的租用戶，會標記藍色圓圈。

STEP 6 | **Edit**（編輯）租用戶授權。

STEP 7 | **Agree to the terms and conditions**（同意條款和條件），然後 **Activate Now**（立即啟動）。