

# Prisma Access Browser 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

Palo Alto Networks, Inc. www.paloaltonetworks.com

© 2024-2024 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

#### Last Revised

July 15, 2024

## Table of Contents

啟動新的 Prisma Access Browser 和 Prisma Access 企業套件授權	5
啟用獨立 Prisma Access Browser 授權	9
在 Strata Cloud Manager 上線 Prisma Access Browser	13
完成預先上線工作	14
新增 IdP 設定	. 14
上線 Prisma Access Browser	16
步驟 1 - 使用者	. 16
第2步-Prisma Access 整合	16
第3步-路由	17
第 4 步 - 強制執行 SSO 應用程式	17
第5步-下載和散佈	. 18
第6步-瀏覽器政策	. 18
上線新使用者	19
指派 Prisma Access Browser 角色	.21

## TECH**DOCS**

# 啟動新的 Prisma Access Browser 和 Prisma Access 企業套件授權

這可在何處使用?	我需要哪些內容?			
Strata Cloud Manager	• 您產品的啟動連結			
• Panorama	• 啟動需要 Strata 記錄服務 (SLS)			
	• 包含雲端識別引擎 (CIE),並在啟動期間啟 動			
	• 客戶支援入口網站 (CSP) 帳戶			



開始此工作之前請先參閱先決條件。

- 雲端
- Panorama

### 雲端管理的 Prisma Access Browser 套件授權

當您收到 Palo Alto Networks 的電子郵件,指明您正在啟動的授權時,請使用啟動連結以開始啟動程序。

**STEP 1** 在您的電子郵件中選取 Activate Subscription (啟動訂閱)。

#### 🊧 paloalto

Your subscription is ready for activation! Click below to get started. Lea	arn more
Secure Enterprise Browser with Prisma Access Enterprise Licensed Quantity: 2000 Mobile Users Service Location: Worldwide	Valid thru: 12/31/2025
Activate Subscription	

- STEP 2 依照 啟動 Prisma Access 授權、配置 Prisma Access 授權,和 規劃服務連線的指示進行操作。
- **STEP 3**| 繼續指派 Prisma Access Secure Enterprise Browser 授權和附加元件。根據您的合約, **Products**(產品)或**Add-ons**(附加元件)預設為啟用。
- **STEP 4** | 選取 Secure Enterprise Browser with Prisma Access Enterprise (具有 Prisma Access 企業的安全企業瀏覽器)。

這與 配置 PA 行動使用者授權類似。您將能夠跨多個 Prisma Access 租用戶部分配置和啟動 Prisma Access Browser 授權。例如:

- 您可以購買 5,000 個 Prisma Access Browser 企業行動使用者。
- 您可以配置:
  - 向 PoC 租用戶提供 1,000 個 (這是所需的最低數量)
  - 生產租用戶 3,000
  - 保留 1,000 個未啟動以供以後使用
- STEP 5| 前往 Prisma Access Browser管理指南來管理您的 Prisma Access Browser。
- **STEP 6**| (選用) 指派角色,以便您的管理員可以管理 Prisma Access Browser。

### Panorama 管理的 Prisma Access Browser 套件授權

當您收到 Palo Alto Networks 的電子郵件,指明您正在啟動的授權時,請使用啟動連結以開始啟動程序。



不適用於 Panorama 多租用戶。

STEP 1 | 在您的電子郵件中選取 Activate Subscription (啟動訂閱)。

#### 🊧 paloalto



- STEP 2| 按照 啟動 Prisma Access (由 Panorama 管理) 授權的指示進行操作。
- STEP 4 | 選取 Secure Enterprise Browser with Prisma Access Enterprise (具有 Prisma Access Enterprise 的安全企業瀏覽器)。
- STEP 5|在 Panorama 中,前往 Panorama tab (Panorama 頁籤) > Cloud Services Plugin (雲端服務<br/>外掛程式) > Prisma Access Browser tab (Prisma Access Browser 頁籤)。

這將啟動一個新頁籤,其中包含 Strata Cloud Manager 的精簡版本,其僅包含 Prisma Access Browser 特定檢視。

- STEP 6| 前往 Prisma Access Browser管理指南來管理您的 Prisma Access Browser。
- STEP 7| (選用)指派角色,以便您的管理員可以管理 Prisma Access Browser。



# 啟用獨立 Prisma Access Browser 授 權

這可在何處使用?	我需要哪些內容?
Strata Cloud Manager	• 您產品的啟動連結
	• 包含雲端識別引擎 (CIE),並在啟動期間啟 動
	• 客戶支援入口網站 (CSP) 帳戶



開始此工作之前請先參閱 先決條件。

當您收到 Palo Alto Networks 的電子郵件,指明您正在啟動的授權時,請使用啟動連結以開始啟動程序。

<pre>//&gt; paloalto*</pre>					
Your subscription is ready for activation! Click below to get st	arted. Learn more				
Prisma Access Secure Enterprise Browser Licensed Quantity: 2000 Mobile Users	Valid thru: 12/31/2025				
Activate Subscription					

- STEP 1 使用您的電子郵件地址登入。
  - 如果您有 Palo Alto Networks 客戶支援帳戶,請輸入您註冊帳戶時所使用的電子郵件地址, 然後選取 Next(下一步)。
  - 如果您沒有 Palo Alto Networks 客戶支援帳戶,請在 Next(下一步) > Create a New Account(建立新帳戶) > Password(密碼)。



本服務使用此電子郵件地址作為指派給您用於此授權的租用戶的使用者帳戶。該租用戶以及透過此電子郵件地址所建立的任何其他租用戶都將具有超級使用者角色。

STEP 2 如果您只有一個與您的使用者名稱相關聯的客戶支援入口網站帳戶,則會預先填入 Customer Support Account (客戶支援帳戶)。

如果您有多個客戶支援入口網站帳戶,則可能會出現您可以預期的其他行為。

STEP 3| 將產品配置給您選擇的 Recipient (收件者)。

為了方便起見,提供的名稱與您的客戶支援入口網站帳戶相符。您可以使用提供的名稱或加以 變更。

- STEP 4 | 選擇您想要部署產品的資料擷取 Region(區域)。
- STEP 5| 指派 Prisma Access Secure Enterprise Browser 授權和附加元件
  - 1. 選取 Prisma Access Secure Enterprise Browser。
  - 2. 這與配置 PA 行動使用者授權類似。您將能夠跨多個 Prisma Access Browser 租用戶部分配 置和啟動 Prisma Access 授權。例如:
    - 您可以購買 1,000 個獨立 Prisma Access Browser
    - 您可以配置:
      - 向 PoC 租用戶提供 200 個 (這是所需的最低數量)
      - 生產租用戶 600
      - 保留 200 個未啟動以供以後使用
- STEP 6| 新增 Strata Logging Service(之前稱為 Cortex 資料湖),用於儲存租用戶資料,例如設定、遙 測日誌、系統日誌和統計資料。您可以選擇現有執行個體或建立新執行個體。
- STEP 7 | 選取雲端識別引擎或建立新的 CIE 執行個體來識別和驗證基礎結構中的所有使用者。

**STEP 8** | Agree to the terms and conditions(同意條款和條件),然後 Activate(啟動)。

Contener Support Account  Select Customer Support Account Illocate This Subscription ocate some or all of the available licenses and add-ons i Specify the Recipient	n this subscription to a recipient.		
Select Customer Support Account	n this subscription to a recipient.		
Ilocate This Subscription ocate some or all of the available licenses and add-ons i Specify the Recipient	in this subscription to a recipient.		
Specify the Recipient			
This is the tenant where the product will be activated.	Learn more about tenants		
Select Tenant 🗸			
Select Region Select Region			
Select Region			
Assign Prisma Access Browser Licensee If you plan on adding more tenants or subtenants after	s and Add-ons activation, only assign what's needed for the re-	cipient tenant.	Done
Add Cortex Data Lake			Done
Cortex Data Lake D	ata Log Storage	SLS Region	
Select CDL Instance	N/A		
CDL instance for this tenant Up	to 0 TB available Data log storage estimator 🗳	This is decided by your region selection	
Cloud Identity Engine			Done
Cloud Identity Engine Select CIE Instance	~		Done
CDL instance for this tenant Up	to 0 TB available Data log storage estimator 📓	This is decided by your region selection	

- STEP 9| 前往 Prisma Access Browser管理指南來管理您的 Prisma Access Browser。
- STEP 10| (選用) 指派角色,以便您的管理員可以管理 Prisma Access Browser。

#### <sup>∞ paloalto</sup> TECH**DOCS**

# 在 Strata Cloud Manager 上線 Prisma Access Browser

這可在何處使用?	我需要哪些內容?
Strata Cloud Manager	<ul> <li>Prisma Access 具有 Prisma Access Browser 套件授權</li> <li>超級使用者或 Prisma Access Browser 角色</li> </ul>

開始此工作之前請先參閱先決條件。

### 完成預先上線工作

在上線 Prisma Access Browser 之前,您必須先執行幾項工作才能繼續。

- STEP 1 定義雲端識別引擎實體。這可以使用您在啟動程序中所選取的雲端識別引擎進行設定。
- STEP 2 | 您需要驗證設定檔和使用者群組,其是您的上線程序的一部分。這些會在雲端識別引擎中進 行設定。如需詳細資訊,請參閱驗證設定檔和使用者群組。
  - 您只能有一個驗證設定檔。如果您使用多個識別提供者 (IdP),則可以為每個設定檔設定多個 IdP。在您設定驗證設定檔時,可以透過選擇 Multiple (多重) Authentication Mode (驗證模式)來完成此操作。

CLOUD IDENTITY ENGINE	Authentication Profiles / Set Up Authentication Profile				
at PALO ALTO RETROBES	Set Up Authentication Profile				
Directory Sync	Add or edit an authentication profile to define how the Cloud Identity Engine authenticates users.				
	Click here to learn more about configuring an authentication profile.				
Directories					
Agents & Certificates	Configure one or more Authentication Types				
Attributes	If you have not already done so, configure an authentication type (such as SAME, 2.0 or a client certificate) to use in the authentication profile.				
	(2) Configure an Authentication Profile				
Authentication	Set Up an Authentication Profile to use a single authentication type (such as SAMI, 2.0 or a client certificate) or multiple authentication types.				
CA Chains	PROFILE NAME				
	Trear Predic Name				
Authentication Types					
Authentication Profiles	Desire Data and a second				
Authentication Logs					
-	Single				
User Context	Mage				
Mappings & Tags					
Secondaria					
Replicito					

新增 IdP 設定

您可以使用目前的 SAML IdP 提供者來管理網路中的一組登入認證。IdP 配置是雲端識別引擎的一個元件,您可以在該工具中對其進行管理。

STEP 1 | 在雲端識別引擎中,選取 Authentication Type (驗證類型)。

**STEP 2**| 按一下 Add New Authentication Type (新增驗證類型)。

	0 IN 50	unvice provider SPI-certil A, authentication your une.	fcate for the Coull klimit	ty Engine has been remewed. To	complete the process, download	The SP metadata for each 5	AM, authoritozitor	you are using	g with the Cloud identity Engin	e and import the SP metad	ata to the IdP. When you ha	we completed this step, click have to verify you't	use updated the metadata-far each
Directory Sync A	Aut 77142 View a	thenticatio	on Types	r add a new authenticat	ion type.								Add New Authentitution Type
Agents & Certificates	SAM												
Atributes			Name	SP Eveny ID	Entity ID	Single Sign On (SSC)	SSOHTTPI	Indeg	Certificate	Force-Authentication	SAMLAge ID	Unit By	Action
Authentication	55-3 8-3-	nd3 a407-4005- 703h10dhorid	Taloracc	https://dead-auth-spain.ig augenic.patializecheark sciencing	Mips:/hts.minikows.mt/% 2060/05-7226-4747-1921 0-4794/5654/07567	Mpc./hgin.microsoftanti microsoftaddiad/5-7226- atto:7-8240- diad/filesoft/filesoft			Morouit Aure Federated \$50 Continue Equitor in 2 years	False		Takon Sec.	T
CA Owins	1.00												
Authentication Types													
Authentication Profiles	Clier	nt Certificate											
Authentication Lags	Ð		Name	6	Owin Name O	A Owin ID		Ukenae	w Athlune Used	h.			Actors
User Context A													
							=						
Third-Party Device-ID													
Settings							No R	esuits Avai	lable				
	0 Res	alla i											
TechDocs	00	c											
A many	Ð		Name	hour URL	Client Name	Client M	- 6	had By					Actions
	(0.3) 204-	612-1606-6803- 61257/Datier	handeye olde	https://doi-4004062.akta.com	00000	OsuhgeriOcBU 2	NONRY N	and a second second	pula				1
Che Feedback	0 Res	dis											
111 All Annihisations													

當您使用 IdP 提供者的資訊填入使用者群組時,您需要確保正確輸入有效的電子郵件地址。UPN 不夠。

STEP 3 | 在 [Set Up Authentication Type (設定驗證類型)]中,按一下 [SAML 2.0 設定]。

- STEP 4| 若要繼續設定 SAML 驗證器,請參閱在雲端識別引擎中設定 SAML 2.0 驗證類型。
- **STEP 5**| (選用)使用 Google Workspace 整合。

### 上線 Prisma Access Browser

完成上線步驟之後,您可以在 Strata Cloud Manager 上線 Prisma Access Browser。

在新增使用者之前。您需要在 Strata Cloud Manager 啟動並設定 Prisma Access Browser。一般來 說,這是一個一次性程序,您只需在啟動整後執行一次,但是您可以在需要修改這些工作時隨時返 回執行這些工作。

您可以使用精靈來完成此程序,並且您可以隨時修改全域設定。此精靈提供有關完成整合每個步驟 的詳細指示。

您看到的控制項取決於您的 Prisma Access Browser 授權; 並非所有授權都可以使用 Strata Cloud Manager 中的所有上線功能。

從 Strata Cloud Manager, 選取 Workflows(工作流程) > Prisma Access Setup(設定) > Prisma Access Browser(Prisma Access 瀏覽器)。

### 步驟1-使用者

定義使用者驗證方法和上線使用者群組。

- STEP 1 | 從下拉清單中,選擇將用於使用者身份驗證的 CIE 設定檔.
- **STEP 2** | 從 User groups 下拉式清單中, 選取 **User groups**(使用者群組)將能夠存取 Prisma Access Browser。
- **STEP 3**| Next: (下一個:) Prisma Access Integration (整合)。

第2步 - Prisma Access 整合

- **STEP 1**| 啟用到 Prisma Access 的外部連線。
  - 1. 選取 Go to Explicit Proxy settings (前往明確 Proxy 設定)。
  - 這將帶您進入 Workflows(工作流程) > Prisma Access Setup(設定) > Explicit Proxy(明確 Proxy)。
  - 3. 啟用 Prisma Access Browser。
  - 4. **Done**(完成)。

STEP 2| 在 Prisma Access 安全性政策中允許 Prisma Access Browser。

- 1. 選取 Manage (管理) > Prisma Access > Security Policy (安全性政策)。
- 2. 這將帶您進入 Manage (管理) > Prisma Access > Security Policy (安全性政策)。
- 3. 在安全性政策中新增允許網頁流量的規則。
- 4. 推送設定以接受規則。
- 5. **Done**(完成)。

STEP3 建立服務連線。

- 1. 選取 Create a service connection (建立服務連線)。
- 這將帶您進入 Workflows(工作流程) > Prisma Access Setup(設定) > Service Connections(服務連線)和 Add Service Connection(新增服務連線)。
- 3. Done (完成)。
- 4. 接下來:路由。

第3步-路由

路由控制項可讓您管理 Prisma Access Browser 處理網路流量的方式。此功能為 Prisma Access Browser 設定預設設定。如果您需要調整特定規則的控制精細度,請參閱流量的瀏覽器自訂控制。

STEP1| 選擇下列其中一個選項:

- Only route private application traffic through Prisma Access (僅透過 Prisma Access 路由私 人應用程式流量)。
- Route all traffic through Prisma Access (透過 Prisma Access 路由所有流量)。
- STEP 2| (選用)確保當瀏覽器偵測到流量在內部網路中執行時, Prisma Access Browser 流量以最佳方式行動。此識別是根據僅在內部網路內部可用的主機所建立的連線。
  - 輸入要解析的 FQDN。
  - 輸入預期的 IP 位址。

**STEP 3** Next:(下一個:) Enforce SSO applications(強制執行 SSO 應用程式)。

第4步-強制執行 SSO 應用程式

重要的是,您的使用者在啟用 SSO 的應用程式上進行驗證的唯一方式是使用 Prisma Access Browser。這將確保外部行為者無法存取您的企業應用程式。若要選取您的 IdP:

STEP 1 在選擇並設定您的識別提供者中,選取可用的 IdP。選項包括:

- Okta
- Microsoft Azure Active Directory
- PingID
- OneLogin
- VMware Workspace ONE Access
- STEP 2| 在您設定本機設定時,請務必記下輸出 IP 位址。

**STEP 3**| 接下來:下載和散佈。

第5步-下載和散佈

您可以下載 Prisma Access Browser 安裝檔案,以便在您自己的裝置上進行測試,然後再將其傳送給您的使用者。對測試感到滿意後,您可以下載相關安裝程式,以便由行動裝置管理 (MDM)應用程式進行散佈。

您還可以對使用者傳送下載連結,以便其可以自己下載 Prisma Access Browser。這是僅適用於 macOS 和 Windows 使用者的單一連結。

STEP 1 | 從可用選項中選取:

- 桌面:
  - macOS
  - Windows
- 行動裝置:
  - iOS
  - Android

您還可以對使用者傳送下載連結,以便其可以自己下載 Prisma Access Browser。這是僅適用於 macOS 和 Windows 使用者的單一連結。



如果您對使用者傳送下載連結,請提醒他們,其只能使用 *IdP* 服務中設定的電子郵件進行登入。

**STEP 2**| Next:(下一個:) Browser Policy(瀏覽器政策)。

第6步-瀏覽器政策

您現在可以開始探索和設定 Prisma Access Browser 政策引擎以建立安全且可靠的使用者環境。

- **STEP 1**| 選取 Browser Policy (瀏覽器政策)。
- STEP 2
   這會將您導向 Manage (管理) > Configuration (設定) > Prisma Access Browser (瀏覽 器) > Policy (政策) > Rules (規則)。
- **STEP 3**| 管理 Prisma Access Browser 政策規則。

### 上線新使用者

入門工作流程是新使用者開始使用瀏覽器時顯示的一系列可設定視窗。

根據 IT 需求和要求,您可以選擇最多八個單獨的頁面,允許使用者可以使用他們的圖片和書籤自 訂瀏覽器,並找到有關瀏覽器的一些基本資訊 - 一種「快速入門」指南。

裝載精靈自訂控制項可以設定裝載工作流程。您可以選取在網路中顯示哪些視窗。

當您建立或編輯 Browser Customization (瀏覽器自訂)設定檔並選擇 Onboarding Wizard (裝載精靈)時,您可以在 Manage (管理) > Configuration (設定) > Prisma Access Browser (Prisma Access 瀏覽器) > Policy (政策) > Profiles (設定檔)中進行設定。如需設定詳 細資料,請參閱裝載精靈的瀏覽器自訂控制。

## TECH**DOCS**

# 指派 Prisma Access Browser 角色

這可在何處使用?	我需要哪些內容?
Strata Cloud Manager	<ul> <li>具有 Prisma Access Browser 套件授權的 Prisma Access 或 Prisma Access Browser 獨 立授權</li> </ul>
	角色:多租用戶超級使用者或有權存取客戶 支援入口網站的超級使用者

您可以為不同類型的 Prisma Access Browser 的管理員建立和管理角色型存取控制。這可讓大型組織中的主要管理員指定其他管理員、與其特定角色相關的權限,其中包括可視性和存取權。

啟動您的授權之後,可以管理管理員使用者存取權限並指派以下 Prisma Access Browser 特定的其中 一個角色:

企業角色	權限	支援的應用程式
PA 瀏覽器存取 權和資料管理員	設定和管理存取與資料原則、定義自訂或私人應 用程式、處理與一般使用者要求相關原則的讀寫 存取權,以及 Prisma Access 瀏覽器管理區段中項 細目錄方面(使用者、裝置、延伸)和任何可視 性方面(儀表板、一般使用者事件)的唯讀權限	• Prisma Access 瀏覽器
PA 瀏覽器自訂 管理員	設定和管理瀏覽器自訂原則的讀寫存取權,以 及 Prisma Access 瀏覽器管理區段中項細目錄方 面(使用者、裝置、應用程式、延伸)和任何可 視性方面(儀表板、一般使用者事件)的唯讀權 限。	• Prisma Access 瀏覽器
PA 瀏覽器權限 要求管理員	處理與一般使用者要求相關原則的讀寫存取權, 以及 Prisma Access 瀏覽器管理區段中可視性方面 (儀表板、一般使用者事件)的唯獨權限。	• Prisma Access 瀏覽器
PA 瀏覽器安全 性管理員	設定和管理瀏覽器安全性原則的讀寫存取權,以及 Prisma Access 瀏覽器管理區段中項細目錄方面(使用者、裝置、應用程式、延伸)和任何可視性方面(儀表板、一般使用者事件)的唯讀權限。	• Prisma Access 瀏覽器

企業角色	權限	支援的應用程式
PA 瀏覽器安全 性和裝置狀態管 理員	設定和管理瀏覽器安全性原則、管理裝置狀態 群組和設定登入規則的讀寫存取權。其也提供 Prisma Access 瀏覽器管理區段中項細目錄方面 (使用者、應用程式、延伸)和任何可視性方面 (儀表板、一般使用者事件)的唯讀權限。	• Prisma Access 瀏覽器
PA 瀏覽器僅檢 視分析	任何 Prisma Access 瀏覽器管理區段中可視性方面 的讀取存取權,其中包括儀表板、詳細的一般使 用者事件和項細目錄方面(使用者、裝置、應用 程式和延伸)。	• Prisma Access 瀏覽器