paloalto TECHDOCS

# Prisma Access 管理

4.00 and 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

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2022-2025 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

### Last Revised

April 23, 2025

# Table of Contents


**Prisma Access 概要 ..... 13**

使用 Prisma Access 保護網際網路流量 ..... 16

網際網路安全性的重要性 ..... 16

Prisma Access 雲端安全 Web 閘道 (SWG) ..... 16

使用 Prisma Access 保護使用者和端點 ..... 16

如何管理 Prisma Access ..... 18

搭配 Strata Cloud Manager 的 Prisma Access 可視性與監控 ..... 22

Prisma Access 個位置 ..... 24

計算位置、城市和國家/地區 ..... 25

劇場和位置群組 ..... 30

依地區劃分的位置 ..... 34

明確 Proxy 位置 ..... 39

Colo-Connect 位置 ..... 40

支援的 Strata Logging Service 地區 ..... 41

遠端網路—高效能、流量複寫和安全輸入存取位置 ..... 42

Prisma Access 中國位置 ..... 45

FedRAMP 中位置和高位置 ..... 45

北美位置地圖 ..... 45

本機區域位置 ..... 46

**Prisma Access** 和相關聯的服務處理位置 ..... 47

Prisma Access 基礎結構管理 ..... 49

Prisma Access API ..... 51

適用於 Prisma Access (Managed by Strata Cloud Manager) 的 API ..... 51

適用於 Prisma Access (Managed by Panorama) 的 API ..... 51

使用瀏覽器和網頁介面存取 Prisma Access (Managed by Panorama) API ..... 51

使用 curl 命令擷取 Panorama 受管理 API 命令 ..... 53

使用 CLI 命令搭配 Prisma Access (Managed by Panorama) ..... 54

Prisma Access 洞察 API ..... 54

將 Prisma Access 從 Panorama 移轉至 Strata Cloud Manager ..... 56

準備移轉至 Prisma Access (Managed by Strata Cloud Manager) ..... 56

將您的 Prisma Access (Managed by Panorama) 部署移轉至 Strata Cloud Manager ..... 57

**Prisma Access 版本和升級 ..... 69**

Prisma Access 版本類型 ..... 70

緊急排程升級 ..... 71

Prisma Access 升級類型 ..... 72




©2025 Palo Alto Networks, Inc.

Prisma Access 的軟體和內容更新節奏 74
Prisma Access 資料平面升級 79
取得升級警示和更新 84
檢視 Prisma Access 軟體版本 89
Prisma Access (Managed by Strata Cloud Manager) 89
Prisma Access (Managed by Panorama) 90

**Prisma Access 設定 95**

設定 Prisma Access 97
設定 Prisma Access 服務基礎結構 104
行動使用者：IP 位址配置 118
範例：公用 IP 位址調整範例（行動使用者） 118
回送 IP 位址配置（行動使用者） 121
遠端網路：IPSec 終端節點和服務 IP 位址 124
遠端網路：與頻寬配置相關的 IP 位址變更 125
遠端網路：服務 IP 位址和輸出 IP 位址配置 128
擷取 Prisma Access 的 IP 位址 129
用於行動使用者—GlobalProtect 部署的 IP 最佳化 152
擷取 Prisma Access IP 位址的 API 範例 154
在 Prisma Access IP 位址變更時收到通知 156
使用舊版指令碼擷取 IP 位址 158
擷取行動使用者 IP 位址 160
擷取公用、回送和輸出 IP 位址 161
Prisma Access 區域 164
DNS for Prisma Access 166
Prisma Access 的高可用性 172
預先定義範本：裝載服務連線或遠端網路 175
常見 SD-WAN 裝置支援的 IKE 和 IPSec 密碼設定檔 180

**Prisma Access 服務連線 183**

規劃服務連線 185
收集此總部或資料中心資訊 185
在 Prisma Access 中設定服務連線 187
使用服務連線啟用行動使用者與遠端網路之間的存取 214
服務連線的動態路由考量 216
運作方式—路由服務連線流量 216
Prisma Access 預設路由 216
熱馬鈴薯路由 219

**Prisma Access ZTNA 連接器 225**


©2025 Palo Alto Networks, Inc.

ZTNA 連接器元件 ..... 226
ZTNA 連接器的使用案例 ..... 227
服務連線和 ZTNA 連接器支援的使用案例 ..... 231
ZTNA 連接器 2.0 原則 ..... 232
ZTNA 連接器需求和指導方針 ..... 233
支援的 Prisma Access 版本和需求 ..... 233
應用程式支援 ..... 233
特徵和功能限制 ..... 234
規模和輸送量考量 ..... 235
支援的應用程式託管環境 ..... 235
網路需求 ..... 236
ZTNA 連接器允許的 IP 位址和 FQDN ..... 238
憑證管理 ..... 241
啟用 ZTNA 連接器 ..... 242
設定 ZTNA 連接器 ..... 248
升級 ZTNA 連接器 ..... 257
ZTNA 連接器診斷工具 ..... 260
刪除連接器 IP 區塊 ..... 267
使用雲端識別引擎設定應用程式的自動探索 ..... 272
私人應用程式目標探索 ..... 273
啟用應用程式搭配 ZTNA 連接器的安全性政策 ..... 280
在您的資料中心裝載 ZTNA 連接器 VM ..... 296
支援的 ZTNA 連接器部署 ..... 296
ZTNA 連接器支援 Microsoft Azure 部署 ..... 298
ZTNA 連接器支援的 Google Cloud Platform 部署 ..... 315
ZTNA 連接器支援 Amazon Web Services 部署 ..... 325
Prisma Access ZTNA 連接器支援的 VMware ESXi 部署 ..... 331
Prisma Access ZTNA 連接器支援 KVM 部署 ..... 342
Prisma Access ZTNA 連接器支援的 Hyper-V 部署 ..... 347
監控 ZTNA 連接器 ..... 360
檢視 ZTNA 連接器日誌 ..... 363
保留 ZTNA 連接器與來源 NAT 連線的 User-ID 對應 ..... 366
設定動態權限存取設定 ..... 375
什麼是動態權限存取？ ..... 376
透過 Common Services 為 Prisma Access 啟用動態權限存取 ..... 377
在雲端識別引擎中授權使用者群組對應進行動態權限存取 ..... 379
啟用存取代理程式 ..... 387
設定代理程式基礎結構進行動態權限存取 ..... 389

 ©2025 Palo Alto Networks, Inc.

設定基礎結構設定 389
選取 Prisma Access 位置 390
為動態權限存取啟用 SC-NAT 支援 394
為動態權限存取啟用路由彙總 395
建立片段 397
設定專案特定的 Prisma Access Agent 設定 407
設定轉送設定檔，為動態權限存取代理程式管理代理程式流量 407
設定 Prisma Access Agent 應用程式設定進行動態權限存取 420
設定 DNS 設定進行動態權限存取。 427
設定 HIP 資料收集設定進行動態權限存取 428
建立專案 432
動態權限存取的流量導向 435
設定 Prisma Access Agent 進行動態權限存取 437
為 Prisma Access Agent 設定分階段推出 437
為 Prisma Access Agents 設定一般全域設定 445
為動態權限存取 Prisma Access Agent 設定 HIP 通知 448
推送 Prisma Access Agent 設定 458
下載已啟用動態權限存取的 Prisma Access Agent 套件 461
使用 Prisma Access Agent 存取您的專案 463
安裝 Prisma Access Agent。 463
登入已啟用動態權限存取的 Prisma Access Agent 471
變更已啟用動態權限存取的 Prisma Access Agent 的偏好設定 476
將已啟用動態權限存取的 Prisma Access Agent 連線到不同的位置 478
切換至不同的租用戶 479
將已啟用動態權限存取的 Prisma Access Agent 連線到不同的伺服器 481
在 Prisma Access Agent 與 GlobalProtect 應用程式之間切換 483
檢視和監控動態權限存取使用者 489
已連線使用者 489
檢視和監控動態權限存取專案 494
專案 494

**Prisma Access Colo-Connect 497**

Colo-Connect 使用案例 499
高頻寬存取私人應用程式 499
私人應用程式的私人連線 499
使用第三方 NaaS 提供者 499
Colo-Connect 與服務連線和 ZTNA 連接器有何不同？ 500
Colo-Connect 不支援的功能 501
Prisma Access Colo-Connect 的需求和先決條件 502

 ©2025 Palo Alto Networks, Inc.

設定 Prisma Access Colo-Connect ..... 504

## Prisma Access 中的應用程式加速 ..... 555

應用程式加速需求和指導方針 ..... 557
設定應用程式加速 ..... 560

## Prisma Access 行動使用者 ..... 583

行動使用者：GlobalProtect ..... 585
規劃 Prisma Access 上 GlobalProtect 的檢查清單 ..... 585
設定 GlobalProtect 行動使用者 ..... 588
GlobalProtect—自訂通道設定 ..... 623
GlobalProtect—自訂應用程式設定 ..... 628
提出票證要求以停用 GlobalProtect ..... 637
GlobalProtect 預先登入 ..... 642
GlobalProtect—無用戶端 VPN ..... 657
監控 GlobalProtect 行動使用者 ..... 659
用於 GlobalProtect 行動使用者部署的 IP 位址集區 ..... 664
GlobalProtect 應用程式如何為行動使用者選取 Prisma Access 位置 ..... 670
允許列出 GlobalProtect 行動使用者 ..... 672
GlobalProtect 應用程式升級 ..... 683
整合 Prisma Access 與內部部署 GlobalProtect 閘道 ..... 691
行動使用者：明確 Proxy ..... 709
明確 Proxy 設定指導方針 ..... 711
Proxy 模式下的 GlobalProtect ..... 715
通道和 Proxy 模式下的 GlobalProtect ..... 728
代理程式型 Proxy 流量的私人 IP 位址可見性和強制執行 ..... 750
用於明確 Proxy 的 SAML 驗證 ..... 752
設定明確 Proxy ..... 755
用於明確 Proxy 部署的 Kerberos 驗證 ..... 776
明確 Proxy 部署的 Cloud Identity Engine 驗證 ..... 808
遠端網路上的 Proxy 模式 ..... 813
明確 Proxy 如何識別使用者 ..... 821
明確 Proxy 轉送設定檔 ..... 822
PAC 檔案指導方針 ..... 831
明確 Proxy 最佳做法 ..... 837
監控明確 Proxy 並針對其進行疑難排解 ..... 838
明確 Proxy 的封鎖設定 ..... 841
使用特殊物件限制明確 Proxy 網際網路流量流向特定的 IP 位址 ..... 843
使用明確 Proxy 存取您的資料中心 ..... 844
應用程式型 Office 365 與明確 Proxy 整合 ..... 849

 ©2025 Palo Alto Networks, Inc.

使用 Blue Coat Proxy 設定 Proxy 鏈結 ..... 853
使用明確 Proxy 搭配 GlobalProtect（或第三方 VPN） ..... 858
明確 Proxy 使用者 - Proxy 部署的 IP 位址最佳化 ..... 871
行動使用者—明確 Proxy 部署的 DNS 解析 ..... 871
檢視使用者至 IP 位址或使用者群組對應 ..... 875
報告行動使用者網站存取問題 ..... 880
啟用行動使用者對 Prisma Access 進行驗證 ..... 882
驗證支援與功能 ..... 883
設定驗證 ..... 887
啟用行動使用者存取公司資源 ..... 893

**Prisma Access 遠端網路 ..... 897**

遠端網路的規劃檢查清單 ..... 898
配置遠端網路頻寬 ..... 903
規劃您移轉至新模型的方式 ..... 918
移轉後彙總頻寬部署的頻寬配置 ..... 921
QoS 移轉指導方針 ..... 922
移轉您的頻寬管理設定 ..... 928
裝載遠端網絡 ..... 935
將遠端網站連線到 Prisma Access ..... 962
新增主要和次要 IPSec VPN 通道 ..... 962
更多 IKE 選項 ..... 963
更多 IPSec 選項 ..... 964
為遠端網路啟用路由 ..... 966
針對網站連線進行疑難排解 ..... 969
裝載多個遠端網路 ..... 971
遠端網路表格中的欄位 ..... 972
驗證遠端網路是否已連線至 Prisma Access ..... 981
驗證遠端連線 BGP 狀態 ..... 983
設定與 WAN 連結連線的遠端網路和服務連線 ..... 985
遠端網路的 QoS ..... 987
變更保證頻寬 ..... 1004
遠端網路—高效能 ..... 1007
遠端網路—高效能的功能與指導方針 ..... 1007
使用終端伺服器整合共用桌面 VDI 與 Prisma Access ..... 1026

**Prisma Access 監控和可視性 ..... 1035**

Prisma Access 日誌 ..... 1036
外部日誌和其他資料 ..... 1037
Prisma Access 活動儀表板和報告 ..... 1038


©2025 Palo Alto Networks, Inc.

在 Strata Cloud Manager 中檢視並監控 Prisma Access ..... 1039
開始在 Strata Cloud Manager 中使用 Prisma Access 監控 ..... 1040
檢視並監控應用程式 ..... 1042
檢視並監控應用程式加速 ..... 1045
檢視行動使用者 ..... 1047
檢視和監控行動使用者的 IPv6 ..... 1047
檢視並監控分支網站 ..... 1049
檢視和監控資料中心 ..... 1057
檢視和監控網路服務 ..... 1076
檢視訂閱使用情況 ..... 1080
檢視和監控 Prisma Access 位置 ..... 1082
檢視和監控第三方 Device-ID ..... 1084
檢視和監控遠端瀏覽器隔離 ..... 1086
Prisma Access 和自發 DEM ..... 1087

**Prisma Access 使用者型政策 ..... 1089**

為 Prisma Access 設定使用者型政策 ..... 1090
整合雲端識別引擎與 Prisma Access ..... 1093
擷取 Prisma Access 的 User-ID 群組對應 ..... 1099
身分重新分配 ..... 1108
在 Prisma Access 中設定第三方 Device-ID ..... 1125
第三方 Device-ID API ..... 1132
更新裁定 ..... 1132
刪除所有裁定 ..... 1134
查詢裁定 ..... 1135
依 IP 位址查詢裁定 ..... 1137
查詢裁定統計資料 ..... 1139

**Prisma Access 多租用戶 ..... 1141**

多租用戶設定概要 ..... 1142
規劃您的多租用戶部署 ..... 1146
建立全新的多租戶部署 ..... 1148
啟用多租戶並移轉第一個租用戶 ..... 1149
將租用戶新增 Prisma Access ..... 1155
刪除租用戶 ..... 1161
建立租用戶層級管理使用者 ..... 1166
控制租用戶層級管理使用者的角色型存取 ..... 1170
移除租用戶層級管理使用者的外掛程式存取 ..... 1171
在多租用戶部署中依裝置群組 ID 排序日誌 ..... 1175

 ©2025 Palo Alto Networks, Inc.

FedRAMP 環境中的 Prisma Access ..... 1177
Prisma Access FedRAMP 需求 ..... 1178
安裝前和產品啟動需求 ..... 1178
所需的 Panorama、外掛程式和 PAN-OS 資料平面版本 ..... 1179
支援的 Prisma Access FedRAMP 位置 ..... 1180
Prisma Access FedRAMP 部署中支援和不支援的功能 ..... 1181
在 FedRAMP 環境中設定 Prisma Access ..... 1182
Prisma Access 進階部署 ..... 1189
為已部署的 Prisma Access 位置新增計算位置 ..... 1191
IPv6 支援 ..... 1193
原生 IPv6 支援概要 ..... 1195
在您的 Prisma Access 基礎結構中啟用並設定 IPv6 網路和 IP 集區 ..... 1198
為行動使用者—GlobalProtect 部署啟用 IPv6 網路 ..... 1206
為服務連線啟用 IPv6 網路 ..... 1210
為遠端網路啟用 IPv6 網路 ..... 1216
行動使用者—GlobalProtect 和遠端網路部署的 DNS 解析 ..... 1226
行動使用者—GlobalProtect 部署的 DNS 解析 ..... 1228
遠端網路的 DNS 解析 ..... 1229
BGP 如何為服務連線和遠端網路連線公告行動使用者 IP 位址集區 ..... 1231
Prisma Access 和 Strata Logging Service 的 Proxy 支援 ..... 1233
封鎖從特定國家/地區傳入的連線 ..... 1234
保護來自 AWS WorkSpace 的網際網路流量 ..... 1235
在 AWS WorkSpace 用戶端上設定 PAC 檔案 ..... 1235
在 AWS 與 Prisma Access 之間設定站台對站台通道 ..... 1237
Prisma Access 用於無預設路由網路 ..... 1238
什麼是無預設路由網路？ ..... 1238
無預設路由網路考量 ..... 1238
保護無預設路由網路進行網際網路存取的部署建議 ..... 1238
關鍵考量 ..... 1239
Prisma Access 服務連線進階部署 ..... 1240
服務連線多重雲端備援 ..... 1240
使用流量導向將網際網路繫結流量轉送到服務連線 ..... 1250
服務連線流量的路由 ..... 1272
使用多個服務連線建立高頻寬網路 ..... 1285
使用來源 NAT 保留服務連線的 User-ID 與 Device-ID 對應 ..... 1298
Prisma Access 行動使用者—GlobalProtect 進階部署 ..... 1306
在 Prisma Access 中設定多個入口網站 ..... 1306
遠端疑難排解和更新的動態 DNS 支援 ..... 1315

 ©2025 Palo Alto Networks, Inc.

行動使用者—GlobalProtect 的動態 DNS 註冊支援 ..... 1331
在 Prisma Access GlobalProtect 部署中識別和隔離遭入侵裝置 ..... 1337
將行動使用者—GlobalProtect 部署中的 IPv6 流量導向至不同的位置 ..... 1346
使用 Prisma Access 重新散佈 HIP 資訊 ..... 1351
檢視 HIP 報告 ..... 1359
無用戶端 VPN 中 Gzip 編碼的支援 ..... 1361
Prisma Access 中的流量複寫 ..... 1363
Prisma Access 遠端網路進階部署 ..... 1375
Prisma Access 內部閘道 ..... 1375
提供對遠端網路位置的安全輸入存取 ..... 1384
**Prisma Access for Clean Pipe ..... 1411**
Prisma Access for Clean Pipe 概要 ..... 1412
Clean Pipe 使用案例 ..... 1412
Clean Pipe 範例 ..... 1412
Clean Pipe 和合作夥伴互連需求 ..... 1413
完成 Clean Pipe 設定 ..... 1416
啟用多租用戶並建立租用戶 ..... 1420

 ©2025 Palo Alto Networks, Inc.

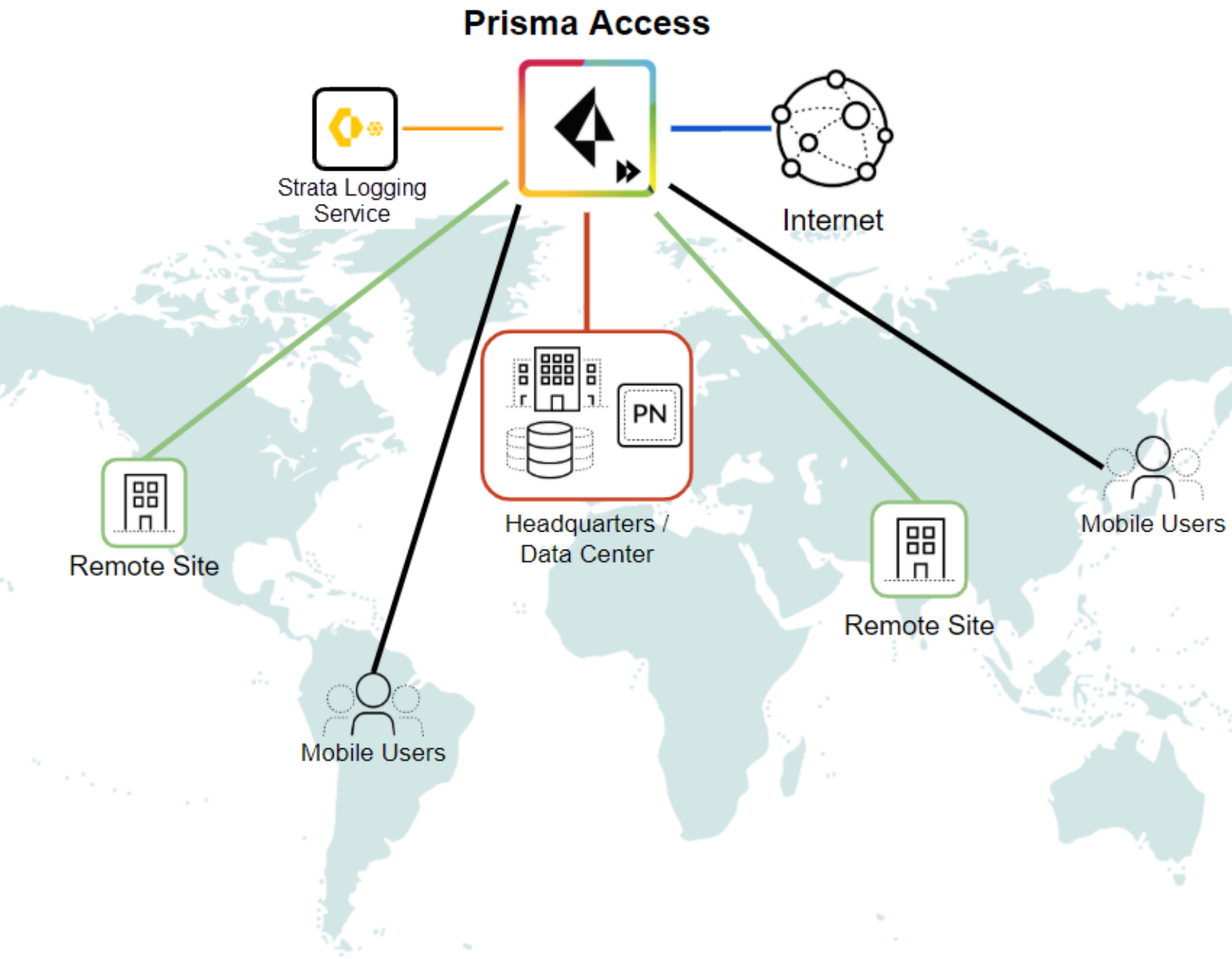
©2025 Palo Alto Networks, Inc.

# Prisma Access 概要

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

為了讓您的應用程式和資料保持安全，您必須始終保護所有位置的所有使用者。但是，當您的足跡在全球範圍內不斷擴大、越來越多的使用者為行動使用者，而您的應用程式和資料正在從您的網路轉移到雲端時，您該如何做到這一點？Prisma Access 透過讓您的使用者能夠安全地存取雲端和資料中心應用程式以及網際網路，無論他們是在總部、分公司還是在路上，都可以啟用這種一致的安全性。Prisma Access 會一直檢查所有連接埠的所有流量，從而可以安全地存取網際網路，以及已認可的 SaaS 應用程式、公用雲端環境，以及資料中心和總部。內建了威脅防護、惡意軟體防護、URL 篩選、SSL 解密和應用程式型政策功能，無論您的使用者身在何處或正在存取什麼資源，都能為您提供相同層級的安全性。所有 Prisma Access 日誌都儲存在 Strata Logging Service 中，從而提供跨所有使用者、應用程式和位置的集中分析、報告和鑑識。

Prisma Access 提供全球覆蓋的大規模保護，因此您不必擔心在分支調整大小和部署硬體防火牆，或在搭配設施中建置和管理設備等問題。Prisma Access 提供網路基礎結構來連線您的所有遠端分支、總部網站、資料中心和行動使用者，而無需您建置自己的全球安全性基礎結構，並擴展您的營運能力。




透過 Prisma Access，Palo Alto Networks 在全球部署和管理安全性基礎結構，以保護您的遠端網路和行動使用者。Prisma Access 會在行動使用者安全性處理節點 (MU-SPN) 與遠端網路安全性處理節點 (RN-SPN) 之間、SPN 與服務連線企業存取節點 (SC-CAN) 之間，以及 SC-CAN 與資料中心之間對資料進行端到端加密。

- 服務基礎結構—Prisma Access 會使用內部服務基礎結構來保護您組織的網路。您為基礎結構提供子網路，並且 Prisma Access 會使用此子網路內的 IP 位址，在您的遠端網路位置與行動使用者之間建立網路基礎結構，以及建立與內部網路資源的服務連線（如果適用）。雲端內的內部通訊是使用動態路由建立的。

 ©2025 Palo Alto Networks, Inc.

- 服務連線—如果您的 Prisma Access 授權包含它，您可以選擇建立 IPSec 通道，以允許網路中的內部資源與行動使用者和遠端網路位置中的使用者進行通訊。例如，您可以建立連線來連線至組織總部或資料中心的驗證伺服器。

  即使您的總部或資料中心不需要服務連線，我們也建議您建立連線，以允許行動裝置使用者與遠端網路位置之間進行網路通訊，以及允許不同地理位置的行動裝置使用者進行網路通訊。
- 行動使用者—為您的行動使用者提供一致的安全性，無論他們是存取資料中心的應用程式、使用 SaaS 應用程式，還是瀏覽網際網路。您可以透過下列方式，使您的行動使用者能夠連線到 Prisma Access：
  - **GlobalProtect**

    您可以將 GlobalProtect 應用程式部署到您的使用者（適用於執行 Microsoft Windows、Apple macOS，以及 iOS、Android、Google Chrome OS 和 Linux 的智慧型手機、平板電腦或筆記型電腦），以便他們可以將流量透過通道傳輸至 Prisma Access，用於政策強制執行和威脅防護。GlobalProtect 應用程式還會提供主機資訊設定檔 (HIP) 報告，以便您可以根據裝置狀態建立細緻政策，以確保端點遵守您的安全標準—例如，它們配備了最新的修補程式、加密和病毒定義—以便存取您最敏感的應用程式。或者，若要啟用對未受管理裝置上使用者的安全存取，您可以啟用無用戶端 **VPN**。Prisma Access 根據您使用者目前所在的位置動態地縮減和擴增每個區域。
  - 明確 **Proxy**

    如果您組織的現有網路已使用明確 Proxy，並在您的用戶端端點上部署 PAC 檔案，則您可以順暢地移轉至 Prisma Access，以保護行動使用者的輸出網際網路流量。
- 遠端網路—使用遠端網路搭配雲端型的新世代防火牆來保護遠端網路位置（例如分支機構）及這些分支機構中的使用者。您可以使用靜態路由、使用 BGP 的動態路由或靜態和動態路由的組合，來允許存取每個遠端網路位置上的子網路。您上線的所有遠端網路位置都是完全互聯的。
- **ZTNA** 連接器—零信任網路存取 (ZTNA) 連接器可讓您簡單且安全地連線到您組織的私人應用程式。ZTNA 連接器會使用自動安全通道，為行動使用者和分支位置的使用者提供對您私人應用程式的存取，無需設定 IPSec 通道和路由定義，即可存取私人應用程式。ZTNA 連接器不需要來自客戶基礎結構的任何路由，並且可以提供對在您網路中使用重疊 IP 位址的應用程式的存取。
- **Strata Logging Service**—Prisma Access 會將所有日誌轉送到 Strata 記錄服務；作為啟動 Prisma Access 的一部分，您將指定要將 Prisma Access 日誌轉送至其中的 Strata Logging Service 執行個體。日誌流量不會使用您為 Prisma Access 購買的授權頻寬。

 ©2025 Palo Alto Networks, Inc.

# 使用 Prisma Access 保護網際網路流量

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access | ❑ Prisma Access 授權 |

## 網際網路安全性的重要性

保護網際網路存取從未如此重要且充滿挑戰。現有的舊版解決方案在偵測逃避性和針對性的網路釣魚及其他 Web 式攻擊方面苦苦掙扎，同時忽視了不安全的 DNS 流量所帶來的新威脅。Palo Alto Networks Prisma Access 擁有的網際網路安全性，其搭配業界首創採用 ML 技術的進階 URL 篩選和 DNS 安全性服務。使用 Prisma Access，您可以即時防止逃避性和針對性的網路釣魚及無檔案攻擊，並防範最新複雜的 DNS 型攻擊。

## Prisma Access 雲端安全 Web 閘道 (SWG)

安全 Web 閘道是當今數位環境中一個至關重要的元素，因為網路威脅的複雜性和頻率不斷上升。網路犯罪分子不斷設計新的戰術和技術來突破安全性防禦，其中一種方法是在看似合法的網站中偽裝惡意程式碼。當使用者存取這些遭入侵的網站時，他們不經意地洩露了憑證或使組織暴露於有害的程式碼中，如果不加以注意，這可能會造成嚴重後果。

在這樣一個充滿風險的環境中，缺乏穩固的安全性閘道會大幅地增加組織數位資產的風險。這種風險可能導致未經授權的存取、資料竊取 和業務營運中斷，特別是在廣泛的網路釣魚和勒索軟體攻擊日益盛行的情況下。若沒有 SWG 提供的安全性屏障，勒索軟體攻擊可能會有效地劫持組織，從而導致財務和聲譽損失。

加密流量的使用現在已經很普遍，而 HTTPS 構成了大多數的網路流量。如果一個組織缺乏可以有效解密和檢查此流量的 SWG，則它會面臨加密通道中隱藏安全性威脅的風險。

但是，使用多點產品進行 SWG、私人應用程式存取和 CASB 只會使事情變得複雜。將孤立的產品拼湊在一起作為一個供應項目，會導致功能上的差距和較差的安全性後果，使您容易受到攻擊。使用這些解決方案，您會獲得不一致的網際網路和私人應用程式安全性。

為了解決這些挑戰，Prisma Access 提供了統一的產品，涵蓋所有功能中所有使用者和應用程式的管理、政策和資料，包括 ZTNA、SWG、NG-CASB、FWaaS、DLP 等等。

客戶可以輕鬆地從舊版內部部署和雲端型 Proxy 解決方案移轉至 Prisma Access，以獲得對網際網路和 SaaS 應用程式流量的內嵌可視性和控制，搭配領先業界採用 AI 技術的安全性防護。

## 使用 Prisma Access 保護使用者和端點

Prisma Access 旨在防止成功的網路攻擊，因此它的作用不只是保護網路安全。若要阻止網路攻擊，必須檢查所有流量。如果不對所有流量進行全面檢查，任何措施都會導致嚴重的安全漏洞。Prisma Access 持續保護所有連接埠和所有應用程式上的所有流量，使您的組織能夠：

- 利用經過驗證的安全性理念和威脅情報來防止成功的網路攻擊，從而取得整個組織的深度可視性和精確控制。

 ©2025 Palo Alto Networks, Inc.

- 在所有連接埠上全面雙向檢查所有應用程式流量（包括 SSL 或 TLS 加密流量），無論是與網際網路、雲端還是分支進行通訊。
- 受益於來自 Palo Alto Networks 和數百個第三方來源的自動威脅資料所提供的全方位威脅情報。

仔細閱讀 Prisma Access 及其解決方案。

 ©2025 Palo Alto Networks, Inc.

# 如何管理 Prisma Access

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

有兩種您可以管理 Prisma Access 的方式，但在啟動 Prisma Access 授權之後，您無法在管理介面之間切換（但使用移轉工作流程從 Prisma Access (Managed by Panorama) 前往 Prisma Access (Managed by Strata Cloud Manager) 部署除外）。因此，開始前您必須確定要如何管理 Prisma Access：

- **Prisma Access (Managed by Strata Cloud Manager)**

  若要從雲端管理 Prisma Access，請使用 Strata Cloud Manager。使用雲端管理，您可以透過工作驅動的工作流程快速裝載分支和行動使用者，而這些工作流程可讓您在幾分鐘內設定並測試您的環境。雲端管理搭配 Strata Cloud Manager 透過根據最佳做法提供預先定義的網際網路

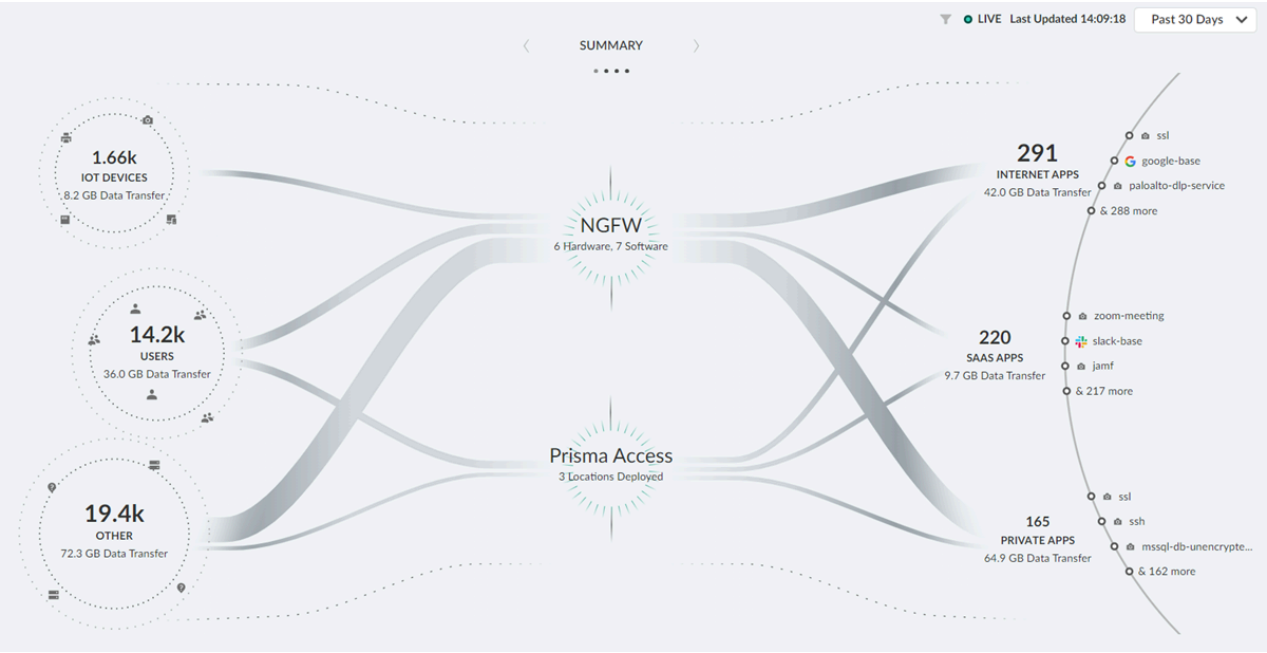

©2025 Palo Alto Networks, Inc.

存取和解密政策規則，簡化了裝載程序。使用適用於最常見支援 IPSec 裝置的預設值快速設定 IPSec 通道，並為建議的 URL 類別啟用 SSL 解密。

**Strata Cloud Manager** 控管中心

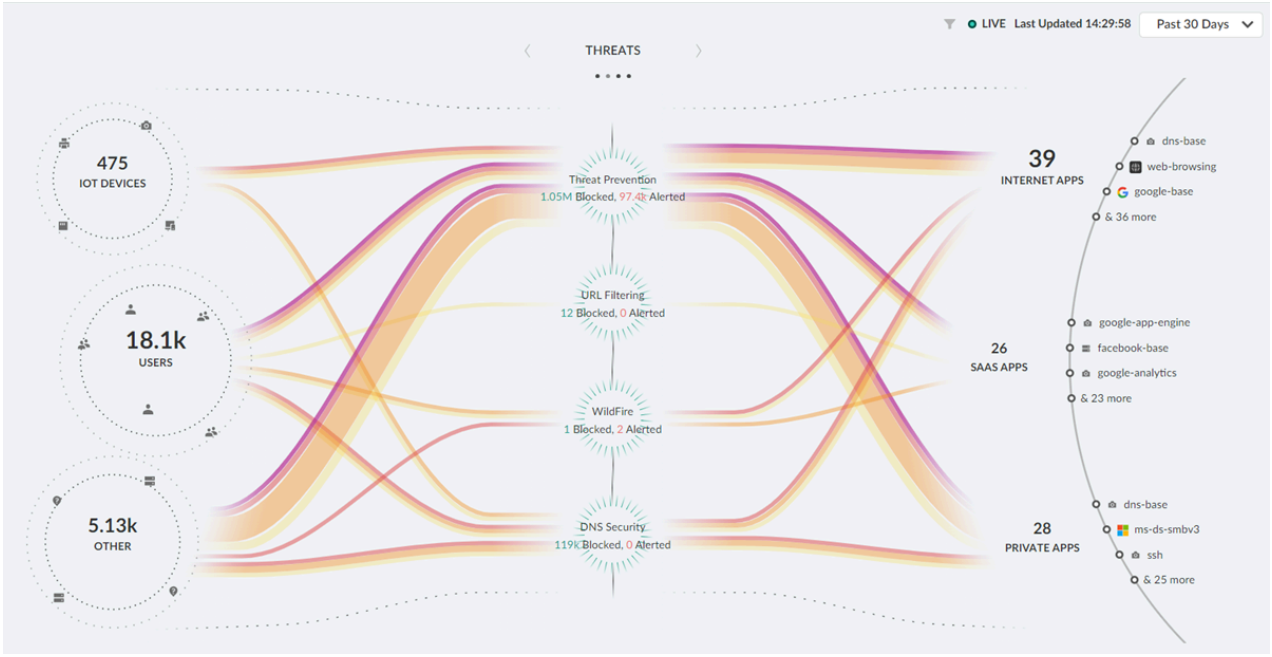
當您啟動 Strata Cloud Manager 時，Strata Cloud Manager 控管中心頁面就會出現。此控管中心可協助您評估網路的健康情況、更好的可視性和資料概要。控管中心具有不同的儀表板來檢視不同類型的報告。

- **Summary**（摘要）：在摘要儀表板中，您可以檢視不同類型的資料來源、平台基礎結構（如 NGFW 或 Prisma Access），資料可以透過其從各種資料來源流向網路中的不同應用程式。

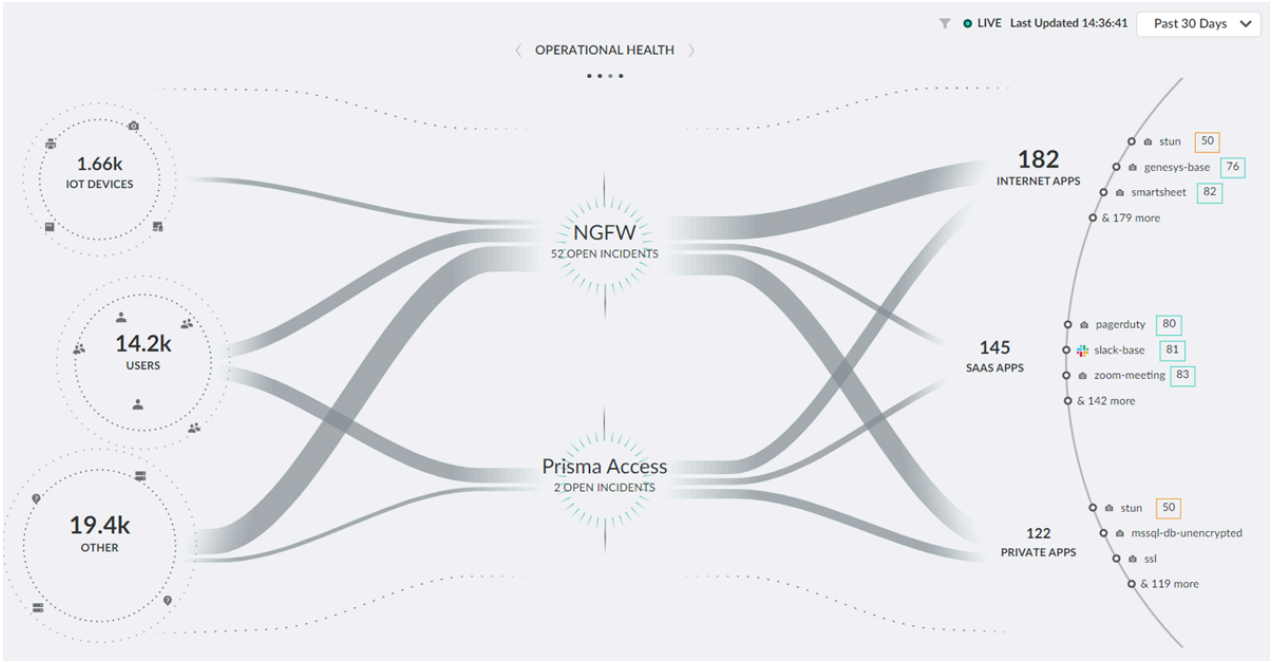



- **Threats**（威脅）：在威脅儀表板中，您可以檢視安全性應用程式偵測到的威脅。您可以使用此儀表板，監控網路上已封鎖和允許的威脅，或調查網路中可能具有低百分比檢查流量的區域。


©2025 Palo Alto Networks, Inc.




- **Operational Health**（操作健康情況）：顯示您的網路在受到 ADEM 監控時的健康情況和使用者體驗。您可以使用此檢視，監控網路上的使用者體驗並檢閱開放事件的嚴重性。




- **Data Security**（資料安全性）：顯示網路中已被 DLP 和 SaaS 安全性訂閱標記為具有敏感資料的流量。您可以使用此檢視，監控流經防火牆和已連線 SaaS 應用程式的資料，以及網路上任何資料風險的嚴重性。


©2025 Palo Alto Networks, Inc.




在儀表板中按一下這些類別中的任何一個以相應地篩選結果。

- **Prisma Access (Managed by Panorama)**

  在 Panorama 上使用雲端服務外掛程式設定和管理 Prisma Access。如果您已在使用 Panorama 管理新世代防火牆，並且有一個通用政策，您想要用於存取公司應用程式，則這是一個不錯的選擇。

即使您使用 *Panorama* 管理 *Prisma Access*，仍然可以使用 *Strata Cloud Manager*，以取得許多 *Prisma Access* 可視性和監控功能。進一步瞭解。

在您確定要使用的管理選項之後，請遵循您所選取選項的授權和啟動工作流程開始：

- 若要開始使用 Prisma Access (Managed by Panorama) Access，請從客戶支援入口網站 (CSP) 執行授權啟動，並在 Panorama 上安裝雲端服務外掛程式。
- 若要開始使用 Cloud Managed Prisma Access，請從中樞執行授權啟動。

***Panorama*** 與雲端管理之間的功能同位檢查

*Prisma Access (Managed by Panorama) Access* 和 *Prisma Access (Managed by Strata Cloud Manager)* 支援的功能有一些差異。如需 *Prisma Access (Managed by Panorama)* 和 *Prisma Access (Managed by Strata Cloud Manager)* 中的功能支援清單，請參閱相容性矩陣.


©2025 Palo Alto Networks, Inc.

# 搭配 Strata Cloud Manager 的 Prisma Access 可視性與監控

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access（Panorama 管理） | • Prisma Access 授權 |

有兩種方式，您可以從中選擇來管理 Prisma Access：

- 對於 Prisma Access (Managed by Strata Cloud Manager)，您可以使用 **Strata Cloud Manager**
- 或者，您可以使用 **Panorama** 來管理 Prisma Access

這兩個管理介面是您為 Prisma Access 環境處理裝載、設定和安全性政策強制執行的方式。不過，Prisma Access 還為您的 Prisma Access 環境包括強大的可視性和監控功能，而這些功能是在 Strata Cloud Manager 上提供的。

重要的是：

無論您為 Prisma Access 使用哪種管理介面（Strata Cloud Manager 或 Panorama），您都可以為許多 Prisma Access 可視性功能使用 Strata Cloud Manager，並可與採用 AI 技術的自發 DEM 等附加訂閱進行互動。

| Strata Cloud Manager 上的 Prisma Access 可視性與監控功能 | |
| --- | --- |
| 自主 DEM | 為安全存取服務邊緣 (SASE) 環境中的所有使用者流量提供原生端對端可視性和洞察。ADEM 功能原生整合到 GlobalProtect 應用程式和 Prisma Access，因此不需要您部署任何額外的設備或代理程式。您可以快速隔離數位體驗問題的根源，並簡化修復過程。<br><br>此功能需要自發 DEM 附加授權，才能與 *Prisma Access (Managed by Panorama) Access* 搭配使用。 |
| Strata Cloud Manager 中的儀表板和報告 | Strata Cloud Manager 中的可視性功能可識別關鍵結果，您可以使用這些結果，來通知您的政策更新並關上企業安全性與使用者生產力缺口。<br>• 互動式儀表板<br>探索網路中正在運作的應用程式、威脅、使用者、安全性訂閱的資料<br>• 報告<br>許多儀表板支援報告，您可以在其中離線分享資料並排程定期更新 |


©2025 Palo Alto Networks, Inc.

| Strata Cloud Manager 上的 Prisma Access 可視性與監控功能 | |
|---|---|
| Strata Cloud Manager 控管中心 | 控管中心是 IoT 裝置、使用者、主機，以及您網路上流量的互動式視覺化摘要。利用來自雲端交付安全性和 ADEM 訂閱的資料，控管中心可以公開有關網路上資料的威脅、使用者體驗和安全性的重要資訊。<br>控管中心可讓您與資料互動並視覺化網路事件之間的關係，以發現異常狀況或增強網路安全性的方法。 |


©2025 Palo Alto Networks, Inc.

# Prisma Access 個位置

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

您可以在您選擇的位置根據資料位置偏好設定和使用者最多的位置來部署 Prisma Access。Prisma Access 在全球提供 100 多個位置，以便您的使用者獲得針對其所在位置量身打造的體驗。所有 Prisma Access 位置都是根據最佳化的效能和延遲對應到安全性計算位置。這意味著某些國家/地區的流量將導向到該定義的計算位置。

如果您需要將計算位置限制在特定國家/地區，請參閱顯示處理 *Prisma Access* 及其相關聯服務所在國家/地區的表格。

有不同的 Prisma Access 位置類型：

- 依計算位置排序的位置—設定遠端網路時，您可以依計算位置配置頻寬。至少兩個（通常更多）地理位置上彼此接近的 Prisma Access 位置會依計算位置構成一個群組。這是您配置頻寬的層級，而不是為個別 Prisma Access 位置或特定遠端網站配置頻寬，並允許 Prisma Access 根據負載或需求動態地將頻寬配置給計算位置中的網站。
- 劇院和位置群組—在行動使用者—GlobalProtect 部署中配置 IP 位址集區時，您可以依位置群組（小於劇院的位置群組）、劇院或全球指定 IP 集區。如果您有服務依賴使用者的來源 IP 位址來識別使用者的詳細資訊（例如位置型服務或基於使用者群組或功能的服務），請使用位置群組特定的 IP 位址集區，以便您可以套用存取控制政策，或在不同國家/地區執行路由或政策操作（如果這些國家/地區位於不同的計算區域）。
- 依區域劃分的位置—每個 Prisma Access 位置都有相關聯的區域。
- 明確 **Proxy** 位置—明確 Proxy 有自己的一組位置，這是 Prisma Access 位置的子集。
- **Colo-Connect** 位置—Colo-Connect 有自己的一組位置，這是 Prisma Access 位置的子集。
- **Strata** 記錄服務區域—Prisma Access 支援 Strata 記錄服務區域的子集。
- 遠端網路—高效能、流量複寫和安全輸入存取位置—高效能遠端網路、流量複寫和安全輸入存取部署使用 Prisma Access 位置的子集。
- **Prisma Access** 中國位置—Prisma Access 中國部署使用中國大陸的位置。
- **FedRAMP** 中位置和高位置—Prisma AccessFedRAMP 中部署和高部署使用 Prisma Access 位置的子集。
- 北美位置地圖—為了協助您選取北美的位置，請參閱此地圖，其中顯示了北美位置的地理覆蓋範圍。

 ©2025 Palo Alto Networks, Inc.

- 本機區域#本機區域將計算、儲存、資料庫和其他服務放置在靠近大量人口和工業中心的地方。這些位置有自己的計算位置。

  若要新增本機區域，請聯繫您的 *Palo Alto Networks* 代表。

  部署本機區域時請記住以下指導方針：

  - 本機區域位置不支援 IPv6。
  - 本機區域位置不使用 Palo Alto Networks 註冊的 IP 位址。
  - 不支援遠端網路的 1 Gbps 支援。
  - 如果您在同一本機區域中部署跨可用性區域的遠端網路和服務連線節點備援，則此備援無法使用，因為這兩個節點都是在單一區域中佈建的。
  - 這些本機區域不使用 Palo Alto Networks 註冊的 IP。如果您在存取 URL 時遇到問題，請使用 https://reportasite.gpcloudservice.com/報告網站問題 或聯繫 Palo Alto Networks 支援。

檢閱 Prisma Access 隱私權資料表，以進一步瞭解 *Prisma Access* 位置和 *Prisma Access* 處理流量所在。

## 計算位置、城市和國家/地區

每個計算位置中列出的第一個位置（以粗體顯示）顯示計算位置的城市和國家/地區。

以兩個星號 (**) 表示的位置是本機區域，這些區域不支援所有 Prisma Access 功能。

| 計算位置 | Prisma Access 位置 | 城市與國家/地區 |
|---|---|---|
| 東北亞 | 日本中部 | 日本，東京 |
| 南亞 | 印度西部<br>孟加拉國<br>印度南部<br>巴基斯坦南部<br>巴基斯坦西部 | 印度，孟買<br>孟加拉，達卡<br>印度，清奈<br>巴基斯坦，卡拉奇<br>巴基斯坦，拉合爾 |
| 東南亞（印尼） | 印尼 | 印尼，雅加達 |
| 東南亞（新加坡） | 新加坡<br>柬埔寨<br>馬來西亞<br>緬甸<br>巴基斯坦西部 (II)<br>菲律賓 | 新加坡<br>柬埔寨，金邊<br>馬來西亞，吉隆坡<br>緬甸，仰光<br>巴基斯坦，伊斯蘭堡<br>菲律賓，奎松市 |


©2025 Palo Alto Networks, Inc.

| 計算位置 | Prisma Access 位置 | 城市與國家/地區 |
|---|---|---|
| | 斯里蘭卡 | 斯里蘭卡，科倫坡 |
| | 泰國 | 泰國，曼谷 |
| | 越南 | 越南，胡志明市 |
| 澳大利亞南部 | 澳大利亞南部 | 澳大利亞，墨爾本 |
| 澳大利亞東南部 | 澳大利亞東南部 | 澳大利亞，雪梨 |
| | 澳大利亞東部 | 澳大利亞，布里斯班 |
| | 紐西蘭 | 紐西蘭，奧克蘭 |
| | 巴布亞紐幾內亞 | 巴布亞紐幾內亞，莫爾茲比港 |
| 澳大利亞西部（珀斯）** | 澳大利亞西部（珀斯）** | 澳大利亞，珀斯 |
| 巴林 | 巴林 | 巴林，麥納麥 |
| 比利時 | 比利時 | 比利時，聖吉斯蘭 |
| | 拉托維亞 | 拉脫維亞，里加 |
| | 塞內加爾 | 塞內加爾，達喀爾 |
| 加拿大中部（蒙特婁） | 加拿大東部 | 加拿大，魁北克省 |
| 加拿大中部（多倫多） | 加拿大中部 | 加拿大，多倫多 |
| 加拿大西部（卡加利） | 加拿大西部 | 加拿大，卡加利 |
| 歐洲中部 | 德國中部 | 德國，法蘭克福 |
| | 奧地利 | 奧地利，維也納 |
| | 保加利亞 | 保加利亞，索菲亞 |
| | 克羅埃西亞 | 克羅埃西亞，薩格勒布 |
| | 捷克共和國 | 捷克共和國，布拉格 |
| | 埃及 | 埃及，開羅 |
| | 德國北部 | 德國，漢堡 |
| | 德國南部 | 德國，慕尼黑 |
| | 希臘 | 希臘，雅典 |
| | 匈牙利 | 匈牙利，布達佩斯 |
| | 科威特 | 科威特，艾哈邁迪 |
| | 列支敦斯登 | 列支敦斯登，沙恩 |


©2025 Palo Alto Networks, Inc.

| 計算位置 | Prisma Access 位置 | 城市與國家/地區 |
|---|---|---|
| | 盧森堡 | 盧森堡，盧森堡市 |
| | 摩爾多瓦 | 摩爾多瓦，基希訥烏 |
| | 奈及利亞 | 奈及利亞，拉各斯 |
| | 羅馬尼亞 | 羅馬尼亞布，加勒斯特 |
| | 斯洛伐克 | 斯洛伐克布，拉迪斯拉發 |
| | 斯洛維尼亞 | 斯洛維尼亞，盧布爾雅那 |
| | 土耳其 | 土耳其，伊斯坦堡 |
| | 烏克蘭 | 烏克蘭，基輔 |
| | 烏茲別克 | 烏茲別克，塔什幹 |
| 歐洲中部（華沙） | 波蘭 | 波蘭，華沙 |
| 歐洲北部 | 芬蘭 | 芬蘭，哈米納 |
| | 白俄羅斯 | 白俄羅斯，明斯克 |
| | 哈薩克 | 哈薩克，阿斯塔納 |
| | 立陶宛 | 立陶宛，維爾紐斯 |
| | 挪威 | 挪威，奧斯陸 |
| | 俄羅斯中部 | 俄羅斯，莫斯科 |
| | 俄羅斯西北部 | 俄羅斯，聖彼得堡 |
| 歐洲北部（斯德哥爾摩） | 瑞典 | 瑞典，斯德哥爾摩 |
| 歐洲西北部 | 英國 | 英國，倫敦 |
| | 迦納 | 加納，阿克拉 |
| 歐洲西北部（巴黎） | 法國南部 | 法國，巴黎 |
| 歐洲南部 | 義大利 | 義大利，米蘭 |
| | 約旦 | 約旦，安曼 |
| | 肯亞 | 肯亞，蒙巴薩 |
| | 摩納哥 | 摩納哥 |
| 歐洲西南部 | 西班牙中部 | 西班牙，馬德里 |
| | 安道爾 | 安道爾，安道爾城 |
| | 葡萄牙 | 葡萄牙，里斯本 |
| | 西班牙東部 | 西班牙，巴塞隆納 |


©2025 Palo Alto Networks, Inc.

| 計算位置 | Prisma Access 位置 | 城市與國家/地區 |
|---|---|---|
| 歐洲西部 | 荷蘭中部<br>丹麥<br>荷蘭南部 | 荷蘭，埃姆斯哈文<br>丹麥，哥本哈根<br>荷蘭，鹿特丹 |
| 法國北部 | 法國北部 | 法國，巴黎 |
| 香港 | 香港 | 中國，香港 |
| 印度北部 | 印度北部 | 印度，新德里 |
| 愛爾蘭 | 愛爾蘭 | 愛爾蘭，都柏林 |
| 日本南部 | 日本南部 | 日本，大阪 |
| 中東中部（卡達） | 卡達 | 卡達，多哈 |
| 中東中部（沙烏地阿拉伯） | 沙烏地阿拉伯 | 沙烏地阿拉伯，利雅得 |
| 中東中部（UAE） | 阿拉伯聯合大陸 | 阿拉伯聯合大公國，杜拜 |
| 中東西部 | 以色列 | 以色列，特拉維夫 |
| 奈及利亞（拉各斯）** | 奈及利亞（拉各斯）** | 奈及利亞，拉各斯 |
| 紐西蘭（奧克蘭）** | 紐西蘭（奧克蘭）** | 紐西蘭，奧克蘭 |
| 南非中部 | 南非中部 | 南非，約翰尼斯堡 |
| 南非西部 | 南非西部 | 南非，開普敦 |
| 南美洲東部 | 巴西南部<br>巴西中部<br>巴西東部<br>巴拉圭<br>委內瑞拉 | 巴西，聖保羅<br>巴西，巴西利亞<br>巴西，里約熱內盧<br>巴拉圭，亞松森<br>委內瑞拉，加拉加斯 |
| 南美洲西部 | 智利<br>阿根廷<br>玻利維亞<br>秘魯<br>烏拉圭 | 智利，聖地牙哥<br>阿根廷，布宜諾斯艾利斯<br>玻利維亞，聖克魯斯德拉謝拉<br>秘魯，利馬<br>烏拉圭，蒙得維的亞 |


©2025 Palo Alto Networks, Inc.

| 計算位置 | Prisma Access 位置 | 城市與國家/地區 |
|---|---|---|
| 南美西部（利馬）** | 南美西部（利馬）** | 秘魯，利馬 |
| 韓國 | 韓國 | 韓國，首爾 |
| 瑞士 | 瑞士<br>烏干達 | 瑞士，蘇黎世<br>烏干達，坎帕拉 |
| 臺灣 | 臺灣 | 台灣，彰化 |
| 美國中部 | 美國中部 | 美國，康瑟爾布拉夫斯 |
| 美國中部（芝加哥）** | 美國中部（芝加哥）** | 美國，芝加哥 |
| 美國中西部 | 美國中西部 | 美國，鹽湖城 |
| 美國東部 | 美國東部<br>美國東北部<br>瓜地馬拉 | 美國，阿什本<br>美國，紐約市<br>瓜地馬拉，瓜地馬拉城 |
| 美國西北部 | 美國西北部 | 美國，達爾斯 |
| 美國南部 | 美國南部<br>墨西哥中部<br>墨西哥西部 | 美國，達拉斯<br>墨西哥，墨西哥城<br>墨西哥，瓜達拉哈拉 |
| 美國東南部 | 美國東南部<br>哥倫比亞<br>哥斯大黎加<br>厄瓜多<br>巴拿馬 | 美國，蒙克斯角<br>哥倫比亞，波哥大<br>哥斯大黎，加聖何塞<br>厄瓜多，瓜亞基爾<br>巴拿馬，巴拿馬城 |
| 美國東南部（邁阿密）** | 美國東南部（邁阿密）** | 美國，邁阿密 |
| 美國西南部 | 美國西南部<br>美國西部 | 美國，洛杉磯<br>美國，舊金山 |


©2025 Palo Alto Networks, Inc.

# 劇場和位置群組

| 劇院/位置群組 | IP 集區群組 ID |
|---|---|
| 哥倫比亞<br>哥斯大黎加<br>厄瓜多<br>瓜地馬拉<br>墨西哥中部<br>巴拿馬<br>美國東部<br>美國東南部<br>美國中部<br>哥斯大黎加<br>美國中北部<br>美國東北部<br>美國南部<br>美國東南部<br>委內瑞拉 | 1 |
| 加拿大東部<br>加拿大中部 | 2 |
| 愛爾蘭 | 3 |
| 法國南部<br>迦納<br>英國 | 4 |
| 法國北部 | 5 |
| 亞洲、澳洲和日本 | 6 |
| 安道爾<br>奧地利<br>保加利亞<br>克羅埃西亞 | 7 |


©2025 Palo Alto Networks, Inc.

| 劇院/位置群組 | IP 集區群組 ID |
| --- | --- |
| 捷克共和國 | |
| 埃及 | |
| 德國中部 | |
| 德國北部 | |
| 德國南部 | |
| 希臘 | |
| 匈牙利 | |
| 以色列 | |
| 義大利 | |
| 約旦 | |
| 肯亞 | |
| 科威特 | |
| 列支敦斯登 | |
| 盧森堡 | |
| 摩爾多瓦 | |
| 摩納哥 | |
| 奈及利亞 | |
| 波蘭 | |
| 葡萄牙 | |
| 羅馬尼亞 | |
| 斯洛伐克 | |
| 斯洛維尼亞 | |
| 沙烏地阿拉伯 | |
| 南非中部 | |
| 西班牙中部 | |
| 西班牙東部 | |
| 土耳其 | |
| 烏克蘭 | |
| 阿拉伯聯合大陸 | |
| 烏茲別克 | |
| 白俄羅斯 | 8 |


©2025 Palo Alto Networks, Inc.

| 劇院/位置群組 | IP 集區群組 ID |
| --- | --- |
| 芬蘭<br>哈薩克<br>立陶宛<br>挪威<br>俄羅斯中部<br>俄羅斯西北部<br>瑞典 | |
| 丹麥<br>荷蘭中部<br>荷蘭南部 | 9 |
| 非洲、歐洲和中東 | 10 |
| 瑞士<br>烏干達 | 11 |
| 比利時<br>拉托維亞<br>塞內加爾 | 12 |
| 巴西中部<br>巴西東部<br>巴西南部<br>巴拉圭<br>委內瑞拉 | 13 |
| 澳大利亞東部<br>澳大利亞南部<br>澳大利亞東南部<br>紐西蘭<br>巴布亞紐幾內亞 | 14 |
| 柬埔寨<br>印尼<br>馬來西亞 | 15 |


©2025 Palo Alto Networks, Inc.

| 劇院/位置群組 | IP 集區群組 ID |
| --- | --- |
| 緬甸<br>菲律賓<br>新加坡<br>泰國<br>越南 | |
| 香港 | 16 |
| 臺灣 | 17 |
| 韓國 | 18 |
| 孟加拉國<br>印度北部<br>印度南部<br>印度西部<br>巴基斯坦西部<br>巴基斯坦南部<br>卡達 | 19 |
| 南非西部<br>瑞典<br>南非西部 | 20 |
| 日本中部<br>日本南部 | 21 |
| 巴林 | 22 |
| 加拿大西部<br>墨西哥中部<br>墨西哥西部<br>美國中西部<br>美國西北部<br>美國西南部<br>美國西部 | 23 |


©2025 Palo Alto Networks, Inc.

| 劇院/位置群組 | IP 集區群組 ID |
| --- | --- |
| 阿根廷<br>玻利維亞<br>智利<br>秘魯<br>烏拉圭 | 24 |

## 依地區劃分的位置

| 位置 |
| --- |
| 非洲地區 |
| 肯亞 |
| 奈及利亞 |
| 塞內加爾 |
| 南非中部 |
| 南非西部 |
| 亞洲地區 |
| 孟加拉國 |
| 柬埔寨 |
| 香港 |
| 印度北部 |
| 印度南部 |
| 印度西部 |
| 印尼 |
| 哈薩克 |
| 馬來西亞 |
| 緬甸 |


©2025 Palo Alto Networks, Inc.

| 位置 |
| --- |
| 巴基斯坦南部 |
| 巴基斯坦西部 |
| 巴基斯坦西部 (II) |
| 巴布亞紐幾內亞 |
| 菲律賓 |
| 新加坡 |
| 韓國 |
| 斯里蘭卡 |
| 臺灣 |
| 泰國 |
| 越南 |
| **ANZ** 地區 |
| 澳大利亞東部 |
| 澳大利亞南部 |
| 澳大利亞東南部 |
| 紐西蘭 |
| 歐洲地區 |
| 安道爾 |
| 奧地利 |
| 白俄羅斯 |
| 比利時 |
| 保加利亞 |
| 克羅埃西亞 |
| 捷克共和國 |


©2025 Palo Alto Networks, Inc.

| 位置 |
| --- |
| 丹麥 |
| 芬蘭 |
| 法國北部 |
| 法國南部 |
| 德國中部 |
| 德國北部 |
| 德國南部 |
| 迦納 |
| 希臘 |
| 匈牙利 |
| 愛爾蘭 |
| 義大利 |
| 拉托維亞 |
| 列支敦斯登 |
| 立陶宛 |
| 盧森堡 |
| 摩爾多瓦 |
| 摩納哥 |
| 荷蘭中部 |
| 荷蘭南部 |
| 挪威 |
| 波蘭 |
| 葡萄牙 |
| 羅馬尼亞 |

 ©2025 Palo Alto Networks, Inc.

| 位置 |
| --- |
| 俄羅斯中部 |
| 俄羅斯西北部 |
| 斯洛伐克 |
| 斯洛維尼亞 |
| 西班牙中部 |
| 西班牙東部 |
| 瑞典 |
| 瑞士 |
| 烏干達 |
| 英國 |
| 烏克蘭 |
| 烏茲別克 |
| 日本地區 |
| 日本中部 |
| 日本南部 |
| 中東地區 |
| 巴林 |
| 埃及 |
| 以色列 |
| 約旦 |
| 科威特 |
| 卡達 |
| 沙烏地阿拉伯 |
| 土耳其 |


©2025 Palo Alto Networks, Inc.

| 位置 |
| --- |
| 阿拉伯聯合大陸 |
| 北美地區 |
| 加拿大中部 |
| 加拿大東部 |
| 加拿大西部 |
| 哥斯大黎加 |
| 墨西哥中部 |
| 墨西哥西部 |
| 巴拿馬 |
| 美國中部 |
| 美國中西部 |
| 美國東部 |
| 美國東北部 |
| 美國西北部 |
| 美國南部 |
| 美國東南部 |
| 美國西南部 |
| 美國西部 |
| 南美洲地區 |
| 阿根廷 |
| 玻利維亞 |
| 巴西中部 |
| 巴西東部 |
| 巴西南部 |


©2025 Palo Alto Networks, Inc.

| 位置 |
| --- |
| 智利 |
| 哥倫比亞 |
| 厄瓜多 |
| 巴拉圭 |
| 秘魯 |
| 烏拉圭 |
| 委內瑞拉 |

## 明確 Proxy 位置

Prisma Access 支援明確 Proxy 的以下位置。明確 Proxy 使用 GeoDNS 解析行動使用者，並將其連線到最近的 Prisma Access 部署位置。

- 非洲、歐洲和中東：
  - 比利時
  - 芬蘭
  - 法國南部
  - 德國中部
  - 以色列
  - 義大利
  - 荷蘭中部
  - 波蘭
  - 卡達
  - 沙烏地阿拉伯
  - 南非中部
  - 西班牙中部
  - 瑞士
  - 英國

 ©2025 Palo Alto Networks, Inc.

- 亞洲、澳洲和日本：
  - 澳大利亞南部
  - 澳大利亞東南部
  - 中國
  - 香港
  - 日本中部
  - 日本南部
  - 印度北部
  - 印度西部
  - 印尼
  - 新加坡
  - 韓國
  - 臺灣
- 北美洲和南美洲：
  - 巴西南部
  - 智利
  - 加拿大中部
  - 加拿大東部
  - 美國中部
  - 美國東部
  - 美國西北部
  - 美國南部
  - 美國東南部
  - 美國西南部
  - 美國中西部

## Colo-Connect 位置

Prisma Access Colo-Connect 支援以下 Prisma Access 位置。當您建立服務連線以支援 Colo-Connect 時，請確保僅在下列位置建立它們。

對於專用互連連結，請使用您可以在其中建立專用互連連線的 GCP 位置清單。

- 澳大利亞南部
- 澳大利亞東南部
- 比利時
- 巴西南部


©2025 Palo Alto Networks, Inc.

- 加拿大中部
- 加拿大東部
- 智利
- 芬蘭
- 法國南部
- 德國中部
- 香港
- 印度北部
- 印度西部
- 印尼
- 義大利
- 日本中部
- 日本南部
- 荷蘭中部
- 卡達
- 沙烏地阿拉伯
- 新加坡
- 南非中部
- 西班牙中部
- 瑞士
- 臺灣
- 英國
- 美國中部
- 美國中西部
- 美國東部
- 美國西北部
- 美國南部
- 美國東南部
- 美國西南部

## 支援的 Strata Logging Service 地區

Prisma Access 支援以下 Strata 記錄服務地區：

- 澳大利亞
- 加拿大
- 法國


©2025 Palo Alto Networks, Inc.

- 德國
- 日本
- 印度
- 印尼
- 以色列
- 荷蘭—歐洲
- 卡達
- 沙烏地阿拉伯
- 新加坡
- 瑞士
- 臺灣
- 英國
- 美國—美洲

## 遠端網路—高效能、流量複寫和安全輸入存取位置

Prisma Access 支援以下高效能遠端網路位置：

- 安道爾
- 阿根廷
- 澳大利亞東部
- 澳大利亞南部
- 澳大利亞東南部
- 奧地利
- 孟加拉國
- 白俄羅斯
- 比利時
- 玻利維亞
- 巴西中部
- 巴西東部
- 巴西南部
- 保加利亞
- 柬埔寨
- 加拿大中部
- 加拿大東部
- 智利
- 哥倫比亞

 ©2025 Palo Alto Networks, Inc.

- 哥斯大黎加
- 克羅埃西亞
- 捷克共和國
- 丹麥
- 厄瓜多
- 埃及
- 芬蘭
- 法國北部
- 法國南部
- 德國中部
- 德國北部
- 德國南部
- 迦納
- 希臘
- 瓜地馬拉
- 香港
- 匈牙利
- 印度北部
- 印度南部
- 印度西部
- 印尼
- 以色列
- 義大利
- 日本中部
- 日本南部
- 約旦
- 哈薩克
- 肯亞
- 科威特
- 拉托維亞
- 列支敦斯登
- 立陶宛
- 盧森堡
- 馬來西亞
- 墨西哥中部

 ©2025 Palo Alto Networks, Inc.

- 墨西哥西部
- 摩爾多瓦
- 摩納哥
- 緬甸
- 荷蘭中部
- 荷蘭南部
- 紐西蘭
- 奈及利亞
- 挪威
- 巴基斯坦南部
- 巴基斯坦西部
- 巴基斯坦西部 (II)
- 巴拿馬
- 巴布亞紐幾內亞
- 巴拉圭
- 秘魯
- 菲律賓
- 波蘭
- 葡萄牙
- 卡達
- 羅馬尼亞
- 俄羅斯中部
- 俄羅斯西北部
- 沙烏地阿拉伯
- 塞內加爾
- 新加坡
- 斯洛伐克
- 斯洛維尼亞
- 南非中部
- 韓國
- 西班牙中部
- 西班牙東部
- 斯里蘭卡
- 瑞士
- 臺灣

 ©2025 Palo Alto Networks, Inc.

- 泰國
- 土耳其
- 烏干達
- 英國
- 烏克蘭
- 烏拉圭
- 美國中部
- 美國中西部
- 美國東部
- 美國東北部
- 美國西北部
- 美國南部
- 美國東南部
- 美國西南部
- 美國西部
- 烏茲別克
- 委內瑞拉
- 越南

## Prisma Access 中國位置

Prisma Access 中國支援中國大陸以下位置：

- 中國北部—北京（使用中國北部計算位置）
- 中國西北部—寧夏（使用中國西北部計算位置）

## FedRAMP 中位置和高位置

在 Prisma SASE FedRAMP 文件中尋找 FedRAMP 位置清單。

## 北美位置地圖

請使用以下地圖作為參考，以在北美洲中選取 Prisma Access 位置時協助您。


©2025 Palo Alto Networks, Inc.




# 本機區域位置

Prisma Access 中的 IPv4 支援以下本機區域：

- 您需要與 *Palo Alto Networks* 代表合作，提出在以下其中一個本機區域進行部署的要求。
- 不支援 *IPv6*。

- 澳洲西部（珀斯）
- 紐西蘭（奧克蘭）
- 奈及利亞（拉各斯）
- 南美洲西（利馬）
- 美國中部（芝加哥）
- 美國東南部（邁阿密）


©2025 Palo Alto Networks, Inc.

# Prisma Access 和相關聯的服務處理位置

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

Prisma Access 在全球 100 多個位置提供本機體驗，並根據最佳化的效能和延遲將每個位置對應到安全性計算位置。

如果您需要將計算位置限制為特定國家/地區，請參閱每個 Prisma Access 位置的國家/地區對應，並僅在 Prisma Access 設定期間部署與這些國家/地區相關聯的這些位置。

下表為您提供了 Strata 記錄服務區域、Strata Cloud Manager（適用於 Prisma Access (Managed by Strata Cloud Manager)）、Prisma Access 洞察、自發 DEM 和 SaaS 安全性內嵌的國家/地區處理位置。

| Strata Logging Service | Strata Cloud Manager 設定 | Prisma Access Insights 資料 | Autonomous DEM | SaaS Security Inline |
| --- | --- | --- | --- | --- |
| 英國 | 英國 | 英國 | 英國 | 英國 |
| 荷蘭 | 德國 | 荷蘭 | 荷蘭 | 德國（歐盟） |
| 德國 | 德國 | 德國 | 德國 | 德國（歐盟） |
| 瑞士 | 瑞士 | 瑞士 | 瑞士 | 德國（歐盟） |
| 法國 | 德國 | 法國 | 法國 | 德國（歐盟） |
| 新加坡 | 新加坡 | 新加坡 | 新加坡 | 新加坡 |
| 印度 | 印度 | 印度 | 印度 | 印度 |
| 日本 | 日本 | 日本 | 日本 | 日本 |
| 加拿大 | 加拿大 | 加拿大 | 加拿大 | 美國 |
| 美國 | 美國 | 美國 | 美國 | 美國 |
| 澳大利亞 | 澳大利亞 | 澳大利亞 | 澳大利亞 | 澳大利亞 |
| 以色列 | 德國 | 以色列 | 以色列 | 德國（歐盟） |
| 卡達 | 卡達 | 卡達 | 卡達 | 德國（歐盟） |
| 沙烏地阿拉伯 | 德國 | 沙烏地阿拉伯 | 沙烏地阿拉伯 | 德國（歐盟） |


©2025 Palo Alto Networks, Inc.

| Strata Logging Service | Strata Cloud Manager 設定 | Prisma Access Insights 資料 | Autonomous DEM | SaaS Security Inline |
|---|---|---|---|---|
| 臺灣 | 新加坡 | 臺灣 | 臺灣 | 新加坡 |
| 印尼 | 新加坡 | 印尼 | 印尼 | 新加坡 |


©2025 Palo Alto Networks, Inc.

# Prisma Access 基礎結構管理

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access（Panorama 管理） | ❑ Prisma Access 授權 |

Prisma Access 使用共用擁有權模型。Palo Alto Networks 管理基礎安全性基礎結構，確保其安全、具彈性、最新狀態，並在您需要時可供您使用。您組織的責任是裝載位置和使用者、推送政策、更新它們、查詢日誌和產生報告。

Palo Alto Networks 管理安全性基礎結構的以下部分。除了安全性基礎結構之外，Prisma Access 還可以管理版本和升級：

- **Prisma Access**
- **Strata Logging Service**—我們管理日誌的交付機制。
- 內容更新—我們管理版本和升級，包括 PAN-OS 更新。對於您的行動使用者，Prisma Access 託管多個版本的 GlobalProtect 應用程式，您可以從該清單中選取作用中的 GlobalProtect 應用程式版本。
- 容錯—我們管理服務的可用性。
- 自動調整—當您新增服務連線或遠端網路時，或當其他行動使用者登入單一區域中的一個或多個閘道時，我們會自動調整服務。
- 佈建—我們為基礎結構佈建所需的一切。
- 服務監控—我們監控服務狀態並保持其運作中。
- 計算位置對應—每個 Prisma Access 位置都會根據最佳化效能和延遲對應到安全性計算位置，這意味著，除非系統管理員另行修改，否則某些國家/地區中的流量將被導向到定義的計算位置。如需位置到計算位置對應，請參閱 Prisma Access 隱私權資料表。

您的組織會管理安全性基礎結構的下列元件。

- 使用者—您管理行動使用者的裝載。
- 驗證—您管理這些使用者的驗證。
- 行動裝置管理 **(MDM)**—您可以使用自己的 MDM 軟體，控制您組織透過 Prisma Access 保護的行動裝置。
- （僅限 Prisma Access (Managed by Panorama)）**Panorama** 和雲端服務外掛程式—您確定雲端服務外掛程式安裝所在的 Panorama 是正在執行支援雲端服務外掛程式的 Panorama 版本。此外，在我們通知您有新的外掛程式可用之後，您會在 Panorama 中升級雲端服務外掛程式。
- 政策建立和管理—您可以在 Panorama 中規劃並建立要與 Prisma Access 搭配使用的政策。
- 日誌分析與鑑識—Prisma Access 會提供日誌，您可以在其中使用我們或其他廠商提供的整合工具進行分析和報告。


©2025 Palo Alto Networks, Inc.

- 內部部署安全性—您在內部部署網路的微分段之間提供內部部署安全性。在某些部署中，您也可以導向所有流量，透過 Prisma Access 保護它們。
- 網路 —您提供 Prisma Access 的網路連線。
- 監控—您監控內部部署網路的狀態。
- 服務連線—您為行動使用者提供 Prisma Access 閘道的連線（例如，提供 ISP），並且還提供內部部署裝置，用作服務連線和遠端網路連線所使用的 IPsec 通道的端點。
- 裝載— 您裝載行動使用者、總部/資料中心網站和分支網站。
- （僅限 Prisma Access (Managed by Panorama)）備份—您管理 Panorama 設定的備份。

 ©2025 Palo Alto Networks, Inc.

# Prisma Access API

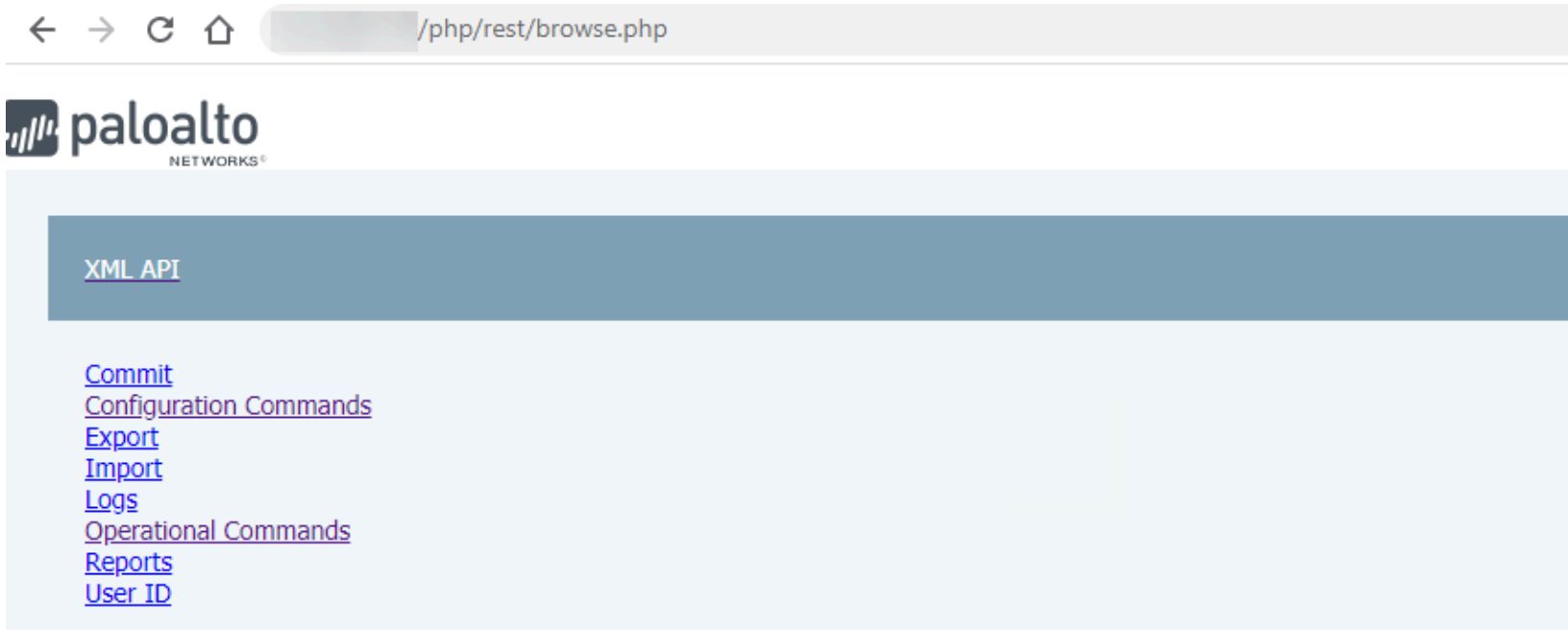
| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

## 適用於 Prisma Access (Managed by Strata Cloud Manager) 的 API

您可以在 pan.dev（這是 Palo Alto Networks 開發人員文件的網站）上找到 Prisma Access (Managed by Strata Cloud Manager) API 的詳細資訊。Prisma Access (Managed by Strata Cloud Manager) 會使用這些 API 進行服務裝載、設定和操作。

## 適用於 Prisma Access (Managed by Panorama) 的 API

除了 Panorama 中可用於設定和管理的 XML API 之外，還有適用於雲端服務外掛程式的 XML API，您可以使用它們來執行 Prisma Access 特定的工作。透過第三方服務、應用程式或指令碼使用這些 API，將 Prisma Access 的設定和報告工作自動化。




## 使用瀏覽器和網頁介面存取 Prisma Access (Managed by Panorama) API

若要使用瀏覽器存取 API，請使用管理員權限登入管理 Prisma Access 的 Panorama，然後在 URL 尾端輸入 /api。此 URL 會變更為 XML API 瀏覽器介面。

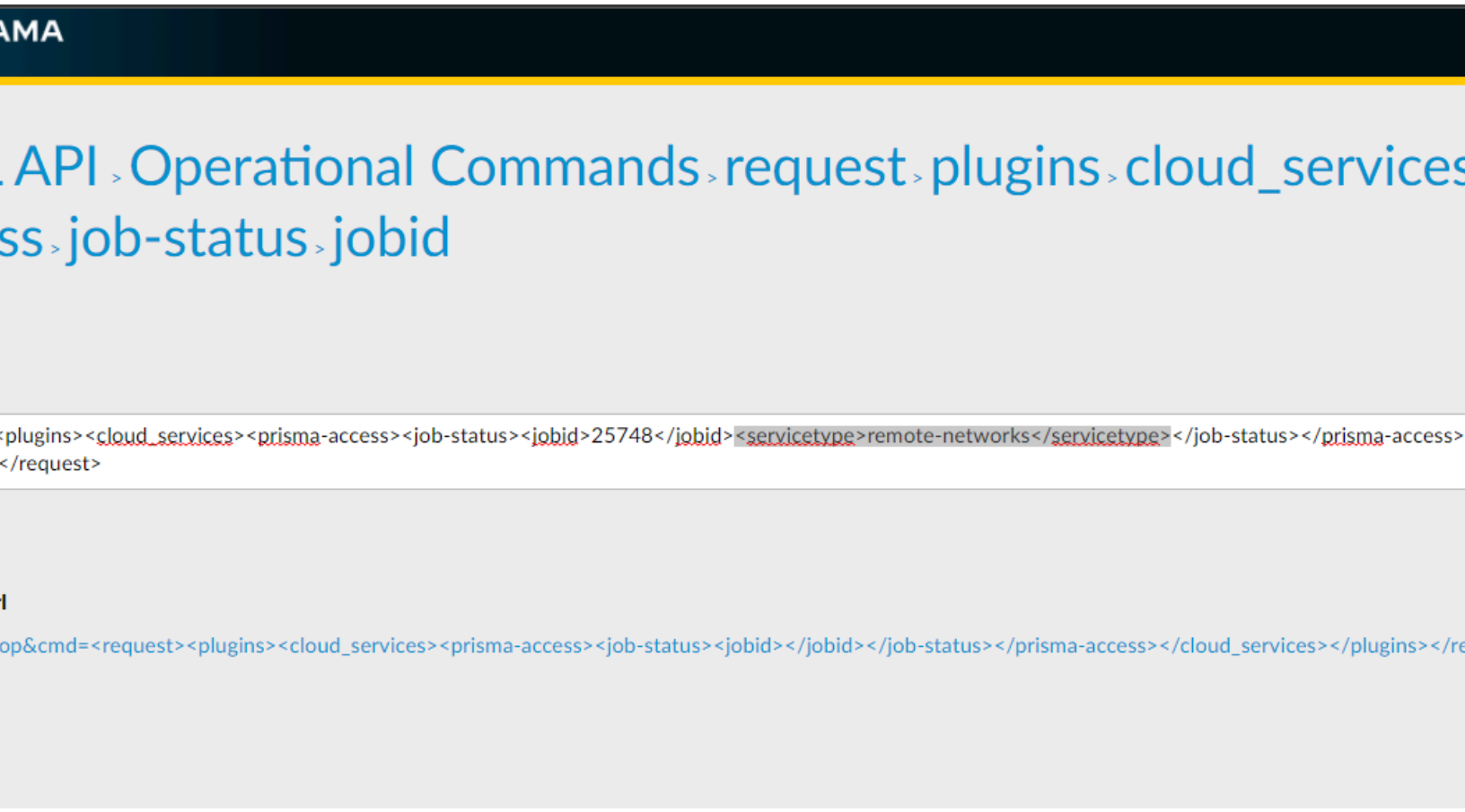
Prisma Access API 位於 XML 樹狀目錄中的下列 XML 路徑語言 (XPath) 節點：


©2025 Palo Alto Networks, Inc.

- 設定命令：**XML API** > **Configuration Commands**（設定命令） > **devices**（裝置） > **entry[@name='localhost.localdomain']** > **plugins**（外掛程式） > **cloud_services**
- 操作命令：**XML API** > **Operational Commands**（操作命令） > **request**（要求） > **plugins**（外掛程式） > **cloud_services** > **prisma-access**

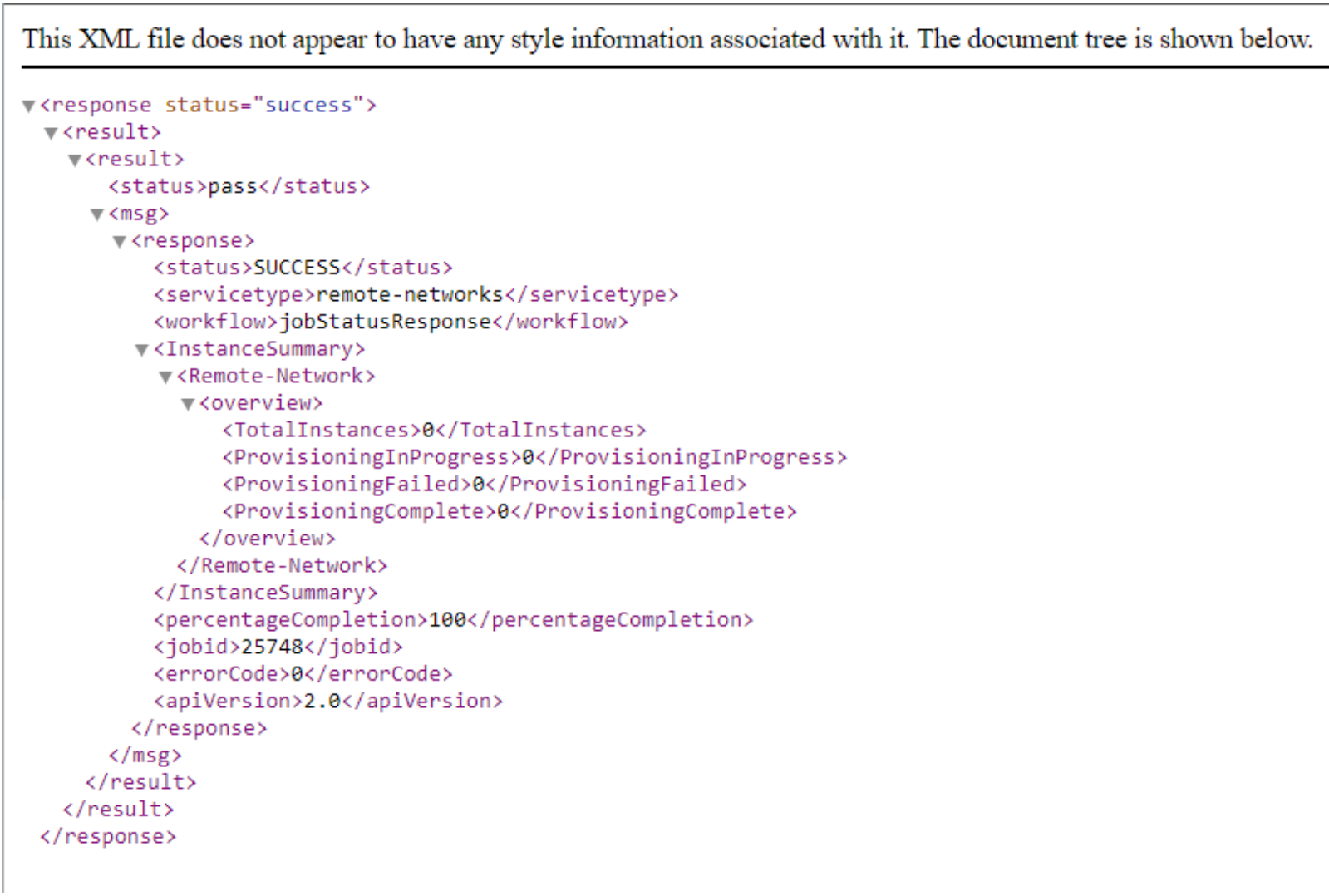
當您在 XML 樹狀目錄中導覽時，Prisma Access 會在 **XML** 區域中填入此樹狀目錄。您可以在 **XML** 區域中輸入所需的值，然後按一下 **Submit**（提交）來處理 XML 要求。例如，若要要求工作的裝載狀態，請導覽至 **XML API** > **Operational Commands**（操作命令） > **request**（要求） > **plugins**（外掛程式） > **cloud_services** > **prisma-access** > **job-status** > **jobid**、在 **jobid** 欄位中輸入工作 ID、輸入服務類型 **servicetype** 區域，然後按一下 **Submit**（提交）以提交您的要求。

此 *XML* 僅擷取工作的裝載狀態。若要擷取所有提交操作的狀態，請使用 *Prisma Access UI*。




Prisma Access 會以 XML 格式傳回輸出。

 ©2025 Palo Alto Networks, Inc.



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<response status="success">
  <result>
    <result>
      <status>pass</status>
      <msg>
        <response>
          <status>SUCCESS</status>
          <servicetype>remote-networks</servicetype>
          <workflow>jobStatusResponse</workflow>
          <InstanceSummary>
            <Remote-Network>
              <overview>
                <TotalInstances>0</TotalInstances>
                <ProvisioningInProgress>0</ProvisioningInProgress>
                <ProvisioningFailed>0</ProvisioningFailed>
                <ProvisioningComplete>0</ProvisioningComplete>
              </overview>
            </Remote-Network>
          </InstanceSummary>
          <percentageCompletion>100</percentageCompletion>
          <jobid>25748</jobid>
          <errorCode>0</errorCode>
          <apiVersion>2.0</apiVersion>
        </response>
      </msg>
    </result>
  </result>
</response>
```

您也可以使用網頁介面，在 Panorama 中尋找 API。

## 使用 curl 命令擷取 Panorama 受管理 API 命令

如果您偏好使用 CLI 擷取 API 命令結果，則可以使用 API 搭配您用來為 Prisma Access 擷取公用和基礎結構 IP 位址的 API。若要這樣做，請使用下列命令：

設定命令：

```
curl -k -X GET "https://<panorama-ip-address>/api/?key=<api-key>&type=config&cmd=<api-parameters></api-parameters>
```

操作命令：

```
curl -k -X GET "https://<panorama-ip-address>/api/?key=<api-key>&type=op&cmd=<api-parameters></api-parameters>
```

其中：

- *<panorama-ip-address>* 是管理 Prisma Access 的 Panorama 的 IP 位址。

 ©2025 Palo Alto Networks, Inc.

- *<api-key>* 是擷取 Prisma Access IP 位址的 API 金鑰（**Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定） > **Generate API Key**（產生 **API** 金鑰））。
- *<api-parameters>* 和 *</api-parameters>* 是您用來從 API 擷取要求資訊的 API 參數。

如果您有多租用戶部署，請將您要擷取其 API 資訊的租用戶名稱新增至 API。

例如，假設有一個 Prisma Access 部署具有以下參數：

- **Panorama IP** 位址：1.2.3.4
- **API** 金鑰：12345abcde
- 租用戶名稱：tenant-1

如果您想要擷取該租用戶的作用中行動使用者數目，請輸入以下 curl 命令：

```
curl -k -X GET "https://1.2.3.4/api/?
key=12345abcde&type=op&cmd=<request><plugins><cloud_services><prisma-
access><multi-tenant><tenant-name><entry%20name='tenant-1'></entry></
tenant-name><remote-active-users-count/></multi-tenant></prisma-
access></cloud_services></plugins></request>"
```

## 使用 CLI 命令搭配 Prisma Access (Managed by Panorama)

Prisma Access 允許您使用 CLI 命令來擷取 Prisma Access 資料。若要存取 CLI，請使用管理 Prisma Access 的 Panorama 的 IP 位址建立 SSH 連線。

CLI 使用相同的模式，並具有與 PAN-OS 命令相同的行為，但需要輸入租用戶名稱進行多租用戶部署；您可以使用 `tenant-name` *tenant-name* 命令輸入租用戶名稱。例如，假設租用戶名稱為 *tenant-1*，請輸入以下命令來擷取多租用戶部署中的作用中使用者計數：

```
admin-Panorama> request plugins cloud_services prisma-access multi-
tenant remote-active-users-count tenant-name tenant-1 pass Current
 User Count:253
```

## Prisma Access 洞察 API

Prisma Access 洞察 API 可讓您查詢 Prisma Access 洞察租用戶以取得資料資源。API 有兩個版本。Prisma Access 洞察 2.0 和 1.0 API 都可讓您查詢 Prisma Access 租用戶，以取得 Prisma Access 網路部署的健康情況。這兩個版本的 API 呼叫都相同；不過，每個版本都使用不同的存取權杖，並且您獲得存取權杖的機制，每個版本都不同。

若要開始使用 Prisma Access Insights API，請前往 歡迎使用 Prisma SASE 中的開發人員指南。

Prisma Access 洞察 API 描述了 Prisma Access 洞察特有的內容，以及 API 2.0 版、API 1.0 版、Prisma Access 洞察 API 範例和 PAI 常見問題的相關資訊。

### 關於 2.0 API

Prisma Access 洞察 2.0 API 適用於 Prisma Access (Managed by Strata Cloud Manager) 客戶，其中租用戶已由 Palo Alto Networks 使用租用戶服務群組 (TSG) 識別碼裝載。若要查看您的租用戶是

 ©2025 Palo Alto Networks, Inc.

否使用 TSG ID，請前往 Prisma Access 中樞、按一下 **Prisma Access** 洞察應用程式名稱，然後在 **Manage Apps**（管理應用程式）區段中查看。

Prisma Access (Managed by Panorama) 客戶也可以使用 2.0 API。在此情況下，如果 Prisma Access (Managed by Panorama) 部署為多租用戶，則只有超級租用戶具有 TSG ID，並且子租用戶會包含在標頭中，租用戶 ID 為 Strata Logging Service。

**API 2.0** 案例

在超級租用戶移轉至 TSG ID 之後，查詢子租用戶時：

標頭需要下列資訊：`Prisma-Tenant:tsg_id:sub_tenant_id`

## 關於 1.0 API

Prisma Access 洞察 1.0 API 適用於所有 Prisma Access (Managed by Strata Cloud Manager) 單一租用戶客戶，以及 Prisma Access (Managed by Panorama) 單一租用戶和多租用戶客戶。

**API 1.0** 案例

在超級租用戶移轉至 TSG ID 之前，當使用 1.0 API 查詢子租用戶資訊時，請在端點上包含超級租用戶 ID：

```
/api/sase/v1.0/resource/tenant/{super_tenant_id}/
```

在呼叫時包含下列標頭：`Prisma-Tenant: {tenant_id}: {sub_tenant_id}`

 ©2025 Palo Alto Networks, Inc.

# 將 Prisma Access 從 Panorama 移轉至 Strata Cloud Manager

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br><br>若要開始從 Prisma Access (Managed by Panorama) 移轉至 Prisma Access (Managed by Strata Cloud Manager)，請聯繫您的 Palo Alto Networks 客戶團隊。 |

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

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

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

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

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

- 何時移轉—請勿在資料平面或基礎結構升級期間執行升級。檢查您的升級偏好設定，以查看是否有即將進行的資料平面升級。
- 從 **Panorama** 單向移轉至 **Prisma Access (Managed by Strata Cloud Manager)**—您只能從 Prisma Access (Managed by Panorama) 移轉至 Prisma Access (Managed by Strata Cloud Manager) 部署。在移轉至 Strata Cloud Manager 之後，您無法返回使用 Panorama 管理您的 Prisma Access 部署。
- 最低 **Panorama** 版本—最低必要 Panorama 版本為 10.0。
- 必要管理員角色—您必須以 Strata Cloud Manager 中的超級使用者身分登入，才能開始移轉。


©2025 Palo Alto Networks, Inc.

- 授權需求#需要有效的 Prisma Access 授權。
- 雲端識別引擎—移轉前您必須已整合雲端識別引擎的目錄同步元件與目前的 Prisma Access (Managed by Panorama) 租用戶。
- 不受支援的功能—移轉程序不支援以下 Prisma Access 功能：
  - 多租用戶部署
  - IoT 安全性
  - 資料篩選（作為替代方案，使用企業 DLP）
  - SSH Proxy
  - GlobalProtect 入口網站和閘道的個別驗證
- 設定差異問題—當您在移轉期間執行設定差異時，請忽略顯示以下物件名稱的任何差異，因為它們不會影響您的設定：
  - Clientless-vpn crypto-settings
  - Hip-profiles rename
  - Mobile-user-redundancy
  - Exclude-video-traffic

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

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

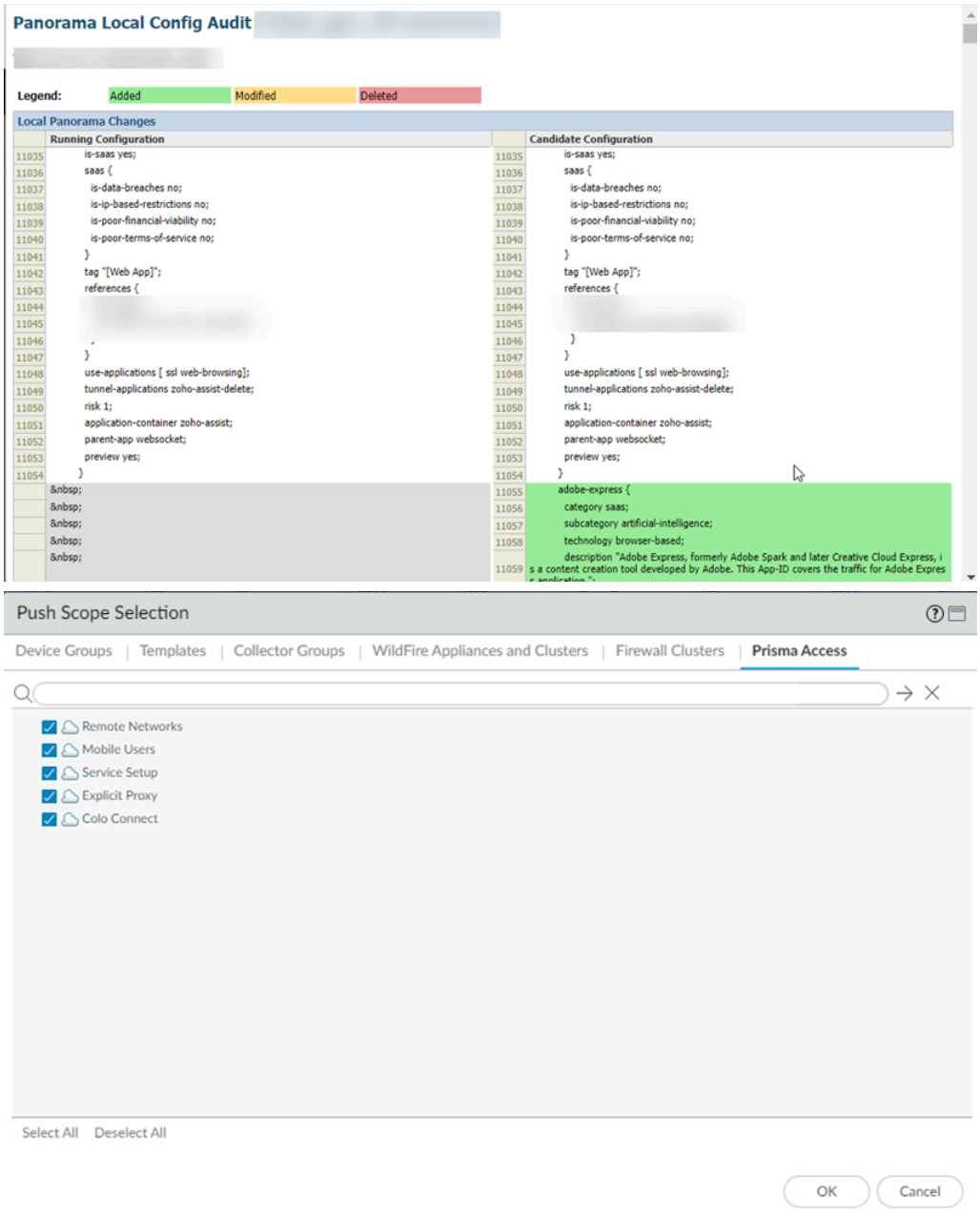
在較高的層級上，您：

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


©2025 Palo Alto Networks, Inc.

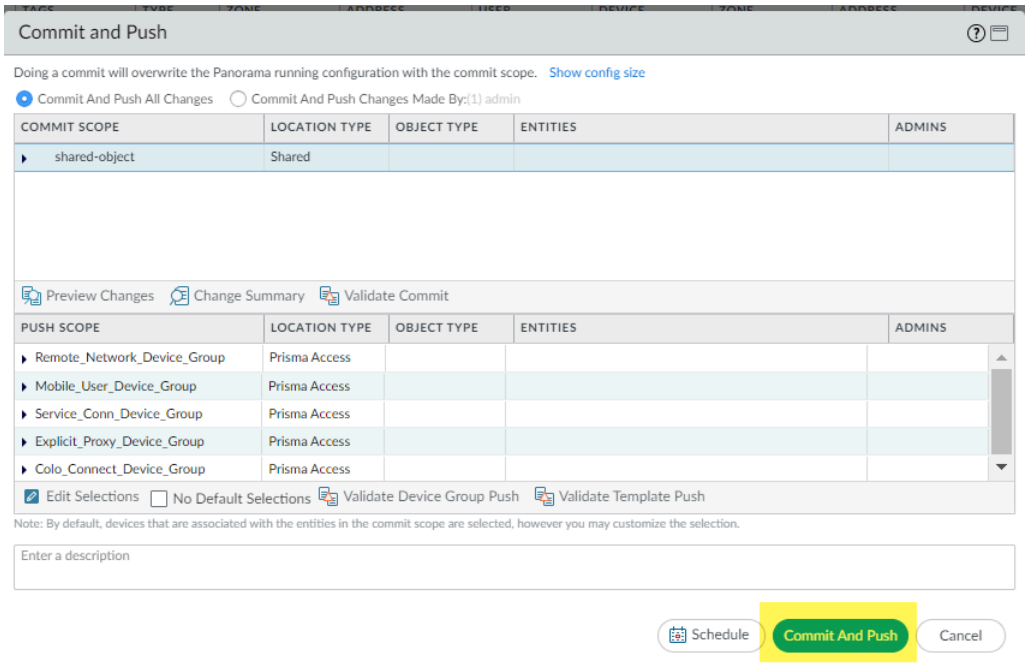
**STEP 1 |** 準備您的 Panorama 進行移轉。

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




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

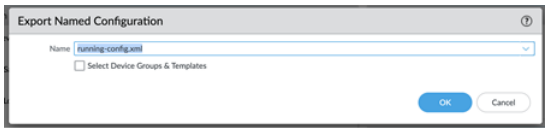

©2025 Palo Alto Networks, Inc.




6. 前往 **Panorama** > **Setup**（設定） > **Operations**（操作），並 **Export named Panorama configuration snapshot**（匯出具名 **Panorama** 設定快照）。

   在移轉過程中，此 .xml 檔案需要上傳至 Strata Cloud Manager。請勿上傳技術支援檔案或 **.xml** 設定檔案以外的任何其他檔案。

7. 選取 **running-config.xml** 設定檔案並選取 **OK**（確定）。

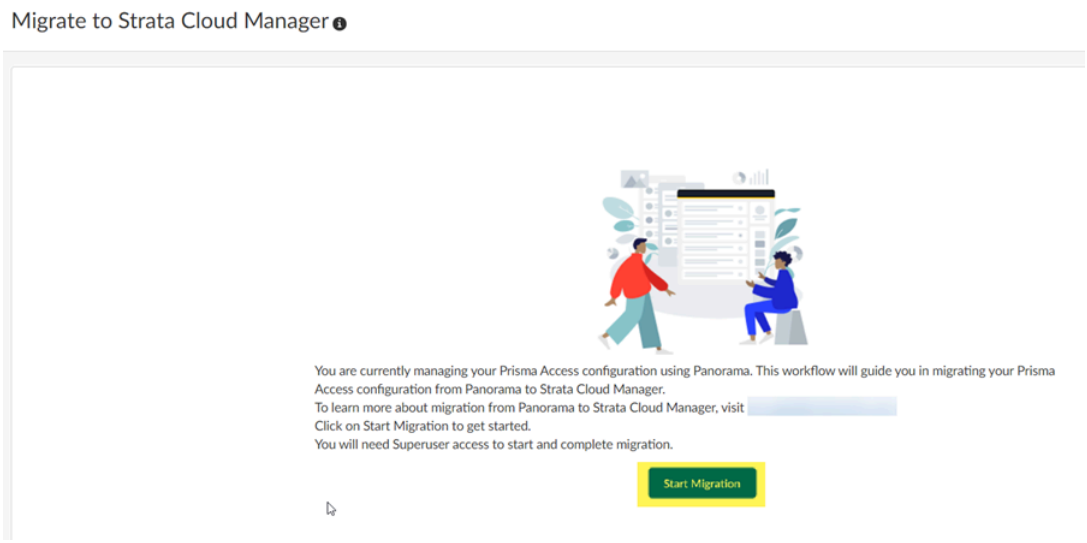



**STEP 2 |** 以具有 超級使用者角色的管理員身分登入 Strata Cloud Manager，並前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**）。

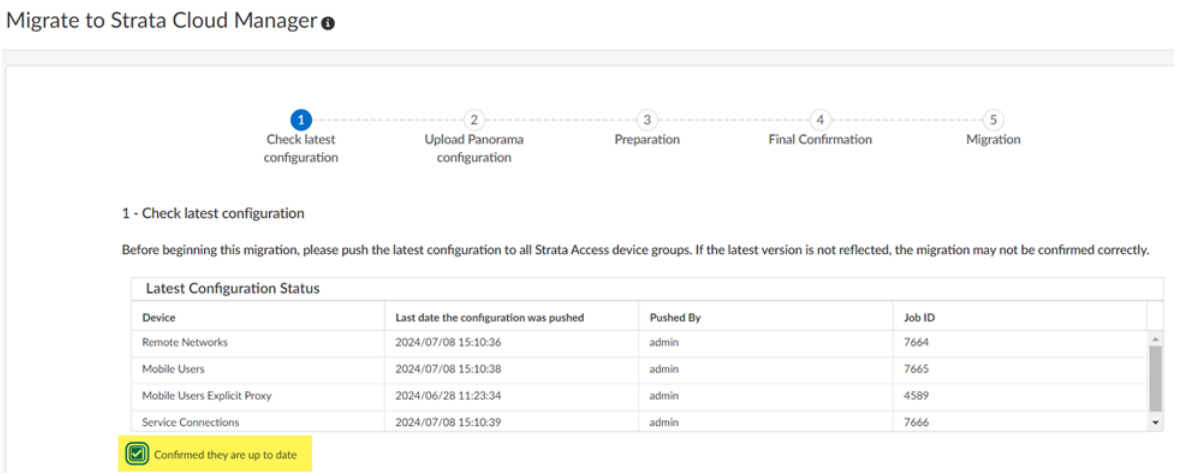
移轉程式偵測到您有 Panorama 受管理部署。

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 開始移轉。



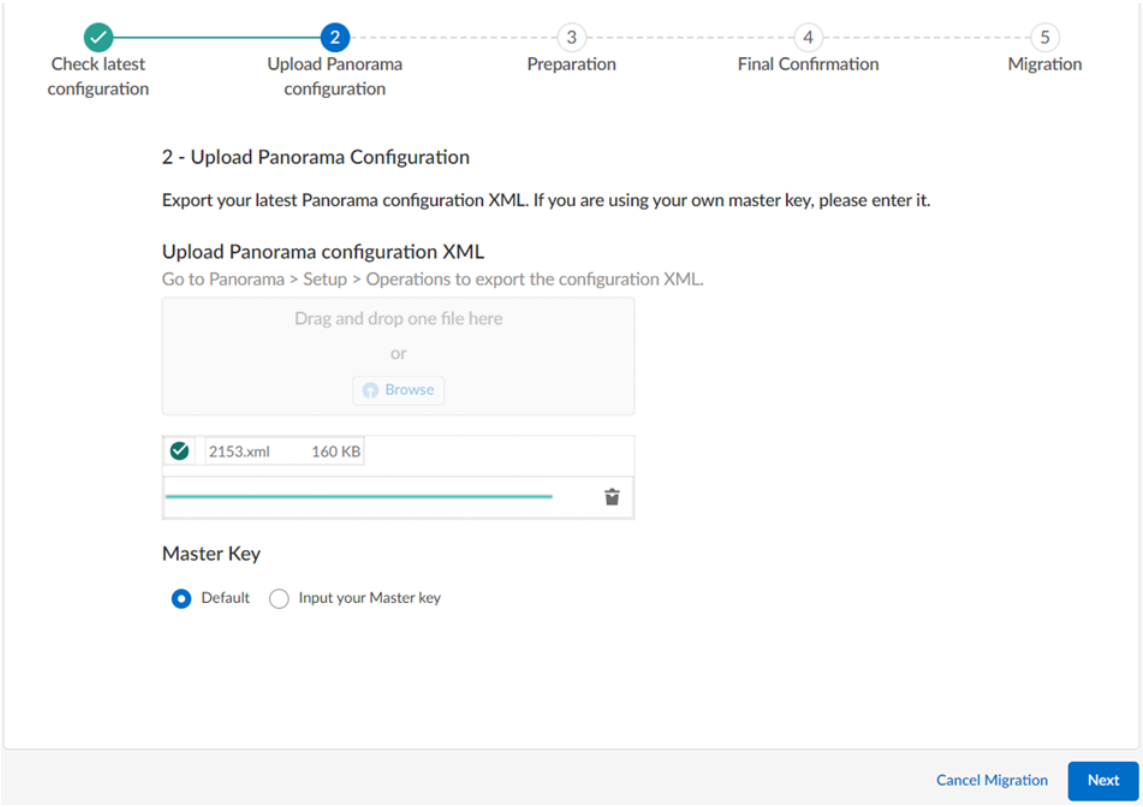

**STEP 4 |** 移轉程式要求您確保您的設定是最新的，並顯示上次更新它的使用者。在驗證了此設定具有最新變更之後，請選取 **Confirmed they are up to date**（已確認它們是最新的），然後按一下 **Next**（下一步）。



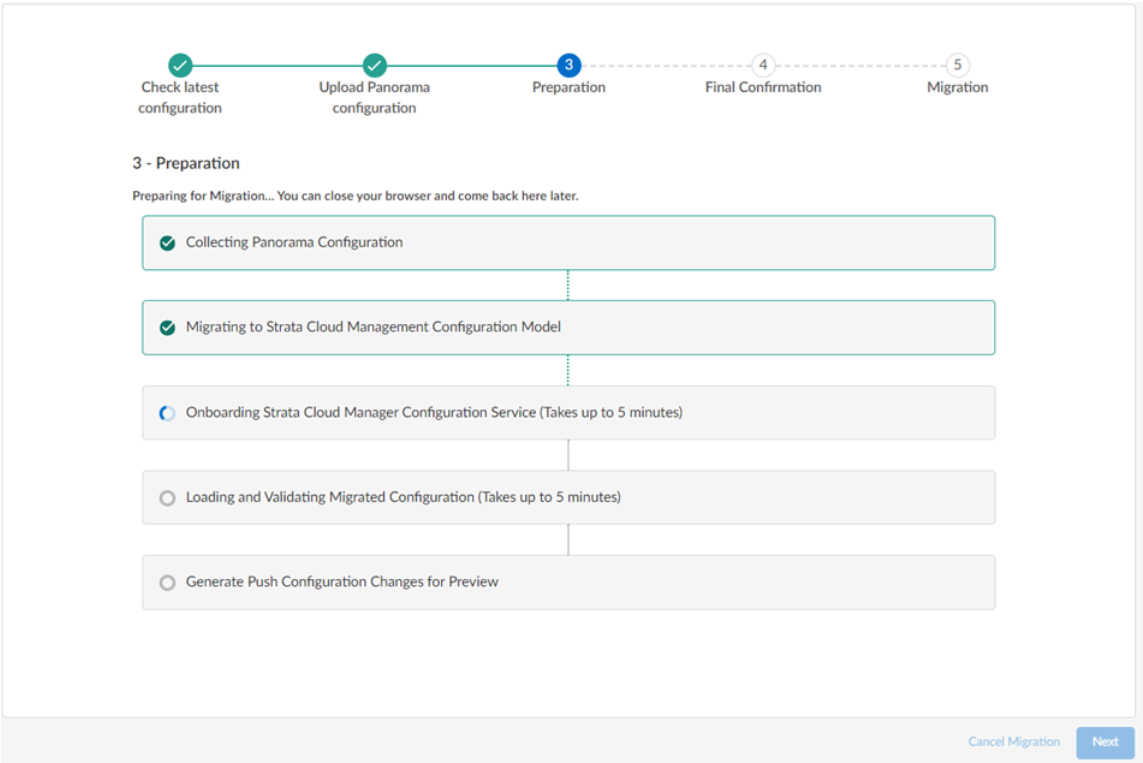

**STEP 5 |** 透過拖放方式選取您在先前步驟中下載的 Panorama 設定 .xml 檔案，或 **Choose File**（選擇檔案）。

 ©2025 Palo Alto Networks, Inc.

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




移轉計劃開始。

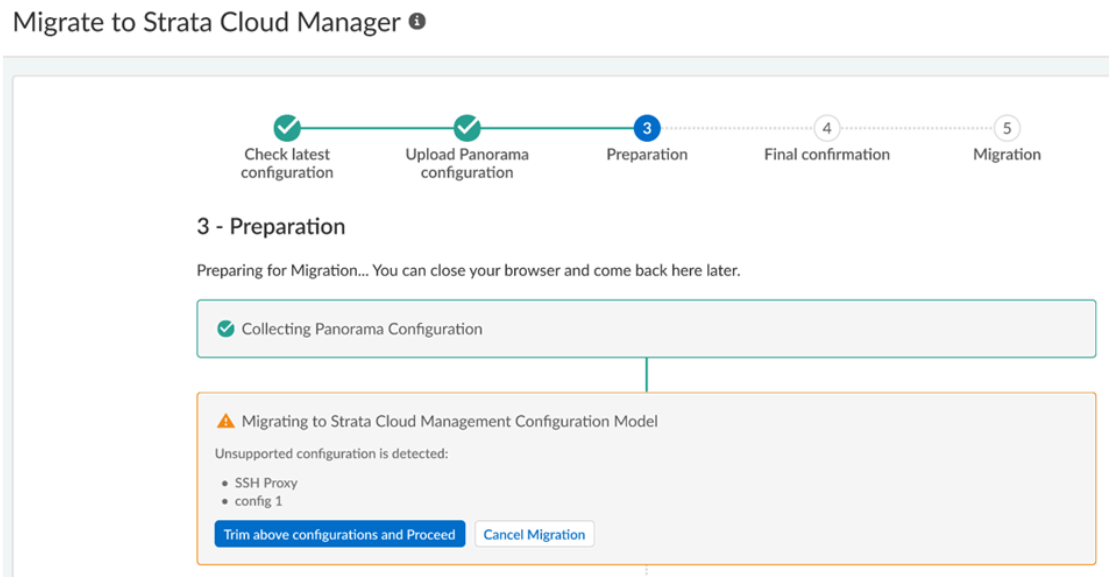




©2025 Palo Alto Networks, Inc.

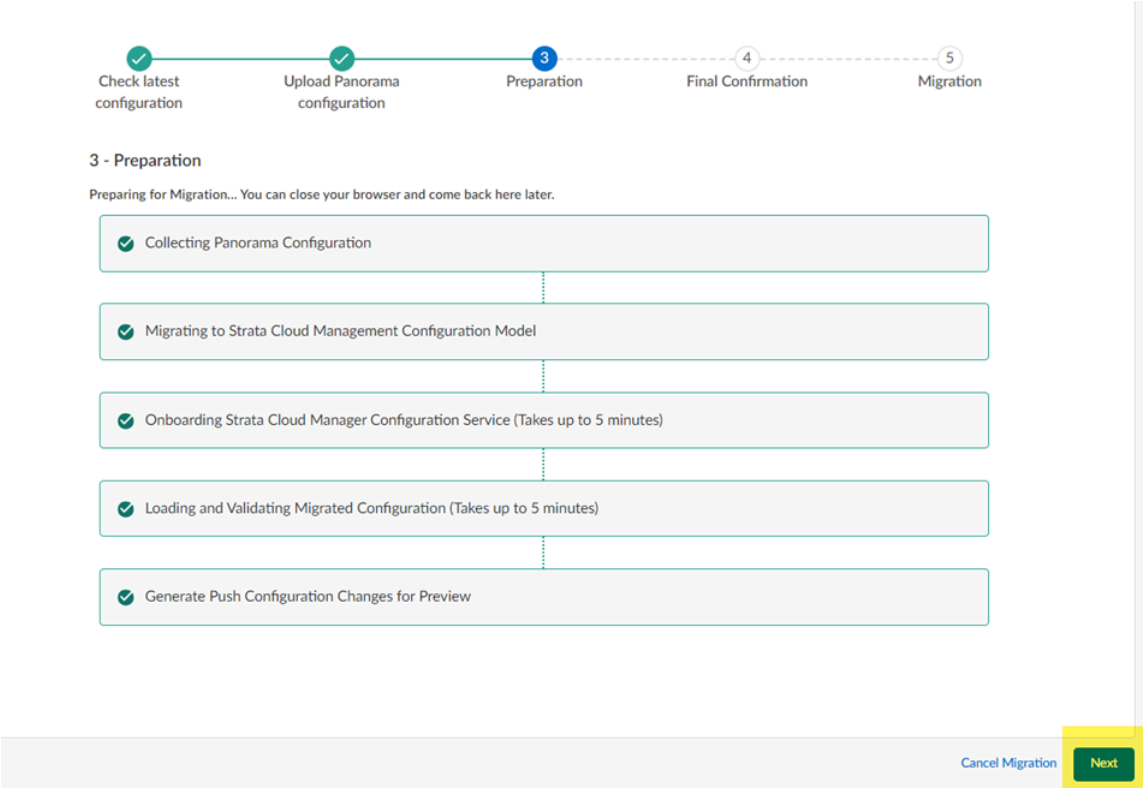
等待所有步驟完成。

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




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

**STEP 8 |** 移轉完成後，請按一下 **Next**（下一步）。



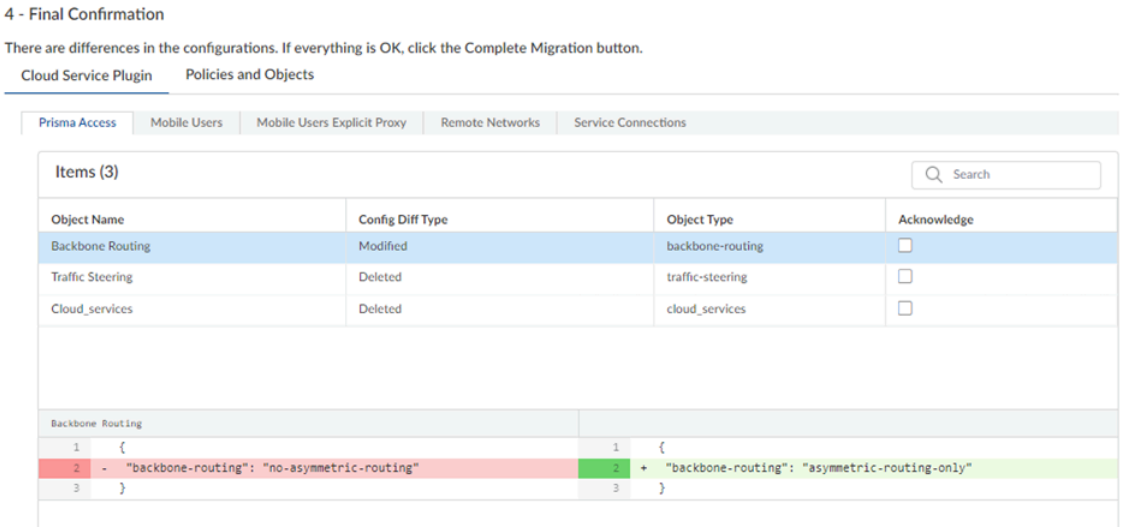

 ©2025 Palo Alto Networks, Inc.

**STEP 9 |** 如果移轉程式進行了變更，請在最終確認畫面中檢閱它們。

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

忽略顯示以下物件名稱的任何差異；它們不會影響您的設定：

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




**STEP 10 |** （選用）對差異進行變更。

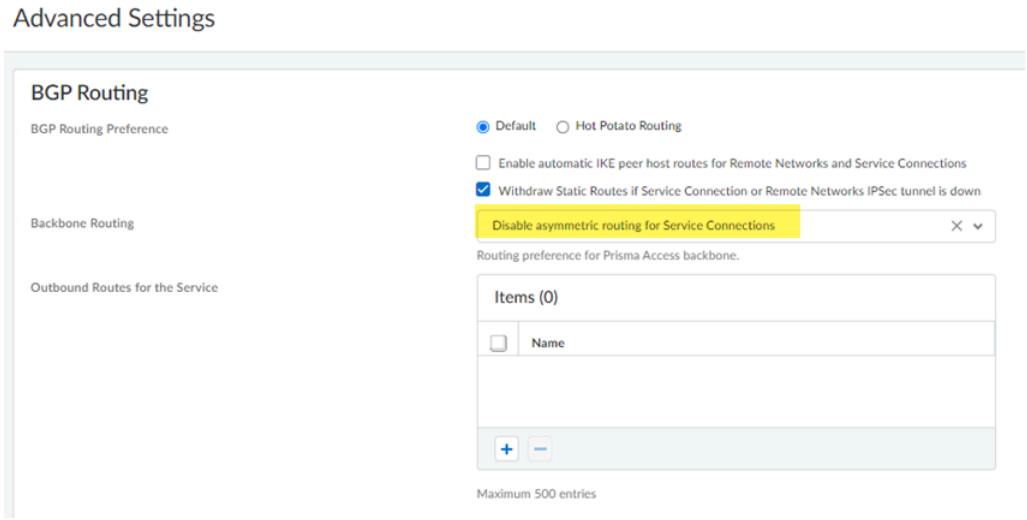
在完成移轉並將您的變更推送到 Strata Cloud Manager 之前，您所做的任何變更都不會提交到您的設定。

1. 導覽至 Prisma Access 設定中的區域，您在其中找到差異並對設定進行變更。

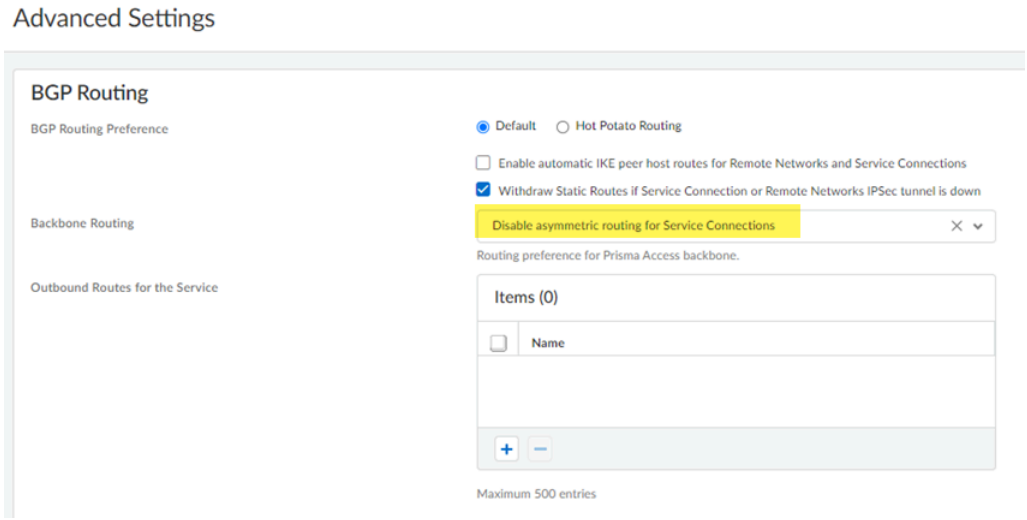
   對於上一個步驟中的範例，移轉程式對骨幹路由進行了變更（從 **no-asym-routing** 變更為 **asymmetry-routing-only**）。若要將此設定變更回您的原始設定，請前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Service Connections**（服務連線） > **Advanced Settings**（進階設定） >，並將


©2025 Palo Alto Networks, Inc.

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



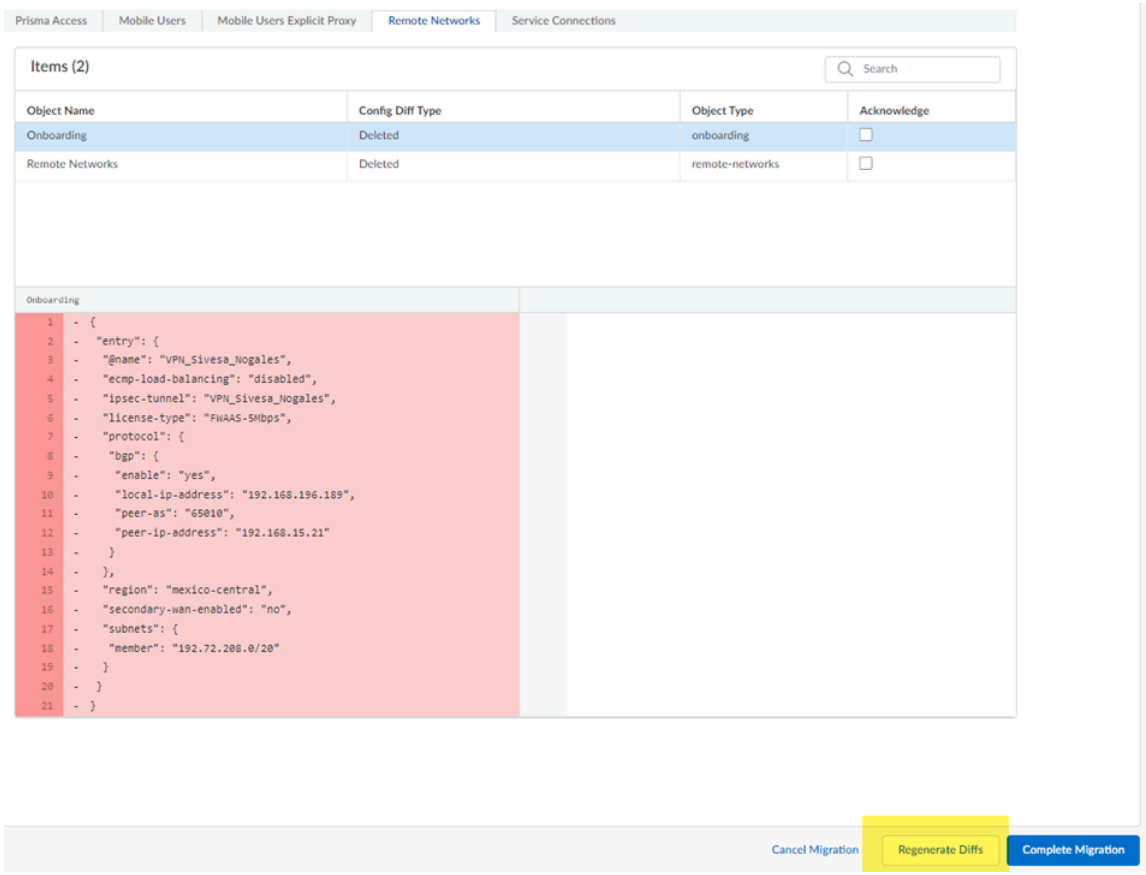

2. （用選）若要追蹤您的變更，請在完成變更時 **Acknowledge**（確認）它們。
   雖然不是必要的，但在進行每個變更時確認這些變更可能很有用，以便您可以追蹤它們。




3. 繼續檢閱變更，然後進行變更並確認它們。


©2025 Palo Alto Networks, Inc.

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

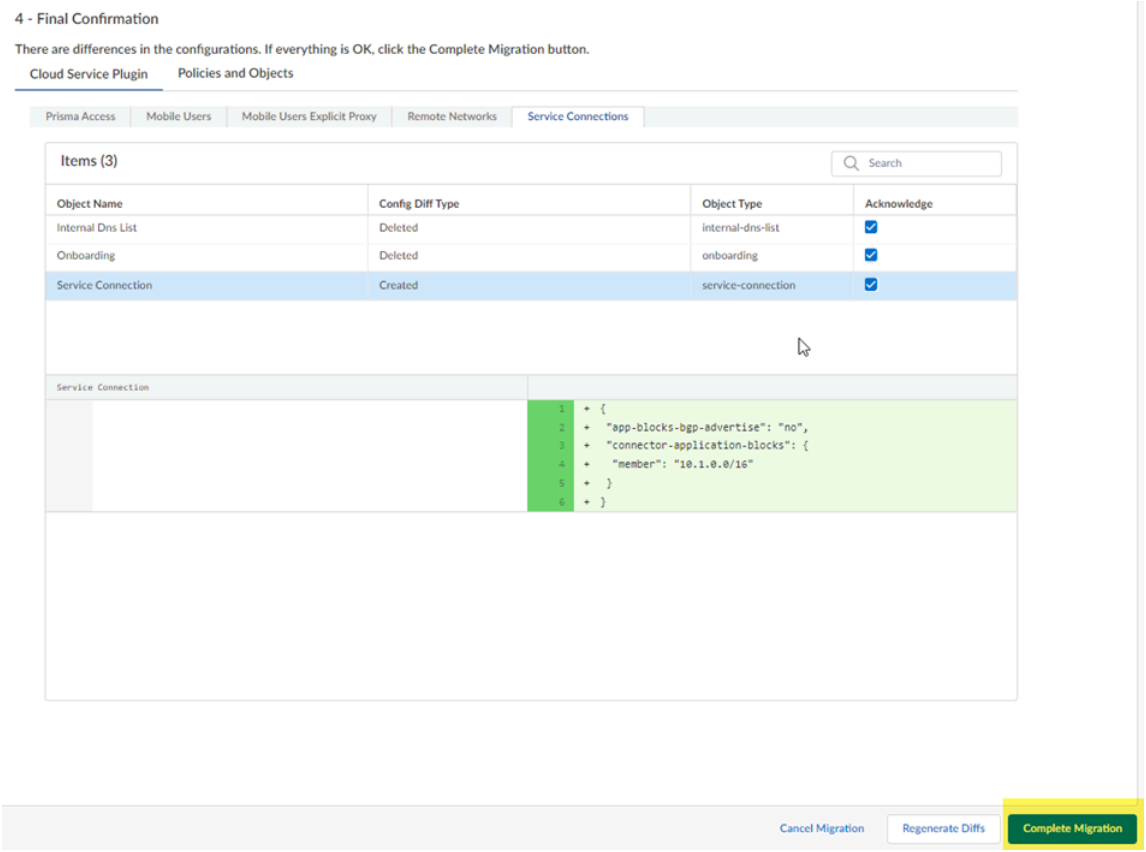



 ©2025 Palo Alto Networks, Inc.

**STEP 12 | Complete Migration**（完成移轉）。

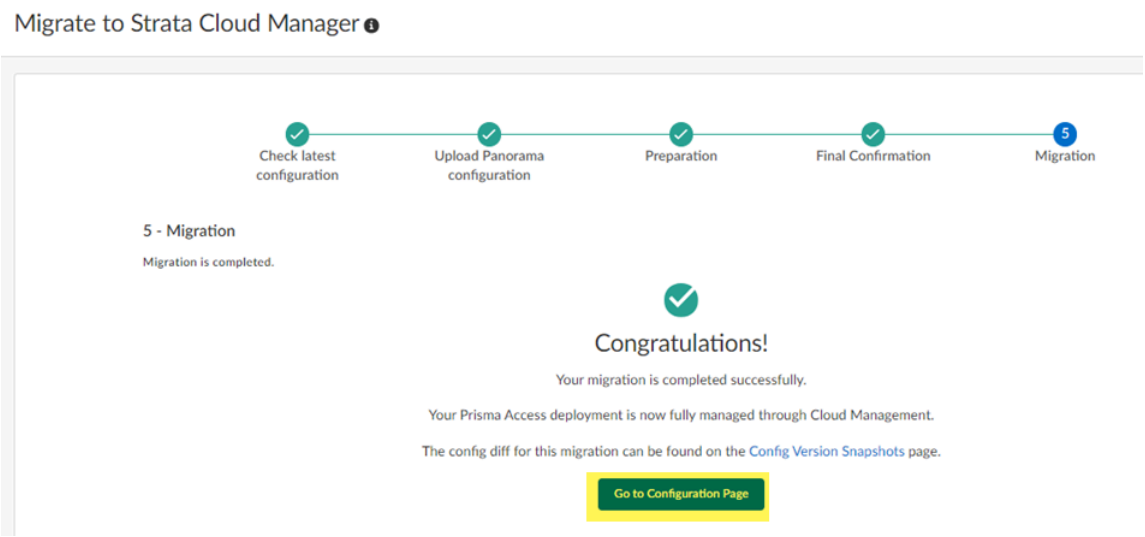
雖然不需要這樣做，但您也可以 **Acknowledge**（確認）您的變更。

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

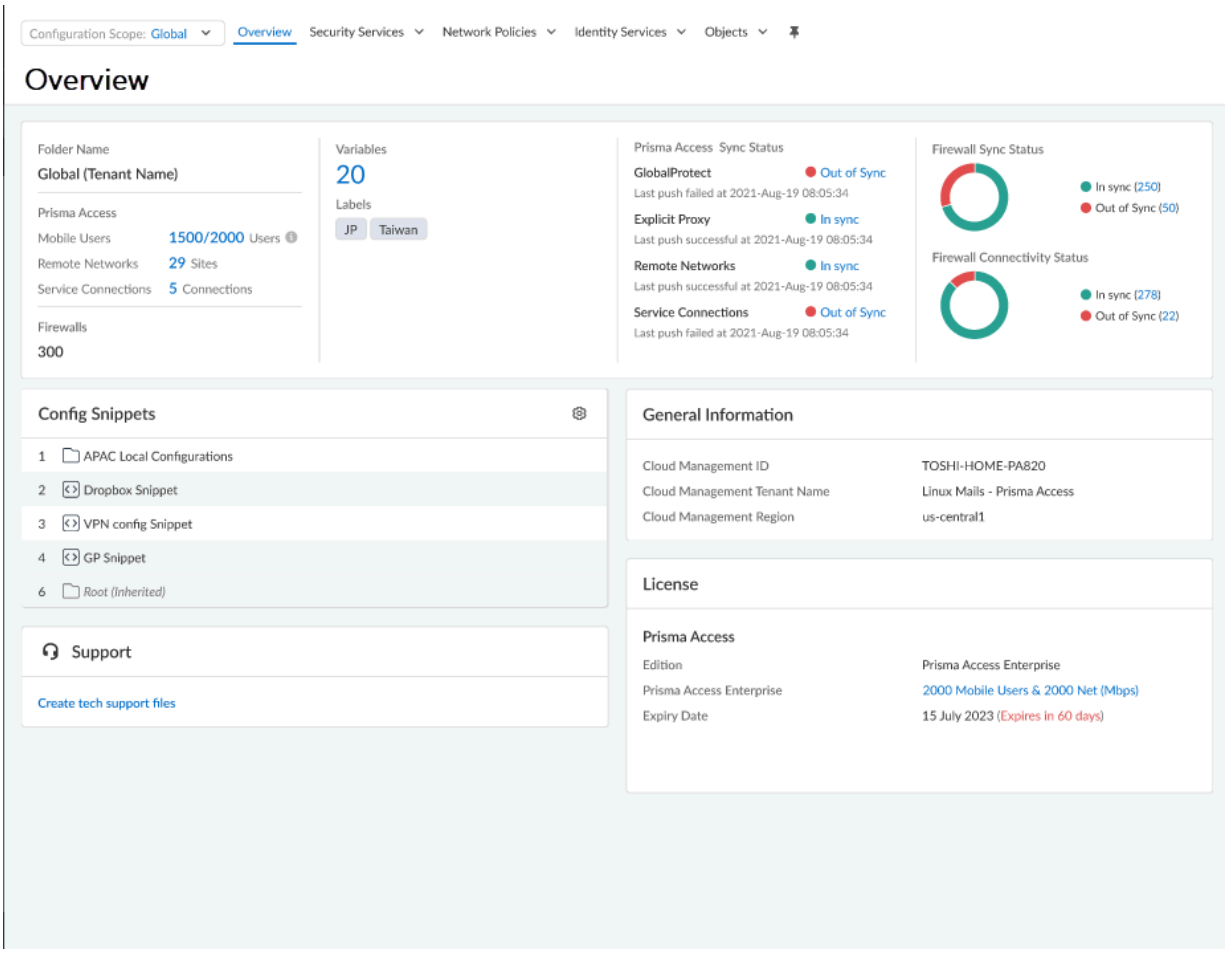



 ©2025 Palo Alto Networks, Inc.

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



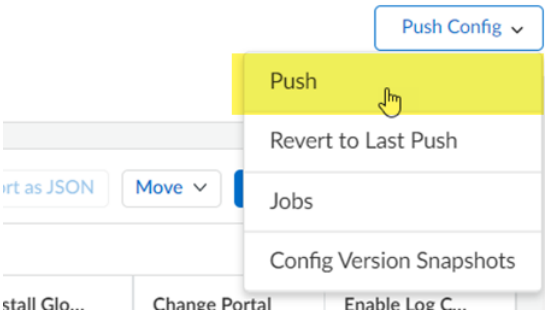

您移轉的部署即會顯示。




 ©2025 Palo Alto Networks, Inc.

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

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




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


©2025 Palo Alto Networks, Inc.

# Prisma Access 版本和升級

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

Prisma Access 版本和更新可讓您掌握最新資訊以及保護使用者。部分更新是由 Palo Alto Networks 所管理（例如 Prisma Access 基礎架構更新），而且您將會提前收到通知，以根據它們進行規劃。其他更新是您的責任，您必須儘早排程指定版本的內容更新、軟體更新和外掛程式版本（視需要）。



您可以透過存取 https://sase.status.paloaltonetworks.com/ 網站來擷取所有雲端服務的狀態，包括 *Prisma Access* 和 *Strata Logging Service*，以及每項服務執行時間的歷程記錄。您也可以在此網站上註冊電子郵件或簡訊更新，以在規劃基礎結構更新時提前通知您，並在更新發生時，以及在 *Palo Alto Networks* 建立、更新或解決事件時，即時通知您。

# Prisma Access 版本類型

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

Prisma Access 可以進行升級，包括主要版本和基礎結構維護，其中包括新功能和最佳化，可為您的遠端網路和行動使用者提供最佳的安全性。

以下清單定義了版本類型，以及我們為每個版本提供的提前通知。若要確保您收到所有版本的通知，請在 https://sase.status.paloaltonetworks.com/ 為 Prisma Access 註冊電子郵件或簡訊，並註冊 Strata Cloud Manager 中的警示。

- 主要版本—主要版本通常包括重要的新功能和最佳化，並且此類更新是透過 Palo Alto Networks 設定的計劃維護時段來推送的。Palo Alto Networks 透過 sase.status.paloaltonetworks.com 經由電子郵件通知客戶此類計畫維護活動。

  通知—Palo Alto Networks 為您提供以下主要版本通知：

| 部署類型 | 通知期間 |
| --- | --- |
| 生產部署 | Palo Alto Networks 在主要版本發佈前 21 天為您提供通知。 |
| 實驗室部署 | Palo Alto Networks 在主要版本發佈前 7 天為您提供通知。 |

除了排程的主要版本升級之外，*Palo Alto Networks* 可能還需要進行緊急排程升級，這些升級遵循不同的排程。

實驗室租用戶未涵蓋在 Prisma Access 服務等級協定 (SLA) 之下，因此強烈建議客戶僅將租用戶用於生產前測試和資格認證目的。

- 基礎結構維護—包括遞增功能和最佳化。在某些情況下，Palo Alto Networks 可能會將修補程式與基礎結構維護結合。

  通知—Palo Alto Networks 為您提供以下通知：

| 部署類型 | 通知期間 |
| --- | --- |
| 生產部署 | Palo Alto Networks 在基礎結構維護前 10 天為您提供通知。 |


©2025 Palo Alto Networks, Inc.

| 部署類型 | 通知期間 |
| --- | --- |
| 實驗室部署 | Palo Alto Networks 在基礎結構維護前 7 天為您提供通知。 |

除了排程的主要版本升級之外，*Palo Alto Networks* 可能還需要進行緊急排程升級，這些升級遵循不同的排程。

- 雲端服務外掛程式版本（僅限 **Panorama** 受管理部署）—如果 Prisma Access 需要新的外掛程式，可透過 Palo Alto Networks 客戶支援入口網站 (CSP) 下載來取得，以及在正式推出 (GA) 版本的日期於 Panorama 上取得。

  Prisma Access 可能會強制所有租用戶升級到特定的雲端服務外掛程式版本，以維護回溯相容性和支援的軟體版本。此類強制執行活動將提前 **14** 天發出通知（透過 sase.status.paloaltonetworks.com 頁面）以規劃外掛程式的升級。該服務強烈建議您在最新外掛程式可供下載後立即升級到該外掛程式。

## 緊急排程升級

Palo Alto Networks 有時必須執行緊急資料平面或基礎結構升級，其中包括 Hotfix 或緊急錯誤修復（例如，零時差威脅修復或外掛程式變更）。Palo Alto Networks 將盡一切努力在緊急排程升級前48 小時通知您；不過，有時您收到緊急排程升級通知的時間會縮短。


©2025 Palo Alto Networks, Inc.

# Prisma Access 升級類型

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

Palo Alto Networks 無需您介入即可升級其雲端型基礎結構。某些升級會要求您執行某個動作，例如安裝新的外掛程式。

以下清單包括不同類型的 Prisma Access 升級：

- 基礎結構升級—Palo Alto Networks 會升級 Prisma Access 基礎結構，也稱為 Prisma Access 控制平面，其中包括基礎服務後端、協調和監控基礎結構。

  您預計每年會收到 4 到 6 次基礎結構升級。
- 資料平面升級—Palo Alto Networks 會升級 Prisma Access 資料平面，從而對您的網路和使用者流量啟用流量檢查和安全性政策強制執行。

  您可以使用應用程式註冊資料平面升級電子郵件警示通知，並指出您的升級偏好設定。
- **Prisma Access** 排程維護—Prisma Access 每兩周預留一個時段，用於執行與基礎架構的 Hotfix 和緊急錯誤修復相關的維護。
- （僅限 Panorama 受管理部署）雲服務外掛程式升級—有新的外掛程式版本可用時，您的網路管理員將需要在管理 Prisma Access 的 Panorama 設備上升級雲端服務外掛程式。
- （僅限 Panorama 受管理部署）**Panorama** 軟體版本升級—升級您的 Panorama 軟體可能需要確保與 Prisma Access 持續相容.

下表向您顯示了每個版本隨附的內容，包括我們提供的維護時段，以及對 Prisma Access 服務的任何影響。

| 升級類型 | 維護時段 | 影響 |
| --- | --- | --- |
| 基礎結構升級 | 2-8 小時 | 對網路流量沒有影響；不過，您無法在維護時段期間執行提交。<br>Palo Alto Networks 將升級排程在當地時間進行，以盡量減少對業務功能的干擾。 |
| 資料平面升級 | 72 小時 | Palo Alto Networks 使用此時段為所有客戶升級資料平面。您可以在此時段期間進行設定變更和提交。我們的目標是最大限度地減少對網路流量的影響，但在某些情況下可能會 |


©2025 Palo Alto Networks, Inc.

| 升級類型 | 維護時段 | 影響 |
| --- | --- | --- |
| | | 出現短暫的中斷。如需詳細資訊，請參閱 Prisma Access 資料平面升級。<br><br>您可以使用應用程式註冊資料平面升級電子郵件警示通知，並指出您的升級偏好設定，包括進行升級的偏好時段。 |
| 雲端服務外掛程式升級（僅限 Panorama 受管理部署） | 當外掛程式可用時，您可以安裝該外掛程式。 | Prisma Access 可能要求您將所有租用戶升級到特定的外掛程式版本，以維護回溯相容性和支援的軟體版本。<br><br>在外掛程式升級期間，您無法在 Panorama 中進行設定變更和提交。 |
| Panorama 軟體版本升級（僅限 Panorama 受管理部署） | 您可以在管理 Prisma Access 的 Panorama 上排程並執行升級. | 當 Prisma Access 在主要版本之後升級其基礎結構和資料平面時，升級可能與早期的 Panorama 版本不相容。由於 Prisma Access 和雲端服務外掛程式的快速發布，Panorama 的軟體相容性（終止支援）日期比 Panorama 版本的軟體使用壽命日期短，並且僅適用於與 Prisma Access 的 Panorama 版本相容性。如需詳細資訊，包括與 Prisma Access 搭配使用時 Panorama 的終止支援日期，請參閱 Palo Alto Networks 相容性矩陣中的 Prisma Access 和 Panorama 版本相容性。 |


©2025 Palo Alto Networks, Inc.

# Prisma Access 的軟體和內容更新節奏

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

- Strata Cloud Manager
- Panorama

## Prisma Access (Managed by Strata Cloud Manager) 的軟體和內容更新節奏

下格描述了 Prisma Access 如何更新其基礎結構元件，包括內容和軟體更新。此表格也會指出 Prisma Access 是否自動更新軟體。如果任何更新不會自動執行，您可以瞭解如何套用這些基礎結構更新。

您還可以從中心檢查所有雲端服務的狀態。

| 元件 | 更新排程 | 註解 |
| --- | --- | --- |
| GlobalProtect 應用程式 | • 主要 **GlobalProtect** 應用程式版本（例如，**x.0** 或 **4.x**）—在該版本的 *x*.0.1 版正式推出後的 7-10 天內，Prisma Access 會將應用程式更新至最新的主要版本。<br>例如，假設有一個應用程式版本為 4.0，Prisma Access 會在 4.0.1 版發行後的 7-10 天內更新應用程式。<br>• 次要 **GlobalProtect** 應用程式版本（例如，**4.1.x**）—在該版本正式推出後的 7-10 天內，Prisma Access 會將應用程式更新至最新的次要版本。 | 雲端控制可供升級的應用程式版本。 |
| Prisma Access 基礎結構中的 PAN-OS 軟體升級—已排程 | 當新版本的 Prisma Access 發行時，Palo Alto Networks® 會升級 PAN-OS 基礎結構。Palo Alto Networks® 會在排程的升級之前提前三週通知您。 | 註冊以透過電子郵件或文字通知在中心接收基礎結構升級。 |
| 應用程式和威脅更新 | 每日以 24 小時為閾值。<br>Palo Alto Networks® 會在每個月第三個星期二發行新的 App-ID。計劃在 24 小時閾值內 | |


©2025 Palo Alto Networks, Inc.

| 元件 | 更新排程 | 註解 |
| --- | --- | --- |
| | 檢閱並納入這些新的 App-ID。使用新的 App-ID 篩選器，將這可能的流量影響降至最低。<br>新的 App-ID 特性可讓您查看網路上的新應用程式，並向您顯示有關新分類的應用程式活動的詳細資訊。獲取到的資訊，可幫助您作出正確決策，恰當更新安全性原則，以執行最新分類的 App-ID。 | |
| 防毒保護 | 每小時，10 分鐘後開始 | Prisma Access 始終使用最新的防毒軟體版本保持最新狀態。 |
| WildFire | 即時 | Prisma Access 始終使用最新的 WildFire 版本保持最新狀態。 |
| GlobalProtect 資料檔案 | 每小時 | Prisma Access 始終使用最新的 GlobalProtect 資料檔案版本保持最新狀態。 |
| 無用戶端 VPN<br>應用程式特徵碼 | 每小時 | Prisma Access 始終使用最新的無用戶端 VPN 應用程式特徵碼版本保持最新狀態。 |

## Prisma Access (Managed by Panorama) 的軟體和內容更新節奏

下表會告知您有哪些軟體和內容更新，以取得最新的應用程式和威脅特徵碼，並利用 Palo Alto Networks 提供的威脅防護功能。如果 **Cloud Controlled?**（是否受雲端控制？）欄的屬性為 **No**（否），您會執行更新元件所需的動作。

| 元件 | 更新排程 | 是否受雲端控制？（是/否） | 註解 |
| --- | --- | --- | --- |
| 升級到 Panorama 軟體以與 Prisma Access 相容 | 對於主要 Prisma Access 版本，您可能需要針對以下使用案例升級 Panorama 版本：<br>• 需要升級—有時，您需要升級 Panorama 上的軟體版本，才能與 | 否。 | 請參閱 Panorama 軟體版本與 Prisma Access 相容性的終止支援 (EoS) 日期，以瞭解 Panorama 版本何時與 Prisma Access 不相容。。請參閱 Prisma Access 與 Panorama 版本相容性，以取得哪些目前支援的 Panorama 版 |


©2025 Palo Alto Networks, Inc.

| 元件 | 更新排程 | 是否受雲端控制？（是/否） | 註解 |
| --- | --- | --- | --- |
| | Prisma Access 維持相容性。<br>• 維護時段—您的組織需要排程一個維護時段來升級 Panorama 軟體版本。<br>• 影響—在升級 Panorama 版本之前，您無法使用新的外掛程式版本。<br>• 通知—Palo Alto Networks 將在已排程的主要版本升級前 100 天通知您。<br>• 選用升級—在其他情況下，您可能需要升級 Panorama 軟體版本，才能使用主要版本中 Prisma Access 支援的新功能。<br>• 維護時段—您的組織需要排程一個維護時段來升級 Panorama 軟體版本。<br>• 影響—您無法使用 Prisma Access 支援的新功能，直到您升級 Panorama。<br>• 通知—Palo Alto Networks 將在排程的主要版本升級前 21 天通知您任何 Panorama 需求，如 Prisma | | 本可與 Prisma Access 搭配使用。若要將 Panorama 升級到新版本，請參閱安裝 Panorama 的內容和軟體更新。 |


©2025 Palo Alto Networks, Inc.

| 元件 | 更新排程 | 是否受雲端控制？（是/否） | 註解 |
|---|---|---|---|
| | Access 版本類型 中所定義。 | | |
| 雲端服務外掛程式版本 | 外掛程式發行後即可使用。 | 否。 | 您會執行工作來升級外掛程式。請參閱 Prisma Access 版本類型，以取得有關 Prisma Access 何時更新其外掛程式版本的詳細資訊。請參閱升級雲端服務外掛程式，以升級 Panorama 裝置中的外掛程式。 |
| GlobalProtect 應用程式 | • 主要 **GlobalProtect** 應用程式版本（例如，**x.0** 或 **5.*x***）—在該版本的 x.0.1 版正式推出後的 7-10 天內，Prisma Access 會使用最新的主要版本更新入口網站上的代理程式。<br>例如，假設代理版本為 5.1，Prisma Access 會在 5.1.1 發行後 7-10 天內更新入口網站上的代理程式。<br>• 次要 **GlobalProtect** 應用程式版本（例如，**5.1.*x***）—在該版本正式推出後 7-10 天內，Prisma Access 會使用最新的基礎結構維護來更新入口網站上的代理程式。 | 是 | 雲端會控制可供升級的應用程式版本；不過，您可以在應用程式的多個不同託管版本之間進行選擇，並可以控制如何以及何時向一般使用者推出 GlobalProtect 應用程式更新。如需詳細資料，請參閱 GlobalProtect 應用程式升級。<br>如果你的 Prisma Access 部署需要 GlobalProtect 應用程式的 Hotfix，請向 Palo Alto Networks 技術支援開啟 支援案例以取得協助。 |


©2025 Palo Alto Networks, Inc.

| 元件 | 更新排程 | 是否受雲端控制？（是/否） | 註解 |
| --- | --- | --- | --- |
| 應用程式和威脅更新 | 每日以 24 小時為閾值。<br>Palo Alto Networks 會在每個月第三個星期二發行新的 App-ID。計劃在 24 小時閾值內檢閱並納入這些新的 App-ID。<br>新的 App-ID 特性可讓您查看網路上的新應用程式，並向您顯示有關新分類的應用程式活動的詳細資訊。獲取到的資訊，可幫助您作出正確決策，恰當更新安全性原則，以執行最新分類的 App-ID。 | 是 | |
| 防毒保護 | 每小時，10 分鐘後開始 | 是 | Prisma Access 始終使用最新的防毒軟體版本保持最新狀態。 |
| WildFire | 即時 | 是 | 一旦 WildFire 公共雲端能夠產生新發現的惡意軟體，Prisma Access 就會擷取 WildFire 特徵碼，以取得此惡意軟體。 |
| GlobalProtect 資料檔案 | 每小時 | 是 | Prisma Access 始終使用最新的 GlobalProtect 資料檔案版本保持最新狀態。 |
| 無用戶端 VPN 應用程式特徵碼 | 每小時 | 是 | Prisma Access 始終使用無用戶端 VPN 應用程式特徵碼版本保持最新狀態。 |


©2025 Palo Alto Networks, Inc.

# Prisma Access 資料平面升級

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

*Prisma Access (Managed by Strata Cloud Manager)* 自動執行資料平面升級，無需您的任何介入。

Prisma Access 會在服務上執行資料平面升級，以提供新的安全性特徵和功能，來協助保護您組織的一般使用者、商業資產和數位轉型。當 Prisma Access 的新版本需要資料平面升級時，您需要瞭解升級程序的運作方式，並在升級之前已將必要的先決條件備妥。

您可以預期您的資料平面一年升級一至兩次。除了必要的資料平面升級之外，某些版本可能還提供選用的資料平面升級，以支援需要它的 Prisma Access 功能。

- 資料平面升級概要
- 資料平面升級範例

## 資料平面升級概要

Prisma Access 會在兩個週末日期分兩個階段升級您的資料平面，並使用 Strata Cloud Manager 通知您升級相關資訊。在高階上，升級過程中會採取以下步驟。

- 來自 Strata Cloud Manager 的電子郵件通知會在排程的資料平面升級開始日期前 21 天送達。此電子郵件通知提供第 1 階段的資料平面升級開始日期。

  您可能會看到 *Strata Cloud Manager* 中填入的日期早於 *21* 天通知，此日期可能不是最終日期，直到您收到 *21* 天通知。
- 在電子郵件中，系統會要求您透過 Strata Cloud Manager 選取並提交一或多個要首先升級的位置，以及偏好的升級時段。

  您可以多次針對給定的租用戶變更並提交最先升級位置和時段。服務將選擇排程開始日期前七天發生的最後一次提交進行升級。升級開始日期的七天內，您無法進行任何變更。

  如果您進行變更，您所做的變更可能最多需要 30 分鐘才會顯示在洞察上的升級儀表板中。當 Prisma Access 已處理並完成變更時，系統將透過電子郵件警示通知您。

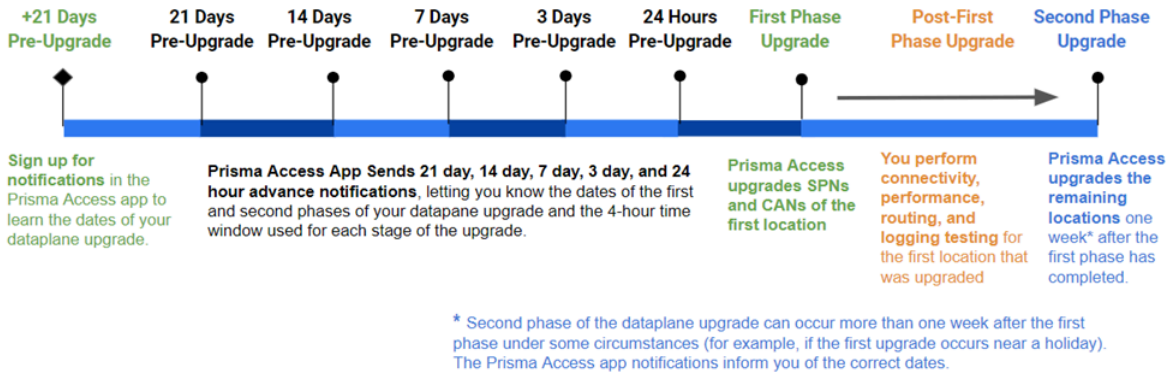
  *Palo Alto Networks* 強烈建議您選取反映整個部署的位置。例如，如果您有行動使用者、服務連線和遠端網路部署，請選取具有所有部署類型的位置。
- Prisma Access 將在為這些位置選取的當地時段內對所選位置執行升級的第 1 階段。
- 如果所選升級位置具有行動使用者—GlobalProtect、行動使用者—明確 Proxy、服務連線或遠端網路的任意組合，則每個部署的資料平面將升級到所需的資料平面版本，如本節稍後所述。
- 一旦在第一個位置完成了升級，您就會透過 Strata Cloud Manager 收到電子郵件通知。Palo Alto Networks 建議您在資料平面升級後立即監控服務是否有任何新問題。


©2025 Palo Alto Networks, Inc.

- 萬一發現新問題，請將問題回報給 Palo Alto Networks 技術支援。

  技術支援團隊將調查該問題並採取更正動作，其中可能還包括回復到先前的資料平面版本。此決策將透過技術支援案例傳達給您。
- 如果沒有新問題或新問題與升級無關，Prisma Access 將在下週末繼續進行資料平面升級。
- 其餘位置的升級將在您為第一個升級選取的相同時段（當地時間）期間進行。
- 在資料平面升級完成之後，系統將會透過電子郵件警示通知您。
- 如果在資料平面升級之後需要外掛程式升級，Palo Alto Networks 建議您在資料平面升級完成之後升級外掛程式。

下圖顯示了用於升級的時間軸，包括您需要執行以進行資料平面升級的工作（以綠色顯示），以及 Prisma Access 執行的步驟。




下一節提供更多有關資料平面升級程序的詳細資訊。

在您註冊通知之後，Prisma Access 會通知您將用於升級程序的兩個週末日期，並在升級第一階段發生前 21 天、14 天、7 天、3 天和 24 小時傳送這些通知。升級程序分兩個階段發生：

- 第 1 階段使用您提供的時段，在第一個週末升級您選擇的一或多個位置，並在升級完成時透過電子郵件通知您。如果您沒有先選擇要升級的位置，或沒有選取時段，則 Prisma Access 會為您做出選擇。

  *Palo Alto Networks* 會在您透過 *Strata Cloud Manager* 選取的四小時時段期間嘗試升級位置。不過，將盡力在此時段期間完成必要的升級，但 *Palo Alto Networks* 無法保證位置將在該時間期間升級。如果升級期間出現任何問題，*Palo Alto Networks* 將在原始四小時時段後 *24* 小時嘗試升級。

  基於這個原因，當資料平面升級進行時，您應該為兩個週末的每一個排程 *72* 小時的變更要求時段，從星期五當地時間晚上 *8* 點開始，於星期一當地時間晚上 *8* 點結束。升級完成時，您將收到一封電子郵件。

  Prisma Access 會在升級第 1 階段期間對您的部署進行下列變更。

| 部署類型 | 升級了什麼 |
| --- | --- |
| 行動使用者—GlobalProtect 部署 | Prisma Access 升級： |


©2025 Palo Alto Networks, Inc.

| 部署類型 | 升級了什麼 |
| --- | --- |
| | • GlobalProtect 閘道，也稱為行動使用者安全性處理節點 *(MU-SPN)*，適用於您選取的一或多個位置。<br>• 與該區域相關聯的 GlobalProtect 入口網站。 |
| 行動使用者—明確 Proxy 部署 | Prisma Access 會針對您指定的一或多個明確 Proxy 位置升級明確 Proxy 節點。 |
| 遠端網路部署 | Prisma Access 會升級備份 (HA) 遠端網路，也稱為遠端網路安全性處理節點 *(RN-SPN)*，然後使備份遠端網路成為您指定的一或多個位置的作用中節點。備份遠端網路連線不會進行升級，直到下一個周末，這時會針對所有位置升級作用中和備份節點。<br>如果選取的位置中有多個 RN-SPN，則所有主要節點都會升級到新的資料平面版本。 |
| 服務連線 | Prisma Access 會升級備份 (HA) 服務連線，也稱為服務連線企業存取節點 (SC-CAN)，然後使備份服務連線成為您指定的一或多個位置的作用中節點。備份服務連線不會進行升級，直到下一個周末，這時會針對所有位置升級作用中和備份節點。<br>如果選取的位置中有多個 SC-CAN，則所有備份節點都會升級到新的資料平面版本。 |
| ZTNA 連接器 | ZTNA 連接器不會升級；您可以視需要升級 ZTNA 連接器。 |

在第一個升級和第二個升級之間，監控第一個升級的位置，並執行連線、效能、路由和記錄測試，以確保位置已成功升級。如果您在升級後遇到影響服務的故障，請開啟支援案例，向 Palo Alto Networks 技術支援尋求協助。Palo Alto Networks 將嘗試在 24 小時內將資料平面回復到先前的資料平面版本來解決此問題。

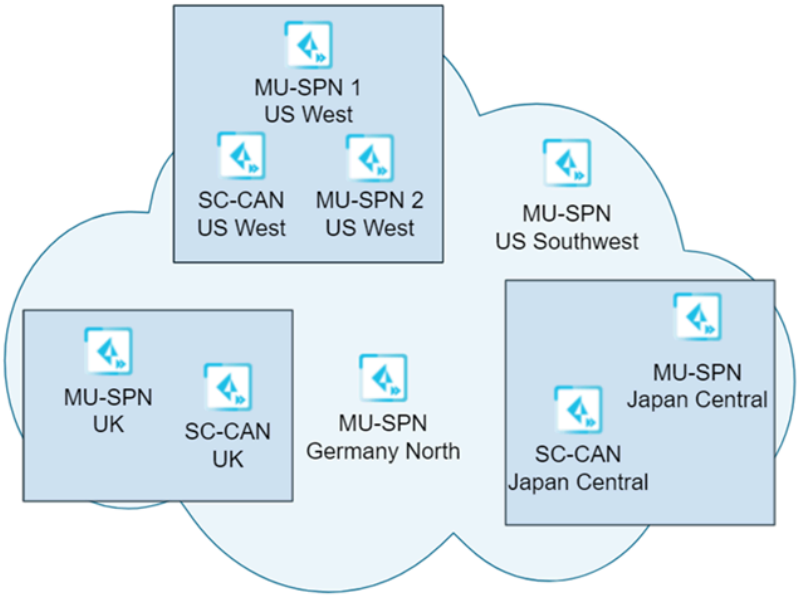
- 在 Prisma Access 升級第一個位置的七天後，Prisma Access 會使用您在第一階段選擇的同一時段升級您的其餘位置（第 2 階段升級），並在升級完成時透過電子郵件通知您。

升級時段可能會更長。例如，如果第 *2* 階段發生在美國的國定假日期間，則升級的第二階段會在第一階段後 *14* 天發生，而不是 *7* 天後。您在 *Strata Cloud Manager* 收到的通知會顯示即將到來的資料平面升級的特定時間軸。


©2025 Palo Alto Networks, Inc.

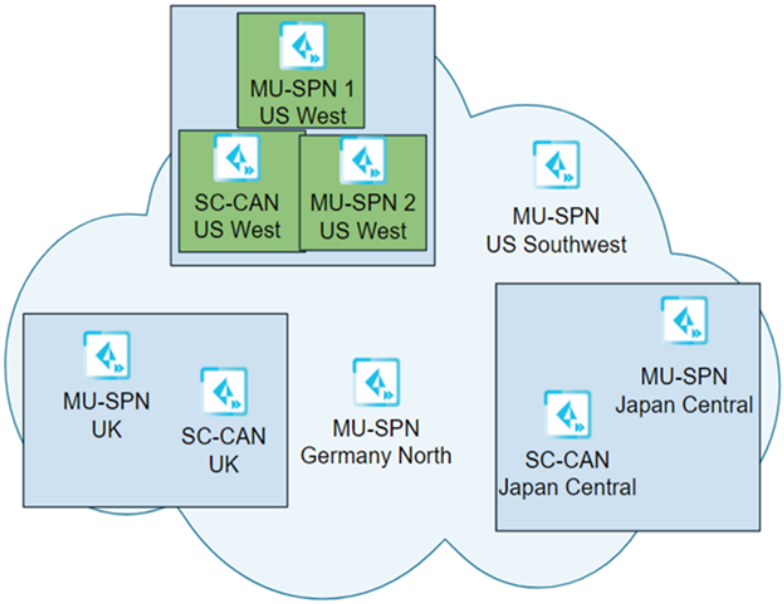
資料平面升級範例

下列範例顯示了行動使用者部署的資料平面升級程序範例，其中有五個閘道 (MU-SPN) 和三個 SC-CAN。由於自動調整事件，美國西部位置具有兩個 MU-SPN（在大量行動使用者登入該位置後新增了一個額外的 MU-SPN）。




在此範例中，您首先選取了要升級的單一位置（美國西部），並要求在星期六上午 8 點至中午 12 點的四小時升級時段進行升級。

在第一個升級周末（第 1 階段）上，美國西部位置中 SC-CAN 和 MU-SPN 的升級會在上午 8 點與中午 12 點之間發生。太平洋時間星期六。

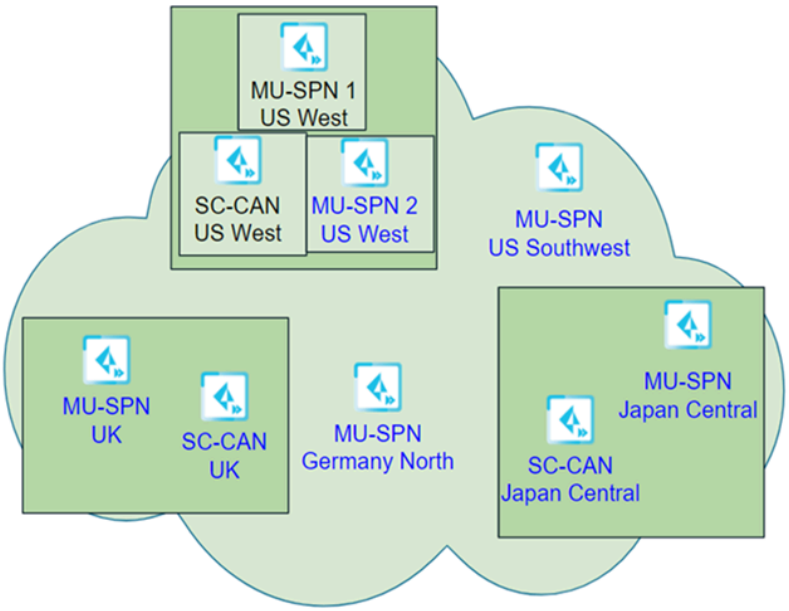



在第一個位置升級後七天，Palo Alto Networks 會使用與升級第一階段相同的四小時時段（星期六上午 8 點至下午 12 點）升級剩餘的元件（第 2 階段）。


©2025 Palo Alto Networks, Inc.

在此範例中，Prisma Access 會在升級資料平面時使用下列時區資訊：

- 日本中部 MU-SPN 和 SC-CAN 使用日本當地時間進行升級。
- 英國 MU-SPN 和 SC-CAN 使用英國當地時間進行升級。
- 美國西南 MU-SPN 使用太平洋時間進行升級。





©2025 Palo Alto Networks, Inc.

# 取得升級警示和更新

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

若要隨時掌握資料平面升級的升級排程，以及若要選取您的升級偏好設定，您必須使用 Strata Cloud Manager 訂閱 Prisma Access 通知。Strata Cloud Manager 會使用電子郵件警示，通知您升級發生的兩個週末日期；您可以選取要先升級的一或多個位置，以及要用於升級的四小時時段。

升級開始後，您也可以使用 Strata Cloud Manager 監控升級的狀態，下列步驟所示。

**STEP 1 |** 從 Strata Cloud Manager 註冊警示通知。

**STEP 2 |** 檢查您的通知以了解即將進行的資料平面升級；然後，使用下列其中一種方法，選取您的升級偏好設定。

- 選取 **Workflows**（工作流程） > **Software Upgrades**（軟體升級） > **Prisma Access** > **Upgrade Preferences**（升級偏好設定）。

  即會顯示升級儀表板。




- 登入 Strata Cloud Manager、檢視頁面頂部的橫幅以取得您的排程升級，然後選取 **Click here**（按一下這裡）。
- 檢查您的電子郵件是否有排程升級的通知，然後按一下電子郵件中的超連結。
- 選取 **Workflows**（工作流程） > **Software Upgrades**（軟體升級） > **Prisma Access** > **Upgrade Preferences**（升級偏好設定）。

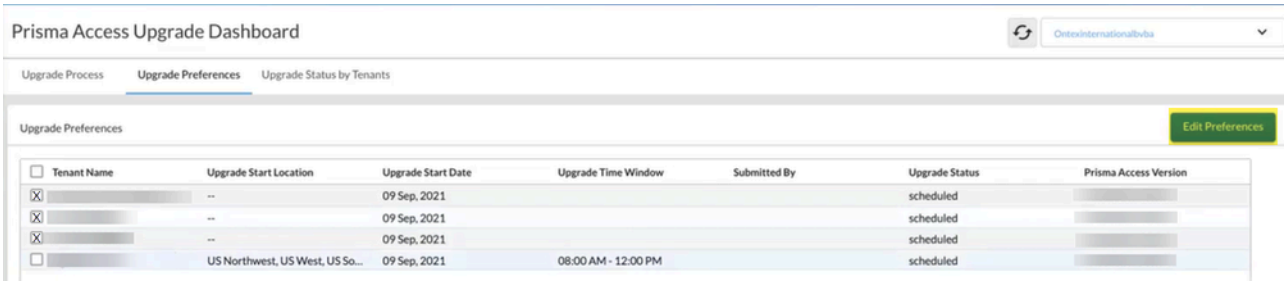
**STEP 3 |** （選用）請閱讀升級程序，以進一步了解升級程序的運作方式。


©2025 Palo Alto Networks, Inc.

**STEP 4 |** 選取您的 **Upgrade Preferences**（升級偏好設定）。

如果您有多租用戶部署，則所有租用戶都會顯示在此區域中。如果您已為部署選取升級偏好設定，這些選項會顯示在這裡。

1. 選取要為其設定升級偏好設定的租用戶，然後選取 **Edit Preferences**（編輯偏好設定）。



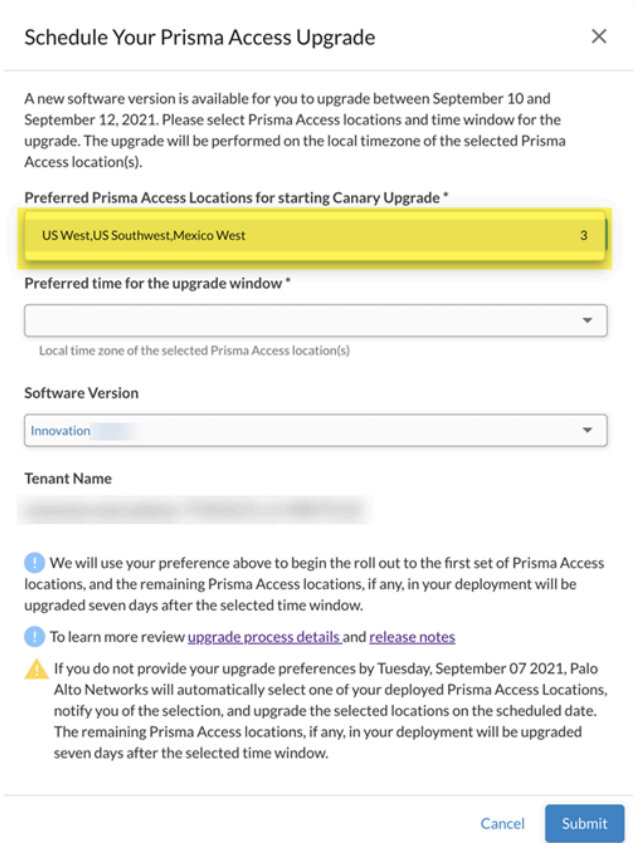

2. 選取您要先升級的 **Preferred Prisma Access Locations**（偏好 **Prisma Access** 位置）。

   *Palo Alto Networks* 強烈建議您選取反映整個部署的位置。例如，如果您有行動使用者、服務連線和遠端網路部署，請選取具有所有部署類型的位置。

   從下拉式清單中的選項中選取。

   - Prisma Access 僅顯示您已部署行動使用者、遠端網路、服務連線或其任何組合的位置。
   - 下拉式清單中的群組屬於相同的計算位置。

   當位置升級時，Prisma Access 將透過電子郵件警示通知您。





©2025 Palo Alto Networks, Inc.

在成功升級第一組 Prisma Access 位置之後，Prisma Access 團隊會監控這些位置七天，然後升級所有剩餘的 Prisma Access 位置。選取單一位置或少量位置，您有機會在一周後升級其餘位置之前監控這些位置。

如果下拉式清單中沒有顯示任何位置，表示您選取了多個沒有部署通用位置的租用戶，或是您尚未為所選租用戶新增任何位置。

3. 從可用選項清單中選取 **Preferred time for the upgrade window**（偏好的升級時段）。

   從以下升級時段中進行選擇。時段是正要升級的一或多個位置的當地時間，並且全部為四小時時段：

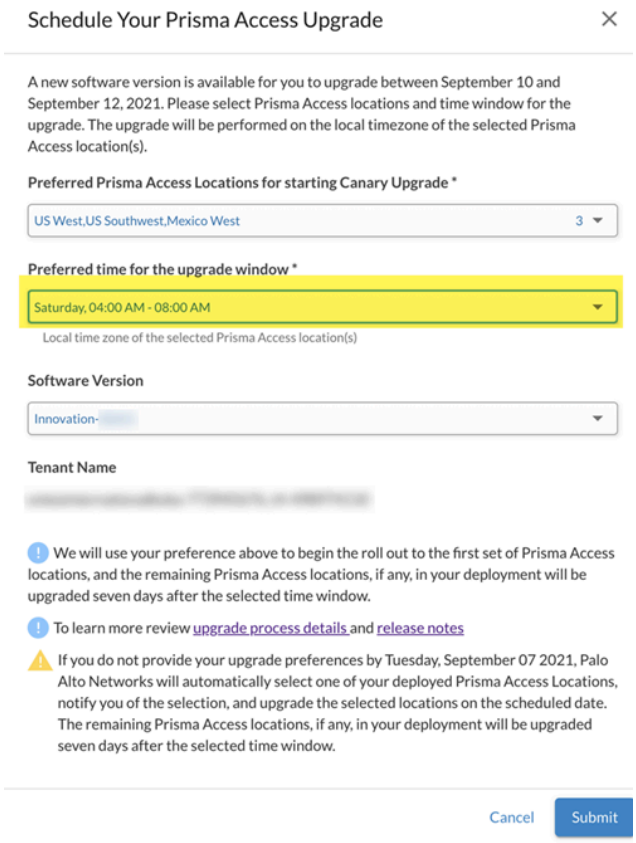
   - 星期五下午 8 點至凌晨 12 點（午夜）
   - 星期六凌晨 12 點（午夜）至凌晨 4 點
   - 星期六凌晨 4 點至上午 8 點
   - 星期六上午 8 點至中午 12 點（中午）
   - 星期六中午 12 點（中午）至下午 4 點
   - 星期六下午 4 點至晚上 8 點

   Palo Alto Networks 會使用您的偏好設定，在您選取的一或多個 Prisma Access 位置開始推出。服務將選擇排程開始日期前七天發生的最後一次提交進行升級。如果您進行變


©2025 Palo Alto Networks, Inc.

更，您所做的變更可能最多需要 30 分鐘才會顯示在洞察上的升級儀表板中。當 Prisma Access 已處理並完成變更時，系統將透過電子郵件警示通知您。

如果您在排程升級時段前七天未提供升級偏好設定，*Palo Alto Networks* 將自動選取第一組您已部署 *Prisma Access* 位置、通知您選取項目，並在排程日期升級所選位置。部署中的剩餘 *Prisma Access* 位置 (如果有的話) 將在選取的時段後七天升級。




4. 如果有多個版本可用，請選取您要升級至的軟體版本。
5. **Submit**（提交）您的變更。


©2025 Palo Alto Networks, Inc.

**STEP 5 |** 開始推出後，請選取 **Workflows**（工作流程） > **Software Upgrades**（軟體升級） > > **Prisma Access** > **Upgrade Status by Tenants**（依租用戶劃分的升級狀態），然後檢視 **Upgrade Status by Location**（依位置劃分的升級狀態）。

此頁面為每個正在升級的位置顯示下列資訊：

- 正在升級的租用戶名稱。
- 升級程序的開始和結束日期。
- 租用戶正在升級至的資料平面版本。
- 偏好的升級時段。
- 正在升級的初始位置。
- 將升級其餘位置的日期。

此外，有一個表格顯示要升級的位置、升級的開始日期和時段，以及用於升級的時區。**Upgrade Status**（升級狀態）欄提供您下列資訊：

| 升級狀態 | 說明 |
|---|---|
| 已排程 | 資料平面升級已排程。 |
| 已開始 | 升級已開始。 |
| 進行中 | 資料平面升級進行中。 |
| 重試中 | 資料平面升級未成功完成，但 Prisma Access 會繼續使用較舊的資料平板版本進行操作。在周末維護時段到期之前，Prisma Access 會重新嘗試升級。 |
| 成功 | 升級成功完成。 |

**STEP 6 |** 在第一組位置已完成資料平面升級之後，請監控升級的位置，並執行連線、效能、路由和記錄測試，以確保它們成功升級。

**STEP 7 |** 當第二組位置排程升級時，請選取 **Workflows**（工作流程） > **Software Upgrades**（軟體升級） > **Prisma Access** > **Upgrade Status by Tenants**（依租用戶劃分的升級狀態），來監控這些位置並檢查其狀態。

Prisma Access 會在資料平面升級完成之後，傳送您一則電子郵件通知。

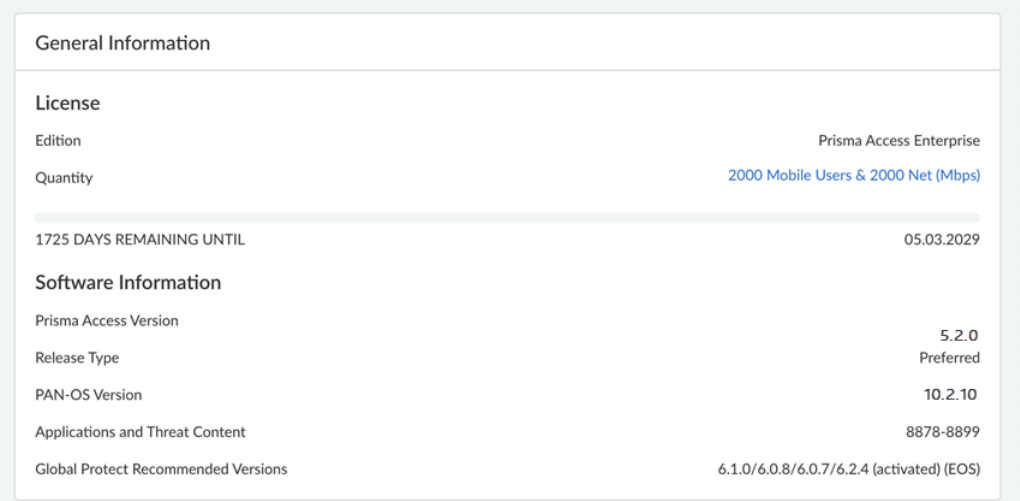

©2025 Palo Alto Networks, Inc.

# 檢視 Prisma Access 軟體版本

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

## Prisma Access (Managed by Strata Cloud Manager)

您可以在 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概要） > **General Information**（一般資訊）中尋找軟體和內容版本資訊。選取 **Prisma Access** 設定範圍。




[General Information（一般資訊）] 頁面為您提供以下資訊：

| 區塊 | 說明 |
| --- | --- |
| 租戶 **ID** | 允許您分享聯絡資訊（公司名稱、聯絡人姓名、電子郵件和電話號碼），以便可以就 Palo Alto Networks 服務升級事宜與您聯絡。<br>租用戶的 ID。 |
| 租用戶名稱 | 租用戶的名稱。 |
| 地區 | 租用戶的區域。 |
| **Prisma Access** 版本 | 目前 Prisma Access 版本 |
| **PAN-OS** 版本 | 您的資料平面正在執行的 PAN-OS 版本。資料平面是 Prisma Access 基礎結構的元件，可對 |


©2025 Palo Alto Networks, Inc.

| 區塊 | 說明 |
| --- | --- |
| | 您的網路和使用者流量啟用流量檢查和政策強制執行。 |
| 發佈類型 | 您正在執行的版本類型（Preferred 或 Innovation）。<br>Innovation 版本需要比 Preferred 版本更高的 PAN-OS 資料平面。 |
| 應用程式和威脅內容 | 您正在執行的應用程式和威脅內容更新版本。 |

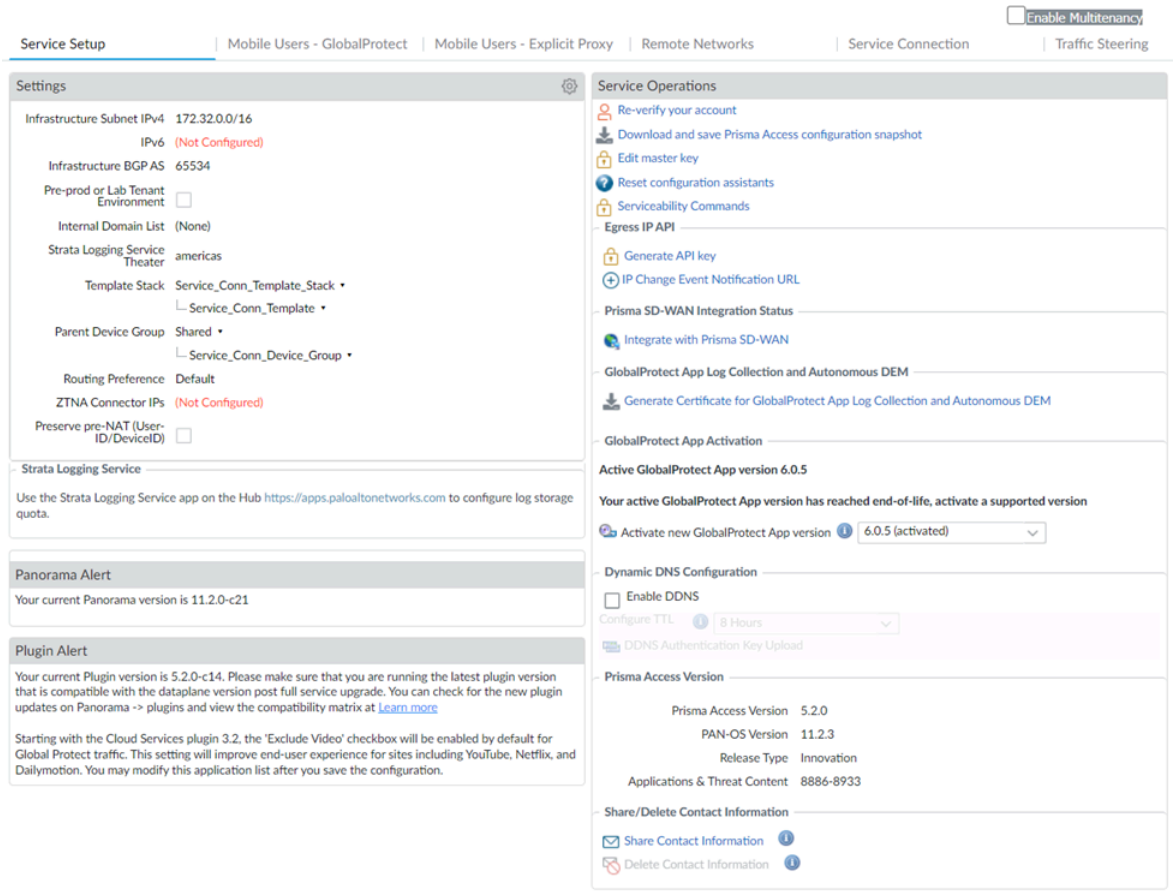
## Prisma Access (Managed by Panorama)

Prisma Access 包括您管理的元件（例如 Panorama 和雲端服務外掛程式）、Prisma Access 管理的元件（例如資料平面版本），以及 Prisma Access 管理但您可以控制其版本的元件（託管於 Prisma Access 入口網站的 GlobalProtect 版本）。[Service Setup（服務設定）] 頁面（**Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定））以單一頁面為您顯示這些元件的狀態。此頁面還包含通知，為您顯示目前正在執行的 Panorama 版本和外掛程式版本何時將終止支援 (EoS) 與 Prisma Access 搭配使用。Palo Alto Networks 會提前通知您 EoS 日期，以便您的組織有足夠的時間來規劃升級。

所有日期均採用國際標準時間 *(UTC)*。

[Service Setup（服務設定）] 頁面為您提供以下資訊：


©2025 Palo Alto Networks, Inc.




| 區塊 | 說明 |
|---|---|
| **Panorama** 警示 | 顯示您目前正在執行的 Panorama 版本。**Upgrade requirements**（升級需求）區域為您提供 Panorama 版本的相關資訊，包括目前相容的 Panorama 版本達到其對管理 Prisma Access 終止支援 (EoS) 的日期。使用此資訊在 EoS 日期之前規劃您的 Panorama 升級。 |
| 外掛程式警示 | 顯示目前在管理 Prisma Access 的 Panorama 上安裝的雲端服務外掛程式。**Upgrade requirements**（升級需求）區域為您提供下一個外掛程式版本的發行日期、升級到下一個外掛程式的截止日期，以及您無法使用早期外掛程式版本進行變更和提交的日期。使用此資訊來規劃下一次雲端服務外掛程式升級。 |
| **Prisma SD-WAN** 整合狀態 | 選取 **Integrate with Prisma SD-WAN**（與 **Prisma SD-WAN** 整合），以啟動 CloudBlade 精簡型用戶端，允許 Prisma SD-WAN 與 Prisma Access 之間的功能。 |


©2025 Palo Alto Networks, Inc.

| 區塊 | 說明 |
| --- | --- |
| **GlobalProtect** 應用程式日誌收集和自發 **DEM** | 如果您已啟用收集 GlobalProtect 應用程式日誌進行故障排除，或若要為行動使用者啟用自主數位體驗管理 (ADEM)，請按一下 **Generate Certificate for GlobalProtect App Log Collection and Autonomous DEM**（為 **GlobalProtect** 應用程式日誌收集和自發 **DEM** 產生憑證）以產生憑證。此憑證允許 GlobalProtect 應用程式透過 Strata Logging Service（收集日誌）和自發 DEM 進行驗證。當您產生憑證時，Prisma Access 也會在 **Shared**（共用）的 **Mobile_User_Template** 範本下將該憑證下載到 Panorama **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證）中的 **Device Certificates**（裝置憑證），以推送至行動裝置。 |
| **GlobalProtect** 應用程式啟動 | 顯示目前正在執行（作用中）的 GlobalProtect 應用程式版本，行動使用者可以從 Prisma Access 入口網站下載，並為您顯示可以升級到的可用 GlobalProtect 應用程式版本。 |
| 動態 **DNS** 設定 | 顯示您是否已啟用動態 DNS (DDNS) 以進行遠端網路疑難排解。 |
| **Prisma Access** 版本 | 目前 Prisma Access 版本 |
| **PAN-OS** 版本 | 您的資料平面正在執行的 PAN-OS 版本。資料平面是 Prisma Access 基礎結構的元件，可對您的網路和使用者流量啟用流量檢查和政策強制執行。 |
| 發佈類型 | 您正在執行的版本類型（Preferred 或 Innovation）。<br>Innovation 版本需要比 Preferred 版本更高的 PAN-OS 資料平面。 |
| 應用程式和威脅內容 | 您正在執行的應用程式和威脅內容更新版本。 |
| 分享/刪除聯絡資訊 | 允許您分享聯絡資訊（公司名稱、聯絡人姓名、電子郵件和電話號碼），以便可以就 Palo Alto Networks 服務升級事宜與您聯絡。<br>如果您先前輸入過聯絡資訊，則可以刪除在此區域輸入的資訊。 |


©2025 Palo Alto Networks, Inc.

| 區塊 | 說明 |
| --- | --- |
| | 請勿在聯絡資訊區域使用以下任何特殊字元：<br>• "（雙引號）<br>• '（撇號）<br>• <（小於符號）<br>• >（大於符號）<br>• & |


©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

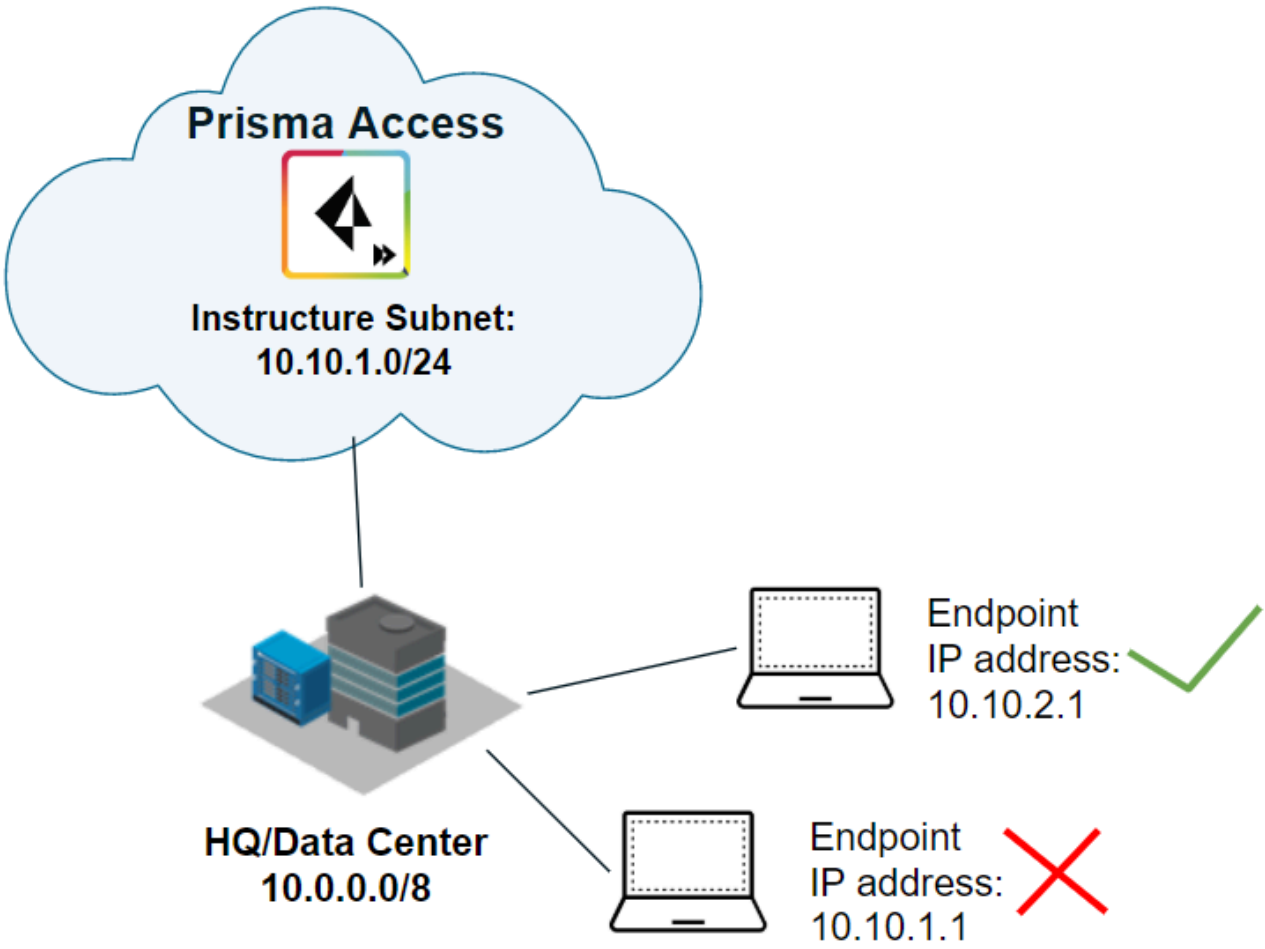
# Prisma Access 設定

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

在新增基礎結構子網路時，請遵循下列建議和需求：

- 您可以為 Prisma Access 從組織 IP 位址集區中的現有超級網路指派基礎結構子網路，但不要為了現有網路中的任何其他用途從基礎結構子網路指派任何 IP 位址。

  以下範例顯示了您從現有超級網路 10.0.0.0/8 指派的 Prisma Access 基礎結構子網路 10.10.1.0/24。將 10.10.1.0/24 指派為基礎結構子網路之後，您的組織無法使用該子網路中的任何 IP 位址。例如，您可以將 10.10.2.1 指派給端點，但不允許 10.10.1.1，因為該 IP 位址是基礎結構子網路的一部分。



- 如果為基礎結構子網路建立新的子網路，請使用不與內部使用的其他 IP 位址重疊的子網路。
- （建議）使用符合 RFC 1918 規範的子網路。雖然使用不符合 RFC 1918 和 RFC 6598 規範的（公用）IP 位址是可行的，但我們不建議這麼做，因為可能會與網際網路公用 IP 位址空間發生衝突。
- 請勿指定與下列 IP 位址和子網路重疊的任何子網路，因為 Prisma Access 會保留這些 IP 位址和子網路供內部使用。
  - 169.254.0.0/16
  - 100.64.0.0/10
- 此子網路無法與 IP 位址集區重疊，您計劃將這些集區用於為行動使用者部署指派的位址集區。
- 因為服務基礎結構可能非常大，所以您必須至少指定一個 /24 子網路。

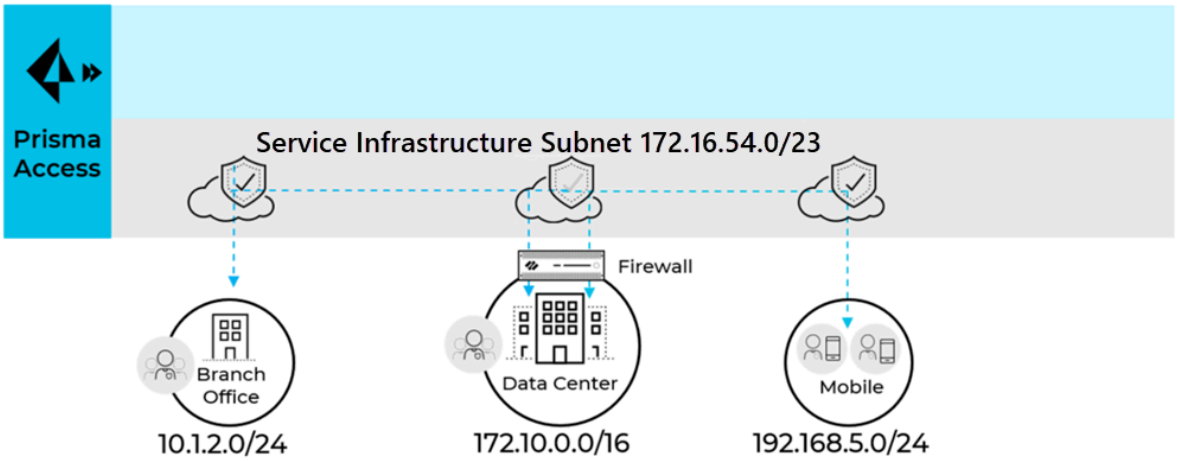

©2025 Palo Alto Networks, Inc.

# 設定 Prisma Access

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

在可以使用 Prisma Access 保護您的遠端網路和行動使用者之前，請設定基礎結構子網路。Prisma Access 會使用此子網路內的 IP 位址，在您的遠端網路位置、行動使用者、總部和資料中心（如果適用）之間建立網路。Prisma Access 也會使用服務連線，從您的總部或資料中心位置存取內部資源。

此子網路將成為您現有網路的延伸。因此，它不應與您網路中的任何現有 IP 子網路重疊。以下範例顯示了一個 172.16.54.0/23 子網路，用於 Prisma Access 基礎結構子網路。




對於少於 50 個網站和少於 2500 個行動使用者的小型網路，請考慮使用 /24 子網路。對於少於 100 個網站和少於 5000 個行動使用者的中型網路，請考慮使用 /23 子網路。在大多數情況下，/23 子網路就足夠了。如果網站超過 100 個或行動使用者超過 5000 個，或者預期未來會增長，請聯絡 Palo Alto Networks 以評估是否需要更大的子網路大小。

瞭解如何設定 Prisma Access。

- Strata Cloud Manager
- Panorama

## 設定 Prisma Access (Strata Cloud Manager)

以下工作流程為您提供了安裝和設定 Prisma Access 所需的摘要步驟。

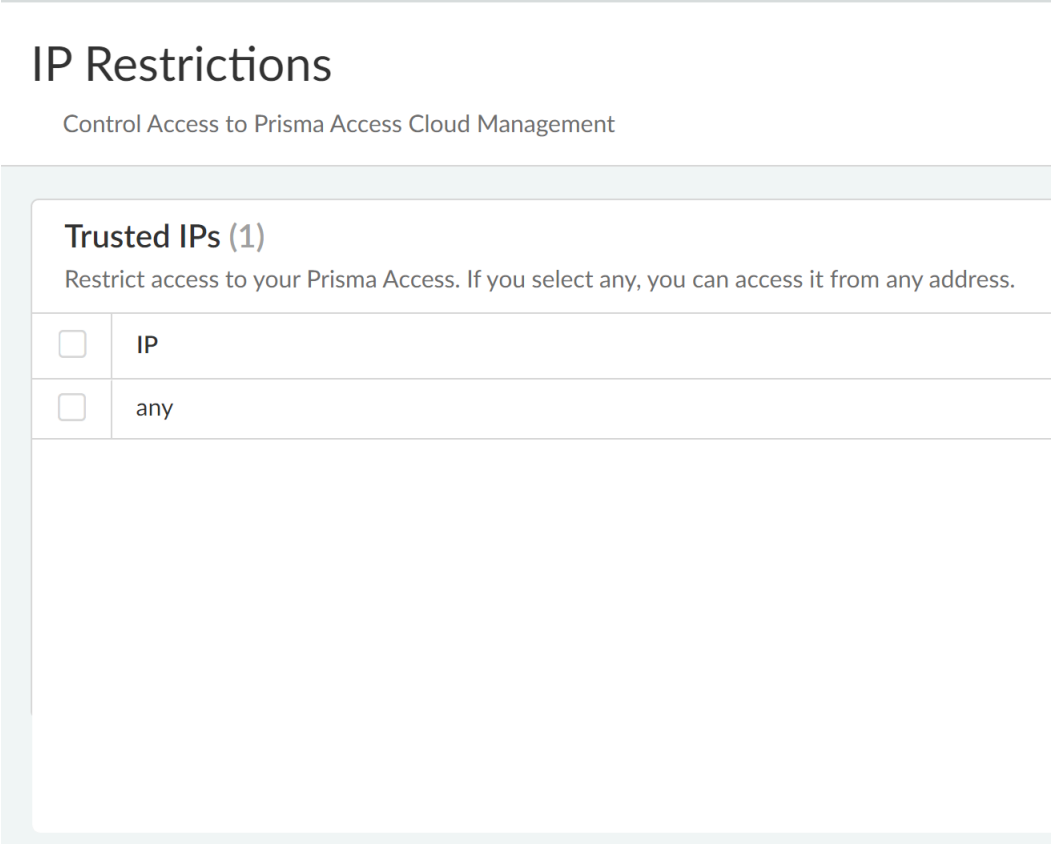
**STEP 1 |** 透過中樞啟動 Strata Cloud Manager。

1. 啟動網際網路瀏覽器並 **Sign In**（登入）中樞。
2. 啟動 Strata Cloud Manager。


©2025 Palo Alto Networks, Inc.

**STEP 2 |** 為 Prisma Access (Managed by Strata Cloud Manager) 管理員指定受信任的 IP 位址。

只有從這些來源 IP 位址登入（並且成功通過驗證）的管理員，才能存取 Prisma Access (Managed by Strata Cloud Manager)。IP 位址必須是公用位址。依預設不會強制執行任何受信任的位址（清單設定為 [any（任何）]）。若要開始，請在左側導覽面板上尋找 **Settings**（設定）功能表，然後按一下 **IP Restrictions**（**IP** 限制）。




**STEP 3 |** 識別您的授權需求；然後啟動並安裝 Prisma Access 元件。

**STEP 4 |** 啟用服務基礎結構，以及允許在 Prisma Access 元素之間進行通訊的服務連線。

**STEP 5 |** 視您部署的需要，使用 GlobalProtect 或明確 Proxy 保護行動使用者。

**STEP 6 |** 規劃、建立和設定遠端網路連線。

**STEP 7 |** （選用）將驗證方法從本機驗證變更為您組織的驗證方法。

**STEP 8 |** （選用）將日誌從 Strata Logging Service 轉送到外部 Syslog 接收器。

**STEP 9 |** （選用）檢查 Prisma Access 的狀態。

您可以擷取所有雲端服務的狀態（包括 Prisma Access 和 Strata Logging Service），以及服務執行時間的歷程記錄，方法是從中樞存取應用程式執行個體。

您也可以註冊電子郵件或簡訊通知，以便在下列情況時收到通知：規劃基礎結構更新、發生更新，以及 Palo Alto Networks® 建立、更新或解決事件。若要註冊電子郵件更新，請前往中

 ©2025 Palo Alto Networks, Inc.

樞首頁的 [Resources（資源）] 區段，然後選取 **Service Status**（服務狀態）。然後，您可以 **Subscribe**（訂閱） 雲端服務的特定更新和事件。

# 設定 Prisma Access (Panorama)

以下工作流程為您提供了安裝和設定 Prisma Access (Managed by Panorama) Access 所需的摘要步驟。

如果要在單一 *Panorama*（多租用戶）上設定一個包含多個 *Prisma Access* 執行個體的部署，請參閱 。大多數組織不需要建立和管理多個租用戶。

**STEP 1 |** 將下列 URL和連接埠新增至任何安全設備上的允許清單，而您會使用這些設備搭配管理 Prisma Access 的 Panorama 設備。

此外，如果您的 Panorama 設備使用 （**Panorama** > **Setup**（設定） > **Service**（服務） > **Proxy Server**（**Proxy** 伺服器）），或者如果您使用 SSL 正向 Proxy 搭配 Prisma Access，請務必將下列 URL 和連接埠新增至 Proxy 或 Proxy 伺服器上的允許清單。

- api.gpcloudservice.com（適用於 Prisma Access）
- api.paloaltonetworks.com（適用於 Prisma Access）
- apitrusted.paloaltonetworks.co（適用於 Prisma Access）
- Strata 記錄服務所需的 FQDN 和連接埠

如果 *Panorama* 設備與網際網路之間有 *Palo Alto Networks* 新世代防火牆，則您必須在防火牆上新增安全性政策規則，以允許 ***paloalto-logging-service*** 和 ***paloalto-shared-services*** *App-ID* 從 *Panorama* 設備傳送到網際網路。這些應用程式允許與 *Prisma Access* 以及與 *Panorama* 設備用來查詢日誌的 *Strata Logging Service* 進行 *SSL* 安全通訊。如果 *Panorama* 設備位於舊版第四層防火牆後面，請允許連接埠 *443* 和 *444* 從 *Panorama* 輸出，以允許來自 *Panorama* 的此流量。請注意，開啟第四層連接埠而不是使用 *Palo Alto Networks App-ID* 較不安全，因此不建議這樣做。

**STEP 2 |** 將 Panorama 使用的連接埠新增至您網路中的允許清單。

**STEP 3 |** 識別您的授權需求；然後啟動並安裝 Prisma Access 元件。

**STEP 4 |** 將您現有的 Panorama 設定匯入至 Prisma Access，或建立新的範本和裝置群組，以開始設定 Prisma Access。

若要將設定（例如安全性政策、驗證政策、伺服器設定檔、安全性設定檔、位址物件和應用程式群組）推送至 Prisma Access，您必須使用要推送至 Prisma Access 的設定，建立新範本和裝


©2025 Palo Alto Networks, Inc.

置群組，或者利用您現有的裝置群組和範本，方法是將它們新增至 Prisma Access 在您裝載服務時建立的範本堆疊和裝置群組階層。

Prisma Access 會建立以下範本和裝置群組，取決於您購買的項目（例如，如果您未購買明確 Proxy 授權，則看不到明確 Proxy 範本和裝置群組）：

- 範本：
  - **Explicit_Proxy_Template**
  - **Explicit_Proxy_Template_Stack**
  - **Mobile_User_Template**
  - **Mobile_User_Template_Stack**
  - **Remote_Network_Template**
  - **Remote_Network_Template_Stack**
  - **Service_Conn_Template**
  - **Service_Conn_Template_Stack**
- 裝置群組：
  - **Explicit_Proxy_Device_Group**
  - **Mobile_User_Device_Group**
  - **Remote_Network_Device_Group**
  - **Service_Conn_Device_Group**

簡化了 Prisma Access 中的設定，因為您不必設定任何基礎結構設定，例如介面和路由通訊協定。此設定是自動進行的，並從 Panorama 推送到服務自動建立的範本和裝置群組。您可以直接從外掛程式設定服務所需的任何基礎結構設定，例如建立 IPSec VPN 通道，通往遠端網路位置中支援 IPSec 的裝置。或者，您可以將範本和裝置群組階層新增到設定，以簡化服務設定。

若要簡化服務設定，請在您開始使用 Prisma Access 的設定工作之前，建立或匯入您需要的範本和裝置群組。

為 Prisma Access 建立範本和裝置群組時，您無需將受管理的裝置指派給它。相反，您會將它們新增到 Prisma Access 建立的範本堆疊和裝置群組階層。請勿將 Prisma Access 建立的任何範本或裝置群組新增至任何其他範本堆疊或裝置群組。

**STEP 5 |** 使用 Strata Cloud Manager 註冊電子郵件通知。

Prisma Access 使用來自此應用程式的通知為您提供有關服務的通知，包括任何資料平面升級。


©2025 Palo Alto Networks, Inc.

**STEP 6 |** 變更 Panorama 和雲端服務外掛程式中的預設主要金鑰。

作為安全性最佳做法，Palo Alto Networks 建議變更 Panorama 和雲端服務外掛程式中的主要金鑰，並且每月變更主要金鑰。

因為 Panorama 和 Prisma Access 主要金鑰不同步，所以 Palo Alto Networks 建議您不要在 Prisma Access 中主要金鑰亦未同步的情況下自動輪換 Panorama 中的主要金鑰。您可以使用 Panorama UI 或 API 命令變更主要金鑰。

請務必追蹤您部署的主要金鑰，因為主要金鑰無法復原。當一個主要金鑰到期時，您必須輸入目前的主要金鑰，才能設定新的主要金鑰。如果您在目前主要金鑰到期時無法提供該金鑰，則必須將 *Panorama* 設備重設為出廠預設值。

1. 變更 Panorama 中的主要金鑰。
   1. 選取 **Panorama** > **Master Key and Diagnostics**（主要金鑰與診斷）。

      請勿指定 **Current Master Key**（目前主要金鑰）。
   2. 設定 **New Master Key**（新主要金鑰） 並 **Confirm Master Key**（確認主要金鑰）。

      記下您設定的主要金鑰。
   3. 設定主要金鑰 Lifetime（生命週期） 與 Time for Reminder（提醒時間）。
   4. 按一下 **OK**（確定）。
2. 變更 Prisma Access 的主要金鑰，方法是選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Operations**（服務操作） > **Edit master key**（編輯主要金鑰），然後輸入您為 Panorama 輸入的同一主要金鑰。

您也可以使用 API 命令變更主要金鑰。這需要兩個步驟：一個變更 Panorama 主要金鑰，另一個變更 Prisma Access 主要金鑰。請使用以下 API 命令變更主要金鑰：

- Panorama:**XML API** > **Operational Commands**（操作命令） > **request**（要求） > **master-key**
- Prisma Access：**XML API** > **Operational Commands**（操作命令） > **request**（要求） > **plugins**（外掛程式） > **cloud_services** > **prisma-access** > **sync**（同步）

**STEP 7 |** 啟用服務基礎結構，以及允許在 Prisma Access 元素之間進行通訊的服務連線。

1. 計劃啟用服務基礎結構和服務連線。
2. 啟用服務基礎結構。
3. 建立服務連線以允許存取您的公司資源。

   如果不需要存取您的公司資源，您仍然應該建立服務連線，以啟用行動使用者與遠端網路之間的存取。


©2025 Palo Alto Networks, Inc.

**STEP 8 |** Prisma Access 行動使用者部署，並視您部署的需要，使用 GlobalProtect 或明確 Proxy 保護行動使用者。

若要在 Prisma Access (Managed by Panorama) 上設定 GlobalProtect：

1. 在 Mobile_User_Template 中建立兩個區域（例如，行動使用者和網際網路），並對應區域來為行動使用者設定區域。您應該將不是 Prisma Access 連線的使用者或總部或分公司的任何區域對應至 [Untrust（不信任）]。

   在 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users**（行動使用者）下，將網際網路對應至 [Untrust（不信任）]；將行動使用者對應至 [Trust（信任）]。
2. 設定驗證。

   我們建議使用本機驗證作為第一步，來驗證服務是否已設定，以及您的使用者是否可以存取網際網路。您稍後可以切換為使用貴公司驗證方法。
3. 設定裝置群組的安全性政策。

   若要建立安全性政策以允許流量流向網際網路，請選取 Mobile_User_Device_Group **Policies**（政策） > **Security**（安全性） > **Prerules**（預先規則） > **Add**（新增）一個規則。例如：行動使用者至網際網路。
4. 提交並推送您的變更以開始使用服務。
5. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Monitor**（監控） > **Mobile Users**（行動使用者），以檢視 **Status**（狀態），並驗證您是否可以 ping（偵測）入口網站 FQDN。
6. 驗證 Prisma Access 是否保護行動使用者的網際網路流量，方法是下載並安裝 GlobalProtect 應用程式、使用應用程式以行動使用者（本機使用者）身分連線到入口網站、瀏覽至網際網路上的幾個網站，然後檢查 Panorama 上的流量日誌。

若要使用明確 Proxy 保護行動使用者：

1. 閱讀 明確 Proxy 設定指導方針。
2. 設定 SAML 驗證。明確 Proxy 需要 SAML 驗證。
3. 使用雲端識別引擎設定群組對應。
4. 完成明確 Proxy 設定。
5. 提交並推送您的變更。

**STEP 9 |** 規劃、建立和設定遠端網路連線。

1. 將一個或多個遠端網路新增至 Prisma Access。

   您可以裝戴一個位置，然後使用大量匯入功能新增其他位置。
2. 建立安全性政策規則，以允許從遠端網路到總部的流量（例如：信任至信任）。
3. 驗證服務連線、遠端網路連線與行動使用者之間的連線。

**STEP 10 |** 執行用來擷取 Prisma Access IP 位址的 API 指令碼和使用舊版指令碼擷取行動使用者 IP 位址。

您可以將這些位址新增至組織網路上的允許清單，以限制對企業網路和應用程式的輸入存取。

 ©2025 Palo Alto Networks, Inc.

**STEP 11 |** （選用）將驗證方法從本機驗證變更為您組織的驗證方法。

1. 建立符合您組織需的驗證設定檔 （SAML、LDAP、RADIUS 等）。
2. 如果您的組織使用內部部署驗證伺服器（例如 RADIUS 或 Active Directory），請將 Prisma Access 針對內部要求用作其來源 IP 位址 (擷取 Prisma Access 的 IP 位址) 的 IP 位址新增至您網路中的允許清單，或允許整個基礎結構子網路的 IP 位址（Prisma Access 會從這個子網路取得回送 IP 位址）。
3. 更新 Prisma Access 入口網站和閘道的驗證設定檔，以使用此新的驗證設定檔。

**STEP 12 |** （選用）將日誌從 Strata Logging Service 轉送到外部 Syslog 接收器。

 ©2025 Palo Alto Networks, Inc.

# 設定 Prisma Access 服務基礎結構

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ **Pre-prod or Lab Tenant**（前置生產或實驗室租用戶）的最低必要 Prisma Access 版本：3.0-Preferred |

Prisma Access 會使用此子網路建立網路主幹，用來聯繫分支網路、行動使用者與 Prisma Access 安全性基礎架構，以及您計劃要透過服務連線連線到 Prisma Access 的總部和資料中心網路。

若要啟用在遠端網路位置、行動使用者以及您計劃透過服務連線連線來連線至 Prisma Access 的總部或資料中心之間進行通訊，請設定服務基礎結構子網路。Prisma Access 會使用此子網路建立網路骨幹，在分公司網路、行動使用者和 Prisma Access 安全基礎結構之間進行通訊，以及與您計劃透過服務連線來連線至 Prisma Access 的總部和資料中心網路進行通訊。

- Strata Cloud Manager
- Panorama

## 設定 Prisma Access 服務基礎結構 (Strata Cloud Manager)

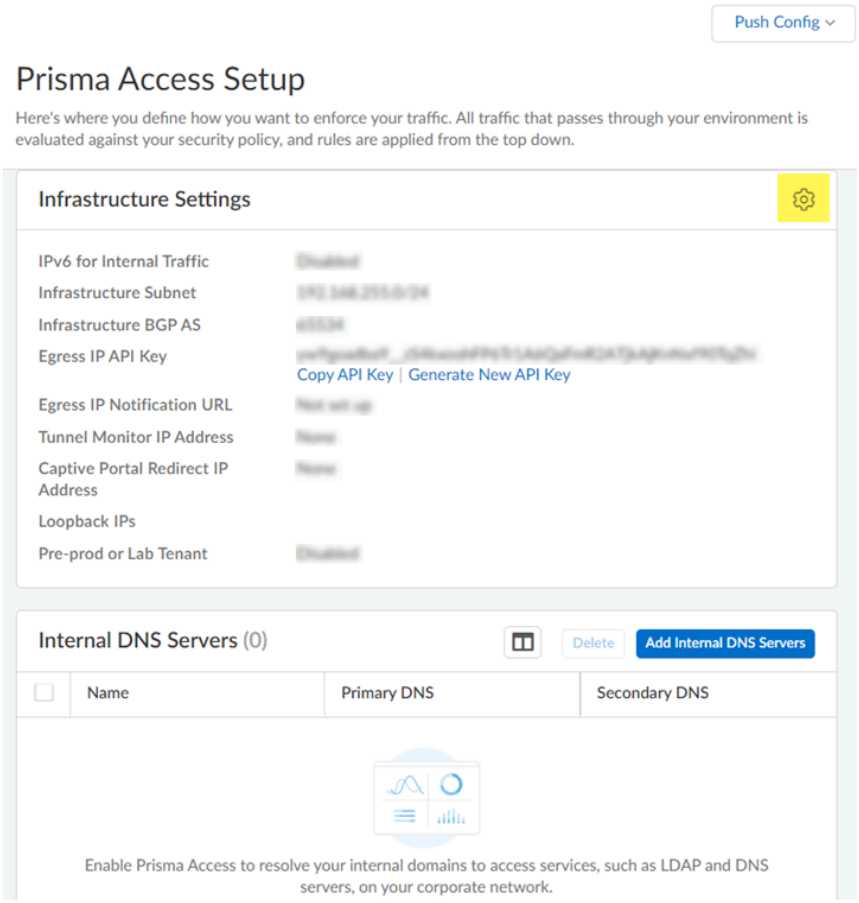
在為 Prisma Access 新增基礎結構子網路時，請遵循下列建議和需求：

- ❑ 使用符合 RFC 1918 規範的子網路。雖然使用不符合 RFC 1918（公用）IP 位址是可行的，但不建議使用，因為可能會與網際網路公用 IP 位址空間發生衝突。
- ❑ 請勿指定任何與 169.254.0.0/16 和 100.64.0.0/10 子網路範圍重疊的子網路，因為 Prisma Access 會保留這些 IP 位址和子網路供內部使用。
- ❑ 此子網路是現有網路的延伸，因此不可與您在公司網路中使用的任何 IP 子網路重疊，或是與您為 Prisma Access for Users 或 Prisma Access for Networks 指派的 IP 位址集區重疊。
- ❑ 由於服務基礎架構需要大量 IP 位址，因此您必須指定 /24 子網路（例如，172.16.55.0/24）。
- ❑ 如果您對遠端網路或服務連線使用動態路由，則也必須設定符合 RFC 6996 規範的 BGP 私人 AS 編號。

**STEP 1 |** 啟動 Prisma Access。


©2025 Palo Alto Networks, Inc.

**STEP 2 |** 前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Prisma Access** > **Infrastructure Settings**（基礎結構設定），然後按一下齒輪以編輯設定。




**STEP 3 |** 輸入一個 **Infrastructure Subnet**（基礎結構子網路），Prisma Access 可以將其用來在您的遠端網路位置、行動使用者，以及您計劃透過服務連線來連線到 Prisma Access 的總部或資料中心之間啟用通訊。

> 將符合 *RFC 1918* 規範的子網路用於基礎架構子網路。雖然使用不符合 *RFC 1918*（公用）*IP* 位址是可行的，但不建議使用，因為可能會與網際網路公用 *IP* 位址空間發生衝突。

**STEP 4 |** （選用）如果您是設定 IPv6，請選取 **IPv6 for Internal Traffic**（內部流量的 **IPv6**），然後選取 IPv6 子網路。

**STEP 5 |** 輸入您想要在 Prisma Access 基礎結構內使用的 **Infrastructure BGP AS**（基礎結構 **BGP AS**）。

如果您想要啟用動態路由，以便 Prisma Access 可以動態探索遠端網路和總部或資料中心裡資源的路由，您必須使用邊界閘道通訊協定 (BGP)。**Infrastructure BGP AS**（基礎結構 **BGP**

 ©2025 Palo Alto Networks, Inc.

**AS**）是自發系統 (AS) 編號，用於識別 BGP 可以透過其傳送流量的路由。如果您未提供 AS 編號，Prisma Access 會使用預設 AS 編號 (65534)。

如果想要指定自己的 AS 編號，則必須使用符合 RFC 6996 規範的私人 AS 編號。接受的格式為 4 位元組 AS Plain [64512-65534]、[4200000000-4294967294] 或 AS Dot [0.64512-0.65534], [64086.59904-65535.65534] 標記法。

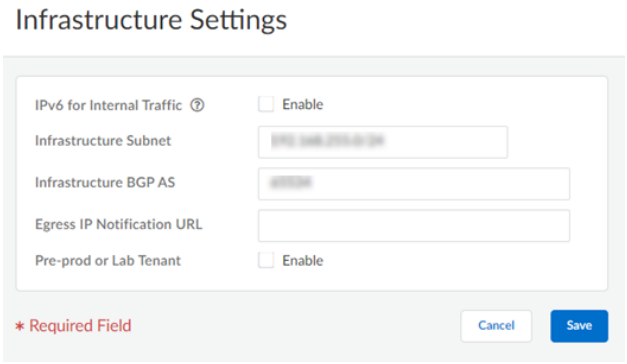
**STEP 6 |** 如果您啟用使用者根據來源 IP 位址存取應用程式，將需要取得流量來源的 IP 位址清單，Prisma Access 會將這些 IP位址用作來源位址，以便您可以在應用程式存取政策中允許它們。

**Copy**（複製）**Egress IP API Key**（輸出 **IP API** 金鑰），以啟用 Prisma Access 輸出 IP 位址 API 的使用。此外，因為 Prisma Access 使用的 IP 位址定期變更—例如，當您新增位置時、當 Prisma Access 需要調整現有位置的資源，或當有基礎結構升級時—您需要知道 IP 位址何時變更，以便您可以更新政策規則，或透過定義 **Egress IP Notification URL**（輸出 **IP** 通知 **URL**）自動進行這些更新。如需更多詳細資訊，請參閱擷取 Prisma Access 的 IP 位址。

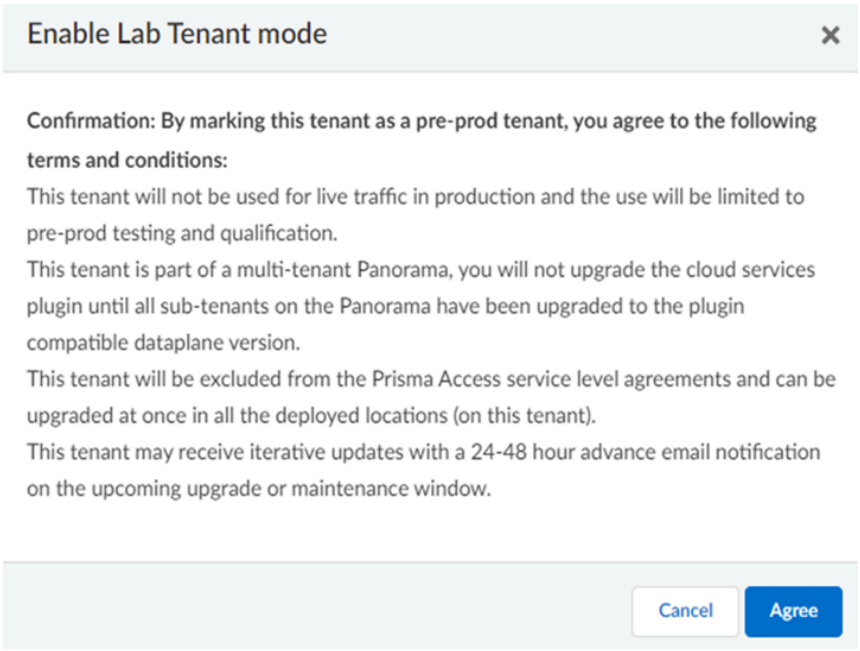

©2025 Palo Alto Networks, Inc.

**STEP 7 |** （選用）啟用租用戶作為前置生產或實驗室租用戶。

1. **Enable**（啟用）租用戶作為 **Pre-prod or Lab Tenant**（前置生產或實驗室租用戶）。




2. **Agree**（同意）確認。




啟用租用戶作為前置生產或實驗室租用戶時，您可以在升級其他生產租用戶之前單獨排程此租用戶的升級。租用戶會在即將進行升級前 24 至 48 小時收到通知。從前置生產或實驗室租用戶中停用租用戶時，它會被視為生產租用戶。

3. **Save**（儲存）變更。

 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** 若要啟用 Prisma Access 解析您的內部網域，請 **Add Internal DNS Servers**（新增內部 **DNS** 伺服器）。

如果您打算設定服務連線，以啟用對您公司網路中資源的存取，並且您還需要 Prisma Access 解析您的內部網域，則必須定義內部網域清單。對內部網域清單所含網域的 DNS 查詢會傳送至您的本機 DNS 伺服器，以確保資源可供 Prisma Access 遠端網路使用者和行動使用者使用。

1. 輸入 Prisma Access 應用來解析內部網域名稱的 **Primary DNS**（主要 **DNS**）伺服器和 **Secondary DNS**（次要 **DNS**）伺服器。
2. **Add**（新增）您想要 Prisma Access 解析的內部 **Domain Names**（網域名稱）。

   您可以在網域清單中的網域前面使用萬用字元 (*)，例如 *.acme.local 或 *.acme.com。

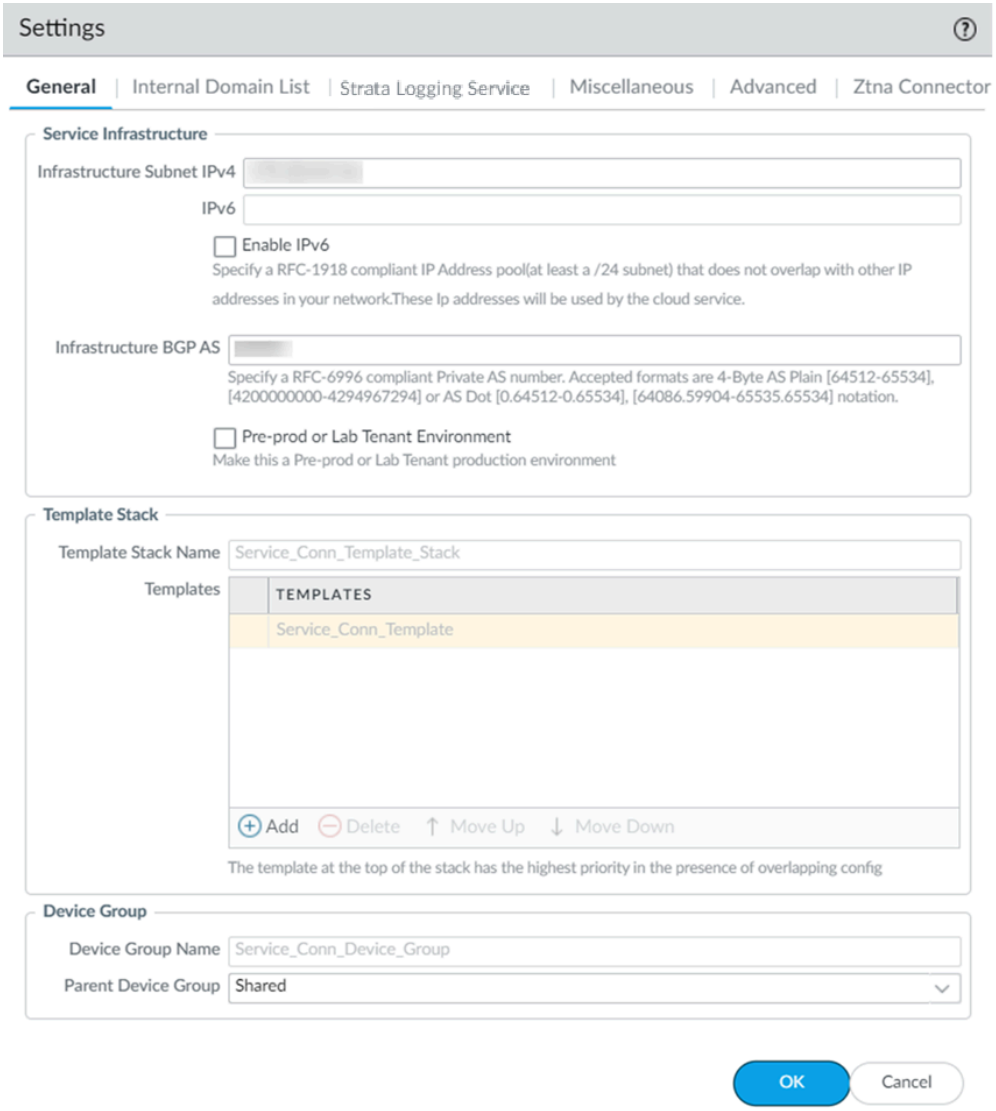
**STEP 9 |** **Push Config**（推送設定）以將您的服務基礎結構設定儲存到 Prisma Access。

## 設定 Prisma Access 服務基礎結構 (Panorama)

在開始設定 Prisma Access 以保護您的遠端網路和/或行動使用者之前，您必須設定基礎結構子網路，Prisma Access 會將其用來建立網路骨幹，在您的服務連線、遠端網路和行動使用者之間進行通訊，以及與您計劃透過服務連線來連線至 Prisma Access 的公司網路通訊。因為設定基礎結構需要大量 IP 位址，所以您必須至少使用 /24 子網路（例如 172.16.55.0/24）。請務必遵循所有指導方針和需求。

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定），然後按一下齒輪圖示以編輯設定。




**STEP 2 |** 在 **General**（一般）頁籤上，指定滿足需求的 **Infrastructure Subnet**（基礎結構子網路），例如，172.16.55.0/24。

**STEP 3 |** （選用）如果您是設定 IPv6，請選取 **IPv6 for Internal Traffic**（內部流量的 **IPv6**），然後選取 IPv6 子網路。

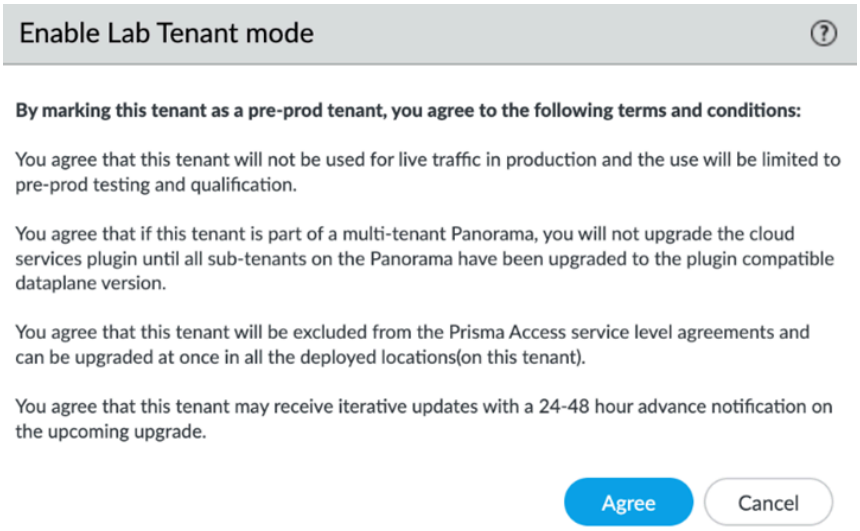
**STEP 4 |** （選用）如果您想要啟用 Prisma Access，以使用 BGP 動態探索遠端網路和總部/資料中心位置上資源的路由，請輸入您想要在 Prisma Access 基礎結構內使用的 **Infrastructure BGP AS**（基礎結構 **BGP AS**）。

如果未提供 AS 編號，則將使用預設 AS 編號 65534。


©2025 Palo Alto Networks, Inc.

**STEP 5 |** （選用）啟用租用戶作為 **Pre-prod or Lab Tenant Environment**（前置生產或實驗室租用戶）。

啟用租用戶作為前置生產或實驗室租用戶時，您可以在升級其他生產租用戶之前單獨排程此租用戶的升級。租用戶會在即將進行升級前 24 至 48 小時收到通知。




從前置生產或實驗室租用戶中停用租用戶時，它會被視為生產租用戶。

*Prisma Access for Clean Pipe* 不支援此功能。

 ©2025 Palo Alto Networks, Inc.

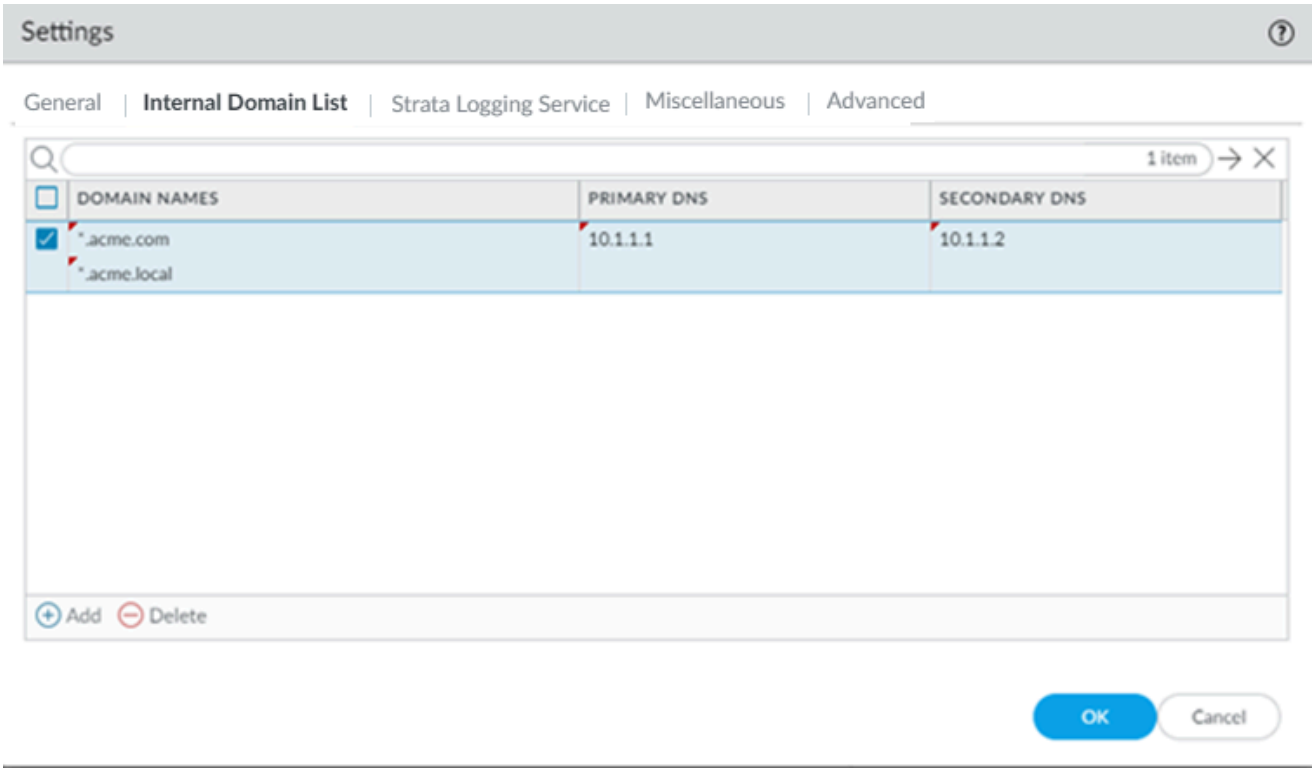
**STEP 6 |** （選用）啟用 Prisma Access 以使用公司 DNS 伺服器解析您的內部網域。

如果需要 Prisma Access 能夠解析您的內部網域，以透過服務連線存取公司網路上的服務，例如 LDAP 伺服器，請使用此步驟。例如，如果您想要公司網域的 DNS 查閱僅前往公司 DNS 伺服器，請在這裡指定公司網域和公司 DNS 伺服器。

1. 選取 **Internal Domain List**（內部網域清單）頁籤。
2. **Add**（新增）您想要 Prisma Access 用來解析內部網域名稱的 **Domain Names**（網域名稱）、**Primary DNS**（主要 **DNS**）和 **Secondary DNS**（次要 **DNS**）伺服器。

   您可以在網域清單中的網域前面使用萬用字元 (*)，例如 *.acme.local 或 *.acme.com。

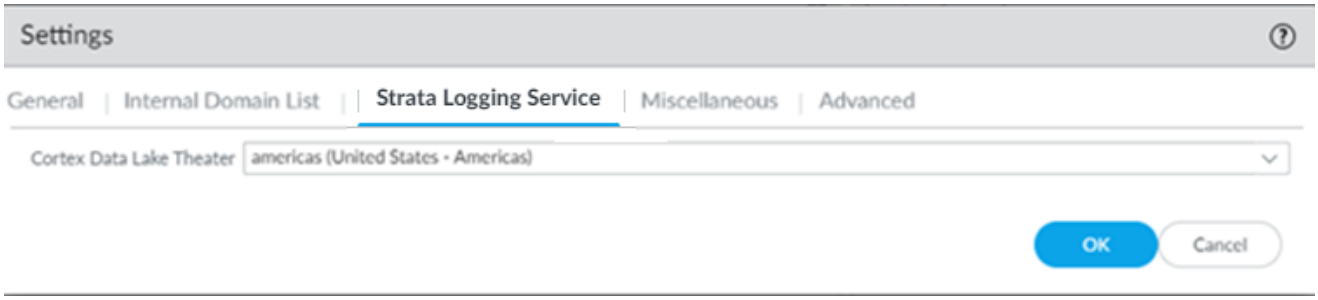
   請勿輸入 *127.0.0.1* 位址，因為它可能會導致 *Prisma Access* 內部路由問題。




 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** 啟用 Strata Logging Service。

1. 選取 **Strata Logging Service**（**Strata** 記錄服務）頁籤。
2. 選取 **Strata Logging Service Theater**（**Strata** 記錄服務劇院），並按一下 **OK**（確定）。




3. 設定您用來搭配日誌轉送設定檔將設定推送到 Prisma Access 的裝置群組，該設定檔會將所需的日誌類型轉送至 **Panorama/Strata Logging Service**（**Panorama/Strata** 記錄服務）。

   在新安裝之後或從 Prisma Access 範本堆疊中移除非 Prisma Access 範本時，雲端服務外掛程式會自動新增下列日誌設定（**Device**（裝置） > **Log Settings**（日誌設定））：

   - 系統日誌 **(system-gpcs-default)**、User-ID 日誌 **(userid-gpcs-default)**、HIP 比對日誌 **(hipmatch-gpcs-default)** 和 GlobalProtect 日誌 **(gp-prismaaccess-default)** 的日誌設定會新增至 Mobile_User_Template。
   - 系統日誌 **(system-gpcs-default)**、User-ID 日誌 **(userid-gpcs-default)** 和 GlobalProtect 日誌 **(gp-prismaaccess-default)** 的日誌設定會新增至 Remote_Network_Template。
   - 系統日誌 **(system-gpcs-default)** 和 GlobalProtect 日誌 **(gp-prismaaccess-default)** 的日誌設定會新增至 Service_Conn_Template。

   這些日誌設定會自動將系統、User-ID、HIP 比對和 GlobalProtect 日誌轉送到 Strata Logging Service。

   若要套用日誌設定變更，請執行下列步驟，然後提交並推送您的變更：

   - 若要將日誌設定套用到行動使用者範本，請選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users**（行動使用者）、按一下齒輪圖示以編輯設定，然後按一下 [OK（確定）]。
   - 若要將日誌設定套用到遠端網路範本，請選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路）、按一下齒輪圖示以編輯設定，然後按一下 [OK（確定）]。
   - 若要將日誌設定套用到服務連線範本，請選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > （服務設定）、按一下齒輪圖示以編輯設定，然後按一下 [OK（確定）]。

   為其他日誌類型啟用日誌轉送的方式取決於類型。對於根據政策比對所產生的日誌，請使用日誌轉送設定檔。如需詳細資訊，請參閱 Strata 記錄服務入門指南。


©2025 Palo Alto Networks, Inc.

**STEP 8 |** （選用）設定 **Miscellaneous**（雜項）設定。

1. （選用）對外部動態清單 (EDL) 或自訂 URL 類別中的 URL 附加結束權杖，方法是選取 **Append the ending token to the URLs in the URL filtering configuration**（將結束權杖附加至 **URL** 篩選設定中的 **UTL**）。

   如果您在 EDL 或自訂 URL 類別中使用 URL，並且未將正斜線 (**/**) 附加至 UR，則可能允許比您預期更多的 URL。例如，輸入 **`example.com`** 作為比對 URL，而不是 **`example.com/`**，也將比對 example.com.網站資訊或 example.com.br。

   透過選取 **Append the ending token to the URLs in the URL filtering configuration**（將結束權杖附加至 **URL** 篩選設定中的 **UTL**），Prisma Access 會將結束權杖設定為 EDL 或自訂 URL 類別中的 URL，這樣，如果您輸入 **`example.com`**，Prisma Access 會像對待 example.com/ 一樣對待它，並且只比對該 URL。

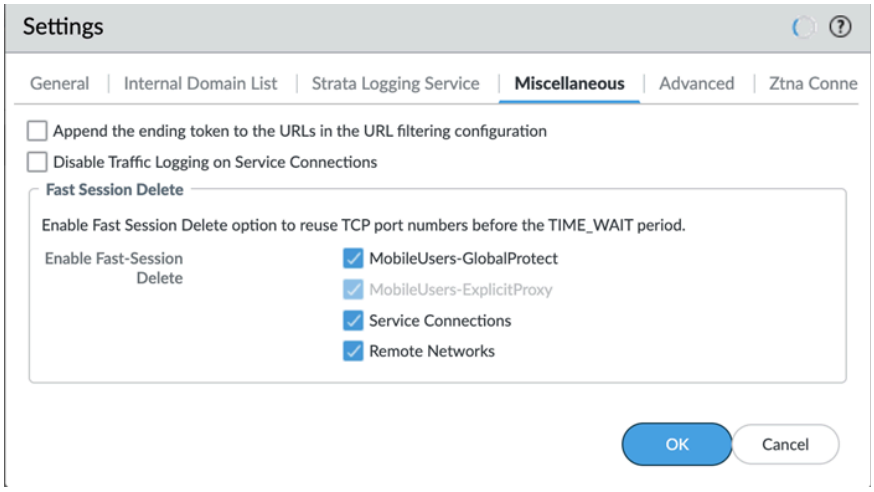
2. （選用）**Disable Traffic Logging on Service Connections**（停用服務連線上的流量記錄），以停用在用於 Prisma Access 部署的服務連線上進行記錄。

   如果服務連線記錄的大多數流量是非對稱的，則可能需要停用服務連線記錄，以減少 Strata Logging Service 記錄儲存空間的耗用。如果您的部署沒有透過服務連線的非對稱流量，則無需停用記錄。

3. （選用）若要為遠端網路、服務連線或行動使用者—GlobalProtect 部署啟用快速工作階段刪除，請選取 **Mobile Users—GlobalProtect**（行動使用者—**GlobalProtect**）、**Service Connections**（服務連線）或 **Remote Networks**（遠端網路）的核取方塊。

   快速工作階段刪除允許 Prisma Access 在 TCP TIME_WAIT 期間到期之前重複使用 TCP 連接埠號碼，並且對於可能短暫存在的 SSL 解密工作階段非常有用。

   對於行動使用者—明確 Proxy 部署，快速工作階段刪除是其功能的關鍵部分，您無法將其停用。




 ©2025 Palo Alto Networks, Inc.

**STEP 9 |** （選用）設定 **Advanced**（進階）設定（路由偏好設定、服務連線的對稱網路路徑選項，以及 HIP 重新散佈）。

1. 指定要與服務連線搭配使用的 **Routing Preference**（路由偏好設定）。

   您可以指定網路偏好設定，以使用您組織的網路或 Prisma Access 網路來處理服務連線流量。

   - **Default**（預設值）—Prisma Access 在其內部網路中使用預設路由。
   - **Hot potato routing**（熱馬鈴薯路由）—Prisma Access 儘快將服務連線流量移交給您組織的 WAN。

   變更 *Prisma Access* 服務連線路由方法需要全面瞭解您組織的拓撲和路由裝置，以及瞭解 *Prisma Access* 路由的運作方式。從預設值變更路由方法之前，我們建議您仔細閱讀 服務連線流量的路由。

2. 設定 **Backbone Routing**（骨幹路由）用於服務連線。

   根據預設，Prisma Access 骨幹要求您對透過服務連線從資料中心或總部位置返回的流量具有對稱網路路徑。如果想要將 ECMP 或另一個負載平衡機制用於來自 CPE 的服務連線，您可以透過 Prisma Access 骨幹啟用對稱流量。

   - 選取 **no-asymmetric-routing**，要求跨服務連線骨幹的對稱流量。
   - 選取 **asymmetric-routing-only**，以允許 Prisma Access 跨服務連線骨幹使用非對稱流量。
   - 如果您與某個位置有多個服務連線，則可以在 Prisma Access 部署中利用負載平衡，方法是選取 **asymmetric-routing-with-load-share**（預設設定）。不過，負載平衡是基於最佳效果完成的，如果其中一個服務連接中斷，負載平衡將失敗。

3. 使用 Prisma Access 重新散佈 HIP 資訊，使用服務連線，重新散佈來自行動使用者和遠端網路使用者的 HIP 資訊。

4. 在 Prisma Access GlobalProtect 部署中識別和隔離遭入侵裝置，讓 Prisma Access 識別並隔離遭入侵裝置，這些裝置與 GlobalProtect 應用程式連線。

5. **Withdraw Static Routes if Service Connection or Remote Network IPSec tunnel is down**（如果服務連線或遠端網路 **IPSec** 通道關閉，則撤回靜態路由）如果您想要 Prisma Access 在通道沒有備份通道的情況下關閉時移除靜態路由。

   Prisma Access 會在以下情況移除路由：

   - 主要通道關閉，沒有次要通道。
   - 如果設定了主要通道和次要通道，但兩者都關閉。

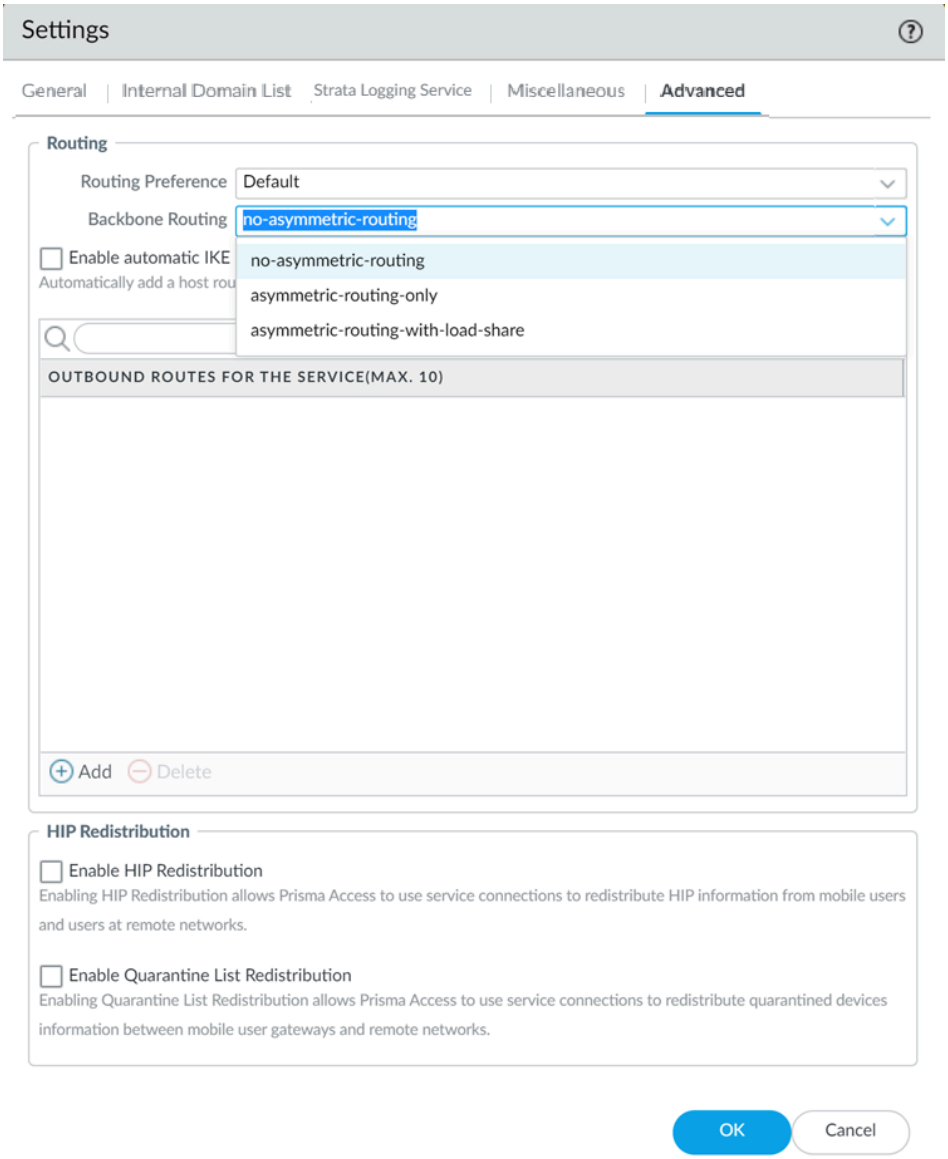
   如果未啟用通道監控，則無法套用此變更。

6. （選用）如果您想要透過網際網路將遠端網路和服務連線 IPSec 通道封包路由至靜態 IKE 閘道，請**Enable automatic IKE peer host routes for Remote Networks and Service Connections**（為遠端網路和服務連線啟用自動 **IKE** 對等主機路由）。

7. （選用）**Specify Outbound Routes for the Service (Max 10)**（指定服務的輸出路由（最多 **10** 個）），方法為新增最多 10 個首碼，而 Prisma Access 會在所有服務連線和遠端

 ©2025 Palo Alto Networks, Inc.

網路連線上為這些首碼新增靜態路由。Prisma Access 接著透過網際網路將流量路由至這些首碼。



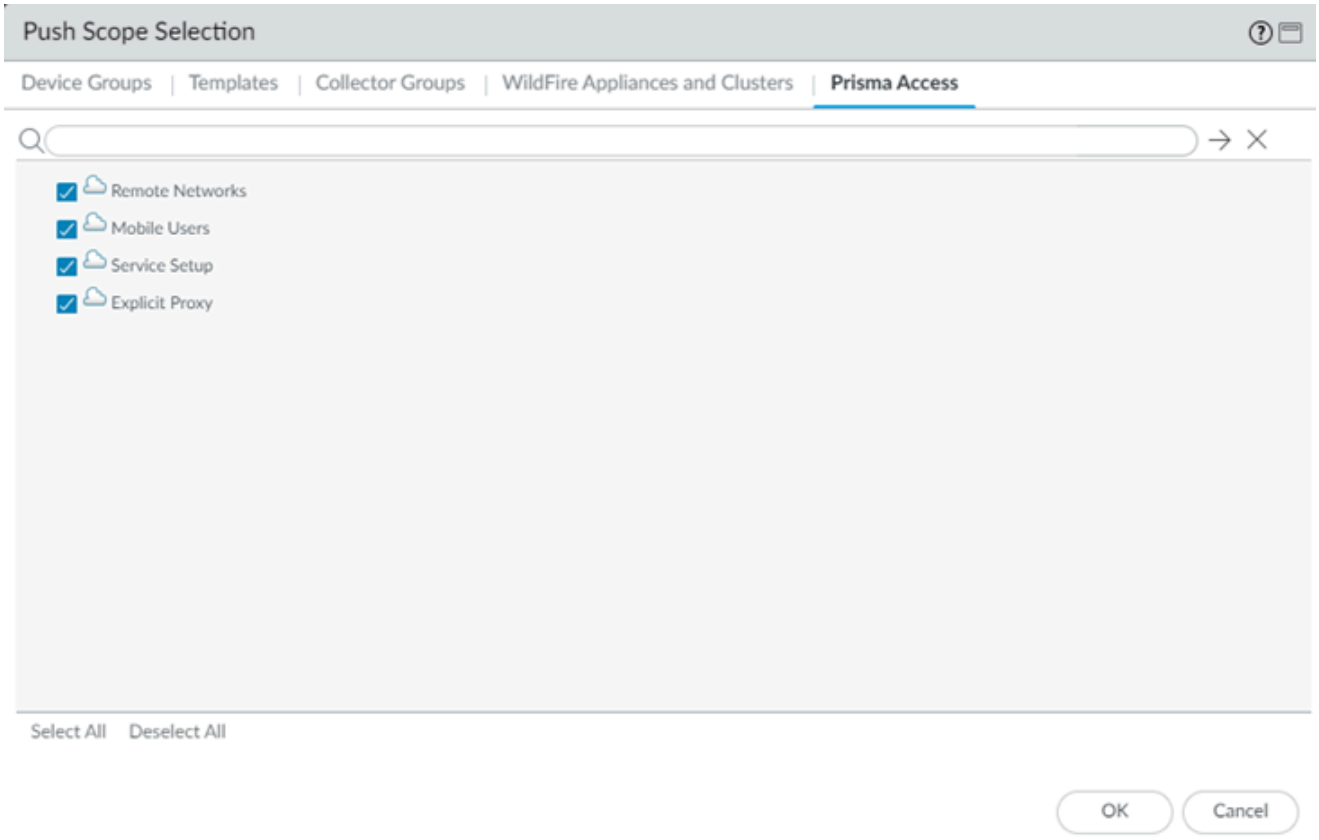

**STEP 10 |** 按一下 **OK**（確定）儲存服務設定。


©2025 Palo Alto Networks, Inc.

**STEP 11 |** 將您的所有變更提交到 Panorama，並將設定變更推送到 Prisma Access。

1. 按一下 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**）。
2. 按一下 **Commit**（提交） > **Push to Devices**（推送至裝置），然後按一下 **Edit Selections**（編輯選取項目）。
3. 在 **Prisma Access** 頁籤上，請確保已選取 **Service setup**（服務設定），然後按一下 **OK**（確定）。

   Prisma Access 應該自動選取需要提交的元件。

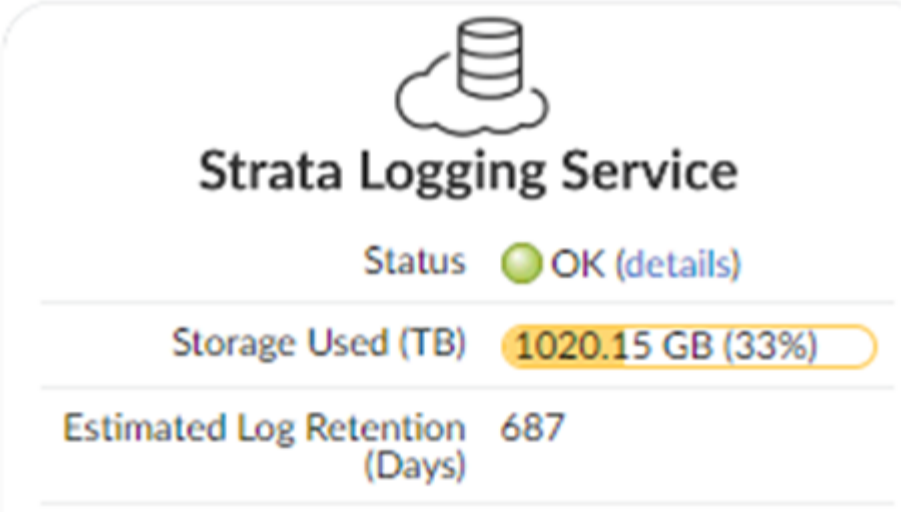



4. 按一下 **Push**（推送）。


©2025 Palo Alto Networks, Inc.

**STEP 12 |** 驗證 Prisma Access 是否已成功連線到 Strata Logging Service。

1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Status**（狀態） > **Strata Logging Service**（**Strata** 記錄服務），然後驗證狀態是否為 **OK**（成功）。




如果狀態為 **Error**（錯誤），請按一下詳細資訊連結以檢視任何錯誤。

**STEP 13 |** 繼續設定 Prisma Access：

- 建立服務連線以允許存取私人應用程式
- 設定 Prisma Access for Networks
- 設定 Prisma Access for Users

 ©2025 Palo Alto Networks, Inc.

# 行動使用者：IP 位址配置

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

在設定您的 Prisma Access 部署之後，瞭解 IP 位址何時變更很有用，如此您就可以主動規劃基礎結構、擷取 IP 位址，並相應地將所需的 IP 位址新增到允許清單。IP 位址變更可能是您所做的變更（例如，新增另一個行動使用者位置）或 Prisma Access 自動執行的變更（例如，大量行動使用者存取單一 Prisma Access 閘道）的結果。

在您第一次為使用者部署 Prisma Access 之後，Prisma Access 會為每個入口網站和閘道指派兩個公用和（如果適用）輸出 *IP* 位址。這些 IP 位址是唯一的，不是共用的，其專用於您的 Prisma Access 部署，並仍配置給您的租用戶，直到 Prisma Access 訂閱到期且寬限期結束為止。

如果您有多租用戶設定，Prisma Access 會為每個租用戶新增專用 IP 位址。

由於公用 IP 位址是 Prisma Access 用於對網際網路型目的地所提出要求的來源 IP 位址，因此您可能需要知道公用 IP 位址是什麼，並將其新增到您網路中的允許清單，讓您的使用者能夠存取 SaaS 應用程式或可公開存取的合作夥伴應用程式等資源。

如果發生以下事件，則可以將新的公用 IP 位址新增到租用戶：

- 大量行動使用者存取同一位置中的位置。

  為了滿足為大量使用者提供服務的容量需求，Prisma Access 可能新增一個或多個閘道，Prisma Access 會新增一或多個閘道，以容納增加的使用者數目、指派一個或多個現有的公用 IP 位址給新閘道，並將一組新的 IP 位址新增到行動使用者位置，以取代已使用的 IP 位址。
- 您會將一或多個位置新增到您的部署。

  當您新增更多位置時，Prisma Access 會為您新增的每個新位置新增另一個閘道和一組新的 IP 位址。

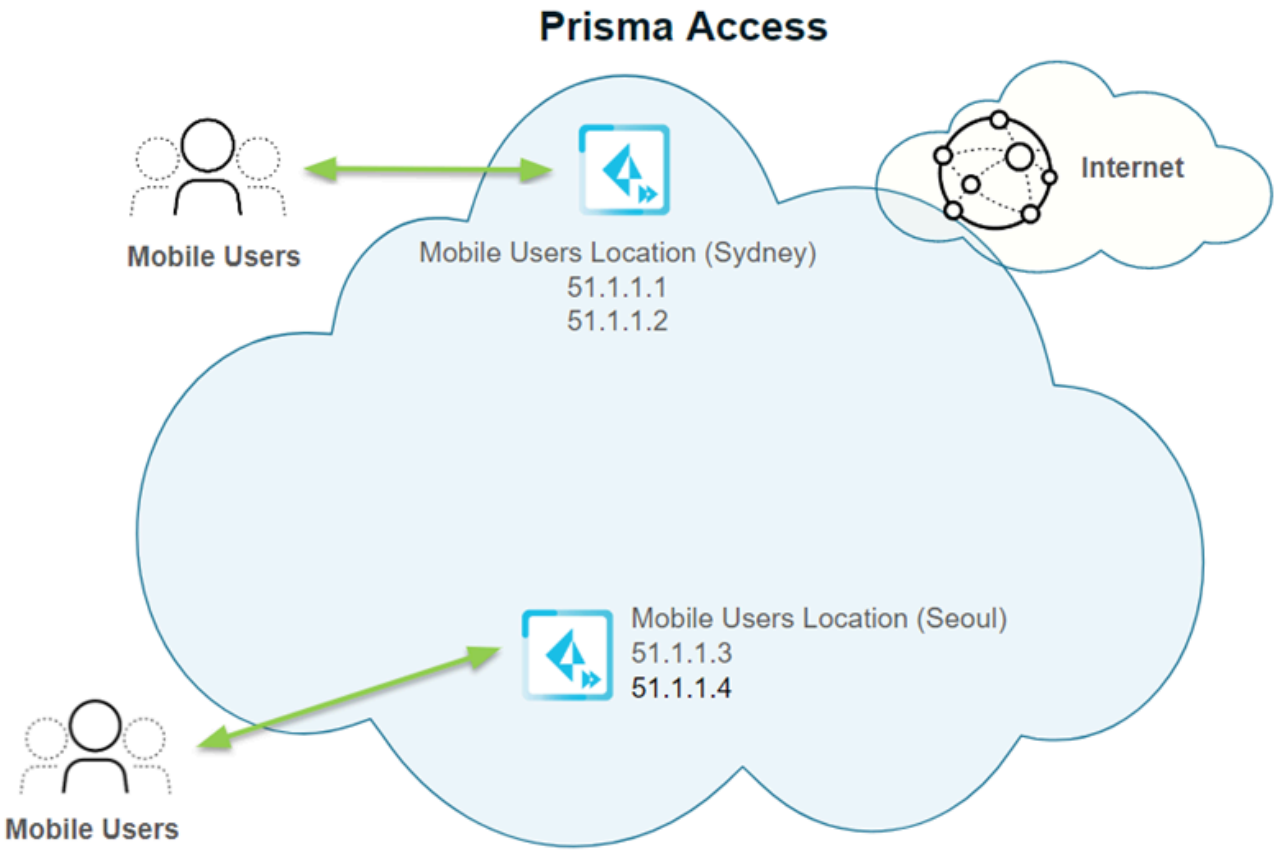
因為 Prisma Access 在調整事件之後以及在您新增位置之後啟用更多的公有 IP 位址，所以您應該新增 IP 變更事件通知 URL，或使用 API 擷取行動使用者位址，以在 IP 位址在您的 Prisma Access 基礎結構中發生變更時收到通知。然後，您可以將任何新增或變更的位址新增到允許清單。

## 範例：公用 IP 位址調整範例（行動使用者）

以下範例說明行動使用者公用 IP 位址配置程序：Prisma Access 會在調整事件期間或新增位置時使用。

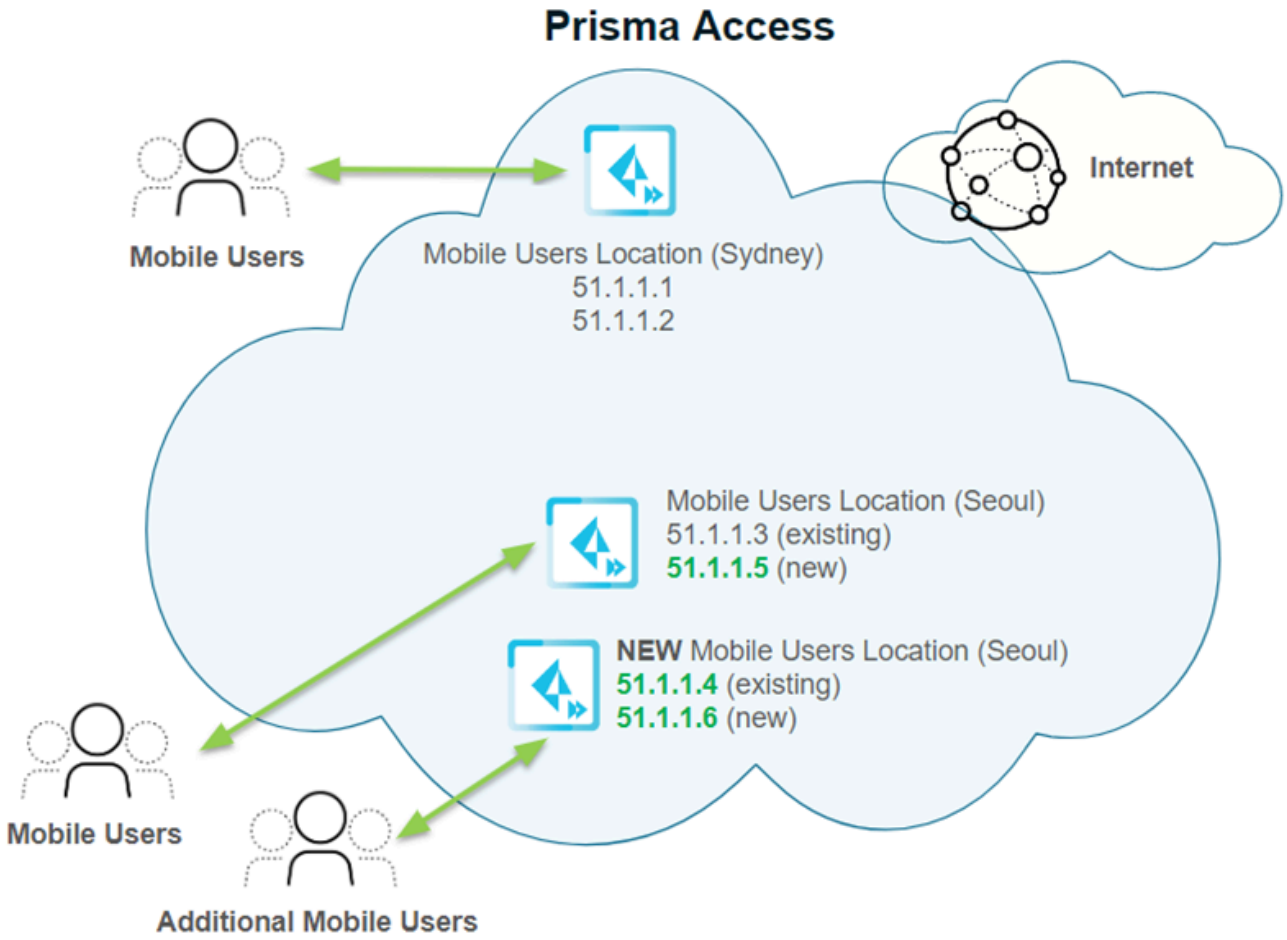
在下列範例中，您已在亞太地區指定兩個位置，進行新的行動使用者部署：雪梨和首爾。每個位置都有兩個閘道 IP 位址。


©2025 Palo Alto Networks, Inc.



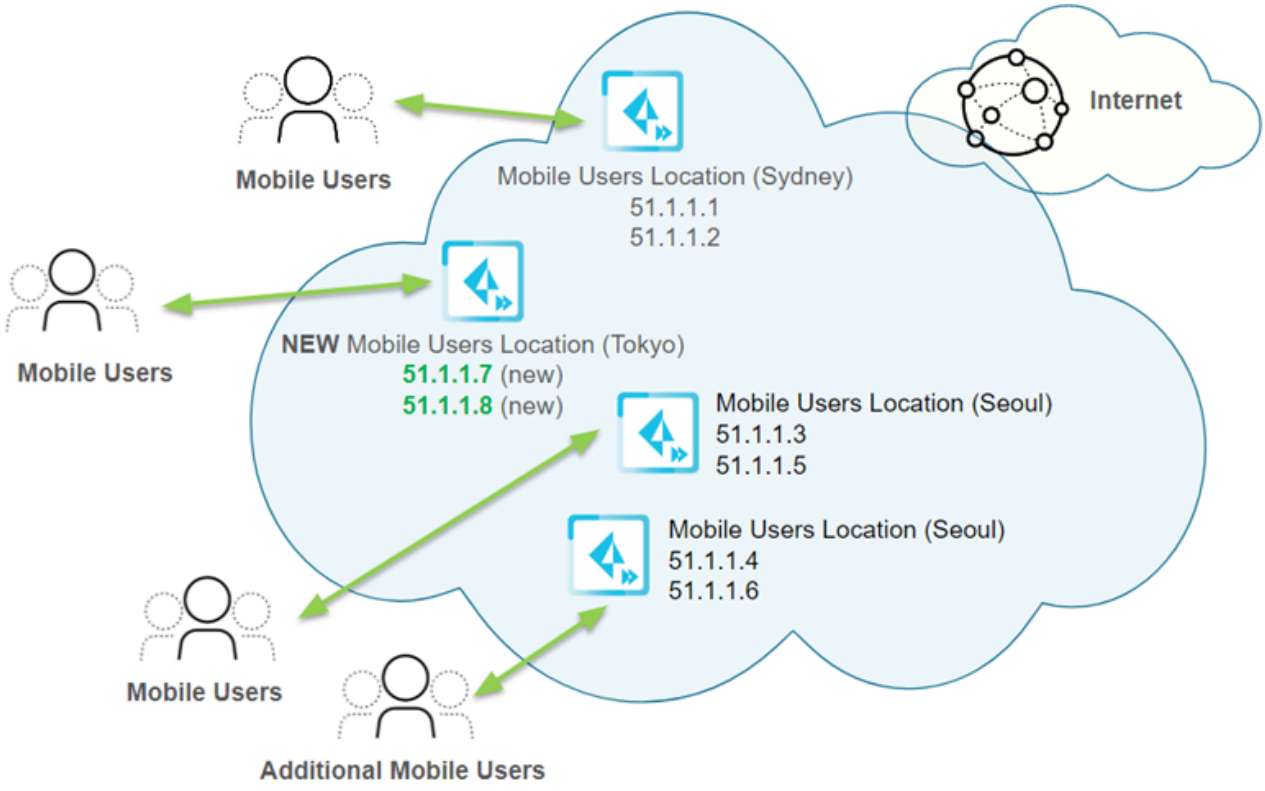

然後，有大量使用者登入首爾位置。為了容納這些額外的使用者，Prisma Access 為首爾位置新增第二個閘道、從第一個首爾閘道取得其中一個閘道位址 (51.1.1.4)，並將其指派給第二個首爾閘道。然後，它會新增兩個額外的 IP 位址（本範例中為 51.1.1.5 和 51.1.1.6），並將它們新增至兩個首爾閘道。

 ©2025 Palo Alto Networks, Inc.




然後在亞太地區新增另一個位置，即東京。Prisma Access 為新閘道建立兩個新的 IP 位址（51.1.1.7 和 51.1.1.8）。


©2025 Palo Alto Networks, Inc.




每次新增位置或有調整事件時，您都應該擷取新的輸出和閘道 IP 位址，這些是 Prisma Access 指派的，並將它們新增到網路中的允許清單。Prisma Access 始終為每個位置的所有作用中閘道保留兩組 IP 位址。

## 回送 IP 位址配置（行動使用者）

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

回送位址是 Prisma Access 用來對內部來源提出要求的 IP 位址，並且是從基礎結構子網路指派的。在基礎結構或資料平面升級期間，回送 IP 位址可以針對行動使用者進行變更。

在基礎結構或資料平面升級期間，回送 *IP* 位址無法針對服務連線或遠端網路連線進行變更；只有行動使用者回送 *IP* 位址才能變更。

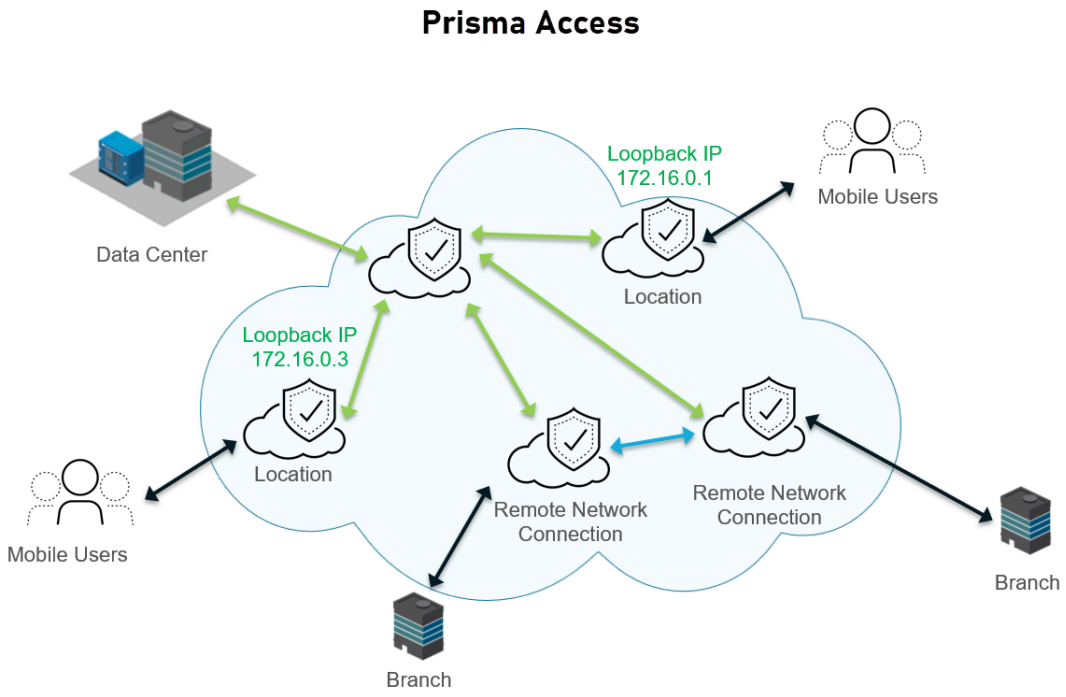
Prisma Access 會從您啟用 Prisma Access 基礎結構時指定的基礎結構子網路中配置回送 IP 位址。您可以將整個基礎結構子網路新增至允許清單，並避免在基礎結構或資料平面升級期間規劃行動使用者回送 IP 變更。若要尋找基礎結構子網路，請選取：


©2025 Palo Alto Networks, Inc.

- Prisma Access (Managed by Strata Cloud Manager)：**Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Prisma Access** > **Infrastructure Settings**（基礎結構設定），並檢視 **Infrastructure Subnet**（基礎結構子網路）
- Prisma Access (Managed by Panorama)：**Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Service Infrastructure**（服務基礎結構），並檢視 **Infrastructure Subnet**（基礎結構子網路）

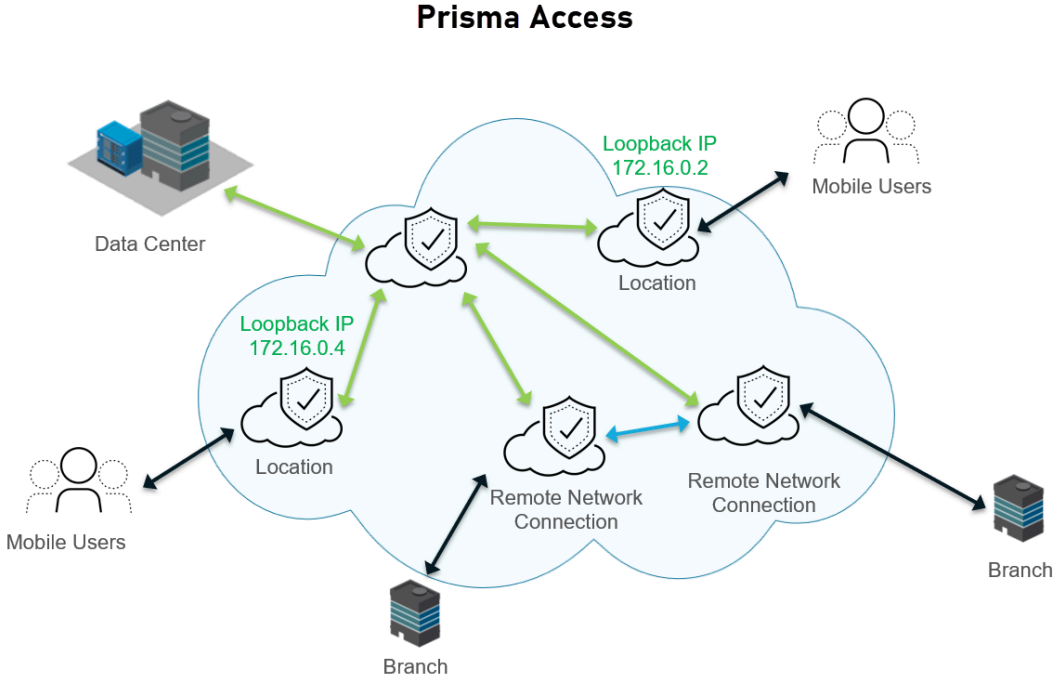
使用用來擷取公用 IP 和回送 IP 位址的 API 擷取這些位址。

下列範例顯示基礎結構子網路為 172.16.0.0/16 的 Prisma Access 部署。Prisma Access 已從基礎結構子網路為行動使用者指派回送 IP 位址 172.16.0.1 和 172.16.0.3。




在基礎結構或資料平面升級（例如，為雲端服務外掛程式的新版本做好準備）之後，Prisma Access 會從基礎結構子網路為行動使用者指派兩個不同的 IP 位址（172.16.0.1 變更為 172.16.0.2，而 172.16.0.3 變更為 172.16.0.4）。


©2025 Palo Alto Networks, Inc.

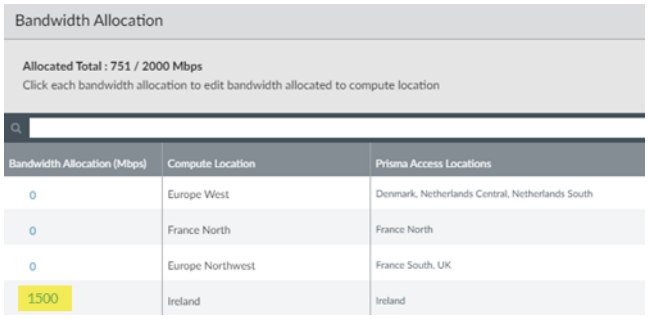



 ©2025 Palo Alto Networks, Inc.

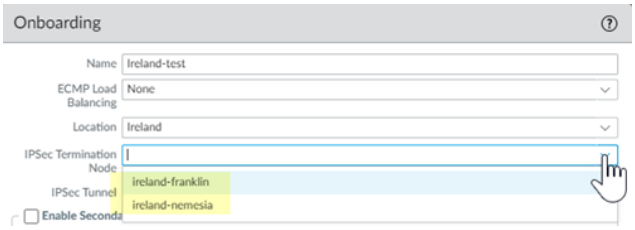
# 遠端網路：IPSec 終端節點和服務 IP 位址

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

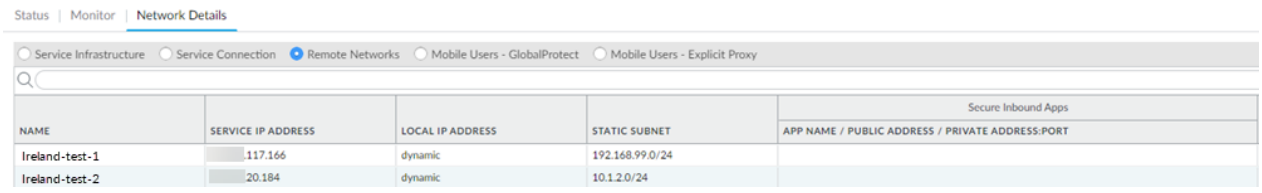
當您裝載遠端網路時，請將其與 *IPSec* 終端節點建立關聯，並且每個 IPSec 終端節點都有一個與其相關聯的 **Service IP Address**（服務 **IP** 位址）。當您為遠端網路連線設定 IPSec 通道時，您會使用此位址作為 CPE 的對等 IP 位址。每個終端節點可以為您提供最多 1,000 Mbps 的頻寬。將超過 1000 Mbps 的頻寬與計算位置建立關聯，可以為您提供多個 **Service IP Address**（服務 **IP** 位址）。




當您在愛爾蘭計算位置裝載遠端網路時，您可以選擇兩個 IPSec 終端節點，因為總頻寬超過 1000 Mbps。




每個 IPSec 終端節點都有自己的 **Service IP Address**（服務 **IP** 位址），如 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Remote Networks**（遠端網路）中所見。




 ©2025 Palo Alto Networks, Inc.

# 遠端網路：與頻寬配置相關的 IP 位址變更

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

如果您有一個舊版 Prisma Access 部署，依位置配置頻寬，則本節適用。任何新部署都依計算位置配置頻寬；若要瞭解 Prisma Access 如何配置這些 IP 位址，請參閱 遠端網路：IPSec 終端節點和服務 IP 位址。

遠端網路連線的 IP 位址是唯一的，不是共用的，並且專用於您的 Prisma Access 部署。這些 IP 位址在 Prisma Access 建立它們作為遠端網路裝載的一部分之後不會變更，而且 IP 位址會在升級後持續存在。不過，在增加現有連線的頻寬時要小心，因為如果該增加導致某個位置的頻寬超過 500 Mbps，則遠端網路的 IP 位址可能會變更。

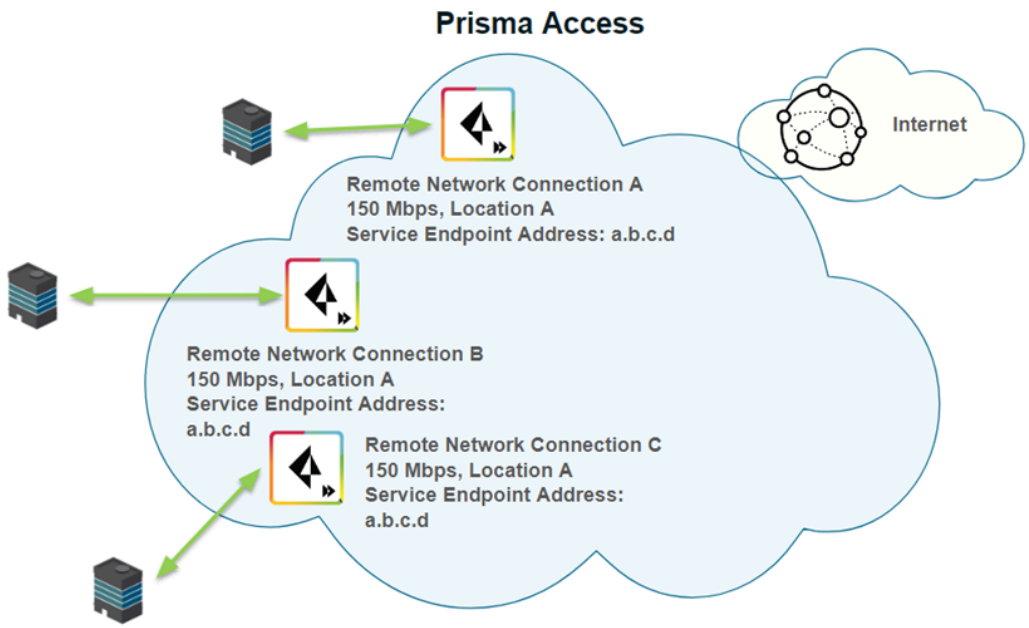
此外，如果 *Prisma Access* 建立新的 *Prisma Access* 計算位置，並且您決定要使用此新的計算位置搭配您已裝載的位置，輸出 *IP* 位址可能會變更。

這些頻寬指導方針僅在您升級現有連線時適用。單一遠端網路連線，即使是 1000 Mbps（預覽）連線，也一律收到單一 **Service IP Address**（服務 **IP** 位址），無論其大小如何。

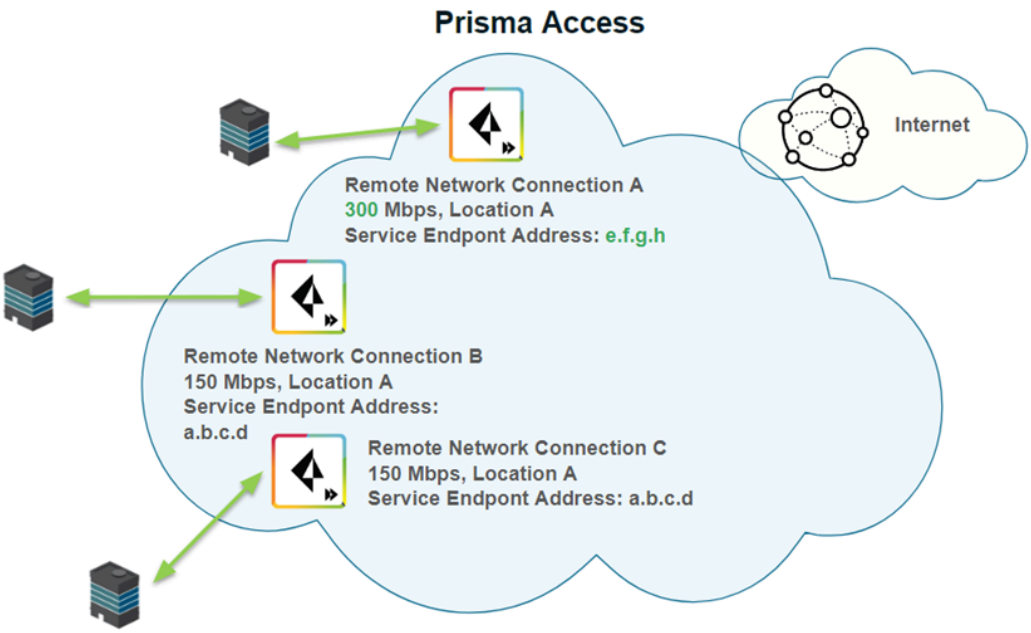
*1000 Mbps* 頻寬選項處於預覽模式。預覽期間的輸送量是盡最大努力提供的，實際效能將視流量混合而有所不同。

以下範例顯示了同一位置的三個遠端網路連線，每個連線的頻寬為 150 Mbps。由於總頻寬為 500 Mbps，因此 Prisma Access 會為該位置中的所有連線指派單一 IP 位址。


©2025 Palo Alto Networks, Inc.




以下範例顯示了遠端網路連線 A 的頻寬從 150 Mbps 增加到 300 Mbps。由於所有連線的總頻寬現在超過 500 Mbps，Prisma Access 會為具有額外頻寬的連線指派新的服務 IP 位址。另一個服務 IP 位址保持不變。




相反，假設有四個頻寬為 100 Mbps 的遠端網路，如果將其中一個遠端網路的頻寬增加到 100 Mbps，則該遠端網路的 **Service IP Address**（服務 **IP** 位址）不會變更，因為總頻寬現在為 500 Mbps。

如果減少遠端網路連線的頻寬，則 ***Service IP Address***（服務 ***IP*** 位址）不會變更。

 ©2025 Palo Alto Networks, Inc.

若要在 Panorama 中尋找服務 IP 位址，請選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊），然後按一下 **Remote Networks**（遠端網路）選項按鈕，以顯示遠端網路的 **Service IP Address**（服務 **IP** 位址），或使用 API 指令碼。


©2025 Palo Alto Networks, Inc.

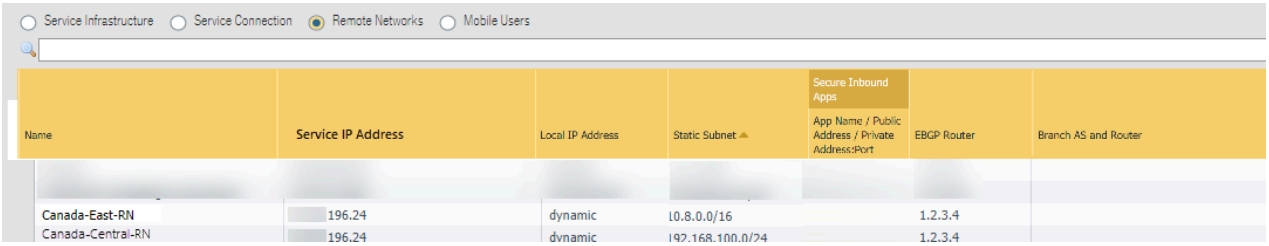
# 遠端網路：服務 IP 位址和輸出 IP 位址配置

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

Prisma Access 具有 100 多個位置可用，以容納全球部署並提供本地化體驗。兩個位置可能對應到相同的位址，當您為遠端網路連線設定 IPsec 通道時，您可以使用這些位址作為對等 IP 位址。不過，位置可能會使用不同的輸出 IP 位址，以確保使用者取得該區域的正確預設語言。

服務連線不支援語言本地化，因為不支援透過服務連線輸出至網際網路。*Prisma Access* 僅配置每個服務連線配一個服務 *IP* 位址，而該 *IP* 位址會在地理上註冊到與您在裝載期間所指定位置對應的計算位置。

下列範例顯示了在加拿大部署了兩個遠端網路位置的客戶部署：加拿大中部和加拿大東部。Prisma Access已將相同的 **Service IP Address**（服務 **IP** 位址）指派給這兩個位置。當您設定遠端網路通道時，請在建立遠端網路連線的 IPsec 通道時，使用此 IP 位址 作為對等 IP 位址。




不過，加拿大東部使用與加拿大中部（英語）不同的預設語言（法語）。因此，Prisma Access 會為其指定不同的輸出 IP 位址。如果您為輸出 IP 位址執行 API 指令碼，則將為這兩個位置收到兩個不同的 IP 位址。


©2025 Palo Alto Networks, Inc.

# 擷取 Prisma Access 的 IP 位址

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

如果您要手動將 Prisma Access 基礎結構的 IP 位址新增到您網路中的允許清單，或是如果使用自動化指令碼，強制執行 IP 型限制，以限制對企業應用程式的輸入存取，您應該瞭解這些位址的作用，以及您需要允許它們的原因，以及擷取它們所執行的工作。

在您完成 Prisma Access 設定之前，Prisma Access 不會佈建這些 IP 位址。部署完成後，您可以使用 API 指令碼擷取這些 IP 位址。API 指令碼會使用您從 Prisma Access UI 取得的 API 金鑰，以及您建立的 .txt 檔案，此檔案會指定您想要擷取的位址。

雖然您不會執行這些工作，直到您完成 Prisma Access 設定，但提前瞭解這些概念非常有用，如此您就能瞭解部署完成後要做什麼。

- Strata Cloud Manager
- Panorama

## 擷取 Prisma Access 的 IP 位址 (Strata Cloud Manager)

### Prisma Access 基礎結構 IP 位址

下表為您提供了 Prisma Access 用於每種部署類型的 IP 位址清單，以及您在執行 API 指令碼以擷取 IP 位址時使用的關鍵字，並指出您是否需要將它們新增到允許清單。

| 部署類型 | IP 位址類型 | 說明 |
| --- | --- | --- |
| 行動使用者 | Prisma Access 閘道 (**gp_gateway**) | 擷取閘道 IP 位址。針對您的行動使用者部署，同時將閘道和入口網站 IP 位址新增至允許清單。<br>行動使用者會連線至 Prisma Access 閘道，以存取您已為其提供存取權的內部或網際網路資源，例如 SaaS 或公用應用程式。 |
| | Prisma Access 入口網站 (**gp_portal**) | 擷取入口網站 IP 位址。針對您的行動使用者部署，同時將閘道和入口網站 IP 位址新增至允許清單。<br>行動使用者登入 Prisma Access 入口網站，來接收其初始設定和閘道位置。 |


©2025 Palo Alto Networks, Inc.

| 部署類型 | IP 位址類型 | 說明 |
| --- | --- | --- |
| | 回送 IP 位址 | 此位址是 Prisma Access 用於對內部來源所提出要求的來源 IP 位址，並且是從基礎結構指派的。將回送 IP 位址新增到您網路中的允許清單，以將 Prisma Access 提供給 RADIUS 或 Active Directory 驗證伺服器等內部資源。<br>Palo Alto Networks 建議您在網路中允許整個基礎結構子網路的所有 IP 位址，因為行動使用者的回送位址可能會變更。 |
| 行動使用者—明確 **Proxy** | 驗證快取服務 (ACS) | Prisma Access 服務的位址，該服務儲存明確 Proxy 使用者的驗證狀態。<br>此位址僅用於行動使用者（明確 Proxy）部署。 |
| | 網路負載平衡器 | Prisma Access 用於明確 Proxy 網路負載平衡器的位址。<br>此位址僅用於行動使用者（明確 Proxy）部署。 |
| 遠端網路 | 遠端網路 IP 位址 (**remote_network**) | 包括 Prisma Access 為 Prisma Access 遠端網路連線指派的 **Service IP Addresses**（服務 **IP** 位址），以及 Prisma Access 用來確保遠端網路使用者為其區域取得正確預設語言的輸出 IP 位址。將這些位址新增到您網路中的允許清單，以將 Prisma Access 提供給網際網路資源。 |
| | 回送 IP 位址 | 這是 Prisma Access 用於對內部來源所提出要求的來源 IP 位址，並且是從基礎結構子網路指派的。將回送 IP 位址新增到允許清單，以將 Prisma Access 提供給 RADIUS 或 Active Directory 驗證伺服器等內部資源。 |

## 執行用來擷取 IP 位址的 API 指令碼

使用以下步驟擷取 Prisma Access 在其基礎結構中使用的 IP 位址。

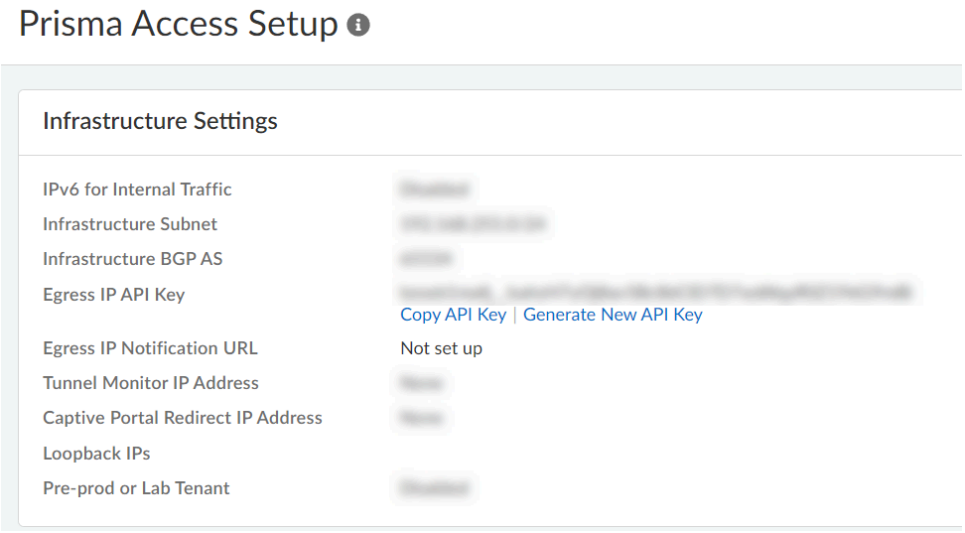
此命令不會擷取回送位址；若要擷取回送 *IP* 位址，請使用舊版 API 命令。

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** 取得 API 金鑰。

您需要此金鑰，向 Prisma Access 進行驗證，並使用 API 命令擷取 IP 位址清單。

1. 前往 Prisma Access (Managed by Strata Cloud Manager)，並選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Prisma Access** > **Infrastructure Settings**（基礎結構設定）。
2. 選取 **Generate New API Key**（產生新的 **API** 金鑰）。




如果您已產生 API 金鑰，則目前金鑰即會顯示。如果您尚未產生金鑰，或想要取代現有金鑰，以符合稽核或合規性檢查，進行金鑰輪換，請按一下 **Generate New API Key**（產生新的 **API** 金鑰）以取得新金鑰。

**STEP 2 |** 建立 .txt 檔案，並將 API 命令選項放入該檔案中。

使用 API 時，要使用的命令是兩步程序。首先，建立 .txt 檔案，為要擷取的 IP 位址指定參數，然後將該檔案儲存在可從命令執行所在位置存取的資料夾中。然後，執行 API 並指定您在命令中建立的 .txt 檔案的名稱和位置。

在 .txt 檔案中指定以下關鍵字和參數。本主題中的範例使用檔案名稱 **options.txt**，但是您可以指定任何檔案名稱，只要您在命令中參考它即可。

| 引數 | 可能選項（關鍵字） | 註解 |
|---|---|---|
| **serviceType** | **all**<br>**remote_network**<br>**gp_gateway**<br>**gp_portal**<br>**swg_proxy**<br>**rbi** | **all**—擷取您需要針對所有服務類型（遠端網路、行動使用者（閘道和入口網站）和 Clean Pipe，適用於您的部署）將其新增到允許清單的 IP 位址。<br>**remote_network**—擷取您需要針對遠端網路部署將其新增到允許清單的 IP 位址。<br>**gp_gateway**—擷取您需要針對行動使用者部署將其新增到允許清單的閘道 IP 位址。 |


©2025 Palo Alto Networks, Inc.

| 引數 | 可能選項（關鍵字） | 註解 |
|---|---|---|
| | | **gp_gp_portal**—擷取您需要針對行動使用者部署將其新增到允許清單的入口網站 IP 位址。<br><br>**swg_proxy**—為每個已部署的明確 Proxy 位置、驗證快取服務 (ACS) 和網路負載平衡器擷取輸出 IP 位址。<br><br>**RBI**—擷取您需要針對遠端瀏覽器隔離 (RBI) 部署將其新增到允許清單，以連線到 SaaS 應用程式的輸出 IP 位址。 |
| **addrType** | **all**<br><br>**active**<br><br>**service_ip**<br><br>**auth_cache_service**<br><br>**network_load_balancer** | **all** 或 **active**—擷取您需要將其新增到允許清單的所有 IP 位址。<br><br>此 API 不會擷取回送 IP 位址。若要擷取回送 IP 位址，請使用舊版 API 命令。<br><br>**service_ip**—擷取 **Service IP Address**（服務 IP 位址），您會在為遠端網路連線設定 IPSec 通道時使用此服務 IP 位址作為對等 IP 位址。<br><br>**auth_cache_service**—為明確 Proxy ACS 擷取 IP 位址（僅適用於行動使用者—明確 Proxy 部署）。<br><br>**network_load_balancer**—為明確 Proxy 網路負載平衡器擷取 IP 位址（僅適用於行動使用者—明確 Proxy 部署）。 |
| **actionType** | **pre_allocate** | 僅限行動使用者部署—**actionType** 若為 **pre_allocate**，可讓您針對行動使用者部署擷取 Prisma Access 閘道和入口網站的 IP 位址或子網路。使用此引數搭配其值為 **gp_gateway** 的 **serviceType**，以擷取預先配置的閘道 IP 位址，以及搭配其值為 **gp_portal** 的 **serviceType**，擷取預先配置的入口網站 IP 位址。<br><br>擷取預先配置的 IP 位址，可讓您在裝載行動使用者位置之前，將閘道和入口網站 IP 位址新增到您組織的允許清單，從而讓行動使用者能夠在您裝載這些位置後立即存取外部 SaaS 應用程式。 |
| **location** | **all**<br><br>**deployed** | **all**—從所有位置擷取 IP 位址。對於行動使用者部署，此關鍵字會針對您在裝載期間新增的位置和您未新增的位置擷取 IP 位址。<br><br>**deployed**—擷取您在行動使用者裝載期間新增的所有位置中的 IP 位址。 |


©2025 Palo Alto Networks, Inc.

| 引數 | 可能選項（關鍵字） | 註解 |
| --- | --- | --- |
| | | 此關鍵字僅適用於行動使用者部署。Prisma Access 會在佈建期間關聯每個行動使用者位置的 IP 位址，即使您在行動使用者裝載期間未選取該位置也一樣。如果您指定 **all**，API 命令會擷取所有行動使用者位置的 IP 位址，包括您未針對部署選取的位置。如果您指定 **deployed**，則 API 命令僅針對您在裝載期間選取的位置擷取 IP 位址。 |

請採取以下格式指定 .txt 檔案中的選項：

```
 { "serviceType": "service-type", "addrType": "address-type",
"location": "location" }
```

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 請輸入下列命令以擷取 IP 位址：

- 若要使用 Prisma Access 2.1 中引進的較新 API，請輸入下列命令：

```
curl -X POST --data @option.txt -H header-api-key:Current-API-Key "https://api.prod.datapath.prismaaccess.com/getPrismaAccessIP/v2"
```

自 *2023* 年 *5* 月起，一些雲端受管理部署會使用 *https://api.prod6.datapath.prismaaccess.com/getPrismaAccessIP/v2*（請注意，*URL* 中的 *prod6*，而不是 *prod*）。

- 若要使用舊版 API，請輸入下列命令。此命令使用將於 2022 年 5 月棄用的舊版 API 端點：

```
curl -X POST --data @option.txt -k -H header-api-key:Current-API-Key "https://api.gpcloudservice.com/getPrismaAccessIP/v2"
```

其中 *option.txt* 是您在上一個步驟中建立的 .txt 檔案，而 *Current-API-Key* 是 Prisma Access API 金鑰。

例如，假設 .txt 檔案名稱為 **option.txt**，而 API 金鑰為 **12345abcde**，請使用以下 API 命令擷取所有位置的公有 IP 位址：

```
curl -X POST --data @option.txt -H header-api-key:12345abcde "https://api.prod.datapath.prismaaccess.com/getPrismaAccessIP/v2"
```

*API* 命令可以傳回大量資訊。為了使輸出更具可讀性，如果您安裝了 *Python*，則可以在 *cURL* 命令尾端新增 `| python -m json.tool`。

API 命令會以下列格式傳回位址：

```
{ "result": [ { "address_details": [ { "address":"1.2.3.4" "allow_listed": false "addressType": "address-type" "serviceType":
```

 ©2025 Palo Alto Networks, Inc.

```
 "service-type" } ], "addresses": [ "1.2.3.4" ] "zone": "zone-
name", "zone_subnet": [zone-subnet ] }, "status": "success"
```

其中：

- **address_details** 顯示每個位置的位址詳細資訊。
  - **serviceType** 顯示 IP 位址的類型（遠端網路 (**remote_network**)、Prisma Access 閘道 (**gp_gateway**)、Prisma Access 入口網站 (**gp_portal**)、Clean Pipe (**clean_pipe**) 或遠端瀏覽器隔離 (**RBI**)。
  - **addressType** 指定使用 `addrType` 關鍵字（**active** 或 **pre-allocated**，如果要為行動使用者位置預先配置 IP 位址）指定的位址類型。
  - **address** 顯示您需要將其新增到允許清單的 IP 位址。

    如果 API 傳回多個 IP 位址，Prisma Access 會在 **addresses**（位址）欄位中彙總這些位址。
- **addresses** 列出您需要將其新增到允許清單的位置的所有 IP 位址。
- **zone** 是與 IP 位址相關聯的 Prisma Access 位置。
- **zone_subnet** 是行動使用者閘道和入口網站的子網路。如果您要為行動使用者位置預先配置 IP 位址，Prisma Access 也會提供此子網路。

如果 .txt 檔案中的選項有任何問題，API 會傳回如下的錯誤：

```
 {"status": "error","result":"Invalid json format in the request.
trace_id: xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx "}
```

**STEP 4 |** 使用您擷取的 IP 位址更新內部部署伺服器或 SaaS 應用程式政策規則上的允許清單。

## API 命令範例

在 .txt 檔案中輸入 API 命令的關鍵字和引數時，請使用下列範例。若要變更命令的輸出，請變更 .txt 檔案中的選項；命令本身不會變更。

| 擷取這些 IP 位址 | 在 .txt 檔案中指定這些參數 | 註解 |
|---|---|---|
| 行動使用者 IP 位址 | | |
| 所有行動使用者 IP 位址 | `{ "serviceType": "gp_gateway", "addrType": "all", "location": "all" }` | *addrType* 若為 *all*，表示 Prisma Access 擷取所有行動使用者閘道 IP 位址。<br>*location* 若為 *all*，表示 Prisma Access 會擷取所有可用位置的 IP 位址，包括您尚未裝載的位置。Prisma Access 保留非裝載位置 IP 位址，以便您可以先將這些 IP 位址新增至您的允許清單，然後再裝載它們。 |


©2025 Palo Alto Networks, Inc.

| 擷取這些 IP 位址 | 在 .txt 檔案中指定這些參數 | 註解 |
|---|---|---|
| 所裝載行動使用者位置的 IP 位址 | `{ "serviceType": "gp_gateway", "addrType": "all", "location": "deployed" }` | *location* 類型若為 *deployed*，表示 Prisma Access 僅為行動使用者裝載期間您選取的位置擷取 IP 位址。 |
| 所裝載行動使用者位置的所有作用中 IP 位址 | `{ "serviceType": "gp_gateway", "addrType": "active", "location": "deployed" }` | *addrType* 若為 *active*，表示 Prisma Access 僅擷取所裝載位置的 IP 位址。 |
| 遠端網路 **IP** 位址 | | |
| 擷取所有遠端網路 IP 位址 | `{ "serviceType": "remote_network", "addrType": "all", "location": "all" }` | 此命令會擷取您已裝載的遠端網路的公用和輸出 IP 位址。請勿使用其值為 *deployed* 的 *location*。您可以使用其值為 *active* 的 *addrType*，但它會擷取相同的位址，就像您已將 *addrType* 指定為 *all* 一樣。 |
| 明確 **Proxy IP** 位址 | | |
| 擷取所部署位置的 ACS IP 位址 | `{ "serviceType": "swg_proxy", "location": "deployed", "addrType": "auth_cache_service" }` | 此命令會針對您的明確 Proxy 部署擷取 ACS IP 位址。輸入其值為 *all* 的 *addrType* 擷取所有位址類型（ACS 和網路負載平衡器 IP 位址）。 |
| 遠端瀏覽器隔離 **IP** 位址 | | |
| 為所部署位置擷取遠端瀏覽器隔離 (RBI) IP 位址 | `{ "serviceType": "rbi", "location": "all", "addrType": "all" }` | 此命令會為每個部署的 RBI 位置擷取輸出 IP 位址。您可以將這些 IP 位址新增至允許清單，以連線到 SaaS 應用程式。 |

## 用來擷取 IP 和回送位址的舊版指令碼

下表顯示的關鍵字和參數可在與 Prisma Access 搭配使用的舊版 API 指令碼中使用，並提供有關要為您具有的部署類型使用哪個 API 的資訊和建議。

這些舊版命令會擷取兩種類型的 IP 位址，即公用 *IP* 和輸出 *IP* 位址。我們為您提供了兩種不同的舊版 API 命令，以便您可以擷取需要新增到允許清單的所有 IP 位址。


©2025 Palo Alto Networks, Inc.

- 公用 *IP* 位址是來源 IP 位址，Prisma Access 將其用於對網際網路型來源提出的要求。將公有 IP 位址新增到您網路中的允許清單，以將 Prisma Access 提供給網際網路資源，例如 SaaS 應用程式或可公開存取的合作夥伴應用程式。

  行動使用者、遠端網路和 Clean Pipe 部署會使用公有 IP 位址。

- 輸出 *IP* 位址是 Prisma Access 用於將流量輸出至網際網路的 IP 位址，並且您還必須將這些位址新增到允許清單，讓 Prisma Access 可以存取網際網路資源。

  除其他目的外，Prisma Access 會使用輸出 IP 位址，以便使用者以他們期望的語言從 Prisma Access 位置接收網頁。所有位置都有公有 IP 位址；不過，並非所有位置都有輸出 IP 位址。以下位置不使用輸出 IP 位址：

  - 巴林
  - 比利時
  - 法國北部
  - 法國南部
  - 香港
  - 愛爾蘭
  - 韓國
  - 臺灣
  - 英國

  行動使用者、遠端網路和 Clean Pipe 部署會使用輸出 IP 位址。

| 行動使用者部署中使用的命令 | |
|---|---|
| 命令名稱 | 註解 |
| **get_egress_ip_all=yes** 命令<br>`curl -k -H header-api-key:`*Current-API-Key*`"https://api.gpcloudservice.com/getAddrList/latest?get_egress_ip_all=yes` | 此命令會擷取您新增到允許清單的所有 IP 位址，以將 Prisma Access 提供給網際網路資源，例如 SaaS 應用程式或可公開存取的合作夥伴應用程式。此命令具有以下限制：<br>• 此命令可以擷取大量位址（超過 200 個）。如果您的企業無法將此數量的 IP 位址新增到允許清單，您可以使用 *gpcs_gp_gw* 和 *gpcs_gp_portal* 關鍵字，僅擷取您目前使用的 IP 位址；不過，每次您新增位置時，都必須重新執行這些命令。此外，如果發生調整事件，您將需要將新的 IP 位址新增到允許清單。<br>• Prisma Access 不會列出與這些 IP 位址相關聯的位置；因此，我們建議您將此命令傳回的所有 IP 位址都新增到允許清單。<br>• 此命令不會為您提供回送位址。 |
| **gpcs_gp_gw** 和 **gpcs_gp_portal** 關鍵字 | 如果您的部署限制了您可以新增到允許清單的 IP 位址數量，請使用此命令。將此命令傳回的所有 IP 位址新增到您網路中的允許清單。您也可以使用此命令擷取回送 IP 位址。 |

 ©2025 Palo Alto Networks, Inc.

| 行動使用者部署中使用的命令 | |
|---|---|
| 命令名稱 | 註解 |
| `curl -k -H header-api-key:`*Current-API-Key*`"https://api.gpcloudservice.com/getAddrList/latest?fwType=gpcs_gp_gw \| gpcs_gp_portal&addrType=public_ip \| egress_ip_list \| loopback_ip"` | |

| 遠端網路部署中使用的命令 | |
|---|---|
| 命令名稱 | 註解 |
| **gpcs_remote_network** 關鍵字<br>`curl -k -H header-api-key:`*Current-API-Key*`"https://api.gpcloudservice.com/getAddrList/latest?fwType=gpcs_remote_network&addrType=public_ip \| egress_ip_list \| loopback_ip"` | 使用此命令，尋找您需要針對遠端網路部署將其新增到允許清單的 IP 位址。<br>您還可以使用此命令，為遠端網路部署尋找輸出 IP 位址；在某些情況下，輸出和 IP 位址可能不同。 |

| **Clean Pipe** 部署中使用的命令 | |
|---|---|
| 命令名稱 | 註解 |
| **gpcs_clean_pipe** 關鍵字<br>`curl -k -H header-api-key:`*Current-API-Key*`"https://api.gpcloudservice.com/getAddrList/latest?fwType=gpcs_clean_pipe&addrType=public_ip \| egress_ip_list \| loopback_ip"` | 使用此命令，尋找您需要針對 Clean Pipe 部署將其新增到允許清單的 IP 位址。 |

為行動使用者部署擷取公有 **IP** 位址和輸出 **IP** 位址

此舊版指令碼已被較新的 API 指令碼所取代。Palo Alto Networks 建議您使用較新的指令碼，來擷取除回送位址外的所有 IP 位址。

如果您要將公有 IP 位址新增至允許清單，讓行動使用者可以存取 SaaS 或公有應用程式，Prisma Access 會為每個閘道和入口網站 IP 位址提供兩個 IP 位址，以便在調整或其他事件期間可以使用

 ©2025 Palo Alto Networks, Inc.

一個 IP 位址。您可以在使用這組 IP 位址之前將其新增到允許清單，從而防止任何問題，讓行動使用者能夠在調整事件期間存取 SaaS 或公用應用程式。

透過完成以下工作來擷取這些新位址：

**STEP 1 |** 選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Prisma Access** > **Infrastructure Settings**（基礎結構設定） > **Generate New API Key**（產生新的 **API** 金鑰）來取得 API 金鑰。

您需要此金鑰，向 Prisma Access 進行驗證，並使用底下所列的 cURL 命令擷取 IP 位址清單。只有 Panorama 管理員或超級使用者才能產生或存取此 API 金鑰。

**STEP 2 |** 請輸入下列命令以擷取行動使用者公用 IP 位址：

```
  curl -k -H header-api-key:Current-API-Key "https://
api.gpcloudservice.com/getAddrList/latest?get_egress_ip_all=yes"
```

其中 *Current-API-Key* 是 Prisma Access API 金鑰。

例如，假設 API 金鑰為 **12345abcde**，請使用以下 API 命令擷取所有位置的公有 IP 位址：

```
  curl -k -H header-api-key:12345abcde "https://
api.gpcloudservice.com/getAddrList/latest?get_egress_ip_all=yes"
```

擷取公用、回送和輸出 **IP** 位址

若要擷取公用、回送和輸出 IP 位址，請完成以下步驟。

**STEP 1 |** 為 Prisma Access 擷取公用 IP 位址、回送 IP 位址或兩者。

手動或在自動化指令碼中使用 API 金鑰和 API 端點 URL：

```
 header-api-key:Current API Key "https://api.gpcloudservice.com/
getAddrList/latest?fwType=$fwType&addrType=$addrType"
```

其中您需要將 Current API Key 取代為您的 API 金鑰，並使用以下一個或兩個關鍵字和引數：

| 關鍵字 | 說明 |
|---|---|
| **fwType** 關鍵字 | |
| **gpcs_gp_gw** | 擷取 Prisma Access 閘道 IP 位址（適用於行動使用者部署）。 |
| **gpcs_gp_portal** | 擷取 Prisma Access 入口網站 IP 位址（適用於行動使用者部署）。 |
| **gpcs_remote_network** | 擷取 Prisma Access 遠端網路 IP 位址（適用於遠端網路部署）。 |
| **gpcs_clean_pipe** | 擷取 Prisma Access Clean Pipe IP 位址。 |
| **addrType** 關鍵字 | |

 ©2025 Palo Alto Networks, Inc.

| 關鍵字 | 說明 |
| --- | --- |
| **public_ip** | 擷取 Prisma Access 用於對網際網路型來源所提出要求的來源 IP 位址。<br>對於行動使用者位置，Prisma Access 會依位置列出 IP 位址。對於遠端網路，Prisma Access 會依遠端網路名稱列出 IP 位址。 |
| **egress_ip_list** | 擷取 Prisma Access 與公用 IP 位址搭配使用的 IP 位址，以取得網際網路的額外輸出流量。<br>對於行動使用者位置，Prisma Access 會依位置列出 IP 位址。對於遠端網路，Prisma Access 依遠端網路名稱列出 IP 位址。 |
| **loopback_ip** | 擷取 Prisma Access 用於對內部來源（例如 RADIUS 或 Active Directory 伺服器）所提出要求的來源 IP 位址，且是從基礎結構子網路指派的。 |

如果未指定關鍵字，則 Prisma Access 會擷取所有 IP 位址。

例如，您可以嘗試以下 cURL 命令，手動擷取所有遠端網路的公用 IP 位址清單：

```
curl -k -H header-api-
key:1234y9ydxb__0UmxetVTbC8XTyFMaoT4RBZBKBjfX419YVufeFG7
 "https://api.gpcloudservice.com/getAddrList/latest?
fwType=gpcs_remote_network&addrType=public_ip"
```

或者，使用簡單的 Python 指令碼來擷取所有 IP 位址的清單，例如：

```
  #!/usr/bin/python import subprocess import json api_key =
 '1234y9ydxb__0UmxetVTbC8XTyFMaoT4RBZBKBjfX419YVufeFG7' # Replace
 with your key api_end_point = 'https://api.gpcloudservice.com/
getAddrList/latest' # This call retrieves IP addresses
 for all your Prisma Access firewalls args = ['curl', '-
k', '-H', 'header-api-key:' + api_key, api_end_point] p =
 subprocess.Popen(args, stdout=subprocess.PIPE) output =
 p.communicate() dout = json.loads(output[0]) addrStrList
 = dout['result']['addrList'] addrList = [] for addr_str
 in addrStrList: addrList.append(addr_str.split(":")[1])
 print(addrList)
```

**STEP 2 |** 使用您擷取的 IP 位址更新內部部署伺服器或 SaaS 應用程式政策規則上的允許清單。

## 為行動使用者位置預先配置 IP 位址

Prisma Access 會將閘道和入口網站 IP 位址用於行動使用者—GlobalProtect 部署，並將驗證快取服務 (ACS) 和網路負載平衡器 IP 位址用於行動使用者—明確 Proxy 部署。行動使用者—GlobalProtect IP 位址稱為*輸出 IP* 位址。如果您需要在裝載位置之前預先配置行動使用者 IP 位址（例如，如果您的組織需要針對行動使用者—GlobalProtect 部署將 IP 位址新增至允許清單，讓行動使用者可以存取外部 SaaS 應用程式），您可以執行 API 指令碼，讓 Prisma Access 提前針對

 ©2025 Palo Alto Networks, Inc.

位置預先配置這些 IP 位址，然後再裝載它。您接著可以在裝載該位置之前。將該位置的輸出 IP 位址新增到組織的允許清單。

API 回應還為要求位置包含輸出 IP 位址的公用 IP 集區子網路。您新增的任何位置的輸出 IP 位址都是此子網路的一部分。將子網路新增到允許清單之後，無需進一步修改允許清單即可在未來新增位置。

Prisma Access 不會預先配置您的 IP 位址和子網路，除非您使用 API 指令碼要求它們。在您執行預先配置指令碼之後，它們的有效期為 90 天。這些 IP 位址和子網路是唯一的，不是共用的，並且在有效期間專用於您的 Prisma Access 部署。您必須在有效期結束之前裝載您的位置，否則您將丟失位址；若要隨時尋找有效期，請執行 API 指令碼。

*Palo Alto Networks* 建議您僅為稍後要裝載的位置預先配置 *IP* 位址。

若要預先配置 IP 位址，請完成以下工作。

**STEP 1 |** 擷取 Prisma Access API 金鑰。

**STEP 2 |** 建立 .txt 檔案，並在您建立的 .txt 檔案中指定以下選項，來預先配置行動使用者輸出 IP 位址。

在 .txt 檔案中輸入以下文字：

- 行動使用者—**GlobalProtect** 部署：

```
 { "actionType": "pre_allocate", "serviceType": "gp_gateway",
"location": ["location"] }
```

- 行動使用者—明確 **Proxy** 部署：

```
{ "actionType": "pre_allocate", "serviceType": "swg_proxy",
 "location": ["location"]}
```

其中 *location* 是您要在其中預先配置 IP 位址的 Prisma Access 位置。

最多可輸入 12 個位置。當 Prisma Access 擷取預先配置的 IP 位址時，輸入超過 12 個位置可能會導致逾時錯誤。

**STEP 3 |** 輸入這個 CURL 命令。

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 透過重新開啟 .txt 檔案、刪除現有資訊並對其進行編輯，來擷取您要求的 IP 位址和子網路，包括其有效期。

- 行動使用者—**GlobalProtect** 部署：
  - 若要要求 Prisma Access 擷取所有預先配置的 IP 位址，請在 .txt 檔案中輸入以下文字。

```
{ "serviceType": "all", "addrType": "pre_allocated",
"location": "all" }
```

  - 若要要求 Prisma Access 為給定位置擷取 Prisma Access 閘道的所有預先配置 IP 位址，請在 .txt 檔案中輸入相同的資訊，但在 .txt 檔案中將 “`all`” 替代為 “`gp_gateway`”。
  - 若要要求 Prisma Access 為給定位置擷取 Prisma Access 入口網站的所有預先配置 IP 位址，請在 .txt 檔案中輸入相同的資訊，但在 .txt 檔案中將 “`all`” 替代為 “`gp_gp_portal`”。
- 行動使用者—明確 **Proxy** 部署：

  若要要求 Prisma Access 為明確 Proxy 部署預先配置您需要將其新增至允許清單的所有 IP 位址，請在 .txt 檔案中輸入以下文字。

```
{ "actionType": "pre_allocate", "serviceType": "swg_proxy",
 "location": ["all"] }
```

Palo Alto Networks 建議您輸入 `all`，以便您可以擷取所有必要且預先配置的輸出 IP 位址，以新增到您的允許清單。



對於行動使用者—*GlobalProtect* 部署，*API* 命令可以傳回大量資訊。為了使輸出更具可讀性，如果您安裝了 *Python*，則可以在 *cURL* 命令尾端新增 `| python -m json.tool`。

**STEP 5 |** 重新輸入此 CURL 命令，來擷取預先配置的位址。

Prisma Access 會以下列格式傳回資訊：

```
    "result": [ { "zone": "prisma-access-zone1", "addresses":
 [ ["ip-address1","ip-address2"] "zone_subnet" : [subnet-and-
mask1","subnet-and-mask2"] "address_details":[ {"address":"ip-
address1", "service_type":"service-type", "addressType":"pre-
allocated", "expiring_in" : "validity-period" }, {"address":"ip-
address2", "service_type":"gp_gateway", "addressType":"pre-
allocated", "validity_period_remaining" :"90 days" } , },
```

其中，變數代表以下 API 命令輸出：

| 變數 | 解釋 |
|---|---|
| *prisma-access-zone1* | 已為其擷取預先配置 IP 位址的 Prisma Access 位置。 |

 ©2025 Palo Alto Networks, Inc.

| 變數 | 解釋 |
| --- | --- |
| *ip-address1* 和 *ip-address2* | Prisma Access 已為指定位置預先配置的輸出 IP 位址。<br>Prisma Access 會為每個位置擷取兩個 IP 位址；您必須將這兩個 IP 位址新增到允許清單。 |
| *subnet-and-mask1* 和 *subnet-and-mask2* | 在您的部署中，Prisma Access 已為輸出 IP 位址預先配置和保留的子網路。 |
| *service-type* | 預先配置的輸出 IP 位址的類型（`gp_portal` 表示 Prisma Access 入口網站或 `gp_gateway` 表示 Prisma Access 閘道）。 |
| *validity-period* | 預先配置的 IP 位址有效的剩餘時間（以天為單位）。<br>在 IP 位址的有效期結束之前，裝載您的行動使用者位置。如果預先配置的 IP 位址到期，您可以重新執行 API 指令碼，以擷取另一組預先配置的 IP 位址。 |

如果您嘗試為符合下列其中一個準則的位置預先配置 IP 位址，則可能會收到錯誤：

- 您已裝載位置。
- 您已裝載位置，然後將其刪除。

  在此情況下，請在 .txt 檔案中輸入以下文字，以擷取該位置的行動使用者—GlobalProtect IP 位址：

  ```
  { "serviceType": "gp_gateway", "addrType": "all", "location": "all" }
  ```

- 您已達到授權允許的行動使用者位置數目上限，並且無法新增更多的位置。
- 您已錯誤地輸入位置名稱。
- 您輸入了 **serviceType**，而不是 **gp_gateway**。
- 您輸入了 **actionType**，而不是 **pre_allocate**。

## 設定 Prisma Access IP 位址變更通知

若要在遠端網路的公用 IP 位址變更，以及服務連線、遠端網路連線和行動使用者的回送 IP 位址變更時收到通知，您可以指定一個 URL，其中會在發生變更時警示您。Prisma Access 會使用 HTTP POST 要求來傳送資訊。此 POST 要求包含以下 JSON 格式的通知資料：

```
{"addrType": "public_ip", "addrChangeType": "add",
"utc_timestamp":"2019-01-31 23:08:19.383894", "text":"Address List
Change Notification"}
```


©2025 Palo Alto Networks, Inc.

```
 {"addrType": "public_ip", "addrChangeType": "delete",
"utc_timestamp":"2019-01-31 23:13:35.882151", "text":"Address List
Change Notification"}
```

```
 {"addrType": "loopback_ip", "addrChangeType": "update",
"utc_timestamp":"2019-01-31 23:29:27.100329", "text":"2018-05-11
23:29:27.100329"}
```

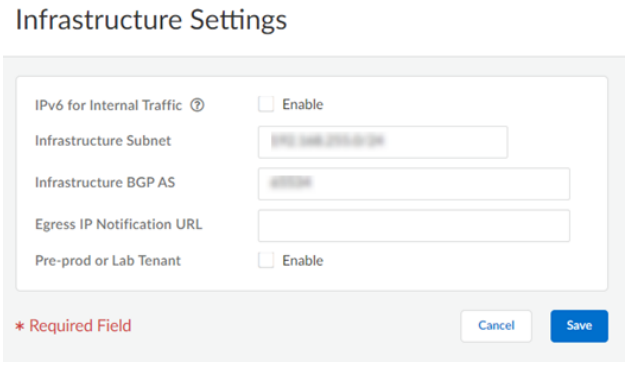
收到通知時，您必須遵循兩步驟程序。首先，您必須手動或以程式設計方式擷取 IP 或回送位址。然後，您必須更新組織相應允許清單中的 IP 位址，以確保使用者不會遭遇任何服務中斷。

*Prisma Access* 會在新 *IP* 位址生效前幾秒鐘傳送此通知。我們建議您使用自動化指令碼，來擷取新的 *IP* 位址並將其新增至網路中的允許清單。

若要新增 IP 通知 URL，請完成下列工作。

**STEP 1 |** 前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Prisma Access** > **Infrastructure Settings**（基礎結構設定）

**STEP 2 |** 新增 **Egress IP Notification URL**（輸出 **IP** 通知 **URL**），其中您可以在 Prisma Access 基礎結構中發生 IP 位址變更時收到通知。




您可以指定 HTTP 或 HTTPS Web 服務的 IP 位址或 FQDN，接聽變更通知。Prisma Access 會使用公用 IP 位址從網際網路傳送這些通知。

您無需推送您的設定，通知 URL 就會生效。

## 擷取 Prisma Access 的 IP 位址 (Panorama)

如果您要手動將 Prisma Access 基礎結構的 IP 位址新增到您網路中的允許清單，或是如果使用自動化指令碼，強制執行 IP 型限制，以限制對企業應用程式的輸入存取，您應該瞭解這些位址的作用，以及您需要允許它們的原因，以及擷取它們所執行的工作。

Prisma Access 不會佈建這些 IP 位址，直到您完成 Prisma Access 設定。部署完成後，您可以使用 API 指令碼擷取這些 IP 位址。API 指令碼會使用您從 Prisma Access UI 取得的 API 金鑰，以及您建立的 .txt 檔案，此檔案會指定您想要擷取的位址。

 ©2025 Palo Alto Networks, Inc.

如果您有行動使用者—*GlobalProtect* 部署，則可以使用 *Prisma Access UI*（而不是此 *API*）來管理公用 *IP* 位址配置，並確認在 *Prisma Access* 釋出 *IP* 位址之前，*IP* 位址已新增至您的允許清單。如此，*Prisma Access* 僅會佈建您已列入允許清單的 *IP* 位址。

下表為您提供了 Prisma Access 用於每種部署類型的 IP 位址清單，以及您在執行 API 指令碼以擷取 IP 位址時使用的關鍵字，並描述您是否應該將它們新增到您組織的允許清單。

| 部署類型 | IP 位址類型 | 說明 |
|---|---|---|
| 行動使用者—**GlobalProtect** | Prisma Access 閘道 (**gp_gateway**) | 閘道 IP 位址針對您的行動使用者部署，您必須同時將閘道和入口網站 IP 位址新增至允許清單。<br><br>行動使用者會連線至 Prisma Access 閘道，以存取您已為其提供存取權的內部或網際網路資源，例如 SaaS 或公用應用程式。<br><br>對於行動使用者，在初始部署期間，Prisma Access 為您部署的每個位置指派兩個 IP 位址。 |
| | Prisma Access 入口網站 (**gp_portal**) | 入口網站 IP 位址。針對您的行動使用者部署，您必須同時將閘道和入口網站 IP 位址新增至允許清單。<br><br>行動使用者登入 Prisma Access 入口網站，來接收其初始設定和閘道位置。 |
| | 回送 IP 位址 | Prisma Access 用於對內部來源所提出要求的來源 IP 位址，並且是從 設定 Prisma Access 服務基礎結構 (Panorama) 指派的。將回送 IP 位址新增到您網路中的允許清單，以將 Prisma Access 提供給 RADIUS 或 Active Directory 驗證伺服器等內部資源。<br><br>Palo Alto Networks 建議您在網路中允許整個基礎結構子網路的所有 IP 位址，因為回送 IP 位址可能會變更。若要尋找基礎結構子網路，請選取 **Panorama** > |


©2025 Palo Alto Networks, Inc.

| 部署類型 | IP 位址類型 | 說明 |
| --- | --- | --- |
| | | **Cloud Services**（雲端服務）> **Status**（狀態）> **Network Details**（網路詳細資訊）> **Service Infrastructure**（服務基礎結構）。子網路會顯示在 **Infrastructure Subnet**（基礎結構子網路）區塊中。<br><br>若要擷取回送 IP 位址，請使用舊版 API 指令碼。 |
| 行動使用者—明確 **Proxy** | 驗證快取服務 (ACS) | Prisma Access 服務的位址，該服務儲存明確 Proxy 使用者的驗證狀態。<br><br>此位址僅用於行動使用者的明確 Proxy。 |
| | 網路負載平衡器 | Prisma Access 用於明確 Proxy 網路負載平衡器的位址。<br><br>此位址僅用於行動使用者的明確 Proxy。 |
| 遠端網路 | 遠端網路 IP 位址 (**remote_network**) | Prisma Access 為 Prisma Access 遠端網路連線指派的 **Service IP Addresses**（服務 **IP** 位址），以及 Prisma Access 用來確保遠端網路使用者為其區域取得正確預設語言的 遠端網路：服務 IP 位址和輸出 IP 位址配置。將這些位址新增到您網路中的允許清單，以將 Prisma Access 提供給網際網路資源。 |
| | 回送 IP 位址 | Prisma Access 用於對內部來源所提出要求的來源 IP 位址，並且是從 設定 Prisma Access 服務基礎結構 (Panorama) 指派的。將回送 IP 位址新增到允許清單，以將 Prisma Access 提供給 RADIUS 或 Active Directory 驗證伺服器等內部資源。若要擷取回送 IP 位址，請使用舊版 API 指令碼。 |


©2025 Palo Alto Networks, Inc.

| 部署類型 | IP 位址類型 | 說明 |
| --- | --- | --- |
| **Clean Pipe** | Clean Pipe IP 位址 (**clean_pipe**) | 將這些 IP 位址新增至允許清單，讓 Clean Pipe 服務可以存取網際網路資源。 |
| | 回送 IP 位址 | Prisma Access 用於對內部來源所提出要求的來源 IP 位址，並且是從 設定 Prisma Access 服務基礎結構 (Panorama) 指派的。將回送 IP 位址新增到允許清單，以將 Prisma Access 提供給 RADIUS 或 Active Directory 驗證伺服器等內部資源。若要擷取回送 IP 位址，請使用舊版 API 指令碼。 |

## 執行用來擷取 Prisma Access IP 位址的 API 指令碼

Prisma Access 提供一個 API 指令碼，您可以用來檢擷取它在其基礎結構中使用的公用和私人 IP 位址。如果您需要將公用 IP 位址新增至組織網路中的允許清單，請使用下列步驟，搭配 API 指令碼擷取這些 IP 位址。

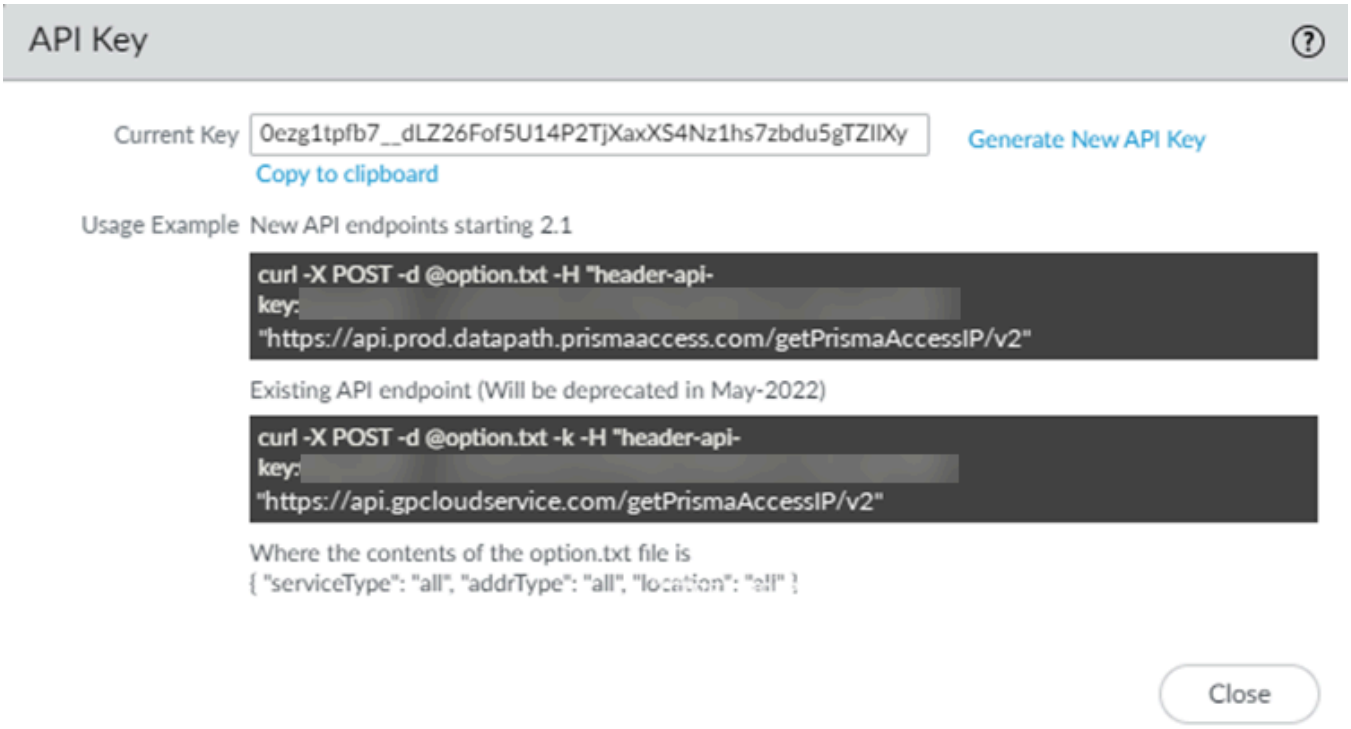
此命令不會擷取回送位址；若要擷取回送 *IP* 位址，請使用舊版 API。


©2025 Palo Alto Networks, Inc.

**STEP 1 |** 取得 API 金鑰。

您需要此金鑰，向 Prisma Access 進行驗證，並使用 API 命令擷取 IP 位址清單。只有 Panorama 管理員或超級使用者才能產生或存取此 API 金鑰。

1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定）。
2. 選取 **Generate API Key**（產生 **API** 金鑰）。




如果您已產生 API 金鑰，則 **Current Key**（目前金鑰）即會顯示。如果您尚未產生金鑰，或想要取代現有金鑰，以符合稽核或合規性檢查，進行金鑰輪換，請按一下 **Generate New API Key**（產生新的 **API** 金鑰）以取得新金鑰。

**STEP 2 |** 建立 .txt 檔案，並將 API 命令選項放入該檔案中。

使用 API 時，要使用的命令是兩步程序。首先，建立 .txt 檔案，為要擷取的 IP 位址指定參數，然後將該檔案儲存在可從命令執行所在位置存取的資料夾中。然後，執行 API 並指定您在命令中建立的 .txt 檔案的名稱和位置。

在 .txt 檔案中指定以下關鍵字和參數。如需範例，請參閱 擷取 Prisma Access IP 位址的 API 範例。本主件中的範例使用檔案名稱 **options.txt**，但是您可以指定任何檔案名稱，只要您在命令中參考它即可。

| 引數 | 可能選項（關鍵字） | 註解 |
|---|---|---|
| **serviceType** | **all**<br>**remote_network**<br>**gp_gateway** | **all**—擷取您需要針對所有服務類型（遠端網路、行動使用者（閘道和入口網站）和 Clean Pipe，適用於您的部署）將其新增到允許清單的 IP 位址。 |


©2025 Palo Alto Networks, Inc.

| 引數 | 可能選項（關鍵字） | 註解 |
| --- | --- | --- |
| | **gp_portal**<br>**clean_pipe**<br>**swg_proxy**<br>**rbi** | **remote_network**—擷取您需要針對遠端網路部署將其新增到允許清單的 IP 位址。<br>**gp_gateway**—擷取您需要針對行動使用者部署將其新增到允許清單的行動使用者—GlobalProtect 閘道 IP 位址。<br>**gp_portal**—擷取您需要針對行動使用者部署將其新增到允許清單的行動使用者—GlobalProtect 入口網站 IP 位址。<br>**clean_pipe**—擷取您需要針對 Clean Pipe 部署將其新增到允許清單的 IP 位址。<br>**swg_proxy**—為每個已部署的明確 Proxy 位置、驗證快取服務 (ACS) 和網路負載平衡器擷取輸出 IP 位址。<br>**RBI**—擷取您需要針對遠端瀏覽器隔離 (RBI) 部署將其新增到允許清單，以連線到 SaaS 應用程式的輸出 IP 位址。 |
| **addrType** | **all**<br>**active**<br>**service_ip**<br>**auth_cache_service**<br>**network_load_balancer** | **all** 或 **active**—擷取您需要將其新增到允許清單的所有 IP 位址。<br>此 API 不會擷取回送 IP 位址。若要擷取回送 IP 位址，請使用舊版 API。<br>**service_ip**—擷取 **Service IP Address**（服務 **IP** 位址），您會在為遠端網路連線設定 IPSec 通道時使用此服務 IP 位址作為對等 IP 位址。<br>**auth_cache_service**—為明確 Proxy ACS 擷取 IP 位址（僅適用於明確 Proxy 部署）。<br>**network_load_balancer**—為明確 Proxy 網路負載平衡器擷取 |


©2025 Palo Alto Networks, Inc.

| 引數 | 可能選項（關鍵字） | 註解 |
| --- | --- | --- |
| | | IP 位址（僅適用於明確 Proxy 部署）。 |
| **actionType** | **pre_allocate** | 僅限行動使用者部署—**actionType** 若為 **pre_allocate**，可讓您針對行動使用者部署擷取 Prisma Access 閘道和入口網站的 IP 位址或子網路。使用此引數搭配其值為 **gp_gateway** 的 **serviceType**，以擷取預先配置的閘道 IP 位址，以及搭配其值為 **gp_portal** 的 **serviceType**，擷取預先配置的入口網站 IP 位址。<br><br>擷取預先配置的 IP 位址，可讓您在裝載行動使用者位置之前，將閘道和入口網站 IP 位址新增到您組織的允許清單，從而讓行動使用者能夠在您裝載這些位置後立即存取外部 SaaS 應用程式。 |
| **location** | **all**<br><br>**deployed** | **all**—從所有位置擷取 IP 位址。對於行動使用者部署，此關鍵字會針對您在裝載期間新增的位置和您未新增的位置擷取 IP 位址。<br><br>**deployed**—擷取您在行動使用者裝載期間新增的所有位置中的 IP 位址。<br><br>此關鍵字僅適用於行動使用者部署。Prisma Access 會在佈建期間關聯每個行動使用者位置的 IP 位址，即使您在行動使用者裝載期間未選取該位置也一樣。如果您指定 **all**，API 命令會擷取所有行動使用者位置的 IP 位址，包括您未針對部署選取的位置。如果您指定 **deployed**，則 API 命令僅針對 |

 ©2025 Palo Alto Networks, Inc.

| 引數 | 可能選項（關鍵字） | 註解 |
| --- | --- | --- |
| | | 您在裝載期間選取的位置擷取 IP 位址。 |

請採取以下格式指定 .txt 檔案中的選項：

```
{ "serviceType": "service-type", "addrType": "address-type",
"location": "location" }
```

**STEP 3 |** 請輸入下列命令以擷取 IP 位址：

- 若要使用 Prisma Access 2.1 中引進的較新 API，請輸入下列命令：

```
curl -X POST --data @option.txt -H header-api-key:Current-
API-Key "https://api.prod.datapath.prismaaccess.com/
getPrismaAccessIP/v2"
```

自 *2023* 年 *5* 月起，一些 *Panorama* 受管理部署會使用 *https://api.prod6.datapath.prismaaccess.com/getPrismaAccessIP/v2*（請注意，*URL* 中的 *prod6*，而不是 *prod*）。

- 若要使用舊版 API，請輸入下列命令。此命令使用將於 2022 年 5 月棄用的舊版 API 端點：

```
curl -X POST --data @option.txt -k -H header-api-key:Current-
API-Key "https://api.gpcloudservice.com/getPrismaAccessIP/v2"
```

其中 *option.txt* 是您在上一個步驟中建立的 .txt 檔案，而 *Current-API-Key* 是 Prisma Access API 金鑰。

例如，假設 .txt 檔案名稱為 **option.txt**，而 API 金鑰為 **12345abcde**，請使用以下 API 命令擷取所有位置的公有 IP 位址：

```
curl -X POST --data @option.txt -H header-api-key:12345abcde
"https://api.prod.datapath.prismaaccess.com/getPrismaAccessIP/v2"
```

*API* 命令可以傳回大量資訊。為了使輸出更具可讀性，如果您安裝了 *Python*，則可以在 *cURL* 命令尾端新增 `| python -m json.tool`。

API 命令會以下列格式傳回位址：

```
{ "result": [ { "address_details": [ { "address":"1.2.3.4"
"allow_listed": false "addressType": "address-type" "serviceType":
```

 ©2025 Palo Alto Networks, Inc.

```
 "service-type" } ], "addresses": [ "1.2.3.4" ] "zone": "zone-
name", "zone_subnet": [zone-subnet ] }, "status": "success"
```

其中：

- **address_details** 顯示每個位置的位址詳細資訊。
  - **serviceType** 顯示 IP 位址的類型（遠端網路 (**remote_network**)、Prisma Access 閘道 (**gp_gateway**)、Prisma Access 入口網站 (**gp_portal**)、Clean Pipe (**clean_pipe**) 或遠端瀏覽器隔離 (**RBI**)。
  - **addressType** 指定使用 `addrType` 關鍵字（**active** 或 **pre-allocated**，如果要為行動使用者位置預先配置 IP 位址）指定的位址類型。
  - **address** 顯示您需要將其新增到允許清單的 IP 位址。

    如果 API 傳回多個 IP 位址，Prisma Access 會在 **addresses**（位址）欄位中彙總這些位址。
- **addresses** 列出您需要將其新增到允許清單的位置的所有 IP 位址。
- **zone** 是與 IP 位址相關聯的 Prisma Access 位置。
- **zone_subnet** 是行動使用者閘道和入口網站的子網路。如果您要為行動使用者位置預先配置 IP 位址，Prisma Access 也會提供此子網路。

如果 .txt 檔案中的選項有任何問題，API 會傳回如下的錯誤：

```
 {"status": "error","result":"Invalid json format in the request.
trace_id: xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx "}
```

**STEP 4 |** 使用您擷取的 IP 位址更新內部部署伺服器或 SaaS 應用程式政策規則上的允許清單。

## 用於行動使用者—GlobalProtect 部署的 IP 最佳化

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
|---|---|
| • Prisma Access (Managed by Panorama)<br>• Prisma Access (Managed by Strata Cloud Manager) | • Prisma Access 授權<br>• Prisma Access 5.0 版或更新版本 |

IP 最佳化是一組架構增強功能，可減少部署中的 IP 位址總數，進而簡化允許清單工作流程，同時提高彈性，並更快速地裝載 Prisma Access 租用戶。

- 用於行動使用者—**GlobalProtect** 部署的更簡單公用 **IP** 位址允許清單 - 在現有 Prisma Access 位置新增 Prisma Access 位置或遭遇調整事件可能會導致新的 IP 位址配置給行動使用者安全性處理節點 (MU-SPN)。最佳做法是擷取新的輸出和閘道 IP 位址，Prisma Access 會指派這些位址，並將其新增到您網路中的允許清單，以避免 SaaS 應用程式或公司防火牆中斷。這可能導致您管理大量 IP 位址的情況。IP 最佳化減少了您必須管理的 IP 位址數目。
- 更快地裝載 **Prisma Access** 租用戶 - 若沒有 IP 最佳化，您必須跨 Prisma Access 和私人網路將唯一的私人 IP 位址指派給每個裝置，這需要您從有限的公司可路由 IP 位址空間中配置大型 IP

 ©2025 Palo Alto Networks, Inc.

區塊。IP 最佳化讓 Prisma Access 從共用位址空間（預設）和 NAT 私人應用程式流量配置位址。

*IP* 最佳化僅適用於新的 *Prisma Access GlobalProtect* 部署。現有的 *GlobalProtect* 部署不符合資格，包括您從現有的多租用戶部署中建立的新租用戶。此外，如果您將 *GlobalProtect* 部署從使用內部部署閘道和入口網站移轉到 *Prisma Access*，請確保所有使用者執行的 *GlobalProtect* 應用程式版本為 *6.1.4* 和更新版本、*6.2.3* 和更新版本，或 *6.3.0* 和更新版本，然後再啟用此功能。

請注意以下 *IP* 最佳化的額外需求：

- *IP* 最佳化需要 *Prisma Access 5.0* 或更新版本以進行行動使用者最佳化，並且可在您首次設定 *GlobalProtect* 時將其啟用。
- 當您首次設定 *GlobalProtect* 時，系統會詢問您是否要啟用 *Prisma Access IP* 最佳化。
- *IP* 最佳化部署不支援 *IPv6* 用於存取公用（外部）應用程式；支援私人應用程式存取。若要為您的新 *Prisma Access* 部署啟用*IPv6*，請聯繫您的 *Palo Alto Networks* 客戶團隊，他們將開啟一個 *TAC* 案例以滿足該要求。
- 即使啟用了 *IP* 最佳化，擷取 Prisma Access IP 位址的 API 仍然繼續如往常一樣運作。


©2025 Palo Alto Networks, Inc.

# 擷取 Prisma Access IP 位址的 API 範例

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

在 .txt 檔案中輸入 API 命令的關鍵字和引數，以擷取基礎結構 IP 位址時，請使用下列範例。若要變更命令的輸出，請變更 .txt 檔案中的選項；命令本身不會變更。

| 擷取這些 IP 位址 | 在 .txt 檔案中指定這些參數 | 註解 |
| --- | --- | --- |
| 行動使用者 IP 位址 | | |
| 所有行動使用者 IP 位址 | `{ "serviceType": "gp_gateway", "addrType": "all", "location": "all" }` | *addrType* 若為 *all*，表示 Prisma Access 會擷取所選位置的所有 IP 位址設定 GlobalProtect 行動使用者 (Panorama)。<br>*location* 若為 *all*，表示 Prisma Access 會擷取所有可用位置的 IP 位址，包括您尚未裝載的位置。Prisma Access 保留非裝載位置 IP 位址，以便您可以先將這些 IP 位址新增至您的允許清單，然後再裝載它們。 |
| 所裝載行動使用者位置的 IP 位址 | `{ "serviceType": "gp_gateway", "addrType": "all", "location": "deployed" }`<br>或<br>`{ "serviceType": "gp_gateway", "addrType": "active", "location": "deployed" }` | *location* 類型若為 *deployed*，表示 Prisma Access 僅擷取所裝載位置的 IP 位址。<br>使用其值為 *all* 或 *active* 的 *addrType*，來擷取這些閘道 IP 位址。 |
| 遠端網路 IP 位址 | | |
| 擷取所有遠端網路 IP 位址 | `{ "serviceType": "remote_network", "ad` | 此命令會擷取您已裝載的遠端網路的公用和輸出 IP 位址。不要使用其值為 *deployed* 的 |


©2025 Palo Alto Networks, Inc.

| 擷取這些 **IP** 位址 | 在 **.txt** 檔案中指定這些參數 | 註解 |
| --- | --- | --- |
| | `drType": "all", "location": "all" }` | *location*。您可以使用其值為 *active* 的 *addrType*，但它會擷取相同的位址，就像您已將 *addrType* 指定為 *all* 一樣。 |
| **Clean Pipe IP** 位址 | | |
| 擷取所有 Clean Pipe IP 位址 | `{ "serviceType": "clean_pipe", "addrType": "all", "location": "all" }` | 此命令會擷取您已裝載的 Clean Pipe 的公用和輸出 IP 位址。不要使用其值為 *deployed* 的 *location*。您可以使用其值為 *active* 的 *addrType*，但它會擷取相同的位址，就像您已將 *addrType* 指定為 *all* 一樣。 |
| 明確 **Proxy IP** 位址 | | |
| 擷取所部署位置的 ACS IP 位址 | `{ "serviceType": "swg_proxy", "location": "all", "addrType": "all" }` | 此命令會為每個部署的明確 Proxy 位置、驗證快取服務 (ACS) 和網路負載平衡器（僅與明確 Proxy 部署相關）擷取輸出 IP 位址。 |
| 遠端瀏覽器隔離 **IP** 位址 | | |
| 為所部署位置擷取遠端瀏覽器隔離 (RBI) IP 位址 | `{ "serviceType": "rbi", "location": "all", "addrType": "all" }` | 此命令會為每個部署的 RBI 位置擷取輸出 IP 位址。您可以將這些 IP 位址新增至允許清單，以連線到 SaaS 應用程式。 |


©2025 Palo Alto Networks, Inc.

# 在 Prisma Access IP 位址變更時收到通知

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

若要在遠端網路的公用 IP 位址變更，以及服務連線、遠端網路連線和行動使用者的回送 IP 位址變更時收到通知，您可以指定一個 URL，其中會在發生變更時警示您。Prisma Access 使用 HTTP POST 要求傳送通知。此 POST 要求包含以下 JSON 格式的通知資料：

```
 {"addrType": "public_ip", "addrChangeType": "add",
"utc_timestamp":"2019-01-31 23:08:19.383894", "text":"Address List
Change Notification"}
```

```
 {"addrType": "public_ip", "addrChangeType": "delete",
"utc_timestamp":"2019-01-31 23:13:35.882151", "text":"Address List
Change Notification"}
```

```
 {"addrType": "loopback_ip", "addrChangeType": "update",
"utc_timestamp":"2019-01-31 23:29:27.100329", "text":"2018-05-11
23:29:27.100329"}
```

收到通知時，您必須遵循兩步驟程序。首先，您必須手動或撰寫程式，來擷取 IP 或回送位址。然後，您必須更新組織相應允許清單中的 IP 位址，以確保使用者不會遭遇任何服務中斷。

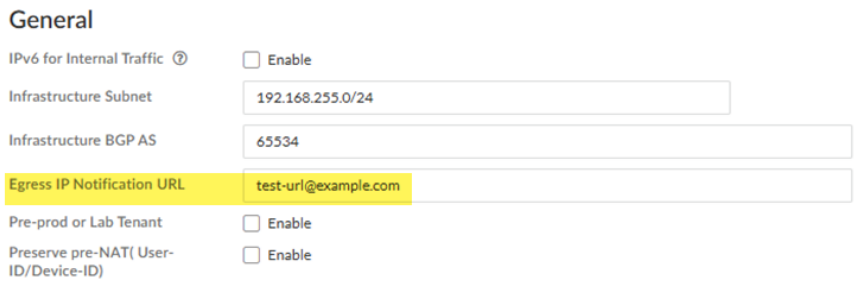
*Prisma Access* 會在新 *IP* 位址生效前幾秒鐘傳送此通知。我們建議您使用自動化指令碼，來擷取新的 *IP* 位址並將其新增至網路中的允許清單。

若要新增 IP 位址通知 URL，請完成下列工作。

- 對於 Prisma Access (Managed by Strata Cloud Manager) 部署，前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Prisma Access** > **Infrastructure Settings**（基礎結構設定）、按一下齒輪以編輯設定、新增 **Egress IP Notification URL**（輸出 **IP** 通知

 ©2025 Palo Alto Networks, Inc.

**URL**）（其中您可以在 Prisma Access 基礎結構中的 IP 位址變更時收到通知），並 **Save**（儲存）您的變更。




- 對於 Prisma Access (Managed by Panorama) 部署，請前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定） 並新增 **IP Change Event Notification URL**（**IP** 變更事件通知 **URL**）（其中您可以在 Prisma Access 基礎結構中的 IP 位址變更時收到通知），然後按一下 **OK**（確定）。




您可以指定 HTTP 或 HTTPS Web 服務的 IP 位址或 FQDN，接聽變更通知。Prisma Access 會使用公用 IP 位址從網際網路傳送這些通知。

您無需提交變更，通知 URL 就會生效。


©2025 Palo Alto Networks, Inc.

# 使用舊版指令碼擷取 IP 位址

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

自 *Prisma Access 1.5* 起，本節中描述的命令已被較新的 *API* 指令碼取代；不過，當您需要取得回送位址時，或者對於在指令碼或其他自動化工具中使用它們的部署，仍然支援這些命令。

下表顯示的關鍵字和參數可在與 Prisma Access 搭配使用的舊版 API 指令碼中使用，並提供有關要為您具有的部署類型使用哪個 API 的資訊和建議。

這些舊版命令也會擷取公用 *IP* 和輸出 *IP* 位址；不過，Palo Alto Networks 建議您使用較新的 API 指令碼來擷取這些命令，並且僅使用舊版 API 來擷取回送 IP 位址。

- 公用 *IP* 位址是來源 IP 位址，Prisma Access 將其用於對網際網路型來源提出的要求。將公有 IP 位址新增到您網路中的允許清單，以將 Prisma Access 提供給網際網路資源，例如 SaaS 應用程式或可公開存取的合作夥伴應用程式。

  行動使用者、遠端網路和 Clean Pipe 部署會使用公有 IP 位址。

- 輸出 *IP* 位址是 Prisma Access 用於將流量輸出至網際網路的 IP 位址，並且您還必須將這些位址新增到允許清單，讓 Prisma Access 可以存取網際網路資源。

  除其他目的外，Prisma Access 會使用輸出 IP 位址，以便使用者以他們期望的語言從 Prisma Access 位置接收網頁。所有位置都有公有 IP 位址；不過，並非所有位置都有輸出 IP 位址。以下位置不會使用輸出 IP 位址：

  - 在發行 Prisma Access 1.4 之前您新增的任何位置。
  - 巴林
  - 比利時
  - 法國北部
  - 法國南部
  - 香港
  - 愛爾蘭
  - 韓國
  - 臺灣
  - 英國

  行動使用者、遠端網路和 Clean Pipe 部署會使用輸出 IP 位址。


©2025 Palo Alto Networks, Inc.

| 行動使用者部署中使用的命令 | |
|---|---|
| 命令名稱 | 註解 |
| **get_egress_ip_all=yes** 命令<br>`curl -H header-api-key:Current-API-Key"https://api.prod.datapath.prismaaccess.com/getAddrList/latest?get_egress_ip_all=yes` | 此命令會擷取您新增到允許清單的所有 IP 位址，以將 Prisma Access 提供給網際網路資源，例如 SaaS 應用程式或可公開存取的合作夥伴應用程式。此命令具有以下限制：<br>• 此命令可以擷取大量位址（超過 200 個）。如果您的企業無法將此數量的 IP 位址新增到允許清單，您可以使用 *gpcs_gp_gw* 和 *gpcs_gp_portal* 關鍵字，僅擷取您目前使用的 IP 位址；不過，每次您新增位置時，都必須重新執行這些命令。此外，如果發生調整事件，您將需要將新的 IP 位址新增到允許清單。<br>• Prisma Access 不會列出與這些 IP 位址相關聯的位置；因此，我們建議您將此命令傳回的所有 IP 位址都新增到允許清單。<br>• 此命令不會為您提供回送位址。 |
| **gpcs_gp_gw** 和 **gpcs_gp_portal** 關鍵字<br>`curl -H header-api-key:Current-API-Key"https://api.prod.datapath.prismaaccess.com/getAddrList/latest?fwType=gpcs_gp_gw \| gpcs_gp_portal&addrType=public_ip \| egress_ip_list \| loopback_ip"` | 如果您的部署限制了您可以新增到允許清單的 IP 位址數量，請使用此命令。您必須將此命令傳回的所有 IP 位址新增到您網路中的允許清單。您也可以使用此命令擷取回送 IP 位址。 |

| 遠端網路部署中使用的命令 | |
|---|---|
| 命令名稱 | 註解 |
| **gpcs_remote_network** 關鍵字<br>`curl -H header-api-key:Current-API-Key"https://api.prod.datapath.prismaaccess.com/getAddrList/latest?fwType=gpcs_remote_network&addrType=public_ip \| egress_ip_list \| loopback_ip"` | 使用此命令，尋找您需要針對遠端網路部署將其新增到允許清單的 IP 位址。<br>您還可以使用此命令，為遠端網路部署尋找輸出 IP 位址；在某些情況下，輸出和 IP 位址可能不同。 |


©2025 Palo Alto Networks, Inc.

| Clean Pipe 部署中使用的命令 | |
|---|---|
| 命令名稱 | 註解 |
| **gpcs_clean_pipe** 關鍵字<br>`curl -H header-api-key:`*Current-API-Key*`"https://api.prod.datapath.prismaaccess.com/getAddrList/latest?fwType=gpcs_clean_pipe&addrType=public_ip \| egress_ip_list \| loopback_ip"` | 使用此命令，尋找您需要針對 Clean Pipe 部署將其新增到允許清單的 IP 位址。 |

# 擷取行動使用者 IP 位址

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

自 *Prisma Access 1.5* 起，此舊版指令碼已被新的 *API* 指令碼取代。*Palo Alto Networks* 建議您使用較新的指令碼，來擷取除回送位址外的所有 *IP* 位址。

如果您要將公有 IP 位址新增至允許清單，讓行動使用者可以存取 SaaS 或公有應用程式，Prisma Access 會為每個閘道和入口網站 IP 位址提供兩個 IP 位址，以便在調整或其他事件期間可以使用一個 IP 位址。您可以在使用這組 IP 位址之前將其新增到允許清單，從而防止任何問題，讓行動使用者能夠在調整事件期間存取 SaaS 或公用應用程式。

透過完成以下工作來擷取這些新位址：

**STEP 1 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定），然後選取 **Generate API Key**（產生 **API** 金鑰），來取得 API 金鑰。

您需要此金鑰，向 Prisma Access 進行驗證，並使用底下所列的 curl 命令擷取 IP 位址清單。只有 Panorama 管理員或超級使用者才能產生或存取此 API 金鑰。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 請輸入下列命令以擷取行動使用者公用 IP 位址：

```
  curl -H header-api-key:Current-API-Key "https://
api.prod.datapath.prismaaccess.com/getAddrList/latest?
get_egress_ip_all=yes"
```

其中 *Current-API-Key* 是 Prisma Access API 金鑰。

例如，假設 API 金鑰為 **12345abcde**，請使用以下 API 命令擷取所有位置的公有 IP 位址：

```
  curl -H header-api-key:12345abcde "https://
api.prod.datapath.prismaaccess.com/getAddrList/latest?
get_egress_ip_all=yes"
```

每次 Prisma Access 使用一組公用 IP 位址，它會配置另一組 IP 位址。如果您認為 Prisma Access 使用了新增的一組公用 IP 位址（例如，如果大量行動使用者有權存取單一位置），則可以再次執行此 API 命令，來尋找新的一組公用 IP 位址。升級後所有 IP 位址持續存在。

# 擷取公用、回送和輸出 IP 位址

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

自 *Prisma Access 1.5* 起，此舊版指令碼已被較新的指令碼所取代。*Palo Alto Networks* 建議您使用較新的指令碼，來擷取除回送位址外的所有 *IP* 位址。

若要擷取公用、回送和輸出 IP 位址，請完成以下步驟。

**STEP 1 |** 取得 API 金鑰，並新增 **IP Change Event Notification URL**（**IP** 變更事件通知），其中您可以在 Prisma Access 基礎結構中發生 IP 位址變更時收到通知。

如需詳細資料，請參閱 在 Prisma Access IP 位址變更時收到通知。

**STEP 2 |** 為 Prisma Access 擷取公用 IP 位址、回送 IP 位址或兩者。

手動或在自動化指令碼中使用 API 金鑰和 API 端點 URL：

```
 header-api-key:Current API Key "https://
api.prod.datapath.prismaaccess.com/getAddrList/latest?
fwType=$fwType&addrType=$addrType"
```

其中您需要將 Current API Key 取代為您的 API 金鑰，並使用以下一個或兩個關鍵字和引數：

| 關鍵字 | 說明 |
| --- | --- |
| **fwType** 關鍵字 | |

 ©2025 Palo Alto Networks, Inc.

| 關鍵字 | 說明 |
| --- | --- |
| **gpcs_gp_gw** | 擷取 Prisma Access 閘道 IP 位址（適用於行動使用者部署）。 |
| **gpcs_gp_portal** | 擷取 Prisma Access 入口網站 IP 位址（適用於行動使用者部署）。 |
| **gpcs_remote_network** | 擷取 Prisma Access 遠端網路 IP 位址（適用於遠端網路部署）。 |
| **gpcs_clean_pipe** | 擷取 Prisma Access Clean Pipe IP 位址。 |
| **addrType** 關鍵字 | |
| **public_ip** | 擷取 Prisma Access 用於對網際網路型來源所提出要求的來源 IP 位址。<br>對於行動使用者位置，Prisma Access 依位置列出 IP 位址。對於遠端網路，Prisma Access 會依遠端網路名稱列出 IP 位址。 |
| **egress_ip_list** | 擷取 Prisma Access 與公用 IP 位址搭配使用的 IP 位址，以取得網際網路的額外輸出流量。<br>對於行動使用者位置，Prisma Access 依位置列出 IP 位址。對於遠端網路，Prisma Access 依遠端網路名稱列出 IP 位址。 |
| **loopback_ip** | 擷取 Prisma Access 用於對內部來源（例如 RADIUS 或 Active Directory 伺服器）所提出要求的來源 IP 位址，且是從基礎結構子網路指派的。 |

如果未指定關鍵字，則 Prisma Access 會擷取所有 IP 位址。

例如，您可以嘗試以下 Curl 命令，手動擷取所有遠端網路的公用 IP 位址清單：

```
curl -H header-api-
key:1234y9ydxb__0UmxetVTbC8XTyFMaoT4RBZBKBjfX419YVufeFG7
 "https://api.prod.datapath.prismaaccess.com/getAddrList/latest?
fwType=gpcs_remote_network&addrType=public_ip"
```

或者，使用簡單的 Python 指令碼來擷取所有 IP 位址的清單，例如：

```
  #!/usr/bin/python import subprocess import json api_key
 = '1234y9ydxb__0UmxetVTbC8XTyFMaoT4RBZBKBjfX419YVufeFG7'
 # Replace with your key api_end_point = 'https://
api.prod.datapath.prismaaccess.com/getAddrList/latest' # This call
```

 ©2025 Palo Alto Networks, Inc.

```
retrieves IP addresses for all your Prisma Access firewalls args =
['curl', '-k', '-H', 'header-api-key:' + api_key, api_end_point]
p = subprocess.Popen(args, stdout=subprocess.PIPE) output
= p.communicate() dout = json.loads(output[0]) addrStrList
= dout['result']['addrList'] addrList = [] for addr_str
in addrStrList: addrList.append(addr_str.split(":")[1])
print(addrList)
```

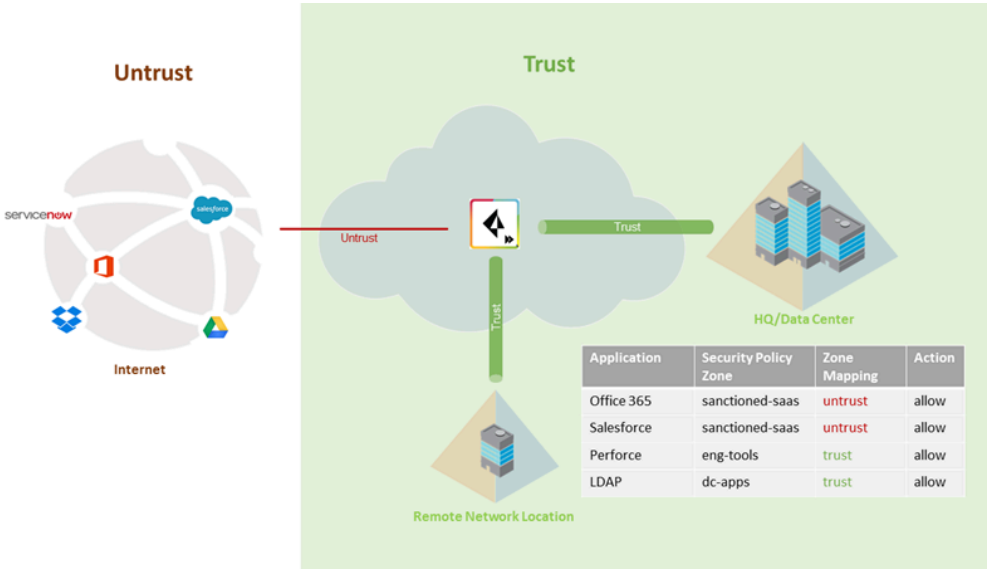
**STEP 3 |** 使用您擷取的 IP 位址更新內部部署伺服器或 SaaS 應用程式政策規則上的允許清單。

 ©2025 Palo Alto Networks, Inc.

# Prisma Access 區域

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

在防火牆上，區域與介面相關聯。但在 Prisma Access 內，自動為您設定網路基礎結構。這意味著您不再需要擔心設定介面，並將它們與您建立的區域建立關聯。不過，若要啟用一致的安全性政策強制執行，您必須建立區域對應，以便 Prisma Access 知道是否將區域與內部（信任）介面或外部（不信任）介面建立關聯。這將確保適當地強制執行您的安全性政策規則。根據預設，您推送到 Prisma Access 的所有區域都會設定為不信任。您應該將與網際網路繫結流量相關聯的任何區域（包括您認可的 SaaS 應用程式）設定為不信任。不過，對於可存取內部網路上或資料中心裡應用程式的所有區域，您必須將它們對應到信任。請注意，在下面的範例中，所有已認可的 SaaS 應用程式（本案例中為 Office 365 和 Salesforce）都被分段至認可的 SaaS 區域，以對這些應用程式的使用啟用可視性和政策強制執行。若要啟用 Prisma Access 將 sanctioned-saas 區域與面向外部的介面建立關聯，您必須將此區域對應到不信任。同樣，eng-tools 和 dc-apps 區域提供對公司辦公室中應用程式的存取，因此您必須將它們指定為受信任區域。




Prisma Access 支援三個區域（信任、不信任和無用戶端 VPN），並透過為您設定它們來簡化政策建立。

| 區 | 說明 |
| --- | --- |
| 信任 | 此區域包含公司網路內所有受信任且已裝載的 IP 位址、服務連線或行動使用者。 |


©2025 Palo Alto Networks, Inc.

| 區 | 說明 |
| --- | --- |
| 不信任 | 公司網路外部所有不受信任的 IP 位址、服務連線或行動使用者。根據預設，任何不受信任的 IP 位址或行動使用者本質上都是不受信任的。 |
| 無用戶端 VPN | 可遠端安全存取使用 HTML、HTML5 和 JavaScript 技術的常用企業 Web 應用程式。使用者具有可從已啟用 SSL 的 Web 瀏覽器進行安全存取的優點，而無需安裝用戶端軟體。當您需要為合作夥伴或派遣員工啟用應用程式存取權時，以及要安全地啟用未受管理的資產（包括個人裝置）時，此功能相當實用。<br><br>無用戶端 *VPN* 的區域預設會對應到信任區域；此設定無法變更。 |

顯示 **inter-fw** 區域的 Prisma Access 日誌是用於 Prisma Access 基礎結構內通訊的日誌。

建立區域時，請勿使用以下任何區域名稱，因為這些名稱用於內部區域：

- 信任
- 不信任
- inter-fw
- 用於遠端網路的任何名稱（遠端網路名稱用作 Strata Logging Service 日誌中的來源區域)

顯示 *inter-fw* 區域的 *Prisma Access* 日誌是用於 *Prisma Access* 基礎結構內通訊的日誌。


©2025 Palo Alto Networks, Inc.

# DNS for Prisma Access

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

Prisma Access 可讓您指定 DNS 伺服器，以解析組織內部網域和外部網域。這樣做可以提供對企業網路上服務 (例如 LDAP 和 DNS 伺服器) 的存取—尤其是如果您計劃在總部或資料中心設定服務連線以提供對這些類型資源的存取。Prisma Access 支援行動使用者 - Global Protect 和遠端網路部署進行 DNS 解析。對內部網域清單所含網域的 DNS 查詢會傳送至您的本機 DNS 伺服器，以確保資源可供 Prisma Access 遠端網路使用者和行動使用者使用。

例如，如果您想要公司網域的 DNS 查閱僅前往公司 DNS 伺服器，請在這裡指定公司網域和公司 DNS 伺服器。若要確保端點使用 **DNS Proxy IP Address**（**DNS Proxy IP** 位址），它們必須設定為透過 **Workflow**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Prisma Access** > **Prisma Access DNS Proxy IP Address**（**Prisma Access DNS Proxy IP** 位址）中顯示的 IP 位址來解析 DNS。

- Strata Cloud Manager
- Panorama

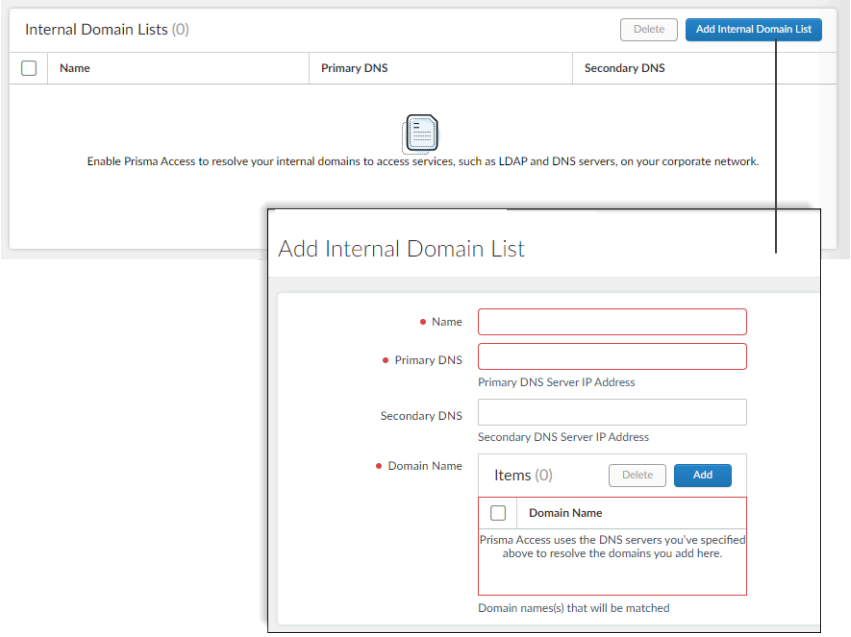
## DNS for Prisma Access (Strata Cloud Manager)

以下是設定 Prisma Access 以解析內部網域的方式，以及如何為行動使用者部署和遠端網站自訂 DNS 設定（解析內部網域和公用網域）的方式。


©2025 Palo Alto Networks, Inc.

設定適用於所有流量的內部網域清單。

1. 選取 **Workflows**（工作流程） > **Prisma Access Setup**設定） > **Prisma Access**， 並 **Add Internal DNS Servers**（新增內部 **DNS** 伺服器）。



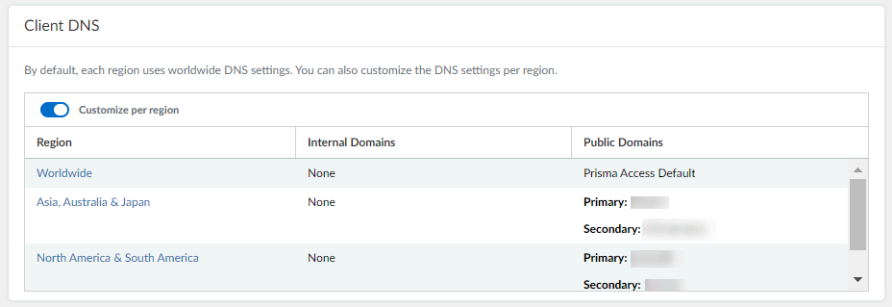

2. 輸入 Prisma Access 應該用來解析內部網域名稱的主要 DNS 伺服器和次要 DNS 伺服器。
3. 新增內部網域名稱以傳送至這些 DNS 伺服器進行解析。

   您可以在網域清單中的網域前面使用萬用字元 (*)， 例如 *.acme.local 或 *.acme.com。

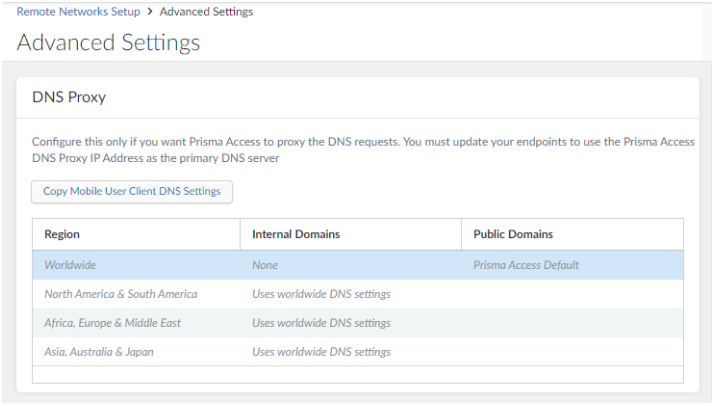
 ©2025 Palo Alto Networks, Inc.

新增僅適用於特定行動使用者部署或遠端網站的內部網域清單。

1. 設定 DNS 設定：
   - 行動使用者—前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **GlobalProtect** > **Infrastructure Settings**（基礎結構設定）尋找 **Client DNS**（用戶端 **DNS**）。




   - 遠端網路—前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Remote Networks**（遠端網路） > **Advanced Settings**（進階設定）尋找 **DNS Proxy**。




2. 使用全球預設值（Prisma Access 預設 DNS 伺服器）或根據區域自訂設定。無論哪種情況，請選取區域來調整並自訂該區域的 DNS 設定。
3. 選取選項以 **use these DNS settings to resolve internal domains**（使用這些 **DNS** 設定來解析內部網域），並選擇性地 **Use the internal DNS Server for resolving public domains too**（也將內部 **DNS** 伺服器用於解析公用網域）。如果您未選取此選項，Prisma Access 會使用其雲端預設 DNS 伺服器來解析公用網域的要求。
4. 允許流量從行動使用者 IP 位址集區中的所有位址流向您的 DNS 伺服器。

   Prisma Access 中的 DNS Proxy 會將要求傳送到您指定的 DNS 伺服器。DNS 要求中的來源位址是 IP 集區中您指派給該區域的第一個 IP 位址。為了確保您的 DNS 要求可以到達伺服器，需要確保您允許流量從行動使用者 IP 位址集區中的所有位址流向 DNS 伺服器。

# DNS for Prisma Access (Panorama)

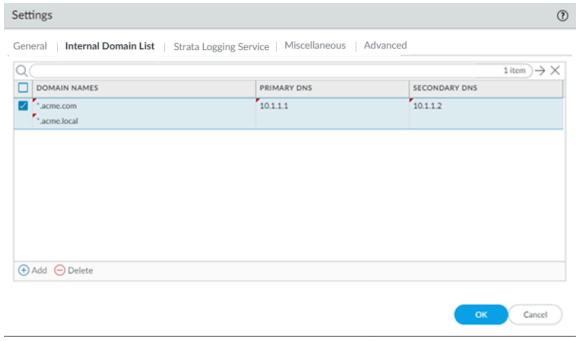
設定 Prisma Access 以解析內部網域。

 ©2025 Palo Alto Networks, Inc.

設定適用於所有流量的內部網域清單。

1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定），然後按一下齒輪圖示以編輯設定。
2. 選取 **Internal Domain List**（內部網域清單）頁籤。
3. 新增您想要 Prisma Access 用來解析內部網域名稱的網域名稱、主要 DNS 和次要 DNS 伺服器。

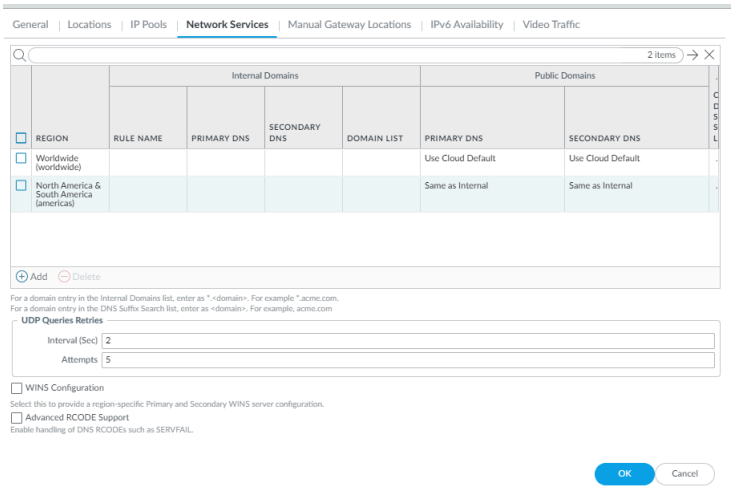
   您可以在網域清單中的網域前面使用萬用字元 (*)，例如 *.acme.local 或 *.acme.com。



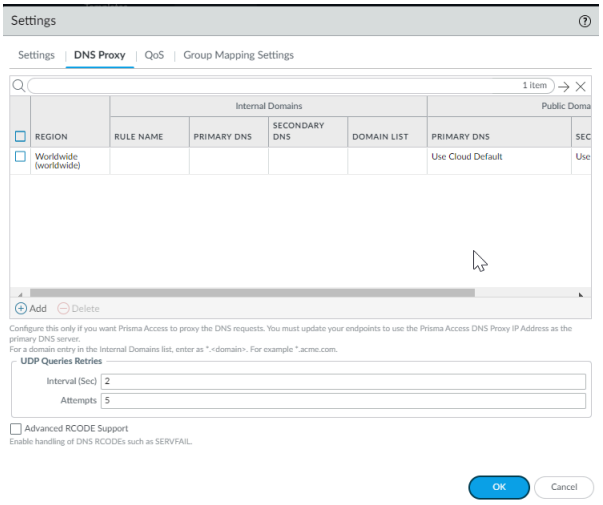

 ©2025 Palo Alto Networks, Inc.

新增僅適用於特定行動使用者部署或遠端網站的內部網域清單。

1. 設定 DNS 設定：
   - 行動使用者—前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users - GlobalProtect**（行動使用者 - **GlobalProtect**），然後選取外部閘道 > 並按一下 **Network Services**（網路服務）。




   - 遠端網路—前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路） > **Settings**（設定） > **DNS Proxy**。




2. 使用全球預設值（Prisma Access 預設 DNS 伺服器）或根據區域自訂設定。無論哪種情況，請選取區域來調整並自訂該區域的 DNS 設定。
3. 新增一或多個規則以設定 **Internal Domain**（內部網域）的 DNS 設定。
   - 為規則輸入唯一的規則名稱。
   - 如果您想要內部 DNS 伺服器僅解析您指定的網域，請在網域清單中輸入要解析的網域。在網域前面指定一個星號；例如，*.acme.com。。您最多可以指定 1,024 個網域項目。

     Prisma Access 具有預先定義的規則，用於使用雲端預設伺服器解析 *.amazonaws.com 網域。如果您想要內部 DNS 伺服器解析更具體的 *.amazonaws.com 網域 (例

 ©2025 Palo Alto Networks, Inc.

如，*.s3.amazonaws.com)，請在網域清單中輸入 URL。Prisma Access 會評估清單中的網域名稱，從最長到最短，然後從上到下。

- 如果您有可以存取內部網域的自訂 DNS 伺服器，請指定主要 DNS 和次要 DNS 伺服器 IP 位址，或選取 [Use Cloud Default（使用雲端預設值）] 以使用預設 Prisma Access DNS 伺服器。

4. 指定 **Public Domains**（公用網域） 的 DNS 設定。
   - **Use Cloud Default**（使用雲端預設值）—使用預設 Prisma Access DNS 伺服器。
   - **Same as Internal Domains**（與內部網域相同）—使用您用來解析內部網域的同一伺服器。選取此選項時，用來解析公用網域的 DNS 伺服器與 **Internal Domains**（內部網域）區段中為第一個規則設定的伺服器相同。
   - **Custom DNS server**（自訂 **DNS** 伺服器）—如果您有可存取公用（外部）網域的 DNS 伺服器，請在該欄位中輸入主要 DNS 伺服器位址。
5. （選用）您可以新增用戶端 DNS 尾碼清單，指定輸入無法解析的不完整主機名稱時，用戶端應在本機使用的尾碼，例如，acme.local。請參閱 Prisma Access 管理員指南（Panorama 管理）。不要在網域尾碼前面輸入萬用字元 (*)（例如，acme.com）。您可以新增多個尾碼。
6. 允許流量從行動使用者 IP 位址集區中的所有位址流向您的 DNS 伺服器。

   Prisma Access 中的 DNS Proxy 會將要求傳送到您指定的 DNS 伺服器。DNS 要求中的來源位址是 IP 集區中您指派給該區域的第一個 IP 位址。為了確保您的 DNS 要求可以到達伺服器，需要確保您允許流量從行動使用者 IP 位址集區中的所有位址流向 DNS 伺服器。

 ©2025 Palo Alto Networks, Inc.

# Prisma Access 的高可用性

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

在高可用性 (HA) 設定中部署 Panorama 設備可在系統或網路發生故障時提供備援，並確保您能夠持續連線至 Prisma Access。在 HA 設定中，一個 Panorama 設備對等是主動-主要，另一個是被動-次要。如果發生容錯移轉，次要對等會變成主動，並接管管理 Prisma Access 的角色。

為了簡化 HA 設定，請在購買 Prisma Access 以及 Strata Logging Service 驗證碼和元件之後，在 HA 中設定 Panorama 設備，並將您計劃安裝雲端服務外掛程式的主要 Panorama 設備的序號與驗證碼建立關聯，但在您 啟動和安裝 Panorama Managed Prisma Access 之前。不過，您也可以使用此程序，設定已安裝外掛程式的現有 Panorama 設備。

無論您是剛開始使用一對新的 Panorama 設備，還是已設定獨立 Panorama 設備，並完成了授權和安裝程序，請務必在啟用 HA 之前檢查先決條件：

- 您必須將 Panorama 設備 HA 對等註冊到客戶支援入口網站 (CSP) 上的同一客戶帳戶。
- Panorama 設備對等必須具有相同的規格（相同型號的硬體設備或相同的虛擬設備）和相同的作業系統版本，並且必須具有相同的授權集。Prisma Access 和 Strata Logging Service 需要進階支援授權。
- 主要 Panorama 設備的序號繫結至您的 Prisma Access 和 Strata Logging Service 驗證碼。如果您已在獨立 Panorama 設備上安裝並設定外掛程式，請確保將該 Panorama 設備用作主要對等。如果您需要將此獨立對等指派為次要 Panorama 設備，請聯絡 Palo Alto Networks 支援，以取得將授權轉移至主要 Panorama 設備對等的協助，然後再繼續。

如果您停用 *Panorama* 配對的 *HA* 並還原到單一 *Panorama* 在其中管理 *Prisma Access* 的設定，您必須重新驗證您的帳戶，以防止擷取 *Prisma Access* 元件的狀態時發生錯誤。

若要在 HA 設定中設定 Panorama 設備，請完成下列步驟。

**STEP 1 |** 在 Panorama 上設定 HA。

將主要 Panorama 設備設定為 **Primary**（主要），並將次要 Panorama 設備設定為 **Secondary**（次要），然後確保主要 Panorama 設備的序號繫結至您的 Prisma Access 和 Strata Logging Service 驗證碼。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 確保主要（主動）和次要（被動）Panorama 設備已同步，並且它們之間的 HA 連結狀態為已啟動。

1. 存取主要 Panorama 設備上的 **Dashboard**（儀表板），並選取 **Widgets** > **System**（系統） > **High Availability**（高可用性）來顯示 HA Widget。
2. **Sync to peer**（同步至對等），按一下 **Yes**（是），等待 **Running Config**（執行中設定）顯示 **Synchronized**（已同步）。
3. 確保 **Local**（本機）對等為 **active**（主動）。
4. 存取被動 Panorama 設備上的 **Dashboard**（儀表板），並選取 **Widgets** > **System**（系統） > **High Availability**（高可用性）來顯示 HA Widget。
5. 確認 **Running Config**（執行中設定）顯示 **Synchronized**（已同步）。
6. 確保 **Local**（本機）對等為 **passive**（被動）。

**STEP 3 |** 在主要 Panorama 設備上安裝 Prisma Access 元件。

1. 登入 主要 Panorama 設備，然後選取 **Panorama** > **Licenses**（授權）。
2. 按一下 **Retrieve license keys from license server**（從授權伺服器擷取授權金鑰）。
3. 啟動並安裝 Panorama Managed Prisma Access，包括產生一次性密碼 (OTP) 和驗證您的帳戶。

**STEP 4 |** 檢查 HA 是否已啟用。

1. 在主要 Panorama 設備上，存取 CLI 並輸入以下操作命令：

   ```
   tail follow yes mp-log plugin_cloud_services.log
   ```

2. 在日誌輸出中尋找以下文字，其中 *X* 是主要 Panorama 設備的序號，*Y* 是次要 Panorama 設備的序號：

   ```
   2017-11-06 15:14:07.790 -0800 INFO: [hainfo] Sending
    update to CSP for HA peer serial information to https://
   updates.paloaltonetworks.com/licensesvc/licenseservice.asmx/
   PanoramaHAInfo (https://updates.paloaltonetworks.com/
   licensesvc/licenseservice.asmx/PanoramaHAInfo)
    2017-11-06 15:14:07.791 -0800 INFO: [hainfo] Data
    string is primarypanoramasn=<varname>X</varname>
    &secondarypanoramasn=<varname>Y</varname> 2017-11-06
    15:14:17.595 -0800 INFO: [hainfo] HTTP_CODE 200, RESPONSE:
    <?xml version="1.0" encoding="utf-8"?> <PanoramaHA
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance (http://
   www.w3.org/2001/XMLSchema-instance)" xmlns:xsd="http://
   www.w3.org/2001/XMLSchema (http://www.w3.org/2001/
   XMLSchema)" xmlns="http://www.paloaltonetworks.com/ (http://
   www.paloaltonetworks.com/)"> <success>true</success> </
   PanoramaHA> 2017-11-06 15:14:17.596 -0800 INFO: [hainfo]
    Cached HA Peer's serial number <varname>Y</varname>
   ```

3. 登入 客戶支援入口網站 (CSP)，並選取 **Assets**（資產） > **Cloud Services**（雲端服務），以驗證這兩個 Panorama 對等是否繫結至您的 Prisma Access 和 Strata Logging Service 授權。

 ©2025 Palo Alto Networks, Inc.

4. 檢查主要和次要 Panorama 設備的欄位。

   主要和次要 Panorama 設備的驗證碼、型號名稱、授權說明和到期日期欄位應相同，因為 Palo Alto Networks 已自動將 Prisma Access 授權與次要 Panorama 設備建立關聯。

**STEP 5 |** 登入次要 Panorama 設備，然後啟動並安裝 Panorama Managed Prisma Access。

當您登入 客戶支援入口網站 (CSP) 以產生 OTP 時，請確保指定次要 Panorama 設備的序號。

**STEP 6 |** 在主要和次要 Panorama 設備上提交您的變更。

1. **Commit**（提交） > **Commit and Push**（提交並推送）您的變更。
2. 按一下 **OK**（確定）與 **Commit**（提交）。

**STEP 7 |** 驗證主要和次要 Panorama 設備是否仍處於同步狀態。

 ©2025 Palo Alto Networks, Inc.

# 預先定義範本：裝載服務連線或遠端網路

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

Prisma Access 包含適用於常見第三方 IPSec 和 SD-WAN 裝置的預先定義 IPSec 範本。這些設定檔加快並簡化了使用其中一個裝置終止連線的服務連線和遠端網路連線的裝載。

共用一個通用範本還可讓您透過常用的共用密碼、預先共用金鑰和對等標別碼，裝載多個相同類型的遠端連線。

- 預先定義範本：裝載服務連線或遠端網路
- 常見 SD-WAN 裝置支援的 IKE 和 IPSec 密碼設定檔

Prisma Access 為您提供下列預先定義範本，您可以使用這些範本，在您的內部部署裝置與 Prisma Access 和之間設定 IPSec 通道：

- IPSec 通道（**Network**（網路） > **IPSec Tunnels**（**IPSec** 通道）），在 Remote_Network_Template 和 Service_Conn_Template 之下。
- IKE 閘道（**Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Gateways**（**IKE** 閘道）），在 Remote_Network_Template 和 Service_Conn_Template 之下。
- IPSec 密碼設定檔（**Network**（網路） > **Network Profiles**（網路設定檔） > **IPSec Crypto**（**IPSec** 密碼）），在 Remote_Network_Template 和 Service_Conn_Template 之下。
- IKE 密碼設定檔（**Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Crypto**（**IKE** 密碼）），在 Remote_Network_Template 和 Service_Conn_Template 之下。

目前，有以下廠商的範本可用：

除了以下範本外，我們還提供一個通用範本，您可以使用該範本搭配這裡未列出的任何內部部署裝置。

- Cisco 設備：
  - Cisco 整合式服務路由器 (ISR)
  - Cisco 自適型安全性設備 (ASA)
- Citrix
- Prisma SD-WAN（舊稱為 CloudGenix）
- Riverbed
- Silver Peak

若要使用 Prisma Access 提供的範本裝載服務連線或遠端網路連線，請完成以下工作。


©2025 Palo Alto Networks, Inc.

**STEP 1 |** 在 Panorama 中，執行設定，以便範本顯示在 Panorama 中。

當您升級雲端服務外掛程式時，新範本不會自動顯示。升級後完成一次此步驟，以使範本永久顯示。新的安裝會在第一次設定時執行此初始設定，因此不需要這個額外的步驟。



如果您刪除這些範本並需要擷取它們，也可以完成此步驟。

- 對於服務連線，選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定）、按一下 **Settings**（設定）區域中的齒輪圖示以開啟 **Settings**（設定），然後按一下 **OK**（確定）。
- 對於遠端網路連線，選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路）、按一下 **Settings**（設定）區域中的齒輪圖示以開啟 **Settings**（設定），然後按一下 **OK**（確定）。

**STEP 2 |** 選取 **Network**（網路），然後選取正確的 **Template**（範本）（如果您是建立遠端網路連線，則選取 **Remote_Network_Template**；如果您是建立服務連線，則選取 **Service_Conn_Template**）。

**STEP 3 |** 確定用來終止服務連線或遠端網路連線的裝置類型，並找出要與該裝置搭配使用的範本。



如果您的 *SD-WAN* 或 *IPSec* 裝置不在清單中，請使用通用設定檔。

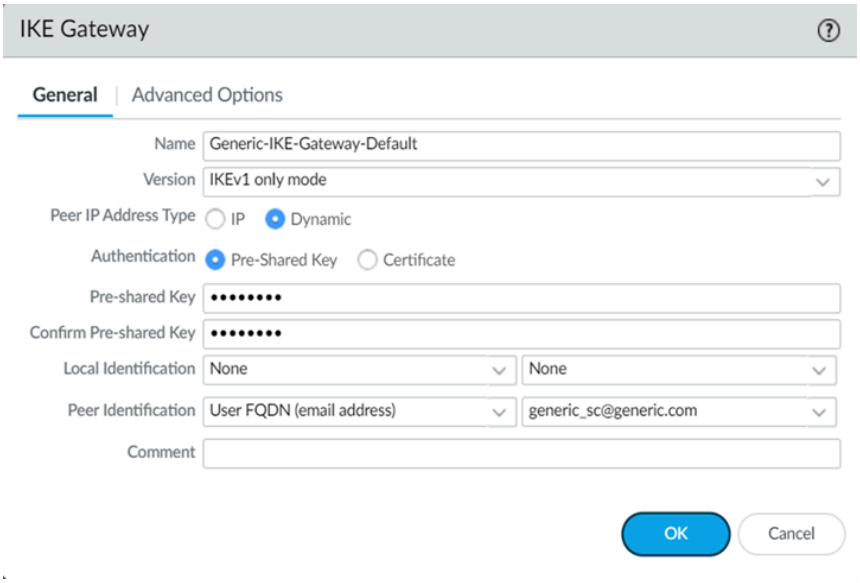

©2025 Palo Alto Networks, Inc.

**STEP 4 |** 選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **IKE Gateways**（**IKE** 閘道），然後為您的裝置對 IKE 閘道設定檔進行以下變更：

您可以使用 IPSec 密碼和 IKE 密碼設定檔，而無需變更；不過，您必須對 IKE 閘道設定檔進行特定變更，以符合網路設定。

- （選用）如果您知道將用來搭配 Prisma Access 設定 IPSec 通道的內部部署裝置的公用 IP 位址，請指定 **Peer IP Address Type**（對等 **IP** 位址類型）為 **IP** 來設定靜態 IP 位址，並輸入 IPSec 通道的 **Peer Address**（對等位址）。
- 如果將預先共用金鑰用於 IPSec 通道，請指定 **Pre-shared Key**（預先共用金鑰）。
- 指定 **Peer Identification**（對等識別）為 **IP Address**（**IP** 位址）或 **User FQDN**（使用者 **FQDN**）。

  請確保在設定用來終止 IPSec 通道另一端的裝置時，您符合這裡指定的設定。




**STEP 5 |** 裝載服務連線或遠端網路連線，同時指定與 IPSec 通道另一端上裝置相符的 **IPSec tunnel**（**IPSec** 通道）設定。

 ©2025 Palo Alto Networks, Inc.

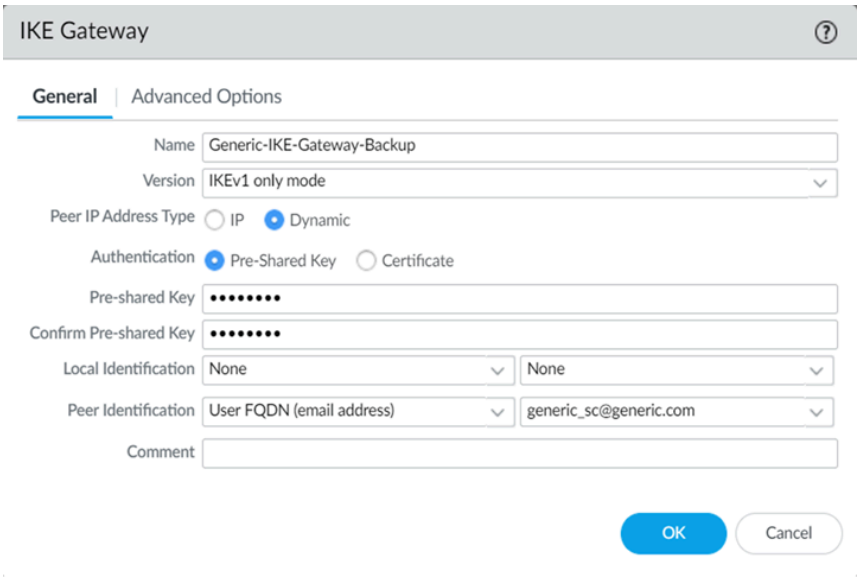
**STEP 6 |** （選用）如果您需要為服務連線或遠端連線新增備用通道（次要 WAN），請執行以下額外的設定步驟。

以下部署不支援設定次要 WAN：

- 如果您的次要 WAN 與主要 IPSec 通道設定為主動-主動模式。
- 如果您的用戶端裝置 (CPE) 在具有主要和次要 IPSec 通道的等價多路徑 (ECMP) 設定中設定。

1. 為備份通道建立一個新的 IKE 閘道，同時從預先定義範本複製您想要重複的設定。

   以下範例為通用網路裝置建立備份通道設定。

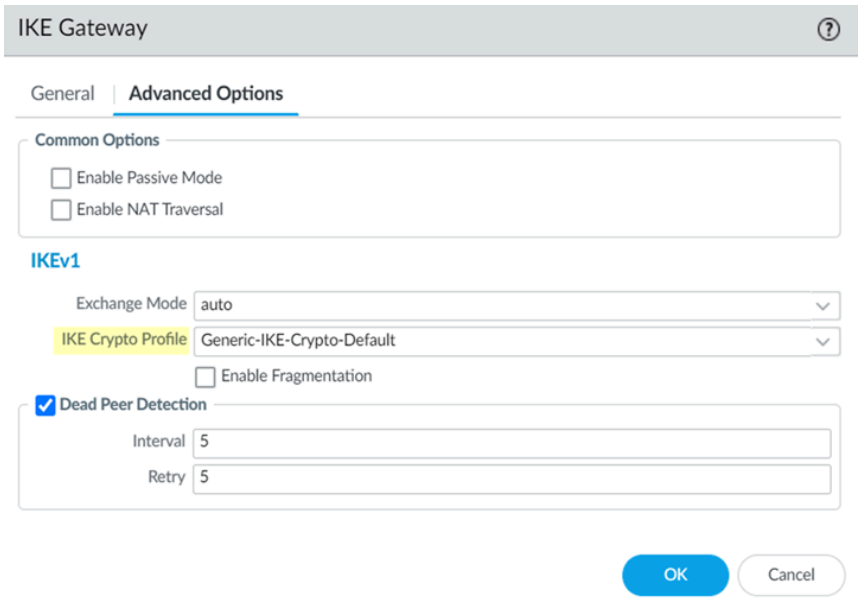



2. 在 **Advanced Options**（進階選項）中，為預先定義範本指定您想要使用的 **IKE Crypto Profile**（**IKE** 密碼設定檔）。

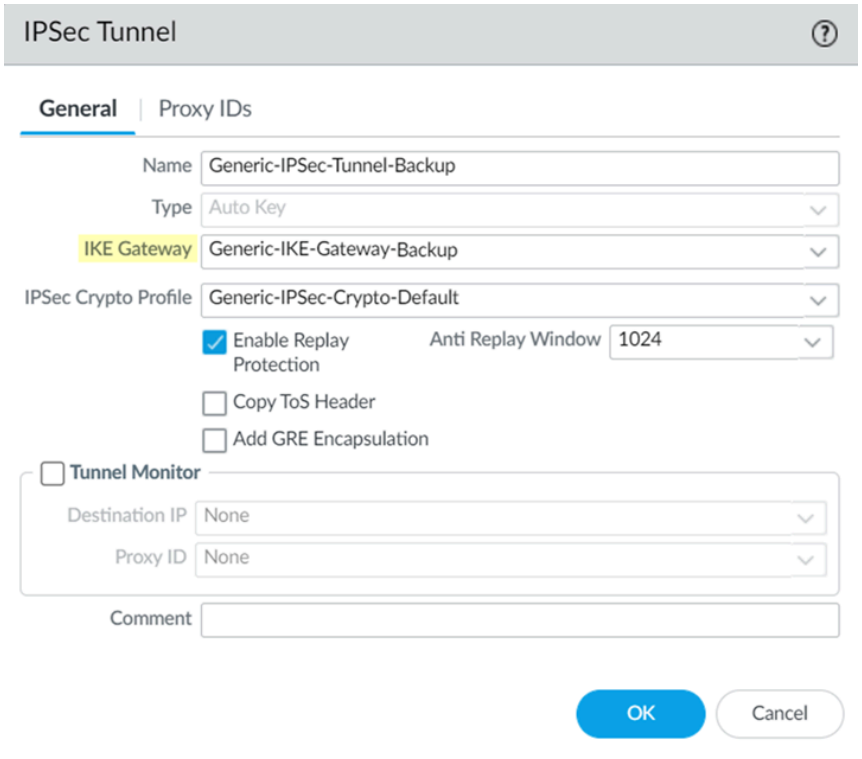
   Palo Alto Networks 建議您對 IPSec 通道使用 GCM 密碼，而不是 CBC 密碼。

   如果您是裝載 Prisma SD-WAN，請選取 **Enable Passive Mode**（啟用被動模式）。

 ©2025 Palo Alto Networks, Inc.

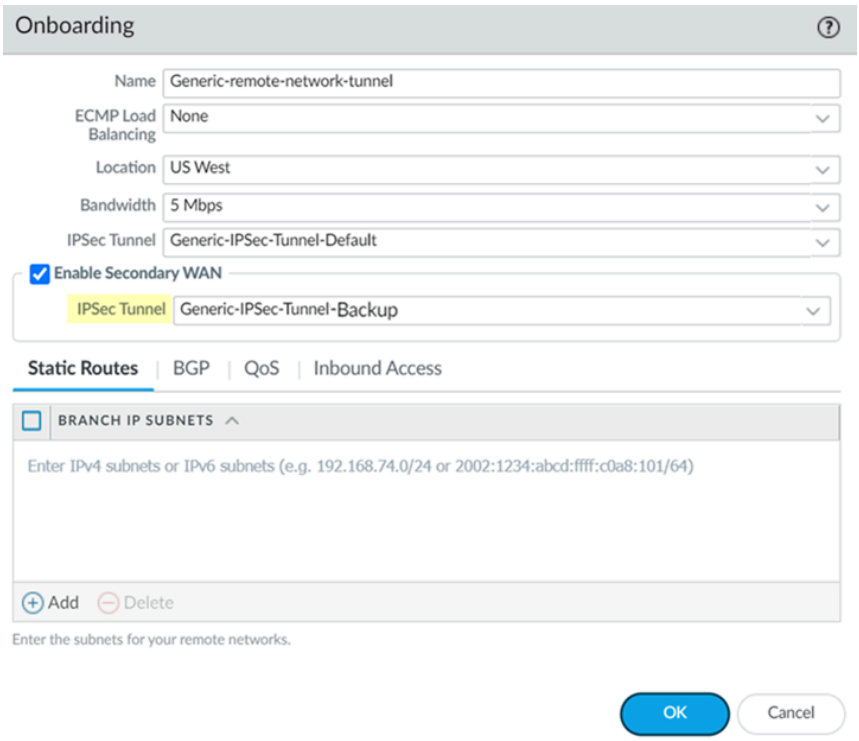



3. 建立一個新的 IPSec 通道，同時指定您建立的新 IKE 通道，但從預設範本中複製所有其他設定。




4. 當您裝載服務連線或遠端網路連線時，請 **Enable Secondary WAN**（啟用次要 **WAN**），並指定您為備份 WAN 建立的通道。


©2025 Palo Alto Networks, Inc.




**STEP 7 |** 完成服務連線或遠端網路連線的設定，方法是在用來終止 IPSec 通道另一端的裝置上，比對密碼、預先共用金鑰和對等識別碼。

**STEP 8 |** （選用）如果您需要裝載多個使用相同類型網路裝置的遠端網路連線，請 **Export**（匯出）遠端網路的設定、編輯設定，然後 **Import**（匯入）該設定。

## 常見 SD-WAN 裝置支援的 IKE 和 IPSec 密碼設定檔

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

本節為您提供許多常見 SD-WAN 裝置所支援的密碼設定檔。如果您是設定 SD-WAN 裝置，請使用這些設定檔作為您可以在 Prisma Access 為遠端網路做何配置的指導方針。

- Aruba SD-WAN 支援 IKE 和 IPSec 密碼設定檔
- Aryaka SD-WAN 支援 IKE 和 IPSec 密碼設定檔
- Citrix SD-WAN 支援 IKE 和 IPSec 密碼設定檔
- Prisma SD-WAN 裝置支援 IKE 和 IPSec 密碼設定檔
- Nuage Networks SD-WAN 支援 IKE 和 IPSec 密碼設定檔
- Riverbed SteelConnect SD-WAN 支援 IKE 和 IPSec 密碼設定檔


©2025 Palo Alto Networks, Inc.

- Silver Peak SD-WAN 支援 IKE 和 IPSec 密碼設定檔
- Viptela SD-WAN 支援 IKE 和 IPSec 密碼設定檔


©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

# Prisma Access 服務連線

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

服務連線也稱為企業存取節點 (CAN)，允許行動使用者和遠端網路上的使用者存取私人應用程式和資源，並可讓您的行動使用者和遠端網路相互通訊。

除了服務連線之外，Palo Alto Networks 還為您提供可以用來存取私人應用程式的其他服務：

- ZTNA 連接器—零信任網路存取 (ZTNA) 連接器可讓您簡單且安全地將 Prisma Access 連線到您組織的私人應用程式。ZTNA 連接器使用自動安全通道，讓行動使用者和分支位置的使用者可以存取您的私人應用程式。您也可以使用雲端識別引擎，自動探索 ZTNA 保護的私人應用程式。
- Prisma Access Colo-Connect—Colo-Connect 允許您使用 Prisma Access 保護私人應用程式，方法是使用可提供高頻寬服務連線的雲端互連。

Palo Alto Networks 建議一律在您的 Prisma Access 部署中建立服務連線。所有服務連線都具有以下特性：

- 服務連線允許存取總部或資料中心的資源。

  例如，如果您的安全性政策要求使用內部部署驗證服務（例如 Active Directory）進行使用者驗證，則您需要啟用 Prisma Access 存取服務所在的公司位置（並設定服務可以用來存取它的服務帳戶）。同樣，如果您有遠端網路和行動使用者需要存取的公司資源，則必須啟用 Prisma Access 存取相應的企業網路。

  如果您由於此原因建立服務連線，則應在實作服務連線之前對其做好規劃。
- 服務連線允許遠端網路和行動使用者相互通訊。

  即使您不需要存取總部或資料中心，也可能需要允許行動使用者存取您的遠端網路位置。在此情況下，您可以使用預留位置值建立服務連線。這是必要的，因為儘管所有遠端網路連線都是完全網狀的，但行動使用者會使用軸輻網路中的服務連線來連線到遠端網路。因此，如果您的現有服務連線不在理想的地理位置，您也可以使用預留位置建立服務連線。
- 服務連線不支援語言本地化，因為不支援透過服務連線輸出到網際網路。Prisma Access 僅指派每個服務連線一個服務 IP 位址，且該 IP 位址在地理上註冊到與您在裝載期間所指定位置相對應的計算位置。

您收到的服務連線數目取決於您的 Prisma Access 授權。

- 如果您有 ZTNA 或企業授權，則服務連線數目取決於您的授權版本。如果您有本機版本，則最多可以設定兩個服務連線；如果您有全球版本，則最多可以設定五個服務連線。
  - ZTNA 連接器可讓您將 Prisma Access 連線到您組織的私人應用程式。ZTNA 連接器使用自動安全通道，讓行動使用者和分支位置的使用者可以存取您的私人應用程式。如需詳細資訊，請參閱 Prisma Access ZTNA 連接器。
- 如果您管理多個租用戶，並具有 ZTNA 或企業授權，則每個租用戶的服務連線數目取決於您為每個租用戶配置的單位數目，以及您具有的授權類型。
  - 如果您具有全域授權，並為一個租用戶配置至少 1,000 個單位，則可以為該租用戶配置最多五個服務連線。
  - 如果您具有全域授權，並為一個租用戶指派 200 到 999 個單元，則可以為該租用戶配置最多兩個服務連線（與本機部署的連線數目相同）。
  - 如果您具有本機授權，則可以為每個租用戶配置最多兩個服務連線，無論您配置的單元數目是否超過下限，即 200 個。

  對於全域和本機授權，如果需要更多授權，您可以為服務連線購買額外的授權。對於進階部署中的服務連線，請參閱 Prisma Access 服務連線進階部署。

在開始設定您的服務連線之前，請檢閱您首先需要收集哪些資訊。


©2025 Palo Alto Networks, Inc.

# 規劃服務連線

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

建立服務連線以允許 Prisma Access 執行以下工作：

- 允許存取總部或資料中心的資源。

  如果您有遠端網路和行動使用者需要存取的公司資源，則必須啟用 Prisma Access 存取相應的企業網路。
- 允許遠端網路和行動使用者彼此通訊。

  即使不需要您的 Prisma Access 使用者連線到總部或資料中心，您可能仍需要允許行動使用者存取您的遠端網路網站。此使用案例需要服務連線，因為雖然所有遠端網路網站都已完全互連，但行動使用者基礎結構卻不是。只需最低限度設定服務連線，即可建立行動使用者存取分支網路所需的軸輻網路。

  若要提高網路效率，請將放置服務連線的位置靠近遠端網路或行動使用者最常存取的網路。

## 收集此總部或資料中心資訊

在開始設定服務連線之前，請為您想要 Prisma Access 能夠連線至的每個總部或資料中心收集以下資訊。

如果您僅建立服務連線，以允許行動使用者存取遠端網路位置，則無需收集此資訊。

對於 **Prisma Access (Managed by Strata Cloud Manager)** 和 **Prisma Access (Managed by Panorama)** 服務連線：

- ❑ 公司網站上支援 IPSec 的防火牆、路由器或 SD-WAN 裝置連線。
- ❑ 用於終止主要 VPN 通道的 IPSec 設定，此通道從 Prisma Access 到公司網路上支援 IPSec 的裝置。
- ❑ 用於終止次要 VPN 通道的 IPSec 設定，此通道從 Prisma Access 到公司網路上支援 IPSec 的裝置。

  如果您有包含 IPSec 通道、通道監控和 IPSec 密碼設定檔設定的現有範本，則可以將該範本新增至範本堆疊，以簡化建立 IPSec 通道的程序。或者，您可以編輯自動建立的 Service_Conn_Template，並建立所需的 IPSec 設定，以建立回到公司網站的 IPSec 通道。Prisma Access 還為您提供了一組預先定義的 IPSec 範本（適用於某些常用的網路裝置），以及一個通用範本（適用於預先定義範本中未包含的任何裝置）。
- ❑ 網站的 IP 子網路清單。
- ❑ Prisma Access 必須能夠解析的內部網域清單。


©2025 Palo Alto Networks, Inc.

- 您網路網站上公司存取節點的 IP 位址，Prisma Access 可以將 ICMP ping（偵測）要求傳送至其中，以進行 IPSec 通道監控。

  確保 ICMP 可從整個 Prisma Access 基礎結構子網路連線此位址。
- 服務基礎結構子網路的網路連線性設定。

  使整個服務基礎結構子網路可從總部或資料中心連線。Prisma Access 會將 IP 位址用於來自這個子網路的所有控制平面流量。

僅適用於 **Prisma Access Panorama** 服務連線：

只有在 ***Prisma Access (Managed by Panorama)*** 規劃服務連線時才需要此資訊。

- 用於驗證的服務帳戶 (如果需要存取)。
- 要與服務連線搭配使用的路由類型 (靜態或動態 (BGP))。

  為了 Prisma Access (Managed by Panorama) 可將使用者路由至他們需要的資源，您必須提供資源的路由。您可以使用下列一或多種方式執行此動作：
  - 定義您想要使用者能夠存取的每個子網路或特定資源的靜態路由。
  - 在您的服務連線位置與 Prisma Access 之間設定 BGP。
  - 使用這兩種方法的組合


©2025 Palo Alto Networks, Inc.

# 在 Prisma Access 中設定服務連線

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

建立服務連線以允許 Prisma Access 執行以下工作：

- 允許存取總部或資料中心的資源。

  如果您有遠端網路和行動使用者需要存取的公司資源，則必須啟用 Prisma Access 存取相應的企業網路。在開始設定服務連線之前，請為您想要 Prisma Access 能夠連線至的每個總部或資料中心收集以下資訊。

  - 公司網站上支援 IPSec 的防火牆、路由器或 SD-WAN 裝置連線。
  - 用於終止主要 VPN 通道的 IPSec 設定，此通道從 Prisma Access 到公司網路上支援 IPSec 的裝置。
  - 用於終止次要 VPN 通道的 IPSec 設定，此通道從 Prisma Access 到公司網路上支援 IPSec 的裝置。

    如果您有包含 IPSec 通道、通道監控和 IPSec 密碼設定檔設定的現有範本，則可以將該範本新增至範本堆疊，以簡化建立 IPSec 通道的程序。或者，您可以編輯自動建立的 Service_Conn_Template，並建立所需的 IPSec 設定，以建立回到公司網站的 IPSec 通道。


©2025 Palo Alto Networks, Inc.

Prisma Access 還為您提供了一組預先定義的 IPSec 範本（適用於某些常用的網路裝置），以及一個通用範本（適用於預先定義範本中未包含的任何裝置）。

- 網站的 IP 子網路清單。
- Prisma Access 必須能夠解析的內部網域清單。
- 您網路網站上公司存取節點的 IP 位址，Prisma Access 可以將 ICMP ping（偵測）要求傳送至其中，以進行 IPSec 通道監控。

  確保 ICMP 可從整個 Prisma Access 基礎結構子網路連線此位址。
- 服務基礎結構子網路的網路連線性設定。

  使整個服務基礎結構子網路可從總部或資料中心連線。Prisma Access 會將 IP 位址用於來自這個子網路的所有控制平面流量。
- （僅限 Prisma Access (Managed by Panorama)）用於驗證的服務帳戶（需要此帳戶才能進行存取）。
- （僅限 Prisma Access (Managed by Panorama)）要與服務連線搭配使用的路由類型（靜態或動態 (BGP)）。
- （僅限 Prisma Access (Managed by Panorama)）若要將使用者路由至他們需要的資源，您必須提供資源的路由。您可以使用下列一或多種方式執行此動作：
  - 定義您想要使用者能夠存取的每個子網路或特定資源的靜態路由。
  - 在您的服務連線位置與 Prisma Access 之間設定 BGP。
  - 使用這兩種方法的組合

- 允許遠端網路和行動使用者彼此通訊。

  即使不需要您的 Prisma Access 使用者連線到總部或資料中心，您可能仍需要允許行動使用者存取您的遠端網路網站。此使用案例需要服務連線，因為雖然所有遠端網路網站都已完全互連，但行動使用者基礎結構卻不是。只需最低限度設定服務連線，即可建立行動使用者存取分支網路所需的軸輻網路。

  若要提高網路效率，請將放置服務連線的位置靠近遠端網路或行動使用者最常存取的網路。

- Strata Cloud Manager
- Panorama

## 在 Prisma Access 中設定服務連線 (Strata Cloud Manager)

若要設定 Prisma Access (Managed by Strata Cloud Manager) 的服務連線，以允許存取私人應用程式或內部公司資源，請完成以下步驟。

**STEP 1 |** 選取 **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）。

**STEP 2 |** 給與服務連線一個描述性 **Name**（名稱）。

**STEP 3 |** 選取您總部或資料中心所在的 **Prisma Access Location**（位置）。

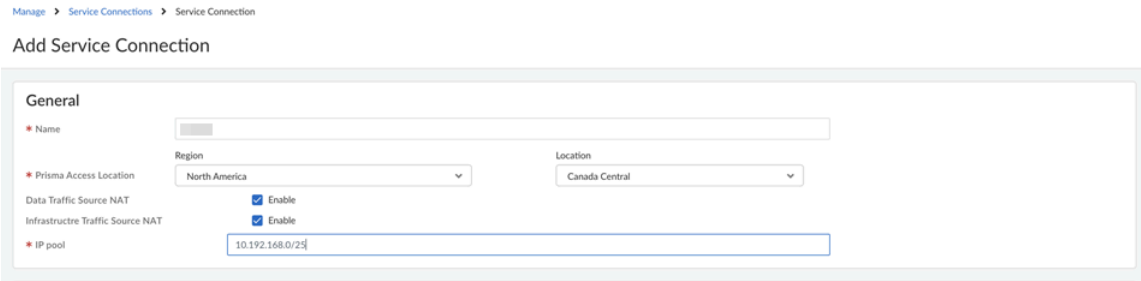

©2025 Palo Alto Networks, Inc.

**STEP 4 |** （選用）為行動使用者—GlobalProtect IP 集區位址、基礎結構子網路中的 IP 位址或兩者啟用來源 NAT。

您可以在一個或多個服務連線上指定子網路，而這些連線用來在 Prisma Access GlobalProtect 行動使用者與資料中心的私人應用程式和資源之間傳送 NAT 流量。

- 資料流量來源 **NAT**—對行動使用者 IP 位址集區位址執行 NAT，以便這些位址不會公告到資料中心，並且僅在資料中心公告和路由您在服務連線中指定的子網路。
- 基礎結構流量來源 **NAT**—對來自基礎結構子網路的位址執行 NAT，以便它們不會公告到資料中心，並且僅在資料中心公告和路由您在服務連線中指定的那些子網路。
- **User-ID**—選取後，Prisma Access 會使用此服務連線進行識別重新散佈。

  ***User-ID*** 重新散佈管理—有時，在特別大規模的 *Prisma Access* 部署中，需要對 *User-ID* 重新散佈進行精細控制。*User-ID* 重新散佈管理可讓您手動停用某些服務連線的預設識別重新散佈行為，方法是刪除 ***User ID***（使用者 ***ID***）欄中的核取標記，然後選取要用於識別重新散佈的特定服務連線。對於大多數設定，沒有必要執行此動作。請聯絡 *Palo Alto Networks* 支援以啟動此功能。
- 來源 **NAT** 集區—指定用來對行動使用者 IP 位址集區、基礎結構子網路或兩者執行 NAT 的 IP 位址集區。
  - 使用私人 IP (RFC 1918) 子網路，或可在路由網域中路由的合適子網路。
  - 確保子網路不與行動使用者—GlobalProtect IP 位址集區、基礎結構子網路或用於此租用戶的任何其他來源 NAT 位址重疊。
  - 輸入介於 /25 和 /32 之間的子網路。




**STEP 5 |** 選取 **IPSec Tunnel**（**IPSec** 通道）。如果尚未設定主要或次要 IPSec 通道，請選取 **Set Up**（設定），然後遵循以下步驟。

1. 為通道指定描述性名稱。
2. 為 IPSec 裝置和您用來與 Prisma Access 建立通道的總部或資料中心選取 **Branch Device Type**（分支裝置類型）。
3. 針對 **Branch Device IP Address**（分支裝置 **IP** 位址），選擇使用可識別通道端點的 **Static IP**（靜態 **IP**）位址或 **Dynamic**（動態）IP 位址。

   如果將 **Branch Device IP Address**（分支裝置 **IP** 位址）設定為 **Dynamic**（動態），您亦須為總部或資料中心（**IKE Local Identification**（**IKE** 本機識別））或為 Prisma

 ©2025 Palo Alto Networks, Inc.

Access（**IKE Peer Identification**（**IKE** 對等識別））新增 IKE ID，以啟用 IPSec 對等進行驗證。

由於在服務連線完全部署之前，您沒有用於 Prisma Access IKE ID（**IKE Peer Identification**（**IKE** 對等識別））的值，因此您通常想要為總部或資料中心（**IKE Local Identification**（**IKE** 本機識別））設定 IKE ID，而不是設定 Prisma Access IKE ID。

**STEP 6 |** 開啟 **Tunnel Monitoring**（通道監控）。

輸入總部或資料中心網路上的通道監控 **Destination IP**（目的地 **IP**）位址，讓 Prisma Access 用來確定通道是否已啟動，此外，如果您的分支 IPSec 裝置使用政策型，請輸入相關聯的 **Proxy ID**。

您輸入的通道監控 IP 位址將自動新增到分支子網路清單中。

**STEP 7 |** **Save**（儲存）通道設定。

**STEP 8 |** 若要新增或調整路由和 Quality of Service (服務品質 - QoS) 設定，請前往 **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）。**Set Up**（設定）或**Edit**（編輯） **Routing**（路由）或 **QoS** 設定。

**STEP 9 |** 設定靜態路由。

1. 對於將流量路由至總部或資料中心，以及從總部或資料中心路由流量的靜態路由，請 **Add**（新增）要在分支上保護的 IP 子網路或 IP 位址。

   如果您對總部或資料中心網路上的 IP 子網路進行任何變更，則必須手動更新靜態路由。

**STEP 10 |** 設定動態路由。

1. 對於公告總部或資料中心子網路的動態路由，**Enable BGP for Dynamic Routing**（啟用 **BGP** 進行動態路由）。
2. （選用）選取 **MRAI Timer**（**MRAI** 計時器）值。

   BGP 路由會提供一個計時器，您可以用來在網路中定制 BGP 路由聚合，稱為最小路由公告間隔 *(MRAI)*。MRAI 會採取行動，根據每個目的地限制更新速率，而且 BGP 路由器至少會等待設定的 MRAI 時間，然後再傳送相同首碼的公告。較小的數字為您提供更快的聚合時間，但會在您的網路中建立更多的公告。較大的數字會減少可以傳送的公告數目，但也會使路由聚合速度變慢。您可以決定在網路中放置的數字，以在更快的路由聚合和更少的公告之間取得最佳平衡。

   設定介於 1 與 600 秒之間的 MRAI 範圍，預設值為 30 秒。
3. 若要減少透過 BGP 對客戶周邊設備 (CPE) 進行的行動使用者 IP 子網路公告數目，請指定 Prisma Access，以在公告子網路之前彙總這些子網路，方法為選取 **Summarize Mobile User Routes before advertising**（在公告之前彙總行動使用者路由）。

   根據預設，Prisma Access 會在 /24 子網路區塊中公告行動使用者 IP 位址集區；如果你彙總它們，Prisma Access 根據您指定的子網路公告該集區。例如，Prisma Access 使用 /20 子網路公告 10.8.0.0/20 的公用使用者行動 IP 集區，而不是先將該集區劃分為 10.8.1.0/24、10.8.2.0/24、10.8.3.0/24 等子網路，再公告它們。彙總這些公告可以減少 CPE 路由表中儲存的路由數目。例如，您可以使用 IP 集區彙總，搭配可接受有限數目路由的雲端 VPN 閘道（虛擬私人閘道 (VGW) 或傳輸閘道 (TGW)）。

 ©2025 Palo Alto Networks, Inc.

4. （選用）若要讓 Prisma Access 使用 eBGP 為遠端網路起始預設路由公告，請選取 **Advertise Default Route**（公告預設路由）。確保您的網路沒有 BGP 公告的其他預設路由，否則可能會在您的網路中引入路由問題。
5. （選用）如果您設定了次要 WAN，並且需要變更次要（備份）BGP 對等的對等位址，請選取 **Use different BGP Peer for Secondary Tunnel**（針對次要通道使用不同的 **BGP** 對等），然後輸入唯一對等，以及選擇性地輸入次要 WAN 的本機 IP 位址。
6. 若要將來自服務連線的社群新增到來自客戶周邊設備 (CPE) 上 eBGP 對等的輸出首碼，請將 **Add no-export community**（新增無匯出社群）設定為 **Enabled Out**（已啟用輸出）。預設會 **Disabled**（停用）此功能。

   不要選取 **Enabled In**（已啟用輸入）或 **Enabled Both**（已啟用兩者），因為不支援這些選項。
7. （選用）選取 **Do Not Export Routes**（不匯出路由），防止 Prisma Access 將路由轉送到總部或資料中心。

   根據預設，Prisma Access 會公告所有 BGP 路由訊息，包括本機路由以及從其他服務連線、遠端網路和行動使用者子網路接收的所有首碼。選取此核取方塊可防止 Prisma Access 傳送任何 BGP 公告，但仍會使用其收到的 BGP 資訊，來了解其他 BGP 芳鄰的路由。

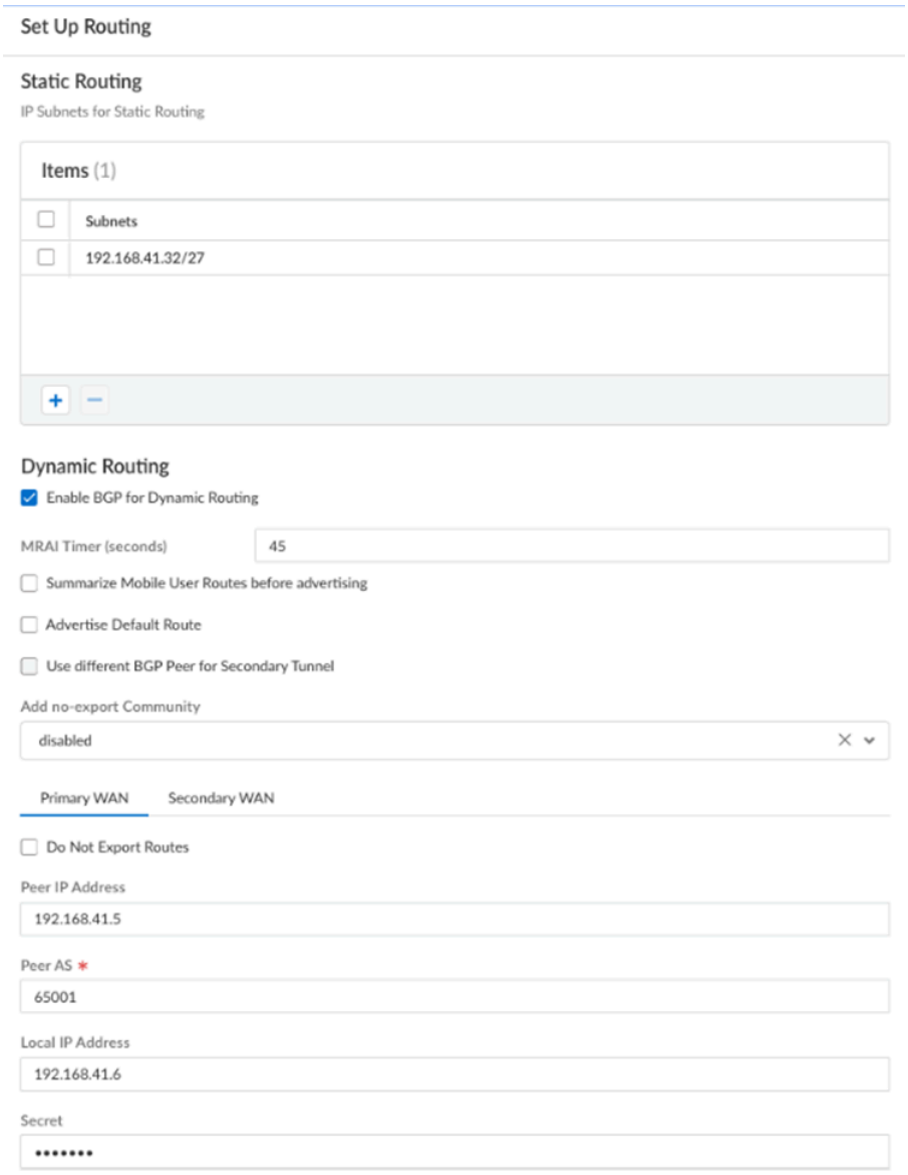
   因為 *Prisma Access* 不傳送 *BGP* 公告後，所以如果您選取此選項，則必須在您的內部部署設備上設定靜態路由，以建立回到 *Prisma Access* 的路由。
8. 輸入 **Peer IP Address**（對等 **IP** 位址），其已指派為總部或資料中心網路上 eBGP 路由器的路由器 ID。
9. 輸入 **Peer AS**（對等 **AS**），這是您網路的自發系統 (AS)。

   使用符合 RFC 6996 的 BGP 私人 AS 編號。
10. 輸入 **Local IP Address**（本機 **IP** 位址），Prisma Access 會將其用作 BGP 的本機 IP 位址。

    僅當您的總部或資料中心裝置需要本機位址，BGP 對等才能成功時，才需要此本機位址。確保您指定的位址不與遠端網路中基礎結構子網路中的 IP 位址衝突或重疊。
11. 輸入 **Secret**（密碼）密碼，驗證 BGP 對等通訊。


©2025 Palo Alto Networks, Inc.

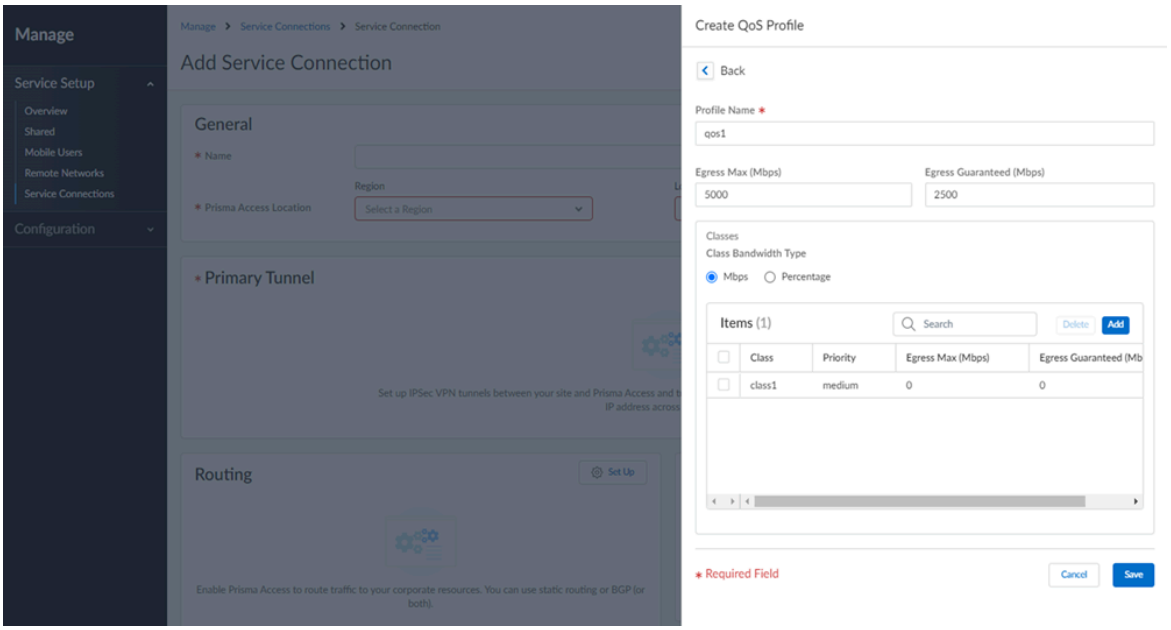
12. 選取 **Confirm Secret**（確認密碼）。




 ©2025 Palo Alto Networks, Inc.

**STEP 11 |** （選用）設定 QoS。

首先，新增 QoS 設定檔以定義 QoS 類別，這些類將形成總部或資料中心與 Prisma Access 之間的流量。然後，您將建立 QoS 政策規則，並將設定檔新增到規則，以在比對總部或資料中心流量時強制執行 QoS。




1. 輸入 **QoS Profile**（**QoS** 設定檔）的名稱。
2. 選取 **Create New**（新建）。
3. 將離開總部或資料中心服務連接的流量輸送量上限（以 Mbps 為單位）設定為 **Egress Max**（輸出上限）。

   您可以指定一值，最高可為總部或資料中心的授權頻寬上限。
4. 將保證頻寬設定為 **Egress Guaranteed**（輸出保證）（以 Mbps 為單位）。

   任何超過輸出保證值的流量是最佳效果，但不加以保證。任何保證但未使用的頻寬仍可供所有流量使用。
5. 定義每個 QoS **Class**（類別），並將其附加到政策規則。

   QoS 類別會針對符合 QoS 政策規則的流量確定其優先順序和頻寬。單一 QoS 設定檔中最多有 8 個可定義的 QoS 類別。除非另有設定，不符合 QoS 類別的流量會被指派至類別 4。
6. 設定 QoS 類別的 **Priority**（優先順序）。

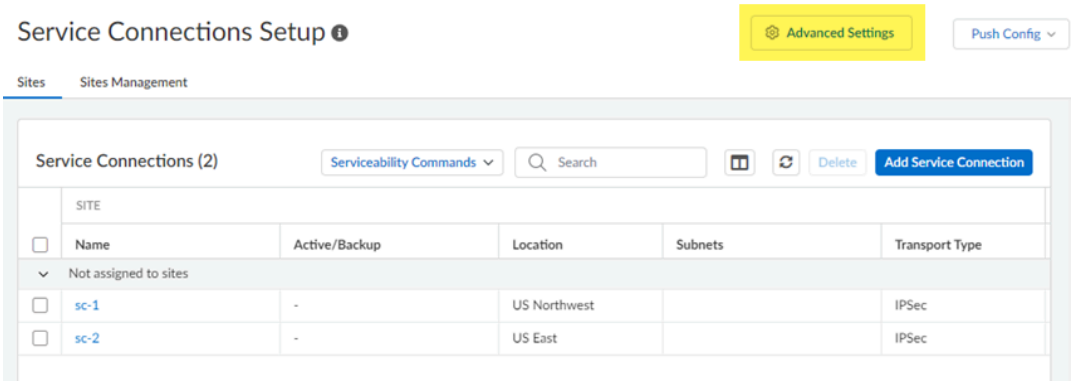
   優先順序包括即時、高、中或低。
7. 設定 **Egress Max**（輸出上限）值。

   一個 QoS 類別的輸出上限值或多個 QoS 類別的合併輸出上限值不得超過 QoS 設定檔的輸出上限。
8. 設定 **Egress Guaranteed**（輸出保證）值。

   指派給 QoS 類別的保證頻寬不是為該類別保留的；未使用的頻寬仍可供所有流量使用。任何超過輸出保證值的類別流量是最佳效果，但不加以保證。


©2025 Palo Alto Networks, Inc.

**STEP 12 |** 為您的服務連線設定 **Advanced Settings**（進階設定）。




1. 指定要與服務連線搭配使用的 **BGP Routing Preferences**（**BGP** 路由偏好設定）。

   您可以指定網路偏好設定，以使用您組織的網路或 Prisma Access 網路來處理服務連線流量。

   - **Default**（預設值）—Prisma Access 在其內部網路中使用預設路由。
   - **Hot potato routing**（熱馬鈴薯路由）—Prisma Access 儘快將服務連線流量移交給您組織的 WAN。

   變更 *Prisma Access* 服務連線路由方法需要全面瞭解您組織的拓撲和路由裝置，以及瞭解 *Prisma Access* 路由的運作方式。從預設值變更路由方法之前，我們建議您仔細閱讀 服務連線流量的路由。
2. **Withdraw Static Routes if Service Connection or Remote Network IPSec tunnel is down**（如果服務連線或遠端網路 **IPSec** 通道關閉，則撤回靜態路由）如果您想要 Prisma Access 在通道沒有備份通道的情況下關閉時移除靜態路由。

   Prisma Access 會在以下情況移除路由：

   - 主要通道關閉，沒有次要通道。
   - 如果設定了主要通道和次要通道，但兩者都關閉。

   如果未啟用通道監控，則無法套用此變更。
3. 設定 **Backbone Routing**（骨幹路由）用於服務連線。

   根據預設，Prisma Access 骨幹要求您對透過服務連線從資料中心或總部位置返回的流量具有對稱網路路徑。如果想要將 ECMP 或另一個負載平衡機制用於來自 CPE 的服務連線，您可以透過 Prisma Access 骨幹啟用對稱流量。

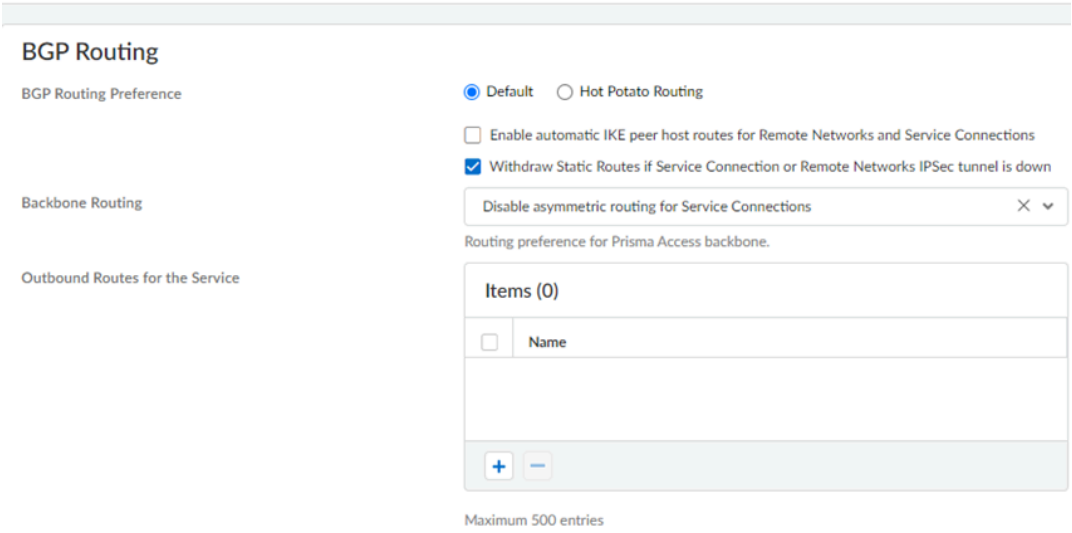
   - 選取 **Disable asymmetric routing for Service Connections**（停用服務連線的非對稱路由，要求跨服務連線骨幹的對稱流量。
   - 選取 **Allow asymmetric routing for Service Connections**（允許服務連線的非對稱路由），以允許 Prisma Access 跨服務連線骨幹使用非對稱流量。
   - 如果您與某個位置有多個服務連線，則可以在 Prisma Access 中利用負載平衡，方法是選取 **Allow asymmetric routing and load sharing across Service Connections**（允許


©2025 Palo Alto Networks, Inc.

跨服務連線進行非對稱路由和負載共用）（預設設定）。不過，負載平衡是基於最佳效果完成的，如果其中一個服務連接中斷，負載平衡將失敗。

當您選取 **Allow asymmetric routing and load sharing across Service Connections**（允許跨服務連線進行非對稱路由和負載共用）時，Prisma Access 會在 GlobalProtect 入口網站和閘道與服務連線之間啟用網路備援。此功能會在行動使用者資料資料平面與不同計算位置中服務連線之間提供備援網路路徑。啟用備援可讓使用者更靈活地存取資料中心或總部位置中服務連線後面的資源。因為行動使用者需要服務連線，才能從遠端網路存取資源，所以使用者在存取遠端網路位置中的資源時也具有更大的彈性。

4. （選用）指定 **Outbound Routes for the Service**（服務的輸出路由），方法為新增最多 500 個首碼，而 Prisma Access 會在所有服務連線和遠端網路連線上為這些首碼新增靜態路由。Prisma Access 接著透過網際網路將流量路由至這些首碼。




## 更多 IKE 選項

根據您選取的 IPSec 裝置類型，Prisma Access 會為 HQ/DC 裝置與 Prisma Access 之間的 IKE 階段 1 金鑰交換過程，提供一組建議的密碼和金鑰存留時間：您可以使用建議的設置，或根據您的環境需求自訂設定。

為您的 IPSec 裝置和 Prisma Access 選取用於 IKE 交涉的 **IKE Protocol Version**（**IKE** 通訊協定版本）。

如果您選取 **IKEv1 Only Mode**（僅 **IKEv1** 模式），Prisma Access 只能使用 IKEv1 通訊協定進行交涉。如果您選取 **IKEv2 Only Mode**（僅 **IKEv2** 模式），Prisma Access 只能使用 IKEv2 通訊協定進行交涉。如果您選取 **IKEv2 Preferred Mode**（**IKEv2** 慣用模式），僅當 IPSec 裝置也支援 IKEv2 時，Prisma Access 才會使用 IKEv2 通訊協定。如果您的 IPSec 裝置不支援 IKEv2，則 Prisma Access 將回復為使用 IKEv1 通訊協定。


©2025 Palo Alto Networks, Inc.

新增 **IKEv1 Crypto Profile**（**IKEv1** 密碼設定檔）以自訂 IKE 密碼設定，這些設定會定義 IKE 階段 1 中金鑰交換過程使用的加密和驗證演算法。

Prisma Access 會根據用於建立此通道的 **Branch Device Type**（分支裝置類型），自動使用預設 IKE 密碼設定檔。

- **Encryption**（加密）—指定 IKE SA 交涉中使用的加密演算法。

  Prisma Access 支援以下加密演算法：3des（168 位元）、aes-128-cbc（128 位元）、aes-192-cbc（192 位元）、aes-256-cbc（256 位元）和 DES（56 位元）。您也可以選取 null（無加密）。
- **Authentication**（驗證）—指定 IKE SA 交涉中使用的驗證演算法。

  Prisma Access 支援以下驗證演算法：sha1（160 位元）、sha256（256 位元）、sha384（384 位元）、sha512（512 位元）和 md5（128 位元）。您也可以選取 null（無驗證）。
- **DH** 群組—指定用於在 IKE SA 交涉中為 IKE 產生對稱金鑰的 Diffie-Hellman (DH) 群組。Diffie-Hellman 演算法使用一方的私密金鑰及另一方的公開金鑰來建立共用金鑰，亦即由 VPN 通道對等雙方共用的加密金鑰。

  Prisma Access 支援以下 DH 群組：群組 1（768 位元）、群組 2（1,024 位元—預設值）、群組 5（1,536 位元）、群組 14（2,048 位元）、群組 19（256 位元橢圓曲線群組）、群組 20（384 位元橢圓曲線群組）。若要獲得最強的安全性，請選取數字最高的群組。
- 存留時間—指定 IKE 階段 1 金鑰有效時間的單位和時間量（預設值為 8 小時）。對於 IKEv1，security association（安全性關聯 - SA）不會在金鑰存留時間到期前主動重設其金鑰。IKEv1 階段 1 的重設金鑰作業僅會在 SA 到期時觸發。對於 IKEv2，SA 必須在金鑰存留時間到期之前重設金鑰。如果 SA 未在到期時重設金鑰，則 SA 必須開始新的階段 1 金鑰。
- **IKEv2 Authentication Multiple**（**IKEv2** 驗證倍數）—指定與金鑰存留時間相乘的值，用於決定驗證計數（範圍為 0-50；預設值為 0）。驗證計數是安全性處理節點可以執行 IKEv2 IKE SA 金鑰重設的次數，此次數後則必須從頭開始重新驗證 IKEv2。預設值為 0，會停用重新驗證功能。

啟用 **IKE Passive Mode**（**IKE** 被動模式），讓 Prisma Access 僅回應 IKE 連線而啟動這些連線。

**IKE NAT Traversal**（**IKE NAT** 周遊）會預設為開啟。

這表示 IKE 和 UDP 通訊協定上會使用 UDP 封裝，以便通過 IPSec VPN 通道端點之間的 network address translation（網路位址轉譯 - NAT）裝置。

## 更多 IPSec 選項

根據您選取的 IPSec 裝置類型，Prisma Access 會提供一組建議的 IPSec 通訊協定和金鑰存留時間設定，在 security association (安全性關聯 - SA) 的 IKE 階段 2 中，於 IPSec 裝置與 Prisma Access 之間保護 IPSec 通道內的資料。您可以使用建議的設置，或根據您的環境需求自訂設定。


©2025 Palo Alto Networks, Inc.

自訂 **IPSec Crypto Profile**（**IPSec** 密碼設定檔），以定義如何在自動金鑰 IKE 為 IKE 階段 2 期間內的 IKE SA 自動產生金鑰時保護通道內的資料。

Prisma Access 會根據 **Branch Device Type**（分支裝置類型）廠商自動設定預設的 IPSec 密碼設定檔。您可以使用預設設定檔或建立自訂設定檔。

- **IPSec Protocol**（**IPSec** 通訊協定）—保護通過 VPN 通道的資料。封裝安全有效承載 **(ESP)** 通訊協定會將資料加密、驗證來源，及驗證資料完整性。驗證標頭 **(AH)** 通訊協定會驗證來源並驗證資料完整性。

  如果使用 **ESP** 作為 IPSec 通訊協定，還需指定 IPSec SA 交涉中使用的 **Encryption**（加密）演算法。

  Prisma Access 支援以下加密演算法：aes-256-gcm（256 位元）、aes-256-cbc（256 位元）、aes-192-cbc（192 位元）、aes-128-gcm（128 位元）、aes-128 -cbc（128 位元）、3des（168 位元）和 DES（56 位元）。您也可以選取 null（無加密）。

**Authentication**（驗證）—指定 IPSec SA 交涉中使用的驗證演算法。

Prisma Access 支援以下驗證演算法：sha1（160 位元）、sha256（256 位元）、sha384（384 位元）、sha512（512 位元）和 md5（128 位元）。如果將 IPSec 通訊協定為 ESP，您也可以選取 [none（無）]（無驗證）。

**DH Group**（**DH** 群組）—在 IPSec security association（安全性關聯 - SA）交涉中指定 IKE 的 Diffie-Hellman (DH) 群組。

Prisma Access 支援以下 DH 群組：群組 1（768 位元）、群組 2（1,024 位元—預設值）、群組 5（1,536 位元）、群組 14（2,048 位元）、群組 19（256 位元橢圓曲線群組）、群組 20（384 位元橢圓曲線群組）。若要獲得最強的安全性，請選取數字最高的群組。如果您不想更新 Prisma Access 在 IKE 階段 1 建立的金鑰，請選取 **no-pfs**（無完美轉送密碼）。如果您選取此選項，Prisma Access 會重複使用目前用於 IPSec SA 交涉的金鑰。

**Lifetime**（存留時間）—指定交涉金鑰有效時間的單位和時間量（預設值為 1 小時）。

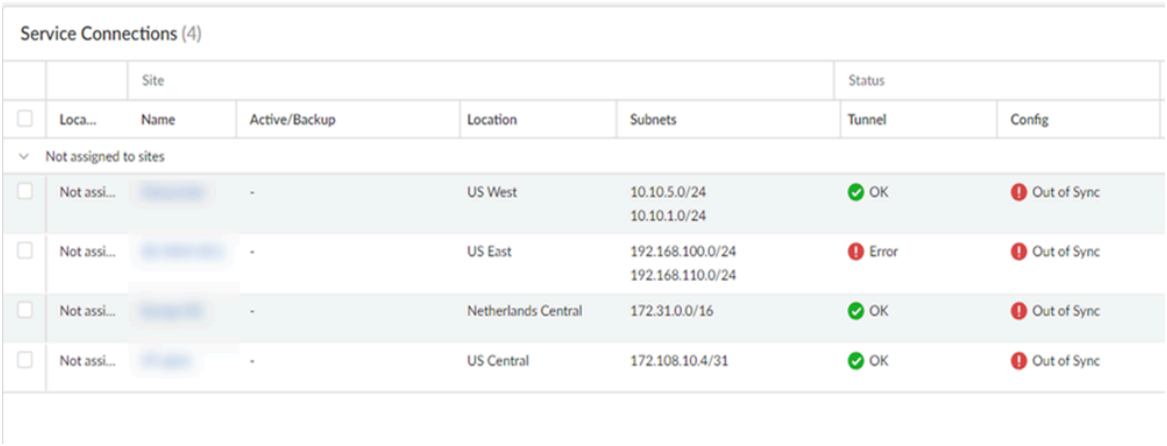
**Lifesize**（存留大小）—指定金鑰可用於加密的資料單位和數量。

## 驗證服務連線狀態

若要驗證服務連線是否已成功設定，請選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Service Connections**（服務連線），然後檢查 **Status**（狀態）是否為 **OK**（成功）。

如果狀態不是 **OK**（成功），請將游標暫留在狀態圖示上，以檢視任何錯誤。


©2025 Palo Alto Networks, Inc.




**Sites**（網站）區域允許您檢視所有已裝載的服務連接，以及其狀態和有關它們的其他詳細資訊。

站台

- **Name**（名稱）—服務連線的名稱。
- **Active/Backup**（作用中/備份）—服務連線的作用中位置和備份位置。
- **Subnets**（子網路）—服務連線的已指派基礎結構子網路。

**STATUS (狀態)**

- **Tunnel**（通道）—Prisma Access 與服務連線之間連線的操作狀態。
- **Config**（設定）—上次推送設定至服務的狀態。如果本機設定和雲端中的設定相符，則設定狀態為 **In sync**（同步）。如果您已在本機進行了變更，但尚未將設定推送到雲端，這可能會顯示狀態 **Out of sync**（不同步）。將游標暫留在狀態指示器上，以取得更多的詳細資訊。在提交並推送設定到 Prisma Access 之後，設定狀態會變更為 **In sync**（同步）。

**Prisma Access**

- **Location**（位置）—服務連線的部署位置。
- **Service IP**（服務 **IP**）—服務連線的 IP 位址。
- **EBGP Router**（**EBGP** 路由器）—服務連線中 EBGP 路由器的 IP 位址。

連結

- **BGP IPv4**—服務連線中 BGP IPv4 路由的狀態。
- **BGP IPv6**—服務連線中 BGP IPv6 路由的狀態。
- **IPSec Tunnel**（**IPSec** 通道）—服務連線的 IPSec 通道。您建立的第一個 IPSec 通道將是 **(Primary)**（（主要））通道。如果您建立了第二個 IPSec 通道，它將是 **(Secondary)**（（次要））通道。
- **Peer IP Address**（對等 **IP** 位址）—服務連線的閘道 IP 位址。

## 在 Prisma Access 中設定服務連線 (Panorama)

若要設定 Prisma Access Panorama 的服務連線，以允許存取私人應用程式或內部公司資源，請完成下列步驟。


©2025 Palo Alto Networks, Inc.

請勿使用 *CLI* 裝載和設定服務連線。如果您需要使用 *CLI* 來裝載服務連線，請聯繫您的 *Palo Alto Networks* 團隊。

**STEP 1 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Connection**（服務連線）。

**STEP 2 |** 將新的服務連線 **Add**（新增）至您的其中一個公司網路網站。

**STEP 3 |** 指定公司網站的 **Name**（名稱）。

**STEP 4 |** 選取最靠近網站所在的 **Location**（位置）。

請參閱本節以取得 Prisma Access 位置清單。

以兩個星號表示的位置為 **Local Zones**（本機區域）。這些位置會將計算、儲存、資料庫和基礎結構服務放置在大型人口和產業中心附近；不過，它們也有一些限制。若要新增本機區域，請聯繫您的 Palo Alto Networks 代表。

**STEP 5 |** 選取或新增新的 **IPSec Tunnel**（**IPSec** 通道）設定，以存取公司位置上的防火牆、路由器或 SD-WAN 裝置：

- 如果您使用現有的 **IPSec Tunnel**（**IPsec** 通道）設定，請從下拉式清單中選取該設定。請注意，您為每個服務連線建立的通道會將 Prisma Access 連線到每個公司位置上支援 IPSec 的

 ©2025 Palo Alto Networks, Inc.

裝置。IKE 閘道設定中的對等位址對於每個通道而言必須是唯一的。但是，您可以重複使用其他一些常見設定元素，例如密碼設定檔。

您選取的 IPSec 通道必須僅使用自動金鑰交換和 IPv4。此外，請確保 IPSec 通道、IKE 閘道和密碼設定檔名稱不超過 31 個字元。

- 若要建立新的 IPsec 通道設定：

  按一下 **New IPSec Tunnel**（新增 **IPSec** 通道）、為其提供 **Name**（名稱），並設定 IKE 閘道、IPSec 密碼設定檔和通道監控設定。

- 如果您總部或資料中心位置上支援 IPsec 的裝置使用政策型 VPN：

  在 **Proxy IDs**（**Proxy ID**）頁籤上 **Add**（新增）與本機 IPSec 裝置上設定相符的 Proxy ID，以確保 Prisma Access 可以成功與您的本機裝置建立 IPSec 通道。

- 若要偵測並抵禦回覆攻擊：

  離開 **Enable Replay Protection**（啟用重播保護）。

- 若要保留原始 ToS 資訊：

  選取 **Copy TOS Header**（複製 **TOS** 標頭），將 Type of Service（服務類型 - ToS）標頭從封裝封包的內部 IP 標頭複製到外部 IP 標頭。

- 若要為服務連線啟用通道監控：

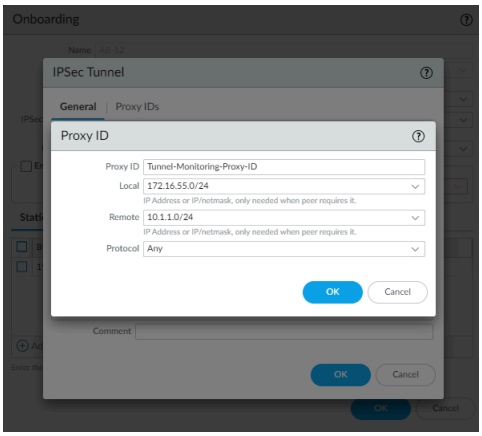
  選取 **Tunnel Monitor**（通道監控）：

  - 請輸入 **Destination IP**（目的地 **IP**）位址。

    在您的總部或資料中心站台上指定 IP 位址，讓Prisma Access 可以向該位址傳送 ICMP ping（偵測）要求以進行 IPSec 通道監控。確保 ICMP 可從整個 Prisma Access 基礎結構子網路存取此位址。

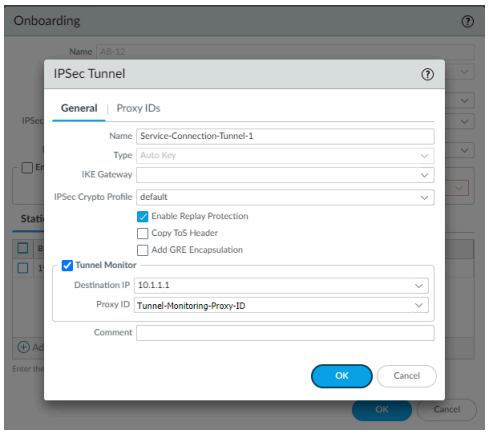
  - 如果您對使用多個 Proxy ID 的對等裝置使用通道監控，請指定一個 **Proxy ID** 或新增 **New Proxy ID**（新的 **Proxy ID**），以允許從基礎結構子網路存取您的總部或資料中心站台。

    下圖顯示 Proxy ID，其中以服務基礎結構子網路（本範例中為 172.16.55.0/24）作為 **Local**（本機）IP 子網路，以總部或資料中心的子網路（本範例中為 10.1.1.0/24）作為 **Remote**（遠端）子網路。




 ©2025 Palo Alto Networks, Inc.

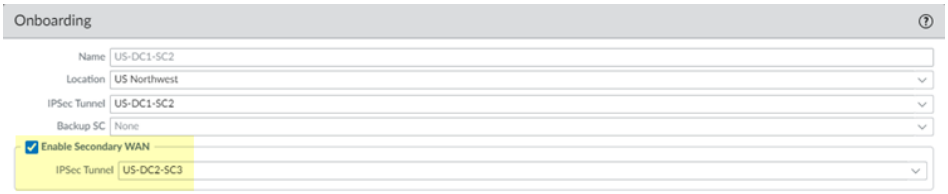
下圖顯示透過在 **Proxy ID** 欄位中指定 Proxy ID 來將您建立的 Proxy ID 套用至通道監控設定。




您必須在 *CPE* 上設定通往通道監控 *IP* 位址的靜態路由，通道監控才能發揮作用。若要針對從資料中心或總部網路到 *Prisma Access* 的通道監控，尋找要使用的目的地 *IP* 位址，請選取 ***Panorama*** > ***Cloud Services***（雲端服務）> ***Status***（狀態）> ***Network Details***（網路詳細資料）、按一下 ***Service Infrastructure***（服務基礎結構），然後尋找 ***Tunnel Monitor IP Address***（通道監控 ***IP*** 位址）。

**STEP 6 |** 僅限 BGP 和熱馬鈴薯 (hot potato) 路由部署—選取服務連線以用來作為偏好備份 **(Backup SC**（備份 **SC**）)。

您可以選取已新增的任何服務連線。Prisma Access 會使用您選取的 **Backup SC**（備份 **SC**）作為連線失敗時的偏好服務連線。選擇備份服務連線可以防止非對稱路由問題（如果您啟用兩個以上的服務連線）。此選擇僅適用於熱馬鈴薯路由模式。




 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** 如果您在此位置有次要 WAN 連結，請選取 **Enable Secondary WAN**（啟用次要 **WAN**），然後選取或設定 **IPSec Tunnel**（**IPSec** 通道），設定方法與設定主要 IPSec 通道相同。

如果主要 WAN 連結發生故障，Prisma Access 會偵測到中斷並透過次要 WAN 連結建立通往總部或資料中心位置的通道。如果主要 WAN 連結變成作用中的狀態，連結將會切換回主要連結。

以下部署不支援設定次要 WAN：

- 如果您的次要 WAN 與主要 IPSec 通道設定為主動/主動模式。
- 如果您的用戶端裝置 (CPE) 在具有主要和次要 IPSec 通道的等價多路徑 (ECMP) 設定中設定。

如果您使用靜態路由，通道容錯移轉時間會小於 15 秒（從偵測到的時間算起），具體取決於您的 WAN 供應商。

如果設定 BGP 路由並啟用通道監控，則確定安全性參數索引 (SPI) 失敗的最短預設保留時間是通道監控，當連續 15 秒偵測到通道故障時，通道監控會刪除通往對等方的所有路由。這樣一來，通道監控就可以決定 BGP 路由的行為。如果如果未設定通道監控，保留計時器會決定刪除路由之前通道關閉的時間。Prisma Access 會使用 RFC 4271 定義的預設 BGP HoldTime 值：90 秒，這是 Prisma Access 刪除非作用 SPI 的路由之前的最長等待時間。。如果對等 BGP 裝置設定的保留時間較短，則 BGP 保留計時器會使用較小的值。

當次要通道安裝成功後，次要路由會優先採用，直到主要通道恢復正常為止。若主要和次要通道皆正常運作，則優先採用主要路由。

如果您使用不同的 *BGP* 對等來作為次要（備份）連線，*Prisma Access* 不會遵守 *CPE* 公告的多出口鑑別器 *(MED)* 屬性。如果您在遠端網路連線或服務連線上使用多個 *BGP* 對等，則此警告適用。


©2025 Palo Alto Networks, Inc.

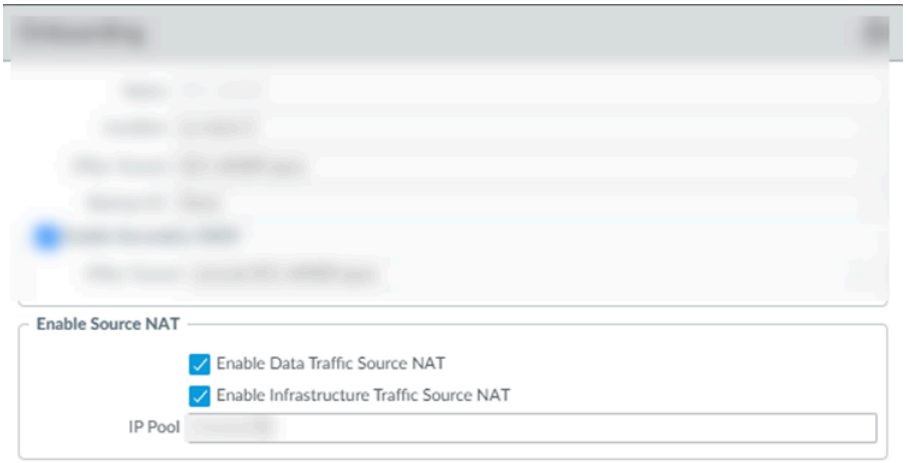
**STEP 8 |** （選用）為行動使用者—GlobalProtect IP 集區位址、基礎結構子網路中的 IP 位址或兩者啟用來源 NAT。

您可以在一個或多個服務連線上指定子網路，而這些連線用來在 Prisma Access GlobalProtect 行動使用者與資料中心的私人應用程式和資源之間傳送 NAT 流量。

- 啟用資料流量來源 **NAT**—對行動使用者 IP 位址集區位址執行 NAT，以便這些位址不會公告到資料中心，並且僅在資料中心公告和路由您在服務連線中指定的子網路。
- 啟用基礎結構流量來源 **NAT**—對來自基礎結構子網路的位址執行 NAT，以便它們不會公告到資料中心，並且僅在資料中心公告和路由您在服務連線中指定的那些子網路。
- **User-ID**—選取後，Prisma Access 會使用此服務連線進行識別重新散佈。

  ***User-ID*** 重新散佈管理—有時，在特別大規模的 *Prisma Access* 部署中，需要對 *User-ID* 重新散佈進行精細控制。*User-ID* 重新散佈管理可讓您手動停用某些服務連線的預設識別重新散佈行為，方法是刪除 ***User ID***（使用者 ***ID***）欄中的核取標記，然後選取要用於識別重新散佈的特定服務連線。對於大多數設定，沒有必要執行此動作。請聯絡 *Palo Alto Networks* 支援以啟動此功能。
- **IP** 集區—指定用來對行動使用者 IP 位址集區、基礎結構子網路或兩者執行 NAT 的 IP 位址集區。

  使用私人 IP (RFC 1918) 子網路，或可在路由網域中路由的適合子網路，且不與行動使用者—GlobalProtect IP 位址集區或基礎架構子網路重疊。輸入介於 /25 和 /32 之間的子網路。



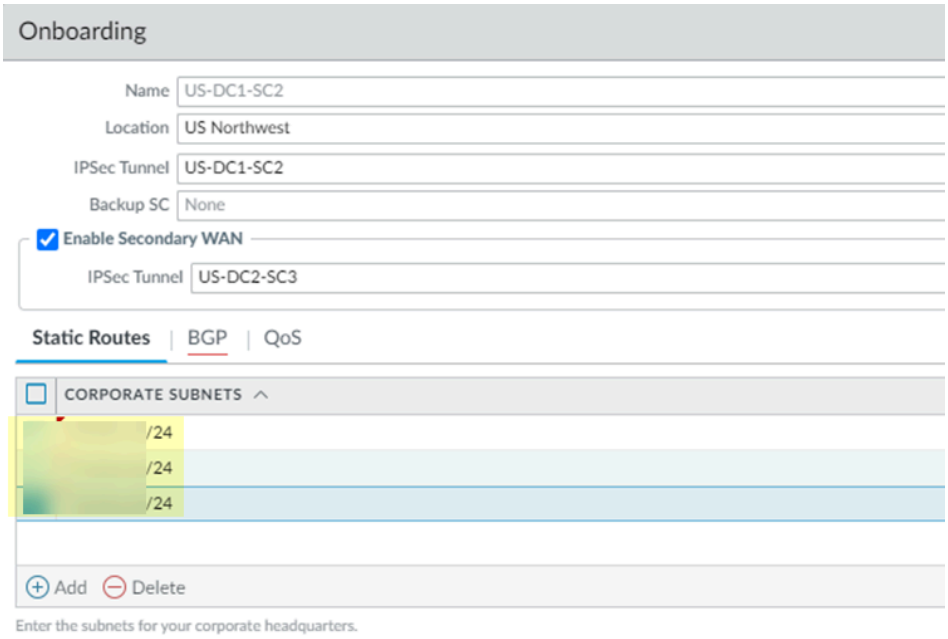

 ©2025 Palo Alto Networks, Inc.

**STEP 9 |** 啟用路由到公司網站上您使用者將需要存取的子網路或個別 IP 位址。

Prisma Access 會使用此資訊將要求路由到適當的網站。每個網站的網路不能彼此重疊，也不能與您為服務基礎結構或為使用者 IP 集區的 Prisma Access 指定的 IP 位址集區重疊。您可以設定 **Static Routes**（靜態路由）、**BGP** 或兩者的組合。

若要設定 **Static Routes**（靜態路由）：

1. 在 **Static Routes**（靜態路由）頁籤上，按一下 **Add**（新增）並輸入遠端使用者將需要存取的資源子網路位址（例如 172.168.10.0/24）或個別 IP 位址，例如 DNS 伺服器（例如，10.32.5.1/32）。
2. 針對 Prisma Access 在此位置需要存取的所有子網路或 IP 位址重複此動作。




若要設定 **BGP**：

1. 在 **BGP** 頁籤上，選取 **Enable**（啟用）。

   當您啟用 BGP 時，Prisma Access 會將外部 BGP (eBGP) 的 time-to-live (存留時間 - TTL) 值設定為 8，以容納 Prisma Access 基礎結構與終止 eBGP 連線的客戶周邊設備 (CPE) 之間可能發生的任何額外躍點。

   *Prisma Access* 不接受服務連線或遠端網路連線的 *BGP* 預設路由公告。

2. （選用）從下列選項中選取：

   - 若要將公司存取節點（服務連線）的 **no-export**（無匯出）社群新增到來自客戶周邊設備 (CPE) 上 eBGP 對等的輸出首碼，請將 **Add no-export community**（新增無匯出社群）設定為 **Enabled Out**（已啟用輸出）。此功能預設為 **Disabled**（已停用）。

     請勿在熱馬鈴薯路由模式下使用此功能。


©2025 Palo Alto Networks, Inc.

- 防止 Prisma Access BGP 對等將路由轉送至您組織的網路。**Don't Advertise Prisma Access Routes**（請勿公告 **Prisma Access** 路由）。

  根據預設，Prisma Access 會公告所有 BGP 路由訊息，包括本機路由以及從其他服務連線、遠端網路和行動使用者子網路接收的所有首碼。選取此核取方塊以防止 Prisma Access 傳送任何 BGP 公告，但仍會使用其收到的 BGP 資訊來瞭解其他 BGP 芳鄰中的路由。

  由於如果您選取此選項，不會傳送 *BGP* 公告，因此您必須在內部部署設備上設定靜態路由，才能建立回到 *Prisma Access* 的路由。*Prisma Access*

- 若要減少透過 BGP 公告至客戶周邊設備 (CPE) 的行動使用者 IP 子網路公告數目，請指定 Prisma Access 以在公告子網路之前彙總這些子網路，方法為選取 **Summarize Mobile User Routes before advertising**（公告前彙總行動使用者路由）。

  根據預設，Prisma Access 會在 /24 子網路區塊中公告行動使用者 IP 位址集區；如果您彙總它們，Prisma Access 會根據您指定的子網路公告集區。例如，Prisma Access 使用 /20 子網路公告 10.8.0.0/20 的公用使用者行動 IP 集區，而不是先將該集區劃分為 10.8.1.0/24、10.8.2.0/24、10.8.3.0/24 等子網路，再公告它們。彙總這些公告可以減少 CPE 路由表中儲存的路由數目。例如，您可以使用 IP 集區彙總，搭配可接受有限數目路由的雲端 VPN 閘道（虛擬私人閘道 (VGW) 或傳輸閘道 (TGW)）。

  如果您已啟用熱馬鈴薯路由並啟用路由彙總，則 *Prisma Access* 不再將 *AS-PATHs* 加至前面，這可能會導致非對稱路由。在使用熱馬鈴薯路由來啟用路由彙總之前，請確保從資料中心或總部位置傳回的流量已保證對稱傳回。

3. （選用）選取 **MRAI Timer**（**MRAI** 計時器）值。

   BGP 路由會提供一個計時器，您可以用來在網路中定制 BGP 路由聚合，稱為最小路由公告間隔 *(MRAI)*。MRAI 會採取行動，根據每個目的地限制更新速率，而且 BGP 路由器至少會等待設定的 MRAI 時間，然後再傳送相同首碼的公告。較小的數字為您提供更快的聚合時間，但會在您的網路中建立更多的公告。較大的數字會減少可以傳送的公告數目，但也會使路由

 ©2025 Palo Alto Networks, Inc.

聚合速度變慢。您可以決定在網路中放置的數字，以在更快的路由聚合和更少的公告之間取得最佳平衡。

設定介於 1 與 600 秒之間的 MRAI 範圍，預設值為 30 秒。

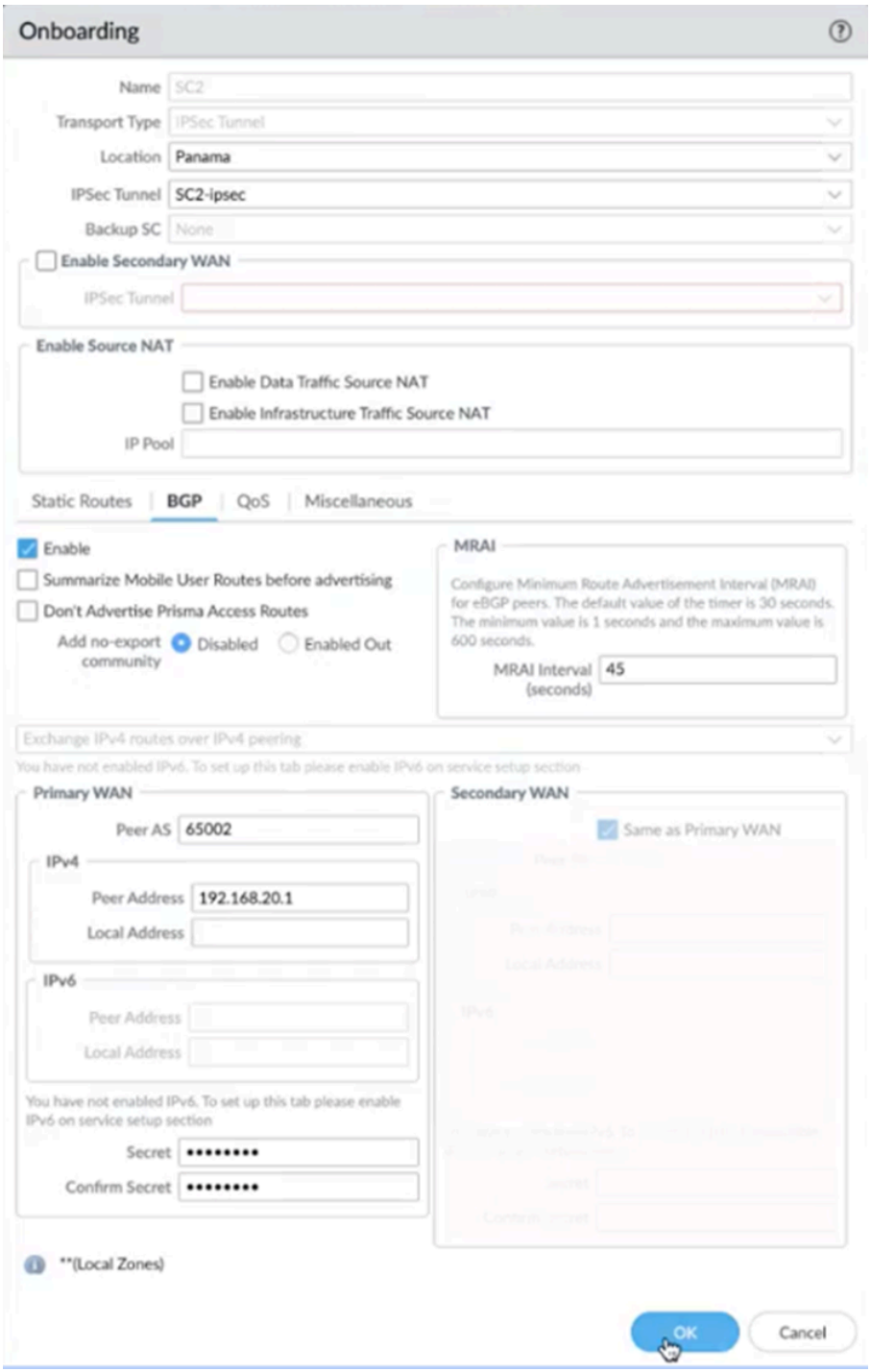
4. 輸入指派為 eBGP 路由器的路由器 ID 的 IP 位址，而此路由器位於您要為其將此連線設定為 **Peer Address**（對等位址）的資料中心/總部網路上。
5. 輸入 **Peer AS**（對等 **AS**），這是遠資料中心/總部網路上防火牆虛擬路由器或 BGP 路由器所屬的自發系統 (AS)。
6. （選用）為 BGP 輸入一個位址，Prisma Access 會使用此位址作為其本機 IP 位址。

   指定 **Local Address**（本機位址）很有用，其中連線另一端的裝置（例如 Amazon Web Service (AWS) 虛擬私人閘道）需要特定的本機 IP 位址，才能使 BGP 對等成功。確定您指定的位址不與基礎結構子網路中的 IP 位址或服務連線中的子網路衝突或重疊。

   您必須在 *CPE* 上設定 *BGP* ***Local Address***（本機位址）的靜態路由。

   如果您使用 IPV6 支援進行服務連線，則可以設定 **IPv6** 位址，以及 **IPv4** 位址。您還需要在 Prisma Access 基礎結構中全域啟用 IPv6 網路，然後才能使用 IPv6 定址。
7. （選用）輸入並確認 **Secret**（密碼）複雜密碼以驗證 BGP 對等通訊。


©2025 Palo Alto Networks, Inc.




**STEP 10 |** （選用）如果您設定了 **Secondary WAN**（次要 **WAN**），並且需要變更次要（備份）BGP 對等的 **Peer Address**（對等位址）或 **Local Address**（本機位址），請取消選取 **Same as**

 ©2025 Palo Alto Networks, Inc.

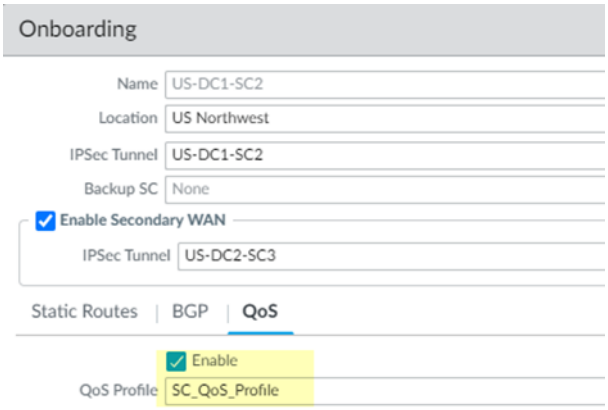
**Primary WAN**（與主要 **WAN** 相同），然後輸入唯一對等，以及選擇性地輸入次要 WAN 的本機 IP 位址。

在某些部署中（例如，使用 BGP 與 AWS VPN 閘道對等時），主要和次要 WAN 的 BGP 對等可能不同。在這些情況下，您可以選擇為次要 WAN 設定不同的 BGP 對等。

對於搭配次要 *WAN* 的 *BGP* 部署，*Prisma Access* 會同時設定處於 ***UP***（啟動）狀態的主要和次要通道，但遵循網路流量的正常 *BGP* 作用中-備份行為。*Prisma Access* 會將主要通道設定為作用中，並僅透過該通道傳送和接收流量；如果主要通道故障，*Prisma Access* 會使用 *BGP* 規則偵測故障、將次要通道設定為作用中，並僅使用次要通道傳送和接收流量。

**STEP 11 |** （選用）為服務連線啟用 **Quality of Service**（服務品質），並指定 QoS 設定檔或新增 **New QoS Profile**（新的 **QoS** 設定檔）。

您可以建立 QoS 設定檔來形成遠端網路和服務連線的 QoS 流量，並將這些設定檔套用至您使用 PAN-OS 安全性政策標記的流量、使用內部部署裝置標記的流量，或 Pan-OS 標記和內部部署標記的流量。如需詳細資料，請參閱 遠端網路的 QoS。

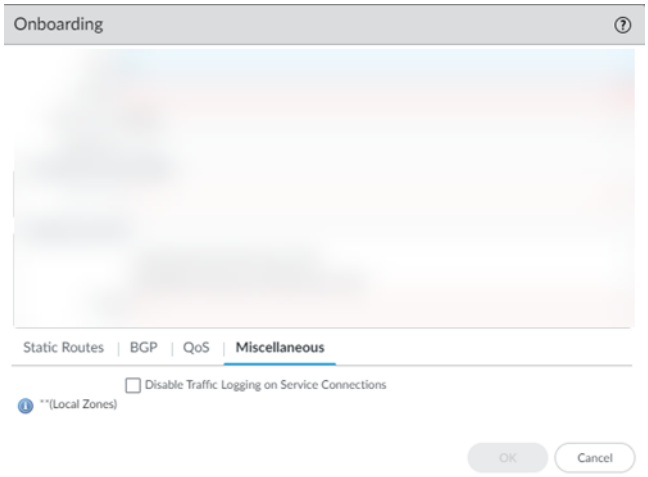



 ©2025 Palo Alto Networks, Inc.

**STEP 12 |** （選用）設定 **Miscellaneous**（雜項）設定。

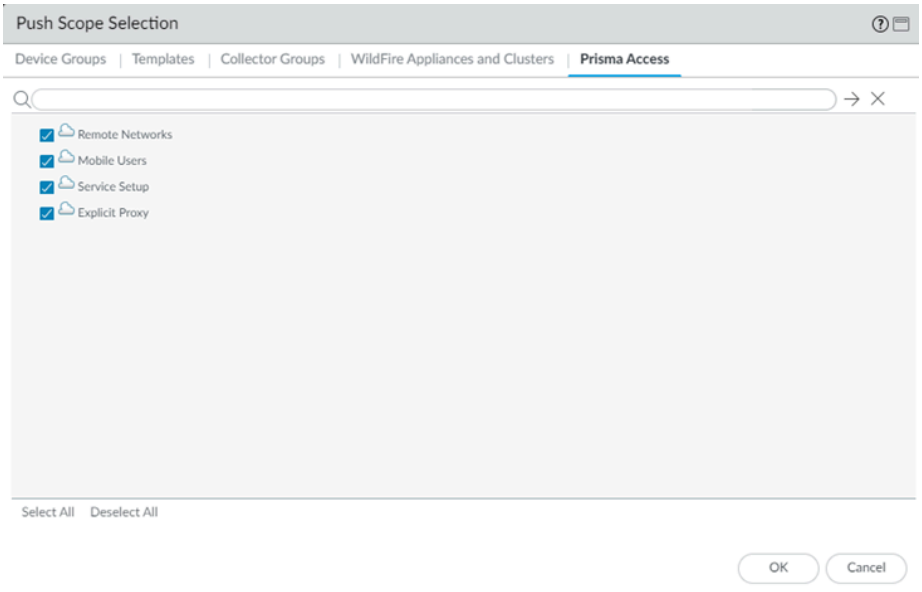
1. （選用）**Disable Traffic Logging on Service Connections**（停用服務連線上的流量記錄），以停用在用於 Prisma Access 部署的服務連線上進行記錄。

   如果服務連線記錄的大多數流量是非對稱的，則可能需要停用服務連線記錄，以減少 Strata Logging Service 記錄儲存空間的耗用。如果您的部署沒有透過服務連線的非對稱流量，則無需停用記錄。




**STEP 13 |** 將您的變更提交到 Panorama，並將設定變更推送到 Prisma Access。

1. 按一下 **Commit**（提交） > **Commit and Push**（提交並推送）。
2. **Edit Selections**（編輯選取項目），並在 **Prisma Access** 頁籤中，確保在 **Push Scope**（推送範圍）中選取了 **Service Setup**（服務設定），然後按一下 **OK**（確定）。




3. 按一下 **Commit and Push**（提交並推送）。

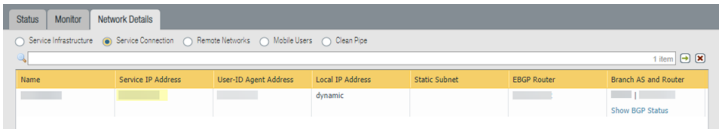
**STEP 14 |** 透過重複步驟 2 到步驟 11 來新增更多服務連線。


©2025 Palo Alto Networks, Inc.

**STEP 15 |** 將來自公司網路上支援 IPsec 的裝置的 IPSec 通道設定回 Prisma Access。

1. 若要確定 Prisma Access 內通道的 IP 位址，請選取 **Panorama > Cloud Services**（雲端服務） **> Status**（狀態） **> Network Details**（網路詳細資訊）、按一下 **Service Connection**（服務連線）選項按鈕，然後記下網站的 **Service IP Address**（服務 **IP** 位址）。

   **Service IP Address**（服務 **IP** 位址）是從支援 IPsec 的裝置建立通道返回服務連線時，您需要連線到的公開位址。



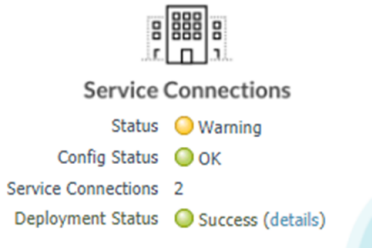

2. 在公司位置中支援 IPsec 的裝置上，設定 IPsec 通道，其會連線至 Prisma Access 內的 **Service IP Address**（服務 **IP** 位址），並在該裝置上提交變更，以便可以建立通道。

## 驗證服務連線狀態

若要驗證服務連線是否已成功設定，請選取 **Panorama > Cloud Services**（雲端服務） **> Status**（狀態） **> Status**（狀態），然後檢查狀態是否為 **OK**（成功）。

如果您已建立一個具有預留位置值的服務連線，以啟用行動使用者與遠端網路使用者之間的通訊，則無需驗證服務連線狀態。

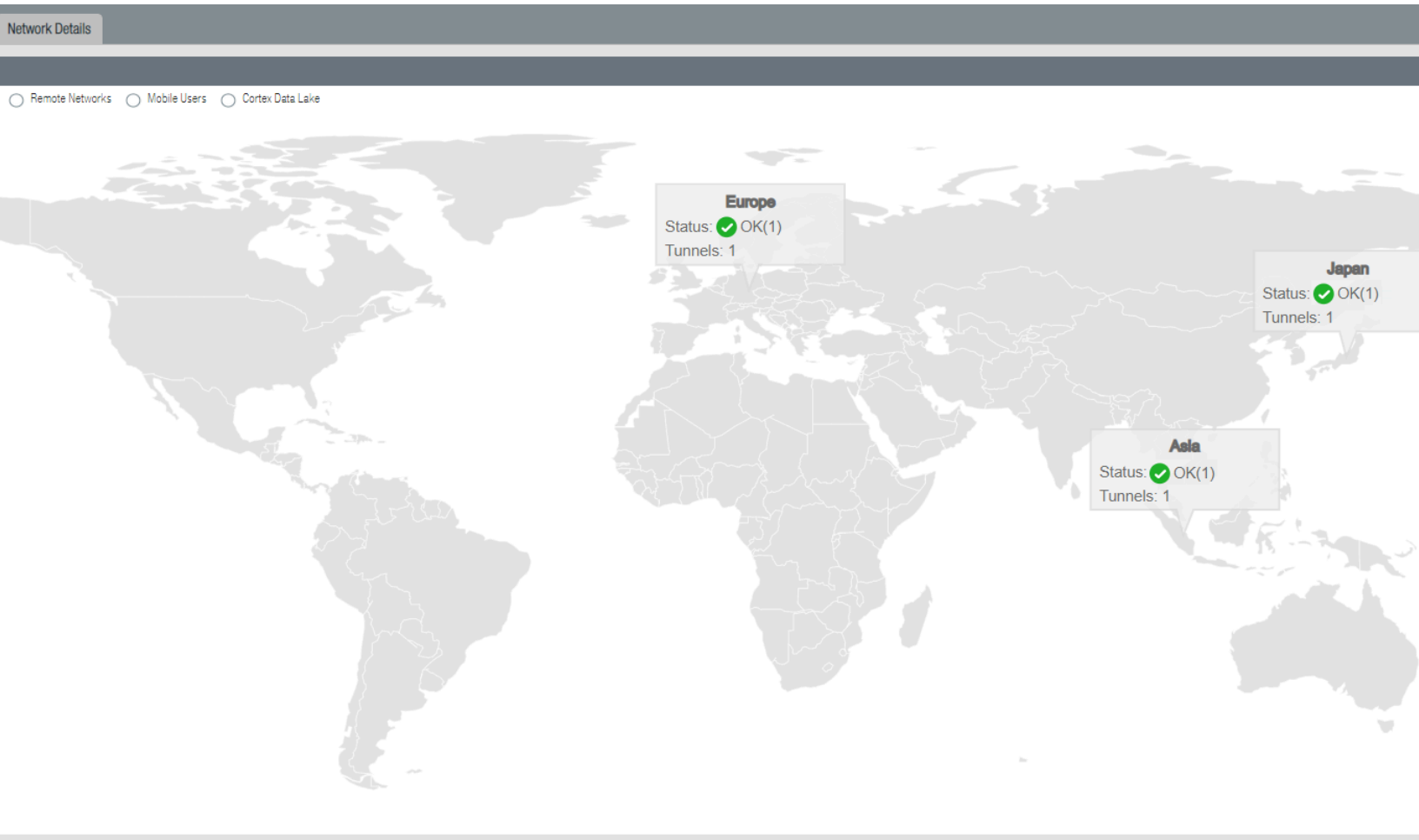
**Deployment Status**（部署狀態）區域允許您在完成裝載和部署工作之前檢視其進度，以及查看有關已完成工作狀態的詳細資訊。



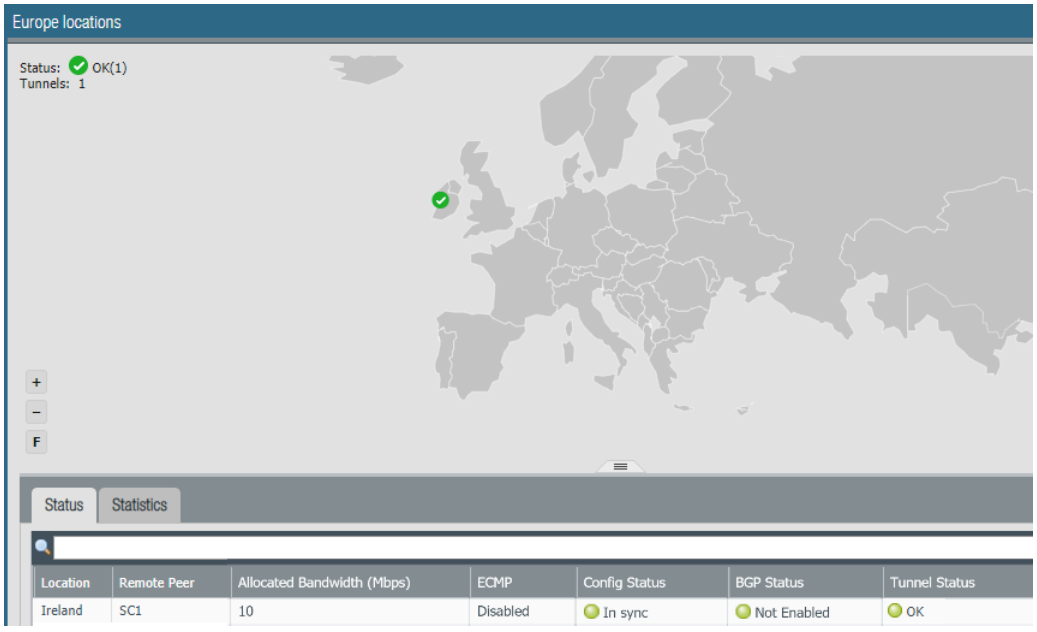

如果狀態不是 **OK**（成功），請將游標暫留在狀態圖示上，以檢視任何錯誤。

若要查看服務連線的圖形表示法，以及狀態詳細資訊，請選取 **Monitor**（監控）頁籤上的 **Service Connection**（服務連線）。

 ©2025 Palo Alto Networks, Inc.




選取一個區域，以取得更多有關該區域的詳細資訊。




按一下地圖下方的頁籤，以查看有關服務連線的其他資訊。


©2025 Palo Alto Networks, Inc.

**Status**（狀態）頁籤：

- **Location**（位置）—服務連線的部署位置。
- **Remote Peer**（遠端對等）—此服務基礎結構設定 IPsec 通道的公司位置。
- **Allocated Bandwidth**（已配置頻寬）—您已配置的服務連線數目乘以 300 Mbps。

  此數目並不會反映可用的服務連線頻寬。

  雖然每個服務連線提供大約 *1 Gbps* 的輸送量，但實際的輸送量取決於幾個因素，包括：

  - 流量混合（例如，框架大小）
  - 服務連線與總部位置或資料中心之間的延遲和封包丟失
  - 服務提供者效能限制
  - 客戶終端裝置效能限制
  - 其他客戶資料中心流量
- **ECMP**—如果您為此服務連線設定了相等成本的多重路徑 (ECMP)。由於 ECMP 不是用於服務連線，因此這個狀態為 **Disabled**（已停用）。
- **Config Status**（設定狀態）—上次推送設定到服務的狀態。如果本機設定和雲端中的設定相符，則設定狀態為 **In sync**（同步）。如果您已在本機進行了變更，但尚未將設定推送到雲端，這可能會顯示狀態 **Out of sync**（不同步）。將游標暫留在狀態指示器上，以取得更多的詳細資訊。在提交並推送設定到 Prisma Access 之後，設定狀態會變更為 **In sync**（同步）。
- **BGP Status**（**BGP** 狀態）—顯示有關公司/總部位置的防火牆或路由器與服務連線建立所在的 Prisma Access 之間的 BGP 狀態的相關資訊。雖然您可能會通過各種 BGP 狀態（**idle**（閒置）、**active**（作用中）、**open send**（開啟傳送）、**open pend**（開啟擱置）、**open confirm**（開啟確認））暫時看到狀態，但 BGP 狀態最常顯示：
  - **Connect**（連線）—資料中心/總部的路由器正在嘗試與 Prisma Access 建立 BGP 對等關係。
  - **Established**（已建立）—已建立 BGP 對等關係。

  此欄位還將顯示 BGP 連線是否處於錯誤狀態：
  - **Warning**（警告）—超過 8 分鐘未更新 BGP 狀態。這可能表示防火牆中斷。
  - **Error**（錯誤）—BGP 狀態未知。
- **Tunnel Status**（通道狀態）—Prisma Access 與服務連線之間連線的操作狀態。

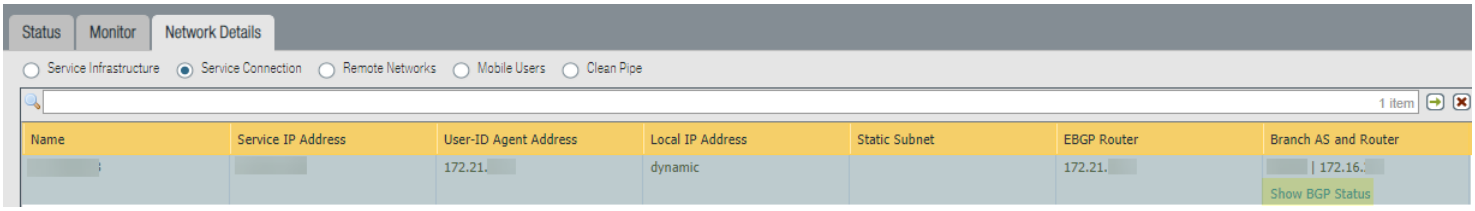
**Statistics**（統計資料）頁籤：

- **Location**（位置）—服務連線的部署位置。
- **Remote Peer**（遠端對等）—服務連線設定 IPsec 通道的公司位置。
- **Ingress Bandwidth (Mbps)**（進入頻寬 **(Mbps)**）—從總部/資料中心位置到 Prisma Access 的頻寬。
- **Ingress Peak Bandwidth (Mbps)**（進入峰值頻寬 **(Mbps)**）—從總部/資料中心位置進入雲端服務的峰值負載。

 ©2025 Palo Alto Networks, Inc.

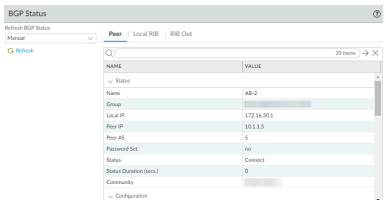
- **Egress Bandwidth (Mbps)**（輸出頻寬 **(Mbps)**）—從 Prisma Access 進入總部/資料中心位置的頻寬。
- **Egress Peak Bandwidth (Mbps)**（輸出峰值頻寬 **(Mbps)**）—從 Prisma Access 進入總部/資料中心位置的峰值負載。
- **QoS**—選取此按鈕以顯示圖形圖表，其中顯示即時和歷史 QoS 統計資料，包括每個類別丟棄的封包數目。此圖表僅為已啟用 QoS 的服務連線或遠端網路連線顯示。

如果您設定了 BGP，則可以選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Service Connection**（服務連線） > **Show BGP Status**（顯示 **BGP** 狀態）來檢查其狀態。




[BGP Status（BGP 狀態）] 對話方塊隨即顯示。此表格為您提供下列資訊：

- 對等—BGP 對等的路由資訊，包括狀態、路由總數、設定，以及執行階段統計資料和計數器。路由總數會顯示在 **bgpAfiIpv4-unicast Counters**（**bgpAfiIpv4-unicast** 計數器）區域的 **Incoming Total**（傳入總數）和 **Outgoing Total**（傳出總數）欄位中。




- 本機 **RIB**—Prisma Access 在本機使用的 BGP 路由。Prisma Access 會從 BGP RIB-In 表格（其中儲存了鄰近網路裝置傳送的資訊）中選取此資訊、套用本機 BGP 匯入政策和路由決策，並將本機 RIB 資訊儲存在路由資訊庫 (RIB) 中。

  請注意，只會顯示前 256 個項目。若要檢視其他項目，請在 [Filter（篩選器）] 欄位中輸入子網路或 IP 位址，然後按一下 [Apply Filter（套用篩選器）]，檢視最多 256 個路由項目的子集。




- **RIB** 輸出—Prisma Access 透過 BGP 更新訊息公告至其對等的路由資訊。

 ©2025 Palo Alto Networks, Inc.

# 使用服務連線啟用行動使用者與遠端網路之間的存取

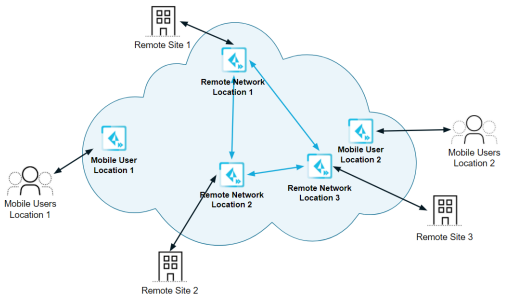
| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權，包括用於站台對站台和使用者對站台存取的網路互連 |

若要設定服務連線以連線行動使用者和遠端網路，請使用以下值 **Add**（新增）一個服務連線：

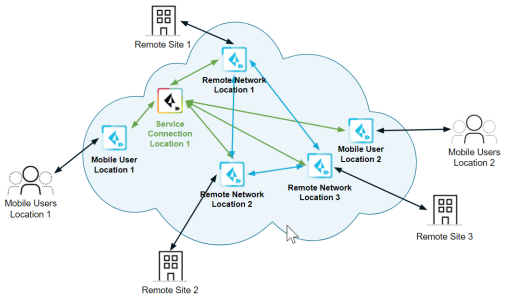
- 指定靠近您行動使用者的 **Region**（區域）。
- 使用預留位置值 **Add**（新增）一個 **IPSec Tunnel**（**IPsec** 通道）和 **IKE Gateway**（**IKE** 閘道）。
- 新增預留位置 **Corporate Subnets**（企業子網路）。

  由於 Prisma Access 不會透過此通道路由任何流量，因此不與其他所設定子網路衝突或重疊的任何值都是有效的。

以下範例顯示一個 Prisma Access 部署，其中行動使用者位於不同的地理區域和遠端網路中。遠端網路連線是在 Prisma Access 基礎結構的網狀網路中連線的，但行動使用者無法連線到遠端網路。此外，若沒有服務連線，不同地理區域中的行動使用者將無法彼此連線。

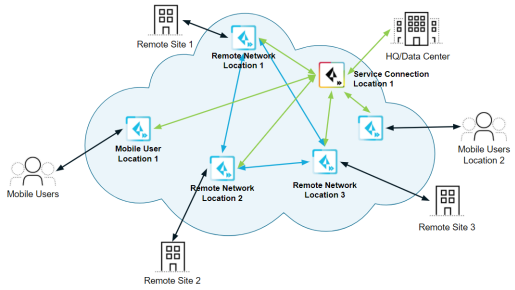



在您新增服務連線之後，該服務連線會連線軸輻網路中的行動使用者和遠端網路。

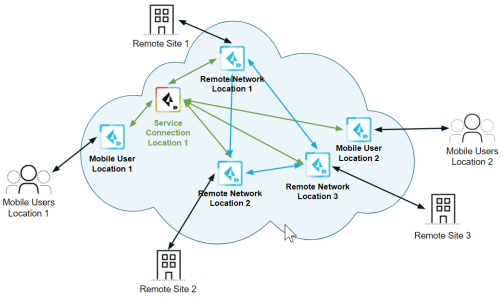



這種類型的服務連線有用的另一種情況是，當服務連線遠離行動使用者時。下圖顯示此網路部署的範例。

 ©2025 Palo Alto Networks, Inc.




新增更靠近行動使用者的第二個服務連線可在行動使用者與遠端網路之間建立更有效率的網路。




 ©2025 Palo Alto Networks, Inc.

# 服務連線的動態路由考量

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

## 運作方式—路由服務連線流量

Prisma Access 會使用 BGP 進行動態路由，並使用 BGP 路徑選擇將路由安裝至路由表。當 Prisma Access 使用服務連線，將流量路由至您的到總部或資料中心時，它會使用有效引導該流量的路由方法。Prisma Access 會使用旨在適應大多數網路部署的預設路由模型；不過，並非所有組織的網路都是相同的。為了適應更廣泛的部署， Prisma Access 允許您為服務連線路由選擇另一種模式。以下幾節描述了 Prisma Access 使用的 BGP 路由方法，以及變更服務連線路由的 Prisma Access 預設方法之前，您需要在組織網路中考量的因素。

變更 *Prisma Access* 服務連線路由方法需要徹底瞭解組織的拓撲和路由裝置，以及瞭解 *Prisma Access* 路由的運作方式，如本節所述。我們建議您在變更預設設定的路由方法之前，請仔細閱讀本節。

Prisma Access 支援靜態路由和使用 BGP 的動態路由，進行服務和遠端網路連線；本節假設您使用 BGP 路由，進行 Prisma Access 部署。當您選取 BGP 路由時，您組織的網路會從 Prisma Access 得知 BGP 資訊。

### 服務連線的路由模式

您可以透過 Prisma Access 從以下路由模式中進行選擇：

- 預設路由#這是 Prisma Access 使用的目前路由模型。

  如果您想要 Prisma Access 使用 BGP 最佳路徑選擇機制，而不調整任何 BGP 屬性，請使用此路由模式。在此模式下，Prisma Access 將遵守用戶端周邊設備 (CPE) 公告的任何屬性。
- 熱馬鈴薯路由—Prisma Access 會儘快地將流量傳遞至您組織的網路。

  如果您想要組織的網路執行大部分路由決策，請使用此路由方法。

## Prisma Access 預設路由

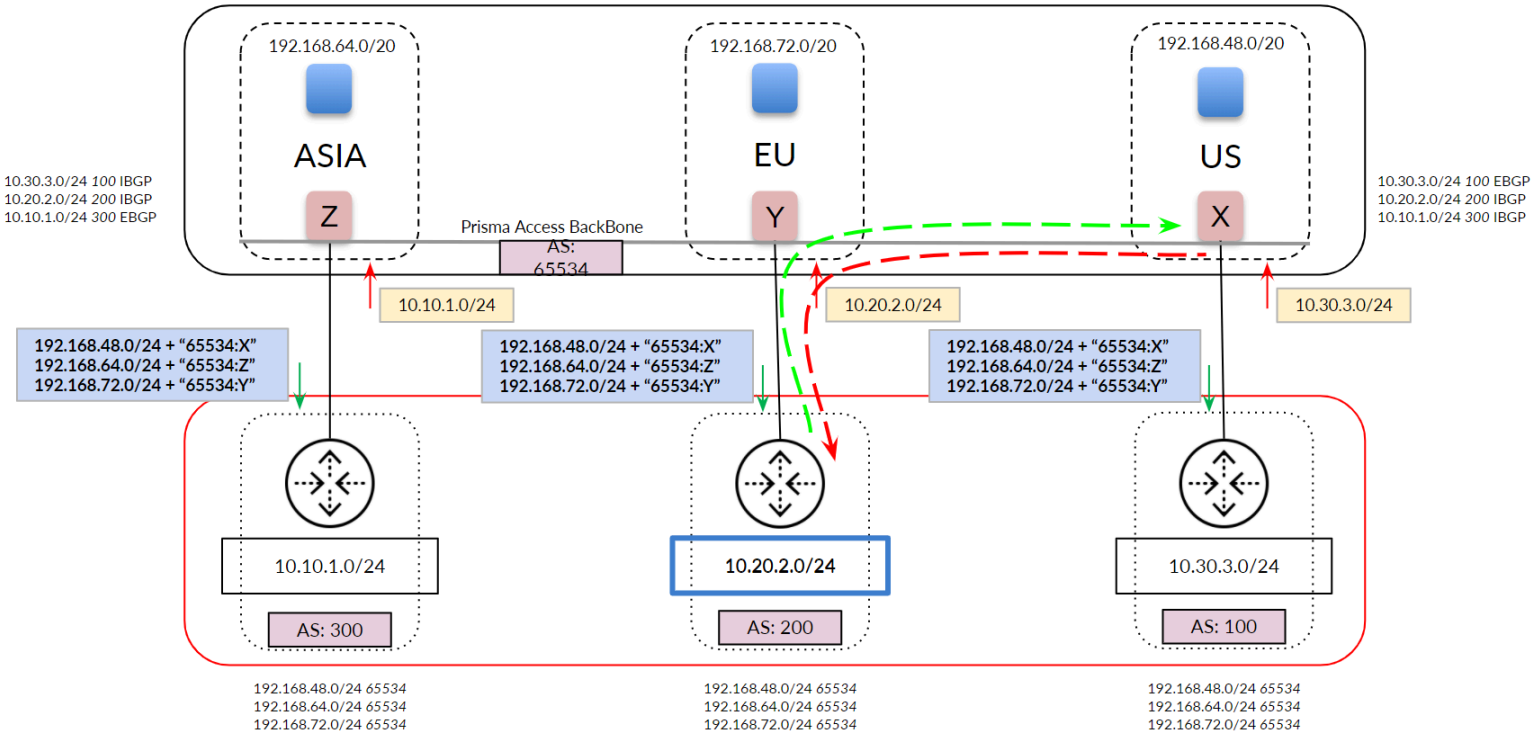
下圖顯示了預設路由模式下 Prisma Access 路由服務連線流量的範例。組織的網路在三個資料中心具有三個獨立的網絡，並且沒有連線網路的骨幹。在預設路由模式下，行動使用者集區平均地公告在三個網路上，如圖片底部所示。

請注意，當 Prisma Access 公告行動使用者路由時，它會在公告它們之前這樣做；因此，它會以 /24 區塊的形式公告 /20 行動使用者子網路，因為首碼是由閘道使用。

記下 Prisma Access 如何使用 BGP 路由公告：


©2025 Palo Alto Networks, Inc.

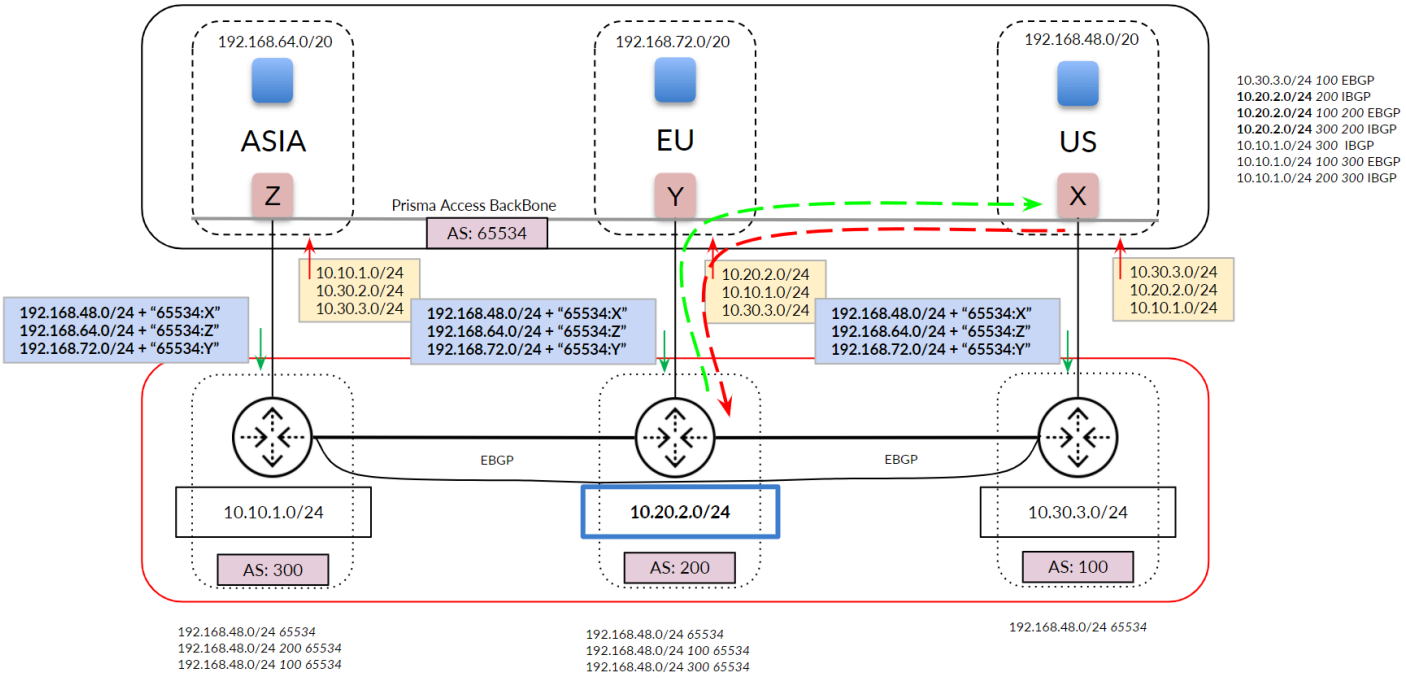
- Prisma Access 不會調整行動使用者公告路由的預設 BGP 屬性（Prisma Access 會將其 AS 編號新增至路由公告）。
- Prisma Access 會公告行動使用者路由，並在其透過服務連線公告的路由中新增 BGP 社群值。下圖顯示一個行動使用者部署，其中具有三個服務連線，以及為下列項目指定的三個不同 IP 位址區塊：`192.168.64.0/20` 用於亞洲、澳洲和日本地區、`192.168.72.0/20` 用於非洲、歐洲和中東地區，而 `192.168.48.0/20` 用於北美和南美洲地區。Prisma Access 會將這些路由劃分為 /24 的區塊，並使用 Prisma Access 的 AS 編號 **65534** 公告它們，但也會將 BGP 社群值附加到公告（**Z** 代表亞洲、**Y** 代表歐盟，而 **X** 代表美國）。這些路由顯示在圖片中間。透過這種方式，您可以區分網路中的服務連線，即使 Prisma Access 將相同的 AS 編號指派給它們也一樣。



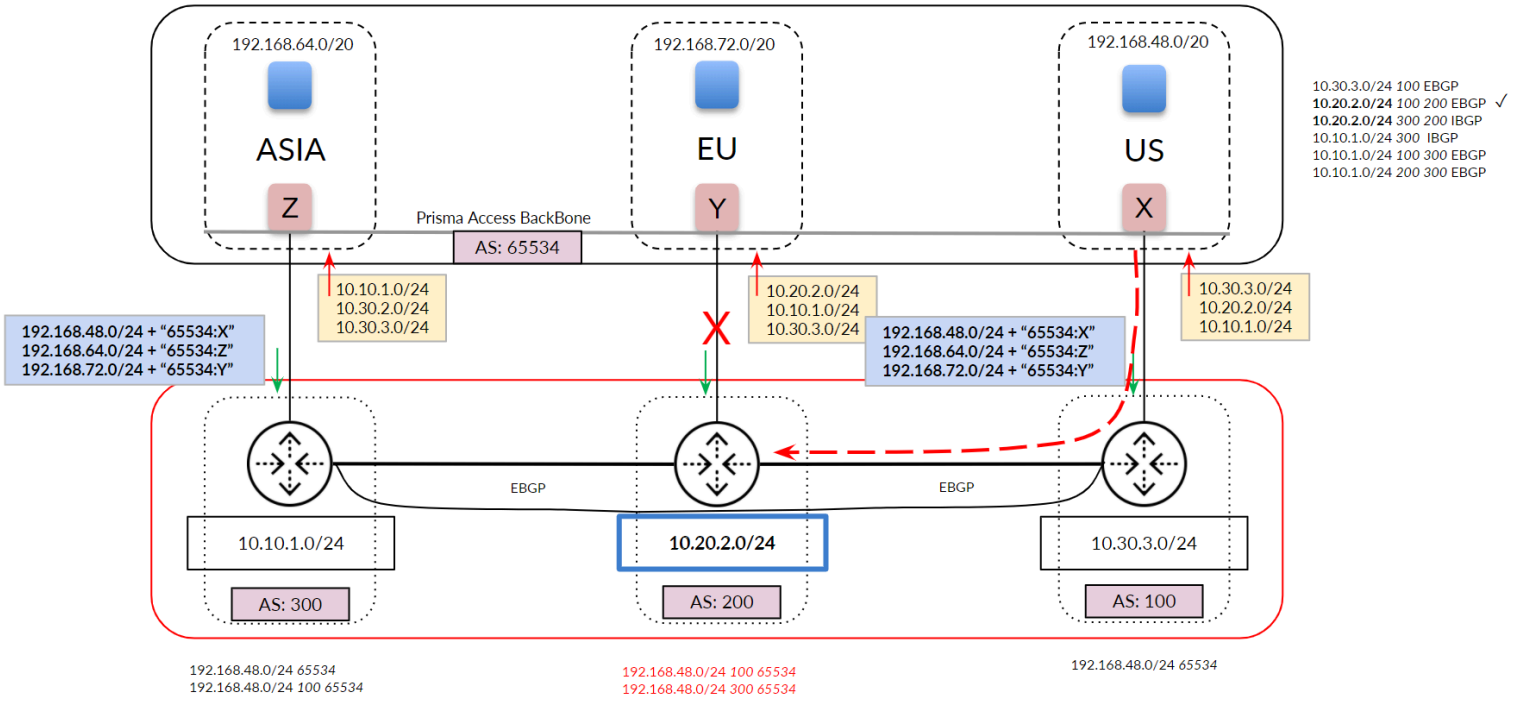

下圖顯示了具有全網狀 eBGP 骨幹的更常見網路。該圖顯示了 Prisma Access 已從右上角組織網路中得知的路由。請注意 Prisma Access 已透過 Prisma Access 骨幹 (iBGP) 和您組織骨幹 (eBGP) 得知的額外路由。

對於 **North America & South America**（北美和南美）地區（圖中的 US）的行動使用者與您組織的**Africa, Europe & Middle East**（非洲、歐洲和中東）地區（圖中的 EU）的資料中心之間的流量，Prisma Access 選擇透過 EU 服務連線的路徑，因為它偏好 AS-PATH 較短的路由。


©2025 Palo Alto Networks, Inc.




在具有全網狀 eBGP 骨幹的部署中，當 Prisma Access 由於客戶資料中心的 ISP/CPE 失敗而無法連線特定資料中心時，可能引發非對稱。下圖顯示了當 EU 服務連線的連結失效時可能發生的情況。您的網路偵測到連結失敗並為 AS 200 建立新的路由表。從 US 服務連線到 AS 200 的流量使用通過 AS 100 的路徑，因為 AS 200 與 AS 100 之間骨幹的 eBGP 路由優先於服務連線 EU 與 US 之間的 iBGP 路由。不過，不保證傳回流量通過相同路徑，因為內部部署 CPE 可以選擇任一路徑（以紅色顯示）來傳回流量。

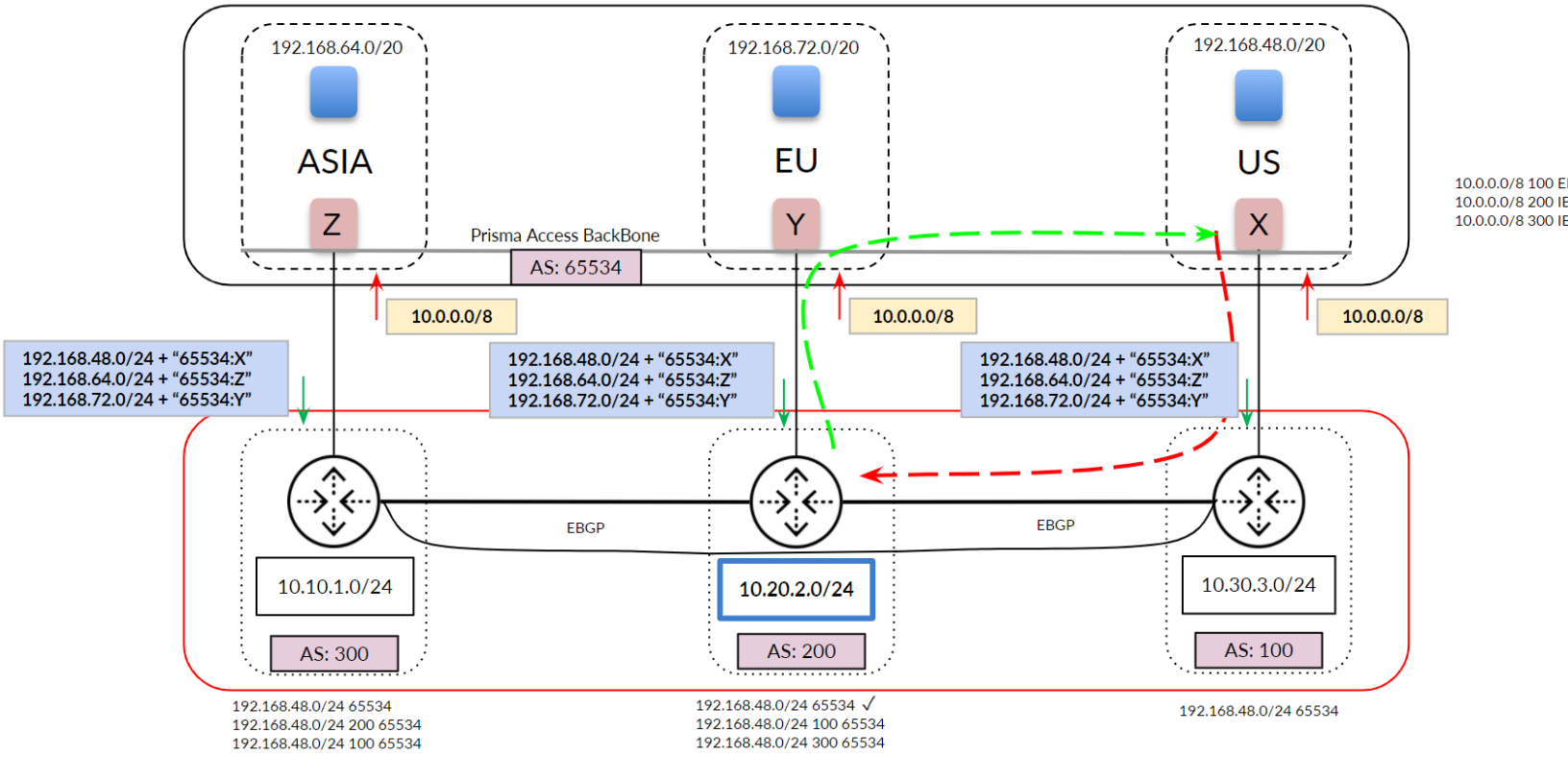



前面的範例顯示了一個未彙總路由的網路（亦即，在將 BGP 路由公告傳送至 Prisma Access 之前，您未執行路由彙總）。以下範例顯示了一個網路，其在將路由傳送到 Prisma Access 之前已將


©2025 Palo Alto Networks, Inc.

該路由彙總為 10.0.0.0/8。如果選取預設路由，此設定可能會造成非對稱路由問題，因為 Prisma Access 無法從匯總路由中確定正確的傳回路徑。

如果你的 *Prisma Access* 部署具有遠端網路，*Palo Alto Networks* 不建議在服務連線上使用路由彙總。服務連線上的路由彙總僅適用於行動使用者部署。




如果您對行動使用者使用路由彙總，我們強烈建議您啟用熱馬鈴薯路由而不是預設路由，其中 Prisma Access 會儘快地將流量傳遞至您組織的網路。此外，我們還建議您依下節所述為每個服務連線選取一個 **Backup SC**（備份 **S**）**C**，以具有決定性的路由行為。

## 熱馬鈴薯路由

當您選取 **Hot Potato Routing**（熱馬鈴薯路由）時,Prisma Access 會儘快從其內部網路輸出繫結至服務連線/資料中心的流量。

透過熱馬鈴薯路由，Prisma Access 會在從閘道傳送的 BGP 首碼公告前面加上 AS 路徑 (AS-PATH)。當這些首碼從服務連線公告至您組織的本機 CPE 時，會在其前面加上此路徑。Prisma Access 會將 AS-PATH 加在前面，以便 CPE 可為主要和次要通道提供正確的優先順序，如此在主要通道失效時，CPE 會選擇次要通道作為備份。

如果您為次要（備份）BGP 對等指定了不同的 IP 位址，則 Prisma Access 根據通道類型新增更多的前置，如下表所示。

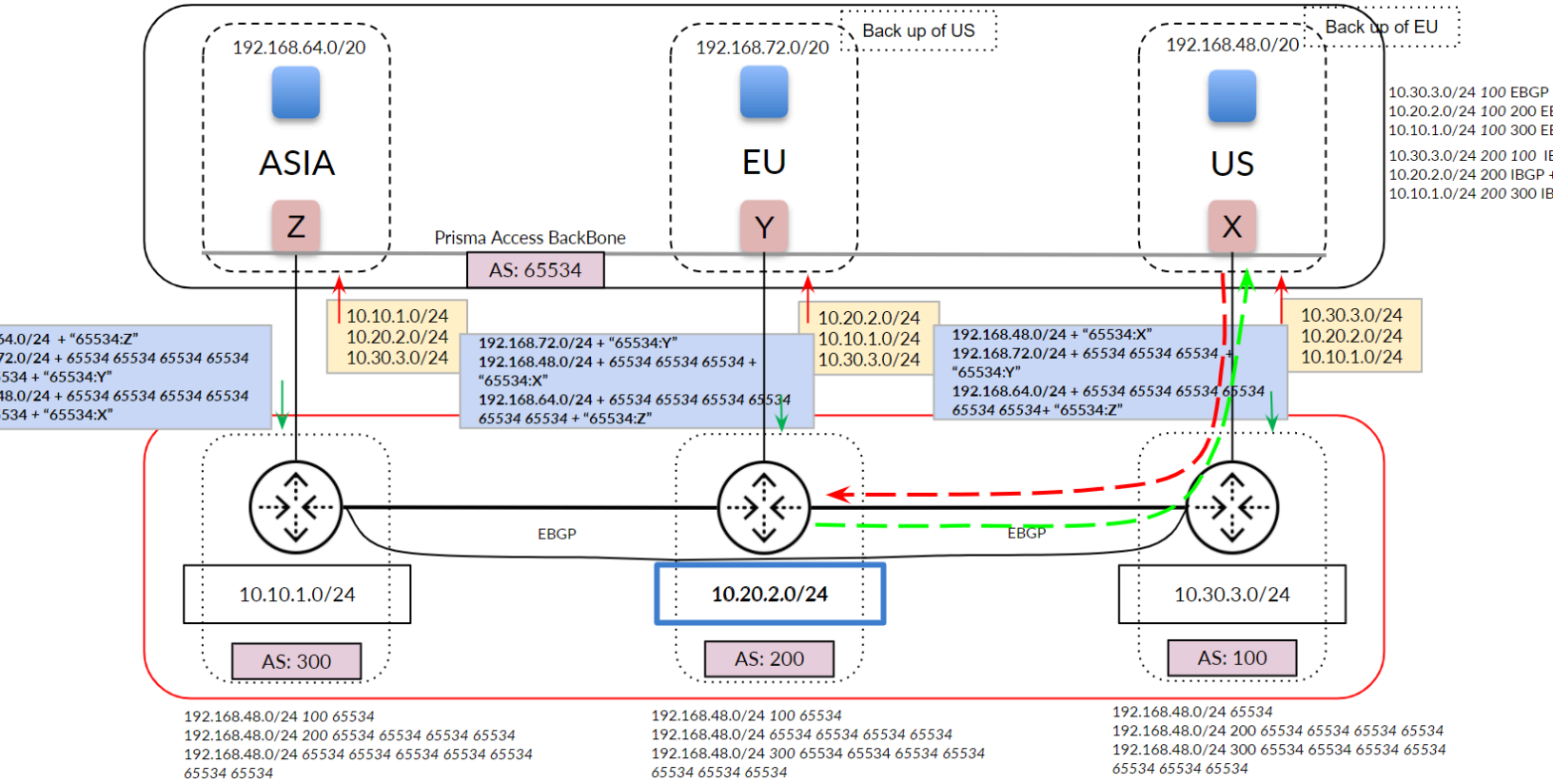

©2025 Palo Alto Networks, Inc.

| 首碼類型 | 服務連線通道類型 | **As-Path** 前置數目 | 在 **CPE** 上看到的 **AS-PATH** 總數 |
|---|---|---|---|
| 來自主要服務連線的閘道首碼 | 具有相同 BGP 對等 IP 位址的主要或次要通道 | 0 | 1 |
| 來自備份服務連線的閘道首碼 | 具有相同 BGP 對等 IP 位址的主要或次要通道 | 3 | 4 |
| 來自所有其他服務連線的閘道首碼 | 具有相同 BGP 對等 IP 位址的主要或次要通道 | 6 | 7 |
| 來自主要服務連線的閘道首碼 | 具有不同 BGP 對等 IP 位址的次要通道 | 1 | 2 |
| 來自備份服務連線的閘道首碼 | 具有不同 BGP 對等 IP 位址的次要通道 | 4 | 5 |
| 來自所有其他服務連線的閘道首碼 | 具有不同 BGP 對等 IP 位址的次要通道 | 7 | 8 |

指定 **Backup Service Connection**（備份服務連線），以便 Prisma Access 在服務連線連結失敗時使用該服務連線作為備份。

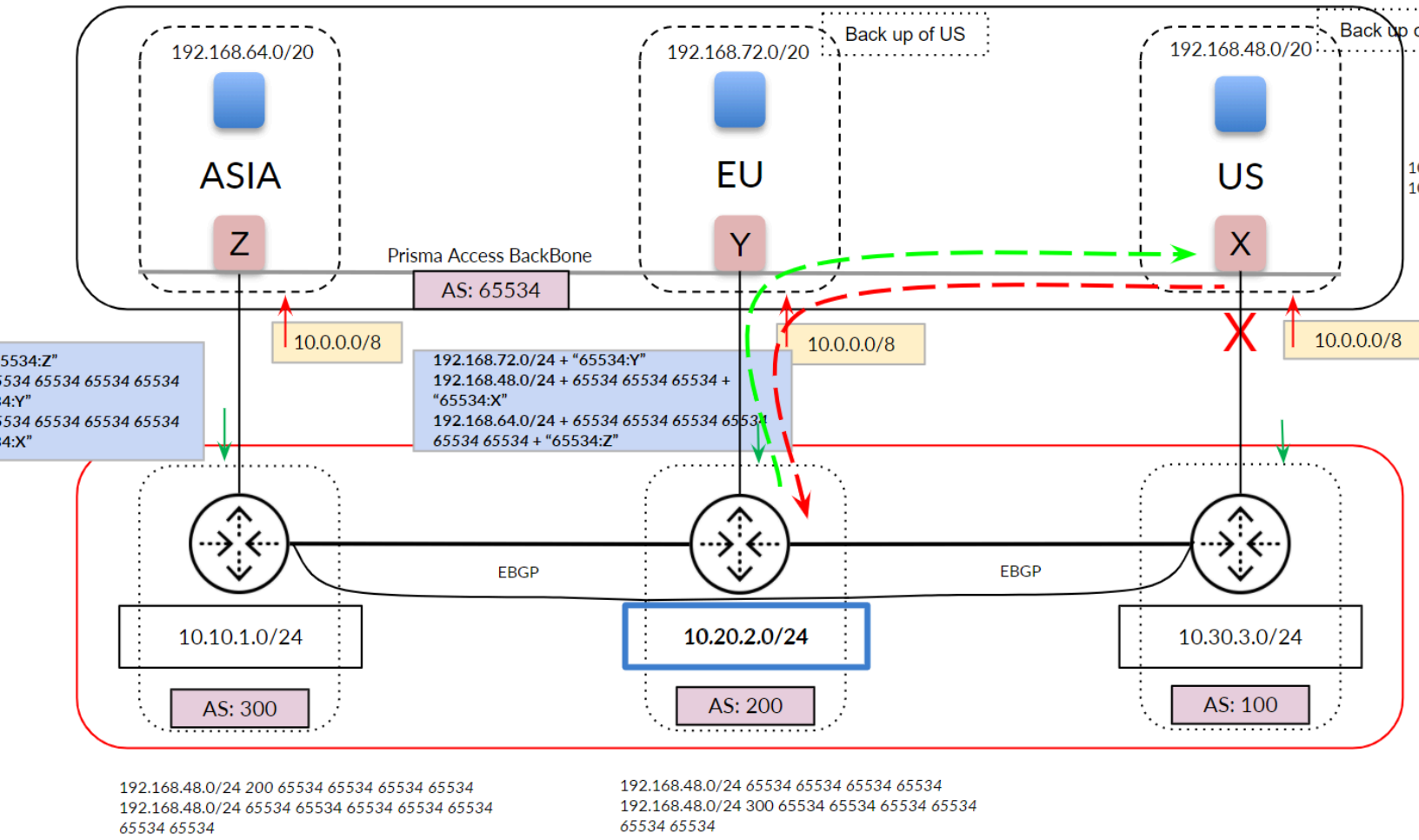
下圖顯示了美國服務連線與 AS 200 之間流量的熱馬鈴薯路由設定，其中歐盟服務連線設定為美國連線的 **Backup Service Connection**（備份服務連線）。使用熱馬鈴薯路由，Prisma Access 透過美國服務連線從其最近的出口路徑傳送流量。傳回流量採取通過 AS100 的相同路徑，因為此路徑具有對美國位置中行動使用者集區較短的 AS-PATH。Prisma Access 會在其首碼公告前面加上 AS-PATH，取決於通道是主要通道、備份通道，還是不用於主要通道或備份通道。

 ©2025 Palo Alto Networks, Inc.



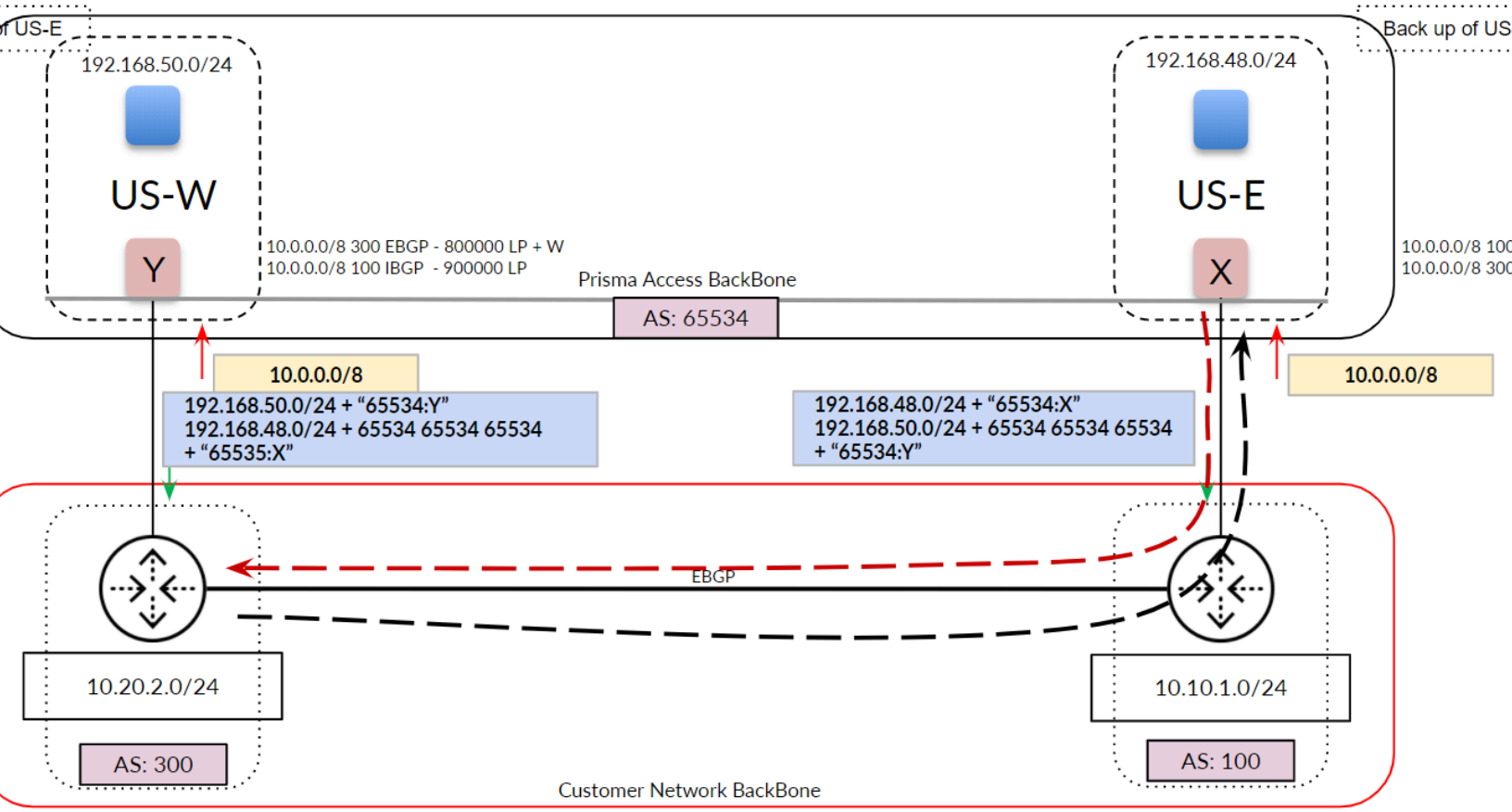

因為您已設定備份服務連線，所以如果美國服務連線的連結失效，熱馬鈴薯路由會使用其最短的路由透過歐盟服務連線將流量傳送出去。此路由案例也適用於使用路由彙總的網路。


©2025 Palo Alto Networks, Inc.




您還可以將備份服務連線用於單一區域中的多個服務連線。下圖顯示了在北美區域具有兩個服務連線的 Prisma Access 部署。在此情況下，您會指定 US-E 的 **Backup Service Connection**（備份服務連線）進行 US-W 服務連線，反之亦然，以確保對稱路由。


©2025 Palo Alto Networks, Inc.




 ©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

# Prisma Access ZTNA 連接器

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 4.0<br>❑ ZTNA 連接器附加元件授權<br>具有附加元件授權的基本授權包括 8 個 ZTNA 連接器、100 個 FQDN 和 4 個 IP 子網路功能。<br>具有附加元件授權的進階授權包括 40 個 ZTNA 連接器、300 個 FQDN 和 1024 個 IP 子網路功能。<br>具有附加元件授權的高級授權包括 200 個 ZTNA 連接器、4000 個 FQDN 和 1024 個 IP 子網路功能。<br>❑ 如果您未購買 ZTNA 連接器附加元件授權，Prisma Access 授權包括四個連接器、40 個 FQDN 和四個 IP 子網路。提供此功能的目的旨在您的環境中試用 ZTNA 連接器。 |

零信任網路存取 (ZTNA) 連接器可讓您簡單且安全地將 Prisma Access 連線到您組織的私人應用程式。ZTNA 連接器使用自動安全通道，讓行動使用者和分支位置的使用者可以存取您的私人應用程式。因為 ZTNA 連接器會自動設定通道，所以您不必手動設定 IPSec 通道，並路由到您私人應用程式所在的資料中心或總部位置、公用雲端位置和合作夥伴網路。

您部署的 ZTNA 連接器 VM 會自動連線到最近的 Prisma Access 位置確保最佳延遲，此外，還將頻寬存取調整為每個連接器最高 2 Gbps，每個連接器群組最高 8 Gbps。

Prisma Access 預設拒絕所有存取，並且管理員必須使用政策規則明確允許存取資源，該規則基於我們已取得專利的 User-ID、App-ID 和 Device-ID 建構，從而協助您減少攻擊面和安全性風險。一旦允許連線，我們就會持續驗證該連線的信任度、持續檢查是否有安全性威脅，並持續檢查資料是否外洩。此外，使用 Prisma Access ZTNA 連接器時，不會公開您應用程式的私人 IP 位址。

# ZTNA 連接器元件

- 連接器- 連接器是為 Prisma Access 建置通道的虛擬機器。ZTNA 連接器自動執行通道管理，而無需指定 IPSec 和 IKE 設定。您可以在 VM 中裝載連接器，而您會將這些 VM 裝載於雲服務端（Amazon Web Services (AWS)、Google Cloud Platform (GCP）、Microsoft Azure 或虛擬伺服器 (VMware ESXi)或核心型虛擬機器 (KVM)。Palo Alto Networks 建議您將與所裝載應用程式位於同一子網路的 VM 部署至 Prisma Access。您還可以提供不同的子網路，只要有從連接器到應用程式的路由。

  在您部署連接器 VM 之後，Prisma Access 會管理 VM，包括為您提供升級 VM 版本的選項。在安裝 ZTNA 連接器 VM 之後，它會探索最近的 Prisma Access 位置，並對 Prisma Access 啟動安全 IPsec 通道。
- 連接器群組—連接器群組是連接器和應用程式的邏輯分組。透過在連接器群組中新增多個連接器，您可以將通道備援和增加的頻寬提供給群組內的應用程式。每個連接器群組最多支援 4個連接器。

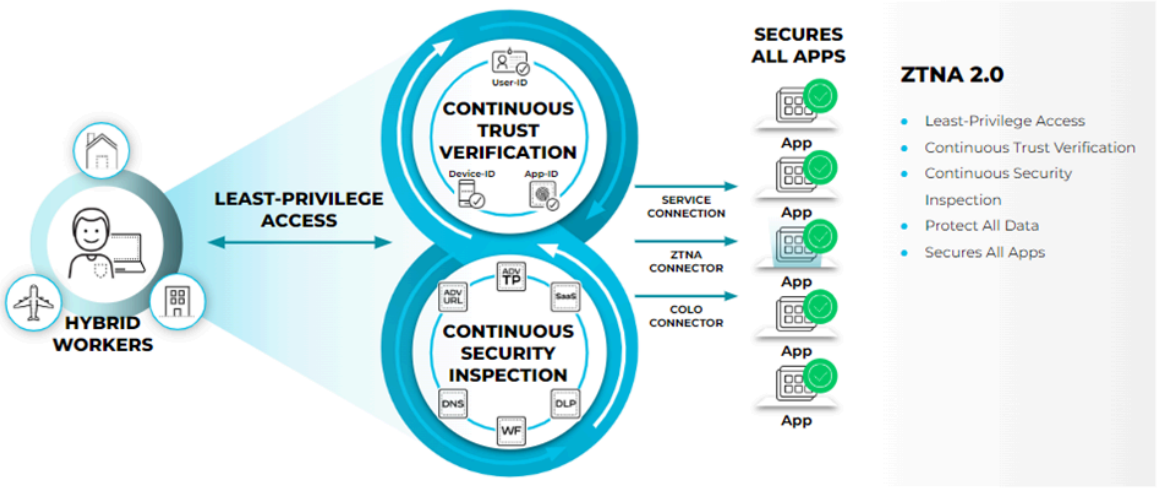
  如果您想要使用不同的連接器提供對特定應用程式的存取，請將連接器放置在個別的群組中。
- 目標—ZTNA 連接器將其裝載至 Prisma Access 的私人應用程式。您可以使用 FQDN（**FQDN Targets**（**FQDN** 目標））、萬用字元（**Wildcard Targets**（萬用字元目標）），或應用程式所在的 IP 位址或子網路。或者，您可以讓 ZTNA 連接器透過從連線到 CIE 的 IdP 中提取應用程式來自動探索這些應用程式。


©2025 Palo Alto Networks, Inc.

# ZTNA 連接器的使用案例

在以下案例中使用 ZTNA 連接器：

- 連線到私人應用程式—將 ZTNA 連接器用於連線到私人應用程式的所有用戶端啟動的流量。



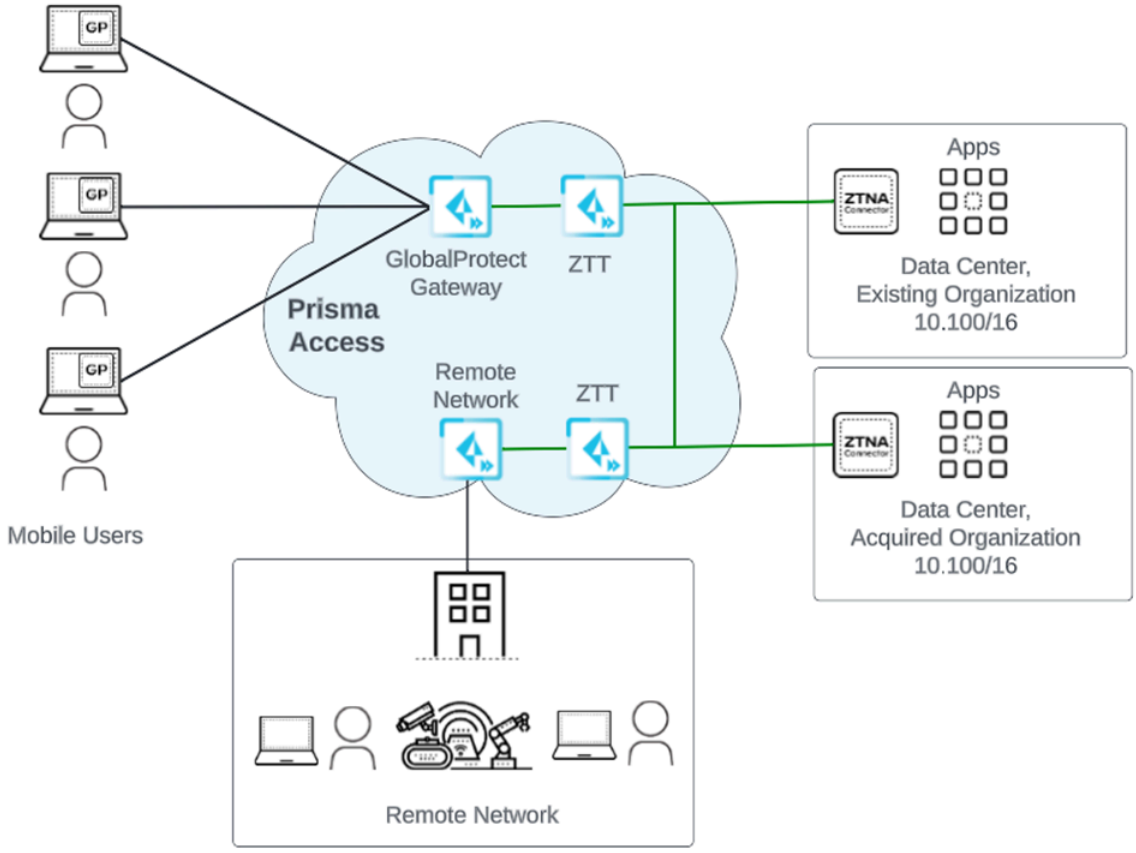

- 重疊的私人網路—如果您是已收購另一個組織或與其合併的大型企業中的網路管理員，則兩個網路可能會使用重疊的位址範圍（例如，RFC 1918 私人網路位址空間）。若要讓您的使用者可以存取重疊網路中託管的應用程式，路由和 NAT 設定可能會變得繁瑣。ZTNA 連接器允許您使用 FQDN、FQDN 萬用字元和 IP 子網路連線到應用程式，而無需設定 IP 路由，從而簡化了重疊網路中的應用程式存取。

  ZTNA 連接器會使用 ZTNA 連接器通道終端器 (ZTT)，讓您的使用者可以安全存取私人應用程式。

  當您在計算區域中啟動 ZTNA 連接器時，ZTT 節點會自動進行裝載。ZTNA 連接器會自動與 ZTT 構成 IPSec 通道。在刪除區域中的所有連接器之後，該區域中的 ZTT 節點會在 24 小時內


©2025 Palo Alto Networks, Inc.

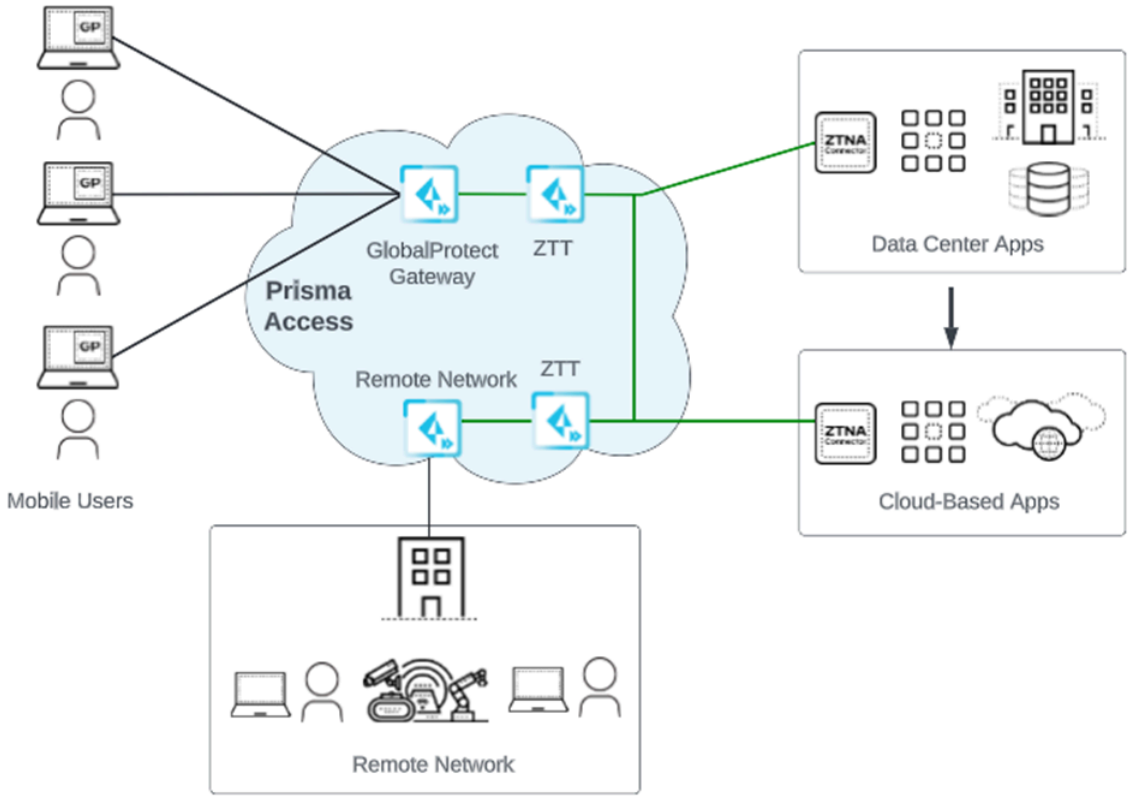
保持作用中狀態。如果在同一區域中刪除所有連接器後 24 小時內部署了新的連接器，它會重複使用現有的 ZTT。如果在 24 小時後啟動了新的 ZTNA 連接器，則會建立新的 ZTT。




- 資料中心至雲端移轉—如果您的組織正在將內部部署應用程式移轉到雲端（使用「直接遷移 (lift and shift)」移轉現有的內部部署應用程式或開發雲端原生應用程式），您可以在

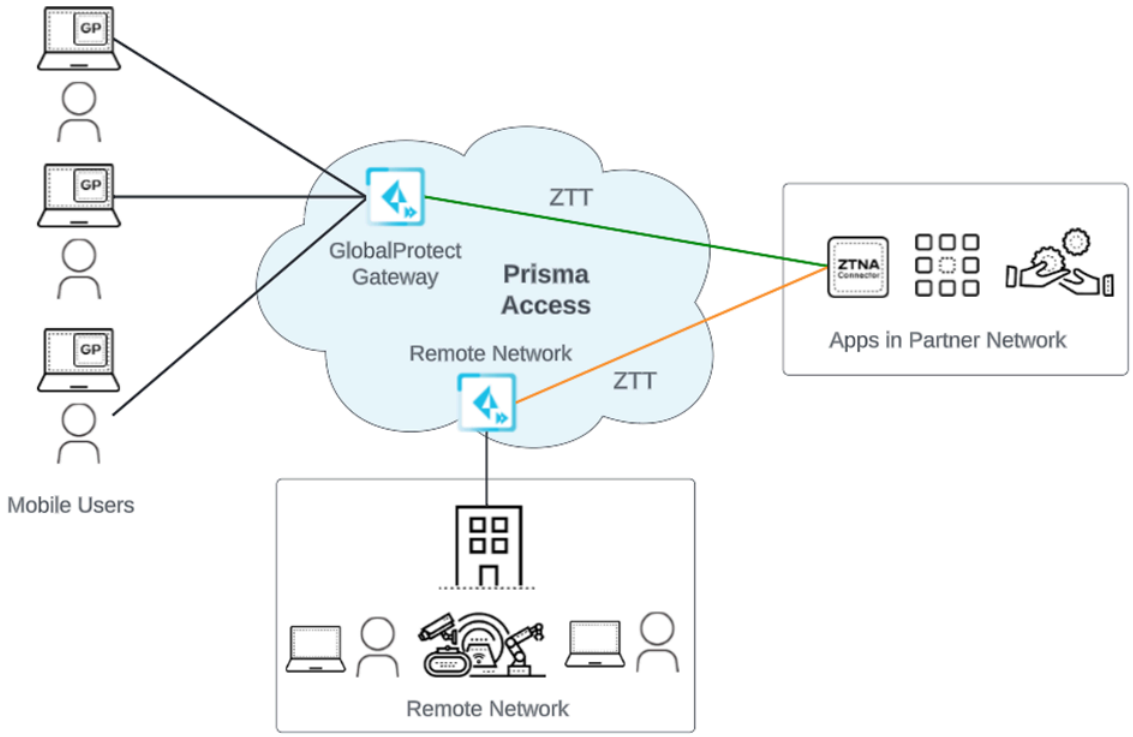
 ©2025 Palo Alto Networks, Inc.

AWS、GCP、Azure 或其他雲端提供者的雲端 VPC 中託管這些應用程式。如果您有數百或數千個 VPC，ZTNA 連接器可以加快提供雲端交付應用程式存取的過程。




 ©2025 Palo Alto Networks, Inc.

- 存取業務合作夥伴網路中的應用程式—某些組織會存取在其業務合作夥伴網路中託管的應用程式。使用服務連線來連線這些應用程式需要手動路由和 NAT 設定。ZTNA 連接器允許您連線到這些應用程式，而無需執行手動 IP 路由設定。




 ©2025 Palo Alto Networks, Inc.

# 服務連線和 ZTNA 連接器支援的使用案例

ZTNA 連接器無法取代服務連線。它可以與服務連線互補或共存，讓您能夠靈活地保護私人應用程式。如果您已部署服務連線，則可以繼續使用它們，除非您想要移到不同的應用程式存取模型。下表顯示了服務連線或 ZTNA 連接器支援和不支援的使用案例。核取標記表示支援使用案例；破折號 (—)表示不支援使用案例。

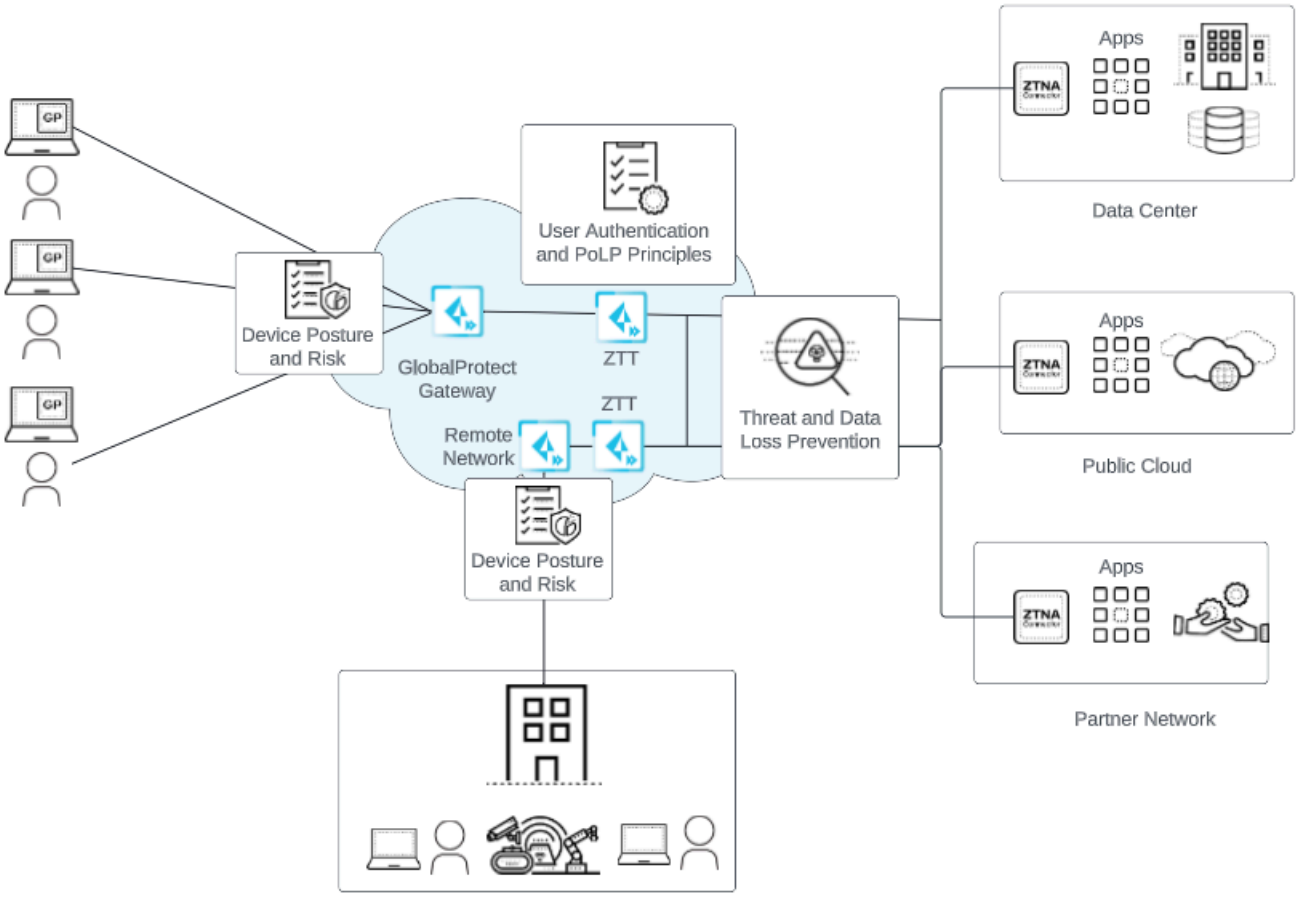
| 使用案例 | ZTNA 連接器支援 | 服務連線支援 |
|---|---|---|
| 存取重疊網路中的應用程式 | √ | — |
| 存取用戶端啟動的應用程式流量的所有連接埠和通訊協定 | √ | √ |
| 為 Prisma Access 自動建立通道 | √ | — |
| 自動 Prisma Access 位置探索 | √ | — |
| 自動調整 Prisma Access 位置，輸送量最高可為 10-Gbps | √ | — |
| 使用 IP 位址和子網路存取私人應用程式 | √ | √ |
| 伺服器啟動的流量（例如遠端服務台）到達受管理的裝置（GlobalProtect 行動使用者或遠端網路）。 | — | √ |
| 需要唯一用戶端 IP 位址的應用程式或服務 | √ | √ |
| 使用動態連接埠（如 FTP 主動模式或 VoIP）存取應用程式 | — | √ |
| 使用內部部署新世代防火牆進行混合部署，其中套用基於 User-ID 的政策規則 | √ | √ |


©2025 Palo Alto Networks, Inc.

# ZTNA 連接器 2.0 原則

ZTNA 連接器可讓您使用以下 ZTNA 連接器 2.0 原則，將私人應用程式連線到 Prisma Access：

- 裝置態勢和風險—使用基於 Prisma Access 中 User-ID 的政策規則，您可以為使用者和裝置（行動使用者和 IoT 裝置）定義一個態勢，以防止未經授權存取私人應用程式。您也可以在 ZTNA 連接器與 Prisma Access 之間建立通用政策規則。
- 使用者驗證和最低權限存取—使用基於使用者或群組的使用者驗證和政策規則，您可以實作最低權限原則 (PoLP)，讓使用者可以存取其所需的應用程式，同時封鎖存取其不需要的應用程式。
- 威脅和資料遺失防護—Prisma Access 和 ZTNA 連接器使用進階安全性功能，例如進階威脅防護、進階 URL 篩選、SaaS 安全性、進階 WildFire 和企業 DLP，以確保您的私人應用程式和應用程式資料是安全的。




 ©2025 Palo Alto Networks, Inc.

# ZTNA 連接器需求和指導方針

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 4.0<br>❑ ZTNA 連接器附加元件授權<br>具有附加元件授權的基本授權包括 8 個 ZTNA 連接器、100 個 FQDN 和 4 個 IP 子網路功能。<br>具有附加元件授權的進階授權包括 40 個 ZTNA 連接器、300 個 FQDN 和 1024 個 IP 子網路功能。<br>具有附加元件授權的高級授權包括 200 個 ZTNA 連接器、4000 個 FQDN 和 1024 個 IP 子網路功能。<br>❑ 如果您未購買 ZTNA 連接器附加元件授權，Prisma Access 授權包括四個連接器、40 個 FQDN 和四個 IP 子網路。提供此功能的目的旨在您的環境中試用 ZTNA 連接器。 |

在設定 ZTNA 連接器之前，請確保您瞭解連接器需求和限制，以及部署連接器時應遵循的指導方針。

## 支援的 Prisma Access 版本和需求

- Prisma Access 4.0 版，具有相容的 SaaS 代理程式。

  將任何早於 4.0 的 Prisma Access 版本（包括任何 Innovation 版本）升級到最低版本 4.0。

  如果您想要使用 FQDN 萬用字元或 IP 子網路存取應用程式，則至少需要 Prisma Access 5.0 版。此外，Prisma Access 5.0 解鎖了傾印概要、封包擷取和技術支援診斷工具的使用。
- 您必須將連接器版本至少升級至 6-2-2-ztna-connector-b1 才能使用 5.0 功能。
- 對於 Prisma Access (Managed by Panorama)，將雲端服務外掛程式版本至少升級到版本 4.0。升級到最新的雲端服務外掛程式以解鎖最新功能。

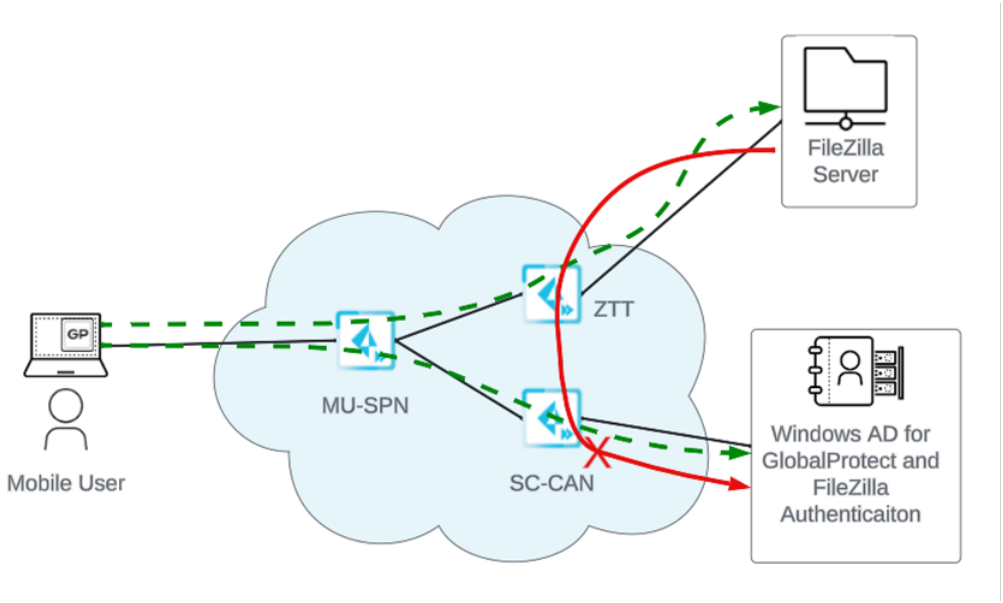
## 應用程式支援

ZTNA 連接器提供對所有私人應用程式流量的存取，但以下情況除外：


©2025 Palo Alto Networks, Inc.

- ZTNA 連接器不支援以下情況：
  - 來自資料中心的流量（例如 SCCM 或遠端服務台流量）。
  - 使用者 ID 重新散佈。
  - 執行連接埠跳躍的應用程式（例如 VoIP 或主動模式 FTP）。
  - 應用程式層級閘道 (ALG) 應用程式，例如主動模式 FTP 和 SIP。
  - 只有當您將資料中心網域控制站和資源裝載為 IP 位址子網路時，才支援應用程式的 Windows 整合式驗證（例如 NTLM 或 Kerberos）。支援 SAML、OAuth 和 LDAP。
  - 服務連線後面應用程式與 ZTNA 連接器後面應用程式之間的通訊。

    例如，您在服務連線後面託管 Windows Active Directory (AD) 伺服器（因為 ZTNA 連接器後面不支援 AD 伺服器），並在 ZTNA 連接器後面託管 FTP (Filezilla) 伺服器。如果 FTP 伺服器需要對 Windows AD 伺服器進行驗證，則驗證會失敗，因為您無法使用 Prisma Access 作為服務連線企業存取節點 (SC-CAN) 與 ZTNA 連接器通道終端器 (ZTT) 之間的骨幹。




## 特徵和功能限制

設定 ZTNA 連接器部署時請記住以下限制：

- 請勿在 ZTNA 物件名稱中使用特殊字元，包括 < > ! @ # $ % ^ &，以及中文、日文或韓文字元。
- 預設 Prisma Access 部署不支援以下功能；請聯繫您的 Palo Alto Networks 團隊來啟動它們：
  - 使用 RFC 6598 位址作為您的 Prisma Access 基礎結構 IP 位址搭配 ZTNA 連接器


©2025 Palo Alto Networks, Inc.

- 連接器群組指導方針—新增連接器群組時，請使用以下建議：
  - 單一連接器群組中的所有應用程式都應使用相同的 DNS 伺服器進行 DNS 解析。
  - 如果您是從資料中心或總部位置存取應用程式，則連接器群組中的所有應用程式都應來自同一資料中心或總部位置。
  - 請勿在單一連接器群組的兩個以上個區域中新增連接器。連接器群組中的所有連接器都應位於同一區域中。
  - 從 Prisma Access 5.01 開始，您可以指定每個 FQDN 目標或萬用字元目標最多四個連接器群組（5.0 版及更早版本支援每個 FQDN 目標或萬用字元目標一個單一連接器群組）。請確保，當您指派每個 FQDN 目標或萬用字元目標的連接器群組時，請勿將相同應用程式指派給每個區域四個以上連接器。

    例如，您已將相同應用程式（FQDN 目標或萬用字元目標）指派給四個連接器群組，每個群組都有一個單一連接器，並且所有連接器都位於同一區域中。此設定是可以接受的，因為您不會在單一區域中指派每個應用程式四個以上的連接器。

    不過，如果您將相同應用程式（FQDN 目標或萬用字元目標）指派給三個連接器群組、每個群組有兩個連接器，並且所有連接器都位於同一區域中，這是無效設定，因為您正在將六個連接器指派給單一區域中的相同應用程式。
- 某些 ZTNA 連接器（例如 AWS 型連接器或 Azure 型連接器）支援自動調整，其中 AWS 或 Azure 監控連接器上的網路頻寬使用率，並自動調整容量以維護應用程式效能。當連接器上的網路頻寬使用率下降時，AWS 或 Azure 會觸發自動相應縮小。如果 ZTNA 連接器中發生相應縮小，則由標記為相應縮小的 ZTNA 連接器所處理的現有長期工作階段會提前終止。此行為不會影響相應縮小後啟動的新流量工作階段。對於長期工作階段（例如 SSH 或 RDP），ZTNA 連接器會在相應縮小期間終止工作階段，並且您必須重新連線該工作階段。

## 規模和輸送量考量

ZTNA 連接器支援以下最大值：

- 所有連接器群組中每個租用戶 4,096 個應用程式
- 每個租用戶 200 個連接器
- 每個連接器群組 512 個應用程式
- 每個連接器群組 4 個連接器
- 每個連接器 200,000 個並行工作階段

  每個連接器可以支援 *200,000* 個並行連線。一個連接器群組最多可有 *4* 個連接器，而每個連接器群組最多 *800,000* 個並行連線。
- 26 個計算地區
- 每個連接器 1 Gbps 輸送量，而每個 Prisma Access 計算位置最多 10 Gbps

## 支援的應用程式託管環境

您可以在具有所指定最低需求的下列資料中心環境部署 ZTNA 連接器 VM：

 ©2025 Palo Alto Networks, Inc.

| 雲端提供者 | 執行個體大小 | CPU 大小 | 記憶體大小 | Disk Size 磁碟大小 |
|---|---|---|---|---|
| Amazon AWS | 每個區域 m5.xlarge | 4 個 vCPU | 16 GB | 40 GB |
| Google Cloud Platform (GCP) | 每個區域 n2-standard-4 | 4 個 vCPU | 16 GB | 40 GB |
| Microsoft Azure | 每個區域 Standard_D4_v3 | 4 個 vCPU | 16 GB | 40 GB |
| KVM | 使用 qcow 映像 | 4 個 vCPU | 16 GB | 40 GB |
| Hyper-V | 使用 vhd 映像 | 4 個 vCPU | 每個 VM 8 GB 記憶體 | 40 GB |
| VMware ESXi | 使用 OVA 映像。在 vSphere 上以及直接在 ESXi 主機上支援 | 每個 VM 4 個 vCPU | 每個 VM 8 GB 記憶體 | 40 GB 磁碟（厚佈健） |

對於 VMware ESXi，連接器 VM 不支援 vMotion、VM 快照或移轉。

對於 KVM，連接器 VM 上不支援即時移轉和快照。

託管 *VM* 並確保它們可以連線到網際網路，這是您的責任。

AWS、GCP 和 Azure 都有 ZTNA 連接器，您可以在其各自的 Marketplace 中取得。您可以從 Palo Alto 客戶支援入口網站下載 VMware ESXi 開放虛擬化應用程式 (OVA) 檔案和 KVM qcow 檔案。

## 網路需求

以下網路需求可在 ZTNA 連接器與 Prisma Access 之間啟用連線：

- 在啟用 ZTNA 連接器之後，Prisma Access 會使用為遠端網路和行動使用者—GlobalProtect 設定的 DNS 規則設定 DNS 要求的 DNS Proxy。
- 在通往 ZTNA 應用程式伺服器的路徑上，UDP 負載大小（包括標頭）不應超過 1,300 位元組的 MTU 大小。Palo Alto Networks 建議將封包保持在此 MTU 大小或以下。
- 允許來自 WAN 介面（連接埠 1）IP 位址的輸出 UDP 連接埠 4500 和 UDP 500，讓 IPSec 和 IKE 連線至 ZTNA 通道終端器 (ZTT)。如果您想要限制啟用輸出 UDP 連接埠 500 和 4500 連線至單一 IP 位址，請為 ZTNA 連接器的 **PA Service IP**（**PA** 服務 **IP**）位址（在 **Workflows**（工作流程）> **ZTNA Connector**（**ZTNA** 連接器）> **Connectors**（連接器）下）啟用它。




 ©2025 Palo Alto Networks, Inc.

- 如果 ZTNA 連接器為其網際網路介面使用公用 IP 位址，則您必須允許 IP/50 封裝安全性負載 (ESP)。
- 允許來自 WAN 介面（連接埠 1）IP 位址 HTTPS 的輸出 TCP 連接埠 443 連線至 ZTNA 連接器控制站。
- ZTNA 連接器自動設定 IPSec 通道的 Prisma Access ZTT 端和 ZTNA 連接器端。為 IKE 和 ESP 的 DH 群組/加密/雜湊設定的演算法為：ecp384/aes256/sha512。
- 請勿終止 ZTNA 連接器建立並用來存取私人應用程式的 IPSec 通道。
- （僅限行動使用者—GlobalProtect 部署）當您首次在 ZTNA 連接器上裝載應用程式時，必須重新整理 GlobalProtect 應用程式，以便行動使用者收到更新的 DNS 伺服器設定。如果您從 ZTNA 連接器中移除了應用程式，則必須重新整理 GlobalProtect 應用程式，以便行動使用者可以接收更新的 DNS 伺服器設定。
- 如果 ZTNA 連接器與私人應用程式之間有防火牆，則防火牆必須允許從 ZTNA 連接器存取應用程式（亦即，您必須允許為私人應用程式存取應用程式伺服器解析的 IP 位址、通訊協定和連接埠）。

  此外，您也需要允許您為應用程式探查應用程式目標健康情況所設定的通訊協定（TCP 或 ICMP）。連接器應用程式會探查應用程式伺服器，以確定它是否可以提供對應用程式的存取，並且您可以將應用程式目標的探查類型設定為 **tcp ping**、**icmp ping**或 **none**（無探查）。如果您指定 **tcp ping**，防火牆必須允許對應用程式的 TCP 存取；如果您指定 **icmp ping**，防火牆必須允許應用程式的 ICMP 回應要求和回覆。
- 在使用 ping 和 traceroute 診斷工具之前，請確保在您的資料中心允許 ICMP。出於安全考量，某些雲端環境不允許使用 ICMP；在此情況下，這些工具不會顯示任何活動。

  traceroute 診斷工具也會使用隨機 UDP 連接埠，因此您必須允許所有 UDP 和 ICMP 錯誤回覆，traceroute 工具才能運作。
- 確保您已在本機介面上設定 DNS 項目，以允許 ZTNA 連接器解析應用程式 FQDN，且該 ZTNA 連接器可在 UDP 連接埠 53（用於 DNS 解析的連接埠）存取 DNS 伺服器。
- （ZTNA 連接器版本 5.0 及更新版本）請確保您已在網路中設定安全性規則，以允許 ZTNA 連接器對您的資料中心執行應用程式探查。ZTNA 連接器會使用其資料中心介面 IP 位址，作為應用程式探查應用程式伺服器的來源 IP 位址。如果應用程式探查成功，則應用程式狀態為 **Up**（啟動），且 ZTNA 連接器的使用者工作階段具有與來源 IP 位址相同的資料中心介面 IP 位址。如果應用程式探查失敗，則應用程式狀態為 **Down**（關閉）；在此情況下，您可以使用 ping 和 tcp ping 診斷工具，來測試與應用程式的連線。
- 如果您在網路內使用 RFC 6598 共用位址，則必須 指定 IP 位址區塊，ZTNA 連接器可以將其用於 Prisma Access 與你連接器之間的路由，以及 Prisma Access 與您私人應用程式之間的路由。

 ©2025 Palo Alto Networks, Inc.

- 如果您需要限制新增至組織允許清單的 IP 位址和 FQDN 清單，請新增 ZTNA 連接器允許的 IP 位址和 FQDN 中列出的 IP 位址和 FQDN。

  例如，如果您要在美國設定 ZTNA 連接器，請將以下 URL 新增至您組織的允許清單：

  - https://controller.cgnx.net
  - https://locator.cgnx.net
  - https://controller.hood.cgnx.net
  - https://vmfg.hood.cgnx.net
  - https://sdwan-stats-hood-us.cgnx.net
  - time.nist.gov (for NTP)
  - 0.cloudgenix.pool.ntp.org (for NTP)
  - 1.cloudgenix.pool.ntp.org (for NTP)
  - 2.cloudgenix.pool.ntp.org (for NTP)
  - 3.cloudgenix.pool.ntp.org (for NTP)

  將先前 *FQDN* 的 *DNS* 解析限制為 *IPv4* 解析。*ZTNA Connector* 不支援使用 *IPv6* 建立與控制器 *FQDN* 的連線。
- 停用工作階段至控制器的 SSL 解密。

# ZTNA 連接器允許的 IP 位址和 FQDN

若要確保 ZTNA 連接器順利運作，請將以下 URL 和 IP 位址新增至您的允許清單。

| 服務名稱 | 連接埠 | 方向 | 來源介面網際網路通訊協定 | 目的地和 IP 位址 |
|---|---|---|---|---|
| ZTNA 連接器對 Prisma Access 的存取 | 443 | 輸出 | ZTNA 連接器 WAN 連接埠 | https://controller.cgnx.net<br>位址：52.8.93.87<br>位址：52.8.25.40<br>https://locator.cgnx.net<br>位址：13.56.217.238<br>位址：13.56.201.169<br>hood:<br>52.40.98.31<br>34.218.98.185<br>sugarloaf:<br>18.200.102.82<br>18.200.135.33<br>faber: |


©2025 Palo Alto Networks, Inc.

| 服務名稱 | 連接埠 | 方向 | 來源介面網際網路通訊協定 | 目的地和 IP 位址 |
|---|---|---|---|---|
| | | | | 18.139.242.53<br>54.255.61.109<br>https://vmfg.cgnx.net<br>位址：52.53.122.104<br>位址：52.53.102.7<br>https://controller.elcapitan.cgnx.net<br>位址：52.8.93.87<br>位址：52.8.25.40<br>https://vmfg.elcapitan.cgnx.net<br>位址：52.53.122.104<br>位址：52.53.102.7<br>https://controller.hood.cgnx.net<br>位址：52.32.167.5<br>位址：54.70.168.33<br>https://vmfg.hood.cgnx.net<br>位址：50.112.136.184<br>位址：34.210.34.87<br>https://controller.sugarloaf.cgnx.net<br>位址：108.128.176.192<br>位址：18.200.144.58<br>https://vmfg.sugarloaf.cgnx.net<br>位址：99.81.179.99<br>位址：99.80.52.255<br>https://sdwan-stats-hood-us.cgnx.net<br>https://sdwan-stats-elcapitan-us.cgnx.net<br>https://sdwan-stats-hood-jp.cgnx.net<br>https://sdwan-stats-elcapitan-jp.cgnx.net |


©2025 Palo Alto Networks, Inc.

| 服務名稱 | 連接埠 | 方向 | 來源介面網際網路通訊協定 | 目的地和 IP 位址 |
|---|---|---|---|---|
| | | | | https://sdwan-stats-hood-sg.cgnx.net<br>https://sdwan-stats-elcapitan-sg.cgnx.net<br>https://sdwan-stats-hood-au.cgnx.net<br>https://sdwan-stats-elcapitan-au.cgnx.net<br>https://sdwan-stats-hood-in.cgnx.net<br>https://sdwan-stats-elcapitan-in.cgnx.net<br>https://sdwan-stats-hood-ca.cgnx.net<br>https://sdwan-stats-elcapitan-ca.cgnx.net<br>https://sdwan-stats-sugarloaf-eu.cgnx.net<br>https://sdwan-stats-sugarloaf-de.cgnx.net<br>https://sdwan-stats-sugarloaf-uk.cgnx.net<br>https://controller.bowfell.cgnx.net<br>位址：13.41.243.90<br>位址：18.171.17.23<br>https://vmfg.bowfell.cgnx.net<br>位址：52.56.35.36<br>位址：52.56.224.242<br>https://controller.faber.cgnx.net<br>位址：52.74.47.220<br>位址：13.251.109.27<br>https://vmfg.faber.cgnx.net<br>位址：18.142.153.59<br>位址：52.74.58.219 |


©2025 Palo Alto Networks, Inc.

| 服務名稱 | 連接埠 | 方向 | 來源介面網際網路通訊協定 | 目的地和 IP 位址 |
|---|---|---|---|---|
| | | | | h<br>ttps://controller.townsend.cgnx.net<br>位址：13.55.31.41<br>位址：3.106.168.215<br>https://vmfg.townsend.cgnx.net<br>位址：52.64.177.240<br>位址：13.55.164.51<br>https://sdwan-stats-faber-sg.cgnx.net<br>https://sdwan-stats-bowfell-uk.cgnx.net<br>https://sdwan-stats-townsend-au.cgnx.net |
| NTP | 123 | 輸出 | ZTNA 連接器 WAN 和 LAN 連接埠 | time.nist.gov<br>0.cloudgenix.pool.ntp.org<br>1.cloudgenix.pool.ntp.org<br>2.cloudgenix.pool.ntp.org<br>3.cloudgenix.pool.ntp.org |
| DNS | 53 | 輸出 | ZTNA 連接器 WAN 和 LAN 連接埠 | 客戶或提供者 DNS 伺服器 |

## 憑證管理

為了確保安全通訊工作階段中的各方能相互信任，Prisma Access 使用數位憑證。各憑證均包含加密金鑰，用於將明文加密或將加密文字解密。各憑證也包含數位簽章，以驗證簽發者的識別。簽發者必須列在驗證方的受信任憑證授權單位 (CA) 清單中。驗證方可選擇性地驗證簽發者是否未撤銷憑證。Prisma Access 會使用憑證來保護解密和驗證之類的功能，以及所有連線至網路的用戶端、伺服器、使用者和裝置之間的通訊。

對於裝載至 ZTNA Connector 的應用程式，請使用 Prisma Access 憑證管理來設定憑證、新增憑證授權單位，並定義憑證檢查。


©2025 Palo Alto Networks, Inc.

# 啟用 ZTNA 連接器

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 4.0<br>❑ ZTNA 連接器附加元件授權<br>具有附加元件授權的基本授權包括 8 個 ZTNA 連接器、100 個 FQDN 和 4 個 IP 子網路功能。<br>具有附加元件授權的進階授權包括 40 個 ZTNA 連接器、300 個 FQDN 和 1024 個 IP 子網路功能。<br>具有附加元件授權的高級授權包括 200 個 ZTNA 連接器、4000 個 FQDN 和 1024 個 IP 子網路功能。<br>❑ 如果您未購買 ZTNA 連接器附加元件授權，Prisma Access 授權包括四個連接器、40 個 FQDN 和四個 IP 子網路。提供此功能的目的旨在您的環境中試用 ZTNA 連接器。 |

在您可以設定 ZTNA 連接器之前，必須在 Prisma Access 內部啟用它。在啟用 ZTNA 連接器之前，請執行以下操作：

- 檢閱 ZTNA 連接器需求和指導方針。
- 識別您的應用程式 IP 和連接器 IP 位址區塊。您必須保留個別的地址集區，以便在內部於 Prisma Access 內使用，將流量路由到您將要裝載的連接器和私人應用程序。Prisma Access 會將您裝載至 ZTNA 連接器的應用程式的 FQDN 解析為應用程式 IP 位址區塊中的 IP 位址。同樣地，Prisma Access 會使用連接器 IP 位址區塊，將流量從遠端網路或行動使用者路由到適當的 ZTNA 連接器。

  您應該為位址集區保留至少一個 /16 子網路。使用 RFC 1918 或 RFC 6598 位址。您可以在 ZTNA 連接器設定期間指定 RFC 1918 位址集區，而不是 RFC 6598；不過，在指定 RFC 1918 之後，您無法將位址集區類型變更回 RFC 6598。
- Strata Cloud Manager
- Panorama

## 啟用 ZTNA 連接器 (Strata Cloud Manager)

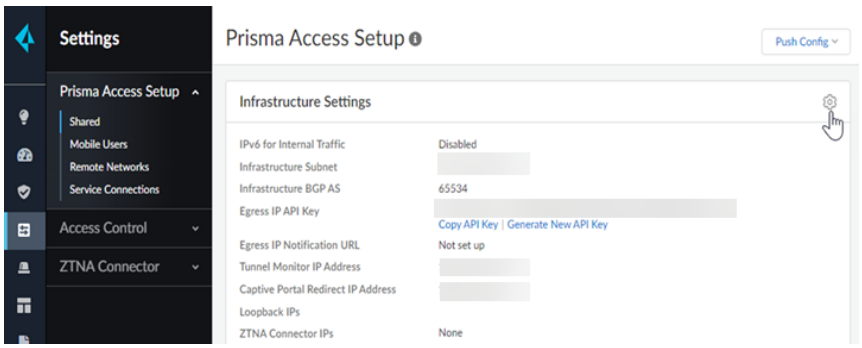
使用下列工作流程，在 Cloud Managed Prisma Access 中啟用 ZTNA 連接器。


©2025 Palo Alto Networks, Inc.

**STEP 1 |** 設定 Prisma Access 將在內部使用的 IP 位址區塊，以將流量路由到 ZTNA 連接器和您裝載的私人應用程式。

您必須為連接器和應用程式定義個別的 IP 位址區塊，而且這些區塊不能與 Prisma Access 基礎結構子網路或您的 GlobalProtect IP 位址集區彼此重疊。

- 選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Prisma Access** > **Infrastructure Settings**（基礎結構設定）。

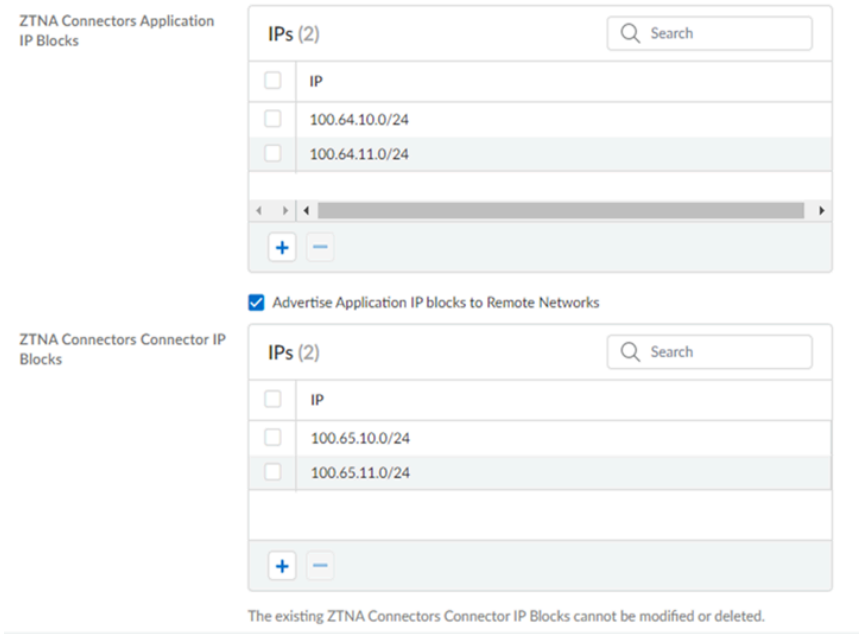



- 新增 **ZTNA Connectors Application IP Blocks**（**ZTNA** 連接器應用程式 **IP** 區塊）。

  您可以新增單一應用程式 IP 區塊或多個區塊，取決於您的部署。例如，輸入 100.64.10.0/24 和 100.64.11.0/24。您也可以 **Advertise Application IP blocks to Remote Networks**（將應用程式 **IP** 區塊公告至遠端網路），以提供遠端網路存取。

- 新增 **ZTNA Connectors Connector IP Blocks**（**ZTNA** 連接器的連接器 **IP** 區塊），Prisma Access 將在內部使用這些區塊，路由行動使用者、遠端網路和資料中心連接器 VM 之間的流量。

  您可以新增單一連接器 IP 區塊或多個區塊，取決於您的部署。例如，輸入 100.65.10.0/24 和 100.65.11.0/24。

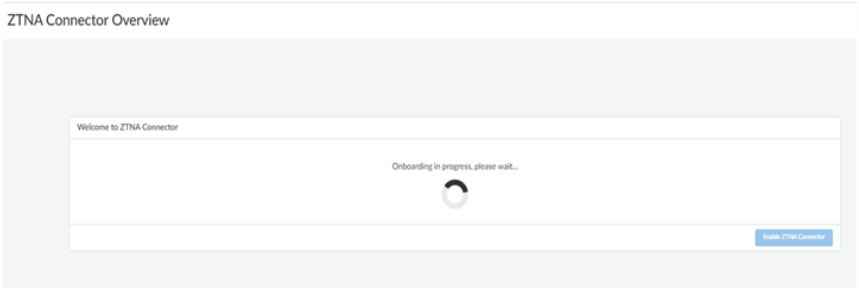



- 按一下 **Save**（儲存）以儲存 IP 位址區塊設定，然後 **Commit**（提交）並推送設定。

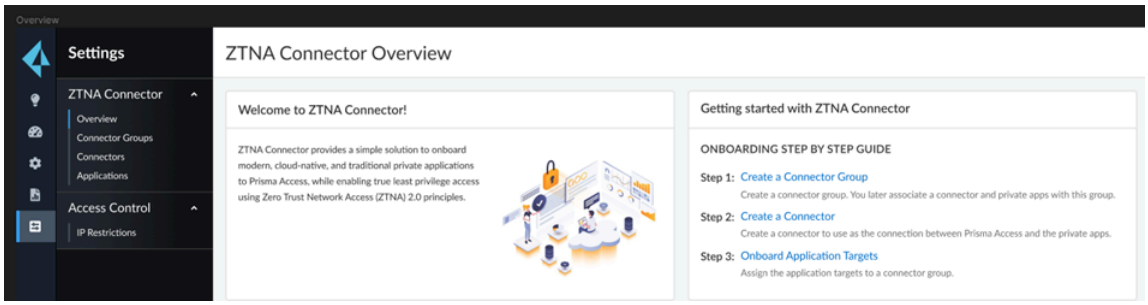
 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 從 Strata Cloud Manager 中啟動 ZTNA 連接器。

- 選取 **Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器）。
- Prisma Access 開始設定 ZTNA 連接器的基礎結構。這可能需要幾分鐘時間。




- 裝載完成時，會顯示 ZTNA 連接器概要。



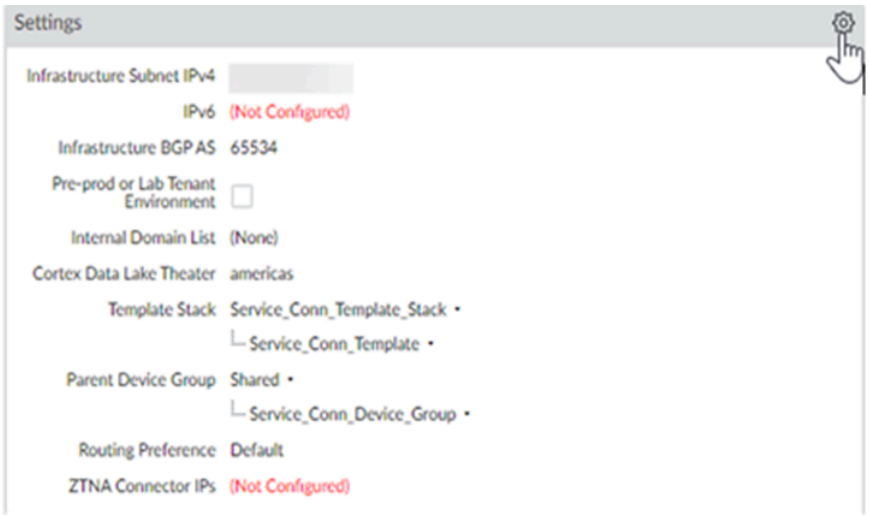

# 啟用 ZTNA 連接器 (Panorama)

使用下列工作流程，在 Prisma Access (Managed by Panorama) 中啟用 ZTNA 連接器。

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** 設定 Prisma Access 將在內部使用的 IP 位址區塊，以將流量路由到 ZTNA 連接器和您裝載的私人應用程式。

- 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定），然後 **Edit**（編輯）**Settings**（設定）。



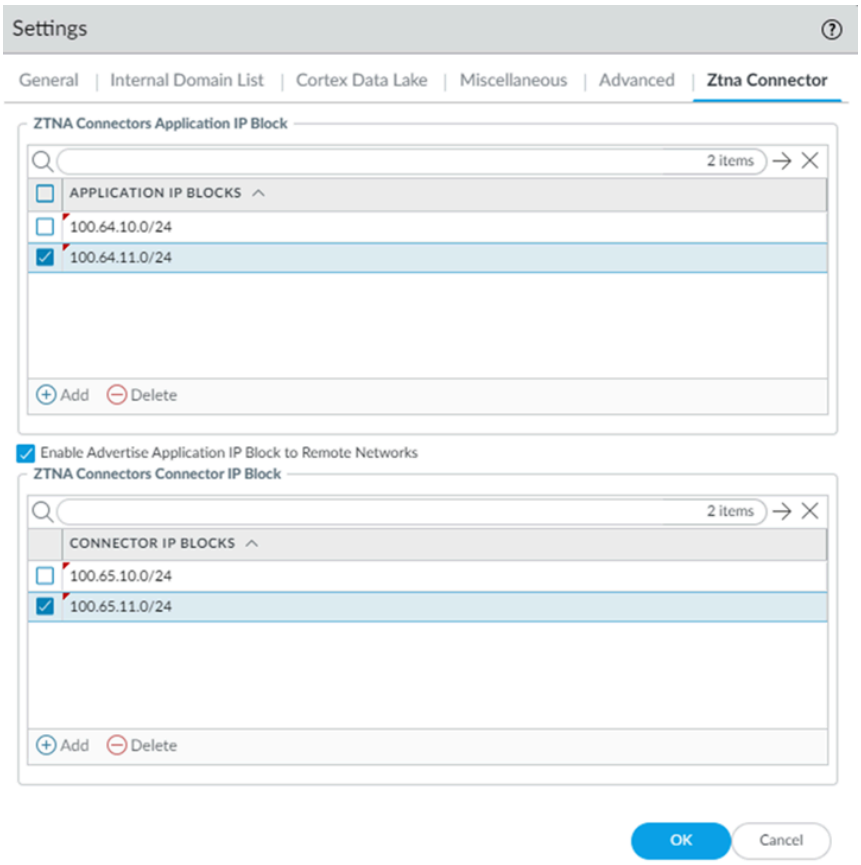

- 在 **ZTNA Connector**（**ZTNA** 連接器）頁籤上，**Add**（新增） **Application IP Block**（應用程式 **IP** 區塊）。

  您可以新增單一應用程式 IP 區塊或多個區塊，取決於您的部署。例如，如果 100.64.10.0/24 和 100.64.11.0/24。您也可以 **Enable Advertise Application IP Block to Remote Networks**（啟用將應用程式 **IP** 區塊公告至遠端網路）。

- 設定 **Connector IP Blocks**（連接器 **IP** 區塊），Prisma Access 將在內部使用這些區塊，在行動使用者、遠端網路和資料中心的連接器 VM 之間路由流量。

  您可以新增單一連接器 IP 區塊或多個區塊，取決於您的部署。例如，輸入 100.65.10.0/24 和 100.65.11.0/24。

 ©2025 Palo Alto Networks, Inc.

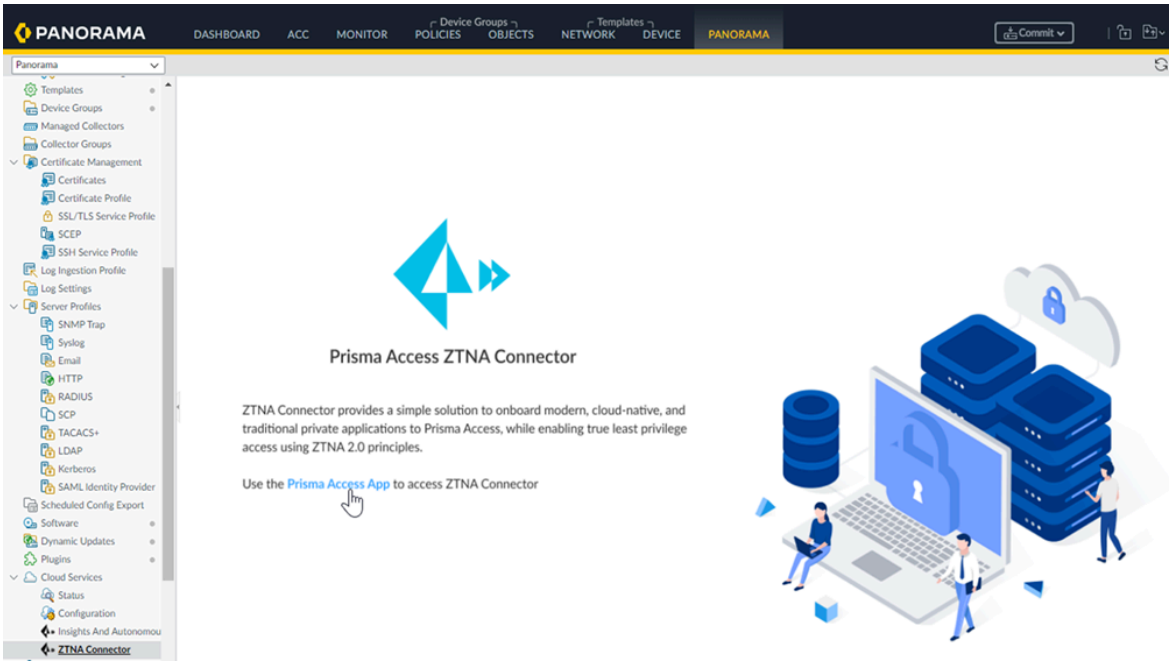



- 按一下 **OK**（確定）以儲存 IP 位址區塊設定，然後 **Commit**（提交）並推送設定。

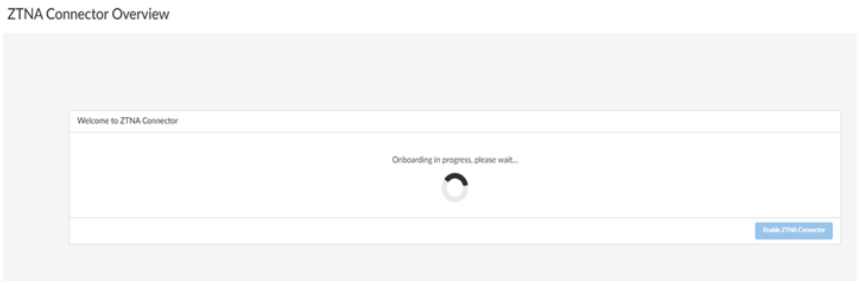

©2025 Palo Alto Networks, Inc.

**STEP 2 |** 從 Panorama 上的雲端服務外掛程式啟動 ZTNA 連接器。

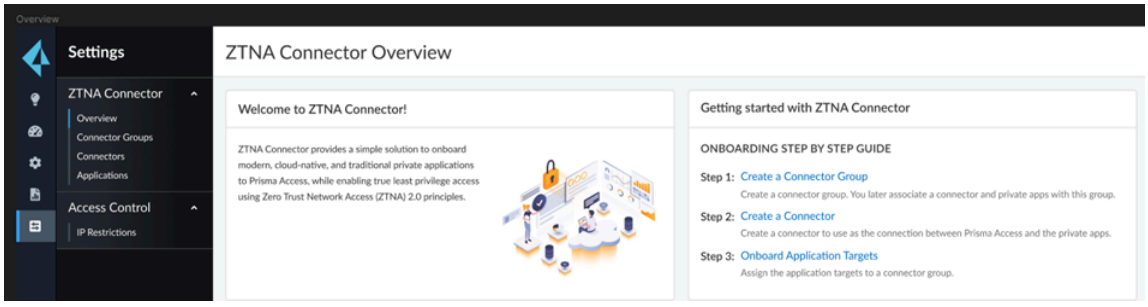
- 選取 **Panorama** > **Cloud Services**（雲端服務） > **ZTNA Connector**（**ZTNA** 連接器）。
- 按一下 Strata Cloud Manager 以啟動中樞上 Strata Cloud Manager 中的 ZTNA 連接器。




- 從 Strata Cloud Manager 中，選取 **Settings**（設定） > **ZTNA Connector**（**ZTNA** 連接器）。
- Prisma Access 開始設定 ZTNA 連接器的基礎結構。這可能需要幾分鐘時間。




- 裝載完成時，會顯示 ZTNA 連接器概要。




 ©2025 Palo Alto Networks, Inc.

# 設定 ZTNA 連接器

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 4.0<br>❑ ZTNA 連接器附加元件授權<br>具有附加元件授權的基本授權包括 8 個 ZTNA 連接器、100 個 FQDN 和 4 個 IP 子網路功能。<br>具有附加元件授權的進階授權包括 40 個 ZTNA 連接器、300 個 FQDN 和 1024 個 IP 子網路功能。<br>具有附加元件授權的高級授權包括 200 個 ZTNA 連接器、4000 個 FQDN 和 1024 個 IP 子網路功能。<br>❑ 如果您未購買 ZTNA 連接器附加元件授權，Prisma Access 授權包括四個連接器、40 個 FQDN 和四個 IP 子網路。提供此功能的目的旨在您的環境中試用 ZTNA 連接器。 |

在您 啟用 ZTNA 連接器 之後，您可以開始設定 ZTNA 連接器元件：

**STEP 1 |** 識別您的應用程式 IP 和連接器 IP 位址區塊，並在 Prisma Access 中新增 IP 位址區塊。



如需 *IP* 位址區塊，請參閱以下建議：

- 為每個應用程式指派個別的 *IP* 位址。
- 為每個連接器指派至少一個 */27 IP* 位址區塊（每個連接器至少 *32* 個 *IP* 位址）。
- 為每個連接器群組指派唯一的 *IP* 位址。

您可以視需要新增更多的連接器或應用程式區塊來滿足需求。

如果您在網路內使用 RFC 6598 位址，則必須保留個別的 RFC 6598 IP 位址集區，以保留給 Prisma Access 內部使用，將流量路由到您將裝載的連接器和私人應用程式。

**STEP 2 |** 建立連接器群組

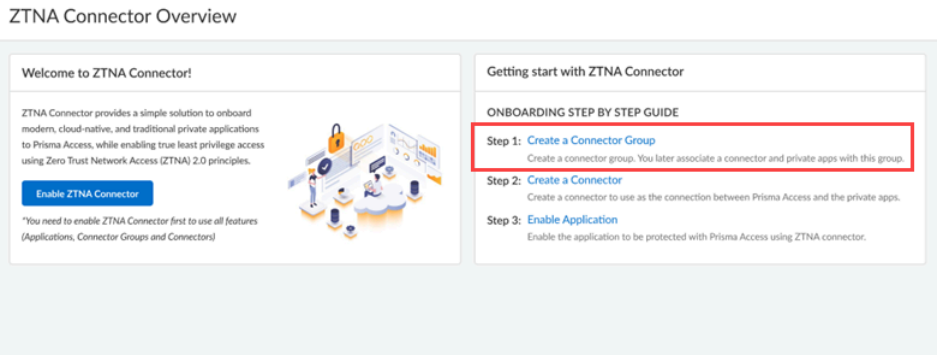
連接器群組是連接器和應用程式的邏輯分組。有許多不同的方式可將應用程式和連接器分組。您可以將不同地理位置的連接器分組以取得備援。或者，您可以在同一資料中心建立多個連

 ©2025 Palo Alto Networks, Inc.

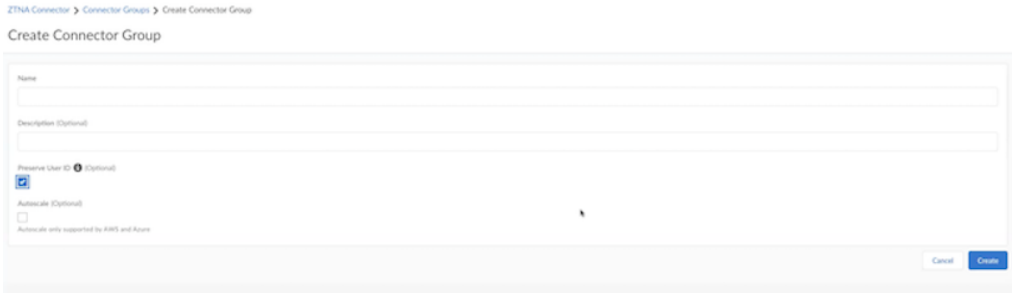
接器以提高輸送量。為了簡化政策管理，您可能想要將相同使用者群組使用的應用程式進行分組。首先建立連接器群組，然後將連接器和應用程式新增至這些群組。

視需要重複此步驟，以建立將連接器和應用程式分組所需的所有連接器群組。

1. 選取**Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器）、選取 **Overview**（概要）或 **Connector Groups**（連接器群組），然後 **Create Connector Group**（建立連接器群組）。




2. 給與連接器群組一個 **Name**（名稱）、啟用 **Preserve User ID**（保留使用者 **ID**），並選擇性地為其提供 **Description**（說明）。




3. （選用）如果您的資料中心位於 Azure 或 AWS，並且您想要使用自動調整功能，請選取 **Autoscale**（自動調整）。如果您已啟用此功能，則無需建立連接器。
4. **Create**（建立）連接器群組。

 ©2025 Palo Alto Networks, Inc.

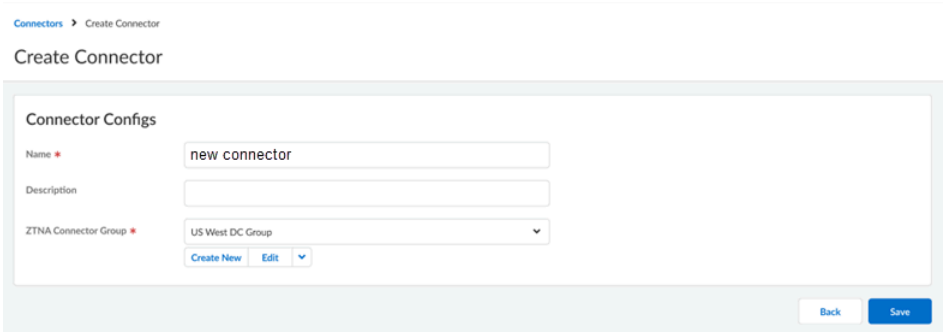
**STEP 3 |** 僅當您選取非自動調整連接器群組時，才會建立連接器並將其新增至連接器群組。

建立連接器並將其新增至連接器群組。

連接器代表在連線至 Prisma Access 的資料中心執行的 VM。您必須在 Prisma Access 內建立連接器，並使用提供的密碼/金鑰，在資料中心裝載對應的連接器 VM。

視需要重複此步驟，建立將資料中心應用程式連線至 Prisma Access 所需數量的連接器。

- 選取**Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器）、選取 **Overview**（概要）或 **Connector**（連接器），然後 **Create Connector**（建立連接器）。
- 輸入連接器的 **Name**（名稱）。




- （選用）新增連接器的 **Description**（說明）。
- 選取應新增連接器的 **Connector Group**（連接器群組）。

為了簡化路由並以最快的速度存取資料中心伺服器，*Palo Alto Networks* 建議連接器和伺服器位於同一子網路中。

- **Create**（建立）連接器。

若要讓 *ZTNA* 連接器保持最新，您可以在 ***ZTNA Connector***（***ZTNA*** 連接器） > ***Connector Groups***（連接器群組）中更新其軟體版本圖示，這些圖示會向您顯示連接器的狀態，以及是否有可用的升級。


©2025 Palo Alto Networks, Inc.

**STEP 4 |** 擷取您將用來設定連接器的金鑰和密碼。

在後續步驟中設定 VM 時，您會使用金鑰和密碼值。

1. 自動調整連接器群組—請遵循下列步驟：
   1. 前往 **Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Connector Groups**（連接器群組）。
   2. 在自動調整連接器群組的 **Actions**（動作）區域中選取 **Copy Token**（複製權杖）；然後，複製 **Key**（金鑰）和 **Secret**（密碼）值。

      您可以使用金鑰和密碼，將您建立的雲端執行個體或 VM 與連接器建立關聯。
2. 非自動調整連接器群組—請遵循下列步驟：
   - 選取 **Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Connector**（連接器）。
   - 選取您要部署的連接器。
   - 在 **Actions**（動作）區域中選取 **Copy Token**（複製權杖）；然後，複製 **Key**（金鑰）和 **Secret**（密碼）值。

     您可以使用金鑰和密碼，將您建立的雲端執行個體或 VM 與連接器建立關聯。

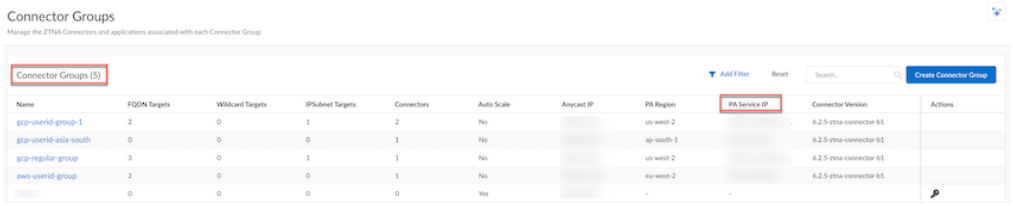



**STEP 5 |** 在您的資料中心部署 ZTNA 連接器 VM。

**STEP 6 |** （選用）選取 **Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Connector Groups**（連接器群組）、記下連接器群組的 **PA Service IP**（**RA** 服務 **IP**），然後將此 IP 位址新增至組織的允許清單。

只有在您裝載連接器之後，才能在 ***Connector Groups***（連接器群組）下看到 ***PA Service IP***（***PA*** 服務 ***IP***）。

如果需要，請將此 IP 位址新增至您的允許清單中，以便您的網路可以傳輸和接收 ZTNA 連接器流量。




 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** 將目標新增至連接器群組。

設定目標以透過 ZTNA 連接器 VM 存取資料中心的私人應用程式。您可以根據 FQDN 萬用字元、FQDN 或 IP 子網路新增目標；ZTNA 連接器負責設定行動使用者和分公司使用者所需的網路和 DNS 設定，以透過 Prisma Access 安全地連線應用程式。

1. 選取 **Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Application Targets**（應用程式目標）。
2. 選取您要建立的目標類型。



透過無提交應用程式裝載增強功能，裝載應用程式現在只需不到一分鐘的時間，從而允許快速存取應用程式。此功能還允許您裝載更多的應用程式。

限制：

- 您無法在多個應用程式目標（具有不同的連接埠/通訊協定）中新增相同的 *FQDN*。
- 當您新增或刪除萬用字元目標時，*MU* 或 *RN* 上會發生提交，以新增或刪除 *DNS Proxy* 轉送規則。不過，後續萬用字元應用程式探索與萬用字元相符的 *FQDN* 時，不需要任何額外的提交，因此，可以快速裝載應用程式，讓您立即存取它們。

若要啟用無提交應用程式裝載功能，請將 *Prisma Access* 資料平面更新至 *11.2.3* 版和更新版本。

- **Wildcard Targets**（萬用字元目標）—使用萬用字元（例如，*.example.com）作為目標。當使用者存取與萬用字元相符的網站時，這些應用程式會自動進行裝載，讓您的行動使用者和遠端網路使用者可透過 ZTNA 連接器存取。例如，假設有 *.example.com 萬用字元，當使用者存取 app1.example.com 中的應用程式時，ZTNA 連接器會自動建立設定，以使用其特定的 FQDN、通訊協定和連接埠來裝載該子應用程式。

  此外，當使用者根據萬用字元（例如，基於 *.example.com 萬用字元的 app1.example.com）存取應用程式時，該應用程式會被發現並自動裝載為 **FQDN Target**（**FQDN** 目標）。

  1. 前往 **Wildcard Targets**（萬用字元目標）和 **Create Wildcard Target**（建立萬用字元目標）。
  2. 輸入目標的唯一 **Name**（名稱）。
  3. 輸入要與目標建立關聯的 **Connector Group**（連接器群組）。

     該群組的類型必須是 **FQDN/Wildcard**（**FQDN/**萬用字元）。

     從 Prisma Access 5.0.1 開始，您可以為萬用字元和 FQDN 目標選取多個連接器群組，每個萬用字元或 FQDN 目標最多可有四個連接器群組。在為每個目標選取多個連接器群組時，請使用指導方針。
  4. 輸入要與目標搭配使用的 **Wildcard**（萬用字元）。

     以 .example.com 或 .my.example.com 格式輸入（UI 會在萬用字元前面隱含地加上星號）。請勿透過指定 *.*、example.*.com 或 *.com 萬用字元來允許所有網站。

 ©2025 Palo Alto Networks, Inc.

5. 選取 **Protocol**（通訊協定）（**tcp**、**udp** 或兩者）。
6. （選用）若要啟用從 GlobalProtect 使用者到 ZTNA 連接器資料中心的 ICMP 通訊協定，請選取 **Allow ICMP Protocol**（允許 **ICMP** 通訊協定）。
7. 選取要用於應用程式的 **Port**（連接埠）。

   輸入單一連接埠、在連接埠之間使用逗號的多個連接埠、使用破折號的連接埠範圍，或兩者。不要在逗號後面加上空格。選取 **Any**（任何）連接埠以比對您指定的任何連接埠，或選取 **Match**（比對）並輸入要比對的一個或多個連接埠。

   如果您在 **Protocol**（通訊協定）下選取了 **both**（兩者），則必須將連接埠新增至 **TCP Port**（**TCL** 連接埠）和 **UDP Port**（**UDP** 連接埠）

   當您在 **Advanced Settings**（進階設定）下的 **TCP Port**（**TCP** 連接埠）欄位中輸入範圍時，**icmp ping** 和 **none**（無） **Probing Type**（探查類型）會啟動。
8. 將 **Probing Type**（探查類型）輸入為 **tcp ping**、**icmp ping** 或 **none**（無），取決於您選取的通訊協定。

   如果選取 **tcp ping**，請選取 **probing port**（探查連接埠），然後輸入單一連接埠。此連接埠不必位於您在 **port**（連接埠）和 **protocol**（通訊協定）區域中輸入的連接埠範圍


©2025 Palo Alto Networks, Inc.

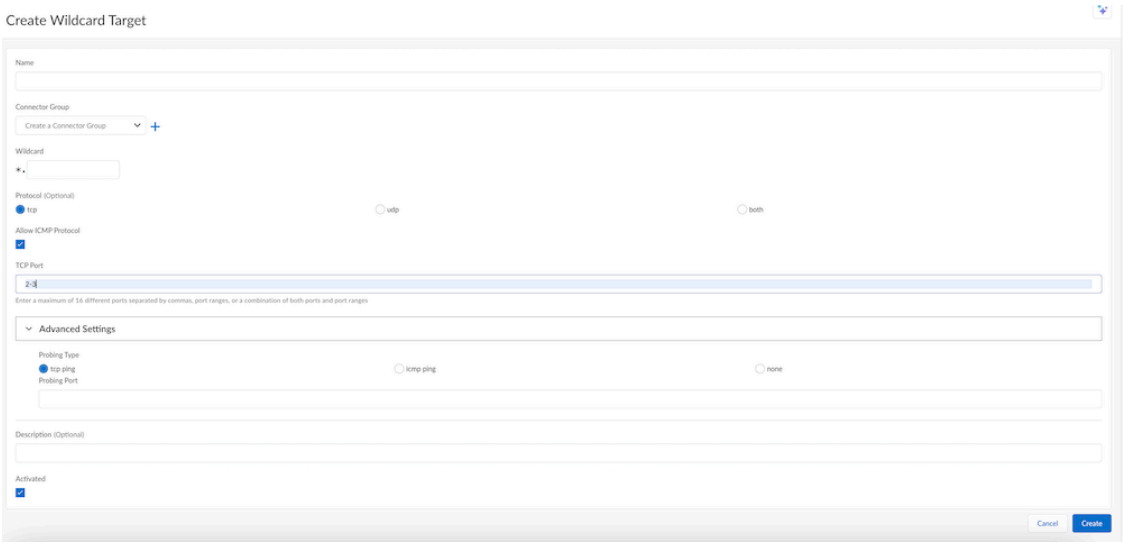
內。ZTNA 連接器透過執行從探查連接埠到 FQDN 已解析 IP 位址的 tcp ping，來確定應用程式的連線性。如果 ping（偵測）成功，則該應用程式會被視為 **Up**（啟動）。

您也可以編輯在應用程式裝載期間新增的探查連接埠。當探查連接埠更新時，ZTNA 連接器會在更新的連接埠上啟動 tcp 探查應用程式，並且應用程式狀態會相應更新。

如果您選取 **icmp ping**，ZTNA 連接器將對 FQDN 已解析 IP 位址執行 ICMP ping。如果收到 ICMP ping 的回應，則應用程式會被視為 **Up**（啟動）。

如果選取 **none**（無），則不會執行任何探查，並且應用程式始終標記為 **Up**（啟動）。

9. 選取 **Activated**（已啟動）並 **Create**（建立）目標。




- **FQDN Targets**（**FQDN** 目標）—若要為單一 FQDN 建立目標，請建立 FQDN 目標。

  從 *Prisma Access 5.0* 開始，對於具有 *5.0* 或更高 *ZTNA* 連接器版本的連接器群組，如果應用程式 *FQDN* 解析為多個私人 *IP* 位址，*ZTNA* 連接器會執行應用程式探查，以確定所有已解析 *IP* 位址的狀態，並對多個已解析 *IP* 位址的 *FQDN* 存取進行負載平衡，而這些位址具有的應用程式狀態為 *[Up*（啟動）*]*。

若要建立 FQDN 目標，請前往 **FQDN Targets**（**FQDN** 目標）和 **Create FQDN Target**（建立 **FQDN** 目標）。您建立 FQDN 目標的方式與建立 FQDN 萬用字元相同，以單一 FQDN 取代 FQDN 萬用字元。

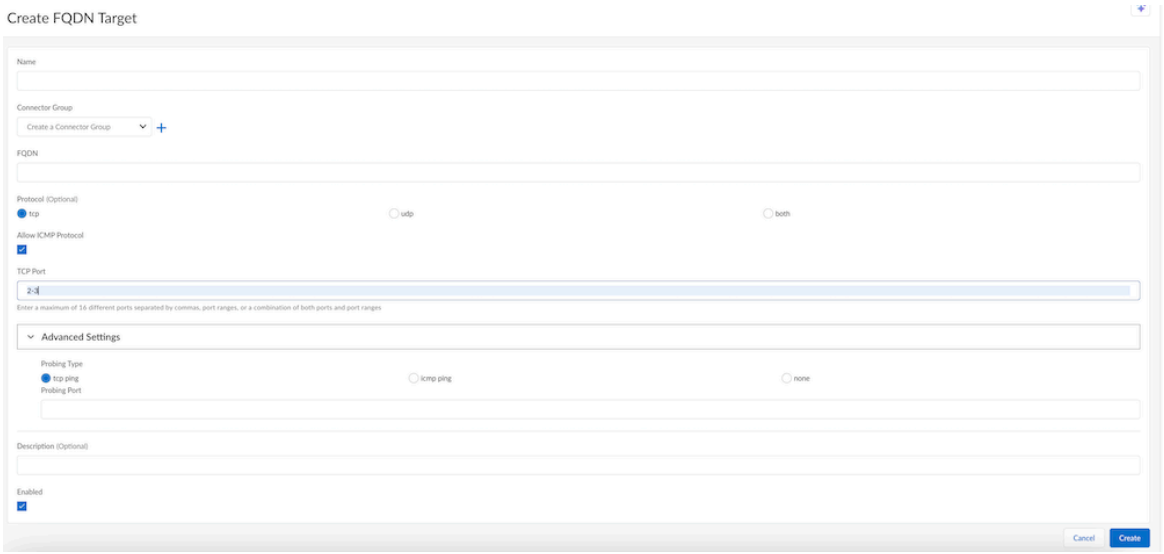
從 Prisma Access 5.0.1 開始，您可以為每個 FQDN 目標以及萬用字元目標選取多個連接器群組，每個 FQDN 或萬用字元目標最多可有四個連接器群組。在為每個目標設定多個連接器群組時，請使用指導方針。

由於萬用字元目標而發現的應用程式也會顯示在這裡。當使用者存取與萬用字元相符的網站時，這些應用程式會自動進行裝載，讓您的行動使用者和遠端網路使用者可透過 ZTNA


©2025 Palo Alto Networks, Inc.

連接器存取。例如，假如有 *.example.com 萬用字元，當使用者存取 app1.example.com 上的應用程式時，ZTNA 連接器會自動將該應用程式新增至 FQDN 目標清單。

從父萬用字元目標探索 FQDN 應用程式之後，對萬用字元目標的任何變更都不會在已探索的應用程式中更新。此外，不會重新探索相同的已探索 FQDN。如果已探索 FQDN 應用程式的特性需要更新，請使用下列步驟，對已探索的應用程式執行手動更新。




- **IP Subnet**（**IP** 子網路）—建立 IP 子網路型目標，以根據 IP 子網路而不是 FQDN 尋找應用程式。

  1. 前往 **IP Subnets**（**IP** 子網路）並 **Create Subnet Rule**（建立子網路規則）。
  2. 輸入目標的唯一 **Name**（名稱）。
  3. 輸入要與目標建立關聯的 **Connector Group**（連接器群組）。

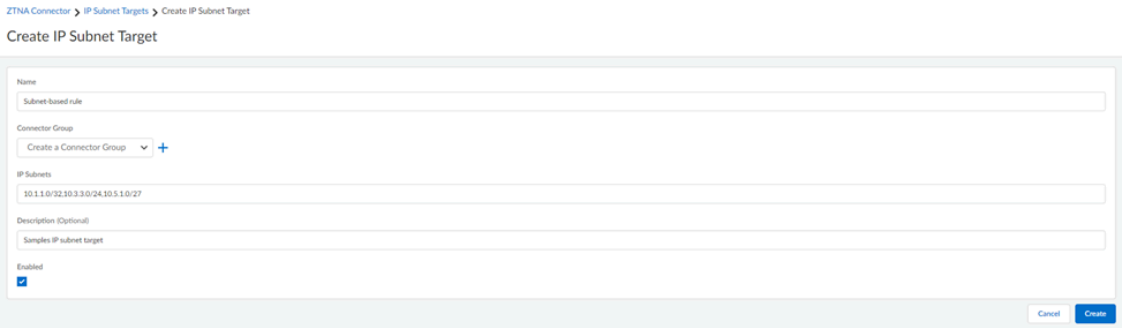
     該群組的類型必須是 **IP Subnet**（**IP** 子網路）。
  4. 指定資料中心 **IP Subnets**（**IP** 子網路），群組中的連接器會提供對這些子網路的 IP 路由存取。

     群組中的所有連接器都會提供對所指定 IP 子網路的路由存取。您可以選取 10.1.1.1/32 形式的單一 IP 位址、單一子網路或以逗號分隔的多個子網路。最多可輸入 16 個子網路。

     IP 子網路必須可在租用戶的 IP 網狀架構內路由，且 IP 子網路無法與租用戶中的任何其他 IP 子網路重疊，包括：

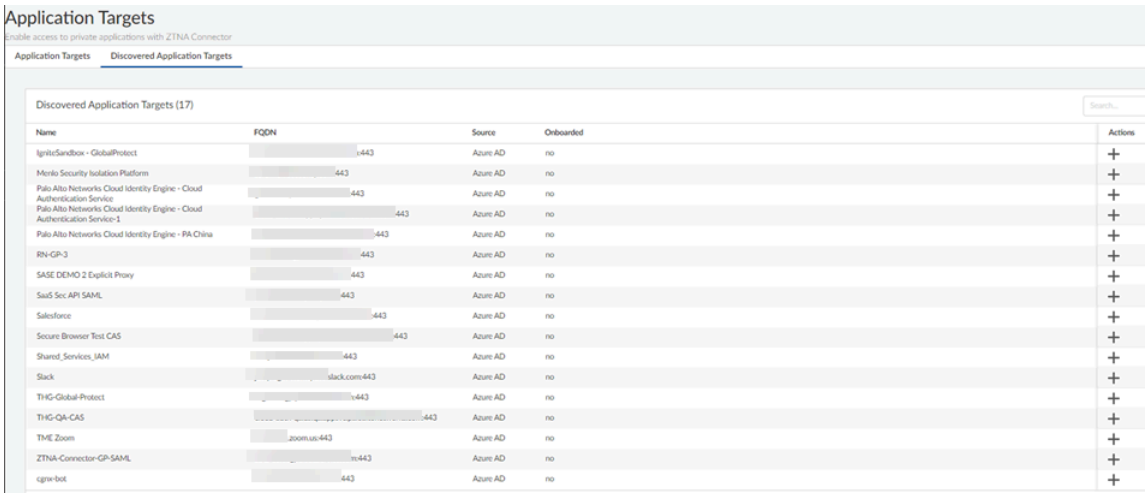
     - 其他 IP 可路由子網路，包括使用者在 Panorama 上設定的靜態路由、從分支公告至遠端網路的路由，或從資料中心公告至服務連線的路由。
     - ZTNA FQDN 應用程式 IP 子網路
     - ZTNA 連接器 IP 子網路
     - 基礎結構子網路 IP 位址
     - 行動使用者用戶—GlobalProtect IP 位址集區
  5. 選取 **Activated**（已啟動）並 **Create**（建立）目標。


©2025 Palo Alto Networks, Inc.




**STEP 8 |** 將 ZTNA 連接器自動探索的應用程式新增至連接器群組。

1. 使用雲端識別引擎設定應用程式的自動探索
2. 選取 **Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Application Targets**（應用程式目標） > **Discovered Application Targets**（已探索的應用程式目標）。




3. 按一下 **Actions**（動作） 下的 + 將應用程式新增至連接器群組。
4. 給與應用程式唯一的 **Name**（名稱）。
5. 選取要與應用程式建立關聯的 **ZTNA Connector Group**（**ZTNA** 連接器群組）。
6. 輸入 **Probing Type**（探查類型）（**tcp ping**、**icmp ping**或 **none**（無））。
   - 如果選取 **tcp ping**，則也會選取 **probing port**（探查連接埠）。此連接埠不必位於您在 **port**（連接埠）和 **protocol**（通訊協定）區域中輸入的連接埠範圍內。如果您選取

 ©2025 Palo Alto Networks, Inc.

**tcp ping** 作為探查類型，Palo Alto Networks 建議您使用相同的連接埠作為 **probing port**（探查連接埠）。

ZTNA 連接器透過執行從探查連接埠到 FQDN 已解析 IP 位址的 tcp ping，來確定應用程式的連線性。如果 ping（偵測）成功，則應用程式會被視為 **Up**（啟動）。

- 您也可以編輯在應用程式裝載期間所新增的探查連接埠。當探查連接埠更新時，ZTNA 連接器會在更新的連接埠上啟動 tcp 探查應用程式，並且應用程式狀態會相應更新。
- 如果您選取 **icmp ping**，ZTNA 連接器會對 FQDN 執行 ICMP ping。如果收到 ICMP ping 的回應，ZTNA 連接器會將應用程式的狀態設定為 **Up**（啟動）。
- 如果選取 **none**（無），則不會執行任何探查，並且應用程式始終標記為 **Up**（啟動）。

7. 選取 **Enabled**（已啟用）。
8. **Create**（建立） 應用程式目標。

**STEP 9 |** 建立安全性政策規則，以允許使用者存取連接器中的應用程式。

**STEP 10 |** （選用）檢視和監控 ZTNA 連接器，以查看 ZTNA 連接器和連接器群組的執行方式。

**STEP 11 |** （選用）如果您在使用 ZTNA 連接器存取私人應用程式時遇到問題，請使用 ping、traceroute 和 nslookup 診斷工具檢查應用程式的連線性。

# 升級 ZTNA 連接器

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 4.0<br>❑ ZTNA 連接器附加元件授權<br>具有附加元件授權的基本授權包括 8 個 ZTNA 連接器、100 個 FQDN 和 4 個 IP 子網路功能。<br>具有附加元件授權的進階授權包括 40 個 ZTNA 連接器、300 個 FQDN 和 1024 個 IP 子網路功能。<br>具有附加元件授權的高級授權包括 200 個 ZTNA 連接器、4000 個 FQDN 和 1024 個 IP 子網路功能。<br>❑ 如果您未購買 ZTNA 連接器附加元件授權，Prisma Access 授權包括四個連接器、40 個 FQDN 和四個 IP 子網路。提供此功能的目的旨在您的環境中試用 ZTNA 連接器。 |

若要保持 ZTNA 連接器的最新狀態，您可以更新其軟體版本。您可能還需要升級您的連接器以支援新功能。


©2025 Palo Alto Networks, Inc.

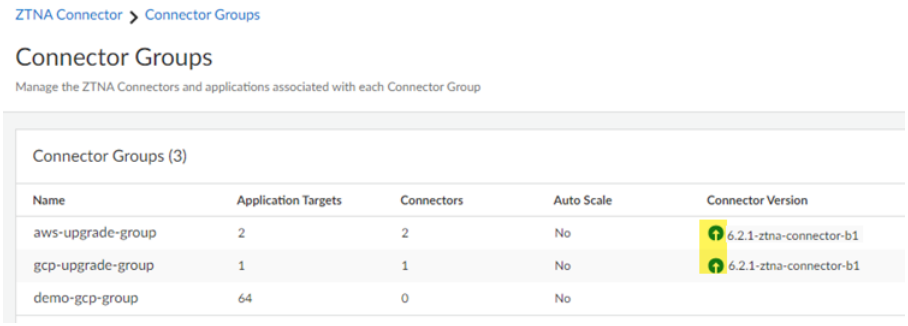
當新的 ZTNA 連接器版本發行時，您部署中的連接器會進行檢查，如果發行的版本比現有版本更新，或者如果群組中的所有連接器不在相同版本上，則 [Connector Group（連接器群組）] 區域中的圖示會顯示有更新可用。如果您選擇更新連接器，則會給您一個選項來升級整個群組。升級一個群組會自動平行升級該群組中的所有連接器。您無法升級個別連接器。

*ZTNA 連接器升級大約需要 8 到 10 分鐘，並且在此過程中連接器會重新啟動。Palo Alto Networks 建議您在停機期間或排程的網路中斷期間排程連接器升級。*

**STEP 1 |** 前往 **ZTNA Connector**（**ZTNA 連接器**） > **Connector Groups**（連接器群組）。綠色箭頭表示有可用的升級。

您只能升級到適用於租用戶的最新映像版本。

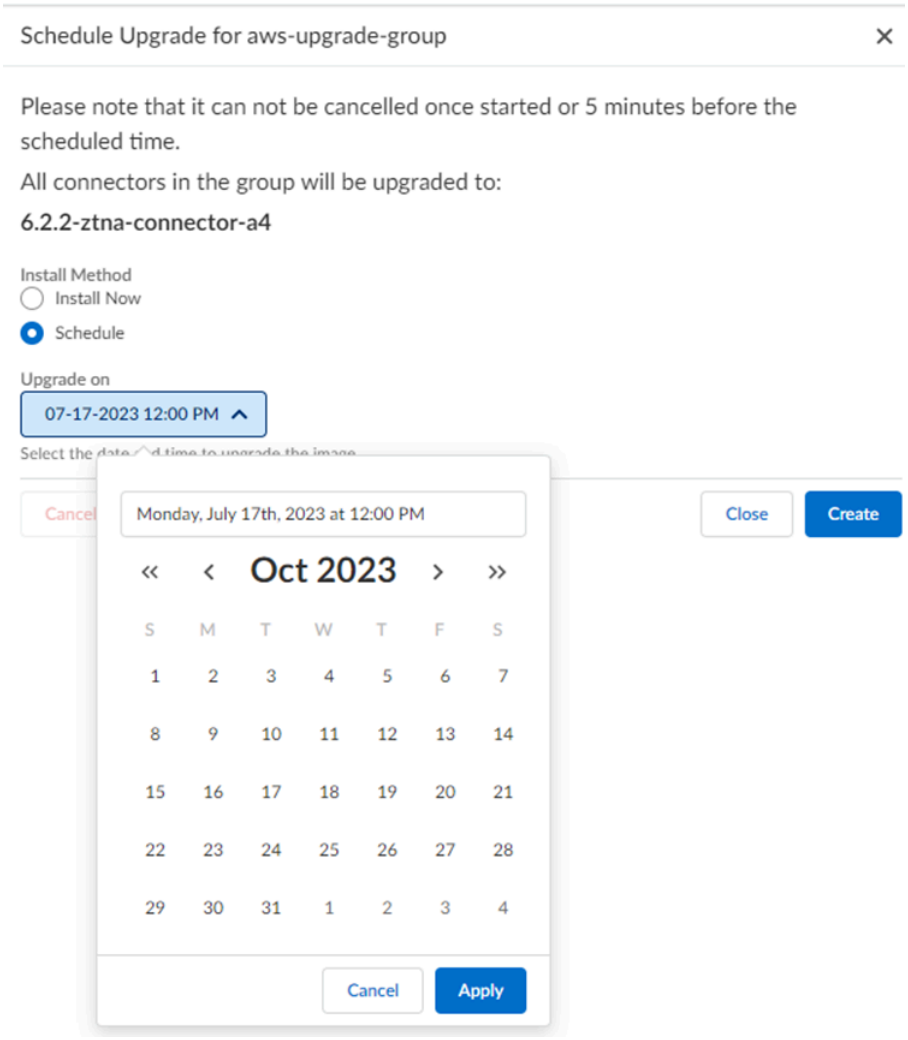
**STEP 2 |** 按一下連接器群組旁邊的綠色箭頭。




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 選取 **Install Now**（立即安裝），以立即升級連接器群組，或**Schedule**（排程）並提供升級的時間和日期。顯示的時間是使用 ZTNA UI 的管理員的當地時區。

您可以在升級開始前最多五分鐘內 **Cancel Scheduled Upgrade**（取消排程升級）。




**STEP 4 |** 檢視 **Connector Version**（連接器版本）下的圖示來檢查連接器的狀態。

| 圖示 | 說明 |
|---|---|
|  | 有升級可用。 |
|  | 升級已排程。 |
|  | 升級已開始且進行中。 |


©2025 Palo Alto Networks, Inc.

| 圖示 | 說明 |
| --- | --- |
| 無圖示（僅顯示連接器版本）<br>6.1.1-ztna-connector-a8 | 升級成功。 |
|  | 並非所有的連接器都已升級。 |
|  | 升級失敗。 |

## ZTNA 連接器診斷工具

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 4.0<br>❑ ZTNA 連接器附加元件授權<br>具有附加元件授權的基本授權包括 8 個 ZTNA 連接器、100 個 FQDN 和 4 個 IP 子網路功能。<br>具有附加元件授權的進階授權包括 40 個 ZTNA 連接器、300 個 FQDN 和 1024 個 IP 子網路功能。<br>具有附加元件授權的高級授權包括 200 個 ZTNA 連接器、4000 個 FQDN 和 1024 個 IP 子網路功能。<br>❑ 如果您未購買 ZTNA 連接器附加元件授權，Prisma Access 授權包括四個連接器、40 個 FQDN 和四個 IP 子網路。提供此功能的目的旨在您的環境中試用 ZTNA 連接器。 |

如果您在使用 ZTNA 連接器存取私人應用程式時遇到問題，則可以使用下列網路工具，從 ZTNA 連接器 UI 執行測試來協助您找出問題：

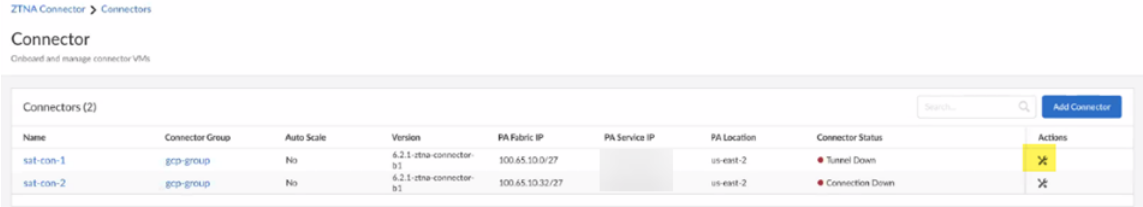
- ping
- TCP Ping
- traceroute
- nslookup
- 傾印概要
- 您也可以獲得封包擷取來協助確定 ZTNA 連接器出現任何問題的原因。

 ©2025 Palo Alto Networks, Inc.

在使用 *ping* 和 *traceroute* 工具之前，請確保您的網路允許 *ICMP*。出於安全考慮，某些雲端環境不允許 *ICMP*，且這些工具不會顯示任何活動。

**STEP 1 |** 前往 **Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Connector**（連接器）。

**STEP 2 |** 為連接器選取 **Actions**（動作） > **Diagnostics**（診斷）。



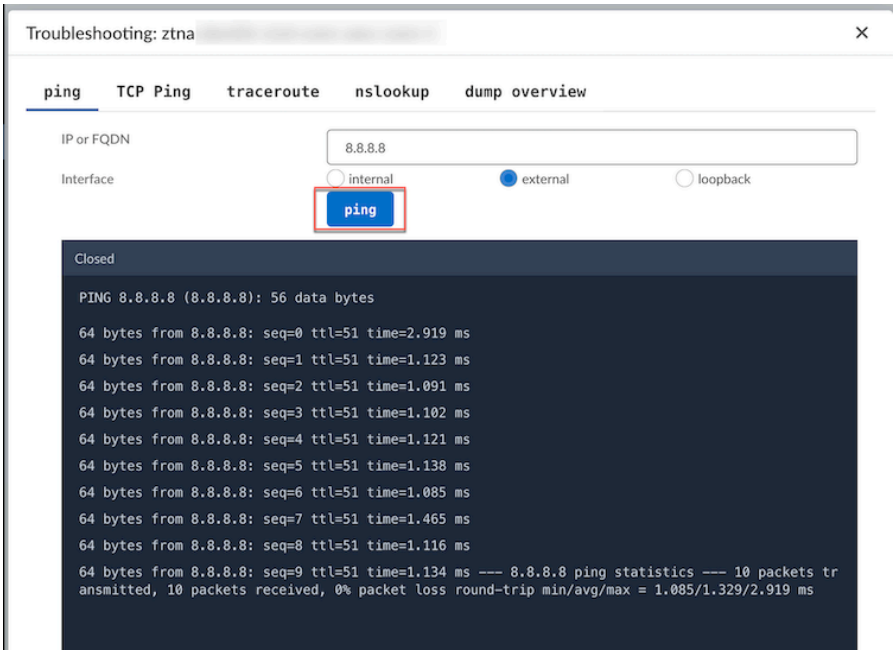

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 執行 ping、TCP Ping、traceroute 或 nslookup 診斷工具。

- **ping**：
  1. 選取您嘗試存取的應用程式的 **IP or FQDN**（**IP** 或 **FQDN**）。
  2. 選取您要從中測試 ping 的 **interface**（介面）。

     如果您已設定 VM 進行雙臂部署，請選取 **internal**（內部），以檢查 VM 的 LAN 端（連接埠 2），並選取 **external**（外部）以檢查 WAN 端（連接埠 1）。

     對於單臂部署，選擇 **internal**（內部）或 **external**（外部），因為 WAN 和 LAN 端都會對應到連接埠 1。
  3. 選取 **ping**。

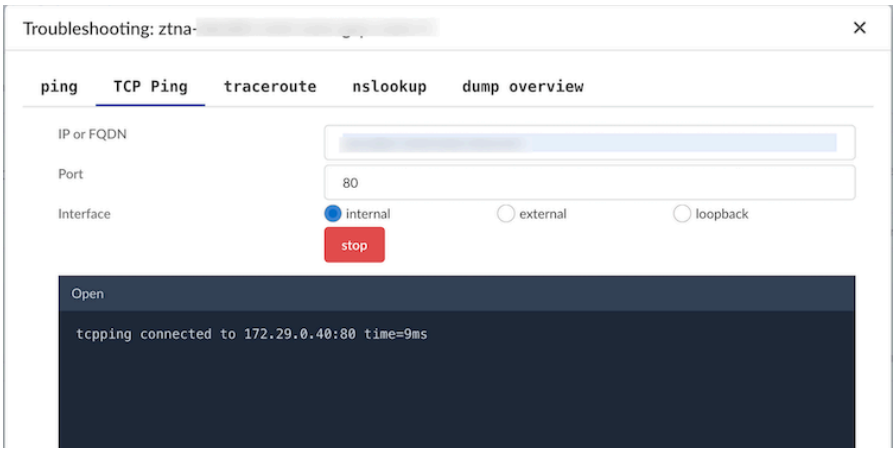
     即會顯示 ping 輸出。
  4. 若要完成測試，請 **Stop**（停止）。
- **TCP Ping**：

  將連接器升級到 *ZTNA* 連接器 *6.2.5-b1* 版本。如果連接器未使用此版本保持最新狀態，則 *Strata Cloud Manager UI* 將不會提供 ***TCP Ping*** 作為診斷工具。

  1. 選取您嘗試存取的應用程式的 **IP or FQDN**（**IP** 或 **FQDN**）。
  2. 選取您要從中測試 ping 的 **interface**（介面）。

     如果您已設定 VM 進行雙臂部署，請選取 **internal**（內部），以檢查 VM 的 LAN 端（連接埠 2），並選取 **external**（外部）以檢查 WAN 端（連接埠 1）。
  3. 選取 **TCP Ping**。

 ©2025 Palo Alto Networks, Inc.

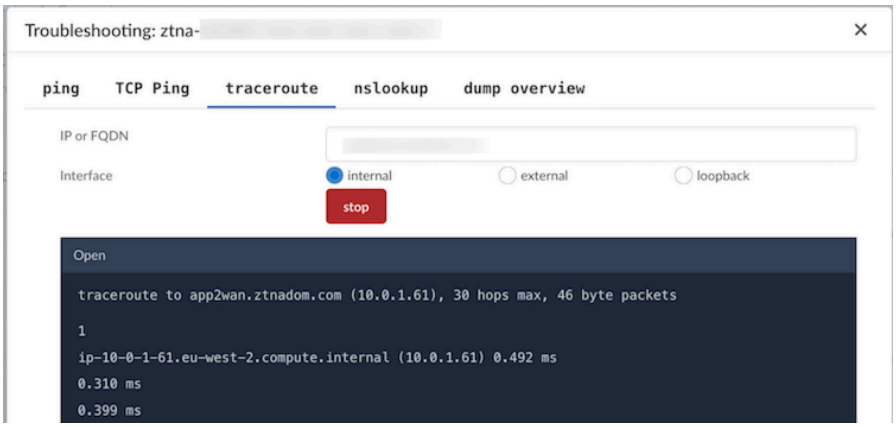



4. 若要完成測試，請 **Stop**（停止）。

- **traceroute**：

1. 選取您嘗試存取的應用程式的 **IP or FQDN**（**IP** 或 **FQDN**）。
2. 選取您要從中測試 ping 的 **interface**（介面）。

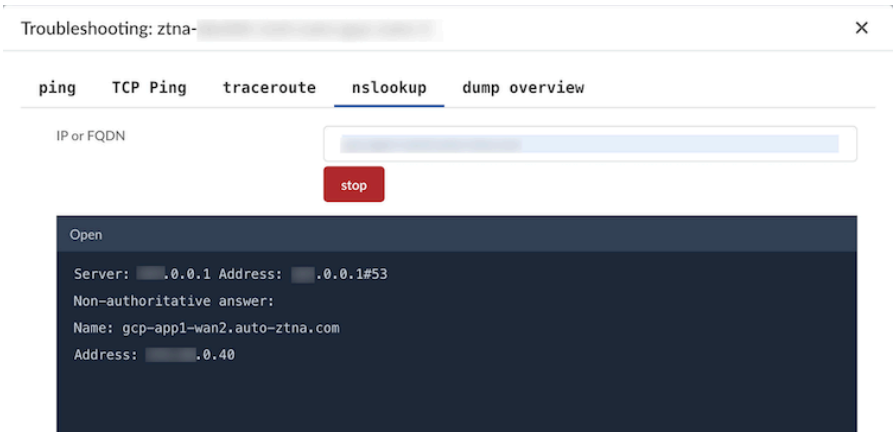
   如果您已設定 VM 進行雙臂部署，請選取 **internal**（內部），以檢查 VM 的 LAN 端（連接埠 2），並選取 **external**（外部）以檢查 WAN 端（連接埠 1）。
3. 選取 **traceroute**。
4. 若要完成測試，請 **Stop**（停止）。




- **nslookup**：

1. 選取您嘗試存取的應用程式的 **IP or FQDN**（**IP** 或 **FQDN**）。
2. 選取 **nslookup**。
3. 若要完成測試，請 **Stop**（停止）。

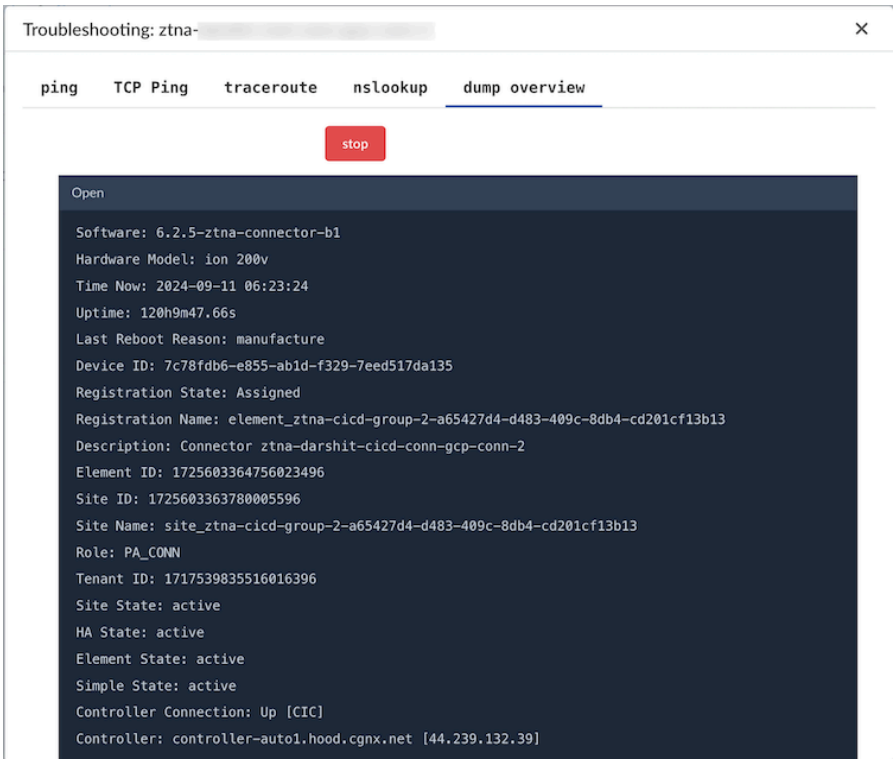
 ©2025 Palo Alto Networks, Inc.




- 傾印概要：

  1. 按一下 **Start**（開始）以下載系統傾印，或按一下 **Stop**（停止） 將其停止。

     傾印概要提供 PANW 疑難排解所需的軟體版本、介面和連線狀態，以及連接器識別資訊。




## 獲得封包擷取

如果您需要封包擷取來進行網路層級疑難排解，您可以獲得封包擷取，從特定連接器擷取網路資料。您也可以根據特定的 IP 位址或通訊協定（例如 TCP）擷取封包。

獲得封包擷取在以下使用案例中非常有用：

- 如果你的通道沒有出現。擷取連接器與 ZTT 之間的 IKE 交涉將有助於確定問題。在這種情況下，選取 **Internet**（網際網路）介面，並使用服務連線的 IP 位址作為來源或目的地介面。

 ©2025 Palo Alto Networks, Inc.

- 如果您的應用程式失效，您可以使用伺服器 IP 位址和連接埠，以及資料中心介面上的連接埠取得 tcpdump，來檢查應用程式的探查情況。
- 如果端對端資料平面無法運作，但通道是應用程式且應用程式已啟動。在此使用案例中，取得 IPsec 通道上前往應用程式網狀架構 IP 位址的使用者流量的 tcpdump 將很有幫助。

**STEP 1 |** 前往 **Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Connector**（連接器）。

**STEP 2 |** 為要疑難排解的連接器選取 **packet capture**（封包擷取）（放大鏡）。




**STEP 3 |** 選取將擷取封包的介面（**internal**（內部）、**external**（外部）或 **tunnel**（通道））。

**STEP 4 |** （選用）指定從中擷取封包的 **Source or Destination IPv4**（來源或目的地 **IPv4**）位址。

如果指定此選項，則僅擷取來自此 IP 位址的封包。

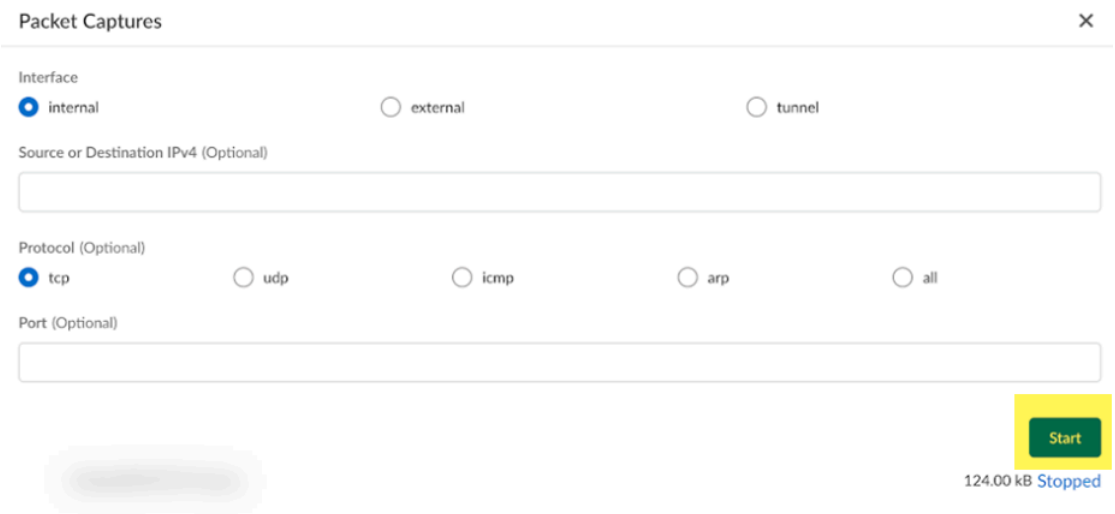
**STEP 5 |** （選用）選取要擷取的封包類型。

您可以選取要擷取的特定通訊協定封包（**tcp**、**udp**、**icmp** 或 **arp**），或選取 **all** 以擷取所有封包。

**STEP 6 |** （選用）選取將從中擷取封包的 **Port**（連接埠）。

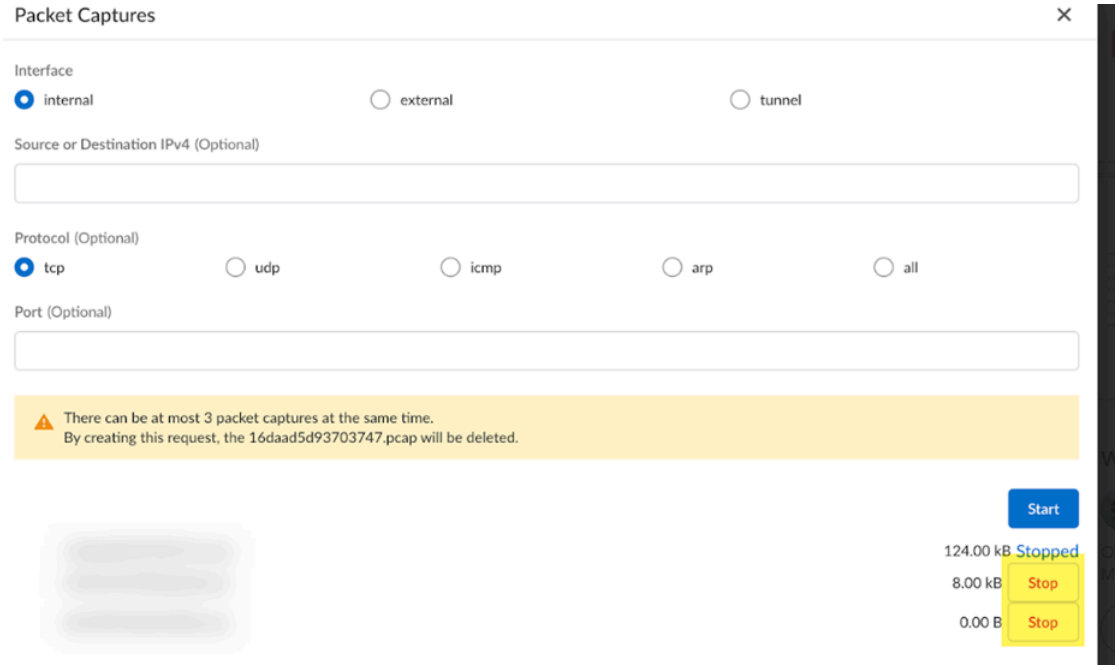
如果指定此選項，則僅擷取來自此連接埠的封包。

**STEP 7 |** **Start**（開始）封包擷取。




 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** 若要停止封包擷取，請按一下 **Stop**（停止）。



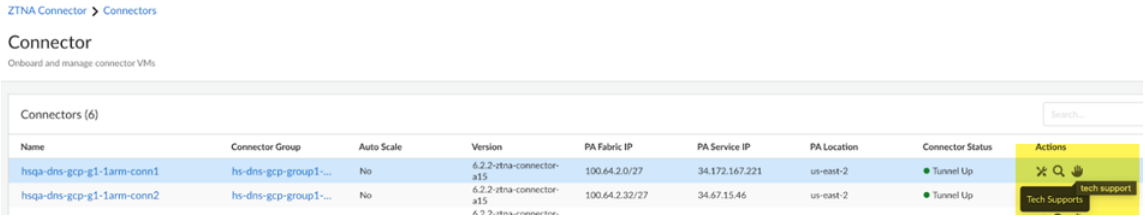

- 封包擷取的檔案大小上限為 5 MB。如果在達到大小上限之前未停止擷取，則會覆寫檔案。
- 連接器上允許最多同時擷取三個封包。如果啟動第四個工作階段，則會終止第一個執行中的工作階段。

## 建立技術支援檔案

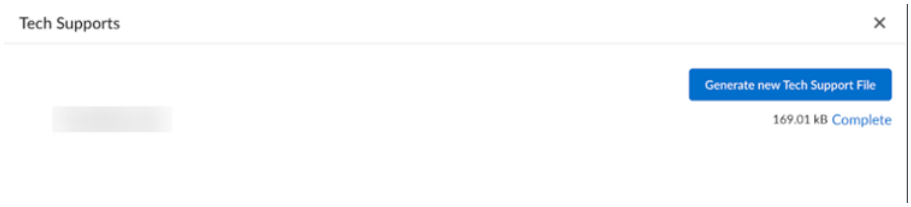
技術支援文件包含您的裝置設定、系統資訊和一些日誌（不是流量）。Palo Alto Networks 可以要求您上傳技術支援檔案，以協助針對 ZTNA 連接器問題進行疑難排解。

**STEP 1 |** 前往 **Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Connector**（連接器）。

**STEP 2 |** 為您要針對其進行疑難排解的連接器選取 **tech support**（技術支援）（手）。




**STEP 3 |** **Generate new Tech Support File**（產生新的技術支援檔案）。




**STEP 4 |** 選取 **Complete**（完成）以將技術支援檔案下載到本機。


©2025 Palo Alto Networks, Inc.

# 刪除連接器 IP 區塊

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 4.0<br>❑ ZTNA 連接器附加元件授權<br>具有附加元件授權的基本授權包括 8 個 ZTNA 連接器、100 個 FQDN 和 4 個 IP 子網路功能。<br>具有附加元件授權的進階授權包括 40 個 ZTNA 連接器、300 個 FQDN 和 1024 個 IP 子網路功能。<br>具有附加元件授權的高級授權包括 200 個 ZTNA 連接器、4000 個 FQDN 和 1024 個 IP 子網路功能。<br>❑ 如果您未購買 ZTNA 連接器附加元件授權，Prisma Access 授權包括四個連接器、40 個 FQDN 和四個 IP 子網路。提供此功能的目的旨在您的環境中試用 ZTNA 連接器。 |

您 啟用 ZTNA 連接器 並新增所需的連接器 IP 區塊，Prisma Access 將在內部使用這些區塊，在行動使用者、遠端網路和資料中心的連接器 VM 之間路由流量。以前，在建立連接器 IP 區塊之後，您無法對其進行任何變更。不過，現在您可以刪除或更新 **Connector IP Blocks**（連接器 **IP** 區塊）。請遵循上述程序刪除或更新這些區塊。

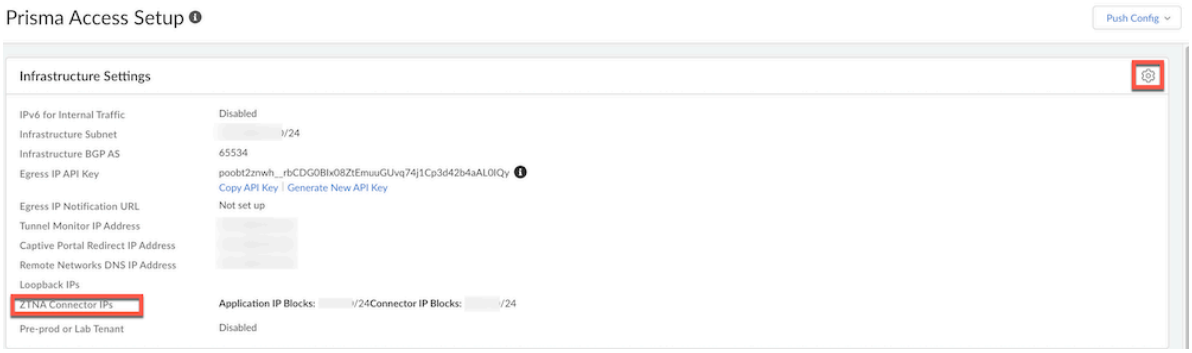
- Panorama
- Strata Cloud Manager

## 刪除連接器 IP 區塊（雲端管理）

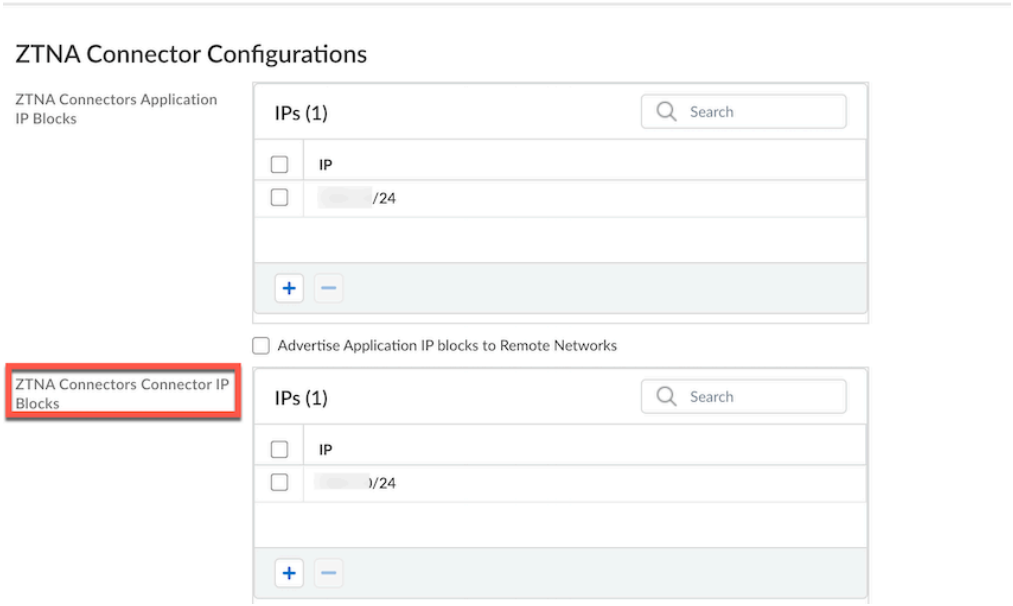
完成下列程序以刪除連接器 IP 區塊。


©2025 Palo Alto Networks, Inc.

**STEP 1 |** 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Prisma Access** > **Infrastructure Settings**（基礎結構設定），然後按一下齒輪以編輯 **Settings**（設定）。



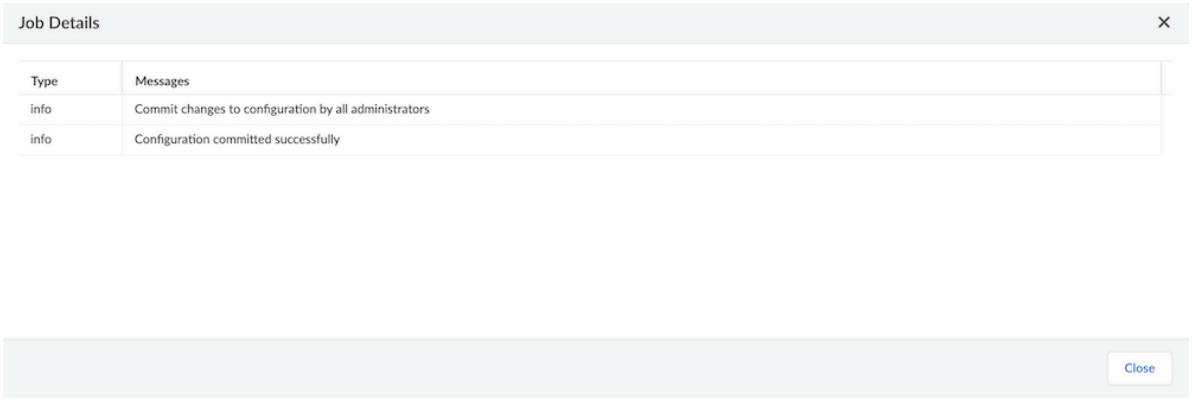

**STEP 2 |** 從 **ZTNA Connector Configurations**（**ZTNA** 連接器設定） > **ZTNA Connectors Connector IP Blocks**（**ZTNA** 連接器連接器 **IP** 區塊）中，選取要刪除的連接器區塊旁邊的核取方塊，然後按一下 **Save**（儲存）。




 ©2025 Palo Alto Networks, Inc.

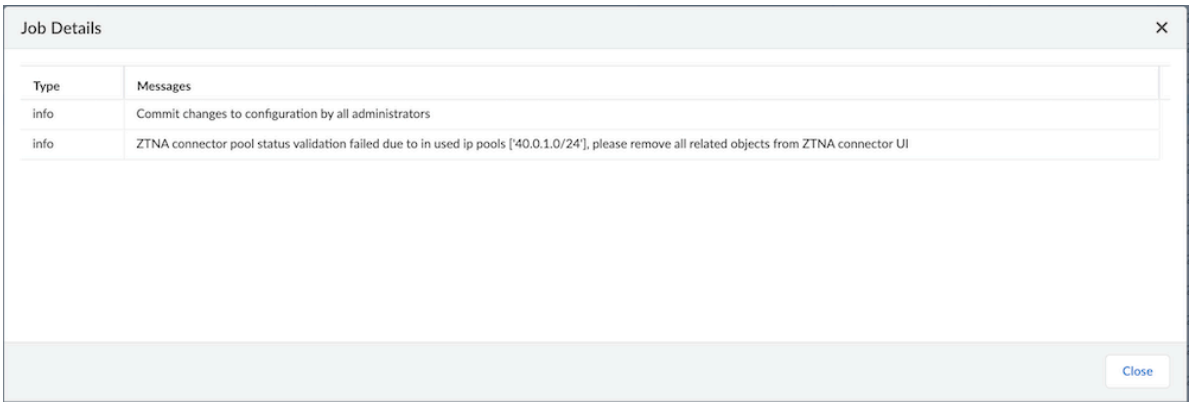
**STEP 3 |** **Commit**（提交）並推送設定變更。

提交通過後會出現一則訊息。




如果您已建立任何 ZTNA 連接器物件（例如連接器、應用程式、萬用字元和連接器群組），並且在未先刪除 ZTNA 連接器物件的情況下嘗試刪除 **Connector IP Block**（連接器 **IP** 區塊），則提交並推送會失敗。

在此情況下，刪除 連接器物件、刪除所需的 **Connector IP Block**（連接器 **IP** 區塊），然後 **Commit**（提交）。第一次提交失敗，但第二次通過。

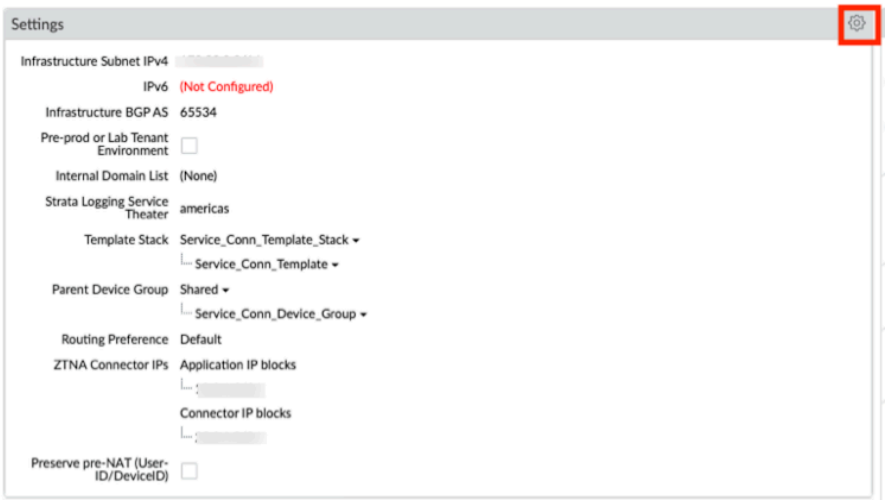



## 刪除連接器 IP 區塊 (Panorama)

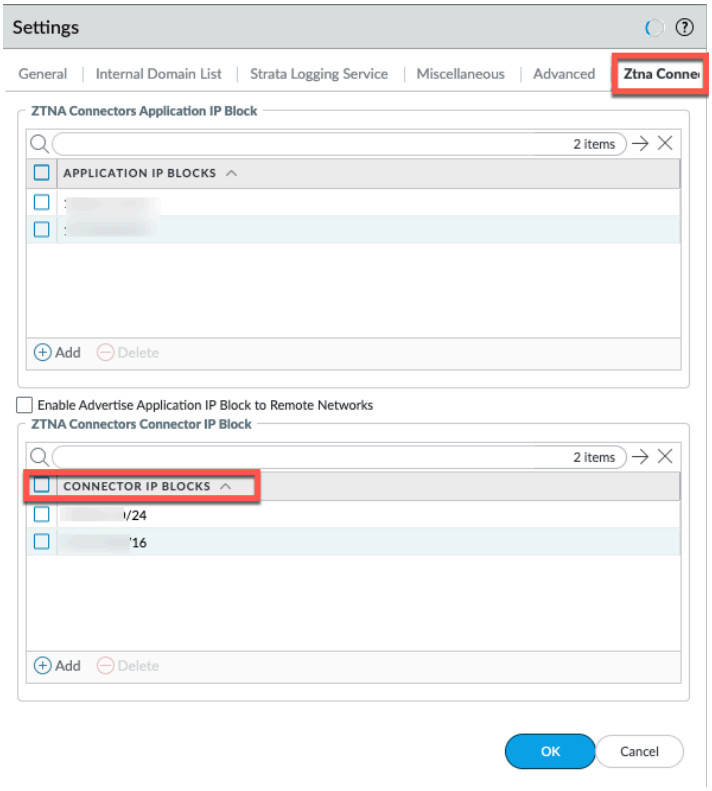
完成下列程序以刪除連接器 IP 區塊。


©2025 Palo Alto Networks, Inc.

**STEP 1 |** 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定），然後按一下齒輪以編輯 **Settings**（設定）。




**STEP 2 |** 選取 **Ztna Connector**（**Ztna** 連接器）。

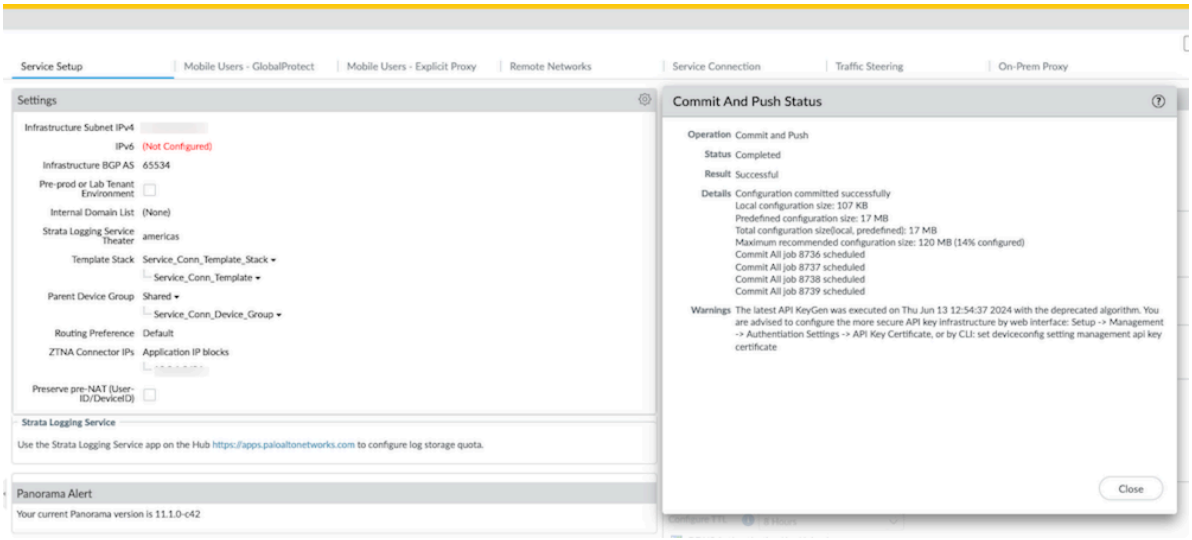



**STEP 3 |** 選取要刪除的連接器區塊旁邊的核取方塊，然後按一下 **OK**（確定）以儲存設定。


©2025 Palo Alto Networks, Inc.

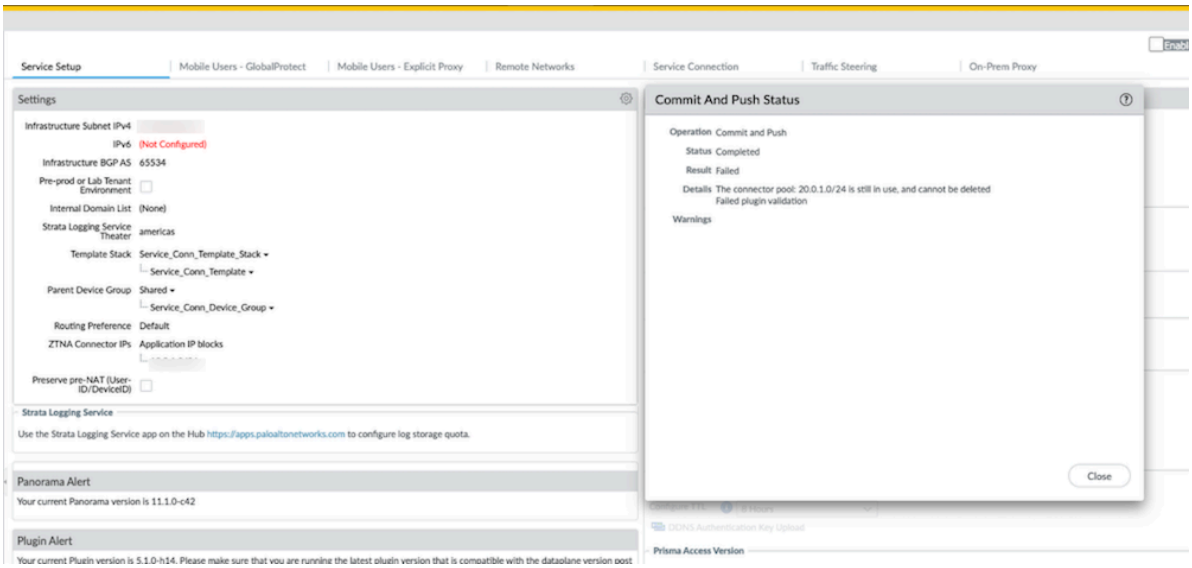
**STEP 4 |** 選取 **Commit**（提交）並推送設定變更。

提交通過後會出現一則訊息。




如果您先前已建立任何 ZTNA 連接器物件（例如連接器、應用程式、萬用字元和連接器群組），並在未刪除 ZTNA 連接器物件的情況下嘗試刪除 **Connector IP Block**（連接器 **IP** 區塊），則提交並推送會失敗。

在此情況下，刪除 連接器物件、刪除所需的 **Connector IP Block**（連接器 **IP** 區塊），然後 **Commit**（提交）並推送兩次。第一次提交失敗，但第二次通過。




 ©2025 Palo Alto Networks, Inc.

# 使用雲端識別引擎設定應用程式的自動探索

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 4.0<br>❑ ZTNA 連接器附加元件授權<br>具有附加元件授權的基本授權包括 8 個 ZTNA 連接器、100 個 FQDN 和 4 個 IP 子網路功能。<br>具有附加元件授權的進階授權包括 40 個 ZTNA 連接器、300 個 FQDN 和 1024 個 IP 子網路功能。<br>具有附加元件授權的高級授權包括 200 個 ZTNA 連接器、4000 個 FQDN 和 1024 個 IP 子網路功能。<br>❑ 如果您未購買 ZTNA 連接器附加元件授權，Prisma Access 授權包括四個連接器、40 個 FQDN 和四個 IP 子網路。提供此功能的目的旨在您的環境中試用 ZTNA 連接器。 |

為了讓 ZTNA 連接器自動探索定義在 Azure Active Directory 或 Okta 目錄中的應用程式，您必須設定以下內容：

- ❑ 在中樞啟動雲端識別引擎，並建立您的第一個租用戶。

  當您在 Azure 或 Okta 中設定雲端型目錄時，必須選取 **Collect enterprise applications**（收集企業應用程式）。
- ❑ 選取您想要雲端識別引擎存取的目錄類型。
- ❑ 設定雲端型目錄，例如 Azure Active Directory (Azure AD) 或 Okta 目錄，以與雲端識別引擎通訊。

支援以下 IdP 與應用程式探索搭配使用：

- Azure AD
- Okta

 ©2025 Palo Alto Networks, Inc.

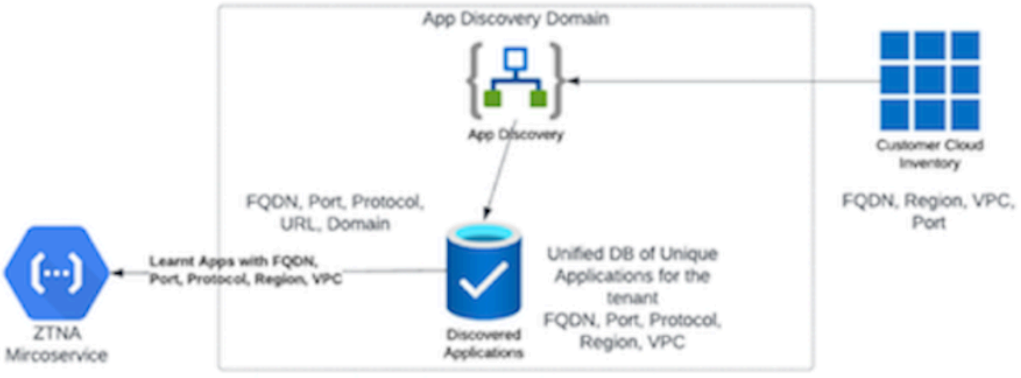
# 私人應用程式目標探索

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 4.0<br>❑ ZTNA 連接器附加元件授權<br>具有附加元件授權的基本授權包括 8 個 ZTNA 連接器、100 個 FQDN 和 4 個 IP 子網路功能。<br>具有附加元件授權的進階授權包括 40 個 ZTNA 連接器、300 個 FQDN 和 1024 個 IP 子網路功能。<br>具有附加元件授權的高級授權包括 200 個 ZTNA 連接器、4000 個 FQDN 和 1024 個 IP 子網路功能。<br>❑ 如果您未購買 ZTNA 連接器附加元件授權，Prisma Access 授權包括四個連接器、40 個 FQDN 和四個 IP 子網路。提供此功能的目的旨在您的環境中試用 ZTNA 連接器。 |

在現代網路基礎結構中，數千個私人應用程式會進行內部部署，以及部署在多雲端資料中心。網路團隊並不知道其網路中或網路中特定子網路內執行的應用程式，導致缺少應用程式可視性。

若要提供對應用程式的安全存取，您必須手動輸入 FQDN、連接埠、應用程式，並知道該應用程式對其他應用程式的相依性。

私人應用程式目標探索提供了一種方式，探索雲端環境中托管的應用程式，並允許這些應用程式裝載在 ZTNA 連接器解決方案上。它也會連線到雲端提供者網路、執行探索，並將其儲存在資料庫中。它還將 API 提供給不同的服務，以取得已探索的應用程式。如果使用者只有服務連線，而不是 ZTNA 連接器，則僅會探索應用程式目標。




私人應用程式目標探索識別：


©2025 Palo Alto Networks, Inc.

- FQDN
- 應用程式的連接埠
- 應用程式的通訊協定

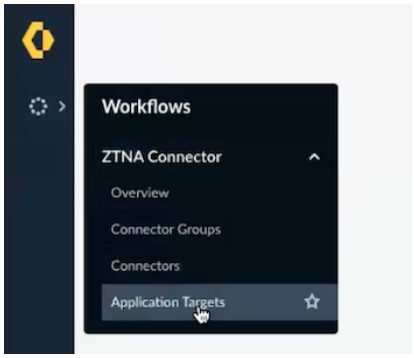
請確保在啟用私人應用程式探索功能之前，先啟動雲端識別引擎 *(CIE)*。

完成以下步驟以新增雲端帳戶、AWS 中的 IAM 角色，並探索目標應用程式。

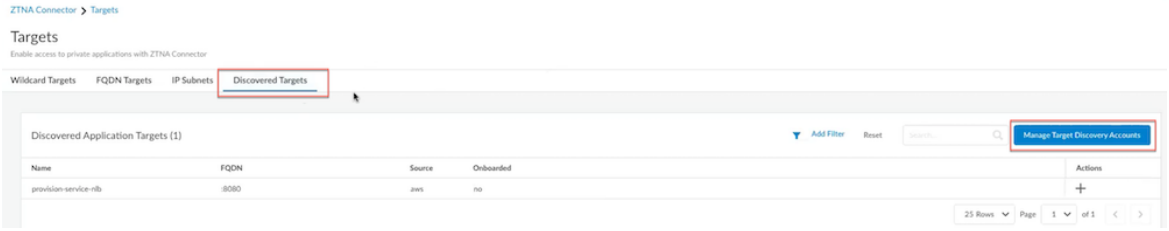

©2025 Palo Alto Networks, Inc.

**STEP 1 |** 取得 CloudFormation 範本 (CFT) 以新增雲端帳戶。

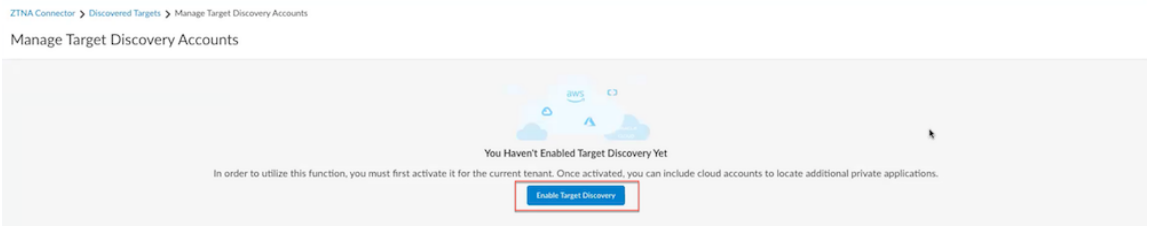
1. 導覽至 **Application Targets**（應用程式目標）（**Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Application Targets**（應用程式目標））。



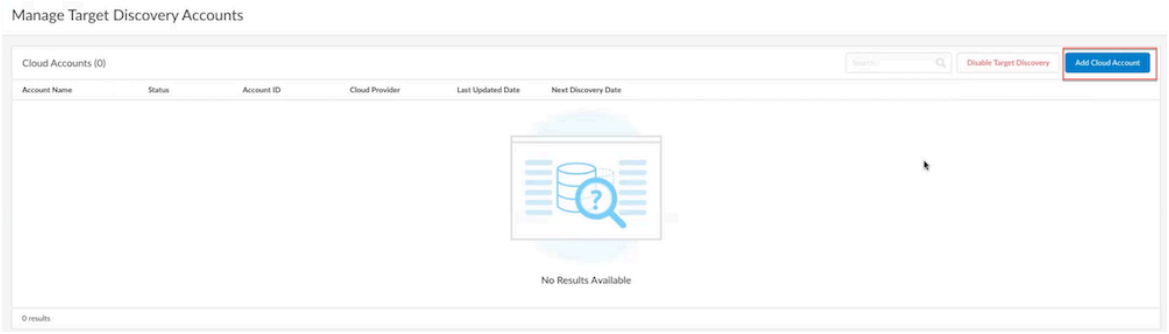

2. 在 **Application Targets**（應用程式目標）頁面上，選取 **Discovered Targets**（探索的目標），然後選取 **Manage Target Discovery Accounts**（管理目標探索帳戶）。




3. 選取 **Enable Target Discovery**（啟用目標探索），然後選取 **Enable**（啟用）。

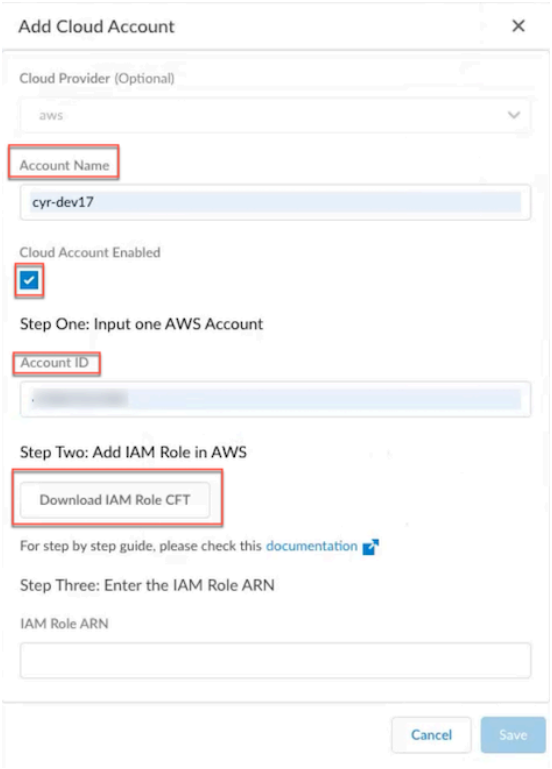



4. 在 **Manage Target Discovery Accounts**（管理目標探索帳戶）頁面上，選取 **Add Cloud Account**（新增雲端帳戶）。



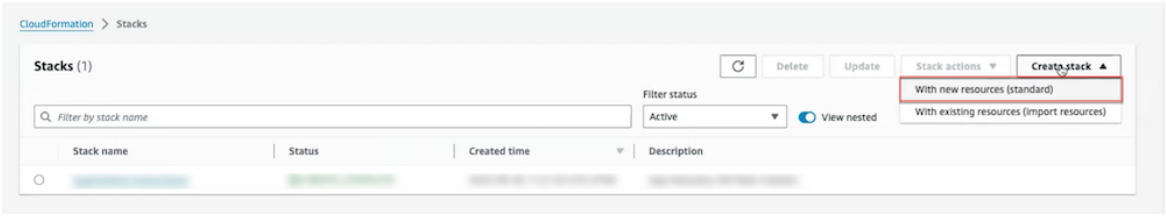

5. 新增 **Account Name**（帳戶名稱），並按一下 **Cloud Account Enabled**（雲端帳戶已啟用）下的核取方塊。新增 **AWS Account ID**（帳戶 **ID**），然後按一下 **Download IAM Role CFT**（下載 **IAM** 角色 **CFT**）以下載檔案。

 ©2025 Palo Alto Networks, Inc.




**STEP 2 |** 在 AWS 中建立 IAM 角色。

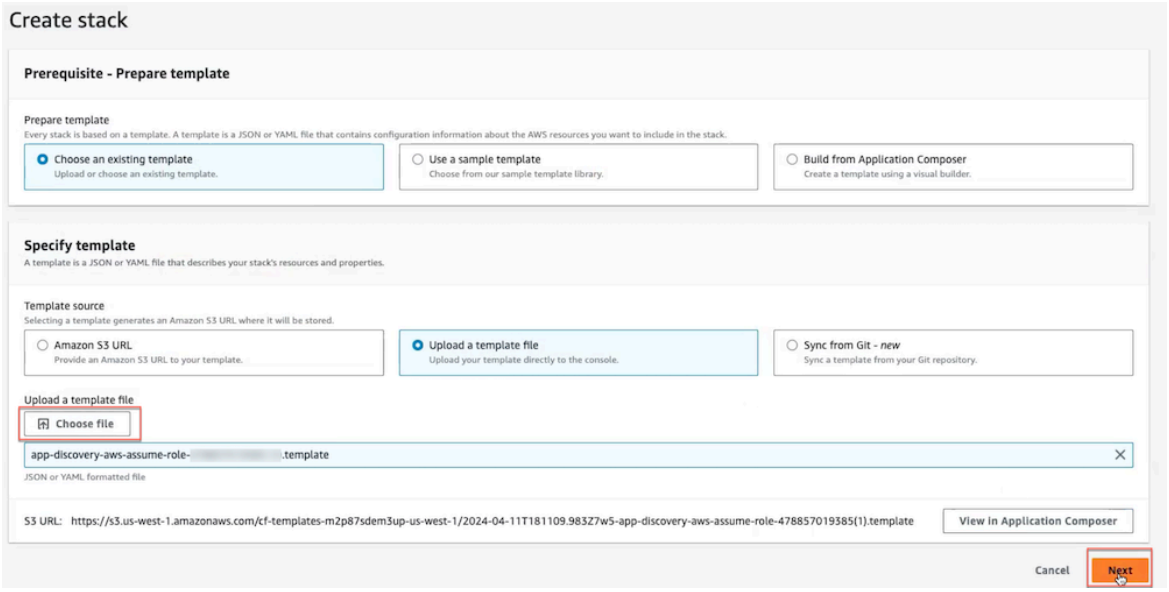
1. 導覽到 AWS 應用程式、選取您的帳戶，然後 **Sign in**（登入）。
2. 導覽到 **CloudFormation** > **Stacks**（堆疊） > **Create stack**（建立堆疊） > **With new resources (standard)**（具有新資源（標準）） 以建立堆疊。



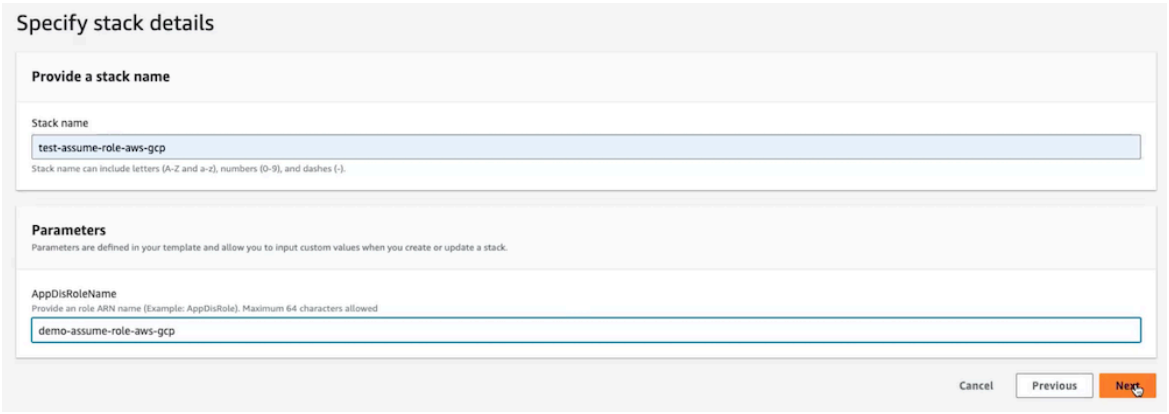

3. 在 **Create stack**（建立堆疊）頁面上，在 **Prerequisite-Prepare template**（**Prerequisite-Prepare** 範本）下，選取 **Choose an existing template**（選擇現有範本）。在 **Specify**

 ©2025 Palo Alto Networks, Inc.

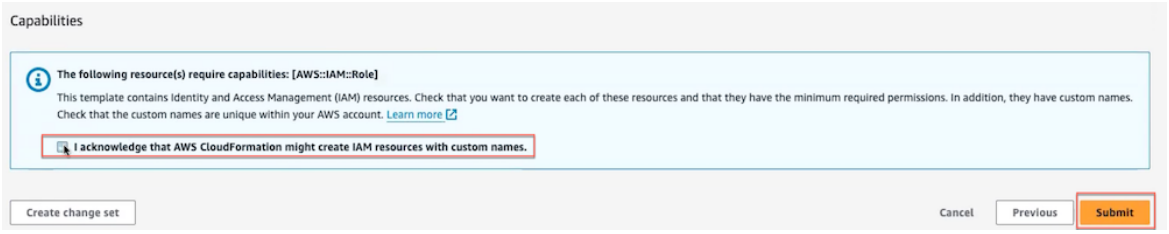
**template**（指定範本）下，選取 **Upload a template file**（上傳範本檔案）。上傳先前在步驟 1 中下載的檔案，然後選取 **Next**（下一步）。



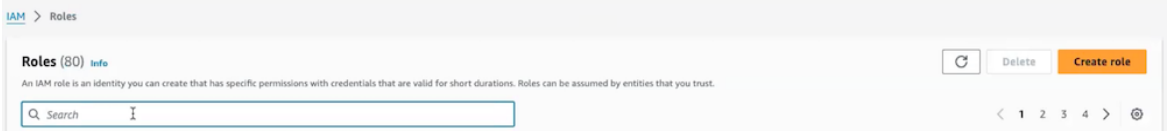

4. 新增 **Stack name**（堆疊名稱）、**AppDisRoleName**，並選取 **Next**（下一步）。




5. 在 **Configure stack options**（設定堆疊選項）頁面上，請勿進行任何更新，然後選取 **Next**（下一步）。
6. 檢閱變更。在 **Capabilities**（功能）下選擇核取方塊，以確認使用自訂名稱建立 IAM 資源，然後選取 **Submit**（提交）。

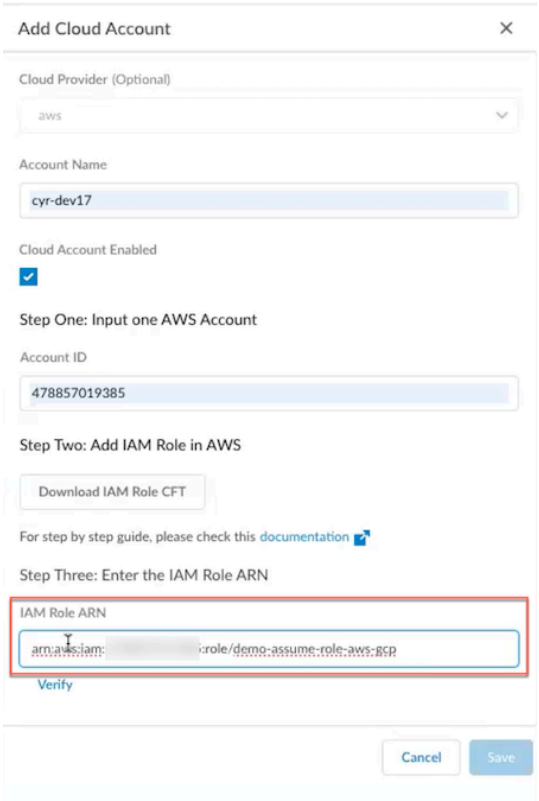



7. 導覽到 **IAM** > **Roles**（角色），並搜尋您定義的角色名稱。選擇角色名稱並複製該角色的 **ARN**。




 ©2025 Palo Alto Networks, Inc.

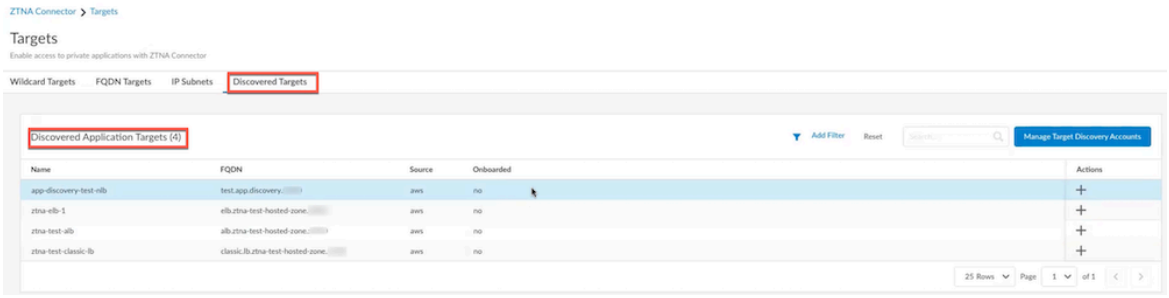
**STEP 3 |** 在 **IAM Role ARN**（**IAM** 角色 **ARN**）文字欄位中貼上 ARN，然後選取 **Verify**（驗證）。當驗證了 ARN 時，請選取 **Save**（儲存）。




如果您在 ***IAM Role ARN***（***IAM*** 角色 ***ARN***）欄位中新增了錯誤 *ARN*，則驗證會失敗並出現錯誤訊息。

在新增帳戶之後，您可以查看狀態、帳戶 ID 和其他詳細資訊。探索的重新整理期間為 24 小時。您也可以將多個帳戶新增到同一租用戶。

**STEP 4 |** 若要識別已探索的應用程式，請選取 **Discovered Targets**（已探索的目標）。您可以在 **Discovered Application Targets**（已探索的應用程式目標）下找到已識別應用程式的清單。

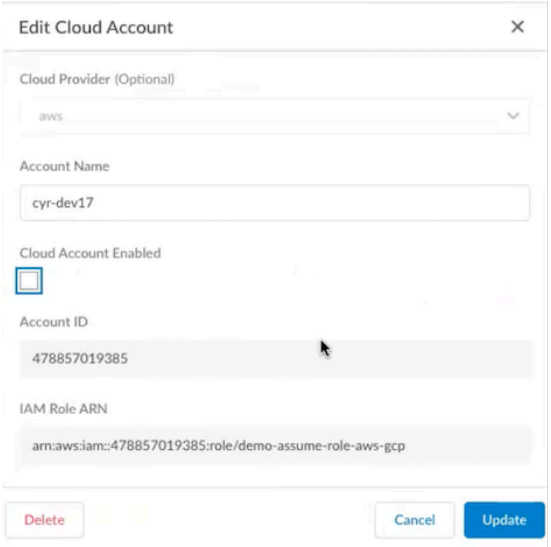



 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** （選用）刪除雲端帳戶。

若要刪除您的雲端帳戶，並在不停用目標探索的情況下新增帳戶，請遵循此程序。不過，如果您想要停用目標探索功能，這些步驟是必要的。

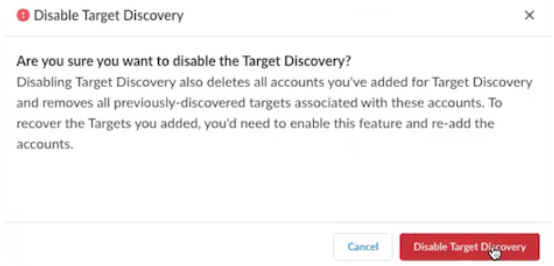
1. 在 **Manage Target Discovery Accounts**（管理目標探索帳戶）下，按一下您想要刪除的 **Account Name**（帳戶名稱）。
2. 停用 **Cloud Account Enabled**（雲端帳戶已啟用），然後選取 **Update**（更新）。當帳戶更新時，請選取 **Delete**（刪除）。帳戶已被刪除。




**STEP 6 |** （選用）停用目標探索。

在停用目標探索之前，請確保所有雲端帳戶都已刪除。

1. 選取 **Disable Target Discovery**（停用目標探索），然後選取 **Disable Target Discovery**（停用目標探索）。




 ©2025 Palo Alto Networks, Inc.

# 啟用應用程式搭配 ZTNA 連接器的安全性政策

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 4.0<br>❑ ZTNA 連接器附加元件授權<br>具有附加元件授權的基本授權包括 8 個 ZTNA 連接器、100 個 FQDN 和 4 個 IP 子網路功能。<br>具有附加元件授權的進階授權包括 40 個 ZTNA 連接器、300 個 FQDN 和 1024 個 IP 子網路功能。<br>具有附加元件授權的高級授權包括 200 個 ZTNA 連接器、4000 個 FQDN 和 1024 個 IP 子網路功能。<br>❑ 如果您未購買 ZTNA 連接器附加元件授權，Prisma Access 授權包括四個連接器、40 個 FQDN 和四個 IP 子網路。提供此功能的目的旨在您的環境中試用 ZTNA 連接器。 |

ZTNA 連接器不會強制執行政策；其會將您現有的 Prisma Access 安全性政策無縫地延伸到其為 Prisma Access 啟用的應用程式。這意味著您可以跨所有應用程式和資料中心使用一個通用政策，而且您不需要針對裝載到 ZTNA 連接器的應用程式單獨編寫安全性政策。

不過，作為設定 ZTNA 連接器的一部分，您確實需要確保您的安全性政策：

允許 **Prisma Access** 與 **ZTNA** 連接器之間的流量

為此，請遵循 ZTNA 連接器需求和指導方針 以確保 ZTNA 連接器可以連線到。Prisma Access。

使用者可以存取 **ZTNA** 連接器後面的應用程式

若要確保您的使用者可以存取 ZTNA 連接器應用程式，請針對您用來管理 Prisma Access 的介面遵循這裡的步驟。

- Strata Cloud Manager
- Panorama

## 啟用應用程式搭配 ZTNA 連接器的安全性政策 (Strata Cloud Manager)

在您將應用程式裝載至 ZTNA 連接器之後，應該設定政策規則以允許和控制對這些應用程式的存取。建立和套用政策的程序有所不同，取決於您的應用程式是由萬用字元、IP 子網路還是 FQDN 定義的。


©2025 Palo Alto Networks, Inc.

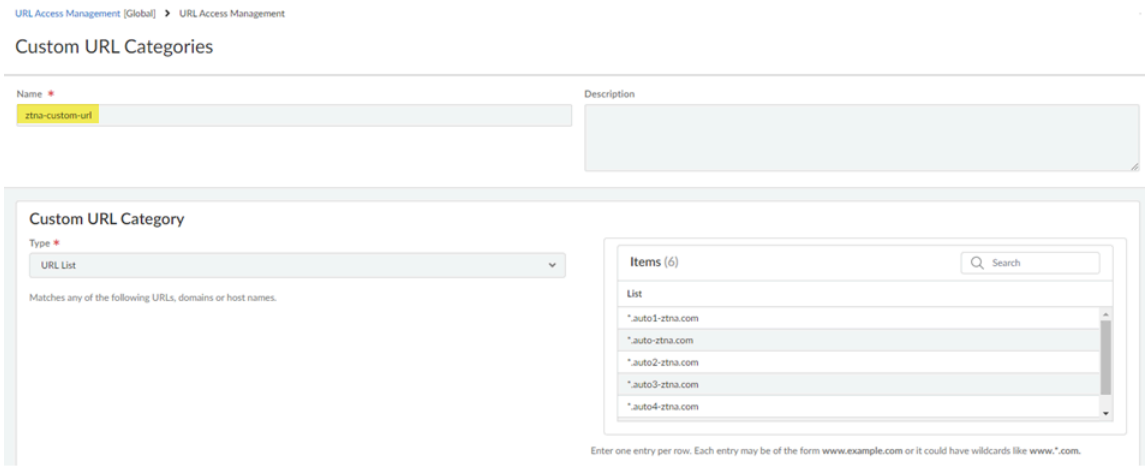
## 萬用字元型應用程式的安全性政策

萬用字元型應用程式（**Settings**（設定） > **ZTNA Connector**（**ZTNA** 連接器） > **Application Targets**（應用程式目標） > **Wildcard Targets**（萬用字元目標））要求您建立一個自訂 URL 類別；不過，該類型的類別僅對 HTTP 和 HTTPS 流量強制執行政策，對其他流量（如 SSH）不允許這樣做。因此，您需要透過允許流量流向 ZTNA 連接器應用程式 IP 區塊來暫時允許存取所有應用程式。

在 ZTNA 連接器得知基於萬用字元的 FQDN 之後，您可以停用允許應用程式 IP 區塊流量的政策，並根據得知的 FQDN 套用政策強制執行。

**STEP 1 |** 建立自訂 URL 類別並將萬用字元 URL 新增到該類別。

1. 前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服務） > **URL Access Management**（**URL** 存取管理）。
2. 在自訂 URL 類別下，**Add Category**（新增類別）。
3. 為自訂 URL 類別提供描述性 **Name**（名稱），並選取 **Type**（類型）為 **URL List**（**URL** 清單）。
4. 將您在 ZTNA 連接器中建立的萬用字元 URL 新增到 **Items**（項目）。
5. **Save**（儲存）變更。

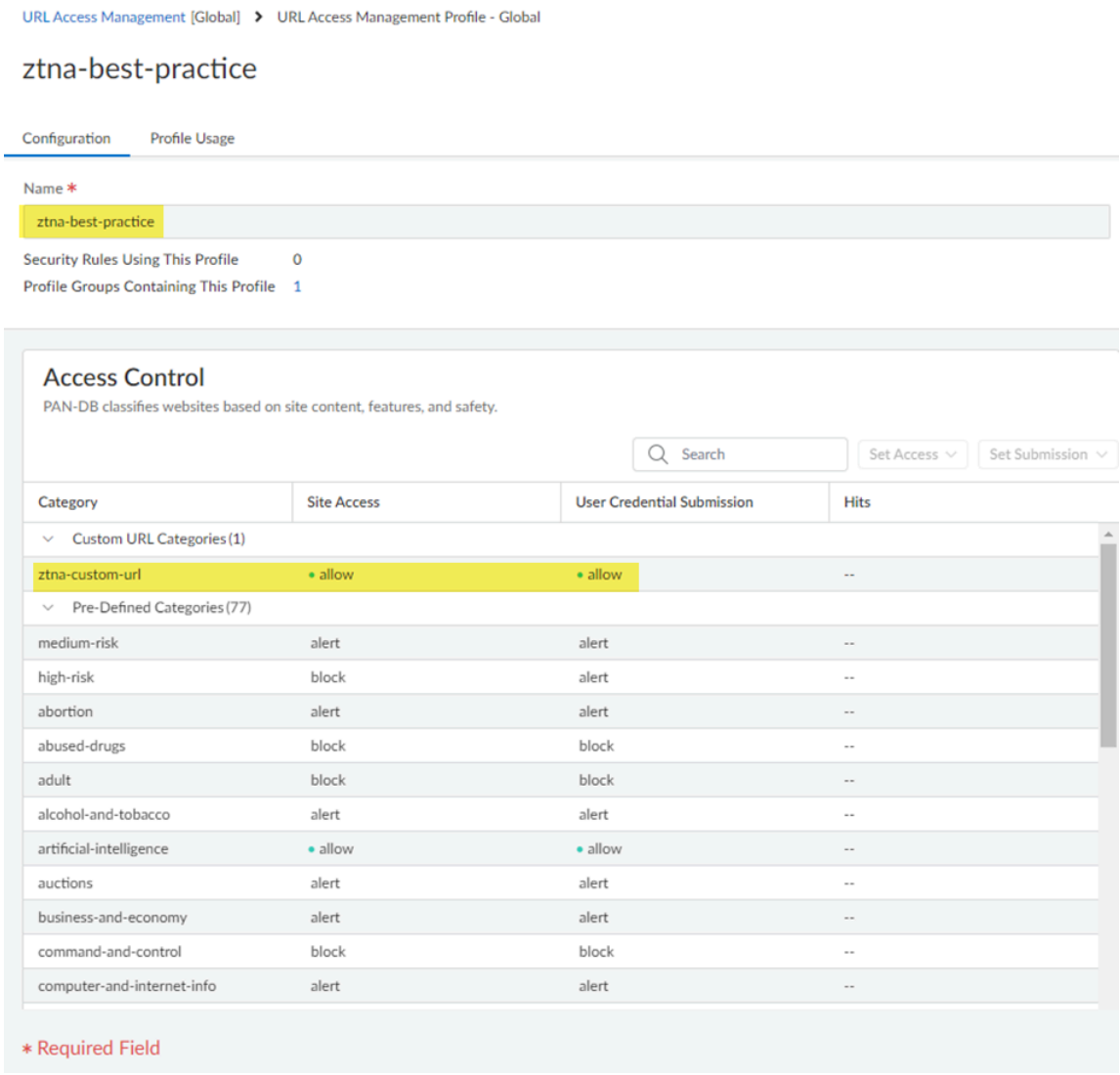




©2025 Palo Alto Networks, Inc.

**STEP 2 |** 建立一個 URL 存取管理設定檔，並將您建立的自訂 URL 類別新增到其中。

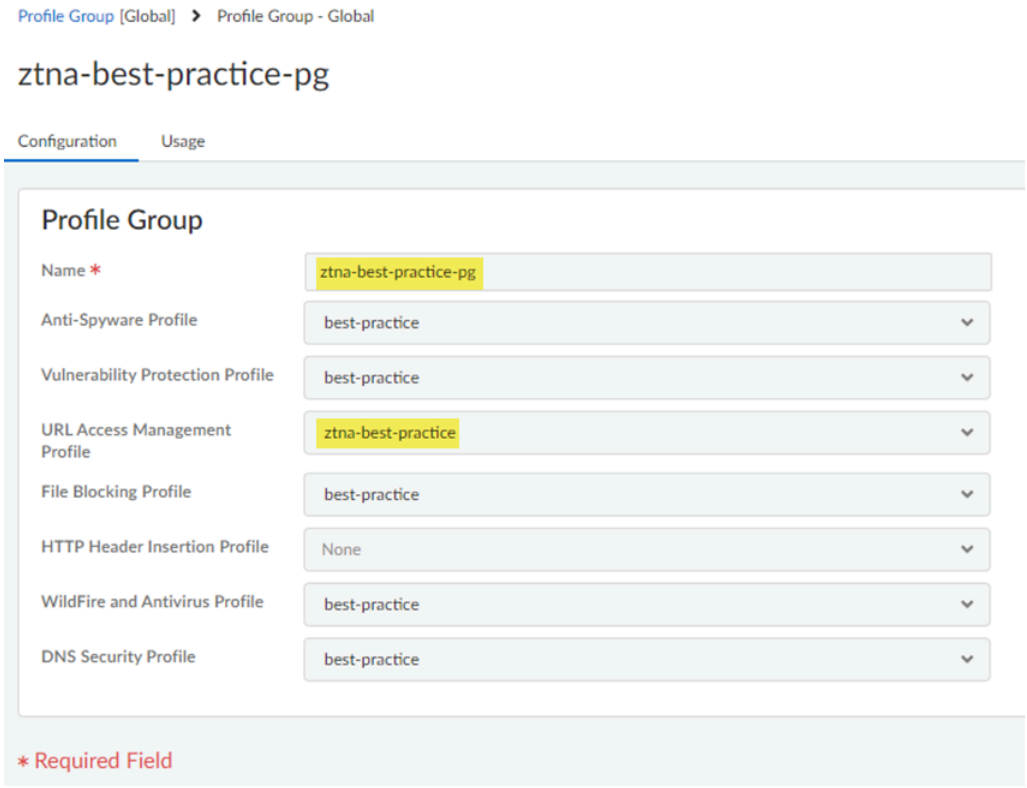
1. 仍在 **URL Access Management**（**URL** 存取管理）區域中時，請選取 **URL Access Management Profiles**（**URL** 存取管理設定檔）。
2. 選取要修改的現有設定檔，或 **Add Profile**（新增設定檔）。
3. 將您建立的自訂 URL 類別新增到設定檔。
4. 選取以下參數：
   - **Site Access**（網站存取）：允許
   - **User Credential Submission**（使用者認證提交）：允許
5. **Save**（儲存）變更。




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 建立一個設定檔群組，並將 URL 存取管理設定檔附加到該群組。

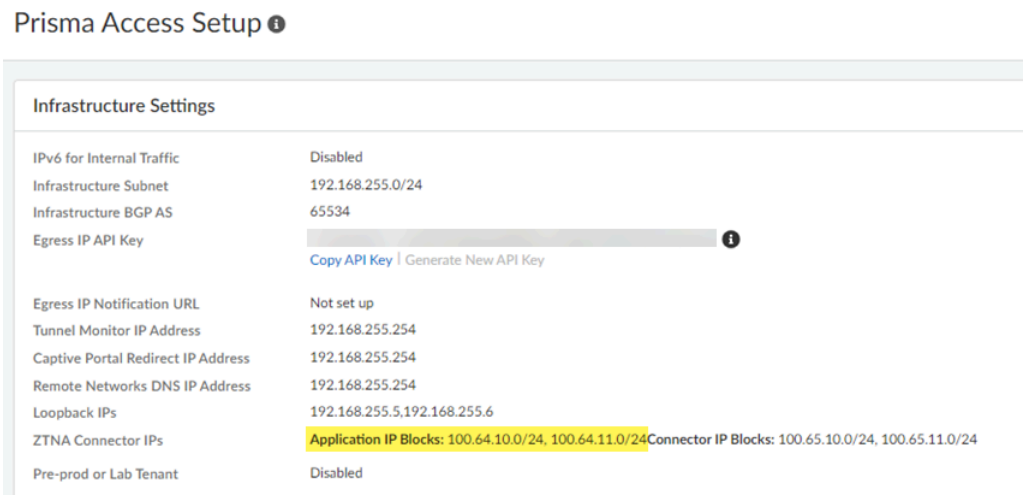
1. 前往 **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全性服務） > **Profile Groups**（設定檔群組）。
2. **Add**（新增）一個設定檔群組，指定您所建立的 URL 存取管理設定檔。




 ©2025 Palo Alto Networks, Inc.

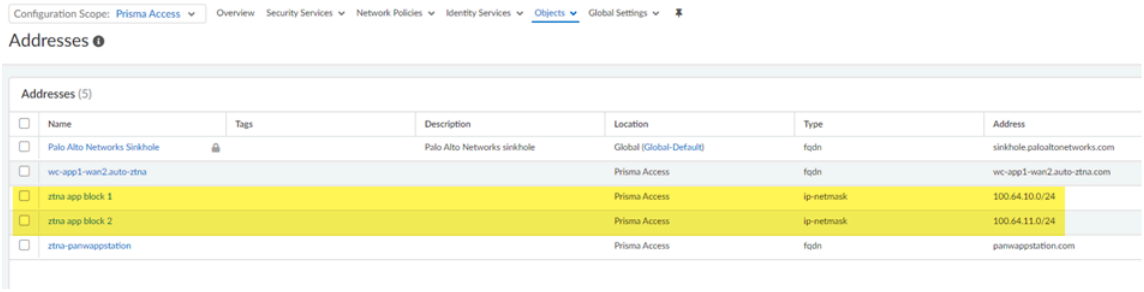
**STEP 4 |** 建立一個政策，以允許 ZTNA 連接器應用程式 IP 區塊的設定檔群組和 IP 位址。

1. 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Prisma Access** > **Prisma Access Setup**（**Prisma Access** 設定），並記下 ZTNA 連接器 IP 下的 **Application IP Blocks**（應用程式 **IP** 區塊）。

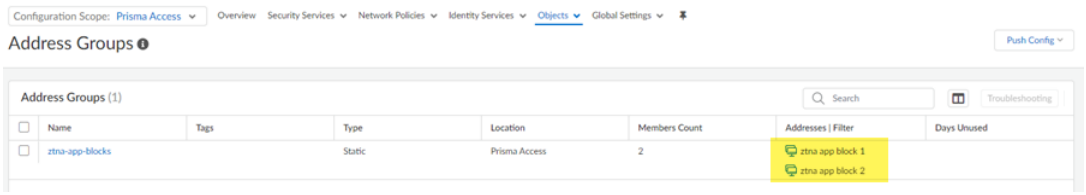



2. 前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（物件） > **Address**（位址） > **Addresses**（位址），並根據您擷取的 IP 位址 **Add**（新增）位址物件。

   如果您有 IP 子網路型應用程式，亦請為這些子網路建立位址物件。




3. 前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（物件） > **Address**（位址） > **Addresses Groups**（位址群組），並將您建立的位址物件 **Add**（新增）至位址群組。



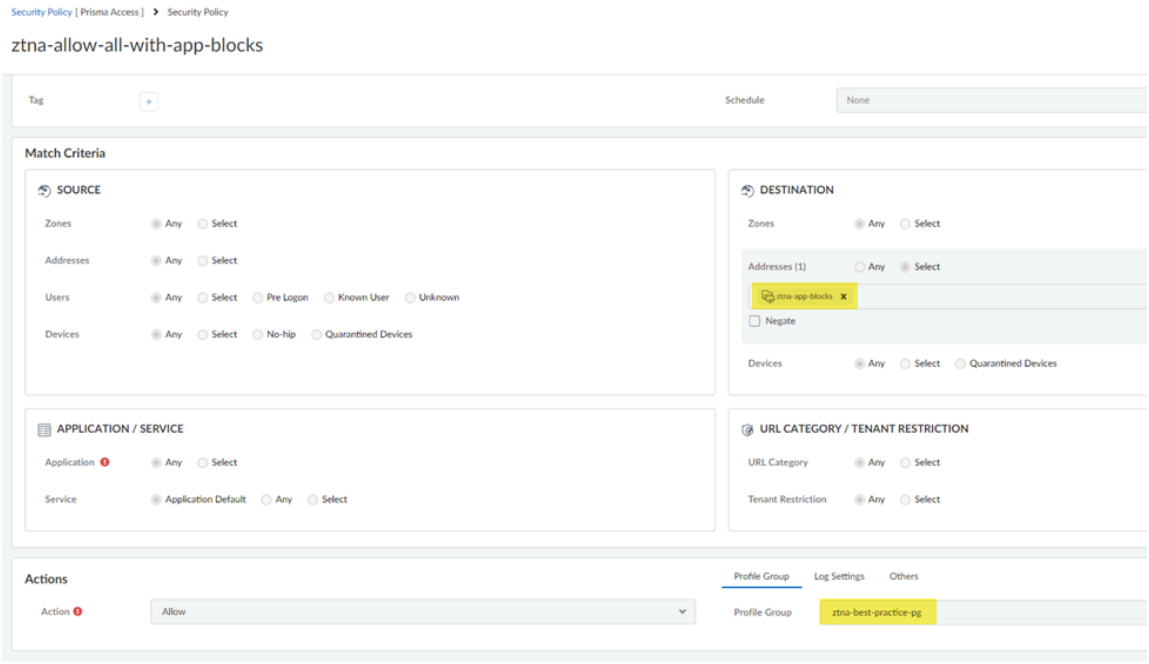

4. 前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全性服務） > **Security Policy**（安全性政策） > **Pre Rules**（前置規則），並 **Add**（新增）安全性政策以允許存取所有應用程式 IP 位址

 ©2025 Palo Alto Networks, Inc.

區塊，指定您在先前步驟中建立的 **Address Group**（位址群組）和 **Profile Group**（設定檔群組）。

新增此安全性政策允許來自萬用字元型應用程式流量的所有流量在 ZTNA 連接器根據萬用字元發現應用程式時通過。若沒有允許應用程式 IP 區塊的規則，使用者將無法存取萬用字元型應用程式。

您可以保留此政策，直到 ZTNA 連接器發現萬用字元型應用程式。然後，您可以選擇停用此政策，並為每個發現的應用程式新增安全性政策規則。





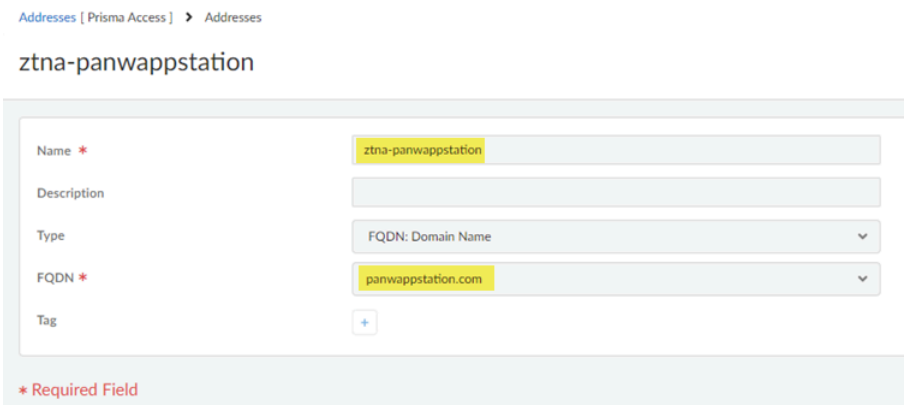
©2025 Palo Alto Networks, Inc.

**STEP 5 |** 在 ZTNA 連接器根據萬用字元發現應用程式之後，為您使用 FQDN 新增的應用程式設定安全性政策。

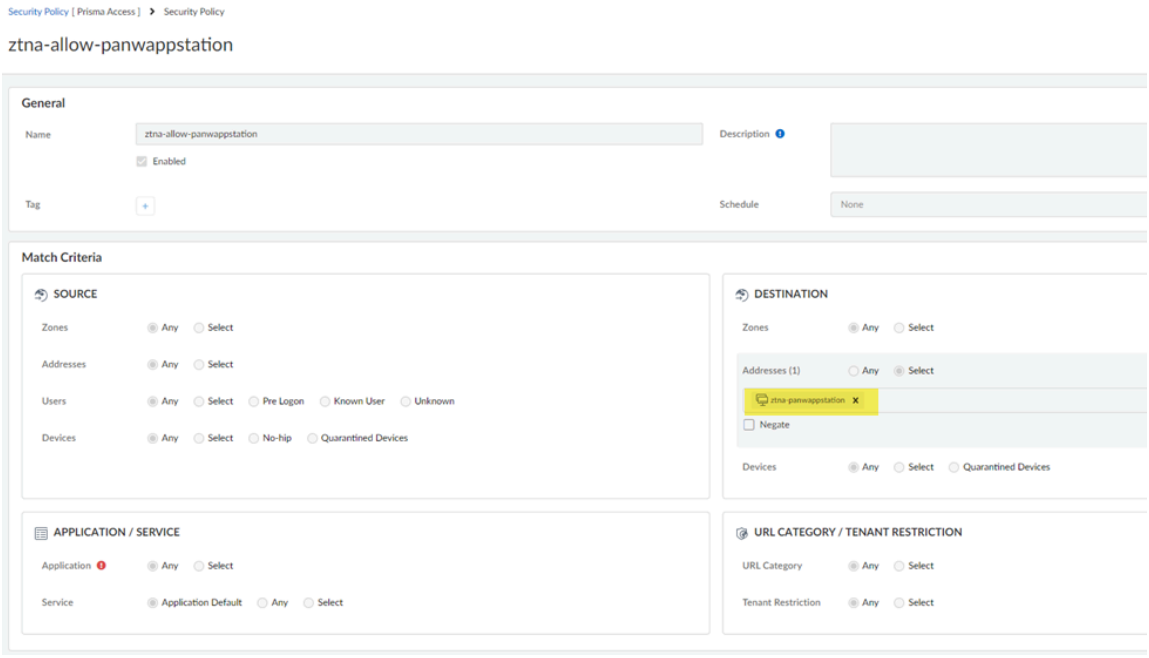
1. 前往 **Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Application Targets**（應用程式目標） > **FQDN Targets**（**FQDN** 目標），並記下應用程式使用的 FQDN。
2. 為 FQDN 建立位址物件（**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（物件） > **Address**（位址） > **Addresses**（位址））。

   選取 **Prisma Access** 設定範圍。
3. **Add**（新增）位址物件，其 **Type**（類型）為 **FQDN:Domain Name**（**FQDN**：網域名稱），並輸入所發現應用程式的 **FQDN**。

   輸入 FQDN 目標的 FQDN。




4. 前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全性服務） > **Security Policy**（安全性政策） > **Pre Rules**（前置規則），並 **Add**（新增）安全性政策以允許存取發現的應用程式。




 ©2025 Palo Alto Networks, Inc.

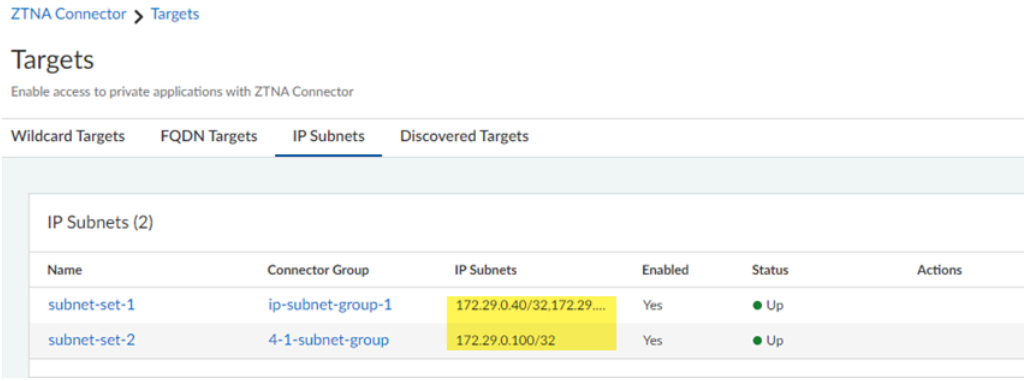
**STEP 6 |** **Push Config**（推送設定）以儲存並推送您的設定變更。

**STEP 7 |** （選用）在根據 FQDN 建立安全性政策之後，移除基於 IP 應用程式區塊的政策。

## IP 子網路型應用程式的安全性政策

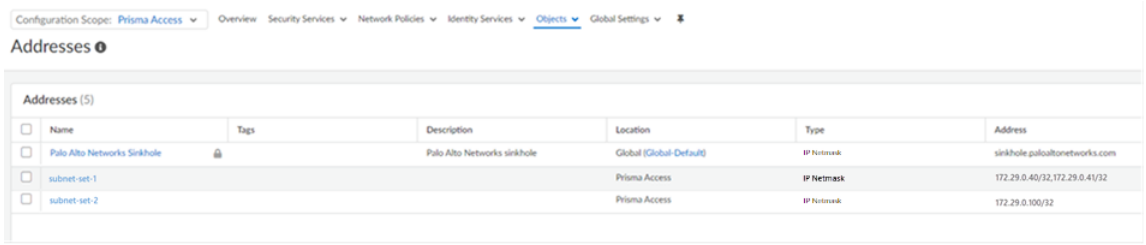
如果您根據 IP 子網路建立了 ZTNA 連接器應用程式目標（**Settings**（設定） > **ZTNA Connector**（**ZTNA** 連接器） > **Connectors**（連接器） > **Application Targets**（應用程式目標） > **IP Subnets**（**IP** 子網路）），請完成以下步驟以允許存取應用程式。

**STEP 1 |** 前往 **Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Application Targets**（應用程式目標） > **IP Subnets**（**IP** 子網路），並記下應用程式使用的 IP 子網路。

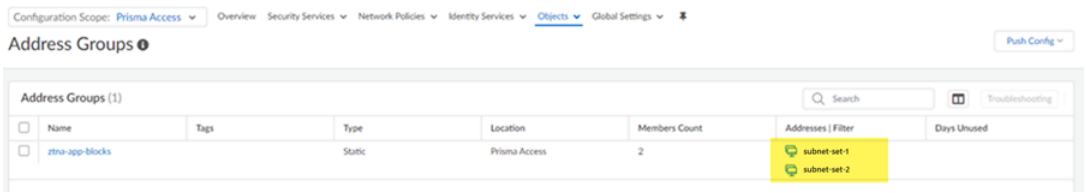



**STEP 2 |** 建立一個政策，以允許用於應用程式的 IP 子網路的 IP 位址。

1. 前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（物件） > **Address**（位址） > **Addresses**（位址），並根據您擷取的 IP 位址 **Add**（新增）位址物件。



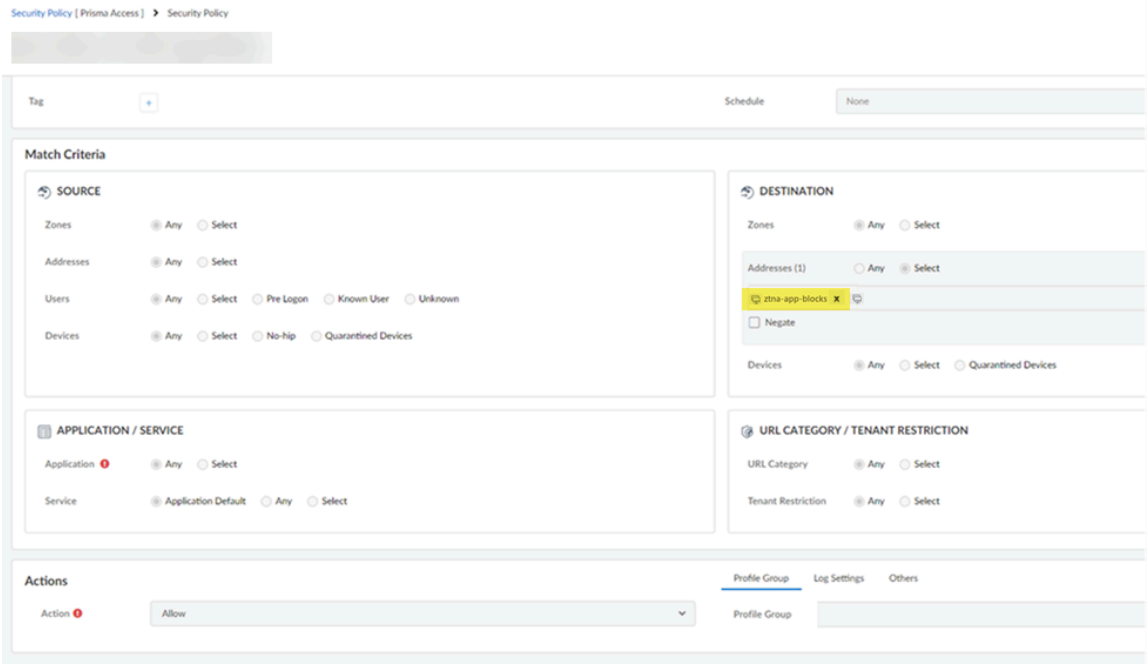

2. 前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（物件） > **Address**（位址） > **Addresses Groups**（位址群組），並將您建立的位址 **Add**（新增）至位址群組。




3. 前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全性服務） > **Security Policy**（安全性政策）

 ©2025 Palo Alto Networks, Inc.

> **Pre Rules**（前置規則），並 **Add**（新增）安全性政策以允許存取應用程式的 IP 子網路，指定您在先前步驟中建立的 **Address**（位址）。




**STEP 3 |** **Push Config**（推送設定）以儲存並推送您的設定變更。

## FQDN 型應用程式的安全性政策

如果您已根據 FQDN 新增目標（**Settings**（設定） > **ZTNA Connector**（**ZTNA** 連接器） > **Connectors**（連接器） > **Application Targets**（應用程式目標） > **FQDN Targets**（**FQDN** 目標）），請完成以下步驟來建立一個位址物件和一個安全性政策，以允許存取應用程式。

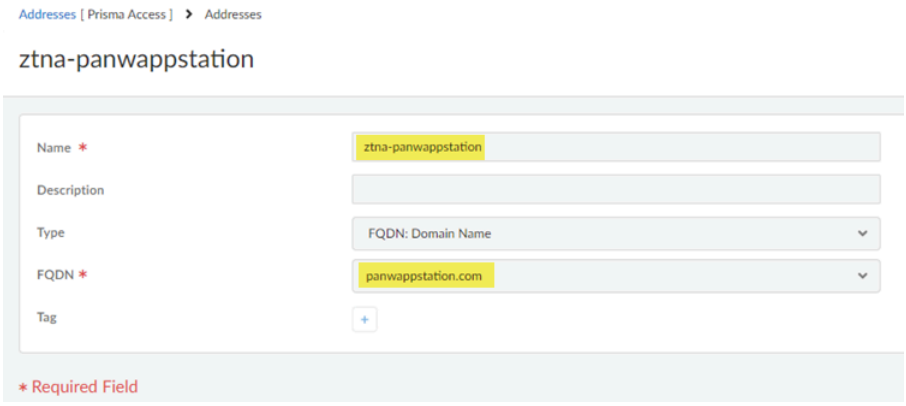
 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** 為您使用 FQDN 新增的應用程式設定安全性政策。

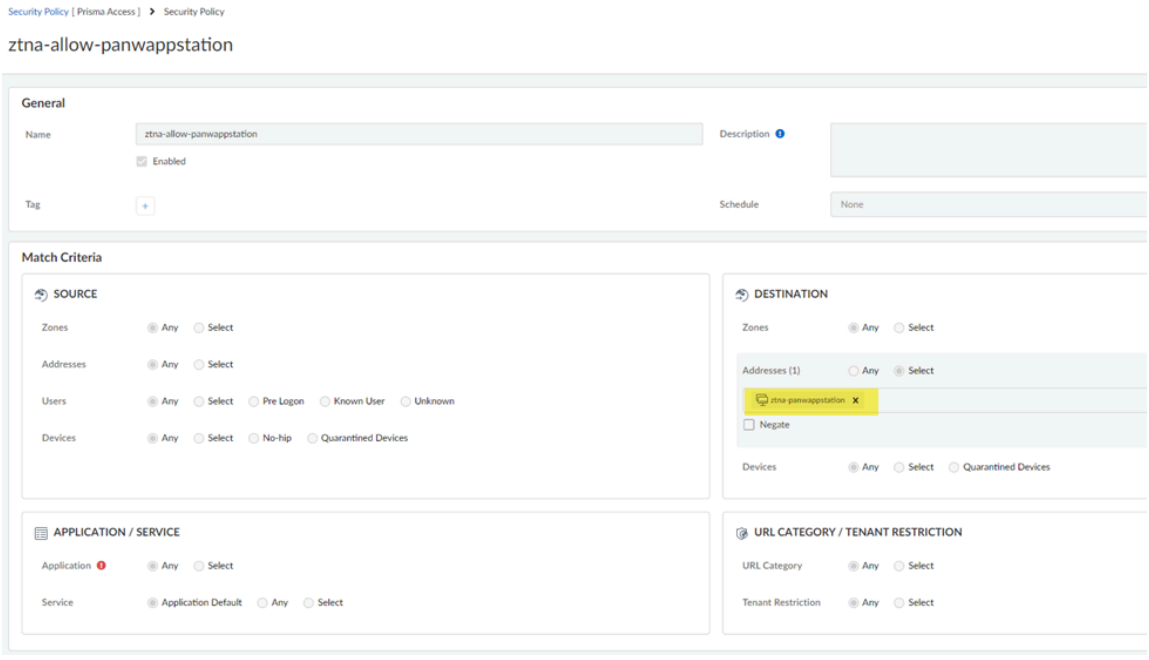
1. 前往 **Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Application Targets**（應用程式目標） > **FQDN Targets**（**FQDN** 目標），並記下應用程式使用的 FQDN。
2. 為 FQDN 建立位址物件（**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（物件） > **Address**（位址） > **Addresses**（位址））。

   選取 **Prisma Access** 設定範圍。
3. **Add**（新增）位址物件，其 **Type**（類型）為 **FQDN:Domain Name**（**FQDN**：網域名稱），並輸入所發現應用程式的 **FQDN**。

   為所有發現的應用程式輸入 FQDN。




4. 選用 前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全性服務） > **Security Policy**（安全性政策） > **Pre Rules**（前置規則），並 **Add**（新增）安全性政策以允許存取發現的應用程式。




 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** **Push Config**（推送設定）以儲存並推送您的設定變更。

# 啟用應用程式搭配 ZTNA 連接器的安全性政策 (Panorama)

在您將應用程式裝載至 ZTNA 連接器之後，應該設定政策規則以允許和控制對這些應用程式的存取。建立和套用政策的程序有所不同，取決於您的應用程式是由萬用字元、IP 子網路還是 FQDN 定義的。

## 萬用字元型應用程式的安全性政策

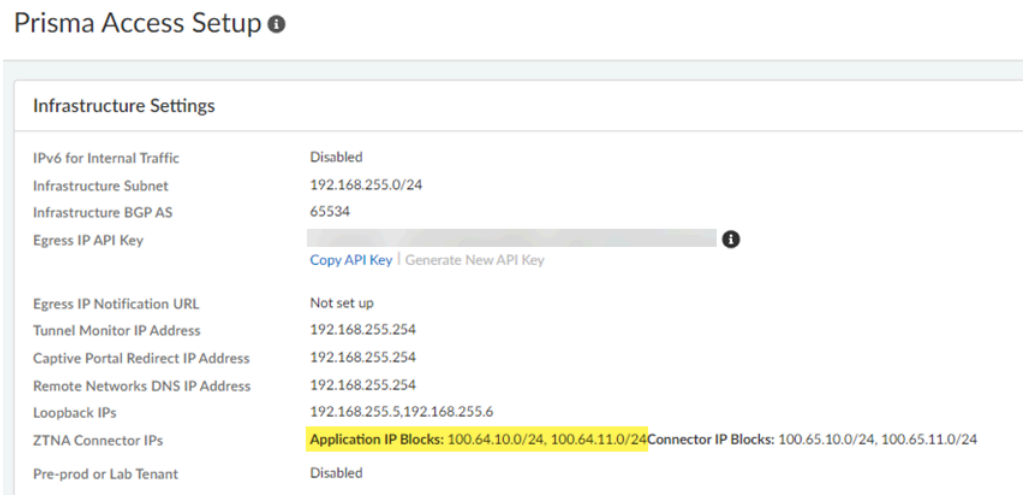
萬用字元型應用程式（**Settings**（設定） > **ZTNA Connector**（**ZTNA** 連接器） > **Application Targets**（應用程式目標） > **Wildcard Targets**（萬用字元目標））要求您建立一個自訂 URL 類別；不過，該類型的類別僅對 HTTP 和 HTTPS 流量強制執行政策，對其他流量（如 SSH）不允許這樣做。因此，您需要透過允許流量流向 ZTNA 連接器應用程式 IP 區塊來暫時允許存取所有應用程式。

在 ZTNA 連接器得知基於萬用字元的 FQDN 之後，您可以停用允許應用程式 IP 區塊流量的政策，並根據得知的 FQDN 套用政策強制執行。

 ©2025 Palo Alto Networks, Inc.

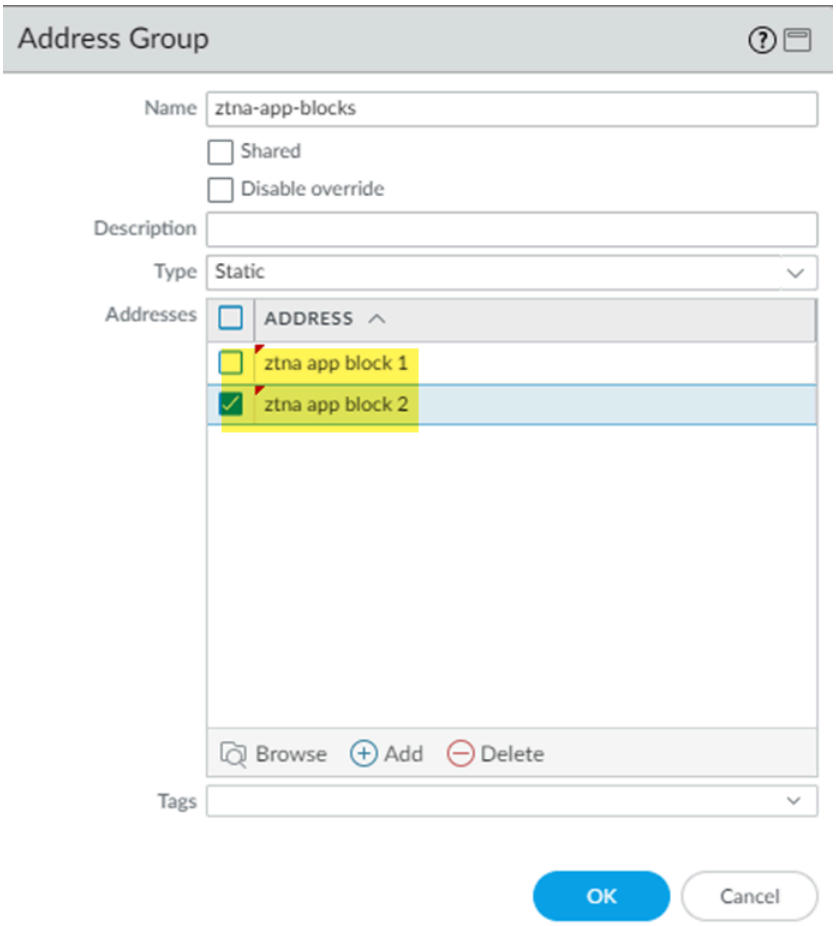
**STEP 1 |** 建立一個政策，以允許 ZTNA 連接器應用程式 IP 區塊的 IP 位址。

1. 從 ZTNA 連接器 UI 中，前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Prisma Access** > **Prisma Access Setup**（**Prisma Access** 設定），並記下 ZTNA 連接器 IP 下的 **Application IP Blocks**（應用程式 **IP** 區塊）。




2. 前往 **Objects**（物件） > **Addresses**（位址），並根據擷取的 IP 位址**Add**（新增）位址物件。
3. 前往 **Objects**（物件） > **Address Groups**（位址群組），並將您建立的位址物件 **Add**（新增）至位址群組。

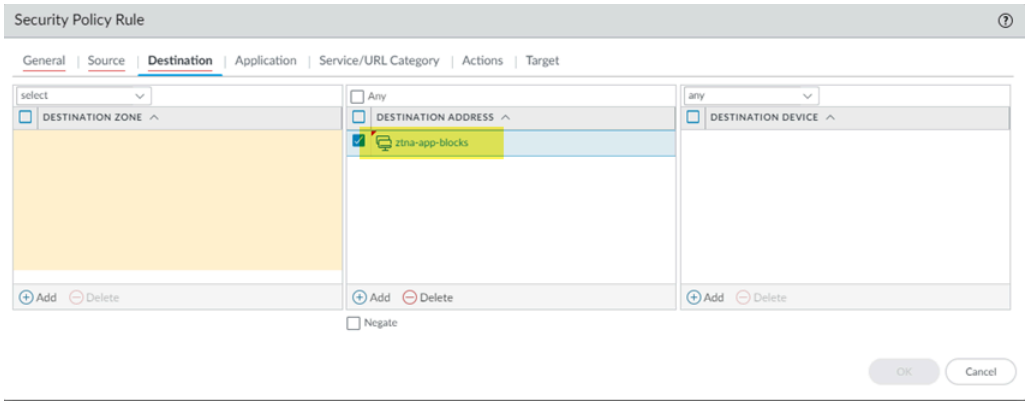
 ©2025 Palo Alto Networks, Inc.




4. 前往 **Policies**（政策） > **Security**（安全性） > **Pre Rules**（前置規則），並 **Add**（新增）安全性政策以允許存取所有應用程式 IP 位址區塊，指定您在先前步驟中建立的 **Address Group**（位址群組）。

   新增此安全性政策允許來自萬用字元型應用程式流量的所有流量在 ZTNA 連接器根據萬用字元發現應用程式時通過。若沒有允許應用程式 IP 區塊的規則，使用者將無法存取萬用字元型應用程式。

   您可以保留此政策，直到 ZTNA 連接器發現萬用字元型應用程式。然後，您可以選擇停用此政策，並為每個發現的應用程式新增安全性政策規則。



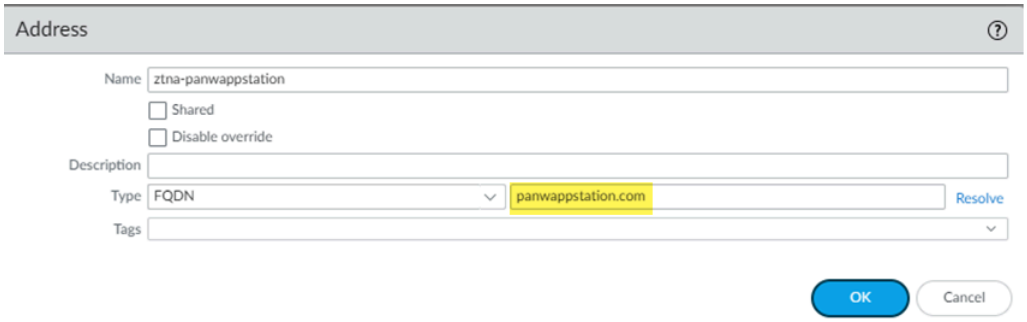

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 在 ZTNA 連接器根據萬用字元發現應用程式之後，為您使用 FQDN 新增的應用程式設定安全性政策。

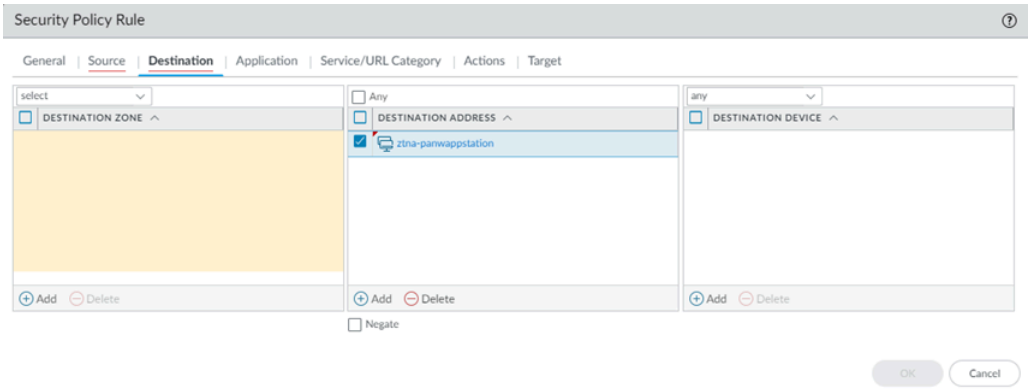
1. 前往 **Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Application Targets**（應用程式目標） > **FQDN Targets**（**FQDN** 目標），並記下應用程式使用的 FQDN。
2. 為 FQDN 建立位址物件（**Objects**（物件） > **Addresses**（位址））。

   選取 **Mobile_User_Device_Group** 或 **Remote_Network_Device_Group**，取決於行動使用者或分支網站使用者是否將存取 ZTNA 連接器後面的私人應用程式。
3. **Add**（新增） **Type**（類型）為 **FQDN** 的位址物件，並輸入所發現應用程式的 **FQDN**。

   輸入 FQDN 目標的 FQDN。




4. 前往 **Policies**（政策） > **Security**（安全性） > **Pre Rules**（前置規則），並 **Add**（新增）安全性政策以允許存取發現的應用程式。




**STEP 3 |** **Commit and Push**（提交並推送）您的變更。

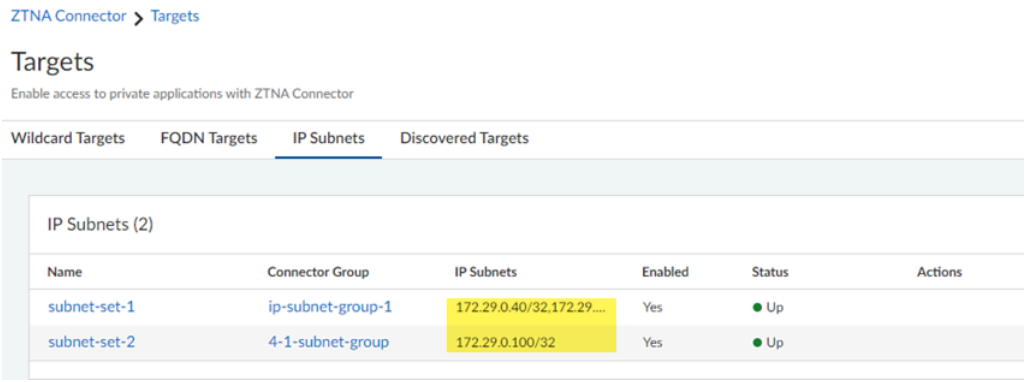
**STEP 4 |** （選用）在根據 FQDN 建立安全性政策之後，移除基於 IP 應用程式區塊的政策。

## IP 子網路型應用程式的安全性政策

如果您根據 IP 子網路建立了 ZTNA 連接器應用程式目標（**Settings**（設定） > **ZTNA Connector**（**ZTNA** 連接器） > **Connectors**（連接器） > **Application Targets**（應用程式目標） > **IP Subnets**（**IP** 子網路）），請完成以下步驟以允許存取應用程式。

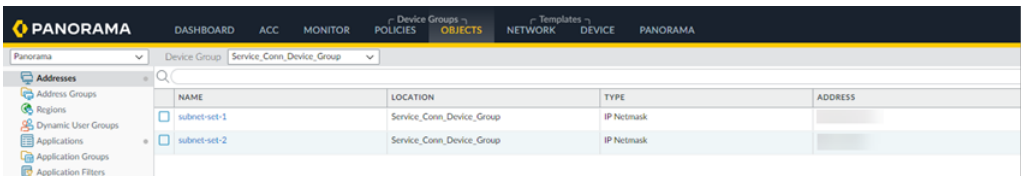

©2025 Palo Alto Networks, Inc.

**STEP 1 |** 前往 **Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Application Targets**（應用程式目標） > **IP Subnets**（**IP** 子網路），並記下應用程式使用的 IP 子網路。

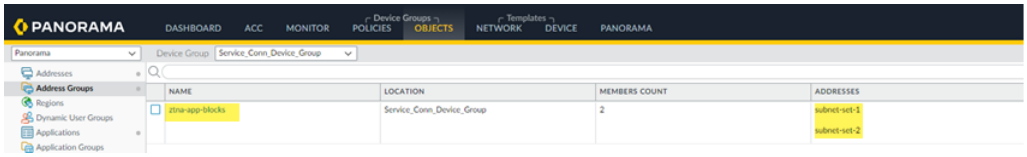



**STEP 2 |** 建立一個政策，以允許用於應用程式的 IP 子網路的 IP 位址。

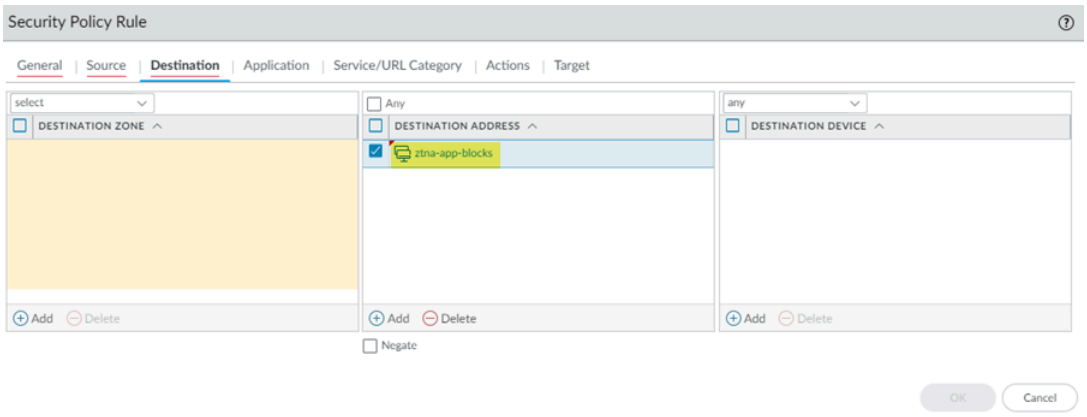
1. 前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（物件） > **Address**（位址） > **Addresses**（位址），並根據您擷取的 IP 位址 **Add**（新增）位址物件。




2. 前往 **Objects**（物件） > **Address Groups**（位址群組），並將您建立的位址 **Add**（新增）至位址群組。




3. 前往 **Policies**（政策） > **Security**（安全性） > **Pre Rules**（前置規則），並 **Add**（新增）安全性政策以允許存取應用程式的 IP 子網路，指定您在先前步驟中建立的 **Address**（位址）。




**STEP 3 |** **Push Config**（推送設定）以儲存並推送您的設定變更。

 ©2025 Palo Alto Networks, Inc.

## FQDN 型應用程式的安全性政策

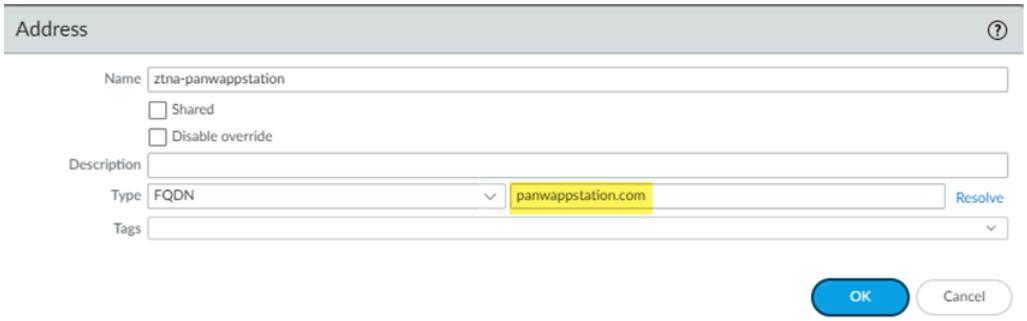
如果您已根據 FQDN 新增目標（**Settings**（設定） > **ZTNA Connector**（**ZTNA** 連接器） > **Connectors**（連接器） > **Application Targets**（應用程式目標） > **FQDN Targets**（**FQDN** 目標）），請完成以下步驟來建立一個位址物件和一個安全性政策，以允許存取應用程式。

**STEP 1 |** 為您使用 FQDN 新增的應用程式設定安全性政策。

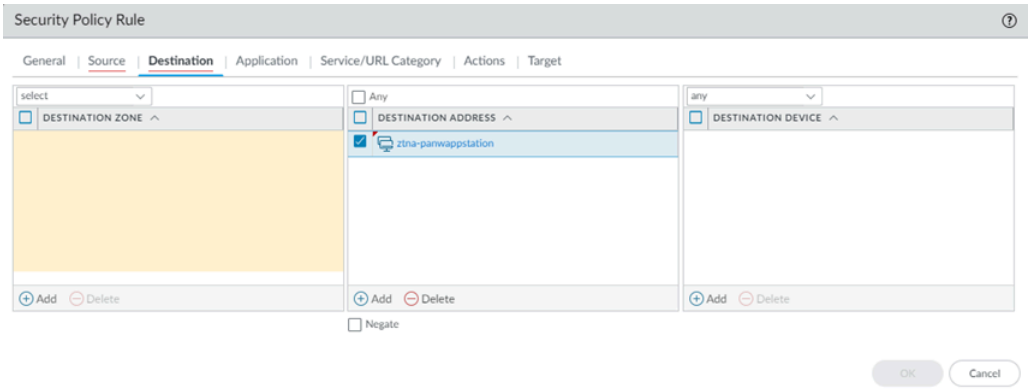
1. 前往 **Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Application Targets**（應用程式目標） > **FQDN Targets**（**FQDN** 目標），並記下應用程式使用的 FQDN。
2. 為 FQDN 建立位址物件（**Objects**（物件） > **Addresses**（位址））。

   選取 **Mobile_User_Device_Group** 或 **Remote_Network_Device_Group**，取決於行動使用者或分支網站使用者是否將存取 ZTNA 連接器後面的私人應用程式。
3. **Add**（新增） **Type**（類型）為 **FQDN** 的位址物件，並輸入所發現應用程式的 **FQDN**。

   為所有發現的應用程式輸入 FQDN。




4. 選用 前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全性服務） > **Security Policy**（安全性政策） > **Pre Rules**（前置規則），並 **Add**（新增）安全性政策以允許存取發現的應用程式。




**STEP 2 |** **Push Config**（推送設定）以儲存並推送您的設定變更。


©2025 Palo Alto Networks, Inc.

# 在您的資料中心裝載 ZTNA 連接器 VM

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 4.0<br>❑ ZTNA 連接器附加元件授權<br>具有附加元件授權的基本授權包括 8 個 ZTNA 連接器、100 個 FQDN 和 4 個 IP 子網路功能。<br>具有附加元件授權的進階授權包括 40 個 ZTNA 連接器、300 個 FQDN 和 1024 個 IP 子網路功能。<br>具有附加元件授權的高級授權包括 200 個 ZTNA 連接器、4000 個 FQDN 和 1024 個 IP 子網路功能。<br>❑ 如果您未購買 ZTNA 連接器附加元件授權，Prisma Access 授權包括四個連接器、40 個 FQDN 和四個 IP 子網路。提供此功能的目的旨在您的環境中試用 ZTNA 連接器。 |

在 Prisma Access 內設定您的連接器群組、連接器和應用程式目標之後，您必須在資料中心部署連接器 VM。為了簡化連接器裝載，可以從 Palo Alto Networks 客戶支援入口網站或從雲端提供者市集取得每個資料中心環境的部署範本。您使用的範本取決於您打算使用單臂部署還是雙臂部署。

## 支援的 ZTNA 連接器部署

ZTNA 連接器起始與雲端中 Prisma Access 公用 IP 位址的連線，您無需定義任何進入防火牆安全性規則。不過，因為 ZTNA 連接器起始連線，所以您需要新增輸出規則以允許 ZTNA 連接器存取雲端控制器，以及與 Prisma Access 資料平面的 IPSec 連線。ZTNA 連接器起始與雲端中的 Prisma Access 公用 IP 位址連線。基於此原因，您需要以下輸出規則，以便 ZTNA 連接器可以對 Prisma Access 建立 IPSec 通道：

- 面向網際網路—允許 HTTPS (TCP 443) 和 IKE/IPSec（UDP 500 和 4500）的輸出
- 面向資料中心—允許輸出應用程式連接埠。

  例如，允許輸出應用程式連接埠 HTTP (80) 和 HTTPS (443)。這些範例連接埠是 TCP 連接埠。如果您的資料中心使用不同的連接埠，請改為允許這些連接埠。

您可以在下列部署拓撲中部署連接器 VM：

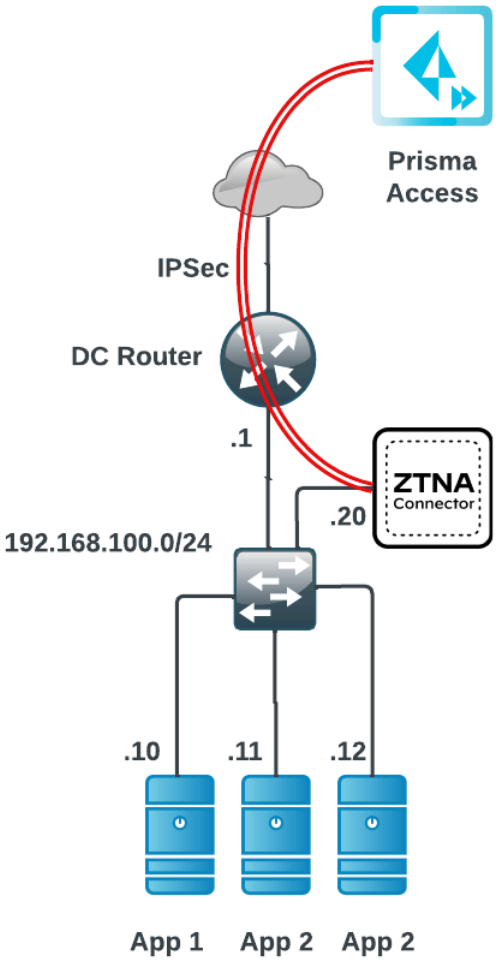
 ©2025 Palo Alto Networks, Inc.

單臂部署

僅在 *AWS*、*Azure* 或 *GCP* 等雲端原生環境中支援單臂部署。對於 *ESXi* 或核心型虛擬機器 *(KVM)* 或 *Microsoft Hyper-V* 等內部部署，請使用雙臂部署。

在此部署中，您的 ZTNA 連接器位於私人資料中心子網路上，可透過資料中心路由器存取網際網路。對應用程式的存取可以在同一子網路上本機進行，也可以透過資料中心路由器進行。

下圖顯示了使用單臂部署的 ZTNA 連接器網路部署範例。



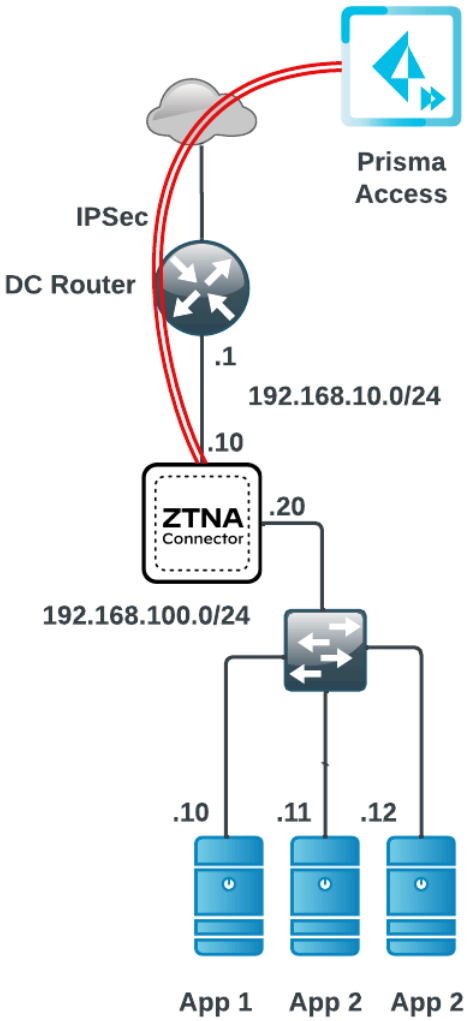

 ©2025 Palo Alto Networks, Inc.

兩臂部署

如果您想要更好地控制進入和輸出安全性規則，或者如果您有內部部署 VM 部署，則可以使用兩臂部署，其中一個介面面向網際網路，一個介面面向資料中心。

在兩臂連接器上設定 *IP* 位址時，請確保在開啟 *VM* 電源之前已正確設定 *ZTNA* 連接器的 *IP* 位址指派。例如，以下範例圖使用 *192.168.10.10* 和 *192.168.10.20 IP* 位址。鑒於這些範例位址，在 *ZTNA* 連接器上設定 *192.168.10.10* 和 *192.168.100.20* 的連接器，否則 *Prisma Access* 無法透過 *ZTNA* 連接器連線資料中心的應用程式。*192.168.10.10* 和 *192.168.100.20* 是範例 *IP* 位址，您不必使用這些 *IP* 位址，您的部署即可運作。

下圖顯示了使用雙臂部署的 ZTNA 連接器網路部署範例。

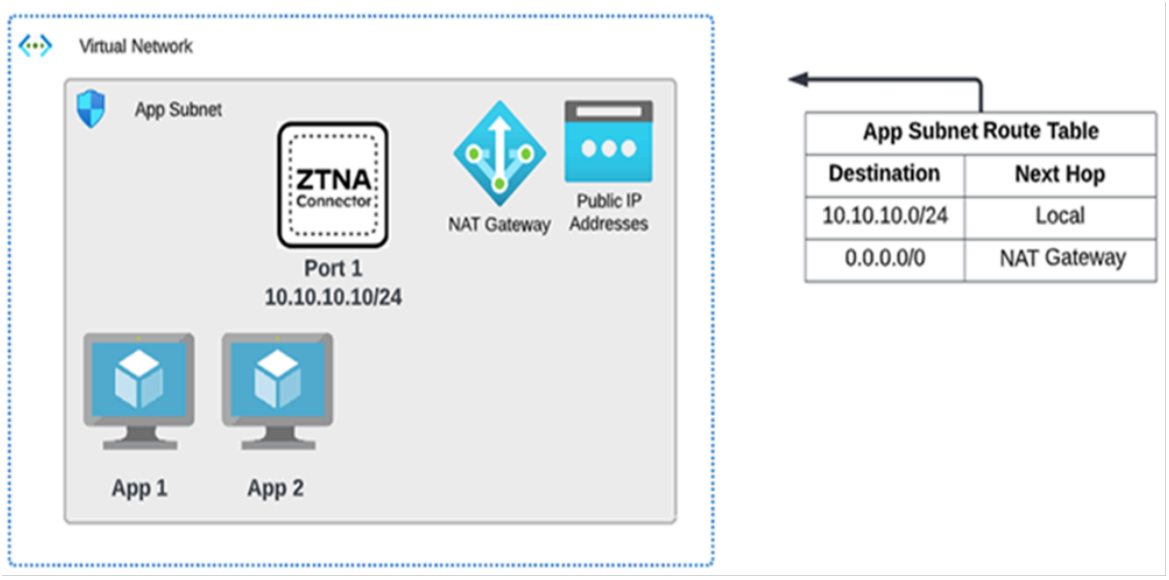



# ZTNA 連接器支援 Microsoft Azure 部署

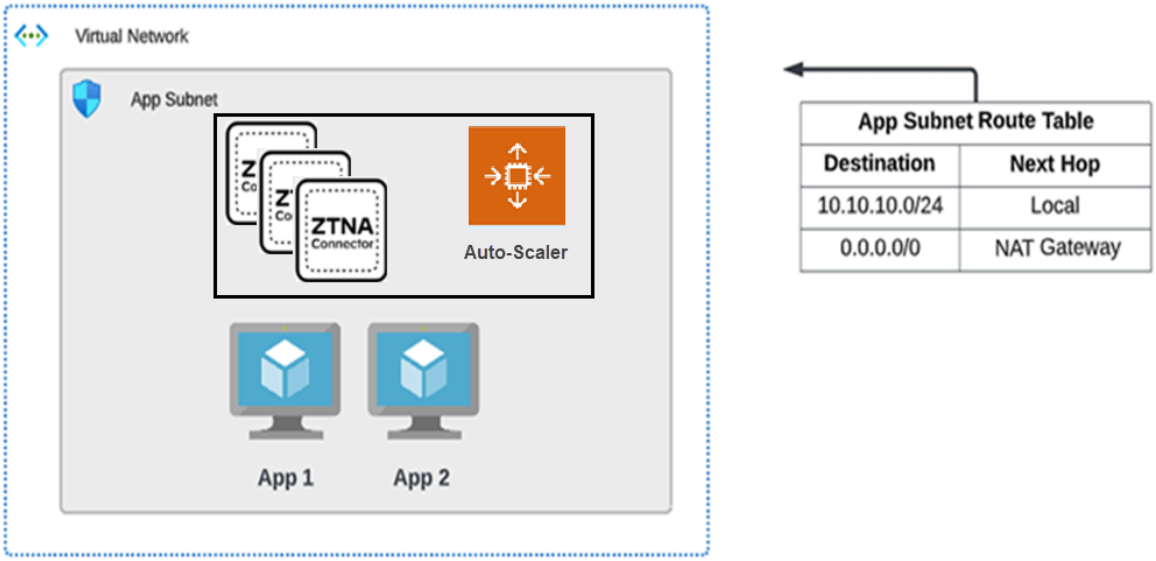
Prisma Access ZTNA 連接器在 Microsoft Azure 中的網路部署支援兩種部署，而且每種部署有一個對應範本。

 ©2025 Palo Alto Networks, Inc.

下圖顯示在 Azure 中使用單臂模式搭配 NAT 閘道進行 Prisma Access ZTNA 連接器部署範例。

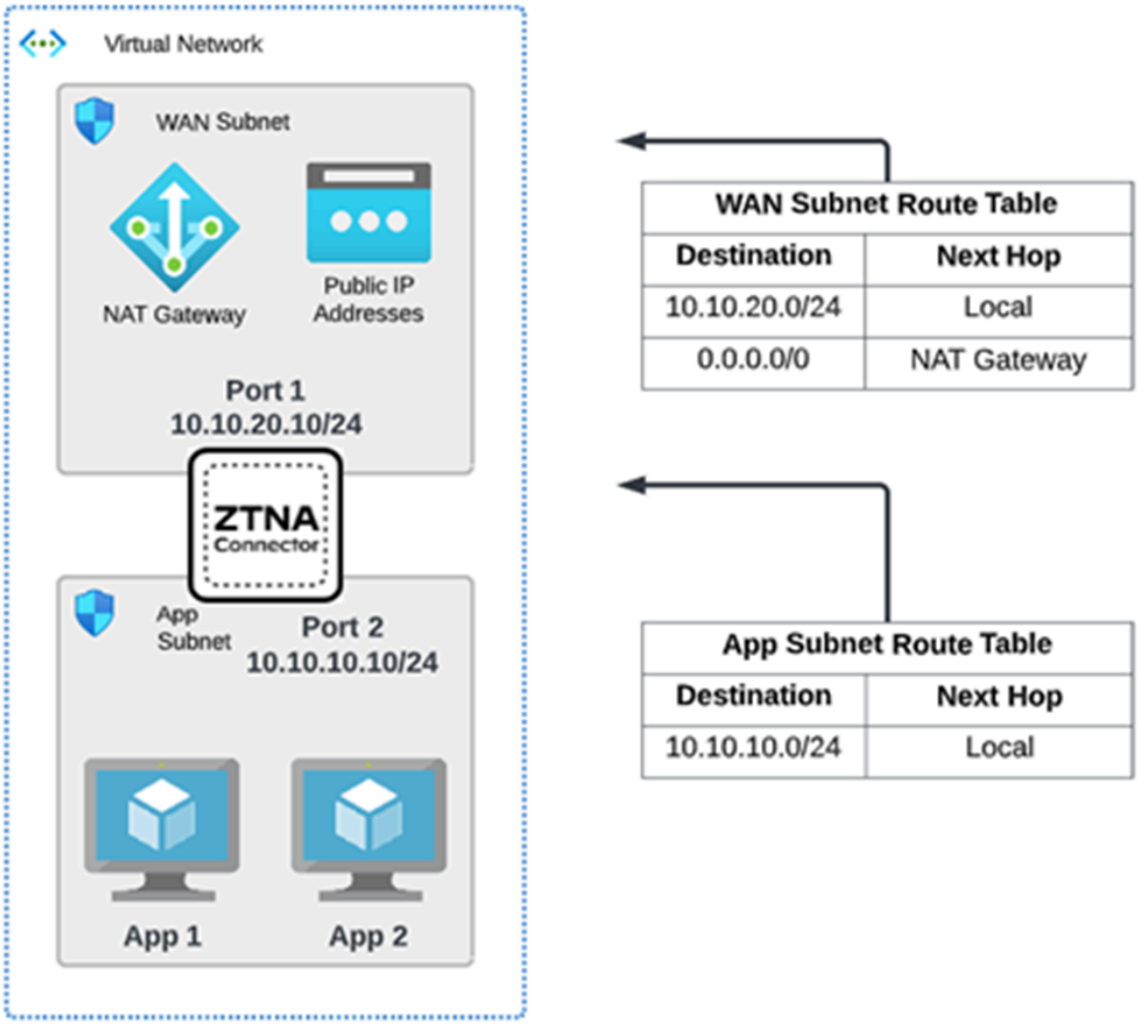



下圖顯示在 AWS 中使用單臂模式搭配 NAT 閘道進行 ZTNA 連接器部署範例。



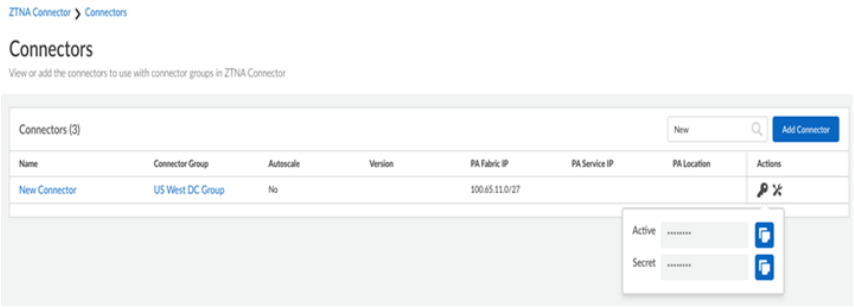

下圖顯示在 Azure 中使用雙臂模式搭配 NAT 閘道進行 Prisma Access ZTNA 連接器部署範例。


©2025 Palo Alto Networks, Inc.



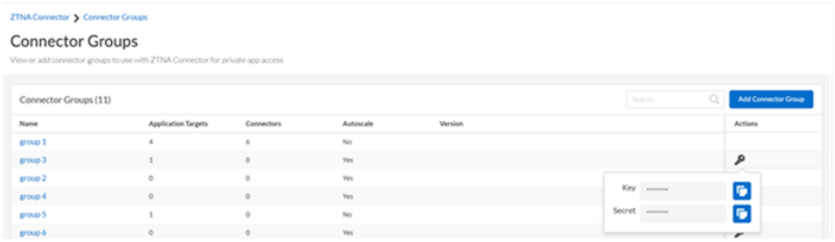

## 在 Microsoft Azure 中裝裝 ZTNA 連接器

- 檢閱需求和指導方針，以及您需要設定的 FQDN 和連接埠，以在 Microsoft Azure 中使用 ZTNA 連接器。
- 在 Prisma SASE 平台上，擷取並複製連接器金鑰和密碼值：**Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Connectors**（連接器），尋找您在 Prisma Access 建立的連接器物件，以將其與此 VM 建立關聯，並選取 **Copy Token**（複製權杖）；然後，複製 **Key**（金鑰）和 **Secret**（密碼）值。




 ©2025 Palo Alto Networks, Inc.

- 對於 **Prisma Access ZTNA** 連接器單臂自動調整部署，您必須擷取並複製連接器群組金鑰和密碼值：**Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Connectors Groups**（連接器群組），尋找您在 Prisma Access 建立的連接器群組物件，以將其與此 VM 建立關聯；並選取 **Copy Token**（複製權杖），然後，複製 **Key**（金鑰）和 **Secret**（密碼）。




在符合了所有先決條件之後，請遵循下列步驟，在 Microsoft Azure 中裝載 ZTNA 連接器。

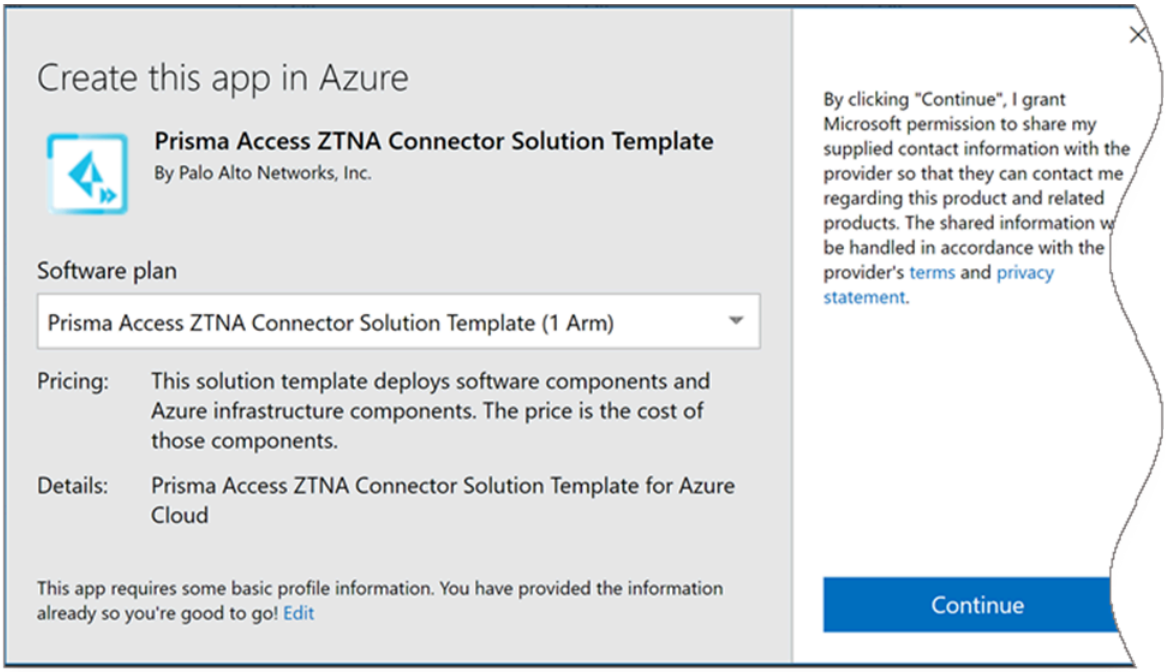
**STEP 1 |** 登入 Azure Marketplace 並搜尋 **Prisma Access ZTNA Connector**（**Prisma Access ZTNA** 連接器）。

**STEP 2 |** 按一下 **Get it Now**（立即取得）。



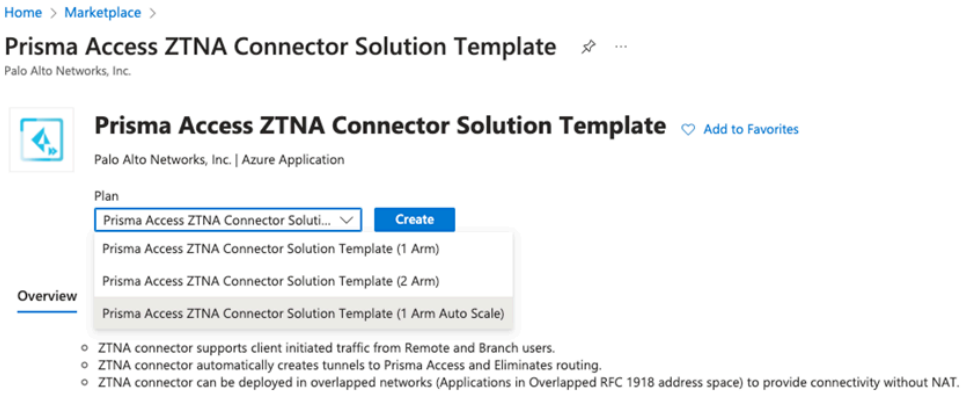

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** **Continue**（繼續）建立程序。




**STEP 4 |** 選擇軟體計畫並在 Azure 中 **Create**（建立）此應用程式：

- Prisma Access ZTNA 連接器解決方案範本（單臂）
- 在 Microsoft Azure 中部署搭配自動調整的 ZTNA 連接器單臂
- Prisma Access ZTNA 連接器解決方案範本（雙臂）



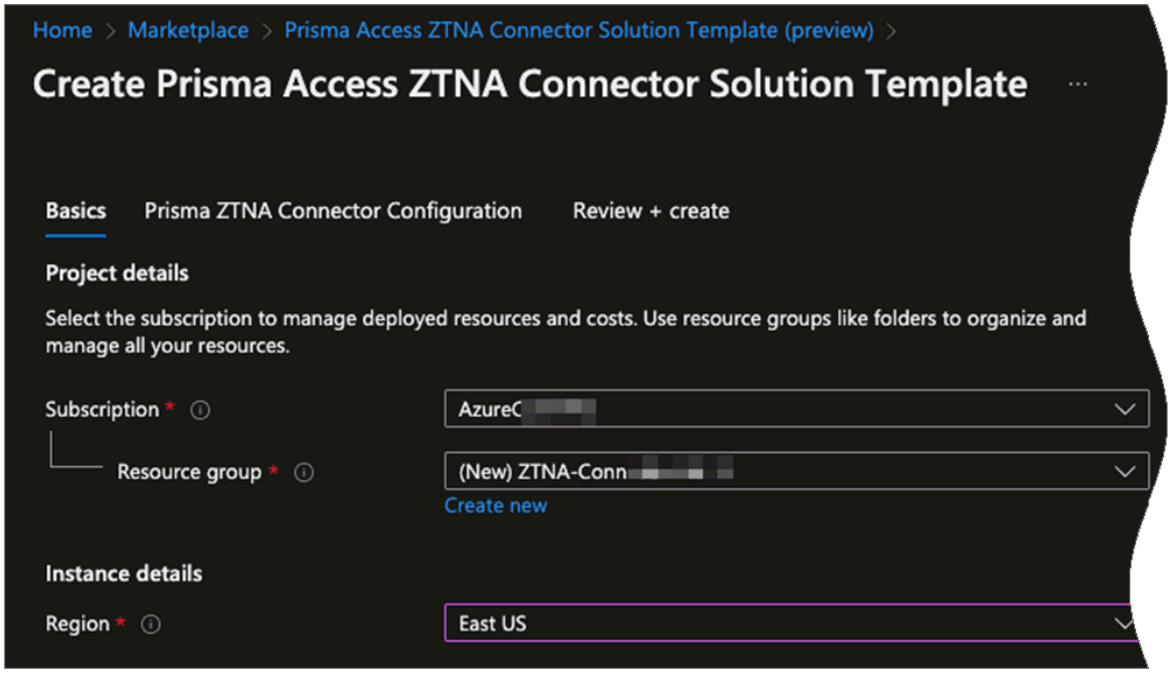

在 **Microsoft Azure** 中部署 **ZTNA** 連接器單臂

請遵循以下步驟，在 Microsoft Azure 中部署單臂 ZTNA 連接器：


©2025 Palo Alto Networks, Inc.

**STEP 1 |** 在 **Basics**（基本）頁籤上設定以下內容：

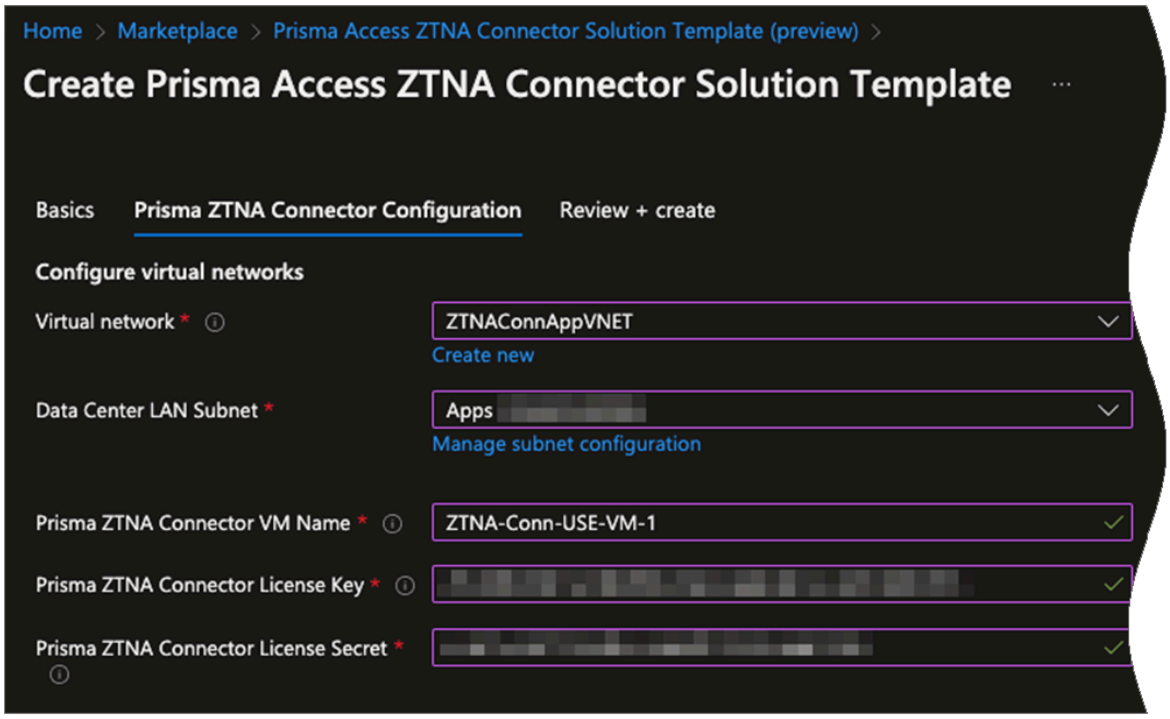
- 選取您的 Azure **Subscription**（訂閱）以管理已部署的資源。
- 選取現有的 **Resource Group**（資源群組）或 **Create new**（建立新的）。
- 選取與您位置相關的 Azure **Region**（區域）。
- 按一下 **Next**（下一步）：**Prisma ZTNA Connector Configuration**（**Prisma ZTNA** 連接器設定）。



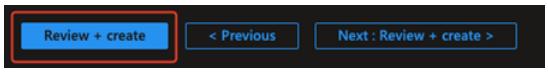

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 在 **Prisma ZTNA Connector Configuration**（**Prisma ZTNA** 連接器設定）頁籤上設定虛擬網路：

- 建立新的虛擬網路或選取現有的 **Virtual network**（虛擬網路）。
- 選取 **Data Center LAN Subnet**（資料中心 **LAN** 子網路），您已在其中佈建了要裝載至此連接器的應用程式。
- 輸入 **Prisma ZTNA Connector VM Name**（**Prisma ZTNA** 連接器 **VM** 名稱）。
- 輸入您從 Prisma SASE 入口網站擷取的 **Prisma ZTNA Connector License Key**（**Prisma ZTNA** 連接器授權金鑰）和 **Prisma ZTNA Connector License Secret**（**Prisma ZTNA** 連接器授權密碼）值。



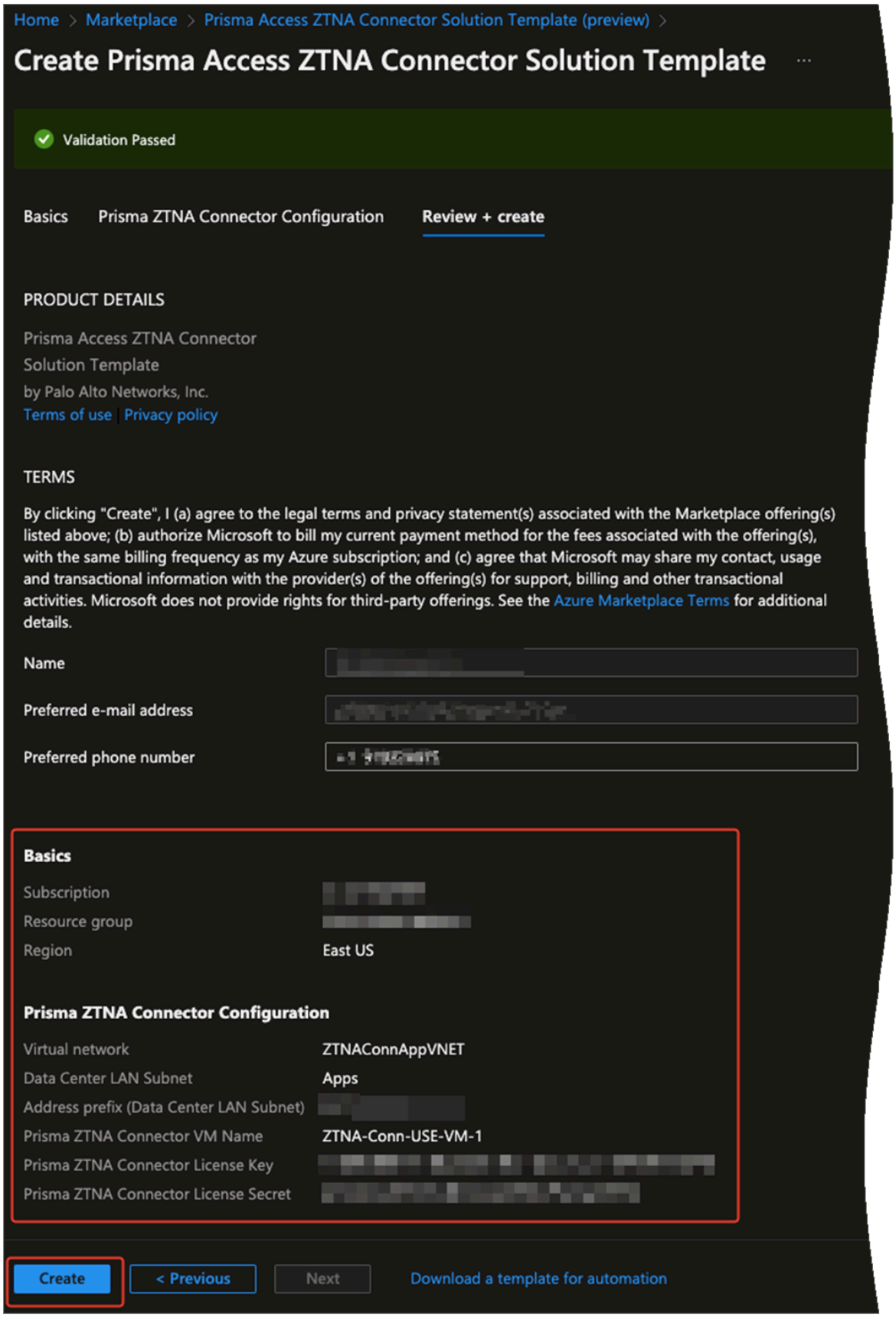

- **Review + create**（檢閱 + 建立）以檢閱您的受管理 Prisma ZTNA 連接器設定。




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 確認您提供的詳細資訊，然後按一下 **Create**（建立）以開始虛擬機器部署。


©2025 Palo Alto Networks, Inc.



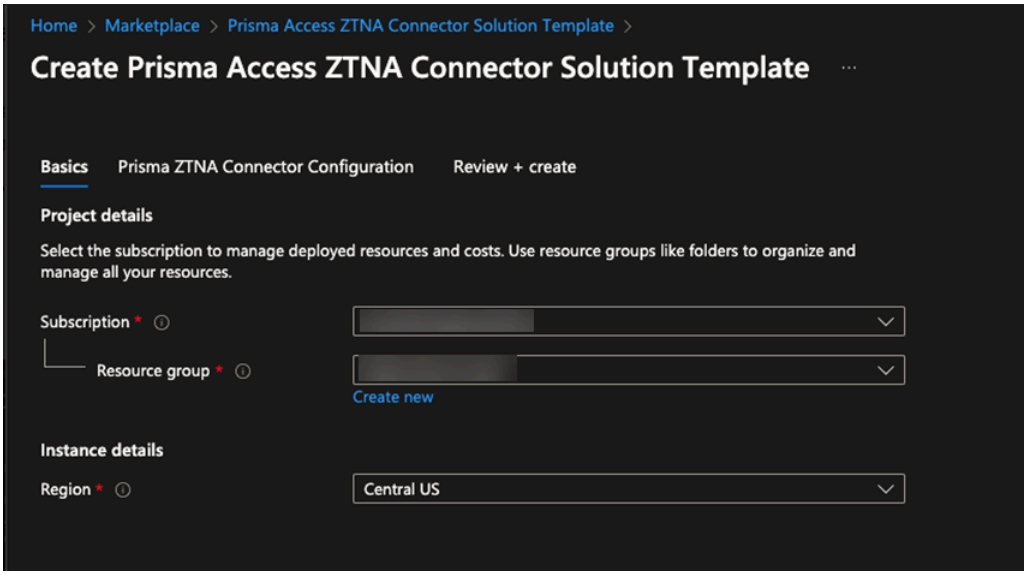

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 部署完成之後，請選取 **Go to resource**（前往資源）。

在 **Microsoft Azure** 中部署搭配自動調整的 **ZTNA** 連接器單臂

**STEP 1 |** 在 **Basics**（基本）頁籤上設定以下內容：

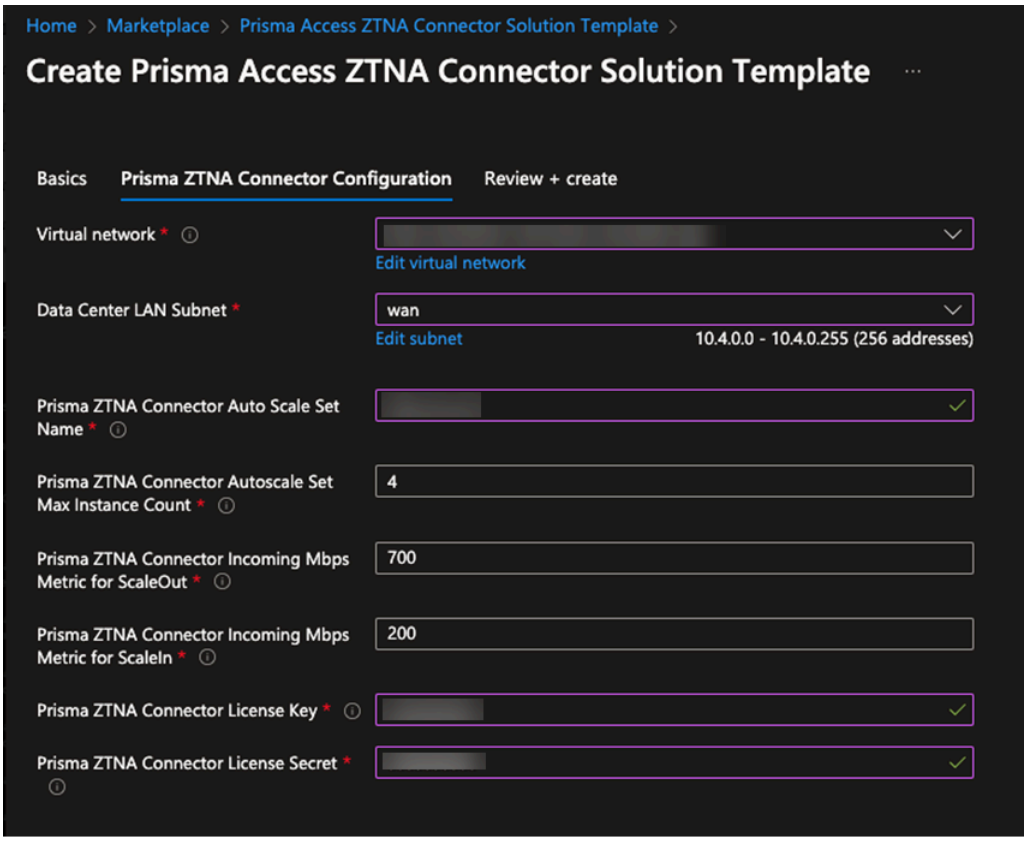
- 選取您的 Azure **Subscription**（訂閱）以管理已部署的資源。
- 選取現有的 **Resource Group**（資源群組）或 **Create new**（建立新的）。
- 選取與您位置相關的 Azure **Region**（區域）。
- 按一下 **Next**（下一步）：**Prisma ZTNA Connector Configuration**（**Prisma ZTNA** 連接器設定）。



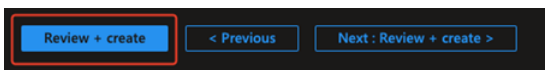

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 在 **Next:Prisma ZTNA Connector Configuration**（下一步：**Prisma ZTNA** 連接器設定）頁籤上，設定虛擬網路：

- 建立新的 **Virtual network**（虛擬網路）或選取現有的 **Virtual network**（虛擬網路）。
- 選取 **Data Center LAN Subnet**（資料中心 **LAN** 子網路），您已在其中佈建了要裝載至此連接器的應用程式。
- 輸入 **Prisma ZTNA Connector Auto Scale Set Name**（**Prisma ZTNA** 連接器自動擴展集名稱），指定在 Azure 中建立的擴展集名稱。
- 輸入 **Prisma ZTNA Connector Autoscale Set Max Instance Count**（**Prisma ZTNA** 連接器自動擴展集最大執行個體計數）。連接器群組中允許的 ZTNA 連接器數目上限為 4。
- 輸入 **Prisma ZTNA Connector Incoming Mbps Metric for ScaleOut**（**Prisma ZTNA** 連接器傳入 **Mbps** 指標進行相應放大）。輸入一個介於 100 到 1000 之間的值。
- 輸入 **Prisma ZTNA Connector Incoming Mbps Metric for ScaleIn**（**Prisma ZTNA** 連接器傳入 **Mbps** 指標進行相應縮小）。輸入一個介於 1 到 500 之間的值。
- 針對您要裝載連接器的連接器群組，輸入您從 Prisma SASE 入口網站擷取的 **Prisma ZTNA Connector License Key**（**Prisma ZTNA** 連接器授權金鑰）和 **Prisma ZTNA Connector License Secret**（**Prisma ZTNA** 連接器授權密碼）值。

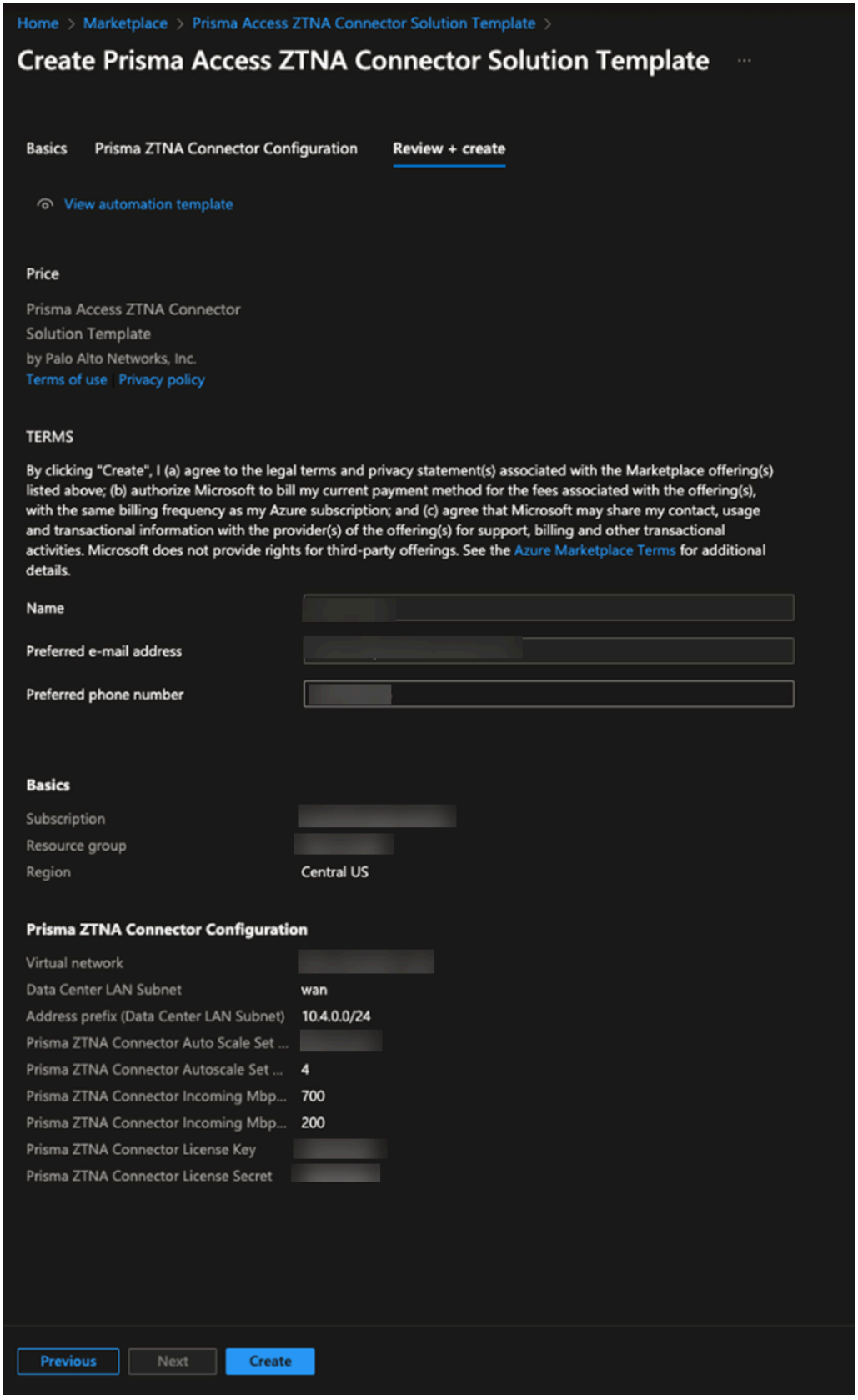



- **Review + create**（檢閱 + 建立）以檢閱您的受管理 Prisma ZTNA 連接器設定。



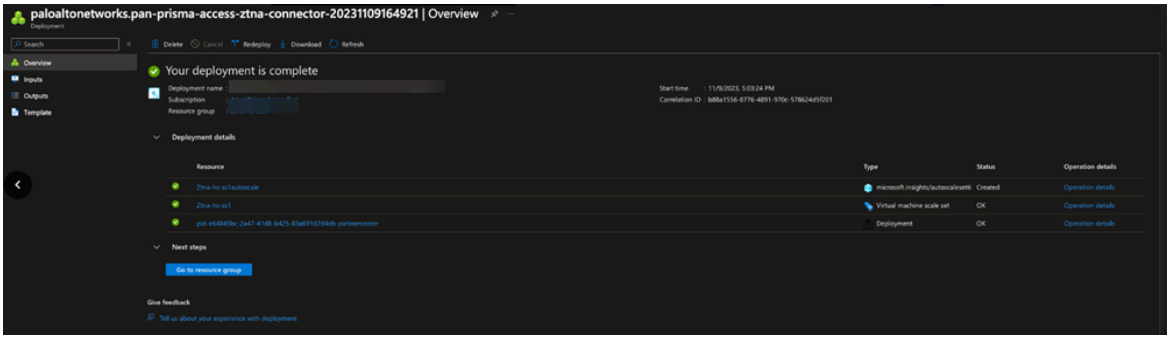

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 確認您提供的詳細資訊，然後按一下 **Create**（建立）以開始虛擬機器部署。




 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 部署完成之後，請選取 **Go to resource group**（前往資源群組）。

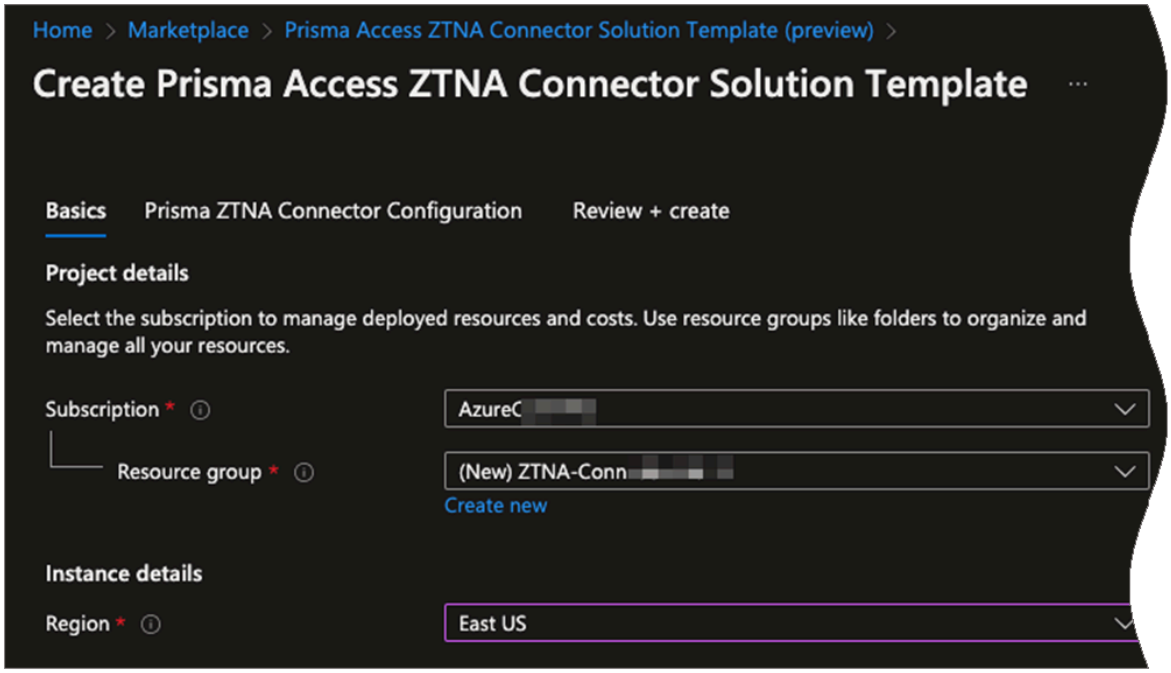



在 **Microsoft Azure** 中部署 **ZTNA** 連接器雙臂

請遵循以下步驟，在 Microsoft Azure 中部署雙臂 ZTNA 連接器：

**STEP 1 |** 在 **Basics**（基本）頁籤上設定以下內容：

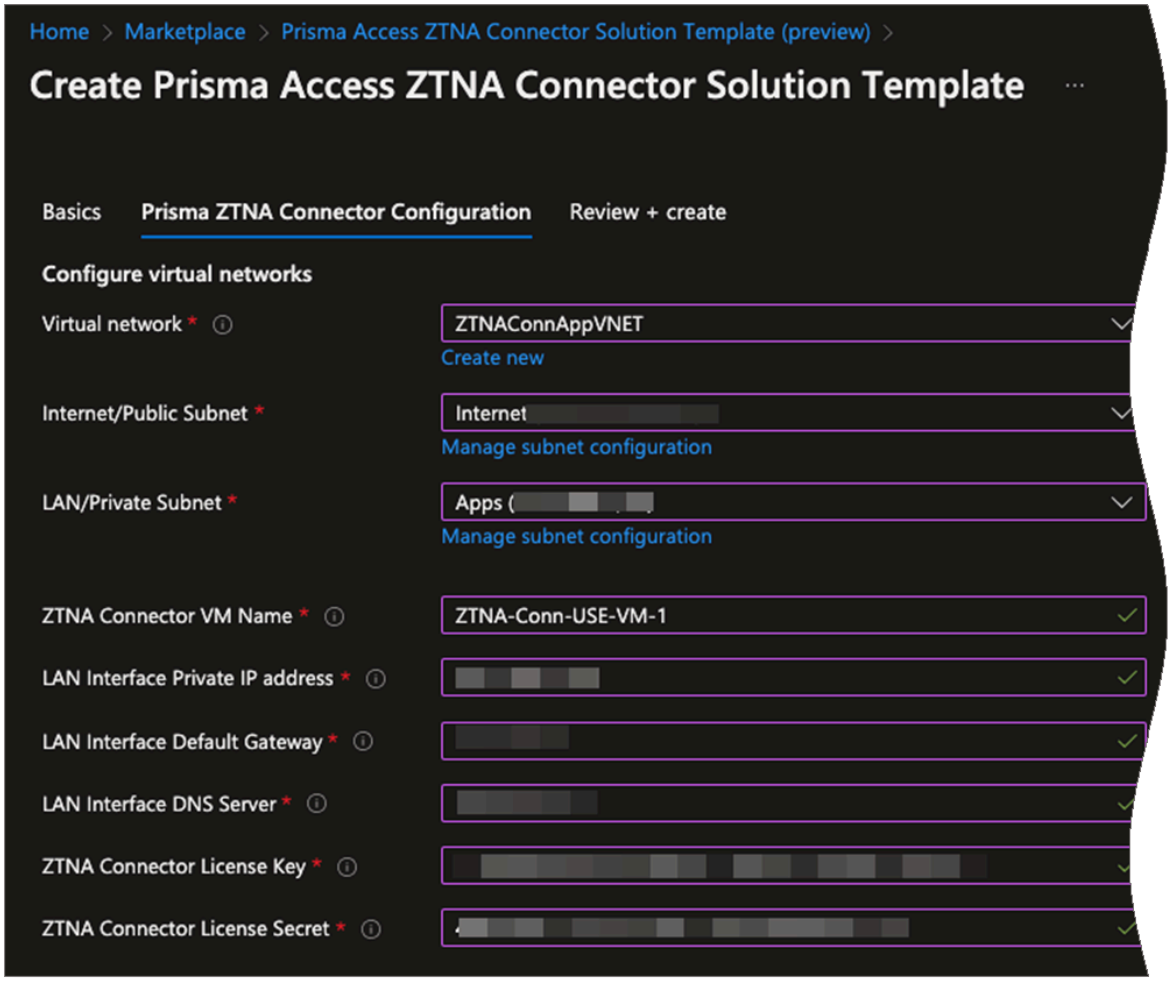
- 選取您的 Azure **Subscription**（訂閱）以管理已部署的資源。
- 選取現有的 **Resource Group**（資源群組）或 **Create new**（建立新的）。
- 選取與您位置相關的 Azure **Region**（區域）。
- 按一下 **Next**（下一步）：**Prisma ZTNA Connector Configuration**（**Prisma ZTNA** 連接器設定）。




 ©2025 Palo Alto Networks, Inc.

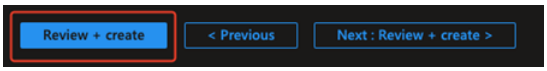
**STEP 2 |** 在 **Next:Prisma ZTNA Connector Configuration**（下一步：**Prisma ZTNA** 連接器設定）頁籤上，設定虛擬網路：

- 建立新的 **Virtual network**（虛擬網路）或使用現有的 **Virtual network**（虛擬網路）。
- 選取 **Internet/Public Subnet**（網際網路/公用子網路），對 IPSec 進行 WAN 連線。您需要具有與 NAT 閘道相關聯的子網路，才能連線網際網路。
- 選取 **Data Center LAN Subnet**（資料中心 **LAN** 子網路），您已在其中佈建了要裝載至此連接器的應用程式。
- 輸入 **Prisma ZTNA Connector VM Name**（**Prisma ZTNA** 連接器 **VM** 名稱）。
- 輸入 **LAN Interface Private IP address**（**LAN** 介面私人 **IP** 位址）。
- 輸入 **LAN Interface Default Gateway**（**LAN** 介面預設閘道）的 IP 位址。
- 輸入 **LAN Interface DNS Server**（**LAN** 介面 **DNS** 伺服器）的 IP 位址。
- 輸入您從 Prisma SASE 入口網站擷取的 **Prisma ZTNA Connector License Key**（**Prisma ZTNA** 連接器授權金鑰）和 **Prisma ZTNA Connector License Secret**（**Prisma ZTNA** 連接器授權密碼）值。




- **Review + create**（檢閱 + 建立）以檢閱您的受管理 Prisma ZTNA 連接器設定。


©2025 Palo Alto Networks, Inc.

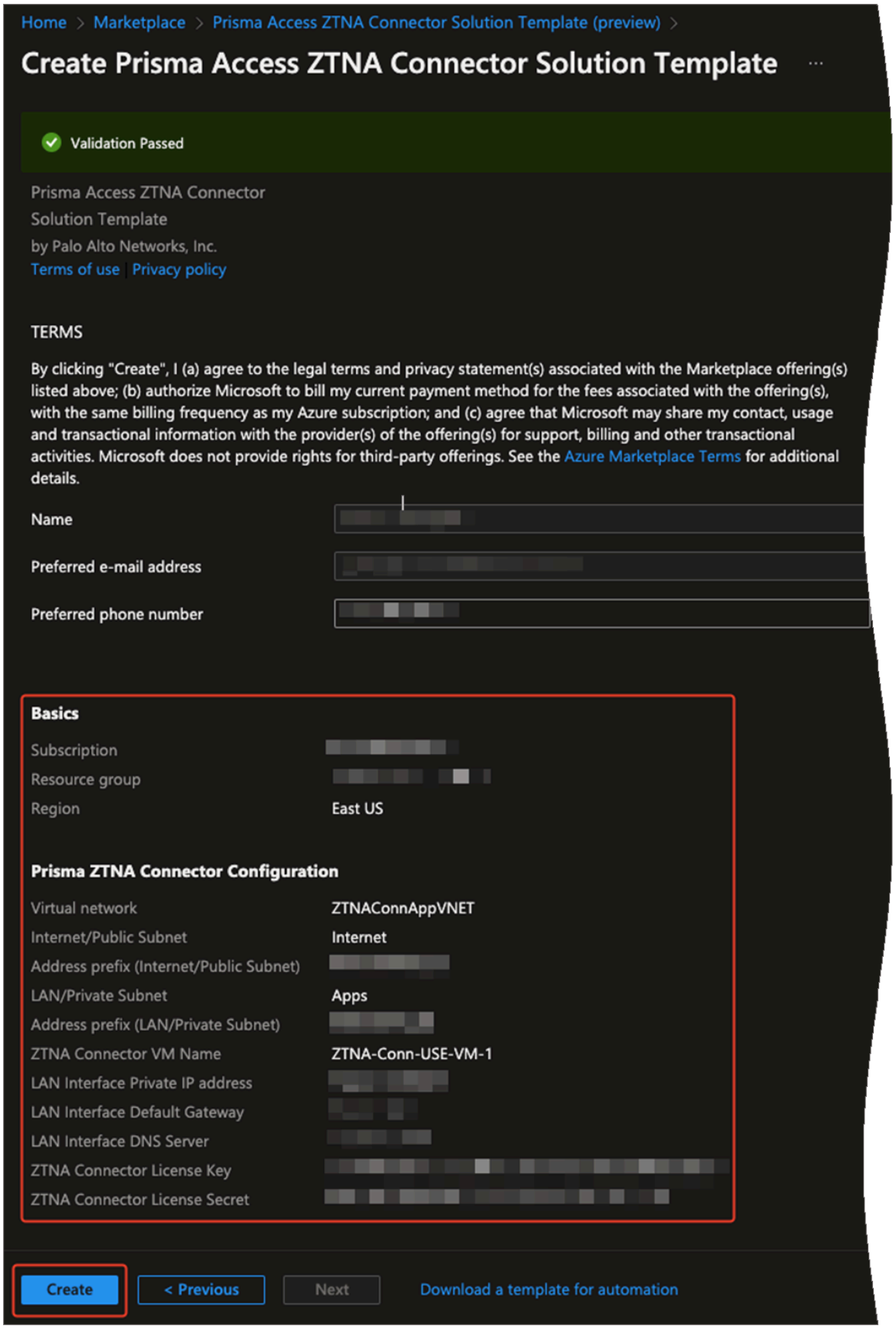




©2025 Palo Alto Networks, Inc.

**STEP 3 |** 確認您提供的詳細資訊，然後按一下 **Create**（建立）以開始虛擬機器部署。

 ©2025 Palo Alto Networks, Inc.



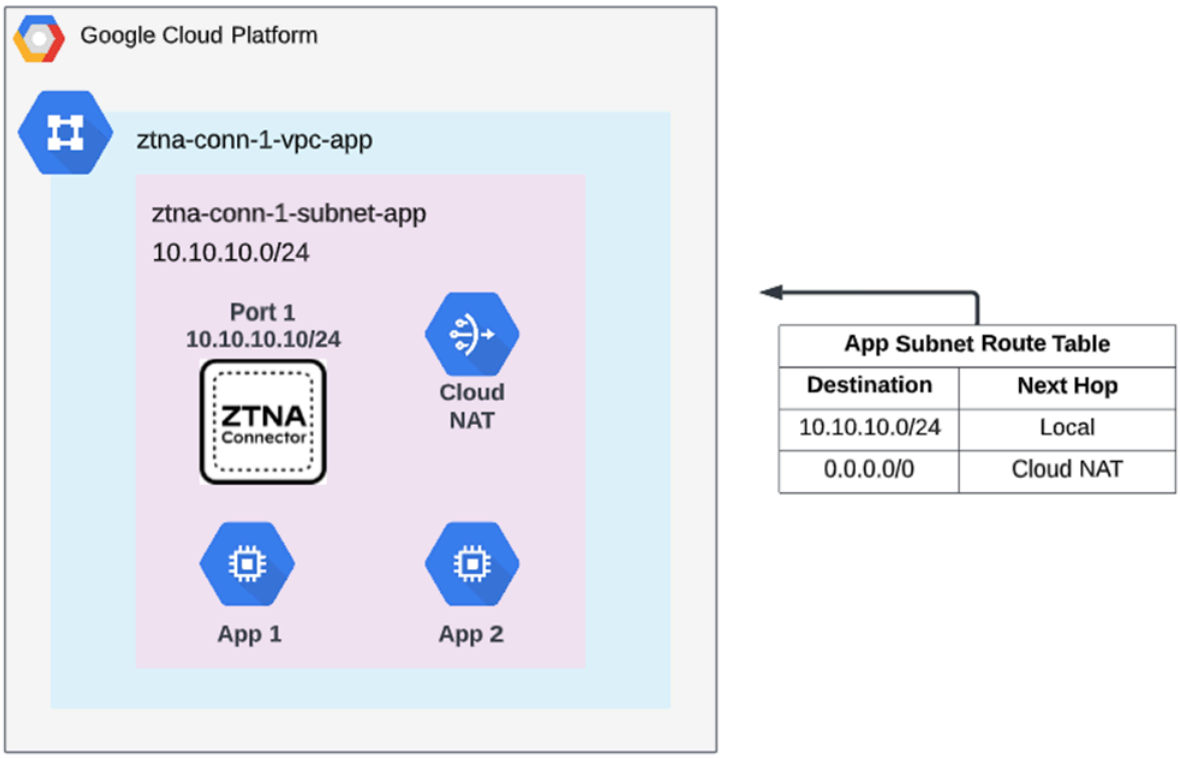

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 部署完成之後，請選取 **Go to resource**（前往資源）。

# ZTNA 連接器支援的 Google Cloud Platform 部署

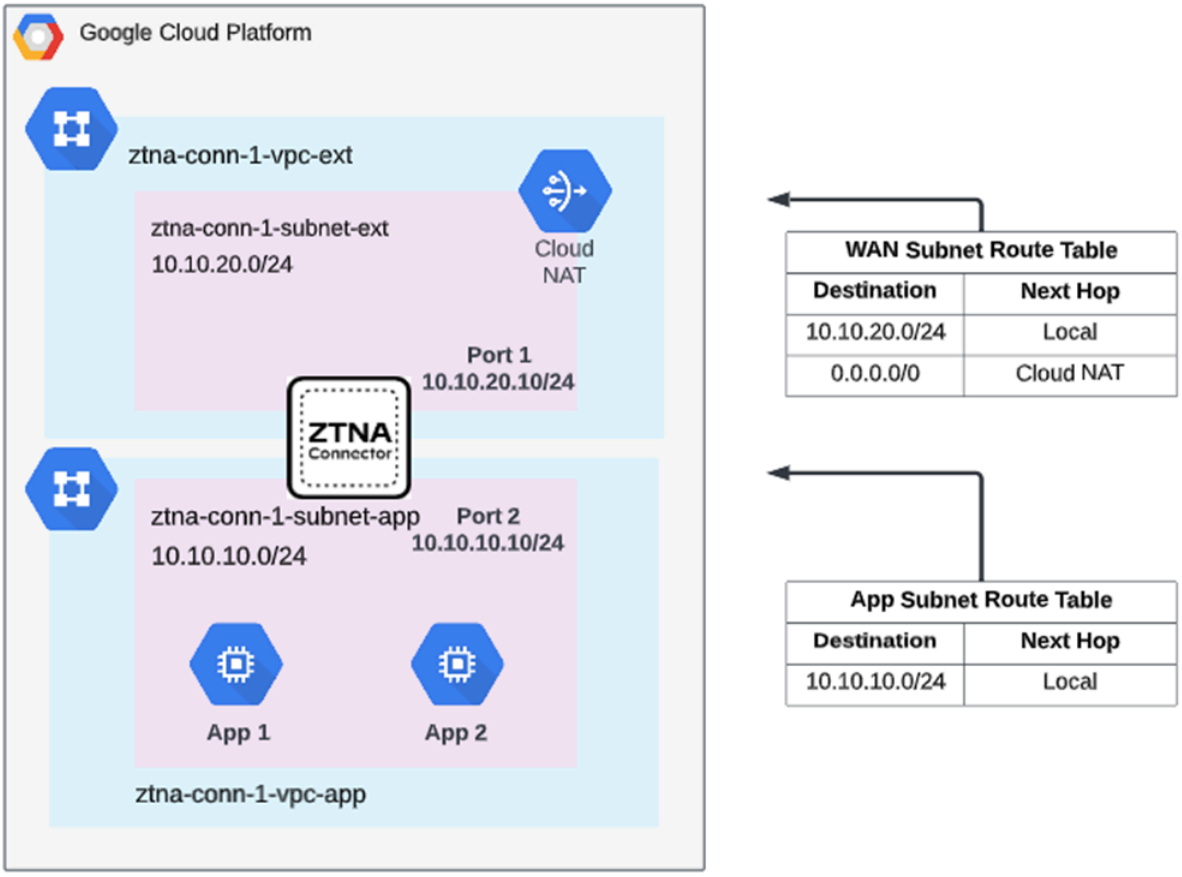
Prisma Access ZTNA 連接器在 Google Cloud Platform (GCP) 中的網路部署支援兩種部署，而且每種部署有一個對應範本。

下圖顯示在 GCP 中使用單臂模式搭配 NAT 閘道進行 Prisma Access ZTNA 連接器部署範例。



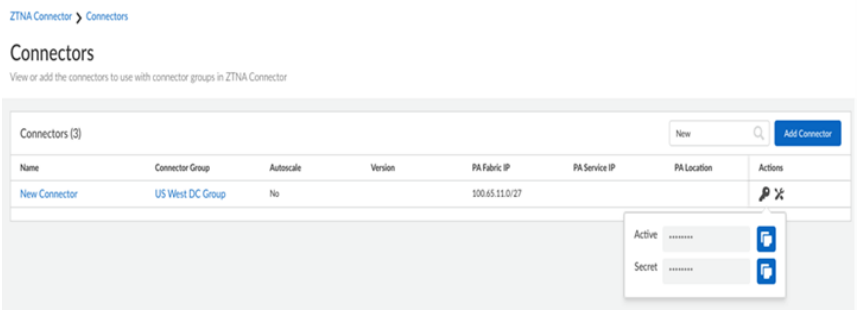

下圖顯示在 GCP 中使用雙臂模式搭配 NAT 閘道進行 Prisma Access ZTNA 連接器部署範例。


©2025 Palo Alto Networks, Inc.




## 在 Google Cloud Platform 中裝載 ZTNA 連接器

- 檢閱需求和指導方針，以及您需要設定的 FQDN 和連接埠，以在 Google Cloud Platform (GCP) 中使用 Prisma Access ZTNA 連接器。
- 擷取並複製 Prisma SASE 入口網站上的連接器金鑰和密碼值：**Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Connectors**（連接器），尋找您在 Prisma Access 建立的連接器物件，以將其與此 VM 建立關聯，並選取 **Copy Token**（複製權杖）；然後，複製 **Key**（金鑰）和 **Secret**（密碼）值。




在符合了所有先決條件之後，請遵循下列步驟，在 GCP 中裝載 Prisma Access ZTNA 連接器。

**STEP 1 |** 前往 GCP Marketplace 並搜尋 **Prisma Access ZTNA Connector**（**Prisma Access ZTNA** 連接器）。

 ©2025 Palo Alto Networks, Inc.

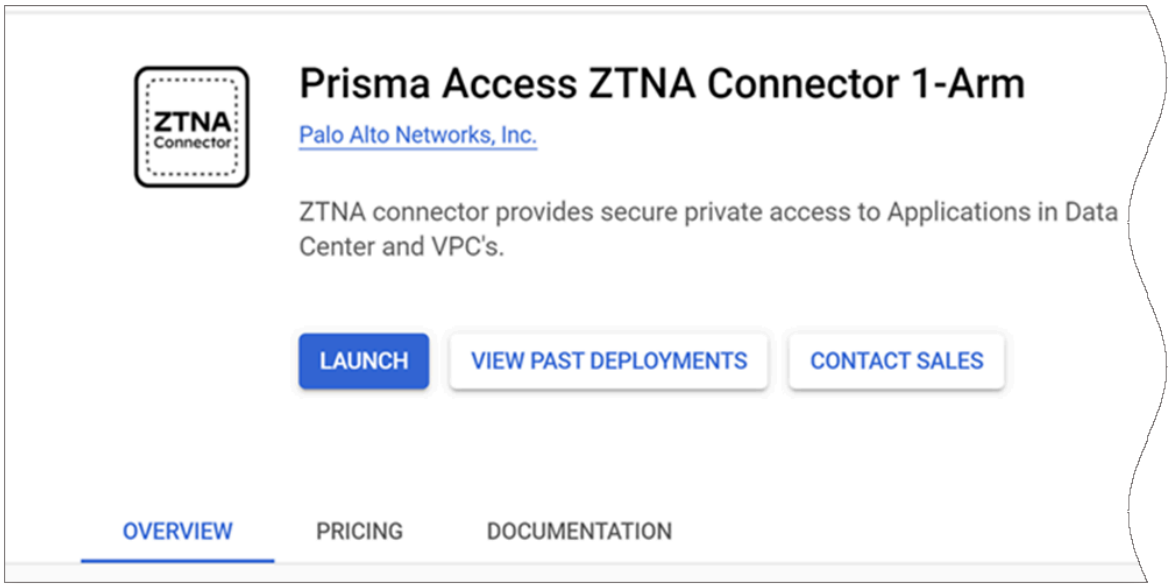
**STEP 2 |** 選擇最符合您需求的軟體計劃。

- Prisma Access ZTNA 連接器單臂
- Prisma Access ZTNA 連接器雙臂

在 **GCP** 中部署 **ZTNA** 連接器單臂

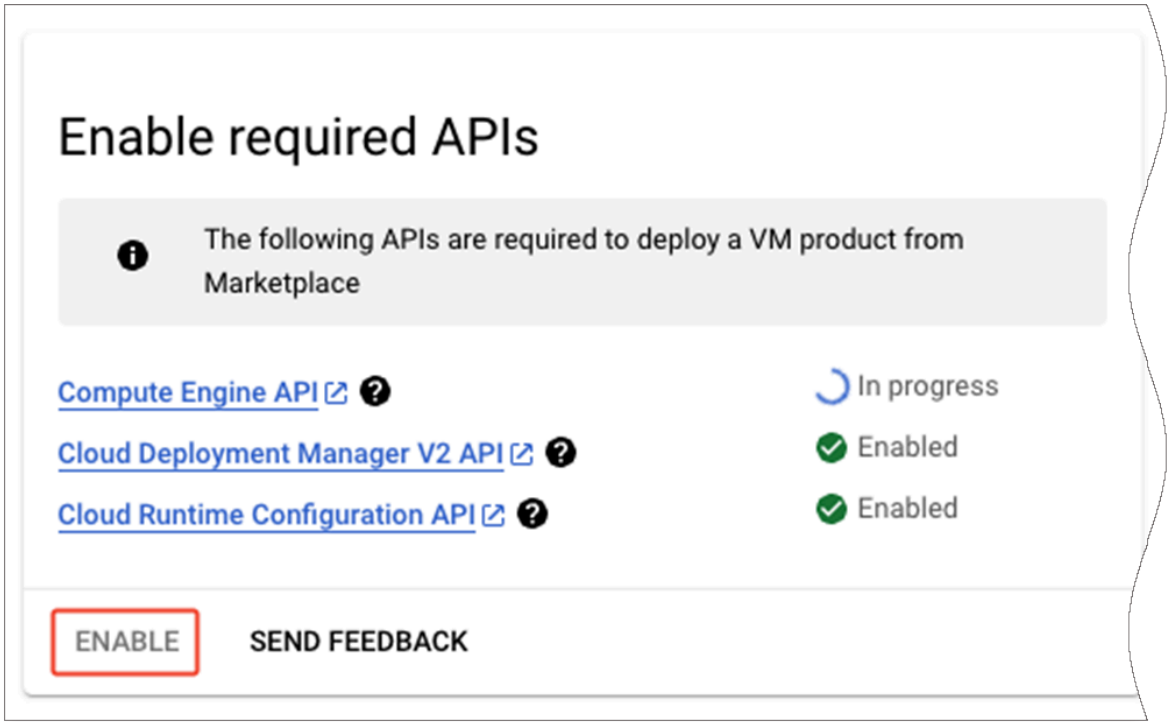
請遵循下列步驟，在 GCP 中部署 ZTNA 連接器單臂：

**STEP 1 |** **LAUNCH**（啟動）以設定 ZTNA 連接器單臂。




 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** （選用）**Enable**（啟用）從 Marketplace 部署虛擬機器所需的 GCP API。

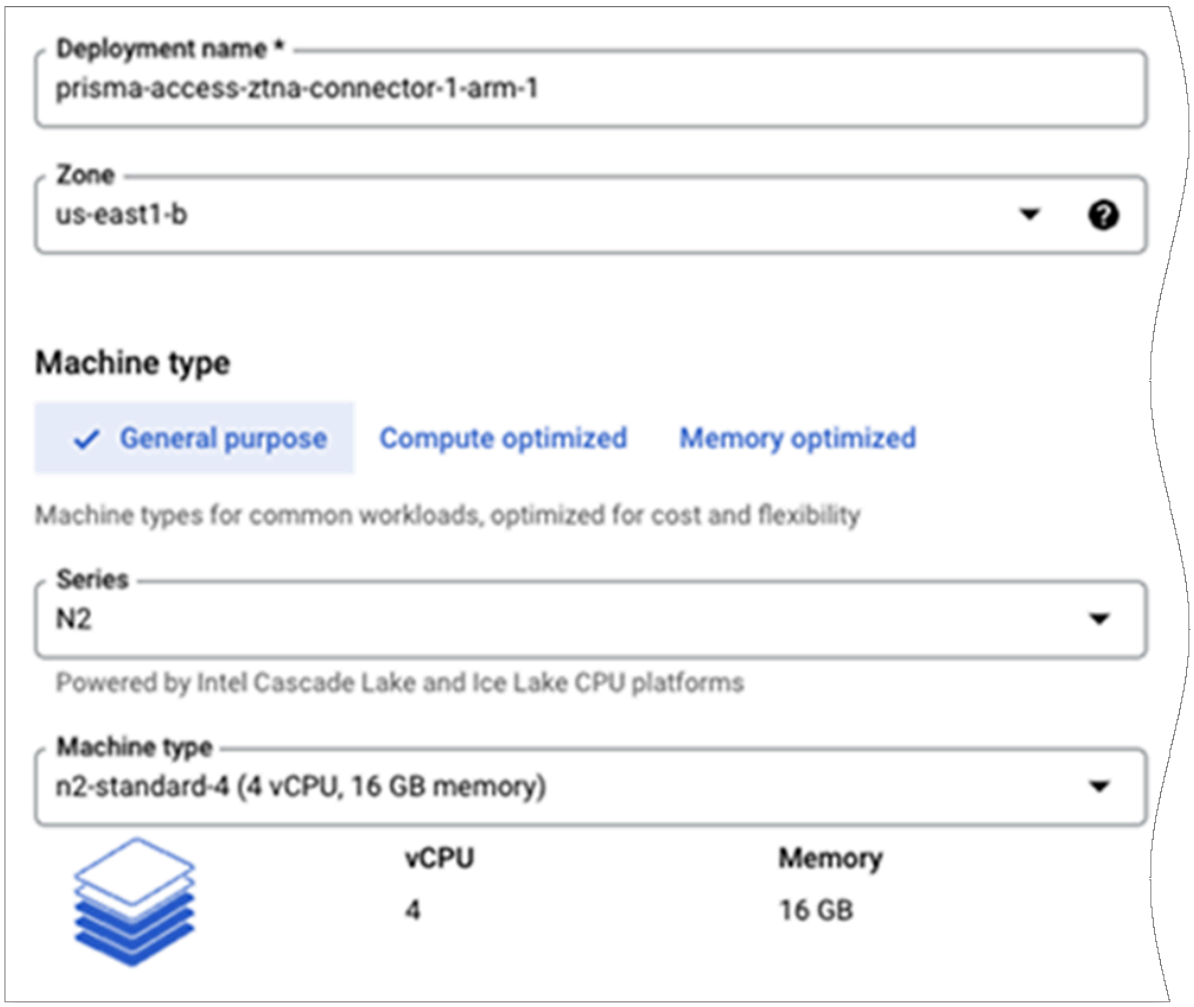




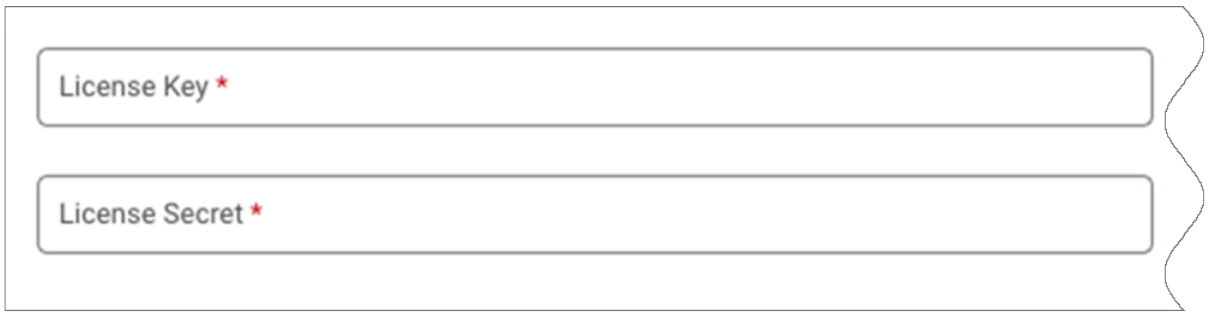
©2025 Palo Alto Networks, Inc.

**STEP 3 |** 設定下列項目：

- 輸入可讓您識別虛擬機器的 **Deployment Name**（部署名稱）。
- 為此連接器選取應用程式所在的 **Zone**（區域）。
- 對 **Machine type**（機器類型）使用預設值。此連接器的合格機器類型是 **n2-standard-4**。

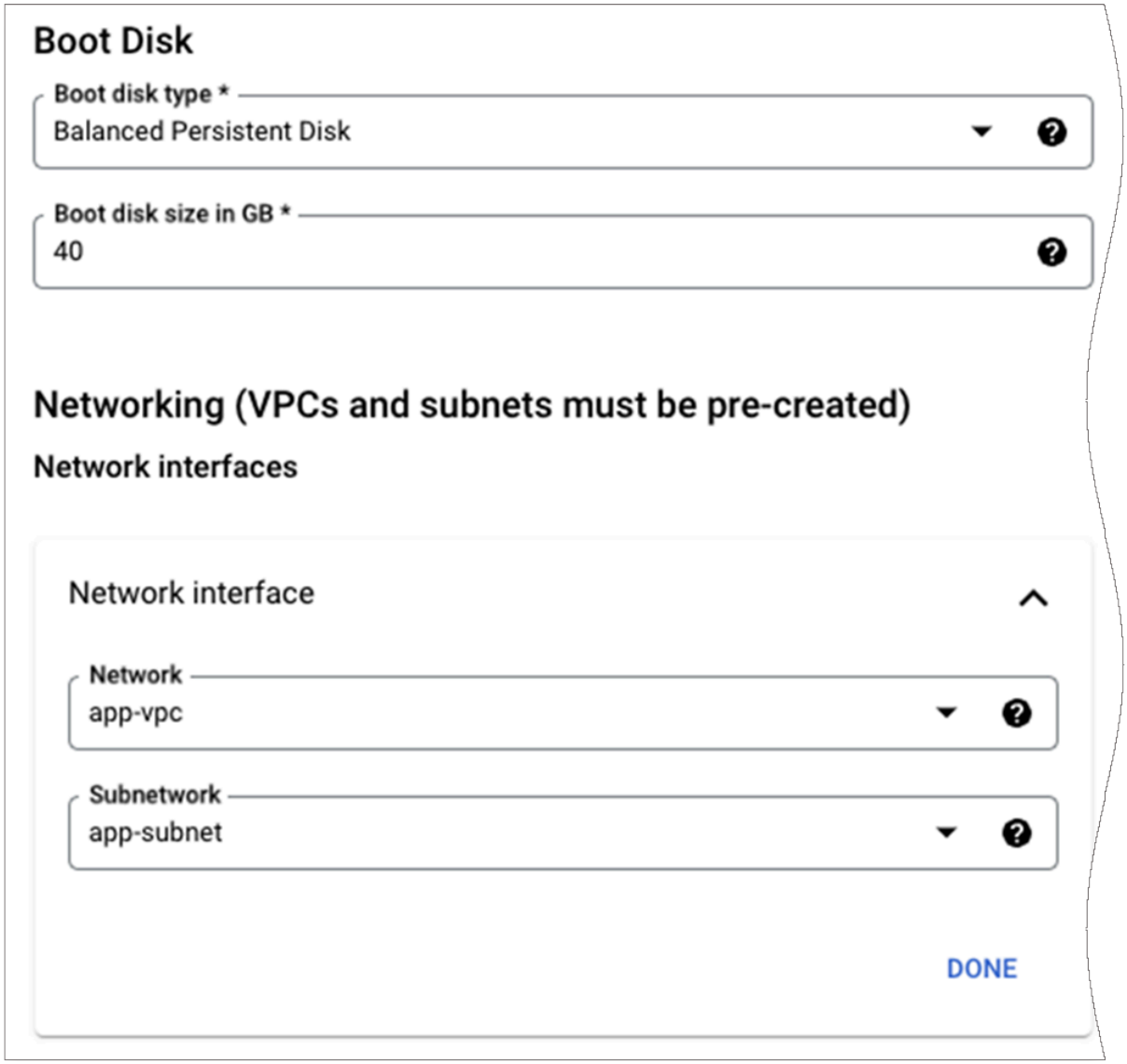



- 輸入您從 Prisma SASE 入口網站擷取的 **Prisma ZTNA Connector License Key**（**Prisma ZTNA** 連接器授權金鑰）和 **Prisma ZTNA Connector License Secret**（**Prisma ZTNA** 連接器授權密碼）值。




 ©2025 Palo Alto Networks, Inc.

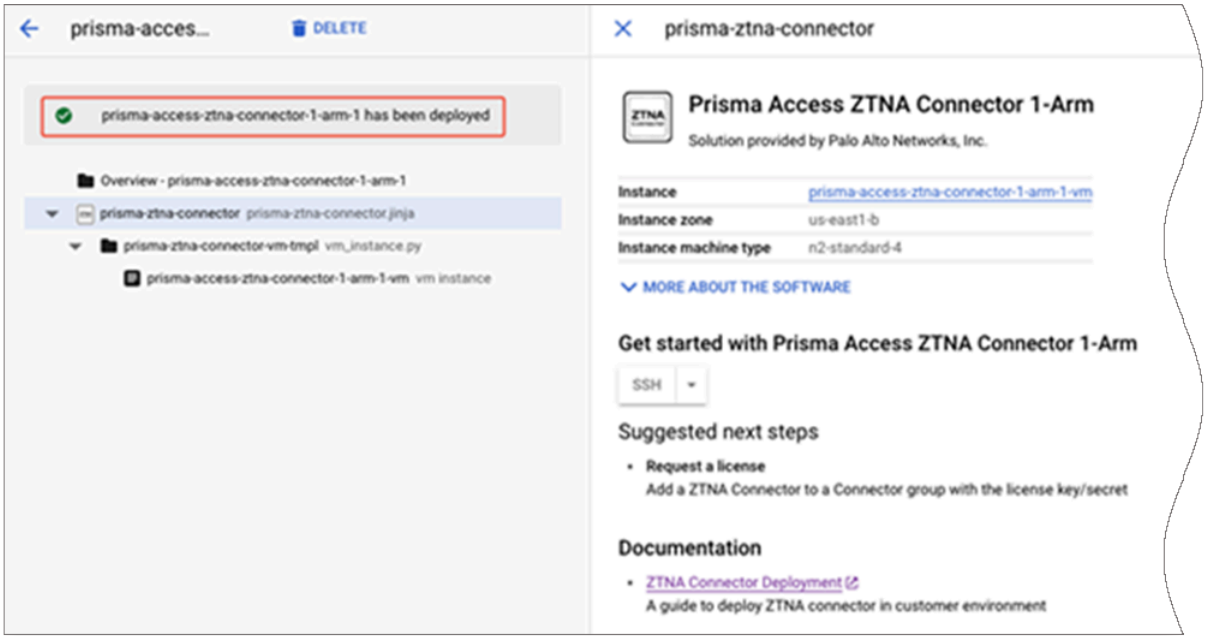
- 在 **Boot Disk**（開機磁碟）區段中設定以下內容：
  - 使用預設的 **Boot disk type**（開機磁碟類型）。
  - 選取 **40 GB** 作為 **Boot disk size in GB**（開機磁碟大小（以 **GB** 為單位））。
- 展開 **Networking (VPCs and subnets must be pre-created)**（網路（必須預先建立 **VPC** 和子網路））區段，並選取 **Network interface**（網路介面） 詳細資訊。
  - 選取包含您所建立子網路的 **Network**（網路）。
  - 選取 **Subnetwork**（子網路）供虛擬機器使用。




**STEP 4 |** 按一下 **Done**（完成）。

 ©2025 Palo Alto Networks, Inc.

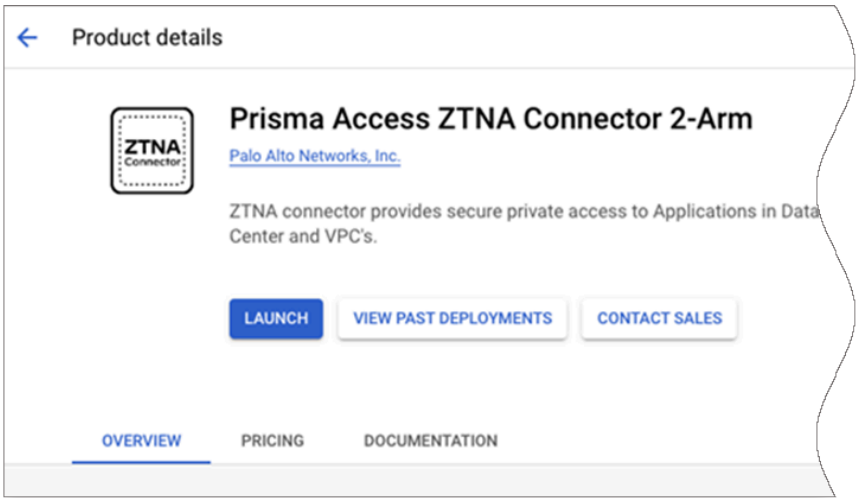
**STEP 5 |** 按一下 **Deploy**（部署）以完成裝載程序。




在 **GCP** 中部署 **ZTNA** 連接器雙臂

請遵循下列步驟，在 GCP 中部署 ZTNA 連接器：

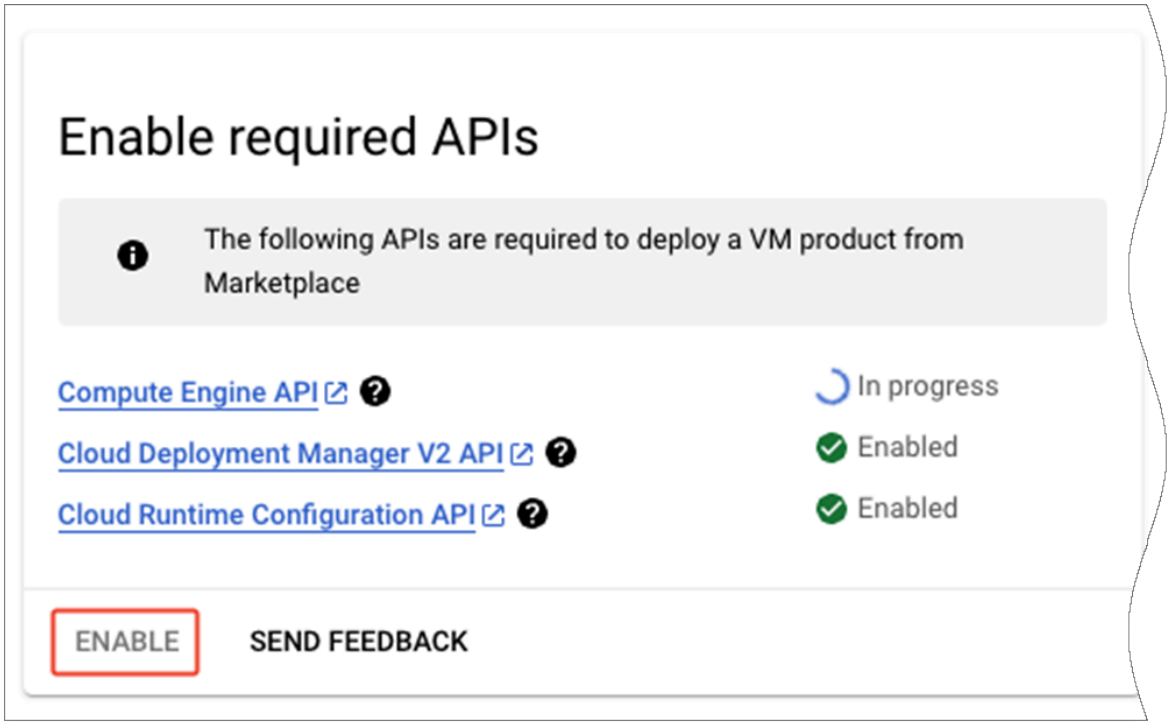
**STEP 1 |** **LAUNCH**（啟動）以進行設定。





©2025 Palo Alto Networks, Inc.

**STEP 2 |** （選用）**Enable**（啟用）從 Marketplace 部署虛擬機器所需的 API。

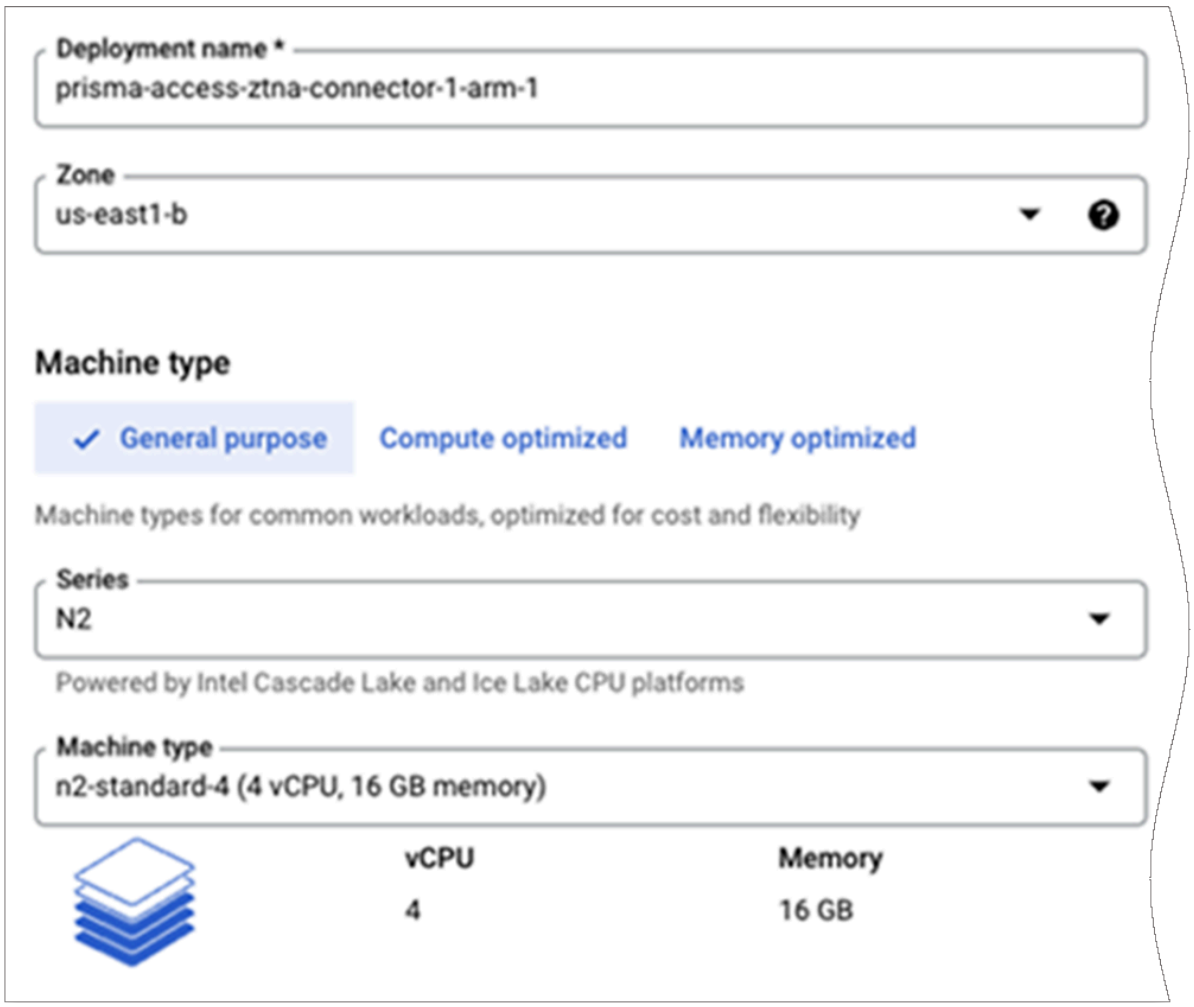




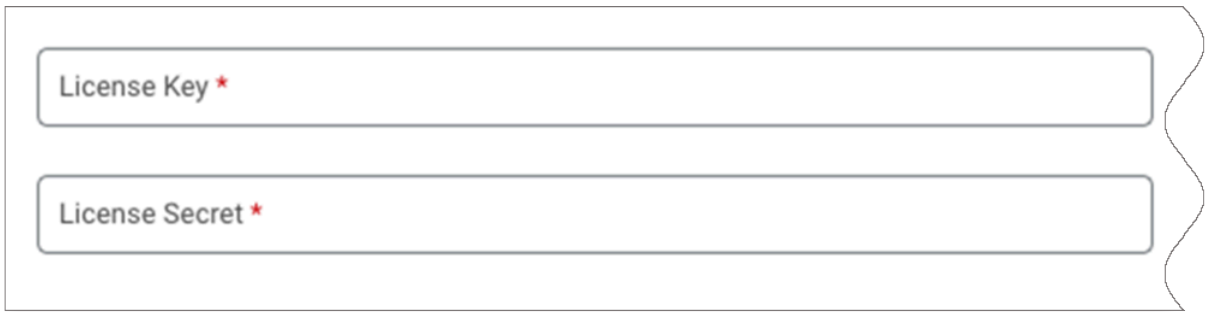
©2025 Palo Alto Networks, Inc.

**STEP 3 |** 設定下列項目：

- 輸入可讓您識別虛擬機器的 **Deployment Name**（部署名稱）。
- 為此連接器選取應用程式所在的 **Zone**（區域）。
- 對 **Machine type**（機器類型）使用預設值。此連接器的合格機器類型是 **n2-standard-4**。

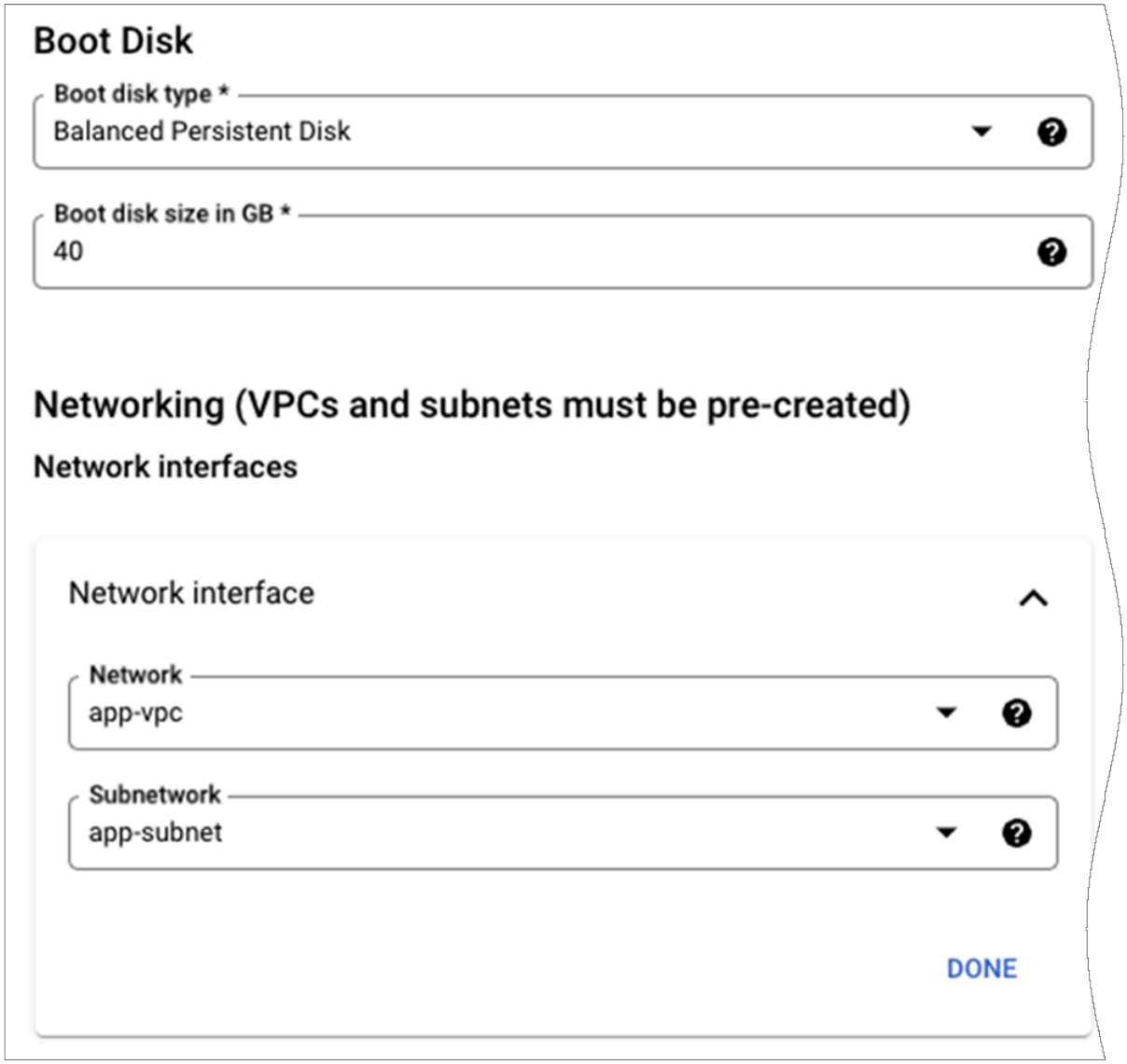



- 輸入您從 Prisma SASE 入口網站擷取的 **Prisma ZTNA Connector License Key**（**Prisma ZTNA** 連接器授權金鑰）和 **Prisma ZTNA Connector License Secret**（**Prisma ZTNA** 連接器授權密碼）值。



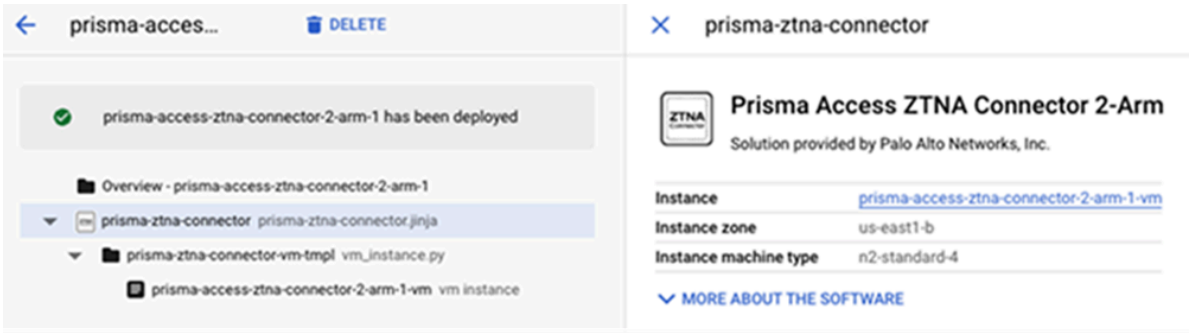

 ©2025 Palo Alto Networks, Inc.

- 在 **Boot Disk**（開機磁碟）區段中：
  - 使用預設的 **Boot disk type**（開機磁碟類型）。
  - 選取 **40 GB** 作為 **Boot disk size in GB**（開機磁碟大小（以 **GB** 為單位））。
- 展開 **Networking (VPCs and subnets must be pre-created)**（網路（必須預先建立 **VPC** 和子網路））區段，並選取 **Network interface**（網路介面） 詳細資訊。
  - 選取包含您所建立子網路的 **Network**（網路）。
  - 選取 **Subnetwork**（子網路）供虛擬機器使用。




 ©2025 Palo Alto Networks, Inc.

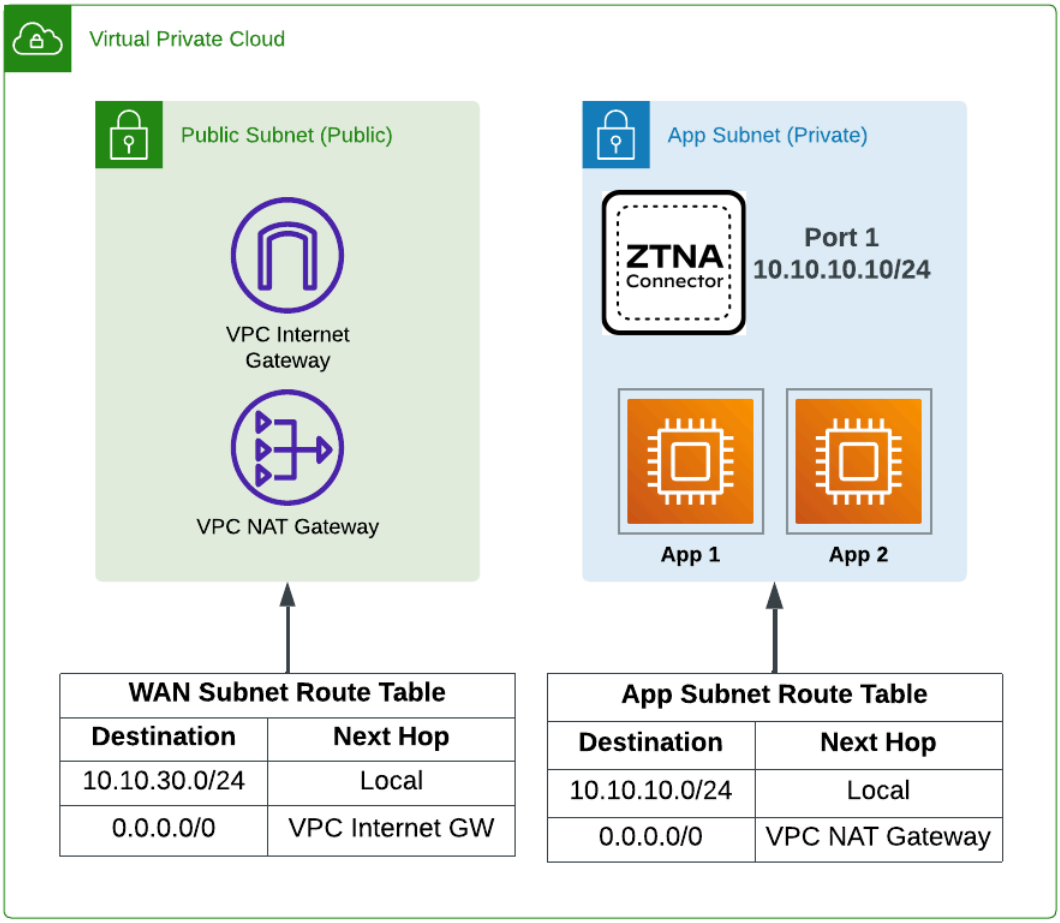
**STEP 4 |** 按一下 **Deploy**（部署）以完成裝載程序。




## ZTNA 連接器支援 Amazon Web Services 部署

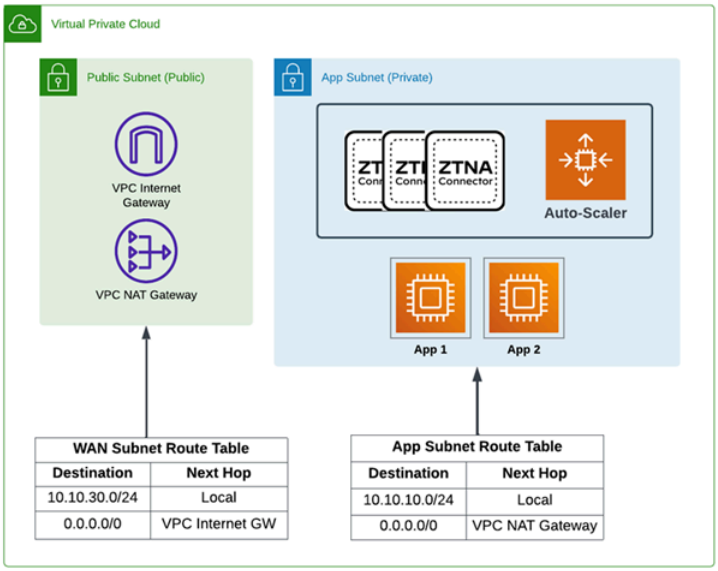
Prisma Access ZTNA 連接器在 Amazon Web Services (AWS) 中的網路部署支援三種部署，以及每種部署有一個對應範本。

下圖顯示在 AWS 中使用單臂模式搭配 NAT 閘道進行 Prisma Access ZTNA 連接器部署範例。

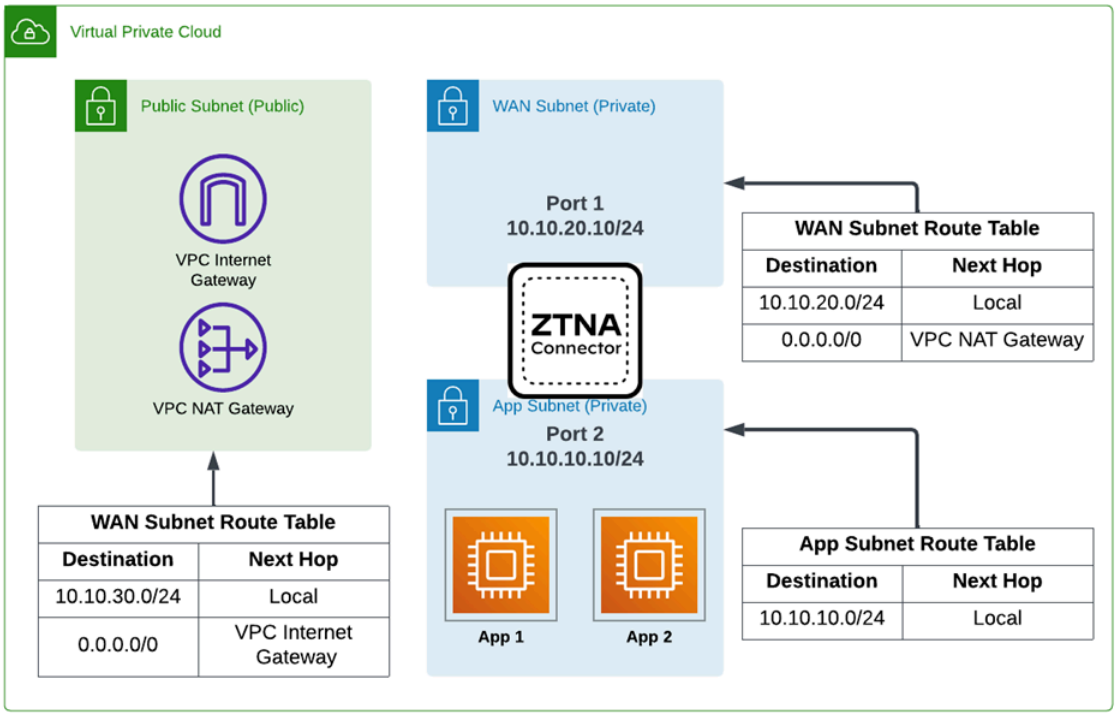



下圖顯示在 AWS 中使用單臂模式搭配 NAT 閘道進行 ZTNA 連接器部署範例。


©2025 Palo Alto Networks, Inc.




下圖顯示在 AWS 中使用雙臂模式搭配 NAT 閘道進行 ZTNA 連接器部署範例。

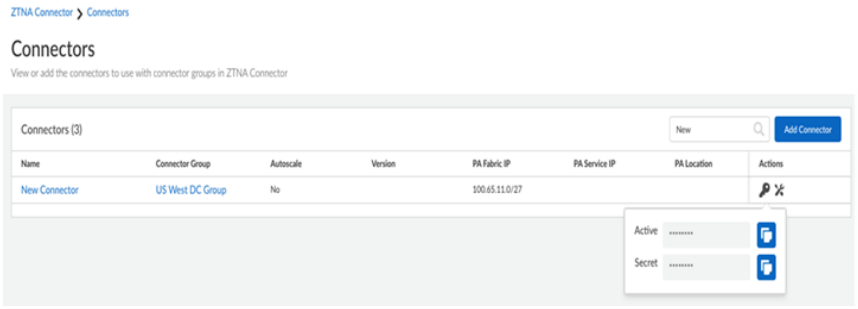



## 在 Amazon Web Services 中裝載 ZTNA 連接器

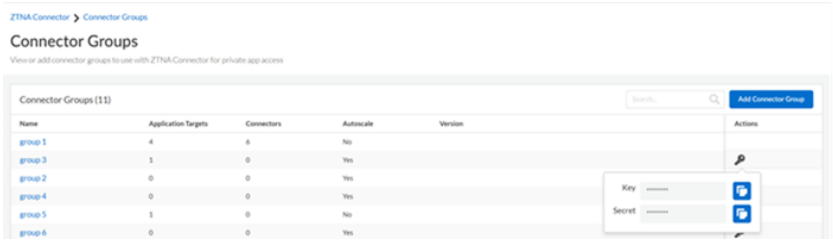
- 檢閱需求和指導方針，以及您需要設定的 FQDN 和連接埠，以在 Amazon Web Services (AWS) 中使用 ZTNA 連接器。
- 在 Prisma SASE 平台上，擷取並複製連接器金鑰和密碼值：**Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Connectors**（連接器），尋找您在 Prisma Access 建立的連接


©2025 Palo Alto Networks, Inc.

器物件，以將其與此 VM 建立關聯，並選取 **Copy Token**（複製權杖）；然後，複製 **Key**（金鑰）和 **Secret**（密碼）值。




- 對於 **Prisma Access ZTNA** 連接器單臂自動調整部署，您必須擷取並複製連接器群組金鑰和密碼值：**Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Connectors Groups**（連接器群組），尋找您在 Prisma Access 建立的連接器群組物件，以將其與此 VM 建立關聯；並選取 **Copy Token**（複製權杖），然後，複製 **Key**（金鑰）和 **Secret**（密碼）。




在符合了所有先決條件之後，請遵循下列步驟，在 AWS 中裝載 Prisma Access ZTNA 連接器。

**STEP 1 |** 前往 AWS Marketplace，並搜尋 **Prisma Access ZTNA Connector**（**Prisma Access ZTNA** 連接器）。

**STEP 2 |** 選擇最符合您需求的軟體計劃。

- Prisma Access ZTNA 連接器單臂
- Prisma Access ZTNA 連接器單臂自動調整
- Prisma Access ZTNA 連接器雙臂

在 **AWS** 中部署 **ZTNA** 連接器單臂

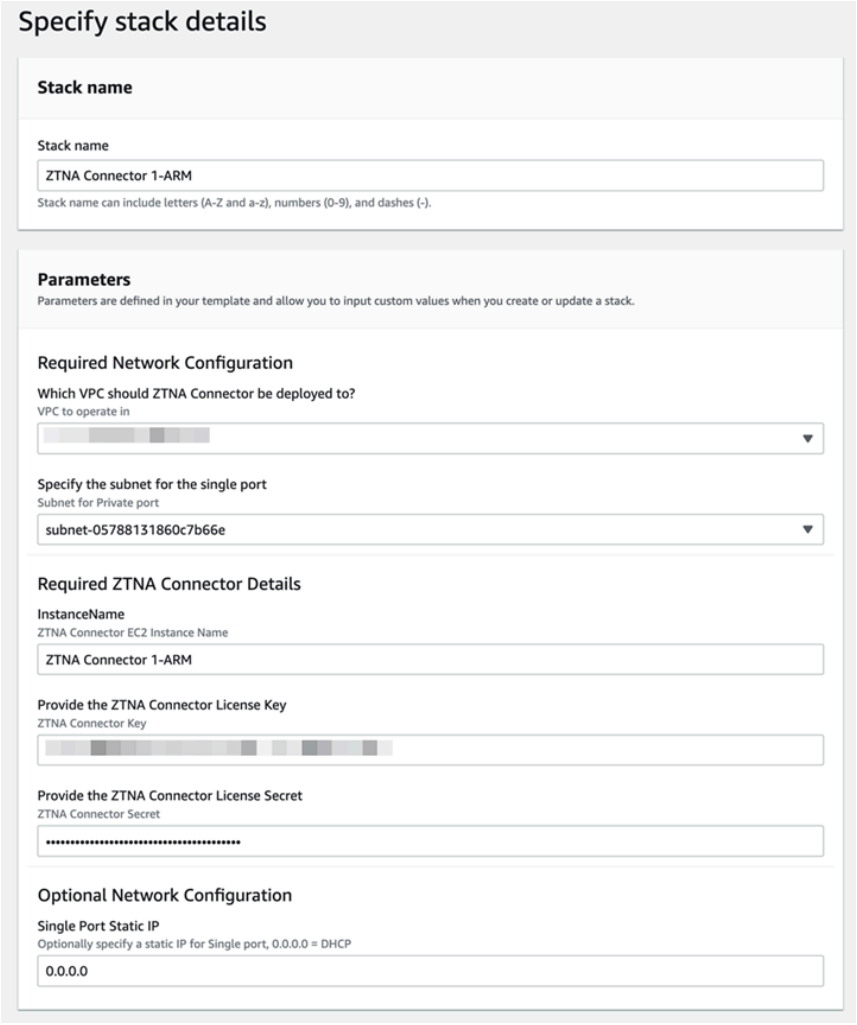
請遵循下列步驟，在 AWS 中部署 ZTNA 連接器單臂。

**STEP 1 |** 選取 **Prisma Access ZTNA Connector 1-Arm**（**Prisma Access ZTNA** 連接器單臂）Cloud Formation 範本。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 在 **Specify stack details**（指定堆疊詳細資訊）頁面上設定這些項目：

- 輸入 **Stack name**（堆疊名稱）以識別堆疊。
- 在 **Parameters**（參數）區段中，指定堆疊範本中定義的參數。
  - 選取 **Which VPC should ZTNA Connector be deployed to**（應將 **ZTNA** 連接器部署到哪個 **VPC**）。
  - **Specify the subnet for the single port**（指定單一連接埠的子網路），您已在其中佈建要裝載至此連接器的應用程式。您需要透過 NAT 閘道從這個子網路存取網際網路。
- 輸入您從 Prisma SASE 入口網站擷取的 Prisma **ZTNA Connector License Key**（**ZTNA** 連接器授權金鑰）和 Prisma **ZTNA Connector License Secret**（**ZTNA** 連接器授權密碼）值。




## 在 AWS 中部署搭配自動調整的 ZTNA 連接器單臂

請遵循下列步驟，在 AWS 中部署搭配自動調整的 ZTNA 連接器單臂。

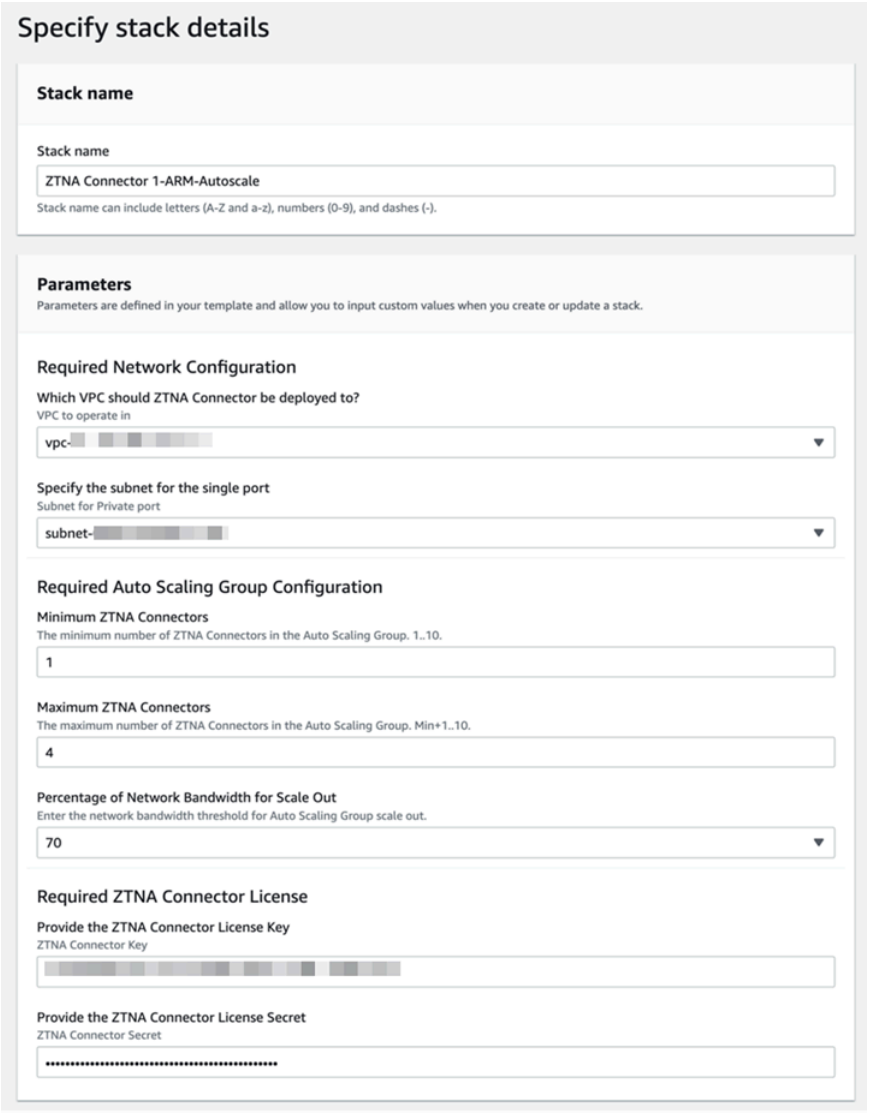
**STEP 1 |** 選取 **Prisma Access ZTNA Connector 1-Arm Auto-Scaling**（**Prisma Access ZTNA** 連接器單臂自動調整）Cloud Formation 範本。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 在 **Specify stack details**（指定堆疊詳細資訊）頁面上設定下列參數：

- 為部署輸入唯一的 **Stack name**（堆疊名稱）。
- 在 **Parameters**（參數）區段中指定堆疊範本中定義的參數：
  - 選取 **Which VPC should ZTNA Connector be deployed to**（應將 **ZTNA** 連接器部署到哪個 **VPC**）。
  - **Specify the subnet for the single port**（指定單一連接埠的子網路），您已在其中佈建要裝載至此連接器的應用程式。您需要透過 NAT 閘道從這個子網路存取網際網路。
- 在 **Required Auto Scaling Group Configuration**（必要的自動調整群組設定）中：
  - 輸入自動調整群組中所需的 **Minimum ZTNA Connectors**（**ZTNA** 連接器數目下限）。
  - 輸入自動調整群組中所需的 **Maximum ZTNA Connectors**（**ZTNA** 連接器數目上限）。連接器群組中允許的 ZTNA 連接器數目上限為 4。
  - 設定 **Percentage of Network Bandwidth for Scale Out**（網路頻寬用於相應放大的百分比）。預設值和建議值為 70%。
- 輸入您從 Prisma SASE 入口網站擷取的 Prisma **ZTNA Connector License Key**（**ZTNA** 連接器授權金鑰）和 **ZTNA Connector License Secret**（**ZTNA** 連接器授權密碼）值。


©2025 Palo Alto Networks, Inc.




## 在 **AWS** 中部署 **ZTNA** 連接器雙臂

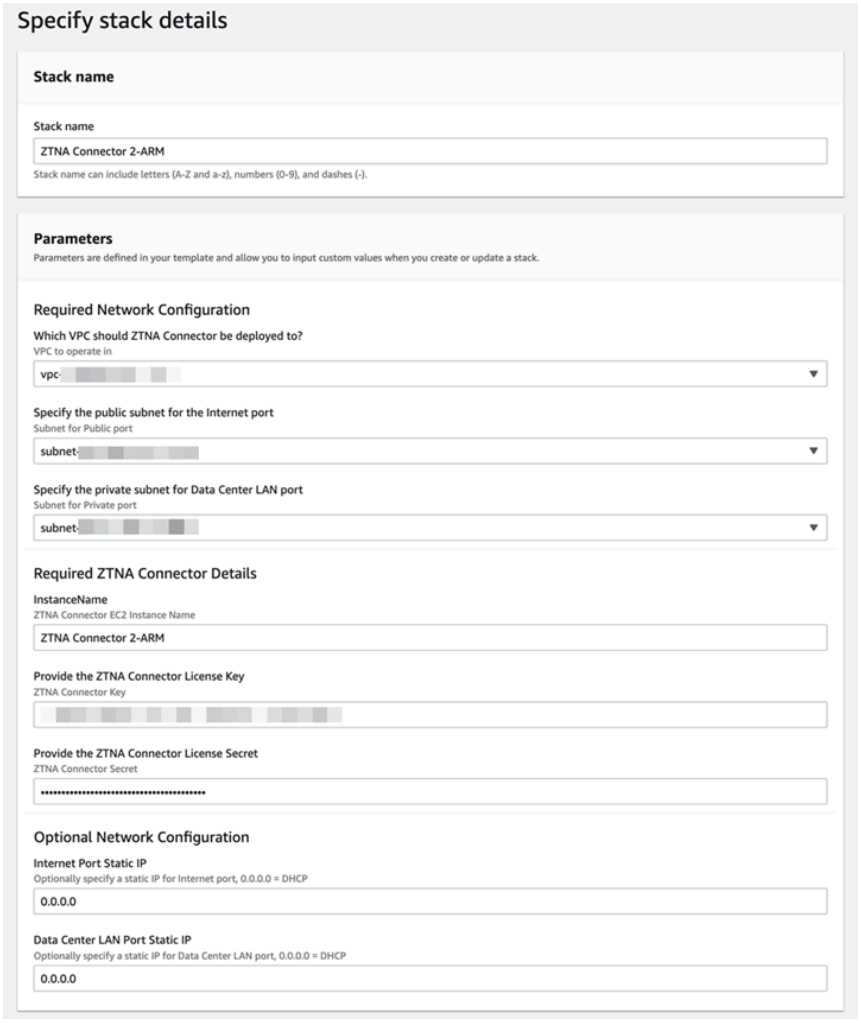
請遵循下列步驟，在 AWS 中部署 ZTNA 連接器雙臂。

**STEP 1 |** 選取 Prisma Access ZTNA 連接器單臂部署 Cloud Formation 範本。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 在 **Specify stack details**（指定堆疊詳細資訊）頁面上：

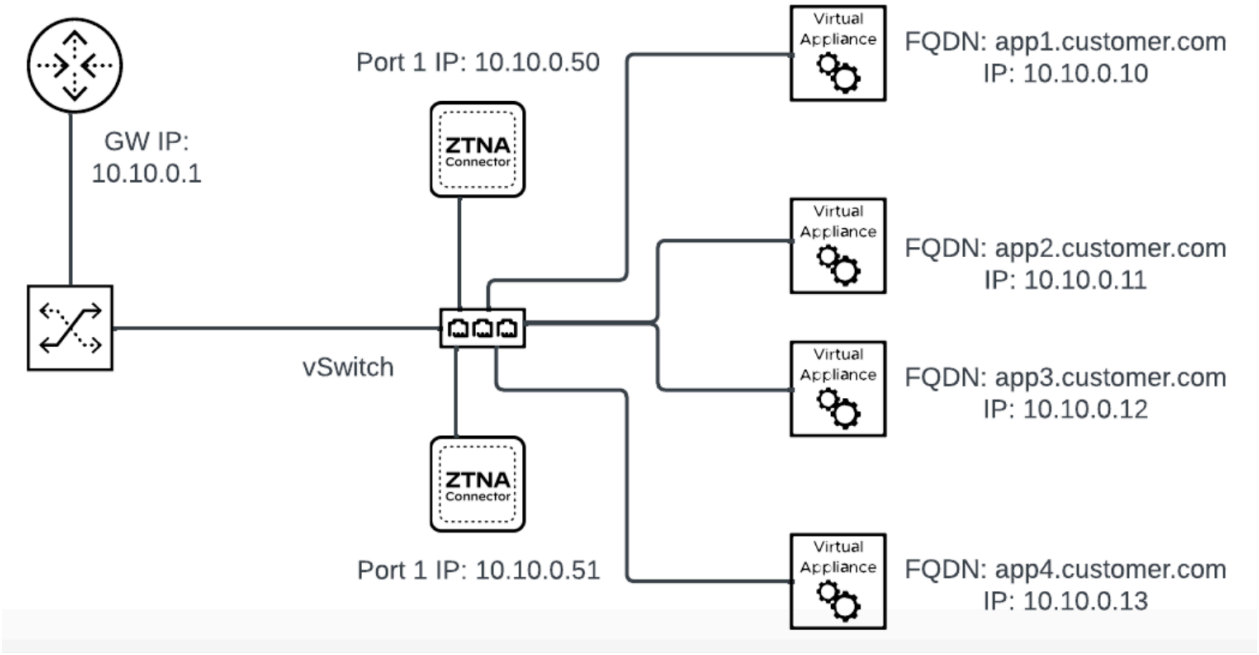
- 為部署輸入 **Stack name**（堆疊名稱）。
- 在 **Parameters**（參數）區段中指定您堆疊範本中定義的參數。
  - 選取 **Which VPC should ZTNA Connector be deployed to**（應將 **ZTNA** 連接器部署到哪個 **VPC**）。
  - **Specify the public subnet for the Internet port**（為網際網路連接埠指定公用子網路），用於對 IPSec 進行 WAN 連線。此子網路需要與 NAT 閘道相關聯，才能連線網際網路。
  - **Specify the private subnet for Data Center LAN port**（為資料中心 **LAN** 連接埠指定私人子網路），您已在其中佈建要裝載至此連接器的應用程式。
- 輸入 **Instance Name**（執行個體名稱）
- 輸入您從 Prisma SASE 入口網站擷取的 Prisma **ZTNA Connector License Key**（**ZTNA** 連接器授權金鑰）和 Prisma **ZTNA Connector License Secret**（**ZTNA** 連接器授權密碼）值。



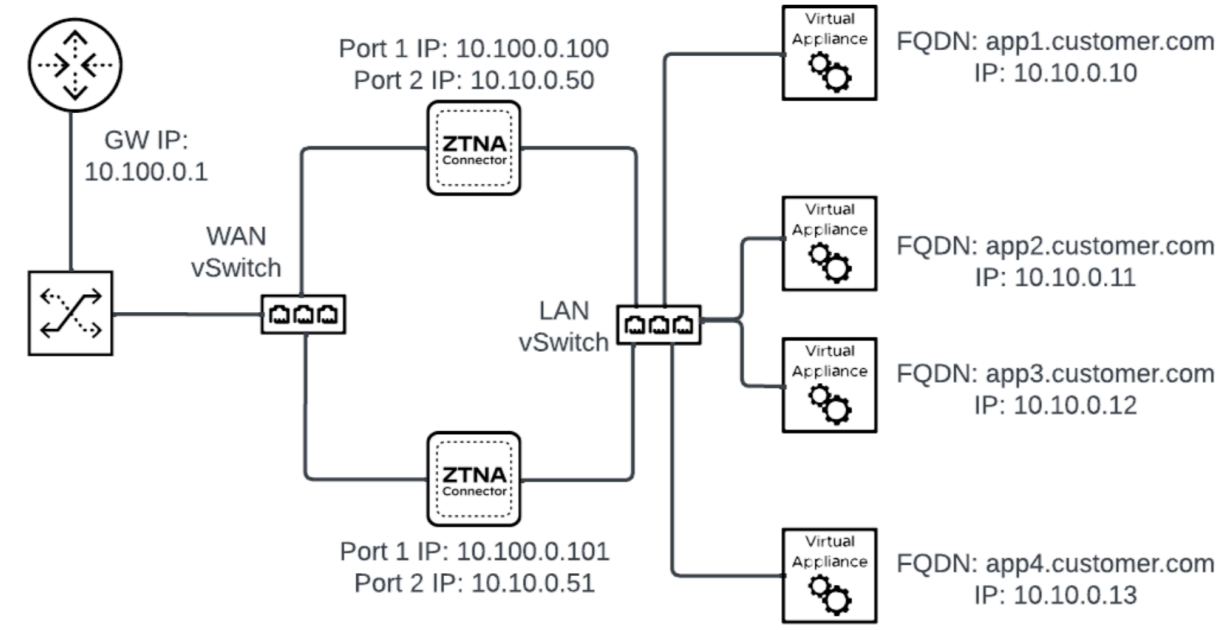

# Prisma Access ZTNA 連接器支援的 VMware ESXi 部署

下圖顯示在單臂模式下使用 VMware ESXi 搭配 NAT 閘道進行 ZTNA 連接器網路部署範例。

 ©2025 Palo Alto Networks, Inc.




下圖顯示在雙臂模式下使用 VMware ESXi 搭配 NAT 閘道進行 ZTNA 連接器網路部署範例。




## 在 VMware ESXi 中裝載 ZTNA 連接器

若要在 VMware ESXi 中裝載 ZTNA 連接器，請完成以下步驟。開始之前，通常務必檢閱 ZTNA 的需求和指導方針，特別是 VMware ESXi 部署。

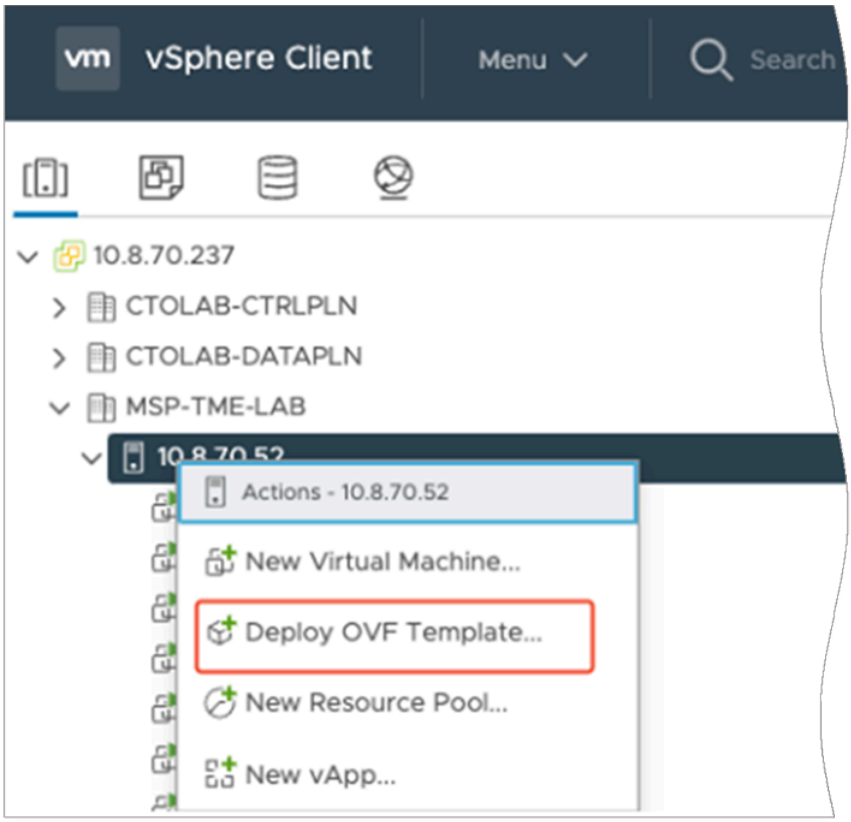
開始之前，檢閱需求和指導方針，以及您需要設定的 FQDN 和連接埠，以使用 ZTNA 連接器搭配 VMware ESXi。


©2025 Palo Alto Networks, Inc.

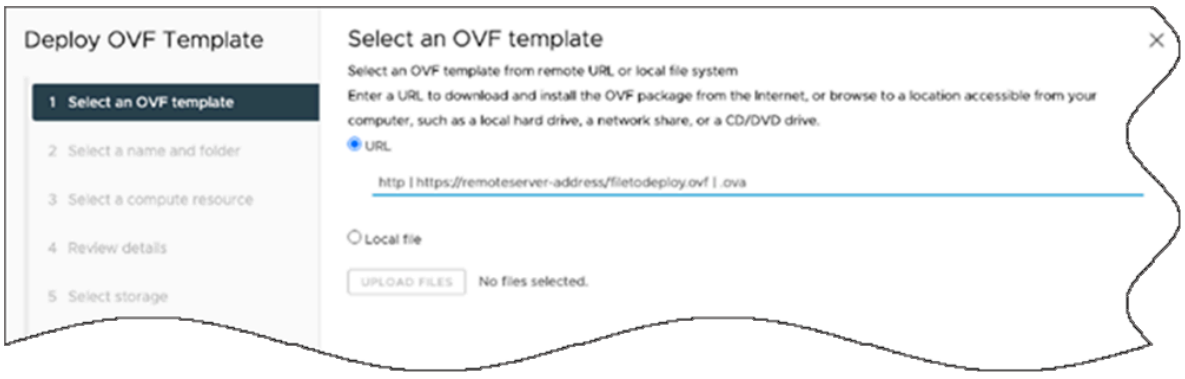
**STEP 1 |** 從客戶支援入口網站 (CSP) 中，於 **Updates**（更新） > **Software Updates**（軟體更新） > **Prisma Access ZTNA Connector for VMware** 下，下載 ZTNA 連接器 VMware ESXi 映像。

下載 *1-nic* 版本檔案以進行單臂部署，以及下載 *two-nic* 版本檔案以進行雙臂部署。

**STEP 2 |** 開啟 VMware vCenter、選取，並以滑鼠右鍵按一下主機，然後選取 **Deploy OVF Template**（部署 **OVF** 範本）。

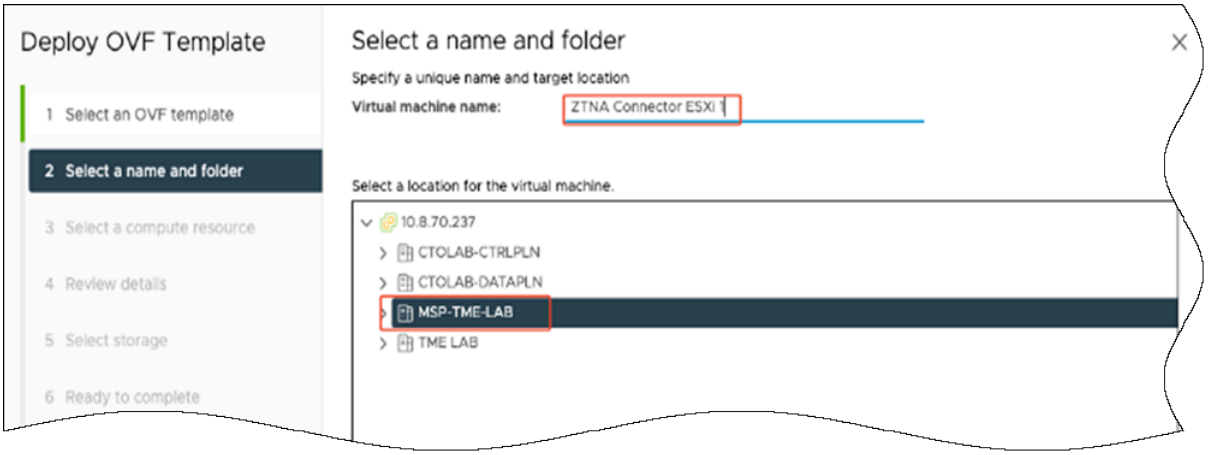



**STEP 3 |** 從連接器 OVA 中選取位置（可以是 URL 或本機檔案），然後選取 **Next**（下一步）。

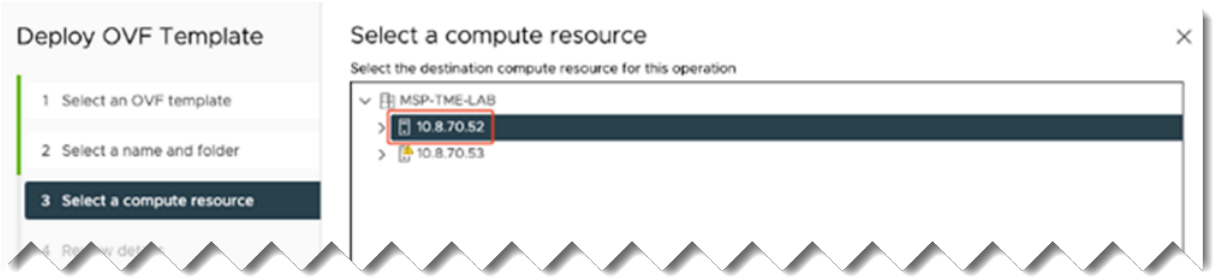



 ©2025 Palo Alto Networks, Inc.

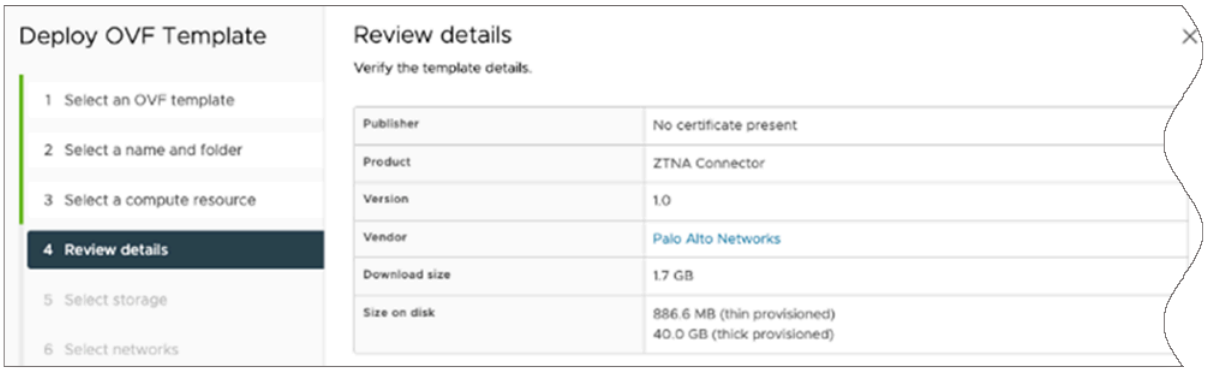
**STEP 4 |** 輸入虛擬機器 (VM) 名稱和 VM 的位置。




**STEP 5 |** 為 VM 選取計算資源。

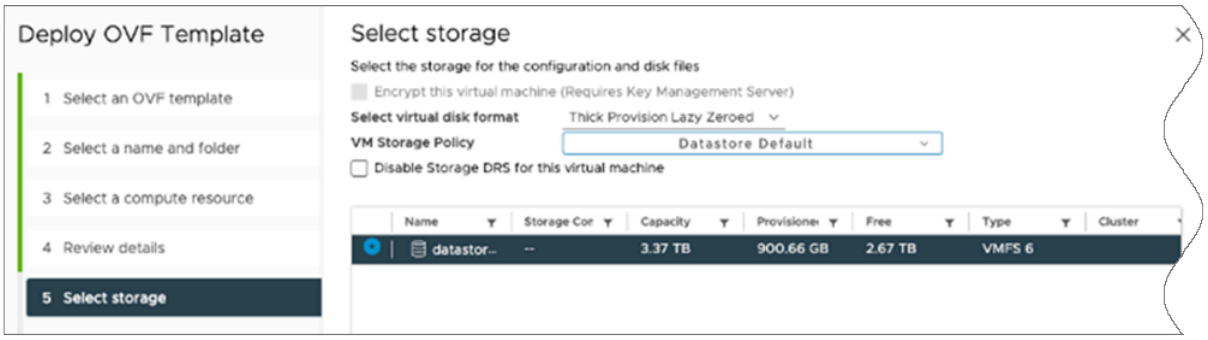



**STEP 6 |** 檢閱範本的詳細資訊，並選取 **Next**（下一步）。




 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** 選取 **Thick Provision Lazy Zeroed**（厚式佈建延遲歸零）作為虛擬磁碟格式，以及選取適合於 ZTNA 連接器 VM 的資料存放區。



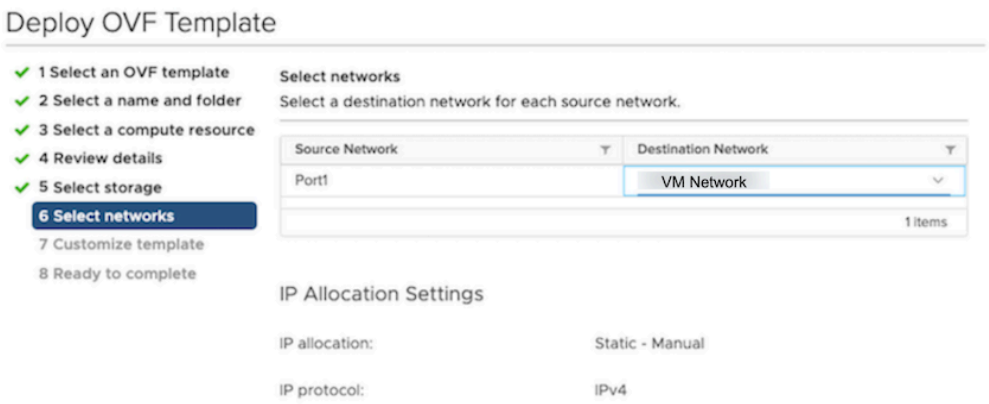

選用 選取 **Thin Provision**（厚式佈建）作為虛擬磁碟格式，以及選取適合於 ZTNA 連接器 VM 的資料存放區，其中伺服器僅配置主機所需的空間，取決於需求。



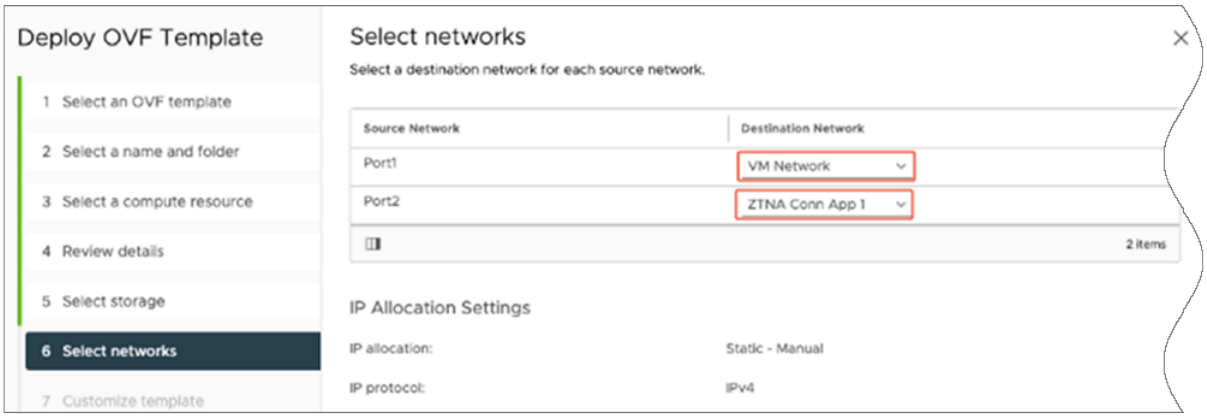

 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** 為您使用 OVA 設定範本建立的介面選取網路（適用於連接埠 1 和連接埠 2）。

1. 如果您正在部署單臂連接器，**Port 1**（連接器 **1**）是可以連線 WAN 和 LAN 應用伺服器的網路。為 **Port 1**（連接埠 **1**）選取 WAN/LAN 網路。




2. 如果您正在部署雙臂連接器，請為 **Port 1**（連接埠 **1**）選取面向網際網路的連接器，以及為 **Port 2**（連接埠 **2**）選取面向應用伺服器的網路。
   - 連接埠 1 是面向 WAN 的連接埠，用於對 Prisma Access 進行 IPSec 連線。
   - 連接埠 2 是面向應用程式的連接埠。




**STEP 9 |** 如果您尚未這樣做，請前往 **Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Connectors**（連接器）、尋找您在 Prisma Access 建立的連接器物件，以將其與此 VM 建立關聯，並從 **Actions**（動作）頁籤（鑰匙圖示）選取 **Copy Token**（複製權杖）；然後，複製 **Key**（金鑰）和 **Secret**（密碼）值。



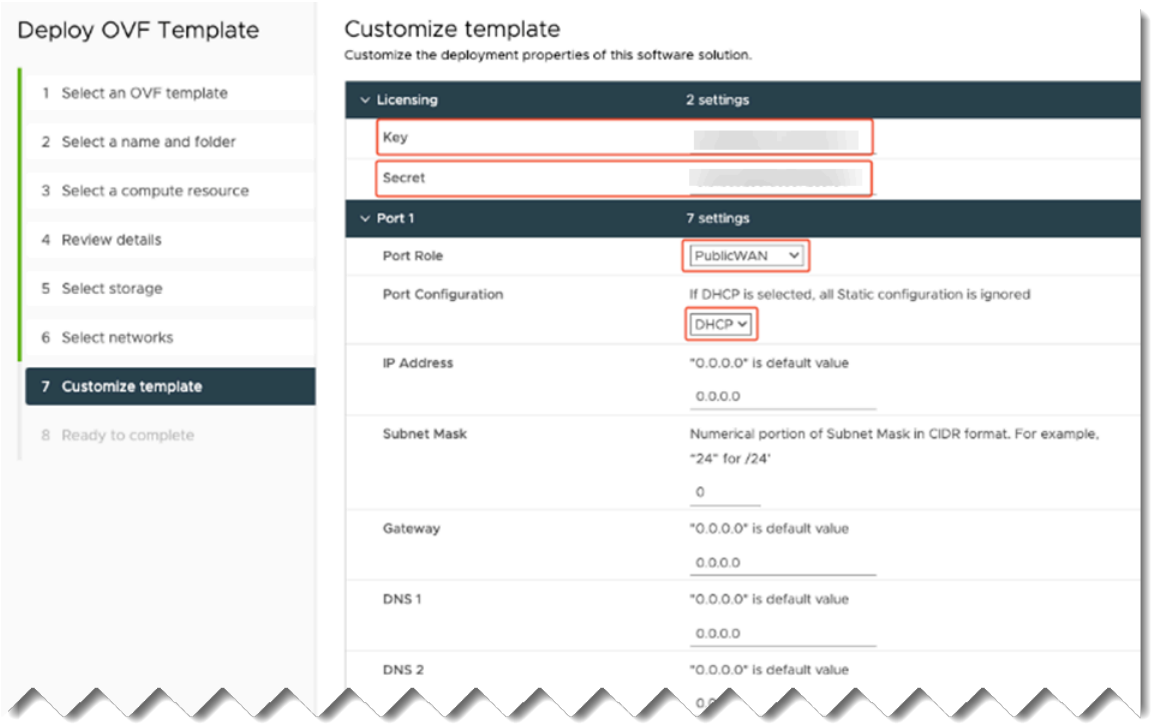

 ©2025 Palo Alto Networks, Inc.

**STEP 10 |** 在 **Customize template**（自訂範本）畫面中，進行以下設定變更：

- **Licensing**（授權）區域—輸入您從 Prisma SASE 入口網站擷取的 **Key**（金鑰）和 **Secret**（密碼）值。
- **Port 1**（連接埠 **1**）（面向 Prisma Access 的連接埠）區域—進行以下變更：
  - **Role**（角色）—公用 WAN。
  - **Port Configuration**（連接埠設定）—選取 **DHCP** 或 **Static**（靜態）。

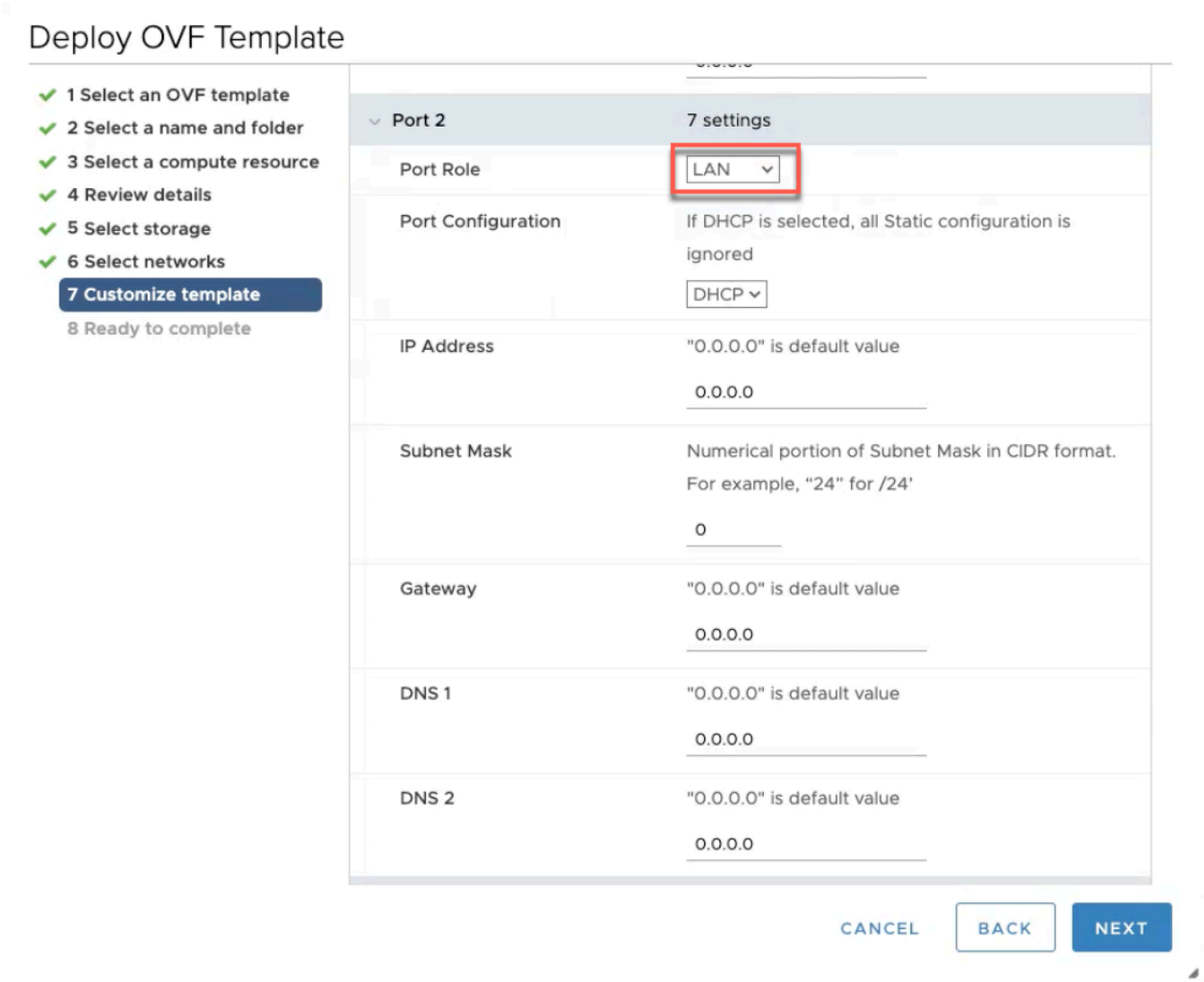
    如果您選取 **Static**（靜態），請輸入 IP 位址、子網路遮罩、閘道，以及一或兩個 DNS 伺服器值。

    如果您使用 DHCP，請將欄位中的預設零留下，如以下螢幕擷取畫面所示。



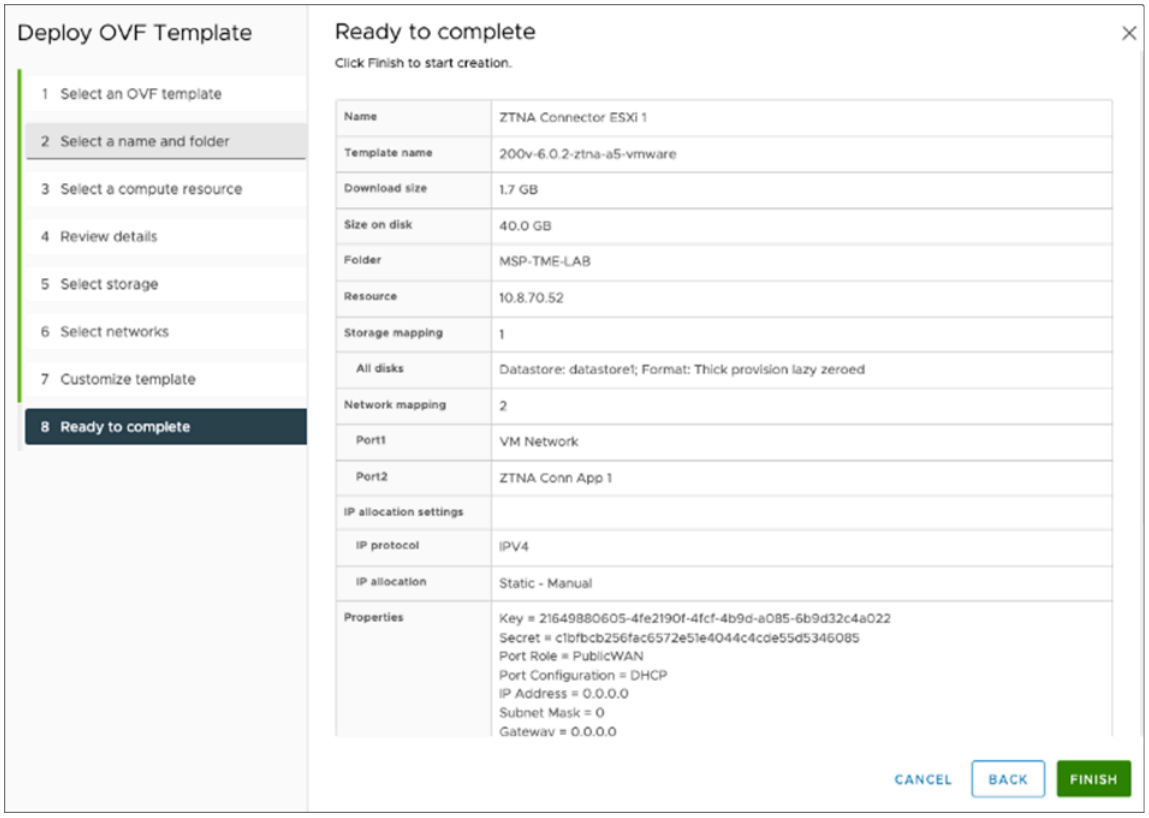

- 僅限雙臂 ESXi 部署 如果您有雙臂部署，請按照步驟 10 中對 **Port 1**（連接埠 **1**）套用的相同規則設定 **Port 2**（連接埠 **2**）LAN IP 介面。

 ©2025 Palo Alto Networks, Inc.




 ©2025 Palo Alto Networks, Inc.

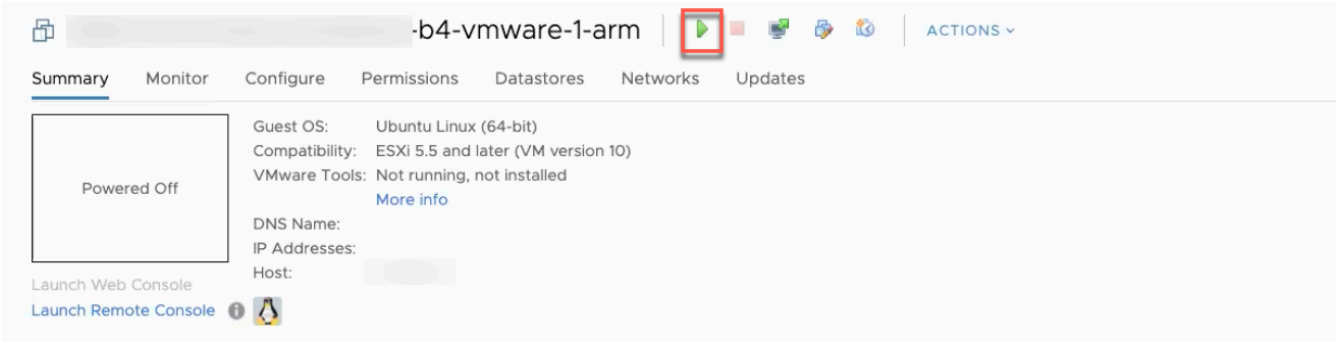
**STEP 11 |** 檢閱摘要，然後選取 **Finish**（完成）。




 ©2025 Palo Alto Networks, Inc.

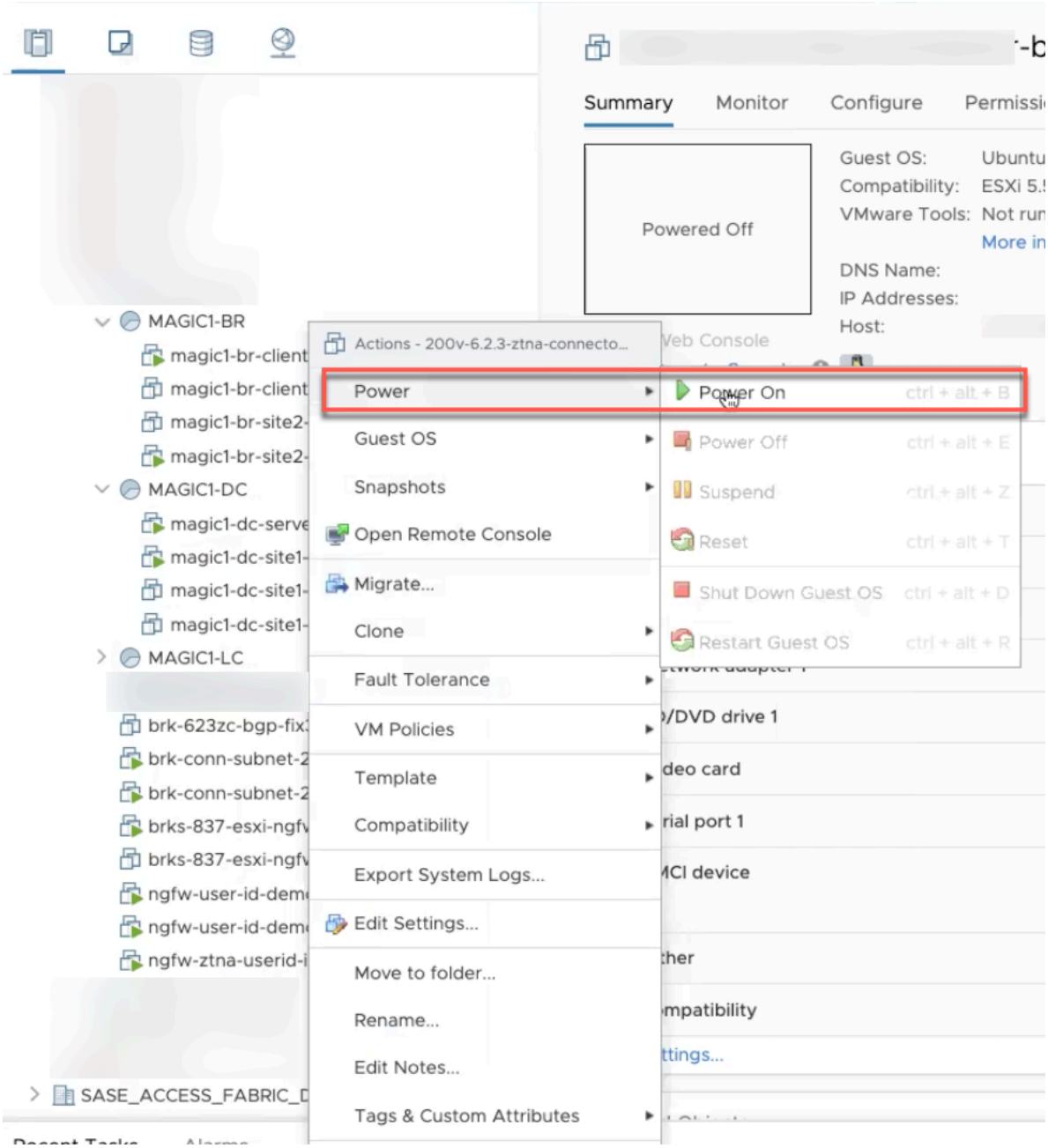
**STEP 12 |** 使用下列其中一種方法開啟 VM 電源。

- 選取 **Power On**（開啟電源）以啟動虛擬伺服器。




- 以滑鼠右鍵按一下介面，然後選取 **Power On**（開啟電源）（電源 > 開啟電源）。

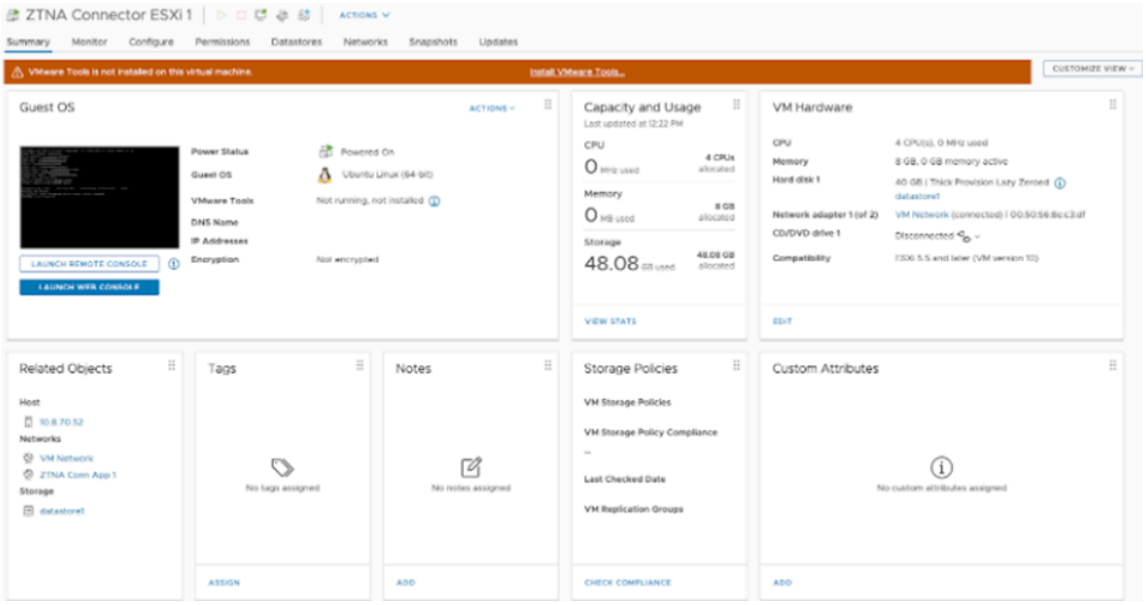

©2025 Palo Alto Networks, Inc.



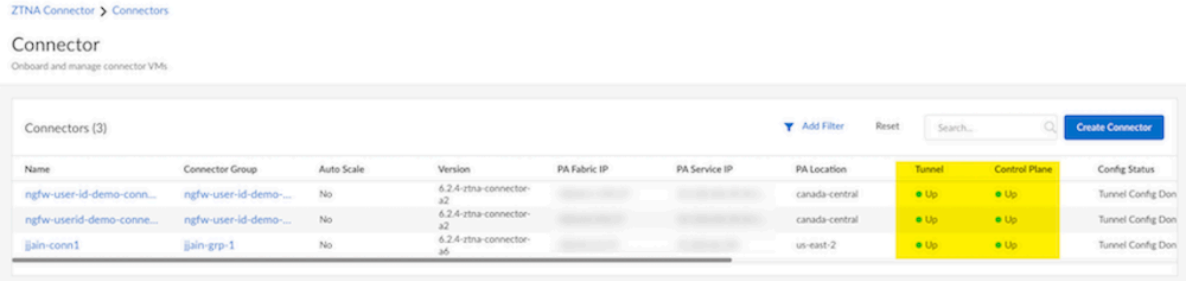

 ©2025 Palo Alto Networks, Inc.

**STEP 13 |** 在部署 VM 之後，確認它已啟動。

在 ESXi 虛擬伺服器啟動之後，Prisma Access 會完成要用作 ZTNA 連接器的裝置設定。



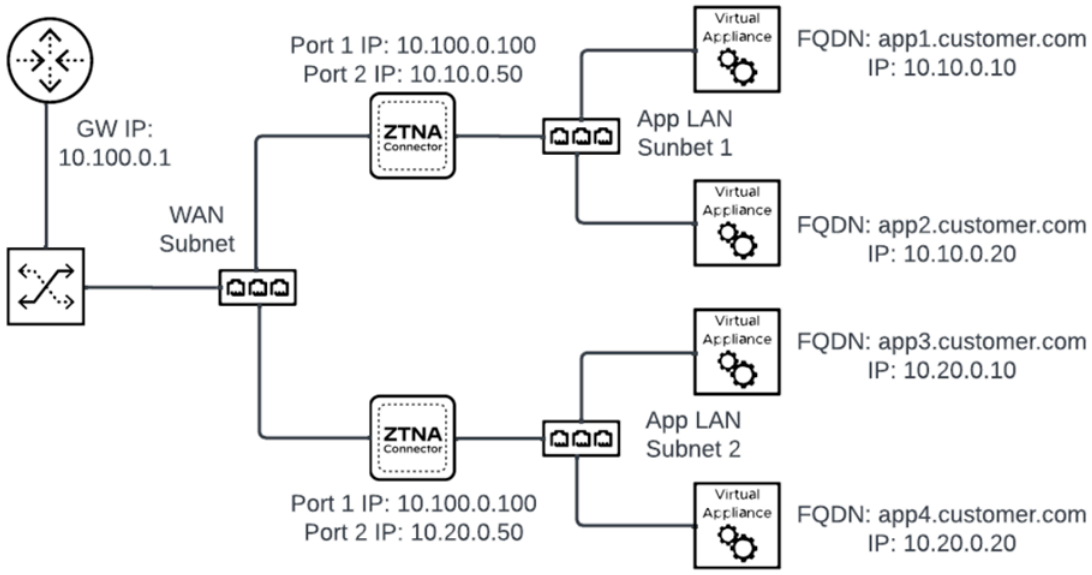

**STEP 14 |** 在 Prisma SASE 入口網站上，前往 **Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Connectors**（連接器）、尋找您要使用的連接器，並確保其顯示 **tunnel up**（通道啟動）。




# Prisma Access ZTNA 連接器支援 KVM 部署

您使用雙臂部署來部署核心型虛擬機器 (KVM)。下圖顯示在雙臂模式下使用 KVM 搭配 NAT 閘道進行 ZTNA 連接器網路部署範例。


©2025 Palo Alto Networks, Inc.




## 使用 KVM 裝載 ZTNA 連接器

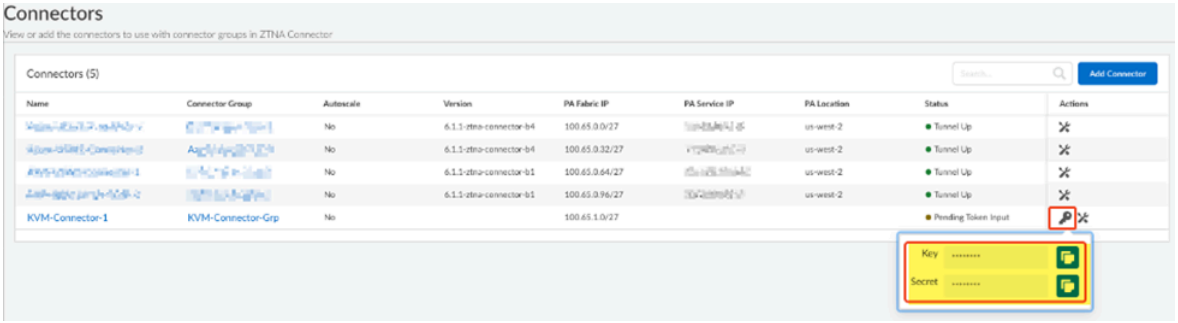
若要使用核心型虛擬機器 (KVM) 裝載 ZTNA 連接器，請完成下列步驟。

開始之前，請確保您具備以下先決條件：

- 從客戶支援入口網站 (CSP) 中，於 **Updates**（更新） > **Software Updates**（軟體更新） > **Prisma Access ZTNA Connector for KVM** 下，下載 ZTNA 連接器 Hyper-V 映像。
- 確保您有符合 ZTNA 連接器最低托管環境的 KVM 主機。

**STEP 1 |** 為 KVM 主機建立一個連接器群組和一個連接器。

**STEP 2 |** 選取 **Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Connectors**（連接器），並尋找您為 KVM 主機建立的連接器、在 **Status**（狀態）區域中 **Copy Token**（複製權杖），然後複製 **Key**（金鑰）和 **Secret**（密碼）值。




**STEP 3 |** 將您從 CSP 下載的 **qcow** 映像上傳到 KVM 主機。


©2025 Palo Alto Networks, Inc.

**STEP 4 |** 如果尚未這樣做，請在 KVM 主機上建置並關聯虛擬橋接器介面，並透過輸入以下命令來準備主機：

- `brctl addbr virbr0`
- `brctl addbr virbr0`
- `brctl addbr virbr1`
- `brctl addif virbr1 ens192`

**STEP 5 |** 透過執行 `virt-install` 命令並設定以下選項，在 KVM 主機上部署 VM：

- `-name` 是虛擬機器的名稱。
- `-vcpu` 是 **4**。
- `-memory` 是 **16384** (16 GB)。
- `-disk` 是 KVM 主機上 **qcow** 映像的位置和名稱。
- `-network` 參考要附加到此 VM 的虛擬介面（您需要為 ZTNA 連接器部署介面）。

以下是用來部署 KVM 主機的範例命令，其中 **<kvm-file-name>** 是您從 CSP 下載的 qcow 檔案名稱：

```
virt-install --name ztna-conn-1 --vcpus 4 --memory 16384 --disk ./
<kvm-file-name> --import --network bridge=virbr0,model=virtio --
network bridge=virbr1,model=virtio
```

**STEP 6 |** 請輸入以下命令連線到 VM 主控台：

```
virsh console ztna-conn-1
```

互動式 CLI 安裝程式即會啟動。

**STEP 7 |** 設定 ION 型號、金鑰和密碼。

1. 從顯示的選項中選取 **1**（ION 型號為 **ION 200v**）。

```
root@ubuntu-kvm-vm:/home/ubuntu-kvm/Desktop# virsh console
 ztna-conn-1 已連線至網域 ztna-conn-1 逸出字元為 ^] 請選取 ION 型
號：1) ion 200v 2) ion 3102v 3) ion 3104v 4) ion 3108v 5) ion
 7108v 6) ion 7116v 7) ion 7132v 8) ion 9100v 選擇一個數字或
 (Q) 退出：1 個 CPU：已通過（需要 4）記憶體：已通過（需要 8.0G）磁碟：無
法驗證（需要 40.0G）網路：已通過（需要 1）選取一個項目進行修改，或提交設
定：1) 型號：ion 200v 2) ION 金鑰：3) 密碼金鑰：4) 控制器 1：控制器 -
 DHCP 5) 連接埠 1：已停用/未使用 6) 連接埠 2：已停用/未使用 7) 連接埠
 3：已停用/未使用 8) 連接埠 4：已停用/未使用 9) 連接埠 5：已停用/未使用
 10) 連接埠 6：已停用/未使用 11) 連接埠 7：已停用/未使用 12) 連接埠 8：
已停用/未使用 13) 連接埠 9：已停用/未使用 14) 提交並重新啟動
```

2. 從連接器輸入金鑰，方法是選取選項 **2**，並輸入您從 ZTNA 連接器 UI 儲存的金鑰。

```
選擇一個數字或 (Q) 退出：2 輸入 ION 金鑰[無]：xxxxxxxxxx-yyyyyyyy-
zzz-1234-1234-abcdefghijkl 選取一個項目進行修改，或提交設定：1) 型
號：ion 200v 2) ION 金鑰：xxxxxxxxx-yyyyyyyy-zzz-1234-1234-
abcdefghijkl 3) 密碼金鑰：4) 控制器 1：控制器 - DHCP 5) 連接埠 1：已
```

 ©2025 Palo Alto Networks, Inc.

```
停用/未使用 6) 連接埠 2：已停用/未使用 7) 連接埠 3：已停用/未使用 8) 連
接埠 4：已停用/未使用 9) 連接埠 5：已停用/未使用 10) 連接埠 6：已停用/未
使用 11) 連接埠 7：已停用/未使用 12) 連接埠 8：已停用/未使用 13) 連接埠
 9：已停用/未使用 14) 提交並重新啟動
```

3. 輸入 ZTNA 連接器密碼，方法是選取選項 **3**，並輸入您從 ZTNA 連接器 UI 儲存的密碼。

```
選擇一個數字或 (Q) 退出：3 輸入 ION 密碼[無]：abcde12345 選取一個項
目進行修改，或提交設定：1) 型號：ion 200v 2) ION 金鑰：xxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) 密碼金鑰：abcde12345 4) 控
制器 1：控制器 - DHCP 5) 連接埠 1：已停用/未使用 6) 連接埠 2：已停用/未
使用 7) 連接埠 3：已停用/未使用 8) 連接埠 4：已停用/未使用 9) 連接埠
 5：已停用/未使用 10) 連接埠 6：已停用/未使用 11) 連接埠 7：已停用/未使
用 12) 連接埠 8：已停用/未使用 13) 連接埠 9：已停用/未使用 14) 提交並重
新啟動
```

**STEP 8 |** 設定 WAN 連接埠選項。

1. 選取選項 **5**（連接埠 1）。

```
選擇一個數字或 (Q) 退出：5 連接埠 1：1) 角色：已停用 2) 取消連接埠變更
 3) 套用並返回
```

2. 選取選項 **1**（公用/WAN）。

```
選擇一個數字或 (Q) 退出：1 選取連接埠角色：1) 面向網際網路的連接埠
 (PublicWAN) 2) 私人 WAN 連接埠 (PrivateWAN) 3) 略過連接埠配對
 1（WAN 連連接埠）4) 略過連接埠配對 1（LAN 連接埠）5) 略過連接埠配對
 2（WAN 連接埠）6) 略過連接埠配對 2（LAN 連接埠）7) 略過連接埠配對
 3（WAN 連接埠）8) 略過連接埠配對 3（LAN 連接埠）9) 略過連接埠配對
 4（WAN 連接埠）10) 略過連接埠配對 4（LAN 連接埠）11) 已停用/未使用
```

3. （選用）如果您需要設定靜態 IP 位址，請選擇選項 **2** 並設定 IP 位址、閘道和 DNS 伺服器參數；否則，請選擇 **1**。

```
選擇一個數字或 (Q) 退出：1 連接埠 1：1) 角色：PublicWAN 2) 設定方
式：DHCP 3) 取消連接埠變更 4) 套用並返回
```

4. 選取選項 **4** 返回主要功能表。

```
選擇一個數字或 (Q) 退出：4 選取一個項目進行修改，或提交設定：1) 型
號：ion 200v 2) ION 金鑰：xxxxxxxxx-yyyyyyyy-zzz-1234-1234-
abcdefghijkl 3) 密碼金鑰：abcde12345 4) 控制器 1：控制器 - DHCP
 5) 連接埠 1：PublicWAN - DHCP 6) 連接埠 2：已停用/未使用 7) 連接埠
 3：已停用/未使用 8) 連接埠 4：已停用/未使用 9) 連接埠 5：已停用/未使
用 10) 連接埠 6：已停用/未使用 11) 連接埠 7：已停用/未使用 12) 連接埠
 8：已停用/未使用 13) 連接埠 9：已停用/未使用 14) 提交並重新啟動 選取一
個項目進行修改，或提交設定：1) 型號：ion 200v 2) ION 金鑰：xxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) 密碼金鑰：abcde12345 4) 控
制器 1：控制器 - DHCP 5) 連接埠 1：PublicWAN - DHCP 6) 連接埠 2：
已停用/未使用 7) 連接埠 3：已停用/未使用 8) 連接埠 4：已停用/未使用
 9) 連接埠 5：已停用/未使用 10) 連接埠 6：已停用/未使用 11) 連接埠 7：
```

 ©2025 Palo Alto Networks, Inc.

```
已停用/未使用 12) 連接埠 8：已停用/未使用 13) 連接埠 9：已停用/未使用
14) 提交並重新啟動
```

**STEP 9 |** 設定 LAN 連接埠選項。

1. 選取選項 **6**（連接埠 2）。

```
選擇一個數字或 (Q) 退出：6 連接埠 2：1) 角色：已停用 2) 取消連接埠變更
3) 套用並返回
```

2. 選取選項 **2** (PrivateWAN)。

```
選擇一個數字或 (Q) 退出：2 選取連接埠角色：1) 面向網際網路的連接埠
(PublicWAN) 2) 私人 WAN 連接埠 (PrivateWAN) 3) 略過連接埠配對
1（WAN 連連接埠）4) 略過連接埠配對 1（LAN 連接埠）5) 略過連接埠配對
2（WAN 連接埠）6) 略過連接埠配對 2（LAN 連接埠）7) 略過連接埠配對
3（WAN 連接埠）8) 略過連接埠配對 3（LAN 連接埠）9) 略過連接埠配對
4（WAN 連接埠）10) 略過連接埠配對 4（LAN 連接埠）11) 已停用/未使用
```

3. （選用）如果您需要設定靜態 IP 位址，請選擇選項 **2** 並設定 IP 位址、閘道和 DNS 伺服器參數；否則，請選擇 **1**。

```
選擇一個數字或 (Q) 退出：2 連接埠 2：1) 角色：PrivateWAN 2) 設定方
式：DHCP 3) 取消連接埠變更 4) 套用並返回
```

4. 選取選項 **4** 返回主要功能表。

```
選擇一個數字或 (Q) 退出：4 選取一個項目進行修改，或提交設定：1) 型
號：ion 200v 2) ION 金鑰：xxxxxxxxx-yyyyyyyy-zzz-1234-1234-
abcdefghijkl 3) 密碼金鑰：abcde12345 4) 控制器 1：控制器 - DHCP
5) 連接埠 1：PublicWAN - DHCP 6) 連接埠 2：PrivateWAN - DHCP
7) 連接埠 3：已停用/未使用 8) 連接埠 4：已停用/未使用 9) 連接埠 5：
已停用/未使用 10) 連接埠 6：已停用/未使用 11) 連接埠 7：已停用/未使用
12) 連接埠 8：已停用/未使用 13) 連接埠 9：已停用/未使用 14) 提交並重新
啟動
```

**STEP 10 |** 儲存並重新啟動連接器。

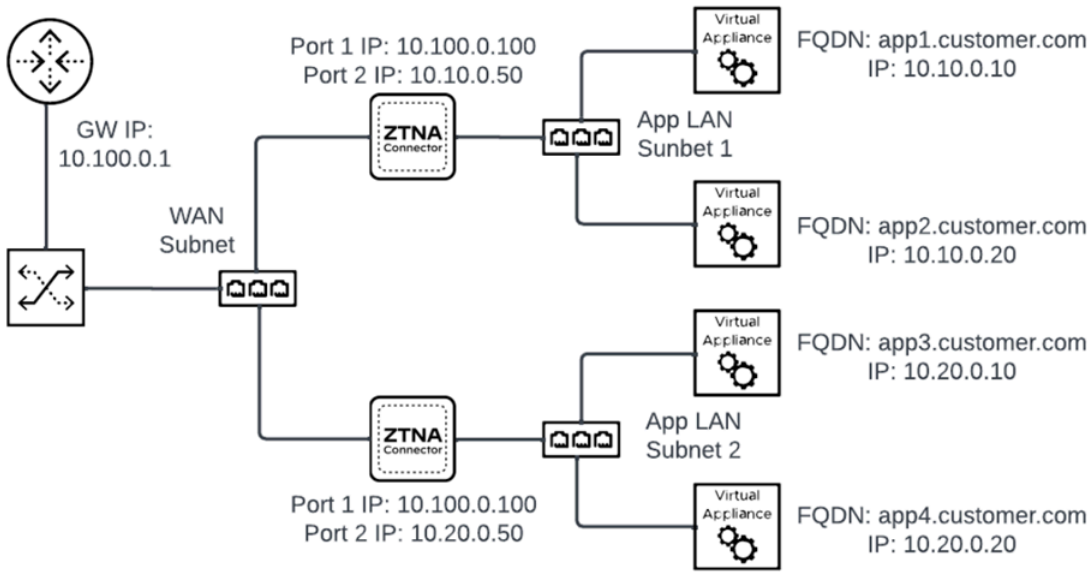
```
選擇一個數字或 (Q) 退出：14 警告#在提交此設定之後，所有硬體將進行簽署、記
錄，並永久地繫結至 Prisma SDWAN 雲端控制器中的 ION 金鑰/密碼金鑰。這意
味著在此 [SUBMIT（提交）] 功能之後，無法新增/移除硬體（磁碟、網路卡）。如
果在此 [SUBMIT（提交）] 之外需要任何硬體變更，則將需要使用新的 ION 金鑰
和密碼金鑰重新部署 ION。如果需要新增或移除硬體，請在下面回答 'N'，然後關閉
ION 並立即進行變更。立即提交這些變更嗎？[N]：y 正在建置設定... [VFF:CFG]
ZeroTouch 設定啟動中 - 設定檔案剖析器 [VFF:CFG] 正在嘗試載入/解析為設
定/INI 檔案。[VFF:CFG] 已成功載入設定樣式檔案。[VFF:CFG] 控制器 1 已成
功設定為 CONTROLLER/DHCP。[VFF:CFG] 連接埠 1 已成功設定為 PUBLICWAN/
DHCP。[VFF:CFG] 連接埠 2 已成功設定為 PRIVATEWAN/DHCP。[VFF:CFG] 警
告：連接埠 3 沒有設定區段。預設為 [Disable（停用）]。[VFF:CFG] 警告：連
接埠 4 沒有設定區段。預設為 [Disable（停用）]。[VFF:CFG] 警告：連接埠
5 沒有設定區段。預設為 [Disable（停用）]。[VFF:CFG] 警告：連接埠 6 沒
有設定區段。預設為 [Disable（停用）]。[VFF:CFG] 警告：連接埠 7 沒有設定
```

 ©2025 Palo Alto Networks, Inc.

```
區段。預設為 [Disable（停用）]。[VFF:CFG] 警告：連接埠 8 沒有設定區段。
預設為 [Disable（停用）]。[VFF:CFG] 警告：連接埠 9 沒有設定區段。預設為
 [Disable（停用）]。[VFF:CFG] 設定/INI 檔案剖析器成功。[VFF:KVM] 功能表設
定結束，繼續正常開機...重新開機原因：製造
```

# Prisma Access ZTNA 連接器支援的 Hyper-V 部署

您可以使用雙臂部署來部署 Microsoft Hyper-V 超管理器。下圖顯示在雙臂模式下使用 Hyper-V 搭配 NAT 閘道進行 ZTNA 連接器網路部署範例。




## 使用 Hyper-V 裝載 ZTNA 連接器

若要使用 Microsoft Hyper-V 虛擬機器 (VM) 來裝載 ZTNA 連接器，請完成以下步驟。

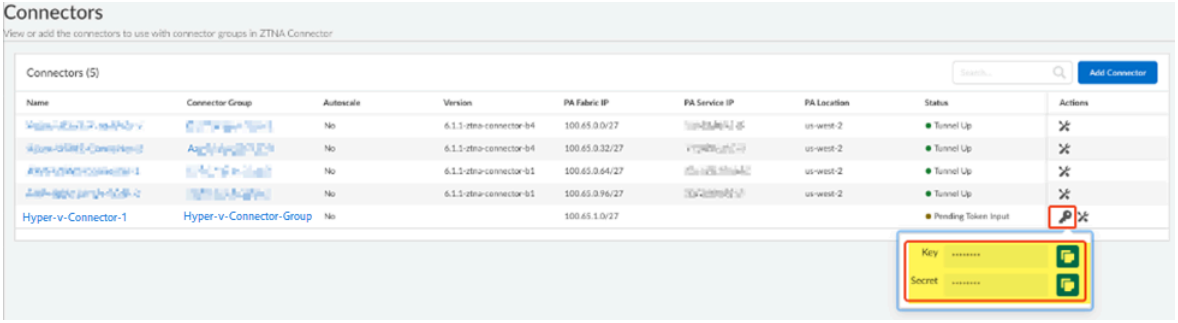
開始之前，請確保您具備以下先決條件：

- 從客戶支援入口網站 (CSP) 中，於 **Updates**（更新） > **Software Updates**（軟體更新） > **Prisma Access ZTNA Connector for Hyper-V** 下，下載 ZTNA 連接器 Hyper-V 映像。
- 確保您有符合 ZTNA 連接器最低托管環境的 Hyper-V VM。

**STEP 1 |** 為 Hyper-V VM 建立一個連接器群組和一個連接器。


©2025 Palo Alto Networks, Inc.

**STEP 2 |** 選取 **Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Connectors**（連接器），並尋找您為 Hyper-V VM 建立的連接器、在 **Status**（狀態）區域中 **Copy Token**（複製權杖），然後複製 **Key**（金鑰）和 **Secret**（密碼）值。



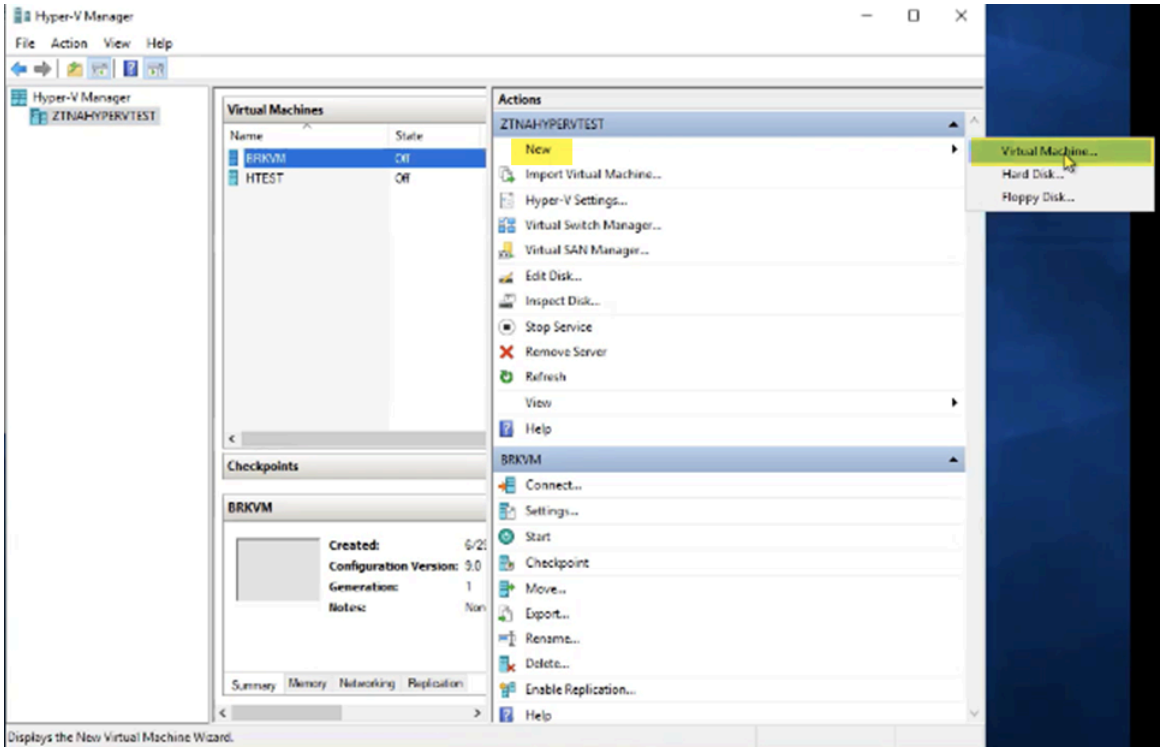

**STEP 3 |** 將您從 CSP 下載的 **vhd** 映像上傳到 Hyper-V VM。

確保您選擇的位置可以從 Hyper-V VM 連線。

每個 Hyper-V VM 都需要一個 (vhd) 檔案。

**STEP 4 |** 前往 Hyper-V 管理員，然後選取 **Actions**（動作） > **New**（新增） > **Virtual Machine**（虛擬機器），來建立一個新的虛擬機器。

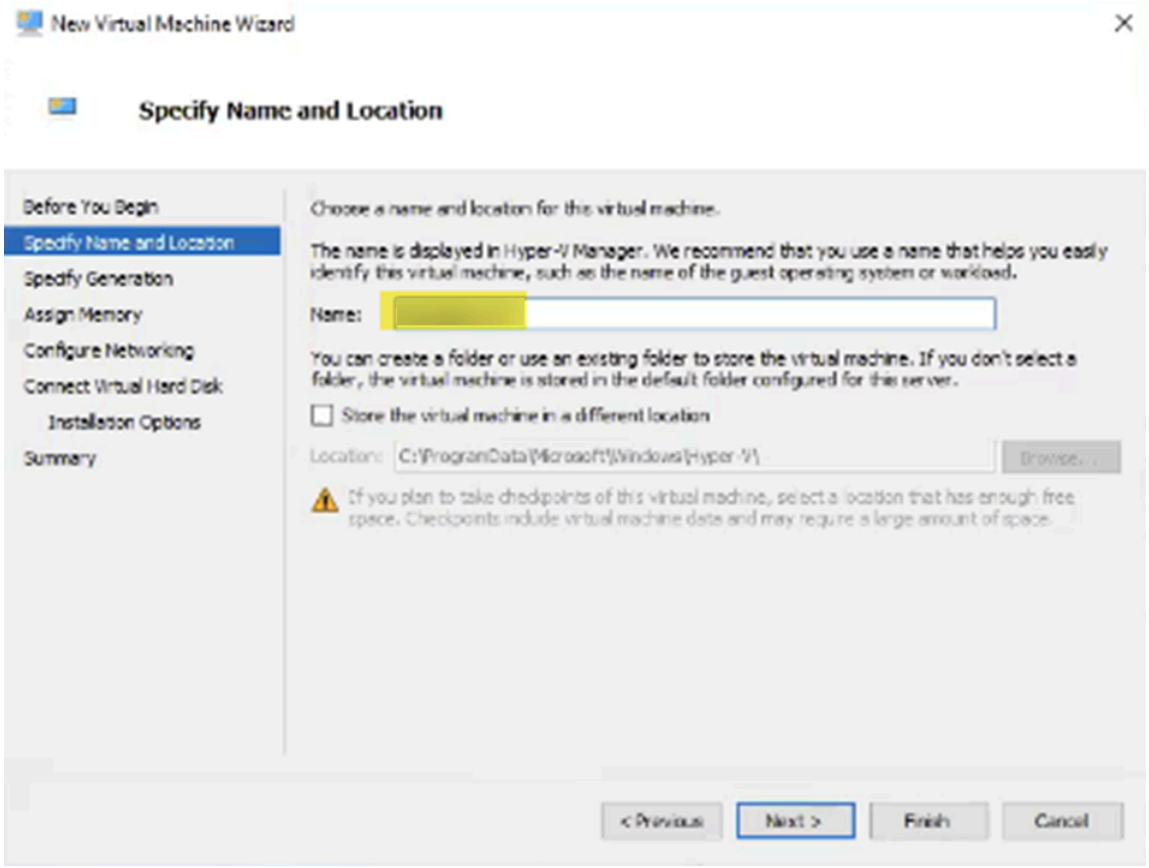
此工作流程顯示您在 Microsoft 伺服器上部署 Hyper-V VM 的步驟。Hyper-V UI 在您的環境中可能看起來不同。




**STEP 5 |** 前往 **Next**（下一個）畫面，並為 VM 輸入唯一的名稱，然後前往 **Next**（下一個）頁面。


©2025 Palo Alto Networks, Inc.

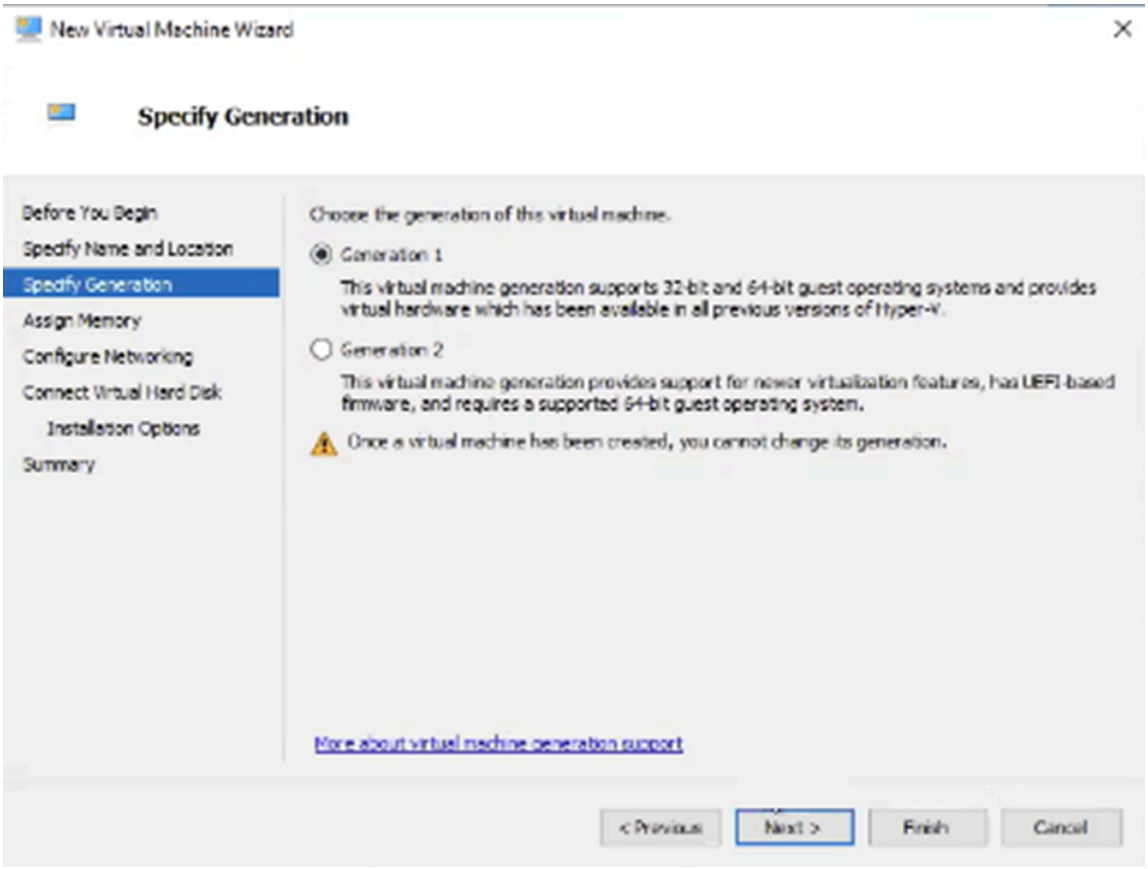
**STEP 6 |** （選用）若要變更 VM 的位址，請選取 **Store the virtual machine in a different location**（將虛擬機器儲存在不同的位置中）並選取位置。




 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** 選取 **Generation 1**（第一代）作為 VM 世代，然後前往 **Next**（下一個） 頁面。

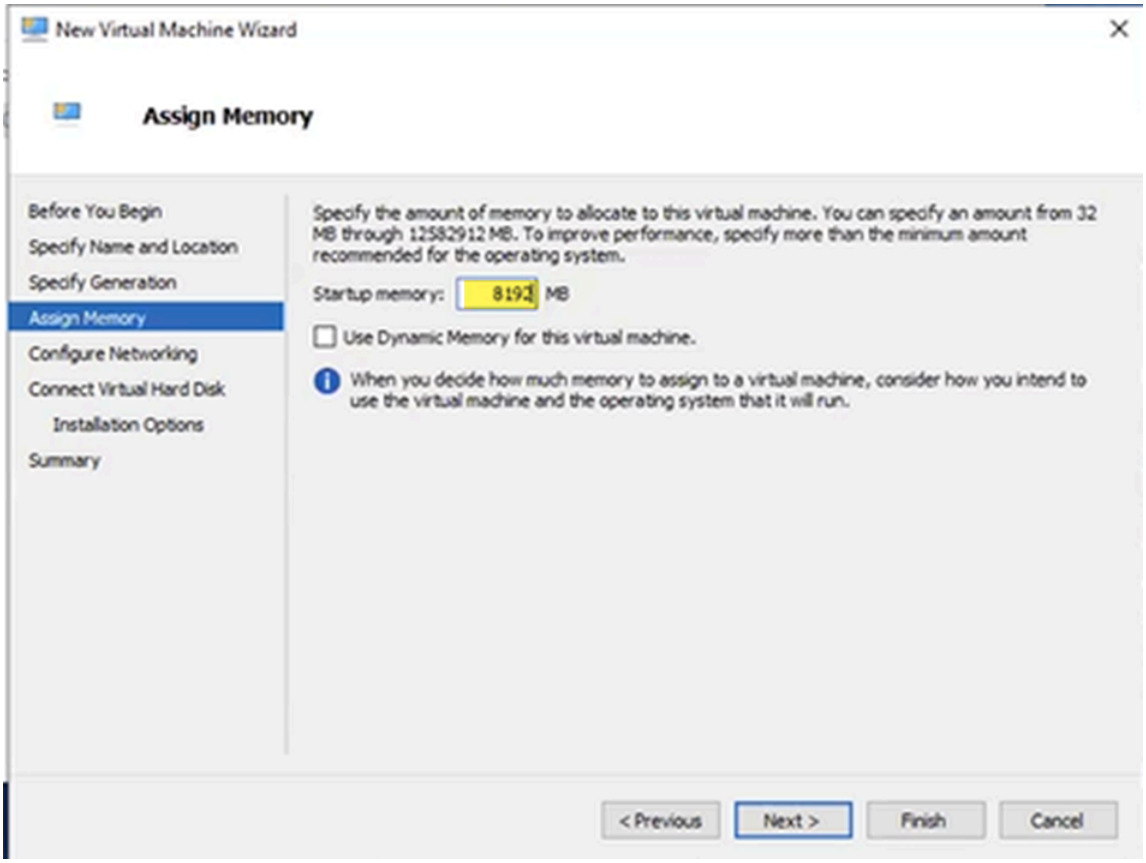
這是 ZTNA 連接器 vhd 檔案支援的世代。




 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** 將記憶體指派 VM。

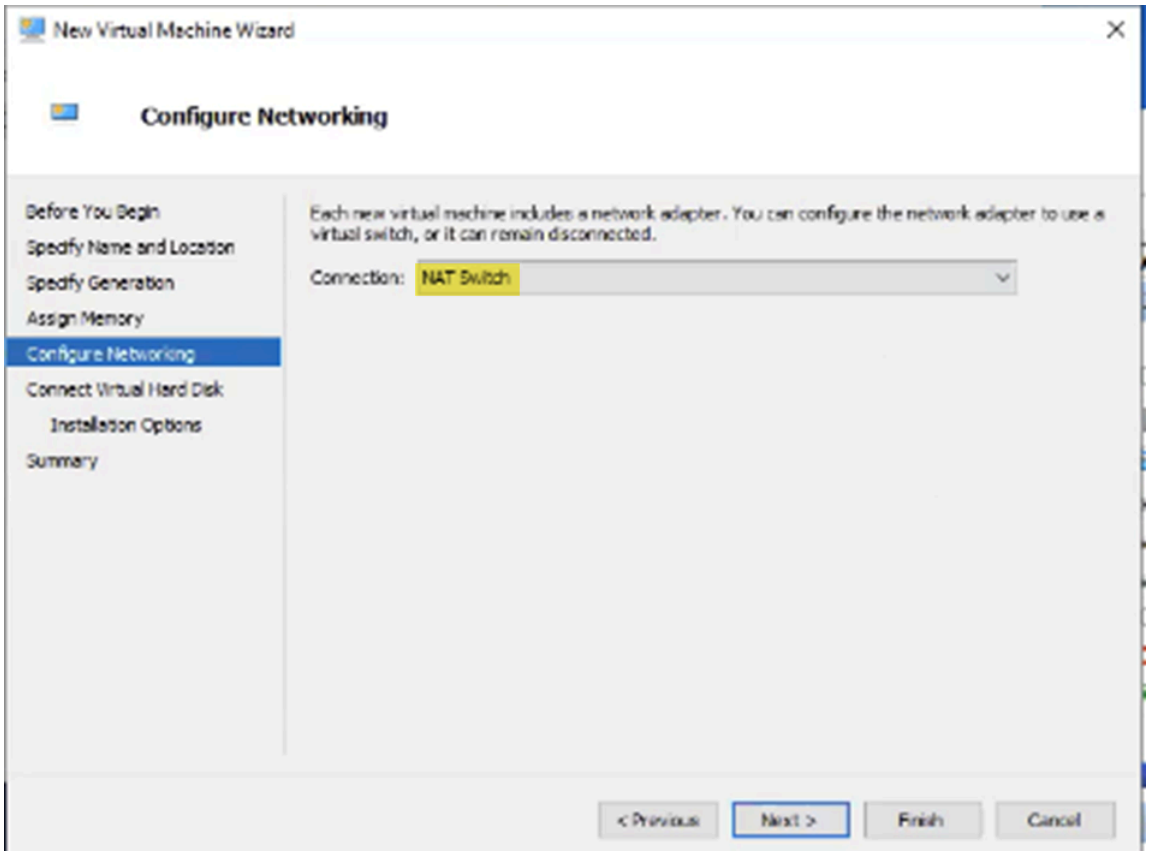
配置至少 **8192 MB** (8 GB) 的記憶體，這符合 Hyper-V VM 的最低需求，然後前往 **Next**（下一個）頁面。




 ©2025 Palo Alto Networks, Inc.

**STEP 9 |** 為您的 VM 設定網路；然後，前往 **Next**（下一個）頁面。

您使用的網路取決於您的設定。這個範例對網路使用 **NAT Switch**（**NAT** 交換機）。

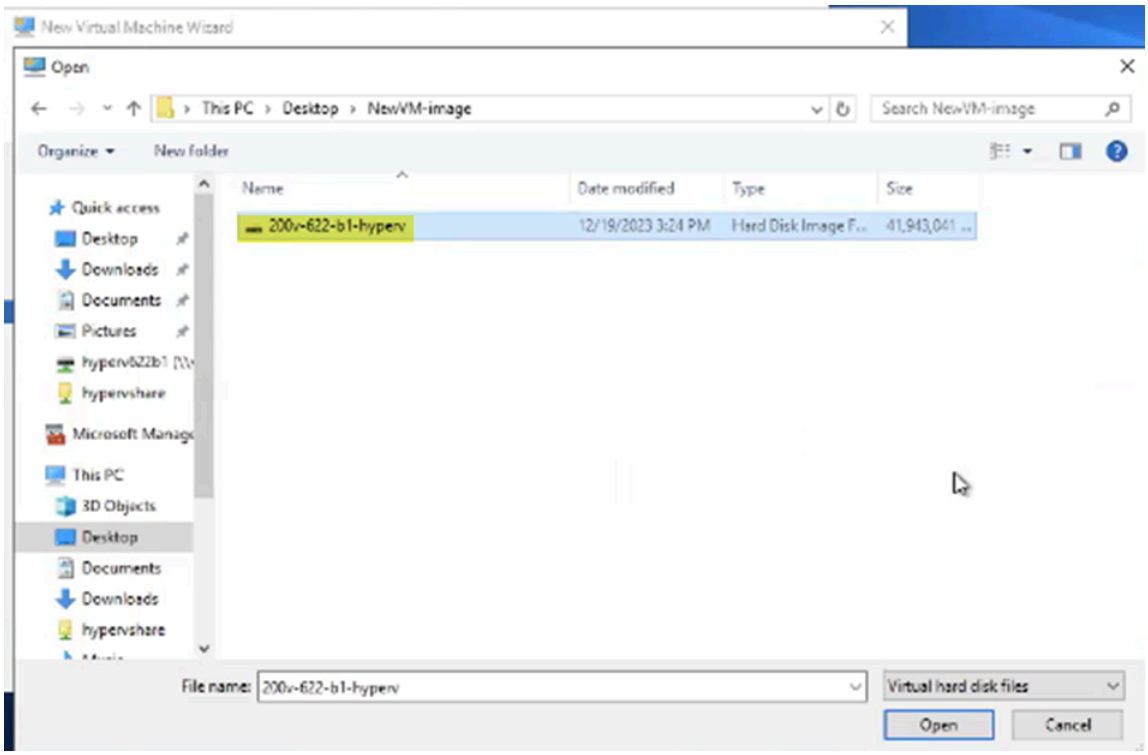




©2025 Palo Alto Networks, Inc.

**STEP 10 |** 連線虛擬硬碟。

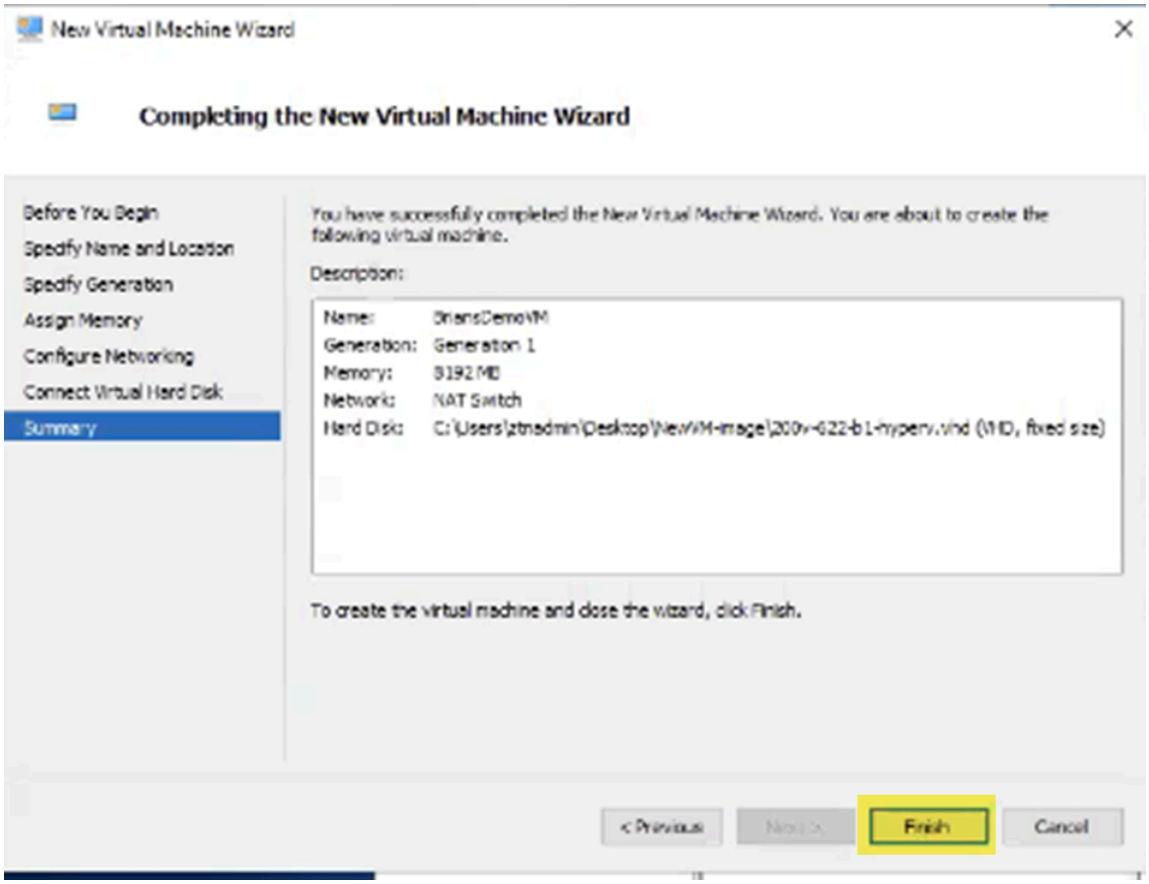
1. 選取 **Use an existing virtual hard disk**（使用現有的虛擬硬碟），並 **Browse**（瀏覽）您下載的 vhd 檔案
2. 選取您下載的 vhd 檔案，並 **Open**（開啟）它；然後，前往 **Next**（下一個）頁面。





©2025 Palo Alto Networks, Inc.

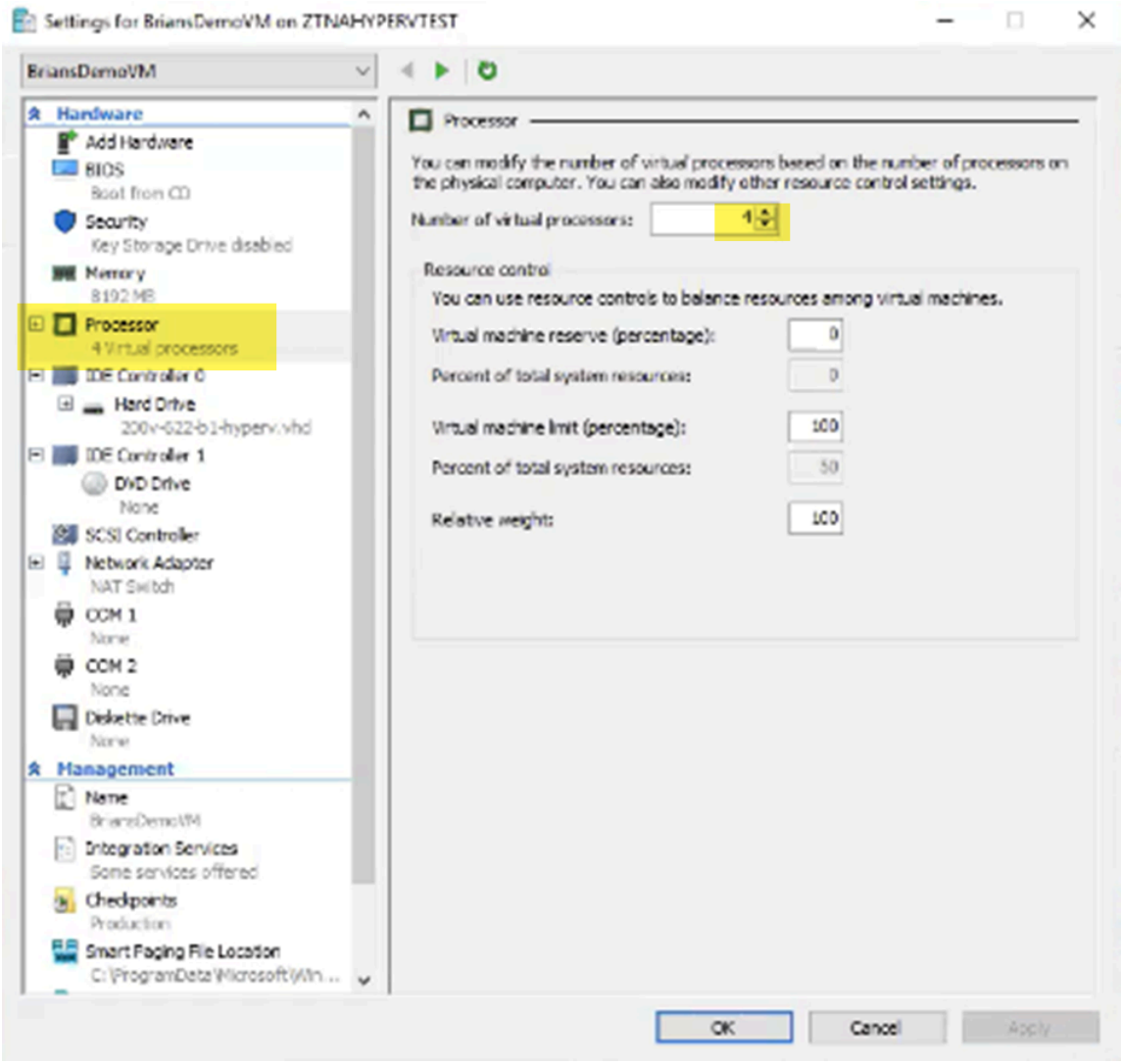
**STEP 11 | Finish**（完成）新的 VM 精靈。




Hyper-V 會建立 VM。

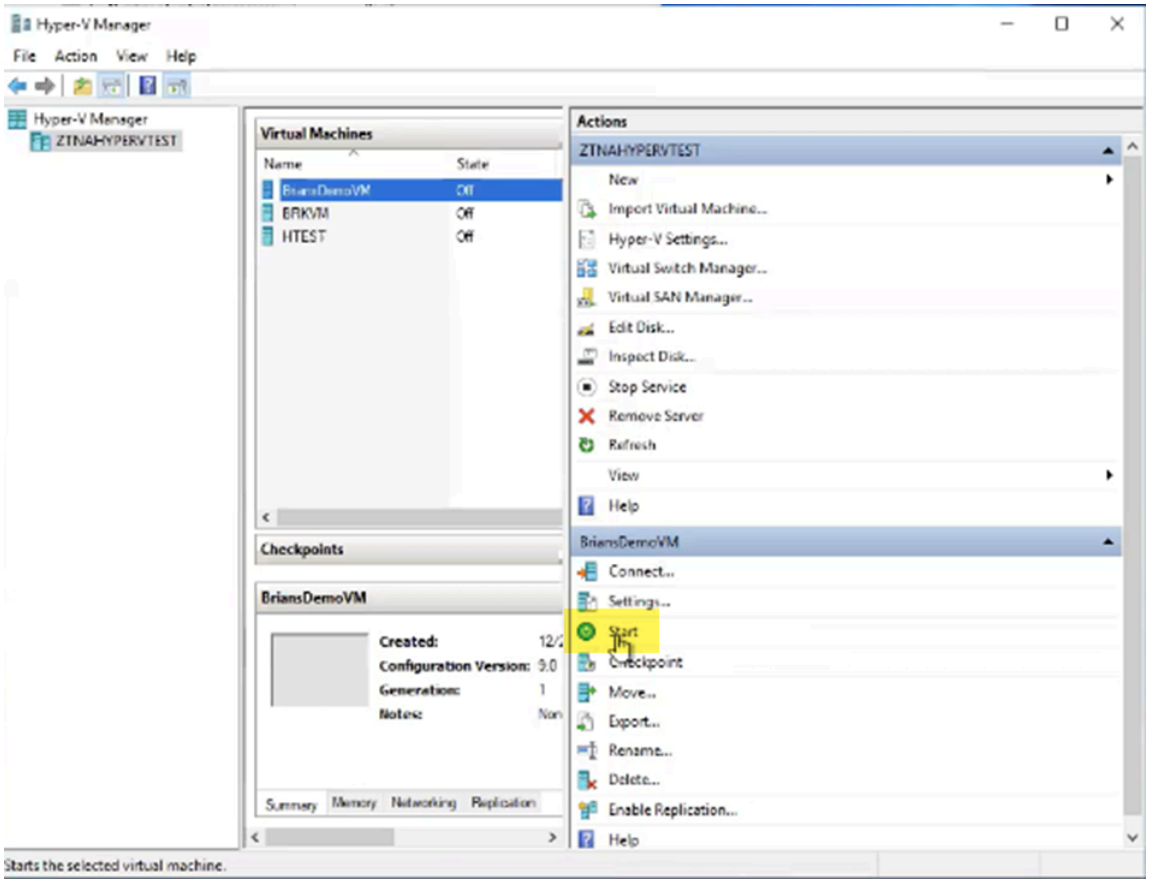
 ©2025 Palo Alto Networks, Inc.

**STEP 12 |** 確保您的 VM 有至少四個處理器，方法是前往 **Processor**（處理器）區域，並確保您選取至少 **4** 個虛擬處理器。

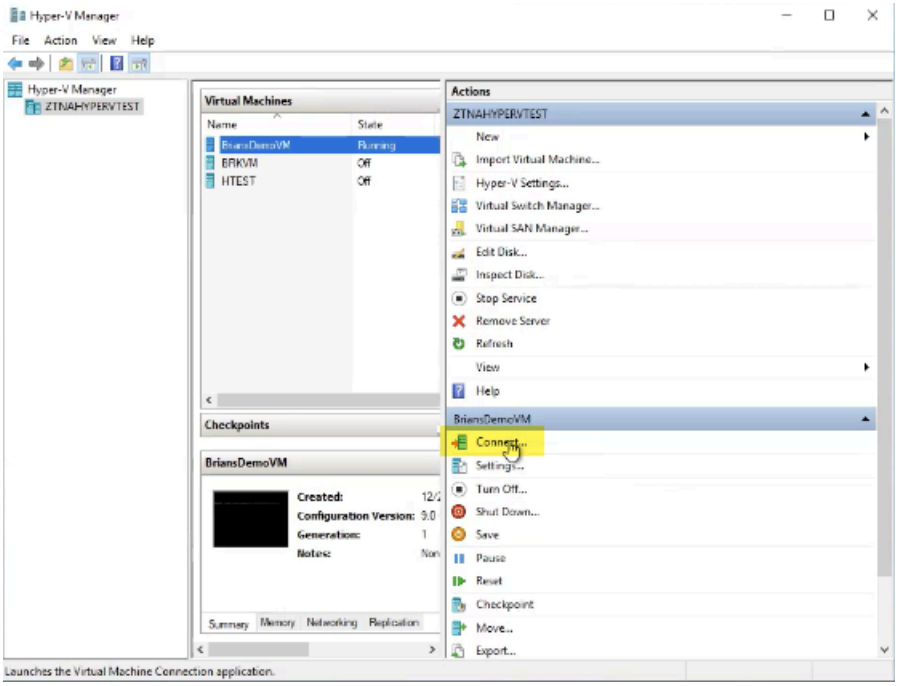



 ©2025 Palo Alto Networks, Inc.

**STEP 13 | Start**（啟動）VM。




**STEP 14 | Connect**（連線）至序列主控台。




 ©2025 Palo Alto Networks, Inc.

**STEP 15 |** 等待互動式 CLI 安裝程式初始化，然後設定 ION 模型、金鑰和密碼。

1. 從顯示的選項中選取 **1**（ION 型號為 **ION 200v**）。

```
選取一個 ION 型號：1) ion 200v 2) ion 3102v 3) ion 3104v 4) ion
 3108v 5) ion 7108v 6) ion 7116v 7) ion 7132v 8) ion 9100v 選
擇一個數字或 (Q) 退出：1 個 CPU：已通過（需要 4）記憶體：已通過（需要
 8.0G）磁碟：無法驗證（需要 40.0G）網路：已通過（需要 1）選取一個項目進行
修改，或提交設定：1) 型號：ion 200v 2) ION 金鑰：3) 密碼金鑰：4) 控制
器 1：控制器 - DHCP 5) 連接埠 1：已停用/未使用 6) 連接埠 2：已停用/未使
用 7) 連接埠 3：已停用/未使用 8) 連接埠 4：已停用/未使用 9) 連接埠 5：
已停用/未使用 10) 連接埠 6：已停用/未使用 11) 連接埠 7：已停用/未使用
 12) 連接埠 8：已停用/未使用 13) 連接埠 9：已停用/未使用 14) 提交並重新
啟動
```

2. 從連接器輸入金鑰，方法是選取選項 **2**，並輸入您從 ZTNA 連接器 UI 儲存的金鑰。

```
選擇一個數字或 (Q) 退出：2 輸入 ION 金鑰[無]：xxxxxxxxxx-yyyyyyyy-
zzz-1234-1234-abcdefghijkl 選取一個項目進行修改，或提交設定：1) 型
號：ion 200v 2) ION 金鑰：xxxxxxxxx-yyyyyyyy-zzz-1234-1234-
abcdefghijkl 3) 密碼金鑰：4) 控制器 1：控制器 - DHCP 5) 連接埠 1：已
停用/未使用 6) 連接埠 2：已停用/未使用 7) 連接埠 3：已停用/未使用 8) 連
接埠 4：已停用/未使用 9) 連接埠 5：已停用/未使用 10) 連接埠 6：已停用/未
使用 11) 連接埠 7：已停用/未使用 12) 連接埠 8：已停用/未使用 13) 連接埠
 9：已停用/未使用 14) 提交並重新啟動
```

3. 輸入 ZTNA 連接器密碼，方法是選取選項 **3**，並輸入您從 ZTNA 連接器 UI 儲存的密碼。

```
選擇一個數字或 (Q) 退出：3 輸入 ION 密碼[無]：abcde12345 選取一個項
目進行修改，或提交設定：1) 型號：ion 200v 2) ION 金鑰：xxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) 密碼金鑰：abcde12345 4) 控
制器 1：控制器 - DHCP 5) 連接埠 1：已停用/未使用 6) 連接埠 2：已停用/未
使用 7) 連接埠 3：已停用/未使用 8) 連接埠 4：已停用/未使用 9) 連接埠
 5：已停用/未使用 10) 連接埠 6：已停用/未使用 11) 連接埠 7：已停用/未使
用 12) 連接埠 8：已停用/未使用 13) 連接埠 9：已停用/未使用 14) 提交並重
新啟動
```

**STEP 16 |** 設定 WAN 連接埠選項。

1. 選取選項 **5**（連接埠 1）。

```
選擇一個數字或 (Q) 退出：5 連接埠 1：1) 角色：已停用 2) 取消連接埠變更
 3) 套用並返回
```

2. 選取選項 **1**（公用/WAN）。

```
選擇一個數字或 (Q) 退出：1 選取連接埠角色：1) 面向網際網路的連接埠
 (PublicWAN) 2) 私人 WAN 連接埠 (PrivateWAN) 3) 略過連接埠配對
 1（WAN 連連接埠）4) 略過連接埠配對 1（LAN 連接埠）5) 略過連接埠配對
 2（WAN 連接埠）6) 略過連接埠配對 2（LAN 連接埠）7) 略過連接埠配對
 3（WAN 連接埠）8) 略過連接埠配對 3（LAN 連接埠）9) 略過連接埠配對
 4（WAN 連接埠）10) 略過連接埠配對 4（LAN 連接埠）11) 已停用/未使用
```


©2025 Palo Alto Networks, Inc.

3. （選用）如果您需要設定靜態 IP 位址，請選擇選項 **2** 並設定 IP 位址、閘道和 DNS 伺服器參數；否則，請選擇 **1**。

```
選擇一個數字或 (Q) 退出：1 連接埠 1：1) 角色：PublicWAN 2) 設定方
式：DHCP 3) 取消連接埠變更 4) 套用並返回
```

4. 選取選項 **4** 返回主要功能表。

```
選擇一個數字或 (Q) 退出：4 選取一個項目進行修改，或提交設定：1) 型
號：ion 200v 2) ION 金鑰：xxxxxxxxx-yyyyyyyy-zzz-1234-1234-
abcdefghijkl 3) 密碼金鑰：abcde12345 4) 控制器 1：控制器 - DHCP
 5) 連接埠 1：PublicWAN - DHCP 6) 連接埠 2：已停用/未使用 7) 連接埠
 3：已停用/未使用 8) 連接埠 4：已停用/未使用 9) 連接埠 5：已停用/未使
用 10) 連接埠 6：已停用/未使用 11) 連接埠 7：已停用/未使用 12) 連接埠
 8：已停用/未使用 13) 連接埠 9：已停用/未使用 14) 提交並重新啟動 選取一
個項目進行修改，或提交設定：1) 型號：ion 200v 2) ION 金鑰：xxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) 密碼金鑰：abcde12345 4) 控
制器 1：控制器 - DHCP 5) 連接埠 1：PublicWAN - DHCP 6) 連接埠 2：
已停用/未使用 7) 連接埠 3：已停用/未使用 8) 連接埠 4：已停用/未使用
 9) 連接埠 5：已停用/未使用 10) 連接埠 6：已停用/未使用 11) 連接埠 7：
已停用/未使用 12) 連接埠 8：已停用/未使用 13) 連接埠 9：已停用/未使用
 14) 提交並重新啟動
```

**STEP 17 |** 設定 LAN 連接埠選項。

1. 選取選項 **6**（連接埠 2）。

```
選擇一個數字或 (Q) 退出：6 連接埠 2：1) 角色：已停用 2) 取消連接埠變更
 3) 套用並返回
```

2. 選取選項 **2** (PrivateWAN)。

```
選擇一個數字或 (Q) 退出：2 選取連接埠角色：1) 面向網際網路的連接埠
 (PublicWAN) 2) 私人 WAN 連接埠 (PrivateWAN) 3) 略過連接埠配對
 1（WAN 連連接埠）4) 略過連接埠配對 1（LAN 連接埠）5) 略過連接埠配對
 2（WAN 連接埠）6) 略過連接埠配對 2（LAN 連接埠）7) 略過連接埠配對
 3（WAN 連接埠）8) 略過連接埠配對 3（LAN 連接埠）9) 略過連接埠配對
 4（WAN 連接埠）10) 略過連接埠配對 4（LAN 連接埠）11) 已停用/未使用
```

3. （選用）如果您需要設定靜態 IP 位址，請選擇選項 **2** 並設定 IP 位址、閘道和 DNS 伺服器參數；否則，請選擇 **1**。

```
選擇一個數字或 (Q) 退出：2 連接埠 2：1) 角色：PrivateWAN 2) 設定方
式：DHCP 3) 取消連接埠變更 4) 套用並返回
```

4. 選取選項 **4** 返回主要功能表。

```
選擇一個數字或 (Q) 退出：4 選取一個項目進行修改，或提交設定：1) 型
號：ion 200v 2) ION 金鑰：xxxxxxxxx-yyyyyyyy-zzz-1234-1234-
abcdefghijkl 3) 密碼金鑰：abcde12345 4) 控制器 1：控制器 - DHCP
 5) 連接埠 1：PublicWAN - DHCP 6) 連接埠 2：PrivateWAN - DHCP
 7) 連接埠 3：已停用/未使用 8) 連接埠 4：已停用/未使用 9) 連接埠 5：
```

 ©2025 Palo Alto Networks, Inc.

```
已停用/未使用 10) 連接埠 6：已停用/未使用 11) 連接埠 7：已停用/未使用
 12) 連接埠 8：已停用/未使用 13) 連接埠 9：已停用/未使用 14) 提交並重新
啟動
```

**STEP 18 |** 儲存並重新啟動連接器。

```
選擇一個數字或 (Q) 退出：14 警告#在提交此設定之後，所有硬體將進行簽署、記
錄，並永久地繫結至 Prisma SDWAN 雲端控制器中的 ION 金鑰/密碼金鑰。這意
味著在此 [SUBMIT（提交）] 功能之後，無法新增/移除硬體（磁碟、網路卡）。如
果在此 [SUBMIT（提交）] 之外需要任何硬體變更，則將需要使用新的 ION 金鑰
和密碼金鑰重新部署 ION。如果需要新增或移除硬體，請在下面回答 'N'，然後關閉
 ION 並立即進行變更。立即提交這些變更嗎？[N]：y 正在建置設定... [VFF:CFG]
 ZeroTouch 設定啟動中 - 設定檔案剖析器 [VFF:CFG] 正在嘗試載入/解析為設
定/INI 檔案。[VFF:CFG] 已成功載入設定樣式檔案。[VFF:CFG] 控制器 1 已成
功設定為 CONTROLLER/DHCP。[VFF:CFG] 連接埠 1 已成功設定為 PUBLICWAN/
DHCP。[VFF:CFG] 連接埠 2 已成功設定為 PRIVATEWAN/DHCP。[VFF:CFG] 警
告：連接埠 3 沒有設定區段。預設為 [Disable（停用）]。[VFF:CFG] 警告：連
接埠 4 沒有設定區段。預設為 [Disable（停用）]。[VFF:CFG] 警告：連接埠
 5 沒有設定區段。預設為 [Disable（停用）]。[VFF:CFG] 警告：連接埠 6 沒
有設定區段。預設為 [Disable（停用）]。[VFF:CFG] 警告：連接埠 7 沒有設定
區段。預設為 [Disable（停用）]。[VFF:CFG] 警告：連接埠 8 沒有設定區段。
預設為 [Disable（停用）]。[VFF:CFG] 警告：連接埠 9 沒有設定區段。預設為
 [Disable（停用）]。[VFF:CFG] 設定/INI 檔案剖析器成功。[VFF:KVM] 功能表設
定結束，繼續正常開機...重新開機原因：製造
```

 ©2025 Palo Alto Networks, Inc.

# 監控 ZTNA 連接器

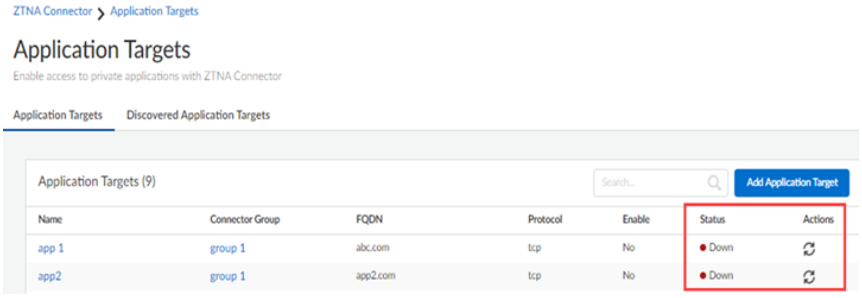
| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 4.0<br>❑ ZTNA 連接器附加元件授權<br>具有附加元件授權的基本授權包括 8 個 ZTNA 連接器、100 個 FQDN 和 4 個 IP 子網路功能。<br>具有附加元件授權的進階授權包括 40 個 ZTNA 連接器、300 個 FQDN 和 1024 個 IP 子網路功能。<br>具有附加元件授權的高級授權包括 200 個 ZTNA 連接器、4000 個 FQDN 和 1024 個 IP 子網路功能。<br>❑ 如果您未購買 ZTNA 連接器附加元件授權，Prisma Access 授權包括四個連接器、40 個 FQDN 和四個 IP 子網路。提供此功能的目的旨在您的環境中試用 ZTNA 連接器。 |

所有 ZTNA 連接器元件都提供清楚的狀態資訊、日誌和診斷工具，以協助您針對任何引發的問題進行疑難排解。使用下列工具監控您的 ZTNA 連接器部署。


©2025 Palo Alto Networks, Inc.

從 Prisma SASE 平台內檢視應用程式和連接器的狀態。

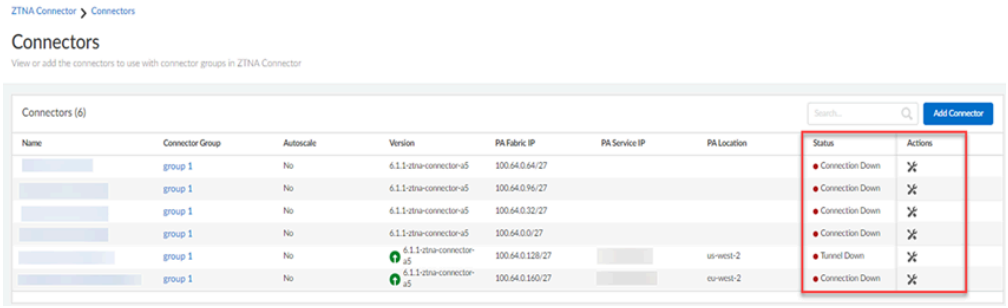
- 選取 **Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Application Targets**（應用程式目標），並驗證所有應用程式目標的 **Status**（狀態） 是否為 **Up**（啟動）。




如果狀態顯示 **Down**（關閉），連接器無法連線您的應用程式。在修復應用程式的問題之後，按一下 **Action**（動作）欄中的重新整理狀態按鈕，並驗證 **Status**（狀態）是否變更為 **Up**（啟動）（狀態每分鐘自動重新整理一次）。

如果可從 ZTNA 連接器連線應用程式（使用上次成功的 DNS 解析結果），但應用程式 FQDN 的 DNS 解析無法從 ZTNA 連接器進行，則狀態也為 [Up（啟動）]。

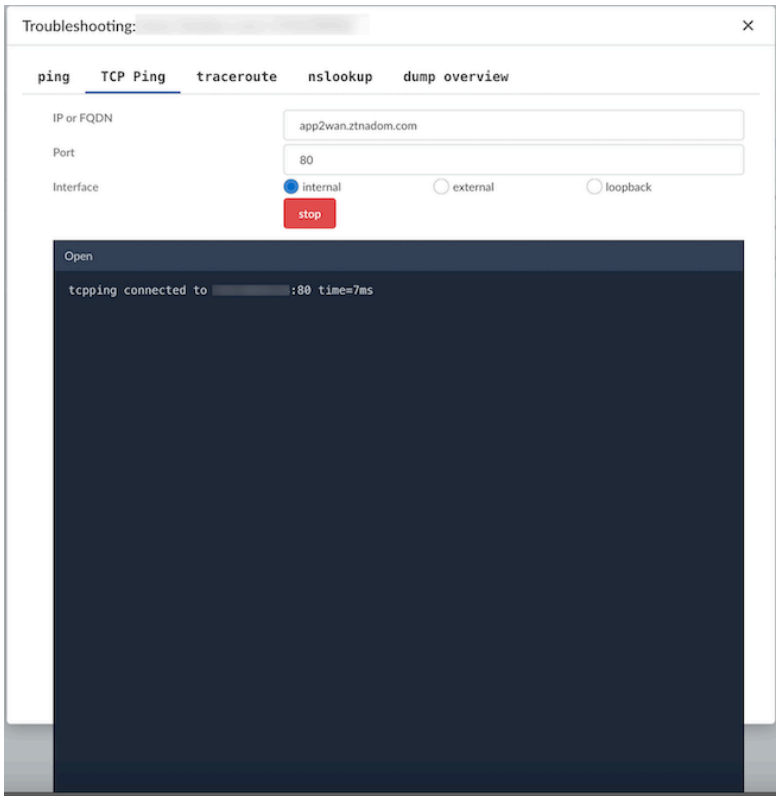
- 選取 **Workflows**（工作流程） > **ZTNA Connector**（**ZTNA** 連接器） > **Connectors**（連接器），並確保所有連接器的 **Status**（狀態）均為 **Up**（啟動）。




如果 **Status**（狀態）顯示 **Tunnel Down**（通道關閉），則表示連接器 VM 與 Prisma Access 之間的 IPSec 通道已關閉。如果 **Status**（狀態） 顯示 **Connection Down**（連線關閉），則表示連接器 VM 已關閉。按一下診斷圖示 啟動連接器的遠端 Shell 連線，以針對問

 ©2025 Palo Alto Networks, Inc.

題進行疑難排解。您可以執行 **ping**、**TCP Ping**、**traceroute**、**nslookup**或 **dump overview** 來協助您診斷連線問題。





©2025 Palo Alto Networks, Inc.

# 檢視 ZTNA 連接器日誌

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 4.0<br>❑ ZTNA 連接器附加元件授權<br>具有附加元件授權的基本授權包括 8 個 ZTNA 連接器、100 個 FQDN 和 4 個 IP 子網路功能。<br>具有附加元件授權的進階授權包括 40 個 ZTNA 連接器、300 個 FQDN 和 1024 個 IP 子網路功能。<br>具有附加元件授權的高級授權包括 200 個 ZTNA 連接器、4000 個 FQDN 和 1024 個 IP 子網路功能。<br>❑ 如果您未購買 ZTNA 連接器附加元件授權，Prisma Access 授權包括四個連接器、40 個 FQDN 和四個 IP 子網路。提供此功能的目的旨在您的環境中試用 ZTNA 連接器。 |

所有 ZTNA 連接器流量都會記錄到 Strata Logging Service。若要將 Prisma Access 日誌儲存在 Strata Logging Service 中，您必須估算並購買 Strata Logging Service 中適當數量的日誌儲存空間。我們建議您將總 Strata Logging Service 容量儲存空間的百分比增加 10%，以儲存 ZTNA 連接器日誌。

請確定您已設定日誌轉送設定檔，將所需日誌類型轉送至 Strata 記錄服務。當日誌儲存空間配額達到 90% 時，Strata Logging Service 會傳送電子郵件通知以購買更多儲存空間。如果您未購買更多儲存空間，舊的日誌將被清除。

無論您用於 Prisma Access 的管理介面為何（Panorama 或雲端管理），您都可以在 **Incidents & Alerts**（事件與警示） > **Log Viewer**（日誌檢視器）下檢視您在 Prisma Access (Managed by Strata Cloud Manager) 中的日誌。

ZTNA 連接器提供下列網路日誌。


©2025 Palo Alto Networks, Inc.

- 稽核日誌 - 可透過 Prisma SASE 平台取得，並提供 ZTNA 連接器中管理員設定變更的記錄。您可以將這些日誌用於合規性和疑難排解目的。

  您可以依時間範圍、網站、裝置和類型篩選稽核日誌。稽核日誌提供下列詳細資訊：

  - 特定使用者從特定 IP 位址嘗試登入企業入口網站的次數。
  - 已裝載還是已刪除應用程式或應用程式連接器。
  - 排程連接器升級時。
  - 檢視所有系統變更和嘗試的存取。

  Prisma Access 網頁介面中無法使用 ZTNA 連接器稽核日誌。若要檢視稽核日誌，您必須向 Palo ALto Networks 技術支援開啟支援案例。
- 流量日誌 - 顯示每個工作階段的開始與結束項目。每個項目都包括日期與時間、來源與目的地區域、位址、連接埠、應用程式名稱、套用至流量的安全性規則名稱、規則動作（允許、拒絕或捨棄）、進入和輸出介面、位元組數，以及工作階段結束原因。
  - [Type（類型）] 欄表示項目用於工作階段的開始還是結束。
  - [Action（動作）] 欄表示防火牆已允許、拒絕還是丟棄工作階段。
  - 丟棄表示封鎖流量的安全性規則指定任何應用程式，而拒絕則表示規則識別特定應用程式。
  - 如果防火牆在識別應用程式之前丟棄流量，例如當規則丟棄特定服務的所有流量時，應用程式欄會顯示「不可應用」。
  - ZTNA 連接器的 App-ID 是自訂的 App-ID。
  - 如果流量命中行動使用者閘道，**Destination Address**（目的地位址）欄會顯示 RFC 6598 IP 位址。
- 設定日誌 - 顯示對 ZTNA 連接器設定進行變更的項目。每個項目都包括日期與時間、管理員使用者名稱、管理員進行變更所在位置的 IP 位址、用戶端類型、執行的命令類型、命令狀態（無論命令成功還是失敗）、設定路徑，以及變更之前和之後的值。
- Strata Cloud Manager
- Panorama

# 檢視 ZTNA 連接器日誌 (Panorama)

使用以下工作流程，在 Prisma Access (Managed by Panorama) Access 中檢視 ZTNA 連接器日誌。

**STEP 1 |** 登入 Prisma Access。

**STEP 2 |** 選擇 **Monitor**（監控） > **Logs**（日誌）。

**STEP 3 |** 從清單中選取日誌類型：**Audit**（稽核）、**Traffic**（流量）和 **Config**（設定）日誌。

**STEP 4 |** 按一下欄標頭右側的箭頭，然後選取 **Columns**（欄）。

**STEP 5 |** 選取要在清單中顯示的欄。日誌會自動更新以符合您選取的項目。

**STEP 6 |** 按一下 **spyglass**（望遠鏡）圖示，以取得特定的日誌項目。**Detailed Log View**（詳細日誌檢視）包含有關工作階段的來源與目的地的更多資訊，以及與日誌項目相關的工作階段清單。


©2025 Palo Alto Networks, Inc.

# 檢視 ZTNA 連接器日誌 (Strata Cloud Manager)

使用下列工作流程，在 Cloud Managed Prisma Access 中檢視 ZTNA 連接器日誌。

**STEP 1 |** 登入 Prisma Access (Managed by Strata Cloud Manager)。

**STEP 2 |** 選取 **Incidents & Alerts**（事件和警示） > **Log Viewer**（日誌檢視器）。

**STEP 3 |** 選取要檢視的日誌類型：稽核防火牆/流量和設定日誌。

**STEP 4 |** 選取您想要檢視日誌的時間範圍。

**STEP 5 |** 提供此查詢字串以縮小 ZTNA 連接器日誌的清單：**Subtype = 'netflow' AND Device Name = 'PA_CONN'** .

日誌包括以下詳細資訊：

- 時間戳記
- 連接器名稱
- 用戶端的原始來源 IP 位址
- 用戶端的原始來源連接埠
- 連接器的轉譯 IP 位址
- 連接器的轉譯連接埠
- 轉譯的目的地 IP 位址
- 轉譯的目的地連接埠


©2025 Palo Alto Networks, Inc.

# 保留 ZTNA 連接器與來源 NAT 連線的 User-ID 對應

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 5.1.1 |

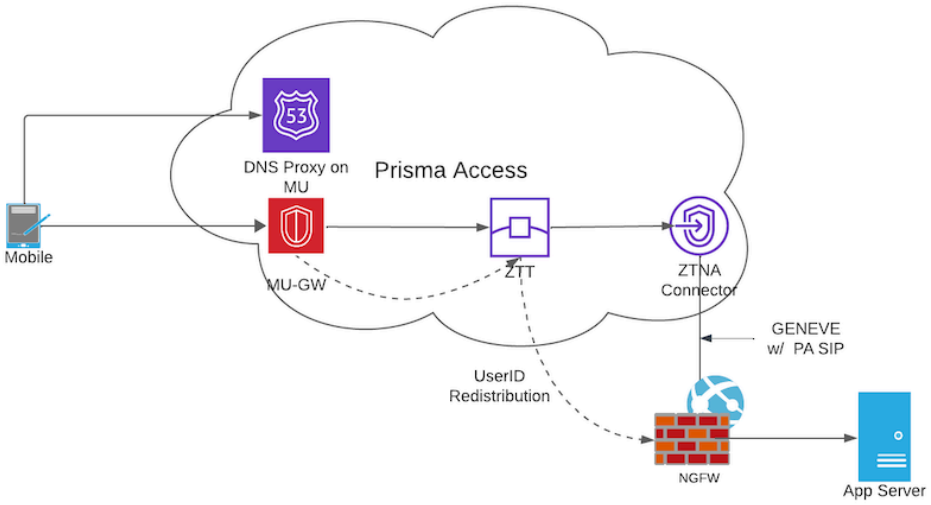
您可以使用 Prisma Access 中的 ZTNA 連接器來保護私人應用程式。若要根據 User-ID 限制對應用程式的存取，您可以在私人應用程式所在的資料中心或總部位置部署新世代防火牆 (NGFW)；然後在 NGFW 上根據 User-ID 對應設定政策規則。

如果您的部署在私人應用程式所在的資料中心或總部位置使用新世代防火牆 (NGFW)，且 ZTNA 連接器執行來源 NAT，則 NGFW 無法擷取 User-ID 對應。ZTNA 連接器上的來源 NAT 會防止 NGFW 取得用戶端 IP 位址，這對於對應而言至關重要。如果 NGFW 無法擷取此用戶端 IP 位址，則它無法強制執行您根據 User-ID 對應在其上建立的區域型安全性政策規則。

ZTNA 連接器具有以下責任，以在 NGFW 保護的資料中心內啟用 User-ID：

1. 提供從 NGFW 到區域 ZTNA 連接器通道終端器 (ZTT) 的安全連線，讓 NGFW 可以連線到其 User-ID 重新散佈代理程式。
2. 對於健康情況探查設定為 tcpping 的 FQDN 應用程式，應用程式會探查資料中心應用程式，以確定該應用程式是否已啟動並可透過此個別連接器進行連線。
3. 將使用者封裝到 Geneve 封包內的應用程式後置 NAT 資料中心空間 IP 封包，包括原始來源 IP 位址作為選項。

下圖說明了將來源 IP 位址至 User-ID 對應提供給 NGFW 的網路元素，其也會將通用網路虛擬化封裝 (Geneve) 封裝的封包（包括原始 Prisma Access 來源 IP 位址選項）傳遞至 NGFW。這些元素使 NGFW 能夠有效地根據 User-ID 強制執行安全性政策規則。




限制：


©2025 Palo Alto Networks, Inc.

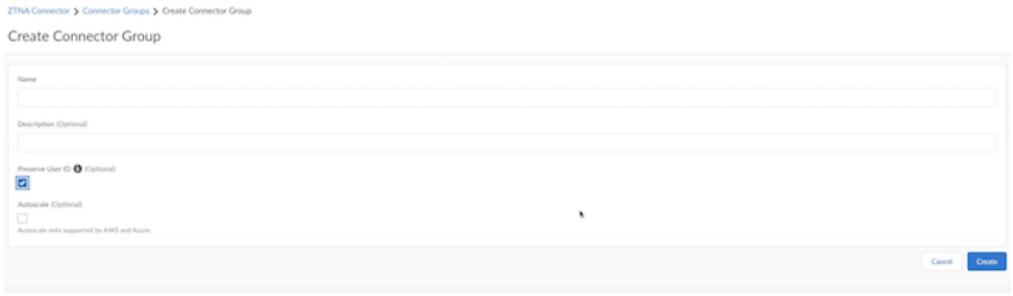
- User-ID 搭配 ZTNA 連接器的支援僅在以下版本之後才提供：
  - Prisma Access 資料平面：10.2.4 版及更新版本
  - Saas_agent：5.1.0 版及更新版本
  - NGFW 版本：11.2.0 版及更新版本
  - 連接器版本：6.2.4-ztna-connector-b3 版本及更新版本
- FQDN 目標不支援 ICMP 探查，這些目標會附加到 User-ID 型連接器群組。
- UID 代理程式的 NGFW 服務路由設定僅支援介面搭配靜態 IP 位址。如果 NGFW 介面設定為處於動態模式（透過 DHCP 指派 IP 位址），則從 NGFW 到 ZTT 的 User-ID 通道無法建立對 ZTNA 連接器 User-ID 的支援。若要解決此問題，您必須使用靜態 IP 位址，設定要在 NGFW 上用於 UID 代理程式的介面。
- User-ID 型連接器不支援 ping 和 traceroute 等診斷工具。

此程序假定您已準備好以下網路設定：

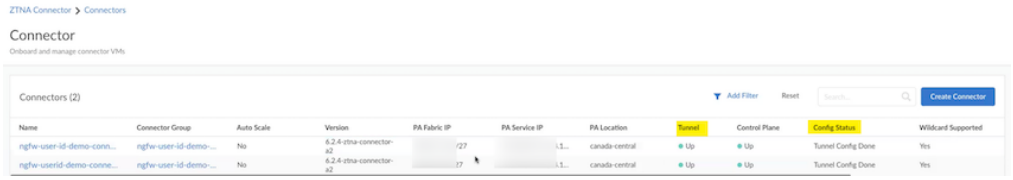
- 您已在私人應用程式所在的總部或資料中心部署了 NGFW。
- 您已根據在 NGFW 中建立的區域（不受信任的區域和受信任的區域）對 NGFW 套用了安全性政策規則。這些安全性政策規則包括 User-ID 強制執行。

若要確保您的網路將 User-ID 對應散佈到總部或資料中心，請完成以下所列的程序，允許 NGFW 根據其從 GlobalProtect 得知的 User-ID 對應強制執行安全性政策規則。

**STEP 1 |** 建立連接器群組、啟用 **Preserve User ID**（保留使用者 **ID**）並新增 Connectors（連接器）。

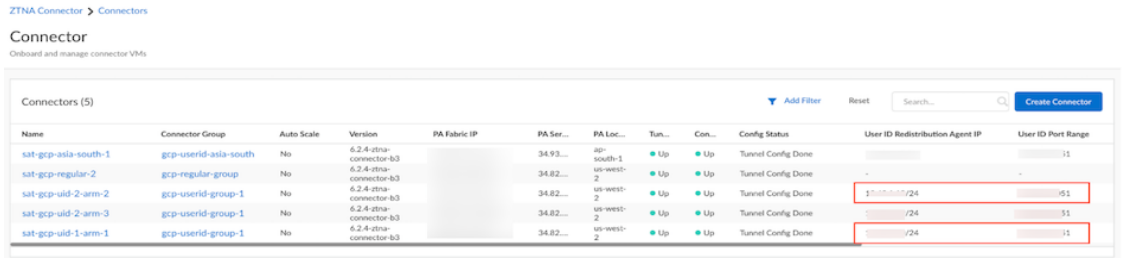



**STEP 2 |** 在資料中心部署並安裝連接器，然後檢查通道是否已啟動並運作。

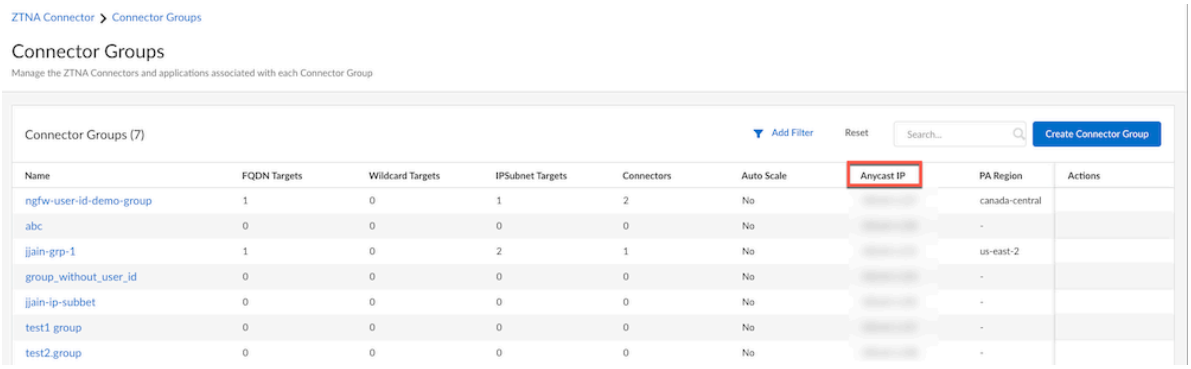



 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 前往 **Connector**（連接器），並為您的連接器記下 **User ID Redistribution Agent IP**（使用者 **ID** 重新散佈代理程式 **IP**）和 **User ID Port Range**（使用者 **ID** 連接埠範圍）。您需要這些 IP 位址和連接埠範圍，才能在 NGFW 上設定 User-ID 重新散佈代理程式。




另外，前往 **Connector Groups**（連接器群組）並記下 **Anycast IP**。需要此 IP 位址，才能設定 NGFW 安全性政策規則，以允許從這個來源 IP 位址進行 TCP 應用程式探查。



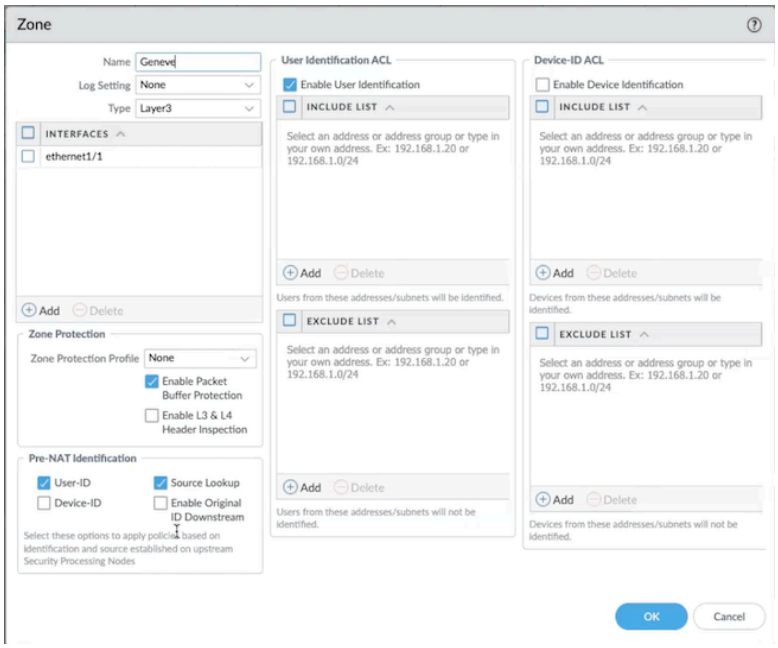

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 在 NGFW 上輸入預先 NAT 識別參數。

1. 登入 NGFW 介面，然後前往 **Network**（網路） > **Zones**（區域），並**Add**（新增）兩個區域（介面連線 ZTNA 連接器所用的區域，以及介面連線應用程式伺服器所用的區域）或選取現有的區域。

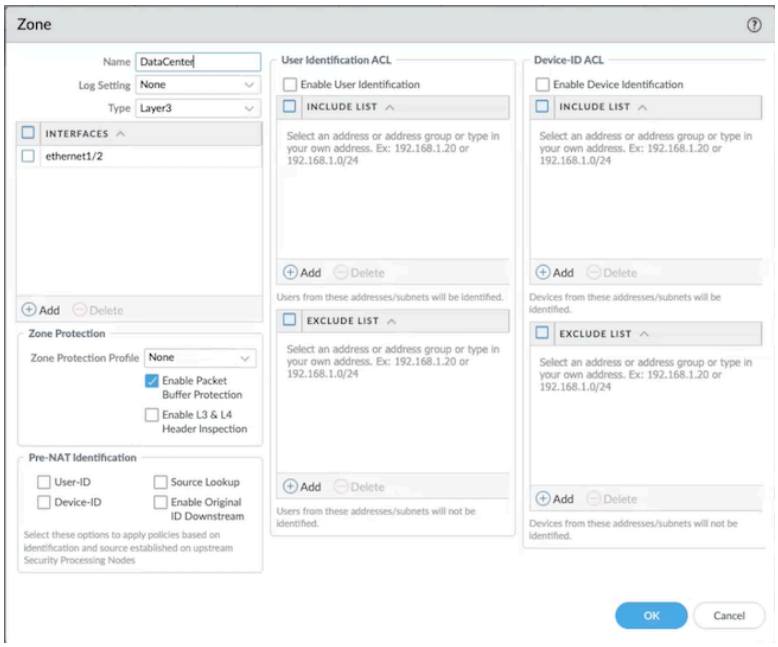
   1. 為其中介面連線 ZTNA 連接器的區域選取以下 **Pre-NAT Identification**（預先 **NAT** 識別）參數：

      - **User-ID**—保留 IP 位址進行 NAT 之前所使用的行動使用者 User-ID 對應。如果您要在安全性政策規則中使用 User-ID，請啟用此項。
      - **Source Looku**（來源查閱）—使您能夠符合從 GlobalProtect 收到的原始來源 IP 位址。




   2. 對於連線至應用程式伺服器區域的介面，您無需選取任何 **Pre-NAT Identification**（預先 **NAT** 識別）參數。

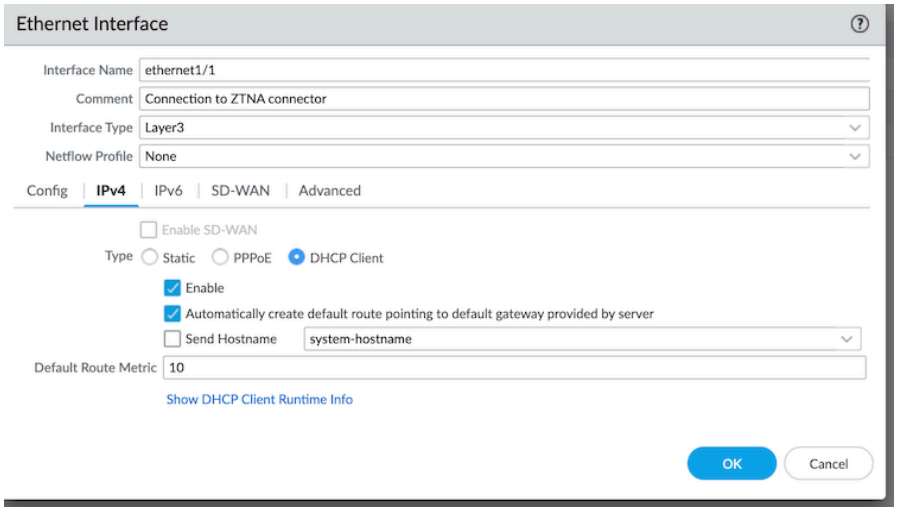
 ©2025 Palo Alto Networks, Inc.




3. 按一下 **OK**（確定）並 **Commit**（交付）變更。

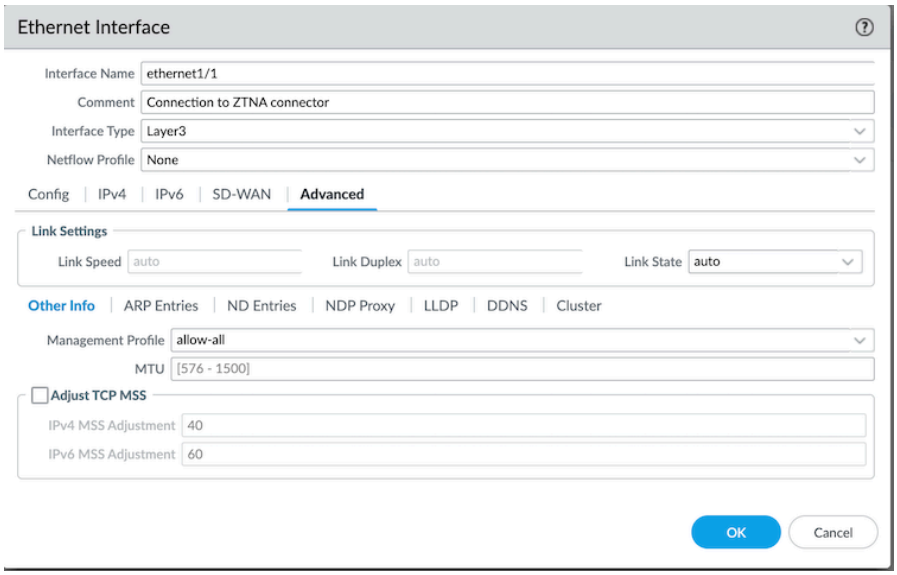
2. 將 IP 位址新增至介面。

   1. 前往 **Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路）。
   2. 選取連線至 ZTNA 連接器和應用程式伺服器的介面，並進行設定。新增 **Interface name**（介面名稱），並將 **Interface type**（介面類型）新增至 **Layer 3**（第三層）。




   3. 對於連線至應用程式伺服器的乙太網路介面，請取消選取 **Automatically create default route pointing to default gateway provided by server**（自動建立指向伺服器所提供之預設閘道的預設路由）核取方塊。

 ©2025 Palo Alto Networks, Inc.




3. 前往 **Interfaces**（介面）並將靜態 IP 位址新增至介面。將面向 ZTNA 連接器的介面新增至 ZTNA 連接器區域 (Geneve)，並將面向應用程式伺服器的介面新增至應用程式伺服器區域（資料中心）。

**STEP 5 |** 使用 NGFW 建立命令列介面 (CLI) 工作階段，並在設定模式下輸入以下命令：

```
set deviceconfig setting preserve-prenat-feature yes
```

如果未來需要停用此功能，請輸入 `set deviceconfig setting preserve-prenat-feature no`。

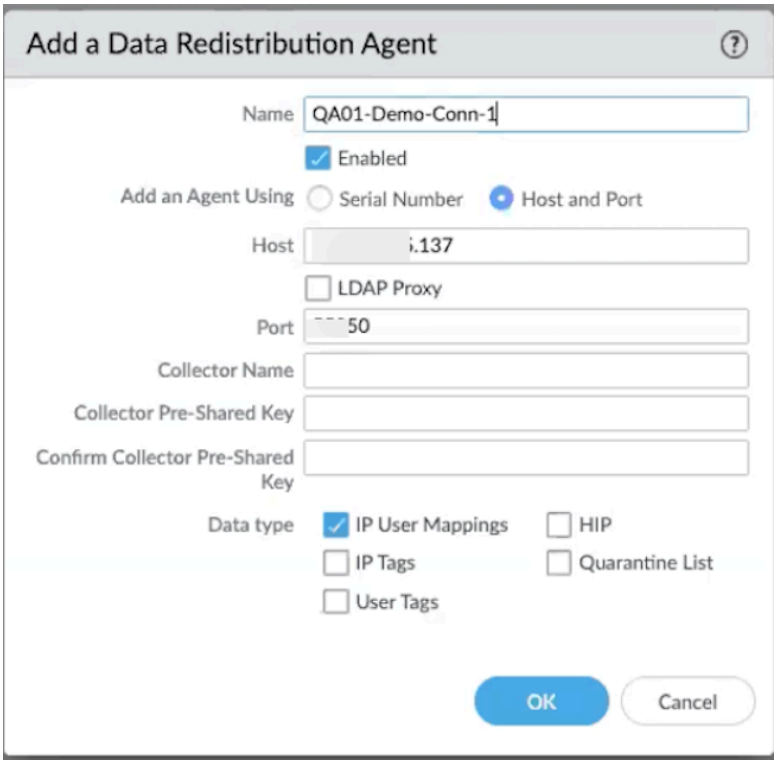

©2025 Palo Alto Networks, Inc.

**STEP 6 |** 設定 *User-ID* 重新散佈時，您必須為步驟 *3* ***User ID Port Range***（使用者 ***ID*** 連接埠範圍）中指定範圍內的每個連接埠新增重新散佈代理程式項目。例如，如果範圍為 *55050-55055*，則您必須設定 *6* 個項目，與您已部署的 *ZTNA* 連接器區域數目保持一致。

對於範圍內的每個連接埠，從步驟 *3* 中的 ***User ID Redistribution Agent IP***（使用者 ***ID*** 重新散佈 ***IP***）為 ***Host***（主機）欄位選取一個 *IP* 位址。如果您需要 *ZTNA* 連接器層級的備援，您可以從 ***User ID Redistribution Agent IP***（使用者 ***ID*** 重新散佈 ***IP***）中選取兩個位址，並為這兩個 *IP* 位址套用完整連接埠範圍。或者，可以設定 ***User ID Redistribution Agent IP***（使用者 ***ID*** 重新散佈 ***IP***）中所有 *IP* 位址上的所有連接埠。

使用 **User ID Redistribution Agent IP**（使用者 **ID** 重新散佈 **IP**）中的一個或多個位址，為範圍 **User ID Port Range**（使用者 **ID** 連接埠範圍）中的每個連接埠新增一個重新散佈代理程式。

1. 在 NGFW UI 上，前往 **Device**（裝置），然後選取 **Data Redistribution**（資料重新散佈）。
2. 按一下 **Add**（新增）、新增 **Name**（名稱），然後選取 **Enabled**（已啟用）核取方塊。
3. 選取 **Host and Port**（主機和連接埠）、在 **Host**（主機）欄位中新增來自步驟 3 的 **User ID Redistribution Agent IP**（使用者 **ID** 重新散佈代理程式 **IP**），然後新增步驟 3 中複製的 **User ID Port Range**（使用者 **ID** 連接埠範圍）。
4. 啟用 **IP User Mappings**（**IP** 使用者對應）核取方塊，並按一下 **OK**（確定）。

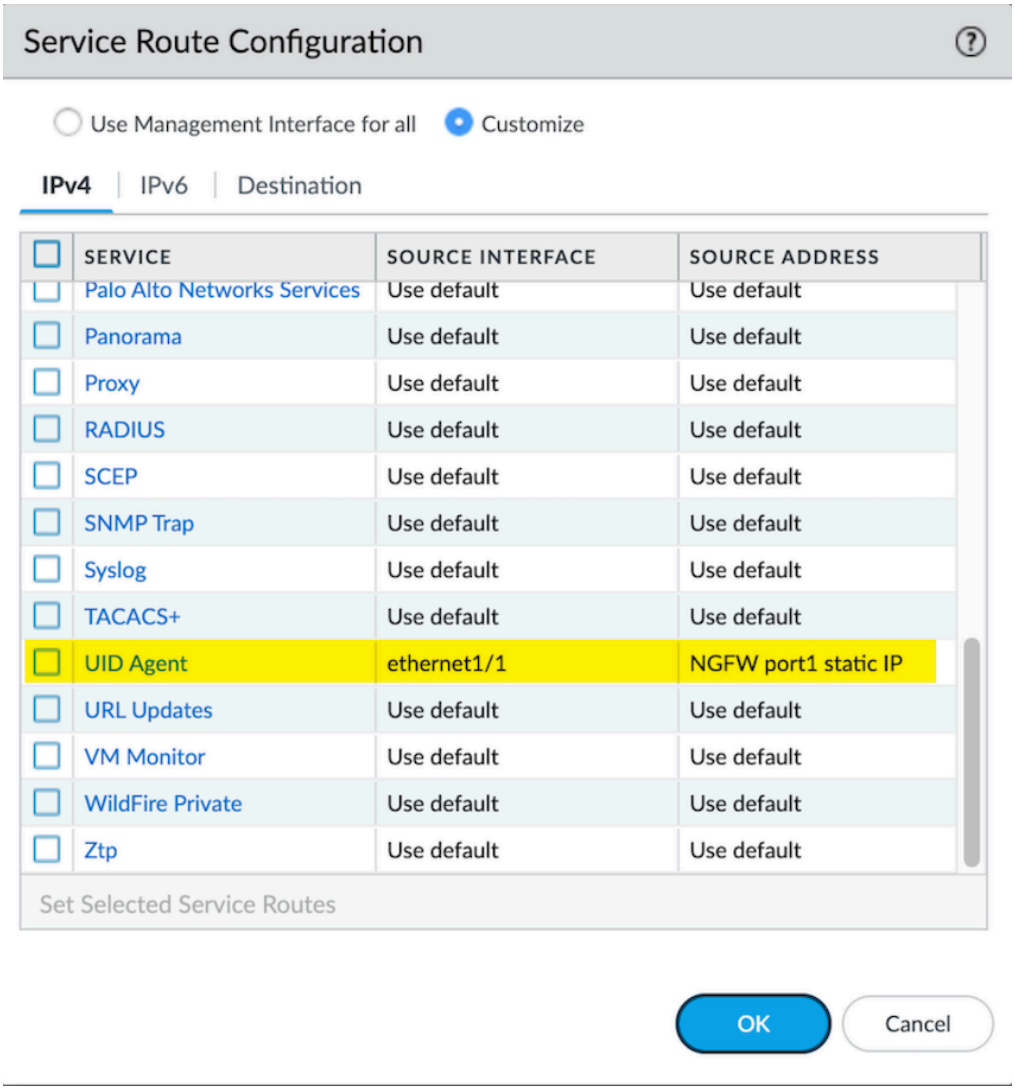



5. **Commit**（提交）以儲存設定。

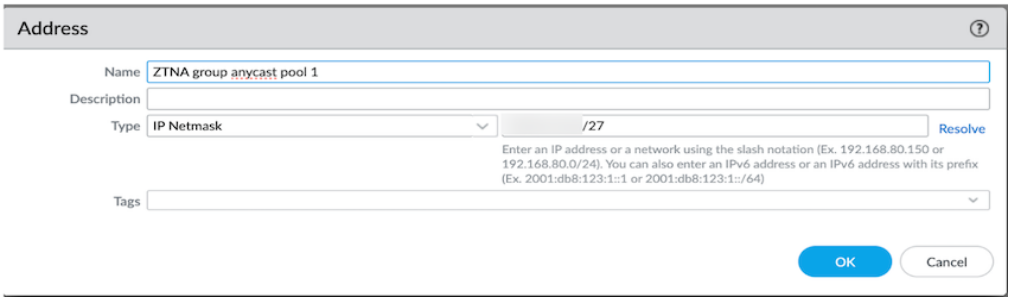

©2025 Palo Alto Networks, Inc.

**STEP 7 |** 在 NGFW UI 上，前往 **Device**（裝置） > **Setup**（設定） > **Services**（服務） > **Service Route Configuration**（服務路由設定） > **Customize**（自訂） > **UID agent**（**UID** 代理程式）。

1. 在 **IPv4** 下，選取 **SOURCE INTERFACE**（來源介面）作為 **Ethernet1/1**（乙太網路**1/1**）（面向 ZTNA 連接器的介面），然後新增 **SOURCE ADDRESS**（來源位址）。



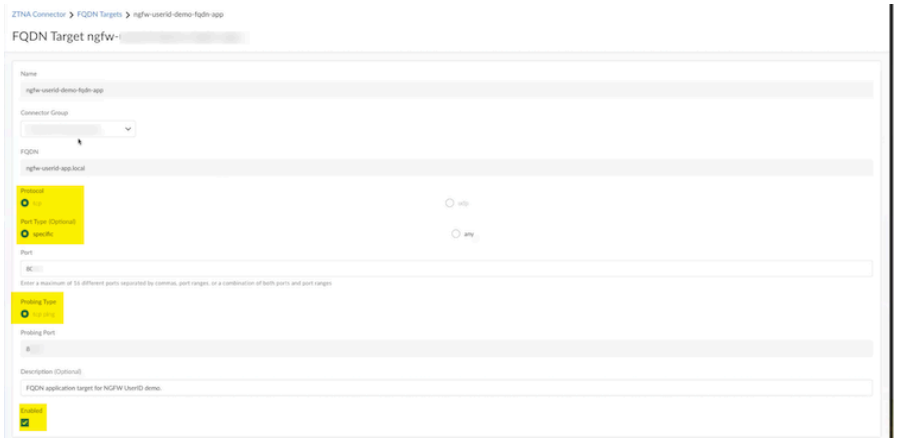

**STEP 8 |** 新增安全性政策規則，允許具有來源 IP 位址的 TCP 封包。新增來源 IP 位址，即步驟 3 中複製的 Anycast IP 位址，然後按一下 **OK**（確定）。



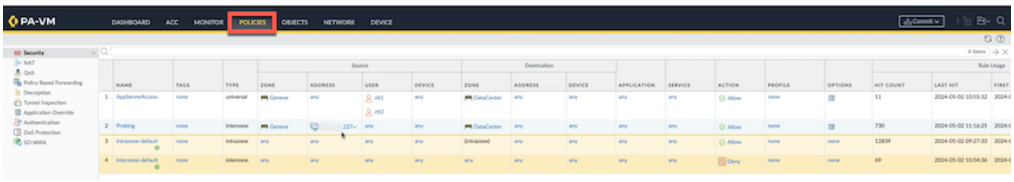

 ©2025 Palo Alto Networks, Inc.

**STEP 9 |** （選用）啟用 TCP 探查。

1. 若要建立 FQDN 目標：
   1. 前往 **Workflows**（工作流程） > **Application Targets**（應用程式目標） > **FQDN Targets**（**FQDN** 目標），然後按一下 **Create FQDN Target**（建立 **FQDN** 目標）。
   2. 新增 **Name**（名稱）並選取 **Connector Group**（連接器群組）。
   3. 啟用 **tcp**、**specific**、**tcp ping** 和 **Enabled**（已啟用）。新增 **Port**（連接埠）並按一下 **Create**（建立）。




**STEP 10 |** 在 NGFW UI 上，前往 **Policies**（政策）並定義 User-ID 型政策。




 ©2025 Palo Alto Networks, Inc.

# 設定動態權限存取設定

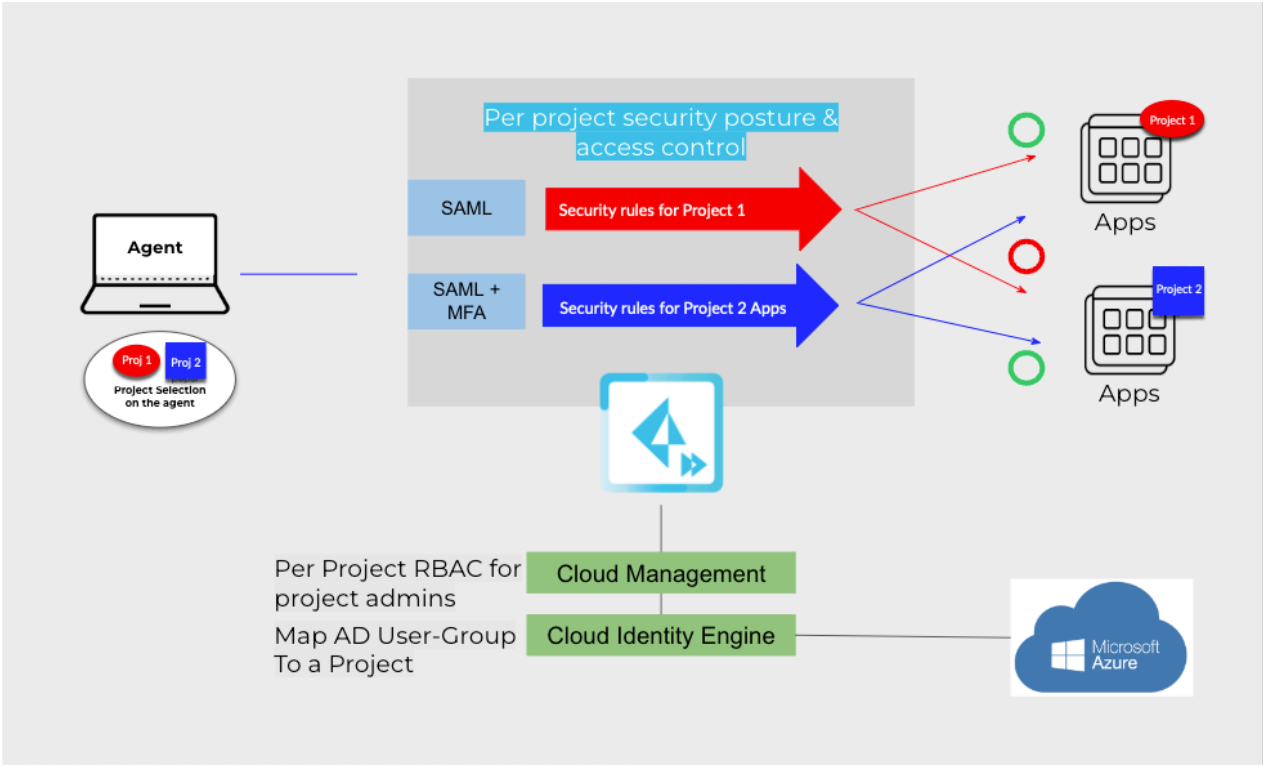
| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 授權<br>❑ Prisma Access 5.1<br>❑ 角色：超級使用者 |

對於需要控制哪些使用者有權存取其客戶專案的 IT 企業和 IT 啟用服務 (ITES) 公司來說，動態權限存取提供一種無縫、安全且隔開的方式，讓您的使用者只能存取指派給他們的專案。這些公司通常會將數個客戶專案指派給員工，並提供對這些專案的獨立存取，以便授權使用者一次只能訪問一個客戶專案。

# 什麼是動態權限存取？

動態權限存取是 Prisma Access 中的功能，根據您使用者在 Prisma Access Agent 選取的工作流程或專案，為您的使用者提供動態權限。您的使用者可以根據指派給專案的使用者群組和 IP 集區組合擁有動態權限。這種獨特的組合定義了一個專案。透過動態權限存取，您可以隔離網路中的資源，以便您的使用者只能根據指派給他們的專案來存取這些資源。

稱為 **Project Admin**（專案管理員）的新預先定義角色可在 Prisma Access 上使用，以允許專案管理員建立和管理專案定義。專案管理員能夠對應項目以選取 Prisma Access 位置群組，並根據專案和位置群組使用 DHCP 建立 IP 位址指派。專案管理員只能管理在 Strata Cloud Manager 中指派給他們的專案。




當您的一般使用者登入在其受管理的裝置上針對動態權限存取而啟用的 Prisma Access Agent，會發生以下工作流程：

1. 您的一般使用者選取指派給他們的專案（例如，專案 1）。
2. 他們的身分會在雲端識別引擎中進行驗證，而該引擎會將使用者的使用者群組對應至專案。
3. 驗證成功且其使用者群組滿足專案管理員設定的專案準則後，使用者可以透過專案 1 的專案特定設定和安全性規則來存取網路中的資源，這些規則會根據每個專案提供安全性態勢和存取控制。安全性基礎結構會套用安全性規則，來限制使用者只能存取屬於該專案的資源和應用程式。不允許存取其他專案中的資源和應用程式。
4. 當使用者切換到不同的專案（例如，專案 2）時，他們會從前一個專案（專案 1）登出。然後，他們可以根據該專案的專案特定設定和安全性規則，存取第二個專案的資源。

您可以使用 Strata Cloud Manager 監控使用者的專案活動，了解您的 Prisma Access Agent 部署，並檢視網路中的服務耗用和安全性態勢。


©2025 Palo Alto Networks, Inc.

# 透過 Common Services 為 Prisma Access 啟用動態權限存取

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 授權，具有行動使用者訂閱<br>❑ 啟動連結<br>❑ Strata Logging Service<br>❑ 雲端識別引擎<br>❑ Prisma Access Agent<br>❑ 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 |

透過動態權限存取，IT 管理員可以將一般使用者對應到數個客戶專案。授權使用者一次只能存取一個客戶專案。

（動態權限存取）是啟動新 Prisma Access 租用戶期間的選用功能。在您啟用此功能且租用戶已啟動之後，DPA 是針對租用戶的壽命設定的，並且您無法將其停用。

僅在第一次啟動新 Prisma Access 租用戶期間，才會提供一次啟用 DPA 的選項。在啟動租用戶之後，該選項會對以下所有啟動（包括附加元件和續訂）隱藏起來。它不適用於現有租用戶。

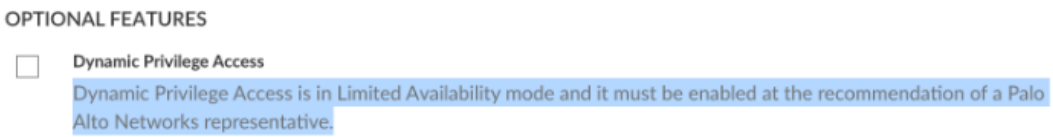
**STEP 1 |** 請聯絡您的 Palo Alto Networks 客戶代表，為您的租用戶啟動此功能。

**STEP 2 |** 啟動 您的 Prisma Access (Managed by Strata Cloud Manager) 授權。

**STEP 3 |** 確保配置授權、規劃服務連線，並相應地 新增其他位置。

**STEP 4 |** 啟用可用的附加元件。

**STEP 5 |** 選取 **Dynamic Privilege Access**（動態權限存取）的核取方塊。




**STEP 6 |** **Agree to the terms and conditions**（同意條款和條件）。

**STEP 7 |** **Activate Now**（立即啟動）。您正在啟動的產品和附加元件（例如 Prisma Access 或 Strata Logging Service）現已完成佈建。當訂閱啟動時，將顯示進度狀態。當程序完成時，租用戶狀態會顯示為 Up（啟動）。您現在已為租用戶佈建了您所購買產品的執行個體。租用戶有一個使用者—您在開始此程序時使用的帳戶。


©2025 Palo Alto Networks, Inc.

**STEP 8 |** 若要完成剩餘的產品設定，您必須存取您購買的產品，並執行任何所需的後置安裝設定。如需您產品的相關資訊，請參閱：

- 開放 API
- Strata Logging Service 入門指南
- Prisma Access (Managed by Strata Cloud Manager) 管理員指南
- 雲端識別引擎入門指南

**STEP 9 |** 新增使用者存取並指派角色。

根據專案以 **Project Admin**（專案管理員）身分將存取權提供給使用者。


©2025 Palo Alto Networks, Inc.

# 在雲端識別引擎中授權使用者群組對應進行動態權限存取

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access授權<br>❑ 最低必要 Prisma Access 版本：5.1<br>❑ 角色：超級使用者 |

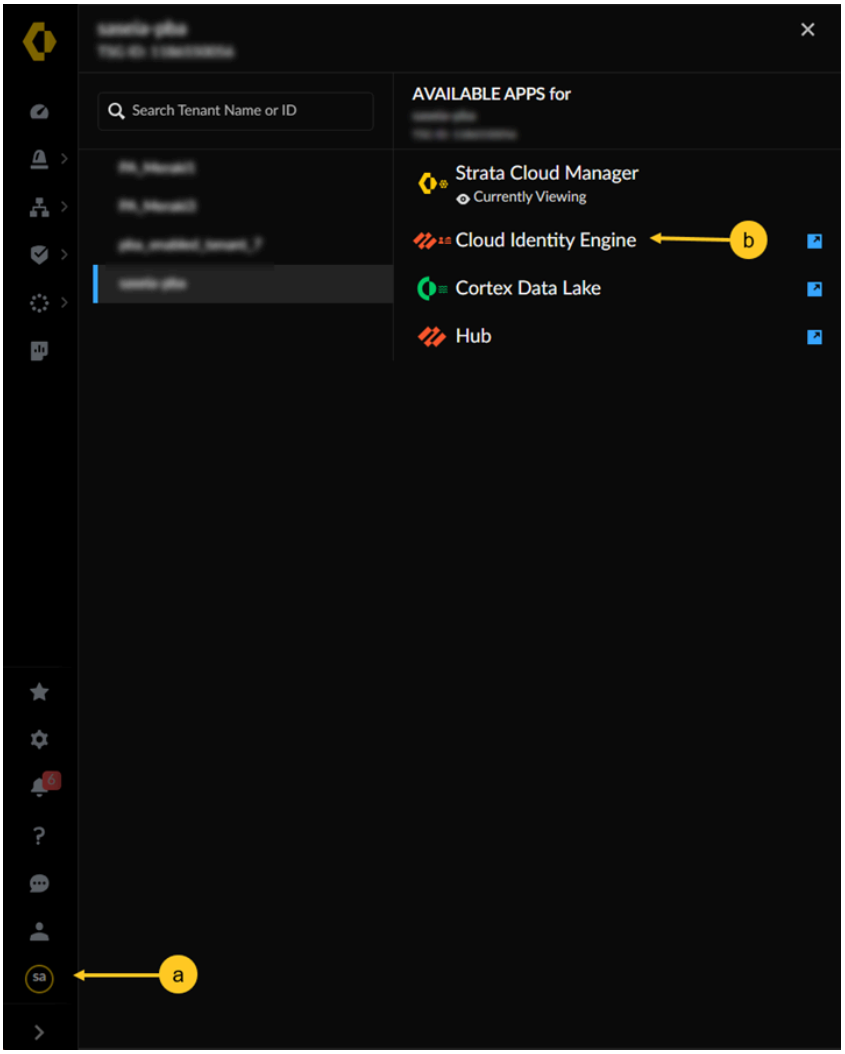
開始之前，請確保您已完成下列先決條件。

- 請聯絡您的 Palo Alto Networks 客戶代表，以啟動動態權限存取功能
- 啟動雲端識別引擎並建立您的第一個租用戶。
- 設定雲端識別引擎。

在此工作流程中，我們已使用 Azure 作為 IdP。您也可以使用 Okta 作為 IdP。


©2025 Palo Alto Networks, Inc.

**STEP 1 |** 從 Strata Cloud Manager 中，開啟與您租用戶相關聯的雲端識別引擎應用程式。



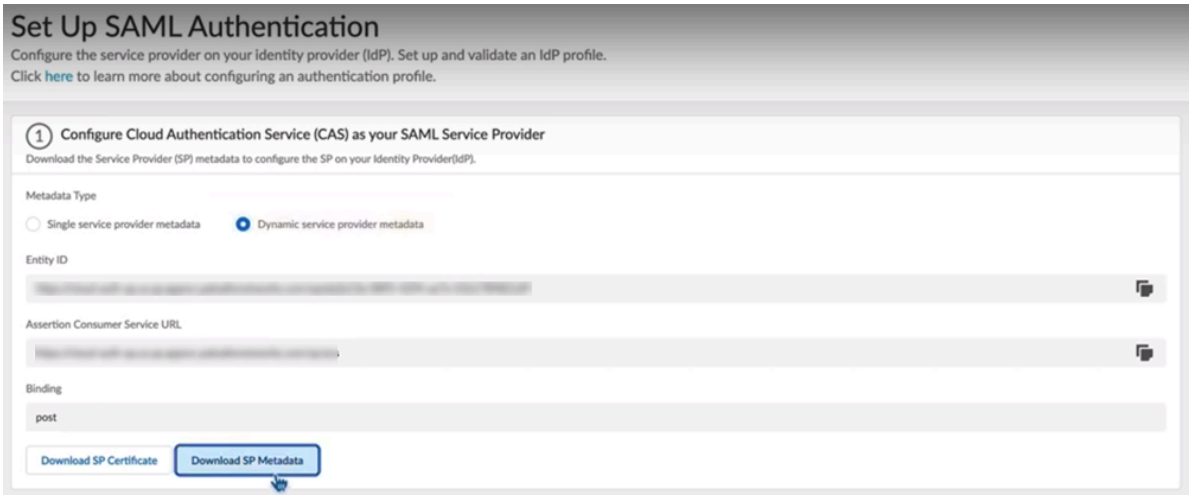

**STEP 2 |** 新增 Azure 目錄 或 Okta 目錄 作為行動使用者的 IdP。


©2025 Palo Alto Networks, Inc.

**STEP 3 |** 下載雲端識別引擎中的 SP 中繼資料。

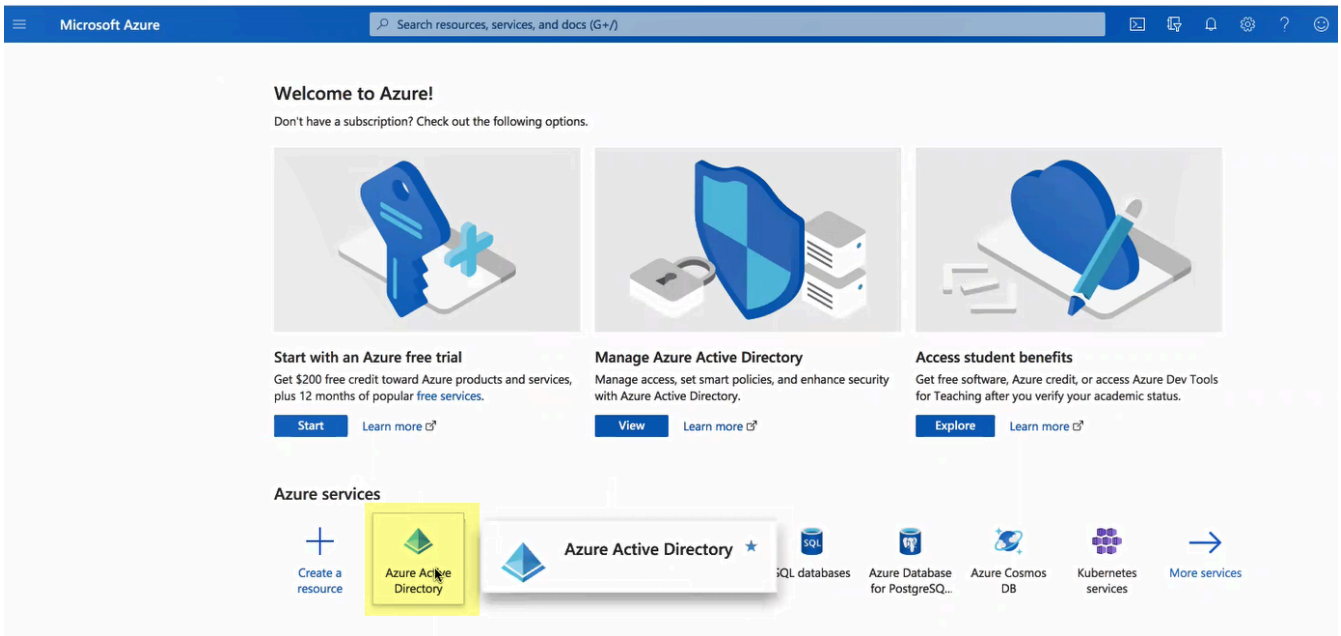
1. 前往 **Authentication**（驗證） > **Authentication Types**（驗證類型） > **Add New Authentication Type**（新增驗證類型）。
2. **Set Up**（設定）SAML 2.0 驗證類型。

   選取 **Dynamic service provider metadata**（動態服務提供者中繼資料）。
3. **Download SP Metadata**（下載 **SP** 中繼資料）。



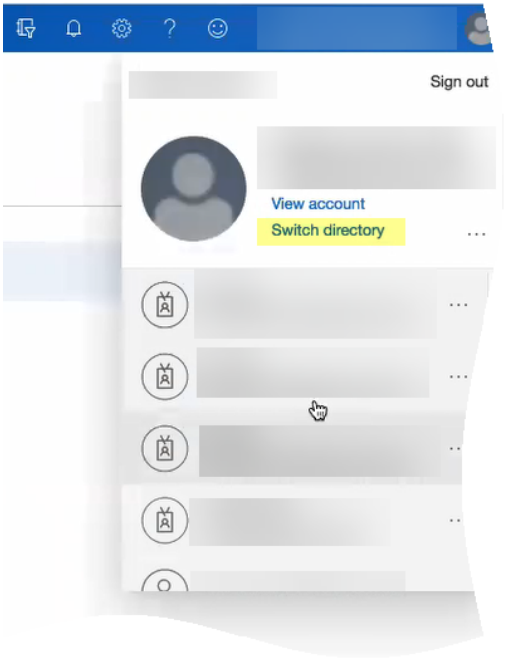

4. 登入 Azure 入口網站並選取 **Azure Active Directory**。

   確保您完成了 Azure 入口網站中所有必要的步驟。

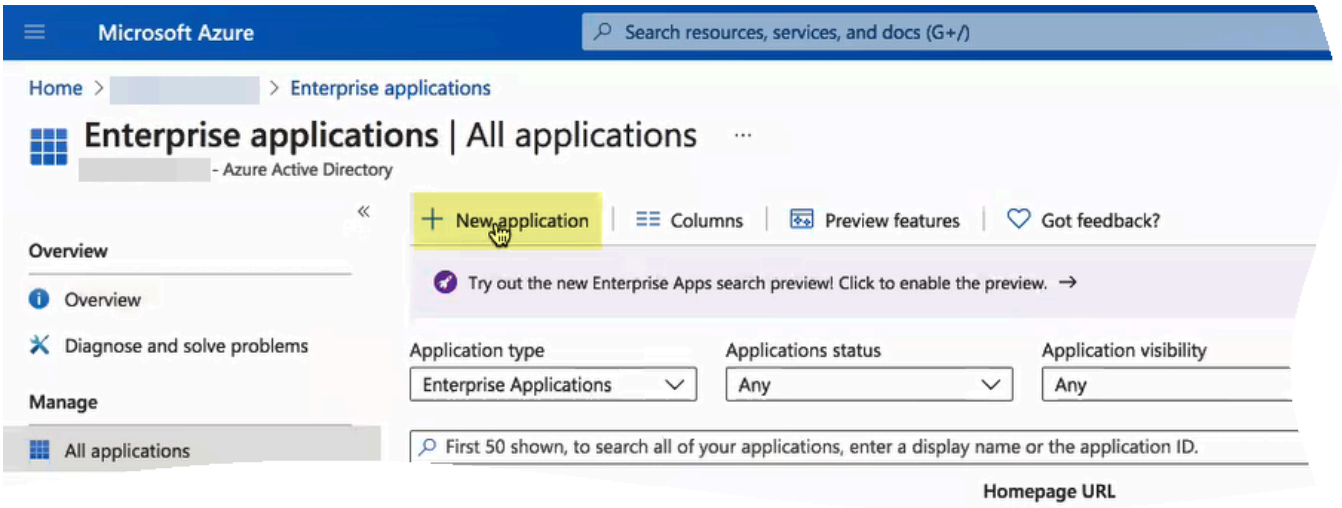



   如果您有多個目錄，請 **Switch directory**（切換目錄）以選取要與雲端識別引擎搭配使用的目錄。


©2025 Palo Alto Networks, Inc.




5. 選取 **Enterprise applications**（企業應用程式）並按一下 **New application**（新增應用程式）。




6. 尋找 **Palo Alto Networks Cloud Identity Engine - Cloud Authentication Service**（**Palo Alto Networks** 雲端驗證服務 **-** 雲端驗證服務，並建立 Azure Active Directory (AD) 單一登入整合。

   在建立應用程式時，如有需要，請自訂應用程式名稱。

7. 在應用程式載入之後，選取 **Users and groups**（使用者和群組），然後選取 **Add user/group**（新增使用者/群組），將它們 **Assign**（指派）給這個應用程式。

   選取要在雲端識別引擎中使用 Azure IdP 進行驗證的使用者和群組。

   務必指派您正在使用的帳戶，以便在設定完成時您可以測試該設定。在新增帳戶之後，您可能需要重新整理頁面才能成功完成測試。


©2025 Palo Alto Networks, Inc.

8. **Set up single sign-on**（設定單一登入），然後選取 **SAML**。
9. **Upload Metadata File**（上傳中繼資料），方法為瀏覽至您在步驟 3.c 中從雲端識別引擎下載的中繼資料檔案，然後按一下 **Add**（新增）。
10. 在中繼資料上傳之後，使用以下格式輸入您的區域端點作為 **Sign-on URL**（登入 **URL**）：https://<RegionUrl>.paloaltonetworks.com/sp/acs（其中 <RegionUrl> 是您的區域端點）。

    或者，將回覆 URL 複製到登入 URL。
11. **Save**（儲存）您的設定。

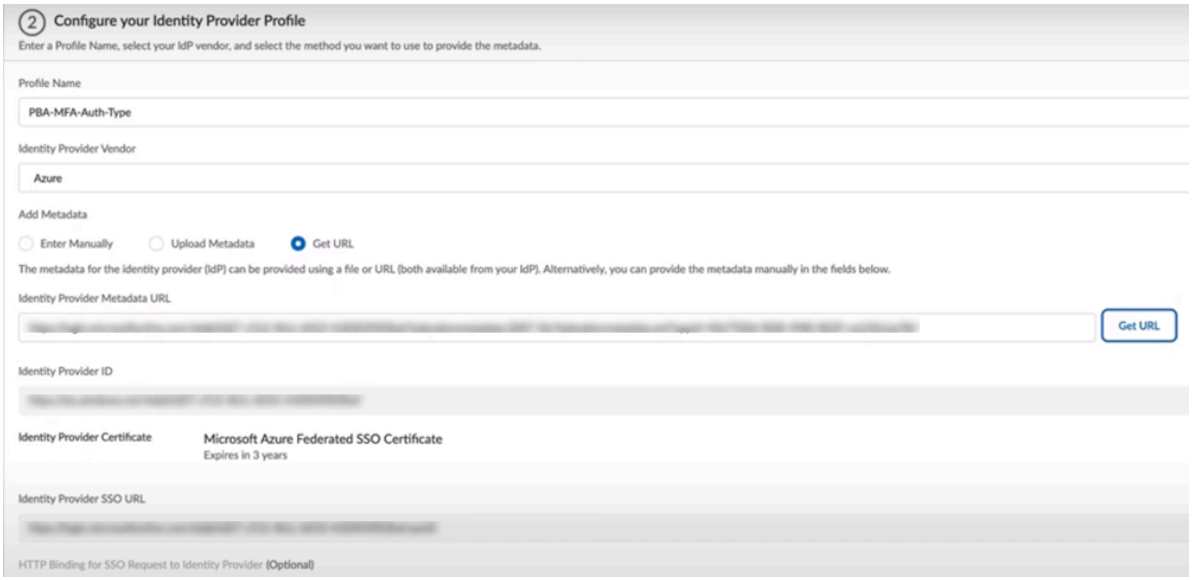
**STEP 4 |** 設定條件式存取政策，以在選取的使用者群組上啟用 MFA。

1. 前往您應用程式的 **Overview**（概要） > **Conditional Access**（條件式存取） > **Create a policy**（建立政策）。
2. 新增 **New Policy**（新政策）。
3. 輸入政策的名稱。
4. 在 **Users**（使用者）區段中，包括 **Select users and groups**（選取使用者和群組），並相應地選擇您的專案群組。
5. 驗證 **Target resources**（目標資源）。
6. 選取觸發政策的 **Conditions**（條件）。
7. 使用 **Require multifactor authentication**（需要多因素驗證），在 **Access Controls**（存取控制）中**Grant**（授與）存取權。
8. 透過將選取器切換到 **ON**（開啟）來啟用政策，然後 **Create**（建立） 條件式存取。

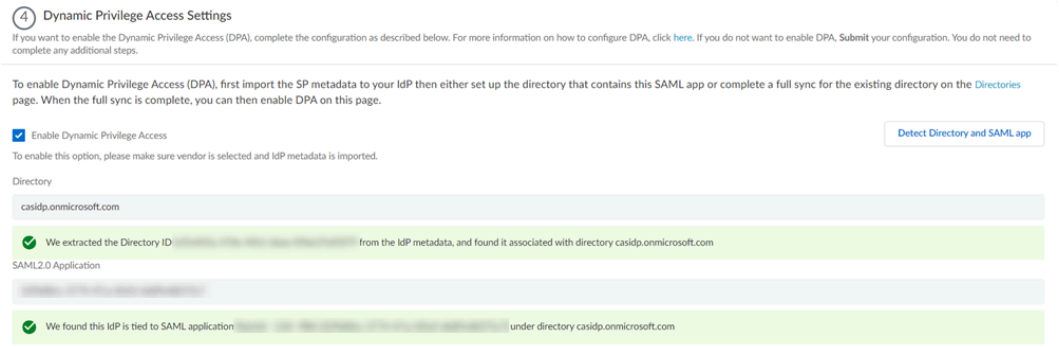

©2025 Palo Alto Networks, Inc.

**STEP 5 |** 將您的 IdP 廠商新增為驗證類型。

1. 選取 **Single sign-on**（單一登入） > **SAML Certificates**（**SAML** 憑證），然後複製 **App Federation Metadata URL**（應用程式聯合中繼資料 **URL**）。
2. 在雲端識別引擎應用程式中，選取 **Authentication**（驗證） > **Authentication Types**（驗證類型） > **Add New Authentication Type**（新增驗證類型）。
3. **Set Up**（設定）SAML 2.0 驗證類型。
4. 在 **Configure your Identity Provider Profile**（設定您的識別提供者設定檔）下，輸入 **Profile Name**（設定檔名稱）。
5. 選取 **Azure** 作為您的 **IDP Vendor**（**IDP** 廠商）。
6. 選取 **Get URL**（取得 **URL**）、貼上步驟 5.a 中的 URL，然後 **Get URL**（取得 **URL**）以取得中繼資料。




7. 啟用 **Multi-factor Authentication is Enabled on the Identity Provider**（在識別提供者上啟用多因素驗證）。
8. **Test SAML Setup**（測試 **SAML** 設置）以驗證設定檔設定。
9. 選取您想要 Prisma Access 用於驗證的 SAML 屬性。
10. 啟用 **Dynamic Privilege Access**（動態權限存取）。
    確保同步您在步驟 2 中新增的目錄和 SAML 應用程式。




11. **Submit**（提交）IdP 設定檔。

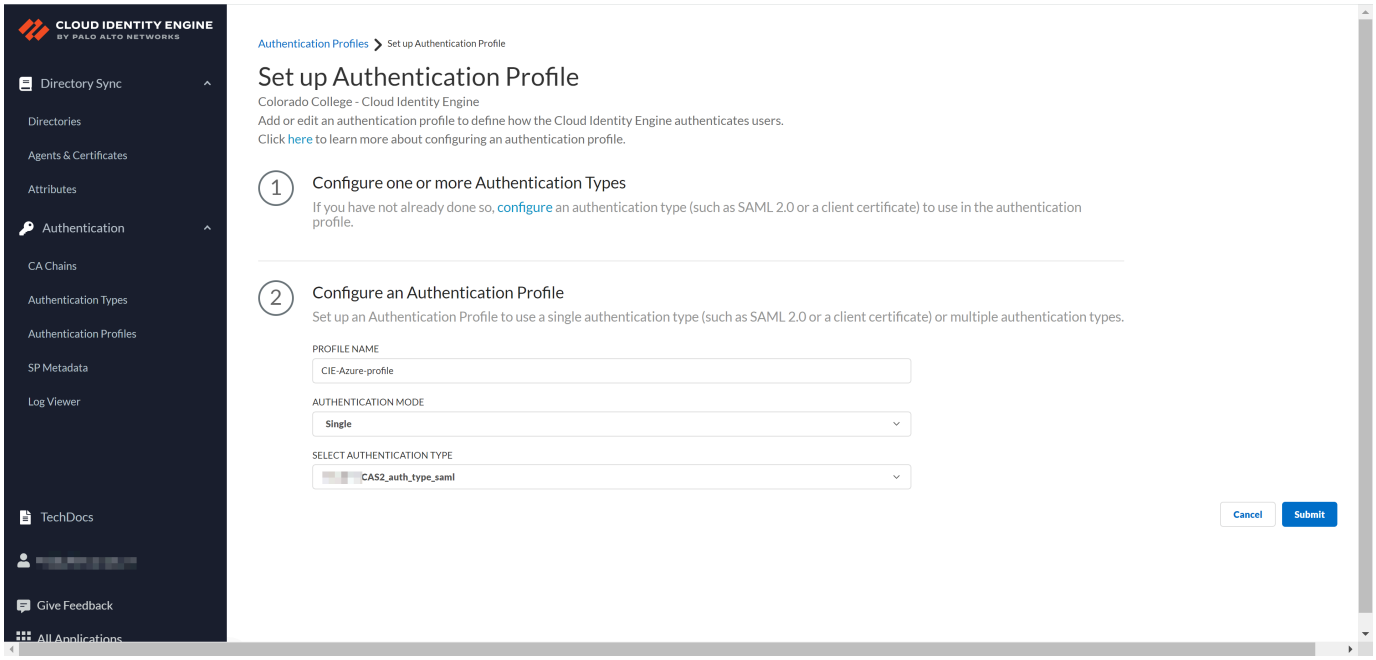
 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** 重複步驟 3 至 5，為不需要 MFA 的使用者群組設定 SAML 應用程式。

不要在步驟 5.g 中，為不需要 *MFA* 的使用者群組中啟用 *MFA*。

**STEP 7 |** 為 MFA 使用者群組和非 MFA 使用者群組新增驗證設定檔。

1. 選取 **Authentication**（驗證） > **Authentication Profiles**（驗證設定檔） > **Add Authentication Profile**（新增驗證設定檔）。
2. 輸入 **PROFILE NAME**（設定檔名稱）。
3. 選取 **Authentication Mode**（驗證模式)。
4. 根據需要 MFA 的使用者群組，從步驟 5 或 6 選取 **Authentication Type**（驗證類型），然後 **Submit**（提交）。

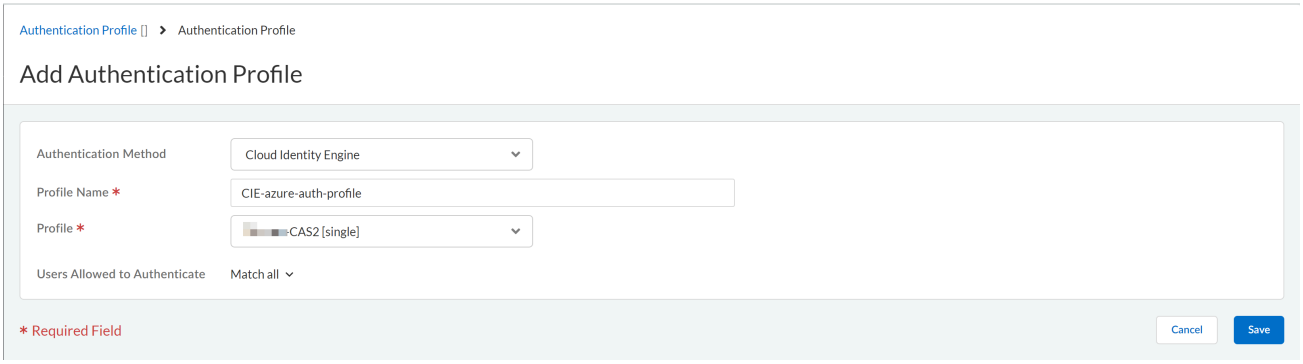



 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** 將驗證設定檔從雲端識別引擎新增至 Prisma Access。

1. 在 Strata Cloud Manager 中，選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Identity Services**（識別服務） > **Authentication**（驗證） > **Authentication Profiles**（驗證設定檔）。

   確保將設定範圍設定為 **Access Agent**（存取代理程式）行動使用者容器。
2. **Add Profile**（新增設定檔）。
3. 選取 **Cloud Identity Engine**（雲端識別引擎） 作為您的 **Authentication Method**（驗證方法）。
4. 輸入 **Profile Name**（設定檔名稱）。
5. 從步驟 7 選取您在雲端識別引擎中新增的 **Profile**（設定檔）。
6. **Save**（儲存）變更。




**STEP 9 |** 將驗證附加至行動使用者。

1. 從 Strata Cloud Manager 啟動 Prisma Access。
2. 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**）。
3. 將範圍設定為您建立的專案片段，然後導覽至 **Security Services**（安全性服務） > **Security Policy**（安全性政策）。
4. 建立一個政策，僅允許來自特定專案 DHCP 範圍和該專案型使用者群組的流量。


©2025 Palo Alto Networks, Inc.

# 啟用存取代理程式

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ Prisma Access 授權，具有行動使用者訂閱<br>❑ 角色：超級使用者 |

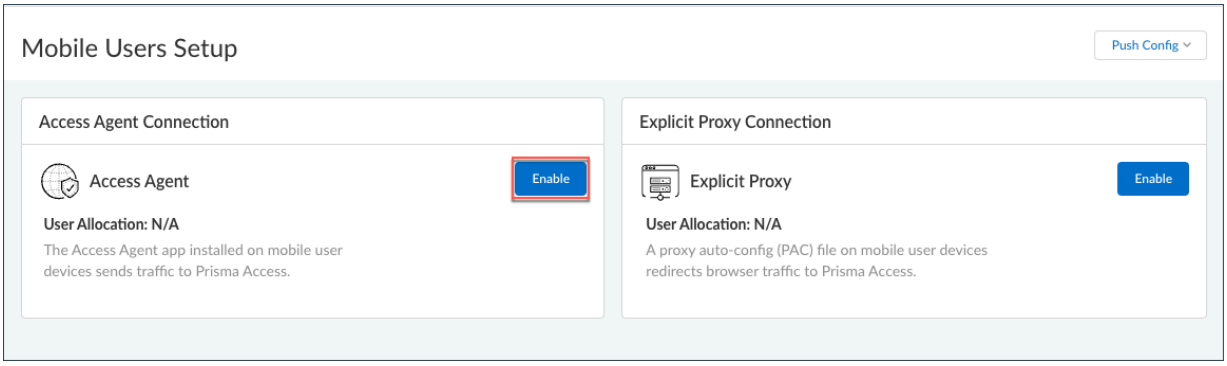
在可以裝載您的使用者之前，您必須使用 Strata Cloud Manager 啟用 **Access Agent**（存取代理程式）作為行動使用者連線類型。在啟用連線類型之後，安裝在行動使用者裝置上的 Prisma Access Agents 將能夠將流量傳送到 Prisma Access。

在開始啟用 Prisma Access Agent 之前，確保您 在雲端識別引擎中授權使用者群組對應進行動態權限存取。

**STEP 1 |** 選取 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Mobile Users**（行動使用者）。

**STEP 2 |** **Enable**（啟用）存取代理程式。

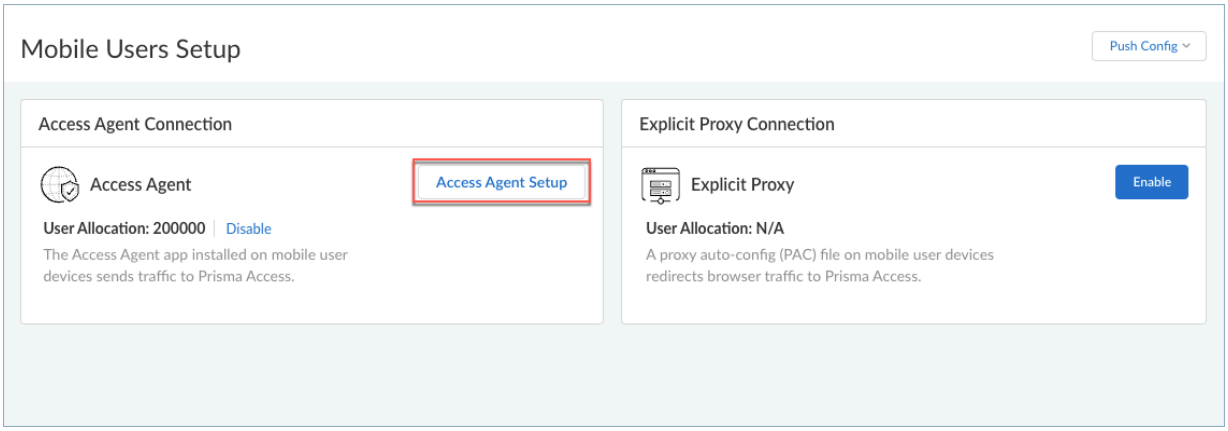
*Prisma Access* 代理程式不支援明確 *Proxy*。



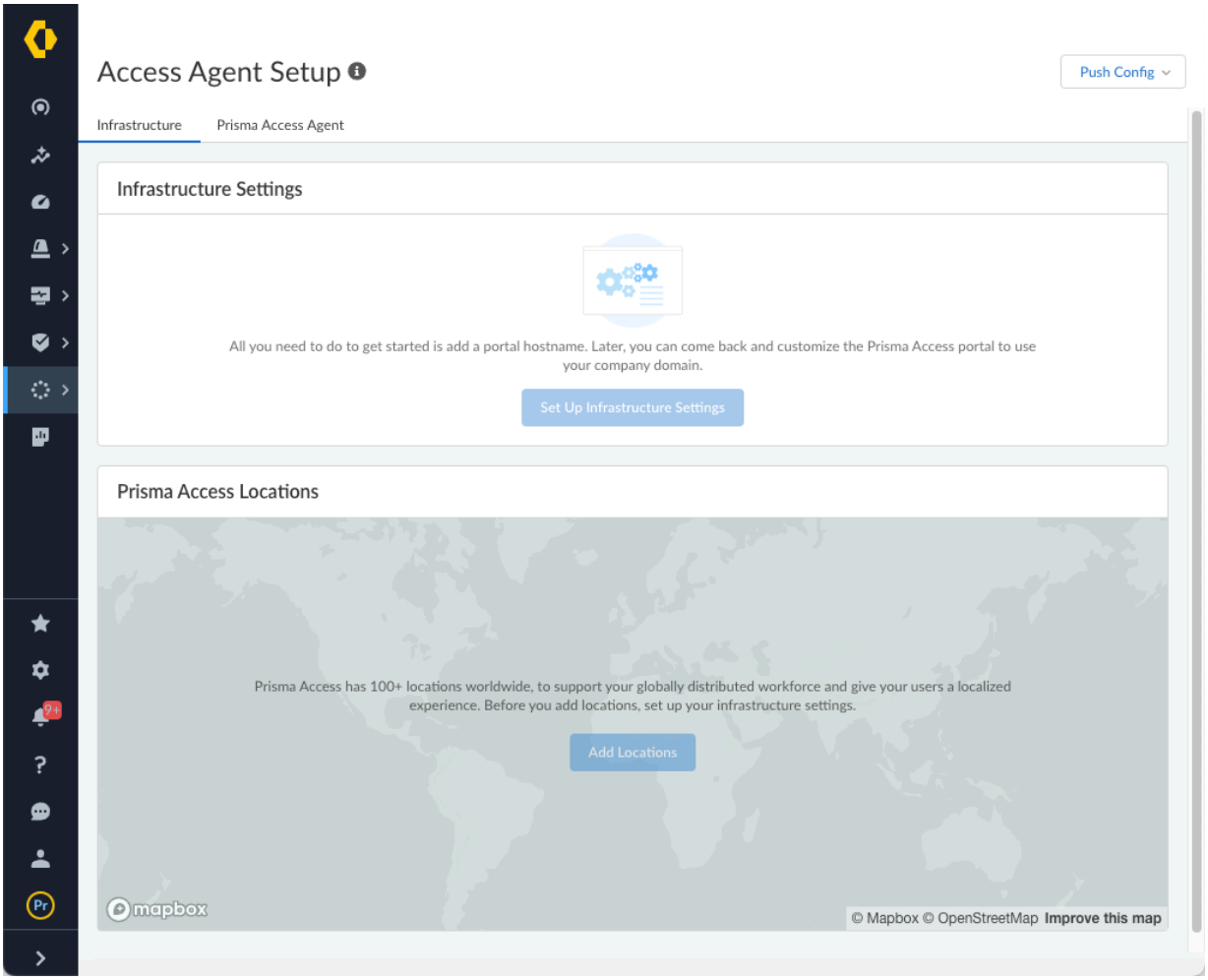


©2025 Palo Alto Networks, Inc.

**STEP 3 |** 按一下 **Access Agent Setup**（存取代理程式設定）以開始裝載行動使用者。




[Access Agent Setup（存取代理程式設定）] 頁面隨即顯示。




 ©2025 Palo Alto Networks, Inc.

# 設定代理程式基礎結構進行動態權限存取

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Prisma Access 授權，具有行動使用者訂閱<br>❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ 角色：超級使用者 |

為 Prisma Access Agent 設定基礎結構設定，以便 Prisma Access 可以佈建您的行動使用者環境。然後，選取您的 Prisma Access Agent 使用者將連線至其中的 Prisma Access 位置。

您也可以選擇性地為動態權限存取啟用 SC-NAT 支援（如果您已建立服務連線，來存取其資料中心或總部位置的私人應用程式），或為動態權限存取啟用路由彙總，以減少傳送到網路的路由數目。

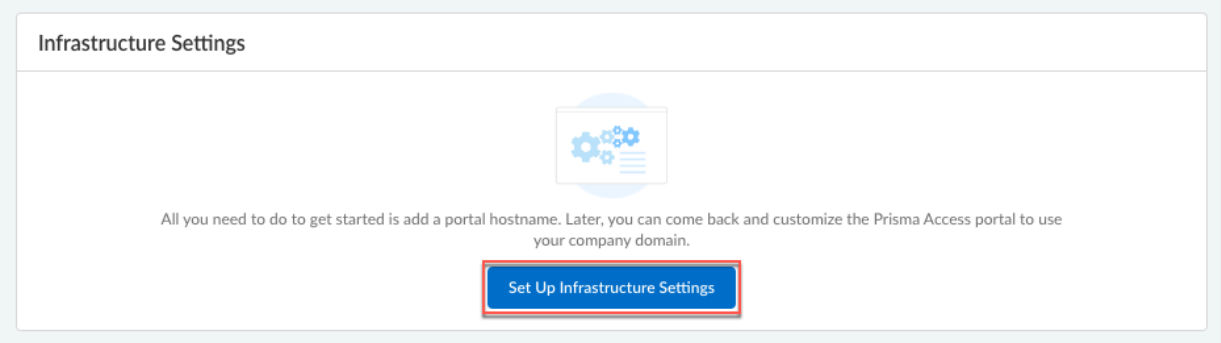
## 設定基礎結構設定

若要僅針對使用者啟用 Prisma Access 進行網際網路存取，Prisma Access 會提供預設 IP 位址集區和雲端預設 DNS 伺服器。不過，如果您想要行動使用者存取總部、資料中心或您已裝載至 Prisma Access 的遠端網站的內部資源，則必須配置用戶端 IP 位址集區。Prisma Access 會使用 IP 位址集區，將 IP 位址指派給您的行動使用者，並設定 Prisma Access 服務基礎結構。

在設定基礎結構設定之前，請確保至少配置一個專案。否則，當您嘗試提交並推送基礎結構提交時，提交將失敗。如需詳細資訊，請參閱建立專案。

**STEP 1 |** 在 Strata Cloud Manager 中，選取 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Access Agent**（存取代理程式） > **Infrastructure**（基礎結構）。

**STEP 2 |** 如果您是第一次設定基礎結構，請按一下 **Set Up Infrastructure Settings**（設定基礎結構設定）。否則，請編輯 **Infrastructure Settings**（基礎結構設定）。

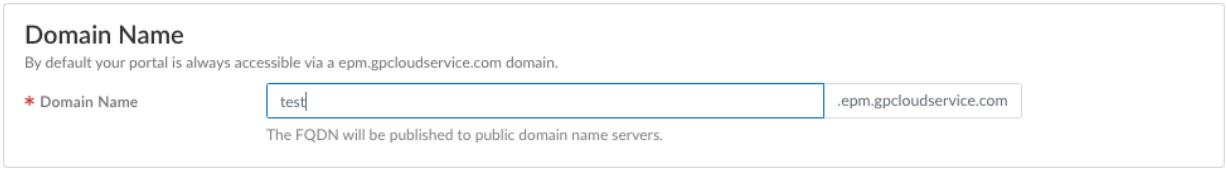




©2025 Palo Alto Networks, Inc.

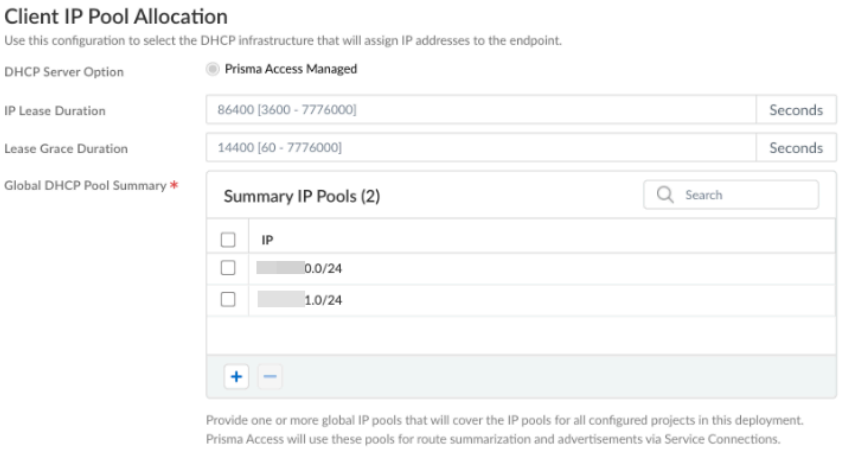
**STEP 3 |** 將主機名稱新增 Prisma Access 代理程式連線之服務的 **Domain Name**（網域名稱）。

依預設，使用者可以使用根據主機名稱的 FQDN 和 **.epm.gpcloudservice.com** 網域來存取服務。




**STEP 4 |** 在 **Client IP Pool Allocation**（用戶端 **IP** 集區配置）中，Prisma Access 提供一部 DHCP 伺服器，其將管理將 IP 位址指派給您端點以進行動態權限存取的操作。

來自 Prisma Access 的專案名稱和位置群組是 DHCP 要求的一部分。每個連線到特定專案的 Prisma Access Agent 都獲指派來自該專案的 IP 子網路的 IP 位址。當使用者變更為不同的專案時，不同的 IP 位址會指派給來自專案 IP 子網路的 Prisma Access Agent。




您可以設定以下選項：

- **IP Lease Duration**（**IP** 租用持續時間）—指定 DHCP 伺服器將網路位址配置給 Prisma Access Agent 的時間量（以秒為單位）。預設 IP 位址租用持續時間為 86,400 秒。
- **Lease Grace Duration**（租用寬限期）—指定 Prisma Access Agent 可以在租用到期後繼續使用其 IP 位址租用的時間量。預設租用寬限期為 14,400 秒。
- **Global DHCP Pool Summary**（全域 **DHCP** 集區摘要）—選取要在其上啟用 SC-NAT 的 IP 集區，或設定並選取全域摘要 IP 集區進行路由彙總。

**STEP 5 |** **Save**（儲存）基礎結構設定。

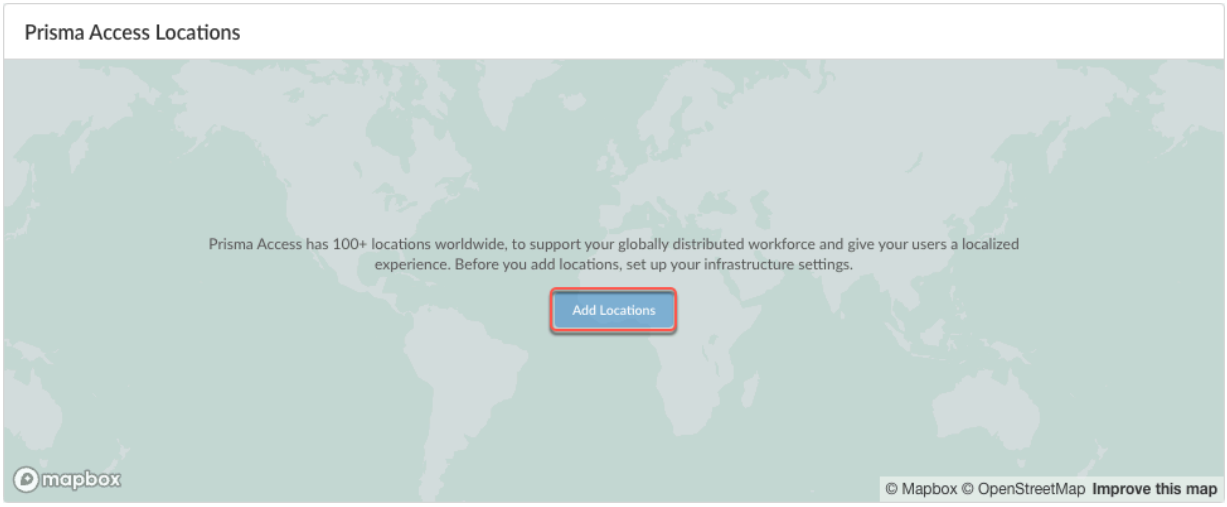
## 選取 Prisma Access 位置

選取您想要支援 Prisma Access Agent 使用者的 Prisma Access 位置。位置群組用於動態權限存取。

**STEP 1 |** 在 Strata Cloud Manager 中，選取 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Access Agent**（存取代理程式） > **Infrastructure**（基礎結構）。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 如果您是第一次設定基礎結構，請按一下 **Add Locations**（新增位置）。否則，請編輯 **Prisma Access Locations**（**Prisma Access** 位置）。




**STEP 3 |** 選取您的行動使用者連線的 Prisma Access 位置。

依據您的授權合約，您可以選取 [Local（本機）] 或 [Worldwide（全世界）] 位置。地圖顯示您可以為使用者部署 Prisma Access 的區域。此外，Prisma Access 在每個區域內提供多個位置，以確保您的使用者可以連線至依據其區域設定提供客製化使用者體驗的位置。為了獲得最佳效能，請 **Select All**（全選）。或者，在每個選定的區域內選取您的使用者需要存取的特定位置。


©2025 Palo Alto Networks, Inc.

將部署限定於單一區域，可以對您部署的區域進行更精細的控制，並排除政策或產業法規要求的區域。

針對 *Prisma Access* 代理程式，您可以將 *Prisma Access* 部署到下列 *Strata* 記錄服務區域：

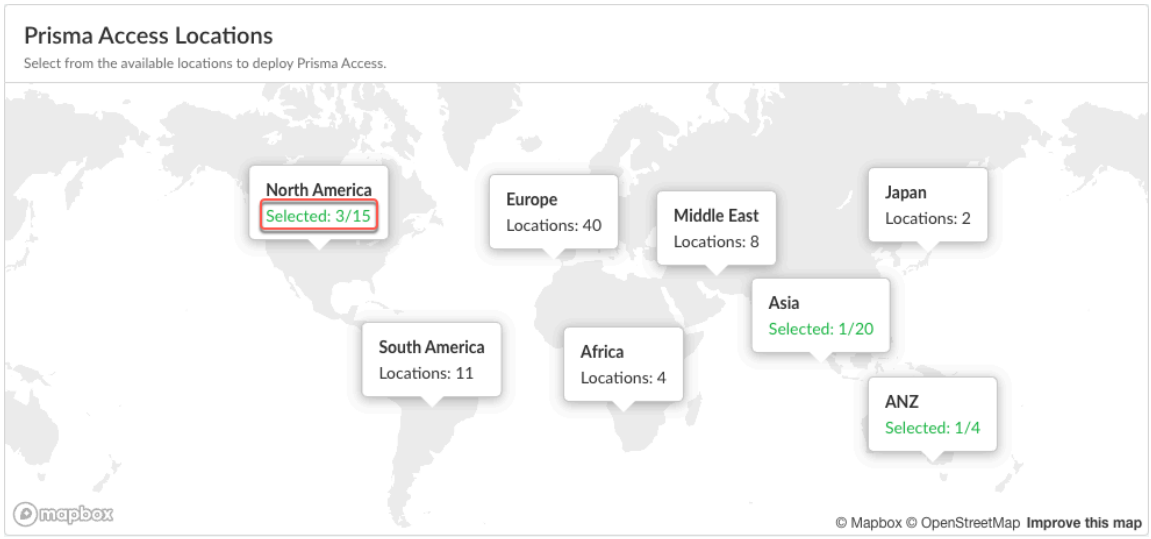
- 美國
- 德國
- 印度

這份清單會隨著更多區域可供使用而更新。

為了獲得最佳使用者體驗，如果您限制了位置數目，請選擇離使用者最近的位置，或位於使用者相同國家/地區的位置。如果您行動使用者所在的國家/地區沒有可用位置，請選擇離使用者最近的位置，以獲得最佳效能。

本節中的影像僅用於說明目的。

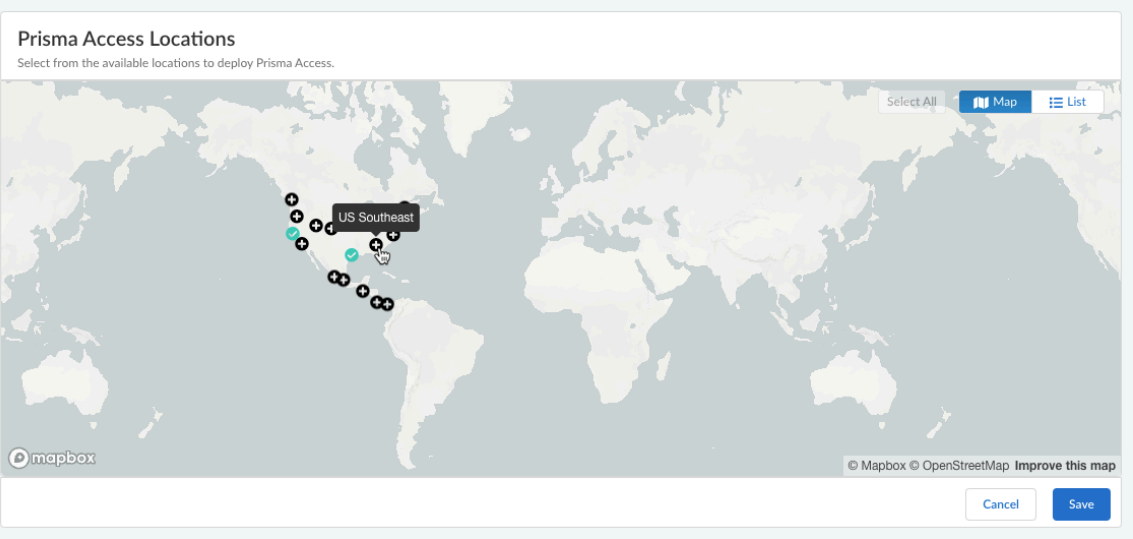
1. 在地圖上選取一個可用區域。



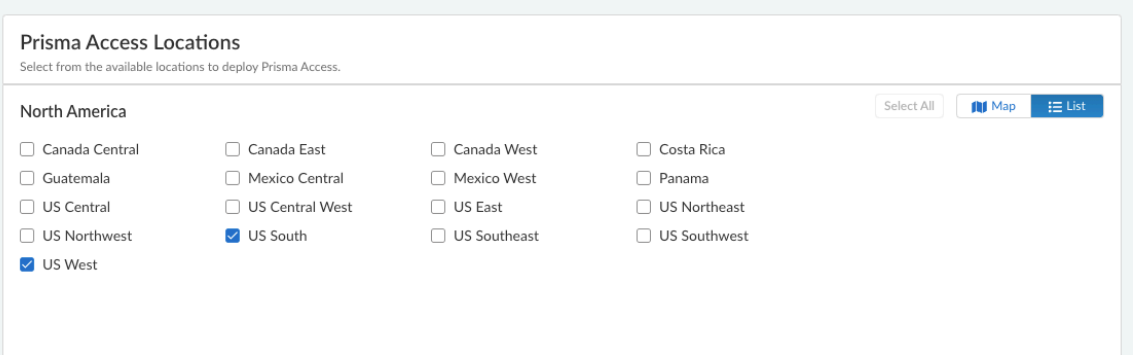

2. 在您想要新增的位置上按一下加號 **+**。

   您可以在 **Map**（地圖）和 **List**（清單）檢視之間切換。您也可以 **Select All**（全選）位置。


©2025 Palo Alto Networks, Inc.




在清單檢視中，您可以從可用位置清單中選取以部署 Prisma Access。您可以選取區域內的 **All**（全部）網站。

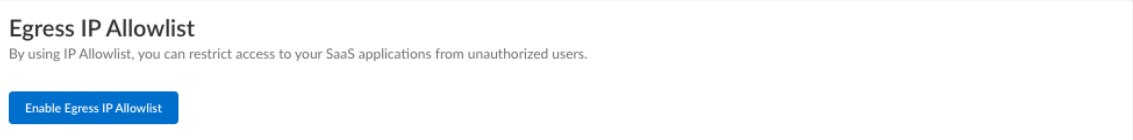



3. **Save**（儲存）您的 Prisma Access 位置設定。

**STEP 4 |** （選用）限制未經授權使用者對您的 SaaS 應用程式的存取。

您可以為現有行動使用者部署和新使用者裝載期間啟用輸出 IP 允許清單。如果您為現有 Prisma Access 部署啟用輸出 IP 允許清單，則 Prisma Access 會將已為您位置配置的所有輸出 IP 位址移轉到輸出 IP 允許清單。對於新的 Prisma Access 部署，在裝載 Prisma Access 代理程式行動使用者時，啟用輸出 IP 允許清單。每當您新增位置或有自動調整事件時，應該擷取 Prisma Access 配置並將其新增至 SaaS 應用程式允許清單中的新輸出 IP 位址。然後，您可以將設定推送至 Prisma Access 部署，以確認為您的位置配置的輸出 IP 允許清單。

1. **Enable Egress IP Allowlist**（啟用輸出 **IP** 允許清單）以顯示所裝載 Prisma Access 位置的 IP 位址。




2. 複製配置的位址並將其新增至 SaaS 應用程式的允許清單。
3. **Migrate**（移轉）以確認為 Prisma Access 中所裝載位置配置的 IP 位址。

 ©2025 Palo Alto Networks, Inc.

4. 為新裝載位置或在自動調整事件期間擷取 IP 位址。
   1. 選取 **Location**（位置）名稱以尋找配置給該位置的新輸出 IP 位址。
   2. 將這些 IP 位址新增到您 Saas 應用程式的允許清單，然後在 Prisma Access 中確認它們。
   3. **Save**（儲存）已配置的輸出 IP 位址。

# 為動態權限存取啟用 SC-NAT 支援

如果您使用 DPA，並已建立服務連線來存取資料中心或總部位置的私人應用程式，則請使用動態權限存取 (DPA) 的 SC-NAT 支援。如果基礎結構子網路的 IP 位址重疊，則 DPA 環境中的多個專案可能會耗盡 IP 位址。為了修正此問題，Prisma Access 可以針對 IP 位址實作來源 NAT (SNAT)，其：

- 讓 Prisma Access 針對使用服務連線來存取私人應用程式的行動使用者對應單一 IP 位址
- 提供 SNAT 以輕鬆進行路由
- 消除 IP 集區重疊
- 消除 Prisma Access 與您資料中心或總部位置之間的 IP 集區 IPv4 耗盡

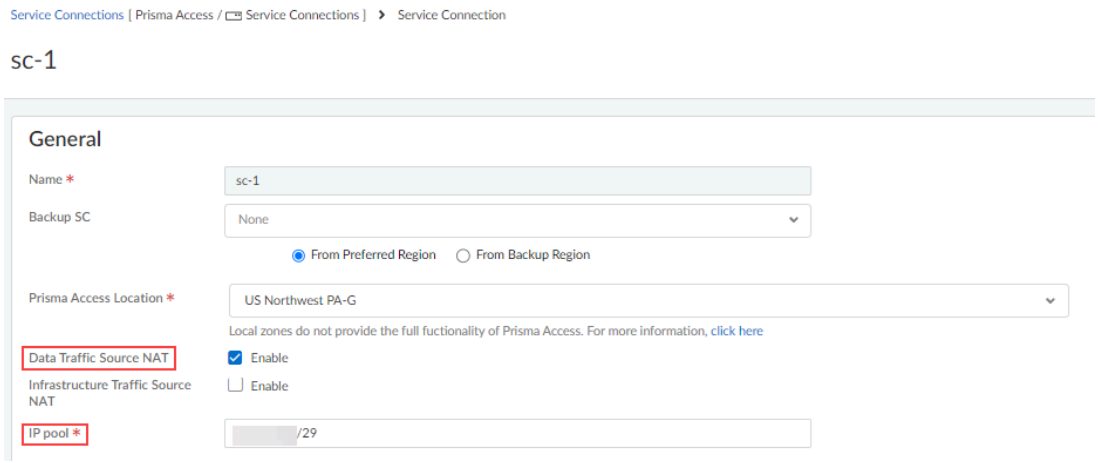
DPA 客戶可以使用服務連線將用戶端位置裝載到 Prisma Access。不過，多個專案可能在多個資料中心具有大型 IP 集區，從而導致私人 IP 集區可能耗盡。為了解決這個問題，Prisma Access 中的動態權限存取為具有已定義集區的 SC-NAT 提供支援。客戶可以選擇使用 SC-NAT 而不是基礎結構子網路，以便劃分 IP 集區。如果您為服務連線企業存取節點 (SC-CAN) 啟用 SC-NAT，則該服務連線將始終支援 SC-NAT。

啟用 DPA 後，您可以根據每個專案開啟 SC-NAT（以使用 SC-NAT）或關閉（以使用基礎結構子網路）。

1. 在 Strata Cloud Manager 中，選取 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Service Connections**（服務連線）。
2. 從 **Service Connections**（服務連線）表格中選取服務連線。
3. 按一下 **Data Traffic Source NAT**（資料流量來源 **NAT**）的核取方塊。
4. 在按一下 **Data Traffic Source NAT**（資料流量來源 **NAT**）核取方塊之後，您會看到必要的 **IP Pool**（**IP** 集區）欄位。輸入要為其啟用 SC-NAT 的子網路。


©2025 Palo Alto Networks, Inc.

5. **Save**（儲存）您的變更。




# 為動態權限存取啟用路由彙總

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.2 Innovation<br>❑ 最低 Prisma Access 資料平面版本：11.2.3<br>❑ Prisma Access 授權，具有行動使用者訂閱<br>❑ 角色：超級使用者 |

對於具有內部部署硬體但其容量受限的企業，例如只能容納幾百個路由的簡單雲路由器，Prisma Access 可以在將路由公告到內部部署網路時彙總行動使用者 (MU) 路由。路由彙總透過保持在資料中心的路由容量範圍內，最大限度地減少了對這些裝置的需求。

若要啟用路由彙總，您可以設定全域摘要集區，其是可跨多個專案使用的大型 IP 集區清單。當使用者使用 Prisma Access 代理程式連線到專案，且該代理程式獲指派全域摘要集區範圍內的 IP 位址時，Prisma Access 服務連線會公通告全域摘要集區，而不是較小的彙總路由。

若要協助說明專案的路由彙總，請考慮以下案例：

- 您設定 10.10.0.0/16 的全域摘要集區，並在服務連線 **SC-A** 上啟用路由彙總選項.
- **User-A** 連線至 **Project-A**，其獲指派 10.10.10.0/24 的 IP 專案集區。連線時，Prisma Access 代理程式會取得 10.10.10.10/32 IP 位址。
- **User-B** 連線至 **Project-B**，其獲指派 10.10.11.0/24 的 IP 專案集區。連線時，Prisma Access 代理程式會取得 10.10.11.10/32 IP 位址。
- 在此情況下，服務連線僅透過 eBGP 將一個子網路（全域摘要集區為 10.10.0.0/16）而不是 /24 彙總路由公告到內部部署網路。



- *Prisma Access* 不會彙總不是專案一部分的 *IP* 集區。
- 專案內的專案 *IP* 集區可以重疊，全域摘要 *IP* 集區也可以重疊。
- 全域摘要集區應該是大型 *IP* 集區，其中包含與多個專案相關聯的專案 *IP* 集區。


©2025 Palo Alto Networks, Inc.

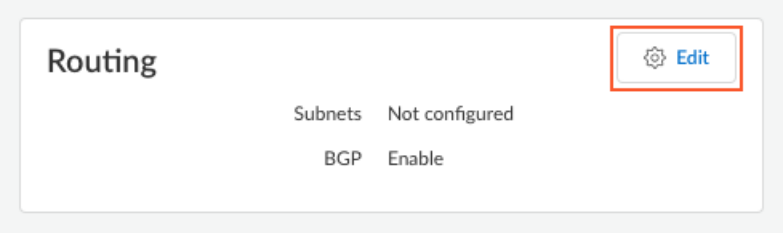
若要在 Strata Cloud Manager 中為專案啟用路由彙總：

**STEP 1 |** 在 **Manage**（管理） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **<Snippet>** > **Objects**（物件） > **Dynamic Privilege Access**（動態權限存取） > **Projects**（專案）的專案設定中，設定專案 IP 集區。

**STEP 2 |** 在 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Access Agent**（存取代理程式） > **Infrastructure Settings**（基礎結構設定）中，設定全域摘要 IP 集區.

**STEP 3 |** 在服務連線中啟用路由彙總。

1. 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Service Connections**（服務連線）。
2. 從 **Service Connections**（服務連線）表格中選取服務連線。
3. **Edit**（編輯）路由設定。




4. 選取 **Summarize Mobile User Routes before advertising**（公告前彙總行動使用者路由）。




**STEP 4 |** **Save**（儲存）路由設定。

**STEP 5 |** **Save**（儲存）服務連線設定。

**STEP 6 |** 對 Prisma Access 執行所有管理員推送設定。


©2025 Palo Alto Networks, Inc.

# 建立片段

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Prisma Access 授權，具有行動使用者訂閱<br>❑ 角色：超級使用者 |

您可以建立一個片段，將 Prisma Access Agents 的設定分組，讓您可以將其快速推送至部署。片段用來標準化一組專案型部署的通用基礎設定，使您能夠使用已知良好的設定快速裝載新裝置，並縮短裝載新裝置所需的時間。

在建立片段之後，您會將該片段與範圍建立關聯、將使用者指派給該範圍，並授與使用者專案管理員角色。然後，使用者能以專案管理員身分登入並使用該片段，來管理 Prisma Access Agent 的專案設定。專案管理員只能變更獲指派片段的 Prisma Access Agent 設定。

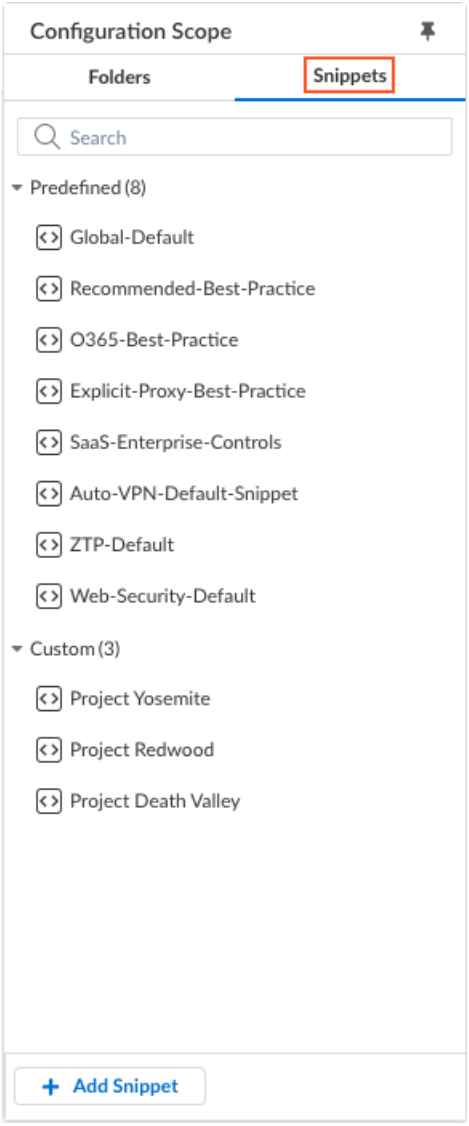
若要建立片段，請完成以下步驟：

**STEP 1 |** 以超級使用者身分登入 Strata Cloud Manager。

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


©2025 Palo Alto Networks, Inc.

**STEP 3 |** 選取 **Overview**（概要），並展開設定範圍以檢視 **Snippets**（片段）。





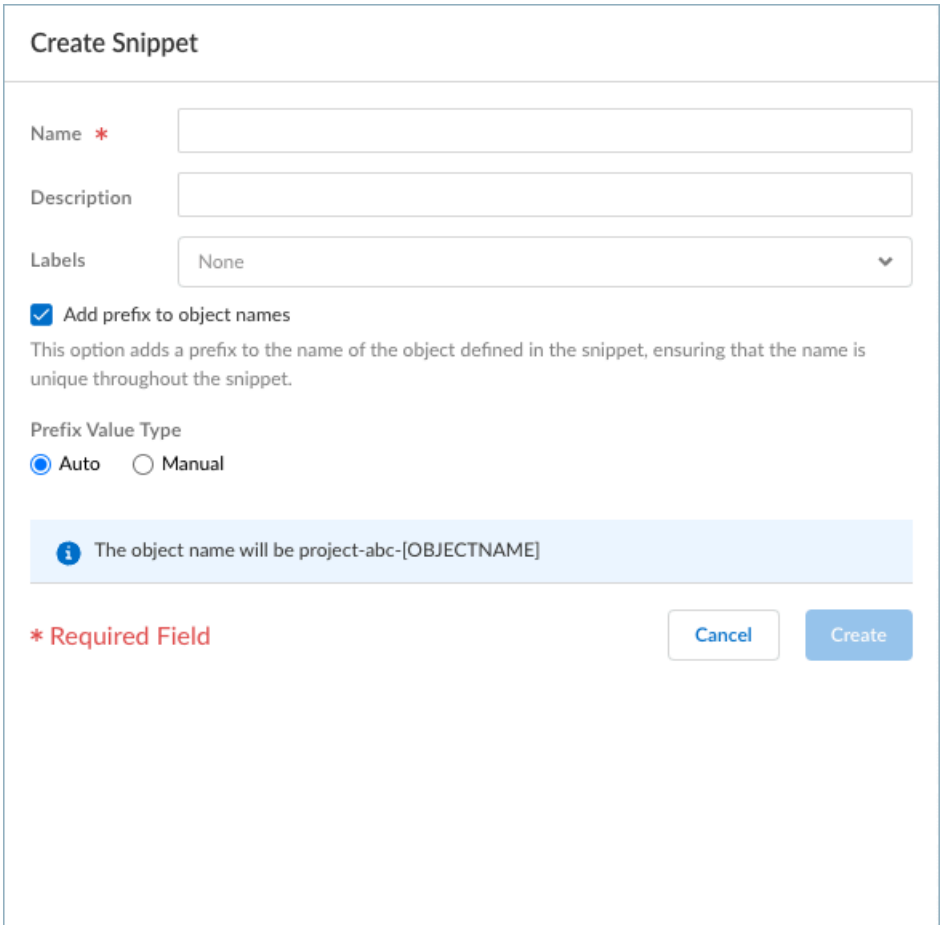
©2025 Palo Alto Networks, Inc.

**STEP 4 |** **Add Snippet**（新增片段）並輸入以下詳細資訊：

1. 輸入片段的 **Name**（名稱）。
2. （選用）輸入片段的說明。
3. （選用）指派一或多個標籤。

   您可以選取現有標籤，或鍵入您要建立的標籤來建立新標籤。
4. 為了確保物件名稱在整個片段中是唯一的，預設會啟用 **Add prefix to object names**（將首碼新增至物件）。

   選擇 **Auto**（自動）產生隨機首碼，還是選取 **Manual**（手動）並新增您自己的 **Prefix Value**（首碼值）。首碼值可以是英數字元，最多六個字元。



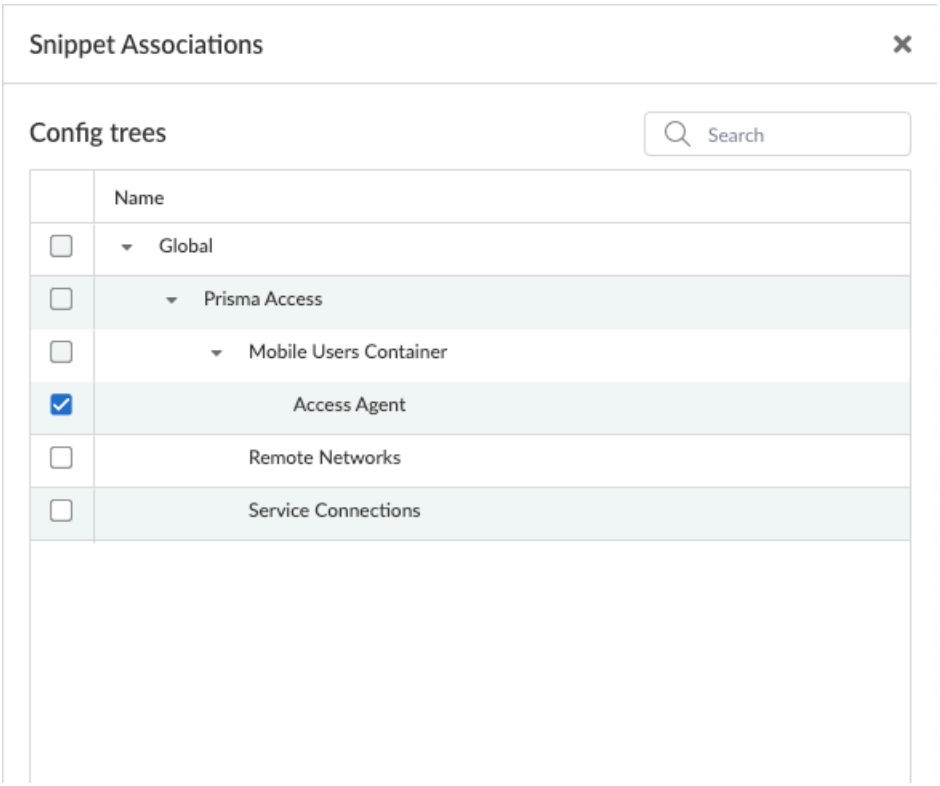

   首碼的格式為 **xxxxxx-**。當您新增物件時，Strata Cloud Manager 會將首碼預先填入物件名稱中。
5. **Create**（建立）片段。

   在建立片段之後，您位於該片段的設定範圍內。您在片段範圍內建立的所有設定，都僅適用於片段。


©2025 Palo Alto Networks, Inc.

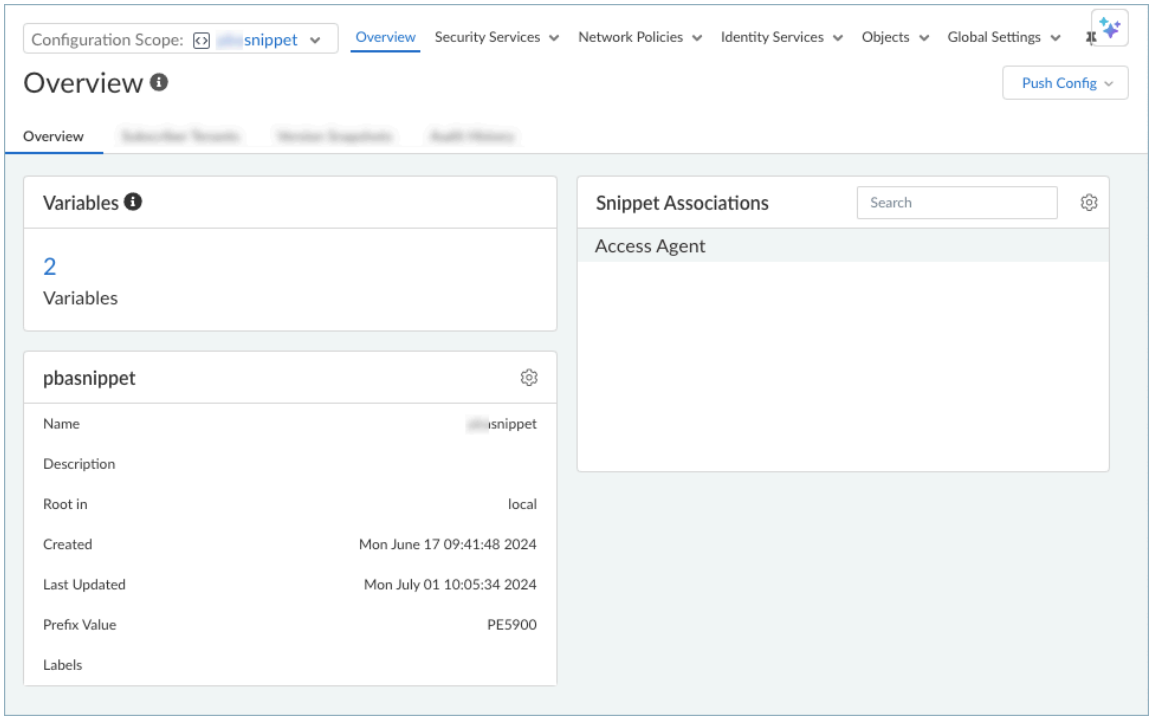
**STEP 5 |** 將片段與 **Access Agent**（存取代理程式）資料夾建立關聯。

1. 在片段的 [Overview（概要）] 頁面中，選取 **Snippet Associations**（片段關聯）設定。
2. 從 **Config trees**（設定樹狀結構）中選取 **Access Agent**（存取代理程式）。




3. 按一下 **X** 關閉 [Snippet Associations（片段關聯）] 視窗。

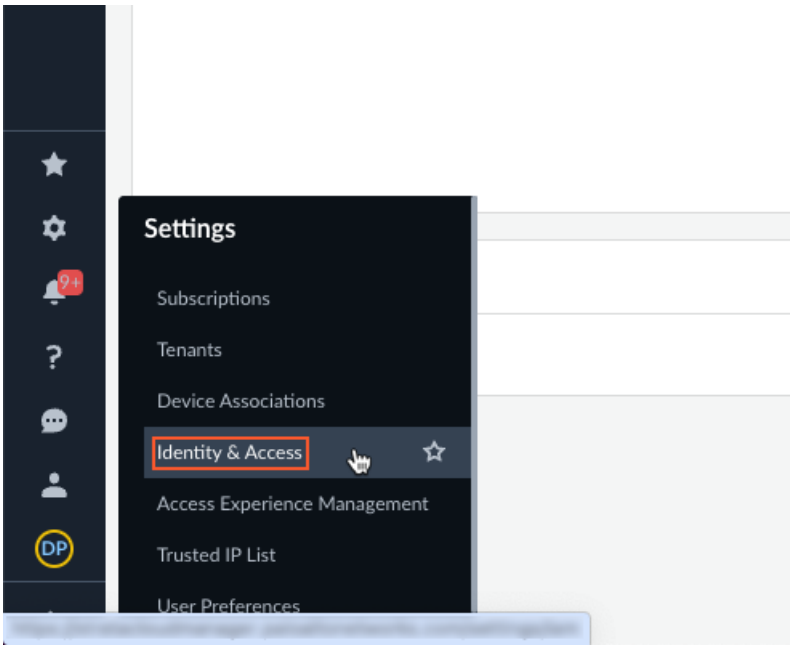
   **Access Agent**（存取代理程式）會出現在片段關聯清單中。



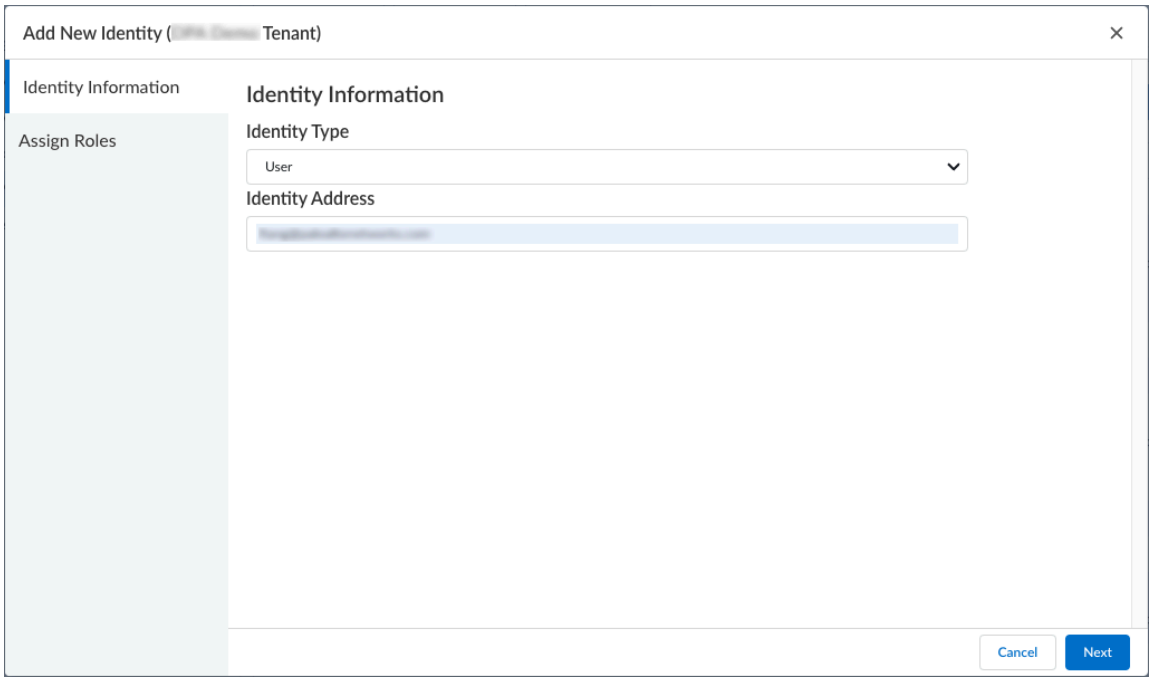

 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** 如果您尚未這樣做，請為將管理專案的使用者建立一個識別，並將專案管理員推送角色指派給該使用者。

1. 從 Strata Cloud Manager 中，選取 **Settings**（設定） > **Identity & Access**（識別與存取）。

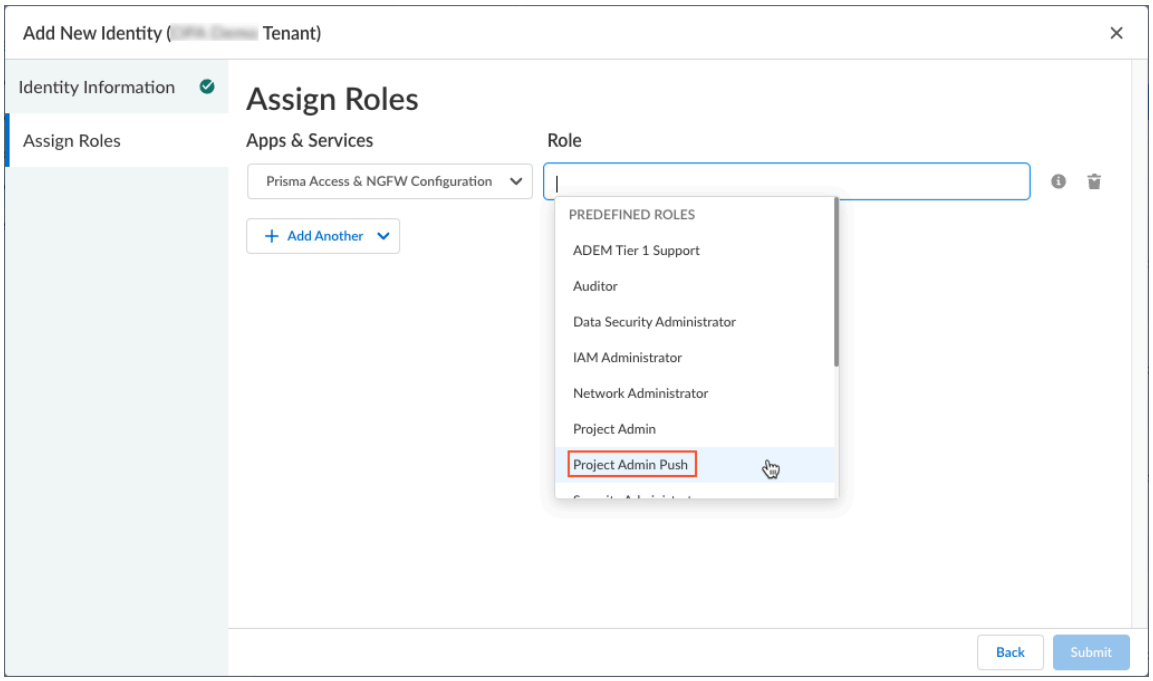



2. 選取 **Add Identity**（新增識別）。
3. 為將成為專案管理員的使用者輸入 **Identity Address**（識別位址），然後按一下 **Next**（下一步）。




4. 選取 **Add Access**（新增存取） > **Prisma Access & NGFW Configuration**（**Prisma Access 和 NGFW** 設定），然後為使用者選取 **Project Admin Push**（專案管理員推送）角色。


©2025 Palo Alto Networks, Inc.



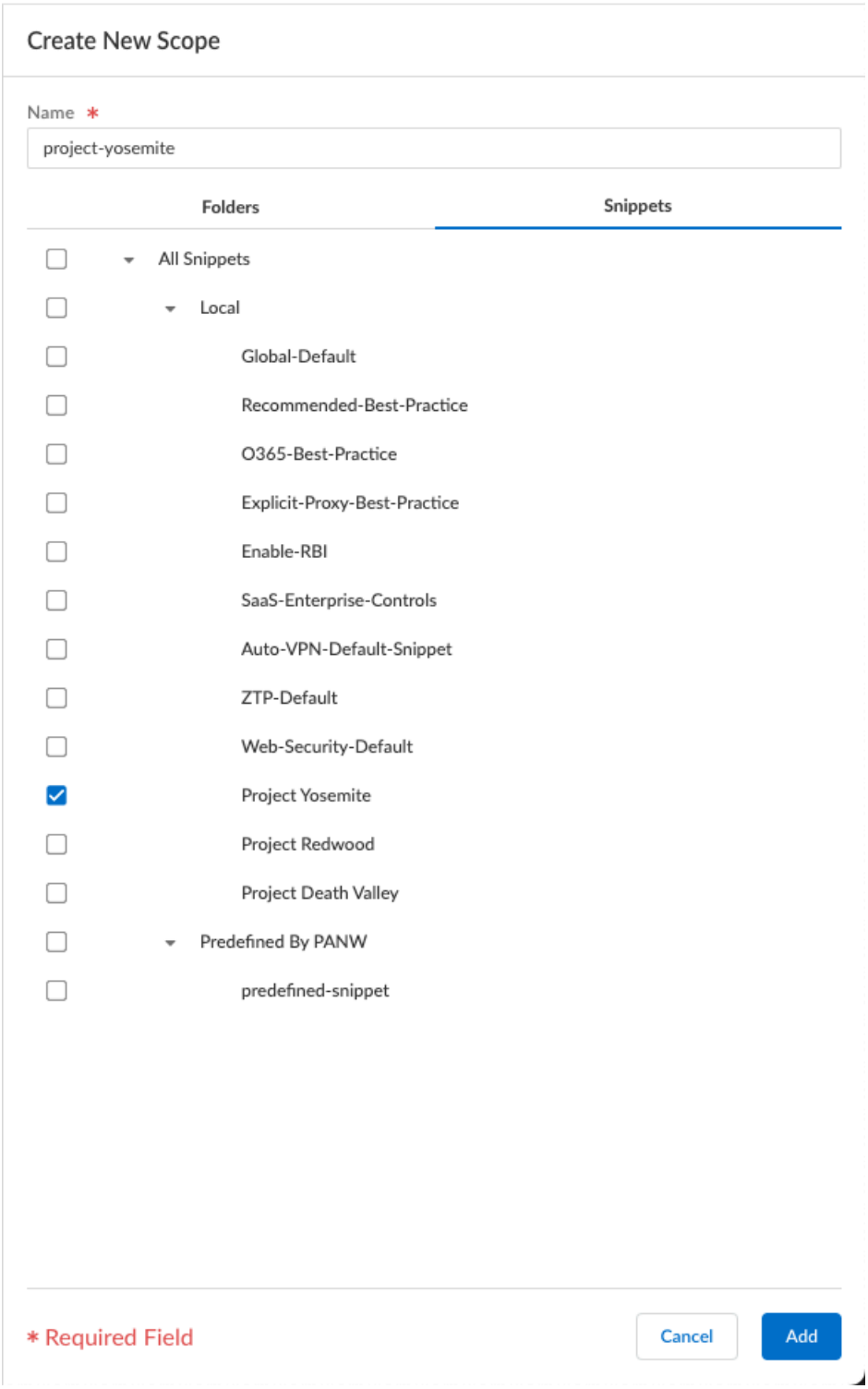

5. 按一下 **Submit**（提交）。

 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** 建立片段的管理範圍並將使用者指派給該範圍。

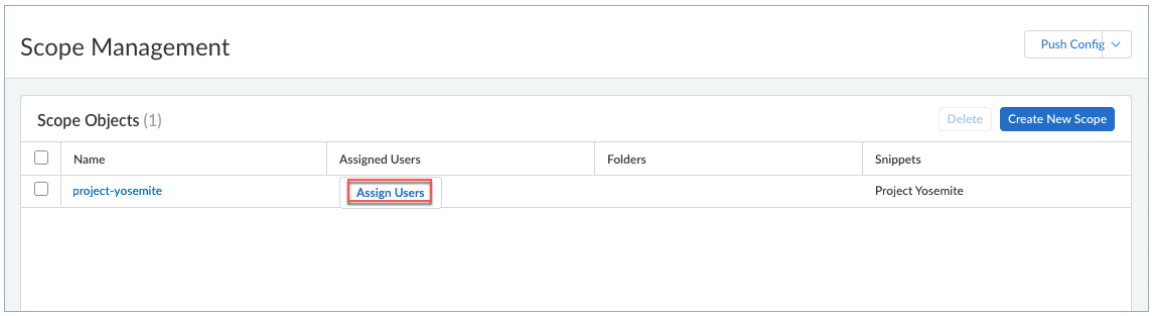
1. 選取 **Manage**（管理） > **Access Control**（存取控制） > **Scope Management**（範圍管理）。
2. 建立新範圍。
3. 輸入範圍的 **Name**（名稱）， 並檢視 **Snippets**（片段）。
4. 將片段與範圍建立關聯。選取您建立的片段並**Add**（新增）它。

 ©2025 Palo Alto Networks, Inc.

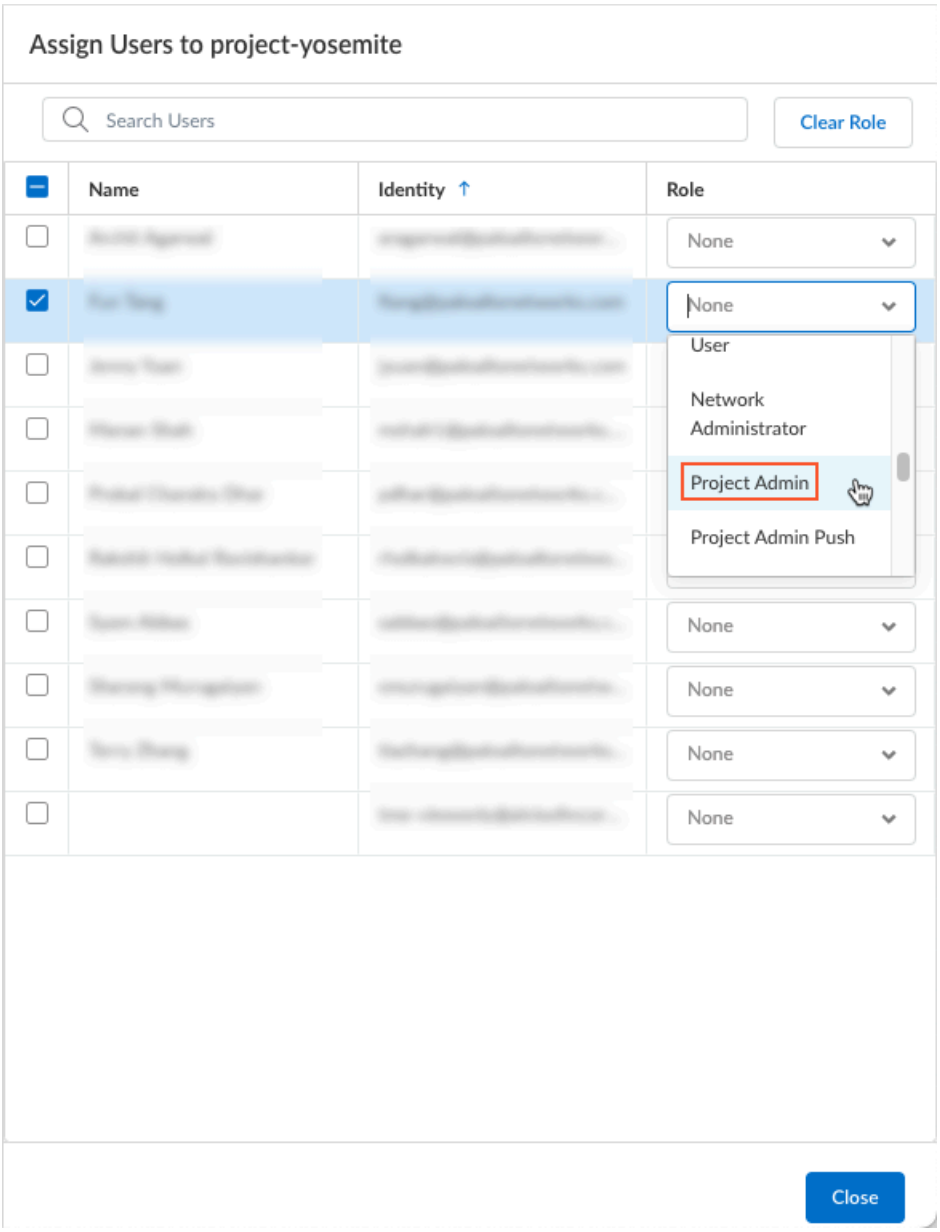



5. 在範圍物件中，**Assign Users**（將使用者指派）給您為片段建立的範圍。


©2025 Palo Alto Networks, Inc.




6. 從清單中選取使用者並授與該使用者 **Project Admin**（專案管理員）角色，將該使用者指派給範圍。




7. **Close**（關閉）視窗。
8. 推送設定。


©2025 Palo Alto Networks, Inc.

1. 選取**Manage**（管理） > **Operations**（操作） > **Push Config**（推送設定）。
2. 選取 **All Admins**（所有管理員）管理員範圍，並選取 **Push Config**（推送設定） > **Push**（推送）。

在推送設定操作完成之後，即會建立片段並將角色與片段建立關聯。

指派的使用者（專案管理員）現在可以登入 Strata Cloud Manager，並使用您建立的片段設定專案特定的 Prisma Access Agent 設定。使用者可以檢視未指派給他們的其他範圍，但無法與其互動，例如變更任何設定。


©2025 Palo Alto Networks, Inc.

# 設定專案特定的 Prisma Access Agent 設定

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Prisma Access 授權，具有行動使用者訂閱<br>❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ 角色：專案管理員 |

在超級使用者管理員設定基礎結構、建立片段，並將此片段指派給您之後，您就能以專案管理員身分登入，來設定專案特定的 Prisma Access Agents 設定，例如私人 IP、分割通道和 DNS 資訊，這些資訊將在端點使用 Prisma Access Agent 登入專案時指派給它們。

您可以為一個或多個 Prisma Access Agents 建立專案特定的設定，或使用預設的代理程式設定。您可以為每個您管理的專案使用不同的代理程式，或與多個專案共享一個代理程式。

# 設定轉送設定檔，為動態權限存取代理程式管理代理程式流量

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Prisma Access 授權，具有行動使用者訂閱<br>❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ 角色：專案管理員 |

轉送設定檔提供單一管理面板，可設定和管理流量轉送規則和流量強制執行，例如設定分割通道設定和管理通道連線外部的流量。轉送設定檔改進了其他行動存取代理程式所經歷的流量政策脫節設定，並大幅擴展了您可以設定的規則和項目數量的限制。透過簡化相關設定並提高清晰度，您可以專注於如何路由和強制執行端點流量。

轉送設定檔是包含多個邏輯和已排序區段的設定檔類型。這些區段說明在代理程式確定如何導向連線之前，連線所經歷的各個階段。此組織結構可以透過在每個區段中顯示已排序項目，協助您瞭解流量以某種方式路由的原因。在每個區段中，您可以新增、編輯、移除或重新排序項目。

設定轉送設定檔後，您可以在 [Agent Settings（代理程式設定）] 頁面中將它們指派給使用者或使用者群組。

流量轉送規則在轉送設定檔中從上到下套用。因此，應採用從上到下的方式來設定轉送設定檔，例如先設定最具體的規則，最後設定最不具體的規則。

轉送規則


©2025 Palo Alto Networks, Inc.

轉送設定檔由一組流量轉送規則組成，這些規則指定哪些來源應用程式或目的地網域和目的地 IP 位址流量通過通道或排除在通道外、是否分割 DNS 流量，以及哪些流量強制執行生效。符合規則的流量將根據流量轉送規範轉送到 Prisma Access。轉送規則中的規範分為以下區段：

- **Source Applications**（來源應用程式）—指定要套用規則的私人或 SaaS 應用程式。當來自端點的流量與來源應用程式相符時，根據轉送規則進行路由流量。
- **Destinations**（目的地）—指定規則套用至其中的網域和 IP 位址。當流量與目的地（指定為 FQDN 或 IP 位址）相符時，根據轉送規則路由流量。

流量強制執行

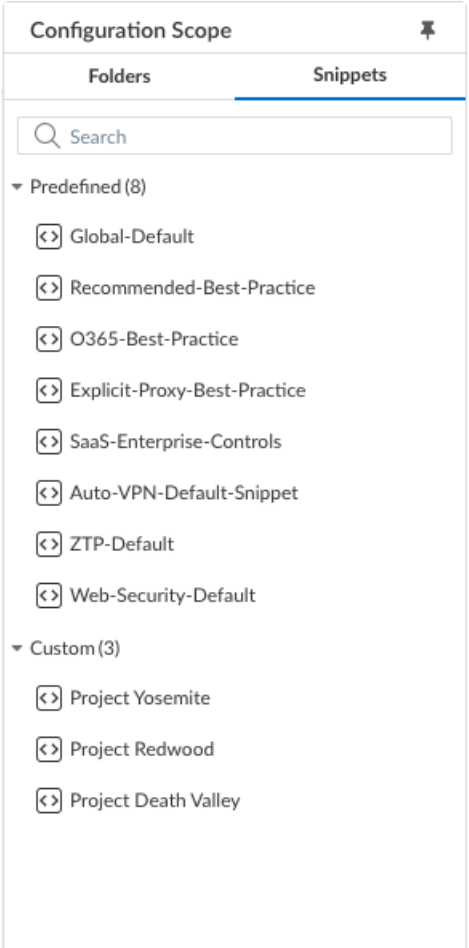
每個轉送設定檔也包含流量強制執行設定，讓您可以：

- 封鎖所有不符合任何轉送規則的輸出流量
- 當代理程式連線到通道時封鎖輸出 LAN 存取
- 當代理程式連線到通道時封鎖輸入存取

若要設定轉送設定檔，請完成以下步驟：

**STEP 1 |** 以專案管理員身份登入 Strata Cloud Manager。

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

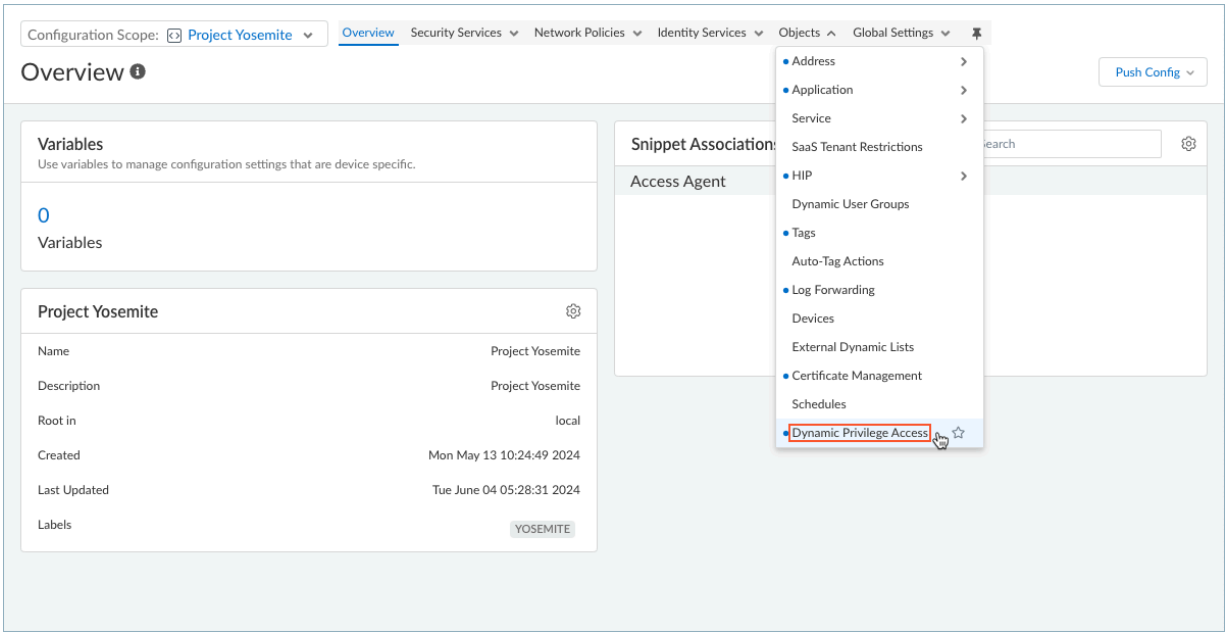



 ©2025 Palo Alto Networks, Inc.

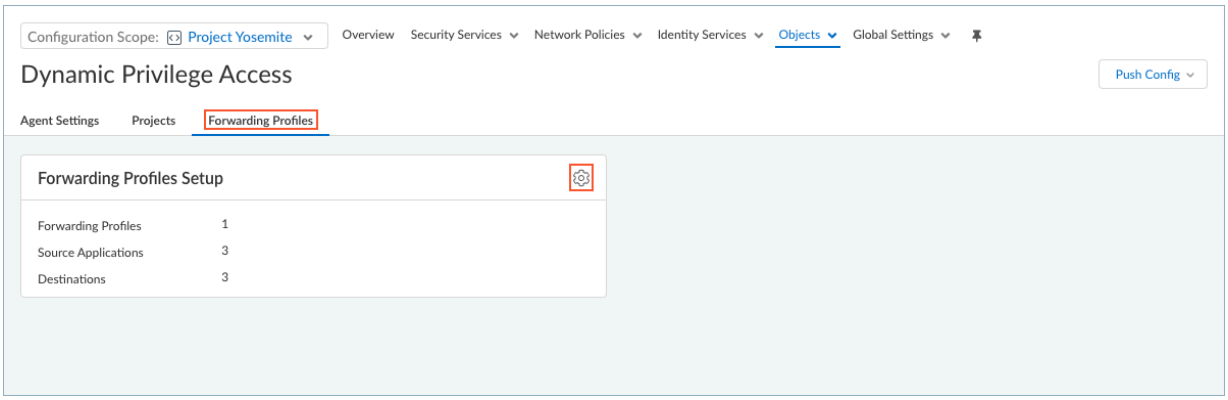
**STEP 3 |** 選取超級使用者管理員指定給您的片段。

您也可以檢視未指派給您的片段，但無法與它們互動，例如變更設定。

**STEP 4 |** 選取 **Objects**（物件） > **Dynamic Privilege Access**（動態權限存取），以開啟動態權限存取設定。



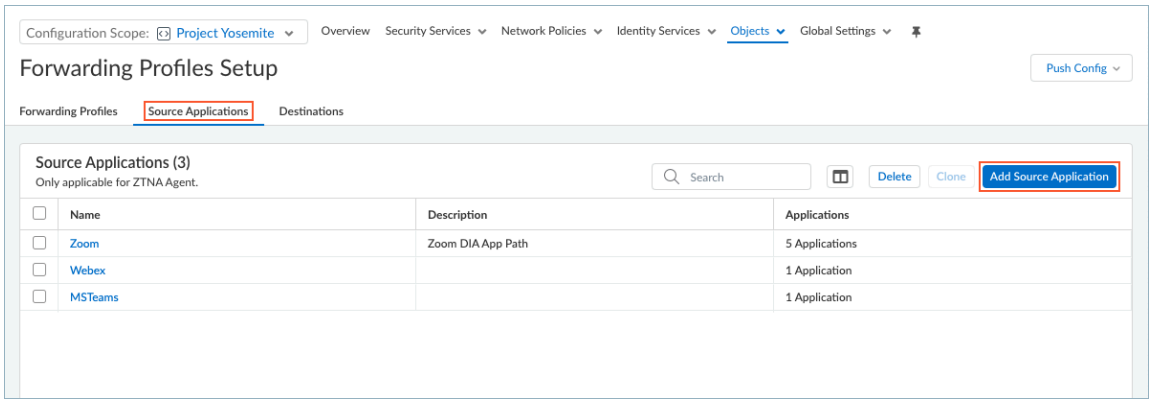

**STEP 5 |** 選取 **Forwarding Profiles**（轉送設定檔）並編輯 **Forwarding Profiles Setup**（轉送設定檔設定）。




 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** 如果您想要根據 SaaS 或公共雲端應用程式名稱建立分割通道，請設定 **Source Applications**（來源應用程式）。

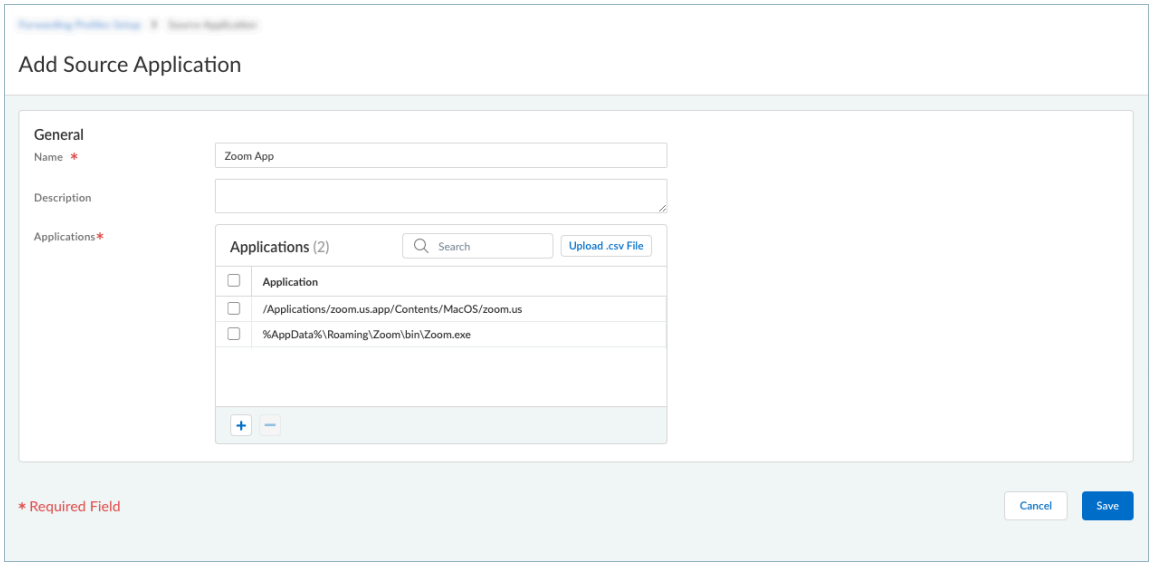
1. 在 [Forwarding Profiles Setup（轉送設定檔設定）] 頁面中，選取 **Source Applications**（來源應用程式） > **Add Source Application**（新增來源應用程式）。




2. 為您想要新增的應用程式輸入有意義的 **Name**（名稱）。
3. 按一下 **Applications**（應用程式）表格中的 **+**，然後輸入應用程式的完整路徑。您可以新增一或多個應用程式，管理要在通道中排除還是包含應用程式流量。

   如果您選擇排除應用程式流量（透過在轉送規則中選取 **Direct**（直接）連線），則來自這些應用程式的流量將透過端點上的實體轉接器傳送，而不是通道（虛擬轉接器）。

   如果您選擇包含應用程式流量（透過在轉送規則中選取 **Tunnel**（通道）連線），這些應用程式的流量將會路由到 Prisma Access，即使符合排除流量準則也一樣。




   例如，若要管理來自 Zoom 應用程式的流量，請新增以下完整路徑：

   - Windows 端點：**`%AppData%\Roaming\Zoom\bin\Zoom.exe`**
   - macOS 端點：**`/Applications/zoom.us.app/Contents/MacOS/zoom.us`**

   如果您有逗號分隔值格式 (`.csv`) 文字檔案的應用程式清單，您可以 **Upload .csv File**（上傳 **.csv** 檔案）。
4. **Save**（儲存）來源應用程式。

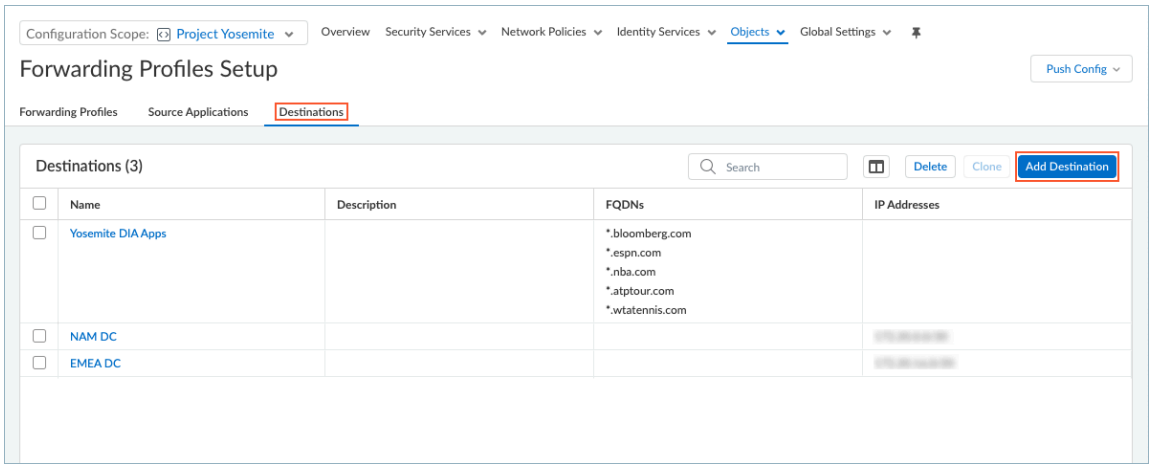
 ©2025 Palo Alto Networks, Inc.

5. 重複這些步驟以新增更多來源應用程式。


©2025 Palo Alto Networks, Inc.

**STEP 7 |** 如果想要根據目的地網域或存取路由建立分割通道，請設定 **Destinations**（目的地）。

1. 在 [Forwarding Profiles Setup（轉送設定檔設定）] 頁面中，選取 **Destinations**（目的地） > **Add Destination**（新增目的地）。

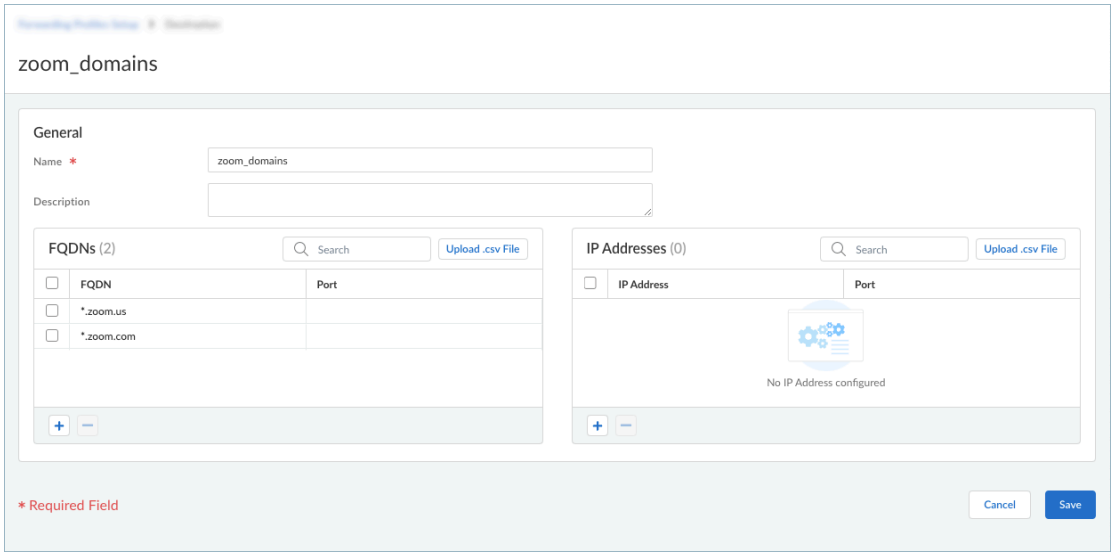



2. 為您想要新增的目的地輸入有意義的 **Name**（名稱）。
3. 透過指定網域名稱、存取路由或兩者來新增目的地。

   - 若要新增目的地網域，請按一下 **FQDN** 表格中的 **+**，然後輸入目的地網域的 FQDN。您可以選擇性地新增連接埠。如果不指定連接埠，則指定網域的所有連接埠均受轉送規則約束。您可以新增一或多個網域來進行流量管理。

     如果您選擇根據網域名稱排除流量（透過在轉送規則中選取 **Direct**（直接）連線），則來自該網域的流量將透過端點上的實體轉接器傳送，而不是通道（虛擬轉接器）。

     如果您選擇根據網域名稱包含流量（透過在轉送規則中選取 **Tunnel**（通道）連線），則來自該網域的流量將會路由到 Prisma Access，即使符合排除流量準則也一樣。




   - 若要新增存取路由，請按一下 **IP Addresses**（IP 位址）表格中的 **+**，然後輸入目的地子網路。您可以新增一或多個存取路由以進行流量管理。

 ©2025 Palo Alto Networks, Inc.

請勿在 *IP* 位址中包含萬用字元。轉送設定檔不支援 *IP* 位址中的萬用字元。

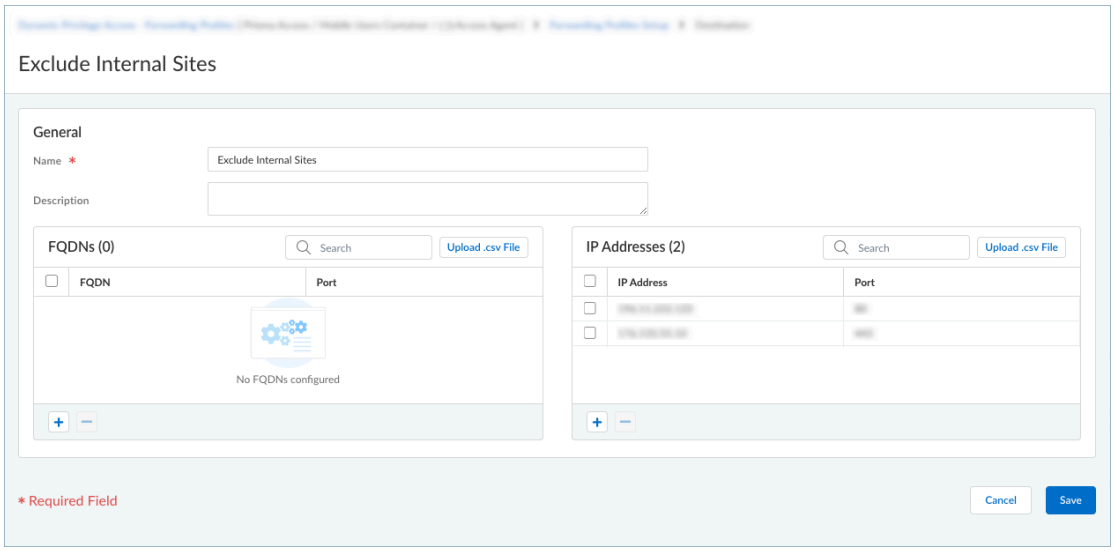
如果未包含或排除路由或應用程式，則每個要求都會路由通過通道（未分割通道）。此外，每當使用者連線到 Prisma Access 時，所有流量都會經過檢查並受到政策強制執行的約束。

當您定義分割通道流量以排除存取路由時（透過在轉送規則中選取 **Direct**（直接）連線），這些路由將透過端點上的實體轉接器傳送，而不是透過虛擬轉接器（通道）透過通道傳送。透過依據存取路由排除分割通道流量，您可以將延遲敏感或高頻寬流量傳送至通道外，而所有其他流量則透過通道路由，以便 Prisma Access 閘道進行檢查和政策強制執行。

當您定義分割通道流量以包含存取路由時（透過在轉送規則中選取 **Tunnel**（通道）連線），Prisma Access 閘道會將這些路由推送到遠端使用者的端點，以指定這些端點可以透過通道傳送哪些流量。

指定比包含路由更明確的排除路由，否則可能會排除掉超出原有預期的流量。

如果您有 `.csv` 格式文字檔案的 IP 位址清單，可以 **Upload .csv File**（上傳 **.csv** 檔案）。

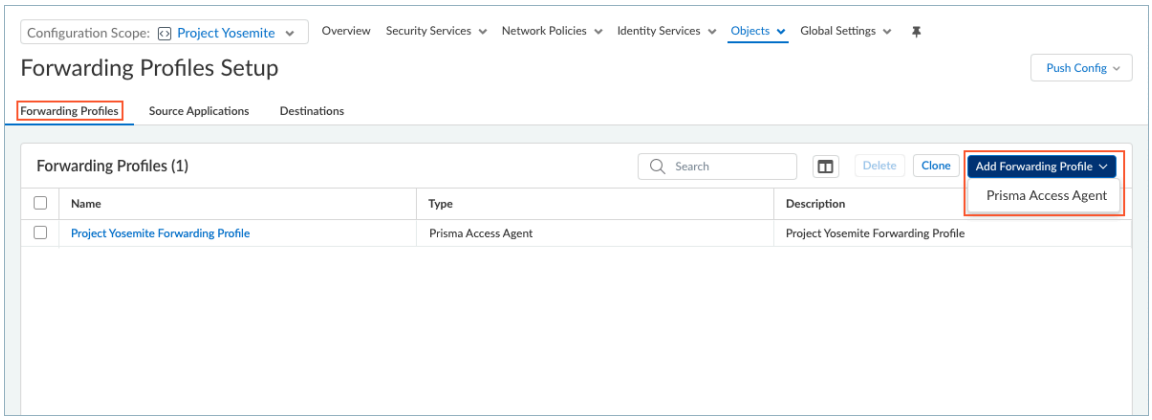



4. **Save**（儲存）目的地。
5. 重複這些步驟以新增更多目的地。


©2025 Palo Alto Networks, Inc.

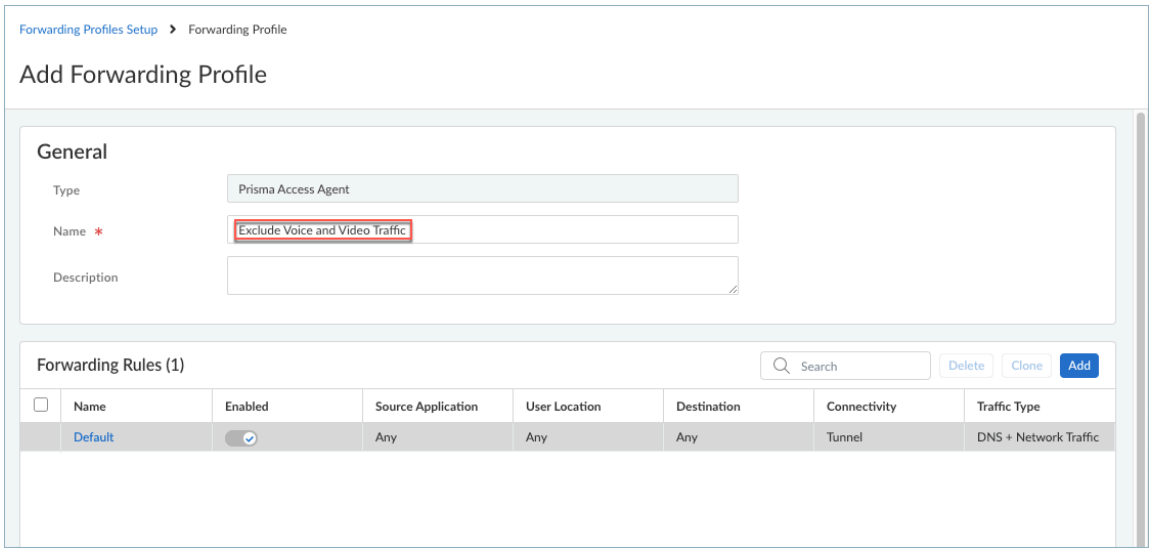
**STEP 8 |** 建立轉送設定檔，根據您設定的來源應用程式或目的地來允許或排除流量。

1. 若要新增轉送設定檔，請選取 **Forwarding Profiles**（轉送設定檔） > **Add Forwarding Profile**（新增轉送設定檔） > **Prisma Access Agent**。




若要編輯轉送設定檔，請在轉送設定檔表格中選取設定檔的名稱。

2. 為轉送設定檔輸入有意義的 **Name**（名稱）。
3. **Add**（新增）轉送規則。

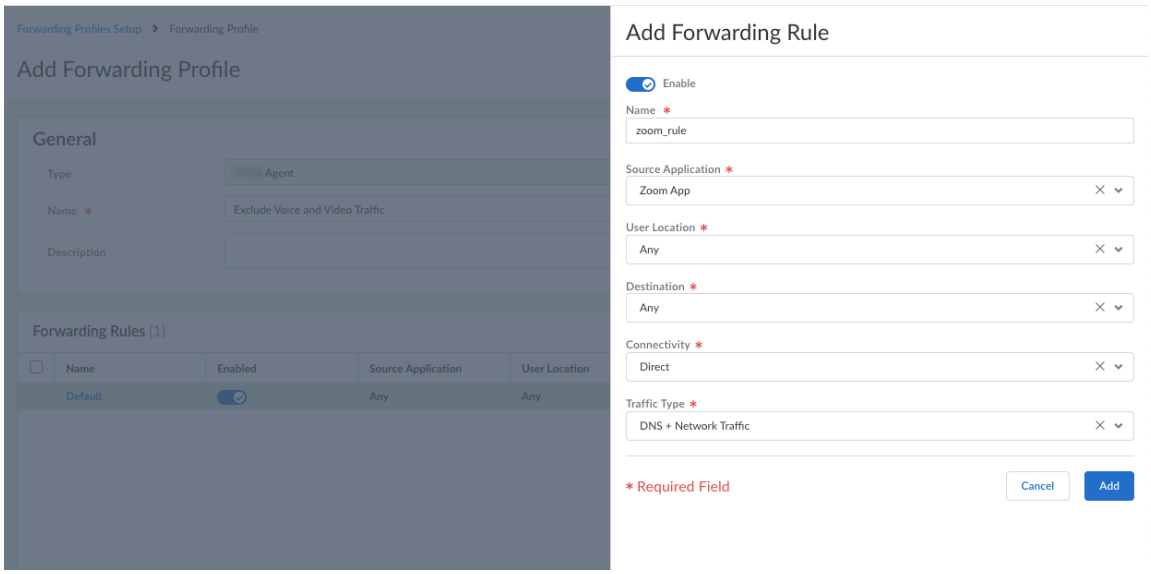



「轉送規則」表格顯示構成轉送設定檔的規則。所有轉送設定檔都包含 **Default**（預設）轉送規則，透過通道傳送所有 DNS 和網路流量。您新增的任何新規則都會放置在預

 ©2025 Palo Alto Networks, Inc.

設規則之上。您無法刪除或移動預設轉送規則，但可以變更其 **Connectivity**（連線）設定。

4. 輸入轉送規則的規格。




1. **Enable**（啟用）規則
2. 輸入規則的 **Name**（名稱）。
3. 選取您先前定義的 **Source Application**（來源應用程式）。如果您選取 **Any**（任何），則轉送規則將套用至來自任何來源應用程式的流量。

   僅當連線由指定來源應用程式建立時，該規則才會相符。
4. 選取 **User Location**（使用者位置）。如果您未設定使用者位置或允許規則比對任何使用者位置，請選取 **Any**（任何）。（不適用於已啟用動態權限存取的代理程式。）

   僅當端點連線到您指定的使用者位置時，該規則才會相符。
5. 選取您先前定義的 **Destination**（目的地）。如果您選取 **Any**（任何），則轉送規則將套用至來自任何目的地網域或 IP 位址的流量。

   只有當連線目的地與指定目的地網域或 IP 位址相符時，該規則才會相符。
6. 選取 **Connectivity**（連線）：
   - **Direct**（直接）—將流量傳送到通道外。已選取應用程式或目的地的所有流量都會直接傳送到端點上的實體轉接器，不經過檢查。
   - **Tunnel**（通道）—透過通道傳送流量。所有流向已選取應用程式或目的地的流量都會透過通道傳送至 Prisma Access，進行檢查和政策強制執行。
7. 選取 **Traffic Type**（流量類型）：

   指定是否使用分割 DNS 以允許使用者透過通道或除了網路流量外在通道外部，導向其應用程式和資源的 DNS 查詢。
   - **DNS + Network Traffic**（**DNS +** 網路流量）—確保按您指定為包含和排除的目的地網域劃分的分割通道，套用至 DNS 流量和該網域的相關網路應用程式流量。

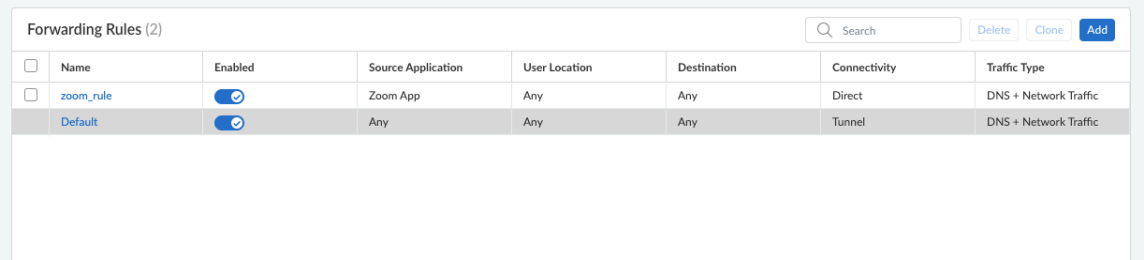

©2025 Palo Alto Networks, Inc.

- **Network Traffic**（網路流量）—包含或排除僅適用於網路應用程式流量但不適用於 DNS 流量的規則。無論按您指定為包含或排除的目的地網域劃分的分割通道如何，所有 DNS 流量都通過通道。

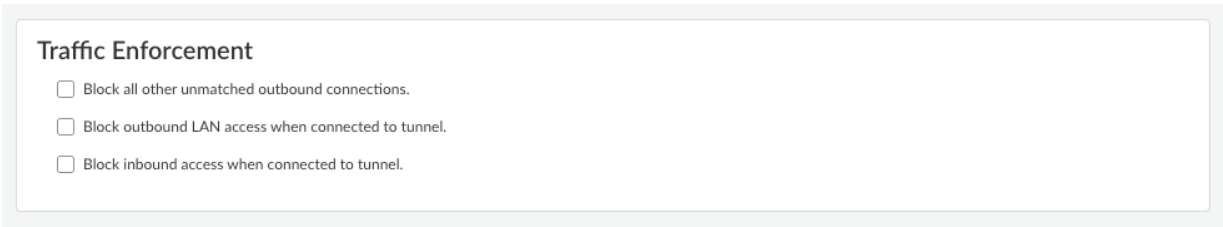
針對 *Windows* 代理程式，***DNS + Network Traffic***（***DNS +*** 網路流量）分割通道選項不支援應用程式型分割通道規則。如果您將分割通道設定為根據應用程式名稱包含或排除通道中的流量，並選取 ***DNS + Network Traffic***（***DNS +*** 網路流量），則排除和包含應用程式的 *DNS* 查詢封包將不遵守分割通道規則。

5. **Add**（新增）轉送規則。

   此規則將會新增至「轉送規則」表格中。您可以將多個規則新增至轉送設定檔。




**STEP 9 |** 設定 **Traffic Enforcement**（流量強制執行）選項來決定您想要如何強制執行流量。




務必取消選取所有這些選項，因為不建議將它們用於動態權限存取。

- **Block all other unmatched outbound connections**（封鎖所有其他不相符的輸出連線）—啟用時會封鎖與任何轉送規則不相符的所有連線。流量不會透過通道傳送。
- **Block outbound LAN access when connected to the tunnel**（連線到通道時封鎖輸出 **LAN** 存取）—啟用時，如果代理程式連線到通道，會封鎖對本機網路的直接存取。

  封鎖對本機網路的存取會導致所有流量，無法傳送到本機轉接器。此外，您的使用者將無法存取本機子網路上的資源，例如印表機。根據存取路由、目的地網域和應用程式分割通道流量仍然如預期般運作。

  如果您停用此選項，您的一般使用者不需先使用 Prisma Access 代理程式連線到 Prisma Access，即可存取本機資源。
- **Block inbound access when connected to the tunnel**（連線到通道時封鎖輸入存取）—啟用時會封鎖來自通道的所有輸入連線。

**STEP 10 |** **Save**（儲存）您的轉送設定檔。


©2025 Palo Alto Networks, Inc.

**STEP 11 |** 透過選取 **Push Config**（推送設定） > **Push**（推送）來推送設定。此動作將使您的轉送設定檔可供在 [Agent Settings（代理程式設定）] 頁面中選取。

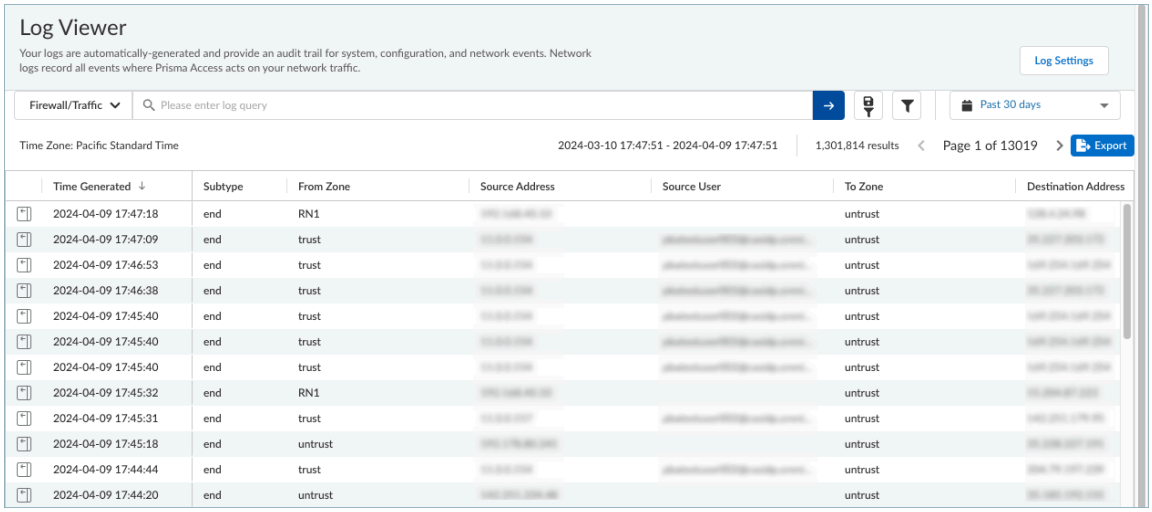
## 驗證動態權限存取代理程式的轉送設定檔設定，並針對其進行疑難排解

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access（由 Strata Cloud Manager 管理） | ❑ Prisma Access 5.1 Preferred 或 Innovation<br>❑ Prisma Access 授權，具有行動使用者訂閱<br>❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ 角色：超級使用者 |

設定轉送設定檔後，您可以透過檢視流量日誌檔案來驗證流量是否如預期般導向。您可以在 Strata Cloud Manager 日誌檢視器中檢視流量日誌，或使用端點上的 Prisma Access 命令列工具 (PACli) 檢視流量日誌。

若要從 Strata Cloud Manager 日誌檢視器檢視流量日誌檔案：

1. 選取 **Incidents & Alerts**（事件和警示） > **Log Viewer**（日誌檢視器）。
2. 檢視 **Firewall/Traffic**（防火牆/流量）日誌以取得詳細資訊。




 ©2025 Palo Alto Networks, Inc.

若要檢視端點上的流量日誌檔案：

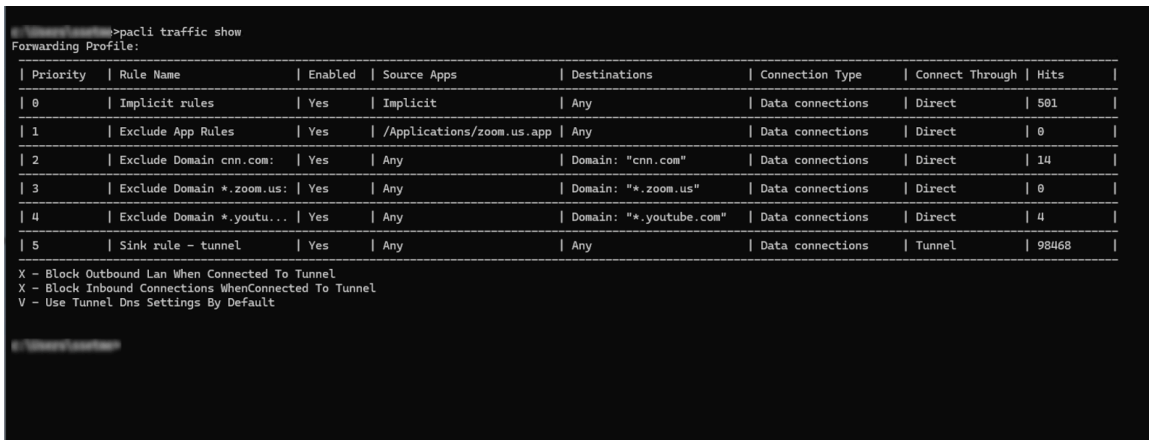
1. 在 **Manage**（管理） > **Prisma Access Agent**（**Prisma Access** 代理程式）中，或在一般使用者的裝置上開啟 Windows 命令提示或 macOS 終端機視窗，來啟動遠端 Shell。
2. 若要顯示轉送設定檔中的轉送規則，請發出下列命令：
   - 在 Windows 上：

     ```
     "C:\Program Files\Palo Alto Networks\Prisma Access Agent
     \pacli" traffic show
     ```

   - 在 macOS 上：

     ```
     /Applications/Prisma\ Access\ Agent.app/Contents/Helpers/
     pacli traffic show
     ```

   如果您為 *PACli* 工具 (*pacli*) 設定環境變數，只需輸入 ***pacli traffic show*** 即可。

   範例 PACli 命令列輸出顯示一個表格，其中包含轉送設定檔中有效的轉送規則，包括轉送規則的優先順序。也顯示了轉送設定檔的流量強制執行選項。此表格對應至您在轉送設定檔中設定的轉送規則。
3. 若要顯示轉送規則的詳細資訊，請發出下列命令：

   ```
   pacli traffic show <number>
   ```

   其中 **<number>** 是 `Priority` 欄的數字，例如：

 ©2025 Palo Alto Networks, Inc.

```
[redacted]>pacli traffic show 1
Printing forwarding profile rule #1
Priority        : 1
Rule Name       : Exclude App Rules
Enabled         : Yes
Source Apps     : /Applications/zoom.us.app
Destinations    : Any
Connection Type : Data connections
Connect Through : Direct
Hits            : 0

[redacted]>pacli traffic show 2
Printing forwarding profile rule #2
Priority        : 2
Rule Name       : Exclude Domain cnn.com:
Enabled         : Yes
Source Apps     : Any
Destinations    : Domain: "cnn.com"
Connection Type : Data connections
Connect Through : Direct
Hits            : 25

[redacted]>
```

4. 若要針對分割通道問題進行疑難排解，您可能需要檢查通道內部或外部的代理程式流量。您可以透過顯示 Prisma Access 代理程式連線日誌來執行此操作。發出下列命令：

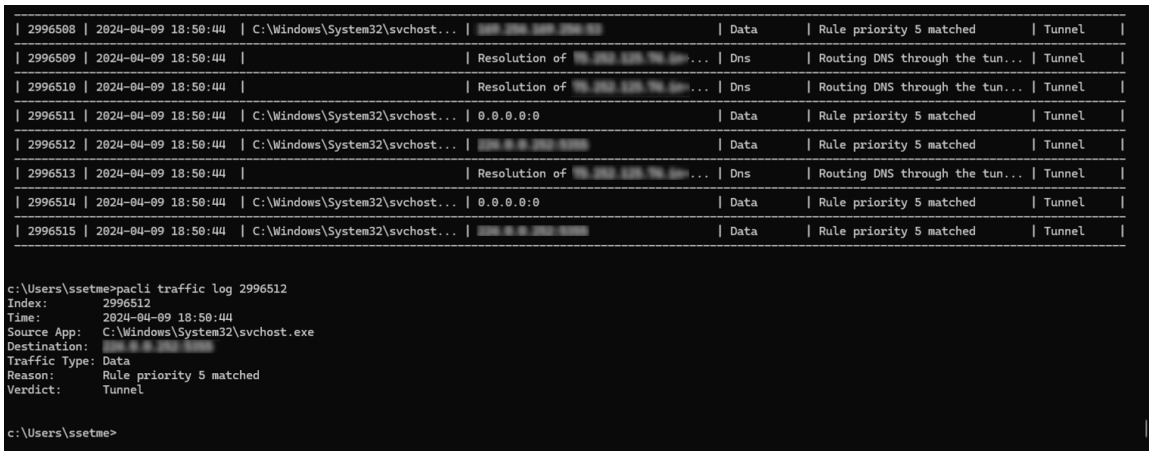
```
pacli traffic log
```

```
[redacted]>pacli traffic log
Network connection log:
 ------------------------------------------------------------------------------------------------------------------------------
 | Index   | Time                | Source App                  | Destination                  | Traffic... | Reason                      | Verdict   |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988329 | 2024-04-09 18:26:36 | C:\Windows\System32\svchost... | [redacted]                | Data       | Rule priority 5 matched     | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988330 | 2024-04-09 18:26:37 | C:\Windows\System32\svchost... | 0.0.0.0:0                    | Data       | Rule priority 5 matched     | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988331 | 2024-04-09 18:26:37 | C:\Windows\System32\svchost... | [redacted]                | Data       | Rule priority 5 matched     | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988332 | 2024-04-09 18:26:37 |                             | Resolution of [redacted]... | Dns        | Routing DNS through the tun... | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988333 | 2024-04-09 18:26:37 |                             | Resolution of [redacted]... | Dns        | Routing DNS through the tun... | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988334 | 2024-04-09 18:26:37 | C:\Windows\System32\svchost... | 0.0.0.0:0                    | Data       | Rule priority 5 matched     | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988335 | 2024-04-09 18:26:37 | C:\Windows\System32\svchost... | [redacted]                | Data       | Rule priority 5 matched     | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988336 | 2024-04-09 18:26:37 |                             | Resolution of [redacted]... | Dns        | Routing DNS through the tun... | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988337 | 2024-04-09 18:26:37 | C:\Windows\System32\svchost... | 0.0.0.0:0                    | Data       | Rule priority 5 matched     | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988338 | 2024-04-09 18:26:37 | C:\Windows\System32\svchost... | [redacted]                | Data       | Rule priority 5 matched     | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988339 | 2024-04-09 18:26:38 | C:\Windows\System32\svchost... | 0.0.0.0:0                    | Data       | Rule priority 5 matched     | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988340 | 2024-04-09 18:26:38 | C:\Windows\System32\svchost... | [redacted]                | Data       | Rule priority 5 matched     | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988341 | 2024-04-09 18:26:38 |                             | Resolution of [redacted]... | Dns        | Routing DNS through the tun... | Tunnel    |
```

若要顯示個別日誌項目，請發出下列命令：

```
pacli traffic log <index>
```

其中 **<index>** 對應至項目的索引號碼。例如：




您也可以透過發出以下命令將連線日誌匯出到檔案以供進一步分析：

```
pacli traffic log export <filename>
```

# 設定 Prisma Access Agent 應用程式設定進行動態權限存取

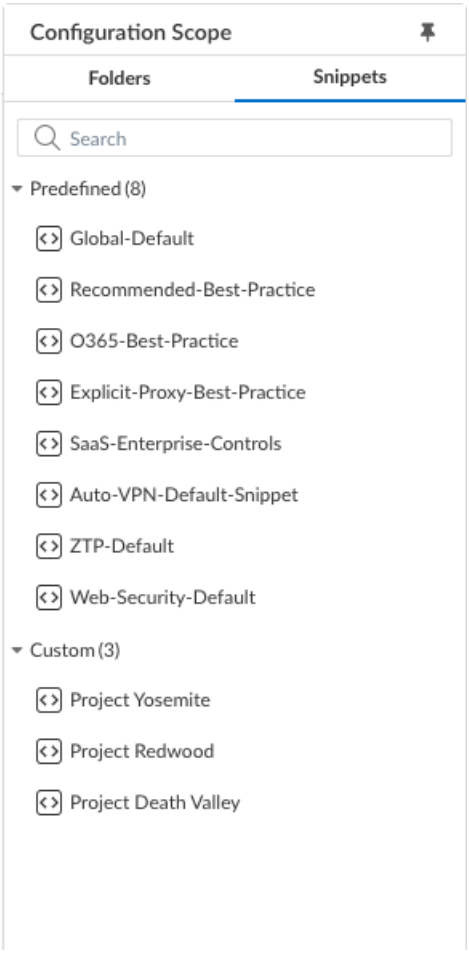
| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Prisma Access 授權，具有行動使用者訂閱<br>❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ 角色：專案管理員 |

Strata Cloud Manager 提供套用至所有專案中所有使用者群組的預設 Prisma Access Agent 應用程式設定。您可以新增應用程式設定，來自訂專案中的一般使用者與 Prisma Access Agent 互動的方式。

**STEP 1 |** 以專案管理員身份登入 Strata Cloud Manager。

 ©2025 Palo Alto Networks, Inc.

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

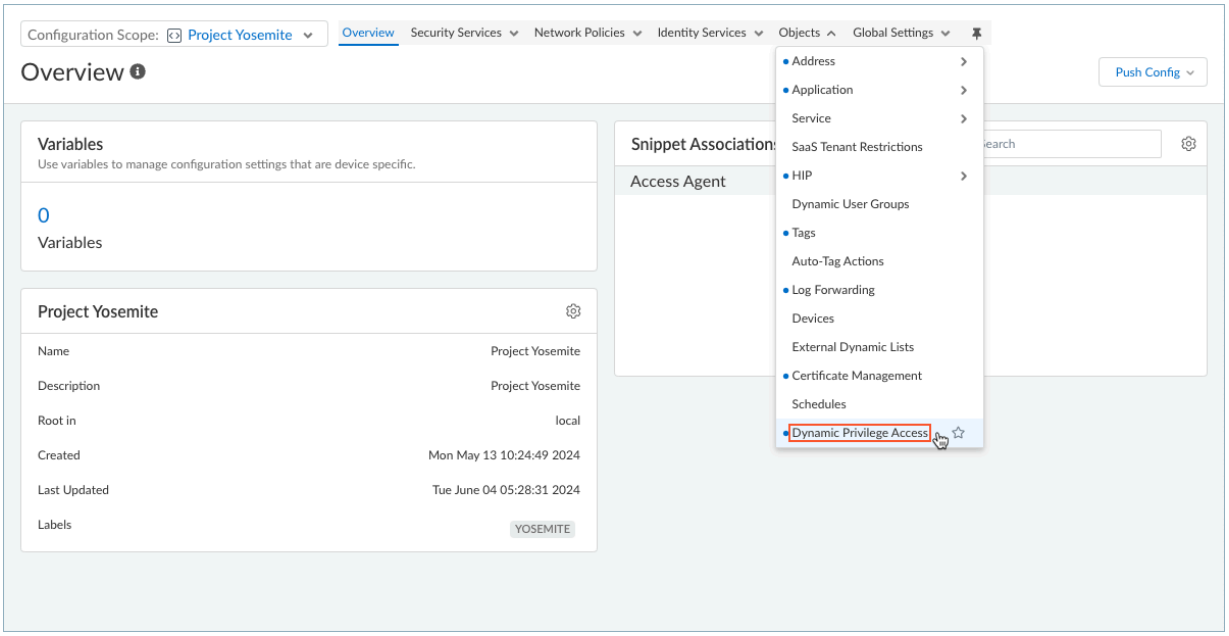



**STEP 3 |** 選取超級使用者管理員指定給您的片段。

您也可以檢視未指派給您的片段，但無法與它們互動，例如變更設定。


©2025 Palo Alto Networks, Inc.

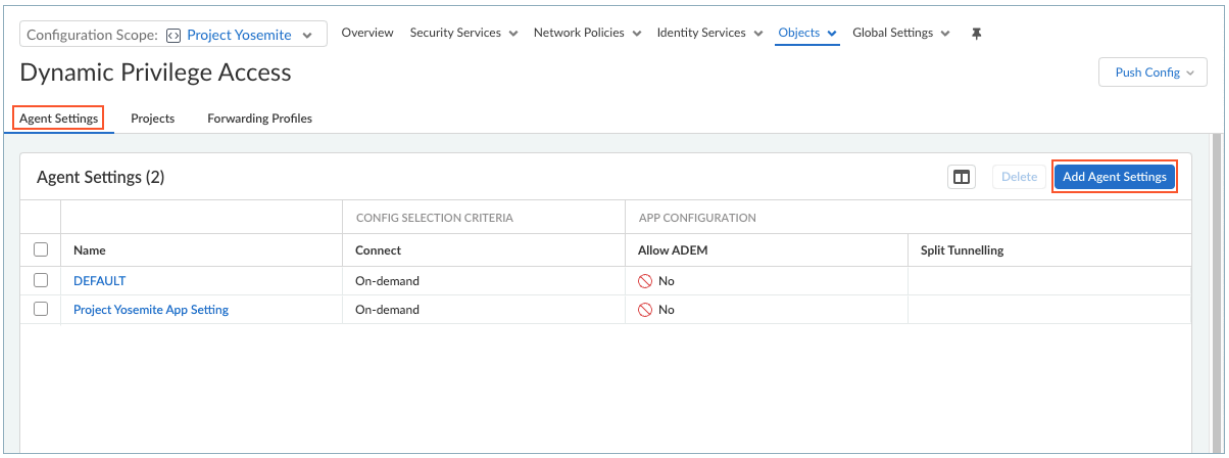
**STEP 4 |** 選取 **Objects**（物件） > **Dynamic Privilege Access**（動態權限存取），以開啟動態權限存取設定。




**STEP 5 |** 選取 **Agent Settings**（代理程式設定）頁籤。

**STEP 6 |** Strata Cloud Manager 為您提供預設代理程式設定。如果您不想要使用預設設定，請選取 **Add Agent Settings**（新增代理程式設定）。

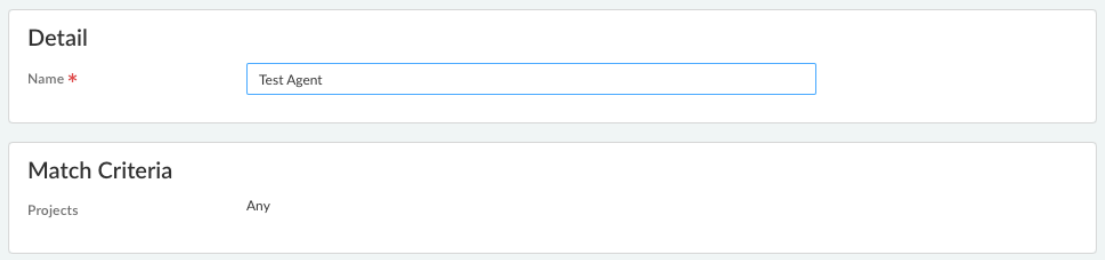
若要編輯代理程式的設定，請從表格中選取代理程式名稱。



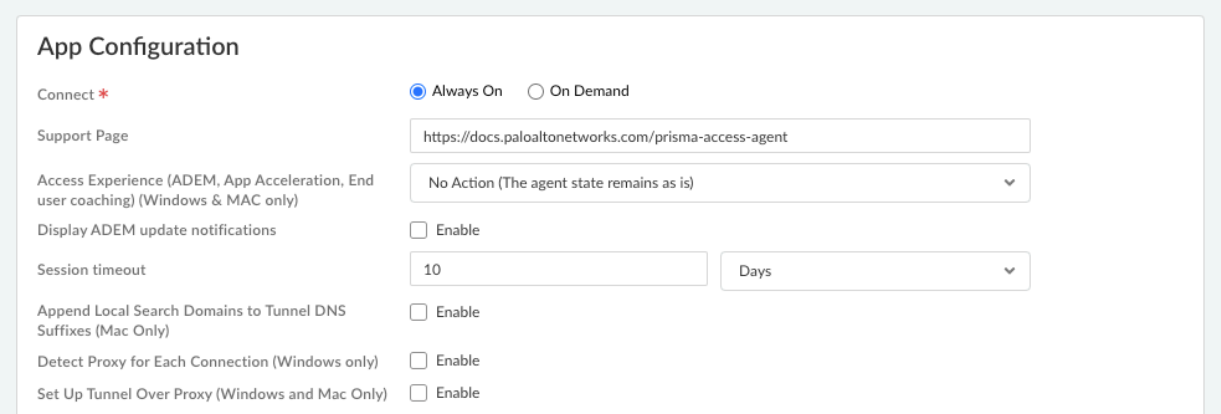

 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** 建立應用程式設定規則。設定規則會將一或多個專案與這些專案專屬的特定設定建立關聯。

1. 輸入規則的 **Name**（名稱）。
2. 透過新增 **Projects**（專案）來指定 **Match Criteria**（比對規則）。符合 **Project**（專案）準則的使用者和群組將在他們使用 Prisma Access Agent 登入專案時收到應用程式設定。
   - 若要將設定部署至所有使用者，請將 **Projects**（專案）設定為 **Any**（任何）。
   - 若要將設定部署至登入特定專案的使用者，請將 **Projects**（專案）設定為 **Add Projects**（新增專案），然後從專案清單中選取。




**STEP 8 |** 設定 Prisma Access 代理程式的應用程式設定。




- **Connect**（連線）—指定 Prisma Access 代理程式連線到 Prisma Access 的方式。這是必要設定。
  - 選取 **Always on**（一律開啟），每當使用者登入端點時，自動建立與 Prisma Access 代理程式的連線。
  - 選擇 僅當使用者按一下「連線（隨選）」時， 僅當使用者按一下 Prisma Access Agent 中的 「連線」（鎖定圖示）時才連線至 Prisma Access。
- **Support Page**（支援頁面）—當使用者按一下 Prisma Access 代理程式中的 **Support Resources**（支援資源）時，進入他們可以存取以獲得協助的網站。

  預設支援頁面是 Prisma Access 代理程式文件的網站。
- **Access Experience (ADEM, App Acceleration, End user coaching) (Windows & MAC only)**（存取體驗（**ADEM**、應用程式加速、一般使用者輔導）（僅限 **Windows** 和 **MAC**））—指定是否要在 Prisma Access 代理程式安裝期間安裝自發 DEM (ADEM) 端點代理程式，並允許一般使用者從應用程式中啟用或停用使用者體驗測試。
  - 安裝

 ©2025 Palo Alto Networks, Inc.

- 無動作（代理程式狀態保持原狀）
- 解除安裝

如需有關在雲端管理的 Prisma Access 上開始使用 ADEM 的詳細資料，請參閱開始使用自發 DEM。

- **Display ADEM update notifications**（顯示 **ADEM** 更新通知）—**Enable**（啟用）此設定，當端點上有更新可用時，顯示 ADEM 的通知。
- **Session timeout**（工作階段逾時）—當使用者連線至 Prisma Access 閘道（位置）並成功驗證時，系統會建立 Prisma Access 代理程式使用者工作階段。工作階段接著會被指派給特定閘道，根據任何已定義的分割通道規則，判斷哪些流量前往通道。Prisma Access 資料 平面最低版本必須為 11.2。

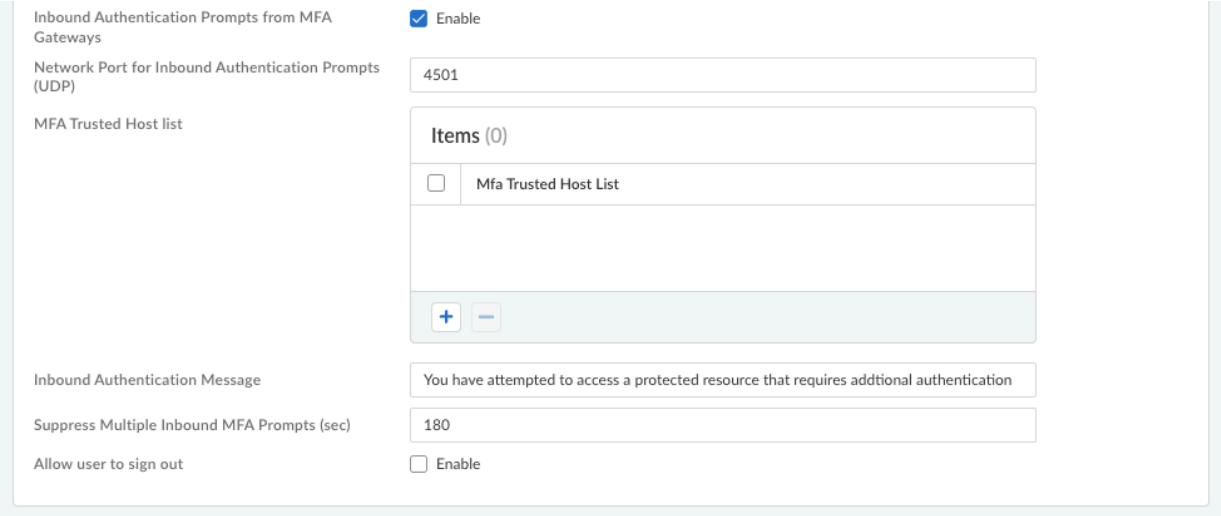
  指定工作階段由於非使用狀態而逾時之前必須經過的時間量。這是必要設定。

  如果您在 *Prisma Access* 中使用 *Nebula (10.2)* 資料平面，***Session timeout***（工作階段逾時）值無法設定且預設為 *7* 天。
- **Append Local Search Domains to Tunnel DNS Suffixes (Mac only)**（將本機搜尋網域附加到通道 **DNS** 尾碼（僅限 **Mac**））—**Enable**（啟用）此設定，將通道 DNS 搜尋網域附加到 macOS 端點上的本機 DNS 搜尋網域。將通道搜尋網域附加到端點的本機 DNS 搜尋網域，可讓使用者快速存取他們經常造訪的本機和遠端公司網站和伺服器，而無需輸入完整位址。
- **Detect Proxy for Each Connection (Windows only)**（偵測每個連線的 **Proxy**（僅限 **Windows**））—**Enable**（啟用）此設定，在每次連線時自動偵測 Proxy。如果您要自動偵測閘道連線的 Proxy，並將該 Proxy 用於與 Prisma Access 的後續連線，請停用此設定。
- **Set Up Tunnel Over Proxy (Windows and Mac Only)**（透過 **Proxy** 設定通道（僅限 **Windows** 和 **Mac**））—**Enable**（啟用）此設定，根據 Prisma Access 代理程式 Proxy 的使用來設定網路流量行為。選取 **Enable**（啟用）以要求 Prisma Access 代理程式使用 Proxy。如果您要要求 Prisma Access 代理程式略過 Proxy，請停用此設定。根據 Prisma Access 代理程式 Proxy 的使用、端點作業系統和通道類型，網路流量的行為將有所不同。

  如果停用此選項，Prisma Access 代理程式將略過 Proxy。與 Proxy 或 PAC 檔案規則相符的所有 HTTP 或 HTTPS 流量，都需要在到達預期目的地之前周遊 Prisma Access 代理程式通

 ©2025 Palo Alto Networks, Inc.

道。透過略過 Proxy，您可以防止使用者設定個人 Proxy 來存取 Web 資源，而無需透過通道進行檢查和政策強制執行。




- **Optimized MTU**（最佳化 **MTU**）—最大傳輸單位 (MTU) 是可在傳輸期間在封包中傳送的最大封包大小。**Enable**（啟用）此選項以自動決定用於封包傳輸的最佳 MTU。

  Prisma Access 代理程式連線可以周遊多個 ISP 和網路躍點，其具有低於標準 1500 位元組的 MTU 值。當靜態代理程式 MTU 值低於 ISP 提供的 MTU 值時，會出現過多的分段和額外負荷，導致輸送量降低。ISP 網路路徑中丟棄的封包也會觸發重新傳輸，導致效能欠佳。

  啟用 **Optimized MTU**（最佳化 **MTU**）可協助您避免繁瑣的手動判斷和設定最佳 MTU 值，並防止使用者體驗到會影響其生產力的不良效能。

  **Optimized MTU**（最佳化 **MTU**）預設為啟用。如果停用，您可以手動設定 MTU。**Configurable MTU (bytes)**（可設定的 **MTU**（位元組））範圍是 256 至 1420 位元組。預設值為 1400 位元組。
- **Inbound Authentication Prompts from MFA Gateways**（來自 **MFA** 閘道的輸入驗證提示）—若要支援多重要素驗證 (MFA)，Prisma Access 代理程式端點必須收到從閘道傳來的


©2025 Palo Alto Networks, Inc.

UDP 提示並進行確認。**Enable**（啟用）此設定以允許 Prisma Access 代理程式端點接收和確認 UDP 提示。此設定預設為啟用。停用此設定以封鎖來自閘道的 UDP 提示。

- **Network Port for Inbound Authentication Prompts (UDP)**（供輸入驗證提示 **(UDP)** 使用的網路連接埠）—指定 Prisma Access 代理程式用來接收來自 MFA 閘道之輸入驗證提示的連接埠號碼。預設連接埠為 4501。若要變更連接埠，請指定 1 到 65535 的數字。
- **MFA Trusted Host list**（**MFA** 受信任主機清單）—為 Prisma Access 代理程式端點可信任多因素驗證的防火牆或驗證閘道**Add**（新增）主機。當端點在指定的網路連接埠上收到 UDP 訊息時，Prisma Access 代理程式只會在 UDP 提示是來自受信任的閘道時顯示驗證訊息。
- **Inbound Authentication Messages**（輸入驗證訊息）—自訂通知訊息，以在使用者嘗試存取需要另外驗證的資源時顯示此訊息。

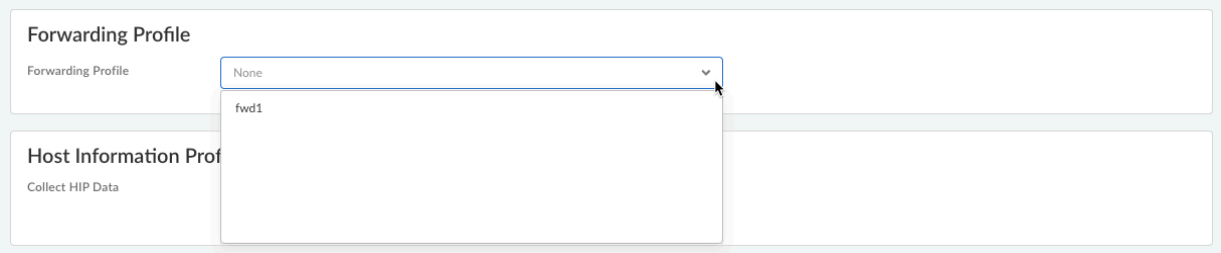
  當使用者嘗試存取需要額外驗證的資源時，Prisma Access 代理程式會收到一個包含輸入驗證提示的 UDP 封包，並顯示此訊息。UDP 封包也包含您在設定多因素驗證時所指定的驗證入口網站頁面 URL。Prisma Access 代理程式會自動將 URL 附加到訊息。

  例如：

  > 您已嘗試存取需要另外驗證的受保護資源。您想繼續嗎？

  此訊息必須為 255 個或更少的字元。
- **Suppress Multiple Inbound MFA Prompts (sec)**（隱藏多個輸入 **MFA** 提示（秒））—指定 Prisma Access 代理程式可以隱藏多個輸入 UDP 提示之前要等待的秒數。預設值是 180 秒。
- **Allow user to sign out**（允許使用者登出）—**Enable**（啟用）此設定以允許您的使用者登出 Prisma Access 代理程式。此設定預設為停用。

**STEP 9 |** 選取您先前設定的 **Forwarding Profile**（轉送設定檔），以管理代理程式與 Prisma Access 之間的流量流動方式。




**STEP 10 |** 設定 DNS 設定進行動態權限存取。

**STEP 11 |** 設定主機資訊設定檔設定

**STEP 12 |** 當完成了設定 Prisma Access Agent 設定時，按一下 **Save**（儲存）。

 ©2025 Palo Alto Networks, Inc.

# 設定 DNS 設定進行動態權限存取。

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Prisma Access 授權，具有行動使用者訂閱<br>❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ 角色：專案管理員 |

您可以設定 DNS 伺服器，以啟用 Prisma Access 解析您的內部網域。

**STEP 1 |** 從 Strata Cloud Manager 中，選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概要），並展開設定範圍以檢視 **Snippets**（片段）。

**STEP 2 |** 選取超級使用者管理員指定給您的片段。

**STEP 3 |** 選取 **Objects**（物件） > **Dynamic Privilege Access**（動態權限存取），以開啟動態權限存取設定。

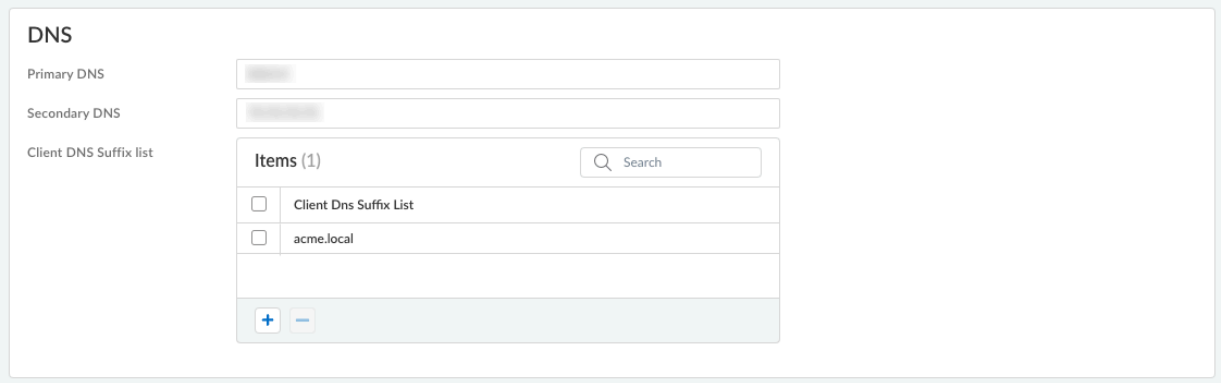
**STEP 4 |** 選取 **Agent Settings**（代理程式設定）頁籤。

**STEP 5 |** **Add Agent Settings**（新增代理程式設定）或從代理程式設定表格中選取現有設定。

**STEP 6 |** 輸入 Prisma Access 應用於解析內部網域名稱的 **Primary DNS**（主要 **DNS**）伺服器和 **Secondary DNS**（次要 **DNS**）伺服器。

**STEP 7 |** 您可以新增 **Client DNS Suffix List**（用戶端 **DNS** 尾碼清單），指定 輸入無法解析的不完整主機名稱時，用戶端應在本機使用的尾碼，例如，**`acme.local`**。

請勿在網域尾碼前面輸入萬用字元 (*)（例如，acme.com）。您可以新增多個尾碼。




 ©2025 Palo Alto Networks, Inc.

# 設定 HIP 資料收集設定進行動態權限存取

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ Prisma Access 授權，具有行動使用者訂閱<br>❑ 角色：專案管理員 |

Prisma Access 代理程式會收集有關其執行之主機的資訊，並在成功連線後將此主機資訊提交至 Prisma Access 位置（閘道）。閘道會將 Prisma Access 代理程式提交的此原始主機資訊與您已定義的任何主機資訊設定檔 (HIP) 物件和 HIP 設定檔相比對。如果發現相符，它會在 HIP 比對日誌中產生項目。此外，如果在原則規則中發現 HIP 設定檔的相符項，則會強制執行對應的安全原則。

在 [Edit Global Agent Settings（編輯全域代理程式設定）] 頁面的 **HIP Notifications**（**HIP** 通知）頁籤中，您可以建立 HIP 通知、建立和管理 HIP 物件，以及建立和管理套用至所有端點的 Prisma Access 代理程式的 HIP 設定檔。

您可以在這裡定義希望 Prisma Access 代理程式收集或排除的自訂 HIP 資料。啟用此選項時，Prisma Access 代理程式會從執行 macOS 或 Windows 作業系統的裝置收集資料。

例如，自訂檢查可讓您瞭解某個應用程式是否已安裝或在端點上執行。您定義在自訂檢查中收集的資料包含在 Prisma Access 代理程式收集的原始主機資訊資料中，然後在 Prisma Access 代理程式連線時提交給 Prisma Access。

**STEP 1 |** 從 Strata Cloud Manager 中，選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Overview**（概要），並展開設定範圍以檢視 **Snippets**（片段）。

**STEP 2 |** 選取超級使用者管理員指定給您的片段。

**STEP 3 |** 選取 **Objects**（物件） > **Dynamic Privilege Access**（動態權限存取），以開啟動態權限存取設定。

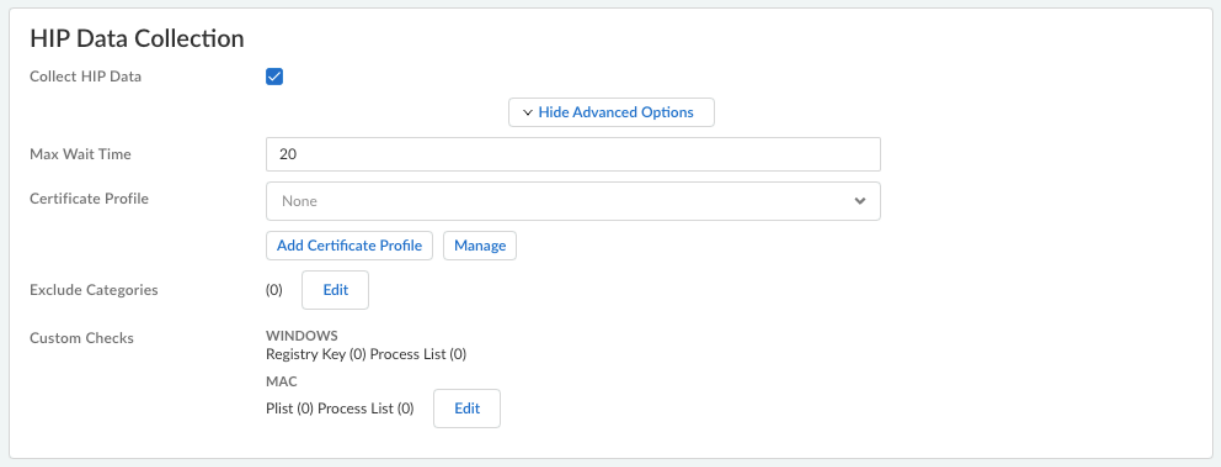
**STEP 4 |** 選取 **Agent Settings**（代理程式設定）頁籤。

**STEP 5 |** **Add Agent Settings**（新增代理程式設定）或從代理程式設定表格中選取現有設定。

**STEP 6 |** 在 [Host Information Profile (HIP)（主機資訊設定檔 (HIP)）] 區段中，選取 **Collect HIP Data**（收集 **HIP** 資料）以在使用專案登入的端點上啟用 HIP 資料收集。


©2025 Palo Alto Networks, Inc.

**STEP 7 |** 選取 **Show Advanced Options**（顯示進階選項）。



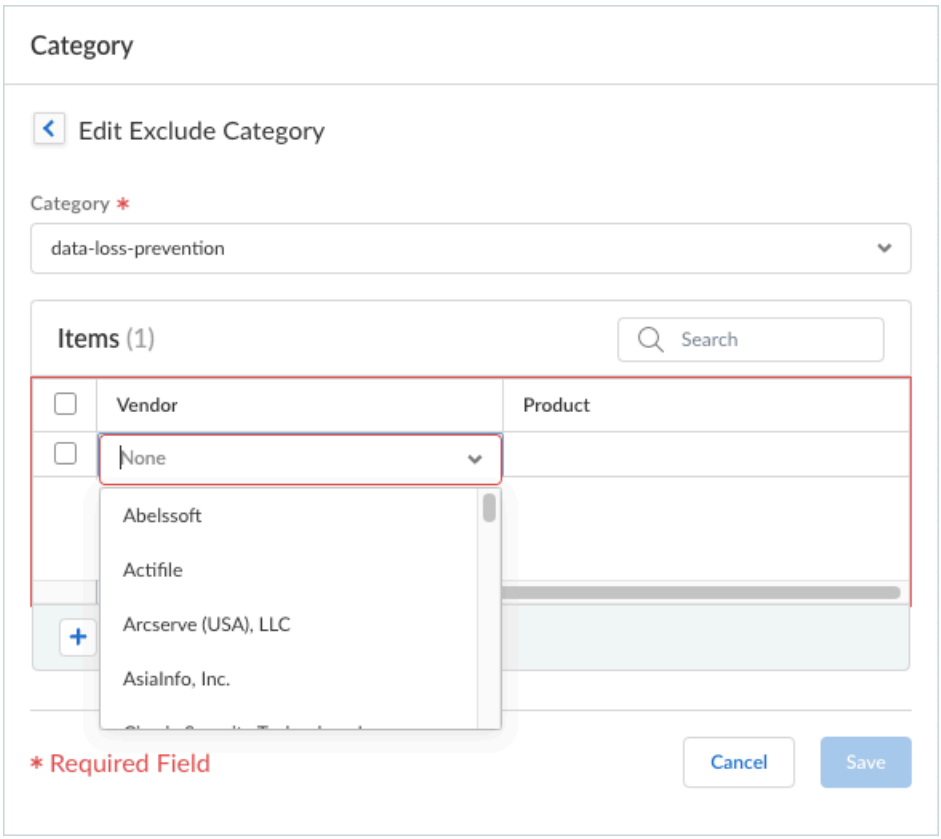

**STEP 8 |** 指定 Prisma Access 代理程式在提交可用資料之前應搜尋 HIP 資料的 **Max Wait Time**（等候時間上限）（秒）。範圍為 10 至 60 秒，預設值為 20 秒。

**STEP 9 |** **Edit**（編輯）排除類別來排除特定類別或 HIP 資料收集類別中的廠商、應用程式或版本。

選取 HIP 收集要排除的 **Category**（類別）（例如資料遺失防護）。在選取類別後，您可 **Add**（新增）特定 **Vendor**（廠商），然後可以從廠商 **Add**（新增）特定 **Product**（產品），視


©2025 Palo Alto Networks, Inc.

需進一步調整排除。您可以將多個廠商與產品新增至排除清單。**Save**（儲存）每個對話方塊中的設定。



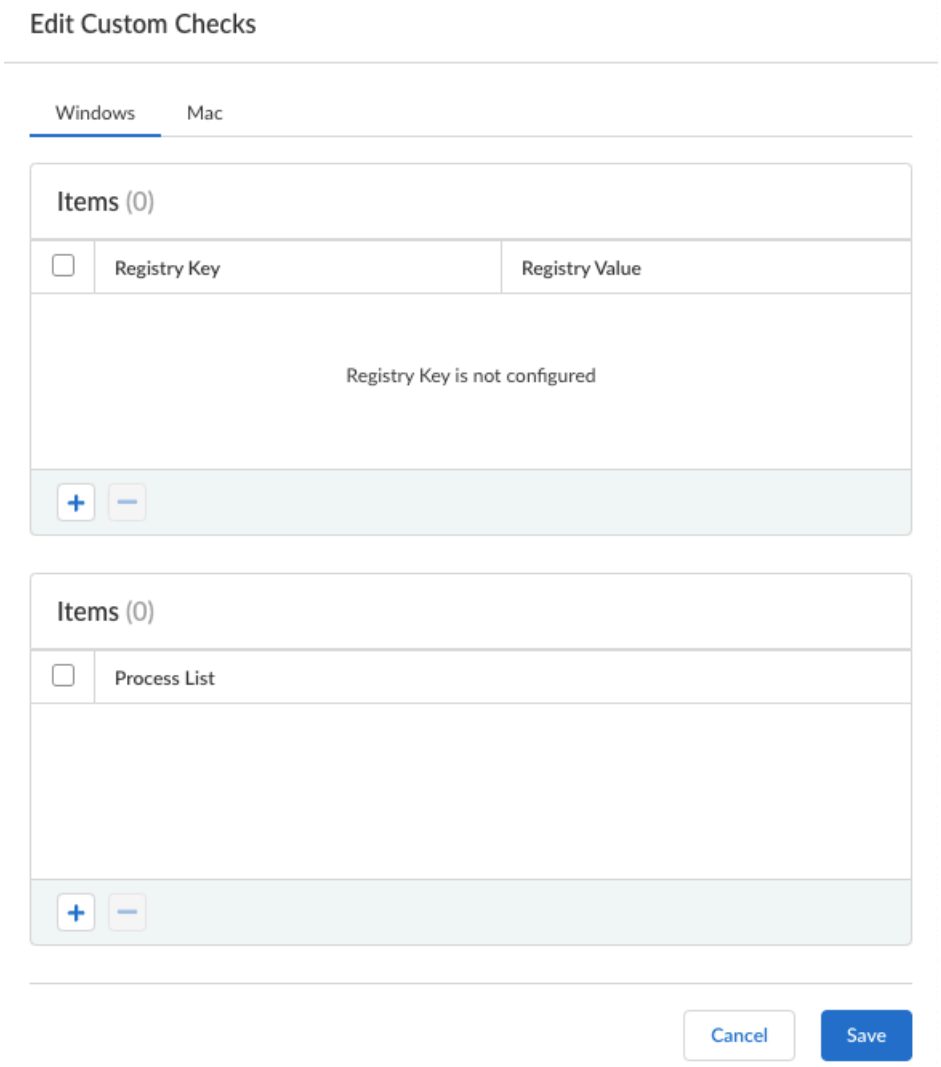

如果您不想排除整個廠商，可以排除某個廠商的特定修補程式。新增廠商後，您可以使用下列格式指定修補程式名稱或編號，以及選擇性地指定從 HIP 報告中排除修補程式更新的日期：

```
不包括：[kb-article-id1:MM/DD/YYYY], [kb-article-id2:MM/DD/YYYY]
```

其中 **<kb-article-id>** 是屬性中的名稱或編號（例如 **<kb-article-id>2267602</kb-article-id>**） 且**MM/DD/YYYY** 指定從 HIP 報告中排除修補程式的日期。如果您未設定日期，修補程式將無限期從 HIP 報告中排除。如果您設定了日期，則在指定日期之前，修補程式將被排除在外。


©2025 Palo Alto Networks, Inc.

**STEP 10 |** **Edit**（編輯）自訂檢查以定義您要從執行此設定之主機收集的任何自訂資料。




例如，如果廠商或產品清單不含建立 HIP 物件所需要的任何應用程式，您可以建立自訂檢查以判定該應用程式是否已安裝（具有對應的 Windows 登錄或 Mac Plist 機碼）或目前正在執行（具有對應的執行中程序）：

- **Windows**—**Add**（新增）特定登錄機碼或登錄值的檢查。若要限制特定登錄值的資料收集，**Add**（新增）然後定義特定登錄值。
- **Mac**—**Add**（新增）特定 **plist** 機碼或**Key**（機碼）值的檢查。若要限制特定機碼值的資料收集，**Add**（新增）機碼值。按一下 [OK（確定）] 以儲存設定。
- 處理清單—**Add**（新增）您想要在使用者端點上檢查是否正在執行的程序。例如，若要確定是否正在執行某軟體應用程式，請將可執行檔的名稱新增至程序清單。您可以將程序新增至 **Windows** 頁籤、**Mac** 頁籤或兩者。

完成後 **Save**（儲存）自訂檢查設定。

**STEP 11 |** 在完成了設定專案特定的 Prisma Access Agent 設定之後，請 **Save**（儲存）設定。


©2025 Palo Alto Networks, Inc.

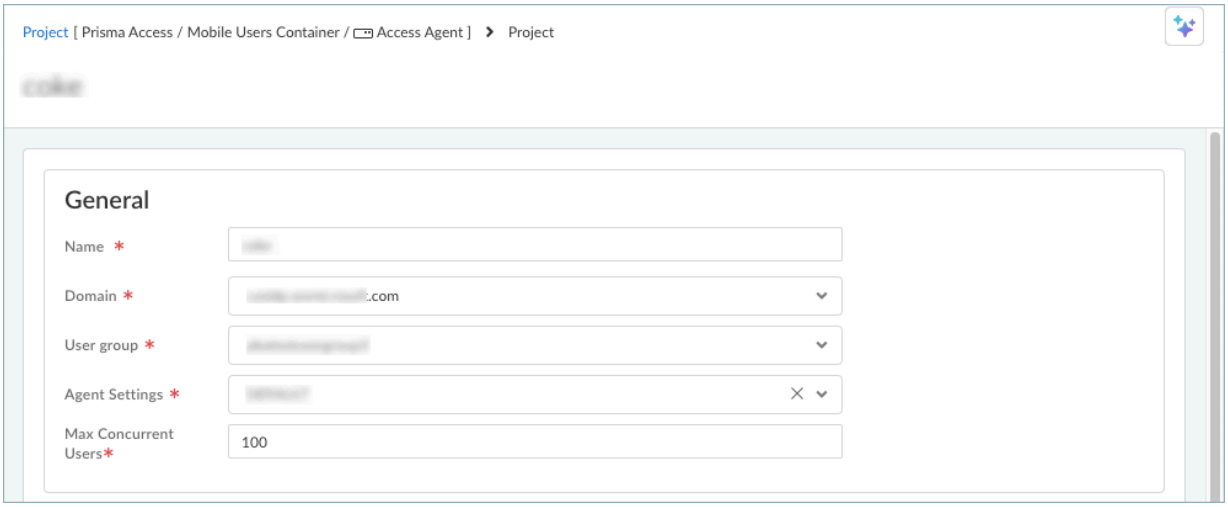
# 建立專案

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access授權<br>❑ 最低必要 Prisma Access 版本：5.1<br>❑ 角色：超級使用者 |

新增您想要使用者使用 Prisma Access Agent 存取的專案。只有專案管理員才能建立並管理專案定義。

**STEP 1 |** 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**）。

**STEP 2 |** 將範圍設定為您所建立的專案片段，然後導覽至 **Objects**（物件） > **Dynamic Privilege Access**（動態權限存取） > **Projects**（專案） > **Add Project**（新增專案）。

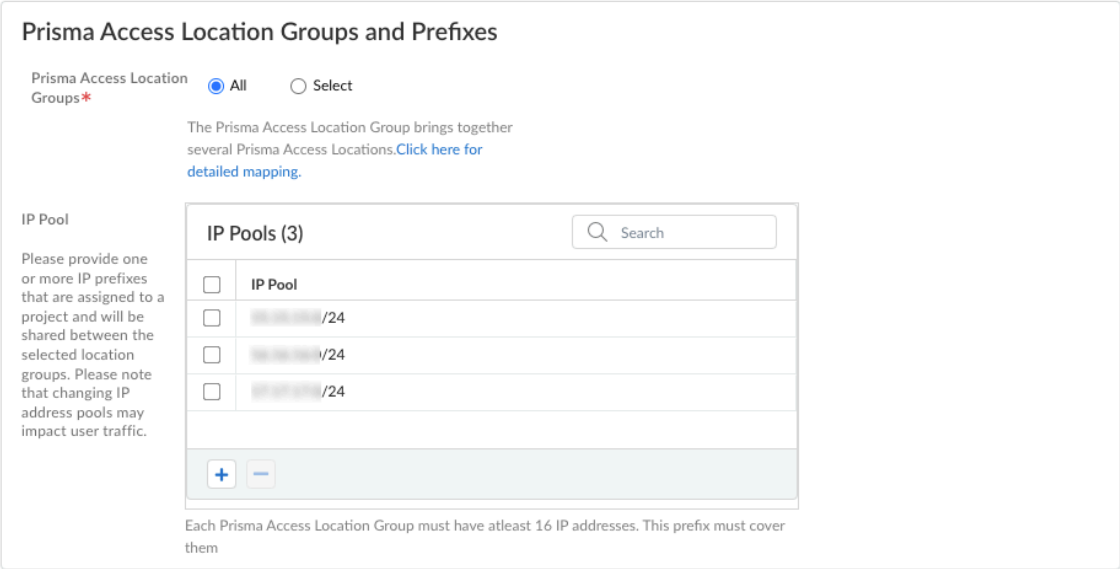



1. 輸入專案 **Name**（名稱）。
2. 選取您已在雲端識別引擎中新增的 **Domain**（網域），以及對應到目錄的 **User Group**（使用者群組）。
3. 選取您先前新增的 **Agent Settings**（代理程式設定），以及專案的 **Max Concurrent Users**（並行使用者數上限）。
4. 選取 **Prisma Access Location Groups**（**Prisma Access** 位置群組）。位置群組清單是根據您新增 GlobalProtect 閘道的位置填入的。

   您正在建立的專案與 IP 集區和位置群組相關聯。使用者將根據他們使用 Prisma Access Agent 連線到的專案和 Prisma Access 計算位置來獲取 IP 位址。一個專案只能連線到位置群組內與該專案相關聯的位置。您可以選取 **Click here for detailed mapping**（按一下


©2025 Palo Alto Networks, Inc.

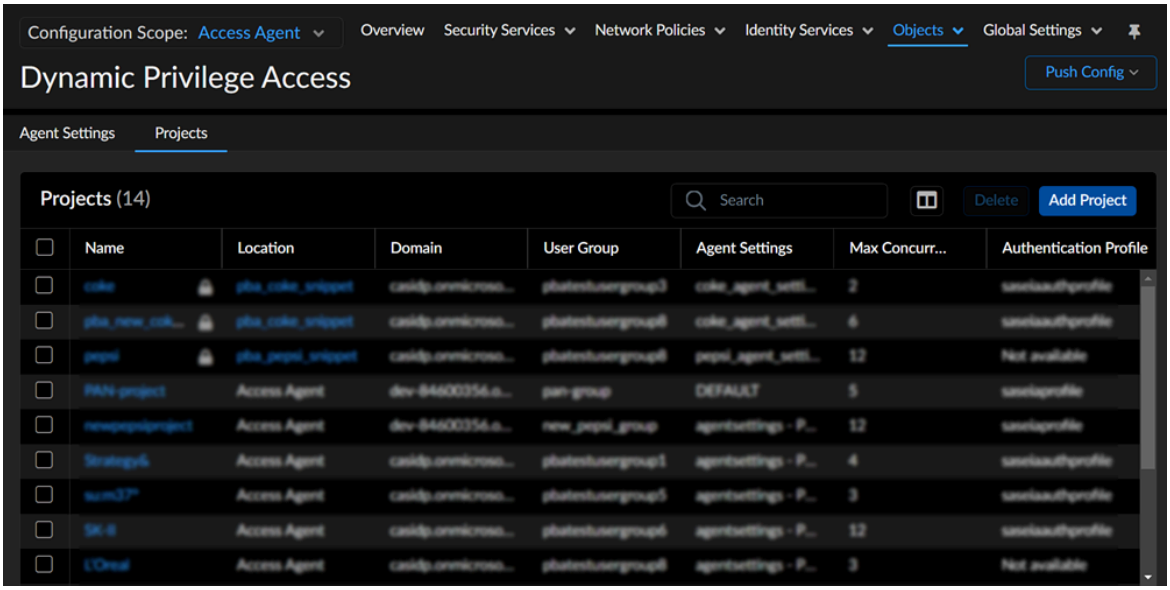
這裡以取得詳細對應），查看 Prisma Access 位置群組與 Prisma Access 計算位置之間的對應。




5. 為您的專案新增或選取 **IP Pools**（**IP** 集區）。IP 首碼會指派給您的專案，並將在您選取的 Prisma Access 位置群組之間共用。

   這些專案 IP 集區可以進行匯總，以減少傳送到網路的路由數目。

6. **Save**（儲存）專案設定。




 ©2025 Palo Alto Networks, Inc.

- 當您在組態範圍中選取專案片段時，只能存取與該特定專案相關的設定和詳細資訊。
- 以專案管理員或專案推送管理員身分登入 *Strata Cloud Manager* 時，您只能檢視您有權存取的專案詳細資訊。如果您選取另一個專案片段的組態範圍，則無法存取另一個專案的設定和詳細資訊。
- 若要在專案之間切換，您必須使用不同專案的認證以不同的專案管理員或專案推送管理員身分重新登入 *Strata Cloud Manager*。

**STEP 3 |** **Push**（推送）您的變更。

在 Prisma Access 建立專案之後，最多可能需要 15 分鐘，然後使用者才能使用 Prisma Access Agent 對該專案進行驗證。

 ©2025 Palo Alto Networks, Inc.

# 動態權限存取的流量導向

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 授權<br>❑ 最低必要 Prisma Access 版本：5.1<br>❑ 角色：專案管理員 |

使用流量導向，將專案的流量轉送到服務連線和專案特定路由。

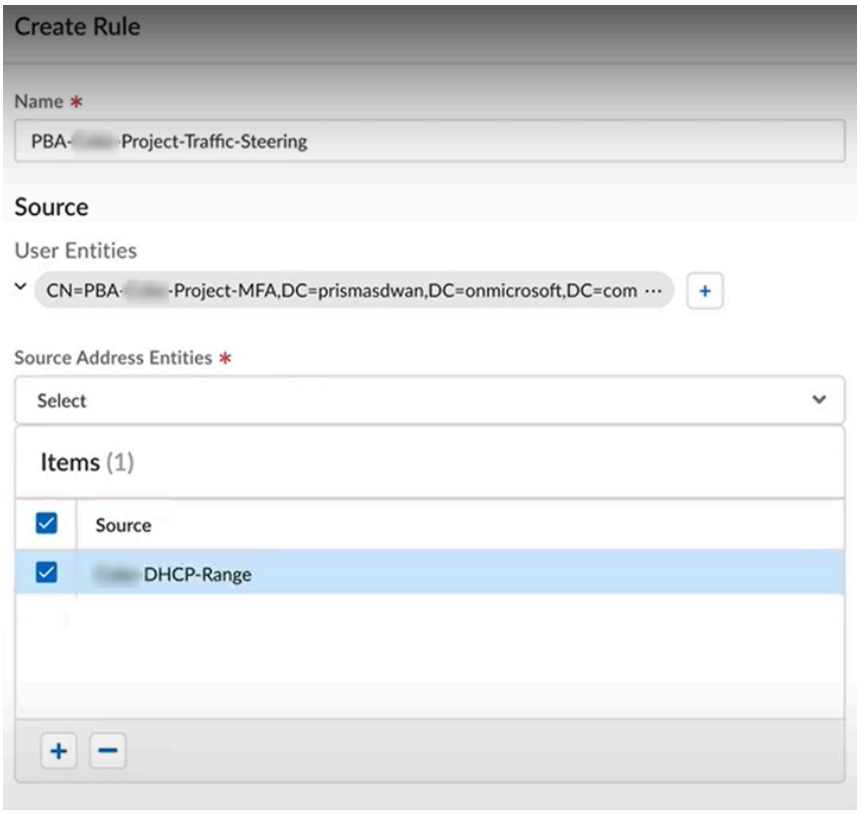
**STEP 1 |** 選取 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Service Connections**（服務連線）。

**STEP 2 |** 新增服務連線。

**STEP 3 |** 編輯 **Advanced Settings**（進階設定）以路由流量。

**STEP 4 |** 為您的專案在 **Traffic Steering**（流量導向）下 **Add Rule**（新增規則）。

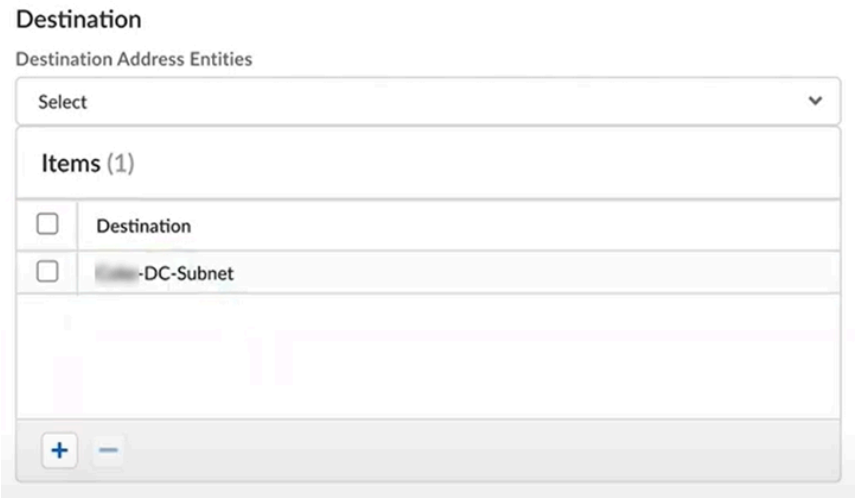
**STEP 5 |** 將 **Source**（來源）與使用者比對，並將專案 DHCP 範圍新增為 **Source Address Entities**（來源位址實體）。



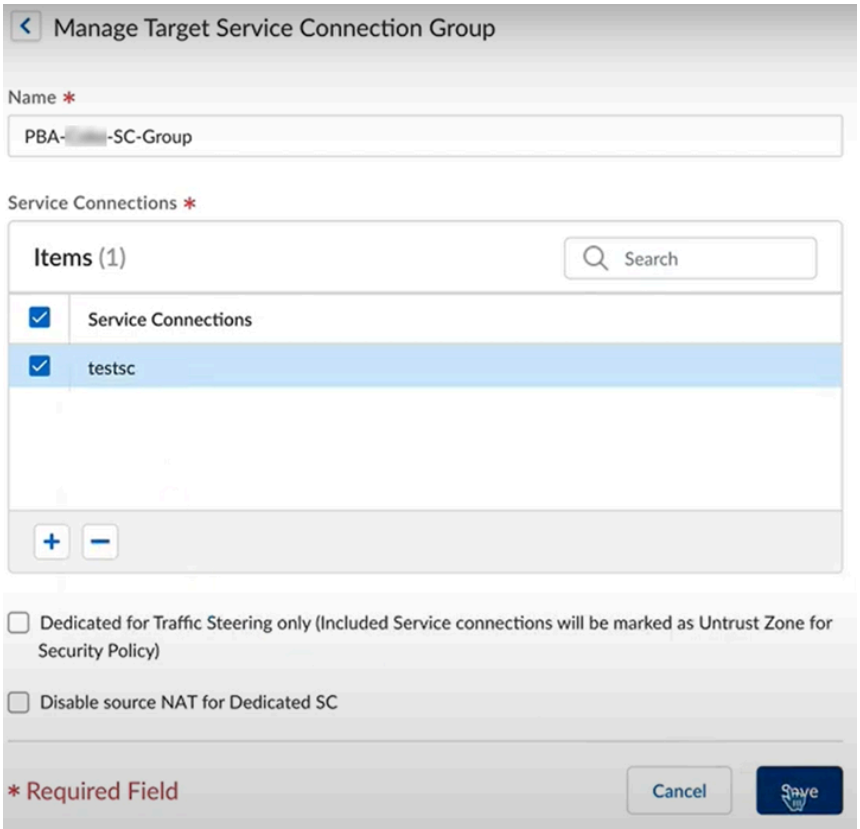


©2025 Palo Alto Networks, Inc.

**STEP 6 |** 比對 **Destination**（目的地）位址實體。




**STEP 7 |** 選取服務和動作。




**STEP 8 |** 提交並推送變更。


©2025 Palo Alto Networks, Inc.

# 設定 Prisma Access Agent 進行動態權限存取

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Prisma Access 授權，具有行動使用者訂閱<br>❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ 角色：超級使用者 |

您的一般使用者將使用 Prisma Access Agent，根據指派給您使用者的客戶專案存取您組織的網路。

在設定專案特定的代理程式設定，並建立了專案之後，您可以設定其他 Prisma Access Agent 設定，例如分階段推出和全域代理程式設定。

您可以設定下列 Prisma Access Agent 設定：

- 為 Prisma Access 代理程式設定分階段推出
- 為 Prisma Access 代理程式設定一般全域設定
- 為 Prisma Access 代理程式設定 HIP 通知

## 為 Prisma Access Agent 設定分階段推出

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access（由 Strata Cloud Manager 管理） | ❑ Prisma Access 5.1 Preferred 或 Innovation<br>❑ Prisma Access 授權，具有行動使用者訂閱<br>❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ 角色：超級使用者 |

Prisma Access 代理程式升級推出功能為管理員提供了一種按特定順序升級裝置群組的方法。隨著升級推出，您不再需要依賴行動裝置管理 (MDM) 軟體（例如 Jamf Pro 和 Microsoft Intune）來升級 Prisma Access 代理程式。

分階段升級推出只能在初始部署 或安裝 一般使用者裝置上的 *Prisma Access* 代理程式之後進行。

若要分階段推出 Prisma Access 代理程式升級，您可以根據使用者、群組和作業系統使用比對規則設定升級環。符合準則的裝置將按升級環的順序進行升級（環 0 到環 4，預設環）。

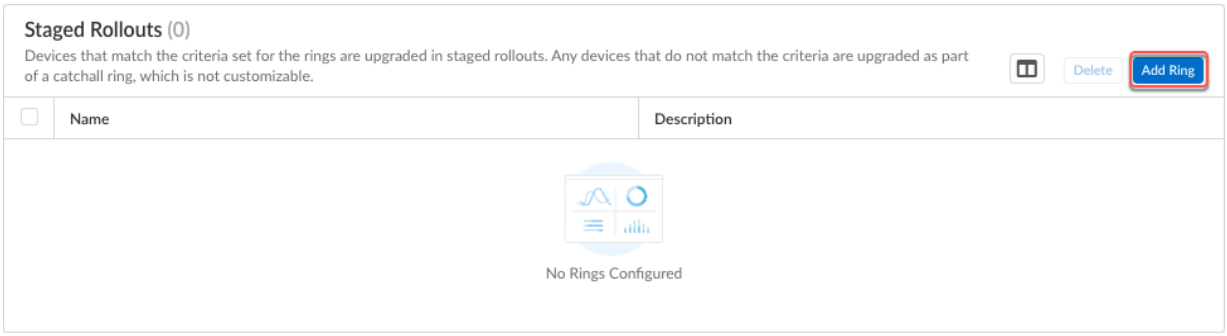

©2025 Palo Alto Networks, Inc.

當您使用 Prisma Access 代理程式的 [Access Agent Setup（存取代理程式設定）] 頁面裝載行動使用者時，您可以選擇性地定義升級環。如果在初始代理程式設定期間選擇不定義升級環，則所有裝置都將置於預設環中。您可以稍後返回 [Prisma Access Agent Setup（Prisma Access 代理程式設定）] 頁面，以定義升級環並將設定推送到 Prisma Access。這些變更將在下一個分階段推出期間生效，或者在您停止然後再開始分階段推出後生效。

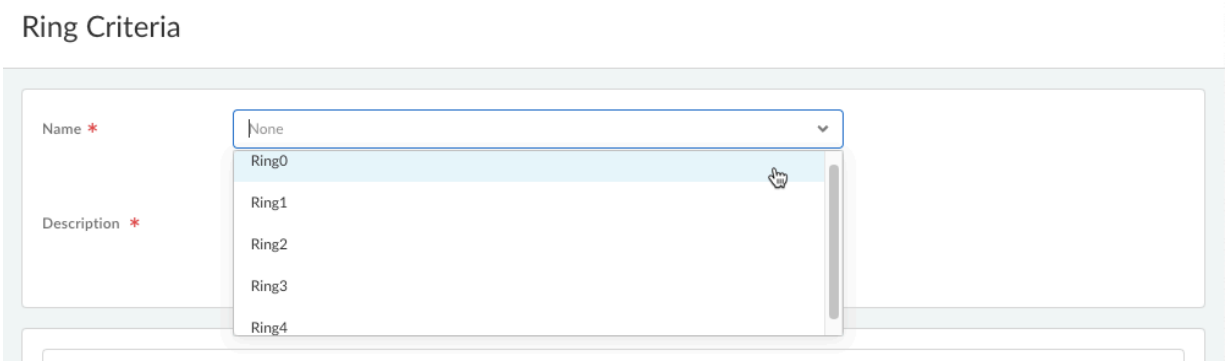
若要設定升級環：

**STEP 1 |** 在 Strata Cloud Manager 中，選取 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Access Agent**（存取代理程式） > **Prisma Access Agent**（**Prisma Access** 代理程式）。

**STEP 2 |** 在 **Staged Rollouts**（分階段推出）區段中，按一下 **Add Ring**（新增環）。




**STEP 3 |** 為環選取預先定義的 **Name**（名稱）。您可以從 **Ring0**（環 **0**） 到 **Ring4**（環 **4**）之間選取。您將新增的第一個環是 **Ring0**（環 **0**）。

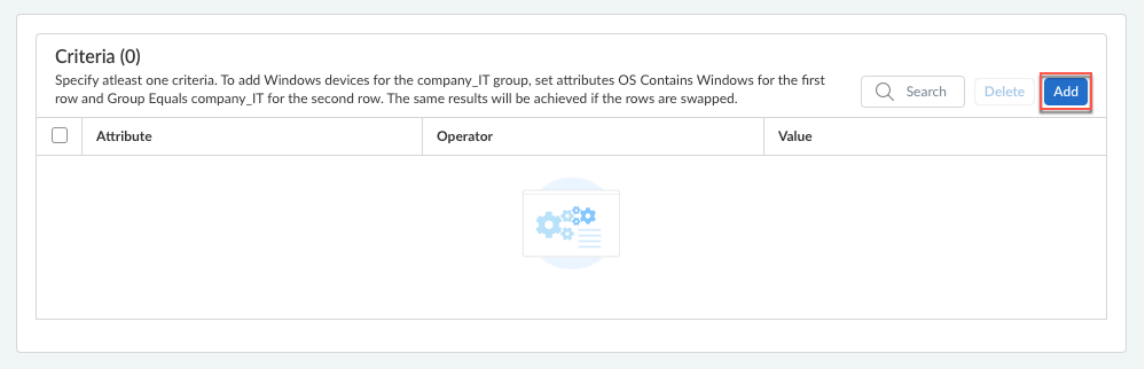



**STEP 4 |** 為環輸入有意義的 **Description**（說明）。


©2025 Palo Alto Networks, Inc.

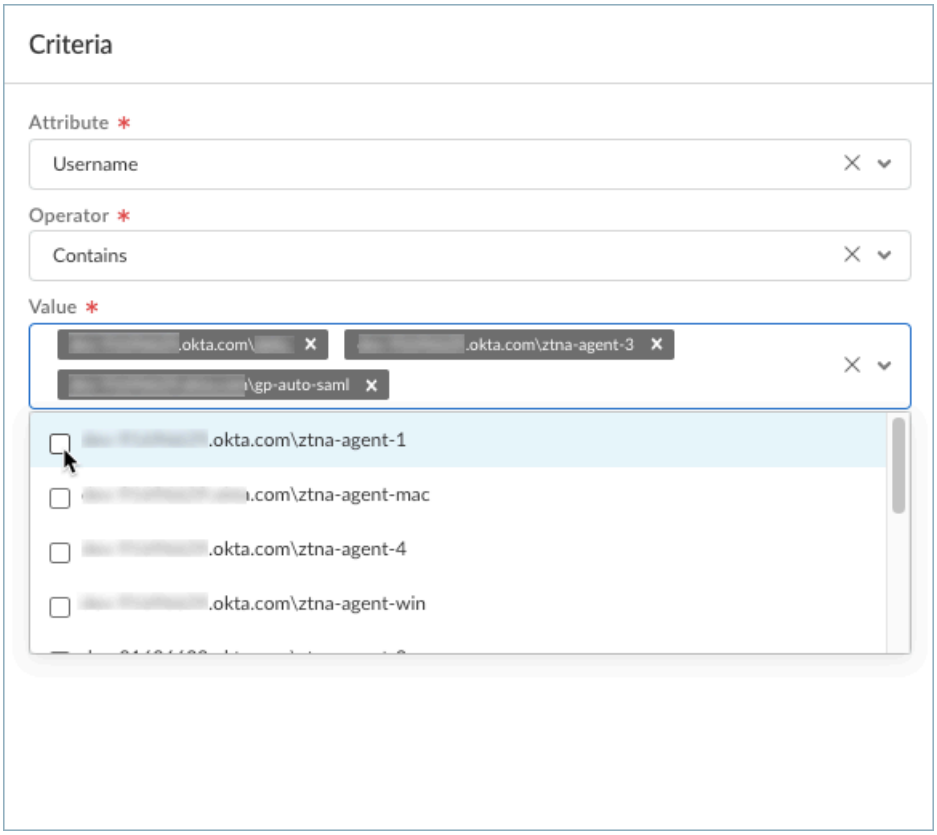
**STEP 5 |** 根據 **User**（使用者）、**Groups**（群組）或 **Device OS**（裝置作業系統）屬性，指定環的準則。

1. **Add**（新增）準則。



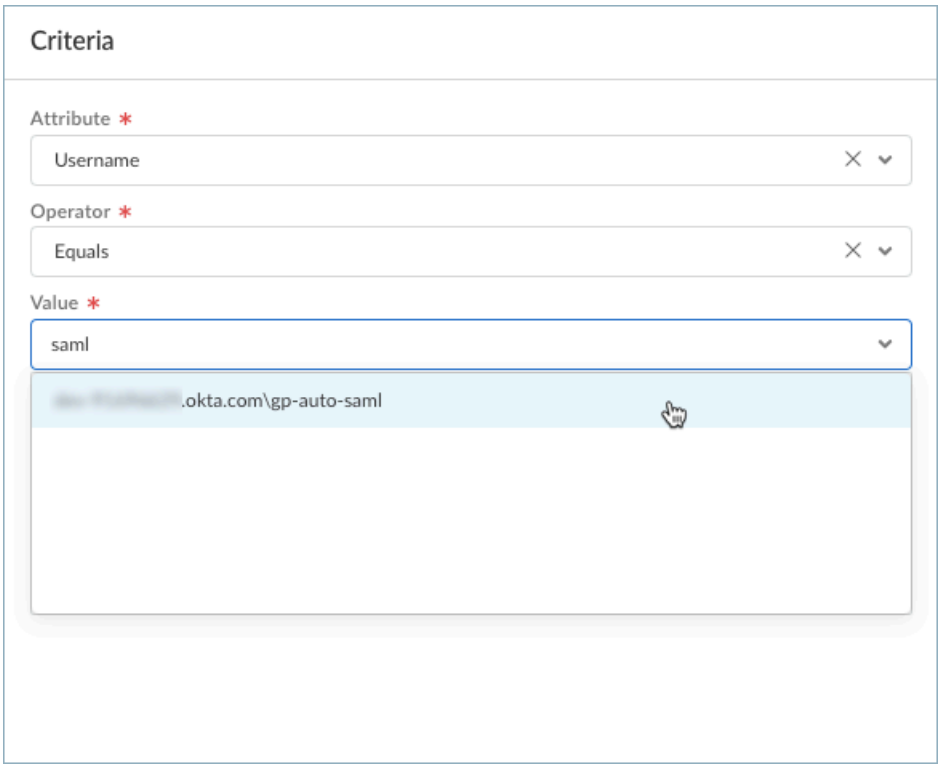

2. 針對每個準則，選取 **Attribute**（屬性）、**Operator**（運算子）、**Value**（值），然後按一下 **Add**（新增）。您只能為每個準則選取一個屬性和運算子。該值取決於您為屬性和運算子選取的項目：

   - 針對 **Username**（使用者名稱）屬性：
     - 如果您選取 **Operator**（運算子） > **Contains**（包含），請從 **Value**（值）清單中選取或搜尋使用者名稱。若要開始搜索，請開始輸入使用者名稱。您可以從清單中選取一或多個使用者名稱。



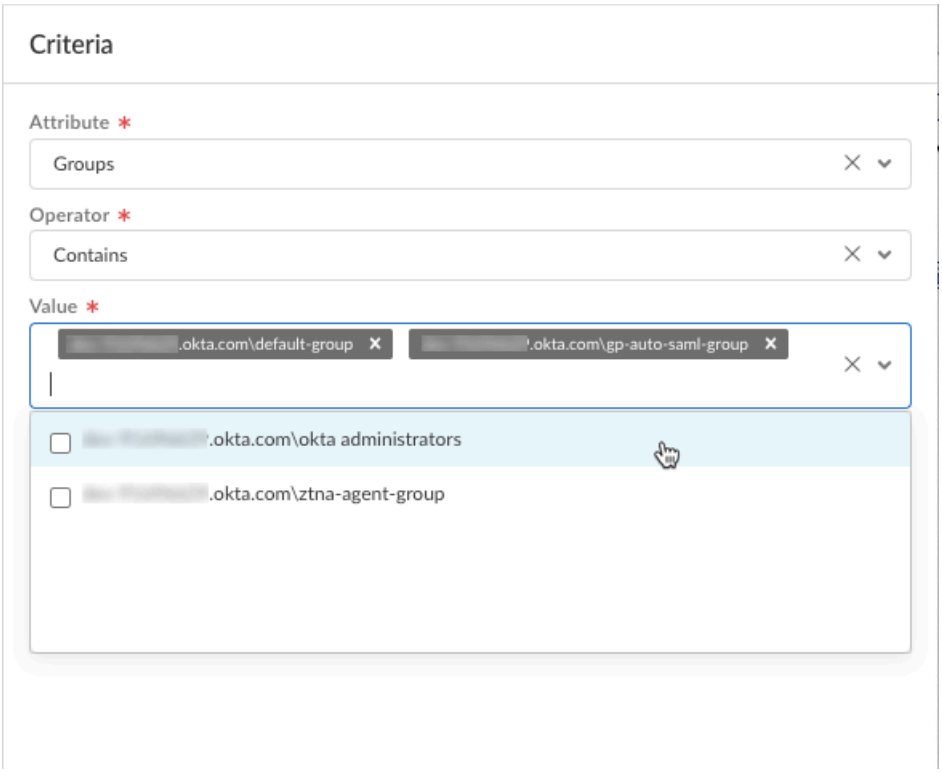

 ©2025 Palo Alto Networks, Inc.

- 如果您選取 **Operator**（運算子） > **Equals**（等於），請從 **Value**（值）清單中選取或搜尋使用者名稱。若要開始搜索，請開始輸入使用者名稱。您可以從清單中選取一個使用者名稱。

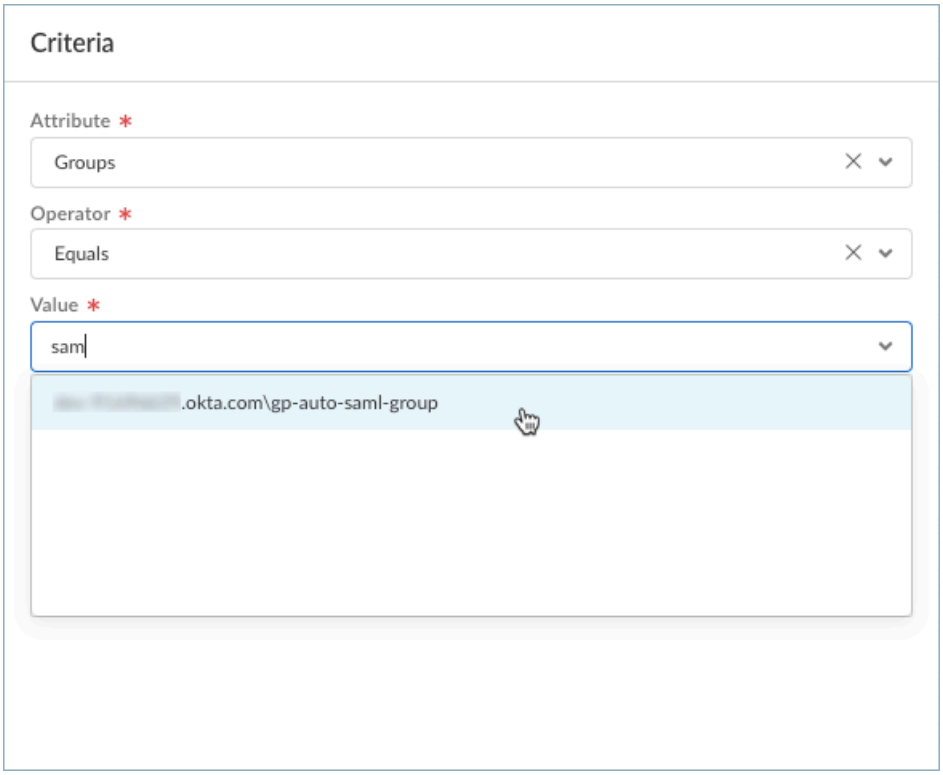



- 針對 **Groups**（群組）屬性：
  - 如果您選取 **Operator**（運算子） > **Contains**（包含），請從 **Value**（值）清單中選取或搜尋群組。若要開始搜索，請開始輸入群組名稱。您可以從清單中選取一或多個群組。

 ©2025 Palo Alto Networks, Inc.



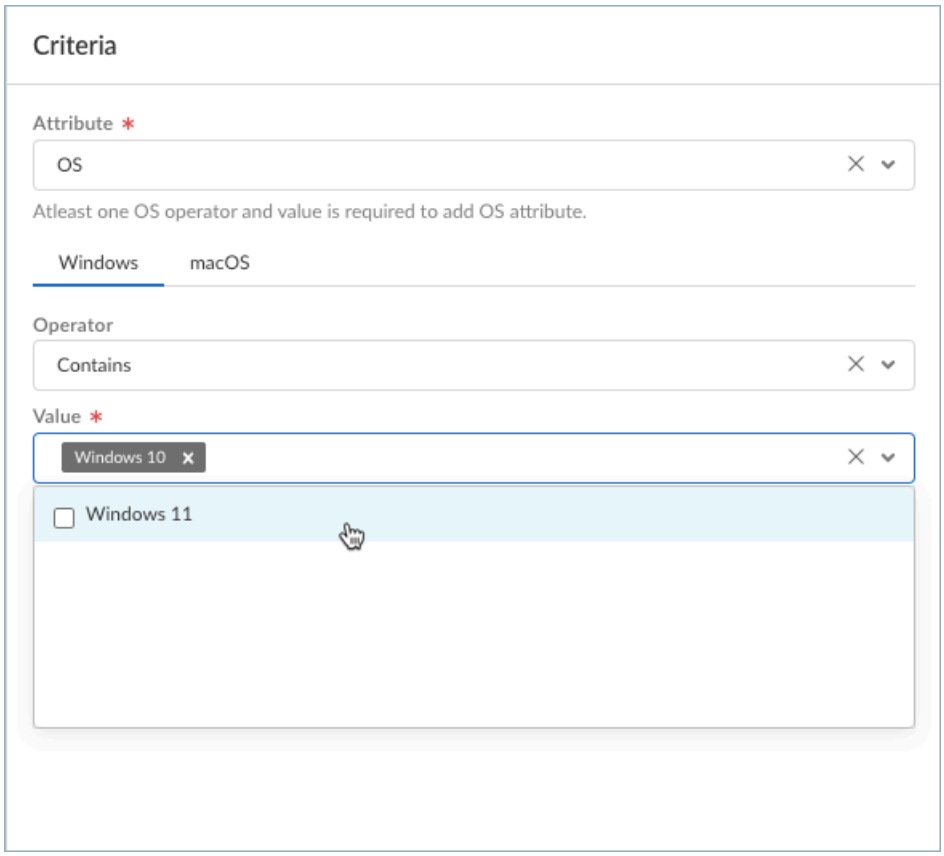

- 如果您選取 **Operator**（運算子） > **Equals**（等於），請從 **Value**（值）清單中選取或搜尋群組。若要開始搜索，請開始輸入群組名稱。您可以從清單中選取一個群組。




- 針對 **OS**（作業系統）屬性，選取作業系統類型（**Windows** 或 **macOS**）。然後：

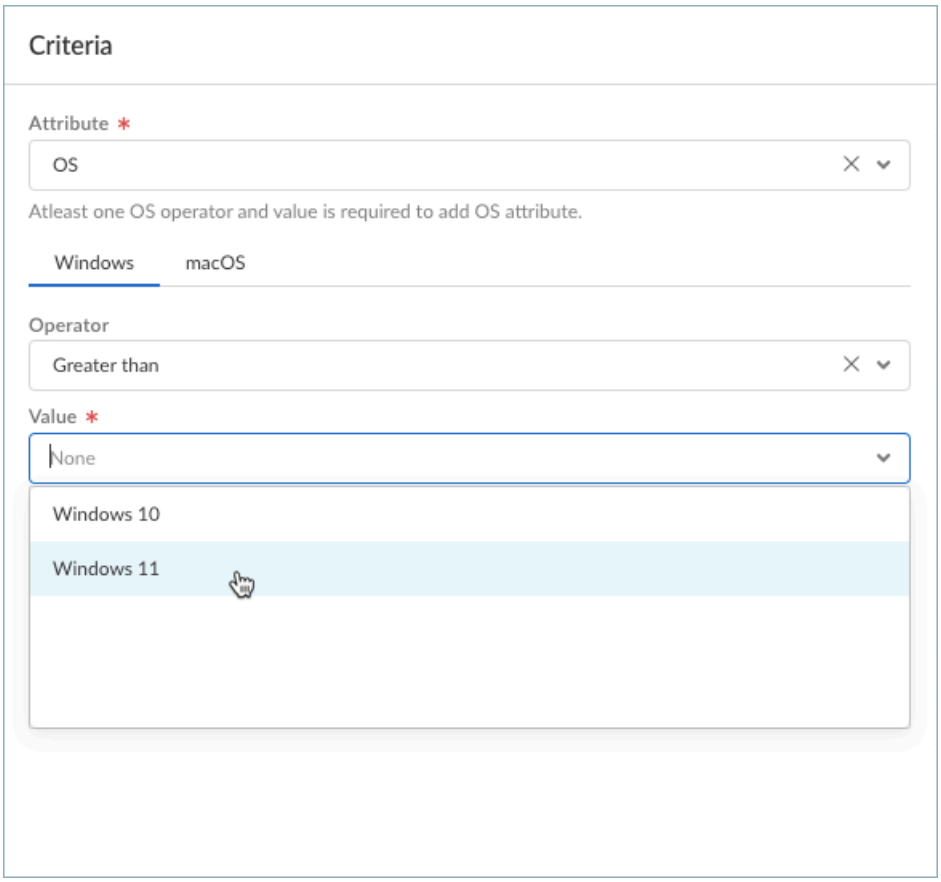
 ©2025 Palo Alto Networks, Inc.

- 如果您選取 **Operator**（運算子） > **Contains**（包含），請從 **Value**（值）清單中搜尋或選取一或多個作業系統版本。若要開始搜索，請開始輸入作業系統和版本。您可以從清單中選取一或多個作業系統版本。




- 如果您選取 **Greater than**（大於）或 **Less than**（小於）運算子，請從 **Value**（值）清單中搜尋或選取作業系統版本。若要開始搜索，請開始輸入作業系統和版本。您可以從清單中選取一個作業系統版本。


©2025 Palo Alto Networks, Inc.

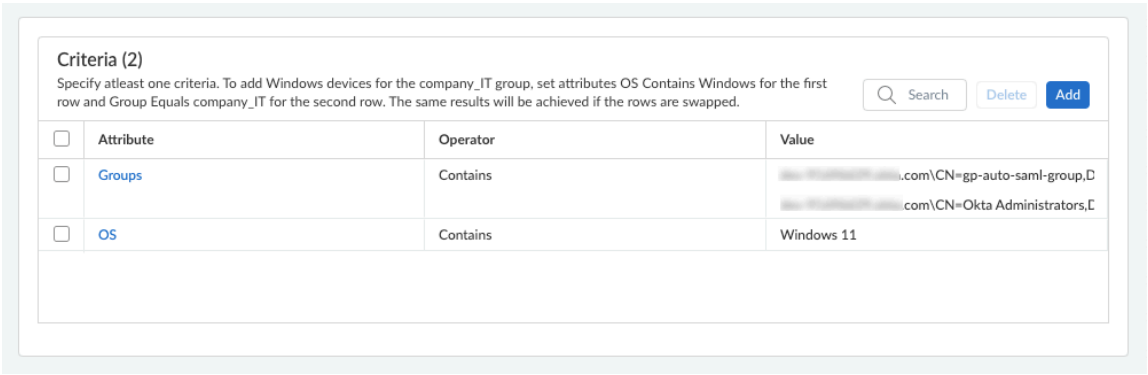



3. 視需要 **Add**（新增） 更多準則。您最多可為每個環指定三個準則。

   您一次只能為每個環使用一個屬性。使用屬性新增準則之後，屬性就不再顯示於 **Attribute**（屬性）下拉式清單中。

   新增準則之後，準則會顯示在 [Ring Criteria（環準則）] 頁面的 **Criteria**（準則）表格中。當 Prisma Access 評估準則時，使用邏輯 OR 運算子評估相同儲存格中列出的值，而使用邏輯 AND 運算子評估列之間的屬性和值。

   例如，下圖中的準則將會比對屬於 **gp-auto-saml-group** 或 **Okta Administrators** 群組且執行 Windows 11 作業系統的裝置。



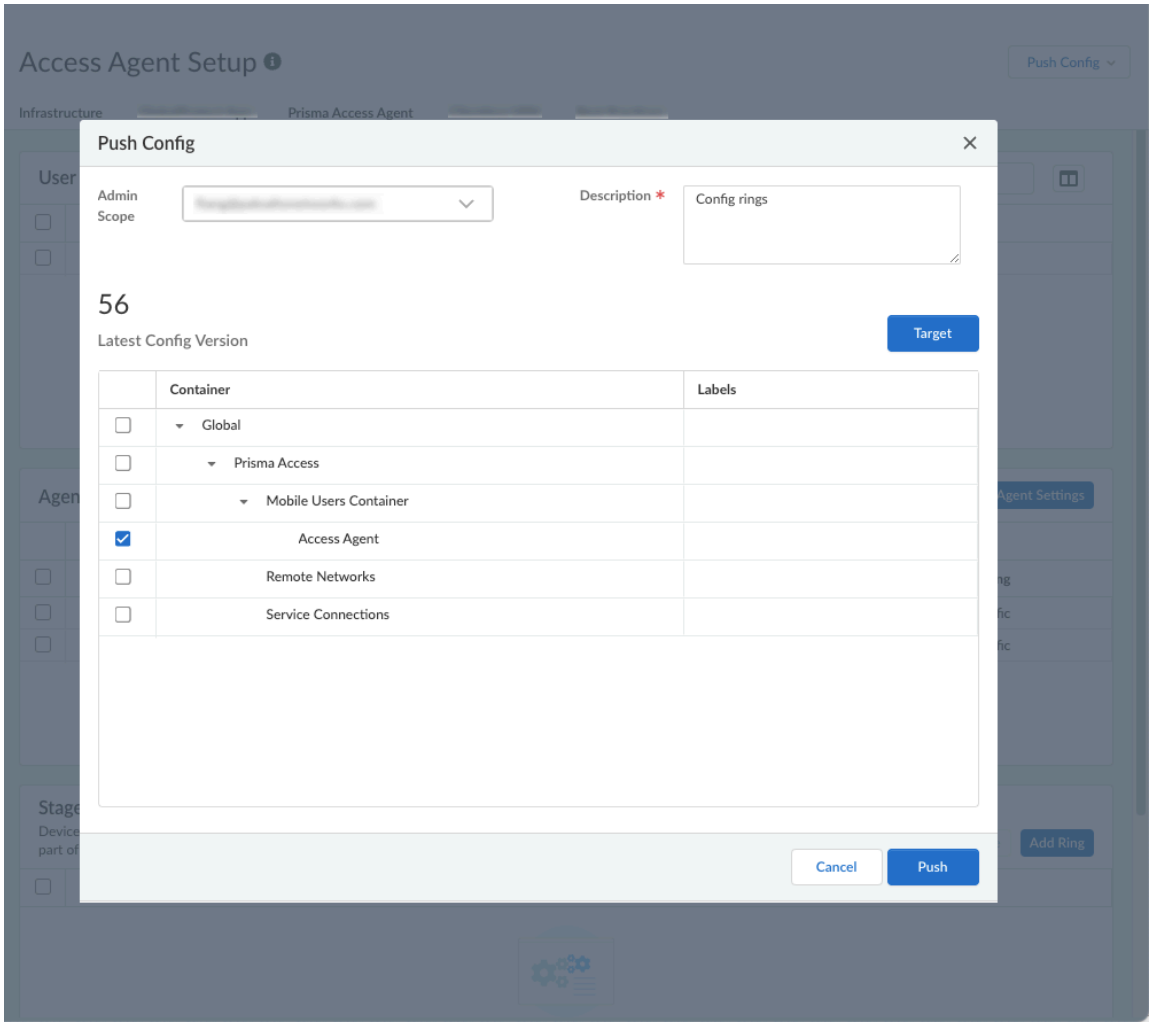

4. **Save**（儲存）環準則。

**STEP 6 |** 若要建立更多環，請重複步驟 2 至 5。您總共可以建立五個環（環 0 至環 4）。

 ©2025 Palo Alto Networks, Inc.

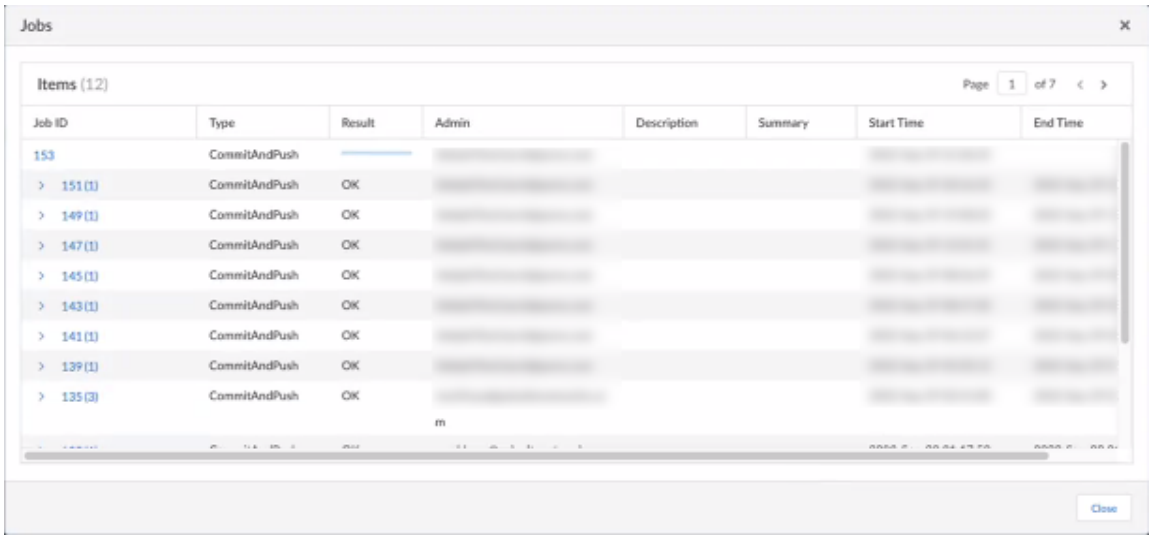
**STEP 7 |** 將設定推送至 Prisma Access。

1. 選取 **Push Config**（推送設定） > **Push**（推送）。
2. 輸入作業的 **Description**（說明）。
3. 選取 **Global**（全域） > **Prisma Access** > **Mobile Users**（行動使用者） > **Access Agent**（存取代理程式）容器，然後按一下 **Push**（推送）。




4. 等待作業完成，然後 **Close**（關閉）[Jobs（作業）] 對話方塊。

 ©2025 Palo Alto Networks, Inc.




**STEP 8 |** 您可以在 Strata Cloud Manager 中的 **Manage**（管理） > **Prisma Access Agent**（**Prisma Access** 代理程式）中監控分階段推出 。

# 為 Prisma Access Agents 設定一般全域設定

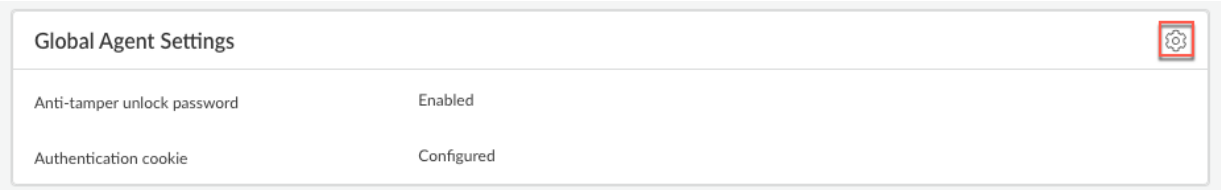
| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Prisma Access 授權，具有行動使用者訂閱<br>❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ 角色：超級使用者 |

您可以自訂可套用至所有端點的 Prisma Access 代理程式的全域代理程式設定。

一般全域代理程式設定包括設定防篡改功能，以防止使用者篡改 Prisma Access 代理程式，例如從一般使用者的裝置中將其解除安裝。此外，您也可以設定驗證覆寫設定、非使用狀態逾時設定，以及封鎖已隔離裝置的登入。

**STEP 1 |** 從 Strata Cloud Manager 中，選取 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Access Agent**（存取代理程式） > **Prisma Access Agent**（**Prisma Access** 代理程式）。

**STEP 2 |** 編輯 **Global Agent Settings**（全域代理程式設定）。




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 選取 **General**（一般）。

**STEP 4 |** 設定防篡改解鎖密碼。

您可以透過啟用防篡改功能來保護 Prisma Access 代理程式，該功能可防止任何未經授權的使用者篡改 Prisma Access 代理程式。防篡改功能可以保護端點上的以下 Prisma Access 代理程式資源：Prisma Access 代理程式資料夾和檔案—未經授權的使用者無法刪除或重新命名任何與 Prisma Access 代理程式相關的檔案和資料夾。Prisma Access 代理程式服務和主機資訊設定檔 (HIP) 程序—未經授權的使用者無法停止任何與 Prisma Access 代理程式相關的服務和 HIP 程序。HIP 程序會收集有關執行 Prisma Access 代理程式之主機的資訊，並將主機資訊提交給 Prisma Access 進行檢查。如果使用者嘗試停止程序，則必須提供防篡改解鎖密碼。Prisma Access 代理程式登錄機碼（Windows 上）或 .plist 檔案（macOS上）—未經授權的使用者無法刪除或更新 Prisma Access 代理程式的 Windows 登錄機碼戶 .plist 檔案。PACli 命令列介面—未經授權的使用者無法使用 PACli 命令列介面停用 Prisma Access 代理程式或防篡改功能。需要在命令列執行特定動作以進行疑難排解的管理員和授權使用者，必須在出現提示時提供防篡改解鎖（監督人）密碼。

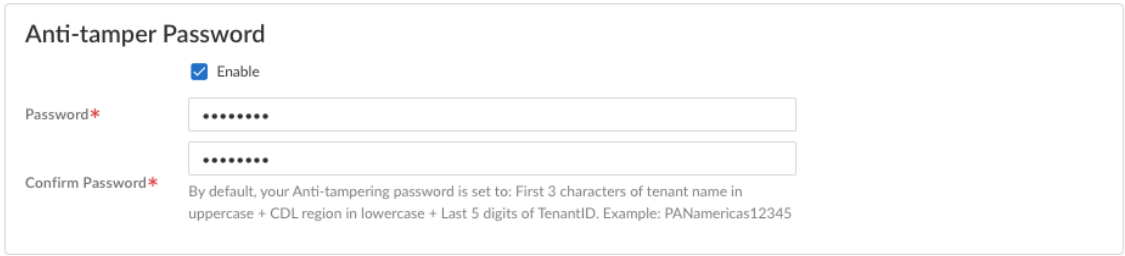
若要解鎖防篡改功能以針對 Prisma Access 代理程式進行疑難排解，您需要設定防篡改解鎖密碼（也稱為監督人密碼）。

1. 防篡改解鎖密碼

   如果未啟用防篡改密碼，則不會指派密碼，且使用者可以在 Prisma Access 代理程式命令列出現提示時輸入任何密碼（包括空白密碼）。

   如果您在啟用防篡改密碼之後將其停用，使用者可以在代理程式上執行特定 PACli 命令，例如 **`pacli disable`**、**`pacli hip status`**、**`pacli protect disable`** 和 **`pacli switchto GlobalProtect`** 命令，不需提供監督人密碼。他們只需要在提示輸入密碼時按 **Enter** 鍵即可。

2. 輸入 **Password**（密碼），然後藉由重新輸入密碼來 **Confirm Password**（確認密碼）。密碼必須至少包含 8 個英數字元。

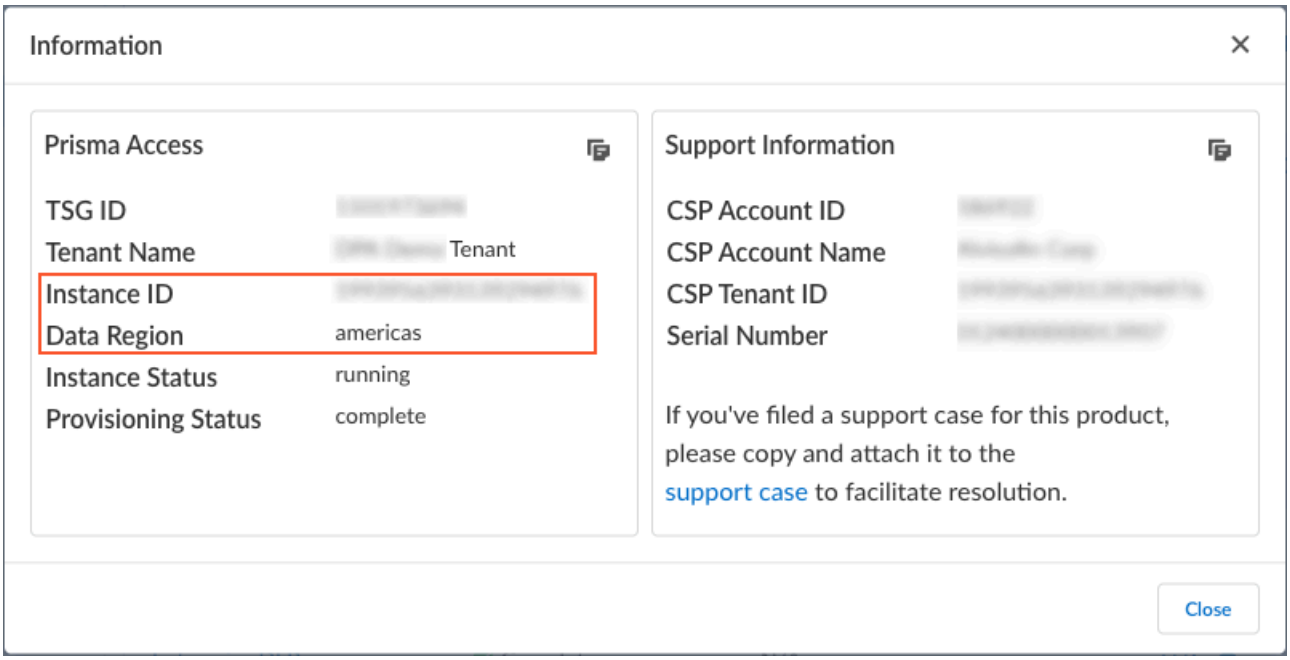



   如果您未提供密碼，則將使用預設密碼。依預設，防篡改密碼是設定為 Prisma Access 租用戶名稱的前三個字元（大寫），加上 Prisma Access **Data Region**（資料區


©2025 Palo Alto Networks, Inc.

域）（小寫），加上 Prisma Access **Instance ID**（執行個體 **ID**）的最後五個數字，例如：**PANamericas56789**。

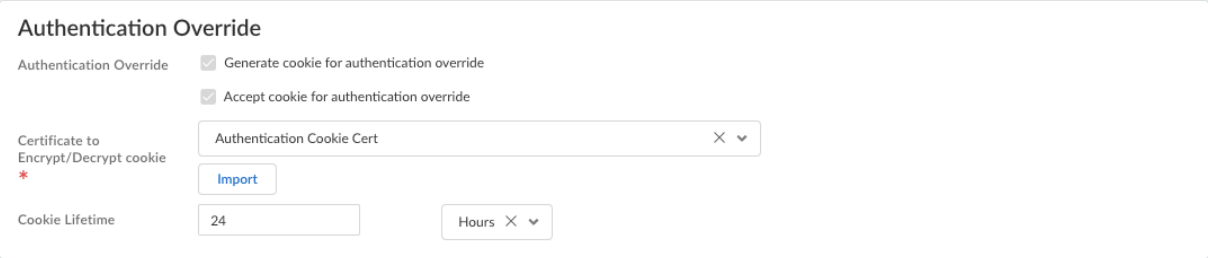
您可以藉由以下方式取得 Prisma Access **Instance ID**（執行個體 **ID**）和 **Data Region**（資料區域）：選取 **Settings**（設定） > **Tenants**（租用戶） > **<your_tenant>**，然後選取 Prisma Access 序號旁邊的 **View Support Info**（檢視支援資訊）工具提示。




若要為您的代理程式提供更高層級的安全性，請設定新的防篡改解鎖密碼以覆寫預設密碼，因為預設密碼可能不是最安全的。


©2025 Palo Alto Networks, Inc.

**STEP 5 |** 設定 **Authentication Override**（驗證覆寫）設定以允許 Prisma Access 產生和接受安全、加密的 Cookie 來驗證使用者。驗證覆寫讓使用者僅需在指定 **Cookie Lifetime**（**Cookie** 生命週期）期間提供登入認證一次。




- **Generate cookie for authentication override**（為驗證取代產生 **cookie**）—啟用 Prisma Access 以產生加密、特定端點的 Cookie 並簽發驗證 Cookie 至端點。
- **Accept cookie for authentication override**（接受用於驗證覆寫的 **Cookie**）—啟用 Prisma Access 以透過有效的加密 Cookie 驗證使用者。應用程式提供有效的 Cookie 後，Prisma Access 可驗證原始由 Prisma Access 加密的 Cookie、解密 Cookie，接著驗證使用者。
- **Certificate to Encrypt/Decrypt Cookie**（用於加密/解密 **Cookie** 的憑證）—選取 RSA 憑證，以用於加密與解密 Cookie。
- **Cookie Lifetime**（**Cookie** 存留時間）—指定 Cookie 有效的小時數、天數或週數（預設為 24 小時）。小時範圍為 1 至 72；週範圍為 1 至 52；天數範圍為 1 至 365。Cookie 到期後，使用者必須重新輸入其登入認證。然後，Prisma Access 會加密要傳送給代理程式的新 Cookie。此值可與您設定的 Cookie 存留時間一致或不同。

**STEP 6 |** 輸入 **Inactivity Logout**（非使用狀態登出）的分鐘數，指定閒置使用者從 Prisma Access 代理程式登出之前的時間量。

您可以使用非使用狀態登出期間來強制執行安全性政策，監控連線到 Prisma Access 時來自端點的流量，並快速登出非使用狀態 Prisma Access 代理程式工作階段。您可以執行更短的非使用狀態登出期間。如果在設定的時間段內，Prisma Access 代理程式沒有透過通道路由流量，或閘道未收到來自端點的 HIP 檢查，則使用者會登出 Prisma Access 代理程式。

**STEP 7 |** **Block Login for Quarantined Devices**（封鎖隔離裝置的登入）以防止 Prisma Access 代理程式使用者從隔離裝置登入。

如果使用者在此設定已啟用時嘗試從隔離裝置登入，則 Prisma Access 代理程式會通知使用者該設備已被隔離，使用者無法從該裝置登入。如果此設定未啟用，使用者會收到通知，但是能夠從該裝置登入。

**STEP 8 |** **Save**（儲存）您的設定。

# 為動態權限存取 Prisma Access Agent 設定 HIP 通知

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Prisma Access 授權，具有行動使用者訂閱 |


©2025 Palo Alto Networks, Inc.

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| | ❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ 角色：超級使用者 |

在 [Edit Global Agent Settings（編輯全域代理程式設定）] 頁面的 **HIP Notifications**（**HIP** 通知）頁籤中，您可以建立主機資訊設定檔通知、建立和管理 HIP 物件，以及建立和管理套用至所有端點的 Prisma Access 代理程式的 HIP 設定檔。

Prisma Access 代理程式會收集有關其執行之主機的資訊，並在成功連線後將此主機資訊提交至 Prisma Access 位置（閘道）。閘道會將 Prisma Access 代理程式提交的此原始主機資訊與您已定義的任何 HIP 物件和 HIP 設定檔相比對。如果發現相符，它會在 HIP 比對日誌中產生項目。此外，如果在原則規則中發現 HIP 設定檔的相符項，則會強制執行對應的安全原則。

當應用程式連線到閘道時會執行 HIP 檢查，在 Prisma Access 代理程式連線的情況下還會每小時執行一次後續檢查。如果之前的 HIP 檢查已變更，Prisma Access 代理程式可以要求更新的 HIP 報告。只有最新 HIP 報告保留在每個端點的閘道上。

針對原則強制執行使用主機訊息設定檔會啟用精細安全性，其可確保在獲得允許存取您的網路資源之前，存取您的關鍵資源的遠端主機能夠受到適當維護並嚴格遵守您的安全性標準。例如，在允許存取最敏感的資料系統之前，您可能需要確定存取資料的主機是否已在其硬碟上啟用加密。如果端點系統已啟用加密，您可以建立僅允許存取應用程式的安全性規則來強制執行此原則。

此外，對於不符合此規則的端點，您可以建立通知訊息，警示使用者為何遭到拒絕存取。您也可以提供位置的連結，他們可在其中存取遺失的加密軟體的安裝程式。若要允許使用者存取該檔案共用，您必須建立對應的安全性規則，允許具有特定 HIP 設定檔相符項的主機存取特定共用。

您可以完成下列工作：

- 為動態權限存取 Prisma Access Agent 建立 HIP 通知
- 為動態權限存取 Prisma Access Agent 建立和管理 HIP 物件
- 為動態權限存取 Prisma Access Agent 建立和管理 HIP 設定檔

## 為動態權限存取 **Prisma Access Agent** 建立 **HIP** 通知

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Prisma Access 授權，具有行動使用者訂閱<br>❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ 角色：超級使用者 |

您可以定義當使用 HIP 設定檔強制執行安全性規則時，一般使用者會看到的通知訊息。

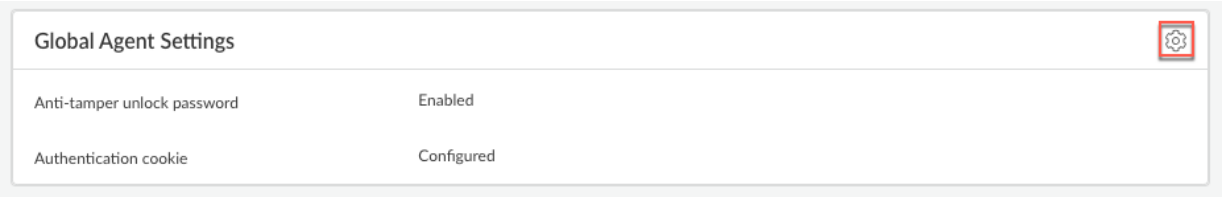

©2025 Palo Alto Networks, Inc.

決定當使用者的設定與政策中的 HIP 設定檔相符或不相符時，是否顯示通知訊息，主要取決於您的政策和 HIP 相符（或不相符）對使用者有何意義。也就是說，相符是否表示他們獲得授與對您的網路資源的完全存取權，還是表示由於不合規問題，他們的存取權受到限制？

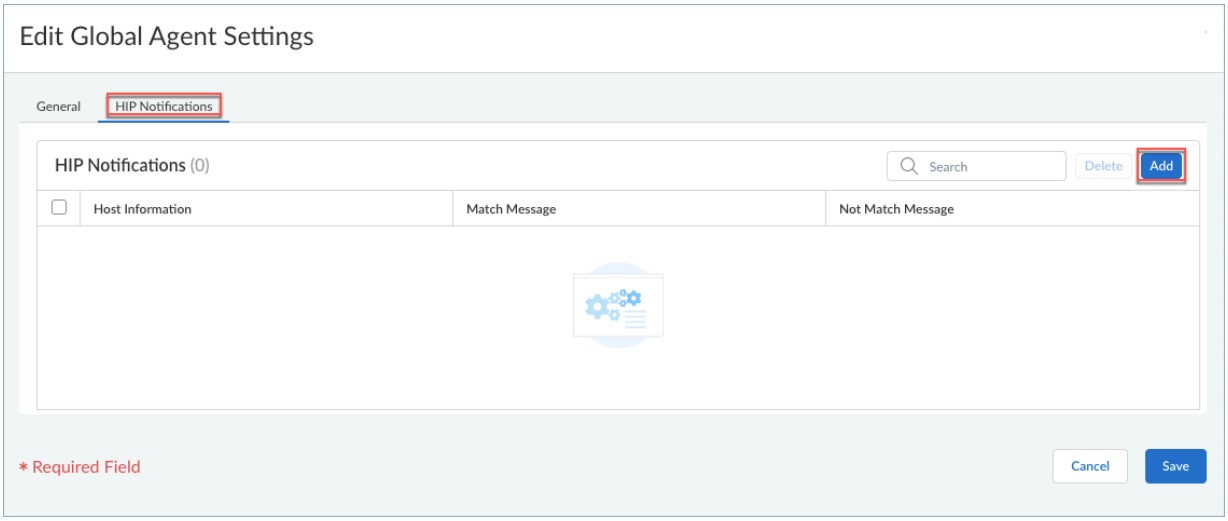
例如，假設您所建立的 HIP 設定檔，會在所需的公司防毒與反間諜軟體套件未安裝時相符。您可以為符合 HIP 設定檔的使用者建立 HIP 通知訊息，告訴他們需要安裝軟體。或者，如果在已安裝那些相同應用程式的情況下，您的 HIP 設定檔相符，則您可能需要為與設定檔不相符的使用者建立訊息。

**STEP 1 |** 從 Strata Cloud Manager 中，選取 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Access Agent**（存取代理程式） > **Prisma Access Agent**（**Prisma Access** 代理程式）。

**STEP 2 |** **Edit**（編輯）**Global Agent Settings**（全域代理程式設定）。



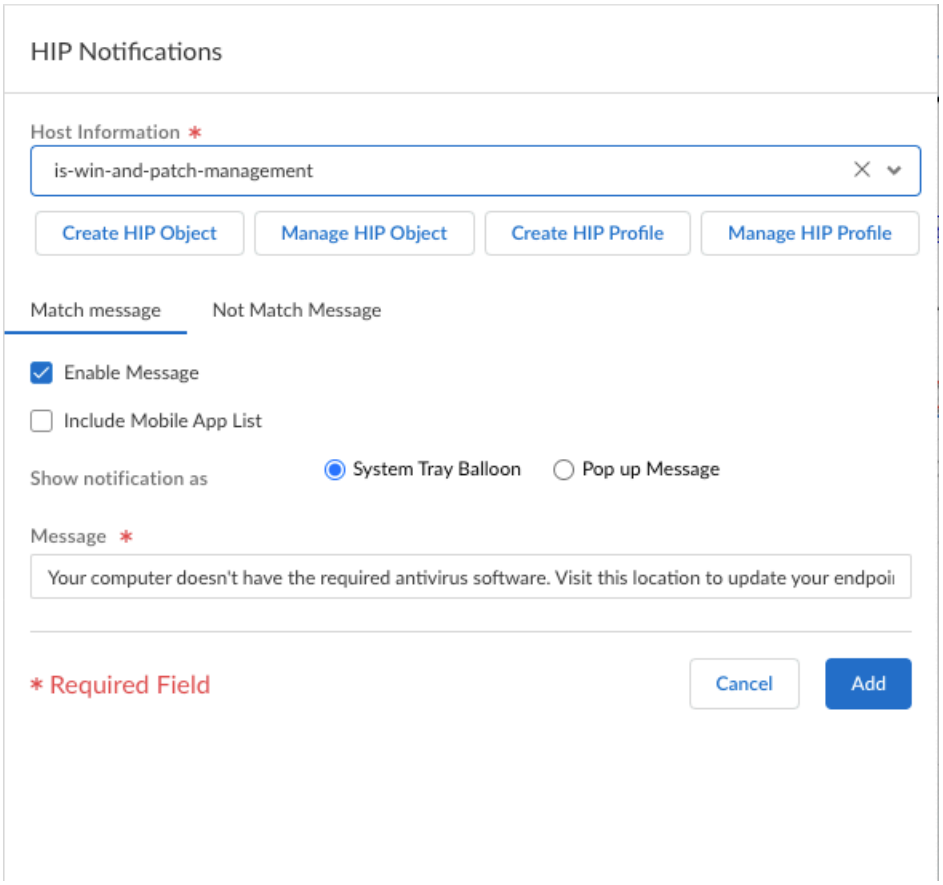

**STEP 3 |** 選取 **HIP Notifications**（**HIP** 通知），然後按一下 **Add**（新增）。





©2025 Palo Alto Networks, Inc.

**STEP 4 |** 從 **Host Information**（主機資訊）下拉式清單選取套用此訊息的 HIP 設定檔。




如果沒有 HIP 設定檔，則需要建立 HIP 設定檔。

**STEP 5 |** 當對應的 HIP 設定檔已進行比對或未比對時，根據您是否要顯示此訊息，選取 **Match Message**（符合訊息）或 **Not Match Message**（不符合訊息）。在某些情況下，您可能需要根據您正在比對的物件與原則的目的，來為相符與非相符項目建立訊息。

**STEP 6 |** 選取 **Enable Message**（啟用訊息），然後選取要將訊息顯示為 **System Tray Balloon**（系統匣球形文字說明）或 **Pop Up Message**（快顯訊息）。

**STEP 7 |** 輸入您的 **Message**（訊息）文字，然後按一下 **Add**（新增）。

**STEP 8 |** 針對每個要定義的訊息重複此程序。

## 為動態權限存取 Prisma Access Agent 建立和管理 HIP 物件

| 這可在何處使用？ | 我需要哪些內容？ |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Prisma Access 授權，具有行動使用者訂閱<br>❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置 |


©2025 Palo Alto Networks, Inc.

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| | ❑ 角色：超級使用者 |

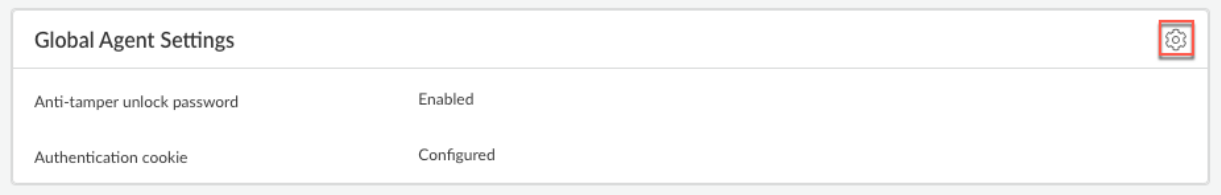
您可以透過在 Prisma Access 開道上建立 HIP 物件和 HIP 設定檔，定義想要監控或用於政策強制執行的主機屬性。

HIP 物件包含比對準則，可用於篩選掉您針對 Prisma Access 代理程式所報告的原始資料強制執行原則時，所慣用的主機資訊。例如，雖然原始主機資料可能包含端點上安裝的數個防毒套件的相關資訊，但您可能只會使用一種您慣用的特定應用程式。在此情況中，您將建立 HIP 物件以符合您想要強制施行的特定應用程式。

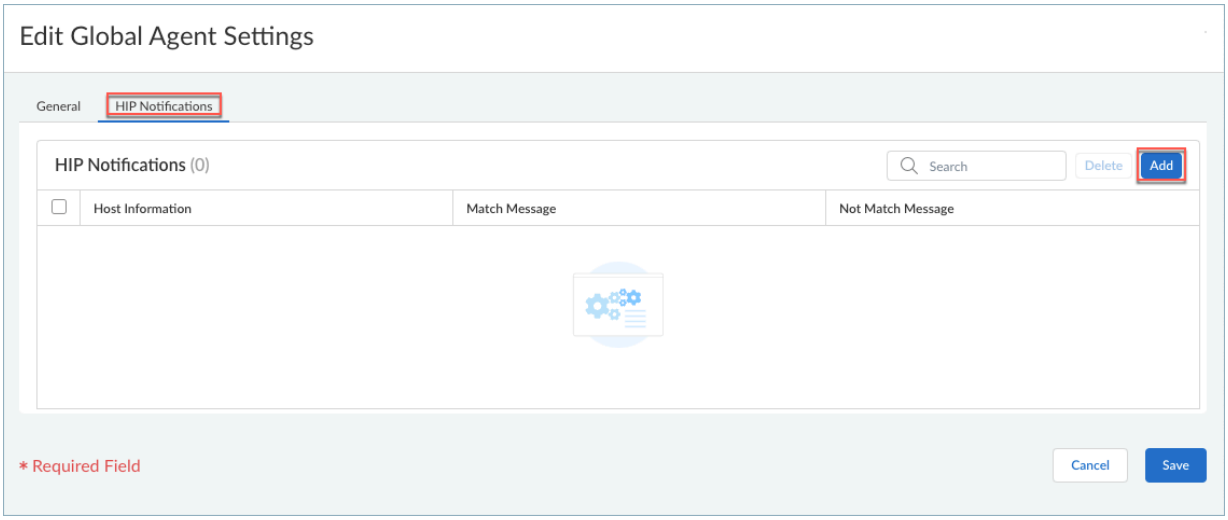
若要判斷需要的 HIP 物件，最好的方法是決定要如何使用收集的主機資訊來強制執行政策。請注意，HIP 物件本身只會建立封鎖，讓您建立在安全性政策中使用的 HIP 設定檔。因此，藉由比對單一項目，嘗試讓物件保持單純，例如，呈現特殊類型的必要軟體、特定網域中的成員資格，或特定作業系統。利用這種做法，您可以靈活建立極精細的 HIP 擴張政策。

**STEP 1 |** 從 Strata Cloud Manager 中，選取 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Access Agent**（存取代理程式） > **Prisma Access Agent**（**Prisma Access** 代理程式）。

**STEP 2 |** **Edit**（編輯）**Global Agent Settings**（全域代理程式設定）。



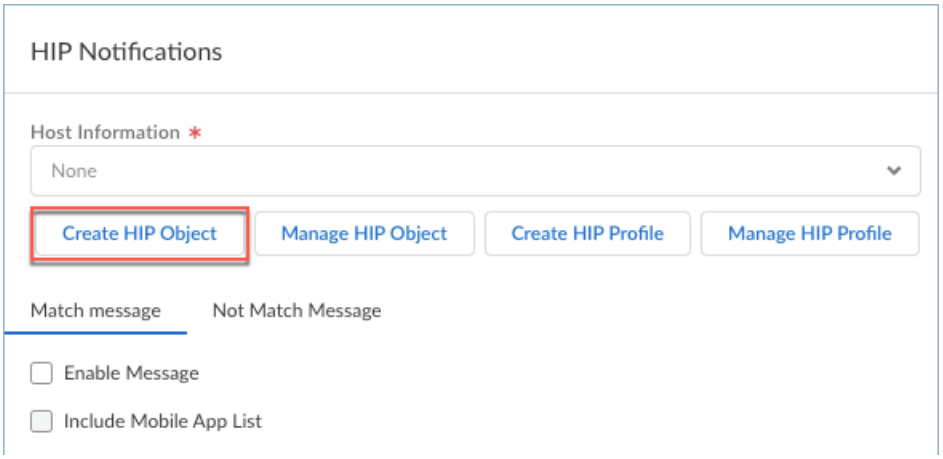

**STEP 3 |** 選取 **HIP Notifications**（**HIP** 通知），然後按一下 **Add**（新增）。





©2025 Palo Alto Networks, Inc.

**STEP 4 |** 按一下 **Create HIP Object**（建立 **HIP** 物件）。



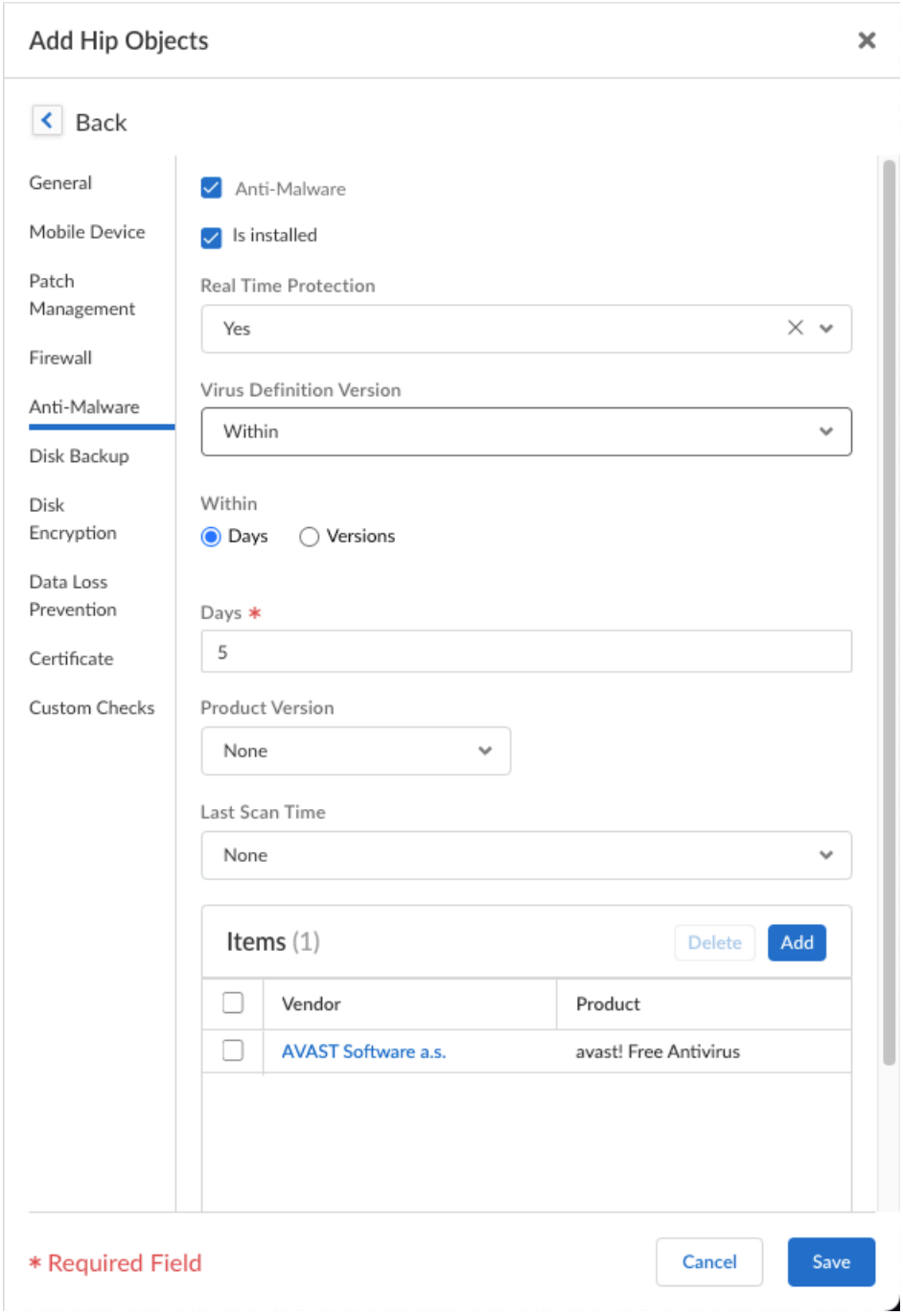

**STEP 5 |** 輸入物件的 **Name**（名稱）和 **Description**（說明）。


©2025 Palo Alto Networks, Inc.

**STEP 6 |** 針對您想要比對的主機資訊類別選取所對應的頁籤，並選取核取方塊來啟用要與類別比對的物件。

例如，若要建立尋找有關防毒或反間諜軟體資訊的物件，請選取 **Anti-Malware**（防惡意軟體）頁籤，然後選取 **Anti-Malware**（防惡意軟體）核取方塊來啟用對應欄位。完成欄位以定義所需比對準則。

例如，下圖顯示如果當端點已安裝 AVAST Free Antivirus 軟體應用程式、已啟用 **Real Time Protection**（即時保護），並且已在最近 5 天內更新惡意軟體定義時，建立要比對 HIP 物件的方法。




 ©2025 Palo Alto Networks, Inc.

針對您要在此物件中比對的每個類別重複此步驟。如需詳細資訊，請參閱 表格：資料收集類別。

**STEP 7 |** **Save**（儲存）並 **Add**（新增）您的 HIP 物件。

**STEP 8 |** 若要管理您的 HIP 物件，您可以從 HIP 通知表格選取現有物件，或按一下 [Edit Global Agent Settings（編輯全域代理程式設定）] 頁面中的 **Add**（新增）以開啟 HIP 通知視窗。

從該處按一下 **Manage HIP Object**（管理 **HIP** 物件）以檢視您設定之 HIP 物件的清單。您可以選取 HIP 物件，然後 **Delete**（刪除）、**Clone**（複製）或 **Move**（移動）該物件。

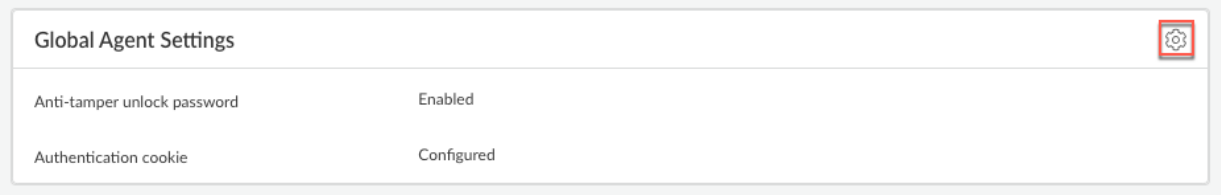
## 為動態權限存取 Prisma Access Agent 建立和管理 HIP 設定檔

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Prisma Access 授權，具有行動使用者訂閱<br>❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ 角色：超級使用者 |

HIP 設定檔是一起評估的主機資訊設定檔物件集合，適用於監控或安全性政策強制執行。建立 HIP 設定檔時，您可以使用布林邏輯來結合先前建立的 HIP 物件和 HIP 設定檔，如此在針對導出的 HIP 設定檔評估流量時，就會得到符合或不符合結果。如果有符合項，則將執行對應的原則規則。如果沒有符合項，則針對下一個規則，及使用任何其他原則比對準則來評估流量。

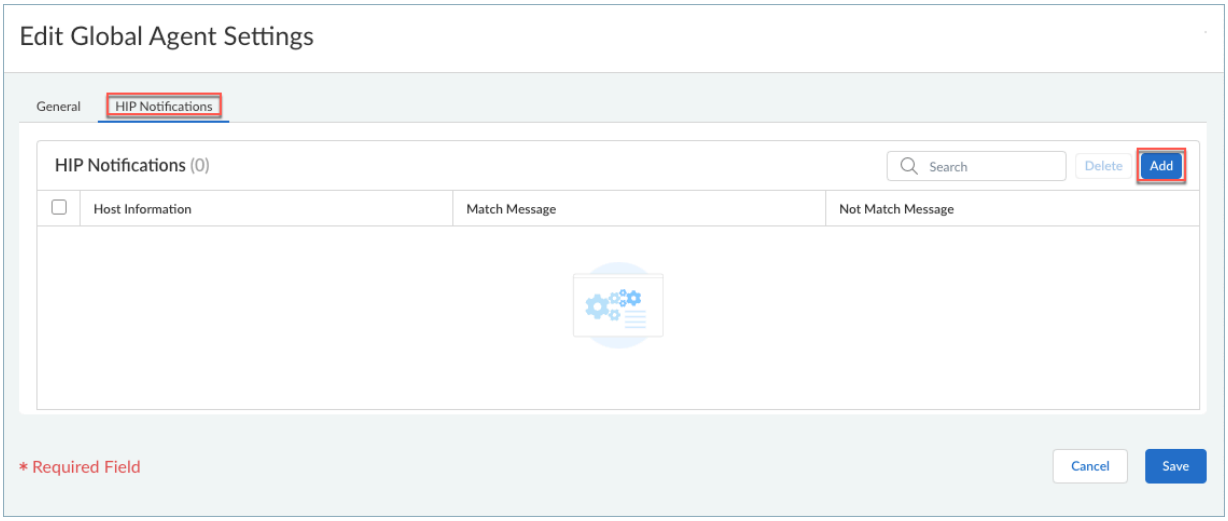
**STEP 1 |** 從 Strata Cloud Manager 中，選取 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Access Agent**（存取代理程式） > **Prisma Access Agent**（**Prisma Access** 代理程式）。

**STEP 2 |** **Edit**（編輯）**Global Agent Settings**（全域代理程式設定）。

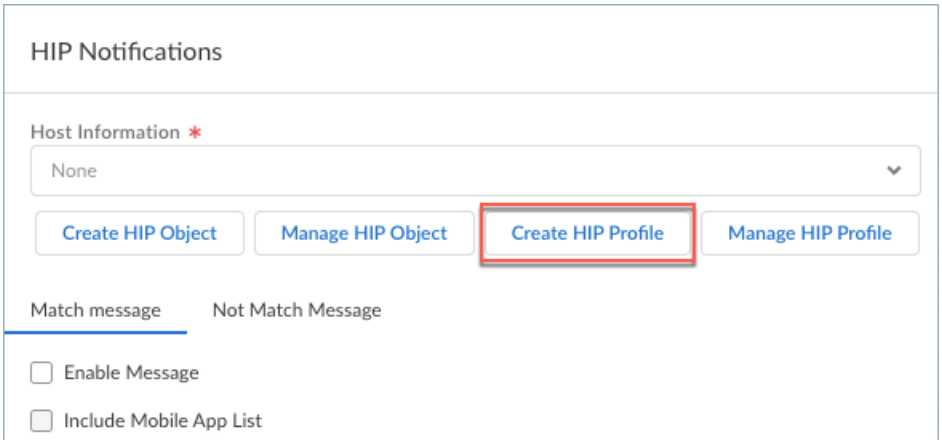



 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 選取 **HIP Notifications**（**HIP** 通知），然後按一下 **Add**（新增）。




**STEP 4 |** 按一下 **Create HIP Profile**（建立 **HIP** 設定檔）。




**STEP 5 |** 輸入 **Name**（名稱）和 **Description**（說明）來識別設定檔。

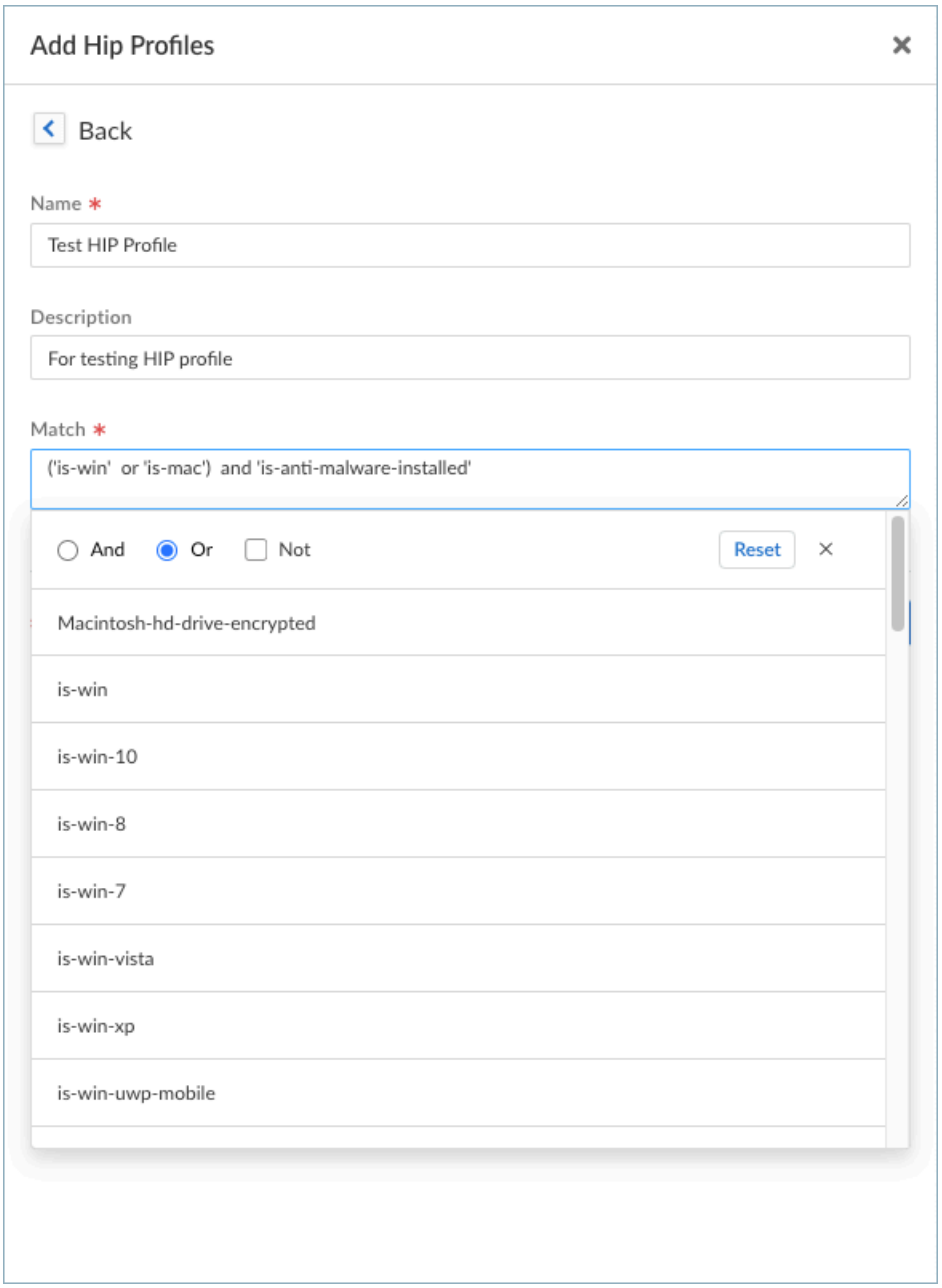
**STEP 6 |** 在 **Match**（比對）欄位內按一下以開啟 HIP 設定檔建立器。

1. 從清單中選取要用來作為比對規則的 HIP 物件或設定檔。
2. 選取布林值運算子（**And**、**And**）。若只有當物件中的準則對流量而言不為 true 時，方允許 HIP 設定檔將物件評估為符合，請先選取 **NOT** 核取方塊再新增物件。
3. 選取另一個 HIP 物件或設定檔，以根據第一個 HIP 物件進行評估。

**STEP 7 |** 為正在建立的設定檔繼續新增比對準則，確定在每次加法之間選取適當的布林運算子選項按鈕（**And** 或 **And**）；再次提醒您，請在適當的情況下使用 **Not** 核取方塊。HIP 設定檔的長度最多可以包含 2,048 個字元。


©2025 Palo Alto Networks, Inc.

**STEP 8 |** 建立複雜的布林值運算式時，則必須在**Match**（比對）文字方塊中，於適當的位置手動新增括號，確保使用所要的邏輯來評估 HIP 設定檔。




**STEP 9 |** **Save**（儲存）並 **Add**（新增）您的 HIP 設定檔。

**STEP 10 |** 若要管理您的 HIP 設定檔，您可以從 HIP 通知表格選取現有設定檔，或按一下 [Edit Global Agent Settings（編輯全域代理程式設定）] 頁面中的 **Add**（新增）以開啟 HIP 通知視窗。

從該處按一下 **Manage HIP Profile**（管理 **HIP** 設定檔）以檢視您設定之 HIP 設定檔的清單。您可以選取 HIP 設定檔，然後 **Delete**（刪除）、**Clone**（複製）或 **Move**（移動）該設定檔。您也可以從這裡 **Add**（新增） HIP 設定檔。


©2025 Palo Alto Networks, Inc.

# 推送 Prisma Access Agent 設定

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Prisma Access 授權，具有行動使用者訂閱<br>❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ 角色：超級使用者 |

在完成 Prisma Access Agent 設定或更新之後，必須將設定推送至 Prisma Access。

在推送提交之前建立至少一個專案，否則提交將失敗。

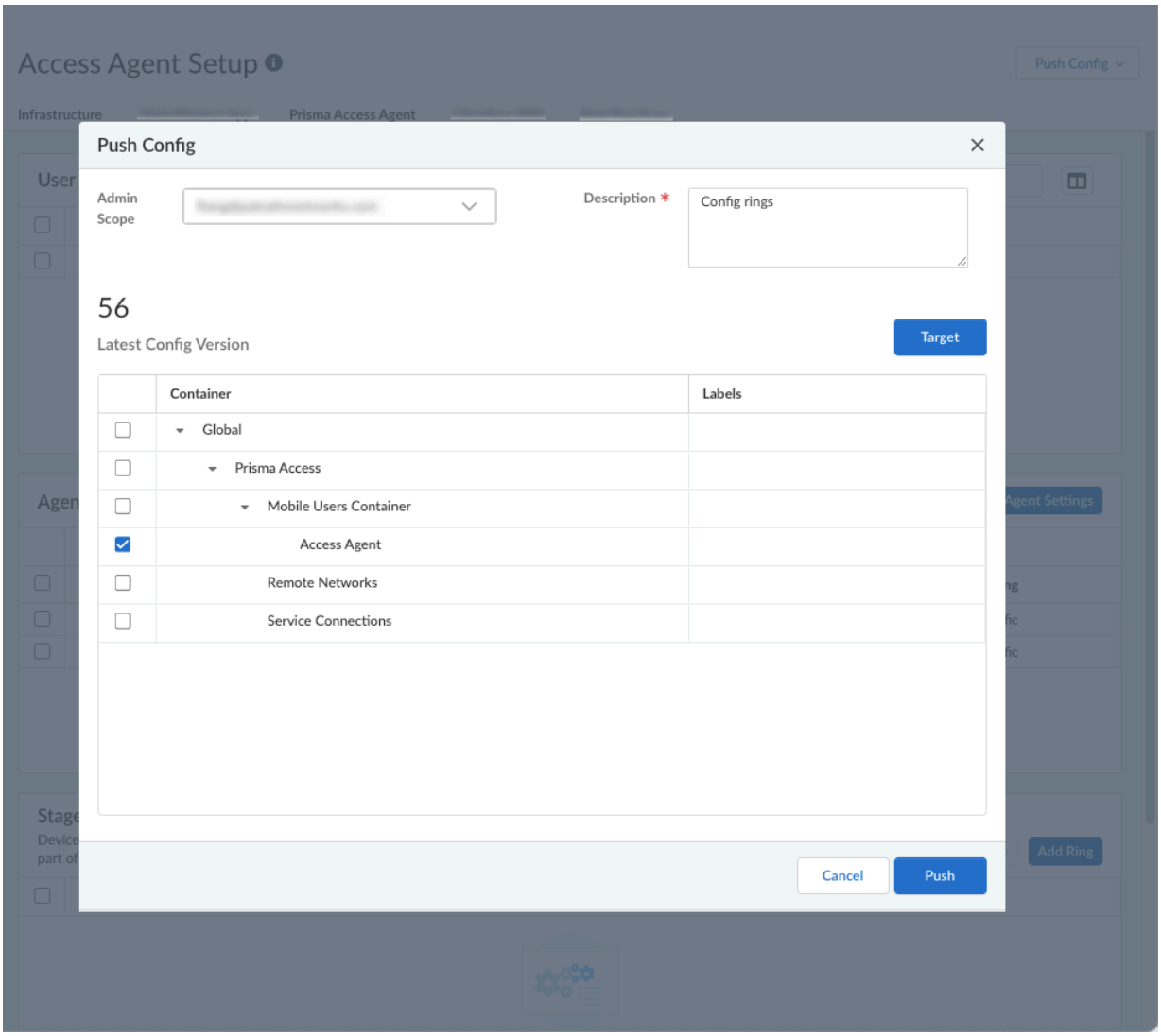
**STEP 1 |** 選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Access Agent**（存取用戶端）。

**STEP 2 |** 選取 **Push Config**（推送設定） > **Push**（推送）。

**STEP 3 |** 輸入工作的 **Description**（說明）。


©2025 Palo Alto Networks, Inc.

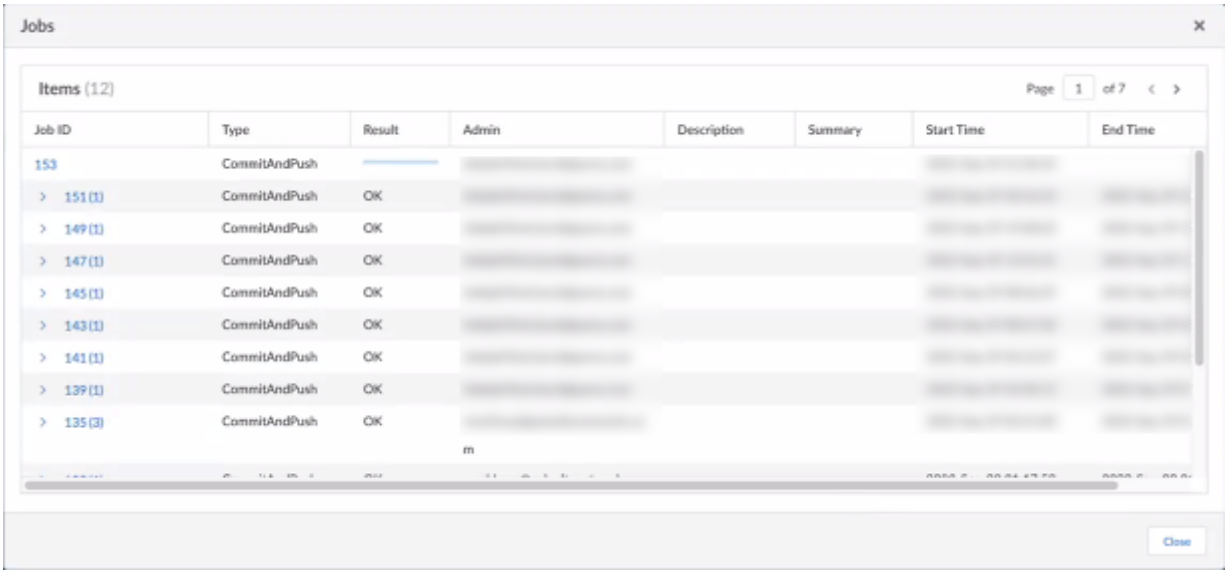
**STEP 4 |** 選取 **Global**（全域） > **Prisma Access** > **Mobile Users**（行動使用者） > **Access Agent**（存取代理程式）容器，然後按一下 **Push**（推送）。





©2025 Palo Alto Networks, Inc.

**STEP 5 |** 等待工作完成，然後 **Close**（關閉）工作對話方塊。




 ©2025 Palo Alto Networks, Inc.

# 下載已啟用動態權限存取的 Prisma Access Agent 套件

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Prisma Access 授權，具有行動使用者訂閱<br>❑ 角色：超級使用者 |

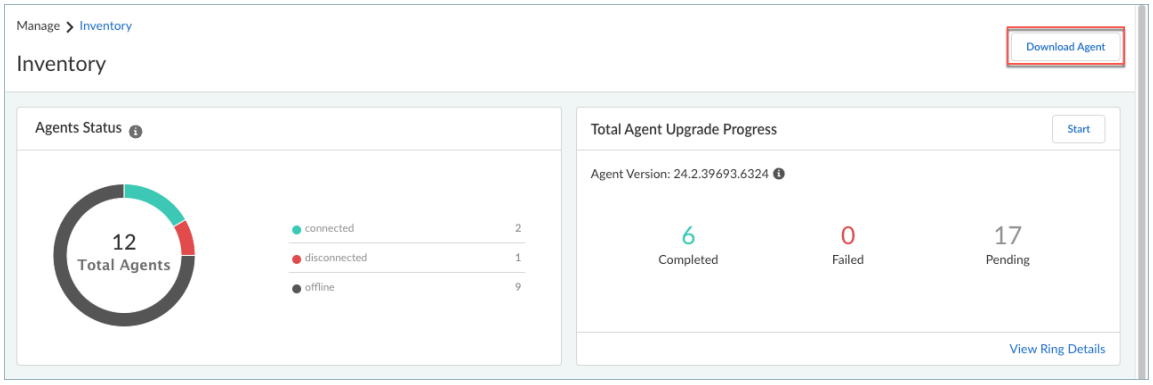
在設定了 Prisma Access Agent 和專案特定的 Prisma Access Agent 設定之後，您可以下載 Prisma Access Agent 套件，以便可以使其可供一般使用者下載和安裝。

此外，也請確保下載設定檔案。您的代理程式和專案特定的代理程式設定，以及 Prisma Access 租用戶 ID 和伺服器域，會儲存到 Prisma Access Agent 設定檔案。此設定檔案將在安裝和註冊 Prisma Access Agent 期間使用。


©2025 Palo Alto Networks, Inc.

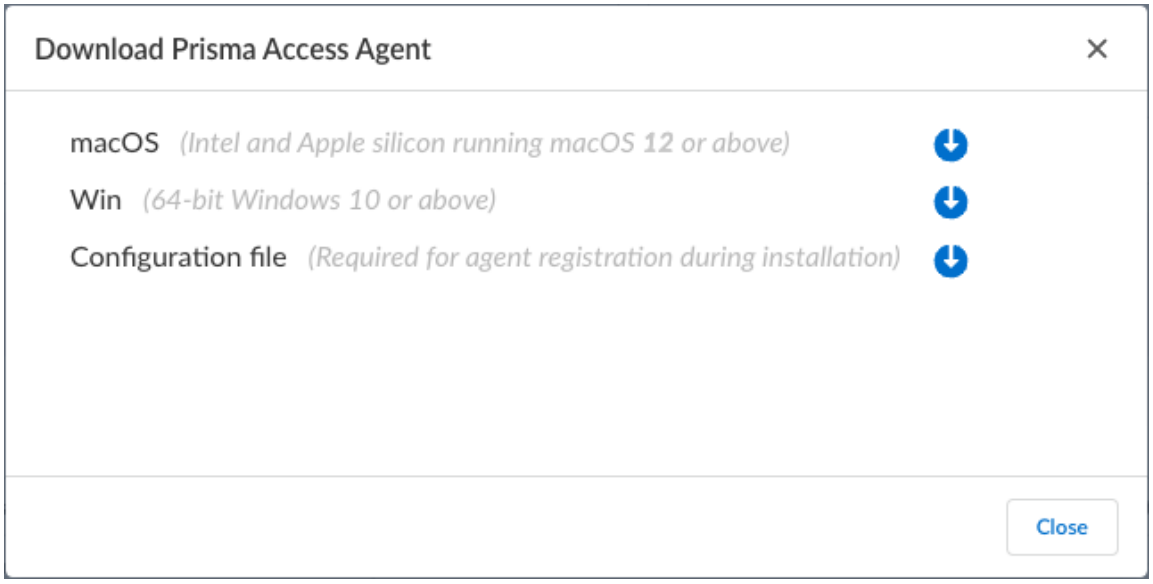
**STEP 1 |** 下載 Prisma Access Agent 套件和設定檔案。

1. 選取 **Manage**（管理） > **Prisma Access Agent** > **Inventory**（庫存）。
2. 按一下 **Download Agent**（下載代理程式）。




3. 按一下與要下載的項目對應的向下箭頭。

   確保您下載 **Configuration file**（設定檔案），因為它將在安裝和註冊 Prisma Access Agent 期間使用。




4. 將套件儲存到系統上的某個位置，然後 **Close**（關閉）[Download Agent（下載代理程式）] 對話方塊。

**STEP 2 |** 將套件上傳到組織網路中的中心位置，或分發套件，以便一般使用者可以下載並安裝 Prisma Access Agent。


©2025 Palo Alto Networks, Inc.

# 使用 Prisma Access Agent 存取您的專案

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access Agent | ❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ 網際網路存取 |

如果您的組織是 IT 或支援 IT 服務 (ITES) 公司，需要控制哪些使用者可以存取其客戶專案，則動態權限存取為您提供了一種無縫、安全且隔開的方式，讓您只能存取指派給您的那些專案。。

如果您的管理員已設定 Prisma Access 和 Prisma Access Agent 進行動態權限存取，您可以使用 Prisma Access Agent 存取和處理指派給您的專案。

在登入您的專案之後，您可以存取組織的網路、網路中的資源，或專案特定的軟體即服務應用程式。瞭解如何：

- 登入支援動態權限存取的 Prisma Access 代理程式
- 檢視您的連線狀態
- 變更支援動態權限存取的 Prisma Access 代理程式的偏好設定
- 連線到不同的 Prisma Access 位置
- 檢視應用程式通知

此外，如果您獲指派處理不同的專案，則可以切換到不同專案或將 Prisma Access 代理程式連線到不同的伺服器。

# 安裝 Prisma Access Agent。

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access Agent | ❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置（具有管理員權限）<br>❑ 網際網路存取 |

如果您的管理員未將 Prisma Access Agent 推送到您的裝置，您可以在 macOS 或 Windows 裝置上手動安裝 Prisma Access Agent。

*Prisma Access Agent* 和 *GlobalProtect* 應用程式可以共存於同一裝置上，但其中只有一個可以連線到 *Prisma Access*。如果您的裝置上還安裝並啟用了 *GlobalProtect* 應用程式，則 *Prisma Access Agent* 安裝將自動停用 *GlobalProtect* 應用程式。若要在安裝 *Prisma Access Agent* 之後使用 *GlobalProtect* 應用程式，您將需要切換到 GlobalProtect 應用程式。


©2025 Palo Alto Networks, Inc.

- macOS
- Windows

## 安裝 Prisma Access Agent (macOS)

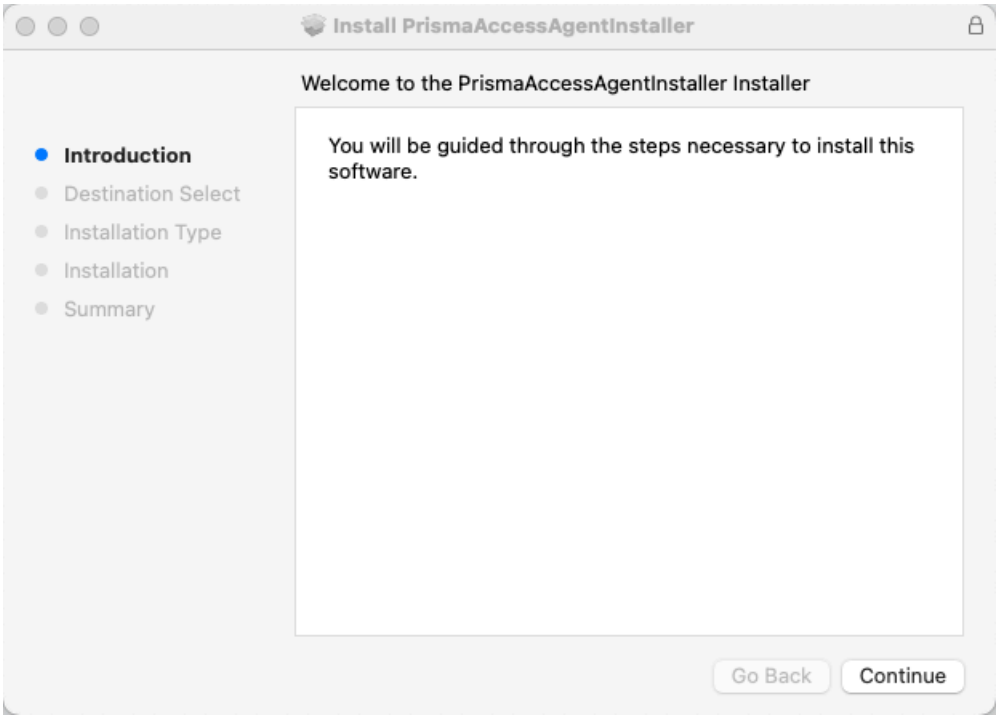
若要在您的 macOS 裝置上手動安裝 Prisma Access 代理程式：

**STEP 1 |** 取得您的管理員提供的 Prisma Access 代理程式套件。該套件名稱的格式如下：
`PrismaAccessAgentInstaller_<version>.pkg`

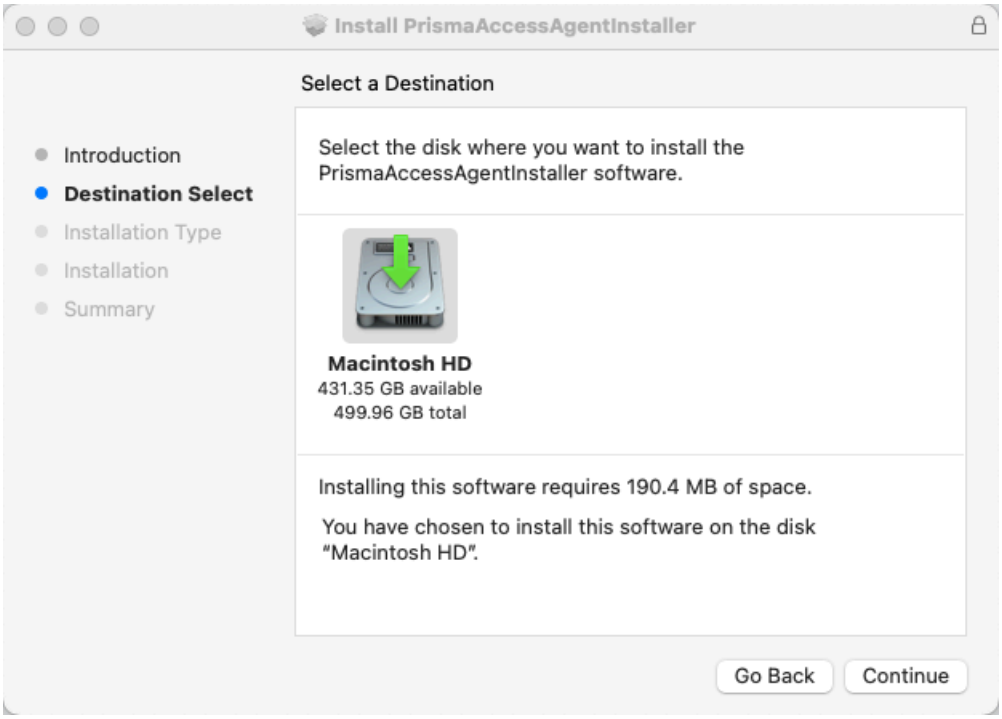

©2025 Palo Alto Networks, Inc.

**STEP 2 |** 在您的「下載」資料夾中（或您放置安裝套件的任何位置），開啟安裝套件並按照提示安裝 Prisma Access 代理程式。

1. 從安裝程式按一下 **Continue**（繼續）。

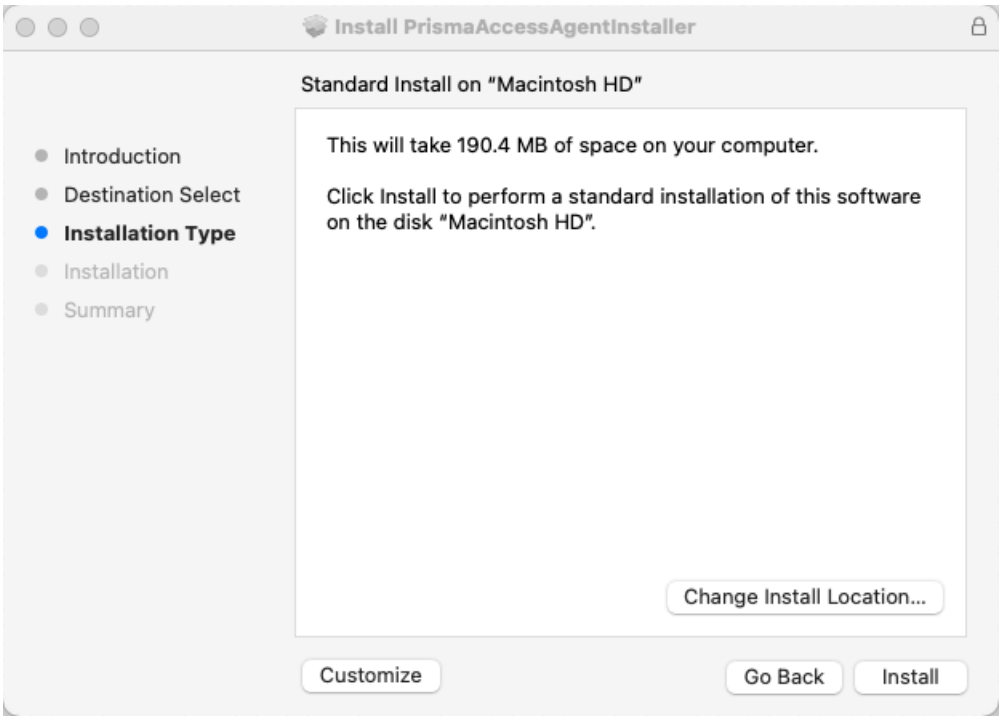



2. 選取 Prisma Access 代理程式的安裝資料夾，然後按一下 **Continue**（繼續）。




3. 檢閱 [Installation Type（安裝類型）] 頁面中的資訊，然後按一下 **Install**（安裝）。

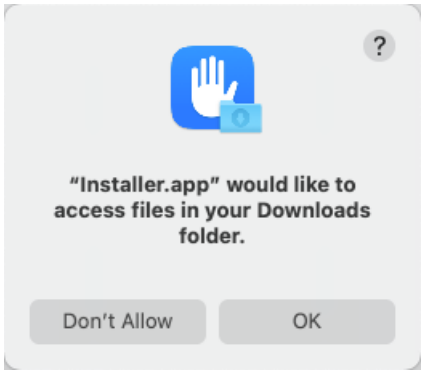

©2025 Palo Alto Networks, Inc.




4. 出現提示時，輸入您的 **User Name**（使用者名稱）和 **Password**（密碼），然後按一下 **Install Software**（安裝軟體）以開始安裝。

   或者，您可以使用 Touch ID（如果已啟用）來完成此步驟。

5. 當提示允許安裝程式存取您下載安裝套件所在資料夾中的檔案時，請按一下 **OK**（確定）。



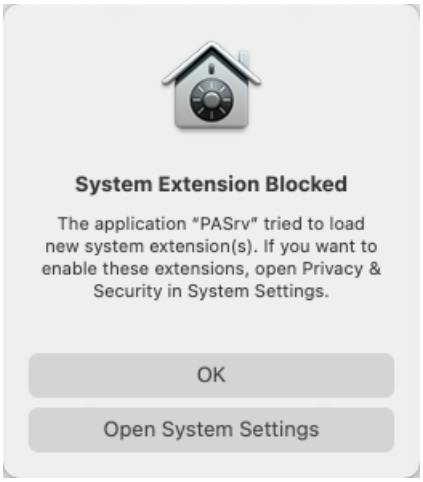

6. 依預設，macOS會封鎖 Prisma Access 代理程式系統延伸模組。如果您的管理員為 Prisma Access 代理程式設定了流量轉送規則，則會顯示系統或網路延伸模組：

   - 分割通道—將網路流量導向通過 Prisma Access 連線或外部。
   - 分割 DNS—除了網路流量之外，將應用程式和資源的 DNS 查詢導向通過 Prisma Access 或 Prisma Access 外部。

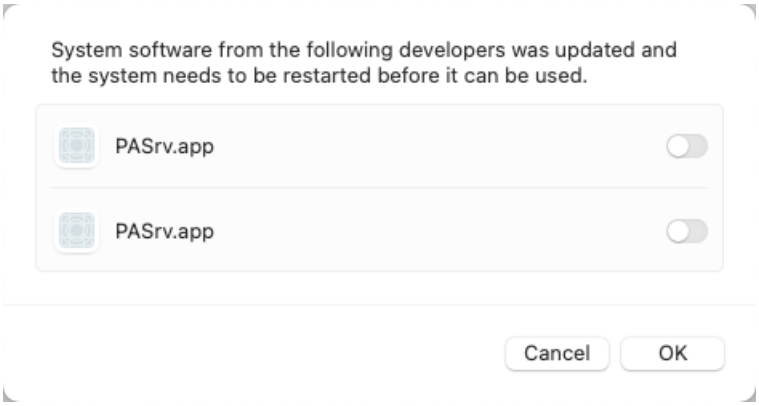
   若要使 Prisma Access 代理程式正常運作，您需要啟用系統延伸模組：

   1. 按一下 **Open System Settings**（開啟系統設定）。

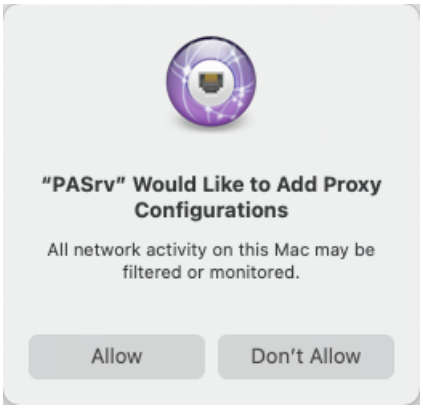
 ©2025 Palo Alto Networks, Inc.




2. 在 [Privacy & Security（隱私權與安全性）] 視窗中，按一下 **Some system software requires your attention before it can be used**（某些系統軟體需要您的注意才能使用）的**Details**（詳細資訊）。
3. 啟用兩個 **PASrv.app** 應用程式並按一下 **OK**（確定）。



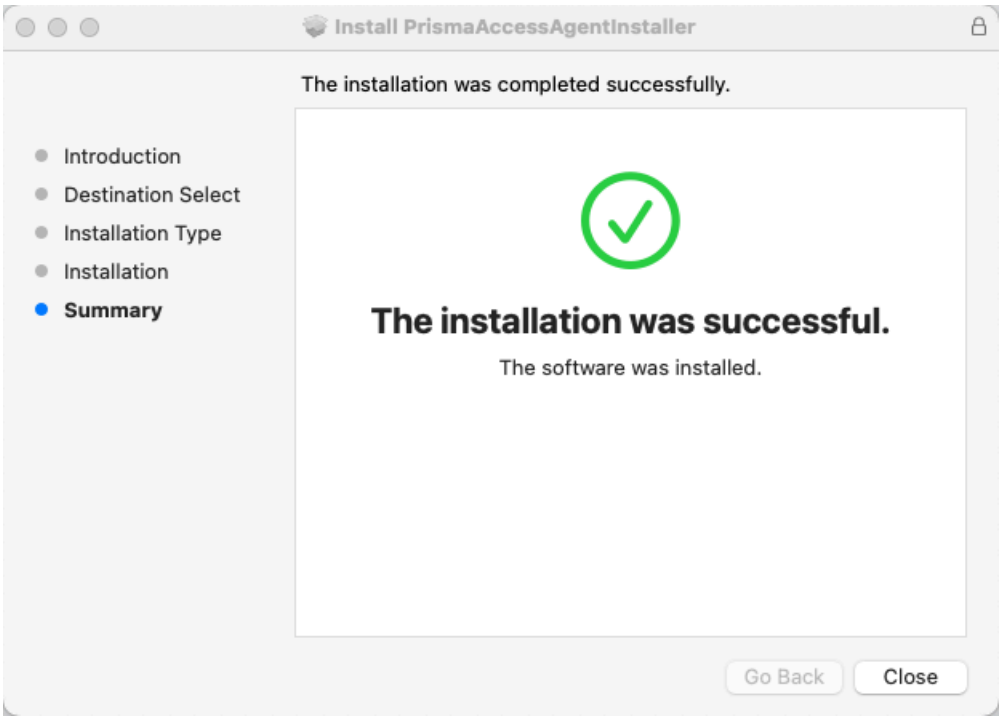

7. 如果您的管理員啟用了強制執行 Prisma Access 連線以進行網路存取的功能，系統將會提示您新增設定以篩選網路內容。若要繼續，請按一下 **Allow**（允許）。




在您允許之後，Prisma Access Agent 將出於安全目的過濾和監控您的網路連線。

8. 安裝完成後，**Close**（關閉）安裝程式。

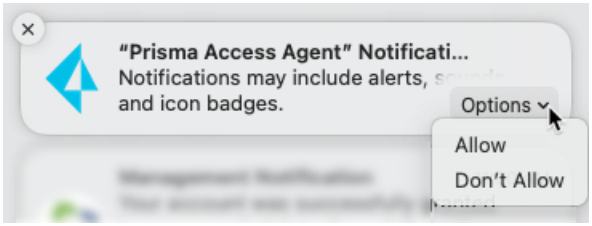
 ©2025 Palo Alto Networks, Inc.




9. 如果您的管理員設定了代理程式以安裝自主 DEM 代理程式和 Prisma Access 代理程式，請按一下 **OK**（確定），您就不會再次收到提示。
10. 按一下 [Prisma Access Agent Notifications（Prisma Access 代理程式通知）] 快顯，開啟通知偏好設定視窗。

**STEP 3 |** 如果收到提示，請啟用 Prisma Access 代理程式通知。

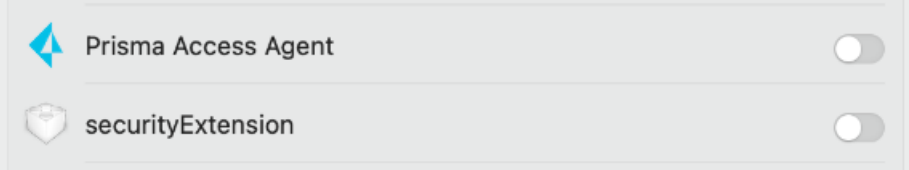
當 Prisma Access 代理程式通知快顯出現在您的桌面上時，將您的游標移至快顯上並選取 **Options**（選項） > **Allow**（允許）。




 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 若要讓 Prisma Access 代理程式存取 Safari 瀏覽器中的資料，您必須對安全性延伸模組和 Prisma Access 代理程式授與完整磁碟存取權。

1. 從 macOS 選取 **System Settings**（系統設定） > **Privacy & Security**（隱私權與安全性） > **Full Disk Access**（完整磁碟存取權）。從應用程式清單中啟用 **Prisma Access Agent**（**Prisma Access** 代理程式）和 **securityExtension**（安全性延伸模組）。




2. 收到提示時，**Quit & Reopen**（結束並重新開啟）Prisma Access 代理程式，讓變更生效。

### 安裝 Prisma Access 代理程式 (macOS)

如果您不再需要使用 Prisma Access Agent，可以手動移除它。請記住，卸載代理程式後，您將無法再存取公司網絡，並且您的端點將不再受到組織的安全策略的保護。

在開始之前，如果管理員為 Prisma Access Agent 啟用了防篡改功能，您必須從管理員取得防篡改解鎖密碼。若要解除安裝代理，您必須具有提升的管理權限。

完成以下步驟從命令列介面卸載 Prisma Access Agent。

**STEP 1 |** 在 macOS 裝置上，開啟終端機視窗並發出以下命令：

```
sudo /應用程式/Prisma\ Access\ Agent.app/Contents/Helpers/
uninstaller
```

**STEP 2 |** 出現提示時輸入管理員密碼。

**STEP 3 |** 如果提示輸入管理員密碼，請輸入防篡改解鎖密碼。否則，按 **Enter** 開始卸載。

Prisma Access Agent 及其擴充功能將被刪除。

## 安裝 Prisma Access Agent (Windows)

若要在您的 Windows 裝置上手動安裝 Prisma Access 代理程式。

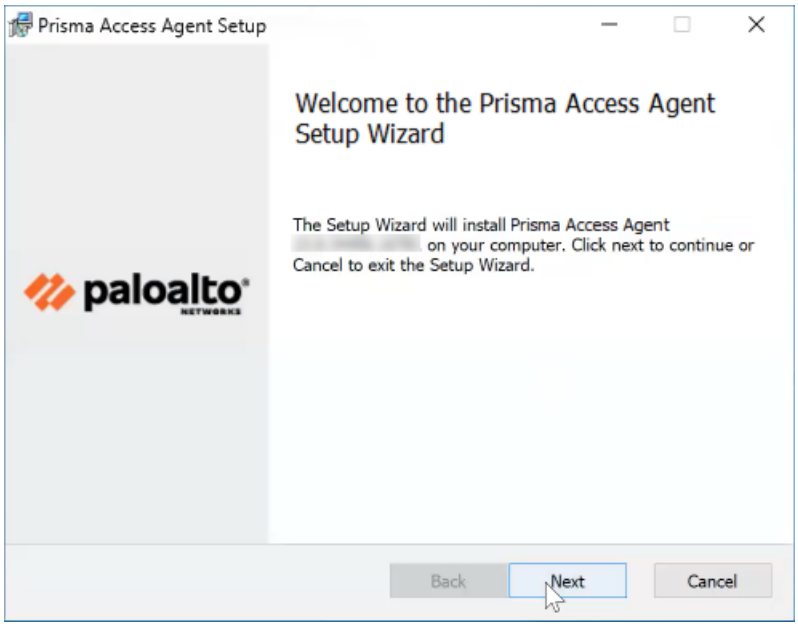
**STEP 1 |** 取得您的管理員提供的 Prisma Access 代理程式套件。該套件名稱的格式如下：

`PrismaAccessAgent_x64_<version>.msi`

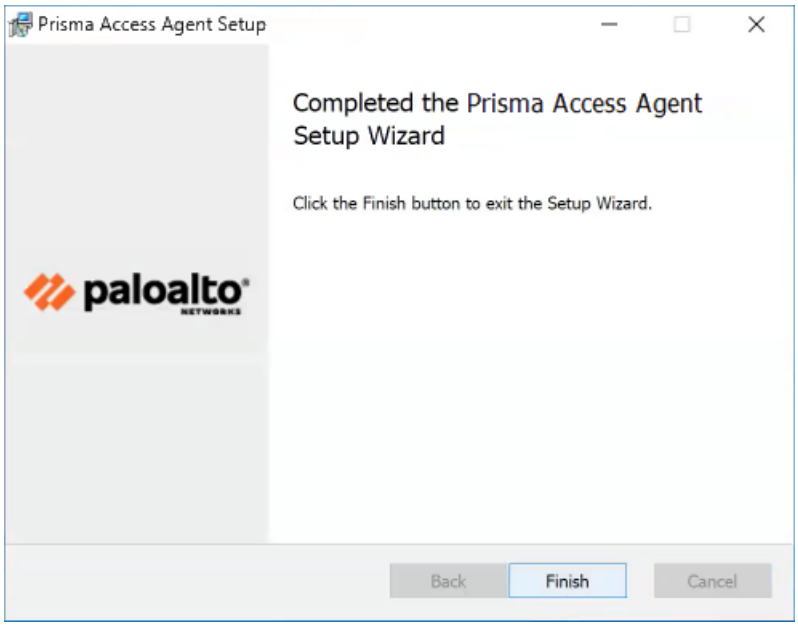
 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 在您的「下載」資料夾中（或您放置安裝套件的任何位置），按兩下安裝套件圖示並按照提示安裝 Prisma Access 代理程式。

1. 當安裝精靈出現時，按一下 **Next**（下一步）繼續。




2. 檢閱一般使用者授權合約，選取 **I accept the terms in the License Agreement**（我接受授權合約中的條款），然後按一下 **Next**（下一步）。
3. 按一下 **Install**（安裝）以開始安裝。
4. 出現 **allow this app to make changes to your device**（允許此應用程式對您的裝置進行變更）的提示時，按一下 **Yes**（是）。
5. 安裝完成時，按一下 **Finish**（完成）。




6. 如果您的管理員設定了代理程式以安裝自主 DEM 代理程式和 Prisma Access 代理程式，請按一下 **OK**（確定），您就不會再次收到提示。


©2025 Palo Alto Networks, Inc.

### 安裝 Prisma Access 代理程式 (Windows)

如果您不再需要使用 Prisma Access Agent，可以手動移除它。請記住，卸載代理程式後，您將無法再存取公司網絡，並且您的端點將不再受到組織的安全策略的保護。

在開始之前，如果 Prisma Access Agent 啟用了防篡改功能，則必須從管理員取得防篡改解鎖密碼。若要卸載代理，您必須具有管理員權限。

完成以下步驟以解除安裝 Prisma Access Agent：

**STEP 1 |** 啟用 Prisma Access 代理程式

1. 在命令提示字元視窗中執行以下命令：

```
"C:\Program Files\Palo Alto Networks\Prisma Access Agent
\pacli" traffic show
```

2. 如果提示輸入管理員密碼，請輸入防篡改解鎖密碼。

**STEP 2 |** 從設定中卸載 Prisma Access Agent。

- 在 Windows 上：
  1. 開啟 “開始” 功能表。
  2. 選擇 “設定” > “應用程式” > “已安裝的應用程式”。
  3. 捲動到 **Prisma Access Agent**。
  4. 選擇 更多選項 > 卸載。
  5. 當提示繼續卸載時，按一下 「是」。
- 在 Windows 上：
  1. 開啟 “開始” 功能表。
  2. 選擇 設定 > 應用程式 > 應用程式和功能。
  3. 捲動到 **Prisma Access Agent**。
  4. 選擇 更多 > 卸載。
  5. 當提示繼續卸載時，按一下 「是」。

## 登入已啟用動態權限存取的 Prisma Access Agent

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access Agent | ❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ 網際網路存取 |

若要存取組織的網路、資源、SaaS 應用程式或網際網路，請使用您的登入認證登入 Prisma Access 代理程式。


©2025 Palo Alto Networks, Inc.

登入 Prisma Access 代理程式後，您會使用最佳 Prisma Access 位置（有時稱為閘道）自動連線到您的網路。自動選擇最佳位置通常以提供最佳效能，進而為您提供更好的體驗，例如檢視以本地語言顯示的網站。當您的裝置位於組織網路外部時，代理程式會找出最佳位置，以便在連線到網路時為您提供最佳效能。

在開始之前，您必須在裝置上安裝 Prisma Access 代理程式。您的管理員通常會將 Prisma Access 代理程式部署到您用於存取組織網路、資源和應用程式的裝置上。代理程式將根據管理員定義的政策規則進行設定，再部署到您的裝置。但是，如果您的管理員未將 Prisma Access 代理程式部署到您的裝置，則您需要手動安裝 Prisma Access 代理程式。

根據在您組織中設定 Prisma Access 的方式，您的管理員應該為您提供以下登入資訊：

- Prisma Access 伺服器的名稱，該伺服器託管管理 Prisma Access Agent 的服務。可能會有多部伺服器，取決於 Prisma Access 設定。

  。
- 如果您的組織使用動態權限存取，您所處理的專案名稱。動態權限存取使您能夠根據獲指派的專案存取您組織的網絡和資源，因此您不會意外存取另一個專案的資源。如果您獲指派處理多個專案，您可以輕鬆地切換專案。



根據作業系統的設定，應用程式圖示和介面可採用深色模式或淺色模式顯示。

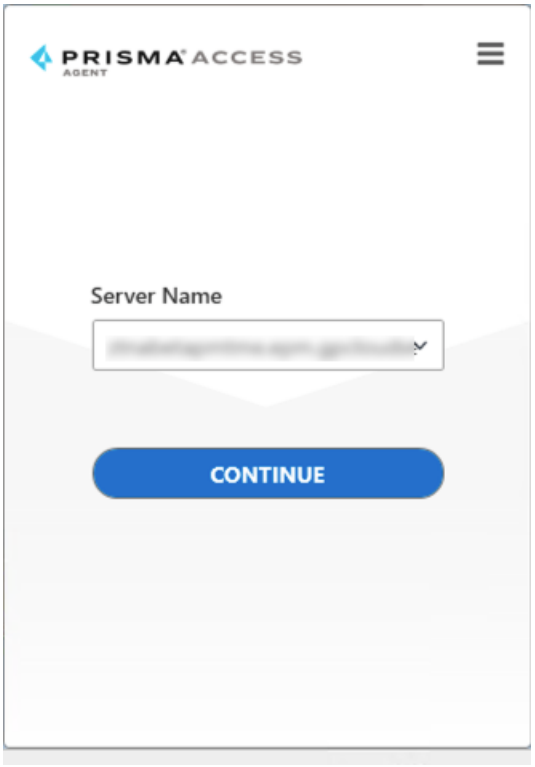
完成下列步驟以登入 Prisma Access 代理程式：

**STEP 1 |** 從 macOS 功能表列或 Windows 工作列按一下 Prisma Access Agent 圖示 啟動 Prisma Access Agent。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 如果出現提示，請輸入或選取管理員提供的 Prisma Access 伺服器的**Server Name**（伺服器名稱），然後選取 **Continue**（繼續）。

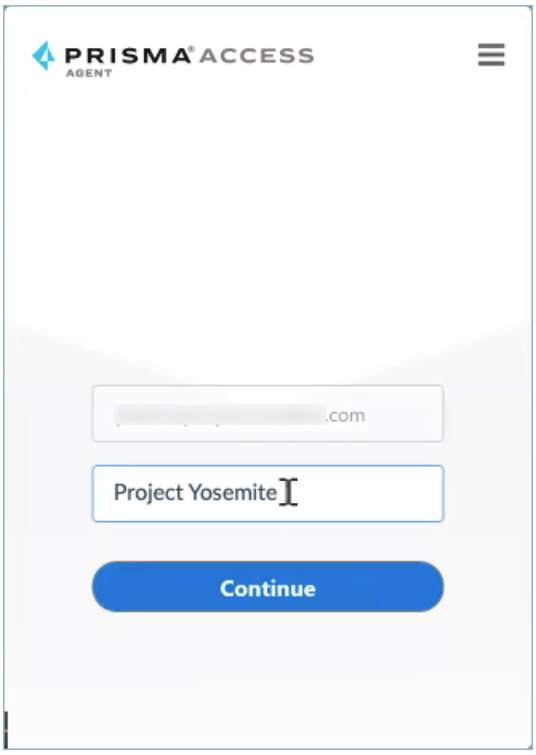
伺服器名稱的格式為 **<example.domain.com>**，沒有 **https://** 通訊協定。伺服器名稱的最大長度為 256 個字元。




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 輸入您管理員傳送給您的專案名稱，然後 **Continue**（繼續）。

專案名稱的長度上限為 32 個字元。



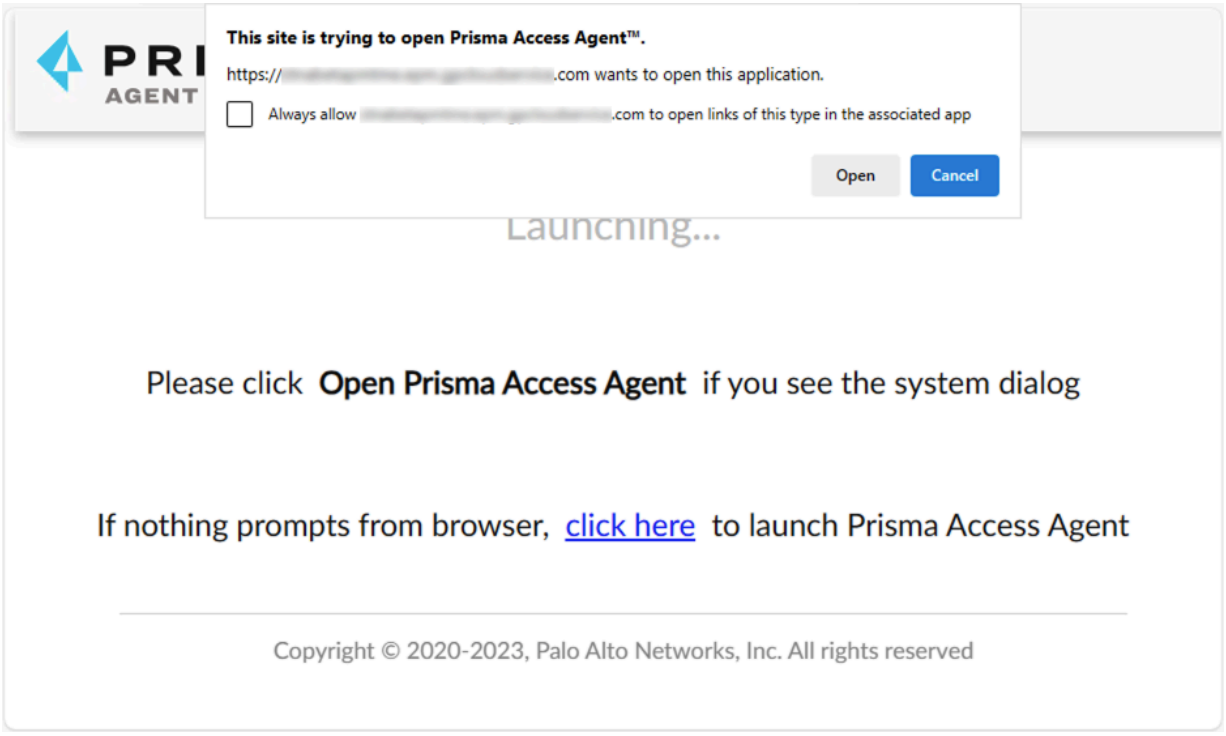

**STEP 4 |** 在預設網頁瀏覽器顯示的登入頁面中，藉由輸入組織的登入認證，登入組織的單一登入 (SSO) 應用程式，例如 Okta 或 Azure Active Directory (AD)。

如果您的管理員啟用了多因素驗證 (MFA)，您需要在登入時於瀏覽器中完成其他驗證。

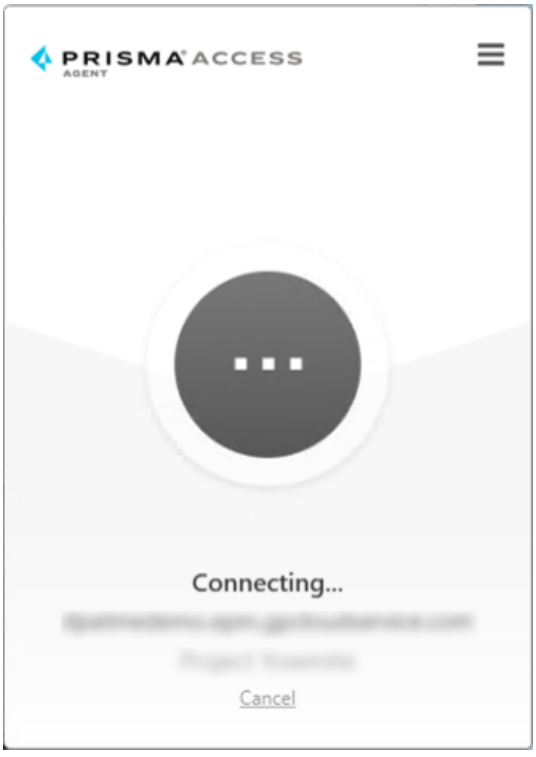

©2025 Palo Alto Networks, Inc.

**STEP 5 |** 當網頁瀏覽器提示時，按一下 **Open**（開啟）。

如果您不希望瀏覽器在您下一次登入時出現提示，請選取 **Always allow <site> to open these types of links in the associated app**（一律允許網站在相關聯應用程式中開啟這些類型的連結），然後按一下 **Open**（開啟）（如果您的預設網頁瀏覽器支援）。

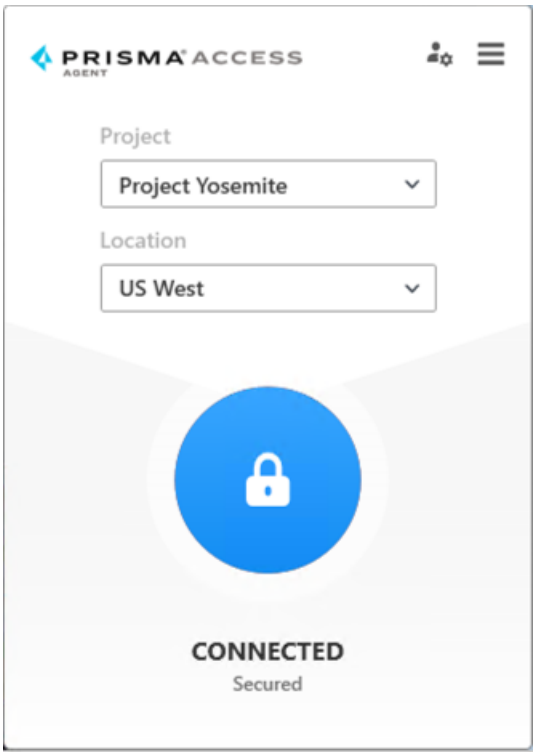



**STEP 6 |** 等待 Prisma Access 代理程式連線到 Prisma Access。




 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** 成功登入後，您會自動連線到最佳可用的 Prisma Access 位置。如果您使用專案登入，則您會連線到專案的最佳可用位置。




您現在可以存取組織的資源和 SaaS 應用程式，以及安全存取網際網路。

如果您的管理員為 啟用了 *Always On*（始終開啟）*Prisma Access Agent* 模式，由於貴組織的政策，您無法與 *Prisma Access* 中斷連線。不過，您仍然可以變更 *Prisma Access* 位置。

如果您的管理員為 *Prisma Access Agent* 啟用了 ***On Demand***（隨選）模式，您必須按一下鎖定圖示以連線到 *Prisma Access*。

# 變更已啟用動態權限存取的 Prisma Access Agent 的偏好設定

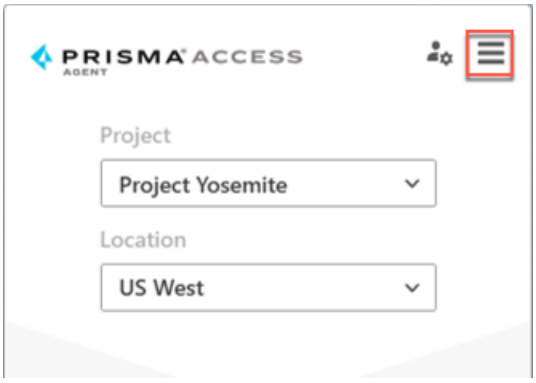
| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access Agent | ❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ 網際網路存取 |

使用 Prisma Access Agent 偏好設定視窗可檢視您裝置的相關資訊，並更改代理程式的選項，例如啟用桌面通知。

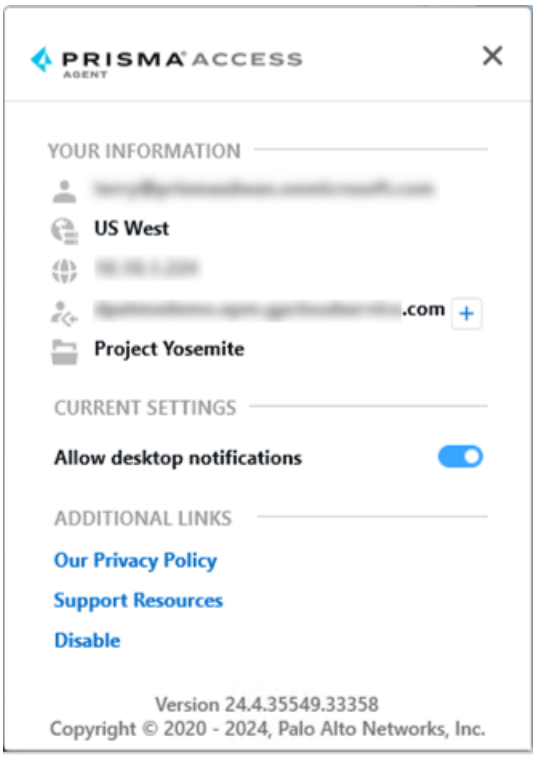
**STEP 1 |** 從從 macOS 功能表列或 Windows 工作列按一下 Prisma Access Agent 圖示 啟動 Prisma Access Agent。


©2025 Palo Alto Networks, Inc.

**STEP 2 |** 按一下漢堡功能表以開啟偏好設定視窗。




**STEP 3 |** 在偏好設定視窗中，您可以檢視以下資訊：




| 圖示 | 說明 |
|---|---|
| | 您的使用者 ID。 |
| | 您裝置連線到的 Prisma Access 位置。 |
| | Prisma Access 裝置的 IP 位址。 |
| | 您連線到的管理介面（伺服器）的主機名稱或 IP 位址。您可以按一下加號 **(+)** 圖示，以連線到不同的伺服器。 |


©2025 Palo Alto Networks, Inc.

| 圖示 | 說明 |
| --- | --- |
|  | 您登入的專案。 |

**STEP 4 |** 在功能表列 (macOS) 或在工作列 (Windows) 中接收 Prisma Access Agent 通知，**Allow desktop notifications**（允許桌面通知）。此設定預設為啟用。

桌面通知將遵循您在安裝時設定的任何請勿打擾設定。作業系統會在安裝時提示您允許來自 Prisma Access Agent 的通知。

**STEP 5 |** 若要瞭解 Prisma Access Agent 會收集哪些資料，以及這些資訊的用途，請檢視 **Our Privacy Policy**（我的隱私權政策）。

**STEP 6 |** 若要取得您使用 Prisma Access Agent 時可能遇到問題的協助，請按一下 **Support Resources**（支援資源）。

**STEP 7 |** 如果您的管理員允許它，您可以 **Sign Out**（登出）Prisma Access Agent。

**STEP 8 |** 如果管理員啟用了該功能，則您可以 **Disable**（停用）Prisma Access Agent，以便您可以切換至 GlobalProtect 應用程式（如果它已安裝在您的裝置上）。

**STEP 9 |** 檢視 Prisma Access Agent 的版本。

**STEP 10 |** 若要關閉視窗，請按一下 **X**。

## 將已啟用動態權限存取的 Prisma Access Agent 連線到不同的位置

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access Agent | ❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ 網際網路存取 |

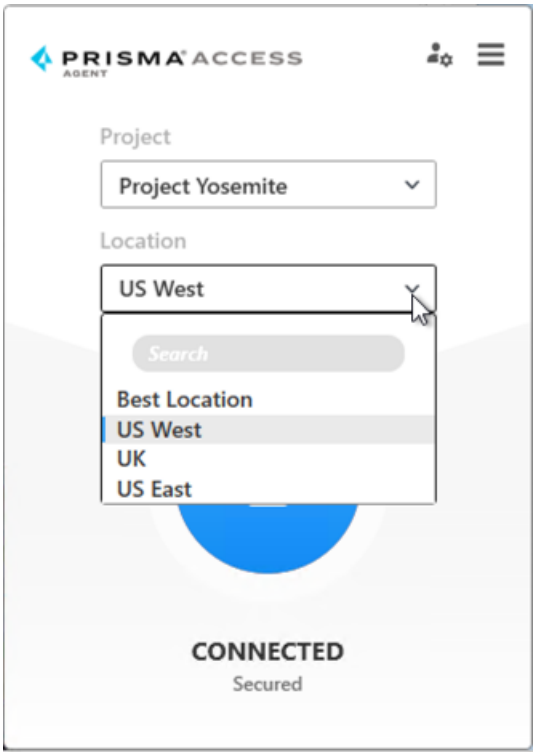
登入 Prisma Access Agent 後，您會自動連線到最佳的可用 Prisma Access 位置。如果想要變更位置，您可以使用 **Location**（位置）下拉式清單進行變更。

**STEP 1 |** 從 macOS 功能表列或 Windows 工作列按一下 Prisma Access Agent 圖示 啟動 Prisma Access Agent。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 選取不同的 **Location**（位置）。您可以 **Search**（搜尋）位置或從清單中選擇位置。

可用位置的清單會根據基於回應時間、可用性和其他因素的最佳體驗進行排序。提供最佳體驗的位置會被列為 **Best Location**（最佳位置）。




**STEP 3 |** 如果您的管理員為 Prisma Access Agent 啟用了 **On Demand**（隨選）模式，請按一下鎖定圖示以連線到新選取的位置。否則，Prisma Access Agent 會繼續變更位置。

## 切換至不同的租用戶

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access Agent | ❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ 網際網路存取 |

如果您指派給組織中的多個專案，您可以切換到另一個專案，以存取與該專案相關聯的網路和資源。

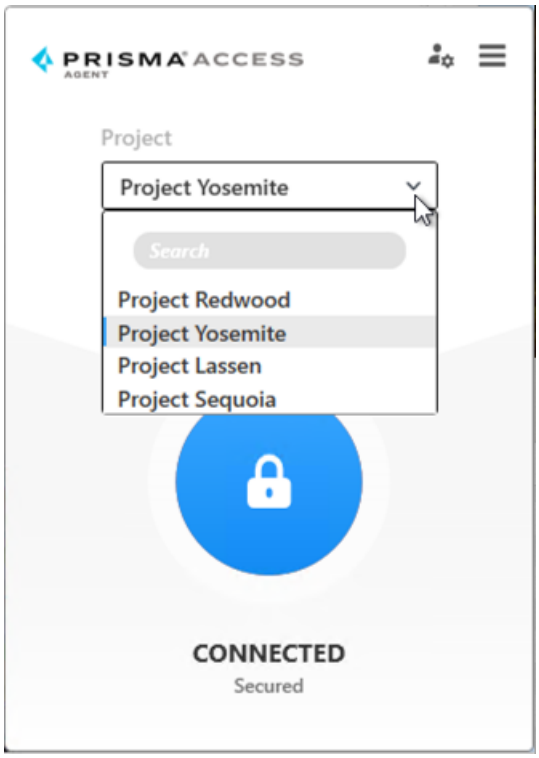
如果您嘗試切換至的專案可以從不同的伺服器存取，您需要先切換到該伺服器。

**STEP 1 |** 從 macOS 功能表列或 Windows 工作列按一下 Prisma Access Agent 圖示 啟動 Prisma Access Agent。


©2025 Palo Alto Networks, Inc.

**STEP 2 |** 選取不同的 **Project**（專案）。您可以 **Search**（搜尋）位置或從清單中選擇位置。

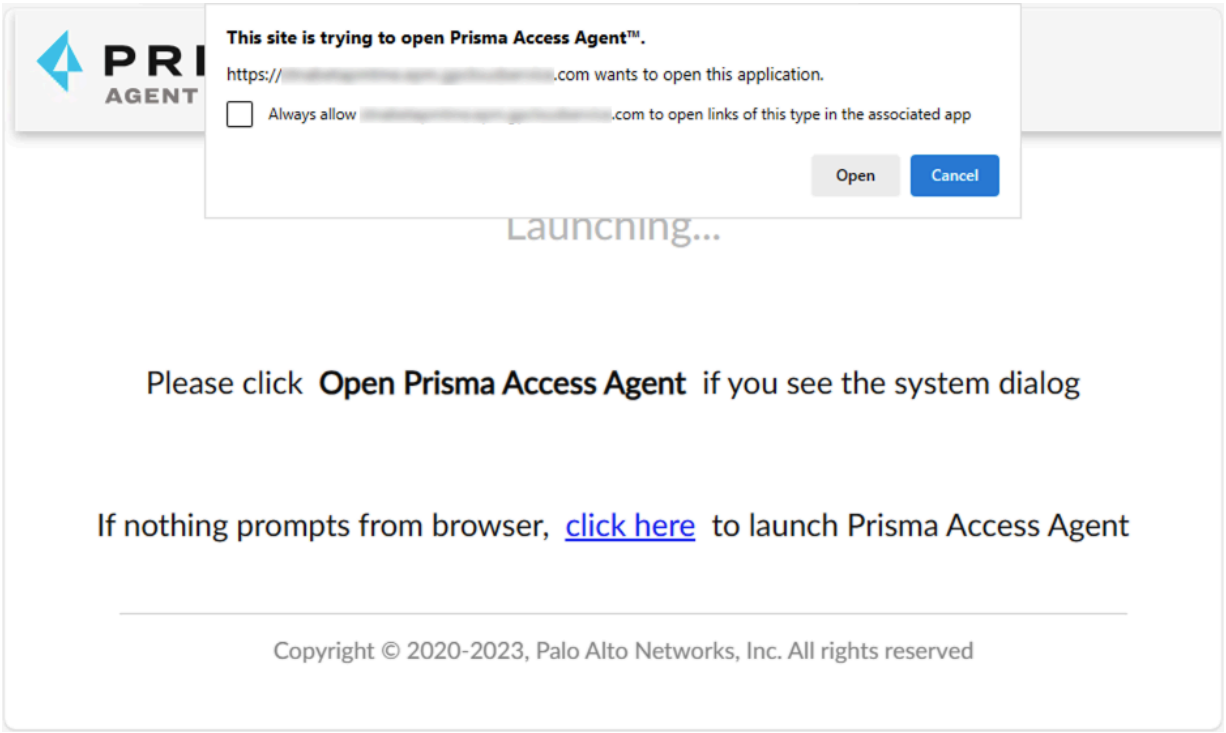
您必須指派給您要切換至的專案。




**STEP 3 |** 如果您的管理員已為 Prisma Access Agent 啟用了 **On Demand**（隨選）模式，請按一下鎖定圖示以切換專案。否則，Prisma Access Agent 會繼續切換專案。


©2025 Palo Alto Networks, Inc.

**STEP 4 |** 每次您切換專案時，Prisma Access Agent 會中斷與目前專案的連線，並連線到新選取的專案。系統可能會提示您再次 **Open**（開啟）Prisma Access Agent。




## 將已啟用動態權限存取的 Prisma Access Agent 連線到不同的伺服器

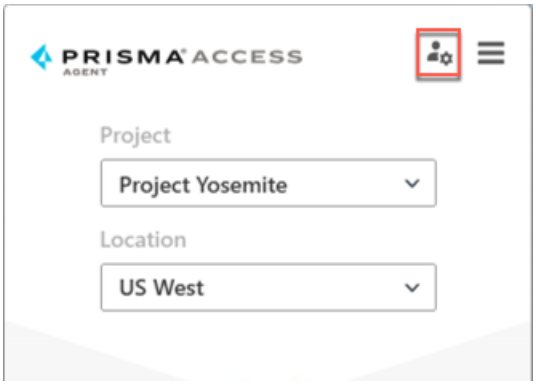
| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access Agent | ❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ 網際網路存取 |

Prisma Access 伺服器的執行個體也稱為租用戶。如果您的管理員設定了多個 Prisma Access 伺服器，您可以連線到不同伺服器，透過該伺服器存取網路或資源。

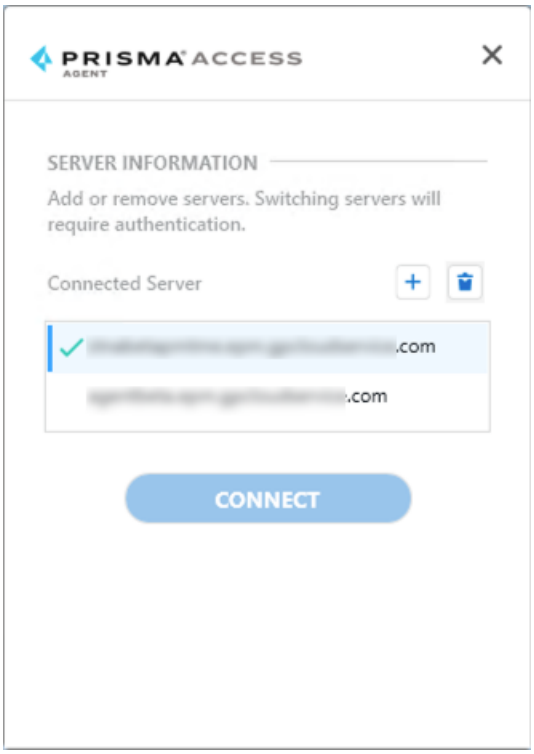
例如，您需要處理不同的專案，但該專案僅可在不同的伺服器上存取。您需要先連線到該伺服器，然後才能變更為該專案。

**STEP 1 |** 從 macOS 功能表列或 Windows 工作列按一下 Prisma Access Agent 圖示 啟動 Prisma Access Agent。

**STEP 2 |** 透過選取伺服器管理圖示來編輯伺服器設定。




**STEP 3 |** 伺服器資訊視窗顯示您連線的伺服器。如果列出其他伺服器，您可以選取其中一部伺服器並與它 **Connect**（連線）。



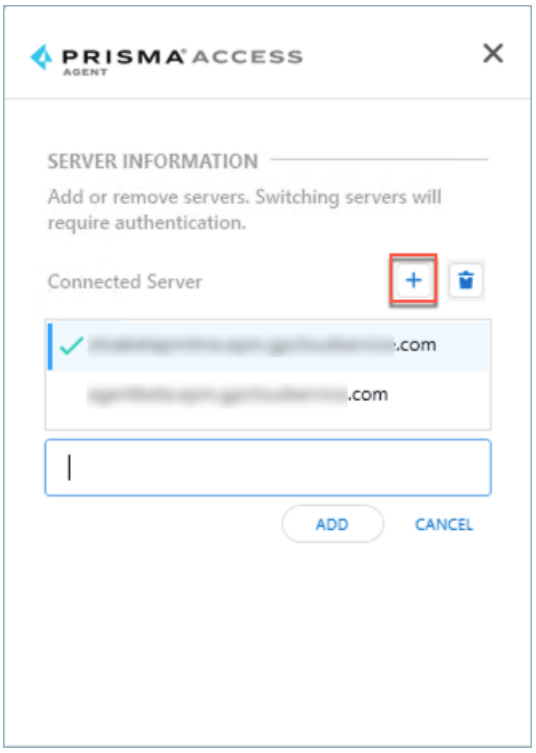


©2025 Palo Alto Networks, Inc.

**STEP 4 |** 如果您需要新增伺服器，請完成以下步驟：

1. 按一下 **+** 符號。
2. 輸入新的伺服器名稱（由您的管理員提供）並 **Add**（新增）。

   伺服器名稱的格式為 **<example.domain.com>**，沒有 **https://**。伺服器名稱的最大長度為 256 個字元。此頁面允許的伺服器數量上限為 20。




3. 新增伺服器之後，加以選取並按一下 **Connect**（連線）。

**STEP 5 |** 當 [Confirmation（確認）] 視窗出現時，按一下 **Yes**（是）與目前的伺服器中斷連線，並連線至其他伺服器。您需要再次提供單一登入認證。

**STEP 6 |** 出現提示時，透過提供專案名稱（如果適用）登入新伺服器。

## 在 Prisma Access Agent 與 GlobalProtect 應用程式之間切換

| 這可在何處使用？ | 我需要哪些內容？ |
|---|---|
| • Prisma Access Agent | ❑ macOS 12 或更新版本的桌面裝置，或 Windows 10 版本 2024 或更新版本或 Windows 11 桌面裝置<br>❑ 網際網路存取 |

在某些組織中，Prisma Access Agent 安裝在已安裝 GlobalProtect 應用程式的使用者裝置上。在安裝 Prisma Access Agent 之後，您可以視需要在 Prisma Access Agent 與GlobalProtect 應用程式之間切換。


©2025 Palo Alto Networks, Inc.

在切換到 GlobalProtect 應用程式之後，Prisma Access 代理程式處於停用狀態。在停用狀態下：

- 流向 Prisma Access 位置的所有流量都會停用，且多因素驗證 (MFA) 也會停用。

  Prisma Access 代理程式和 GlobalProtect 都使用相同的 GlobalProtect 連接埠，來接聽 MFA 要求（針對特定應用程式進行額外驗證），但一次只有一個代理程式可以使用該連接埠。當您停用 Prisma Access 代理程式時，該連接埠將被釋出，以供 GlobalProtect 使用。
- 與伺服器的通訊仍會持續，因此代理程式可以繼續接收分階段的推出升級、ADEM 通知、來自管理員的遠端 Shell 要求，以及執行 HIP 檢查。
- 如果由管理員設定，防篡改功能將繼續運作，以保護代理程式免遭未經授權的篡改。
- 在 macOS 裝置上，Prisma Access 代理程式的系統和網路延伸模組將繼續處於作用中狀態，而內容篩選器也將繼續處於作用中狀態。
- 如果您切換到另一部伺服器，Prisma Access 代理程式將自動重新啟用。如果您在代理程式停用時嘗試連線至 Prisma Access 位置，則代理程式將連線至最佳位置。

您可以使用 Prisma Access 代理程式應用程式或 Prisma Access 命令列工具 (PACli)，在兩個應用程式之間切換。

- Prisma Access 代理程式應用程式
- Prisma Access 命令列 (PACli)

## 在 Prisma Access Agent 與 GlobalProtect 應用程式之間切換（使用 Prisma Access 代理程式應用程式）

在切換到 GlobalProtect™ 應用程式之前，您需要停用 Prisma Access Agent。如果您的管理員設定了該功能以允許使用者停用 Prisma Access Agent，則您可以使用該應用程式停用 Prisma Access Agent。停用 Prisma Access Agent 後，您可以啟動 GlobalProtect 應用程式。

您的管理員必須聯絡 *Palo Alto Networks* 團隊才能啟用此租用戶級功能。它不作為代理設置 。

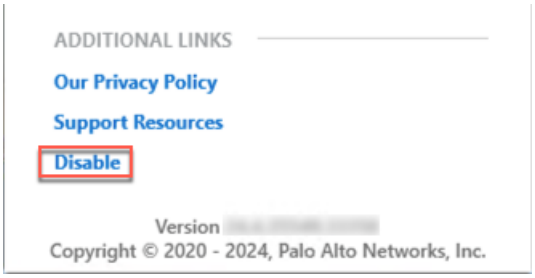

©2025 Palo Alto Networks, Inc.

若要從 Prisma Access 代理程式切換到 GlobalProtect 應用程式：

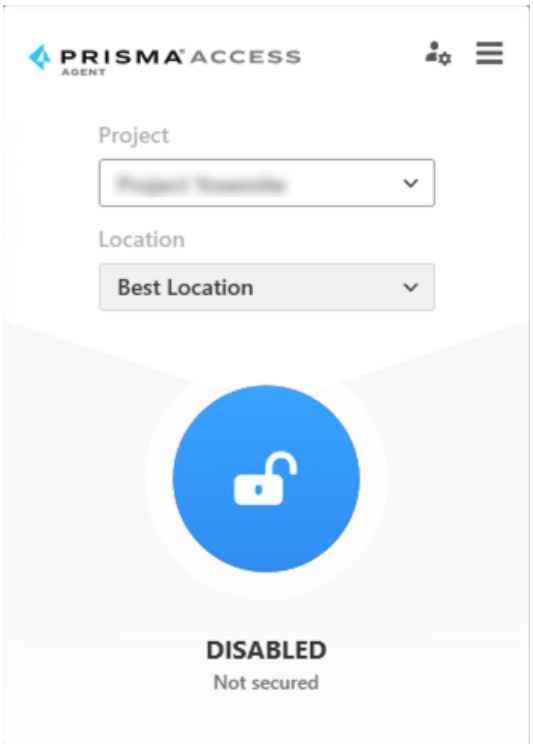
1. 啟用 Prisma Access 代理程式

   如果您是第一次停用代理，請開啟 Prisma Access Agent 應用程式並退出 Prisma Access Agent。

   1. 選擇漢堡選單並選擇“退出”。
   2. 再次登入 Prisma Access Agent 應用程序，使 「停用」 連結出現在首選項視窗中。
2. 按一下漢堡功能表以開啟偏好設定視窗。
3. 啟用 Prisma Access 代理程式

   
   
4. 點選 **X**關閉首選項視窗。

   Prisma Access Agent 已停用。

   
   
5. 啟動 GlobalProtect 應用程式並 連接 到 GlobalProtect。


©2025 Palo Alto Networks, Inc.

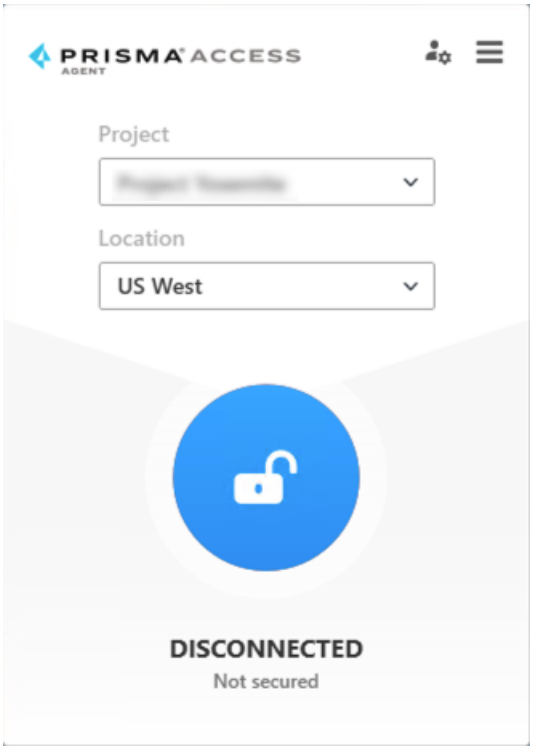
若要從 Prisma Access 代理程式切換到 GlobalProtect 應用程式：

1. 開啟 GlobalProtect 應用程式。
2. 點擊選項選單並選擇 斷開連接。
3. 登入 Prisma Access 代理程式
4. 按一下漢堡功能表以開啟偏好設定視窗。
5. 啟用 Prisma Access 代理程式




6. 點選 **X**關閉首選項視窗。
7. 如果代理程式處於始終開啟模式，則代理程式將啟用並連線到最佳位置。

   如果代理程式處於按需模式，則 Prisma Access Agent 已啟用但仍處於中斷連線狀態。按一下鎖定圖示即可連接到 Prisma Access 位置。




## 在 Prisma Access Agent 與 GlobalProtect 應用程式之間切換（使用 PACli 工具）

若要在 Prisma Access 代理程式與 GlobalProtect 應用程式之間切換，請執行 Prisma Access 命令列工具 (PACli)。切換到 GlobalProtect 應用程式時，如果管理員在 Prisma Access Agent 入職期間


©2025 Palo Alto Networks, Inc.

設定了防篡改解鎖密碼，PACli 工具會提示您輸入防篡改解鎖密碼。切換到所需的應用程式會停用您目前正在使用的應用程式。

**STEP 1 |** 若要從 Prisma Access 代理程式切換到 GlobalProtect 應用程式：

1. 執行 **switchto** 命令來切換代理程式：
   - 在 macOS 裝置上，開啟終端機視窗並發出以下命令：

     ```
     sudo /Applications/Prisma\ Access\ Agent.app/Contents/
     Helpers/pacli switchto GlobalProtect
     ```

   - 在 Windows 裝置上，開啟命令提示視窗並發出以下命令：

     ```
     "C:\Program Files\Palo Alto Networks\Prisma Access Agent
     \pacli" switchto GlobalProtect
     ```

2. （macOS）出現提示時輸入管理員密碼。
3. 如果出現提示，請輸入 **Y** 切換到 GlobalProtect 應用程式。
4. 如果提示輸入管理員密碼，請輸入防篡改解鎖密碼。

   以下文字顯示了在 macOS 裝置上從 Prisma Access Agent 切換到 GlobalProtect 的範例：

   ```
   <username@hostname>~#cd /應用程式/Prisma \ Access \ Agent.app/
   Contents/Helpers <username@hostname> 助手#sudo./pacli switchto
    GlobalProtect輸入管理員密碼：已停用 Prisma Access Agent。啟動
    GlobalProtect 服務。這最多可能需要 15 分鐘。成功啟動 GlobalProtect。
   切換完成。<username@hostname> 助手 %
   ```

   此動作會停止 GlobalProtect 服務，並啟動 Prisma Access 代理程式服務以及防篡改功能。在 Prisma Access Agent 日誌中寫入一條條目，表示 Prisma Access Agent 已被停用。例如，記錄以下事件：

   ```
   <username@hostname>~#cd /應用程式/Prisma \ Access \ Agent.app/
   Contents/Helpers <username@hostname> 助手 %./pacli 事件。 。740
    2024-12-11 23:20:57 竄改偵測代理程式已停用 741 2024-12-11
    23:20:57 代理隧道已斷線。 。
   ```

5. （可選）透過執行 **pacli switchto status** 指令顯示 **switchto** 指令的狀態。

   以下文字顯示了在 macOS 上檢查 **switchto** 命令狀態的範例：

   ```
   <username@hostname>~#cd /應用程式/Prisma \ Access \ Agent.app/
   Contents/Helpers <username@hostname> 助手#sudo./pacli switchto
    status Prisma Access Agent：已停用 GlobalProtect：已啟用
    <username@hostname> 助手 %
   ```

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 若要切換回 Prisma Access 代理程式：

1. 執行 **switchto** 命令來切換代理程式：
   - 在 macOS 裝置上，開啟終端機視窗並發出以下命令：

     ```
     sudo /Applications/Prisma\ Access\ Agent.app/Contents/
     Helpers/pacli switchto PrismaAccessAgent
     ```

   - 在 Windows 裝置上，開啟命令提示視窗並發出以下命令：

     ```
     "C:\Program Files\Palo Alto Networks\Prisma Access Agent
     \pacli" switchto PrismaAccessAgent
     ```

2. （macOS）出現提示時輸入管理員密碼。
3. 如果出現提示，請輸入 **Y** 切換到 Prisma Access 代理程式。
4. 如果提示輸入管理員密碼，請輸入防篡改解鎖密碼。

   以下文字顯示了在 macOS 裝置上從 GlobalProtect 應用程式切換到 Prisma Access Agent 的範例：

   ```
   <username@hostname>~#cd /應用程式/Prisma \ Access \ Agent.app/
   Contents/Helpers <username@hostname> 助手#sudo./pacli switchto
    PrismaAccessAgent 密碼：輸入管理者密碼：停止 GlobalProtect 服務。
   這最多可能需要 15 分鐘。已停用 GlobalProtect。成功啟動 Prisma Access
    Agent。切換完成。<username@hostname> 助手 %
   ```

   此動作會停止 GlobalProtect 服務，並啟動 Prisma Access 代理程式服務以及防篡改功能。在 Prisma Access Agent 日誌中寫入一條條目，表示 Prisma Access Agent 已啟用。例如，記錄以下事件：

   ```
   <username@hostname>~#cd /應用程式/Prisma \ Access \ Agent.app/
   Contents/Helpers <username@hostname> 助手 %./pacli 事件。 。742
    2024-12-11 23:21:05 竄改偵測代理程式已啟用 743 2024-12-11
    23:21:21 代理隧道 隧道已連線。 。
   ```

   切換回 Prisma Access Agent 後，如果代理程式處於 Always On 模式，則代理程式將啟用並連線到最佳位置。如果代理程式處於按需模式，則代理程式將啟用但斷開連線。

5. （可選）透過執行 **pacli switchto status** 指令顯示 **switchto** 指令的狀態。

   以下文字顯示了在 macOS 上檢查 **switchto** 命令狀態的範例：

   ```
   <username@hostname>~#cd /應用程式/Prisma \ Access \ Agent.app/
   Contents/Helpers <username@hostname> 助手#sudo./pacli switchto
    status Prisma Access Agent：已啟用 GlobalProtect：已停用
    <username@hostname> 助手 %
   ```

 ©2025 Palo Alto Networks, Inc.

# 檢視和監控動態權限存取使用者

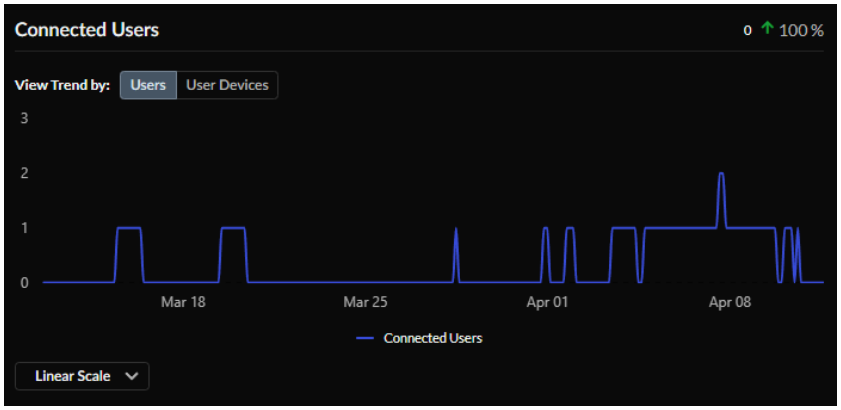
| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 授權 |

動態權限存取使 Prisma Access 能夠根據使用者正在處理的專案將不同的網路和安全性政策規則套用至行動使用者流量。前往 Strata Cloud Manager 控管中心的 **Insights**（洞察） > **Users**（使用者），以檢視您環境中的使用者型存取資訊。

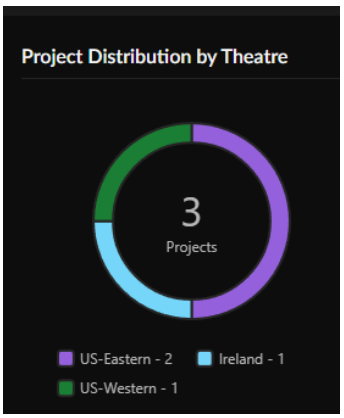
## 已連線使用者

檢視 **Connected Users**（已連線使用者），以檢視目前已連線的使用者或已連線的使用者裝置。向上或向下箭頭可將此時間範圍與之前的時間範圍進行比較，以確認已連線使用者或裝置數目中的差異（以百分比為單位）。

選取 **View Trend by Users**（依使用者檢視趨勢），以檢視目前連線到 Prisma Access 代理程式的使用者數目，然後按一下 **View Trend by User Devices**（依使用者裝置檢視趨勢），以檢視目前連線到 Prisma Access 代理程式的使用者裝置數目。



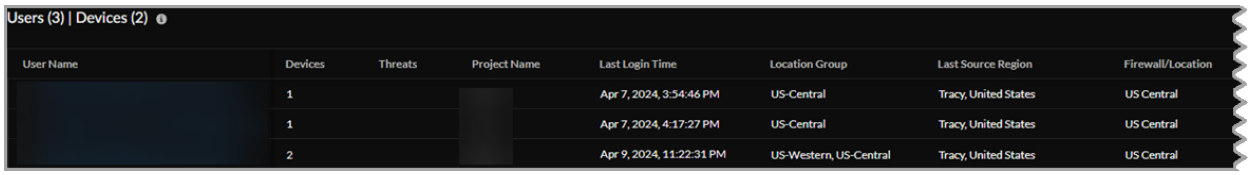

檢視 **Project Distribution by Theatre**（依劇院進行專案分佈），依位置或劇院檢視專案數目。





©2025 Palo Alto Networks, Inc.

**Users | Devices**（使用者 | 裝置）表格顯示與每個使用者和裝置相關聯的 **Project Name**（專案名稱）。您也可以依使用者、上次登入時間、上次來源位置、上次連線的 Prisma Access 位置、來源網際網路通訊協定，以及作業系統系列和版本，查看已連線多少裝置。

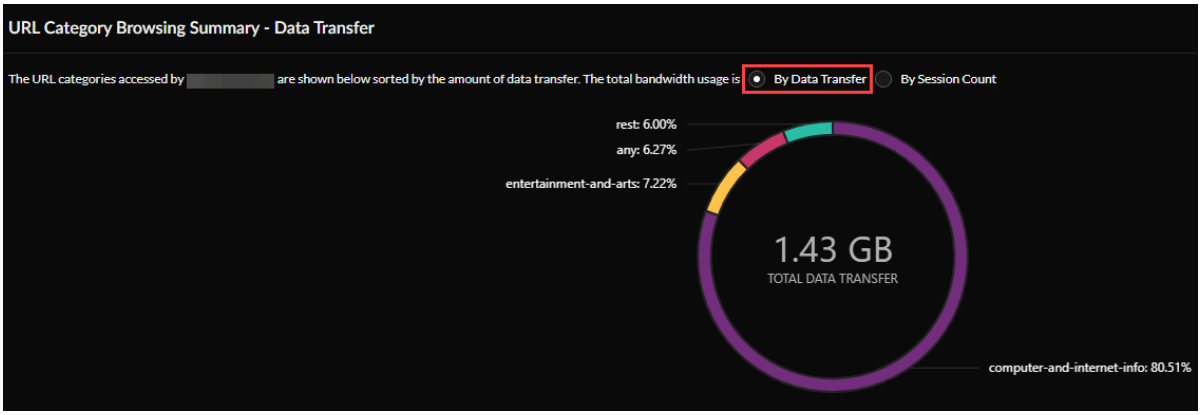


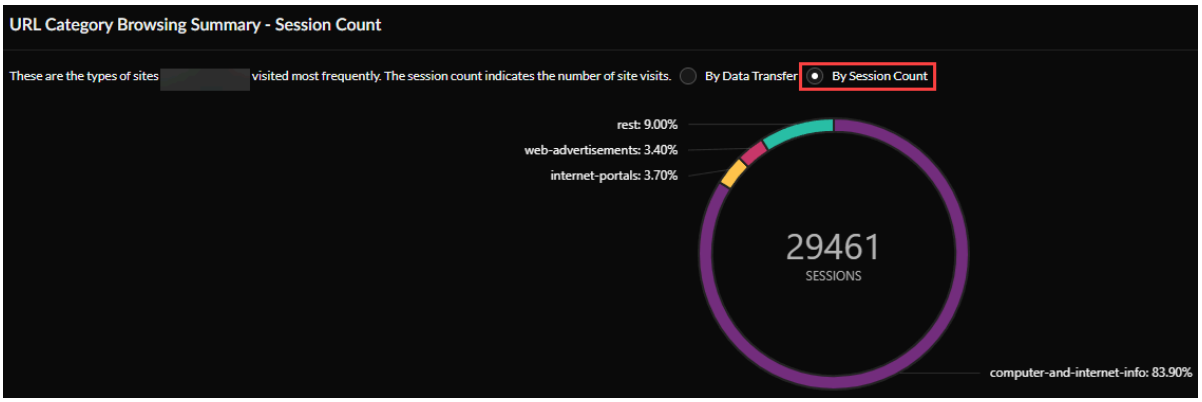

選取任何 **Project Name**（專案名稱）以前往 **Projects**（專案）頁面。

選取任何 **User Name**（使用者名）以檢視使用者詳細資訊，例如 **Activity**（活動）和 **Connectivity**（連線）。

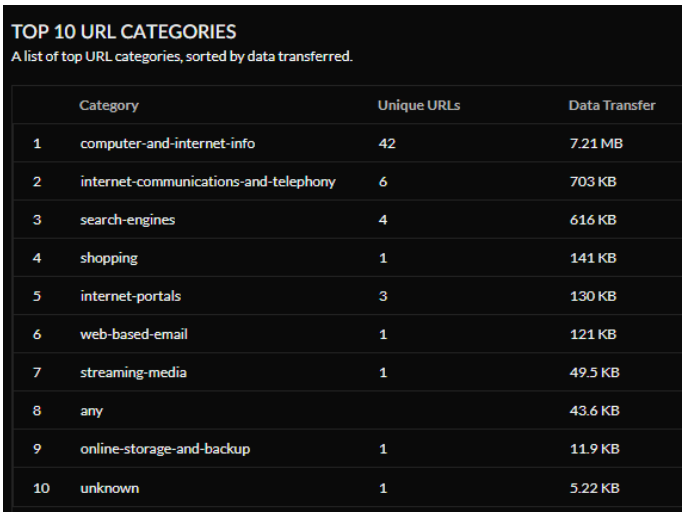
## 活動

**URL Browsing Category Summary- Data Transfer**（**URL** 瀏覽類別摘要 - 資料傳輸）—**By Data Transfer**（依資料傳輸）或 **By Session Count**（依工作階段計數）檢視您的瀏覽類別資料傳輸摘要。您還可以檢視 **Top 10 URL Categories**（前 **10** 個 **URL** 類別）的清單，依傳輸的資料排序。




 ©2025 Palo Alto Networks, Inc.

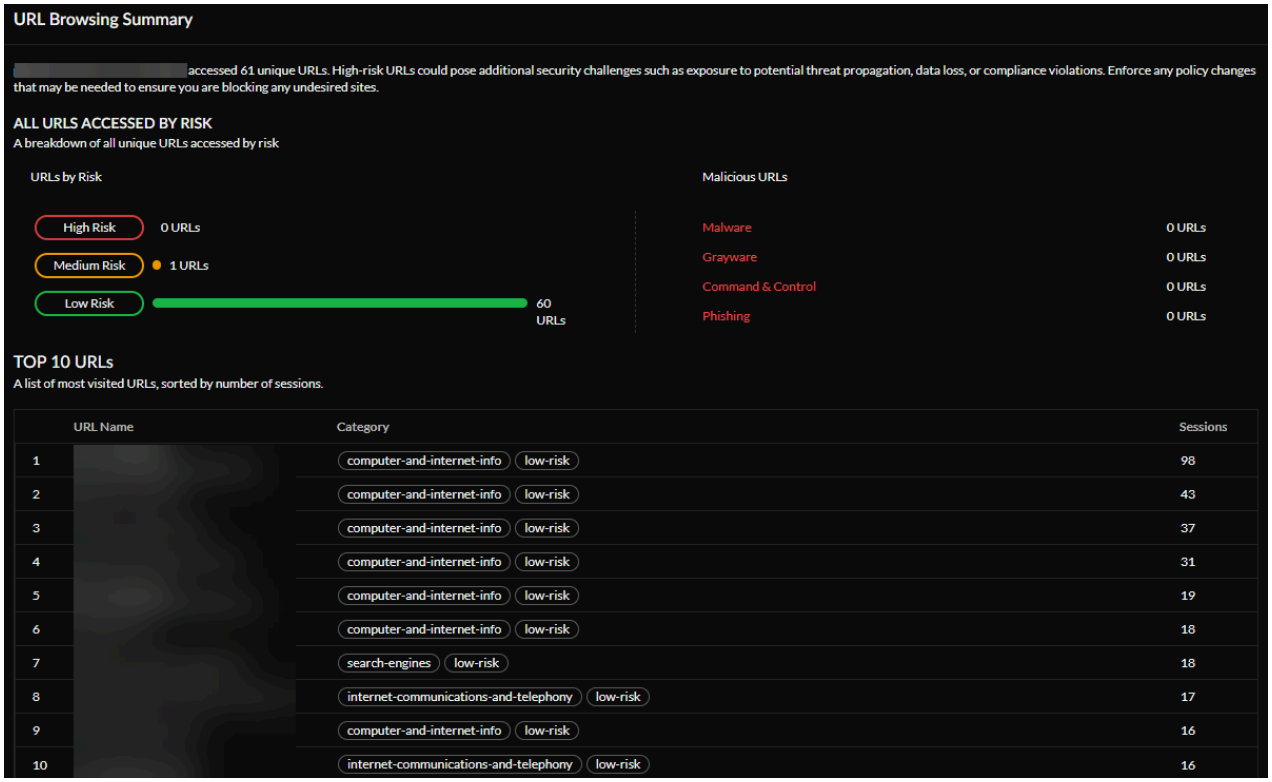


TOP 10 URL CATEGORIES

A list of top URL categories, sorted by data transferred.

| | Category | Unique URLs | Data Transfer |
|---|---|---|---|
| 1 | computer-and-internet-info | 42 | 7.21 MB |
| 2 | internet-communications-and-telephony | 6 | 703 KB |
| 3 | search-engines | 4 | 616 KB |
| 4 | shopping | 1 | 141 KB |
| 5 | internet-portals | 3 | 130 KB |
| 6 | web-based-email | 1 | 121 KB |
| 7 | streaming-media | 1 | 49.5 KB |
| 8 | any | | 43.6 KB |
| 9 | online-storage-and-backup | 1 | 11.9 KB |
| 10 | unknown | 1 | 5.22 KB |

**URL Browsing Summary**（**URL** 瀏覽摘要）—查看您的 URL 瀏覽摘要，包括您依風險存取的所有 URL。您可以檢視依風險（高、中或低）細分的 URL，並查看您已存取多少惡意 URL。您也可以檢視已造訪的 **Top 10 URLs**（前 **10** 個 **URL**）清單，以及您已存取每個 URL 多少次。



URL Browsing Summary

[redacted] accessed 61 unique URLs. High-risk URLs could pose additional security challenges such as exposure to potential threat propagation, data loss, or compliance violations. Enforce any policy changes that may be needed to ensure you are blocking any undesired sites.

ALL URLS ACCESSED BY RISK

A breakdown of all unique URLs accessed by risk

URLs by Risk

High Risk 0 URLs

Medium Risk 1 URLs

Low Risk 60 URLs

Malicious URLs

Malware 0 URLs

Grayware 0 URLs

Command & Control 0 URLs

Phishing 0 URLs

TOP 10 URLs

A list of most visited URLs, sorted by number of sessions.

| | URL Name | Category | Sessions |
|---|---|---|---|
| 1 | [redacted] | computer-and-internet-info low-risk | 98 |
| 2 | | computer-and-internet-info low-risk | 43 |
| 3 | | computer-and-internet-info low-risk | 37 |
| 4 | | computer-and-internet-info low-risk | 31 |
| 5 | | computer-and-internet-info low-risk | 19 |
| 6 | | computer-and-internet-info low-risk | 18 |
| 7 | | search-engines low-risk | 18 |
| 8 | | internet-communications-and-telephony low-risk | 17 |
| 9 | | computer-and-internet-info low-risk | 16 |
| 10 | | internet-communications-and-telephony low-risk | 16 |

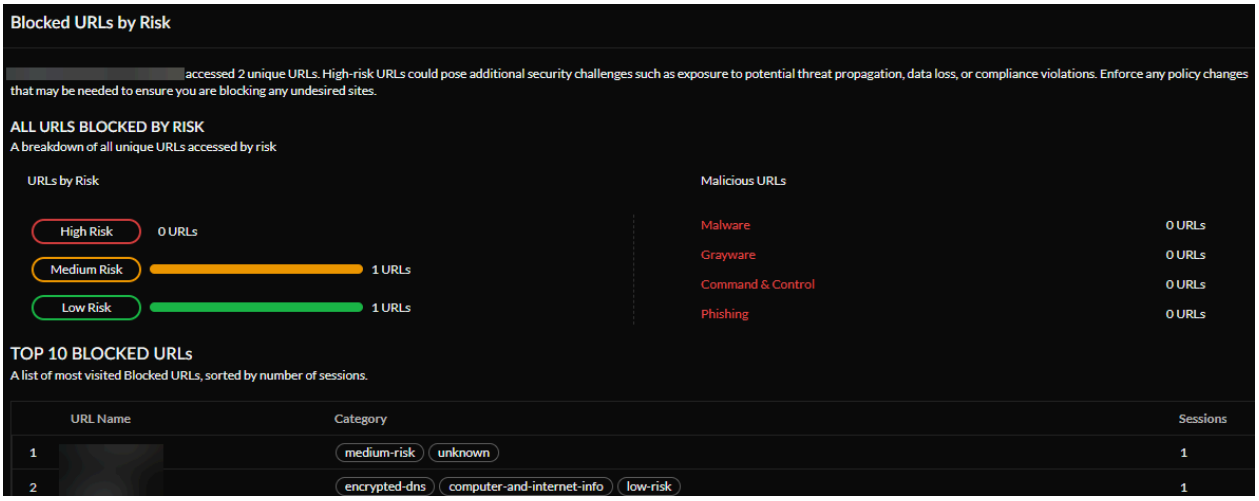
**View URL Filtering Logs**（檢視 **URL** 篩選日誌）—選取 **View URL Filtering Logs**（檢視 **URL** 篩選日誌），以檢視有關總資料傳輸量的詳細資訊。這些日誌提供系統、設定和網路事件的稽核線索。網路日誌會記錄 Prisma Access 在其中對您網路採取行動的所有事件。

- 檢視所有日誌資料，或使用下拉式清單，透過 **Firewall/URL**（防火牆/**URL**）、**Common**（通用）或 **Endpoint**（端點）進行篩選.其中每個篩選器也有數個子篩選器可供選擇。
- 輸入日誌查詢。按一下此欄位，以檢視要開始的查詢選取項目，並建置您的查詢。
- 選取時間範圍。預設值為過去 60 分鐘。

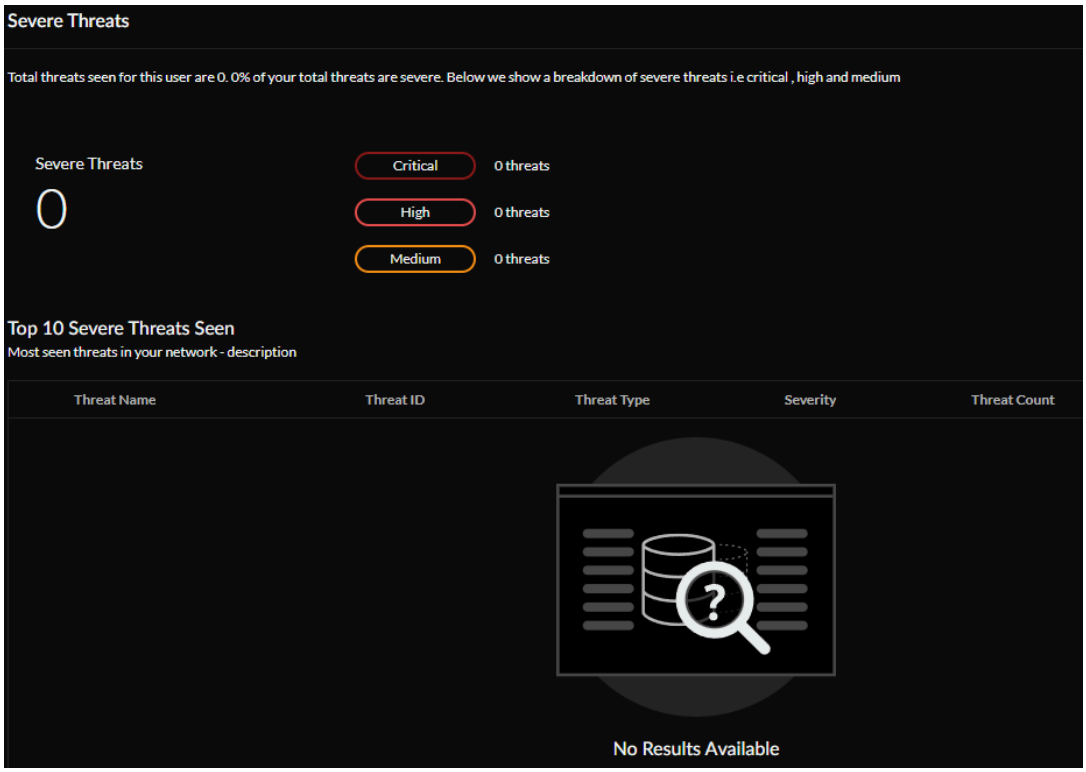

©2025 Palo Alto Networks, Inc.

- 選取 **Log Settings**（日誌設定）以檢視 Strata 記錄服務儀表板。Strata 記錄服務管理日誌的交付機制。

**Blocked URLs by Risk**（依風險封鎖的 **URL**）—查看您是否已存取或嘗試存取任何遭風險封鎖的 URL。高風險 URL 可能會帶來額外的安全性挑戰，例如暴露於潛在威脅傳播、資料遺失或違反合規性。強制執行任何封鎖任何不需要的網站所需的政策變更。您也可以查看最常造訪的 **Top 10 Blocked URLs**（前 **10** 個遭封鎖 **URL**）清單，依工作階段數目排序。




**Severe Threats**（嚴重威脅）—查看您的威脅中有多少是嚴重的。嚴重威脅進一步細分為嚴重、高和中威脅。您也可以檢視您環境中的 **Top 10 Severe Threats Seen**（所見的十大嚴重威脅）清單。




 ©2025 Palo Alto Networks, Inc.

## 連線

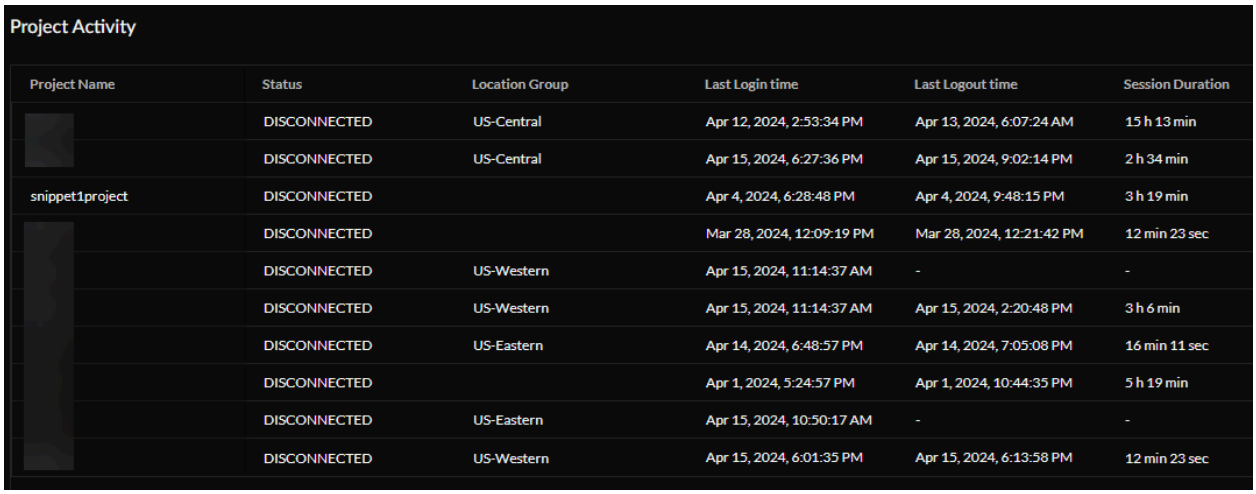
檢視任何 **User**（使用者）名稱，以檢視有關所選 **Time Range**（時間範圍）期間使用者 **Connectivity**（連線）的資訊。

**Active Projects**（作用中專案）—您可以查看在所選時間範圍期間哪些專案作用中，以及每個專案變成作用中的日期。

**Connected User's Devices Trend** 和 **Connected User's Devices**（已連線使用者的裝置趨勢和已連線使用者的裝置）—在主要 [Users（使用者）] 頁面上，您可以查看所有已連線的使用者及其專案。在 **Connectivity**（連線）頁面上，檢視所選時間範圍期間您的個別 **Connected User's Devices**（已連線使用者的裝置）趨勢，以及有關 **Connected User's Devices**（已連線使用者的裝置）的詳細資訊，例如裝置名稱、上次使用者來源 IP 位址、上次私人 IP 位址、上次使用者位置、上次登入時間、上次登出時間，以及上次工作階段持續時間。




**Project Activity**（專案活動）—依工作階段檢視使用者的專案活動。您可以查看工作階段的目前狀態、使用者登入每個專案的時間、他們登出的時間，以及每個工作階段持續多長時間。




**Total User Activity by Project**（依專案劃分的使用者活動總計）—檢視使用者在所選時間範圍期間花費在每個專案的時間。


©2025 Palo Alto Networks, Inc.

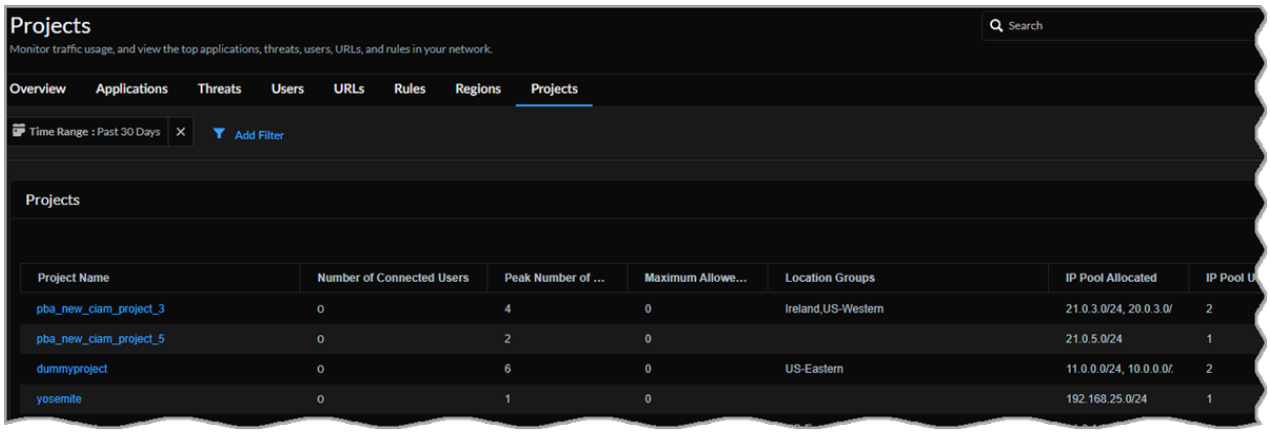
# 檢視和監控動態權限存取專案

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

使用 Strata Cloud Manager 監控您的使用者專案活動，以了解您的 Prisma Access 代理程式部署。前往 Strata Cloud Manager 控管中心的 **Activity Insights**（活動洞察） > **Projects**（專案），以檢視您環境中的專案型存取資訊。

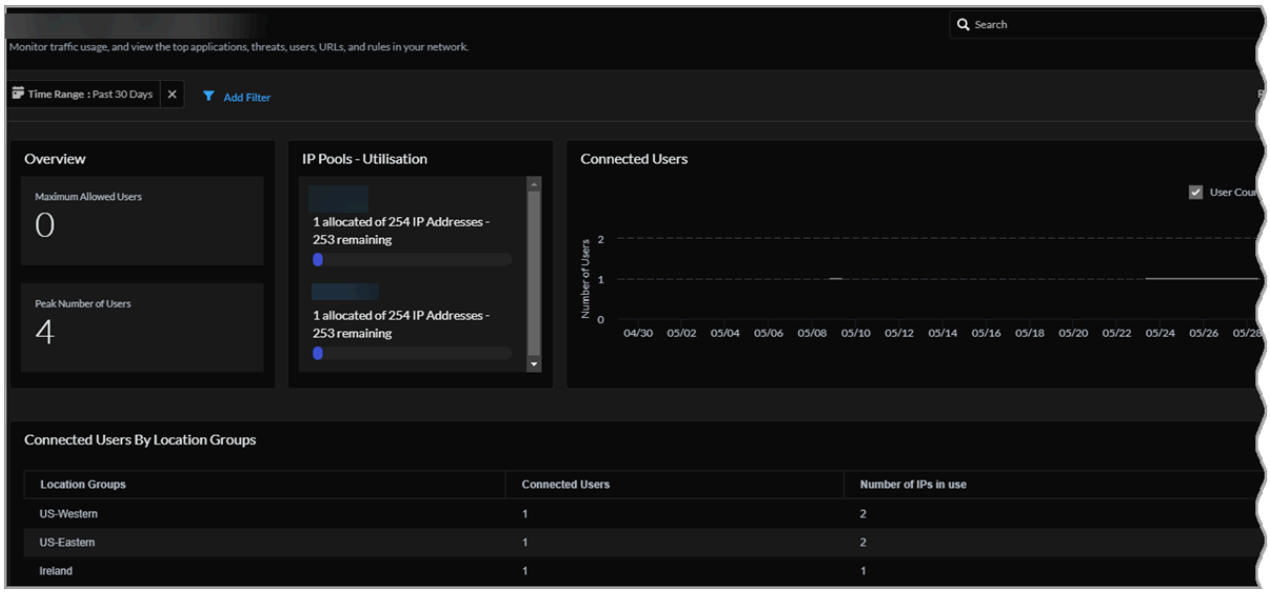
## 專案

**Projects**（專案）表格提供了有關您使用者在所選時間範圍期間使用 Prisma Access 存取的專案的整體檢視。您可以查看每個專案的已連線使用者數目、峰值使用者數目、允許的使用者數目上限、Prisma Access 位置群組、配置的 IP 位址集區、使用的 IP 集區、可用的 IP 位址數目，以及上次連線的 Prisma Access 位置。




選取一個 **Project Name**（專案名稱），前往該專案的詳細資訊頁面。專案名稱（下圖中經過模糊處理）出現在頁面的左上角。


©2025 Palo Alto Networks, Inc.

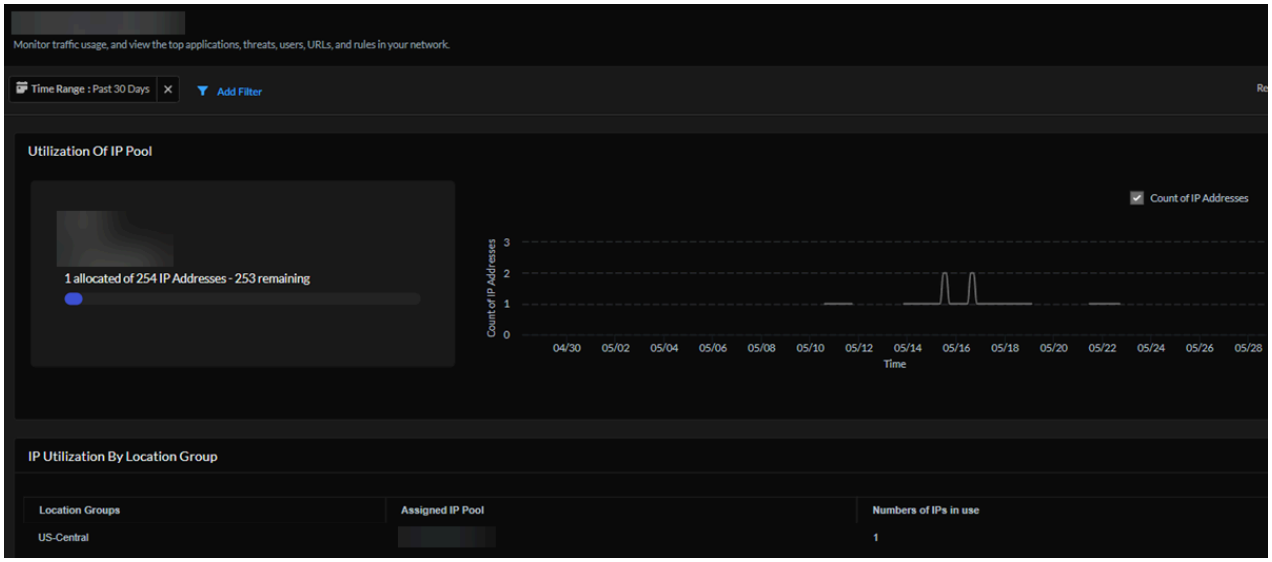



## 概要

在專案詳細資訊頁面上，**Overview**（概要）會顯示此專案允許的使用者數目上限，以及所選時間範圍期間的峰值使用者數目。

## IP 集區 - 使用率

檢視使用中的 IP 數目，以及此專案中集區仍可用的 IP 數目。選取特定 IP 集區以前往其詳細資訊頁面（請參閱下圖），您可以在其中查看此 IP 集區的使用率、使用的 IP 位址數目，以及依 Prisma Access 位置群組劃分的 IP 位址使用率。




## 已連線使用者

檢視在所選時間範圍期間連線的使用者的圖表。將游標暫留在圖形中的任意點上，即可查看該點的使用者計數。


©2025 Palo Alto Networks, Inc.

## 依位置群組劃分的已連線使用者

檢視依使用者所在的 Prisma Access **Location Group**（位置群組）劃分的使用者數目。您還可以查看每個 **Location Group**（位置群組）的使用中 IP 位址數目。

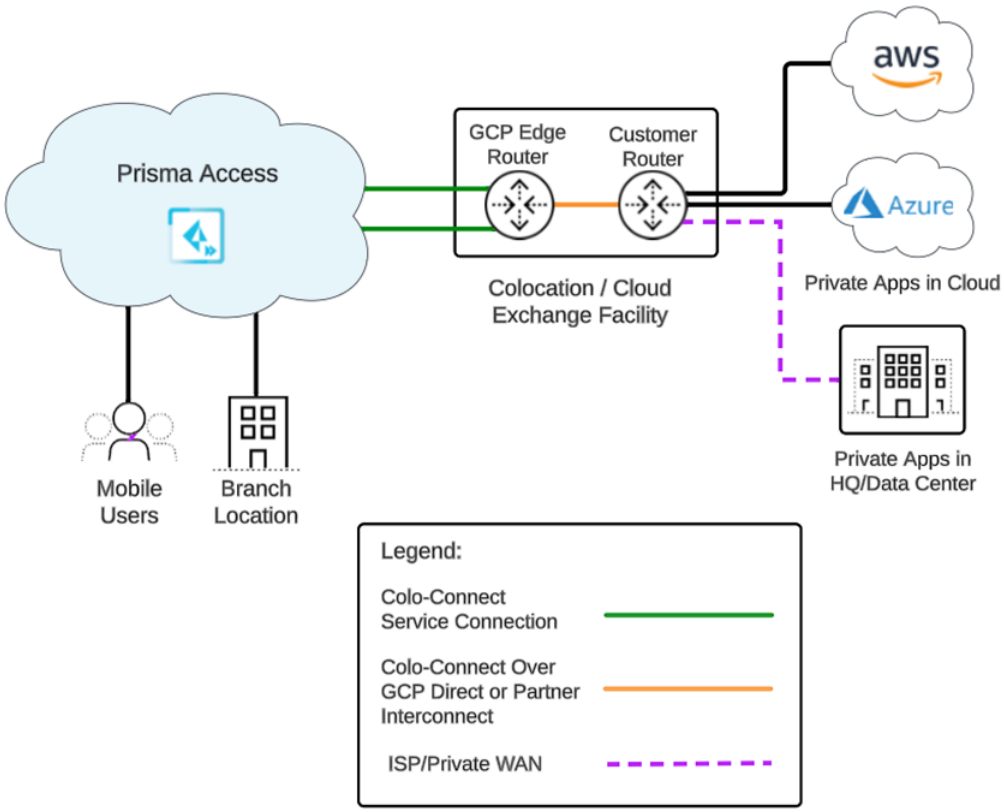

©2025 Palo Alto Networks, Inc.

# Prisma Access Colo-Connect

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ 執行最低雲端服務外掛程式版本為 4.1 和最低資料平面版本為 10.2.4 的 Prisma Access (Managed by Panorama) 部署<br>❑ Colo-Connect 附加元件授權 |

如今，由於高頻寬和低延遲需求，大型企業正在建置 Colo 型效能中樞，以在混合多雲架構中連線私人應用程式。通常，這些中樞包括與一或多個雲端提供者的互連，以及透過私人或租賃 WAN 與內部部署資料中心的連線。效能中樞可以高速路由公共雲端與內部部署基礎結構之間的流量，並且由於基礎互連基礎結構而具有彈性。

Colo-Connect 是根據 Colo 型效能中心概念所建置，提供高頻寬（高達 20 Gbps）私人連線，以及從現有效能中心到 Prisma Access 的無縫第 2/3 層連線。下圖顯示使用服務連線和直接或合作夥伴互連，在 GCP 執行個體中裝載 Prisma Access。此設定限制暴露至網際網路，並允許使用私人連線進行私人應用程式連線。




Prisma Access Colo-Connect 利用雲端原生 GCP 互連技術，為您的私人應用程式提供高頻寬服務連線，具有下列功能：

- 每個區域的高頻寬 (高達 20 Gbps) 輸送量，用於私人應用程式存取

- 支援使用 Google Cloud Platform (GCP) 進行專用和合作夥伴互連
- 支援每個互連連結有多個 VLAN 附件。
- 區域備援

 ©2025 Palo Alto Networks, Inc.

# Colo-Connect 使用案例

Prisma Access Colo-Connect 提供高頻寬雙向連線，以保護私人應用程式，如下列使用案例所示。

## 高頻寬存取私人應用程式

如果您的組織在 Colo 中有網路存在，並且您正在利用 Colo 設施，來建置與內部部署、公共雲端中或兩者託管的應用程式的私人連線，則 Prisma Access 可以透過 Colo-Connect 成為該 Colo 基礎結構的一部分。您可以使用 GCP 提供的專用或合作夥伴互連來設定 C olo-Connect，以便每個區域獲得高達 20 Gbps 輸送量，進行私人應用程式存取。

例如，您有一個或多個資料中心或總部位置可直接連線到 Colo，並且您想連線至 Prisma Access 進行高頻寬、安全的私人應用程式存取。在此情況下，您可以使用合作夥伴互連搭配 Prisma Access Colo-Connect，讓使用者可安全存取應用程式。由於 Colo 中的設備與公共雲端以及資料中心對等，因此您也可以提供對託管在公共雲端中的任何私人應用程式的存取。

Colo-Connect 與現有 IPsec 通道型服務連線共存，因此如果您必須為不需要高頻寬、多 gigabit (Gb) 輸送量的小型資料中心提供私人應用程式存取權，您也可以使用與這些資料中心的服務連線。您可以使用 BGP 路由來設定服務連線，使您的網路與服務連線和 Colo-Connect 連線相容。

## 私人應用程式的私人連線

Colo-Connect 可以利用私人網路，讓使用者存取私人應用程式，而不是透過網際網路存取它們，從而為私人應用程式新增額外的控制和安全性等級。

## 使用第三方 NaaS 提供者

在此使用案例中，您正在利用第三方網路即服務 (NaaS) 提供者（例如 Megaport 和 PacketFabric），在 Colo 與您在公共雲端中執行的應用程式之間連線，或與 SaaS 提供者 (例如 salesforce.com 或 Box) 連線。您想要在第三方網路與 Prisma Access 之間建立網路連線，並提供對連線服務、雲端和應用程式的高頻寬存取。您可以：

- 使用來自 NaaS 提供者的網路設備作為中樞，在使用者與執行於公共雲端 VPC 的應用程式或給定區域中的公用 SaaS 提供者之間提供連線。
- 在 NaaS 提供者的網路設備與 Prisma Access 之間建立 BGP 工作階段。

使用第三方 *NaaS* 解決方案搭配 *Prisma Access Colo-Connect* 未經 *Palo Alto Networks* 驗證。建議您與第三方提供者一起評估支援的功能，包括設定 *GCP* 的互連，以及建立 *Prisma Access* 的 *GRE* 通道，進行 *Colo-Connect* 服務連線。


©2025 Palo Alto Networks, Inc.

# Colo-Connect 與服務連線和 ZTNA 連接器有何不同？

Palo Alto Networks 提供三種安全存取私人應用程式的方式：服務連線、ZTNA 連接器和 Colo-Connect。服務連線和 ZTNA 連接器都可以保護透過網際網路對私人應用程式的存取，而 Colo-Connect 建立與您資料中心的私人連線。如需頻寬和差異因素的比較，請參閱下表。

| 部署類型 | | | |
|---|---|---|---|
| 功能 | **Colo-Connect** | **ZTNA 連接器** | 服務連線 |
| 每個計算區域的頻寬上限 | 20 Gbps | 10 Gbps | 5 Gbps |
| 吞吐量 | 與資料中心的 20 Gbps 雙向私人連線 | 每個資料中心最高 10 Gbps | 每個連線 1 Gbps |
| 與 SDN/NAAS 提供者相容，例如 Equinix Cross-Connect 和 Megaport | 是 | 否。 | 否。 |
| 跨資料中心的重疊網路 | 否。 | 是 | 否。 |
| 其他優勢 | 透過 Colo 輕鬆裝載至現有的混合雲端和多雲端部署 | 簡化了混合雲端與多雲端部署中的私人應用程式裝載 | 支援內部部署 Active Directory |
| 是否需要內部部署？ | 否。 | 是 | 否。 |


©2025 Palo Alto Networks, Inc.

# Colo-Connect 不支援的功能

Colo-Connect 不支援下列功能：

- 使用流量導向時，將 Colo-Connect 服務連線設定為目標服務連線
- IPv6 支援私人應用程式存取
- 透過 IPv6 進行 EBGP 對等


©2025 Palo Alto Networks, Inc.

# Prisma Access Colo-Connect 的需求和先決條件

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ 一個 Prisma Access (Managed by Panorama) 部署，執行最低雲端服務外掛程式版本 4.1 和最低 資料平面版本 10.2.4<br>❑ 一個 Colo-Connect 附加授權 |

在開始 Colo-Connect 裝載和設定之前，請遵循此檢查清單了解所需的資訊和先決條件。

- ❑ 確保您有權存取 Colo 設施提供者（例如，您有權存取 Equinix 客戶入口網站）。
- ❑ 確保您的 CPE 可以支援 GRE 和 BGP。

  Colo-Connect 服務連線使用 GRE 通道。
- ❑ 確定您將用於 Colo-Connect 的互連類型（合作夥伴或專用互連）。
  - 合作夥伴互連—合作夥伴互連需要來自 Prisma Access 的配對金鑰。您會 Prisma Access 裝載期間收到此金鑰。

    如果您建立合作夥伴互連，請確保服務提供者 (SP) 是搭配 GCP 的已核准 SP，並且 SP 與 GCP 之間的連線已建立。
  - 專用互連—
    - 開始在 Prisma Access 裝載之前，確定將連線交叉連接電纜的 Colo 位置。Palo Alto Networks 需要 Colo 位置才能訂購專用連結
    - 熟悉基本網路互連，以便您可以設定電路。
    - 在佈建專用互連之後，您必須測試它。
- ❑ 子網路需求—確定您將根據區域用於每個 Colo-Connect 連線的 RFC-1918 IPv4 子網路。Prisma Access 會使用這些子網路進行內部通訊和聯網。

  使子網路在給定租用戶的所有 Colo-Connect 區域中是唯一的。Colo-Connect 子網路不能與 Prisma Access 基礎子網路和行動使用者集區重疊。使用最小子網路大小 /28。
- ❑ 連結（互連）需求—設定連結時請遵循以下指導方針：
  - 每個 Colo-Connect 附加授權都包含一個容量 10 Gbps 的連結。您至少需要兩個連結，這意味著您需要在 Colo-Connect 部署中購買至少兩個授權。
  - 在每個區域中裝載兩個連結。

    這兩個連結應該位於不同的可用性區域（邊緣網域）。
  - （僅限專用互連部署）如果您想要在租用戶中裝載六個以上的連結，請聯繫您的 Palo Alto Networks 客戶代表或合作夥伴，他們將聯絡網站可靠性工程 (SRE) 團隊，並提交為給定租用戶增加配額的要求。


©2025 Palo Alto Networks, Inc.

- 連線需求—
  - 在每個區域中裝載兩個連線。

    這兩個連線應該位於不同的邊緣網域。
  - 作用中/備份或主動/主動模式下的連線必須具有相同的頻寬。
  - 確定您想要在主動/主動還是作用中/備份設定中設定連線。
- **Colo-Connect** 服務連線需求—
  - 每個服務連線需要兩個連線。
  - 給定服務連線的每個連線必須位於不同的連結和不同的邊緣網域。
  - 記下將用作 BGP IP 位址搭配 colo-router 和 GRE 通道本機 IP 位址的位址。您會在服務連線建立期間使用這些位址。
  - 服務連線必須位於相同的連結類型（合作夥伴互連連結或專用互連連結）。
- 與現有 **IPSec** 型服務連線的互通性—Palo Alto Networks 強烈建議您在不同區域部署 Colo-Connect 和 IPSec 通道型服務連線。此外，如果您是從 IPSec 通道型服務連接移轉到 Colo-Connect 服務連線，則必須排程維護時段。在您已從 IPSec 通道型服務連線移轉到 Colo-Connect 服務連線之後，請在 Colo-Connect 服務連線已啟動並執行中之後，且在維護時段到期之前移除IPSec 型服務連線。

 ©2025 Palo Alto Networks, Inc.

# 設定 Prisma Access Colo-Connect

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ 執行最低雲端服務外掛程式版本為 4.1 和最低資料平面版本為 10.2.4 的 Prisma Access (Managed by Panorama) 部署<br>❑ Colo-Connect 附加元件授權 |

Prisma Access Colo-Connect 包含下列元件：

- Col@@ **o**—一種託管設施，可提供機架空間、電源和連線，以託管網路、私人和公共雲端基礎結構（例如 Equinix）。
- 專用互連—您路由器與給定 GCP 計算區域中 GCP 邊緣路由器之間的專用第二層或第三層實體連線。專用互連可在內部部署網路與 Google 網路之間提供直接實體連線。

  互連在 Prisma Access UI 中稱為連結。
- **GCP VLAN** 附件—透過連結的邏輯第二層連線，此連結會將流量與共用相同連結的任何其他邏輯連線分開。

  VLAN 附件在 Prisma Access UI 中稱為連線。
- 合作夥伴互連—服務提供者自有路由器與給定 GCP 計算區域中 GCP 邊緣路由器之間的第三層實體連線。合作夥伴互連可透過支援的服務提供者，提供您的內部部署與 VPC 網路之間的連線。

  Colo-Connect 同時支援專用互連和合作夥伴互連。
- **Colo (**客戶**)** 路由器—Colo 設施中的路由裝置，其會透過 Colo 設施中的互連與 GCP 雲端路由器建立 eBGP，以及透過 GRE 通道與 Colo-Connect 服務連線建立 eBGP。對於專用互連，或者如果服務提供者透過合作夥伴互連，與 GCP 具有第二層連線，它是客戶路由器。當服務提供者與 GCP 雲端路由器具有第三層連線時，其擁有 Colo 路由器。
- **GCP** 邊緣路由器—GCP 的網路邊緣設備，可通過 Colo 在 GCP 與客戶/合作夥伴網路之間提供實體連線。
- 雲端路由器—雲端中的 GCP 軟體構建，其會在 Prisma Access 與您網路之間的 Colo 和路由器流量中與網路裝置（例如，路由器或第三層防火牆）建立 BGP 工作階段。您不需要設定此元件；此設定是由 Prisma Access 自動完成。

若要設定 Colo-Connect，您必須先收集有關現有網路環境的資訊，並確定所有必要的網路元件都已到位。確保您具有所有先決條件；然後，使用合作夥伴或專用互連，在您組織的網路中部署 Colo-Connect。

- Strata Cloud Manager
- Panorama


©2025 Palo Alto Networks, Inc.

# 設定 Prisma Access Colo-Connect (Strata Cloud Manager)

若要設定 Colo-Connect，首先您必須收集有關現有網路環境的資訊，並確定所有必要的網路元件到位。確保您擁有所有先決條件；然後使用合作夥伴或專用互連，在您組織的網路中部署 Colo-Connect。

## 使用合作夥伴互連設定 Prisma Access Colo-Connect—部署

若要使用 合作夥伴互連設定 Prisma Access Colo-Connect，請完成以下步驟。

**STEP 1 |** 為您的 Colo-Connect 連線建立子網路。

您可以在後續步驟中建立的連線和服務連線中使用您在這裡建立的子網路。

1. 從 Strata Cloud Manager 中，前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Colo-Connect**。
2. **Add Prefix**（新增首碼），並為其新增 Colo-Connect 子網路和 Prisma Access 位置。

   請在這裡查看支援的 colo-connect 位置清單。輸入至少 /28 的子網路。
3. （選用）如果您計劃為多個位置建立 Colo-Connect 執行個體，請根據每個位置新增更多子網路。

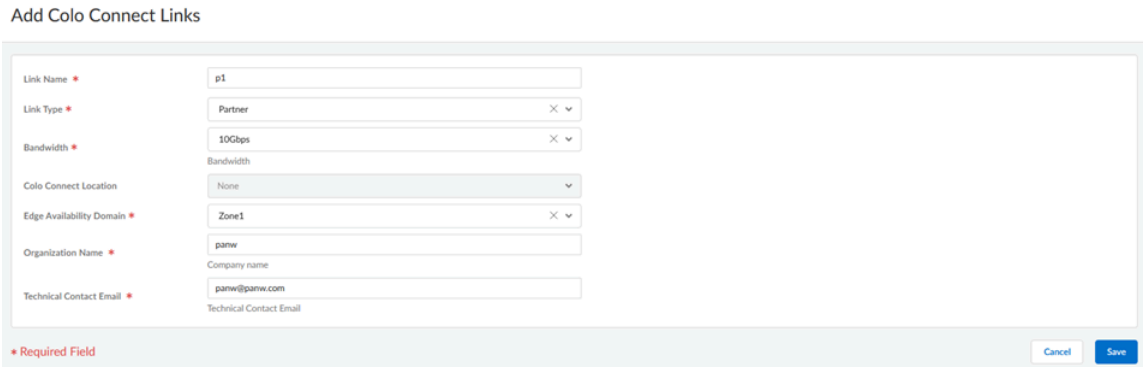
   您可以設定每個位置一個子網路。




 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 新增 Colo-Connect 連結（也稱為互連）。

1. 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Colo-Connect** 和 **Add Link**（新增連結）。
2. 給與連結唯一的 **Link Name**（連結名稱）。
3. 選取 **Partner**（合作夥伴）互連作為 **Link Type**（連結類型）。
4. 指定剩餘的 Colo-Connect 連結參數。
   - 選取 **10Gbps** 或 **20Gbps** 作為 **Bandwidth**（頻寬）。
   - 選取 **Zone1** 或 **Zone2** 作為 **Edge Availability Domain**（邊緣可用性網域）。從用於邊緣可用性網域的 GCP 區域中取得此值。
   - 輸入要用於此連結的 **Organization Name**（組織名稱）。
   - 輸入要用於此連結的 **Email**（電子郵件）。任何電子郵件地址都可以接受。




5. 重複步驟 2.a, 2.d, 並使用不同的 **Edge Availability Domain**（邊緣可用性網域）建立另一個連結。


©2025 Palo Alto Networks, Inc.

**STEP 3 |** 建立 Colo-Connect 的連線（也稱為 *VLAN* 附件）。

1. 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Colo-Connect** 和 **Add Connection**（新增連線）。
2. 進行連線設定。
   - 輸入唯一的 **Connection Name**（連線名稱）。
   - 從您在上一個步驟中設定的連結中選取 **Link Name**（連結名稱）。

     您不需要輸入 **VLAN ID**；無法針對在合作夥伴互連上建立的 VLAN 進行設定。
   - 選取連線的 **Bandwidth**（頻寬）。

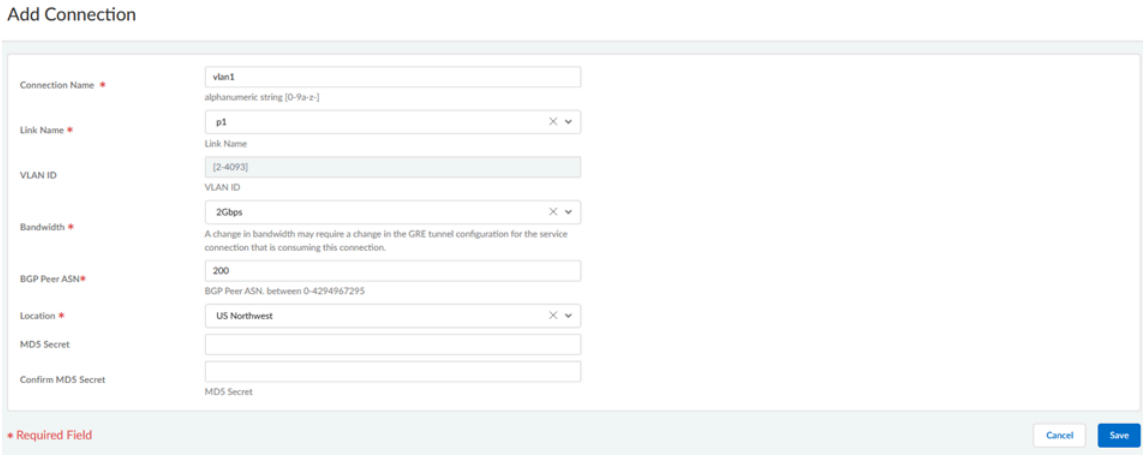
     您可以在 **1 Gbps**、**2 Gbps**、**5 Gbps**、**10 Gbps** 或 **20 Gbps** 之間選取。

     如果設定多個連線進行互連，請確定連線的總頻寬不超過互連的頻寬。例如，若合作夥伴互連為 10 Gbps，您可以設定 10 個連線，每個連線為 1 Gbps，但所有連線總共不得超過 10 Gbps。

     如果您的部署需要超過 *16* 個連線，請聯繫您的 *Palo Alto Networks* 客戶團隊，他們將開啟 *SRE* 案例以滿足要求。
   - 輸入 **BGP Peer ASN**（**BGP** 對等 **ASN**）。

     在 Colo 中輸入客戶內部部署路由器的自發系統 (AS) 編號。範圍介於 1 與 4294967295 之間。
   - 從您在上一個步驟中建立的連線名稱中選取 **Location**（位置）。

     您必須已為指定的任何位置新增子網路。
   - （選用）輸入 BGP **MD5 Secret**（**MD5** 密碼）。




3. 繼續建立連線，直到完成。

   建立兩個連線。這兩個連線都必須位於相同的區域中，而每個連線都必須位於單獨的區域中。您會在後續步驟中建立的服務連線中使用這些連線。

**STEP 4 |** **Push Config**（推送設定）。

在提交工作完成後重新整理瀏覽器，以檢視 **Connections**（連線）下的配對金鑰。

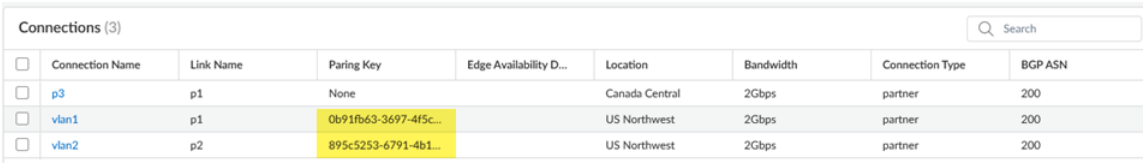
 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** 擷取 **Pairing Key**（配對金鑰），並在 GCP 中完成您的合作夥伴互連設定。

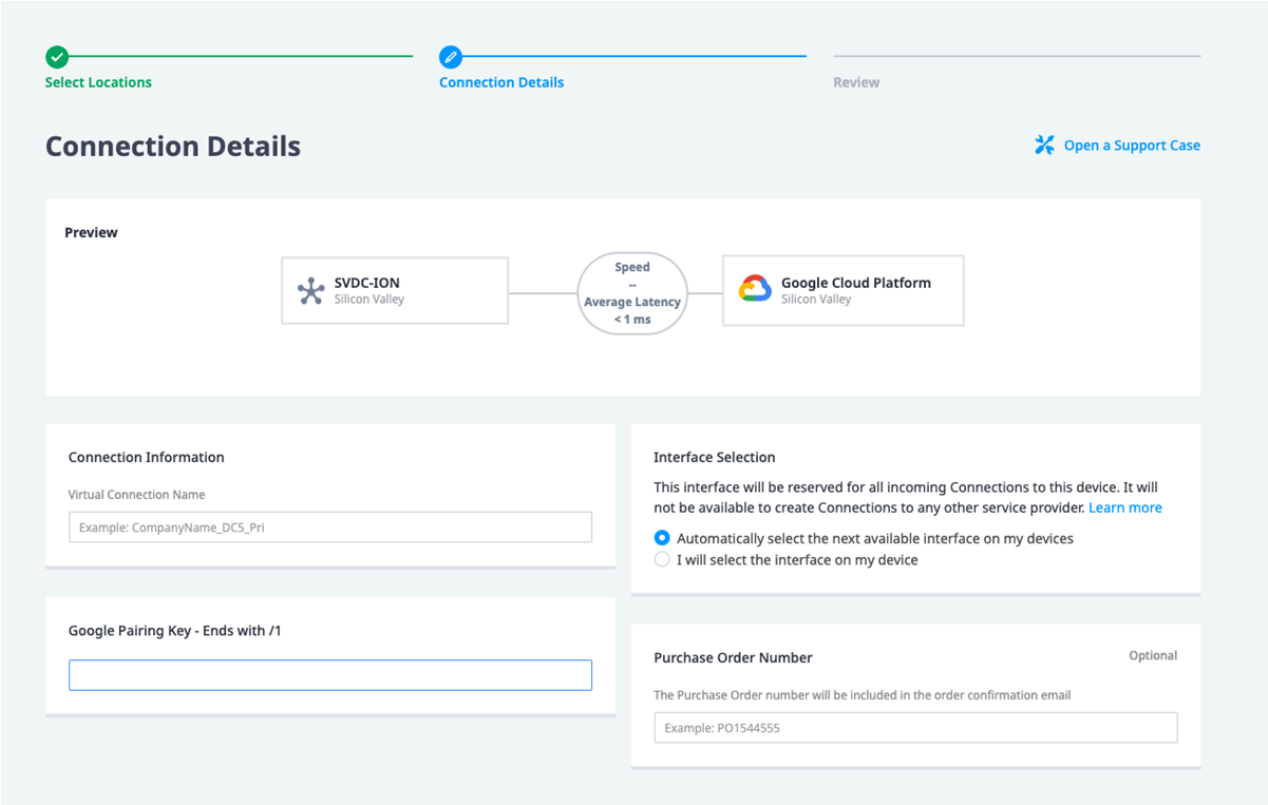
在 Colo 中設定合作夥伴互連時，您會使用此配對金鑰。

當您第一次裝載新連線時，**Connections**（連線）區域中的 **Status**（狀態）會將 **Status**（狀態）顯示為 **PENDING_PARTNER**，以及將 **BGP Status**（**BGP** 狀態）顯示為 **DOWN**（關閉）。若要將連線狀態帶至 **ACTIVE**（作用中），請擷取配對金鑰並在 Colo 的連線中輸入。

1. 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Colo-Connect** > **Connections**（連線），並複製 **Pairing Key**（配對金鑰）。




2. 在 Colo 中建立新的 VLAN 連線。




3. 在 Colo VLAN 中貼上配對金鑰。

GCP 會偵測何時耗用配對金鑰、將 VLAN 狀態帶至 **ACTIVE**（作用中），並產生 BGP IP 位址，讓您在 Colo 內部部署路由器上進行設定。Prisma Access 會使用這些 IP，在 Colo 路由器與 GCP 雲端路由器之間透過每個關聯的 VLAN 啟動 eBGP 相鄰項。

**STEP 6 |** 在客戶 (Colo) 路由器上建立 eBGP 路由，進行 Colo-Connect 連線。

您需要設定 BGP 對等，以確保客戶路由器與雲端路由器之間的連線。

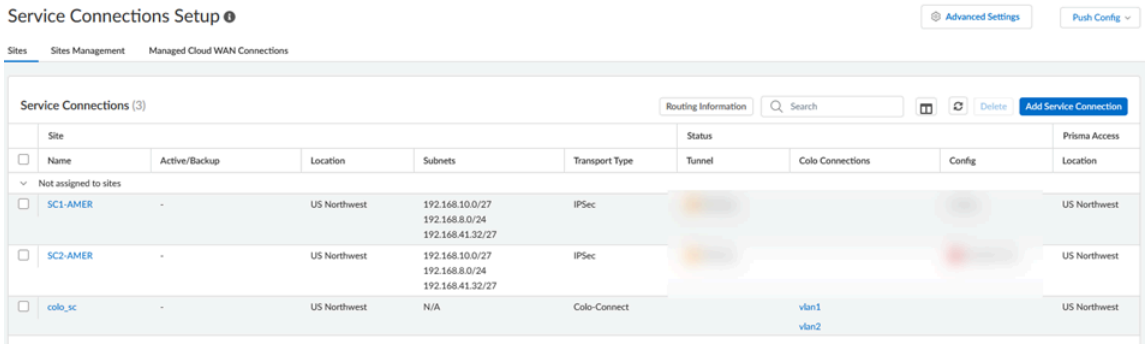
**STEP 7 |** 設定服務連線以與 Colo-Connect 搭配使用。


©2025 Palo Alto Networks, Inc.

**STEP 8 |** **Push Config**（推送設定）。

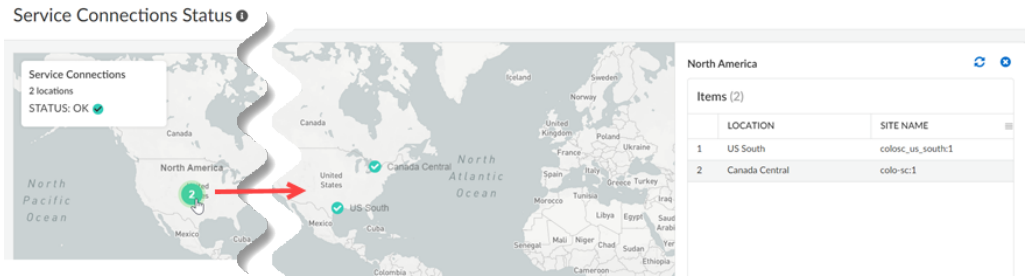
**STEP 9 |** 檢查 Colo-Connect 連線的狀態。

1. 若要檢查 Colo-Connect 連線所使用的服務連線狀態，請前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Service Connection**（服務連線）。




2. 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**）。將 **Configuration Scope**（設定範圍）設定為 **Prisma Access**。在 Prisma Access 同步狀態下，選取 **Service Connections**（服務連線）的 **In Sync**（同步）狀態。選取已部署 Colo-Connect 連線的區域。

   - 如果 Colo-Connect 連線和 BGP 路由都已啟動，狀態會顯示 **OK**（成功）。
   - 如果 Colo-Connect 連線已啟動，但 BGP 路由未啟動，狀態會顯示 **Warning**（警告）。
   - 如果 Colo-Connect 連線和 BGP 路由都已關閉，狀態會顯示 **Down**（關閉）。
   - 如果 Colo-Connect 連線關閉，但 BGP 路由已啟動，狀態會顯示 **Error**（錯誤）。




3. 如需詳細資訊，請按一下區域方塊，然後檢視 **Status**（狀態）頁籤中的資訊。

**STEP 10 |** 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Colo Connect**，檢查 Colo-Connect 連線的連線詳細資訊，包括配對金鑰。

## 使用專用互連設定 Prisma Access Colo-Connect—部署

若要使用 專用互連設定 Prisma Access Colo-Connect，請完成以下步驟。


©2025 Palo Alto Networks, Inc.

**STEP 1 |** 為您的 Colo-Connect 連線建立子網路。

您可以在後續步驟中建立的連線和服務連線中使用您在這裡建立的子網路。

1. 從 Strata Cloud Manager 中，前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Colo-Connect**，然後按一一下齒輪圖示以編輯設定。
2. 為 **Colo-Connect Subnet**（**Colo-Connect** 子網路）**Add Prefix**（新增首碼），並為它選取 Prisma Access 位置（**PA Location**（**PA** 位置））。

   輸入至少 /28 的子網路。
3. （選用）如果您計劃為多個位置建立 Colo-Connect 執行個體，請根據每個位置新增更多子網路。

   每個位置只能設定一個子網路。

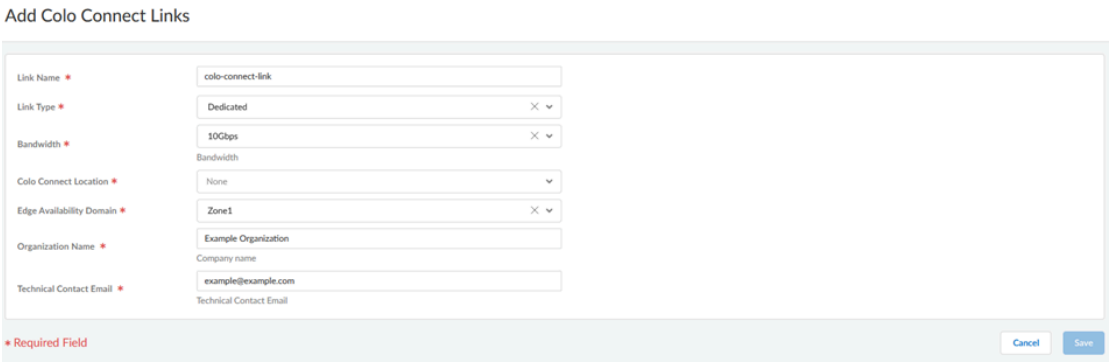
**STEP 2 |** 新增 Colo-Connect 連結（也稱為互連）。

1. 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Colo-Connect** 和 **Add Link**（新增連結）。
2. 給與連結唯一的 **Link Name**（連結名稱）。
3. 選取 **Dedicated**（專用）互連作為 **Link Type**（連結類型）。
4. 指定剩餘的 Colo-Connect 連結參數。
   - 選取 **10Gbps** 或 **20Gbps** 作為 **Bandwidth**（頻寬）。

     如果您選取 *20 Gbps*，則必須使用 LACP 將專用互連連結彙總為兩個 *10 Gbps* 連結。

     在指定專用互連連結的頻寬，且提交並推送您的變更之後，您就無法變更該頻寬。
   - 從下拉式清單中選取 **Colo-Connect Location**（**Colo-Connect** 位置）。

     請確定您選取用於專用互連的同一位置。
   - 選取 **Zone1** 或 **Zone2** 作為 **Edge Availability Domain**（邊緣可用性網域）。從用於邊緣可用性網域的 GCP 區域中取得此值。
   - 輸入要用於此連結的 **Organization Name**（組織名稱）。
   - 輸入您要從雲端提供者接收 LOA-CFA 詳細資料的 **Email**（電子郵件）。
     - GCP 會使用此電子郵件傳送授權書和連線設施指派 (LOA-CFA)。請確定 LOA-CFA 傳送給您的 Colo 提供者，以便他們可以開始安裝您的連線。




 ©2025 Palo Alto Networks, Inc.

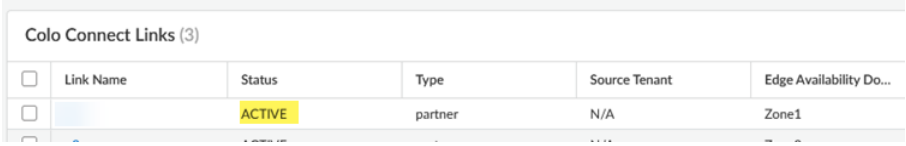
**STEP 3 |** 在建立專用連線之後，Colo 設施會測試您的連線，並通知您它們已測試且可供使用。

此步驟不需要任何 Prisma Access 設定。在 Colo 設施讓您知道它們已測試之前，請勿在 Prisma Access 中建立 Colo-Connect 連線。


©2025 Palo Alto Networks, Inc.

**STEP 4 |** 建立 Colo-Connect 的連線（也稱為 *VLAN* 附件）。

1. 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Colo-Connect** > **Colo Connect Links**（**Colo Connect** 連結），確定專用連結狀態為 [Active（作用中）]。
   在專用連結狀態為 [Active（作用中）] 之前，您無法建立 Colo-Connect 連結。




2. 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Colo-Connect** 和 **Add Connection**（新增連線）。
3. 進行連線設定。
   - 輸入連線的唯一 **Name**（名稱）。
   - 從您在上一個步驟中設定的連結中選取 **Link Name**（連結名稱）。
   - （選用） 輸入連線的 **VLAN ID**。

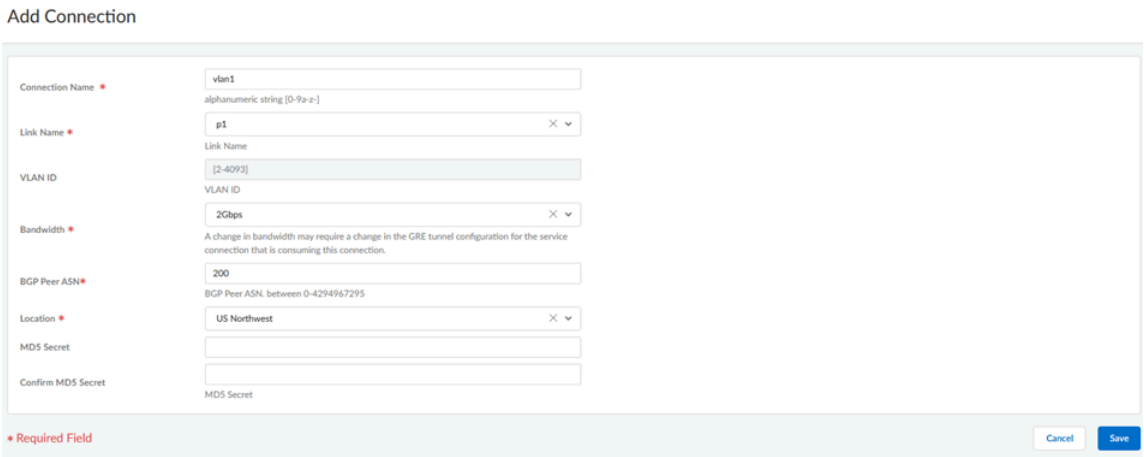
     如果您沒有手動輸入一值，則互連廠商 (GCP) 會產生 VLAN ID。
   - 選取連線的 **Bandwidth**（頻寬）。

     您可以在 **1 Gbps**、**2 Gbps**、**5 Gbps**、**10 Gbps** 或 **20 Gbps** 之間選取。

     如果設定多個連線進行互連，請確定連線的總頻寬不超過互連的頻寬。例如，若專用互連為 20 Gbps，您可以設定 10 個連線，每個連線為 2 Gbps，但所有連線總共不得超過 20 Gbps。
   - 輸入 **BGP Peer ASN**（**BGP** 對等 **ASN**）。

     在 Colo 中輸入客戶內部部署路由器的自發系統 (AS) 編號。範圍介於 1 與 4294967295 之間。
   - 從您在上一個步驟中建立的連線名稱中選取 **Location**（位置）。

     您必須已為指定的任何位置新增子網路。
   - （選用）輸入 BGP **MD5 Secret**（**MD5** 密碼）。




4. 繼續建立連線，直到完成。

 ©2025 Palo Alto Networks, Inc.

建立兩個連線。這兩個連線都必須位於相同的區域中，而每個連線都必須位於單獨的區域中。您會在後續步驟中建立的服務連線中使用這些連線。

**STEP 5 |** **Push Config**（推送設定）。

**STEP 6 |** 在客戶路由器上設定 eBGP 路由。

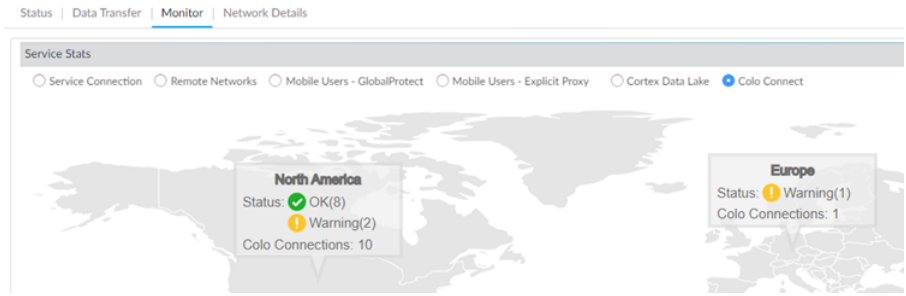
您需要設定 BGP 對等，以確保客戶路由器之間的連線。

**STEP 7 |** 設定服務連線以與 Colo-Connect 搭配使用。

**STEP 8 |** **Commit and Push**（提交並推送）您的組態變更，確保在 **Push Scope**（推送範圍）中選取了 **Colo-Connect**。

**STEP 9 |** 檢查 Colo-Connect 連線的狀態。

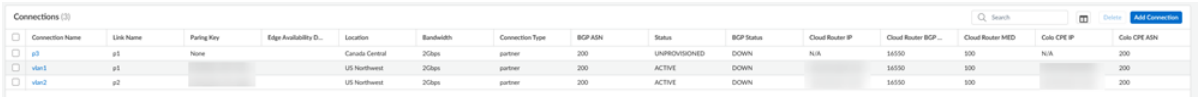
1. 若要檢查 Colo-Connect 連線所使用的服務連線狀態，請前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**）。將 **Configuration Scope**（設定範圍）設定為 **Prisma Access**。
2. 將游標暫留在已部署 Colo-Connect 連線的區域上。
   - 如果 Colo-Connect 連線和 BGP 路由都已啟動，狀態會顯示 **OK**（成功）。
   - 如果 Colo-Connect 連線已啟動，但 BGP 路由未啟動，狀態會顯示 **Warning**（警告）。
   - 如果 Colo-Connect 連線和 BGP 路由都已關閉，狀態會顯示 **Down**（關閉）。
   - 如果 Colo-Connect 連線關閉，但 BGP 路由已啟動，狀態會顯示 **Error**（錯誤）。




3. 如需詳細資訊，請按一下區域方塊，然後檢視 **Status**（狀態）頁籤中的資訊。

**STEP 10 |** 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Colo-Connect** > **Connections**（連線），並檢視詳細資訊，來檢查 Colo-Connect 連線的網路詳細資訊。

對於專用連結，**Pairing Key**（配對金鑰）會顯示為 **N/A**。



## 在客戶路由器上設定 VLAN eBGP 路由

在部署的下列階段期間，GCP 會為客戶 (Colo) 路由器和雲端路由器建立 IP 位址：

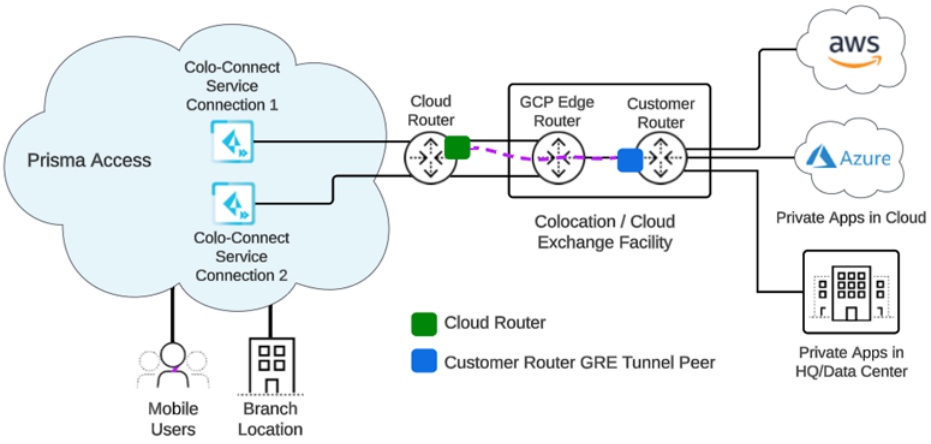
 ©2025 Palo Alto Networks, Inc.

- 對於合作夥伴互連，GCP 會在您的 Colo（例如，Equinix）耗用配對金鑰之後建立 IP 位址。
- 對於專用互連，GCP 會在您裝載 Colo-Connect 連線（VLAN 附件） 且提交並推送您的變更之後建立 IP 位址。

若要確保正確的路由，您必須：

- 將 Colo 路由器 IP 位址（Prisma Access 中的 **Colo CPE IP**）設定為本機 eBGP IP 位址
- 將雲端路由器 IP 位址（**Cloud Router IP**（雲端路由器 **IP**））設定為 Colo 路由器上的 eBGP 對等地址。

完成時，會針對 Colo 路由器與雲端路由器之間的連線（VLAN 附件）設定 eBGP。




建立此路由是設定 GRE 通道路由的第一步。在服務連線設定期間設定 GRE 通道時，您會完成 GRE 通道路由。

使用下列步驟來設定 Colo 與雲端路由器之間的路由。

**STEP 1 |** 從 Strata Cloud Manager 中，建立子網路、連結和連線，然後 **Push Config**（推送設定）。

使用互連類型特定的工作流程（合作夥伴或專用）對於合作夥伴互連，請確定已將配對金鑰貼入 Colo VLAN 中。

**STEP 2 |** 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Colo-Connect** > **Connection**（連線）。

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 請記下列連接元素：

- **Colo CPE IP**
- 雲端路由器 **IP**
- 雲端路由器 **BGP ASN**

在下列範例中：

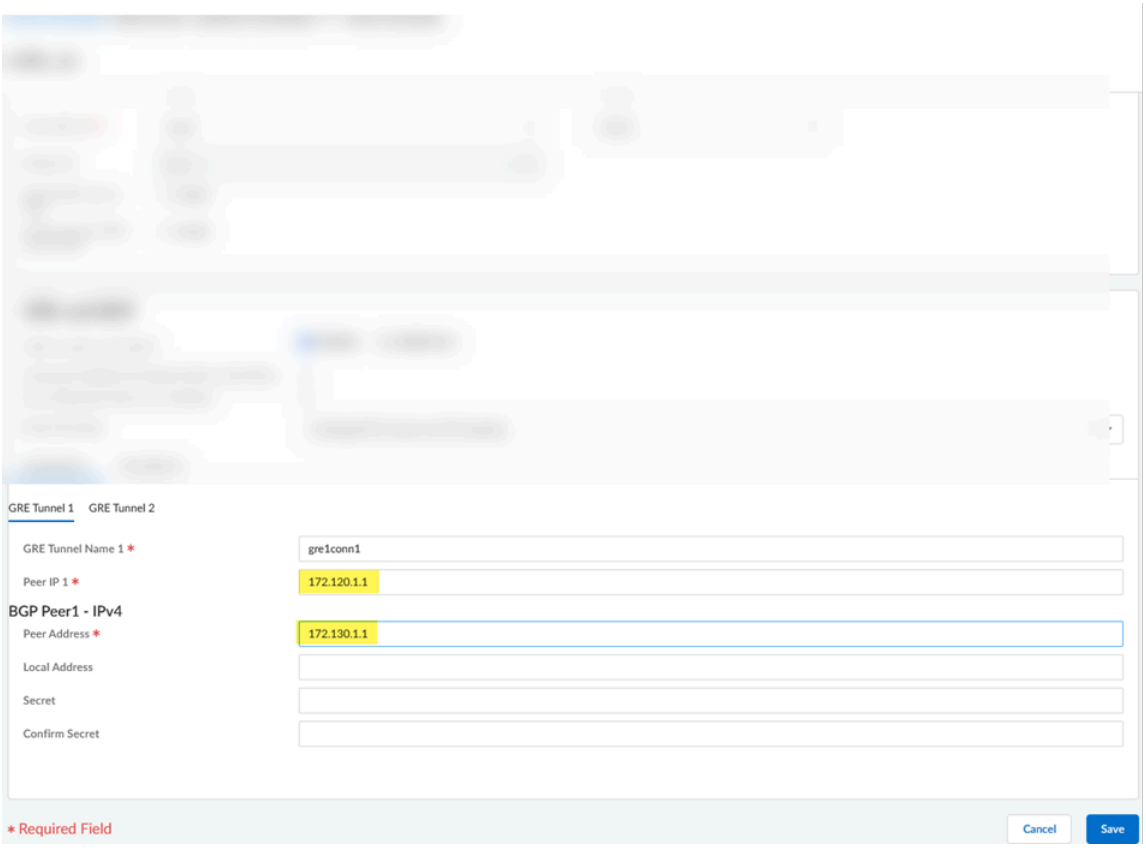
- 對於 vlan-central-1 連線，**Colo CPE IP** 是 169.254.24.170/29、**Cloud Router IP**（雲端路由器 **IP**）是 169.254.24.169/29，而 **Cloud Router BGP ASN**（雲端路由器 **BGP ASN**）是 16550
- 對於 vlan-central-2 連線，**Colo CPE IP** 是 169.254.120.74/29、**Cloud Router IP**（雲端路由器 **IP**）是 169.254.120.73/29，而 **Cloud Router BGP ASN**（雲端路由器 **BGP ASN**）是 16550。
- .




 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 確定您在設定 Colo-Connect 服務連線時將用於本機 GRE IP 位址的 IP 位址。

設定 Colo-Connect 服務連線（**Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Service Connections**（服務連線））時，您可以進行這些設定。在 **Peer IP 1**（對等 **IP 1**）和（如果需要）**Peer IP 2**（對等 **IP 2**）區域中。




如果您要設定服務連線以支援最高 10 Gbps 輸送量，請在 **Connection 1**（連線 **1**）和 **Connection 2**（連線 **2**）中每個放置一個通道，而每個服務連線總共有兩個通道。

如果您要設定服務連線以支援 10 Gbps 以上的輸送量（最高 20 Gbps），請在 **Connection 1**（連線 **1**）和 **Connection 2**（連線 **2**）中每個放置兩個通道，而每個服務連線總共有四個通道。

下列範例顯示一個要為 10 Gbps 以上輸送量設定的通道，因此使用每個連線兩個通道，並且它們會使用下列對等 IP 位址：

- 172.120.1.1 用於連線 1
- 172.130.1.1 用於連線 1
- 172.121.1.1 用於連線 2
- 172.131.1.1 用於連線 2

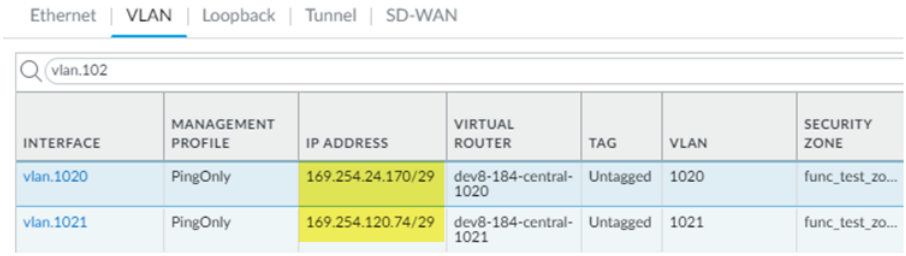
**STEP 5 |** 登入 Colo 路由器。

下列設定螢幕擷取畫面使用 Palo Alto Networks 新世代防火牆作為 Colo 路由器。

 ©2025 Palo Alto Networks, Inc.

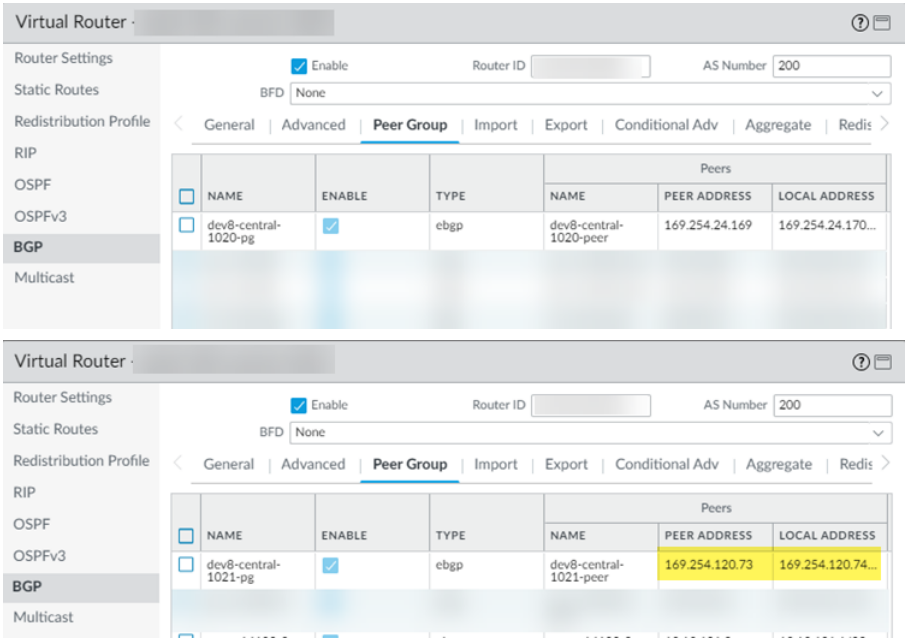
**STEP 6 |** 新增 VLAN 介面，指定 **Colo CPE IP** 位址作為 IP 位址。

如果您是使用新世代防火牆作為 Colo 路由器，請前往 **Network**（網路） > **Interfaces**（介面） > **VLAN**，然後 **Add**（新增） VLAN 介面，指定 **Virtual Router**（虛擬路由器），並




**STEP 7 |** 將 Colo 路由器 IP 位址 (**Colo CPE IP**) 設定為本機 eBGP IP 位址，並將雲端路由器 IP 位址（**Cloud Router IP**（雲端路由器 **IP**）） 設定為 Colo 路由器上的 eBGP 對等位址。

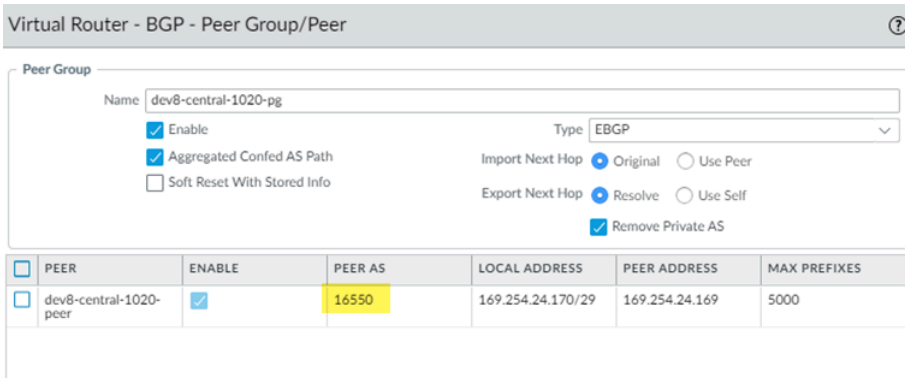
如果您是使用新世代防火牆作為 Colo 路由器，請前往 **Network**（網路） > **Virtual Routers**（虛擬路由器）、**Add**（新增）虛擬路由器、前往 **BGP** > **Peer Group**（對等群組），然後輸入 **Colo CPE IP** 作為 **Peer Address**（對等位址），以及 **Cloud Router IP**（雲端路由器 **IP**）作為 **Local Address**（本機位址）。




 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** 將 **Cloud Router BGP ASN**（雲端路由器 **BGP ASN**）設定為 eBGP 對等自發系統編號 (ASN)。

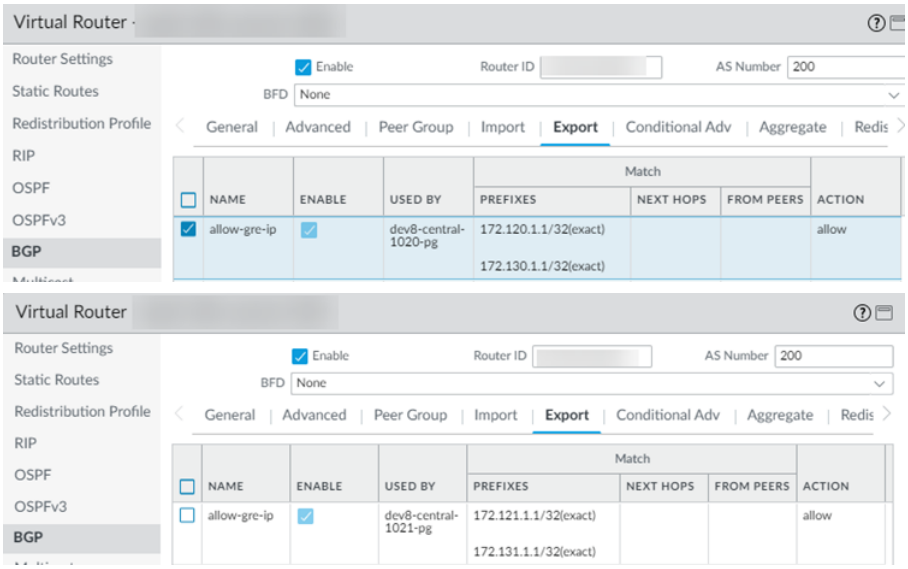
如果您是使用新世代防火牆作為 Colo 路由器，請前往 **Network**（網路） > **Virtual Routers**（虛擬路由器）、**Add**（新增）虛擬路由器、前往 **BGP** > **Peer Group**（對等群組）、**Add**（新增）對等群組，然後選取 **Peer AS**（對等 **AS**）為 **16500**。




**STEP 9 |** 建立一個 BGP 匯出政策，只允許本機 GRE IP 位址公告到雲端路由器對等 IP 位址。

因為雲端路由器只能接收有限數目的路由，所以您需要建立政策，以便只有服務連線 GRE 通道的 IP 位址之間的路由會傳送到雲端路由器。

如果您是使用新世代防火牆作為 Colo 路由器，請前往 **Network**（網路） > **Virtual Routers**（虛擬路由器）、**Add**（新增）虛擬路由器、前往 **BGP** > **Export**（匯出）、**Add**（新增）匯出規則、**Match**（比對）用作對等 IP 位址的 IP 位址，然後建立 **Allow**（允許） **Action**（動作）.。




**STEP 10 |** 建立 Colo-Connect 服務連線。

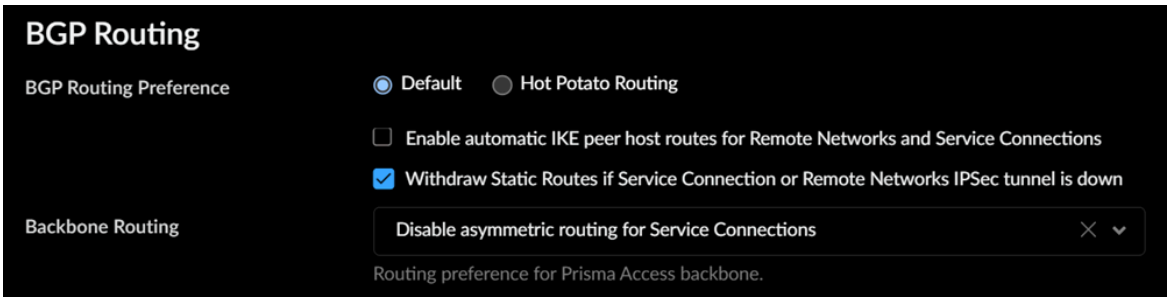
## 建立 Colo-Connect 服務連線

Colo-Connect 使用服務連線，但它們與Prisma Access服務連線不同，因為它們使用 GRE 通道而不是 IPsec 通道，並一律使用 BGP 進行路由。若要設定 Colo-Connect 服務連線，請完成下列步驟。


©2025 Palo Alto Networks, Inc.

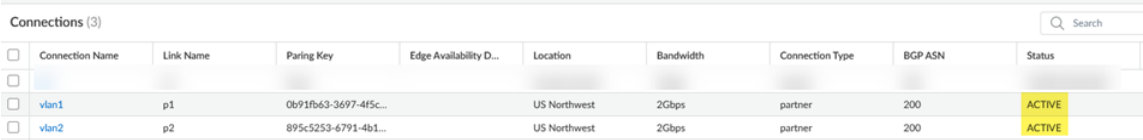
**STEP 1 |** 確定 Prisma Access 撤銷靜態路由，方法是前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Service Connections**（服務連線） > **Advanced Settings**（進階設定），然後選取 **Withdraw Static Routes if Service Connection or Remote Network IPSec tunnel is down**（如果服務連線或遠端網路 **IPSec** 通道關閉，則撤銷靜態路由）。

選取此選項可確保如果 GRE 通道關閉，GRE 通道使用的靜態路由會被撤銷。




**STEP 2 |** 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Colo-Connect** > **Connections**（連線），然後透過檢查連線的 **Status**（狀態），確保連線處於 **Active**（作用中）狀態。

在連線的 **Status**（狀態）為 **Active**（作用中）之前，您無法設定服務連線。

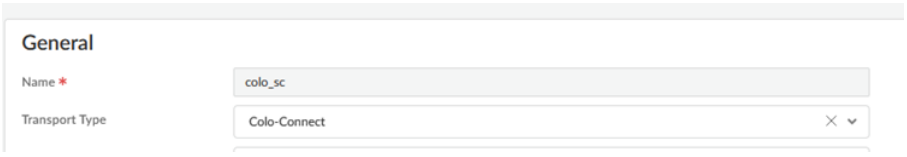



**STEP 3 |** 前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**），然後將設定範圍設定為 **Prisma Access**。

**STEP 4 |** 重新整理 **Prisma Access Sync Status**（**Prisma Access** 同步狀態），以便 Colo-Connect 設定佈建在服務連線區域中。

**STEP 5 |** 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Service Connection**（服務連線）、**Add Service Connection**（新增服務連線）、給與它唯一 的 **Name**（名稱），然後選取 **Transport Type**（傳輸類型）為 **Colo-ConnectColo-Connect**。

請確定您輸入的名稱長度為 *31* 個字元或以下；輸入 *32* 個字元或更長的名稱會導致通道在 *Prisma Access* 基礎結構中對應不正確。




 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** 選取要與服務連線搭配使用的兩個連線（**Connection 1**（連線 **1**）和 **Connection 2**（連線 **2**））。

這些連線必須位於兩個不同的區域中。




**STEP 7 |** 為 **Connection 1**（連線 **1**）和 **Connection 2**（連線 **2**）選取 **Active**（作用中）或 **Backup**（備份）

設定服務連線時，請使用下列準則：

- 您可以在下列模式下設定連線：
  - **Active**（主動）**/Active**（主動）
  - **Active**（作用中）**/Backup**（備份）
  - **Backup**（備份）**/Active**（作用中）

  在 **Backup**（備份）**/Backup**（備份）模式下設定兩個連線無效且不受支援。
- 所有模式的連線頻寬必須相同。
- 連線必須位於不同的區域中。
- 您可以為服務連線指定的頻寬上限為 20 Gbps。如果您為連線指定 **20 Gbps** 的 **Bandwidth**（頻寬），則無法在 **Active**（主動）**/Active**（主動）設定中使用該連線（必須設定為 **Active**（作用中）**/Backup**（備份））。
- 請勿在同一服務連線中混合專用和合作夥伴互連，並確保服務連線使用不同的區域。此表格顯示服務連線的允許和不允許設定，假設區域、位置、頻寬和角色遵循服務連線指導方針和需求：

| 連線 **1** 屬於 | 連線 **2** 屬於 | 有效的 **Colo-Connect** 服務連線設定？ |
|---|---|---|
| 合作夥伴連線 1 | 合作夥伴連線 2 | 是 |
| 專用連線 1 | 專用連線 2 | 是 |
| 合作夥伴連線 1 | 合作夥伴連線 1 | 否 |
| 專用連線 1 | 專用連線 1 | 否 |
| 合作夥伴連線 | 專用連線 | 否 |

 ©2025 Palo Alto Networks, Inc.

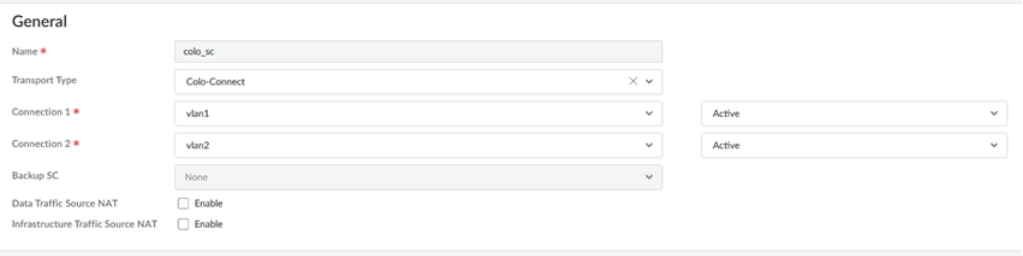
**STEP 8 |** （選用且僅適用於熱馬鈴薯路由部署）選取要在熱馬鈴薯路由設定中用作偏好備份（即 **Backup SC**（備份 **SC**））的服務連線。

您只能選取已設定為 Colo-Connect 服務連線的服務連線。在連線失敗時，Prisma Access 會使用您選取的備份 SC 作為偏好的服務連線。選取備份服務連線可以防止非對稱路由問題（如果您已建立兩個以上的服務連線）。

**STEP 9 |** （選用）為行動使用者—GlobalProtect IP 集區位址、基礎結構子網路中的 IP 位址或兩者啟用來源 NAT。

您可以在一個或多個服務連線上指定子網路，而這些連線用來在 Prisma Access GlobalProtect 行動使用者與資料中心的私人應用程式和資源之間傳送 NAT 流量。

- 啟用資料流量來源 **NAT**—對行動使用者 IP 位址集區位址執行 NAT，以便這些位址不會公告到資料中心，並且僅在資料中心公告和路由您在服務連線中指定的子網路。
- 啟用基礎結構流量來源 **NAT**—對來自基礎結構子網路的位址執行 NAT，以便它們不會公告到資料中心，並且僅在資料中心公告和路由您在服務連線中指定的那些子網路。
- **IP** 集區—指定用來對行動使用者 IP 位址集區、基礎結構子網路或兩者執行 NAT 的 IP 位址集區。使用私人 IP (RFC 1918) 子網路，或可在路由網域中路由的適合子網路，且不與行動使用者—GlobalProtect IP 位址集區或基礎架構子網路重疊。輸入介於 /25 和 /32 之間的子網路。




**STEP 10 |** 在 **GRE and BGP**（**GRE** 和 **BGP**）區域中，設定服務連線的 GRE 通道和 BGP 設定。

BGP 一律設定為 **Enable**（啟用）。

1. （選用）從下列選項中選取：

   - 若要將公司存取節點（服務連線）的 **no-export**（無匯出）社群新增到來自客戶周邊設備 (CPE) 上 eBGP 對等的輸出首碼，請將 **Add no-export community**（新增無匯出社群）設定為 **Enabled Out**（已啟用輸出）。預設會 **Disabled**（停用）此功能。

     請勿在熱馬鈴薯路由模式下使用此功能。

   - 若要減少透過 BGP 公告至客戶周邊設備 (CPE) 的行動使用者 IP 子網路公告數目，請選取**Summarize Mobile User Routes before advertising**（公告前彙總行動使用者路由。

     根據預設，Prisma Access 會在 /24 子網路區塊中公告行動使用者 IP 位址集區；如果你彙總它們，Prisma Access 根據您指定的子網路公告該集區。例如，Prisma Access 使用 /20 子網路公告 10.8.0.0/20 的公用使用者行動 IP 集區，而不是先將該集區劃分為 10.8.1.0/24、10.8.2.0/24、10.8.3.0/24 等子網路，再公告它們。彙總這些公告可

 ©2025 Palo Alto Networks, Inc.

以減少 CPE 路由表中儲存的路由數目。例如，您可以使用 IP 集區彙總，搭配可接受有限數目路由的雲端 VPN 閘道（虛擬私人閘道 (VGW) 或傳輸閘道 (TGW)）。

如果您已啟用熱馬鈴薯路由並啟用路由彙總，則*Prisma Access* 不再前置 *AS-PATH*，這可能會導致非對稱路由。在使用熱馬鈴薯路由來啟用路由彙總之前，請確保從資料中心或總部位置傳回的流量已保證對稱傳回。

- 防止 Prisma Access BGP 對等將路由轉送至您組織的網路。**Don't Advertise Prisma Access Routes**（請勿公告 **Prisma Access** 路由）。

  根據預設，Prisma Access 會公告所有 BGP 路由訊息，包括本機路由以及從其他服務連線、遠端網路和行動使用者子網路接收的所有首碼。選取此核取方塊可防止 Prisma Access 傳送任何 BGP 公告，但仍會使用其收到的 BGP 資訊，來了解其他 BGP 芳鄰的路由。

  自從 *Prisma Access* 不傳送 *BGP* 公告後，如果您選取此選項，則必須在內部部署設備上設定靜態路由，以建立回到 *Prisma Access* 的路由。

- 什麼是「路由交換」設定？

2. 使用 GRE 通道設定服務連線路由。
3. 從 Strata Cloud Manager中，返回 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Service Connection**（服務連線）**Connection 1**（連線 **1**） 的 GRE 通道，方法為輸入 **Connection 1**（連線 **1**）的 **GRE Tunnel Name 1**（**GRE** 通道名稱 **1**）和 **Peer IP 1**（對等 **IP 1**），並且如果需要 10 Gbps 以上的頻寬，則輸入連線

 ©2025 Palo Alto Networks, Inc.

1 第二個通道的 **GRE Tunnel Name 2**（**GRE** 通道名稱 **2**）和 **Peer IP 2**（對等 **IP 2**）；然後，重複這些相同步驟建立 **Connection 2**（連線 **2**）的 GRE 通道。

連線中的每對 GRE 通道最多支援 10 Gbps 的頻寬。如果您需要 10 Gbps 以上的頻寬，請設定每個連線兩個通道。例如：

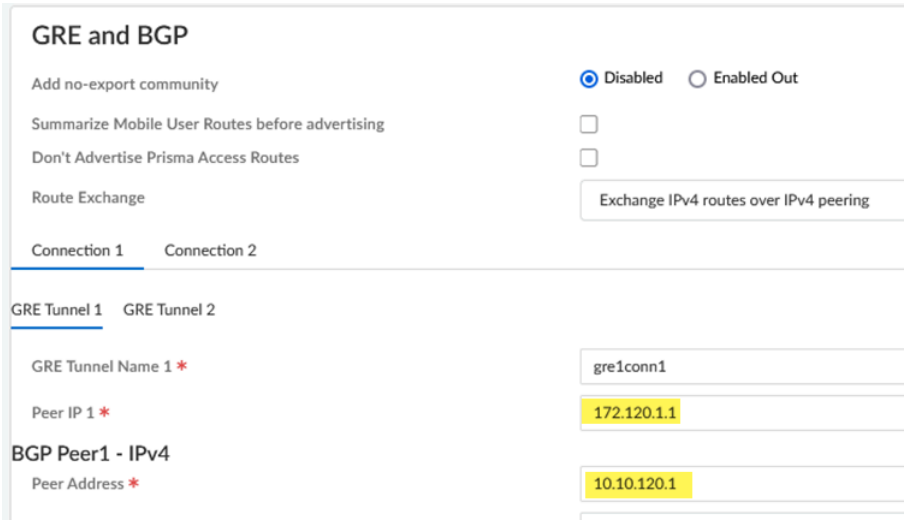
對於對等 IP，請在 Colo 中輸入內部部署路由器的 GRE IP 位址。

使用 IPv4 位址作為 BGP 值；不支援 IPv6。

4. 輸入 BGP 對等 1 的 **Peer Address**（對等位址）和 **Local Address**（本機位址），如果連線 1 需要第二個，則輸入 BGP 對等 2。

   對於 **Peer Address**（對等位址），輸入 Colo 路由器的 BGP 對等 IP 位址；對於 **Local Address**（本機位址），輸入將用於透過 GRE 通道建立 BGP 網路的位址。

5. （選用）若要設定 BGP 密碼，請輸入 **Secret**（密碼）和 **Confirm Secret**（確認密碼）值。

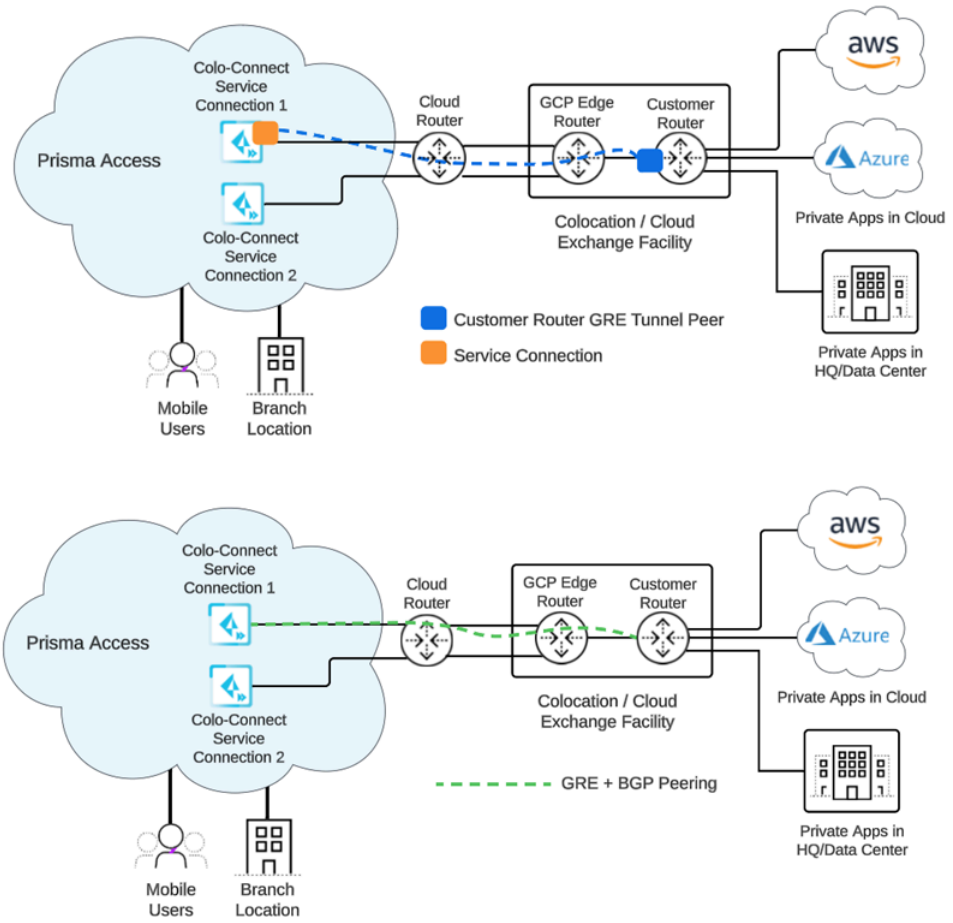



**STEP 11 |** **Commit and Push**（提交並推送）您的組態變更，確保在 **Push Scope**（推送範圍）中選取了 **Colo-Connect**。

## 使用 GRE 通道設定服務連線路由。

Colo 路由器會將其 GRE 通道對等 IP 地址公告至雲端路由器，並從雲端路由器得知 GRE 通道的子網絡。當第一次設定了透過客戶路由器上 VLAN 的 eBGP 路由，您已公告 GRE 通道的本機連線性。在雲端路由器和 Colo 路由器公告，並從彼此得知 Colo 子網路和本地 GRE IP 位址的路由之後，服務連線使用的 GRE 通道會變為作用中（啟動）。


©2025 Palo Alto Networks, Inc.




若要設定路由並將 GRE 通道新增至服務連線，請完成下列步驟。

**STEP 1 |** 記下您將為 BGP 對等 1 的 **Peer Address**（對等位址）和 **Local Address**（本機位址）使用的 IP 位址，以及如果連線 1 需要第二個，則為 BGP 對等 2。

下列範例使用下列對等和本機位址：

- **Peer Address**（對等位址）—10.10.120.0 和 10.10.130.1（用於連線 1）、10.10.120.2 和 10.10.130.2（用於連線 2）
- **Local Address**（本機位址）—10.10.120.2 和 10.10.130.2（用於連線 1）、10.10.121.2 和 10.10.131.2（用於連線 2）

**STEP 2 |** 記下您將用於 **Peer IP 1**（對等 **IP 1**）的 IP 位址，以及如果需要，則為服務連線中的 **Peer IP 2**（對等 **IP 2**）位址。

您可以使用這些 IP 位址來建立拒絕政策，防止本機 GRE IP 位址公告至 Colo-Connect 服務連線。

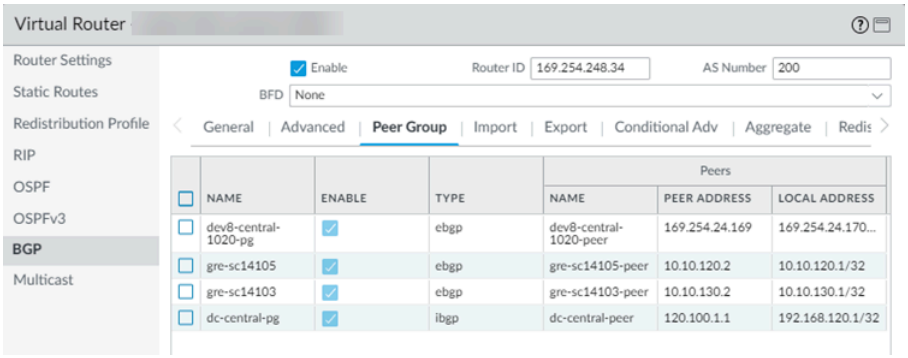
本文件中的所有範例都會使用以下 IP 位址：

- 172.120.1.1 用於連線 1
- 172.121.1.1 用於連線 2


©2025 Palo Alto Networks, Inc.

**STEP 3 |** 設定對等和本機 IP 位址的對等群組。

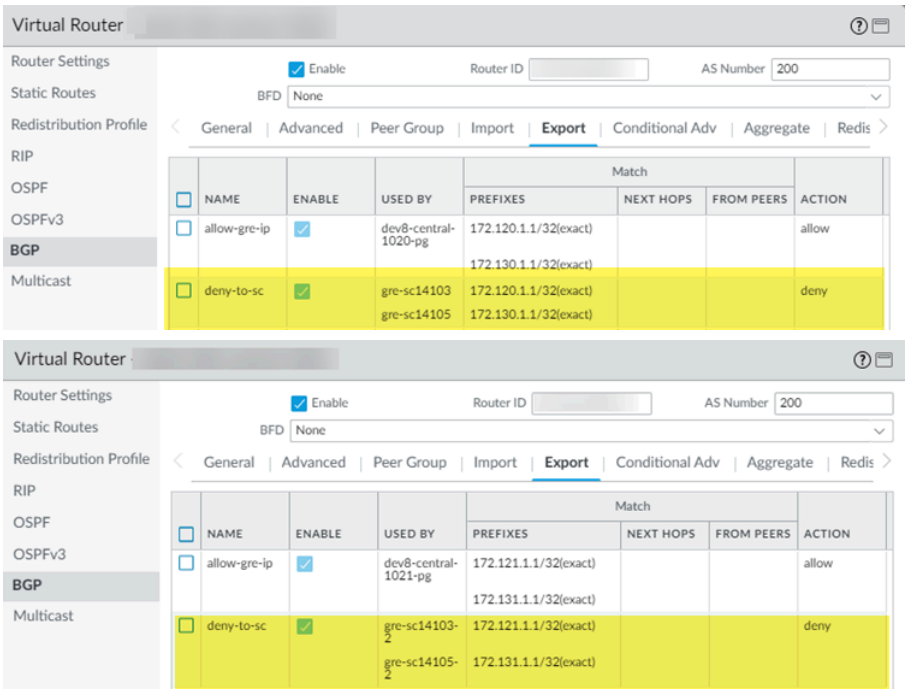
如果您是使用新世代防火牆作為 Colo 路由器，請前往 **Network**（網路） > **Virtual Routers**（虛擬路由器）、**Add**（新增）虛擬路由器、前往 **BGP** > **Peer Group**（對等群組），然後輸入對等位址作為 **Peer Address**（對等位址），以及輸入 **Local Address**（本機位址）作為 **Local Address**（本機位址）。




**STEP 4 |** 建立 BGP 匯出政策，以拒絕您設定的對等 IP 位址（172.120.1.1、172.130.1.1、172.121.1.1 和 172.131.1.1），並將它們套用至您建立的對等群組。

此匯出政策會在本機 GRE 通道對等 IP 位址上放置 DENY 規則，並允許將所有其他路由公告至服務連線。

如果您是使用新世代防火牆作為 Colo 路由器，請前往 **Network**（網路） > **Virtual Routers**（虛擬路由器）、**Add**（新增）虛擬路由器、前往 **BGP** > **Export**（匯出）、**Add**（新增）匯出規則、**Match**（比對）用作對等 IP 位址的 IP 位址，然後建立 **Deny**（拒絕） **Action**（動作）。




 ©2025 Palo Alto Networks, Inc.

## 增加或減少 Colo-Connect 服務連線的頻寬

設定服務連線時，您會根據與其相關聯的連線 (VLAN 附件) 來設定頻寬。您可以配置每個服務連線兩個連線，然後配置每個連線一個或兩個 GRE 通道。

雖然每個 Colo-Connect 服務連線最多支援 20 Gbps，但服務連線中的每個 GRE 通道都支援 10 Gbps。因此，您可能必須在 Colo-Connect 服務連接中新增或刪除 GRE 通道、變更連結中的總頻寬，這會導致服務連線頻寬高於或低於 10 Gbps。

### 增加 Colo-Connect 服務連線的頻寬

若要將現有服務連線的頻寬增加至 10 Gbps 以上，請完成下列步驟：

**STEP 1 |** 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Colo-Connect**。

**STEP 2 |** 選取與服務連線相關聯的 **Link Name**（連結名稱）。

**STEP 3 |** 增加連結的 **Bandwidth**（頻寬）（互連）。

**STEP 4 |** **Push Config**（推送設定）。

**STEP 5 |** 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Service Connection**（服務連線）。

**STEP 6 |** 將額外的 GRE 通道新增至 Colo-Connect 服務連線。

**STEP 7 |** **Push Config**（推送設定）。

**STEP 8 |** 針對 GRE 通道的 VLAN eBGP 路由和服務連線路由，將 GRE 本機 (對等) IP 位址新增至您的匯出政策。

### 減少 Colo-Connect 服務連線的頻寬

若要將現有服務連線的頻寬減少至 10 Gbps 以下，請完成下列步驟：

**STEP 1 |** 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Colo-Connect**。

**STEP 2 |** 選取與服務連線相關聯的 **Link Name**（連結名稱）。

**STEP 3 |** 減少連結的 **Bandwidth**（頻寬）（互連）。

**STEP 4 |** **Push Config**（推送設定）。

您不必重新設定服務連線，即可移除額外的 GRE 通道；當您在服務連線推送範圍中提交並推送您的變更時，Prisma Access 會偵測並降低連結的頻寬，然後移除額外的通道。

## 刪除 Colo-Connect 連線

若要刪除 Colo-Connect 連線，請完成下列步驟，遵循設定連線的相反順序進行：

**STEP 1 |** 刪除與連線相關聯的服務連線，方法為前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Service Connections**（服務連線）、選取服務連線，然後將其 **Delete**（刪除）。


©2025 Palo Alto Networks, Inc.

**STEP 2 |** **Push Config**（推送設定）。

**STEP 3 |** 刪除與連線相關聯的 Colo-Connect 連線，方法為前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Colo-Connect**、在 **Onboarding**（裝載）區段中選取 **Connection Name**（連線），然後將其 **Delete**（刪除）。

**STEP 4 |** 刪除 Colo-Connect 連結，方法為選取 **Link Name**（連結名稱），然後將其 **Delete**（刪除）。

**STEP 5 |** 針對 GRE 通道的 VLAN eBGP 路由和服務連線路由，從您的匯出政策中刪除 GRE 本機（對等）IP 位址。

# 設定 Prisma Access Colo-Connect (Panorama)

## 使用合作夥伴互連設定 Prisma Access Colo-Connect—部署

若要使用 合作夥伴互連設定 Prisma Access Colo-Connect，請完成以下步驟。

**STEP 1 |** 為您的 Colo-Connect 連線建立子網路。

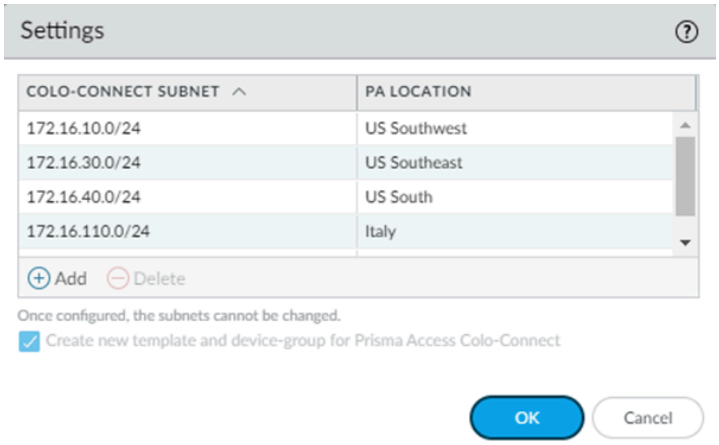
您可以在後續步驟中建立的連線和服務連線中使用您在這裡建立的子網路。

1. 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Colo-Connect**，然後按一下齒輪圖示以編輯設定。
2. **Add**（新增）一個 **Colo-Connect Subnet**（**Colo-Connect** 子網路），並為它選取 Prisma Access 位置（**PA Location**（**PA** 位置））。

   輸入至少 /28 的子網路。
3. （選用）如果您計劃為多個位置建立 Colo-Connect 執行個體，請根據每個位置新增更多子網路。

   您可以設定每個位置一個子網路。
4. 選取 **Create new templates and device-group for Prisma Access Colo-Connect**（為 **Prisma Access Colo-Connect** 建立新範本和裝置群組）。

   第一次設定 Colo-Connect 部署時，請選取此核取方塊，以便為 Colo-Connect 建立範本和裝置群組（分別為 Colo_Connect_Template 和 Colo_Connect_Device_Group）。在建立這些範本和裝置群組之後，此核取方塊會呈現灰色。



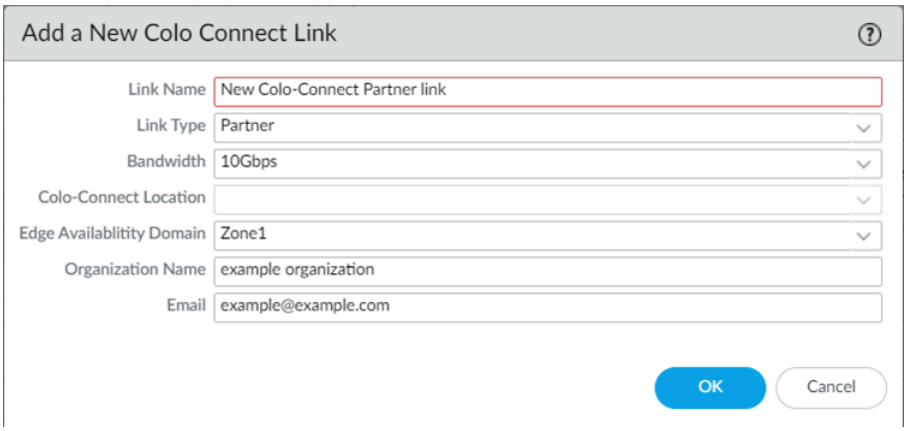

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 新增 Colo-Connect 連結（也稱為互連）。

1. 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Colo-Connect** > **Colo Connect Link**（**Colo Connect** 連結），並 **Add**（新增）Colo-Connect 連結。
2. 給與連結唯一的 **Link Name**（連結名稱）。
3. 選取 **Partner**（合作夥伴）互連。

   您無需輸入 **VLAN ID**。您的 Colo 在使用配對金鑰完成 VLAN 附件的設定時會提供一個。
4. 指定剩餘的 Colo-Connect 連結參數。
   - 選取 **10Gbps** 或 **20Gbps** 作為 **Bandwidth**（頻寬）。

     在指定專用互連連結的頻寬，且提交並推送您的變更之後，您就無法變更該頻寬。
   - 選取 **Zone1** 或 **Zone2** 作為 **Edge Availability Domain**（邊緣可用性網域）。從用於邊緣可用性網域的 GCP 區域中取得此值。
   - 輸入要用於此連結的 **Organization Name**（組織名稱）。
   - 輸入要用於此連結的 **Email**（電子郵件）。任何電子郵件地址都可以接受。




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 建立 Colo-Connect 的連線（也稱為 *VLAN* 附件）。

1. 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Colo-Connect** > **Onboarding**（裝載），並 **Add**（新增）連線。
2. 進行連線設定。
   - 輸入連線的唯一 **Name**（名稱）。
   - 從您在上一個步驟中設定的連結中選取 **Link Name**（連結名稱）。
   - 選取連線的 **Bandwidth**（頻寬）。

     您可以在 **1 Gbps**、**2 Gbps**、**5 Gbps**、**10 Gbps** 或 **20 Gbps** 之間選取。

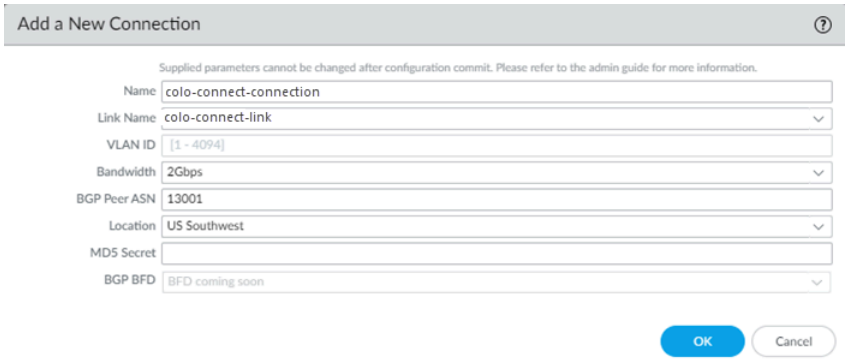
     如果設定多個連線進行互連，請確定連線的總頻寬不超過互連的頻寬。例如，若合作夥伴互連為 10 Gbps，您可以設定 10 個連線，每個連線為 1 Gbps，但所有連線總共不得超過 10 Gbps。

     如果您的部署需要超過 *16* 個連線，請聯繫您的 *Palo Alto Networks* 客戶團隊，他們將開啟 *SRE* 案例以滿足要求。
   - 輸入 **BGP Peer ASN**（**BGP** 對等 **ASN**）。

     在 Colo 中輸入客戶內部部署路由器的自發系統 (AS) 編號。範圍介於 1 與 4294967295 之間。
   - 從您在上一個步驟中建立的連線名稱中選取 **Location**（位置）。

     您必須已為指定的任何位置新增子網路。
   - （選用）輸入 BGP **MD5 Secret**（**MD5** 密碼）。

     忽視 ***BGP BFD*** 欄位；它保留給未來的 *Colo-Connect* 版本。



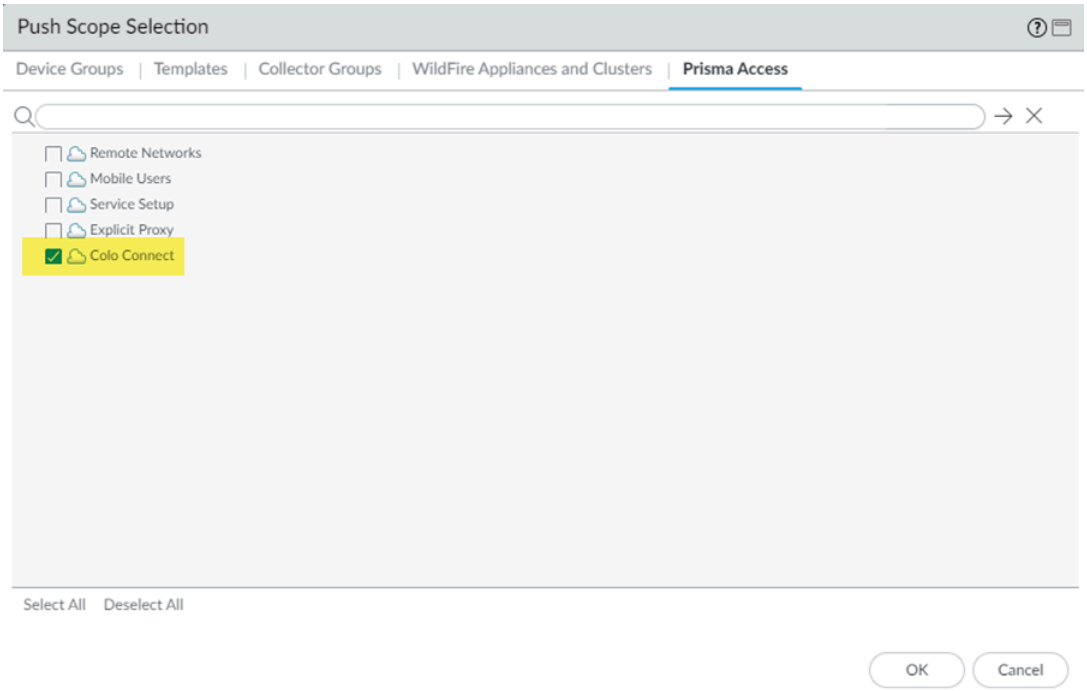

3. 繼續建立連線，直到完成。

   您必須建立兩個連線。這兩個連線都必須位於相同的區域中，而每個連線都必須位於單獨的區域中。您會在後續步驟中建立的服務連線中使用這些連線。

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 提交並推送您的變更。

1. 前往 **Commit**（提交） > **Commit and Push**（提交並推送）。
2. **Edit Selections**（編輯選取項目），並確保在推送範圍內選取了 Colo-Connect。



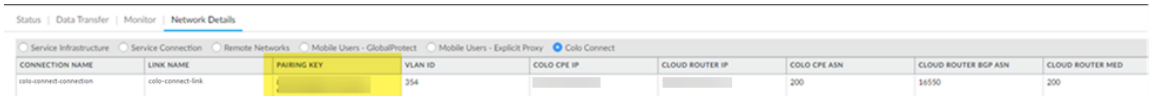

3. 按一下 **Ok**（確定），以儲存您對 Push Scope（推送範圍）所做的變更。
4. **Commit and Push**（提交並推送）您的變更。

**STEP 5 |** 擷取 **Pairing Key**（配對金鑰），並在 GCP 中完成您的合作夥伴互連設定。

在 Colo 中設定合作夥伴互連時，您會使用此配對金鑰。

當您第一次裝載新連線時，Colo-Connect 裝戴區域中的狀態會將 **Status**（狀態）顯示為 **PENDING_PARTNER**，並將 **BGP Status**（**BGP** 狀態）顯示為 **DOWN**（關閉）。若要將連線狀態帶至 **ACTIVE**（作用中），請擷取配對金鑰並在 Colo 的連線中輸入。

1. 前往 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Colo Connect**，並複製 **Pairing Key**（配對金鑰）。




2. 在 Colo 中建立新的 VLAN 連線（例如，Equinix）。
3. 在 Colo VLAN 中貼上配對金鑰。

   GCP 會偵測何時耗用配對金鑰、將 VLAN 狀態帶至 **ACTIVE**（作用中），並產生 BGP IP 位址，讓您在 Colo 內部部署路由器上進行設定。這些動作透過 Colo 路由器與 GCP 雲端路由器之間的 VLAN 啟動 eBGP 路由。

**STEP 6 |** 在客戶 (Colo) 路由器上建立 eBGP 路由，進行 Colo-Connect 連線。

您需要設定 BGP 對等，以確保客戶路由器與雲端路由器之間的連線。

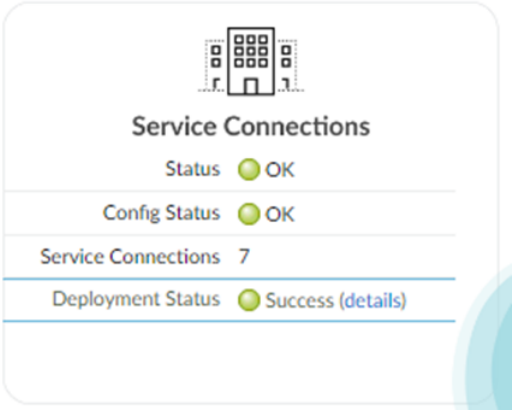
 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** 設定服務連線以與 Colo-Connect 搭配使用。

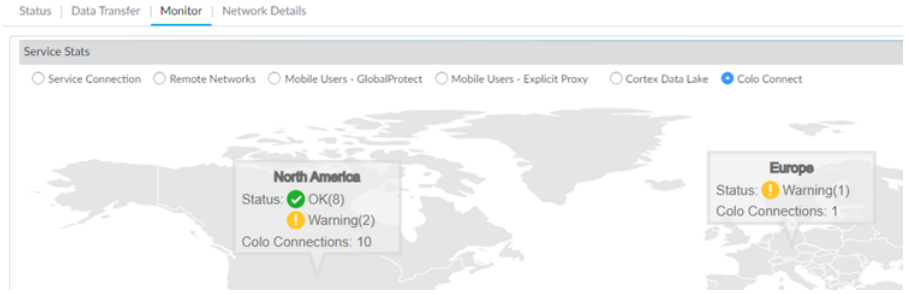
**STEP 8 |** **Commit and Push**（提交並推送）您的設定變更，確保在 **Push Scope**（推送範圍）中選取了 **Colo-Connect**。

**STEP 9 |** 檢查 Colo-Connect 連線的狀態。

1. 若要檢查 Colo-Connect 連線所使用的服務連線狀態，請前往 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > > **Colo Connect** > **Monitor**（監控）




2. 將游標暫留在已部署 Colo-Connect 連線的區域上。
   - 如果 Colo-Connect 連線和 BGP 路由都已啟動，狀態會顯示 **OK**（成功）。
   - 如果 Colo-Connect 連線已啟動，但 BGP 路由未啟動，狀態會顯示 **Warning**（警告）。
   - 如果 Colo-Connect 連線和 BGP 路由都已關閉，狀態會顯示 **Down**（關閉）。
   - 如果 Colo-Connect 連線關閉，但 BGP 路由已啟動，狀態會顯示 **Error**（錯誤）。




3. 如需詳細資訊，請按一下區域方塊，然後檢視 **Status**（狀態）頁籤中的資訊。

**STEP 10 |** 檢查網路詳細資訊，包括 Colo-Connect 連線的配對金鑰，方法為前往 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Colo Connect**，並檢視下列欄位中的資訊。

## 使用專用互連設定 Prisma Access Colo-Connect—部署

若要使用 專用互連設定 Prisma Access Colo-Connect，請完成以下步驟。


©2025 Palo Alto Networks, Inc.

**STEP 1 |** 為您的 Colo-Connect 連線建立子網路。

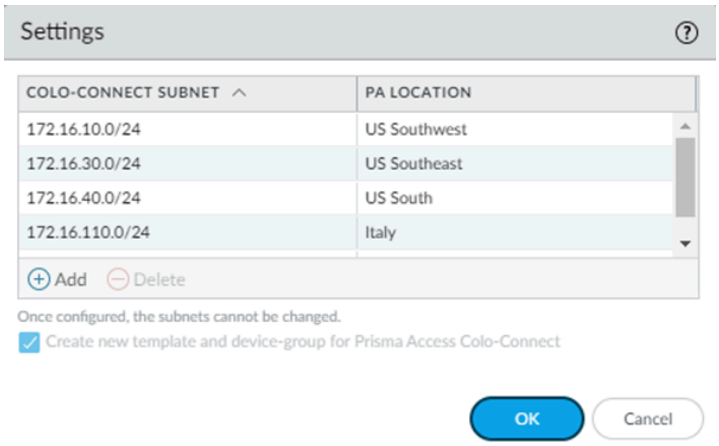
您可以在後續步驟中建立的連線和服務連線中使用您在這裡建立的子網路。

1. 從管理 Prisma Access 的 Panorama 中，前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Colo-Connect**，然後按一下齒輪圖示以編輯設定。
2. **Add**（新增）一個 **Colo-Connect Subnet**（**Colo-Connect** 子網路），並為它選取 Prisma Access 位置（**PA Location**（**PA** 位置））。

   輸入至少 /28 的子網路。
3. （選用）如果您計劃為多個位置建立 Colo-Connect 執行個體，請根據每個位置新增更多子網路。

   每個位置只能設定一個子網路。
4. 選取 **Create new templates and device-group for Prisma Access Colo-Connect**（為 **Prisma Access Colo-Connect** 建立新範本和裝置群組）。

   第一次設定 Colo-Connect 部署時，請選取此核取方塊，以便為 Colo-Connect 建立範本和裝置群組（分別為 Colo_Connect_Template 和 Colo_Connect_Device_Group）。在建立這些範本和裝置群組之後，此核取方塊會呈現灰色。




 ©2025 Palo Alto Networks, Inc.

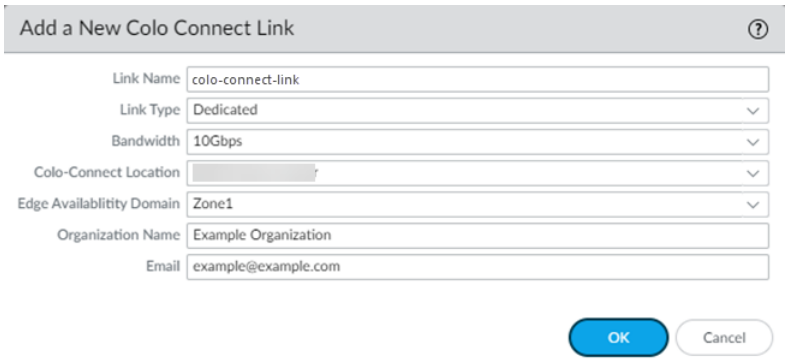
**STEP 2 |** 新增 Colo-Connect 連結（也稱為互連）。

1. 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Colo-Connect** > **Colo Connect Link**（**Colo Connect** 連結），並 **Add**（新增）Colo-Connect 連結。
2. 給與連結唯一的 **Link Name**（連結名稱）。
3. 選取 **Dedicated**（專用）互連。
4. 指定剩餘的 Colo-Connect 連結參數。
   - 選取 **10Gbps** 或 **20Gbps** 作為 **Bandwidth**（頻寬）。

     如果您選取 *20 Gbps*，則必須使用 LACP 將專用互連連結彙總為兩個 *10 Gbps* 連結。

     在指定專用互連連結的頻寬，且提交並推送您的變更之後，您就無法變更該頻寬。
   - 從下拉式清單中選取 **Colo-Connect Location**（**Colo-Connect** 位置）。

     請確定您選取用於專用互連的同一位置。
   - 選取 **Zone1** 或 **Zone2** 作為 **Edge Availability Domain**（邊緣可用性網域）。從用於邊緣可用性網域的 GCP 區域中取得此值。
   - 輸入要用於此連結的 **Organization Name**（組織名稱）。
   - 輸入您要從雲端提供者接收 LOA-CFA 詳細資料的 **Email**（電子郵件）。
     - GCP 會使用此電子郵件傳送授權書和連線設施指派 (LOA-CFA)。請確定 LOA-CFA 傳送給您的 Colo 提供者，以便他們可以開始安裝您的連線。




**STEP 3 |** 在建立專用連線之後，Colo 設施會測試您的連線，並通知您它們已測試且可供使用。

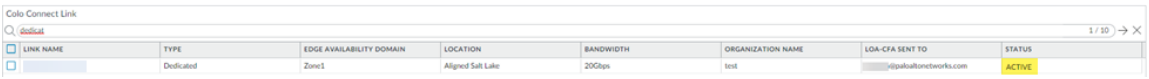
此步驟不需要任何 Prisma Access 設定。在 Colo 設施讓您知道它們已測試之前，請勿在 Prisma Access 中建立 Colo-Connect 連線。


©2025 Palo Alto Networks, Inc.

**STEP 4 |** 建立 Colo-Connect 的連線（也稱為 *VLAN* 附件）。

1. 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Colo-Connect** > **Colo Connect Link**（**Colo Connect** 連結），確定專用連結狀態為 [Active（作用中）]。

   在專用連結狀態為 [Active（作用中）] 之前，您無法建立 Colo-Connect 連結。




2. 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Colo-Connect** > **Onboarding**（裝載），並 **Add**（新增）連線。
3. 進行連線設定。
   - 輸入連線的唯一 **Name**（名稱）。
   - 從您在上一個步驟中設定的連結中選取 **Link Name**（連結名稱）。
   - （選用） 輸入連線的 **VLAN ID**。

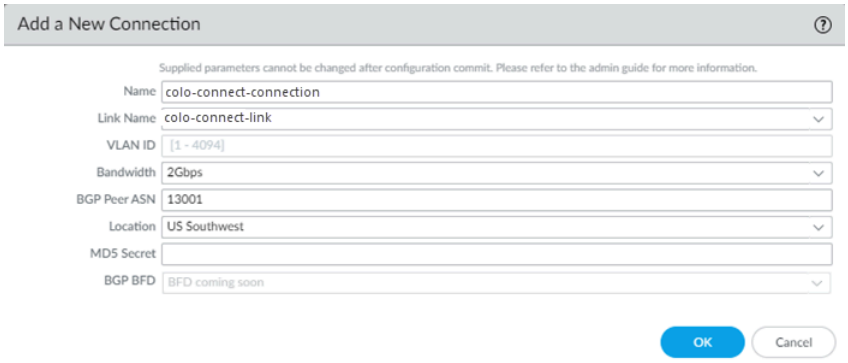
     如果您沒有手動輸入一值，則互連廠商 (GCP) 會產生 VLAN ID。
   - 選取連線的 **Bandwidth**（頻寬）。

     您可以在 **1 Gbps**、**2 Gbps**、**5 Gbps**、**10 Gbps** 或 **20 Gbps** 之間選取。

     如果設定多個連線進行互連，請確定連線的總頻寬不超過互連的頻寬。例如，若專用互連為 20 Gbps，您可以設定 10 個連線，每個連線為 2 Gbps，但所有連線總共不得超過 20 Gbps。
   - 輸入 **BGP Peer ASN**（**BGP** 對等 **ASN**）。

     在 Colo 中輸入客戶內部部署路由器的自發系統 (AS) 編號。範圍介於 1 與 4294967295 之間。
   - 從您在上一個步驟中建立的連線名稱中選取 **Location**（位置）。

     您必須已為指定的任何位置新增子網路。
   - （選用）輸入 BGP **MD5 Secret**（**MD5** 密碼）。



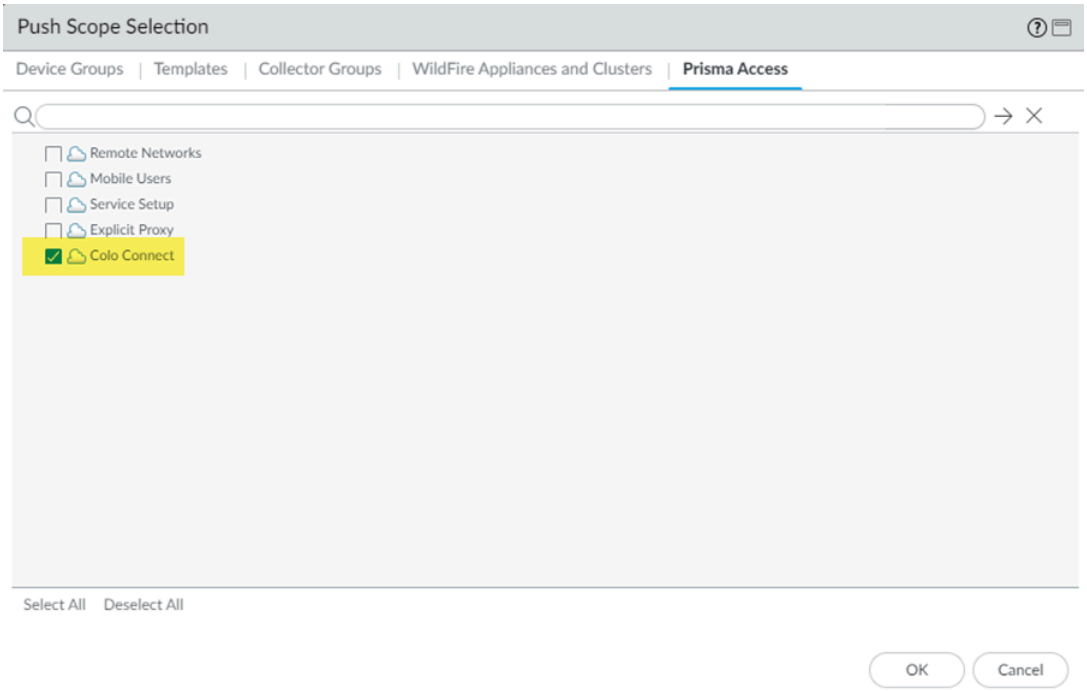

4. 繼續建立連線，直到完成。

   您必須建立兩個連線。這兩個連線都必須位於相同的區域中，而每個連線都必須位於單獨的區域中。您會在後續步驟中建立的服務連線中使用這些連線。

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** 提交並推送您的變更。

1. 前往 **Commit**（提交） > **Commit and Push**（提交並推送）。
2. **Edit Selections**（編輯選取項目），並確保在推送範圍內選取了 Colo-Connect。




3. 按一下 **Ok**（確定），以儲存您對 Push Scope（推送範圍）所做的變更。
4. **Commit and Push**（提交並推送）您的變更。

**STEP 6 |** 在客戶路由器上設定 eBGP 路由。

您需要設定 BGP 對等，以確保客戶路由器之間的連線。

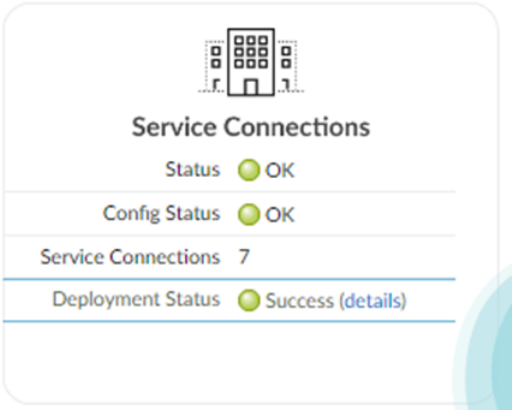
**STEP 7 |** 設定服務連線以與 Colo-Connect 搭配使用。

**STEP 8 |** **Commit and Push**（提交並推送）您的設定變更，確保在 **Push Scope**（推送範圍）中選取了 **Colo-Connect**。

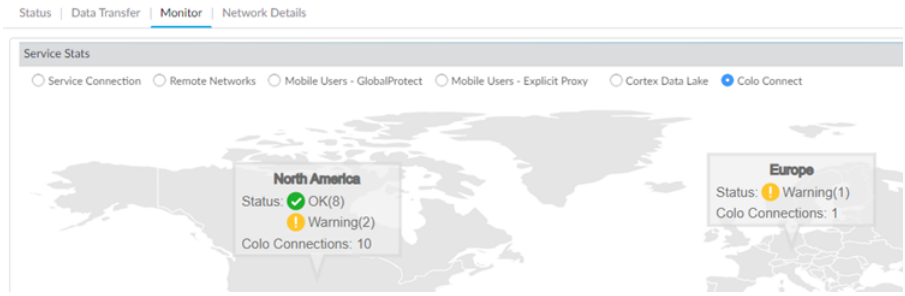

©2025 Palo Alto Networks, Inc.

**STEP 9 |** 檢查 Colo-Connect 連線的狀態。

1. 若要檢查 Colo-Connect 連線所使用的服務連線狀態，請前往 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > > **Colo Connect** > **Monitor**（監控）。



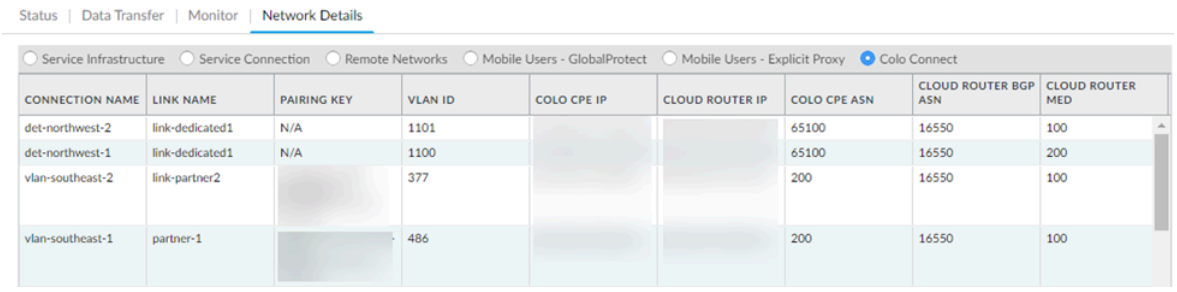

2. 將游標暫留在已部署 Colo-Connect 連線的區域上。
   - 如果 Colo-Connect 連線和 BGP 路由都已啟動，狀態會顯示 **OK**（成功）。
   - 如果 Colo-Connect 連線已啟動，但 BGP 路由未啟動，狀態會顯示 **Warning**（警告）。
   - 如果 Colo-Connect 連線和 BGP 路由都已關閉，狀態會顯示 **Down**（關閉）。
   - 如果 Colo-Connect 連線關閉，但 BGP 路由已啟動，狀態會顯示 **Error**（錯誤）。




3. 如需詳細資訊，請按一下區域方塊，然後檢視 **Status**（狀態）頁籤中的資訊。

**STEP 10 |** 檢查 Colo-Connect 連線的網路詳細資訊，方法為前往 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Colo Connect**，並檢視詳細資訊。

對於專用連結，**Pairing Key**（配對金鑰）會顯示為 **N/A**。




| CONNECTION NAME | LINK NAME | PAIRING KEY | VLAN ID | COLO CPE IP | CLOUD ROUTER IP | COLO CPE ASN | CLOUD ROUTER BGP ASN | CLOUD ROUTER MED |
|---|---|---|---|---|---|---|---|---|
| det-northwest-2 | link-dedicated1 | N/A | 1101 | | | 65100 | 16550 | 100 |
| det-northwest-1 | link-dedicated1 | N/A | 1100 | | | 65100 | 16550 | 200 |
| vlan-southeast-2 | link-partner2 | | 377 | | | 200 | 16550 | 100 |
| vlan-southeast-1 | partner-1 | | 486 | | | 200 | 16550 | 100 |

 ©2025 Palo Alto Networks, Inc.

## 在客戶路由器上設定 VLAN eBGP 路由

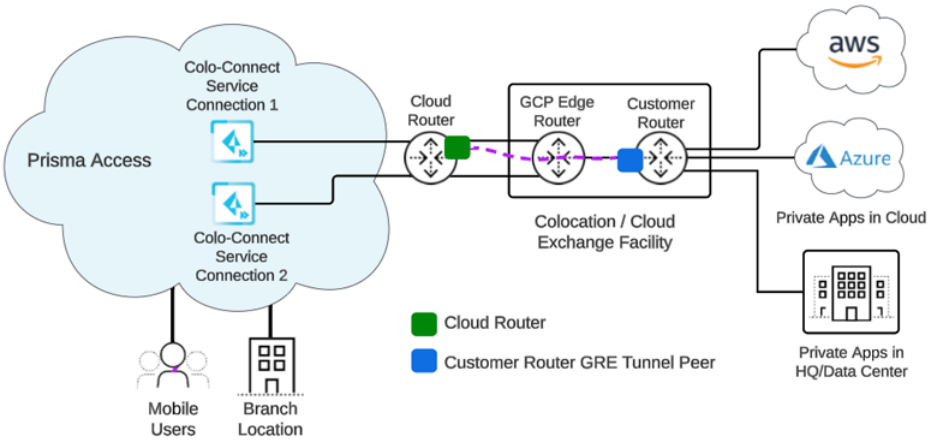
在部署的下列階段期間，GCP 會為客戶 (Colo) 路由器和雲端路由器建立 IP 位址：

- 對於合作夥伴互連，GCP 會在您的 Colo（例如，Equinix）耗用配對金鑰之後建立 IP 位址。
- 對於專用互連，GCP 會在您裝載 Colo-Connect 連線（VLAN 附件） 且提交並推送您的變更之後建立 IP 位址。

若要確保正確的路由，您必須：

- 將 Colo 路由器 IP 位址（Prisma Access UI 中的 **Colo CPE IP**）設定為本機 VLAN IP 位址和本機 eBGP IP 位址
- 將雲端路由器 IP 位址（**Cloud Router IP**（雲端路由器 **IP**））設定為 Colo 路由器上的 eBGP 對等地址。

完成時，會針對 Colo 路由器與雲端路由器之間的連線（VLAN 附件）設定 eBGP。




建立此路由是設定 GRE 通道路由的第一步。在服務連線設定期間設定 GRE 通道時，您會完成 GRE 通道路由。

使用下列步驟來設定 Colo 與雲端路由器之間的路由。

**STEP 1 |** 從管理 Prisma Access 的 Panorama 中，建立子網路、連結和連線，然後 **Commit and Push**（提交並推送）您的變更。

使用互連類型特定的工作流程（合作夥伴或專用）對於合作夥伴互連，請確定已將配對金鑰貼入 Colo VLAN 中。

**STEP 2 |** 前往 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Colo Connect**。

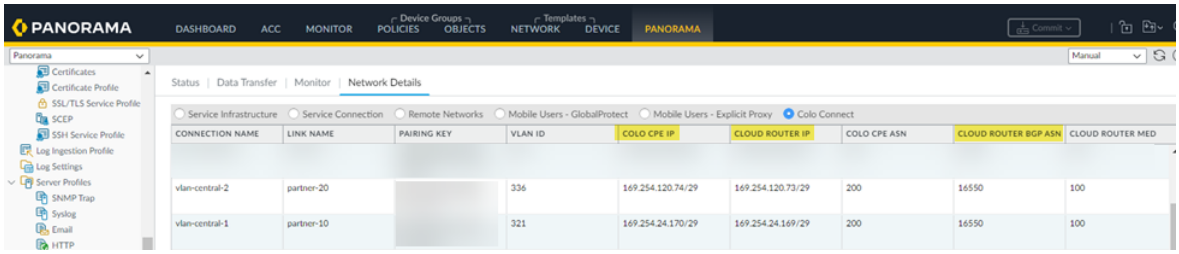

©2025 Palo Alto Networks, Inc.

**STEP 3 |** 請記下列連接元素：

- **Colo CPE IP**
- 雲端路由器 **IP**
- 雲端路由器 **BGP ASN**

在下列範例中：

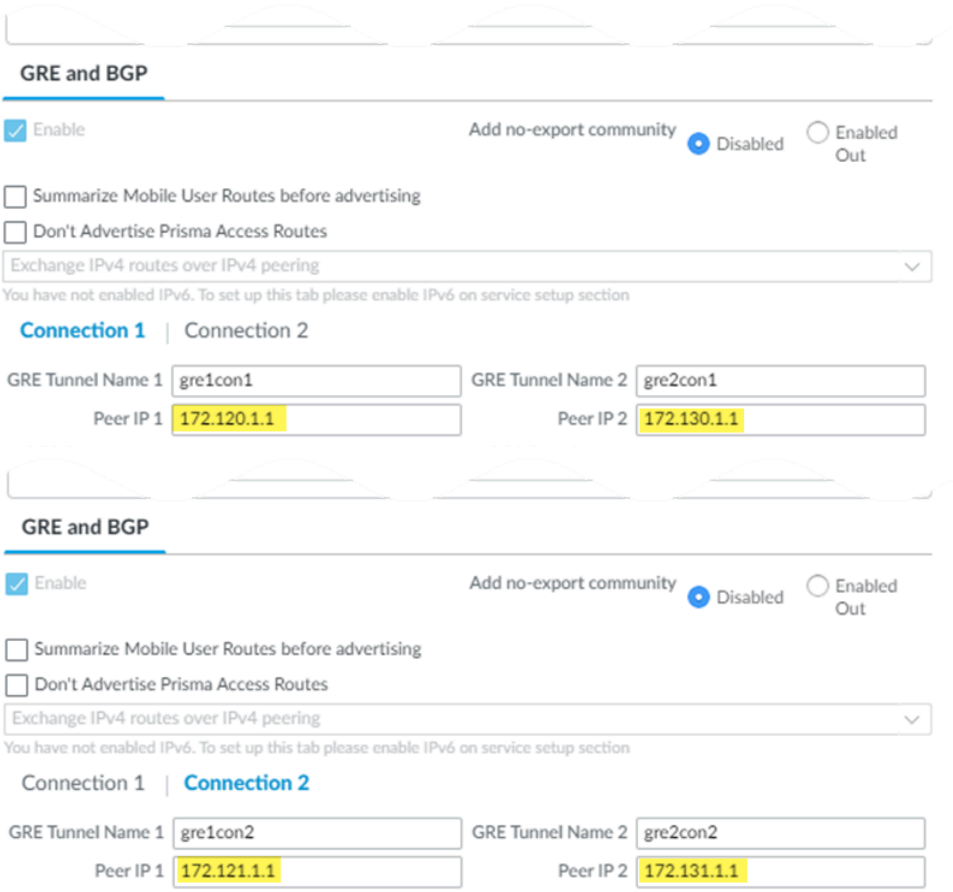
- 對於 vlan-central-1 連線，**Colo CPE IP** 是 169.254.24.170/29、**Cloud Router IP**（雲端路由器 **IP**）是 169.254.24.169/29，而 **Cloud Router BGP ASN**（雲端路由器 **BGP ASN**）是 16550
- 對於 vlan-central-2 連線，**Colo CPE IP** 是 169.254.120.74/29、**Cloud Router IP**（雲端路由器 **IP**）是 169.254.120.73/29，而 **Cloud Router BGP ASN**（雲端路由器 **BGP ASN**）是 16550。
- .




 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 確定您在設定 Colo-Connect 服務連線時將用於本機 GRE IP 位址的 IP 位址。

在 **Peer IP 1**（對等 **IP 1**） 和 **Peer IP 2**（對等 **IP 2**） 區域中 Colo-Connect 服務連線（**Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Connection**（服務連線））時，您會設定這些項目。




如果您要設定服務連線以支援最高 10 Gbps 輸送量，請在 **Connection 1**（連線 **1**）和 **Connection 2**（連線 **2**）中每個放置一個通道，而每個服務連線總共有兩個通道。

如果您要設定服務連線以支援 10 Gbps 以上的輸送量（最高 20 Gbps），請在 **Connection 1**（連線 **1**）和 **Connection 2**（連線 **2**）中每個放置兩個通道，而每個服務連線總共有四個通道。

下列範例顯示一個要為 10 Gbps 以上輸送量設定的通道，因此使用每個連線兩個通道，並且它們會使用下列對等 IP 位址：

- 172.120.1.1 用於連線 1
- 172.130.1.1 用於連線 1
- 172.121.1.1 用於連線 2
- 172.131.1.1 用於連線 2

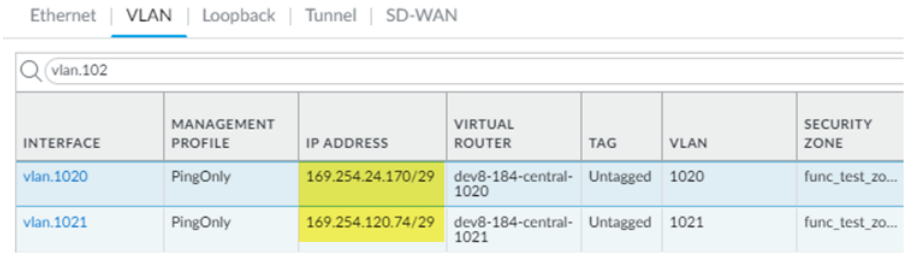
**STEP 5 |** 登入 Colo 路由器。

下列設定螢幕擷取畫面使用 Palo Alto Networks 新世代防火牆作為 Colo 路由器。

 ©2025 Palo Alto Networks, Inc.

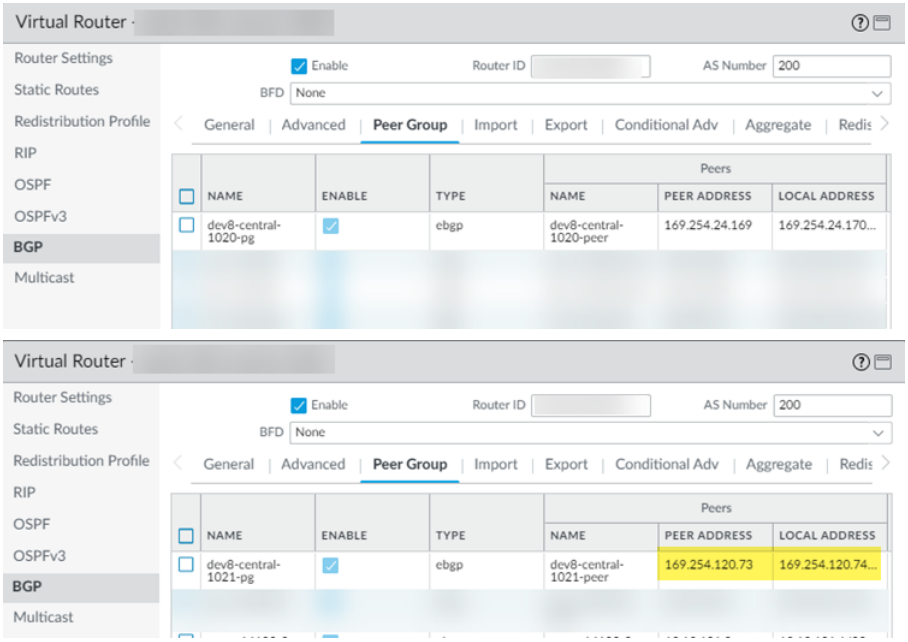
**STEP 6 |** 新增 VLAN 介面，指定 **Colo CPE IP** 位址作為 IP 位址。

如果您是使用新世代防火牆作為 Colo 路由器，請前往 **Network**（網路） > **Interfaces**（介面） > **VLAN**，然後 **Add**（新增） VLAN 介面，指定 **Virtual Router**（虛擬路由器），並




**STEP 7 |** 將 Colo 路由器 IP 位址 (**Colo CPE IP**) 設定為本機 eBGP IP 位址，並將雲端路由器 IP 位址（**Cloud Router IP**（雲端路由器 **IP**）） 設定為 Colo 路由器上的 eBGP 對等位址。

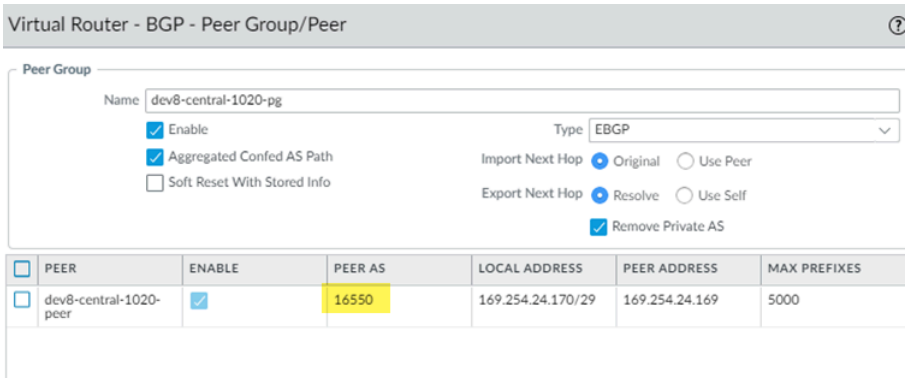
如果您是使用新世代防火牆作為 Colo 路由器，請前往 **Network**（網路） > **Virtual Routers**（虛擬路由器）、**Add**（新增）虛擬路由器、前往 **BGP** > **Peer Group**（對等群組），然後輸入 **Colo CPE IP** 作為 **Peer Address**（對等位址），以及 **Cloud Router IP**（雲端路由器 **IP**）作為 **Local Address**（本機位址）。




 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** 將 **Cloud Router BGP ASN**（雲端路由器 **BGP ASN**）設定為 eBGP 對等自發系統編號 (ASN)。

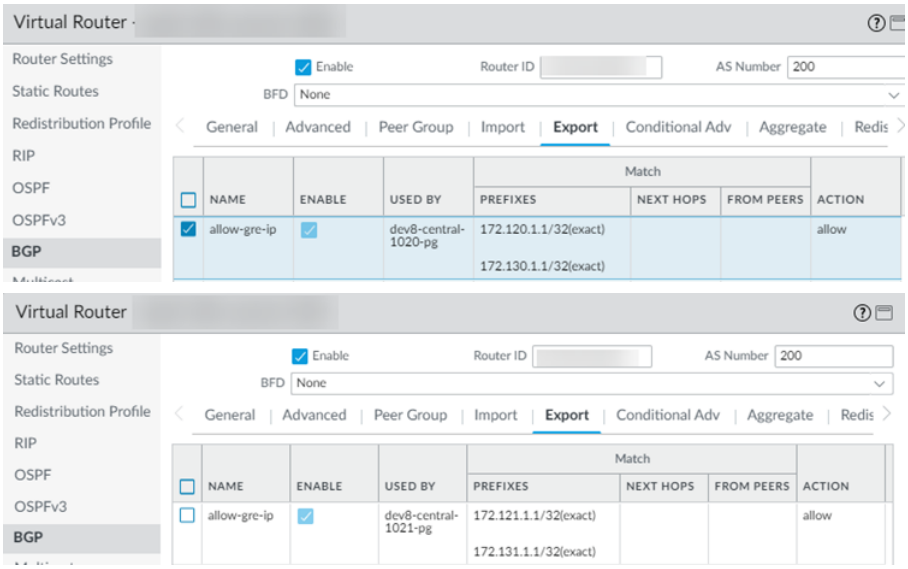
如果您是使用新世代防火牆作為 Colo 路由器，請前往 **Network**（網路） > **Virtual Routers**（虛擬路由器）、**Add**（新增）虛擬路由器、前往 **BGP** > **Peer Group**（對等群組）、**Add**（新增）對等群組，然後選取 **Peer AS**（對等 **AS**）為 **16500**。




**STEP 9 |** 建立一個 BGP 匯出政策，只允許本機 GRE IP 位址公告到雲端路由器對等 IP 位址。

因為雲端路由器只能接收有限數目的路由，所以您需要建立政策，以便只有服務連線 GRE 通道的 IP 位址之間的路由會傳送到雲端路由器。

如果您是使用新世代防火牆作為 Colo 路由器，請前往 **Network**（網路） > **Virtual Routers**（虛擬路由器）、**Add**（新增）虛擬路由器、前往 **BGP** > **Export**（匯出）、**Add**（新增）匯出規則、**Match**（比對）用作對等 IP 位址的 IP 位址，然後建立 **Allow**（允許） **Action**（動作）.。




**STEP 10 |** 建立 Colo-Connect 服務連線。

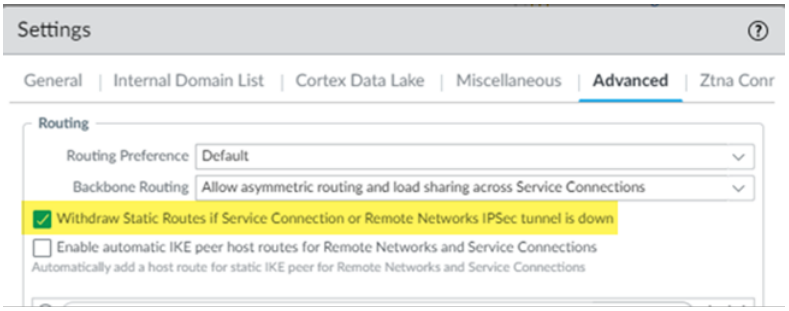
## 建立 Colo-Connect 服務連線

Colo-Connect 使用服務連線，但它們與Prisma Access服務連線不同，因為它們使用 GRE 通道而不是 IPsec 通道，並一律使用 BGP 進行路由。若要設定 Colo-Connect 服務連線，請完成下列步驟。


©2025 Palo Alto Networks, Inc.

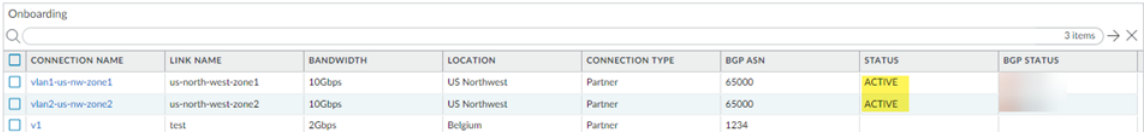
**STEP 1 |** 從管理 Prisma Access 的 Panorama 中，確保 Prisma Access 撤銷靜態路由，方法為前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定）、按一下齒輪圖示以編輯 **Settings**（設定），然後選取 **Withdraw Static Routes if Service Connection or Remote Network IPSec tunnel is down**（如果服務連線或遠端網路 **IPSec** 通道關閉，則撤銷靜態路由）。

選取此選項可確保如果 GRE 通道關閉，GRE 通道使用的靜態路由會被撤銷。



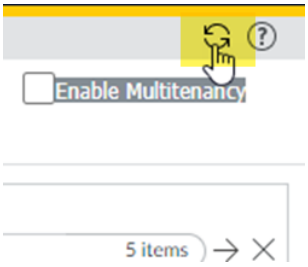

**STEP 2 |** 前往 **Colo-Connect** 頁籤，並透過裝載區域中的 **Status**（狀態）欄位，確保連線處於 **Active**（作用中）狀態。

在連線的 **Status**（狀態）為 **Active**（作用中）之前，您無法設定服務連線。




**STEP 3 |** 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Connection**（服務連線）。

**STEP 4 |** 按一下 Panorama 右上方的 **Refresh**（重新整理），以便在服務連線區域中佈建 Colo-Connect 設定。




**STEP 5 |** **Add**（新增）一個服務連線、給與它唯一的 **Name**（名稱），然後選取 **Transport Type**（傳輸類型）為 **Colo-Connect**。

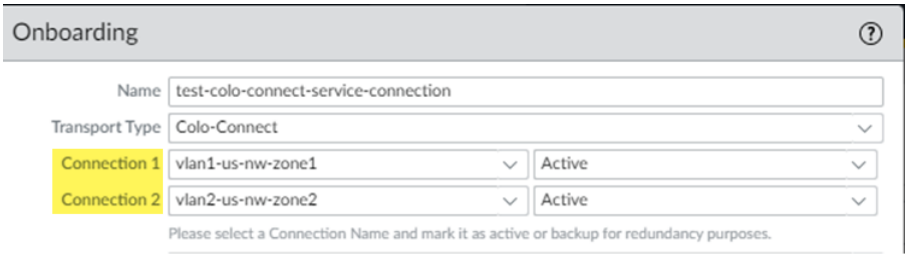
請確定您輸入的名稱長度為 *31* 個字元或以下；輸入 *32* 個字元或更長的名稱會導致通道在 *Prisma Access* 基礎結構中對應不正確。




 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** 選取要與服務連線搭配使用的兩個連線（**Connection 1**（連線 **1**）和 **Connection 2**（連線 **2**））。

這些連線必須位於兩個不同的區域中。




**STEP 7 |** 為 **Connection 1**（連線 **1**）和 **Connection 2**（連線 **2**）選取 **Active**（作用中）或 **Backup**（備份）

設定服務連線時，請使用下列準則：

- 您可以在下列模式下設定連線：
  - **Active**（主動）**/Active**（主動）
  - **Active**（作用中）**/Backup**（備份）
  - **Backup**（備份）**/Active**（作用中）

  在 **Backup**（備份）**/Backup**（備份）模式下設定兩個連線無效且不受支援。
- 所有模式的連線頻寬必須相同。
- 連線必須位於不同的區域中。
- 您可以為服務連線指定的頻寬上限為 20 Gbps。如果您為連線指定 **20 Gbps** 的 **Bandwidth**（頻寬），則無法在 **Active**（主動）**/Active**（主動）設定中使用該連線（必須設定為 **Active**（作用中）**/Backup**（備份））。
- 請勿在同一服務連線中混合專用和合作夥伴互連，並確保服務連線使用不同的區域。此表格顯示服務連線的允許和不允許設定，假設區域、位置、頻寬和角色遵循服務連線指導方針和需求：

| 連線 **1** 屬於 | 連線 **2** 屬於 | 有效的 **Colo-Connect** 服務連線設定？ |
|---|---|---|
| 合作夥伴連線 1 | 合作夥伴連線 2 | 是 |
| 專用連線 1 | 專用連線 2 | 是 |
| 合作夥伴連線 1 | 合作夥伴連線 1 | 否 |
| 專用連線 1 | 專用連線 1 | 否 |
| 合作夥伴連線 | 專用連線 | 否 |

 ©2025 Palo Alto Networks, Inc.

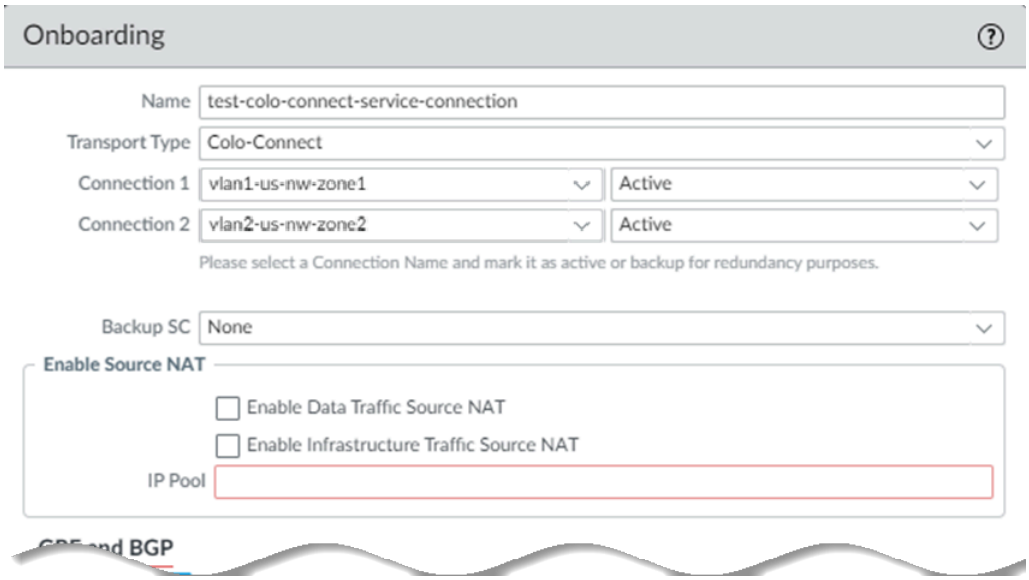
**STEP 8 |** （選用，僅限 BGP 和熱馬鈴薯路由部署）選取服務連線以用作偏好備份（備份 SC）。

您只能選取已設定為 Colo-Connect 服務連線的服務連線。在連線失敗時，Prisma Access 會使用您選取的備份 SC 作為偏好的服務連線。選取備份服務連線可以防止非對稱路由問題（如果您已建立兩個以上的服務連線）。

**STEP 9 |** （選用）為行動使用者—GlobalProtect IP 集區位址、基礎結構子網路中的 IP 位址或兩者啟用來源 NAT。

您可以在一個或多個服務連線上指定子網路，而這些連線用來在 Prisma Access GlobalProtect 行動使用者與資料中心的私人應用程式和資源之間傳送 NAT 流量。

- 啟用資料流量來源 **NAT**—對行動使用者 IP 位址集區位址執行 NAT，以便這些位址不會公告到資料中心，並且僅在資料中心公告和路由您在服務連線中指定的子網路。
- 啟用基礎結構流量來源 **NAT**—對來自基礎結構子網路的位址執行 NAT，以便它們不會公告到資料中心，並且僅在資料中心公告和路由您在服務連線中指定的那些子網路。
- **IP** 集區—指定用來對行動使用者 IP 位址集區、基礎結構子網路或兩者執行 NAT 的 IP 位址集區。使用私人 IP (RFC 1918) 子網路，或可在路由網域中路由的適合子網路，且不與行動使用者—GlobalProtect IP 位址集區或基礎架構子網路重疊。輸入介於 /25 和 /32 之間的子網路。




 ©2025 Palo Alto Networks, Inc.

**STEP 10 |** 在 **GRE and BGP**（**GRE** 和 **BGP**） 區域中，設定服務連線的 GRE 通道和 BGP 設定。

BGP 一律設定為 **Enable**（啟用）。

1. （選用）從下列選項中選取：

   - 若要將公司存取節點（服務連線）的 **no-export**（無匯出） 社群新增到來自客戶周邊設備 (CPE) 上 eBGP 對等的輸出首碼，請將 **Add no-export community**（新增無匯出社群）設定為 **Enabled Out**（已啟用輸出）。預設會 **Disabled**（停用）此功能。

     請勿在熱馬鈴薯路由模式下使用此功能。

   - 防止 Prisma Access BGP 對等將路由轉送至您組織的網路。**Don't Advertise Prisma Access Routes**（請勿公告 **Prisma Access** 路由）。

     根據預設，Prisma Access 會公告所有 BGP 路由訊息，包括本機路由以及從其他服務連線、遠端網路和行動使用者子網路接收的所有首碼。選取此核取方塊可防止 Prisma Access 傳送任何 BGP 公告，但仍會使用其收到的 BGP 資訊，來了解其他 BGP 芳鄰的路由。

     自從 *Prisma Access* 不傳送 *BGP* 公告後，如果您選取此選項，則必須在內部部署設備上設定靜態路由，以建立回到 *Prisma Access* 的路由。

   - 若要減少透過 BGP 公告至客戶周邊設備 (CPE) 的行動使用者 IP 子網路公告數目，請選取**Summarize Mobile User Routes before advertising**（公告前彙總行動使用者路由。

     根據預設，Prisma Access 會在 /24 子網路區塊中公告行動使用者 IP 位址集區；如果你彙總它們，Prisma Access 根據您指定的子網路公告該集區。例如，Prisma Access 使用 /20 子網路公告 10.8.0.0/20 的公用使用者行動 IP 集區，而不是先將該集區劃分為 10.8.1.0/24、10.8.2.0/24、10.8.3.0/24 等子網路，再公告它們。彙總這些公告可以減少 CPE 路由表中儲存的路由數目。例如，您可以使用 IP 集區彙總，搭配可接受有限數目路由的雲端 VPN 閘道（虛擬私人閘道 (VGW) 或傳輸閘道 (TGW)）。

     如果您已啟用熱馬鈴薯路由並啟用路由彙總，則*Prisma Access* 不再前置 *AS-PATH*，這可能會導致非對稱路由。在使用熱馬鈴薯路由來啟用路由彙總之前，請確保從資料中心或總部位置傳回的流量已保證對稱傳回。

2. 使用 GRE 通道設定服務連線路由。
3. 從管理 Prisma Access 的 Panorama 中，返回 **Panorama** > **Cloud Service**（雲端服務） > **Configuration**（設定） > **Service Connection**（服務連線）**Connection 1**（連線 **1**）的 GRE 通道，方法為輸入 **Connection 1**（連線 **1**）的 **GRE Tunnel Name 1**（**GRE** 通道名稱 **1**）和 **Peer IP 1**（對等 **IP 1**），並且如果需要 10 Gbps 以上的頻寬，則輸入連線 1 第二

 ©2025 Palo Alto Networks, Inc.

個通道的 **GRE Tunnel Name 2**（**GRE** 通道名稱 **2**）和 **Peer IP 2**（對等 **IP 2**）；然後，重複這些相同步驟建立 **Connection 2**（連線 **2**）的 GRE 通道。

連線中的每對 GRE 通道最多支援 10 Gbps 的頻寬。如果您需要 10 Gbps 以上的頻寬，請設定每個連線兩個通道。例如：

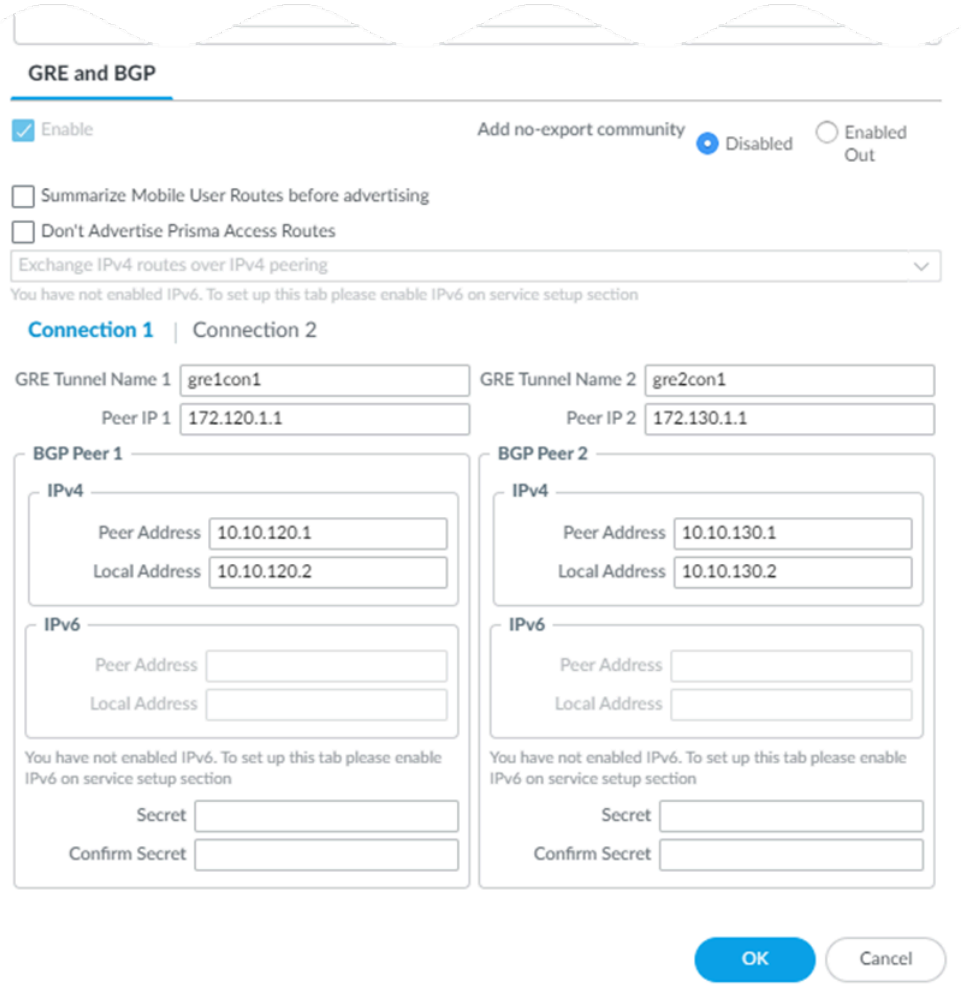
對於對等 IP，請在 Colo 中輸入內部部署路由器的 GRE IP 位址。

使用 IPv4 位址作為 BGP 值；不支援 IPv6。

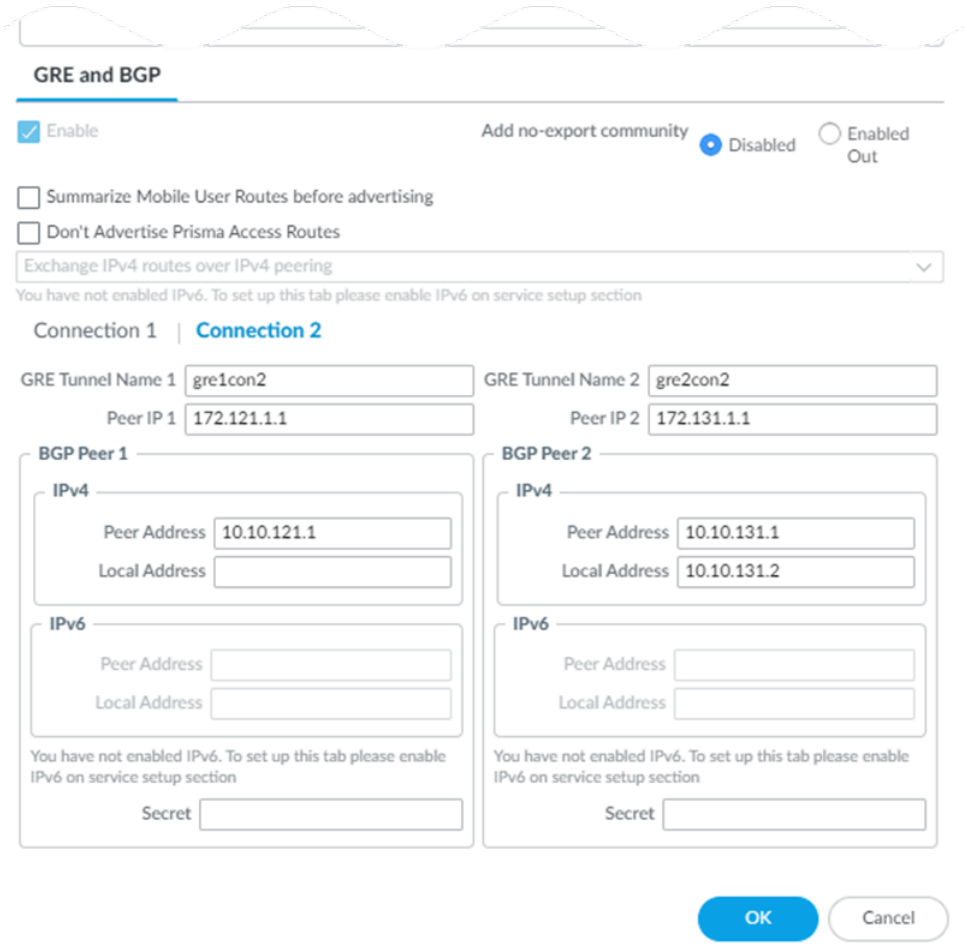
4. 輸入 BGP 對等 1 的 **Peer Address**（對等位址）和 **Local Address**（本機位址），如果連線 1 需要第二個通道，則輸入 BGP 對等 2。

   對於 **Peer Address**（對等位址），輸入 Colo 路由器的 BGP 對等 IP 位址；對於 **Local Address**（本機位址），輸入將用於透過 GRE 通道建立 BGP 網路的位址。

5. （選用）若要設定 BGP 密碼，請輸入 **Secret**（密碼）和 **Confirm Secret**（確認密碼）值。




 ©2025 Palo Alto Networks, Inc.

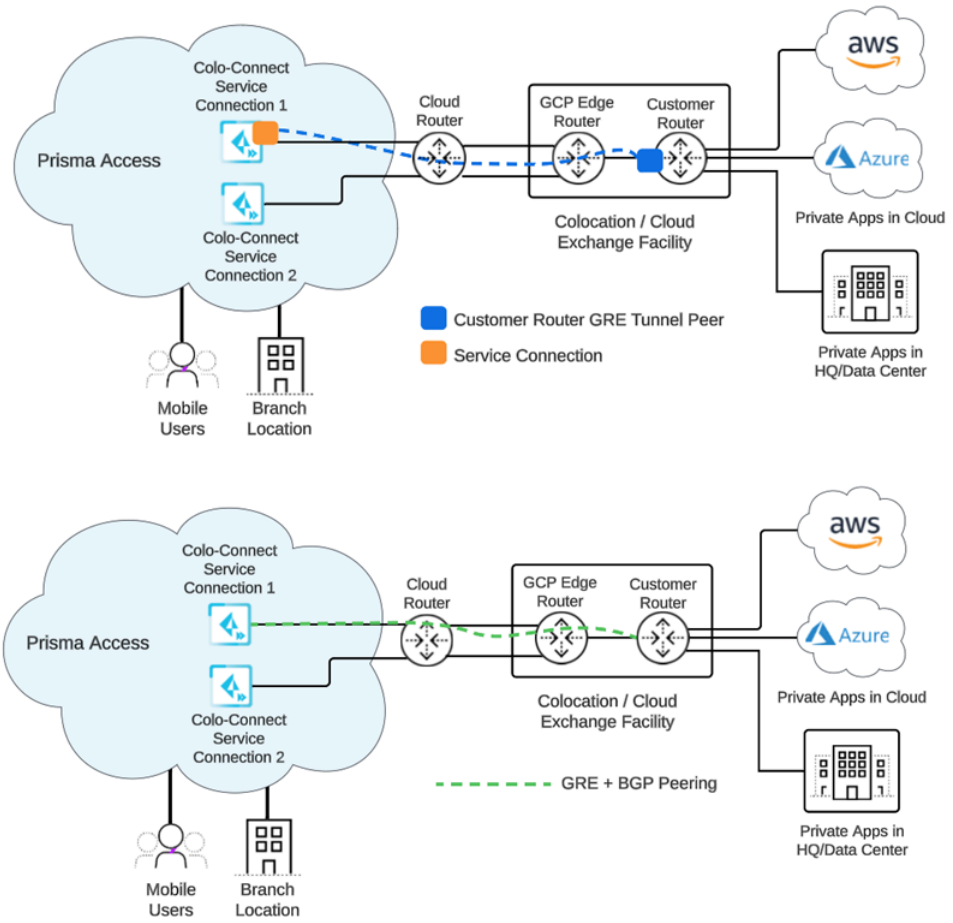



**STEP 11 |** **Commit and Push**（提交並推送）您的設定變更，確保在 **Push Scope**（推送範圍）中選取了 **Colo-Connect**。

## 使用 GRE 通道設定服務連線路由。

Colo 路由器會將其 GRE 通道對等 IP 地址公告至雲端路由器，並從雲端路由器得知 GRE 通道的子網絡。當第一次設定了透過客戶路由器上 VLAN 的 eBGP 路由，您已公告 GRE 通道的本機連線性。在雲端路由器和 Colo 路由器公告，並從彼此得知 Colo 子網路和本地 GRE IP 位址的路由之後，服務連線使用的 GRE 通道會變為作用中（啟動）。


©2025 Palo Alto Networks, Inc.




若要設定路由並將 GRE 通道新增至服務連線，請完成下列步驟。

**STEP 1 |** 記下您將為 BGP 對等 1 的 **Peer Address**（對等位址）和 **Local Address**（本機位址）使用的 IP 位址，以及如果連線 1 需要第二個通道，則為 BGP 對等 2。

下列範例使用下列對等和本機位址：

- **Peer Address**（對等位址）—10.10.120.0 和 10.10.130.1（用於連線 1）、10.10.120.2 和 10.10.130.2（用於連線 2）
- **Local Address**（本機位址）—10.10.120.2 和 10.10.130.2（用於連線 1）、10.10.121.2 和 10.10.131.2（用於連線 2）

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 記下您將用於 **Peer IP 1**（對等 **IP 1**）的 IP 位址，以及如果需要，則為服務連線中的 **Peer IP 2**（對等 **IP 2**）位址。

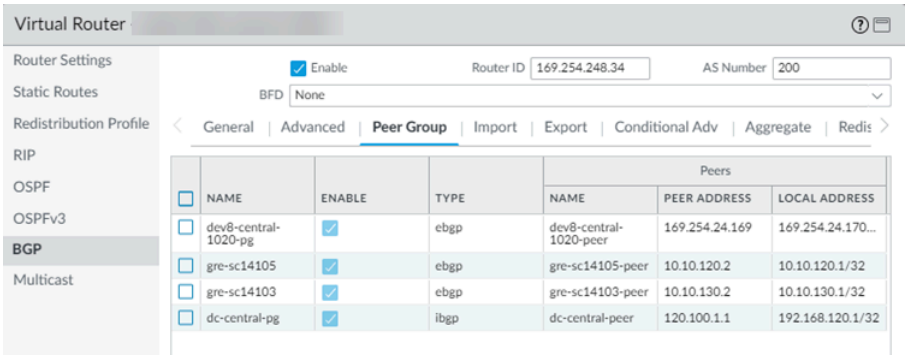
您可以使用這些 IP 位址來建立拒絕政策，防止本機 GRE IP 位址公告至 Colo-Connect 服務連線。

本文件中的所有範例都會使用以下 IP 位址：

- 172.120.1.1 用於連線 1
- 172.130.1.1 用於連線 1
- 172.121.1.1 用於連線 2
- 172.131.1.1 用於連線 2

**STEP 3 |** 設定對等和本機 IP 位址的對等群組。

如果您是使用新世代防火牆作為 Colo 路由器，請前往 **Network**（網路） > **Virtual Routers**（虛擬路由器）、**Add**（新增）虛擬路由器、前往 **BGP** > **Peer Group**（對等群組），然後輸入對等位址作為 **Peer Address**（對等位址），以及輸入 **Local Address**（本機位址）作為 **Local Address**（本機位址）。

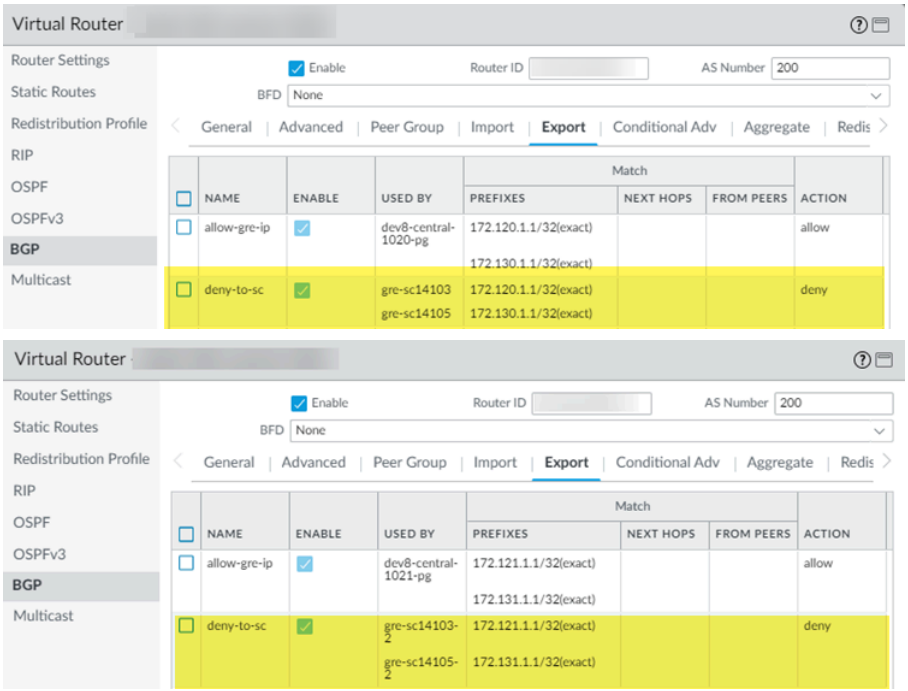



 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 建立 BGP 匯出政策，以拒絕您設定的對等 IP 位址（172.120.1.1、172.130.1.1、172.121.1.1 和 172.131.1.1），並將它們套用至您建立的對等群組。

此匯出政策會在本機 GRE 通道對等 IP 位址上放置 DENY 規則，並允許將所有其他路由公告至服務連線。

如果您是使用新世代防火牆作為 Colo 路由器，請前往 **Network**（網路） > **Virtual Routers**（虛擬路由器）、**Add**（新增）虛擬路由器、前往 **BGP** > **Export**（匯出）、**Add**（新增）匯出規則、**Match**（比對）用作對等 IP 位址的 IP 位址，然後建立 **Deny**（拒絕）**Action**（動作）。




## 增加或減少 Colo-Connect 服務連線的頻寬

設定服務連線時，您會根據與其相關聯的連線 (VLAN 附件) 來設定頻寬。您可以配置每個服務連線兩個連線，然後配置每個連線一個或兩個 GRE 通道。

雖然每個 Colo-Connect 服務連線最多支援 20 Gbps，但服務連線中的每個 GRE 通道都支援 10 Gbps。因此，您可能必須在 Colo-Connect 服務連接中新增或刪除 GRE 通道、變更連結中的總頻寬，這會導致服務連線頻寬高於或低於 10 Gbps。

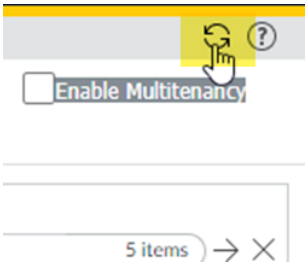
### 增加 Colo-Connect 服務連線的頻寬

若要將現有服務連線的頻寬增加至 10 Gbps 以上，請完成下列步驟：

**STEP 1 |** 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Colo-Connect**。

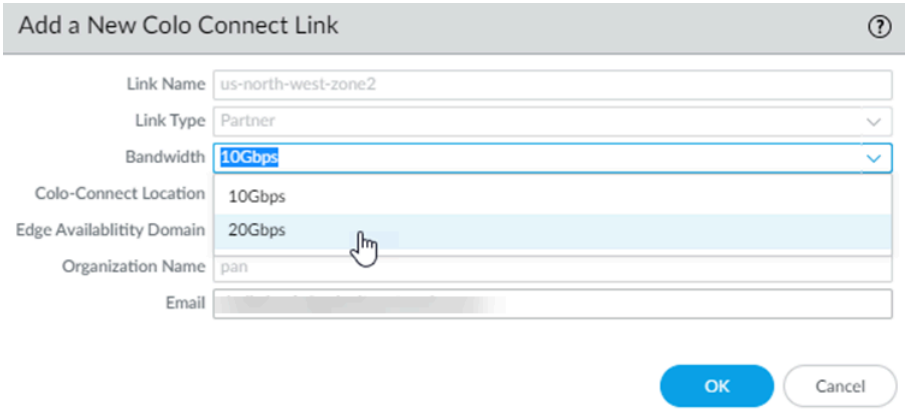
 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Connection**（服務連線），然後按一下 Panorama UI 右上角的 **Refresh**（重新整理），以便在服務連線區域中佈建 Colo-Connect 設定。




**STEP 3 |** 選取與服務連線相關聯的 **Link Name**（連結名稱）。

**STEP 4 |** 增加連結的 **Bandwidth**（頻寬）（互連）。

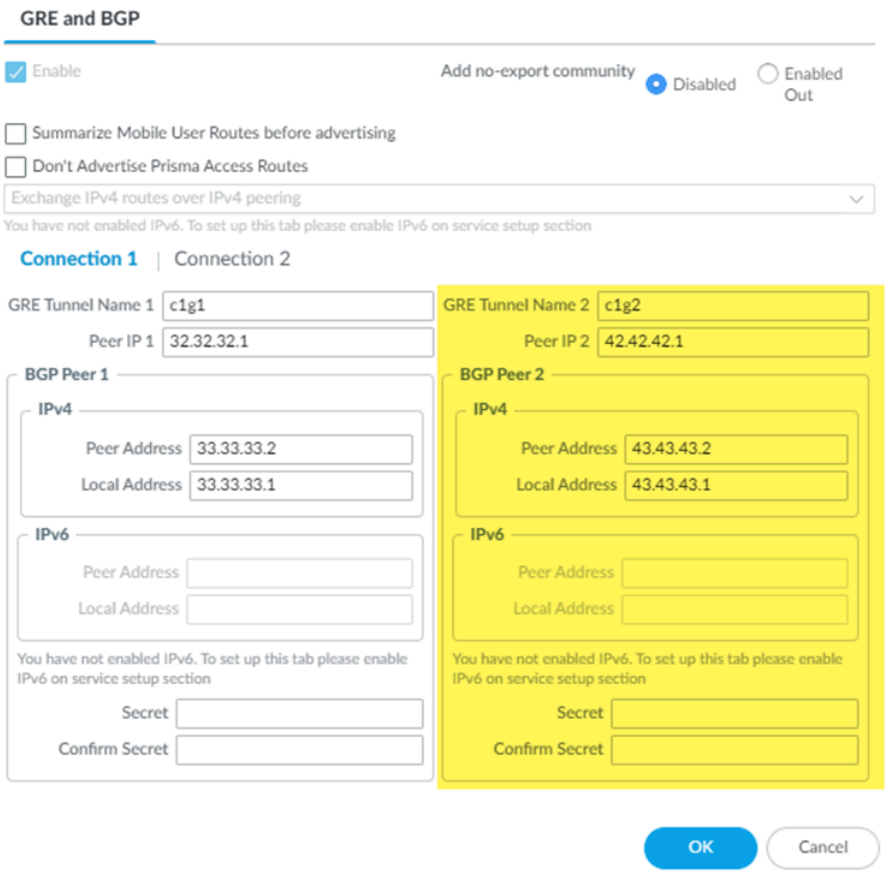



**STEP 5 |** **Commit and Push**（提交並推送）您的變更，僅在 **Push Scope**（推送範圍）中選取 **Colo-Connect**。

**STEP 6 |** 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Connection**（服務連線） > ***<service-connection-name>*** > **Onboarding**（裝載）。

 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** 將額外的 GRE 通道新增至 Colo-Connect 服務連線。




**STEP 8 |** **Commit and Push**（提交並推送）您的變更，僅在 **Push Scope**（推送範圍）中選取 **Service Connections**（服務連線）。

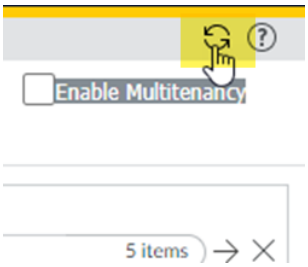
**STEP 9 |** 針對 VLAN eBGP 路由和 GRE 通道的服務連線路由，將 GRE 本機 (對等) IP 位址新增至您的匯出政策。

減少 **Colo-Connect** 服務連線的頻寬

若要將現有服務連線的頻寬減少至 10 Gbps 以下，請完成下列步驟：

**STEP 1 |** 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Colo-Connect**

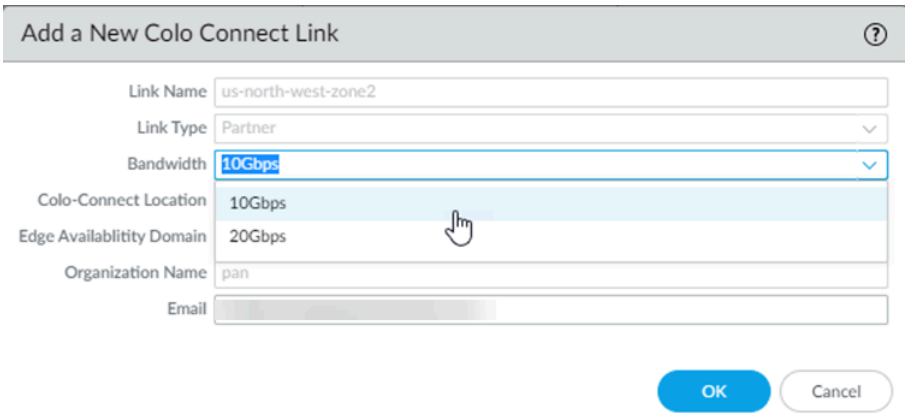
**STEP 2 |** 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Connection**（服務連線），然後按一下 Panorama UI 右上角的 **Refresh**（重新整理），以便在服務連線區域中佈建 Colo-Connect 設定。




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 選取與服務連線相關聯的 **Link Name**（連結名稱）。

**STEP 4 |** 減少連結的 **Bandwidth**（頻寬）（互連）。




**STEP 5 |** **Commit and Push**（提交並推送）您的變更，僅在 **Push Scope**（推送範圍）中選取 **Colo-Connect**。

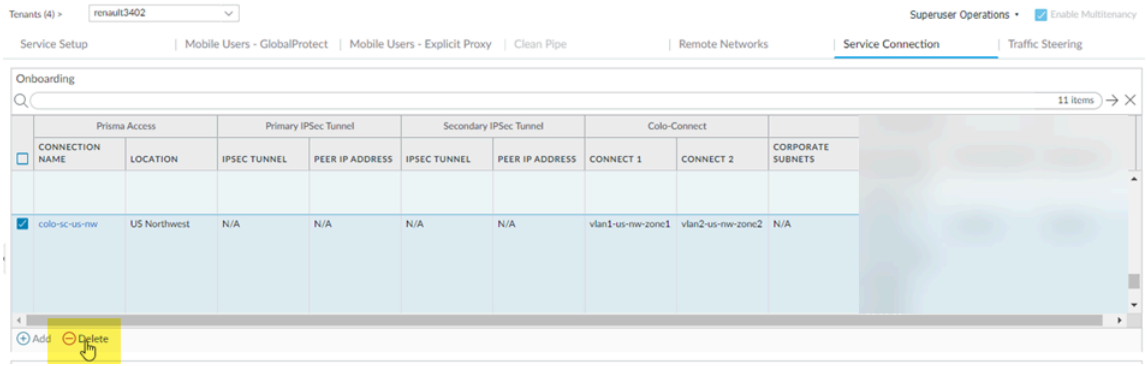
**STEP 6 |** **Commit and Push**（提交並推送）您的變更，僅在 **Push Scope**（推送範圍）中選取 **Service Connections**（服務連線）。

您不必重新設定服務連線，即可移除額外的 GRE 通道；當您在服務連線推送範圍中提交並推送您的變更時，Prisma Access 會偵測並降低連結的頻寬，然後移除額外的通道。

## 刪除 Colo-Connect 連線

若要刪除 Colo-Connect 連線，請完成下列步驟，遵循設定連線的相反順序進行：

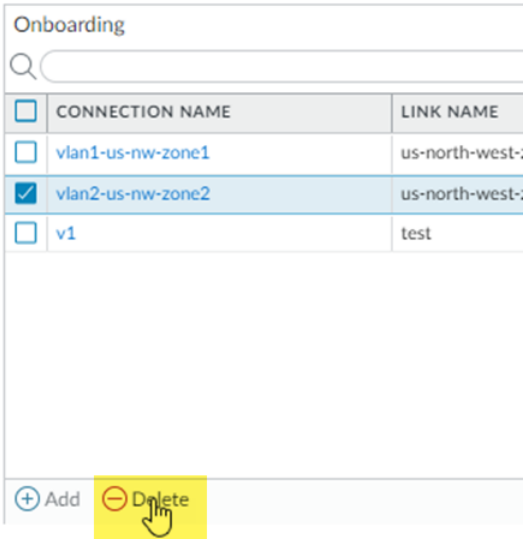
**STEP 1 |** 刪除與連線相關聯的服務連線，方法為前往 **Panorama** > **Cloud Services**（服務連線） > **Configuration**（設定） > **Service Connection**（服務連線）、選取服務連線，然後將其 **Delete**（刪除）。



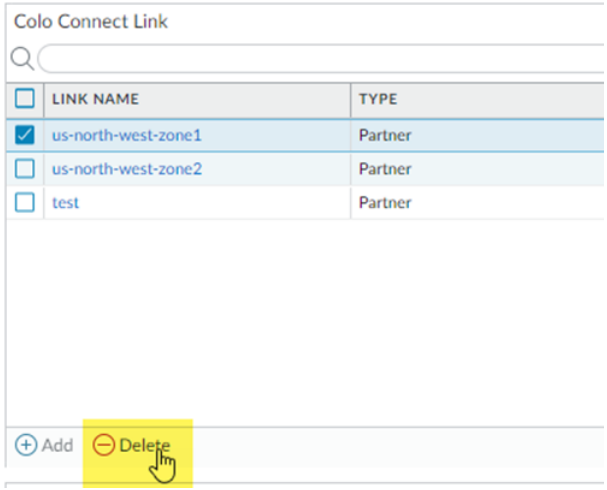

**STEP 2 |** **Commit and Push**（提交並推送）您的變更，僅在 **Push Scope**（推送範圍）中選取 **Service Connections**（服務連線）。


©2025 Palo Alto Networks, Inc.

**STEP 3 |** 刪除與連線相關聯的 Colo-Connect 連線，方法為前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Colo-Connect**、在 **Onboarding**（裝載）區段中選取 **Connection Name**（連線），然後將其 **Delete**（刪除）。




**STEP 4 |** 刪除 Colo-Connect 連結，方法為選取 **Link Name**（連結名稱），然後將其 **Delete**（刪除）。




**STEP 5 |** 針對 VLAN eBGP 路由和 GRE 通道的服務連線路由，從您的匯出政策中刪除 GRE 本機（對等）IP 位址。


©2025 Palo Alto Networks, Inc.

# Prisma Access 中的應用程式加速

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ 最低版本為 Prisma Access 5.0 版 Innovation<br>❑ Prisma Access 授權<br>❑ 應用程式加速需要 Prisma Access 資料平面 10.2.10 版。<br>❑ 應用程式加速附加元件授權<br>應用程式加速權包括 30 天的自發 DEM (ADEM) 評估授權，因此您可以從 ADEM 擷取應用程式加速效能指標。 |

應用加速直接解決了應用程式效能不佳的原因，並即時採取行動來緩解它們，從而大幅改善 Prisma Access GlobalProtect 和遠端網路使用者的使用者體驗。

存取應用程式時使用者體驗不佳的主要原因是動態內容（必須根據需求為每個使用者個別處理的內容）和網路連線問題。

應用程式加速為您提供以下功能：

上層 **SaaS** 應用程式的加速— Prisma SASE 加速可加速動態內容，以縮短上層 SaaS 應用程式的回應時間。在使用者要求它之前，它會安全、聰明地準備每個使用者所需的動態內容。

因此，應用程式加速大幅減少了應用程式和支援它們的 API 的回應時間，從而改善使用者體驗並提高生產力。

支援的應用程式一節中列出了加速的應用程式。

網路加速—當您的使用者存取應用程式時，他們可能會遇到因輸送量下降而導致應用程式效能不佳的情況，起因可能是封包遺失、無線連線效能下降、網路擁塞和其他因素。這些網路問題可能會對員工體驗產生不利影響並降低他們的生產力。

當初構思網際網路時，網路是同質的，無線連線還處於起步階段。TCP 等基本通訊協定最初是為這些網路建立的。如今，網路不再是同質的，而無線連線創造了高度多變的使用者體驗。當使用者遇到網路狀況下降時，TCP 無法區分問題是由於裝置限制、網路限制還是物理限制而發生。

無需對您的用戶端設定或應用程式進行任何變更，應用程式加速即可讓您牢牢了解：

- 裝置能力#用戶端端點的類型
- 網路能力#網路類型
- 應用程式內容—正在使用的應用程式類型

應用程式加速利用對裝置、網路和應用程式內容的理解，最大限度地提高輸送量並即時調整以適應不斷變化的網路狀況。

與直接網際網路存取相比時，應用程式加速在透過 Prisma Access 連線時可顯著提高 TCP 流量的輸送量。

您可以在 Prisma SASE 事件和警示中檢視應用程式加速對輸送量的改善。採用 AI 技術的自發 DEM (ADEM) 與應用程式加速整合成，為您提供加速的應用程式數目和整體效能提升等指標。


©2025 Palo Alto Networks, Inc.

# 應用程式加速需求和指導方針

設定應用程式加速時，請注意以下指導方針和需求：

- 支援的應用程式—應用程式加速支援以下應用程式：
  - Amazon S3
  - Azure Storage
  - Box
  - Google Drive
  - Microsoft 365：
    - 我的內容
  - Microsoft OneDrive
  - Salesforce
  - SAP Ariba
  - ServiceNow
  - Slack（檔案下載）
  - Zoom：
    - 聊天檔案下載
    - 雲端錄音下載
    - Zoom Team Chat
- 支援的位置—應用程式加速適用於所有 Prisma Access 位置，但以下位置除外：
  - 所有 本地區域
  - 巴林
  - 中國
  - 愛爾蘭
  - 南非西部
  - 瑞典
  - 阿拉伯聯合大公國
- 受信任的根 **CA** 上傳—您需要設定受信任的根 CA 並執行提交並推送作業，然後在應用程式加速設定期間選取它，如以下程序中所示。如果使用 Strata Cloud Manager 設定應用程式加速，請在 Prisma Access 範圍中設定根 CA。如果變更您使用的憑證，則您還必須先提交並推送變更的憑證，然後才能選取它。
- 轉送信任憑證和受信任的根 **CA**—啟用您上傳的 CA/憑證作為轉送信任憑證和受信任的根 CA，如下列程序中所示。如果 SSL 解密套用任何加速的應用程式，您必須將憑證標記為轉送信任憑證和受信任的根 CA，否則使用者在嘗試存取這些應用程式時將遇到 SSL 錯誤。

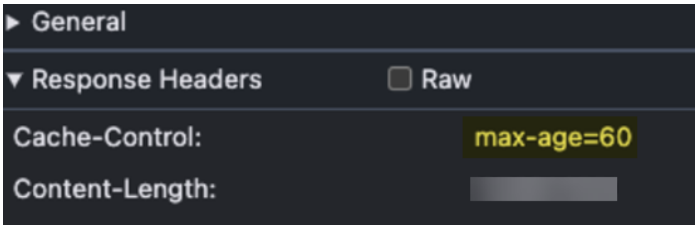

©2025 Palo Alto Networks, Inc.

- 不受支援的 **Prisma Access** 功能—以下功能不支援應用程式加速，且啟用這些功能的 Prisma Access 部署不會加速：
  - IPv6

    設定 IPv6 時，應用程式加速與 IPv6 網路共存；不過，只有 IPv4 TCP 流量會加速。IPv6 流量不會加速，但功能正常。
  - 使用重疊子網路的遠端網路（預設在 Prisma Access (Managed by Strata Cloud Manager) 部署中支援），可在 Prisma Access (Managed by Panorama) 部署中設定。
- 應用程式加速指導方針：
  - **QUIC** 通訊協定支援—某些瀏覽器（例如 Google Chrome）可能預設使用快速 UDP 網際網路連線 (QUIC) 通訊協定。第七層應用程式加速不能用於使用 QUIC 的流量。權宜方案為在設定應用程式加速時停用 QUIC 通訊協定。
  - **SaaS** 應用程式和 **Zy-*** 回應標頭—使用者若連線到為上層 SaaS 應用程式啟用應用程式加速的 Prisma Access 部署，可以預期看到名稱為 Zy-* 的回應標頭，例如 Zy-Server 和 Zy-Accelerated，以及 zy_sid 工作階段 cookie。

    如果回應標頭是 Zy-Accelerated，則值 **1** 表示回應已加速，而值 **0** 表示回應未加速。
  - 內容本地語言化—如果加速的 SaaS 應用程式僅根據使用者的 IP 位址或使用者 ID 將內容本地語言化，則為該應用程式啟用加速時，其內容將不會本地語言化。
  - 變更安全性政策規則的預設行為，動作設定為拒絕—如果您有動作設定為 **Deny**（拒絕）的安全性政策規則，其會套用至使用基於來源或目的地位址、應用程式或服務的規則通過應用程式加速的流量，則流量將完成三向交握，但 Prisma Access 將封鎖它，且 **Deny**（拒絕）政策會如所設定一般運作。
  - **Amazon S3** 和 **Azure Blob Storage** `cache-control`—Amazon S3 和 Azure Blob Storage 貯體和檔案具有一系列與其相關聯的 HTTP 回應標頭。其中一個值之一是 `cache-control`。這些檔案不會加速，如果 `cache-control` 值為:
    - 取消設定
    - 將值設定為 `max-age=0`
    - 將值設定為 `max-age=no-cache`

    若要取得 Amazon S3 和 Azure Blob Storage 的應用程式加速優勢，請將 `cache-control max-age` 值設定為大於零的值。

    
    
- 活動洞察中具有共用網域的應用程式—使用應用程式加速時，第七層加速基於網域。在某些情況下，如果兩個應用程式共用相同網域，則活動洞察中的應用程式報告可能會將某個應用程式的第七層流量歸因於另一個應用程式。例如，如果來自 MS Teams 和 OneDrive 應用程式的某些流量共用相同網域，則 MS Teams 應用程式報告將顯示在 OneDrive 下。

 ©2025 Palo Alto Networks, Inc.

- 長期連線和系統日誌—當個別 TCP 連線結束時，應用程式加速會寫入第四層日誌。對於短期連線，此行為是透明的，因為短期連線是由應用程式頻繁建立的。

  應用程式加速會收集連線作用中的整個期間的指標。對於長期連線（例如已掛載 SMB 網路磁碟機所使用的連線），此行為可能會使指標看起來好像僅在連線結束時收集。

 ©2025 Palo Alto Networks, Inc.

# 設定應用程式加速

若要在 Prisma Access 中設定應用程式加速，請選取下列其中一個頁籤，取決於您的部署（Prisma Access (Managed by Strata Cloud Manager) 或者 Prisma Access (Managed by Panorama)）。

- Strata Cloud Manager
- Panorama


©2025 Palo Alto Networks, Inc.

# 在 Prisma Access 中設定應用程式加速 (Strata Cloud Manager)

若要在 Prisma Access (Managed by Strata Cloud Manager) 部署中設定應用程式加速，請完成此工作。


©2025 Palo Alto Networks, Inc.

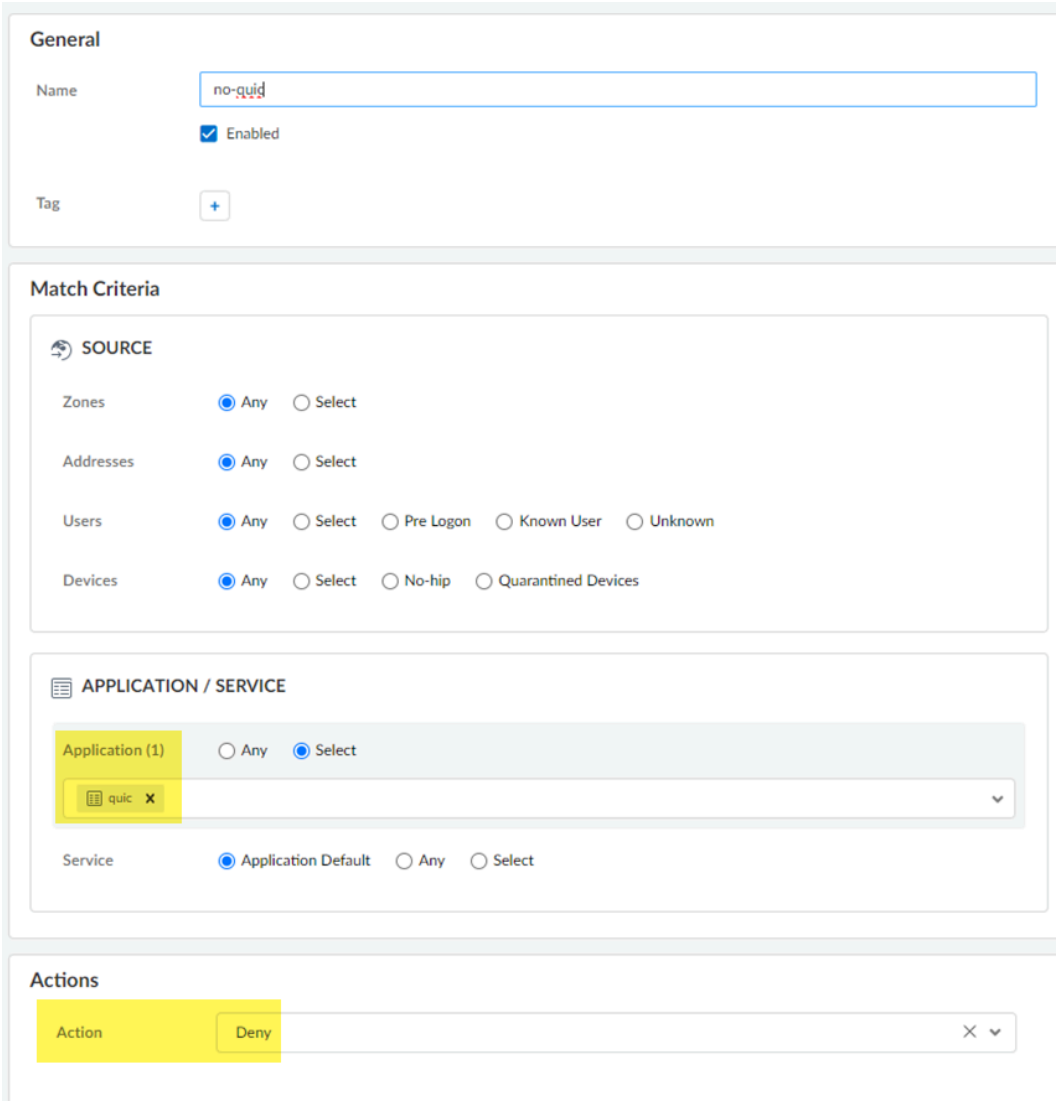
**STEP 1 |** （選用）停用快速 UDP 網際網路連線 (QUIC) 通訊協定。

若未停用 QUIC，應用程式加速無法在第七層加速應用程式。

1. 前往 **Manage**（管理） > **Configuration**（設定） > **NGFW & Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全性服務） > **Security Policy**（安全性政策） 和 **Add Rule**（新增規則） > **Pre Rules**（前置規則）。

   在 **Global**（全域）設定範圍中建立此安全性政策規則。

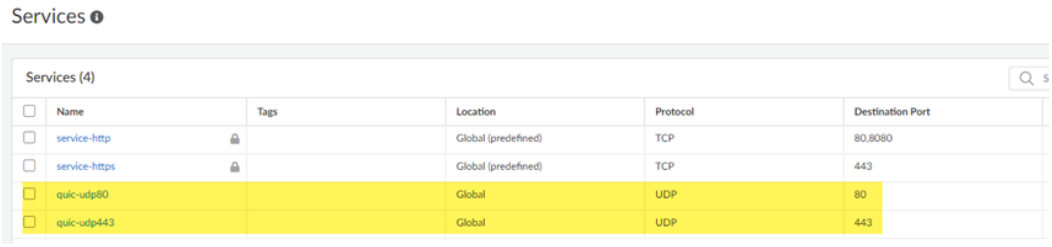
2. 選取 **Application / Service**（應用程式/服務）為 **quic**，並選取 **Actions**（動作）為 **Deny**（拒絕）。




3. **Save**（儲存）變更。
4. 前往 **Manage**（管理） > **Configuration**（設定） > **NGFW & Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（物件） > **Services**（服務） > **Service**（服務），並為 UDP 連接埠 80 和 UDP 連接埠 443 **Add**（新增）服務。

   Palo Alto Networks 建議為 UDP 連接埠 80 和 UDP 連接埠 443 新增服務，並建立額外的安全性政策以封鎖這些連接埠上的 UDP 流量，因為較新版本的 QUIC 可能會被錯誤識別為 **unknown-udp**。。

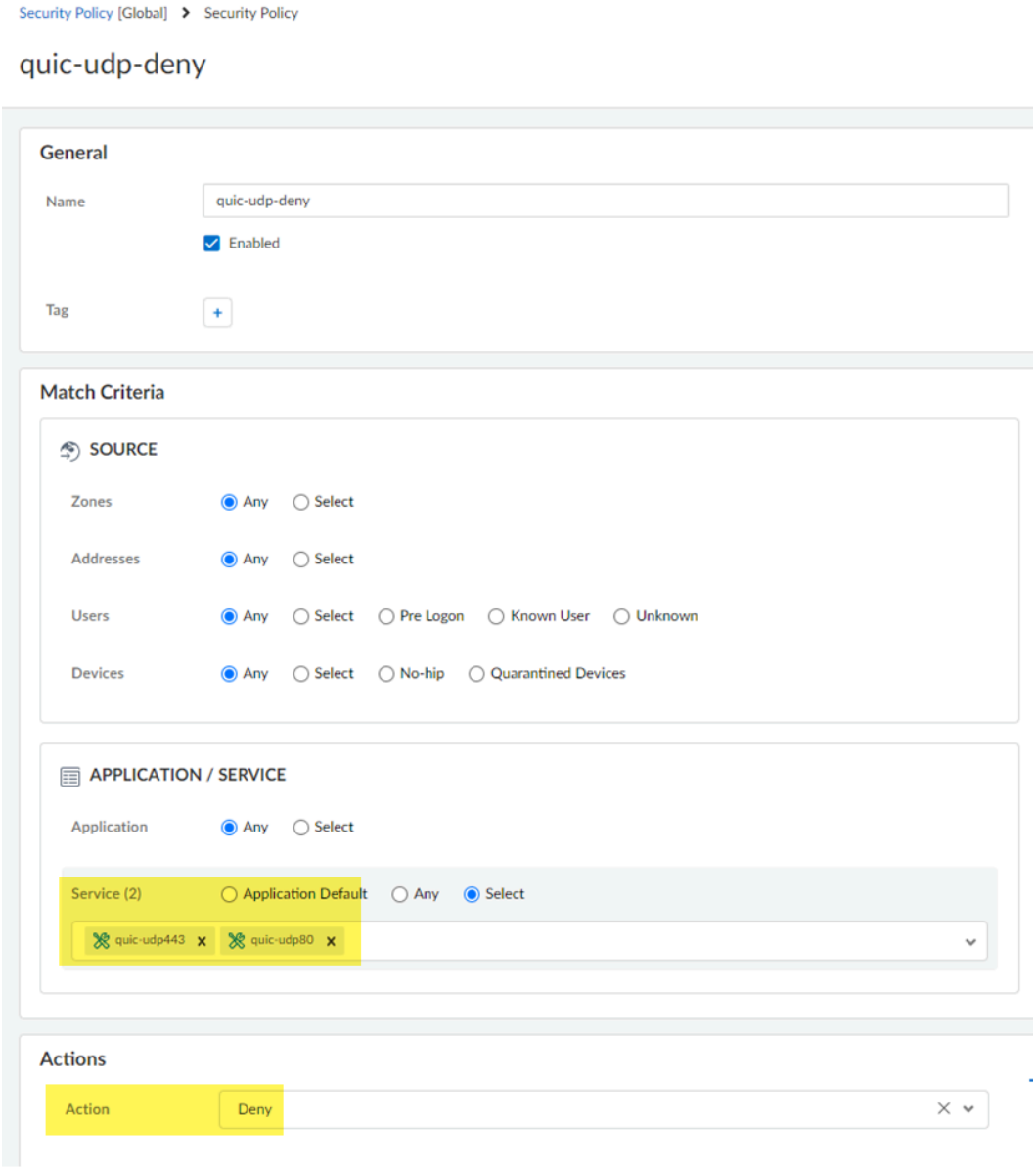
 ©2025 Palo Alto Networks, Inc.




5. 返回 **Manage**（管理） > **Configuration**（設定） > **NGFW & Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全性服務） > **Security Policy**（安全性政策）為

 ©2025 Palo Alto Networks, Inc.

第二個安全性政策**Add Rule**（新增規則），在 **Application / Services**（應用程式和服務）下指定服務，並將 **Action**（動作）指定為 **Deny**（拒絕）。




完成時，您將具有兩個安全性政策：一個封鎖 QUIC 通訊協定，一個封鎖 UDP 連接埠 80 和 443 上的流量。




 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 在 Prisma Access 範圍中匯入 Strata Cloud Manager 中的根憑證授權單位 (CA) 憑證和私密金鑰，與應用程式加速搭配使用並推送您的變更。

自我簽署根 CA/憑證是憑證鏈結中最上層的憑證。應用程式加速會使用根 CA/憑證，為加速的應用程式建立憑證。在 Prisma Access 中推送根 CA/憑證，以便應用程式加速可以開始建立應用程式特定的憑證。

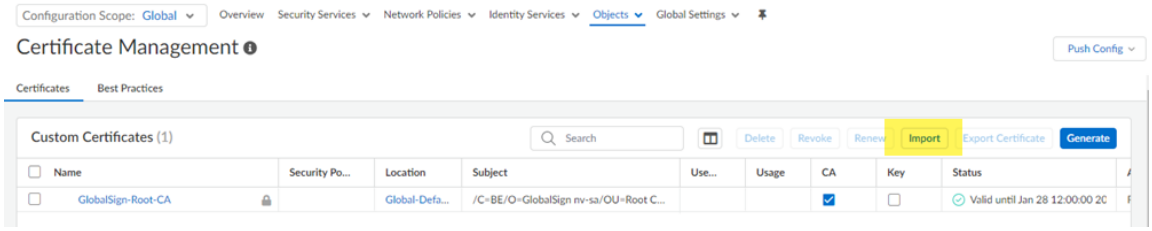
根 CA/憑證必須具有以下特性：

- CA 必須是受信任的 CA。
- （建議）CA 應該是唯一的，並且僅用於應用程式加速。
- CA 不能過期。記下 CA 到期日，並在憑證到期之前更新該憑證。如果應用程式加速使用中的 CA/憑證到期，使用者在嘗試存取加速的應用程式時將收到 SSL 錯誤。當您的組織使用應用程式加速時，確保 CA 有效至關重要。
- 它必須包含一個金鑰。
- 它必須使用複雜密碼。
- 它必須在 **Prisma Access** 範圍內。
- （僅限行動使用者—GlobalProtect 部署）它必須安裝在本機根憑證儲存區中。

  您可以依此程序中所述將此安裝新增至受信任憑證清單來執行此安裝，或者如果您使用的是 ActiveDirectory，則可以使用 Active Directory 群組政策物件 (GPO) 從 AD 散發根 CA。

如果您曾經需要變更根 CA/憑證，則必須上傳它並提交您的變更，然後才能使用變更後的憑證。

1. 移至**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（物件） > **Certificate Management**（憑證管理）。
2. **Import**（匯入）憑證。




3. 選取以下參數：
   - 為憑證輸入唯一的 **Certificate Name**（憑證名稱），例如 `AppAcceleration_CA`。

     此名稱區分大小寫，長度最多為 31 個字元。請在名稱中僅使用字母、數字、連字號與底線。
   - **Choose File**（選擇檔案）並瀏覽從 CA 收到的 **Certificate File**（憑證檔案），然後將其 **Open**（開啟）。
   - 選取 **Format**（格式）：
     - **Encrypted Private Key and Certificate (PKCS12)**（加密的私密金鑰與憑證 **(PKCS12)**）—這是預設值，也是最常見的格式，其中金鑰與憑證是在單一容器內（憑證檔案）。

 ©2025 Palo Alto Networks, Inc.

- **Base64 Encoded Certificate (PEM)**（**Base64** 編碼憑證 **(PEM)**）—您必須將金鑰與憑證分開匯入。如果您選取此格式，則需要選取一個 **Key File**（金鑰檔案）。
- 輸入 **Passphrase**（複雜密碼）和 **Confirm Passphrase**（確認複雜密碼）。

4. **Save**（儲存）變更。



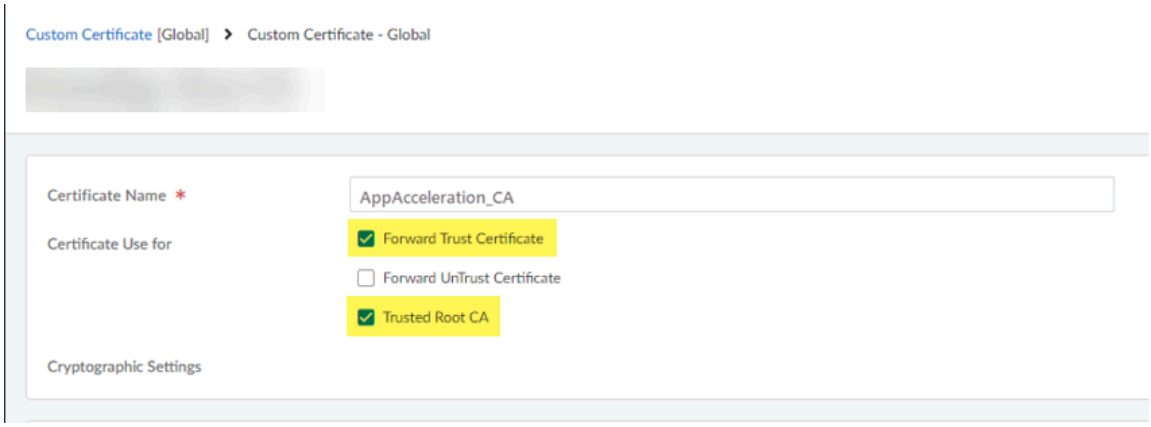


©2025 Palo Alto Networks, Inc.

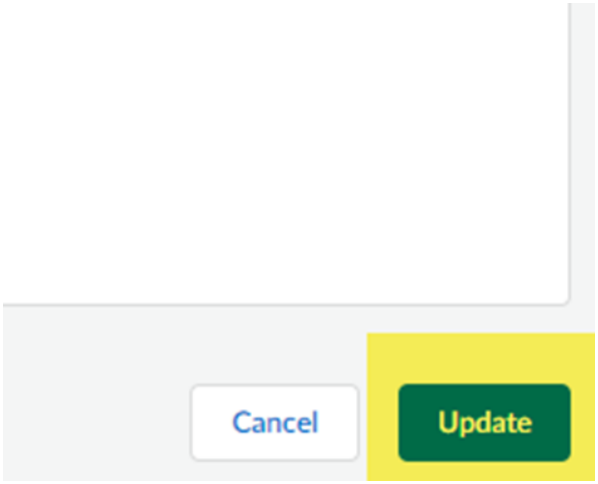
**STEP 3 |** 將您新增的根 CA/憑證標記為轉送信任憑證和受信任的根 CA。

如果您未將憑證指定為轉送信任憑證和受信任的根 CA，則使用者會在使用 SSL 解密嘗試存取加速的應用程式時遇到 SSL 錯誤。

1. 選取您已新增的根 CA/憑證。
2. 選取憑證作為 **Forward Trust Certificate**（轉送信任憑證）和 **Trusted Root CA**（受信任的根 **CA**）。



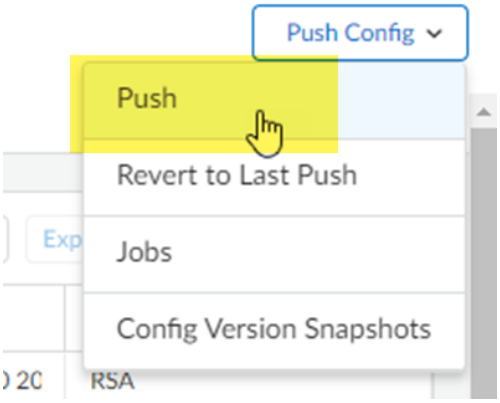

3. **Update**（更新）憑證。





©2025 Palo Alto Networks, Inc.

**STEP 4 |** **Push**（推送）您的變更。



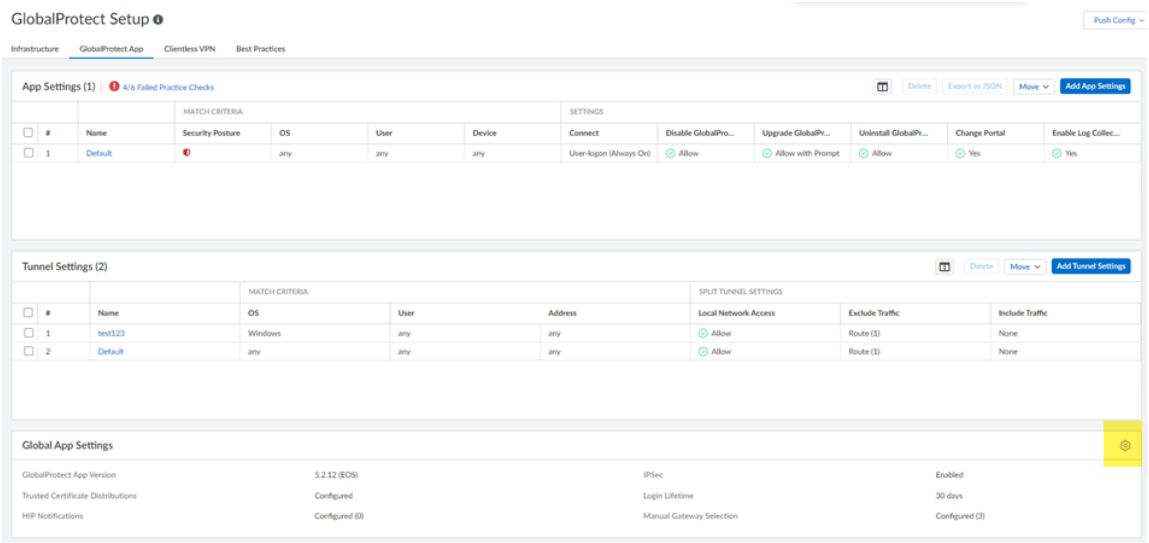


©2025 Palo Alto Networks, Inc.

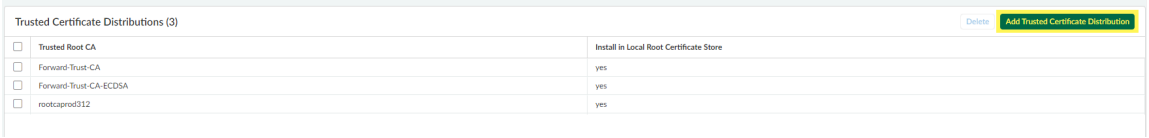
**STEP 5 |** （僅限行動使用者—GlobalProtect 部署）將您新增的根 CA/憑證新增至 GlobalProtect 受信任憑證清單，並將其安裝在本機根憑證儲存區中。

或者，如果您使用的是 *ActiveDirectory*，則可以使用 *Active Directory GPO* 從 *AD* 散發根 *CA*。

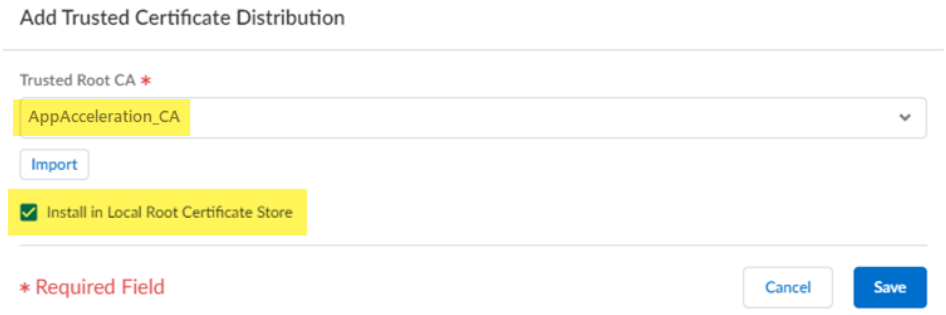
1. 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **GlobalProtect** > **GlobalProtect App**（**GlobalProtect** 應用程式） > **Global App Settings**（全域應用程式設定）。
2. 按一下齒輪以編輯 **Settings**（設定）。




3. **Add Trusted Certificate Distribution**（新增受信任憑證散發）。




4. 選取您在上一個步驟中建立的 **Trusted Root CA**（受信任根 **CA**），然後選取 **Install in Local Root Certificate Store**（安裝在本機根憑證儲存區中）。

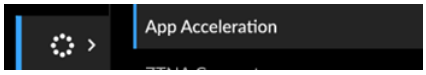



5. **Save**（儲存）變更。
6. **Push**（推送）您的變更。

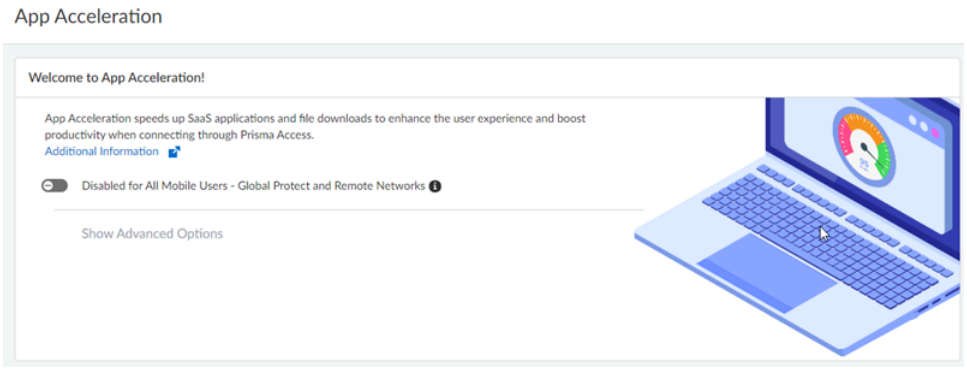
 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** 啟用應用程式加速並選擇您建立的憑證檔案。

1. 從左側導覽列前往 **Workflows**（工作流程） > **App Acceleration**（應用程式加速）。

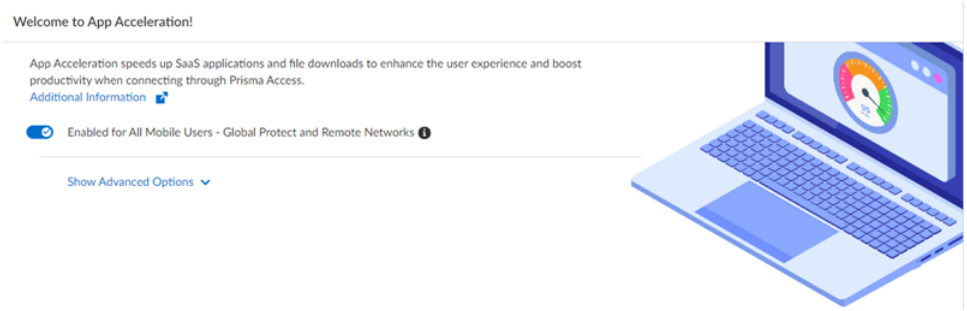



[App Acceleration（應用程式加速）] 視窗隨即顯示。




2. 將滑桿向右移動，以使應用程式加速 **Enabled for all Mobile Users—GlobalProtect and Remote Networks**（針對所有行動使用者—**GlobalProtect** 和遠端網路啟用）。

如果提交正在進行，應用程式加速設定將在所有提交完成後生效。

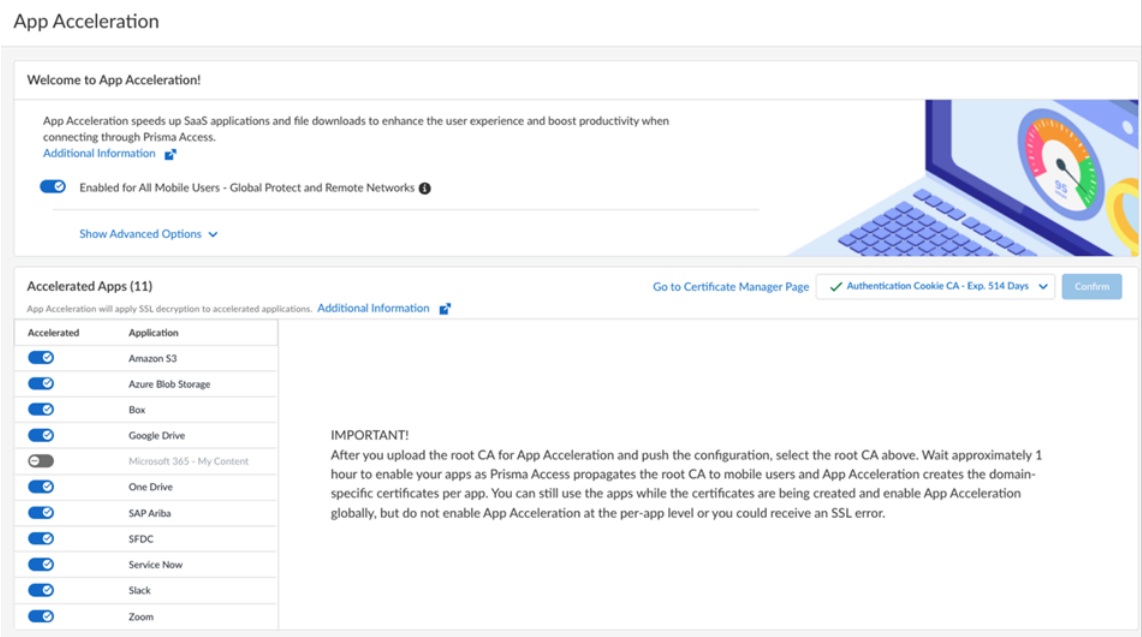



應用程式加速將針對所有 TCP 流量啟用。如果您想要加速 SaaS 應用程式，則需要選取根 CA/憑證，如下一個步驟所示。


©2025 Palo Alto Networks, Inc.

**STEP 7 |** 選取您在上一個步驟中建立的憑證。

如果您需要變更現有憑證，請確保您已將該憑證提交並推送至防火牆和使用者，然後在此處選取它。您必須先提交新憑證，然後才能選取它。




在匯入憑證之後，您必須等待直到應用程式加速為每個應用程式產生網域特定的憑證。此程序可能最多需要一小時。同時，您可以將 ***Accelerated Apps***（加速的應用程式）的滑桿向左移動，以暫時停用應用程式加速並存取應用程式，直到產生憑證；如果不這樣做，您可能會收到 *SSL* 錯誤，直到產生憑證。

為給定應用程式開啟加速之後，允許最多 *10* 分鐘讓加速作用中。

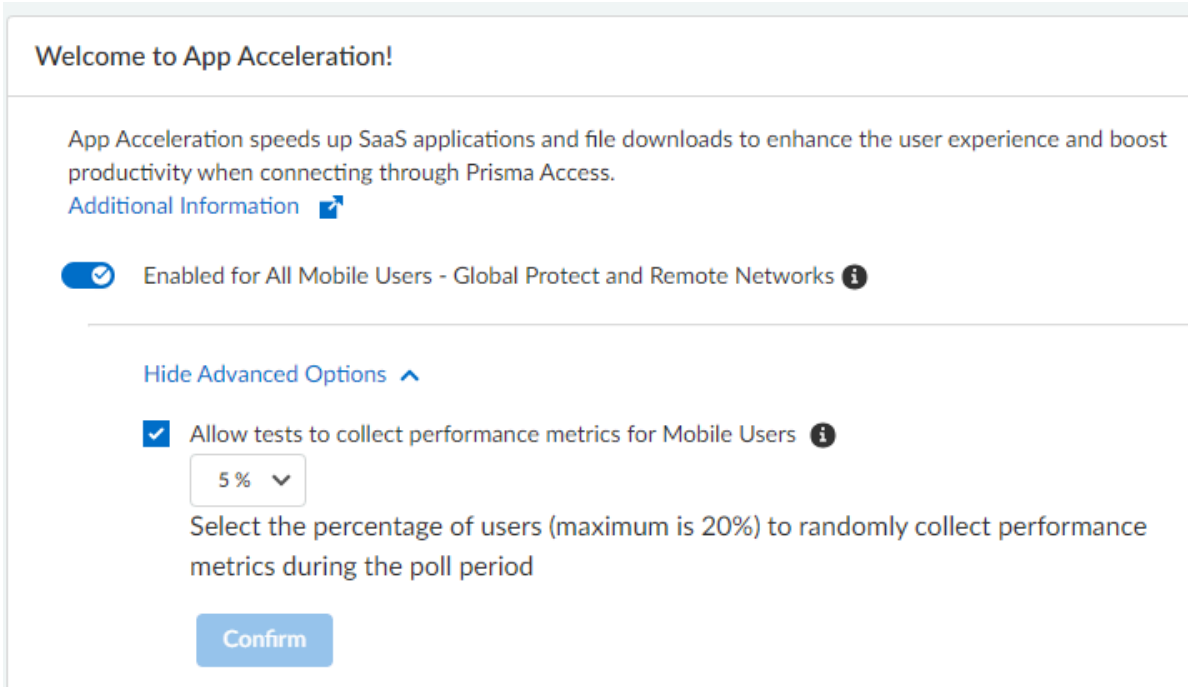

©2025 Palo Alto Networks, Inc.

**STEP 8 |** （選用）**Show Advanced Options**（顯示進階選項）並變更指標測試參數。

- （選用）若要停用指標收集以取得效能訊息，請取消選取 **Allow tests to collect performance metrics for Mobile Users**（允許測試收集行動使用者的效能指標）。

  Palo Alto Networks 建議您在使用應用程式加速時啟用指標收集，以檢視應用程式效能改進。

- （選用）若要變更處理預測測試的使用者百分比（預設為 5%），請在下拉式清單中選取另一個百分比，並 **Confirm**（確認）變更。




 ©2025 Palo Alto Networks, Inc.

# 在 Prisma Access 中設定應用程式加速 (Panorama)

若要在 Prisma Access (Managed by Panorama) 部署中設定應用程式加速，請完成此工作。

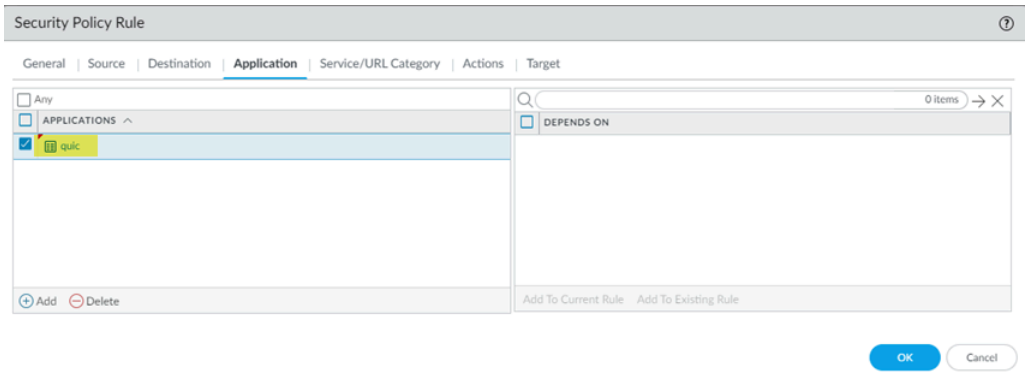
**STEP 1 |** （選用）停用快速 UDP 網際網路連線 (QUIC) 通訊協定。

若未停用 QUIC，應用程式加速無法在第七層加速應用程式。

1. 前往 **Policies**（政策） > **Security**（安全性） > **Pre Rules**（前置規則），並 **Add**（新增）安全性政策。

   在 **Shared**（共用） 裝置群組中建立此安全性政策規則。

2. 選取 **Application**（應用程式）為 **quic**，並選取 **Actions**（動作）為 **Deny**（拒絕）。




3. **Add**（新增）第二個安全性政策。

   QUIC 的較新版本可能被錯誤識別為 **unknown-udp**。基於此原因，Palo Alto Networks 建議為 UDP 連接埠 80 和 UDP 連接埠 443 新增服務，並建立額外的安全性政策以封鎖這些連接埠上的 UDP 流量。

4. 在 **Service/URL Category**（服務/**URL** 類別）下，為 UDP 連接埠 80 和 UDP 連接埠 443 **Add**（新增）服務，並新增 **Action**（動作）為 **Deny**（拒絕）。

   完成時，您將具有兩個安全性政策：一個封鎖 QUIC 通訊協定，一個封鎖 UDP 連接埠 80 和 443 上的流量。

| | NAME | LOCATION | APPLICATION | TAGS | ACTION | SERVICE | PROFILE |
|---|---|---|---|---|---|---|---|
| 1 | quic-deny | Shared | quic | none | Deny | application-... | none |
| 2 | quic-udp-deny | Shared | any | none | Deny | quic-udp80<br>quic-udp443 | none |


©2025 Palo Alto Networks, Inc.

**STEP 2 |** 在 Panorama 中匯入根憑證授權單位 (CA) 憑證和私密金鑰，與應用程式加速搭配使用，然後提交並推送您的變更。

自我簽署根 CA/憑證是憑證鏈結中最上層的憑證。應用程式加速會使用根 CA/憑證，為加速的應用程式建立憑證。在 Prisma Access 中推送根 CA/憑證，以便應用程式加速可以開始建立應用程式特定的憑證。

根 CA/憑證必須具有以下特性：

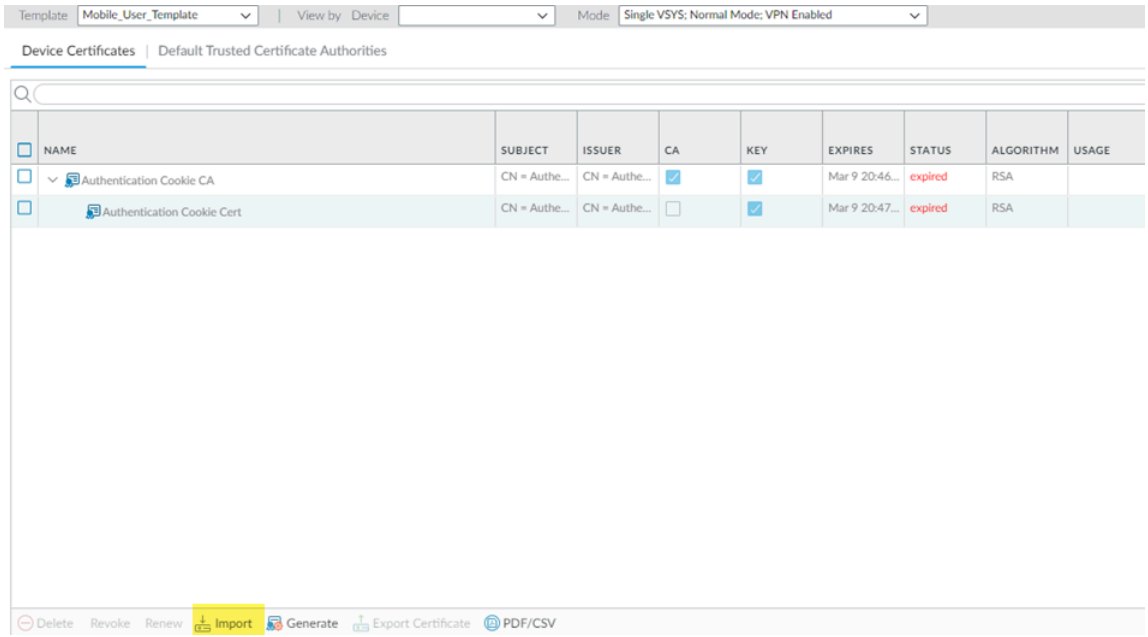
- CA 必須是受信任的 CA。
- （建議）CA 應該是唯一的，並且僅用於應用程式加速。
- CA 不能過期。記下 CA 到期日，並在憑證到期之前更新該憑證。如果應用程式加速使用中的 CA/憑證到期，使用者在嘗試存取加速的應用程式時將收到 SSL 錯誤。當您的組織使用應用程式加速時，確保 CA 有效至關重要。
- 它必須包含一個金鑰。
- 它必須使用複雜密碼。
- （僅限行動使用者—GlobalProtect 部署）它必須安裝在本機根憑證儲存區中。

  您可以依此程序中所述將此安裝新增至受信任憑證清單來執行此安裝，或者如果您使用的是 ActiveDirectory，則可以使用 Active Directory 群組政策物件 (GPO) 從 AD 散發根 CA。

如果您曾經需要變更根 CA/憑證，則必須上傳它，且提交並推送您的變更，然後才能使用變更後的憑證。

1. 前往 **Device**（裝置） > **Certificates**（憑證） > **Certificate Management**（憑證管理）。

   確保您在 Mobile_User_Template 中。
2. **Import**（匯入）憑證。



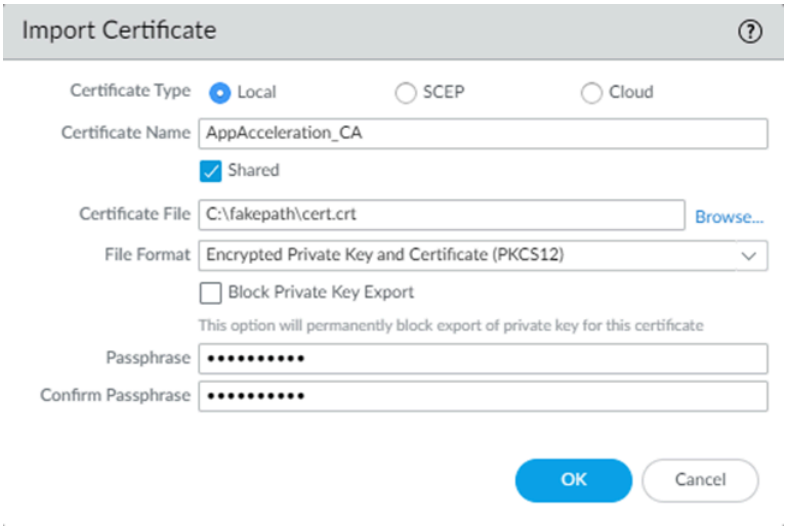

3. 選取以下參數：
   - 為憑證輸入唯一的 **Certificate Name**（憑證名稱），例如 `AppAcceleration_CA`。

 ©2025 Palo Alto Networks, Inc.

此名稱區分大小寫，長度最多為 31 個字元。請在名稱中僅使用字母、數字、連字號與底線。

- 瀏覽從 CA 收到的 **Certificate File**（憑證檔案），然後將其 **Open**（開啟）。
- 選取 **Format**（格式）：
  - **Encrypted Private Key and Certificate (PKCS12)**（加密的私密金鑰與憑證 **(PKCS12)**）—這是預設值，也是最常見的格式，其中金鑰與憑證是在單一容器內（憑證檔案）。
  - **Base64 Encoded Certificate (PEM)**（**Base64** 編碼憑證 **(PEM)**）—您必須將金鑰與憑證分開匯入。如果您選取此格式，則需要 **Import Private Key**（匯入私密金鑰），並選取一個 **Key File**（金鑰檔案）。
  - 輸入 **Passphrase**（複雜密碼）和 **Confirm Passphrase**（確認複雜密碼）。

4. 按一下 **OK**（確定）。




5. 重複這些步驟，將 Remote_Network_Template 替代為 Mobile_User_Template。

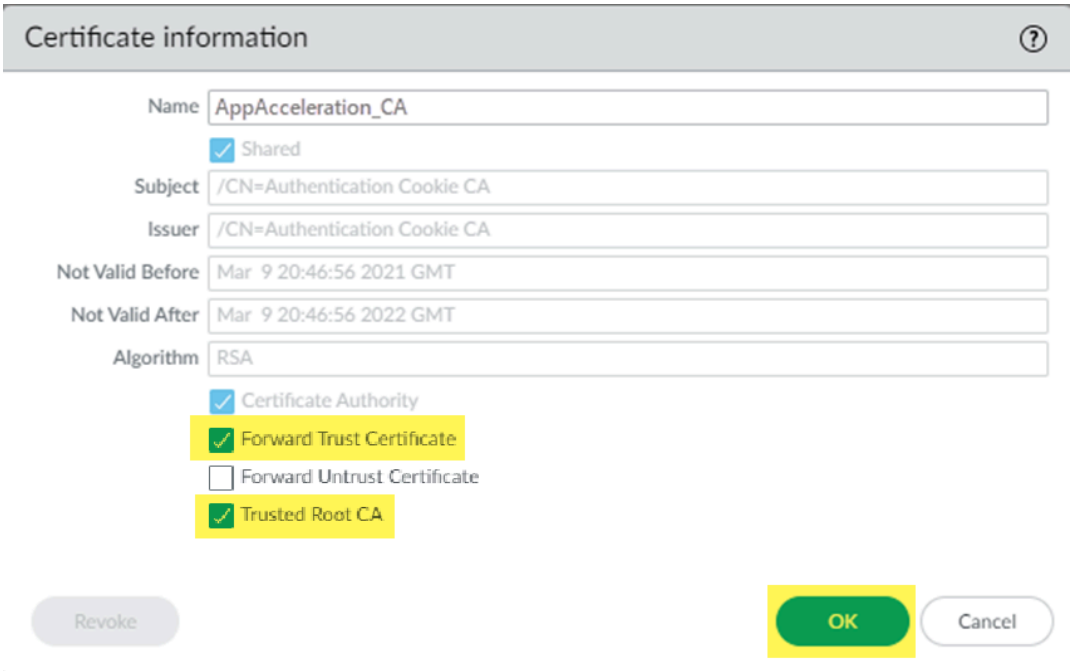
   您必須在 Mobile_User_Template 和 Remote_Network_Template 中匯入這些憑證，才能為您的行動使用者和遠端網路網站的使用者加速應用程式。


©2025 Palo Alto Networks, Inc.

**STEP 3 |** 將您新增的根 CA/憑證標記為轉送信任憑證和受信任的根 CA。

如果您未將憑證指定為轉送信任憑證和受信任的根 CA，則使用者會在使用 SSL 解密嘗試存取加速的應用程式時遇到 SSL 錯誤。如果您在 Mobile_User_Template 和 Remote_Network_Template 中具有憑證，請在這兩個範本執行此步驟。

1. 選取您已新增的根 CA/憑證。
2. 選取憑證作為 **Forward Trust Certificate**（轉送信任憑證）和 **Trusted Root CA**（受信任的根 **CA**），然後按一下 **OK**（確定）。



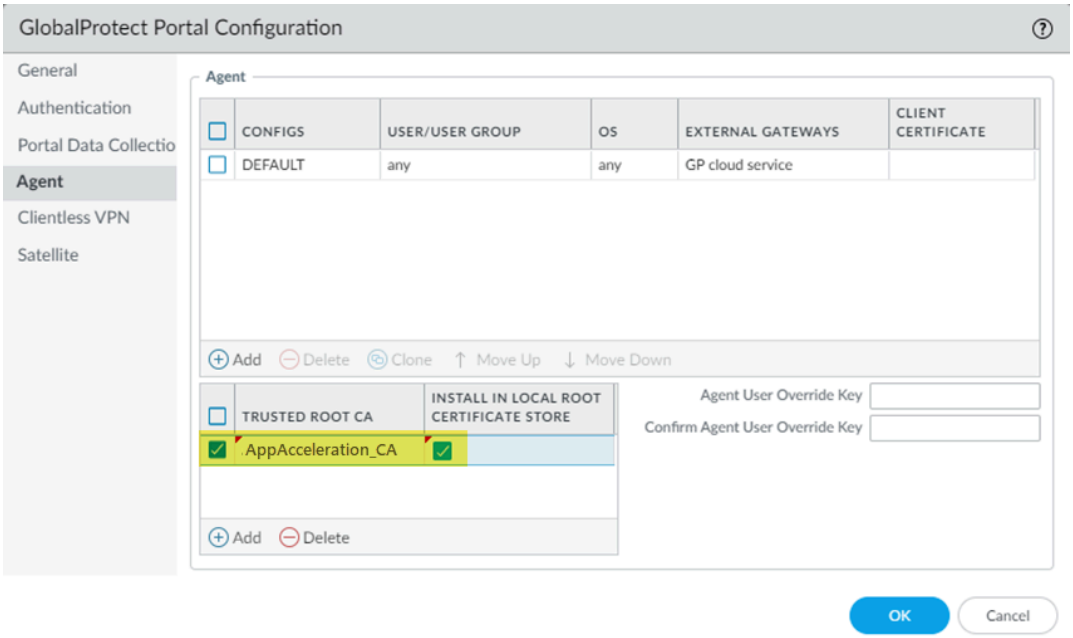

**STEP 4 |** **Commit and Push**（提交並推送）您的變更。


©2025 Palo Alto Networks, Inc.

**STEP 5 |** （僅限行動使用者—GlobalProtect 部署）將您新增的根 CA/憑證新增至 GlobalProtect 入口網站設定中的 GlobalProtect 受信任憑證清單。

或者，如果您使用的是 *ActiveDirectory*，則可以使用 *Active Directory GPO* 從 *AD* 散發根 *CA*。

1. 前往 **Network**（網路） > **GlobalProtect** > **Portals**（入口網站） > **GlobalProtect_Portal** > **Agent**（代理程式）。
   確保您在 Mobile_User_Template 中。
2. **Add**（新增）您在上一個步驟中建立的根 CA。
3. 選取 **Install in Local Root Certificate Store**（安裝在本機根憑證存放區中）。
4. 按一下 **OK**（確定）。

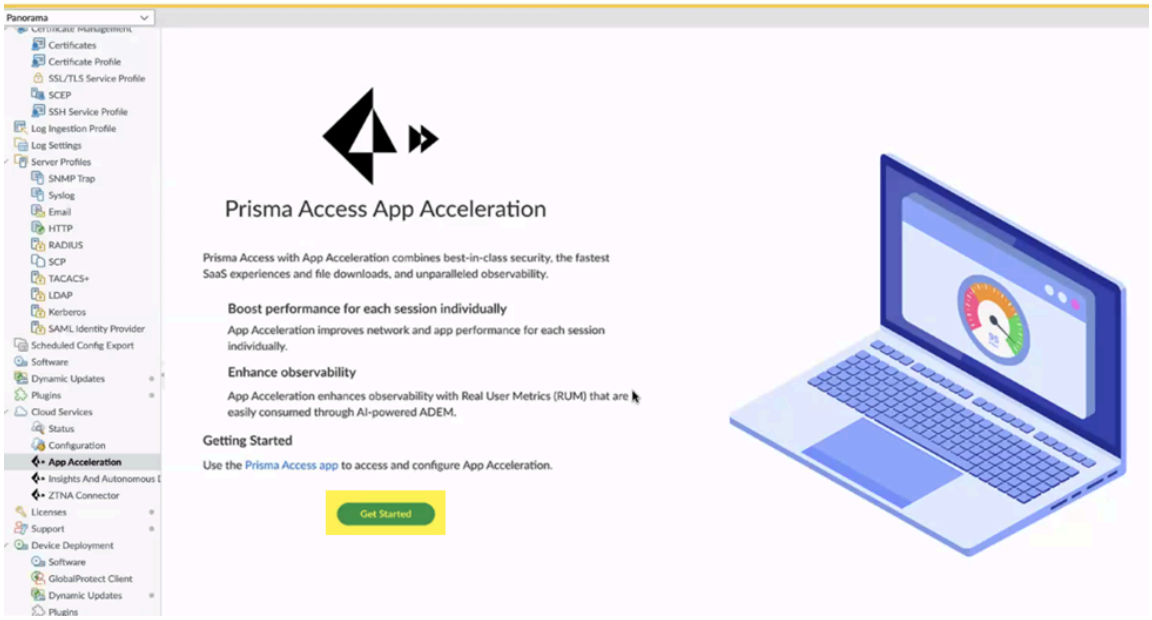



5. **Commit and Push**（提交並推送）您的變更。

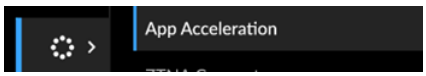
 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** 啟用應用程式加速並選擇您建立的憑證檔案。

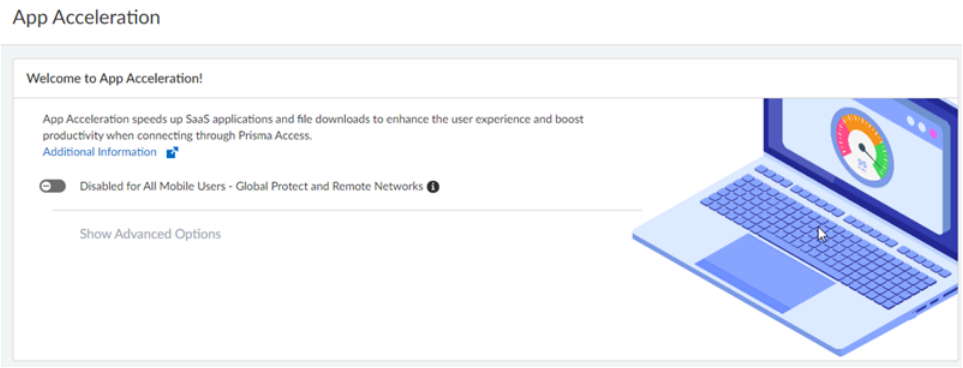
1. 前往 **Panorama** > **Cloud Services**（雲端服務） > **App Acceleration**（應用程式加速）和 **Get Started**（開始）使用應用程式加速。




2. 從左側導覽列前往 **Workflows**（工作流程） > **App Acceleration**（應用程式加速）。



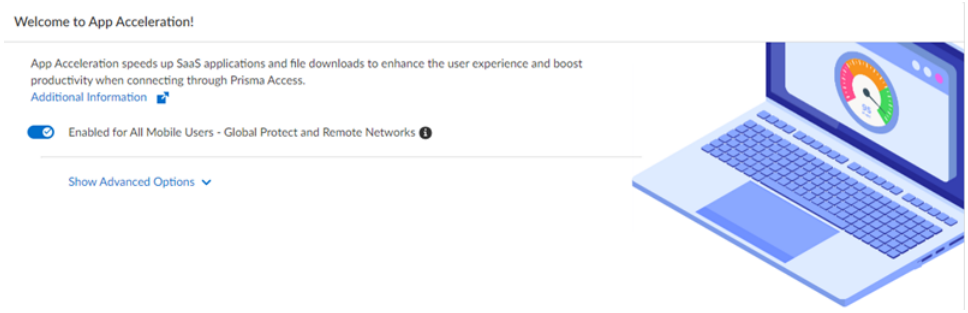

[App Acceleration（應用程式加速）] 視窗隨即顯示。




3. 將滑桿向右移動，以使應用程式加速 **Enabled for all Mobile Users—GlobalProtect and Remote Networks**（針對所有行動使用者—**GlobalProtect** 和遠端網路啟用）。

如果提交正在進行，應用程式加速設定將在所有提交完成後生效。

 ©2025 Palo Alto Networks, Inc.



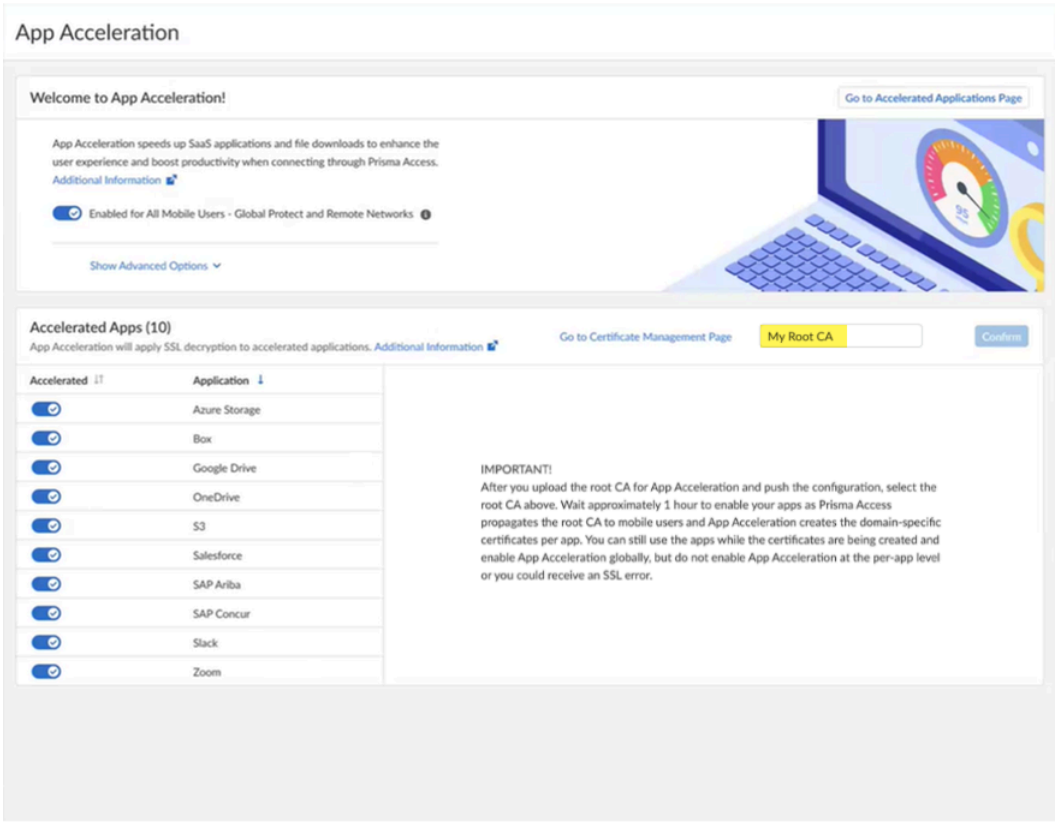

應用程式加速將針對所有 TCP 流量啟用。如果您想要加速 SaaS 應用程式，則需要選取根 CA/憑證，如下一個步驟所示。


©2025 Palo Alto Networks, Inc.

**STEP 7 |** 在應用程式加速設定中，請確切地輸入您在先前步驟中建立的憑證名稱，與 Panorama 中列出的名稱完全相同。

請確保在輸入憑證之前，您已提交並推送該憑證。

如果您需要變更現有憑證，請輸入新名稱。您必須輸入名稱（您無法從清單中選取），並且在輸入名稱之前，您必須提交並推送新的憑證。




在匯入憑證之後，您必須等待直到應用程式加速為每個應用程式產生網域特定的憑證。此程序可能最多需要一小時。同時，您可以將 ***Accelerated Apps***（加速的應用程式）的滑桿向左移動，以暫時停用應用程式加速並存取應用程式，直到產生憑證；如果不這樣做，您可能會收到 *SSL* 錯誤，直到產生憑證。

為給定應用程式開啟加速之後，允許最多 *10* 分鐘讓加速作用中。

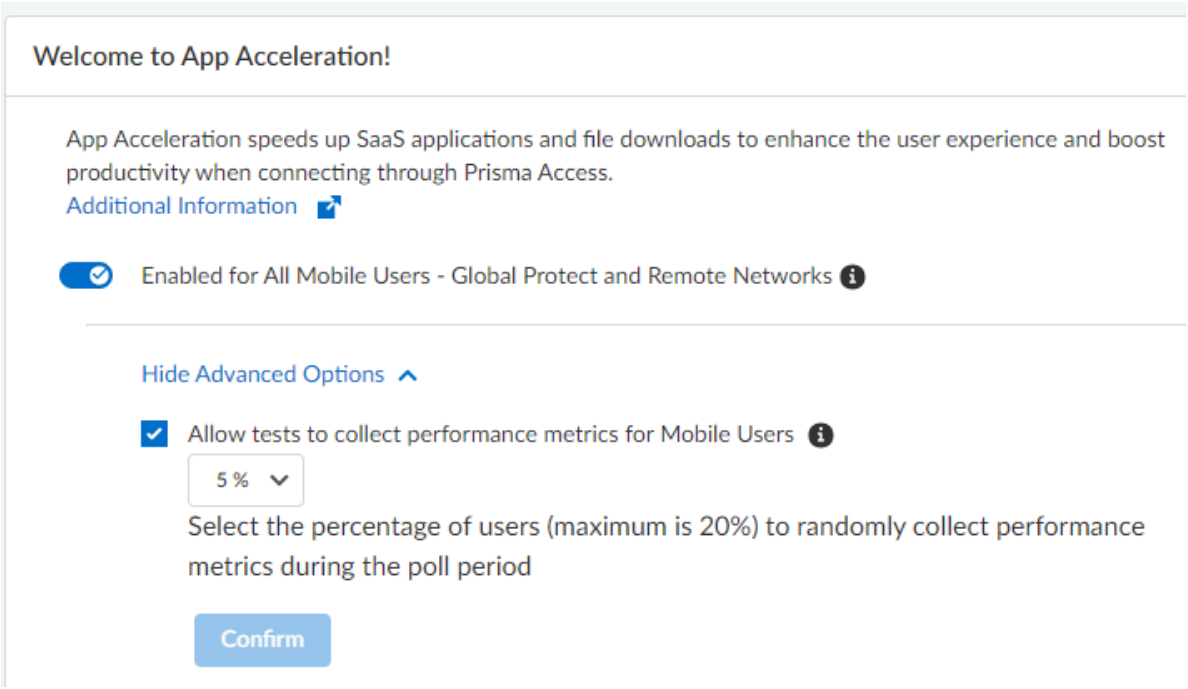

©2025 Palo Alto Networks, Inc.

**STEP 8 |** （選用）**Show Advanced Options**（顯示進階選項）並變更指標測試參數。

- （選用）若要停用指標收集以取得效能訊息，請取消選取 **Allow tests to collect performance metrics for Mobile Users**（允許測試收集行動使用者的效能指標）。

  Palo Alto Networks 建議您在使用應用程式加速時啟用指標收集，以檢視應用程式效能改進。

- （選用）若要變更處理預測測試的使用者百分比（預設為 5%），請在下拉式清單中選取另一個百分比，並 **Confirm**（確認）變更。





©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

# Prisma Access 行動使用者

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

Prisma Access 提供兩種連線方法來保護行動使用者：使用者可以使用 GlobalProtect 應用程式或使用 Proxy 自動設定 (PAC) 檔案連線到 Prisma Access。

- 使用 **GlobalProtect** 應用程式保護行動使用者

  您可以在下列模式下使用 GlobalProtect：

  - 通道模式—Prisma Access 中 GlobalProtect 的預設代理程式模式。建立通往 Prisma Access 的通道（IPSec 或 SSL），以保護行動使用者對所有應用程式、連接埠和通訊協定的存取，並獲得一致的安全性，無論使用者位於網路內部還是外部。

    安裝在使用者端點上的 GlobalProtect 應用程式可保護網際網路、SaaS 應用程式，以及內部和公用雲端資源的使用者流量。將 GlobalProtect 應用程式部署到您的使用者（適用於執行 Microsoft Windows、Apple macOS，以及 iOS、Android、Google Chrome OS 和 Linux 的智慧型手機、平板電腦或筆記型電腦），以便他們可以將流量透過通道傳輸至 Prisma Access，用於政策強制執行和威脅防護。GlobalProtect 應用程式還會提供主機資訊設定檔 (HIP) 報告，以便您可以根據裝置狀態建立細緻規則，以確保端點遵守您的安全標準—例如，它們配備了最新的修補程式、加密和病毒定義—以存取您最敏感的應用程式。或者，若要啟用對未受管理裝置上使用者的安全存取，您可以啟用無用戶端 VPN。Prisma Access 根據您使用者目前所在的位置動態地縮減和擴增每個區域。
  - Proxy 模式—此模式使您能夠在使用第三方 VPN 代理程式，同時仍然使用 Prisma Access 作為 安全 Web 閘道，取得一致且卓越的 SaaS 安全性。如果您尚未準備好取代現有的私人應用程式 VPN，但想要取代安全 Web 閘道，則此連線方法是理想的選擇。例如，您正在使用第三方 VPN 代理程式進行私人存取，但您只想要為了您的網際網路安全性使用 Prisma Access。這種連線方法的優點包括：
    - 滿足需要 Proxy 的合規性或網路需求
    - 減輕 PAC 檔案管理的負擔，並支援瀏覽器以外的 Proxy 感知應用程式
    - 無需回傳到內部部署 Web Proxy，從而改善使用者體驗
  - 通道和 Proxy 模式—此模式使您能夠透過 Proxy 模式安全地存取網際網路和 SaaS 應用程式，並透過通道模式安全地存取私人應用程式。如果您需要以最快、最低延遲存取私人應用程式，並且您的 Prisma Access 位置不在您所在的區域，此模式特別有用。

    在此模式下，GlobalProtect 應用程式首先評估您已定義的明確 Proxy 轉送規則，並將所有網際網路繫結流量傳送到 Prisma Access 明確 Proxy。對於所有其他流量，應用程式根據您已定義的任何分割通道規則確定哪些流量透過通道傳送至 GlobalProtect 閘道，以及哪些流量從通道中排除。您也可以使用通道來保護任何沒有 Proxy 感知的應用程式。

- 使用 **PAC** 檔案保護行動使用者

  除了使用 GlobalProtect 保護行動使用者之外，您還可以使用 Prisma Access 設定明確 Proxy。透過明確 Proxy，端點會使用 PAC 檔案，指示 Web 瀏覽器和 Proxy 感知應用程式將流量轉送到 Web Proxy 伺服器，而不是目的地伺服器，從而保護 Web 式網際網路（HTTP 和 HTTPS）流量。

  如果您組織的現有網路已使用明確 Proxy，並在您的用戶端端點和伺服器上部署 PAC 檔案，則您可以順暢地從舊版 Proxy 型 SWG 解決方案移轉至 Prisma Access，以保護行動使用者的輸出網際網路流量。如果需要基於稽核或合規性目的使用 Proxy，您也可以使用明確 Proxy。

- 使用 **Prisma Access Browser Mobile** 保護行動使用者

  Prisma Access Browser Mobile 透過將強大的存取控制與明確、直覺的介面結合，簡化了行動使用者的保護。它允許使用者安全地存取私人應用程式，而無需依賴 VPN、憑證或行動裝置管理 (MDM) 系統，從而降低複雜性並簡化連線。

  它專為自攜裝置 (BYOD) 環境而設計，可確保安全地存取未受管理裝置上的私人應用程式，使組織能夠將重要資源延伸到其全體勞動力。平板電腦透過 Prisma Access Browser Mobile 成為多功能桌面替代方案，從而提供與傳統端點相同等級的安全性和存取權。

  透過 Prisma Access Browser Mobile，您的組織可以簡化對私人應用程式的存取、提高平板電腦型生產力，並在不同的行動平台上維護可靠的安全性。


©2025 Palo Alto Networks, Inc.

# 行動使用者：GlobalProtect

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

GlobalProtect 可讓您透過在行動使用者的端點上安裝 GlobalProtect 應用程式，並在 Prisma Access 中設定 GlobalProtect 設定來保護行動使用者。GlobalProtect 可讓您保護行動使用者對所有應用程式、連接埠和通訊協定的存取，並取得一致的安全性，無論使用者位於您的網路內部還是外部。

當您使用 GlobalProtect 保護行動使用者時，將需要定義設定以在雲端中設定入口網站和閘道。例如，您將定義入口網站主機名稱、為行動使用者設定 IP 位址集區，以及為內部網域設定 DNS 設定。您可以藉助將現有的設定用於某些必要的設定，例如使用哪個驗證設定檔來驗證行動使用者。如果您已有一個範本包含您的驗證設定檔、憑證、憑證設定檔和伺服器設定檔，則可以在裝載期間將該範本新增至預先定義的範本堆疊，以簡化設定程序。

此外，如果您想要行動使用者能夠連線到遠端網路位置，或者如果您有位於不同地理區域的行動使用者，他們需要直接存取彼此的端點，則必須設定至少一個具有預留位置的服務連線，即使您不打算使用該連線，來提供對資料中心或總部位置的存取也一樣。需要這樣做的原因是，雖然所有遠端網路位置都已完互聯，但 Prisma Access 閘道（也稱為位置）會連線到中樞和支點架構中的服務連線，以提供對您 Prisma Access 基礎結構中內部網路的存取。

- 規劃 Prisma Access 上 GlobalProtect 的檢查清單
- 設定 GlobalProtect 行動使用者
- GlobalProtect—自訂通道設定
- 提出票證要求以停用 GlobalProtect (Strata Cloud Manager)
- 監控 GlobalProtect 行動使用者
- 用於 GlobalProtect 行動使用者部署的 IP 位址集區
- GlobalProtect 應用程式如何為行動使用者選取 Prisma Access 位置
- 允許列出 GlobalProtect 行動使用者
- GlobalProtect 應用程式升級
- 整合 Prisma Access 與內部部署 GlobalProtect 閘道

## 規劃 Prisma Access 上 GlobalProtect 的檢查清單

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | • Prisma Access 授權 |


©2025 Palo Alto Networks, Inc.

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | |

如果您使用 GlobalProtect 保護行動使用者，請使用以下檢查清單，確保您能夠成功啟用服務，並對您的行動使用者執行一致的政策（保護在其端點上安裝了 GlobalProtect 應用程式的使用者，並允許使用者安全地使用無用戶端 VPN 存取應用程式）。

- 安裝前檢查清單：
  - **IP** 位址集區—若要設定 Prisma Access for Users，您需要提供一個 IP 位址集區，其不與您內部使用的其他 IP 位址重疊，也不與您指定給基礎結構子網路的 IP 位址集區重疊。

    我們建議使用符合 *RFC 1918* 的 *IP* 位址集區。雖然使用不符合 *RFC 1918*（公用）*IP* 位址是可行的，但我們不建議這麼做，因為可能會與網際網路公用 *IP* 位址空間發生衝突。

    請勿指定與下列 IP 位址和子網路重疊的任何子網路，因為 Prisma Access 會保留這些 IP 位址和子網路供內部使用：

    169.254.0.0/16 和 100.64.0.0/10

    Prisma Access 使用此 IP 位址集區，在端點的虛擬網路介面卡使用 GlobalProtect 應用程式連線至 Prisma Access 時，將 IP 位址指派給這些介面卡。每個連線到 Prisma Access 行動使用者閘道的裝置都需要自己的 IP 位址。您在行動使用者裝載過程中指定這些集區。

    Palo Alto Networks 建議集區中的 IP 位址數目是將連線至 Prisma Access 的行動使用者裝置數目的 2 倍如果您的組織有自攜裝置 (BYOD) 政策，或如果單一使用者有多個使用者帳戶，請確保在配置您的 IP 集區時將這些額外的裝置和帳戶納入考慮。如果 IP 位址集區達到其限制，額外的行動使用者裝置將無法連線。

    當行動使用者裝置連線到閘道時，Prisma Access 會從您指定的集區中取得 IP 位址，並將其與 /24 區塊中的閘道建立關聯。當 /24 區塊隨著更多使用者裝置登入而達到其限制時，Prisma Access 會從集區中將更多的 /24 區塊配置給閘道。根據其閘道指派，Prisma Access 會在這些 /24 子網路進行配置時將其公告至骨幹。
  - 範本—Prisma Access GlobalProtect 部署會自動建立一個範本堆疊和一個最上層範本。如果已在內部部署執行 GlobalProtect，並且想要利用現有的設定，您可以將額外的範本新增到堆疊，以將現有的 GlobalProtect 入口網站、GlobalProtect 閘道、User-ID、伺服器設定檔（例如，用於連線到您的驗證服務）、憑證，以及 SSL/TLS 服務設定檔設定推送至 Prisma Access for Users。如果您沒有範本具有現有的設定，則可以在 Prisma Access (Managed by Panorama) 上設定 GlobalProtect 時手動輸入所需的設定。此外，您新增至堆疊的任何範本必須包含區域的區域設定，而您會使用這些區域，為行動使用者強制執行安全性政策。
  - 父系裝置群組—當設定 Prisma Access for Users 時，您必須指定一個父系裝置群組，以在推送位址群組和安全性政策、安全性設定檔、其他政策物件（例如應用程式群組和物

 ©2025 Palo Alto Networks, Inc.

件）、HIP 物件和設定檔，以及服務為遠端使用者強制執行一致政策所需的驗證服務時使用此父系裝置群組。

- 要裝載的位置—Prisma Access 為您提供全球位置，其中您可以在 Prisma Access (Managed by Panorama) 上設定 GlobalProtect。在裝載您的位置之前，請檢視此清單，以確定您應裝載哪些位置，進行您的行動使用者部署。

  選擇離您使用者最近的位置或與您使用者位於同一國家/地區的位置。如果在您行動使用者所在的國家/地區沒有可用的位置，您可以挑選一個使用與您行動使用者相同語言的位置。

  您也可以依地理區域劃分位置。將所有位置保留在單一區域內，允許您僅為該區域指定 IP 位址集區，這在您可以配置給該集區的 IP 位址數目有限的情況下非常有用。單一區域 IP 位址集區也提供對已部署區域的更細緻控制，並允許您依據政策或行業法規排除區域。

  如果您具有 Prisma Access for Users 的本機授權，並且同時具有 GlobalProtect 部署以及明確 Proxy 部署，則對於這兩個結合的部署，您可以部署最多五個位置。您需要在這兩個部署之間配置五個位置（例如，行動使用者—GlobalProtect 兩個位置，行動使用者—明確 Proxy 三個位置）。如果您具有全球授權，則位置數目上限沒有任何限制。

- 入口網站主機名稱—Prisma Access for Users 可讓您快速且輕鬆地使用預設網域名稱 (`.gpcloudservice.com`) 設定入口網站主機名稱。在此情況下，雲端服務會自動將主機名稱發佈到公用 DNS 伺服器，並處理所有憑證生成。不過，您可以選擇在入口網站主機名稱中使用您自己的公司網域。如果您打算使用公司網域名稱，則必須為入口網站取得您自己的憑證，並在設定服務之前將 SSL/TLS 服務設定檔設定為指向該憑證。此外，如果您在入口網站主機名稱中使用自己的網域名稱，則還需要設定您的 DNS 伺服器，以指向設定過程中提供的入口網站 DNS CNAME。

- 服務連線—如果您想要讓行動使用者能夠存取內部網路上的驗證伺服器等資源（例如，資料中心或總部位置的驗證伺服器），或者讓行動使用者能夠存取您的遠端網路位置，則您必須建立並設定服務連線。

  即使您不打算使用該連線，來提供對內部資源的存取，如果您想要行動使用者能夠連線到遠端網路位置，或者如果您在不同地理區域有需要直接存取彼此端點的行動使用者，則您必須使用預留位置值設定至少一個服務連線。

- 在您的網路中使用 **IPv6**—確定您是否想要為網路中的 IPv6 流量執行任何緩解方式，以減少攻擊面。在可以同時處理 IPv4 和 IPv6 流量的雙堆疊端點中，行動使用者 IPv6 流量預設不會傳送到 Prisma Access，而是傳送到端點上的本機網路介面卡。因此，Palo Alto Networks 建議您將 Prisma Access 設定為排除 IPv6 流量。

- 為 **GlobalProtect** 端點進行記錄—您有兩種選項，可從使用 GlobalProtect 應用程式的行動使用者收集日誌：

  - 從 **GlobalProtect** 端點手動收集日誌—讓行動使用者從 GlobalProtect 應用程式中收集 Windows、macOS 和 Linux 裝置的日誌。此選項不需要額外的設定。

  - 收集 **GlobalProtect** 應用程式日誌進行疑難排解—允許 GlobalProtect 應用程式執行端到端診斷測試，以解決連線、效能和存取問題，並產生疑難排解和診斷日誌，以傳送至 Strata Logging Service 進一步分析。您需要產生憑證，以便 GlobalProtect 應用程式可以使用 Strata Logging Service 進行驗證，以收集疑難排解日誌。使用 **Prisma Access (Managed by Strata Cloud Manager)**，您可以啟用 GlobalProtect 應用程式從 Strata Logging Service 收集日誌以進行疑難排解。對於 **Prisma Access (Managed by Panorama)**，這項功能位於 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定） > **Generate Certificate for**

 ©2025 Palo Alto Networks, Inc.

**GlobalProtect App Log Collection and Autonomous DEM**（為 **GlobalProtect** 應用程式日誌收集和自發 **DEM** 產生憑證）之下。如需設定詳細資訊，請參閱收集 GlobalProtect 應用程式日誌以進行疑難排解。

- 安裝後檢查清單：
  - 將公用 **IP** 位址新增到您網路中的允許清單—在裝載您的位置之後，您需要取得每個位置使用的公用和 IP 位址，並將這些位置的 IP 位址新增到您網路中的允許清單，以允許行動使用者存取 SaaS 或公用應用程式。如果您新增更多位置，還需要擷取 Prisma Access 為剛新增位置配置的新 IP 位址。
  - 閘道命名一致性—如果您有現有的行動使用者—GlobalProtect 部署，並且您的組織有併購 (M&A) 活動，則可能需要現有的閘道不參考早期的品牌名稱，或參考新的品牌名稱。在此情況下，請聯繫您的 Palo Alto Networks 客戶團隊，他們將會開啟 SRE 案例來滿足此要求。Palo Alto Networks 建議您在維護時段或非尖峰時刻排程此變更。Palo Alto Networks 會在維護時段期間升級您部署中所有需要變更名稱的閘道。

# 設定 GlobalProtect 行動使用者

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

設定行動使用者之前，請確定您擁有所需的授權（行動使用者的 Prisma Access 授權，和有適當防火牆儲存空間的 Strata Logging Service 授權）。如果行動使用者要連線至其他連線網路，您將需要零信任網路存取 (ZTNA) 或 Enterprise Edition Prisma Access 授權，以提供連線所需的企業存取節點 (CAN)。

若要為行動使用者設定 Prisma Access，您將需要以下內容：

- 行動使用者的 Prisma Access 授權驗證是否已啟動行動使用者的 Prisma Access 授權。
- 行動使用者的 IP 位址集區：驗證您是否有一或多個非重疊 IP 位址集區可供行動使用者使用。
- 入口網站主機名稱：確保您知道入口網站的完全合格網域名稱 (FQDN)。
- 適用於行動使用者的 GlobalProtect 代理程式：適用於行動使用者的 Prisma Access，需要在每個支援的端點上有 GlobalProtect 應用程式。您需要一個部署策略，以便在行動使用者裝置上安裝 GlobalProtect 代理程式。
- 安全性政策規則資訊：您將會部署安全性政策規則，以允許或拒絕流量通過 Prisma Access。在為行動使用者設定 Prisma Access 時，您需要知道要部署哪些規則。
- 您行動使用者的地理位置：在佈建行動使用者時，您應該選取靠近行動使用者的可用地理位置。

瞭解如何將 GlobalProtect 行動使用者裝載至 Prisma Access。

- Strata Cloud Manager
- Panorama

 ©2025 Palo Alto Networks, Inc.

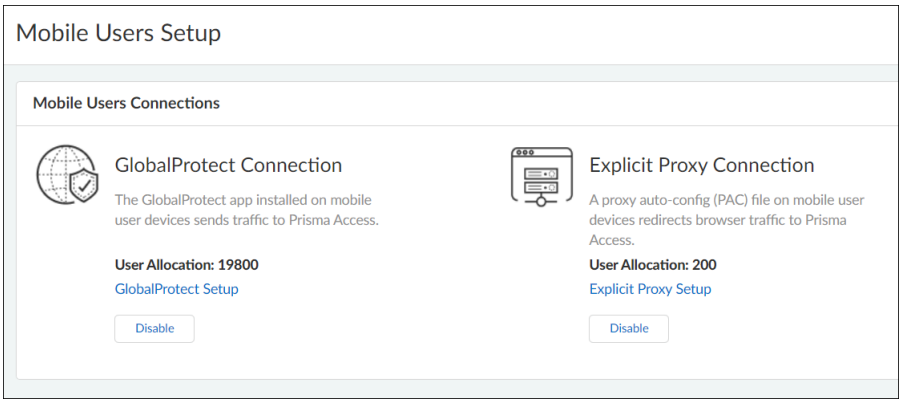
## 設定 GlobalProtect 行動使用者 (Strata Cloud Manager)

只需幾個步驟即可開始將 GlobalProtect 行動使用者裝載至 Prisma Access。

1. 啟用 **GlobalProtect** 作為行動使用者連線類型

   前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Mobile Users**（行動使用者）。

   您可以將行動使用者授權劃分為 GlobalProtect 和明明確 Proxy 連線；有些使用者可透過 GlobalProtect 連線，其他則透過明確 Proxy 連線。透過 **GlobalProtect** 連線，安裝在行動使用者裝置上的 GlobalProtect 應用程式會將流量傳送至 Prisma Access。

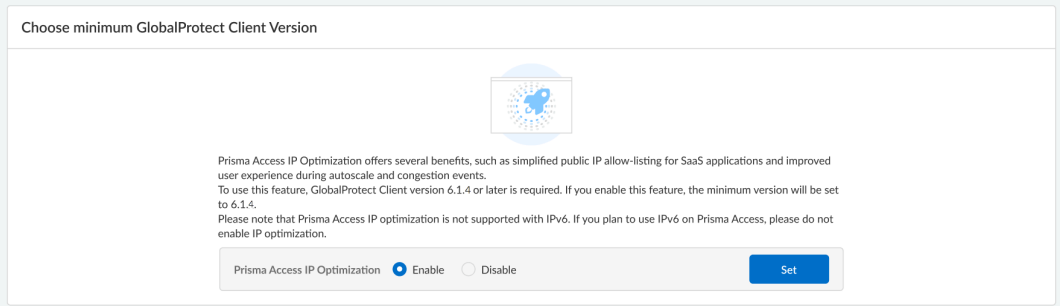



 ©2025 Palo Alto Networks, Inc.

2. 設定基本基礎結構設定

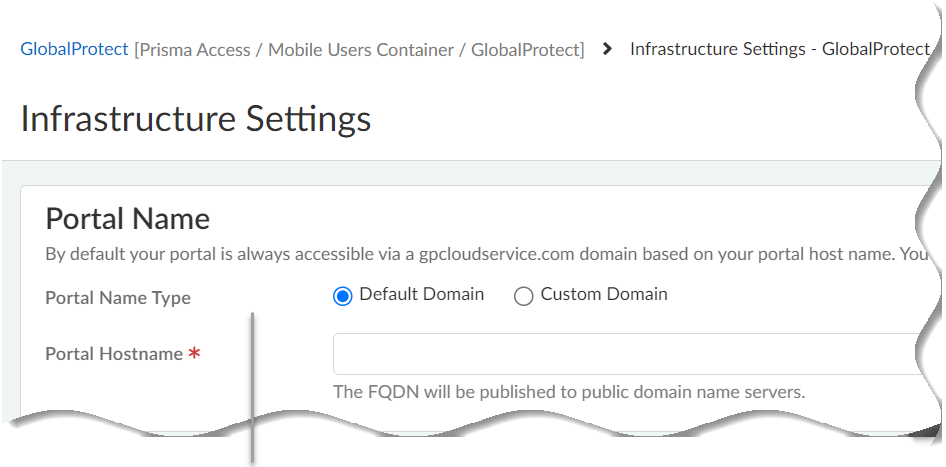
   設定 GlobalProtect 特定的基礎結構設定。您需要最初填寫一些必要設定，以便 Prisma Access 可以佈建您的行動使用者環境。

   - 當您首次設定 *GlobalProtect* 時，您將決定是否要啟用 *Prisma Access IP* 最佳化。選擇啟用 *IP* 最佳化需要 GlobalProtect 用戶端版本 *6.1.4* 及更新版本、*6.2.3* 及更新版本，或 *6.3.0* 及更新版本，並且不支援 *IPv6*。請仔細選擇，因為稍後無法變更此設定。
   - *IP* 最佳化功能僅適用於新的 *Prisma Access GlobalProtect* 部署。現有的 *GlobalProtect* 部署，包括您從現有的多租用戶部署中建立的新租用戶，不符合資格。
   - 如果您將 *GlobalProtect* 部署移轉到 *Prisma Access*（遠離使用內部部署閘道和入口網站），請確保所有使用者執行的 *GlobalProtect* 應用程式版本為 *6.1.4* 及更新版本、*6.2.3* 及更新版本，或 *6.3* 及更新版本，然後再啟用此功能。

   前往 **Workflows(工作流程)** > **Prisma Access Setup**（設定） > **GlobalProtect** > **Infrastructure**（基礎結構） > **Infrastructure Settings**（基礎結構設定）。

 ©2025 Palo Alto Networks, Inc.




**GlobalProtect Infrastructure Settings**

- 指定 **Portal Name**（入口網站名稱）。
  - **Default Domain**（預設網域）—如果選取此選項，則入口網站主機名稱會使用預設網域名稱：`.gpcloudservice.com`。在此情況下，只需輸入 **Portal Hostname**（入口網站主機名稱）以附加到預設網域名稱。Prisma Access for Users 將自動建立必要的憑證，並將主機名稱發佈到公用 DNS 伺服器。
  - **Custom Domain**（自訂網域）—如果您想要入口網站主機名稱中的網域符合貴公司網域名稱（例如，myportal.mydomain.com），您也可以自訂入口網站位址。
- 為您的 GlobalProtect 部署輸入 **Client DNS**（用戶端 **DNS**）解析設定。
  - 為 **DNS Servers**（**DNS** 伺服器）選取區域（**Add Region**（新增區域））。

    選取 **Worldwide**（全世界）或劇院。如果您指定多個 Proxy 設定，其中混合了全世界和劇院設定，則 Prisma Access 會先使用位置群組的設定，接著是劇院，然後全世界。Prisma Access 會在清單中從上到下評估規則。
  - 選擇是否想要 Prisma Access **Resolve internal domains**（解析內部網域）；如果您想要的話，請 **Add**（新增）一或多個 **Internal Domain Resolve Rules**（內部網域解析規則）。
  - 輸入規則的唯一 **Name**（名稱）。
  - 選取 **Prisma Access Default**（預設），以使用預設 Prisma Access DNS 伺服器來解析內部網域。如果您想要內部 DNS 伺服器僅解析您指定的網域，請在 **Domain List**（網域清


©2025 Palo Alto Networks, Inc.

單）中輸入要解析的網域。在網域前面指定一個星號；例如，*.acme.com。。您最多可以指定 1,024 個網域項目。

- 如果您有 **Custom**（自訂）DNS 伺服器可存取您的內部網域，請指定 **Primary DNS**（主要 **DNS**）和 **Secondary DNS**（次要 **DNS**）伺服器 IP 位址。
- 如果您想要內部 DNS 伺服器僅解析您指定的網域，請在 **Domain Lists**（網域清單）中輸入要解析的網域。在網域前面指定一個星號；例如，*.acme.com。。您最多可以指定 1,024 個網域項目。
- 完成時 **Save**（儲存）您的變更。

- （選用）指定 **Client IP Pool**（用戶端 **IP** 集區）。

  根據預設，Prisma Access 為您提供 100.127.0.0/16 的預設行動使用者 IP 位址集區，可以在全球任何位置使用。Prisma Access 將來自此集區的 IP 位址指派給每個連線 GlobalProtect 的裝置。您可以選擇性地在這裡根據每個區域新增 IP 位址集區。

  - 為每個位置輸入所需的最小子網路 /23（512 個 IP 位址）。其他位置至少需要 /23 子網路。如果您指定全球子網路，則所需的子網路最低為 /23，但我們建議 用於 GlobalProtect 行動使用者部署的 IP 位址集區 配置一組等於或大於授權行動使用者數目的 IP 位址，讓行動使用者可以同時登入。

    請勿指定與您內部使用的其他網路重疊的位址，也不要指定與您 設定 Prisma Access 服務基礎結構 (Panorama) 時指派的集區重疊的位址。此外，請勿使用以下 IP 位址和子網路，因為 Prisma Access 會保留這些 IP 位址和子網路供內部使用：

    - 169.254.0.0/16
    - 100.64.0.0/10

    建議使用符合 *RFC 1918* 和 *RFC 6598* 規範的 *IP* 位址集區。雖然支援針對行動使用者使用不符合 *RFC 1918*（公用）規範的 *IP* 位址，但不建議使用這些位址，因為可能與網際網路公用 *IP* 位址空間發生衝突。

- 指定 **Primary DNS for public domains**（公用網域的主要 **DNS**）和 **Secondary DNS for public domains**（公用網域的次要 **DNS**）的 DNS 設定。
  - **Prisma Access Default**（預設）—使用預設 Prisma Access DNS 伺服器。
  - **Internal DNS**（內部 **DNS**）—使用您用於解析內部網域的相同伺服器。
  - **Custom**（自訂）—如果您有可存取公用（外部）網域的 DNS 伺服器，請在該欄位中輸入主要 DNS 伺服器位址。
  - 您可以新增 **Client DNS Suffix List**（用戶端 **DNS** 尾碼清單），指定 輸入無法解析的不完整主機名稱時，用戶端應在本機使用的尾碼，例如，acme.local。請勿在網域尾碼前面輸入萬用字元 (*)（例如，acme.com）。您可以新增多個尾碼。

3. 設定 **Advanced Settings**（進階設定）。

- （選用）使用 **Static Entries**（靜態項目）將 FQDN 解析為特定 IP 位址。

  如果您的組織中有來賓網際網路服務，並且您想要來賓安全地使用搜尋引擎，防止他們搜索可能違反公司政策的可能不適當或冒犯性資料，則此功能可能非常有用。若要這樣做，請為

 ©2025 Palo Alto Networks, Inc.

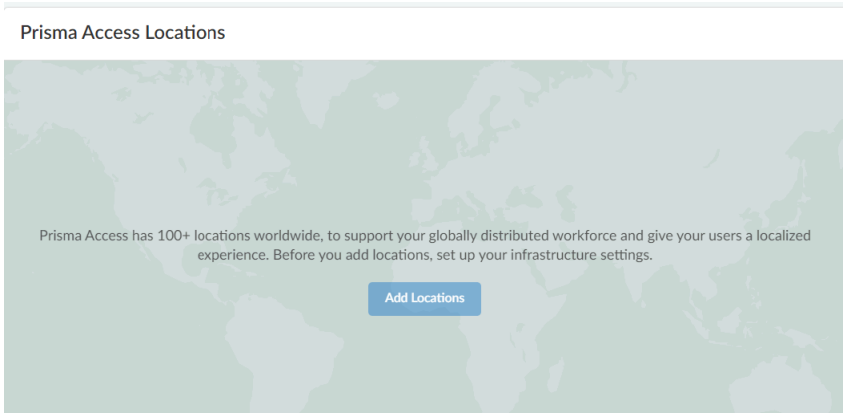
靜態項目規則輸入唯一的 **Name**（名稱），並輸入 **FQDN** 和應該在其中導向 FQDN 要求的 IP **Address**（位址）。




- 如果想要 Prisma Access 對 DNS 要求進行 Proxy，請設定 **UDP Queries Retries**（**UDP** 查詢重試）的值（以秒為單位重試查詢的 **Interval (Sec)**（間隔（秒））），以及重試 **Attempts**（嘗試）的執行次數）。

4. 選擇您的 **GlobalProtect** 使用者將連線至其中的 **Prisma Access** 位置

   新增您想要支援 GlobalProtect 使用者的 Prisma Access 位置。前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **GlobalProtect** > **Infrastructure**（基礎結構） > **Prisma Access Locations**（位置）。




   地圖會顯示您可以為使用者部署 Prisma Access 的全球區域。此外，Prisma Access 在每個區域內提供多個位置，以確保您的使用者可以連線至依據其區域設定提供客製化使用者體驗的位置。為了獲得最佳效能，請 **Select All**（全選）。或者，在每個選定的區域內選取您的使用者需要存取的特定位置。將部署限定於單一區域，可以對您部署的區域進行更精細的控制，並排除政策或產業法規要求的區域。

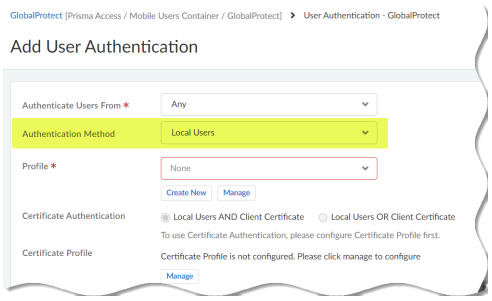
   為了獲得最佳使用者體驗，如果您限制了位置數目，請選擇離使用者最近的位置，或位於使用者相同國家/地區的位置。如果您行動使用者所在的國家/地區沒有可用位置，請選擇離使用者最近的位置，以獲得最佳效能。


©2025 Palo Alto Networks, Inc.

5. 驗證 **GlobalProtect** 使用者

   設定使用者驗證，僅允許合法使用者存取您的服務和應用程式。前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **GlobalProtect** > **Infrastructure**（基礎結構） > **User Authentication**（使用者驗證位置）。

   若要測試您的設定，您可以新增 Prisma Access 在本機驗證的使用者，或者，您可以直接設定企業層級的驗證。進一步瞭解如何 啟用行動使用者對 Prisma Access 進行驗證。




6. Prisma Access 預設強制執行最佳做法安全性政策規則。這些規則允許您的使用者安全地瀏覽至一般的網際網路網站。使用者：

   - 已被封鎖根據 URL 造訪已知的不良網站
   - 已被封鎖上傳或下載已知為惡意的檔案
   - 受到保護免於未知、從未見過的威脅
   - 受到保護免於惡意軟體、間諜軟體（命令和控制攻擊）及漏洞

   完成初始設定後，您可以檢閱並更新這些預設規則，以符合您的企業需求。

7. 驗證行動使用者的位置是否作用中

   將您的初始設定推送至 Prisma Access 後，Prisma Access 就會開始佈建您的 GlobalProtect 行動使用者環境。這最多可能需要 15 分鐘。

   您還可以選取 ***Workflows***（工作流程） > ***Prisma Access Setup***（設定） > ***Prisma Access*** > ***Infrastructure Settings***（基礎結構設定）來驗證您的設定，然後編輯基礎結構設定，以確認閘道設定在您所佈建的每個位置中。

**GlobalProtect**—自訂入口網站位址

Prisma Access 只需要最少的設定，即可佈建行動使用者的環境，以便您可以對其進行測試。如果您想要在入口網站位址中使用您的公司網域，則可以在初始環境設定之後變更該地位址。

根據預設，Prisma Access 會使用 *gpcloudservice.com* 網域，來設定行動使用者需要連線至其中的 Prisma Access 入口網站位址，以安全地存取網際網路以及總部和資料中心。您必須在初始設定和測試環境時使用此預設網域。如果您想要在初始設定之後自訂網域名稱以使用您的公司網域，您可以返回並編輯環境設定，以便您使用者連線至其中的入口網站位址包含您自己的公司網域（例如，prisma-access.acme.com）。

*.gpcloudservice.com 網域與 *Palo Alto Networks* 應用程式相關聯。

若要設定 Prisma Access 以使用您自己的網域，您必須：

 ©2025 Palo Alto Networks, Inc.

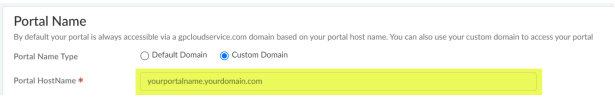
- 取得服務的憑證。
- 在您的 DNS 伺服器上建立 DNS CNAME 項目，其會使用預設網域將預設入口網站位址對應至使用您公司網域的自訂入口網站位址。您需要這樣做，因為在初始佈建期間 Prisma Access 會將您設定的入口網站位址發佈到公用網域伺服器。

**STEP 1 |** 選取 **Workflows(工作流程) > Prisma Access Setup**（設定） **> GlobalProtect > Infrastructure**（基礎結構），並編輯 **Infrastructure Settings**（基礎結構設定）。

在 *Strata Cloud Manager* 中，預設會在入口網站或閘道與服務連線之間啟用網路備援，確保行動使用者對可存取服務和應用程式的備援連線。

**STEP 2 |** 將入口網站名稱類型設定為 **Custom Domain**（自訂網域）。

**STEP 3 |** 輸入您要使用的 **Portal Hostname**（入口網站主機名稱）。




**STEP 4 |** 新增要對應 DNS 伺服器項目的 **Portal DNS CNAME**（入口網站 **DNS CNAME**）。

**STEP 5 |** **Import**（匯入）您針對自訂網域入口網站位址佈建的 **Certificate**（憑證）。

1. 為要匯入的憑證選取憑證 **Format**（格式）：
   - **Encrypted Private Key and Certificate (PKCS12)**（加密的私密金鑰與憑證 **(PKCS12)**）—金鑰與憑證位於單一容器（憑證檔案）內。按一下 **Choose File**（選擇檔案），然後瀏覽至要匯入的 PKCS12 檔案。
   - **Base64 Encoded Certificate (PEM)**（**Base64** 編碼憑證 **(PEM)**）—如果選取此選項，您必須將 **Key File**（金鑰檔案）與憑證分開匯入。若要匯入 PEM 憑證和金鑰檔案，請按一下 **Choose File**（選擇檔案）。
2. 輸入 **Passphrase**（複雜密碼）來加密金鑰並 **Confirm Passphrase**（確認複雜密碼），然後按一下 **Save**（儲存）。

**STEP 6 |** 如果您尚未這樣做，請將 DNS 伺服器設定為指向您定義的 Prisma Access DNS CNAME。

**STEP 7 |** **Save**（儲存）環境設定，並**Push Config**（推送設定）至 Prisma Access。

務必同時選取 **Explicit Proxy**（明確 **Proxy**）和 **GlobalProtect** 設定範圍。

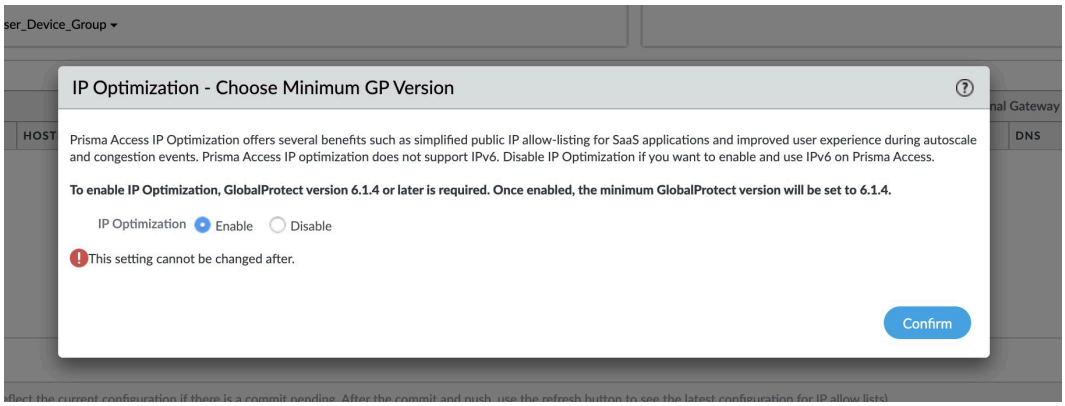
## 設定 GlobalProtect 行動使用者 (Panorama)

若要設定行動使用者—GlobalProtect 部署，請完成下列步驟。開始之前，請確保您瞭解 Prisma Access 的運作方式，並使用檢查清單，為您的 GlobalProtect 部署做好規劃。


©2025 Palo Alto Networks, Inc.

**STEP 1 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users**—**GlobalProtect**（行動使用者—**GlobalProtect**）。

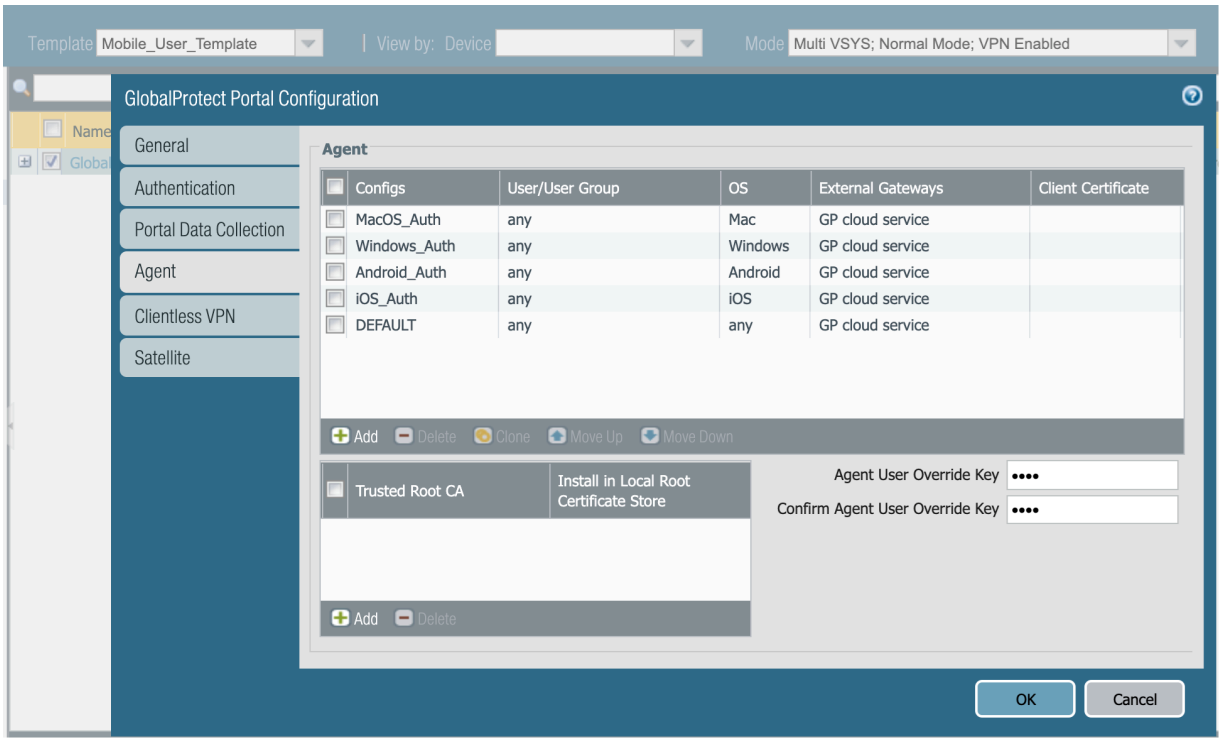
- 當您首次設定 *GlobalProtect* 時，系統會詢問您是否要啟用 *Prisma Access IP* 最佳化。選擇啟用 *IP* 最佳化需要 GlobalProtect 用戶端版本 *6.1.4* 及更新版本、*6.2.3* 及更新版本，或 *6.3.0* 及更新版本，並且不支援 *IPv6*。請仔細選擇，因為稍後無法變更此設定。
- *IP* 最佳化功能僅適用於新的 *Prisma Access GlobalProtect* 部署。現有的 *GlobalProtect* 部署，包括您從現有的多租用戶部署中建立的新租用戶，不符合資格。
- 如果您將 *GlobalProtect* 部署移轉到 *Prisma Access*（遠離使用內部部署閘道和入口網站），請確保所有使用者執行的 *GlobalProtect* 應用程式版本為 *6.1.4* 及更新版本、*6.2.3* 及更新版本，或 *6.3* 及更新版本，然後再啟用此功能




**STEP 2 |** （選用）如果您想要自訂 Prisma Access 推送至用戶端的代理程式設定，請編輯 Mobile_User_Template 中的 GlobalProtect 入口網站設定，以新增代理程式設定。在設定代

 ©2025 Palo Alto Networks, Inc.

理程式設定之後，將其移至範本中預先定義的 DEFAULT 代理程式設定之上，以確保您的設定優先於預設設定。編輯此範本時，請勿刪除或變更外部閘道項目。

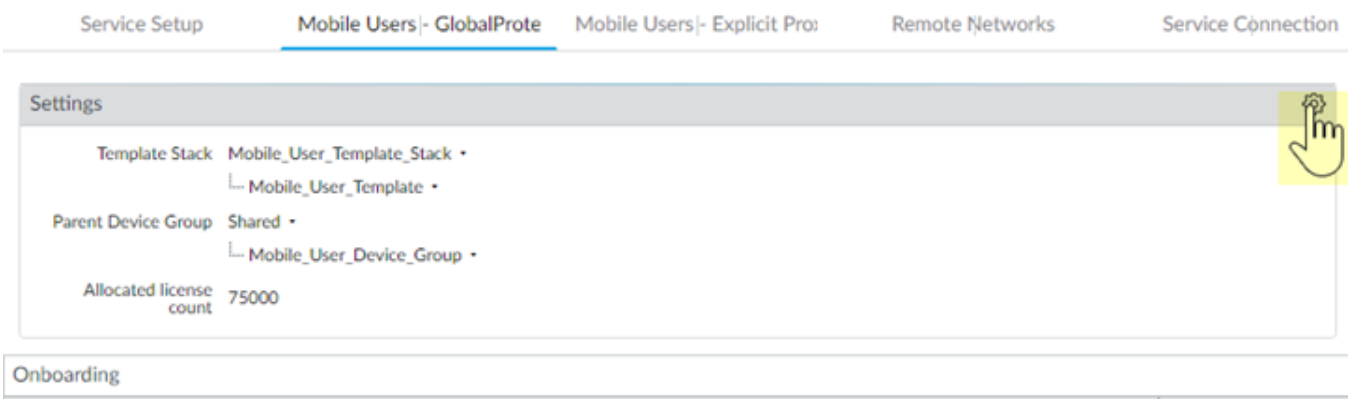




©2025 Palo Alto Networks, Inc.

**STEP 3 |** 設定雲端服務將推送到入口網站和閘道的裝置群組階層。

1. 編輯 **Settings**（設定）。



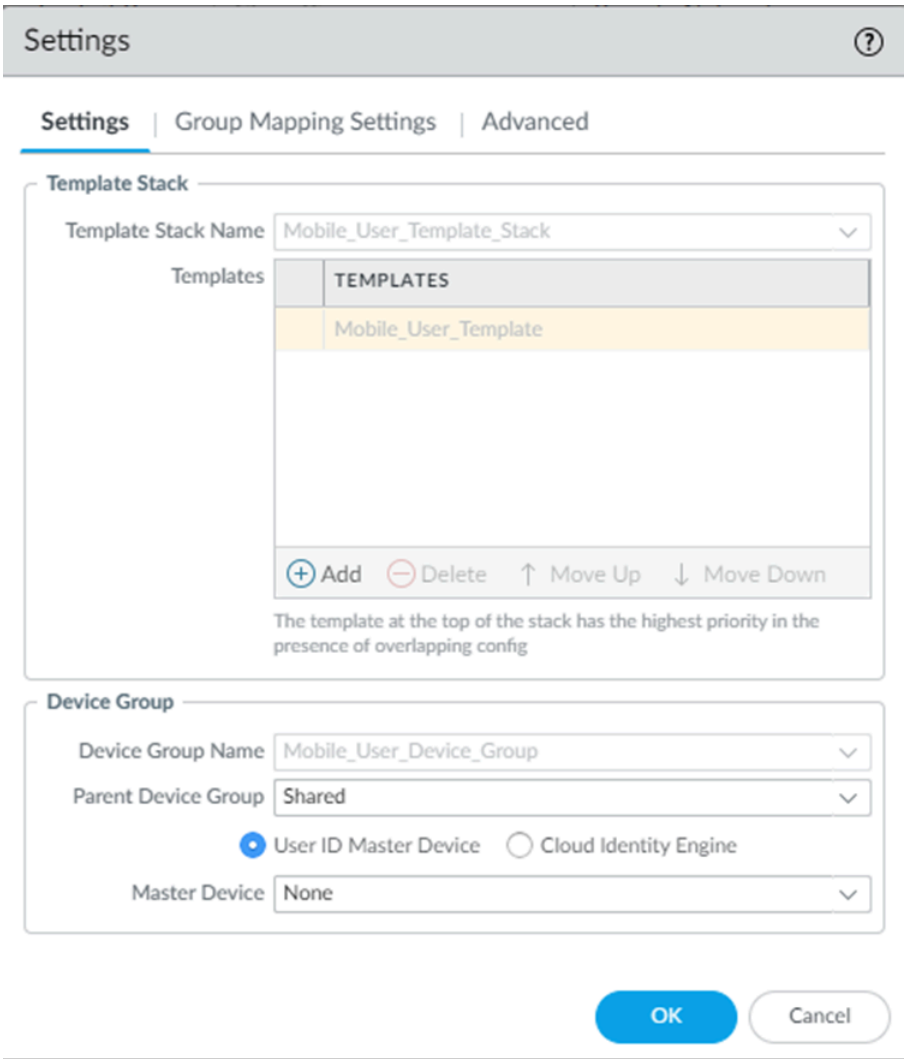

2. 在 [Device Group（裝置群組）] 區段中，選取 **Parent Device Group**（父系裝置群組），其中包含您想要推送至 Prisma Access for Users 的設定，或者將父系裝置群組保留為 **Shared**（共用），以使用 Prisma Access 裝置群組共用階層。

   您將推送所有設定—包括位址群組、安全性政策、安全性設定檔和其他政策物件（例如應用程式群組和物件）、HIP 物件和設定檔，以及驗證政策—Prisma Access for Users 需要使用您在這裡指定的 device group hierarchy（裝置群組階層），對行動使用者強制執行一致的政策。此外，您必須確保已設定日誌轉送設定檔，將所需的日誌類型轉送至裝置群組中的 **Panorama/Strata** 記錄服務，而此裝置群組推送至 Prisma Access for Users；這是雲端服務知道哪些日誌要轉送至 Strata Logging Service 的唯一方法。

3. （選用）如果您已將新世代防火牆設定為主要裝置，或已新增雲端識別引擎設定檔，讓使用者和群組資訊可在安全性政策中選取，請選取 **User-ID Master Device**（**User-ID** 主要

 ©2025 Palo Alto Networks, Inc.

裝置）或 **Cloud Identity Engine**（雲端識別引擎）；然後，選取您建立的主要裝置或雲端識別引擎設定檔。




**STEP 4 |** （選用）設定 Prisma Access 以使用雲端識別引擎的目錄同步元件，來擷取使用者和群組資訊。

在 Prisma Access **Group Mapping Settings**（群組對應設定）中啟用和設定目錄同步整合之前，您必須設定雲端識別引擎的目錄同步元件，以從雲端目錄或 Active Directory (AD) 擷取使用者和群組資訊。

**STEP 5 |** 按一下 **OK**（確定）以儲存行動使用者設定。

**STEP 6 |** 將範本堆疊內設定的區域對應為受信任的或不受信任的。

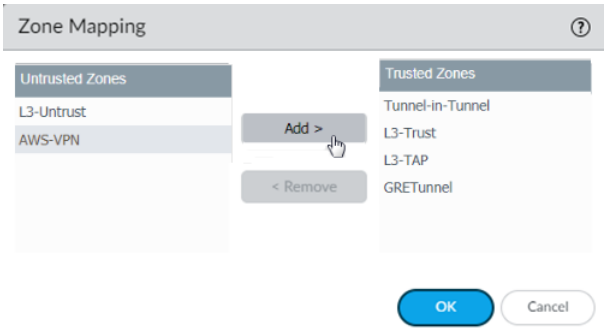
在 Palo Alto Networks 新世代防火牆上，安全性政策是在區域之間強制執行，這些區域對應到防火牆上的實體或虛擬介面。不過，使用 Prisma Access for Users，網路基礎結構會自動為您設定，這意味著您不再需要設定介面，並將其與區域建立關聯。不過，若要啟用一致的安全


©2025 Palo Alto Networks, Inc.

性政策強制執行，您必須將組織內使用的區域對應為信任或不信任，以便 Prisma Access for Users 可以將您推送到雲端服務的政策規則轉譯為網路基礎結構內的內部區域。

1. 編輯區域對應設定。

   根據預設，Mobile_User_Template_Stack 中的所有區域都會分類為不受信任的區域。
2. 對於要指定為受信任的每個區域，請選取它並按一下 **Add**（新增），以將其移至 **Trusted Zones**（受信任區域）的清單。




3. 按一下 **OK**（確定）儲存您的變更。

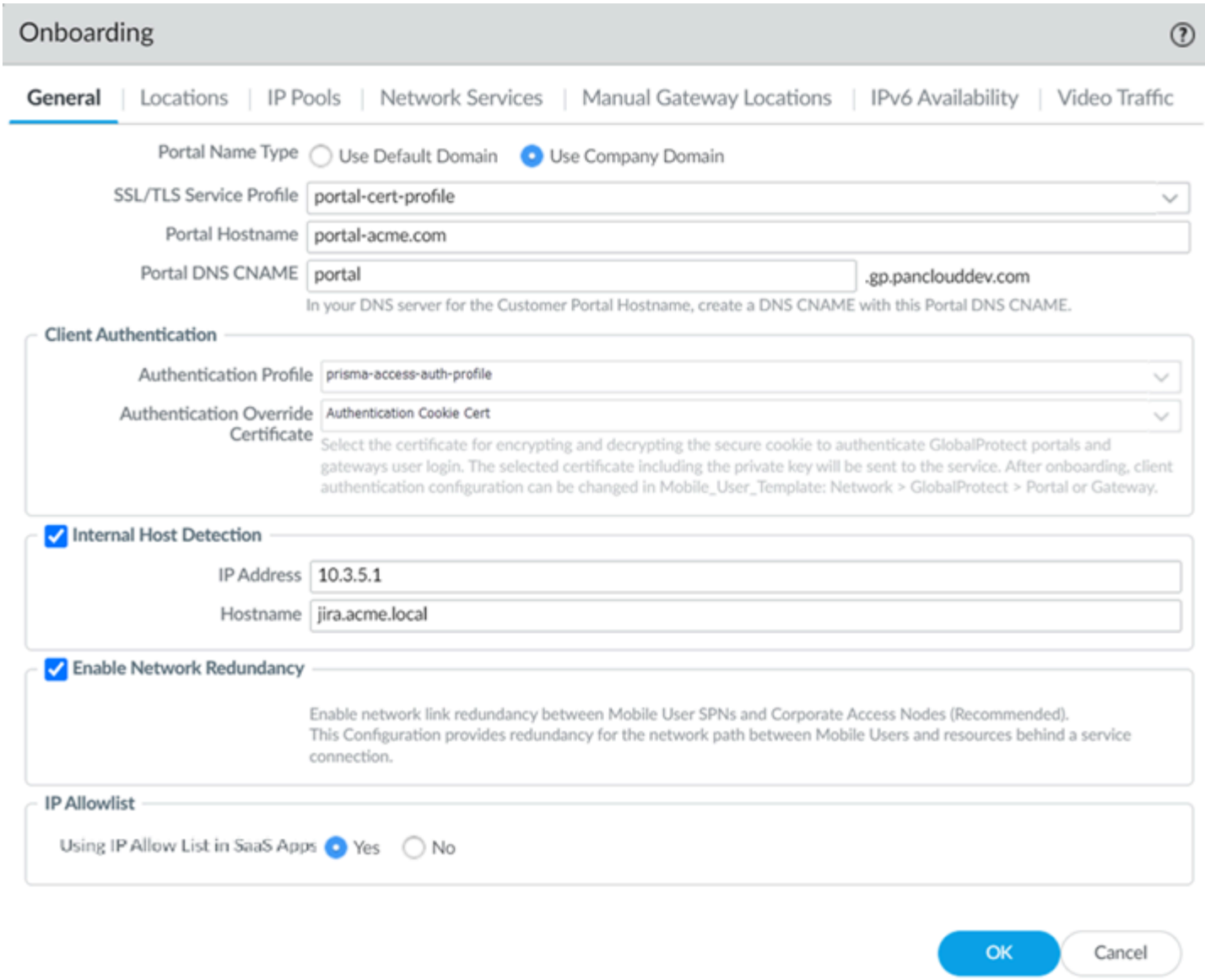
**STEP 7 |** 設定 GlobalProtect 入口網站和外部閘道設定。

您可以設定 Prisma Access 閘道僅作為外部閘道，而不作為內部閘道。

1. 在裝載區域中，按一下 **Configure**（設定）。
2. 在 **General**（一般）頁籤上，指定 **Portal Name Type**（入口網站名稱類型）：
   - **Default Domain**（預設網域）—如果選取此選項，則入口網站主機名稱會使用預設網域名稱：`.gpcloudservice.com`。在此情況下，只需輸入 **Portal Hostname**（入口

 ©2025 Palo Alto Networks, Inc.

網站主機名稱）以附加到預設網域名稱。Prisma Access for Users 將自動建立必要的憑證，並將主機名稱發佈到公用 DNS 伺服器。




如果您已有 GlobalProtect 部署具有現有的入口網站名稱，並且想要繼續使用該入口網站名稱，請新增一個 CNAME 項目，將 Prisma Access 入口網站名稱對應至您現有的入口網站名稱。例如，如果您有一個名為 portal.acme.com 的現有入口網站，並且想要將新的 Prisma Access 入口網站對應至這個相同名稱，您可以將 gpcs2.gpcloudservice.com 的 CNAME 新增到現有入口網站的 DNS 項目。

*.gpcloudservice.com 網域與 *Palo Alto Networks* 應用程式相關聯。

- **Use Company Domain**（使用公司網域）—如果您想要入口網站主機名稱中的網域符合貴公司網域名稱（例如，myportal.mydomain.com），請選取此選項。如果想要使用此選項，您必須首先取得自己的憑證，並設定指向該憑證的 SSL/TLS 服務設定檔。然後，您可以選取 **SSL/TLS Service Profile**（**SSL/TLS** 服務設定檔），並輸入 **Portal**

 ©2025 Palo Alto Networks, Inc.

**Hostname**（入口網站主機名稱）來設定入口網站名稱。如果使用此選項，則您必須將內部 DNS 伺服器指向 **Portal DNS CNAME**（入口網站 **DNS CName**），它是具有 `.gpcloudservice.com` 網域的入口網站的主機名稱。例如，如果您指定了 acme-portal.acme.com 的 DNS 主機名稱，則需要建立一個 DNS CNAME 項目，將該主機名稱對應到內部 DNS 伺服器上的 acme-portal.gpcloudservice.com。



如果需要上傳新憑證，請匯入憑證和金鑰；然後，在 ***Network***（網路）**>** ***GlobalProtect*** **>** ***Portals***（入口網站）**>** ***GlobalProtect_Portal*** **>** ***Authentication***（驗證）下檢視 *Prisma Access* 正在使用的 *SSL/TLS* 服務，並檢查 ***SSL/TLS Service Profile***（***SSL/TLS*** 服務設定檔**)**名稱。僅在您使用公司網域而不是預設網域時，此欄位才會顯示。然後，您可以選取 ***Device***（裝置）**>** ***Certificate Management***（憑證管理）**>** ***SSL/TLS Certificate Profile***（***SSL/TLS*** 憑證設定檔），並將入口網站使用的 *SSL/TLS* 設定檔中的憑證取代為您匯入的憑證。

3. 選取一個 **Authentication Profile**（驗證設定檔**)**，指定 Prisma Access 應如何驗證行動使用者，或建立新的驗證設定檔。

   如果您新增了包含驗證設定檔設定的父系裝置群組，則應該會在可用設定檔的清單中看到它。如果您未推送裝置群組中的設定檔，現在可以建立驗證設定檔。

   在提交並推送您的變更之後，您無法對此區域中的驗證設定檔和驗證覆寫憑證進行任何變更，並且選項會變成唯讀。若要在初始裝載之後進行變更，請在 ***Mobile_User_Template*** 下修改或新增一個或多個 *GlobalProtect* 用戶端驗證設定。

4. 選取 **Authentication Override Certificate**（驗證覆寫憑證），以加密行動使用者向入口網站和閘道進行驗證的安全性 Cookie。

   如果您新增的父系裝置群組包含要用來加密驗證 Cookie 的憑證，您應該會在可用憑證的清單中看到它。如果您未推送裝置群組中的憑證，現在可以匯入或產生一個。

5. （選用）若要確保您的行動使用者始終有權存取可從服務連線存取的服務和應用程式，請在入口網站或閘道與服務連線之間 **Enable Network Redundancy**（啟用網路備援**)**。

   此功能會在行動使用者資料資料平面與不同計算位置中服務連線之間提供備援網路路徑。啟用備援可讓使用者更靈活地存取資料中心或總部位置中服務連線後面的資源。因為行動

 ©2025 Palo Alto Networks, Inc.

使用者需要服務連線，才能從遠端網路存取資源，所以使用者在存取遠端網路位置中的資源時也具有更大的彈性。

6. （選用）如果您不需要 GlobalProtect 端點在位於內部網路上時具有通道連線，請啟用 **Internal Host Detection**（內部主機偵測）。
   1. 選取 **Internal Host Detection**（內部主機偵測）核取方塊。
   2. 輸入使用者只能從內部網路連線之主機的 **IP Address**（IP 位址）。
   3. 為您輸入 IP 位址輸入 DNS **Hostname**（主機名稱）。嘗試連線的用戶端會對指定位址執行反向 DNS 查閱。如果查閱失敗，則用戶端確定其需要與 Prisma Access for Users 的通道連線。

   *Prisma Access* 會將您在這裡指定的內部主機偵測設定複製到 GlobalProtect 入口網站設定 中的預設代理程式設定（***Network***（網路） > ***GlobalProtect*** > ***Portals***（入口網站） > ***<portal-config>*** > ***Agent***（代理程式） > ***DEFAULT***（預設） > ***Internal***（內部））。如果您已在 *GlobalProtect* 入口網站中輸入預設代理程式的內部主機偵測設定，則將無法在這裡變更選項，而且必須在入口網站中變更它。如果您需要多個代理程式設定，請在 *GlobalProtect* 入口網站中輸入預設代理程式設定的設定，並將這些設定用於 *Prisma Access*，然後選取 ***Network***（網路） > ***GlobalProtect*** > ***Portals***（入口網站） > ***<Portal-config>*** > ***Agent***（代理程式），然後 ***Add***（新增）非預設設定，並在部署的其他部分中指定該設定。
7. （選用）如果您的組織使用允許清單來控制對公用或 SaaS 應用程式的存取，請指定您是否 **Using IP Allow Lists in SaaS Apps**（在 **SaaS** 應用程式中使用 **IP** 允許清單）。

   若要讓您可為 GlobalProtect 新增公用（輸出）IP 位址—行動使用者部署到您在組織內使用的任何 SaaS 應用程式允許清單，Prisma Access 會提供 IP 位址，並讓您在環境中使用它們之前，驗證是否已將它們新增至允許清單。對於現有部署和新部署，您可以實作 Prisma Access 輸出 IP 位址的允許清單。
8. （選用）自訂 GlobalProtect 應用程式設定（例如，設定 GlobalProtect 使用的連線方法），方法是選取 **Network**（網路） > **GlobalProtect** > **Portals**（入口網站） > **GlobalProtect_Portal** > **Agent**（代理程式）、選取您要自訂的設定，或選取 **DEFAULT**（預設）、選取 **App**（應用程式），然後自訂 GlobalProtect 應用程式。

**STEP 8 |** 選取 **Locations**（位置），以及與您要部署行動使用者的這些位置相關聯的區域。

**Locations**（位置）頁籤顯示一張地圖。反白顯示地圖會顯示全球區域（美洲、歐洲和亞太地區）以及每個區域內可用的位置。選取一個區域，然後選取您想要在每個區域中部署的位置。限制您部署至單一區域提供對已部署區域的更細緻控制，並允許您依據政策或行業法規排除區

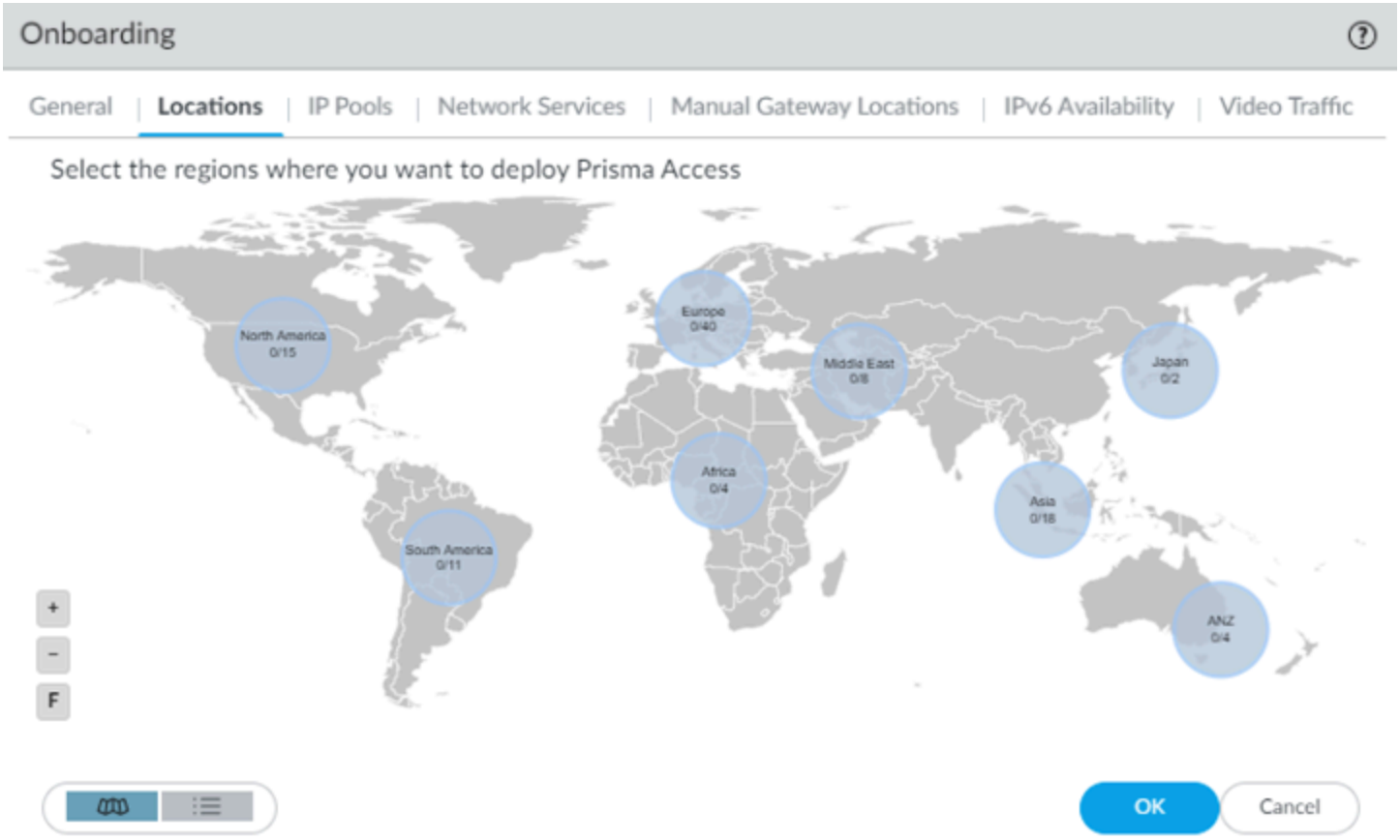
 ©2025 Palo Alto Networks, Inc.

域。您可以選取區域中距離行動使用者最近的位置，也可以根據您的政策或行業法規視需要選取位置。

如果其他位置不可用，則 *Prisma Access* 會使用香港、荷蘭中部和美國西北部位置作為回復行動使用者位置。基於此原因，*Palo Alto Networks* 強烈建議您在行動使用者裝載期間至少啟用其中一個位置。

以兩個星號表示的位置為 **Local Zones**（本機區域）。這些位置會將計算、儲存、資料庫和基礎結構服務放置在大型人口和產業中心附近；不過，它們也有一些限制。若要新增本機區域，請聯繫您的 Palo Alto Networks 代表。

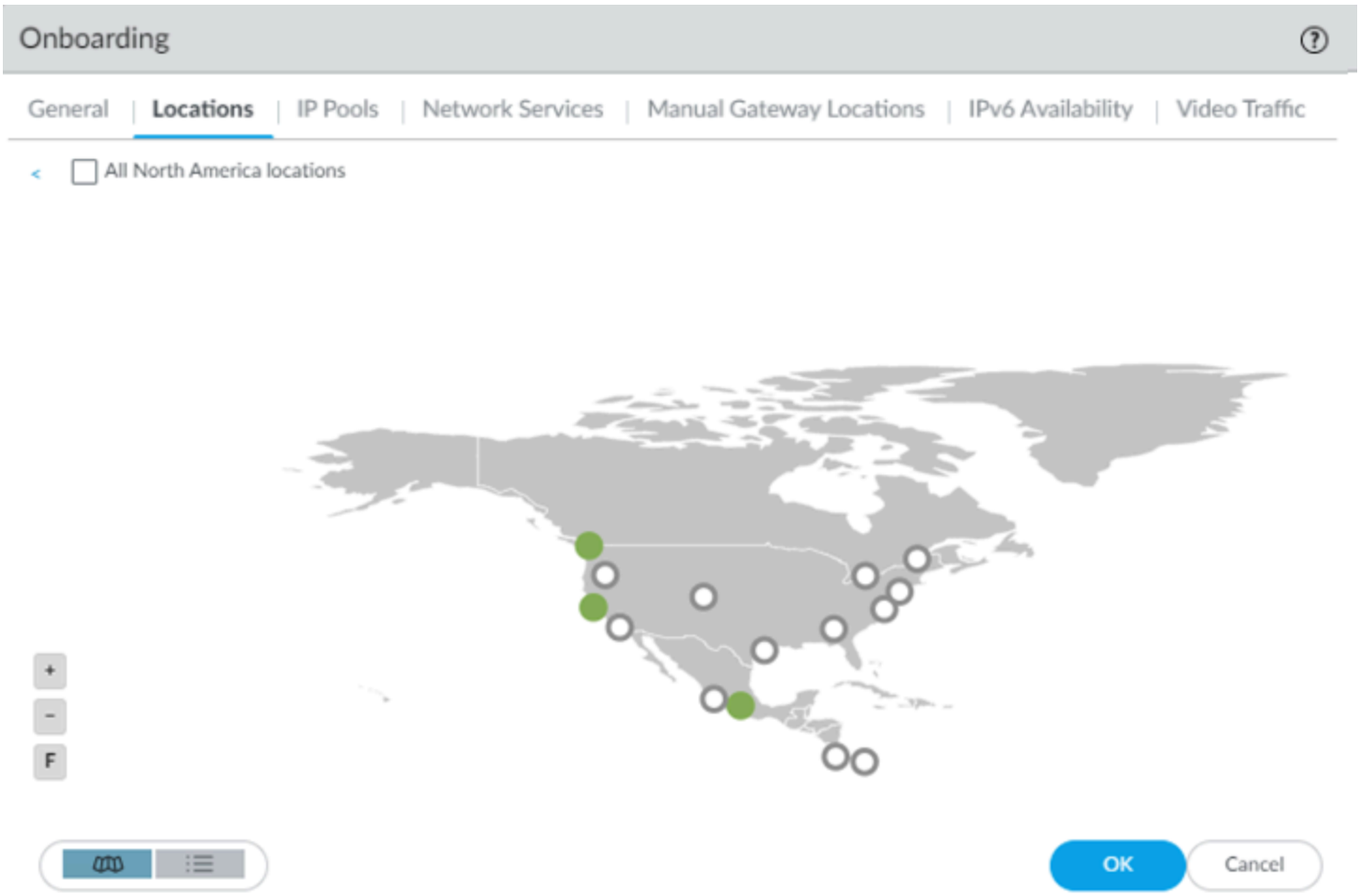
1. 按一下 **Locations**（位置）頁籤並選取一個區域。




2. 使用地圖在您選取的區域內選取一或多個 Prisma Access 閘道。

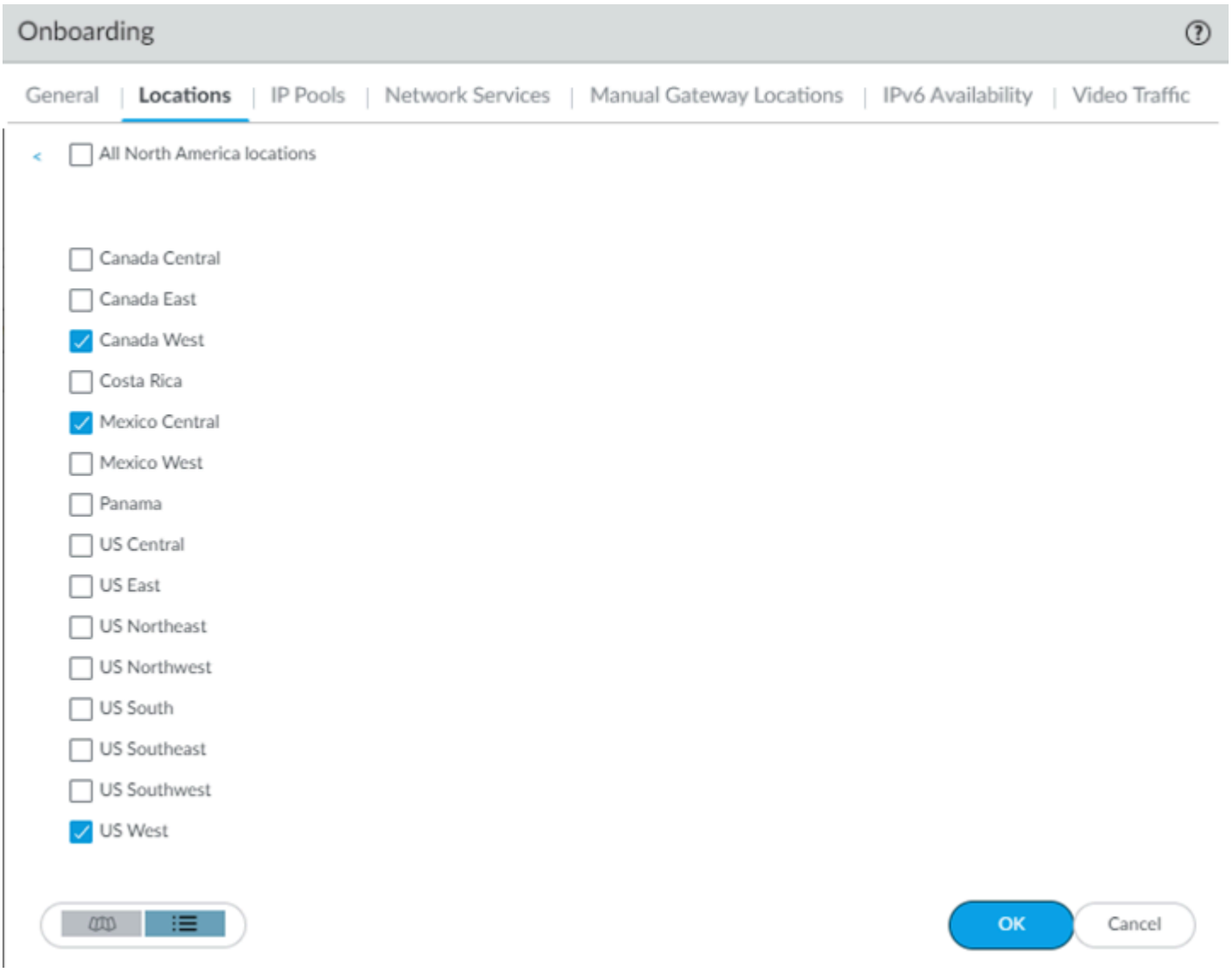
   將游標暫留在某個位置上，即會反白顯示該位置。白色圓圈表示可用位置；綠色圓圈表示您已選取該位置。

 ©2025 Palo Alto Networks, Inc.




除了地圖檢視外，您還可以檢視區域和位置的清單。從左下角在地圖檢視和清單檢視之間進行選擇。在清單檢視中，清單顯示依欄排序的區域，而所有位置都是依區域排序。您可以選取一個區域內的 **All**（所有）網站（對話方塊頂部）。


©2025 Palo Alto Networks, Inc.




**STEP 9 |** 選取 **IP Pools**（**IP** 集區）頁籤，來設定用來將 IP 位址指派給 GlobalProtect 端點的 IP 位址，並 **Add**（新增）IP 位址集區。

1. 為 IP 位址集區指定一個 **Region**（區域）。

   您可以為全球（**Worldwide**（全世界））的所有 GlobalProtect 端點使用單一 IP 位址集區，可以為擁有行動使用者的每個劇院使用個別集區，也可以為每個位置群組（小於劇院的位置群組）指定集區。您也可以指定全世界、每個劇院或每個位置群組 IP 集區的組合。例如，您可以為特定位置群組新增一個集區，然後新增一個 **Worldwide**（全世界）集區以用於所有其他位置。

   如果您有服務依賴使用者的來源 IP 位址來識別使用者的詳細資訊（例如位置型服務或基於使用者群組或功能的服務），請使用位置群組特定的 IP 位址集區，以便您可以套用存取控制政策，或在不同國家/地區執行路由或政策操作（如果這些國家/地區位於不同的計

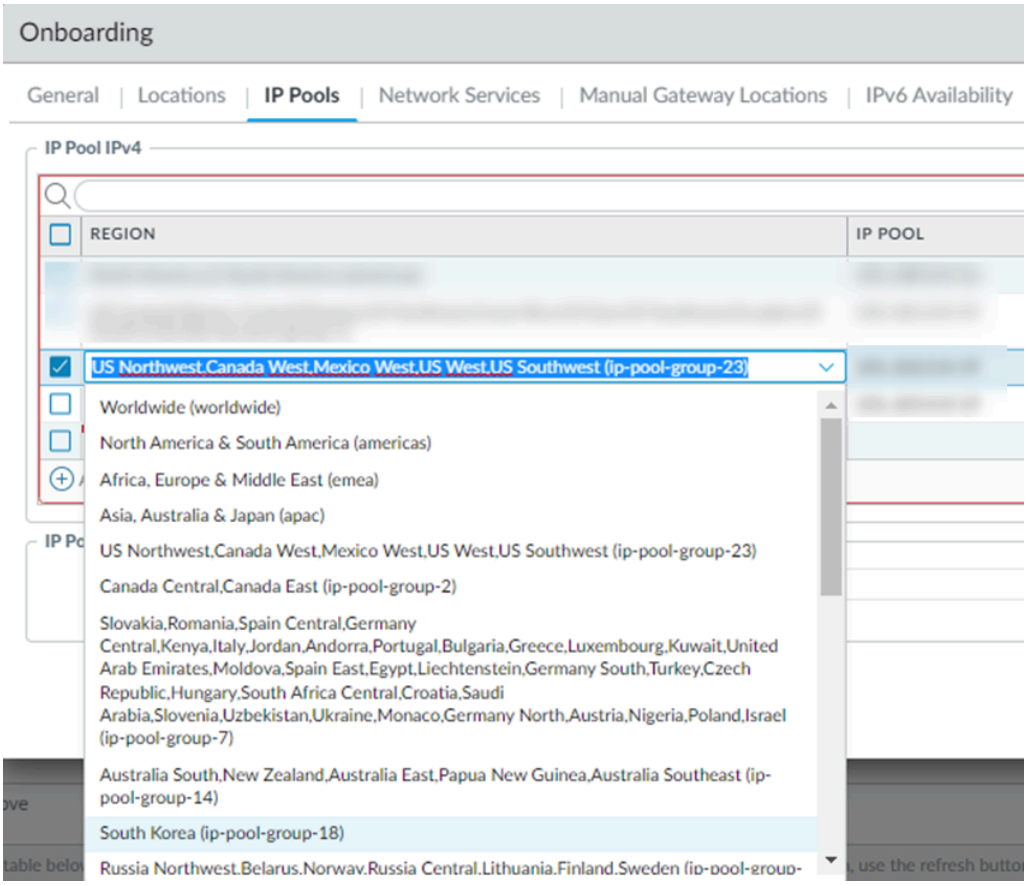
 ©2025 Palo Alto Networks, Inc.

算區域）。例如，您可以針對加拿大使用個別 IP 位址集區，針對巴西使用另一個 IP 位址集區，它們位於不同計算位置，以提供不同的存取和安全性控制。

若要使用位置群組特定 *IP* 位址集區，您也必須指定「全世界」或劇院特定 *IP* 位址集區。

GlobalProtect 行動使用者首先耗用位置群組中的 IP 位址，然後使用劇院特定的 IP 位址，最後使用全球 IP 位址。例如，如果您為位置群組和全世界指定一個集區，然後用盡位置群組集區中的可用 IP 位址，則 Prisma Access 將從 **Worldwide**（全球）集區取得 IP 位址以在該位置群組中使用。

- 若要指定所有 GlobalProtect 行動使用者可以使用的 IP 集區，請選取 **Worldwide**（全世界）。
- 若要指定特定劇院中 GlobalProtect 使用者可以使用的 IP 集區，請選取劇院。
- 若要指定位置群組特定的 IP 集區，請從清單中選取該位置群組。




2. 輸入在您選取的區域中要指派給端點的 **IP Pool**（**IP** 集區）。
   - 為每個位置輸入所需的最小子網路 /23（512 個 IP 位址）。其他位置至少需要 /23 子網路。如果您指定全球子網路，則所需的子網路最低為 /23，但我們建議 用於

 ©2025 Palo Alto Networks, Inc.

GlobalProtect 行動使用者部署的 IP 位址集區 配置一組等於或大於授權行動使用者數目的 IP 位址，讓行動使用者可以同時登入。

請勿指定與您內部使用的其他網路重疊的位址，也不要指定與您 設定 Prisma Access 服務基礎結構 (Panorama) 時指派的集區重疊的位址。此外，請勿使用以下 IP 位址和子網路，因為 Prisma Access 會保留這些 IP 位址和子網路供內部使用：

- 169.254.0.0/16
- 100.64.0.0/10



我們建議使用符合 *RFC 1918* 的 *IP* 位址集區。雖然支援針對行動使用者使用不符合 *RFC 1918*（公用）規範的 *IP* 位址，但不建議使用這些位址，因為可能與網際網路公用 *IP* 位址空間發生衝突。

**STEP 10 |** 若要為內部和外部（公用）網域指定 DNS 解析設定，請選取 **Network Services**（網路服務）頁籤並 **Add**（新增）設定。

具有作用中通道連線的 GlobalProtect 端點會使用其虛擬網路介面卡而不是實體網路介面卡，因此需要個別的 DNS 解析設定。

在 **Network Services**（網路服務）視窗中設定網路設定。

- 從下拉式清單中選取一個 **Region**（區域）。

  選取 **Worldwide**（全世界）、選取一個劇院，或選取一個要全域套用 DNS 設定的位置群組。如果您指定多個 Proxy 設定，其中混合了全世界、劇院和位置群組特定的設定，則

 ©2025 Palo Alto Networks, Inc.

Prisma Access 會先使用位置群組的設定，接著是劇院，然後全世界。Prisma Access 會在清單中從上到下評估規則。

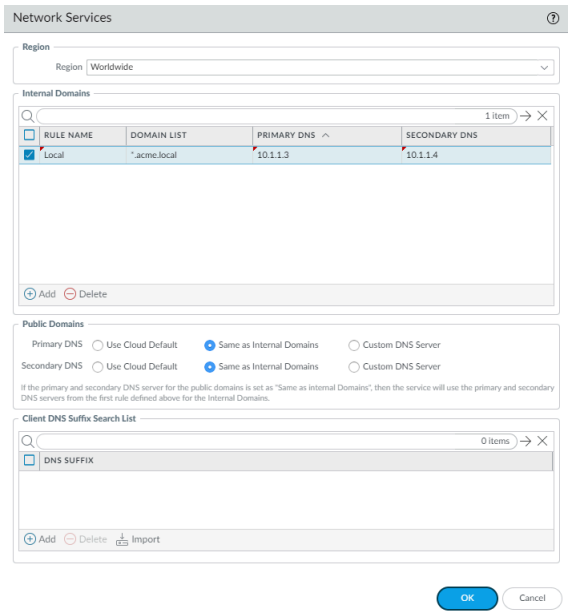
- **Add**（新增）一或多個規則以設定 **Internal Domain**（內部網域）的 DNS 設定。
  - 為規則輸入唯一的 **Rule Name**（規則名稱）。
  - 請勿輸入 127.0.0.1 位址，因為它可能會導致 Prisma Access 內部路由問題。
  - 如果您想要內部 DNS 伺服器僅解析您指定的網域，請在 **Domain List**（網域清單）中輸入要解析的網域。在網域前面指定一個星號；例如，*.acme.com。。您最多可以指定 1,024 個網域項目。

    *Prisma Access* 有一個預先定義的規則，使用 *Cloud Default* 伺服器解析 **.amazonaws.com*、**.aws.amazon.com*、**.googleapis.com* 和 **.google.internal* 網域。如果您想要內部 *DNS* 伺服器解析更具體的網域（例如 **.s3.amazonaws.com* 而不是 **.amazonaws.com*），請在 ***Domain List***（網域清單）中輸入 *URL*。*Prisma Access* 會在清單中從最長到最短，然後從上到下評估網域名稱。
  - 如果您有可以存取內部網域的 **Custom DNS server**（自訂 **DNS** 伺服器），請指定 **Primary DNS**（主要 **DNS**）和 **Secondary DNS**（次要 **DNS**）伺服器 IP 位址，或選取 **Use Cloud Default**（使用雲端預設值）以使用預設 Prisma Access DNS 伺服器。
- 指定 **Public Domains**（公用網域） 的 DNS 設定。
  - **Use Cloud Default**（使用雲端預設值）—使用預設 Prisma Access DNS 伺服器。
  - **Same as Internal Domains**（與內部網域相同）—使用您用來解析內部網域的同一伺服器。選取此選項時，用來解析公用網域的 DNS 伺服器與 **Internal Domains**（內部網域）區段中為第一個規則設定的伺服器相同。
  - **Custom DNS server**（自訂 **DNS** 伺服器）—如果您有可存取公用（外部）網域的 DNS 伺服器，請在該欄位中輸入主要 DNS 伺服器位址。

  （選用）您可以**Add**（新增）一個 **DNS Suffix**（**DNS** 尾碼），以指定輸入無法解析的不完整主機名稱時，用戶端應在本機使用的尾碼，例如，acme.local。請勿在網域尾碼前面輸入萬用字元 (*)（例如，acme.com）。您可以新增多個尾碼。
- 如果想要 Prisma Access 對 DNS 要求進行 Proxy，請設定 UDP 查詢的值（以秒為單位重試查詢的 **Interval**（間隔），以及重試 **Attempts**（嘗試）的執行次數）。

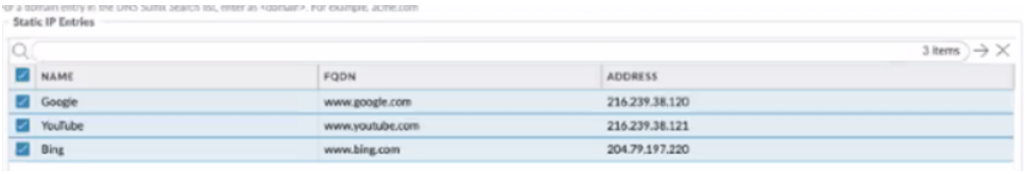
  如需 Prisma Access 如何對 DNS 要求進行 Proxy 的詳細資訊，請參閱行動使用者—GlobalProtect 部署的 DNS 解析。

 ©2025 Palo Alto Networks, Inc.




**STEP 11 |** （選用）使用 **Static IP Entries**（靜態 **IP** 項目）將 FQDN 解析為特定 IP 位址。

如果您的組織中有來賓網際網路服務，並且您想要來賓安全地使用搜尋引擎，防止他們搜索可能違反公司政策的不適當或冒犯性資料，則此功能可能非常有用。若要這樣做，請為靜態項目規則輸入唯一的 **Name**（名稱），並輸入 **FQDN** 和應該在其中導向 FQDN 要求的 IP **Address**（位址）。



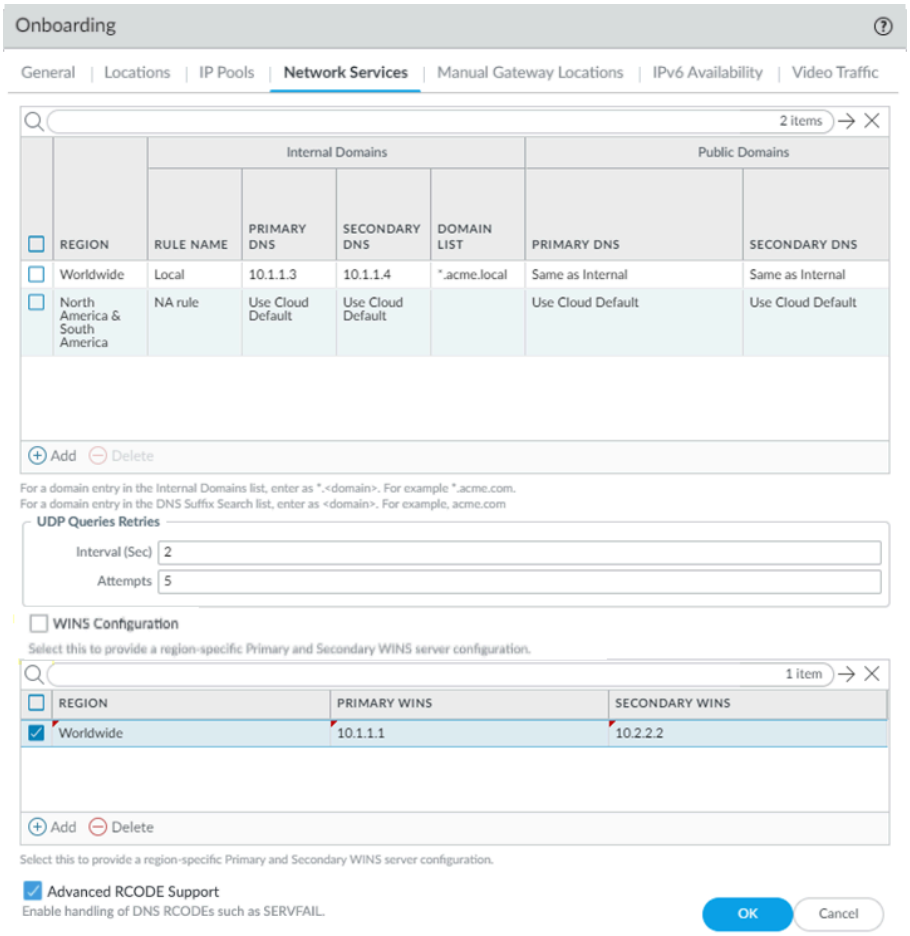

**STEP 12 |** （選用）如果您的部署使用 Windows 網際網路名稱服務 (WINS) 型，則您可以指定 WINS 伺服器來解析 NetBIOS 名稱至 IP 位址對應，方法是選取 **WINS Configuration**（**WINS** 設定）；為 WINS 伺服器選取一個區域，或選取 [Worldwide（全世界）] 以全世界套用 WINS 設定，然後指定 **Primary WINS**（主要 **WINS**），並選擇性地指定 **Secondary WINS**（次要 **WINS**）伺服器位址。

在您啟用 WINS 之後，Prisma Access 可以透過 GlobalProtect 將 WINS 設定推送到行動使用者的端點。

 ©2025 Palo Alto Networks, Inc.

**STEP 13 |** （選用）選取 [Advanced RCODE Support（進階 RCODE 支援）]，當收到 RCODE 2 (SERVFAIL) 和 RCODE 5 (REFUSED) DNS 傳回代碼時，允許主要 DNS 伺服器容錯移轉至次要 DNS 伺服器

DNS 回應代碼 SERVFAIL 表示與主要 DNS 伺服器的通訊錯誤，DNS 回應代碼 REFUSED 表示主要 DNS 伺服器拒絕提供要求的資訊。在這兩種情況下，服務都會容錯移轉到次要 DNS 伺服器。




 ©2025 Palo Alto Networks, Inc.

**STEP 14 |** （選用）如果您允許行動使用者從 GlobalProtect 應用程式手動選取閘道，請選取使用者可以從其 GlobalProtect 應用程式檢視的 **Manual Gateway Locations**（手動閘道位置）。

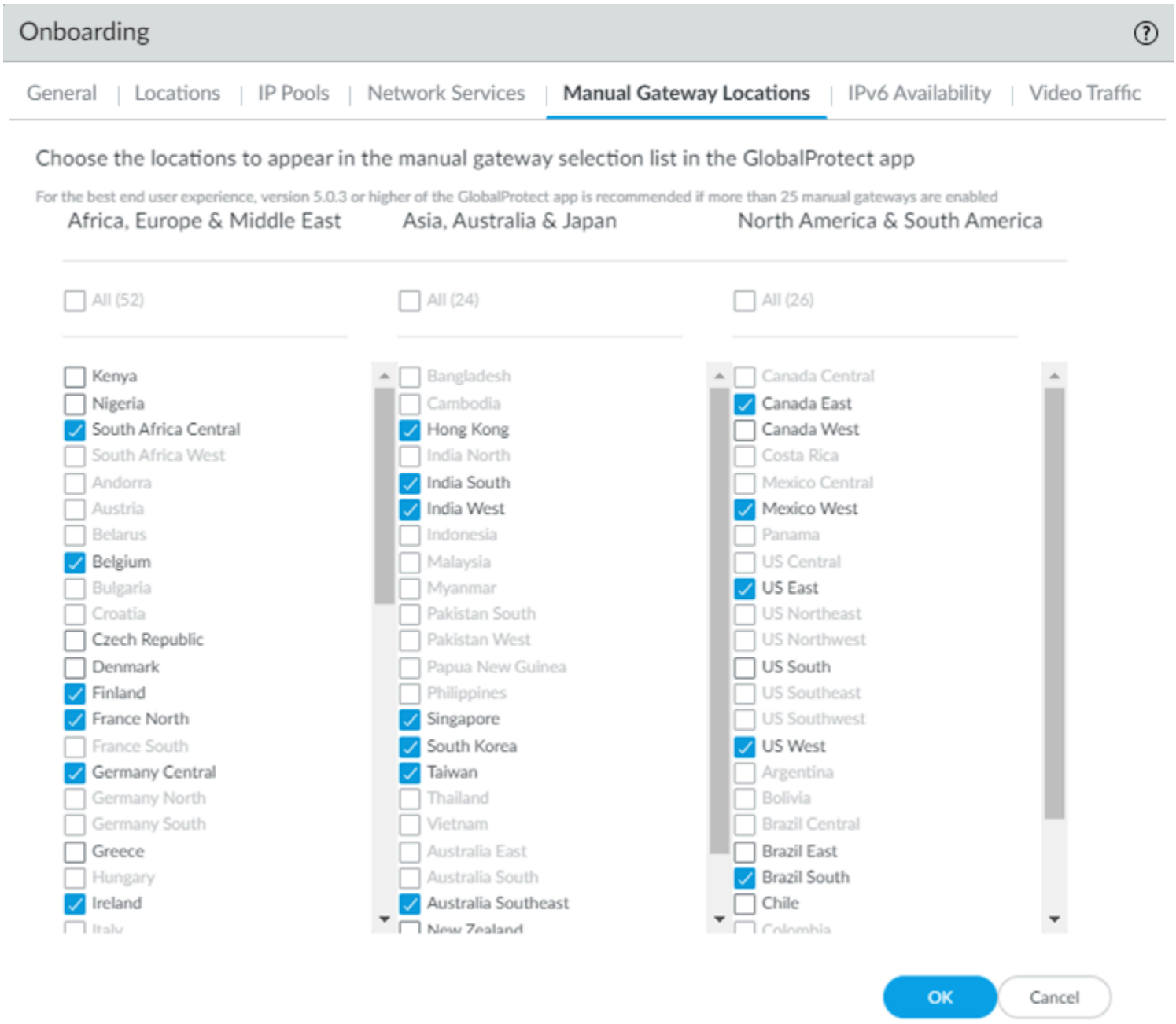
選擇裝載位置的子集會減少行動使用者可以在其 GlobalProtect 應用程式中檢視以進行手動閘道選擇的可用閘道數目。

如果您未在此頁籤中選取手動閘道，Prisma Access 預設選取以下閘道清單。

- 澳大利亞東南部
- 比利時
- 巴西南部
- 加拿大東部
- 芬蘭
- 法國北部
- 德國中部
- 香港
- 印度西部
- 愛爾蘭
- 以色列
- 日本中部
- 荷蘭中部
- 沙烏地阿拉伯
- 新加坡
- 南非中部
- 韓國
- 臺灣
- 英國
- 美國東部
- 美國西部

Prisma Access 讓您僅選取已裝載的閘道。例如，如果您在選取位置時未選擇 **UK**（英國），則無法選取 **UK**（英國）作為手動閘道（該位置呈灰色）。

 ©2025 Palo Alto Networks, Inc.




如果您需要在裝載位置之後將其刪除，且其被選為其中一個 ***Manual Gateway Locations***（手動閘道位置），請務必在這裡以及 ***Locations***（位置）頁籤中取消選取它。

**STEP 15 |** 按一下 **OK**（確定）以儲裝載設定。

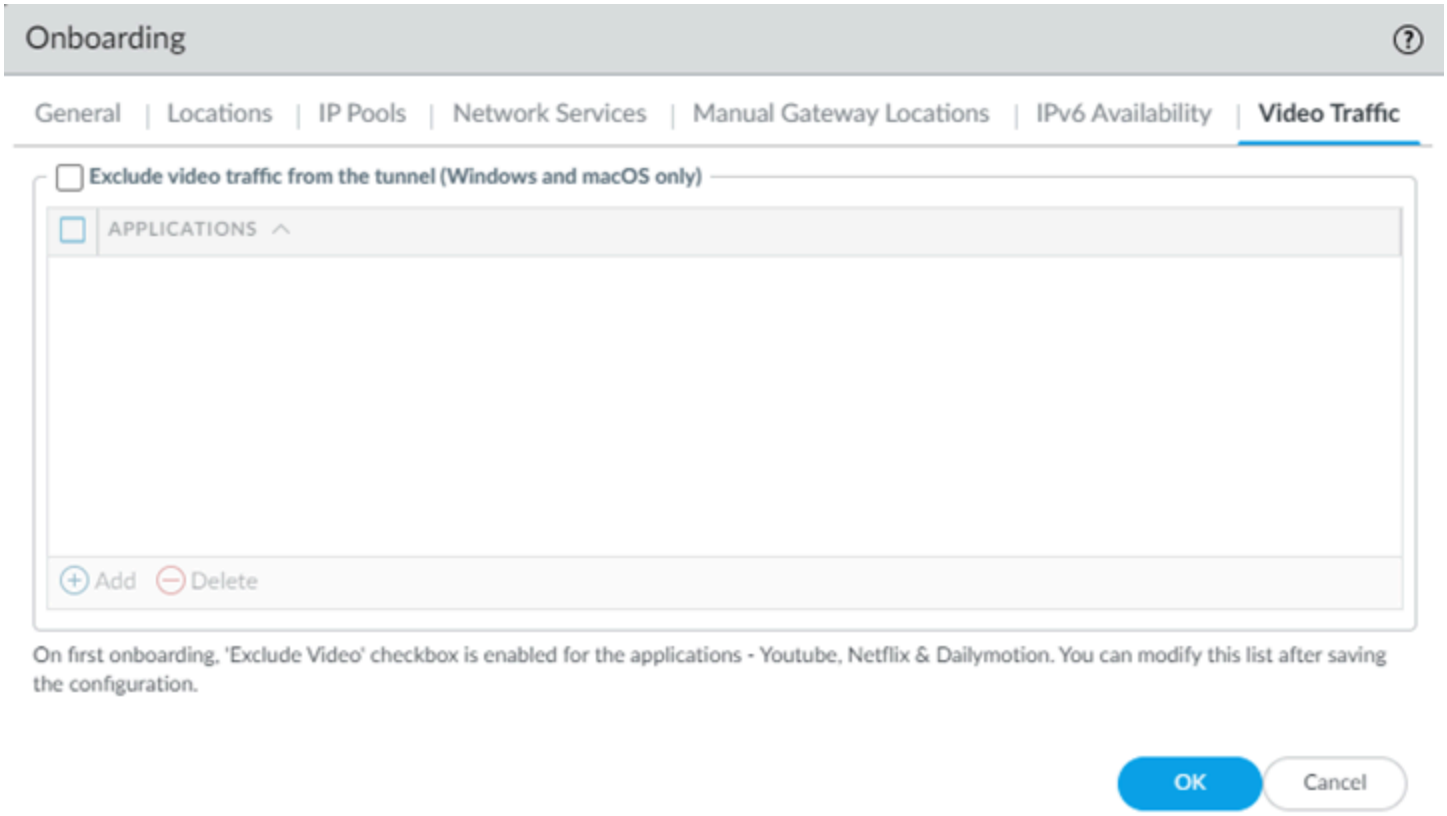
**STEP 16 |** 設定 **IPv6 Availability**（**IPv6** 可用性）選項。

如果您在 Mobile Users-GlobalProtect 部署中使用 IPv6 網路，則可以設定 Prisma Access，在行動使用者網路中使用 IPv6 位址。您還需要在 Prisma Access 基礎結構中全域啟用 IPv6 網路，然後才能使用 IPv6 定址。


©2025 Palo Alto Networks, Inc.

**STEP 17 |** （選用，僅限 Windows 和 macOS）從 GlobalProtect 通道中排除視訊流量。

**Exclude video traffic from the tunnel**（從通道中排除視訊流量）；然後，**Add**（新增）或 **Delete**（刪除）要從 GlobalProtect 通道中排除的視訊串流應用程式。




**STEP 18 |** 建立安全性政策規則以保護您行動使用者的流量。

1. 選取要在其中新增政策規則的 **Device Group**（裝置群組）。您可以選取 Mobile_User_Device_Group 或您在為行動使用者設定 Prisma Access 時選取的父系裝置群組。
2. 建立安全性政策規則。確保您沒有定義安全性政策規則來允許從任何區域到任何區域的流量。在安全性政策規則中，使用您在範本堆疊中定義的區域。

**STEP 19 |** 設定要轉送到 Strata Logging Service 的日誌。

在新安裝之後或從 Prisma Access 範本堆疊中移除非 Prisma Access 範本時，雲端服務外掛程式會自動新增下列日誌設定（**Device**（裝置） > **Log Settings**（日誌設定））：

- 系統日誌 (**system-gpcs-default**)、User-ID 日誌 (**userid-gpcs-default**)、HIP 比對日誌 (**hipmatch-gpcs-default**) 和 GlobalProtect 日誌 (**gp-prismaaccess-default**) 的日誌設定會新增至 Mobile_User_Template。
- 系統日誌 (**system-gpcs-default**)、User-ID 日誌 (**userid-gpcs-default**) 和 GlobalProtect 日誌 (**gp-prismaaccess-default**) 的日誌設定會新增至 Remote_Network_Template。
- 系統日誌 (**system-gpcs-default**) 和 GlobalProtect 日誌 (**gp-prismaaccess-default**) 的日誌設定會新增至 Service_Conn_Template。

這些日誌設定會自動將系統、User-ID 和 HIP 比對日誌轉送到 Strata Logging Service。

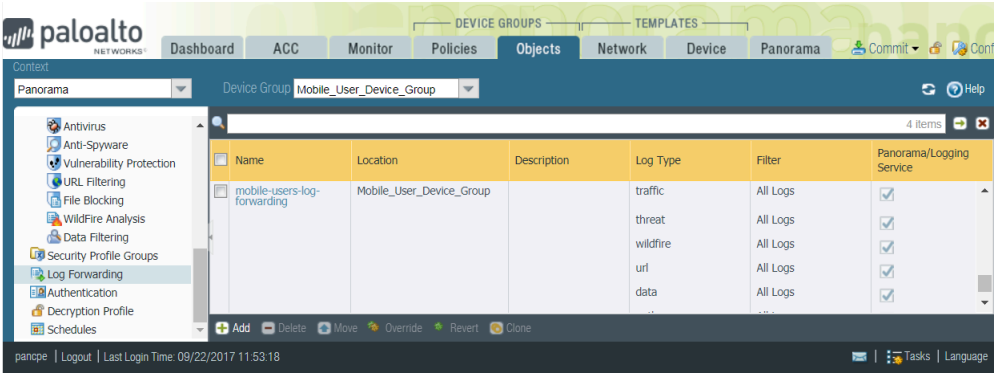
 ©2025 Palo Alto Networks, Inc.

**STEP 20 |** （選用）將其他日誌類型的日誌轉送到 Strata Logging Service。

若要這樣做，您必須建立一個日誌轉送設定檔，並將其附加至每個您想要為其轉送日誌的政策規則。

1. 選取已在其中新增政策規則的 **Device Group**（裝置群組）。
2. 選取 **Objects**（物件） > **Log Forwarding**（日誌轉寄），然後 **Add**（新增） 設定檔。在日誌轉送設定檔比對清單中，**Add**（新增）您想要轉送的每一種日誌類型。

   以下範例啟用流量、威脅防護、WildFire 提交、URL 篩選、資料篩選和驗證日誌的轉送。
3. 選取 **Panorama/Strata Logging Service**（**Panorama/Strata** 記錄服務）作為轉送方法。當您選擇 Panorama 時，日誌會轉送到 Strata Logging Service。您將能夠監控日誌並從 Panorama 產生報告。Strata Logging Service 提供無縫整合來儲存日誌，無需將其回傳到公司總部的 Panorama，並且 Panorama 可以視需要查詢 Strata Logging Service。

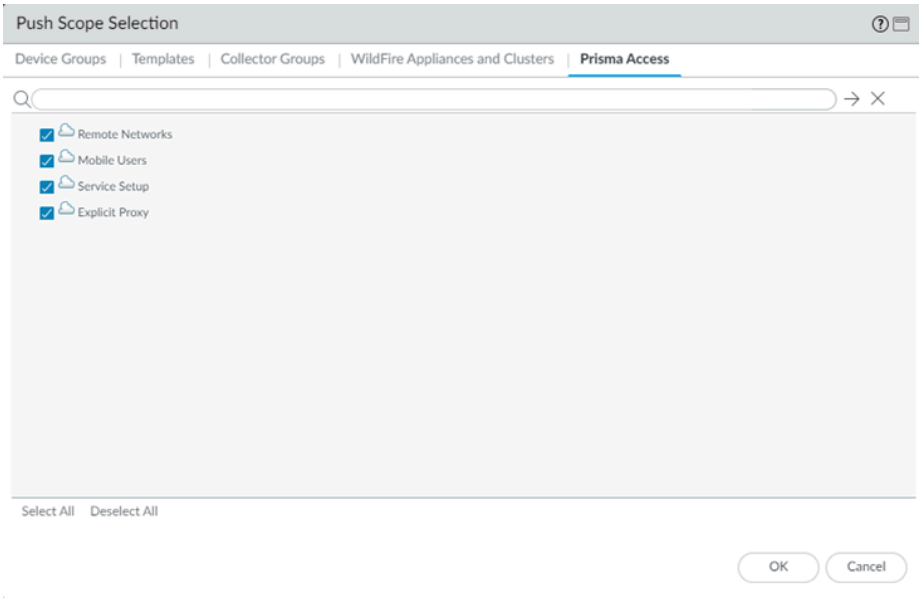



4. 選取 **Policies**（政策） > **Security**（安全性），然後編輯政策規則。在 **Actions**（動作）中，選取所建立的日誌轉送設定檔。

 ©2025 Palo Alto Networks, Inc.

**STEP 21 |** 將您的所有變更提交到 Panorama，並將設定變更推送到 Prisma Access。

1. 按一下 **Commit**（提交） > **Commit and Push**（提交並推送）。
2. **Edit Selections**（編輯選取項目），並在 **Prisma Access** 頁籤中，確保在 **Push Scope**（推送範圍）中選取了 **Mobile Users**（行動使用者）和 **Explicit Proxy**（明確 **Proxy**），然後按一下 **OK**（確定）。



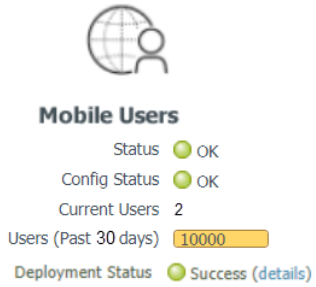

3. 在 **Device Groups**（裝置群組）頁籤中，請確保您已選取 **Explicit Proxy**（明確 **Proxy**）和 **GlobalProtect** 裝置群組。
4. 按一下 **Commit and Push**（提交並推送）。


©2025 Palo Alto Networks, Inc.

**STEP 22 |** 若要驗證 Prisma Access for Users 是否已部署並作用中，請選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Status**（狀態）。

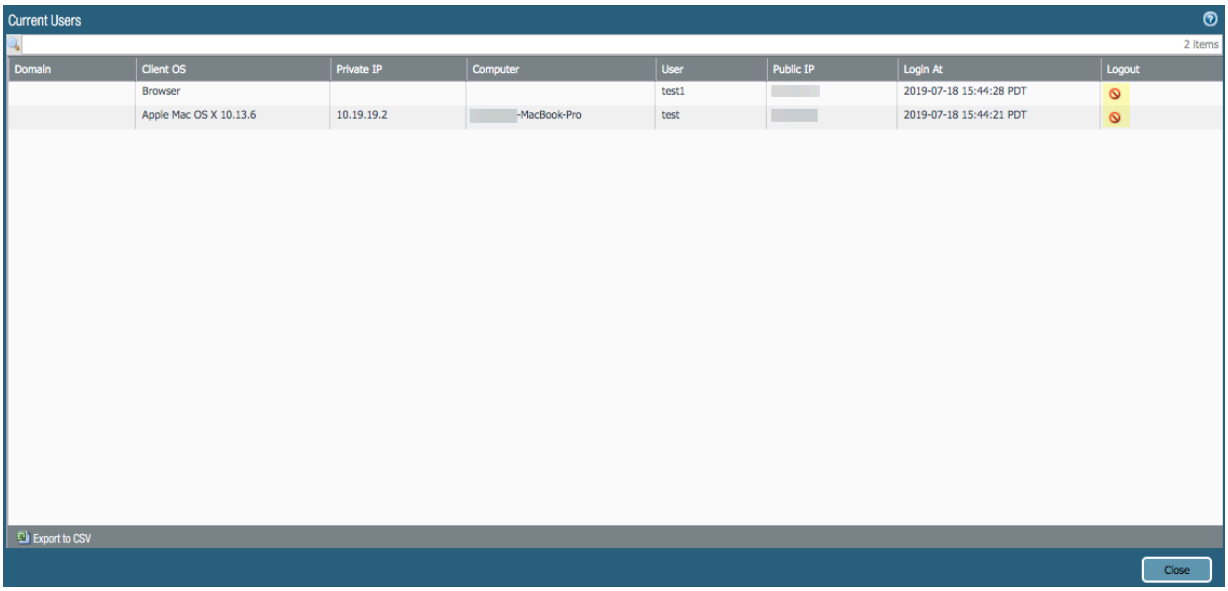
在佈建完成之後，行動使用者的 **Status**（狀態）和 **Config Status**（設定狀態）應顯示 **OK**（成功）。

**Deployment Status**（部署狀態）區域允許您在完成裝載和部署工作之前檢視其進度，以及查看有關已完成工作狀態的詳細資訊。




若要檢視目前登入的唯一使用者數目，或若要登出已登入的使用者，請按一下 **Current Users**（目前使用者）旁邊的超連結數字。

 ©2025 Palo Alto Networks, Inc.

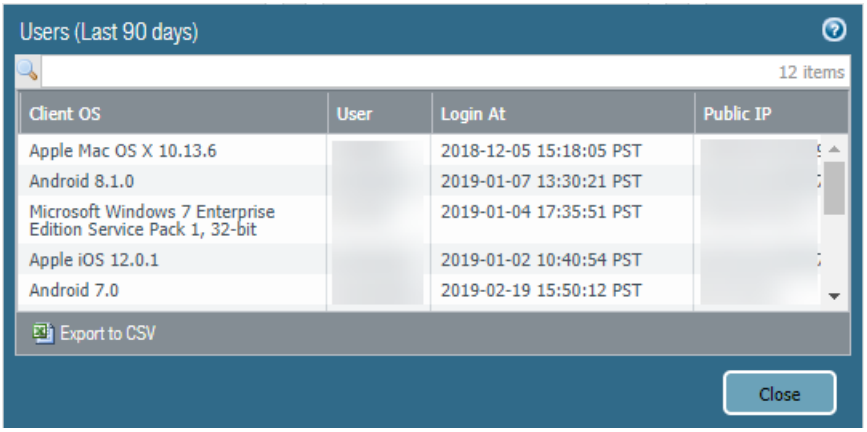



若要檢視先前 90 天內登入的使用者的歷程資訊，請按一下 **Users (Last 90 days)**（使用者（過去 **90** 天））旁邊的數字。

當 [Users (Last 90 days)（使用者（過去 90 天））] 欄位中的使用者數目達到授權總數的 80% 時，該數字會以紅色顯示。

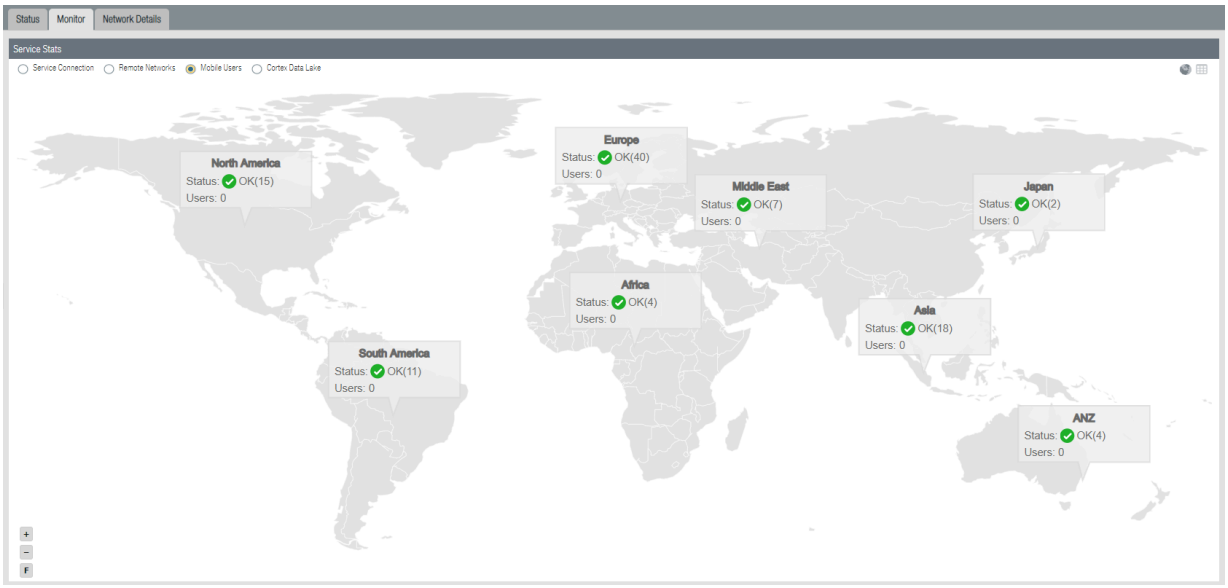
若要將使用者清單匯出到 CSV 檔案，請選取 **Export to CSV**（匯出至 **CSV**）。請注意，最多可以將 45,000 個使用者匯出到 CSV 檔案。


©2025 Palo Alto Networks, Inc.




若要顯示一張地圖，其中顯示在您所選區域中執行的Prisma Access 入口網站和閘道的位置，請選取 **Monitor**（監控）；然後，選取 **Mobile Users**（行動使用者）。

 ©2025 Palo Alto Networks, Inc.




選取一個區域，以取得更多有關該區域的詳細資訊。

- **Location**（位置）—部署雲端服務基礎結構以保護網路上行動使用者的位置。

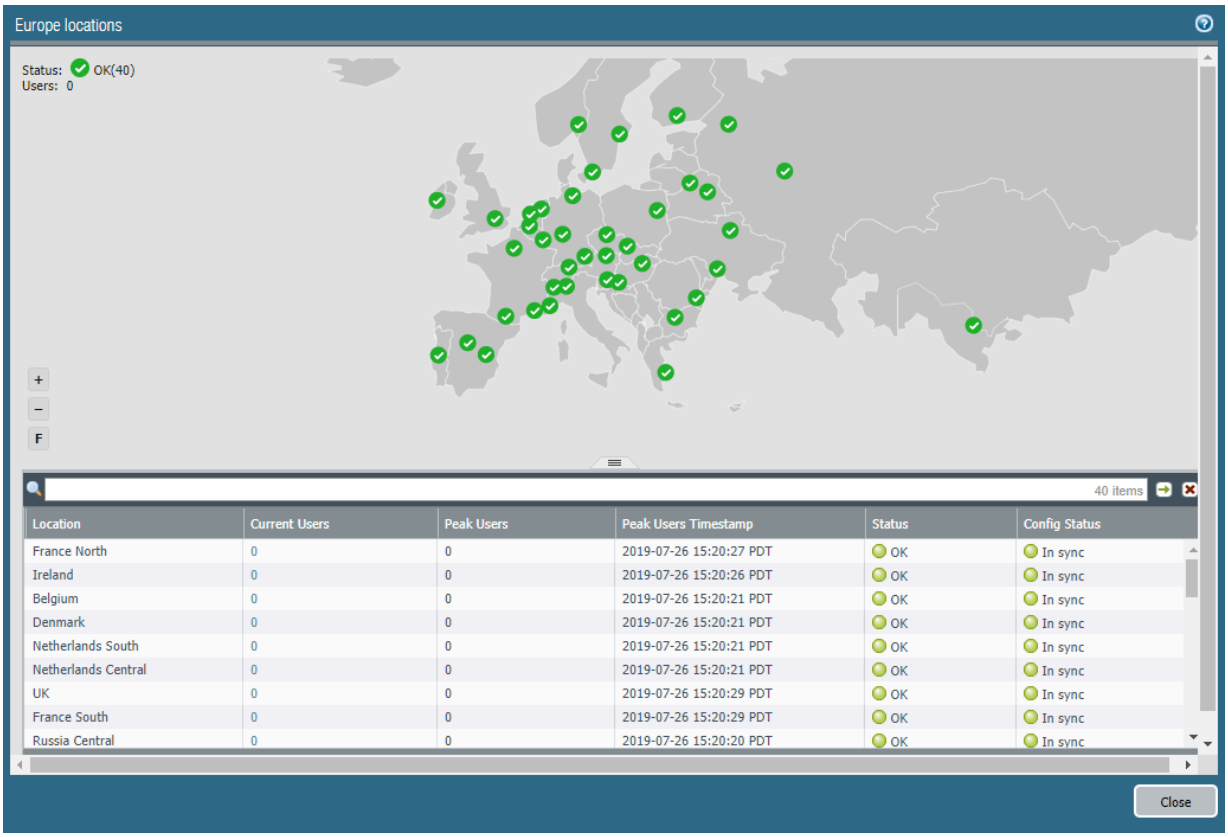

©2025 Palo Alto Networks, Inc.

- **Current Users**（目前使用者）—已連線並受服務保護的使用者數目。

  當目前行動使用者數目達到授權總數的 80% 時，此數字會以紅色顯示。
- **Peak Users**（峰值使用者）—並行使用者數目上限的計數。
- **Peak Users Timestamp**（峰值使用者時間戳記）—上次擷取峰值使用者資料時的時間戳記。
- **Status**（狀態）—Prisma Access 與您行動使用者之間連線的操作狀態。
- **Config Status**（設定狀態）—上次推送設定到服務的狀態。如果您已在本機進行了變更，但尚未將設定推送到雲端，這可能會顯示狀態 **Out of sync**（不同步）。將游標暫留在狀態指


©2025 Palo Alto Networks, Inc.

示器上，以取得更多的詳細資訊。在提交並推送設定到 Prisma Access 之後，設定狀態會變更為 **In sync**（同步）。




**STEP 23 |** 如果您選擇要為入口網站主機名稱 **Use Company Domain**（使用公司網域），則必須在內部 DNS 伺服器上新增 DNS 項目，以將您定義的入口網站主機名稱對應至 **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users**（行動使用者） > **Onboarding**（裝載） > **General**（一般）頁籤上顯示的入口網站 DNS CNAME（例如，*<portal_hostname>*.gpcloudservice.com）。

 ©2025 Palo Alto Networks, Inc.

**STEP 24 |** 將 GlobalProtect 應用程式軟體部署至您的一般使用者。

對於 Mac OS 或 Windows 使用者，您可以將這些使用者導向至 Prisma Access 入口網站位址，他們可以在這裡從入口網站下載 GlobalProtect 應用程式。

*Prisma Access* 會管理入口網站上 *GlobalProtect* 應用程式的版本，而且您可以從 *Prisma Access* 託管的版本中選取作用中版本，以及控制使用者下載該版本的能力。

或者，您可以為 Mac OS 和 Windows 使用者在 Web 伺服器上託管 GlobalProtect 應用程式軟體。Prisma Access 與未列示為生命週期結束的任何 GlobalProtect 應用程式版本相容。

行動應用程式使用者可以從適合其作業系統的應用程式商店下載並安裝 GlobalProtect 行動應用程式。

# GlobalProtect—自訂通道設定

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

為 GlobalProtect 應用程式建立以連線至 Prisma Access 的 VPN 通道自訂設定。通道設定包括分割通道選項，您可以使用這些選項，定義應用程式傳送至 Prisma Access 的流量，以及哪些流量可以在本機路由（例如不需要用於商業用途的帶寬密集型應用程式）。

您為通道設定定義的 **Match Criteria**（比對規則）告訴 Prisma Access 應該接收這些設定的使用者、裝置或系統。例如，您可以指定通道設定規則適用於特定區域中 GlobalProtect 應用程式的所有執行個體。在 Prisma Access (Managed by Panorama) 中，您可以根據存取路由以及網域和應用程式設定分割通道設定。

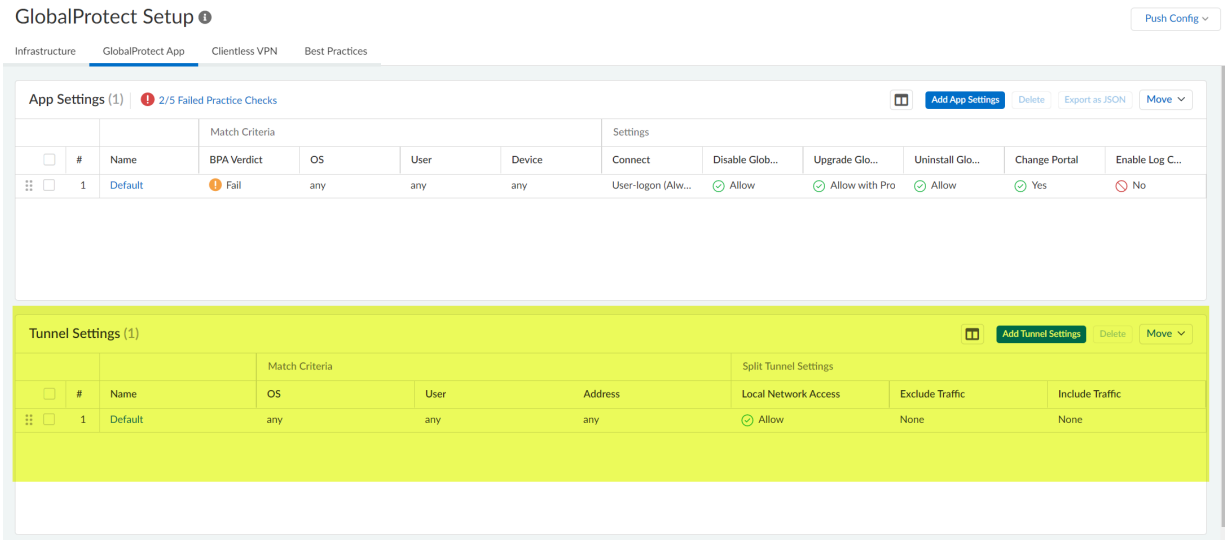
- Strata Cloud Manager
- Panorama

## GlobalProtect—自訂通道設定 (Strata Cloud Manager)

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** 按一下 **Manage**（管理）**> Service Setup**（服務設定）**> Mobile Users**（行動使用者）**> GlobalProtect Setup**（**GlobalProtect** 設定）**> GlobalProtect App**（**GlobalProtect** 應用程式）**> Add Tunnel Settings**（新增通道設定）。

如果您使用的是 *Strata Cloud Manager*，請按一下 ***Workflow***（工作流程）***> Prisma Access Setup***（***Prisma Access*** 設定）***> Mobile User***（行動使用者）***> GlobalProtect Setup***（***GlobalProtect*** 設定）***> GlobalProtect App***（***GlobalProtect*** 應用程式）***> Add Tunnel Settings***（新增通道設定）。




**STEP 2 |** 輸入名稱和 **Match Criteria**（比對規則），以指定應該接收設定的使用者、裝置或系統。例如，您可以指定通道設定規則適用於特定區域中 GlobalProtect 應用程式的所有執行個體。

**STEP 3 |** 為 Prisma Access 啟用 **Authentication Override**（驗證覆寫），產生並接受安全、加密的 Cookie 以進行使用者驗證。此設定可讓使用者在指定的時段內僅提供一次登入認證。

- **Generate cookie for authentication override**（為驗證取代產生 **cookie**）—啟用 Prisma Access 以產生加密、端點特定的 Cookie，並向端點發出驗證 Cookie。
- **Accept cookie for authentication override**（接受用於驗證覆寫的 **Cookie**）—可讓 Prisma Access 透過有效的加密 Cookie 驗證使用者。當應用程式呈現有效的 Cookie 時，Prisma Access 會驗證該 Cookie 是否最初由 Prisma Access 加密、解密該 Cookie，然後驗證使用者。

*GlobalProtect* 應用程式必須知道連線使用者的使用者名稱，以比對並從使用者的端點擷取相關聯的驗證 *Cookie*。在應用程式擷取 *Cookie* 之後，其會將這些 *Cookie* 傳送至 *Prisma Access* 進行使用者驗證。


©2025 Palo Alto Networks, Inc.

**STEP 4 |** 啟用 **Split Tunneling**（分割通道）以定義 GlobalProtect 應用程式允許或限制通過 VPN 通道流向 Prisma Access 的流量。分割通道會保留頻寬，方法是排除不是業務關鍵或無法提高生產力的 Prisma Access 流量。

- **Local Network Access**（區域網路存取）—讓 Windows 和 Mac 使用者可以存取本機資源，無需他們先連線到 Prisma Access。

  **Exclude Traffic**（排除流量）—根據應用程式、網域和路由（如 IP 位址）指定要從 Prisma Access 政策檢查和強制執行中排除的流量。

  **Customize Include Traffic**（自訂包含流量）—根據預設，GlobalProtect 應用程式會將所有流量路由到 Prisma Access，但排除清單中的流量除外。指定 GlobalProtect 應用程式應一律路由到 Prisma Access 的流量，即使它符合排除清單準則也是如此。

**STEP 5 |** **Exclude Video Stream Traffic**（排除視訊串流流量），不將視訊串流流量從列出的應用程式傳送至 Prisma Access。透過從 VPN 通道排除低風險視訊串流流量（如 YouTube 與 Netflix），您可以減少頻寬消耗。視訊串流排除適用於 GlobalProtect 應用程式傳送至 Prisma Access 的所有流量，而不只是您已對此規則定義的比對規則。

**STEP 6 |** 儲存設定。重複上述步驟以新增更多的通道設定。

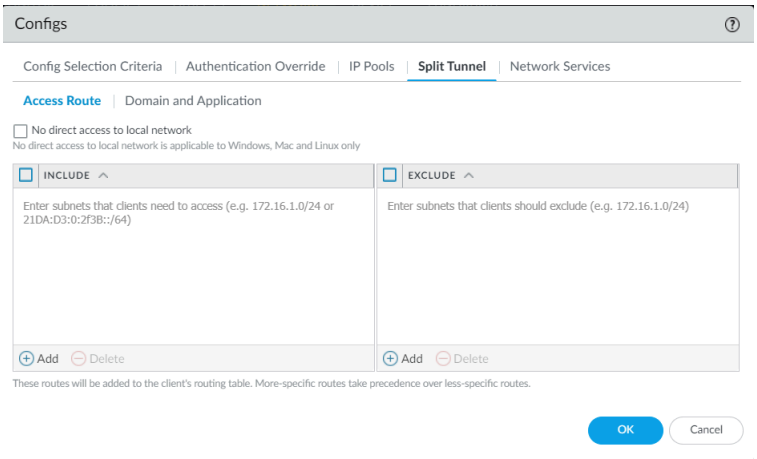
**STEP 7 |** （選用）移動以設定在連線至 Prisma Access 時使用 VPN 通道設定的優先順序。

## GlobalProtect—自訂通道設定 (Panorama)

您可以根據存取路由或網域和應用程式設定分割通道設定。

 ©2025 Palo Alto Networks, Inc.

- 根據存取路由設定分割通道設定。
  1. 按一下 **Panorama > Network**（網路）**> GlobalProtect > Gateways**（閘道），然後選取您要自訂的閘道。
  2. 按一下 **Agent**（代理程式）**> Client Settings**（用戶端設定），然後選取設定。
  3. 按一下 **Split Tunnel**（分割通道）**> Access Route**（存取路由）。當 GlobalProtect 應用程式與 Prisma Access 建立閘道時，分割通道設定會指派給端點上的虛擬網路卡。您可以包含或排除透過 VPN 通道傳送的特定目的地 IP 子網路流量。




  4. 啟用 **No direct access to local network**（無法直接存取區域網路）選項，以阻止使用者在連線到 GlobalProtect 時直接將流量傳送到 Proxy 或本機資源。

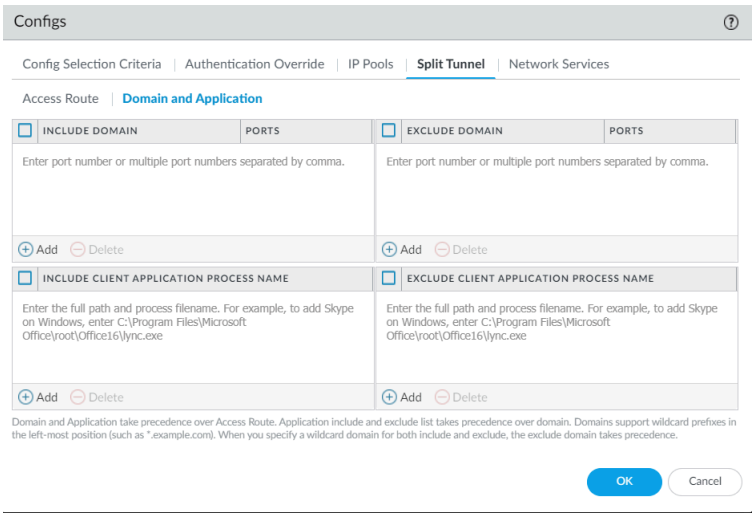
     啟用 ***No direct access to local network***（無法直接存取區域網路）設定，以降低不受信任網路（例如惡意 *Wi-Fi* 存取點）帶來的風險。
  5. 選取 **Includes**（包含）區域並 **Add**（新增）目的地子網路或位址物件（類型為 IP 網路遮罩），僅將以您的 LAN 為目標的流量路由至 GlobalProtect。您可以包含 IPv6 或 IPv4 子網路。若要包含所有目的地子網路或位址物件，請 **Include**（包含） 0.0.0.0/0 以及 ::/0 作為存取路由。
  6. 選取 **Excludes**（排除），並**Add**（新增）您想要應用程式排除的目的地子網路或位址物件（類型為 IP 網路遮罩）。排除的路由應比包含的路由更明確，否則可能會排除掉超出原有預期的流量。您可以排除 IPv6 或 IPv4 子網路。

     您無法在 *Chromebooks* 上排除執行 *Android* 之端點的存取路由。*Chromebooks* 只支援 *IPv4* 路由。
  7. 儲存通道設定。


©2025 Palo Alto Networks, Inc.

- 根據網域和應用程式設定分割通道設定。
  1. 按一下 **Panorama > Network**（網路）**> GlobalProtect > Gateways**（閘道），然後選取您要自訂的閘道。
  2. 按一下 **Agent**（代理程式）**> Client Settings**（用戶端設定），然後選取設定。
  3. 按一下 **Split Tunnel**（分割通道）**> Domain and Application**（網域和應用程式）頁籤，以根據目的地網域設定分割通道設定。

     在 *macOS* 端點上使用 *Sophos* 等第三方端點安全性產品時，您可能會遇到一些不相容性問題。




     - （選用）選取 **Include Domain**（包含網域），並 **Add**（新增）您想要使用目的地網域和連接埠透過 VPN 連線路由至 GlobalProtect 的 SaaS 或公共雲端應用程式您可新增最多 200 個項目至清單。例如，新增 *.gmail.com 以允許所有 Gmail 流量通過 VPN 通道。
     - （選用）選取 **Exclude Domain**（排除網域），並 **Add**（新增）您想要使用目的地網域和連接埠從 VPN 通道排除的 SaaS 或公共雲端應用程式。您可新增最多 200 個項目至清單。例如，新增 *.target.com 以從 VPN 通道排除所有 Target 流量。
  4. 根據應用程式設定分割通道設定。

     *Safari* 流量無法新增至 *macOS* 端點上的應用程式型分割通道規則。

     您可以使用環境變數，根據 *Windows* 和 *macOS* 端點上的應用程式設定分割通道。

     - （選用）選取 **Include Client Application Process Name**（包含用戶端應用程式處理序名稱），並 **Add**（新增）您想要使用應用程式處理序名稱透過 VPN 連線路由至 GlobalProtect 的 SaaS 或公共雲端應用程式。您可以將最多 200 個項目新增至清單。
     - （選用）選取 **Exclude Client Application Process Name**（排除用戶端應用程式處理序名稱），並 **Add**（新增）您想要使用應用程式處理序名稱從 VPN 通道排除的 SaaS 或公共雲端應用程式。您可以將最多 200 個項目新增至清單。
  5. 儲存通道設定。

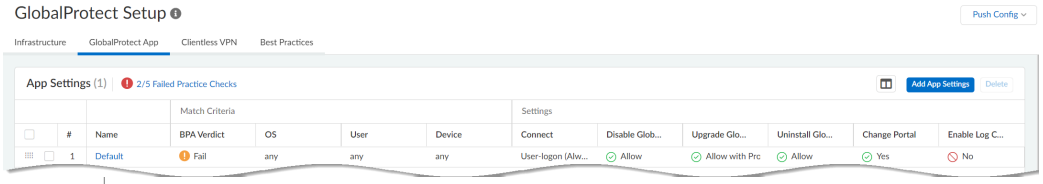
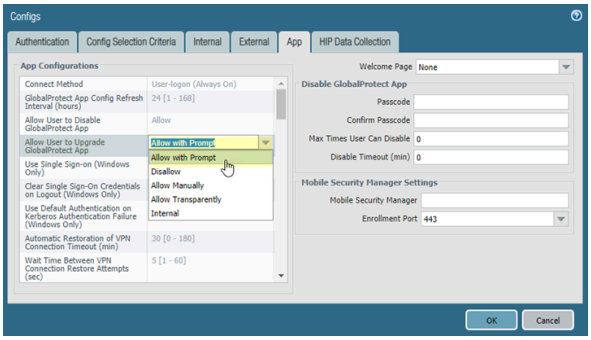
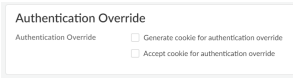

©2025 Palo Alto Networks, Inc.

# GlobalProtect—自訂應用程式設定

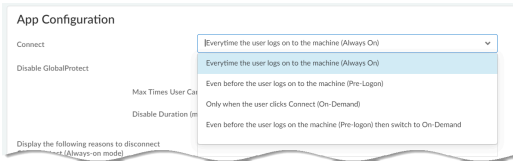
| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

自訂一般使用者與 GlobalProtect 應用程式互動的方式。

有一些您可以全域自訂的設定。這些 **global app settings**（全域應用程式設定）適用於所有裝置上的 GlobalProtect 應用程式。其他 GlobalProtect 應用程式設定是透過預設值設定的。然後，您可以自訂這些選項，並根據 **match criteria**（比對規則）將它們的目標設為特定的使用者和裝置。您為應用程式設定定義的比對規則告訴 Prisma Access，應接收設定的使用者、裝置或系統。例如，您可以指定規則僅適用於序號與 Active Directory 項目相符的裝置。

| GlobalProtect 應用程式設定 | |
| --- | --- |
| 在這裡探索和自訂應用程式設定（雲端管理範例如下所示）—> | Prisma Access (Managed by Strata Cloud Manager)<br>  <br>Panorama Managed Prisma Access<br>  |
| 驗證覆寫 | 可讓 Prisma Access 產生並接受安全、加密的 Cookie，以進行使用者驗證。開啟此功能可讓使用者在指定的時段內僅提供一次登入認證。<br>  <br>• **Generate cookie for authentication override**（產生 **Cookie** 進行驗證覆寫）—可讓 Prisma Access 產生加密、端點特定的 Cookie，並向端點發出驗證 cookie。 |

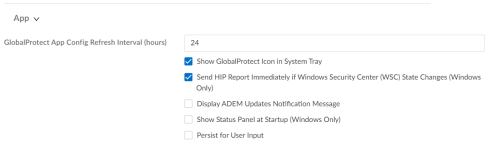
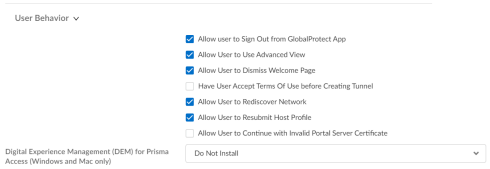
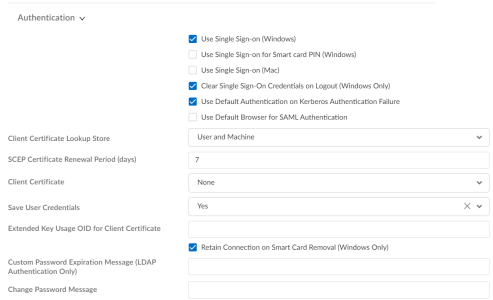
 ©2025 Palo Alto Networks, Inc.

| GlobalProtect 應用程式設定 | |
|---|---|
| | • **Accept cookie for authentication override**（接受用於驗證覆寫的 **Cookie**）—可讓 Prisma Access 透過有效的加密 Cookie 驗證使用者。當應用程式提供有效的 Cookie 時，Prisma Access 會驗證 Cookie 原先是否已由 Prisma Access 加密、解密 Cookie，然後驗證使用者。<br><br>*GlobalProtect* 應用程式必須知道連線使用者的使用者名稱才能比對和擷取來自使用者端點的驗證 *cookie*。在應用程式擷取 *Cookie* 之後，其會將這些 *Cookie* 傳送至 *Prisma Access* 進行使用者驗證。<br>• **Cookie Lifetime**（**Cookie** 存留時間）—指定 Cookie 有效的小時數、天數或週數（預設為 24 小時）。小時範圍為 1 至 72；週範圍為 1 至 52；天數範圍為 1 至 365。在 Cookie 到期之後，使用者必須重新輸入登入認證，然後 Prisma Access 會加密新 Cookie 以傳送至應用程式。此值可與您設定的 Cookie 存留時間一致或不同。<br>• **Certificate to Encrypt/Decrypt Cookie**（用於加密/解密 **Cookie** 的憑證）—選取 RSA 憑證，以用於加密與解密 Cookie。 |
| 連線設定 | 指定 GlobalProtect 應用程式用來 **Connect**（連線）至 Prisma Access 的方法。<br><br>  <br>• **User-logon (Always On)**（使用者登入（始終開啟））—使用者一登入，GlobalProtect 應用程式就會自動連線到 Prisma Access。與 SSO 搭配使用（僅限 Windows 端點）時，登入對於一般使用者而言是透明的。<br><br>在 *iOS* 端點上，因為 *GlobalProtect* 應用程式強制所有流量經過通道，此設定會防止一次性密碼 *(OTP)* 應用程式運作。<br>• **Pre-logon (Always On)**（預先登入（始終開啟））—在使用者登入之前，GlobalProtect 應用程式會驗證使用者並建立 Prisma Access 的 VPN 通道。此選項要求您使用外部 PKI 解決方案，以將機器憑證預先部署至接收此設定的各裝置。<br>• **On-demand (Manual user initiated connection)**（視需要（手動使用者起始的連線））—使用者將必須手動啟動應用程式來連線至 GlobalProtect。 |

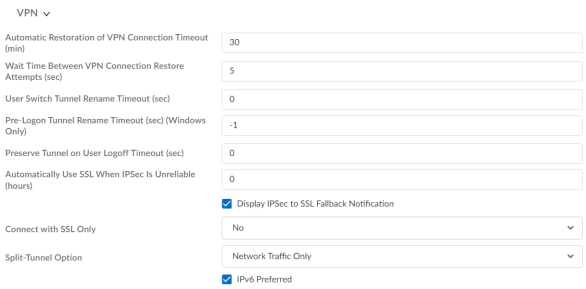
 ©2025 Palo Alto Networks, Inc.

| GlobalProtect 應用程式設定 | |
|---|---|
| | • **Pre-logon then On-demand**（預先登入然後視需要）—與 [Pre-logon (Always On)（預先登入（始終開啟））] 連線方法類似，此連線方法（需要內容發行版本 590-3397 或以上）讓 GlobalProtect 應用程式在使用者登入端點之前驗證使用者，並建立 Prisma Access 的 VPN 通道。與預先登入連線方法不同，在使用者登入之後，如果連線由於任何原因終止，使用者必須手動啟動應用程式以連線至 GlobalProtect。此選項的好處是，您可以讓使用者在密碼過期或忘記密碼後，指定一個新密碼，但仍需要此使用者在登入後手動啟動連線。 |
| **GlobalProtect** | 確定使用者可以調整哪些 GlobalProtect 應用程式設定：<br>• **Disable GlobalProtect**（停用 **GlobalProtect**）—確決使用者是否可以停用 GlobalProtect 應用程式。停用 GlobalProtect 應用程式的使用者無法連線到 Prisma Access（以及您受保護的公司資源）直到他們重新開啟該應用程式。<br>• **Upgrade GlobalProtect**（升級 **GlobalProtect**）—指定應用程式升級的運作方式，包括使用者是否可以啟動更新。<br>如果您想要控制使用者在何時能升級，您可以基於組態來自訂應用程式升級。舉例來說，如果您想在將版本部署至整個使用者群之前，先以一小群使用者測試，您可以建立組態，且該組態只套用到 IT 群組，如此能讓該群組的使用者升級並測試，而所有其他使用者/群組的組態則關閉升級。在您完全測試完新版本之後，可以針對剩餘使用者修改代理程式設定以允許升級。<br>• **Allow with Prompt**（透過提示允許）—當應用程式有新版本可用時提示使用者升級。<br>• **Allow Transparently**（明顯允許）—無需與使用者互動就會自動升級。<br>• **Internal**（內部）—當使用者連線到 Prisma Access 時，自動進行升級，無需使用者互動。<br>• **Disallow**（不允許）—防止應用程式升級。<br>• **Allow Manually**（手動允許）—讓使用者從 GlobalProtect 應用程式內啟動應用程式升級。<br>• **Uninstall GlobalProtect**（解除安裝 **GlobalProtect**）—允許使用者解除安裝 GlobalProtect 應用程式、防止其解除安裝 GlobalProtect 應用程式，或允許其在指定您建立的密碼時解除安裝。<br>• **User Can Change Portal**（使用者可以變更入口網站）—讓使用者可以變更 GlobalProtect 應用程式用來連線至 Prisma Access 的入口網站。 |

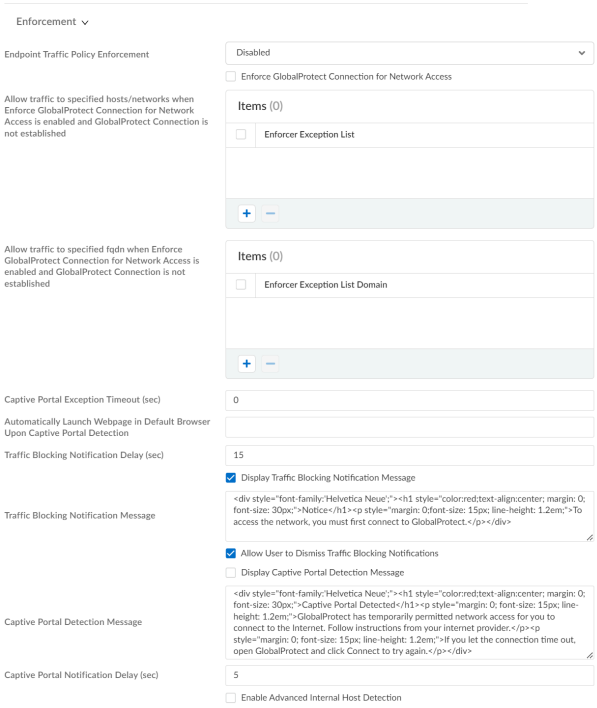
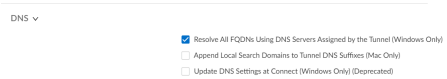
 ©2025 Palo Alto Networks, Inc.

| GlobalProtect 應用程式設定 | |
|---|---|
| 應用程式設定 - 進階選項 | |
| 應用程式設定 | • Send HIP Report Immediately if Windows Security Center (WSC) State Changes (Windows Only)（如果 Windows 安全中心 (WSC) 狀態變更，立即傳送 HIP 報告（僅限 Windows））—選取 [No（否）] 防止 GlobalProtect 應用程式在 Windows 安全中心 (WSC) 變更時傳送 HIP 資料。選取 [Yes（是）]（預設值），在 WSC 狀態變更時立即傳送 HIP 資料。<br>  |
| 使用者行為設定 | 使用者行為設定包括：<br>  |
| 驗證設定 | 驗證設定包括：<br>  |
| **VPN** 設定 | 設定 VPN 逾時和通道設定：<br>• **Display IPSec to SSL Fallback Notification**（顯示 **IPSec** 到 **SSL** 回復通知）— 選取 **No**（否） 防止在 GlobalProtect 應用程式無法建立與 IPSec 通道的連線，並回復到 SSL 通道時快顯通知。選取 **Yes**（是）（預設值）允許在連線變更時快顯通知。 |

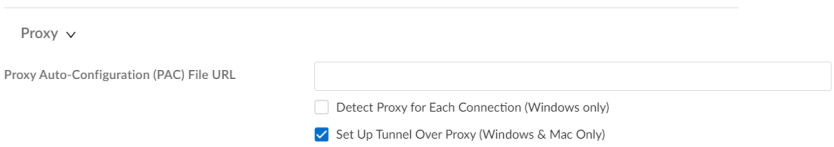
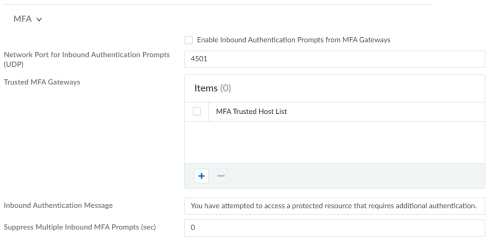
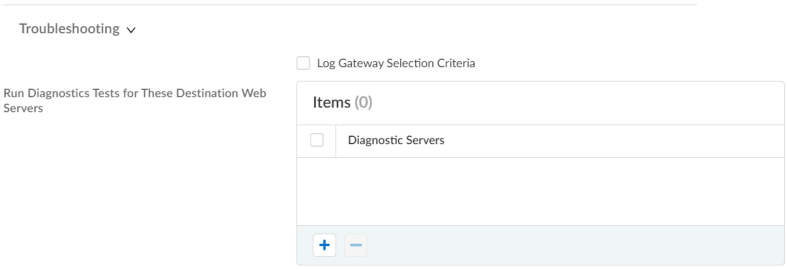
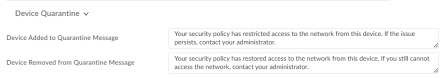
 ©2025 Palo Alto Networks, Inc.

| GlobalProtect 應用程式設定 | |
|---|---|
| |  |
| 強制執行設定 | 對指定的流量強制執行設定：<br>• 已啟用對網路存取強制執行 **GlobalProtect** 連線並建立 **GlobalProtect** 連線時允許流向指定 **FQDN** 的流量—進一步瞭解。<br>• 在執行被控制的入口網站偵測時自動在預設瀏覽器中啟動網頁 — 若要自動啟動您的預設 Web 瀏覽器，以便使用者可以無縫登入驗證入口網站，請輸入您想要用於初次連線嘗試的網站的完全合格網域名稱 (FQDN) 或 IP 位址，以在預設 Web 瀏覽器啟動時啟動 Web 流量（最大長度為 256 個字元）。然後，驗證入口網站會攔截此網站連線嘗試，並將預設 Web 瀏覽器重新導向至驗證入口網站登入頁面。若此欄位為空的（預設值），則 Prisma Access 不會在驗證入口網站偵測時自動啟動預設 Web 瀏覽器。<br>• 啟用進階內部主機偵測—啟用進階內部主機偵測，以在 GlobalProtect 應用程式進行內部主機偵測期間新增額外的安全層。利用進階內部主機偵測，除了對內部主機執行反向 DNS 查閱以確定應用程式是否在企業網路內部之外，應用程式還會驗證內部閘道的伺服器憑證。啟用進階內部主機偵測可阻止惡意行為者在內部主機偵測期間詐騙反向 DNS 伺服器回應，從而防止對企業網路中的端點進行未經 |

 ©2025 Palo Alto Networks, Inc.

| GlobalProtect 應用程式設定 | |
|---|---|
| | 授權的存取。如果您未啟用進階內部主機偵測，現有內部主機偵測會如預期運作。<br>  |
| 連線行為設定 | 連線行為設定包括：<br>  <br>進一步瞭解。 |
| **DNS** 設定 | DNS 設定包括：<br>  |
| **Proxy** 設定 | 指定要推送到端點以進行 Proxy 設定的 **Proxy Auto-Configuration (PAC) File URL**（**Proxy** 自動設定 **(PAC)** 檔案 **URL**）。最大 URL 長度為 256 個字元。支援以下 Proxy 自動設定 (PAC) 檔案 URL 方法：<br>• Proxy 自動設定 (PAC) 標準（例如，http://pac.<hostname or IP>/proxy.pac）。<br>• Web Proxy 自動探索通訊協定 (WPAD) 標準（例如，http://wpad.<hostname or IP>/wpad.dat）。 |

 ©2025 Palo Alto Networks, Inc.

| GlobalProtect 應用程式設定 | |
|---|---|
| |  |
| **MFA** 設定 | MFA 設定包括：<br>  |
| 疑難排解設定 | 疑難排解設定包括：<br>  |
| 裝置隔離設定 | 裝置隔離設定包括：<br>  |
| 內部主機偵測 | 如果您不需要行動使用者在他們位於內部網路時連線到 Prisma Access，請啟用內部主機偵測，讓 GlobalProtect 應用程式能夠確定是否其位於內部網路還是外部網路。<br>• 輸入只能從內部網路解析的主機 IP 位址（IPv4 或 IPv6）。<br>• 輸入解析為您所輸入 IP 位址的 DNS 主機名稱。<br>當行動使用者連線到 Prisma Access 時，GlobalProtect 應用程式會嘗試對指定的位址進行反向 DNS 查閱。如果查閱失敗，GlobalProtect 應用程式確定其位於外部網路，然後啟動 Prisma Access 的連線。 |
| 啟用內部主機偵測 | 如果在沒有外部閘道的情況下設定內部閘道和內部主機偵測，並且內部主機偵測失敗時，您想要 GlobalProtect 應用 |

 ©2025 Palo Alto Networks, Inc.

| GlobalProtect 應用程式設定 | |
|---|---|
| | 程式重試網路探索，請將 **Enable Intelligent Internal Host Detection**（啟用智慧內部主機偵測） 參數設為 yes。 |
| 閘道 | 根據預設，Prisma Access 位置中的所有閘道都可供使用者使用。如果您有其他 GlobalProtect 閘道（內部或外部），想要您的使用者能夠連線至其中，您可以在這裡新增這些閘道。 |
| **HIP** 資料收集 | 定義您想要應用程式從集合中收集或排除的自訂主機資訊設定檔 (HIP) 資料。啟用此選項時，應用程式會從執行 Windows、Mac 或 Linux 作業系統的裝置收集資料。<br><br>例如，自訂檢查可讓您知道某個應用程式是安裝在端點上，還是在其上執行。您定義要在自訂檢查中收集的資料包含在原始主機資訊資料中，GlobalProtect 應用程式會收集此資料，然後在該應用程式啟動時將其提交至 Prisma Access。<br><br>若要監控透過自訂檢查收集的資料，請建立 HIP 物件。接著，您可以將 HIP 物件新增至 HIP 設定檔，以使用收集到的資料來比對端點流量，並強制執行安全性規則。<br><br>前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（物件） > **HIP**，以及 **HIP Objects**（**HIP** 物件）或 **HIP Profiles**（**HIP** 設定檔）。選取 **Prisma Access** > **Mobile Users Container**（行動使用者容器） > **GlobalProtect** 設定範圍。 |
| 逾時設定 | • 在 [GlobalProtect Setup（GlobalProtect 設定）] 頁面上，選取 [Global App Settings（全域應用程式設定）] 區域中的齒輪圖示。<br>• 修改單一閘道登入工作階段的最大 **Login Lifetime**（登入存留時間）（預設值為 30 天）。在這段存留時間內，閘道只要在 **Inactivity Logout**（非使用狀態登出）時間內收到來自端點的 HIP 檢查，使用者即可保持登入。在此時間之後，登入工作階段自動結束。<br>• 設定提前通知使用者的時間量，以指出其應用程式工作階段由於登入存留時間到期而即將到期。預設值是 30 分鐘。可接受的範圍是 0-60 分鐘。<br>• 自訂逾時通知訊息。<br>• 修改 **Inactivity Logout**（非使用狀態登出）期間，以指定一個時間段，當閒置使用者達到該時間後將從 GlobalProtect 中登出。您可以強制執行安全性政策，在連線到 GlobalProtect 時監控來自端點的流量，以及設定較短的非使用狀態登出期間，以快速登出非作用中的 GlobalProtect 工作階段。如果在設定的時間段內，GlobalProtect 應用程式沒有透過 VPN 通道路由流 |

 ©2025 Palo Alto Networks, Inc.

| GlobalProtect 應用程式設定 | |
|---|---|
| | 量，或閘道未收到來自端點的 HIP 檢查，則使用者會登出 GlobalProtect。<br><br>預設值為 180 分鐘。可接受的範圍是 5-43200 分鐘。<br>• 設定提前通知使用者的時間量，以指出其應用程式工作階段由於非使用狀態而即將到期。預設值是 30 分鐘。可接受的範圍是 0-60 分鐘。<br>• 自訂非使用狀態通知訊息。<br>• 指定是否在管理員將一般使用者登出時通知他們，並設定顯示訊息。<br>• 按一下 **Save**（儲存）。 |
| 為驗證 **cookie** 強制執行來源 **IP** 位址 | 設定 VPN 連線設定和驗證 cookie 使用限制，以增強安全性態勢。<br>• 在 [GlobalProtect Setup（GlobalProtect 設定）] 頁面上，選取 [Global App Settings（全域應用程式設定）] 區域中的齒輪圖示。<br>• 設定 SSL VPN 通道的自動還原。<br><br>如果在 GlobalProtect 入口網站上啟用了 VPN 連線的自動還原，您可以透過選取 **Disable Automatic Restoration of SSL VPN**（停用 **SSL VPN** 的自動還原），為此閘道停用它。<br>• 為驗證 cookie 強制執行來源 IP 位址。<br><br>您可以設定 GlobalProtect 入口網站或閘道，以僅在端點的 IP 位址與為其發佈 cookie 的原始來源 IP 位址或特定網路 IP 位址範圍相符時，才從端點接收 cookie。您可使用 CIDR 子網路遮罩（例如 /24 或 /32）定義網路 IP 位址範圍。例如，如果驗證 cookie 最初發佈給公用來源 IP 位址為 201.109.11.10 的端點，且網路 IP 位址範圍的子網路遮罩設為 /24，驗證 cookie 隨後會在公共來源 IP 位址在 201.109.11.0/24 網路 IP 位址範圍內的端點上有效。<br><br>在 [Authentication Cookie Usage Restrictions（驗證 Cookie 使用限制）] 區段中，選取 **Restrict Authentication Cookie Usage (for Automatic Restoration of VPN tunnel or Authentication Override)**（限制驗證 **Cookie** 使用（用於自動還原 **VPN** 通道或驗證覆寫），然後設定下列其中一個條件：<br>• 如果您選取 **The original Source IP for which the authentication cookie was issued**（為其發佈驗證 **cookie** 的原始來源 **IP**），只有當嘗試使用 cookie 之端點的公用來源 IP 位址與最初為其發佈 cookie 之端點的公用來源 IP 位址相同時，驗證 cookie 才有效。 |

 ©2025 Palo Alto Networks, Inc.

| GlobalProtect 應用程式設定 | |
|---|---|
| | • 如果您選取 **The original Source IP network range**（原始來源 **IP** 網路範圍），只有當嘗試使用 cookie 之端點的公用來源 IP 位址在指定網路 IP 位址範圍內時，驗證 cookie 才有效。輸入來源 IPv4 網路遮罩或來源 IPv6 網路遮罩 以定義驗證 Cookie 有效的網路 IP 位址範圍的子網路遮罩（例如，32 或 128）。 |

# 提出票證要求以停用 GlobalProtect

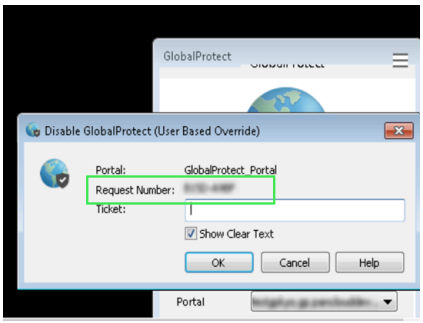
| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

您可以允許使用者建立票證，以停用 GlobalProtect，而不是直接讓使用者停用 GlobalProtect。然後，GlobalProtect 管理員可以決定是否允許每個特定使用者停用 GlobalProtect。

## 其運作方式為何

在您設定了此功能之後，以下是提出票證要求停用 GlobalProtect 的工作流程：

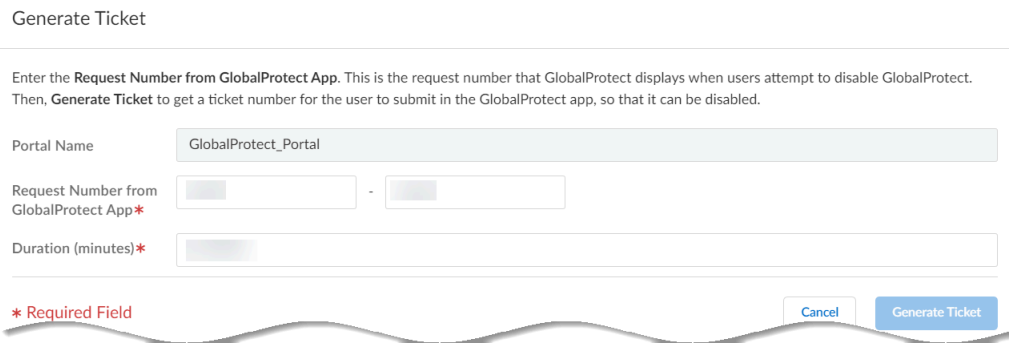
- 使用者嘗試在 GlobalProtect 應用程式中停用 GlobalProtect。GlobalProtect 會向使用者顯示要求號碼。



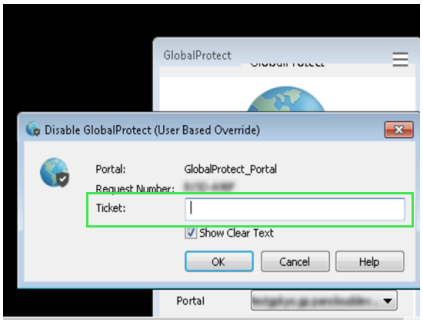

- 使用者與 GlobalProtect 管理員共用要求號碼。

 ©2025 Palo Alto Networks, Inc.

- GlobalProtect 管理員會登入 Prisma Access (Managed by Strata Cloud Manager) 並使用要求號碼產生票證。




- GlobalProtect 管理員與使用者共用票證號碼。使用者會將票證號碼輸入至應用程式，以停用 GlobalProtect。




設定它

- Strata Cloud Manager
- Panorama

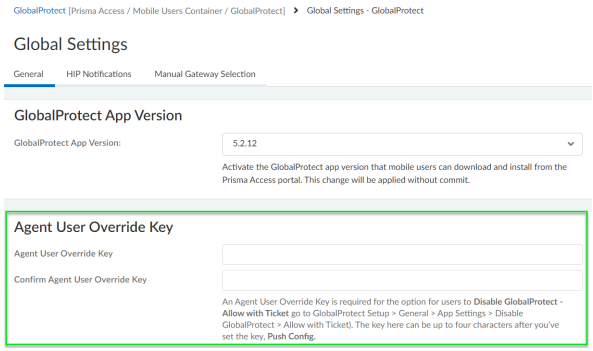
## 提出票證要求以停用 GlobalProtect (Strata Cloud Manager)


©2025 Palo Alto Networks, Inc.

**STEP 1 |** 設定代理程式覆寫金鑰

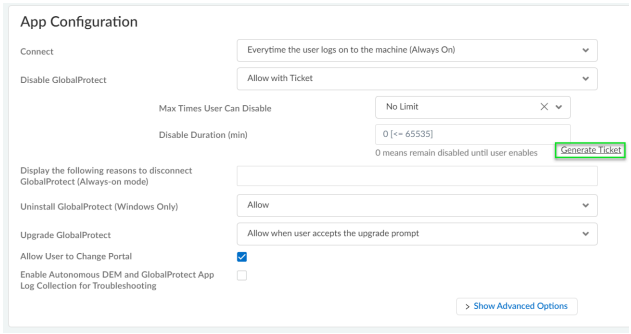
在可以啟用選項，讓使用者提出票證要求停用 GlobalProtect 之前，您首先需要設定代理程式使用者覆寫金鑰。

前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **GlobalProtect** > **GlobalProtect App**（**GlobalProtect** 應用程式） > **Global App Settings**（全域應用程式設定），然後輸入四字元金鑰，以設定 **Agent Override Key**（代理程式覆寫金鑰）。




**STEP 2 |** 允許使用票證停用 GlobalProtect

前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **GlobalProtect** > **GlobalProtect App**（**GlobalProtect** 應用程式） > **App Settings**（應用程式設定） > **App Configuration**（應用程式設定） > **Disable GlobalProtect**（停用 **GlobalProtect**），然後將選項設定為 **Allow with Ticket**（透過票證允許）。

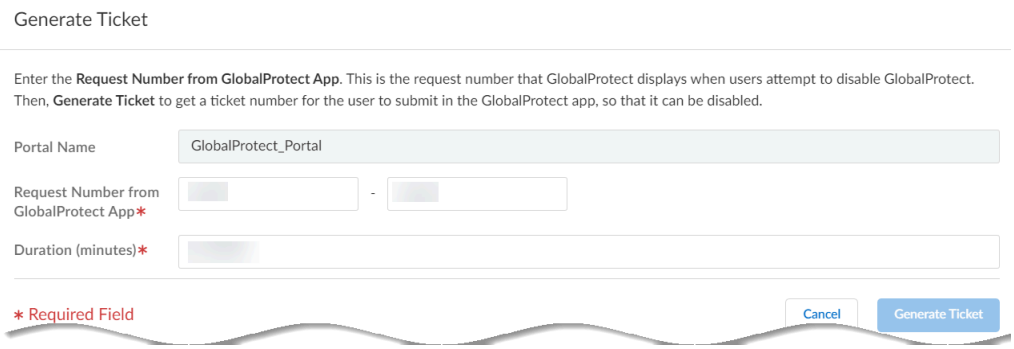



 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 產生票證

在設定 **Agent Override Key**（代理程式覆寫金鑰），並將選項設定為 **Allow with Ticket**（透過票證允許）之後，您將能夠 **Generate Ticket**（產生票證）。

當使用者嘗試在應用程式中停用 GlobalProtect 時，GlobalProtect 將向他們顯示要求編號。請在這裡提交該要求編號以產生票證，讓該使用者停用 GlobalProtect。

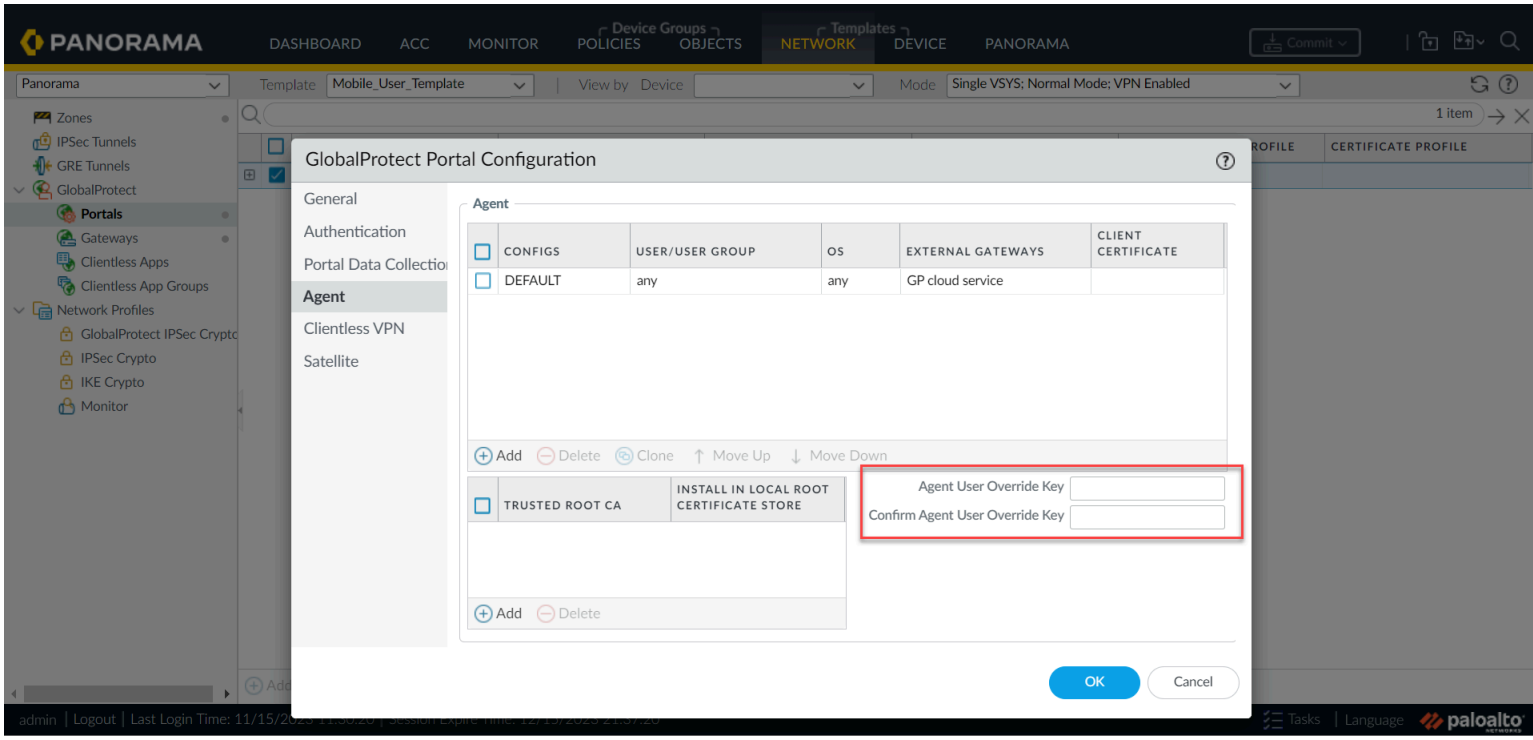



## 提出票證要求以停用 GlobalProtect (Panorama)

**STEP 1 |** 設定代理程式覆寫金鑰

在可以啟用選項，讓使用者提出票證要求停用 GlobalProtect 之前，您首先需要設定代理程式使用者覆寫金鑰。

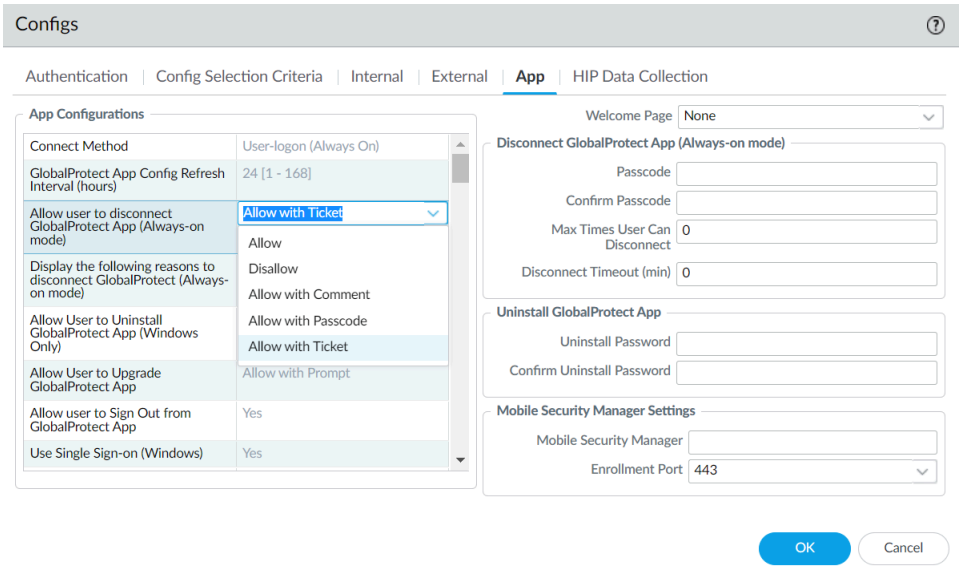
前往 **Network**（網路） > **GlobalProtect** > **Portals**（入口網站），然後選取要設定覆寫金鑰的連線名稱。選取 **Agent**（代理程式），然後輸入金鑰以設定 **Agent Override Key**（代理程式覆寫金鑰）。




 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 允許使用票證停用 GlobalProtect

前往 **Network**（網路） > **GlobalProtect** > **Portals**（入口網站），然後選取您想要允許使用者與其中斷連線的連線名稱。選取 **Agent**（代理程式）、選擇 **Config**（設定）、選取 **App**（應用程式） > **App Configurations**（應用程式設定） > **Allow user to disconnect GlobalProtect App (Always-on mode)**（允許使用者中斷連線 **GlobalProtect** 應用程式（一律開啟模式）），然後將選項設定為 **Allow with Ticket**（透過票證允許）。

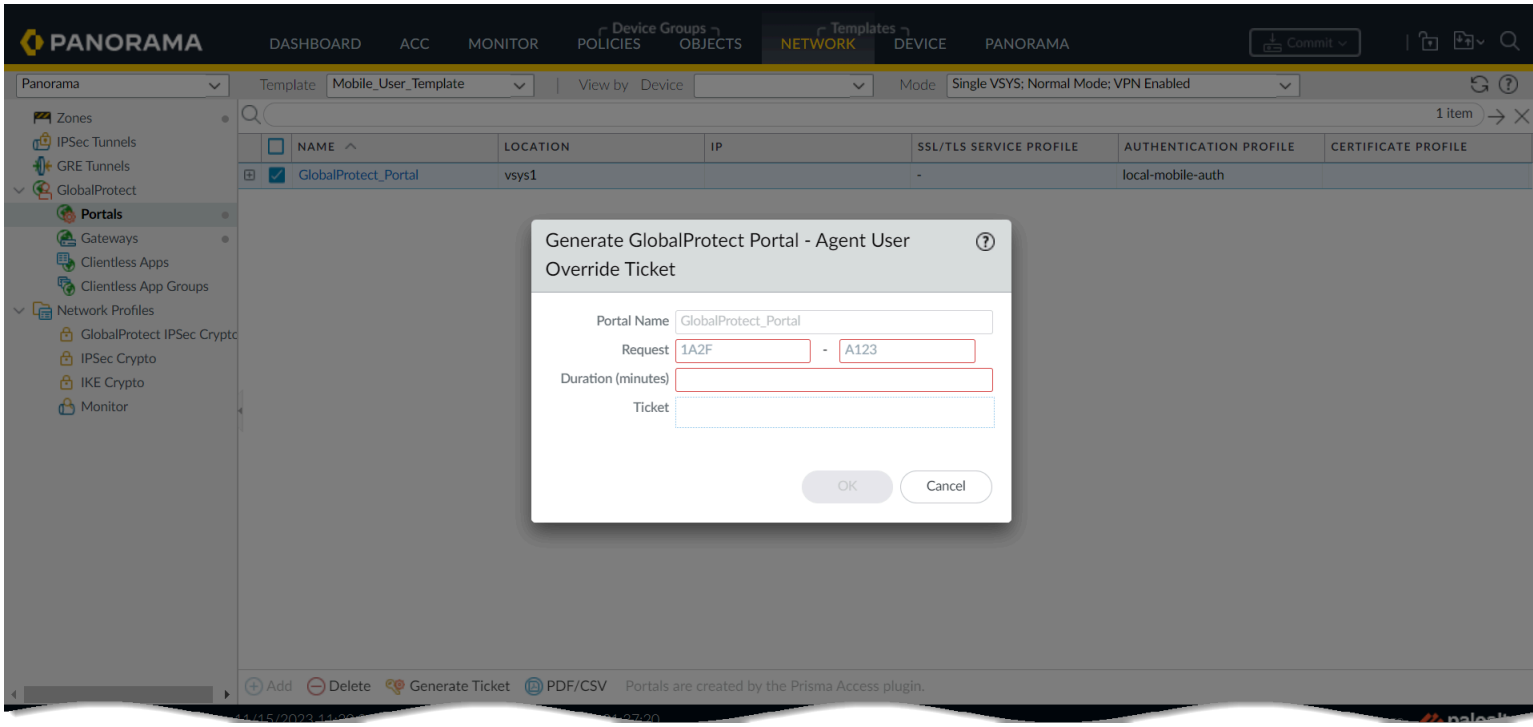



 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 產生票證

在設定 **Agent Override Key**（代理程式覆寫金鑰），並將選項設定為 **Allow with Ticket**（透過票證允許）之後，您將能夠 **Generate Ticket**（產生票證）。

當使用者嘗試在應用程式中停用 GlobalProtect 時，GlobalProtect 將向他們顯示要求編號。請在這裡提交該要求編號以產生票證，讓該使用者停用 GlobalProtect。




# GlobalProtect 預先登入

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 授權<br>❑ 管理員存取端點以安裝電腦憑證<br>❑ 已在端點上部署的受信任 PKI 憑證 |

預先登入是在使用者登入之前建立 VPN 通道的連線方法。預先登入的目的是驗證端點，而不是使用者，並讓網域指令碼或其他工作只要端點一開啟電源就會執行。電腦憑證讓端點能夠建立通向 GlobalProtect 閘道的 VPN 通道。IT 管理員的普通做法是在使用者端點預備階段安裝電腦憑證。預先登入 VPN 通道會使用通用的預先登入使用者名稱，因為使用者尚未登入。若要允許端點存取資源，您必須建立安全性政策規則，比對預先登入使用者。這些政策規則應僅允許存取基本服務以啟動系統，例如，DHCP、DNS、特定的 Active Directory 服務、防毒或其他更新服務。在使用者對閘道進行驗證之後，GlobalProtect 應用程式會將 VPN 通道重新指派給該使用者。Prisma Access 上的 IP 位址對應會從預先登入端點變更為已驗證的使用者。

 ©2025 Palo Alto Networks, Inc.

用於預先登入驗證的憑證會常駐在端點的個人憑證存放區中。使用受信任的第三方 CA、自我簽署 CA 或內部 PKI CA 以發出電腦憑證。您需要將電腦憑證設定為驗證方法，以在登入 Prisma Access 之前從端點建立通道，然後建立一個憑證設定檔，其中包含預先登入 CA 憑證。

- Strata Cloud Manager
- Panorama

## GlobalProtect 預先登入 (Strata Cloud Manager)

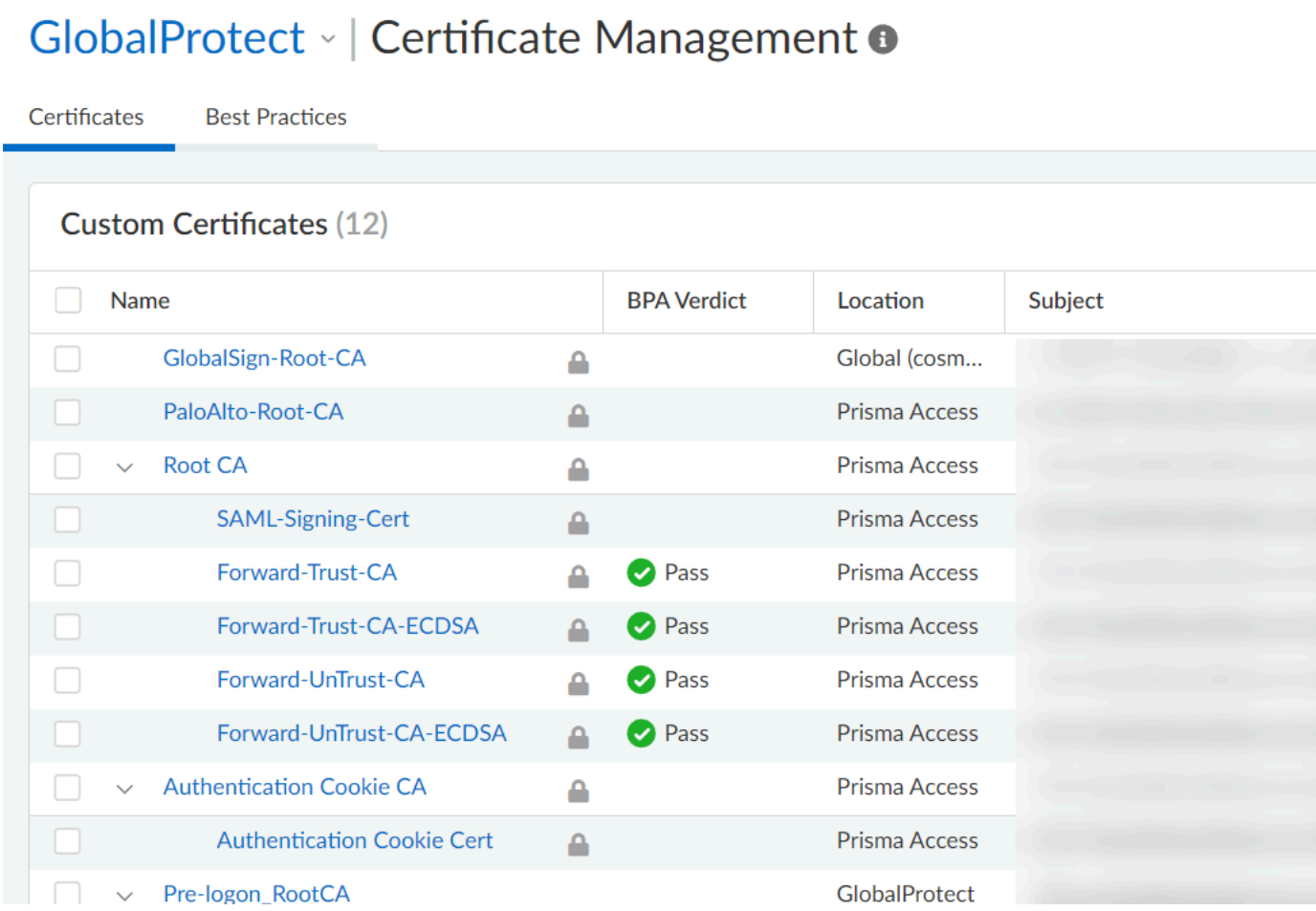
匯入第三方根 **CA** 憑證

使用電腦憑證作為驗證方法，在登入 Prisma Access 之前從端點建立通道。

**STEP 1 |** 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（物件） > **Certificate Management**（憑證管理）。選取**Prisma Access** 設定範圍

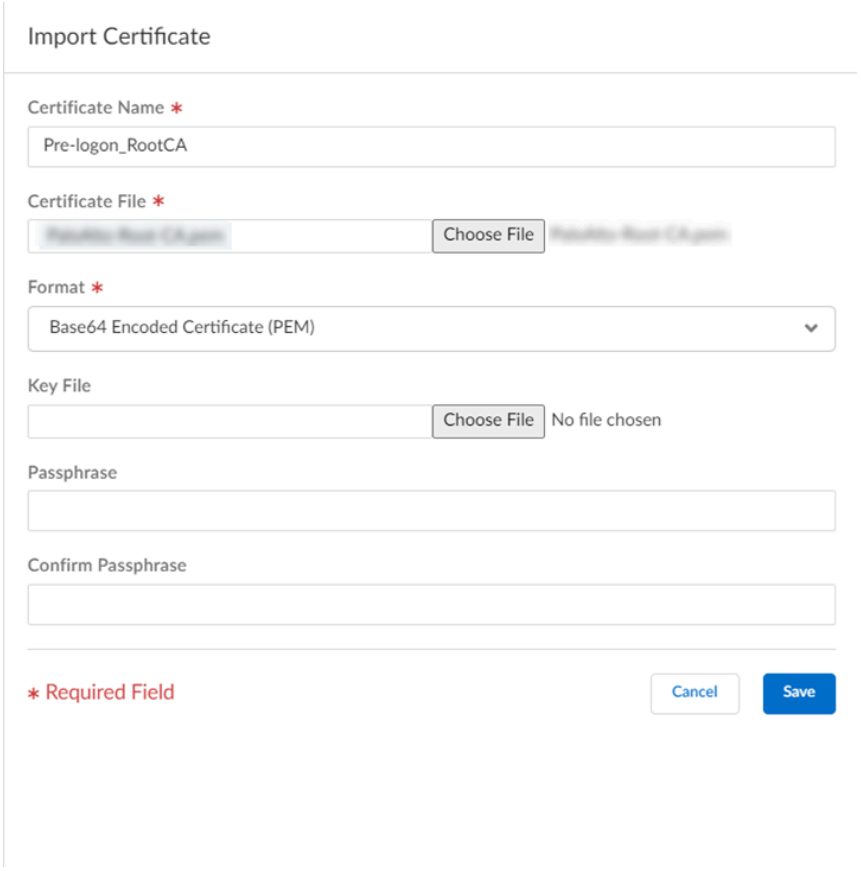
確保您正在匯入 GlobalProtect 行動使用者的憑證。

**STEP 2 |** **Import**（匯入）自訂憑證。




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 輸入值，然後 **Save**（儲存）憑證設定。




建立預先登入憑證設定檔

建立憑證設定檔並包含自我簽署根 CA。此 CA 會在預先登入期間驗證 GlobalProtect 行動使用者的電腦憑證。

**STEP 1 |** 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW 和 Prisma Access**） > **Objects**（物件） > **Certificate Management**（憑證管理）。選取**Prisma Access** 設定範圍

**STEP 2 |** **Add Profile**（新增設定檔）。

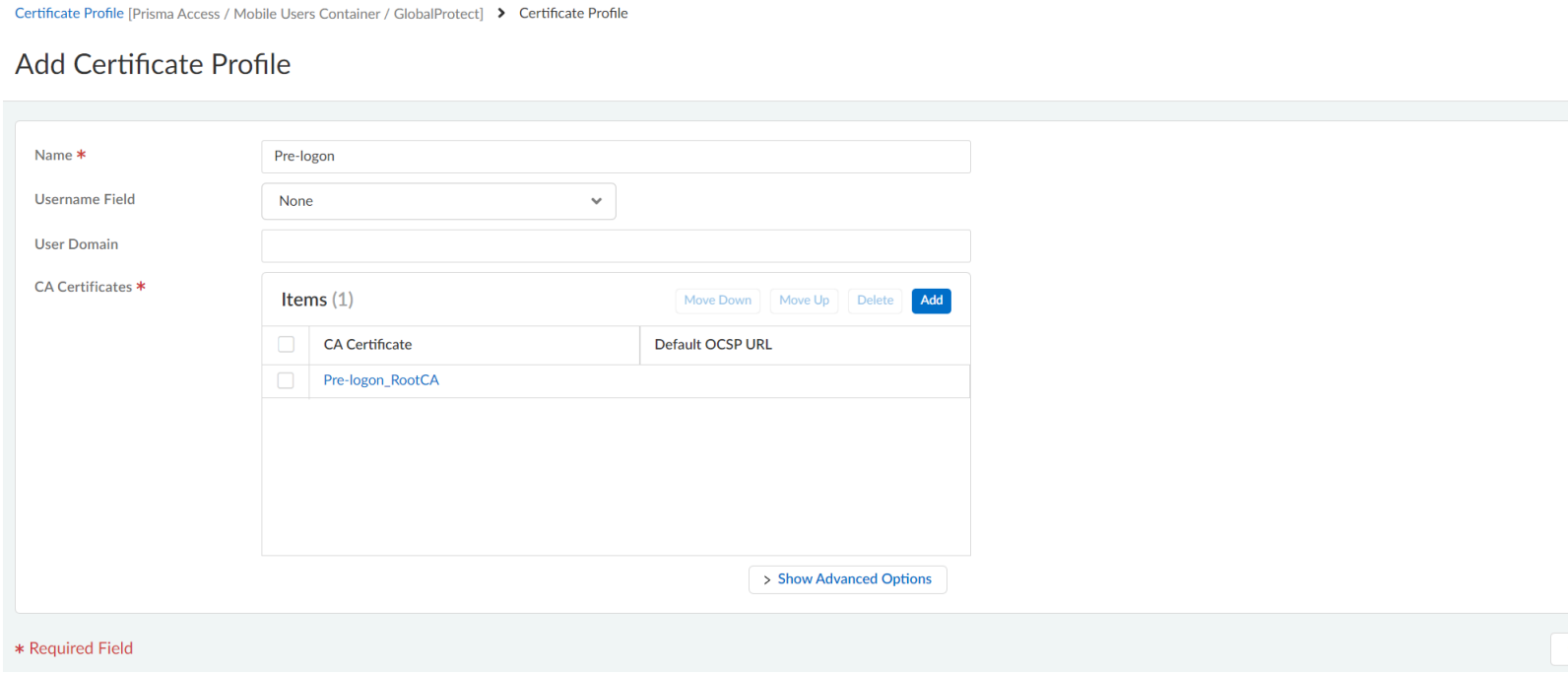

©2025 Palo Alto Networks, Inc.

**STEP 3 |** 輸入值。

1. 確保 **Username Field**（使用者名稱欄位）為 **None**（無），以防止憑證對應到使用者。

   如果您透過任何驗證方法或步驟 2 中提到的用戶端憑證來驗證您的憑證，則 ***Username Field***（使用者欄位）不能為 ***None***（無）。

2. **Add**（新增）您在步驟 1 中匯入的根預先登入 CA 憑證 。
3. **Save**（儲存）憑證設定檔設定。




設定 **GlobalProtect** 入口網站進行預先登入

設定 GlobalProtect 入口網站，以使用電腦憑證驗證連線。

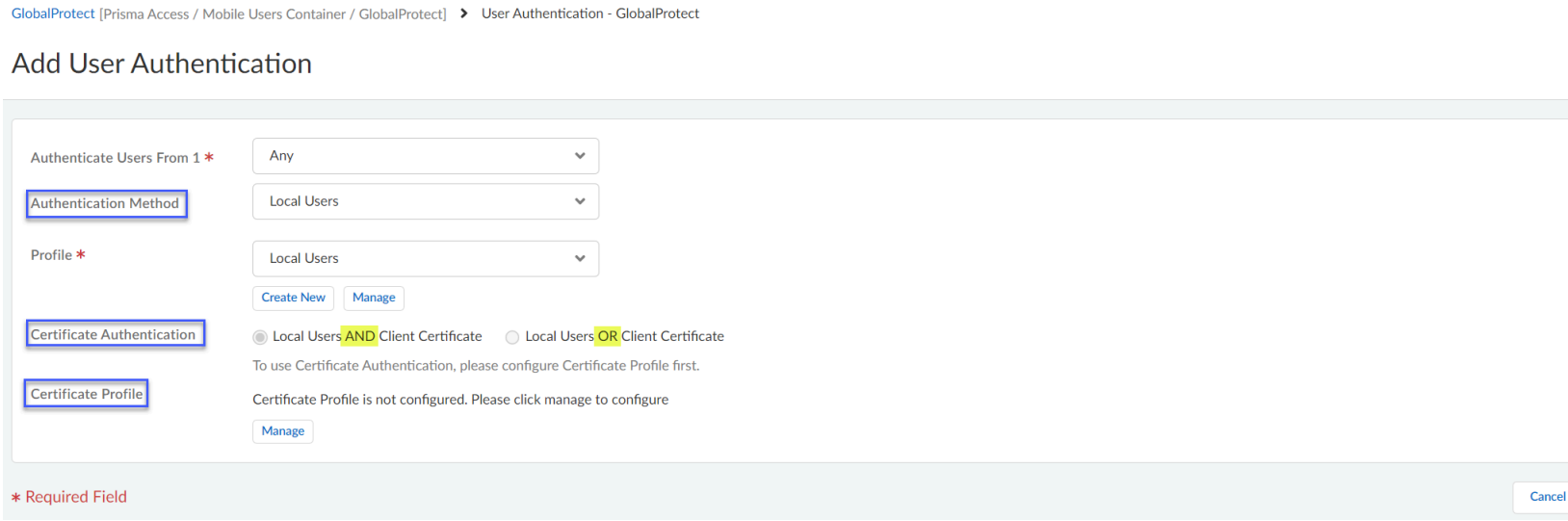
**STEP 1 |** 選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **GlobalProtect** > **Infrastructure**（基礎結構）。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 編輯使用者驗證設定。

選取 GlobalProtect 支援的驗證方法、您建立的 預先登入憑證設定檔，以及憑證驗證。

選擇 *GlobalProtect* 支援的任何憑證驗證。

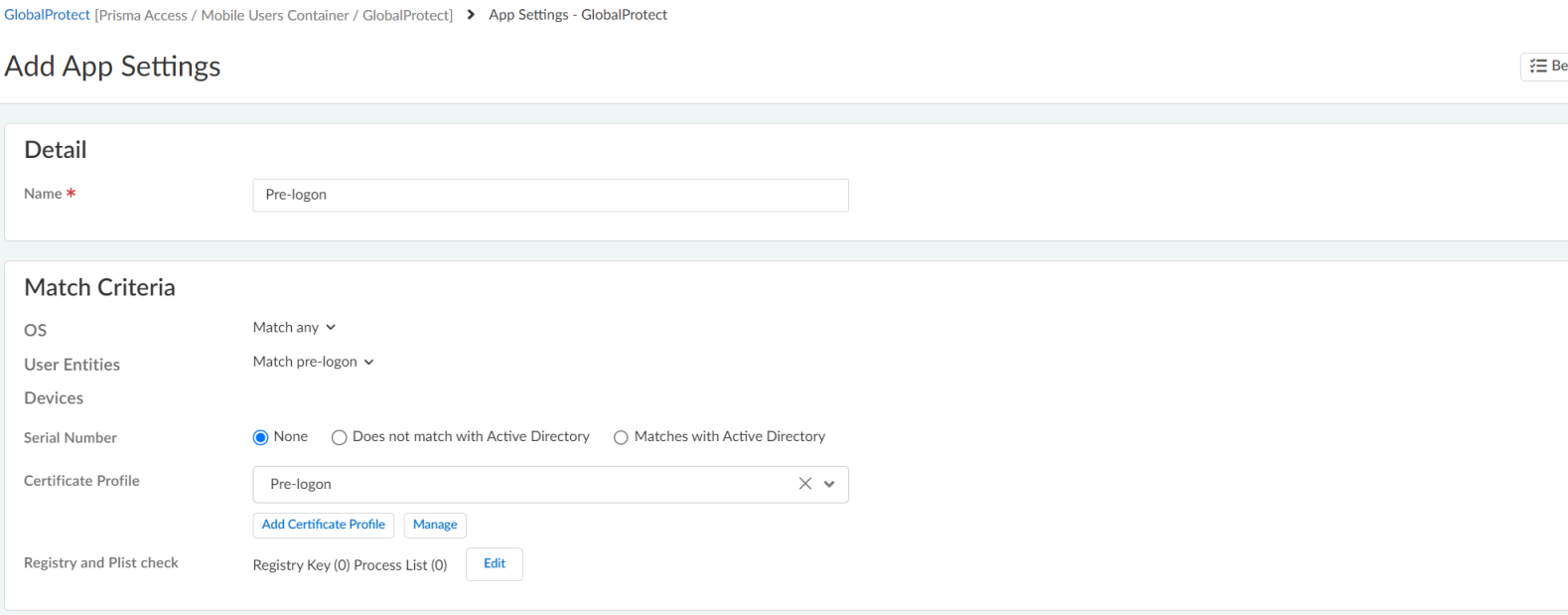



 ©2025 Palo Alto Networks, Inc.

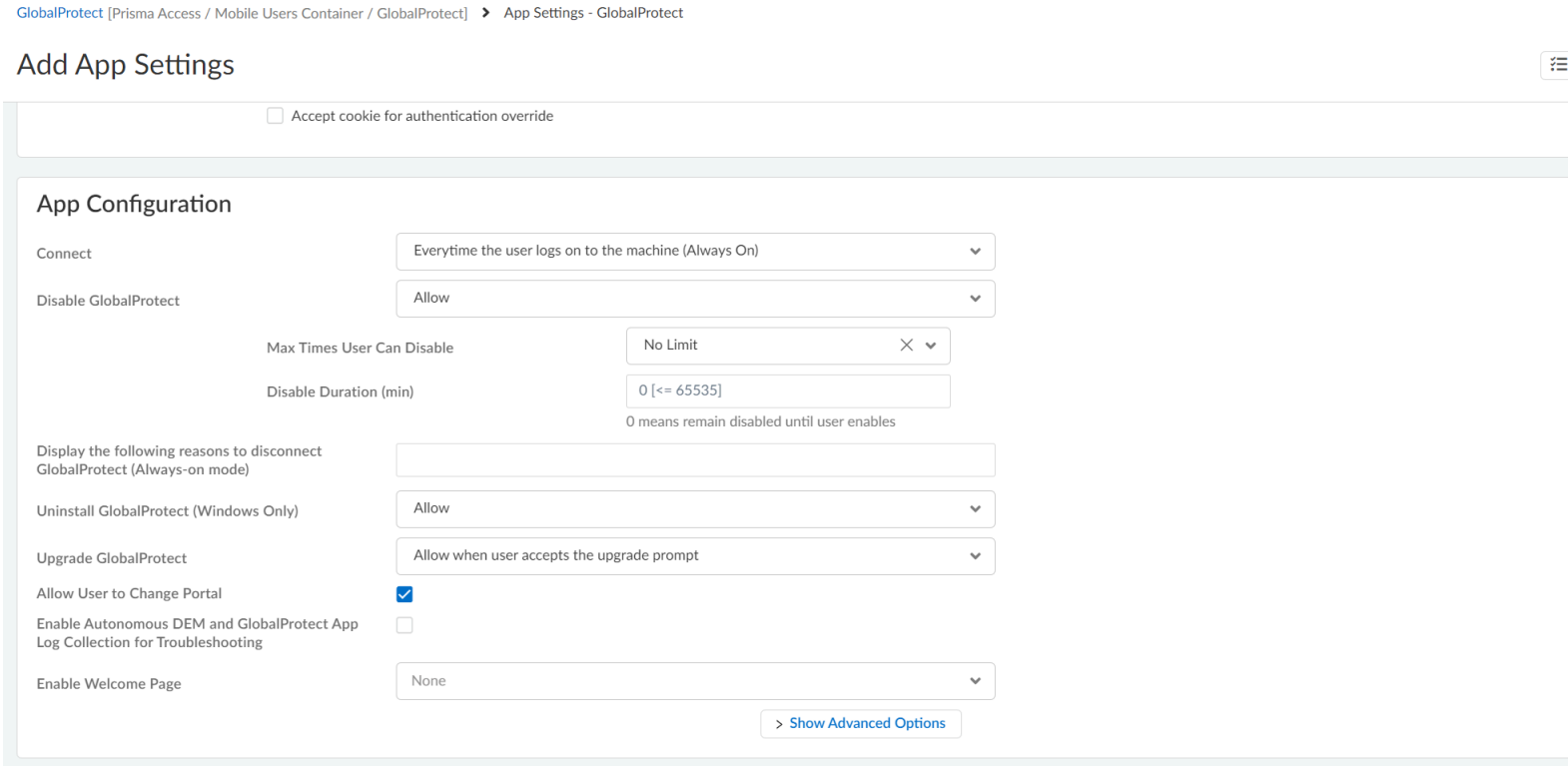
**STEP 3 |** 設定 GlobalProtect 應用程式設定以比對預先登入準則。

1. 導覽至 **GlobalProtect App**（**GlobalProtect** 應用程式）頁籤。
2. 新增應用程式設定。

輸入值時，請確保 ***Match pre-logon***（比對預先登入）使用者實體和預先登入憑證設定檔。

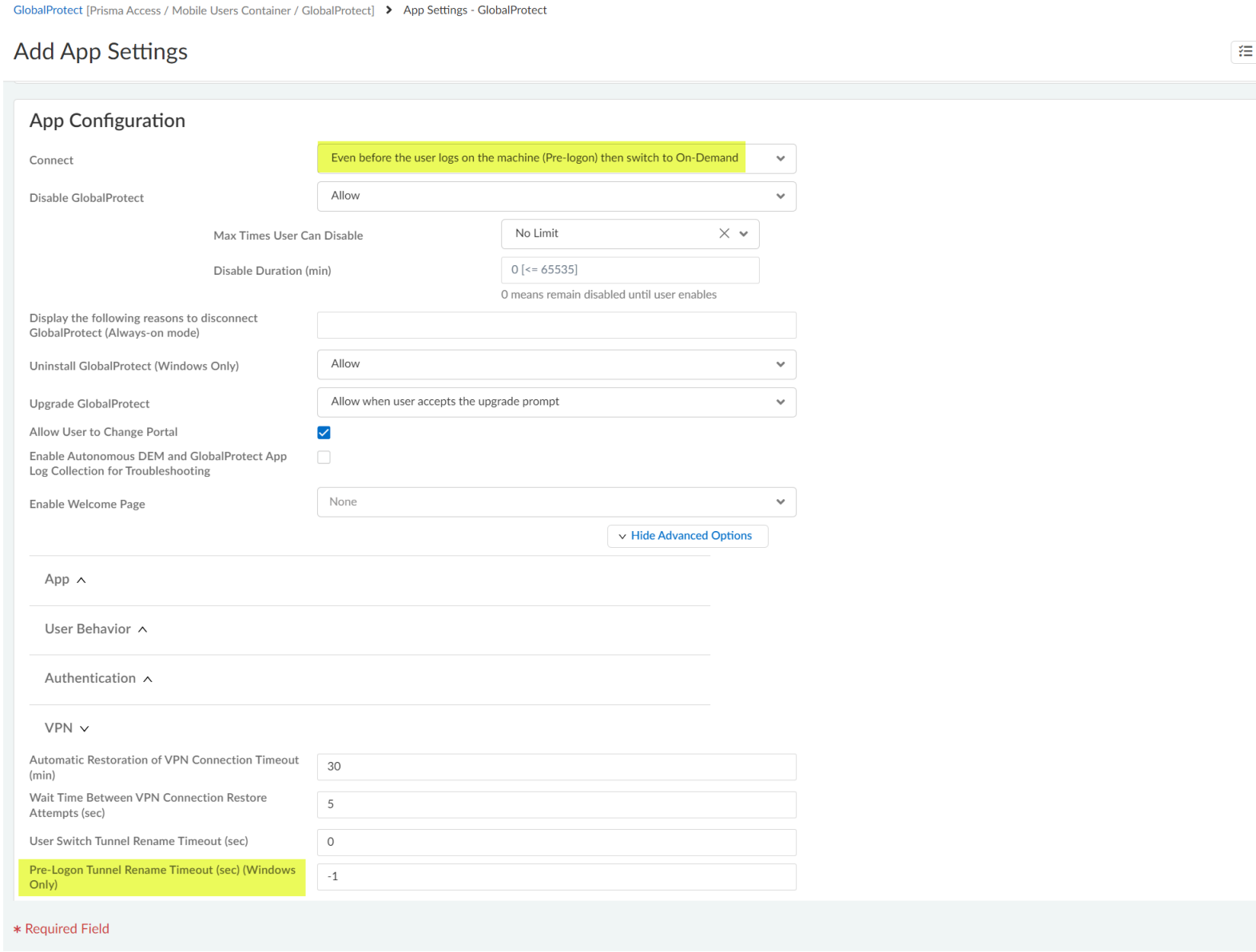



- 選取預先登入連線方法。




 ©2025 Palo Alto Networks, Inc.

- 如果您選取 **Even before the user logs on the machine (Pre-logon) then switch to On-Demand**（甚至在使用者登入電腦（預先登入）之前，然後切換到隨選），請將 **Pre-logon Tunnel Rename Timeout**（預先登入通道重新命名逾時）的值設定為 **–1**。檢視 VPN 進階選項以編輯此欄位。




3. 將預先登入應用程式設定移至其他應用程式設定之上。
4. 編輯已驗證使用者的所有其他應用程式設定。

   更新連線方法和憑證設定檔。

**STEP 4 |** 將變更推送到 Prisma Access。

安裝電腦憑證—**Windows**

在端點安裝用於驗證的電腦憑證。

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** 以 **Binary Encoded Certificate (DER)**（二進位編碼憑證 **(DER)**）格式從您的 PKI 匯出自我簽署根 CA 憑證。

**STEP 2 |** 將憑證檔案傳輸到 Windows 電腦。

**STEP 3 |** 在本機電腦的 **Trusted Root Certification Authorities**（受信任的根憑證授權單位）存放區中安裝根預先登入 CA 憑證。

**STEP 4 |** 在本機電腦存放區位置安裝預先登入電腦憑證。

**STEP 5 |** 繼續安裝、出現提示時輸入密碼，然後完成安裝。

**STEP 6 |** 連線到 GlobalProtect 入口網站，並刪除主機中的所有 Cookie。

**STEP 7 |** （選用）登出您的電腦，並檢視 GlobalProtect 日誌以驗證預先登入連線。

## GlobalProtect 預先登入 (Panorama)

設定預先登入憑證和設定檔

將電腦憑證設定為驗證方法，以在登入 Prisma Access 之前從端點建立通道，然後建立一個憑證設定檔，其中包含預先登入 CA 憑證。

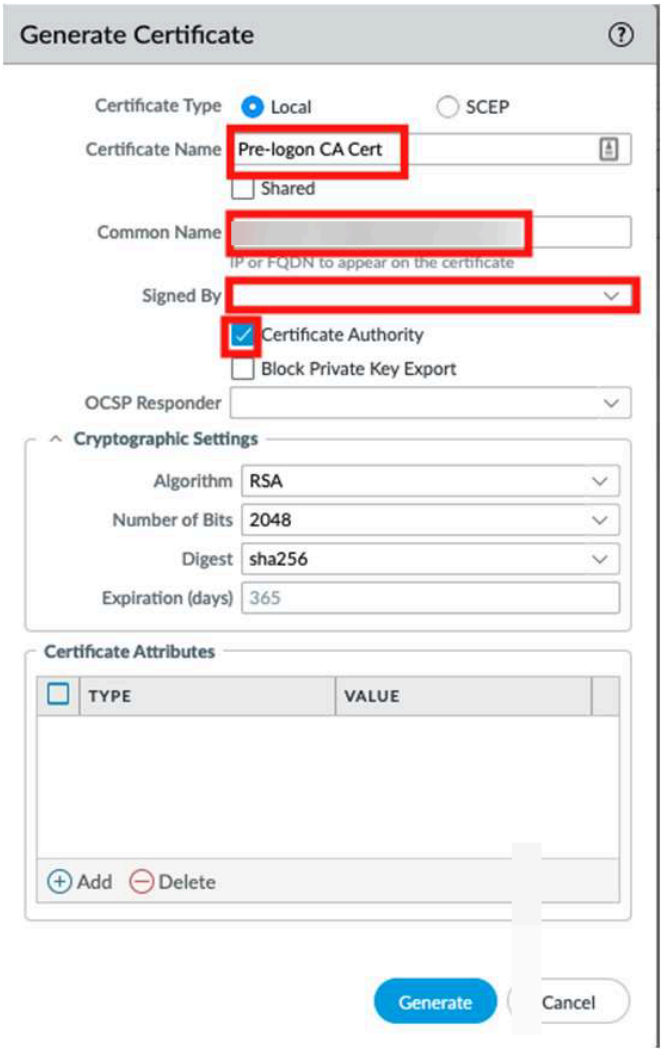
 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** 設定自我簽署 CA，並使用它在行動使用者範本中產生電腦憑證。前往 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證）。

請確定您在 **Mobile_User_Template** 中，且 **Location**（位置）設定為 **Shared**（共用）。

1. 命名憑證；例如，**Pre-logon CA Cert**。
2. 輸入 **Common Name**（通用名稱）。

   通用名稱 (CN) 是您想要使用憑證保護的網域名稱，例如 www.yourdomainname.com,。
3. 將 **Signed By**（簽署者）欄位保留空白，然後按一下 **Certificate Authority**（憑證授權單位）核取方塊。
4. **Generate**（產生）憑證，用於預先登入連線。

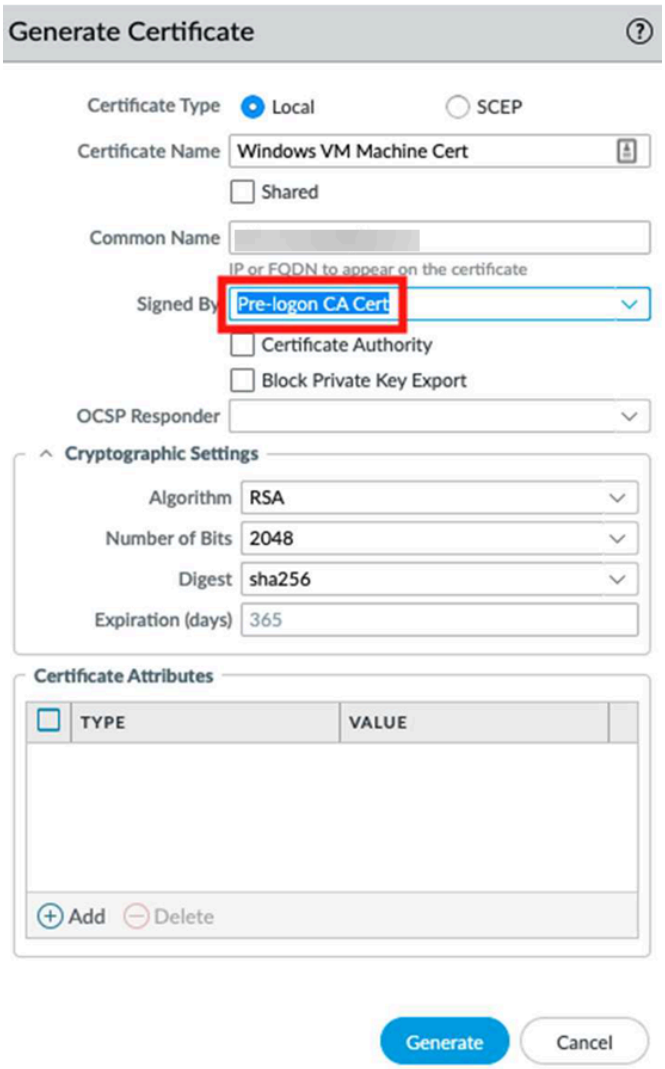



 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 在設定自我簽署 CA 之後，產生電腦憑證。

1. 輸入 **Certificate Name**（憑證名稱）和 **Common Name**（通用名稱）。
2. 在 **Signed By**（簽署者）下拉式清單中，選取您在步驟 1 中建立的 **Pre-logon CA Cert**（預先登入 **CA** 憑證）。
3. **Generate**（產生）您稍後在 Windows 電腦上安裝的 **Windows VM** 電腦憑證。

   此憑證是預先登入 CA 的子項。

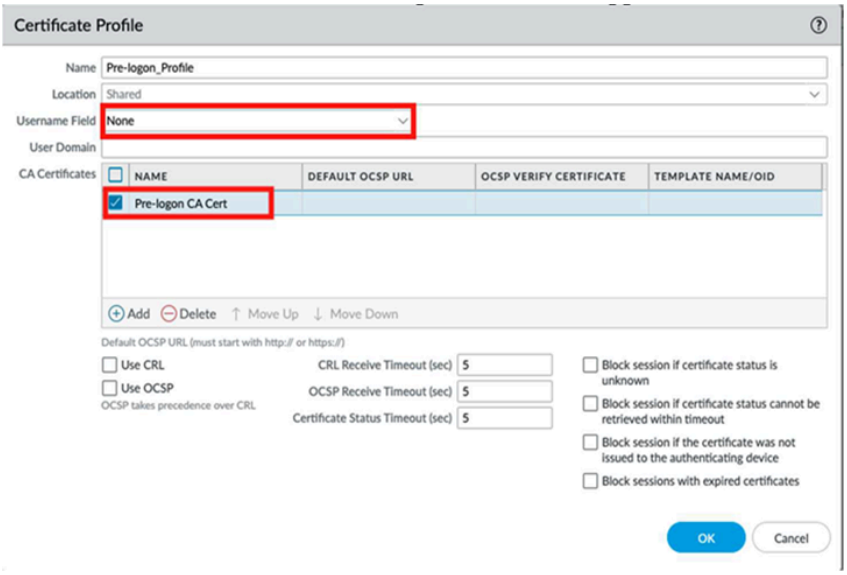



**STEP 3 |** 若要建立一個包含預先登入 CA 憑證的憑證設定檔，請前往 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificate Profile**（憑證設定檔）。

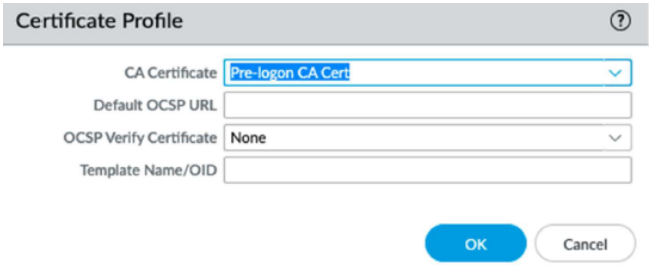
使用此 CA 來驗證 GlobalProtect 用戶端在預先登入通道初始化期間所呈現的電腦憑證。


©2025 Palo Alto Networks, Inc.

**STEP 4 |** 建立並命名設定檔。確定 **Username Field**（使用者名稱欄位）為 **None**（無），以防止憑證對應至使用者。




**STEP 5 |** 在 **CA Certificates**（**CA** 憑證）下，選取 **Add**（新增），然後從下拉式清單中選取 **Pre-logon CA Cert**（預先登入 **CA** 憑證）。




**STEP 6 |** 選取 **OK**（確定），然後再次選取 **OK**（確定）。

## 設定 GlobalProtect 入口網站進行預先登入

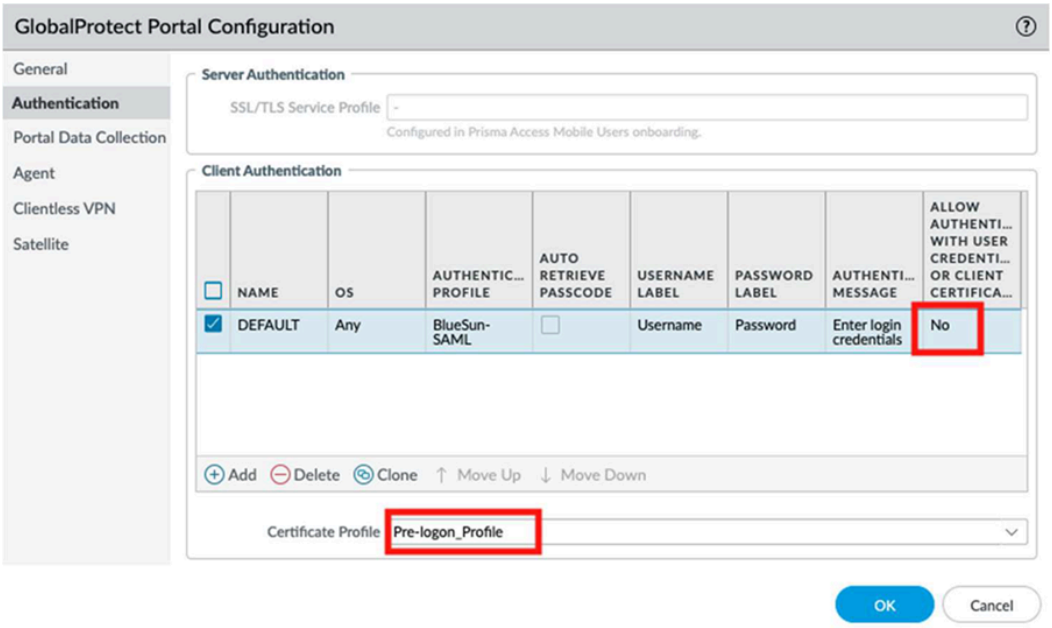
設定 GlobalProtect 入口網站，以使用電腦憑證驗證連線。

**STEP 1 |** 前往 **Network**（網路） > **GlobalProtect** > **Portals**（入口網站） > **GlobalProtect_Portal** > **Authentication**（驗證）。

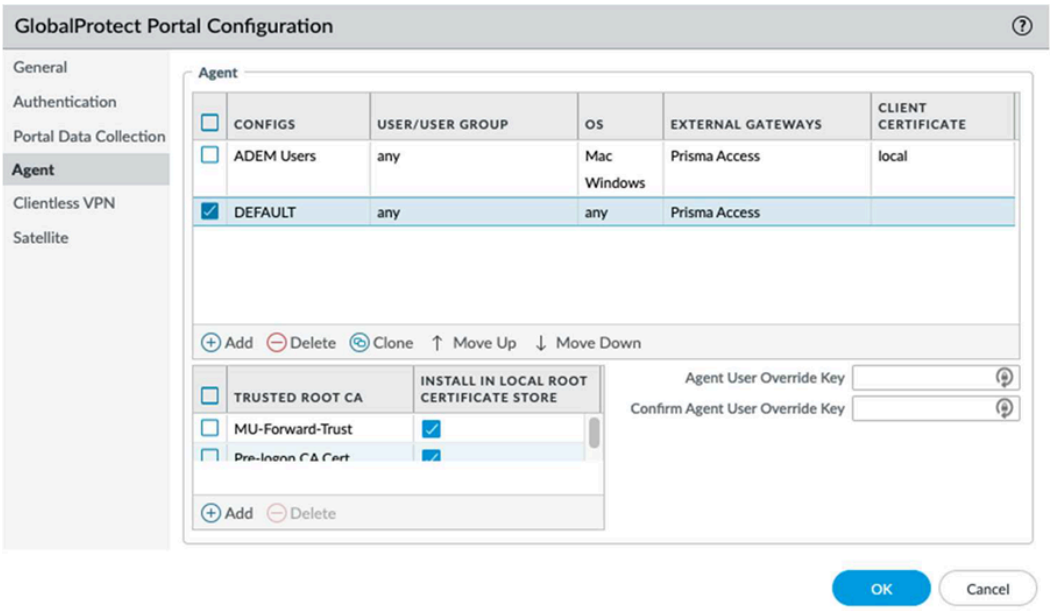
**STEP 2 |** 在 **Allow Authentication with User Credentials OR Client Certificate**（允許使用使用者認證或用戶端憑證進行驗證）下，選取 **No**（否），僅強制執行憑證型驗證。

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 對於 **Certificate Profile**（憑證設定檔），選取您建立的 **Pre-logon_Profile**，然後按一下 **OK**（確定）。



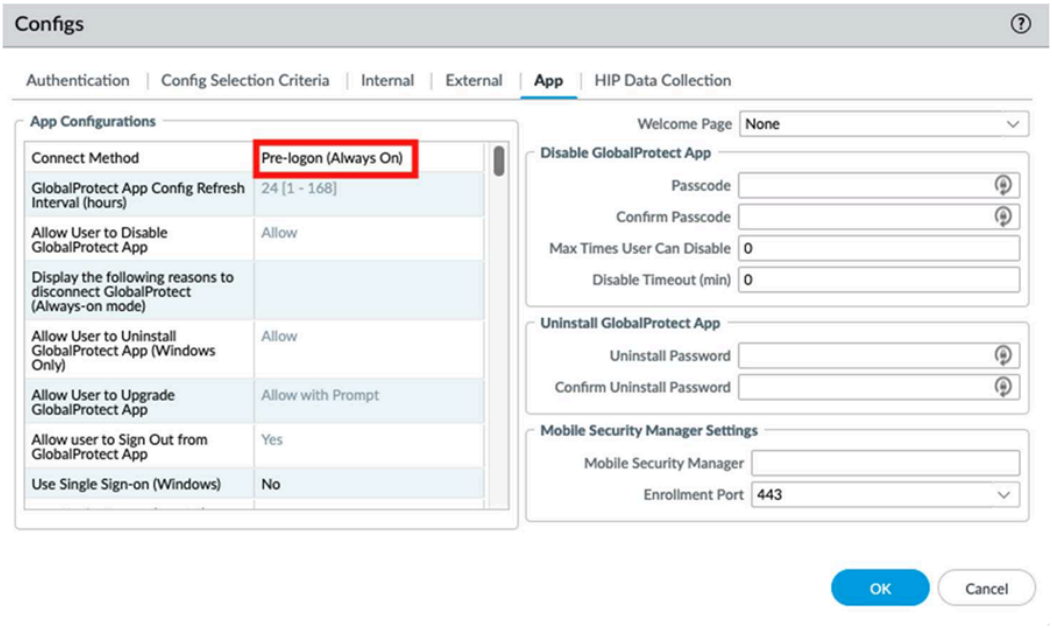

**STEP 4 |** 選取 **Agent**（代理程式），然後開啟已驗證使用者的代理程式設定。




**STEP 5 |** 選取 **App**（應用程式）頁籤。


©2025 Palo Alto Networks, Inc.

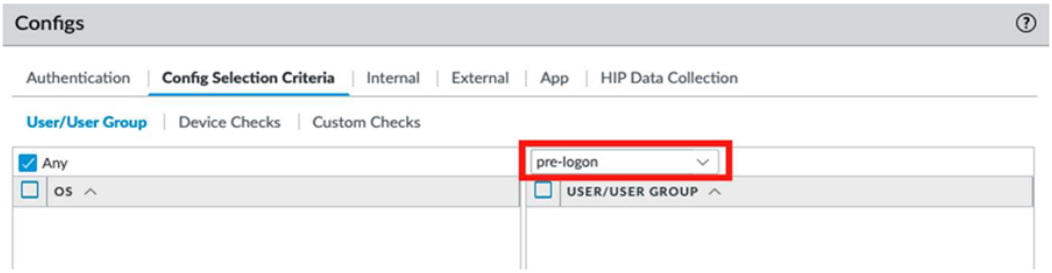
**STEP 6 |** 選取 **Pre-logon (Always On)**（預先登入（始終開啟））， 然後選取 **OK**（確定)返回代理程式區域。




**STEP 7 |** 在代理程式區域中， **Clone**（複製）預設設定。將設定名稱變更為 **Pre-logon**， 以比對連線方法進行電腦憑證驗證。

**STEP 8 |** 選取新複製的代理程式設定。

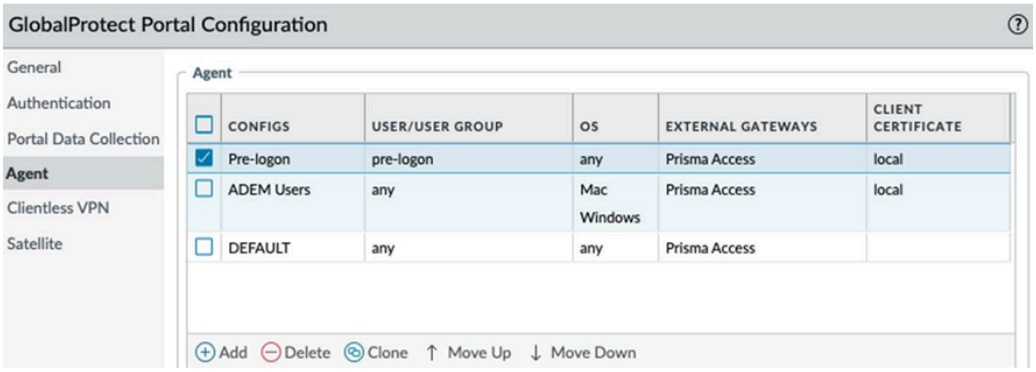
**STEP 9 |** 選取 **Config Selection Criteria**（設定選取條件)。在 **User/User Group**（使用者/使用者群組）設定下， 從 **USER/USER Group**（使用者/使用者群組）設定方塊上方的下拉式清單中選取 **pre-logon**（預先登入）， 並確定設定已設為 **Any**（任何）。




**STEP 10 |** 視需要設定應用程式設定， 然後選取 **OK**（確定）。確定您同時為預先登入和目前設定選取預先登入連線方法。


©2025 Palo Alto Networks, Inc.

**STEP 11 |** 將預先登入代理程式設定移至 **CONFIGS** 清單頂部，以確保它首先與預先登入條件進行比對。




**STEP 12 |** 按一下確定儲存入口網站設定。

設定 **Prisma Access GlobalProtect** 閘道

在 Panorama Managed Prisma Access 中設定 GlobalProtect 閘道。

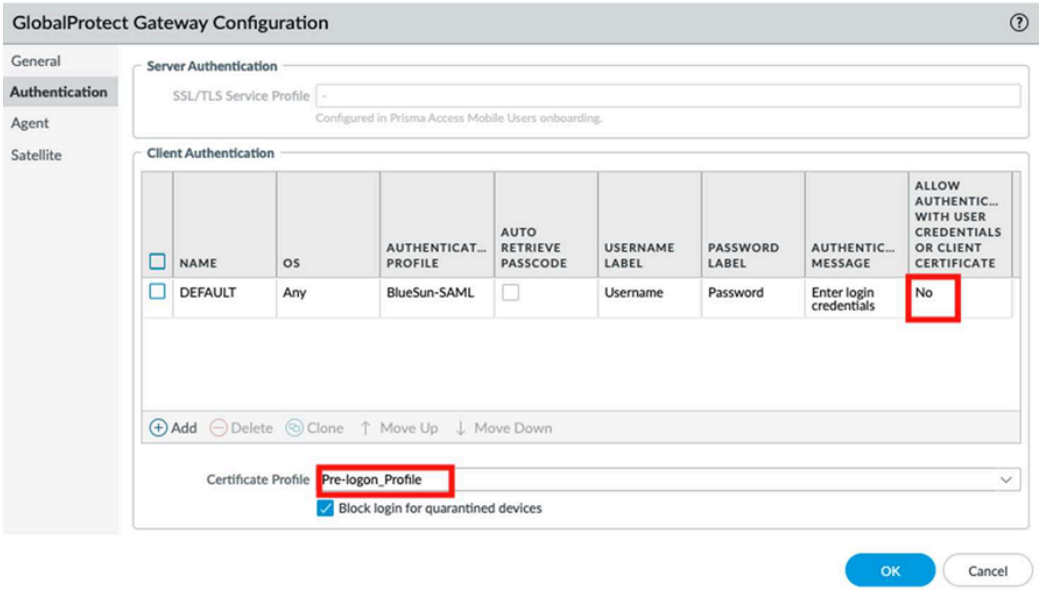
此設定僅強制執行憑證型驗證。

**STEP 1 |** 前往 **Network**（網路） > **GlobalProtect** > **Gateways**（閘道） > **GlobalProtect_External_Gateway** > **Authentication**（驗證）。

**STEP 2 |** 選取 **Default**（預設）驗證方法。

如果您已設定用戶端驗證（例如 SAML），請選取此驗證，而不是 **Default**（預設）。

**STEP 3 |** 在 **Allow Authentication with User Credentials or Client Certificate**（允許使用使用者認證或用戶端憑證進行驗證）下，選取 **No**（否），然後選取 **OK**（確定），以儲存設定。



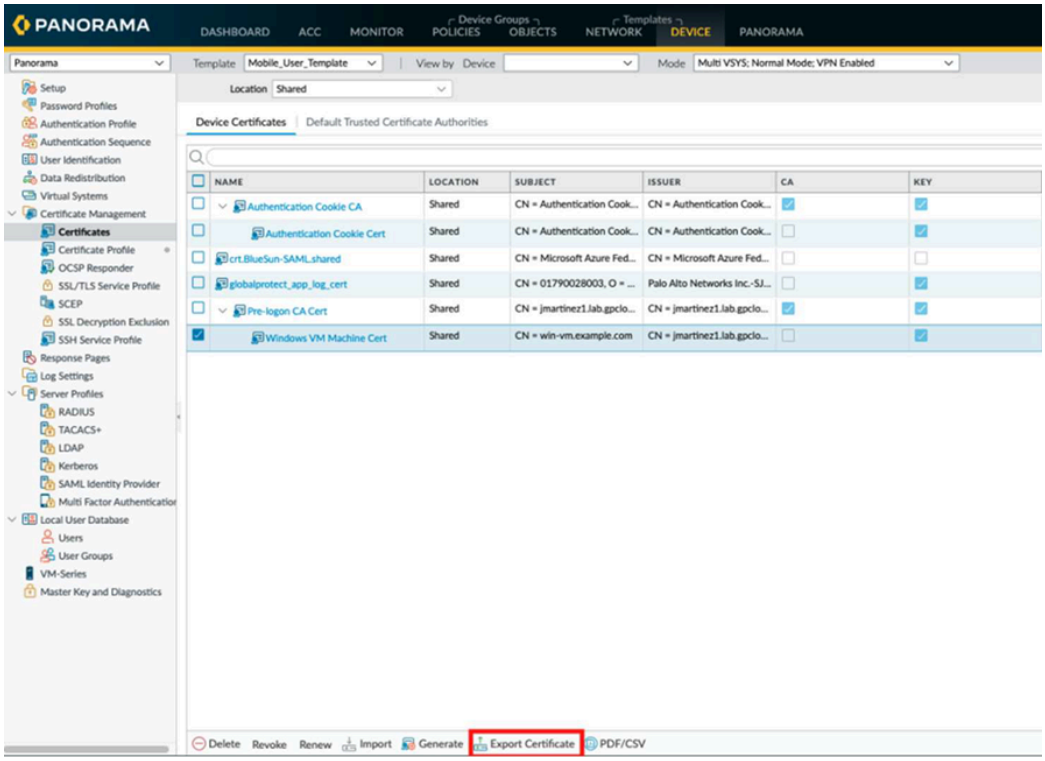

 ©2025 Palo Alto Networks, Inc.

安裝電腦憑證—**Windows**

在行動使用者用於驗證的端點上安裝電腦憑證。

**STEP 1 |** 前往 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證）。

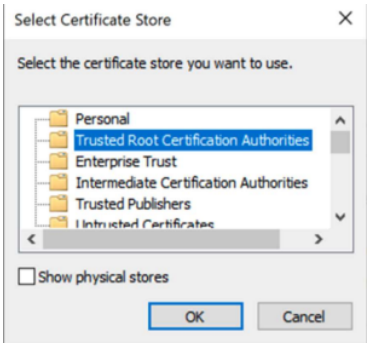
**STEP 2 |** 確定您仍在 Mobile_User_Template 中。選取先前建立的 **Windows VM Machine Cert**（**Windows VM** 電腦憑證），然後選取 **Export Certificate**（匯出憑證），將其下載為具有複雜密碼的 PKCS12 檔案。




**STEP 3 |** 將預先登入 CA 憑證匯出為 base64 編碼憑證。

**STEP 4 |** 將憑證檔案傳輸到 Windows 電腦。

**STEP 5 |** 在本機電腦的 **Trusted Root Certification Authorities**（受信任的根憑證授權單位）存放區中安裝根預先登入 CA 憑證。




**STEP 6 |** 在本機電腦存放區位置安裝預先登入電腦憑證。完成權限，然後選取 **Next**（下一步）以繼續安裝。


©2025 Palo Alto Networks, Inc.

**STEP 7 |** 驗證憑證的檔案名稱，然後選取 **Next**（下一步）。

**STEP 8 |** 輸入密碼，這是您從 Panorama 匯出憑證期間使用的複雜密碼，然後選取 **Next**（下一步）。

**STEP 9 |** 在 **Certificate Store**（憑證存放區）對話方塊中，選取 **Place all certificates in the following store**（將所有憑證放置在下列存放區中），然後選取 **Browse**（瀏覽）。

**STEP 10 |** 選取要安裝電腦憑證的 **Personal folder**（個人資料夾），然後選取 **OK**（確定）。

**STEP 11 |** 選取 **Next**（下一步）以繼續安裝。

**STEP 12 |** 連線到 GlobalProtect 入口網站，並刪除主機中的所有 Cookie。

**STEP 13 |** （選用）登出您的電腦，並檢視 GlobalProtect 日誌以驗證預先登入連線。

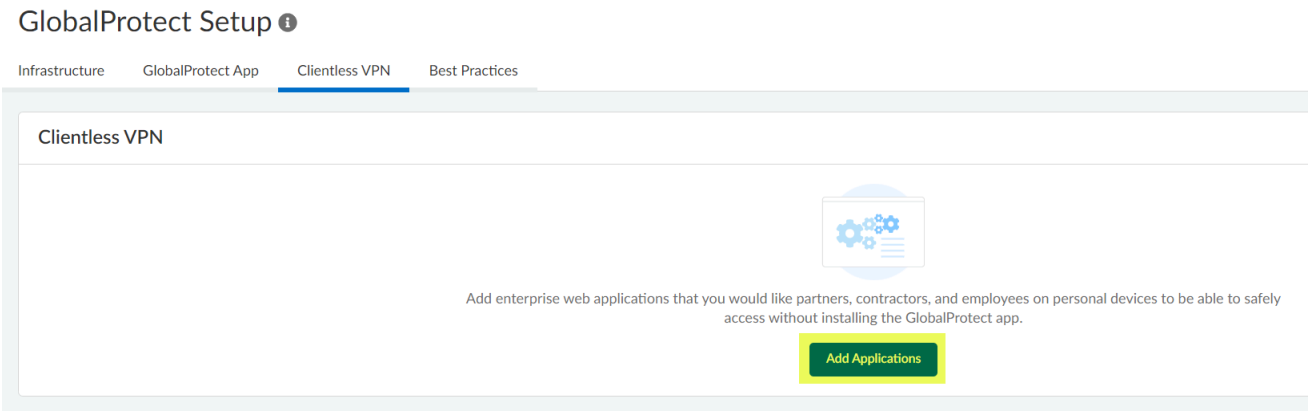
## GlobalProtect—無用戶端 VPN

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

無用戶端 VPN 可讓您從啟用 SSL 的 Web 瀏覽器安全地遠端存取企業應用程式。使用無用戶端 VPN，一般使用者無需在其端點上安裝 GlobalProtect 應用程式軟體，當您需要讓合作夥伴或承包商能夠存取應用程式並安全地啟用未受管理的資產（包括個人端點）時，這樣做很有用。

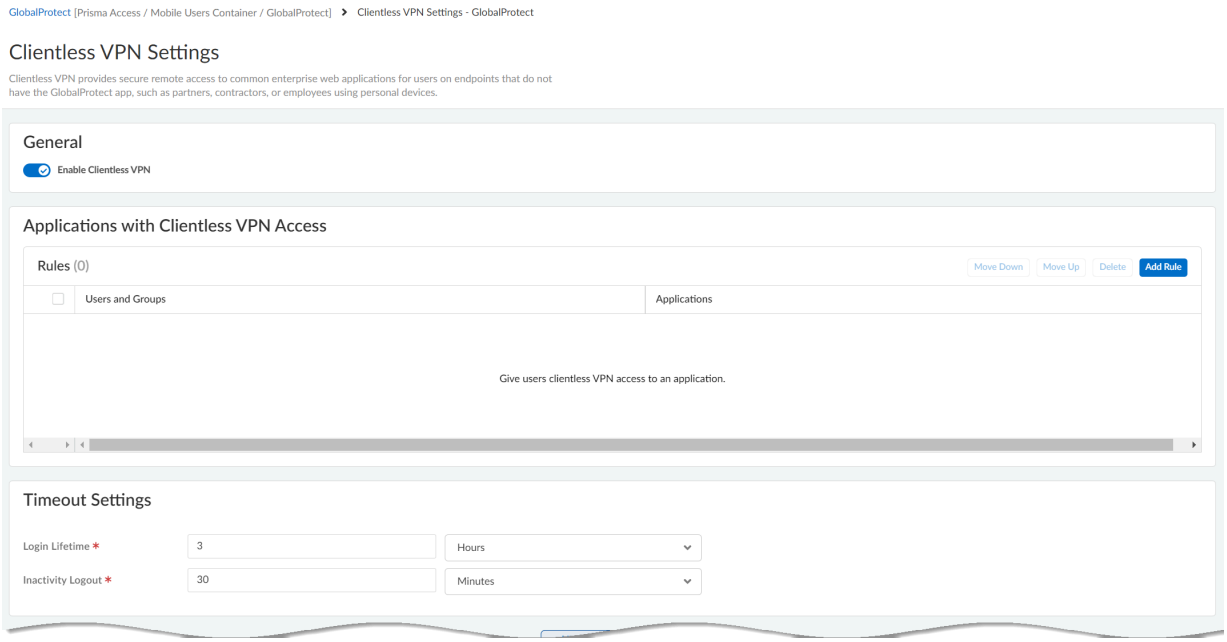
請使用下列步驟設定無用戶端 VPN Prisma Access:

**STEP 1 |** 前往 **Settings**（設定） > **Prisma Access Setup**（設定） > **GlobalProtect** > **GlobalProtect Setup**（**GlobalProtect** 設定） > **Clientless VPN**（無用戶端 **VPN**）和 **Add Applications**（新增應用程式）。




 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** **Enable Clientless VPN**（啟用無用戶端 **VPN**）。




**STEP 3 |** 新增無用戶端 VPN 規則。

指定可以使用無用戶端 VPN 的使用者和應用程式。

**STEP 4 |** 如果使用者需要透過 Proxy 伺服器連線到應用程式，請指定 **Add Proxy**（新增 **Proxy**）。

僅支援對 Proxy 基本驗證（使用者名稱和密碼）。您可以新增多個 Proxy 伺服器設定，每個網域集一個。要新增的一些設定包括：

- **Domains**（網域）—新增由 Proxy 伺服器所提供的網域。您可以在網域名稱的開頭使用萬用字元 (*) 來指出多個網域。
- **Enable Proxy**（啟用 **Proxy**）—指派要提供網域存取權的 Proxy 伺服器。
- **Server**（伺服器）—指定 Proxy 伺服器的 IP 位址或主機名稱。
- **Port**（連接埠）—指定與 Proxy 伺服器通訊的連接埠。
- **User and Password**（使用者和密碼）—指定要登入 Proxy 伺服器所需的使用者和密碼認證。再次指定密碼以進行驗證。

**STEP 5 |** 修改預設 **Crypto Settings**（加密設定），針對 Prisma Access 與使用無用戶端 VPN 的應用程式之間的 SSL 工作階段，指定驗證和加密演算法。


©2025 Palo Alto Networks, Inc.

**STEP 6 |** 將網域新增至 **Rewrite Exclude Domain List**（重新寫入排除網域清單）。

無用戶端 VPN 會作為反向 Proxy 並且會修改已發行之 Web 應用程式所傳回的 Web 頁面。它會重新寫入所有 URL，並對遠端使用者呈現已重新寫入的頁面，如此當他們存取其中任何 URL 時，要求便會通過 GlobalProtect 入口網站。在某些情況下，應用程式可能會有不需透過入口網站存取的頁面（例如，應用程式可能包含來自 yahoo.finance.com 的金融指數顯示板）。您可以排除這些頁面。您新增至 **Rewrite Exclude Domain List**（重新寫入排除網域清單）的網域會從重新寫入規則中排除，而且無法重新寫入。網域名稱中不支援路徑。網域名稱的萬用字元 (*) 只能出現在名稱開頭處（例如，*.etrade.com）。

# 監控 GlobalProtect 行動使用者

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

## Prisma Access (Managed by Strata Cloud Manager)

Prisma Access (Managed by Strata Cloud Manager) 使用者可以使用 **Monitor**（監控） > **Users**（使用者）。選取 **GlobalProtect** 或 **Explicit Proxy**（明確 **Proxy**）連線方法。**Mobile Users**（行動使用者）是您正在使用的連線方法特有的。

## Prisma Access (Managed by Panorama)

Panorama 中有數個位置，您可以在其中檢視已登入使用者的清單。您可以檢視唯一使用者、使用者登入的位置，以及提供額外資訊的表格。瞭解 Prisma Access 如何計算行動使用者—GlobalProtect 部署中每個位置的使用者數目也很重要。

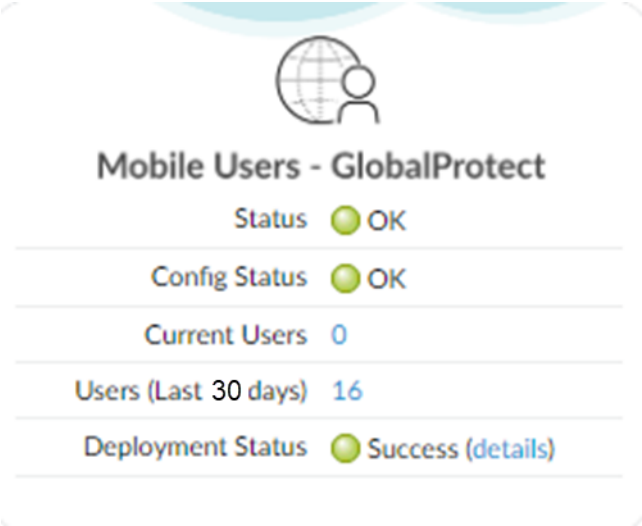
您可以從數個位置取得使用者的詳細檢視：

- 若要查看使用者的整體檢視，以及開啟允許您檢視已登入使用者並將其登出的表格，請選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Status**（狀態）。
- 若要在地圖檢視中查看使用者的圖形檢視，以及依區域和位置檢視使用者，請選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Service Stats**（服務統計資料） > **Mobile Users - GlobalProtect**（行動使用者—**GlobalProtect**）。
- 您還可以進一步瞭解 Prisma Access 計算行動使用者數目的方式。

從 **[Status**（狀態）**]** 頁籤檢視 **GlobalProtect** 行動使用者

若要檢視目前在所有位置登入的唯一使用者總數，請選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Status**（狀態） > **Mobile Users—GlobalProtect**（行動使用者—**GlobalProtect**）。

 ©2025 Palo Alto Networks, Inc.



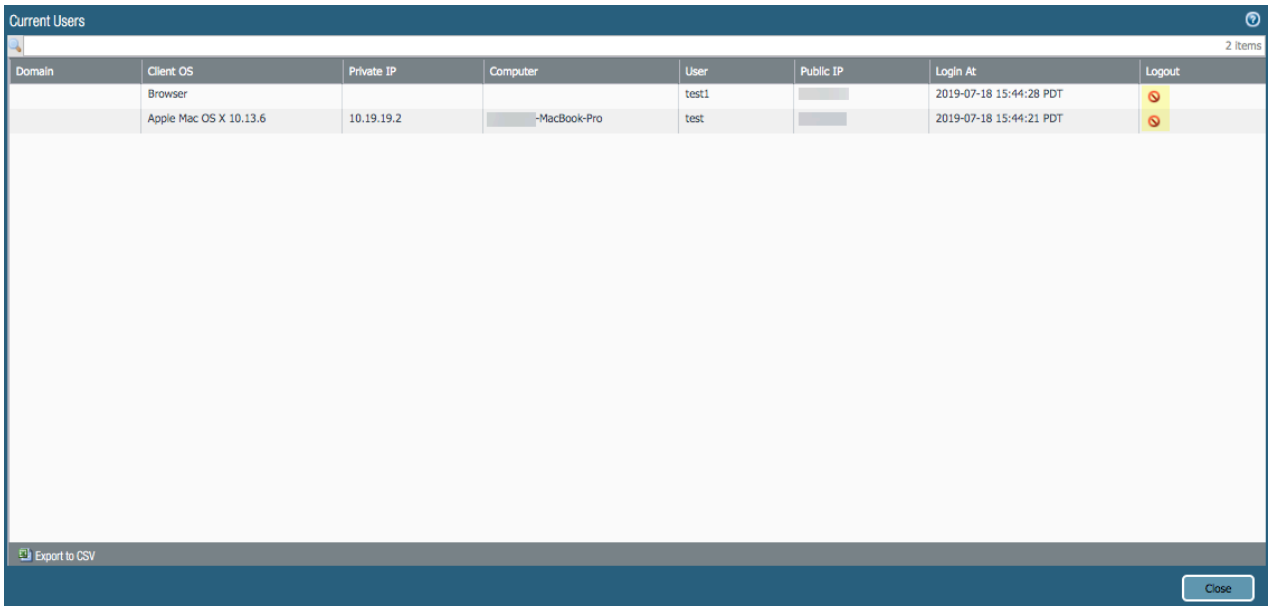

若要檢視有關目前登入使用者的更多詳細資訊，請按一下 **Current Users**（前使用者）旁邊的超連結數字，以顯示 **Current Users**（前使用者）表格。

狀態頁面中顯示的使用者總數與快顯表格中顯示的使用者總數可能不同；表格中顯示的數字可能會更大。

您可以從 **Current Users**（目前使用者）表格登出作用中使用者；若要這樣做，請選取使用者並按一下 **Logout**（登出）。請注意，您可能必須關閉畫面，然後將其重新開啟，以讓 Prisma Access 從 **Current Users**（目前使用者）頁面中移除已登出的使用者。

以下畫面顯示已使用 GlobalProtect 應用程式和無用戶端 VPN 登入的使用者。此畫面顯示使用者的使用者名稱、公用 IP 和上次登入時間。如果使用者透過 GlobalProtect 應用程式登入，它還會顯示其用戶端作業系統、私人 IP 位址和電腦名稱。

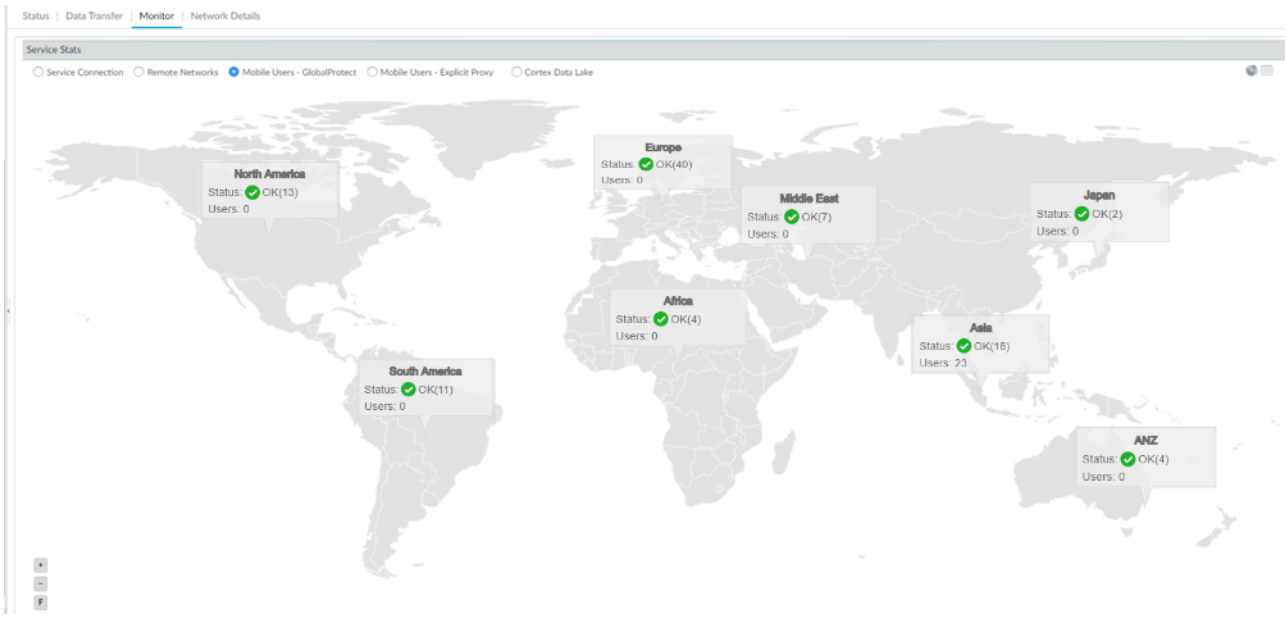
 ©2025 Palo Alto Networks, Inc.




從 **[Monitor**（監控）**]** 頁籤檢視 **GlobalProtect** 行動使用者

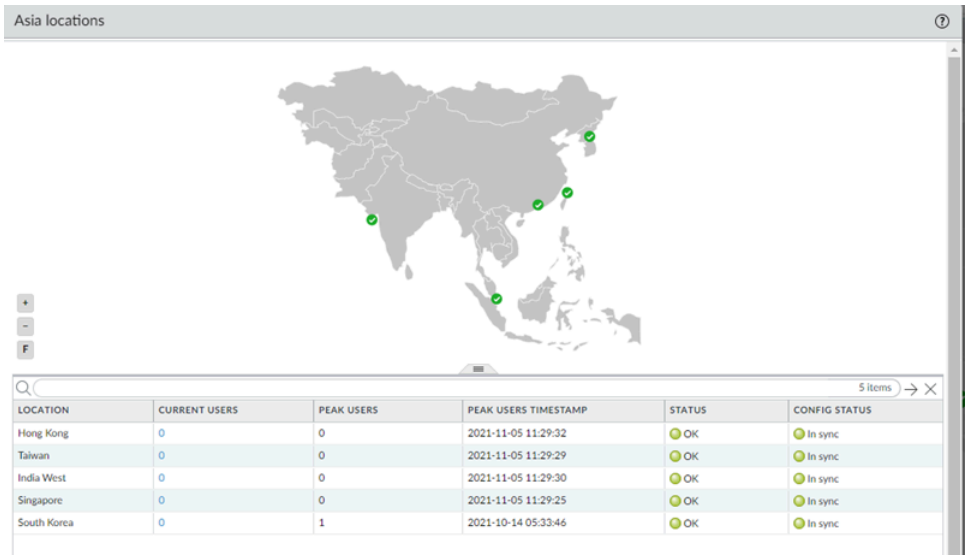
若要檢視每個區域登入的唯一使用者數目，請選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Service Stats**（服務統計資料） > **Mobile Users**—**GlobalProtect**（行動使用者—**GlobalProtect**）。

 ©2025 Palo Alto Networks, Inc.




若要檢視某個區域中位置的詳細資訊，請按一下該區域。

全域地圖檢視頁面中顯示的使用者數目和每個區域的表格中顯示的使用者數目可能會有所不同；表格中顯示的數字可能會更大。




### Prisma Access GlobalProtect 如何計數行動使用者

狀態區域中顯示的使用者總數可能與關聯表格中顯示的數目不同。下節描述了這些差異。

- **Status**（狀態）頁籤（**Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Status**（狀態））—在主要頁面的 **Mobile Users—GlobalProtect**（行動使用者—**GlobalProtect**）區域中顯示的使用者數量，可能與您按一下 **Current Users**（目前使用者）超連結時表格中顯示的數目不同。**Mobile Users—GlobalProtect**（行動使用者—**GlobalProtect**）區域中顯示的數字計算唯一

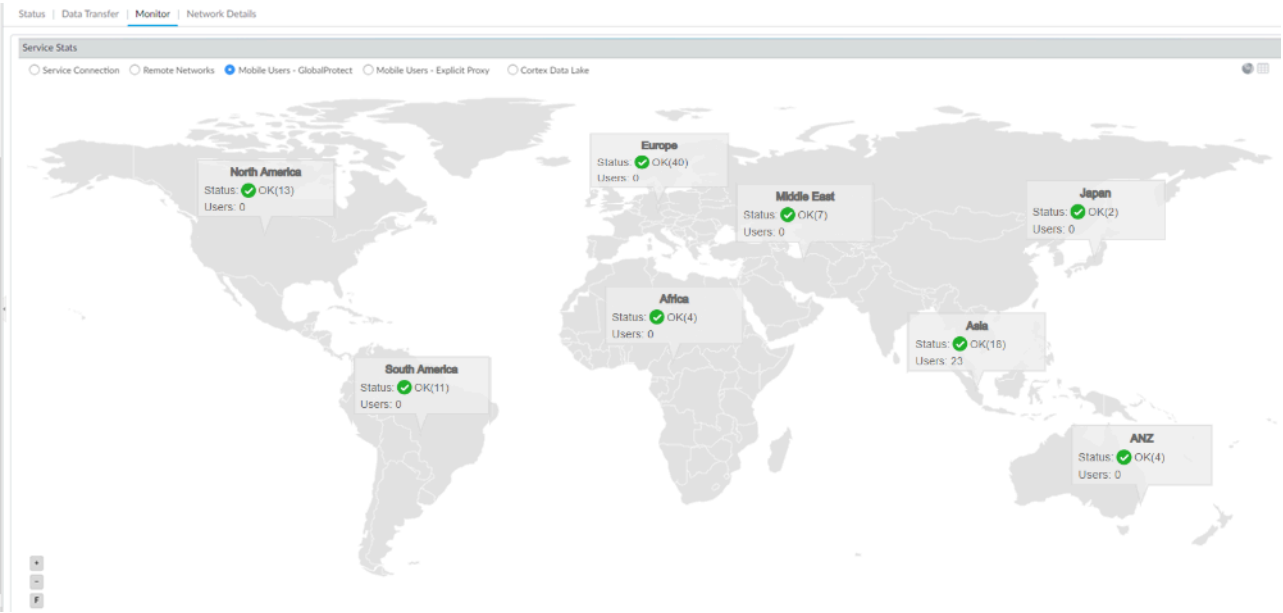
 ©2025 Palo Alto Networks, Inc.

使用者的數目；**Current Users**（目前使用者）表格中的使用者清單計數每次登入或連線時的所有使用者。如果單一使用者登入多個閘道或與多個裝置連線，表格中的數字可能會更大

例如，使用者 **user1** 登入 **United Kingdom**（英國） 位置中的兩個閘道；發生這種情況的原因可能是，當大量使用者登入相同位置時，Prisma Access 會自動新增閘道。在此情況下，Prisma Access 會在 **Mobile Users—GlobalProtect**（行動使用者—**GlobalProtect**）區域中對 **user1** 計數一次，但在 **Current Users**（目前使用者）表格中計數兩次。

- **Monitor**（監控）頁籤（**Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Service Stats**（服務統計資料） > **Mobile Users—GlobalProtect**（行動使用者—**GlobalProtect**））—您在全球地圖中看到的 **Users**（使用者）數目可能與您選取區域時顯示在表格的數目不同。登入多個閘道或與多個裝置連線的使用者可能會在表格中顯示多次。

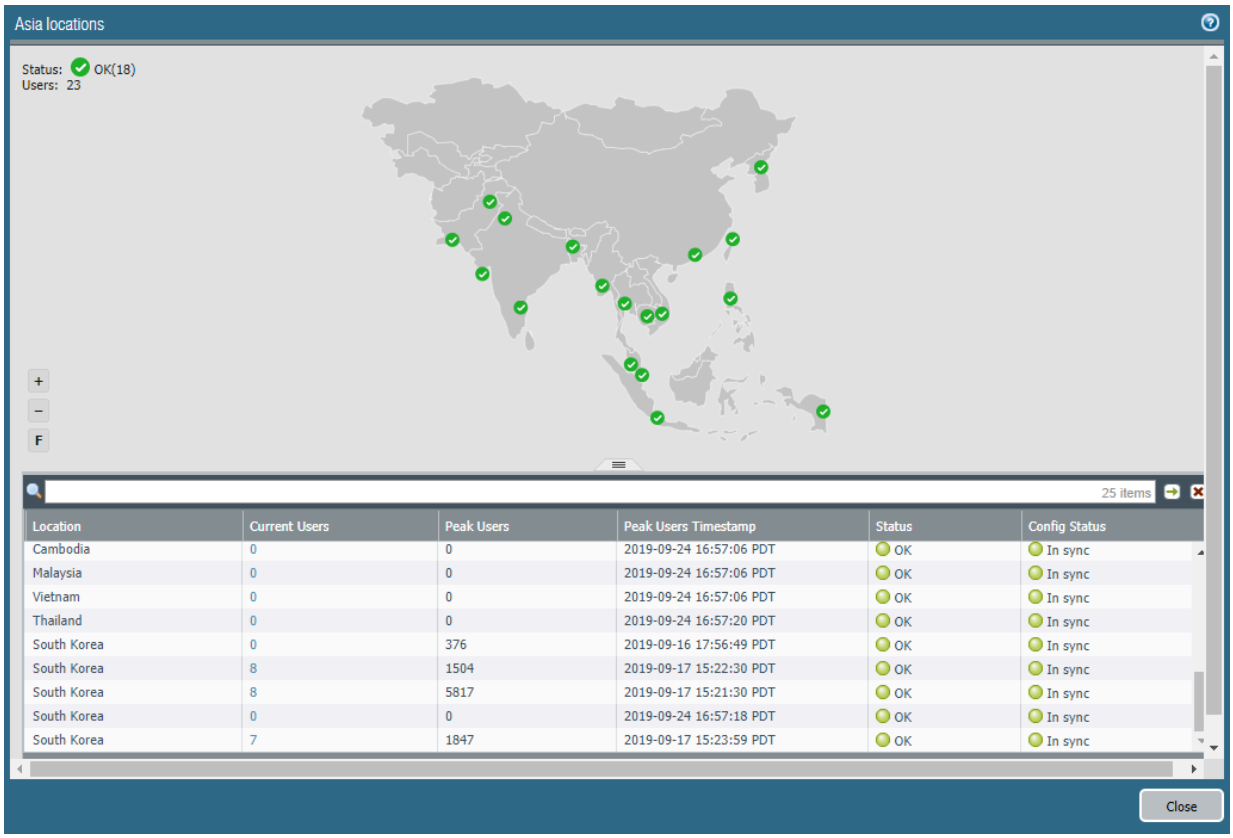
  以下螢幕擷取畫面提供一個範例。有 23 個唯一使用者登入 **Asia**（亞洲）地區，如全球地圖所示。




如果您選取 **Asia**（亞洲）地區，Prisma Access 會在區域頁面左上角給出唯一使用者數目 (23)。不過，有兩個使用者在 **South Korea**（韓國） 位置透過多個裝置（例如智慧型手機和電腦）進

 ©2025 Palo Alto Networks, Inc.

行連線。因為使用者有兩個個別的連線，所以 Prisma Access 會在表格中對它們計數兩次，因而在表格中給出總數 25。




# 用於 GlobalProtect 行動使用者部署的 IP 位址集區

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | • Prisma Access 授權 |


©2025 Palo Alto Networks, Inc.

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | |

請確定您已指定一個 IP 位址集區，允許為組織中的行動使用者提供足夠的涵蓋範圍。請務必記住，每個唯一使用者都可以使用多個裝置同時連線到 Prisma Access，而且每個連線的裝置都需要來自集區的唯一 IP 位址。此集區中的位址不得與您內部使用的其他位址集區，或您在啟用服務基礎結構時指派的 IP 子網路重疊。

我們建議集區中的 IP 位址數目是將連線至 Prisma Access 的行動使用者裝置數目的 2 倍如果您的組織有自攜裝置 (BYOD) 政策，或如果單一使用者有多個使用者帳戶，請確保在配置您的 IP 集區時將這些額外的裝置和帳戶納入考慮。如果您的集區空間有限，您可以指定較小的位址集區；不過，如果您的 IP 位址集區達到其限制，額外的行動使用者裝置將無法連線。

UI 會驗證您是否輸入有效的 IP 子網路（例如，如果您輸入子網路小於 /23 的集區，它將提示您將其變更）。不過，它不會檢查以確保您已為部署配置了足夠的 IP 位址。

如果您使用 *CLI* 設定位置，則此驗證無法進行。如果您使用 *CLI* 部署所有位置，我們建議您在全球集區中為行動使用者新增 */18* 位址。

Prisma Access 會檢查您的設定以確保您已指定以下最小 IP 位址集區：

- 全球或地區位址集區至少需要 /23（512 個 IP 位址）。
- 如果現有位置轉換為計算位置，則轉換後該位置至少需要 /23 子網路。
- 如果您沒有在一個區域中裝載任何 Prisma Access 閘道，則不需要該區域的 IP 位址集區。例如，如果您在美國東部、美國西北和美國東北位置指定閘道，則只需為北美和南美區域指定 IP 位址集區。相反，如果您在歐洲啟用行動使用者位置，但未在非洲、歐洲和中東指定全球位址集區或 IP 位址集區，您的部署將會失敗。
- GlobalProtect 行動使用者首先耗用位置群組中的 IP 位址，然後使用劇院特定的 IP 位址，最後使用全球 IP 位址。例如，如果您為位置群組和全世界指定一個集區，然後用盡位置群組集區中的可用 IP 位址，則 Prisma Access 將從 **Worldwide**（全球）集區取得 IP 位址以在該位置群組中使用。

  如果您指定多個 IP 位址集區區塊，Prisma Access 會依您在行動使用者設定期間輸入的順序使用集區。

## 行動使用者—GlobalProtect 部署的靜態 IP 位址配置

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | • Prisma Access 5.2.1 版<br>• PAN-OS 資料平面版本 11.2.4<br>包括活動洞察、使用者群組和位置群組支援<br>• GlobalProtect 版本 6.1.4 |

 ©2025 Palo Alto Networks, Inc.

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| | 這是一個有限的可用性版本。若要啟動此功能，請在啟動租用戶之後聯繫您的 *Palo Alto Networks* 客戶代表。 |

一些舊版網路會使 IP 位址型授權，限制使用者對內部或外部資源的存取。一個 Prisma Access 行動使用者—GlobalProtect 部署會從您在裝入期間指派的行動使用者 IP 位址集區中為使用者指派一個 IP 位址，並且此使用者至 IP 位址對應可以在後續登入中變更。若要保留使用者至 IP 位址對應，Prisma Access 允許您將靜態 IP 位址指派給使用者。

此功能僅適用於新的 *Prisma Access* 部署。

若要建立 IP 集區設定檔，請使用以下一個或多個準則：

- 一家劇院—根據您使用者所在的劇院配置 IP 位址。例如，您可以為特定劇院建立 /30 子網路。這些 IP 位址對於該劇院來說是靜態的。您可以根據劇院套用對資源的存取，方法是使用您為該劇院指定的 IP 位址建立安全性政策規則。
- 一個使用者—根據 User-ID 配置 IP 位址，方法是在行動使用者 IP 位址集區中指定 /30 或 /32 位址，並使用比對規則將該使用者與 IP 位址建立關聯。透過這種方式，您可以指派 Prisma Access 保留給特定使用者的靜態 IP 位址，從而允許您保留目前 IP 位址型安全性政策規則，以控制使用者對資源的存取。
- 一個使用者群組—根據使用者群組配置 IP 位址。如果使用者是所設定使用者群組的一部分，則使用者將從定義的 IP 集區子網路取得 IP 位址。
- 一個位置群組—根據 IP 集區設定檔中定義的位置群組配置 IP 位址。

配置靜態 IP 位址時，請使用以下指導方針：

- 如果指定多個 IP 集區，則 Prisma Access 從上到下評估規則，並根據規則清單中的第一個相符項配置 IP 位址。
- 如果您想要使用 User-ID 或 User-Group 作為比對 IP 集區的準則，請整合您的 Prisma Access 部署與雲端識別引擎。
- 每個租用戶支援以下配置上限：
  - 20,000 個使用者
  - 5,000 個使用者群組，每個使用者群組 50,000 個使用者
  - 10,000 個 IP 位址集區設定檔
  - 10,000 個 IP 位址集區
- 輸入介於 /23 與 /32 之間的首碼長度。
- 對於您建立的每個行動使用者 **Client IP Pool**（用戶端 **IP** 集區）設定檔：
  - 最多支援 10 個 IP 首碼。
  - 最多支援 256 個使用者。

 ©2025 Palo Alto Networks, Inc.

- 靜態 IP 定址使用 **Lease Period**（租用期）和 **Grace Period**（寬限期），指定 Prisma Access 保留使用者至 IP 位址關聯多長時間。
  - **Lease Period**（租用期）是使用者至 IP 位址對應在您配置它之後有效的時間量。

    預設租用期為 86400 秒（24小時）。

    最短租用期為 3600 秒（1 小時）。

    最長租用期為 7776000 秒（90 天）。
  - **Grace Period**（寬限期）是租用期到期後 Prisma Access 保留該使用者至 IP 位址對應，而不將其指派給另一個使用者的時間量。

    預設寬限期為 14400 秒（4 小時）。

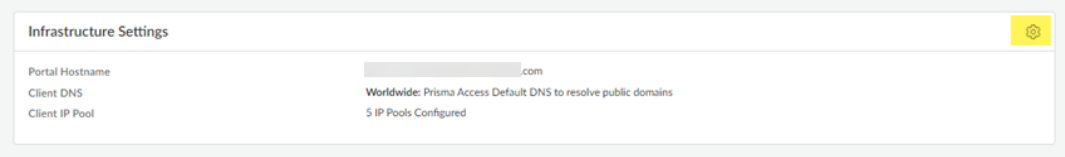
    最短寬限期為 60 秒。

    最長寬限期為 7776000 秒（90 天）。

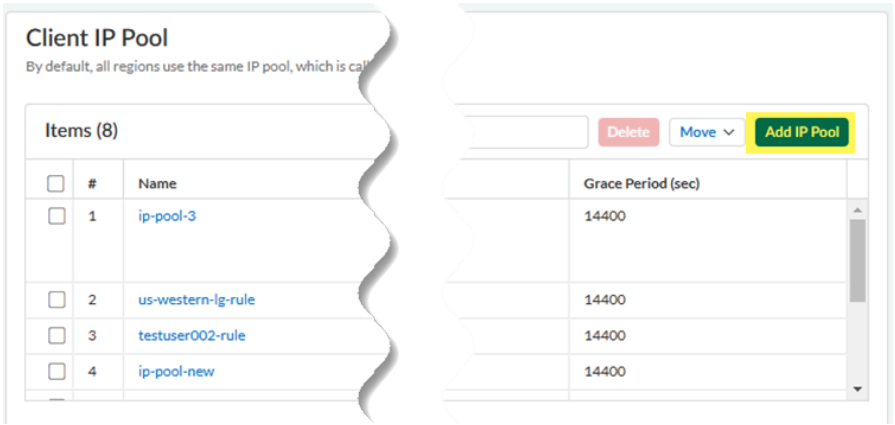
設定靜態 **IP** 位址配置

若要在 設定靜態 IP 位址配置，請完成以下步驟。

**STEP 1 |** 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **GlobalProtect**，然後按一下齒輪以反白顯示 **Infrastructure Settings**（基礎結構設定）。



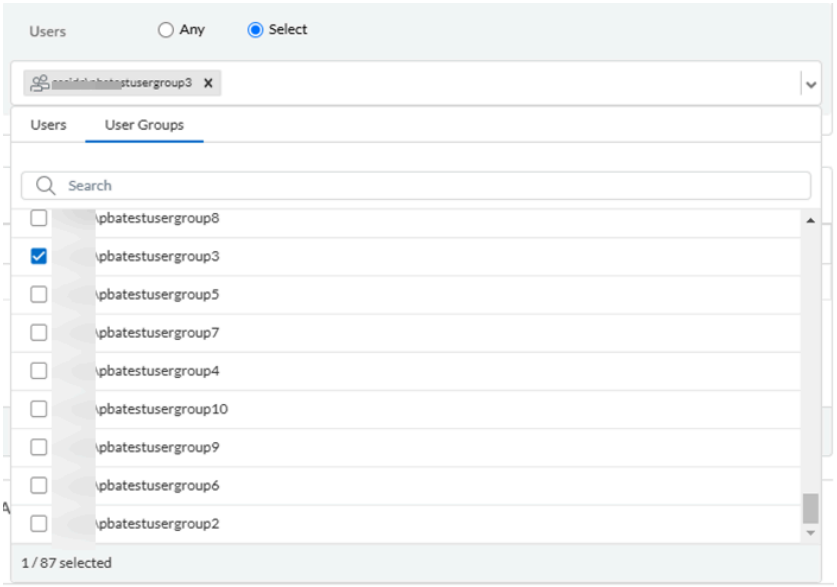

**STEP 2 |** 在 [Client IP Pool（用戶端 IP 集區）] 區域中，為靜態 IP 位址 **Add IP Pool**（新增 **IP** 集區）。




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 將靜態 IP 位址指派給劇院、Prisma Access 位置群組或使用者。

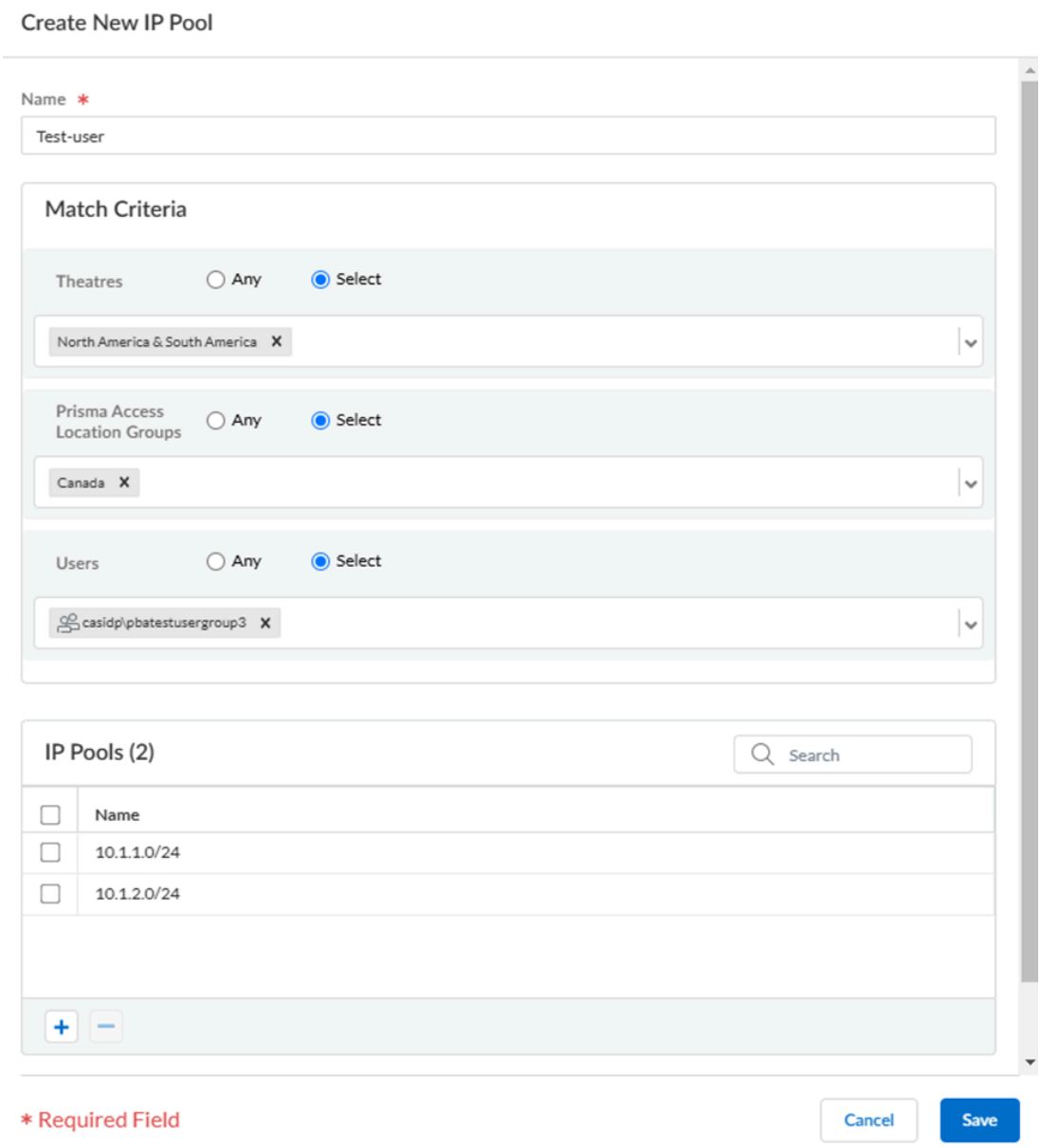
1. 給與 IP 位址集區唯一的 **Name**（名稱）。
2. **Select**（選取）一個或多個 **Theatres**（劇院），以允許在這些劇院中使用集區，或選取 **Any**（任何），以允許在所有劇院中使用集區。
3. **Select**（選取）一個或多個 **Prisma Access Location Groups**（**Prisma Access** 位置群組），以允許在該位置群組中使用集區，或選取 **Any**（任何），以允許在所有位置群組中使用集區。
4. **Select**（選取）使用者或使用者群組，或選取 **Any**（任何），以允許將集區用於任何使用者或使用者群組。
   - 若要將一個或多個使用者指派給 IP 位址集區，請在 **Users**（使用者）頁籤中選取使用者。
   - 若要將一個或多個使用者群組指派給 IP 位址集區，請在 **User Groups**（使用者群組）頁籤中選取使用者群組。




5. 在 **IP Pools**（**IP** 集區）區域中，輸入 IP 位址集區。

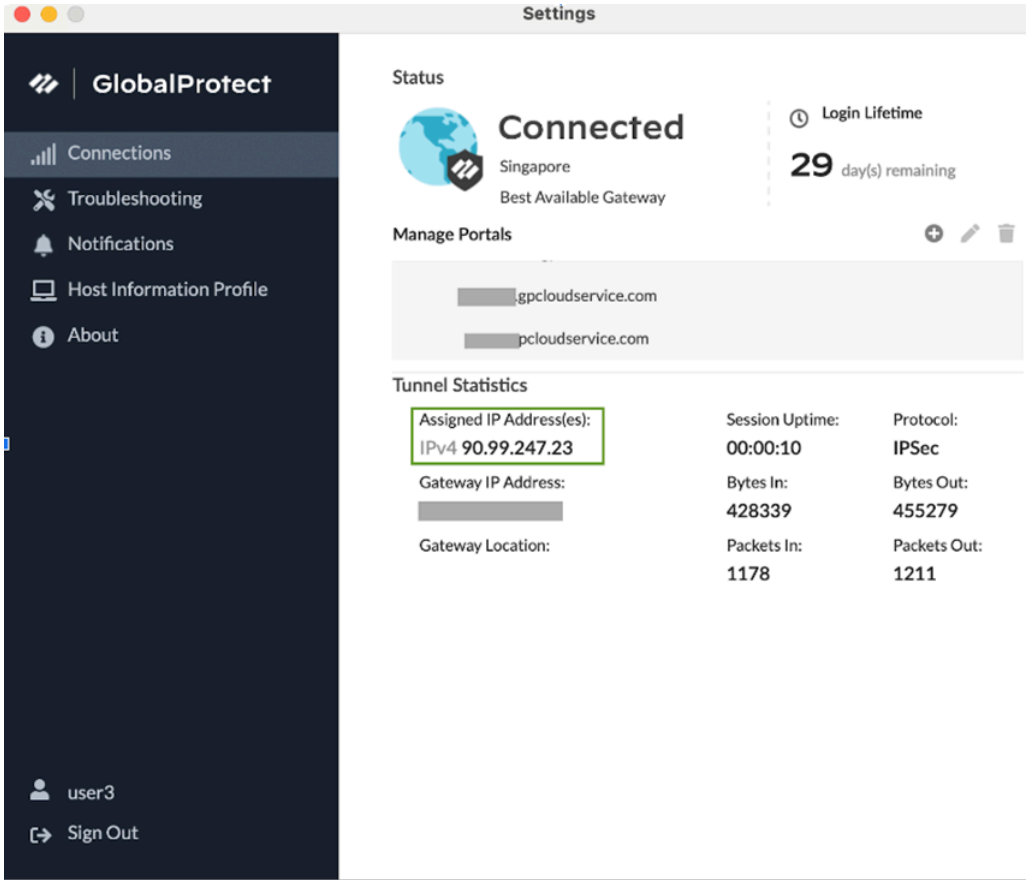
   若要將使用者限制為單一 *IP* 位址，請指定 */30* 或 */32 IP* 位址；*Prisma Access* 會將使用者指派給該位址。由於 */32* 僅會提供一個 *IP* 位址，因此我們建議最小子網路為 */30*，並將使用者限制在該子網路內。
6. （選用）為使用者至 IP 位址對應輸入 **Lease Period**（租用期）和 **Grace Period**（寬限期）。
7. **Save**（儲存）變更。


©2025 Palo Alto Networks, Inc.




 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 前往用戶端電腦上的 **GlobalProtect > Settings**（設定）、檢視 **Tunnel Statistics**（通道統計資料），並驗證 **Assigned IP Address(es)**（指派的 **IP** 位址），來驗證您的變更。




## GlobalProtect 應用程式如何為行動使用者選取 Prisma Access 位置

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

當行動使用者連線到 Prisma Access 位置時，應用程式會使用以下選取程序來確定它連線到哪個位置。

您可以啟用您想要 *Prisma Access* 在行動使用者裝載期間出現在其中的行動使用者位置。如果您在裝載期間未選取位置，*Prisma Access* 不會在您的部署中使用它。

- 如果行動使用者在具有 Prisma Access 位置的國家/地區進行連線，則使用者會連線到該國家/地區的位置。

 ©2025 Palo Alto Networks, Inc.

- 如果行動使用者由於任何原因無法連線到國內位置，Prisma Access 會從下列其中一個行動使用者位置進行選取，以根據區域連線使用者。
  - 亞洲、澳洲和日本：香港、日本中部或日本南部
  - 非洲、歐洲和中東：荷蘭中部
  - 北美洲和南美洲：美國西北部

  Palo Alto Networks 建議您在行動使用者裝載期間至少在其各自區域中啟用其中一個位置，以提供備援。如果您有行動使用者連線到 Prisma Access，但其來自一個沒有 Prisma Access 位置的國家/地區，則必須至少啟用先前清單的其中一個回復位置。

  香港、日本中部、日本南部、荷蘭中部和美國西北部位置可以接受來自任何地方的用戶端連線，並被稱為全域回復位置。除了這些位置之外，您還可以啟用下列一個或多個位置，這些位置也充當全域回復位置：
  - 巴林
  - 法國北部
  - 愛爾蘭
  - 南非西部
  - 韓國
- Palo Alto Networks 建議您基於備援目的在多個計算位置中啟用位置。
- 如果使用內部部署閘道搭配 Prisma Access 位置，您可以指定 Prisma Access 中的優先順序，讓行動使用者連線到特定的內部部署 GlobalProtect 閘道或 Prisma Access 位置。如需詳細資訊，請參閱管理 Prisma Access 和內部部署閘道的優先順序。
- 當行動使用者連線時，GlobalProtect 應用程式不會在自動閘道選取過程中使用以下 Prisma Access 位置，即使您在裝載期間選取了外掛程式中的 Prisma Access 位置也一樣。不過，行動使用者仍然可以手動選取其中一個位置，並將其設定為慣用位置（閘道），只要您允許他們在行動使用者裝載期間手動選取這些位置即可：
  - 澳洲：澳洲東部
  - 巴西：巴西東部和巴西中部
  - 法國：法國南部
  - 德國：德國北部和德國南部
  - 印度：印度南部
  - 墨西哥：墨西哥西部
  - 荷蘭：荷蘭南部
  - 巴基斯坦：巴基斯坦西部
  - 俄羅斯：俄羅斯西北部
  - 西班牙：西班牙東部

  您可能必須將 ***Connect Method***（連線方法）變更為 ***On-Demand***（隨選），讓行動使用者手動連線到閘道。

 ©2025 Palo Alto Networks, Inc.

# 允許列出 GlobalProtect 行動使用者

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ Minimum Required Prisma Access Version：3.0 Preferred |

瞭解如何為現有行動使用者啟用輸出 IP 允許清單。

若要讓您可為 GlobalProtect 新增公用（輸出）IP 位址—行動使用者部署到您在組織內使用的任何 SaaS 應用程式允許清單，Prisma Access 會提供 IP 位址，並讓您在環境中使用它們之前，驗證是否已將它們新增至允許清單。如果您為現有 Prisma Access 部署啟用輸出 IP 允許清單，則 Prisma Access 會將已為您位置配置的所有輸出 IP 位址移轉到輸出 IP 允許清單。對於新的 Prisma 部署，在裝載 Global Protect 行動使用者時，啟用輸出 IP 允許清單。

在您已將輸出 IP 位址新增至您組織的允許清單之後，您會返回 Prisma Access UI、確認 GlobalProtect 輸出 IP 位址列入允許清單，以及 **Push**（推送）您的變更。Prisma Access 接著會釋出這些輸出 IP 位址，並將它們新增至您的部署。如果 Prisma Access 在初始設定之後由於自動調整事件而新增更多 IP 位址，則在 Prisma Access 將新的輸出 IP 位址新增至您的部署之前，確認已新增這些位址。

一旦啟用，輸出 IP 允許清單表格就會提供已確認或尚未確認的 IP 位址相關資訊，以及它們的佈建狀態。

- Strata Cloud Manager
- Panorama

## 允許列出 GlobalProtect 行動使用者 (Strata Cloud Manager)

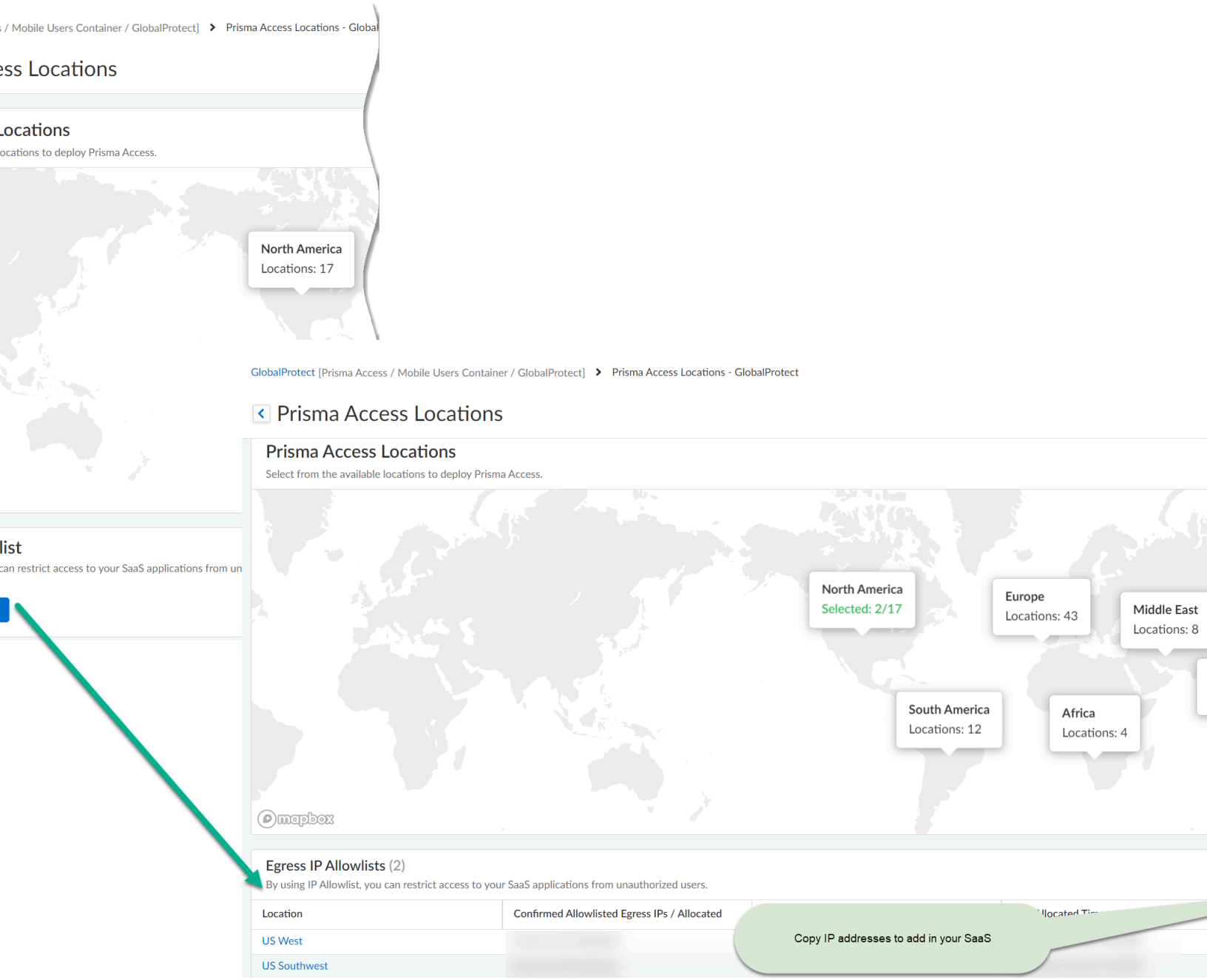
讓 Prisma Access 能夠顯示 Prisma Access 流量的輸出 IP 位址。在您 SaaS 應用程式的 IP 允許清單中使用這些 IP 位址，您可以在其中限制授權使用者或來源的使用。

**STEP 1 |** 前往**Workflows**（工作流程） > **Prisma Access Setup**（設定） > **GlobalProtect** > **Infrastructure**（基礎結構），並編輯 **Prisma Access Locations**（位置）設定。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 顯示 Prisma Access 位置的 IP 位址。

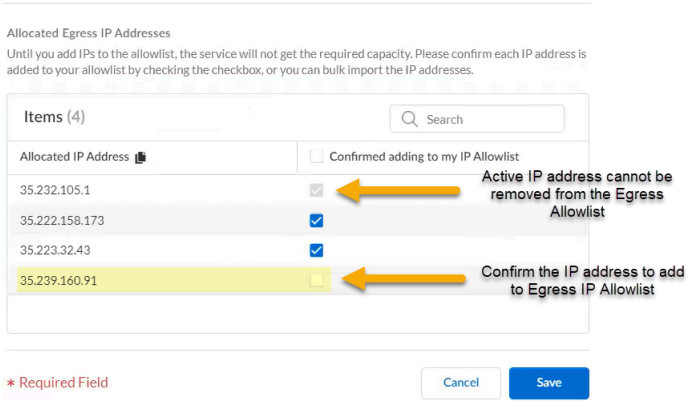
1. 啟用輸出 IP 允許清單，以顯示所裝載 Prisma Access 位置的 IP 位址。
2. 複製配置的 IP 位址並將其新增至 SaaS 應用程式的允許清單。
3. 移轉以確認為 Prisma Access 中所裝載位置配置的 IP 位址。




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 為新裝載位置或在自動調整事件期間擷取 IP 位址。

1. 選取位置名稱以尋找配置給該位置的新輸出 IP 位址。
2. 選取 **Confirmed adding to my IP Allowlist**（已確認新增至我的 **IP** 允許清單），將這些 IP 位址新增到您 Saas 應用程式的允許清單，然後在 Prisma Access 中確認它們。




如果您有 IPv6 位址，請選取 **Confirmed adding to my IPv6 Allowlist**（已確認新增至我的 **IPv6** 允許清單）。




**STEP 4 |** 將您的變更推送至 Prisma Access。

所配置輸出 **IP** 位址的狀態

輸出 IP 允許清單中的狀態欄指出所有為位置配置的 IP 位址是否針對您的部署所佈建的。請繼續閱讀以瞭解每種狀態。

已佈建 - 您已將輸出 IP 位址新增至 SaaS 應用程式的允許清單、確認了 Prisma Access 中的 IP 位址，並推送您的變更以使其完全佈建。

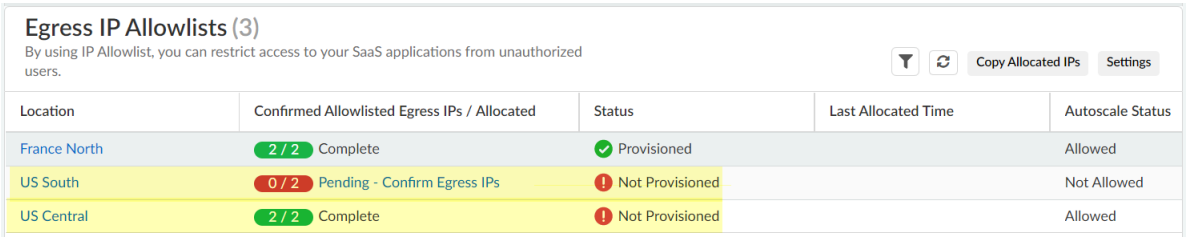
部分佈建 - 您已新增第一組輸出 IP 位址、在 Prisma Access 中確認了它們，並推送您的變更。不過，Prisma Access 已新增另一組 IP 位址作為自動調整事件的一部分，並且這些 IP 位址未在 Prisma Access 中確認。

未佈建 - Prisma Access 已為該位置配置 IP 位址，並且您已將輸出 IP 位址新增至 SaaS 應用程式的允許清單，然後在 Prisma Access 中確認了它們，但您尚未裝載此位置。

無法佈建 - 您已裝載此位置，但尚未在 Prisma Access 中確認，並已推送你的變更。

輸出 IP 允許清單表格也指出 Prisma Access 中已確認和尚未確認的 IP 位址數目。例如，1/2 表示為該位置配置的 2 個 IP 位址中的 1 個已在 Prisma Access 中確認。


©2025 Palo Alto Networks, Inc.




## 允許列出 GlobalProtect 行動使用者 (Panorama)

若要讓您可為 GlobalProtect 新增公用（輸出）IP 位址—行動使用者部署到您在組織內使用的任何 SaaS 應用程式允許清單，Prisma Access 會提供 IP 位址，並讓您在環境中使用它們之前，驗證是否已將它們新增至允許清單。

此輸出 IP 位址配置方法具有以下優點：

- 它確保 Prisma Access 只提供您已將其列入允許清單的 IP 位址。
- 它可防止行動使用者嘗試從您組織網路封鎖的 IP 位址連線至 Prisma Access。在您確認 IP 位址已列入允許清單之前，Prisma Access 不會將 IP 位址釋出至您的部署。
- 它提供了一種在不使用 API 的情況下擷取目前輸出 IP 位址的方法。

Prisma Access 會在下列情況下配置輸出 IP 位址：

- 當您在行動使用者裝載期間裝載您的位置時。

  Prisma Access 會為您裝載的每個位置配置兩個閘道 IP 位址。

  如果您裝載一個位置，而同一計算位置中的其他位置遭遇自動調整事件，則 *Prisma Access* 可能會為新位置配置兩個以上的 *IP* 位址。在這種情況下，請確定您將所有這些 *IP* 位址新增至允許清單，並確認所有位址 ***Added to My Allow List***（已新增至我的允許清單）。


©2025 Palo Alto Networks, Inc.

- 在大型調整事件期間。

  如果行動使用者數目超過兩個預先配置的 IP 位址的容量，則 Prisma Access 會再配置一組兩個 IP 位址。

  自動調整事件會影響計算位置中的所有裝載位置。當某個位置發生自動調整事件，而您尚未確認位址已新增至允許清單時，該計算位置中所有位置的 **Autoscale Status**（自動調整狀態）將顯示為 **Not Allowed**（不允許）。

  ***Autoscale Status***（自動調整狀態）顯示 *Prisma Access* 中自動調整的狀態。

  - ***Allowed***（已允許）—您已將 *IP* 位址新增至允許清單。如果大量行動使用者登入單一位置，並觸發自動調整事件，則 *Prisma Access* 會將列入允許清單的 *IP* 位址用於自動調整事件。
  - ***Not Allowed***（不允許）—您尚未在 *Prisma Access UI* 中將所有 *IP* 位址指定為新增至允許清單，或者在將您的變更標記為已新增之後，您未提交並推送這些變更。如果 *Prisma Access* 觸發自動調整事件，則 *Prisma Access* 不會佈建更多 *IP* 位址，為該位置新增更多容量。

    每次新增位置時，或是每次 *Prisma Access* 由於自動調整事件而新增 *IP* 位址時，您都需要重新整理包含 ***Egress IP Allow List***（輸出 ***IP*** 允許清單）表格的頁面、指定 ***Added to My Allow List***（已新增至我的允許清單）以將 *IP* 位址標記為已新增至您組織的允許清單，然後 ***Commit and Push***（提交並推送）您的變更。

  若要在 *Prisma Access* 由於自動調整事件而新增任何 *IP* 位址時告知您，您可以設定一個 URL，其中 *Prisma Access* 將通知您 *IP* 位址變更。

  您不需要啟用此功能；您可以選擇是否要讓 Prisma Access 釋出 IP 位址，直到確認它們已在 UI 中列入允許清單。

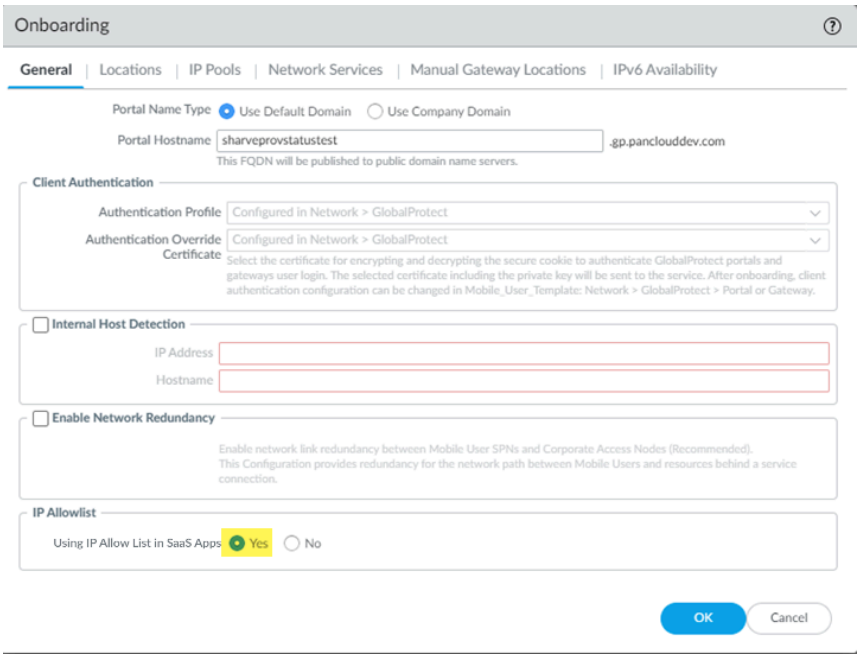
  若要防止 Prisma Access 將公用（輸出）GlobalProtect IP 位址佈建至您的部署，直到您已將其新增至允許清單，請在行動使用者—GlobalProtect 裝載期間，於 **Using IP Allow List in SaaS Apps**（在 **SaaS** 應用程式中使用 **IP** 允許清單）中指定 **Yes**（是）。透過完成下列工作，確認您已在 Prisma Access UI 中新增它們。

**STEP 1 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users—GlobalProtect**（行動使用者—**GlobalProtect**）。

**STEP 2 |** 選取您的 **Hostname**（主機名稱），並 **Configure**（設定） 它（適用於現有部署）或第一次 **Configure**（設定）您的部署（適用於新部署）。

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 將 **Using IP Allow List in SaaS Apps**（在 **SaaS** 應用程式中使用 **IP** 允許清單）指定為 **Yes**（是）。




**STEP 4 |** 繼續您的 Prisma Access 裝載，包括選取要在行動使用者—GlobalProtect 部署中使用的位置，以及 **Commit and Push**（提交並推送）您的變更。

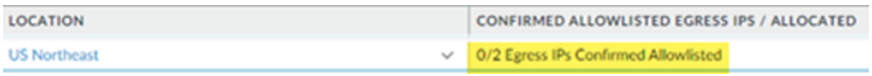
這些變更可能最多需要一分鐘才能反映在 UI 中。如果您在提交並推送變更之前檢視 **Egress IP Allow List**（輸出 **IP** 允許清單），則其會將狀態顯示為 **0/0 Egress IPs Confirmed Allow Listed**（**0/0** 輸出 **IP** 已確認列入允許清單），因為 Prisma Access 未將任何輸出 IP 位址指派給您的部署。

 ©2025 Palo Alto Networks, Inc.

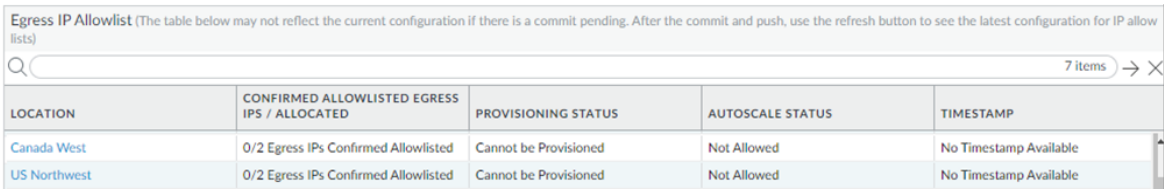
**STEP 5 |** 檢視 **Egress IP Allow List**（輸出 **IP** 允許清單）表格，並記下需要新增至允許清單的輸出 IP 位址。

您可以在 **Egress IP Allow List**（輸出 **IP** 允許清單）表格的 **Confirmed Allow Listed Egress IPs / Allocated**（已確認列入允許清單的輸出 **IP**/已配置）欄位中檢視輸出 IP 位址。第一個數字表示 IP 位址是否已確認為已新增至您的允許清單。

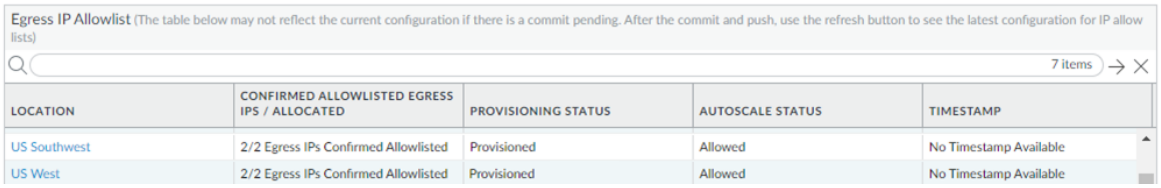
下列範例顯示了美國東北部位置的 IP 位址。`0/2 Egress IPs Confirmed Allow Listed`（`0/2` 輸出 `IP` 已確認列入允許清單）的說明表示，兩個輸出 IP 位址中沒有一個標記為已新增至您的允許清單，您需要新增它們。




如果您有新的 Prisma Access 部署，或者如果您已新增位置或有自動調整事件，表格會顯示沒有任何輸出 IP 位址新增至您組織的允許清單。

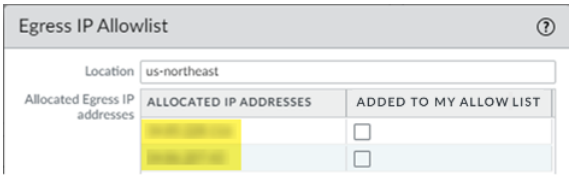



如果您有現有的 Prisma Access 部署，表格會將 **Provisioning Status**（佈建狀態）顯示為 **Provisioned**（已佈建），並將 **Autoscale Status**（自動調整狀態）顯示為 **Allowed**（已允許），這表示 Prisma Access 已將輸出 IP 位址標記為已新增。




Prisma Access 將為每個新增的位置配置兩個位址。當大量行動使用者同時登入單一位置時，如果現有位置之前已有自動調整事件，則 Prisma Access 會以 2 的倍數配置額外的輸出 IP 位址，而現有位置可能有四個或更多位址。

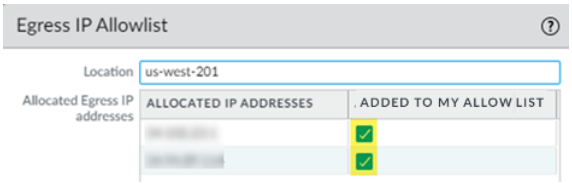
**STEP 6 |** 透過選取表格中的 **Location**（位置）名稱，尋找需要新增至您組織允許清單的新輸出 IP 位址。



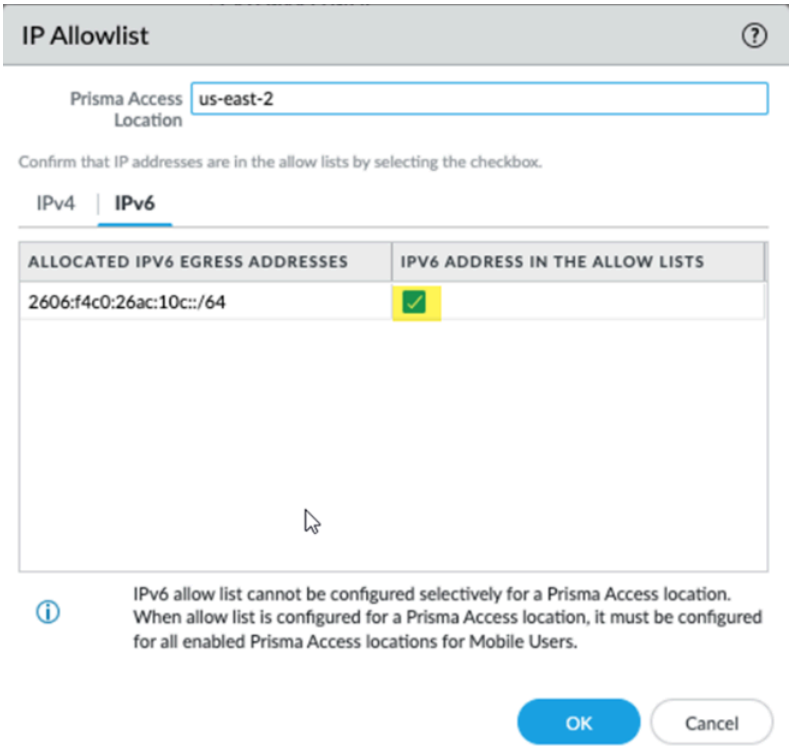

**STEP 7 |** 將這些輸出 IP 位址新增至您組織的允許清單。

 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** 在您已將輸出 IP 位址列入允許清單之後，請返回輸出 IP 區域，並透過選取 **Added to My Allow List**（已新增至我的允許清單），指出您已將它們新增至您的允許清單。

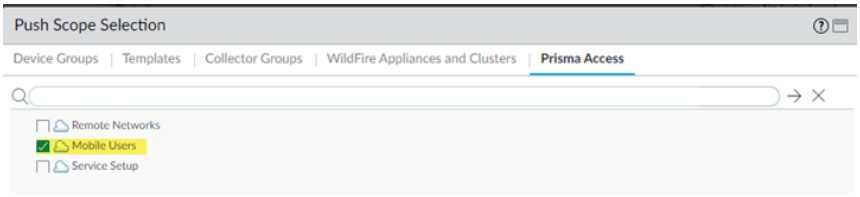



如果您有 IPv6 位址，請選取 **IPv6 Address in the Allow Lists**（允許清單中的 **IPv6** 位址）。




**STEP 9 |** 提交並推送您的變更，以使其在 Prisma Access 作用中。

1. 在推送範圍中選取 **Commit**（提交） > **Commit and Push**（提交並推送）和 **Edit Selections**（編輯選取項目）。
2. 選取 **Prisma Access**，然後確定已選取 **Mobile Users**（行動使用者）。

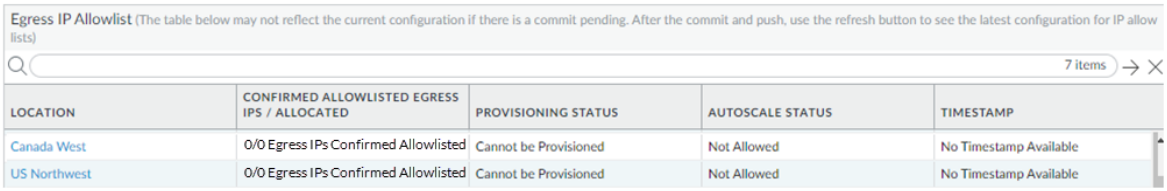



3. 按一下 **Ok**（確定），以儲存您對 Push Scope（推送範圍）所做的變更。
4. **Commit**（提交）並 **Push**（推送）您的變更。

如果您在提交並推送變更之前檢視 **Egress IP Allow List**（輸出 **IP** 允許清單）表格，則已確認欄會將狀態顯示為 **0/0 Egress IPs Confirmed Allow Listed**（**0/0** 輸出 **IP** 已確認列入允許清單），

 ©2025 Palo Alto Networks, Inc.

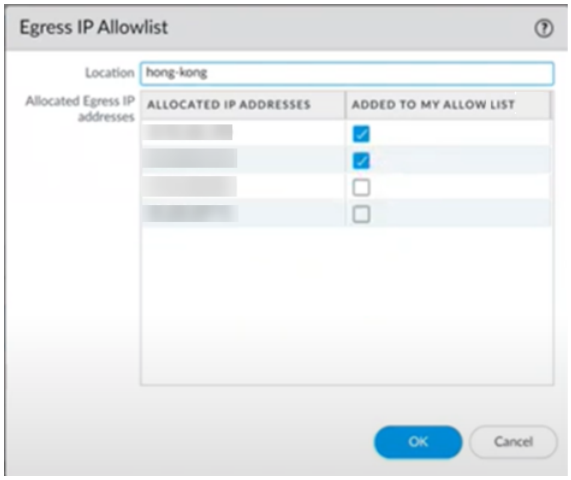
因為 Prisma Access 未將任何 IP 位址指派給您的部署，直到您 **Commit and Push**（提交並推送）。




**Egress IP Allow List**（輸出 **IP** 允許清單）表格包含下列其他欄位：

| 欄位 | 說明 |
|---|---|
| 位置 | 已裝載的行動使用者位置。 |
| 已確認列入允許清單的輸出 **IP**/已配置 | 已確認為列入允許清單的輸出 IP 位址數目，以及已配置的輸出 IP 位址數目。 |
| 佈建狀態 | 輸出 IP 位址的允許清單狀態。<br>• **Provisioned**（已佈建）—您已將輸出 IP 位址新增至您組織的允許清單、已確認它們已在 Prisma Access UI 中新增（方法為核取 **Added to My Allow List**（已新增至我的允許清單）），且已提交並推送您的變更以使其進行完全佈建。<br>• **Not Provisioned**（未佈建）—Prisma Access 已為該位置配置 IP 位址，且您已將輸出 IP 位址新增至您組織的允許清單，並已確認它們已在 Prisma Access UI 中新增，但您尚未裝載此位置。<br>• **Cannot Be Provisioned**（無法佈建）—您已裝載此位置，但尚未核取 **Added to My Allow List**（已新增至我的允許清單），且已提交並推送您的變更。<br>在您於 Prisma Access 中指定已將這些輸出 IP 新增至您組織的允許清單，且 **Commit and Push**（提交並推送）您的變更之前，Prisma Access 不會將這些 IP 位址佈建至您的部署。<br>• **Provisioned with partial capacity**（已佈建部分容量）—您已新增第一組輸出 IP 位址、已確認它們已在 Prisma Access UI 中新增，且已提交並推送您的變更。不過，Prisma Access已新增另一組 IP 位址作為自動調整事 |

 ©2025 Palo Alto Networks, Inc.

| 欄位 | 說明 |
| --- | --- |
| | 件的一部分，而這些 IP 位址尚未指定為已新增至 Prisma Access UI 中您的允許清單。<br><br>下面螢幕擷取畫面顯示一個部署範例，該部署將標記為 **Provisioned with partial capacity**（已佈建部分容量）。兩個 IP 位址已標記為 **Added to My Allow List**（已新增至我的允許清單）；不過，Prisma Access 已將另外兩個 IP 位址新增至此位置，而這些位置尚未在 UI 中新增。<br><br>  |
| 自動調整狀態 | 顯示 Prisma Access 中自動調整的狀態。<br><br>• **Allowed**（已允許）—您已將 IP 位址新增至允許清單。如果大量行動使用者登入單一位置，並觸發自動調整事件，則 Prisma Access 會將列入允許清單的 IP 位址用於自動調整事件。<br>• **Not Allowed**（不允許）—您尚未在 Prisma Access UI 中將所有 IP 位址指定為新增至允許清單，或者在將您的變更標記為已新增之後，您未提交並推送這些變更。如果 Prisma Access 觸發自動調整事件，則 Prisma Access 不會佈建更多 IP 位址，為該位置新增更多容量。<br><br>每次新增位置時，或是每次 Prisma Access 由於自動調整事件而新增 IP 位址時，您都需要重新整理包含 **Egress IP Allow List**（輸出 IP 允許清單）表格的頁面、指定 **Added to My Allow List**（已新增至我的允許清單）以將 IP 位址標記為已新增至您組織的允許清單，然後 **Commit and Push**（提交並推送）您的變更。 |

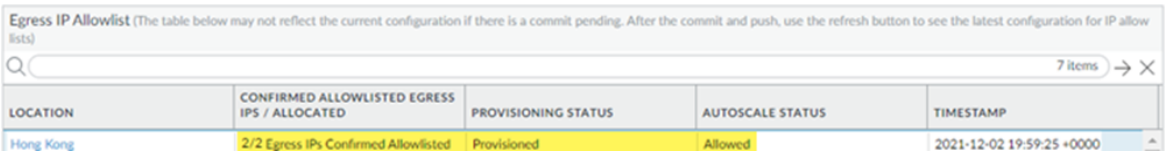
 ©2025 Palo Alto Networks, Inc.

| 欄位 | 說明 |
| --- | --- |
| | 若要在 *Prisma Access* 由於自動調整事件而新增任何 *IP* 位址時告知您，您應該設定一個 *URL*，其中 *Prisma Access* 將通知您 *IP* 位址變更。 |
| 時間戳記 | 上次為此區域配置 IP 的已知時間，以國際標準時間 (UTC) 表示。 |

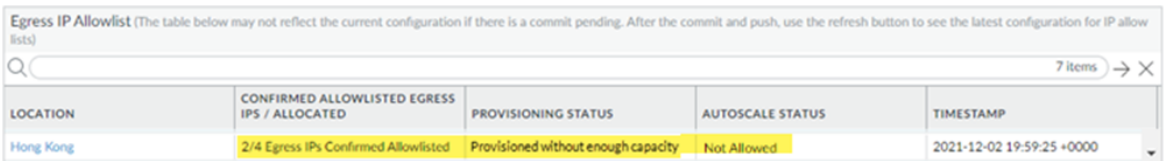
在您 **Commit and Push**（提交並推送）之後，已確認欄會將狀態顯示為 **0/2 Egress IPs Confirmed Allow Listed**（**0/2** 輸出 **IP** 已確認列入允許清單），因為您尚未確認 IP 位址已允許在 Prisma Access UI 中列出。

當您裝載行動使用者位置時，Prisma Access 會為您提供兩個輸出 IP 地址 - 一個作用中 IP 位址和一個要在發生自動調整事件時使用的位址。以下提供 Prisma Access 如何在自動調整事件之後配置和佈建輸出 IP 位址的範例。

自動調整事件—如果大量行動使用者同時登入一個行動使用者位置，則該事件可能會導致 Prisma Access 配置另一組兩個輸出 IP 位址，以容納大量使用者。在您已將前兩個輸出 IP 位址列入允許清單之後，自動調整事件之前的狀態會將兩個輸出 IP 位址顯示為列入允許清單，其中已確認狀態為 **2/2 Egress IPs Confirmed Allow Listed**（**2/2** 輸入 **IP** 已確認列入允許清單）、佈建狀態為 **Provisioned**（已佈建），以及自動調整狀態為 **Allowed**（已允許），如下列螢幕擷取畫面中香港位置所示。

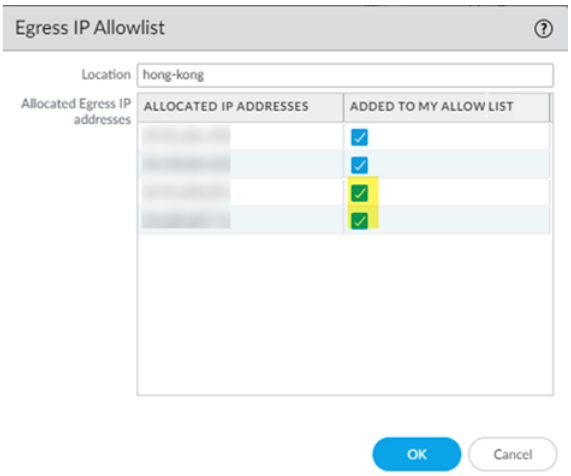



如果大量行動使用者同時登入香港位置，則 Prisma Access 會使備份輸出 IP 位址作用中，並配置另外兩個 IP 位址，並使其中一個 IP 位址作用中。發生自動調整事件時，輸出 IP 位址已配置但未佈建、已確認狀態為 **2/4 Egress IPs Confirmed Allow Listed**（**2/4** 輸入 **IP** 已確認列入允許清單），並且佈建狀態顯示 **Provisioned without enough capacity**（已佈建但沒有足夠的容量）。此外，自動調整狀態會顯示 **Not Allowed**（不允許），這表示如果發生自動調整事件，則 Prisma Access 不會將額外的輸出 IP 位址佈建至您的部署。

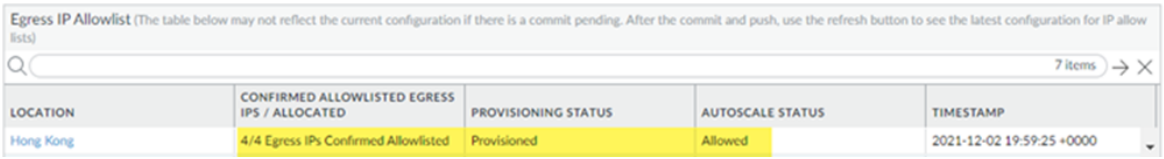



 ©2025 Palo Alto Networks, Inc.

在您已將新的輸出 IP 位址新增至允許清單之後，請選取位置名稱；然後，針對已新增的兩個 IP 位址選取 **Added to My Allow List**（已新增至我的允許清單），然後 **Commit and Push**（提交並推送）您的變更。




完成時，香港位置會顯示所有四個輸出 IP 位址都已確認並佈建，且自動調整作用中。




# GlobalProtect 應用程式升級

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

Prisma Access 託管您組織中 macOS 和 Windows 使用者可以從 Prisma Access 入口網站下載的 GlobalProtect 應用程式版本。Prisma Access 提供 GlobalProtect 應用程式的數個版本，而且您可以選擇使其中一個版本成為作用中版本。您還可以管理行動使用者對 GlobalProtect 應用程式的存取，或執行分階段升級。

- 為 Prisma Access 選取作用中的 GlobalProtect 應用程式版本
- 允許使用者升級 GlobalProtect 應用程式
- 錯開 GlobalProtect 應用程式更新


©2025 Palo Alto Networks, Inc.

# 為 Prisma Access 選取作用中的 GlobalProtect 應用程式版本

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

Prisma Access 為您組織中的 Windows 和 macOS 使用者管理 GlobalProtect 應用程式版本。雖然 Prisma Access 託管多個 GlobalProtect 應用程式版本，但其中只有一個託管版本作用中。當行動使用者登入 Prisma Access 入口網站時，作用中版本是可供行動使用者在其 Windows 和 macOS 裝置上下載並安裝的版本。

您可以在多租用戶部署中選取多個 GlobalProtect 版本。您套用的 GlobalProtect 應用程式版本設定是根據租用戶，而不是全域；您根據每個租用戶控制應用程式版本。

某些功能（例如 IP 最佳化）要求使用者處於足夠更新的 GlobalProtect 版本上。繼續閱讀以瞭解如何在 Prisma Access 中選取作用中的 GlobalProtect 應用程式版本。.

- Strata Cloud Manager
- Panorama

## 為 **Prisma Access (Managed by Strata Cloud Manager)** 選取作用中的 **GlobalProtect** 應用程式版本

您可以完成以下步驟，將目前作用中的版本取代為來自 [Service Setup（服務設定）] 頁面的另一個託管版本。

**STEP 1 |** 選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Mobile Users**（行動使用者），然後尋找 **GlobalProtect Connection**（**GlobalProtect** 連線）面板。

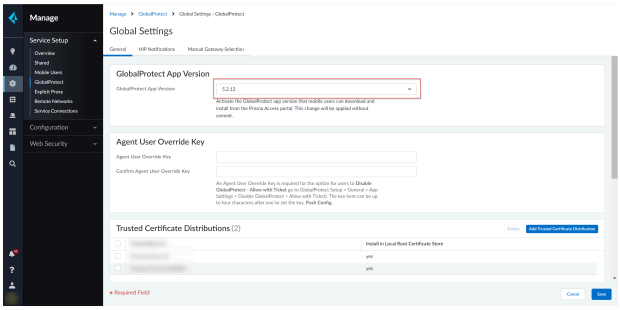
**STEP 2 |** 如果尚未啟用 GlobalProtect，請選取 **GlobalProtect Setup**（**GlobalProtect** 設定）或 **Enable**（啟用） > **GlobalProtect Setup**（**GlobalProtect** 設定）。

**STEP 3 |** 選取 **GlobalProtect App**（**GlobalProtect** 應用程式）頁籤，然後編輯 **Global App Settings**（全域應用程式設定）。


©2025 Palo Alto Networks, Inc.

**STEP 4 |** 在 **Global Settings**（全域設定）頁面的 **General**（一般）頁籤上，選取您想要允許行動使用者從 Prisma Access 入口網站下載並安裝的 **GlobalProtect App Version**（**GlobalProtect** 應用程式版本）。

下拉式清單中指出了作用中版本。




為 **Prisma Access (Managed by Panorama)** 選取作用中的 **GlobalProtect** 應用程式版本

如果您目前作用中的版本已終止使用，Prisma Access 會通知您，並要求您啟動支援的版本。

您可以完成以下步驟，將目前作用中的版本取代為來自 [Service Setup（服務設定）] 頁面的另一個託管版本。

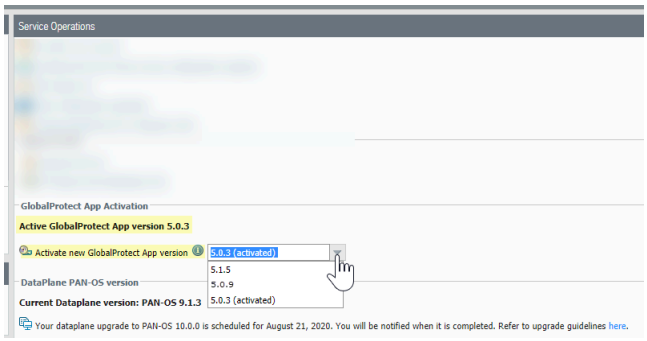
如果您要在 FedRAMP 環境中使用 *Prisma Access*，則必須使用經過 *FIPS* 認證的 *GlobalProtect* 版本，即版本 *5.1.4*。如果您從 *5.1.4* 變更預設的 GlobalProtect 版本，則無法從 *Panorama UI* 中選取版本 *5.1.4*，而且必須透過 *Palo Alto Networks* 技術支援開啟支援案例以將其加回來。

**STEP 1 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定）。

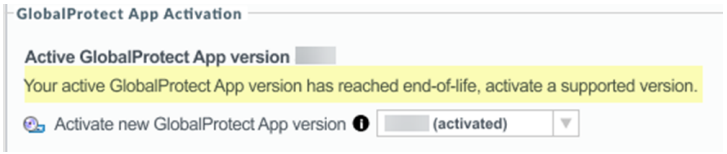

©2025 Palo Alto Networks, Inc.

**STEP 2 |** 選取 **Activate new GlobalProtect App version**（啟動新的 **GlobalProtect** 應用程式版本)。

下拉式清單中指出了作用中版本。

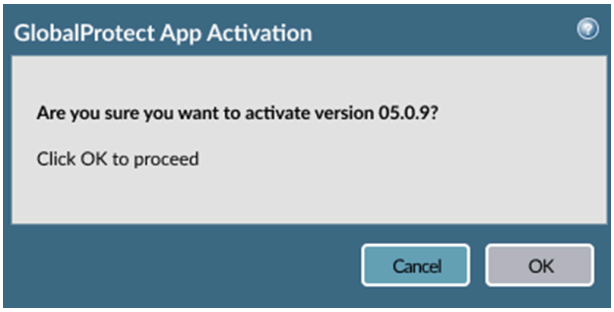



如果您目前的 *GlobalProtect* 版本已終止使用 *(EoL)*，則 *[Service Setup*（服務設定）*]* 頁面上的這個區域中會顯示一則訊息；如果您收到此訊息，請繼續下一個步驟來升級您的 *GlobalProtect* 應用程式版本。

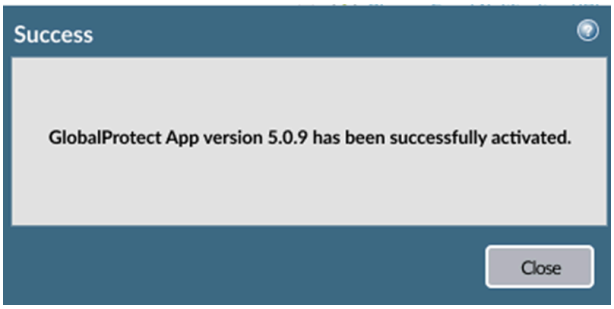



**STEP 3 |** 選取您要升級至哪個版本，然後按一下 **OK**（確定）。

即會顯示一個視窗來驗證您的選項。




在應用程式啟動之後，您會收到一則成功訊息。




 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 檢視 [System Status（系統狀態）] 頁面，以驗證 **Active GlobalProtect App version**（作用中的 **GlobalProtect** 應用程式版本）。

## 允許使用者升級 GlobalProtect 應用程式

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

瞭解如何控制您的行動使用者對 GlobalProtect 應用程式版本的存取，以進行 Prisma Access GlobalProtect 部署。

- Strata Cloud Manager
- Panorama

### 允許使用者升級 GlobalProtect 應用程式 (Strata Cloud Manager)

您可以管理行動使用者對 Prisma Access 託管的作用中 GlobalProtect 應用程式版本的存取。若要在 Prisma Access (Managed by Strata Cloud Manager) 中執行此動作，請設定 **Upgrade Global Protect**（升級 **Global Protect**） 設定。對於 Prisma Access (Managed by Strata Cloud Manager)，請完成下列步驟。

**STEP 1 |** 選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Mobile Users**（行動使用者），然後尋找 **GlobalProtect Connection**（**GlobalProtect** 連線）面板。

**STEP 2 |** 如果尚未啟用 GlobalProtect，請選取 **GlobalProtect Setup**（**GlobalProtect** 設定）或 **Enable**（啟用） > **GlobalProtect Setup**（**GlobalProtect** 設定）。

**STEP 3 |** 選取 **GlobalProtect App**（**GlobalProtect** 應用程式）頁籤，然後選取 **Add App Settings**（新增應用程式設定）。

**STEP 4 |** 在 **App Configuration**（應用程式設定）區域中，選取 **Upgrade GlobalProtect App**（升級 **GlobalProtect** 應用程式）中的一個選項，以指定行動使用者是否可以將 GlobalProtect 應用程式版本升級至 Prisma Access 上託管的作用中版本，以及如果他們可以，是否可以選擇何時升級：

- **Allow when user accepts the upgrade Prompt**（使用者接受升級提示時允許）（預設值）—啟動新版本時提示使用者，並允許使用者在方便時升級其軟體。
- 不允許 — 防止使用者升級應用程式軟體。
- 允許手動 — 允許使用者手動檢查，並在 GlobalProtect 應用程式中選取 **Check Version**（檢查版本）來啟動升級。
- 允許（以透明方式）—每當入口網站上有可用的新版本時，即自動升級應用程式軟體。
- **Allow when the user is in the corporate network**（使用者位於公司網路時允許）—每當入口網站中有新版本可用，等到端點內部連線到公司網路後，就會自動升級應用程式軟體。這可防止因為連線頻寬不足而在升級時導致系統延遲。

 ©2025 Palo Alto Networks, Inc.

### 允許使用者升級 GlobalProtect 應用程式 (Panorama)

您可以管理行動使用者對 Prisma Access 託管的作用中 GlobalProtect 應用程式版本的存取。若要在 Prisma Access (Managed by Strata Cloud Manager) 中執行此動作，請設定 **Upgrade Global Protect**（升級 **Global Protect**） 設定。對於 Prisma Access (Managed by Panorama)，請完成下列步驟。

**STEP 1 |** 選取 **Network**（網路） > **GlobalProtect** > **Portals**（入口網站）。

**STEP 2 |** 從 **Template**（範本）下拉式清單中，選取 **Mobile_User_Template**。

**STEP 3 |** 選取 **GlobalProtect_Portal** 以編輯 Prisma Access 入口網站設定。

**STEP 4 |** 選取 **Agent**（代理程式）頁籤，然後選取應用程式設定。

**STEP 5 |** 選取 **App**（應用程式）頁籤。

**STEP 6 |** 在 **App Configuration**（應用程式設定）區域中，選取 **Allow User to Upgrade GlobalProtect App**（允許使用者升級 **GlobalProtect** 應用程式）中的一個選項，以指定行動使用者是否可以將 GlobalProtect 應用程式版本升級至 Prisma Access 上託管的作用中版本，以及如果他們可以，是否可以選擇何時升級：

- **Allow with Prompt**（透過提示允許）（預設值）—啟動新版本時提示使用者，並允許使用者在方便時升級其軟體。
- 不允許 — 防止使用者升級應用程式軟體。
- 允許手動 — 允許使用者手動檢查，並在 GlobalProtect 應用程式中選取 **Check Version**（檢查版本）來啟動升級。
- 允許（以透明方式）—每當入口網站上有可用的新版本時，即自動升級應用程式軟體。
- 內部—每當入口網站中有新版本可用，等到端點內部連線到公司網路後，就自動升級應用程式軟體。這可防止因為連線頻寬不足而在升級時導致系統延遲。

## 錯開 GlobalProtect 應用程式更新

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

如果您管理一家大型組織，可能想要分階段將行動使用者更新至最新版本的 GlobalProtect 應用程式。例如，您可以先指派較小的群組，以更新其 GlobalProtect 應用程式，然後再將更新推出至您組織中的所有人。若要這樣做，請完成以下工作。

**STEP 1 |** 如果您尚未建立它，請為您想要將 GlobalProtect 應用程式更新推出至其中的第一個使用者群組建立一個使用者群組。

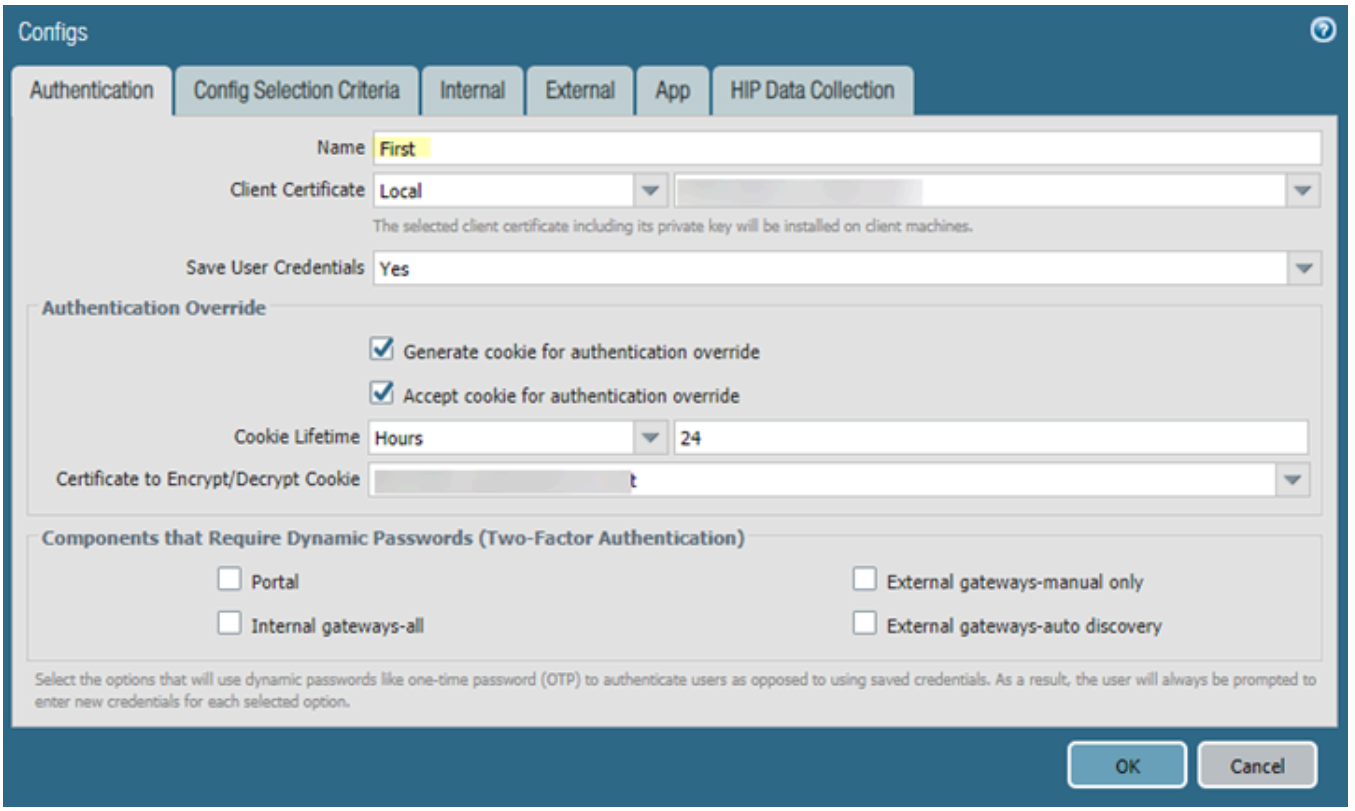
您可以使用，將使用者對應至群組，或選取 **Device**（裝置） > **Local User Database**（本機使用者資料庫） > **User Groups**（使用者群組）來手動建立一個群組。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 建立新的 GlobalProtect 代理程式設定，以用於第一個使用者群組。

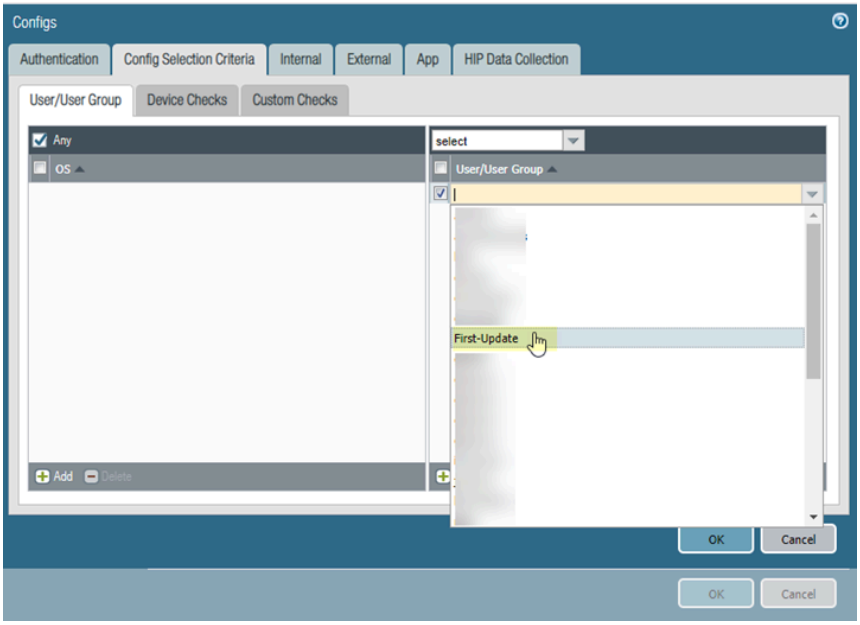
1. 在 Panorama 中，選取 **Network**（網路） > **GlobalProtect** > **Portals**（入口網站）。
2. 從 **Template**（範本）下拉式清單中，選取 **Mobile_User_Template**。
3. 選取 **GlobalProtect_Portal** 以編輯 Prisma Access 入口網站設定。
4. 選取 **Agent**（代理程式）頁籤。
5. 選取 **DEFAULT** 設定並 **Clone**（複製）它。

   您也可以 **Add**（新增） 設定；但複製現有設定會複製新設定所需的資訊。
6. 指定設定的 **Name**（名稱）。



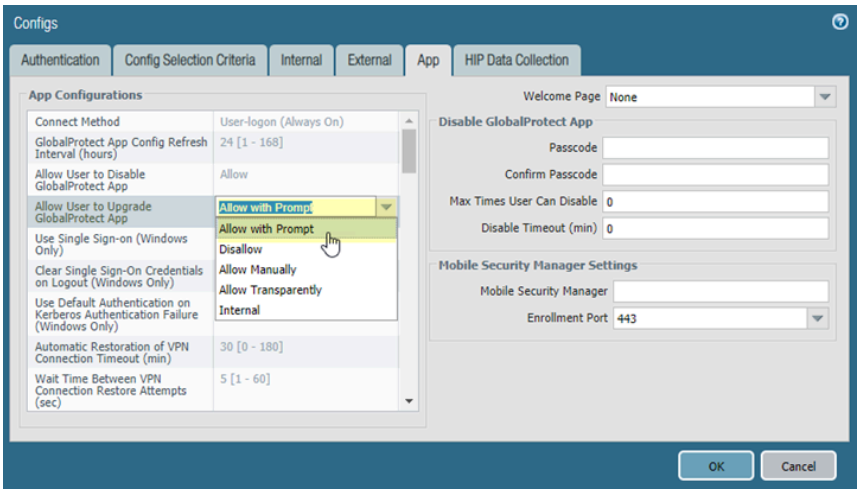

7. 選取 **Config Selection Criteria**（設定選取準則）頁籤。
8. 在 **User/User Group**（使用者/使用者群組）區域中，選取您在步驟 1 建立的使用者。

 ©2025 Palo Alto Networks, Inc.




9. 選取 **App**（應用程式）頁籤。
10. 將 **Allow User to Upgrade GlobalProtect App**（允許使用者升級 **GlobalProtect** 應用程式）變更為 **Allow with Prompt**（透過提示允許）或 **Allow Transparently**（透明允許）。

    **Allow with Prompt**（透過提示允許）會在新版本啟動時提示使用者，並允許他們在方便時升級其軟體；每當新版本在入口網站上變成可用時，**Allow Transparently**（透明允許）就會自動升級應用程式軟體。

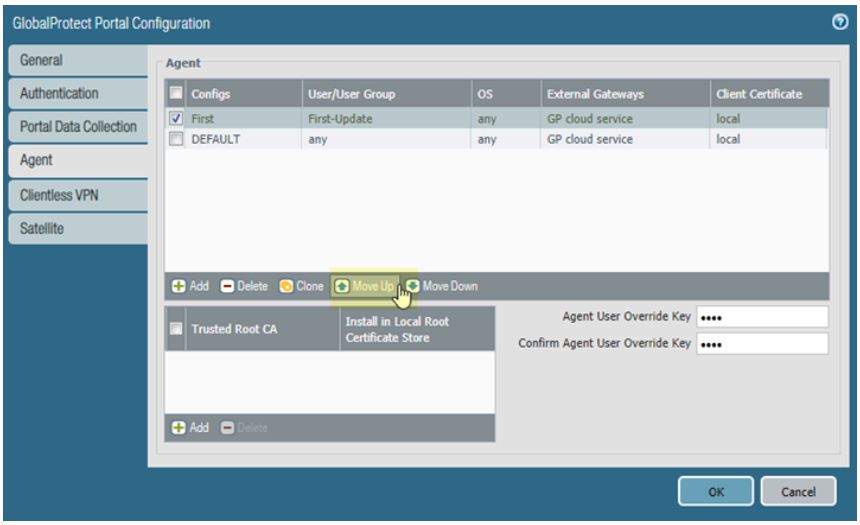



11. 按一下 **OK**（確定）儲存您的變更。

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 選取 **Move Up**（上移）以將您的設定移到預設設定之上。

當應用程式連線時，入口網站會將封包中的來源資訊與您已定義的代理程式組態進行比較。藉助安全性規則評估，入口網站會從清單頂端開始尋找符合項。找到符合項目時，會將對應的設定傳遞給應用程式。




**STEP 4 |** 對於 **DEFAULT** 設定，重複這些步驟，但將 **Allow User to Upgrade GlobalProtect App**（允許使用者升級 **GlobalProtect** 應用程式）變更為 **Disallow**（不允許），以防止用戶更新至最新的 GlobalProtect 應用程式軟體。

**STEP 5 |** 當您想要讓其餘使用者更新其應用程式時，請在 **DEFAULT** 設定中將 **Allow User to Upgrade GlobalProtect App**（允許使用者升級 **GlobalProtect** 應用程式）變更為允許它的選項（**Allow with Prompt**（透過提示允許）或 **Allow Transparently**（透明允許））。

# 整合 Prisma Access 與內部部署 GlobalProtect 閘道

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
|---|---|
| • Prisma Access (Managed by Panorama)<br>• Prisma Access (Managed by Strata Cloud Manager) | • Prisma Access 授權 |

Prisma Access 可讓您將 Palo Alto Networks 安全性平台擴展到您的遠端網路位置和行動使用者，而無需建置自己的全域安全性基礎結構並擴大您的營運能力。如果已在您已有基礎結構管理它的區域中部署 GlobalProtect 閘道，您可以透過設定 Prisma Access 來利用這項投資，適時將行動使用者導向至您現有的外部閘道。

您可以管理 Prisma Access 和內部部署閘道的優先順序，這允許您為內部部署和 Prisma Access 閘道指定優先順序。管理員無法指定行動使用者連線到特定的 Prisma Access 閘道；不過，管理員可以允許行動使用者手動選取特定的 Prisma Access 閘道，方法是使用 GlobalProtect 應用程式。

您無法使用自己的入口網站搭配 *Prisma Access*。您只能使用在為行動使用者佈建 *Prisma Access* 時部署的入口網站。


©2025 Palo Alto Networks, Inc.

- Strata Cloud Manager
- Panorama

## 整合 Prisma Access 與內部部署 GlobalProtect 閘道 (Prisma Access (Managed by Strata Cloud Manager))

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** 將您的內部部署閘道新增到代理程式設定中的閘道清單。

1. 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **GlobalProtect**，並選取 **GlobalProtect App**（**GlobalProtect** 應用程式）頁籤。
2. **Add App Settings**（新增應用程式設定）。




3. **Add**（新增）外部閘道。




如果您新增代理程式設定，並且想要將 *Prisma Access* 閘道新增到該設定中的外部閘道清單，則必須將 ***Name***（名稱） 設定為 ***GP cloud service***（***GP*** 雲端服務），並將 ***Address***（位址）設定為 ***gpcloudservice.com***。請完全按照所示輸入這些值，並且您無法將這些值的任何一個用於非 *Prisma Access* 閘道。

4. 輸入閘道的 **Name**（名稱），並在 **Address**（位址）欄位中指定閘道的 **FQDN** 或 **IP** 位址；此值必須與閘道憑證中的通用名稱 (CN) 完全相符。
5. （選用） 如果您想要行動使用者僅在位於對應區域時才連線到閘道，**Add**（新增）**Source Region**（來源區域）以將閘道限制為該區域。例如，如果您在法國有一個閘道，則將會選取 FR（法國）。如果您在瑞典有一個閘道，則將會選取 SE（瑞典）。

   這樣做的一個好處是，使用者將能夠存取一個閘道，啟用以他們自己的語言存取網際網路資源。
6. （選用）在您的閘道設定中指定優先順序。

   您可以將內部部署閘道設定為更高的優先順序或較低的優先順序。

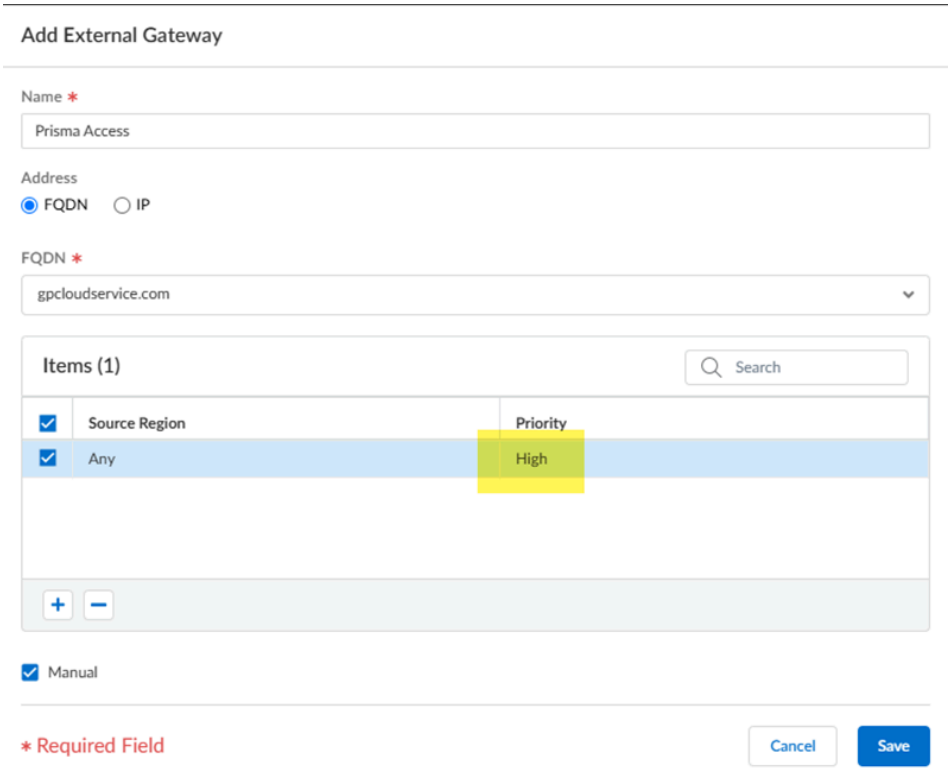
   - 若要將內部部署閘道設定為低於預設 Prisma Access 閘道的優先順序，請將 **Priority**（優先順序）設定為 **High**（高）或 **Medium**（中）。

     如果您新增更多閘道，並想要為每個閘道設定不同的優先順序，則可以將 **Priority**（優先順序）設定為 **High**（高）、**Medium**（中）、**Low**（低）或 **Lowest**（最低）。

 ©2025 Palo Alto Networks, Inc.

- 若要將內部部署閘道設定為比預設值更高的優先順序，請將 **Priority**（優先順序）設定為 **Highest**（最高）。

  如果要將內部部署閘道設定為更高的優先順序，還必須編輯預設 **Prisma Access** 閘道，並將優先順序設定為低於 **Highest**（最高）的 **Priority**（優先順序）。

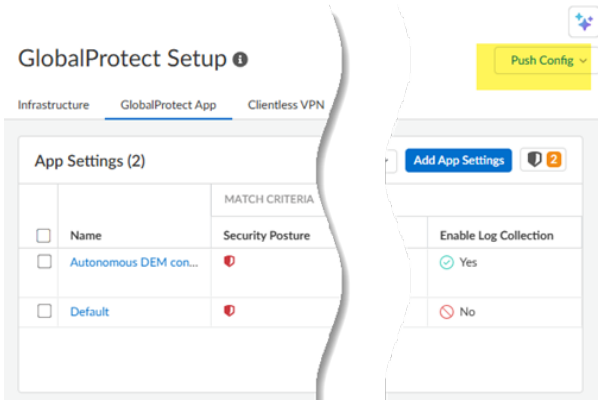



7. 選取 **Manual**（手動）。

   選取此核取方塊，以允許 GlobalProtect 使用者在其 GlobalProtect 應用程式中手動選取此外部閘道。

**STEP 2 |** **Save**（儲存）變更。

**STEP 3 |** **Push Config**（推送設定）。




 ©2025 Palo Alto Networks, Inc.

## 整合 Prisma Access 與內部部署 GlobalProtect 閘道 (Prisma Access (Managed by Panorama))

若要設定其中一個混合 Prisma Access 部署，您必須在Mobile_User_Template 內編輯 GlobalProtect_Portal 設定，才能將內部部署閘道新增適當的區域。

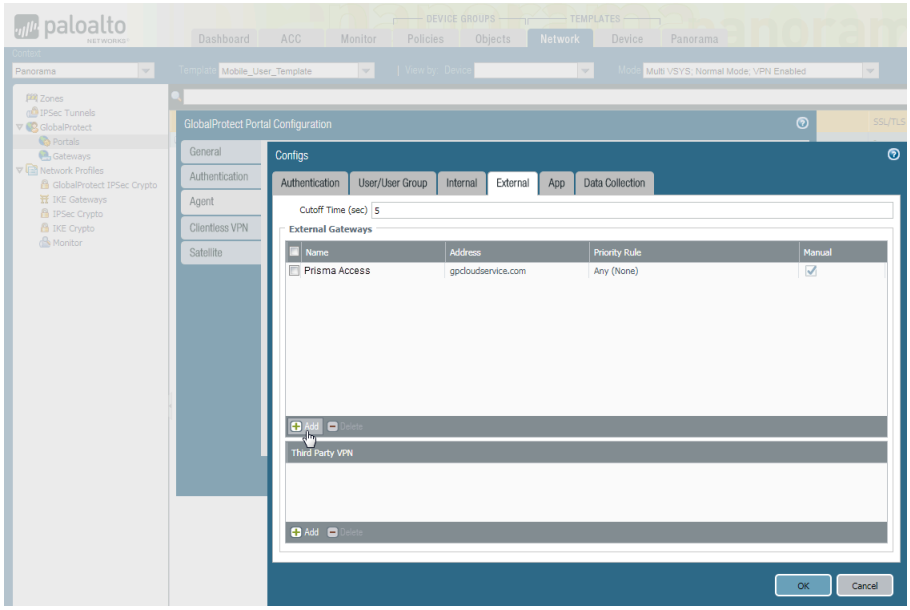
**STEP 1 |** 編輯 Prisma Access 入口網站設定。

1. 若要將現有閘道新增到可用閘道清單，請選取 **Network**（網路） > **GlobalProtect** > **Portals**（入口網站）。
2. 從 **Template**（範本）下拉式清單中，選取 **Mobile_User_Template**。
3. 選取 **GlobalProtect_Portal** 以編輯 Prisma Access 入口網站設定。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 將您的內部部署閘道新增到代理程式設定中的閘道清單。

1. 選取 **Agent**（代理程式）頁籤，然後選取 **DEFAULT**（預設）代理程式設定或 **Add**（新增）設定。
2. 選取 **External**（外部）頁籤和，並**Add**（新增） 您的內部部署閘道。




如果您新增代理程式設定，並且想要將 *Prisma Access* 閘道新增到該設定中的外部閘道清單，則必須將 ***Name***（名稱） 設定為 ***GP cloud service***（***GP*** 雲端服務），並將 ***Address***（位址）設定為 ***gpcloudservice.com***。您必須完全按照所示輸入這些值，並且您無法將這些值的任何一個用於非 *Prisma Access* 閘道。

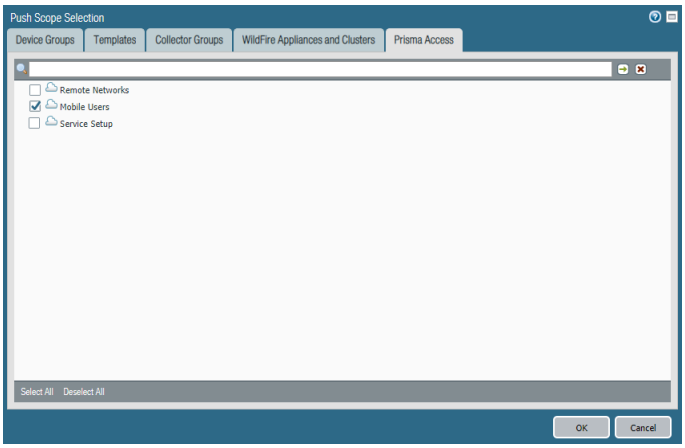
3. 輸入閘道的 **Name**（名稱），並在 **Address**（位址）欄位中指定閘道的 **FQDN** 或 **IP** 位址；此值必須與閘道憑證中的通用名稱 (CN) 完全相符。
4. （選用） 如果您想要行動使用者僅在位於對應區域時才連線到閘道，**Add**（新增）**Source Region**（來源區域）以將閘道限制為該區域。例如，如果您在法國有一個閘道，則將會選取 FR（法國）。如果您在瑞典有一個閘道，則將會選取 SE（瑞典）。

   這樣做的一個好處是，使用者將能夠存取一個閘道，啟用以他們自己的語言存取網際網路資源。
5. （選用）設定閘道的優先順序。
6. 視需要設定其他 agent settings（代理程式設定）以完成代理程式設定。
7. 按一下確定儲存入口網站設定。

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 將您的所有變更提交到 Panorama，並將設定變更推送到 Prisma Access。

1. 按一下 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**）。
2. 按一下 **Commit**（提交） > **Push to Devices**（推送至裝置），然後按一下 **Edit Selections**（編輯選取項目）。
3. 在 **Prisma Access** 頁籤中，請確保已選取 **Prisma Access for users**，然後按一下 **OK**（確定）。




4. 按一下 **Push**（推送）。

## 設定 Prisma Access 和內部部署閘道的優先順序

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
|---|---|
| • Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

您可以選取實際上最接近行動使用者的內部部署閘道，並允許使用者連線至不同的閘道（內部部署或雲端），以確保行動使用者在變更位置時可以安全存取。您也可以指定與行動使用者位於相同國家/地區或語言區域的閘道優先順序。

如果要求使用者連線至特定 Prisma Access閘 道，您可以允許行動使用者手動選取特定 Prisma Access 閘道。行動使用者會使用安裝在其端點上的 GlobalProtect 應用程式選取其中一個 Prisma Access 閘道。

完成下列工作流程，在 Prisma Access 中設定閘道優先順序。

- 為內部部署和 Prisma Access 閘道設定相同的閘道優先順序
- 為內部部署閘道設定更高的閘道優先順序
- 為多個內部部署閘道設定更高的優先順序
- 設定 Prisma Access 和內部部署閘道的優先順序

### 為內部部署和 **Prisma Access** 閘道設定相同的閘道優先順序

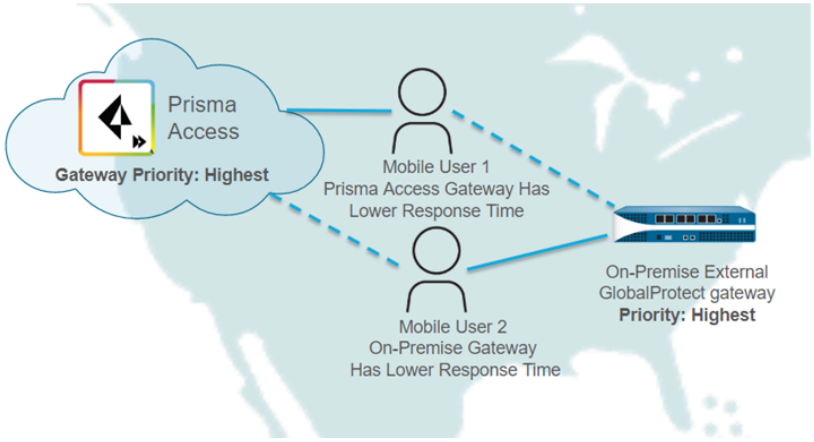
若要為行動勞動力（無論他們位於何處）啟用安全存取，您都可以為內部部署 GlobalProtect 閘道和 Prisma Access 閘道設定相同的優先順序。GlobalProtect 應用程式會使用多重閘道設定中的閘道優先順序來確定偏好的閘道。

 ©2025 Palo Alto Networks, Inc.

如果行動使用者最常靠近內部部署閘道，您可以使用此設定。當使用者變更位置時，GlobalProtect 應用程式會根據最高優先順序和最低回應時間選擇另一個閘道（內部部署或 Prisma Access 閘道）。

下圖顯示了北美兩個行動使用者的範例設定。您可以將 Prisma Access 閘道和內部部署閘道的閘道優先順序設定為 **Highest**（最高）。

在此範例中，使用者 1 的 GlobalProtect 應用程式確定 Prisma Access 閘道具有內部部署閘道更低的回應時間，而使用者 2 的 GlobalProtect 應用程式確定內部部署閘道具有較低的回應時間。由於所有閘道都有相同的優先順序，因此使用者 1 會根據較低的回應時間連線到 Prisma Access 閘道，而使用者 2 則連線到內部部署閘道。




為內部部署閘道設定更高的閘道優先順序

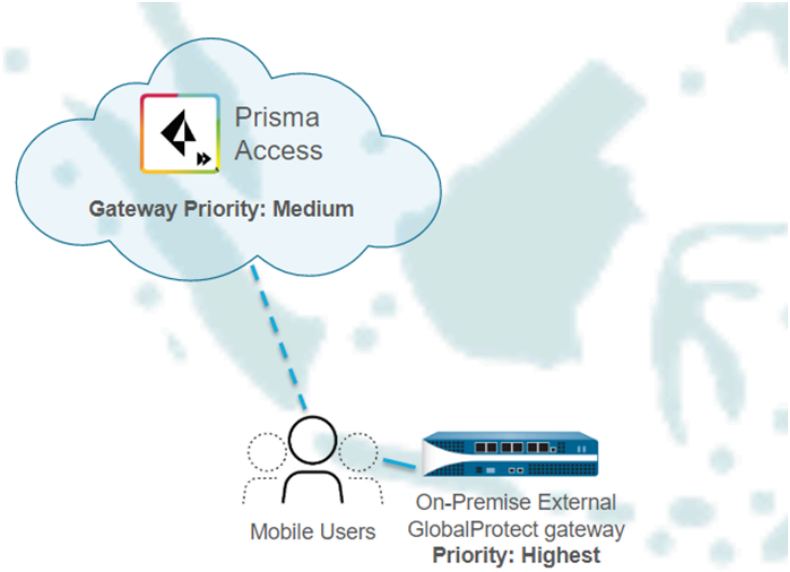
在您想要引導行動使用者使用內部部署閘道而不是 Prisma Access 閘道的情況下，請指定具有來源區域且優先順序比 Prisma Access 閘道更高的內部部署閘道。

下圖顯示了印尼行動使用者的範例設定。若要避免行動使用者可能連線到新加坡中最接近的 Prisma Access 閘道，請將印尼內部部署閘道的閘道優先順序設定為 **Highest**（最高），並將 Prisma Access 閘道的優先順序設定為 **Medium**（中）。

此範例還為內部部署閘道指定印尼的來源區域。我們基於下列原因建議指定來源區域：

- 指定內部部署閘道的來源區域可讓區域中的使用者存取該閘道，並防止該區域以外的使用者連線到該閘道。在此範例中，只有印尼行動使用者才能連線到具有印尼來源區域的內部部署閘道，而優先順序較高意味著內部部署閘道優先於 Prisma Access 閘道。
- 如果您為印尼內部部署閘道設定 **Any**（任何）的來源區域，組織中的每個行動使用者都會偏好印尼的內部部署閘道，因為其優先順序更高且可在全世界存取。此設定意味著行動使用者可能永遠不會連線到 Prisma Access 閘道。


©2025 Palo Alto Networks, Inc.




為多個內部部署閘道設定更高的優先順序

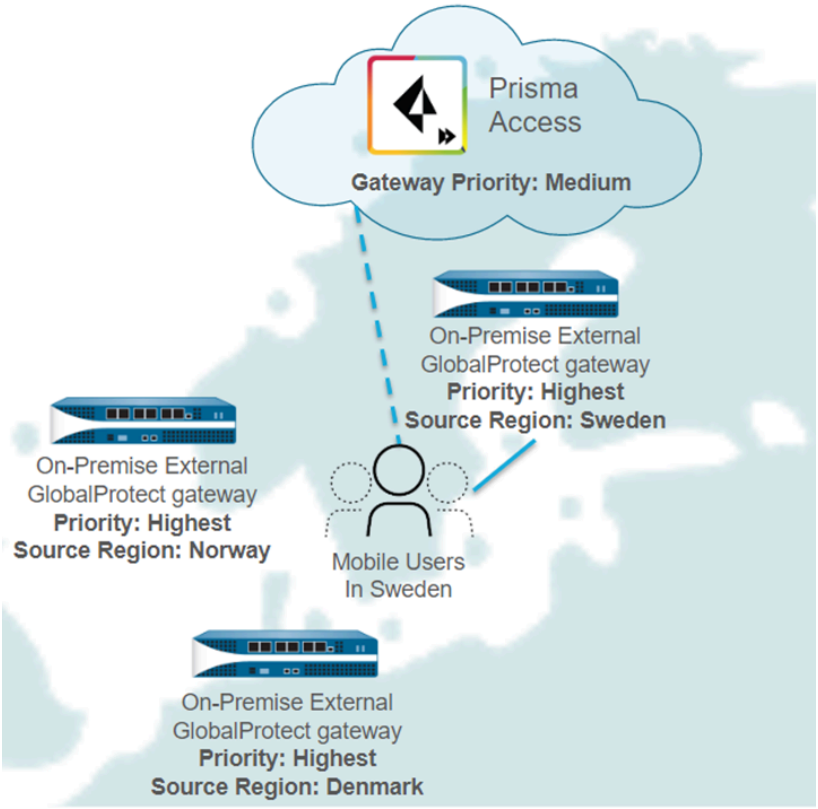
若要確保網際網路的流量保持在語言特定區域中，您可以在多個來源區域中設定多個閘道，同時將內部部署閘道的優先順序設定為 **Highest**（最高），而將 Prisma Access 閘道的優先順序設定為 **Medium**（中）。

下圖顯示了斯堪的納維亞行動使用者的範例設定。使用此設定，當行動使用者存取網際網路網站時，網站會其語言特有的字元編碼集。

在此範例中，您可以設定具有丹麥、挪威和瑞典來源區域的內部部署閘道。您將這些閘道的優先順序設定為 **Highest**（最高），並將 Prisma Access 閘道的優先順序設定為 **Medium**（中）。指定內部部署閘道的來源區域可讓這些區域的使用者存取這些閘道，並防止這些區域以外的使用者連線到這些閘道。

在此範例中，由於來源區域和更高的閘道優先順序，瑞典行動使用者的 GlobalProtect 應用程式會選取瑞典的內部部署閘道。

 ©2025 Palo Alto Networks, Inc.




設定 **Prisma Access** 和內部部署閘道的優先順序

使用此工作流程，為使用內部部署閘道搭配 Prisma Access 的部署設定優先順序。

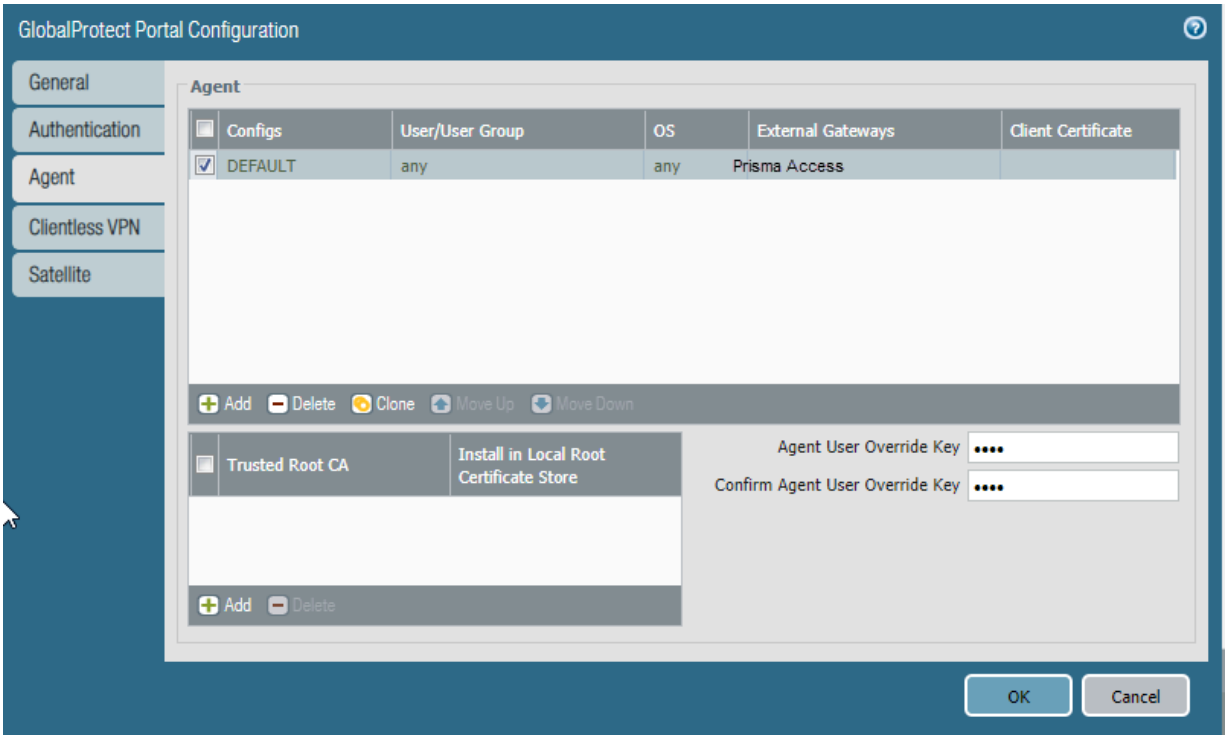
**STEP 1 |** 登入 Prisma Access。

**STEP 2 |** 在 **Mobile_User_Template** 範本中，選取 **Network**（網路） > **GlobalProtect** > **Portals**（入口網站）。

**STEP 3 |** 按一下 **Name**（名稱）欄位中的入口網站名稱。

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 按一下 **Agent**（代理程式）頁籤。




**STEP 5 |** 按一下要設定的代理程式名稱。

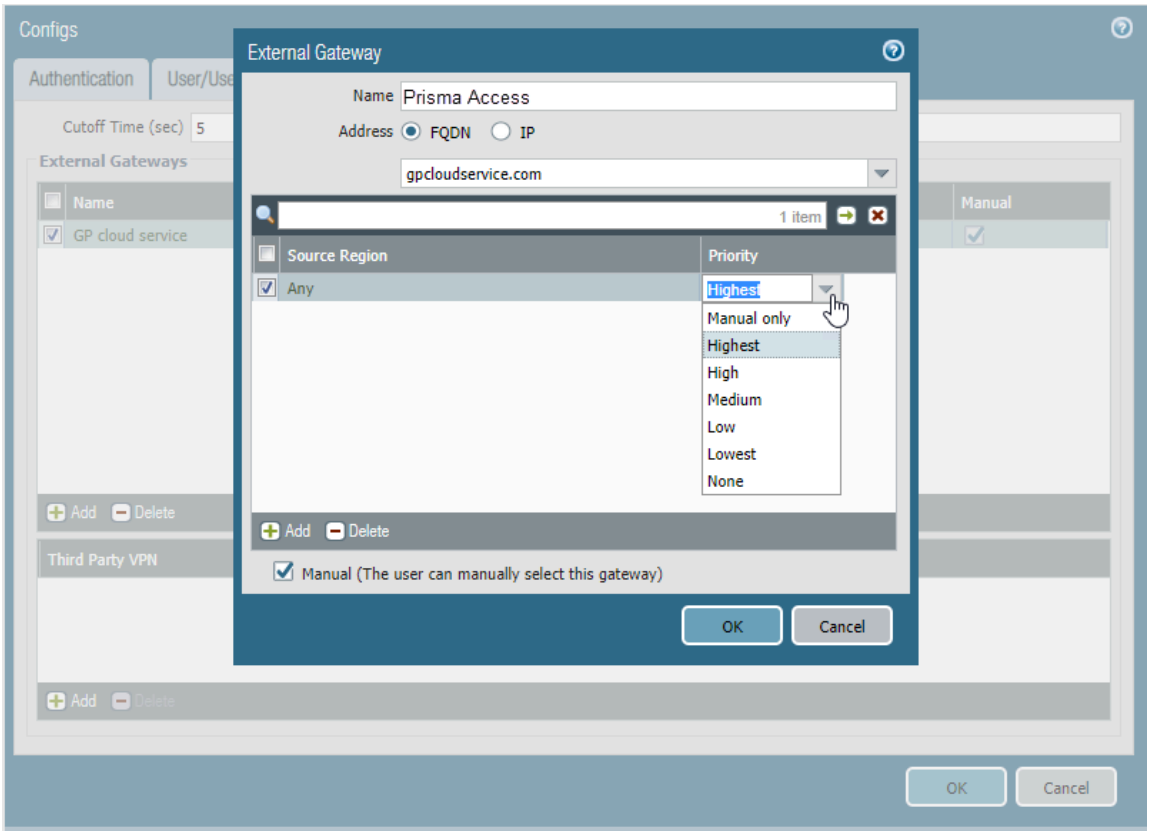
預設代理程式名為 **DEFAULT**。

**STEP 6 |** 按一下 **External**（外部）頁籤。


©2025 Palo Alto Networks, Inc.

**STEP 7 |** 設定 Prisma Access 閘道的優先順序。

1. 按一下 **GP cloud service**（**GP** 雲端服務）。
2. 設定您偏好設定的優先順序。
   - 若要為內部部署和 Prisma Access 閘道設定相同的閘道優先順序，請將優先順序從 **None**（無）變更為 **Highest**（最高）。
   - 若要為內部部署閘道設定更高的閘道優先順序，或為多個內部部署閘道設定更高的優先順序，請將優先順序從 **None**（無）變更為 **Medium**（中）。




3. 請確定已選取 **Manual**（手動）核取方塊。

   核取**Manual**（手動）核取方塊可確保行動使用者可在需要時選取特定 Prisma Access 閘道。

   請勿新增 *Prisma Access* 閘道的來源區域；您指定的任何區域都不會套用至設定。

 ©2025 Palo Alto Networks, Inc.

4. 按一下 **OK**（確定）。


©2025 Palo Alto Networks, Inc.

**STEP 8 |** 將一或多個內部部署外部閘道 **Add**（新增）至您的設定。

1. 輸入閘道的描述性 **Name**（名稱）。

   您輸入的名稱應該符合您在設定閘道時所定義的名稱，而且該名稱應該具有足夠的描述性，讓使用者能夠知道他們連線至其中的閘道位置。

2. 在 [Address（位址）] 欄位中輸入設定閘道所在介面的 FQDN 或 IP 位址。

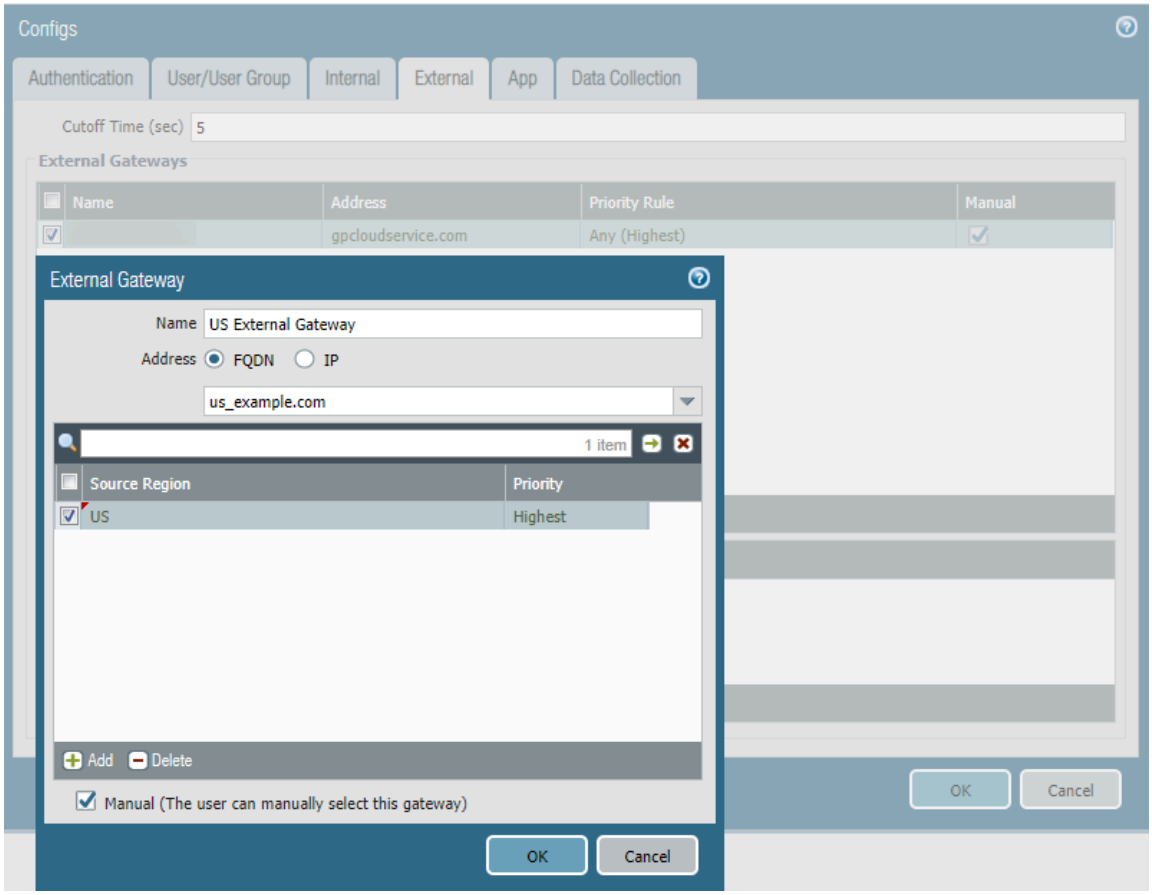
   您可以設定 IPv4 位址。您指定的位址必須與閘道伺服器憑證中的通用名稱 (CN) 完全符合。

3. 為內部部署閘道新增一或多個 **Source Regions**（來源區域），或選取 **Any**（任何）以讓閘道可供所有區域使用。

   如果您將內部部署外部閘道的優先順序設定高於 *Prisma Access* 閘道，我們建議您指定外部閘道的來源區域。如果您為區域指定 ***Any***（任何），*GlobalProtect* 應用程式可能永遠不會選取 *Prisma Access* 閘道，只會選取內部部署閘道，因為內部部署閘道的優先順序較高。

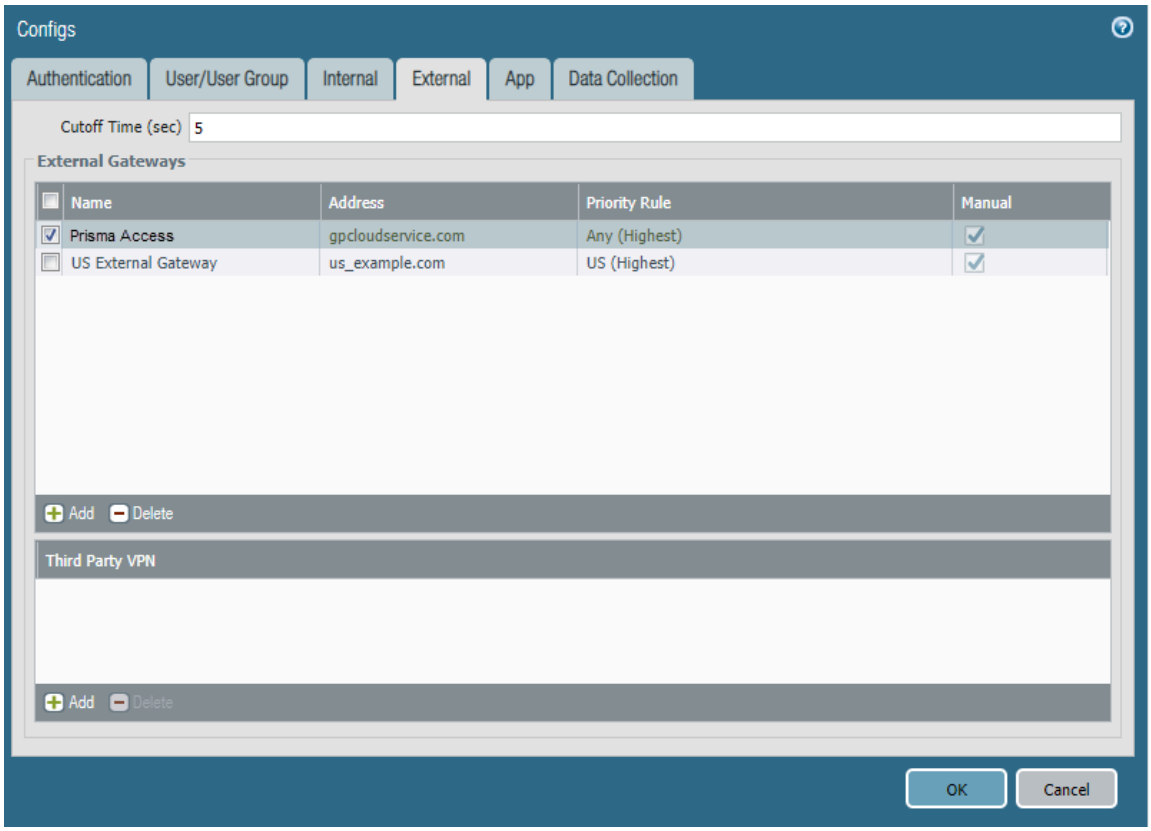
4. 選取 **Manual**（手動）核取方塊以讓使用者能夠手動切換至閘道。
5. 將內部部署閘道的 **Priority**（優先順序）設定為 **Highest**（最高）（預設值）。


©2025 Palo Alto Networks, Inc.




6. 按一下 **OK**（確定）。


©2025 Palo Alto Networks, Inc.





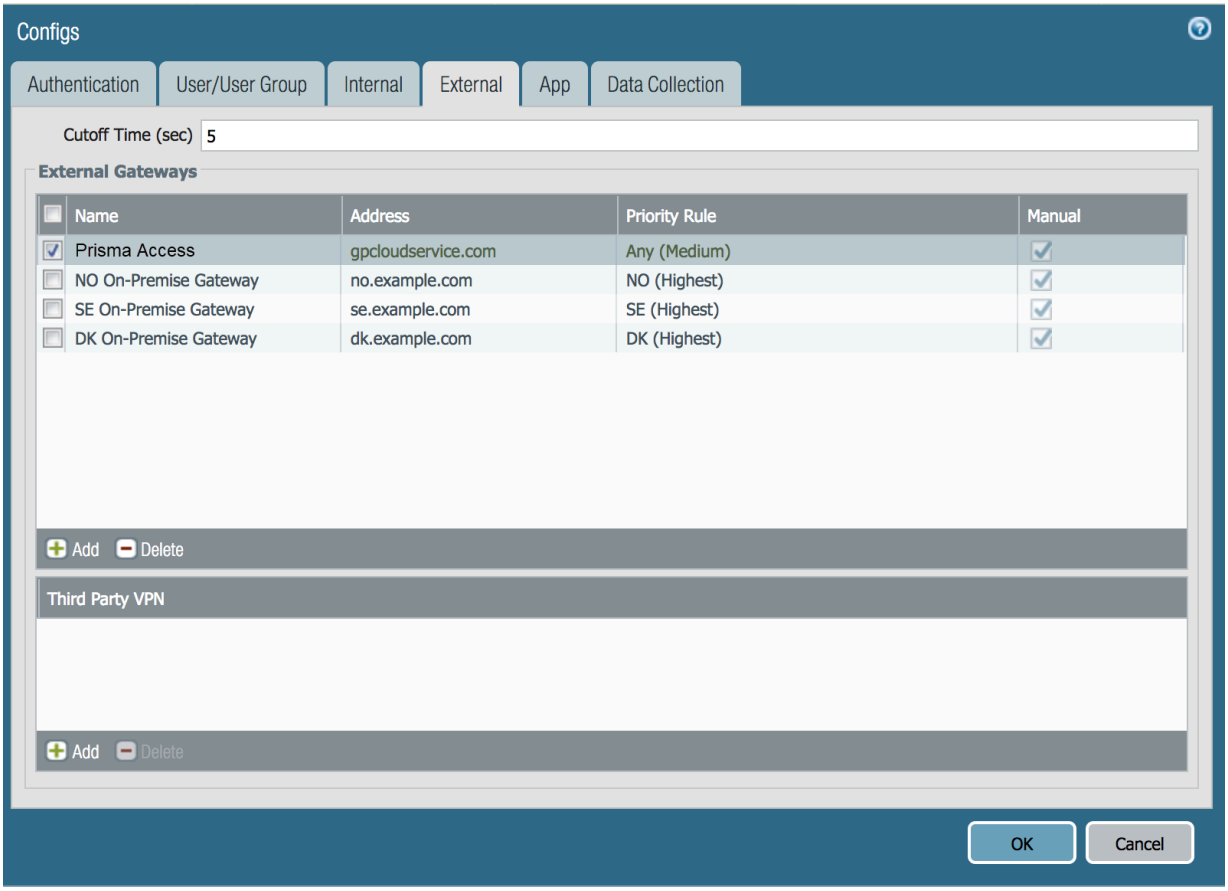
©2025 Palo Alto Networks, Inc.

**STEP 9 |** （選用）透過重複步驟 8 來設定其他閘道的優先順序。

請務必指定正確的來源區域。

下圖顯示一個範例設定，其中多個閘道具有挪威、瑞典和丹麥來源區域。請注意，已選取 **Manual**（手動）核取方塊，這表示行動使用者可以手動選取其中任何閘道。


©2025 Palo Alto Networks, Inc.





©2025 Palo Alto Networks, Inc.

# 行動使用者：明確 Proxy

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

Prisma Access by Palo Alto Networks 是一種安全服務邊緣 (SSE) 解決方案，其會提供一流的雲端 SWG 功能，包括進階 URL 篩選、SSL 解密、SaaS 應用程式控制，以及進階威脅防護。Prisma Access 利用由 Palo Alto Networks 完全管理的普遍且始終開啟的雲端原生基礎結構，實施新世代安全性部署。行動使用者和遠端網站可以根據公司政策安全地存取網際網路和 SaaS 應用程式。Prisma Access 提供靈活的連線選項：PAC 檔案、代理程式、無代理程式和站台對站台 IPSEC，確保任何舊版或替代雲端 Proxy 架構都可以在最少網路變更的情況下移到 Prisma Access。

明確 **Proxy**

Prisma Access 提供完整的雲端安全 Web 閘道 (SWG) 功能，包括基於雲端的明確 Proxy 連線方法。如果您組織的現有網路已使用明確 Proxy，並在您的用戶端端點上部署 PAC 檔案，則您可以順暢地從舊版 Proxy 型 SWG 解決方案移轉至 Prisma Access，以保護行動使用者的輸出網際網路流量。如果需要基於合規性目的使用 Proxy，您也可以使用明確 Proxy。明確 Proxy 使用行動使用者授權。

如果您使用多個 PAC 檔案，來定義如何將 Web 流量導向至不同的使用者或系統，則 Prisma Access 可讓您將這些 PAC 檔案與轉送設定檔建立關聯，以便您可以一次使用數個 PAC 檔案。此外，完全不需編寫 PAC 檔案，轉送設定檔即可讓您設定簡單的轉送規則，來定義 Web 流量的方向。


- 支援的位置
- 明確 Proxy 搭配 GlobalProtect 應用程式
  - Proxy 模式下的 GlobalProtect
  - 通道和 Proxy 模式下的 GlobalProtect
- 明確 Proxy 搭配 PAC 檔案
  - 使用 SAML 進行設定
  - 使用 Kerberos 進行設定
- 轉送設定檔
  - 多個 PAC 檔案支援
  - 轉送規則
  - 使用 GlobalProtect 轉送設定檔


**Prisma Access** 明確 **Proxy** 功能

 ©2025 Palo Alto Networks, Inc.

| 功能 | 說明 |
| --- | --- |
| App-ID | 不論攻擊者使用哪個連接埠、TLS/SSL 加密或技術逃避偵測，都會持續將所有應用程式分類。與套用應用程式分類之前依賴第三層和第四層作為第一控制層的舊版解決方案不同，Prisma Access 會套用 App-ID 以及其他第七層控制項 (例如 User-ID)。 |
| 使用者-ID | 與廣泛的使用者識別存放庫整合，以便您的政策遵循您的使用者和群組，無論其位置如何。 |
| SSL 解密 | 檢查政策並將其套用至 TLS/SSL 加密的流量。為了隱私權和法規合規性，您可以根據 URL、來源、目的地、使用者、使用者群組和連接埠彈性地啟用或停用解密。 |
| AI/ML 型偵測 | 提供內嵌、無特徵碼攻擊偵測和零時差入侵防護。Prisma Access 會適應並提供即時防護和排程更新。它會立即防止高達 95% 的未知威脅，以不到 10 秒的時間提供特徵碼，從而減少了 99.5% 的受感染系統。 |
| DNS 安全性 | 套用即時防護和內嵌機器學習，以中斷使用 DNS 的 C2 回呼和其他攻擊。進階 DNS 安全性原生整合至 Prisma Access，可提供自動保護功能，防止攻擊者繞過安全性措施，並且不需要對 DNS 路由使用獨立工具或進行變更。 |
| 進階 URL 篩選 | 防範 Web 式威脅（例如網路釣魚、惡意軟體和 C2）的卓越防護，結合了強大的資料庫防護與支援 ML 的 Web 安全性引擎，可即時分類並封鎖新的惡意 URL。領先業界的網路釣魚防護可解決最常見的漏洞原因，讓您透過精細的控制和政策設定，根據使用者、風險評級和內容類別自動執行安全性動作，讓您重新控制 Web 流量。 |
| 進階威脅防護 | 利用領先業界的威脅防護功能，阻止零時差威脅、已知入侵、惡意軟體、間諜軟體，以及惡意命令與控制 (C2)。比傳統 Intrusion Prevention 系統，防止未知注入攻擊的能力增加 60%，以及防止高度逃避 C2 流量的能力增加 48%。 |
| 進階 WildFire | 使用業界最大的威脅情報和惡意軟體防護引擎，以快 60 倍的速度自動防止已知、未知和高度逃避的惡意軟體，以確保檔案安全。 |
| NG-CASB* | 獲得主動式 SaaS 可視性、防範錯誤設定，以及即時保護資料以實現同級最佳的 SaaS 安全性。 |
| 資料遺失防護 (DLP)* | 包括一組工具和程序，可協助您保護敏感資料，以防被未經授權存取、誤用、擷取或共用。Prisma Access 上的 DLP 可讓您強制執行資料安全性政策，並防止在行動使用者和遠端網路之間丟失敏感資料。 |
| 遠端瀏覽器隔離支援 | 透過 CloudBlades，利用現有的 NGFW URL 分類和 URL 重寫功能，與第三方 RBI 雲端整合，將選取/所有網際網路繫結流量轉送到 RBI 雲端，。此功能提供無縫的使用者體驗，同時將某些流量（未知或高風 |


©2025 Palo Alto Networks, Inc.

| 功能 | 說明 |
| --- | --- |
| | 險類別）轉送到 RBI 以進行額外檢查，而剩餘的流量可以透過 Prisma Access 進行檢查並直接輸出到網際網路。 |
| 報告 | 標準包括詳細、可自訂的 SaaS 應用程式使用情況報告，該報告提供了對您網路上所有 SaaS 流量（已認可和未認可）的洞察。您還可以根據需求建立自訂報告，並輕鬆排程、下載，以及與組織中的其他人分享這些報告。 |
| 使用者驗證 | 支援所有現有的 PAN-OS 驗證方法，包括 Kerberos、RADIUS、SAML、LDAP、用戶端憑證和本機使用者資料庫。僅使用 PAC，才支援 Kerberos 和 SAML。 |
| 站台對站台 IPsec VPN | 支援透過 IPv4 和 IKEv1/IKEv2 的站台對站台通道，以確保相容性。對於多個連線網站，ECMP 路由可以透過可用的網際網路連線平衡工作階段來提供額外的備援和成本效率。 |
| 記錄 | 顯示整體流量、應用程式、使用者、威脅、URL 和資料篩選器記錄，以透過雲端型 Strata 記錄服務促進資料的整理。 |
| 轉送設定檔 | 讓多個 PAC 檔案能夠用於不同的使用者群組或系統。還支援建立轉送規則，用於定義 Web 流量方向，以提供更簡單的建立和維護 PAC 檔案的替代方案。 |

* 需要附加授權。

如需產品特徵和功能的詳細說明，請參閱 Prisma Access 資料表。

## 明確 Proxy 設定指導方針

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

系統需求和支援的功能

這些是您可以與明確 Proxy 搭配使用的不同連線方法的系統需求和支援功能。

| | 無代理程式 **SAML** | 無代理程式 **Kerberos** | 代理程式上的 **Proxy** 模式（需要 **GP 6.2** 或更新版本） | 遠端網路上的 **Proxy** 模式 |
| --- | --- | --- | --- | --- |
| 應用程式和作業系統支援 | | | | |


©2025 Palo Alto Networks, Inc.

| | | | | |
|---|---|---|---|---|
| 流量類型 | 僅限網際網路和公用 SaaS 流量 | 僅限網際網路和公用 SaaS 流量 | 僅限網際網路和公用 SaaS 流量 | 僅限網際網路和公用 SaaS 流量 |
| 通訊協定支援 | Proxy 感知 HTTP 或 HTTPS | Proxy 感知 HTTP 或 HTTPS | Proxy 感知 HTTP 或 HTTPS | Proxy 感知 HTTP 或 HTTPS |
| **Prisma Access** 的運輸通道 | HTTP 連線 | HTTP 連線 | TLS 內的 HTTP 連線 | IPsec 內的 HTTP 連線，從分支到遠端網路安全性處理節點 (SPN) |
| 支援的環境 | Windows、Mac、Linux、ChromeOS、VDI | Windows、Mac、Linux、ChromeOS、VDI | Windows 和 Mac | Windows、Mac、Linux、ChromeOS、VDI |
| 應用程式支援 | Proxy 感知 HTTP(s) 應用程式 | 任何遵守 PAC 檔案或系統 Proxy 設定並支援 Kerberos 的應用程式 | Proxy 感知 HTTP(s) 應用程式 | Proxy 感知 HTTP(s) 應用程式 |
| 瀏覽器支援 | Chrome#、Edge、Firefox 版本 115 或更新版本 | Chrome#、Edge、Firefox 版本 115 或更新版本 | Chrome#、Edge、Firefox 版本 115 或更新版本* | Chrome#、Edge、Firefox 版本 115 或更新版本 |
| **O365** 支援† | 瀏覽器和用戶端應用程式 | 瀏覽器和用戶端應用程式 | 瀏覽器和用戶端應用程式 | 瀏覽器和用戶端應用程式 |
| 識別 | | | | |
| **User-ID**‡ | 已解密和非 HTTP CORS 流量 | 所有支援的流量 | 所有支援的流量 | 取決於您使用 SAML 還是 Kerberos：已解密/non-CORS X-Authenticated-User 流量 |
| 支援的驗證 | SAML（任何 SAML 2.0 IDP 或通過 CIE） | Kerberos | 所有 GlobalProtect 支援的驗證 | SAML、Kerberos、X-Authenticated-User-based |
| 跳過驗證 | 依網域和依來源 IP | 依網域和依來源 IP | 依網域 | 依網域和依來源 IP |
| 使用者群組目錄 | 所有 CIE 支援的目錄 | 所有 CIE 支援的目錄 | 所有 CIE 支援的目錄 | 所有 CIE 支援的目錄 |


©2025 Palo Alto Networks, Inc.

| | | | | |
|---|---|---|---|---|
| 授權 | 每個使用者的行動使用者單位 | 每個使用者的行動使用者單位 | 每個使用者的行動使用者單位 | 每個使用者的行動使用者單位，或用於遠端網路頻寬的無頭裝置和 NET 單位 |
| 管理 | | | | |
| 多租用戶 **Panorama** | 第一租用戶支援 | 第一租用戶支援 | 第一租用戶支援 | 第一租用戶支援 |
| 多租用戶雲端管理 | 支援 | 支援 | 支援 | 支援 |
| 安全性服務 | | | | |
| **SaaS** 內嵌 | 支援 | 支援 | 支援 | 支援 |
| **DLP** | 支援 | 支援 | 支援 | 支援 |
| **DNS** 安全性§ | 支援 | 支援 | 支援 | 支援 |
| 進階 **URL** 篩選 | 支援 | 支援 | 支援 | 支援 |
| 進階 **WildFire** | 支援 | 支援 | 支援 | 支援 |
| 進階威脅防護 | 支援 | 支援 | 支援 | 支援 |
| 遠端瀏覽器隔離 | 支援 | 支援 | 支援 | 支援 |
| 私人 **IP** 可視性和強制執行 | 不支援 | 不支援 | 已知網站或分支支援 | 支援 |
| 輸出 **NAT** | 支援 | 支援 | 支援 | 支援 |
| 私人應用程式存取 | 不支援 | 不支援 | 透過服務連線支援 | 不支援 |
| 所有 **TCP** 流量 | 不支援 | 不支援 | 支援（透過 GlobalProtect 6.3.1 版） | 不支援 |
| **ZTNA** 連接器 | 不支援 | 不支援 | 支援 | 不支援 |
| **Colo Connect** | 不支援 | 不支援 | 支援 | 不支援 |
| 服務連線 | 支援 | 支援 | 支援 | 支援 |


©2025 Palo Alto Networks, Inc.

| | | | | |
|---|---|---|---|---|
| **HIP** 支援（通道和 **Proxy** 模式） | 不支援 | 不支援 | 支援 | 不支援 |

# 對於 Chrome 瀏覽器，如果啟用了解密，請遵循下面列出的指示，停用 TLS 1.3 Kyber：

1. 開啟 Chrome 瀏覽器。
2. 在位址欄中新增 `chrome://flags/#enable-tls13-kyberchrome://flags/#enable-tls13-kyber` 並停用它。
3. 按一下 **Relaunch**（重新啟動）。

* 對於代理程式上的 Proxy 模式，Firefox 需要透過行動裝置管理推送的手動政策規則，指示它遵守系統 Proxy

† 明確 Proxy 僅支援 HTTP 流量，不支援 UDP。使用 SAML，明確 Proxy 不會為用戶端應用程式流程提供 User-ID。對於代理程式 Proxy，您需要使用 PAC 檔案，將用戶端應用程式驗證流程傳送到雲端 Proxy。

‡ 沒有 User-ID 可用於驗證略過。

§ 您無法將 DNS 安全性設定檔套用至明確 Proxy 流程。改為封鎖網域。

應用程式支援考量

1. 明確 Proxy 不支援需要 IP 相似性的應用程式。對於給定的使用者工作階段，該應用程式必須支援來自其中多個 IP 的流量。
2. 明確 Proxy 會將解密的 HTTP/2 流程降級為 HTTP/1。
3. 明確 Proxy 不會擷取內部部署外部動態清單。
4. 僅限無代理程式 SAML：
   1. 設定 SSL 解密政策，以透過 SAML 驗證允許無代理程式 PAC 型明確 Proxy 的網域進行驗證略過

      *Prisma Access* 需要解密，才能讀取 *Prisma Access* 在行動使用者瀏覽器上設定的驗證狀態 *Cookie*。無法強制執行解密，這會使得濫用明確 *Proxy* 作為開放 *Proxy*，攻擊者可以將其用作轉送服務進行拒絕服務攻擊。
   2. 在流量日誌中，明確 Proxy 會將未解密和 HTTP-CORS 移動使用者流量日誌顯示為 SWG 驗證的使用者。
   3. 請注意下列瀏覽器需求和使用指導方針：
      - 如果您使用明確 Proxy，請勿在瀏覽器中停用 Cookie；如果停用，則無法瀏覽任何網頁。
      - 如果您使用明確 Proxy 搭配 Microsoft Edge，請務必將 **Settings**（設定） > **Privacy, Search, and Services**（隱私權、搜尋和服務） > **Tracking prevention**（防止追蹤）設定為 **Basic**（基本）。

連線需求

如果行動使用者使用明確 Proxy，從遠端網站或總部或資料中心位置連線，則行動使用者端點必須能夠連線和路由至 IdP、ACS FQDN、明確 Proxy URL，以及 Prisma Access 所託管 PAC 檔案的 URL。

 ©2025 Palo Alto Networks, Inc.

**PAC** 檔案需求與指導方針—設定 PAC 檔案與明確 Proxy 搭配使用時，請遵循 PAC 檔案指導方針。

**Proxy** 鏈結指導方針—如果您使用從第三方 Proxy 到明確 Proxy 的 Proxy 鏈結，請在第三方 Proxy 中指定 **Explicit Proxy URL**（明確 **Proxy URL**），以將流量轉送到明確 Proxy

內部部署支援—明確 Proxy 是雲端型 Proxy 解決方案，而不是內部部署產品。對於內部部署 Proxy 解決方案，請設定 PAN-OS Web Proxy。

## Proxy 模式下的 GlobalProtect

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• Prisma Access (Managed by Strata Cloud Manager)<br>如果您想在 Prisma Access 環境中使用此功能，請與您的帳戶團隊聯繫以瞭解更多資訊。 | • Prisma Access 5.2<br>• 適用於 Windows 或 macOS 的 GlobalProtect 應用程式 6.2 版<br>• 內容發行版本 8700-7994<br>• Prisma Access 行動使用者授權 |

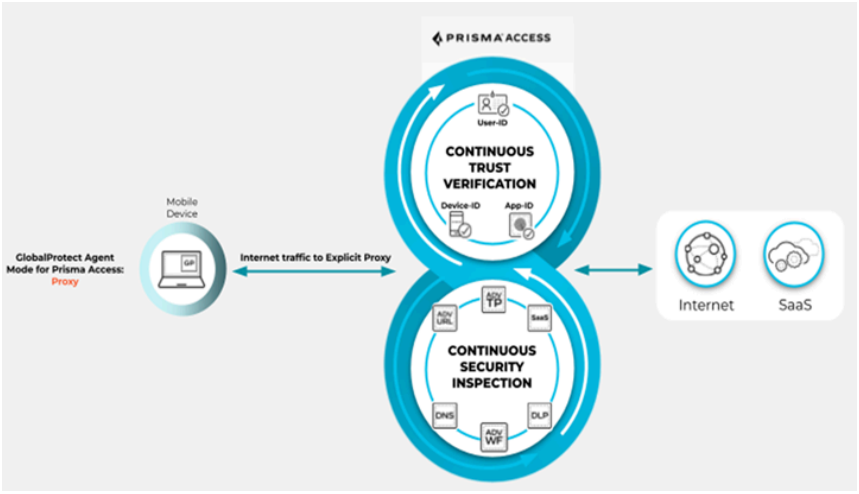
透過 **Proxy** 模式，GlobalProtect 應用程式提供一直開啟的網際網路安全性。在此模式下，GlobalProtect 應用程式會根據來自 PAC 檔案（託管於 Prisma Access 或您的環境中）的轉送規則和邏輯，透過 Proxy 將流量轉送至 Prisma Access。如果您有現有（舊式）Proxy 架構，或出於法規或合規性原因需要維護 Proxy 架構，這非常有用。

代理程式型 Proxy 功能可促進 GlobalProtect 應用程式與第三方 VPN 的共存和互通性，其中您可以透過 GlobalProtect 應用程式保護行動使用者的網際網路流量傳送到明確 Proxy，並使用您選擇的第三方 VPN 來保護私人應用程式存取。

你需要適用於 *Strata Cloud Manager GlobalProtect Proxy* 通道的 *GlobalProtect* 代理程式版本 *6.3.0*，以支援所有 *IPv4 TCP* 連線，包括非 *Proxy* 感知流量。為了確保無縫功能，端點上設定的 *DNS* 必須能夠解析目的地 *FQDN*。

在此情況下，GlobalProtect 應用程式會根據您定義的 PAC 檔案規則，將網際網路應用程式流量傳送至 Prisma Access，而端點會使用 IPSec/TLS 通道透過第三方 VPN 路由對您私人應用程式的存取。

 ©2025 Palo Alto Networks, Inc.



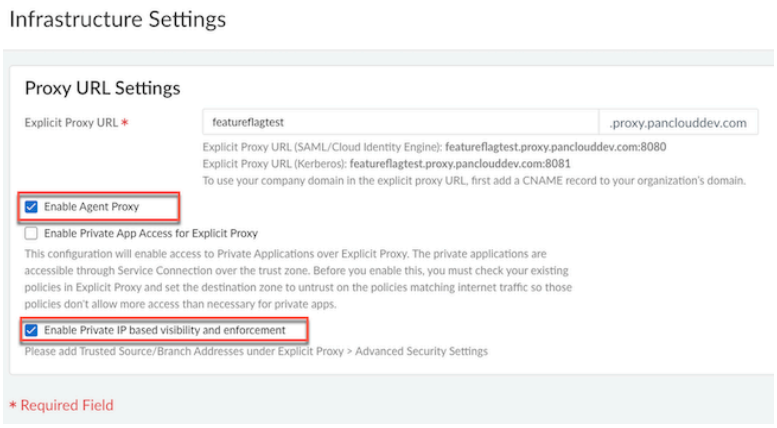

- Strata Cloud Manager
- Panorama

## Proxy 模式下的 GlobalProtect (Strata Cloud Manager)

 ©2025 Palo Alto Networks, Inc.

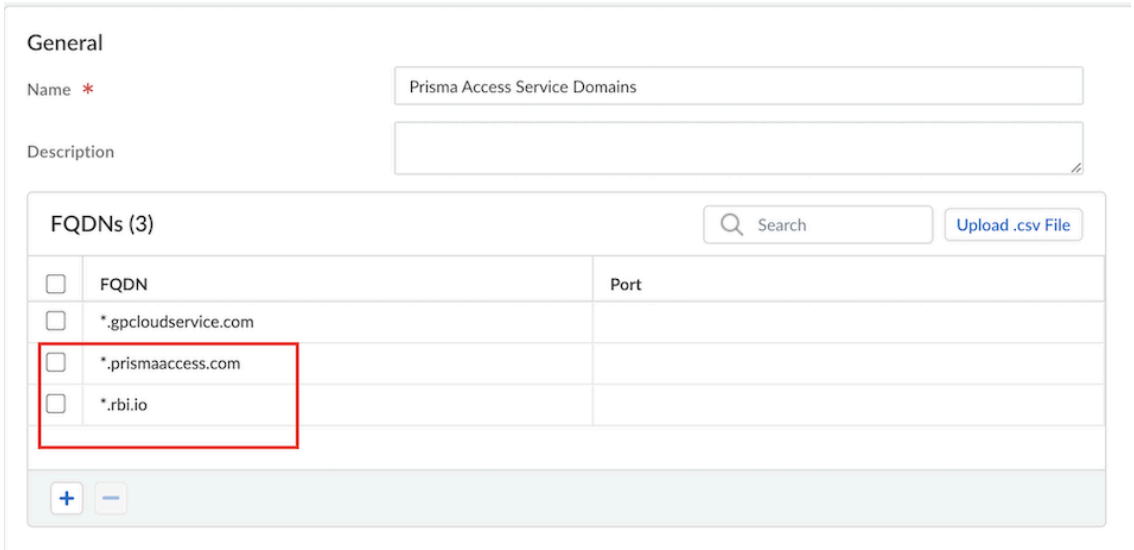
**STEP 1 |** 在 Prisma Access 上為行動使用者啟用代理程式型 Proxy 功能。

1. 啟用明確 Proxy。
   1. 選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Mobile Users**（行動使用者），然後按一下 **Explicit Proxy Setup**（明確 **Proxy** 設定）。
   2. 在基礎結構設定區域中，按一下 **Setup Proxy Settings**（設定 **Proxy** 設定），並指定 **Explicit Proxy URL**（明確 **Proxy URL**）。
2. **Enable Agent Proxy**（啟用代理程式 **Proxy**），並選擇性地啟用私人 **IP** 型可視性和強制執行，然後按一下 **Save(**儲存**)**。




3. 選擇 Prisma Access 位置，您想要在其中支援行動使用者。

   為了獲得最佳使用者體驗，如果您限制了位置數目，請選擇離一般使用者最近的位置。如果您行動使用者所在的國家/地區沒有可用位置，請選擇離行動使用者最近的位置。
4. 建立轉送設定檔，以定義您要透過明確 Proxy 傳送的流量。設定轉送設定檔時，略過 *.prismaaccess.com 和 *.gpcloudservice.com 網域。

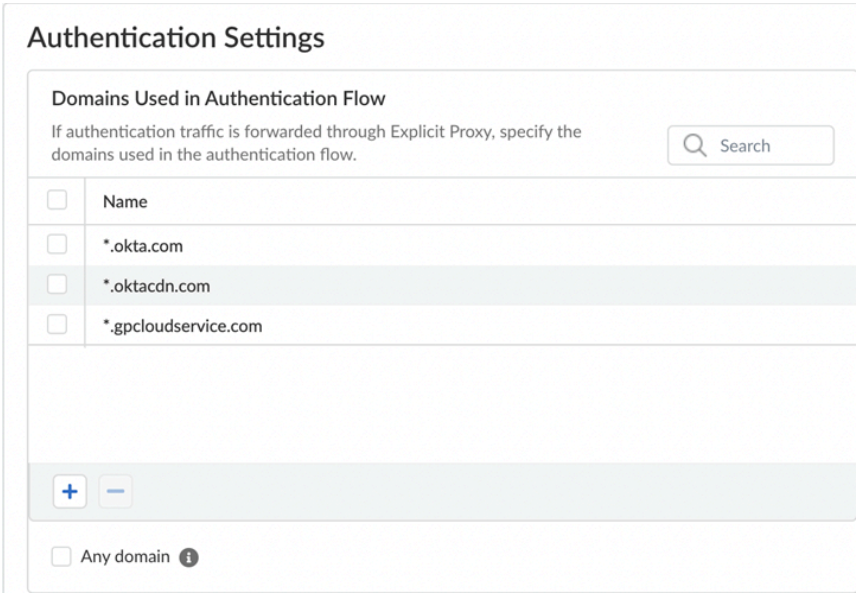



5. 將轉送設定檔附加到 GlobalProtect 應用程式設定。
6. 選取 **Workflows**（工作流程） > **Setup**（設定） > **Explicit Proxy**（明確 **Proxy**） > **Advanced Security Settings**（進階安全性設定） > **Authentication Settings**（驗證設定），並新增您需要略過的網域。

 ©2025 Palo Alto Networks, Inc.

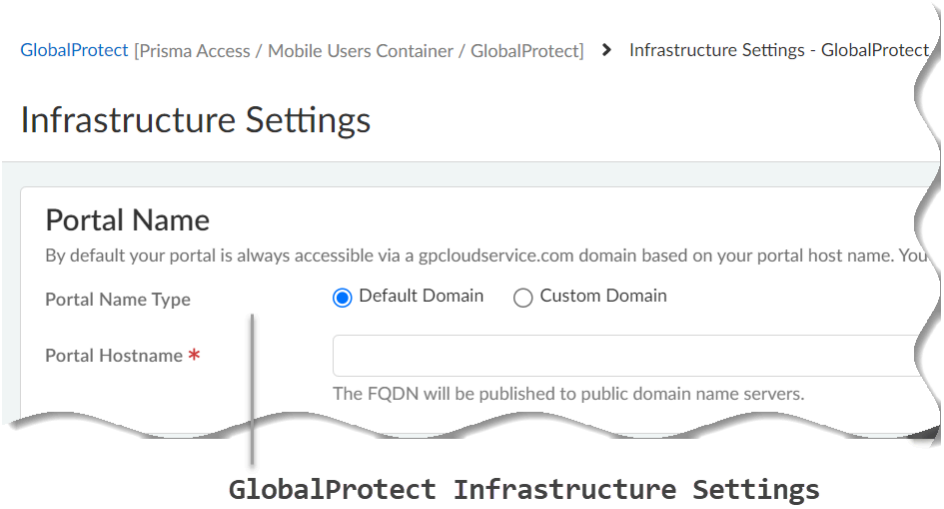
所有對 Proxy 的要求都會進行驗證。不過，如果您透過 Proxy 傳遞 IdP 流程，則需要略過它們，驗證才能成功。

在此範例中，我們略過 GlobalProtect 入口網站和 Okta，但請根據您使用的 IdP 自訂這些項目。




**STEP 2 |** 設定 GlobalProtect 入口網站、進行驗證，並為 GlobalProtect 應用程式設定 Proxy 模式。

1. 選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **GlobalProtect** > **Infrastructure**（基礎結構） > **Infrastructure Settings**（基礎結構設定），然後指定 **Portal Name**（入口網站名稱）。




**GlobalProtect Infrastructure Settings**

- **Default Domain**（預設網域）—如果選取此選項，則入口網站主機名稱會使用預設網域名稱：`.gpcloudservice.com`。在此情況下，只需輸入 **Portal Hostname**（入口

 ©2025 Palo Alto Networks, Inc.

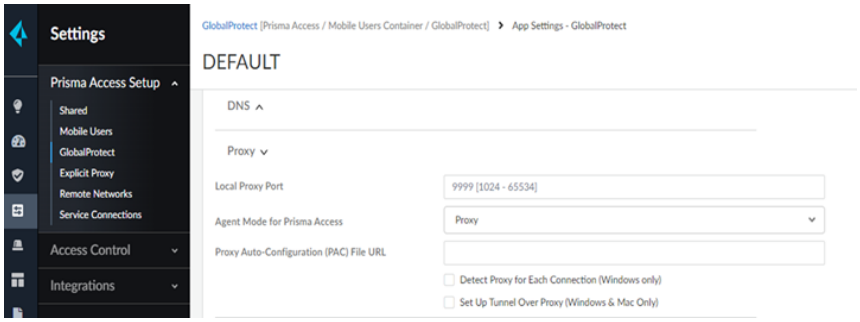
網站主機名稱）以附加到預設網域名稱。Prisma Access for Users 將自動建立必要的憑證，並將主機名稱發佈到公用 DNS 伺服器。

- **Custom Domain**（自訂網域）—如果您想要入口網站主機名稱中的網域符合貴公司網域名稱（例如，myportal.mydomain.com），您也可以自訂入口網站位址。

2. 啟用行動使用者對 Prisma Access 進行驗證。
3. 在 GlobalProtect 應用程式設定中，為 Prisma Access 啟用 GlobalProtect Proxy 模式，以將網際網路流量傳送到代理程式型 Proxy。

   *GlobalProtect* 連線方法不適用於 *Proxy* 模式，因為它一直開啟。

   - 選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **GlobalProtect**。
   - 在 **GlobalProtect App**（**GlobalProtect** 應用程式）頁籤上，按一下 **Default**（預設值）以自訂應用程式設定，或按一下 **Add App Settings**（新增應用程式設定）以新增組態。
   - 按一下 **Show Advanced Options**（顯示進階選項），並在 **App Configuration**（應用程式組態）區段中，
   - 將 **Agent Mode for Prisma Access**（將 **Prisma Access** 的代理程式模式） 設定為 **Proxy**，以指示 GlobalProtect 應用程式將網際網路流量傳送到 Prisma Access 上的明確 Proxy。
   - （選用）設定本機 Proxy 連接埠。連接埠範圍為 1024 到 65534，預設連接埠為 9999。如果預設連接埠不可用，GlobalProtect 將嘗試 9999 到 10009 範圍內的其他 10 個連接埠，並使用可用的連接埠。您還可以在該範圍內挑選自己的連接埠號碼。
   - （選用）如果要將 Proxy 設定的新 PAC URL 推送到端點，請設定 PAC 自動設定 (PAC) 檔案 URL。一旦使用者連線，PAC URL 就會推送到端點。當使用者中斷連線 GlobalProtect 應用程式，端點 Proxy 設定會自動停用並還原為以前的設定。
   - （選用）如果您想要使用者檢查入口網站是否有任何新設定，請啟用允許使用者重新探索網路。
   - （選用）設定 GlobalProtect 應用程式設定重新整理間隔（小時）。根據預設，GlobalProtect 用戶端每 24 小時重新整理一次快取的入口網站設定。您可以根據業務需求變更重新整理間隔。
   - 停用 **Set Up Tunnel Over Proxy (Windows & Mac Only)**（透過 **Proxy** 設定通道（僅限 **Windows** 和 **Mac**））。

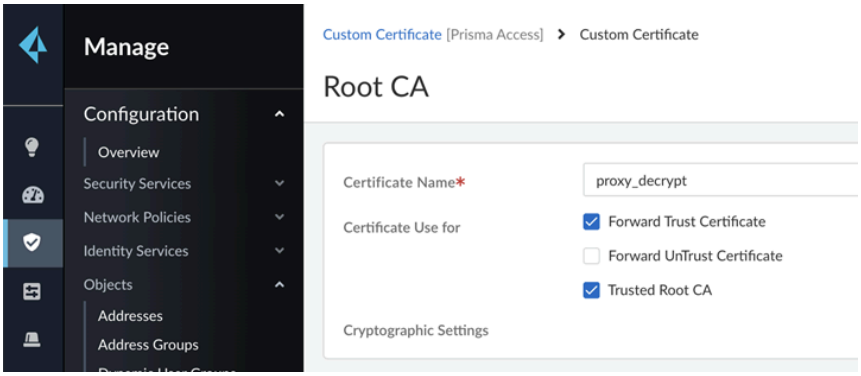



 ©2025 Palo Alto Networks, Inc.

4. 透過在 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **GlobalProtect** > **GlobalProtect App**（**GlobalProtect** 應用程式） > **Add App Settings**（新增應用程式設定） 頁面上設定下列設定，啟用一直開啟網際網路安全性：
   1. 將停用 GlobalProtect 設定為 **Disallow**（不允許）、**Allow with Passcode**（透過密碼允許）或 **Allow with Ticket**（透過票證允許）。
   2. 停用允許使用者從 GlobalProtect 應用程式登出。

**STEP 3 |** 為明確 Proxy 流量設定解密。

- 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and** （**NGFW** 及 ） > **Security Services**（安全性服務） > **Decryption**（解密）。
- 如果您啟用解密，請確保您將解密憑證設定為受信任的根 CA。




**STEP 4 |** 為明確 Proxy 流量設定安全性政策規則。

- 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 及 **Prisma Access**） > **Security Services**（安全性服務） > **Security Policy**（安全性政策）。
- 遵循網際網路閘道安全性政策最佳做法。

**STEP 5 |** （選用）在無預設路由網路中以 Proxy 模式設定 GlobalProtect 應用程式。

- （選用）在內部託管 PAC 檔案，並新增 Prisma Access 明確 Proxy FQDN 作為 PAC 檔案中的 Proxy，或將 PAC 檔案託管在轉送設定檔中，並在您的網路中新增 PAC 服務IP 位址的路由。
- 在 PAC 檔案中，將 IdP URL 和 Prisma Access 入口網站 URL 轉送至明確 Proxy。
- 在明確 Proxy 上，從驗證設定中排除 IdP 和入口網站 URL。將 IdP 和入口網站 URL 新增到驗證流程中使用的網域。
- 在週邊裝置上設定明確 Proxy FQDN 或 IP 位址的路由，以允許使用者透過明確 Proxy 存取網際網路。
- （選用）如果使用者無法解析分支網路中的公用網域，並將內部 IP 位址的目的地 NAT 新增到明確 Proxy FQDN 或 IP 位址，請新增 DNS 記錄以將 Prisma Access 明確 Proxy FQDN 解析為內部 IP 位址。

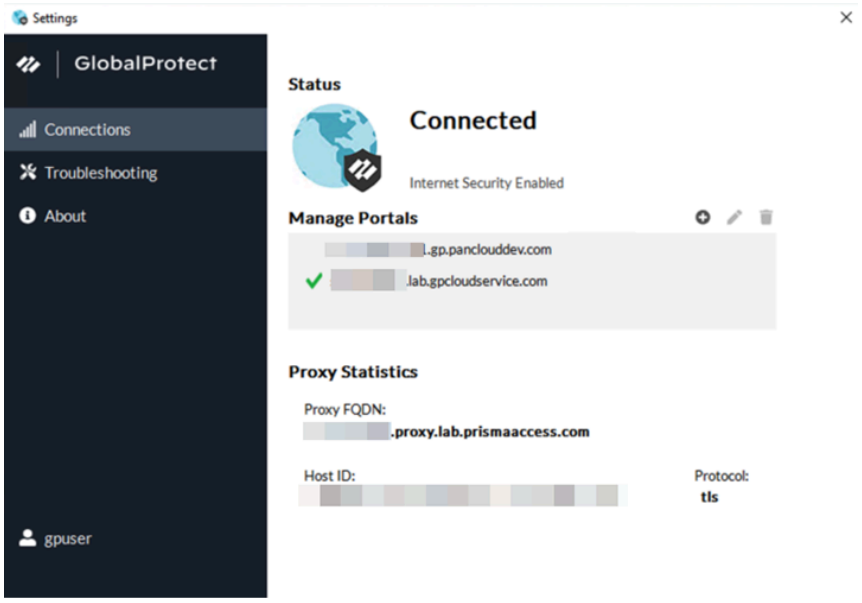
**STEP 6 |** 按一下 **Save**（儲存）並 **Push Config**（推送組態）至 **GlobalProtect** 和 **Explicit Proxy**（明確 **Proxy**）。

 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** 驗證代理程式 Proxy 部署並針對其進行疑難排解。

1. 在 GlobalProtect 應用程式 **Connections**（連線）頁籤上，於 **Settings**（設定）下驗證網路連線的相關資訊。

   1. 開啟 GlobalProtect 應用程式。
   2. 選取 **Settings**（設定）以開啟 GlobalProtect 設定面板，然後選取 **Connections**（連線）。




2. 檢視並收集 GlobalProtect 日誌

   檢視 PanGPS 日誌以驗證 GlobalProtect 入口網站上的 Proxy 模式組態。

   您可以透過在 PanGPS 日誌中尋找以下事件來驗證 Proxy 模式是否已設定：

   `OnProxyAgentMode`：僅 `Proxy` 模式

   若要檢視 中的 GlobalProtect 日誌，請選取 **Incidents & Alerts**（事件與警示） > **Log Viewer**（日誌檢視器），以及：

   - **GlobalProtect**，適用於驗證日誌
   - **Traffic**（流量）和 **Decryption**（解密），適用於使用者存取日誌

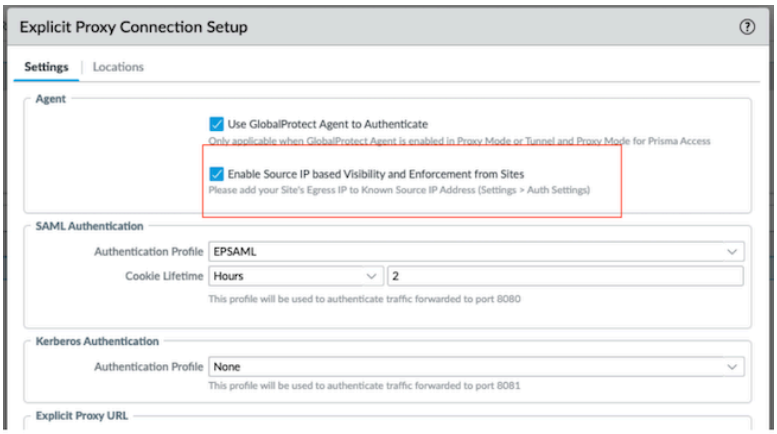
## Proxy 模式下的 GlobalProtect (Panorama)

如果您將單一租用戶 *Prisma Access (Managed by Panorama)* 部署轉換為多租戶，則只有第一個租用戶（您移轉的租用戶）支援此功能。此外，在這個第一個租用戶中，您必須在預先定義的 *Explicit_Proxy_Device_Group* 中設定您的政策規則，而不是在自訂裝置群組中。您在第一個租用戶之後為多租戶部署而建立的任何後續租用戶都不支援此功能。


©2025 Palo Alto Networks, Inc.

**STEP 1 |** 為行動使用者啟用代理程式型 Proxy 功能。

1. 啟用明確 Proxy。
   1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（組態） > **Mobile Users**—**Explicit Proxy**（行動使用者—明確 **Proxy**）。
   2. **Configure**（設定）明確 Proxy 設定以指定 **Explicit Proxy URL**（明確 **Proxy URL**）。
2. 選取 **Use GlobalProtect app to Authenticate**（使用 **GlobalProtect** 應用程式進行驗證），以啟用代理程式型 Proxy 功能，並選擇性地 **Enable Source IP based Visibility and Enforcement from Sites**（從網站啟用來源 **IP** 型可視性和強制執行）。




3. 輸入 **PAC (Proxy Auto-Configuration) File**（**PAC**（**Proxy** 自動設定）檔案） URL。確保在 PAC 檔案中輸入 8080 連接埠。
   - 確保在 PAC 檔案中輸入 8080 連接埠。
   - PAC 檔案中的 Proxy 陳述式必須使用您在上面設定的 Prisma Access FQDN。
   - PAC 檔案必須設定為略過第三方 VPN 流量。

   範例 PAC 檔案：

```
function FindProxyForURL (url, host) { /* Bypass localhost
 and Private IPs * / var resolved_ ip = dnsResolve (host) ;
 if (isplainHostName (host) || shExpMatch (host,"* ,local")
 || isInNet (resolved_ip,"10.0.0.0", "255.0.0.0") ||
 isInNet (resolved ip,"172.16.0.0","255.240.0.0") ||
 isInNet (resolved_ip,"192.168.0.0","255.255.0.0") ||
 isInNet (resolved ip, "127.0.0.0", "255.255.255.0" ))
 return "DIRECT"; /* Bypass Non-HTTP * / if (url.substring
 (0,4) == "ftp: ") return "DIRECT"; /* Bypass VPN */ if
 (shExpMatch (host, "vpn. acme.com") || shExpMatch (host,
 "gateway. acme.com" )) return "DIRECT"; /* Bypass Private
 Apps */ if (shExpMatch (host,"internalapps. acme.com" ) )
 return "DIRECT"; /* Forward to  */ return "PROXY acme-
demo.proxy.prismaaccess.com:8080";}
```

4. 為您設定的明確 Proxy 設定選取 **Connection Name**（連線名稱）。
5. 選取您要為行動使用者部署明確 Proxy 的 **Locations**（位置）和區域。

   Prisma Access 會將 Proxy 節點新增至您選取的每個位置。明確 Proxy 支援所有 Prisma Access 位置的子集。為了獲得最佳使用者體驗，如果您限制了位置數目，請選擇

 ©2025 Palo Alto Networks, Inc.

離一般使用者最近的位置。如果您行動使用者所在的國家/地區沒有可用位置，請選擇離行動使用者最近的位置。

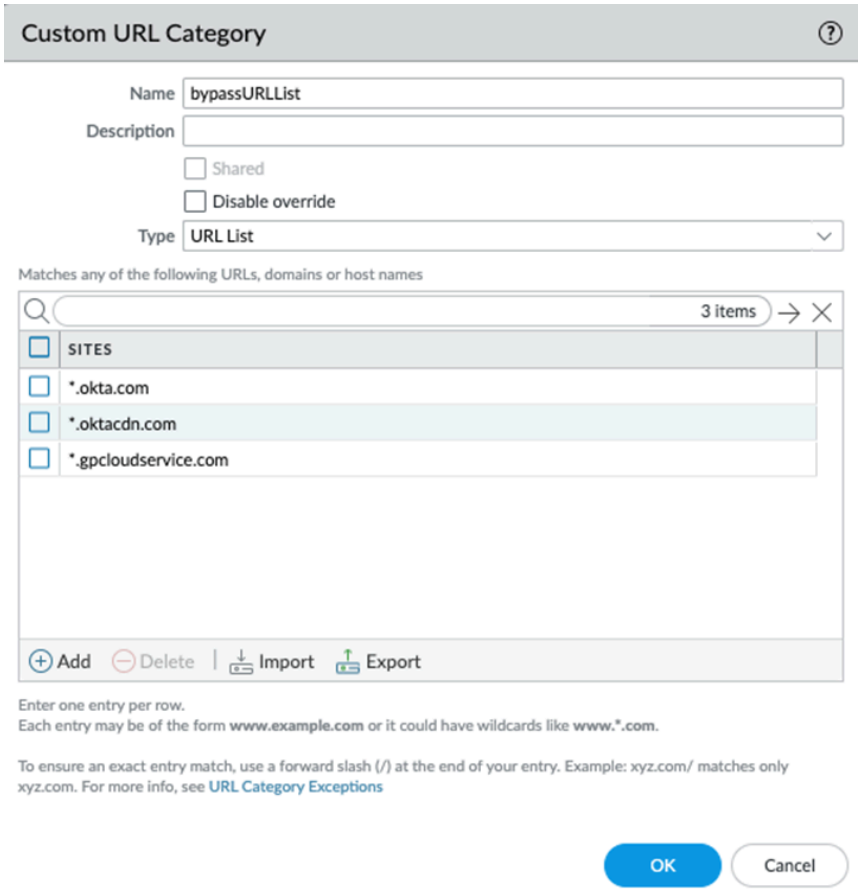
 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 略過識別提供者 (IDP)。

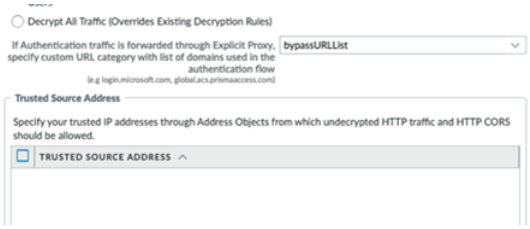
所有對 Proxy 的要求都會進行驗證。不過，如果您透過 Proxy 傳遞 IDP 流程，則需要略過它們，驗證才能成功。

在此範例中，我們略過 GlobalProtect 入口網站和 Okta，但請根據您使用的 IDP 自訂這些項目。

1. 在選取 **Explicit_Proxy_Device_Group** 後，選取 **Object**（物件） > **Custom Objects**（自訂物件） > **URL Category**（**URL** 類別），並建立自訂 URL 類別。
2. 在自訂 URL 類別中，新增需要略過 EP 驗證的所有 FQDN 網域。




3. 選取 **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users**（行動使用者） > **Explicit Proxy**（明確 **Proxy**） > **Settings**（設定） > **Authentication Settings**（驗證設定），並附加自訂 URL 類別。




4. 提交並推送到 **Explicit_Proxy_Device_Group**。


©2025 Palo Alto Networks, Inc.

**STEP 3 |** 設定 GlobalProtect 入口網站。

在 *Proxy* 模式下，您設定的連線方法不會變更 *Proxy* 功能的行為。即使您設定了隨選連線方法，但基於一直開啟網際網路安全性，所有網際網路繫結流量仍將透過 *Proxy* 傳送。

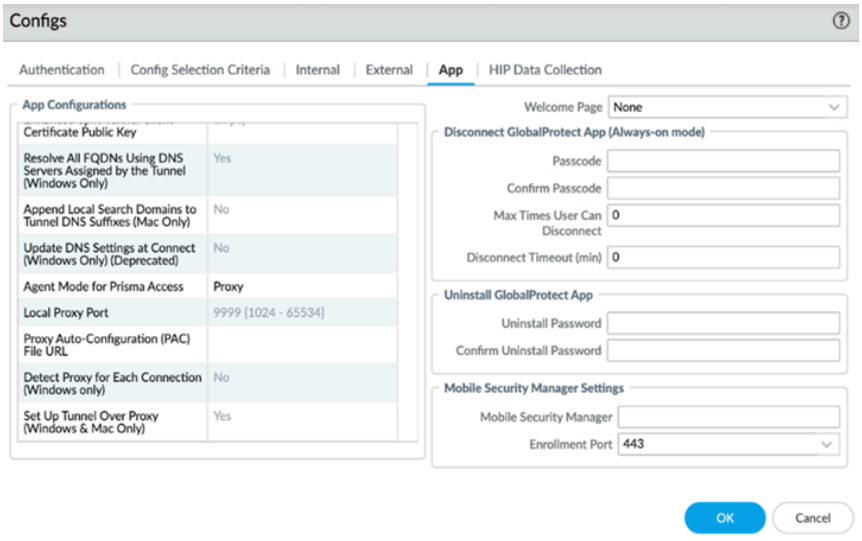
1. 在裝載區域中，按一下 **Configure**（設定）。
2. 在 **General**（一般）頁籤上，指定 **Portal Name Type**（入口網站名稱類型）：

   **Use Default Domain**（使用預設網域）—如果您選取此選項，您的入口網站主機名稱會使用預設網域名稱：.gpcloudservice.com.在此情況下，只需輸入一個入口網站主機名稱以附加到預設網域名稱。Prisma Access 將自動建立必要的憑證，並將主機名稱發佈到公用 DNS 伺服器。

   **Use Company Domain**（使用公司網域）—如果您想要入口網站主機名稱中的網域符合貴公司網域名稱（例如，myportal.mydomain.com），請選取此選項。
3. 選取一個 **Authentication Profile**（驗證設定檔），指定 Prisma Access 應如何驗證行動使用者，或建立新的驗證設定檔。
4. （選用）選取一個 **Authentication Override Certificate**（驗證覆寫憑證），以加密行動使用者用來驗證入口網站和閘道的安全 cookie。

**STEP 4 |** 在 GlobalProtect 上啟用 Proxy 模式。

1. 選取 **Network**（網路） > **GlobalProtect Portals**（**GlobalProtect** 入口網站）。
2. 選取您新增代理程式組態的入口網站組態，然後選取 **Agent**（代理程式）頁籤。
3. 在 **Agent**（代理程式）頁籤上，選取 **App**（應用程式）。
4. 在應用程式組態設區域中，將 **Agent Mode for Prisma Access**（**Prisma Access** 的代理程式模式）設定為 **Proxy**，以將網際網路流量傳送到 GlobalProtect 代理程式型 Proxy




 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** 執行選用的組態。

1. （選用）設定本機 Proxy 連接埠。連接埠範圍為 1024 到 65534，預設連接埠為 9999。如果預設連接埠不可用，GlobalProtect 將嘗試 9999 到 10009 範圍內的其他 10 個連接埠，並使用可用的連接埠。您還可以在該範圍內挑選自己的連接埠號碼。
2. （選用）如果要將 Proxy 設定的自訂 PAC URL 推送到端點，請設定 PAC 自動設定 (PAC) 檔案 URL。一旦使用者連線，PAC URL 就會推送到端點。當使用者中斷連線 GlobalProtect 應用程式，端點 Proxy 設定會自動停用並還原為以前的設定。
3. （選用）如果您想要使用者檢查入口網站是否有任何新設定，請啟用允許使用者重新探索網路。
4. （選用）設定 GlobalProtect 應用程式設定重新整理間隔（小時）。根據預設，GlobalProtect 用戶端每 24 小時重新整理一次快取的入口網站設定。您可以根據業務需求變更重新整理間隔。

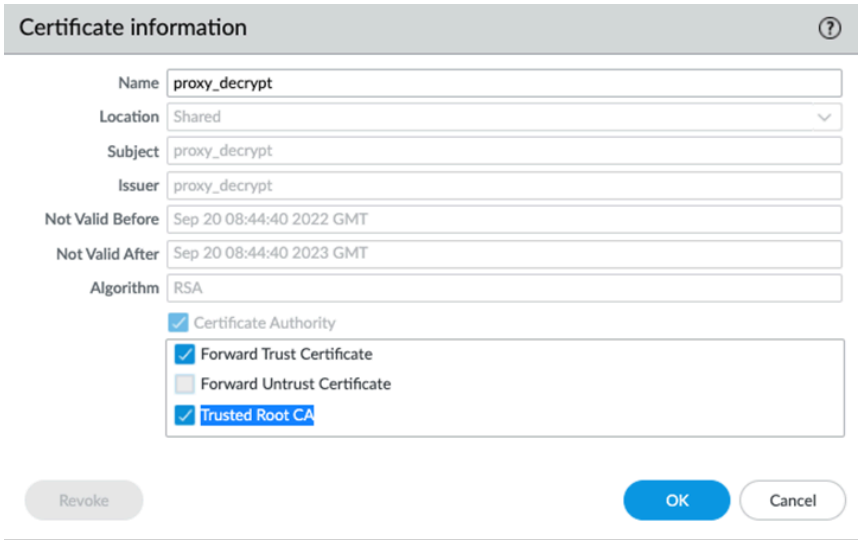
**STEP 6 |** 透過設定下列設定來啟用一直開啟網際網路安全性：

1. 將允許使用者停用 GlobalProtect 設定為 **Disallow**（不允許）、**Allow with Passcode**（透過密碼允許）或 **Allow with Ticket**（透過票證允許）。
2. 將允許使用者從 GlobalProtect 應用程式登出設定為 **No**（否）。

**STEP 7 |** （選用）為明確 Proxy 流量 設定解密政策。

如果啟用解密，請確保解密憑證也設定為受信任的根 CA。

1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證），並建立一個憑證，作為受信任根 CA 和轉送信任憑證。




2. 使用 SSL 正向 Proxy 在 **Explicit_Proxy_Device Group** 下建立解密規則。

**STEP 8 |** 為明確 Proxy 流量設定安全性政策規則。

1. 選取 **Policies**（政策） > **Security**（安全性）。
2. 將 **Device Group**（裝置群組）設定為 **Explicit_Proxy_Device_Group**。
3. 遵循網際網路閘道安全性政策最佳做法。


©2025 Palo Alto Networks, Inc.

**STEP 9 |** （選用）在非預設路由網路中以 Proxy 模式設定 GlobalProtect 應用程式。

- （選用）在內部託管 PAC 檔案，並新增 Prisma Access 明確 Proxy FQDN 作為 PAC 檔案中的 Proxy，或將 PAC 檔案託管在轉送設定檔中，並在您的網路中新增 PAC 服務IP 位址的路由。
- 在 PAC 檔案中，將 IDP URL 和 Prisma Access 入口網站 URL 轉送至明確 Proxy。
- 在明確 Proxy 上，從驗證設定中排除 IDP 和入口網站 URL。將 IDP 和入口網站 URL 新增到驗證流程中使用的網域。
- 在週邊裝置上設定明確 Proxy FQDN 或 IP 位址的路由，以允許使用者透過明確 Proxy 存取網際網路。
- （選用）如果使用者無法解析分支網路中的公用網域，並將內部 IP 位址的目的地 NAT 新增到明確 Proxy FQDN 或 IP 位址，請新增 DNS 記錄以將 Prisma Access 明確 Proxy FQDN 解析為內部 IP 位址。

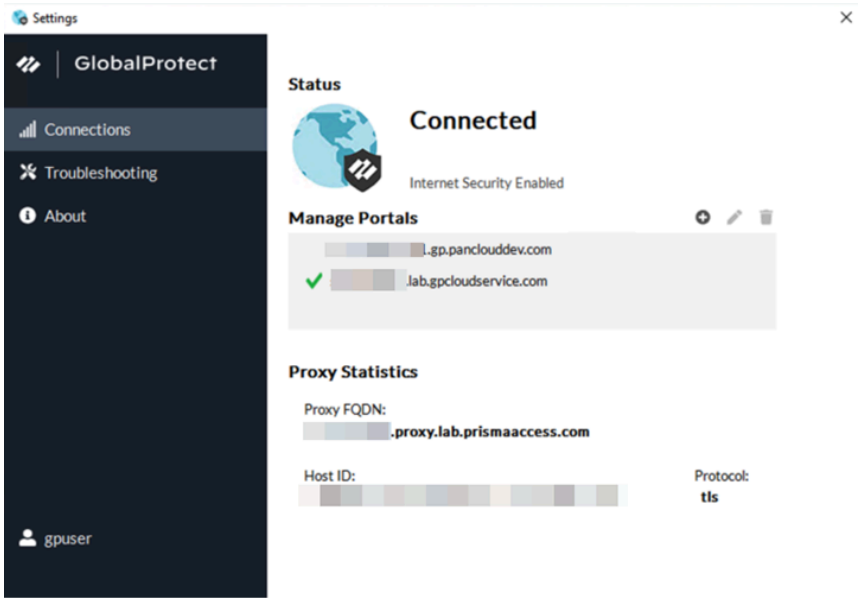
**STEP 10 |** **Commit**（提交）您的變更至 Panorama，並 **Commit and Push**（提交並推送）組態變更至 Prisma Access **Mobile Users**（行動使用者）和 **Explicit Proxy**（明確 **Proxy**）。

 ©2025 Palo Alto Networks, Inc.

**STEP 11 |** 驗證代理程式 Proxy 部署並針對其進行疑難排解。

1. 在 GlobalProtect 應用程式 **Connections**（連線）頁籤上，於 **Settings**（設定）下驗證網路連線的相關資訊。

   1. 開啟 GlobalProtect 應用程式。
   2. 選取 **Settings**（設定）以開啟 GlobalProtect 設定面板，然後選取 **Connections**（連線）。




2. 檢視並收集 GlobalProtect 日誌

   檢視 PanGPS 日誌以驗證 GlobalProtect 入口網站上的 Proxy 模式組態。

   您可以透過在 PanGPS 日誌中尋找以下事件來驗證 Proxy 模式是否已設定：

   `OnProxyAgentMode`：僅 `Proxy` 模式

   若要在 Panorama 中檢視 GlobalProtect 日誌，請選取 **Monitor**（監控） > **Logs**（日誌）和：

   - **GlobalProtect**，適用於驗證日誌
   - **Traffic**（流量）和 **Decryption**（解密），適用於使用者存取日誌

# 通道和 Proxy 模式下的 GlobalProtect

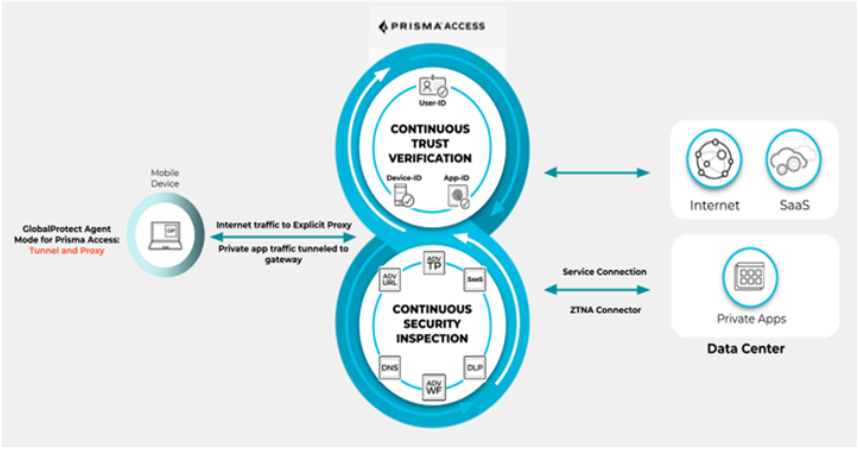
| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• Prisma Access (Managed by Strata Cloud Manager)<br>如果您想在 Prisma Access 環境中使用此功能，請與您的帳戶團隊聯繫以瞭解更多資訊。 | • Prisma Access 5.2<br>• 適用於 Windows 或 macOS 的 GlobalProtect 應用程式 6.2 版<br>• 內容發行版本 8700-7994<br>• Prisma Access 行動使用者授權 |


©2025 Palo Alto Networks, Inc.

在 **Tunnel and Proxy**（通道和 **Proxy)**模式下，GlobalProtect 應用程式會根據您在 PAC 檔案中定義的規則，將網際網路繫結流量傳送至明確 Proxy。對於其餘流量，它會使用 PAC 檔案中定義的分割通道規則和邏輯，來確定哪個流量透過通道傳送，以及哪個流量可以略過通道。如果您沒有定義分割通道規則，應用程式會透過通道傳送所有剩餘流量。

在通道和 *Proxy* 模式下執行 *GlobalProtect* 應用程式時，僅支援主機資訊設定檔 *(HIP)* 功能透過 *GlobalProtect* 通道傳送流量。

您需要 *Strata Cloud Manager* 和適用於 *GlobalProtect Proxy* 通道的 *GlobalProtect* 代理程式版本 *6.3.0*，才能支援所有 *IPv4 TCP* 連線，包括非 *Proxy* 感知流量。為了確保無縫功能，端點上設定的 *DNS* 必須能夠解析目的地 *FQDN*。



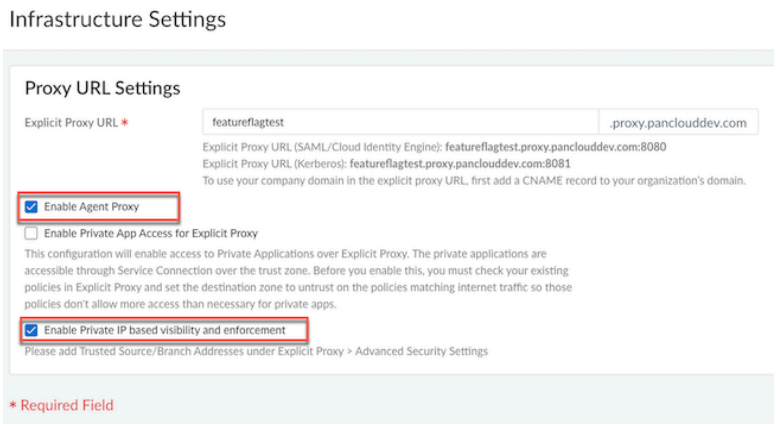

- Strata Cloud Manager
- Panorama

## 通道和 **Proxy** 模式下的 **GlobalProtect**（**Strata Cloud Manager**）

 ©2025 Palo Alto Networks, Inc.

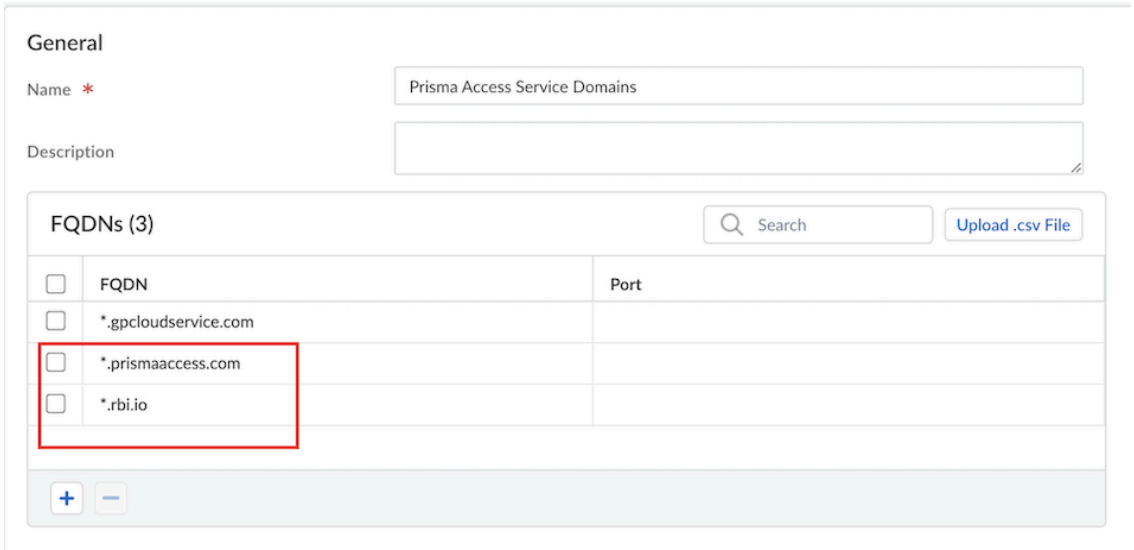
**STEP 1 |** 在 Prisma Access 上為行動使用者啟用代理程式型 Proxy 功能。

1. 啟用明確 Proxy。
   1. 選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Explicit Proxy**（明確 **Proxy**）。
   2. 在基礎結構設定區域中，按一下 **Setup Proxy Settings**（設定 **Proxy** 設定），並指定 **Explicit Proxy URL**（明確 **Proxy URL**）。
2. **Enable Agent Proxy**（啟用代理程式 **Proxy**），並選擇性地啟用私人 **IP** 型可視性和強制執行，然後按一下 **Save(**儲存**)**。




3. 選擇 Prisma Access 位置，您想要在其中支援行動使用者。

   為了獲得最佳使用者體驗，如果您限制了位置數目，請選擇離一般使用者最近的位置。如果您行動使用者所在的國家/地區沒有可用位置，請選擇離行動使用者最近的位置。
4. 建立轉送設定檔，以定義您要透過明確 Proxy 傳送的流量。設定轉送設定檔時，略過 *.prismaaccess.com 和 *.gpcloudservice.com 網域。

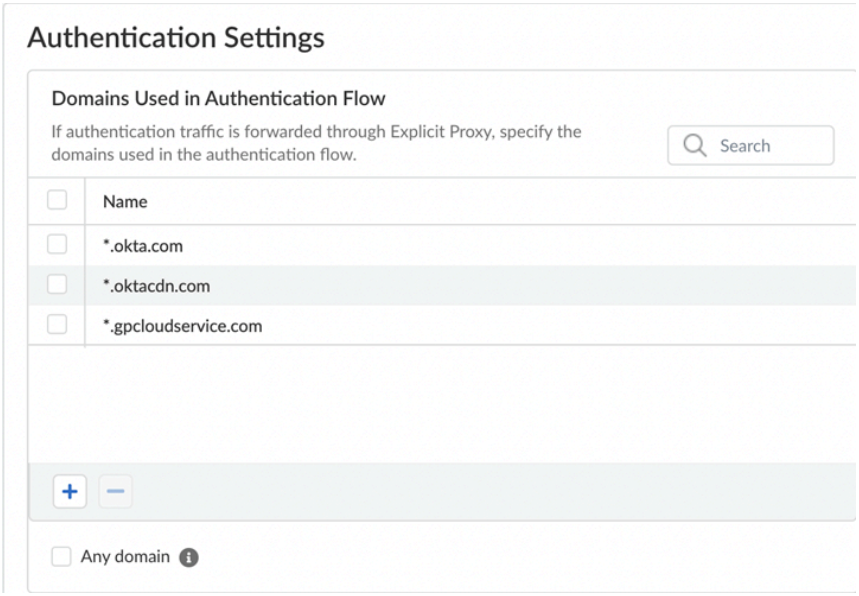



5. 將轉送設定檔附加到 GlobalProtect 應用程式設定。
6. 選取 **Workflows**（工作流程） > **Setup**（設定） > **Explicit Proxy**（明確 **Proxy**） > **Advanced Security Settings**（進階安全性設定） > **Authentication Settings**（驗證設定），並新增您需要略過的網域。

 ©2025 Palo Alto Networks, Inc.

所有對 Proxy 的要求都會進行驗證。不過，如果您透過 Proxy 傳遞 IdP 流程，則需要略過它們，驗證才能成功。

在此範例中，我們略過 GlobalProtect 入口網站和 Okta，但請根據您使用的 IdP 自訂這些項目。

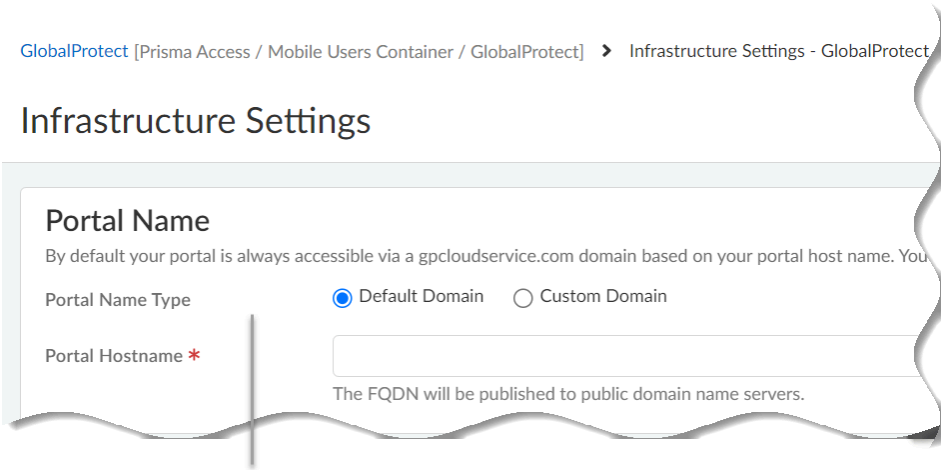



 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 在 Prisma Access 上為 GlobalProtect 應用程式設定通道和 Proxy 模式。

在通道和 *Proxy* 模式中，您設定的連線方法僅適用於透過 *GlobalProtect* 以通道傳送的流量。代理程式型 *Proxy* 功能將提供一直開啟網際網路安全性。即使您設定了隨選連線方法，但基於一直開啟網際網路安全性，即使使用者中斷 *GlobalProtect* 應用程式連線，所有網際網路繫結流量仍將透過 *Proxy* 傳送。

1. 選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **GlobalProtect** > **Infrastructure**（基礎結構） > **Infrastructure Settings**（基礎結構設定），然後指定 **Portal Name**（入口網站名稱）。



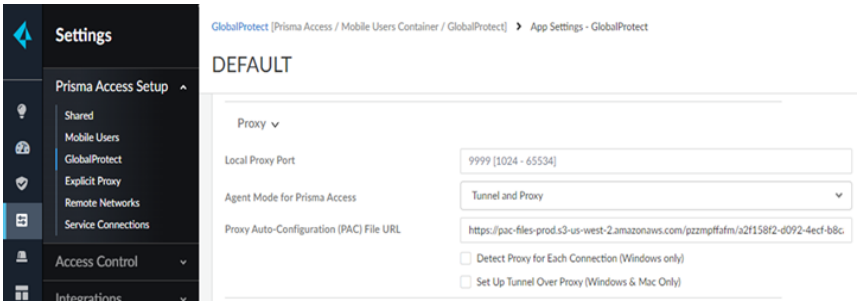

**GlobalProtect Infrastructure Settings**

   - **Default Domain**（預設網域）—如果選取此選項，則入口網站主機名稱會使用預設網域名稱：`.gpcloudservice.com`。在此情況下，只需輸入 **Portal Hostname**（入口網站主機名稱）以附加到預設網域名稱。Prisma Access for Users 將自動建立必要的憑證，並將主機名稱發佈到公用 DNS 伺服器。
   - **Custom Domain**（自訂網域）—如果您想要入口網站主機名稱中的網域符合貴公司網域名稱（例如，myportal.mydomain.com），您也可以自訂入口網站位址。
2. 啟用行動使用者對 Prisma Access 進行驗證。
3. 在 GlobalProtect 應用程式設定中，為 Prisma Access 啟用 GlobalProtect 通道和 Proxy 模式，以將網際網路流量傳送到代理程式型 Proxy。
   - 選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **GlobalProtect**。
   - 在 **GlobalProtect App**（**GlobalProtect** 應用程式）頁籤上，按一下 **Default**（預設值）以自訂應用程式設定，或按一下 **Add App Settings**（新增應用程式設定）以新增組態。
   - 按一下 **Show Advanced Options**（顯示進階選項），並在 **App Configuration**（應用程式組態）區段中，
   - 在 **Proxy** 區段中，將 **Agent Mode for Prisma Access**（**Prisma Access** 的代理程式模式）設定為 **Tunnel and Proxy**（通道和 **Proxy**），以指示 GlobalProtect 應用程式將網際網路流量傳送到 Prisma Access 上的明確 Proxy，以及將私人應用程式流量傳送至 VPN。在您於 Prisma Access 上設定 **Tunnel and Proxy**（通道和 **Proxy**）模式之後，即

 ©2025 Palo Alto Networks, Inc.

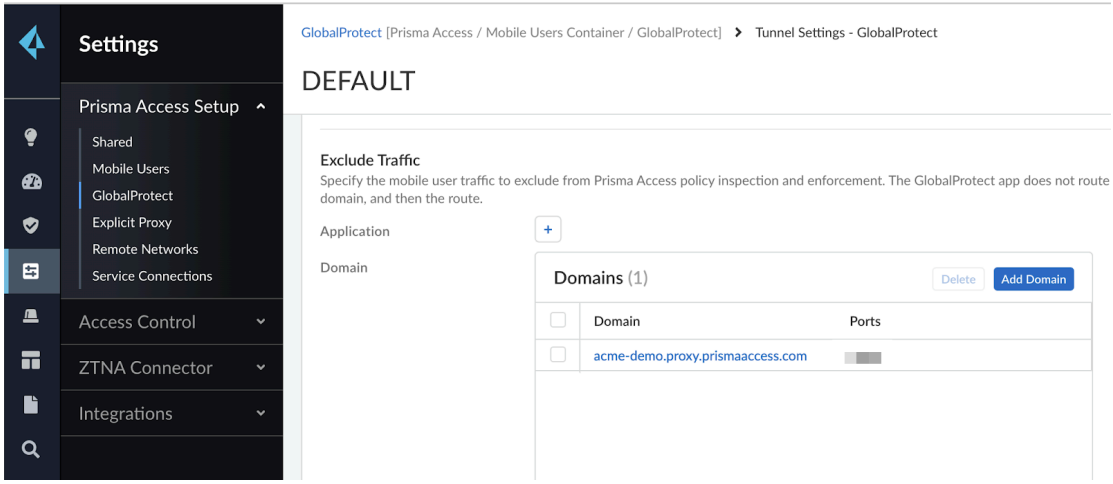
使使用者中斷連線或停用 GlobalProtect 應用程式，使用者仍可以透過 Prisma Access 安全地存取網際網路。

- （選用）設定本機 Proxy 連接埠。連接埠範圍為 1024 到 65534，預設連接埠為 9999。如果預設連接埠不可用，GlobalProtect 將嘗試 9999 到 10009 範圍內的其他 10 個連接埠，並使用可用的連接埠。您還可以在該範圍內挑選自己的連接埠號碼。
- （選用）如果要將 Proxy 設定的新 PAC URL 推送到端點，請設定 PAC 自動設定 (PAC) 檔案 URL。一旦使用者連線，PAC URL 就會推送到端點。當使用者中斷連線 GlobalProtect 應用程式，端點 Proxy 設定會自動停用並還原為以前的設定。
- （選用）如果您想要使用者檢查入口網站是否有任何新設定，請啟用允許使用者重新探索網路。
- （選用）設定 GlobalProtect 應用程式設定重新整理間隔（小時）。根據預設，GlobalProtect 用戶端每 24 小時重新整理一次快取的入口網站設定。您可以根據業務需求變更重新整理間隔。
- 停用 **Set Up Tunnel Over Proxy (Windows & Mac Only)**（透過 **Proxy** 設定通道（僅限 **Windows** 和 **Mac**））。




4. 在 **Split Tunnel**（分割通道）組態中，排除明確 Proxy FQDN 和 PAC 檔案 FQDN。
   - 選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **GlobalProtect**。
   - 在 **GlobalProtect App**（**GlobalProtect** 應用程式）頁籤上，按一下 **Default**（預設值）以自訂通道設定，或按一下 **Add Tunnel Settings**（新增通道設定）以新增組態。
   - 在 **Exclude Traffic**（排除流量）下，**Add Domain**（新增網域）。

 ©2025 Palo Alto Networks, Inc.




將映像中的 *FQDN* 取代為您的 *Proxy FQDN*。

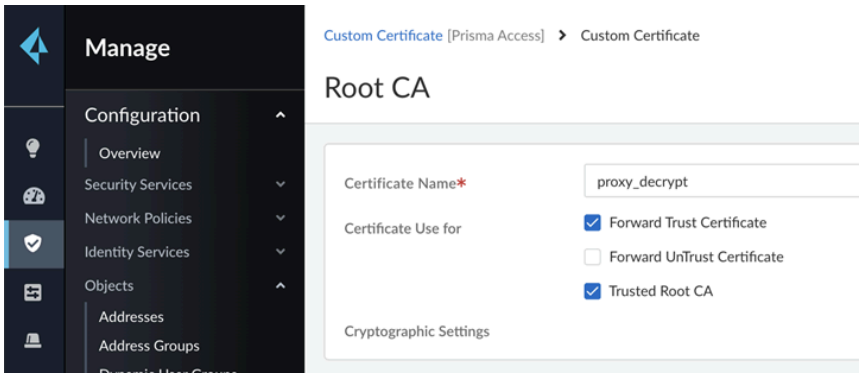
**STEP 3 |** 透過在 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **GlobalProtect** > **GlobalProtect App**（**GlobalProtect** 應用程式） > **Add App Settings**（新增應用程式設定） 頁面上設定下列設定，啟用一直開啟安全性：

1. 將停用 GlobalProtect 設定為 **Disallow**（不允許）、**Allow with Passcode**（透過密碼允許）或 **Allow with Ticket**（透過票證允許）。
2. 停用允許使用者從 GlobalProtect 應用程式登出。


©2025 Palo Alto Networks, Inc.

**STEP 4 |** 為明確 Proxy 流量設定解密。

- 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and** （**NGFW** 及 ） > **Security Services**（安全性服務） > **Decryption**（解密）。
- 如果您啟用解密，請確保您將解密憑證設定為受信任的根 CA。




**STEP 5 |** 為明確 Proxy 流量設定安全性政策規則。

- 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 及 **Prisma Access**） > **Security Services**（安全性服務） > **Security Policy**（安全性政策）。
- 遵循網際網路閘道安全性政策最佳做法。

**STEP 6 |** （選用）在非預設路由網路中以 Proxy 和通道模式設定 GlobalProtect 應用程式。

- （選用）在內部託管 PAC 檔案，並新增 Prisma Access 明確 Proxy FQDN 作為 PAC 檔案中的 Proxy，或將 PAC 檔案託管在轉送設定檔中，並在您的網路中新增 PAC 服務IP 位址的路由。
- 將驗證要求轉送到網際網路，以取得入口網站和閘道 FQDN，以及 IdP URL。
- 在週邊裝置上設定明確 Proxy FQDN 或 IP 位址的路由，以允許使用者透過明確 Proxy 存取網際網路。
- （選用）如果使用者無法解析分支網路中的公用網域，並將內部 IP 位址的目的地 NAT 新增到明確 Proxy FQDN 或 IP 位址，請新增 DNS 記錄以將 Prisma Access 明確 Proxy FQDN 解析為內部 IP 位址。
- 若要讓使用者在辦公室時可直接存取私人應用程式：
  - **Direct Access**（直接存取）：啟用內部主機偵測並將內部閘道清單保持空白。

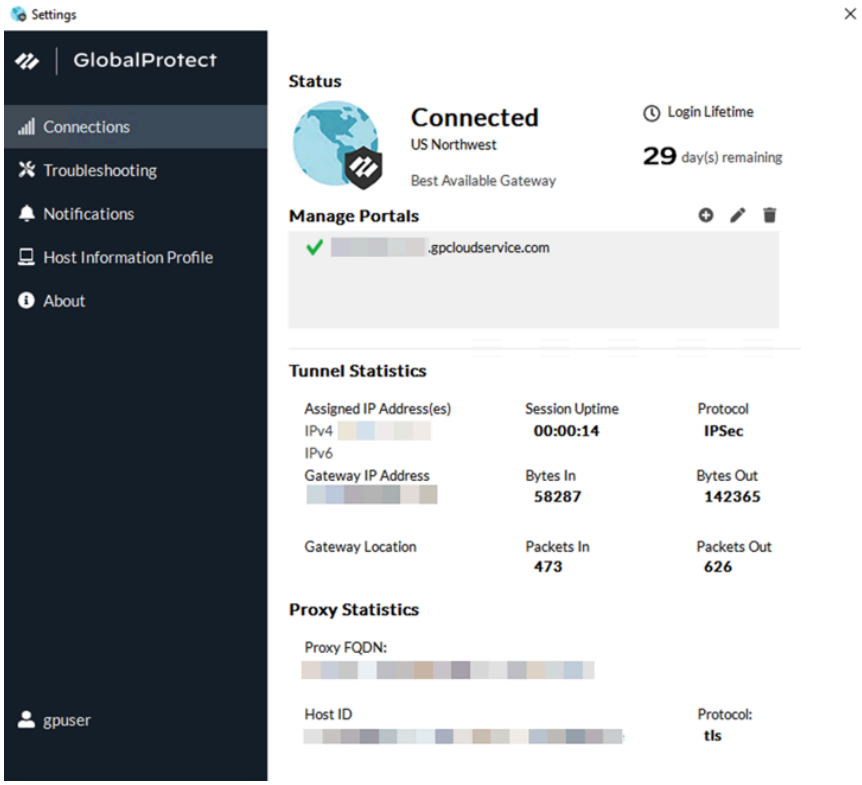
**STEP 7 |** 按一下 **Save**（儲存）並 **Push Config**（推送組態）至 **GlobalProtect** 和 **Explicit Proxy**（明確 **Proxy**）。

 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** 驗證代理程式 Proxy 部署並針對其進行疑難排解。

1. 在 GlobalProtect 應用程式 **Connections**（連線）頁籤上，於 **Settings**（設定）下驗證網路連線的相關資訊。

   1. 開啟 GlobalProtect 應用程式。
   2. 選取 **Settings**（設定）以開啟 GlobalProtect 設定面板，然後選取 **Connections**（連線）。




2. 檢視並收集 GlobalProtect 日誌

   檢視 PanGPS 日誌以驗證 GlobalProtect 入口網站上的 Proxy 模式組態。

   您可以透過在 PanGPS 日誌中尋找以下事件來驗證 Proxy 模式是否已設定：

   `OnProxyAgentMode`：混合模式

   若要檢視 中的 GlobalProtect 日誌，請選取 **Incidents & Alerts**（事件與警示） > **Log Viewer**（日誌檢視器），以及：

   - **GlobalProtect**，適用於驗證日誌
   - **Traffic**（流量）和 **Decryption**（解密），適用於使用者存取日誌

使用一直開啟連線方法中斷連線並停用通道和 **Proxy** 模式

從 GlobalProtect 6.3.1 版開始，當您將 GlobalProtect 應用程式的 **Tunnel and Proxy**（通道和 **Proxy**）模式，以及 **Always-On**（一直開啟）模式設定為連線方法，並想要中斷連線通道和 Proxy 模式時，必須執行以下步驟：

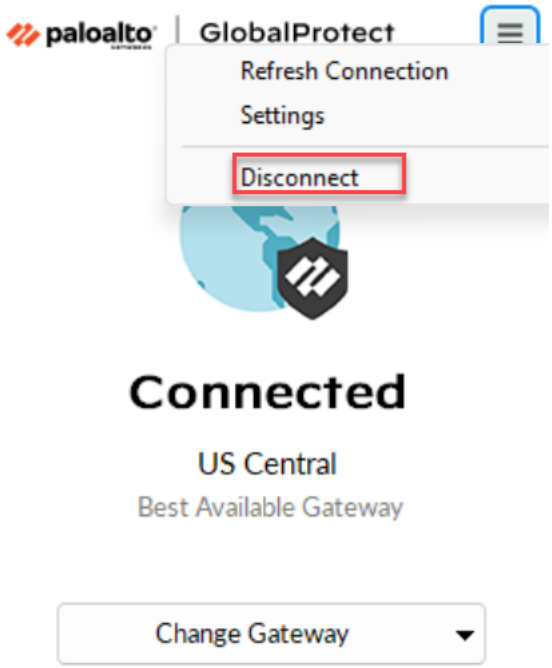
1. 中斷連線 GlobalProtect 應用程式以中斷通道 (VPN) 連線。當您中斷連線應用程式時，通道 (VPN) 連線會中斷，而應用程式仍將透過 Proxy 模式保持連線。

 ©2025 Palo Alto Networks, Inc.

2. 停用 GlobalProtect 應用程式以同時中斷連線通道和 Proxy 模式。當您停用應用程式時，通道和 Proxy 模式都將中斷連線，而且應用程式將不再連線。

若要中斷連線和停用透過 **Tunnel and Proxy**（通道和 **Proxy**）（混合模式）和 **Always-On**（一直開啟）連線方法設定的 GlobalProtect 應用程式，您必須：

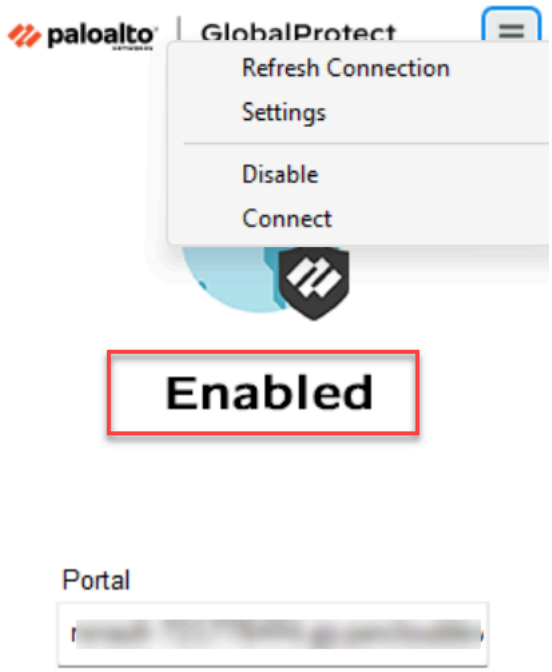
1. 使用漢堡功能表中的 **Disconnect**（中斷連線）選項來中斷連線 GlobalProtect 應用程式。當您中斷連線應用程式時，通道 (VPN) 連線會中斷。



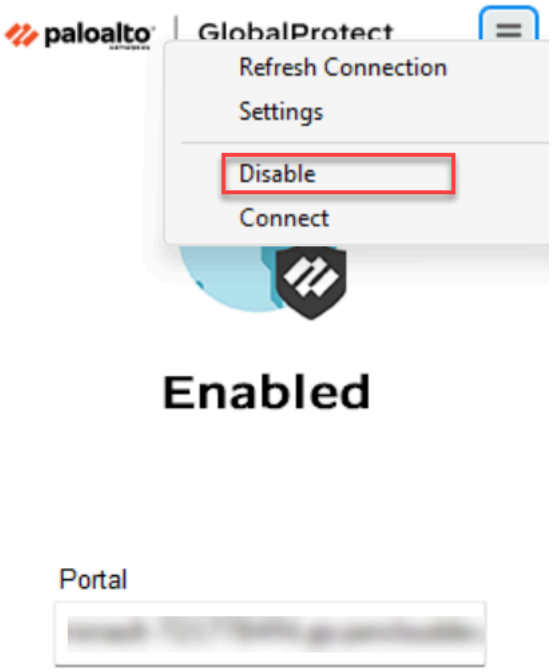

在您中斷連線應用程式之後，VPN 連線會中斷，但 Proxy 模式會啟用。該應用程式仍將透過 Proxy 模式連線，並且其會將狀態顯示為 **Enabled**（已啟用）。

如果您想要重新連線通道 *(VPN)*，可以使用漢堡功能表中的 ***Connect***（連線）選項。

 ©2025 Palo Alto Networks, Inc.

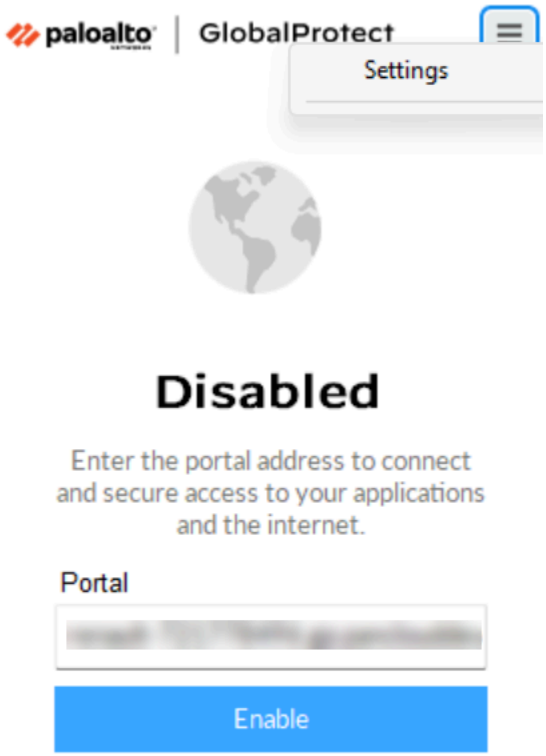



2. 使用漢堡功能表中的 **Disable**（停用）選項停用 GlobalProtect 應用程式。在您停用應用程式之後，通道和 Proxy 連線都會中斷。




該應用程式將被停用，且其會將狀態顯示為 **Disabled**（已停用）。

 ©2025 Palo Alto Networks, Inc.



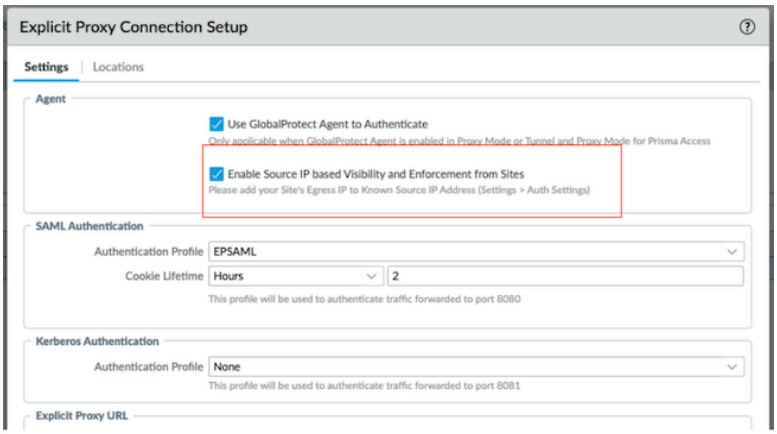

## 通道和 **Proxy** 模式下的 **GlobalProtect**（**Panorama**）

如果您將單一租用戶 *Prisma Access (Managed by Panorama)* 部署轉換為多租戶，則只有第一個租用戶（您移轉的租用戶）支援此功能。此外，在這個第一個租用戶中，您必須在預先定義的 *Explicit_Proxy_Device_Group* 中設定您的政策規則，而不是在自訂裝置群組中。您在第一個租用戶之後為多租戶部署而建立的任何後續租用戶都不支援此功能。


©2025 Palo Alto Networks, Inc.

**STEP 1 |** 為行動使用者啟用代理程式型 Proxy 功能。

1. 啟用明確 Proxy。
   1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（組態） > **Mobile Users**—**Explicit Proxy**（行動使用者—明確 **Proxy**）。
   2. **Configure**（設定）明確 Proxy 設定以指定 **Explicit Proxy URL**（明確 **Proxy URL**）。
2. 選取 **Use GlobalProtect app to Authenticate**（使用 **GlobalProtect** 應用程式進行驗證），以啟用代理程式型 Proxy 功能，並選擇性地 **Enable Source IP based Visibility and Enforcement from Sites**（從網站啟用來源 **IP** 型可視性和強制執行）。




3. 輸入 **PAC (Proxy Auto-Configuration) File**（**PAC**（**Proxy** 自動設定）檔案） URL。確保在 PAC 檔案中輸入 8080 連接埠。
   - PAC 檔案中的 Proxy 陳述式必須使用您在上面設定的 Prisma Access FQDN。
   - 必須將 PAC 檔案設定為排除 GlobalProtect 閘道 (*.gp.gpcoudservice.com)。
4. 為您設定的明確 Proxy 設定選取 **Connection Name**（連線名稱）。
5. 選取您要為行動使用者部署明確 Proxy 的 **Locations**（位置）和區域。

   Prisma Access 會將 Proxy 節點新增至您選取的每個位置。明確 Proxy 支援所有 Prisma Access 位置的子集。為了獲得最佳使用者體驗，如果您限制了位置數目，請選擇離一般使用者最近的位置。如果您行動使用者所在的國家/地區沒有可用位置，請選擇離行動使用者最近的位置。

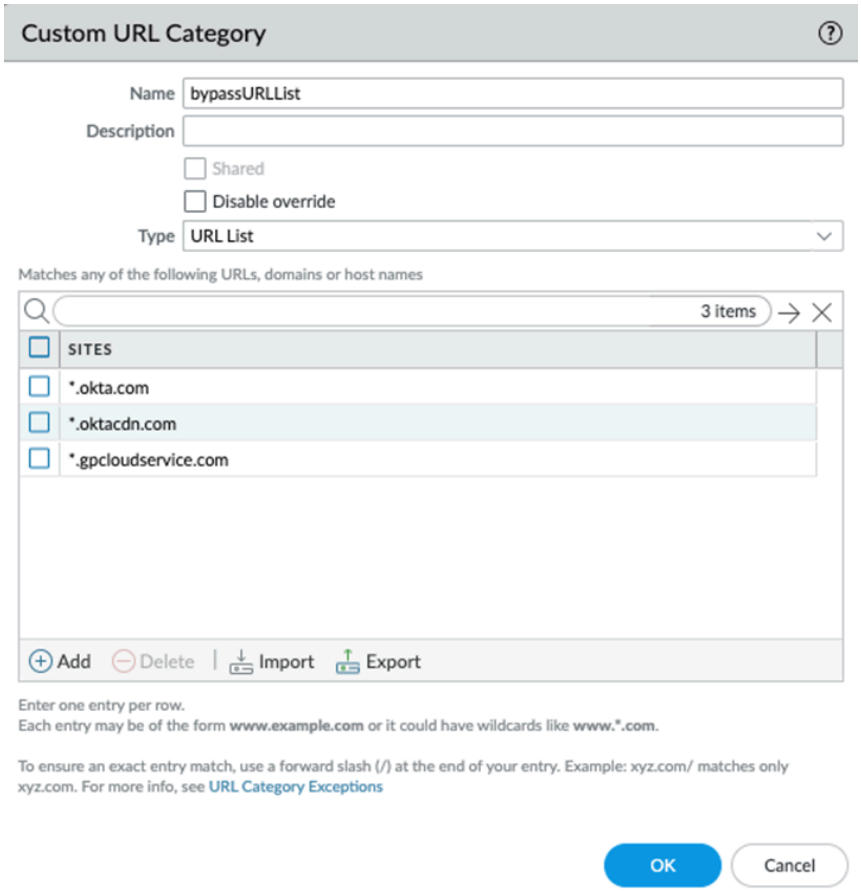
 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 略過識別提供者 (IDP)。

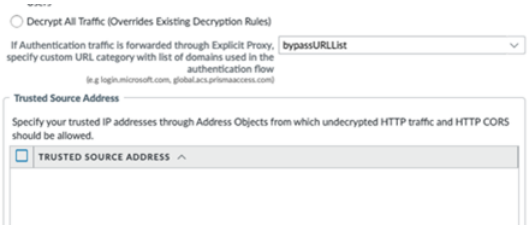
所有對 Proxy 的要求都會進行驗證。不過，如果您透過 Proxy 傳遞 IDP 流程，則需要略過它們，驗證才能成功。

在此範例中，我們略過 GlobalProtect 入口網站和 Okta，但請根據您使用的 IDP 自訂這些項目。

1. 在選取 **Explicit_Proxy_Device_Group** 後，選取 **Object**（物件） > **Custom Objects**（自訂物件） > **URL Category**（**URL** 類別），並建立自訂 URL 類別。
2. 在自訂 URL 類別中，新增需要略過 EP 驗證的所有 FQDN 網域。




3. 選取 **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users**（行動使用者） > **Explicit Proxy**（明確 **Proxy**） > **Settings**（設定） > **Authentication Settings**（驗證設定），並附加自訂 URL 類別。




4. 提交並推送到 **Explicit_Proxy_Device_Group**。

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 設定 GlobalProtect 入口網站。

在通道和 *Proxy* 模式中，您設定的連線方法僅適用於透過 *GlobalProtect* 以通道傳送的流量。代理程式型 *Proxy* 功能將提供一直開啟網際網路安全性。即使您設定了隨選連線方法，但基於一直開啟網際網路安全性，即使使用者中斷 *GlobalProtect* 應用程式連線，所有網際網路繫結流量仍將透過 *Proxy* 傳送。

1. 在裝載區域中，按一下 **Configure**（設定）。
2. 在 **General**（一般）頁籤上，指定 **Portal Name Type**（入口網站名稱類型）：

   **Use Default Domain**（使用預設網域）—如果您選取此選項，您的入口網站主機名稱會使用預設網域名稱：.gpcloudservice.com.在此情況下，只需輸入一個入口網站主機名稱以附加到

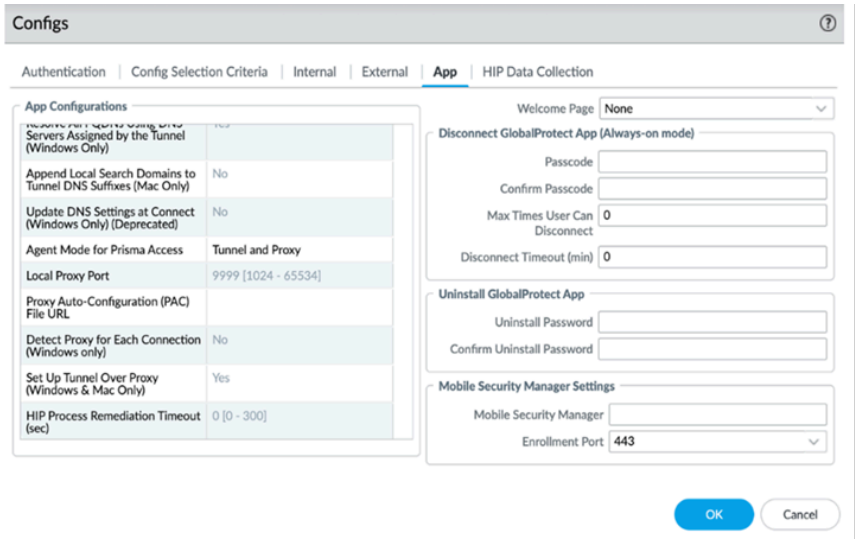
 ©2025 Palo Alto Networks, Inc.

預設網域名稱。Prisma Access 將自動建立必要的憑證，並將主機名稱發佈到公用 DNS 伺服器。

**Use Company Domain**（使用公司網域）—如果您想要入口網站主機名稱中的網域符合貴公司網域名稱（例如，myportal.mydomain.com），請選取此選項。

3. 選取一個 **Authentication Profile**（驗證設定檔），指定 Prisma Access 應如何驗證行動使用者，或建立新的驗證設定檔。
4. （選用）選取一個 **Authentication Override Certificate**（驗證覆寫憑證），以加密行動使用者用來驗證入口網站和閘道的安全 cookie。

1. 在 GlobalProtect 上啟用通道和 Proxy 模式。
   1. 選取 **Network**（網路） > **GlobalProtect Portals**（**GlobalProtect** 入口網站）。
   2. 選取您新增代理程式組態的入口網站組態，然後選取 **Agent**（代理程式）頁籤。
   3. 在 **Agent**（代理程式）頁籤上，選取 **App**（應用程式）。
   4. 在應用程式組態區域中，將 **Agent Mode for Prisma Access**（**Prisma Access** 的代理程式模式）設定為 **Tunnel and Proxy**（通道和 **Proxy**），以將網際網路流量傳送至 Prisma Access 明確 Proxy，並將私人應用程式流量傳送到 VPN。




2. 執行選用的組態。
   1. （選用）設定本機 Proxy 連接埠。連接埠範圍為 1024 到 65534，預設連接埠為 9999。如果預設連接埠不可用，GlobalProtect 將嘗試 9999 到 10009 範圍內的其他 10 個連接埠，並使用可用的連接埠。您還可以在該範圍內挑選自己的連接埠號碼。
   2. （選用）如果要將 Proxy 設定的自訂 PAC URL 推送到端點，請設定 PAC 自動設定 (PAC) 檔案 URL。一旦使用者連線，PAC URL 就會推送到端點。當使用者中斷連線 GlobalProtect 應用程式，端點 Proxy 設定會自動停用並還原為以前的設定。
   3. （選用）如果您想要使用者檢查入口網站是否有任何新設定，請啟用允許使用者重新探索網路。
   4. （選用）設定 GlobalProtect 應用程式設定重新整理間隔（小時）。根據預設，GlobalProtect 用戶端每 24 小時重新整理一次快取的入口網站設定。您可以根據業務需求變更重新整理間隔。
3. 在 分割通道組態中，排除明確 Proxy FQDN 和 PAC 檔案 FQDN。


©2025 Palo Alto Networks, Inc.

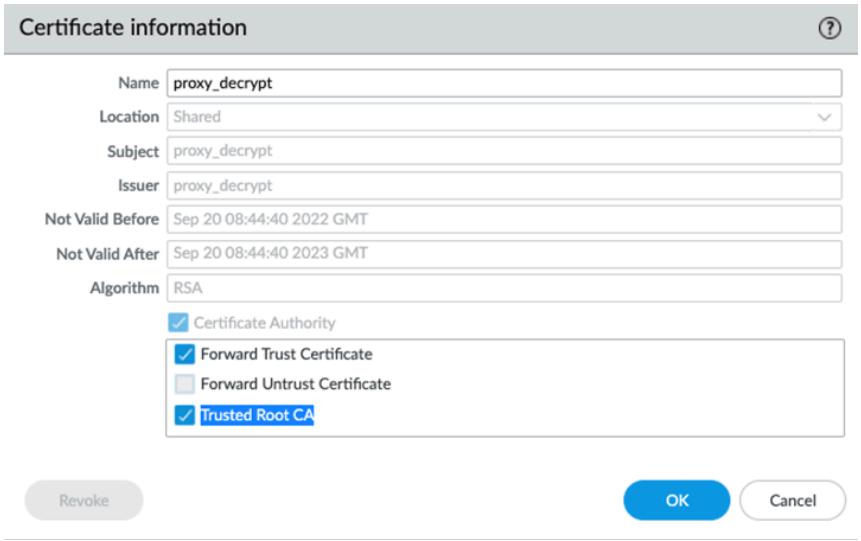
**STEP 4 |** 透過設定下列設定來啟用一直開啟網際網路安全性：

1. 將允許使用者停用 GlobalProtect 設定為 **Disallow**（不允許）、**Allow with Passcode**（透過密碼允許）或 **Allow with Ticket**（透過票證允許）。
2. 將允許使用者從 GlobalProtect 應用程式登出設定為 **No**（否）。

**STEP 5 |** （選用）為明確 Proxy 流量 設定解密政策。

如果啟用解密，請確保解密憑證也設定為受信任的根 CA。

1. 選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證），並建立一個憑證，作為受信任根 CA 和轉送信任憑證。




2. 使用 SSL 正向 Proxy 在 **Explicit_Proxy_Device Group** 下建立解密規則。

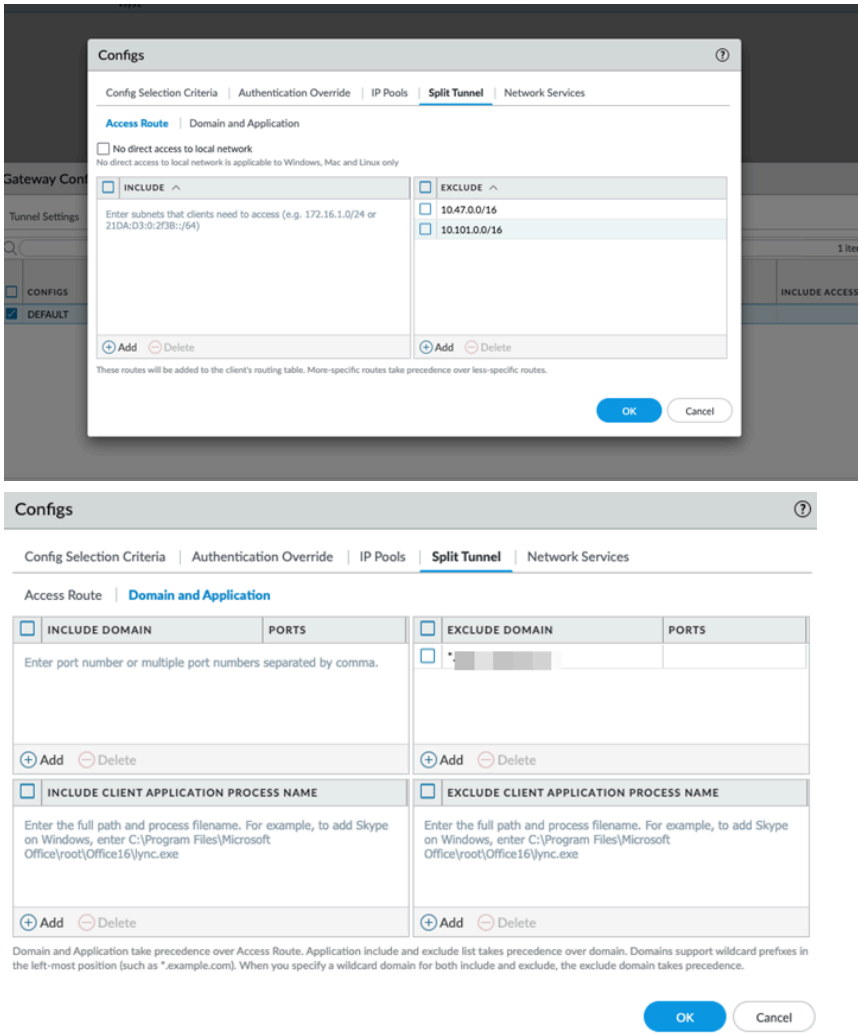
**STEP 6 |** 為明確 Proxy 流量設定安全性政策規則。

- 選取 **Manage**（管理） > **Security Services**（安全性服務） > **Security Policy**（安全性政策） > 。
- 遵循網際網路閘道安全性政策最佳做法。


©2025 Palo Alto Networks, Inc.

**STEP 7 |** 在 Panorama 上設定分割通道。

1. 選取 **Network**（網路） > **Mobile User Template**（行動使用者範本） > **Gateways**（閘道） > **GlobalProtect_ExternalGateway** > **Agent**（代理程式） > **Client Settings**（用戶端設定） > **Split**（分割）。
2. 根據路由和網域設定通道。







 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** （選用）在非預設路由網路中以通道和 Proxy 模式設定 GlobalProtect 應用程式。

- （選用）在內部託管 PAC 檔案，並新增 Prisma Access 明確 Proxy FQDN 作為 PAC 檔案中的 Proxy，或將 PAC 檔案託管在轉送設定檔中，並在您的網路中新增 PAC 服務IP 位址的路由。
- 驗證 GlobalProtect 入口網站 URL 和 IDP URL 是否正在轉送到 Prisma Access 明確 Proxy。
- 在週邊裝置上設定明確 Proxy FQDN 或 IP 位址的路由，以允許使用者透過明確 Proxy 存取網際網路。
- （選用）如果使用者無法解析分支網路中的公用網域，並將內部 IP 位址的目的地 NAT 新增到明確 Proxy FQDN 或 IP 位址，請新增 DNS 記錄以將 Prisma Access 明確 Proxy FQDN 解析為內部 IP 位址。
- 若要讓使用者在辦公室時可直接存取私人應用程式：
  - 直接存取—啟用內部主機偵測並將內部閘道清單保持空白。

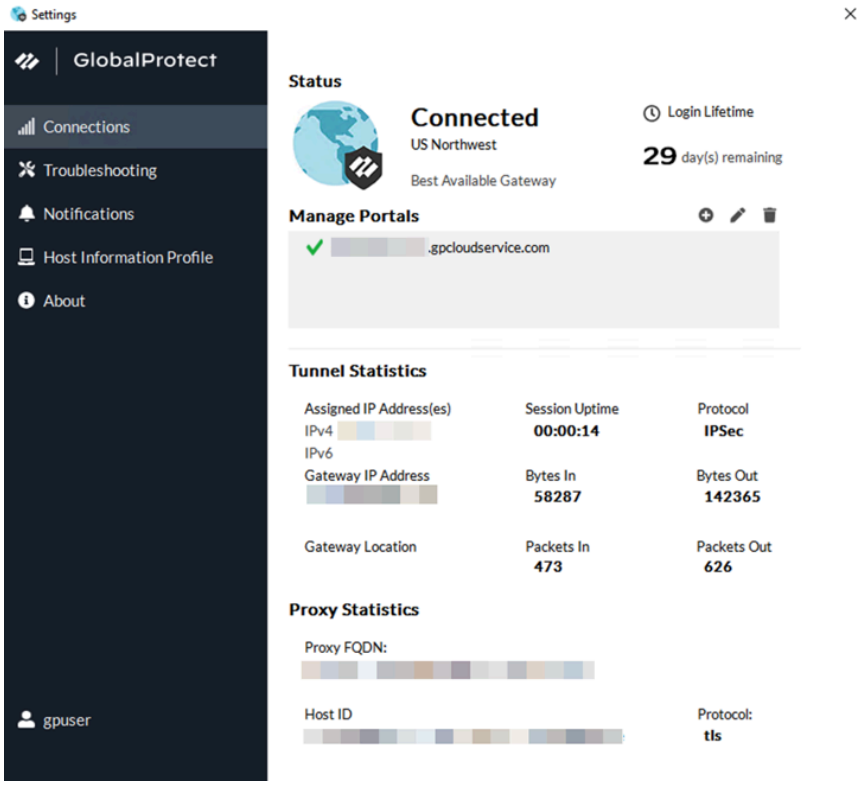
**STEP 9 |** **Commit**（提交）您的變更至 Panorama，並 **Commit and Push**（提交並推送）組態變更至 Prisma Access **Mobile Users**（行動使用者）和 **Explicit Proxy**（明確 **Proxy**）。

 ©2025 Palo Alto Networks, Inc.

**STEP 10 |** 驗證代理程式 Proxy 部署並針對其進行疑難排解。

1. 在 GlobalProtect 應用程式 **Connections**（連線）頁籤上，於 **Settings**（設定）下驗證網路連線的相關資訊。

   1. 開啟 GlobalProtect 應用程式。
   2. 選取 **Settings**（設定）以開啟 GlobalProtect 設定面板，然後選取 **Connections**（連線）。




2. 檢視並收集 GlobalProtect 日誌

   檢視 PanGPS 日誌以驗證 GlobalProtect 入口網站上的 Proxy 模式組態。

   您可以透過在 PanGPS 日誌中尋找以下事件來驗證 Proxy 模式是否已設定：

   `OnProxyAgentMode`：混合模式

   若要在 Panorama 中檢視 GlobalProtect 日誌，請選取 **Monitor**（監控） > **Logs**（日誌）和：

   - **GlobalProtect**，適用於驗證日誌
   - **Traffic**（流量）和 **Decryption**（解密），適用於使用者存取日誌

使用一直開啟連線方法中斷連線並停用通道和 **Proxy** 模式

從 GlobalProtect 6.3.1 版開始，當您將 GlobalProtect 應用程式的 **Tunnel and Proxy**（通道和 **Proxy**）模式，以及 **Always-On**（一直開啟）模式設定為連線方法，並想要中斷連線通道和 Proxy 模式時，必須執行以下步驟：

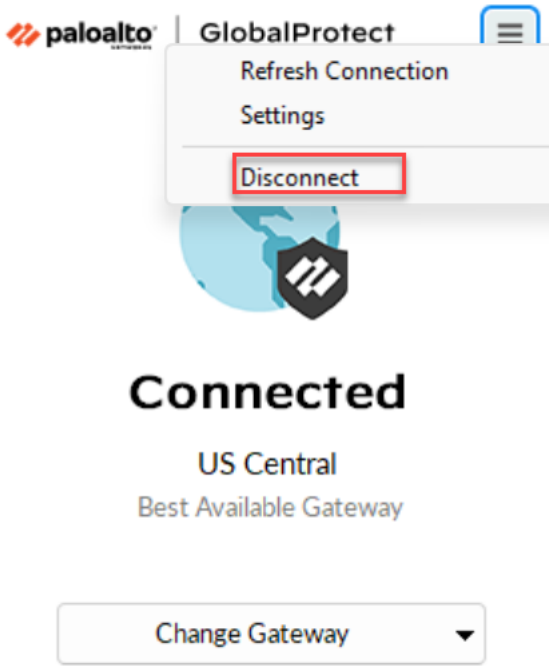
1. 中斷連線 GlobalProtect 應用程式以中斷通道 (VPN) 連線。當您中斷連線應用程式時，通道 (VPN) 連線會中斷，而應用程式仍將透過 Proxy 模式保持連線。

 ©2025 Palo Alto Networks, Inc.

2. 停用 GlobalProtect 應用程式以同時中斷連線通道和 Proxy 模式。當您停用應用程式時，通道和 Proxy 模式都將中斷連線，而且應用程式將不再連線。

若要中斷連線和停用透過 **Tunnel and Proxy**（通道和 **Proxy**）（混合模式）和 **Always-On**（一直開啟）連線方法設定的 GlobalProtect 應用程式，您必須：

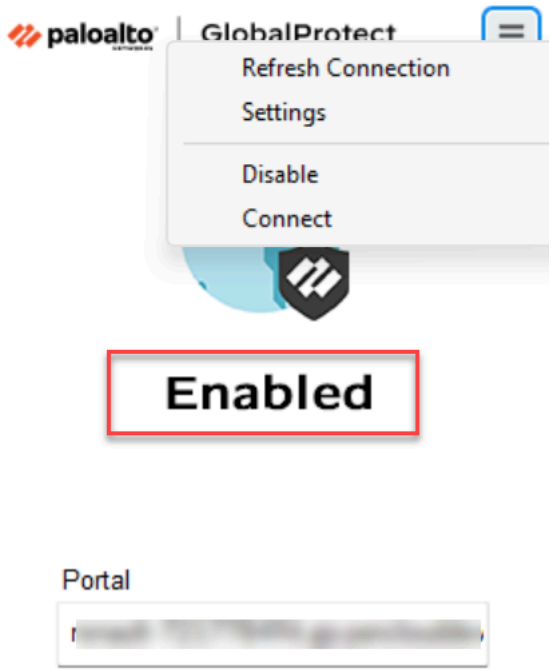
1. 使用漢堡功能表中的 **Disconnect**（中斷連線）選項來中斷連線 GlobalProtect 應用程式。當您中斷連線應用程式時，通道 (VPN) 連線會中斷。



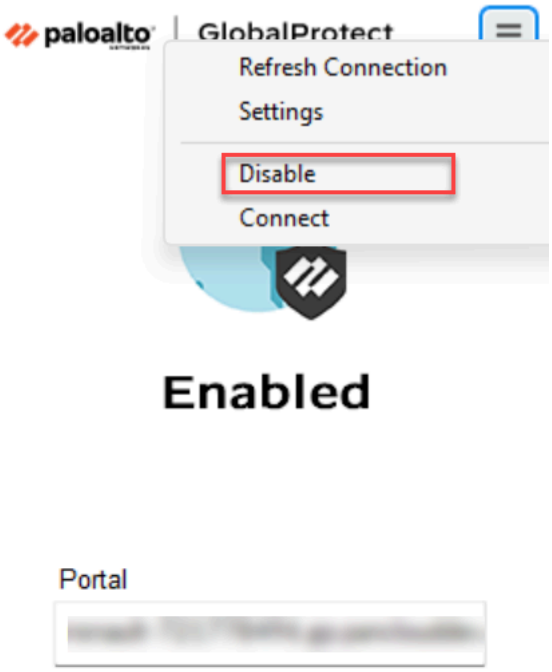

在您中斷連線應用程式之後，VPN 連線會中斷，但 Proxy 模式會啟用。該應用程式仍將透過 Proxy 模式連線，並且其會將狀態顯示為 **Enabled**（已啟用）。

如果您想要重新連線通道 *(VPN)*，可以使用漢堡功能表中的 ***Connect***（連線）選項。


©2025 Palo Alto Networks, Inc.

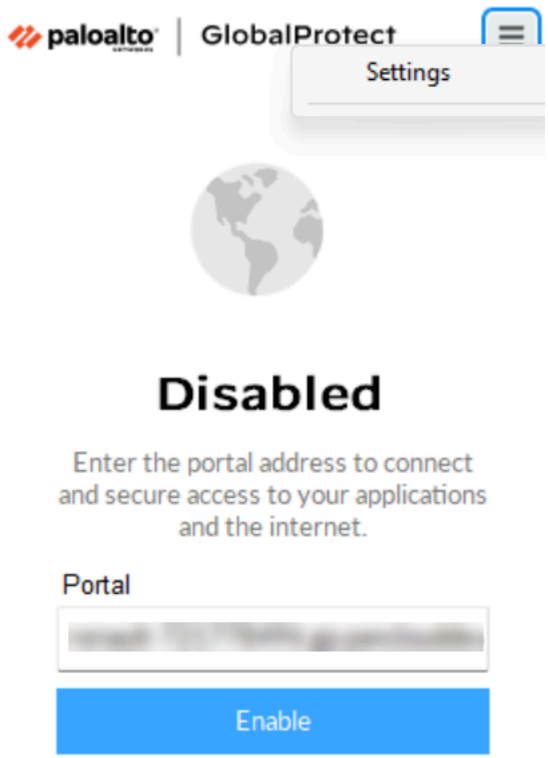



2. 使用漢堡功能表中的 **Disable**（停用）選項停用 GlobalProtect 應用程式。在您停用應用程式之後，通道和 Proxy 連線都會中斷。




該應用程式將被停用，且其會將狀態顯示為 **Disabled**（已停用）。

 ©2025 Palo Alto Networks, Inc.




# 代理程式型 Proxy 流量的私人 IP 位址可見性和強制執行

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• Prisma Access (Managed by Strata Cloud Manager) | • Prisma Access 5.2<br>• 適用於 Windows 或 macOS 的 GlobalProtect 應用程式 6.3.1 版<br>• Prisma Access 資料平面 10.2.4<br>• Prisma Access 行動使用者授權<br>• Panorama 外掛程式 5.2.0 版 |

透過分支的 GlobalProtect 代理程式連線至 Prisma Access 明確 Proxy 的使用者可以利用端點的私人 IP 位址來進行記錄或套用 IP 位址型強制執行。

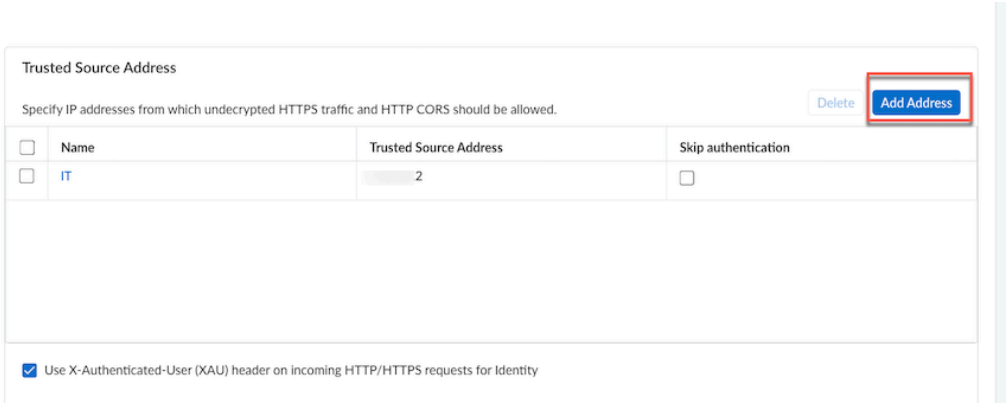
- Strata Cloud Manager
- Panorama

## 代理程式型 Proxy 流量的私人 IP 位址可視性和強制執行 (Strata Cloud Manager)

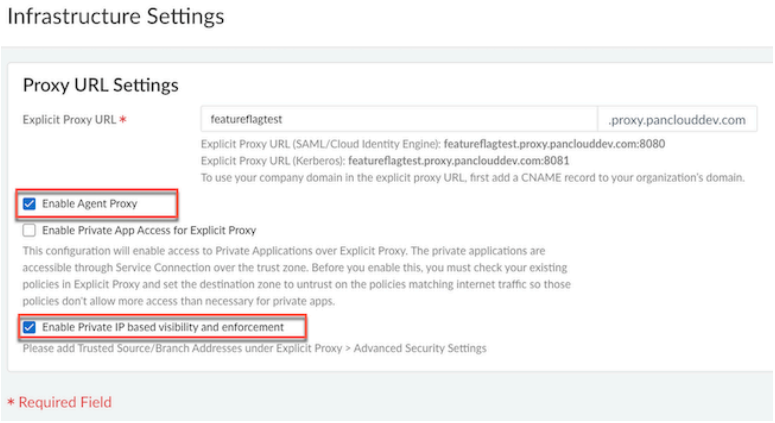
**STEP 1 |** 為行動使用者啟用代理程式型 Proxy 功能（Proxy 模式或通道和 Proxy 模式）。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 導覽至 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Explicit Proxy**（明確 **Proxy**） > **Advanced Security Settings**（進階安全性設定），然後按一下設定圖示。在 **Trusted Source Address**（受信任的來源位址）下，新增分支輸出 IP 位址。




**STEP 3 |** 導覽至 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Explicit Proxy**（明確 **Proxy**） > **Infrastructure Settings**（基礎結構設定）。在 **Proxy URL Settings**（**Proxy URL** 設定）下，啟用 **Enable Source IP based visibility and enforcement**（來源 **IP** 型可視性和強制執行），然後按一下 **Save**（儲存）。




**STEP 4 |** （選用）使用端點的來源 IP 位址設定 安全性規則。

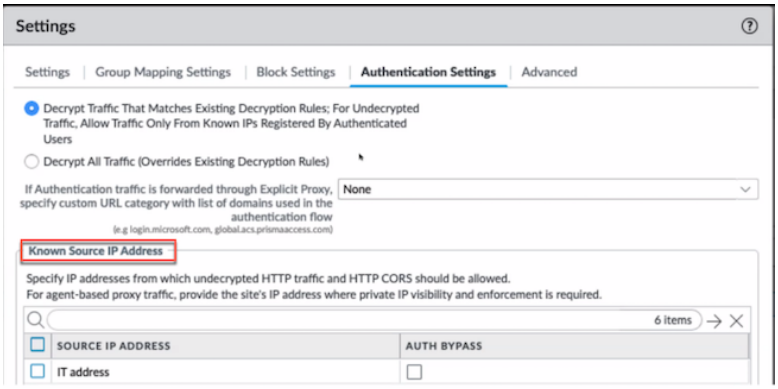
**STEP 5 |** **Push Config**（推送組態）至 **Explicit Proxy**（明確 **Proxy**）。

## 代理程式型 Proxy 流量的私人 IP 位址可視性和強制執行 (Panorama)

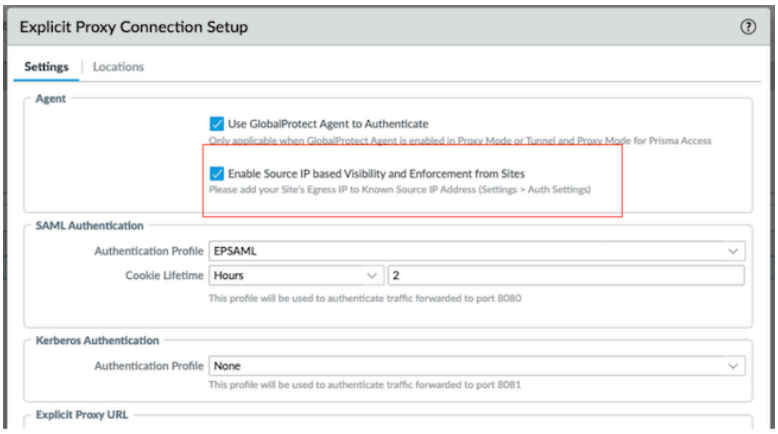
**STEP 1 |** 為行動使用者啟用代理程式型 Proxy 功能（Proxy 模式和通道和 Proxy 模式）。


©2025 Palo Alto Networks, Inc.

**STEP 2 |** 導覽至 **Cloud Services**（雲端服務） > **Configuration**（組態） > **Mobile Users**（行動使用者） > **Explicit Proxy**（明確 **Proxy**） > **Settings**（設定） > **Authentication Settings**（驗證設定），然後在 **Known Source IP Address**（已知來源 **IP** 位址）下新增分支輸出 IP 位址。.




**STEP 3 |** 導覽至 **Cloud Services**（雲端服務） > **Configuration**（組態） > **Mobile Users-Explicit Proxy**（行動使用者-明確 **Proxy**）。在 **Agent**（代理程式）下，啟用 **Enable Source IP based Visibility and Enforcement from Sites**（從網站啟用來源 **IP** 型可視性和強制執行），然後按一下 **OK**（確定）。




**STEP 4 |** （選用）使用端點的來源 IP 位址設定 安全性規則。

**STEP 5 |** 提交並推送到 **Explicit_Proxy_Device_Group**。

# 用於明確 Proxy 的 SAML 驗證

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | Prisma Access 授權 |

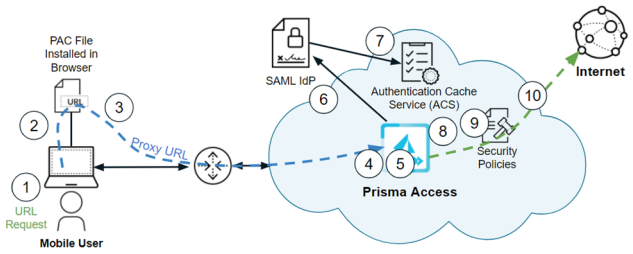
瞭解具有 SAML 的明確 Proxy 如何運作，以及如何設定它。

- 具有 SAML 的明確 Proxy 如何處理流量
- 設定具有 SAML 的明確 Proxy

 ©2025 Palo Alto Networks, Inc.

## 具有 SAML 的明確 Proxy 如何處理流量

以下是具有 SAML 的明確 Proxy 的運作方式。沿著看看流量採取的路徑：




**STEP 1 |** 行動使用者透過使用 Web 瀏覽器輸入 URL 或 IP 位址，瀏覽網際網路或存取 SaaS 應用程式。

**STEP 2 |** 行動使用者端點上的瀏覽器會檢查是否有 PAC 檔案。

此 PAC 檔案指定 URL 或 SaaS 要求應該前往 Prisma Access 明確 Proxy。

**STEP 3 |** HTTPS 用戶端（行動使用者端點上的瀏覽器）會將 URL 要求轉送至 Proxy URL。

**STEP 4 |** 流量會重新導向到明確 Proxy，而 Proxy 會解密流量。

**STEP 5 |** Proxy 會檢查流量並檢查是否有 Prisma Access 明確 Proxy 設定的驗證 Cookie。

Cookie 包含可識別行動使用者的資訊，並使用 Cookie 來驗證使用者。

**STEP 6 |** 如果在檢查 Cookie 後，Prisma Access 確定使用者未進行驗證，則其會重新導向使用者進行驗證。

**STEP 7 |** 在 IdP 驗證使用者之後，Prisma Access 將在驗證快取服務 (ACS) 中儲存使用者的驗證狀態。驗證的有效期基於您在明確 Proxy 設定期間指定的 **Cookie Lifetime**（**Cookie** 存留時間）值。

**STEP 8 |** 明確 Proxy 會檢查我們的 Cookie 是否存在且有效。如果 Cookie 不存在或無效，則使用者將重新導向到 ACS。在 ACS 確認使用者的驗證之後，該使用者會使用權杖重新導向回到明確 Proxy。然後，Proxy 會驗證該權杖，並為該使用者設定該網域的 Cookie。

**STEP 9 |** Prisma Access 根據管理員已設定的安全性政策規則套用安全性強制執行。

**STEP 10 |** 如果安全性政策規則未封鎖 URL，Prisma Access 會將 URL 要求傳送到網際網路。

**STEP 11 |** （選用）為了始終開啟網際網路安全性，在 GlobalProtect 中設定明確 Proxy 連線。啟用此功能以實現網際網路流量的始終開啟安全性，同時透過 GlobalProtect 或第三方 VPN 提供對私人應用程式的隨選存取。

## 設定具有 SAML 的明確 Proxy

遵循下列步驟設定具有 SAML 驗證的明確 Proxy。

- Strata Cloud Manager
- Panorama


©2025 Palo Alto Networks, Inc.

## 使用 SAML 設定明確 Proxy (Strata Cloud Manager)

**STEP 1 |** 設定明確 Proxy。

**STEP 2 |** （選用）為明確 Proxy 設定 Cloud Identity Engine 驗證。

**STEP 3 |** 設定 安全性政策規則。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Configuration Scope:Explicit Proxy**（設定範圍：明確 **Proxy**） > **Security Services**（安全性服務） > **Security Policy**（安全性政策）。
2. 根據您的需求和網際網路閘道安全性政策最佳做法自訂預設政策規則。

   使用 *Prisma Access 5.1* 和 *PAN-OS 10.2.10* 或更高版本的 資料平面，您只需要 ***Allow Web Access to Known Users***（允許已知使用者進行 ***Web*** 存取）安全性政策規則。

**STEP 4 |** 推送您的設定變更。

## 使用 SAML 設定明確 Proxy (Panorama)

**STEP 1 |** 設定明確 Proxy。

**STEP 2 |** （選用）為明確 Proxy 設定 Cloud Identity Engine 驗證。

**STEP 3 |** 根據您的 Prisma Access 版本和資料平面版本，設定單一政策規則或多個政策規則。

| 版本需求 | 組態設定 |
| --- | --- |
| Prisma Access 5.1 或更高版本，以及 PAN-OS 10.2.10 或更高版本的資料平面。 | 為預先驗證使用者流量設定安全性政策規則。<br>1. 選取 **Explicit_Proxy_Device_Group**。<br>2. 使用 **Web App** 標籤建立應用程式篩選器。<br>3. 選取 **Policies**（政策） > **Pre Rules**（前置規則） > **Add**（新增）。<br>4. 建立規則。<br>   1. **Add**（新增）規則。<br>   2. 給與它一個描述性名稱。<br>      例如，**`allow-pre-auth`**<br>   3. 在 **Application**（應用程式）頁籤下，**Add**（新增） **Web App** 應用程式篩選器。<br>   4. 在 **Source**（來源）頁籤下，**Add**（新增）**known-user**。 |


©2025 Palo Alto Networks, Inc.

| 版本需求 | 組態設定 |
| --- | --- |
| 所有其他 Prisma Access 和資料平面版本。 | 根據您的需求和網際網路閘道安全性政策最佳做法設定安全性政策規則。 |

**STEP 4 |** **Commit**（提交）組態。

# 設定明確 Proxy

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>如果您想要在 Prisma Access 環境中於明確 Proxy 上啟用私人來源 IP 型可視性和強制執行，請與您的客戶團隊聯繫以進一步瞭解。 | • Prisma Access 授權 |

使用明確 Proxy 透過將瀏覽器流量重新導向到 Prisma Access 來保護行動使用者。

裝載指導方針—當您授權和裝載明確 Proxy 部署時，請使用以下指導方針：

- 明確 Proxy 支援 Prisma Access 位置的子集。
- 您無法新增以兩個星號表示的位置；這些是本機區域，且 Prisma Access 不支援這些區域。
- 如果您具有 Prisma Access for Users 的本機或評估授權，並且您有行動使用者—GlobalProtect 部署，以及行動使用者—明確 Proxy 部署，則可以為每個部署最多部署5 個位置（行動使用者—GlobalProtect 最多五個位置，行動使用者—明確 Proxy 最多五個位置）。如果您具有全球授權，則位置數目上限沒有任何限制。
- 明確 Proxy 在以下條件下支援多租用戶：如果您有現有的 Prisma Access 非多租用戶部署，並將其轉換為多租用戶部署，則只有第一個租用戶（您移轉的租用戶）支援明確 Proxy。您在第一個租用戶之後為多租戶部署而建立的任何後續租用戶都不支援明確 Proxy。
- 裝載明確 Proxy 部署時，Palo Alto Networks 建議在單一瀏覽器中執行所有設定。不過，您可以從多個瀏覽器或瀏覽器工作階段中新增安全性政策。
- 不支援 URL 篩選動作為 **continue**（繼續）或 **override**（覆寫），且這些動作不會使用明確 Proxy。

瞭解如何設定明確 Proxy。

- Strata Cloud Manager
- Panorama

## Cloud Management

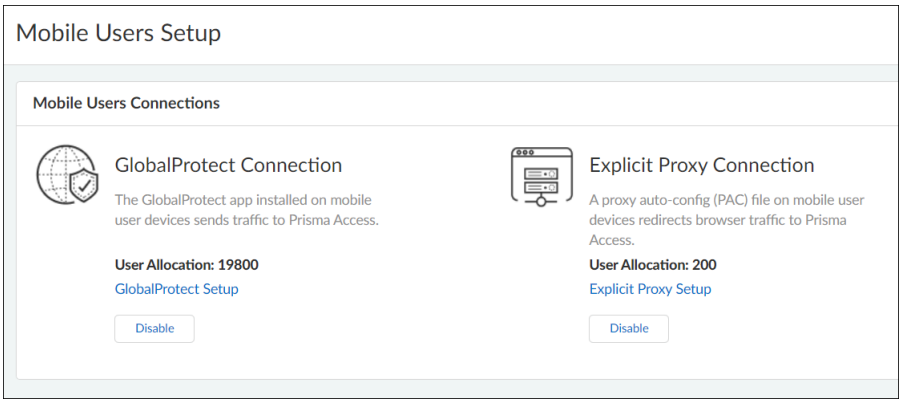
為行動使用者設定明確 Proxy 連線；透過明確 Proxy，行動使用者裝置上的 Proxy 自動設定 (PAC) 檔案會將瀏覽器流量重新導向到 Prisma Access。

開始之前，請確保您檢閱了明確 Proxy 指導方針。


©2025 Palo Alto Networks, Inc.

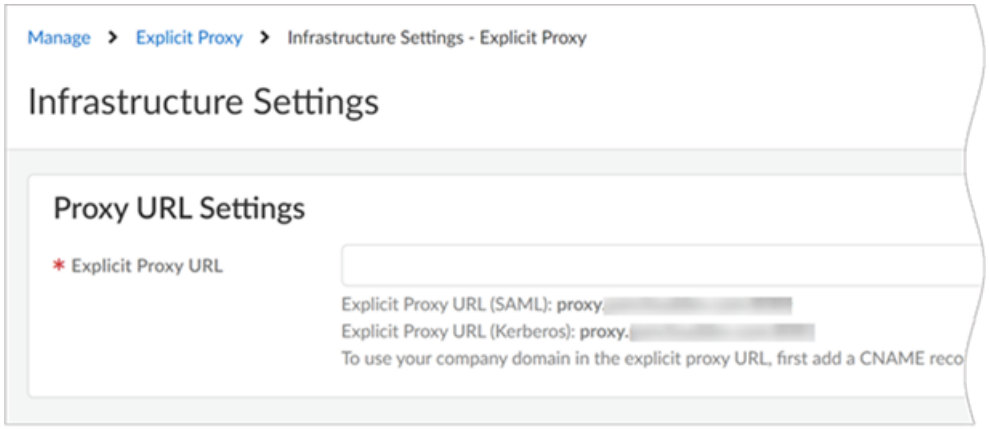
**STEP 1 |** 啟用明確 **Proxy** 並配置使用者

前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Mobile Users**（行動使用者），以開始設定明確 Proxy。當您啟用明確 Proxy 時，系統會提示您指定將使用此連線類型的行動使用者數目。




**STEP 2 |** 新增行動使用者將用來連線至 **Prisma Access** 的 **Proxy** 設定

前往 **Infrastructure Settings**（基礎結構設定）：




1. 指定明確 Proxy URL。

   根據預設，名稱為 *proxyname*.proxy.prismaaccess.com，其中 *proxyname* 是您指定的子網域，並使用連接埠 8080。若要在明確 Proxy 中使用您的公司網域，請將 CNAME 記錄新增至您組織的網域。

   您可以使用 SAML 或 Kerberos 驗證類型來驗證行動使用者。

2. （選用）選取 **Enable Agent Proxy**（啟用代理程式 **Proxy**），以啟用代理程式型 Proxy 功能。

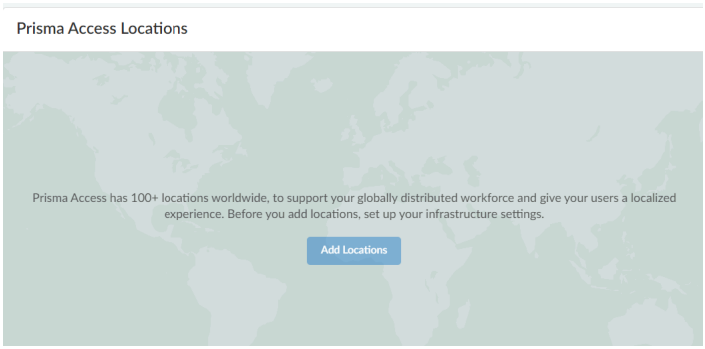
   啟用此功能以在 Proxy Mode（Proxy 模式）或 Tunnel and Proxy Mode（通道和 Proxy 模式）下設定明確 Proxy。

3. 使用轉送規則來編寫符合您需求的 PAC 檔案，或將您自己的 PAC 檔案上傳到轉送設定檔。

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 選擇您的行動使用者將連線至其中的 **Prisma Access** 位置

新增您想要支援行動使用者的 Prisma Access 位置。




地圖顯示 Prisma Access 位置。

為了獲得最佳使用者體驗，如果您限制了位置數目，請選擇離使用者最近的位置，或位於使用者相同國家/地區的位置。如果您行動使用者所在的國家/地區沒有可用位置，請選擇離使用者最近的位置，以獲得最佳效能。

您應該在至少兩個區域啟用明確 *Proxy* 位置，以確保區域備援。

**STEP 4 |** 驗證行動使用者

設定 **User Authentication**（使用者驗證），以便僅合法使用者有權存取您的服務和應用程式。

SAML 和 Kerberos 是支援的驗證通訊協定。Prisma Access 支援 PingOne、Azure AD 和 Okta 作為 SAML 驗證提供者，但您應該能夠使用任何支援 SAML 2.0 的廠商作為 SAML 識別提供者 (IdP)。進一步瞭解如何啟用行動使用者對 Prisma Access 進行驗證。

**STEP 5 |** 檢閱預設開啟的最佳做法安全性政策

Prisma Access 預設強制執行最佳做法安全性政策規則。這些規則允許您的使用者安全地瀏覽至一般的網際網路網站。使用者：

- 已被封鎖根據 URL 造訪已知的不良網站
- 已被封鎖上傳或下載已知為惡意的檔案
- 受到保護免於未知、從未見過的威脅
- 受到保護免於病毒、間諜軟體（命令和控制攻擊）及漏洞

完成初始設定後，您可以檢閱並更新這些預設規則，以符合您的企業需求。

**STEP 6 |** 驗證行動使用者位置是否作用中

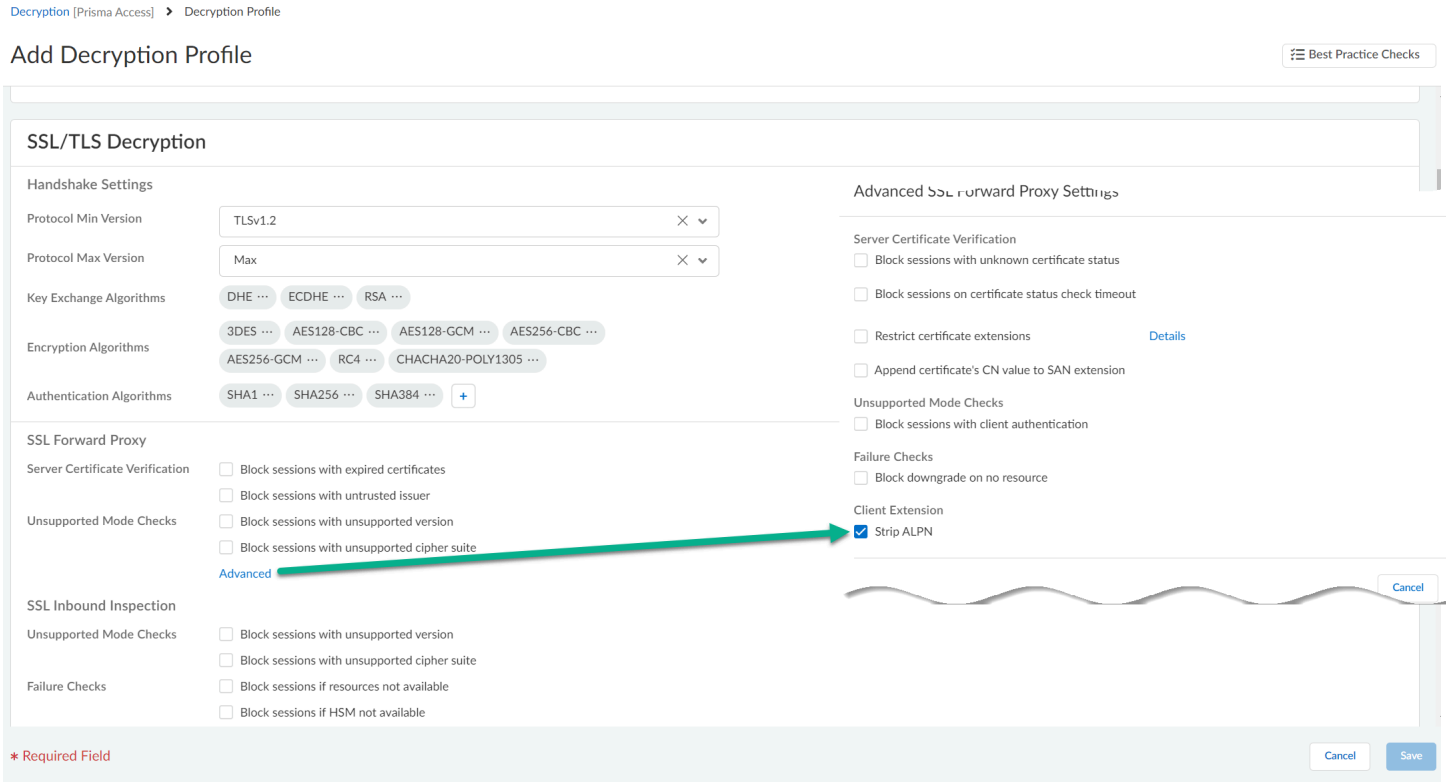
將您的初始設定推送至 Prisma Access 後，Prisma Access 就會開始佈建您的行動使用者環境。這最多可能需要 15 分鐘。您的行動使用者位置啟動並執行時，您可以在 [Mobile Users setup（行動使用者設定）] 頁面、[Overview（概要）] 上以及洞察內驗證他們。

您還可以選取 ***Manage***（管理） ***> Service Setup***（服務設定） ***> Mobile Users***（行動使用者）來驗證您的設定，然後編輯基礎結構設定，以確認閘道設定在您所佈建的每個位置中。


©2025 Palo Alto Networks, Inc.

**STEP 7 |** 為明確 **Proxy** 流量啟用解密

- 將最大支援的 TLS 版本設定為 1.2。
- 設定 **Strip ALPN**（除去 **ALPN**）（進階 SSL 正向 Proxy 設定），因為明確 Proxy 不支援原生 HTTP/2，而且您必須移除 ALPN 標頭。




**STEP 8 |** 下載根 CA 並將其安裝在您的端點上，以進行 SSL 解密。

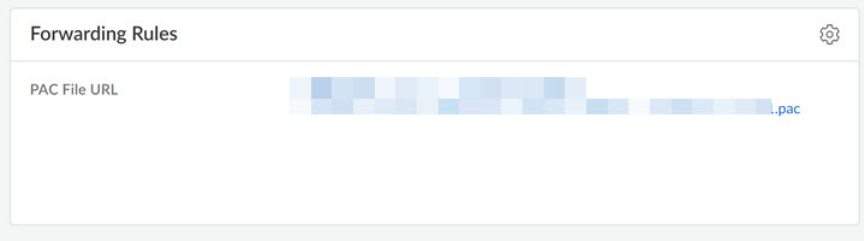

©2025 Palo Alto Networks, Inc.

**STEP 9 |** **Edit the PAC file content**（編輯 **PAC** 檔案內容）。

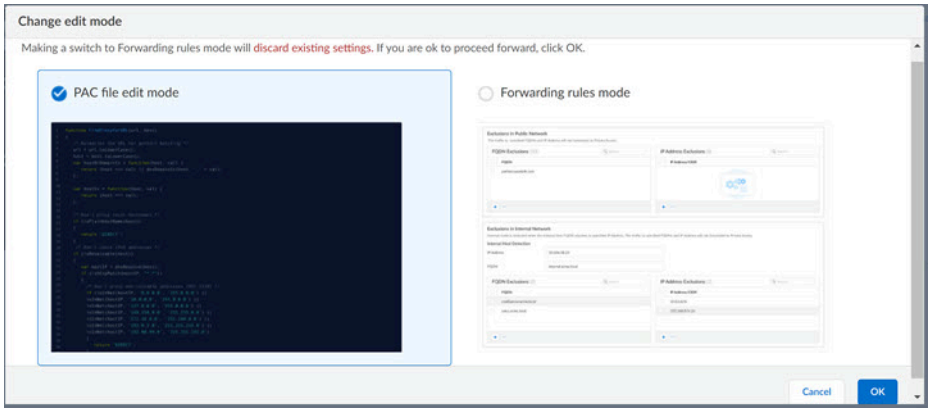
使用轉送設定檔來管理 *PAC* 檔案。

為符合您需求的明確 Proxy 編輯 Proxy 自動設定 (PAC) 檔案。GlobalProtect 應用程式根據 PAC 檔案中的轉送規則和邏輯將流量 Proxy 至 Prisma Access。

前往 **Forwarding Rules**（轉送規則）：




1. 下載 PAC 檔案並進行自訂，以便其符合您的需求。然後，在這裡再次匯入它，我們將為您提供 Prisma Access 託管 PAC 檔案所在位置的 URL。
2. 使用 **PAC File Editor**（**PAC** 檔案編輯器）模式或 **Forwarding rules mode**（轉送規則模式）編輯 PAC 檔案。
3. 預設會選取 **PAC File Editor**（**PAC** 檔案編輯器）模式。按一下 **OK**（確定），以在 PAC 檔案編輯模式下編輯。
4. 選取 **Forwarding rules mode**（轉送規則模式），然後按一下 **OK**（確定）。以在轉送規則模式下編輯。切換到轉送規則模式會捨棄現有的設定。

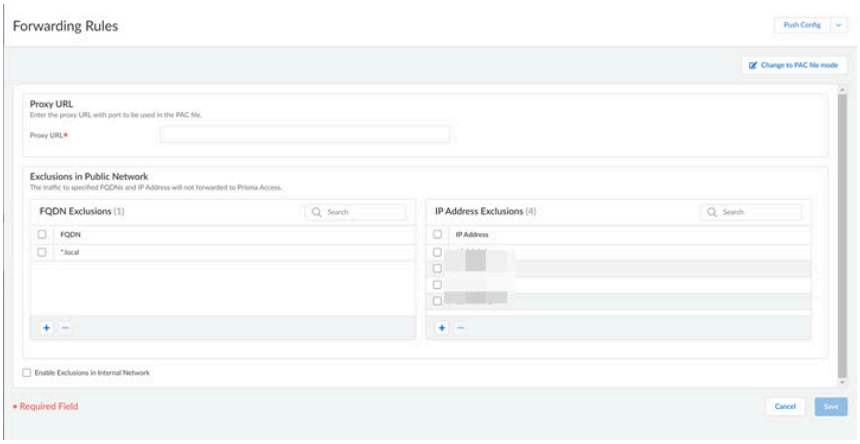



- 指定明確 **Proxy URL**，其中具有要在 PAC 檔案中使用的連接埠。

  根據預設，名稱為 proxyname.proxy.prismaaccess.com，其中 proxyname 是您指定的子網域，並使用連接埠 8080。
- 當您的明確 Proxy 行動使用者從公用網路連線到 Prisma Access 時，請 **Exclusions in Public Network**（公用網路中的排除）。
  - 設定 **FQDN Exclusions**（**FQDN** 排除）和 **IP Address Exclusions**（**IP** 位址排除）。將不會從 Prisma Access 轉送已排除的 FQDN 和 IP 位址。

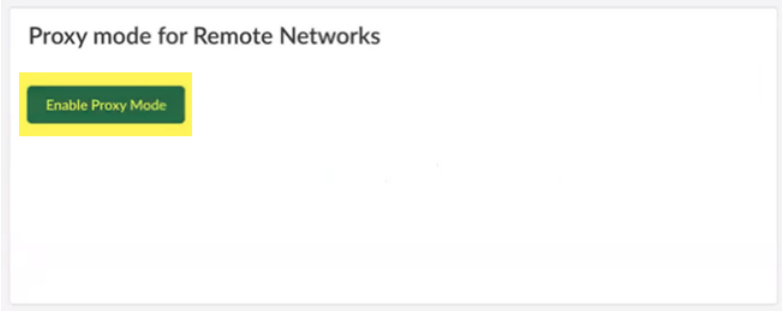
 ©2025 Palo Alto Networks, Inc.

- **Enable Exclusions in Internal Network**（在內部網路中啟用排除），以在明確 Proxy 行動使用者連線到內部網路上的 Prisma Access 時，為特定的 IP 位址或 FQDN 設定排除。
  - 指定以下排除，以在使用者位於內部網路時具有不同的流量排除。
    - 輸入只能從內部網路解析之主機的 **IP Address**（**IP** 位址）。
    - 輸入解析為您所輸入 IP 位址的 **FQDN**。
  - 為特定的 FQDN 和 IP 位址設定排除。將不會從 Prisma Access 轉送所指定 FQDN 和 IP 位址的流量。
- **Save**（儲存）變更。




**STEP 10 |** 設定 **Advanced Security Settings**（進階安全性設定）。

- 如果您想要透過安全 IPSec 通道將流量從您的分支轉送至明確 Proxy，請 **Enable Proxy Mode**（啟用 **Proxy** 模式），並擷取 Anycast IP 位址，如果您想要將明確 Proxy 與 Prisma Access 遠端網路結合使用的話。




  此解決方案會使用 Anycast 位址搭配遠端網路 IPSec 通道，以允許明確 Proxy 用於遠端網站或分支位置的中使用者和裝置。
- 僅限 Proxy 模式部署 如果在您的遠端網路上啟用了 Proxy 模式，請新增一個政策，以允許流量繫結至遠端網路上的 Anycast 和單點傳送 IP。如果您已啟用 **Source IP visibility**

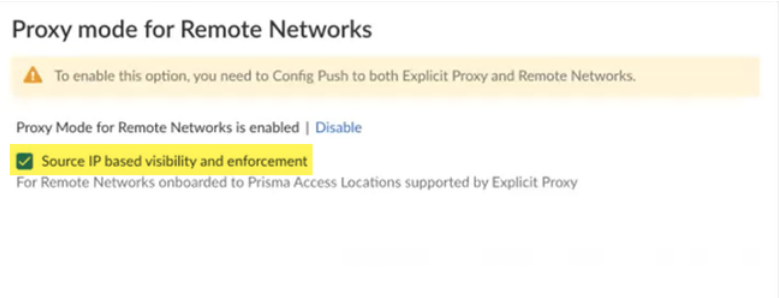
 ©2025 Palo Alto Networks, Inc.

**and enforcement**（來源 **IP** 可視性和強制執行），請在明確 Proxy 中使用安全性政策中的 **Source IP**（來源 **IP**）欄位來保護流量。您需要遠端網路中的額外政策。

- （選用）如果您啟用 Proxy 模式，則若要利用分支位置中將流量轉送到明確 Proxy 的系統私人 IP 位址，請選取 **Source IP based visibility and enforcement**（來源 **IP** 型可視性和強制執行）。

  此功能具有以下需求：

  - Prisma Access 資料平面至少為 10.2.4
  - 雲端服務外掛程式至少為 4.1 的 Prisma Access (Managed by Panorama) 部署
  - 來源 IP 位址僅針對明確 Proxy 支援的遠端網路位置顯示。




- 指定 **Block Sources**（封鎖來源）。

  將任何應該封鎖的來源 IP 位址流量新增到 **Block Source Address**（封鎖來源位址）清單。

  指定一個位址、位址群組或 EDL。

  若要從強制執行中排除 IP 位址清單項目，請 **Add Exception**（新增例外狀況），並選取要從封鎖中排除的 IP 位址。

- 指定 **Blocked Domains**（已封鎖的網域）。

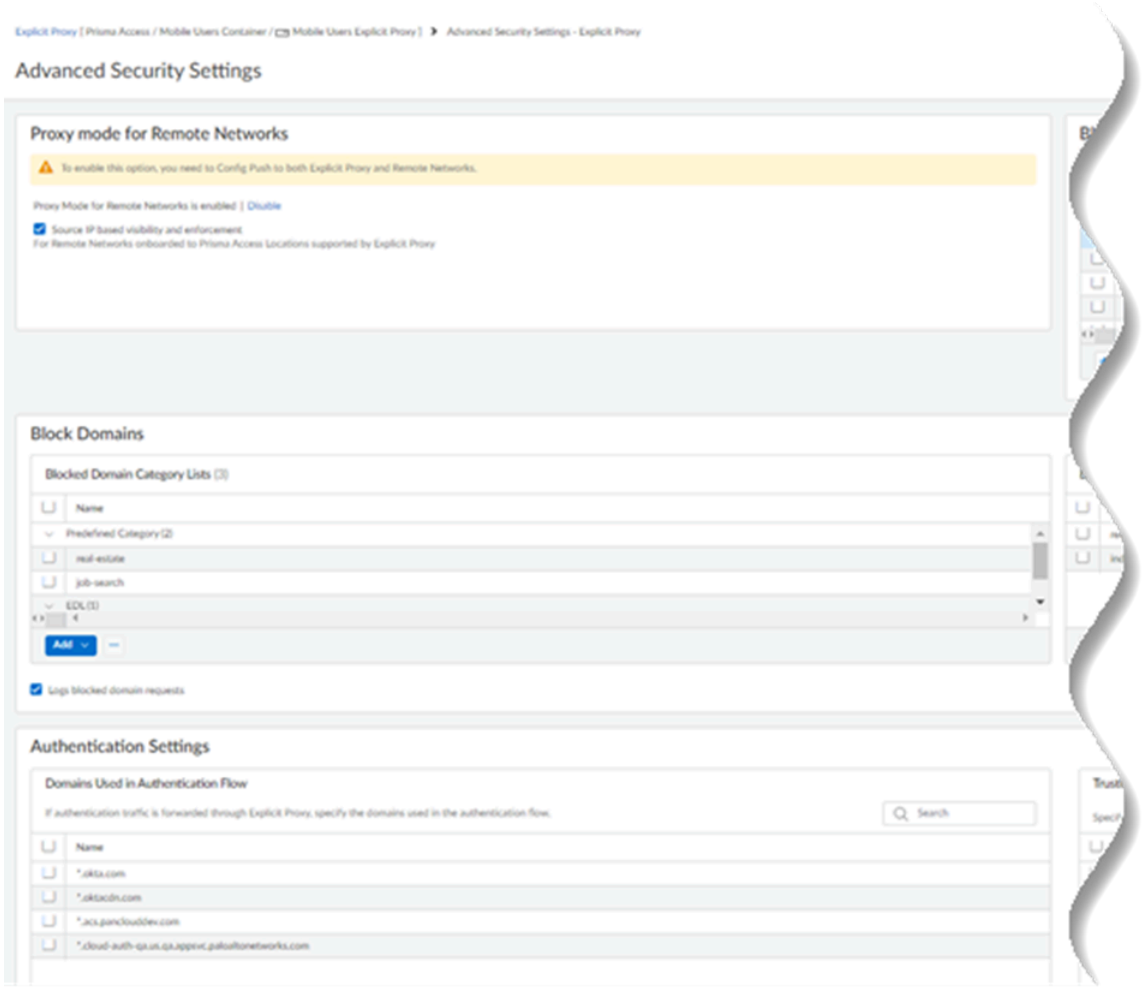
  為惡意網站或為您不想要使用者存取的任何網站指定網域或網域類別。當使用者起始 HTTP GET（用於未加密的要求）或 HTTP CONNECT（用於加密的請求）時，Prisma Access 會阻

 ©2025 Palo Alto Networks, Inc.

止使用者存取您在此區域中指定的 URL 和 IP 位址。當使用者嘗試存取遭封鎖的網站時，他們會收到一個封鎖頁面。

- 如果想要豁免封鎖的網域類別清單中包括的任何網域，請在 **Exception List**（例外清單）中指定它們。

  輸入的任何網域都會豁免而不被封鎖，即使它們出現在您已封鎖的網域類別中也一樣。
- 明確 Proxy 需要解密以驗證使用者。輸入 **Domains used in the authentication flow**（驗證流程中使用的域網域）。
-



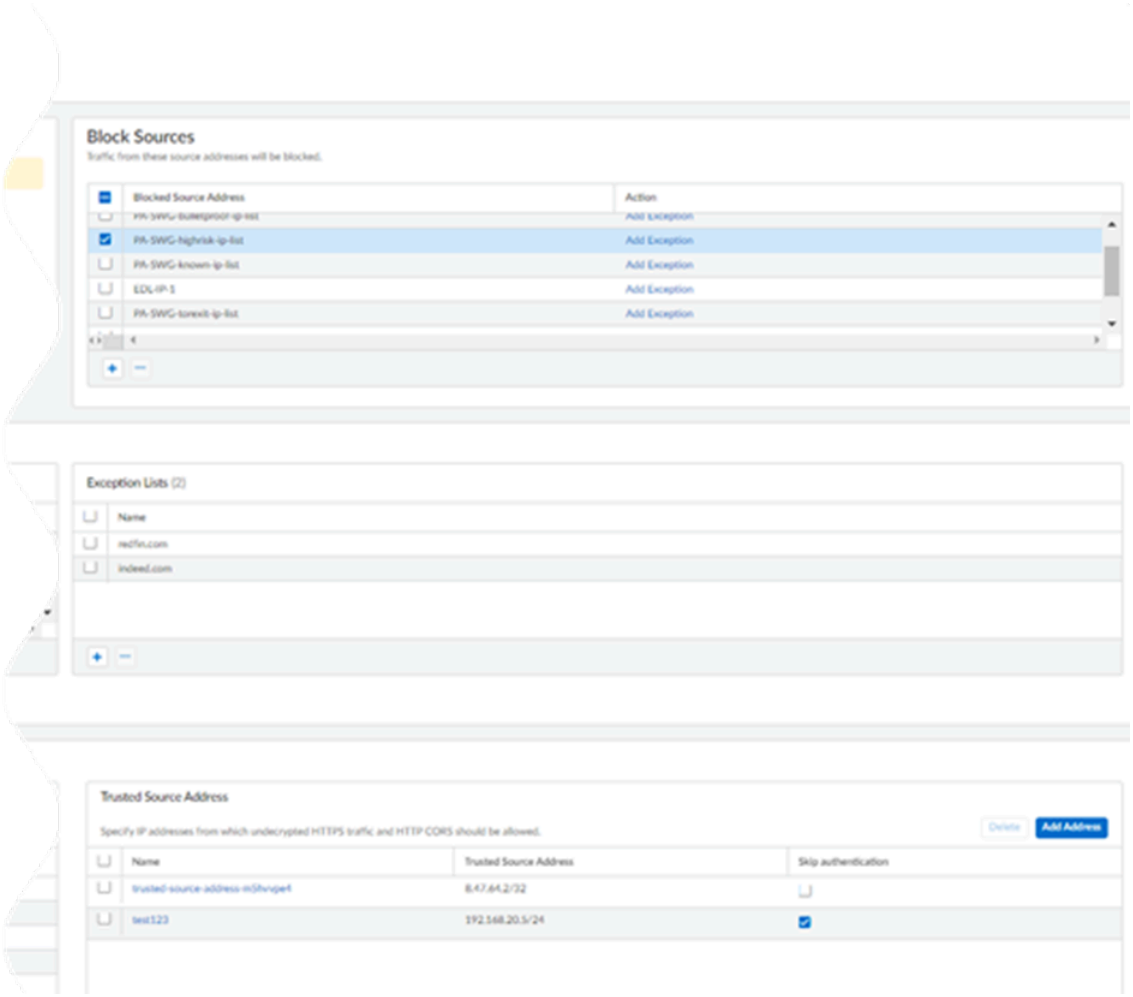

- 輸入其中未解密 HTTPS 或 HTTP 跨來源資源共用 (CORS) 流量被允許流向 **Trusted Source Address**（受信任的來源位址）的任何 IP 位址。
- 若要略過您所輸入的任何受信任來源位址的驗證，請選取 **Skip authentication**（跳過驗證）。

  您可以使用 **Skip authentication**（跳過驗證）搭配 **Source IP based visibility and enforcement**（來源 **IP** 型可視性和強制執行），來跳過無法驗證的無頭系統的驗證、設定安全性政策，以及獲得 Prisma Access 明確 Proxy 上流量的可視性。

  您可以新增 *IP* 位址或子網路。在擴展子網路之後，最多支援 *100,000* 個 *IP* 位址。

 ©2025 Palo Alto Networks, Inc.

如果您選取 **Skip authentication**（跳過驗證）來跳過位址物件的驗證，但稍後想要取消選取該位址物件的 **Skip authentication**（跳過驗證）來啟用驗證，則在您進行變更且提交並推送您的變更之後，最多可能需要 24 小時變更才會生效。

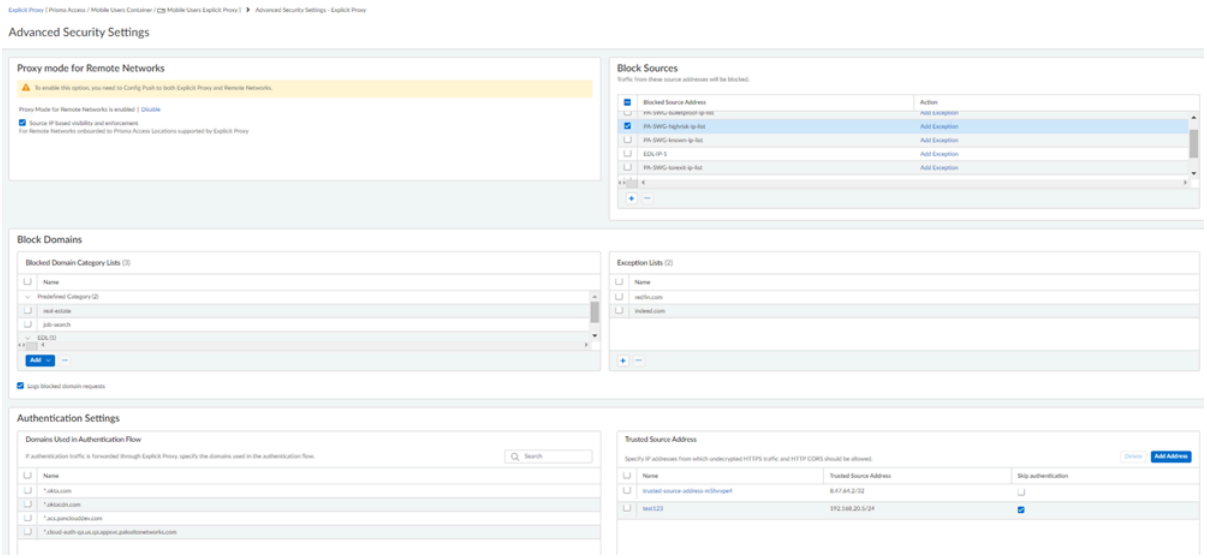
- 


- 如果您有明確 Proxy 部署並已新增受信任來源 IP 位址的清單，則可以 **Use X-Authenticated-User (XAU) headers on incoming HTTP/HTTPS requests for identity**（在傳

 ©2025 Palo Alto Networks, Inc.

入 **HTTP/HTTPS** 要求中使用 **X-Authenticated-User (XAU)** 標頭來進行驗證）。使用此功能以允許從另一個 Proxy 登入的使用者使用 XAU 標頭進行驗證。

您必須按一下 ***Save***（儲存），*XAU* 設定才會生效。




## 設定明確 Proxy (Panorama)

若要透過明確 Proxy 保護行動使用者，請完成下列步驟。

在您設定明確 Proxy 之前，請先查看計劃檢查清單，並瞭解如何設定明確 Proxy PAC 檔案。


©2025 Palo Alto Networks, Inc.

**STEP 1 |** 為明確 Proxy 設定驗證。

SAML 和 Kerberos 是支援的驗證類型。

為 IdP 和 Panorama 設定 SAML 驗證時，請使用以下指導方針：

- **Panorama** 指導方針：
  - 為 Prisma Access 設定 **SAML Identity Provider**（**SAML** 識別提供者）和 **Authentication Profile**（驗證設定檔）。您指定在稍後步驟中建立的驗證設定檔。
  - 確保您在 **Explicit_Proxy_Template** 下設定驗證設定檔。
  - 在 IdP 伺服器設定檔中以及在 Panorama 上 **Authentication Profile**（驗證設定檔）中使用 **mail** 作為使用者屬性。
  - 明確 Proxy 不支援在 SAML 識別提供者伺服器設定檔中 **Sign SAML Message to IdP**（將 **SAML** 訊息簽署至 **IdP**）。
  - 當您設定雲端識別引擎以擷取使用者和群組對應資訊時，請使用 **mail** 或 **userPrincipalName** 作為群組對應中的 **SamAccountName**。
  - 在明確 Proxy 設定期間設定 **Group Mapping Settings**（群組對應設定）時，請為主要使用者名稱和電子郵件使用相同的目錄屬性，否則 Prisma Access 無法準確反映使用者計數。例如，假設使用者設定檔如下：

    ```
    sAMAccountName: muser Netbios: example userPrincipalName:
     muser@example.com mail: mobile.user@example.com
    ```

    如果在雲端識別引擎設定中，您使用的 **Primary Username**（主要使用者名稱）是 `userPrincipalName`，而 **E-Mail**（電子郵件）是 `mail`，則 Strata Logging Service 在流量日誌中傳回的使用者資訊和 ACS 在驗證日誌中傳回的使用者資訊將會不同。在這個範例中，ACS 會將 **mail** 屬性 (mobile.user@example.com) 傳送到驗證日誌，而 Strata Logging Service 會將 **userPrincipalName** 屬性 (muser@example.com) 傳送到流量日誌。由於此不相符，當您在狀態（**Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Status**（狀態））頁面中檢查明確 Proxy 狀態時，在 **Current Users**（目前使用者）和 **Users (Last 90 days)**（使用者（過去 **90** 天））欄位中，您的使用者計數將不準確。基於此原因，在指定 **Group Mapping Settings**（群組對應設定）時，請對 **Primary Username**（主要使用者名稱）和 **E-Mail**（電子郵件）使用相同的目錄屬性（例如，**mail**）。

 ©2025 Palo Alto Networks, Inc.

- 使用 Panorama 來管理 Prisma Access 時，雲端識別引擎不會將使用者和群組資訊自動填入安全性政策規則中。

- **IdP** 指導方針：
  - 設定 SAML 時，請使用以下 URL：

    **SAML Assertion Consumer Service** URL：**`https://global.acs.prismaaccess.com/saml/acs`**

    實體 **ID** URL：**`https://global.acs.prismaaccess.com/saml/metadata`**
  - 如果您使用 Okta 作為 IdP，請對 **Name ID Format**（名稱 **ID** 格式）設定使用 **EmailAddress**。
  - 輸入單一登入 URL，即 `https://global.acs.prismaaccess.com/saml/acs`。
  - 不支援單一登出 (SLO)。
  - 若要針對 IdP 驗證問題進行疑難排解，請使用 IdP 的監控和疑難排解功能。ACS 不會記錄 IdP 驗證失敗。
  - 為 SAML IdP 建立 **Authentication Profile**（驗證設定檔）時，在 **Advanced**（進階）頁籤中，於 **Allow List**（允許清單）中選取 **all**（全部），否則明確 Proxy 將無法擷取群組對應。

**STEP 2 |** 設定明確 Proxy 設定

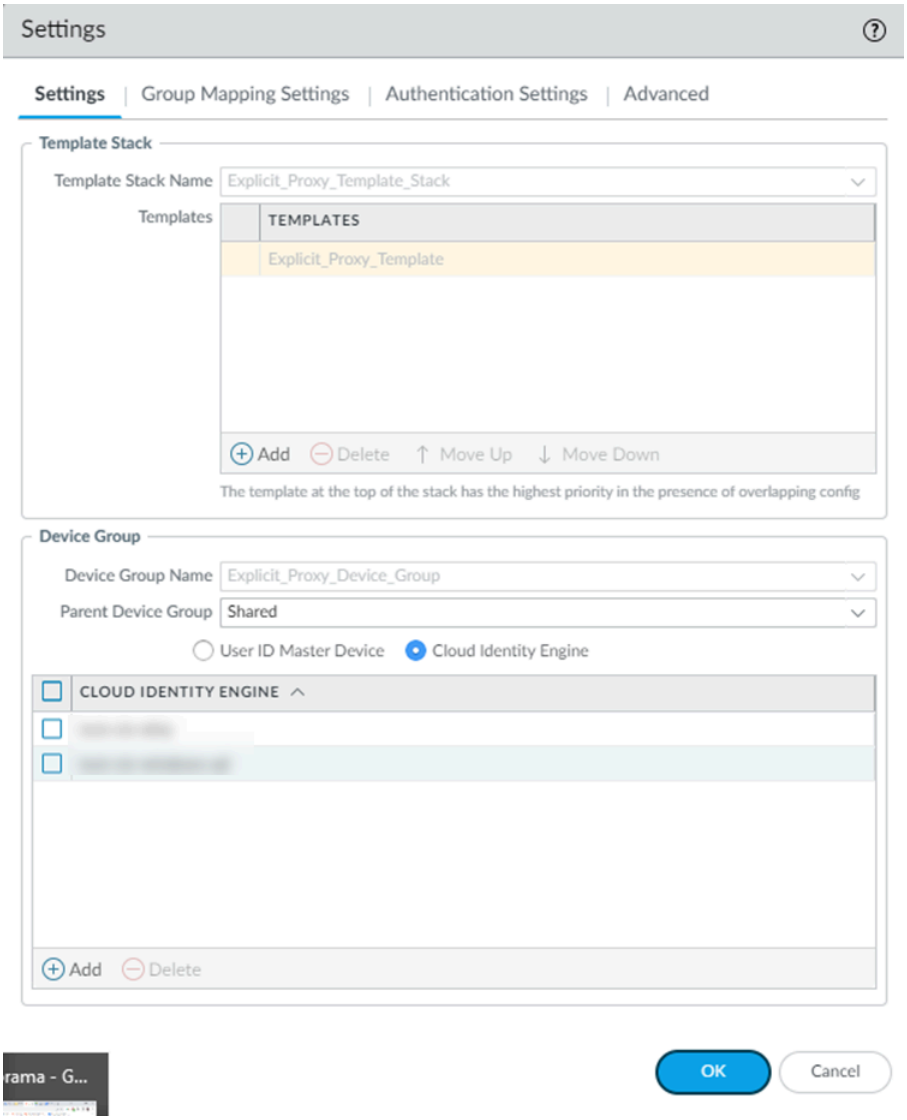
1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users—Explicit Proxy**（行動使用者—明確 **Proxy**），然後按一下齒輪圖示以編輯明確 Proxy **Settings**（設定）。
2. 在 **Settings**（設定）頁籤中，編輯以下設定：
   - （選用）驗證範本和範本堆疊名稱。

     根據預設，Prisma Access 會建立新的範本堆疊 **Explicit_Proxy_Template_Stack** 和新的範本 **Explicit_Proxy_Template**。確保在 Panorama 中建立和編輯 **Device**（裝置）設定時使用此範本。
   - 在 [Device Group（裝置群組）] 區段中，選取 **Parent Device Group**（父系裝置群組），其中包含您想要為明確 Proxy 推送的設定，或者將父系裝置群組保留為

 ©2025 Palo Alto Networks, Inc.

**Shared**（共用），以使用 Prisma Access 裝置群組共用階層。無法變更 **Device Group Name**（裝置群組名稱）。

- (選用）如果您已將新世代防火牆設定為主要裝置，或已新增雲端識別引擎設定檔，將使用者和群組資訊填入安全性政策規則中，請選取 User-ID 主要裝置或雲端識別引擎；然後，選取您建立的主要裝置或雲端識別引擎設定檔。
- 在 [License Allocation（授權配置）] 區段中，指定要為明確 Proxy 配置的行動使用者數目。

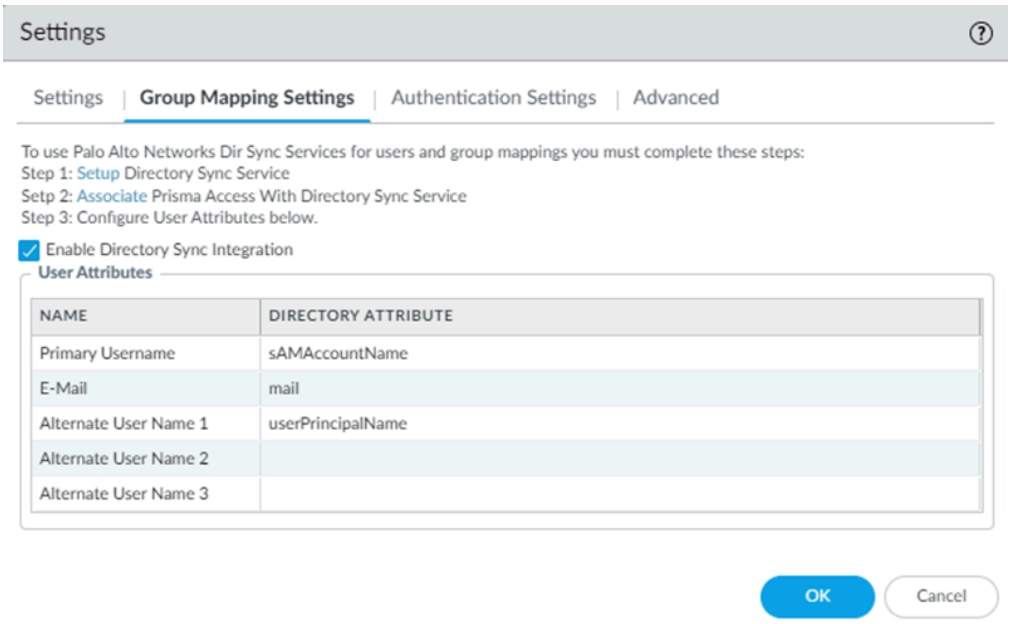



3. 在 **Group Mapping Settings**（群組對應設定）頁籤中，**Enable Directory Sync Integration**（啟用目錄同步整合）（現在稱為雲端識別引擎），以將 Prisma Access 設定為使用雲端識別引擎來擷取使用者和群組資訊。

   您使用雲端識別引擎，來填入使用者和群組對應資訊，進行明確 Proxy 部署。

   為 **Primary Username**（主要使用者名稱）欄位中的目錄屬性輸入 **mail**，以及為 **E-Mail**（電子郵件）欄位輸入 **mail**。

 ©2025 Palo Alto Networks, Inc.




4. 完成時請按一下 **OK**（確定）。

**STEP 3 |** （選用）設定 Block Settings（封鎖設定）。

使用封鎖設定，在 DNS 解析階段封鎖對網際網路目的地的存取。

若要限制僅特定的來源 *IP* 位址可存取明確 *Proxy*，您也可以使用特殊物件。這些使用特定名稱的地址物件、位址群組和外部動態清單 *(EDL)* 允許您為網際網路流量指定的 *IP* 位址，並封鎖任何其他 *IP* 位址。

**STEP 4 |** 在 **Authentication Settings**（驗證設定）頁籤中，設定解密、X-Authenticated-User (XAU) 和驗證設定。

1. 為解密的流量設定您的設定。
   - 選取 **Decrypt Traffic That Matches Existing Decryption rules; For Undecrypted Traffic, Allow Traffic Only From Known IPs Registered By Authenticated Users**（解密符合現有解密規則的流量；對於未解密的流量，僅允許來自已驗證使用者註冊的已知 **IP** 的流量），來設定以下解密規則：
     - 符合您設定的解密政策規則的流量，若其 **Action**（動作）為 **Decrypt**（解密）或 **Decrypt and Forward**（解密並轉送），將進行解密。

       如果使用者存取未解密的 HTTPS 網站，並且使用者尚未從該 IP 位址向明確 Proxy 進行驗證，則該使用者會遭到封鎖。不過，使用者可以存取造解密的網站、完成驗證，然後存取未解密的網站。
     - 允許未解密的流量來自已從中驗證行動使用者的 IP 位址。

     明確 Proxy 需要解密以驗證使用者。輸入可以在自訂 URL 類別中解密的網域；然後，在 **If Authentication traffic is forwarded through Explicit Proxy, specify the domains**

 ©2025 Palo Alto Networks, Inc.

**used in the authentication flow**（如果驗證流量透過明確 **Proxy** 轉送，請指定驗證流程中使用的網域）中指定這些類別。

僅將驗證所需的網域新增到您指定的自訂 *URL* 類別，包括所有 *ACS* 和 *IdP FQDN*。您必須將驗證 *URL* 新增到自訂 *URL* 類別，即使您已將它們新增到解密政策也一樣。

- 若要允許所有流量進行解密，請選取 **Decrypt All traffic (Overrides Existing Decryption Rules)**（解密所有流量（覆寫現有的解密規則））。

  如果您選取此選項按鈕，請確保：

  - 您在解密政策中沒有例外狀況。
  - 您在安全性政策中套用來源 IP 位址型限制。

  若無法遵循這些建議，可讓明確 *Proxy* 當作開放 *Proxy* 濫用，而此開放 *Proxy* 被廣泛誤用為轉送服務，進行拒絕服務攻擊。

  - 您至少有一個 SSL 正向 Proxy 憑證指定為 **Forward Trust Certificate**（轉送信任憑證）。

    如果您沒有轉送信任憑證，請在 Panorama 上建立一個；然後，**Commit and Push**（提交並推送）您的變更至 Prisma Access。無法具有轉送信任憑證，將導致在提交您的明確 Proxy 變更時發生提交錯誤。

2. （選用）輸入其中未解密的 HTTP 或 HTTP 跨來源資源共用 (CORS) 流量應被允許流向 **Trusted Source Address Auth Bypass**（受信任的來源位址驗證略過）的任何 IP 位址。

   將 IP 位址新增至 IP 位址型位址物件，並在欄位中 **Add**（新增）位址物件。

   最多可輸入 100,000 個位址。確保位址物件僅使用 IP 位址。

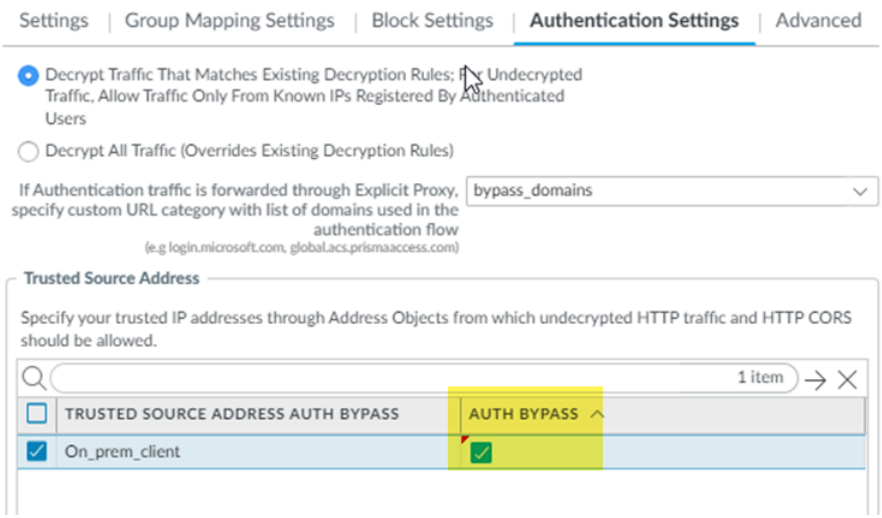
3. （選用）若要略過您輸入的任何受信任來源位址的驗證，請選取 **Auth Bypass**（驗證略過）。

   您可以使用 **Auth Bypass**（驗證略過）搭配 **Source IP based visibility and enforcement**（來源 **IP** 型可視性和強制執行），來跳過無法驗證的無頭系統的驗證、設定安全性政策，以及獲得 Prisma Access 明確 Proxy 上流量的可視性。

   您可以新增 *IP* 位址或子網路。在擴展子網路之後，最多支援 *100,000* 個 *IP* 位址。

   如果您選取 **Auth Bypass**（驗證略過），以跳過位址物件的驗證，但稍後想要為該位址物件取消選取 **Auth Bypass**（驗證略過）來啟用驗證，則在您進行變更且提交並推送您的變更之後，最多可能需要 24 小時，變更才會生效。


©2025 Palo Alto Networks, Inc.




4. （選用）若要允許受信任的來源位址 IP 位址，使用 XAU 進行識別，請選取 **Use X-Authenticated-User (XAU) header on incoming HTTP/HTTPS requests for Identity**（對傳入 **HTTP/HTTPS** 要求使用 **X-Authenticated-User (XAU)** 標頭以進行識別）。

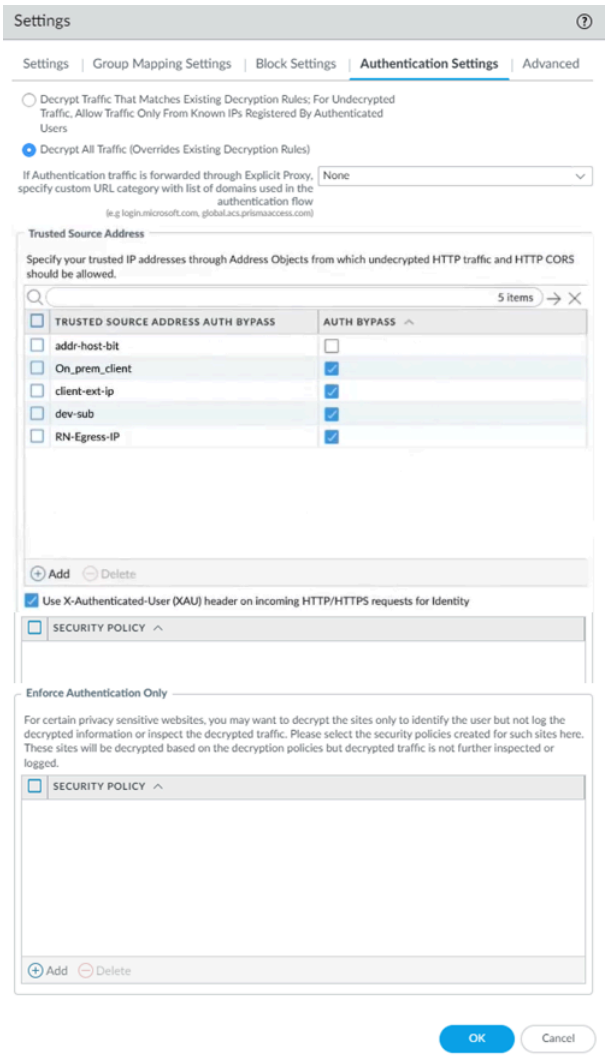
   如果您是使用從第三方 Proxy 到明確 Proxy 的 Proxy 鏈結、使用者已在該 Proxy 中進行驗證，且 Proxy 使用 XAU 標頭，請選取此選項。

   XAU 標頭是唯一支援的 HTTP 標頭，用於明確 Proxy 標頭擷取。不支援 X-Forwarded-For (XFF) 標頭。

5. （選用）為隱私敏感的網站指定設定，方法是為這些網站建立安全性政策規則，然後在 **Enforce Authentication Only**（僅強制驗證）區域中為這些網站指定一或多個 **Security Policy**（安全性政策）。

   對於您在新增的一或多個 **Security Policy**（安全性政策）指定的任何網站，明確 Proxy 根據解密政策解密這些網站，但不檢查或記錄解密的流量。


©2025 Palo Alto Networks, Inc.




**STEP 5 |** （選用）設定 **Advanced**（進階）設定。

1. 如果您想要透過安全 IPSec 通道將流量從您的分支轉送至明確 Proxy，請 **Enable Proxy Mode**（啟用 **Proxy** 模式），並擷取 Anycast IP 位址，如果您想要將明確 Proxy 與 Prisma Access 遠端網路結合使用的話。

   此解決方案會使用 Anycast 位址搭配遠端網路 IPSec 通道，以允許明確 Proxy 用於遠端網站或分支位置的中使用者和裝置。

2. （選用）若要利用分支位置中將流量轉送到明確 Proxy 的系統私人 IP 位址，請選取 **Source IP based visibility and enforcement**（來源 **IP** 型可視性和強制執行）。

   此功能具有以下需求：

   - Prisma Access 資料平面至少為 10.2.4
   - 雲端服務外掛程式至少為 4.1 的 Prisma Access (Managed by Panorama) 部署
   - 來源 IP 位址僅針對在您已設定遠端網路明確 Proxy 部署之後，來自遠端網路的 IP 位址顯示，以及僅針對明確 Proxy 支援的遠端網路位置中的來源位址顯示。

3. 僅限 Proxy 模式部署 如果在您的遠端網路上啟用了 Proxy 模式，請新增一個政策，以允許流量繫結至遠端網路上的 Anycast 和單點傳送 IP。如果您已啟用 **Source IP visibility**

 ©2025 Palo Alto Networks, Inc.

**and enforcement**（來源 **IP** 可視性和強制執行），請在明確 Proxy 中使用安全性政策中的 **Source IP**（來源 **IP**）欄位來保護流量。您需要遠端網路中的額外政策。

4. 按一下 **OK**（確定）。

**STEP 6 |** 按一下 **Configure**（設定）以設定明確 Proxy 設定。

1. 指定 **Explicit Proxy FQDN**（明確 **Proxy FQDN**）。

   根據預設，名稱為 *proxyname*.proxy.prismaaccess.com，其中 *proxyname* 是您指定的子網域，並使用連接埠 8080。如果您想要在明確 Proxy URL 中使用您組織的網域名稱（例如，thisproxy.proxy.mycompany.com），請為您組織的網域輸入 CNAME 記錄。

   例如，若要將名為 thisproxy.prismaaccess.com 的Proxy URL 對應至名為 thisproxy.proxy.mycompany.com 的 Proxy，您會將 thisproxy.proxy.prismaaccess.com 的 CNAME 新增至組織網域中的 CNAME 記錄。

2. （選用）選取 **Use GlobalProtect Agent to Authenticate**（使用 **GlobalProtect** 代理程式進行驗證），以啟用代理程式型 Proxy 功能。

   啟用此功能以在 Proxy Mode（Proxy 模式）或 Tunnel and Proxy Mode（通道和 Proxy 模式）下設定明確 Proxy。您還必須選取此核取方塊，以啟用 **Source IP based visibility and enforcement**（來源 **IP** 型可視性和強制執行）。

3. 指定 **Authentication Profile**（驗證設定檔）和 **Cookie Lifetime**（**Cookie** 存留時間）。

   - 指定您在步驟 1 中使用的 **Authentication Profile**（驗證設定檔），或新增要與 Prisma Access 搭配使用的**New**（新）驗證設定檔。

     您必須設定 SAML 驗證，包括設定 **SAML Identity Provider**（**SAML** 識別提供者）(IdP) 和 **Authentication Profile**（驗證設定檔），以使用明確 Proxy。

   - （選用）為儲存使用者驗證認證的 Cookie 指定 **Cookie Lifetime**（**Cookie** 存留時間）。

     Prisma Access 快取使用者的認證，並以 cookie 的形式存儲它們。若要變更值，請指定要使用的時間長度，以秒、分鐘、小時或天為單位。

     為了防止使用者在 *Cookie* 存留時間到期之前無法下載大型檔案，或者 *Cookie* 在使用者長時間存取單一網站時過期，*Palo Alto Networks* 建議您設定至少一天的 *Cookie* 存留時間。如果明確 *Proxy* 使用者遇到 *Cookie* 存留時間到期問題，他們可以瀏覽到其他網站，以重新向 *ACS* 進行驗證並重新整理 *ACS Cookie*。

     如果您正在下載檔案，而檔案下載所需的時間超過了 **Cookie Lifetime**（**Cookie** 存留時間），則在存留時間到期時，檔案下載就會終止。基於此原因，如果您下載需要長時間下載的大型檔案，請考慮使用更長的 **Cookie Lifetime**（**Cookie** 存留時間）。

 ©2025 Palo Alto Networks, Inc.

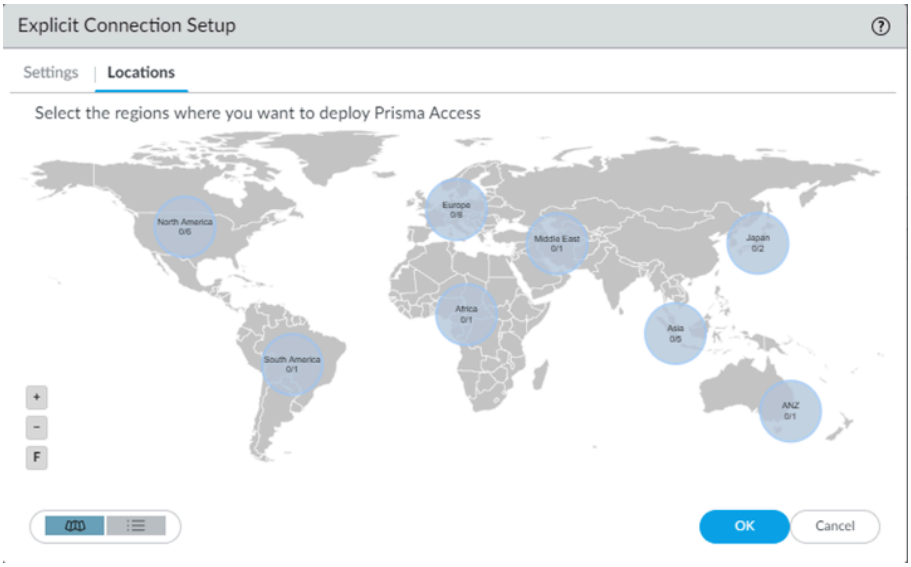
**STEP 7 |** 選取 **Locations**（位置）和區域，它們與您想要為行動使用者部署明確 Proxy 的這些位置相關聯。Prisma Access 會將 Proxy 節點新增到您選取的每個位置。

明確 Proxy 支援所有 Prisma Access 位置的子集。如需位置清單，請參閱 明確 Proxy 設定指導方針。

**Locations**（位置）頁籤顯示一張地圖。反白顯示地圖會顯示全球區域（美洲、歐洲和亞太地區）以及每個區域內可用的位置。選取一個區域，然後選取您想要在每個區域中部署的位置。

您應該在至少兩個區域啟用明確 *Proxy* 位置，以確保區域備援。

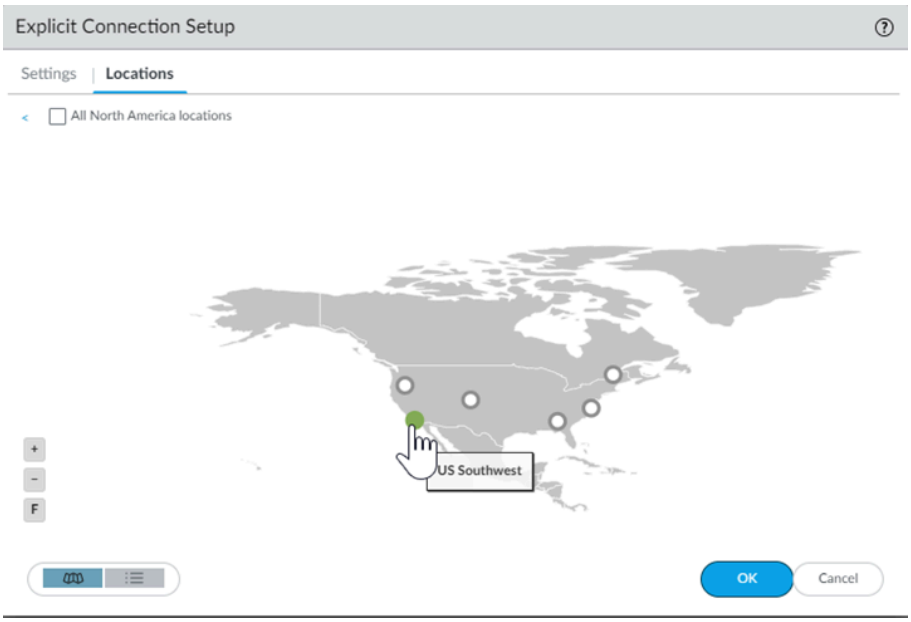
1. 按一下 **Locations**（位置）頁籤並選取一個區域。



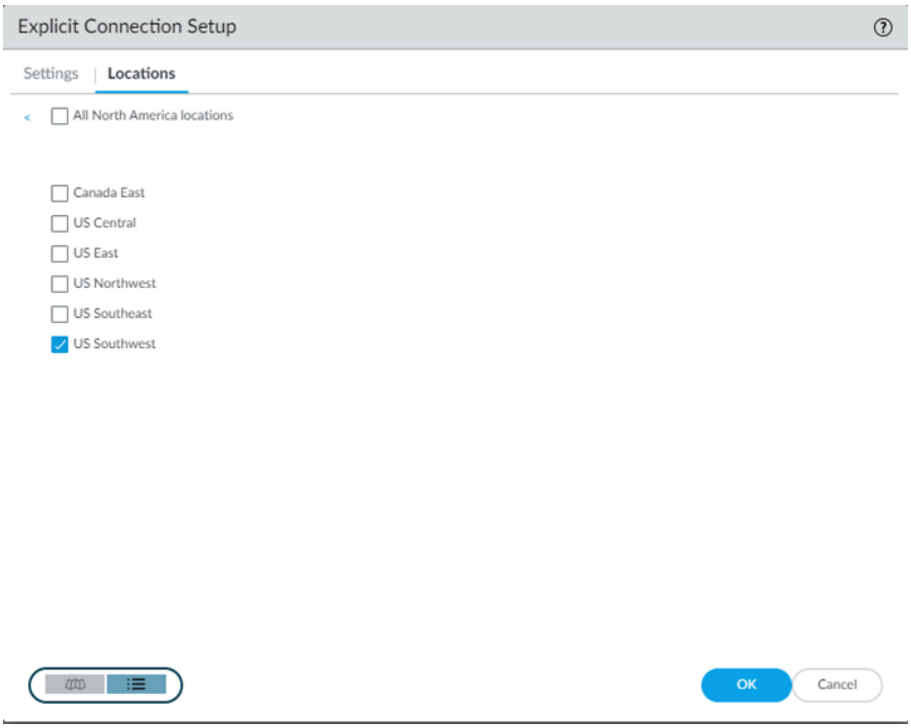

2. 使用地圖在您選取的區域內選取一或多個明確 Proxy 位置。

   將游標暫留在某個位置上，即會反白顯示該位置。白色圓圈表示可用位置；綠色圓圈表示您已選取該位置。

 ©2025 Palo Alto Networks, Inc.




除了地圖檢視外，您還可以檢視區域和位置的清單。從左下角在地圖檢視和清單檢視之間進行選擇。在清單檢視中，清單顯示依欄排序的區域，而所有位置都是依區域排序。您可以選取一個區域內的 **All**（所有）網站（對話方塊頂部）。




3. 按一下 **OK**（確定）來新增位置。


©2025 Palo Alto Networks, Inc.

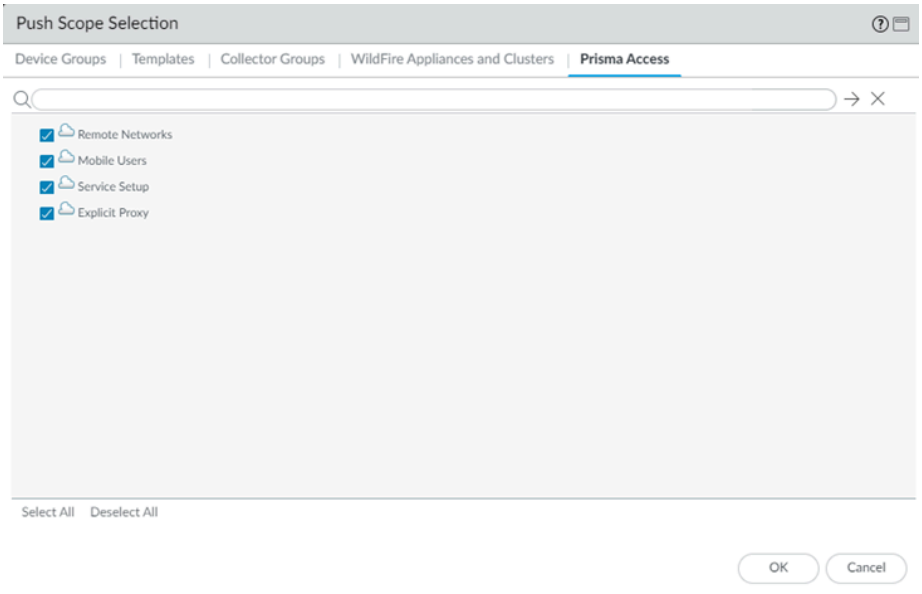
**STEP 8 |** 設定安全性政策規則以強制執行您組織的安全性政策。

若要進行必要的設定變更，並控制行動使用者可從明確 Proxy 存取的 URL，請使用安全性政策。在設定您的安全性政策時，請遵循下列指導方針和需求：

- 根據您的業務目標，為已認可的網際網路和 SaaS 應用程式建立安全性政策，方法是使用需要存取這些應用程式的 App-ID 和使用者群組。
- 將安全性設定檔附加到所有安全性政策規則，以便您可以遵循安全性設定檔最佳做法來防止已知和未知的威脅。

**STEP 9 |** 將您的變更提交到 Panorama，並將設定變更推送到 Prisma Access。

1. 按一下 **Commit**（提交） > **Commit and Push**（提交並推送）。
2. **Edit Selections**（編輯選取項目），並在 **Prisma Access** 頁籤中，確保在 **Push Scope**（推送範圍）中選取了 **Explicit Proxy**（明確 **Proxy**），然後按一下 **OK**（確定）。




3. 按一下 **Commit and Push**（提交並推送）。

 ©2025 Palo Alto Networks, Inc.

**STEP 10 |** 選取要與明確 Proxy 搭配使用的 PAC 檔案。

1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users**行動使用者） > **Explicit Proxy** （明確 **Proxy**）。

   確保在 PAC 檔案中輸入 8080 連接埠。
2. 為您剛設定的明確 Proxy 設定選取 **Connection Name**（連線名稱）。
3. 輸入要用於明確 Proxy 的 **PAC (Proxy Auto-Configuration) File**（**PAC**（**Proxy** 自動設定）檔案）。

   確保您瞭解 *PAC* 檔案的運作方式，以及如何修改它們，然後再將它們上傳至 *Prisma Access*。

   **Browse**（瀏覽） 並上傳該檔案。

   Prisma Access 為您提供一個範例 PAC 檔案；您可以 **Download sample PAC file**（下載範例 **PAC** 檔案）、修改值，然後上傳該檔案。請參閱設定您的明確 Proxy PAC 檔案，以取得 PAC 檔案需求和指導方針，以及範例 PAC 檔案內容的說明。

# 用於明確 Proxy 部署的 Kerberos 驗證

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

Prisma Access Mobile—明確 Proxy 部署支援 Kerberos 驗證。如果您有伺服器、IoT 裝置或無頭電腦無法使用 SAML 進行驗證，則可以改用 Kerberos 驗證。

如果您的部署同時使用 SAML 和 Kerberos 進行驗證，您可以在單一明確 Proxy 部署中設定這兩種驗證類型。透過這種方式，您可以使用 SAML 驗證行動使用者，同時使用 Kerberos 驗證伺服器、IoT 裝置或無頭電腦。Prisma Access 明確 Proxy 會處理驗證，取決於用於驗證流量的連接埠：

- 如果驗證流量使用連接埠 8080，則明確 Proxy 會使用 SAML 驗證。
- 如果驗證流量使用連接埠 8081，則明確 Proxy 會使用 Kerberos 驗證。

如果只設定一個連接埠，則未設定的連接埠會使用與所設定連接埠相同的驗證設定檔。

*Kerberos SSO* 僅適用於有權存取 *Kerberos* 基礎結構的端點和系統。無權存取 *Kerberos* 基礎結構的端點和系統必須使用 *SAML SSO*。

- 部署 Kerberos 進行明確 Proxy 部署的需求和建議
- 建立 Kerberos 金鑰標籤

 ©2025 Palo Alto Networks, Inc.

- 設定 Kerberos 驗證進行明確 Proxy 部署

## 部署 Kerberos 進行明確 Proxy 部署的需求和建議

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 授權<br>❑ 所需的最低資料平面版本：PAN-OS 10.1.3 或更新版本 |

在您建立 Kerberos 金鑰標籤，以在明確 Proxy 部署中實作 Kerberos 之前，請確保您的 Kerberos 部署具有以下需求和先決條件：

- 將您的資料平面更新至 PAN-OS 10.1.3 或更新版本。
- 確保您具有一個 Kerberos 帳戶，可供 Prisma Access 用來驗證伺服器或裝置。

  需要一個帳戶才能建立 Kerberos 金鑰標籤，此金鑰標籤是一種檔案，其中包含主體名稱與加密的 Kerberos 密碼。
- 確保伺服器和端點已加入網域，這樣使用者和電腦就可以使用其工作網路認證安全地連線到其工作網域。
- 確保您在行動使用者的 PAC 檔案中或在端點或伺服器上的 Proxy 設定中，將 Kerberos 驗證流量轉送到連接埠 8081。

  明確 Proxy 使用連接埠 8081 進行 Kerberos 驗證，以及使用連接埠 8080 進行 SAML 驗證。
- 確保您的 Kerberos 管理員有能力建立和匯出金鑰標籤。
- 確保您具有伺服器、IoT 裝置或無頭電腦所在分支或校園位置的輸出 IP 位址。

  您將這些 IP 位址新增到明確 Proxy 信任的位址清單。

 ©2025 Palo Alto Networks, Inc.

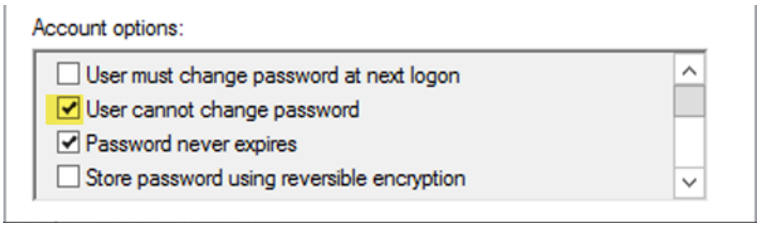
- 遵循 Kerberos 使用者驗證和建立的最佳做法。

  遵循最佳做法以保護其 Kerberos 環境，並防止密碼外洩，這是 Kerberos 帳戶管理員的責任。在建立使用者帳戶、密碼和服務主體名稱（SPN）時，請遵循以下最佳做法。

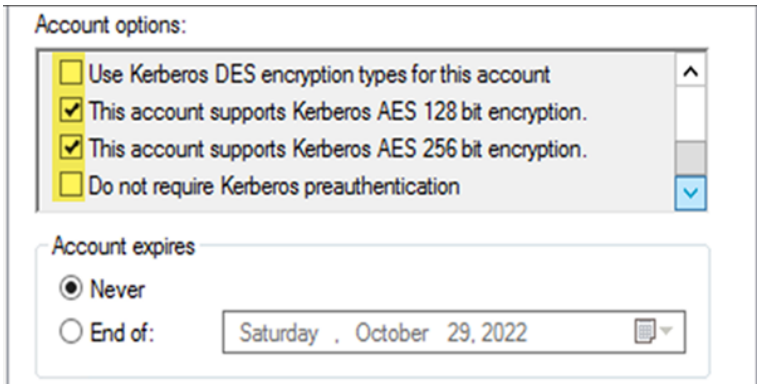
  **Kerberos** 使用者帳戶建立最佳做法：

  - 請勿重複使用管理員使用者帳戶。

    為要與 Prisma Access 明確 Proxy 搭配使用的 Kerberos 帳戶建立唯一的帳戶名稱。
  - 請勿與任何其他服務共用此帳戶；請為 Prisma Access 明確 Proxy 使用專用的使用者帳戶。
  - 確保使用者無法變更 Kerberos 帳戶的密碼。

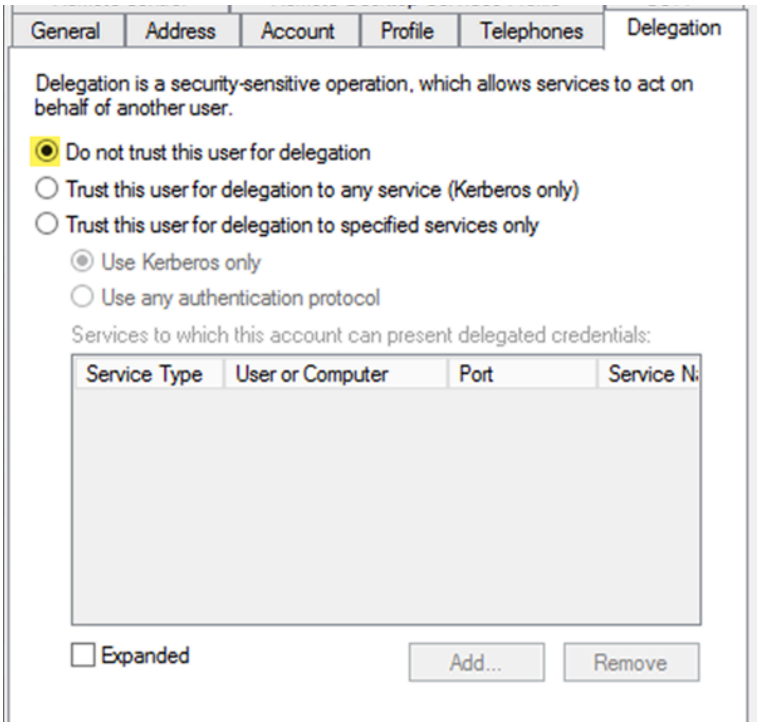
    
    

  - 在選取 Kerberos 帳戶選項時，請取消選取 **Use Kerberos DES encryption types for this account**（為此帳戶使用 **Kerberos DES** 加密類型）和 **Do not require Kerberos preauthentication**（不需要 **Kerberos** 預先驗證）。
  - 啟用 AES-128 和 AES-256 位元加密。

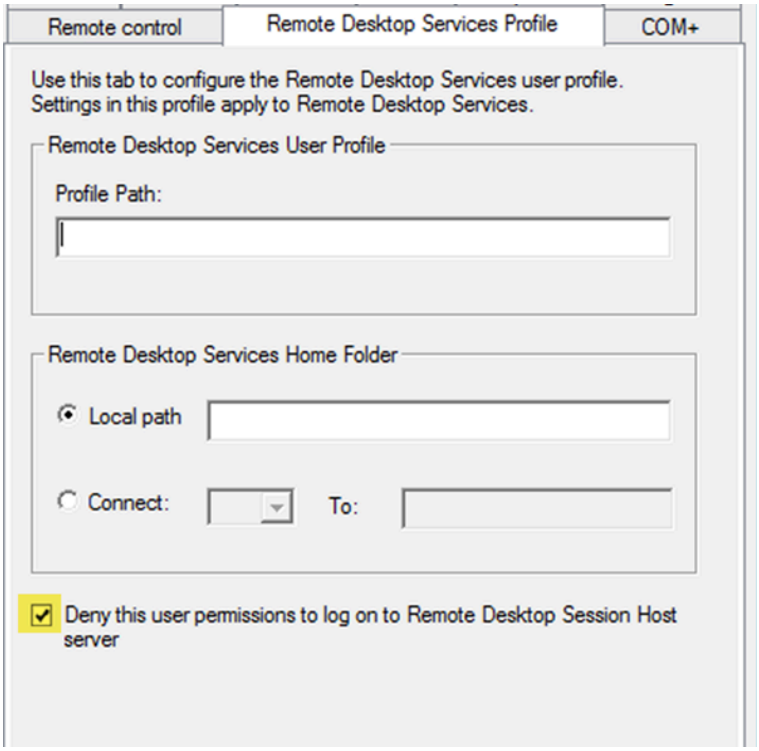
    
    

  - 停用使用者的委派。

 ©2025 Palo Alto Networks, Inc.

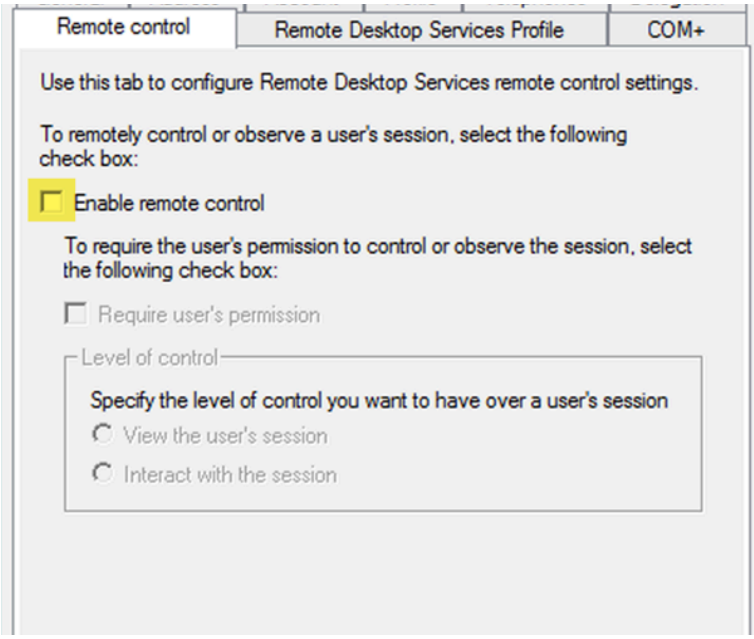



- 拒絕登入遠端桌面工作階段的能力。

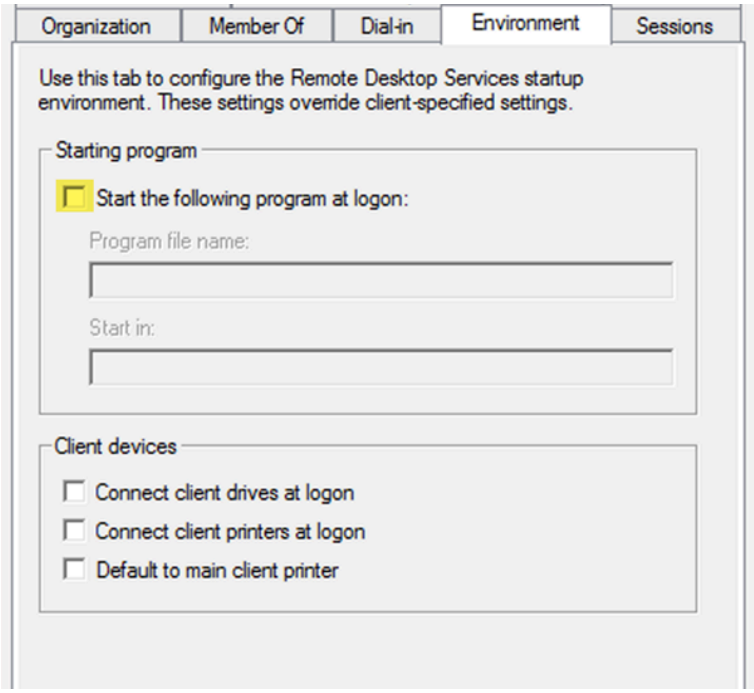



- 請勿啟用遠端控制。

 ©2025 Palo Alto Networks, Inc.




- 不允許使用者在登入時啟動程式。




- 您可以在所建立驗證設定檔的允許清單中指定使用者或使用者群組，以限制驗證僅限於具有合法業務需求的使用者或機器。

**SPN** 和 **Keytab** 最佳做法：

- 確保 SPN 不與多個用戶帳戶相關聯，這可能會導致重複的 SPN 失敗。
- RC4-HMAC-NT 使用弱式 NTML 雜湊。遵循您組織的安全性政策和指導方針，以包含或排除 RC5 密碼。
- DES-CBC-CRC 和 DES-CBC-MD5 密碼已被棄用，而且不受 Prisma Access 支援。

 ©2025 Palo Alto Networks, Inc.

- 定期輪換 SPN 的密碼。遵循您組織的安全性政策和指導方針，進行密碼輪換。
- 遵循您組織的密碼複雜性做法（例如，以真正隨機的方式建立 SPN 密碼，使其無法被人類讀取和猜測）。
- 如果您變更服務使用者的密碼，或變更任何其他屬性，請更新並重新產生新的金鑰標籤，並將其上傳至 Prisma Access。
- 如果裝載新的 PA 區域，您必須為該區域產生新的金鑰標籤，如以下步驟所示。

以下範例輸出顯示了使用 Kerberos 最佳做法所建立的帳戶。

```
PS C:\Users\Administrator> Get-ADUser example -Properties "*"
 AccountNotDelegated :True AllowReversiblePasswordEncryption :False
 CannotChangePassword :True CN : example
 Deleted :DoesNotRequirePreAuth :False Enabled :True
 GivenName :PrismaAccess EP Service User KerberosEncryptionType :
 {AES128, AES256} msDS-SupportedEncryptionTypes :24 Name :
 example PasswordExpired :False PasswordNeverExpires :True
 PasswordNotRequired :False PrincipalsAllowedToDelegateToAccount :
 {} ProtectedFromAccidentalDeletion :True SamAccountName :
 example servicePrincipalName : {HTTP/us-west-2.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM, HTTP/us-east-2.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM, HTTP/us-south-1.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM} ServicePrincipalNames :
 {HTTP/us-west-2.prisma-abcde12345.proxy.prismaaccess.com@EXMP.COM,
 HTTP/us-east-2.prisma-abcde12345.proxy.prismaaccess.com@EXMP.COM,
 HTTP/us-south-1.prisma-abcde12345.proxy.prismaaccess.com@EXMP.COM}
 SmartcardLogonRequired :False TrustedForDelegation :False
 TrustedToAuthForDelegation :False UseDESKeyOnly :False
 UserPrincipalName :HTTP/us-south-1.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM
```

## 建立 Kerberos 金鑰標籤

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 授權<br>❑ 所需的最低資料平面版本：PAN-OS 10.1.3 或更新版本 |

在檢閱為明確 Proxy 部署 Kerberos 的需求和建議之後，您已準備好建立 Kerberos 金鑰標籤。

如需最佳效能，金鑰標籤檔案的大小應小於 *60 KB*。

**STEP 1 |** 設定您的 明確 Proxy 部署。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 取得設定 Kerberos 驗證所需的 FQDN、Proxy FQDN 和 DNS CNAME。

Kerberos 驗證會使用從 Prisma Access API 指令碼取得的資訊 以建立並設定 Kerberos 金鑰標籤。API 指令碼會擷取以下資訊：

- **ep_geo_lb_fqdn**—明確 Proxy 網路負載平衡器設定中使用的明確 Proxy DNS FQDN。此 FQDN 與明確 Proxy 的 **Explicit Proxy URL**（明確 **Proxy URL**）相同，此 URL 位於 Prisma Access UI 的 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Explicit Proxy**（明確 **Proxy**） > **Infrastructure Settings**（基礎結構設定） > **Explicit Proxy URL**（明確 **Proxy URL**）下。
- **ep_geo_lb_cname**—明確 Proxy 租用戶的 DNS CNAME。
- **ep_regional_fqdn**—用於所裝載明確 Proxy 位置的 FQDN。

  明確 Proxy 給與每個位置網路負載平衡器的公用 IP 位址；ep_regional_fqdn 是與該 IP 位址相關聯的 FQDN。如果多個位置共用相同的公用 IP 位址，則這些位置使用相同的區域 FQDN。

1. 產生 API 金鑰以用作 curl 命令的一部分。
   - 在 Prisma Access (Managed by Strata Cloud Manager) 中，選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Prisma Access** > **Infrastructure Settings**（基礎結構設定） > **Generate New API Key**（產生新的 **API** 金鑰）。
   - 在 Panorama Managed Prisma Access 上，選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定） > **Generate API Key**（產生 **API** 金鑰）
2. 建立一個 .txt 檔案，並在該檔案中輸入以下命令選項：

   ```
   { "serviceType": "swg_proxy", "location": "deployed",
    "addrType": "network_load_balancer" }
   ```

3. 輸入以下命令，擷取所需的 FQDN 以使用 Kerberos 驗證：

   ```
   curl -X POST --data @option.txt -H header-api-key:Current-
   API-Key "https://api.prod.datapath.prismaaccess.com/
   getPrismaAccessIP/v2"
   ```

   其中 `option.txt` 是您在上一個步驟中建立的 .txt 檔案，`Current-API-Key` 是 Prisma Access API 金鑰。
4. 記下 FQDN。

   每個裝載位置至少有 1 個 **ep_geo_lb_fqdn**、1 個 **ep_geo_lb_cname** 和 1 個 **ep_regional_fqdn**。

**STEP 3 |** 輸入以下命令，為您組織 Active Directory (AD) 中的 Prisma Access 明確 Proxy 服務建立新的使用者：

```
New-ADUser -Name "USER_NAME" -GivenName "USER_GIVEN_NAME"
 -SamAccountName "USER_SAMACCOUNTNAME" -UserPrincipalName
 "USER_NAME@DNS_DOMAIN_NAME" -Path "X_500_PATH" –AccountPassword
```

 ©2025 Palo Alto Networks, Inc.

```
(ConvertTo-SecureString “PASSWORD” -AsPlainText -force) -Enabled
$true -KerberosEncryptionType RC4,AES128,AES256
```

其中：

- *USER_NAME* 是使用者物件的名稱。
- *USER_GIVEN_NAME* 是使用者的名字。
- *USER_SAMACCOUNTNAME* 是使用者的安全性帳戶管理員 (SAM) 名稱。
- *USER_NAME@DNS_DOMAIN_NAME* 是使用者的使用者主體名稱 (UPN)。
- *X_500_PATH* 是在其中建立新物件的 OU 或容器的 X.500 路徑（例如，`DC=EXAMPLE,DC=COM`。）
- *PASSWORD* 是要用於帳戶的密碼。

以下 CLI 範例的使用者名稱為 `example`、SAM 名稱為 `example`、名字為 `PrismaAccess EP Service User`、UPN 為 `example@exmp.com`、路徑為 `DC=EXMP,DC=COM`、密碼為 Ex@mple123：

```
New-ADUser -Name "example" -GivenName "PrismaAccess EP
 Service User" -SamAccountName "example" -UserPrincipalName
 "example@exmp.com" -Path "DC=EXMP,DC=COM" –AccountPassword
 (ConvertTo-SecureString “Ex@mple123” -AsPlainText -force) -Enabled
 $true -KerberosEncryptionType RC4,AES128,AES256
```

上一個命令指定了 *RC4* 加密類型，其使用弱式 *NTLM* 雜湊。請遵循您組織的安全性政策和指導方針，在此命令中包含或排除 *RC4*。

**STEP 4 |** 輸入以下命令以防止密碼過期並防止密碼遭到變更：

```
Get-ADUser USER_NAME|Set-ADUser -PasswordNeverExpires:$True -
CannotChangePassword:$true
```

請遵循您組織的安全性政策，以及密碼到期和輪換政策的指導方針。

**STEP 5 |** 輸入以下命令以顯示新建立的使用者帳戶：

```
Get-ADUser USER_NAME -property msDS-KeyVersionNumber
```

**STEP 6 |** 關聯 SPN 並匯出金鑰標籤檔案，以與 Windows AD 中的 Kerberos 驗證搭配使用。

金鑰標籤檔案允許明確 Proxy 驗證流量來自使用者、伺服器、IoT 裝置或其他無頭電腦期間所提供的 Kerberos 驗證權杖。在建立金鑰標籤檔案期間，明確 Proxy 要求您在先前步驟中使用

 ©2025 Palo Alto Networks, Inc.

API 擷取的值作為 ServicePrincipalNames (SPN) 與您在該步驟之後步驟中建立的使用者帳戶相關聯。

使用 **ep_geo_lb_fqdn**、**ep_geo_lb_cname** 和 **ep_regional_fqdn** 值。這些值允許明確 Proxy 對流向其中任一 Proxy 網域的流量進行驗證。

1. 輸入以下指令，使用 **ep_geo_lb_fqdn** 值作為服務主體名稱 (SPN) 產生並匯出金鑰標籤：

   ```
   ktpass -princ HTTP/ep_geo_lb_fqdn@REALM -
   mapuser DOMAIN\USER_NAME -ptype KRB5_NT_PRINCIPAL -crypto all
    -pass PASSWORD -out KEYTAB_NAME_1.keytab
   ```

   其中：

   - *ep_geo_lb_fqdn* 是從明確 Proxy API 指令碼傳回的 **ep_geo_lb_fqdn** 值。
   - *REALM* 是領域（例如，`EXMP.COM`）。

     在大多數情況下，您使用大寫字母輸入領域。
   - *DOMAIN\USER_NAME* 是網域層級登入名稱（例如，`EXMP\example`）。
   - *PASSWORD* 是用於金鑰標籤的密碼。此密碼不必與使用者密碼相符，但必須與您在後續步驟中為 **ep_geo_lb_cname** 和 **ep_regional_fqdn** SPN 建立的值相符。
   - *KEYTAB_NAME_1* 是金鑰標籤的名稱。金鑰標籤名稱對於此 SPN 必須是唯一的。

   請務必遵循建立 *SPN* 和密碼的最佳做法。

   以下 CLI 範例的 *ep_geo_lb_fqdn* 為 `example.proxy.prismaaccess.com`、*REALM* 為 `EXMP.COM`、*DOMAIN\USER_NAME* 為 `EXMP\example`、*PASSWORD* 為 `Ex@mple123`，而匯出的金鑰標籤名稱為 `exmp1.keytab`：

   ```
   ktpass -princ HTTP/example.proxy.prismaaccess.com@EXMP.COM -
   mapuser EXMP\example -ptype KRB5_NT_PRINCIPAL -crypto all -
   pass Ex@mple123 -out exmp1.keytab
   ```

2. 輸入以下命令，使用 **ep_geo_lb_cname** 值作為 SPN 產生並匯出金鑰標籤：

   ```
   ktpass -princ HTTP/ep_geo_lb_cname@REALM -
   mapuser DOMAIN\USER_NAME -ptype KRB5_NT_PRINCIPAL -crypto all
    -pass PASSWORD -out KEYTAB_NAME_2.keytab
   ```

   其中：

   - *ep_geo_lb_cname* 是從明確 Proxy API 指令碼傳回的 **ep_geo_lb_cname** 值。
   - *REALM* 是領域，例如，`EXMP.COM`
   - *DOMAIN\USER_NAME* 是網域層級登入名稱（例如，`EXMP\example`）。
   - *PASSWORD* 是用於金鑰標籤的密碼。此密碼必須與 **ep_geo_lb_fqdn** 和 **ep_regional_fqdn** SPN 密碼相符。


©2025 Palo Alto Networks, Inc.

- *KEYTAB_NAME_2* 是您要匯出的金鑰標籤名稱。此名稱應與您建立的其他 SPN 金鑰標籤名稱不同。

以下 CLI 範例的 *ep_geo_lb_cname* 為 `abcde12345.proxy.prismaaccess.com`、*REALM* 為 `EXMP.COM`、*DOMAIN\USER_NAME* 為 `EXMP\example`、*PASSWORD* 為 `Ex@mple123`，而匯出的金鑰標籤名稱為 `exmp2.keytab`：

```
ktpass -princ HTTP/prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM -mapuser EXMP
\example -ptype KRB5_NT_PRINCIPAL -crypto all -pass Ex@mple123
 -out exmp2.keytab
```

3. 輸入以下命令，使用 **ep_regional_fqdn** 值作為 SPN 產生並匯出金鑰標籤：

```
ktpass -princ HTTP/ep_regional_fqdn@REALM -
mapuser DOMAIN\USER_NAME -ptype KRB5_NT_PRINCIPAL -crypto all
 -pass PASSWORD -out KEYTAB_NAME_3.keytab
```

其中：

- *ep_regional_fqdn* 是從明確 Proxy API 指令碼傳回的 **ep_regional_fqdn** 值。
- *REALM* 是領域（例如，`EXMP.COM`）。
- *DOMAIN\USER_NAME* 是網域層級登入名稱（例如，`EXMP\example`）。
- *PASSWORD* 是用於金鑰標籤的密碼。此密碼必須與 **ep_geo_lb_fqdn** 和 **ep_geo_lb_cname** SPN 密碼相符。
- *KEYTAB_NAME_3* 是您要匯出的金鑰標籤名稱。此名稱應與您建立的其他 SPN 金鑰標籤名稱不同。

以下 CLI 範例的 *ep_regional_fqdn* 為 `us-west-2.prisma-abcde12345.proxy.prismaaccess.com`、*REALM* 為 `EXMP.COM`、*DOMAIN\USER_NAME* 為 `EXMP\example`、*PASSWORD* 為 `Ex@mple123`，而匯出的金鑰標籤名稱為 `exmp3.keytab`：

```
ktpass -princ HTTP/us-west-2.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM -mapuser EXMP
\example -ptype KRB5_NT_PRINCIPAL -crypto all -pass Ex@mple123
 -out exmp3.keytab
```

4. （選用）如果您有其他位置使用不同的 **ep_regional_fqdn** 值，並且想要為這些位置建立金鑰標籤，請重複步驟 6.c，為這些位置使用 **ep_regional_fqdn** 值，以產生並匯出一個或多個額外的金鑰標籤。

為每個唯一的 **ep_regional_fqdn** 建立唯一的金鑰標籤名稱。例如，如果另一個位置的 **ep_regional_fqdn** 是 `us-east-2.prisma-`


©2025 Palo Alto Networks, Inc.

abcde12345.proxy.prismaaccess.com，請使用唯一的匯出金鑰標籤檔案名稱輸入以下範例 CLI：

```
ktpass -princ HTTP/us-east-2.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM -mapuser EXMP
\example -ptype KRB5_NT_PRINCIPAL -crypto all -pass Ex@mple123
 -out exmp4.keytab
```

**STEP 7 |** 在 Ubuntu 中輸入以下 `ktutil` 指令，來刪除所建立金鑰標籤中不受支援的密碼。

以下系統輸出提供了清除各種密碼的範例：

```
slot KVNO Principal ---- ----
 ---------------------------------------------------------------------
 1 3 HTTP/us-west-2.prisma-
abcde12345.proxy.prismaaccess.com@PANW.COM (des-cbc-crc) 2 3
 HTTP/us-west-2.prisma-abcde12345.proxy.prismaaccess.com@PANW.COM
 (des-cbc-md5) 3 3 HTTP/us-west-2.prisma-
abcde12345.proxy.prismaaccess.com@PANW.COM (arcfour-hmac) 4 3
 HTTP/us-west-2.prisma-abcde12345.proxy.prismaaccess.com@PANW.COM
 (aes256-cts-hmac-sha1-96) 5 3 HTTP/us-west-2.prisma-
abcde12345.proxy.prismaaccess.com@PANW.COM (aes128-cts-hmac-
sha1-96)
```

```
# display all keytabs, get the key entry numbers to remove DES-
CBC-MD5 and DES-CBC-CRC. # Also, enable or disable RC4-HMAC based
 on your organization's policy. for i in `ls keytab_name*.keytab`;
 do echo $i; klist -Kte -k $i; done # cleanup unsupported
 ciphers # entry #1 is typically des-cbc-crc # entry #2 is
 typically des-cbc-md5 # entry #3 is typically arcfour-hmac ktutil
 rkt KEYTAB_NAME_1.keytab delent 2 delent 1 wkt new1.keytab quit
 ktutil rkt KEYTAB_NAME_2.keytab delent 2 delent 1 wkt new2.keytab
 quit ktutil rkt KEYTAB_NAME_3.keytab delent 2 delent 1 wkt
 new3.keytab quit
```

Where *KEYTAB_NAME_1*.keytab, *KEYTAB_NAME_2*.keytab, and *KEYTAB_NAME_3*.keytab 是您在上一個步驟建立的金鑰標籤。

**STEP 8 |** （選用）如果您為其他區域建立了更多金鑰標籤，請移除這些金鑰標籤上不受支援的密碼，方法是輸入先前的 `ktutil` 命令，將 *KEYTAB_NAME_1*.keytab 取代為您用於一個或多個區域的金鑰標籤名稱，並指定不同的輸出檔案（例如，`new4.keytab`、`new5.keytab` 等）。


©2025 Palo Alto Networks, Inc.

**STEP 9 |** 輸入以下 `ktutil` 命令合併您建立的金鑰標籤，其中 new1.keytab、new2.keytab 和 new3.keytab 是您在上一個步驟中建立的金鑰標籤。請務必在此命令中包含所有區域特定的金鑰標籤。

```
ktutil rkt new1.keytab rkt new2.keytab rkt new3.keytab # if you
 created any additional region-specific keytab files, add them
 here. wkt papxv1.keytab quit
```

完成時，您可以使用您建立的金鑰標籤（本範例中的 `papxv1.keytab`）作為要與明確 Proxy 搭配使用的金鑰標籤。

## 設定 Kerberos 驗證進行明確 Proxy 部署

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

- Strata Cloud Manager
- Panorama

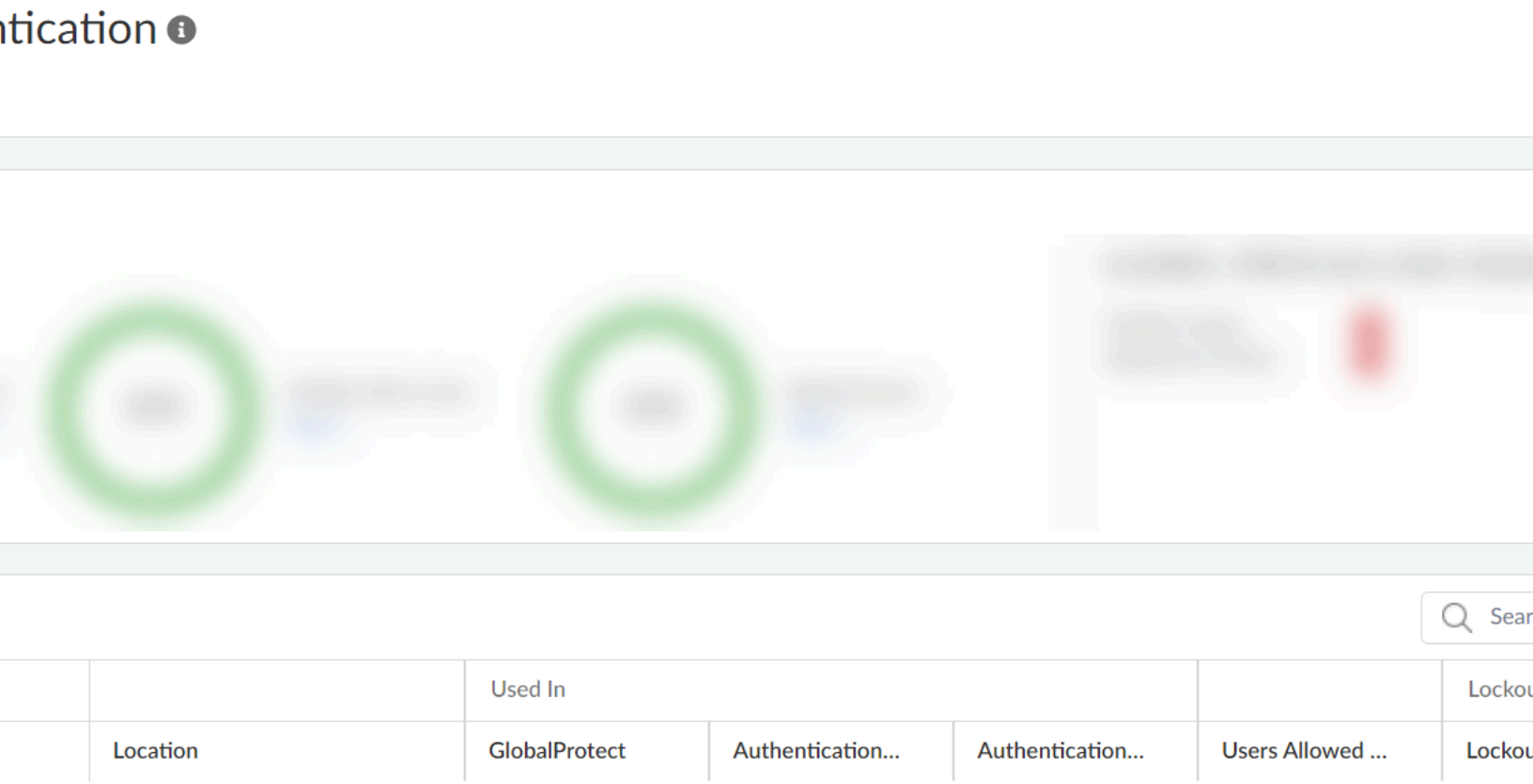
 ©2025 Palo Alto Networks, Inc.

### 設定 Kerberos 驗證進行明確 Proxy 部署 (Strata Cloud Manager)

**STEP 1 |** 設定 Kerberos 驗證設定檔。

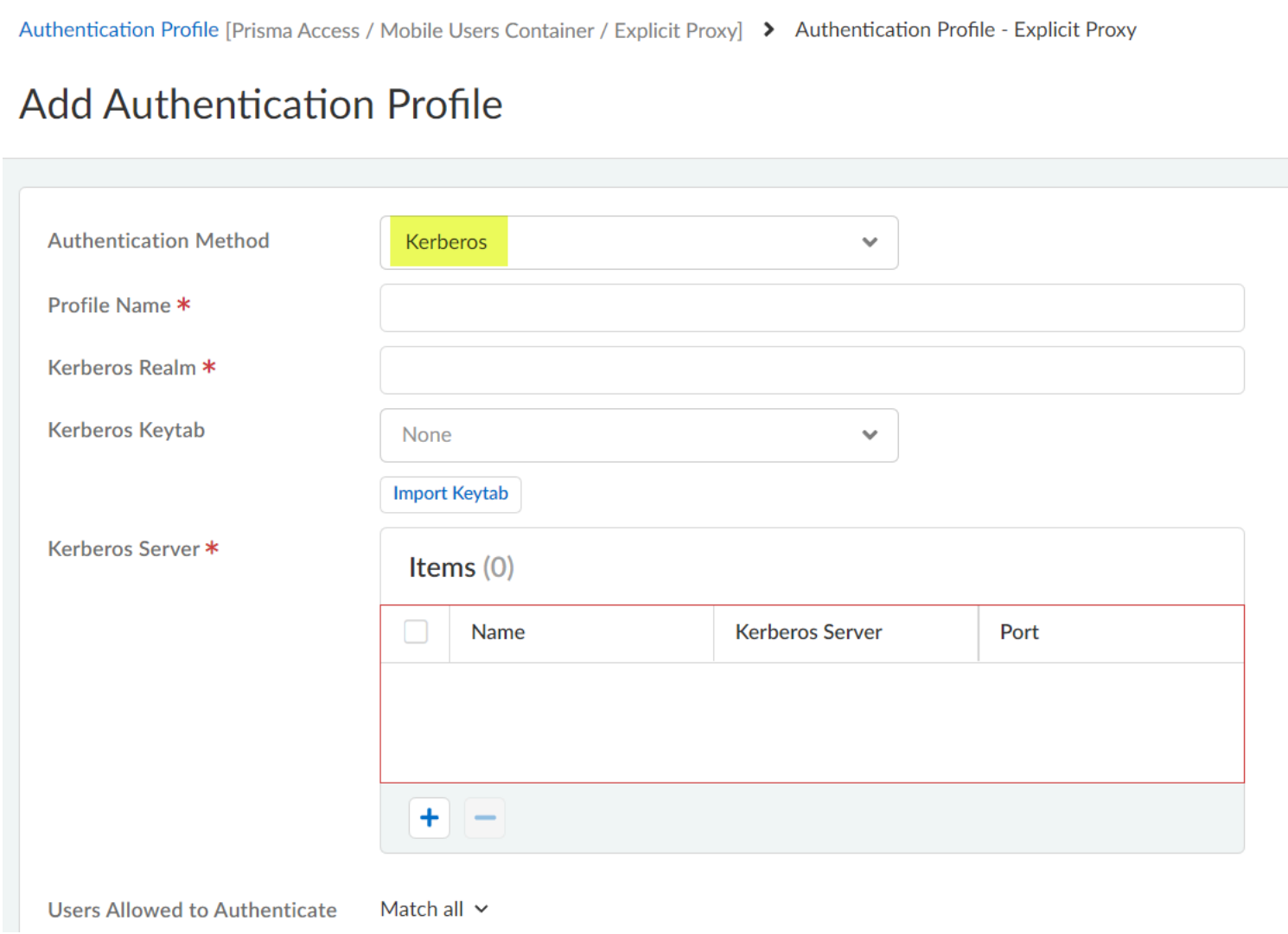
此設定檔定義明確 Proxy 程式如何連線到 Kerberos 伺服器，進行行動使用者驗證。

1. 前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Identity Services**（識別服務） > **Authentication**（驗證） > **Authentication Profiles**（驗證設定檔）和 **Add Profile**（新增設定檔）。




2. 選取 **Authentication Method**（驗證方法）：**Kerberos**。

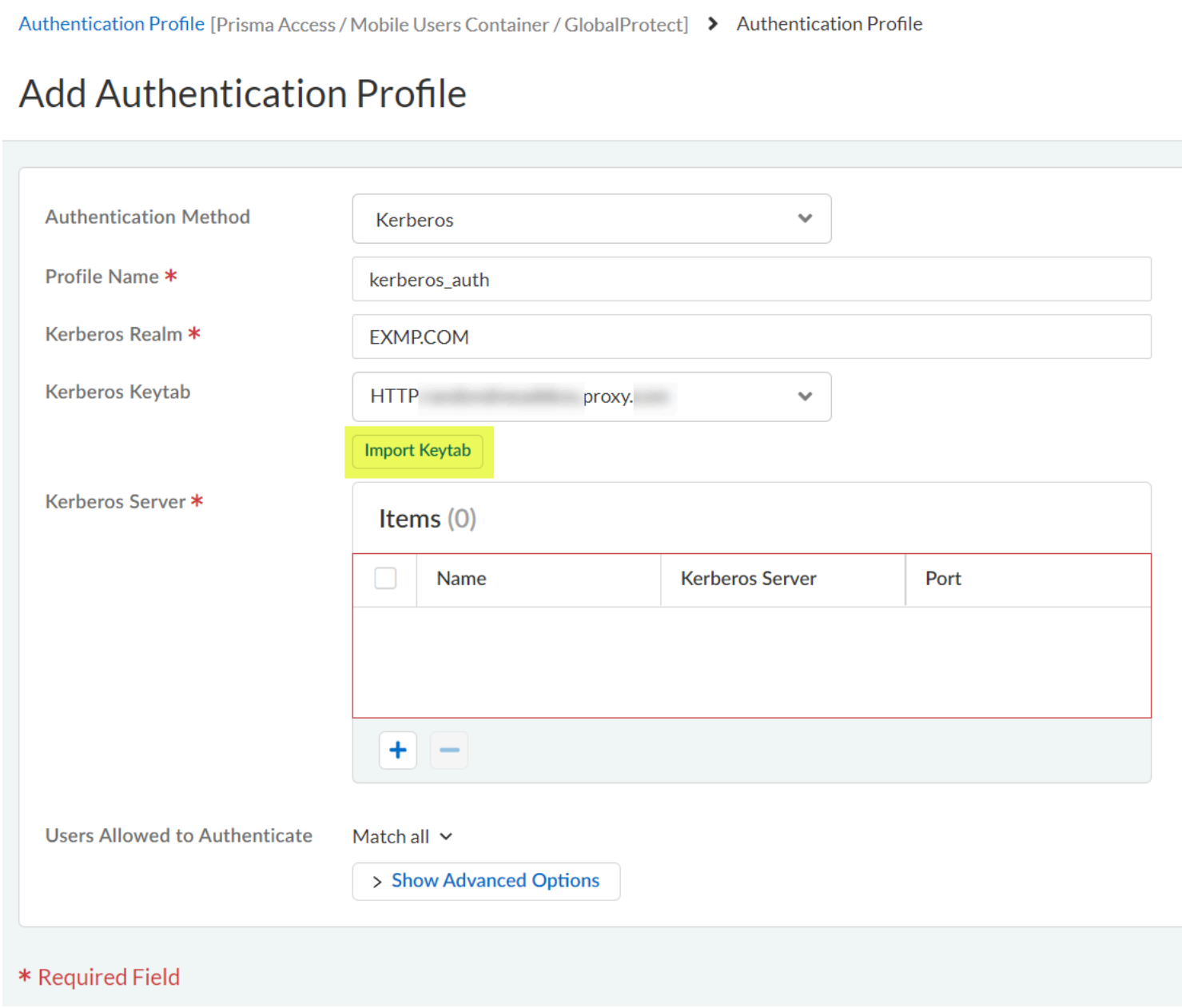
 ©2025 Palo Alto Networks, Inc.




3. 輸入用來識別伺服器設定檔的 **Profile Name**（設定檔名稱）。

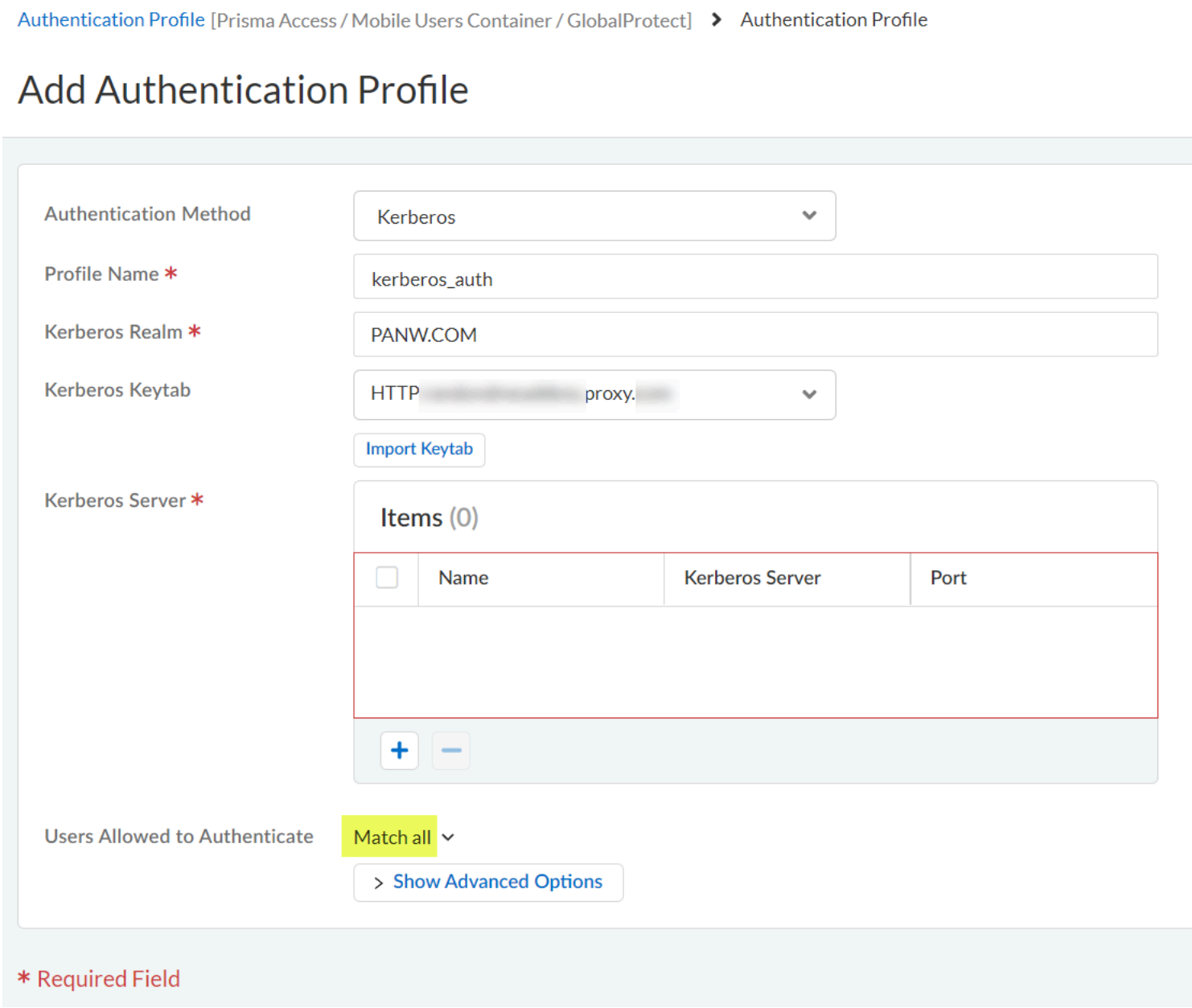
   驗證設定檔指定入口網站或閘道在驗證使用者時使用的伺服器設定檔。
4. 輸入 **Kerberos Realm**（**Kerberos** 領域）（最多 127 個字元）以指定使用者登入名稱的主機名稱部分。例如，使用者帳戶名稱 user@EXMP.COM 具有領域 EXMP.COM。
5. 匯入您先前建立的 **Kerberos Keytab**（**Kerberos** 金鑰標籤）（**Import Keytab**（匯入金鑰標籤））。

 ©2025 Palo Alto Networks, Inc.




6. 使用此設定檔新增 **Users Allowed to Authenticate**（允許進行驗證的使用者）。
   - 若要選取所有使用者，請 **Match all**（比對全部）。
   - 如果您是使用雲端識別引擎填入使用者清單，請從清單中選擇使用者，或選取 **all**（全部）以允許所有使用者進行驗證。
   - 若要新增可以使用 Kerberos 登入的本機使用者，請 **Add Local User**（新增本機使用者）、新增 **Name**（名稱）並建立 **Password**（密碼）。
     - 設定使用者驗證和使用者對應時，請使用 userPrincipalName (UPN) 的格式；不支援其他格式（例如 samAccountName）。
     - 不支援 Unicode 字元使用者名稱。


©2025 Palo Alto Networks, Inc.

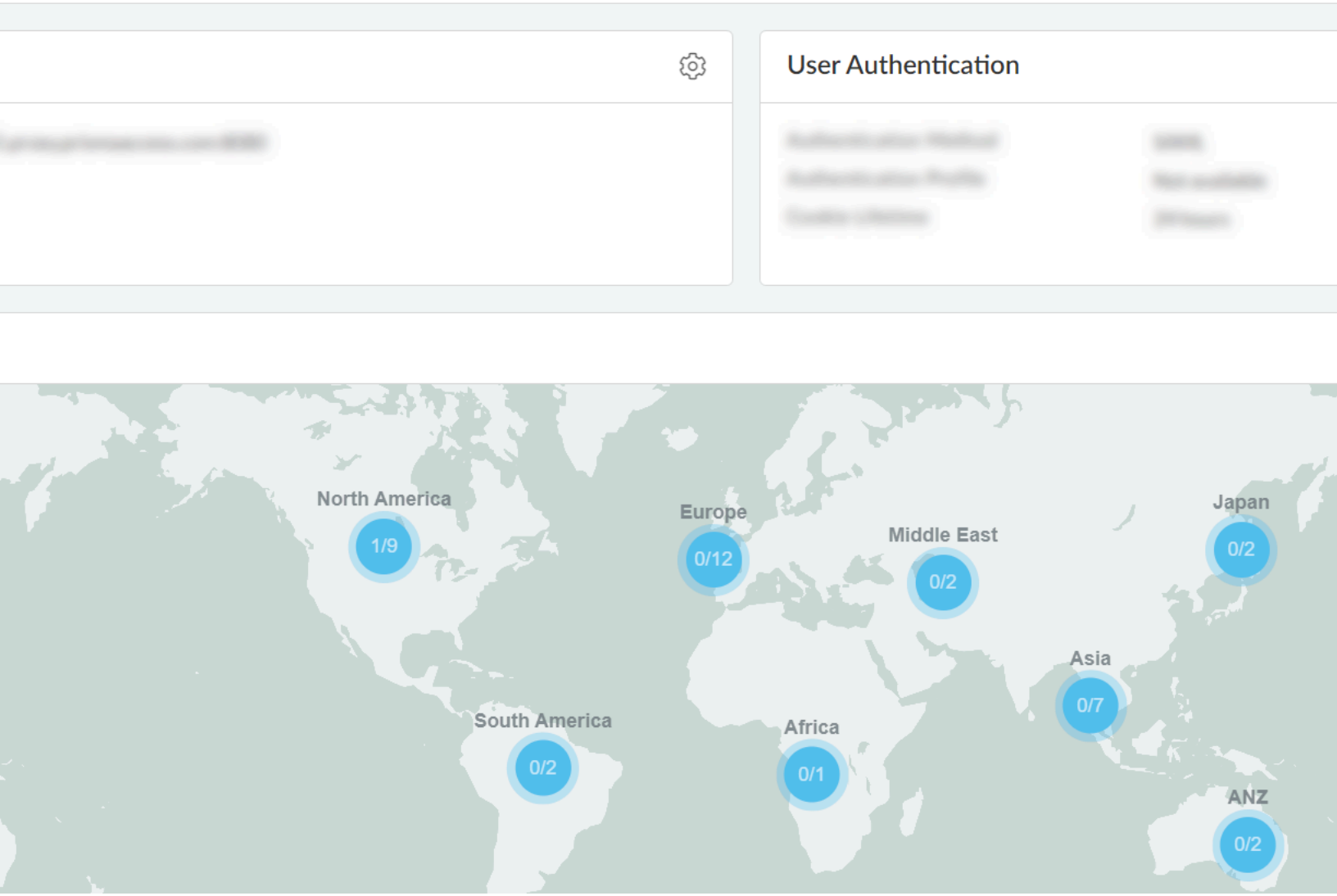



7. **Save**（儲存）變更。

 ©2025 Palo Alto Networks, Inc.

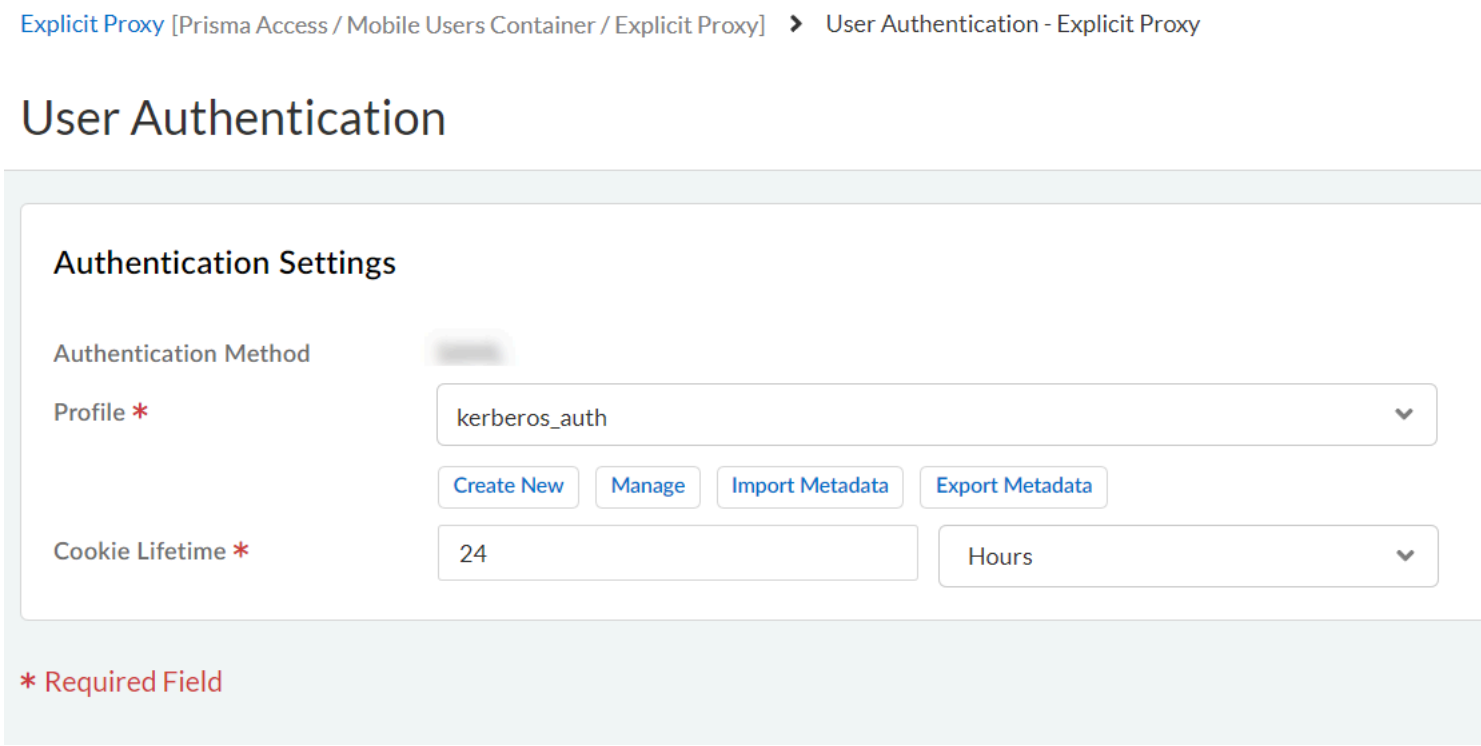
**STEP 2 |** 將驗證設定檔與驗證方法建立關聯。

1. 前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Explicit Proxy**（明確 Proxy） > **User Authentication**（使用者驗證）。




2. 選取 **Connection Name**（連線名稱）。
3. 選取 **Kerberos** 作為 **Authentication Method**（驗證方法）， 並選取您建立的 Kerberos **Profile**（設定檔）。

 ©2025 Palo Alto Networks, Inc.




4. **Save**（儲存）變更。

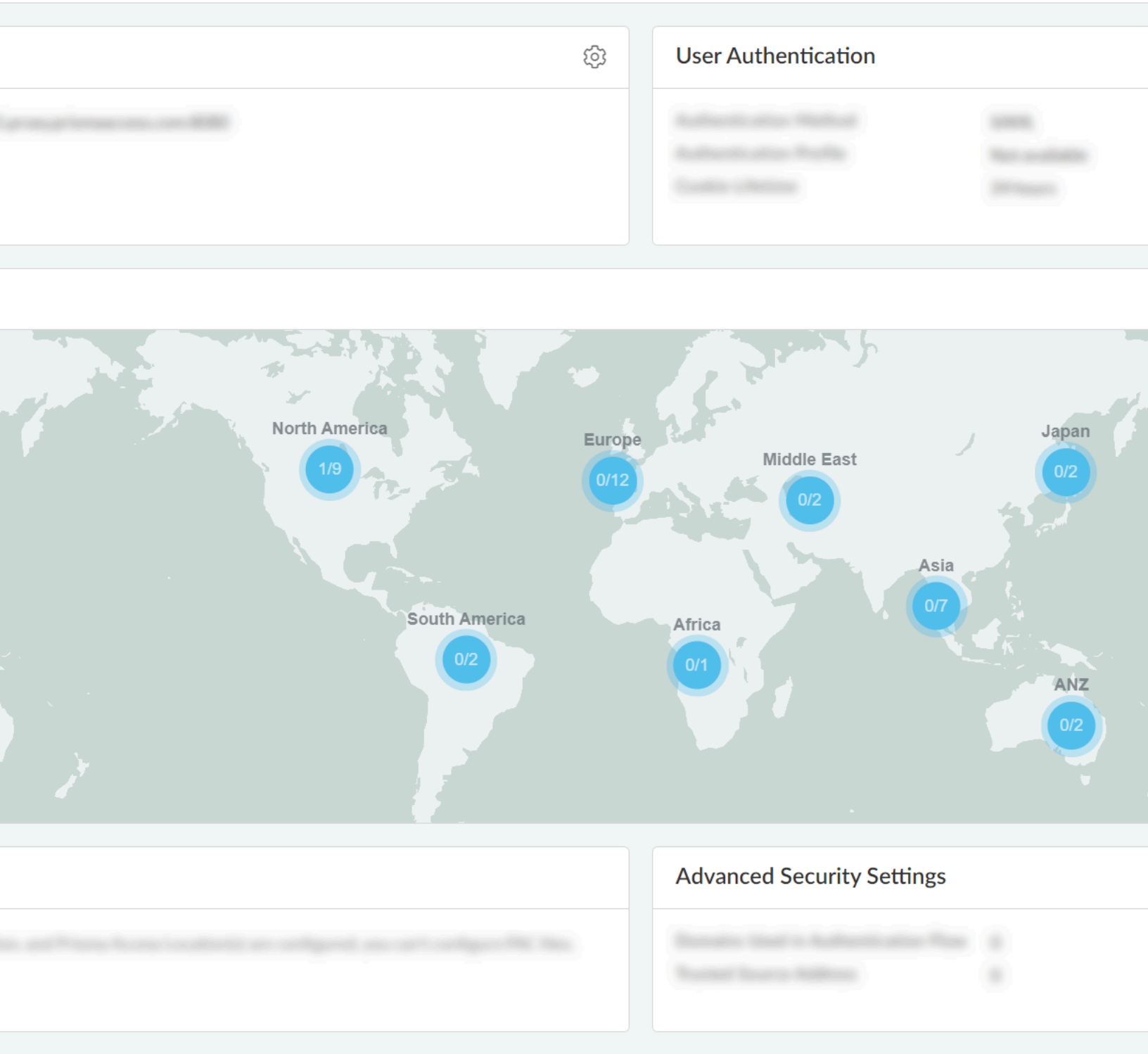
 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** （選用）將使用者、伺服器、IoT 裝置或無頭電腦所在分公司或園區位置的輸出 IP 位址新增至受信任的明確 Proxy 位址清單。

只有當您想要針對特定 IP 位址 **Skip Authentication**（跳過驗證）或 **Use X-Authenticated User (XAU) header on incoming HTTP/HTTPS requests for identity**（對傳入 **HTTP/HTTPS** 要求使用 **X** 驗證使用者 **(XAU)** 標頭進行識別）時，才需要這樣做。

1. 前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Explicit Proxy**（明確 **Proxy**） > **Advanced Security Settings**（進階安全性設定）。

 ©2025 Palo Alto Networks, Inc.

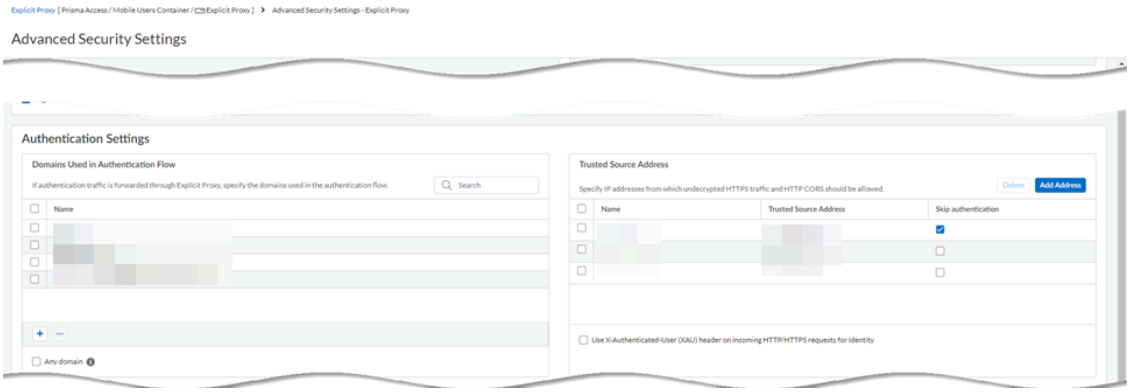



2. **Add Address**（新增位址）（一個或多個）至 **Trusted Source Address**（受信任的來源位址）欄位。


©2025 Palo Alto Networks, Inc.

如果您未將輸出端點 IP 位址新增至受信任清單，則明確 Proxy 會強制使用者和電腦使用 SAML 和 Kerberos 進行驗證。

最多輸入 100,000 個 IP 位址。




3. **Save**（儲存）變更。

**STEP 4 |** 建立 allow-all 政策規則進行使用者驗證。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全性服務） > **Security Policy**（安全性政策） > **Add Rule**（新增規則） > **Pre Rules**（前置規則） > 。.
2. 命名規則。
3. 將所有必要的比對規則設定為 **Any**（任何）。
4. 將使用者設定為 **Known**（已知）
5. 將動作設定為 **Allow**（允許）。
6. **Save**（儲存）規則。

**STEP 5 |** 推送您的設定變更。

 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** 透過檢視流量和驗證日誌，確認 Kerberos 驗證是否正在使用 Prisma Access。

1. （僅限解密流量）前往 **Activity**（活動） > **Log Viewer**（日誌檢視器） > **Firewall/Traffic**（防火牆/流量），並檢查 Kerberos 驗證是否正常運作。

   如果您使用的是 *Strata Cloud Manager*，請前往 ***Incidents & Alerts***（事件與警示） > ***Log Viewer***（日誌檢視器） > ***Firewall/Traffic***（防火牆/流量）。

   解密流量會在流量日誌中顯示使用者名稱。

2. （僅限未解密流量）前往 **Activity**（活動） > **Log Viewer**（日誌檢視器） > **Firewall/Authentication**（防火牆/驗證），並檢查 Kerberos 驗證是否正常運作。

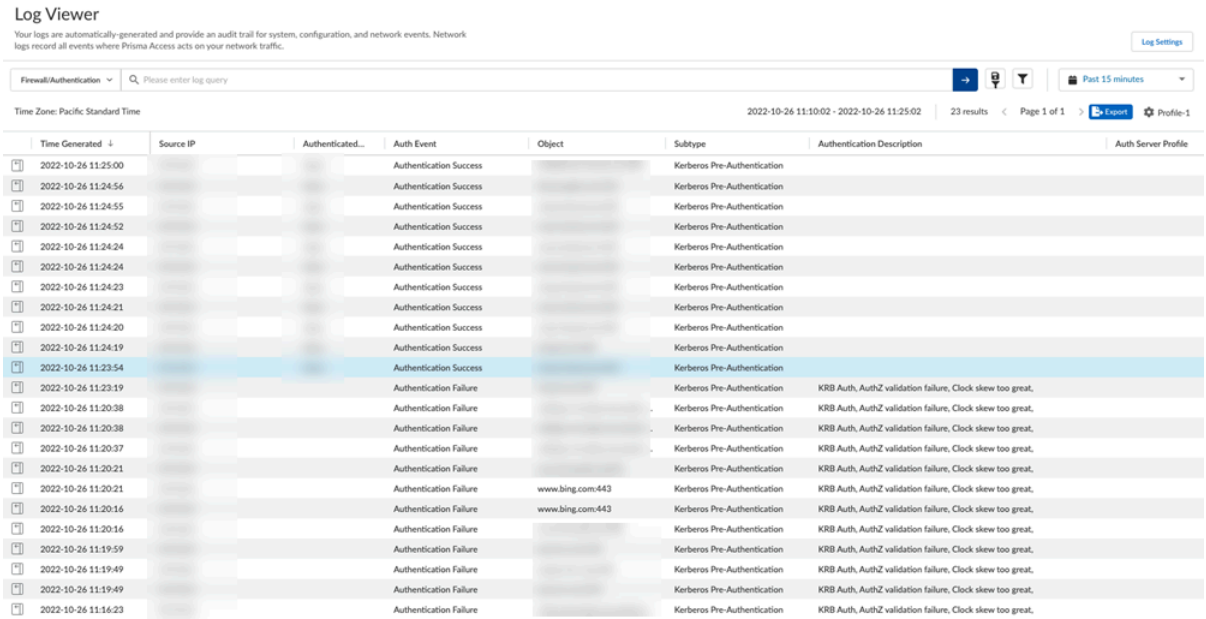
   如果您使用的是 *Strata Cloud Manager*，請前往 ***Incidents & Alerts***（事件與警示） > ***Log Viewer***（日誌檢視器） > ***Firewall/Authentication***（防火牆/驗證）。

   以下欄位提供有關驗證事件的詳細資訊：

   - **Object**（物件）—使用者在重新導向到 Kerberos 進行驗證之前嘗試存取的網站。
   - **Auth Event**（驗證事件）—驗證嘗試的狀態。

     **Authentication Success**（驗證成功）表示驗證事件成功；**Authentication Failure**（驗證失敗）表示嘗試失敗並產生日誌。
   - **Authentication Description**（驗證說明）—如果驗證嘗試失敗，則有關失敗類型的其他資訊。

     例如，**user not allowed**（使用者不被允許）表示不允許使用者或群組使用 Kerberos 進行驗證，可能是因為它未新增到驗證設定檔中的 **Allow List**（允許清單）。



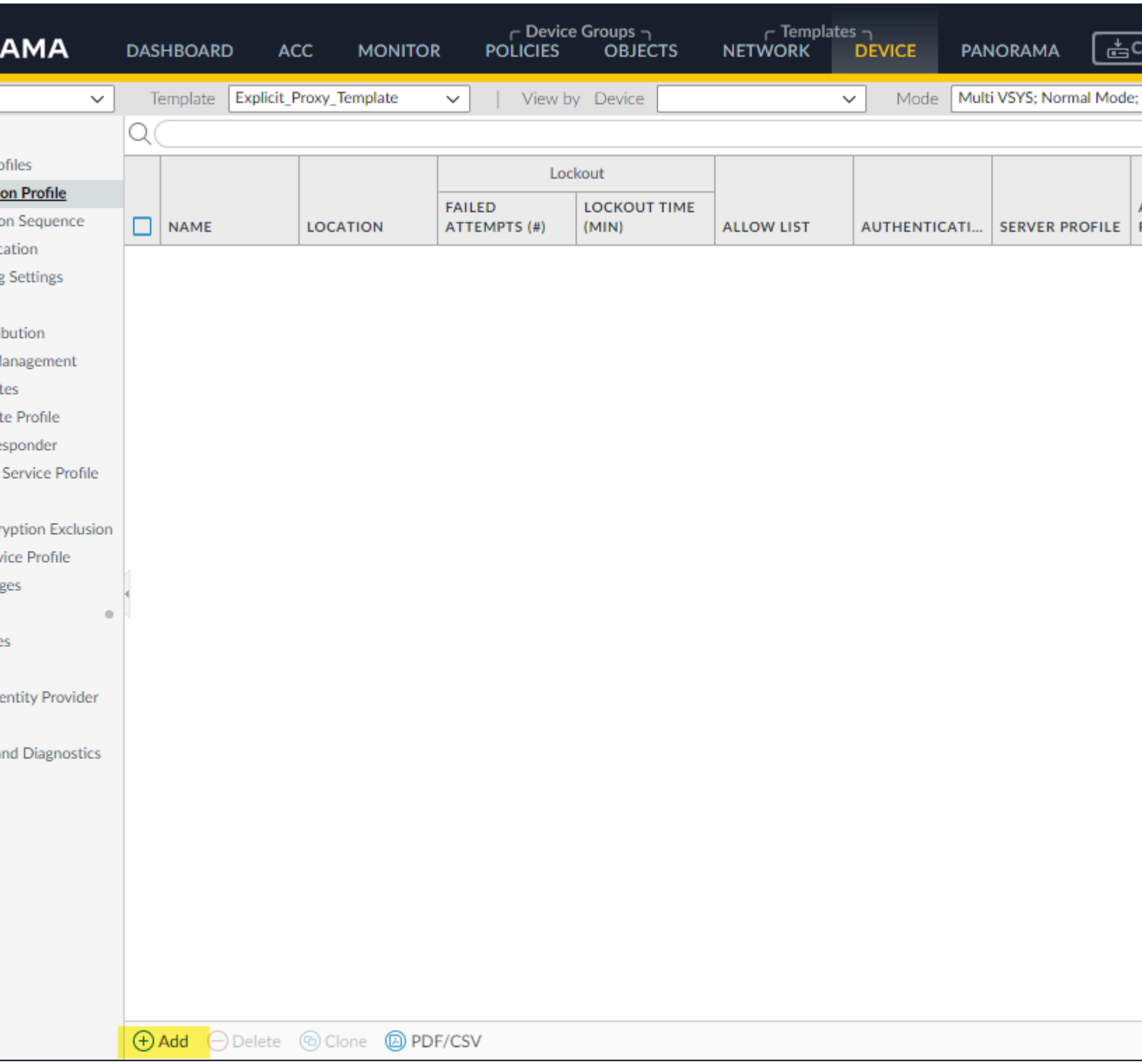

設定 **Kerberos** 驗證進行明確 **Proxy** 部署 **(Panorama)**

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** 設定 Kerberos 驗證設定檔。

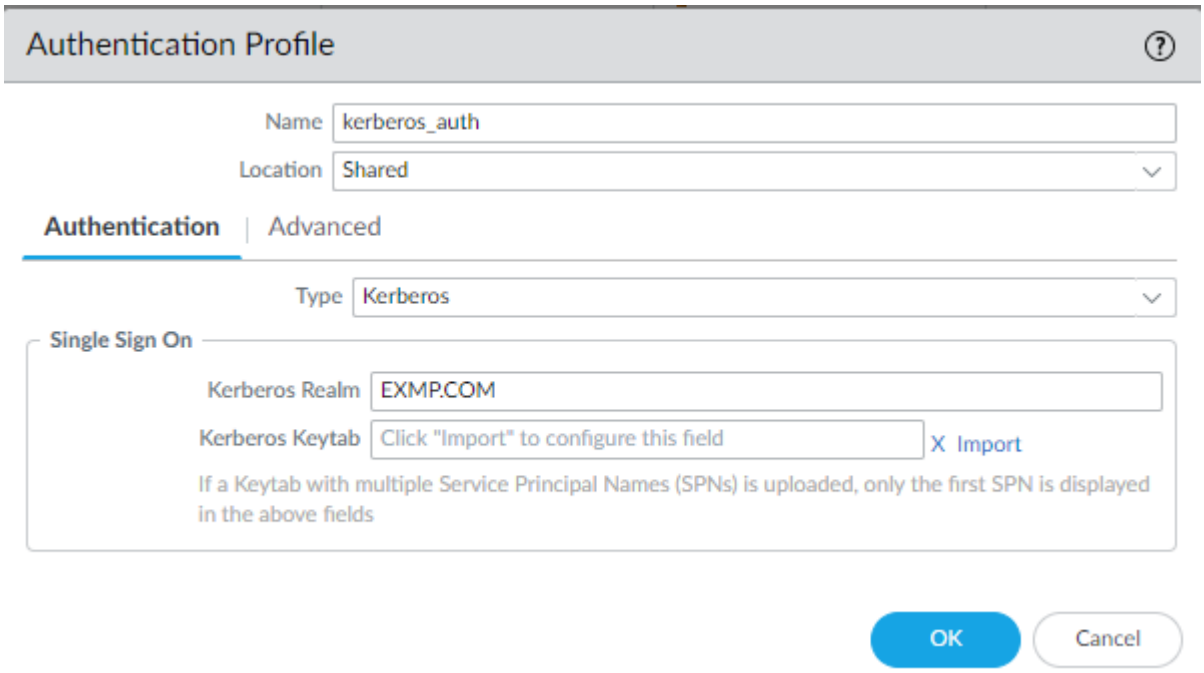
此設定檔定義明確 Proxy 程式如何連線到 Kerberos 伺服器，進行行動使用者驗證。

1. 前往 **Device**（裝置） > **Authentication Profile**（驗證設定檔） > **+ Add**（+ 新增）。

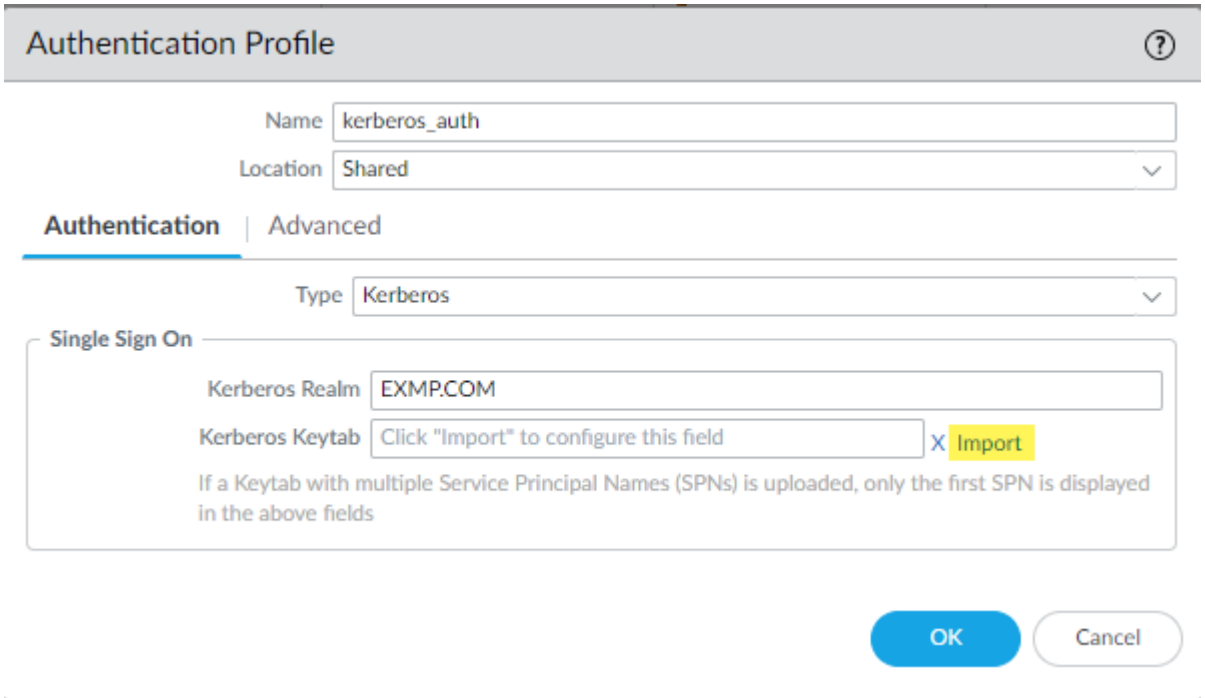



2. 選取 **Type**（類型）：**Kerberos**。

 ©2025 Palo Alto Networks, Inc.



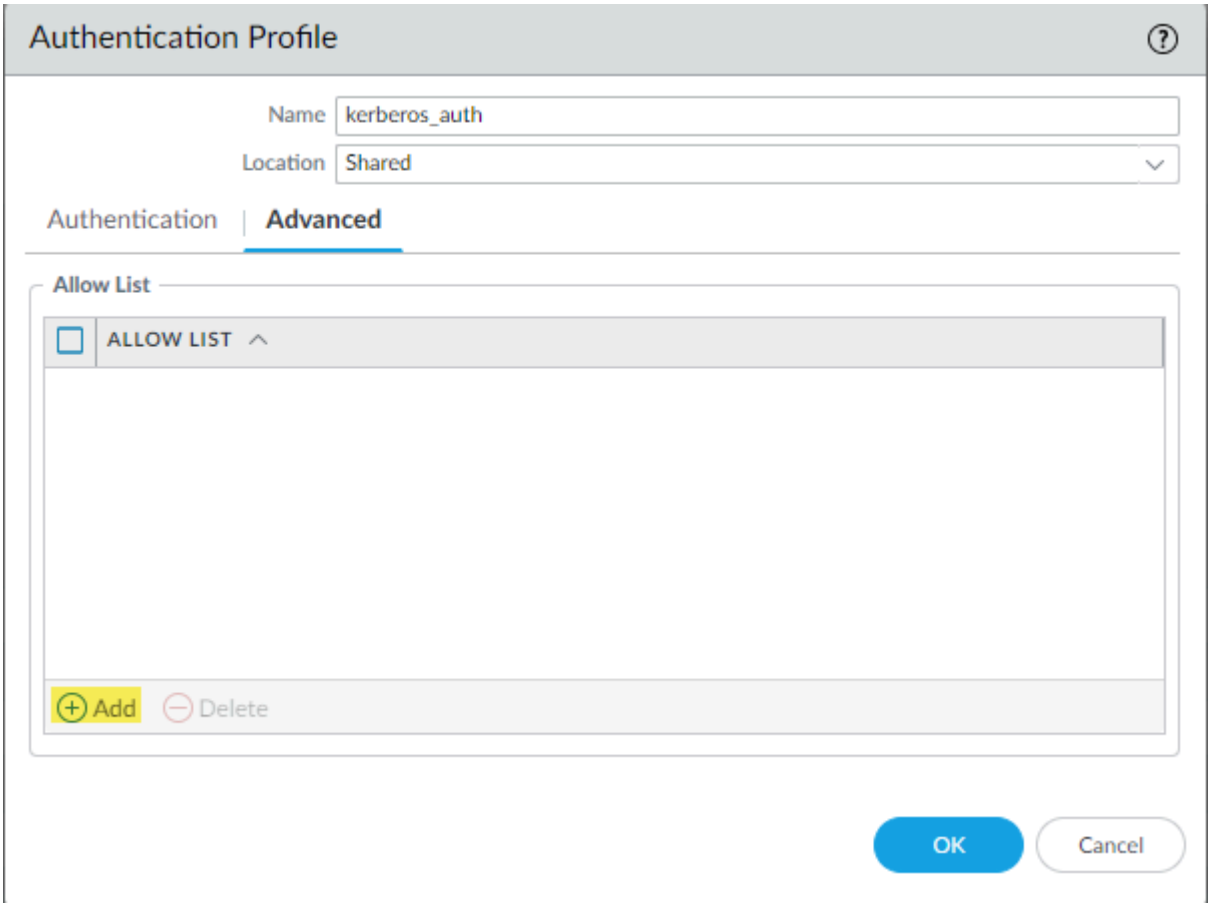

3. 輸入用來識別驗證設定檔的 **Name**（名稱）。
4. 輸入 **Kerberos Realm**（**Kerberos** 領域）（最多 127 個字元）以指定使用者登入名稱的主機名稱部分。例如，使用者帳戶名稱 user@EXMP.COM 具有領域 EXMP.COM。
5. 匯入您先前建立的 **Kerberos Keytab**（**Kerberos** 金鑰標籤）。




6. 使用此設定檔新增允許進行驗證的使用者。
   - 選取 **Advanced**（進階） > **+ Add**（+ 新增）。
   - 若要選取所有使用者，請選取 **all**（全部）。

 ©2025 Palo Alto Networks, Inc.

- 如果您是使用雲端識別引擎填入使用者清單，請從清單中選擇使用者，或選取 **all**（全部）以允許所有使用者進行驗證。
- 若要新增可以使用 Kerberos 登入的本機使用者，請輸入他們的使用者名稱。
  - 設定使用者驗證和使用者對應時，請使用 userPrincipalName (UPN) 的格式；不支援其他格式（例如 samAccountName）。
  - 不支援 Unicode 字元使用者名稱。



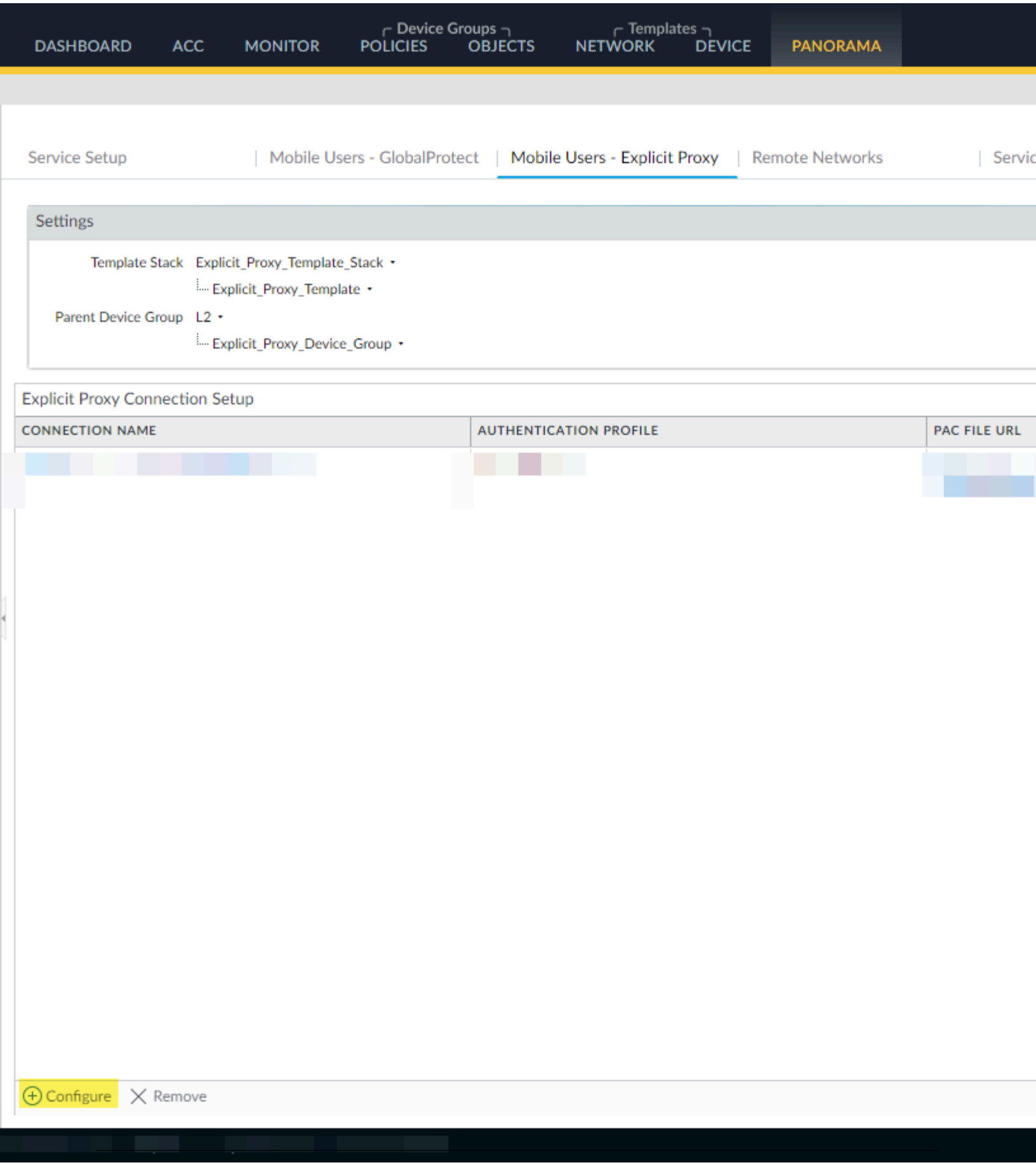

7. **Save**（儲存）變更。


©2025 Palo Alto Networks, Inc.

**STEP 2 |** 將驗證設定檔與驗證方法建立關聯。

1. 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **+ Configure**（+ 設定）。

 ©2025 Palo Alto Networks, Inc.





©2025 Palo Alto Networks, Inc.

2. 設定 **Explicity Proxy FQDN**（明確 **Proxy FQDN**）。
3. 選取您建立的 Kerberos **Profile**（設定檔）。
4. 選取 **OK**（確定）來儲存您的變更。

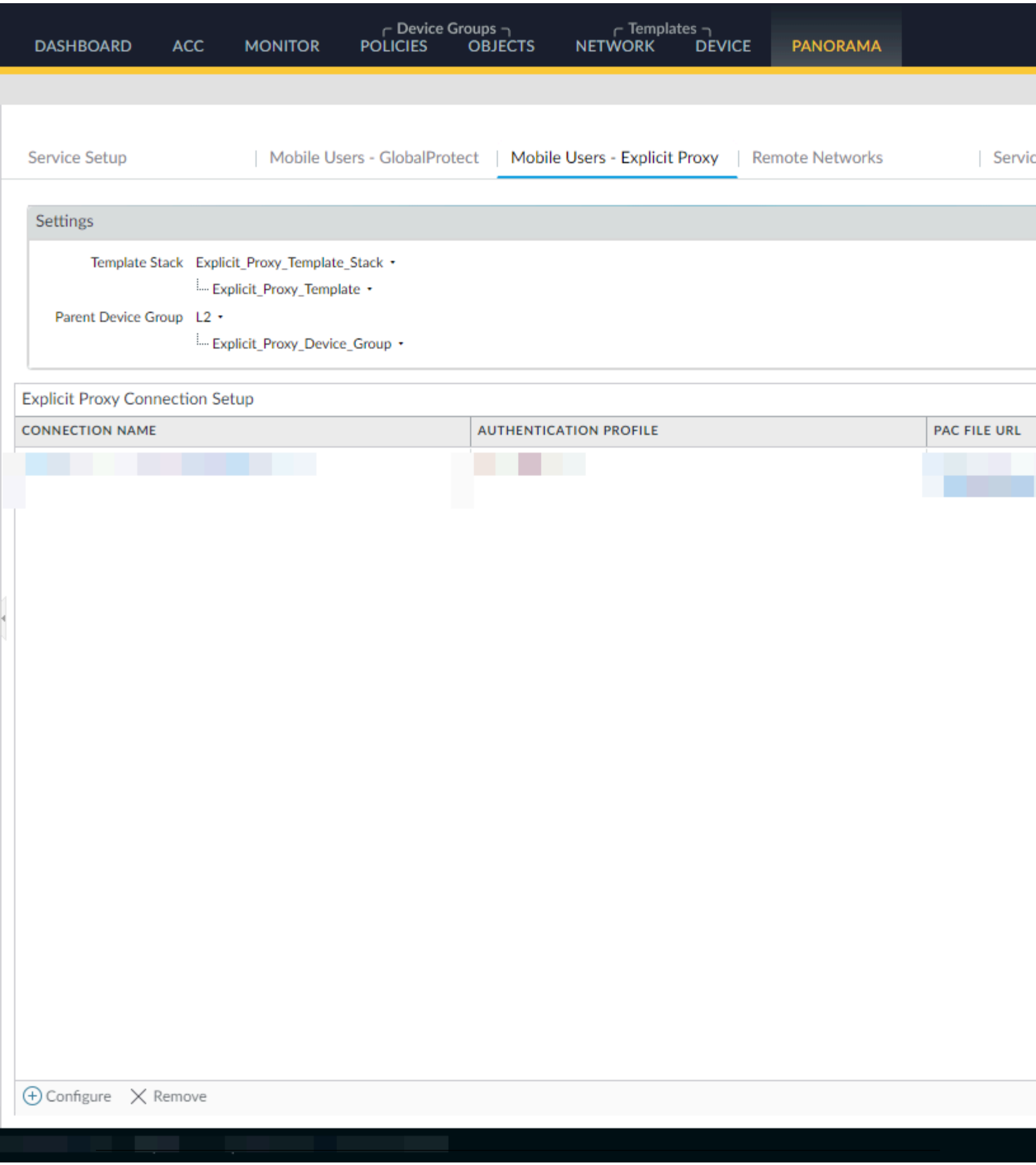

©2025 Palo Alto Networks, Inc.

**STEP 3 |** （選用）將使用者、伺服器、IoT 裝置或無頭電腦所在分公司或園區位置的輸出 IP 位址新增至受信任的明確 Proxy 位址清單。

只有當您想要針對特定 IP 位址 **Skip Authentication**（跳過驗證）或 **Use X-Authenticated User (XAU) header on incoming HTTP/HTTPS requests for identity**（對傳入 **HTTP/HTTPS** 要求使用 **X** 驗證使用者 **(XAU)** 標頭進行識別）時，才需要這樣做。

1. 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Settings gear**（設定齒輪） > **Authentication Settings**（驗證設定）。

 ©2025 Palo Alto Networks, Inc.





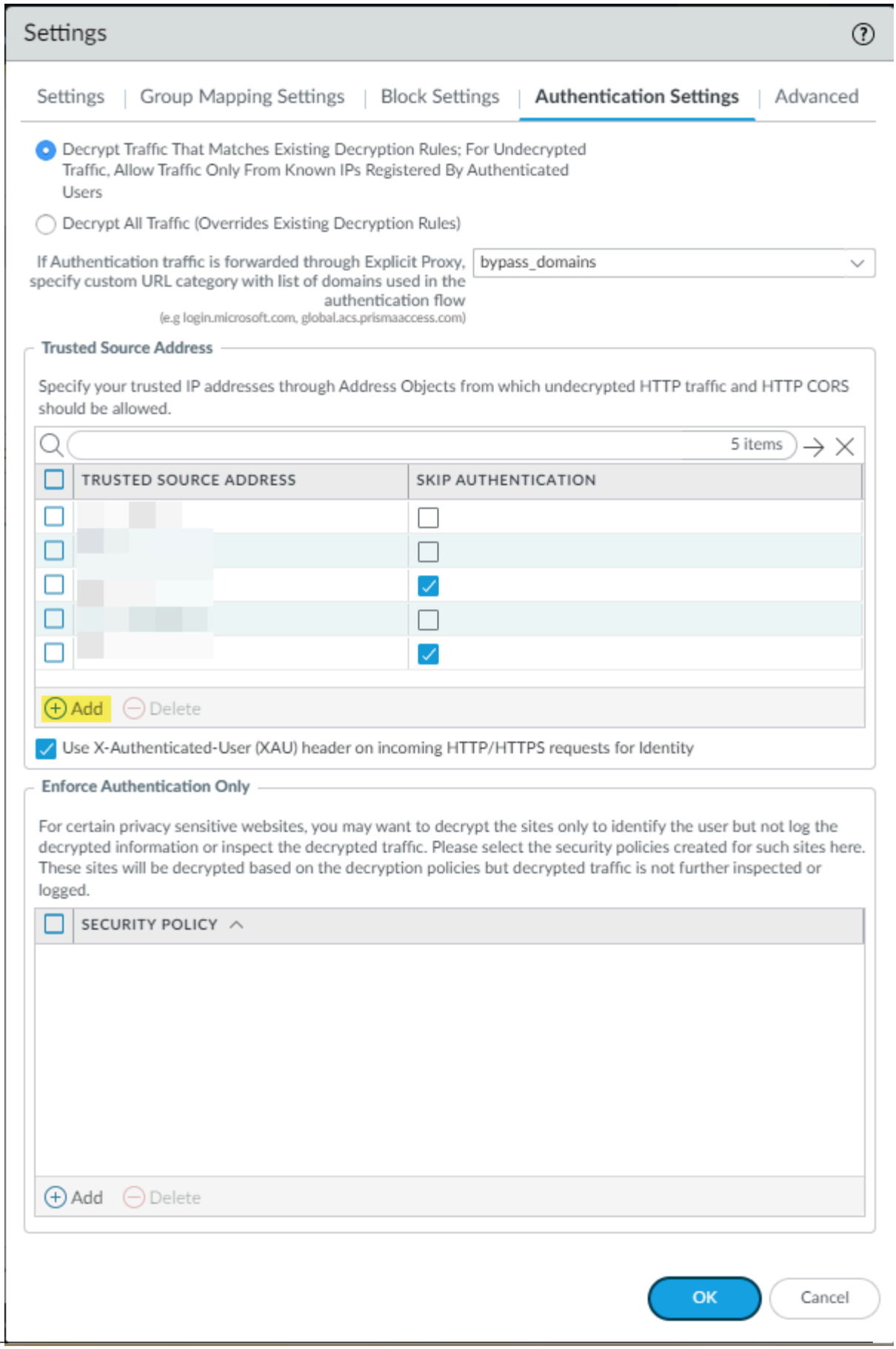
©2025 Palo Alto Networks, Inc.

2. **Add**（新增）位址至 **Trusted Source Address**（受信任的來源位址）欄位。

   如果您未將輸出端點 IP 位址新增至受信任清單，則明確 Proxy 會強制使用者和電腦使用 SAML 和 Kerberos 進行驗證。

   最多輸入 100,000 個 IP 位址。


©2025 Palo Alto Networks, Inc.





©2025 Palo Alto Networks, Inc.

3. 選取 **OK**（確定）來儲存您的變更。

**STEP 4 |** 建立 allow-all 政策規則進行使用者驗證。

1. 選取 **Policies**（政策） > **Pre Rules**（前置規則） > **+ Add**（+新增）。
2. 命名規則。
3. 選取 **Source**（來源）
4. 將來源使用者設定為 **known-user**
5. 將所有其他必要值設定為 **Any**（任何）。
6. 選取 **OK**（確定）來儲存規則。

**STEP 5 |** 提交並推送您的設定變更。

**STEP 6 |** 透過檢視流量和驗證日誌，確認 Kerberos 驗證是否正在使用 Prisma Access。

1. （僅限解密流量）前往 **Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量），並檢查 Kerberos 驗證是否正常運作。

   解密流量會在流量日誌中顯示使用者名稱。

2. （僅限未解密流量）前往 **Monitor**（監控） > **Logs**（日誌） > 驗證（流量），並檢查 Kerberos 驗證是否正常運作。

   以下欄位提供有關驗證事件的詳細資訊：

   - **Object**（物件）—使用者在重新導向到 Kerberos 進行驗證之前嘗試存取的網站。
   - **Auth Event**（驗證事件）—驗證嘗試的狀態。

     **Authentication Success**（驗證成功）表示驗證事件成功；**Authentication Failure**（驗證失敗）表示嘗試失敗並產生日誌。
   - **Authentication Description**（驗證說明）—如果驗證嘗試失敗，則有關失敗類型的其他資訊。

     例如，**user not allowed**（使用者不被允許）表示不允許使用者或群組使用 Kerberos 進行驗證，可能是因為它未新增到驗證設定檔中的 **Allow List**（允許清單）。

## 明確 Proxy 部署的 Cloud Identity Engine 驗證

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

使用雲端識別引擎，為 Prisma Access—明確 Proxy 部署中的行動使用者提供使用者識別和使用者驗證。


©2025 Palo Alto Networks, Inc.

雲端身分引擎為內部部署、雲端型或混合網路環境中的集中式雲端型解決方案提供使用者識別和使用者驗證。雲端識別引擎可讓您根據使用者和群組撰寫安全性政策，並透過強制執行行為型安全性動作來協助保護您的網路。

透過持續同步您目錄中的資訊，無論它們是內部部署、雲端型還是混合，確保您的使用者資訊準確且最新，並且即使雲端識別提供者暫時無法使用，政策強制執行也會根據對應繼續。

- 明確 Proxy 部署的雲端識別引擎驗證 (Strata Cloud Manager)
- 明確 Proxy 部署的雲端識別引擎驗證 (Panorama)

## 明確 Proxy 部署的雲端識別引擎驗證 (Strata Cloud Manager)

雲端識別引擎可為 Prisma Access—明確 Proxy 部署中的行動使用者提供使用者識別和使用者驗證。雲端識別引擎可與明確 Proxy 驗證快取服務 (ACS) 整合，並使用 SAML 識別提供者 (IdP) 提供明確 Proxy 行動使用者的驗證。

若要使用雲端識別引擎，為行動使用者—明確 Proxy 部署設定驗證，請完成以下步驟。

**STEP 1 |** 在 Prisma Access (Managed by Strata Cloud Manager) 中，為您的租用戶設定明確 Proxy。

在設定明確 Proxy 之前，請在設定它時注意明確 Proxy 的運作方式和使用指導方針。

如果您有多個租用戶，請為每個需要明確 Proxy 的租用戶設定明確 Proxy。

**STEP 2 |** 登入中樞，然後從雲端識別引擎應用程式中，設定驗證類型和驗證提供者。

您可以透過租用戶或支援帳戶，檢視中樞內的應用程式。

1. 在雲端識別引擎引擎中，設定 SAML 驗證類型。

   雲端識別引擎入門指南具有您在雲端識別引擎中設定 SAML IdP 所需的程序：

   - 在雲端識別引擎中將 Azure 設定為 IdP
   - 在雲端識別引擎中將 Okta 設定為 IdP
   - 在雲端識別引擎中將 PingOne 設定為 IdP
   - 在雲端識別引擎中將 PingFederate 設定為 IdP
   - 在雲端識別引擎中將 Google 設定為 IdP

   請勿設定單一登出，因為不支援。
2. 在雲端識別引擎中設定驗證設定檔，然後選取可以使用此驗證方法的使用者和群組。

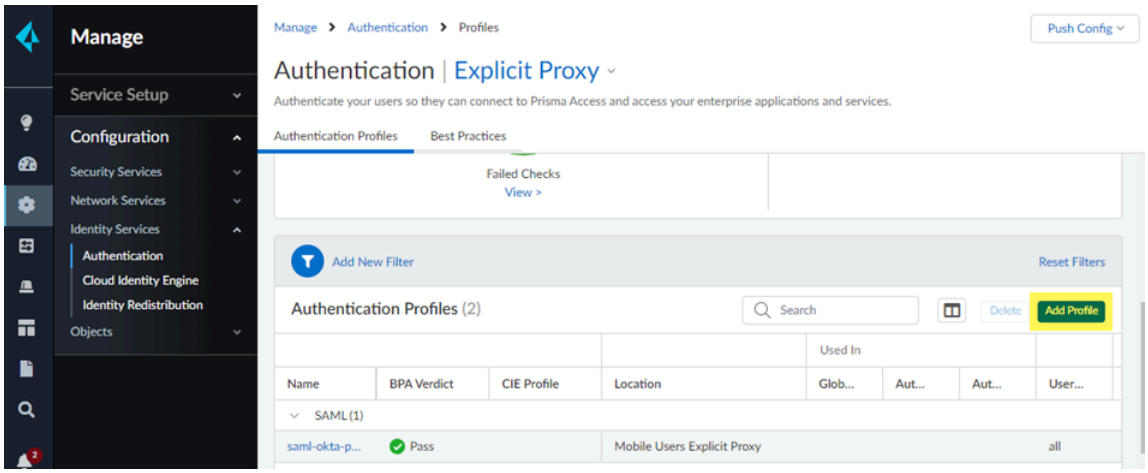
   在後續步驟中，當您在 Prisma Access (Managed by Strata Cloud Manager) 中建立驗證設定檔時指定此設定檔。

**STEP 3 |** 返回 Prisma Access (Managed by Strata Cloud Manager) 並建立要與雲端驗證引擎搭配使用的驗證設定檔。

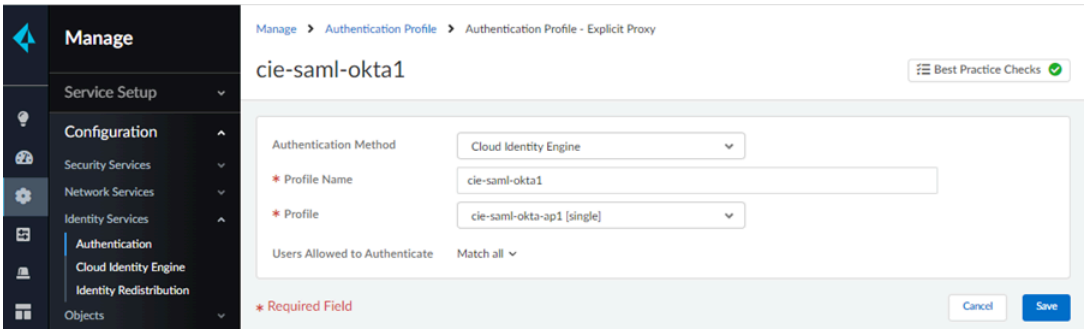
1. 前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW 和 Prisma Access**） > **Identity Services**（識別服務） > **Authentication**（驗證），然後將

 ©2025 Palo Alto Networks, Inc.

範圍設定為 **Explicit Proxy**（明確 **Proxy**），並新增驗證設定檔（**Add Profile**（新增設定檔））。




2. 選取 **Cloud Identity Engine**（雲端識別引擎）作為 **Authentication Method**（驗證方法）。
3. 給與設定檔一個 **Profile Name**（設定檔名稱）。
4. 選取您在上一個步驟中建立的雲端識別引擎驗證設定檔。

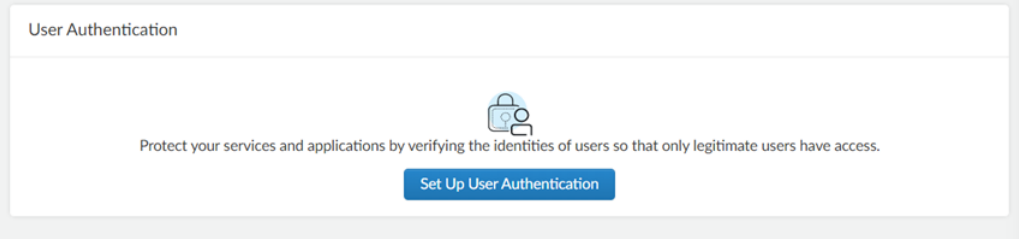



5. **Save**（儲存）變更。


©2025 Palo Alto Networks, Inc.

**STEP 4 |** 在明確 Proxy 中設定使用者驗證。

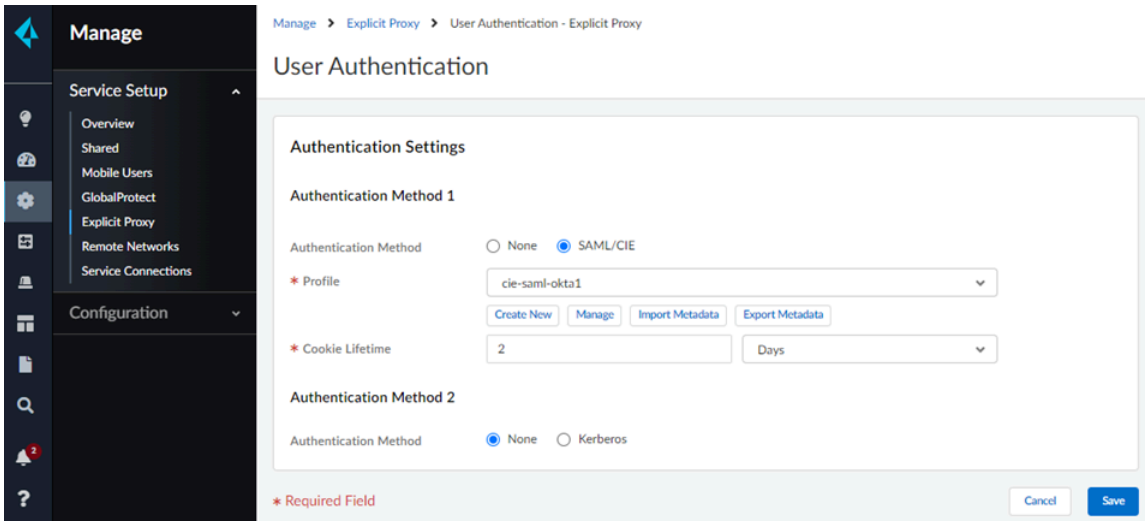
1. 前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Explicit Proxy**（明確 Proxy）和 **Set Up User Authentication**（設定使用者驗證）。




2. 選取 **SAML/CIE** 作為 **Authentication Method**（驗證方法）。
3. 選取您在 Cloud Managed Prisma Access 中建立的驗證設定檔。
4. 為儲存使用者驗證認證的 Cookie 指定 **Cookie Lifetime**（**Cookie** 存留時間）。

   在 IdP 驗證使用者之後，Prisma Access 將在驗證快取服務 (ACS) 中儲存使用者的驗證狀態。驗證的有效期基於您在這裡指定的 Cookie 存留時間值。

   為了防止使用者在 Cookie 存留時間到期之前無法下載大型檔案，或者 Cookie 在使用者長時間存取單一網站時過期，Palo Alto Networks 建議您設定至少一天的 **Cookie Lifetime**（**Cookie** 存留時間）。如果明確 Proxy 使用者遇到 Cookie 存留時間到期問題，他們可以瀏覽到其他網站，以重新向 ACS 進行驗證並重新整理 ACS Cookie。

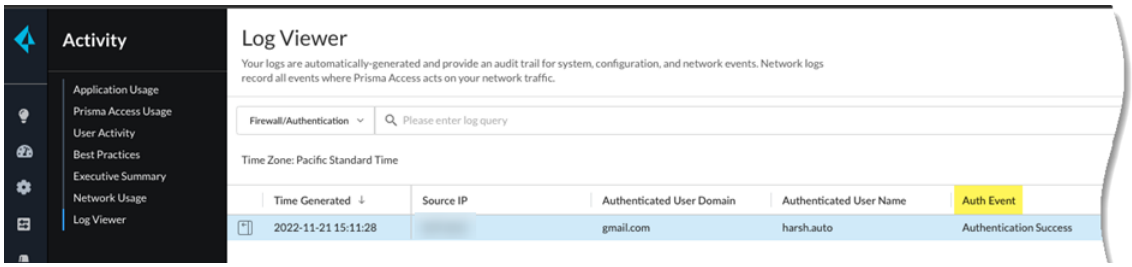



5. **Save**（儲存）變更。

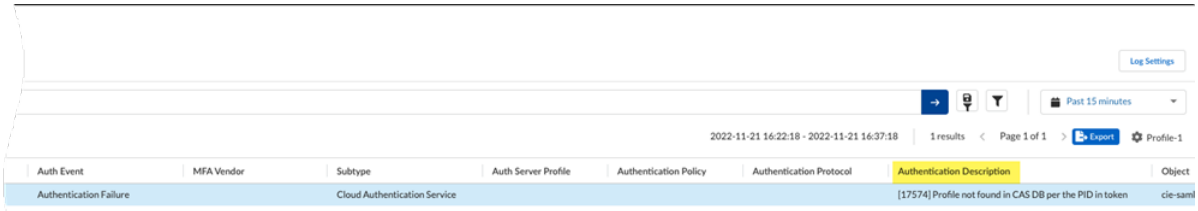

©2025 Palo Alto Networks, Inc.

**STEP 5 |** 驗證雲端識別引擎是否已成功驗證您的明確 Proxy 行動使用者。

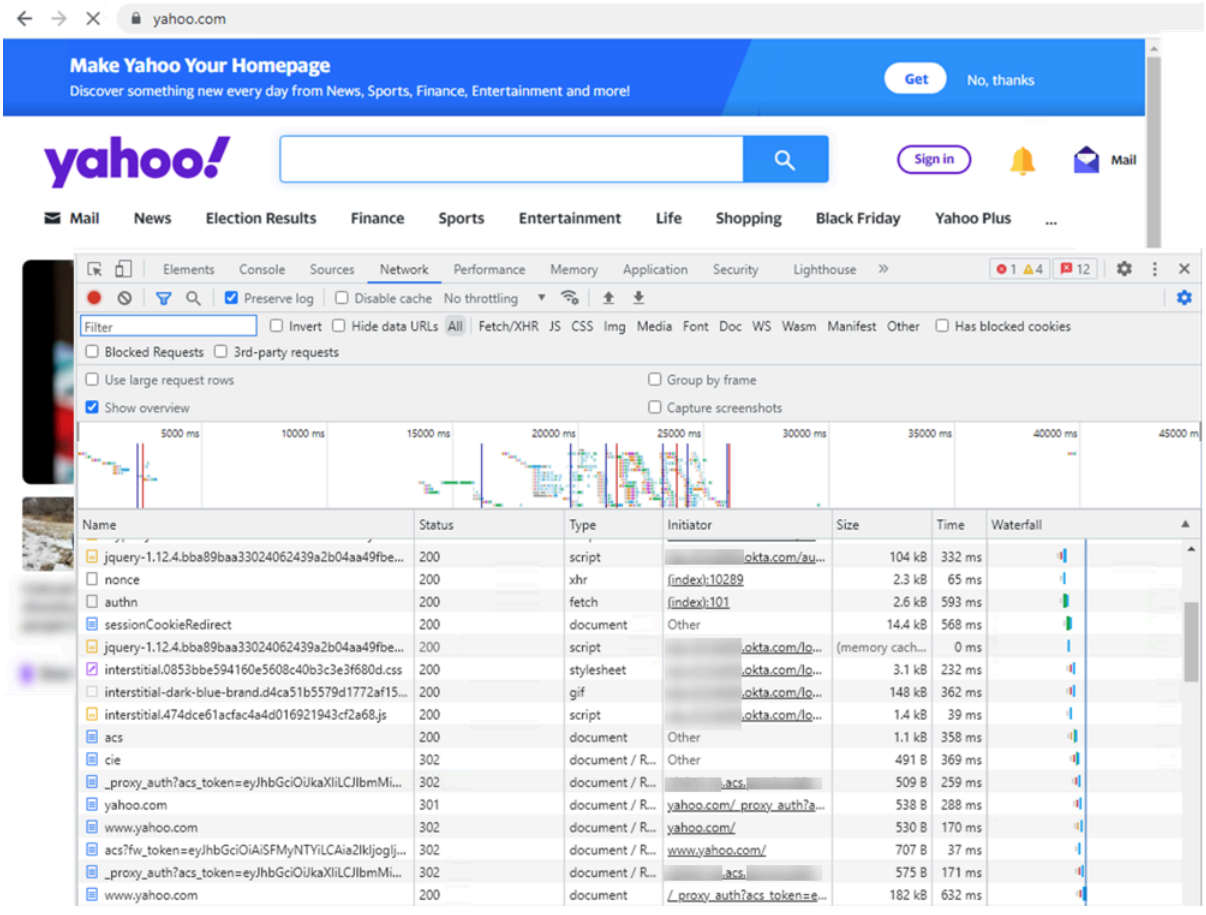
1. 從 Prisma Access (Managed by Strata Cloud Manager) 中，選取 **Incidents & Alerts**（事件與警示） > **Log Viewer**（日誌檢視器） > **Firewall/Authentication**（防火牆/驗證）。
2. 檢視 **Auth Event**（驗證事件）狀態。




如果驗證失敗，請檢視 **Authentication Description**（驗證說明），以取得有關失敗的詳細資訊。




3. 從行動使用者的端點中，使用開發工具檢視雲端識別引擎驗證流程。




 ©2025 Palo Alto Networks, Inc.

明確 Proxy 部署的雲端識別引擎驗證 (Panorama)

使用雲端識別引擎驗證 Prisma Access (Managed by Panorama) 明確 Proxy 行動使用者

# 遠端網路上的 Proxy 模式

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>如果您想要在 Prisma Access 環境中於明確 Proxy 上啟用私人來源 IP 型可視性和強制執行，請與您的客戶團隊聯繫以進一步瞭解。 | • Prisma Access 授權<br>遠端網路的 Proxy 模式需要 Prisma Access 行動使用者授權和 Prisma Access 遠端網路授權。 |

遠端網路上的 Proxy 模式有助於保護您分支中使用者和伺服器的輸出網際網路流量，而這些使用者和伺服器由於網路或合規性原因需要 PAC 型連線方法。

您可以對遠端網路使用 Proxy：

- 保護來自使用非預設路由的分支網站的網際網路流量。
- 保護來自您分支的網際網路繫結流量，無需將其回傳到資料中心或總部。
- 透過私人 IP 位址連線至 Prisma Access 明確 Proxy。

  Prisma Access 為您全域提供四個 Anycast IP 位址，以及每個遠端網路一個單點傳送 IP 位址，您用來將流量轉送至明確 Proxy。
- 根據分支中系統的來源 IP 強制執行安全性控制並取得可視性。
- 根據來源 IP 位址跳過伺服器的驗證。
- 透過 IPSec 通道從您的分支連線到 Prisma Access。
- 如果您需要超過 1000 Mbps 的頻寬，則可以使用多個遠端網路連線，建立高頻寬遠端網路連線，並在每個連線中指定明確 Proxy Anycast 和單點傳送位址。

下圖顯示一個已為沒有設定預設路由的網站設定的遠端網路。為了使用明確 Proxy 保護網站中的使用者和無頭裝置，管理員已進行以下設定變更：

- 已裝載遠端網路和明確 Proxy 位置，並已擷取 Prisma Access 從其基礎結構子網路取得的 Anycast 和單點傳送 IP 位址。

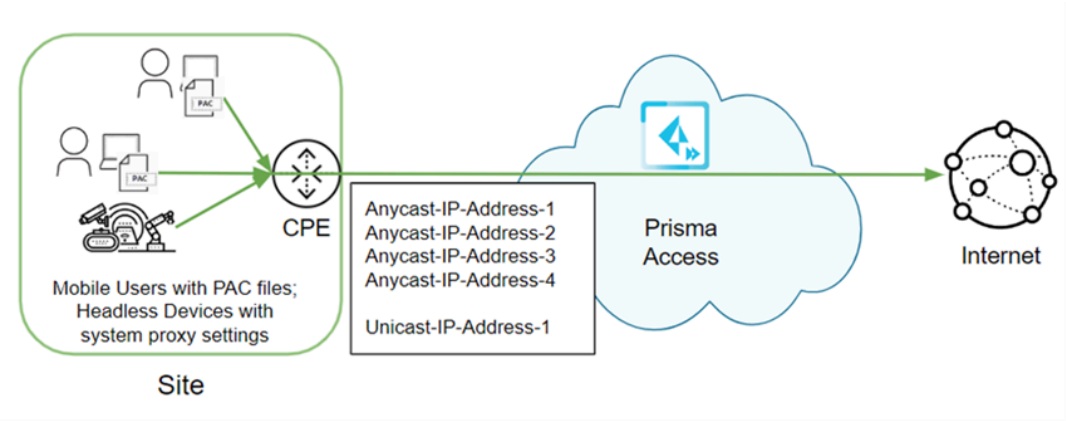
  

  您還可以為明確 *Proxy* 導向的流量建立主機名稱，並將明確 *Proxy* 單點傳送和 *Anycast IP* 位址新增到該主機名稱。
- 已設定 CPE 將明確 Proxy 流量轉送到這些 Anycast 和單點傳送位址。

  使用 PAC 檔案中的 Anycast IP 位址，讓 Prisma Access 從任何裝載的遠端網路通道中選取，以將流量轉送到明確 Proxy。使用單點傳送位址，讓 Prisma Access 透過特定的遠端網路通道轉送流量。在這個範例中，您可以使用 Anycast 或單點傳送位址，因為流量僅通過一個遠端網路 IPSec 通道。
- 在使用者端點的 PAC 檔案中，以及在無頭裝置的系統 Proxy 設定中指定這些 IP 位址。

 ©2025 Palo Alto Networks, Inc.

在設定完成之後，Prisma Access 會將流量從遠端網路通道轉送到明確 Proxy。




- Strata Cloud Manager
- Panorama

## 遠端網路上的 Proxy 模式 (Strata Cloud Manager)

若要在 Cloud Managed Prisma Access 中使用明確 Proxy 保護遠端網路中的使用者，請完成下列步驟。

**STEP 1 |** 設定您的明確 Proxy 設定，並裝載您要新增的明確 Proxy 位置。

**STEP 2 |** 如果您還沒有這樣做，請裝載遠端網路。

您必須在明確 Proxy 支援的位置中啟用 *Prisma Access* 遠端網路。

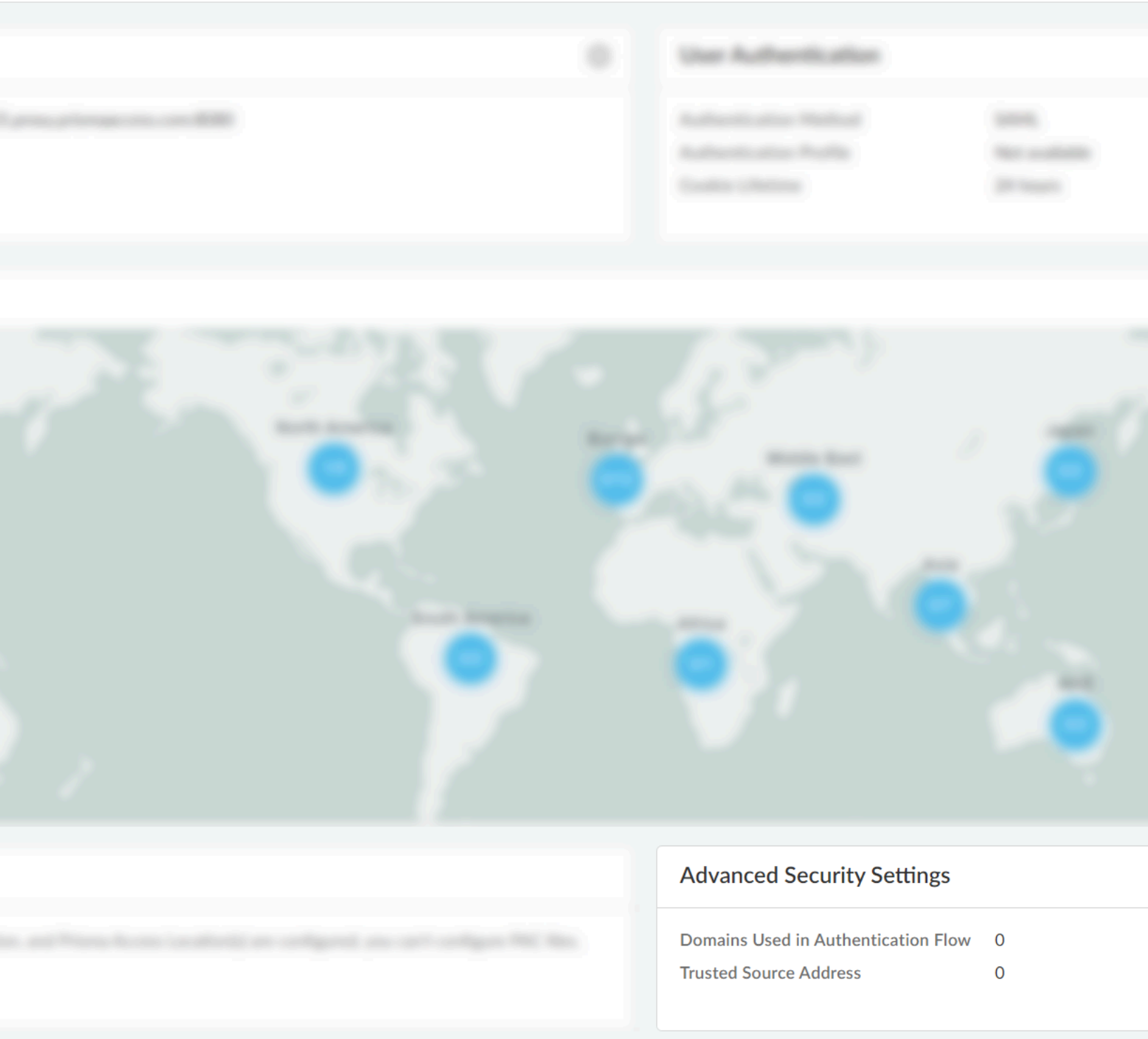
**STEP 3 |** **Push Config**（推送設定），確保在 **Push**（推送）範圍中，選取 **Mobile Users**—**Remote Workforce**（行動使用者—遠端勞動力）和 **Remote Networks**（遠端網路）。

推送操作會擷取 Anycast 位址，您需要這些位址，以整合明確 Proxy 與遠端網路。


©2025 Palo Alto Networks, Inc.

**STEP 4 |** 取得您用於明確 Proxy/遠端網路部署的 Anycast IP 位址。

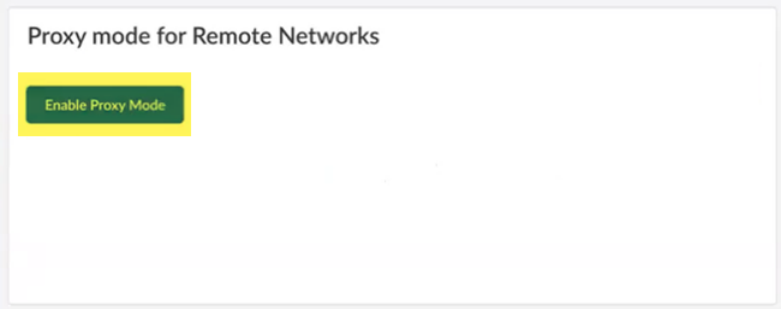
1. 前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Explicit Proxy**（明確 Proxy） > **Advanced Security Settings**（進階安全性設定）。



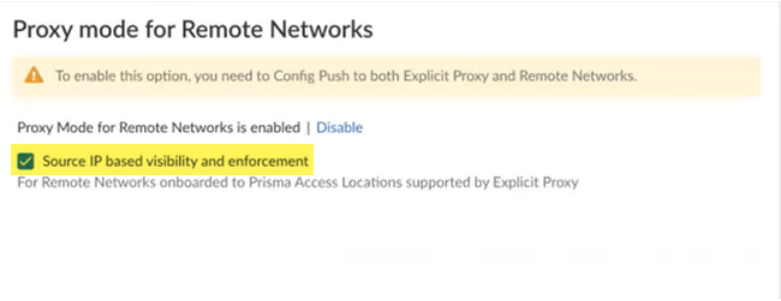


©2025 Palo Alto Networks, Inc.

2. **Enable Proxy Mode**（啟用 **Proxy** 模式）。




3. 若要利用分支位置中將流量轉送到明確 Proxy 的系統來源 IP 位址，請選取 **Source IP based visibility and enforcement**（來源 **IP** 型可視性和強制執行）。
   此功能具有以下需求：
   - Prisma Access 資料平面至少為 10.2.4
   - 您必須僅使用明確 Proxy 支援的遠端網路位置。




4. 新增一個政策，以允許遠端網路上繫結至 Anycast 和單點傳送 IP 的流量。如果您已啟用 **Source IP visibility and enforcement**（來源 **IP** 可視性和強制執行），請在明確 Proxy 中

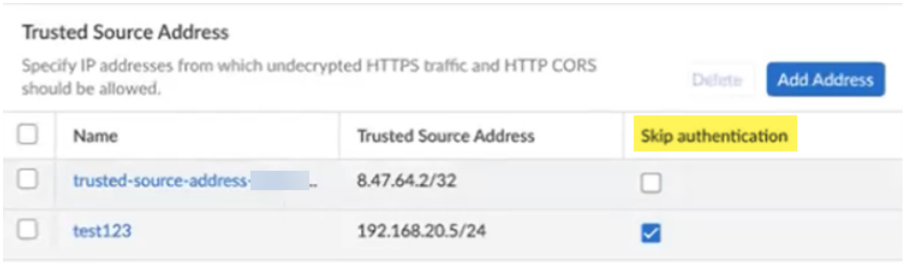

©2025 Palo Alto Networks, Inc.

使用安全性政策中的 **Source IP**（來源 **IP**）欄位來保護流量。您需要遠端網路中的額外政策。

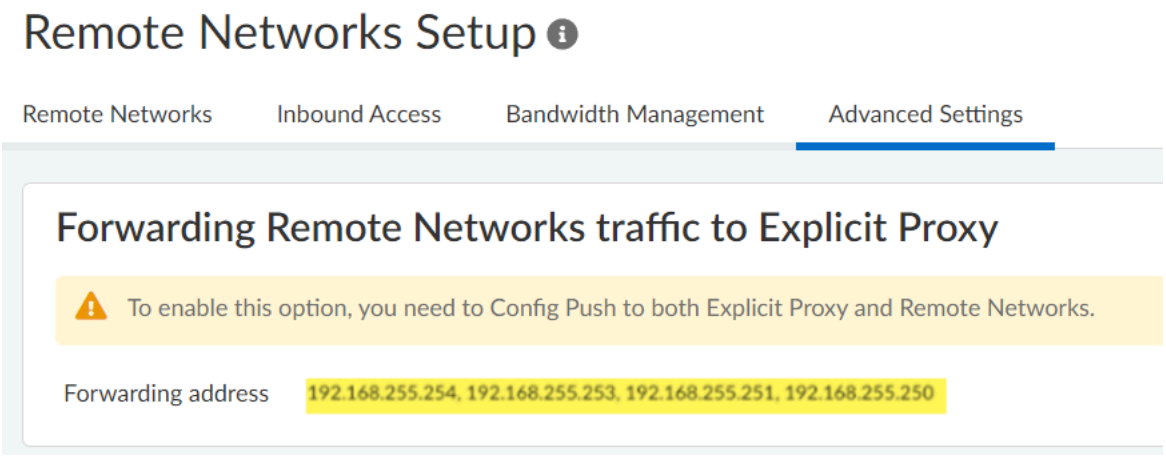
5. （選用）若要略過您輸入的任何受信任來源位址的驗證，請在 **Trusted Source Address**（受信任的來源位址）區域中指定應跳過驗證的 IP 位址，然後選取 **Skip authentication**（跳過驗證）。

   您可以使用 **Skip authentication**（跳過驗證）搭配 **Source IP based visibility and enforcement**（來源 **IP** 型可視性和強制執行），來跳過無法驗證的無頭系統的驗證、設定安全性政策，以及獲得 Prisma Access 明確 Proxy 上流量的可視性。

   您可以新增 *IP* 位址或子網路。在擴展子網路之後，最多支援 *100,000* 個 *IP* 位址。




6. 前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Remote Networks**（遠端網路）。
7. **Push Config**（推送設定），確保在 **Push**（推送）範圍中，選取 **Mobile Users**—**Remote Workforce**（行動使用者—遠端勞動力）和 **Remote Networks**（遠端網路）。
8. 前往遠端網路設定中的 **Advanced Settings**（進階設定），並尋找用來將流量轉送至明確 Proxy 的 Anycast IP 位址。



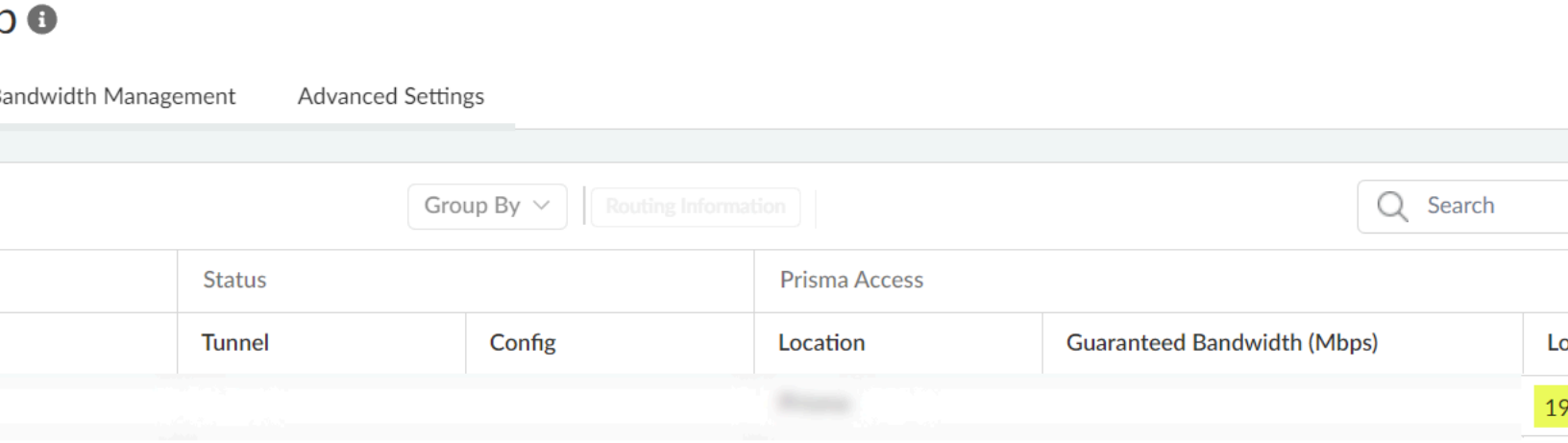

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** （選用）尋找用於明確 Proxy/遠端網路部署的單點傳送位址。

僅在您想要將特定遠端網路設為目標，以將流量轉送至明確 Proxy 時，才會使用 PAC 檔案中的單點傳送 IP 位址。如果您想要使用所有部署的遠端網路，將流量轉送至明確 Proxy，請使用 Anycast 位址。

1. 前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Remote Networks**（遠端網路）。
2. 記下 **Loopback IP**（回送 **IP**）位址。

   如果您有 IPv4 和 IPv6 位址，請記下 IPv4 位址。




## 遠端網路上的 Proxy 模式 (Panorama)

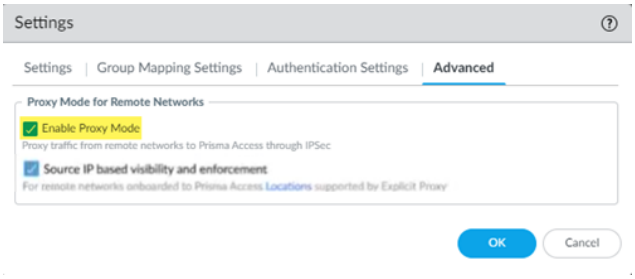
若要在 Prisma Access (Managed by Panorama) Access 中使用明確 Proxy 保護遠端網路中的使用者，請完成下列步驟。

**STEP 1 |** 設定您的明確 Proxy 部署，並裝載您要新增的明確 Proxy 位置。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 擷取您用於明確 Proxy/遠端網路部署的 Anycast IP 位址。

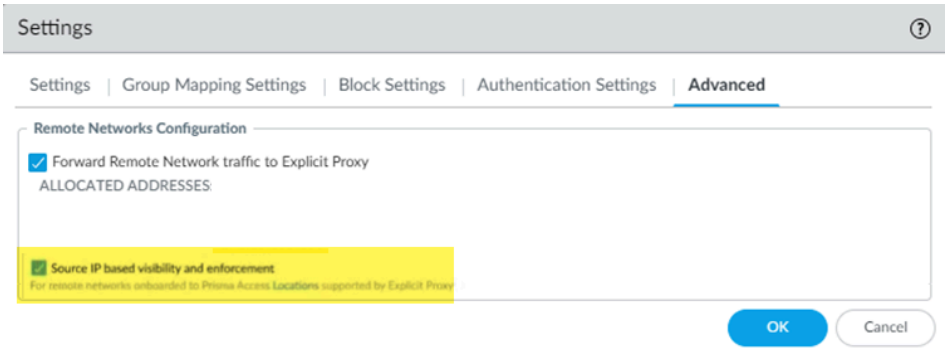
1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users—Explicit Proxy**（行動使用者—明確 **Proxy**）。
2. 選取齒輪圖示以編輯 **Settings**（設定）。
3. 選取 **Enable Proxy Mode**（啟用 **Proxy** 模式）。




4. 若要利用分支位置中將流量轉送到明確 Proxy 的系統私人 IP 位址，請選取 **Source IP based visibility and enforcement**（來源 **IP** 型可視性和強制執行）。

   此功能具有以下需求：

   - 至少為 10.2.4 的 Prisma Access 資料平面
   - 雲端服務外掛程式至少為 4.1 的 Prisma Access (Managed by Panorama) 部署
   - 您必須僅使用明確 Proxy 支援的遠端網路位置。




5. 新增一個政策，以允許遠端網路上繫結至 Anycast 和單點傳送 IP 的流量。如果您已啟用 **Source IP visibility and enforcement**（來源 **IP** 可視性和強制執行），請在明確 Proxy 中

 ©2025 Palo Alto Networks, Inc.

使用安全性政策中的 **Source IP**（來源 **IP**）欄位來保護流量。您需要遠端網路中的額外政策。

6. （選用）在 **Authentication Settings**（驗證設定）下，輸入其中未解密的 HTTP 或 HTTP 跨來源資源共用 (CORS) 流量應被允許流向 **Trusted Source Address Auth Bypass**（受信任的來源位址驗證略過）的任何 IP 位址。

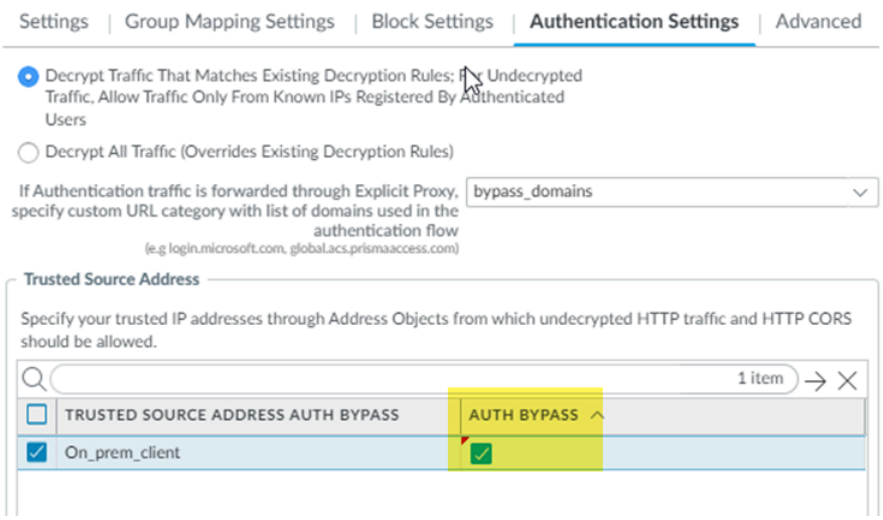
   將 IP 位址新增至 IP 位址型位址物件，並在欄位中 **Add**（新增）位址物件。

   最多可輸入 100,000 個位址。確保位址物件僅使用 IP 位址。

7. （選用）若要略過您輸入的任何受信任來源位址的驗證，請選取 **Auth Bypass**（驗證略過）。

   您可以使用 **Auth Bypass**（驗證略過）搭配 **Source IP based visibility and enforcement**（來源 **IP** 型可視性和強制執行），來跳過無法驗證的無頭系統的驗證、設定安全性政策，以及獲得 Prisma Access 明確 Proxy 上流量的可視性。

   您可以新增 *IP* 位址或子網路。在擴展子網路之後，最多支援 *100,000* 個 *IP* 位址。




8. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路）。
9. 如果您還沒有這樣做，請裝載您的遠端網路位置。

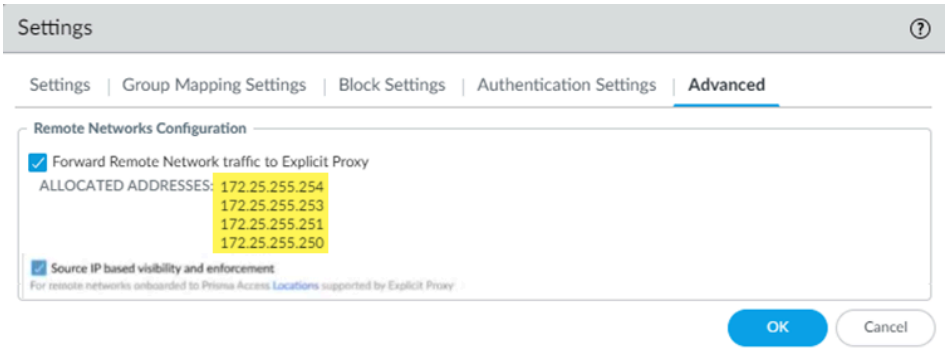
   您必須在明確 Proxy 支援的位置中啟用 *Prisma Access* 遠端網路。

10. 按一下 **Commit**（提交） > **Commit and Push**（提交並推送）。
11. **Edit Selections**（編輯選取項目），並在 **Prisma Access** 頁籤中，確保在 **Push Scope**（推送範圍）中選取了 **Prisma Access for networks**，然後按一下 **OK**（確定）。
12. **Commit and Push**（提交並推送）您的變更。

    您必須對遠端網路執行提交並推送，使 Prisma Access 可以擷取明確 Proxy/遠端網路部署中使用的 IP 位址。


©2025 Palo Alto Networks, Inc.

13. 返回明確 Proxy **Settings**（設定）（**Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users**—**Explicit Proxy**（行動使用者—明確 **Proxy**） > **Settings**（設定） > **Advanced**（進階）），並記下 **Remote Networks Configuration**（遠端網路設定）下顯示的 **ALLOCATED ADDRESSES**（已配置位址）。



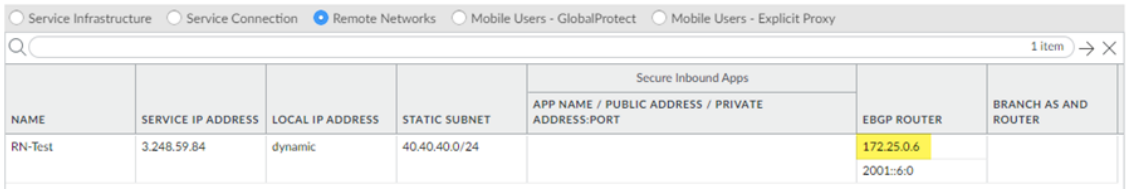

**STEP 3 |** （選用）尋找您用於明確 Proxy/遠端網路部署的單點傳送位址。

僅在您想要將特定遠端網路設為目標，以將流量轉送至明確 Proxy 時，才會使用 PAC 檔案中的單點傳送 IP 位址。如果您想要使用所有部署的遠端網路，將流量轉送至明確 Proxy，請使用 Anycast 位址。

1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Remote Networks**（遠端網路）。
2. 記下 **EBGP Router**（**EBGP** 路由器）位址。

   如果您有 IPv4 和 IPv6 位址，請記下 IPv4 位址。

   此位址也稱為回送位址。如果您已進行設定變更，變更了 *EBGP* 路由器位址，則可以使用 *Prisma Access* 舊版 API 擷取回送 *IP* 位址。




**STEP 4 |** 確保網路中的 CPE 已正確設定，使端點可以透過 Anycast 和單點傳送 IP 位址將流量轉送至明確 Proxy。

## 明確 Proxy 如何識別使用者

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | Prisma Access 授權 |


©2025 Palo Alto Networks, Inc.

明確 Proxy 會識別流量日誌中的使用者，取決於使用者使用 Proxy 進行驗證的方式，如下表所示。

| 驗證類型 | 流量日誌中的使用者識別 |
| --- | --- |
| 使用 SAML 驗證和解密登入的使用者 | 使用者名稱。 |
| 從使用 X-Authenticated-User (XAU) 標頭的另一個 Proxy 登入的使用者 | XAU 標頭資訊。<br>明確 Proxy 僅允許來自特定 IP 位址的流量使用 XAU 進行驗證。您可以建立位址物件，並指定允許 XAU 進行驗證的 IP 位址；然後，在明確 Proxy 設定期間於 **Trusted Source Address**（受信任來源位位）欄位中新增位址物件。 |
| 已驗證的跨來源資源共用 (CORS) 要求 | `swg-authenticated-ip-user` 使用者。<br>一些流量來自已驗證的使用者，這些使用者的瀏覽器無法傳送 Cookie 或執行驗證重新導向，例如 CORS 要求。在如此情況下，明確 Proxy 會將 `swg-authenticated-ip-use` 新增到流量日誌。 |
| 未解密的流量（如果您已允許明確 Proxy 允許來自使用者先前已驗證的 IP 位址的未解密流量） | `swg-authenticated-ip-user` 使用者。<br>您可以指定明確 Proxy，以允許來自使用者已驗證的 IP 位址的未解密流量；若要這樣做，請在設定明確 Proxy 時指定 **Decrypt traffic that matches existing decryption rules; for undecrypted traffic, allow traffic only from known IPs registered by authenticated users**（解密與現有解密規則相符的流量；對於未解密的流量，僅允許來自已驗證用戶註冊的已知 **IP** 的流量）。在這些設定中，明確 Proxy 會將 `swg-authenticated-ip-user` 新增到流量日誌。 |
| 您已選擇略過驗證的網域流量 | *swg-known-auth-bypass* 使用者。<br>當您設定明確 Proxy，您可以選擇從特定網域略過驗證。來自這些網域的流量，其使用者名稱會在日誌中顯示為 *swg-known-auth-bypass*。 |

## 明確 Proxy 轉送設定檔

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 行動使用者授權 |


©2025 Palo Alto Networks, Inc.

明確 Proxy 轉送設定檔可讓您使用多個 PAC 檔案，定義要轉送到 Prisma Access 的流量。轉送設定檔還可讓您選擇建立易於使用的轉送規則，而不是處理編寫和維護 PAC 檔案的複雜性。

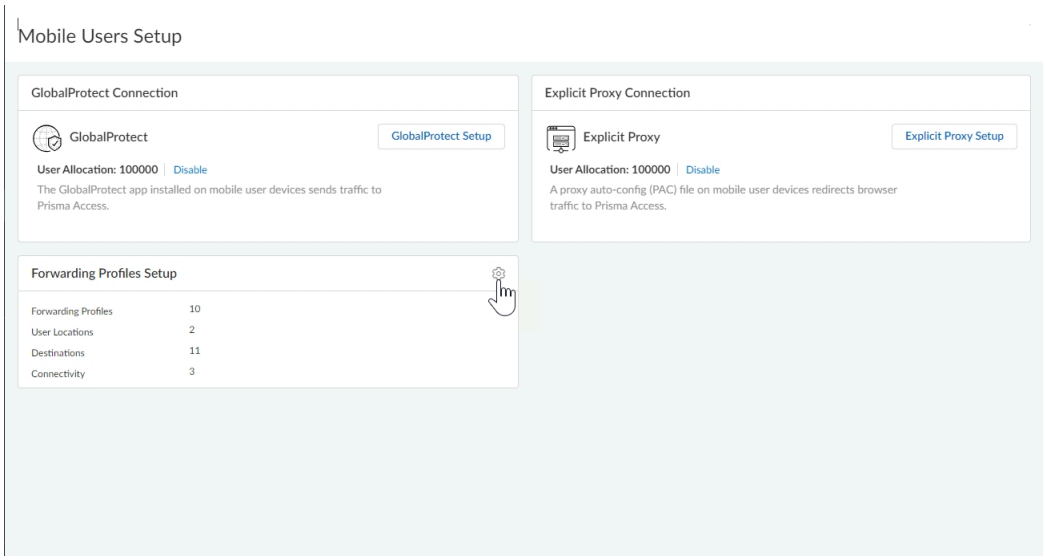
- 使用轉送設定檔定義多個 PAC 檔案
- 使用轉送規則定義哪個流量要轉送至明確 Proxy
- 將轉送設定檔附加到 GlobalProtect 應用程式設定

## 使用轉送設定檔定義多個 PAC 檔案

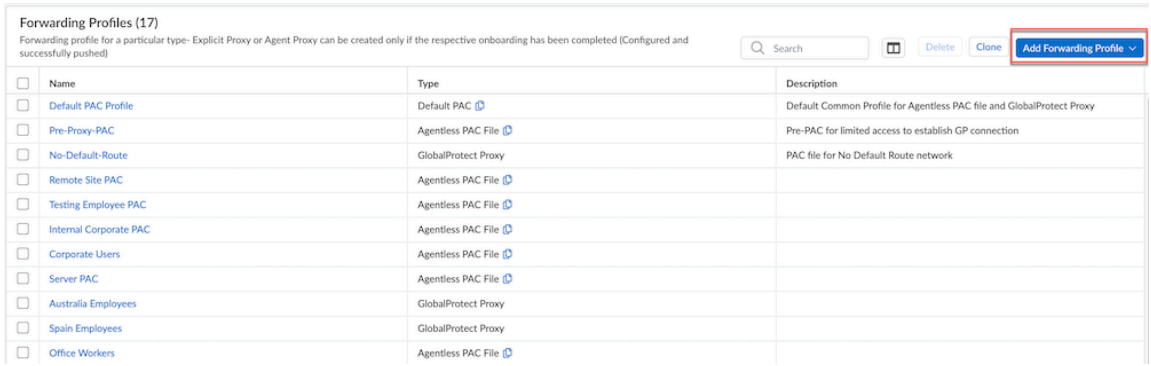
轉送設定檔可讓您在部署中同時使用多個 PAC 檔案，以便您可以定義要轉送至 Prisma Access 的流量。

**STEP 1 |** 建立一個轉送設定檔。

1. 從 Strata Cloud Manager 中，選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Mobile Users**（行動使用者） > **Forwarding Profiles Setup**（轉送設定檔設定）。




2. **Add Forwarding Profile**（新增轉送設定檔）。



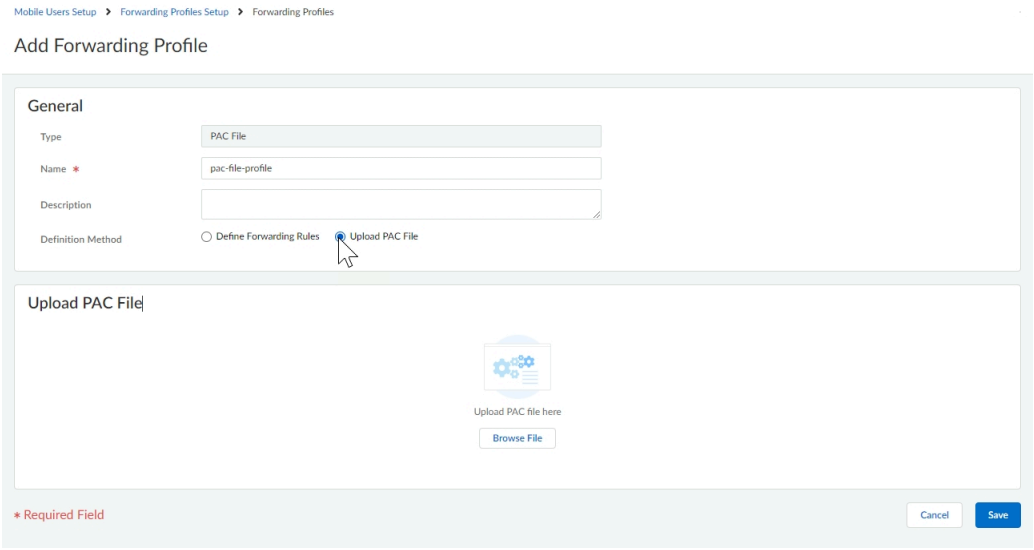

**STEP 2 |** 選取 **PAC File**（**PAC** 檔案）。

**PAC File**（**PAC** 檔案）適用於 Prisma Access 明確 Proxy。**GlobalProtect Proxy** 適用於在 Proxy 模式下使用 GlobalProtect。

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 上傳 PAC 檔案。

1. 選擇 **Upload PAC File**（上傳 **PAC** 檔案）以上傳現有 PAC 檔案，或使用 PAC 檔案指導方針建立 PAC 檔案。




2. **Browse file**（瀏覽檔案）以瀏覽檔案系統取得 PAC 檔案。
3. **Save**（儲存）設定檔。

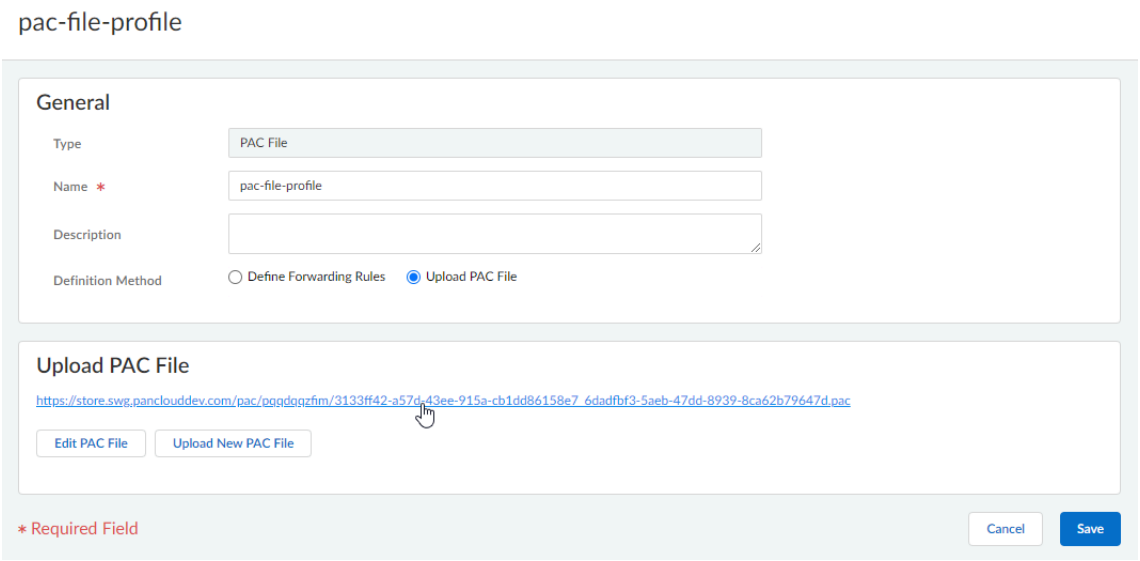
**STEP 4 |** 重複前面的兩個步驟以使用不同的 PAC 檔案建立另一個轉送設定檔。

現在，這兩個 PAC 檔案同時在您的部署中操作。

**STEP 5 |** 擷取 PAC 檔案 URL。

1. 返回您已將 PAC 檔案上傳至其中的設定檔。

   您應該會看到託管 PAC 檔案的 URL。





©2025 Palo Alto Networks, Inc.

**STEP 6 |** （選用）編輯 PAC 檔案。

若要快速變更 PAC 檔案，您可以直接在網頁介面內進行編輯

1. 從轉送設定檔內，**Edit PAC File**（編輯 **PAC** 檔案）。
2. 進行變更並 **Save**（儲存）。



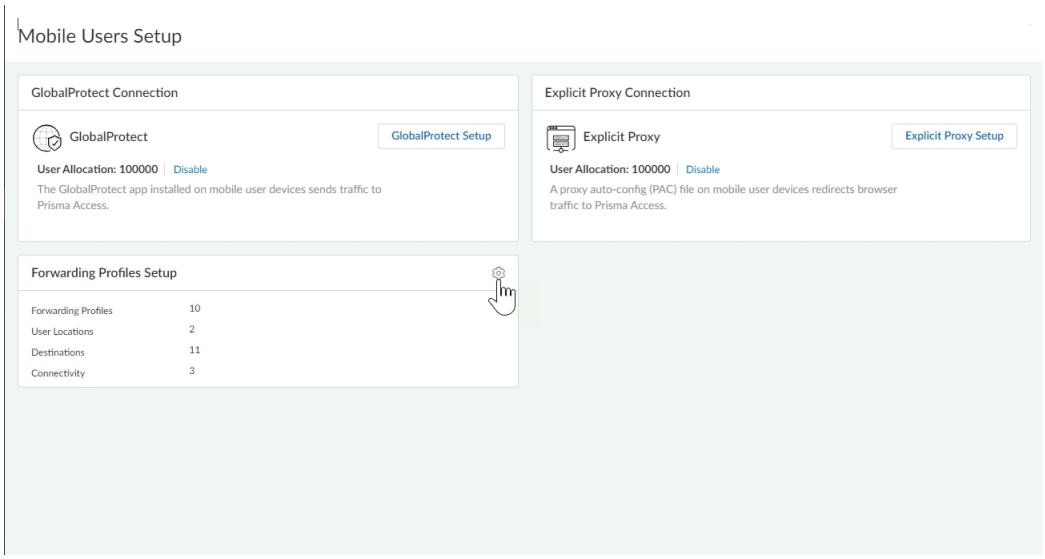

## 使用轉送規則定義哪個流量要轉送至明確 Proxy

您可以建立簡單的轉送規則來產生 PAC 檔案，而不是從頭開始編寫自己的 PAC 檔案。

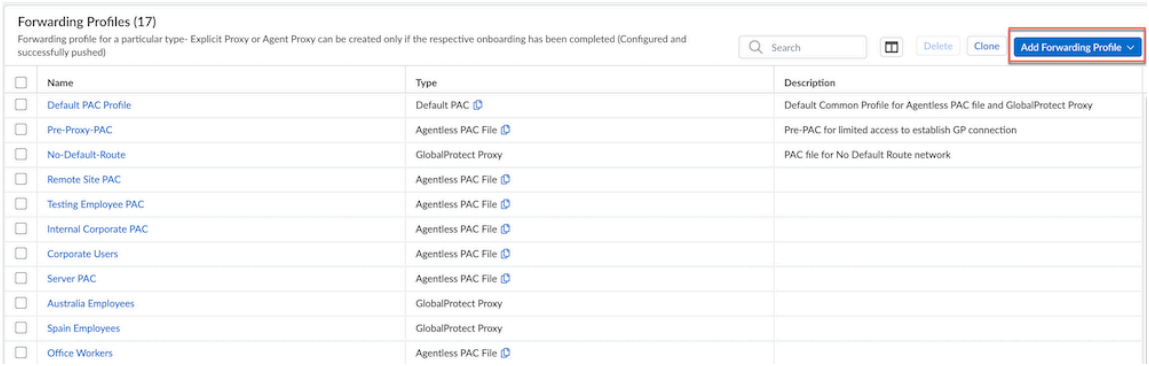

©2025 Palo Alto Networks, Inc.

**STEP 1 |** 建立一個轉送設定檔。

1. 從 Strata Cloud Manager 中，選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Mobile Users**（行動使用者） > **Forwarding Profiles Setup**（轉送設定檔設定）。




2. **Add Forwarding Profile**（新增轉送設定檔）。



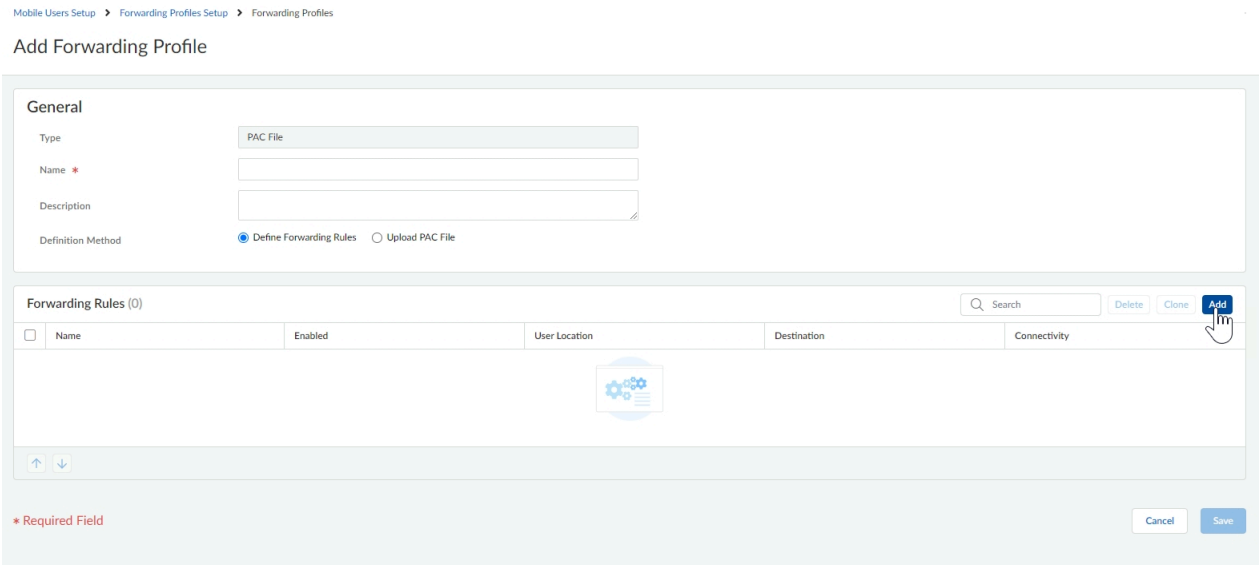

**STEP 2 |** 選取 **PAC File**（**PAC** 檔案）。

**PAC File**（**PAC** 檔案）適用於 Prisma Access 明確 Proxy。**GlobalProtect Proxy** 適用於在 Proxy 模式下使用 GlobalProtect。

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 新增轉送規則。

1. 選取新增。




2. 完成必要欄位：

| | |
|---|---|
| 名稱 | 設定檔的名稱。 |
| 使用者位置 | 您要為其建立轉送規則的使用者位置。您可以從 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Mobile Users**（行動使用者） > **Forwarding Profiles Setup**（轉送設定檔設定） > **User Locations**（使用者位置行動使用者）建立自訂位置。<br><br>根據 *IP* 位址設定自訂使用者位置時，您無法使用萬用字元。 |
| 目的地 | Web 流量的目的地。您可以從預先定義的目的地中進行選取，也可以從 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Mobile Users**（行動使用者） > **Forwarding Profiles Setup**（轉送設定檔設定） > **Destinations**（目的地）建立自訂目的地。 |
| 連線 | **Direct**（直接）導致流量略過過 Proxy。<br><br>**Global Proxy** 使流量通過 Proxy。 |

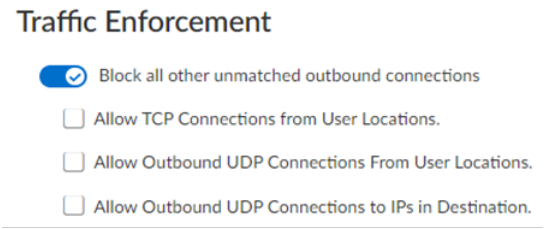
3. 完成後選取 **Add**（新增）。


©2025 Palo Alto Networks, Inc.

4. 如果想要封鎖所有不符合轉送規則的輸出流量（例如 UDP），請啟用 **Traffic Enforcement**（流量強制執行）。此選項需要 GlobalProtect 代理程式 6.3.1 版，且預設為停用。如果您有需要您允許 UDP 連線的應用程式，則可以使用使用者位置或目的地物件新增這些例外。

   您可以自訂封鎖動作，如下所示：

   - 封鎖來自端點的所有 UDP 輸出連線。
   - 允許來自特定位置的 TCP。例如，您可以允許來自辦公室的所有 TCP 流量。
   - 允許來自特定位置的 UDP。例如，您可以允許來自辦公室的所有 TCP 流量。
   - 如果某些應用程式需要 UDP 連線，您可以允許輸出 UDP 連線到特定目的地。

5. 使用您建立的轉送規則 **Save**（儲存）設定檔。

   該設定檔會出現在您的轉送設定檔清單中。當您開啟它時，您將看到根據規則所產生的 PAC 檔案的 URL。**View PAC file**（檢視 **PAC** 檔案）以查看其內容。

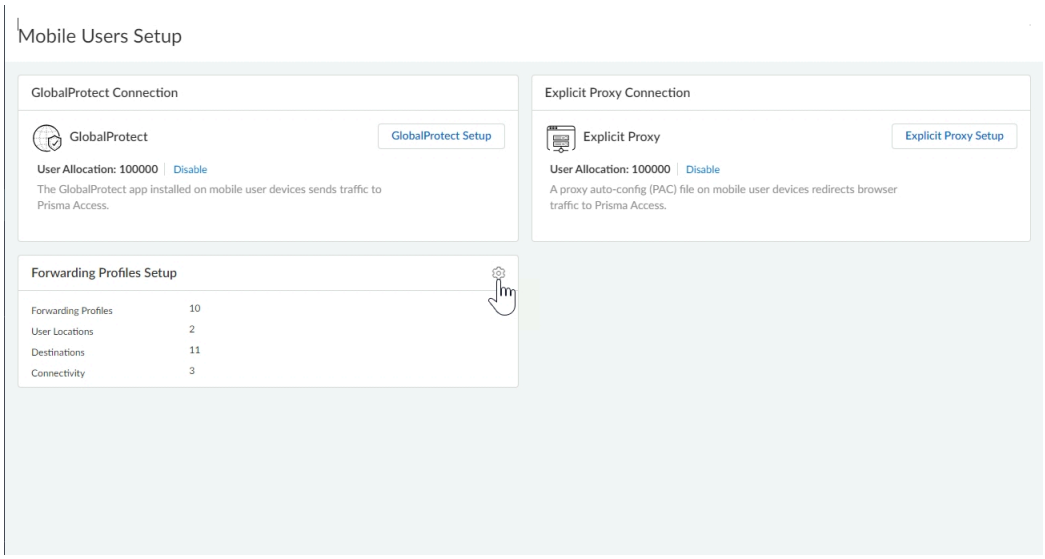
## 將轉送設定檔附加到 GlobalProtect 應用程式設定

您可以使用轉送設定檔，簡化 GlobalProtect 應用程式 Proxy 的設定。

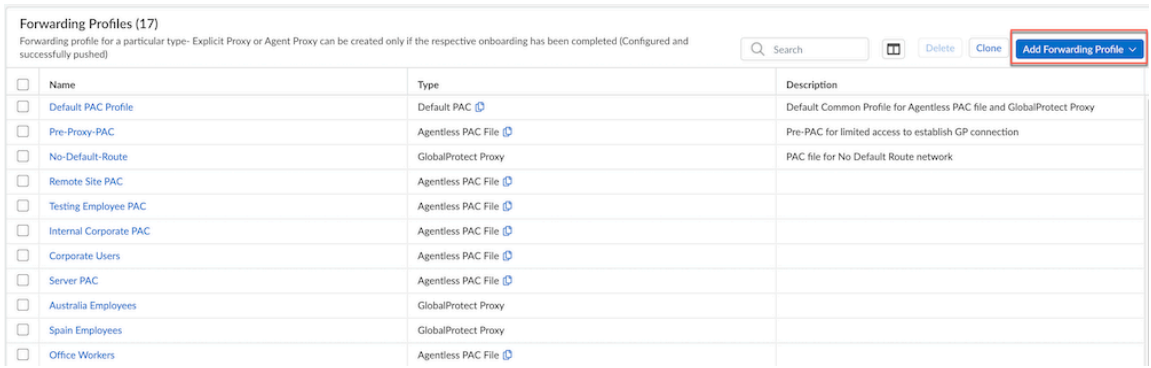
 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** 建立一個轉送設定檔。

1. 從 Strata Cloud Manager 中，選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Mobile Users**（行動使用者） > **Forwarding Profiles Setup**（轉送設定檔設定）。




2. **Add Forwarding Profile**（新增轉送設定檔）。



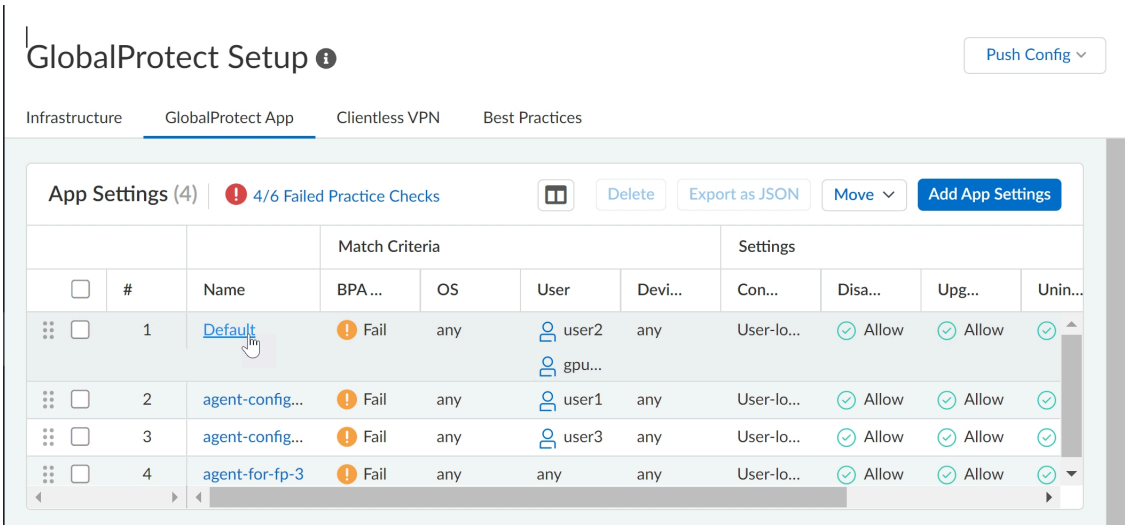

**STEP 2 |** 選取 **GlobalProtect Proxy**。

**STEP 3 |** 透過上傳 PAC 檔案或建立轉送規則來設定轉送設定檔。

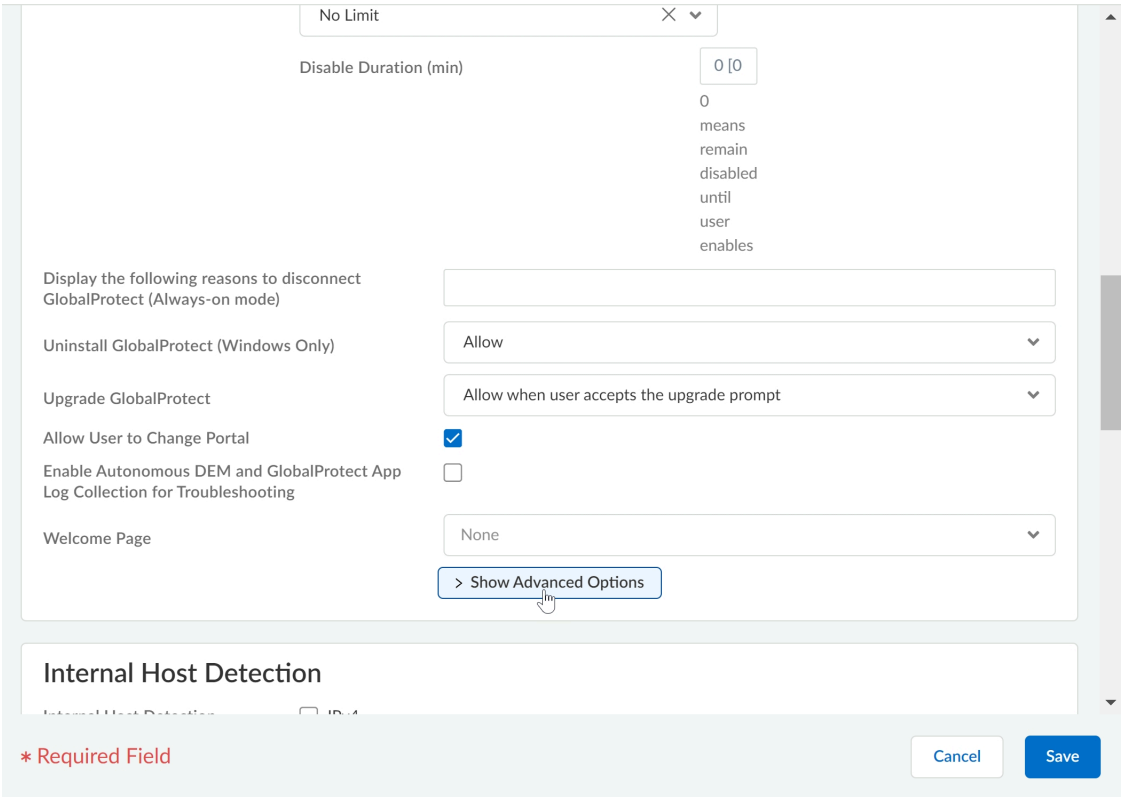
 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 將轉送設定檔新增至您的 GlobalProtect app Proxy 設定。

1. 選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **GlobalProtect** > **GlobalProtect App**（**GlobalProtect** 應用程式）。
2. 選取設定檔案。




3. 在應用程式設定下，**Show Advanced Options**（顯示進階選項）。

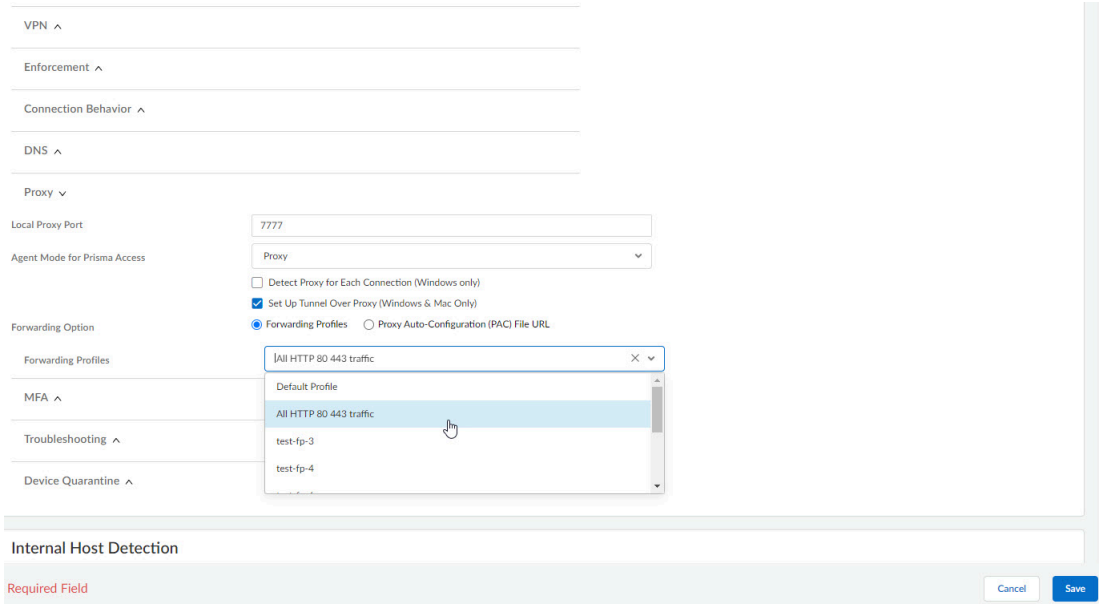



4. 展開 **Proxy** 設定。
5. 選取 **Proxy** 或 **Tunnel and Proxy**（通道和 **Proxy**），取決於您的 GlobalProtect 代理程式模式

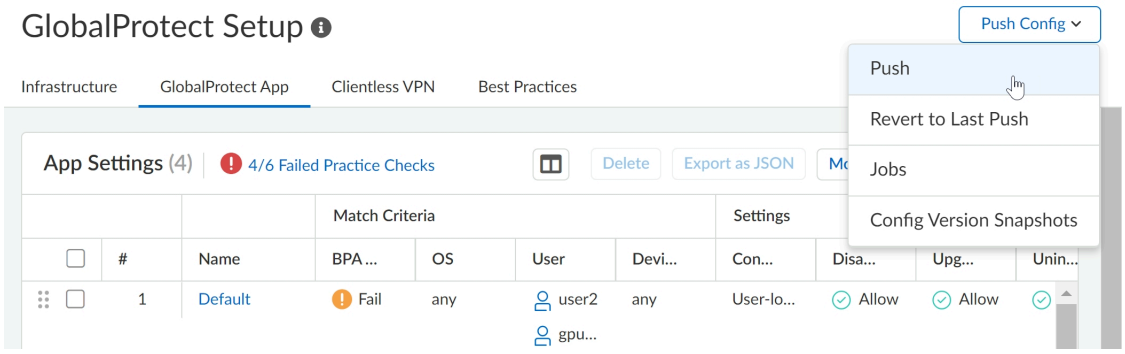
 ©2025 Palo Alto Networks, Inc.

如果選取 ***Tunnel***（通道）模式，則無法新增轉送設定檔。

6. 選取 **Forwarding Profiles**（轉送設定檔），並選擇您要使用的轉送設定檔。




7. **Save**（儲存）變更。
8. 選取 **Push Config**（推送設定） > **Push**（推送）。




# PAC 檔案指導方針

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

- Strata Cloud Manager
- Panorama


©2025 Palo Alto Networks, Inc.

## PAC 檔案指導方針 (Strata Cloud Manager)

設定 PAC 檔案與明確 Proxy 搭配使用時，請遵循下列指導方針和需求：

- 請注意，如果您在 Proxy 模式下使用 GlobalProtect 代理程式，此代理程式會將 PAC 檔案散佈至您的主機。此代理程式會透過 HTTPS 存取 PAC 檔案。PAC 檔案是公用的。
- PAC 檔案會將使用者流量導向到明確 Proxy。
- 您只能託管一個 PAC 檔案，與 Prisma Access 搭配使用，而明確 Proxy PAC 檔案託管於美國。如果您需要在美國以外進行替代 PAC 檔案存取，您可以在您企業中託管 PAC 檔案。
- 若要存取 PAC 檔案，請確定您的端點可以連線下列 IP 位址：
  - 34.111.7.85
  - 34.160.172.204
  - 34.110.206.116
  - 34.95.107.244
  - 34.149.8.36

  如果您沒有無預設路由網路，則必須為這些 *IP* 位址新增路由，才能存取 *PAC* 檔案。
- PAC 檔案僅支援 ASCII 文字格式。Palo Alto Networks 建議您在 VI 或 Vim 等文字編輯器中建立並儲存 PAC 檔案。
- 在建立明確 Proxy 設定，且提交並推送您的變更之後，請上傳 PAC 檔案，或在 PAC 檔案編輯器中指定 PAC 設定。
- 您必須在 `return"PROXY foo.proxy.prismaaccess.com:8080";` 陳述式中有至少一個明確 Proxy URL，流量才能開始進入 Prisma Access。使用您推送變更時使用的所設定網域，或使用有效的 IPv4 位址或 DIRECT 關鍵字，例如 `PROXY paloaltonetworks-245139.proxy.prismaaccess.com:8080` or `PROXY 1.2.3.4:8080` 等。
- 如果未略過 Proxy，則您必須提供 PROXY 關鍵字。如果沒有設定 `DIRECT` 關鍵字以略過 Proxy，則需要有效的 Proxy 陳述式。
- 如果在無效的 PROXY 陳述式之前找到有效的 PROXY 陳述式，則明確 Proxy 將跳過第一個之後所有 PROXY 陳述式上的有效性檢查。例如，包含有效陳述式 `PROXY paloaltonetworks-245139.proxy.prismaaccess.com:8080`（後面跟著無效的陳述式 `PROXY foo.proxy.prismaacess.com:8080`）的 PAC 檔案將被視為有效，因為明確 Proxy 會跳過 `foo.proxy.prismaacess.com:8080` 的有效性檢查。
- 如果您使用 PROXY 陳述式，讓 ACS 流量略過 Prisma Access Proxy，則 PROXY 陳述式不應使用明確 Proxy URL。在此設定中，明確 Proxy 會提供錯誤訊息，但允許您上傳 PAC 檔案。您可以使用有效的 FQDN 或 IPv4 位址，將 ACS 流量導向至其他 Proxy，或使用 `DIRECT` 關鍵字直接導向到網際網路。
- PROXY 陳述式中僅支援 IPv4 位址。請不要在 PROXY 陳述式中使用 IPv6 位址。
- PAC 檔案的檔案大小上限為 750 KB。
- 如果 ACS/Idp 流量需要通過明確 Proxy，則將這些網域新增到驗證略過清單和無解密政策規則。


©2025 Palo Alto Networks, Inc.

- 如果您在預設路由環境中設定明確 Proxy，則必須排除入口網站、閘道和 SAML FQDNS。您可以使用 PAC 檔案略過 FQDNS。
- 您無法在上傳 PAC 檔案之後將其刪除。不過，您可以上傳新的 PAC 檔案，或在 PAC 檔案編輯器中進行編輯，以覆寫現有的 PAC 檔案。

明確 Proxy 為您提供一個範例 PAC 檔案，您可以加以修改並將其用作明確 Proxy 部署的 PAC 檔案。Prisma Access 提供的範例 PAC 檔案包含下列資料：

```
function FindProxyForURL(url, host) { /* Bypass localhost and Private
 IPs */ var resolved_ip = dnsResolve(host); if (isPlainHostName(host)
 || shExpMatch(host, "*.local") || isInNet(resolved_ip, "10.0.0.0",
 "255.0.0.0") || isInNet(resolved_ip, "172.16.0.0", "255.240.0.0")
 || isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") ||
 isInNet(resolved_ip, "127.0.0.0", "255.255.255.0")) return
 "DIRECT"; /* Bypass FTP */ if (url.substring(0,4) == "ftp:")
 return "DIRECT"; /* Bypass SAML, e.g. Okta */ if (shExpMatch(host,
 "*.okta.com") || shExpMatch(host, "*.oktacdn.com"))
 return "DIRECT"; /* Bypass ACS */ if (shExpMatch(host,
 "*.acs.prismaaccess.com")) return "DIRECT"; /* Forward to Prisma
 Access */ return "PROXY foo.proxy.prismaaccess.com:8080";
```

如果想要使用 Prisma Access 提供的預設 PAC 檔案，您可以選擇性地修改 PAC 檔案中的欄位，如下表所述。

| 文字 | 說明 |
|---|---|
| `var resolved_ip = dnsResolve(host); ... return "DIRECT";` | 如果您未修改此檔案中的資料，下列主機名稱和 IP 位址會略過明確 Proxy：<br>• `if (isPlainHostName(host)`—對於沒有包含點的主機名稱（例如，http://intranet），略過明確 Proxy 。<br>• `shExpMatch(host, "*.local") ||`—對於內部網路中託管的任何主機名稱 (localhost)，略過 Proxy。<br>• `isInNet(resolved_ip, "10.0.0.0", "255.0.0.0") || isInNet(resolved_ip, "172.16.0.0", "255.240.0.0") || isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") || isInNet(resolved_ip, "127.0.0.0", "255.255.255.0"))`—對於位於私人或回送 IP 位址範圍的任何 IP 位址，略過 明確 Proxy。 |
| `if (url.substring(0,4) == "ftp:") return "DIRECT";` | 略過 FTP 工作階段的明確 Proxy。 |

 ©2025 Palo Alto Networks, Inc.

| 文字 | 說明 |
| --- | --- |
| `if (shExpMatch(host, "*.okta.com") \|\| shExpMatch(host, "*.oktacdn.com")) return "DIRECT";` | 略過 SAML IdP 的明確 Proxy。請務必新增 IdP 所使用的所有 FQDN。<br>如果您使用 Okta 作為用於 SAML 驗證的 IdP，請輸入 **`*.okta.com`** 和 **`*.oktacdn.com`**。 |
| `if (shExpMatch(host, "*.acs.prismaaccess.com")) return "DIRECT";` | 略過 Prisma Access 驗證快取服務 (ACS) 的明確 Proxy。<br>您可以為部署新增特定的 **ACS FQDN**，而不是使用萬用字元。在 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Mobile Users—Explicit Proxy**（行動使用者—明確 **Proxy**） > **ACS FQDN**。 |
| `return "PROXY foo.proxy.prismaaccess.com:8080"` | 略過明確 Proxy URL 的明確 Proxy。<br>您必須在 `return"PROXY foo.proxy.prismaaccess.com:8080";` 陳述式中有至少一個明確 Proxy URL，流量才能進入 Prisma Access。使用您推送變更時使用的所設定網域，或使用有效的 IPv4 位址或 DIRECT 關鍵字，例如 PROXY `paloaltonetworks-245139.proxy.prismaaccess.c` 或 PROXY `1.2.3.4:8080`。 |

## PAC 檔案指導方針 (Panorama)

設定 PAC 檔案與明確 Proxy 搭配使用時，請遵循下列指導方針和需求：

- 請注意，如果您在 Proxy 模式下使用 GlobalProtect 代理程式，此代理程式會將 PAC 檔案散佈至您的主機。此代理程式會透過 HTTPS 存取 PAC 檔案。PAC 檔案是公用的。
- PAC 檔案會將使用者流量導向到明確 Proxy。
- 您只能託管一個 PAC 檔案，與 Prisma Access 搭配使用，而明確 Proxy PAC 檔案託管於美國。如果您需要在美國以外進行替代 PAC 檔案存取，您可以在您企業中託管 PAC 檔案。
- 若要存取 PAC 檔案，請確定您的端點可以連線下列 IP 位址：
  - 34.111.7.85
  - 34.160.172.204
  - 34.110.206.116
  - 34.95.107.244
  - 34.149.8.36


©2025 Palo Alto Networks, Inc.

- PAC 檔案僅支援 ASCII 文字格式。Palo Alto Networks 建議您在 VI 或 Vim 等文字編輯器中建立並儲存 PAC 檔案。
- 在建立明確 Proxy 設定，且提交並推送您的變更之後，上傳 PAC 檔案。在上傳 PAC 檔案之後，不需要提交並推送操作。
- 您必須在 `return"PROXY foo.proxy.prismaaccess.com:8080";` 陳述式中有至少一個明確 Proxy URL，流量才能開始進入 Prisma Access。使用您推送變更時使用的所設定網域，或使用有效的 IPv4 位址或 DIRECT 關鍵字，例如 `PROXY paloaltonetworks-245139.proxy.prismaaccess.com:8080` or `PROXY 1.2.3.4:8080` 等。
- 如果未略過 Proxy，則您必須提供 PROXY 關鍵字。如果沒有設定 `DIRECT` 關鍵字以略過 Proxy，則需要有效的 Proxy 陳述式。
- 如果在無效的 PROXY 陳述式之前找到有效的 PROXY 陳述式，則明確 Proxy 將跳過第一個之後所有 PROXY 陳述式上的有效性檢查。例如，包含有效陳述式 `PROXY paloaltonetworks-245139.proxy.prismaaccess.com:8080`（後面跟著無效的陳述式 `PROXY foo.proxy.prismaacess.com:8080`）的 PAC 檔案將被視為有效，因為明確 Proxy 會跳過 `foo.proxy.prismaacess.com:8080` 的有效性檢查。
- 如果您使用 PROXY 陳述式，讓 ACS 流量略過 Prisma Access Proxy，則 PROXY 陳述式不應使用明確 Proxy URL。在此設定中，明確 Proxy 會提供錯誤訊息，但允許您上傳 PAC 檔案。您可以使用有效的 FQDN 或 IPv4 位址，將 ACS 流量導向至其他 Proxy，或使用 `DIRECT` 關鍵字直接導向到網際網路。
- PROXY 陳述式中僅支援 IPv4 位址。請不要在 PROXY 陳述式中使用 IPv6 位址。
- PAC 檔案的檔案大小上限為 256 KB。
- 如果 ACS/Idp 流量需要通過明確 Proxy，則將這些網域新增到驗證略過清單和無解密政策規則。
- 如果您在預設路由環境中設定明確 Proxy，則必須排除入口網站、閘道和 SAML FQDNS。您可以使用 PAC 檔案略過 FQDNS。
- 您無法在上傳 PAC 檔案之後將其刪除。不過，您可以上傳新的 PAC 檔案，以覆寫現有的 PAC 檔案。
- 如果您變更 Prisma Access 中的明確 Proxy URL，但未變更 PAC 檔案來反映此變更，則不會套用此變更。您必須上傳一個指定新明確 Proxy URL 的新 PAC 檔案。

明確 Proxy 為您提供一個範例 PAC 檔案，您可以加以修改並將其用作明確 Proxy 部署的 PAC 檔案。Prisma Access 提供的範例 PAC 檔案包含下列資料：

```
function FindProxyForURL(url, host) { /* Bypass localhost and Private
 IPs */ var resolved_ip = dnsResolve(host); if (isPlainHostName(host)
 || shExpMatch(host, "*.local") || isInNet(resolved_ip, "10.0.0.0",
 "255.0.0.0") || isInNet(resolved_ip, "172.16.0.0", "255.240.0.0")
 || isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") ||
 isInNet(resolved_ip, "127.0.0.0", "255.255.255.0")) return
 "DIRECT"; /* Bypass FTP */ if (url.substring(0,4) == "ftp:")
 return "DIRECT"; /* Bypass SAML, e.g. Okta */ if (shExpMatch(host,
 "*.okta.com") || shExpMatch(host, "*.oktacdn.com"))
 return "DIRECT"; /* Bypass ACS */ if (shExpMatch(host,
```

 ©2025 Palo Alto Networks, Inc.

```
"*.acs.prismaaccess.com")) return "DIRECT"; /* Forward to Prisma
Access */ return "PROXY foo.proxy.prismaaccess.com:8080";
```

如果想要使用 Prisma Access 提供的預設 PAC 檔案，您可以選擇性地修改 PAC 檔案中的欄位，如下表所述。

| 文字 | 說明 |
|---|---|
| `var resolved_ip = dnsResolve(host); ... return "DIRECT";` | 如果您未修改此檔案中的資料，下列主機名稱和 IP 位址會略過明確 Proxy：<br>• `if (isPlainHostName(host)`—對於沒有包含點的主機名稱（例如，http://intranet），略過明確 Proxy 。<br>• `shExpMatch(host, "*.local") ||`—對於內部網路中託管的任何主機名稱 (localhost)，略過 Proxy。<br>• `isInNet(resolved_ip, "10.0.0.0", "255.0.0.0") || isInNet(resolved_ip, "172.16.0.0", "255.240.0.0") || isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") || isInNet(resolved_ip, "127.0.0.0", "255.255.255.0"))`—對於位於私人或回送 IP 位址範圍的任何 IP 位址，略過 明確 Proxy。 |
| `if (url.substring(0,4) == "ftp:") return "DIRECT";` | 略過 FTP 工作階段的明確 Proxy。 |
| `if (shExpMatch(host, "*.okta.com") || shExpMatch(host, "*.oktacdn.com")) return "DIRECT";` | 略過 SAML IdP 的明確 Proxy。請務必新增 IdP 所使用的所有 FQDN。<br>如果您使用 Okta 作為用於 SAML 驗證的 IdP，請輸入 **`*.okta.com`** 和 **`*.oktacdn.com`**。 |
| `if (shExpMatch(host, "*.acs.prismaaccess.com")) return "DIRECT";` | 略過 Prisma Access 驗證快取服務 (ACS) 的明確 Proxy。<br>您可以為部署新增特定的 **ACS FQDN**，而不是使用萬用字元。在 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Mobile Users—Explicit Proxy**（行動使用者—明確 **Proxy**） > **ACS FQDN**。 |


©2025 Palo Alto Networks, Inc.

| 文字 | 說明 |
| --- | --- |
| `return "PROXY foo.proxy.prismaaccess.com:8080"` | 略過明確 Proxy URL 的明確 Proxy。<br>您必須在 `return"PROXY foo.proxy.prismaaccess.com:8080";` 陳述式中有至少一個明確 Proxy URL，流量才能進入 Prisma Access。使用您推送變更時使用的所設定網域，或使用有效的 IPv4 位址或 DIRECT 關鍵字，例如 PROXY `paloaltonetworks-245139.proxy.prismaaccess.c` 或 PROXY `1.2.3.4:8080`。 |

## 明確 Proxy 最佳做法

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

在實作明確 Proxy 部署時，請使用建議的最佳做法，以獲得最佳效能和理想的使用者體驗：

- 一般明確 **Proxy** 部署最佳做法：
  - 在至少兩個區域中部署明確 Proxy 進行備援。
  - 如果您的所有使用者都位於 NAT 裝置後面，並且如果明確 Proxy 將 NAT 裝置的 IP 位址視為來源 IP 位址，則您應該每 500 個行動使用者配置一個 NAT IP 位址。
  - 使用轉送設定檔來設定 PAC 檔案。
- **PAC** 檔案最佳做法—當時，略過所有 SAML、CIE 和驗證快取服務 (ACS) URL。
- **SAML** 驗證最佳做法：
  - 將 SAML 驗證 **Cookie Lifetime**（**Cookie** 存留時間） 設定為 24 小時，以獲得最佳使用者體驗，而無需中斷驗證。
  - 如果您已在代理模式下設定 GlobalProtect 或在通道和 Proxy 模式下設定 GlobalProtect，請將 GlobalProtect 入口網站上的**Cookie Lifetime**（**Cookie** 存留時間） 設定為 12 小時。
- **Kerberos** 驗證最佳做法—金鑰標籤檔案大小應小於 60 KB。
- 安全性政策規則最佳做法—使用安全性政策規則最佳做法，方法是將政策中的 **Action**（動作）設定為 **Deny**（拒絕），而不是 **Drop**（捨棄）或 **Reset**（重設）。此動作有助於在明確 Proxy 安全性處理節點 (EP-SPN) 中快速釋放資源，以取得最佳效能。
- 解密最佳作法—至少設定一個解密政策和一個解密憑證。
- **Ip** 來源位址最佳做法—若要將對明確 Proxy 的存取限制為特定來源 IP 位址，請使用特殊物件，其中包括位址物件、位址群組和外部動態清單 (EDL)。


©2025 Palo Alto Networks, Inc.

# 監控明確 Proxy 並針對其進行疑難排解

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

瞭解如何監控您的 Prisma Access 明確 Proxy 部署並針對其進行疑難排解。

- Strata Cloud Manager
- Panorama

## 監控明確 Proxy 並針對其進行疑難排解 (Strata Cloud Manager)

監控 Prisma Access 明確 Proxy 部署詳細資訊，以協助您針對任何問題進行疑難排解。

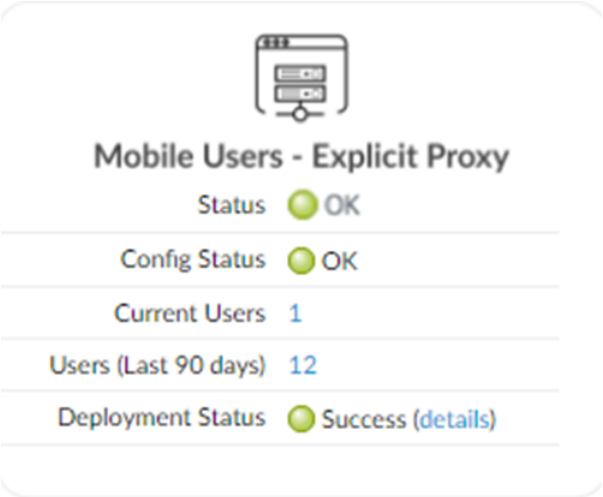
- 按一下 **Monitor**（監控） > **Users**（使用者），並選取 **Explicit Proxy**（明確 **Proxy**）連線方法。
- 選取 **Monitor**（監控） > **Users**（使用者），並選取連線方法作為 **Explicit Proxy**（明確 **Proxy**），以檢視在其裝置的 Web 瀏覽器上透過明確 Proxy 連線至 Prisma Access 安全性服務的行動使用者。
- 選取 **Monitor**（監控）> **Prisma Access Locations**（位置）> **Explicit Proxy Mobile Users**（明確 **Proxy** 行動使用者），為行動使用者查看您所有 Prisma Access 位置的健康情況概要。
- 檢查流量日誌（**Incidents & Alerts**（事件和警示）> **Log Viewer**（日誌檢視器），並選取日誌類型 **Traffic**（流量））和驗證日誌（**Incidents & Alerts**（事件和警示）> **Log Viewer**（日誌檢視器），並選取日誌類型 **Authentication**（驗證）），以針對驗證相關問題進行疑難排解。

## 監控明確 Proxy 並針對其進行疑難排解 (Panorama)

在您為行動使用者設定了明確 Proxy 之後，請透過檢查 Prisma Access 明確 Proxy 部署的狀態監控狀態，並針對任何問題進行疑難排解。


©2025 Palo Alto Networks, Inc.

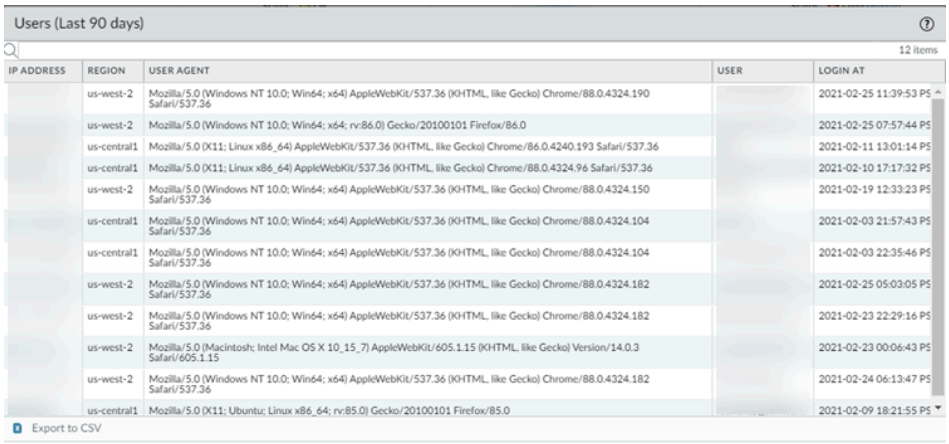
- 選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Status**（狀態），以查看明確 Proxy 狀態。




行動使用者 **Status**（狀態）和 **Config Status**（設定狀態）欄位指出 Prisma Access 與您行動使用者之間的連線 **OK**（成功）、無法擷取通道上的狀態（**Warning**（警告）），還是行動使用者無法連線到明確 Proxy（**Error**（錯誤））.

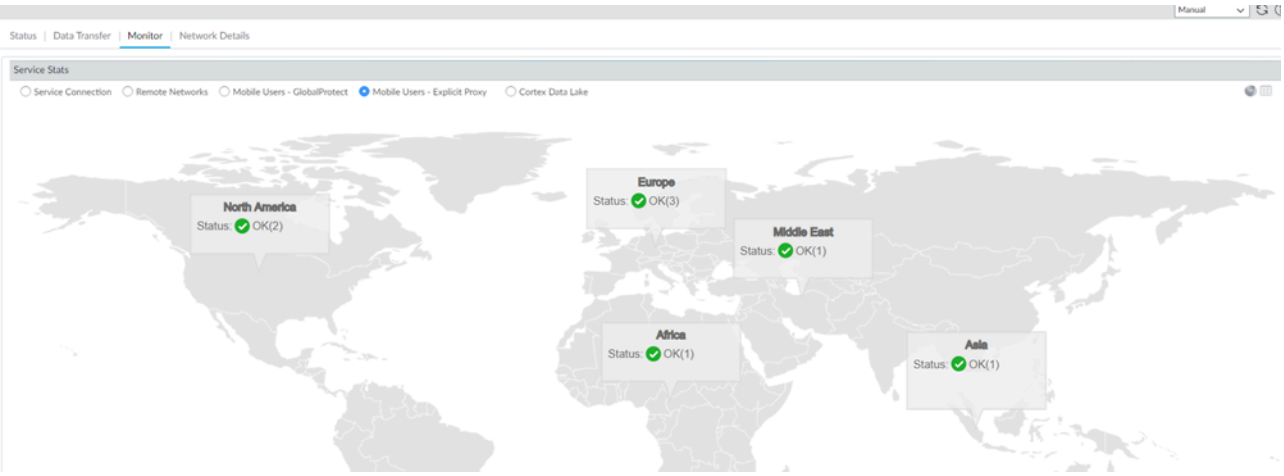
按一下 **Current Users**（目前使用者）和 **Users (Last 90 days)**（使用者（過去 **90** 天））旁邊的超連結，以取得行動使用者的詳細資訊。

- **Current Users**（目前使用者）—過去 5 分鐘內已瀏覽流量的已驗證使用者目前數目。
- **Users (Last 90 days)**（使用者（過去 **90** 天））—過去 90 天內唯一已驗證的明確 Proxy 使用者數目。

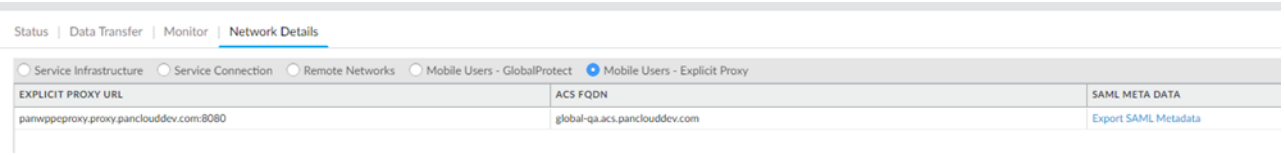



 ©2025 Palo Alto Networks, Inc.

- 選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Monitor**（監控） > **Mobile Users**—**Explicit Proxy**（行動使用者—明確 **Proxy**），以顯示一張地圖，其中顯示已部署的明確 Proxy 位置。




- 選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Mobile Users**—**Explicit Proxy**（行動使用者—明確 **Proxy**），以檢視以下詳細資訊：




  - **Explicit Proxy URL**（明確 **Proxy URL**）—用於明確 Proxy 的 URL。
  - **ACS FQDN**—ACS 的 FQDN。
  - **SAML Meta Data**（**SAML** 中繼資料）—SAML 使用的驗證設定檔中繼資料。您可以 **Export SAML Metadata**（匯出 **SAML** 中繼資料）以儲存中繼資料檔案。
- 若要針對驗證相關問題進行疑難排解，請檢查流量日誌（**Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量））和驗證日誌（**Monitor**（監控） > **Logs**（日誌） > **Authentication**（驗證））。明確 Proxy 會在日誌中顯示以下 IP 位址和位置：
  - **IP** 位址—如果行動使用者略過 PAC 檔案中的 ACS FQDN，則流量日誌中 **Source**（來源）欄顯示的 IP 位址，以及驗證日誌中 **IP Address**（**IP** 位址）欄顯示的 IP 位址，在 **Explicit_Proxy_Device_Group** 下檢視時，將與行動使用者的 IP 位址相同。如果使用者未略過 PAC 檔案中的 ACS FQDN，則來源 IP 位址是明確 Proxy 雲端防火牆的公用 IP 位址，其中重新導向是前往 ACS。
  - 位置—如果行動使用者略過 PAC 檔案中的 ACS FQDN，則 **Authentication Logs**（驗證日誌）中 **Region**（區域）欄顯示的區域名稱、**Current Users**（目前使用者）和 **Users (Last 90 days)**（使用者（過去 **90** 天））是部署了 ACS 的 5 個區域（us-west-2、us-east-1、eu-west-2、eu-west-3、ap-south-1）之一，並顯示明確 Proxy 從用戶端瀏覽器執行重新導向的區域。如果使用者略過 PAC 檔案中的 ACS FQDN，則 **Authentication Logs**（驗證日誌）中 **Region**（區域）欄顯示的區域名稱、**Current Users**（目前使用者）和 **Users (Last 90 days)**（使用者（過去 **90** 天））是部署了 ACS 的 5 個區域（us-west-2、us-east-1、eu-west-2、eu-west-3、ap-south-1）之一，並顯示明確 Proxy 從明確 Proxy 防火牆執行重新導向的區域。


©2025 Palo Alto Networks, Inc.

# 明確 Proxy 的封鎖設定

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Panorama Managed Prisma Access | • Prisma Access 授權 |

若要啟用此功能，請聯繫您的**Palo Alto Networks** 客戶代表或合作夥伴，他們將聯絡網站可靠性工程 **(SRE)** 團隊並提交要求。

當使用者使用明確 Proxy 存取網際網路目的地時，網際網路目的地的 DNS 解析由明確 Proxy 執行。若要在 DNS 解析階段封鎖對網際網路目的地的存取，您可以使用封鎖設定。您可以根據 DNS 安全性類別、URL 篩選類別或外部動態清單 (EDL) 進行封鎖。

對於您封鎖的網域，Prisma Access 會封鎖網域，並且使用者會在 HTTP GET 要求（用於未加密的網站）或 HTTP Connect 要求（用於加密的網站）期間收到封鎖頁面，這意味著網域在初始連線要求期間遭到封鎖。當您封鎖對網站的存取時，在使用者完成驗證流程之後，會向使用者顯示一個封鎖頁面，並擷取使用者名稱以進行進一步取證和安全性作業中心 (SOC) 工作流程。

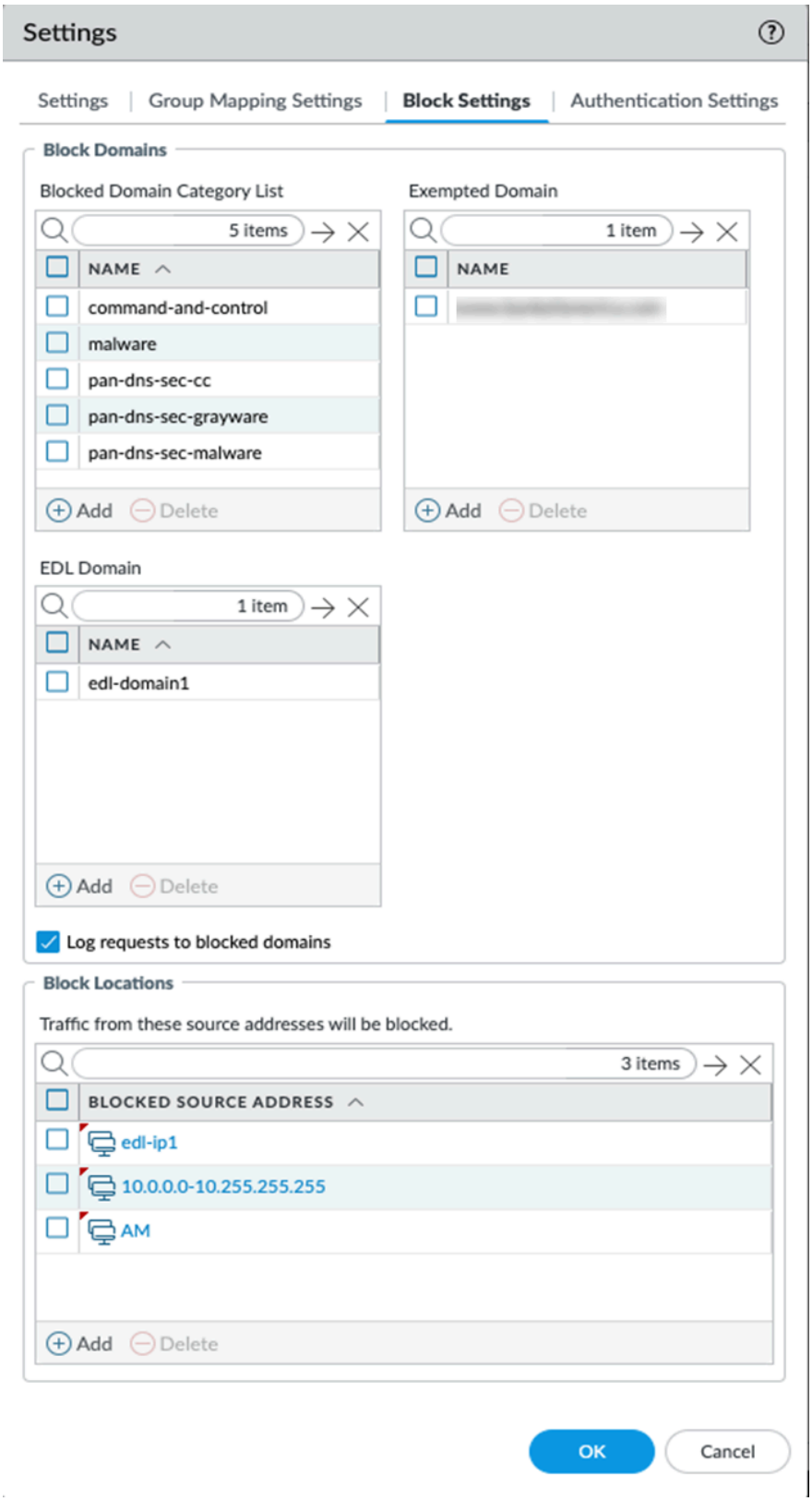
如果您使用的是 Prisma Access (Managed by Strata Cloud Manager)，請參閱 設定明確 Proxy 中的步驟 8。若要在 Panorama Manage Prisma Access 設定封鎖設定，請完成以下步驟。

**STEP 1 |** 設定 **Block Settings**（封鎖設定）以封鎖網域或網域類別。

為惡意網站或為您不想要使用者存取的任何網站指定網域或網域類別。當使用者起始 HTTP GET（用於未加密的要求）或 HTTP CONNECT（用於加密的請求）時，Prisma Access 會阻止


©2025 Palo Alto Networks, Inc.

使用者存取您在此區域中指定的 URL 和 IP 位址。當使用者嘗試存取遭封鎖的網站時，他們會收到一個封鎖頁面。




 ©2025 Palo Alto Networks, Inc.

1. 在 **Blocked Domain Category List**（封鎖的網域類別清單）中，輸入要封鎖的預先定義類別。

   不支援自訂 URL 類別。
2. 在 **EDL Domain**（**EDL** 網域）中，輸入要封鎖的網域型外部動態清單 (EDL)。

   您只能選取 EDL 類型為 **Dynamic Domain Lists**（動態網域清單）的 EDL；不允許動態 IP 清單和動態 URL 清單。
3. 如果想要豁免 **Blocked Domain Category List**（封鎖的網域類別清單）中包括的任何網域，請將它們指定為 **Exempted Domain**（豁免網域）。

   輸入的任何網域都會豁免而不被封鎖，即使它們出現在您已封鎖的網域類別中也一樣。

   - 您最多可以輸入 100 個網域。
   - 網域記錄的長度上限為 256 個字元。

**STEP 2 |** 在 **Blocked Source Address**（封鎖的來源位址） 區域中選取要封鎖的 IP 位址。

您可以 **Add**（新增）位址、位址群組、IP 位址型 EDL，或區域和國家/地區型 IP 位址。

請使用以下 IP 位址指導方針：

- 僅使用 **Type**（類型）為 **IP List**（**IP** 清單）或 **Predefined IP List**（預先定義的 **IP** 清單）的 EDL。
- 僅使用類型為 **IP Range**（**IP** 範圍）或 **IP Netmask**（**IP** 網路遮罩）的位址物件。
- 不支援具有動態物件成員資格的位址群組。
- 不要在 IP 位址物件中使用自訂區域；請改用預先定義的區域。

**STEP 3 |** 選取 **Log requests to blocked domains**（記錄對已封鎖網域的要求），以使 Prisma Access 記錄已封鎖的網域要求。

由於封鎖的網域日誌可能會從 botnet 產生大量流量，因此在啟用記錄時要小心，或者僅將其用於疑難排解目的。如果您限制使用 Proxy（例如，如果您限制使用特定 IP 位址），則能夠啟用沒有限制的記錄。

## 使用特殊物件限制明確 Proxy 網際網路流量流向特定的 IP 位址

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

明確 Proxy 提供您特殊的位址物件、位址群組和外部動態清單 (EDL)，以限制只有特定的來源 IP 位址才能存取明確 Proxy。當您使用以下確切名稱建立其中一個或多個特殊物件時，明確 Proxy 允許您指定的來源 IP 位址，並封鎖任何其他 IP 位址。

- 位址物件—在 Explicit_Proxy_Device_Group 中選取 **Objects**（物件） > **Addresses**（位址），並建立一個名為 **Palo Alto Networks Explicit Proxy Allowed Source Address** 的物件。

 ©2025 Palo Alto Networks, Inc.

- 位址群組—在 Explicit_Proxy_Device_Group 中選取 **Objects**（物件） > **Address Groups**（位址群組），並建立一個名為 **Palo Alto Networks Explicit Proxy Allowed Source Address Group** 的物件。
- 外部動態清單 **(EDL)**—在 Explicit_Proxy_Device_Group 中選取 **Objects**（物件） > **External Dynamic Lists**（外部動態清單），並建立一個名為 **Palo Alto Networks Explicit Proxy Allowed Source List** 的 EDL，然後建立一個類型為 **IP List**（IP 清單）的 EDL。

您可以指定 IP 位址，例如分公司的輸出 IP 位址。

使用萬用字元（例如 *.*）跳過大量網域的明確 Proxy 驗證是不允許的，除非您使用其中一個特殊物件將您的來源流量限制為特定的來源 IP 位址。

單獨或聯合使用位址物件、位址群組或 EDL；例如，您可以僅建立一個位址群組，無需建立位址物件或 EDL。

## 使用明確 Proxy 存取您的資料中心

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ （適用於 ZTNA 連接器和 Colo-Connect）Prisma Access 5.2.1 版<br>❑ （適用於服務連線）Prisma Access 5.0 版<br>❑ （適用於私人和合作夥伴應用程式存取）適用於 Windows 或 macOS 的 GlobalProtect app 6.2 版 |

您可以使用服務連線、ZTNA 連接器或 colo-connect，存取資料中心資源，例如外部動態清單或私人和合作夥伴應用程式，同時仍可從明確 Proxy 連線中受益。

不支援下列 *RFC 6598 IP* 位址經由服務連線、*Colo-Connect* 或 *ZTNA* 連接器透過明確 *Proxy* 存取私人應用程式：

- *100.64.0.0/15*
- *100.88.0.0/15*
- *100.72.0.0/15*

在 *ZTNA* 連接器應用程式 *IP* 區塊或連接器 *IP* 區塊中使用這些 *IP* 位址的現有 *ZTNA* 連接器，無法透過明確 *Proxy* 在 *Proxy* 模式下使用 *Prisma Access Browser* 或 *GlobalProtect* 代理程式。您必須聯繫 *Palo Alto Networks* 代表，才能將您的 *IP* 位址移轉到不同的區塊。

- Strata Cloud Manager
- Panorama


©2025 Palo Alto Networks, Inc.

## 使用明確 Proxy 存取您的資料中心 （Strata Cloud Manager)

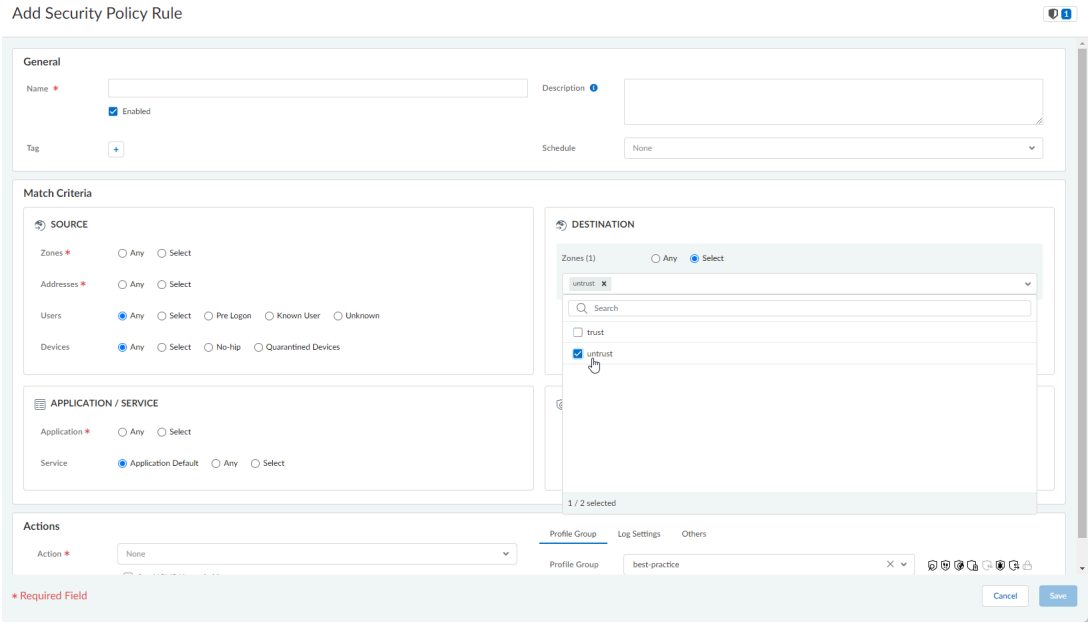
**STEP 1 |** 根據您的需求，在 Prisma Access 中設定服務連線、Colo-Connect 或 ZTNA 連接器。

**STEP 2 |** 設定 DNS 設定

**STEP 3 |** 確保網際網路繫結流量的 **DESTINATION Zones**（目的地區域）設定為 **untrust**（不信任），而不是 **any**（任何）。

> 無法執行此步驟，可能會導致意外存取您的資料中心。

1. 前往 **Manage**（管理） > **Configuration**（組態） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**），將 **Configuration Scope**（組態範圍）設定為 **Prisma Access** > **Mobile Users Container**（行動使用者容器） > **Explicit Proxy**（明確 **Proxy**），然後選取 **Security Policy**（安全性政策） > **Security Services**（安全性服務）。
2. 開啟網際網路繫結流量的規則。
3. 確保 **DESTINATION**（目的地）下的 **Zones**（區域）設定為 **untrust**（不信任）。




4. 針對所有網際網路繫結流量規則重複此動作。

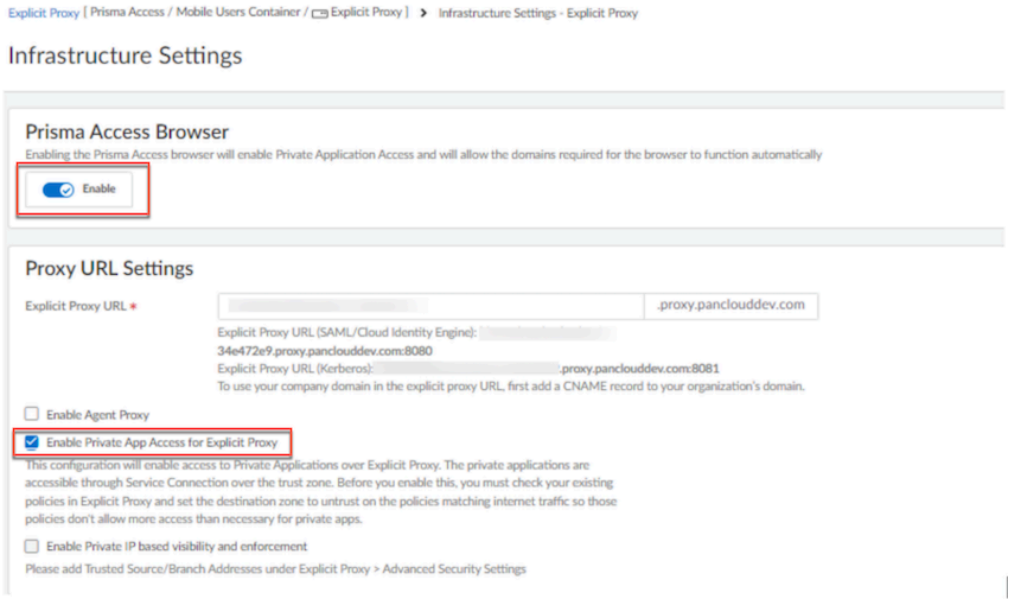
**STEP 4 |** 啟用私人應用程式存取。

- 使用 Prisma Access Browser

  1. 啟用私人應用程式存取 選取 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Explicit Proxy**（明確 **Proxy**） > **Infrastructure Settings**（基礎結構設定）和 **Enable**（啟用）Prisma Access Browser。在 **Proxy URL Settings**（**Proxy URL**

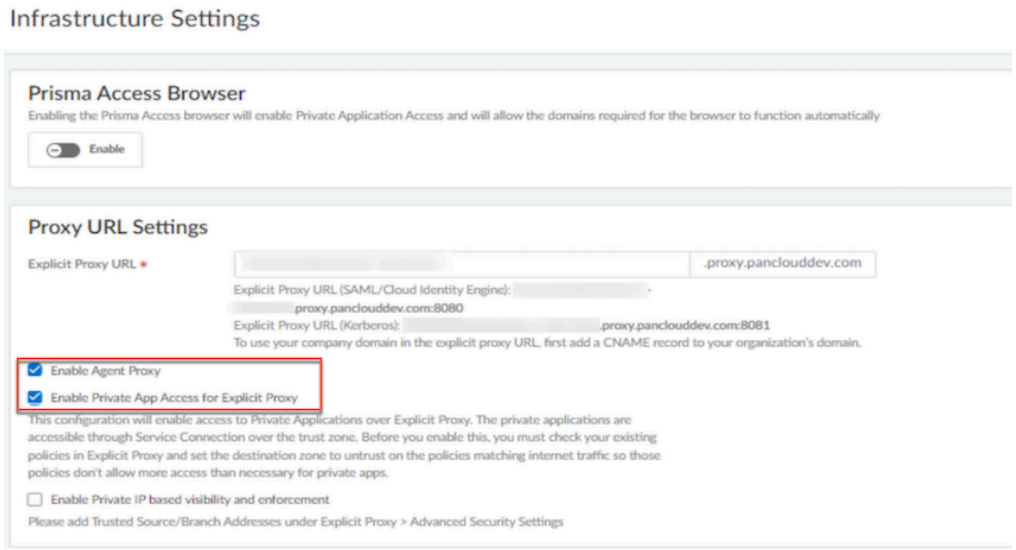
 ©2025 Palo Alto Networks, Inc.

設定）下，選取 **Enable Private App Access for Explicit Proxy**（為明確 **Proxy** 啟用私人應用程式存取）




- 使用一般瀏覽器

  1. 啟用私人應用程式存取 選取 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Explicit Proxy**（明確 **Proxy**） > **Infrastructure Settings**（基礎結構設定） > **Enable Agent Proxy**（啟用代理程式 **Proxy**） > **Enable Private App Access for Explicit Proxy**（為明確 **Proxy** 啟用私人應用程式存取）。



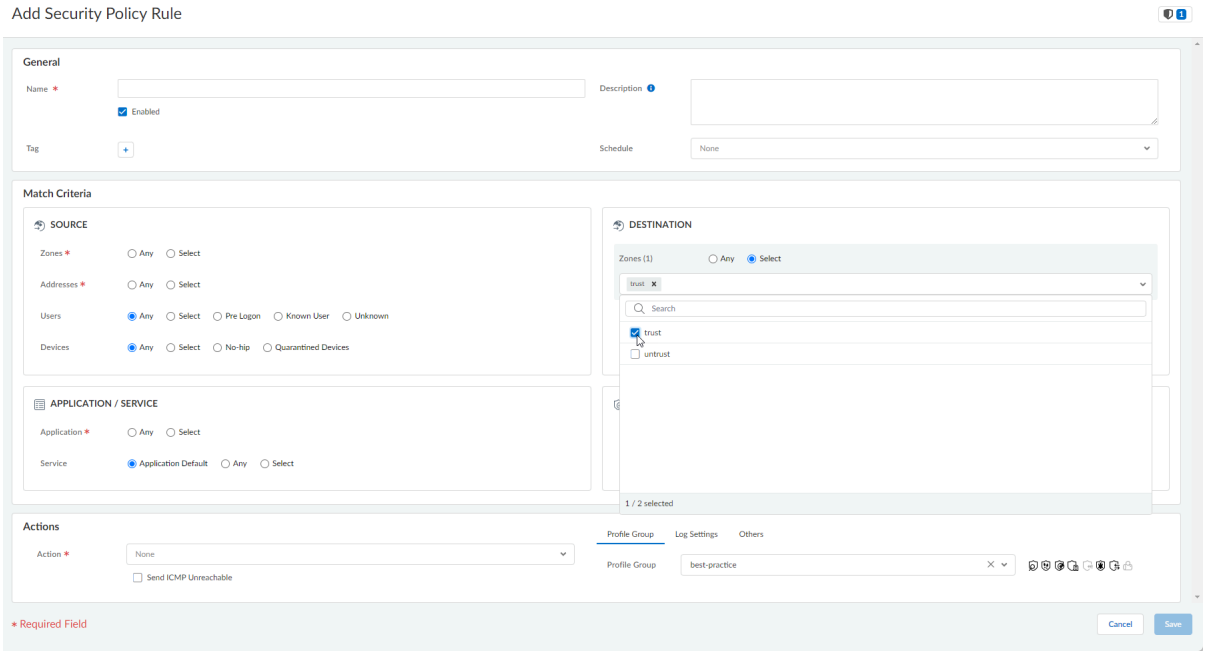

**STEP 5 |** 為您想要存取的資料中心建立安全性政策規則。

1. 前往 **Manage**（管理） > **Configuration**（組態） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**），將 **Configuration Scope**（組態範圍）設定為 **Prisma Access** > **Mobile Users Container**（行動使用者容器） > **Explicit Proxy**（明確 **Proxy**），然後選取 **Security Policy**（安全性政策） > **Security Services**（安全性服務）。


©2025 Palo Alto Networks, Inc.

2. 建立安全性政策規則。

在用於資料中心存取的規則中，確保 DESTINATION（目的地）下的 **Zones**（區域）設定為 **trust**（信任）.




**STEP 6 |** 如果您在明確 Proxy 下啟用私人應用程式存取，請在裝載 ZTNA 連接器之後，**Push Config**（推送組態）以儲存您的組態變更。

## 使用明確 Proxy 存取您的資料中心 （Panorama）

**STEP 1 |** 根據您的需求，在 Prisma Access 中設定服務連線、Colo-Connect 或 ZTNA 連接器。

**STEP 2 |** 設定 DNS 設定

**STEP 3 |** 設定區域對應。

1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（組態） > **Mobile Users - Explicit Proxy**（行動使用者 - 明確 **Proxy**） > **Zone Mapping**（區域對應）
2. 將您將用來存取資料中心資源的區域新增至 **Trusted Zones**（受信任區域）。

**STEP 4 |** 確保政策規則中網際網路繫結流量的 Destination ZONE（目的地區域）設定為不受信任的區域，而不是 any（任何）。

無法執行此步驟，可能會導致意外存取您的資料中心。

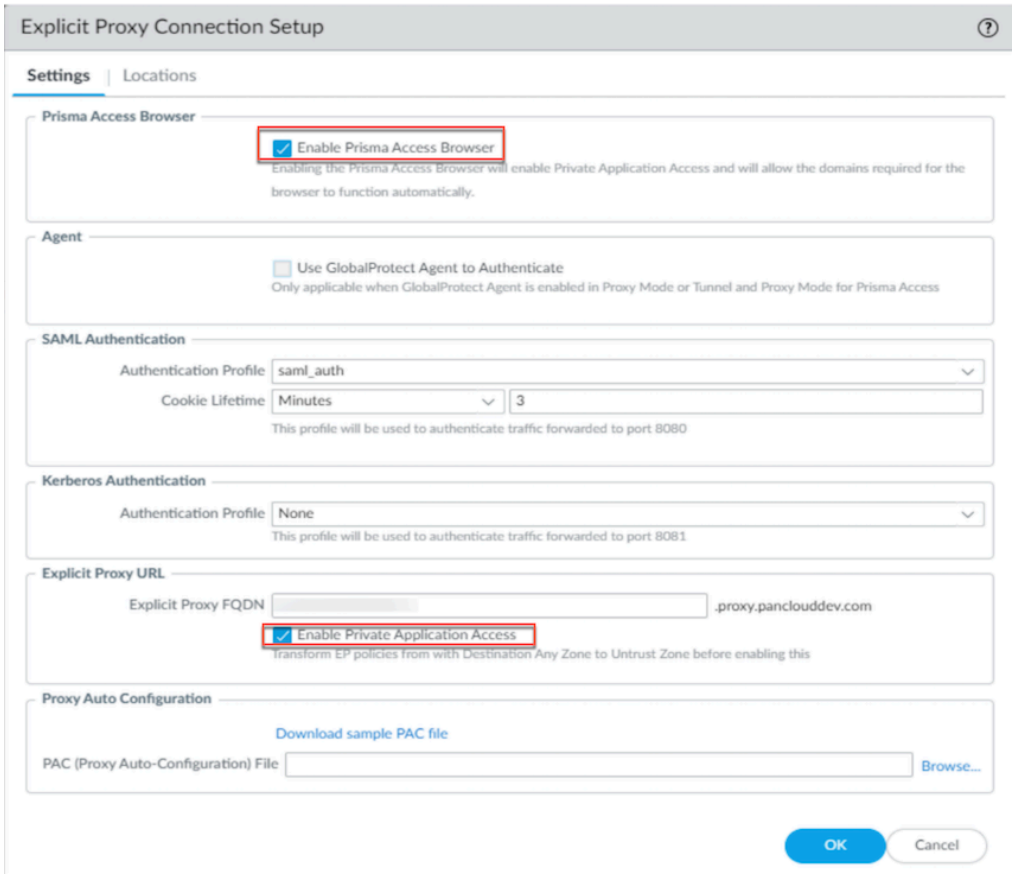
1. 選取 **Policies**（原則）。
2. 將 Device Group（裝置群組）設定為 **Explicit_Proxy_Device_Group**。
3. 將 Destination ZONE（目的地目的地）從 any（任何） 變更為您在先前步驟中設定的其中一個不受信任的區域。


©2025 Palo Alto Networks, Inc.

**STEP 5 |** 啟用私人應用程式存取。

- 使用 Prisma Access Browser

  1. 啟用私人應用程式存取 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（組態） > **Mobile Users - Explicit Proxy**（行動使用者 - 明確 **Proxy**） > **Settings**（設定） > **Advanced**（進階） > **Enable Prisma Access Browser**（啟用 **Prisma Access** 瀏覽器） > **Enable Private Application Access**（啟用私人應用程式存取）

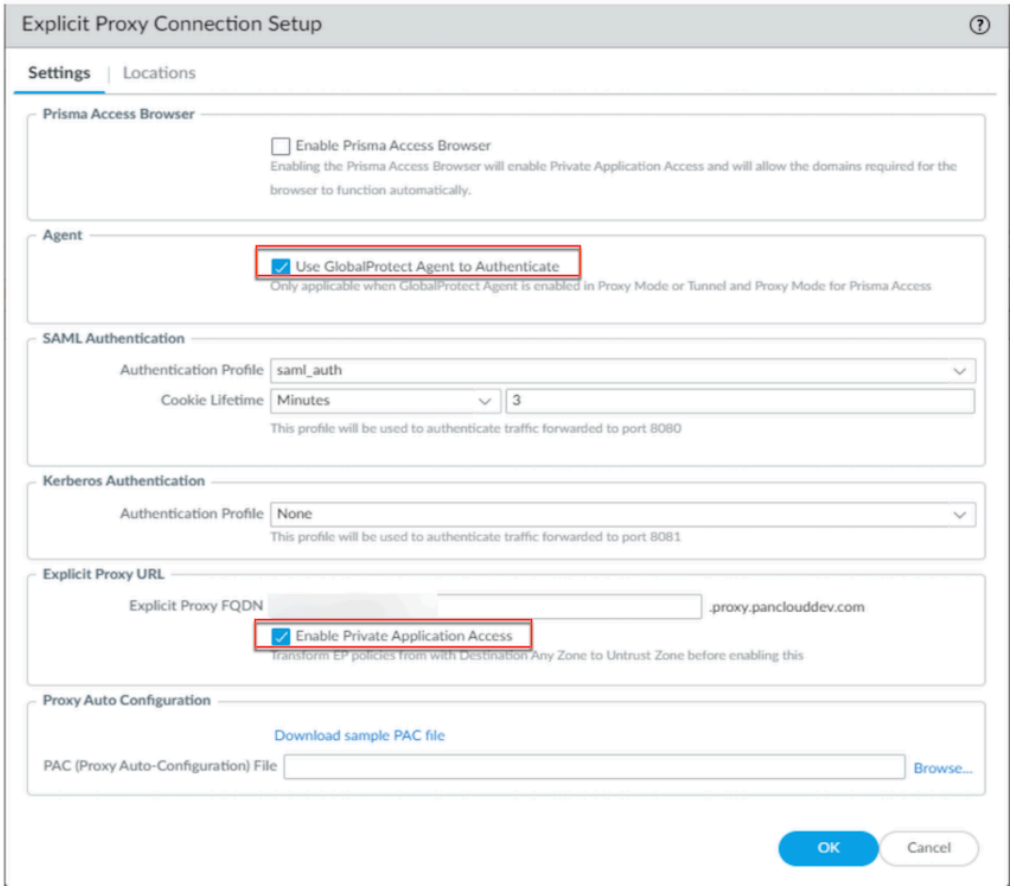



- 使用一般瀏覽器

  1. 啟用私人應用程式存取 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（組態） > **Mobile Users - Explicit Proxy**（行動使用者 - 明確 **Proxy**） > **Settings**（設定） > **Advanced**（進階） > **Use GlobalProtect Agent to**


©2025 Palo Alto Networks, Inc.

**Authenticate**（使用 **GlobalProtect** 代理程式來驗證） > **Enable Private Application Access**（啟用私人應用程式存取）




**STEP 6 |** 為您想要存取的資料中心建立安全性政策規則。

1. 選取 **Policies**（原則）。
2. 將 `Device Group`（裝置群組）設定為 **Explicit_Proxy_Device_Group**。
3. 建立安全性政策規則。

   在用於資料中心存取的規則中，確保使用您在先前步驟中設定的 **Trusted**（受信任）區域。

# 應用程式型 Office 365 與明確 Proxy 整合

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • 行動使用者授權 |

瞭解如何整合瀏覽器型 Office 365 版本與明確 Proxy。

- Strata Cloud Manager


©2025 Palo Alto Networks, Inc.

- Panorama

## 應用程式型 Office 365 與明確 Proxy 整合 (Panorama)

Prisma Access 明確 Proxy 支援瀏覽器型 Office 365 (M365) 版本，包括 Office Online (office.com)。請遵循下列步驟，整合瀏覽器型 Office 365 版本與明確 Proxy。

雖然明確 Proxy 不支援應用程式型 Office 365 版本，但您可以遵循下列準則，使用明確 Proxy 搭配 Office 365 應用程式型政策。

### 設定瀏覽器型 Office 365 與 Prisma Access 明確 Proxy 整合

如果您使用瀏覽器型 Office 365 版本，請完成下列工作，以整合 Office 365 與明確 Proxy。

**STEP 1 |** （選用）如果您想要使用租用戶型限制（僅限制特定數目的租用戶對 Office 365 的存取控制），請使用具有自訂 URL 類別的 HTTP 標頭插入，來允許特定租用戶存取 Office 365。

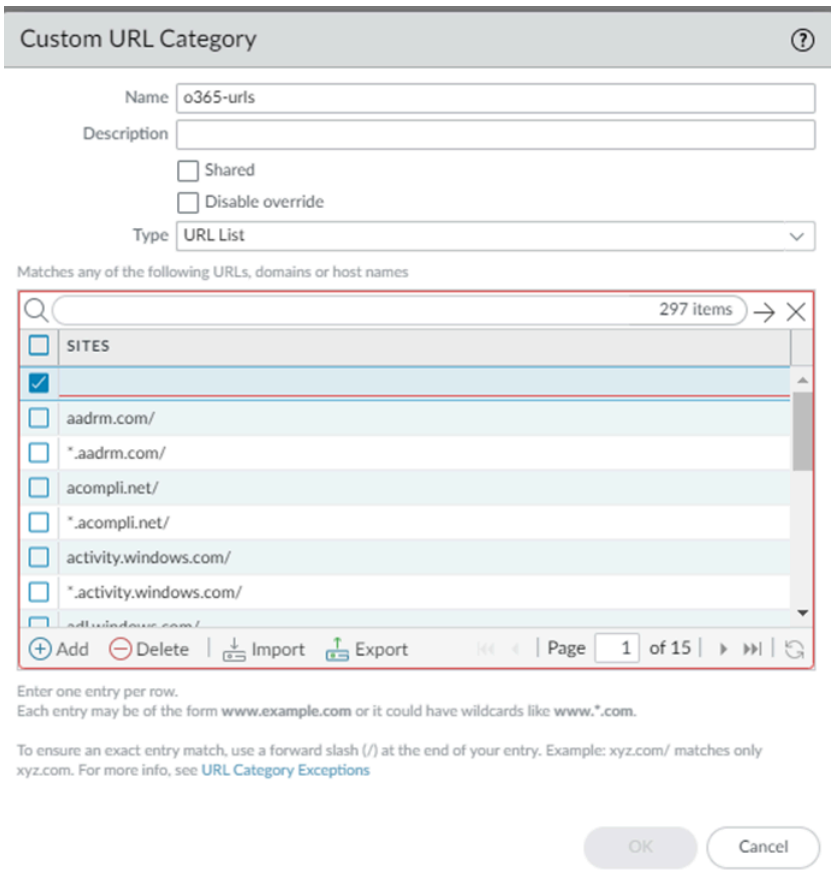
 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 為用於 Office 365 的 URL 新增解密政策。

1. 選取 **Objects**（物件） > **Custom Objects**（自訂物件） > **URL Category**（**URL** 類別），然後 **Add**（新增）自訂 URL 類別。

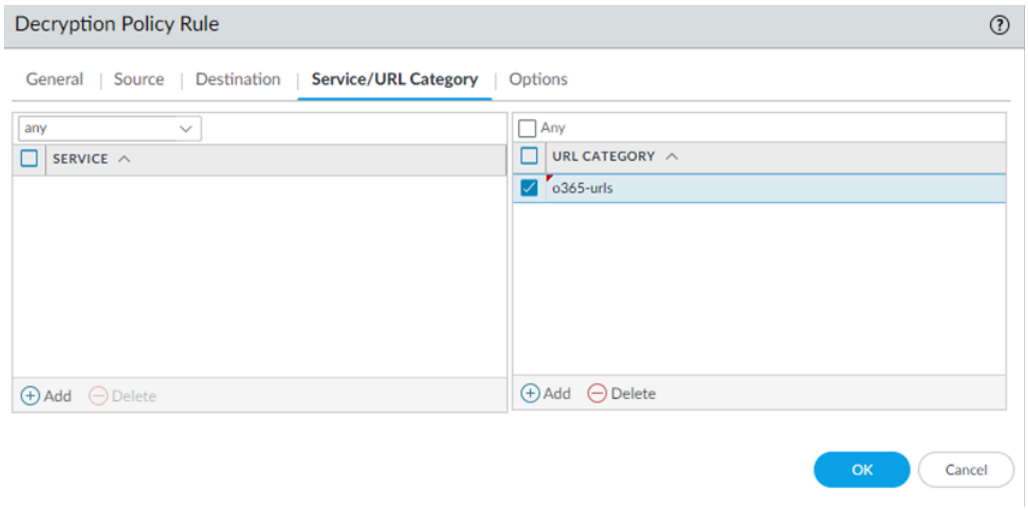
   確保您位於 **Explicit_Proxy_Device_Group**。
2. 指定 **Type**（類型）為 **URL List**（**URL** 清單）。
3. **Add**（新增）網站清單以啟用 Office 365 整合。

   為了簡化 URL 的上傳，您可以複製 https://saasedl.paloaltonetworks.com/feeds/m365/worldwide/any/all/url 上的 Office 365 URL 清單、將這些 URL 儲存到檔案，然後將檔案 **Import**（匯入）至自訂 URL 類別。




4. 選取 **Policies**（原則） > **Decryption**（解密） > **Pre Rules**（預先規則），然後 **Add**（新增）解密政策規則。
5. 指定您建立的 **URL Category**（**URL** 類別）。


©2025 Palo Alto Networks, Inc.




6.

**STEP 3 |** 為資料和威脅防護功能新增解密政策，例如企業資料遺失防護（企業 DLP）、WildFire、威脅防護或 SaaS 安全性。

**STEP 4 |** 使用 EDL 主機服務來建立外部動態清單。

**STEP 5 |**

設定應用程式型 **Office 365** 與明確 **Proxy** 整合

明確 Proxy 不支援完整用戶端型（應用程式）Office 365 版本，因為 Office 365 使用非 Web 連接埠和通訊協定，以及釘選的憑證，這會阻止使用解密。如果需要保護來自 Office 365 用戶端應用程式的流量，您可以使用下列其中一個 Prisma Access 功能來執行此操作：

- 部署行動使用者—GlobalProtect 部署搭配明確 Proxy，並使用 GlobalProtect 分割通道選項，將流量從 Office 365 應用程式路由至 GlobalProtect 通道，同時根據 PAC 檔案，以及 GlobalProtect 通道包含和排除選項指定要傳送至 GlobalProtect 通道、導向至網際網路，或傳送至明確 Proxy明確的其他網際網路流量。
- 如果您的組織要求網際網路繫結流量通過明確 Proxy，或者如果您的網路沒有預設路由，則您可以部署遠端網路部署搭配明確 Proxy遠端網路部署搭配明確 Proxy。在此部署中，明確 Proxy 為您提供 Anycast 和單點傳送位址清單，而且您可以將 CPE 設定為透過這些位址將流量路由到遠端網絡，然後從那裡路由到明確 Proxy 再到網際網路。

  若要使用 Office 365 搭配此部署類型，請指定 PAC 檔案規則，以略過非 Web Office 365 直接路由至網際網路。
- 如果無法在您的環境中部署 GlobalProtect 或 Prisma Access 遠端網路，您可以設定明確 Proxy PAC 檔案以略過 Office 365 流量。使用要略過的 URL 清單。

要啟用 *Office 365* 與 *Prisma Access* 明確 *Proxy* 整合的 *URL* 清單

您可以用來整合非瀏覽器 Office 365 應用程式與明確 Proxy 的選項，就是指定 Office 365 相關 URL，並在明確 Proxy PAC 檔案中略過這些 URL。使用下列其中一種方法，取得要略過的 URL 清單：

 ©2025 Palo Alto Networks, Inc.

- 將來自 Palo Alto Networks EDL 託管服務的 EDL URL 用於 Microsoft 365 應用程式。

  使用託管服務可以透過利用摘要 URL 作為 EDL 來源，減輕保護 SaaS 應用程式流量的操作負擔。當 SaaS 提供者為 SaaS 應用程式新增端點時，對應摘要 URL 會更新。

  對於全球 Microsoft 365 URL，請使用 https://saasedl.paloaltonetworks.com/feeds/m365/worldwide/any/all/url URL。也為 IPv4 和 IPv6 以及國家/地區特定的應用程式和政府應用程式提供其他 URL。
- 擷取 Microsoft 在 https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges 提供的 Office 365 IP 位址和 URL 清單。Microsoft 也在 https://learn.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-ip-web-service上提供了 Office 365 IP 位址和 URL Web 服務。

# 使用 Blue Coat Proxy 設定 Proxy 鏈結

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 授權。 |

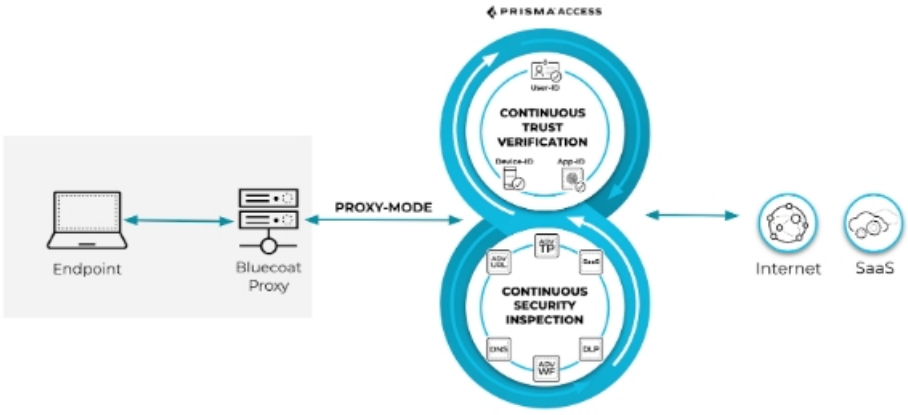
為了額外的安全層或由於合規性，Proxy 鏈結透過串聯多個 Proxy 伺服器，建立多重躍點網際網路路徑。每個伺服器都會將您的流量轉送到下一個伺服器，最終到達網際網路。此技術使用您現有的網路基礎結構，並可讓您連線到上游 Proxy 以進行安全的 HTTP 和 HTTPS 通訊。此整合保留了使用者瀏覽器設定，同時增強了安全性和控制。

企業為何使用 Proxy 鏈結功能：

1. 透過提供多層保護和略過地理限制來增強隱私權和匿名性。
2. 透過為使用者的瀏覽體驗新增額外的安全層來篩選惡意內容、垃圾郵件和網路釣魚嘗試，從而實現安全性和控制。
3. 公司可以使用 Proxy 鏈結，根據使用者角色或位置限制對某些網站或服務的存取，從而強制執行內部政策規則。
4. Proxy 連結可讓您透過連線到上游 Proxy 伺服器來執行特定工作，從而利用現有的網路基礎結構，而不是部署新系統。這可能是一種符合成本效益且高效的解決方案。

進一步瞭解 Prisma Access 明確 Proxy 的運作方式。

 ©2025 Palo Alto Networks, Inc.




以下是客戶想要 Proxy 將流量從內部部署 Blue Coat Proxy 鏈結到 Prisma Access 明確 Proxy 的案例。內部部署 Blue Coat Proxy 會驗證使用者，並對 Blue Coat Proxy 使用 X-Authenticated-User (XAU) 標頭插入，將使用者名稱傳遞給 Prisma Access 明確 Proxy。

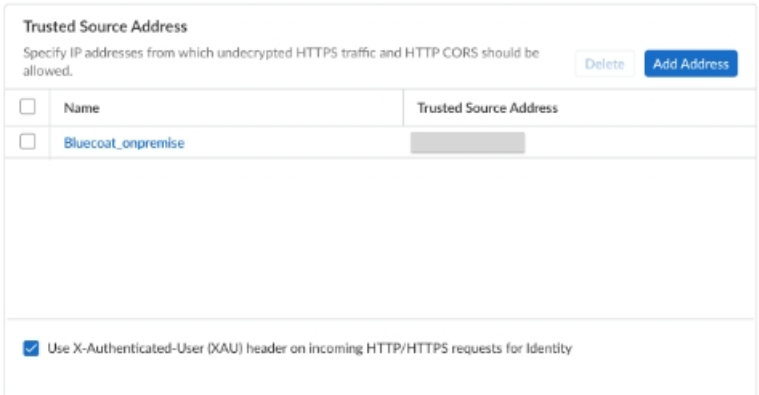
在無預設路由網路中，需要明確 *Proxy IP* 位址的靜態路由和目的地 *NAT*。

**STEP 1 |** 設定 Prisma Access。

1. 設定明確 Proxy。
2. 新增 Blue Coat 明確 Proxy 作為受信任來源位址。
   1. 選取 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Explicit Proxy**（明確 **Proxy**） > **Advanced Security Settings**（進階安全性設定） > **Add Address**（新增位址）。
   2. 輸入 Blue Coat 明確 Proxy 的 IP 位址。

      您可以新增 *IP* 位址或子網路。

   3. 選取 **Use X-Authenticated-User (XAU) header on incoming HTTP/HTTPS requests for Identity**（對傳入 **HTTP/HTTPS** 要求使用 **X-Authenticated-User (XAU)** 標頭以進行識別）。

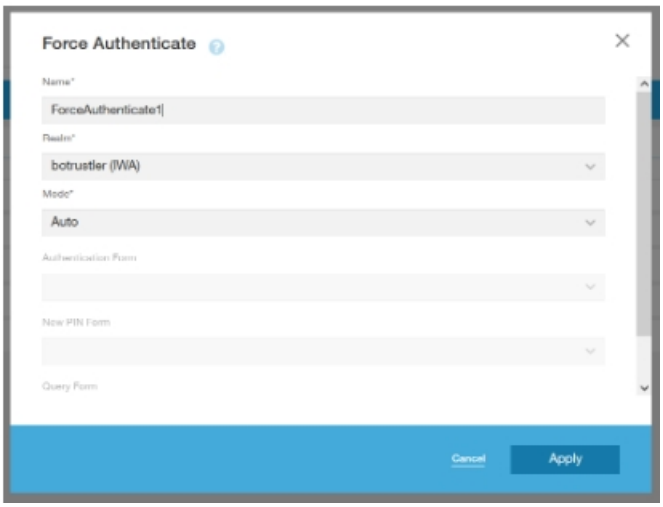



 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 在 Blue Coat Proxy 上執行設定。

1. 強制執行驗證,



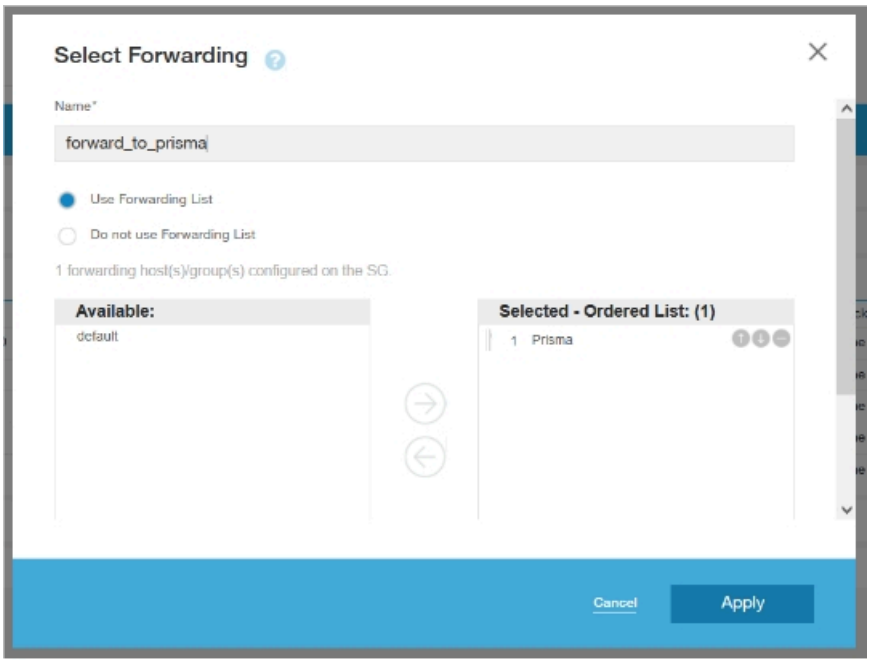



2. 設定轉送層。




1. 取得 Prisma Access 明確 Proxy 的 IP 位址。
    1. 在 Strata Cloud Manager 中，選取 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Explicit Proxy**（明確 **Proxy**） > **Infrastructure Settings**（基礎結構設定）。
    2. 複製 Proxy FQDN。

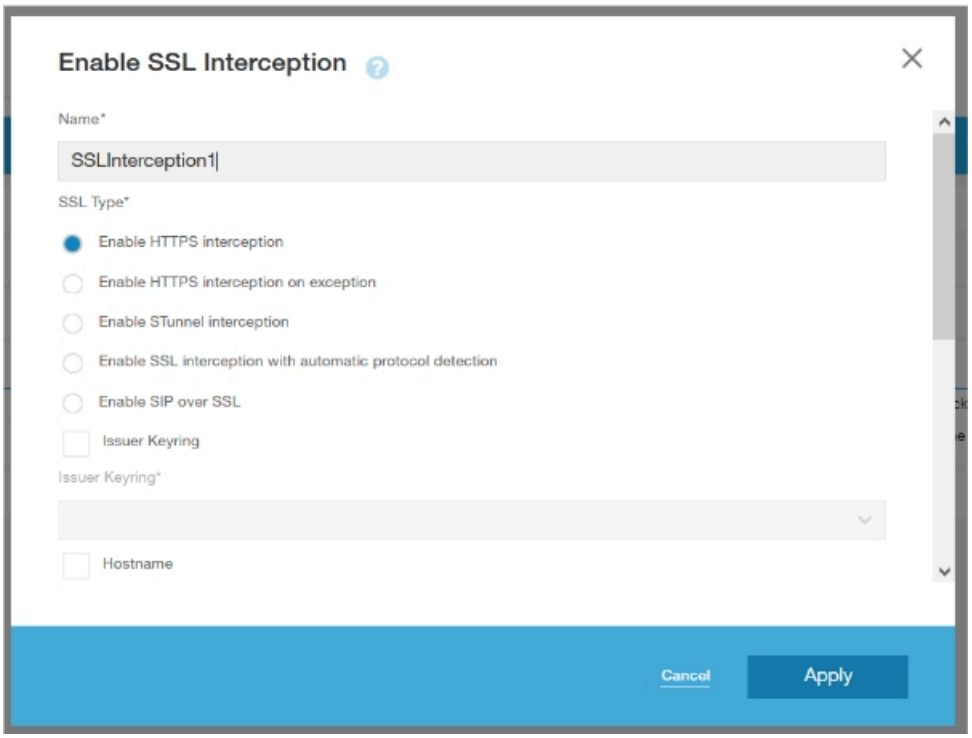
 ©2025 Palo Alto Networks, Inc.






2. 啟用 HTTPS 解密進行標頭插入。

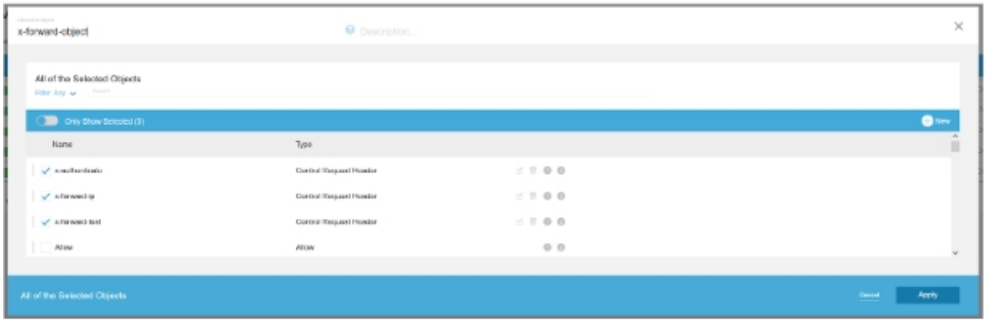
   對於標頭插入，解密是必要的。

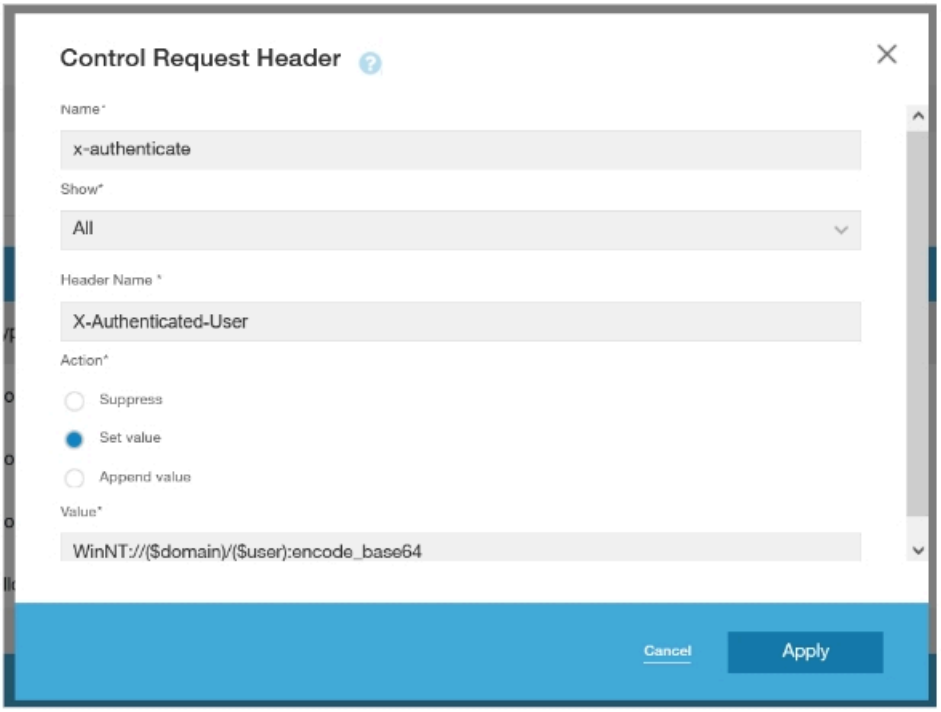



 ©2025 Palo Alto Networks, Inc.



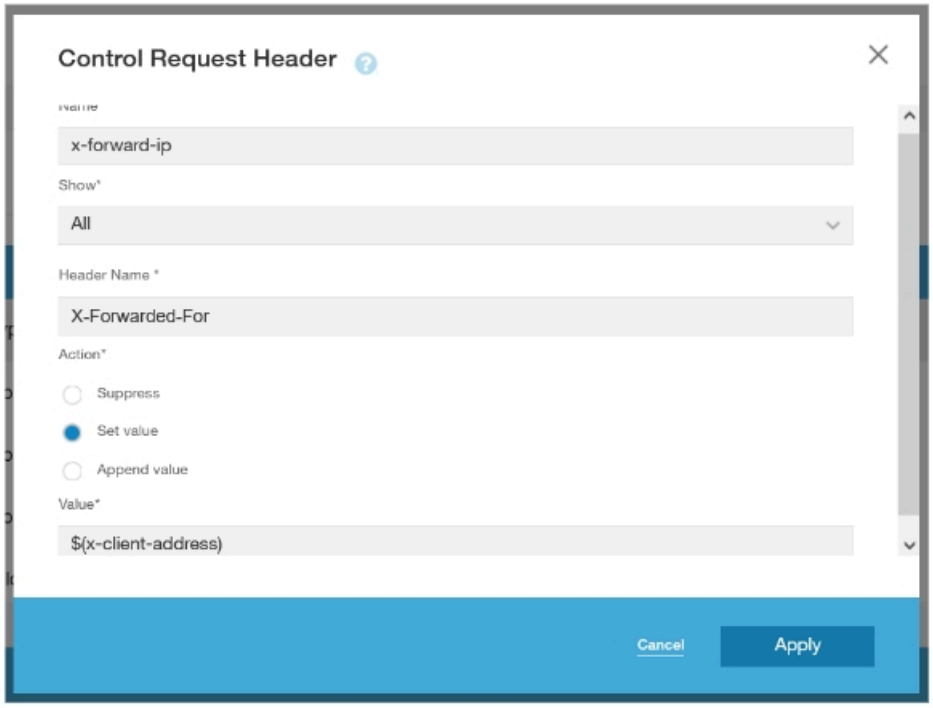
3. 設定標頭轉送。







©2025 Palo Alto Networks, Inc.




透過 *XFF* 標頭接收的用戶端 *IP* 位址僅加以記錄，不能用於政策。

4. 將標頭值編碼設定為 base64：

```
define action Encode_All_XFF set( request.x_header.X-
Authenticated-User, "$(user:encode_base64)" ) end define action
 x-authenticate set( request.x_header.X-Authenticated-User,
 "WinNT://($$domain)/($$user):encode_base64" ) end
```

**STEP 3 |** 確認組態。

1. 在 Strata Cloud Manager 中，選取 **Incidents and Alerts**（事件和警示） > **Log Viewer**（日誌檢視器）
2. 檢查 `X-Forwarded-For` 和 `Users`（使用者）欄，以驗證使用者和 IP 位址資訊在 Prisma Access 上是否可見。

**STEP 4 |** 請考慮以下幾點：

1. Blue Coat Proxy 需要驗證和解密才能插入 XAU 標頭資訊。
2. X-Authenticated-User 驗證標頭值應採用 Base64 格式。
3. Prisma Access 明確 Proxy 可以查看解密流量的使用者識別。

## 使用明確 Proxy 搭配 GlobalProtect（或第三方 VPN）

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | • Prisma Access 授權 |

 ©2025 Palo Alto Networks, Inc.

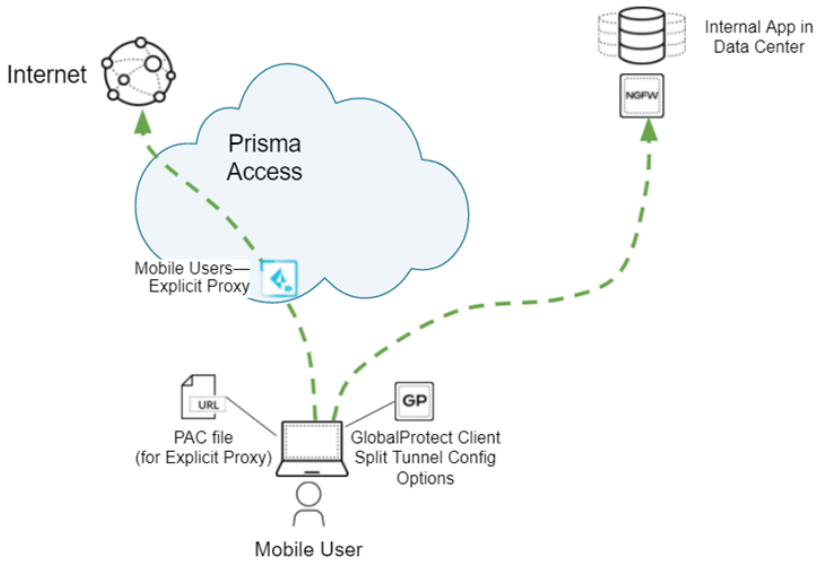
| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | |

您可以結合明確 Proxy 與 GlobalProtect（或第三方 VPN）：

- 明確 **Proxy** 和 **GlobalProtect**
  - 在分割通道模式下使用 GlobalProtect，僅提供對私人應用程式的安全存取。
  - 使用明確 Proxy 來保護公用應用程式，包括網際網路流量和外部 SaaS 應用程式。
- 明確 **Proxy** 和第三方 **VPN**

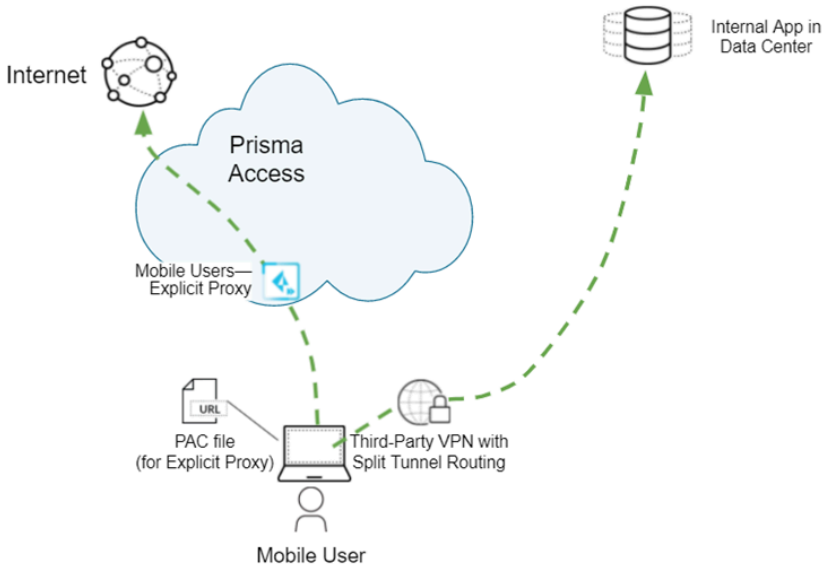
  如果您要使用 VPN 用戶端存取資料中心和私人應用程式，則可以繼續使用該用戶端，來保護對私人應用程式的安全存取，同時使用明確 Proxy 和 PAC 檔案，保護對公用應用程式的存取。您可以將明確 Proxy 部署在靠近行動使用者的位置，這樣就無需為了 Web 安全性而將流量回傳到您的資料中心。

下圖顯示了使用 GlobalProtect 閘道搭配明確 Proxy 的部署。GlobalProtect 使用 GlobalProtect 用戶端將流量路由到 Palo Alto Networks 新世代防火牆。若要設定此部署，請在 GlobalProtect 中建立一個分割通道，允許使用 GlobalProtect 保護私人應用程式，並使用明確 Proxy 保護公用應用程式。設定完成時，行動使用者會使用 GlobalProtect 連線到您組織資料中心的私人應用程式，並使用明確 Proxy 連線到私人網際網路型應用程式。




如果您有第三方 VPN，則可以使用它，連線至資料中心的私人應用程式，同時使用明確 Proxy 保護公用應用程式，如下圖所示。


©2025 Palo Alto Networks, Inc.




開始使用：

- 其運作方式為何
- 明確 Proxy—指導方針
- 明確 Proxy 和 GlobalProtect：設定它
- 明確 Proxy 搭配第三方 VPN

## 使用明確 Proxy 搭配 GlobalProtect 或第三方 VPN 的需求

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

在開始您的設定之前，請確保遵循使用 GlobalProtect 或第三方 VPN 部署明確 Proxy 所需的需求和建議：

- 若要使用明確 Proxy 搭配 GlobalProtect，您必須部署 GlobalProtect（行動使用者—GlobalProtect 部署或使用 GlobalProtect 閘道和入口網站的獨立 GlobalProtect 部署）。

  您可以在 GlobalProtect 中設定分割通道設定。本節中的範例顯示了根據網域 (URL) 或應用程式分割流量；不過，您也可以根據存取路由分割流量。

  您也可以在 GlobalProtect 中設定分割 DNS 選項，以設定透過 VPN 指派的 DNS 伺服器解析的網域和透過本機 DNS 伺服器解析的網域。
- 若要使用明確 Proxy 搭配第三方 VPN，您必須部署 VPN 解決方案。


©2025 Palo Alto Networks, Inc.

- 列出要使用行動使用者—GlobalProtect 或第三方 VPN 部署保護的應用程式。

  例如，如果您是使用 GlobalProtect 設定明確 Proxy，則應將 GlobalProtect 設定為保護對私人應用程式或資源的所有存取，同時將明確 Proxy PAC 檔案設定為保護公用應用程式或 SaaS 應用程式。本節中的設定範例具有解析內部網域的 GlobalProtect 和解析外部域的明確 Proxy。
- 為明確 Proxy 和 GlobalProtect 或第三方 VPN 設定驗證。
  - 對於明確 Proxy，您必須使用 SAML 驗證。在明確 Proxy 部署中遵循設定 SAML 的指導方針，包括用於 SAML 登入的 URL。
  - 對於行動使用者—GlobalProtect 部署，如果您使用 SAML 驗證，Okta 作為識別提供者 (IdP)，請參閱 Prisma Access 整合指南（Panorama 管理）中您使用 Okta 設定 SAML 驗證所使用的程序。
  - 對於獨立 GlobalProtect 部署，您可以在 PAN-OS 中設定 SAML 驗證。
  - 對於第三方 VPN，請參閱該 VPN 的產品文件。

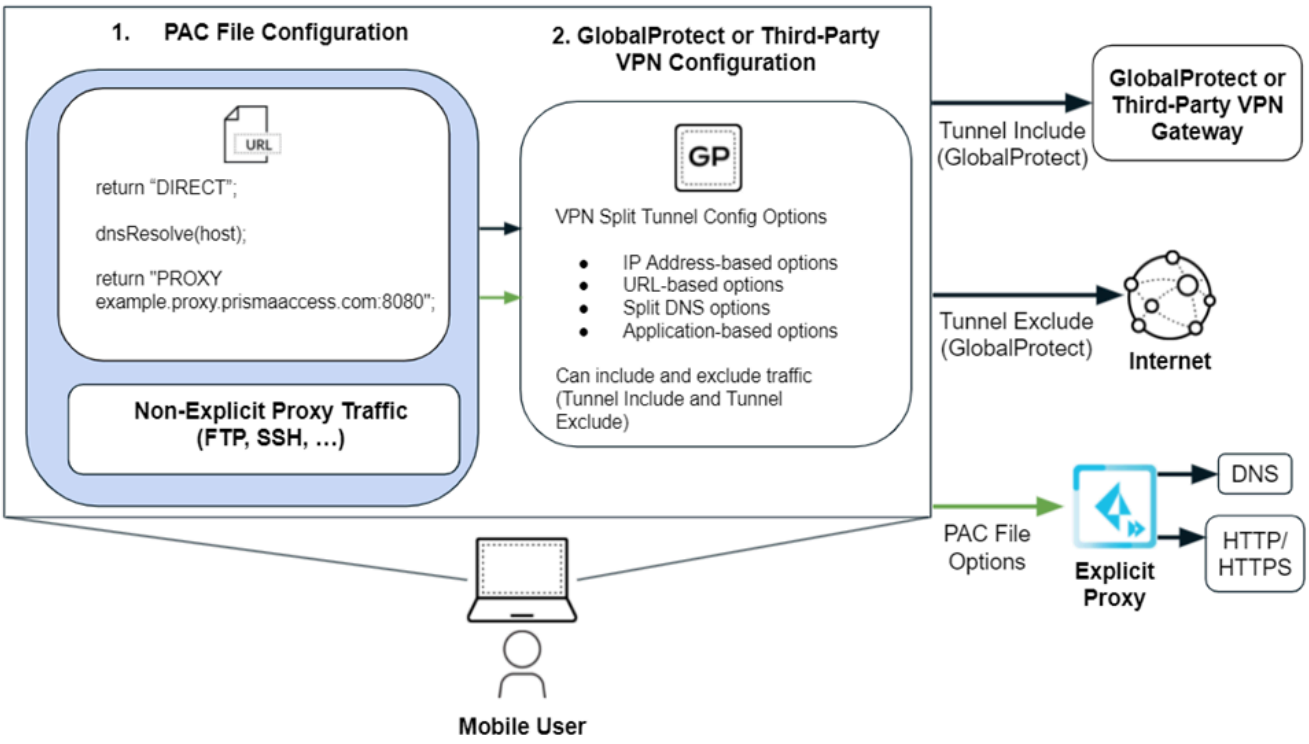
  Palo Alto Networks 建議您在每個行動使用者的端點上使用預設瀏覽器進行 SAML 驗證，以便您可以透過編輯入口網站設定來利用單一登入 (SSO)，如 設定明確 Proxy 中所示。
- 您必須確保行動使用者使用的瀏覽器遵守 PAC 檔案中的設定.

## 明確 Proxy 和 GlobalProtect：其運作方式為何

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

在確定您應該使用明確 Proxy 保護哪些應用程式或流量，以及應該使用 GlobalProtect 或第三方 VPN 保護哪些應用程式之前，應該瞭解 GlobalProtect 和 Prisma Access 如何根據明確 Proxy 和 VPN 設定做出其轉送決策。本節中的範例假設您已將明確 Proxy 和 GlobalProtect 部署到您組織的網路，並已設定 GlobalProtect 分割通道選項。下圖顯示其中過程。


©2025 Palo Alto Networks, Inc.




當行動使用者要求私人或網際網路型資源或應用程式時，該要求是由端點上的明確 Proxy PAC 檔案進行評估。

- PAC 檔案中的 `return "DIRECT";` 函數會導致運算式中指定的流量略過明確 Proxy 處理。

  明確 Proxy 為您提供一個範例 PAC 檔案，其會使用 `return "DIRECT";` 函數搭配 IP 位址和 URL。請參閱，以查看 PAC 檔案的內容以及如何其使用方式的說明。
- PAC 檔案中的 `dnsresolve(host)` 函數會強制端點進行 DNS 查詢，將主機名稱解析為 IP 位址。然後，此查詢會遵循 VPN 政策（例如，分割通道或分割 DNS），以將 DNS 要求轉送到目的地 DNS 伺服器。

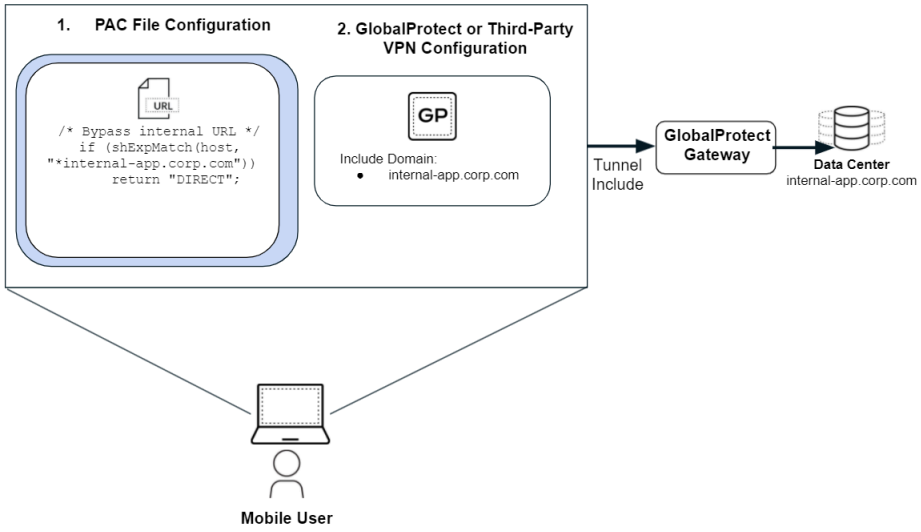
  隨明確 Proxy 提供的 PAC 檔案會在運算式中同時使用 `dnsresolve(host)`、`return"DIRECT";` 和私人 IP 位址。如果在 DNS 查閱之後，傳回的 IP 位址隨附在運算式中的私人 IP 位址中，則與私人 IP 位址相關聯的流量會略過明確 Proxy 處理。
- 在 PAC 檔案中指定為 `return"PROXY` *`sitename`*`:8080";` 的流量會轉送到明確 Proxy。

在 Web 要求根據 PAC 檔案中的條件進行評估之後，它會傳送到端點上的 GlobalProtect 或第三方 VPN 設定進行處理，且流量會在 GlobalProtect 應用程式中針對分割通道設定選項進行評估。您可以根據網域 (URL) 或應用程式或子網路分割流量。如果您已在 GlobalProtect 中設定分割 DNS 選項，則流量也會根據這些 DNS 選項進行評估。

在處理流量之後，該流量會根據 PAC 檔案和 VPN 處理，傳送到 GlobalProtect、導向到網際網路，或者傳送到明確 Proxy。

下圖顯示行動使用者正在嘗試使用 URL **`internal-app.corp.com`** 存取私人資源。


©2025 Palo Alto Networks, Inc.

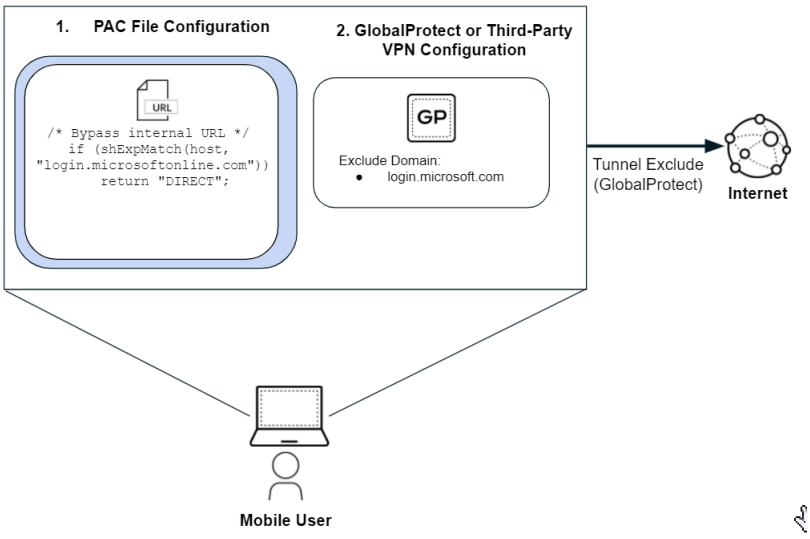



- PAC 檔案具有下列設定，以允許 **internal-app.corp.com** 略過明確 Proxy。

```
    /* Bypass internal URL */ if (shExpMatch(host, "*internal-
app.corp.com")) return "DIRECT";
```

- 當行動使用者從其瀏覽器要求 **internal-app.corp.com** 時，瀏覽器會評估 PAC 檔案中的條件。根據該評估，瀏覽器不會將要求轉送至 Proxy，而是將其直接傳送到 GlobalProtect 應用程式。
- GlobalProtect 注意到 **internal-app.corp.com** 列示在 **Include Domain**（包含網域）中，並透過 VPN 通道傳送。
- GlobalProtect 會根據 GlobalProtect 中的設定選項將要求傳送到 **internal-app.corp.com** 中的資源。

您可能想要設定某些資源 (例如登入資源)，以便其不會使用明確 Proxy 或 GlobalProtect 或第三方 VPN 進行處理。下圖顯示了使用者透過從瀏覽器輸入 **login.microsoftonline.com** 登入 Microsoft Online。




 ©2025 Palo Alto Networks, Inc.

- PAC 檔案具有下列設定，以允許 **internal-app.corp.com** 略過明確 Proxy 流量。

```
   /* Bypass internal URL */ if (shExpMatch(host,
"login.microsoftonline.com")) return "DIRECT";
```

- 當行動使用者從其瀏覽器要求 **login.microsoftonline.com** 時，PAC 檔案會評估來自行動使用者端點中 PAC 檔案的要求，然後將其傳送至 GlobalProtect VPN 設定（此情況下的 GlobalProtect) 進行處理。
- GlobalProtect 應用程式注意到 **login.microsoftonline.com** 列示在 **Exclude Domain**（排除網域）中。
- GlobalProtect 會略過 VPN，並根據 GlobalProtect 中的設定選項將要求直接傳送到網際網路。

## 明確 Proxy 和 GlobalProtect：設定它

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

為了讓您的行動使用者安全連線，您可以結合明確 Proxy 與 GlobalProtect 或第三方 VPN。

- 明確 Proxy 和 GlobalProtect
  - 在分割通道模式下使用 GlobalProtect，僅提供對私人應用程式的安全存取。
  - 使用明確 Proxy 來保護公用應用程式，包括網際網路流量和外部 SaaS 應用程式。
- 明確 Proxy 和第三方 VPN
  - 使用 VPN 用戶端，存取資料中心和私人應用程式，並安全存取私人應用程式。
  - 使用明確 Proxy 和 PAC 檔案來保護對公用應用程式的存取。

在確定您應該使用明確 Proxy，以及使用 GlobalProtect 或第三方 VPN 保護哪些應用程式或流量之前，應該瞭解 GlobalProtect 和 Prisma Access 如何根據明確 Proxy 和 VPN 設定做出其轉送決策。

當行動使用者要求私人或網際網路型資源或應用程式時，此要求會傳送至安裝在端點上的明確 Proxy PAC 檔案。

- PAC 檔案中指定為 return "DIRECT" 的流量；略過明確 Proxy 處理。與 return "DIRECT" 搭配使用的 DNS 解析（主機）；允許指定的 IP 透過明確 Proxy 處理。
- 在 PAC 檔案中指定為 return "PROXY sitename:8080"; 的流量會轉送到明確 Proxy。

在處理流量之後，該流量會根據 PAC 檔案和 VPN 處理，傳送到 GlobalProtect、導向到網際網路，或者傳送到明確 Proxy。

PAC 檔案具有設定，以允許 "internal-app.corp.com" 略過明確 Proxy。當行動使用者從其瀏覽器要求 "internal-app.corp.com" 時，瀏覽器會評估 PAC 檔案中的條件。GlobalProtect 注意到 "internal-app.corp.com" 列示在包含網域中，並透過 VPN 通道傳送。GlobalProtect 會根據 GlobalProtect 中的設定選項將要求傳送到 "internal-app.corp.com" 中的資源。


©2025 Palo Alto Networks, Inc.

- Strata Cloud Manager
- Panorama

明確 **Proxy** 和 **GlobalProtect**：設定它 （**Strata Cloud Manager**）

若要透過明確 Proxy 實作 GlobalProtect—行動使用者，請完成下列步驟。

這些設定步驟對您的網路環境做出以下假設；如果您的網路環境不同，設定可能會有所不同：

- 行動使用者能夠連線並解析 GlobalProtect 入口網站主機名稱、閘道 FQDN、明確 Proxy URL 和 PAC 檔案 URL。

  您可以在這裡找到此資訊：

  - **GlobalProtect** 閘道 **FQDN** 和入口網站主機名稱

    # 前往 **Workflows(**工作流程**) > Prisma Access Setup**（設定） **> GlobalProtect > Infrastructure**（基礎結構），並編輯 **Infrastructure Settings**（基礎結構設定）。
  - 明確 **Proxy URL** 和 **PAC** 檔案 **URL**

    # 前往 **Workflows(**工作流程**) > Prisma Access Setup**（設定） **> Explicit Proxy**（明確 **Proxy**） **> Infrastructure**（基礎結構），並編輯 **Infrastructure Settings**（基礎結構設定）。
- 行動使用者能夠解析來自 GlobalProtect 的內部網域。

**STEP 1 |** 確定要將哪些應用程式傳送到 GlobalProtect，以及要將哪些應用程式傳送到明確 Proxy。

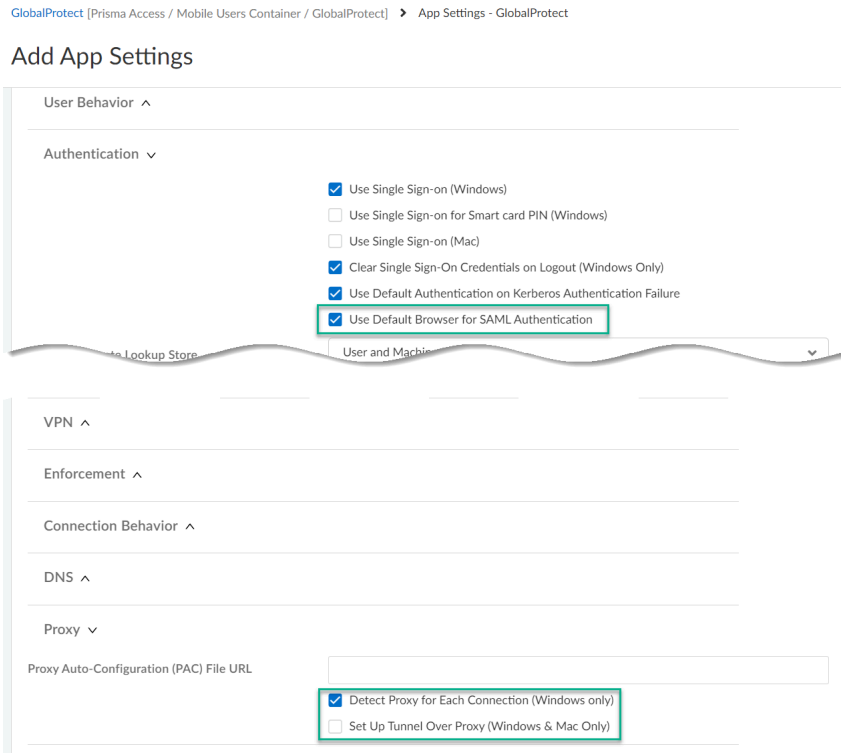
以下步驟會將資料中心託管的私人應用程式導向到 GlobalProtect，並將對網際網路和公用 SaaS 應用程式的要求導向到明確 Proxy。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 編輯 GlobalProtect 入口網站設定。

前往 **GlobalProtect** > **App Settings**（應用程式設定） > **App Configuration**（應用程式設定） > **Advanced Settings**（進階設定）

1. 在 **Proxy** 設定中：
   - 核取 **Detect Proxy for Each Connection**（偵測每個連線的 **Proxy**）
   - 清除 **Set Up Tunnel Over Proxy (Windows & Mac Only)**透過 **Proxy** 設定通道（僅限 **Windows** 和 **Mac**）
2. 在 **Authentication**（驗證）設定中：
   - 核取 **Use Default Browser for SAML Authentication**（使用預設瀏覽器進行 **SAML** 驗證）




**STEP 3 |** 在 GlobalProtect 中建立分割通道，允許您將內部流量導向至 GlobalProtect。

前往 **GlobalProtect** > **Tunnel Settings**（通道設定） > **Split Tunneling**（分割通道）。根據網域 (FQDN)、存取路由或應用程式設定分割通道。

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 設定 PAC 檔案以排除您為 GlobalProtect 分割通道指定的網域。

若要下載 PAC 檔案，以便可以進行編輯，請前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Explicit Proxy**（明確 **Proxy**） > **Infrastructure**（基礎結構） > **Infrastructure Settings**（基礎結構設定） > **Proxy Auto Configuration**（**Proxy** 自動設定）。

以下範例顯示了一個 PAC 檔案，其中 URL 託管略過內部 Proxy 的私人應用程式 (internal-app.corp.com)。以下 PAC 檔案中的參數均為範例值：

- 入口網站主機名稱為 `splittunnel.gpcloudservice.com`。
- 行動使用者閘道包含在萬用字元 FQDN`*examplegateways.gw.gpcloudservice.com` 中。
- TPAC 檔案 URL 為 `https://pacfileurl.pac`。
- `internal-app.corp.com` 正在託管受行動使用者—GlobalProtect 保護的私人應用程式。
- Okta 用於 SAML 驗證。
- 明確 Proxy URL 為 `example.proxy.prismaacess.com`。

```
function FindProxyForURL(url, host) { /* Bypass FTP */ if
 (url.substring(0,4) == "ftp:") return "DIRECT"; /* Bypass
 the Prisma Access Portal Hostname */ if (shExpMatch(host,
 "*.splittunnel.gpcloudservice.com")) return "DIRECT"; /*
 Bypass the Prisma Access Gateway */ if (shExpMatch(host,
 "*examplegateways.gw.gpcloudservice.com")) return "DIRECT"; /*
 Bypass the Prisma Access PAC File URL */ if (shExpMatch(host,
 "https://pacfileurl.pac")) return "DIRECT"; /* Bypass the URLs
 Being Sent to the GlobalProtect Portal */ if (shExpMatch(host,
 "*.internal-app.corp.com")) return "DIRECT"; /* Bypass ACS
 */ if (shExpMatch(host, "*.acs.prismaaccess.com")) return
 "DIRECT"; /* Forward to Prisma Access */ return "PROXY
 example.proxy.prismaaccess.com:8080"; }
```

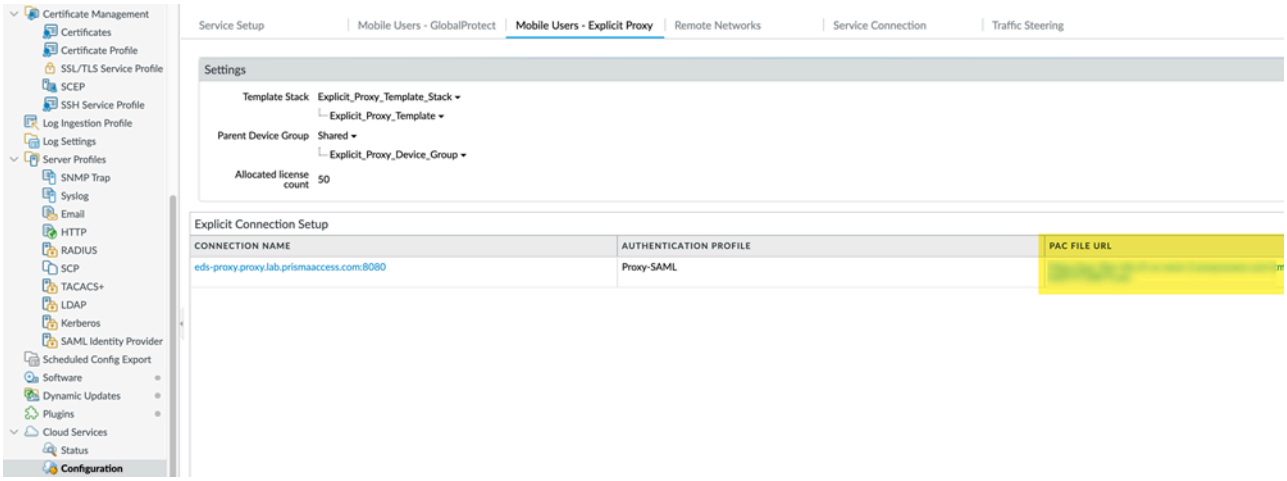
明確 **Proxy** 和 **GlobalProtect**：設定它 （**Panorama**）

若要透過明確 Proxy 實作 GlobalProtect—行動使用者，請完成下列步驟。

這些設定步驟對您的網路環境做出以下假設；如果您的網路環境不同，設定可能會有所不同：

 ©2025 Palo Alto Networks, Inc.

- 行動使用者能夠連線並解析 GlobalProtect 入口網站主機名稱、閘道 FQDN、明確 Proxy URL 和 PAC 檔案 URL。
  - 若要尋找閘道 FQDNS，請選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Mobile Users—GlobalProtect**（行動使用者—**GlobalProtect**） > **Gateways**（閘道）。
  - 若要尋找 **PAC File URL**（**PAC** 檔案 **URL**），請選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users—Explicit Proxy**（行動使用者—**Explicit Proxy**） > **PAC File URL**（**PAC** 檔案 **URL**）。




- 行動使用者能夠解析來自 GlobalProtect 的內部網域。

**STEP 1 |** 規劃您的行動使用者—明確 Proxy 部署和您的 GlobalProtect 部署（您的行動使用者—GlobalProtect 或獨立 GlobalProtect 部署）。

**STEP 2 |** 確定要將哪些應用程式傳送到 GlobalProtect，以及要將哪些應用程式傳送到明確 Proxy。

以下步驟會將資料中心託管的私人應用程式導向到 GlobalProtect，並將對網際網路和公用 SaaS 應用程式的要求導向到明確 Proxy。

**STEP 3 |** 在管理 Prisma Access 的 Panorama 中，設定 GlobalProtect 入口網站設定。

1. 選取 **Network**（網路） > **GlobalProtect** > **Portals**（入口網站）。

   確定您在來自 **Template**（範本）下拉式清單的 **Mobile_User_Template** 中。
2. 選取 **GlobalProtect_Portal** 以編輯 Prisma Access 入口網站設定。
3. 選取 **Agent**（代理程式）頁籤，然後選取 **DEFAULT**（預設）設定或 **Add**（新增）設定。
4. 選取 **App**（應用程式）頁籤。
5. 進行下列應用程式設定變更：
   - 在 **Detect Proxy for Each Connection**（偵測每個連線的 **Proxy**）中，選取 **Yes**（是）。
   - 在 **Set Up Tunnel Over Proxy (Windows & Mac Only)**（透過 **Proxy** 設定通道（僅限 **Windows** 和 **Mac**））中，選取 **No**（否）。
   - 在 **Use Default Browser for SAML Authentication**（使用預設瀏覽器進行 **SAML** 驗證）中，選取 **Yes**（是）。

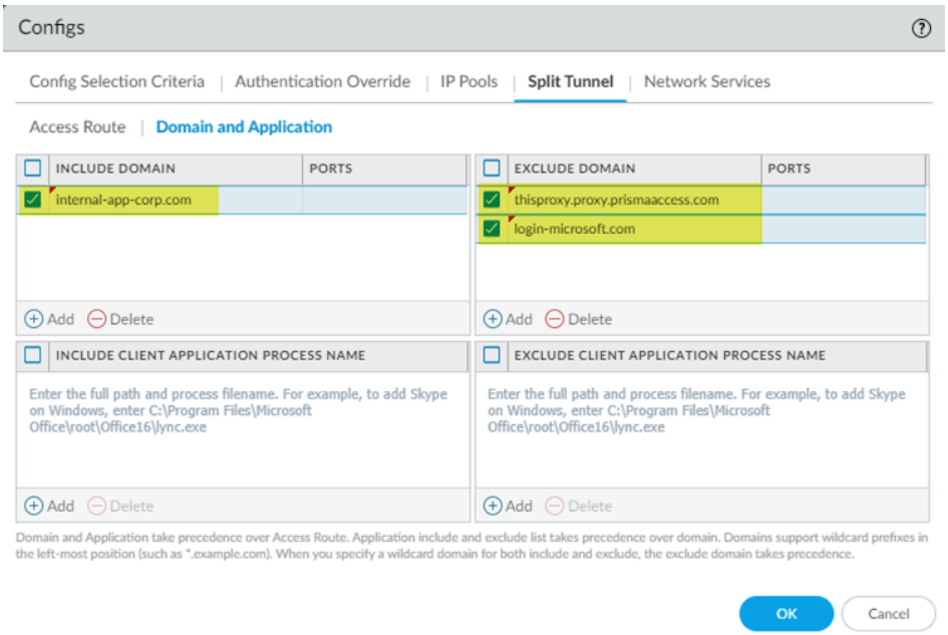
 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 在 GlobalProtect 中建立分割通道，允許您將內部流量導向至 GlobalProtect。

下列範例使用分割通道，根據網域 (FQDN) 導向流量；您也可以根據流量的存取路由設定分割道道。

1. 當您仍處於 GlobalProtect 代理程式設定（**Network**（網,路） > **GlobalProtect** > **Gateways**（閘道） > **GlobalProtect External Gateway**（**GlobalProtect** 外部閘道）)中時，請選取 **Agent**（代理程式） > **Client Settings**（用戶端設定）。
2. 選取 **DEFAULT**（預設）設定或 **Add**（新增）一個。
3. 選取 **Split Tunnel**（分割通道） > **Domain and Application**（網域和應用程式）。
4. **Add**（新增） **Include Domain**（包含網域），並選擇性地新增 **Ports**（連接埠），與網域搭配使用。

   此範例使用 internal-app.corp.com 作為您用來在資料中心中託管應用程式的 URL。您可以在 **Exclude Domain**（排除網域）中新增此 URL 和 SAML 驗證 URL。




5. 按一下 **OK**（確定）儲存您的變更。
6. **Commit and Push**（提交並推送）您的變更。

**STEP 5 |** 設定 PAC 檔案以排除您為分割通道輸入的網域。

以下範例顯示了一個 PAC 檔案，其中 URL 託管略過內部 Proxy 的私人應用程式 (internal-app.corp.com)。以下 PAC 檔案中的參數均為範例值：

- 入口網站主機名稱為 `splittunnel.gpcloudservice.com`。
- 行動使用者閘道（**Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Mobile Users—GlobalProtect**（行動使用者

 ©2025 Palo Alto Networks, Inc.

—**GlobalProtect**） > **Gateways**（閘道））包含在萬用字元 FQDN * `examplegateways.gw.gpcloudservice.com` 中。

- **PAC File URL**（**PAC** 檔案 **URL**）（**Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users**—**Explicit Proxy**（行動使用者—明確 **Proxy**） > **PAC File URL**（**PAC** 檔案 **URL**））是 `https://pacfileurl.pac`。
- `internal-app.corp.com` 正在託管受行動使用者—GlobalProtect 保護的私人應用程式。
- Okta 正在用於 SAML 驗證。
- 明確 Proxy URL 是 `example.proxy.prismaacess.com`。

```
function FindProxyForURL(url, host) { /* Bypass FTP */ if
 (url.substring(0,4) == "ftp:") return "DIRECT"; /* Bypass
 the Prisma Access Portal Hostname */ if (shExpMatch(host,
 "*.splittunnel.gpcloudservice.com")) return "DIRECT"; /*
 Bypass the Prisma Access Gateway */ if (shExpMatch(host,
 "*examplegateways.gw.gpcloudservice.com")) return "DIRECT"; /*
 Bypass the Prisma Access PAC File URL */ if (shExpMatch(host,
 "https://pacfileurl.pac")) return "DIRECT"; /* Bypass the URLs
 Being Sent to the GlobalProtect Portal */ if (shExpMatch(host,
 "*.internal-app.corp.com")) return "DIRECT"; /* Bypass ACS
 */ if (shExpMatch(host, "*.acs.prismaaccess.com")) return
 "DIRECT"; /* Forward to Prisma Access */ return "PROXY
 example.proxy.prismaaccess.com:8080"; }
```

## 明確 Proxy 搭配第三方 VPN

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

若要使用第三方 VPN 搭配明確 Proxy，您必須能夠在網路中進行以下變更：

- 您必須設定第三方 VPN 以執行分割通道，將網際網路流量導向到明確 Proxy。

  如需設定第三方 VPN 的任何協助，請聯繫第三方 VPN 廠商。
- 修改 PAC 檔案，讓明確 Proxy 略過以下任何 VPN 元件：
  - 與第三方 VPN 相關聯的任何 IP 位址
  - 第三方 VPN 所需的任何登入 URL

在以下範例中，您已設定 PAC 檔案，以便明確 Proxy 可以使用私人 IP 位址略過內部資源，以及驗證流量。

```
++++++++++++++++ function FindProxyForURL(url, host) { if
 (isPlainHostName(host) || shExpMatch(host, "*.local")
 || isInNet(dnsResolve(host), "10.0.0.0", "255.0.0.0") ||
 isInNet(dnsResolve(host), "127.0.0.0", "255.255.255.0"))
 return "DIRECT"; /* Bypass SAML for AnyConnect Azure */
```

 ©2025 Palo Alto Networks, Inc.

```
if (shExpMatch(host, "login.microsoftonline.com")) return
"DIRECT"; if (shExpMatch(host, "login.windows.net")) return
"DIRECT"; if (shExpMatch(host, "login.microsoft.com"))
return "DIRECT"; /* Forward to Prisma Access */ return "PROXY
example.proxy.prismaaccess.com:8080"; }
```

## 明確 Proxy 使用者 - Proxy 部署的 IP 位址最佳化

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>如果您想在 Prisma Access 環境中使用此功能，請與您的帳戶團隊聯繫以瞭解更多資訊。 | • Prisma Access 5.2<br>• Prisma Access 資料平面 10.2.4<br>• Panorama 外掛程式 5.2.0 版 |

IP 位址最佳化是一組架構增強功能，可減少部署中的 IP 位址總數，進而簡化允許清單工作流程，同時提高彈性，並更快速地裝載 Prisma Access 租用戶。

**IP** 位址黏性

透過 IP 位址黏性，您可以保護 SaaS 應用程式和網站，而其需要使用者工作階段在整個使用者工作階段期間維護 Prisma Access 的相同輸出 IP 位址。

簡化 **SaaS** 應用程式裝載

新增 Prisma Access 位置或在現有 Prisma Access 位置遇到調整事件可能會導致將新的 IP 位址配置給您的明確 Proxy 部署。最佳做法是擷取新的輸出和閘道 IP 位址，並將其新增至 SaaS 應用程式的允許清單。IP 位址最佳化可減少您必須在大型部署中管理的 IP 位址數目。

疑難排解

如果要將特定應用程式設為目標，進行 IP 位址最佳化，您可以將它們新增到 URL 類別或外部動態清單 (EDL)。在您設定特殊物件之後，只有這些物件中包含的網域才會取得 IP 位址最佳化。

Panorama - 將 URL 類別設定為 **PANW EP IP** 親和性 **URL** 清單，或將 EDL 設定為 **PANW EP IP** 親和性清單。避免萬用字元項目（範例 **.***）或最上層網域（例如 **.com**）。

Strata Cloud Manager - 支援 URL 清單作為 **PANW EP** 親和性 **URL** 清單。

## 行動使用者—明確 Proxy 部署的 DNS 解析

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• 如果您想在 Prisma Access 環境中使用此功能，請與您的帳戶團隊聯繫以瞭解更多資訊。 | ❑ Prisma Access 授權<br>❑ Prisma Access 5.2.0 版 |


©2025 Palo Alto Networks, Inc.

Prisma Access 可讓您指定 DNS 伺服器，以解析組織內部網域和外部網域。Prisma Access 根據您 DNS 伺服器的設定對 DNS 要求進行 Proxy。明確 Proxy 支援以下 DNS 功能：

- 使用第三方瀏覽器搭配明確 Proxy
- 使用每個區域 DNS 伺服器搭配 Prisma Access Browser

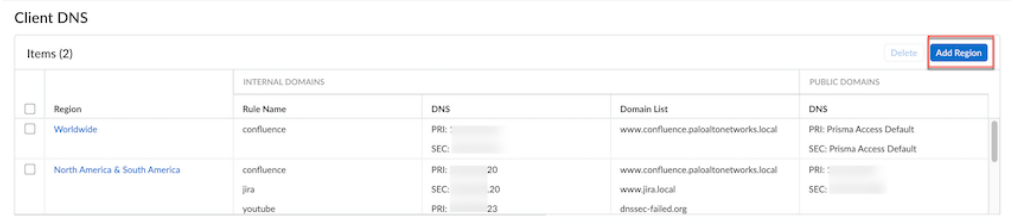
- 明確 *Proxy* 的 *DNS Proxy* 設定優先於 ***Prisma Access Setup***（***Prisma Access*** 設定）定義的內部 *DNS* 伺服器。
- 在啟用明確 *Proxy* 的 *DNS Proxy* 之後，您必須將現有的 *DNS* 設定從 ***Prisma Access Setup***（***Prisma Access*** 設定）> ***Internal DNS Servers***（內部 ***DNS*** 伺服器）移轉至 ***Workflows***（工作流程）> ***Prisma Access Setup***（***Prisma Access*** 設定）> ***Explicit Proxy***（明確 ***Proxy***）> ***Infrastructure Settings***（基礎結構設定）> ***DNS Proxy***

設定 **DNS** 設定

若要設定 DNS Proxy 設定，請完成以下步驟：

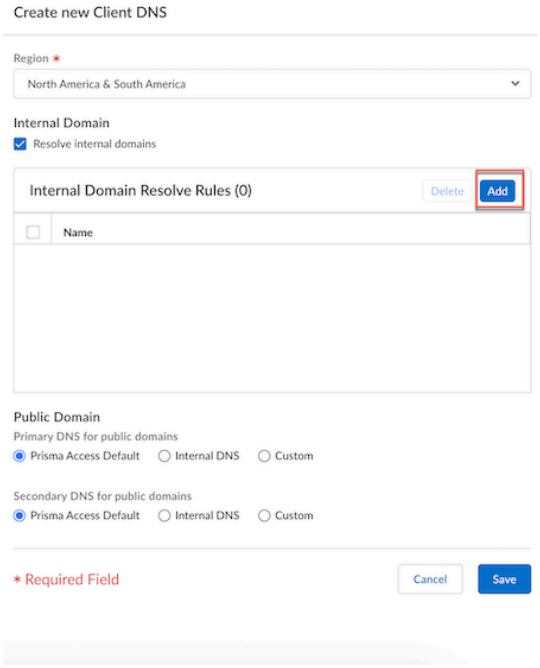
1. 新增明確 Proxy DNS 伺服器規則。
   1. 前往 **Workflows**（工作流程）> **Prisma Access Setup**（**Prisma Access** 設定）> **Explicit Proxy**（明確 **Proxy**）> **Infrastructure Settings**（基礎結構設定）。
   2. 按一下設定圖示，然後前往 **Client DNS**（用戶端 **DNS**）。
   3. **Add Region**（新增區域），並給與它唯一的名稱。
   4. 選取區域或位置，或者選取 **Worldwide**（全世界）。

      如果您指定多個 *Proxy* 設定，其中混合了 *[Worldwide*（全世界）*]* 和 *[theater*（劇院）*]* 設定，則 *Prisma Access* 會先使用位置群組的設定，接著是劇院，然後全世界。*Prisma Access* 從上到下評估清單中的規則。
   5. 新增 DNS 伺服器的 IP 位址。




 ©2025 Palo Alto Networks, Inc.

2. 選擇是否想要 Prisma Access **Resolve internal domains**（解析內部網域）；如果您想要的話，請 **Add**（新增）一或多個 **Internal Domain Resolve Rules**（內部網域解析規則）。



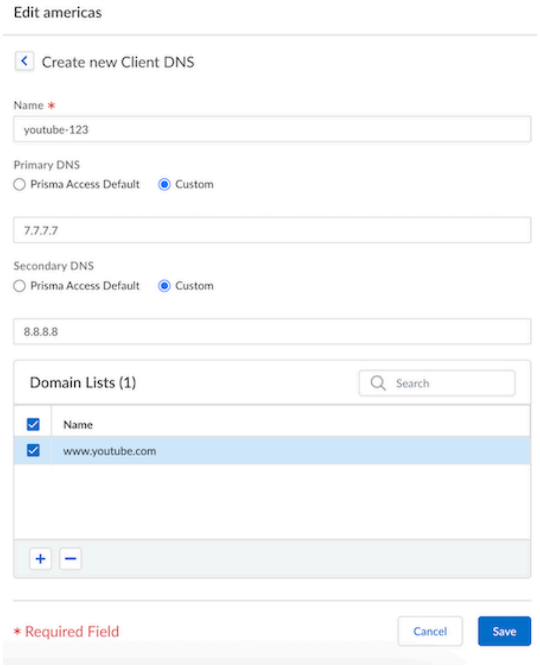

3. **Add**（新增）並定義 **Internal Domain Resolve Rules**（內部網域解析規則）。

   目前，僅 *Prisma Access Browser* 和代理程式 *Proxy* 支援***Internal Domain Resolve Rules***（內部網域解析規則）。

4. 新增規則的唯一 **Name**（名稱），並在 **Primary DNS**（主要 **DNS**）和 **Secondary DNS**（次要 **DNS**）下新增自訂 IP 位址。
5. 選取 **Prisma Access Default**（**Prisma Access** 預設），使用預設 Prisma Access DNS 伺服器以解析內部網域。如果您想要內部 DNS 伺服器僅解析您指定的網域，請在 **Domain List**（網域清單）中輸入要解析的網域。


©2025 Palo Alto Networks, Inc.

6. 如果您有 **Custom**（自訂）DNS 伺服器可存取您的內部網域，請指定 **Primary DNS**（主要 **DNS**）和 **Secondary DNS**（次要 **DNS**）伺服器 IP 位址。




7. 如果您想要內部 DNS 伺服器僅解析您指定的網域，請在 **Domain Lists**（網域清單）中輸入要解析的網域。在網域前面指定一個星號；例如，*.acme.com。。按一下 **Save**（儲存）。
8. **Push Config**（推送設定）以儲存並推送您的設定變更。


©2025 Palo Alto Networks, Inc.

# 檢視使用者至 IP 位址或使用者群組對應

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Panorama Managed Prisma Access | • Prisma Access 授權 |

Prisma Access 洞察讓您即時檢視行動使用者的使用者至 IP 位址對應或使用者至群組對應。對於遠端網路和服務連線，您可以檢視使用者至使用者群組對應。

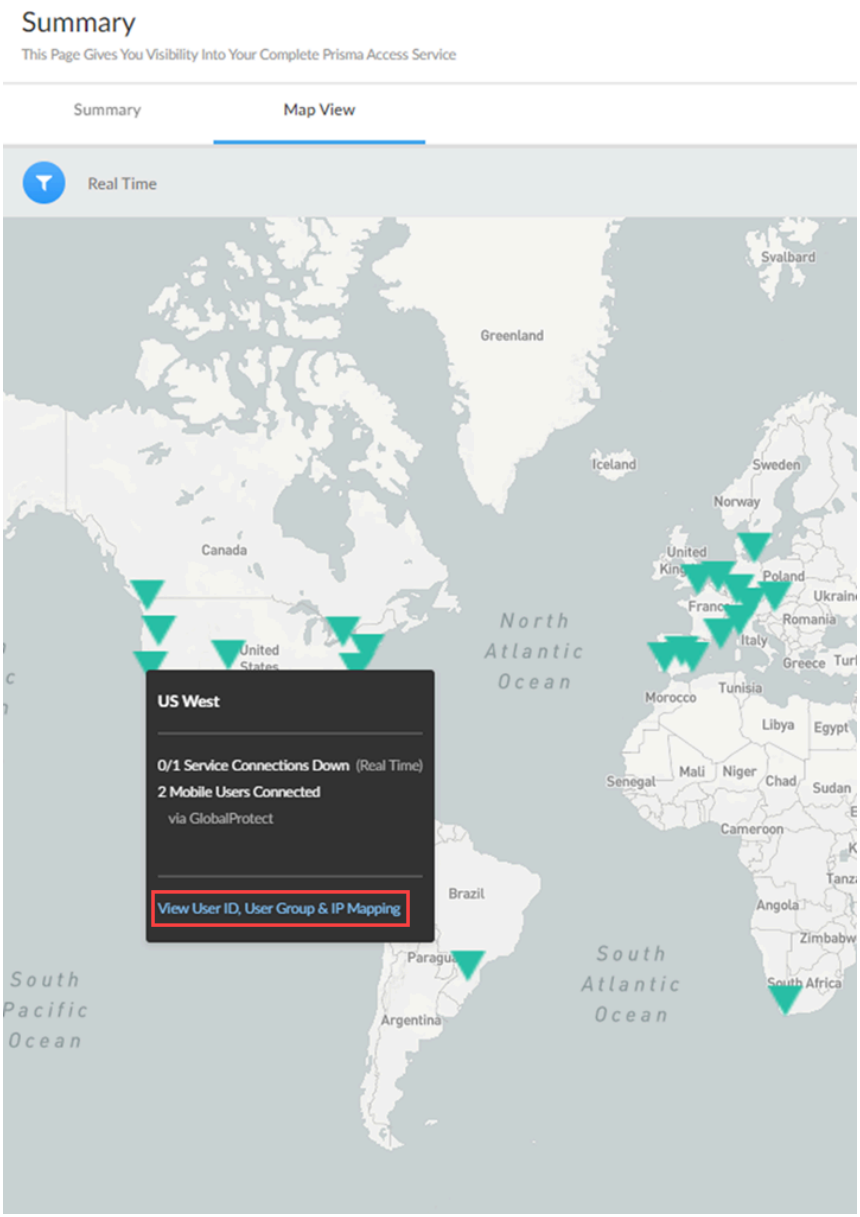
地圖上的倒三角形是以顏色編碼方式來指示 Prisma Access 位置狀態：

- 綠色：所有執行個體都已啟動。
- 紅色：所有執行個體都已關閉。
- 黃色：執行個體是已啟動、已關閉和未知的組合，可能需要您注意。
- 灰色：所有執行個體都是未知的。

**STEP 1 |** 從 **Summary**（摘要）儀表板中，選取 **Map View**（地圖檢視）。


©2025 Palo Alto Networks, Inc.

**STEP 2 |** 將游標暫留在在某個位置上，直到快顯對話方塊出現。




**STEP 3 |** 從對話方塊中選取 **View User ID, User Groups & IP Mapping**（檢視使用者 **ID**、使用者群組和 **IP** 對應）。**UserID and User Group Distribution Check**（使用者 **ID** 和使用者群組散佈檢查）對話方塊即會開啟。

**STEP 4 |** 選取 **Prisma Access Location**（位置）和 **Node Type**（節點類型）。當 **Node Type**（節點類型）為 **Mobile Users (GlobalProtect)**（行動使用者 **(GlobalProtect)**）時，**Prisma Access Location filter**（位置篩選器）不會納入考慮。

對於遠端網路和服務連線，您只能看到使用者 ID 至使用者群組對應。

1. 選取 **Prisma Access Location**（**Prisma Access** 位置）。如果您選取的 Prisma Access 位置沒有任何相關聯的遠端網路或服務連線，則您會在 **Remote Networks Site**（遠端網站）欄位或 **Service Connections Site**（服務連線網站）欄位中看到「No Data Available（無可用


©2025 Palo Alto Networks, Inc.

資料）」訊息（視情況而定），並且 **Show User Groups**（顯示使用者群組）和 **Export to CSV**（匯出至 **CSV**）按鈕已停用。

2. 從 **Node Type**（節點類型）中，選取遠端網路或服務連線。
3. 從 **Remote Networks Site**（遠端網站）或 **Service Connections Site**（服務連線網站）欄位中，選取您想要從中擷取資料的網站。
4. 在檢視中，選取您想要查看使用者 ID 屬於哪個使用者群組（使用者），或哪些使用者是與該網站相關聯的特定群組（群組）的一部分。

   - 如果您選取 **User**（使用者），請輸入使用者的 **User ID**（使用者 **ID**）（例如，saas\testuser3），以取得使用者 ID 至使用者群組對應，然後選取 **Show User Groups**（顯示使用者群組）。使用者 ID 所屬之所有群組的清單顯示在 **User ID-IP Mappings**（使用者 **ID-IP** 對應）下。

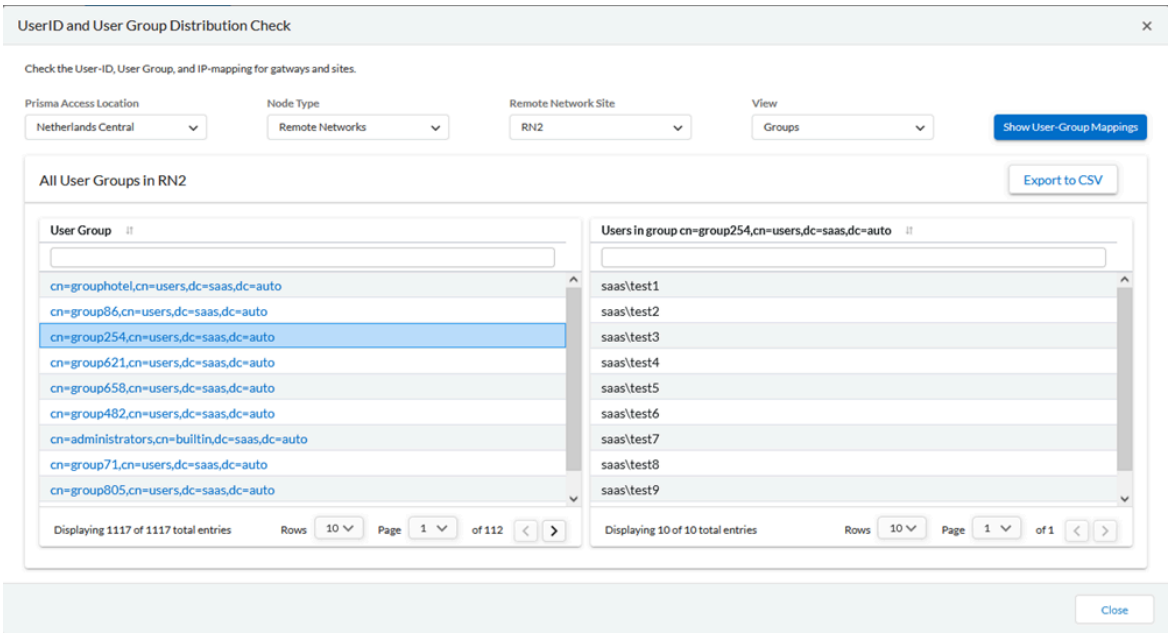
     您可以透過輸入群組名稱或包含在您要尋找的群組名稱內的字串來搜尋特定群組，方法是在 **User Group**（使用者群組）文字方塊中輸入它。如果您搜尋一個不存在的群組，您會看到一個錯誤，顯示「No data is available（沒有可用的資料）」。您也可以透過切換 **User Group**（使用者群組）旁邊的箭頭圖示來排序群組清單。您可以選取要顯示的項目數目，也可以透過按一下向前和向後箭頭來翻頁。

     如果您選取 **Groups**（群組），選取 **Show User-Group Mappings**（顯示使用者-群組對應）會在 **All User Groups in *<selected_site>***（***<selected_site>*** 中的所有使用者群組）下顯示網站中所有可用的群組。如果您選取一個群組，則所有屬於該群組的使用者會顯示在右側窗格中。**Export to CSV**（匯出至 **CSV**）按鈕即會變成啟動狀態，而且您可以將屬於該群組的所有使用者匯出至 CSV 檔案。匯出的 CSV 檔案包含該群組的所有項目，即使它們在匯出時未顯示在 UI 中也一樣。

     您可以透過輸入群組名稱或包含在您要尋找的群組名稱內的字串來搜尋特定群組，方法是在 **User Group**（使用者群組）文字方塊中輸入它。如果您搜尋一個不存在的群組，您會看到一個錯誤，顯示「No data is available（沒有可用的資料）」。您也可以透過切換


©2025 Palo Alto Networks, Inc.

**User Group**（使用者群組）旁邊的箭頭圖示來排序群組清單。您可以選取要顯示的項目數目，也可以透過選取向前和向後箭頭來翻頁。




**Node Type**（節點類型）：**Mobile Users (GlobalProtect)**（行動使用者 **(GlobalProtect)**）

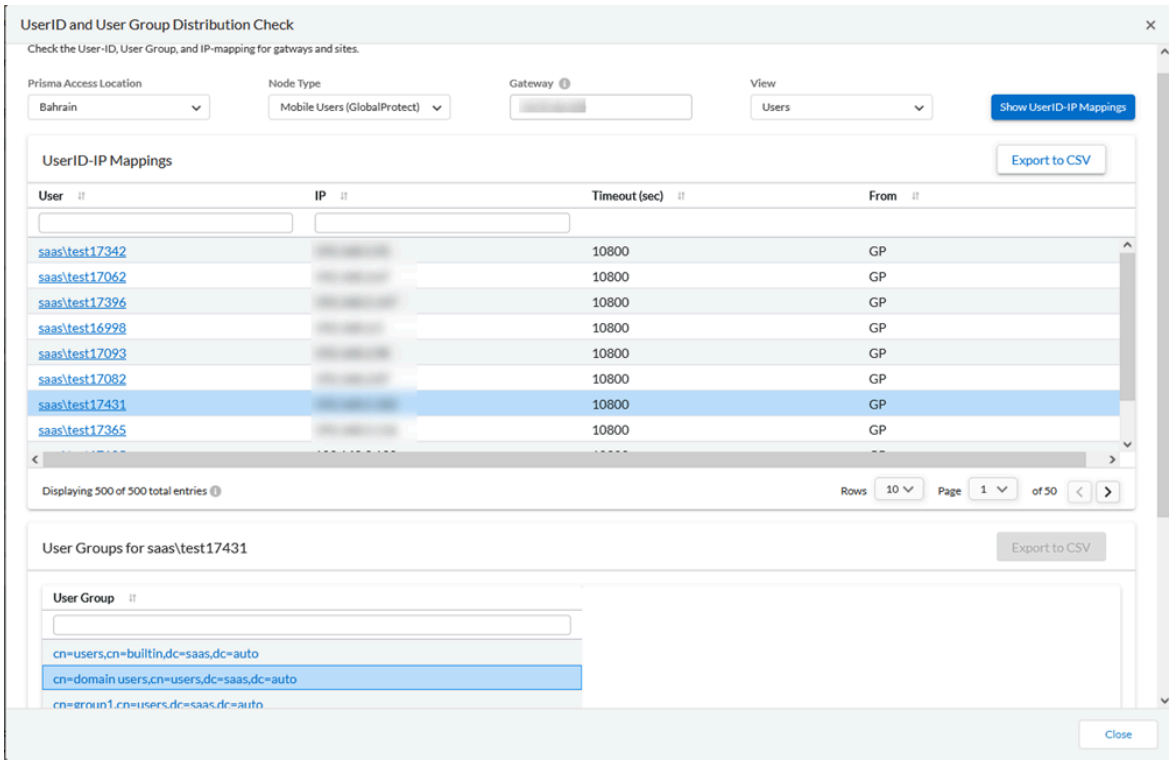
您可以查看使用者 ID 至 IP 對應，以及使用者 ID 至使用者群組對應。當選取的 **Node Type**（節點類型）為 **Mobile Users (GlobalProtect)**（行動使用者 **(GlobalProtect)**）時，**Prisma Access Location**（**Prisma Access** 位置）篩選器不會納入考慮。相反，Prisma Access 洞察會使用 GlobalProtect 閘道 IP 位址來尋找資料。

1. 在 **Gateway**（閘道）文字方塊中輸入 GlobalProtect IP 閘道位址。
2. 選取您是否要為連線到所指定 GlobalProtect 閘道的使用者 **View**（檢視）使用者 ID 至使用者 IP 對應（**Users**（使用者））或使用者 ID 至使用者群組對應（**Groups**（群組））。

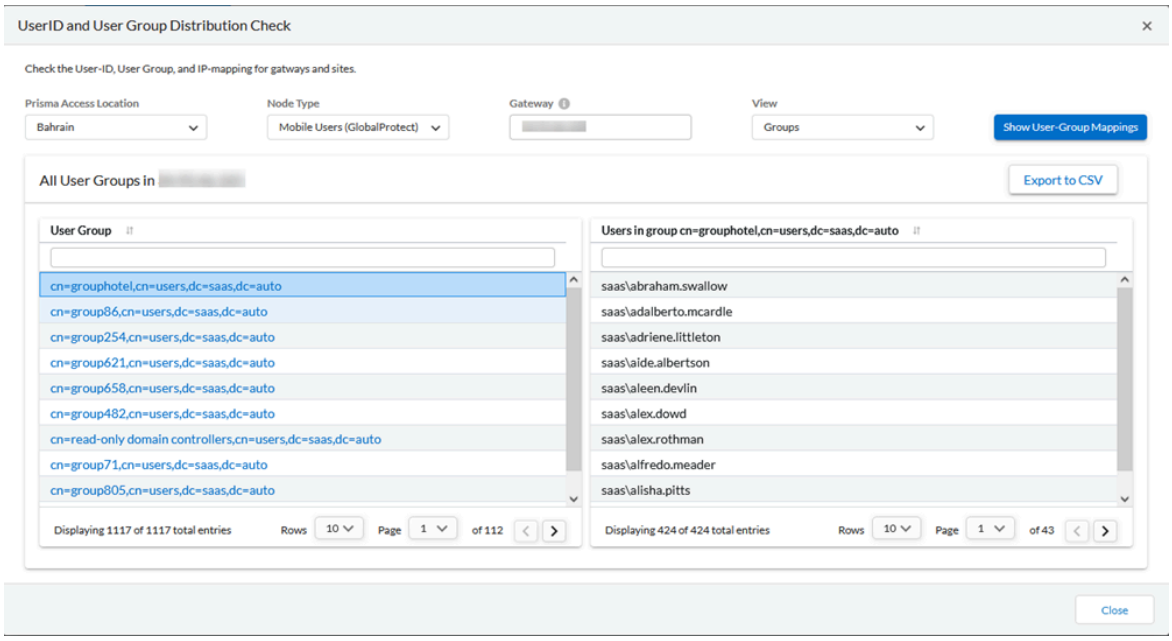
   如果您選取了 **Users**（使用者），請選取 **Show UserID-IP Mappings**（顯示使用者 **ID-IP** 對應）。即會顯示使用者 ID 至其使用者 IP 對應的表格，以及 **Timeout**（逾時），其中為您顯示使用者 ID 至使用者 IP 項目的有效時間（以秒為單位）。選取特定使用者會顯示該使用者所屬的群組。選擇一個群組會顯示所有屬於該群組的使用者。它也會啟用 **Export to**


©2025 Palo Alto Networks, Inc.

**CSV**（匯出至 **CSV**）按鈕，讓您可以匯出該群組中的所有使用者，而不管 UI 中顯示的任何篩選檢視。




如果您選取了 **Groups**（群組），請選擇 **Show User-Group Mappings**（顯示使用者-群組對應）。屬於該 GlobalProtect 閘道的所有使用者群組的清單會出現在 **User Group**（使用者群組）之下。選取一個使用者群組會在右側窗格中顯示所有屬於該群組的使用者。它也會啟用 **Export to CSV**（匯出至 **CSV**）按鈕，讓您可以匯出該群組中的所有使用者，而不管 UI 中顯示的任何篩選檢視。



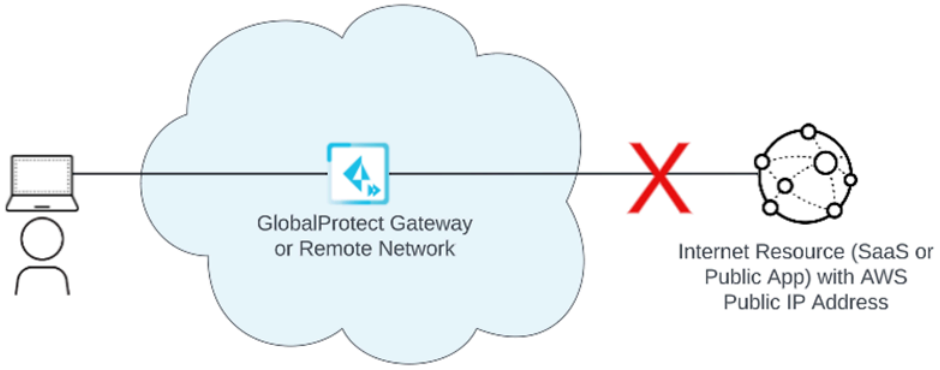

 ©2025 Palo Alto Networks, Inc.

# 報告行動使用者網站存取問題

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

有些網站，例如 stubhub.com、ticketmaster.com 或 dollartree.com，會封鎖來自 AWS 雲端 IP 位址範圍的流量。當 Prisma Access 保護的使用者嘗試存取這些網站時，他們的存取可能遭拒，而 Web 瀏覽器上會出現下列訊息：

```
拒絕存取。您沒有在此伺服器上存取 "http://www.dollartree.com/" 的權限。Reference #18.7f955b8.1509600370.44eb7c8
```




若要報告此問題，請從 Web 瀏覽器輸入 https://reportasite.gpcloudservice.com/，並提供無法存取的網站的 URL。在 24-48 小時後，返回 https://reportasite.gpcloudservice.com/ 並輸入相同的 URL 以查看其狀態。

Palo Alto Networks 會為您提供 URL 使用的 IP 位址；在某些情況下，您必須將此 IP 位址新增至組織的允許清單，以便此流量不會變成黑洞。如果您有重新導向的 URL，請將以下 IP 位址新增至您的允許清單：

- 65.154.226.160
- 154.59.126.110
- 66.232.36.110

**Prisma Access URL 重新導向程序**

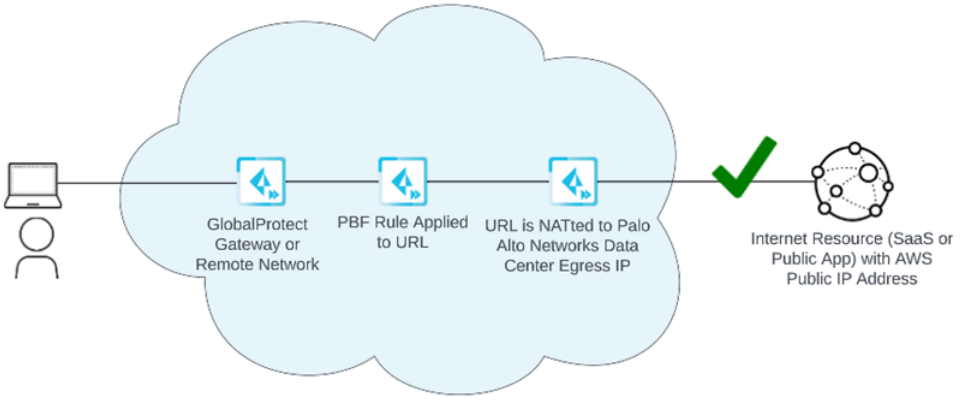
有些網站會封鎖來自雲端 IP 位址範圍的流量。當 Prisma Access 保護的使用者嘗試存取這些網站時，他們的存取可能遭拒。為了確保還原對這些網站的存取，Palo Alto Networks 會檢閱所有這類報告的網站，如果發現存取問題，則會對該網站進行分類，並新增一個輸出政策，透過 NAT 將 IP


©2025 Palo Alto Networks, Inc.

位址轉譯為可存取的網站。Palo Alto Networks 會徹底檢閱這些網站以確定其信譽，而且僅信譽良好的網站才會新增到輸出規則中，而其他網站則會遭到拒絕，使用以下程序：

1. 您使用 https://reportasite.gpcloudservice.com/ 通知我們出現存取問題的 URL。
2. 網站可靠性工程 (SRE) 自動化會檢閱 URL。
3. 如果 SRE 確定 URL 是安全的，則基於政策的轉送 (PBF) 規則會套用至 URL 及其父網域。
4. 流量會透過 Prisma Access 從 GlobalProtect 閘道或遠端網路路由至 URL 處理中樞（其中 PBF 規則會套用至網域），以及從中樞路由至 Palo Alto Networks 資料中心。
5. 當流量從資料中心輸出時，URL 會透過來源 NAT 轉譯為資料中心的 IP 位址。

由於這些動作，不會丟棄往返 SaaS 應用程式的流量，因為資料中心 IP 位址的信譽良好。





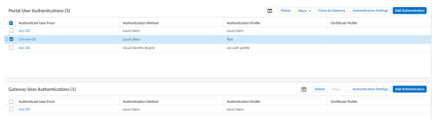
©2025 Palo Alto Networks, Inc.

# 啟用行動使用者對 Prisma Access 進行驗證

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

您可以使用任何支援的驗證類型，對 Prisma Access 驗證行動使用者。請遵循以下步驟，為 GlobalProtect 或明確 Proxy 行動使用者設定驗證。

**STEP 1 |** 前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定），然後前往您的 行動使用者：GlobalProtect 或 明確 Proxy 設定，並 **Set Up User Authentication**（設定使用者驗證）。



**STEP 2 |** 從支援的驗證類型中選擇您的 **Authentication Method**（驗證方法）。

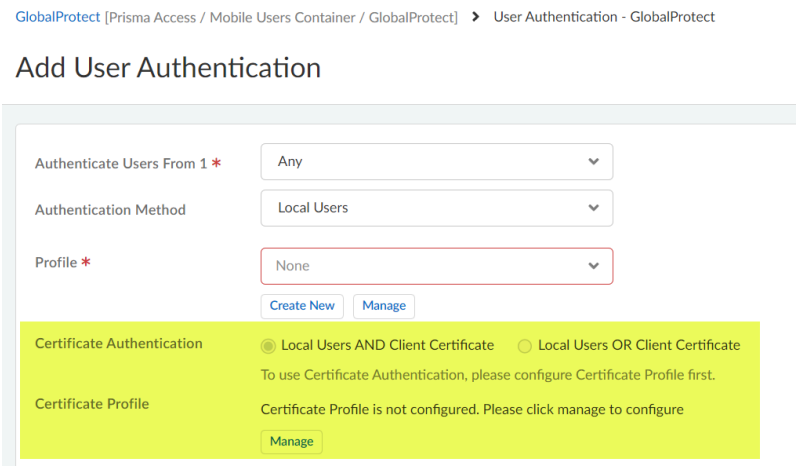
如果您還沒有整合 Prisma Access 與驗證服務，方法如下。

**STEP 3 |** 選擇您已設定的驗證 **Profile**（設定檔），以啟用 Prisma Access 連線到您要用來驗證使用者的服務。

- 如果您在步驟 2 中使用了 SAML，請指定 SAML 驗證 **Profile**（設定檔），或建立新的 SAML 驗證設定檔，與 Prisma Access 搭配使用。
- 如果您在步驟 2 中使用了 CIE，請指定 CIE 驗證 設定文件，或 建立新的 Kerberos 驗證設定檔，與 Prisma Access 搭配使用。
- 如果您在步驟 2 中使用了 Kerberos，請指定 Kerberos 驗證 設定文件，或 建立新的 CIE 驗證設定檔，與 Prisma Access 搭配使用。


©2025 Palo Alto Networks, Inc.

**STEP 4 |** 指定憑證驗證設定：




- 憑證驗證

  為了增強安全性，請使用憑證（除了您的驗證服務之外）來取得使用者名稱並對 Prisma Access 驗證使用者。若要根據用戶端憑證驗證使用者，其中一個憑證欄位（如主旨名稱欄位）必須識別使用者名稱。透過用戶端憑證驗證成功驗證的行動使用者無法選擇退出 GlobalProtect 應用程式。

  透過 Prisma Access，您可以選擇要求行動使用者同時通過憑證驗證和基於驗證類型的驗證，或者只要行動使用者成功通過其中一項檢查，就授予他們存取權限。

- 憑證設定檔

  使用選用的憑證設定檔，來驗證行動使用者透過連線要求呈現給 Prisma Access 的憑證。憑證設定當指定使用者名稱和使用者網域欄位內容；列出 CA 憑證；封鎖工作階段條件；並提供確定 CA 憑證撤銷狀態的方法。因為憑證是行動使用者驗證的一部分，所以您必須在使用者初次登入之前將憑證設定檔中使用的憑證預先部署到該使用者。如果憑證設定檔指定 [Username Field] 中的 [主旨]，端點所出示的憑證必須包含通用名稱才能讓端點連線。如果憑證設定檔指定了電子郵件或主體名稱作為使用者名稱欄位的 Subject-Alt，則憑證必須包含對應欄位，當 GlobalProtect 應用程式對 Prisma Access 進行驗證時，這些欄位將用作使用者名稱。

**STEP 5 |** 為儲存使用者驗證認證的 Cookie 指定 **Cookie Lifetime**（**Cookie** 存留時間）。

在 IdP 驗證使用者之後，Prisma Access 將在驗證快取服務 (ACS) 中儲存使用者的驗證狀態。驗證的有效期基於您在這裡指定的 **Cookie Lifetime**（**Cookie** 存留時間）值。

為了防止使用者在 Cookie 存留時間到期之前無法下載大型檔案，或者 Cookie 在使用者長時間存取單一網站時過期，Palo Alto Networks 建議您設定至少一天的 Cookie 存留時間。如果明確 Proxy 使用者遇到 Cookie 存留時間到期問題，他們可以瀏覽到其他網站，以重新向 ACS 進行驗證並重新整理 ACS Cookie。

## 驗證支援與功能

以下是與 Prisma Access 整合用以提供驗證的服務，以及您在規劃驗證設定時所應考量的功能：

驗證支援：

- 雲端識別引擎

 ©2025 Palo Alto Networks, Inc.

- SAML
- TACACS+
- RADUIS
- LDAP
- Kerberos
- MFA
- 本機資料庫驗證

驗證功能重點：

- SSO
- 驗證入口網站
- 驗證順序

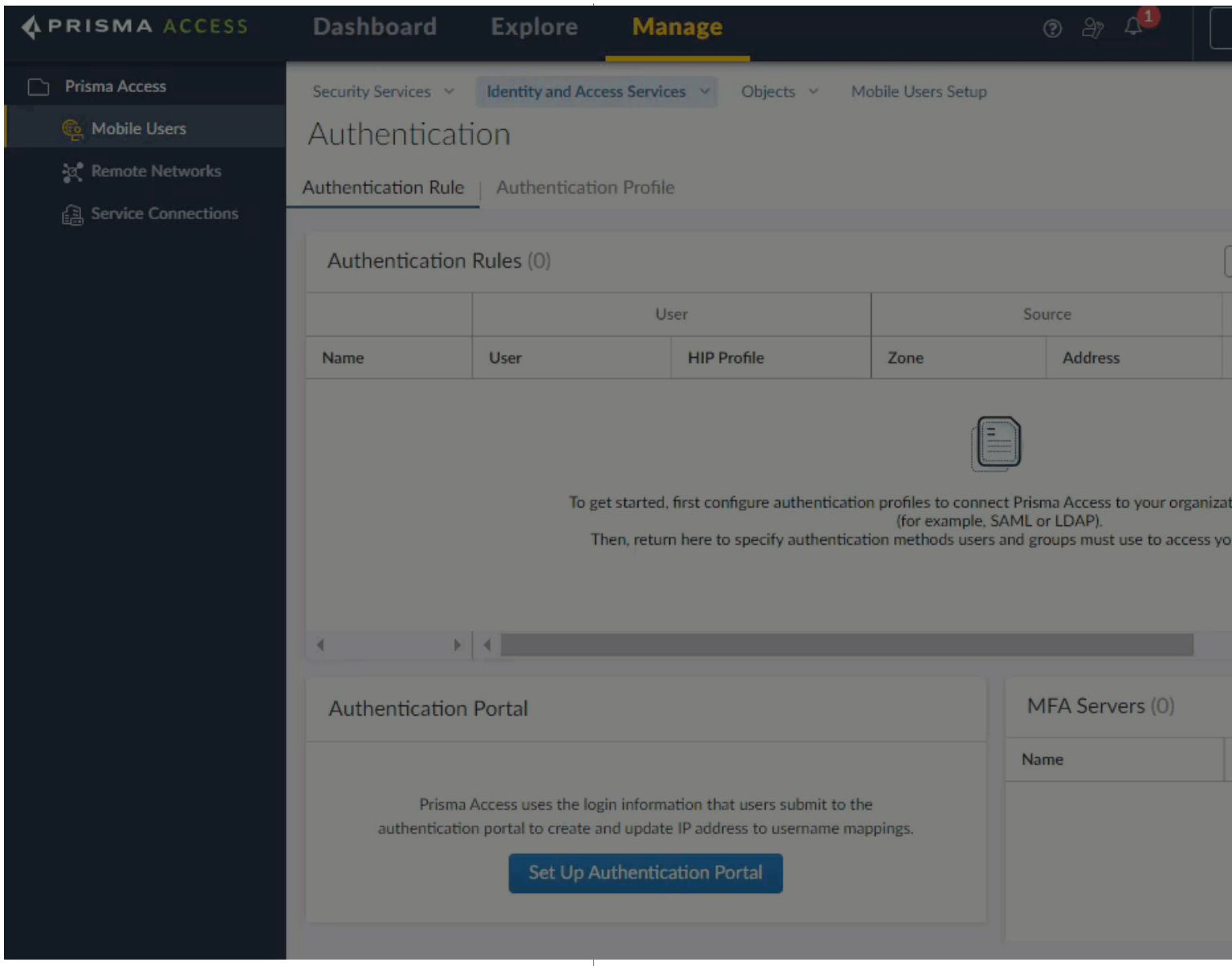
## 驗證支援

| | |
|---|---|
| 雲端識別引擎 | 您可以部署雲端識別引擎以進行使用者驗證，方法為設定 SAML 2.0 型識別提供者 (IdP)、用戶端憑證和憑證授權單位 (CA) 鏈結，或兩者。在指定您想要如何驗證使用者之後，請設定您的驗證設定檔以定義驗證安全性政策，並選擇性地在防火牆或 Panorama 上設定驗證政策。 |
| **SAML** | 如果您的使用者存取網路外部服務和應用程式，則您可以使用 SAML 來整合 Prisma Access 與識別提供者 (IdP)，藉以控制對外部和內部服務和應用程式的存取。SAML 單一登入 (SSO) 可讓您在登入一次後存取多個應用程式；若在您的環境中，每個使用者存取許多應用程式，每個應用程式逐一進行驗證將影響使用者的工作效率，SSO 將有所幫助。在此情況下，SAML 單一登入 (SSO) 可讓您在登入一次後存取多個應用程式。同樣地，SAML 單一登出 (SLO) 將允許使用者登出一個工作階段即可結束多個應用程式的工作階段。SSO 適用於透過 GlobalProtect 應用程式存取應用程式的行動使用者，或在遠端網路上透過驗證入口網站存取應用程式的使用者。SLO 可供 GlobalProtect 應用程式使用者使用。<br><br>您不能在驗證順序中使用 *SAML* 驗證設定檔。 |
| **TACACS+** | 終端存取控制器存取控制系統 + (TACACS+) 是一個通訊協定家族，允許透過集中伺服器進行 |


©2025 Palo Alto Networks, Inc.

| | |
|---|---|
| | 驗證和授權。TACACS+ 會加密使用者名稱和密碼，因此比 RADIUS 更安全，因為後者僅加密密碼。TACACS+ 更加可靠，因為它使用了 TCP，則 RADIUS 則使用 UDP。 |
| **RADIUS** | 遠端驗證撥號使用者服務 (RADIUS) 是一種受到普遍支援的網路通訊協定，提供集中驗證和授權。您也可以將 RADIUS 伺服器新增至 Prisma Access，以實作多因素驗證。 |
| **LDAP** | 輕量型目錄存取通訊協定 (LDAP) 是用於存取資訊目錄的標準通訊協定。您可以使用 LDAP 對透過驗證入口網站存取應用程式或服務的使用者進行驗證。 |
| **Kerberos** | Kerberos 是一種驗證通訊協定，可讓您使用唯一金鑰（稱為票證）在各方之間安全地交換資訊，以識別各方。透過 Kerberos，您可以對透過驗證入口網站存取應用程式的使用者進行驗證。啟用 Kerberos SSO 後，使用者僅需要在首次存取網路時登入（例如登入 Microsoft Windows）。在首次登入之後，使用者便可存取網路中任何以瀏覽器為基礎的服務，而不必再次登入，直到 SSO 工作階段到期為止。<br><br>若要使用 Kerberos，首先必須要有 Prisma Access 的 Kerberos 帳戶，以對使用者進行驗證。必須有帳戶才能建立 Kerberos 金鑰標籤，即包含防火牆或 Panorama 主體名稱與雜湊密碼的檔案。SSO 程序需要金鑰標籤。<br><br>Kerberos SSO 僅適用於 Kerberos 環境內部的服務和應用程式。若要為外部服務和應用程式啟用 SSO，請使用 SAML。 |
| **MFA** | 多因素驗證 (MFA) 可讓您實作不同類型（稱為因素）的多重驗證挑戰，以保護您最敏感的服務和應用程式。例如，您可能希望對重要財務文件實作比搜尋引擎更強的驗證措施。<br><br>Prisma Access 具有支援的 MFA 廠商內建清單，且清單會隨著廠商的新增而自動更新： |


©2025 Palo Alto Networks, Inc.




| | |
|---|---|
| 本機資料庫驗證 | 建立在 Prisma Access 本機執行、且包含使用者帳戶（使用者名稱和密碼或雜湊密碼）和使用者群組的資料庫。這種驗證方法適用於當您僅知道雜湊密碼而不知道純文字密碼時，重複使用現有 Unix 帳戶憑證建立使用者帳戶。對於使用純文字密碼的帳戶，您還可以定義密碼複雜性和過期設定。此驗證方法適用於透過驗證入口網站或 GlobalProtect 應用程式存取服務和應用程式的使用者。 |


©2025 Palo Alto Networks, Inc.

驗證功能重點

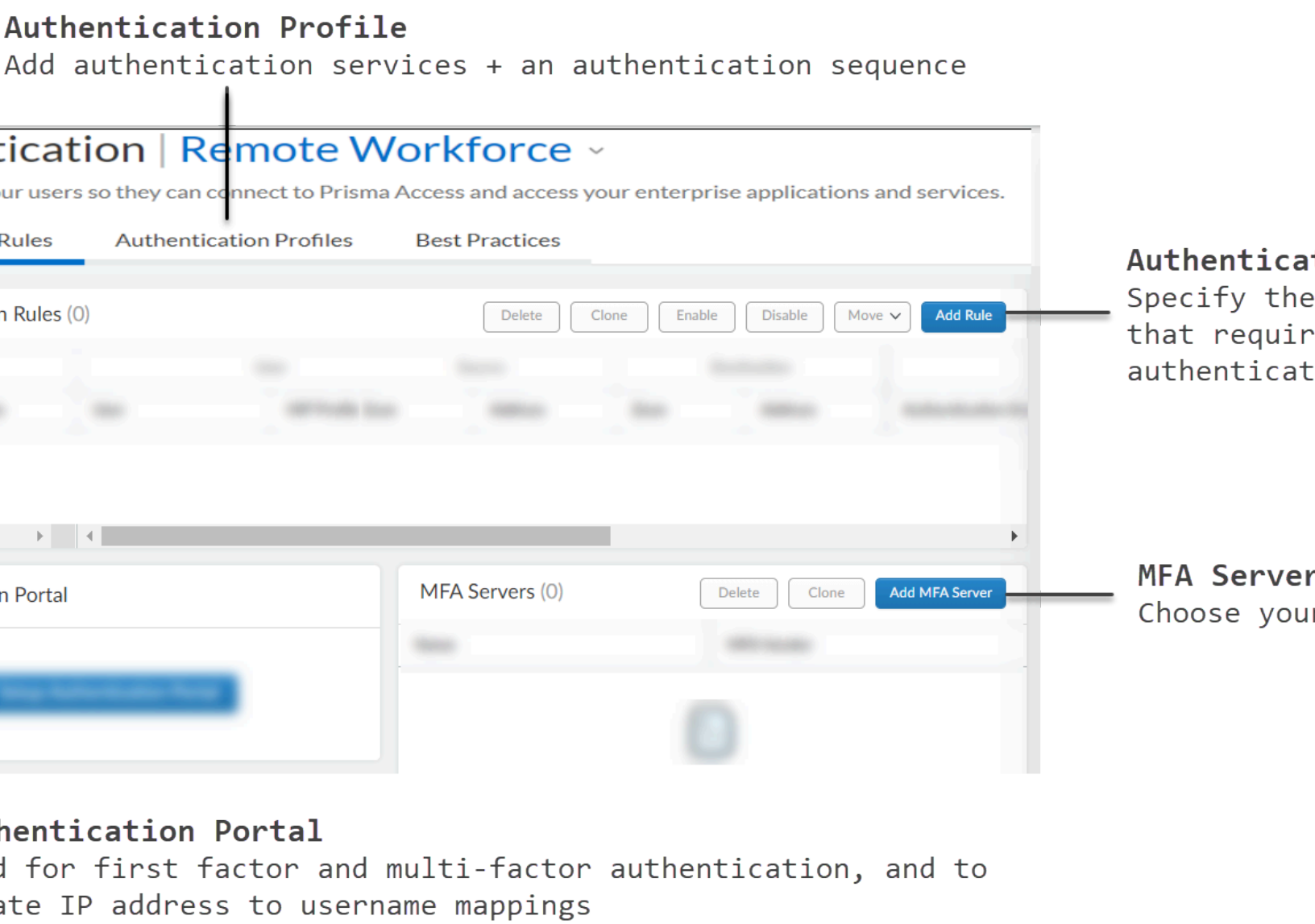
| | |
|---|---|
| **SSO** | 如果您使用 SAML 或 Kerberos，則可以實作單一登入 (SSO)，讓使用者只需進行一次驗證即可存取多項服務和應用程式。SAML 和 Kerberos 支援 SSO。 |
| 驗證入口網站 | 將與驗證規則相符的 Web 要求重新導向至會提示他們進行驗證的 Prisma Access 登入頁面。Prisma Access 會使用使用者提交到此驗證入口網站的資訊，來建立或更新 IP 位址至使用者名稱對應。<br><br>這對於遠端網路特別有用，您可以繼續根據使用者（或群組）來監控及強制執行流量。當使用者啟動與驗證規則相符的 Web 流量（HTTP 或 HTTPS）時， Prisma Access 會提示使用者透過驗證入口網站進行驗證。Prisma Access 根據使用者提交至入口網站的資訊建立或更新 IP 位址至使用者名稱對應。這可以確保您能確切得知誰正在遠端網站上存取最敏感的應用程式和資料。 |
| 驗證順序 | 如果出於不同目的使用多種類型的驗證，您可以設定驗證順序來對您的設定檔進行排名。Prisma Access 會根據您的排名檢查每個設定檔，直到成功驗證使用者為止。 |

## 設定驗證

若要設定 Prisma Access 驗證，首先將您的驗證服務新增至 Prisma Access。然後，指定您認為需要驗證的流量。基於這些設定新增更多驗證功能，例如 MFA、驗證順序，或讓 Prisma Access 能夠建立和更新 IP 位址至使用者名稱對應。

以下說明如何開始使用—啟用 Prisma Access 驗證所需的所有設定都位於同一個位置：**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW 和 Prisma Access**） > **Identity Services**（識別服務） > **Authentication**（驗證）。選取 **Prisma Access** 設定範圍。


©2025 Palo Alto Networks, Inc.




驗證規則 您可以在此處指定需要驗證的流量

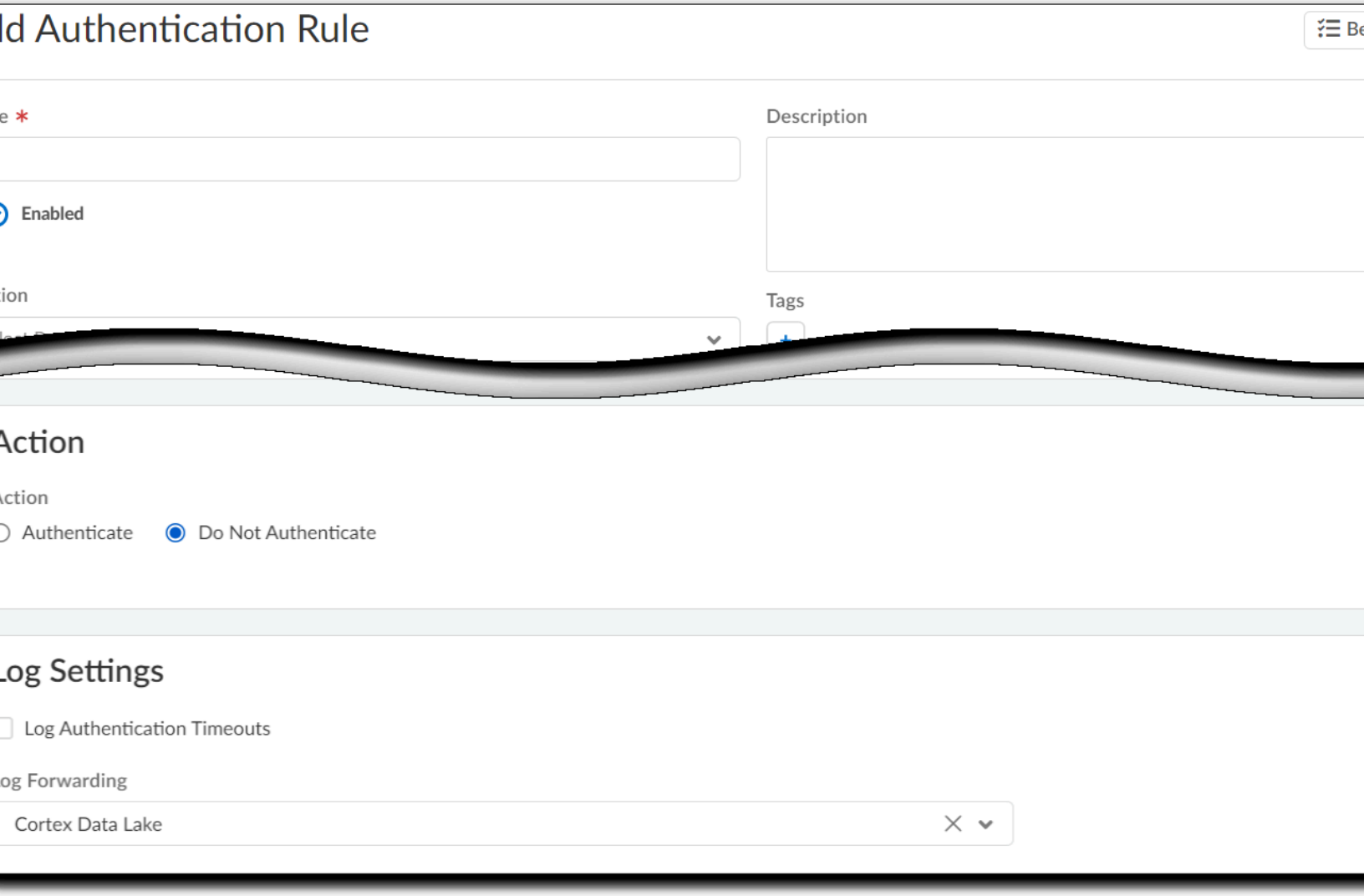
設定驗證規則的一部分，包括將驗證設定檔新增至規則。Prisma Access 在偵測到符合驗證規則的流量時，即會將定義於驗證設定檔中的驗證方法和設定套用至相符的流量。設定檔定義了使用者需要進行驗證的方式。

1. 前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW 和 Prisma Access**） > **Identity Services**（識別服務） > **Authentication**（驗證） >

 ©2025 Palo Alto Networks, Inc.

**Authentication Rule**（驗證規則），並 **Add Authentication Rule**（新增驗證規則）。選取 **Prisma Access** 設定範圍。

2. 定義需要驗證的使用者、服務和 URL 類別。
3. 將規則動作設定為 **Authenticate**（驗證），然後選擇 **Profile**（設定檔）以定義符合此規則的流量所要使用的驗證方法。



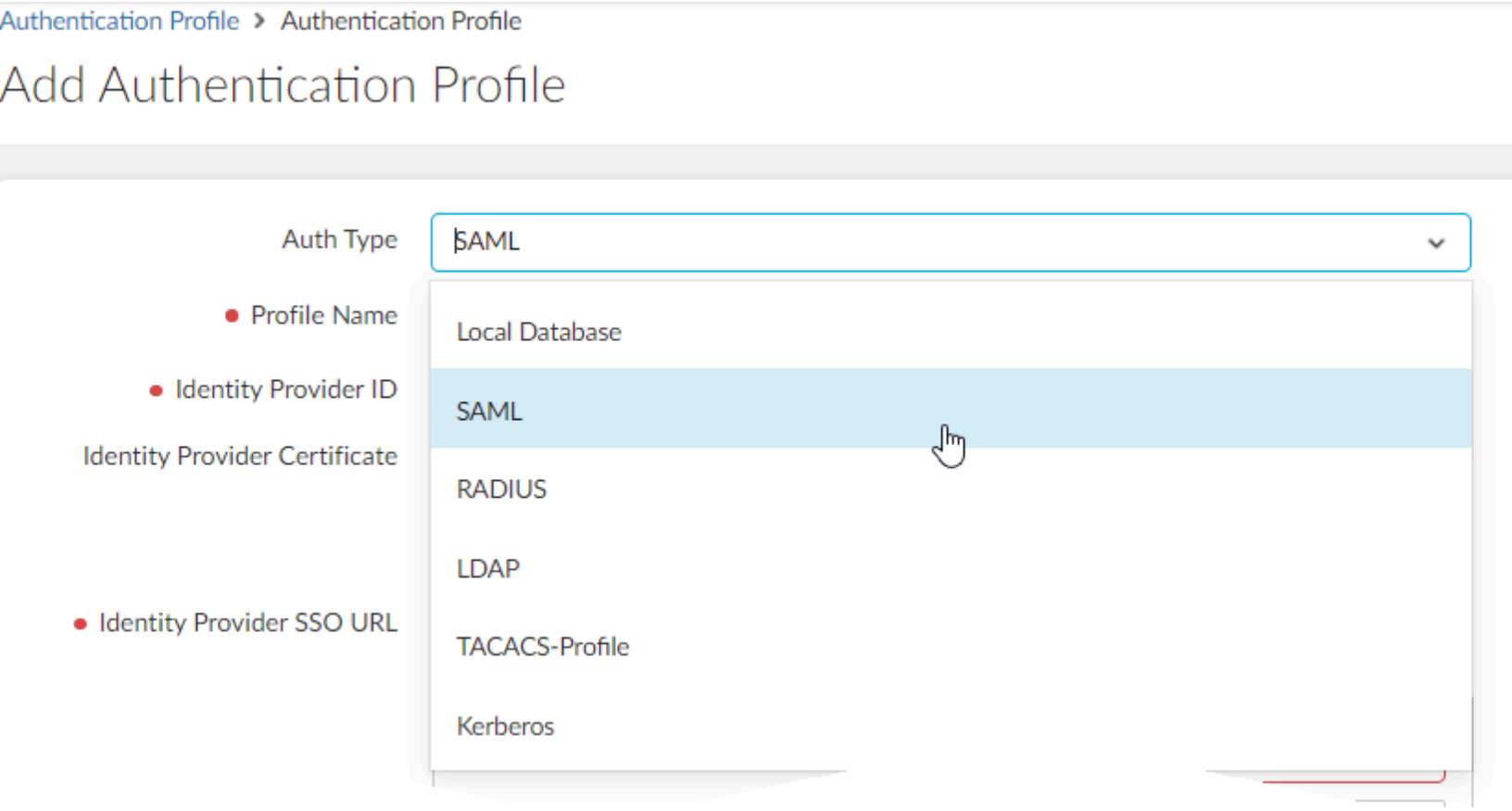

 ©2025 Palo Alto Networks, Inc.

驗證設定檔 在此處新增您的驗證服務，並定義驗證設定

將 Prisma Access 連線至您要用來驗證使用者的服務（SAML、TACACS+、RADIUS、LDAP 或 Kerberos），並定義驗證設定（例如，設定失敗登入嘗試的限制）。

如果您使用內部部署驗證服務，則必須先建立服務連線，以將內部部署驗證服務連線至 *Prisma Access*。然後，返回此處設定您的驗證設定檔。

前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Identity Services**（識別服務） > **Authentication**（驗證） > **Authentication Profile**（驗證設定檔） > **Add Profile**（新增設定檔），然後開始設定設定檔 **Auth Type**（驗證類型）。選取 **Prisma Access** 設定範圍：

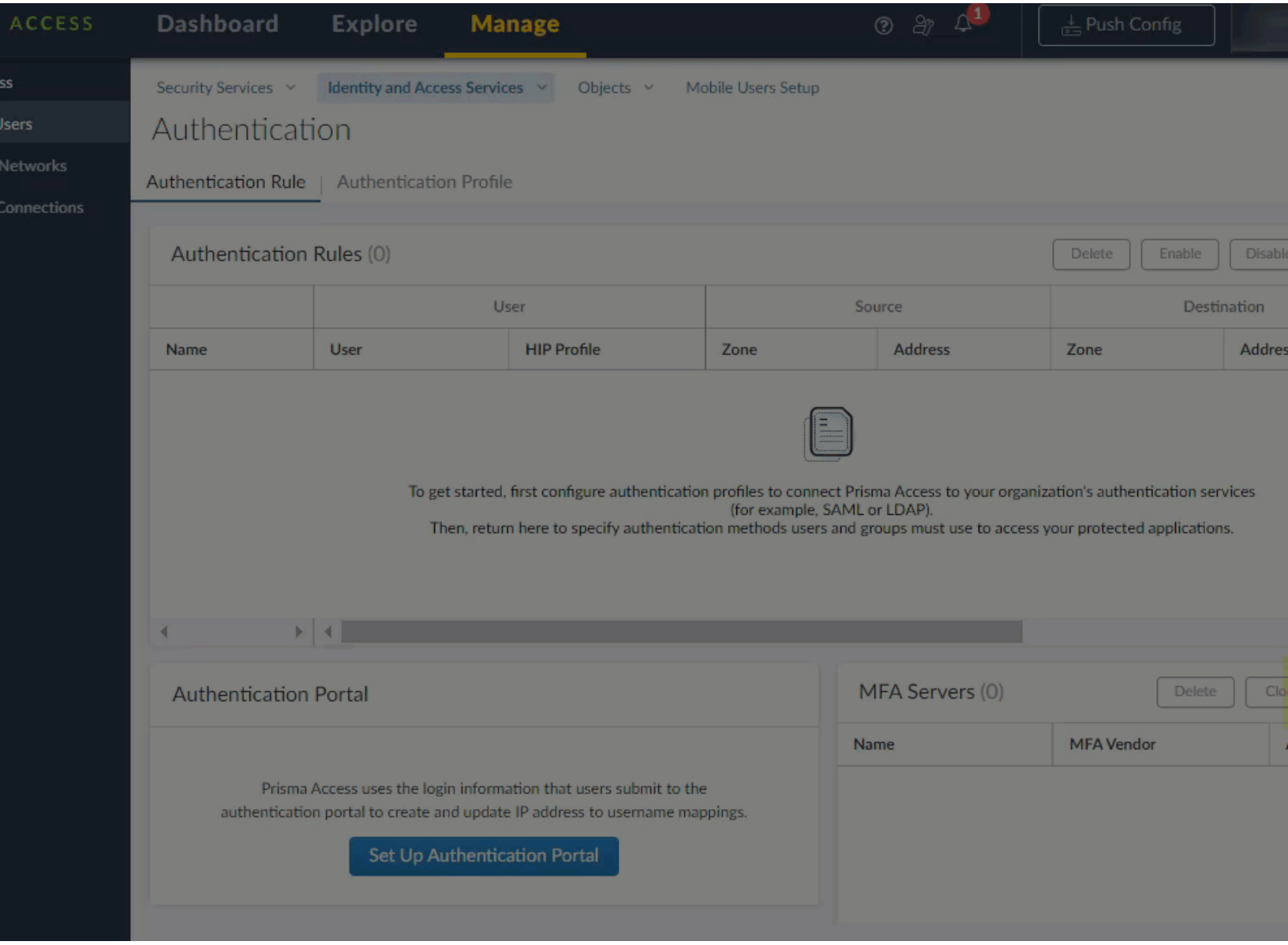



系統會提示您新增與您選擇的驗證服務有關的詳細資料，使 Prisma Access 能夠連線至該服務，以及讀取使用者認證和角色權限。設定檔中提供了用來自訂驗證的其他設定，具體可能會隨著您設定的驗證類型而有所不同。

 ©2025 Palo Alto Networks, Inc.

**MFA** 伺服器 指定您所使用的 MFA 廠商

若要使用多種方法對敏感的應用程式進行使用者驗證，請先新增您要使用的 MFA 廠商（**Add MFA Server**（新增 **MFA** 伺服器））。Prisma Access 會提供 MFA 廠商清單，供您從中選擇。



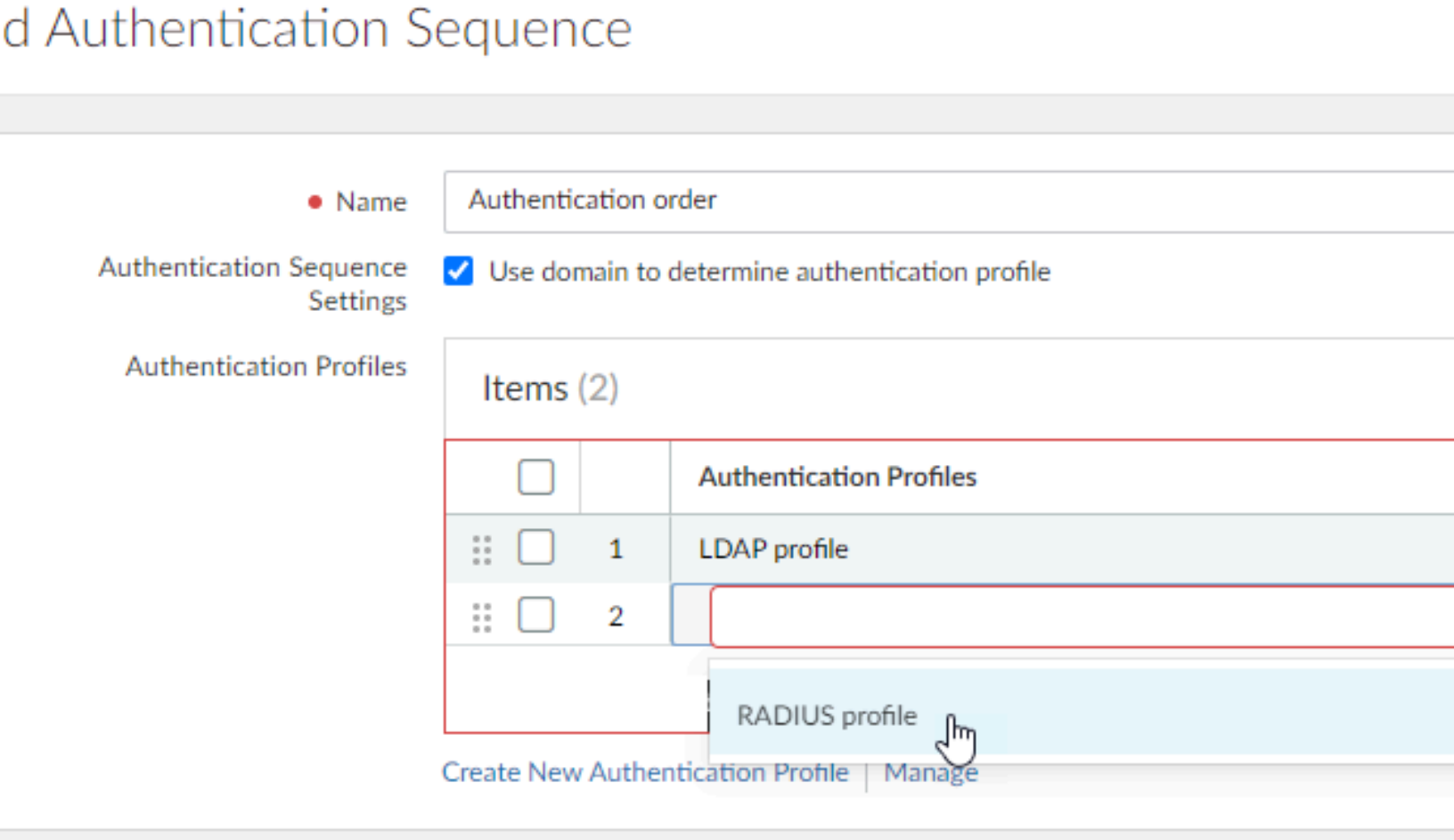

驗證入口網站 為遠端網站的使用者設定驗證入口網站（舊稱為被控制的入口網站），並且使 Prisma Access 能夠建立 IP 位址至使用者名稱對應

對於第一因素驗證（登入名稱和密碼），遠端網站的使用者必須透過驗證入口網站進行驗證。如果驗證成功，Prisma Access 會為所需的每個額外驗證因素顯示 MFA 登入頁面。Prisma Access 會使用使用者提交的憑證，來建立和更新 IP 位址至使用者名稱對應。這意味著您隨時都知道誰正在遠端網站上存取 Web 內容和企業應用程式。


©2025 Palo Alto Networks, Inc.

驗證順序 依照您希望 Prisma Access 嘗試的順序對驗證設定檔進行排名

選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW 和 Prisma Access**） > **Identity Services**（識別服務） > **Authentication**（驗證） > **Authentication Profile**（驗證設定檔） > **Add Authentication Sequence**（新增驗證順序）。選取 **Prisma Access** 設定範圍。Prisma Access 會依序檢查各項，直到成功驗證使用者為止。




 ©2025 Palo Alto Networks, Inc.

# 啟用行動使用者存取公司資源

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Panorama Managed Prisma Access | • Prisma Access 授權 |

若要啟用 Prisma Access，讓使用者僅啟用網際網路存取，您不需要設定任何網路服務，因為 Prisma Access 提供預設 IP 位址集區和雲端預設 DNS 伺服器。

不過，如果您想要行動使用者能夠存取總部、資料中心或您已裝載到 Prisma Access 的遠端網站的內部資源，則必須：

- 定義 Prisma Access 用來將 IP 位址指派給行動使用者的 IP 位址集區、
- 設定 Prisma Access 服務基礎結構、
- 並且若要允許存取您的總部或資料中心，請裝載服務連線。

如果您想要行動使用者連線到遠端網站，則必須至少設定一個服務連線，即使您不打算使用該連線，來提供對資料中心或總部位置的存取。儘管所有分支機構都是完全互聯的，但行動使用者連線卻不是。建立服務連線可建立使行動使用者流量能夠路由到分公司網路所需的中樞和支點架構。在此情況下，您可以最小程度地設定服務連線，如下所示：

- 當您裝載服務連線時，請使用靠近您行動使用者的 Prisma Access 位置。
- 當您為服務連線設定主要 IPSec 通道時，請使用預留位置值設定 IPSec 對等驗證和通道設定。
- 當您為服務連線啟用路由和 QoS 時，請新增預留位置 IP 子網路。

  因為 Prisma Access 不會透過此通道路由任何流量，所以只需確保您使用的 IP 子網路不會與連線到 Prisma Access 的其他已設定子網路衝突或重疊 。

**STEP 1 |** 前往 **Manage**（管理） > **Mobile Users**（行動使用者） > **Mobile Users Setup**（行動使用者設定），並編輯 **Infrastructure Settings**（基礎結構設定） 以調整行動使用者的網路設定。


©2025 Palo Alto Networks, Inc.

**STEP 2 |** 檢查或調整 Prisma Access 用來將 IP 位址指派給行動使用者的 **Client IP Pool**（用戶端 **IP** 集區）。

- 根據預設，**Worldwide**（全球） IP 集區可供所有行動使用者使用。
- 您可以 **Customize per region**（自訂每個區域），以使用專用於區域或位置的已設定 IP 集區。對於未指定 IP 集區的區域或位置，Prisma Access 會使用全球 IP 集區。

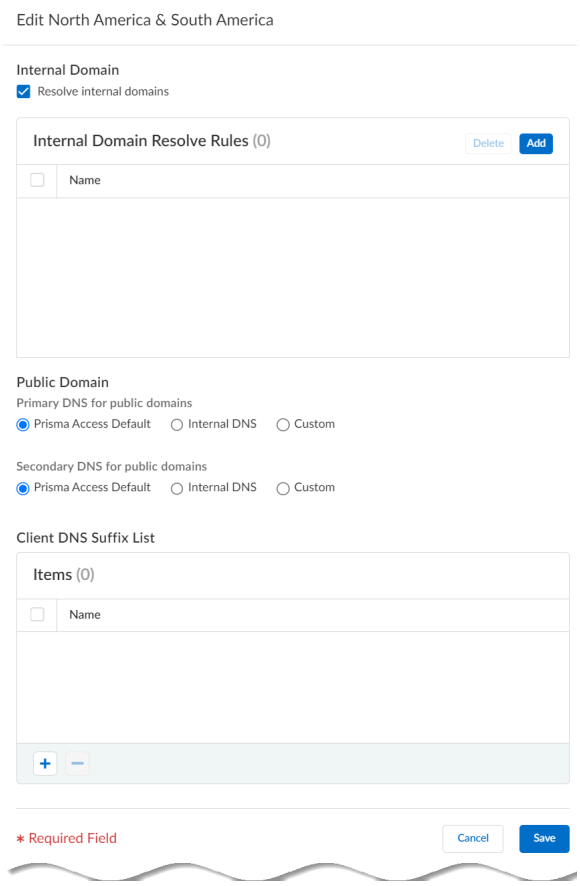
您定義的 IP 位址集區必須符合下列需求：

- 最佳做法是，定義符合 RFC 1918 的 IP 位址集區，以防止 IP 位址衝突。
- 確保您定義的 IP 位址集區不會與您內部使用的其他 IP 位址重疊。
- 確保您定義的 IP 位址集區不會與用於 Prisma Access 的基礎結構 IP 位址集區重疊。
- 請勿指定任何與 169.254.0.0/16 和 100.64.0.0/10 子網路範圍重疊的子網路，因為 Prisma Access 會保留這些 IP 位址和子網路供內部使用。
- 請確保根據下列指導方針指定一個 IP 位址集區，其能夠為您組織中的所有行動使用者提供足夠的覆蓋範圍：
- 如果您打算使用部署在一或兩個區域的全球位址集區，則所需的最低 IP 位址集區為 /23（512 個 IP 位址）。
- 如果您打算使用部署在三個以上區域的全球位址集區，則所需的最低IP 位址集區為/19（8,192 個 IP 位址），無論是在單一IP 位址集區中或分佈在多個集區中。
- 如果您打算為每個區域定義 IP 位址集區，則任何區域中的最小集區大小為 /23（512 個 IP 位址）。
- 您不需要在不打算部署 Prisma Access 的區域中指派 IP 位址集區。例如，僅當您裝載 Prisma Access for Users 時，才會選取美國東部（北維吉尼亞）、美國東部（俄亥俄）和美國西部（北加利福尼亞）區域，而您只需為美洲區域指定 IP 位址集區。但請記住，其他區域的使用者將無法連線到 Prisma Access。
- 如果打算定義混合的全球和區域集區，請確保配置每個區域至少 512 個 IP 位址。例如，對於三區域部署，您可以在歐洲區域指定 1,024 個位址，以及全球指定 512 個位址。
- 最佳做法是，指定 IP 位址集區，以便您組織中的每個唯一行動使用者至少具有一個 IP 位址，以便他們可以同時登入。如果您指定了 IP 位址數目少於授權使用者數目的 IP 位址集區，Prisma Access 將顯示警告訊息。不過，如果您的 IP 位址集區有限，並且您並未預期所有使用者同時登入，則可以略過該訊息並使用較小的集區大小。

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 新增 **Client DNS**（用戶端 **DNS**）設定—您可以使用 **Worldwide**（全球）預設值或根據區域自訂設定。

選取您要自訂 DNS 設定的區域：




選取選項以 **use these DNS settings to resolve internal domains**（使用這些 **DNS** 設定來解析內部網域），並選擇性地 **Use the internal DNS Server for resolving public domains too**（也將內部 **DNS** 伺服器用於解析公用網域）。如果您未選取此選項，Prisma Access 會使用其雲端預設 DNS 伺服器來解析公用網域的要求。

*Prisma Access* 中的 *DNS Proxy* 會將要求傳送到您指定的 *DNS* 伺服器。*DNS* 要求中的來源位址是 *IP* 集區中您指派給該區域的第一個 *IP* 位址。為了確保您的 *DNS* 要求可以到達伺服器，需要確保您允許流量從行動使用者 *IP* 位址集區中的所有位址流向 *DNS* 伺服器。

**STEP 4 |** 如果您想要行動使用者能夠存取總部或資料中心網路或其他分公司位置的資源，您必須設定 Prisma Access 基礎結構設定，以啟用網路骨幹。

前往 **Manage**（管理） > **Prisma Access** > **Prisma Access Setup**（設定）。

**STEP 5 |** 若要啟用行動使用者存取總部或資料中心的資源，請建立服務連線以將這些網站連線到 Prisma Access。

前往 **Manage**（管理） > **Service Connections**（服務連線） > **Service Connections Setup**（服務連線設定）.


©2025 Palo Alto Networks, Inc.

**STEP 6 |** 備妥後，**Push Config**（推送設定）至 Prisma Access，以儲存您的行動使用者設定。


©2025 Palo Alto Networks, Inc.

# Prisma Access 遠端網路

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

隨著您的業務規模不斷擴大，並且辦公室位置在地理上不斷地分散，Prisma Access for Networks 可讓您快速裝載遠端網路位置，並為您的使用者提供最佳的安全性。它提供了一種便利的選項，消除了在每個遠端位置設定和管理裝置的複雜性。此服務提供了一種有效的方式，可以輕鬆地新增遠端網路位置，並最大限度地減少營運挑戰，確保這些位置的使用者始終保持連線和安全，並且允許您從 Panorama 集中管理政策，從而為您的遠端網路位置提供一致且簡化的安全性。

若要將您的遠端網路位置連線到 Prisma Access，您可以使用 Palo Alto Networks 新世代防火牆或第三方 IPSec 相容裝置（包括 SD-WAN），這些裝置可以建立通往服務的 IPSec 通道。

除了 IPSec 通道連線外，Prisma SD-WAN 還可讓您使用裝載為遠端網路的 CloudBlade，將 Prisma SD-WAN 控制器和 ION 裝置與 Prisma Access 整合在一起。

# 遠端網路的規劃檢查清單

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

在開始裝載遠端網路之前，請確定您已準備好下列設定項目，以確保您能夠成功啟用服務，並針對遠端網路位置中的使用者強制執行政策：

- 需要存取公司資源嗎？

  如果您的遠端網路需要存取總部或資料中心的基礎結構或資源，請建立 Prisma Access 與公司網站的服務連線。如果遠端網路位置是自發的，且不需要存取其他位置的基礎結構，則您無需這樣做。

- **Prisma Access** 個位置

  當您分公司的使用者連線到 Prisma Access 時，您選擇的 Prisma Access 位置會確定以哪種語言提供網際網路的內容。如需最佳使用者體驗，請選取與分公司同一縣的區域和位置，以確保最佳的使用者體驗。如果與您分公司相同的國家/地區沒有可用的位置，請選取一個使用與網站上大多數使用者相同語言的位置。

  少數位置會標記為 **Local Zones**（本機區域）。這些位置提供靠近大型人口和產業中心的 Prisma Access 計算位置。

- **IP** 子網路

  若要 Prisma Access 將流量路由到遠端網路，您需要為您要 Prisma Access 保護的子網路提供路由資訊。您可以採取幾種方式來執行此動作。您可以定義遠端網路位置上每個子網路的靜態路由，也可以在服務連線位置與 Prisma Access 之間設定 BGP，或使用這兩種方法的組合。如果同時設定靜態路由並啟用 BGP，則靜態路由優先。雖然如果您的遠端網路位置只有幾個子網路，使用靜態路由可能很方便，但在其中遠端網路具有重疊子網路的大型部署中，BGP 將使您能夠更輕鬆地進行調整。

- 彙總頻寬模型—遠端網路位置的頻寬會以每個計算位置的彙總層級進行配置。您裝載的每個位置都有一個為其配置頻寬的計算位置。您可以配置每個計算位置的頻寬，而不是每個位置。此方法稱為彙總頻寬模型。

  彙總頻寬模型適用於所有新的部署。如果您有一個依位置配置頻寬的現有部署，則可以從配置每個位置的頻寬移轉至配置每個計算位置的頻寬。

  在移轉至彙總頻寬模型之前，您應該檢閱 規劃您移轉至新模型的方式。

  您裝載的所有位置都會共用該計算位置的配置頻寬。例如，您需要在新加坡、泰國和越南位置使用遠端網路裝載四個分公司。所有這些位置都會對應到東南亞計算位置。如果您將 200 Mbps 頻寬配置給東南亞計算位置，Prisma Access 會在您在該位置裝載的四個分公司之間分配 200


©2025 Palo Alto Networks, Inc.

Mbps 的頻寬。如果您也在香港新增一個位置，則您會注意到香港對應到香港計算位置，並且需要將頻寬新增至該計算位置。指定每個計算位置的最小頻寬為 50 Mbps。

Prisma Access 根據每個位置的負載或需求動態配置頻寬。使用前面的範例，其中四個網站總共使用多達 200 Mbps，如果一個或多個網站使用的頻寬不如其他網站站多，Prisma Access 會為需求更大的位置提供更多頻寬，讓您能夠更有效地利用配置的頻寬。此外，如果其中一個網站關閉，Prisma Access 會在該計算位置中仍啟動的其他網站之間重新配置頻寬。

標記為 **Local Zones**（本機區域）的位置支援遠端網路的頻寬上限為 500 Mbps。若要支援 1 Gbps 的頻寬，請聯絡 Palo Alto Networks 支援。這些位置提供靠近大型人口和產業中心的 Prisma Access 計算位置；不過，它們也有一些限制。若要新增本機區域，請聯繫您的 Palo Alto Networks 代表。

- 如果您在存取 URL 時遇到問題，請向 Palo Alto Networks 支援報告網站問題。
- 調整大小指導方針和頻寬配置考量

  計算網站上您所需的頻寬量時，請考慮頻寬使用量包括遠端網路連線的輸出和進入流量（亦即，配置的頻寬是進入和輸出的總和），並且您裝載的所有位置都會共用該計算位置的配置頻寬。為了協助您確定特定網站需要多少頻寬，請考慮每個位置可從 ISP 取得的頻寬。
- 重疊子網路

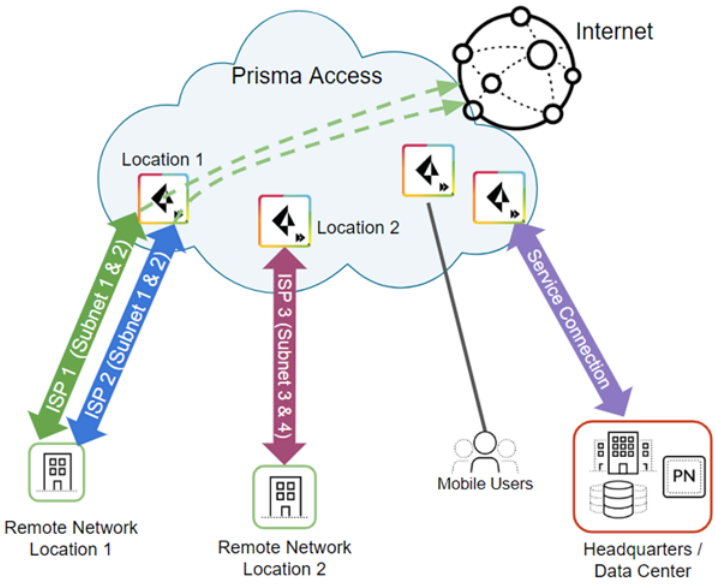
  一般而言，您無法在 Prisma Access 執行個體內有任何重疊的子網路。也就是說，所有遠端網路位置、服務連線，以及 Prisma Access for Mobile Users IP 位址集區的子網路不能重疊。不過，在某些情況下，您無法避免具有重疊的子網路，例如，如果您收購的公司使用與現有子網路重

 ©2025 Palo Alto Networks, Inc.

疊的子網路。在某些情況下，您可能想要根據設計設定兩個具有重疊子網路的區域；例如，如果您想要在零售商店位置建立具有不同政策規則的個別來賓網路。

Prisma Access 可讓您裝載具有重疊子網路的遠端網路位置，但只有子網路重疊的分支才支援網際網路繫結流量。在同一租用戶中沒有重疊子網路的分支，可從 Prisma Access 得到完整的功能。如需更多詳細資訊，請參閱下圖中的表格。

| Traffic Flow | Supported? |
|---|---|
| Remote Network to Internet | Yes |
| Remote Network to Remote Network (Overlapping Subnets) | No |
| Remote Network to Remote Network (No Overlapping Subnets) | Yes |
| Remote Network to HQ (Overlapping Subnets) | No |
| Remote Network to HQ (No Overlapping Subnets) | Yes |
| HQ to Remote Network (Overlapping Subnets) | No |
| Mobile Users to and from Remote Network (Overlapping Subnets) | No |
| Mobile Users to and from Remote Network (No Overlapping Subnets) | Yes |




不過，請記住，子網路重疊的網站具有下列限制：

- 沒有輸入遠端網路到遠端網路流量。其他遠端網路位置不會知道何處路由流量，因為多個遠端網路位置路由到相同的子網路。不過，任何遠端網路位置的使用者和服務都可以存取其他遠端網路位置的資源，前提是網站上沒有重疊的子網路，且任何網站都可以透過 Prisma Access 基礎結構存取網際網路。
- 來自服務連線的流量無法存取子網路重疊的任何遠端網路位置的資源，因為它不知道哪個遠端網路位置路由流量。不過，子網路重疊的遠端網路位置可以從服務連線存取資源。
- 由於輸入路由限制，行動使用者無法存取子網路重疊的遠端網路位置的資源。

如果您使用 *Strata Cloud Manager* 管理 *Prisma Access*，請前往 ***Workflows***（工作流程）> ***Prisma Access Setup***（***Prisma Access*** 設定）> ***Remote Networks***（遠端網路）> ***Advanced Settings***（進階設定）。編輯 ***Overlapped Subnets***（重疊子網路）設定，以啟用重疊的子網路。如果您使用 *Panorama* 來管理 *Prisma Access*，請前 ***Panorama*** > ***Cloud Services***（雲端服務）> ***Configuration***（設定）> ***Remote Networks***（遠端網路），然後核取 ***Overlapped Subnets***（重疊的子網路）。

- **IPsec** 終端節點—在裝載期間，將 *IPsec* 終端節點指派給遠端網路。您可以指定每個 IPsec 終端節點最多 500 個遠端網站 (適用於 Prisma Access 5.0 和更新版本) 或 400 個遠端網站 (適用於

 ©2025 Palo Alto Networks, Inc.

5.0 以前的 Prisma Access 版本)。為對應至 IPsec 終端節點的計算位置配置 500 以上的 Mbps，以支援允許的遠端網路數目上限。

您可以在計算位置中最多有 200 個 IPsec 終端節點。每個 IPsec 終端節點可為您提供最高 1,000 Mbps 的頻寬。如果您將 1,000 Mbps 以上的頻寬配置給計算位置，則 Prisma Access 會為您提供額外的 IPsec 終端節點。

- **IPsec** 終端節點與從 **3.2** 以前的版本進行升級—在 3.2 之前，計算位置中每 500 Mbps 的配置頻寬已配置一個 IPsec 終端節點。如果您有早於 3.2 的遠端網路部署，並升級至 3.2.1 版或更新版本，以及如果遠端網路位置有 500 以上的 Mbps 配置給其對應計算位置，則與 IPsec 終端節點相關聯的每個遠端網路最高可以支援 1,000 Mbps 的頻寬。在您升級至 3.2 或更新版本之後，Prisma Access 會針對每 1,000 Mbps 的配置頻寬，部署一個 IPsec 終端節點。對於現有的遠端網路，Prisma Access 可以使用自動調整機制增加遠端網路的頻寬，此機制會在遠端網路上的頻寬耗用量需要額外容量時觸發。如需詳細資訊，請參閱 Prisma Access（Panorama 管理）版本資訊中預設行為的變更。

  升級至 3.2 之後，目前的 IPsec 終端節點至遠端網路對應會保持不變，而且 IPsec 終端節點數目仍保持相同。只有當您增加或減少現有計算位置的頻寬，或是為遠端網路裝載新的計算位置時，才會新增或刪除 IPsec 終端節點。

- 服務連線—如果您的遠端網路位置需要存取公司總部的基礎結構，來驗證使用者或啟用對關鍵網路資產的存取，則您必須建立服務連線，以便連線總部和遠端網路位置。如果遠端網路位置是自發的，且不需要存取其他位置的基礎結構，則您無需設定服務連線（除非您的行動使用者需要存取）。
- 範本—Prisma Access 自動為 Prisma Access for Networks 建立範本堆疊 (Remote_Network_Template_Stack) 和最上層範本 (Remote_Network_Template)。若要裝載和設定遠端網路，您需要從頭開始設定最上層範本，或者利用現有的設定，如果您已在內部部署執行 Palo Alto Networks 防火牆。範本需要設定來建立 IPsec 通道和網際網路金鑰交換 (IKE) 設定（用於在遠端網路位置與 Prisma Access for Networks 之間進行通訊協定交涉）、您可以在安全性政策中參考的區域，以及日誌轉送設定檔，以便您可以將日誌從 Prisma Access for Remote Networks 轉送至 Strata Logging Service。
- **IPsec** 通道設定—如果您有包含 IPSec 通道、通道監控和 IPSec 密碼設定檔設定的現有範本，則可以將該範本新增至 Remote_Network_Template_Stack，以簡化建立 IPSec 通道的程序。或者，您可以編輯自動建立的 Remote_Network_Template，並建立所需的 IPSec 設定，以建立回到公司網站的 IPSec 通道。Prisma Access 還為您提供了一組預先定義的 IPSec 範本（適用於某些常用的網路裝置），以及一個通用範本（適用於預先定義範本中未包含的任何裝置）。設定遠端網路通道時，請務必遵循 IPsec 通道建議。
- 確定路由方法 **(**靜態或動態**)**—為了讓 Prisma Access 將流量路由到遠端網路，您必須為要使用 Prisma Access 保護的子網路提供路由資訊。您可以採取幾種方式來執行此動作。您可以定義遠端網路位置上每個子網路的靜態路由，也可以在服務連線位置與 Prisma Access 之間設定 BGP，或使用這兩種方法的組合。如果同時設定靜態路由並啟用 BGP，則靜態路由優先。雖然如果您的遠端網路位置只有幾個子網路，使用靜態路由可能很方便，但在其中許多遠端網路具有重疊子網路的大型部署中，BGP 將使您能夠更輕鬆地進行調整。
- 父系裝置群組—Prisma Access for Networks 要求您指定一個父系裝置群組，其中將包括您的安全性政策、安全性設定檔和其他政策物件 (例如應用程式群組和物件，以及位址群組)，還包括驗證政策，以便 Prisma Access for Networks 可以一致地對透過 IPsec 通道路由至 Prisma

 ©2025 Palo Alto Networks, Inc.

Access for Networks 的流量強制執行該政策。您需要在 Panorama 上定義政策規則和物件，或使用現有的裝置群組來保護遠端網路位置中的使用者。



如果您使用參考區域的現有裝置群組，請務必將定義區域的對應範本新增至 *Remote_Network_Template_Stack*。這樣做可讓您在裝載和設定遠端網路時完成區域對應。

 ©2025 Palo Alto Networks, Inc.

# 配置遠端網路頻寬

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

遠端網路用來保護遠端網路位置（例如分支），以及這些分支中的使用者。

遠端網路是計量的，這意味著特定數量的頻寬會配置給計算位置，並有與此所配置頻寬相關聯的成本。

在準備將遠端網路連線至 Prisma Access 時，您必須知道有多少個網站要裝載，以及每個網站的頻寬需求。

瞭解如何配置遠端網路頻寬。

- Strata Cloud Manager
- Panorama

## 配置遠端網路頻寬 (Strata Cloud Manager)

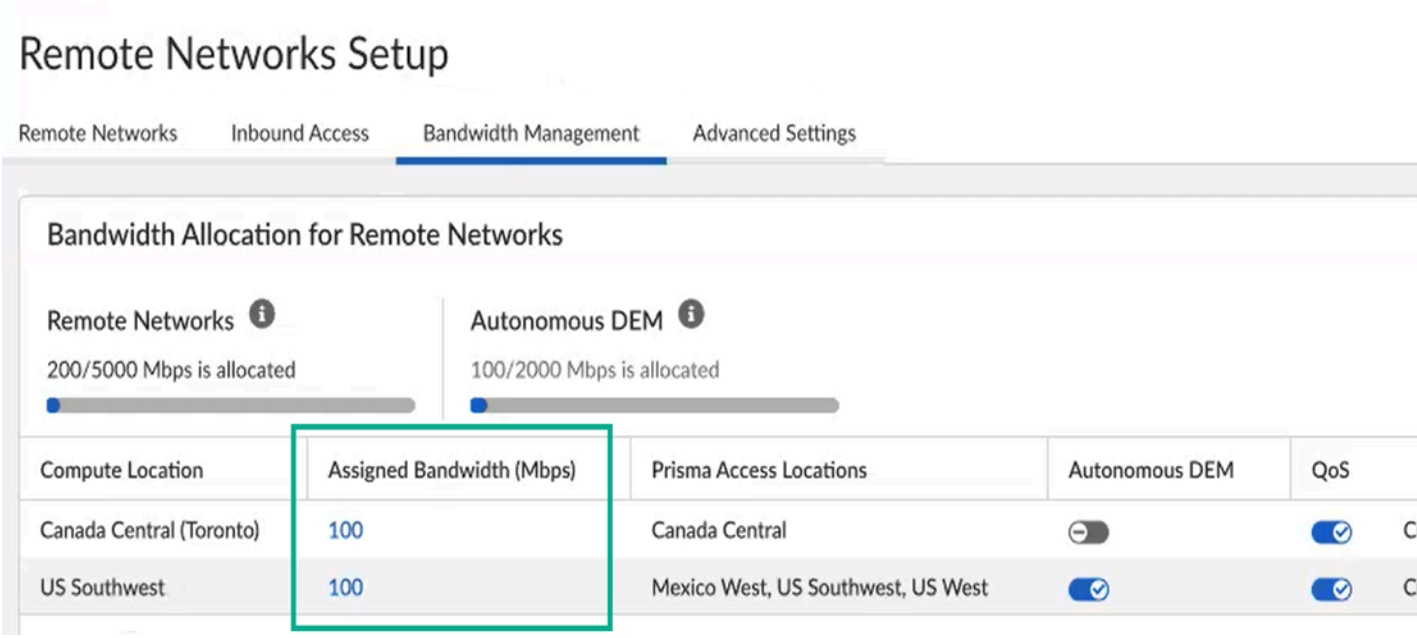
至少兩個（通常更多）地理上彼此接近的 Prisma Access 位置被分組為計算位置。這是您配置頻寬的等級，而不是為個別 Prisma Access 位置或特定遠端網路網站配置頻寬。這意味著 Prisma Access 可以根據負載或需求動態地將頻寬配置給計算位置中的網站。

例如，您需要在新加坡、泰國和越南位置使用遠端網路裝載四個分公司。所有這些位置都會對應到東南亞計算位置。如果您將 200 Mbps 頻寬配置給東南亞計算位置，Prisma Access 會在您在該位置裝載的四個分公司之間分配 200 Mbps 的頻寬。如果您也在香港新增一個位置，則您會注意到香港對應到香港計算位置，並且需要將頻寬新增至該計算位置。指定每個計算位置的最小頻寬為 50 Mbps。

Prisma Access 根據每個位置的負載或需求動態配置頻寬。使用前面的範例，其中四個網站總共使用多達 200 Mbps，如果一個或多個網站使用的頻寬不如其他網站站多，Prisma Access 會為需求更大的位置提供更多頻寬，讓您能夠更有效地利用配置的頻寬。此外，如果其中一個網站關閉，Prisma Access 會在該計算位置中仍啟動的其他網站之間重新配置頻寬。

若要開始，請前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Remote Networks**（遠端網路） > **Bandwidth Management**（頻寬管理）。


©2025 Palo Alto Networks, Inc.




當您根據位置配置頻寬時，仍需考慮每個網站需要多少頻寬

為了協助您確定特定網站需要多少頻寬，請考慮每個位置可從 ISP 取得的頻寬。計算您在一個網站所需的頻寬量時，請注意到頻寬使用量包含遠端網路連線的輸出和進入流量。

當您跨位置配置頻寬時，不支援遠端網路網站的安全輸入存取和遠端網路的服務品質 *(QoS)*。

## 配置遠端網路頻寬 (Panorama)

若要設定依計算位置配置頻寬的 Prisma Access 遠端網路部署，請完成下列步驟。

如果您需要裝載許多遠端網路（高達 *1,000* 個），您可以使用以下程序裝載遠端網路，然後將遠端網路設定匯出到 CSV 檔案、將您要裝載的其他遠端網路新增至 *CSV* 檔案，然後匯入該 *CSV* 檔案以將此設定儲存至 *Prisma Access*。

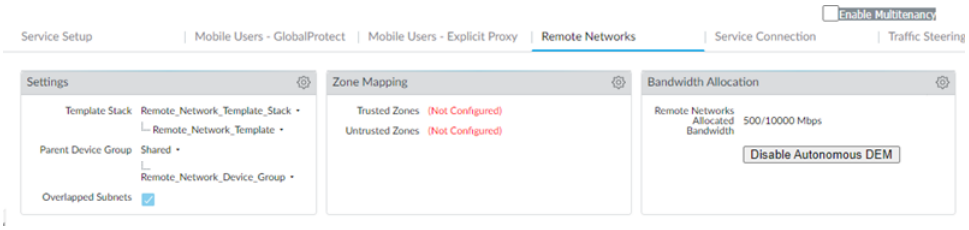
**STEP 1 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路）。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 按一下 **Bandwidth Allocation**（頻寬配置）區域中的齒輪圖示，為您想要裝載的位置配置頻寬。

您可以按每個計算位置的彙總層級配置頻寬。如需詳細資料，請參閱 Prisma Access 遠端網路。

如果您已將自發 DEM 當作附加授權移除，或如果從授權中移除遠端網路的自發 *DEM*，請選取 ***Disable Autonomous DEM***（停用自發 ***DEM***）。如果您移除遠端網路的自發 *DEM*，但未停用自發 *DEM*，您將在提交時收到錯誤。




如果您現有的遠端網路部署目前依位置裝載遠端網路，則會顯示一個快顯視窗，詢問您是否要移轉到彙總頻寬模型。按一下 **Migrate**（移轉）以繼續，或按一下 **Cancel**（取消）以取消移轉。

移轉至彙總頻寬模型是永久且不可逆的。移轉前，請先檢閱移轉前檢查清單。您必須 ***Commit and Push***（提交並推送）變更才能使其生效。

**Service IP Address**（服務 **IP** 位址）（用於 IPSec 通道的 Prisma Access 端進行遠端網路連線的公用 IP 位址），在您將部署移轉到彙總頻寬模型時不會變更，且無需重新設定 IPSec 通道。

**STEP 3 |** 為與您要裝載的 **Prisma Access Locations**（位置）相關聯的每個 **Compute Location**（計算位置）輸入您想要的 **Bandwidth Allocation**（頻寬配置）。

若要驗證您輸入的頻寬量，請選取頻寬量旁邊的核取記號；若要取消該數量，請選取 **x**。

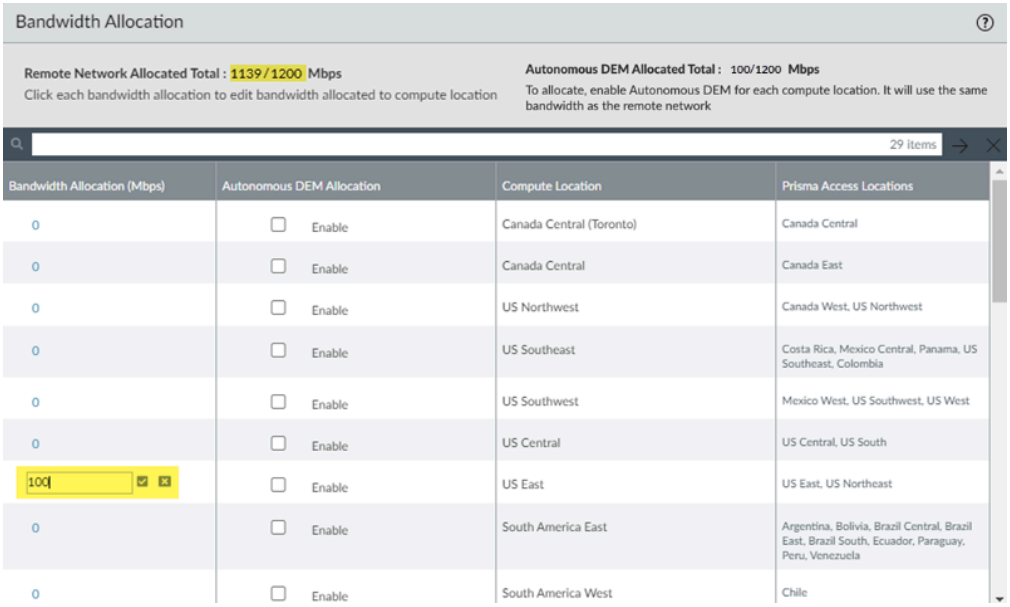
指定最小頻寬為 50 Mbps，最大頻寬為最大剩餘授權頻寬。

**STEP 4 |** （選用，僅使用遠端網路授權的自發 DEM 進行部署）為已配置頻寬的計算位置 **Enable**（啟用） **Autonomous DEM Allocation**（自發 **DEM** 配置）。

如果您為計算位置啟用自發 DEM，則自發 DEM 授權所使用的頻寬量與您為計算位置指定的頻寬量相同。**Autonomous DEM Allocated Total**（自發 **DEM** 已配置總數）顯示自發 DEM 使用了多少頻寬以及剩餘多少。如需詳細資訊，請參閱自發 DEM 指南。


©2025 Palo Alto Networks, Inc.

**STEP 5 |** 等待頻寬反映在頁面頂部的 **Allocated Total**（已配置總數）欄位中；然後按一下 **OK**（確定）。




**STEP 6 |** （選用）如果您想要設定遠端網路，以提供對遠端網路位置的安全輸入存取，請按一下 **Inbound Access Remote Networks**（輸入存取遠端網路）頁籤，並遵循工作流程為遠端網路設定安全輸入存取。

**STEP 7 |** **Add**（新增）遠端網路並指定 **Name**（名稱）。

輸入遠端網路位置的名稱之後，您無法變更該名稱。在開始裝載之前，請確保您了解遠端網路的命名計劃。

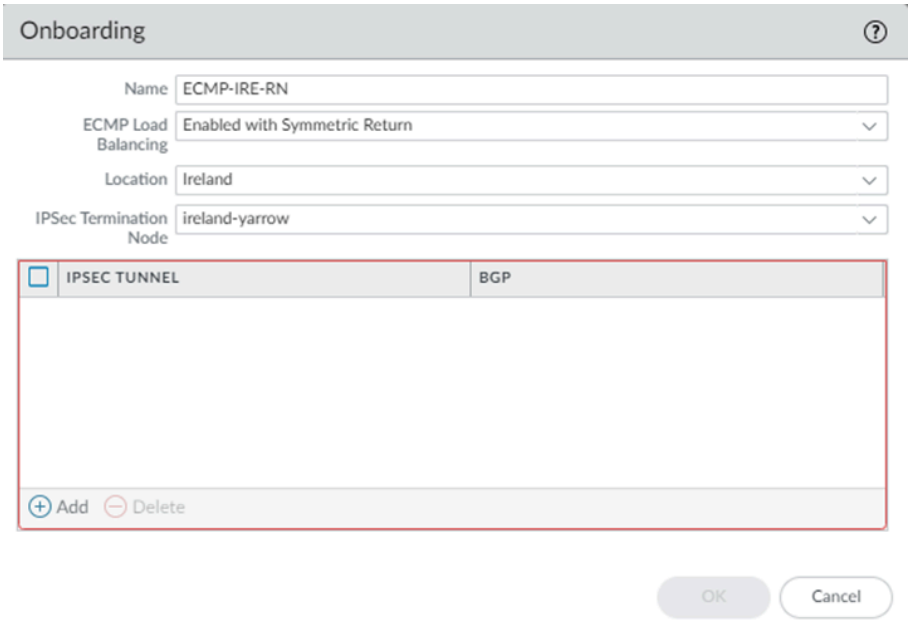

©2025 Palo Alto Networks, Inc.

**STEP 8 |** （選用，僅限 BGP 部署）建立一個設定，以便您的遠端網路連線可以為其流量使用最多四個 IPSec 通道（**ECMP Load Balancing**（**ECMP** 負載平衡））。

不支援靜態路由（需要 BGP），並且如果設定了 QoS，則您無法變更 ECMP 連結的配置比。如果您的部署使用一個 IPSec 通道進行其遠端網路連線或使用靜態路由，請為 **ECMP Load Balancing**（**ECMP** 負載平衡） 選取 **None**（無），然後繼續執行步驟 11。

1. 選取其中一個選項以啟用或停用 ECMP 負載平衡。
   - **None**（無）—不使用 ECMP 負載平衡（使用單一遠端網路通道進行此遠端網路連線）。這是您可以對靜態路由做出的唯一選擇；ECMP 負載平衡需要 BGP。
   - **Enabled with Symmetric Return**（啟用對稱傳回）—指定最多四個 IPSec 通道進行此遠端網路連線，並強制 Prisma Access 使用與其用來傳送流量相同的連結來傳回流量。

     如果您使用一個或多個通道作為僅在其中一個主要通道發生故障時才使用的備份通道，請選取此選項。如果連結失敗，Prisma Access 會使用其他通道之一對稱地發送和接收流量。




2. **Add**（新增） IPSec 通道進行遠端網路連線並指定下列值：
   - **Enable**（啟用）—為 IPSec 通道啟用 BGP。

     此選擇是無法設定的；您必須啟用 BGP 才能設定 ECMP。
   - **Summarize Mobile User Routes before advertising**（公告前彙總行動使用者路由）—減少透過 BGP 公告至客戶周邊設備 (CPE) 的行動使用者 IP 子網路公告數目，方法為彙總這些公告。

     根據預設，Prisma Access 會在 /24 子網路區塊中公告行動使用者 IP 位址集區；如果你彙總它們，Prisma Access 根據您指定的子網路公告該集區。例如，Prisma Access 使用 /20 子網路公告 10.8.0.0/20 的公用使用者行動 IP 集區，而不是先將該集區劃分為 10.8.1.0/24、10.8.2.0/24、10.8.3.0/24 等子網路，再公告它們。彙總這些公告可

 ©2025 Palo Alto Networks, Inc.

以減少 CPE 路由表中儲存的路由數目。例如，您可以使用 IP 集區彙總，搭配可接受有限數目路由的雲端 VPN 閘道（虛擬私人閘道 (VGW) 或傳輸閘道 (TGW)）。

如果您為使用 *ECMP* 的位置啟用路由彙總，則必須在該位置的所有連結上啟用路由彙總，否則您將在提交期間收到錯誤。

Prisma Access 會將所彙總行動使用者路由的社群字串設定為 `0xFFFE:0xFFF0`。

- **Advertise Default Route**（公告預設路由）—Prisma Access 使用 eBGP 為遠端網路起始預設路由公告。

  確保您的網路沒有 *BGP* 公告的其他預設路由，否則可能會在您的網路中引入路由問題。

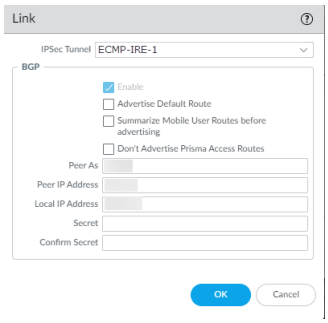
- **Don't Advertise Prisma Access Routes**（不公告 **Prisma Access** 路由）—防止 Prisma Access BGP 對等將路由轉送至組織的網路。

  根據預設，Prisma Access 會公告所有 BGP 路由訊息，包括本機路由以及從其他服務連線、遠端網路和行動使用者子網路接收的所有首碼。選取此核取方塊可防止 Prisma


©2025 Palo Alto Networks, Inc.

Access 傳送任何 BGP 公告，但仍會使用其收到的 BGP 資訊，來了解其他 BGP 芳鄰的路由。

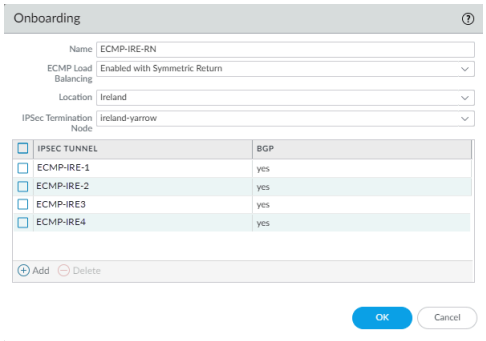
自從 Prisma Access 不傳送 BGP 公告後，如果您選取此選項，則必須在內部部署設備上設定靜態路由，以建立回到 Prisma Access 的路由。




- **Peer AS**（對等 **AS**）—指定遠端網路上防火牆、虛擬路由器或 BGP 路由器所屬的自發系統 (AS)。
- **Peer IP Address**（對等 **IP** 位址）—輸入指派為 eBGP 路由器的路由器 ID 的 IP 位址，而此路由器位於您要為其設定此連線的遠端網路上。
- **Local IP Address**（本機 **IP** 位址）（選用）—輸入一個位址，Prisma Access 會使用此位址作為 BGP 的本機 IP 位址。指定要在通道的 Prisma Access 端使用的 IP 位址。

  指定 **Local Address**（本機位址）很有用，其中連線另一端的裝置（例如 Amazon Web Service (AWS) 虛擬私人閘道）需要特定的本機 IP 位址，才能使 BGP 對等成功。確保您指定的位址不會與基礎結構子網路或遠端網路中子網路中的 IP 位址衝突或重疊。
- **Secret**（密碼）和 **Confirm Secret**（確認密碼）（選用）—輸入並確認複雜密碼以驗證 BGP 對等通訊。

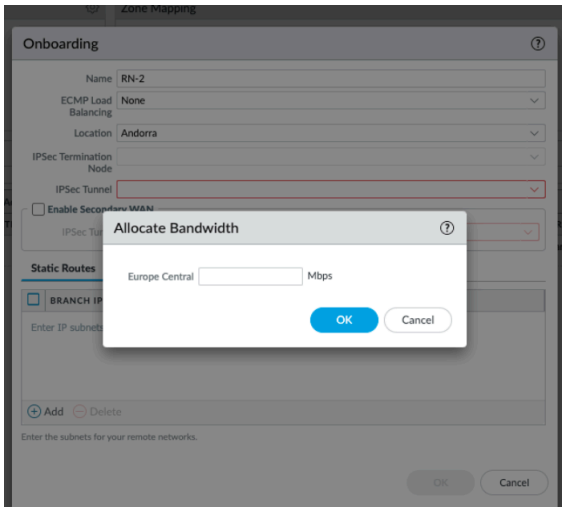
3. 重複上一步，新增最多四個通道與遠端網路連線搭配使用。




 ©2025 Palo Alto Networks, Inc.

**STEP 9 |** 選取 Prisma Access 將在其中部署保護您遠端網路位置所需基礎結構的 **Location**（位置）。此區域在地理上應靠近您的遠端網路位置。

如果您尚未為該位置對應的計算位置配置頻寬，Prisma Access 會提示您輸入該計算位置的頻寬。




**STEP 10 |** 選取要用於此遠端網路的 **IPSec Termination Node**（**IPsec** 終端節點）。

Prisma Access 會使用此節點將遠端網路位置與計算位置建立關聯。

**STEP 11 |** （僅限靜態路由或單一通道部署）選取或新增新的 **IPSec Tunnel**（**IPSec** 通道）設定，以存取公司位置上的防火牆、路由器或 SD-WAN 裝置：

- 在 Remote_Network_Template 中選取其中一個預先定義的 IPSec 範本，或是，如果您已將範本新增至包含 IPSec 通道設定的 Remote_Network_Template_Stack（或修改了預先定義的 Remote_Network_Template），請從下拉清單中選取該 **IPSec Tunnel**（**IPSec** 通道）。請注意，您為每個遠端網路連線建立的通道會將 Prisma Access 連線到每個分支位置上支援 IPSec 的裝置。

  設定 IPSec 通道時請遵循下列準則：

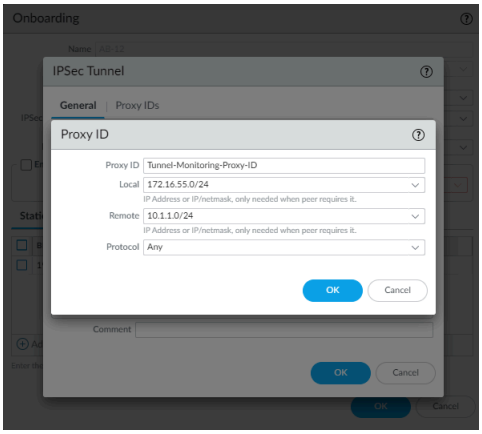
  - IKE 閘道設定中的對等位址對於每個通道而言必須是唯一的。但是，您可以重複使用其他一些常見設定元素，例如密碼設定檔。
  - 您從範本中選取的 IPSec 通道必須僅使用自動金鑰交換和 IPv4。
  - IPSec 通道、IKE 閘道和密碼設定檔名稱不能超過 31 個字元。
  - 如果您使用動態 IKE 對等將多個遠端網路上線到相同位置，則必須對所有遠端網路設定使用相同的 IKE 密碼設定檔。
- 若要建立新的 IPSec 通道設定，請按一下 **New IPSec Tunnel**（新增 **IPSec** 通道），為其提供 **Name**（名稱）並設定 IKE 閘道、IPSec 密碼設定檔和通道監控設定。
  - 如果分支位置上支援 IPSec 的裝置使用政策型 VPN，請在 **Proxy IDs**（**Proxy ID**）頁籤上 **Add**（新增）與本機 IPSec 裝置上設定相符的 Proxy ID，以確保 Prisma Access 可以成功與您的本機裝置建立 IPSec 通道。
- 保持選取 **Enable Replay Protection**（啟用重放保護）以偵測並抵禦重放攻擊。

 ©2025 Palo Alto Networks, Inc.

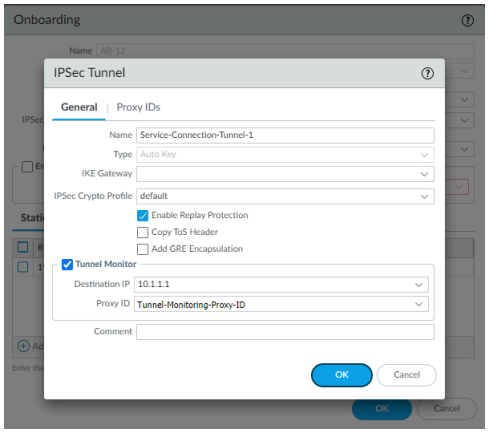
- 選取 **Copy ToS Header**（複製 **ToS** 標頭），將 Type of Service（服務類型 - ToS）標頭從封裝封包的內部 IP 標頭複製到外部 IP 標頭，以保留原始 ToS 資訊。
- 若要為服務連線啟用通道監控，請選取 **Tunnel Monitor**（通道監控）。
  - 請輸入 **Destination IP**（目的地 **IP**）位址。

    在您的分支位置上指定 IP 位址，讓 Prisma Access 可以向該位址傳送 ICMP ping（偵測）請求以進行 IPSec 通道監控。確保 ICMP 可從整個 Prisma Access 基礎結構子網路存取此位址。
  - 如果您對使用多個 Proxy ID 的對等裝置使用通道監控，請指定一個 **Proxy ID** 或新增 **New Proxy ID**（新的 **Proxy ID**），以允許從基礎結構子網路存取您的分支位置。

    下圖顯示 Proxy ID，其中以服務基礎結構子網路（本範例中為 172.16.55.0/24）作為 **Local**（本機）IP 子網路，以分支位置的子網路（本範例中為 10.1.1.0/24）作為 **Remote**（遠端）子網路。




    下圖顯示透過在 **Proxy ID** 欄位中指定 Proxy ID 來將您建立的 Proxy ID 套用至通道監控設定。




您必須在 *CPE* 上設定通往通道監控 *IP* 位址的靜態路由，通道監控才能發揮作用。若要針對從分支位置到 *Prisma Access* 的通道監控，尋找要使用的目的地 *IP* 位址，請選取 ***Panorama > Cloud Services***（雲端服務***) > Status***（狀態***) > Network Details***（網路詳細資料***)***、按一下 ***Service Infrastructure***（服務基礎結構***)***，然後尋找 ***Tunnel Monitor IP Address***（通道監控 ***IP*** 位址***)***。


©2025 Palo Alto Networks, Inc.

**STEP 12 |** 如果您在此位置上有次要 WAN 連結，請選取 **Enable Secondary WAN**（啟用次要 **WAN)**。

務必為每個遠端網路的次要 *WAN* 建立唯一的 *IPSec* 通道；*Prisma Access* 不支援在多個遠端網路中對次要 *WAN* 重複使用相同的 *IPSec* 通道。

以下部署不支援設定次要 WAN：

- 如果您的次要 WAN 與主要 IPSec 通道設定為主動-主動模式。
- 如果您的用戶端裝置 (CPE) 在具有主要和次要 IPSec 通道的等價多路徑 (ECMP) 設定中設定。

如果您使用靜態路由，通道容錯移轉時間會小於 15 秒（從偵測到的時間算起），具體取決於您的 WAN 供應商。

如果設定 BGP 路由並啟用通道監控，則確定安全性參數索引 (SPI) 失敗的最短預設保留時間是通道監控，當連續 15 秒偵測到通道故障時，通道監控會刪除通往對等方的所有路由。這樣一來，通道監控就可以決定 BGP 路由的行為。如果如果未設定通道監控，保留計時器會決定刪除路由之前通道關閉的時間。Prisma Access 會使用 RFC 4271 定義的預設 BGP HoldTime 值：90 秒，這是 Prisma Access 刪除非作用 SPI 的路由之前的最長等待時間。。如果對等 BGP 裝置設定的保留時間較短，則 BGP 保留計時器會使用較小的值。

當次要通道安裝成功後，次要路由會優先採用，直到主要通道恢復正常為止。若主要和次要通道皆正常運作，則優先採用主要路由。

如果您使用不同的 *BGP* 對等來作為次要（備份）連線，*Prisma Access* 不會遵守 *CPE* 公告的多出口鑑別器 *(MED)* 屬性。如果您在遠端網路連線或服務連線上使用多個 *BGP* 對等，則此警告適用。


©2025 Palo Alto Networks, Inc.

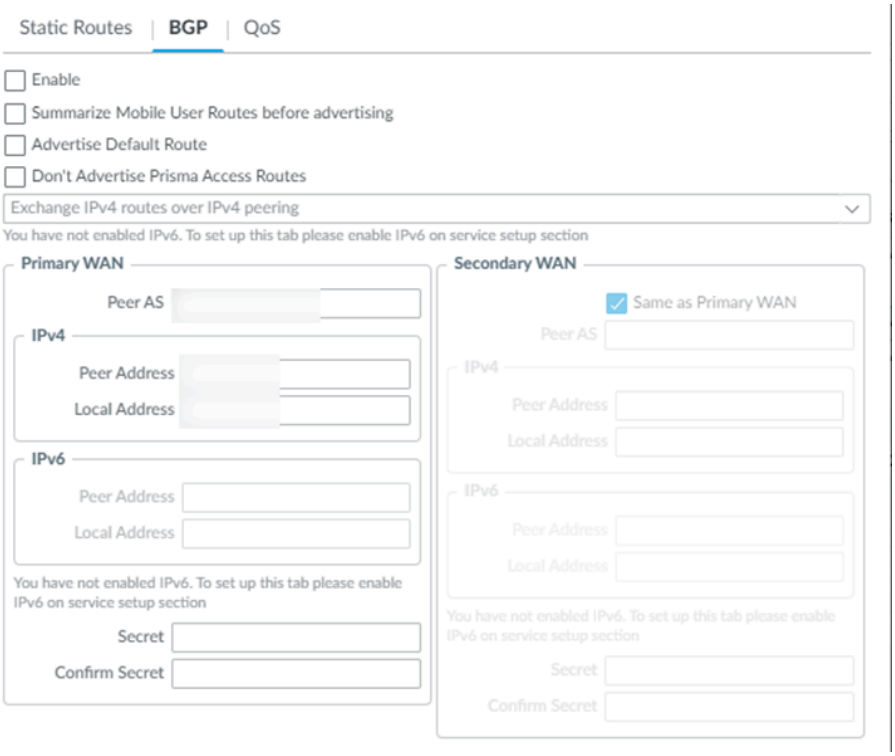
**STEP 13 |** 啟用路由到遠端網路網站上您使用者將需要存取的子網路或個別 IP 位址。

Prisma Access 會使用此資訊將要求路由到適當的網站。每個網站的網路不能彼此重疊，也不能與您為服務基礎結構或為使用者 IP 集區的 Prisma Access 指定的 IP 位址集區重疊。您可以設定 **Static Routes**（靜態路由）、**BGP** 或兩者的組合。

- 若要設定 **Static Routes**（靜態路由）：
  1. 在 **Static Routes**（靜態路由）頁籤上，按一下 **Add**（新增）並輸入遠端使用者將需要存取的資源子網路位址（例如 172.168.10.0/24）或個別 IP 位址，例如 DNS 伺服器（例如，10.32.5.1/32）。
  2. 對 Prisma Access 將需要在此位置存取的所有子網路或 IP 位址重複此動作。




- 若要設定 **BGP**：
  1. 選取 **BGP** 頁籤。
  2. （選用）選取 **ECMP Load Balancing**（**ECMP** 負載平衡）選項。請參閱步驟 8。
  3. 如果為 **ECMP Load Balancing**（**ECMP** 負載平衡）選取 **None**（無），請輸入 BGP 選項。




 ©2025 Palo Alto Networks, Inc.

4. 若要為遠端網路連線啟用 BGP，請選取 **Enable**（啟用）。

   當您啟用 BGP 時，Prisma Access 會將外部 BGP (eBGP) 的存留時間 (TTL) 值設定為 8，以容納 Prisma Access 基礎結構與終止 eBGP 連線的客戶周邊設備 (CPE) 之間可能發生的任何額外躍點。

5. 若要減少透過 BGP 公告至客戶周邊設備 (CPE) 的行動使用者 IP 子網路公告數目，方法為彙總這些公告，請選取**Summarize Mobile User Routes before advertising**（公告前彙總行動使用者路由。

   根據預設，Prisma Access 會在 /24 子網路區塊中公告行動使用者 IP 位址集區；如果你彙總它們，Prisma Access 根據您指定的子網路公告該集區。例如，Prisma Access 使用 /20 子網路公告 10.8.0.0/20 的公用使用者行動 IP 集區，而不是先將該集區劃分為 10.8.1.0/24、10.8.2.0/24、10.8.3.0/24 等子網路，再公告它們。彙總這些公告可以減少 CPE 路由表中儲存的路由數目。例如，您可以使用 IP 集區彙總，搭配可接受有限數目路由的雲端 VPN 閘道（虛擬私人閘道 (VGW) 或傳輸閘道 (TGW)）。

   Prisma Access 會將所彙總行動使用者路由的社群字串設定為 `0xFFFE:0xFFF0`。

6. 若要允許 Prisma Access 使用 eBGP 公告遠端網路的預設路由，請選取 **Advertise Default Route**（公告預設路由）。

   如果您選取 **Advertise Default Route**（公告預設路由），請確保您的網路沒有 BGP 公告的其他預設路由，否則可能會在您的網路中引入路由問題。

   > 您必須先發佈預設路由，然後才能做出此選擇以公告它們。此外，確保您的網路沒有 *BGP* 公告的其他預設路由，否則可能會在您的網路中引入路由問題。

7. 若要防止 Prisma Access 防火牆上的 BGP 對等將路由轉送到您組織的網路，請選取 **Don't Advertise Prisma Access Routes**（不公告 **Prisma Access** 路由）。

   根據預設，Prisma Access 會公告所有 BGP 路由訊息，包括本機路由以及從其他服務連線、遠端網路和行動使用者子網路接收的所有首碼。選取此核取方塊可防止 Prisma


©2025 Palo Alto Networks, Inc.

Access 傳送任何 BGP 公告，但仍會使用其收到的 BGP 資訊，來了解其他 BGP 芳鄰的路由。

自從 Prisma Access 不傳送 BGP 公告後，如果您選取此選項，則必須在內部部署設備上設定靜態路由，以建立回到 Prisma Access 的路由。

8. 輸入 **Peer AS**（對等 **AS**），這是遠端網路上防火牆、虛擬路由器或 BGP 路由器所屬的自發系統 (AS)。
9. 輸入指派為 eBGP 路由器的路由器 ID 的 IP 位址，而此路由器位於您要為其將此連線設定為 **Peer Address**（對等位址）的遠端網路上。
10. （選用）為 BGP 輸入一個位址，Prisma Access 會使用此位址作為其本機 IP 位址。

    指定 **Local Address**（本機位址）很有用，其中連線另一端的裝置（例如 Amazon Web Service (AWS) 虛擬私人閘道）需要特定的本機 IP 位址，才能使 BGP 對等成功。確保您指定的位址不會與基礎結構子網路或遠端網路中子網路中的 IP 位址衝突或重疊。

    您必須在 *CPE* 上設定 *BGP* ***Local Address***（本機位址）的靜態路由。
11. （選用）輸入並確認複雜密碼以驗證 BGP 對等通訊。
12. （選用）如果您設定了 **Secondary WAN**（次要 **WAN**），並且需要變更次要（備份）BGP 對等的 **Peer Address**（對等位址）或 **Local Address**（本機位址），請取消選取 **Same as Primary WAN**（與主要 **WAN** 相同），然後輸入唯一對等，以及選擇性地輸入次要 WAN 的本機 IP 位址。

    如果您在遠端網路部署中使用 IPv6 網路，則可以設定 **IPv6** 位址以及 **IPv4** 位址。您還需要在 Prisma Access 基礎結構中全域啟用 IPv6 網路，然後才能使用 IPv6 定址。

    在某些部署中（例如，使用 BGP 與 AWS VPN 閘道對等時），主要和次要 WAN 的 BGP 對等可能不同。在這些情況下，您可以選擇為次要 WAN 設定不同的 BGP 對等。

    對於搭配次要 *WAN* 的 *BGP* 部署，*Prisma Access* 會同時設定處於 ***UP***（啟動）狀態的主要和次要通道，但遵循網路流量的正常 *BGP* 作用中-備份行為。*Prisma Access* 會將主要通道設定為作用中，並僅透過該通道傳送和接收流量；如果主要通道故障，*Prisma Access* 會使用 *BGP* 規則偵測故障、將次要通道設定為作用中，並僅使用次要通道傳送和接收流量。

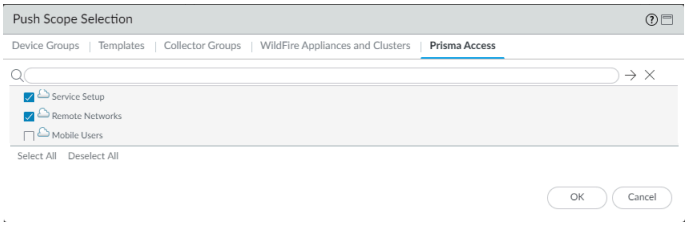
**STEP 14 |** （選用）為該位置啟用 **QoS**，並指定 **QoS Profile**（**QoS** 設定檔）。

您可以在 **Settings**（設定）中根據計算位置指定 QoS 選項和總體設定；不過，您可以在這裡啟用或停用 QoS 或根據位置變更 QoS 設定檔。

 ©2025 Palo Alto Networks, Inc.

**STEP 15 |** 將設定變更提交到 Panorama，並為網路將設定推送到 Prisma Access。

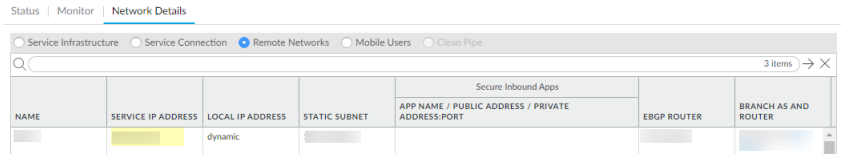
1. 按一下 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**）。
2. 按一下 **Commit**（提交） > **Commit and Push**（提交並推送）。按一下 **Edit Selections**（編輯選取項目） > **Prisma Access**，然後同時選取網路的 Prisma Access 和 Prisma Access 進行服務設定，以將設定推送到服務。




3. 按一下 **OK**（確定）與 **Commit**（提交）。

**STEP 16 |** 在遠端網路位置設定支援 IPSec 的裝置，設定與網路的 Prisma Access 的 IPSec 連線。

1. 為此遠端網路連線尋找 **Service IP Address**（服務 **IP** 位址），方法為選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊）、按一下 **Remote Networks**（遠端網路）選項按鈕，然後檢視 **Service IP Address**（服務 **IP** 位址）欄位。網路基礎結構的 Prisma Access已指派此 IP 位址進行 Prisma Access 遠端網路連線，而且您必須將此項設定為對等 IP 位址，才能在遠端網路位址與網路的 Prisma Access 之間設定 IPSec 通道。




2. 在 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Remote Networks**（遠端網路）頁面上，檢查遠端網路位置上裝置的 **Local IP address**（本機 **IP** 位址）如果您在遠端網路位置執行 NAT，則**Local IP address**（本機 **IP** 位址）會在 NAT 之後面顯示裝置的 IP 位址。

**STEP 17 |** 為了保護遠端網路位置的流量，您必須建立安全性政策規則。

1. 選取 **Policies**（原則）。
2. 選取要在其中新增政策規則的 **Device Group**（裝置群組）。您可以選取 Remote_Network_Device_Group 或您為了定義政策以保護遠端網路位置而選取的父系裝置群組。
3. 建立安全性政策規則。確保您沒有定義安全性政策規則來允許從任何區域到任何區域的流量。在安全性政策規則中，使用您在範本中定義的區域。

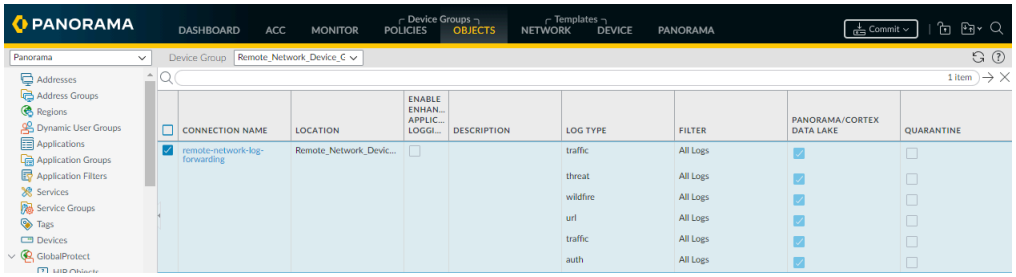
   如果您網路上的使用者存取網站遭拒，請在向 Palo Alto Networks 開立票證之前報告網站存取問題。


©2025 Palo Alto Networks, Inc.

**STEP 18 |** 啟用記錄到 Strata Logging Service。您必須建立一個日誌轉送設定檔，並將此設定檔附加至每個您想要為其轉送日誌的政策規則。

1. 選取 **Objects**（物件）**> Log Forwarding**（日誌轉送）。
2. 選取您已在其中新增政策規則的 **Device Group**（裝置群組），例如 Remote_Network_Device_Group。
3. **Add**（新增）日誌轉送設定檔。在日誌轉送設定檔比對清單中，**Add**（新增）您想要轉送的每一種 **Log Type**（日誌類型）。
4. 選取 **Panorama/Strata Logging Service**（**Panorama/Strata** 記錄服務）作為轉送方法，讓 Prisma Access 可將日誌轉送到 Strata Logging Service。您將能夠監控日誌並從 Panorama 產生報告。Strata Logging Service 提供無縫整合來儲存日誌，無需將其回傳到公司總部的 Panorama，並且 Panorama 可以視需要查詢 Strata Logging Service。

   以下範例啟用將流量、威脅防護、WildFire 提交、URL 篩選、資料篩選和驗證日誌轉送到 Strata Logging Service。




5. 選取 **Policies**（政策）**> Security**（安全性），然後編輯政策規則。在 **Actions**（動作）中，選取所建立的日誌轉送設定檔。

**STEP 19 |** 將您的所有變更提交到 Panorama，並將設定變更推送到 Prisma Access。

1. 按一下 **Commit**（提交）**> Commit and Push**（提交並推送）。
2. **Edit Selections**（編輯選取項目），並在 **Prisma Access** 頁籤中，確保在 **Push Scope**（推送範圍）中選取了 **Prisma Access for networks**（網路的 **Prisma Access**），然後按一下 **OK**（確定）。
3. **Commit and Push**（提交並推送）您的變更。

**STEP 20 |** 檢查遠端網路狀態。

如需詳細資料，請參閱 驗證遠端網路是否已連線至 Prisma Access。


©2025 Palo Alto Networks, Inc.

# 規劃您移轉至新模型的方式

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

新 Prisma Access 遠端網路部署的頻寬是根據每個計算位置的彙總層級配置的，也稱為彙總頻寬模型。在計算位置層級配置頻寬為您在配置授權遠端網路頻寬方面提供了更多彈性，因為 Prisma Access 根據負載或需求動態配置每個位置的頻寬。

如果有一個現有的部署，依 Prisma Access 位置配置頻寬，則您可以移轉到彙總頻寬模型。您也可以移轉遠端網路 QoS 部署。移轉時，所有遠端網路都會使用彙總頻寬模型。

請使用以下檢查清單，為移轉至彙總頻寬模型做好規劃：

- ❑ 請注意以下在移轉後保持不變的遠端網路元件：
  - 資料平面沒有變更。流量會繼續流經 Prisma Access 資料平面，而不會對現有設定做出任何變更。
  - 移轉不會影響現有的通道。

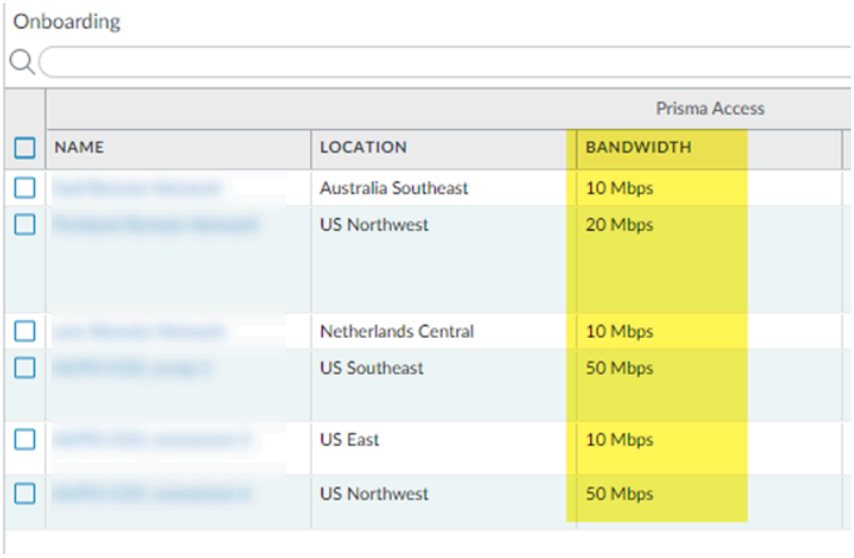
    不需要重新設定您的 IPSec 通道參數。IKE 閘道、IKE 和 IPSec 密碼設定檔，以及 IPSec 通道設定保持不變。
  - 遠端網路 **Service IP Address**（服務 **IP** 位址）（用於 IPSec 通道 Prisma Access 端進行遠端網路連線的 公用 IP 位址），在您將部署移轉到彙總頻寬模型時，不會為每個遠端網路進行變更。
- ❑ Prisma Access 會在移轉到彙總頻寬模型期間指派 IPSec 終端節點，並將頻寬配置給遠端網路。在移轉之前，您應該瞭解這個模型的運作方式。

  如果您想要在移轉後將現有的遠端網路重新指派給另一個 *IPSec* 終端節點，則在提交並推送您的變更之後，*Prisma Access* 會將另一個 ***Service IP Address***（服務 ***IP*** 位址）指派給遠端網路。在此情況下，您需要重新設定您的 *CPE*，以指向遠端網路通道的新 *IP* 位址。
- ❑ 如果您有不受支援的設定，將看不到 [Bandwidth Allocation（頻寬配置）] 頁籤，也無法檢視要移轉的橫幅。不支援以下設定移轉至彙總頻寬模型：
  - 頻寬為 **1000 Mbps** 的遠端網路。
  - 與版本早於 3.0 的 Prisma Access 的 Prisma SD-WAN CloudBlade 整合。
  - 在 2.1 Innovation 之前，對遠端網站上應用程式提供安全輸入存取的遠端網站設定。

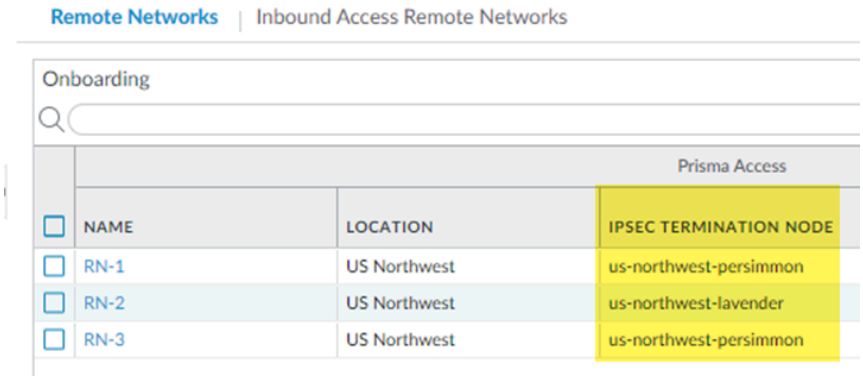
  如果您使用 QoS 搭配遠端網路，請務必在移轉之前遵循 QoS 移轉指導方針。


©2025 Palo Alto Networks, Inc.

- 如果您不確定您的部署正在使用哪個模型，請選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路）。
  - 如果您在遠端網路區域看到 **Bandwidth**（頻寬）欄位，則表示您正在依 Prisma Access 位置配置頻寬，並且可以移轉到彙總頻寬模型。



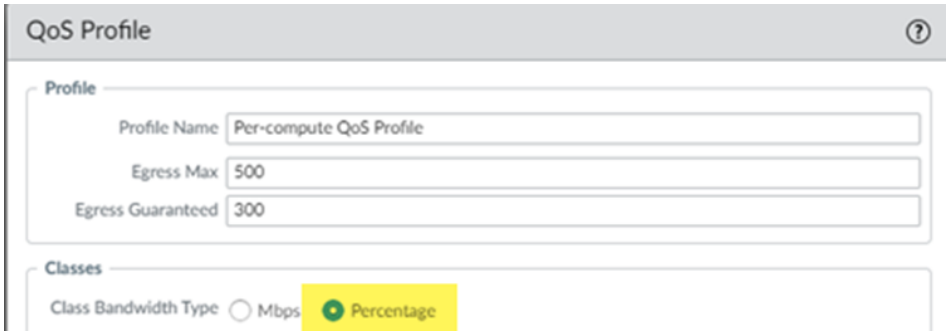

  - 如果看到 **IPSec Termination Node**（**IPSec** 終端節點），則您已移轉到彙總頻寬模型。




- 在移轉到彙總頻寬模型之後，變更是永久的，您無法還原為具有依 Prisma Access 位置配置頻寬的部署。
- 您必須具有至少 50 Mbps 的可用頻寬，才能移轉到彙總頻寬模型。


©2025 Palo Alto Networks, Inc.

- 如果您想要在移轉後實作 QoS，請瞭解有關為彙總頻寬部署設定 QoS 的差異。
  - 請務必在您的 QoS 設定檔中使用 **Percentage**（百分比）的 **Class Bandwidth Type**（類別頻寬類型），而不是 **Mbps**。對於依計算位置配置頻寬的部署，Prisma Access 不支援 QoS 設定檔中 **Mbps** 的頻寬類型。




  - 瞭解如何指定保證頻寬比，以及如何自訂每個網站的頻寬。

    使用保證頻寬比，您可以在計算位置配置總配置頻寬的百分比。Prisma Access 會依計算位置中的 IPSec 終端節點數目均分保證頻寬。

    透過自訂每個網站的頻寬，您可以為單一 IPSec 終端節點上的網站套用一個配置比，並在遠端網路 **Settings**（設定）中指定每個網站的 QoS 設定檔。或者，您可以在遠端網路設定期間指定 QoS 設定檔，方法是選取遠端網路，並在 **QoS** 頁籤中指定 QoS 設定檔。

- 如果您已設定遠端網路，對您的遠端網路位置提供安全輸入存取，則所有現有的輸入存取功能均受到支援，例如啟用次要 WAN 連結（**Enable Secondary WAN**（啟用次要 **WAN**））、BGP、QoS 和來源 NAT 選項。也沒有對 Prisma Access 配置的公用 IP 位址所消耗頻寬進行任何變更（5 個 IP 位址佔用遠端網路授權配置的 150 Mbps，而 10 個 IP 位址佔用 300 Mbps）。

  如果您需要在移轉後設定輸入存取，請使用彙總頻寬模型特有的輸入存取程序。

- Palo Alto Networks 建議您在移轉前記下您現有的頻寬設定和總授權頻寬。

  雖然 *Prisma Access* 會在移轉期間移轉您的頻寬；但您應該記下目前設定作為最佳做法，並在移轉後對計算位置頻寬進行任何調整。

  - 檢查您現有的頻寬設定，方法是選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路），並記下每個遠端網路連線可用的現有 **Bandwidth**（頻寬）。
  - 導覽至 **Panorama** > **Licenses**（授權），並針對遠端網路檢查您的總授權頻寬（以 Mbps 為單位）。此資訊包含在 **Prisma Access Net Capacity**（網路容量）或 **GlobalProtect Cloud Service for Mobile Users**（適用於行動使用者的 **GlobalProtect Cloud Service**）中，取決於您的授權類型。

移轉後，請注意以下的部署差異：

- 您使用彙總頻寬遠端網路裝載程序裝載所有新的遠端網路。
- 當您檢視頻寬使用統計資料時，您會在每個 IPSec 終端節點層級檢視它們。

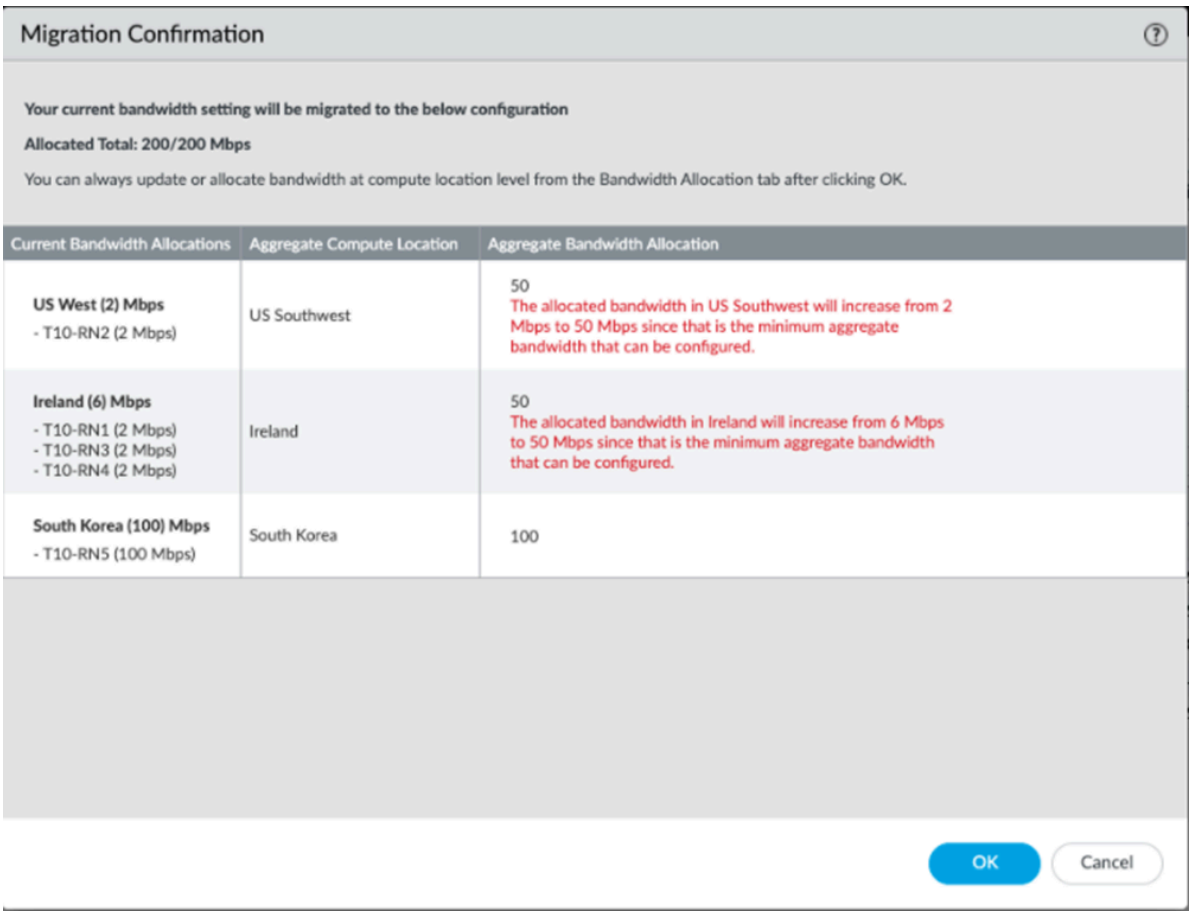

©2025 Palo Alto Networks, Inc.

# 移轉後彙總頻寬部署的頻寬配置

如果您有一個部署，依 Prisma Access 位置配置頻寬，則在您移轉至彙總頻寬模型時，Prisma Access 會進行以下變更。

- Prisma Access 會將給定計算位置的所有頻寬相加，並將相加的頻寬配置給該計算位置。

  例如，您在墨西哥西部、美國西南部和美國西部有三個位置（位置 **1**、位置 **2** 和位置 **3**），而且每個現有位置都有 50 Mbps 的頻寬。由於每個位置都位於美國西南部計算位置，因此 Prisma Access 會將三個位置的頻寬相加，並將 150 Mbps 的頻寬配給置美國西南部位置。
- 如果計算位置中所有位置的頻寬總計小於 50 Mbps，Prisma Access 將會將該計算位置的頻寬增加到 50 Mbps。Prisma Access 為您提供移轉過程中需要增加頻寬的位置。



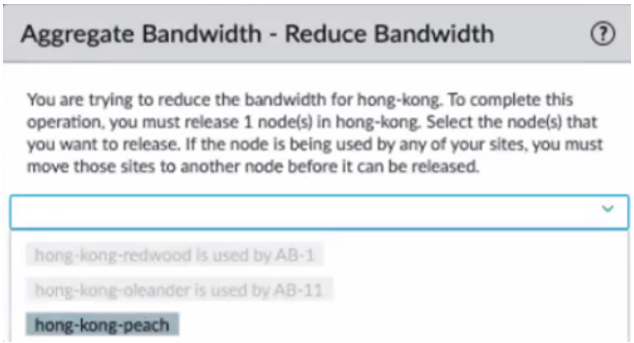

 ©2025 Palo Alto Networks, Inc.

- Prisma Access 會在彙總頻寬部署中使用 IPSec 終端節點。移轉期間，Prisma Access 會為每 1,000 Mbps 的配置頻寬提供每個計算位置一個 IPSec 終端節點。例如，如果您在計算位置配置 1500 Mbps 的頻寬，則 Prisma Access 會為該位置提供兩個 IPSec 終端節點。

  您會在遠端網路裝載時將 IPSec 終端節點配置給遠端網路。在彙總頻寬移轉中，Prisma Access 會在移轉期間將 IPSec 終端節點與遠端網路建立關聯。下列清單為移轉提供了一些 IPSec 終端節點關聯範例：

  - 如果您有四個遠端網路位於同一計算位置，並且這些位置每個都有 50 Mbps 的頻寬，則 Prisma Access 會將 200 Mbps 的頻寬配置給該計算位置、為該計算位置提供單一 IPSec 終端節點，並將該 IPSec 終端節點與所有四個遠端網路建立關聯。
  - 如果您在同一計算位置有三個遠端網路，每個遠端網路有 100 Mbps，則 Prisma Access 會將 300 Mbps 的頻寬配置給該計算位置、為該計算位置提供單一 IPSec 終端節點，並將該 IPSec 終端節點與所有三個遠端網路建立關聯。
  - 如果您在同一計算位置有七個遠端網路，其中兩個遠端網路各有 500 Mbps，五個遠端網路各有 100 Mbps，則 Prisma Access 會將 1500 Mbps 的頻寬配置給該計算位置。因為該計算位置中的總配置頻寬大於 1,000 Mbps，所以 Prisma Access 會配置兩個 IPSec 終端節點並建立以下關聯：
    - 這兩個 500 Mbps 遠端網路獲指派一個 IPSec 終端節點（每個 1,000 Mbps 遠端網路一個節點）。
    - 五個 100 Mbps 遠端網路獲指派一個 IPSec 終端節點。

  移轉後，您可以變更 IPsec 終端節點關聯，以增加位置的頻寬。例如，假設一個計算位置有兩個 IPsec 終端節點，您可以將單一 IPsec 終端節點重新指派給單一位置，並將其他 IPsec 終端節點重新指派給剩餘的位置，這可有效地提供不與更多頻寬共用 IPsec 終端節點的位置。
- 如果您想要減少足夠多的頻寬，則可能需要釋出一個 IPsec 終端節點。例如，如果您將計算位置中的頻寬從 1500 Mbps 減少至 800 Mbps，將需要移除其中一個現有的 IPSec 終端節點。如果這些節點中的任何一個正在被現有位置使用，您必須在刪除 IPSec 終端節點之前重新指派 IPSec 終端節點。




## QoS 移轉指導方針

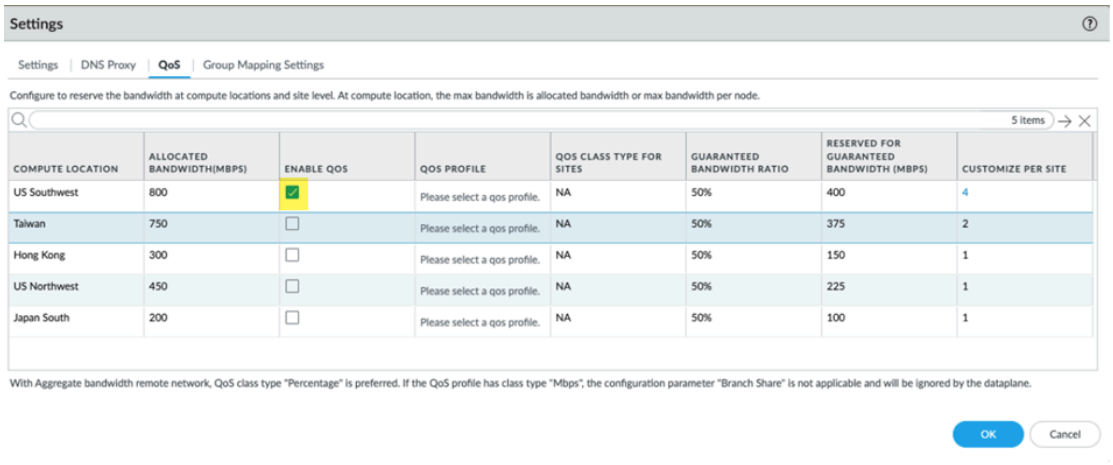
如果您使用 QoS 搭配目前的 Prisma Access 遠端網路部署，並依位置配置頻寬，則可以移轉到彙總頻寬部署，同時又保留現有的 QoS 政策和設定檔。

使用彙總頻寬模型，您在每個計算位置的彙總層級配置頻寬，而且 Prisma Access 會根據每個位置的負載或需求動態配置頻寬。

 ©2025 Palo Alto Networks, Inc.

移轉後，**QoS** 頁籤顯示遠端網路設定中的 QoS 設定（**Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路） > **Settings**（設定））。對應到已啟用 QoS 的位置的任何計算位置都選取了 **Enable QoS**（啟用 **QoS**）；對應到未啟用 QoS 的位置的任何計算位置都取消選取了 **Enable QoS**（啟用 **QoS**）。

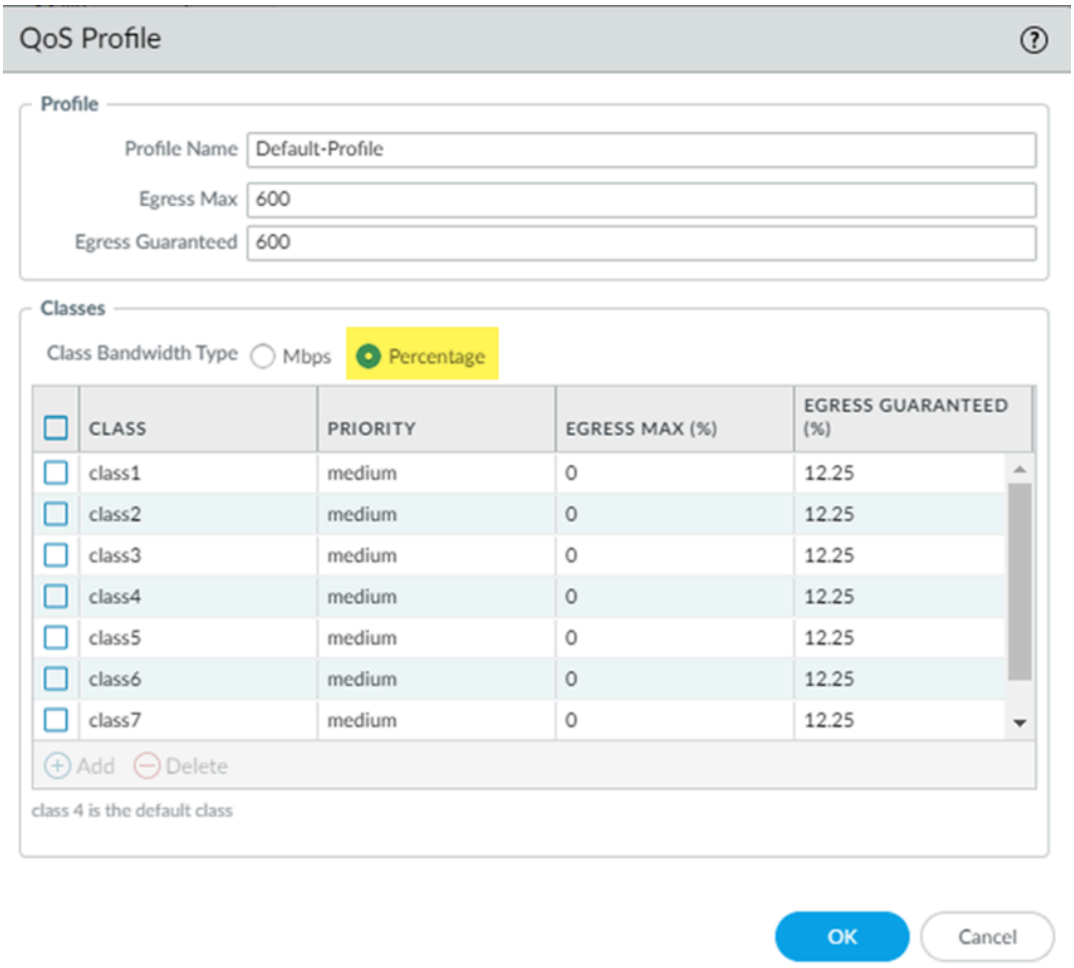
以下螢幕擷取畫面顯示了移轉後的 QoS 頁籤範例。美國西部位置的遠端網路已啟用 QoS，其他位置則未啟用 QoS。由於美國西部位置對應到美國西南部計算位置，因此 **QoS** 頁籤顯示美國西南部計算位置已啟用 QoS。




Palo Alto Networks 對於彙總頻寬部署中的 QoS 提出了以下建議和需求。


©2025 Palo Alto Networks, Inc.

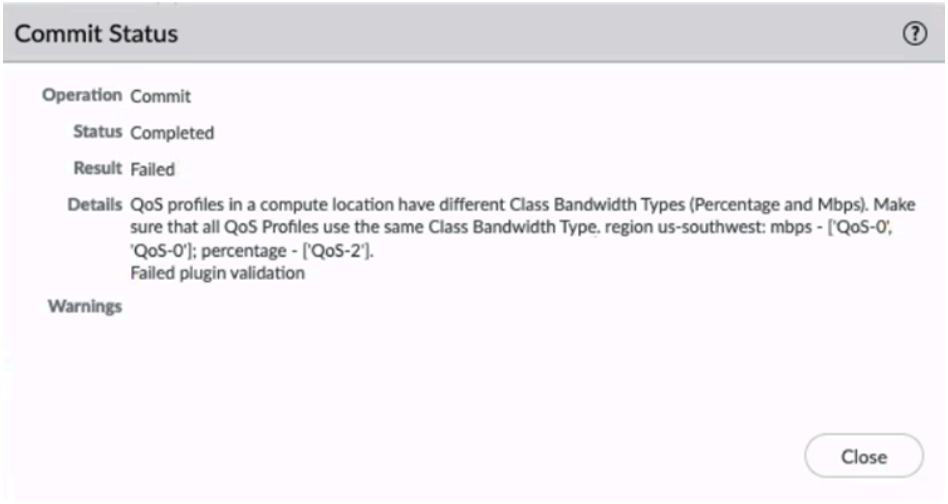
- 因為單一計算位置中的所有位置共用頻寬，所以您應該將 **Mbps** 的 **Class Bandwidth Type**（類別頻寬類型）變更為 **Percentage**（百分比）。唯一支援頻寬類型為 **Mbps** 的時候，是您有一個現有的部署，依位置配置頻寬，然後您再移轉到彙總頻寬部署。




- 您無法根據設定檔中的 Mbps 調整 QoS 頻寬配置；對於使用 **Percentage**（百分比）頻寬類型的設定檔，您可以透過調整保證頻寬比和自訂每個網站的 QoS 設定檔來變更每個位置的 QoS 頻寬。


©2025 Palo Alto Networks, Inc.

- 您無法在計算位置中混合頻寬類型；如果這樣做，您在提交時會收到錯誤訊息。

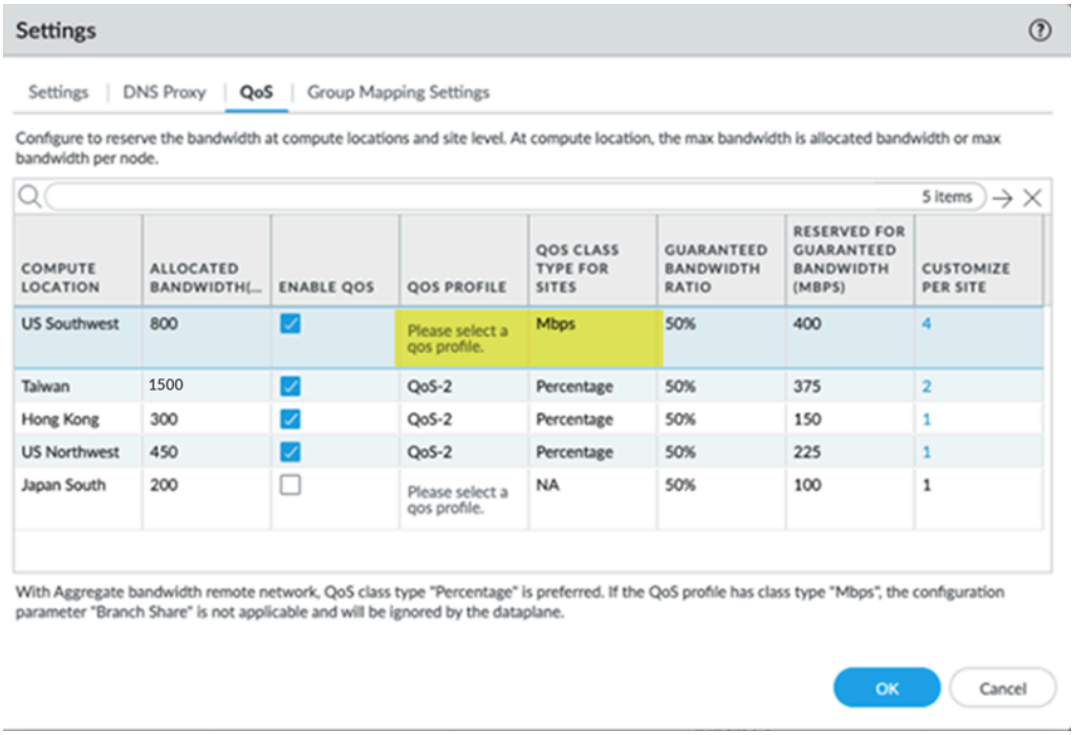



- 如果您新增位置，而這些位置屬於新的計算位置，您將只能夠在新的計算位置中建立 **Class Bandwidth Type**（類別頻寬類型）為 **Percentage**（百分比）的設定檔。
- 如果您保留 **Class Bandwidth Type**（類別頻寬類型）為 **Mbps** 的 QoS 設定檔，則您對保證頻寬比所做的任何變更或自訂每個網站的 QoS 設定檔會被忽略。
- 移轉後，若有任何位置使用 **Class Bandwidth Type**（類別頻寬類型）為 **Mbps** 的 QoS 設定檔，則在 **QoS** 頁籤中會為其對應計算位置顯示 **QoS Class Type For Sites**（網站的 **QoS** 類別類


©2025 Palo Alto Networks, Inc.

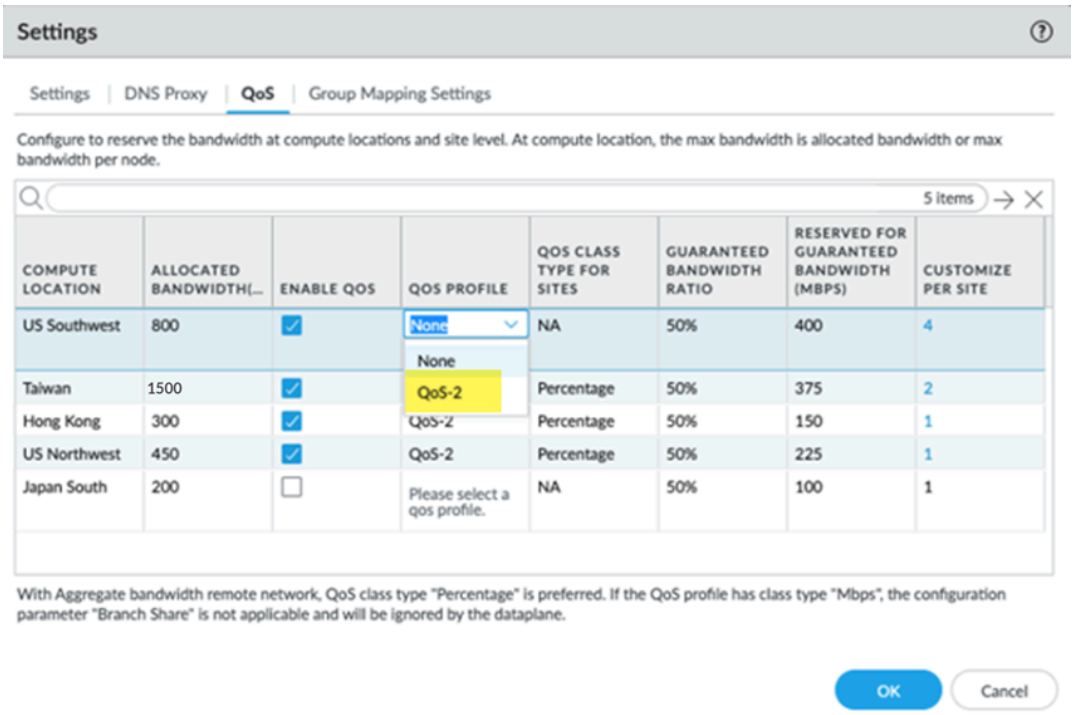
型）為 **Mbps**。**Class Bandwidth Type**（類別頻寬類型）為 **Percentage**（百分比）的 QoS 設定檔顯示 **QoS Class Type For Sites**（網站的 **QoS** 類別類型）為 **Percentage**（百分比）。

此外，您無法選取 **Class Bandwidth Type**（類別頻寬類型）為 **Mbps** 的任何 QoS 設定檔。以下螢幕擷取畫面顯示美國西南部計算位置使用 **Class Bandwidth Type**（類別頻寬類型）為 **Mbps** 的 QoS 設定檔。該選項無法在 **QoS Profile**（**QoS** 設定檔）區域的下拉式清單中選取。

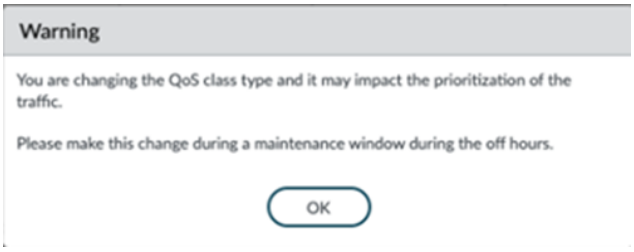



不過，您可以選取其使用的 **Class Bandwidth Type**（類別頻寬類型）為 **Percentage**（百分比）的 QoS 設定檔（此範例中的 QoS-2）。


©2025 Palo Alto Networks, Inc.

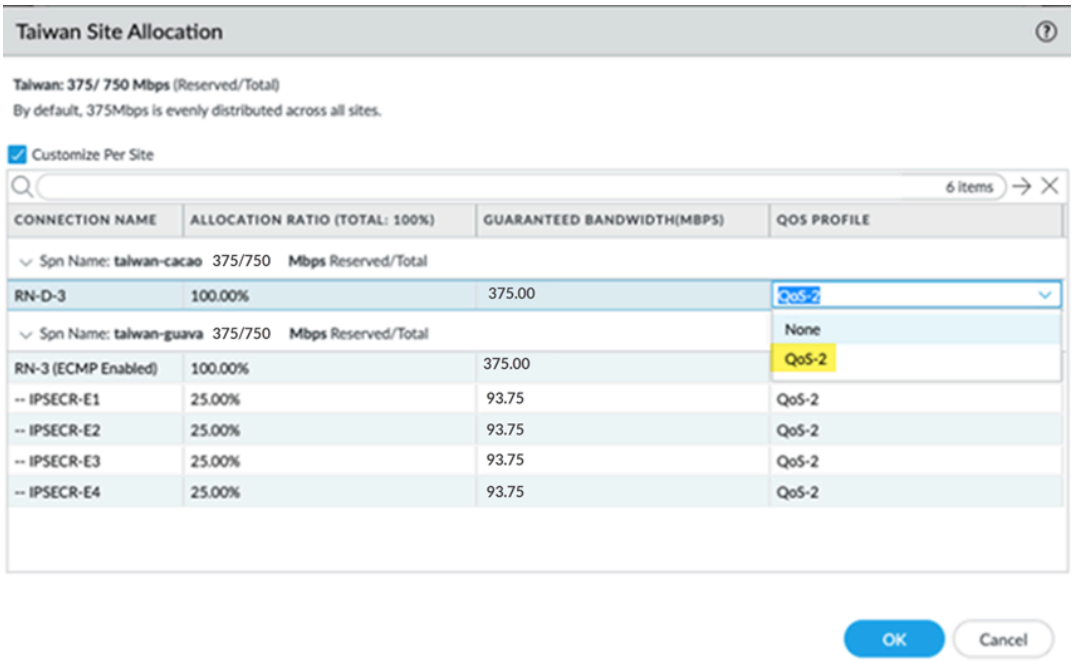



- 如果您將計算位置的 QoS 設定檔，其 **Class Bandwidth Type**（類別頻寬類型）從 **Mbps** 變更為 **Percentage**（百分比），則您應在維護時段或非高峰時段進行變更。變更 QoS 設定檔可能會變更流量優先順序。




 ©2025 Palo Alto Networks, Inc.

- 自訂每個網站的 QoS 設定檔時，您只能選取 **Class Bandwidth Type**（類別頻寬類型）為 **Percentage**（百分比）的 QoS 設定檔。




# 移轉您的頻寬管理設定

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

瞭解如何移轉您的頻寬管理設定。

如果你有一個依位置配置頻寬的 Prisma Access 遠端網路部署，Prisma Access 允許您移轉到依計算位置配置頻寬的部署（彙總頻寬模型），使您的部署更加靈活且可調整。在檢閱移轉計劃檢查清單之後，請使用下列步驟移轉至彙總頻寬模型。您也可以移轉遠端網路 QoS 部署。遷移時，所有遠端網路都會使用彙總頻寬模型。

在移轉頻寬設定之前，請記住以下幾點：

- 以下遠端網路元件在移轉後保持不變：
  - Prisma Access 資料平面。
  - 對現有通道沒有影響。
  - 無需重新設定 IPSec 通道參數。
  - IKE 閘道、IKE 和 IPSec 密碼設定檔，以及 IPSec 通道設定保持不變。
  - 對於每個遠端網路，遠端網路 **Service IP Address**（服務 **IP** 位址）不會變更。
- Prisma Access 會在移轉到彙總頻寬模型期間配置 IPSec 終止節點，並將頻寬配置給遠端網路。


©2025 Palo Alto Networks, Inc.

- 如果您有不受支援的設定，將看不到 [Bandwidth Allocation（頻寬配置）] 頁籤，也無法檢視要移轉的橫幅。
- 如果您有 QoS 搭配遠端網路，請務必在移轉之前遵循 QoS 移轉指導方針。
- 在移轉到彙總頻寬模型之後，變更是永久的，您無法還原為具有依 Prisma Access 位置配置頻寬的部署。
- 您必須具有至少 50 Mbps 的可用頻寬，才能移轉到彙總頻寬模型。
- 如果您想要在移轉後實作 QoS，請瞭解有關為彙總頻寬部署設定 QoS 的差異。
- 一旦移轉，您就會使用彙總頻寬遠端網路裝載程序裝載所有新的遠端網路。
- 一旦移轉，當您檢視頻寬使用統計資料時，您就會在每個 IPSec 終止節點層級查看它們。
- 請勿使用 CLI 執行移轉；僅使用 UI 進行移轉。
- Strata Cloud Manager
- Panorama

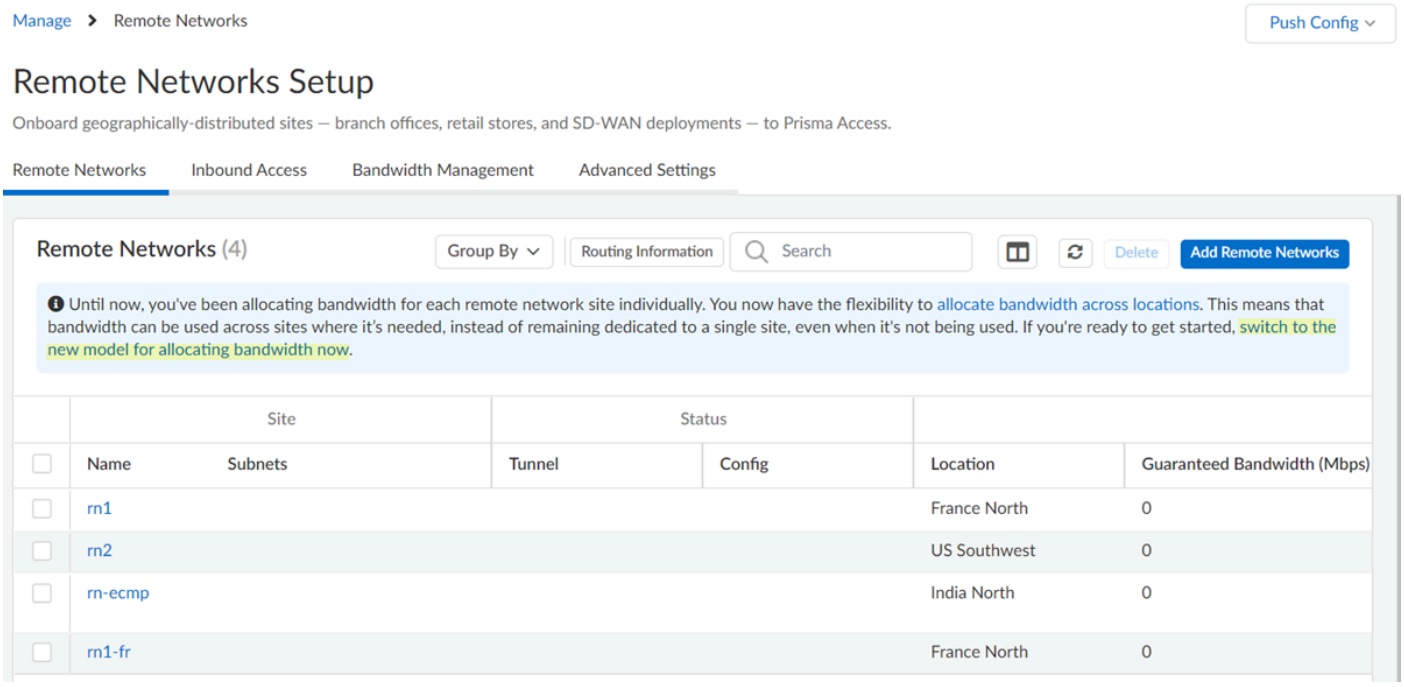
## 移轉您的頻寬管理設定 (Strata Cloud Manager)

如果你有一個依位置配置頻寬的 Prisma Access 遠端網路部署，Prisma Access 允許您移轉到依計算位置配置頻寬的部署（彙總頻寬模型），使您的部署更加靈活且可調整。在檢閱移轉計劃檢查清單之後，請使用下列步驟移轉至彙總頻寬模型。

**STEP 1 |** 選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Remote Networks**（遠端網路）。

 ©2025 Palo Alto Networks, Inc.

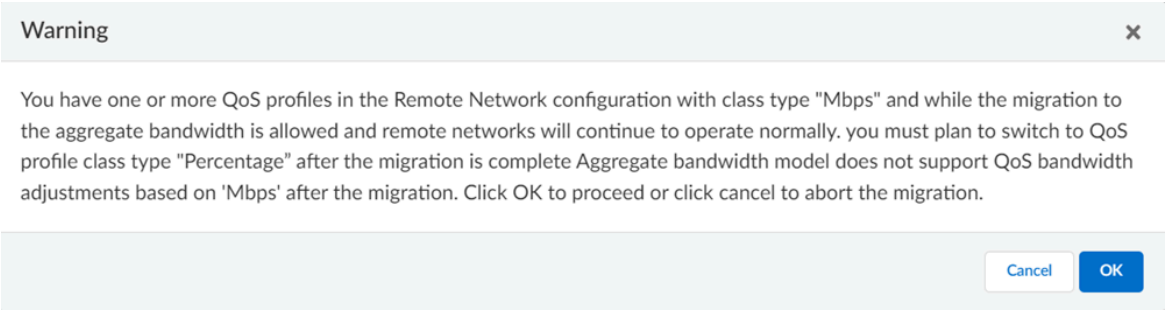
**STEP 2 |** 現在切換到新的頻寬配置模型。



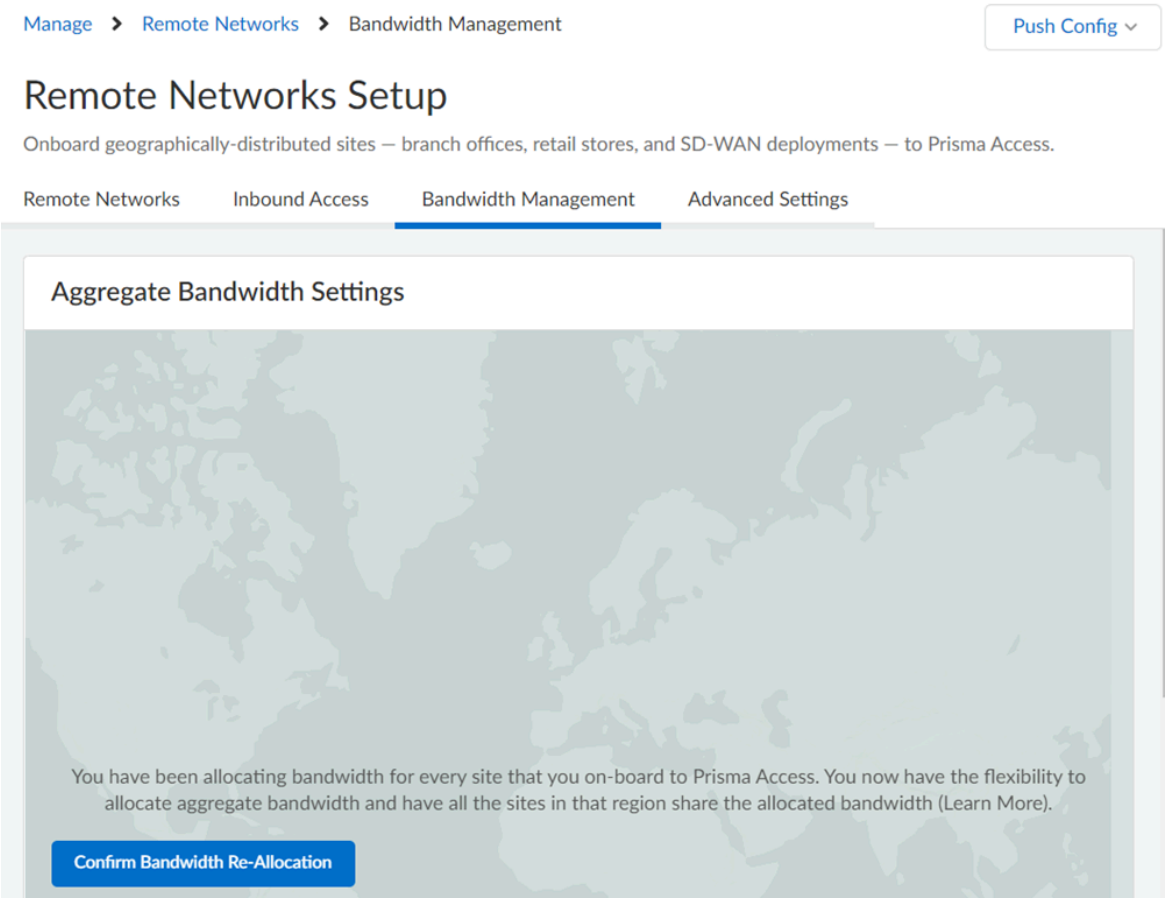


©2025 Palo Alto Networks, Inc.

- 如果您有 ***Class Bandwidth Type***（類別頻寬類型）為 ***Mbps*** 的 *QoS* 設定檔，*Prisma Access* 會通知您應計劃將這些設定檔的 ***Class Bandwidth Type***（類別頻寬類型）變更為 ***Percentage***（百分比）。



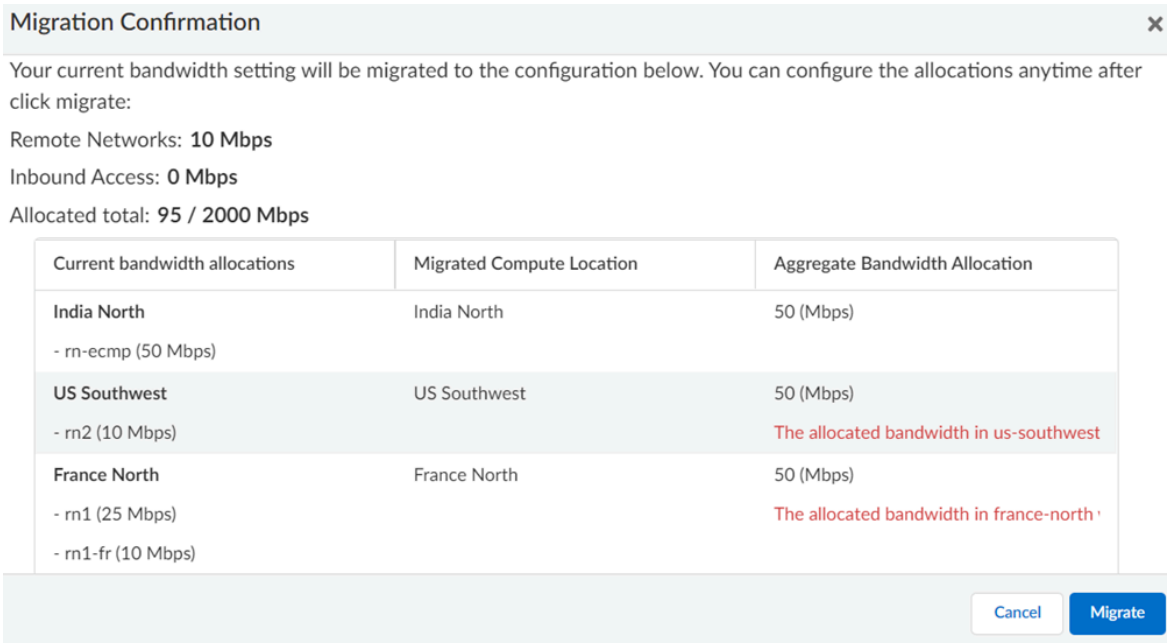

- 或者，在 ***Bandwidth Management***（頻寬管理）頁籤中，選取 ***Confirm Bandwidth Re-Allocation***（確認頻寬重新配置）。




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 檢閱資訊並在顯示的快顯視窗中選取 **Migrate**（移轉）。

如果計算位置中所有位置的頻寬總計小於 *50 Mbps*，*Prisma Access* 將會將該計算位置的頻寬增加到 *50 Mbps*。*Prisma Access* 為您提供移轉過程中需要增加頻寬的位置。




移轉至彙總頻寬模型是永久且不可逆的。移轉前，請先檢閱移轉前檢查清單。您必須 ***Commit and Push***（提交並推送）變更才能使其生效。

Prisma Access 會將您配置的遠端網路頻寬移轉到彙總頻寬模型。

**STEP 4 |** **Commit and Push**（提交並推送）您的變更。

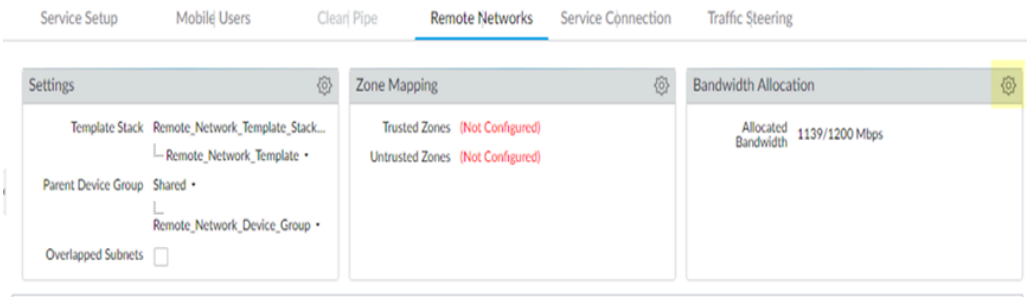
## 移轉您的頻寬管理設定 (Panorama)

如果你有一個依位置配置頻寬的 Prisma Access 遠端網路部署，Prisma Access 允許您移轉到依計算位置配置頻寬的部署（彙總頻寬模型），使您的部署更加靈活且可調整。在檢閱移轉計劃檢查清單之後，請使用下列步驟移轉至彙總頻寬模型。

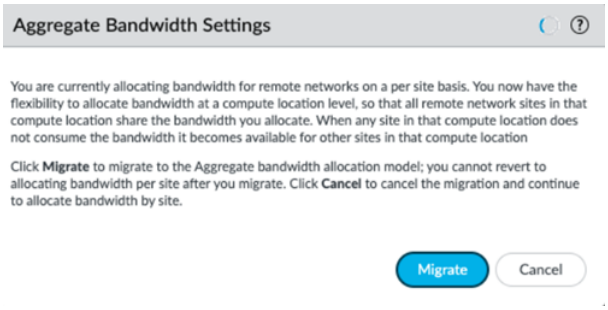
**STEP 1 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路）。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 按一下 **Bandwidth Allocation**（頻寬配置）區域中的齒輪圖示來編輯設定。

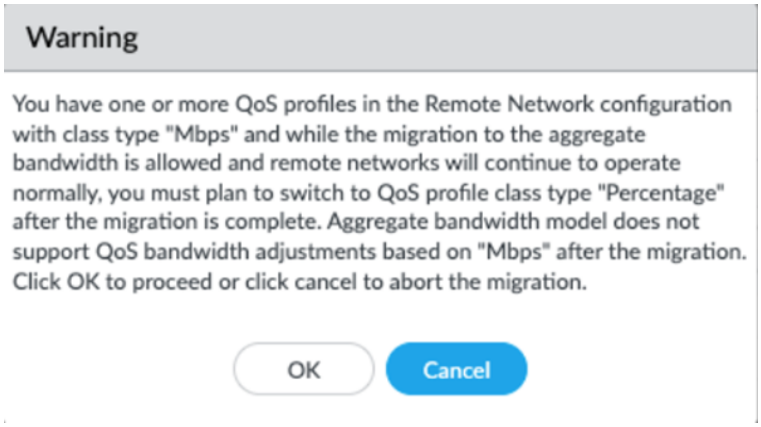



**STEP 3 |** 在顯示的快顯視窗中選取 **Migrate**（移轉）。




移轉至彙總頻寬模型是永久且不可逆的。移轉前，請先檢閱移轉前檢查清單。您必須 ***Commit and Push***（提交並推送）變更才能使其生效。

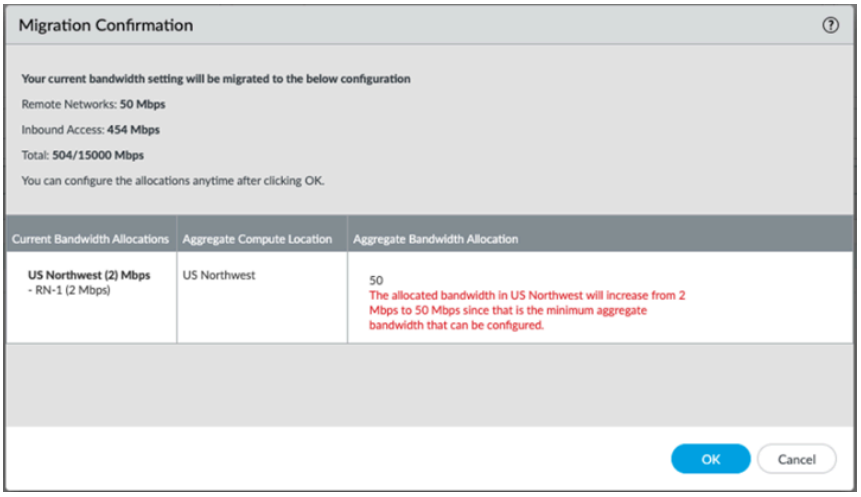
如果您有 ***Class Bandwidth Type***（類別頻寬類型）為 ***Mbps*** 的 *QoS* 設定檔，*Prisma Access* 會通知您應計劃將這些設定檔的 ***Class Bandwidth Type***（類別頻寬類型）變更為 ***Percentage***（百分比）。



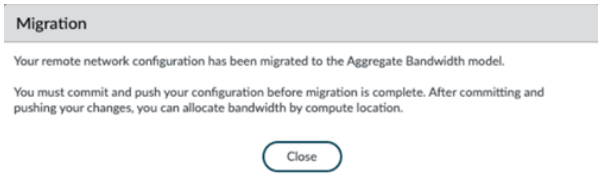

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 檢閱 **Migration Confirmation**（移轉確認）視窗中的資訊，然後按一下 **OK**（確定）。

如果計算位置中所有位置的頻寬總計小於 *50 Mbps*，*Prisma Access* 將會將該計算位置的頻寬增加到 *50 Mbps*。*Prisma Access* 為您提供移轉過程中需要增加頻寬的位置。




Prisma Access 會將您配置的遠端網路頻寬移轉到彙總頻寬模型，並顯示確認視窗。按一下 **Close**（關閉）以關閉視窗。




**STEP 5 |** **Commit and Push**（提交並推送）您的變更。


©2025 Palo Alto Networks, Inc.

# 裝載遠端網絡

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

一旦您為遠端網路進行規計劃，就可以開始設定程序。這包括裝載遠端網路、將遠端網站連線至 Prisma Access，以及為遠端網路啟用路由和 QoS。針對您想要使用 Prisma Access for Networks 保護的每個遠端網路，請將所需的政策設定推送至 Prisma Access，並裝載每個遠端網路，以便您可以開始從遠端網站透過 IPsec 通道將流量傳送至 Prisma Access。請使用下列其中一個程序來裝載您的遠端網路，取決於您的頻寬配置類型：

瞭解如何裝載遠端網路。

- Strata Cloud Manager
- Panorama

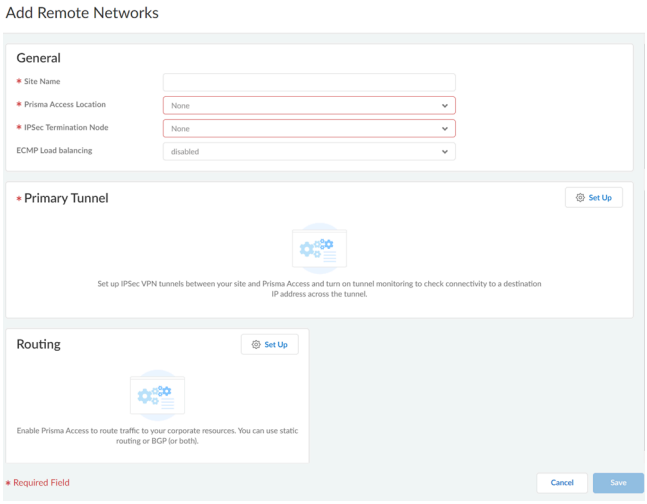
## 裝載遠端網路 (Strata Cloud Manager)

以下是將新的遠端網站新增至 Prisma Access 的方式。首先指定位置並定義要配置給連線的頻寬量。

**STEP 1 |** 啟動 Prisma Access (Managed by Strata Cloud Manager)。

**STEP 2 |** 確保您已將頻寬配置給將在其中部署遠端網路的位置。請參閱 遠端網路的規劃檢查清單。

**STEP 3 |** 前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Remote Networks**（遠端網路） > **Add Remote Networks**（新增遠端網路）。




**STEP 4 |** 給與遠端網路描述性 **Site Name**（網站名稱）。


©2025 Palo Alto Networks, Inc.

**STEP 5 |** 選取網站所在的 **Region**（區域），以及最近的 Prisma Access **Location**（位置）。

**STEP 6 |** （僅當您計劃使用 BGP 進行動態路由時）啟用 **ECMP Load Balancing**（**ECMP** 負載平衡），以便遠端網站最多可以使用四個 IPSec 通道。

ECMP 負載平衡需要 BGP；不支援 QoS 和靜態路由。

當您啟用 ECMP 時，遠端網路流量將透過您設定的通道進行負載平衡。

**STEP 7 |** 設定 **Advanced Settings**（進階設定）。

- （選用）使用 **Static Entries**（靜態項目）將 FQDN 解析為特定 IP 位址。

  如果您的組織中有來賓網際網路服務，並且您想要來賓安全地使用搜尋引擎，防止他們搜索可能違反公司政策的可能不適當或冒犯性資料，則此功能可能非常有用。若要這樣做，請為靜態項目規則輸入唯一的 **Name**（名稱），並輸入 **FQDN** 和應該在其中導向 FQDN 要求的 IP **Address**（位址）。

- 如果想要 Prisma Access 對 DNS 要求進行 Proxy，請設定 **UDP Queries Retries**（**UDP** 查詢重試）的值（以秒為單位重試查詢的 **Interval (Sec)**（間隔（秒））），以及重試 **Attempts**（嘗試）的執行次數）。

**STEP 8 |** 將遠端網站連線到 Prisma Access，您將在其中建立一個 IPSec VPN 通道，以將遠端網站連線到 Prisma Access.

**STEP 9 |** 設定靜態路由。

1. 對於將流量路由至總部或資料中心，以及從總部或資料中心路由流量的靜態路由，請 **Add**（新增）要在分支上保護的 IP 子網路或 IP 位址。

   如果您對總部或資料中心網路上的 IP 子網路進行任何變更，則必須手動更新靜態路由。

**STEP 10 |** 設定動態路由。

1. 對於公告總部或資料中心子網路的動態路由，**Enable BGP for Dynamic Routing**（啟用 **BGP** 進行動態路由）。
2. （選用）選取 **MRAI Timer**（**MRAI** 計時器）值。

   BGP 路由會提供一個計時器，您可以用來在網路中定制 BGP 路由聚合，稱為最小路由公告間隔 *(MRAI)*。MRAI 會採取行動，根據每個目的地限制更新速率，而且 BGP 路由器至少會等待設定的 MRAI 時間，然後再傳送相同首碼的公告。較小的數字為您提供更快的聚合時間，但會在您的網路中建立更多的公告。較大的數字會減少可以傳送的公告數目，

 ©2025 Palo Alto Networks, Inc.

但也會使路由聚合速度變慢。您可以決定在網路中放置的數字，以在更快的路由聚合和更少的公告之間取得最佳平衡。

設定介於 1 與 600 秒之間的 MRAI 範圍，預設值為 30 秒。

3. 若要減少透過 BGP 對客戶周邊設備 (CPE) 進行的行動使用者 IP 子網路公告數目，請指定 Prisma Access，以在公告子網路之前彙總這些子網路，方法為選取 **Summarize Mobile User Routes before advertising**（在公告之前彙總行動使用者路由）。

   根據預設，Prisma Access 會在 /24 子網路區塊中公告行動使用者 IP 位址集區；如果你彙總它們，Prisma Access 根據您指定的子網路公告該集區。例如，Prisma Access 使用 /20 子網路公告 10.8.0.0/20 的公用使用者行動 IP 集區，而不是先將該集區劃分為 10.8.1.0/24、10.8.2.0/24、10.8.3.0/24 等子網路，再公告它們。彙總這些公告可以減少 CPE 路由表中儲存的路由數目。例如，您可以使用 IP 集區彙總，搭配可接受有限數目路由的雲端 VPN 閘道（虛擬私人閘道 (VGW) 或傳輸閘道 (TGW)）。

4. （選用）若要讓 Prisma Access 使用 eBGP 為遠端網路起始預設路由公告，請選取 **Advertise Default Route**（公告預設路由）。確保您的網路沒有 BGP 公告的其他預設路由，否則可能會在您的網路中引入路由問題。

5. （選用）如果您設定了次要 WAN，並且需要變更次要（備份）BGP 對等的對等位址，請選取 **Use different BGP Peer for Secondary Tunnel**（針對次要通道使用不同的 **BGP** 對等），然後輸入唯一對等，以及選擇性地輸入次要 WAN 的本機 IP 位址。

6. （選用）選取 **Do Not Export Routes**（不匯出路由），防止 Prisma Access 將路由轉送到總部或資料中心。

   根據預設，Prisma Access 會公告所有 BGP 路由訊息，包括本機路由以及從其他服務連線、遠端網路和行動使用者子網路接收的所有首碼。選取此核取方塊可防止 Prisma Access 傳送任何 BGP 公告，但仍會使用其收到的 BGP 資訊，來了解其他 BGP 芳鄰的路由。

   因為 *Prisma Access* 不傳送 *BGP* 公告後，所以如果您選取此選項，則必須在您的內部部署設備上設定靜態路由，以建立回到 *Prisma Access* 的路由。

7. 輸入 **Peer IP Address**（對等 **IP** 位址），其已指派為總部或資料中心網路上 eBGP 路由器的路由器 ID。

8. 輸入 **Peer AS**（對等 **AS**），這是您網路的自發系統 (AS)。

   使用符合 RFC 6996 的 BGP 私人 AS 編號。

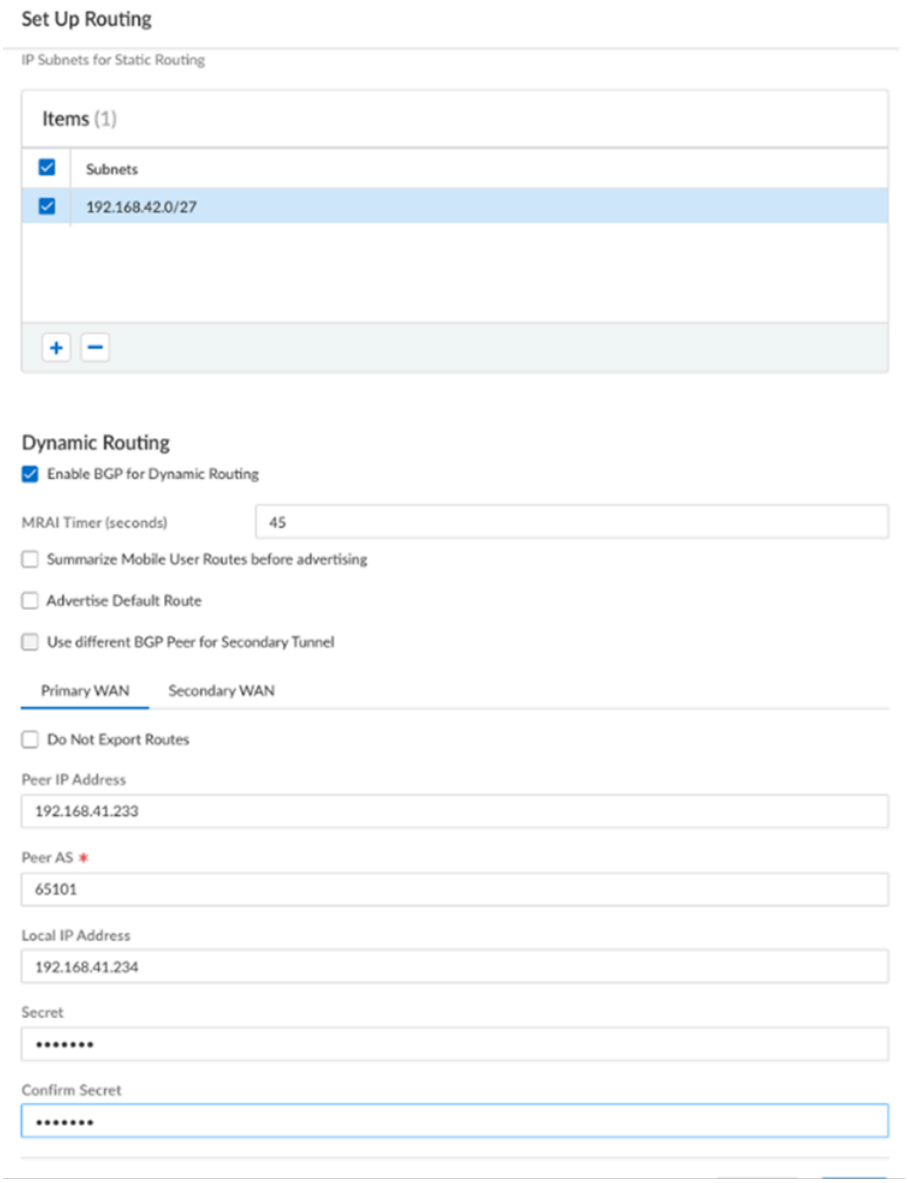
9. 輸入 **Local IP Address**（本機 **IP** 位址），Prisma Access 會將其用作 BGP 的本機 IP 位址。

   僅當您的總部或資料中心裝置需要本機位址，BGP 對等才能成功時，才需要此本機位址。確保您指定的位址不與遠端網路中基礎結構子網路中的 IP 位址衝突或重疊。

10. 輸入 **Secret**（密碼）密碼，驗證 BGP 對等通訊。

 ©2025 Palo Alto Networks, Inc.

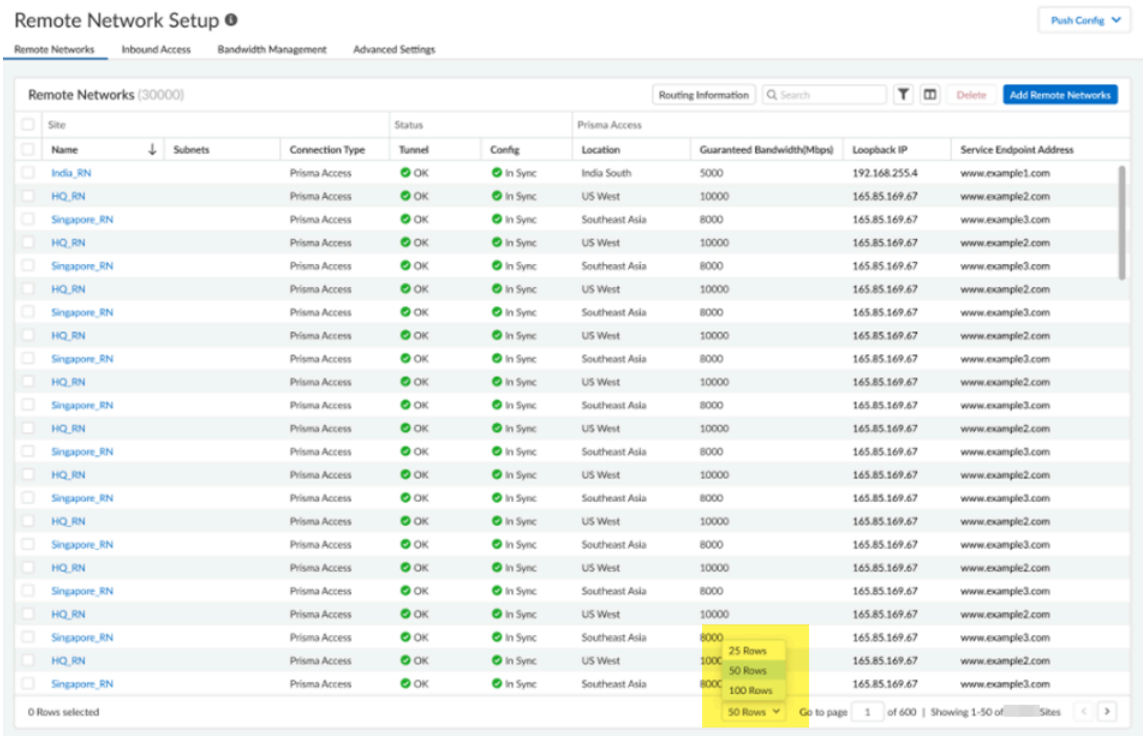
11. 選取 **Confirm Secret**（確認密碼）。




從 *Prisma Access 5.2* 開始，您可以在 *Prisma Access* 部署中每個租用戶最多裝載 *25,000* 個遠端網路和 *50,000* 個 *IKE* 閘道。為了適應這項增強功能，已對 *Strata Cloud Manager* 網頁介面進行下列變更：

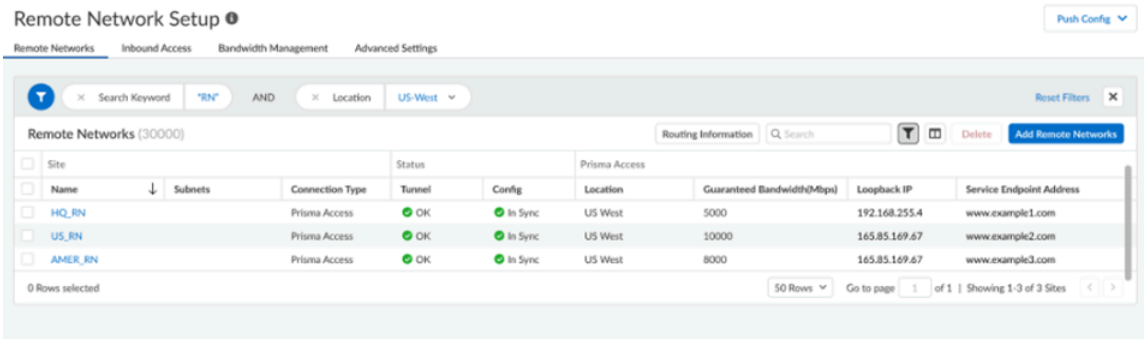
- 啟用分頁，以便您可以選擇要在給定頁面中顯示的列數。


©2025 Palo Alto Networks, Inc.

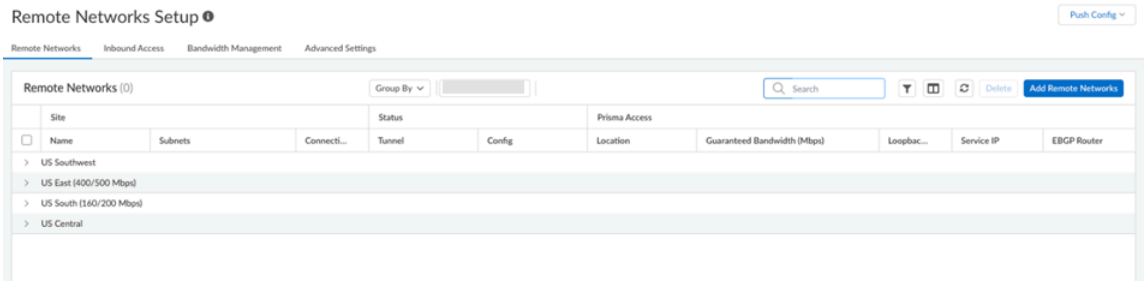



- 啟用遠端網路的篩選。

  套用篩選之後，您可以依名稱來排序所產生的輸出。



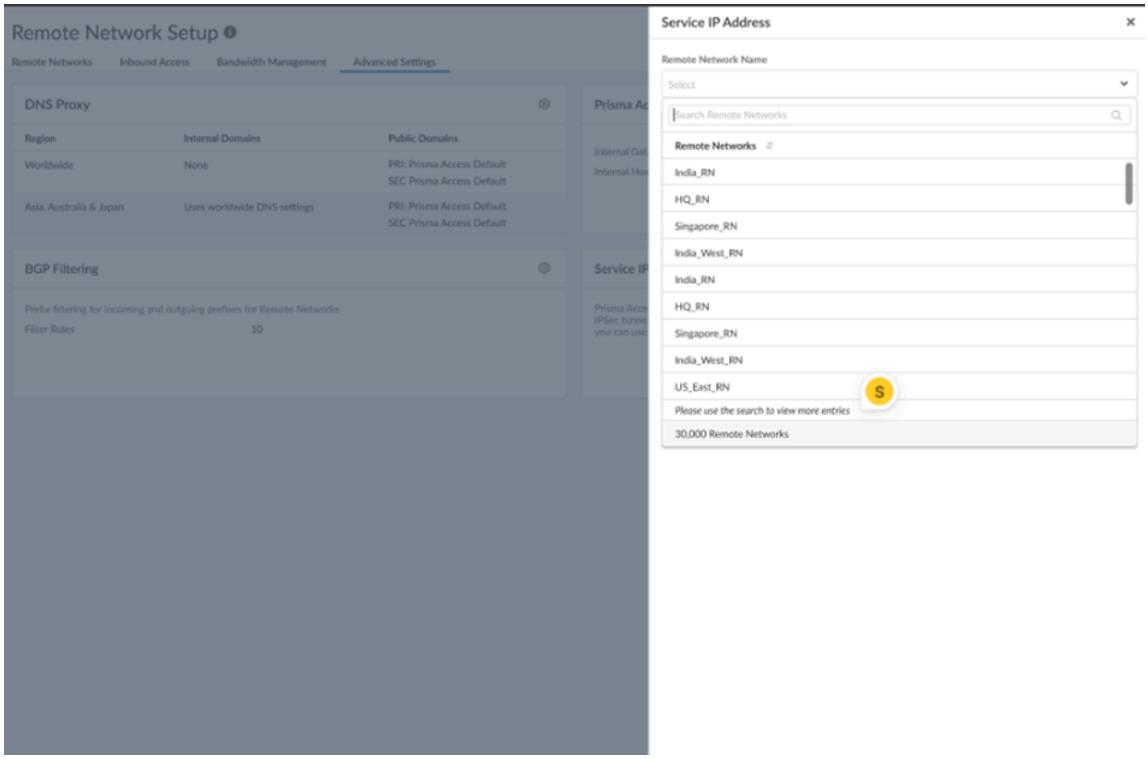

- 新增了 **Group By**（分組方式）欄位。如果您選取分組方式 **Compute Location**（計算位置），則會顯示但摺疊所有群組，而且您已選取的頁面大小會套用至這些群組。如果您選取計算位置以將其展開，則會根據您已選取的頁面大小來顯示列。




 ©2025 Palo Alto Networks, Inc.

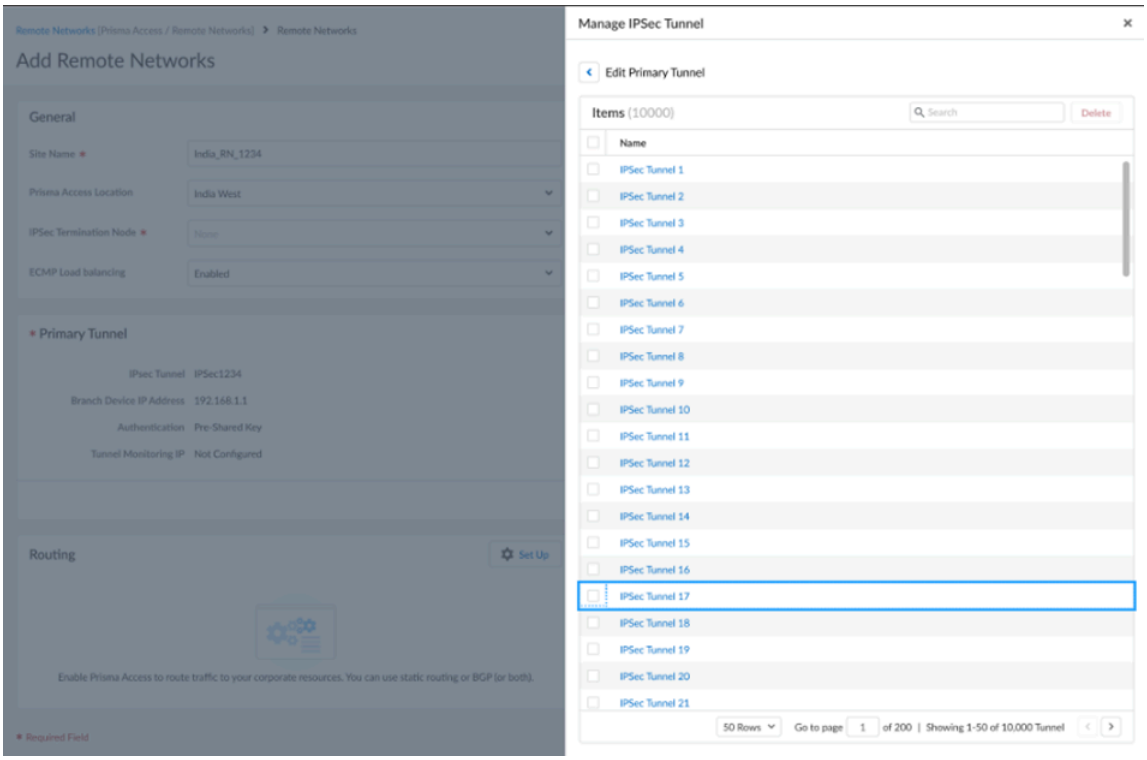
- 以下拉式清單顯示遠端網路時，網頁介面會顯示前 500 個項目。您可以在文字方塊中輸入內容，於清單中找到所需的遠端網路。

  此外，還會顯示遠端網路的總數。

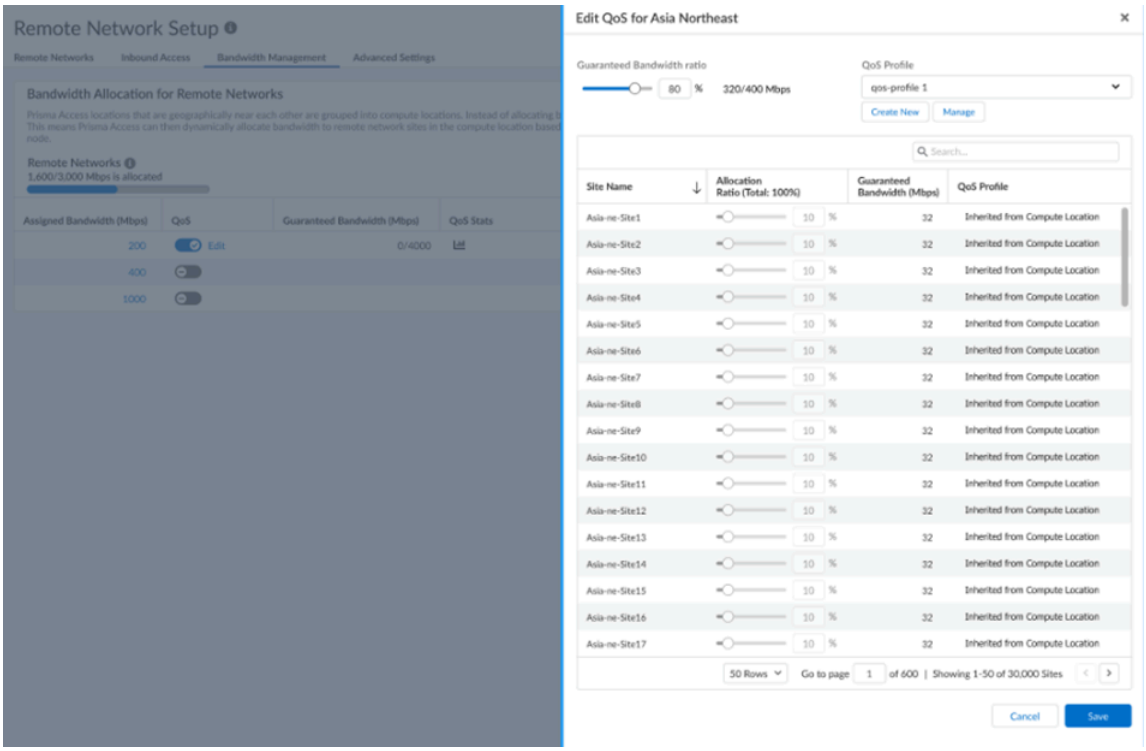



- 下列額外頁面已套用分頁：
  - IPSec 通道：

 ©2025 Palo Alto Networks, Inc.

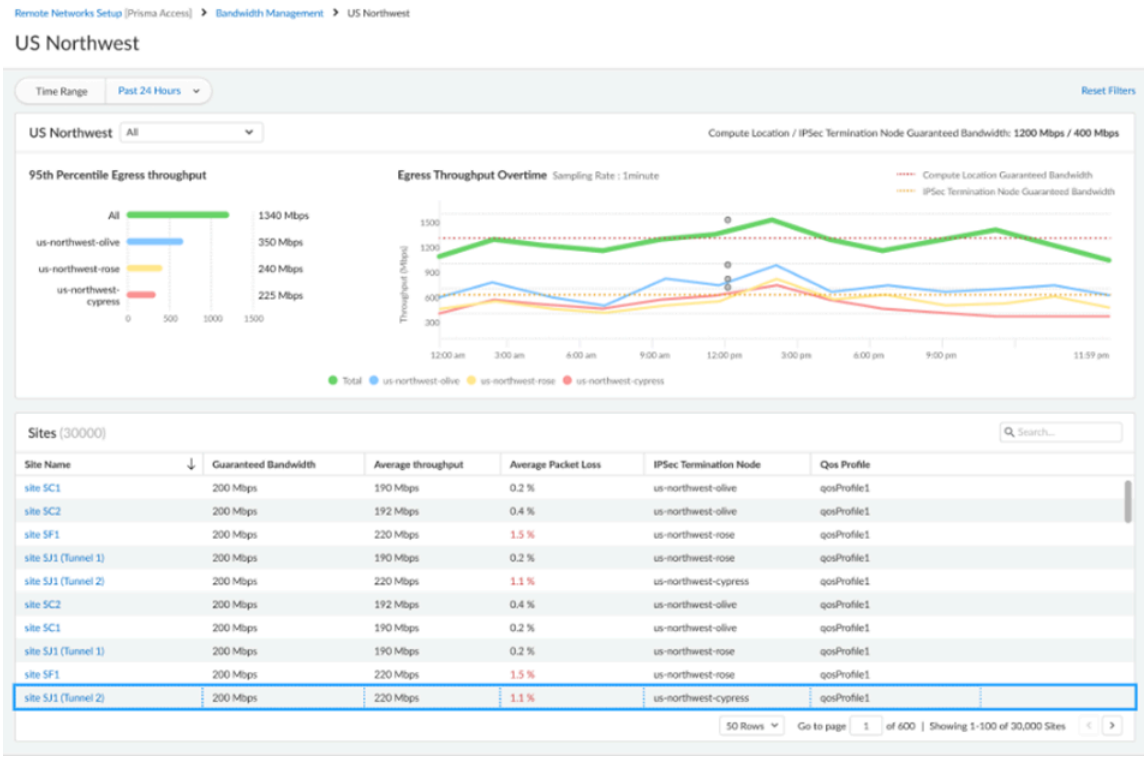



- QoS：

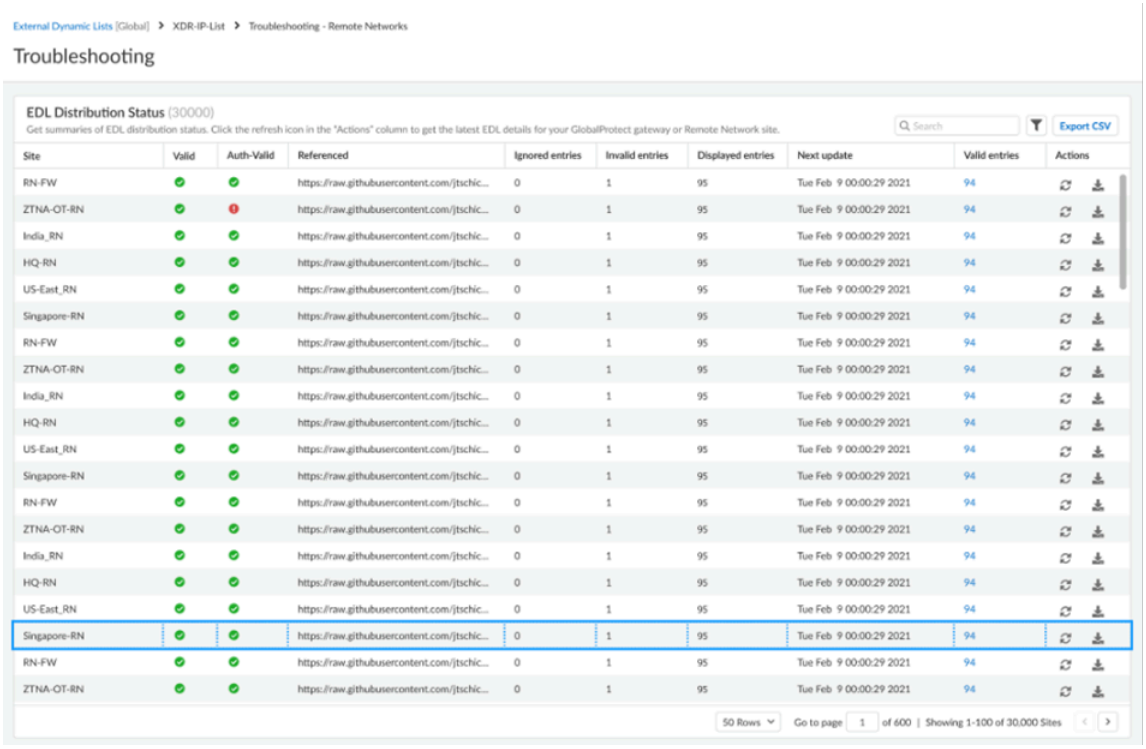



- QoS 統計資料：

 ©2025 Palo Alto Networks, Inc.




- **External Dynamic Lists**（外部動態清單）下方的 **Troubleshooting**—**Remote Networks**（疑難排解—遠端網路）：




# 裝載遠端網路 (Panorama)

若要設定依計算位置配置頻寬的 Prisma Access 遠端網路部署，請完成下列步驟。

 ©2025 Palo Alto Networks, Inc.

如果您需要裝載許多遠端網路（高達 *1,000* 個），您可以使用以下程序裝載遠端網路，然後將遠端網路設定匯出到 CSV 檔案、將您要裝載的其他遠端網路新增至 *CSV* 檔案，然後匯入該 *CSV* 檔案以將此設定儲存至 *Prisma Access*。

**STEP 1 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路），並按一下 **Settings**（設定）區域中的齒輪圖示編輯設定。

1. 在 [Templates（範本）] 區段中，**Add**（新增）任何範本，其中包含您要推送到 Prisma Access for Networks 的設定。例如，如果您有包含區域設定，或 IPSec 通道、IKE 閘道，或密碼設定檔設定的現有範本，則可以將它們新增到預先定義的 Remote_Network_Template_Stack，以簡化裝載程序。

   您可以將多個範本 **Add**（新增）至堆疊，然後使用 **Move Up**（上移）和 **Move Down**（下移）適當地排序它們.這一點很重要，因為 Panorama 會在堆疊中從上到下進行評估，堆疊中較高範本中的設定優先於堆疊中較低範本中指定的相同設定。請注意，您無法從堆疊頂部移動預設範本。

   雖然您可以從外掛程式將現有範本新增到堆疊，但無法從外掛程式建立新範本。相反，請使用工作流程來 Add（新增）範本。
2. 為 Prisma Access for Remote Networks 選取 **Parent Device Group**（父系裝置群組）。您可以選取現有的裝置群組或使用 **Shared**（共用）。

   您將推送所有設定—包括 安全性政策、安全性設定檔和其他政策物件（例如應用程式群組和物件，以及位址群組）、HIP 物件和設定檔，以及驗證政策—Prisma Access for Networks 需要使用您在這裡指定的 device group hierarchy（裝置群組階層），對遠端網路使用者強制執行一致的政策。

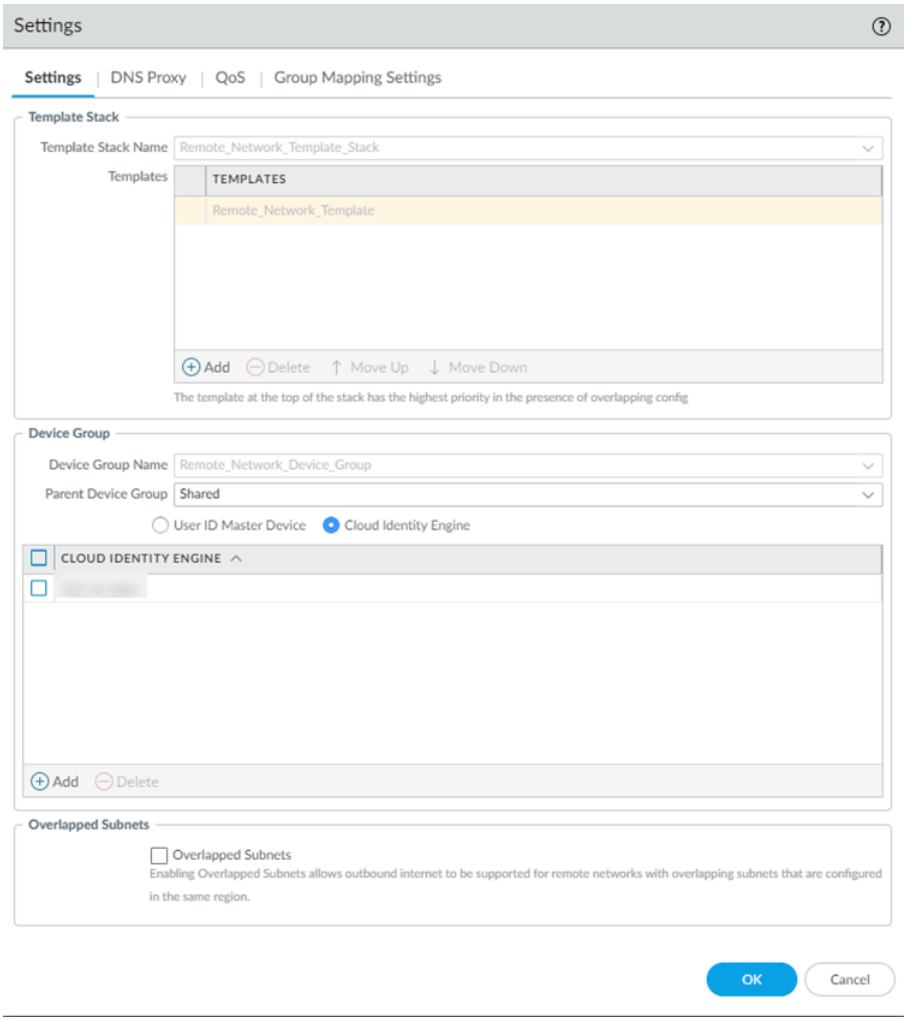
   您不需要定義將推送到遠端網路的所有政策。相反，請設定要裝載遠端網站的設定。然後，您可以返回並新增具有完整設定的範本和裝置群組，以將一致的政策推送到您的遠端網路。
3. （選用）如果您已將新世代防火牆設定為主要裝置，或已新增雲端識別引擎設定檔，讓使用者和群組資訊可在安全性政策中選取，請選取 **User-ID Master Device**（**User-ID** 主要

 ©2025 Palo Alto Networks, Inc.

裝置）或 **Cloud Identity Engine**（雲端識別引擎）；然後，選取您建立的主要裝置或雲端識別引擎設定檔。

4. 如果將要設定具有重疊子網路的遠端網路，請選取 **Overlapped Subnets**（重疊子網路）核取方塊，為這些位置啟用輸出網際網路存取。

   雖然設定子網路重疊的遠端網路位置會引入一些限制，但在某些情況下是可以接受的（例如，如果要在零售店位置新增來賓網路）。



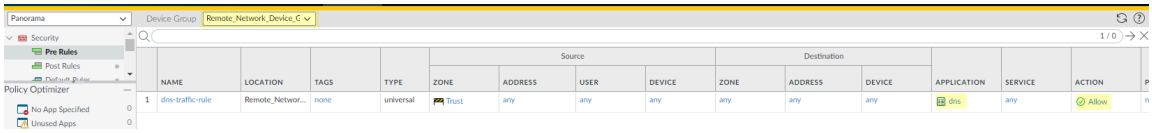

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** （選用）為您的遠端網路設定 **DNS Proxy** 設定。

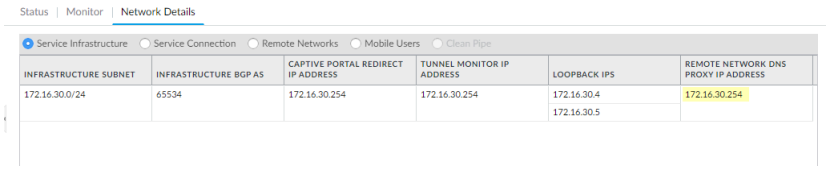
Prisma Access 可讓您指定 DNS 伺服器，以解析組織內部網域和外部網域。如果未指定任何設定，則 Prisma Access 不會對遠端網路的 DNS 要求進行 Proxy。

1. 在 **Remote_Network_Device_Group** 裝置群組中，選取 **Policies**（政策） > **Security**（安全性），並 **Add**（新增）安全性政策規則，其中 **Application**（應用程式）為 **DNS**，而 **Action**（動作）為 **Allow**（允許），以允許 DNS 流量。

   若沒有允許 DNS 流量的安全性政策規則，則 DNS 解析不會發生。




2. 如果您將 Prisma Access 設定為從遠端網路對 DNS 要求進行 Proxy，請更新該網路中所有端點上的 DNS 設定，以使用 Prisma Access **Remote Network DNS Proxy IP Address**（遠端網路 **DNS Proxy IP** 位址）作為主要 DNS 伺服器，並使用您的 DNS 伺服器作為次要 DNS 伺服器。您可以從 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Service Infrastructure**（服務基礎結構）取得此 DNS Proxy IP。




3. **Add**（新增）一或多個 **DNS Proxy** 設定，輸入下列值：

   - 從視窗頂部的下拉式清單中選取一個 **Region**（區域）。

     選取 **Worldwide**（全球）以全域套用 DNS 設定、選取特定劇院，或選取每個位置群組的設定（小於劇院的位置群組）。如果新增多個設定，則首先使用位置群組設定，接著是劇院設定，然後是全球設定。Prisma Access 在清單中從上到下評估規則。

   - **Add**（新增）一或多個規則以設定 **Internal Domain**（內部網域）的 DNS 設定。
     - 為規則輸入唯一的 **Rule Name**（規則名稱）。
     - 如果您想要內部 DNS 伺服器僅解析您指定的網域，請在 **Domain List**（網域清單）中輸入要解析的網域。在網域前面指定一個星號；例如，*.acme.com。。您最多可以指定 1,024 個網域項目。
     - 如果您有可以存取內部網域的 **Custom DNS server**（自訂 **DNS** 伺服器），請指定 **Primary DNS**（主要 **DNS**）和 **Secondary DNS**（次要 **DNS**）伺服器 IP 位址，或

 ©2025 Palo Alto Networks, Inc.

選取 **Use Cloud Default**（使用雲端預設值）以使用預設 Prisma Access DNS 伺服器。

- 指定 **Public Domains**（公用網域） 的 DNS 設定。
  - **Use Cloud Default**（使用雲端預設值）—使用預設 Prisma Access DNS 伺服器。
  - **Same as Internal Domains**（與內部網域相同）—使用您用來解析內部網域的同一伺服器。選取此選項時，用來解析公用網域的 DNS 伺服器與 **Internal Domains**（內部網域）區段中為第一個規則設定的伺服器相同。
  - **Custom DNS server**（自訂 **DNS** 伺服器）—如果您有可存取公用（外部）網域的 DNS 伺服器，請在該欄位中輸入主要 DNS 伺服器位址。

  （選用）您可以**Add**（新增）一個 **DNS Suffix**（**DNS** 尾碼），以指定輸入無法解析的不完整主機名稱時，用戶端應在本機使用的尾碼，例如，acme.local。請勿在網域尾碼前面輸入萬用字元 (*)（例如，acme.com）。您可以新增多個尾碼。
- 如果想要 Prisma Access 對 DNS 要求進行 Proxy，請設定用於UDP 查詢的值（以秒為單位重試查詢的 **Interval**（間隔）和重試 **Attempts**（嘗試）的執行次數）。

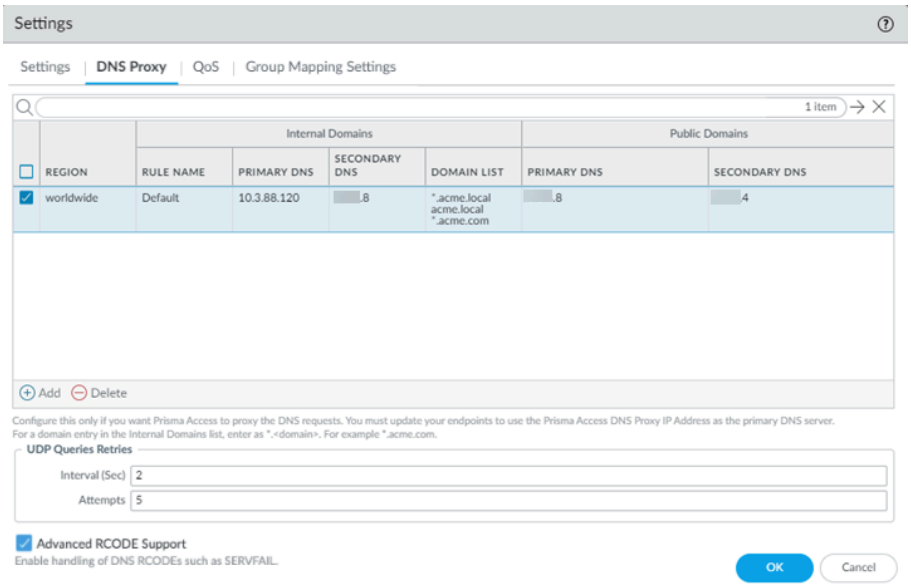
  如果想要 Prisma Access 為您的 GlobalProtect 使用者對 DNS 要求進行 Proxy，您必須更新端點以使用 **Remote Network DNS Proxy IP Address**（遠端網路 **DNS Proxy IP** 位址）作為主要 DNS 伺服器（**Panorama** > **Cloud Services**（雲端服務） > **Status**（狀


©2025 Palo Alto Networks, Inc.

態） > **Network Details**（網路詳細資訊） > **Service Infrastructure**（服務基礎結構））。

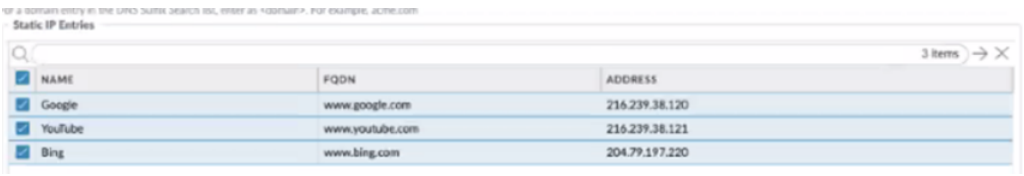
4. （選用）選取 [Advanced RCODE Support（進階 RCODE 支援）]，當收到 RCODE 2 (SERVFAIL) 和 RCODE 5 (REFUSED) DNS 傳回代碼時，允許主要 DNS 伺服器容錯移轉至次要 DNS 伺服器

   DNS 回應代碼 SERVFAIL 表示與主要 DNS 伺服器的通訊錯誤，DNS 回應代碼 REFUSED 表示主要 DNS 伺服器拒絕提供要求的資訊。在這兩種情況下，服務都會容錯移轉到次要 DNS 伺服器。




5. （選用）使用 **Static IP Entries**（靜態 **IP** 項目）將 FQDN 解析為特定 IP 位址。

   如果您的組織中有來賓網際網路服務，並且您想要來賓安全地使用搜尋引擎，防止他們搜索可能違反公司政策的不適當或冒犯性資料，則此功能可能非常有用。若要這樣做，請為靜態項目規則輸入唯一的 **Name**（名稱），並輸入 **FQDN** 和應該在其中導向 FQDN 要求的 IP **Address**（位址）。




**STEP 3 |** （選用）為您的遠端網路部署啟用 **QoS**，並指定 **QoS Profile**（**QoS** 設定檔）、**Guaranteed Bandwidth Ratio**（保證頻寬比）、**Reserved for Guaranteed Bandwidth (Mbps)**（預留保證頻寬 **(Mbps)**）的數量，並且選擇性地自訂每個位置的網站選項（**Customize Per Site**（自訂每個網站））。

您可以在計算位置層級啟用 QoS；不過，在後續步驟中新增遠端網路時，您可以指定根據每個網站啟用或停用 QoS，以及根據每個網站指定 QoS 設定檔。在設定 QoS 之前，您應該瞭解 QoS 如何針對依計算位置配置頻寬的遠端網路運作，包括指定保證頻寬和 customizing bandwidth per site（自訂每個網站的頻寬）。


©2025 Palo Alto Networks, Inc.

**STEP 4 |** （選用）設定 **Group Mapping Settings**（群組對應設定），讓 Prisma Access 使用雲端識別引擎的目金錄同步元件擷取使用者和群組資訊。

您必須設定雲端識別引擎，從 Active Directory (AD) 擷取使用者和群組資訊，然後再使用 **Group Mapping Settings**（群組對應設定），於 Prisma Access 中啟用群組對應。

**STEP 5 |** 在堆疊的其中一個範本建立新區域（**Network**（網路）**> Zones**（區域）**> Add**（新增））或將您新增到堆疊的現有範本中參考的區域對應為受信任的或不受信任的。在 Panorama 上，政策規則定義在裝置群組中，而區域定義在範本中。因此，您需要確保將參考政策規則中所包含區域的範本新增到範本堆疊。

在 Palo Alto Networks® 新世代防火牆上，安全性政策是在區域之間強制執行，這些區域對應到防火牆上的實體或虛擬介面。不過，由於 Prisma Access for Networks 只有兩個區域（信任和不信任），因此您需要將流量繫結至網際網路的任何區域（包括已認可的 SaaS 應用程式）對應為不信任，並將所有內部區域對應為信任。

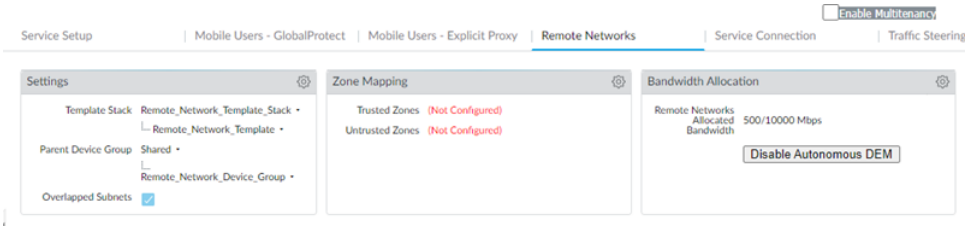
1. （選用）編輯 zone mapping（區域對應）設定。

   根據預設，Prisma Access for Networks 範本堆疊中的所有區域都會分類為不受信任的區域。如果尚未定義區域，或者如果 Remote_Network_Template_Stack 中的範本沒有區域設定，則您可以返回並在將政策推送到 Prisma Access for Networks 時新增它們。
2. 對於要指定為受信任的每個區域，請選取它並按一下 **Add**（新增），以將其移至 **Trusted Zones**（受信任區域）的清單。
3. 按一下 **OK**（確定）來儲存對應。

**STEP 6 |** 按一下 **Bandwidth Allocation**（頻寬配置）區域中的齒輪圖示，為您想要裝載的位置配置頻寬。

您可以按每個計算位置的彙總層級配置頻寬。如需詳細資料，請參閱 Prisma Access 遠端網路。

如果您已將自發 DEM 當作附加授權移除，或如果從授權中移除遠端網路的自發 *DEM*，請選取 ***Disable Autonomous DEM***（停用自發 ***DEM***）。如果您移除遠端網路的自發 *DEM*，但未停用自發 *DEM*，您將在提交時收到錯誤。




如果您現有的遠端網路部署目前依位置裝載遠端網路，則會顯示一個快顯視窗，詢問您是否要移轉到彙總頻寬模型。按一下 **Migrate**（移轉）以繼續，或按一下 **Cancel**（取消）以取消移轉。

移轉至彙總頻寬模型是永久且不可逆的。移轉前，請先檢閱移轉前檢查清單。您必須 ***Commit and Push***（提交並推送）變更才能使其生效。

**Service IP Address**（服務 **IP** 位址）（用於 IPSec 通道的 Prisma Access 端進行遠端網路連線的公用 IP 位址），在您將部署移轉到彙總頻寬模型時不會變更，且無需重新設定 IPSec 通道。


©2025 Palo Alto Networks, Inc.

**STEP 7 |** 為與您要裝載的 **Prisma Access Locations**（位置）相關聯的每個 **Compute Location**（計算位置）輸入您想要的 **Bandwidth Allocation**（頻寬配置）。

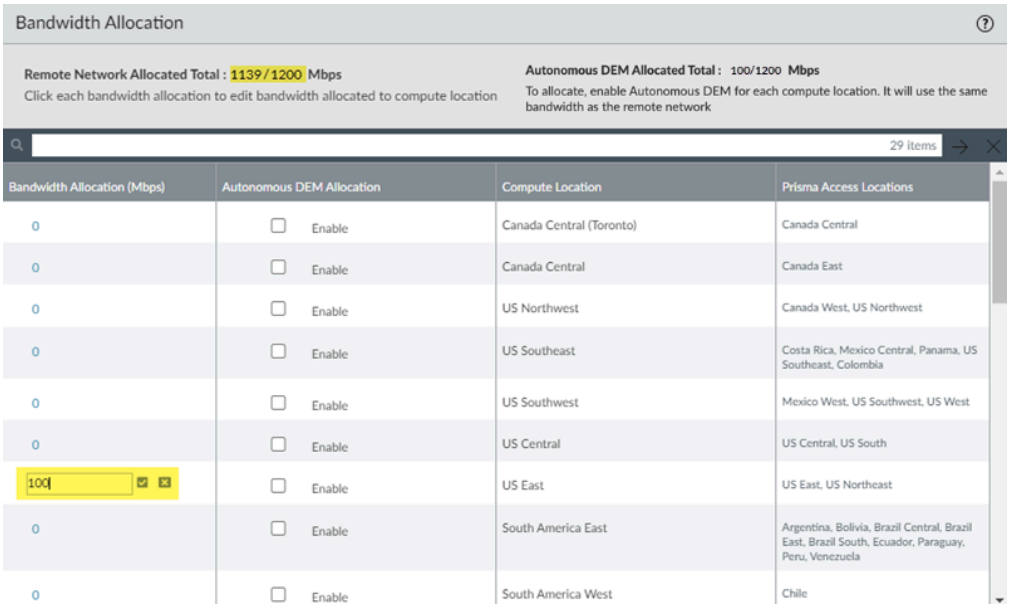
若要驗證您輸入的頻寬量，請選取頻寬量旁邊的核取記號；若要取消該數量，請選取 **x**。

指定最小頻寬為 50 Mbps，最大頻寬為最大剩餘授權頻寬。

**STEP 8 |** （選用，僅使用遠端網路授權的自發 DEM 進行部署）為已配置頻寬的計算位置 **Enable**（啟用） **Autonomous DEM Allocation**（自發 **DEM** 配置）。

如果您為計算位置啟用自發 DEM，則自發 DEM 授權所使用的頻寬量與您為計算位置指定的頻寬量相同。**Autonomous DEM Allocated Total**（自發 **DEM** 已配置總數）顯示自發 DEM 使用了多少頻寬以及剩餘多少。如需詳細資訊，請參閱自發 DEM 指南。

**STEP 9 |** 等待頻寬反映在頁面頂部的 **Allocated Total**（已配置總數）欄位中；然後按一下 **OK**（確定）。




**STEP 10 |** （選用）如果您想要設定遠端網路，以提供對遠端網路位置的安全輸入存取，請按一下 **Inbound Access Remote Networks**（輸入存取遠端網路）頁籤，並遵循工作流程為遠端網路設定安全輸入存取。

**STEP 11 |** **Add**（新增）遠端網路並指定 **Name**（名稱）。

輸入遠端網路位置的名稱之後，您無法變更該名稱。在開始裝載之前，請確保您了解遠端網路的命名計劃。

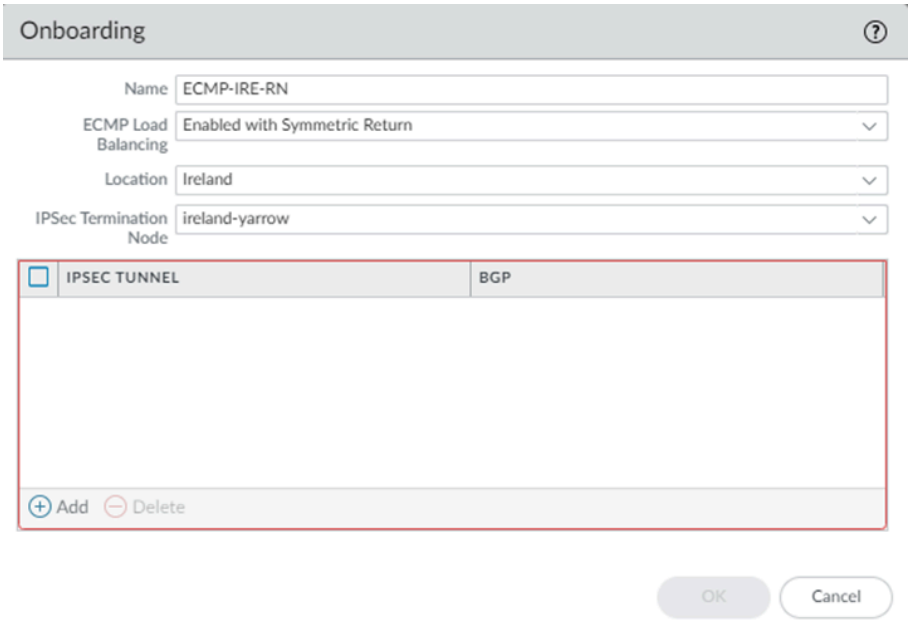

©2025 Palo Alto Networks, Inc.

**STEP 12 |** （選用，僅限 BGP 部署）建立一個設定，以便您的遠端網路連線可以為其流量使用最多四個 IPSec 通道（**ECMP Load Balancing**（**ECMP** 負載平衡））。

不支援靜態路由（需要 BGP），並且如果設定了 QoS，則您無法變更 ECMP 連結的配置比。如果您的部署使用一個 IPSec 通道進行其遠端網路連線或使用靜態路由，請為 **ECMP Load Balancing**（**ECMP** 負載平衡） 選取 **None**（無），然後繼續執行步驟 15。

1. 選取其中一個選項以啟用或停用 ECMP 負載平衡。
   - **None**（無）—不使用 ECMP 負載平衡（使用單一遠端網路通道進行此遠端網路連線）。這是您可以對靜態路由做出的唯一選擇；ECMP 負載平衡需要 BGP。
   - **Enabled with Symmetric Return**（啟用對稱傳回）—指定最多四個 IPSec 通道進行此遠端網路連線，並強制 Prisma Access 使用與其用來傳送流量相同的連結來傳回流量。

     如果您使用一個或多個通道作為僅在其中一個主要通道發生故障時才使用的備份通道，請選取此選項。如果連結失敗，Prisma Access 會使用其他通道之一對稱地發送和接收流量。




2. **Add**（新增） IPSec 通道進行遠端網路連線並指定下列值：
   - **Enable**（啟用）—為 IPSec 通道啟用 BGP。

     此選擇是無法設定的；您必須啟用 BGP 才能設定 ECMP。
   - **Summarize Mobile User Routes before advertising**（公告前彙總行動使用者路由）—減少透過 BGP 公告至客戶周邊設備 (CPE) 的行動使用者 IP 子網路公告數目，方法為彙總這些公告。

     根據預設，Prisma Access 會在 /24 子網路區塊中公告行動使用者 IP 位址集區；如果你彙總它們，Prisma Access 根據您指定的子網路公告該集區。例如，Prisma Access 使用 /20 子網路公告 10.8.0.0/20 的公用使用者行動 IP 集區，而不是先將該集區劃分為 10.8.1.0/24、10.8.2.0/24、10.8.3.0/24 等子網路，再公告它們。彙總這些公告可

 ©2025 Palo Alto Networks, Inc.

以減少 CPE 路由表中儲存的路由數目。例如，您可以使用 IP 集區彙總，搭配可接受有限數目路由的雲端 VPN 閘道（虛擬私人閘道 (VGW) 或傳輸閘道 (TGW)）。

如果您為使用 *ECMP* 的位置啟用路由彙總，則必須在該位置的所有連結上啟用路由彙總，否則您將在提交期間收到錯誤。

Prisma Access 會將所彙總行動使用者路由的社群字串設定為 `0xFFFE:0xFFF0`。

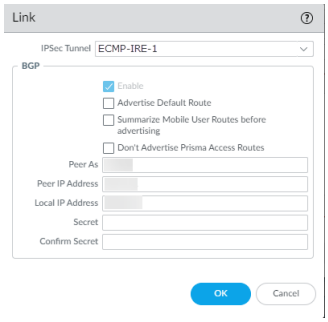
- **Advertise Default Route**（公告預設路由）—Prisma Access 使用 eBGP 為遠端網路起始預設路由公告。

  確保您的網路沒有 *BGP* 公告的其他預設路由，否則可能會在您的網路中引入路由問題。

- **Don't Advertise Prisma Access Routes**（不公告 **Prisma Access** 路由）—防止 Prisma Access BGP 對等將路由轉送至組織的網路。

  根據預設，Prisma Access 會公告所有 BGP 路由訊息，包括本機路由以及從其他服務連線、遠端網路和行動使用者子網路接收的所有首碼。選取此核取方塊可防止 Prisma Access 傳送任何 BGP 公告，但仍會使用其收到的 BGP 資訊，來了解其他 BGP 芳鄰的路由。

  自從 Prisma Access 不傳送 BGP 公告後， 如果您選取此選項，則必須在內部部署設備上設定靜態路由，以建立回到 Prisma Access 的路由。




- （選用）選取 **MRAI** 計時器值。

  BGP 路由會提供一個計時器，您可以用來在網路中定制 BGP 路由聚合，稱為最小路由公告間隔 *(MRAI)*。MRAI 會採取行動，根據每個目的地限制更新速率，而且 BGP 路由器至少會等待設定的 MRAI 時間，然後再傳送相同首碼的公告。較小的數字為您提供更快的聚合時間，但會在您的網路中建立更多的公告。較大的數字會減少可以傳送的

 ©2025 Palo Alto Networks, Inc.

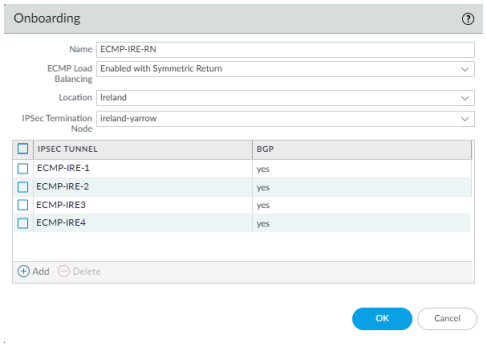
公告數目，但也會使路由聚合速度變慢。您可以決定在網路中放置的數字，以在更快的路由聚合和更少的公告之間取得最佳平衡。

設定介於 1 與 600 秒之間的 MRAI 範圍，預設值為 30 秒。

- **Peer AS**（對等 **AS**）—指定遠端網路上防火牆、虛擬路由器或 BGP 路由器所屬的自發系統 (AS)。
- **Peer IP Address**（對等 **IP** 位址）—輸入指派為 eBGP 路由器的路由器 ID 的 IP 位址，而此路由器位於您要為其設定此連線的遠端網路上。
- **Local IP Address**（本機 **IP** 位址）（選用）為 BGP 輸入一個位址，Prisma Access 會使用此位址作為其本機 IP 位址。指定要在通道 Prisma Access 端上使用的 IP 位址。

  指定 **Local Address**（本機位址）很有用，其中連線另一端的裝置（例如 Amazon Web Service (AWS) 虛擬私人閘道）需要特定的本機 IP 位址，才能使 BGP 對等成功。確保您指定的位址不會與基礎結構子網路或遠端網路中子網路中的 IP 位址衝突或重疊。
- **Secret**（密碼）和 **Confirm Secret**（確認密碼）（選用）—輸入並確認複雜密碼以驗證 BGP 對等通訊。

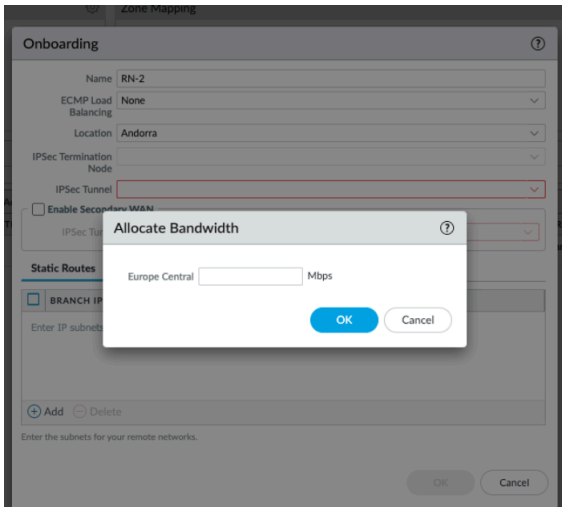
3. 重複上一步，新增最多四個通道與遠端網路連線搭配使用。




 ©2025 Palo Alto Networks, Inc.

**STEP 13 |** 選取 Prisma Access 將在其中部署保護您遠端網路位置所需基礎結構的 **Location**（位置）。此區域在地理上應靠近您的遠端網路位置。

如果您尚未為該位置對應的計算位置配置頻寬，Prisma Access 會提示您輸入該計算位置的頻寬。




以兩個星號表示的位置為 **Local Zones**（本機區域）。這些位置會將計算、儲存、資料庫和基礎結構服務放置在大型人口和產業中心附近；不過，它們也有一些限制。若要新增本機區域，請聯繫您的 Palo Alto Networks 代表。

**STEP 14 |** 選取要用於此遠端網路的 **IPSec Termination Node**（**IPsec** 終端節點）。

Prisma Access 會使用此節點將遠端網路位置與計算位置建立關聯。

**STEP 15 |** （僅限靜態路由或單一通道部署）選取或新增新的 **IPSec Tunnel**（**IPSec** 通道）設定，以存取公司位置上的防火牆、路由器或 SD-WAN 裝置：

- 在 Remote_Network_Template 中選取其中一個預先定義的 IPSec 範本，或是，如果您已將範本新增至包含 IPSec 通道設定的 Remote_Network_Template_Stack（或修改了預先定義的 Remote_Network_Template），請從下拉式清單中選取該 **IPSec Tunnel**（**IPSec** 通道）。請注意，您為每個遠端網路連線建立的通道會將 Prisma Access 連線到每個分支位置上支援 IPSec 的裝置。

  設定 IPSec 通道時請遵循下列準則：

  - IKE 閘道設定中的對等位址對於每個通道而言必須是唯一的。但是，您可以重複使用其他一些常見設定元素，例如密碼設定檔。
  - 您從範本中選取的 IPSec 通道必須僅使用自動金鑰交換和 IPv4。
  - IPSec 通道、IKE 閘道和密碼設定檔名稱不能超過 31 個字元。
  - 如果您使用動態 IKE 對等將多個遠端網路上線到相同位置，則必須對所有遠端網路設定使用相同的 IKE 密碼設定檔。


©2025 Palo Alto Networks, Inc.

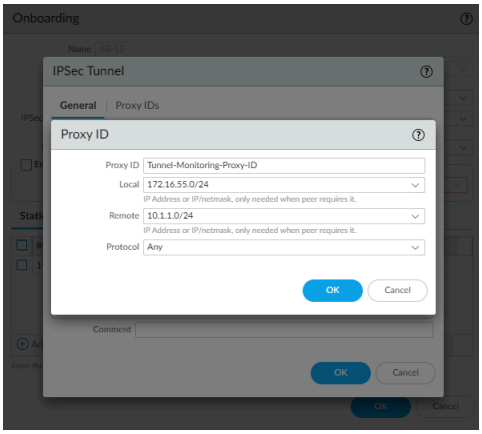
- 若要建立新的 IPSec 通道設定，請按一下 **New IPSec Tunnel**（新增 **IPSec** 通道），為其提供 **Name**（名稱）並設定 IKE 閘道、IPSec 密碼設定檔和通道監控設定。
  - 如果分支位置上支援 IPSec 的裝置使用政策型 VPN，請在 **Proxy IDs**（**Proxy ID**）頁籤上 **Add**（新增）與本機 IPSec 裝置上設定相符的 Proxy ID，以確保 Prisma Access 可以成功與您的本機裝置建立 IPSec 通道。
- 保持選取 **Enable Replay Protection**（啟用重放保護）以偵測並抵禦重放攻擊。
- 選取 **Copy ToS Header**（複製 **ToS** 標頭），將 Type of Service（服務類型 - ToS）標頭從封裝封包的內部 IP 標頭複製到外部 IP 標頭，以保留原始 ToS 資訊。


©2025 Palo Alto Networks, Inc.

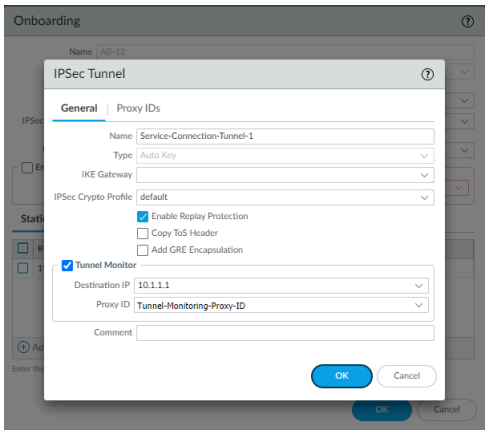
- 若要為服務連線啟用通道監控，請選取 **Tunnel Monitor**（通道監控）。
  - 請輸入 **Destination IP**（目的地 **IP**）位址。

    在您的分支位置上指定 IP 位址，讓 Prisma Access 可以向該位址傳送 ICMP ping（偵測）請求以進行 IPSec 通道監控。確保 ICMP 可從整個 Prisma Access 基礎結構子網路存取此位址。
  - 如果您對使用多個 Proxy ID 的對等裝置使用通道監控，請指定一個 **Proxy ID** 或新增 **New Proxy ID**（新的 **Proxy ID**），以允許從基礎結構子網路存取您的分支位置。

    下圖顯示 Proxy ID，其中以服務基礎結構子網路（本範例中為 172.16.55.0/24）作為 **Local**（本機）IP 子網路，以分支位置的子網路（本範例中為 10.1.1.0/24）作為 **Remote**（遠端）子網路。




    下圖顯示透過在 **Proxy ID** 欄位中指定 Proxy ID 來將您建立的 Proxy ID 套用至通道監控設定。




您必須在 *CPE* 上設定通往通道監控 *IP* 位址的靜態路由，通道監控才能發揮作用。若要針對從分支位置到 *Prisma Access* 的通道監控，尋找要使用的目的地 *IP* 位址，請選取 ***Panorama > Cloud Services***（雲端服務***) > Status***（狀態***) > Network Details***（網路詳細資料***)***、按一下 ***Service Infrastructure***（服務基礎結構***)***，然後尋找 ***Tunnel Monitor IP Address***（通道監控 ***IP*** 位址***)***。


©2025 Palo Alto Networks, Inc.

**STEP 16 |** 如果您在此位置上有次要 WAN 連結，請選取 **Enable Secondary WAN**（啟用次要 **WAN**)。

務必為每個遠端網路的次要 *WAN* 建立唯一的 *IPSec* 通道；*Prisma Access* 不支援在多個遠端網路中對次要 *WAN* 重複使用相同的 *IPSec* 通道。

以下部署不支援設定次要 WAN：

- 如果您的次要 WAN 與主要 IPSec 通道設定為主動-主動模式。
- 如果您的用戶端裝置 (CPE) 在具有主要和次要 IPSec 通道的等價多路徑 (ECMP) 設定中設定。

如果您使用靜態路由，通道容錯移轉時間會小於 15 秒（從偵測到的時間算起），具體取決於您的 WAN 供應商。

如果設定 BGP 路由並啟用通道監控，則確定安全性參數索引 (SPI) 失敗的最短預設保留時間是通道監控，當連續 15 秒偵測到通道故障時，通道監控會刪除通往對等方的所有路由。這樣一來，通道監控就可以決定 BGP 路由的行為。如果未設定通道監控，保留計時器會決定刪除路由之前通道關閉的時間。Prisma Access 會使用 RFC 4271 定義的預設 BGP HoldTime 值：90 秒，這是 Prisma Access 刪除非作用 SPI 的路由之前的最長等待時間。如果對等 BGP 裝置設定的保留時間較短，則 BGP 保留計時器會使用較小的值。

當次要通道安裝成功後，次要路由會優先採用，直到主要通道恢復正常為止。若主要和次要通道皆正常運作，則優先採用主要路由。

如果您使用不同的 *BGP* 對等來作為次要（備份）連線，*Prisma Access* 不會遵守 *CPE* 公告的多出口鑑別器 *(MED)* 屬性。如果您在遠端網路連線或服務連線上使用多個 *BGP* 對等，則此警告適用。


©2025 Palo Alto Networks, Inc.

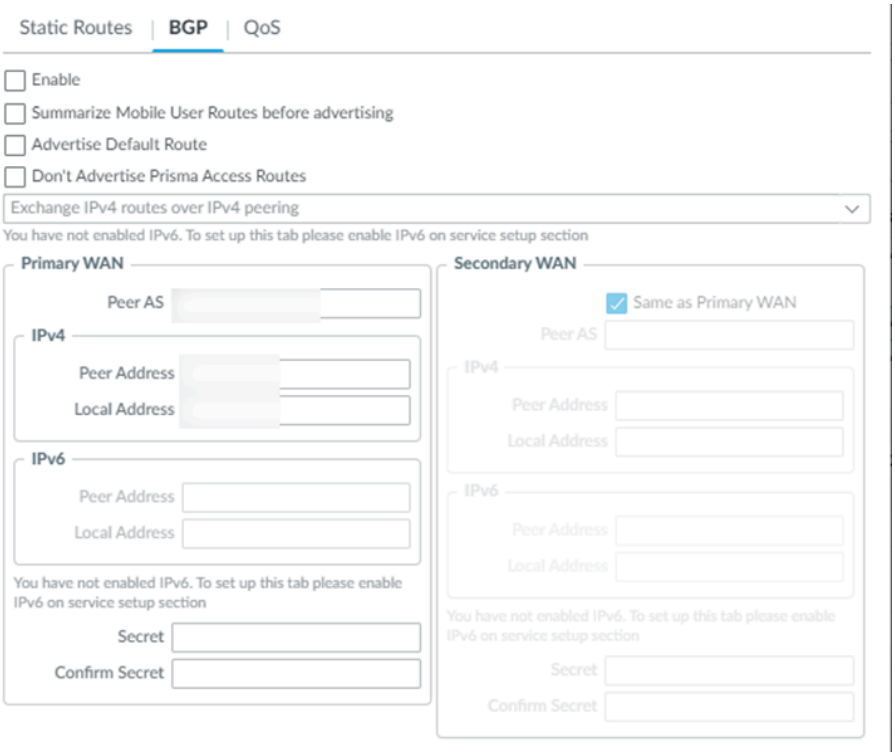
**STEP 17 |** 啟用路由到遠端網路網站上您使用者將需要存取的子網路或個別 IP 位址。

Prisma Access 會使用此資訊將要求路由到適當的網站。每個網站的網路不能彼此重疊，也不能與您為服務基礎結構或為使用者 IP 集區的 Prisma Access 指定的 IP 位址集區重疊。您可以設定 **Static Routes**（靜態路由）、**BGP** 或兩者的組合。

- 若要設定 **Static Routes**（靜態路由）：
  1. 在 **Static Routes**（靜態路由）頁籤上，按一下 **Add**（新增）並輸入遠端使用者將需要存取的資源子網路位址（例如 172.168.10.0/24）或個別 IP 位址，例如 DNS 伺服器（例如，10.32.5.1/32）。
  2. 對 Prisma Access 將需要在此位置存取的所有子網路或 IP 位址重複此動作。




- 若要設定 **BGP**：
  1. 選取 **BGP** 頁籤。
  2. （選用）選取 **ECMP Load Balancing**（**ECMP** 負載平衡）選項。請參閱步驟 12。
  3. 如果為 **ECMP Load Balancing**（**ECMP** 負載平衡）選取 **None**（無），請輸入 BGP 選項。




 ©2025 Palo Alto Networks, Inc.

4. 若要為遠端網路連線啟用 BGP，請選取 **Enable**（啟用）。

   當您啟用 BGP 時，Prisma Access 會將外部 BGP (eBGP) 的存留時間 (TTL) 值設定為 8，以容納 Prisma Access 基礎結構與終止 eBGP 連線的客戶周邊設備 (CPE) 之間可能發生的任何額外躍點。

5. 若要減少透過 BGP 公告至客戶周邊設備 (CPE) 的行動使用者 IP 子網路公告數目，方法為彙總這些公告，請選取**Summarize Mobile User Routes before advertising**（公告前彙總行動使用者路由。

   根據預設，Prisma Access 會在 /24 子網路區塊中公告行動使用者 IP 位址集區；如果你彙總它們，Prisma Access 根據您指定的子網路公告該集區。例如，Prisma Access 使用 /20 子網路公告 10.8.0.0/20 的公用使用者行動 IP 集區，而不是先將該集區劃分為 10.8.1.0/24、10.8.2.0/24、10.8.3.0/24 等子網路，再公告它們。彙總這些公告可以減少 CPE 路由表中儲存的路由數目。例如，您可以使用 IP 集區彙總，搭配可接受有限數目路由的雲端 VPN 閘道（虛擬私人閘道 (VGW) 或傳輸閘道 (TGW)）。

   Prisma Access 會將所彙總行動使用者路由的社群字串設定為 `0xFFFE:0xFFF0`。

6. 若要允許 Prisma Access 使用 eBGP 公告遠端網路的預設路由，請選取 **Advertise Default Route**（公告預設路由）。

   如果您選取 **Advertise Default Route**（公告預設路由），請確保您的網路沒有 BGP 公告的其他預設路由，否則可能會在您的網路中引入路由問題。

   > 您必須先發佈預設路由，然後才能做出此選擇以公告它們。此外，確保您的網路沒有 *BGP* 公告的其他預設路由，否則可能會在您的網路中引入路由問題。

7. 若要防止 Prisma Access 防火牆上的 BGP 對等將路由轉送到您組織的網路，請選取 **Don't Advertise Prisma Access Routes**（不公告 **Prisma Access** 路由）。

   根據預設，Prisma Access 會公告所有 BGP 路由訊息，包括本機路由以及從其他服務連線、遠端網路和行動使用者子網路接收的所有首碼。選取此核取方塊可防止 Prisma


©2025 Palo Alto Networks, Inc.

Access 傳送任何 BGP 公告，但仍會使用其收到的 BGP 資訊，來了解其他 BGP 芳鄰的路由。

自從 Prisma Access 不傳送 BGP 公告後，如果您選取此選項，則必須在內部部署設備上設定靜態路由，以建立回到 Prisma Access 的路由。

8. 輸入 **Peer AS**（對等 **AS**），這是遠端網路上防火牆、虛擬路由器或 BGP 路由器所屬的自發系統 (AS)。
9. 輸入指派為 eBGP 路由器的路由器 ID 的 IP 位址，而此路由器位於您要為其將此連線設定為 **Peer Address**（對等位址）的遠端網路上。
10. （選用）為 BGP 輸入一個位址，Prisma Access 會使用此位址作為其本機 IP 位址。

    指定 **Local Address**（本機位址）很有用，其中連線另一端的裝置（例如 Amazon Web Service (AWS) 虛擬私人閘道）需要特定的本機 IP 位址，才能使 BGP 對等成功。確保您指定的位址不會與基礎結構子網路或遠端網路中子網路中的 IP 位址衝突或重疊。

    您必須在 *CPE* 上設定 *BGP* ***Local Address***（本機位址）的靜態路由。
11. （選用）輸入並確認複雜密碼以驗證 BGP 對等通訊。
12. （選用）如果您設定了 **Secondary WAN**（次要 **WAN**），並且需要變更次要（備份）BGP 對等的 **Peer Address**（對等位址）或 **Local Address**（本機位址），請取消選取 **Same as Primary WAN**（與主要 **WAN** 相同），然後輸入唯一對等，以及選擇性地輸入次要 WAN 的本機 IP 位址。

    如果您在遠端網路部署中使用 IPv6 網路，則可以設定 **IPv6** 位址以及 **IPv4** 位址。您還需要在 Prisma Access 基礎結構中全域啟用 IPv6 網路，然後才能使用 IPv6 定址。

    在某些部署中（例如，使用 BGP 與 AWS VPN 閘道對等時），主要和次要 WAN 的 BGP 對等可能不同。在這些情況下，您可以選擇為次要 WAN 設定不同的 BGP 對等。

    對於搭配次要 *WAN* 的 *BGP* 部署，*Prisma Access* 會同時設定處於 ***UP***（啟動）狀態的主要和次要通道，但遵循網路流量的正常 *BGP* 作用中-備份行為。*Prisma Access* 會將主要通道設定為作用中，並僅透過該通道傳送和接收流量；如果主要通道故障，*Prisma Access* 會使用 *BGP* 規則偵測故障、將次要通道設定為作用中，並僅使用次要通道傳送和接收流量。

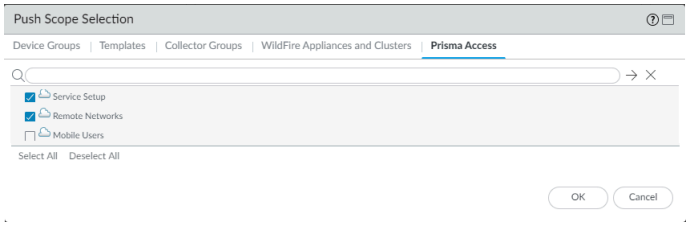
**STEP 18 |** （選用）為該位置啟用 **QoS**，並指定 **QoS Profile**（**QoS** 設定檔）。

您可以在 **Settings**（設定）中根據計算位置指定 QoS 選項和總體設定；不過，您可以在這裡啟用或停用 QoS 或根據位置變更 QoS 設定檔。


©2025 Palo Alto Networks, Inc.

**STEP 19 |** 將設定變更提交到 Panorama，並為網路將設定推送到 Prisma Access。

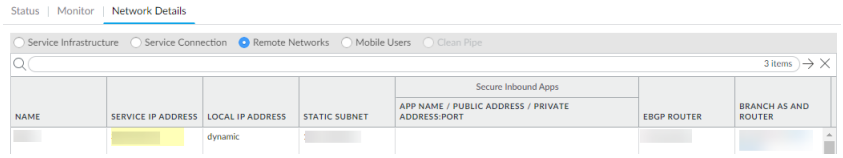
1. 按一下 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**）。
2. 按一下 **Commit**（提交） > **Commit and Push**（提交並推送）。按一下 **Edit Selections**（編輯選取項目） > **Prisma Access**，然後同時選取網路的 Prisma Access 和 Prisma Access 進行服務設定，以將設定推送到服務。




3. 按一下 **OK**（確定）與 **Commit**（提交）。

**STEP 20 |** 在遠端網路位置設定支援 IPSec 的裝置，設定與網路的 Prisma Access 的 IPSec 連線。

1. 為此遠端網路連線尋找 **Service IP Address**（服務 **IP** 位址），方法為選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊）、按一下 **Remote Networks**（遠端網路）選項按鈕，然後檢視 **Service IP Address**（服務 **IP** 位址）欄位。網路基礎結構的 Prisma Access已指派此 IP 位址進行 Prisma Access 遠端網路連線，而且您必須將此項設定為對等 IP 位址，才能在遠端網路位址與網路的 Prisma Access 之間設定 IPSec 通道。




2. 在 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Remote Networks**（遠端網路）頁面上，檢查遠端網路位置上裝置的 **Local IP address**（本機 **IP** 位址）如果您在遠端網路位置執行 NAT，則**Local IP address**（本機 **IP** 位址）會在 NAT 之後面顯示裝置的 IP 位址。

**STEP 21 |** 為了保護遠端網路位置的流量，您必須建立安全性政策規則。

1. 選取 **Policies**（原則）。
2. 選取要在其中新增政策規則的 **Device Group**（裝置群組）。您可以選取 Remote_Network_Device_Group 或您為了定義政策以保護遠端網路位置而選取的父系裝置群組。
3. 建立安全性政策規則。確保您沒有定義安全性政策規則來允許從任何區域到任何區域的流量。在安全性政策規則中，使用您在範本中定義的區域。

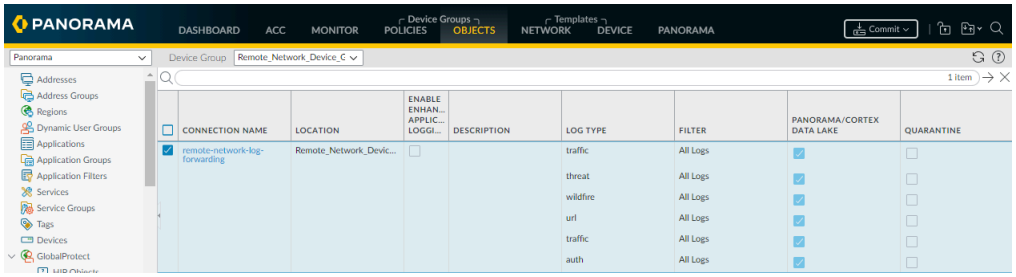
   如果您網路上的使用者存取網站遭拒，請在向 Palo Alto Networks 開立票證之前報告網站存取問題。

 ©2025 Palo Alto Networks, Inc.

**STEP 22 |** 啟用記錄到 Strata Logging Service。您必須建立一個日誌轉送設定檔，並將此設定檔附加至每個您想要為其轉送日誌的政策規則。

1. 選取 **Objects**（物件）**> Log Forwarding**（日誌轉送）。
2. 選取您已在其中新增政策規則的 **Device Group**（裝置群組），例如 Remote_Network_Device_Group。
3. **Add**（新增）日誌轉送設定檔。在日誌轉送設定檔比對清單中，**Add**（新增）您想要轉送的每一種 **Log Type**（日誌類型）。
4. 選取 **Panorama/Strata Logging Service**（**Panorama/Strata** 記錄服務）作為轉送方法，讓 Prisma Access 可將日誌轉送到 Strata Logging Service。您將能夠監控日誌並從 Panorama 產生報告。Strata Logging Service 提供無縫整合來儲存日誌，無需將其回傳到公司總部的 Panorama，並且 Panorama 可以視需要查詢 Strata Logging Service。

   以下範例啟用將流量、威脅防護、WildFire 提交、URL 篩選、資料篩選和驗證日誌轉送到 Strata Logging Service。




5. 選取 **Policies**（政策）**> Security**（安全性），然後編輯政策規則。在 **Actions**（動作）中，選取所建立的日誌轉送設定檔。

**STEP 23 |** 將您的所有變更提交到 Panorama，並將設定變更推送到 Prisma Access。

1. 按一下 **Commit**（提交）**> Commit and Push**（提交並推送）。
2. **Edit Selections**（編輯選取項目），並在 **Prisma Access** 頁籤中，確保在 **Push Scope**（推送範圍）中選取了 **Prisma Access for networks**，然後按一下 **OK**（確定）。
3. **Commit and Push**（提交並推送）您的變更。

**STEP 24 |** 檢查遠端網路狀態。

如需詳細資訊，請參閱驗證遠端網路連線狀態。


©2025 Palo Alto Networks, Inc.

# 將遠端網站連線到 Prisma Access

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 授權 |

設定 IPSec VPN 通道以將您的遠端網站連線到 Prisma Access。您必須建立從分支 IPSec 裝置到 Prisma Access 的 IPsec 通道。

您建立的第一個通道是遠端網站的主要通道。然後，您可以重複此工作流程以選擇性地設定次要通道。當兩條通道都已啟動時，主要通道的優先順序會高於次要通道。如果遠端網站的主要通道發生故障，則遠端網路會回復到次要通道，直到主要通道恢復正常。

根據您用來在遠端網站建立通道的 IPSec 裝置，Prisma Access 會提供內建的建議 IKE 和 IPSec 安全性設定。您可以使用建議設定來快速開始，或根據您的環境需求自訂設定。

- 新增主要和次要 IPSec VPN 通道
- 更多 IKE 選項
- 更多 IPSec 選項

## 新增主要和次要 IPSec VPN 通道

**STEP 1 |** 啟動 Prisma Access。

**STEP 2 |** 前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Remote Networks**（遠端網路） > **Add Remote Networks**（新增遠端網路），並 **Set Up**（設定）主要通道。如果您已經設定了主要通道，則可以繼續在此處新增次要通道。

1. 為通道指定描述性名稱。
2. 為遠端網站上您用來與 Prisma Access 建立通道的 IPSec 裝置選取 **Branch Device Type**（分支裝置類型）。
3. 針對 **Branch Device IP Address**（分支裝置 **IP** 位址），選擇使用可識別通道端點的 **Static IP**（靜態 **IP**）位址或 **Dynamic**（動態）IP 位址。

   如果將 **Branch Device IP Address**（分支裝置 **IP** 位址）設定為 **Dynamic**（動態），您還必須為遠端網站（**IKE Local Identification**（**IKE** 本機識別））或為 Prisma Access（**IKE Peer Identification**（**IKE** 對等識別））新增 IKE ID，讓 IPSec 對等能夠進行驗證。

   由於在遠端網路完全部署之前，您沒有用於 Prisma Access IKE ID（**IKE Peer Identification**（**IKE** 對等識別））的值，因此您通常需要為遠端網站（**IKE Local Identification**（**IKE** 本機識別））設定 IKE ID，而不是設定 Prisma Access IKE ID。

**STEP 3 |** 開啟通道監控。

輸入遠端網路上的通道監控 **Destination IP**（目的地 **IP**）位址，讓 Prisma Access 用來確定通道是否已啟動，此外，如果您的分支 IPSec 裝置使用政策型 VPN，請輸入相關聯的 **Proxy ID**。

您輸入的通道監控 IP 位址將自動新增到分支子網路清單中。

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** **Save**（儲存）通道設定。

若要繼續：

- 設定和自訂 IKE 和 IPSec 的進階密碼設定。請參閱更多 IKE 選項和更多 IPSec 選項。
- 為遠端網路啟用路由.

## 更多 IKE 選項

根據您選取的 IPSec 裝置類型，Prisma Access 會為遠端網站裝置與 Prisma Access 之間的 IKE 階段 1 金鑰交換過程，提供一組建議的密碼和金鑰存留時間：您可以使用建議的設置，或根據您的環境需求自訂設定。

為您的分支裝置和 Prisma Access 選取用於 IKE 交涉的 **IKE Protocol Version**（**IKE** 通訊協定版本）。

如果您選取 **IKEv1 Only Mode**（僅 **IKEv1** 模式），Prisma Access 只能使用 IKEv1 通訊協定進行交涉。如果您選取 **IKEv2 Only Mode**（僅 **IKEv2** 模式），Prisma Access 只能使用 IKEv2 通訊協定進行交涉。如果您選取 **IKEv2 Preferred Mode**（**IKEv2** 慣用模式），僅當分支 IPSec 裝置也支援 IKEv2 時，Prisma Access 才會使用 IKEv2 通訊協定。如果您的分支 IPSec 裝置不支援 IKEv2，則 Prisma Access 將回復為使用 IKEv1 通訊協定。

新增 **IKEv1 Crypto Profile**（**IKEv1** 密碼設定檔）以自訂 IKE 密碼設定，這些設定會定義 IKE 階段 1 中金鑰交換過程使用的加密和驗證演算法。

Prisma Access 會根據用於建立此通道的 **Branch Device Type**（分支裝置類型），自動使用預設 IKE 密碼設定檔。

- **Encryption**（加密）—指定 IKE SA 交涉中使用的加密演算法。

  Prisma Access 支援以下加密演算法：3des（168 位元）、aes-128-cbc（128 位元）、aes-192-cbc（192 位元）、aes-256-cbc（256 位元）和 des（56 位元）。您也可以選取 null（無加密）。
- **Authentication**（驗證）—指定 IKE SA 交涉中使用的驗證演算法。

  Prisma Access 支援以下驗證演算法：sha1（160 位元）、sha256（256 位元）、sha384（384 位元）、sha512（512 位元）和 md5（128 位元）。您也可以選取 null（無驗證）。
- **DH** 群組—指定用於在 IKE SA 交涉中為 IKE 產生對稱金鑰的 Diffie-Hellman (DH) 群組。Diffie-Hellman 演算法使用一方的私密金鑰及另一方的公開金鑰來建立共用金鑰，亦即由 VPN 通道對等雙方共用的加密金鑰。

  Prisma Access 支援以下 DH 群組：群組 1（768 位元）、群組 2（1024 位元—預設值）、群組 5（1536 位元）、群組 14（2048 位元）、群組 19（256 位元橢圓曲線群組）、群組 20（384 位元橢圓曲線群組）。若要獲得最強的安全性，請選取數字最高的群組。
- 存留時間—指定 IKE 階段 1 金鑰有效時間的單位和時間量（預設值為 8 小時）。對於 IKEv1，security association（安全性關聯 - SA）不會在金鑰存留時間到期前主動重設其金

 ©2025 Palo Alto Networks, Inc.

鑰。IKEv1 階段 1 的重設金鑰作業僅會在 SA 到期時觸發。對於 IKEv2，SA 必須在金鑰存留時間到期之前重設金鑰。如果 SA 未在到期時重設金鑰，則 SA 必須開始新的階段 1 金鑰。

- **IKEv2 Authentication Multiple**（**IKEv2** 驗證倍數）—指定與金鑰存留時間相乘的值，用於決定驗證計數（範圍為 0-50；預設值為 0）。驗證計數是安全性處理節點可以執行 IKEv2 IKE SA 金鑰重設的次數，此次數後則必須從頭開始重新驗證 IKEv2。預設值為 0，會停用重新驗證功能。

啟用 **IKE Passive Mode**（**IKE** 被動模式），讓 Prisma Access 僅回應 IKE 連線而啟動這些連線。

**IKE NAT Traversal**（**IKE NAT** 周遊）會預設為開啟。

這表示 IKE 和 UDP 通訊協定上會使用 UDP 封裝，以便通過 IPSec VPN 通道端點之間的 network address translation（網路位址轉譯 - NAT）裝置。

## 更多 IPSec 選項

根據您選取的 IPSec 裝置類型，Prisma Access 會提供一組建議的 IPSec 通訊協定和金鑰存留時間設定，在 security association (安全性關聯 - SA) 的 IKE 階段 2 中，於分支裝置與 Prisma Access 之間保護 IPSec 通道內的資料。您可以使用建議的設置，或根據您的環境需求自訂設定。

自訂 **IPSec Crypto Profile**（**IPSec** 密碼設定檔），以定義如何在自動金鑰 IKE 為 IKE 階段 2 期間內的 IKE SA 自動產生金鑰時保護通道內的資料。

Prisma Access 會根據 **Branch Device Type**（分支裝置類型）廠商自動設定預設的 IPSec 密碼設定檔。您可以使用預設設定檔或建立自訂設定檔。

- **IPSec Protocol**（**IPSec** 通訊協定）—保護通過 VPN 通道的資料。封裝安全有效承載 **(ESP)** 通訊協定會將資料加密、驗證來源，及驗證資料完整性。驗證標頭 **(AH)** 通訊協定會驗證來源並驗證資料完整性。

  如果使用 **ESP** 作為 IPSec 通訊協定，還需指定 IPSec SA 交涉中使用的 **Encryption**（加密）演算法。

  Prisma Access 支援以下加密演算法：aes-256-gcm（256 位元）、aes-256-cbc（256 位元）、aes-192-cbc（192 位元）、aes-128-gcm（128 位元）、aes-128 -cbc（128 位元）、3des（168 位元）和 des（56 位元）。您也可以選取 null（無加密）。

**Authentication**（驗證）—指定 IPSec SA 交涉中使用的驗證演算法。

Prisma Access 支援以下驗證演算法：sha1（160 位元）、sha256（256 位元）、sha384（384 位元）、sha512（512 位元）和 md5（128 位元）。如果將 IPSec 通訊協定為 ESP，您也可以選取 [none（無）]（無驗證）。

**DH Group**（**DH** 群組）—在 IPSec security association（安全性關聯 - SA）交涉中指定 IKE 的 Diffie-Hellman (DH) 群組。

Prisma Access 支援以下 DH 群組：群組 1（768 位元）、群組 2（1024 位元—預設值）、群組 5（1536 位元）、群組 14（2048 位元）、群組 19（256 位元橢圓曲線群組）、群組 20（384 位元橢圓曲線群組）。若要獲得最強的安全性，請選取數字最高的群組。如果您不想

 ©2025 Palo Alto Networks, Inc.

更新 Prisma Access 在 IKE 階段 1 建立的金鑰，請選取 **no-pfs**（無完美轉送密碼）。如果您選取此選項，Prisma Access 會重複使用目前用於 IPSec SA 交涉的金鑰。

**Lifetime**（存留時間）—指定交涉金鑰有效時間的單位和時間量（預設值為一小時）。

**Lifesize**（存留大小）—指定金鑰可用於加密的資料單位和數量。

 ©2025 Palo Alto Networks, Inc.

# 為遠端網路啟用路由

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 授權 |

為了讓 Prisma Access 將流量路由到遠端網路，您必須為要使用 Prisma Access 保護的子網路提供路由資訊。您可以採取數種方式執行此操作。您可以定義遠端網站上每個子網路的靜態路由，也可以在服務連線位置與 Prisma Access 之間設定 BGP，或使用這兩種方法的組合。

如果同時設定靜態路由並啟用 BGP，則靜態路由優先。雖然如果您的遠端網路位置只有幾個子網路，使用靜態路由可能很方便，但在其中許多遠端網路具有重疊子網路的大型部署中，BGP 將使您能夠更輕鬆地進行調整。

- 靜態路由—若要啟用往返 Prisma Access 遠端網站的靜態路由，識別遠端網站上的子網路或個別 IP 位址，您想要 Prisma Access 保護它們（適用於輸入和輸出流量）。每個網站的子網路不得彼此重疊、也不得與您為 Prisma Access for Users 指定的 IP 集區，或與基礎結構子網路重疊。
- **BGP**—如果您想要啟用 BGP，以動態地將流量路由到遠端網路，或從中路由流量，則需要為分支 eBGP 路由器提供 BGP 資訊：
  - 分支路由器自發系統 **(AS)** 編號—遠端網路中 eBGP 路由器所屬的 AS。這稱為 **Peer AS**（對等 **AS**）.
  - 路由器 **ID**—指派為遠端網路上 eBGP 路由器的路由器 ID 的 IP 位址。這稱為 **Peer Address**（對等位址）。

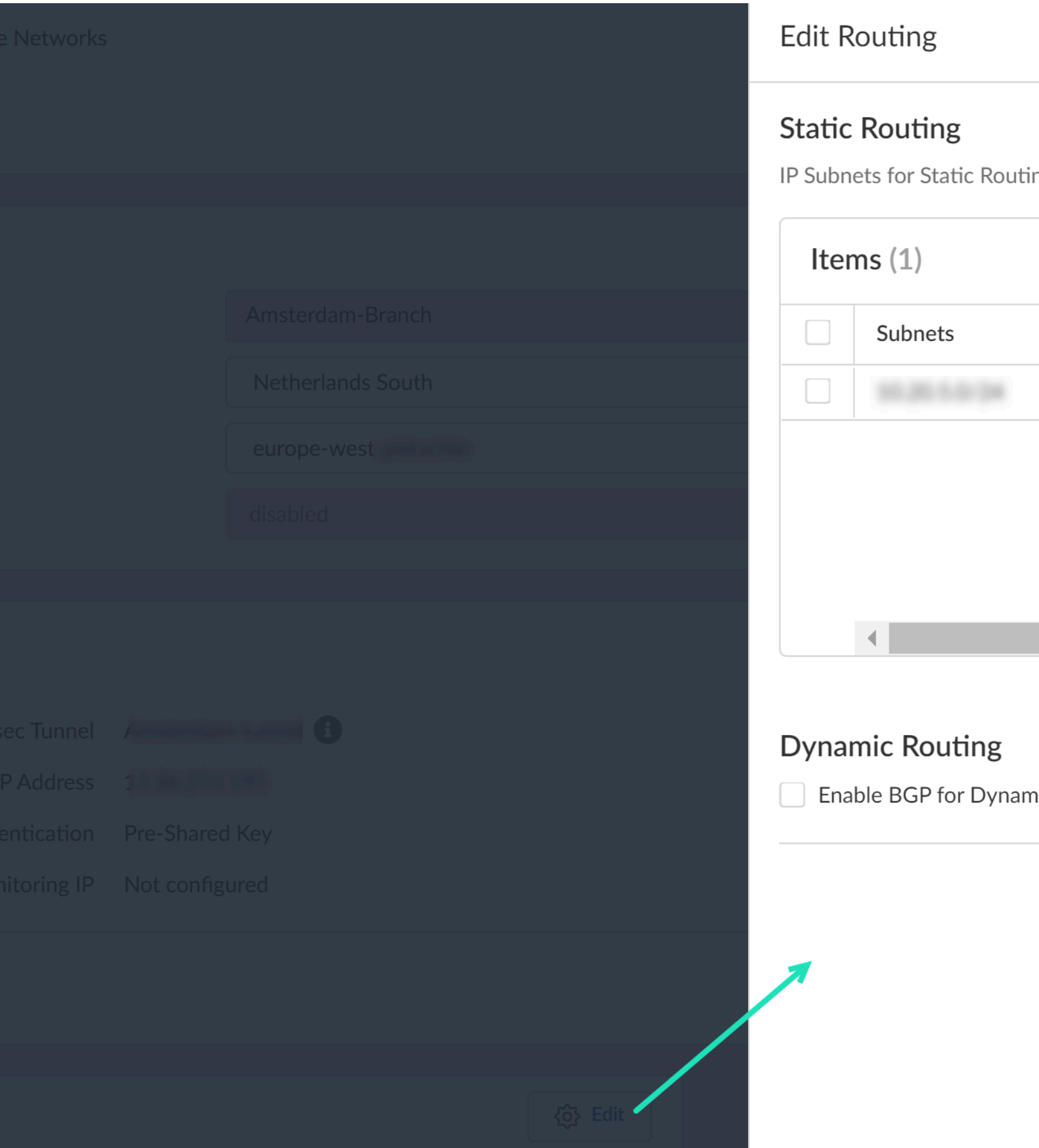
  如果同時設定靜態路由和 BGP 路由，則靜態路由優先。

以下是為遠端網站設定路由設定的方法。


©2025 Palo Alto Networks, Inc.

若要新增或調整路由設定，請前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Remote Networks**（遠端網路），以及新增或編輯遠端網站。


©2025 Palo Alto Networks, Inc.





©2025 Palo Alto Networks, Inc.

設定靜態路由。

如果您使用靜態路由，將流量路由至分支以及從中路由流量，請 **Add**（新增）要在分支上保護的 IP 子網路或 IP 位址。如果您對分支上的 IP 子網路進行任何變更，則必須手動更新靜態路由。

設定動態路由。

若要使用動態路由來公告您的分支子網路，請**Enable BGP for Dynamic Routing**（為動態路由啟用 **BGP**），然後設定以下設定：

- 不匯出路由—防止 Prisma Access 將路由轉送到您的遠端網路。

  根據預設，Prisma Access 會公告所有 BGP 路由訊息，包括本機路由以及從其他服務連線、遠端網路和行動使用者子網路接收的所有首碼。選取此核取方塊可防止 Prisma Access 傳送任何 BGP 公告，但仍會使用其收到的 BGP 資訊，來了解其他 BGP 芳鄰的路由。

  因為 *Prisma Access* 不傳送 *BGP* 公告後，所以如果您選取此選項，則必須在您的內部部署設備上設定靜態路由，以建立回到 *Prisma Access* 的路由。
- 對等 **IP** 位址—輸入指派為遠端網路上 eBGP 路由器的路由器 ID 的對等 IP 位址。
- 對等 **AS**—輸入對等 AS，這是您網路的自發系統 (AS)。

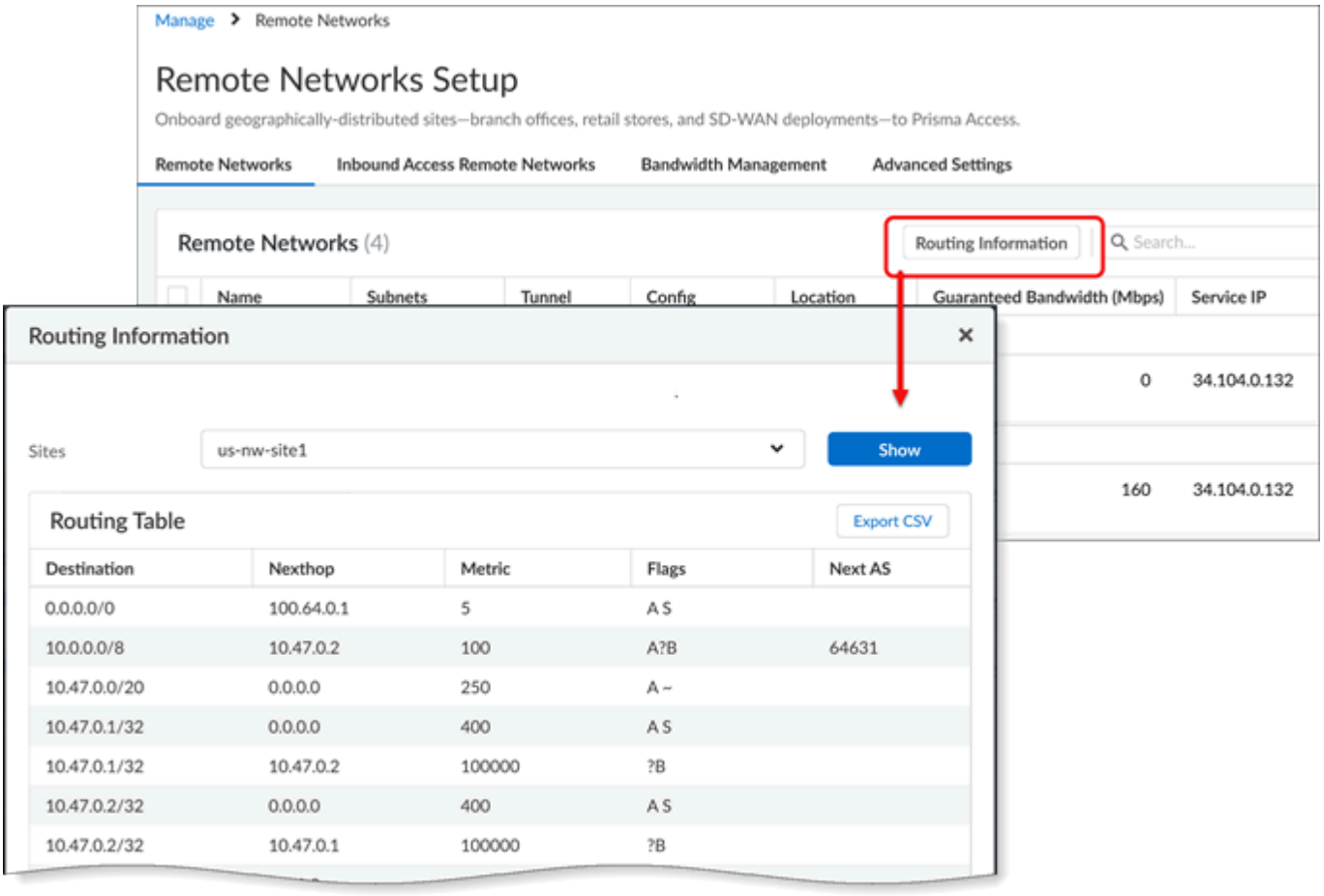
  您必須使用符合 RFC 6996 的 BGP 私人 AS 編號。
- 本機 **IP** 位址—輸入 IP 位址，Prisma Access 會將其用作 BGP 的本機 IP 位址。

  僅當遠端網站裝置需要本機位址，BGP 對等才能成功時，才需要本機位址。確保您指定的位址不與遠端網路中基礎結構子網路中的 IP 位址衝突或重疊。
- 密碼—輸入密碼以驗證 BGP 對等通訊，然後 **Confirm Secret**（確認金鑰）。

## 針對網站連線進行疑難排解

出於疑難排解目的，您現在可以檢視遠端網站或服務連線網站的路由表。在遠端網路或服務連線儀表板上尋找 **Routing Information**（路由資訊）按鈕。

 ©2025 Palo Alto Networks, Inc.




 ©2025 Palo Alto Networks, Inc.

# 裝載多個遠端網路

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

若要簡化裝載和設定遠端網路的程序，您可以選擇裝載至少一個遠端網路，然後將這些設定匯出到逗號分隔值 (CSV) 文字檔。CSV 檔案包含您為了匯出所選取網路的 IPSec 通道和 IKE 閘道設定值，然後您可以編輯這些設定，並使它們對於您可能想要裝載的每個新網路都是唯一的。您可以修改 CSV 檔案以包含 100 個新的遠端網路，然後將 CSV 檔案匯回其中，以加快裝載新遠端網路位置的程序。

CSV 檔案不包括金鑰或密碼，例如 BGP 共用密碼、IKE 預先共用金鑰、Proxy ID、IKE 密碼設定檔、IPSec 密碼設定檔。因此，IPSec 通道和 IKE 閘道設定所需的任何金鑰和密碼都是從您在啟動 CSV 檔案匯入時選取的網路繼承的。

使用此大量匯入程序時，您必須等待 Prisma Access 部署用於保護這些位置的基礎結構。

**STEP 1 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路）（在 [Onboarding（裝載）] 區段中）。

**STEP 2 |** 選取一個位置，然後 **Export**（匯出）您之前裝載的遠端網路設定。

如果您尚未新增任何位置，則需要 **Add**（新增）一個位置，然後下載其設定。您必須選取一個遠端網路，然後按一下 **Export**（匯出）。包含設定的 CSV 檔案會下載到您的電腦。

**STEP 3 |** （僅依計算位置配置頻寬的部署）確保您已為要裝載的位置配置了頻寬。

您裝載的每個位置都有一個為其配置頻寬的計算位置。

1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路），然後按一下 **Bandwidth Allocation**（頻寬配置）區域中的齒輪。
2. 在顯示的表格中檢查 **Bandwidth Allocation**（頻寬配置） 欄位。

   此區域中的表格顯示計算位置到 Prisma Access 位置對應。您必須為與您要裝載的位置相關聯的計算位置配置頻寬。例如，若要裝載日本中部位置，請確保您已在東北亞計算位置配置頻寬。
3. 如果您尚未為與您要裝載的位置相關聯的計算位置配置頻寬，請立即新增。

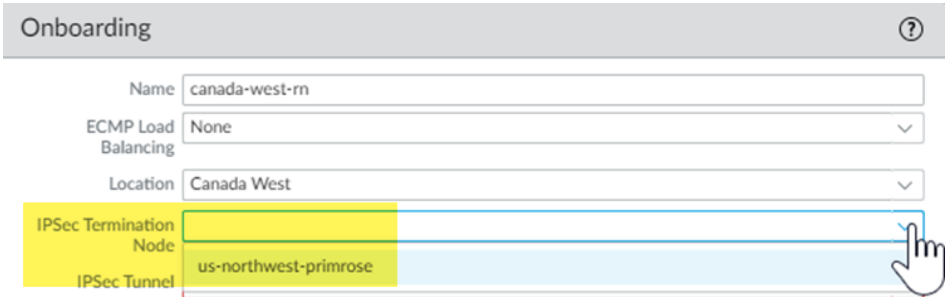

©2025 Palo Alto Networks, Inc.

**STEP 4 |** （僅依計算位置配置頻寬的部署）尋找與您要裝載的一個或多個位置相關聯的 **IPSec Termination Node**（**IPsec** 終端節點）。

您會在裝載期間將一個 *IPSec* 終端節點指派給遠端網路，並在 CSV 檔案的 **spn-name** 欄中輸入此值。每個 IPSec 終端節點可以提供高達 1000Mbps 的頻寬。

若要尋找 IPSec 終端止節點，請執行下列其中一個動作：

- 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路）、**Add**（新增）遠端網路並選取您要裝載的位置，然後記下裝載區域中的 IPsec 終端節點選項。




- 使用管理 Prisma Access 的 Panorama 開啟命令列介面 (CLI) 工作階段，並輸入 `show plugins cloud_services remote-networks agg-bandwidth region` *compute-location-name*，其中 *compute-location-name* 是與您要裝載的位置相關聯的計算位置。IPsec 終端節點會顯示在 `spn-name-list` 欄位中。

**STEP 5 |** 修改 CSV 檔案以新增遠端網路的設定。

請參閱 遠端網路表格中的欄位，以取得此檔案中欄位和可能值的說明。

您必須重新命名所匯出檔案中列出的網路。如果該檔案具有重複的名稱，則匯入將失敗。

**STEP 6 |** **Import**（匯入）CSV 檔案。

來自該檔案的設定會顯示在畫面上。您已選取要匯入該檔案的遠端網路將充當模型設定，而且該檔案中列出的遠端網路將繼承金鑰和任何缺失值，而它們在這裡不必是唯一的。

**STEP 7 |** 提交並推送您的變更。

1. **Commit**（提交） > **Commit and Push**（提交並推送）您的變更。
2. 按一下 **OK**（確定）與 **Commit**（提交）。

## 遠端網路表格中的欄位

下表提供了遠端網路表格中欄位的說明。**Required**（必要）列中標記為 **Y** 的欄位是必要欄位，而標記為 **N** 的欄位是選用欄位。

| 欄位 | 說明 | 必要？**(Y/N)** |
|---|---|---|
| name | 遠端網路的名稱。 | Y |

 ©2025 Palo Alto Networks, Inc.

| 欄位 | 說明 | 必要？(Y/N) |
|---|---|---|
| 頻寬 | （僅依位置配置頻寬的部署）遠端網路的已配置頻寬。可接受的值如下：<br>• 2 Mbps<br>• 5 Mbps<br>• 10 Mbps<br>• 20 Mbps<br>• 25 Mbps<br>• 50 Mbps<br>• 100 Mbps<br>• 150 Mbps<br>• 300 Mbps<br>• 500 Mbps<br>• 1000 Mbps<br>*1000 Mbps* 頻寬選項處於預覽模式。預覽期間的輸送量是盡最大努力提供的，實際效能將視流量混合而有所不同。 | Y |
| 地區 | 遠端網路的位置。<br>輸入與本文件中完全相同的位置（例如，**US West**（美國西部）或 **Japan South**（日本南部））。 | Y |
| 子網路 | 遠端網路 LAN 端的靜態路由子網路。使用逗號來區隔多個子網路。 | N |
| bgp_peer_as | 遠端網路對等裝置的 BGP 自發系統編號 (ASN)。 | N |
| bgp_peer_address | 遠端網路對等裝置的 BGP 對等位址。 | N |
| tunnel_name | IPSec 通道設定的名稱。需要唯一值。 | Y |
| gateway_name | IKE 閘道設定的名稱。需要唯一值。 | Y |
| peer_ip_address | Prisma Access 對等裝置的 IP 位址。 | N |
| local_id_type | Prisma Access 呈現給對等裝置的 IKE ID 類型。如果您在此檔案匯入其中的遠端網路中使用憑 | N |

 ©2025 Palo Alto Networks, Inc.

| 欄位 | 說明 | 必要？(Y/N) |
|---|---|---|
| | 證，則指定的所有匯入類型都將參考設定的憑證值。 | |
| local_id_value | Prisma Access 呈現給對等裝置的 IKE ID 值。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考設定的憑證值。 | N |
| peer_id_type | 對等呈現給 Prisma Access 的 IKE ID 值。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考對等憑證值。 | N |
| peer_id_value | Prisma Access 呈現給對等裝置的 IKE ID 值。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考對等憑證值。 | N |
| monitor_ip | 雲端將用來確定 IPSec 通道已啟動且對等網路可連線的通道監控 IP 位址。<br>您無法匯出 *proxy-ID* 值進行通道監控。 | N |
| proxy_ids | 為對等設定的 proxy ID。對於路由型 VPN，請將此欄位留空。採用下列 CSV 設定格式指定 Proxy ID：<br>[{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}] | N |
| sec_wan_enabled | 指定是否啟用次要 IPsec 通道。可接受的值為 yes（是）和 no（否）。 | N |
| sec_tunnel_name | 次要 IPSec 通道設定的名稱。如果指定次要通道，則需要唯一值。 | N |
| sec_gateway_name | 次要 IKE 閘道設定的名稱。如果指定次要通道，則需要唯一值。 | N |
| sec_peer_ip_address | 次要 IPsec 通道的 Prisma Access 次要裝置的 IP 位址。 | N |
| sec_local_id_type | Prisma Access 為次要 IPsec 通道呈現給對等裝置的 IKE ID 類型。如果您在此檔案匯入其中的遠端 | N |

 ©2025 Palo Alto Networks, Inc.

| 欄位 | 說明 | 必要？(Y/N) |
|---|---|---|
| | 網路中使用憑證，則指定的所有匯入類型都將參考設定的憑證值。 | |
| sec_local_id_value | Prisma Access 為次要 IPsec 通道呈現給對等裝置的 IKE ID 值。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考設定的憑證值。 | N |
| sec_peer_id_type | 對等為次要 IPsec 通道呈現給 Prisma Access 的 IKE ID 值。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考對等憑證值。 | N |
| sec_peer_id_value | Prisma Access 為次要 IPsec 通道呈現給對等裝置的 IKE ID 值。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考對等憑證值。 | N |
| sec_monitor_ip | 雲端將用於次要 IPSec 通道的通道監控 IP 位址，以確定 IPSec 通道是否已啟動且對等網路可連線。<br>您無法匯出 *proxy-ID* 值進行通道監控。 | N |
| sec_proxy_ids | 為次要 IPsec 通道的對等設定的 Proxy ID。對於路由型 VPN，請將此欄位留空。採用下列 CSV 設定格式指定 Proxy ID：<br>[{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}] | N |
| ecmp_link_1_tunnel_name | （僅限 ECMP 部署）ECMP 通道 1 的 IPSec 通道設定名稱。需要唯一值。 | |
| ecmp_link_1_gateway_name | （僅限 ECMP 部署）ECMP 通道 1 的 IKE 閘道設定名稱。需要唯一值。 | |
| ecmp_link_1_peer_ip_address | （僅限 ECMP 部署）ECMP 通道 1 的 Prisma Access 對等裝置的 IP 位址。 | |


©2025 Palo Alto Networks, Inc.

| 欄位 | 說明 | 必要？(Y/N) |
|---|---|---|
| ecmp_link_1_local_id_type | （僅限 ECMP 部署）Prisma Access 為 ECMP 通道 1 呈現給對等裝置的 IKE ID 類型。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考設定的憑證值。 | |
| ecmp_link_1_local_id_value | （僅限 ECMP 部署）Prisma Access 為 ECMP 通道 1 呈現給對等裝置的 IKE ID 值。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考設定的憑證值。 | |
| ecmp_link_1_peer_id_type | （僅限 ECMP 部署）對等為 ECMP 通道 1 呈現給 Prisma Access 的 IKE ID 值。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考對等憑證值。 | |
| ecmp_link_1_peer_id_value | （僅限 ECMP 部署）Prisma Access 為 ECMP 通道 1 呈現給對等裝置的 IKE ID 值。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考對等憑證值。 | |
| ecmp_link_1_monitor_ip | （僅限 ECMP 部署）雲端將用來確定 IPSec 通道已啟動，且 ECMP 通道 1 的對等網路可連線的通道監控 IP 位址。<br>您無法匯出 *proxy-ID* 值進行通道監控。 | |
| ecmp_link_1_proxy_ids | （僅限 ECMP 部署）為 ECMP 通道 1 的對等設定的 Proxy ID。對於路由型 VPN，請將此欄位留空。採用下列 CSV 設定格式指定 Proxy ID：<br>[{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}] | |
| ecmp_link_1_bgp_peer_as | （僅限 ECMP 部署）ECMP 通道 1 的遠端網路對等裝置的 BGP 自發系統編號 (ASN)。 | |
| ecmp_link_1_bgp_peer_address | （僅限 ECMP 部署）ECMP 通道 1 的遠端網路對等裝置的 BGP 對等位址。 | |


©2025 Palo Alto Networks, Inc.

| 欄位 | 說明 | 必要？(Y/N) |
|---|---|---|
| ecmp_link_2_tunnel_name | （僅限 ECMP 部署）ECMP 通道 2 的 IPSec 通道設定名稱。需要唯一值。 | |
| ecmp_link_2_gateway_name | （僅限 ECMP 部署）ECMP 通道 2 的 IKE 閘道設定名稱。需要唯一值。 | |
| ecmp_link_2_peer_ip_address | （僅限 ECMP 部署）ECMP 通道 2 的 Prisma Access 對等裝置的 IP 位址。 | |
| ecmp_link_2_local_id_type | （僅限 ECMP 部署）Prisma Access 為 ECMP 通道 2 呈現給對等裝置的 IKE ID 類型。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考設定的憑證值。 | |
| ecmp_link_2_local_id_value | （僅限 ECMP 部署）Prisma Access 為 ECMP 通道 2 呈現給對等裝置的 IKE ID 值。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考設定的憑證值。 | |
| ecmp_link_2_peer_id_type | （僅限 ECMP 部署）對等為 ECMP 通道 2 呈現給 Prisma Access 的 IKE ID 值。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考對等憑證值。 | |
| ecmp_link_2_peer_id_value | （僅限 ECMP 部署）Prisma Access 為 ECMP 通道 2 呈現給對等裝置的 IKE ID 值。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考對等憑證值。 | |
| ecmp_link_2_monitor_ip | （僅限 ECMP 部署）雲端將用來確定 IPSec 通道已啟動，且 ECMP 通道 2 的對等網路可連線的通道監控 IP 位址。<br><br>您無法匯出 *proxy-ID* 值進行通道監控。 | |
| ecmp_link_2_proxy_ids | （僅限 ECMP 部署）為 ECMP 通道 2 的對等設定的 Proxy ID。對於路由型 VPN，請將此欄位留空。採用下列 CSV 設定格式指定 Proxy ID：<br><br>[{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", | |


©2025 Palo Alto Networks, Inc.

| 欄位 | 說明 | 必要？(Y/N) |
|---|---|---|
| | `"remote":"3.4.5.6/32", "protocol":{"tcp":{"local-port":234,"remote-port":345}}}]` | |
| ecmp_link_2_bgp_peer_as | （僅限 ECMP 部署）ECMP 通道 2 的遠端網路對等裝置的 BGP 自發系統編號 (ASN)。 | |
| ecmp_link_2_bgp_peer_address | （僅限 ECMP 部署）ECMP 通道 2 的遠端網路對等裝置的 BGP 對等位址。 | |
| ecmp_link_3_tunnel_name | （僅限 ECMP 部署）ECMP 通道 3 的 IPSec 通道設定名稱。需要唯一值。 | |
| ecmp_link_3_gateway_name | （僅限 ECMP 部署）ECMP 通道 3 的 IKE 閘道設定名稱。需要唯一值。 | |
| ecmp_link_3_peer_ip_address | （僅限 ECMP 部署）ECMP 通道 3 的 Prisma Access 對等裝置的 IP 位址。 | |
| ecmp_link_3_local_id_type | （僅限 ECMP 部署）Prisma Access 為 ECMP 通道 3 呈現給對等裝置的 IKE ID 類型。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考設定的憑證值。 | |
| ecmp_link_3_local_id_value | （僅限 ECMP 部署）Prisma Access 為 ECMP 通道 3 呈現給對等裝置的 IKE ID 值。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考設定的憑證值。 | |
| ecmp_link_3_peer_id_type | （僅限 ECMP 部署）對等為 ECMP 通道 3 呈現給 Prisma Access 的 IKE ID 值。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考對等憑證值。 | |
| ecmp_link_3_peer_id_value | （僅限 ECMP 部署）Prisma Access 為 ECMP 通道 3 呈現給對等裝置的 IKE ID 值。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考對等憑證值。 | |
| ecmp_link_3_monitor_ip | （僅限 ECMP 部署）雲端將用來確定 IPSec 通道已啟動，且 ECMP 通道 3 的對等網路可連線的通道監控 IP 位址。<br>  您無法匯出 *proxy-ID* 值進行通道監控。 | |


©2025 Palo Alto Networks, Inc.

| 欄位 | 說明 | 必要？(Y/N) |
|---|---|---|
| ecmp_link_3_proxy_ids | （僅限 ECMP 部署）為 ECMP 通道 3 的對等設定的 Proxy ID。對於路由型 VPN，請將此欄位留空。採用下列 CSV 設定格式指定 Proxy ID：<br>[{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}] | |
| ecmp_link_3_bgp_peer_as | （僅限 ECMP 部署）ECMP 通道 3 的遠端網路對等裝置的 BGP 自發系統編號 (ASN)。 | |
| ecmp_link_3_bgp_peer_address | （僅限 ECMP 部署）ECMP 通道 3 的遠端網路對等裝置的 BGP 對等位址。 | |
| ecmp_link_4_tunnel_name | （僅限 ECMP 部署）ECMP 通道 4 的 IPSec 通道設定名稱。需要唯一值。 | |
| ecmp_link_4_gateway_name | （僅限 ECMP 部署）ECMP 通道 4 的 IKE 閘道設定名稱。需要唯一值。 | |
| ecmp_link_4_peer_ip_address | （僅限 ECMP 部署）ECMP 通道 4 的 Prisma Access 對等裝置的 IP 位址。 | |
| ecmp_link_4_local_id_type | （僅限 ECMP 部署）Prisma Access 為 ECMP 通道 4 呈現給對等裝置的 IKE ID 類型。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考設定的憑證值。 | |
| ecmp_link_4_local_id_value | （僅限 ECMP 部署）Prisma Access 為 ECMP 通道 4 呈現給對等裝置的 IKE ID 值。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考設定的憑證值。 | |
| ecmp_link_4_peer_id_type | （僅限 ECMP 部署）對等為 ECMP 通道 4 呈現給 Prisma Access 的 IKE ID 值。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考對等憑證值。 | |
| ecmp_link_4_peer_id_value | （僅限 ECMP 部署）Prisma Access 為 ECMP 通道 4 呈現給對等裝置的 IKE ID 值。如果您在此檔案匯入其中的遠端網路中使用憑證，則指定的所有匯入類型都將參考對等憑證值。 | |


©2025 Palo Alto Networks, Inc.

| 欄位 | 說明 | 必要？(Y/N) |
|---|---|---|
| ecmp_link_4_monitor_ip | （僅限 ECMP 部署）雲端將用來確定 IPSec 通道已啟動，且 ECMP 通道 4 的對等網路可連線的通道監控 IP 位址。<br><br>您無法匯出 *proxy-ID* 值進行通道監控。 | |
| ecmp_link_4_proxy_ids | （僅限 ECMP 部署）為 ECMP 通道 4 的對等設定的 Proxy ID。對於路由型 VPN，請將此欄位留空。採用下列 CSV 設定格式指定 Proxy ID：<br><br>[{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}] | |
| ecmp_link_4_bgp_peer_as | （僅限 ECMP 部署）ECMP 通道 4 的遠端網路對等裝置的 BGP 自發系統編號 (ASN)。 | |
| ecmp_link_4_bgp_peer_address | （僅限 ECMP 部署）ECMP 通道 4 的遠端網路對等裝置的 BGP 對等位址。 | |
| spn-name | （僅依計算位置配置頻寬的部署）IPSec 終端節點的名稱。依計算位置配置頻寬的部署需要此欄位。 | |


©2025 Palo Alto Networks, Inc.

# 驗證遠端網路是否已連線至 Prisma Access

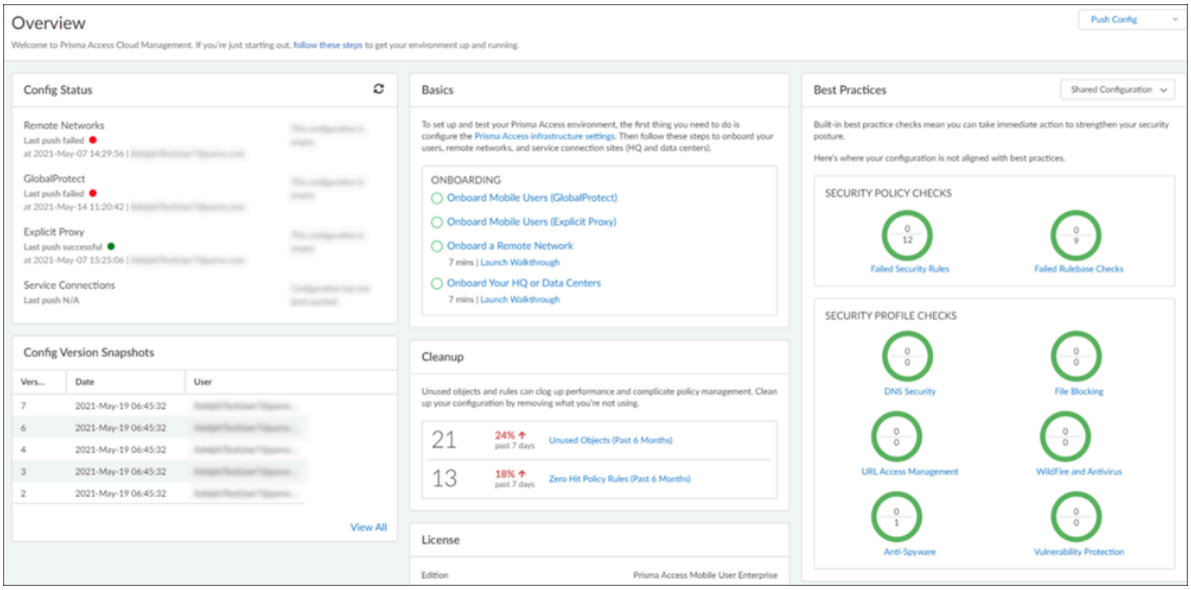
| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

在遠端網路上設定了 IPSec VPN 裝置之後，請驗證通道狀態。在驗證遠端網路的狀態時，請記住以下幾點：

- 驗證 IPsec 通道至遠端網路的狀態。
- 驗證遠端網路時的最終步驟是檢閱日誌並確保流量流經 Prisma Access。如果有錯誤或警告，請檢閱 Prisma Access 中的系統日誌和遠端網路裝置上的本機日誌。在繼續設定之前解決任何錯誤或警告。
- 視需要繼續新增遠端網路。
- Strata Cloud Manager
- Panorama

## 驗證遠端網路是否已連線至 Prisma Access (Strata Cloud Manager)

選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**）、將 **Configuration Scope**（設定範圍）變更為 **Prisma Access**，然後選取 **Prisma Access Sync Status**（同步狀態） > **Remote Networks**（遠端網路）。





©2025 Palo Alto Networks, Inc.

# 驗證遠端網路是否已連線至 Prisma Access (Panorama)

**STEP 1 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Status**（狀態），以驗證遠端網路連線是否已成功部署。

**Deployment Status**（部署狀態）區域允許您在完成裝載和部署工作之前檢視其進度，以及查看有關已完成工作狀態的詳細資訊。

**STEP 2 |** 若要顯示一個地圖，顯示您所選區域中遠端網路的位置，請選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Monitor**（監控），然後按一下 **Remote Networks**（遠端網路）頁籤。

**STEP 3 |** 選取一個區域，以取得更多有關該區域的詳細資訊。

**STEP 4 |** 按一下地圖下方的頁籤，以查看額外的遠端網路統計資料。

**Status**（狀態）頁籤：

- **Location**（位置）—遠端網路的部署位置。
- **Remote Peer**（遠端對等）—遠端網路與其具有 IPSec 通道連線的對等。
- **IPSec Termination Node**（**IPsec** 終端節點）—與遠端網路相關聯的 IPsec 終端節點。此欄位僅在您依計算位置配置頻寬時才會顯示。
- **ECMP**—您是否已在此遠端網路連線上啟用 **ECMP Load Balancing**（**ECMP** 負載平衡）。
- **Config Status**（設定狀態）—上次推送設定到服務的狀態。如果您已在本機進行了變更，但尚未將設定推送至雲端，則狀態會顯示 **Out of sync**（不同步）。將游標暫留在狀態指示器上，以取得更多的詳細資訊。在提交並推送設定到 Prisma Access 之後，設定狀態會變更為 **In sync**（同步）。
- **BGP Status**（**BGP** 狀態）—顯示遠端網路位置的防火牆或路由器與 Prisma Access 之間的 BGP 狀態的相關資訊。雖然您可能會通過各種 BGP 狀態（**idle**（閒置）、**active**（作用中）、**open send**（開啟傳送）、**open pend**（開啟擱置）、**open confirm**（開啟確認））暫時看到狀態，但 BGP 狀態最常顯示：
  - **Connect**（連線）—遠端網路位置的路由器正在嘗試與 Prisma Access 建立 BGP 對等關係。


©2025 Palo Alto Networks, Inc.

- **Established**（已建立）—已建立 BGP 對等關係。

  此欄位還將顯示 BGP 連線是否處於錯誤狀態：

- **Warning**（警告）—超過 8 分鐘未更新 BGP 狀態。這可能表示防火牆中斷。
- **Error**（錯誤）—BGP 狀態未知。

- **Tunnel Status**（通道狀態）—Prisma Access 與遠端網路之間連線的操作狀態。

**Statistics**（統計資料）頁籤：

- **Location**（位置）—遠端網路的部署位置。
- **Remote Peer**（遠端對等）—此遠端網路設定 IPsec 通道的公司位置。
- **Ingress Bandwidth (Mbps)**（進入頻寬 **(Mbps)**）—從遠端網路位置到 Prisma Access 的頻寬。

  對於進入頻寬、進入峰值頻寬、輸出頻寬和輸出峰值頻寬欄位，當遠端網路的頻寬消耗超過所配置頻寬的 *80%* 時，數字會以紅色顯示。

- **Ingress Peak Bandwidth (Mbps)**（進入峰值頻寬 **(Mbps)**）—從遠端網路位置進入雲端服務的峰值負載。
- **Egress Bandwidth (Mbps)**（輸出頻寬 **(Mbps)**）—從 Prisma Access 進入遠端網路位置的頻寬。
- **Egress Peak Bandwidth (Mbps)**（輸出峰值頻寬 **(Mbps)**）—從 Prisma Access 進入遠端網路位置的峰值負載。

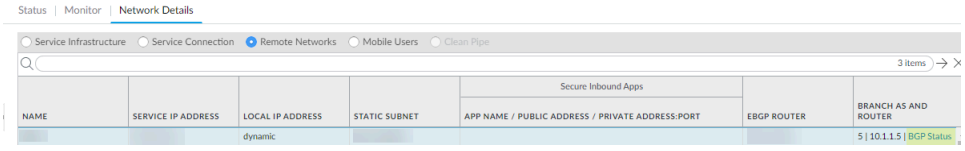
若要尋找有關區域中位置的統計資料，請選取 **Bandwidth Usage**（頻寬使用量）。

選取一個位置的核取標記以查看詳細的頻寬使用量。對於依計算位置配置頻寬的部署，選取一個 IPsec 終端節點，以檢視該節點的統計資料。Prisma Access 會使用第 95 個百分位數標準來收集統計資料，從而追蹤峰值使用率的頻寬，並忽略前 5% 的使用率峰值和大暴增。

## 驗證遠端連線 BGP 狀態

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

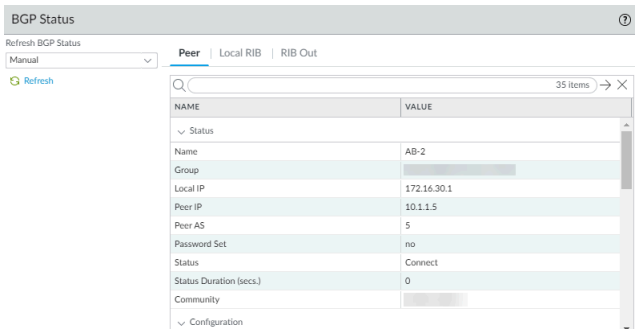
如果您設定了 BGP，則可以選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Remote Networks**（遠端網路） > **BGP Status**（**BGP** 狀態）來檢查其狀態。



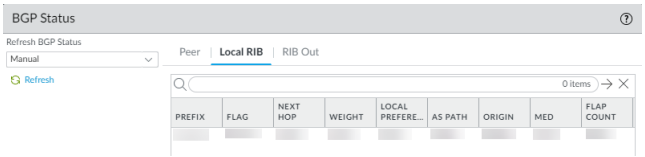

[BGP Status（BGP 狀態）] 對話方塊隨即顯示。此表格為您提供下列資訊：

 ©2025 Palo Alto Networks, Inc.

- 對等—BGP 對等的路由資訊，包括狀態、路由總數、設定，以及執行階段統計資料和計數器。路由總數會顯示在 **bgpAfiIpv4-unicast Counters**（**bgpAfiIpv4-unicast** 計數器）區域的 **Incoming Total**（傳入總數）和 **Outgoing Total**（傳出總數）欄位中。




- 本機 **RIB**—從不同對等收到且儲存在路由資訊庫 (RIB) 的路由資訊。




- **RIB** 輸出—Prisma Access 透過 BGP 更新訊息公告至其對等的路由資訊。如需此表格的範例，以及如需 BGP 如何利用您為行動使用者建立的 IP 位址集區的相關資訊，請參閱 BGP 如何為服務連線和遠端網路連線公告行動使用者 IP 位址集區。


©2025 Palo Alto Networks, Inc.

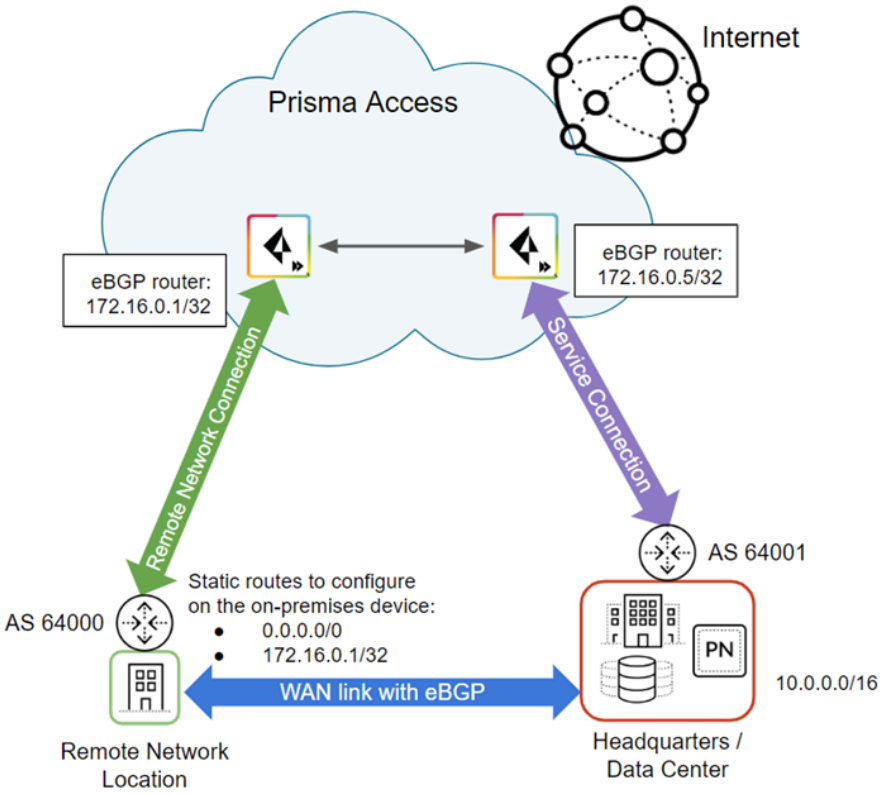
# 設定與 WAN 連結連線的遠端網路和服務連線

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

如果您有一個部署，其中遠端網路位置和具有服務連線的總部或資料中心透過 WAN 連路直接連線，則為了確保最佳路由（搭配 eBGP），您必須：

- 將靜態路由新增至 eBGP 路由器位址。除了將所有流量傳送到 Prisma Access 的預設路由外，您還必須在遠端網路中支援 IPSec 的裝置或路由器上本機新增靜態路由。
- 篩選從總部支援 IPSec 的裝置或路由器公告至 eBGP 對等（位於其他直接連線的位置）的路由。最佳做法是將總部的 BGP 路由器設定為僅公告您想要跨 WAN 連路允許的路由；確保總部的 eBGP 路由器不會將其從 Prisma Access 得知的路由公告至受 Prisma Access 保護的其他遠端網路位置。在此範例中，總部的 eBGP 路由器僅公告分公司員工需要連線到總部伺服器（子網路）的路由。

下圖顯示了一個零售企業，其有兩條路徑通往總部位置的伺服器。一條路徑是 WAN 連結，為存取總部伺服器的員工提供直接連線，而另一條路徑保護該位置其他使用者產生的流量。例如，客戶透過 Wifi 存取零售商網站或使用分公司自助服務機檢查庫存所產生的流量。此流量透過通道傳送到遠端網路，再傳送至總部。

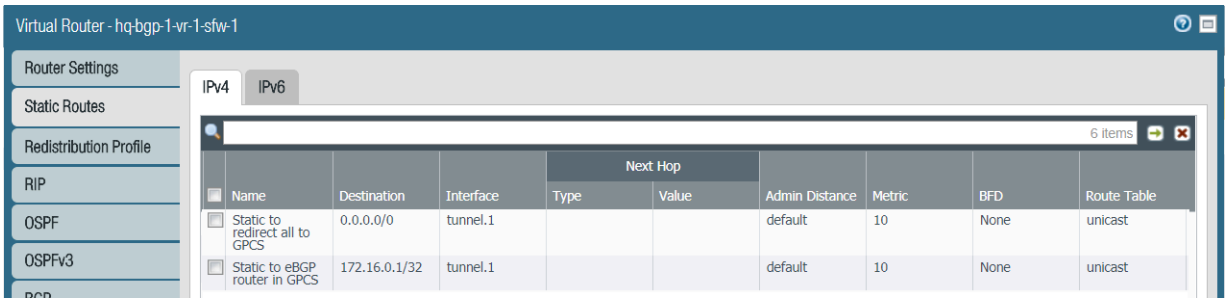



若要進行此設定，請建立遠端網路連線，並建立服務連接以裝載遠端網路和總部位置。下面的詳細資訊顯示了如何在每個位置進行路由器設定以確保最佳路由：


©2025 Palo Alto Networks, Inc.

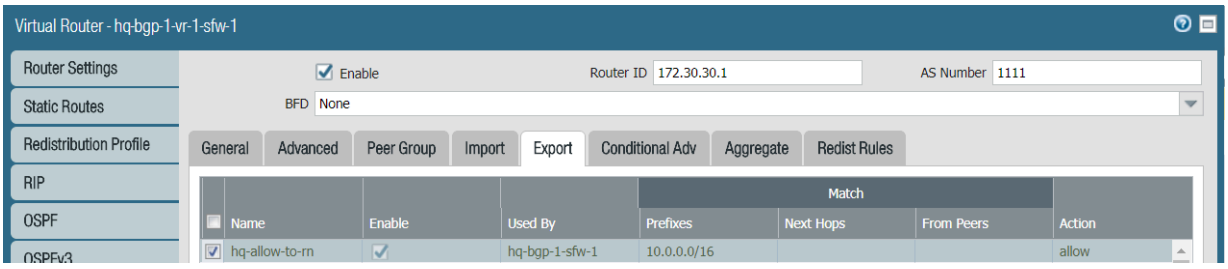
**STEP 1 |** 在遠端網路位置的路由器或支援 IPSec 的內部部署裝置上新增靜態路由。

如果您在 WAN 連結邊緣有 Palo Alto Networks 防火牆，請在 **Network**（網路） > **Virtual Routers**（虛擬路由器） > **Static Routes**（靜態路由）上，**Add**（新增）靜態路由：




**STEP 2 |** 設定要您想要透過 WAN 連結公告至另一個直接連線位置的路由。

在此範例中，您需要在總部位置進行此設定。如果您在 WAN 連結邊緣有內部部署 Palo Alto Networks 防火牆，則可以設定路由重新散佈，並在 **Network**（網路） > **Virtual Routers**（虛擬路由器） > **BGP** 上設定要匯出的 BGP 路由。




 ©2025 Palo Alto Networks, Inc.

# 遠端網路的 QoS

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ Minimum Required Prisma Access Version：3.0 Preferred |

新的 Prisma Access 部署依計算位置裝載遠端網路的頻寬。若要使用 QoS 搭配遠端網路，您可以啟用或停用 QoS，並指定計算位置層級的保證頻寬。不過，您仍然可以透過自訂每個網站的頻寬，來量身打造 QoS 和每個位置層級的保證頻寬。

Prisma Access 會使用 *IPSec* 終端節點劃分計算位置頻寬。每個 IPsec 終端節點可為您提供最高 1,000 Mbps 的頻寬。如果您將 1,000 Mbps 以上的頻寬配置給計算位置，則 Prisma Access 會為您提供額外的 IPsec 終端節點。

- Strata Cloud Manager
- Panorama

## 遠端網路的 QoS (Strata Cloud Manager)

使用 QoS 來優先處理您遠端網路中的關鍵流量，並為計算位置中的遠端網路網站設定最大和保證頻寬。

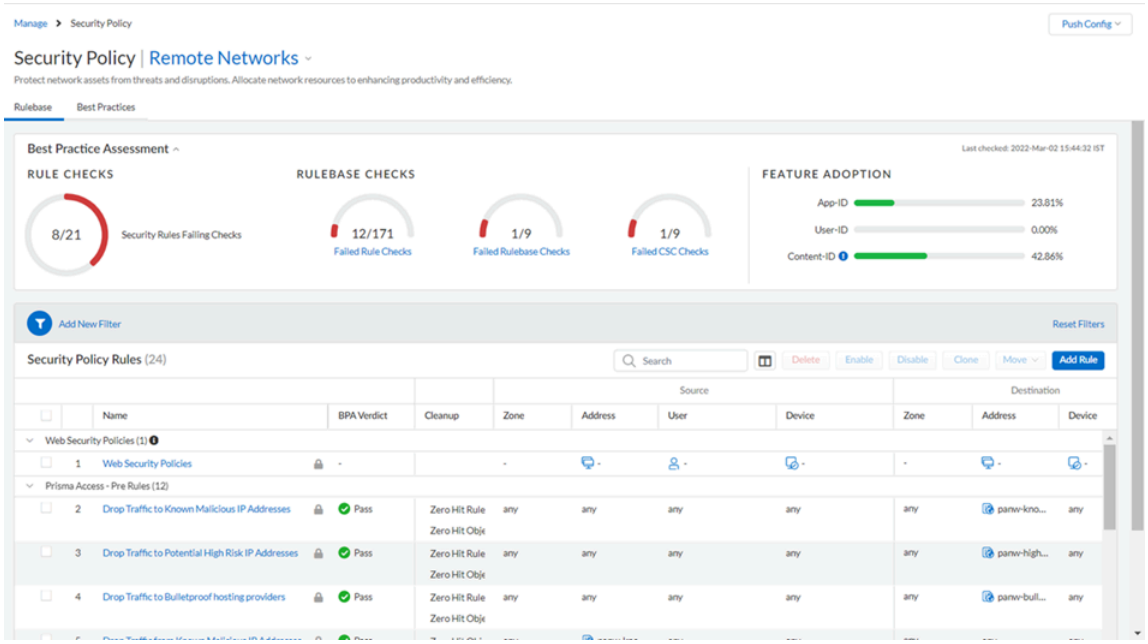

©2025 Palo Alto Networks, Inc.

**STEP 1 |** 標記您想要接收 QoS 處理方式的流量。

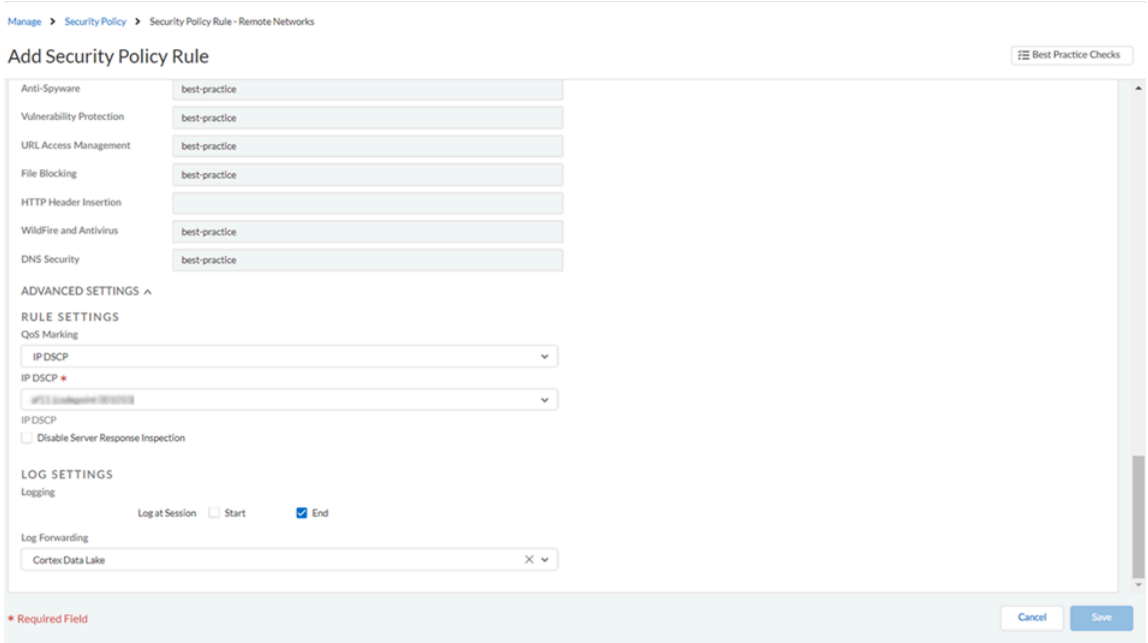
1. 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW 和 Prisma Access**） > **Security Services**（安全性服務） > **Security Policy**（安全性政策）。

   確保您正在建立遠端網路的政策。

2. **Add Rule**（新增規則）。




3. 在 **Advanced Settings**（進階設定）中指派 DSCP 值來標記傳入流量，並儲存政策。

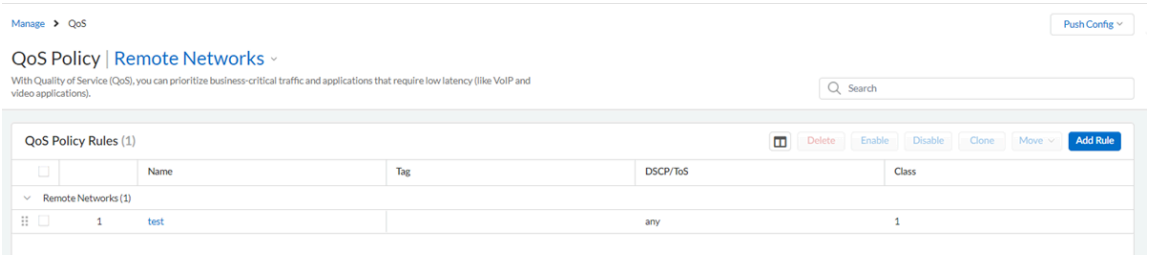



 ©2025 Palo Alto Networks, Inc.

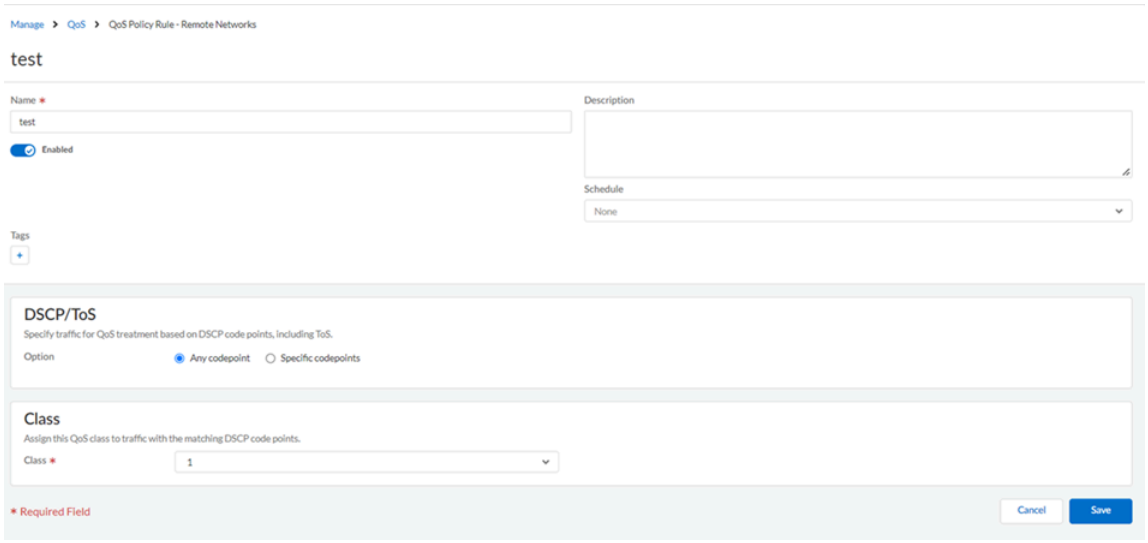
**STEP 2 |** 新增一個或多個 QoS 政策規則。

您使用 QoS 政策，將 DSCP 標記繫結至八個可用類別之一。您將在後續步驟中定義 QoS 類別所接收的處理方式。QoS 類別為符合 QoS 政策規則的流量確定優先順序和頻寬。

1. 選取 **Monitor**（監控） > **Network Services**（網路服務） > **QoS**。
2. **Add Rule**（新增規則）。




3. 輸入值並儲存政策。



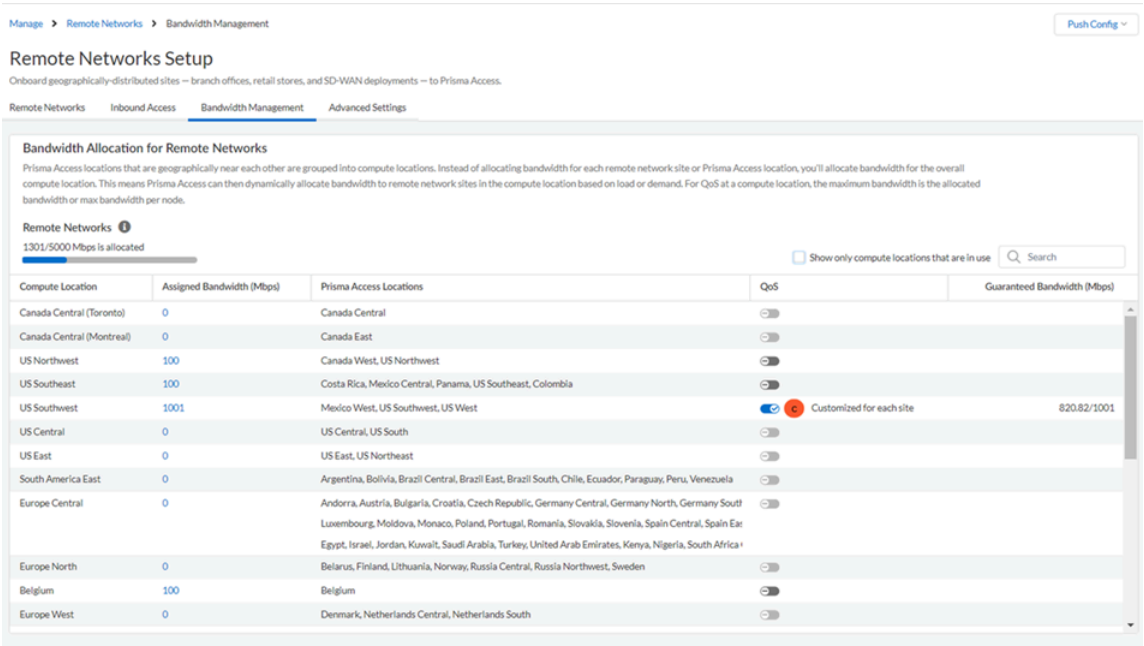

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 為您的遠端網路位置啟用 QoS。

1. 選取 **Manage**（管理） > **Service Setup**（服務設定） > **Remote Networks**（遠端網路） > **Bandwidth Management**（頻寬管理）。
2. 確定您想要部署 QoS 的 Prisma Access 位置；然後尋找與每個 Prisma Access 位置相對應的計算位置。

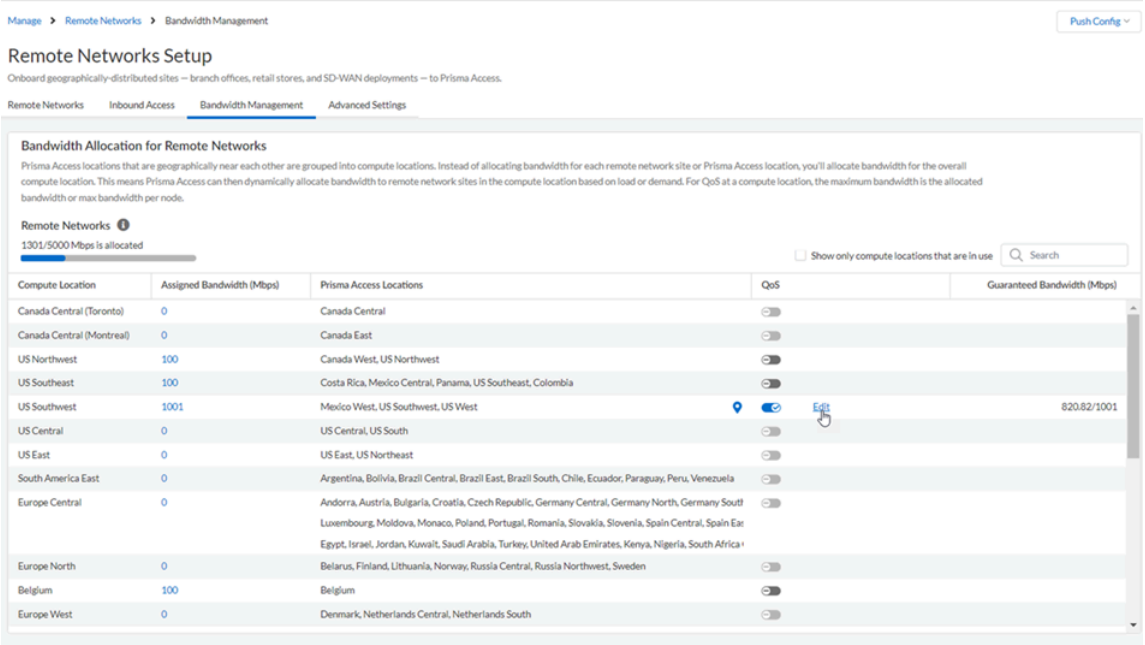
   每個 Prisma Access 位置都從其計算位置配置頻寬，而且對於您想要配置 QoS 的位置，您必須知道其計算位置的名稱。
3. 在 **QoS** 欄中，於計算位置層次啟用 QoS。

   無論您輸入什麼設定，都適用於與此計算位置相對應的所有位置。




 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** **Edit**（編輯）計算位置的 QoS 設定。




1. 選取保證頻寬比，這是一個基於計算位置整個配置頻寬的比率。

   例如，如果您為美國西南部計算位置配置 1001 Mbps 的頻寬，並且輸入 82% 的 **Guaranteed Bandwidth Ratio**（保證頻寬比），則該計算位置的保證頻寬為 820.82 Mbps。

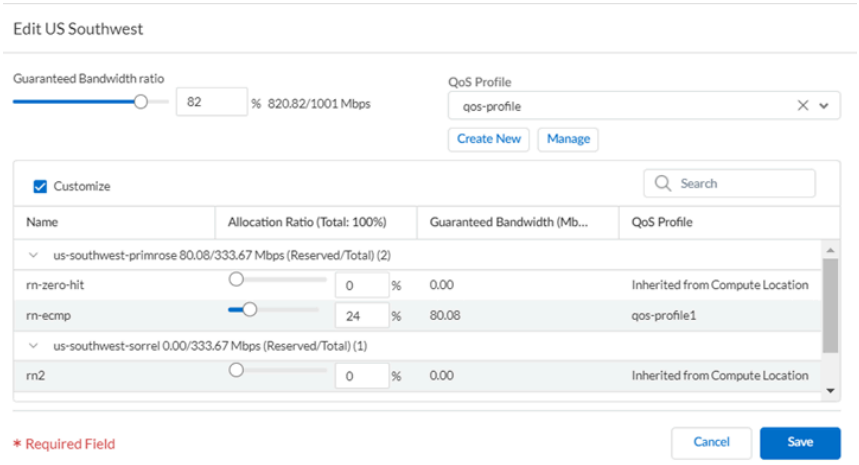
   根據預設，會給與每個遠端網路等於連線數目的百分比。例如，假設一個計算位置中有 4 個連線，總保證頻寬為 820.82 Mbps，則每個位置會收到該頻寬的 25%，即 205.2 Mbps。

   如果啟用了採用 AIOps 技術的 ADEM 授權，則該授權會針對所有計算位置自動啟用。

2. **Create New**（建立新的）QoS 設定檔，或 **Manage**（管理）現有的 QoS 設定檔。

   您使用 QoS 設定檔來塑造輸出點的流量。

3. （選用）自訂計算位置中遠端網路網站的 QoS 設定。如果每個計算位置有多個遠端網路，並且您想要變更每個遠端網路的頻寬比或 QoS 設定檔，請選取 **Customize**（自訂）並變更頻寬配置比、或兩者。




 ©2025 Palo Alto Networks, Inc.

如果您選取 ***Customize***（自訂），然後在同一 *IPSec* 終止節點上裝載其他遠端網路，則新裝載的網站會得到 *0* 的配置比，您必須手動重新平衡現有網站與新裝載網站之間的配置比。

**STEP 5 |** **Save**（儲存）變更。

**STEP 6 |** **Push**（推送）設定。

## 遠端網路的 QoS (Panorama)

完成下列工作，以在 Prisma Access 中設定 Quality of Service (服務品質 - QoS)。

**STEP 1 |** 為遠端網路和行動使用者新增一或多個安全性政策規則，以標記 QoS 的進入流量。

您可以使用這些政策，來比對流量並為其指派選取的 DSCP 值。

1. 選擇 **Policies**（政策） > **Security**（安全性） > **Pre Rules**（預先規則）。

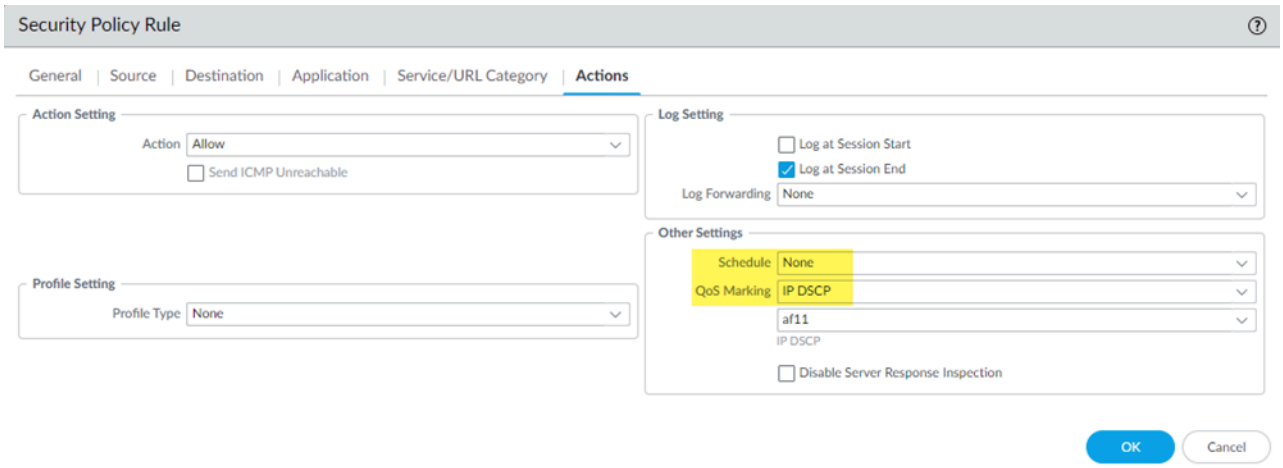
   或者，選取 **Policies**（政策） > **Security**（安全性） > **Post Rules**（後續規則），以在規則順序的底部新增一個規則，該規則會在預先規則之後進行評估。

   確保您選取正確的 ***Device Group***（裝置群組）。若要為遠端網路建立安全性規則，請選取遠端網路的裝置群組（例如，***Remote_Network_Device_Group***）；對於行動使用者，選取行動使用者的裝置群組（例如，***Mobile_User_Device_Group***）。

2. **Add**（新增）安全性政策規則。
3. 輸入規則的 **Name**（名稱）。
4. 為封包中的來源或目的地欄位定義比對規則。

   如需詳細資訊，請參閱建立安全性政策規則。
5. 按一下 **Actions**（動作），然後選取 **QoS Marking**（QoS 標記）為 **IP DSCP** 或 **IP Precedence**（IP 優先順序）。
6. 以二進位形式輸入 QoS 值，或從下拉式清單中選取值。

   以下螢幕擷取畫面顯示了一個安全性政策規則，比對以 **af11** 的 **IP DSCP** 值標記的流量。




 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 新增一個或多個 QoS 政策規則。

您使用 QoS 政策，將 DSCP 標記繫結至八個可用類別之一。稍後當您建立一個或多個 QoS 設定檔時，您會使用這些類別。

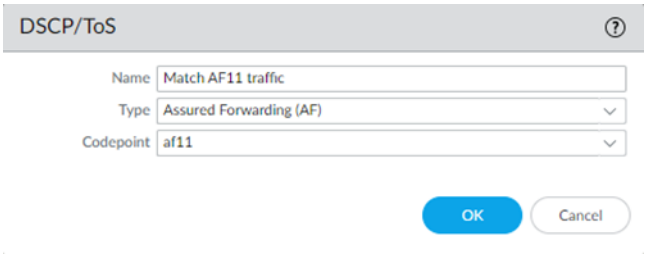
1. 選取 **Policies**（政策） > **QoS** > **Pre Rules**（預先規則）。

   或者，使用後續規則（**Policies**（政策） > **QoS** > **Post Rules**（後續規則）），在規則順序的底部新增一個規則，該規則會在預先規則之後進行評估。

   服務連線不支援 QoS 後續規則；僅使用預先規則搭配服務連線。

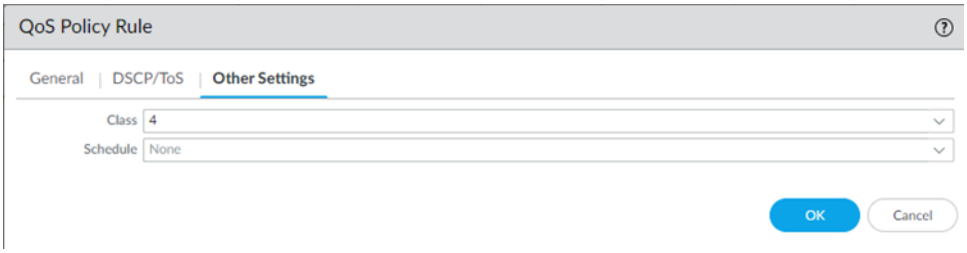
   確保為服務連線（例如，**Service_Conn_Device_Group**）或遠端網路連線（例如，**Remote_Network_Device_Group**）選取正確的 **Device Group**（裝置群組）。如果共用裝置群組中規則所定義的值不是 **General**（一般）、**DSCP/ToS** 和 **Other**（其他）設定區域中的值，則 Prisma Access 不會對遠端網路和服務連線套用該規則。
2. **Add**（新增）QoS 政策規則。
3. 按一下 **General**（一般）並輸入政策規則的名稱。
4. 按一下 **DSCP/ToS** 頁籤，然後按一下 **Codepoints**（代碼點），並 **Add**（新增）一個或多個新的代碼點。

   對於 Clean Pipe 部署，您可以在政策中指定其他 QoS 設置，例如來源、目的地或應用程式。
5. 指定 DSCP/ToS 規則的 **Name**（名稱），然後選取 **Type**（類型）和 **Codepoint**（代碼點）。




   或者，保留預設值（**Any**（任何），以允許政策比對流量，無論為流量定義的 Differentiated Services Code Point（區別服務代碼點 - DSCP）值或 IP 優先順序/Type of Service（服務類型 - ToS）為何。
6. 按一下 **Other Settings**（其他設定）頁籤，然後選擇要指派給規則的 QoS **Class**（類別）。

   您會在 QoS 設定檔中定義類別特性。
7. 按一下 **OK**（確定）。




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 建立一個或多個 QoS 設定檔，以製作輸出上的 QoS 流量，進行服務連線和遠端網路連線。

您可以使用設定檔，透過定義 QoS 類別並將頻寬指派給它們，來製作輸出點的流量。為 Prisma Access 啟用 QoS 時，您必須選取現有的 QoS 設定檔或建立新的 QoS 設定檔。

1. 為您要建立的設定檔選取正確的範本（**Remote_Network_Template** 或 **Service_Conn_Template**）；然後選取 **Network**（網路） > **Network Profiles**（網路設定檔） > **QoS Profile**（**QoS** 設定檔），並
2. **Add**（新增）設定檔。
3. 輸入設定檔 **Name**（名稱）。
4. 為 QoS 設定檔規則設定整體頻寬限制：
   - 輸入 **Egress Max**（輸出上限），表示離開服務連線或遠端網路連線的流量的最大輸送量（以 Mbps 為單位）。
     - 對於服務連線，指定最多 1 Gbps (1,000 Mbps) 的數量。

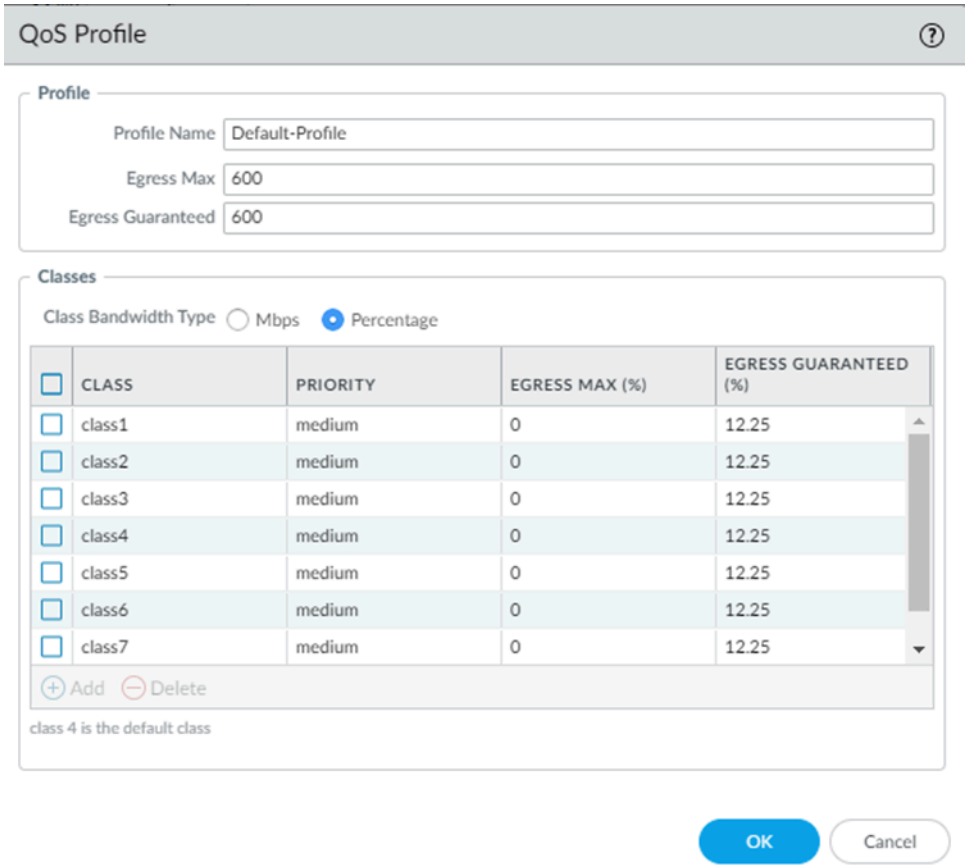
       請勿輸入大於 *1 Gbps* 的數量；*Prisma Access* 會計算每個服務連線 *IPSec* 通道的服務連線頻寬，而不是跨多個通道進行累積。
   - 對於遠端網路連線，請輸入值 **0**。
   - 輸入 **Egress Guaranteed**（輸出保證） 值。頻寬是此設定檔的保證頻寬（以 Mbps 為單位）。
     - 對於服務連線，輸入 **Egress Guaranteed**（輸出保證）頻寬，其是此設定檔的保證頻寬（以 Mbps 為單位）。

       任何超過 Egress Guaranteed（輸出保證）值的流量為盡力超過，但不保證一定超過。保證但未使用的頻寬繼續對所有流量保持可用。
     - 對於遠端網路連線，請輸入值 **0**。
5. 在 [Classes（類別）] 區段中，**Add**（新增）一個或多個類別，並指定如何標記最多八個單獨的 QoS 類別。
   - 對於依計算位置配置頻寬的遠端網路使用的 QoS 設定檔，將 **Class Bandwidth Type**（類別頻寬類型） 變更為 **Percentage**（百分比），並輸入 **Egress Max**（輸出上限）與您在此區域中輸入的 **Egress Guaranteed**（輸出保證）值的百分比。
   - 對於服務連線或依位置配置頻寬的遠端網路所使用的 QoS 設定檔，請指定 **Mbps** 類型。
   - 為類別選取 **Priority**（優先順序）（**real-time**（即時）、**high**（高）、**medium**（中）或 **low**（低））。
   - 為指派給您建立的每個 QoS 類別的流量輸入 **Egress Max**（輸出上限）。
     - 對於依計算位置配置頻寬的遠端網路，請輸入 **0**。
     - 對於頻寬型的 QoS 設定檔（由服務連線或依位置指派頻寬的遠端網路使用），請輸入以 Mbps 為單位的值。QoS 類別的輸出上限必須小於或等於 QoS 設定檔的輸出上限。
   - 為每個 QoS 類別輸入 **Egress Guaranteed**（輸出保證）百分比或頻寬（以 Mbps 為單位）。對於遠端網路的 QoS 設定檔，輸入百分比。

 ©2025 Palo Alto Networks, Inc.

指派給某一等級的保證頻寬未保留用於該等級 — 未使用的頻寬可繼續用於其他流量。當某個類別的流量超過輸出保證頻寬時，Prisma Access 盡最大努力傳遞該流量。

- 為設定檔輸入 **Class Bandwidth Type**（類別頻寬類型）。




6. 按一下 **OK**（確定）。

**STEP 4 |** （僅限服務連線）為服務連線啟用 QoS 並將 QoS 設定檔套用至該連線。

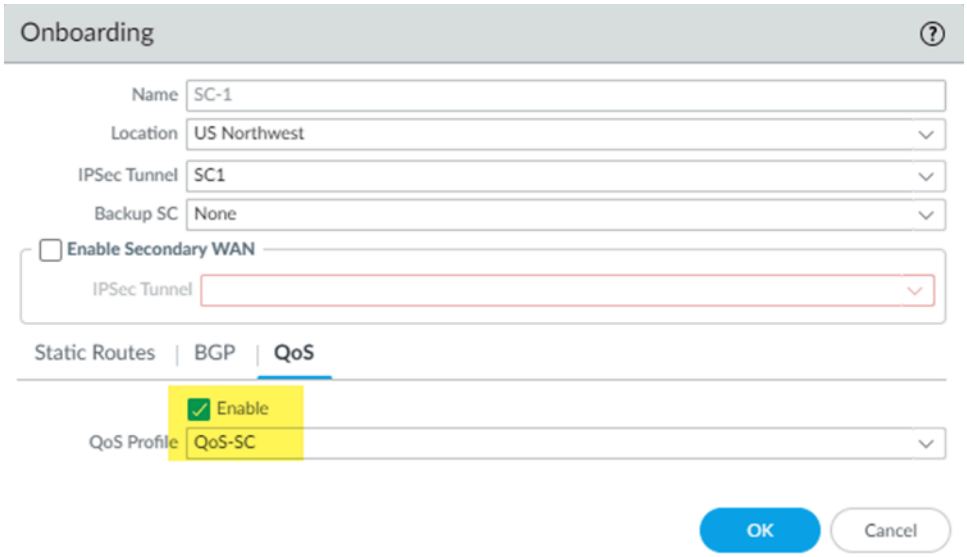
1. 透過選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定）、選取 **Connection Name**（連線名稱）、按一下 **QoS** 頁來啟用 QoS；然後 **Enable**（啟用）QoS。

   如果您透過 Prisma Access 遠端網路 而不是計算位置配置遠端網路頻寬，請以您對服務連線所做的方式設定 QoS。選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路）、為遠端網路連線 **Name**（名

 ©2025 Palo Alto Networks, Inc.

稱）選取超文字、按一下 **QoS** 頁籤，然後 **Enable**（啟用）QoS。如果您依計算位置配置頻寬（預設方法），請繼續執行步驟 5，為遠端網路設定 QoS。

2. 選取 QoS 設定檔並按一下 **OK**（確定）。




**STEP 5 |** （僅限依計算位置配置頻寬的遠端網路部署）為遠端網路位置啟用 QoS。

1. 確定您想要部署 QoS 的 Prisma Access 位置；然後尋找與每個位置對應的計算位置。

   每個位置都從其計算位置配置頻寬，並且您必須知道要配置 QoS 的位置的計算位置名稱。如需計算位置至位置對應的清單，請參閱 Prisma Access 個位置，或選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路） > **Aggregate Bandwidth**（彙總頻寬），並按一下齒輪圖示；對應會顯示在 **Compute Location**（計算位置）和 **Prisma Access Location**（**Prisma Access** 位置）欄中。

2. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路） > **Settings**（設定）、按一下齒輪以編輯設定，然後選取 **QoS**。

3. 在計算位置層級 **Enable QoS**（啟用 **QoS**）。

   您輸入的任何設定都適用於與此計算位置對應的所有位置。

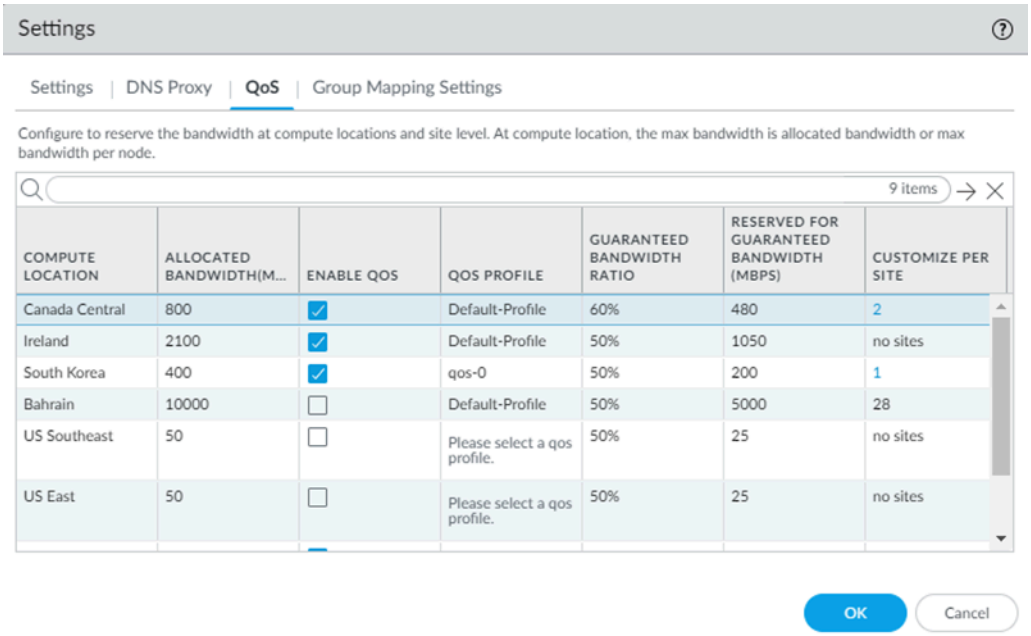

©2025 Palo Alto Networks, Inc.

4. 輸入 **QoS Profile**（**QoS** 設定檔）、**Guaranteed Bandwidth Ratio**（保證頻寬比）和 **Reserved for Guaranteed Bandwidth (Mbps)**（保留給保證頻寬 **(Mbps)**）。
   - 輸入要與此計算位置搭配使用的 **QoS Profile**（**QoS** 設定檔）。

     如果您想要每個遠端網路使用不同的 QoS 設定檔，請使用 **Customize Per Site**（自訂每個網站），如後續步驟所述。
   - 輸入保證頻寬比，這是基於計算位置整個配置頻寬的比率。

     例如，如果您為加拿大中部計算位置配置了 800 Mbps 的頻寬，且輸入 **Guaranteed Bandwidth Ratio**（保證頻寬比）為 **60%**，則該計算位置的保證頻寬為 480 Mbps。
   - 為您選取的 QoS 設定檔和計算位置輸入 **Reserved for Guaranteed Bandwidth (Mbps)**（保留給保證頻寬 **(Mbps)**）的頻寬量。

   以下螢幕擷取畫面顯示了為加拿大中部、愛爾蘭和韓國計算位置啟用的 QoS。




5. （選用）如果每個計算位置有多個遠端網路連線，並且想要變更每個位置的頻寬比或 QoS 設定檔，請裝載您的遠端網路位置；然後，選取 **Customize Per Site**（自訂每個網站），並變更頻寬配置比、QoS 設定檔或兩者。
   - 若要自訂保證頻寬，請按一下 **Customize Per Site**（自訂每個網站）區域中的數字、選取 **Customize Per Site**（自訂每個網站），然後變更 **Allocation Ratio**（配置比）。

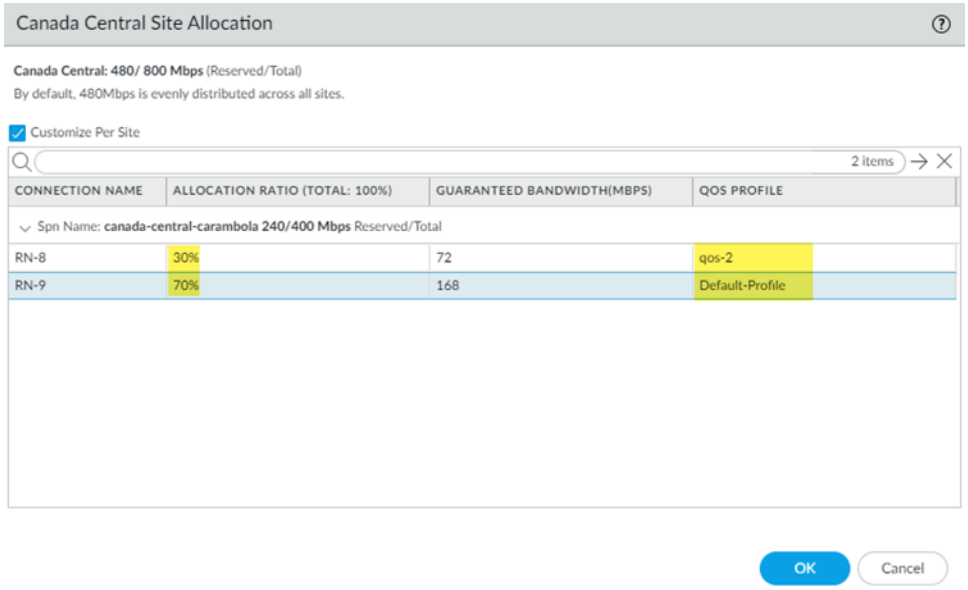
     根據預設，會給與每個遠端連線等於連線數目的百分比。例如，假設一個計算位置中有 4 個連線，總保證頻寬為 100 Mbps，則每個位置會收到該頻寬的 25% 或 25 Mbps。


©2025 Palo Alto Networks, Inc.

如果您選取 ***Customize Per Site***（自訂每個網站），然後在同一 *IPSec* 終止節點上裝載其他遠端網路，則新裝載的網站會得到 ***0*** 的配置比，您必須手動重新平衡現有網站與新裝載網站之間的配置比。

如果您不 ***Customize Per Site***（自訂每個網站），則當您新增遠端網路時，頻寬百分比會自動重新平衡。例如，如果您未選取 ***Customize Per Site***（自訂每個網站），並且已裝載四個遠端網路，則其中每個遠端網路的配置比為 *25%*。如果新增第五個遠端網路，所有五個網站都會重新平衡並得到 *20%* 的保證頻寬。

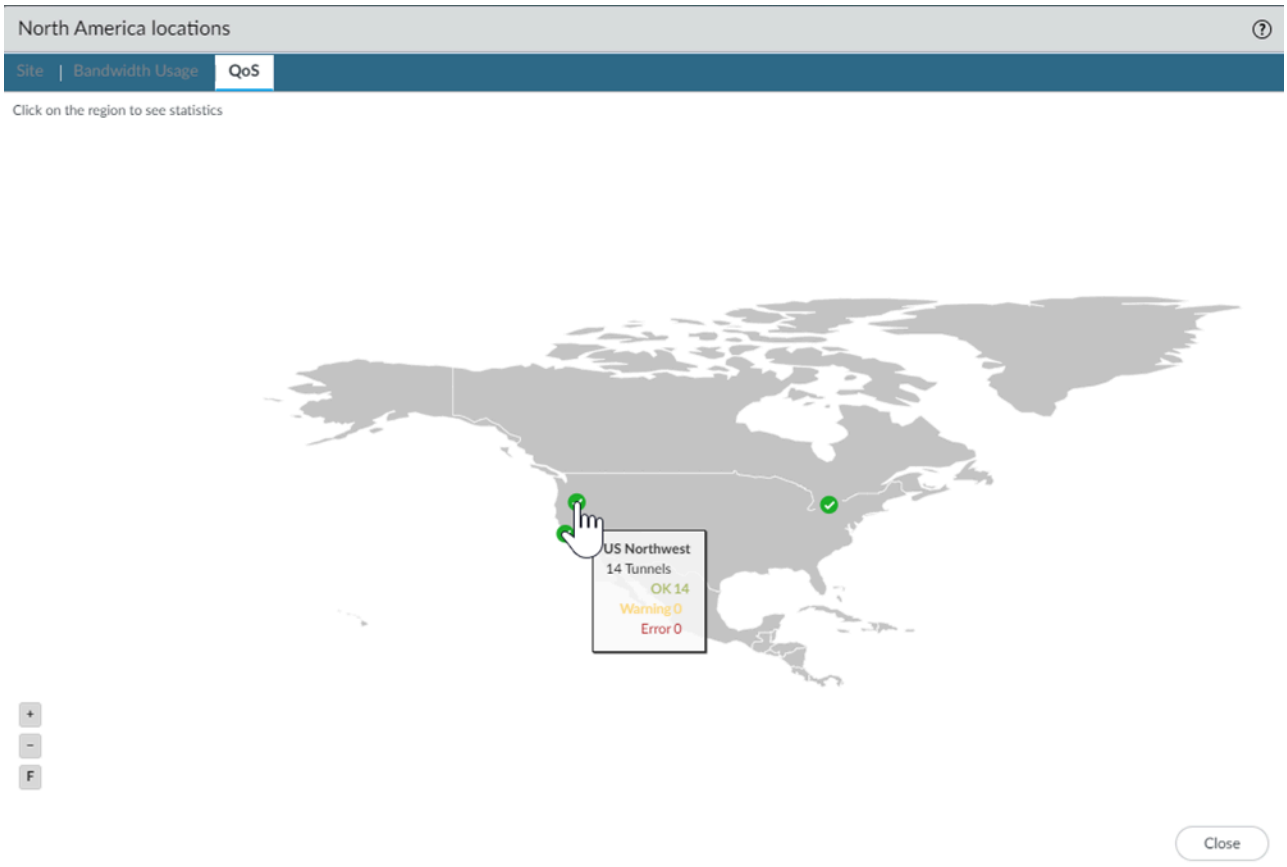
- 如果您想要在每個遠端網路層級指定 QoS 設定檔，請為遠端網路選取不同的 **QoS Profile**（**QoS** 設定檔）。




 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** 檢查 QoS 狀態。

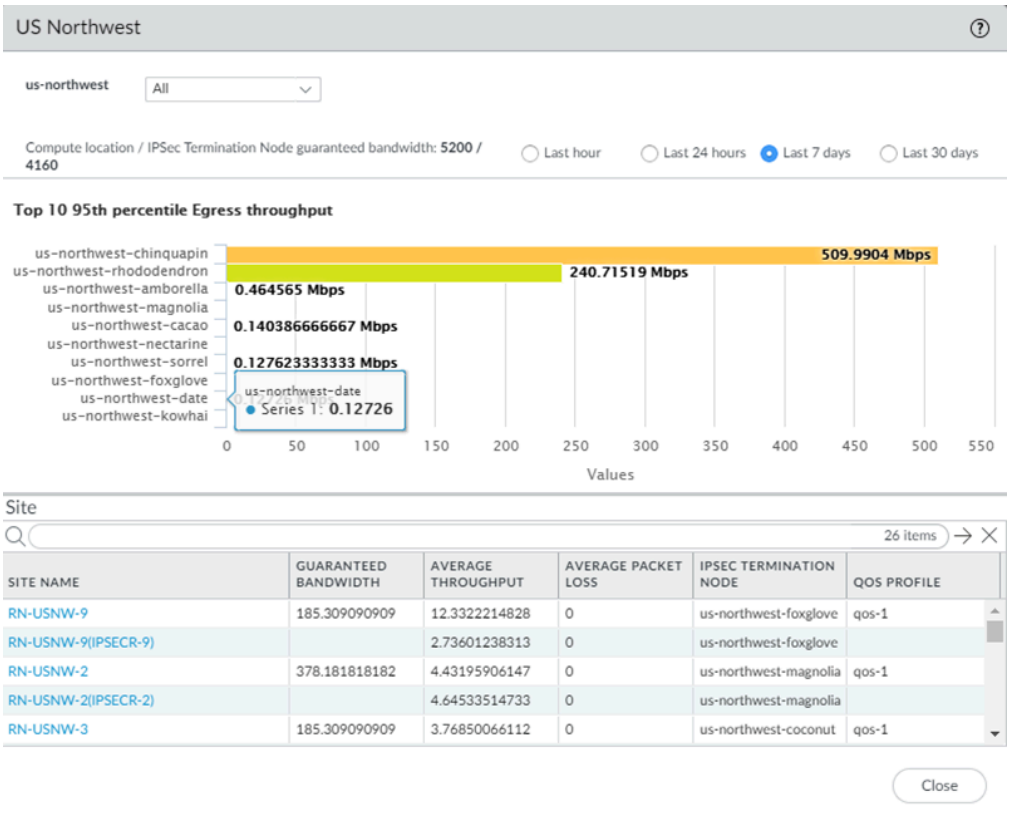
- 對於遠端網路，選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Monitor**（監控） > **Remote Networks**（遠端網路）、從對應中選擇一個區域、選取 **QoS**，然後選取一個位置。




遠端網路統計資訊隨即為具有最高輸送量的 10 個 IPSec 終止節點顯示。Prisma Access 使用第 95 個百分位數標準來收集統計資料，該統計資料追蹤峰值使用率時的頻寬，並忽略前 5% 的使用率峰值和大暴增。

選取時間範圍（**Last hour**（過去 **1** 小時）、**Last 24 hours**（過去 **24** 小時）、**Last 7 days**（過去 **7** 天）或 **Last 30 days**（過去 **30** 天）），以檢視該時段的統計資料。


©2025 Palo Alto Networks, Inc.

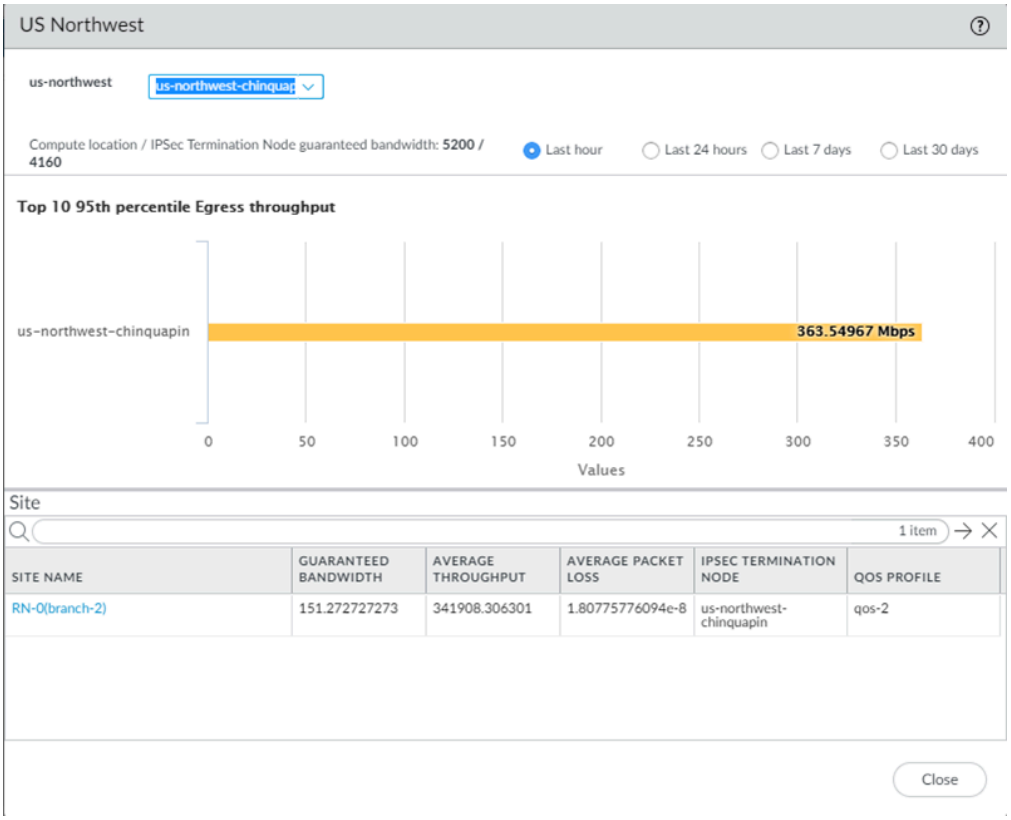



具有最高輸出頻寬使用量的遠端網路顯示在 **Site**（網站）區域中，以及遠端網路位置的 **Guaranteed Bandwidth**（保證頻寬）、**Average Throughput**（平均輸送量）、**Average**

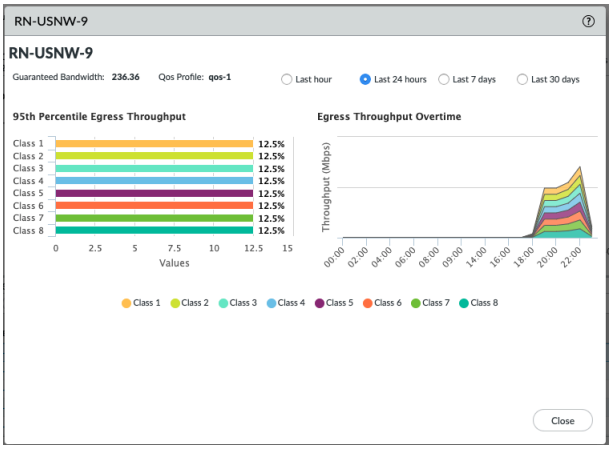
 ©2025 Palo Alto Networks, Inc.

**Packet Loss**（平均封包遺失），以及遠端網路使用的 **IPSec Termination Node**（**IPSec** 終止節點）和 **QoS Profile**（**QoS** 設定檔）的統計資料。您也可以 **Search**（搜尋）位置。

若要檢視與特定 IPSec 終止節點相關聯的遠端網路，請將頁面頂部的下拉式清單從 **All**（全部）變更為特定 IPSec 終止節點，以檢視該 IPSec 終止節點和該網站遠端網路的統計資料。

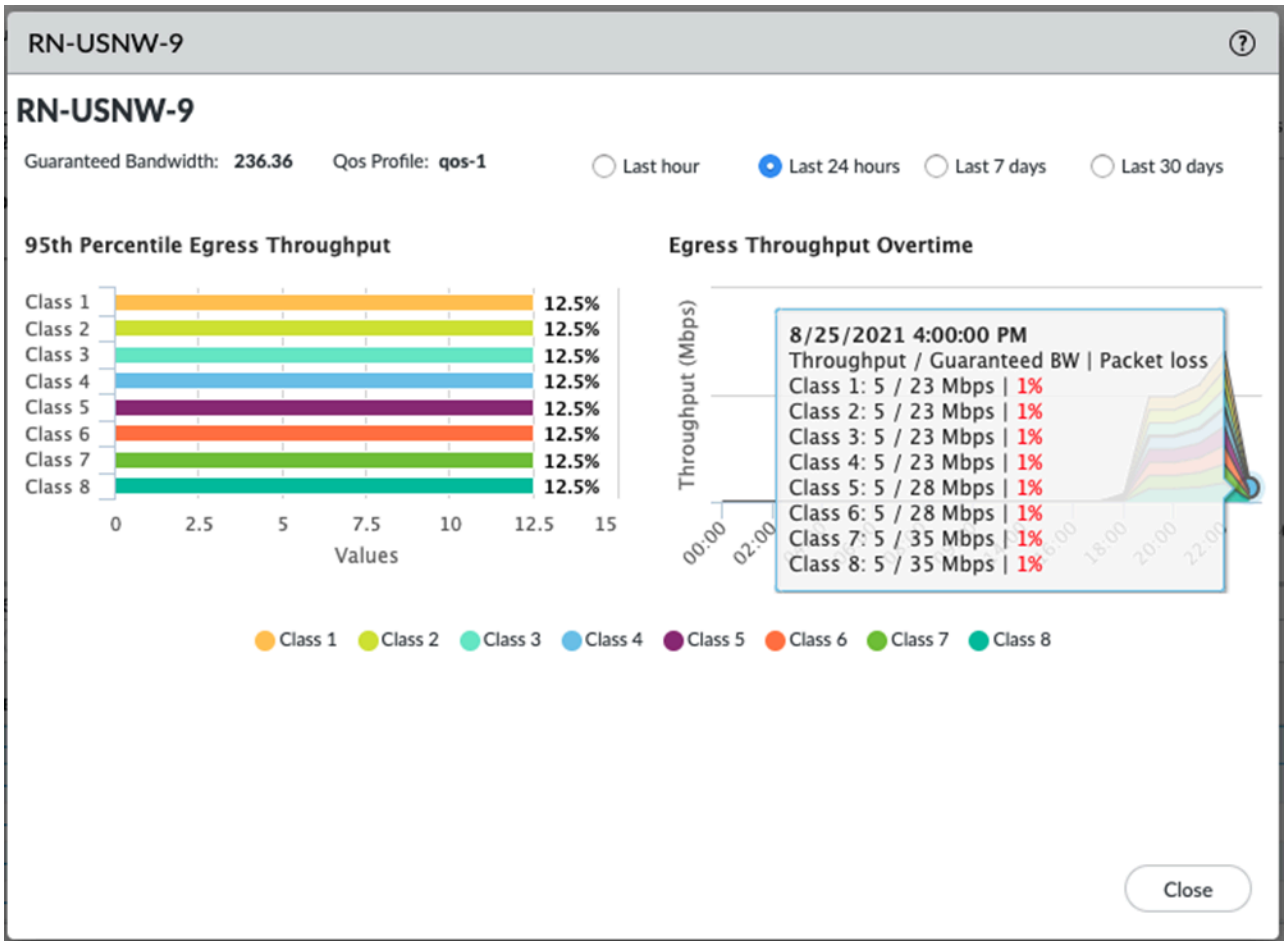



若要檢視依 QoS 類別排序的網站特定流量，請按一下 **Site Name**（網站名稱）。保證頻寬、輸出輸送量和隨時間變化的輸送量隨即為遠端網路網站顯示。您也可以針對過去一小時、過去 24 小時、過去 7 天或過去 30 天排序此資訊。




將游標暫留右側圖形上即可取得特定時段的詳細資訊。

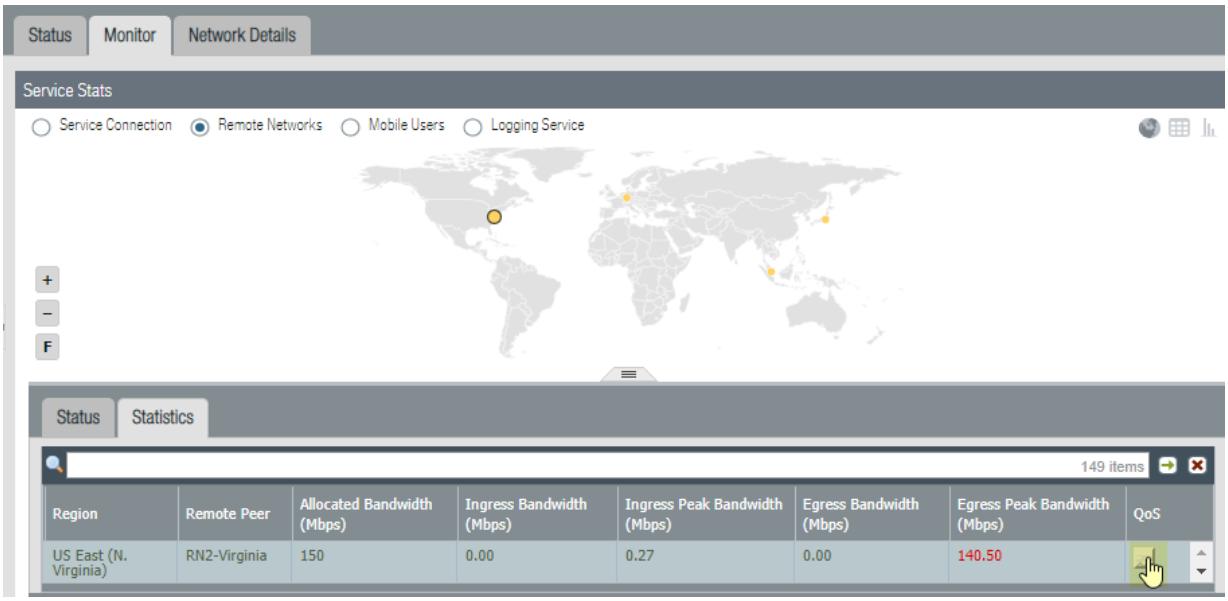

©2025 Palo Alto Networks, Inc.




- 對於服務連線，選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Monitor**（監控） > **Service Connection**（服務連線）、選擇一個區域，然後 **Monitor**（監控）**Statistics**（統計資料）。

按一下 **QoS**，以檢視具有 QoS 統計資料的頁面。

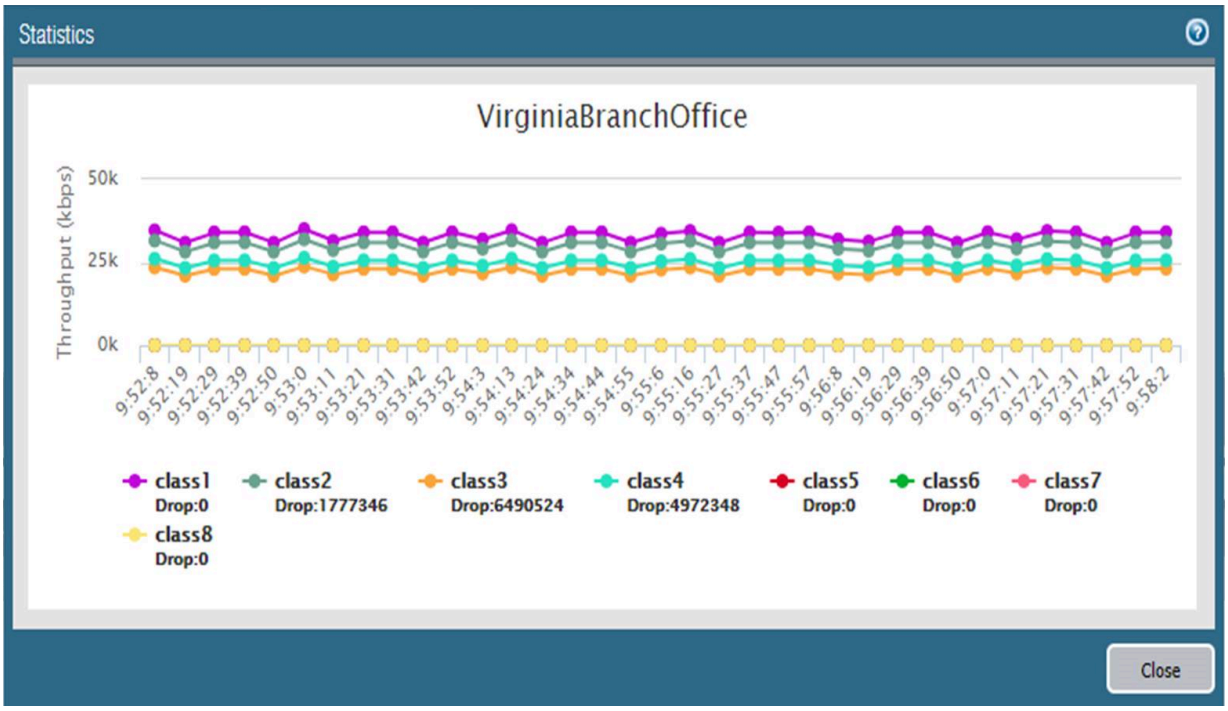

©2025 Palo Alto Networks, Inc.




此頁面顯示具有即時和歷程 QoS 統計資料的圖表，包括每個類別丟棄的封包數目。此圖表僅為啟用了 QoS 的服務連線或遠端網路連線顯示，顯示最後五分鐘的連線網路活動，並每 10 秒重新整理一次。

下圖顯示了針對類別 1、2、3 和 4 傳遞的流量。圖片下的資料顯示根據類別 2、3 和 4 的 QoS 設定丟棄的封包數目。


©2025 Palo Alto Networks, Inc.




變更保證頻寬

# 變更保證頻寬

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

如果您有多個遠端網路位置與一個 IPSec 終端節點相關聯，則可以變更每個網站的保證頻寬。在以下範例中，您想要加拿大東部位置接收的頻寬比加拿大中部位置多；若要這樣做，請完成以下步驟。

**STEP 1 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路） > **Settings**（設定）。

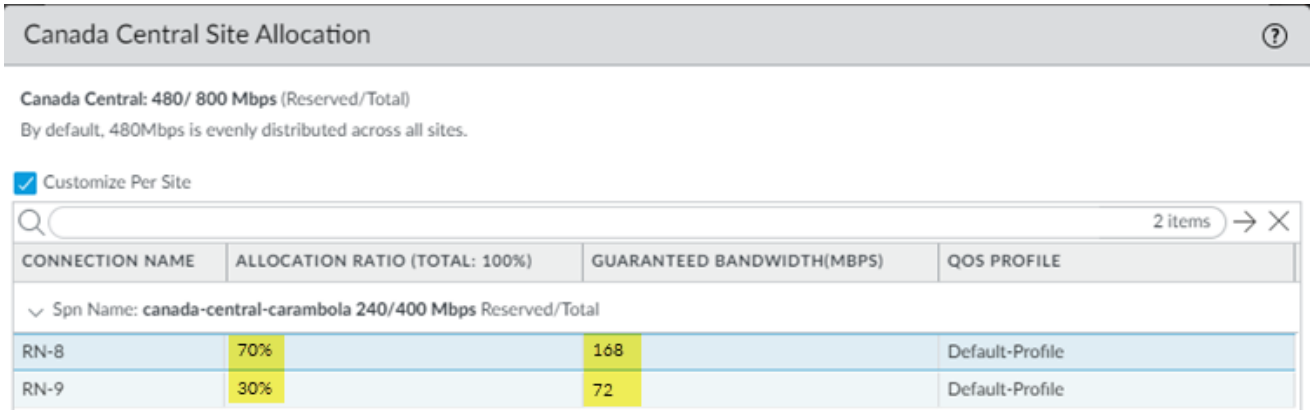
**STEP 2 |** 按一下齒輪以編輯設定，然後選取 **QoS**。

**STEP 3 |** **Enable QoS**（啟用 **QoS**），將 **QoS Profile**（**QoS** 設定檔）（此範例中的 **Default-Profile**）和 **Guaranteed Bandwidth Ratio**（保證頻寬比）指派給加拿大中部計算位置。

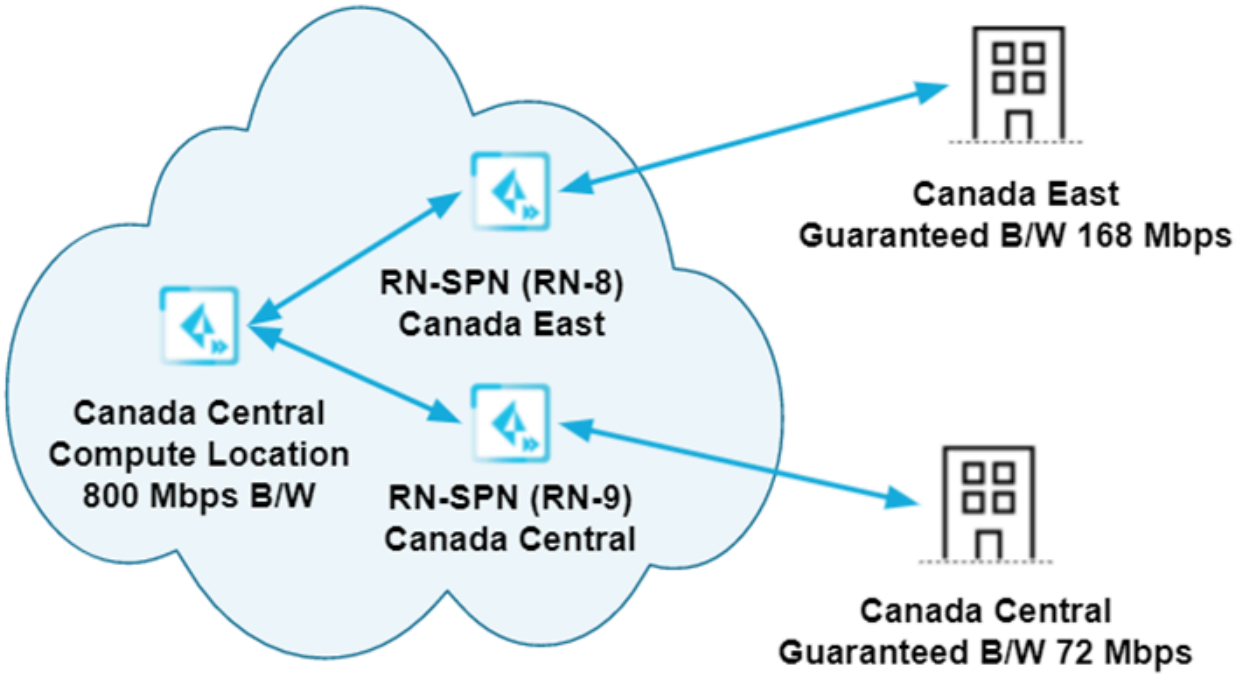
 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 選取**Customize Per Site**（自訂每個網站）、啟用 **Customize Per Site**（自訂每個網站），然後將更高的頻寬 **Allocation Ratio**（配置比）套用於 RN-8 遠端網路（適用於加拿大東部位置），而不是 RN-9 遠端網路（適用於加拿大中部位置）。

以下範例顯示 RN-8 的 **Allocation Ratio**（配置比）為 70%，而 RN-9 為 30%。**Guaranteed Bandwidth (Mbps)**（保證頻寬 **(Mbps)**）會相應地變更，顯示新的保證頻寬量。



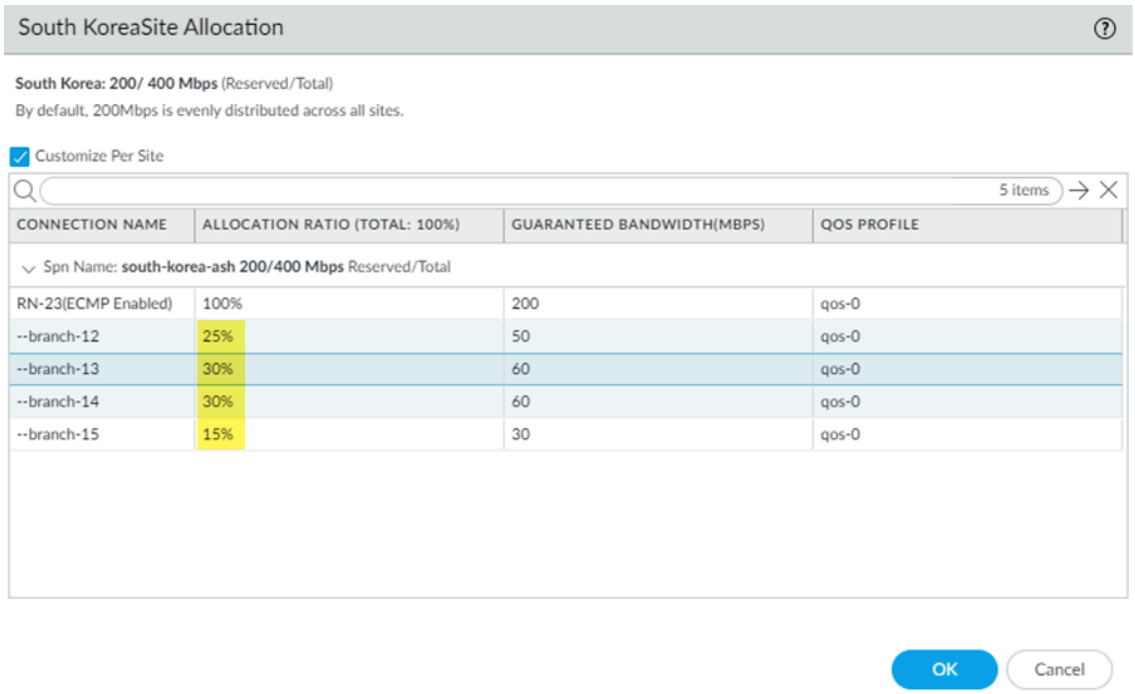

完成後，您的設定將對這兩個網站具有以下保證頻寬配置。




您還可以指派每個遠端網路位置不同的 QoS 設定檔。若要指派不同的設定檔，請啟用 **Customize Per Site**（自訂每個網站）功能，並為每個遠端網路位置選取不同的 QoS 設定檔。

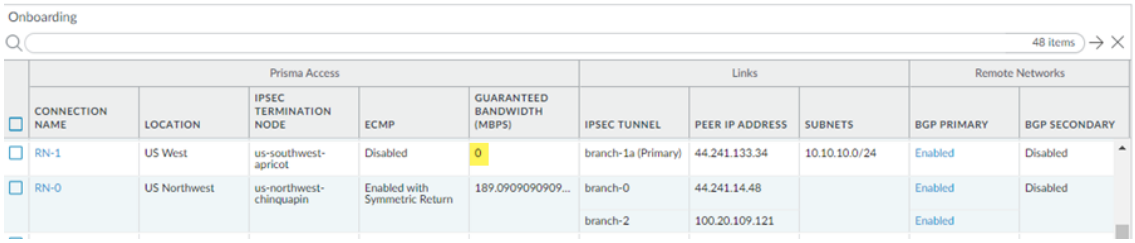
如果您有一個遠端網路啟用了 ECMP，以對單一遠端網路使用多個 IPSec 通道，則可以針對 IPSec 通道變更用於該遠端網路位置的 **Allocation Ratio**（配置比）。


©2025 Palo Alto Networks, Inc.




**STEP 5 |** 儲存並提交您的變更。

保證頻寬值顯示在 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Monitor**（監控） > **Remote Networks**（遠端網路）區域（位於 **Guaranteed Mbps**（保證 **Mbps**）區域）中。如果未指定頻寬，則顯示為 0。




 ©2025 Palo Alto Networks, Inc.

# 遠端網路—高效能

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權<br><br>這是一個有限的可用性版本。若要啟動此功能，請聯繫您的 *Palo Alto Networks* 客戶代表。 |

隨著您的業務規模不斷擴大，並且辦公室位置在地理上不斷地分散，Prisma Access 遠端網路可讓您快速裝載分支網站，並為您的使用者提供最佳的安全性。若要裝載一個具有高頻寬的分支網站，Prisma Access 會為您提供遠端網路—高效能。

若要裝載遠端網路—高效能，請指定分支網站的位置，然後 Prisma Access 會選取最接近該網站的位置。您可以選擇性地設定網站的次要（備份）位置，以取得備援和復原能力。高效能遠端網路為每 3 Gbps 的頻寬使用單一服務 IP 位址，這消除了在每個遠端位置設定和管理多個 IPSec 裝置的複雜性。

不支援次要位置進行 *Prisma Access (Managed by Panorama)* 部署。

在您已為您的遠端網路—高效能進行規劃之後，您可以開始設定程序，其中包括將高效能遠端網路裝載至 Prisma Access，並啟用 QoS 和路由。

## 遠端網路—高效能的功能與指導方針

高效能遠端網路為您提供以下核心功能：

- 一個計算區域中每個節點最高可達 3 Gbps 的彙總頻寬
- 來自遠端網站的每個遠端網路通道最高可達 2 Gbps 頻寬
- 進行 Prisma SD-WAN 和延伸（第三方）CPE 部署時，每個服務 IP 位址最多可有 500 個遠端分支

為分支網站設定高效能遠端網路時，請注意以下指導方針，以及網站與遠端網路之間的差異：

- **Prisma Access** 位置—遠端網路—高效能支援 Prisma Access 位置的子集。
- 服務品質 **(QoS)**—對於分支網站，Prisma Access 支援每個網站層級的 QoS，而且您選取的 QoS 設定檔會套用至整個網站。
- 提交資訊速率 **(CIR)**—若要保護並提交每個網站使用的頻寬量，請指定一個 CIR。如果在計算位置中有多個共用頻寬的遠端網路，則當與該計算位置中的其他網站存在頻寬競爭時，遠端網路—高效能至少會得到 CIR 中指定的頻寬。


©2025 Palo Alto Networks, Inc.

- **IPSec** 終端節點—與遠端網路不同，您在為 Prisma Access (Managed by Strata Cloud Manager) 部署進行裝載期間不需要選取 IPSec 終端節點。Prisma Access 自動針對遠端網路連線進行負載平衡，以最大程度地將頻寬配置給網站。

  您仍需要為從 Panorama 裝載的遠端網路選取一個 IPSec 終端節點。
- 通道和計算位置備援以及每個網站的通道數上限—高效能遠端網路讓您可以同時設定位置和 IPSec 備援。
  - 位置備援（在某個計算位置中指定 **Primary**（主要）位置，並在個別的計算位置中指定 **Secondary**（次要）位置）。

    設定次要位置是選用的，而且次要位置必須位於與主要位置不同的計算位置。
  - IPSec 通道備援（指定為 **Active/Active**（主動/主動）或 **Active/Passive**（主動/被動））。

  下表為您提供每個通道的位置數下限和上限。

| 位置部署類型 | 通道部署類型 | 通道數下限 | 通道數上限 |
|---|---|---|---|
| 僅限主要 | 主動/被動 | 1 | 2 |
| 僅限主要 | 主動/主動 | 2 | 4 |
| 主要和次要 | 主動/被動 | 2 | 4 |
| 主要和次要 | 主動/主動 | 4 | 8 |

- 根據部署類型配置服務 **IP** 位址—您收到的服務 IP 位址數目取決於您在單一位置中設定了高效能遠端網路，還是已在主要和次要部署中使用兩個不同的位置設定它們。
  - 如果您在單一位置中設定了高效能遠端網路，但沒有次要位置，Prisma Access 會為您提供單一服務 IP 位址。
  - 如果您在主要和次要設定中設定了計算位置備援，Prisma Access 會為您提供兩個服務 IP 位址（主要和次要設定各有一個）。

  如果您在主動/被動設定中設定了 IPSec 通道，則 Prisma Access 會為您提供這兩個通道的單一服務 IP 位址（與標準 Prisma Access 遠端網路設定相同）。
- 根據頻寬配置服務 **IP** 位址—Prisma Access 會在計算位置中為您提供每 3 Gbps 頻寬一個單一的 IP 位址或 FQDN。
- 每個計算位置的頻寬—您配置每個計算位置的頻寬方式與為標準遠端網路配置頻寬的方式相同。您可以在開始設定之前或在高效能遠端網路建立期間規劃和配置頻寬。
- **IPv6** 支援—不支援 IPv6 進行遠端網路—高效能部署。

請使用下列其中一個程序來裝載您的遠端網路，取決於您的頻寬配置類型：

- Prisma Access (Managed by Strata Cloud Manager)
- Prisma Access (Managed by Panorama)

## Strata Cloud Manager

以下是使用 Strata Cloud Manager 新增遠端網路—高效能的方式。

 ©2025 Palo Alto Networks, Inc.

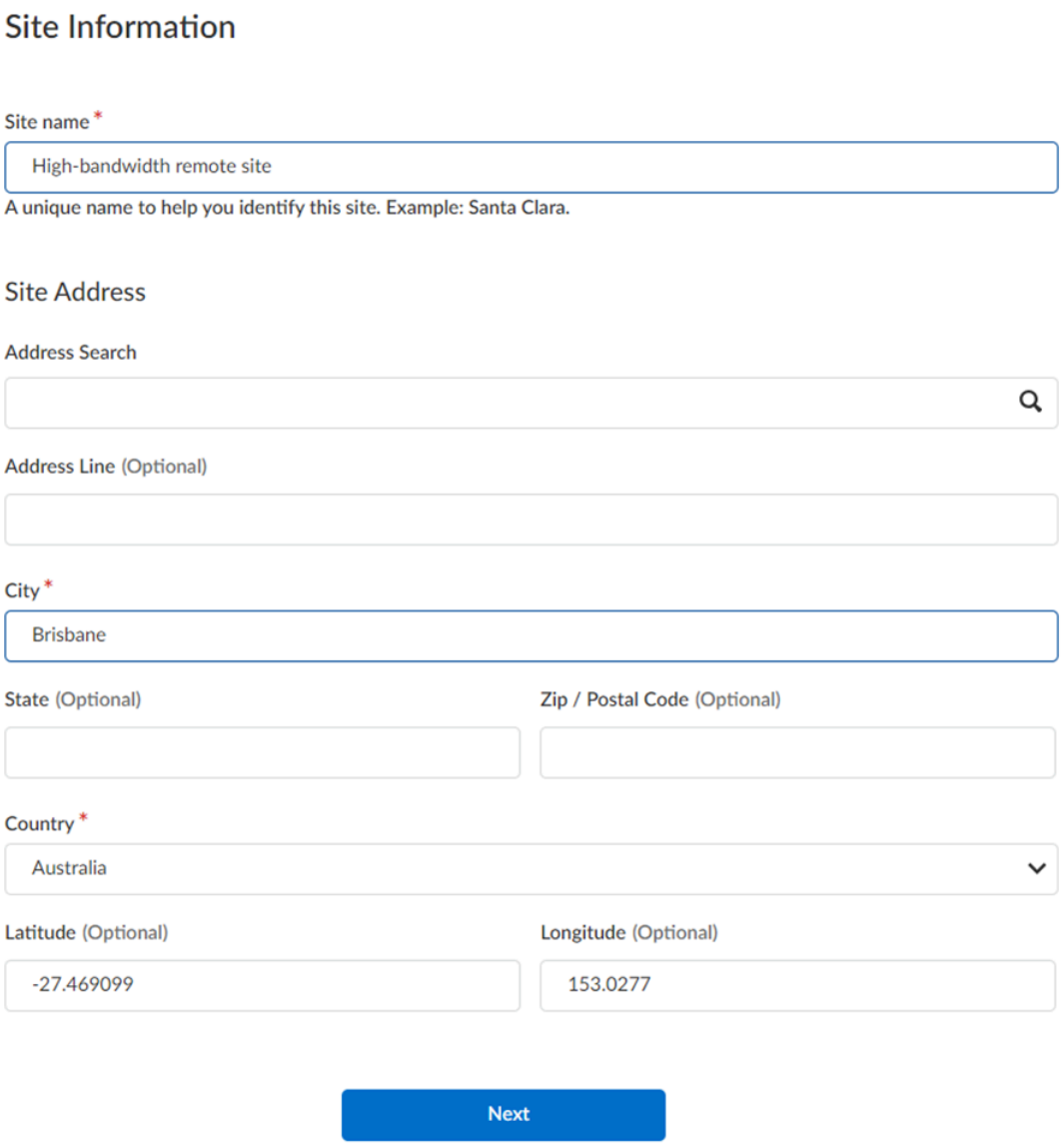
**STEP 1 |** 從 Strata Cloud Manager 中，前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Branch Sites**（分支網站）。

此選項表示您為分支網站建立的通道由您的 CPE（Palo Alto Networks 新世代防火牆或第三方 CPE）終止。

**STEP 2 |** **Add Site**（新增網站），並給與遠端網路一個描述性 **Site Name**（網站名稱）。

**STEP 3 |** 選取網站的 **City**（城市）和 **Country**（國家/地區）。

如需更精確的搜索，請新增位址。




**STEP 4 |** 按一下 [Next（下一步）]。

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** 輸入 **QoS CIR (Committed Information Rate)**（**QoS CIR**（提交資訊速率））， 以 Mbps 為單位。

如果您在計算位置中有多個共用頻寬的遠端網路， 並且如果與該計算位置中的其他網站存在頻寬競爭， 則遠端網路—高效能至少會得到 CIR 中指定的頻寬。

如果您設定主要和次要網站， 請指定不同的計算區域， 而且次要區域會獲得 20% 的 CIR。 例如， 如果您對網站設定 100 Mbps 的 CIR， 則 Prisma Access 會為主要網站提供 100 Mbps CIR， 而為次要網站提供 20 Mbps CIR。

如果 CIR 是 500 Mbps， 以及如果計算位置中所有剩餘的頻寬都被其他網站使用， 則 Prisma Access 會丟棄超過 500 Mbps 的任何頻寬。不過， 如果其他網站未使用頻寬， 則高效能遠端網路的頻寬可以超過 500 Mbps， 直到計算位置中配置的頻寬。

輸入至少 1 Mbps 和至多 2000 Mbps 的 CIR。請勿超過您為計算區域指定的頻寬。

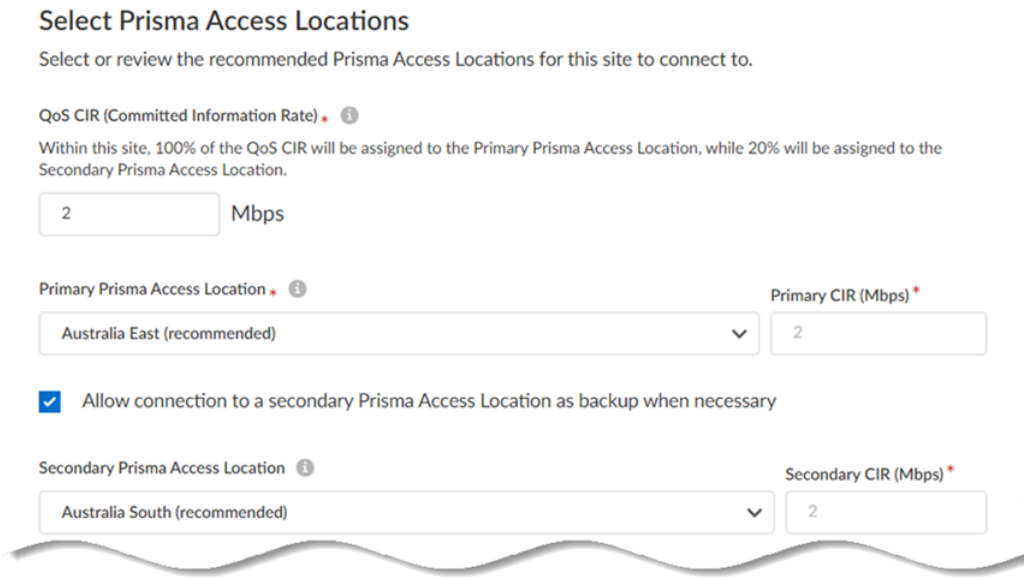
**STEP 6 |** 選取 **Primary Prisma Access Location**（主要 **Prisma Access** 位置）。

如果清單中建議了多個位置， 請選取最適合您部署的位置。

 ©2025 Palo Alto Networks, Inc.

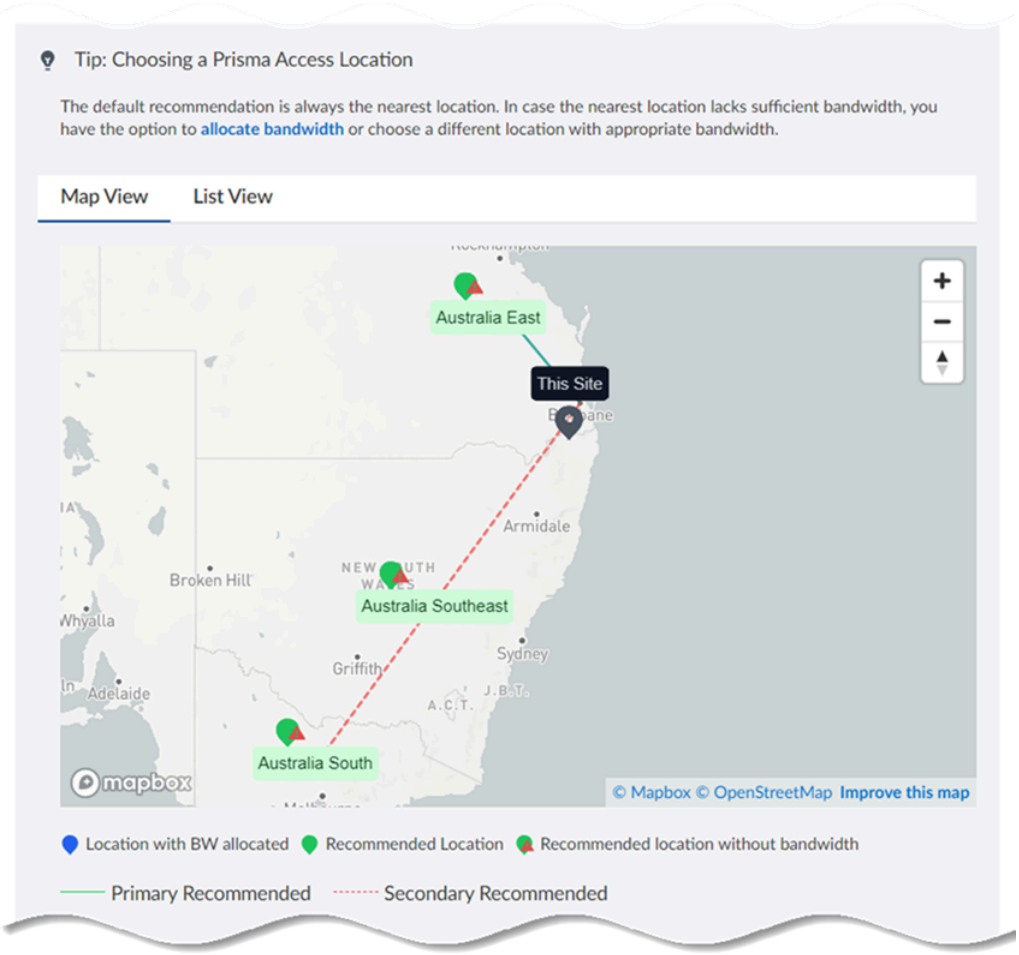
**STEP 7 |** （選用）若要建立一個次要（備份）網站，請選取 **Allow connection to a secondary Prisma Access Location as backup when necessary**（必要時允許連線至次要 **Prisma Access** 位置作為備份），然後選取 **Secondary Prisma Access Location**（次要 **Prisma Access** 位置）。

如果您選取此選項，Prisma Access 會自動填入其所在計算位置與主要位置不同的最佳次要位置。如果建議多個位置，請選取最適合您部署的位置。




Prisma Access 提供您一張地圖，其中建議的位置可協助您選擇一個。

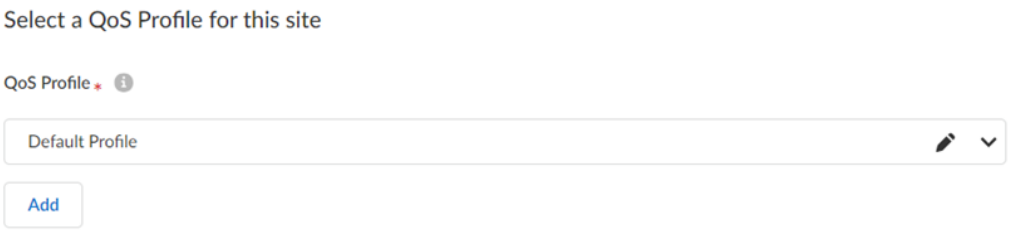
 ©2025 Palo Alto Networks, Inc.




 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** 選擇一個 **QoS Profile**（**QoS** 設定檔） 以用於此網站。

遠端網路—高效能使用單一 QoS 設定檔。

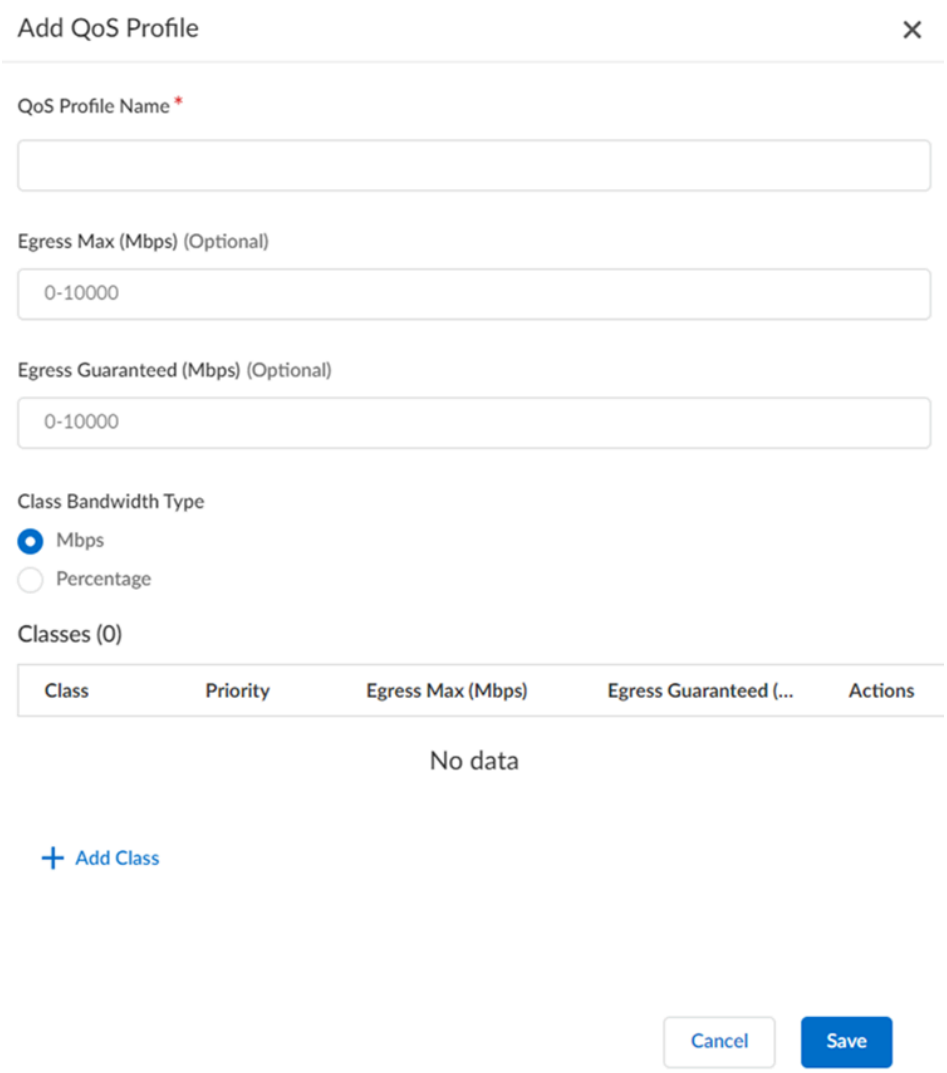



如果您尚未建立 QoS 設定檔，請 **Add**（新增）一個 QoS 設定檔，同時指定以下值：

- 輸入唯一的 **QoS Profile Name**（**QoS** 設定檔名稱）。
- （選用）輸入 **Egress Max**（輸出上限），表示離開服務連線或遠端網路連線的流量的最大輸送量（以 Mbps 為單位）。
- （選用）輸入一個 **Egress Guaranteed (Mbps)**（輸出保證 **(Mbps)**） 值，該值代表此設定檔的保證頻寬，以 Mbps 為單位。
- 輸入 **Class Bandwidth Type**（類別頻寬類型）為 **Percentage**（百分比）或 **Mbps**。

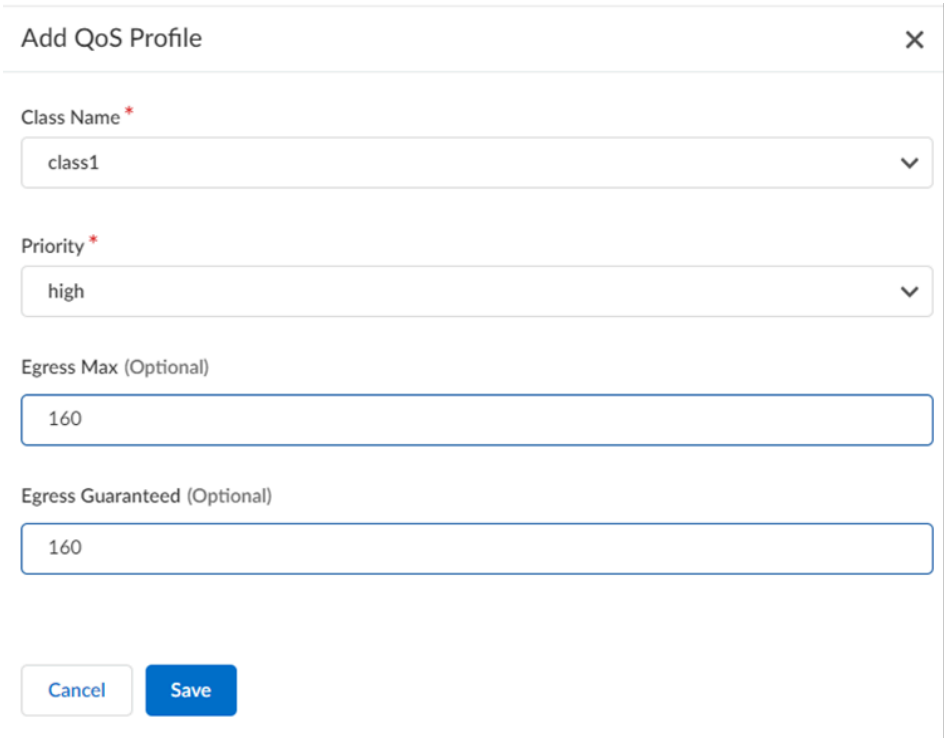
  遠端網路—高效能的 QoS 不會使用保證頻寬比。

 ©2025 Palo Alto Networks, Inc.




- 在 [Classes（類別）] 區段中，**Add Class**（新增類別），並指定如何標記最多八個單獨的 QoS 類別。
  - 輸入 **Class Name**（類別名稱）。
  - 為類別選取 **Priority**（優先順序）（**real-time**（即時）、**high**（高）、**medium**（中）或 **low**（低））。
  - 輸入 **Egress Max**（輸出上限），表示離開服務連線或遠端網路連線的流量的最大輸送量（以 Mbps 為單位）。
  - 輸入一個 **Egress Guaranteed (Mbps)**（輸出保證 **(Mbps)**）值，該值代表此設定檔的保證頻寬，以 Mbps 為單位。
- **Save**（儲存）變更。


©2025 Palo Alto Networks, Inc.

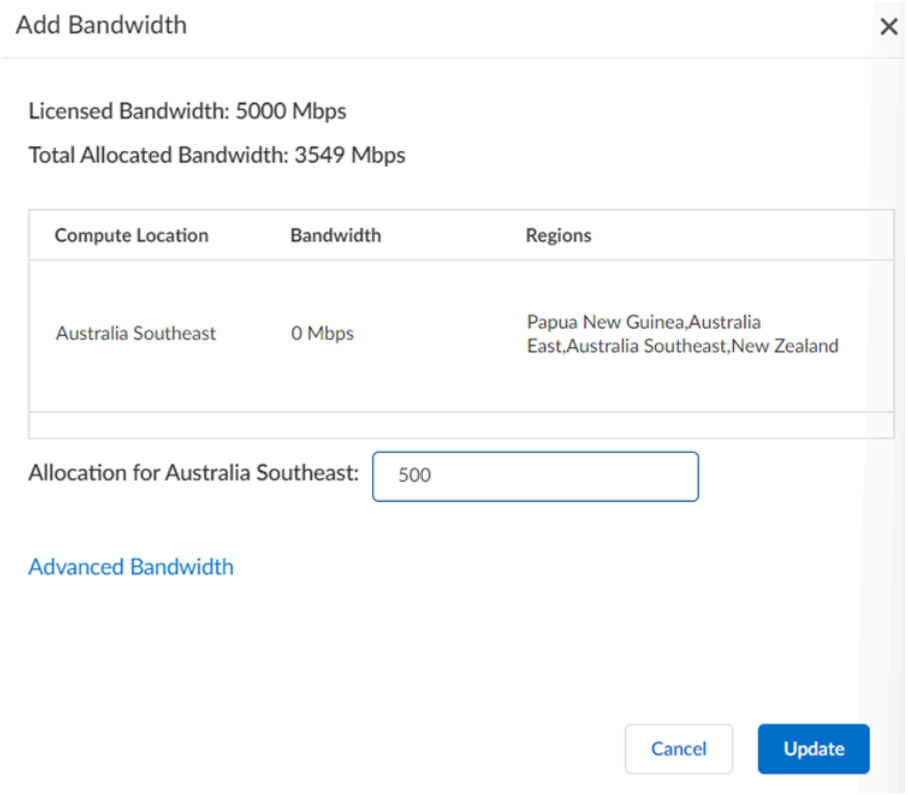



**STEP 9 |** 如果您尚未配置頻寬，Prisma Access 會提示您為與所選位置相關聯的計算位置 **allocate**（配置）頻寬。指定每個計算位置的最小頻寬為 50 Mbps。




 ©2025 Palo Alto Networks, Inc.

**STEP 10 |** 如果您尚未這樣做，請為您選取的位置配置頻寬；然後，**Update**（更新）您的變更。




**STEP 11 |** 按一下 [Next（下一步）]。

**STEP 12 |** 定義 **Tunnel & Circuit Settings**（通道與電路設定）。

1. 選取 **Tunnel Mode**（通道模式）：**Active/Active**（主動/主動）或 **Active/Passive**（主動/被動）。

   通道模式指定您想要為高效能遠端網路使用多少個 ISP 電路。

   - 如果您選取 **Active/Active**（主動/主動），則 Prisma Access 會使用四條 ISP 電路來建立兩個或四個主動通道。
   - 如果您選取 **Active/Passive**（主動/被動），則 Prisma Access 會使用兩個 ISP 電路來建立兩個主動通道。如果主動通道失效，被動通道會變成主動。

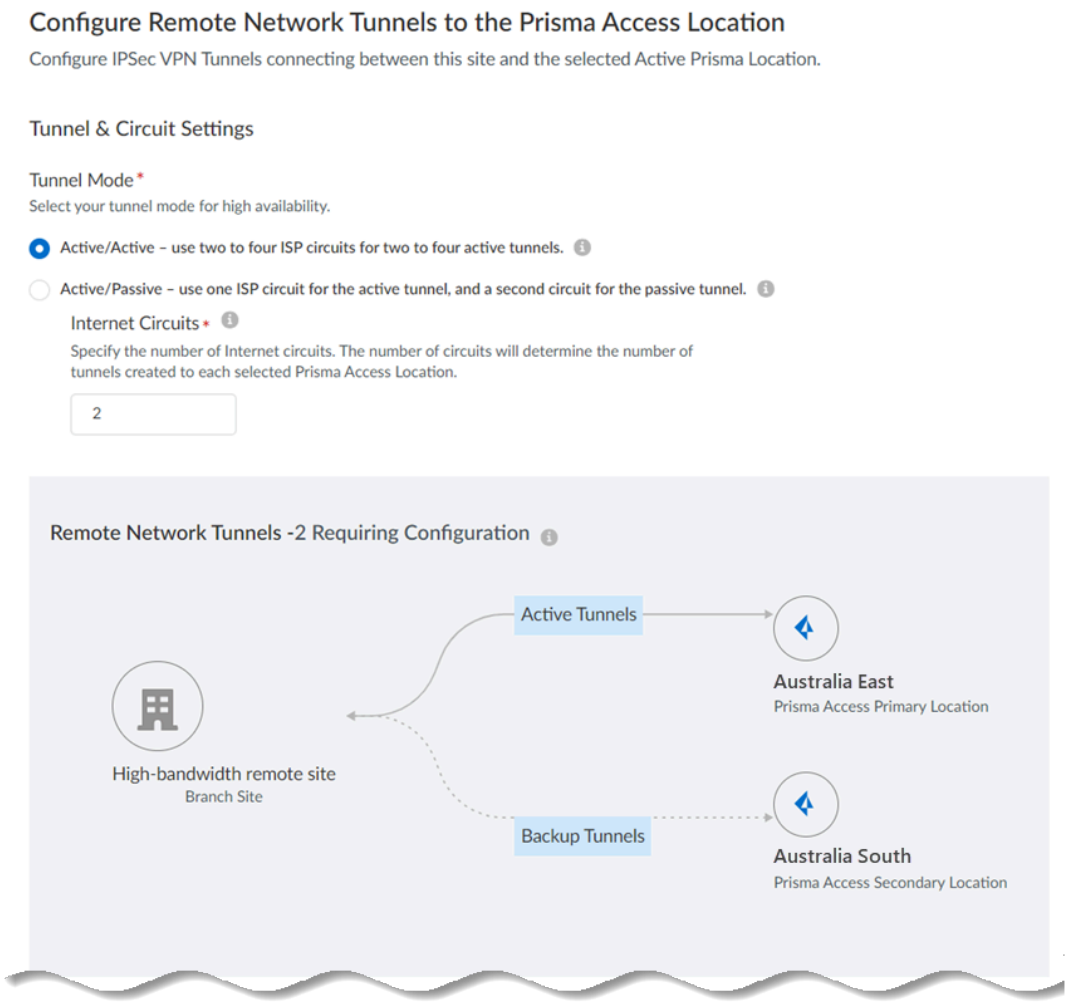
2. 選取要使用的 **Internet Circuits**（網際網路電路）數目。

   Prisma Access 根據您在這裡指定的電路數目，以及您的部署是主動/主動還是主動/被動來指派通道，如下表所示。

| 電路數目 | 部署類型 | 通道數目 |
|---|---|---|
| 1 | 主動/被動 | 1（一個用於主動通道)。 |
| 2 | 主動/主動 | 2（每個主動通道各有一個）。 |


©2025 Palo Alto Networks, Inc.

| 電路數目 | 部署類型 | 通道數目 |
|---|---|---|
| | | 如果您選取主要和次要位置，則 Prisma Access 會為主要位置建立一個主動通道，以及為次要位置建立一個主動通道。 |
| 2 | 主動/被動 | 2（每個主動通道各有一個）。<br>如果您選取主要和次要位置，則 Prisma Access 會為主要位置建立一個主動和被動通道，以及為次要位置建立一個主動和被動通道。如果主動通道失效，則 Prisma Access 會為變成主動的被動通道使用相同的服務 IP 位址或 FQDN。 |
| 4 | 主動/主動 | 4（每個主動通道各有一個）。<br>如果您選取主要和次要位置，則 Prisma Access 會為主要位置建立兩個主動通道，以及為次要位置建立兩個主動通道。 |

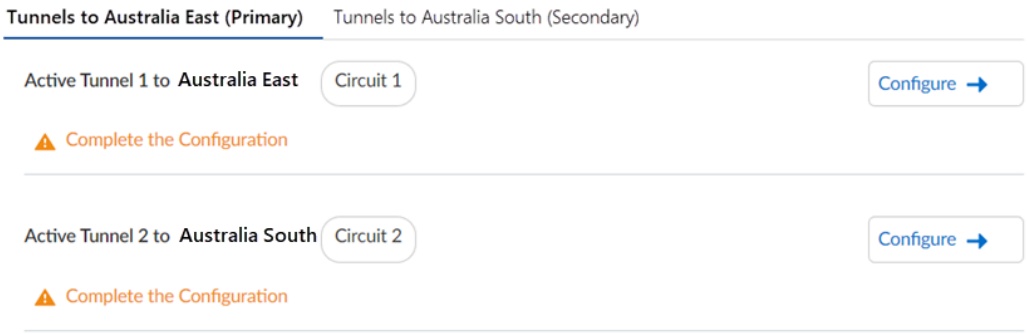



 ©2025 Palo Alto Networks, Inc.

3. （選用）**Configure**（設定）您的 IPSec 通道設定。

   Prisma Access 為您提供預設的 IPSec 通道設定。這些設定確定遠端網路通道的 IPSec 和 IKE 密碼設定。如果您想變更它們，請選取 **Primary Tunnel**（主要通道）並 **Edit**（編輯）您的設定。

   如果您指定次要位置，則Prisma Access 會將這些值從主要通道自動填入到次要通道；若要編輯次要通道，請選取該通道並 **Edit**（編輯）設定。




   請記下這些設定；您必須在終止您網站上 IPSec 通道的 CPE 上比對這些設定。

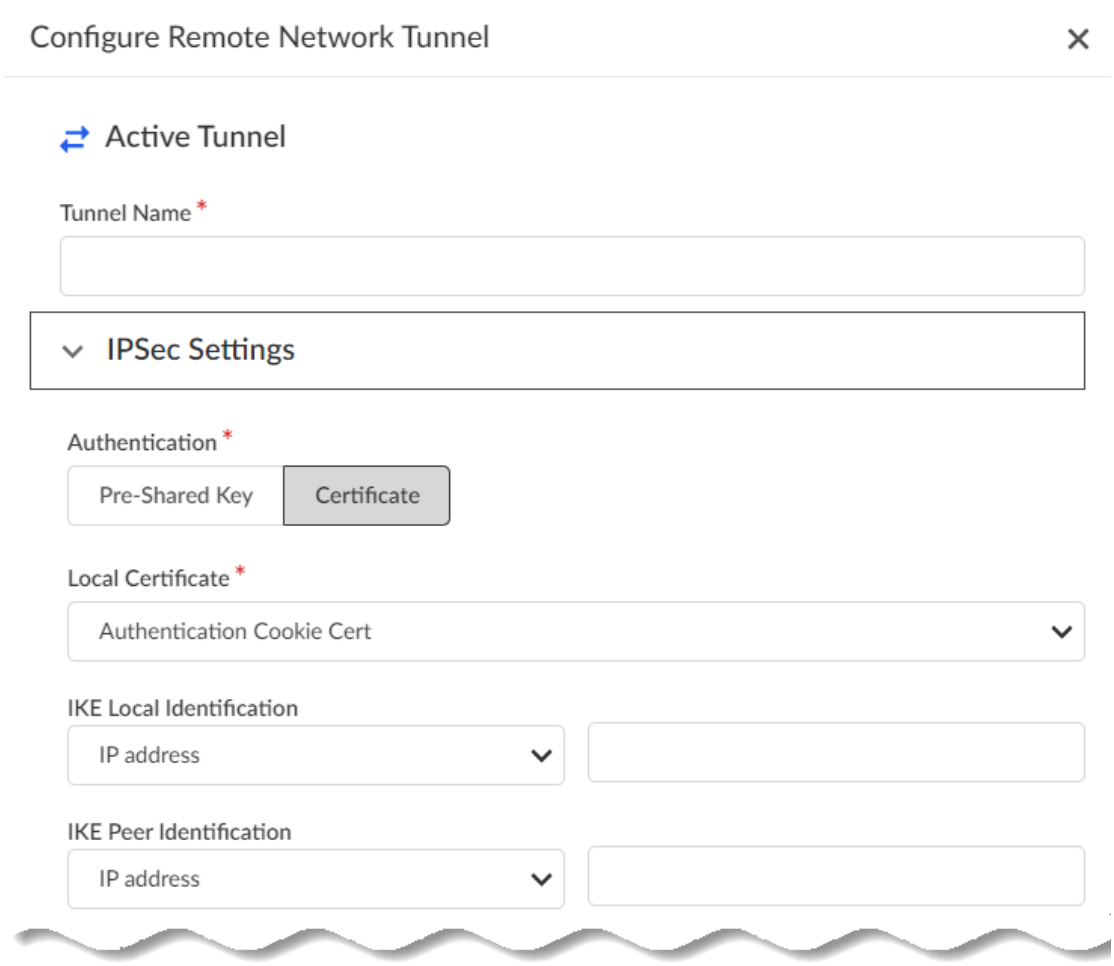
   - 給與主動通道唯一的 **Tunnel Name**（通道名稱）。
   - 指定 **IPSec Settings**（**IPSec** 設定）。
     - 指定 **Authentication**（驗證類型）（**Pre-Shared Key**（預先共用金鑰）或 **Certificate**（憑證））。

       如果您指定 **Pre-Shared Key**（預先共用金鑰），請輸入並確認 **Pre-Shared Key**（預先共用金鑰）。

       如果您指定 **Certificate**（憑證），請輸入要使用的 **Local Certificate**（本機驗證）。此憑證必須已存在於 Strata Cloud Manager。
     - 指定 **IKE Local Identification**（**IKE** 本機識別）（**IP Address**（**IP** 位址）、**Distinguished Name (Subject)**（辨別名稱（主旨））、**User FQDN (email address)**（使用者 **FQDN**（電子郵件））或 **FQDN (hostname)**（**FQDN**（主機名稱））。
     - 指定 **IKE Peer Identification**（**IKE** 對等識別）（**IP Address**（**IP** 位址）、**Distinguished Name (Subject)**（辨別名稱（主旨））、**User FQDN (email**


©2025 Palo Alto Networks, Inc.

**address)**（使用者 **FQDN**（電子郵件））或 **FQDN (hostname)**（**FQDN**（主機名稱））。

- 


- 指定對等 ID 檢查的類型：
  - **Exact**（完全符合）—確保本機設定和對等 IKE ID 承載完全相符。
  - **Wildcard**（萬用字元）—讓對等識別比對出萬用字元 **(*)** 之前的每個相符字元。萬用字元之後的字元不需要比對。
- （選用）如果即使對等識別不符合憑證中的對等識別，也仍然想要允許成功的 IKE 安全性關聯 (SA)，請 **Permit peer identification and certificate payload identification mismatch**（容許對等識別與憑證承載識別不相符）。
- 選擇 **Certificate Profile**（憑證設定檔）。憑證設定檔包含關於如何驗證對等閘道的資訊。
- （選用）若要嚴格控制金鑰的使用方式，請 **Enable strict validation of peer's extended key use**（對對等的擴充金鑰使用方法啟用嚴格驗證）。
- 選擇 **Branch Device IP Address**（分支裝置 **IP** 位址）（**Static**（靜態）或 **Dynamic**（動態））。
  - 如果您選取 **Static**（靜態），請輸入要用於 IPsec 通道的 **Static IP Address**（靜態 **IP** 位址）。

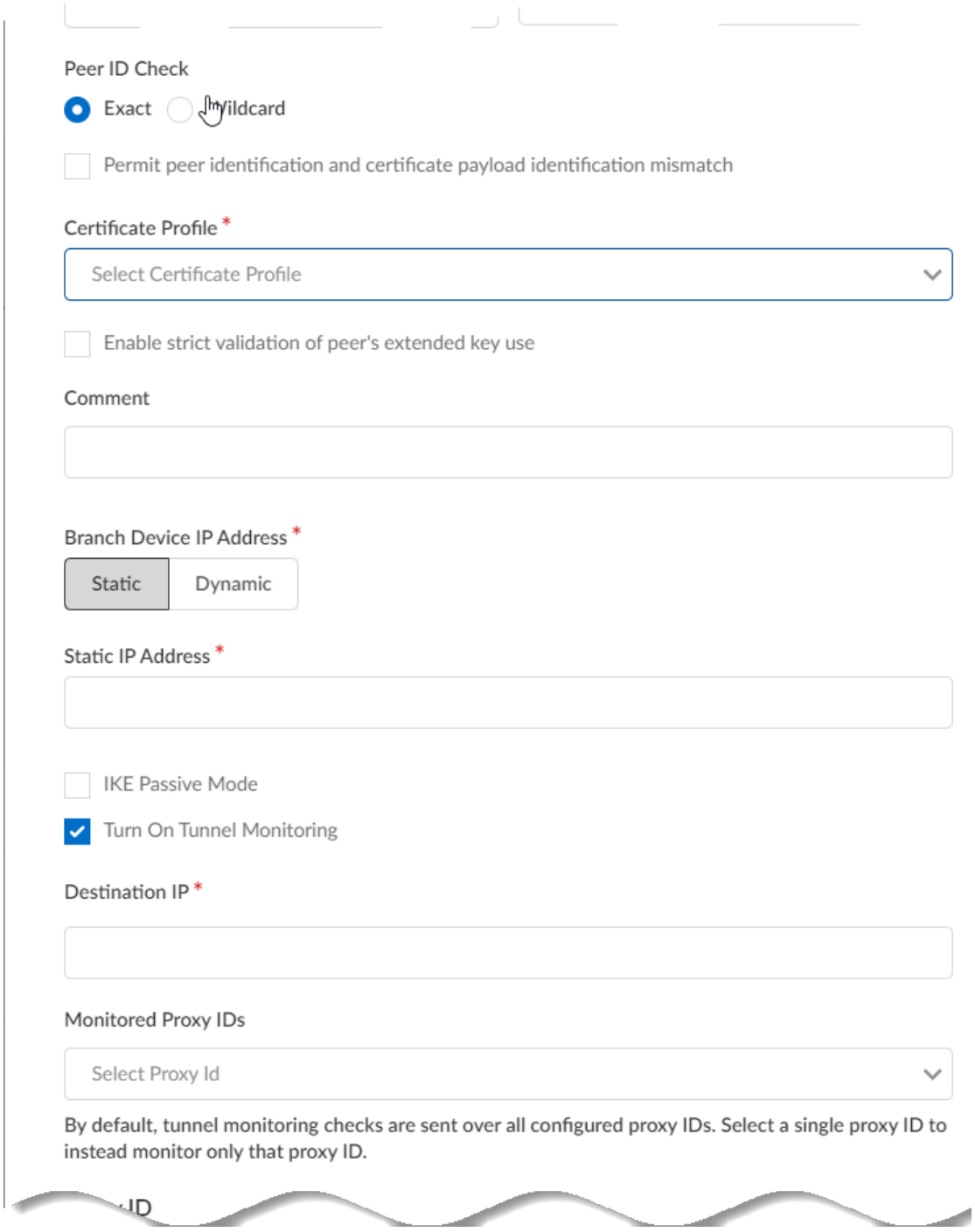

©2025 Palo Alto Networks, Inc.

  - 指定 **Dynamic**（動態）以自動取得 IP 位址。
- （選用，建議）啟用 **IKE Passive Mode**（**IKE** 被動模式），使 Prisma Access 回應 IKE 連線，但不起始這些連線。

  雖然不是必要的，但建議使用 **IKE Passive Mode**（**IKE** 被動模式）。
- （選用）**Turn on Tunnel Monitoring**（開啟通道監控）。

  輸入遠端網路上的通道監控 **Destination IP**（目的地 **IP**）位址，讓 Prisma Access 用來確定通道是否已啟動，此外，如果您的分支 IPSec 裝置使用政策型 VPN，請輸入相關聯的 **Proxy ID** 作為 **Monitored Proxy ID**（監控的 **Proxy ID**）。

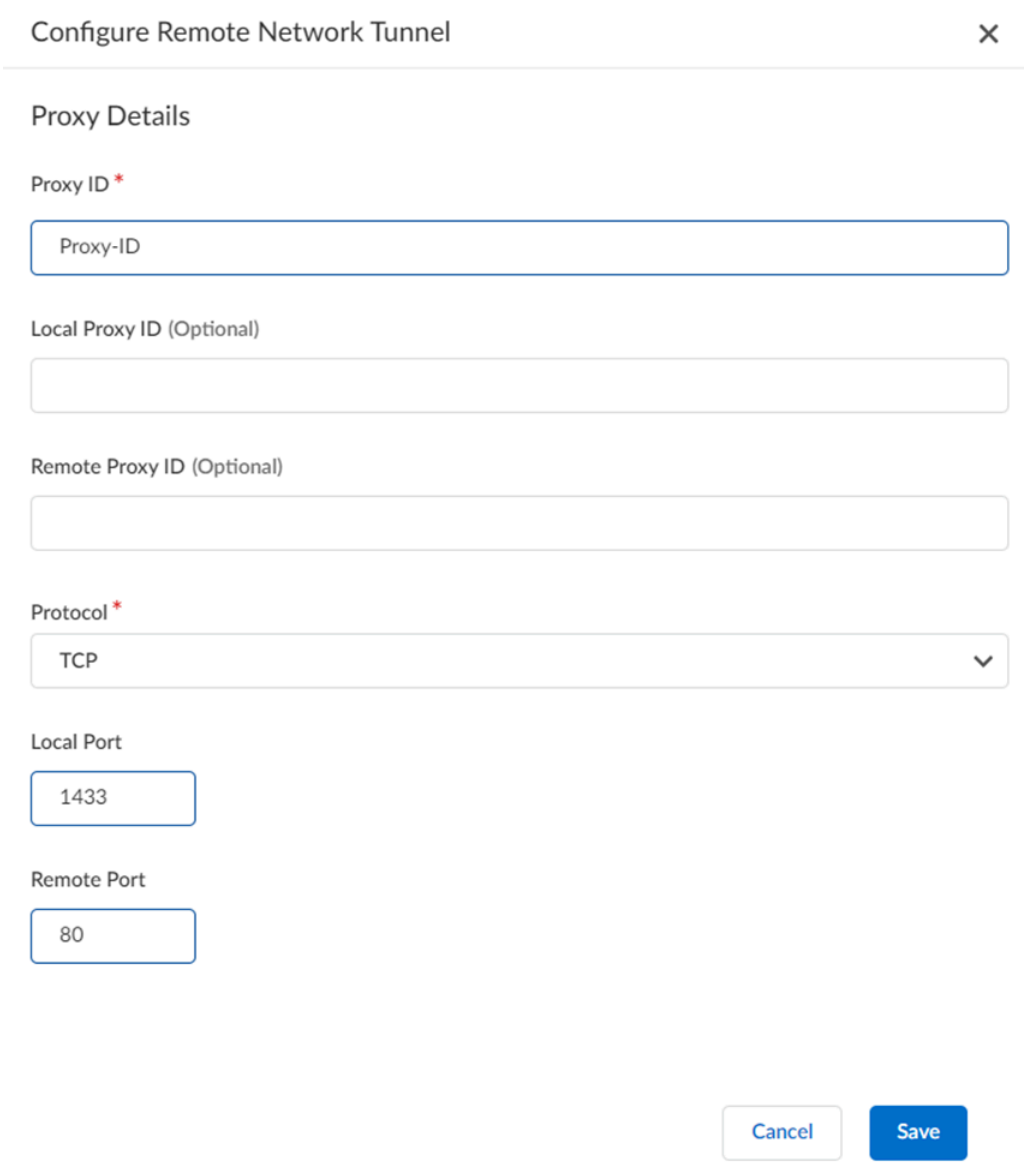
 ©2025 Palo Alto Networks, Inc.




- （選用）如果您需要 Proxy ID：
  - **Add Proxy ID**（新增 **Proxy ID**）並輸入 **Proxy ID**。
  - 選擇性地輸入 **Local Proxy ID**（遠端 **Proxy ID**）和 **Remote Proxy ID**（遠端 **Proxy ID**）。
  - 輸入要用於 Proxy ID 的 **Protocol**（通訊協定）。輸入 **Number**（數字）、**TCP** 或 **UDP**。


©2025 Palo Alto Networks, Inc.

- 指定 TCP 或 UDP 的 **Local Port**（本機連接埠）和 **Remote Port**（遠端連接埠），或指定
- **Save**（儲存）您的變更。



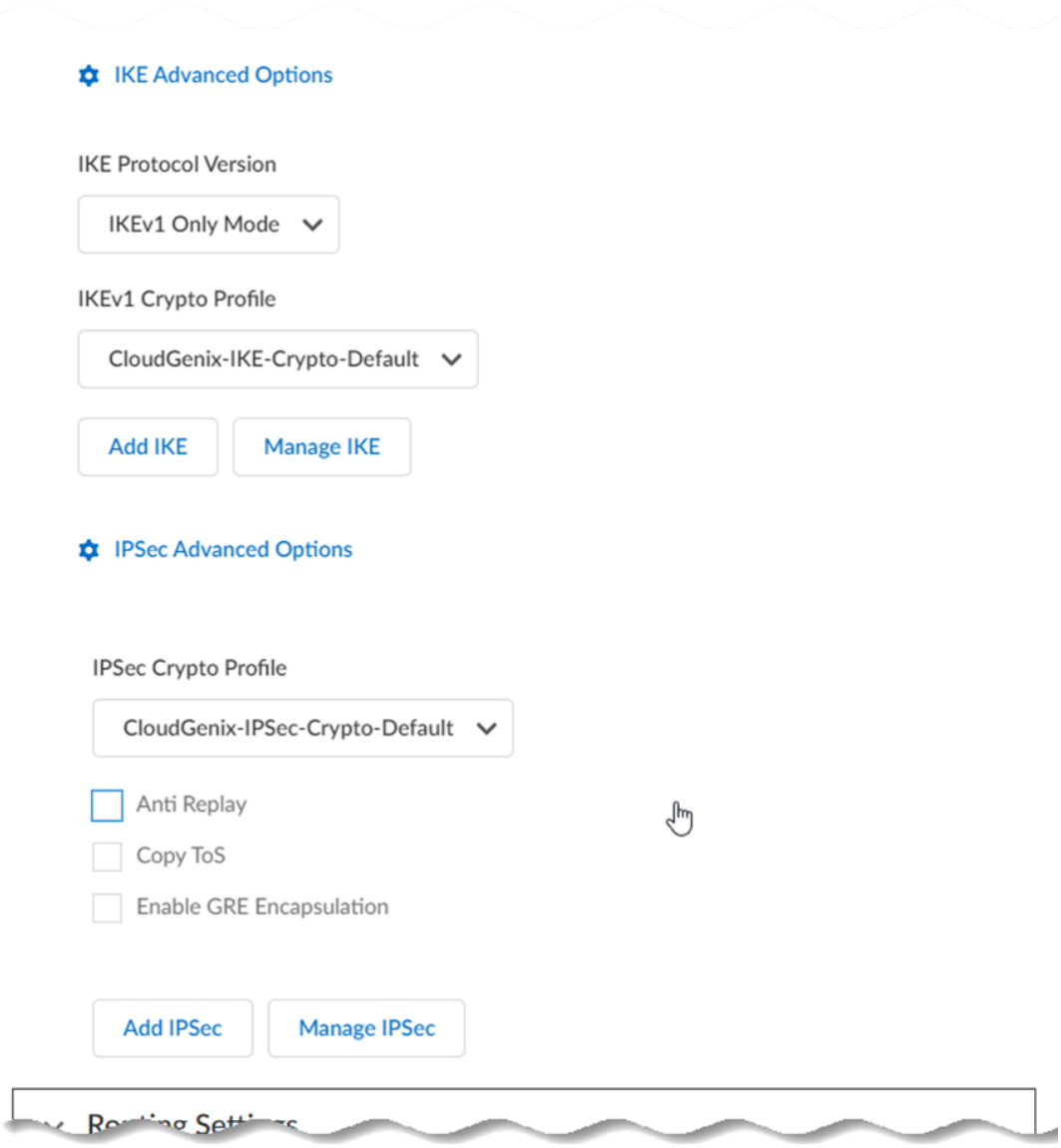

- 指定 **IKE Advanced Options**（**IKE** 進階選項）。
  - 選取 **IKE Protocol Version**（**IKE** 通訊協定版本）。
  - 選取 **IKEv1 Crypto Profile**（**IKEv1** 加密設定檔）。

    若要新增密碼設定檔，請 **Add IKE**（新增 **IKE**）。若要管理現有的 IKE 設定檔，請 **Manage IKE**（管理 **IKE**） 並選取要編輯的設定檔。
  - 選取 **IKEv2 Crypto Profile**（**IKEv2** 密碼設定檔）。

    若要新增加密設定檔，請 **Add IKE**（新增 **IKE**）。若要管理現有的 IKE 設定檔，請 **Manage IKE**（管理 **IKE**） 並選取要編輯的設定檔。


©2025 Palo Alto Networks, Inc.

- 指定 **IPSec Advanced Options**（**IPSec** 進階選項）。
  - 選取 **IPSec Crypto Profile**（**IPSec** 密碼設定檔）。

    若要新增加密設定檔，請 **Add IPSec**（新增 **IPSec**）。若要管理現有的 IPSec 設定檔，請 **Manage IPSec**（管理 **IPSec**） 並選取要編輯的設定檔。
- 

- 選擇您的 **Routing Settings**（路由設定）。
  - 選取 **Routing Type**（路由類型）（**Static**（靜態）或 **Dynamic**（動態））。

    如果您選取 **Static**（靜態），請 **Add**（新增）您想要在網站上保護的 IP 子網路或 IP 位址。

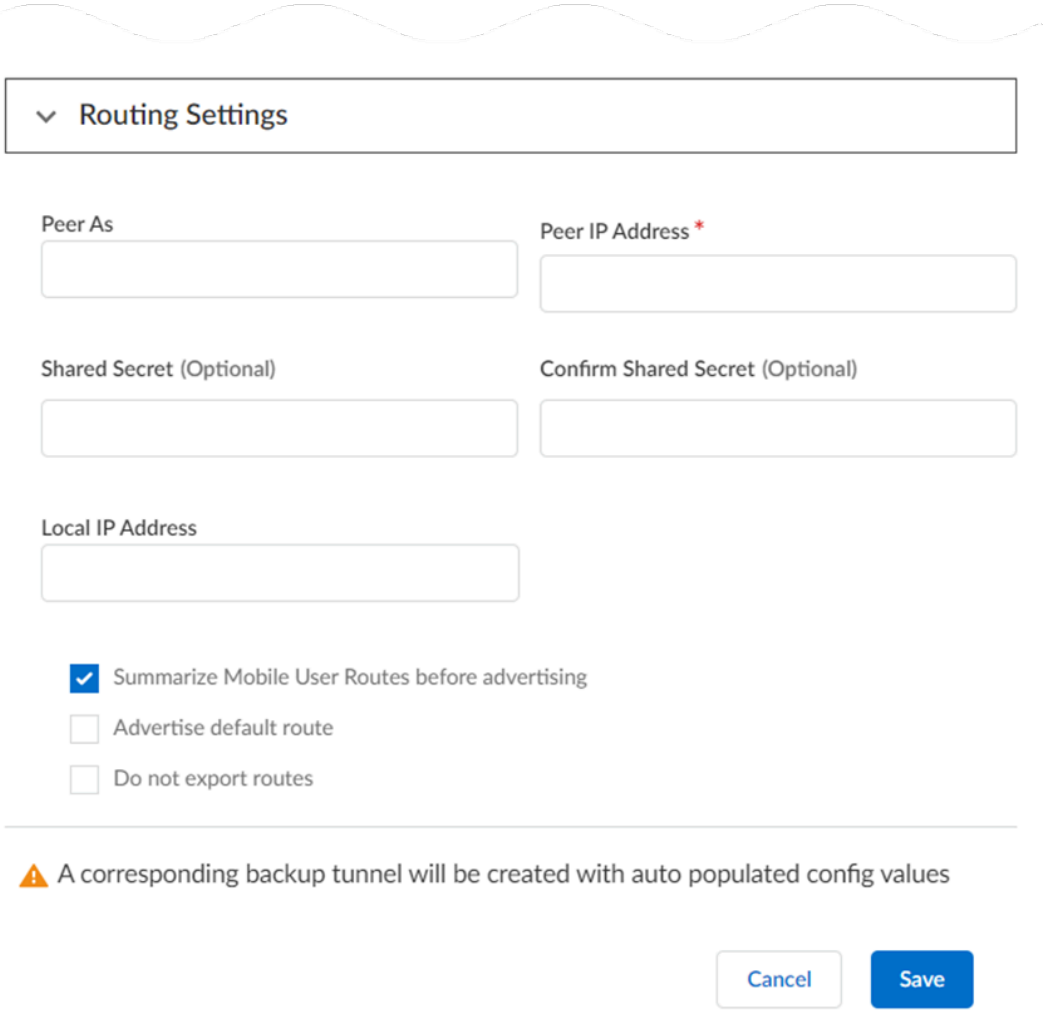
    如果您選取 **Dynamic**（動態）：
    - 輸入 **Peer AS**（對等 **AS**）（您網路的自發系統 (AS)）。

      使用符合 RFC 6996 規範的 BGP 私人 AS 編號。

 ©2025 Palo Alto Networks, Inc.

- 輸入 **Peer IP Address**（對等 **IP** 位址），其已指派為總部或資料中心網路上 eBGP 路由器的路由器 ID。
- （選用）輸入 **Shared Secret**（共用密碼）密碼，驗證 BGP 對等通訊。
- 輸入 **Local IP Address**（本機 **IP** 位址），Prisma Access 會將其用作 BGP 的本機 IP 位址。
- （選用）選取 **Summarize Mobile User Routes before advertising**（在公告之前彙總行動使用者路由），以減少透過 BGP 對客戶周邊設備 (CPE) 進行的行動使用者 IP 子網路公告數目，方法是讓 Prisma Access 在公告子網路之前彙總這些子網路。
- （選用）選取 **Advertise Default Route**（公告預設路由），讓 Prisma Access 使用 eBGP 為遠端網路起始預設路由公告。確保您的網路沒有 BGP 公告的其他預設路由，否則可能會在您的網路中引入路由問題。
- （選用）選取 **Do Not Export Routes**（不匯出路由），防止 Prisma Access 將路由轉送到總部或資料中心。

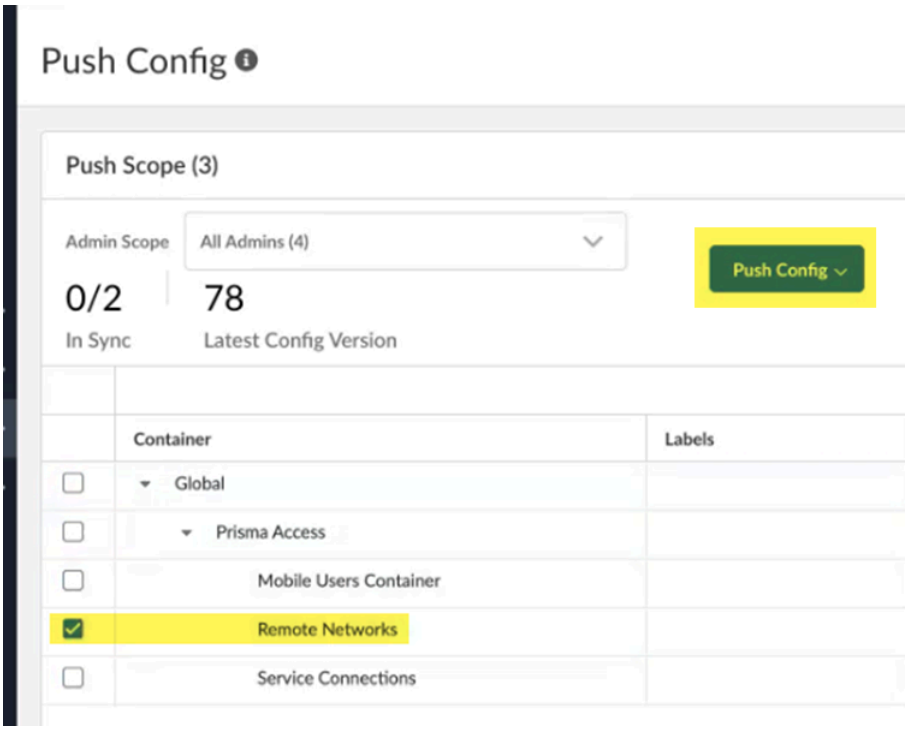
4. **Save**（儲存）您的 IPsec 通道變更。




**STEP 13 | Save & Exit**（儲存並結束）。

 ©2025 Palo Alto Networks, Inc.

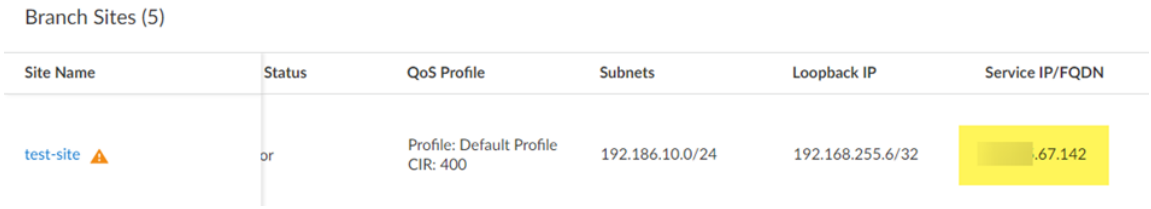
**STEP 14 |** **Push Config**（推送設定）以儲存您的設定變更，確保在 **Push Scope**（推送範圍）中選取 **Remote Networks**（遠端網路）。




**STEP 15 |** 尋找您在 CPE 上指定的 **Service IP**（服務 **IP**）位址。

當您設定遠端網路時，請使用服務 IP 位址作為您 CPE 上的對等 IP 位址，以終止 IPSec 通道。

1. 前往 **Workflows**（工作流程） > **Prisma SASE Setup**（**Prisma SASE** 設定） > **Branch Site Management**（分支網站管理） > **Extended CPE Site**（延伸 **CPE** 網站）。
2. 尋找 **Service IP/FQDN**（服務 **IP/FQDN**）位址。




# Panorama

設定遠端網路—高效能的步驟與在 Prisma Access (Managed by Panorama) 中裝載標準遠端網路相同，包括在裝載期間選擇 **IPSec Termination Node**（**IPsec** 終端節點)。

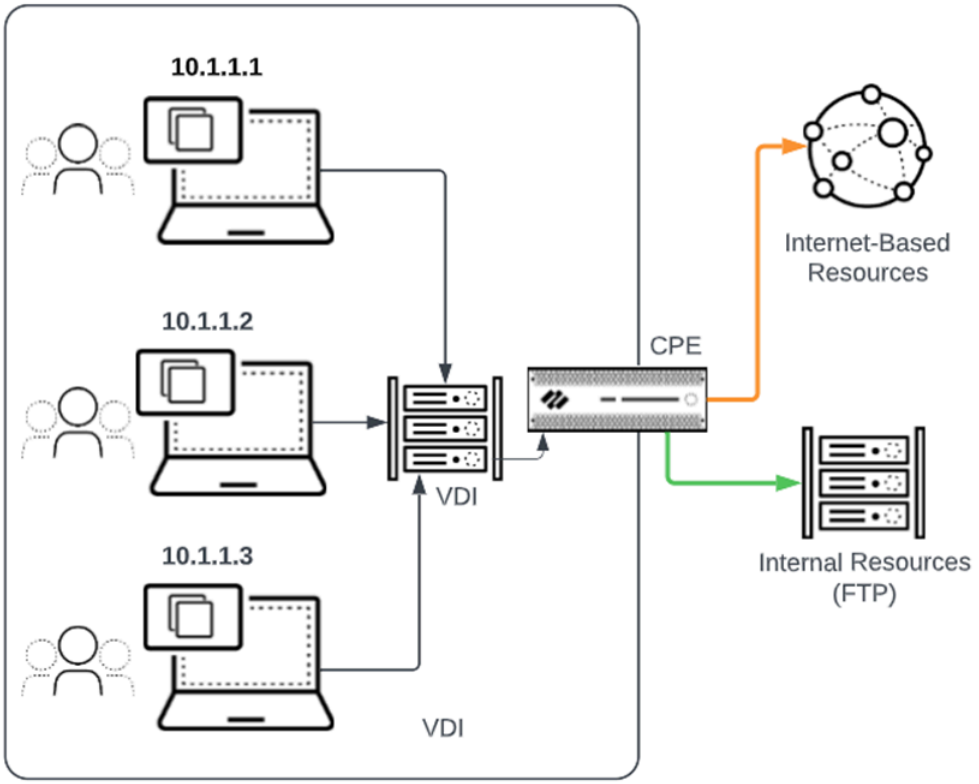

©2025 Palo Alto Networks, Inc.

# 使用終端伺服器整合共用桌面 VDI 與 Prisma Access

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 授權 |

虛擬桌面基礎結構 (VDI) 是一種使用虛擬機器來佈建和管理虛擬桌面的技術。VDI 使用受管理伺服器部署桌面環境，並根據要求將其部署至一般使用者。一般使用者從其佈建的 VDI 桌面存取所需的資源，例如基於網際網路的公用應用程式和資源，或可透過 FTP 連線取得的私人應用程式和資源。

VDI 拓樸可以使用共用桌面或專用桌面加以實作。如果桌面是共用的，則多個使用者位在單一 IP 位址後面，且連接埠用來區分用戶。




如果您的 VDI 部署使用共用桌面實作，Prisma Access 會提供一個解決方案，允許一般使用者使用單一登入安全地存取網際網路和 FTP 資源，同時保護您組織的 VDI 使用者，以及內部和外部資源。此解決方案使用您 安裝在 VDI 伺服器上的 Palo Alto Networks TS 代理程式。

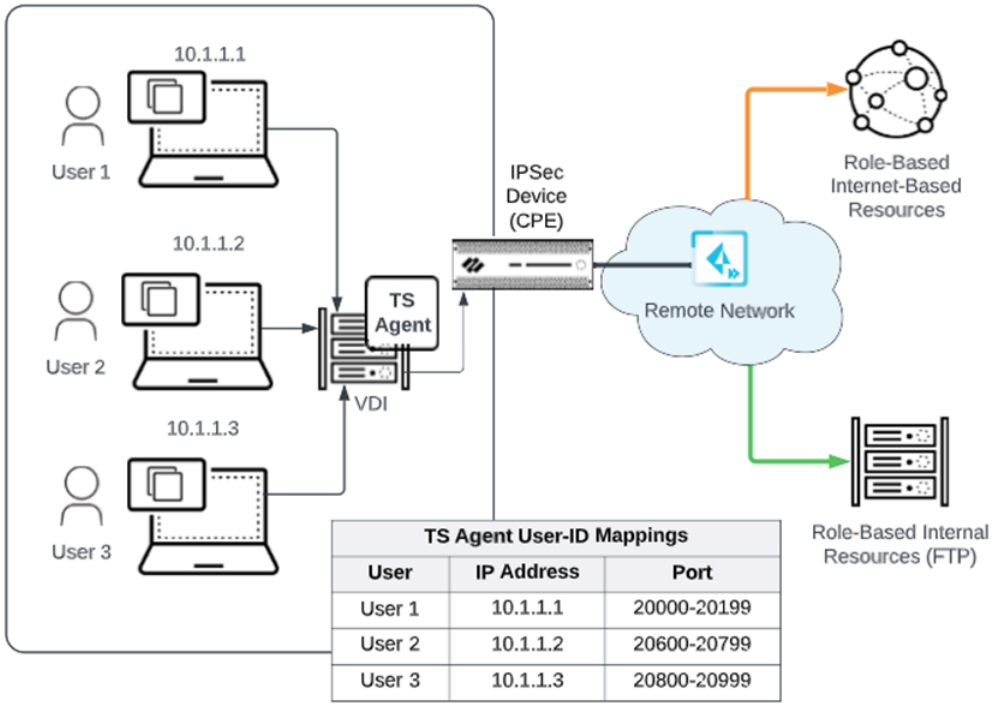
TS 代理程式是一種 User-ID 軟體，其安裝用來解決與使用者共用 IP 位址時識別使用者名稱到 IP 位址對應相關聯的挑戰。在安裝 TS 代理程式之後，所有登入的使用者都會受到監控，並為個別使用者指派一組特定的連接埠。當 Prisma Access 從 VDI 接收此 VDI 網路流量時，它會根據使用者的來源連接埠識別使用者。此部署為您提供了雲端型解決方案，允許管理員為 VDI 一般使用者建立安全性政策規則，以控制其對網際網路和內部網站的存取。


©2025 Palo Alto Networks, Inc.

如果您的網路有預設路由，您可以裝載一個或多個遠端網路並實作 TS 代理程式，以輕鬆簡單地保護您組織中的使用者和資源。

在此部署中：

- 您會在 TS 代理程式上指定連接埠範圍，以識別 Windows 型終端伺服器上的特定使用者。TS 代理程式會向 Prisma Access 指出已配置的連接埠範圍，以便 Prisma Access 可以根據使用者和使用者群組強制執行政策。
- 遠端網路會對 FTP 和網際網路型資源強制執行安全性和存取控制。




| TS Agent User-ID Mappings | | |
|---|---|---|
| User | IP Address | Port |
| User 1 | 10.1.1.1 | 20000-20199 |
| User 2 | 10.1.1.2 | 20600-20799 |
| User 3 | 10.1.1.3 | 20800-20999 |

您無法重新散佈從 *TS* 代理程式收集的使用者對應資訊。

若要整合使用 TS 代理程式的 VDI 與 Cloud Managed Prisma Access 中的 Prisma Access 遠端網路，請完成以下步驟。

**STEP 1 |** 在 VDI 伺服器上安裝並設定 Palo Alto Networks TS 代理程式。

若要對應所有使用者，您必須在使用者登入的所有終端機伺服器上安裝 TS 代理程式。

1. 在 VDI Windows 伺服器上，安裝並設定 Palo Alto Networks 終端伺服器 (TS) 代理程式。
2. 定義 TS 代理程式配置給一般使用者的連接埠範圍。

   從相容性矩陣中驗證 *TS* 代理程式支援的規模計數。

3. （選用）如果有多部 VDI 伺服器，請在每部上設定一個TS 代理程式。

**STEP 2 |** 裝載遠端網路並將其連線至 Cloud Managed Prisma Access 中的 VDI 分支網站（如果您還沒有這樣做）。


©2025 Palo Alto Networks, Inc.

**STEP 3 |** 在分支的 IPSec 裝置 (CPE) 上設定選項，以允許遠端網路與 VDI 通訊。

- 為 IPSec 通道設定與您在 Prisma Access 中所設定參數相符的 IPSec 和 IKE 密碼參數。
- 使用 **Service IP**（服務 **IP**）位址（**Manage**（管理） > **Remote Networks**（遠端網路） > **Service IP**（服務 **IP**））作為遠端網路 IPSec 通道的 Prisma Access 端。
- 在 IPSec 裝置上設定路由，以允許 VDI 流量流到遠端網路通道。
- 在 IPSec 裝置上設定路由，以允許遠端網路流量透過通道流到 TS 代理程式。
- 如果需要，請在 IPSec 裝置上設定安全性政策，允許流量通過通道。

**STEP 4 |** 設定 TS 代理程式以允許遠端網路中的使用者對應。

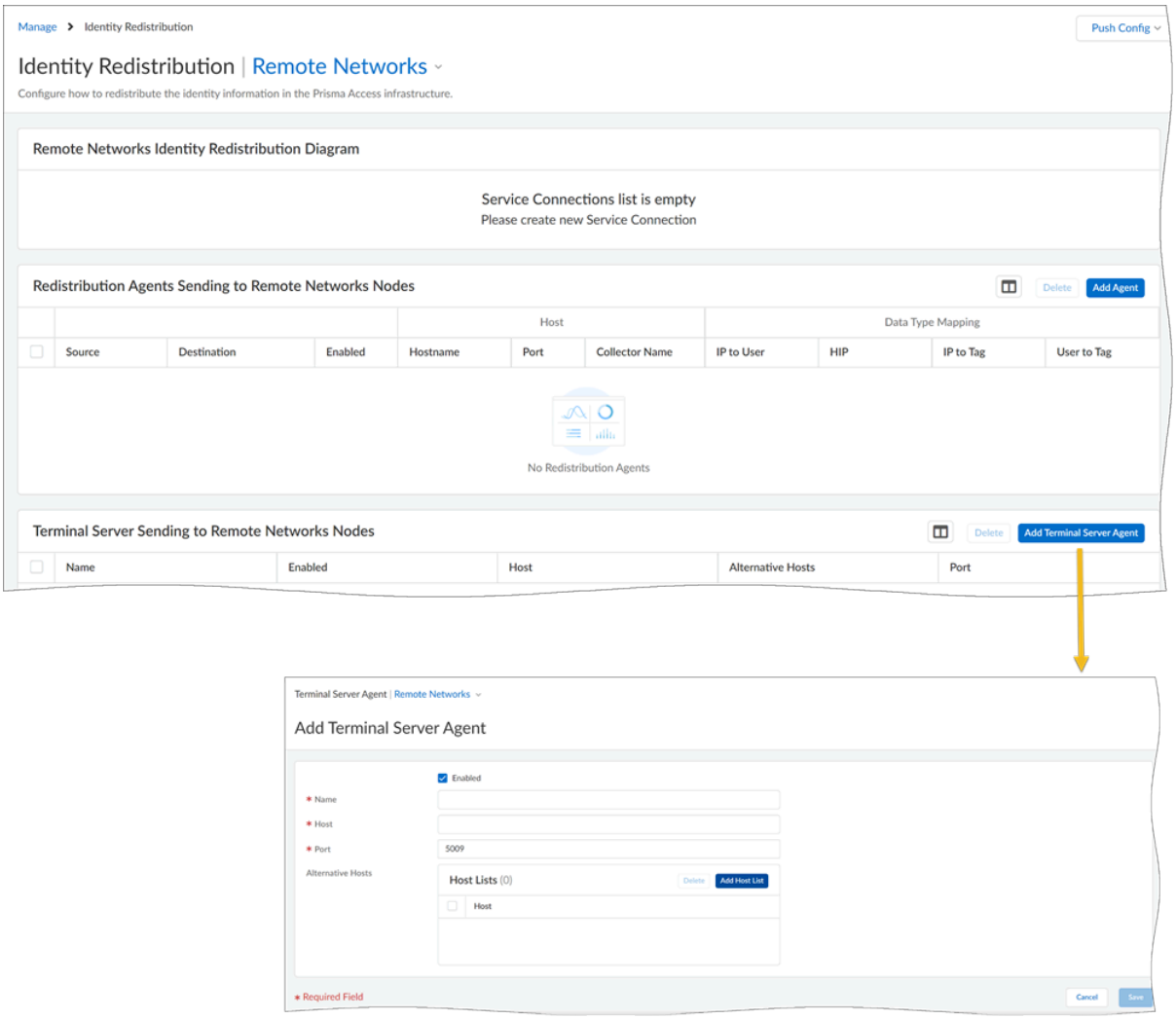
前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Identity Services**（識別服務） > **Identity Redistribution**（識別重新散

 ©2025 Palo Alto Networks, Inc.

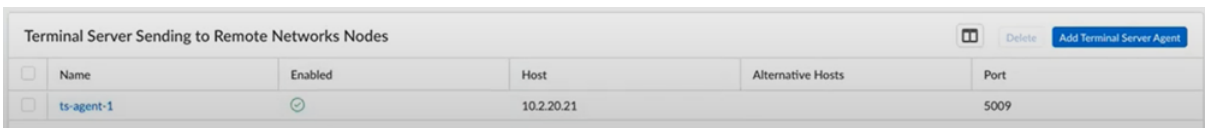
佈）、將 **Configuration Scope**（設定範圍）設定為 **Remote Networks**（遠端網絡），然後 **Add Terminal Server Agent**（新增終端伺服器代理程式）。

- 確保該代理程式 **Enabled**（已啟用）。
- 輸入 TS 代理程式的名稱。
- 輸入安裝 TS 代理程式之 Windows 主機的 IP 位址。
- 輸入代理程式用來接聽使用者識別要求的連接埠號碼。

  此連接埠預設為 5009。
- **Save**（儲存）變更。




以下範例已設定主機位址為 10.2.20.21 和連接埠為 5009 的代理程式。



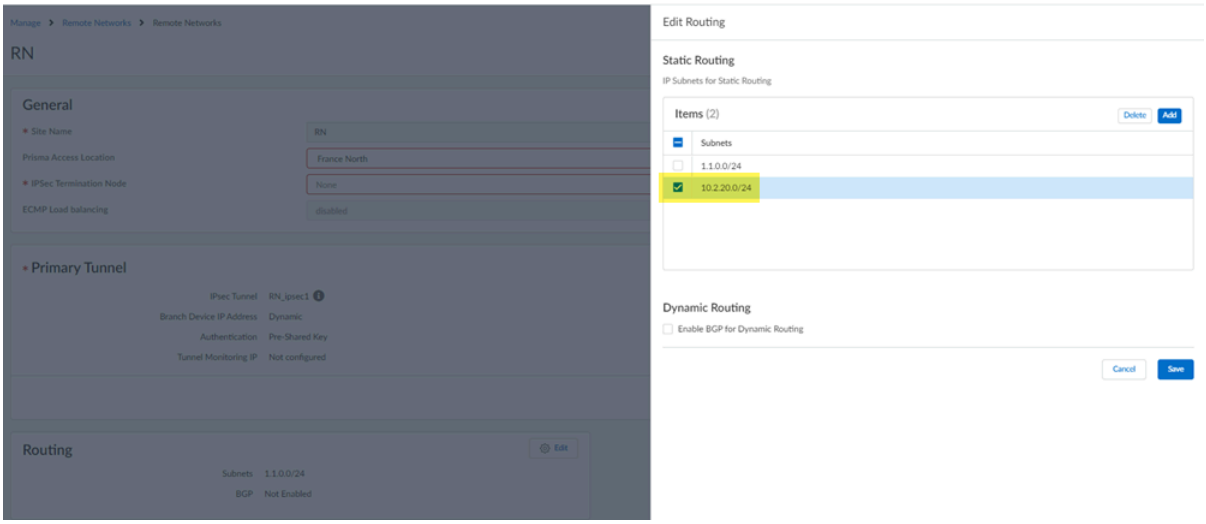


©2025 Palo Alto Networks, Inc.

**STEP 5 |** 允許在 VDI 與 Prisma Access 遠端網路之間路由。

1. 前往 **Manage**（管理） > **Service Setup**（服務設定） > **emote Networks**（遠端網路） > ***remote-network-name*** > **Routing**（路由），並 **Add**（新增）路由至 VDI 子網路。

   新增此子網路允許 TS 代理程式與遠端網路進行通訊。在下列範例螢幕擷取畫面中，VDI 子網路為 10.2.20.0/24。




2. 前往 **Manage**（管理） > **Configuration**（設定） > **Security Services**（安全性服務） > **Security Policy**（安全性策略）、將範圍設定為 **Remote Networks**（遠端網絡），然後新

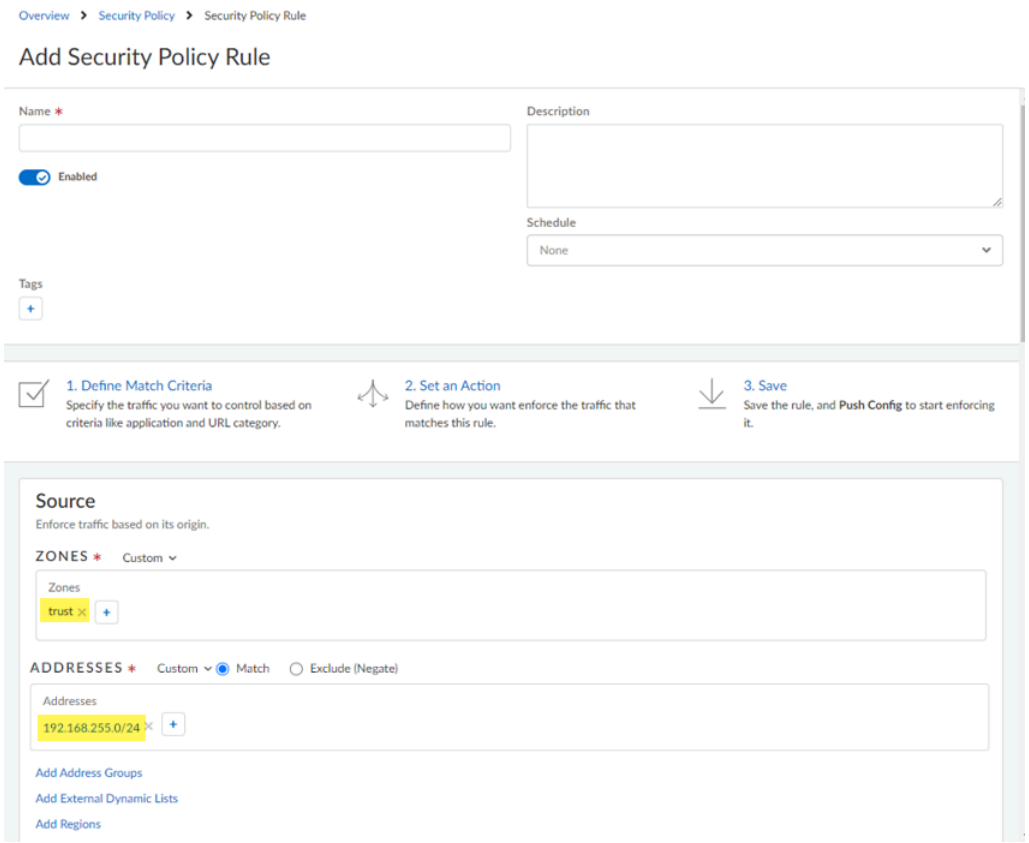
 ©2025 Palo Alto Networks, Inc.

增安全性政策規則（**Add Rule**（新增規則）），以允許 VDI 子網路與遠端網路之間的流量。

遠端網路中從 VDI 連線到 Prisma Access 的使用者會從 Prisma Access 基礎結構子網路獲指派一個 IP 位址，而且您必須允許基礎結構子網路與 VDI 子網路之間的路由。

- 確保該規則 **Enabled**（已啟用）。
- **Source**（來源）—設定以下參數：
  - **Zones**（區域）—設定為 **Trust**（信任）。
  - **Addresses**（位址）—為基礎結構子網路建立位址物件（**Manage**（管理） > **Shared**（共用） > **Infrastructure Settings**（基礎結構設定） > **Infrastructure Subnet**（基礎結構子網路）），並在這裡新增位址物件。

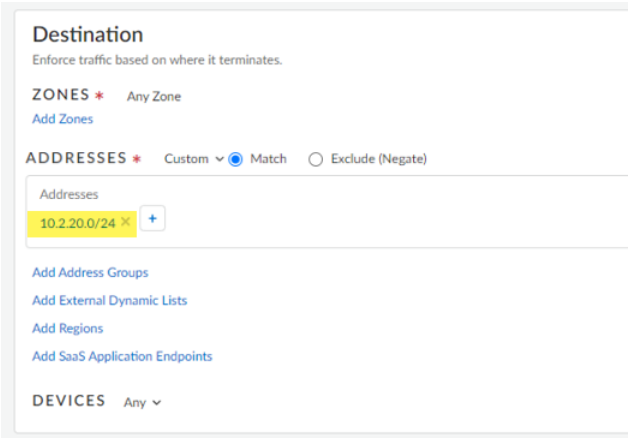
    位址物件優先於輸入實際基礎結構子網路，因為如果子網路變更，您可以變更位址物件，並且變更會套用到使用該位址物件的所有設定。



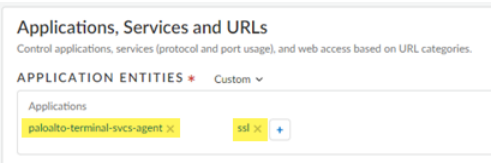

- **Destination**（目的地）—將正在執行 TS 代理程式的 VDI 主機新增至 **Addresses**（位址）。

  如果您已在多個 VDI 主機上設定 TS 代理程式，請在這裡新增它們全部。

 ©2025 Palo Alto Networks, Inc.



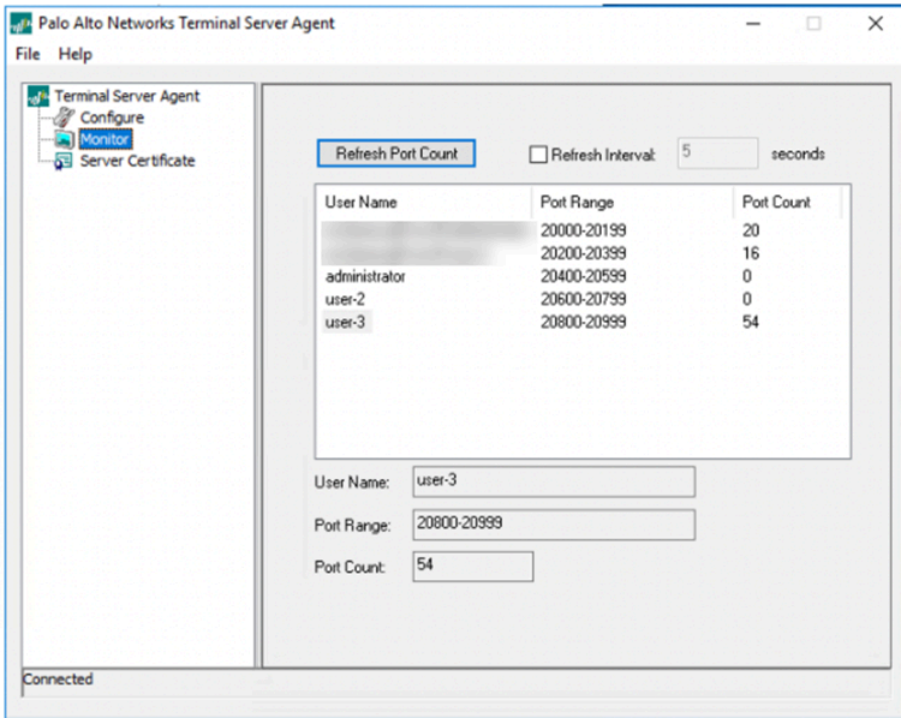

- **Applications, Services and URLs**（應用程式、服務和 **URL**）—將 **paloalto-terminal-svcs-agent** 新增至 **Application Entities**（應用程式實體）。



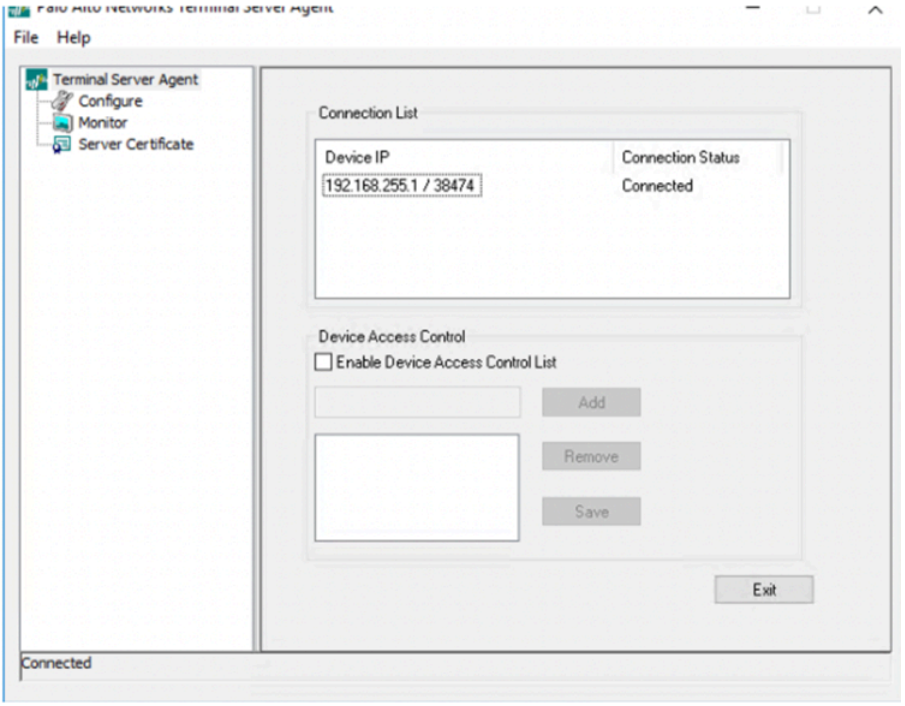

 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** 驗證實作是否正常運作。

1. 在 TS 代理程式中，**Monitor**（監控）代理程式的狀態，並驗證 TS 代理程式是否反映了正確的使用者名稱到連接埠對應。

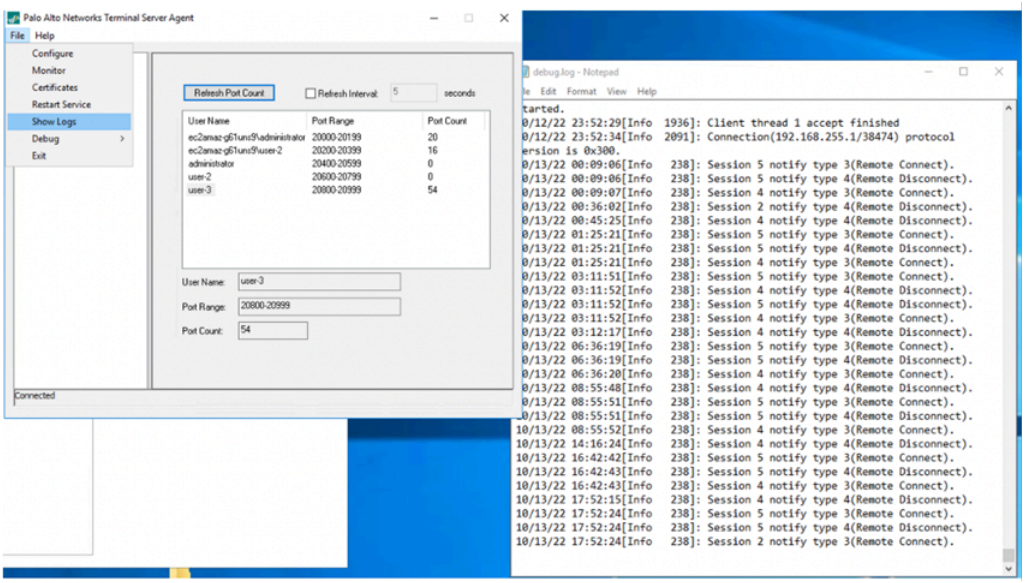



2. 驗證遠端網路的 IP 位址是否已連線至 TS 代理程式。

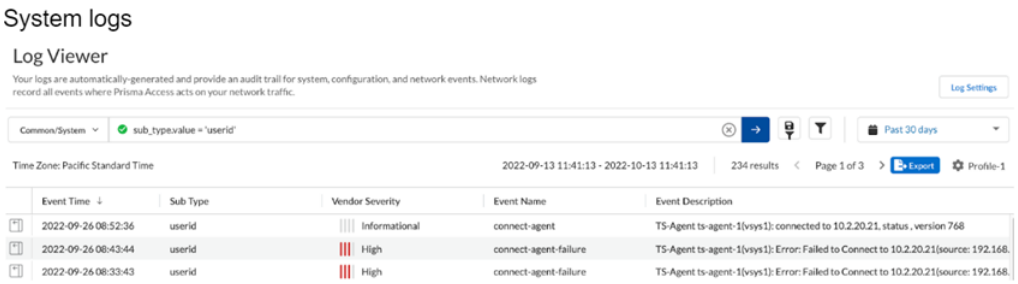



3. 前往 **File**（檔案） > **Show Logs**（顯示日誌），並檢視 TS 代理程式的日誌訊息。

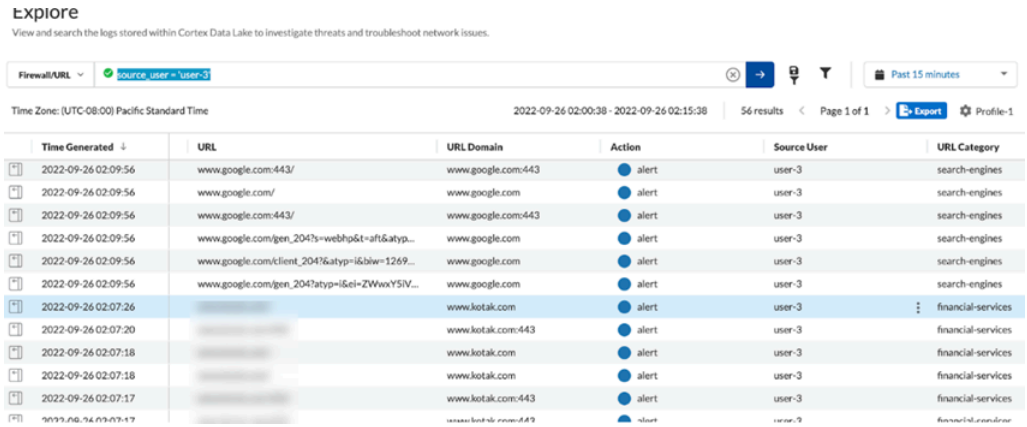

©2025 Palo Alto Networks, Inc.




4. 在 Prisma Access (Managed by Strata Cloud Manager) 中，前往 **Activity**（活動） > **Log Viewer**（日誌檢視器） > **Common/System**（通用/系統），並驗證遠端網路是否能夠連線到 TS 代理程式。




5. 前往 **Activity**（活動） > **Log Viewer**（日誌檢視器） > **Firewall/URL**（防火牆/**URL**），並驗證遠端網路是否能夠強制執行識別型政策。




 ©2025 Palo Alto Networks, Inc.

# Prisma Access 監控和可視性

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ 需要 ADEM Observability 授權才能存取 Autonomous DEM。 |

Prisma Access 提供以下功能，來洞察您的安全性活動並監控您的部署。這些功能透過日誌、跨遠端網路、服務連線、行動使用者和授權實體的警示通知，以及互動式儀表板提供對網路和使用者流量的可視性，全面檢視有關在您網路中運作的應用程式、威脅、使用者和安全性訂閱的資料。您也可以在 Strata Cloud Manager 中監控 Prisma Access。

- Prisma Access 日誌

  您的日誌是自動產生的，並提供系統、組態和網路事件的稽核線索。網路日誌會記錄 Prisma Access 在其中對您網路流量採取行動的所有事件。例如，當 Prisma Access 根據安全性規則封鎖流量、根據驗證規則授與使用者存取權，或根據 QoS 規則塑造流量。您可以在 Strata Cloud Manager 和 Panorama 管理介面中檢視 Prisma Access 日誌。
- Prisma Access 活動儀表板和報告

  活動為您提供了網路中發生什麼情況的全面檢視，從日誌資料到您可以用來通知政策更新的關鍵結果，並關上企業安全性與使用者生產力缺口。
- 在 Strata Cloud Manager 中監控 Prisma Access
- 使用 Strata Cloud Manager 的 Monitor（監控）和 Workflows（工作流程）區段，全面了解您的網路流量以及您正在管理的產品和訂閱。
- Prisma Access 和自發 DEM

  Autonomous DEM 為 Secure Access Service Edge (Strata Cloud Manager) 中的所有使用者流量提供原生端對端可視性和洞察。Autonomous DEM 功能原生整合到 GlobalProtect 應用程式和 Prisma Access，因此不需要您部署任何額外的設備或代理程式。您可以快速隔離數位體驗問題的根源，並簡化修復過程。
- Strata Cloud Manager 控管中心

  控管中心是 IoT 裝置、使用者、主機，以及您網路上流量的互動式視覺化摘要。利用來自雲端交付安全性和 ADEM 訂閱的資料，控管中心可以公開有關網路上資料的威脅、使用者體驗和安全性的重要資訊。

  控管中心可讓您與資料互動並視覺化網路事件之間的關係，以發現異常狀況或增強網路安全性的方法。

# Prisma Access 日誌

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

日誌是一個自動產生、帶時間戳記的檔案，為 Prisma Access 監控的系統事件或網路流量事件提供稽核線索。日誌項目包含構件，即與記錄事件關聯的屬性、活動或行為，例如應用程式類型或攻擊者的 IP 位址。每種日誌類型會記錄單獨事件類型的資訊。例如，Prisma Access 可能會產生威脅日誌，以記錄與間諜軟體、弱點或病毒特徵碼相符的流量。Prisma Access (Managed by Strata Cloud Manager) 會提供網路日誌（例如流量、威脅、URL、檔案、HIP 比對）、端點日誌和常用日誌（系統和設定）。您可以檢視每個日誌項目的詳細資訊，並且對於威脅日誌，您可以檢閱威脅詳細資訊，並查看是否存在任何威脅覆寫。

- Strata Cloud Manager
- Panorama

## Prisma Access 日誌 (Strata Cloud Manager)

如果您是使用 **Strata Cloud Manager**，請前往 **Incidents & Alerts**（事件與警示） > **Log Viewer**（日誌檢視器）。

Prisma Access (Managed by Strata Cloud Manager) 會提供網路日誌（流量、威脅、URL、檔案、HIP 比對）和通用日誌（系統和設定）。

您可以檢視每個日誌項目以及威脅日誌的詳細資訊，您也可以檢閱威脅詳細資訊，並查看是否有任何威脅覆寫到位。進一步瞭解。

## Prisma Access 日誌 (Panorama)

您也可以檢視 Prisma Access (Managed by Panorama) 介面中的 Prisma Access 日誌。Prisma Access 基礎結構會將所有日誌轉送到 Strata Logging Service。Prisma Access 會使用雲端服務外掛程式從 Strata Logging Service 中擷取日誌結果，並提供遠端網路和行動使用者流量日誌的彙總檢視。無論您用於 Prisma Access 的管理介面為何—Panorama或Strata Cloud Manager—您可以在 **Activity**（活動） > **Logs**（日誌） > **Log Viewer**（日誌檢視器）下檢視 Prisma Access (Managed by Strata Cloud Manager) 中您的日誌。

除了來自 Prisma Access 雲端服務基礎結構的日誌外，您還可以直接從管理 Prisma Access 的 Panorama 設備檢視日誌。若要檢視日誌，請前往 **Monitor**（監控） > **Logs**（日誌）。進一步瞭解。


©2025 Palo Alto Networks, Inc.

# 外部日誌和其他資料

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

您可能已經習慣了從 **Activity**（活動） > **Logs**（日誌）中檢視 Strata Logging Service 中儲存的 Prisma Access 日誌，以及與這些日誌互動。但是，您知道嗎，當您具有 Cortex XDR Pro per TB 授權資料湖時，Prisma Access 還支援從各種外部第三方來源擷取日誌和其他資料？一旦完成設定，您就可以使用中樞上的 Strata Logging Service 應用程式，檢視日誌並設定日誌轉送。支援的廠商包括：

| | | |
| --- | --- | --- |
| • 啟動 Windows 事件收集器 | • Corelight Zeek | • PAN IoT Security |
| • Amazon S3 | • ElasticSearch Filebeat | • PingFederate |
| • Apache Kafka | • Forcepoint DLP | • PingOne for Enterprise |
| • AWS | • Fortinet Fortigate | • Prisma Cloud |
| • AWS CloudTrail 和 Amazon CloudWatch | • Google Cloud Platform | • Prisma Cloud Compute |
| • Azure Event Hub | • Google Kubernetes Engine | • Proofpoint Targeted Attack Protection |
| • Azure Network Watcher | • Google Workspace | • ServiceNow CMDB |
| • BeyondTrust Privilege Management Cloud | • Microsoft Azure | • 使用 Elasticsearch Filebeat 的 Windows DHCP |
| • Check Point FW1/VPN1 | • Microsoft Office 365 | • Workday |
| • Cisco ASA | • Okta | • Zscaler 雲端防火牆 |

您可以將從第三方來源擷取的日誌用作唯一的資料來源，也可以使用這些日誌搭配 Palo Alto Networks Prisma Access 日誌和其他資料來源。

使用 Palo Alto Networks，透過收集、整合和標準化來自所有資料來源（網路、端點和雲端）的資料，減輕您的營運負擔並從根本上簡化您的 SOC 營運。獲取整個企業應用程式使用情況、流量模式、威脅和事件的統一檢視和可操作見解。


©2025 Palo Alto Networks, Inc.

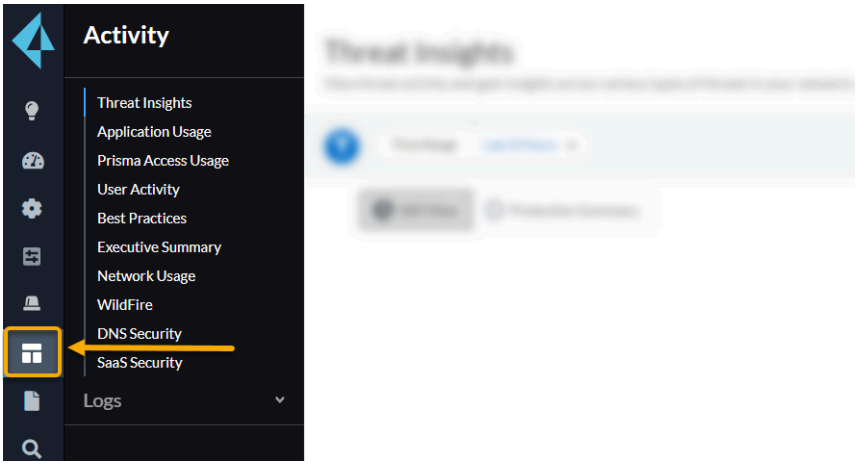
# Prisma Access 活動儀表板和報告

| 這可在何處使用？ | 我需要什麼？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Panorama Managed Prisma Access | ❑ Prisma Access 授權<br>❑ 檢閱活動儀表板和報告的授證和其他需求 |

活動識別了您可以用來通知政策更新並縮小企業安全性與使用者生產力差距的關鍵結果。活動為您提供：

- 互動式儀表板，您可以在其中探索網路中正在運作的應用程式、威脅、使用者和安全性訂閱的資料。
- 您可以離線共用並排程定期更新的報告。
- 日誌檢視器提供系統、設定和網路事件的稽核追蹤。您可以從儀表板跳到日誌檢視器，以取得更多內容並深入了解資料。
- 搜尋安全性構件可協助您搜尋檔案雜湊、URL、網域或 IP 位址（IPv4 或 IPv6）等構件，以僅與該構件的資料互動。搜尋結果包括構件的歷程記錄、構件的威脅情報，以及構件的第三方分析結果。

Prisma Access (Managed by Strata Cloud Manager) 和 Panorama Managed Prisma Access 使用者可以使用 Prisma Access (Managed by Strata Cloud Manager) 應用程式中的 **Activity**（活動）。首先，啟動 Prisma Access (Managed by Strata Cloud Manager)，然後按一下左側導覽窗格中的 **Activity**（活動） 頁籤。




支援洞察作為 Prisma SASE FedRAMP 高「進行中」認證的一部分。支援活動作為 Prisma SASE FedRAMP 高「進行中」認證的一部分。

- 開始使用活動


©2025 Palo Alto Networks, Inc.

# 在 Strata Cloud Manager 中檢視並監控 Prisma Access

| 這可在何處使用？ | 我需要什麼？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ 這是 Prisma Access 洞察功能。 |

Palo Alto Networks Strata Cloud Manager 控管中心是一個採用 AI 技術的網路安全性平台。透過 Strata Cloud Manager 和 Strata Cloud Manager 控管中心，您可以從單一簡化的使用者介面輕鬆管理 Palo Alto Networks 網路安全性基礎結構。

您可以使用控管中心的 Activity Insights（活動洞察），以及控管中心的 Monitor（監控）和 Workflows（工作流程）區段，全面了解網路流量以及您正在管理的產品和訂閱。

- **View and Monitor Applications**（檢視並監控應用程式）—前往 **Activity Insights**（活動洞察）> **Applications**（應用程式），以取得您正在使用的應用程式的相關資訊。
- **View and Monitor App Acceleration**（檢視並監控應用程式加速）—應用程式加速可處理應用程式效能不佳的原因，並即時採取行動來緩解這些原因，從而改善 Prisma Access GlobalProtect 和遠端網路使用者的使用者體驗。前往 **Activity Insights**（活動洞察）> **Applications**（應用程式），以檢視有關所有加速應用程式的詳細資訊。
- **View Mobile Users**（檢視行動使用者）—所有使用者提供連線到 Palo Alto Networks 安全性解決方案的所有使用者的概要，這些解決方案包括新世代防火牆 (NGFW) 和 Prisma Access。您可以輕鬆確定使用者與 NGFW 或 Prisma Access 的連線狀態，無論是在分支網站、服務連線，還是遠端位置。前往 **Activity Insights**（活動洞察）> **Insights**（洞察）> **Users**（使用者），以檢視 Prisma Access **Agent Users**（代理程式使用者）、**Agentless Proxy Users**（無代理程式 **Proxy** 使用者）、**Office Users**（辦公室使用者）和 **Other Users**（其他使用者）的相關資訊
- **View and Monitor Branch Sites**（檢視並監控分支網站）—前往 **Monitor**（監控）> **Branch Sites**（分支網站）> **Prisma Access**，以檢視遠端網路的健康情況與連線，以及部署在不同 Prisma Access 位置的所有遠端網路的使用情況。您將會看到即時連線狀態和頻寬消耗詳細資訊，以及其他部署詳細資訊。行動使用者、分公司和零售地點連線至遠端網路。您也可以檢視在「遠端網路」和「行動使用者」中設定之通道的健康情況。
- **View and Monitor Data Centers**（檢視並監控資料中心）—前往 **Monitor**（監控）> **Data Centers**（資料中心）> **Service Connections**（服務連線），以查看彙總的服務連線資料以及個別服務連線的相關資訊。

  前往 **Monitor**（監控）> **Data Centers**（資料中心）> **ZTNA Connectors**（**ZTNA** 連接器），以檢視 ZTNA 連接器群組和個別 ZTNA 連接器的健康情況和狀態。
- 前往 **Monitor**（監控）> **Data Centers**（資料中心）> **ZTNA Access Objects**（**ZTNA** 存取物件），以了解您的 ZTNA 連接器存取物件。
- **View and Monitor Network Services**（檢視並監控網路服務）—前往 **Monitor**（監控）> **Network Services**（網路服務）> **GlobalProtect Authentication**（**GlobalProtect** 驗證），以檢視影響使用者存取應用程式體驗的常見網路服務的效能。網路服務包括報告 GlobalProtect 驗證成功和失敗的次數，作為行動使用者能夠連線至 Prisma Access 的衡量標準。前往 **Monitor**（監

 ©2025 Palo Alto Networks, Inc.

控） > **Network Services**（網路服務） > **DNS**，以檢視在您指定的時間範圍內轉送至伺服器的 DNS Proxy 要求和回應。

- **View and Monitor Subscription Usage**（檢視並監控訂閱使用情況）—選取 **Monitor**（監控） > **Subscription Usage**（訂閱使用情況），以檢視有關 **Prisma Access Base Subscriptions**（**Prisma Access** 基礎訂閱）的詳細資訊，包括您迄今為止已消耗的授權數量。
- **View and Monitor Prisma Access Locations**（檢視並監控 **Prisma Access**位置）—前往 **Monitor**（監控） > **Prisma Access Locations**（**Prisma Access** 位置），以檢視遠端網路和行動使用者的所有 Prisma Access 位置的健康情況概,要。您可以選取時間範圍來檢視該時間期間的 Prisma Access 位置狀態和 Strata Logging Service 連線、檢視列出所有 Prisma Access 位置的表格，並依名稱選取個別 Prisma Access 以檢視其詳細資訊。
- **View Prisma Access Upgrades**（檢視 **Prisma Access** 升級）—選取 **Workflows**（工作流程） > **Software Upgrades**（軟體升級） > **Prisma Access**，以檢視 Prisma Access 升級程序的相關資訊。
- **View and Monitor Third-Party Device-IDs**（檢視並監控第三方 **Device-ID**）—前往 **Monitor**（監控） > **Devices**（裝置） > **IOT**，洞察您的 IoT 裝置，例如過去 30 分鐘內連線的 IoT 裝置數目、所選時間範圍期間連線的所有 IoT 裝置，以及有關所有連線 IoT 裝置的詳細資訊。
- **View and Monitor Remote Browser Isolation**（檢視並監控遠端瀏覽器隔離）—選取 **Monitor**（監控） > **Users**（使用者），透過檢視作用中 RBI 使用者數目、趨勢、連線狀態、RBI 位置狀態、流量測量和授權消耗等指標來了解您的 RBI 部署。

# 開始在 Strata Cloud Manager 中使用 Prisma Access 監控

| 這可在何處使用？ | 我需要什麼？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ 這是 Prisma Access Insights 功能。 |

Prisma Access 為您提供了一種在 Strata Cloud Manager 控管中心持續監控 Prisma Access 環境的方式。多個儀表板可讓您集中檢視不同的部署、警示和 Prisma Access 基礎結構。當事件或狀態需要您注意時，Prisma Access 向您傳送警示通知，以便您可以快速查明可以修復的問題。它還能夠讓您瞭解 Prisma Access 團隊正在努力的修復。您可以透過選取或設定時間範圍來篩選要查看的資料，並在 [Monitor（監控）] 頁面中使用 Autonomous DEM 授權檢視基準線資訊。

## 時間範圍選取篩選器

**Time Range**（時間範圍）選取篩選器出現在儀表板頂部，您想要在其中依時間範圍篩選資訊。

該時間已本地化的，因此您可以根據您所在地區的當地時間進行篩選。每分鐘擷取一次資料，但大多數直方圖中顯示的資料點會根據選取的 **Time Range**（時間範圍）而有所不同。

為了您的方便，Prisma Access 讓你從幾個預先定義的範圍挑擇 **Time Range**（時間範圍），或設定您自己的日期和時間範圍：

 ©2025 Palo Alto Networks, Inc.

- 過去 **15** 分鐘

  每 3 分鐘 1 個資料點，總共 5 個資料點。
- 過去 **1** 小時

  每 3 分鐘 1 個資料點，總共 20 個資料點。
- 過去 **3** 小時

  每 3 分鐘 1 個資料點，總共 60 個資料點。
- 過去 **24** 小時

  每 5 分鐘 1 個資料點，總共 288 個資料點。
- 前 **7** 天

  每 30 分鐘 1 個資料點，總共 336 個資料點。
- 過去 **30** 天

  每 3 小時 1 個資料點，總共 180 個資料點。
- 自訂

  除了可在篩選器選取的預先填入 **Time Range**（時間範圍）外，您可以設定自訂時間間隔（例如，從 6 月 1 日下午 5 點開始，於 6 月 2 日下午 4 點結束的日期和時間範例）。

  若要設定開始時間，首先在日曆中選取日期，然後在 **Start**（開始）下選取時間。**Apply**（套用）開始時間，然後在日曆中選取結束日期，並在 **End**（結束）下選取時間，來設定結束時間。

  一旦您設定了自訂時間範圍，它就會加以保存，並套用至洞察內使用時間範圍篩選器來顯示資料而不是即時資料的所有 Widget。

  您可以針對自訂時間間隔從預先填入的 **Time Range**（時間範圍）選取項目進行挑選：

  - 過去 **15** 分鐘

    每 3 分鐘 1 個資料點，總共 5 個資料點。
  - 過去 **1** 小時

    每 3 分鐘 1 個資料點，總共 20 個資料點。
  - 過去 **3** 小時

    每 3 分鐘 1 個資料點，總共 60 個資料點。
  - 過去 **24** 小時

    每 5 分鐘 1 個資料點，總共 288 個資料點。
  - 過去 **48** 小時

    每 30 分鐘 1 個資料點，總共 96 個資料點。
  - 前 **7** 天

    每 30 分鐘 1 個資料點，總共 336 個資料點。
  - 過去 **30** 天

    每 3 小時 1 個資料點，總共 240 個資料點。

 ©2025 Palo Alto Networks, Inc.

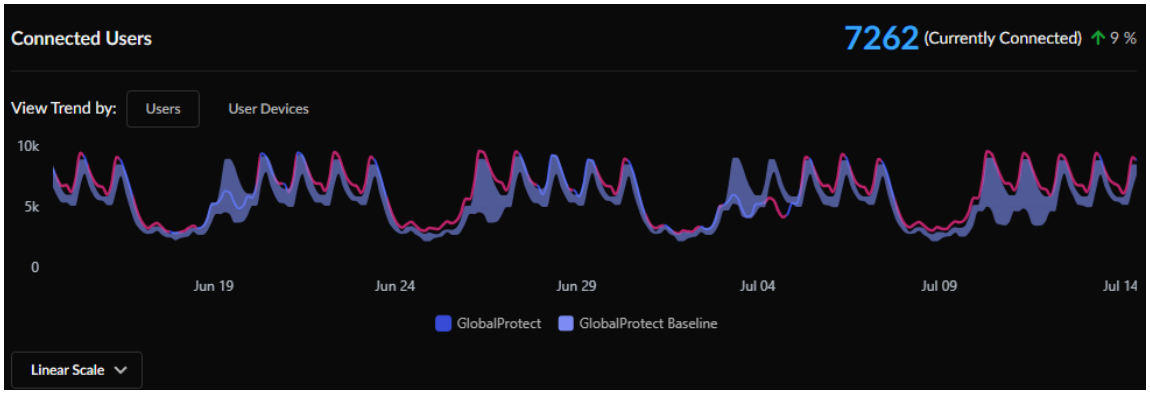
### Widget 中的基準線

如果購買了 AI-Powered ADEM 授權，您會在以下 [Monitor（監控）] 頁面上看到整個趨勢 Widget 的基準線資料帶：使用者、分支網站、資料中心和網路服務。Widget 會在整個趨勢線的背景中顯示基準線。這可讓您一目了然地檢視資料是否已越過基準線的上限或下限。

基準線資料是以 1 小時 Bin 大小計算的，並考慮了過去 28 天的資料，這些資料來自特定通道、網站、Prisma Access 位置或 GlobalProtect 使用者計數的那些一小時 Bin。例如，從星期二下午 1 點到下午 2 點的基準線是根據前四個星期二下午 1 點到下午 2 點時間範圍計算得出的。下限是所收集歷程資料的第 10 個百分位數，上限是其第 90 個百分位數。這可讓您查看頻寬、使用者計數、驗證計數，以及 DNS Proxy 要求和回應的趨勢。因為基準線資料取自過去 28 天的歷程資料，所以新裝載的租用戶需要持續 28 天的資料，才能正確算出基準線。如果您的資料少於 28 天，您可能會看到一些差異。

當 Widget 中趨勢線的值偏離基準線的上限或下限時，該期間的趨勢線會以紅色出現在網頁介面中。

以下範例顯示了來自 [Users（使用者）] 頁面上 **Connected User**（已連線使用者）Widget 的 GlobalProtect 基準線。




## 檢視並監控應用程式

| 這可在何處使用？ | 我需要什麼？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ 這是 Prisma Access Insights 功能。 |

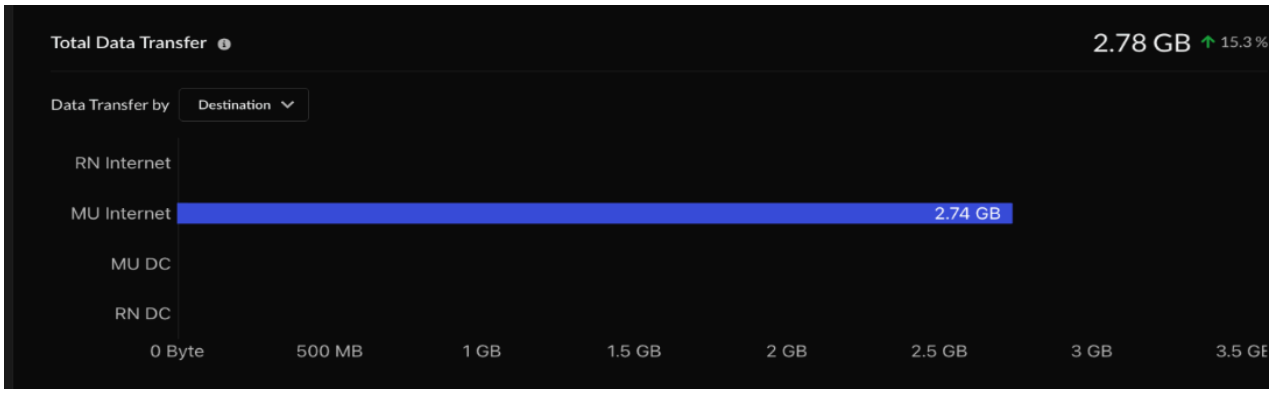
使用 Strata Cloud Manager 控管中心，來監控您網路中的 Prisma Access 應用程式、使用該應用程式的使用者，以及其潛在的安全性影響。前往 **Insights**（洞察） > **Applications**（應用程式），以獲取 Prisma Access 應用程式的可視性，以及有關威脅、使用者、資料傳輸、風險評分和應用程式使用者體驗的資訊。

### 總資料傳輸量

**Total Data Transfer**（總資料傳輸量）為您顯示在所選時間範圍內跨 Prisma Access 防火牆的總資料傳輸量。使用 **Add Filter**（新增篩選器）下拉式清單以取得其他篩選選項。在範例中，您會看到

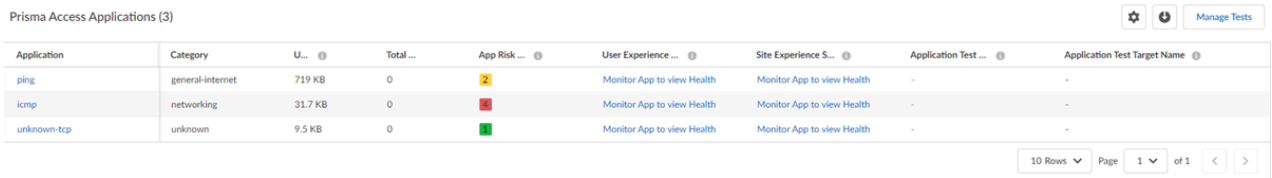
 ©2025 Palo Alto Networks, Inc.

依 **Application Category**（應用程式類別）劃分的資料傳輸，其中顯示了熱門應用程式，以及這些應用程式的總資料傳輸量。您也可以依 **Destination**（目的地）檢視總資料傳輸量。




## Prisma Access 應用程式

使用此 Widget 查看哪些應用程式正監控，同時其上正在執行綜合測試。表格中也顯示其體驗分數，這可以讓您得知每個應用程式的健康情況。按一下 **Manage Tests**（管理測試）按鈕，以檢視已為應用程式測試表格中您的所有應用程式設定的所有綜合測試。




| 欄 | 說明 |
|---|---|
| 應用程式 | 受監控應用程式的應用程式 ID。 |
| 類別 | 應用程式類型。 |
| 使用方式 | Prisma Access 基礎結構中偵測到流向特定應用程式的總流量。 |
| 威脅總數 | 應用程式遭遇的威脅總數。 |
| 應用程式風險分數 | 此特定應用程式的威脅資料。1 是最低風險，5 是最高風險。 |
| 使用者體驗 | Autonomous DEM 收集的應用程式體驗分數。它是針對此應用程式所有受監控使用者彙總的。 |
| 網站體驗分數 | 此特定分支網站的應用程式體驗分數。 |
| 應用程式測試名稱 | 使用者為此應用程式設定的測試名稱。 |


©2025 Palo Alto Networks, Inc.

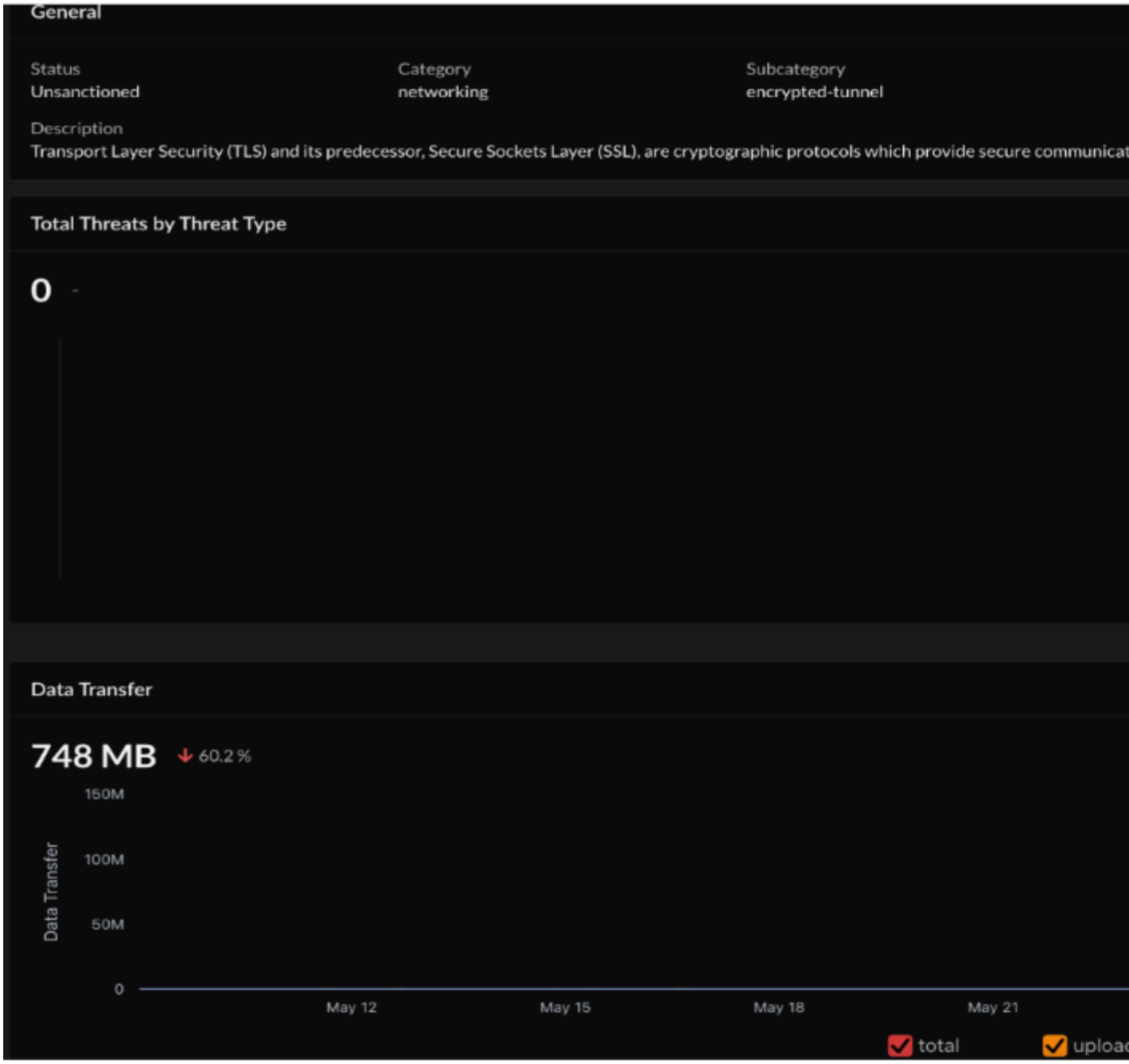
| 欄 | 說明 |
| --- | --- |
| 應用程式測試目標名稱 | 從各個端點針對綜合測試的 FQDN 的 IP 位址。 |

應用程式詳細資料

選取任何應用程式以檢視其 **General**（一般）詳細資訊，例如狀態、類別、子類別、連接埠、技術和風險分數。

- **Total Threats by Threat Type**（依威脅類型劃分的威脅總數）—應用程式的目前威脅。
- **Total Users**（使用者總數）—在指定的時間範圍內存取此應用程式的使用者總數。
- **Data Transfer**（資料傳輸）—查看已針對此應用程式上傳或下載的資料。


©2025 Palo Alto Networks, Inc.




# 檢視並監控應用程式加速

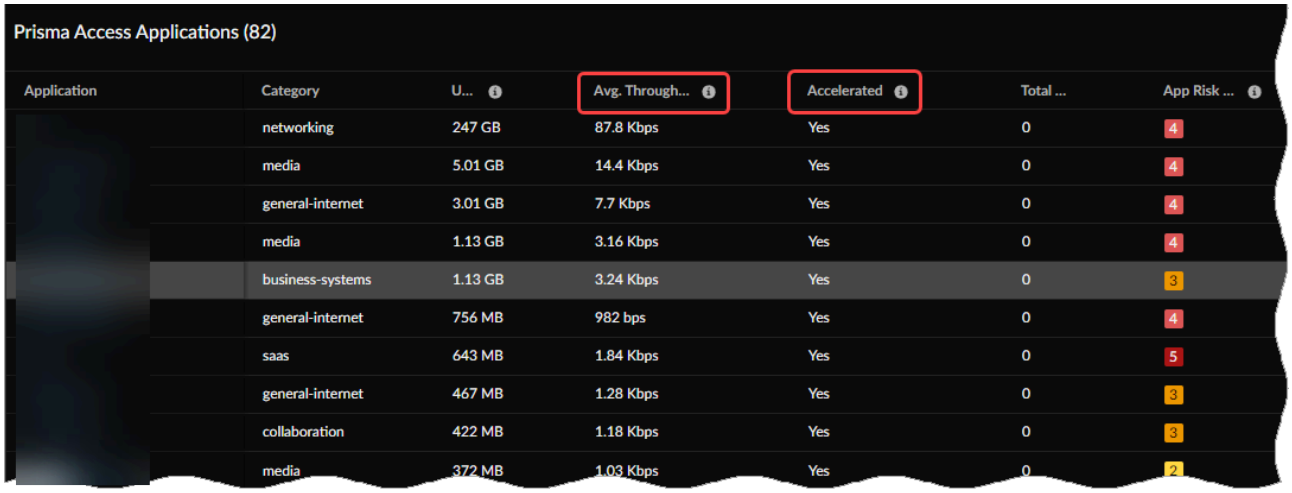
| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |


©2025 Palo Alto Networks, Inc.

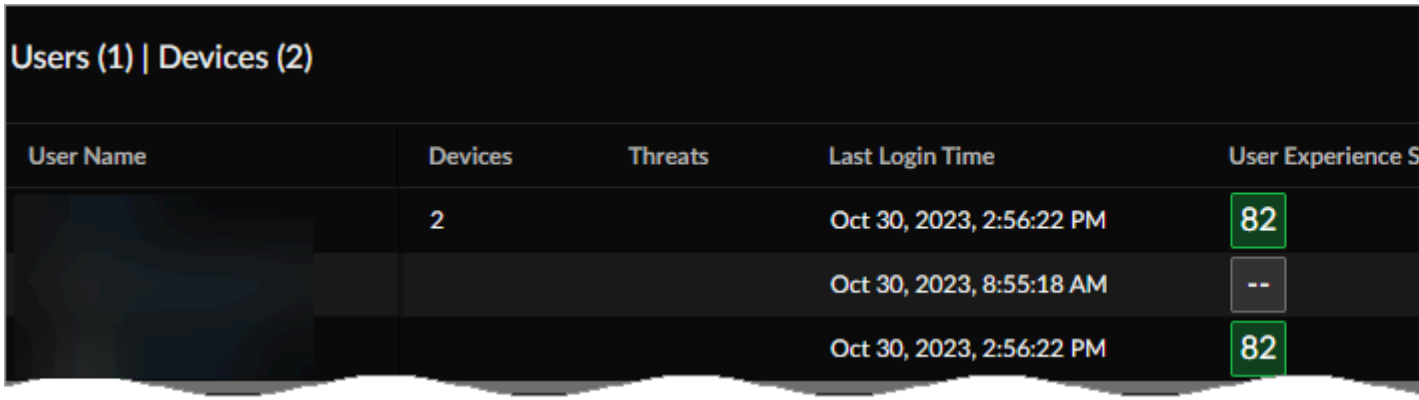
應用程式加速解決了應用程式效能不佳的原因，並即時採取行動以緩解這些原因，從而改善 Prisma Access GlobalProtect 和遠端網路使用者的使用者體驗。

當您的使用者存取應用程式時，他們可能會遇到因輸送量下降而導致應用程式效能不佳的情況，起因可能是無線連線效能下降、網路擁塞和其他因素。這些網路問題可能會對員工體驗產生不利影響並降低他們的生產力。應用程式加速安全地建立對裝置功能、網路功能和應用程式環境的理解，最大限度地提高輸送量並即時調整以適應不斷變化的網路狀況。

在 Strata Cloud Manager 控管中心，前往 **Insights**（洞察） > **Applications**（應用程式），以檢視您環境中已加速的應用程式的詳細資訊。Prisma Access 應用程式表格包含 [Avg.(Average) Throughout（平均輸送量）] 欄（只在您的使用者流量加速才會看到），以及 [Accelerated（已加速）] 欄，其中顯示您的部分或全部應用程式流量已加速。




前往 **Insights**（洞察） > **Users**（使用者），以檢視您環境中應用程式加速使用者的相關資訊。在其環境中已啟用應用程式加速的使用者具有使用者 | 裝置表格，其中顯示 [Traffic Accelerated（流量加速）] 欄。此欄指出部分或全部使用者的應用程式流量已加速。




採用 AI 技術的自發 DEM (ADEM) 與應用程式加速整合成，為您提供加速的應用程式數目和整體效能提升等指標。前往 **SASE Health**（SASE 健康情況） > **Experience**（體驗），以檢視 **Accelerated Applications**（已加速的應用程式）和 **Monitored Applications**（受監控應用程式）頁籤中的 ADEM performance metrics（ADEM 效能指標）。


©2025 Palo Alto Networks, Inc.

# 檢視行動使用者

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma® Access（由 Strata Cloud Manager 管理） | • Prisma Access 授權<br>• 採用 AI 技術的 ADEM 授權 |

檢視活動洞察：使用者，大致了解連線到 Palo Alto Networks 的 Prisma Access 安全性解決方案的所有使用者和主機。您可以輕鬆確定使用者或主機與 Prisma Access 的連線狀態，無論是在分支網站、服務連線，還是遠端位置。檢視：

- 目前連線到 Palo Alto Networks 安全性解決方案的唯一使用者總數，以及連線到 Prisma Access 的使用者總數。
- 在特定時間範圍期間連線的使用者數目，依透過 Prisma Access 連線的使用者細分。
- 透過 Prisma Access 連線的代理程式型使用者。
- 連線到 Prisma Access 的代理程式型或瀏覽器型明確 Proxy 使用者。
- 透過 Prisma Access Browser 連線的使用者。
- 存取 Prisma Access 的未受管理裝置使用者清單。
- 從分支位置連線到 Prisma Access 的使用者清單。
- 使用特定服務連線來連線其資料中心的使用者清單。

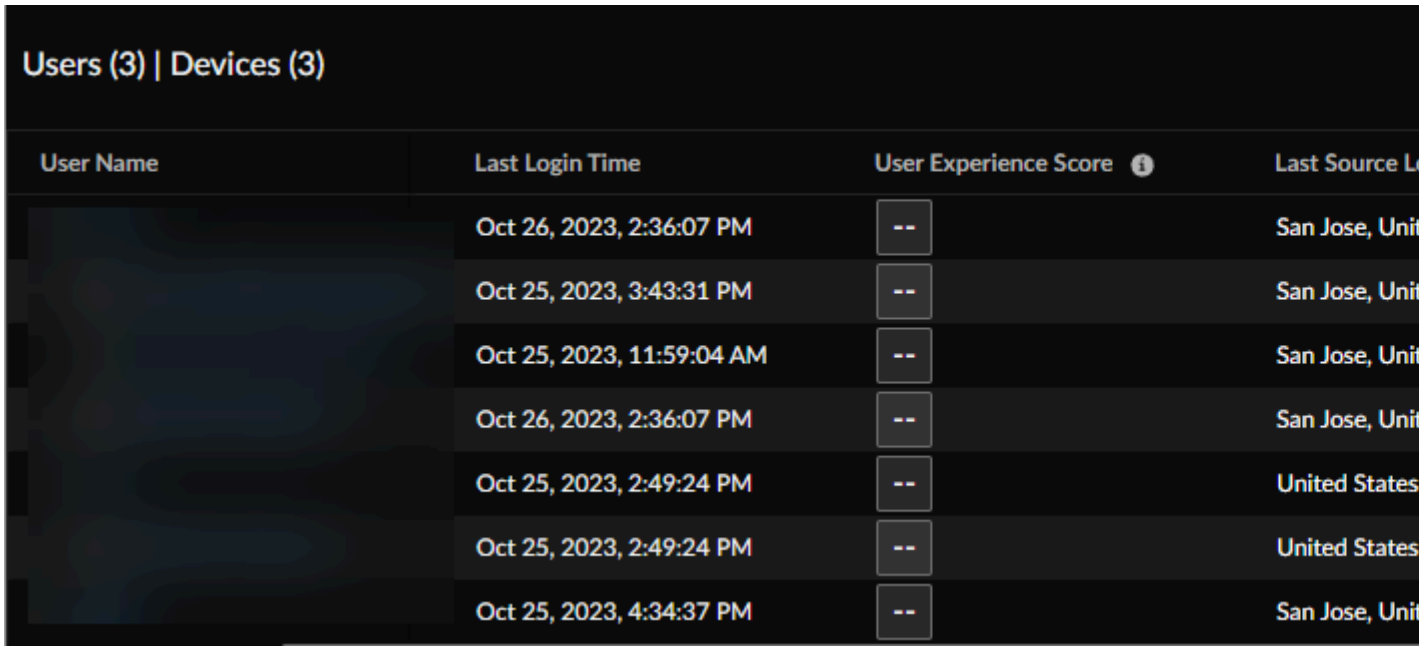
# 檢視和監控行動使用者的 IPv6

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 5.0 Innovation<br>❑ Prisma Access 授權 |

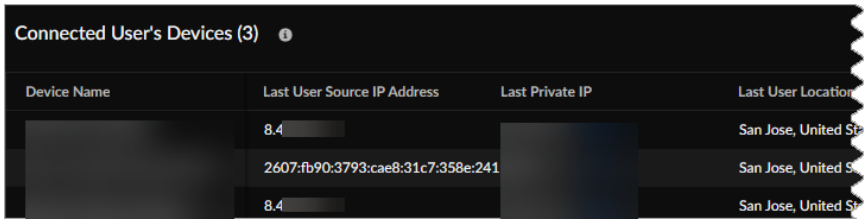
如果您在行動使用者 - GlobalProtect 部署中使用 IPv6 網路，則可以設定 Prisma Access，在行動使用者網路中使用 IPv6 位址。您還需要在 Prisma Access 基礎結構中全域啟用 IPv6 網路，然後才能使用 IPv6 定址。

在 GlobalProtect 部署中使用 IPv6，使用者 | 裝置表格會在來源 IP 位址欄中顯示 IPv4 或 IPv6 位址。

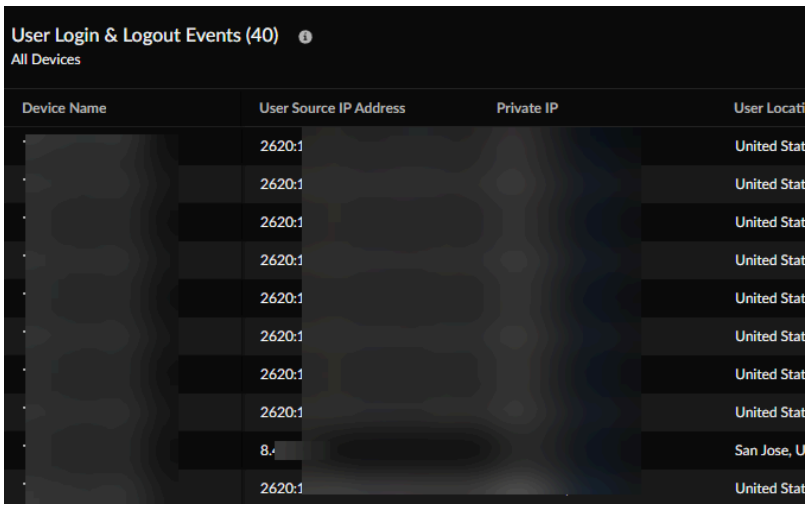

©2025 Palo Alto Networks, Inc.




選取任何已連線的使用者，以查看有關其裝置趨勢的資訊。已連線使用者裝置表格顯示有關使用者裝置的資料，包括上次使用者來源 IP 位址和上次專用 IP，兩者都可以包含單一裝置項目的 IPv4 和 IPv6 位址。




您可以在使用者登入和登出事件表格中檢視 IPv6 位址資訊。使用者來源 IP 位址和私人 IP 位址欄顯示 IPv4 或 IPv6 位址。



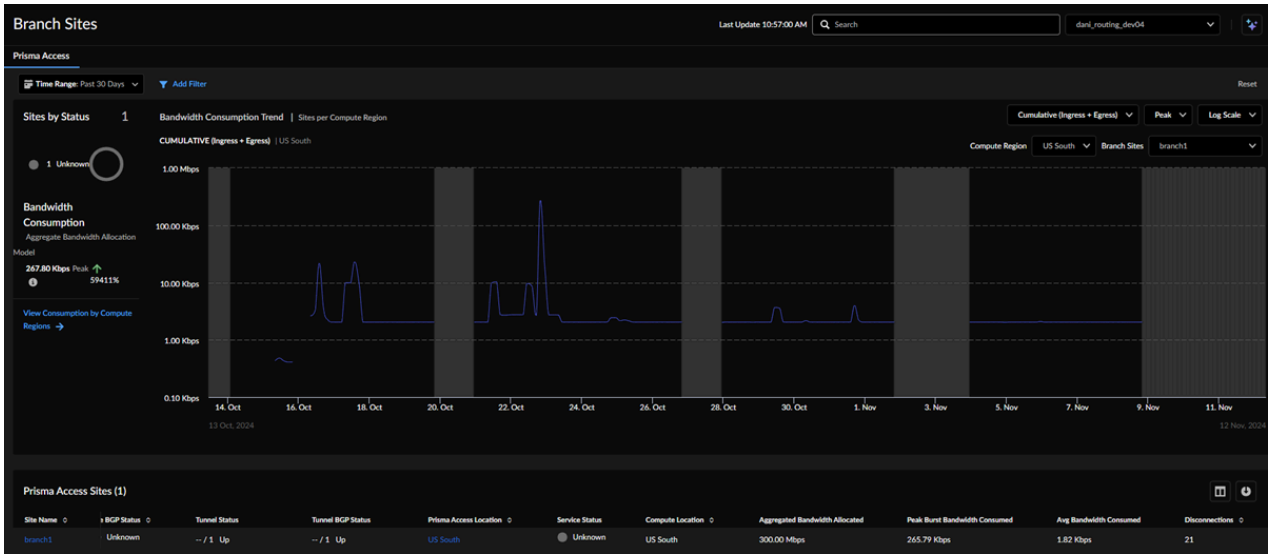

 ©2025 Palo Alto Networks, Inc.

# 檢視並監控分支網站

| 這可在何處使用？ | 我需要什麼？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ adem-aiops-value |

選取 **Monitor**（監控） > **Branch Sites**（分支網站） > **Prisma Access**，以檢視遠端網路的健康情況與連線，以及部署在不同 Prisma Access 位置的所有遠端網路的使用情況。其中顯示即時連線狀態和頻寬消耗詳細資料，以及其他部署詳細資料。您也可以檢視在遠端網路中設定之通道的健康情況。

如需如何規劃遠端網路、配置遠端網路頻寬和裝載遠端網路的相關資訊，請參閱 Prisma Access 遠端網路。若要檢視您的分支網站，請前往 **Monitor**（監控） > **Branch Sites**（分支網站） > **Prisma Access**。




## 依狀態劃分的網站

檢視 **Sites by Status**（依狀態劃分的遠端網站）。您可以查看多少網站處於 **Up**（啟動）、**Down**（關閉）、**Inactive**（非作用中）或 **Not Available**（不可用）狀態，以及多少網站在選取的 **Time Range**（時間範圍）期間出現 **Warning**（警告）。



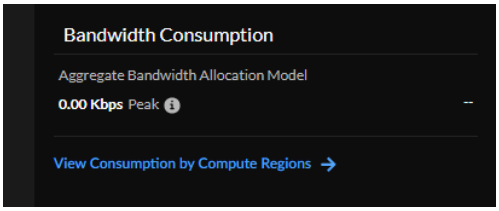


©2025 Palo Alto Networks, Inc.

## 頻寬消耗

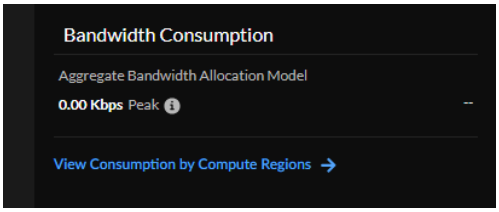
**Bandwidth Consumption**（頻寬消耗）顯示彙總頻寬配置模型中所有租用戶計算區域中某個計算區域消耗的最高峰值頻寬。針對每個網站頻寬配置模型，顯示所有網站中某個網站消耗的最高峰值頻寬。峰值是針對所選時間篩選器持續時間計算的。

選取 **View Consumption by Compute Region**（依計算地區檢視耗用量），以檢視所有計算地區及其設定的 IPSec 終端節點的耗用值和趨勢圖。




依計算地區檢視耗用量

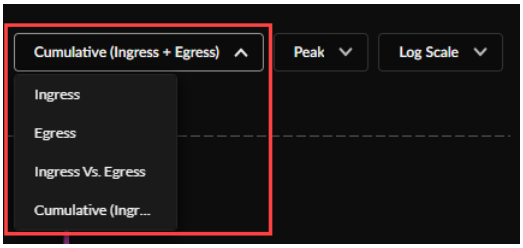
導覽至 **Monitor**（監控） > **Branch Sites**（分支網站） > **Prisma Access**。使用彙總頻寬配置模型時，在 **Bandwidth Consumption**（頻寬消耗） Widget 中選取 **View Consumption by Compute Region**（依計算地區檢視耗用量），以查看您所在地區的頻寬消耗和趨勢。




**Compute Regions**（計算地區）頁面顯示您所選 **Time Range**（時間範圍）期間的頻寬消耗資料。您可以檢視一個表格，其中包含計算地區的 **Average Bandwidth**（平均頻寬）、**Median Bandwidth**（中位數頻寬）和 **Peak Bandwidth**（峰值頻寬）。

**Bandwidth Consumption Trend by Compute Region**（依計算地區劃分的頻寬消耗趨勢）圖顯示有關您的計算地區的資料。篩選資料以精簡您要檢視的資訊。

- 從下拉式清單中選取 **Cumulative (Ingress + Egress)**（累計（進入 + 輸出））、**Ingress**（進入）、**Egress**（輸出）或 **Ingress vs.Egress**（進入與輸出）。




- 檢視所選時間範圍期間的 **Peak**（峰值）、**Median**（中位數）或 **Average**（平均）頻寬消耗趨勢。預設設定是 **Peak**（峰值）頻寬消耗。




 ©2025 Palo Alto Networks, Inc.

- **Log Scale**（對數刻度）或 **Linear Scale**（線性刻度）。
- **Compute Region**（計算地區）—選取一或多個要檢視的地區。

**IPSec Termination Node Utilization**（**IPSec** 終端節點使用率）圖可讓您檢視在特定計算地區設定的 IPsec 終端節點的頻寬消耗。請篩選資料以精簡您要檢視的資訊：

- 選取您要檢視其資料的計算地區。
- 選取您要查看的計算地區的特定網站。
- 選取 **Node Aggregate**（節點彙總）或 **Breakdown by Sites**（依網站細分），以檢視終止於所選 IPsec 終端節點的網站的頻寬消耗趨勢。
- 檢視 **Peak**（峰值）、**Average**（平均值）或 **Median**（中位數）。
- 檢視 **Log Scale**（對數刻度）或 **Linear Scale**（線性刻度）。



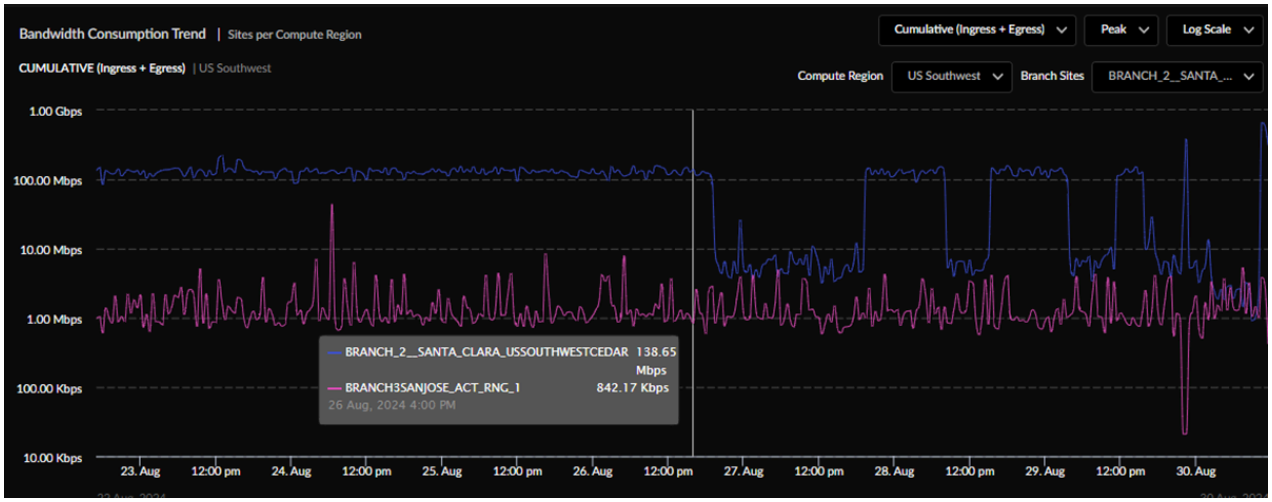

## 頻寬消耗趨勢

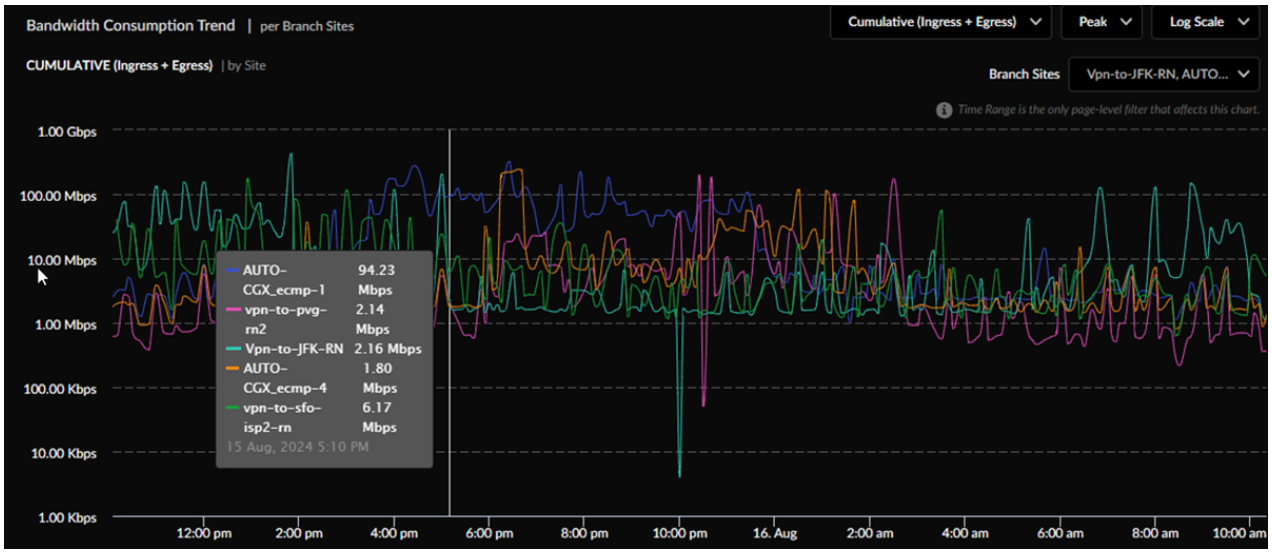
在主要 **Branch Sites**（分支網站）頁面上，您可以檢視在使用彙總頻寬配置模型時所有計算地區的 **Bandwidth Consumption Trend Sites per Compute Region**（每個計算地區的網站頻寬消耗趨勢），或使用 **Per-Site Bandwidth Allocation Model**（每網站頻寬配置模型）時的 **Bandwidth Consumption Trend per Branch Sites**（每個分支網站的頻寬消耗趨勢）。對於彙總頻寬配置模


©2025 Palo Alto Networks, Inc.

型，您可以選取一個計算地區，然後選取該計算地區中您對其頻寬消耗趨勢感興趣的網站。篩選資料以精簡您想要檢視的資訊，而且您可以將游標暫留在圖表上，以檢視網站目前的頻寬消耗：

- 預設檢視顯示 **Cumulative (Ingress + Egress)**（累計（進入 + 輸出））頻寬消耗。其他選項為 **Ingress**（進入）、**Egress**（輸出）或 **Ingress vs.Egress**（進入與輸出）。
- 檢視所選時間範圍期間的 **Peak**（峰值）、**Median**（中位數）或 **Average**（平均）頻寬消耗趨勢。預設設定是 **Peak**（峰值）頻寬消耗。
- **Log Scale**（對數刻度）或 **Linear Scale**（線性刻度）。
- **Compute Region**（計算地區）—當租用戶使用彙總頻寬配置模型時，請檢視將終止於地區的網站進行細分的計算地區。對於每個計算地區，選取終止於該計算地區的網站以檢視其頻寬消耗趨勢。
- **Branch Sites**（分支網站）—選取最少 1 個網站、最多 10 個網站，以在所選時間範圍期間在圖表上檢視其趨勢線。



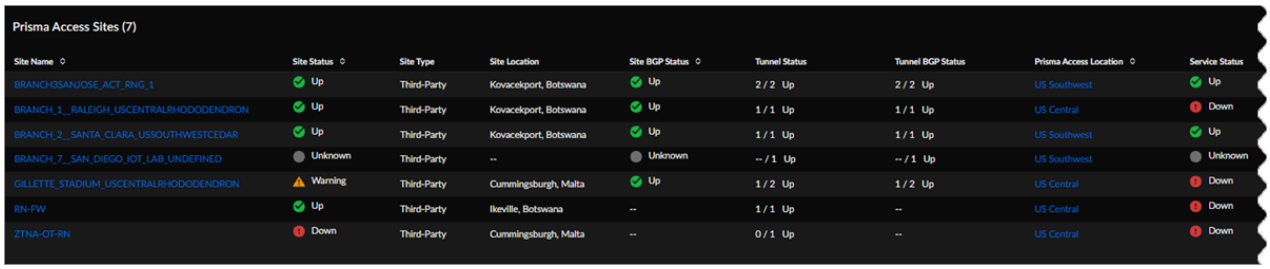

## Prisma Access 網站

**Prisma Access Sites**（網站）表格列出了您的遠端 Prisma Access 網站和資訊。

- **Site Name**（網站名稱）—Prisma Access 網站的唯一名稱。

 ©2025 Palo Alto Networks, Inc.

- **Site Status**（網站狀態）—**Up**（啟動）、**Down**（關閉）、**Warning**（警告）或 **Unknown**（未知）。
- **Site Type**（網站類型）—第三方。
- **Site Location**（網站位置）—Prisma Access 網站位置。
- **Site BGP Status**（網站 **BGP** 狀態）—網站 BGP 狀態為 **Up**（啟動）、**Down**（關閉）或 **Unknown**（未知）。
- **Tunnel Status**（通道狀態）—網站通道的數目以及其中有多少通道處於啟動狀態。
- **Tunnel BGP Status**（通道 **BGP** 狀態）—每個通道的 BGP 狀態。
- **Prisma Access Location**（**Prisma Access** 位置）—此 Prisma Access 網站的位置。選取一個位置以檢視其 Prisma Access 位置詳細資訊。
- **Service Status**（服務狀態）—此欄位指出網站所連線的執行個體或防火牆的狀態。狀態可以是 **Up**（啟動）、**Down**（關閉）或 **Unknown**（未知）。
- **Compute Location**（計算位置）—所有 Prisma Access 位置都是根據最佳化的效能和延遲對應到安全性處理計算位置或地區。至少兩個（通常更多）地理上彼此接近的 Prisma Access 位置會分組為單一計算位置。
- **Aggregated Bandwidth Allocated**（已配置的彙總頻寬）—在所選時間範圍期間為網站配置的彙總頻寬。只有當您使用彙總頻寬模型時，此欄才會出現。
- **Peak Burst Bandwidth Consumed**（已消耗的峰值暴增頻寬）—透過在所選時間範圍期間合併此網站的進入和輸出值而取得的累計峰值。
- **Avg Bandwidth Consumed**（平均消耗的頻寬）—透過在所選時間範圍期間合併此網站的進入和輸出值而取得的累計平均值。
- **Disconnections**（中斷連線）—在所選時間範圍期間此網站發生了多少次中斷連線。
- **Disconnections Duration**（中斷連線持續時間）—在所選時間範圍期間網站中斷連線的總時間量（以秒為單位）。




高效能分支網站可視性

高效能分支 (RN-HP) 具有與舊版分支不同的屬性，並且兩者將在您的租用戶中共存。Prisma Access 中的高效能分支網站具有以下優勢：

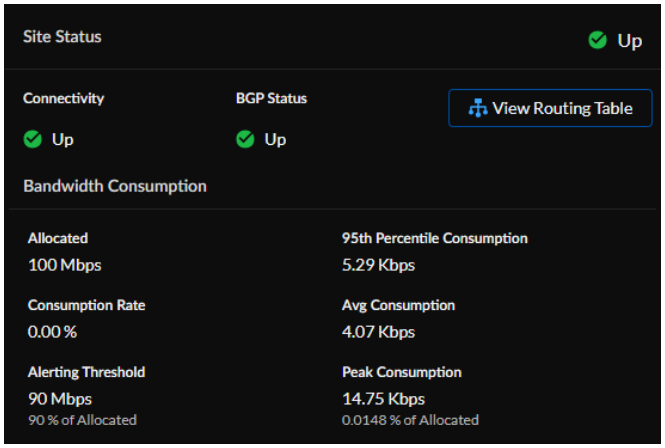
- 該架構透過將網路處理功能與安全性處理功能分開來提高容量效率。具有大型封包處理能力的 ION 裝置可終止容量最高 5 Gbps 的多個分支連線，並將安全性處理散佈至 SPN。
- 您可以使用單一 IP 或 FQDN，將地區中的多個分支終止到單一網路處理節點 (NPN)。
- 您再也不必監控和管理分支網站終止至 IPSec 終端節點的情況。適當的 SPN 會實施分支流量檢查，而且 NPN 會執行負載平衡。
- 您可以藉由能夠為備援指定不同地區來取得真正的高可用性。

 ©2025 Palo Alto Networks, Inc.

您可以在環境中同時檢視高效能分支和舊版分支。在 Strata Cloud Manager 中，前往 **Monitor**（監控） > **Branch Sites**（分支網站） > **Prisma Access**，然後從 **Prisma Access Sites**（**Prisma Access** 網站）表格中選取分支網站。

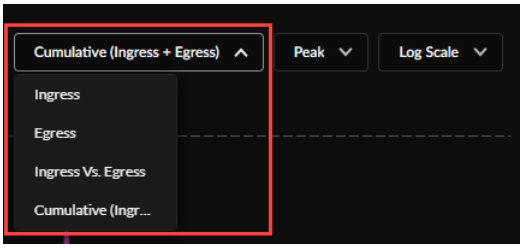
*Prisma Access* 網站詳細資訊

選取任何 Prisma Access **Site Name**（網站名稱），以檢視其 **Site Status**（網站狀態），您可以在其中查看其 **Connectivity**（連線）和 **BGP Status**（**BGP** 狀態）（**Up**（啟動）、**Down**（關閉）、**Inactive**（非作用中）或 **Not Available**（不可用））。檢視所選時間間隔的頻寬 **Peak Consumption**（峰值耗用量）。




您可以在 **Bandwidth Consumption Trend**（頻寬消耗趨勢）圖中檢視 **Cumulative (Ingress + Egress)**（累計（進入 + 輸出）資訊。

- 使用下拉式清單，依 **Ingress**（進入）、**Egress**（輸出）、**Ingress Vs.Egress**（進入與輸出）或 **Cumulative (Ingress + Egress)**（累計（進入 + 輸出））。

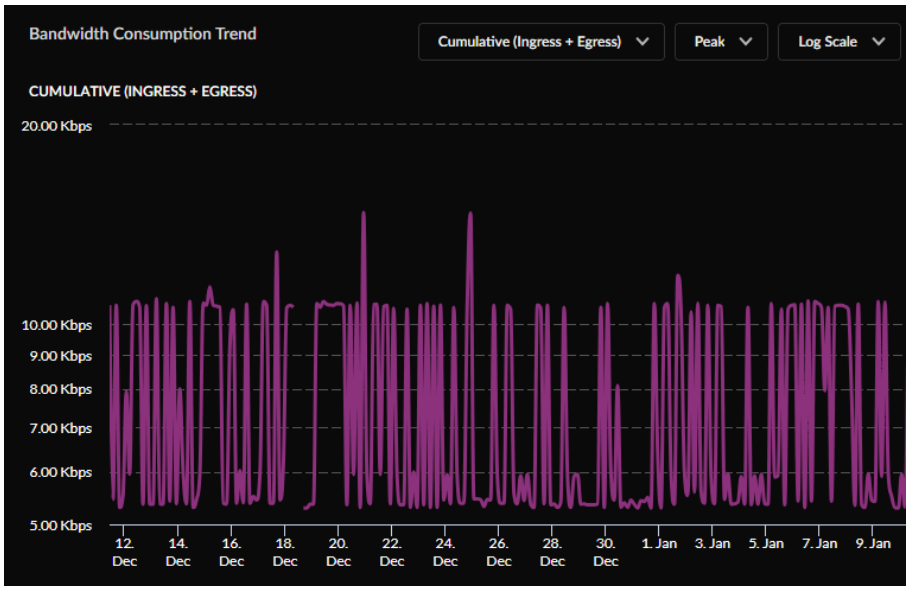



- 依分支網站的 **Peak**（峰值）（預設值）、**Average**（平均值）或 **Median**（中位數）檢視頻寬消耗趨勢圖指標。





©2025 Palo Alto Networks, Inc.




路由表可視性

為了協助您解決連線性挑戰，我們在每個遠端網站上提供路由表的可視性。您可以執行路由表搜尋，取得目的地 IP 位址，以確定是否有路由可用來連線至所需的目的地。利用此資訊，您可以調查其他潛在的失敗原因。此知識使可讓您集中精力解決可能影響連線性的任何問題。

選取 **View Routing Table**（檢視路由表），以檢視此分支的 **Routing Table**（路由表），其中具有 Prisma Access 分支可用的目的地的 IP 路由。

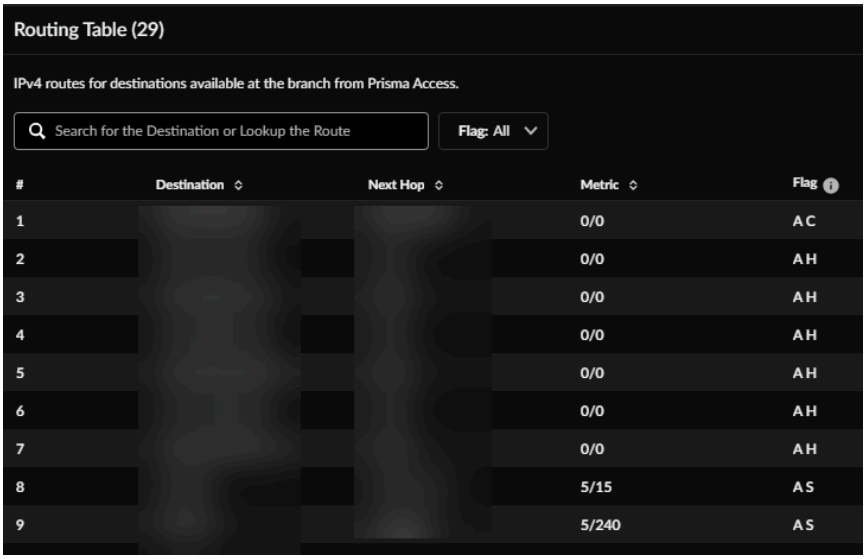
- 使用搜尋列來選取目的地或查閱路由。
- 使用下拉式清單，依 **Flag**（旗標）進行篩選。

路由表顯示：

- **#**—路由編號。
- **Destination**（目的地）—可連線網路的 IP 位址和子網路。
- **Next Hop**（下一個躍點）—前往目的地網路的下一個躍點處閘道的 IP 位址。下一個躍點若為 0.0.0.0 表示預設路由。
- **Metric**（指標）—由路由通訊協定決定的路由指標。
- **Flag**（旗標）—此路由的資訊，如下：
- • **A B**—主動並從 BGP 得知。
  - **A C**—主動且已連線。目的地—網路。
  - **A H**—主動且已連線。目的地#僅限主機。
  - **A R**—主動並從 RIP 得知。
  - **O1**—OSPF 外部類型-1。
  - **O2**—OSPF 外部類型-2。
  - **Oi**—OSPF 區域內。
  - **Oo**—OSPF 區域間。
  - **S**—主動且為靜態。

 ©2025 Palo Alto Networks, Inc.

- **A S**—主動且為靜態。




通道

檢視此網站的通道和通道資料。

- **Tunnel Name**（通道名稱）—通道的唯一名稱。
- **Prisma Access Location**（**Prisma Access** 位置）—此遠端網路的 Prisma Access 位置。
- **Tunnel Status**（通道狀態）—**Up**（啟動）、**Down**（關閉）、**Init**（起始）或 **Unavailable**（無法使用）。
- **Tunnel BGP Status**（通道 **BGP** 狀態）—**Up**（啟動）、**Down**（關閉）或 **Unknown**（未知）。
- **Tunnel Monitoring**（通道監控）—如果您已啟用 **Tunnel Monitoring**（通道監控），此欄會顯示它是 **Up**（啟動）還是 **Down**（關閉）。如果您尚未將其啟用，此欄會顯示 **Not Configured**（未設定）。
- **Average Throughput**（平均輸送量）—所選時間範圍通道的平均頻寬，同時考慮到您選取的 **Ingress**（進入）、**Egress**（輸出）、**Ingress Vs.Egress**（進入與輸出）或 **Cumulative (Ingress + Egress)**（累計（進入 **+** 輸出））值。
- **Peak Throughput**（峰值輸送量）—所選時間範圍通道的峰值頻寬，同時考慮到您選取的 **Ingress**（進入）、**Egress**（輸出）、**Ingress Vs.Egress**（進入與輸出）或 **Cumulative (Ingress + Egress)**（累計（進入 **+** 輸出））。
- **Source IP Address**（來源 **IP** 位址）—來源 IP 位址。
- **Destination Endpoint Address**（目的地端點位址）—Prisma Access 的 IP 或 FQDN 位址，用來確定通道是否已啟動。
- **Disconnections**（中斷連線）—所選時間範圍期間中斷連線的數目。
- **Disconnections Duration**（中斷連線持續時間）—在所選時間範圍期間通道中斷連線多久時間（以秒為單位）

選取 **Tunnel Name**（通道名稱），以查看其 **Tunnel Status**（通道狀態）、**Bandwidth Consumption Trend**（頻寬消耗趨勢）和其他通道詳細資訊。


©2025 Palo Alto Networks, Inc.

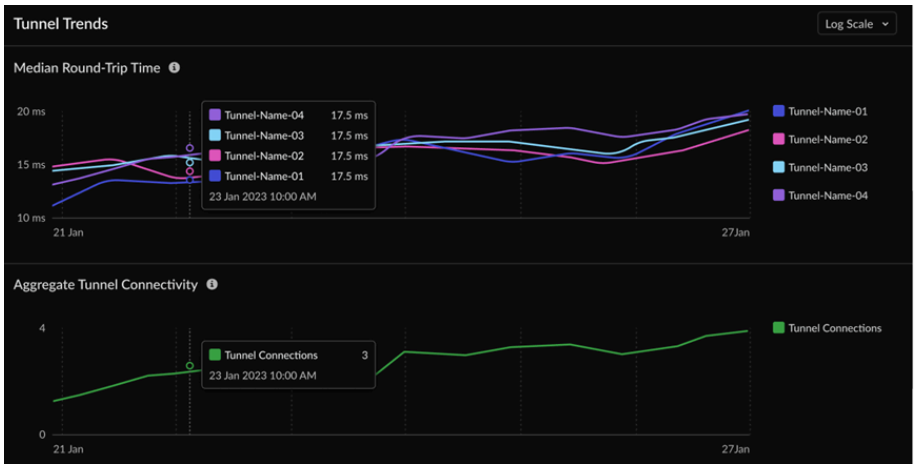


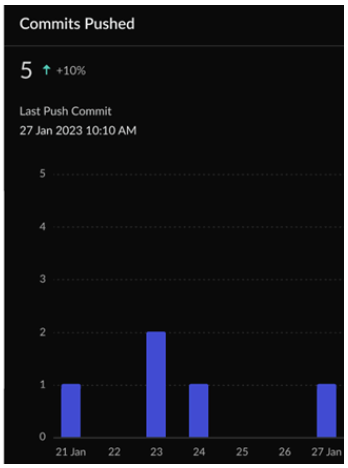

通道趨勢

啟用 **Tunnel Monitoring**（通道監控）後，您可以選取多個通道並檢視其平均 **Round-Trip Time**（往返時間）。如果您未指定一組通道，則預設會針對具有觀察到最高 RTT 的 10 個通道計算 RTT 中位數。

**Aggregated Tunnel Connectivity**（彙總的通道連線）向您顯示所選時間範圍已連線通道的總數。將游標暫留在任一圖形上即可查看特定時間的連線數目。

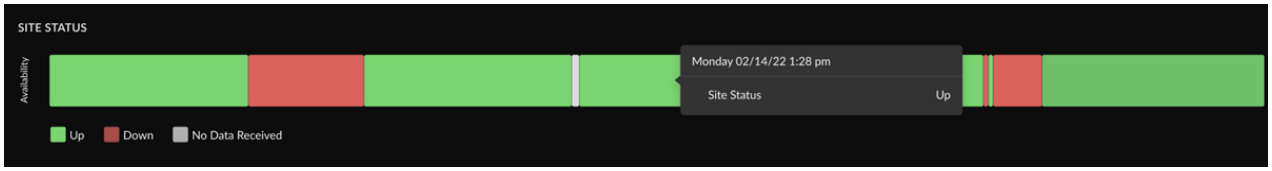
**Commits Pushed**（已推送提交）顯示在選取的 **Time Range**（時間範圍）期間以及 **Last Push Commit**（上次推送提交）發生時推送了多少提交。




站台狀態

**Site Status**（網站狀態）顯示所選時間範圍期間網站的可用性。綠色表示網站在此期間已啟動、紅色表示網站已關閉，而灰色表示在顯示的時間期間沒有可用資料。




# 檢視和監控資料中心

| 這可在何處使用？ | 我需要什麼？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

 ©2025 Palo Alto Networks, Inc.

## 服務連線

服務連線也稱為企業存取節點 (CAN)，允許行動使用者和遠端網路上的使用者存取私人應用程式和資源，並可讓您的行動使用者和遠端網路相互通訊。Palo Alto Networks 建議一律在您的 Prisma Access 部署中建立服務連線。所有服務連線允許存取總部或資料中心的資源，並允許遠端網路和行動使用者相互通訊。

您收到的服務連線數目取決於您的 Prisma Access 授權。如需有關服務連線以及如何設定它們的詳細資訊，請參閱 Prisma Access 服務連線。

在 Strata Cloud Manager 中，選取 **Monitor**（監控） > **Data Centers**（資料中心） > **Service Connections**（服務連線），以了解您的服務連接。

## ZTNA 連接器

零信任網路存取 (ZTNA) 連接器可讓您將 Prisma Access 連線到您組織的私人應用程式。ZTNA 連接器使用自動安全通道，讓行動使用者和分支位置的使用者可以存取您的私人應用程式。ZTNA 連接器會自動設定通道，因此您不必手動設定 IPSec 通道，並路由到您私人應用程式所在的資料中心或總部位置、公用雲端位置和合作夥伴網路。

在 Strata Cloud Manager 中，選取 **Monitor**（監控） > **Data Centers**（資料中心） > **ZTNA Connectors**（**ZTNA** 連接器），以了解您的 ZTNA 連接器。

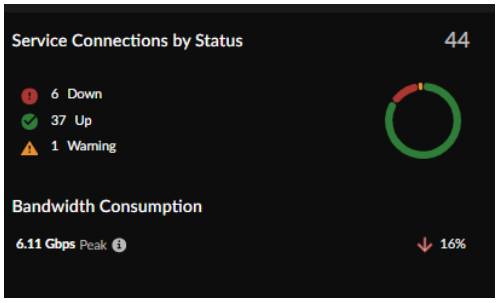
## 檢視和監控服務連線

| 這可在何處使用？ | 我需要什麼？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

檢視彙總的服務連線資料，以及個別服務連線的相關資訊。服務連線支援行動使用者和遠端網路。除了提供對公司資源的存取，服務連線也允許您的行動使用者連線到分支位置。您可以在 Strata Cloud Manager 中檢視您的服務連線，以查看服務連線狀態、頻寬消耗趨勢、通道資料和趨勢，以及整體服務連線健康情況的相關資訊。首先，選取 **Monitor**（監控） > **Data Centers**（資料中心） > **Service Connections**（服務連線）。

依狀態劃分的服務連線

您可以檢視所有服務連線的健康情況狀態。顏色編碼的圖表向您顯示多少服務連線啟動、關閉或需要注意的散佈情況。您可以檢視服務連線過去 30 天消耗的頻寬概要。




 ©2025 Palo Alto Networks, Inc.

**Bandwidth Consumption**（頻寬消耗）針對每個網站頻寬配置模型，顯示所有網站中某個網站消耗的最高峰值頻寬。峰值是針對所選時間篩選器持續時間計算的。

頻寬消耗趨勢

檢視 **Bandwidth Consumption Trend per Service Connection**（每個服務連線的頻寬消耗趨勢）。趨勢顯示每個服務連線的頻寬消耗，以及其平均和峰值使用率。

- 預設檢視顯示 **Cumulative (Ingress + Egress)**（累計（進入 + 輸出））頻寬消耗。其他選項為 **Ingress**（進入）、**Egress**（輸出）或 **Ingress vs.**輸出。
- 檢視所選時間範圍期間的 **Peak**（峰值）、**Median**（中位數）或 **Average**（平均）頻寬消耗趨勢。預設設定是 **Peak**（峰值）頻寬消耗。
- **Log Scale**（對數刻度）或 **Linear Scale**（線性刻度）。
- 選取 1 至 10 個 **Service Connections**（服務連線），以在圖形上檢視其在所選時間範圍期間的趨勢線。將游標暫留在圖形上，即可查看您所選每個服務連線的相關資訊。



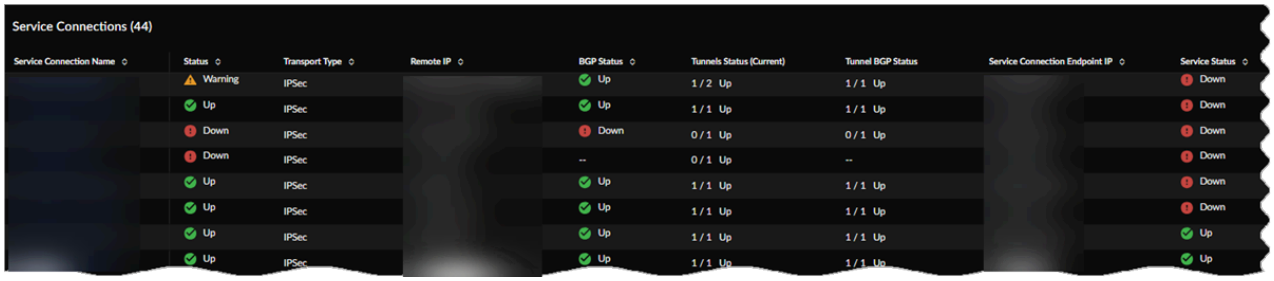

服務連線表格

**Service Connections**（服務連線）表格為您顯示服務連線的相關資料，例如狀態、遠端 IP 位址、BGP 狀態、目前通道狀態和其他資料。選取 **Service Connection Name**（服務連線名稱），以取得有關該服務連線的詳細資訊。

- **Service Connection Name**（連線名稱）—服務連線的唯一名稱。
- **Status**（狀態）—**Up**（啟動）、**Down**（關閉）、**Warning**（警告）或 **Unknown**（未知）。
- **Transport Type**（傳輸類型）—IPSec。
- **Remote IP**（遠端 **IP**）—遠端 IP 位址。
- **BGP Status**（**BGP** 狀態）—網站 BGP 狀態是 **Up**（啟動）、**Down**（關閉）還是 **Unknown**（未知）。
- **Tunnel Status (Current)**（通道狀態（目前））—網站通道的數目以及其中有多少通道處於啟動狀態。
- **Tunnel BGP Status**（通道 **BGP** 狀態）—每個通道的 BGP 狀態。
- **Service Connection Endpoint IP**（服務連線端點 **IP**）—服務連線的端點 IP 位址。
- **Service Status**（服務狀態）—此欄位指出網站所連線的執行個體或防火牆的狀態。狀態可以是 **Up**（啟動）、**Down**（關閉）或 **Unknown**（未知）。

 ©2025 Palo Alto Networks, Inc.

- **Prisma Access Location**（**Prisma Access** 位置）—服務連線的 Prisma Access 位置。
- **Average Bandwidth Consumptio**（平均頻寬消耗）—平均頻寬消耗，以 Kbps 為單位。
- **Peak Bandwidth Consumptio**（峰值頻寬消耗）—峰值頻寬消耗，以 Kbps 為單位。

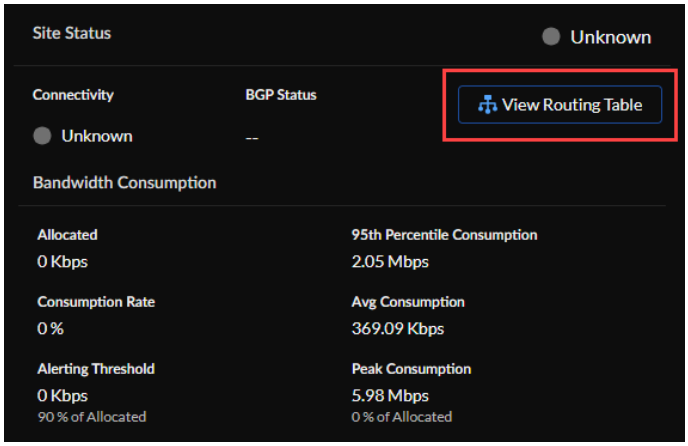



服務連線詳細資訊

選取任何 **Service Connection Name**（服務連線名稱）以檢視其詳細資料。檢視其過去 30 天的 **Service Connection Status**（服務連線狀態）、**Bandwidth Consumed**（頻寬消耗）。**Bandwidth Consumption Trend**（頻寬消耗趨勢）圖表顯示您的每個服務連線在所選時間範圍期間的頻寬消耗。

站台狀態

選取任何 **Service Connection Name**（服務連線名稱），以檢視其 **Site Status**（網站狀態），您可以在其中查看其 **Connectivity**（連線）和 **BGP Status**（**BGP** 狀態）（**Up**（啟動）、**Down**（關閉）、**Inactive**（非作用中）或 **Not Available**（不可用））。檢視所選時間間隔的頻寬 **Peak Consumption**（峰值耗用量）。




路由表可視性

為了協助您解決連線性挑戰，我們在每個服務連線上提供路由表的可視性。您可以執行路由表搜尋，取得目的地 IP 位址，以確定是否有路由可用來連線至所需的目的地。透過此資訊，您可以從 Prisma Access 基礎結構收到指引，以調查其他潛在失敗原因。此知識使可讓您集中精力解決影響連線性的任何問題。

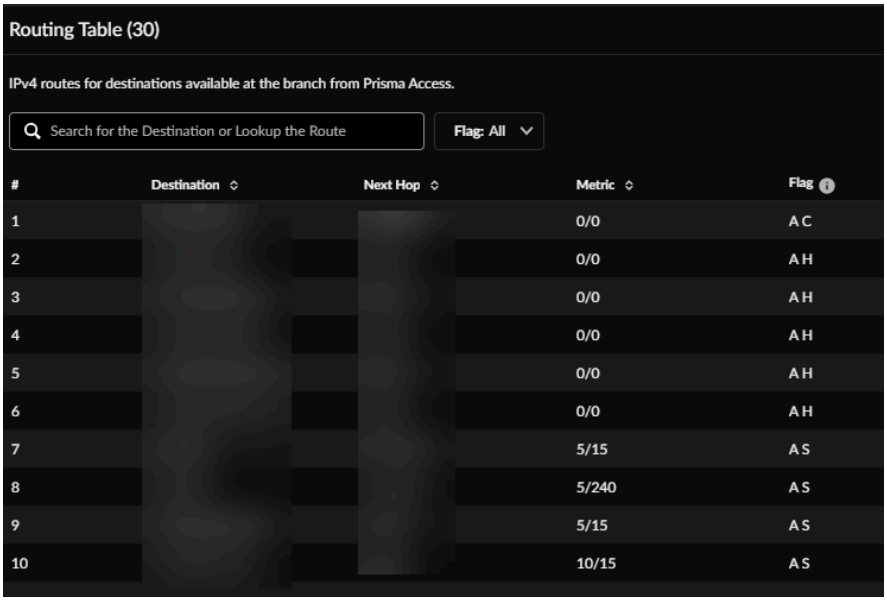
選取 **View Routing Table**（檢視路由表），以檢視此分支的 **Routing Table**（路由表），其中具有 Prisma Access 分支可用的目的地的 IP 路由。

- 使用搜尋列來選取目的地或查閱路由。
- 使用下拉式清單，依 **Flag**（旗標）進行篩選。

 ©2025 Palo Alto Networks, Inc.

路由表顯示：

- **#**—Route number（路由編號）
- **Destination**（目的地）—I可連線網路的 IP 位址和子網路。
- **Next Hop**（下一個躍點）—前往目的地網路的下一個躍點處閘道的 IP 位址。下一個躍點若為 0.0.0.0 表示預設路由。
- **Metric**（指標）—由路由通訊協定決定的路由指標。
- **Flag**（旗標）—此路由的資訊，如下：
- • **A B**—主動並從 BGP 得知。
  - **A C**—主動且已連線。目的地—網路。
  - **A H**—主動且已連線。目的地—僅限主機。
  - **A R**—主動並從 RIP 得知。
  - **O1**—OSPF 外部類型-1。
  - **O2**—OSPF 外部類型-2。
  - **Oi**—OSPF 區域內。
  - **Oo**—OSPF 區域間。
  - **S**—主動且為靜態。
  - **A S**—主動且為靜態。

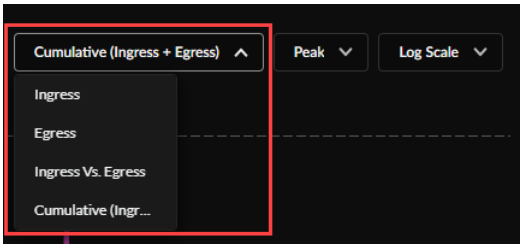



頻寬消耗趨勢

**Bandwidth Consumption Trend**（頻寬消耗趨勢）預設顯示 **Cumulative (Ingress + Egress)**（累計（進入 + 輸出）資訊。

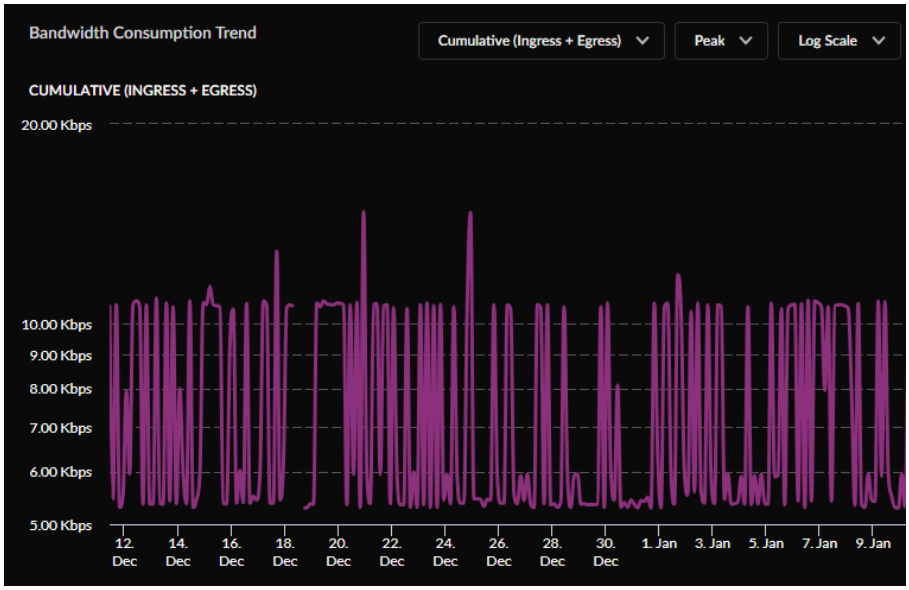
 ©2025 Palo Alto Networks, Inc.

- 使用下拉式清單，依 **Ingress**（進入）、**Egress**（輸出）、**Ingress Vs.Egress**（進入與輸出）或 **Cumulative (Ingress + Egress)**（累計（進入 + 輸出））。



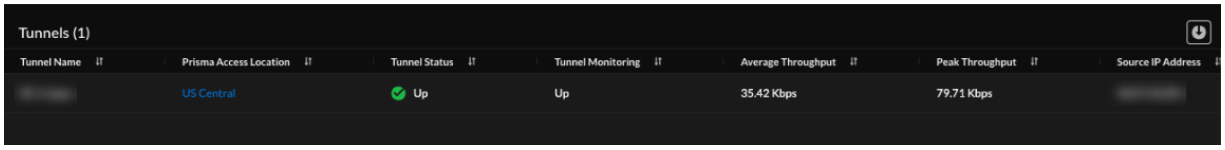

- 依分支網站的 **Peak**（峰值）（預設值）、**Average**（平均值）或 **Median**（中位數）檢視頻寬消耗趨勢圖指標。




通道

查看此服務連線有多少 **Tunnels**（通道），並檢視每個通道的詳細資訊。若要下載 **Tunnels**（通道）資料，請選取下載圖示。



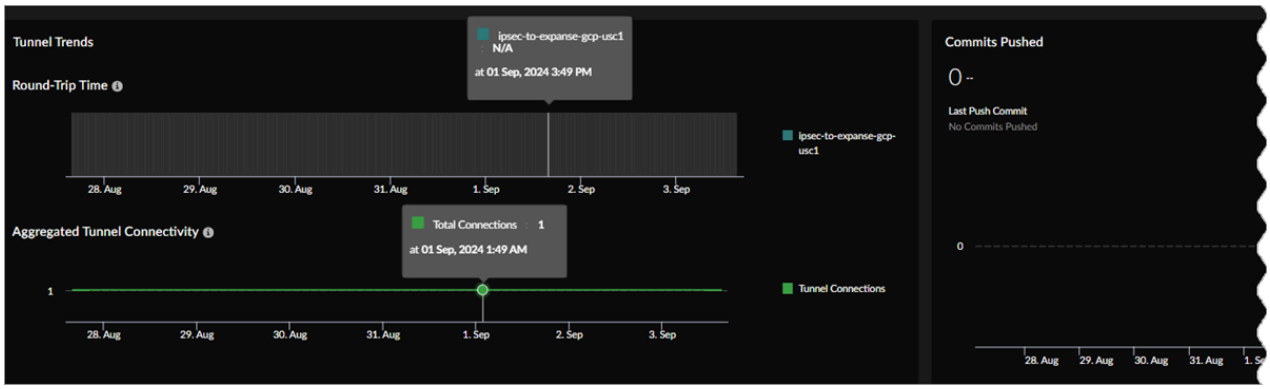

通道趨勢

您可以選取多個通道，並檢視其中位數 **Round-Trip Time**（往返時間）。如果您未指定一組通道，則會針對具有觀察到最高 RTT 的 10 個通道計算 RTT 中位數。

**Aggregated Tunnel Connectivity**（彙總的通道連線）向您顯示所選時間範圍已連線通道的總數。將游標暫留在任一圖形上即可查看特定時間的連線數目。

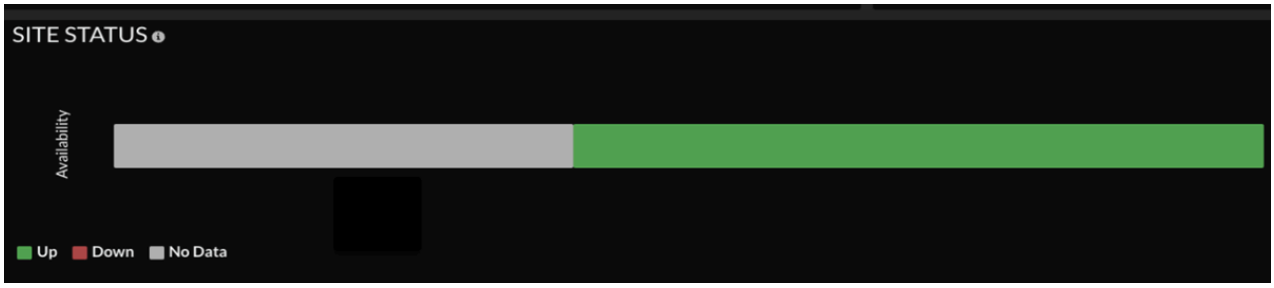
 ©2025 Palo Alto Networks, Inc.

**Commits Pushed**（已推送提交）顯示在選取的 **Time Range**（時間範圍）期間以及 **Last Push Commit**（上次推送提交）發生時推送了多少提交。



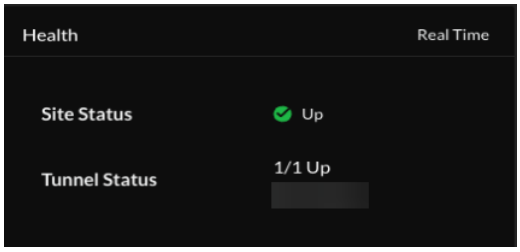

站台狀態

**Site Status**（網站狀態）顯示所選時間範圍期間網站的可用性。綠色表示網站在此期間已啟動、紅色表示網站已關閉，而灰色表示在顯示的時間期間沒有可用資料。



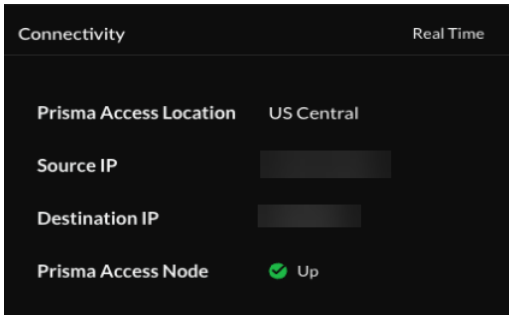

健康情況

**Health**（健康情況）為您顯示 **Site Status**（網站狀態），並顯示網站中每個通道的名稱和狀態。




連線

**Connectivity**（連線）顯示網站連線至其中的 Prisma Access 位置、其來源和目的地 IP，以及 Prisma Access 節點狀態。




 ©2025 Palo Alto Networks, Inc.

耗用量

**Consumption**（耗用量）顯示頻寬消耗詳細資訊。

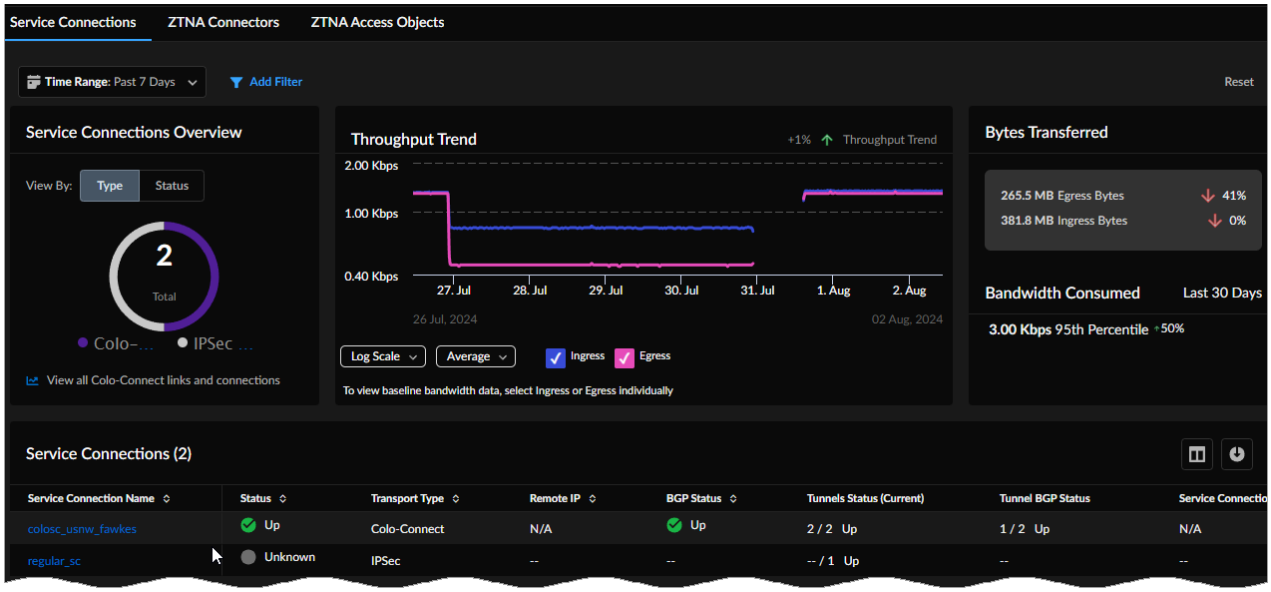


## 檢視和監控 Colo-Connect

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | Prisma Access 授權 |

Prisma Access Colo-Connect 利用雲端原生 GCP 互連技術來提供與您私人應用程式的高頻寬服務連線。Colo-Connect 與現有 IPsec 通道型服務連線共存，因此如果您必須為不需要高頻寬輸送量的小型資料中心提供私人應用程式存取權，您也可以使用與這些資料中心的服務連線。透過檢視 Colo-Connect 連結數目和狀態、輸送量趨勢以及個別通道、連線和連結詳細資訊等指標，了解 Colo-Connect 部署。透過檢視有關 Colo-Connect 服務連線的資料，您可以得到部署的健康情況與連線全貌。

若要檢視和監控透過雲端互連以與混合雲端和內部部署資料中心的私人連線，請前往 **Monitor**（監控） > **Data Centers**（資料中心） > **Service Connections**（服務連線）。




服務連線概要

服務連線概要依傳輸 **Type**（類型）顯示服務連線的數目。

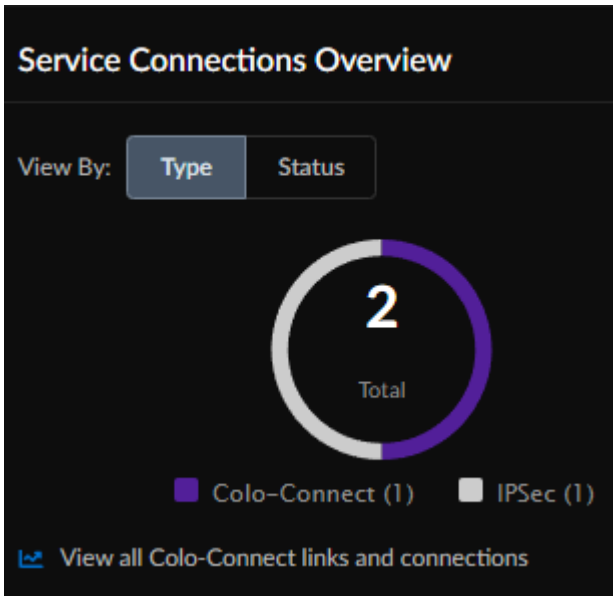
您可以依 **Type**（類型）或其可用性 **Status**（狀態）查看已連線傳輸的彙總。

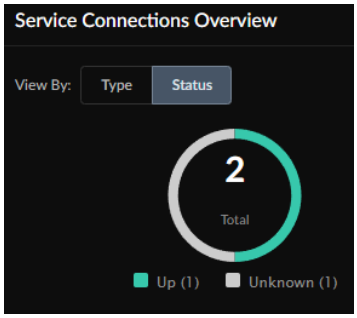
- **IPSec**
- **Colo-Connect**

您可以依狀態檢視通道傳輸類型：**Up**（啟動）、**Down**（關閉）、**Degraded**（已降級）或 **Unknown**（未知）。

 ©2025 Palo Alto Networks, Inc.

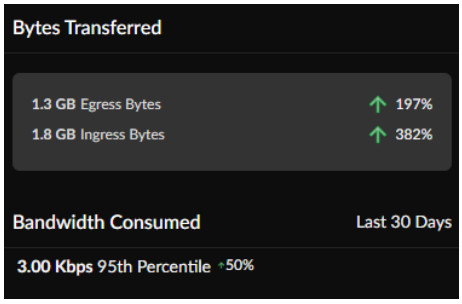
選取 **View all Colo-Connect links and connections**（檢視所有 **Colo-Connect** 連結和連線），以檢視 Colo-Connect 詳細資訊頁面。




服務連線概要：已傳輸的位元組和消耗的頻寬

**Bytes Transferred**（已傳輸的位元組）顯示消耗的進入和輸出位元組的彙總，以及與先前所選時間範圍的消耗差異。**Bandwidth Consumed**（消耗的頻寬）顯示過去 30 天所消耗頻寬的第 95 個百分位數。



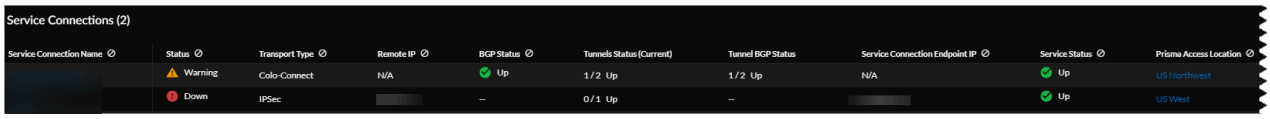

服務連線

**Service Connections**（服務連線）表格為每個指示的服務連線顯示以下詳細資訊：

- **Service Connection Name**（服務連線名稱）—Colo-Connect 或 IPSec 服務連線的名稱。選取一個 **Service Connection Name**（服務連線名稱）以前往其詳細資訊頁面。
- **Status**（狀態）—Up（啟動）、Down（關閉）、Degraded（已降級）或 Unknown（未知）。


©2025 Palo Alto Networks, Inc.

- **Transport Type**（傳輸類型）—Colo-Connect 或 IPSec。
- **Remote IP**（遠端 **IP**）—目的地 IP。
- **BGP Status**（**BGP** 狀態）—Up（啟動）、Down（關閉）或 Warning（警告）（如果某些 BGP 通道已啟動，某些通道已關閉）。
- **Tunnel Status (Current)**（通道狀態（目前））—目前通道狀態。
- **Tunnel BGP Status**（通道 **BGP** 狀態）—依 BGP 狀態（Up（啟動）、Down（關閉）或 Warning（警告））劃分的通道數目。
- **Service Connection Endpoint IP**（服務連線端點 **IP**）—Prisma Access 節點 IP 位址。
- **Service Status**—服務狀態由作用中服務連線或一或多個資料中心叢集（超過一個叢集）的狀態（Up（啟動）、Down（關閉）或 Warning（警告））決定。
- **Prisma Access Location**（**Prisma Access** 位置）—選取 **Prisma Access Location**（**Prisma Access** 位置）。
- **Average Bandwidth Consumption**（平均頻寬消耗）—網站在所選時間範圍期間的平均頻寬消耗。
- **Peak Bandwidth Consumption**（峰值頻寬消耗）—網站在所選時間範圍期間的峰值頻寬消耗。




服務連線詳細資訊

從主要頁面上的 **Service Connections**（服務連線）表格中，選取一個傳輸 **Type**（類型）為 Colo-Connect 的 **Service Connection**（服務連線），以前往其其詳細資訊頁面。




服務連線狀態、*Colo-Connect* 和並行工作階段

- 請參閱服務連線的 **Access Location**（存取位置）和 **GRE Tunnels**（**GRE** 通道）狀態（Up（啟動）、Down（關閉）或 Warning（警告））。
- 檢視 **Colo-Connect** 連結和連線的總數。
- **Concurrent Sessions**（並行工作階段）顯示目前工作階段數目和過去 30 天的工作階段總數。

 ©2025 Palo Alto Networks, Inc.

輸送量趨勢

**Throughput Trend**（輸送量趨勢）顯示此服務連線在所選時間範圍期間消耗的進入和輸出輸送量流量。

已傳輸的位元組和消耗的頻寬

**Bytes Transferred**（已傳輸的位元組）顯示此服務連線消耗的進入和輸出位元組的彙總，以及與先前所選時間範圍的消耗差異。**Bandwidth Consumed**（消耗的頻寬）顯示服務連線過去 30 天所消耗頻寬的第 95 個百分位數。

*GRE* 通道

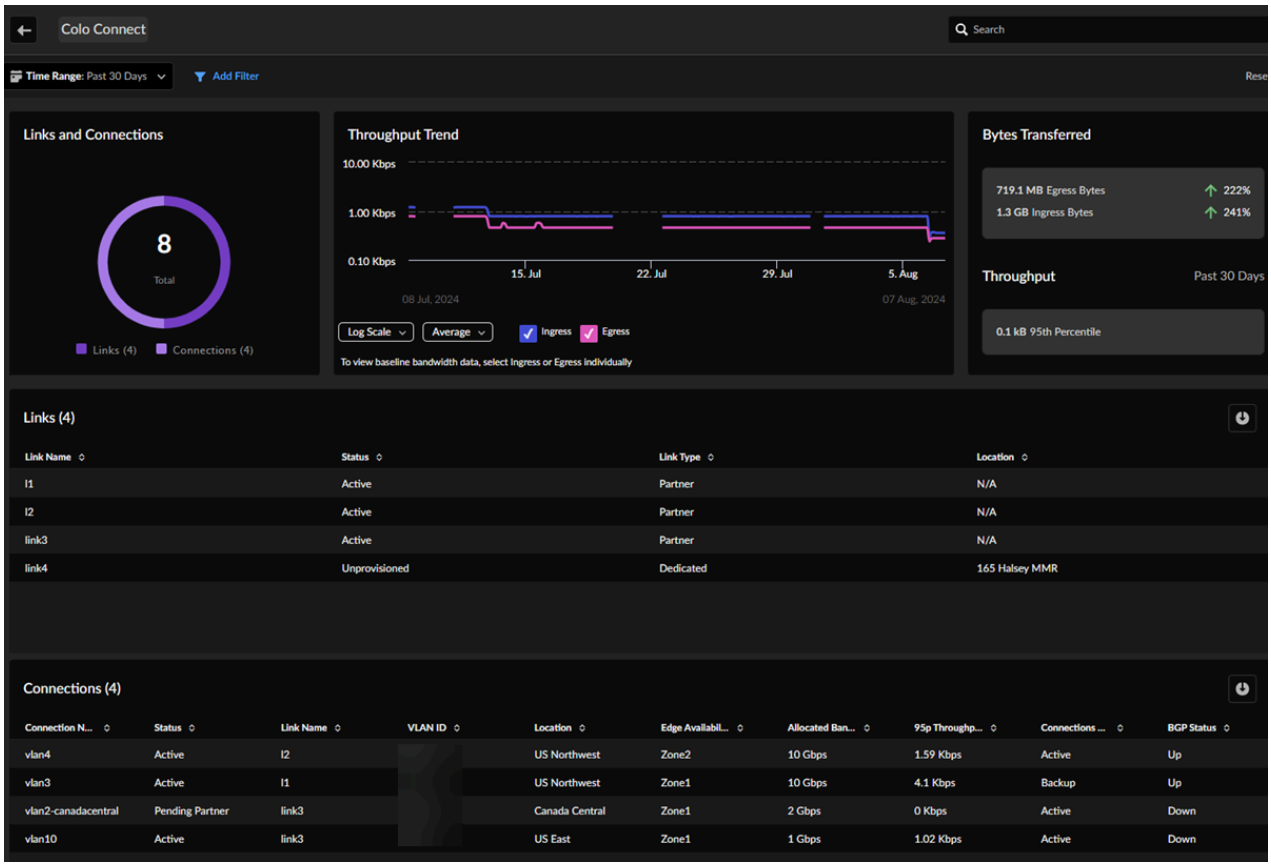
檢視有關此服務連線中通道的詳細資訊：

- **Tunnel Name**（通道名稱）—唯一的通道名稱。
- **Tunnel Status**（通道狀態）—Up（啟動）、Down（關閉）或 Unknown（未知）。
- **Connection Name**（連線名稱）—連線的唯一名稱。
- **Tunnel State**（通道狀態）—連線狀態（Active（作用中）或 Backup（備份））。
- **Remote IP**（遠端 **IP**）—目的地 IP 位址。
- **Source IP**（來源 **IP**）—本機裝置的 IP 位址。
- **95% Throughput**（**95%** 輸送量）—過去 30 天所消耗頻寬的第 95 個百分位數。
- **Peak Throughput**（峰值輸送量）—所選時間範圍期間的峰值輸送量。
- **BGP Status**（**BGP** 狀態）—Up（啟動）、Down（關閉）、Degraded（已降級）或 Unknown（未知）。
- **BGP Local IP**（**BGP** 本機 **IP**）—BGP 本機 IP。
- **Disconnections**（中斷連線）—此通道中斷連線的次數。
- **Disconnections Duration**（中斷連線持續時間）—中斷連線持續了多長時間。
- **Ingress Bytes**（進入位元組）—在所選時間範圍期間消耗了多少進入位元組。
- **Egress Bytes**（輸出位元組）—在所選時間範圍期間消耗了多少輸出位元組。
- **Ingress Packet Count**（進入封包計數）—進入封包計數。
- **Egress Packet Count**（輸出封包計數）—輸出封包計數。

*Colo-Connect* 詳細資訊

從主要 **Service Connections**（服務連線）頁面中，選取 **Service Connections Overview**（服務連線概要）Widget 中的 **View all Colo-Connect links and connections**（檢視所有 **Colo-Connect** 連結和連線），以開啟 **Colo-Connec** 詳細資訊頁面。此頁面上的 Widget 會顯示您目前的詳細資訊（目前定義為過去 20 分鐘）。


©2025 Palo Alto Networks, Inc.




連結與連線

圓圈圖顯示目前 Colo-Connect 連結和連線的總數。

連結

此表格顯示有關您目前 Colo-Connect 連結的詳細資訊。

- **Link Name**（連結名稱）—唯一的 Colo-Connect 連結名稱。
- **Status**（狀態）—Active（作用中）或 Maintenance（維護）.
- **Link Type**（連結類型）—Partner（合作夥伴）或 Dedicated（專用）。
- **Location**（位置）—Prisma Access 位置。

連線

檢視有關您目前每一個 Colo-Connect 連結的詳細資訊。將游標暫留在連線上即可查看有關所顯示狀態的資訊。

- **Connection Name**（連線名稱）—唯一的 Colo-Connect 連線名稱。
- **Status**（狀態）—Acrtive（作用中）、Pending Partner（擱置合作夥伴）、Defunct（失效）。
- **Link Name**（連結名稱）—連線的連結名稱。
- **VLAN ID**—連線的 VLAN ID。
- **Location**（位置）—Prisma Access 位置。
- **Edge Availability Zone**（邊緣可用性區域）—區域 1 或區域 2。
- **Allocated Bandwidth**（配置的頻寬）—1 Gbps、2 Gbps、5 Gbps、10 Gbps 或 20 Gbps。

 ©2025 Palo Alto Networks, Inc.

- **95% Throughput**（**95%** 輸送量）—所消耗頻寬的第 95 個百分位數。
- **Connection State**（連線狀態）—Active（作用中）或 Backup（備份）。
- **BGP Status**（**BGP** 狀態）—Up（啟動）或 Down（關閉）。

## 檢視和監控 ZTNA 連接器

| 這可在何處使用？ | 我需要什麼？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ 這是 Prisma Access Insights 功能。 |

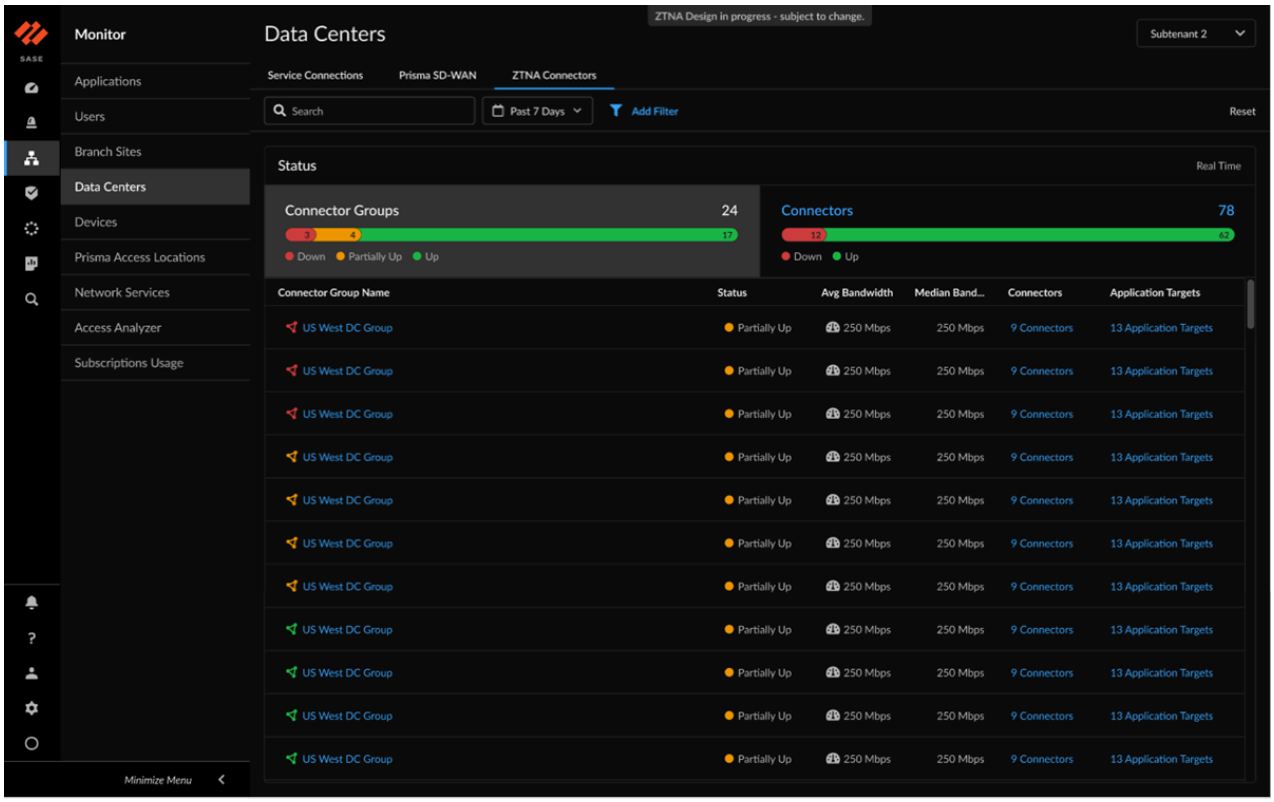
零信任網路存取 (ZTNA) 連接器可簡化所有應用程式的私人應用程式存取。您環境中的 ZTNA 連接器 VM 會自動在您的私人應用程式與 Prisma Access 之間形成通道。檢視所有已設定的 ZTNA 連接器的摘要，包括與連接器相關聯的 **Application Targets**（應用程式目標）、其平均頻寬和中位數頻寬，以及 **Status**（狀態）（開啟、部分開啟、關閉）。在 Strata Cloud Manager 中選取 **Monitor**（監控） > **Data Centers**（資料中心） > **ZTNA Connectors**（**ZTNA** 連接器），以查看 ZTNA 連接器和連接器群組的執行方式。

**ZTNA** 連接器群組狀態

每個群組中的連接器決定連接器群組的 **Status**（狀態）。

- 如果 **Connector Group**（連接器群組）中的所有 **Connectors**（連接器）都已啟動，狀態 **Status**（狀態）為 **Up**（啟動）（綠色）。
- 如果所有 **Connectors**（連接器）都已關閉，狀態為 **Down**（關閉）（紅色）。
- 如果一些連接器已啟動，一些已關閉，則狀態為 **Status**（狀態）為 **Partially Up**（部分啟動）（橘色）。
- 已停用的連接器顯示為灰色。

 ©2025 Palo Alto Networks, Inc.




**ZTNA** 連接器狀態

檢視所有已設定的連接器的摘要，包括與連接器相關聯的應用程式目標和 **Status**（狀態）。

選取任何 **Connector Name**（連接器名稱），以查看有關相關聯連接器群組以及與每個連接器相關聯的應用程式目標的詳細資訊。

## 檢視和監控 ZTNA 連接器存取物件

| 這可在何處使用？ | 我需要什麼？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

了解透過 ZTNA 連接器存取物件新增的私人應用程式，方法是檢視如下資料：FQDN、IP 子網路和萬用字元新增的應用程式數目、每個存取物件的連線狀態，以及與每個存取物件相關聯的連接器群組和連接器。透過檢視此資訊，您可以得到部署的健康情況與連線全貌。

資料中心的私人應用程式會透過您的連接器虛擬機器 (VM) 連線到 Prisma Access。您可以根據這些存取物件（FQDN、FQDN 萬用字元或 IP 子網路）新增應用程式。

- **FQDN**—Prisma Access 將您裝載到 ZTNA 連接器的應用程式的 FQDN 解析為應用程式 IP 位址區塊中的 IP 位址。
- 萬用字元—對於萬用字元型應用程式，建立一個 FQDN 型連接器群組，然後指定要使用的萬用字元（例如，*.example.com）作為應用程式目標。當使用者存取與萬用字元相符的網站時，這些應用程式會自動進行裝載，讓您的行動使用者和遠端網路使用者可透過 ZTNA 連接器存取。

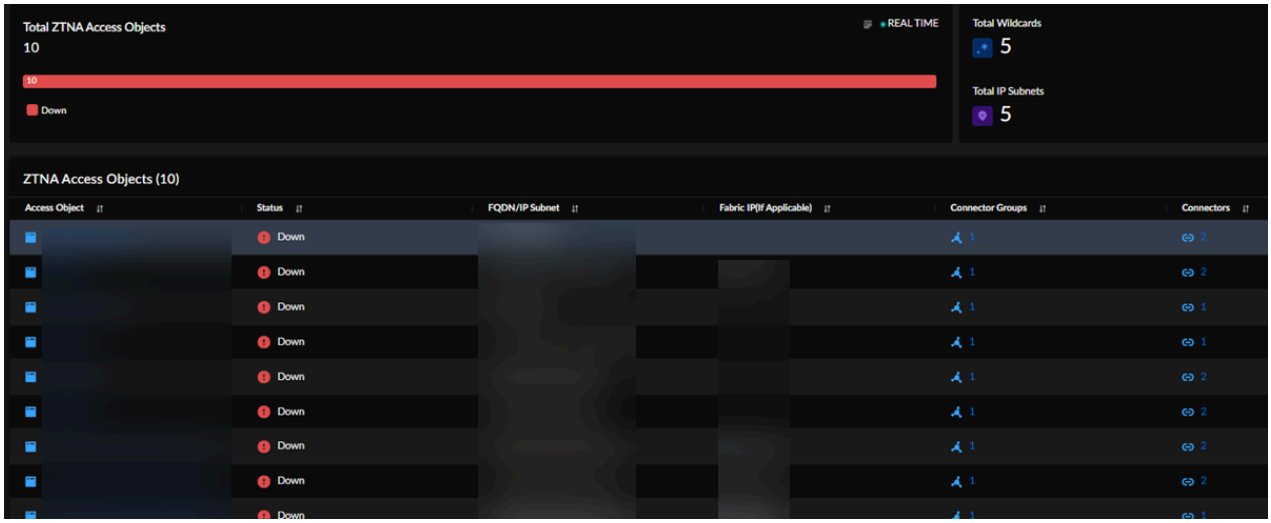
 ©2025 Palo Alto Networks, Inc.

- **IP** 子網路—建立一個 IP 子網路型連接器群組，然後輸入要用於應用程式目標的 IP 子網路。

在 Strata Cloud Manager 中，前往 **Monitor**（監控） > **Data Centers**（資料中心） > **ZTNA Access Objects**（**ZTNA** 存取物件），以了解您的 ZTNA 連接器存取物件。

所有存取物件

檢視 **Total ZTNA Access Objects**（**ZTNA** 存取物件總數），以即時檢視所有 ZTNA 連接器存取物件（FQDN、萬用字元和 IP 子網路）的相關資訊。**Total ZTNA Access Objects**（**ZTNA** 存取物件總數）和 **ZTNA Access Objects**（**ZTNA** 存取物件）表格中的數字應該相符，代表 FQDN 應用程式、子網路應用程式和探索到的萬用字元應用程式的數目。



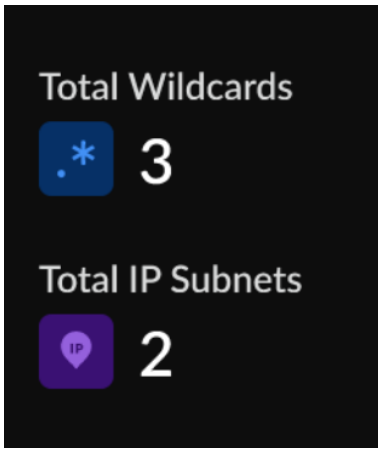

- 依狀態檢視您環境中 **Total ZTNA Access Objects**（**ZTNA** 存取物件總數）的圖形，這意味著存取物件的自動安全通道處於 Up（啟動）、Partially Up（部分啟動）、Down（關閉）或 Disabled（已停用）狀態。如果狀態為關閉，與此存取物件相關聯的連接器無法連線至您的應用程式。
  - **Up**（啟動）—所有通道都已啟動。
  - **Partially Up**（部分啟動）—一些通道已啟動，而其他通道已關閉或已停用。
  - **Down**（關閉）—所有通道都已關閉。
  - **Disabled**（已停用）—所有通道都已停用。

  在 **Total ZTNA Access Objects**（**ZTNA** 存取物件總數） Widget 中選擇一個狀態顏色方塊，以在 **ZTNA Access Objects**（**ZTNA** 存取物件）表格中依狀態對存取物件進行排序。

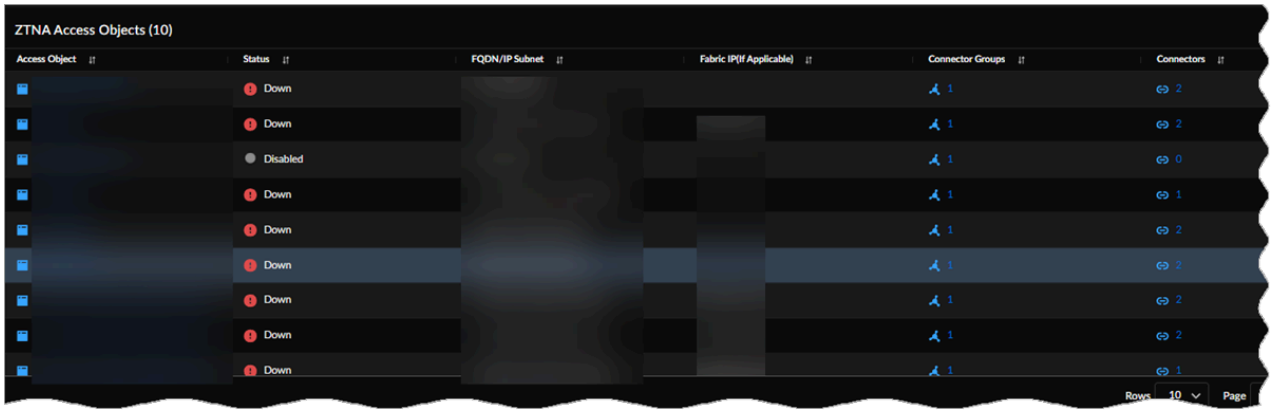



 ©2025 Palo Alto Networks, Inc.

- **Total Wildcards and Total IP Subnets**（萬用字元總數和 **IP** 子網路總數）彙總了您已裝載多少 IP 子網路和萬用字元規則。這是您建立的萬用字元規則數目，與由於建立這些規則而探索到的應用程式數目完全不同。




- **ZTNA Access Objects**（**ZTNA** 存取物件）提供有關您所有存取物件的資訊。
  - **Access Object**（存取物件）—選取特定的存取物件以檢視其詳細資訊。
  - **Status**（狀態）—存取物件的自動安全通道為 Up（啟動）、Partially Up（部分啟動）、Down（關閉）或 Disabled（已停用）。
  - **FQDN/IP Subnet**（**FQDN/IP** 子網路）—用來新增此存取物件的 FQDN 或 IP 子網路。
  - **Fabric IP (If Applicable)**（網狀架構 **IP**（如果適用））—與此存取物件相關聯的網狀架構 IP。
  - **Connector Groups**（連接器群組）—連接器群組是連接器和應用程式的邏輯分組。檢視與存取物件相關聯的連接器群組。
  - **Connectors**（連接器）—連接器代表在連線至 Prisma Access 的資料中心執行的 VM。檢視與存取物件相關聯的連接器。

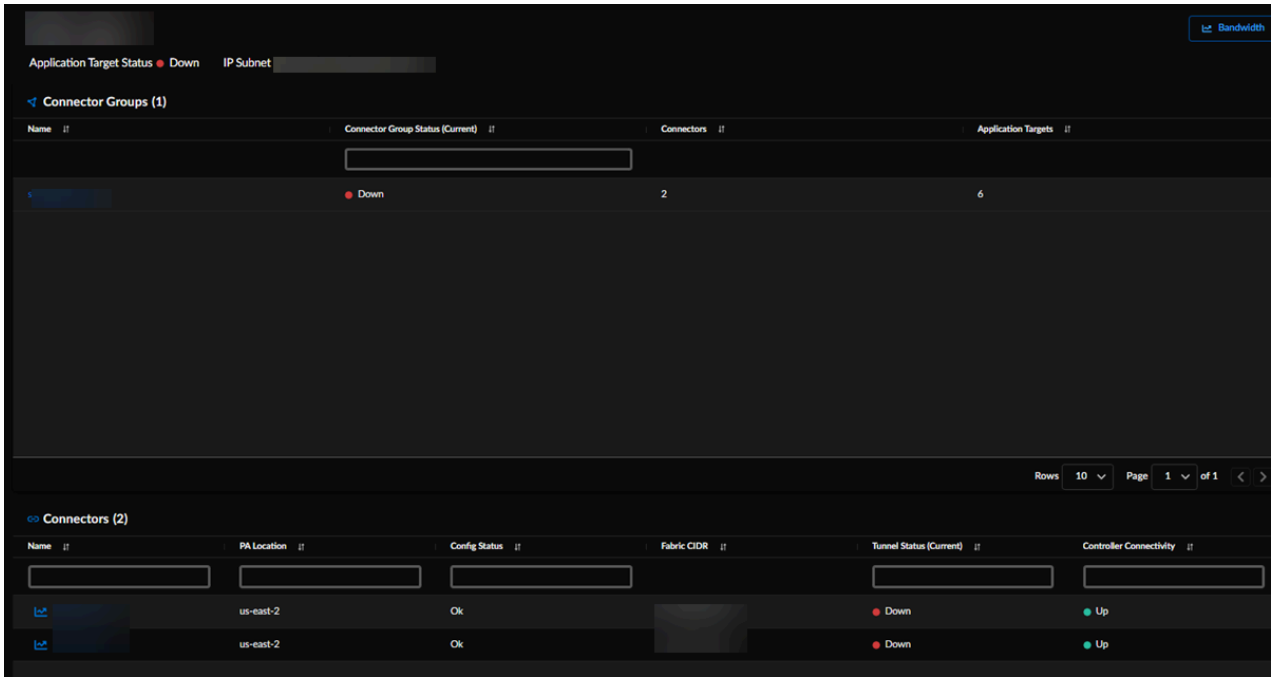



選擇任何 **Access Object**（存取物件）以檢視其詳細資訊。

- **Connector Groups**（連接器群組）—查看多少連接器群組與此存取物件相關。選取一個連接器群組以檢視其服務連線的相關資訊。
- **Connector Group Status (Current)**（連接器群組狀態（目前））—Up（啟動）、Partially Up（部分啟動）、Down（關閉）或 Disabled（已停用）。

 ©2025 Palo Alto Networks, Inc.

- **Connectors**（連接器）—此連接器群組中的連接器數目。
- **Application Targets**（應用程式目標）—此連接器群組中的應用程式目標數目。
- **Bandwidth**（頻寬）—選取 **Bandwidth**（頻寬）按鈕以檢視此存取物件的頻寬資訊。



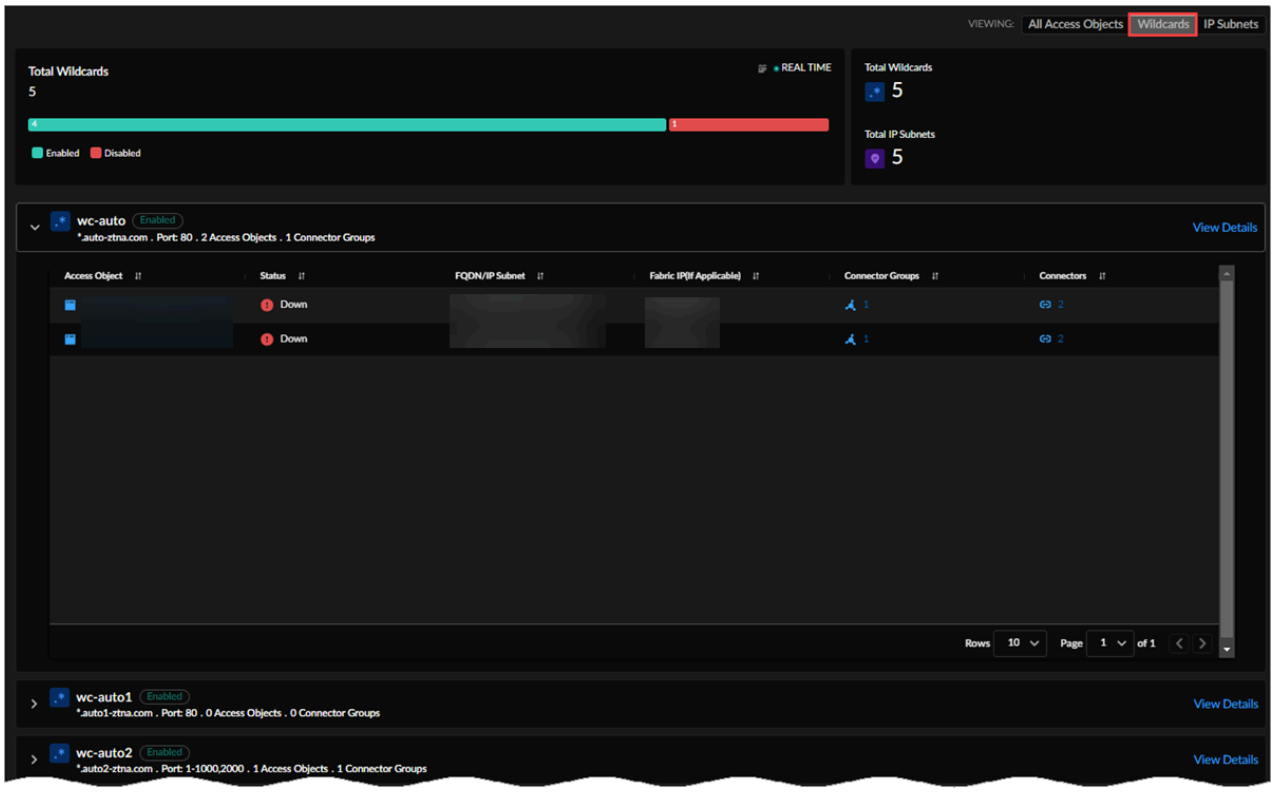

選擇任一個存取物件的 **Connectors**（連接器）以檢視其詳細資訊。

- **PA (Prisma Access) Location**（**PA (Prisma Access)** 位置）—與每個連接器相關聯的 Prisma Access 位置。
- **Config status**（設定狀態）—連接器的配置狀態為 OK（成功）或 Error（錯誤）。如果狀態為 Error（錯誤），ZTNA 連接器尚未完成裝載。
- **Fabric CIDR**（網狀架構 **CIDR**）—與此連接器相關聯的網狀架構 CIDR。
- **Tunnel Status (Current)**（通道狀態（目前））—此連接器的自動安全通道狀態。
- **Controller Connectivity**（控制器連線）—Up（啟動）、Partially Up（部分啟動）、Down（關閉）或 Disabled（已停用）。

萬用字元

選取 **Wildcards**（萬用字元）以查看您的萬用字元存取物件。檢視依狀態劃分的 **Total Wildcards**（萬用字元總數），以及 **Total Wildcards**（萬用字元總數）和 **Total IP Subnets**（**IP** 子網路總數）的數字。


©2025 Palo Alto Networks, Inc.




選取萬用字元旁邊的箭頭或選取 **View Details**（檢視詳細資訊），以取得構成此萬用字元的存取物件的相關資訊。

- **Access Object**（存取物件）—選取特定的存取物件以檢視其詳細資訊。
- **Status**（狀態）—存取物件的自動安全通道為 Up（啟動）、Partially Up（部分啟動）、Down（關閉）或 Disabled（已停用）。
- **FQDN/IP Subnet**（**FQDN/IP** 子網路）—用來新增此存取物件的 FQDN 或 IP 子網路。
- **Fabric IP (If Applicable)**（網狀架構 **IP**（如果適用））—與此存取物件相關聯的網狀架構 IP。
- **Connector Groups**（連接器群組）—連接器群組是連接器和應用程式的邏輯分組。檢視與存取物件相關聯的連接器群組。
- **Connectors**（連接器）—連接器代表在連線至 Prisma Access 的資料中心執行的 VM。檢視與存取物件相關聯的連接器。




選擇任何 **Access Object**（存取物件）以檢視其詳細資訊。

- **Connector Groups**（連接器群組）—查看多少連接器群組與此存取物件相關。選取一個連接器群組以檢視其服務連線的相關資訊。
- **Connector Group Status (Current)**（連接器群組狀態（目前））—Up（啟動）、Partially Up（部分啟動）、Down（關閉）或 Disabled（已停用）。
- **Connectors**（連接器）—此連接器群組中的連接器數目。

 ©2025 Palo Alto Networks, Inc.

- **Application Targets**（應用程式目標）—此連接器群組中的應用程式目標數目。
- **Bandwidth**（頻寬）—選取 **Bandwidth**（頻寬）按鈕以檢視此存取物件的頻寬資訊。

選取 **Connector Groups**（連接器群組）或 **Connectors**（連接器），以查看與萬用字元中存取物件相關聯的唯一連接器群組或連接器。

**IP** 子網路

選取 **IP Subnets**（**IP** 子網路）以查看您的 IP 子網路存取物件總數。一個 IP 子網路存取物件包含數個不同應用程式的分組。

依狀態（Up（啟動）、Partially Up（部分啟動）、Down（關閉）或 Disabled（已停用））檢視您環境中的 **Total IP Subnets**（**IP** 子網路總數）。

**IP Subnet ZTNA Access Objects**（**IP** 子網路 **ZTNA** 存取物件）提供所有存取物件的相關資訊。

- • **Access Object**（存取物件）—選取特定的存取物件以檢視其詳細資訊。
  - **Status**（狀態）—Up（啟動）、Partially Up（部分啟動）、Down（關閉）或 Disabled（已停用）。
  - **IP Subnet**（**IP** 子網路）—用來新增此存取物件的 IP 子網路。
  - **Connector Groups**（連接器群組）—連接器群組是連接器和應用程式的邏輯分組。檢視與存取物件相關聯的連接器群組。
  - **Connectors**（連接器）—連接器代表在連線至 Prisma Access 的資料中心執行的 VM。檢視與存取物件相關聯的連接器。




選擇任何 **Access Object**（存取物件）以檢視其詳細資訊。

- **Connector Groups**（連接器群組）—查看多少連接器群組與此存取物件相關。選取一個連接器群組以檢視其服務連線的相關資訊。
- **Connector Group Status (Current)**（連接器群組狀態（目前））—Up（啟動）、Partially Up（部分啟動）、Down（關閉）或 Disabled（已停用）。
- **Connectors**（連接器）—此連接器群組中的連接器數目。
- **Application Targets**（應用程式目標）—此連接器群組中的應用程式目標數目。
- **Bandwidth**（頻寬）—選取 **Bandwidth**（頻寬）按鈕以檢視此存取物件的頻寬資訊。

選取 **Connector Groups**（連接器群組）或 **Connectors**（連接器），以查看與IP 子網路中存取物件相關聯的唯一連接器群組或連接器。


©2025 Palo Alto Networks, Inc.

# 檢視和監控網路服務

| 這可在何處使用？ | 我需要什麼？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ 這是 Prisma Access Insights 功能。 |

您可以檢視對存取應用程式的使用者體驗造成影響的常用網路服務的效能。網路服務包括報告 GlobalProtect 驗證成功和失敗的次數，作為行動使用者能夠連線至 Prisma Access 的衡量標準，以及顯示在您指定的時間範圍期間轉送至伺服器的 DNS Proxy 要求和回應。

## GlobalProtect 驗證

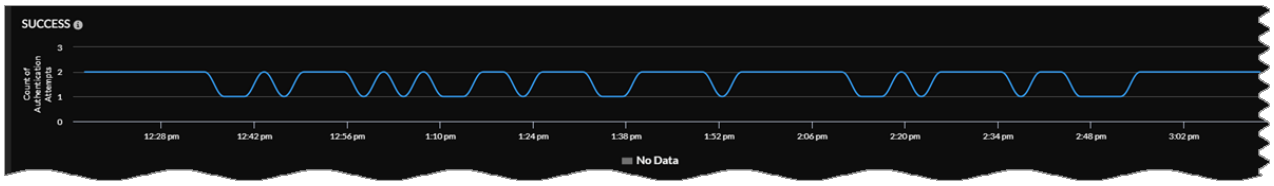
前往 Strata Cloud Manager 中的 **Monitor**（監控） > **Network Services**（網路服務） > **GlobalProtect Authentication**（**GlobalProtect** 驗證），以查看影響您環境的 GlobalProtect 認證成功和失敗。

- 設定 **Time Range**（時間範圍） 篩選器以檢閱該時間範圍的網路服務資料。
- 指定一個 **Prisma Access Location**（位置），以檢視其在所選時間範圍內的驗證成功數、失敗總數、逾時失敗數。

這些資料表示在特定時間內有多少行動使用者正在嘗試向 GlobalProtect 入口網站進行驗證，然後將用於驗證的行動使用者憑證傳送到內部部署 Active Directory (AD)，從而導致驗證成功或失敗。如果看到大量驗證失敗，您可以將這些失敗與網路事件關聯起來，而此網路事件指出某個位置出現問題，或內部部署驗證伺服器發生故障。這些圖表中的資料為解決網路問題的網路管理員提供了疑難排解的見解。您可以在 GlobalProtect 入口網站和閘道檢視行動使用者驗證成功或失敗趨勢的計數、使用此資料了解一段時間後驗證成功或失敗的模式，並建立在您的 Prisma Access 部署中可能正常或異常的計數範圍。例如，異常計數可能表示現有使用者由於 GlobalProtect 入口網站的可用性問題或驗證伺服器速度緩慢而無法連線到 Prisma Access。或者，異常計數可能代表大量使用者一次全部裝載至客戶的網路。

### GlobalProtect 驗證成功

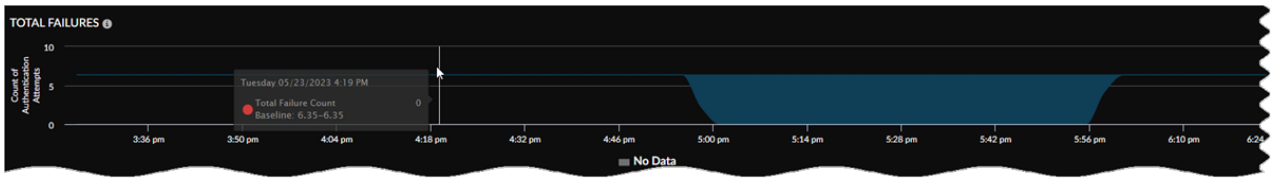
檢視 GlobalProtect 在不同位置的驗證成功計數具體資料。將游標暫留在圖形中的任意點上，即可查看有關特定時間顯示的不同 Prisma Access 位置網站上驗證成功使用者計數的詳細資訊。




### GlobalProtect 驗證失敗總數

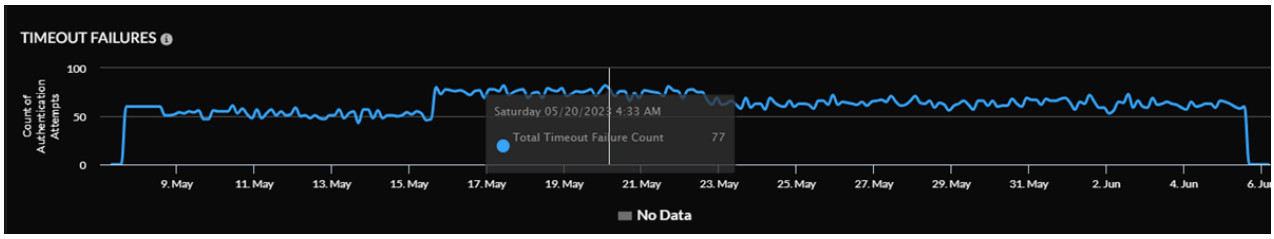
檢視 GlobalProtect 在不同位置的驗證失敗計數具體資料。將游標暫留在圖形中的任意點上，即可查看有關特定時間顯示的不同 Prisma Access 位置網站（例如美國東部和加拿大東部）上驗證失敗使用者計數的詳細資訊。


©2025 Palo Alto Networks, Inc.




**GlobalProtect** 驗證逾時失敗

檢視 GlobalProtect 在不同位置的驗證失敗計數具體資料。將游標暫留在圖形中的任意點上，即可查看有關特定時間顯示的不同 Prisma Access 位置網站（例如美國東部和加拿大東部）上驗證失敗使用者計數的詳細資訊。




## DNS

前往 Strata Cloud Manager 中的 **Monitor**（監控） > **Network Services**（網路服務） > **GlobalProtect Authentication**（**GlobalProtect** 驗證），以檢視在您指定的時間範圍期間轉送至伺服器的 DNS Proxy 要求和回應。

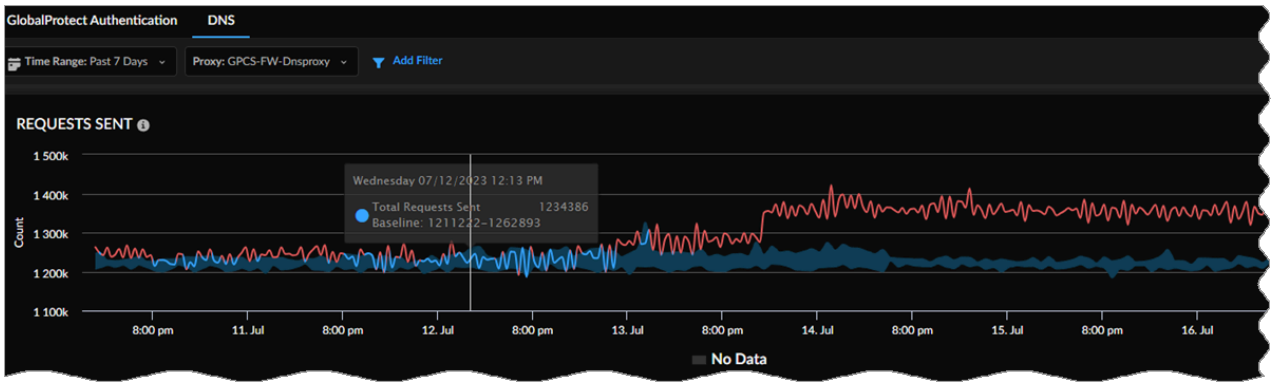
您可以使用的篩選器如下：

- 時間範圍
- **DNS Proxy** 名稱

DNS Proxy 篩選器值與最近 30 天有關，且會在您載入時自動選取（也就是說，如果沒有明確 Proxy 資料，則沒有明確 Proxy 篩選器）。將游標暫留在圖形上，即可查看有關在特定時間 DNS Proxy 所有 **Requests Sent**（已傳送的要求）和 **Requests Received**（收到的要求）的詳細資訊。

已傳送的要求

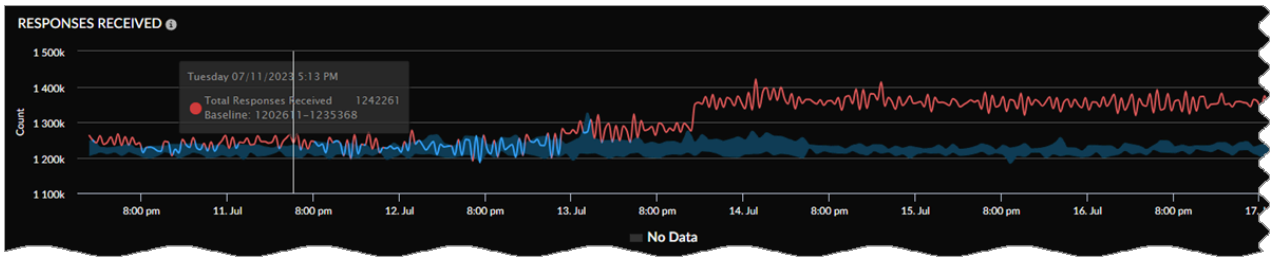
檢視在您指定的時間範圍轉送到伺服器的網路要求和查詢。將游標暫留在圖形中的任意點上，即可查看當時傳送到 DNS Proxy 伺服器的要求的相關資訊。如果您選取了要篩選的 Proxy 名稱，則會看到該 Proxy 的資料。




 ©2025 Palo Alto Networks, Inc.

收到的回應

檢視在您指定的時間範圍期間跨租用戶收到的回應總數。將游標暫留在圖形中的任意點上，即可查看當時收到的回應的相關資訊。如果您選取了要篩選的 Proxy 名稱，則會看到該 Proxy 的資料。




## 檢視和監控網路服務：GlobalProtect 驗證

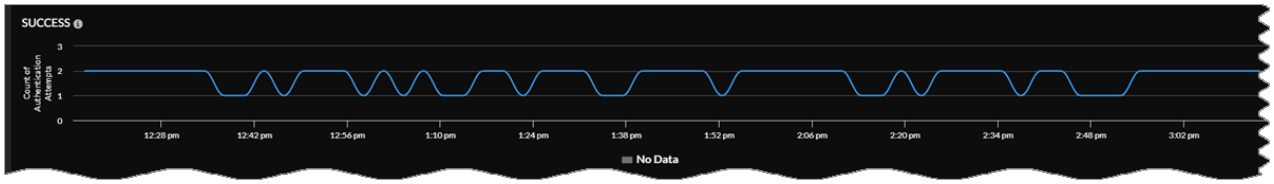
| 這可在何處使用？ | 我需要什麼？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ 這是 Prisma Access Insights 功能。 |

網路服務包括報告 GlobalProtect 驗證成功和失敗的次數，作為行動使用者能夠連線至 Prisma Access 的衡量標準。首先，在 Strata Cloud Manager 中選取 **Monitor**（監控） > **Network Services**（網路服務） > **GlobalProtect Authentication**（**GlobalProtect** 驗證）。

- 設定 **Time Range**（時間範圍） 篩選器以檢閱該時間範圍的網路服務資料。
- 指定一個 **Prisma Access Location**（位置），以檢視其在所選時間範圍內的驗證成功數、失敗總數、逾時失敗數。

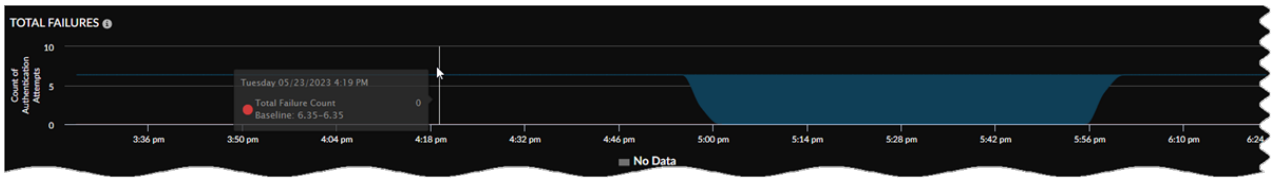
### GlobalProtect 驗證成功

檢視 GlobalProtect 在不同位置的驗證成功計數具體資料。將游標暫留在圖形中的任意點上，即可查看有關特定時間顯示的不同 Prisma Access 位置網站上驗證成功使用者計數的詳細資訊。




### GlobalProtect 驗證失敗總數

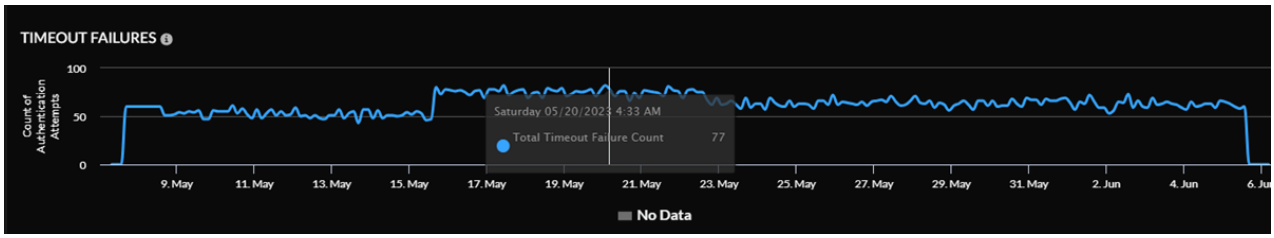
檢視 GlobalProtect 在不同位置的驗證失敗計數具體資料。將游標暫留在圖形中的任意點上，即可查看有關特定時間顯示的不同 Prisma Access 位置網站（例如美國東部和加拿大東部）上驗證失敗使用者計數的詳細資訊。




 ©2025 Palo Alto Networks, Inc.

### GlobalProtect 驗證逾時失敗

檢視 GlobalProtect 在不同位置的驗證失敗計數具體資料。將游標暫留在圖形中的任意點上，即可查看有關特定時間顯示的不同 Prisma Access 位置網站（例如美國東部和加拿大東部）上驗證失敗使用者計數的詳細資訊。




## 檢視和監控網路服務：DNS

| 這可在何處使用？ | 我需要什麼？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ 這是 Prisma Access 洞察功能。 |

網路服務：**DNS** 顯示在您指定的時間範圍期間轉送到伺服器的 DNS Proxy 要求和回應。

您可以使用的篩選器：

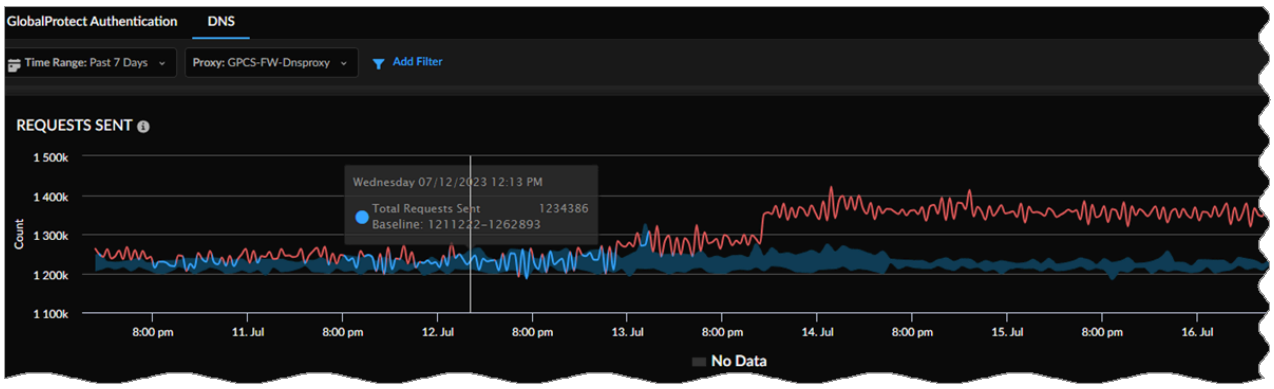
- 時間範圍
- **DNS Proxy** 名稱

DNS Proxy 篩選器值與最近 30 天有關，且會在您載入時自動選取（也就是說，如果沒有明確 Proxy 資料，則沒有明確 Proxy 篩選器）。

將游標暫留在圖形上，即可查看有關在特定時間 DNS Proxy 所有 **Requests Sent**（已傳送的要求）和 **Requests Received**（收到的要求）的詳細資訊。

已傳送的要求

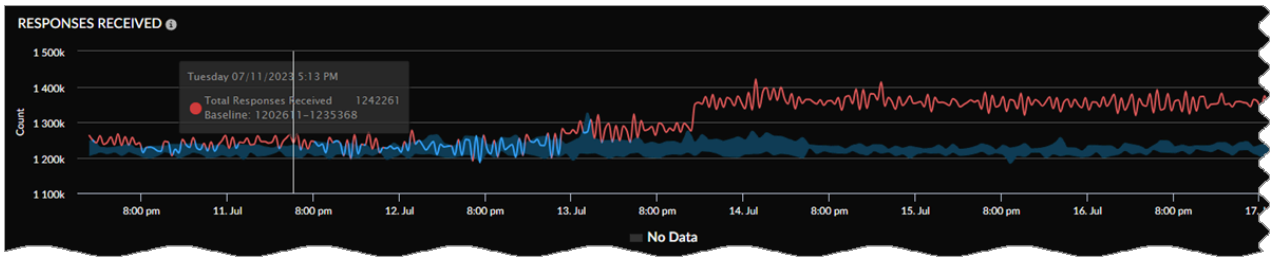
檢視在您指定的時間範圍轉送到伺服器的網路要求和查詢。將游標暫留在圖形中的任意點上，即可查看當時傳送到 DNS Proxy 伺服器的要求的相關資訊。如果您選取了要篩選的 Proxy 名稱，則會看到該 Proxy 的資料。




 ©2025 Palo Alto Networks, Inc.

收到的回應

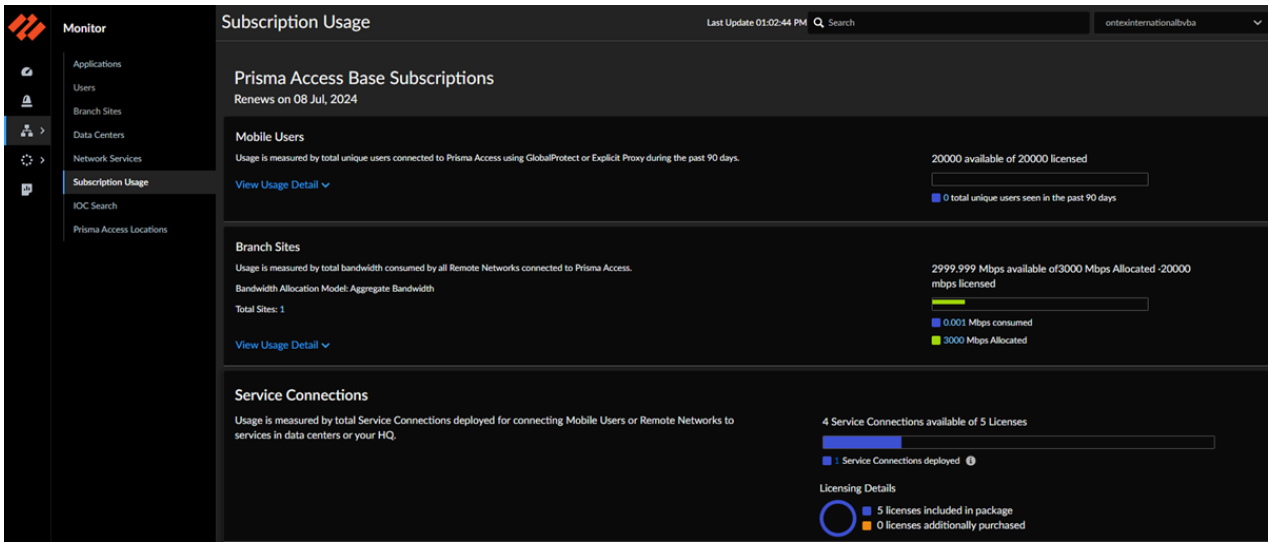
檢視在您指定的時間範圍期間跨租用戶收到的回應總數。將游標暫留在圖形中的任意點上，即可查看當時收到的回應的相關資訊。如果您選取了要篩選的 Proxy 名稱，則會看到該 Proxy 的資料。




# 檢視訂閱使用情況

| 這可在何處使用？ | 我需要什麼？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

選取 **Monitor**（監控） > **Subscription Usage**（訂閱使用情況），以檢視有關 **Prisma Access Base Subscriptions**（基礎訂閱）的詳細資訊，包括您迄今為止已耗用的授權數目。

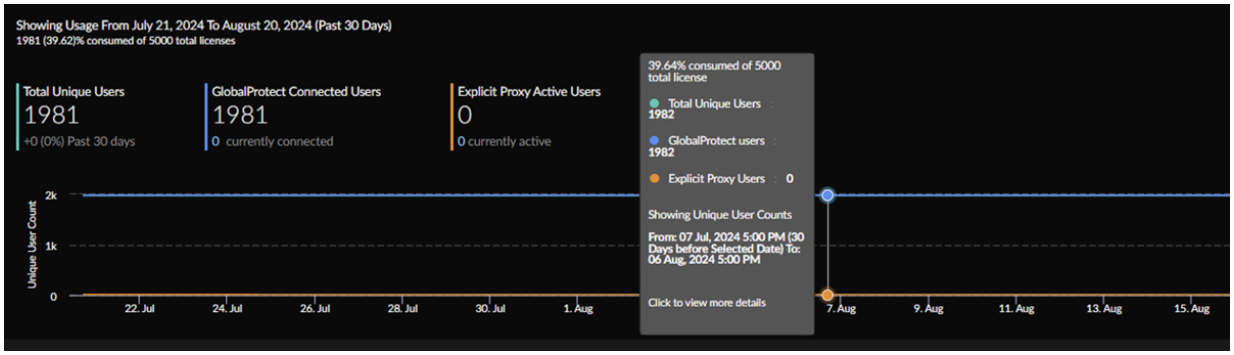



- **Mobile Users**（行動使用者）—檢視您到目前為止已耗用多少唯一的 **Mobile Users**（行動使用者）授權。此 Widget 會顯示連線至 Prisma Access 的唯一行動使用者在過去 30 天內耗用的授

 ©2025 Palo Alto Networks, Inc.

權總數，因為授權使用是以過去 30 天的 Prisma Access 登入資料為準的。過去 30 天內至少曾登入 Prisma Access 一次的使用者，會消耗一個行動使用者授權。

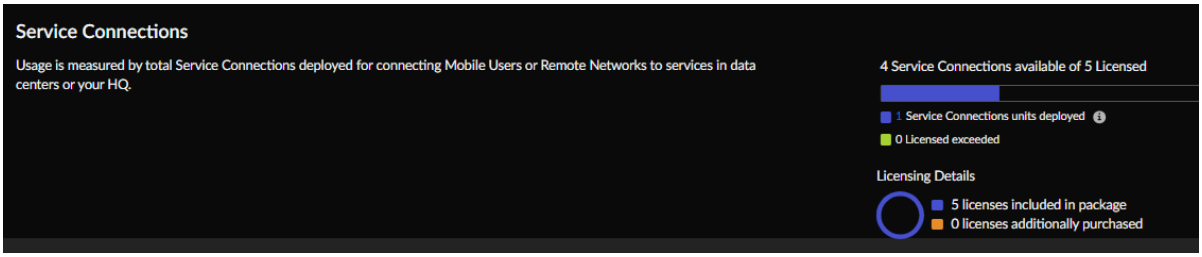
選取 **View Usage Detail**（檢視使用情況詳細資訊），以查看過去 30 天期間有關授權使用的詳細資訊。您可以檢視過去 30 天期間的唯一使用者總數、GlobalProtect 連線使用者總數，以及明確 Proxy 作用中使用者總數。將游標暫留在圖形上，即可查看當時耗用的授權。




- **Branch Sites**（分支網站）—查看所有連線至 Prisma Access 的遠端網路的總頻寬使用量。檢視您配置了多少頻寬，以及耗用了多少頻寬（以 Mbps 為單位）。您可以按所有連線至 Prisma Access 的遠端網路所耗用的總頻寬，來查看使用量。

  選取 **View Usage Detail**（檢視使用情況詳細資訊），根據您的頻寬配置模型依計算地區或分支網站查看授權頻寬消耗。在每種情況下，都會針對授權所考慮的 30 天中的每一天指示每日峰值頻寬消耗值。您可以透過選取計算地區或分支網站來篩選圖形檢視。圖表中每個計算地區或每個網站繪製了三條線，指示每日峰值消耗值、配置給計算地區或網站的頻寬，以及從每日峰值獲得的第 95 個百分位數值。

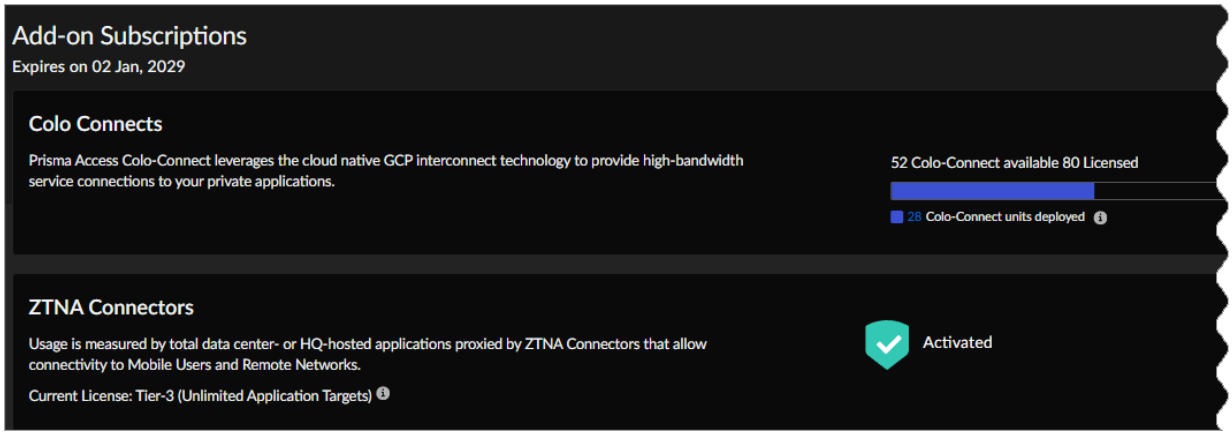
- **Service Connections**（服務連線）—查看您到目前為止已耗用多少 **Service Connections**（服務連線）授權。



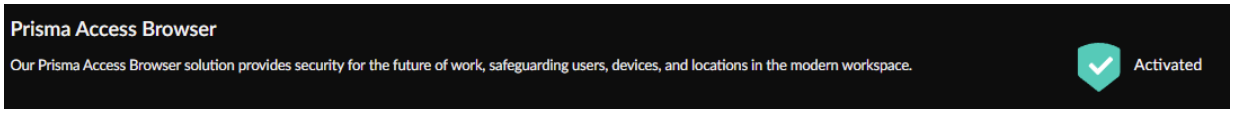

請參閱本頁面上的 **Add-On Subscriptions**（附加元件訂閱）區段，查看您已購買的附加元件授權。您可以查看已購買的授權總數，以及迄今為止未使用的授權數量。下列影像描述了您可以購買的一些附加元件授權。

 ©2025 Palo Alto Networks, Inc.

- **Colo-Connects**—Prisma Access Colo-Connect 利用雲端原生 GCP 技術，為您的私人應用程式提供高頻寬服務連線。




- **Prisma Access Browser**—Prisma Access Secure Enterprise Browser（Prisma Access Browser）是唯一可同時保護受管理和未受管理裝置的解決方案，其工具為原生整合、可將保護延伸至未受管理裝置的企業瀏覽器。Prisma Access Browser 透過在瀏覽器中放置安全性來保護業務應用程式和資料。您的 Prisma Access Browser 訂閱將出現在 **Add-on Subscriptions**（附加元件訂閱）或 **Prisma Access Base Subscriptions**（**Prisma Access** 基礎訂閱）中。
  - **Prisma Access Base Subscriptions**（**Prisma Access** 基礎訂閱）—租用戶具有 Prisma Access Browser 獨立授權。
  - **Add-on Subscriptions**（附加元件訂閱）—當您為所有行動使用者購買了 Prisma Access Browser 授權時，Prisma Access Browser 訂閱即會處於 **Activated**（已啟動）狀態。




# 檢視和監控 Prisma Access 位置

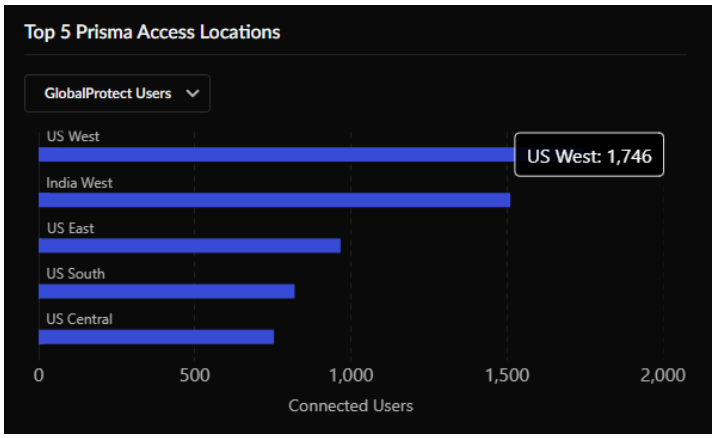
| 這可在何處使用？ | 我需要什麼？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ 這是 Prisma Access Insights 功能。 |

選取 **Monitor**（監控） > **Prisma Access Locations**（位置），以查看遠端網路和行動使用者的所有 Prisma Access 位置的健康情況概要。

## 前 5 個 Prisma Access 位置

根據所選時間範圍期間消耗的總頻寬，長條圖為遠端網路、服務連線、GlobalProtect 行動使用者或明確 Proxy 行動使用者（從下拉式清單中選擇）顯示有關前 5 個 Prisma Access 位置的資料。將游標暫留在任何列上，即可查看該特定位置有多少使用者。

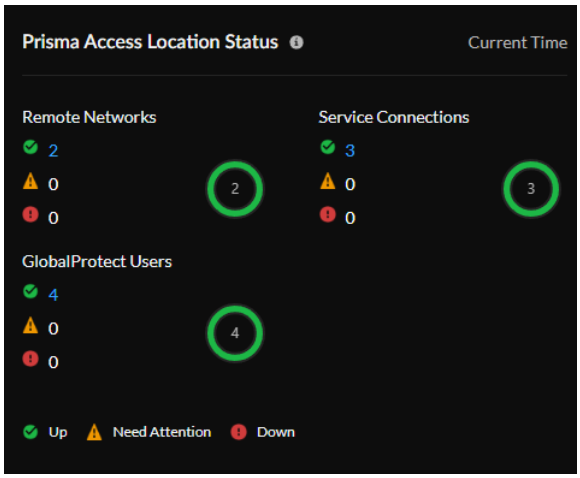

©2025 Palo Alto Networks, Inc.




## Prisma Access 位置狀態

根據您的授權，此 Widget 顯示已連線的遠端網站數目、服務連線網站數目、唯一 GlobalProtect 使用者數目，以及登入 Prisma Access 的唯一明確 Proxy 使用者數目。Widget 的顏色代碼是基於多少遠端網路、服務連線、GlobalProtect 使用者和明確 Proxy 使用者處於下列狀態：

- **Connected**（已連線）（綠色）—所有 Prisma Access 位置已連線。
- **Disconnected**（已中斷連線）（紅色）—所有 Prisma Access 位置已中斷連線。
- **Partially Connected**（已部分連線）（橘色）—一或多個 Prisma Access 位置已中斷連線。




## Strata Logging Service 連線

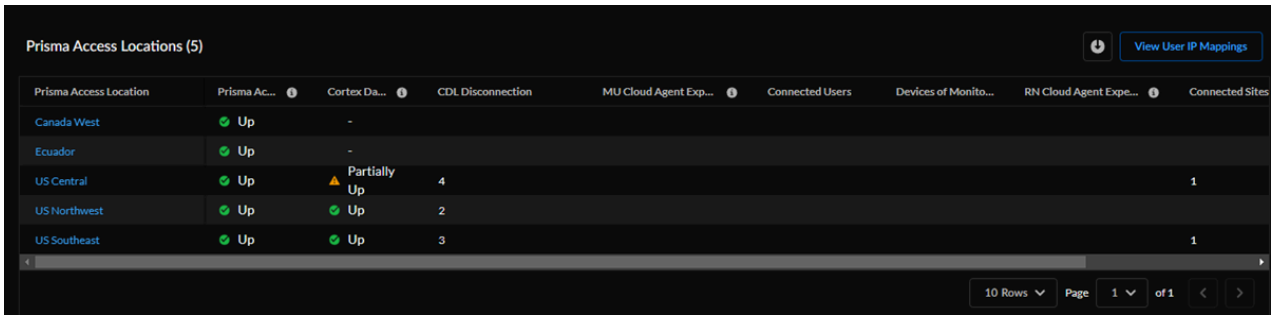
**Strata Logging Service Connectivity**（連線）Widget 讓您可以了解來自 Strata Logging Service 區域所有 Prisma Access 執行個體的 Strata Logging Service 連線健康情況狀態，此區域是您在 Prisma Access 授權啟動期間選取的。它可以協助您確定防火牆是否已與 Strata Logging Service 中斷連線，並且您不再取得防火牆日誌。每個租用戶只能在其選擇的任何區域中連線到一個 Strata Logging Service。Prisma Access 每 5 分鐘輪詢一次 Strata Logging Service 資料庫，以檢查節點（行動使用者、遠端網路和服務連線）與 Strata Logging Service 資料庫之間是否連線.

## Prisma Access 位置狀態

即時檢視 **Prisma Access Locations**（位置）狀態。在特定位置內，如果使用者從多個主機登入，則該使用者會被計為單一使用者，但如果任何使用者中斷與某個位置的連線，並從另一個位置登

 ©2025 Palo Alto Networks, Inc.

入，以從兩個不同的 Prisma Access 位置登入，則該使用者會被計為兩個使用者。選取一個位置以檢視詳細資訊，例如消耗的頻寬、狀態、Strata Logging Service 連線，以及使用者 ID 和群組對應。




# 檢視和監控第三方 Device-ID

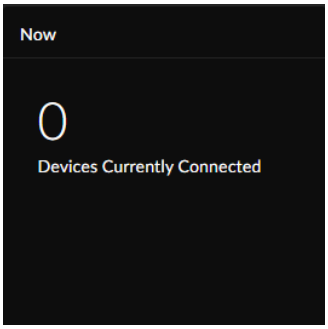
| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

您可以使用雲端識別引擎搭配 Prisma Access，套用來自第三方 IoT 偵測來源的資訊，以簡化網路中裝置識別和封閉安全性間距的工作。如需設定的詳細資訊，請參閱在 Prisma Access 中設定第三方 Device-IDD。

前往 **Monitor**（監控） > **Devices**（裝置） > **IOT**，洞察您的 IoT 裝置，例如過去 30 分鐘內連線的 IoT 裝置數目、所選時間範圍期間連線的所有 IoT 裝置，以及有關所有連線 IoT 裝置的詳細資訊。

## 目前連線的裝置

檢視過去 30 分鐘已連線的裝置數目（如果有的話）。**Now**（現在）一律僅顯示過去 30 分鐘 **Devices Currently Connected**（目前已連線的裝置）。




## 已連線的 IoT 裝置

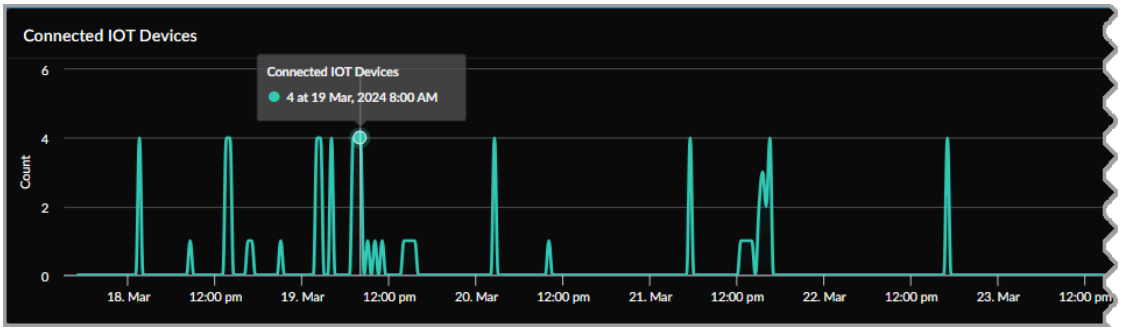
**Connected IoT Devices**（已連線的 **IoT** 裝置）顯示已透過 **Time Range**（時間範圍）篩選的已連線裝置數目。從 **Add Filters**（新增篩選器）下拉式清單中選取其他篩選器選項來自訂顯示的資料。

- **Category**（類別）—此裝置所屬的類別。


©2025 Palo Alto Networks, Inc.

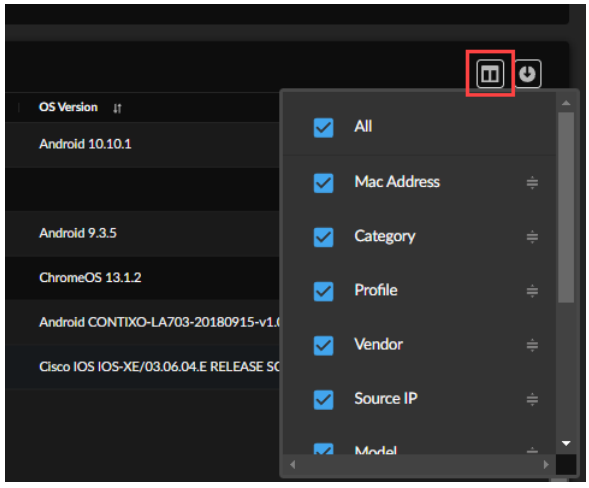
- **Mac Address**（**Mac** 位址）—裝置的 MAC 位址。
- **Profile**（設定檔）—裝置設定檔。
- **Vendor**（廠商）—裝置廠商。
- **Source IP**（來源 **IP**）—裝置的 IP 位址。
- **Prisma Access Location**（**Prisma Access** 位置）—裝置的 Prisma Access 位置。
- **Branch Site**（分支網站）—裝置所在的分支網站。

將游標暫留在圖表中的某個點上，即可查看特定時間的使用者數目。知道特定時間段的使用者趨勢可以協助您監控使用情況並調查任何異常模式。




## IoT 裝置

檢視所選 **Time Range**（時間範圍）期間連線的IoT 裝置數目。使用欄下拉式清單選取或取消選取表格中顯示的欄。

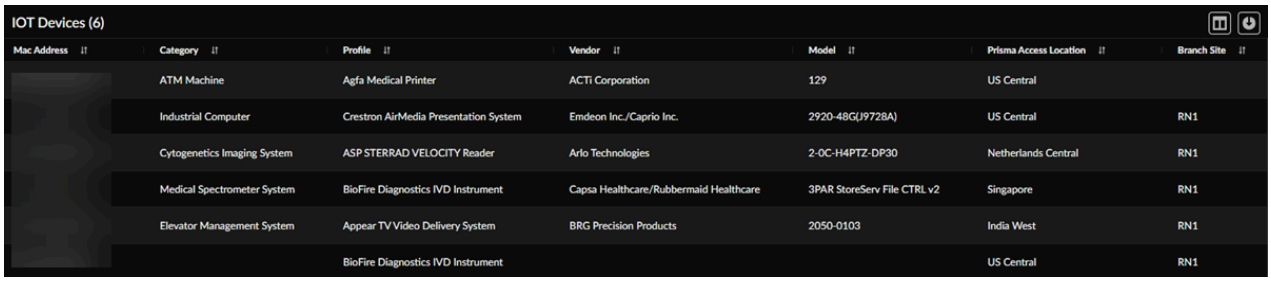



- **Mac Address**（**Mac** 位址）—裝置的 MAC 位址。
- **Category**（類別）—此裝置所屬的類別。
- **Profile**（設定檔）—裝置設定檔。
- **Vendor**（廠商）—裝置廠商。
- **Source IP**（來源 **IP**）—裝置的 IP 位址。
- **Model**（型號）—裝置型號。
- **OS Version**（作業系統版本）—作業系統版本。

 ©2025 Palo Alto Networks, Inc.

- **OS Family**（作業系統系列）—裝置所屬的作業系統系列。
- **Prisma Access Location**（**Prisma Access** 位置）—使用的 Prisma Access 位置。
- **Branch Site**（分支網站）—裝置所在的分支網站。

以下 IOT 裝置表格顯示自訂的欄選取項目。若要顯示表格中的所有欄，請在下拉式清單中選取所有選項。




# 檢視和監控遠端瀏覽器隔離

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 5.0 Innovation |

您可以使用 Strata Cloud Manager 全面了解網路流量和遠端瀏覽器隔離 (RBI)，方法是使用 Strata Cloud Manager 的 Monitor（監控）和 Workflows（工作流程）區段。透過檢視作用中 RBI 使用者數目、趨勢、連線狀態、RBI 位置狀態、流量測量和授權消耗等指標來了解您的 RBI 部署。透過檢視有關您使用者的資料，您可以得到部署的健康情況與連線全貌。

RBI 會將使用者的網際網路瀏覽活動重新導向至由 RBI 提供者託管的隔離環境。該網站是為使用者呈現的，這些使用者可在其中檢視需要的資源，而無需從其裝置和網路直接存取未知或有風險的網站。Prisma Access 可以輕易與 RBI 提供者整合，以進行此類型的瀏覽器重新導向。

 ©2025 Palo Alto Networks, Inc.

# Prisma Access 和自發 DEM

| 這可在何處使用？ | 我需要什麼？ |
| --- | --- |
| • Strata Cloud Manager Managed Prisma Access<br>• Panorama Managed Prisma Access | ❑ Prisma Access 授權<br>❑ Autonomous DEM 授權 |

開始使用 Prisma Access 中的自發 DEM，持續監控 SASE 環境中所有使用者、應用程式和遠端網站的數位體驗。只要您擁有相應的授權，就可以為連線到 Prisma Access 的 GlobalProtect 行動使用者啟用 Autonomous DEM。

- 速查表：具有 Prisma Access 的 ADEM
- 開始使用自發 DEM
- 使用自發 DEM 監控使用者流量和應用程式


©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

# Prisma Access 使用者型政策

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• Cloud Identity Engine | • Prisma Access 授權 |

Prisma Access 要求您設定 IP 位址至使用者名稱對應，為行動使用者戶和遠端網路位置的使用者一致地強制執行使用者型政策。此外，如果您想要根據群組成員資格強制執行政策，則需要設定使用者名稱至使用者群組對應。

若要在 Panorama 中建立和設定政策時，從下拉式清單中選取群組，您也可以設定 Panorama，以取得從使用者名稱至使用者群組對應中擷取的使用者群組清單。

以下幾節提供了概要和您所需執行的步驟，以設定和實作 User-ID，以及使用雲端識別引擎，在 Prisma Access 中取得 IP 位址至使用者名稱和使用者名稱至使用者群組對應。

# 為 Prisma Access 設定使用者型政策

- Strata Cloud Manager
- Panorama


©2025 Palo Alto Networks, Inc.

# Prisma Access 使用者型政策 (Strata Cloud Manager)

在整合雲端識別引擎與 Prisma Access 之後，您必須確認 Prisma Access 已連線至雲端識別引擎，且雲端識別引擎正在與 Prisma Access 共用目錄資訊。

檢查您是否可在 Prisma Access 中查看您的目錄。

前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Identity Services**（識別服務） > **Cloud Identity Engine**（雲端識別引擎）。

驗證您可將使用者和群組新增至政策規則。

選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 及 **Prisma Access**） > **Security Services**（安全性服務） > **Decryption**（解密）。

在安全性或解密政策規則中，確認 **Users**（使用者）下拉式清單顯示了您的 Active Directory 使用者和群組項目。現在，您可以開始將這些使用者和群組新增至安全性和解密政策規則。

當確認了雲端識別引擎已成功連線時，您可以開始執行使用者活動報告，以更好地查看使用者庫的行為。


©2025 Palo Alto Networks, Inc.

# Prisma Access 使用者型政策 (Panorama)

本節提供了您為 Prisma Access 設定 User-ID 所需執行的步驟。

**STEP 1 |** 為行動使用者和遠端網路位置的使用者設定 IP 位址至使用者名稱對應。

- 對於行動使用者—GlobalProtect 部署，Prisma Access 中的 GlobalProtect 代理程式會自動執行 User-ID 對應。
- 對於遠端網路的使用者，設定 User-ID 進行遠端網路部署，以將 IP 位址對應至使用者 ID。

**STEP 2 |** 為行動使用者和遠端網路位置的使用者設定使用者名稱到使用者群組對應。

對於行動使用者—GlobalProtect、明確 Proxy 和遠端網路部署，設定的目錄同步元件，以從 Active Directory (AD) 擷取使用者和群組資訊；然後在行動使用者—GlobalProtect 或遠端網路部署中設定 **Group Mapping Settings**（群組對應設定）。

或者，您可以使用 LDAP 伺服器設定檔，為行動使用者和遠端網路的使用者啟用使用者名稱到使用者群組對應。



我們建議在 *LDAP* 伺服器設定檔中使用群組包含清單，以便您可以指定要擷取的群組，而不是擷取所有群組資訊。

**STEP 3 |** 請完成下列其中一個動作，允許 Panorama 在安全性政策中使用使用者名稱到使用者群組對應：

- 設定的目錄同步元件，以從 Active Directory (AD) 擷取使用者和群組資訊；然後在行動使用者—GlobalProtect、行動使用者—明確 Proxy 或遠端網路部署中設定 **Group Mapping Settings**（群組對應設定）。
- 透過指定群組的完整識別名稱 (DN) 來設定群組型政策。

**STEP 4 |** 將 HIP 資訊重新散佈到 Panorama。


©2025 Palo Alto Networks, Inc.

# 整合雲端識別引擎與 Prisma Access

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

- Strata Cloud Manager
- Panorama

## 整合雲端識別引擎與 Prisma Access (Strata Cloud Manager)

雲端識別引擎（目錄同步）為 Prisma Access 提供對 Active Directory 資訊的唯讀存取權，讓您能夠輕鬆設定及管理使用者和群組的安全性與解密政策。

雲端識別引擎可與內部部署 Active Directory 和 Azure Active Directory 搭配運作。

若要使用 Prisma Access 設定雲端識別引擎，請先移至中樞啟動雲端識別引擎，並將其新增至 Prisma Access。然後前往 Prisma Access 來驗證 Prisma Access 能夠存取目錄資料。




©2025 Palo Alto Networks, Inc.

**STEP 1 |** 啟動雲端識別引擎

雲端識別引擎可以與中樞上任何支援的應用程式共用 Active Directory 資訊。它是免費的，且無需授權碼即可開始使用。雲端識別引擎設定包括在中樞啟動雲端識別引擎應用程式、設定雲端識別引擎代理程式以收集 Active Directory 對應，並設定雲端識別與代理程式之間的相互驗證。

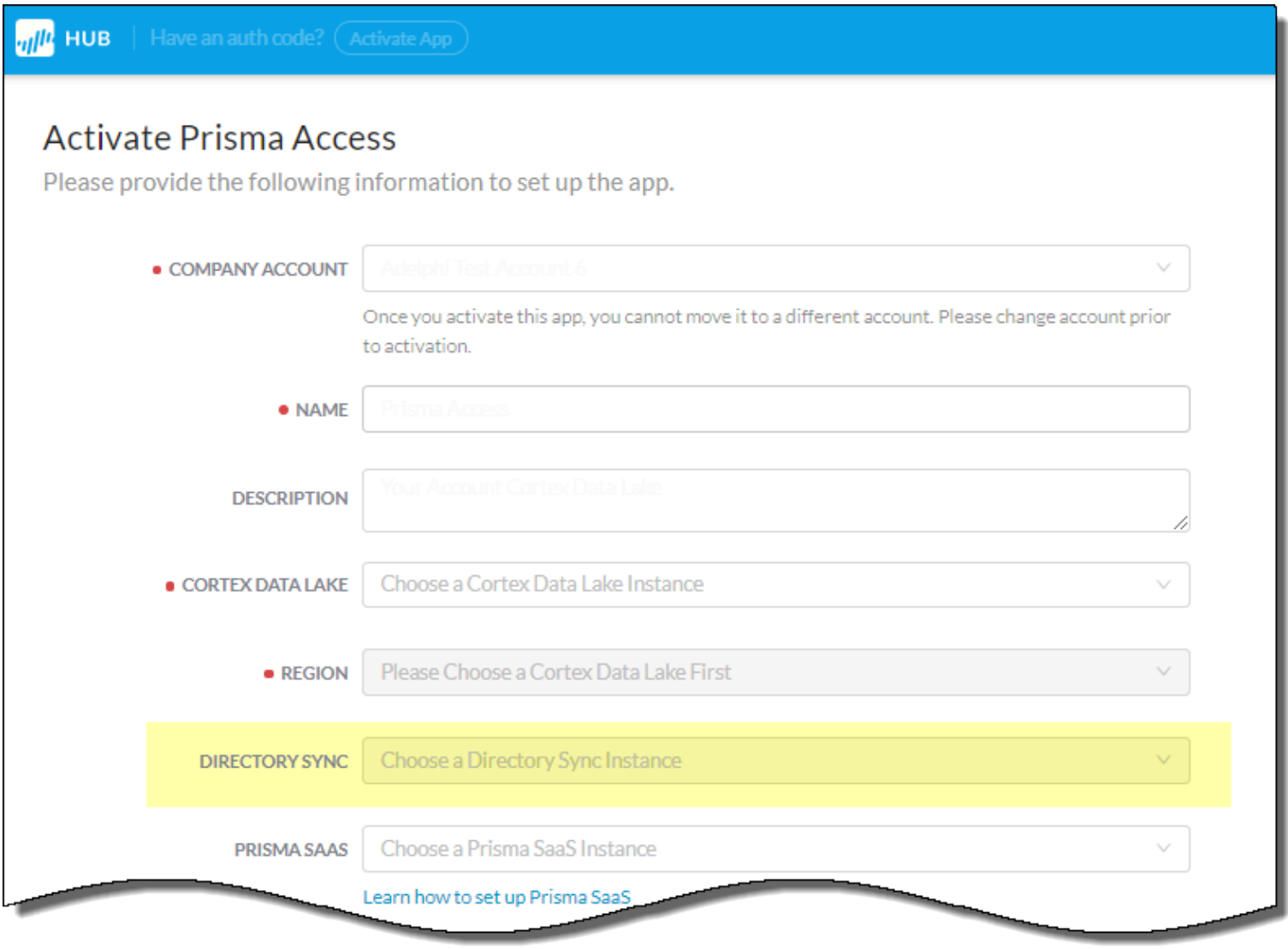
請確實將雲端識別引擎執行個體部署在先前部署 Prisma Access 和 Strata Logging Service 的相同區域中。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 為 Prisma Access 啟用雲端識別引擎。

您可以在首次啟動 Prisma Access 時或後續的任何時間，將 Prisma Access 與雲端識別引擎建立關聯：

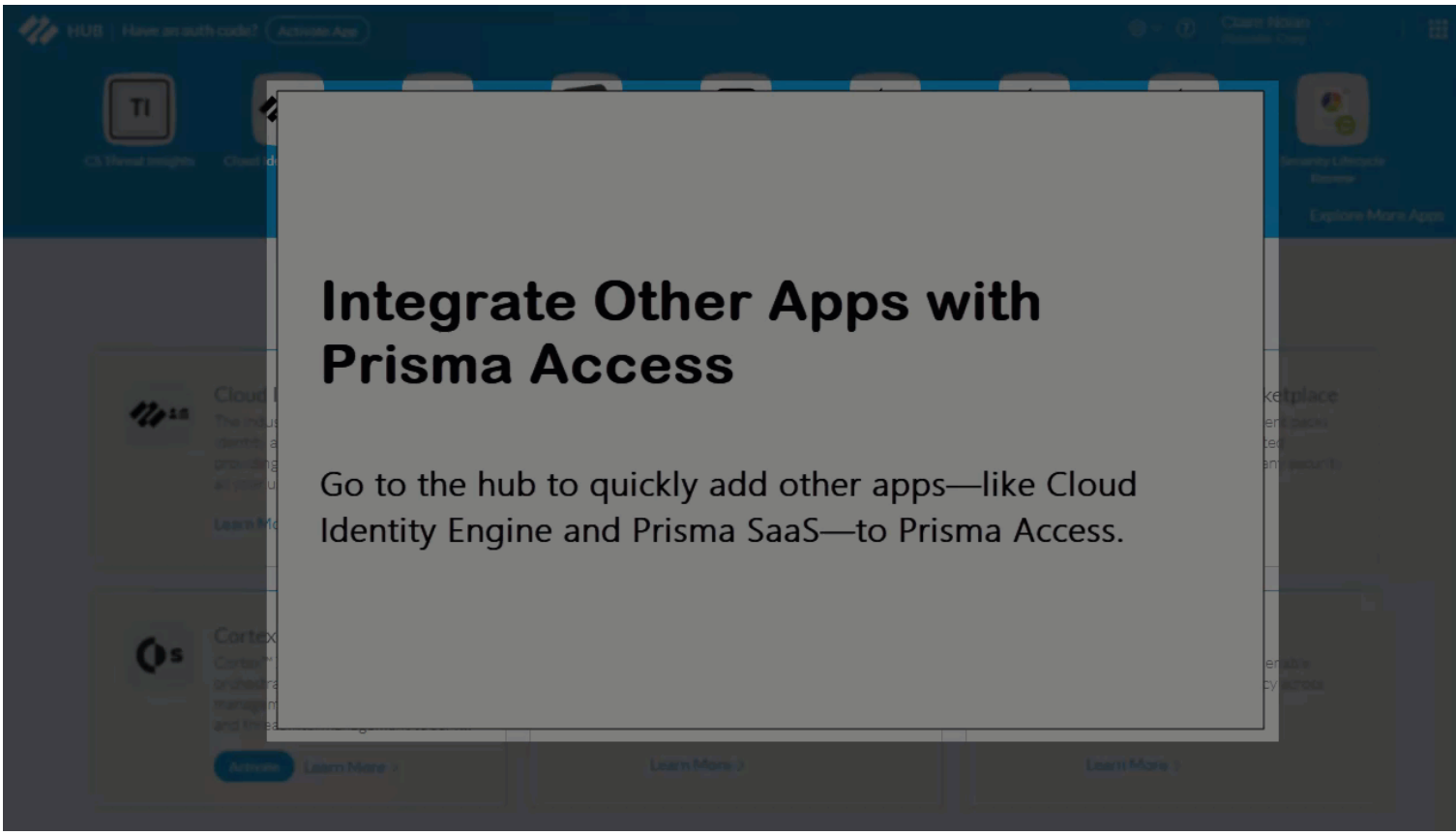
- 當您啟動 **Prisma Access** 時：首次啟動 Cloud Managed Prisma Access 時，您可以選擇一個雲端識別引擎執行個體供 Prisma Access 使用。務必選取與 Prisma Access 部署在相同區域中的執行個體。




- 在啟動了 **Prisma Access** 之後：若要為現有的 Prisma Access 執行個體啟用雲端識別引擎，請登入中樞。從中樞設定下拉式清單（請參閱頂端功能表列上的齒輪）中，選取 **Manage**


©2025 Palo Alto Networks, Inc.

**Apps**（管理應用程式）。找出您要更新的 Prisma Access 執行個體，然後選取要讓 Prisma Access 使用的雲端識別引擎執行個體。




**STEP 3 |** 確認 Prisma Access 已連線至雲端識別引擎。

## 整合雲端識別引擎與 Prisma Access (Panorama)

Prisma Access 從您組織的雲端目錄或 Active Directory (AD) 擷取使用者和群組資訊，以強制執行使用者和群組型政策。Prisma Access 選擇性地從某些雲端目錄廠商（例如 Azure Active Directory）擷取使用者行為型風險訊號，以強制執行自動化的安全性動作。您可以使用雲端識別引擎來簡化使用者和群組資訊的擷取。

除了簡化使用者和群組資訊擷取外，整合雲端識別引擎與 Prisma Access 可以釋放雲端目錄或 AD 上的頻寬和負載。

您可以透過完成下列步驟，使用雲端識別引擎為行動使用者、遠端網路或兩者擷取 Prisma Access 的使用者和群組資訊。

雲端身分引擎與 Prisma Access 整合具有下列實作限制：

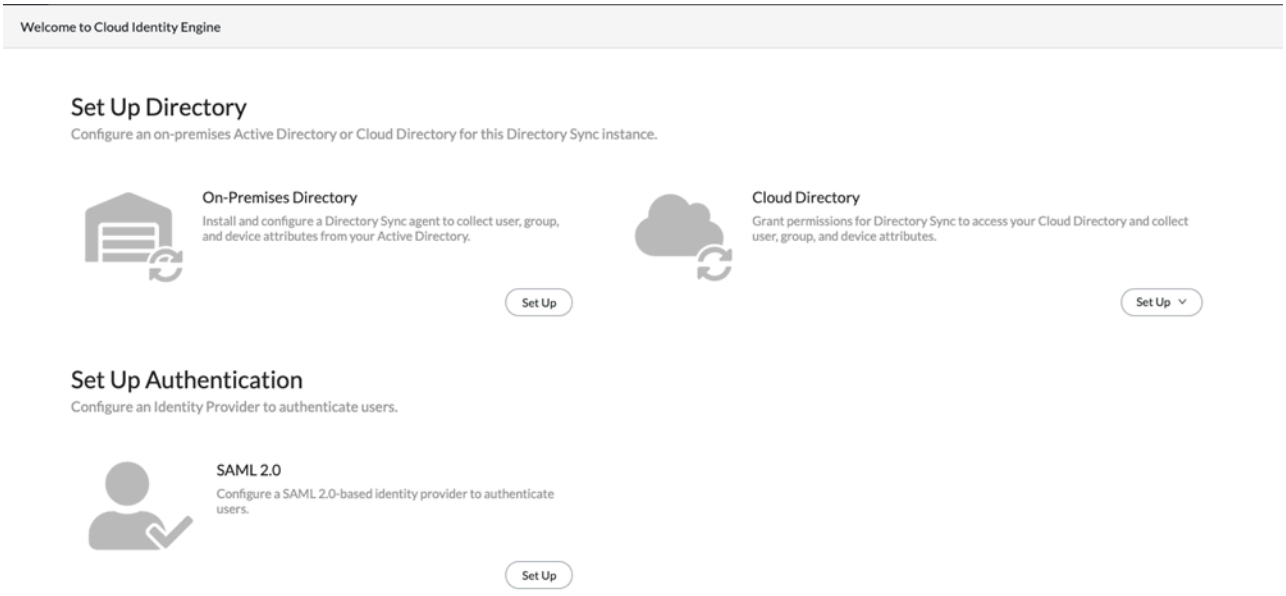

©2025 Palo Alto Networks, Inc.

- 請確定您搭配雲端識別引擎使用的群組沒有下列任何特殊字元，因為 Prisma Access 不支援在群組中使用以下特殊字元，並且提交操作將會失敗：
  - "（雙引號）
  - '（撇號）
  - <（小於符號）
  - >（大於符號）
  - &
- 如果您將雲端識別引擎與 Prisma Access 建立關聯，則您的使用者名稱必須使用包含網域的 NetBIOS 格式。您可以採用電子郵件格式 (*username*@*domain*)、**NetBIOS\sAMAccountName** 格式或使用者主體名稱 (UPN) 格式 (*username*@*domain*.com) 指定使用者名稱。
- 以 **distinguishedName** 格式輸入群組名稱（例如，**CN=Users,CN=Builtin,DC=Example,DC=com**）。
- 雲端識別引擎不會套用您在群組包括清單中指定的任何設定（**Device**（裝置） > **User Identification**（使用者識別） > **Group Mapping Settings**（群組對應設定） > **Group Include List**（群組包括清單））；相反，從您的整個組態中擷取使用者和群組資訊，包括所有裝置群組和範本中使用的群組。

**STEP 1 |** 為 Prisma Access 建立雲端識別引擎執行個體，並記下執行個體名稱。

當您啟動雲端識別引擎時，它會建立一個執行個體。在後續步驟中將雲端識別引擎與 Prisma Access 建立關聯時，您會使用執行個體名稱。或者，如果您需要建立個別的 Prisma Access 執行個體，請建立該執行個體並記下其名稱。

**STEP 2 |** 設定雲端識別引擎以擷取您的目錄資料。




**STEP 3 |** （僅使用內部部署 Active Directory 進行部署）如果您使用內部部署 Active Directory，請安裝並設定雲端識別代理程式以與內部部署 AD 通訊，並設定雲端識別引擎服務與代理程式之間的相互驗證。

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 在 Prisma Access 上啟用雲端識別引擎。

1. 在管理 Prisma Access 的 Panorama 上，選取使用者名稱到使用者群組對應設定頁籤。
   - 對於行動使用者—GlobalProtect 部署，選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users—GlobalProtect**（行動使用者—**GlobalProtect**）、選取齒輪圖示以編輯設定，然後選取 **Group Mapping Settings**（群組對應設定）。
   - 對於行動使用者—明確 Proxy 部署，選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users—Explicit Proxy**（行動使用者—明確 **Proxy**）、選取齒輪圖示以編輯設定，然後選取 **Group Mapping Settings**（群組對應設定）。
   - 對於遠端網路部署，請選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路）、選取齒輪圖示以編輯設定，然後選取 **Group Mapping Settings**（群組對應設定）。
2. 選取 **Enable Directory Sync Integration**（啟用目錄同步整合），以使用 Prisma Access 啟用雲端識別引擎。
3. 輸入下列資訊：
   - 輸入 **Primary Username**（主要使用者名稱）。此欄位為必填。

     **Primary Username**（主要使用者名稱）屬性控制日誌和報告中使用的格式。如果主要使用者名稱屬性是 **UserPrincipalName** (UPN)，則所有日誌和報告項目都會以該格式顯示來源使用者。許多部署使用 UPN、**sAMAccountName**或 **mail**（郵件）格式。如果您的組織使用另一個屬性，您可以在這裡指定它，以確保記錄和報告在整個組織的一致性。

     如果您將 Azure AD 或 Okta Directory 設定為雲端識別引擎中的識別提供者 (IdP)，請將 **Primary Username**（主要使用者名稱）指定為 **userPrincipalName**。Prisma Access 支援與 Azure AD 和 Okta Directory 搭配使用的 userPrincipalName (UPN) 屬性。
   - （選用）輸入 **E-Mail**（電子郵件）屬性（例如 **mail**（郵件））。
   - （選用）如果您將替代名稱屬性用於使用者，請輸入它們。您最多可以輸入三個替代使用者名稱（**Alternate User Name 1**（替代使用者名稱 **1**）、**Alternate User Name 2**（替代使用者名稱 **2**）和 **Alternate User Name 3**（替代使用者名稱 **3**））。
4. 完成後按一下 **OK**（確定）。

**STEP 5 |** 提交並推送（**Commit**（提交） > **Commit and Push**（提交並推送））您的變更。

 ©2025 Palo Alto Networks, Inc.

# 擷取 Prisma Access 的 User-ID 群組對應

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• Cloud Identity Engine | • Prisma Access 授權 |

在 Prisma Access 中設定 User-ID 對應之後，您需要能夠擷取行動使用者和遠端網路使用者的目前使用者名稱至使用者群組資訊。當設定雲端識別引擎中的群組對應執行使用者名稱至使用者群組對應時，這些使用者群組無法在安全性政策規則中選取。您可以將新世代防火牆設定為主要裝置或設定雲端識別引擎，來填入這些群組，以允許在安全性政策規則下拉式清單中選取它們。

- 雲端識別引擎
- 主要裝置
- 長格式識別名稱項目

## 雲端識別引擎

除了使用雲端識別引擎擷取使用者和群組資訊外，您還可以使用雲端識別引擎，在安全性政策規則中填入使用者群組名稱。此整合讓您無需基於此目的將內部部署或 VM-Series 新世代防火牆設定為主要裝置；不過，仍支援主要裝置。

您還可以使用雲端識別引擎，在 Panorama 受管理多租用戶部署中填入群組名稱，這在使用主要裝置時是不可能的。

若要啟用雲端識別引擎，在安全性政策規則中填入群組名稱，請完成以下步驟。

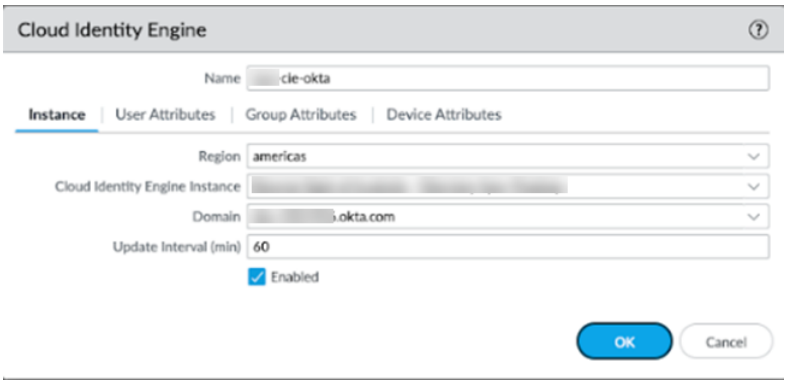
**STEP 1 |** 在雲端識別引擎中，啟動雲端識別引擎，並新增 on-premises 或 cloud-based 目錄（如果還未這樣做）。


©2025 Palo Alto Networks, Inc.

**STEP 2 |** 將雲端識別引擎設定為對應來源。

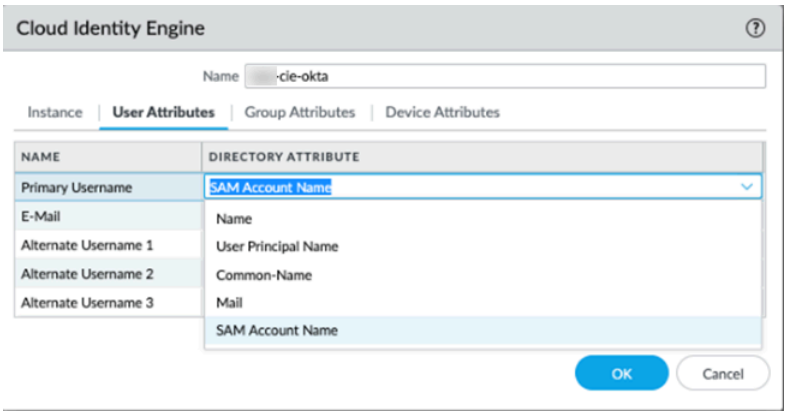
1. 從管理 Prisma Access 的 Panorama 中，選取 **Panorama** > **User Identification**（使用者識別） > **Cloud Identity Engine**（雲端識別引擎），然後 **Add**（新增）一個設定檔。
2. 對於 **Instance**（執行個體），請指定以下參數：
   - **Region**（區域）—為您的租用戶選取區域端點。

     您選取的區域必須與您啟動雲端識別引擎租用戶時所選取的區域相符。
   - **Cloud Identity Engine Instance**（雲端識別引擎執行個體）—選取要與設定檔建立關聯的雲端識別引擎執行個體。
   - 網域—選取包含您想要使用的目錄的網域。
   - **Update Interval (min)**（更新間隔（分鐘））—輸入您想要 Panorama 等待更新從雲端識別引擎應用程式到 Panorama 的分鐘數（也稱為重新整理間隔）。預設值為 60 分鐘，範圍為 5-1440。
3. 確認設定檔為 **Enabled**（已啟用）。



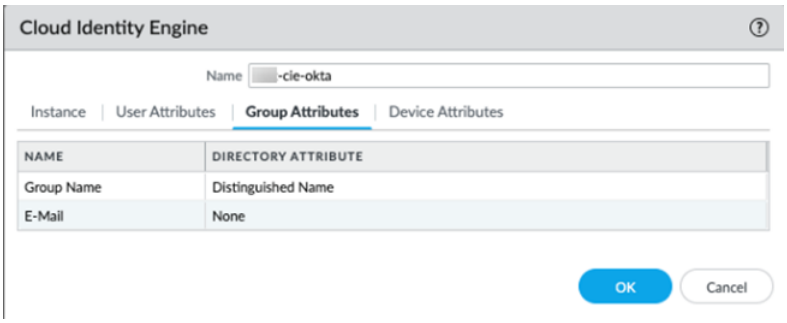

4. 對於 **User Attributes**（使用者屬性），選取 **Primary Username**（主要使用者名稱）的格式。您可以選擇性地為電子郵件和替代使用者名稱選取格式。如果您的使用者使用多個使用者名稱格式登入，您可以設定最多三種備用使用者名稱格式。

   當您在安全性政策規則中檢視使用者時，使用者名稱會以您在這裡選取的主要使用者名格式顯示。

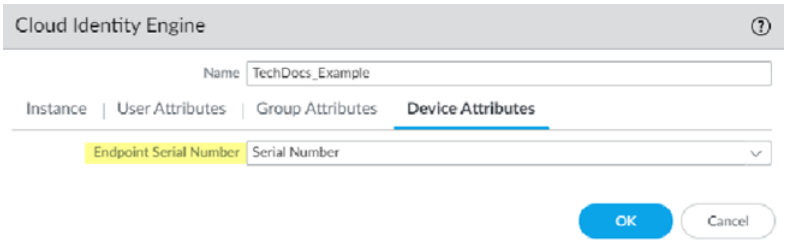



5. 對於 **Group Attributes**（群組屬性），選取 **Group Name**（群組名稱）的格式。

 ©2025 Palo Alto Networks, Inc.



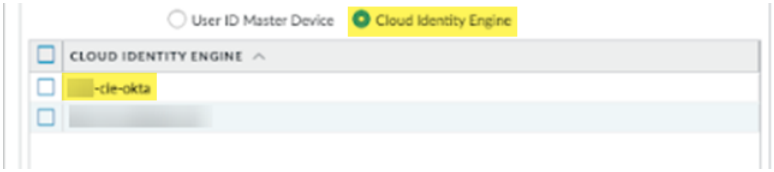

6. 將 **Device Attributes**（裝置屬性）保留為 **None**（無）。




7. 按一下 **OK**（確定），然後 **Commit and Push**（提交並推送）您的變更。

**STEP 3 |** 將您的設定檔附加到您的 Prisma Access 設定。

1. 前往您正在新增的部署的設定。
   - 對於行動使用者—GlobalProtect 部署，請選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users—GlobalProtect**（行動使用者—**GlobalProtect**），然後按一下齒輪以編輯 **Settings**（設定）。
   - 對於行動使用者—明確 Proxy 部署，請選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users—Explicit Proxy**（行動使用者—明確 **Proxy**），然後按一下齒輪以編輯 **Settings**（設定）。
   - 對於行動使用者—遠端網路部署，請選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users—Remote Networks**（行動使用者—遠端網路），然後按一下齒輪以編輯 **Settings**（設定）。
2. 選取 **Cloud Identity Engine**（雲端識別引擎）。
3. 選取您建立的雲端識別引擎設定檔。



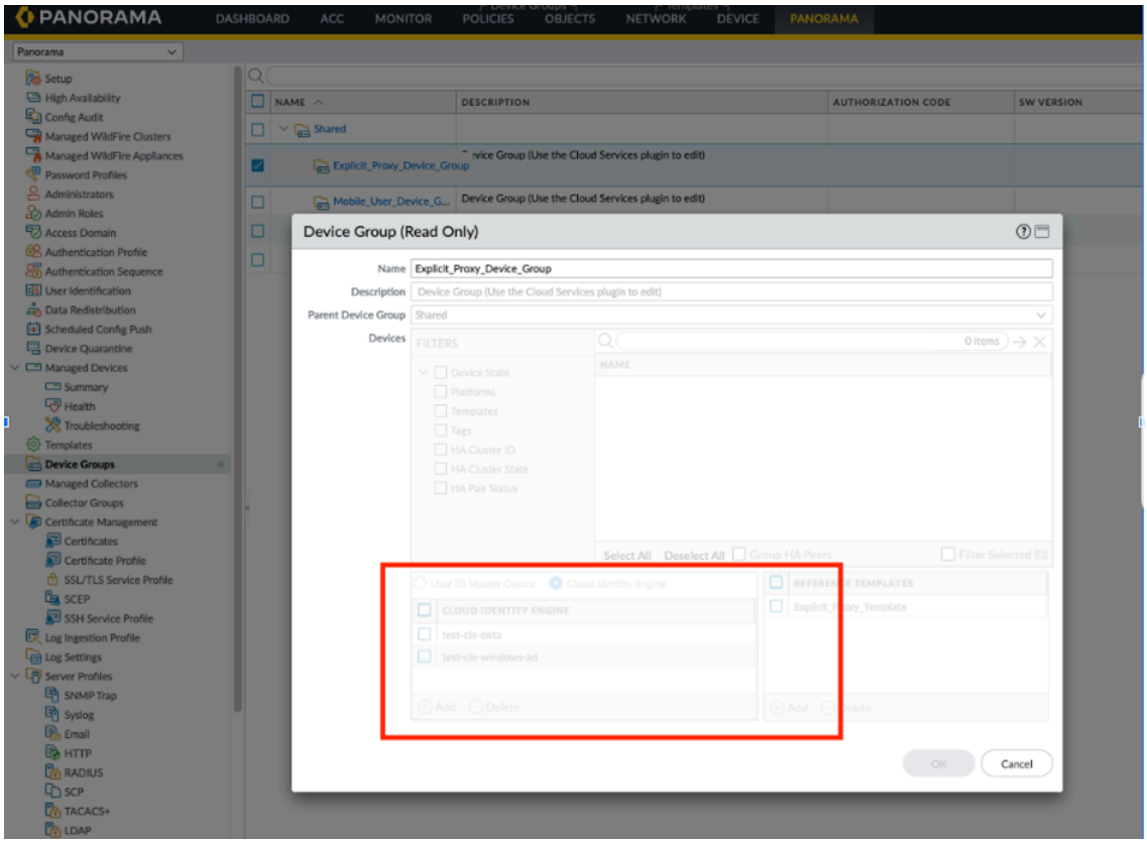

**STEP 4 |** 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**），然後 **Commit**（提交）您的變更。


©2025 Palo Alto Networks, Inc.

**STEP 5 |** 驗證 Prisma Access 是否具有來自雲端識別引擎的對應資訊。

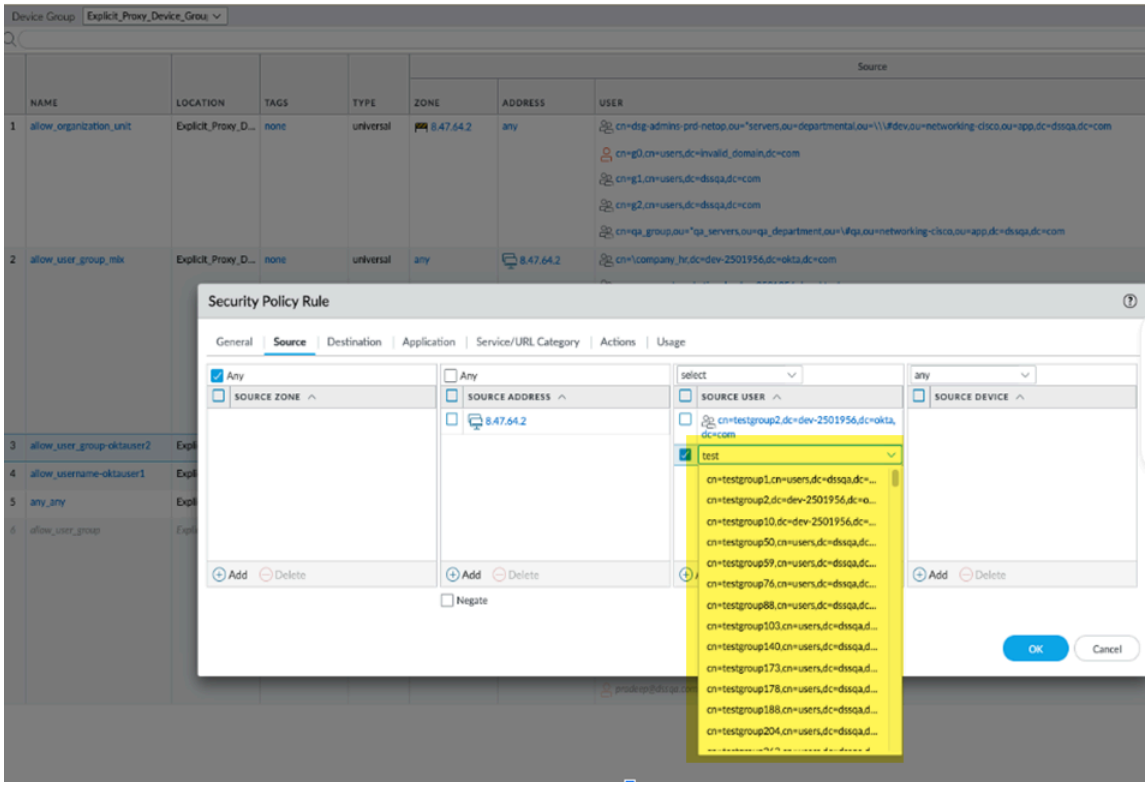
1. 選取 **Panorama** > **Device Groups**（裝置群組） > ***<template-name>***，其中 *<template-name>* 是您正在設定的部署的範本，並驗證雲端識別引擎設定檔是否已附加到裝置群組。

   以下範例顯示裝置群組已成功附加到 Explicit_Proxy_Device_Group。




2. 選取 **Objects**（物件） > **Security**（安全性） > **Pre Rules**（預先規則）、**Add**（新增）安全性政策規則，然後驗證使用者區域中是否已填入群組。

 ©2025 Palo Alto Networks, Inc.




## 主要裝置

當設定雲端識別引擎中的群組對應執行使用者名稱至使用者群組對應時，這些使用者名稱和使用者群組不會填入安全性政策中。若要簡化使用者和群組型政策的建立或修改，您可以使用主要裝置，將群組名稱新增到安全性政策規則中的下拉式清單。您需要為每個裝置群組指定一個防火牆作為主要裝置。在您新增主要裝置之後，裝置群組會繼承主要裝置上定義的所有政策；因此，它應該是一個獨立的專用裝置，用於該裝置群組。

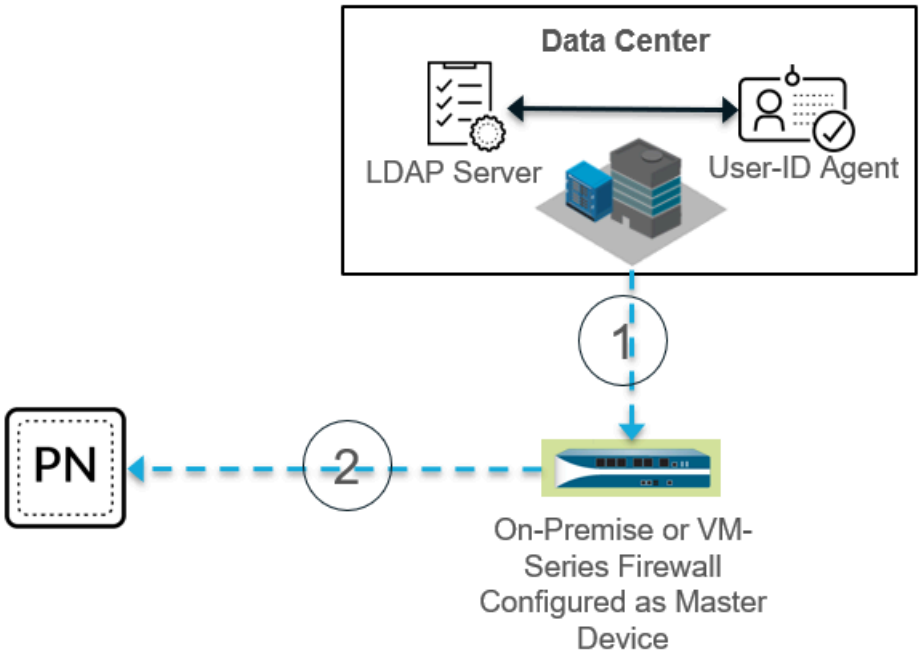
為了允許在安全政策的下拉式清單中選取群組名稱，Palo Alto Networks 建議您為每個裝置群組指定一個 **Master Device**（主要裝置）。您可以將內部部署防火牆或 VM-Series 防火牆設定為主要裝置。

下圖顯示了 User-ID 部署，其中管理員已將內部部署裝置設定為 **Master Device**（主要裝置）。圖中的標註顯示了過程。

1. 管理員已將其設定為主要裝置的新世代內部部署或 VM-Series 防火牆，可從資料中心的 LDAP 伺服器和 User-ID 代理程式中擷取最新的使用者名稱至使用者群組對應。
2. Panorama 會從主要裝置取得使用者名稱至使用者群組對應。

   Panorama 僅基於將群組名稱填入安全性政策中下拉式清單的目的使用此對應，因此簡化了根據群組建立政的過程。


©2025 Palo Alto Networks, Inc.




## 將內部部署或 VM-Series 防火牆設定為主要裝置

使用以下程序，將內部部署或 VM-Series 防火牆設定為主要裝置。

每個裝置群組只能使用一個主要裝置；如果您需要為不同的裝置群組設定主要裝置，則需要為每個裝置群組建立個別的主要裝置。

**STEP 1 |** 請確保您想要用作主要裝置的裝置由管理 Prisma Access 的同一 Panorama 所管理。

您可以在 **Panorama** > **Managed Devices**（受管理的裝置）下檢查受管理的裝置。

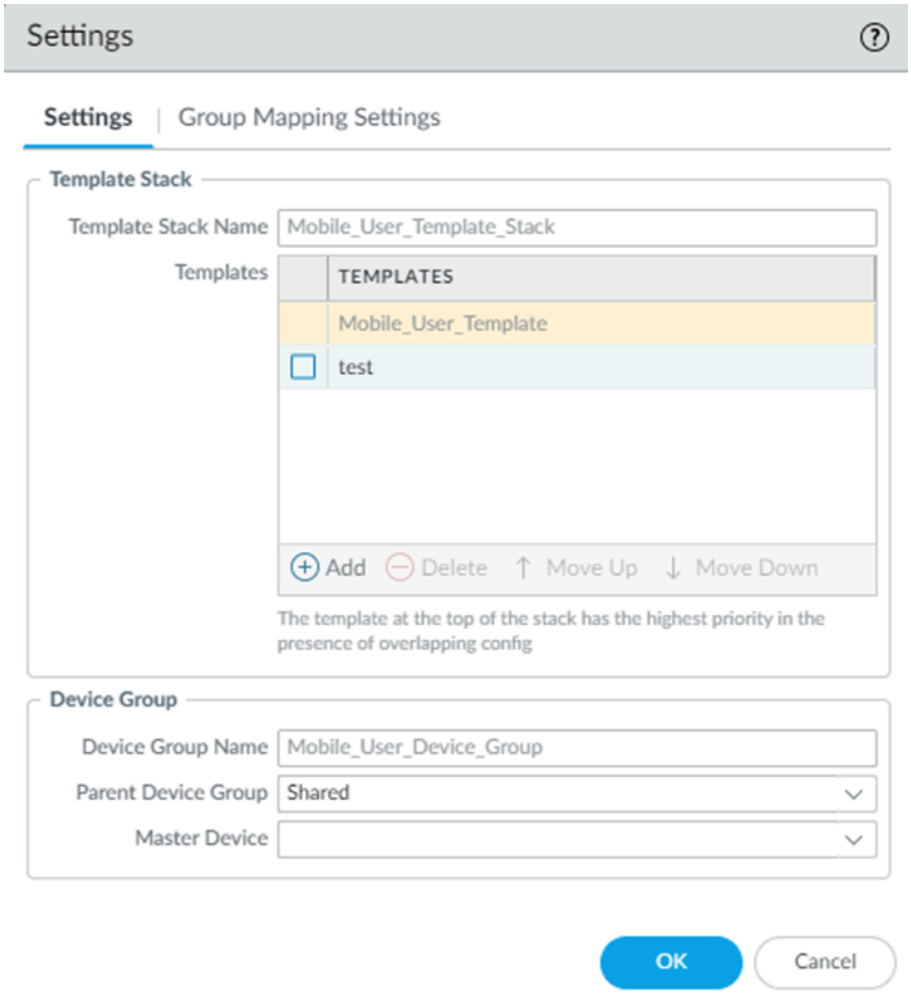
**STEP 2 |** 將主要裝置新增到您的 Prisma Access 行動使用者或遠端網路部署。

- 對於行動使用者—GlobalProtect 部署，選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users—GlobalProtect**（行動使用者—**GlobalProtect**）、

 ©2025 Palo Alto Networks, Inc.

按一下 **Settings**（設定）中的齒輪圖示，然後選取您要指定為 **Master Device**（主要裝置）的內部部署防火牆。

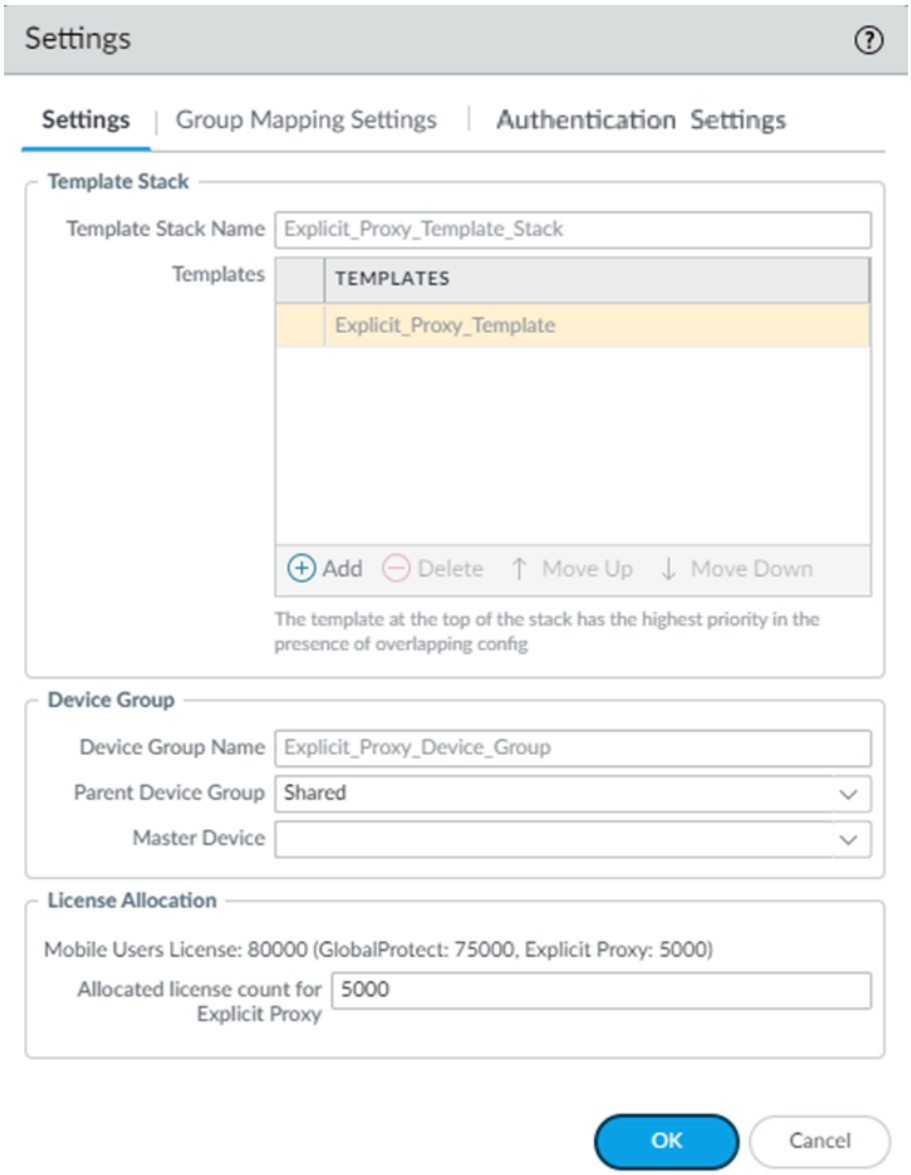
如果您使用預設的 ***Device Group Name***（裝置群組名稱）（在此情況下為 ***Mobile_User_Device_Group***）和 ***Parent Device Group***（父系裝置群組）（在此情況下為 ***Shared***（共用）），則未與其他裝置群組相關聯的任何裝置都會顯示在下拉式選項中。如果您已將主要裝置與另一個裝置群組建立關聯，請選取與該裝置群組相關聯的 ***Parent Device Group***（父系裝置群組），讓它顯示在下拉式清單中。




- 對於行動使用者—明確 Proxy 部署，選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users**—**Explicit Proxy**（行動使用者—明確 **Proxy**）、

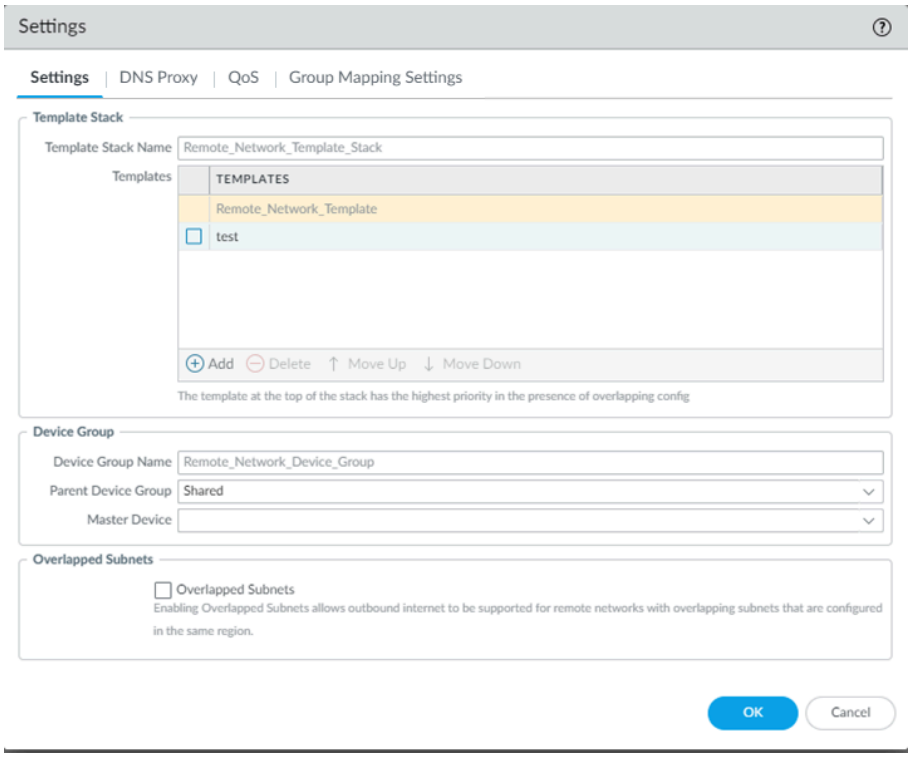
 ©2025 Palo Alto Networks, Inc.

按一下 **Settings**（設定）中的齒輪圖示，然後選取您已建立的 **Master Device**（主要裝置）。




- 對於遠端網路部署（具有遠端網路連線的裝置群組），選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路）、按一下 **Settings**（設定）中的齒輪圖示，然後選取您已建立的 **Master Device**（主要裝置）。


©2025 Palo Alto Networks, Inc.




*Prisma Access* 會自動為僅與主要裝置相關聯的裝置群組填入使用者名稱至使用者群組對應。對於此範例，自動填入僅會發生在 ***Remote_Network_Device_Group*** 裝置群組中，並不會填入到任何其他裝置群組。

**STEP 3 |** 按一下 **OK**（確定）。

## 長格式識別名稱項目

如果您尚未將新世代防火牆設定為主要裝置，或尚未將雲端識別引擎設定為在安全性政策規則中填入使用者和群組，則可以改為在 Panorama 中使用長格式識別名稱 (DN) 項目。Prisma Access 會使用 DN 項目來評估您在 Panorama 中設定的 User-ID 型政策。

例如，假設有一個使用者名為 **Bob Alice**，從事 IT 並位於一樓，則比對安全性政策可能具有 `cn=first_floor, ou=it_staff, dc=dev, dc=example, dc=com`（如果此政策適用於一樓的所有 IT 員工），或 `cn=Bob Alice, ou=it_staff, dc=dev, dc=example, dc=com`（如果此政策僅適用於 Bob Alice）。


©2025 Palo Alto Networks, Inc.

# 身分重新分配

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

這樣您就可以一致地強制執行您的安全性政策略，Prisma Access 會在整個 Prisma Access 環境中共用 GlobalProtect 在本機探索的識別資料。Prisma Access 也可以與遠端網站或服務連線網站（總部和資料中心）的內部部署裝置共用識別資料。

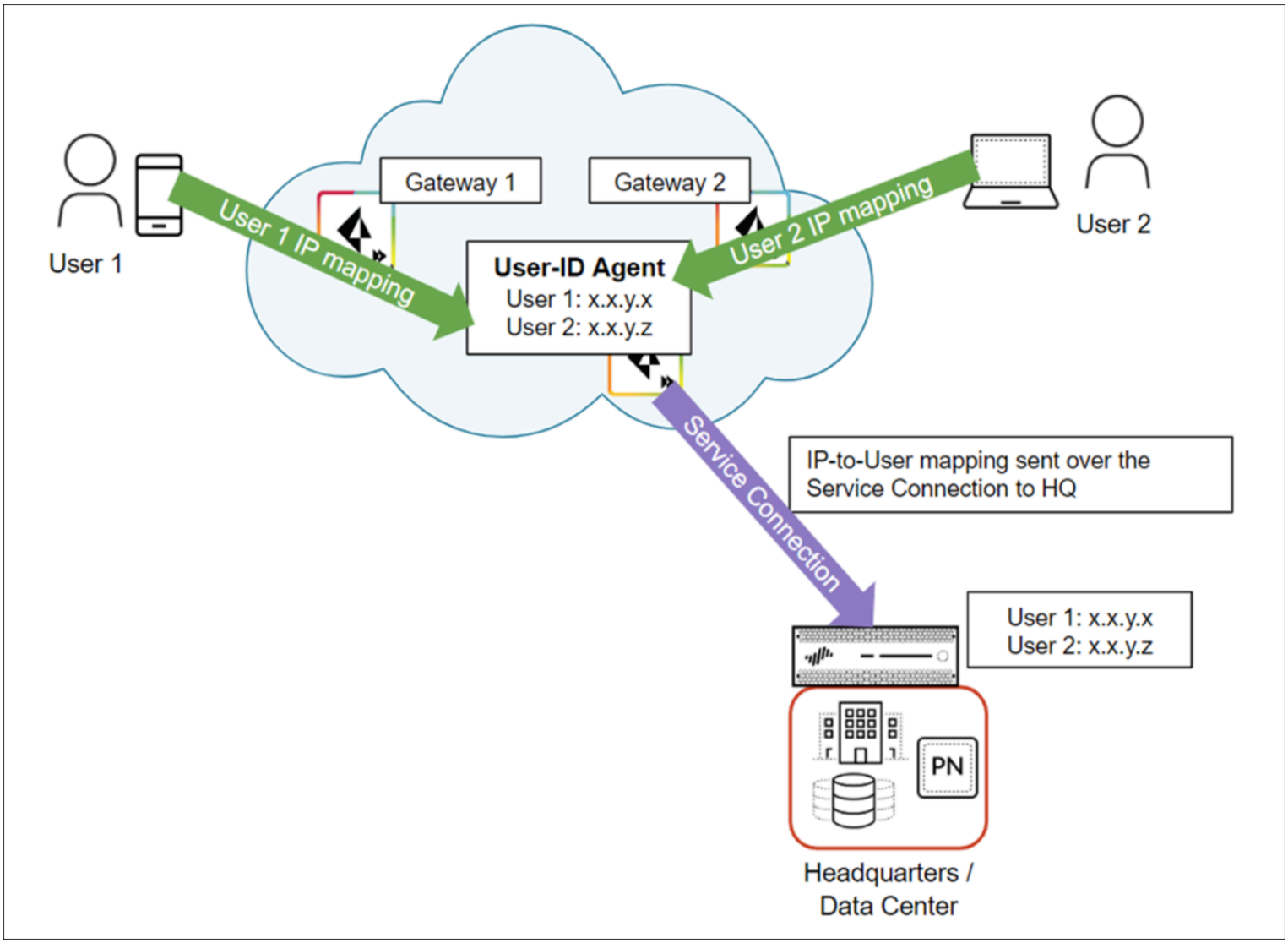
若要讓行動使用者存取遠端網路位置或 HQ/資料中心上的資源，而這些位置受到裝置的使用者政策保護，這時您就必須將 Prisma Access 行動使用者和遠端網路使用者的識別資料重新散佈至該內部部署裝置。

當使用者連線至 Prisma Access 時，PPrisma Access 會收集使用者的識別資料並加以儲存。

以下範例顯示了兩個行動使用者，他們在 Prisma Access 中具有現有的 IP 位址至使用者名稱對應。然後，Prisma Access 透過服務連線方式將此對應重新散佈至保護總部/資料中心的內部部署裝置。

Prisma Access (Managed by Strata Cloud Manager) 會自動啟用服務連線，作為識別重新散佈代理程式（也稱為 User-ID 代理程式）。


©2025 Palo Alto Networks, Inc.




- Strata Cloud Manager
- Panorama

## 識別重新散佈 (Strata Cloud Manager)

這樣您就可以一致地強制執行您的安全性政策略，Prisma Access 會在整個 Prisma Access 環境中共用 GlobalProtect 在本機探索的識別資料。Prisma Access 也可以與遠端網站或服務連線網站（總部和資料中心）的內部部署裝置共用識別資料。

對於 Prisma Access (Managed by Strata Cloud Manager)，我們預設啟用了某種程度的識別資料重新散佈，對其餘部分，我們則經由設定簡化了重新散佈的流程（只需選取核取方塊來選取要共用的資料即可）。

在 [Identity Distribution（識別散佈）] 儀表板中，您可以查看識別資料的共用方式，以及管理資料重新散佈（**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Identity Services**（識別服務））。

您可以重新散佈的識別資料包括：

 ©2025 Palo Alto Networks, Inc.

- HIP 資料
- IP 位址到標籤的對應
- IP 位址到使用者的對應
- 使用者到標籤的對應
- 隔離裝置

開始進行識別重新散佈

- 設定識別重新散佈
- 識別和隔離遭入侵裝置

## 設定識別重新散佈

設定識別重新散佈

確認您的服務連線設定。

如果您尚未為 HQ 或資料中心設定服務連線，請先設定服務連線。必須要有服務連線，Prisma Access 才能在您的環境中共用識別資料；Prisma Access 會自動啟用服務連線，作為重新散佈代理程式。當您看到新建立的服務連線站台已被指派 User-ID 代理程式位址時，該站台即可作為重新散佈代理程式（Prisma Access 會自動執行此動作，且只需要幾分鐘）。

> ***User-ID*** 重新散佈管理—有時，在特別大規模的 *Prisma Access* 部署中，需要對 *User-ID* 重新散佈進行精細控制。*User-ID* 重新散佈管理可讓您手動停用某些服務連線的預設識別重新散佈行為，方法是刪除 ***User ID***（使用者 ***ID***）欄中的核取標記，然後選取要用於識別重新散佈的特定服務連線。對於大多數設定，沒有必要執行此動作。請聯絡 *Palo Alto Networks* 支援以啟動此功能。

前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Identity Services**（識別服務） > **Identity Redistribution**（識別重新散佈），並將設定範圍設定為 **Service Connections**（服務連線），以驗證服務連線 User-ID 代理程式詳細資料。

將識別資料從 Prisma Access 傳送至內部部署裝置。

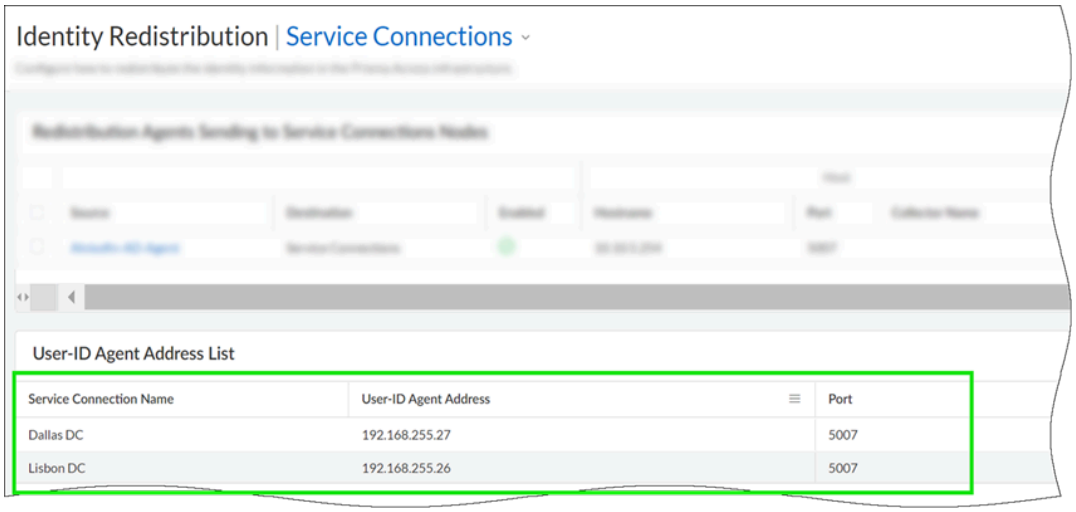
您只需設定服務連線的 User-ID 代理程式資訊，即可將 Prisma Access 設定為將識別資料散佈至內部部署裝置。

前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Identity Services**（識別服務） > **Identity Redistribution**（識別重新散

 ©2025 Palo Alto Networks, Inc.

佈），並將設定範圍設定為 **Service Connections**（服務連線），以取得服務連線 User-ID 代理程式詳細資料。

使用這些詳細資料，將 Prisma Access 設定為 Panorama 或 Palo Alto Networks NGFW 上的資料重新散佈代理程式。



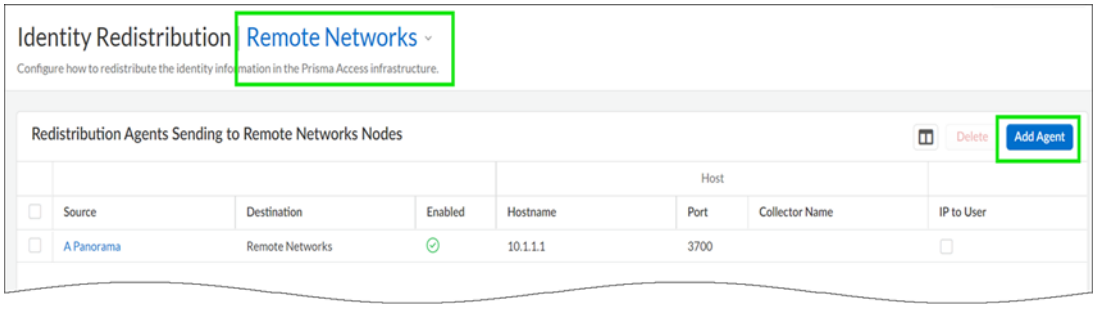

 ©2025 Palo Alto Networks, Inc.

將識別資料從內部部署裝置傳送至 Prisma Access。

將內部部署裝置新增至 Prisma Access 作為重新散佈代理程式；您新增的裝置將能夠將識別資料散佈至 Prisma Access。

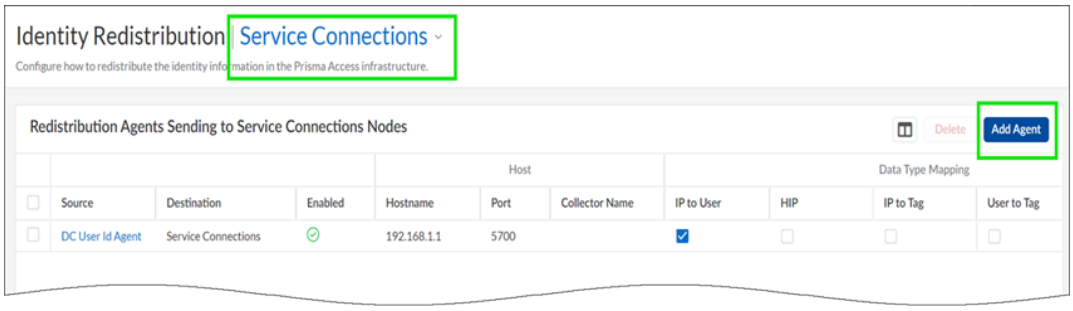
- 從遠端網站上的裝置：

  移至 **Identity Redistribution**（識別重新散佈）儀表板，將設定範圍設定為 **Remote Networks**（遠端網路），然後新增代理程式。除了指定主機詳細資料以外，也請選取裝置與 Prisma Access 共用的資料類型。選用設定包括裝置的名稱和預先共用金鑰。




- 從服務連線站台上的裝置：

  移至 **Identity Redistribution**（識別重新散佈）儀表板，將設定範圍設定為 **Service Connections**（服務連線），然後新增代理程式。除了指定主機詳細資料以外，也請選取裝置與 Prisma Access 共用的資料類型。選用設定包括裝置的名稱和預先共用金鑰。



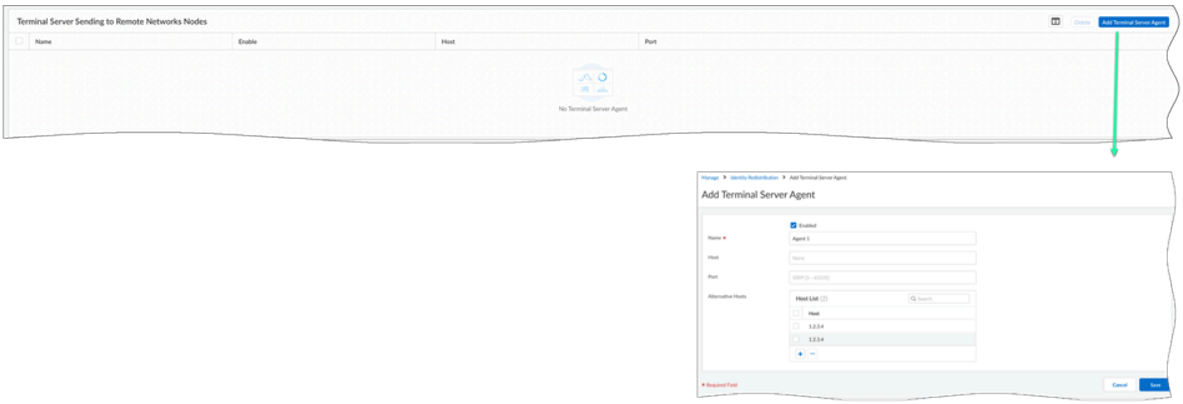

 ©2025 Palo Alto Networks, Inc.

為使用者對應設定終端伺服器代理程式。

終端伺服器 (TS) 代理程式會為每個使用者指派一個連接埠範圍，以識別 Windows 型終端伺服器上的特定使用者。TS 代理程式會向 Prisma Access 指出已配置的連接埠範圍，讓 Prisma Access 能夠根據使用者和使用者群組強制執行政策。

在 **Identity Redistribution**（識別重新散佈）儀表板上，將設定範圍設定為 **Remote Networks**（遠端網路），並在 **Terminal Server Sending to Remote Networks Nodes**（傳送至遠端網路節點的終端伺服器）底下新增終端伺服器代理程式。

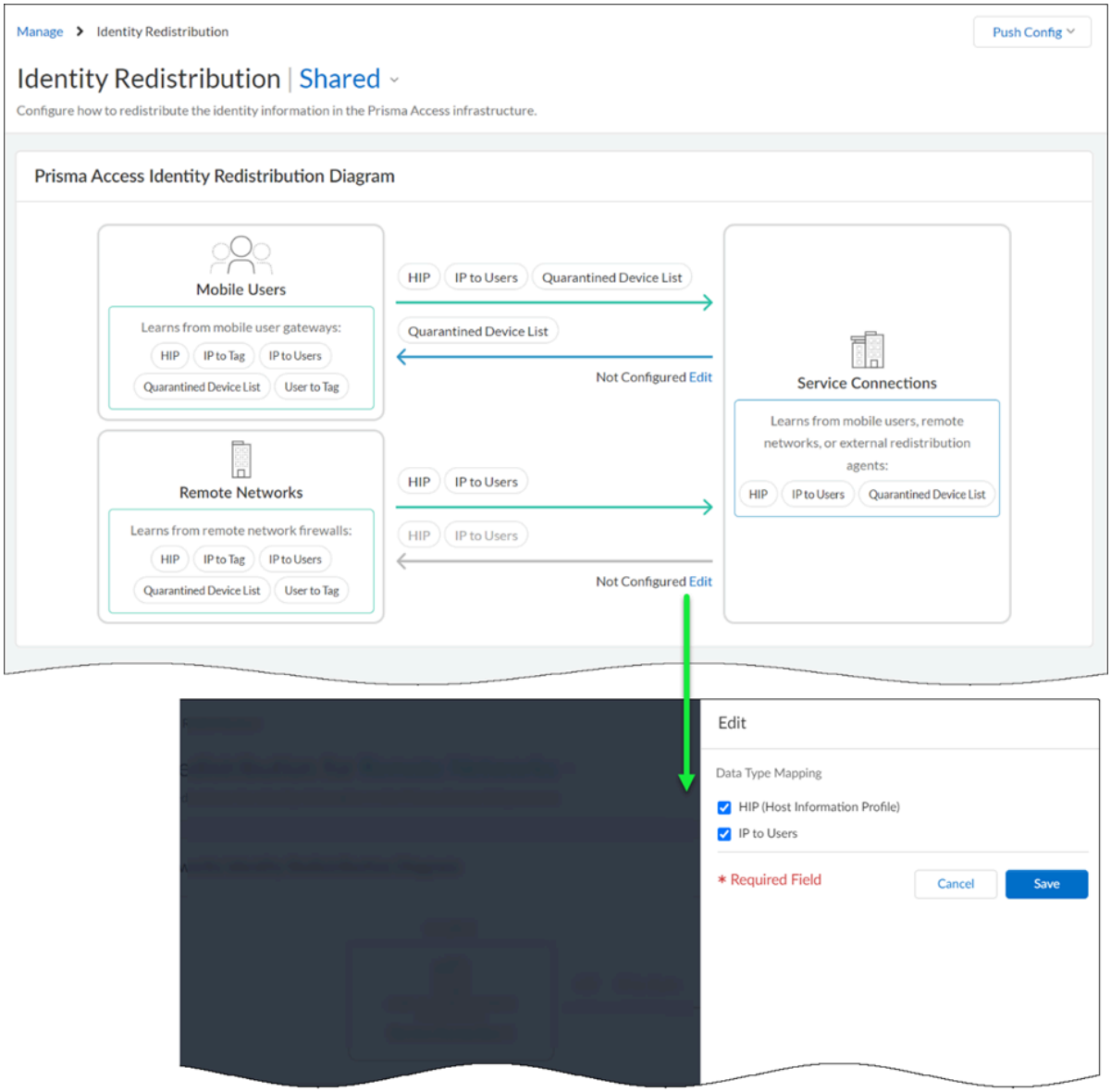
- 依預設會啟用該設定。
- 輸入 TS 代理程式的 **Name**（名稱）。
- 輸入安裝 TS 代理程式所在 Windows **Host**（主機）的 IP 位址。
- 輸入代理程式用來接聽使用者識別要求的連接埠號碼。此連接埠預設為 5009。
- **Save**（儲存）變更。




 ©2025 Palo Alto Networks, Inc.

跨 Prisma Access 環境中散佈識別資料。

在 **Identity Redistribution**（識別重新散佈）儀表板上，編輯圖表以指定您要從每個來源收集，並在 Prisma Access 中共用的識別資料。




若要啟動您的變更，請將設定推送至 Prisma Access。

## 識別重新散佈 (Panorama)

在設定使用者識別之後，您透過將 IP 位址至使用者名稱對應從 Prisma Access 重新散佈至所有對存取網路資源提供保護的新世代防火牆，為所有行動使用者和遠端網路位置的使用者一致地強制執行安全性政策。請使用下列其中一種方法，將 IP 位址至使用者名稱對應從內部部署新世代防火牆重新散佈至行動使用者和遠端網路中的使用者，反之亦然：

- 將 User-ID 資訊從 Prisma Access 重新散佈至內部部署防火牆


©2025 Palo Alto Networks, Inc.

- 將 User-ID 資訊從內部部署防火牆重新散佈至 Prisma Access

## 將 User-ID 資訊從 Prisma Access 重新散佈至內部部署防火牆

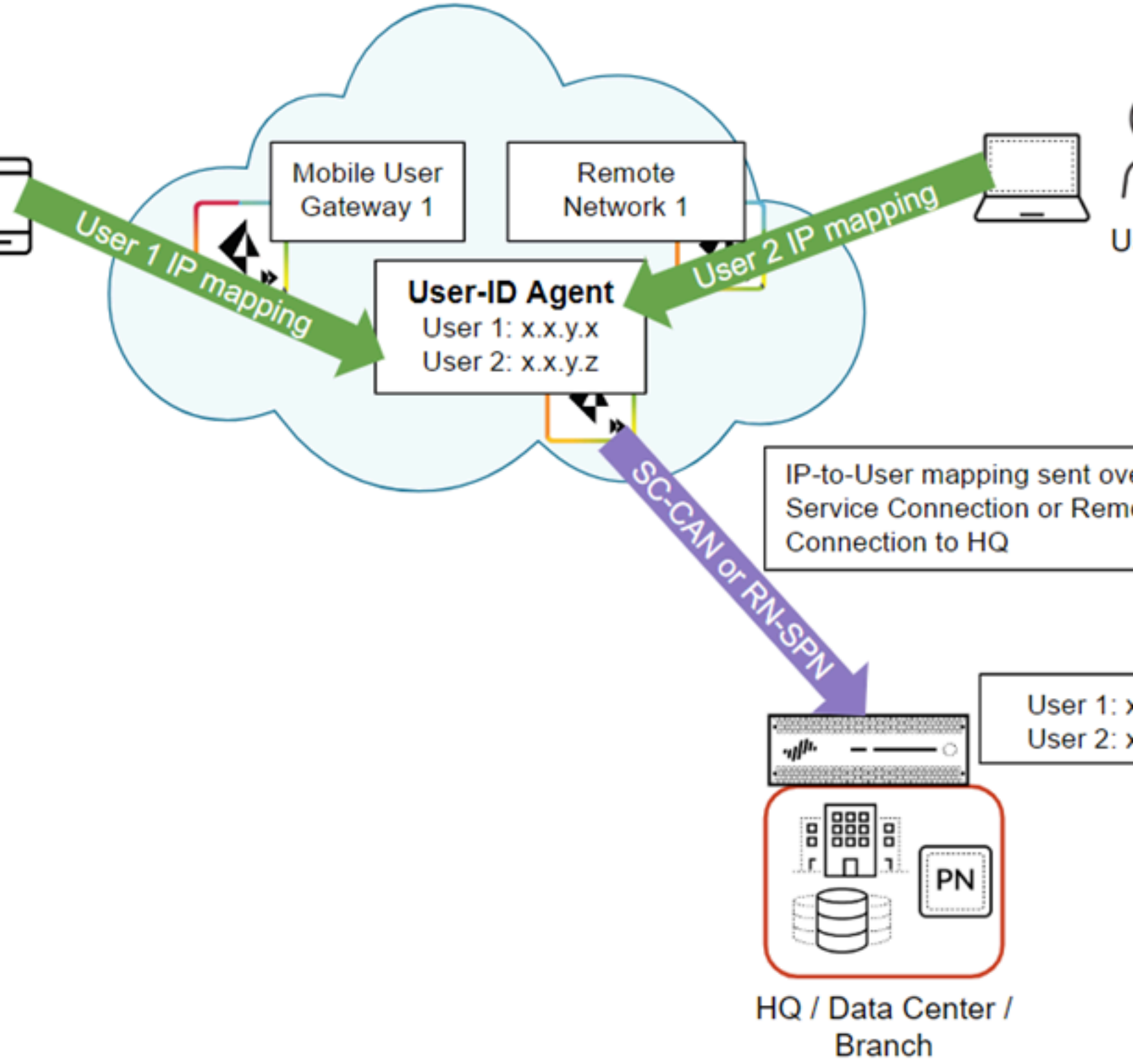
將 **User-ID** 資訊從 **Prisma Access** 重新散佈至內部部署防火牆。

在行動使用者需要存取遠端網路位置或總部/資料中心上的資源，並且該資源由內部部署新世代防火牆透過使用者型政策保護的情況下，您必須將 IP 位址至使用者名稱對應從 Prisma Access 行動使用者和遠端網路中的使用者重新散佈至內部部署防火牆。當使用者連線到 Prisma Access 時，它會收集此使用者至 IP 位址對應並將其存儲。

下圖顯示了兩個行動使用者，他們在 Prisma Access 中具有現有的 IP 位址至使用者名稱對應。然後，Prisma Access 藉由服務連線 (SC-CAN) 或遠端網路連線 (RN-SPN) 方式，將此對應重新散佈至保護總部/資料中心的內部部署防火牆。

*Prisma Access* 會使用服務連線或遠端網路連線作為 *IPSec* 通道，充當第三層網路的底層路徑。您可以使用任何透過 *IPSec* 受信任通道的路由路徑，讓私人存取的目的地重新散佈此對應。


©2025 Palo Alto Networks, Inc.



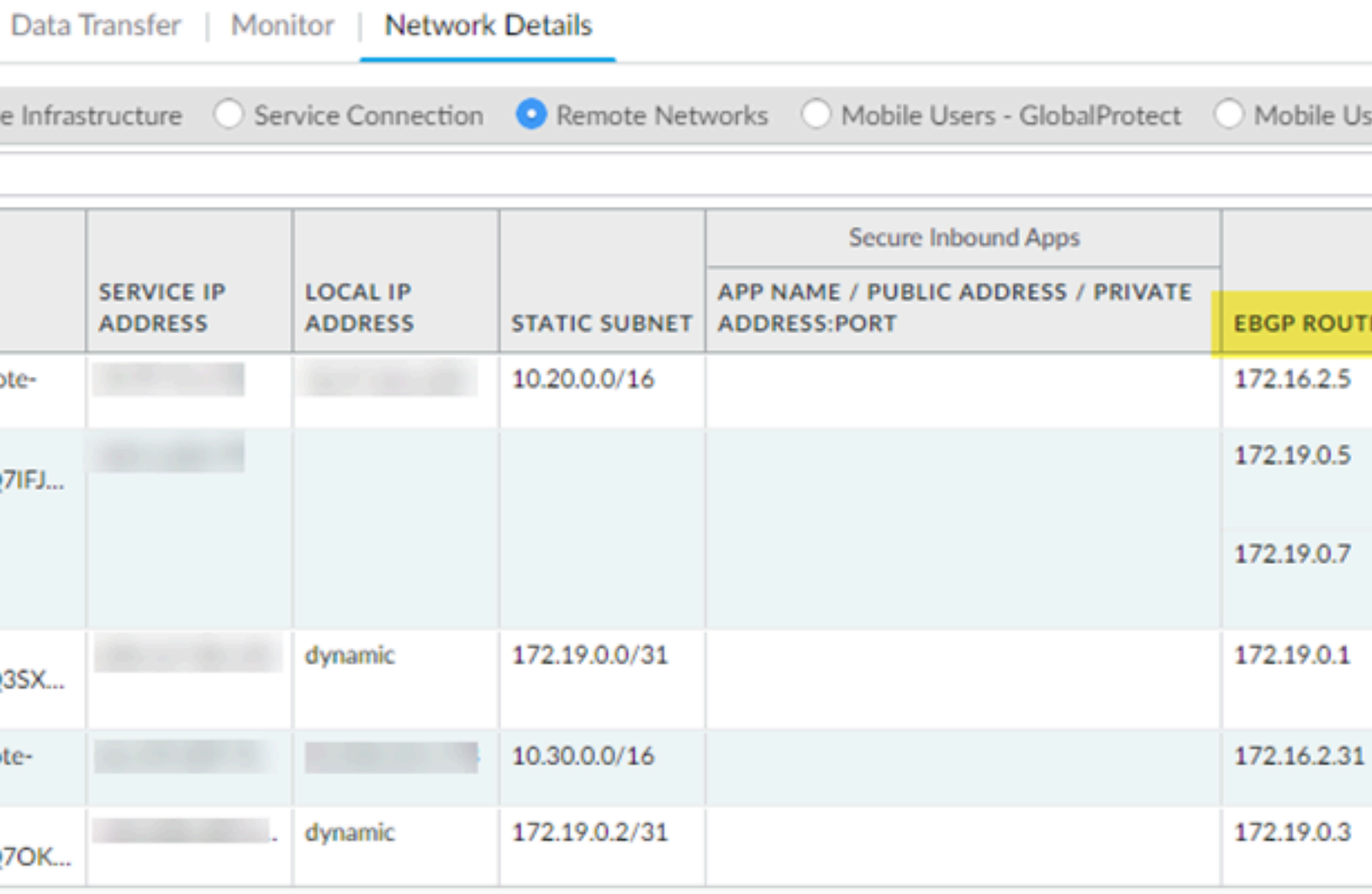

若要將 User-ID 對應從 Prisma Access 重新散佈至內部部署防火牆，請完成以下步驟。


©2025 Palo Alto Networks, Inc.

確保您不對將使用者識別重新散佈至內部部署防火牆（*SC-CAN* 或 *RN-SPN*）的任何連線套用任何 *SSL* 解密，包括任何在重新散佈路徑中的防火牆。或者，您可以將解密排除套用至重新散佈流量。

**STEP 1 |** 記下要在您設定資料重新散佈代理程式時使用的 IP 位址。

- 對於遠端網路連線，尋找 **EBGP Router**（**EBGP** 路由器）位址（**Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Remote Networks**（遠端網路） > **EBGP Router**（**EBGP** 路由器））。



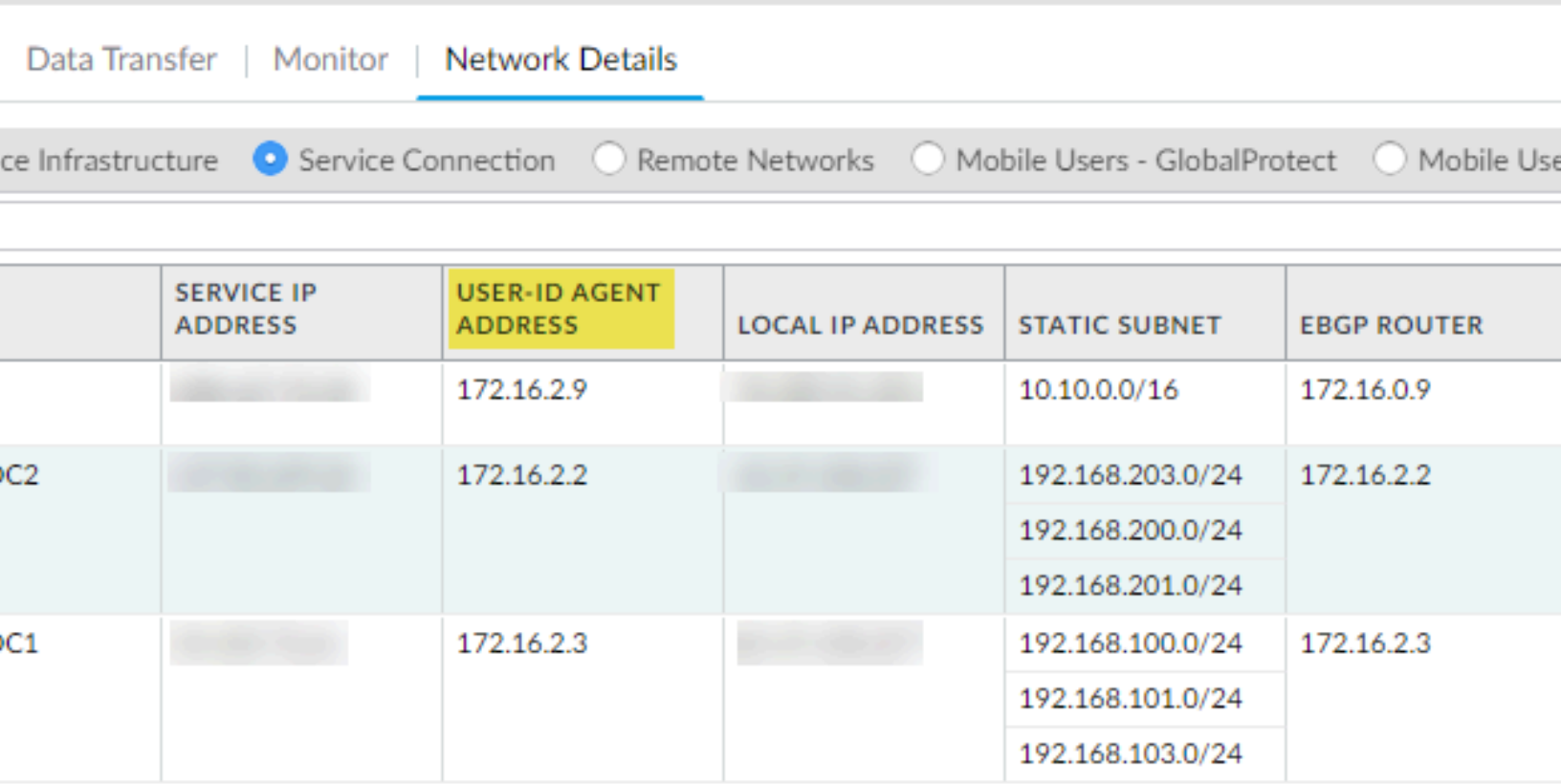

- 對於服務連線，尋找 **User-ID Agent Address**（**User-ID** 代理程式位址）（**Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Service Connection**（服務連線） > **User-ID Agent Address**（**User-ID** 代理程式位址））。

  如果您尚未為 HQ 或資料中心設定服務連線，請先設定服務連線。Prisma Access 會使用服務連線，跨您的環境共用識別資料；Prisma Access 會自動啟用服務連線，當作重新散佈代

 ©2025 Palo Alto Networks, Inc.

理程式運作。當您看到新建立的服務連線網站已獲指派 User-ID 代理程式位址時，該網站準備好作為重新散佈代理程式（Prisma Access 會自動執行此動作，且只需要幾分鐘）。

**User-ID** 重新散佈管理—有時，在特別大規模的 *Prisma Access* 部署中，需要對 *User-ID* 重新散佈進行精細控制。*User-ID* 重新散佈管理可讓您手動停用某些服務連線的預設識別重新散佈行為，方法是刪除 ***User ID***（使用者 ***ID***）欄中的核取標記，然後選取要用於識別重新散佈的特定服務連線。對於大多數設定，沒有必要執行此動作。請聯絡 *Palo Alto Networks* 支援以啟動此功能。

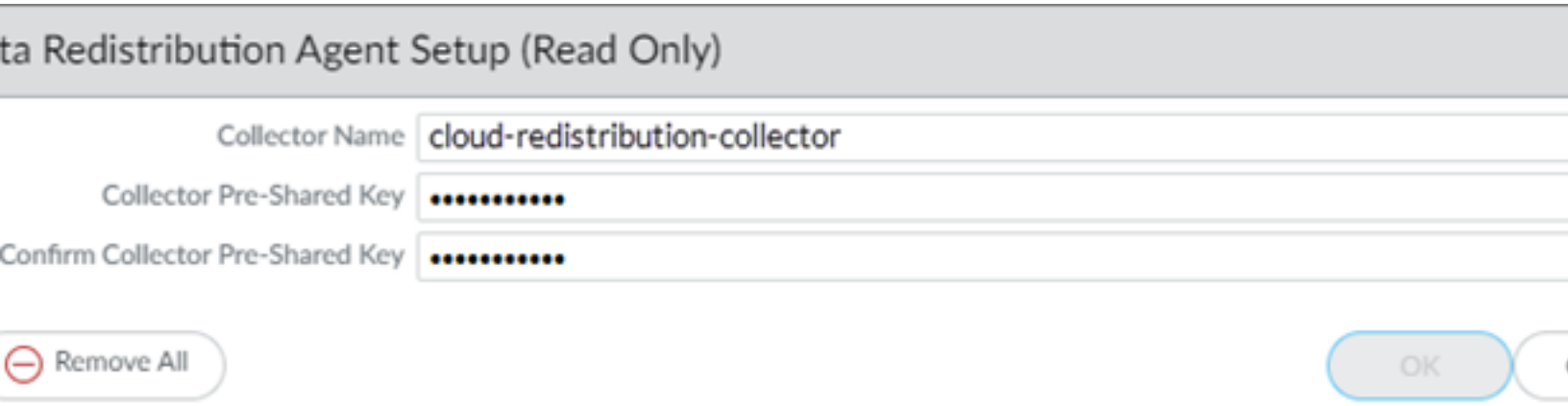



 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 將 Prisma Access 設定為重新散佈使用者對應資訊的 User-ID 代理程式。

1. 在管理 Prisma Access 的 Panorama 中，選取 **Device**（裝置） > **Data Redistribution**（資料重新散佈） > **Collector Settings**（收集器設定）。

   若要在服務連線上設定收集器，請選取 **Service_Conn_Template**；若要在遠端網路連線上設定收集器，請選取 **Remote_Network_Template**。
2. 按一下齒輪圖示以編輯設定。
3. 提供 **Collector Name**（收集器名稱）和 **Collector Pre-Shared Key**（收集器預先共用金鑰），以將 Prisma Access 識別為 User-ID 代理程式。
4. 按一下 **OK**（確定）儲存您的變更。

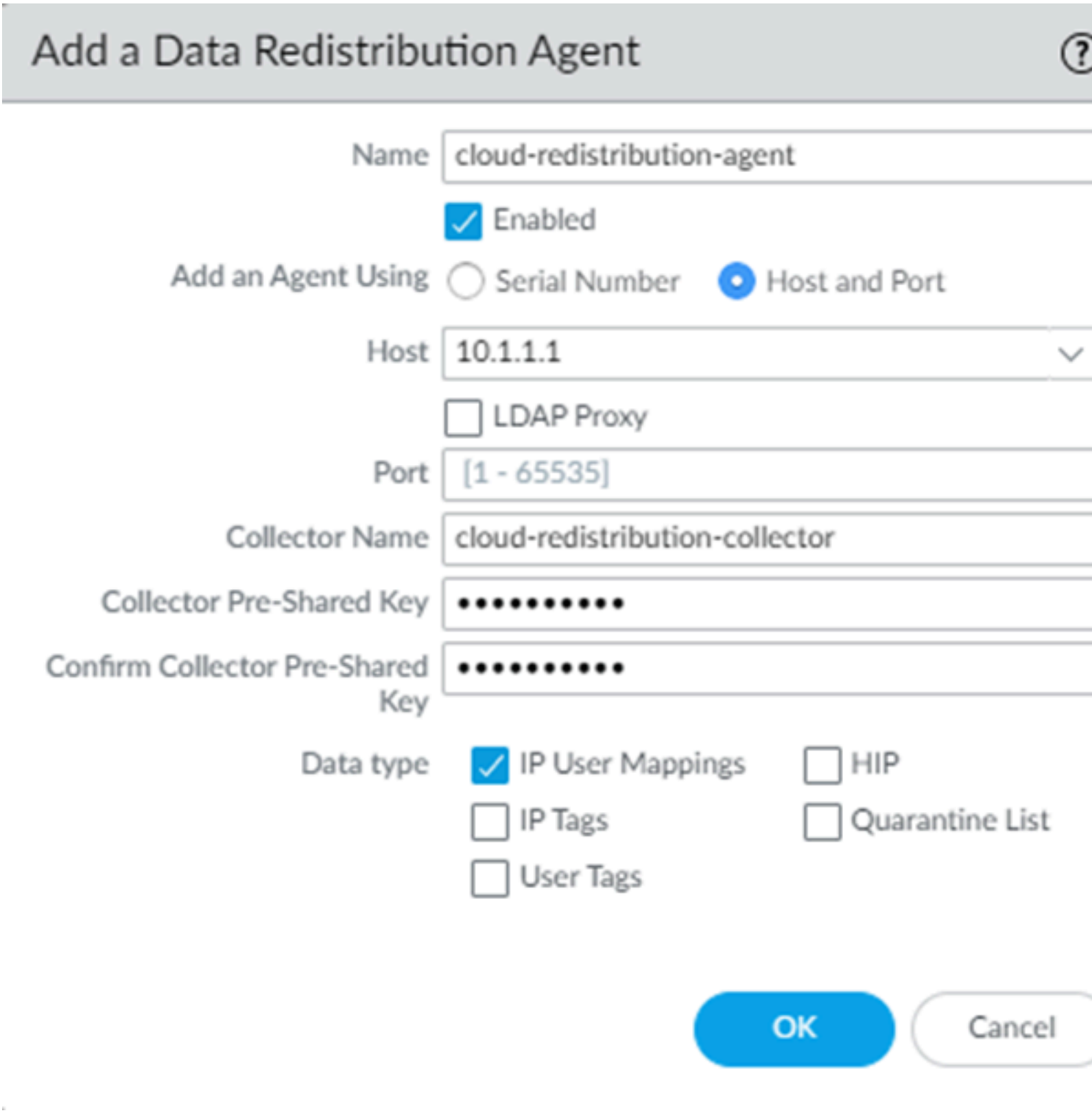



 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 設定內部部署防火牆，從 Prisma Access 收集 User-ID 對應。

1. 從內部部署防火牆中，選取 **Device**（裝置） > **Data Redistribution**（資料重新散佈） > **Agents**（代理程式）。
2. **Add**（新增）一個 User-ID 代理程式並給與它一個 **Name**（名稱）。
3. 選取 **Host and Port**（主機和連接埠）。
4. 在 **Host**（主機）欄位中，輸入來自 Prisma Access 的 **User-ID Agent Address**（**User-ID** 代理程式位址）（用於服務連線）或 **EBGP Router Address**（**EBGP** 路由器地址）（用於遠端網路連線）。
5. 為您先前在程序中建立的 Prisma Access 收集器輸入 **Collector Name**（收集器名稱）和 **Collector Pre-Shared Key**（收集器預先共用金鑰）。
6. 選取 **IP User Mappings**（**IP** 使用者對應）。
7. 按一下 **OK**（確定）。
8. 對於您想要重新散佈其對應的每個服務連線或遠端網路連線重複這些步驟。


©2025 Palo Alto Networks, Inc.




## 將 User-ID 資訊從內部部署防火牆重新散佈至 Prisma Access

將 **User-ID** 資訊從內部部署防火牆重新散佈至 **Prisma Access**。

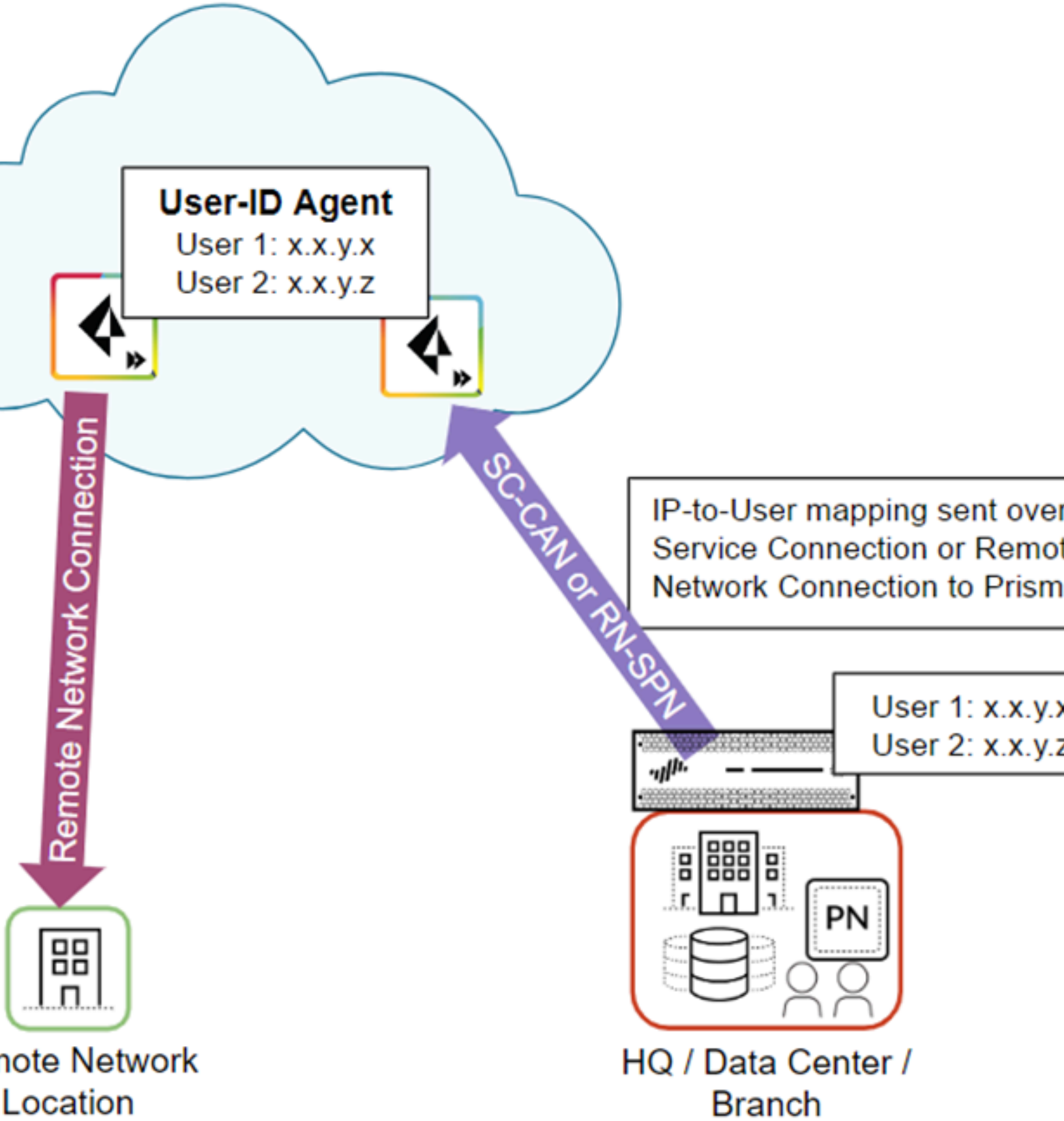

©2025 Palo Alto Networks, Inc.

在使用者位於由內部部署新世代防火牆透過使用者型政策保護的分支位置或總部，以及他們需要存取另一個分支位置中您透過 Prisma Access 保護的資源的情況下，您必須將 IP 位址至使用者名稱對應從內部部署防火牆重新散佈至 Prisma Access。

下圖顯示了一個總部/資料中心，其中內部部署新世代防火牆具有現有的 IP 位址至使用者名稱對應。Prisma Access 透過服務連線 (SC-CAN) 或遠端網路連線 (RN-SPN) 連線至防火牆，而且內部部署防火牆將對應重新散佈至 Prisma Access。

下圖顯示了用來重新散佈對應的 Prisma Access 服務連線或遠端網路連線。您可以使用任何透過 IPSec 受信任通道的路由路徑，讓私人存取的目的地重新散佈此對應。

 ©2025 Palo Alto Networks, Inc.





©2025 Palo Alto Networks, Inc.

若要將 User-ID 對應從內部部署防火牆重新散佈至 Prisma Access，請完成以下步驟。

**STEP 1 |** 設定內部部署防火牆，將 User-ID 資訊重新散佈至 Prisma Access。

1. 從內部部署防火牆中，選取 **Device**（裝置） > **Data Redistribution**（資料重新散佈） > **Collector Settings**（收集器設定）。
2. 按一下齒輪圖示以編輯設定。
3. 提供 **Collector Name**（收集器名稱）和 **Collector Pre-Shared Key**（收集器預先共用金鑰），以將內部部署防火牆識別為 User-ID 代理程式。
4. 按一下 **OK**（確定）儲存您的變更。

**STEP 2 |** 設定 Prisma Access，從內部部署防火牆收集 User-ID 對應。

1. 從管理 Prisma Access 的 Panorama 中，選取 **Device**（裝置） > **Data Redistribution**（資料重新散佈） > **Agents**（代理程式）。

   確保您在頁面頂部的 **Templates**（範本）下拉式清單中選取了 **Service_Conn_Template**（用於服務連線）或 **Remote_Network_Template**（用於遠端網路連線）。
2. **Add**（新增）一個 User-ID 代理程式並給與它一個 **Name**（名稱）。
3. 選取 **Host and Port**（主機和連接埠）。
4. 在 **Host**（主機）欄位中，輸入防火牆用來傳送使用者對應的 MGT 介面或服務路由的 IP 位址。

   對於 MGT 介面，您可以輸入主機名稱，而不輸入 IP 位址。
5. 使用您在步驟 1 中用於內部部署防火牆的收集器值，輸入 **Collector Name**（收集器名稱）和 **Collector Pre-Shared Key**（收集器預先共用金鑰）。
6. 選取 **IP User Mappings**（**IP** 使用者對應）。
7. 按一下 **OK**（確定）。

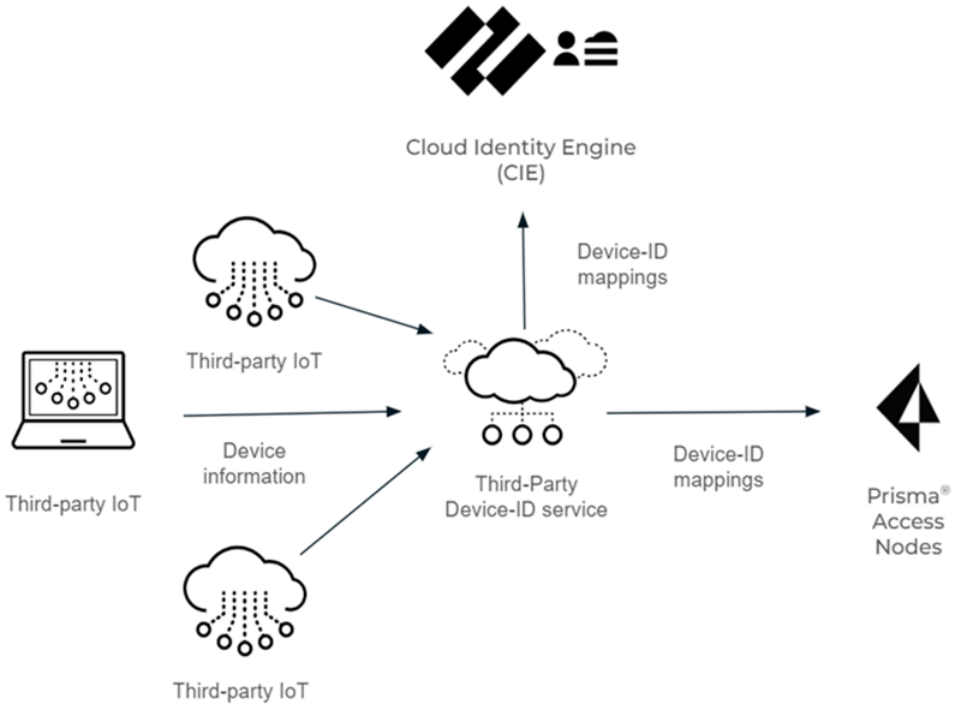
 ©2025 Palo Alto Networks, Inc.

# 在 Prisma Access 中設定第三方 Device-ID

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>如果您想在 Prisma Access 環境中使用此功能，請與您的帳戶團隊聯繫以瞭解更多資訊。 | ❑ Prisma Access 授權，Cloud Identity Engine 功能已啟用 |

您可以使用雲端識別引擎搭配 Prisma Access，套用來自第三方 IoT 偵測來源的資訊，以簡化網路中裝置識別和封閉安全性間距的工作。在使用 API 於雲端識別引擎中設定第三方 Device-ID 之後，您可以在 Prisma Access 設定裝置物件和安全性政策規則，以透過雲端識別引擎從第三方 IoT 可視性解決方案取得並使用資訊，以實現裝置可視性和控制。

在下圖中，第三方 Device-ID 會從第三方 IoT 解決方案接收裝置資訊，然後以 IP 位址至裝置對應形式傳輸至雲端識別引擎和 Prisma Access 安全性處理節點 (SPN)。




- Strata Cloud Manager
- Panorama


©2025 Palo Alto Networks, Inc.

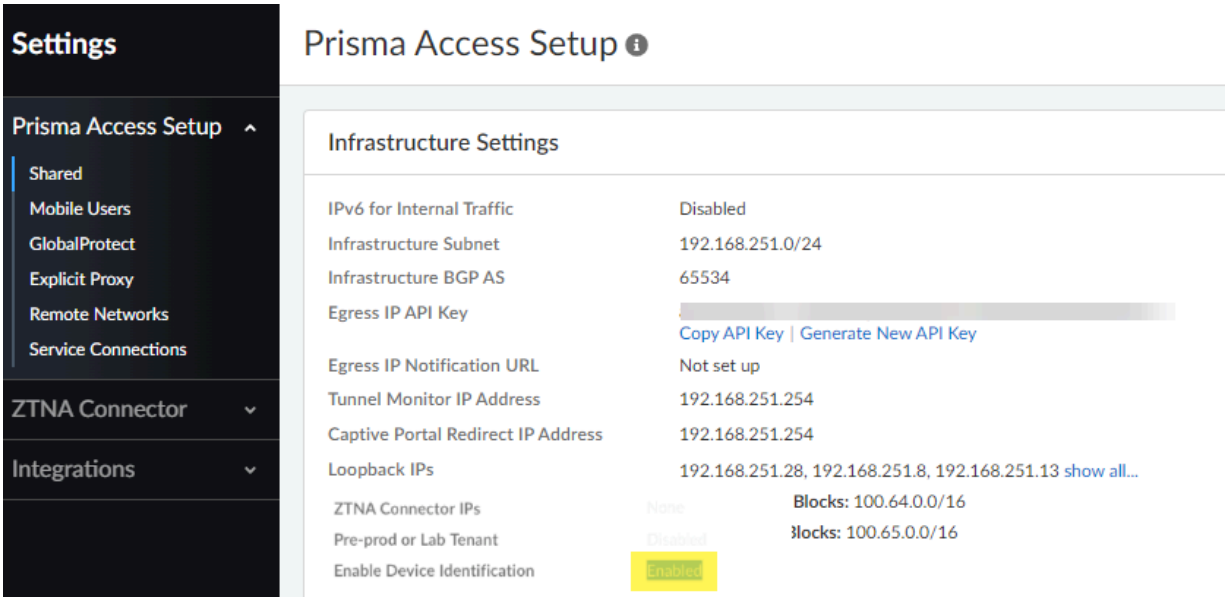
# 在 Prisma Access 中設定第三方 Device-ID (Strata Cloud Manager)

若要設定第三方 Device-ID，請完成以下工作。

**STEP 1 |** 在雲端識別引擎中啟動第三方 Device-ID。

此程序包括上傳簽署的憑證，並使用該憑證搭配 API 與第三方 IoT 廠商進行通訊，並從該廠商下載 Device-ID 資訊。

**STEP 2 |** 在 Prisma Access 中啟動第三方 Device-ID，方法為前往 **Settings**（設定） > **Prisma Access Setup**（設定） > **Shared**（共用）或 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Prisma Access**，然後將 **Enable Device Identification**（啟用裝置識別）設定為 **Enabled**（已啟用）。



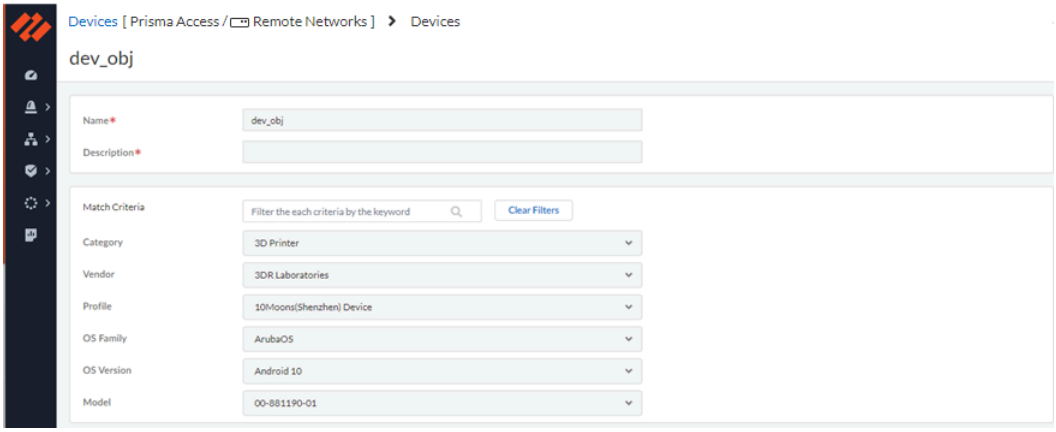

**STEP 3 |** 設定裝置物件並輸入裝置屬性。**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**）、將設定範圍設定為 **Remote Networks**（遠端網


©2025 Palo Alto Networks, Inc.

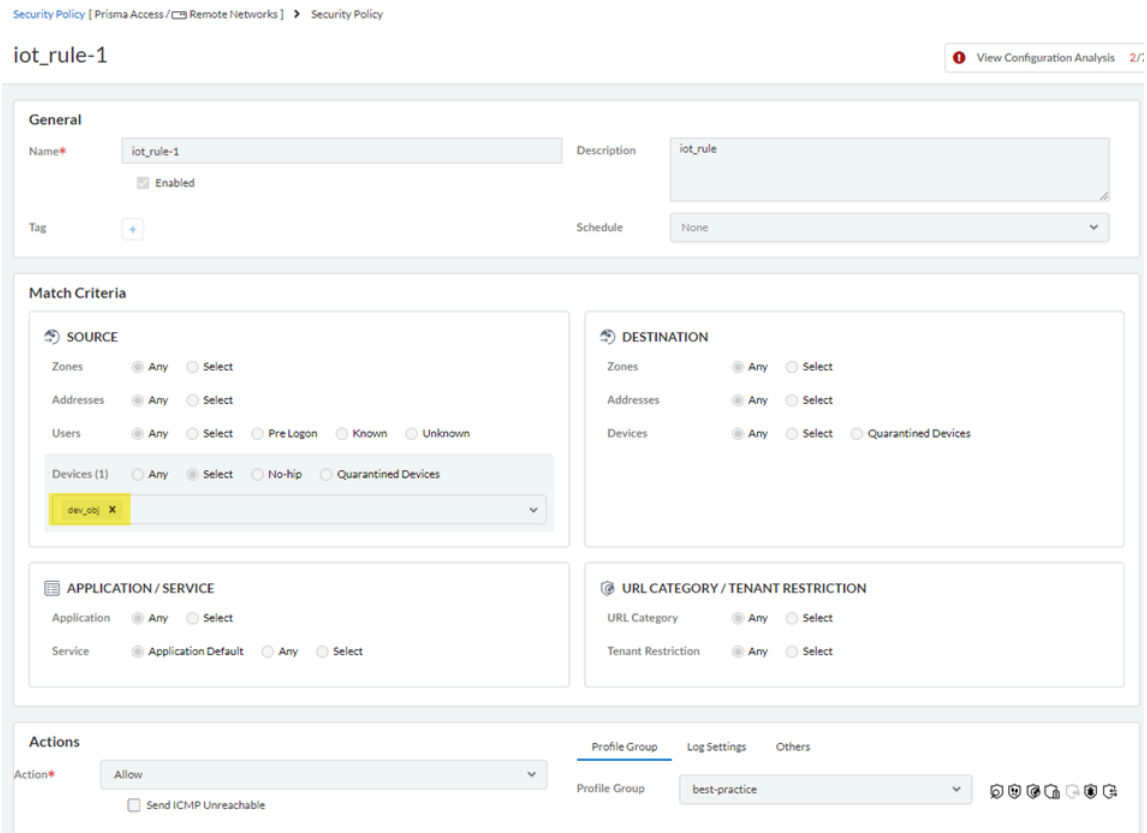
路），然後選取 **Objects**（物件） > **Devices**（裝置），並 **Add Devices**（新增裝置）。請確保您在遠端網路裝置群組中。

1. 新增一個裝置物件，符合第三方物件的屬性。

   雲端識別引擎 **Mappings**（對應）區域顯示第三方裝置的屬性；您可以使用從那裡擷取的任何屬性。




**STEP 4 |** 前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**）、將設定範圍設定為 **Remote Networks**（遠端網路），然後選取 **Security Services**（安全性服務） > **Security Policy**（安全性政策），並 **Add**（新增）安全性政策，新增您在 **Devices**（裝置）區域中建立的裝置物件。

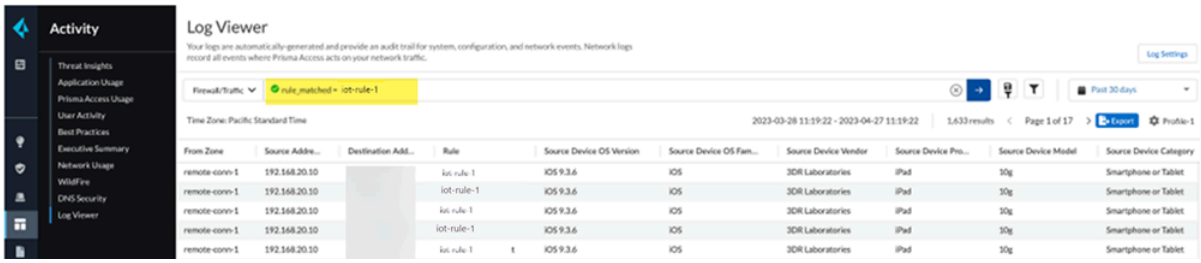



 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** **Push Config**（推送設定）以儲存您對 Prisma Access 設定的變更，確保在推送範圍中選取 **Remote Networks**（遠端網路）。

**STEP 6 |** 驗證 Prisma Access 是否正在接收 Device-ID 日誌，方法是前往 **Incidents & Alerts**（事件與警示） > **Log Viewer**（日誌檢視器）、選取 **Firewall/Traffic**（防火牆/流量），然後輸入 `rule_matched = rulename`（其中 *rulename* 是您為第三方 IoT 裝置建立的安全性政策規則）根據您建立的規則搜尋流量。

Device-ID 與 IP 位址對應會顯示在日誌中。




# 在 Prisma Access 中設定第三方 Device-ID (Panorama)

若要設定第三方 Device-ID，請完成以下工作。

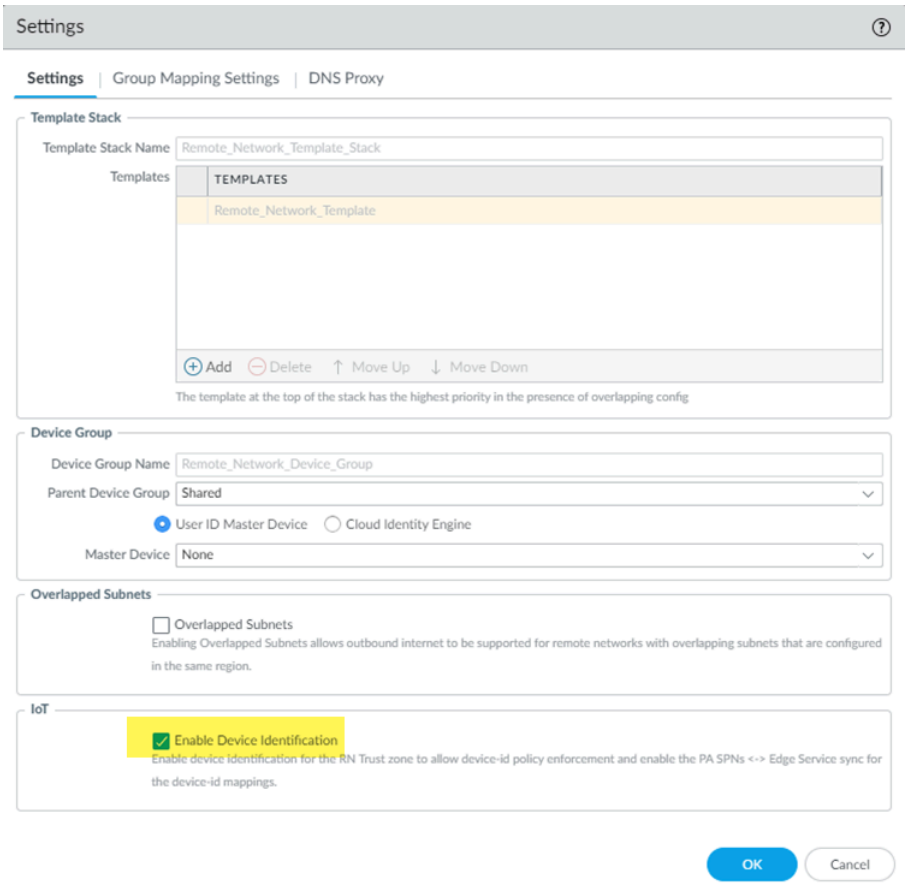
**STEP 1 |** 在雲端識別引擎中啟動第三方 Device-ID。

此程序包括上傳簽署的憑證，並使用該憑證搭配 API 與第三方 IoT 廠商進行通訊，並從該廠商下載 Device-ID 資訊。

**STEP 2 |** 在 Prisma Access 中啟動第三方 Device-ID，方法是前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路） > **Settings**（設定）、


©2025 Palo Alto Networks, Inc.

按一下齒輪以編輯 **Settings**（設定），然後選取 **Enable Device Identification**（啟用裝置識別）。




 ©2025 Palo Alto Networks, Inc.

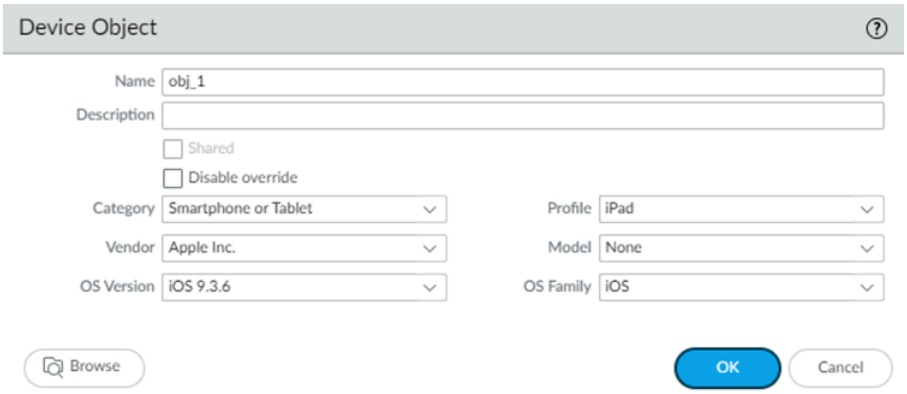
**STEP 3 |** 設定裝置物件並輸入裝置屬性。

1. 前往 **Objects**（物件） > **Devices**（裝置），並 **Add**（新增）一個裝置物件，符合所有裝置 ID 屬性。

   確保您是在 **Remote_Network_Device_Group** 或 **Shared**（共用）裝置群組中。

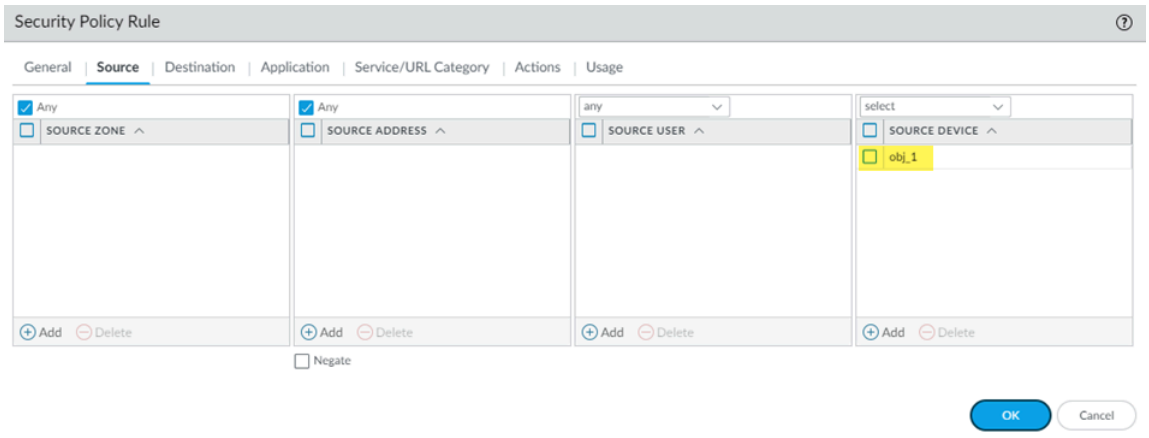
2. **Add**（新增）一個裝置物件，符合第三方物件的屬性。

   雲端識別引擎 ***Mappings***（對應）區域顯示第三方裝置的屬性；您可以使用從那裡擷取的任何屬性。




**STEP 4 |** 前往 **Policies**（政策） > **Security**（安全性） > **Pre Rules**（預先規則），並 **Add**（新增）一個安全性政策，新增您在 **Devices**（裝置）區域中建立的裝置物件，作為 **Source Device**（來源裝置）。

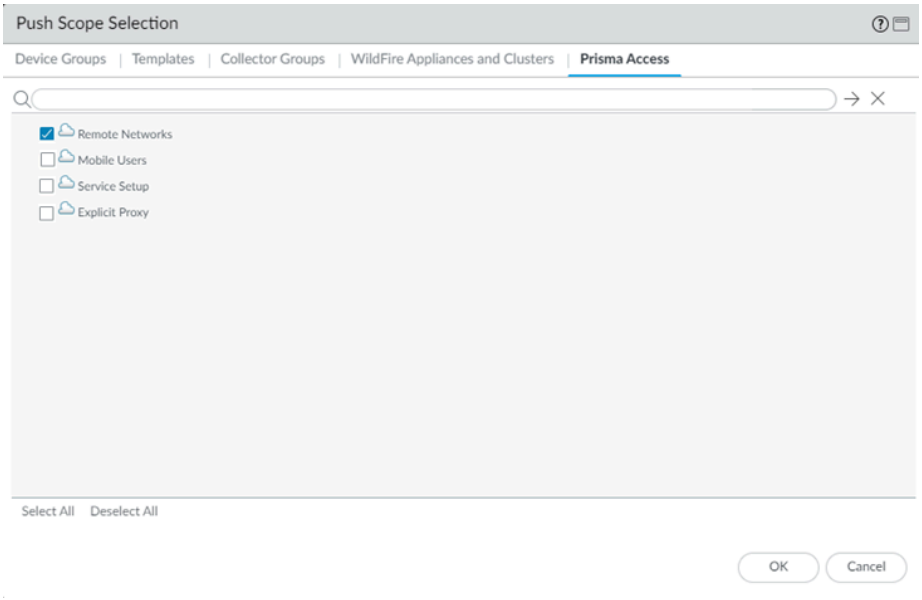
確保您是在 **Remote_Network_Device_Group** 或 **Shared**（共用）裝置群組中。




 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** 提交並推送您的變更，確保在 **Push Scope**（推送範圍）中選取了 **Remote Networks**（遠端網路）。

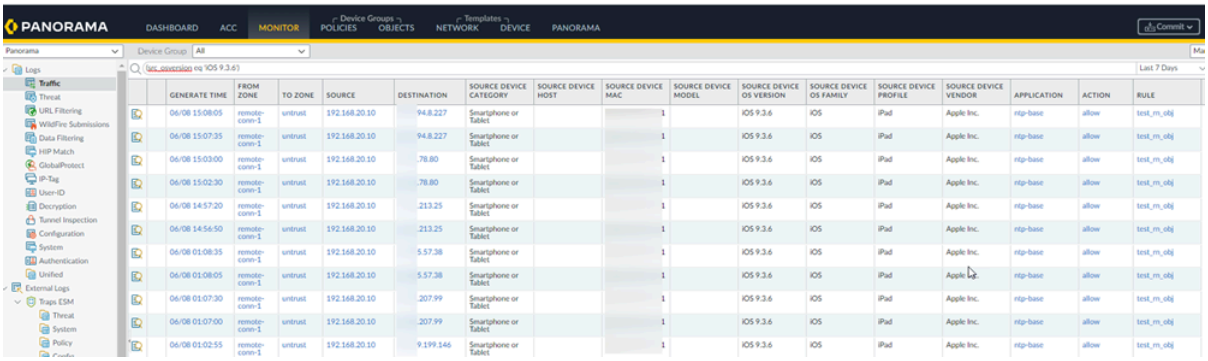
1. 按一下 **Commit**（提交） > **Commit and Push**（提交並推送）。
2. **Edit Selections**（編輯選取項目），並在 **Prisma Access** 頁籤中，確保在 **Push Scope**（推送範圍）中選取了 **Remote Networks**（遠端網路），然後按一下 **OK**（確定）。




3. 按一下 **Commit and Push**（提交並推送）。

**STEP 6 |** 驗證 Prisma Access 是否正在接收 Device-ID 日誌，方法是前往 **Monitor**（監控） > **Logs**（日誌），然後輸入 `rule_matched = rulename`（其中 *rulename* 是您為第三方 IoT 裝置建立的安全性政策規則）根據您建立的規則搜尋 **Traffic**（流量）日誌取得流量。

Device-ID 與 IP 位址對應會顯示在日誌中。




 ©2025 Palo Alto Networks, Inc.

# 第三方 Device-ID API

在已使用雲端識別引擎使用者介面裝載至第三方 Device-ID 服務之後，您可以使用這些 API，管理在您網路中偵測到並儲存在第三方 Device-ID 服務的裁定或 IP 位址至裝置對應。這些對應告訴 Prisma Access 哪些屬性屬於具有特定 IP 位址的裝置，以便您可以定義安全性政策，將具有特定屬性的裝置設為目標。

這些 API 不會直接存取雲端識別引擎租用戶中儲存的資料。相反，API 會與第三方 Device-ID 服務中的 IP 位址至裝置對應進行互動，從而與雲端識別引擎共用這些對應。

第三方 Device-ID API 會使用憑證、API 金鑰和基本 URL 提出 API 要求。若要驗證第三方 Device-ID API 要求，您必須使用裝載期間您在雲端識別引擎使用者介面中取得的簽署憑證和 API 權杖。

具有憑證和 API 金鑰時，您可以針對第三方 Device-ID 服務提出要求。在每個要求中提供憑證及其金鑰、API 金鑰和基本 URL。範例：

```
curl --cert onida1.crt --key onida.key "https://device-identity-
broker-beta.service-edge.panservicetest.com/:443/api/v1/token/
{apiKey}/verdicts"
```

- 更新裁定
- 刪除所有裁定
- 查詢裁定
- 依 IP 位址查詢裁定
- 查詢裁定統計資料

## 更新裁定

新增、修改或刪除 IP 位址至裝置對應。

概要

| | |
|---|---|
| URI | `/api/v1/token/{apiKey}/verdicts:update` |
| HTTP 方法 | POST |

說明

第三方 Device-ID 會從您網路中的第三方 IoT 偵測來源擷取資料，並建立 IP 位址至裝置對應，Prisma Access 可以使用這些對應，強制執行裝置特定的安全性政策規則。使用此 API 新增對應、修改現有對應或刪除對應。

您可以使用 `update` 欄位更新或修改對應，然後使用 `delete` 欄位刪除對應。

如果對應已存在，則 `update` 會使用要求內文中指定的屬性覆寫現有的裝置屬性。如果對應不存在，則 update 會建立新對應。


©2025 Palo Alto Networks, Inc.

此 API 不支援部分更新。如果您想要更新對應的特定屬性，則亦須為您不想要更新的屬性重新輸入先前的值。將屬性保留空白將消除現有值。

您一次最多可以更新或刪除 10,000 個對應。要求是原子級：成功回應意味著系統處理了一切，失敗回應意味著系統什麼都沒處理。

欄位

| 欄位 | 說明 |
| --- | --- |
| update | 一種 JSON 物件，其提供您想要更新或建立的 IP 位址至裝置對應的屬性。必須填入 IP 和至少一個其他屬性。 |
| delete | 一種 JSON 物件，其指定您要刪除的對應的 IP 位址。 |

例如：

```
{ "update": [ { "ip": "string", "serialNo": "string", "mac":
 "string", "category": "string", "vendor": "string", "model":
 "string", "os": "string", "osFamily": "string", "hostname":
 "string", "profile": "string", } ], "delete": [ { ip: "string" } ] }
```

成功回應

成功時，HTTP 回應代碼為 200。此外，回應還包含一個 JSON 物件，其中包含以下欄位：

| 欄位 | 說明 |
| --- | --- |
| updateTime | 一個 unix 時間戳記，表示要求何時成功。 |

例如：

```
{ "updateTime": unix-timestamp }
```

錯誤回應

發生錯誤時，HTTP 回應代碼為下列其中一個：

| 回應代碼 | 說明 |
| --- | --- |
| 400 | 要求無效。要求不完整或格式錯誤。請修復該要求，然後重試一次。 |
| 401 | 未授權的權杖。請嘗試重新產生 API 權杖。如果不起作用，請聯絡支援。 |


©2025 Palo Alto Networks, Inc.

| 回應代碼 | 說明 |
| --- | --- |
| 409 | 衝突。無法處理要求，因為還有另一個正在進行的更新或刪除工作。請在其他工作完成之後再試一次。 |
| 429 | 要求太多。無法處理要求，因為系統在特定時段發出了太多的要求。每秒不要超過一個要求。請稍候，然後再試一次。 |

此外，回應內文還包含以下欄位：

| 欄位 | 說明 |
| --- | --- |
| 代碼 | 錯誤代碼。 |
| 訊息 | 錯誤訊息。 |

### 更新物件

包含更新 IP 位址至裝置對應所需的資訊。此 JSON 物件具有以下欄位：

| 欄位 | 說明 |
| --- | --- |
| ip | 裝置的 IP 位址。 |
| updateTime | Unix 時間戳記，表示上次更新對應的時間。 |
| 類別 | 裝置類型。範例：印表機 |
| 廠商 | 裝置廠商。範例：SHARP Corporation |
| 型號 | 裝置型號。範例：MX-6070N |
| os | 裝置作業系統。範例：ThreadX 5 |
| osFamily | 裝置作業系統所屬的系列。範例：ThreadX RTOS |
| profile | 裝置設定檔。範例：Sharp 印表機 |

## 刪除所有裁定

從第三方 Device-ID 服務中刪除所有 IP 位址到裝置對應。

概要

| URI | /api/v1/token/{apiKey}/verdicts:all |
| --- | --- |


©2025 Palo Alto Networks, Inc.

| | |
|---|---|
| HTTP 方法 | DELETE |

說明

要求第三方 Device-ID 服務刪除第三方 Device-ID 服務中的所有 IP 位址到裝置對應。成功回應意味著該服務已刪除所有對應。錯誤回應意味著它無法刪除任何對應。

成功回應

成功時，HTTP 回應代碼為 200。回應內文是空的。

錯誤回應

發生錯誤時，HTTP 回應代碼為下列其中一個：

| 回應代碼 | 說明 |
|---|---|
| 401 | 未授權的權杖。請嘗試重新產生 API 權杖。如果不起作用，請聯絡支援。 |
| 409 | 衝突。系統無法處理要求，因為還有另一個正在進行的更新或刪除工作。請在其他工作完成之後再試一次。 |
| 429 | 要求太多。系統無法處理請求，因為系統在特定時段發出了太多的要求。每秒不要超過一個要求。請稍候，然後再試一次。 |

此外，回應內文還包含以下欄位：

| 欄位 | 說明 |
|---|---|
| 代碼 | 錯誤代碼。 |
| 訊息 | 錯誤訊息。 |

# 查詢裁定

擷取第三方 Device-ID 服務中的 IP 位址至裝置對應。

概要

| | |
|---|---|
| URI | /api/v1/token/{apiKey}/verdicts?<br>bookmark={STRING}&pageLen={INTEGER} |
| HTTP 方法 | GET |


©2025 Palo Alto Networks, Inc.

說明

傳回所有對應或子集。

若要傳回所有對應，請傳送一次要求，沒有任何參數。記下回應中的 `nextBookmark` 值。為附加至 URI 的 `bookmark` 使用該值來傳送另一個要求。呼叫者將重複查詢，直到回應中的 `count` 為空，表示其已傳回所有對應。

若要傳回對應的子集，請使用 `pageLen` 指定您要傳回的對應數目，最多 10000 個。

參數

此 API 接受下列參數：

| 參數 | 說明 |
| --- | --- |
| bookmark | （選用）在第一個要求之後使用，以傳回所有對應。 |
| pageLen | （選用）要擷取的對應數目。範圍為 1-10000。如果未指定，則預設值為 10000。 |

成功回應

成功時，HTTP 回應代碼為 200。此外，回應還包含一個 JSON 物件，其中包含以下欄位：

| 欄位 | 說明 |
| --- | --- |
| nextBookmark | 您在 bookmark 參數中使用的值，用來執行重複查詢，直到傳回了所有對應。 |
| count | 整數表示回應中傳回的對應數目。 |
| verdicts | 此物件包含要求中指定的對應。 |

例如：

```
{ "nextBookmark":CkcKVxdWVuY2USAggEEjFqCHN, "count":1,
 "verdicts" : [ { "ip":"10.10.10.10", "updateTime":1623974506,
 "mac":"0a:d4:5f:e9:96:10", "category":"Smartphone or Tablet",
 "vendor":"Apple Inc.", "model": "iPad2", "os": "iOS 9.3.6",
 "osFamily": "iOS", "profile": "iPad" } ] } }
```

錯誤回應

發生錯誤時，HTTP 回應代碼為下列其中一個：

| 回應代碼 | 說明 |
| --- | --- |


©2025 Palo Alto Networks, Inc.

| | |
|---|---|
| 400 | 要求無效。要求不完整或格式錯誤。<br>您應該在重試之前修復該要求。 |
| 401 | 未授權的權杖。 |
| 429 | 要求太多。無法處理要求，因為在特定時段發出了太多的要求。每秒不允許超過<br>候，然後重試一次。 |

此外，回應內文還包含以下欄位：

| 欄位 | 說明 |
|---|---|
| 代碼 | 錯誤代碼。 |
| 訊息 | 錯誤訊息。 |

### verdicts 物件

成功查詢 IP 位址至裝置對應時傳回的物件。此物件包含以下資訊：

| 欄位 | 說明 |
|---|---|
| ip | 裝置的 IP 位址。 |
| updateTime | Unix 時間戳記，表示上次更新對應的時間。 |
| 類別 | 裝置類型。範例：印表機 |
| 廠商 | 裝置廠商。範例：SHARP Corporation |
| 型號 | 裝置型號。範例：MX-6070N |
| os | 裝置作業系統。範例：ThreadX 5 |
| osFamily | 裝置作業系統所屬的系列。範例：ThreadX RTOS |
| profile | 裝置設定檔。範例：Sharp 印表機 |

## 依 IP 位址查詢裁定

根據 IP 位址擷取 IP 位址至裝置對應。


©2025 Palo Alto Networks, Inc.

概要

| URI | /api/v1/token/{apiKey}/verdicts?ip={STRING} |
|---|---|
| HTTP 方法 | GET |

說明

使用 IP 位址傳回對應的裝置對應。您可以提供最多 10 個 IP 位址的清單（以逗號分隔）來擷取多個對應，將其附加到 URI。

如果服務找不到與 IP 位址相關聯的對應，則不會傳回該 IP 位址的對應。

成功回應

成功時，HTTP 回應代碼為 200。此外，回應還包含一個 JSON 物件，其中包含以下欄位：

| 欄位 | 說明 |
|---|---|
| count | 整數表示回應中傳回的對應數目。 |
| verdicts | 此物件包含要求中指定的對應。 |

例如：

```
{ "count":1, "verdicts" : [ { "ip":"10.10.10.10",
 "updateTime":1623974506, "mac":"0a:d4:5f:e9:96:10",
 "category":"Smartphone or Tablet", "vendor":"Apple Inc.",
 "model": "iPad2", "os": "iOS 9.3.6", "osFamily": "iOS", "profile":
 "iPad" } ] } }
```

錯誤回應

發生錯誤時，HTTP 回應代碼為下列其中一個：

| 回應代碼 | 說明 |
|---|---|
| 400 | 要求無效。要求不完整或格式錯誤。<br>請修復該要求，然後重試一次。 |
| 401 | 未授權的權杖。 |
| 429 | 要求太多。系統無法處理要求，因為系統在特定時段發出了太多的要求。每秒不<br>請稍候，然後再試一次。 |

此外，回應內文還包含以下欄位：


©2025 Palo Alto Networks, Inc.

| 欄位 | 說明 |
| --- | --- |
| 代碼 | 錯誤代碼。 |
| 訊息 | 錯誤訊息。 |

## 查詢裁定統計資料

擷取有關第三方 Device-ID 服務的統計資料。

概要

| | |
| --- | --- |
| URI | /api/v1/token/{apiKey}/verdicts:statistics |
| HTTP 方法 | GET |

成功回應

成功時，HTTP 回應代碼為 200。此外，回應還包含一個 JSON 物件，其中包含以下欄位：

| 欄位 | 說明 |
| --- | --- |
| verdicts | 此物件包含有關租用戶中 IP 位址至裝置對應的統計資料。包含下列欄位：<br>• totalCount - 租用戶中 IP 位址至裝置對應的總數。<br>• totalUpdate - IP 位址至裝置對應自建立以來已更新的數目。<br>• totalDelete - IP 位址至裝置對應自建立以來已刪除的數目。 |
| requestRcvd | 此物件包含租用戶收到每種類型要求的次數：<br>• update - 收到的 更新裁定 要求數目。<br>• deleteAll - 收到的 刪除所有裁定 要求數目。<br>• query - 收到的 查詢裁定 和 依 IP 位址查詢裁定 要求數目。<br>• Statistics - 收到的 查詢裁定統計資料 要求數目。 |

例如：

```
{ "verdicts: { "totalCount":1, "totalUpdate":0, "totalDelete":0, },
 "requestRcvd": { "update":1, "deleteAll":0, "query":0,
 "statistics":1 } }
```

錯誤回應

發生錯誤時，HTTP 回應代碼為下列其中一個：

 ©2025 Palo Alto Networks, Inc.

| 回應代碼 | 說明 |
| --- | --- |
| 401 | 未授權的權杖。 |
| 429 | 要求太多。無法處理要求，因為在特定時段發出了太多的要求。每秒不允許超過<br>候，然後重試一次。 |

此外，回應內文還包含以下欄位：

| 欄位 | 說明 |
| --- | --- |
| 代碼 | 錯誤代碼。 |
| 訊息 | 錯誤訊息。 |


©2025 Palo Alto Networks, Inc.

# Prisma Access 多租用戶

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• 如需在 Prisma Access (Managed by Strata Cloud Manager) 管理多個租用戶的詳細資訊，請參閱 Prisma SASE。 | ❑ Prisma Access 授權 |

本節僅提供有關在 Prisma Access (Panorama) 中管理多個租用戶的資訊。如需在 Prisma Access (Managed by Strata Cloud Manager) 管理多個租用戶的詳細資訊，請參閱 Prisma SASE。

為了可讓您建立和管理多個 Prisma Access 執行個體，Prisma Access 提供多租用戶功能，這使您可以在單一 Panorama 設備（或在高可用性（HA）模式下的 2 個設備）上最多建立 200 個執行個體（租用戶），每個租用戶都有自己個別的範本和範本堆疊、裝置群組，以及存取網域。

現有或未來的非多租用戶部署不受多租用戶影響，將繼續正常運作。我們建議您僅在您的組織需要在 Prisma Access 中管理多個租用戶時才啟用多租用戶功能。

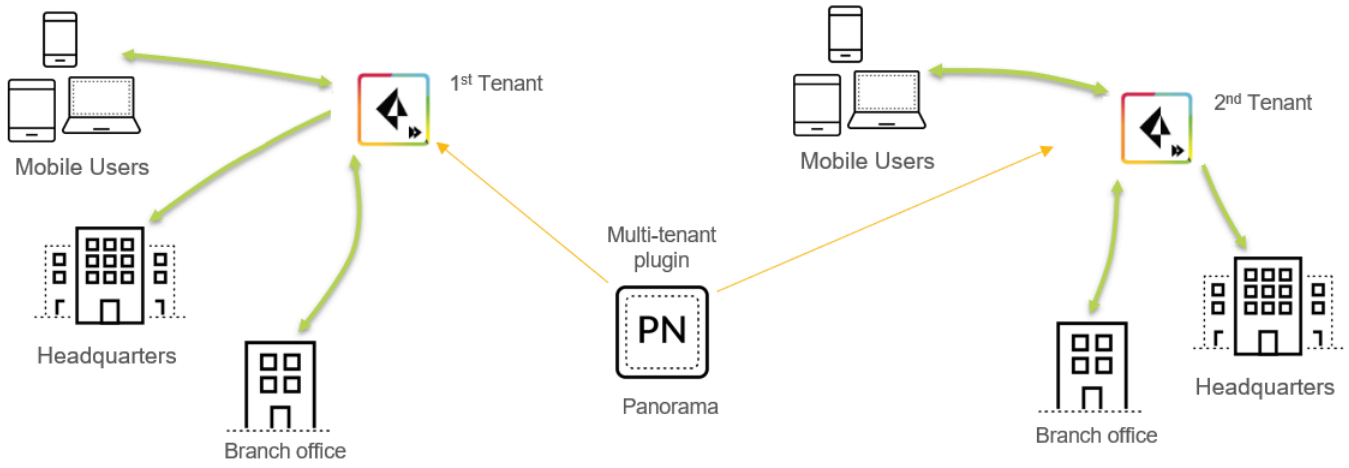
本節僅提供您為遠端網路、行動使用者或遠端網路與行動使用者部署的組合設定租用戶所執行的工作。若要設定 Clean Pipe 服務，請參閱 Prisma Access for Clean Pipe。

# 多租用戶設定概要

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• 如需在 Prisma Access (Managed by Strata Cloud Manager) 管理多個租用戶的詳細資訊，請參閱 Prisma SASE。 | ❑ Prisma Access 授權 |

啟用多租用戶可讓您在單一的 Panorama 設備上托管多個 Prisma Access 執行個體。每個執行個體稱為租用戶。

Prisma Access 租用戶會取得自己的專用 Prisma Access 執行個體，並且這些執行個體不會在租用戶之間共用。



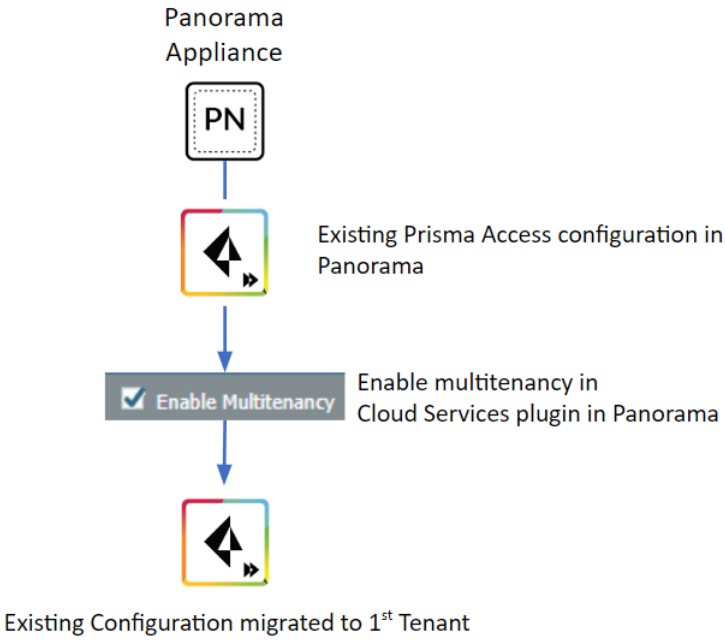

使用以下工作流程，來設定在單一 Panorama 設備中管理多個租用戶的能力：


©2025 Palo Alto Networks, Inc.

**STEP 1 |** 啟用多租用戶。如果您有現有的 Prisma Access 執行個體，啟用多租用戶會自動將您現有的 Prisma Access 設定移轉到第一個租用戶。

您會給與第一個（已移轉）租用戶一個名稱，並指定存取網域。Prisma Access 會移轉範本、範本堆疊，以及與現有設定相關聯的裝置群組，並將它們與您建立的存取網域建立關聯。

在您移轉初始設定之後，Panorama 中的管理使用者會成為超級使用者，具備建立和管理所有 Prisma Access 租用戶的能力。




**STEP 2 |** 然後，將租用戶新增到 Prisma Access。

若要部署多個租用戶，請確保您有以下授權最低需求：

若要確定您從 *Panorama* 獲得的 *Prisma Access* 授權類型，請選取 ***Panorama*** > ***Licenses***（授權）。

- 如果您有商業、商業進階、零信任網路存取 **(ZTNA)** 安全網際網路閘道 **(SIG)** 或企業授權，請使用下列下限作為指導方針：

  **Prisma Access for Networks** 和 **Prisma Access for Users**：

  如果您有 **Local**（本機）版本，每個租用戶需要至少 200 個單位，而且所有租用戶都將是本機。

  如果您有 **Worldwide**（全球）版本，則需要至少 1,000 個單位，才能建立 **Worldwide**（全球）租用戶。如果您為租用戶配置 200 到 999 個單位，則 Prisma Access 會建立一個

 ©2025 Palo Alto Networks, Inc.

**Local**（本機）租用戶；如果您為租用戶配置 1000 個或更多單位，則 Prisma Access 會建立一個 **Worldwide**（全球）租用戶。

單位對應於 Prisma Access for Remote Networks 的頻寬 (以 Mbps 為單位)，以及 Prisma Access for Users 的行動使用者數目。

- 如果您的授權類型以 **GlobalProtect Cloud Service**（**GlobalProtect** 雲端服務）開頭，請使用下列下限作為指導方針：

  **Prisma Access for Networks**—在您的授權中您必須具有至少 200 Mbps 可供每個租用戶使用。

  **Prisma Access for Users**—在您的授權中您必須具有至少 200 個行動使用者可供每個租用戶使用。

  在這兩種類型的 Prisma Access 設定中，您可以新增任一類型的額外授權（超過這些下限）。您可以在裝載之後為任何租用戶增加或減少頻寬或行動使用者配置，只要您保留每個租用戶最低的必要配置，以及不超過整體授權容量。

您可以僅為遠端網路、僅為行動使用者或為兩者設定多租用戶設定。啟用多租用戶時，您會根據每個租用戶配置授權。

如果您有遠端網路和行動使用者的授權，則可以設定個別租用戶，其中僅包含行動使用者或僅包含遠端網路。例如，如果您的 Prisma Access 部署具有行動使用者和遠端網路的 **Worldwide**（全球）版本授權，則您可以僅為行動使用者設定一個租用戶，只要您為租用戶指定至少 1,000 個行動使用者。

對於您在第一個租用戶之後建立的每個租用戶，Prisma Access 自動為每個租用戶建立範本、範本堆疊和裝置群組組，並將它們與您建立的存取網域建立關聯。Prisma Access 會建立此環境，以允許您根據租用戶的裝置群組和範本使用管理角色，然後根據該角色建立管理使用者，來建

 ©2025 Palo Alto Networks, Inc.

立租用戶層級管理使用者。這樣，您會建立一個管理使用者，存取單一租用戶，但不允許該使用者存取 Panorama 設備管理的其他租用戶。

Prisma Access 使用以下命名慣例來建立範本堆疊、範本和裝置群組：

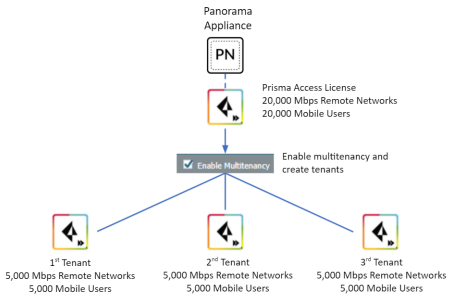
- 一個名為 **sc-stk-***tenant* 的服務連線範本堆疊，其中 *tenant* 是租用戶的名稱。
- 一個名為 **sc-tpl-***tenant* 的服務連線範本。
- 一個名為 **sc-dg-***tenant* 的服務連線裝置群組。
- 一個名為 **mu-stk-***tenant* 的行動使用者範本堆疊。
- 一個名為 **mu-tpl-***tenant* 的行動使用者範本。
- 一個名為 **mu-dg-***tenant* 的行動使用者裝置群組。
- 一個名為 **rn-stk-***tenant* 的遠端網路範本堆疊。
- 一個名為 **rn-tpl-***tenant* 的遠端網路範本。
- 一個名為 **rn-dg-***tenant* 的遠端網路裝置群組。
- 一個名為 **ep-stk-***tenant* 的明確 Proxy 範本堆疊。
- 一個名為 **ep-tpl-***tenant* 的明確 Proxy 範本。
- 一個名為 **ep-dg-***tenant* 的明確 Proxy 裝置群組。
- 一個名為 **cp-stk-***tenant* 的 Clean Pipe 範本堆疊。
- 一個名為 **cp-tpl-***tenant* 的 Clean Pipe 範本。
- 一個名為 **cp-dg-***tenant* 的 Clean Pipe 裝置群組.

所有 Prisma Access 類型都會建立範本堆疊、範本和裝置群組，即使是您可能未獲得授權的類型。例如，如果您購買遠端網路的授權，則 Prisma Access 會自動為遠端網路、行動使用者和 Clean Pipe 建立範本堆疊、範本和裝置群組。

如果您新增自訂範本，它們不能優先於 Prisma Access 建立的範本。

您根據與 Panorama 中雲端服務外掛程式相關聯的授權，為每個租用戶配置遠端網路和行動使用者授權資源。

下圖顯示一個範例，其中使用一個授權搭配 20,000 Mbps 遠端網路頻寬集區和 20,000 個行動使用者進行 Prisma Access 部署。管理員已為現有設定配置了 5000 Mbps 遠端網路頻寬和 5000 個行動使用者。在管理員啟用了多租用戶之後，授權配置隨著所有其他設定移轉到第一個租用戶。然後，管理員建立了額外的租用戶，每個租用戶具有 5,000 Mbps 的遠端網路頻寬集區，以及每個租用戶 5,000 個行動使用者。Prisma Access 會從整體授權配置中配置授權資源。在您完成此設定之後，授權中有 5,000 Mbps 的遠端網路頻寬和 5,000 個行動使用者可用。




 ©2025 Palo Alto Networks, Inc.

# 規劃您的多租用戶部署

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• 如需在 Prisma Access (Managed by Strata Cloud Manager) 管理多個租用戶的詳細資訊，請參閱 Prisma SASE。 | • Prisma Access 授權 |

在啟用多租用戶、移轉第一個租用戶，並建立其他租用戶之前，請完成以下工作，確保您具有執行此操作所需的所有資訊和資源：

- 如果您是將現有的單一租用戶部署移轉至多租用戶部署，請注意以下不支援的 Prisma Access 功能。如需不受支援的功能清單，請參閱 Palo Alto Networks 相容性矩陣。
- 如果沒有現有的 Prisma Access 設定，您可以 **Enable Multitenancy**（啟用多租用戶），並新增您的租用戶；然後，在建立租用戶之後對其進行設定。如需詳細資訊，請參閱 建立全新的多租戶部署。
- 記下遠端網路和行動使用者的授權配置。

  開啟您的授權（**Panorama > Licenses**（授權）），然後尋找遠端網路的 Prisma Access **Total Mbps**（總 **Mbps**）（遠端網路頻寬集區），以及行動使用者的 **User Limit**（使用者限制）（授權使用者總數）。

  建立租用戶時，您可以從這個授權配置中為遠端網路和行動使用者指派資源。如果用光了遠端網路或行動使用者所需的最低授權 Mbps，則您無法建立額外的租用戶。

  您還應記下現有設定的頻寬和行動使用者配置。將您的設定移轉到第一個租用戶後，請檢查這些值以驗證是否已正確移轉第一個租用戶。
- 列出您將用來識別每個租用戶的名稱。

  建立租用戶名稱時，請避免使用類似 *Tenant-1*、*Tenant-2*、*Tenant-3* 等名稱。系統日誌會在日誌輸出中為租用戶名稱保留少量字元，如果租用戶具有相似的名稱，則可能難以將租用戶與日誌建立關聯。我們建議為租用戶使用唯一且簡短的名稱（例如，*Acme or Hooli*）。
- 列出您將為每個租用戶建立和指派的管理使用者，並記下可以同時登入的管理使用者數目。

  當管理使用者執行正常的多租用戶操作（例如設定變更和提交操作）時，我們建議最多 12 個管理使用者同時登入 Panorama。

  可以管理多個租用戶的管理使用者可以透過單一提交操作同時佈建最多 200 個租用戶。
- 確保您有足夠的授權資源來啟用多個租用戶。

  每個租用戶的最低授權配置為每個遠端網路 200 Mbps，或 200 個行動使用者。您還可以建立一個僅有遠端網路或行動使用者的租用戶，並可以在同一 Panorama 上設定不同設定的租用戶。例如，您可以建立僅有遠端網路的租用戶、僅有行動使用者的租用戶，或同時具有行動使用者和遠端網路的租用戶，只要每個租用戶都符合最低授權配置需求，而且相關授權已啟動，並與您在其中設定租用戶的 Panorama 相關聯。


©2025 Palo Alto Networks, Inc.

- 在多租用戶模式下設定租用戶時，請為每個 IPSec 通道和 IKE 閘道建立唯一名稱，進行服務連線和遠端網路連線，並嘗試使用另一個租用戶將不會複製的名稱。雖然對功能沒有影響，但如果另一個租用戶正在使用同名的通道或閘道，則您無法刪除 IPSec 通道或 IKE 閘道。

  此警告適用於所有物件，包括 QoS 設定檔（如果其中一個物件被另一個租用戶參考，則您無法刪除多租用戶部署中具有重複名稱的物件）。
- 單一租用戶使用者無法檢視系統日誌；只有超級使用者才能檢視。不過，您可以依租用戶排序日誌。
- 當行動使用者登入單一 Prisma Access 租用戶時，使用者會耗用一個授權單位。如果使用者在單一多租用戶部署下登入其他租用戶，則該使用者會針對其登入的每個租用戶耗用一個授權單位。例如，如果單一使用者登入 5 個租用戶，則該使用者總共耗用 5 個行動使用者授權單位。
- 使用多租用戶功能，並以租用戶層級管理使用者身分登入時，開啟 Panorama 工作管理員（按一下 Panorama 網頁介面底部的 **Tasks**（工作））會顯示所有租用戶的所有工作，包括在超級使用者 (Admin) 層級完成的任何工作。
- 不支援一些 Prisma Access 功能與多租用戶搭配使用。如需詳細資訊，請參閱 Palo Alto Networks 相容性矩陣中不支援多租用戶的功能。
- 如果您備份 Panorama 設定，然後將其還原至先前儲存的設定，則若您依下列順序執行下列動作。Panorama 無法還原至您儲存的設定：

  1. 備份 Panorama 設定。
  2. 刪除租用戶。
  3. 還原設定。

  如果刪除租用戶，則您無法使用在刪除租用戶之前儲存的任何先前備份。不過，您可以使用在刪除租用戶之後所做的任何備份。


©2025 Palo Alto Networks, Inc.

# 建立全新的多租戶部署

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• 如需在 Prisma Access (Managed by Strata Cloud Manager) 管理多個租用戶的詳細資訊，請參閱 Prisma SASE。 | ❑ Prisma Access 授權 |

如果想要建立多租用戶部署且沒有現有的 Prisma Access 設定，您可以 **Enable Multitenancy**（啟用多租用戶）並新增您的租用戶；然後在建立租用戶之後對其進行設定。

如果您有現有的單一租用戶部署，並想要移轉到多租用戶部署，請使用工作流程啟用多租用戶並移轉第一個租用戶。

當您在沒有現有設定的情況下建立第一個租用戶時，請確保遵循以下差異和指導方針：

- 由於沒有要移動的設定，因此 Prisma Access 會為每個租用戶建立範本、範本堆疊和裝置群組，並將它們與您在建立租用戶期間建立的存取網域建立關聯。如需 Prisma Access 使用的命名慣例，請參閱 多租用戶設定概要。
- 或者，在建立租用戶層級存取網域之後，您可以 建立一個管理使用者，透過將管理員與存取網域建立關聯來允許對單一租用戶進行管理。
- 如果您有任何現有範本或裝置群組（例如，來自內部部署裝置的範本，此裝置是由 Prisma Access 也應使用的 Panorama 管理），請確保在建立和設定 **Access Domain**（存取網域）時將這些裝置群組和範本網域新增至其中。如果未將裝置群組和範本新增至存取網域，則在雲端服務外掛程式中設定 Prisma Access 元件時，您無法檢視或選取它們。


©2025 Palo Alto Networks, Inc.

# 啟用多租戶並移轉第一個租用戶

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• 如需在 Prisma Access (Managed by Strata Cloud Manager) 管理多個租用戶的詳細資訊，請參閱 Prisma SASE。 | ❑ Prisma Access 授權 |

使用下列工作流程啟用多租用戶，並將現有設定移轉到您建立的第一個租用戶。如果沒有任何現有的設定，您可以啟用多租用戶並新增租用戶；然後設定它們。

當您啟用多租用戶時，Prisma Access 會移轉以下設定元件：

- 所有服務連線和遠端網路通道裝載訊息，包括通道設定。
- 現有行動使用者裝載資訊。
- Strata Logging Service 資訊。
- 現有的自發 DEM (ADEM) 設定
- 用於服務連線、遠端網路和行動使用者的範本、範本堆疊和裝置群組。

您需要指定要為每個部署配置的使用者數目（用於行動使用者部署）、頻寬（用於遠端網路部署）和自發 DEM (ADEM)（如果您已購買 ADEM 授權）。

由於這些裝置群組變更，您需要建立一個存取網域，並新增移轉的裝置群組、範本和範本堆疊，如下列工作流程所示。

如果您沒有現有的 *Prisma Access* 設定，並且您正在建立全新的多租用戶部署，請勿使用此工作流程；相反，請完成 將租用戶新增 Prisma Access 中的步驟建立第一個租用戶。

**STEP 1 |** 確定要指派給此部署的授權單元數目。

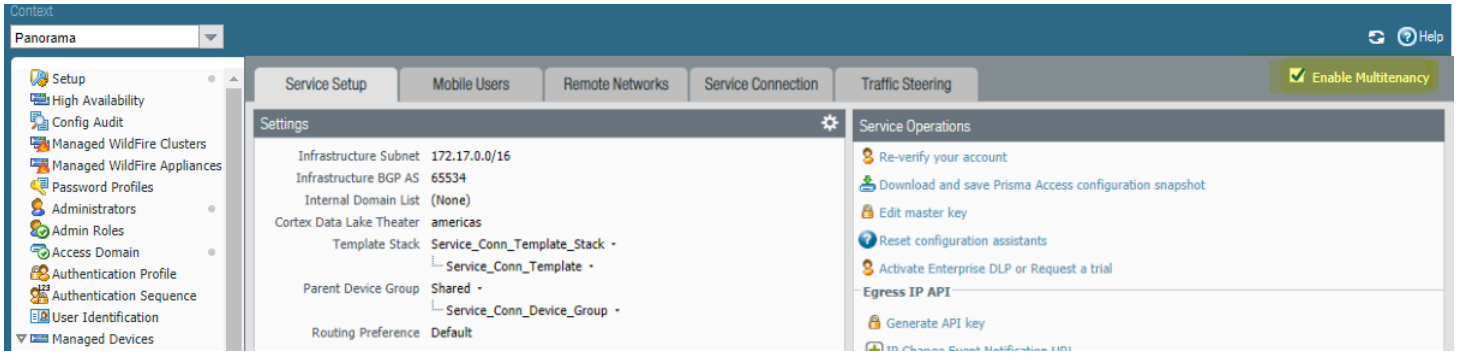
儘管 Prisma Access 將您的設定移轉到第一個租用戶，但您需要指定：

- 要為租用戶的遠端使用者部署配置的 **Bandwidth**（頻寬）（如果適用）。
- 要為租用戶的行動使用者部署配置的 **Users**（使用者）（如果適用）。
- 要為行動使用者和遠端網路配置的 ADEM 單元數目（如果適用）。

**STEP 2 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定）。


©2025 Palo Alto Networks, Inc.

**STEP 3 |** 選取 **Enable Multitenancy**（啟用多用租戶）（位於頁面右上角）。




在啟用多租用戶之後，Panorama 會顯示一則通知，告知您現有的 Prisma Access 設定移至第一個租用戶。

在啟用多租用戶之後，您的部署會永久變更為多租用戶部署，且您無法將其還原為單一租用戶模式。

**STEP 4 |** 按一下 **OK**（確定），將現有設定移轉到第一個租用戶。

即會顯示 **Tenants**（租用戶）頁面，並在視窗中央顯示圓餅圖。

- 如果您有遠端網路或行動使用者授權，則會顯示授權遠端網路頻寬和行動使用者的可用數量。
- （僅限遠端網路和行動使用者部署）如果已購買自發 DEM 授權，則會顯示供 ADEM 使用的可用單元數目。
- 如果您有 Clean Pipe 部署，則會顯示租用戶的頻寬量。

**STEP 5 |** 選擇要用於租用戶的部署類型。

- 對於遠端網路、行動使用者部署，或若要為租用戶設定兩種部署類型，請選取 **Remote Networks/Mobile Users**（遠端網路/行動使用者）。
- 對於 Clean Pipe 部署，請選取 **Clean Pipe**。

  本節僅描述如何為遠端網路、行動使用者或遠端網路和行動使用者部署類型設定租用戶。若要設定 Clean Pipe 服務，請參閱 Prisma Access for Clean Pipe。


©2025 Palo Alto Networks, Inc.

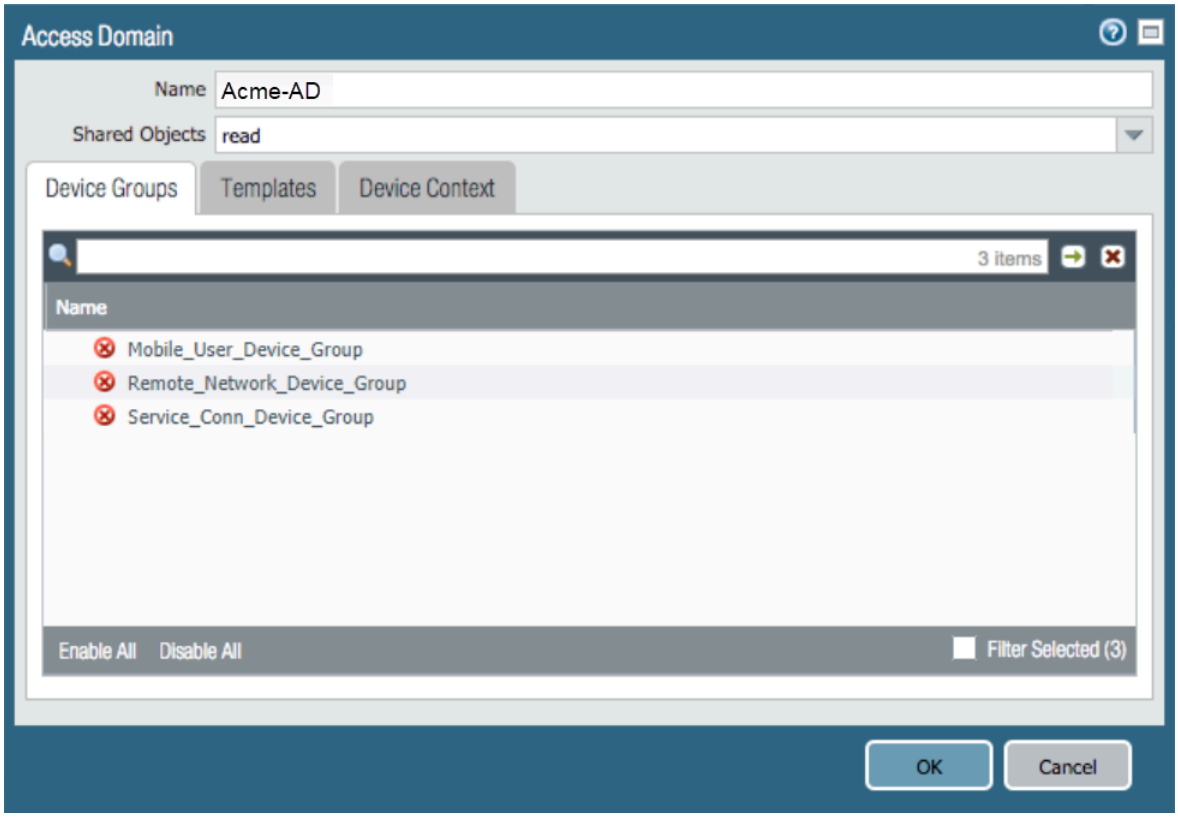
**STEP 6 |** 將現有設定移轉到第一個租用戶。

第一個移轉的子租用戶的名稱是從您正在移轉的租用戶中自動填入的，並且無法進行編輯。

1. 按一下向下箭頭選取 **New Access Domain**（新增存取網域）來建立新的 **Access Domain**（存取網域）。
2. 輸入存取網域的 **Name**（名稱），並按一下 **OK**（確定）。

   Prisma Access 會將 **Mobile_User_Device_Group**、**Remote_Network_Device_Group** 和 **Service_Conn_Device_Group Device Groups**（裝置群組）新增至新的存取網域。

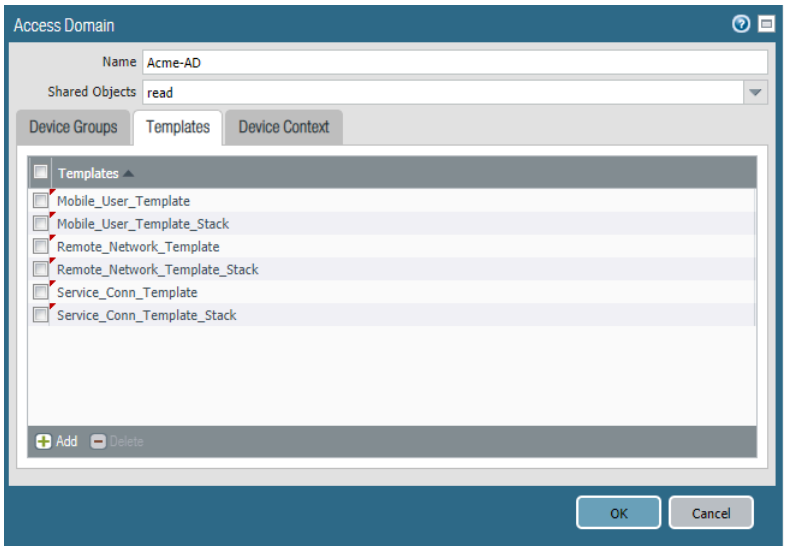
   請勿將預設裝置群組和範本與第一個移轉的子租用戶以外的其他子租用戶建立關聯。




3. （選用）按一下 **Templates**（範本） 以驗證 Prisma Access 是否已新增以下範本和範本堆疊：
   - **Explicit_Proxy_Template**
   - **Explicit_Proxy_Template_Stack**
   - **Mobile_User_Template**
   - **Mobile_User_Template_Stack**
   - **Remote_Network_Template**
   - **Remote_Network_Template_Stack**
   - **Service_Conn_Template**
   - **Service_Conn_Template_Stack**

 ©2025 Palo Alto Networks, Inc.

這些是標準 Prisma Access 部署的預設範本堆疊和範本；如果您新增了其他範本，請確保 Prisma Access 已新增它們。

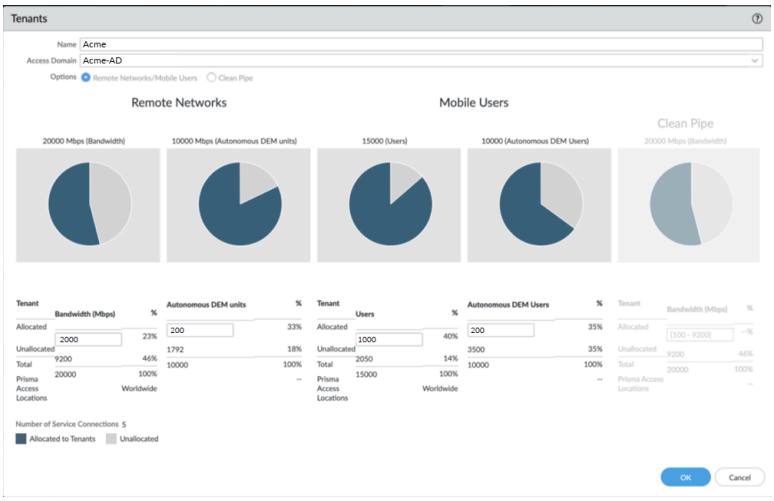



4. （選用）如果您有與此設定相關聯的其他範本，請選取它們。
5. 按一下 **OK**（確定）以關閉 **Access Domain**（存取網域）頁面，並返回 **Tenants**（租用戶）頁面。

**STEP 7 |** 在遠端網路的 **Bandwidth (Mbps)**（頻寬 **(Mbps)**）、行動使用者的 **Users**（使用者），以及要為每種部署類型配置的 **Autonomous DEM Users**（自發 **DEM** 使用者）數目中輸入值。

為租用戶配置 ADEM 單元時，請使用以下指導方針：

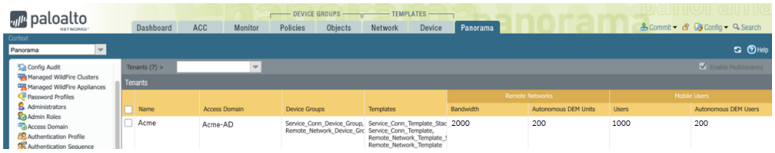
- 您可以為行動使用者和遠端網路配置的 ADEM 單元數目只能等於或小於基礎授權。
- 您可以配置的單位數目下限為 200。
- 為租用戶配置 ADEM 單元之後，您可以編輯或移除這些單位。
- 如果您沒有為部署類型（行動使用者或遠端網路）購買 ADEM 授權，則該選項會呈現灰色。




 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** 按一下 **OK**（確定）。

**Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定）頁面顯示第一個成功移轉的租用戶，並且在 **Tenants**（租用戶）區域上方新增了 **Tenants**（租用戶）下拉式清單。



**STEP 9 |** 確保所有範本和裝置群組都已填入租用戶中。

1. 從下拉式清單中選取租用戶。
2. 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定）。
3. 選取 **Service Setup**（服務設定）。
4. 按一下齒輪以編輯 **Settings**（設定）。
5. 確保正確的範本堆疊、範本和裝置群組（分別為 Service_Conn_Template_Stack、Service_Conn_Template 和 Service_Conn_Device_Group）已填入設定中。
6. 前往您具有其現有設定的其他標籤（例如，**Mobile Users**—**GlobalProtect**（行動使用者—**GlobalProtect**）、**Mobile Users**—**Explicit Proxy**（行動使用者—明確 **Proxy**）、**Remote Networks**（遠端網路）或 **Service Connection**（服務連線）），按一下齒輪以編輯 **Settings**（設定），並確保正確的範本堆疊、範本和裝置群組已填入設定中。

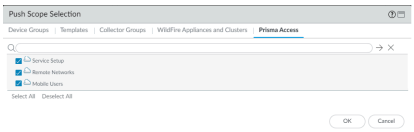
**STEP 10 |** 在本機將您的變更提交到 Panorama (**Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**）。

**STEP 11 |** 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**），以在管理 Prisma Access 的 Panorama 上本機儲存您的變更。

如果您未執行本機提交，則在提交並推送您的變更時，Prisma Access 元件不會顯示在推送範圍中。

**STEP 12 |** 提交並推送您的變更，以使其在 Prisma Access 作用中。

1. 選取 **Commit**（提交） > **Commit and Push**（提交並推送），然後在 Push Scope（推送範圍）中 **Edit Selections**（編輯選擇）。
2. 選取 **Prisma Access**，然後選取您建立的租用戶、**Service Setup**（服務設定）、**Remote Networks**（遠端網路）和 **Mobile Users**（行動使用者）。

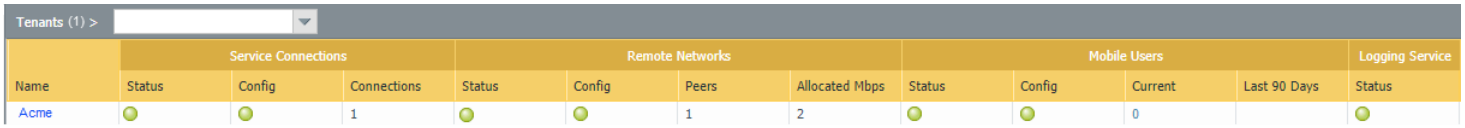


3. 按一下 **Ok**（確定），以儲存您對 Push Scope（推送範圍）所做的變更。
4. **Commit**（提交）並 **Push**（推送）您的變更。

 ©2025 Palo Alto Networks, Inc.

**STEP 13 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態）。

狀態頁面顯示所有租用戶的狀態。因為您僅建立了一個租用戶，所以該租用戶是唯一顯示的租用戶。如果從下拉式清單中選取該租用戶，則會顯示該租用戶的詳細狀態。




從下拉式清單中選取一個租用戶，您將返回該租戶的狀態頁面。

**STEP 14 |** 繼續新增更多租用戶至 Prisma Access。

 ©2025 Palo Alto Networks, Inc.

# 將租用戶新增 Prisma Access

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• 如需在 Prisma Access (Managed by Strata Cloud Manager) 管理多個租用戶的詳細資訊，請參閱 Prisma SASE。 | ❑ Prisma Access 授權 |

以第一個租用戶身分移轉現有資訊之後，您可以建立和設定其他租用戶。對於您在第一個租用戶之後建立的每個租用戶，Prisma Access 會建立個別的存取網域，其中包含自己的一組範本堆疊和範本，以及自己的網域群組。

使用此工作流程，將更多租用戶新增至 Prisma Access。

如果您要建立全新的多租戶部署，請使用此工作流程來新增第一個租用戶，以及其他租用戶。如需詳細資訊，請參閱 建立全新的多租戶部署。

**STEP 1 |** 以超級使用者身分登入 Panorama。

**STEP 2 |** 新增和設定租用戶。

1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定），然後 **Add**（新增）租用戶。

   確定您選取 **Remote Networks/Mobile Users**（遠端網路/行動使用者）；若要建立和設定 Clean Pipe 部署，請參閱Prisma Access for Clean Pipe。
2. 為租用戶指定描述性 **Name**（名稱）。
3. **Add**（新增）**Access Domain**（存取網域）、為它提供描述性 **Name**（名稱），然後按一下 **OK**（確定），以回到 **Tenants**（租用戶）視窗。

   在您按一下 **OK**（確定）之後，Prisma Access 會自動建立範本、範本堆疊和裝置群組，並將它們與您建立的存取網域建立關聯。

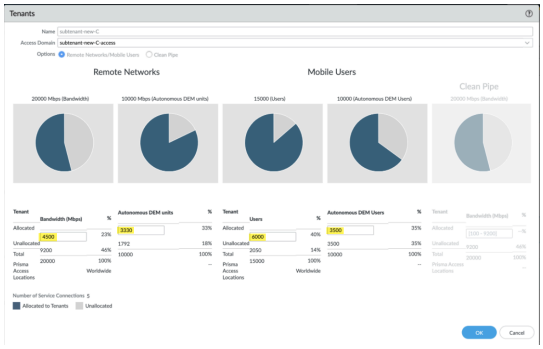
**STEP 3 |** 指定要為 **Remote Networks**（遠端網路）配置的 **Bandwidth (Mbps)**（頻寬 **(Mbps)**）數量，以及要為 **Mobile Users**（行動使用者）配置的 **Users**（使用者）數目。


©2025 Palo Alto Networks, Inc.

**STEP 4 |** (僅使用自發 DEM 進行部署）如果您購買了自發 DEM (ADEM) 授權，請選取要為 ADEM 配置的單位數目。

為租用戶配置 ADEM 單元時，請使用以下指導方針：

- 您可以為行動使用者和遠端網路配置的 ADEM 單元數目只能等於或小於基礎授權。
- 您可以配置的單位數目下限為 200。
- 為租用戶配置 ADEM 單元之後，您可以編輯或移除這些單位。
- 如果您沒有為部署類型（行動使用者或遠端網路）購買 ADEM 授權，則該選項會呈現灰色。

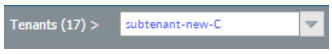



**STEP 5 |** 按一下 **OK**（確定）以建立第一個租用戶。

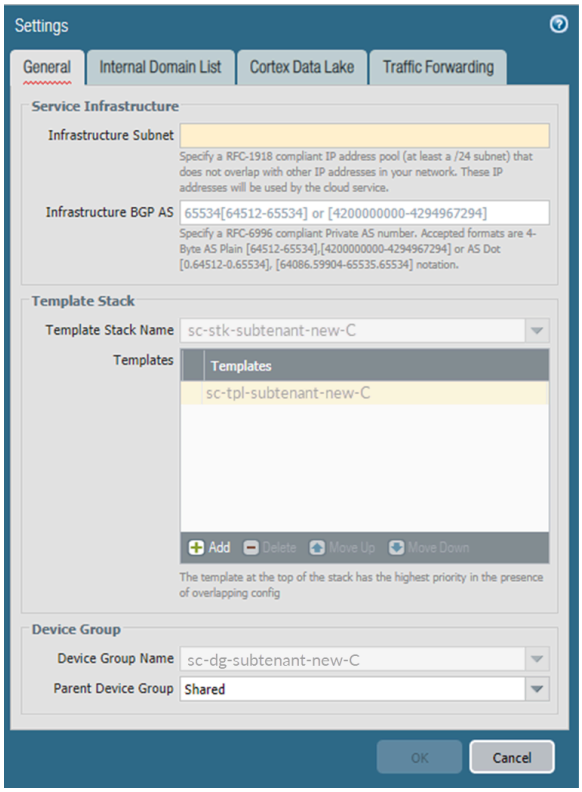

©2025 Palo Alto Networks, Inc.

**STEP 6 |** 確保 Prisma Access 已將範本堆疊、範本和裝置群組連線設定套用至您剛建立的租用戶的服務連線設定。

1. 從 **Tenant**（租用戶）下拉式清單中選取您建立的租用戶。



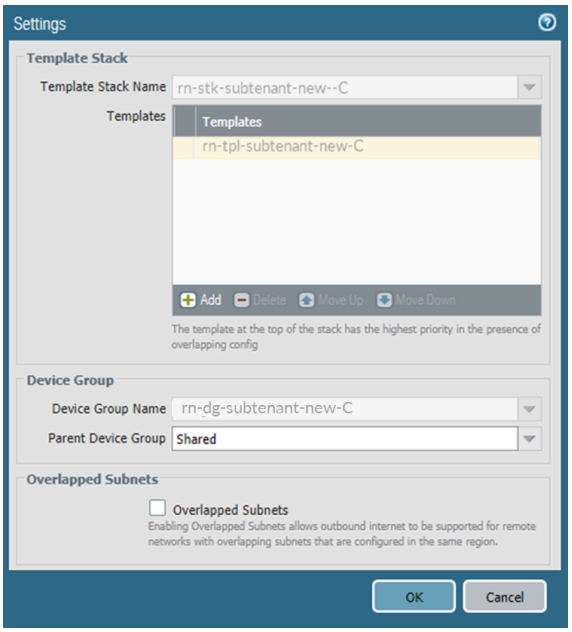

2. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定）。
3. 按一下 **Settings**（設定）區域右側的齒輪圖示以編輯設定。
4. 確保 Prisma Access 已將範本堆疊 **(sc-stk-*tenant*)**、範本 **(sc-tpl-*tenant*)** 和裝置群組 **(sc-dg-*tenant*)** 新增到您的服務連線設定。
5. 確保 **Parent Device Group**（父系裝置群組)設定為 **Shared**（共用），然後按一下 **OK**（確定）。




 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** 確保 Prisma Access 已將範本堆疊、範本和裝置群組新增到遠端網路設定。

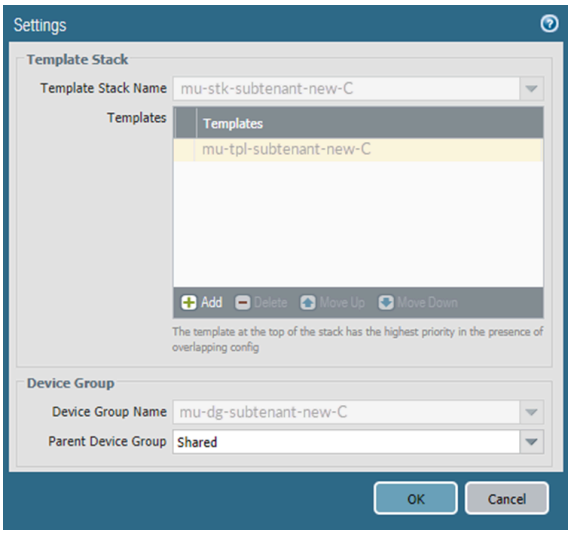
1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（組態） > **Remote Networks**（遠端網路），然後按一下 **Settings**（設定）區域右側的齒輪圖示以編輯設定。。
2. 確保 Prisma Access 已將範本堆疊 **(rn-stk-*tenant*)**、範本 **(rn-tpl-*tenant*)** 和裝置群組 **(rn-dg-*tenant*)** 新增到您的遠端網路設定。
3. 確保 **Parent Device Group**（父系裝置群組)設定為 **Shared**（共用），然後按一下 **OK**（確定）。




 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** 確保 Prisma Access 已將範本堆疊、範本和裝置群組新增到行動使用者設定。

1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（組態） > **Mobile Users**（行動使用者），然後按一下 **Settings**（設定）區域右側的齒輪圖示以編輯設定。。
2. 確保 Prisma Access 已將範本堆疊 **(mu-stk-*tenant*)**、範本 **(mu-tpl-*tenant*)** 和裝置群組 **(mu-dg-*tenant*)** 新增到您的遠端網路設定。
3. 確保 **Parent Device Group**（父系裝置群組)設定為 **Shared**（共用），然後按一下 **OK**（確定）。




**STEP 9 |** 在本機將您的變更提交到 Panorama **(Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**）。

**STEP 10 |** **(**僅限行動使用者部署）—新增基礎結構子網路，然後提交並推送您的變更以使其在 Prisma Access 作用中.

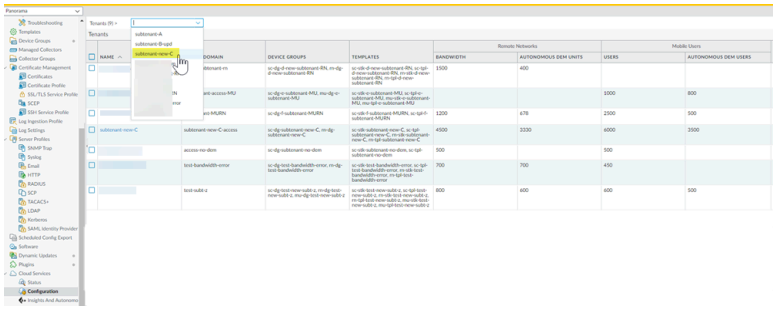
行動使用者變更若要生效，需要這些步驟。

1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（組態） > **Service Setup**（服務設定）、按一下齒輪圖示以編輯設定，然後設定基礎結構子網路。
2. 在推送範圍中選取 **Commit**（提交） > **Commit and Push**（提交並推送）、**Edit Selections**（編輯選取項目），並確保已選取 **Mobile Users(**行動使用者**)**。
3. 按一下 **Ok**（確定），以儲存您對 Push Scope（推送範圍）所做的變更。
4. **Commit**（提交）並 **Push**（推送）您的變更。

 ©2025 Palo Alto Networks, Inc.

**STEP 11 |** 選取您透過選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（組態） > ***tenant-name*** 所建立的新租用戶，然後繼續設定您的租用戶。

1. 設定服務基礎結構。
2. 建立服務連線以允許存取私人應用程式。.
3. 裝載和設定遠端網路，如果您已獲得遠端網路授權的話。
4. 為 Prisma Access (Managed by Panorama) 設定全域保護，如果您已獲得遠端使用者授權的話。



 ©2025 Palo Alto Networks, Inc.

# 刪除租用戶

完成以下步驟來刪除 Prisma Access (Managed by Panorama) 部署中的租用戶。

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• 如需管理 Prisma Access (Managed by Strata Cloud Manager) 中多個租用戶的詳細資訊，請參閱 Prisma SASE。 | ❑ Prisma Access 授權 |

- 雖然您可以刪除多租用戶部署中的所有租用戶，但無法刪除您在其中新增或刪除租用戶的管理員層級 *Prisma Access* 設定。
- 當您刪除租用戶時，*Prisma Access* 會刪除您獲授權的範本和裝置群組集，但不會刪除未獲授權的集。例如，如果您有一個 *Prisma Access for Users* 授權，並刪除租用戶，*Prisma Access* 會刪除行動使用者相關的範本堆疊、範本和裝置群組，但不會刪除為未授權 *Prisma Access for Networks* 建立的集。您可以在刪除租用戶之後手動刪除這些未使用的範本和裝置群組集。

**STEP 1 |** 從管理 Prisma Access 的 Panorama 中，選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定）。

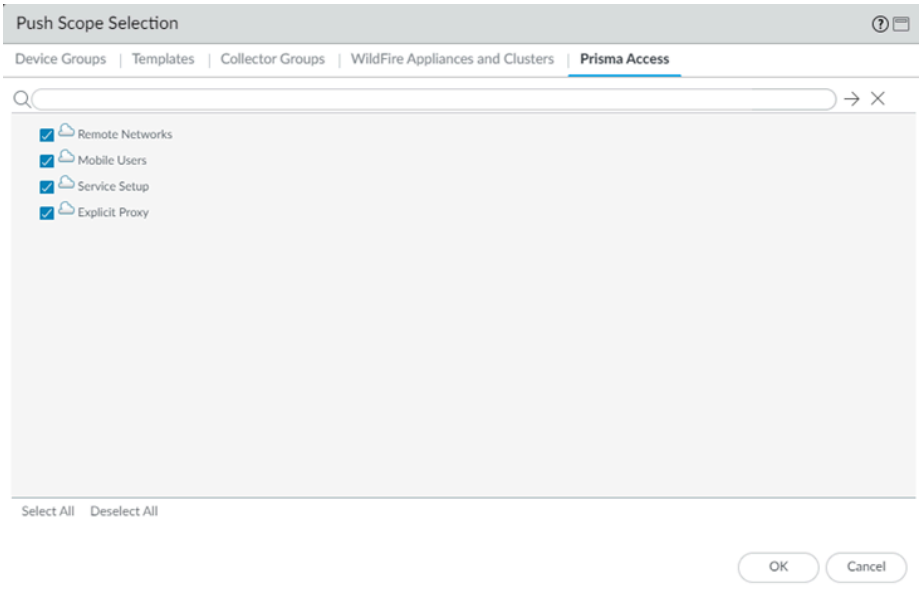
**STEP 2 |** 選取租用戶，然後刪除與其相關聯的所有設定。

執行此步驟作為最佳做法，以確保從租用戶中刪除所有設定，包括任何服務連線、行動使用者、遠端網路或 Clean Pipe 設定。


©2025 Palo Alto Networks, Inc.

**STEP 3 |** 提交並推送您對 Prisma Access 的變更。

1. 選取 **Commit**（提交） > **Push to Devices**（推送至裝置）。
2. **Edit Selections**（編輯選取項目），並確保您刪除的所有元件（包括遠端網路、行動使用者、服務設定、明確 Proxy 和 Clean Pipe，取決於您的部署）都已選取。




3. 按一下 **Push**（推送）。

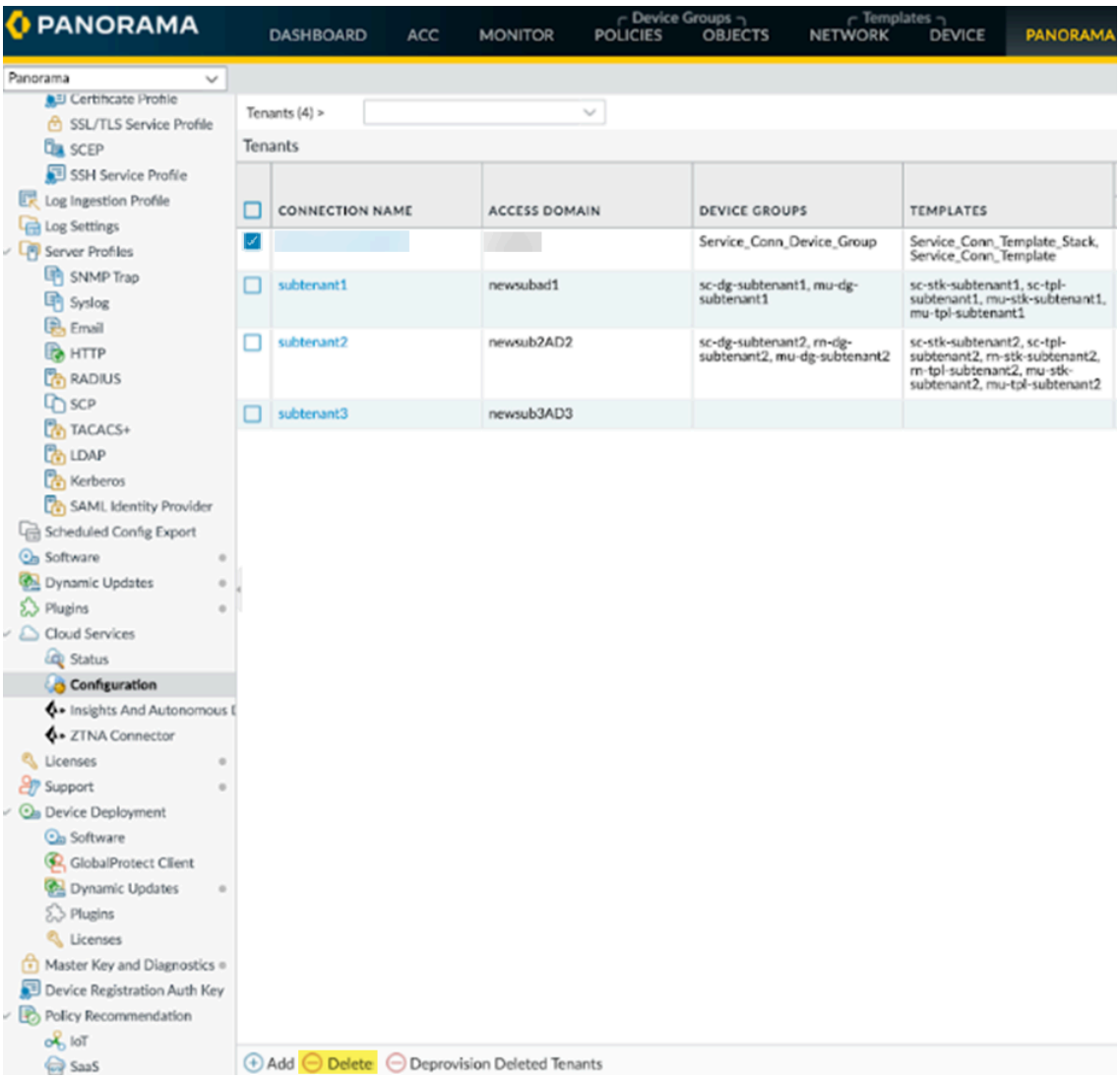
 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 選取一個或多個租用戶，然後將其 **Delete**（刪除）。

刪除租用戶會從 Panorama 中移除該租用戶，但不會從 Prisma Access 基礎結構中移除該租用戶。若要刪除租用戶並將其從基礎結構中移除，您可以將其刪除、執行本機提交，然後取消佈建它，如以下步驟所示。

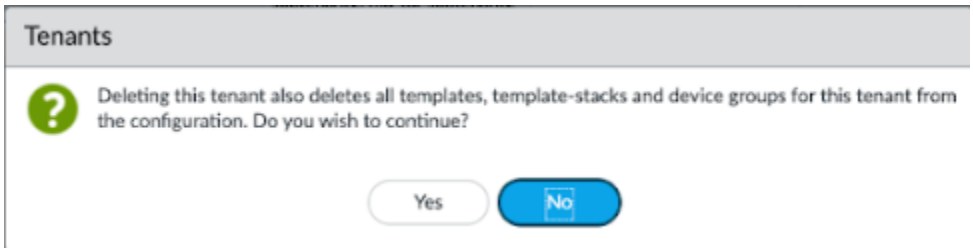
如果您刪除租用戶但未取消佈建它，則仍然可以透過聯絡 Palo Alto Networks 支援來擷取它。

如果您在 *HA* 設定中設定了 *Panorama*，則僅會從 *HA* 配對中的作用中 *Panorama* 執行刪除和取消佈建操作。



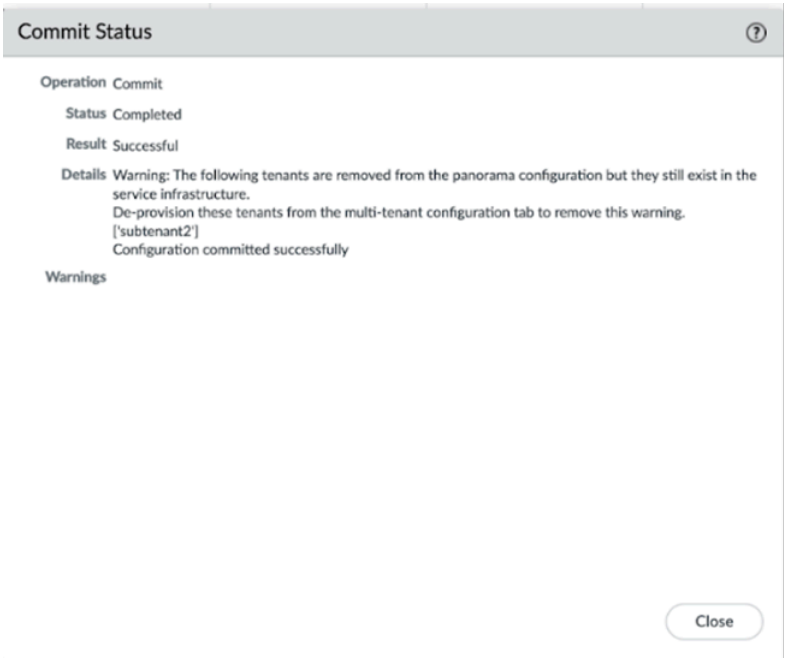

這時會顯示一個快顯視窗，確認租用戶刪除程序。按一下 **Yes**（是）以繼續，或按一下 **No**（否）以取消刪除。

 ©2025 Palo Alto Networks, Inc.




**STEP 5 |** 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**），並 **Commit**（提交）您的變更，以在本機將您的變更提交至 Panorama。

在進行本機提交之後，租用戶會被標記為進行刪除並從租用戶清單中移除，但不會從 Prisma Access 基礎結構中刪除。這時會顯示一個快顯視窗，顯示已刪除的租用戶。




 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** （選用）若要從 Prisma Access 基礎結構中完全移除租用戶，請**Deprovision Deleted Tenants**（取消佈建已刪除的租用戶）。

取消佈建租用戶：

- 將其從您的設定和 Prisma Access 基礎結構中移除，且您無法擷取它。
- 重新獲得已配置給租用戶的授權。

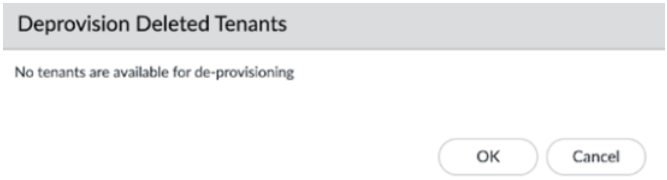



這時會顯示確認訊息，其中包含將取消佈建的租用戶名稱；按一下 **OK**（確定）以繼續取消佈建租用戶，或 **Cancel**（取消）此操作。

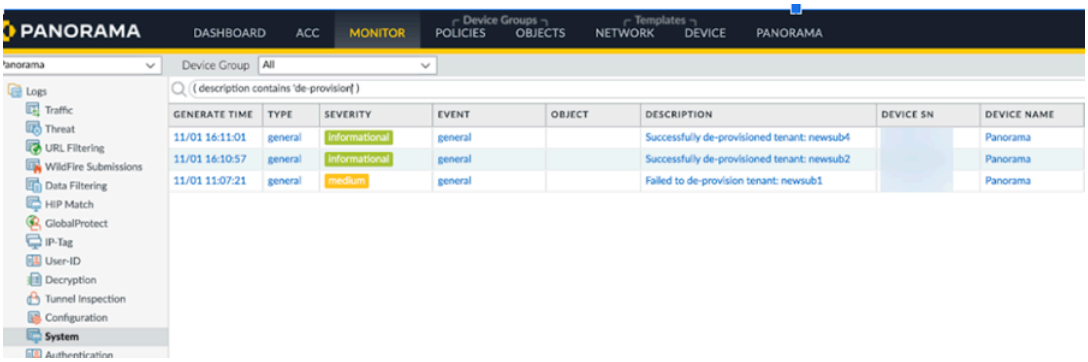
取消佈建租用戶時，您會完全刪除該租用戶，以及為其配置的所有資源，並重新獲得已配置給這些租用戶的授權。無法擷取租用戶。




如果不需要取消佈建任何租用戶，則會顯示以下訊息。




**STEP 7 |** （選用）前往 **Monitor**（監控） > **Logs**（日誌） > **System**（系統），檢查取消佈建操作的狀態。取消佈建操作和租用戶名稱會顯示在日誌中。




 ©2025 Palo Alto Networks, Inc.

# 建立租用戶層級管理使用者

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• 如需在 Prisma Access (Managed by Strata Cloud Manager) 管理多個租用戶的詳細資訊，請參閱 Prisma SASE。 | ❑ Prisma Access 授權 |

您應該為每個租用戶建立一個管理使用者。如此，租用戶層級管理員就可以檢視並變更其租用戶設定，但無權存取其他租用戶。若要為特定租用戶建立管理使用者，請完成下列工作。如需租用戶層級管理使用者的角色型存取控制 (RBAC) 詳細資訊，請參閱 控制租用戶層級管理使用者的角色型存取。

管理單一租用戶的使用者無法檢視系統日誌，因為 ***Monitor***（監控） ***> Logs***（日誌） ***> System***（系統）選項不可用。此限制適用於具有 ***Device Group and Template***（裝置群組與範本） 管理角色的所有管理員。只有超級使用者才能在多租用戶模式下檢視系統日誌。


©2025 Palo Alto Networks, Inc.

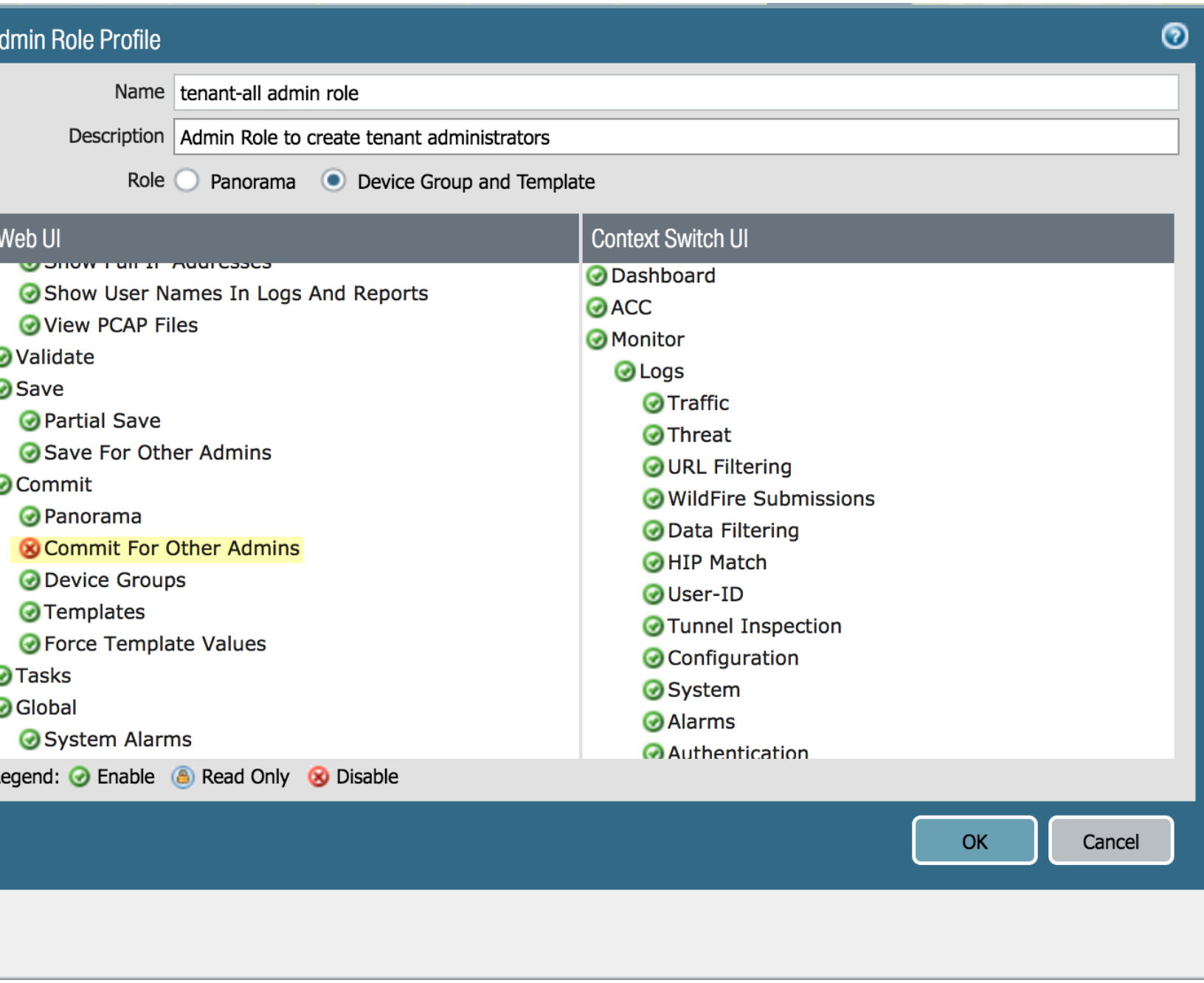
**STEP 1 |** 建立類型為 **Device Group and Template**（裝置群組與範本）的管理角色。

1. 選取 **Panorama** > **Admin Roles**（管理員角色）。
2. **Add**（新增）**Role**（角色）為 **Device Group and Template**（裝置群組與範本）的管理員角色設定檔。
3. 按一下 **OK**（確定）。

您可以建立單一管理員角色設定檔，並在多個租用戶之間共用；不過，您必須為每個租用戶建立個別的管理員。

當您根據組織的需求定制管理角色時，我們建議取消選取 ***Commit for Other Admins***（為其他管理員提交）。取消選取此選項允許租用戶層級使用者僅提交他們所做的變更，並防止他們無意中提交其他租用戶層級管理使用者已做出但尚未提交的其他變更。

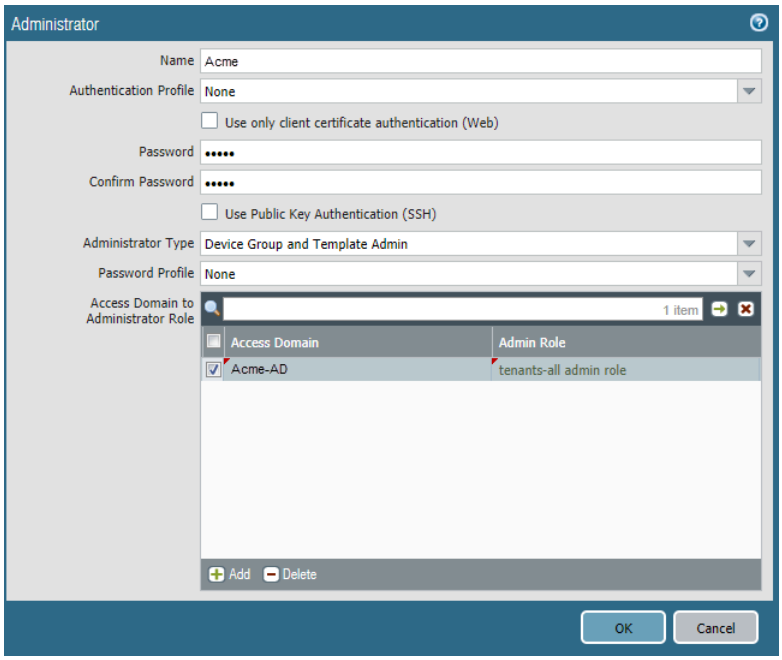

©2025 Palo Alto Networks, Inc.




 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 為租用戶建立並設定管理員。

1. 選取 **Panorama** > **Administrators**（管理員）。
2. **Add**（新增）管理員。
3. 輸入並確認新管理員的 **Password**（密碼）。
4. 指定 **Administrator Type**（管理員類型）為 **Device Group and Template Admin**（裝置群組和範本管理員）。
5. 指定與該租用戶的裝置群組相關聯的 **Access Domain**（存取網域）。
6. 指定您在步驟 1 中為租用戶建立的 **Admin Role**（管理員角色）。




**STEP 3 |** 按一下 **OK**（確定）。

**STEP 4 |** 重複步驟 2 和 3 視需要新增其他使用者來管理您的租用戶。

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


©2025 Palo Alto Networks, Inc.

# 控制租用戶層級管理使用者的角色型存取

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• 如需在 Prisma Access (Managed by Strata Cloud Manager) 管理多個租用戶的詳細資訊，請參閱 Prisma SASE。 | ❑ Prisma Access 授權 |

如果您管理多租用戶部署，則可以使用角色型存取控制 (RBAC) 來建立租用戶層級管理使用者。

若要在 Panorama 中修改租用戶層級管理使用者的 RBAC 層級存取，請建立租用戶層級管理使用者、使用管理員角色設定檔（**Role**（角色）為 **Device Group and Template**（裝置群組和範本），然後 **Enable**（啟用）、**Disable**（停用）或給與 Panorama **Web UI** 區域的 **Read Only**（唯讀）存取權。使用此方法，可為租用戶層級使用者管理對所有 Panorama 元件的存取，但對雲端服務外掛程式（您可在其中管理 Prisma Access）的存取除外 .

如果想要限制租用戶層級使用者不得設定 Panorama 中的 Prisma Access 元件，您不能使用管理員角色。若要不允許使用者設定 Prisma Access 特定的設定工作，您必須防止使用者存取雲端服務外掛程式，這也會防止他們檢視該外掛程式。使用此方法，您可以為安全性專業人員建立一個管理使用者，其有權變更安全政策並將這些變更推送到 Panorama，但無法檢視 Prisma Access 設定，或對其進行任何變更。

您可以為使用者啟用或停用對雲端服務外掛程式的存取，但不能給與使用者唯讀存取權；如果使用者有權檢視雲端服務外掛程式，則使用者還可以對其元件進行設定變更，包括 *Prisma Access*。

下表顯示了範例租用戶層級管理角色，以及您建立這些角色時執行的步驟。

| 租用戶層級設定範例 | 設定工作 |
| --- | --- |
| 建立以網路為中心的使用者，該使用者：<br>• 可以編輯外掛程式設定<br>• 可以提交至 Panorama<br>• 可以將設定推送至 Prisma Access | 建立租用戶層級管理使用者，啟用 **Admin Role Profile**（管理員角色設定檔）中的 **Save**（儲存）和 **Commit**（提交）權限，然後停用 **Read Only**（唯讀），或使其成為您不想要租用戶層級管理使用者具有的任何權限。 |
| 建立以安全性為中心的使用者，該使用者：<br>• 可以檢視和變更安全性政策<br>• 可以提交至 Panorama<br>• 無法檢視或變更雲端服務外掛程式 | 若要防止租用戶層級管理使用者檢視或存取外掛程式，請移除租用戶層級管理員的外掛程式存取權。對於所有其他與 Panorama 相關的權限，請變更使用者的管理員角色權限。 |


©2025 Palo Alto Networks, Inc.

| 租用戶層級設定範例 | 設定工作 |
| --- | --- |
| • 無法將設定推送至 Prisma Access（需要超級使用者才能推送設定） | |
| 建立一個混合使用者，其：<br>• 具有雲端服務外掛程式的唯讀存取權<br>• 具有安全性政策的讀寫存取權<br>• 無法將設定推送至 Prisma Access（需要超級使用者才能推送設定） | 此設定是不可行的。您無法使雲端服務外掛程式成為唯讀。您只能將存取權提供給管理員使用者，以檢視它並使用它進行設定變更，或不允許他們檢視它。 |

# 移除租用戶層級管理使用者的外掛程式存取

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• 如需在 Prisma Access (Managed by Strata Cloud Manager) 管理多個租用戶的詳細資訊，請參閱 Prisma SASE。 | ❑ Prisma Access 授權 |

在正常的多租用戶設定中，您使用存取網域 將租用戶新增 Prisma Access，並將每個存取網域與一個租用戶建立關聯。若要防止租用戶層管理使用者檢視 Prisma Access，或對進行設定變更，,請建立存取網域，但不將其與租用戶建立關聯。

因為您已將存取網域與租用戶的裝置群組和範本堆疊建立關聯，所以租用戶層級管理使用者在租用戶層級具有 RBAC 存取權，並且只能為該租用戶執行設定。因為您未將存取網域與 Prisma Access 中的租用戶建立關聯，所以存取網域無法檢視雲端服務外掛程式，而該外掛程式提供對 Prisma Access 的存取。透過這種方式，您建立了一個使用者，其可以執行租用戶層級設定工作，而無法存取、檢視 Prisma Access 或對其進行設定變更。

若要為管理層級使用者移除 Prisma Access，請完成以下工作。

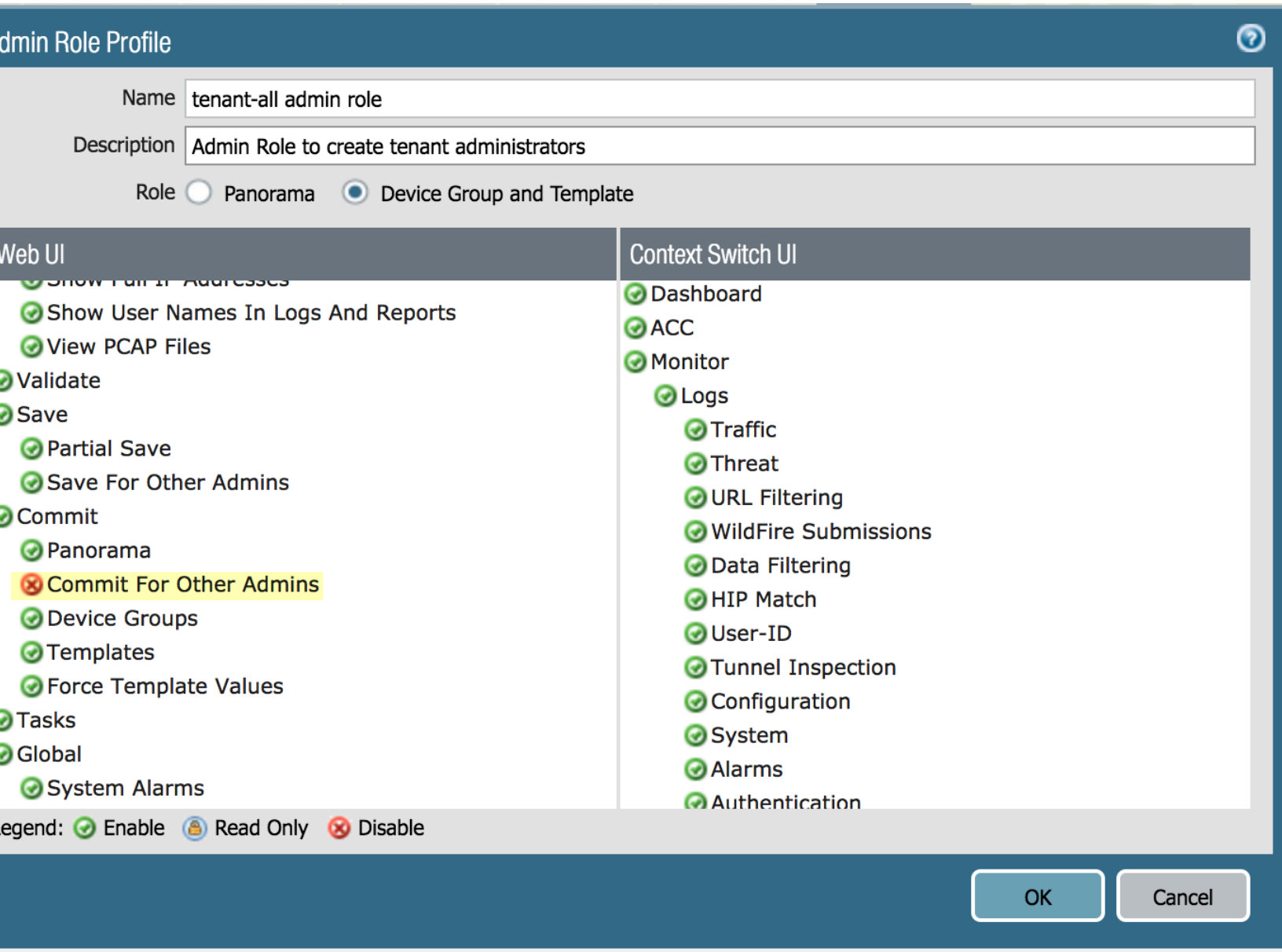
這項工作假設您具有租用戶的 將租用戶新增 Prisma Access 範本、範本堆疊和裝置群組；您會將它們與租用戶層級管理使用者建立關聯。


©2025 Palo Alto Networks, Inc.

**STEP 1 |** 建立類型為 **Device Group and Template**（裝置群組與範本）的管理角色。

1. 選取 **Panorama** > **Admin Roles**（管理員角色）。
2. **Add**（新增）**Role**（角色）為 **Device Group and Template**（裝置群組與範本）的管理員角色設定檔。
3. 按一下 **OK**（確定）。

   您可以建立單一管理員角色設定檔，並在多個租用戶之間共用。

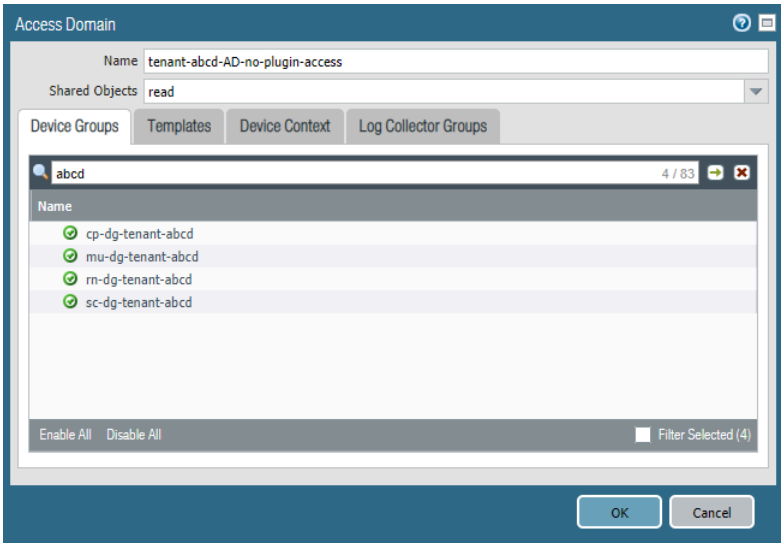


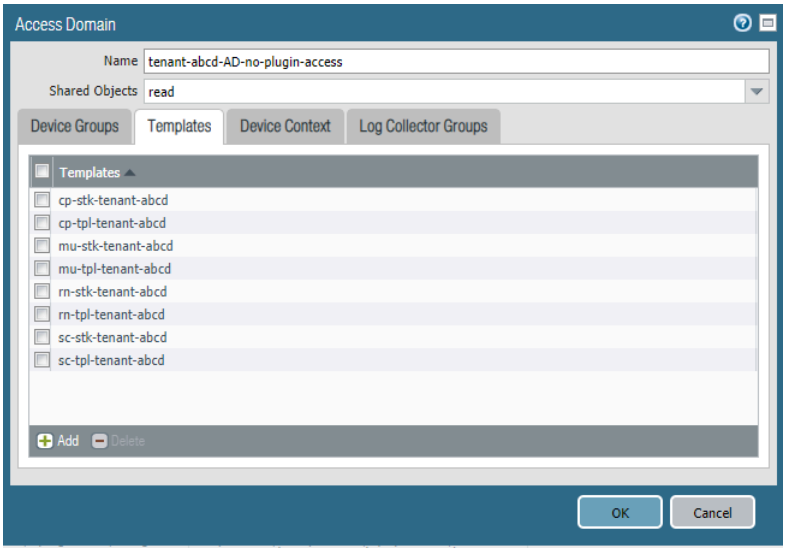

**STEP 2 |** 選取 **Panorama** > **Access Domain**（存取網域），然後 **Add**（新增）Access Domain（存取網域）。


©2025 Palo Alto Networks, Inc.

**STEP 3 |** 指定與租用戶相關聯的 **Device Groups**（裝置群組）和 **Templates**（範本）。

如果您建立了任何裝置群組，作為 ***Shared***（共用）父系裝置群組下其他裝置群組的子系或孫系，請僅選取最低層級的裝置群組（子系或孫系）；請勿選取父系，否則在提交時會發生錯誤。



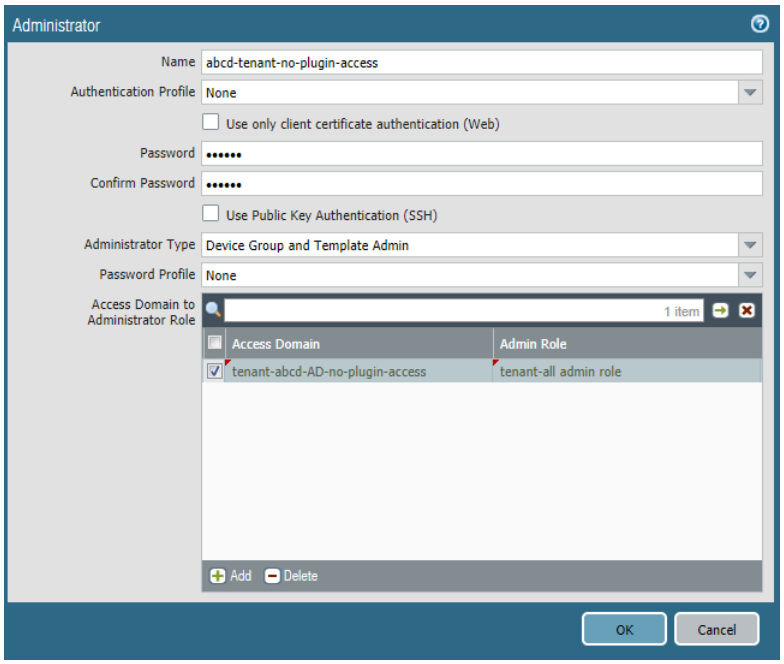




 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 為租用戶層級管理使用者建立和設定管理員，同時指定您剛建立的存取網域。

1. 選取 **Panorama** > **Administrators**（管理員）。
2. **Add**（新增）管理員。
3. 輸入並確認新管理員的 **Password**（密碼）。
4. 指定 **Administrator Type**（管理員類型）為 **Device Group and Template Admin**（裝置群組和範本管理員）。
5. 指定與該租用戶的裝置群組相關聯的 **Access Domain**（存取網域）。
6. 指定您在步驟 1 中為租用戶建立的 **Admin Role**（管理員角色）。

   當您完成此範例時，**abcd-tenant-no-plugin-access** 管理使用者將根據您在管理員角色設定檔中定義的內容擁有權限，但將無法檢視或設定雲端服務外掛程式（包括 Prisma Access）。不過，請注意，他們無法將所做的任何變更推送到雲端。




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


©2025 Palo Alto Networks, Inc.

# 在多租用戶部署中依裝置群組 ID 排序日誌

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• 如需在 Prisma Access (Managed by Strata Cloud Manager) 管理多個租用戶的詳細資訊，請參閱 Prisma SASE。 | ❑ Prisma Access 授權 |

若要在 Panorama 中依租用戶手動排序日誌，請選取 **Monitor**（監控） > **Logs**（日誌），並選擇與該租用戶相關聯的 **Device Group**（裝置群組），以顯示該裝置群組的日誌。不過，如果您要將日誌轉送到外部裝置，可能需要在租用戶層級排序這些日誌。若要這樣做到，請在日誌中尋找與裝置群組相關聯的裝置群組 ID，並使用該群組 ID 至裝置群組對應，將日誌與租用戶建立關聯。

有四個欄位與日誌中的裝置群組相關聯：**DG Hierarchy Level 1**（**DG** 階層層級 **1**）、**DG Hierarchy Level 2**（**DG** 階層層級 **2**）、**DG Hierarchy Level 3**（**DG** 階層層級 **3**）和 **DG Hierarchy Level 4**（**DG** 階層層級 **4**）。這些欄位顯示其階層中的裝置群組 ID。共用裝置群組（層級 0）不包括在此結構中。

**DG Hierarchy Level 1**（**DG** 階層層級 **1**）指的是階層中的第一個裝置群組層級。如果您新增了子系裝置群組或孫子系裝置群組，則 **DG Hierarchy Level 2**（**DG** 階層層級 **2**）至 **DG Hierarchy Level 4**（**DG** 階層層級 **4**）欄位分別顯示從子系群組到曾孫系群組的階層。

若要依租用戶尋找日誌，請完成下列工作。

**STEP 1 |** 尋找與裝置群組相關聯的裝置群組 ID。

- 若要使用 CLI 命令尋找此資訊，請以超級使用者（管理員層級使用者）身分登入 Panorama、在設定模式下輸入 `show readonly` 命令，然後檢視 **device-group** 標題中的值。裝置群組的 ID 會顯示在裝置群組名稱下。以下範例顯示 **acme-sc** 裝置群組的裝置 ID 為 **20**。

  請注意，這些裝置群組是在階層中的第一層（**DG Hierarchy Level 1**（**DG** 階層層級 **1**））；您會在下一個步驟的查詢中使用該資訊。

  ```
  admin# show readonly ... device-group { acme-sc { id 20; } acme-
  rn { id 39; } acme-mu { id 40; } hooli-rn { id 56; } hooli-sc
   { id 57; } hooli-mu {
  ```

- 若要使用 API 查詢，請輸入以下 API 命令：

  ```
  /api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>
  ```

  如需使用 *API* 搭配日誌的詳細資訊，請參閱擷取日誌 (API)。

**STEP 2 |** 使用裝置群組 ID 至裝置群組名稱對應，將日誌與租用戶建立關聯。


©2025 Palo Alto Networks, Inc.

**STEP 3 |** **Add**（新增）**Forwarding**（轉送） 參數，以選取您想要轉送的日誌。


©2025 Palo Alto Networks, Inc.

# FedRAMP 環境中的 Prisma Access

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ 雲端服務外掛程式版本 3.2.1-h94+、4.0.0-h88+、4.1.0-h58+、5.0.0-h31+ |

聯邦風險與授權管理計劃 (FedRAMP) 是美國政府範圍的計劃，為政府使用者的雲端產品和服務提供標準化的安全評估、授權和持續監控方法。Palo Alto Networks 已為 Prisma Access (Managed by Panorama) 展示 FedRAMP Moderate 合規性。閱讀以下主題，進一步瞭解如何設定 Prisma Access 以確保 FedRAMP Moderate 合規性。

對於雲端型服務，例如 Prisma Access，美國政府需要一個特定層級的保證，稱為 *Moderate*，其中若失去機密性、完整性和可用性將對機構的營運、資產或個人造成嚴重的不利影響。嚴重的不利影響可能包括對機構資產造成重大營運損害、財務損失或非人員傷亡或身體傷害。

Prisma Access 符合 FedRAMP Moderate 需求，並已從聯邦政府獲得營運授權 (ATO)。若要確保 FedRAMP Moderate 合規性，您必須使用以下主題中列出的需求和指導方針，來安裝並設定 Prisma Access。

# Prisma Access FedRAMP 需求

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ 雲端服務外掛程式版本 3.2.1-h94+、4.0.0-h88+、4.1.0-h58+、5.0.0-h31+ |

FedRAMP 是美國政府使用的計劃，為雲端服務產品 (CSO) 提供標準的合規方法。若要確保您的 Prisma Access (Managed by Panorama) Access 符合 FedRAMP Moderate，請在安裝、啟動、首次設定和設定 Prisma Access 時使用這些指導方針和需求。

## 安裝前和產品啟動需求

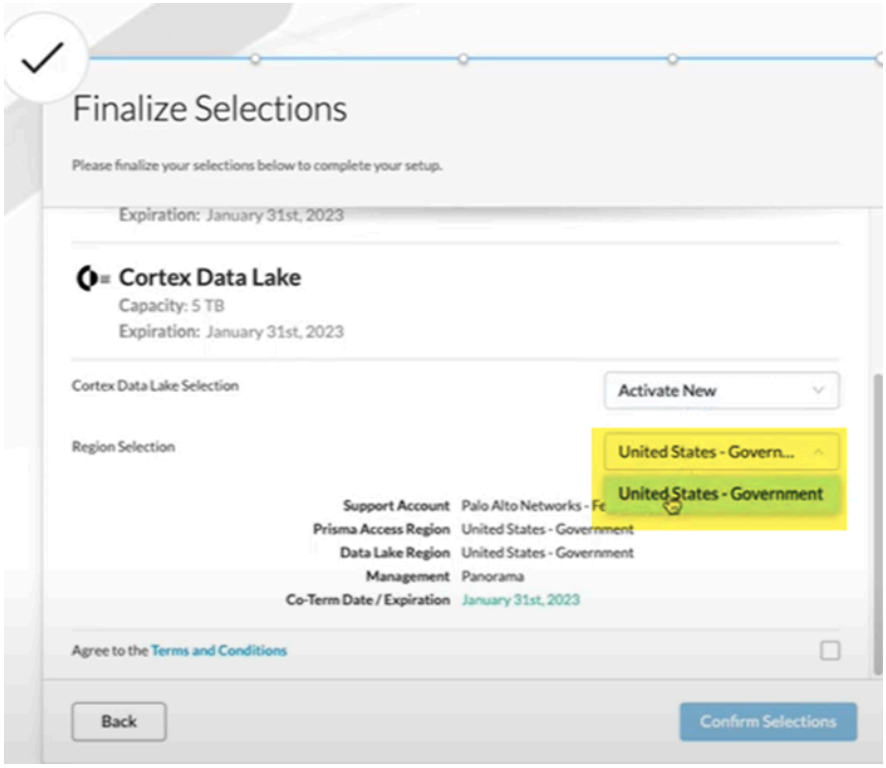
若要確保您的 Prisma Access 部署保持合規，請務必遵循這些安裝和產品啟動需求。

- 安裝前需求：
  - 部署類型（新的或現有）—FedRAMP Moderate 環境支援新的 Prisma Access 部署。不支援從現有 Prisma Access 部署升級到 FedRAMP Moderate Prisma Access 部署
  - 必要 **SKU**—當您購買 Prisma Access 進行 FedRAMP Moderate 部署時，Prisma Access 需要 FedRAMP Moderate 環境特有的 SKU。與您授權的 Palo Alto Networks 代表或合作夥伴合作，以確保您購買正確的 SKU 進行 FedRAMP Moderate 部署。
  - 僅使用 所需的 Panorama、外掛程式和 PAN-OS 資料平面版本 中列出的 Panorama 版本、GlobalProtect 版本和雲端服務外掛程式版本。
  - 允許清單 **Strata Logging Service** 公用 **IP** 位址—Strata Logging Service 聯邦區域使用的 IP 位址區塊是 34.67.50.64/28.如果您的企業使用允許清單，請務必將這些 IP 位址新增到您的允許清單，以確保 Strata Logging Service 可以從 Prisma Access 接收日誌。
  - **API URL** 的變更—當您執行 API 指令碼以擷取 Prisma Access 使用的公用 IP 位址時，請將 API 的 URL 從 **`https://api.gpcloudservice.com/GetPrismaAccessIP/v2`** 變更為 **`https://api.fed.prismaaccess.com/GetPrismaAccessIP/v2`**。

    如果您的 Panorama 裝置使用 Proxy 伺服器（**Panorama** > **Setup**（設定） > **Service**（服務） > **Proxy Server**（**Proxy** 伺服器）），或者如果您使用 SSL 正向 Proxy 解密搭配 Prisma Access，請確保將 api.fed.prismaaccess.com URL 新增至 Proxy 或Proxy 伺服器上的允許清單。
  - **GlobalProtect** 入口網站名稱變更—Prisma Access FedRAMP 行動使用者—GlobalProtect 的預設入口網站主機名稱與非 FedRAMP 部署不同。入口網站名稱為 <*portal-name*>.fed.prismaaccess.com.，而不是 <*portal-name*>.gpcloudservice.com。
  - 支援需求—Prisma Access FedRAMP Moderate 需要 Palo Alto Networks 美國政府支援服務，其中包括對美國境內人員的 24 小時全天候支援。


©2025 Palo Alto Networks, Inc.

- 啟動要求—當您啟動並安裝您的 Prisma Access 部署時，啟動和安裝工作類似於非 FedRAMP 部署。不過，在產品啟動期間，您必須選取 **Strata Logging Service**（**Strata** 記錄服務）區域為 **United States—Government**（美國—政府）。




## 所需的 Panorama、外掛程式和 PAN-OS 資料平面版本

為了確保 Prisma Access 符合 FedRAMP Moderate 需求，請確定您的 Prisma Access (Managed by Panorama) 部署使用以下 Panorama、雲端服務外掛程式和 GlobalProtect 版本。

| 元件 | 所需版本 |
|---|---|
| Panorama PAN-OS 版本 | 10.2.8-h3 或更新的 10.2.8 hotfix PAN-OS 版本<br>10.2.9-h1 或更新的 10.2.9 hotfix PAN-OS 版本<br>在管理 Prisma Access 的 Panorama 上啟用處理標準和通用準則 (FIPS-CC) 是與 FedRAMP 控制一致的建議最佳做法。在 Panorama 上啟用 FIPS-CC 支援需要存取維護復原工具 (MRT)。 |


©2025 Palo Alto Networks, Inc.

| 元件 | 所需版本 |
| --- | --- |
| | 若要簡化安裝和啟動程序，您可以選取已在 *FIPS* 模式下設定的現有 *Panorama*（如果您已註冊 *Panorama*、安裝了授權，並在客戶支援入口網站 (CSP) 上啟動了支援授權）。如果您已將 *Panorama* 序號新增到您想要在其上部署 *Prisma Access* 的同一 *CSP* 帳戶，則可以在安裝期間選取此 *Panorama* 設備的序號。<br><br>您無法使用已用來管理另一個 Prisma Access 或 Strata Logging Service 部署的 Panorama。 |
| 雲端服務外掛程式版本 | • 3.2.1-h94+<br>• 4.0.0-h88+<br>• 4.1.0-h58+<br>• 5.0.0-h31+ |
| GlobalProtect 版本 | 5.1.4+ and 6.0.7+<br><br>5.1.4 已獲 FIPS 認證，並且是用於聯邦政府型部署的預設版本。如果您從 5.1.4 變更預設的 GlobalProtect 版本，則無法從 Panorama UI 中選取版本 5.1.4，而且必須透過 Palo Alto Networks 技術支援開啟支援案例以將其加回來。 |

## 支援的 Prisma Access FedRAMP 位置

以下位置獲授權可在 FedRAMP Moderate 環境中與 Prisma Access 搭配使用，其中包括對美國本土 (CONUS) 和美國境外 (OCONUS) 位置的支援：

- 澳大利亞東南部
- 比利時
- 巴西南部
- 加拿大東部
- 芬蘭
- 德國中部
- 印度西部
- 日本中部
- 日本南部
- 荷蘭中部


©2025 Palo Alto Networks, Inc.

- 新加坡
- 瑞士
- 臺灣
- 英國
- 美國中部
- 美國東部
- 美國西北部
- 美國東南部
- 美國西南部

## Prisma Access FedRAMP 部署中支援和不支援的功能

在 FedRAMP Moderate 環境中，支援進行私人應用程式存取的 IPv6 支援Prisma Access。

不支援以下應用程式和功能在 Prisma Access FedRAMP Moderate 環境中使用：

- Prisma Access 洞察
- 自主 DEM
- 明確 Proxy
- Prisma Access for Clean Pipe
- 企業 DLP
- IoT Security
- SaaS 安全性內嵌支援—可視性

 ©2025 Palo Alto Networks, Inc.

# 在 FedRAMP 環境中設定 Prisma Access

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ 雲端服務外掛程式版本 3.2.1-h94+、4.0.0-h88+、4.1.0-h58+、5.0.0-h31+ |

在滿足了需求之後，請完成以下步驟，為 FedRAMP Moderate 環境完成 Prisma Access 部署的設定。

在開始之前，請注意 *Prisma Access FedRAMP* 部署特有的需求和指導方針，包括在 *FIPS-CC* 模式下設定 *Panorama* 設備，以及 *Panorama*、雲端服務外掛程式和 *GlobalProtect* 所需的特定版本。

**STEP 1 |** 確保您擁有一個可以專用於 FedRAMP 部署的客戶支援入口網站 (CSP) 帳戶。

您無法在單一 CSP 帳戶中進行 FedRAMP 和非 FedRAMP 部署。因此，Palo Alto Networks 建議您建立新的 CSP 帳戶，僅用作 FedRAMP 帳戶。

**STEP 2 |** 準備要在 Prisma Access FedRAMP 環境中使用的 Panorama 設備。

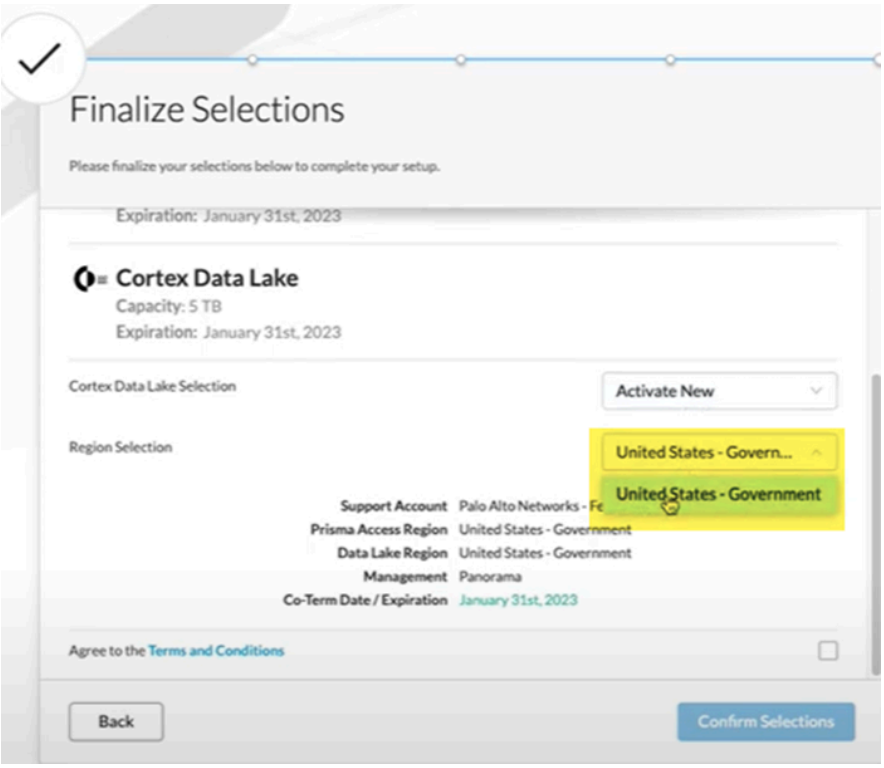
1. 安裝 Panorama 設備（M-Series 設備或虛擬設備）。
2. （選用，建議）在 Panorama 設備上啟用 Federal Information Processing Standard (聯邦資訊處理標準 - FIPS) 和通用準則 (FIPS-CC) 支援。

   啟用 FIPS 支援需要存取維護復原工具 (MRT)。
3. 將您的 Panorama 版本升級至 所需的 Panorama、外掛程式和 PAN-OS 資料平面版本 中列出的版本。


©2025 Palo Alto Networks, Inc.

**STEP 3 |** 確定您的授權需求；然後啟動並安裝 Prisma Access 授權元件。

在產品啟動期間選取 **United States—Government**（美國—政府）的 **Strata Logging Service**（**Strata** 記錄服務）區域。




**STEP 4 |** 將下列 URL、IP 位址和連接埠新增至任何安全設備上的允許清單，而您會使用這些設備搭配管理 Prisma Access 的 Panorama 設備。

此外，如果您的 Panorama 裝置使用 Proxy 伺服器（**Panorama** > **Setup**（設定） > **Service**（服務） > **Proxy Server**（**Proxy** 伺服器）），或者如果您使用 SSL 正向 Proxy 搭配 Prisma Access，請務必將下列 URL、IP 位址和連接埠新增至 Proxy 或 Proxy 伺服器上的允許清單。

- api.gpcloudservice.com（適用於 Prisma Access）
- api.paloaltonetworks.com（適用於 Prisma Access）
- api.fed.prismaaccess.com（適用於 Prisma Access）
- apitrusted.paloaltonetworks.co（適用於 Prisma Access）
- Strata 記錄服務所需的 FQDN 和連接埠
- 34.67.50.64/28

  Strata Logging Service 聯邦地區使用的 IP 位址區塊為 34.67.50.64/28。將這些 IP 位址新增至您的允許清單，以便 Strata Logging Service 可從 Prisma Access 接收日誌 。
- Panorama 使用的連接埠。


©2025 Palo Alto Networks, Inc.

**STEP 5 |** 在客戶支援入口網站 (CSP) 中開啟一個案例，讓 Palo Alto Networks 將 Strata Logging Service 的來源和目的地連接埠列入允許清單。

若要在 Prisma Access 在環境中使用 Strata Logging Service，您必須建立一個案例，以便 Palo Alto Networks 可在內部將來源和目的地連接埠列入允許清單。

**STEP 6 |** 選取 **Device**（裝置） > **Setup**（設定） > **WildFire**，並輸入 **`wildfire.gov.paloaltonetworks.com`**。

FedRAMP 部署要求您使用 WildFire 美國政府雲端。

**STEP 7 |** 如果您的部署有此需要，請裝載行動使用者並使用 GlobalProtect 保護他們。

我們建議使用本機驗證作為第一步，來驗證服務是否已設定，以及您的使用者是否可以存取網際網路。您稍後可以切換為使用貴公司驗證方法。

1. 設定 GlobalProtect 行動使用者。
2. 設定行動使用者的區域。
   1. 在行動使用者範本中建立兩個區域。例如，行動使用者和網際網路。
   2. 對應區域。將不是 Prisma Access 連線的使用者或總部或分公司的任何區域對應至 [Untrust（不信任）]。

      在 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users**（行動使用者）下，將網際網路對應至 [Untrust（不信任）]；將行動使用者對應至 [Trust (信任)]。
3. 設定裝置群組的安全性政策。

   若要建立安全性政策以允許網際網路的流量，請選取 Mobile_User_Device_Group **Policies**（政策） > **Security**（安全性） > **Prerules**（前置規則） > **Add**（新增）規則。例如：行動使用者至網際網路。
4. 提交並推送您的變更以開始使用服務。
   1. 在 Panorama 上進行本機 **Commit**（提交）。
   2. **Commit and Push**（提交並推送）至 Prisma Access。
   3. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Monitor**（監控） > **Mobile Users**（行動使用者），以檢視 **Status**（狀態），並驗證您是否可以 ping（偵測）入口網站 FQDN。
5. 驗證 Prisma Access 是否正在保護行動使用者的網際網路流量。
   1. 下載並安裝 GlobalProtect 應用程式。
   2. 使用該應用程式以行動使用者（本機使用者）身分連線到入口網站。
   3. 瀏覽網際網路上的一些網站並檢查 Panorama 上的流量日誌。

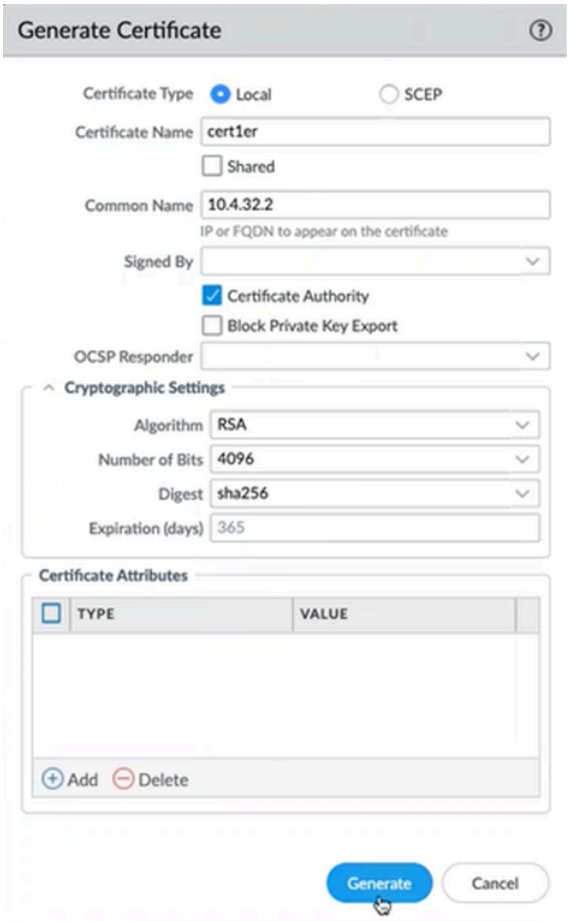
 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** （僅限行動使用者—GlobalProtect 部署）在行動使用者—GlobalProtect 部署中建立驗證覆寫憑證，其符合在 FIPS 模式下執行的 Panorama 需求，然後將該憑證套用至您的部署。

產生新憑證，因為行動使用者—GlobalProtect 的預設憑證（即 **Authentication Cookie CA**（驗證 **Cookie CA**））不符合在 FIPS-CC 模式下執行的 Panorama 的最低密碼套件需求。

1. 從管理 Prisma Access 的 Panorama 中，選取 **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證）。

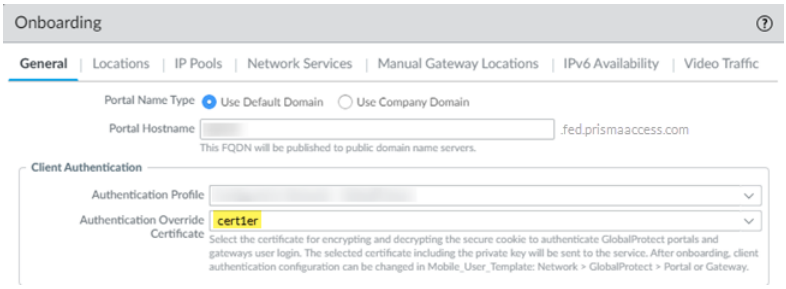
   確保您位於 **Mobile_User_Template** 中。
2. 產生一個憑證，符合 FIPS-CC 模式下 Panorama 的最低密碼套件需求。




3. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users—GlobalProtect**（行動使用者—**GlobalProtect**）、選取 **Hostname**（主機名稱），

 ©2025 Palo Alto Networks, Inc.

然後在 **Client Authentication**（用戶端驗證）區域中，選取您建立的 **Authentication Override Certificate**（驗證覆寫憑證）。




如果您已建立行動使用者—*GlobalProtect* 設定，則此區域會呈現灰色。若要變更驗證覆寫憑證，請選取 ***Network***（網路） **>** ***GlobalProtect*** **>** ***Portals***（入口網站） **>** ***<portal-config>*** **>** ***Agent***（代理程式） **>** ***DEFAULT***（預設值） **>** ***Authentication***（驗證），並在 ***Certificate to Encrypt/Decrypt Cookie***（要加密/解密的憑證 ***Cookie***）下選取此憑證。

**STEP 9 |** 啟用服務基礎結構，以及允許在 Prisma Access 元素之間進行通訊的服務連線。

1. 計劃啟用服務基礎結構和服務連線。
2. 啟用服務基礎結構。
3. 建立服務連線以允許存取您的公司資源。

   如果不需要存取您的公司資源，您仍然應該建立服務連線，以啟用行動使用者與遠端網路之間的存取。

**STEP 10 |** 規劃、建立和設定遠端網路連線。

1. 將一個或多個遠端網路新增至 Prisma Access。

   您可以裝戴一個位置，然後使用大量匯入功能新增其他位置。
2. 建立安全性政策規則，以允許從遠端網路到總部的流量（例如：信任至信任）。
3. 驗證服務連線、遠端網路連線與行動使用者之間的連線。

**STEP 11 |** 擷取 Prisma Access 公用和私人 IP 位址。

您可以將這些位址新增至組織網路上的允許清單，以限制對企業網路和應用程式的輸入存取。

如果您有行動使用者—*GlobalProtect* 部署，則可以使用 *Prisma Access UI*（而不是此 *API*）來管理公用 *IP* 位址配置，並確認在 *Prisma Access* 釋出 *IP* 位址之前，*IP* 位址已新增至您的允許清單。如此，*Prisma Access* 僅會佈建您已列入允許清單的 *IP* 位址。


©2025 Palo Alto Networks, Inc.

**STEP 12 |** （選用）將驗證方法從本機驗證變更為您組織的驗證方法。

請使用以下其中一個方法，為行動使用者設定 SAML 驗證：

- 設定 Azure AD SAML 驗證進行行動使用者部署

  僅設定此設定的 GlobalProtect 部分，並省略明確 Proxy 設定。
- 使用 Okta 作為行動使用者的 IdP 設定 SAML 驗證
- 將 ADFS 設定為行動使用者的 SAML 提供者

雖然在設定驗證之後，您可以使用雲端識別引擎擷取使用者和群組資訊，但您無法僅使用雲端識別引擎驗證使用者。

**STEP 13 |** （選用）將日誌從 Strata Logging Service 轉送到外部 Syslog 接收器，方法為設定日誌轉送應用程式。

 ©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

# Prisma Access 進階部署

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

某些 Prisma Access 路由和網路部署需要全面瞭解您組織的拓撲和路由裝置，以及瞭解 Prisma Access 路由的運作方式。在本節中閱讀這些進階部署以及如何設定它們

適用於服務連線、行動使用者和遠端網路的進階部署：

- 為已部署的 Prisma Access 位置新增計算位置
- IPv6 支援
- 行動使用者—GlobalProtect 和遠端網路部署的 DNS 解析
- BGP 如何為服務連線和遠端網路連線公告行動使用者 IP 位址集區
- Prisma Access 和 Strata Logging Service 的 Proxy 支援
- 封鎖從特定國家/地區傳入的連線
- 保護來自 AWS WorkSpace 的網際網路流量
- Prisma Access 用於無預設路由網路

服務連線進階部署

- 服務連線多重雲端備援
- 使用流量導向將網際網路繫結流量轉送到服務連線
- 服務連線流量的路由
- 使用來源 NAT 保留服務連線的 User-ID 與 Device-ID 對應

行動使用者—GlobalProtect 進階部署:

- 在 Prisma Access 中設定多個入口網站
- 遠端疑難排解和更新的動態 DNS 支援
- 行動使用者—GlobalProtect 的動態 DNS 註冊支援
- 在 Prisma Access GlobalProtect 部署中識別和隔離遭入侵裝置
- 將行動使用者—GlobalProtect 部署中的 IPv6 流量導向至不同的位置
- 使用 Prisma Access 重新散佈 HIP 資訊
- 檢視 HIP 報告
- 無用戶端 VPN 中 Gzip 編碼的支援
- Prisma Access 中的流量複寫

遠端網路進階部署：

- 提供對遠端網路位置的安全輸入存取
- 為遠端網站建立高頻寬網路

 ©2025 Palo Alto Networks, Inc.

# 為已部署的 Prisma Access 位置新增計算位置

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

為了最佳化效能並改善延遲，Prisma Access 可以為您已部署的位置引入新的計算位置，作為外掛程式升級的一部分。當您升級外掛程式時，現有的計算位置到位置對應不會變更，但您可以選擇利用新的計算位置。如果您變更計算位置，則 Prisma Access 會為新計算位置與其相關聯的位置變更閘道和入口網站 IP 位址（適用於行動使用者），以及服務 IP 位址（適用於遠端網路）。如果您在網路中使用允許清單，為使用者提供對網際網路資源的存取，例如 SaaS 應用程式或可公開存取的合作夥伴應用程式，則需要將這些新的 IP 位址新增到您的允許清單。

若要新計算位置在變成可用之後進行升級，請完成以下工作。

由於您需要挪出時間來刪除和新增現有位置，以及變更您的允許清單（適用於行動使用者）或對等 IPSec 通道 IP 位址（適用於遠端網路部署），因此 Palo Alto Networks 建議您在維護時段或非高峰時段排程計算位置變更。

為了減少行動使用者部署的停機時間，請在執行這些步驟之前使用 API 預先配置新的行動使用者閘道和入口網站 IP 位址。

**STEP 1 |** 為新的遠端網路計算位置新增頻帶。

1. （僅限依計算位置配置遠端網路頻寬的遠端網路部署）選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路）。
2. 按一下 **Bandwidth Allocation**（頻寬配置）區域中的齒輪圖示，並為新的計算位置新增 **Bandwidth Allocation (Mbps)**（頻寬配置 **(Mbps)**）。
3. 請等待頻寬反映在頁面頂部的 [Allocated Total（已配置總計）] 欄位中；然後，按一下 **OK**（確定）。

**STEP 2 |** （僅限行動使用者部署）使用 API 指令碼擷取新的閘道和入口網站 IP 位址，並將它們新增到您的允許清單。

**STEP 3 |** 刪除與新計算位置相關聯的服務連線、遠端網路連線或行動使用者位置。

**STEP 4 |** 提交並推送您的變更。

**STEP 5 |** 重新新增您剛剛刪除的位置。

**STEP 6 |** 提交並推送您的變更。

**STEP 7 |** （僅限遠端網路和服務連線部署）將您的 CPE 變更為指向 IPSec 通道的新 IP 位址，進行遠端網路連線或服務連線。

對於遠端網路連線，選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Remote Networks**（遠端網路）、記下服務 **Service IP**

 ©2025 Palo Alto Networks, Inc.

**Address**（服務 **IP** 位址），並將新的 **Service IP Address**（服務 **IP** 位址）設定為 CPE 上遠端網路 IPSec 通道的對等 位址。

對於服務連線，選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Service Connection**（服務連線）、記下服務 **Service IP Address**（服務 **IP** 位址），並將新的 **Service IP Address**（服務 **IP** 位址）設定為 CPE 上服務連線 IPSec 通道的對等 IP 位址。

**STEP 8 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Remote Networks**（遠端網路）、記下服務 **Service IP Address**（服務 **IP** 位址），並將新的 **Service IP Address**（服務 **IP** 位址）設定為 CPE 上遠端網路 IPSec 通道的對等 位址。

當您刪除並重新新增遠端網路連線時，Prisma Access 端上 IPSec 通道的 IP 位址會變更。

**STEP 9 |** （僅限行動使用者部署）在重新對應位置之後，擷取新的閘道 FQDN 並將其新增到 SAML 提供者的驗證設定。

如果重新對應了行動使用者位置，則 FQDN 可能會在基礎結構升級之後變更，這可能會導致 SAML 驗證出現問題。若要尋找閘道名稱：

- 在 Prisma Access (Managed by Strata Cloud Manager) 中，選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **GlobalProtect** > **GlobalProtect Setup**（**GlobalProtect** 設定） > **Infrastructure**（基礎結構） > **Infrastructure Settings**（基礎結構設定）、按一下齒輪以檢視基礎結構設定，並複製閘道 FQDN 區域中的已重新命名閘道。
- 在 Prisma Access (Managed by Panorama) 中，選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Mobile Users—GlobalProtect**（行動使用者—**GlobalProtect**），並在閘道區域中複製已重新命名的閘道。

 ©2025 Palo Alto Networks, Inc.

# IPv6 支援

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 2.2 版 Preferred 和更新版本<br>❑ 對公用和私人應用程式的原生 IPv6 存取需要以下最低版本：<br>• Prisma Access (Managed by Strata Cloud Manager):2024 年 6 月發行<br>• Prisma Access (Managed by Panorama):Prisma Access 5.1.1 僅適用於新部署。<br>任何其他部署（包括現有的 Prisma Access (Managed by Panorama) 部署）僅支援私人應用程式存取。 |

如果您的組織使用 IPv6 定址，則 Prisma Access 可讓您存取位於 IPv6 位址後面的內部（私人）應用程式。根據您的 Prisma Access 版本，您可以使用 IPv6 存取私人（內部）應用程序，或者同時存取 GlobalProtect 和遠端網路的內部和公用（外部）應用程式。

對於存取外部應用程式，某些 *Prisma Access* 元件預設不啟用 *IPv6* 功能。在您啟用原生 *IPv6* 進行公用應用程式存取之前，請聯繫您的 *Palo Alto Networks* 客戶團隊，並開啟 *TAC* 票證以開始啟用程序。

原生 IPv6 支援的一個好處是，僅限 IPv6 和雙堆疊端點的行動使用者能夠使用 GlobalProtect 透過 IPv6 連線來連線至 Prisma Access。另一個好處是 GlobalProtect 和遠端網路能夠透過網際網路存取網際網路和公用 SaaS 應用程式，其中這些網際網路目的地需要 IPv6 連線。

IPv6 提供了比 IPv4 明顯大很多的位址空间，允許幾乎不限數目的唯一 IP 位址。同時，雙堆疊是一種過渡方法，允許網路和裝置同時使用 IPv4 和 IPv6 操作。原生 IPv6 支援使 Prisma Access 與 IPv6 和雙堆疊連線相容，讓從 IPv4 到 IPv6 的移轉程序輕鬆執行、確保回溯相容性，並促成您通往雲端和 IPv6 啟用網路的旅程。

您會在以下 Prisma Access 網路元件中設定 IPv6：

- 啟用 IPv6 並在您的基礎結構子網路中指定一個 IPv6 子網路，來建立 IPv6 網路基礎結構，以在您的遠端網路（分支位置）、行動使用者和服務連線（資料中心或總部位置）之間啟用通訊。

  如需最佳結果，請提供您自己的 *IPv6*（公用或私人）位址集區，首碼長度為 */64*，例如 *3005:10:209:55::/64*。

 ©2025 Palo Alto Networks, Inc.

- 對於行動使用者—GlobalProtect 部署，請指定是否應該為與您行動使用者位置相關聯的計算位置使用 IPv6 網路。

  您可以視需要指定 IPv6 行動使用者 IP 位址集區和 IPv6 DNS 伺服器位址。

  如需最佳結果，請提供您自己的 *IPv6*（公用或私人）位址集區，首碼長度為 */64*，例如 *3001:192:168:32::/64*，套用於全球層級。

  *Prisma Access* 為每個計算區域指派一個來自 */80* 子網路的集區，以及為每個位置（閘道）指派一個來自 */112* 子網路的集區。因為每個 *GlobalProtect* 連線都使用來自集區的一個 *IP* 位址，所以此配置允許將超過 *65,000* 個可用 *IPv6* 位址 *(/128)* 指派給每個位置的使用者端點。
- 對於服務連線和遠端網路連線，您可以為連線使用的路由類型（靜態或 BGP 路由）指定 IPv6 定址。
  - 對於靜態路由，請為用於靜態路由的子網路指定一個 IPv6 位址。
  - 對於 BGP 路由，請指定 IPv6 **Peer Address**（對等位址）和 **Local Address**（本機位址）。

    您還可以指定用來交換 BGP 對等資訊的傳輸方法。您可以指定使用 IPv4 來交換所有 BGP 對等資訊（包括 IPv4 和 IPv6）、使用 IPv6 來交換所有 BGP 對等資訊，或使用 IPv4 來交換 IPv4 BGP 對等資訊，以及使用 IPv6 來交換 IPv6 BGP 對等資訊。

  如需最佳結果，請提供您自己的 *IPv6*（公用或私人）位址集區，首碼長度上限為 */64*，例如 *2005:10:209:79::/64*。
- 對於遠端網路，您可以為 DNS 伺服器新增 IPv6 位址。

  如需最佳結果，請提供您自己的 *IPv6*（公用或私人）位址集區，首碼長度上限為 */64*，例如 *2001:10:209:65::/64*。

  每個分公司應使用唯一的 */112*（長度上限）子網路，允許超過 *65,000* 個唯一主機。

- 您提供的 *IPv6* 位址不應與 *Prisma Access BYOIP* 公用 *IPv6* 位址空間重疊。
- 您的 *IP* 集區、分公司（遠端網路）子網路、公司（服務連線）子網路和基礎結構子網路不應該彼此重疊（應該是互斥的）。

以下計算位置不支援IPv6：

- 韓國
- 東北亞
- 南美洲東部
- 巴林
- 南非西部
- 歐洲北部（斯德哥爾摩）
- 中東中部（UAE）

以下位置不支援 IPv6：

 ©2025 Palo Alto Networks, Inc.

- 所有本機區域位置
- 加拿大西部
- 南非中部

以下部署不支援 IPv6 定址：

- 遠端網路—高效能
- IP 最佳化

  IP 最佳化部署不支援 IPv6 用於存取公用（外部）應用程式；支援私人應用程式存取。若要為您的新 Prisma Access 部署啟用IPv6，請聯繫您的 Palo Alto Networks 客戶團隊，他們將開啟一個 TAC 案例以滿足該要求。
- Clean Pipe 部署
- 流量導向（使用流量導向規則，以使用服務連線重新導向網際網路連結流量）
- 服務連線和遠端網路連線的服務輸出路由

*Prisma Access* 不公告 *IPv6* 預設路由。

## 原生 IPv6 支援概要

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 2.2 版 Preferred 和更新版本<br>❑ 對公用和私人應用程式的原生 IPv6 存取需要以下最低版本：<br>• Prisma Access (Managed by Strata Cloud Manager):2024 年 6 月發行<br>• Prisma Access (Managed by Panorama):Prisma Access 5.1.1 僅適用於新部署。<br>任何其他部署（包括現有的 Prisma Access (Managed by Panorama) 部署）僅支援私人應用程式存取。 |

Prisma Access 擴大對 IPv6 的支援，使其不再僅限於存取私人應用程式，而是 GlobalProtect 和遠端網路可以原生支援 IPv6。

原生 IPv6 支援的一個好處是，僅限 IPv6 和雙堆疊端點的行動使用者能夠使用 GlobalProtect 透過 IPv6 連線來連線至 Prisma Access。另一個好處是 GlobalProtect 和遠端網路能夠透過網際網路存取網際網路和公用 SaaS 應用程式，其中這些網際網路目的地需要 IPv6 連線。

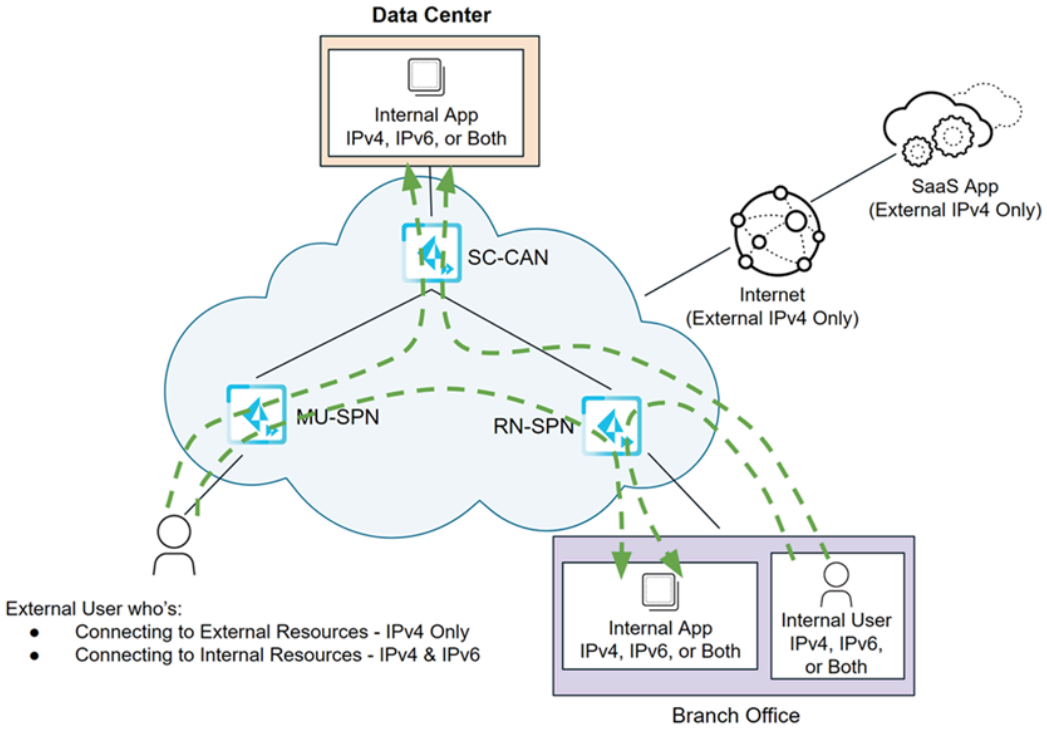
IPv6 提供了比 IPv4 明顯大很多的位址空间，允許幾乎不限數目的唯一 IP 位址。同時，雙堆疊是一種過渡方法，允許網路和裝置同時使用 IPv4 和 IPv6 操作。原生 IPv6 支援使 Prisma Access 與

 ©2025 Palo Alto Networks, Inc.

IPv6 和雙堆疊連線相容，讓從 IPv4 到 IPv6 的移轉程序輕鬆執行、確保回溯相容性，並促成您通往雲端和 IPv6 啟用網路的旅程。

### 私人應用程式支援

一些 Prisma Access 部署支援內部「私人」應用程式的 IPv6 連線。Prisma Access 使用底層連線到資料中心（服務連線）和分公司（遠端網路），其中 IPv6 流量透過 IPv4 通道傳遞。



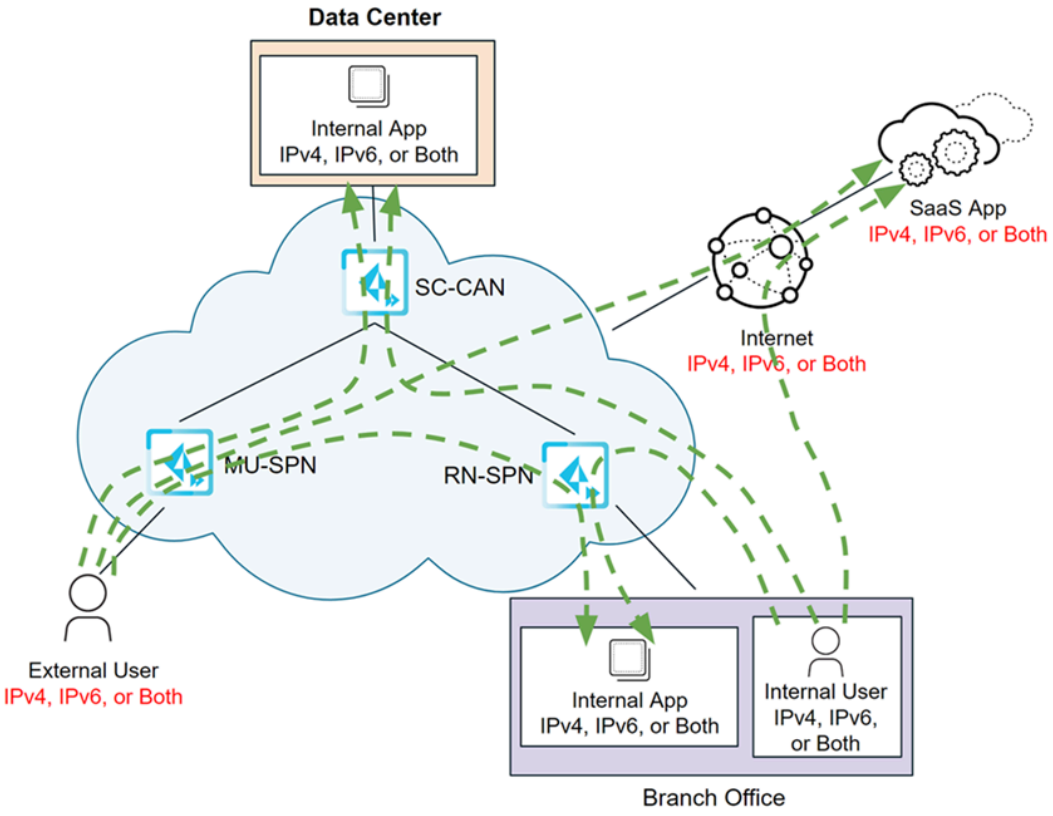

## Prisma Access 中的原生 IPv6

Prisma Access

- Prisma Access 的雙堆疊 IPv4/IPv6 輸入連線
- 網際網路和 SaaS 應用程式透過網際網路的雙堆疊 IPv4/IPv6 輸出連線

現在，使用者可以使用 IPv6 透過網際網路連線到網際網路和「公用」SaaS 應用程式。


©2025 Palo Alto Networks, Inc.




外部使用者（行動使用者）需要使用下列其中一個支援的 *GlobalProtect* 版本，本機 *IPv6* 才能運作：

- *5.2.13-c418 (Win/Mac)*
- *6.0.7-c378 (Win/Mac)*
- *6.0.7-c20 (Linux)*
- *6.1.2 (Win/Mac/Linux)*
- *6.2.0-c89 (Win/Mac)*

下表顯示了 IPv4 和 IPv6 Prisma Access 部署支援的連線。核取記號表示支援此連線，破折號表示不支援此連線。


©2025 Palo Alto Networks, Inc.

### IPv6 Not Enabled

| Mobile User IP Version | GlobalProtect IP Version | Internet Destination Gateway ➞ Internet | | Private App Access Service Connection ➞ Internet | | GlobalProtect Tunnel | NAT Gateway ➞ Internet |
|---|---|---|---|---|---|---|---|
| | | IPv4 | IPv6 | IPv4 | IPv6 | ESP | IPv4 ➞ IPv4 |
| IPv4 | IPv4 | ✓ | — | ✓ | — | IPv4 | NAT44 |
| Dual Stack | Dual Stack | ✓ | ✓ Sinkhole | ✓ | ✓ | IPv4 | NAT44 |
| IPv6 | — | — | — | — | — | — | — |

### IPv6 Enabled

| Mobile User IP Version | GlobalProtect IP Version | Internet Destination Gateway ➞ Internet | | Private App Access Service Connection ➞ Internet | | GlobalProtect Tunnel | NAT Gateway ➞ Internet | |
|---|---|---|---|---|---|---|---|---|
| | | IPv4 | IPv6 | IPv4 | IPv6 | ESP | IPv6 ➞ IPv4 | IPv6 ➞ IPv6 |
| IPv4 | IPv4 | ✓ | — | ✓ | — | IPv4 | NAT64 | NPTv6 |
| Dual Stack | Dual Stack | ✓ | ✓ | ✓ | ✓ | IPv6 | NAT64 | NPTv6 |
| IPv6 | Dual Stack | ✓ (DNS64 & NAT64 Req'd) | ✓ | ✓ (Custom DNS64 + NAT64) | ✓ | IPv6 | NAT64 | NPTv6 |

請遵循這些工作流程，在您的設定中啟用 IPv6。

- ❑ 在 Prisma Access 基礎結構中啟用和設定 IPv6 網路和 IP 集區
- ❑ 為行動使用者—GlobalProtect 部署啟用 IPv6 網路
- ❑ 為服務連線啟用 IPv6 網路
- ❑ 為遠端網路啟用 IPv6 網路

# 在您的 Prisma Access 基礎結構中啟用並設定 IPv6 網路和 IP 集區

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 2.2 版 Preferred 和更新版本 |


©2025 Palo Alto Networks, Inc.

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| | ❑ 對公用和私人應用程式的原生 IPv6 存取需要以下最低版本：<br>• Prisma Access (Managed by Strata Cloud Manager):2024 年 6 月發行<br>• Prisma Access (Managed by Panorama):Prisma Access 5.1.1 僅適用於新部署。<br>任何其他部署（包括現有的 Prisma Access (Managed by Panorama) 部署）僅支援私人應用程式存取。 |

對於任何 Prisma Access 部署時，您需要全域啟用 IPv6，並在基礎結構子網路中指定 IPv6 子網路，以便 Prisma Access 可在遠端網路位置、行動使用者和服務連線之間建立 IPv6 網路基礎結構。若要這樣做，請完成以下步驟。

- Strata Cloud Manager
- Panorama

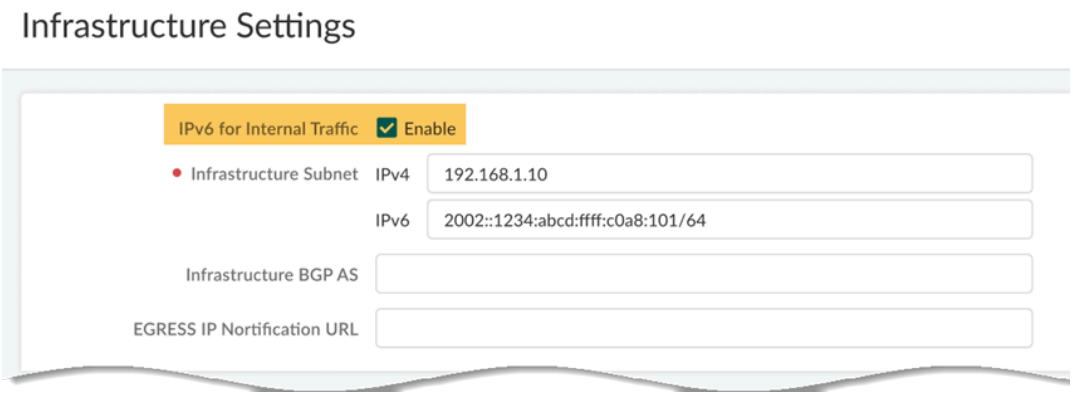
## 在您的 Prisma Access 基礎結構中啟用並設定 IPv6 網路和 IP 集區 (Strata Cloud Manager)

**STEP 1 |** 選取 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Prisma Access**，然後選取齒輪圖示以編輯設定。

**STEP 2 |** 選取核取方塊，為內部流量 **Enable**（啟用） IPv6。

啟用或停用 IPv6 會導致短暫的流量中斷（最多 120 秒），同時資料平面準備接受或拒絕 Prisma Access 骨幹上的 IPv6 路由。我們建議您在維護時段或非尖峰時刻推送此設定變更。

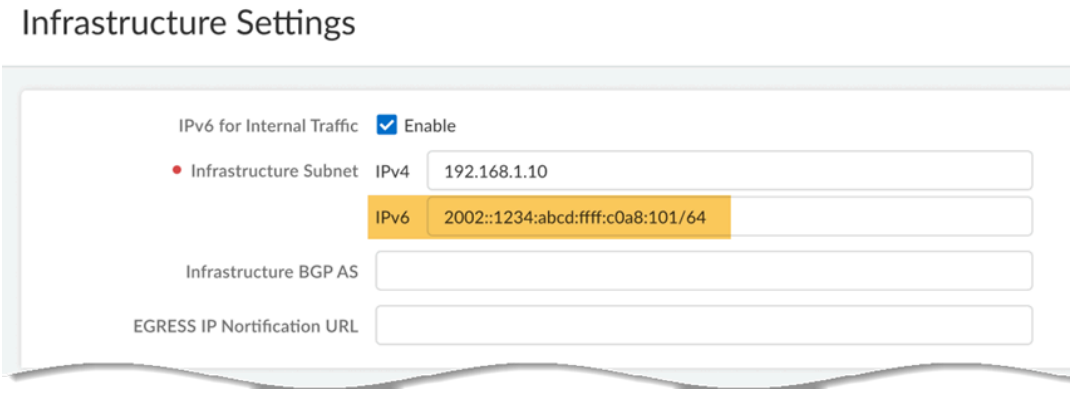
如果您需要刪除 *IPv6*，請先刪除所有設定（包括行動使用者、遠端網路和服務連線（如果適用）），然後再取消選取為內部流量 ***Enable***（啟用） *IPv6* 核取方塊。




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 指定 **IPv6** 基礎結構子網路和 **Infrastructure BGP AS**（基礎設施 **BGP AS**）。

- 指定最小子網路為 /96。
- 您還必須輸入 IPv4 子網路；Prisma Access 需要其網路基礎結構中的 IPv4 和 IPv6 子網路才能使用 IPv6。如需詳細資料，請參閱 Prisma Access 基礎結構管理。
- Palo Alto Networks 建議您使用私人（非公用）IPv4 和 IPv6 位址。
- 請勿使用 IPv6 連結本機位址 (fe80::/10)。




**STEP 4 |** 輸入您想要在 Prisma Access 基礎結構內使用的 **Infrastructure BGP AS**（基礎結構 **BGP AS**）。

如果您想要使用動態路由來啟用 Prisma Access，以動態探索遠端網路和總部/資料中心位置上資源的路由，請指定自發系統 (AS) 編號。如果未提供 AS 編號，則將使用預設 AS 編號 65534。

**STEP 5 |** 如果您還沒有這樣做，請考慮新增內部 DNS 伺服器，啟用 Prisma Access 解析您的內部網域，以存取公司網路上的服務，例如 LDAP 和 DNS 伺服器。

如需詳細資料，請參閱 Prisma Access 基礎結構管理。


©2025 Palo Alto Networks, Inc.

**STEP 6 |** （僅限行動使用者部署）為您的行動使用者—GlobalProtect 部署新增 IPv6 IP 位址集區。

行動使用者—GlobalProtect 部署需要 IP 位址集區。IPv4 和 IPv6 IP 位址集區是啟用 IPv6 功能所必需的。您在區域或全球層級套用 IPv4 位址；您在全球層級套用 IPv6 位址。指定最小 /80 子網路。

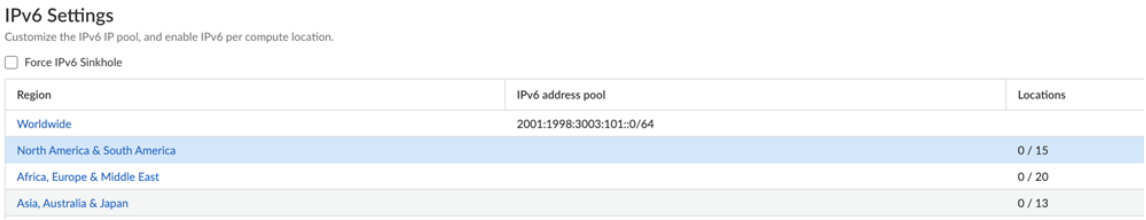
Prisma Access 使用以下方法細分全球 IPv6 位址：

- Prisma Access 為每個位置（閘道）從 /112 子網路指派一個集區。因為每個 GlobalProtect 連線都使用來自集區的一個 IP 位址，所以此配置允許將超過 65,000 個可用 IPv6 位址指派給每個位置的使用者端點。

  如果您遇到自動調整事件（如果大量使用者登入單一 Prisma Access 位置），Prisma Access 可以新增另一個位置搭配另一個 /112 子網路。
- 當您啟用某個位置使用 IPv6 時，Prisma Access 將 IPv6 位址集區指派給該位置所屬的區域，並在已啟用 IPv6 的區域總數之間分割集區。

請勿在 *IP* 位址集區中使用本機連結位址 *(fe80::/10)*。

1. 選取 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **GlobalProtect**，然後選取齒輪圖示以編輯基礎結構設定。
2. 在 [Client IP Pools（用戶端 IP 集區）] 區段中，選取一個 **Region**（區域），或選取 **Add IP Portal**（新增 **IP** 入口網站）。
3. 輸入 **IPv6 Address Pool**（**IPv6** 位址集區）。
   - 您必須為行動使用者輸入 IPv4 和 IPv6 IP 位址。使用 IPv6 時，Prisma Access 需要 IPv4 和 IPv6 位址來支援其內部基礎結構。
   - 輸入最小 IPv6 子網路 /80。
   - Prisma Access 根據區域細分每個子網路。



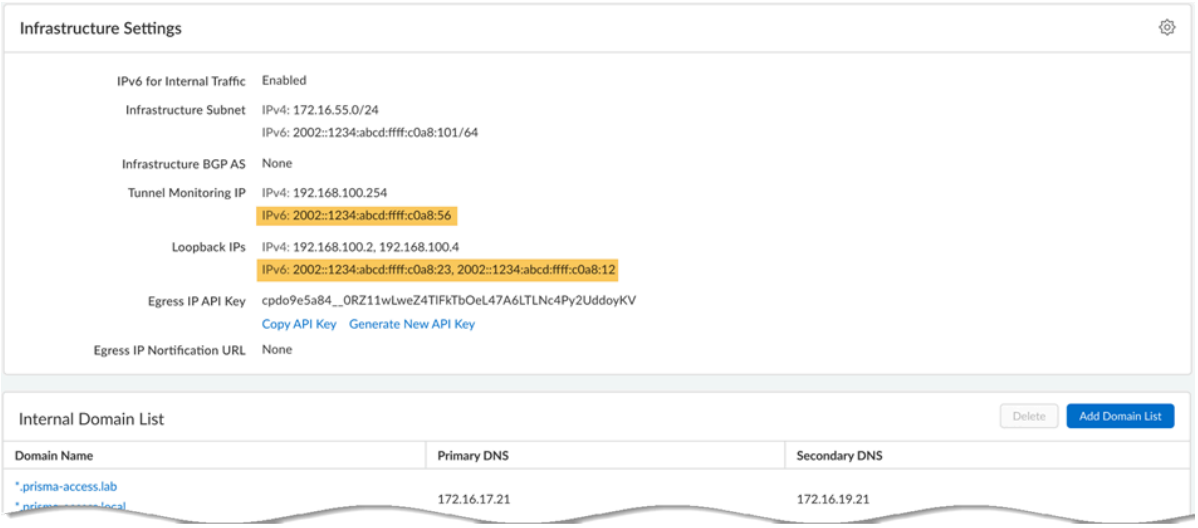

**STEP 7 |** **Save**（儲存）並 **Push Config**（推送設定）。

 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** 選取 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Prisma Access**，並記下基礎結構設定中的下列 IPv6 位址：

- **Captive Portal Redirect IP Addresses**（被控制的入口網站重新導向 **IP** 位址）—已與驗證入口網站型 User-ID 對應搭配使用
- **Tunnel Monitor IP Address**（通道監控 **IP** 位址）—用於通道監控

因為 GlobalProtect 行動使用者需要 VPN 通道的 IPv4 位址，所以其 IP 位址取自基礎結構子網路的回送位址仍使用 IPv4 位址。




## 在您的 Prisma Access 基礎結構中啟用並設定 IPv6 網路和 IP 集區 (Panorama)

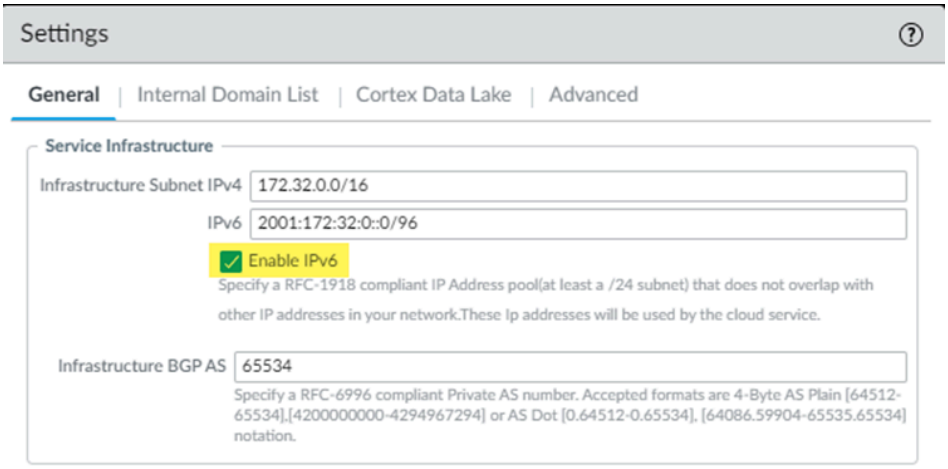
**STEP 1 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定），然後按一下齒輪圖示以編輯設定。


©2025 Palo Alto Networks, Inc.

**STEP 2 |** 在 **General**（一般）頁籤上，選取 **Enable IPv6**（啟用 **IPv6**）。

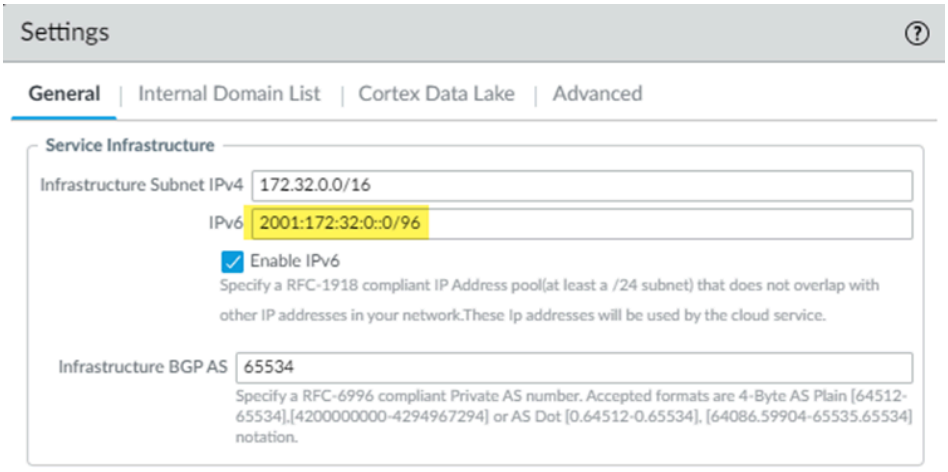
啟用或停用 IPv6 會導致短暫的流量中斷（最多 120 秒），同時資料平面準備接受或拒絕 Prisma Access 骨幹上的 IPv6 路由。Palo Alto Networks 建議您在維護時段或非尖峰時刻提交此組態變更。

如果您需要刪除 *IPv6*，請先刪除所有設定（包括行動使用者、遠端網路和服務連線（如果適用）），然後再取消選取 ***Enable IPv6***（啟用 ***IPv6***）核取方塊。




**STEP 3 |** 指定 **IPv6** 基礎結構子網路和 **Infrastructure BGP AS**（基礎設施 **BGP AS**）。

- 指定最小子網路為 /96。
- 您還必須輸入 IPv4 子網路；Prisma Access 需要其網路基礎結構中的 IPv4 和 IPv6 子網路才能使用 IPv6。如需詳細資料，請參閱 設定 Prisma Access 服務基礎結構 (Panorama)。
- Palo Alto Networks 建議您使用私人（非公用）IPv4 和 IPv6 位址。
- 請勿使用 IPv6 連結本機位址 (fe80::/10)。




 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 輸入您想要在 Prisma Access 基礎結構內使用的 **Infrastructure BGP AS**（基礎結構 **BGP AS**）。

如果您想要使用動態路由來啟用 Prisma Access，以動態探索遠端網路和總部/資料中心位置上資源的路由，請指定自發系統 (AS) 編號。如果未提供 AS 編號，則將使用預設 AS 編號 65534。

**STEP 5 |** 如果您尚未完成服務設定，請輸入 **Internal Domain List**（內部網域清單）、**Strata Logging Service**（**Strata** 記錄服務）和 **Advanced**（進階）設定。

如需詳細資料，請參閱 設定 Prisma Access 服務基礎結構 (Panorama)。

 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** （僅限行動使用者部署）為您的行動使用者—GlobalProtect 部署新增 IPv6 IP 位址集區。

行動使用者—GlobalProtect 部署需要 IP 位址集區。IPv4 和 IPv6 IP 位址集區是啟用 IPv6 功能所必需的。您在區域或全球層級套用 IPv4 位址；您在全球層級套用 IPv6 位址。指定最小 /80 子網路。

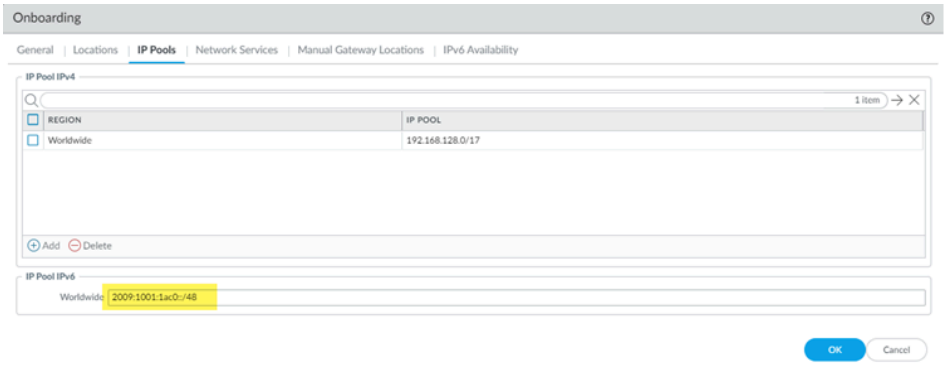
Prisma Access 使用以下方法細分全球 IPv6 位址：

- Prisma Access 為每個位置（閘道）從 /112 子網路指派一個集區。因為每個 GlobalProtect 連線都使用來自集區的一個 IP 位址，所以此配置允許將超過 65,000 個可用 IPv6 位址指派給每個位置的使用者端點。

  如果您遇到自動調整事件（如果大量使用者登入單一 Prisma Access 位置），Prisma Access 可以新增另一個位置搭配另一個 /112 子網路。
- 當您啟用某個位置使用 IPv6 時，Prisma Access 將 IPv6 位址集區指派給該位置所屬的區域，並在已啟用 IPv6 的區域總數之間分割集區。

請勿在 *IP* 位址集區中使用本機連結位址 *(fe80::/10)*。

1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users—GlobalProtect**（行動使用者—**GlobalProtect**）。
2. 在 [Onboarding（裝載）] 區段中，選取入口網站 **Hostname**（主機名稱）或選取 **Configure**（設定）。
3. 選取 **IP Pools**（**IP** 集區）頁籤。
4. 輸入一個 **IP Pool IPv6**（**IP** 集區 **IPv6**）。
   - 您必須為行動使用者輸入 IPv4 和 IPv6 IP 位址。使用 IPv6 時，Prisma Access 需要 IPv4 和 IPv6 位址來支援其內部基礎結構。
   - 輸入最小 IPv6 子網路 /80。
   - Prisma Access 根據區域細分每個子網路。



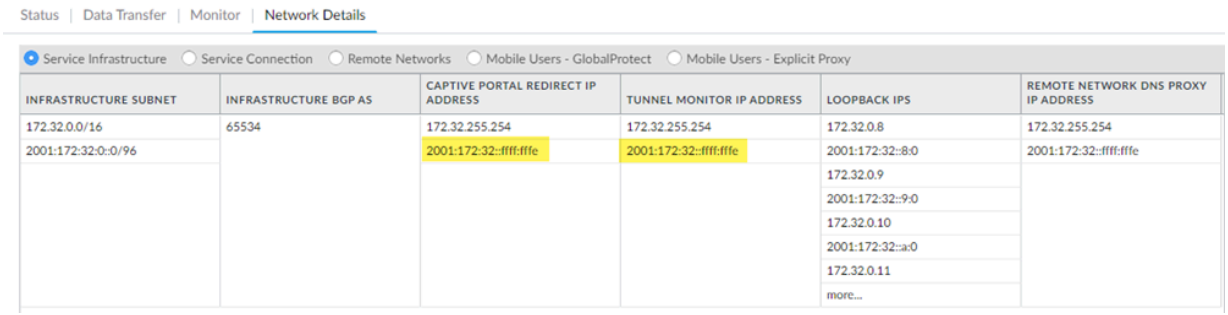

**STEP 7 |** **Commit and Push**（提交並推送）您的變更。

 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Service Infrastructure**（服務基礎結構），並記下以下 IPv6 位址：

- **Captive Portal Redirect IP Addresses**（被控制的入口網站重新導向 **IP** 位址）—已與驗證入口網站型 User-ID 對應搭配使用
- **Tunnel Monitor IP Address**（通道監控 **IP** 位址）—用於通道監控

因為 GlobalProtect 行動使用者需要 VPN 通道的 IPv4 位址，所以其 IP 位址取自基礎結構子網路的回送位址仍使用 IPv4 位址。




# 為行動使用者—GlobalProtect 部署啟用 IPv6 網路

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 2.2 版 Preferred 和更新版本<br>❑ 對公用和私人應用程式的原生 IPv6 存取需要以下最低版本：<br>• Prisma Access (Managed by Strata Cloud Manager):2024 年 6 月發行<br>• Prisma Access (Managed by Panorama):Prisma Access 5.1.1 僅適用於新部署。<br>任何其他部署（包括現有的 Prisma Access (Managed by Panorama) 部署）僅支援私人應用程式存取。 |

除了指定行動使用者 IP 位址集區之外，您還必須為行動使用者—GlobalProtect 部署設定 **IPv6 Availability**（**IPv6** 可用性）。如果您的網路使用 IPv6 DNS 伺服器來解析內部網域，您也可以為主要和次要 DNS 伺服器指定 IPv6 位址，如下節所示。

- Strata Cloud Manager
- Panorama

 ©2025 Palo Alto Networks, Inc.

## 為行動使用者—GlobalProtect 部署啟用 IPv6 網路 (Strata Cloud Manager)

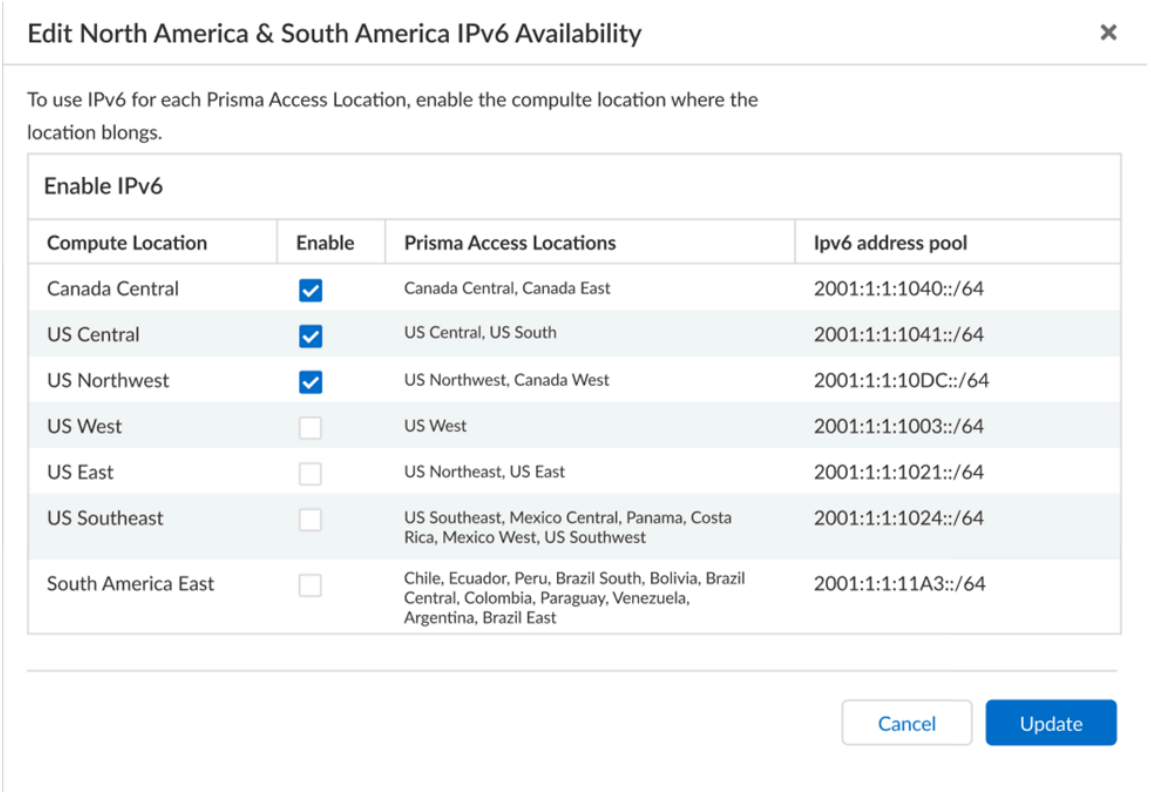
除了指定行動使用者 IP 位址集區之外，您還必須為行動使用者—GlobalProtect 部署設定 **IPv6 Availability**（**IPv6** 可用性）。如果您的網路使用 IPv6 DNS 伺服器來解析內部網域，您也可以為主要和次要 DNS 伺服器指定 IPv6 位址，如下節所示。

**STEP 1 |** 請規劃您想要在整個 Prisma Access 部署中部署 IPv6，還是僅針對一定數目的計算位置進行部署。

**STEP 2 |** 為要部署 IPv6 的區域設定 IPv6 可用性。

1. 選取 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **GlobalProtect**，然後選取齒輪圖示以編輯 **Infrastructure Settings**（基礎結構設定）。
2. 在 **IPv6 Settings**（**IPv6** 設定）區段中，選擇要 **Enable**（啟用）IPv6 的位置。

   所有位置都與一個計算位置相關聯。如果計算位置中的位置未啟用 IPv6，請取消選取該計算位置。




**STEP 3 |** （選用）如果您使用的內部 DNS 伺服器可透過 IPv6 位址連線，請從 **Client DNS**（用戶端 **DNS**）區段中選取 **Add Region**（新增區域）、選取 **Resolve Internal Domains**（解析內部網域）的核取方塊、**Add**（新增）規則或指定預設規則，然後為 **Primary DNS**（主要 **DNS**）和 **Secondary DNS**（次要 **DNS**）伺服器指定 **Custom**（自訂）DNS 伺服器 IPv6 位址。

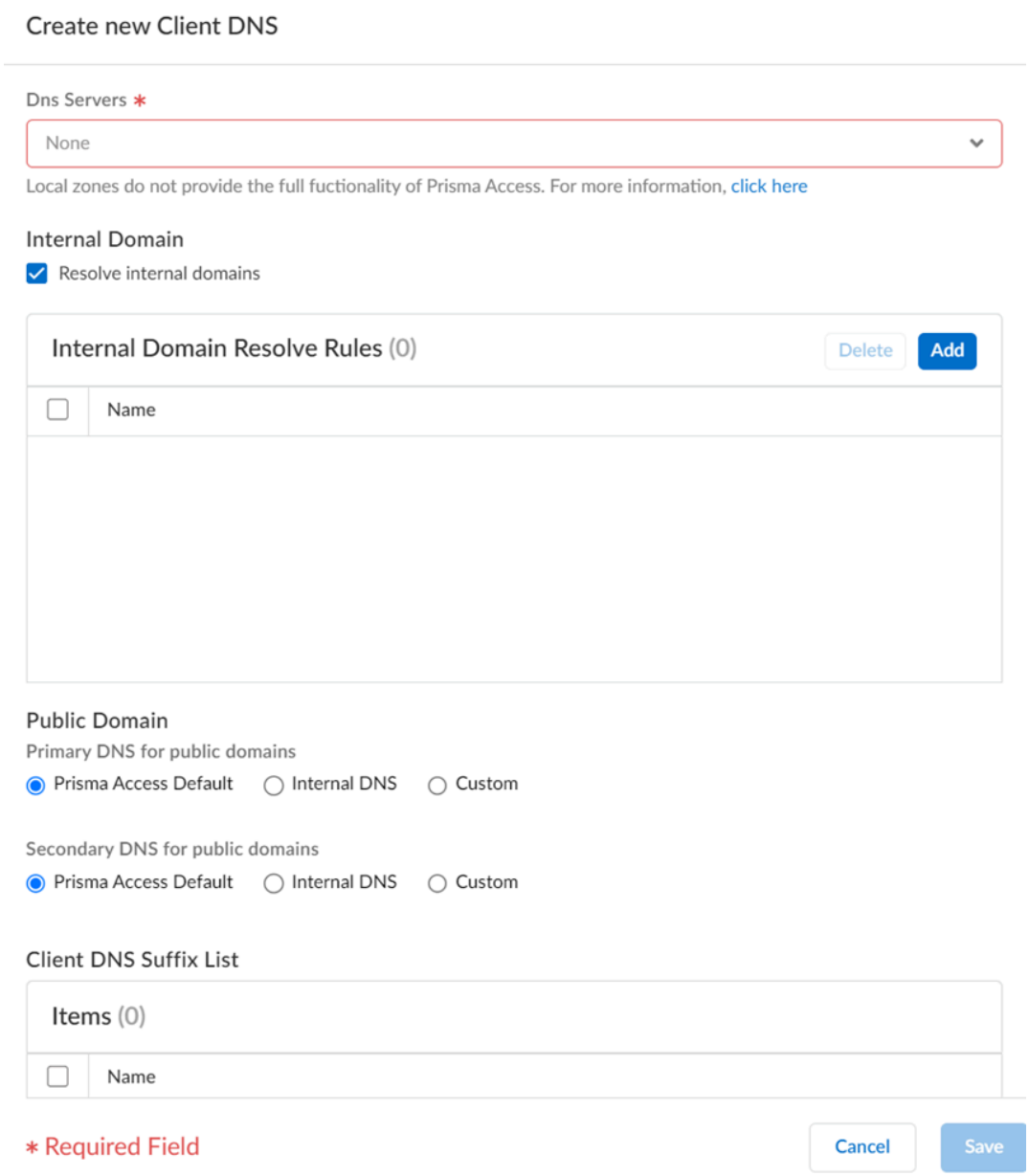
如果您輸入 DNS 伺服器的 IPv6 位址，您的行動使用者 IP 位址集區中也必須具有 IPv6 位址。

您可以為主要和次要 DNS 伺服器輸入 IPv4 或 IPv6 位址的任意組合。如果您為主要 DNS 伺服器輸入 IPv6 位址，為次要 DNS 伺服器輸入 IPv4 位址，並且從未啟用 **IPv6 Availability**（**IPv6**

 ©2025 Palo Alto Networks, Inc.

可用性）的計算位置收到 DNS 查詢，Prisma Access 使用次要 DNS 伺服器，因為它使用 IPv4 位址。

*IPv4* 位址使用 *A* 記錄，而 *IPv6* 位址使用 *AAAA* 記錄。有些 *DNS* 伺服器可以透過 *IPv4* 傳輸執行 *AAAA DNS* 查閱；因此，您可能不需要具有 *IPv6 IP* 位址的伺服器。




**STEP 4 |** （選用）如果您尚未完成行動使用者設定，請立即完成。如需詳細資訊，請參閱設定 GlobalProtect 行動使用者。

**STEP 5 |** **Push Config**（推送設定）以將您的變更部署到您的網路。


©2025 Palo Alto Networks, Inc.

## 為行動使用者—GlobalProtect 部署啟用 IPv6 網路 (Panorama)

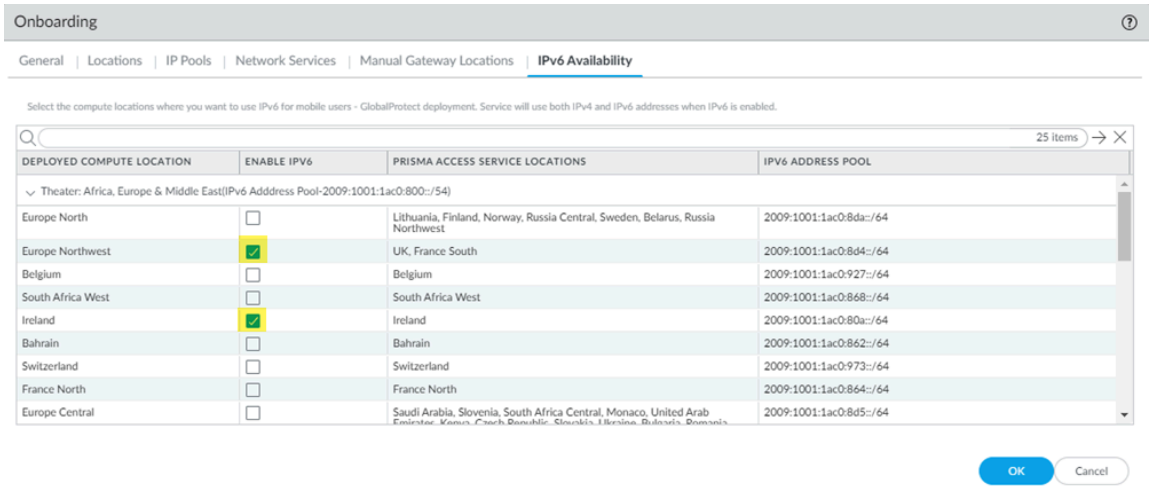
除了指定行動使用者 IP 位址集區之外，您還必須為行動使用者—GlobalProtect 部署設定 **IPv6 Availability**（**IPv6** 可用性）。如果您的網路使用 IPv6 DNS 伺服器來解析內部網域，您也可以為主要和次要 DNS 伺服器指定 IPv6 位址，如下節所示。

**STEP 1 |** 請規劃您想要在整個 <ph keyref="pa"/> 部署中部署 IPv6，還是僅針對一定數目的計算位置進行部署。

**STEP 2 |** 為要部署 IPv6 的區域設定 IPv6 可用性。

1. 在 **IPv6 Availability**（**IPv6** 可用性）頁籤中，為要啟用 IPv6 的位置 **Enable IPv6**（啟用 **IPv6**）。

   所有位置都與一個計算位置相關聯。如果計算位置中的位置未啟用 IPv6，請取消選取該計算位置。




**STEP 3 |** （選用）如果您使用的內部 DNS 伺服器可透過 IPv6 位址連線，請按一下 **Network Services**（網路服務）、**Add**（新增）規則或指定預設規則，然後為 **Primary DNS**（主要 **DNS**）和 **Secondary DNS**（次要 **DNS**）伺服器指定 **Custom**（自訂）DNS 伺服器 IPv6 位址。

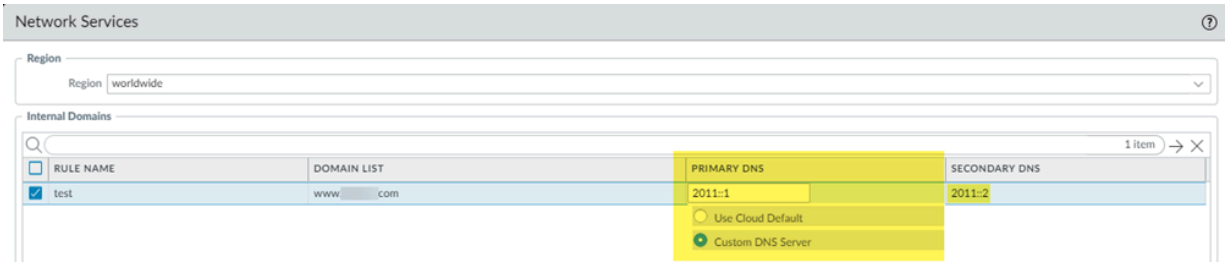
如果您輸入 DNS 伺服器的 IPv6 位址，您的行動使用者 IP 位址集區中也必須具有 IPv6 位址。

您可以為主要和次要 DNS 伺服器輸入 IPv4 或 IPv6 位址的任意組合。如果您為主要 DNS 伺服器輸入 IPv6 位址，為次要 DNS 伺服器輸入 IPv4 位址，並且從未啟用 **IPv6 Availability**（**IPv6**

 ©2025 Palo Alto Networks, Inc.

可用性）的計算位置收到 DNS 查詢，<ph keyref="pa"/> 使用次要 DNS 伺服器，因為它使用 IPv4 位址。

*IPv4* 位址使用 *A* 記錄，而 *IPv6* 位址使用 *AAAA* 記錄。有些 *DNS* 伺服器可以透過 *IPv4* 傳輸執行 *AAAA DNS* 查閱；因此，您可能不需要具有 *IPv6 IP* 位址的伺服器。




**STEP 4 |** （選用）如果您尚未完成行動使用者設定，請立即完成。如需詳細資訊，請參閱設定 GlobalProtect 行動使用者。

**STEP 5 |** **Commit and Push**（提交並推送）您的變更。

# 為服務連線啟用 IPv6 網路

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 2.2 版 Preferred 和更新版本<br>❑ 對公用和私人應用程式的原生 IPv6 存取需要以下最低版本：<br>• Prisma Access (Managed by Strata Cloud Manager):2024 年 6 月發行<br>• Prisma Access (Managed by Panorama):Prisma Access 5.1.1 僅適用於新部署。<br>任何其他部署（包括現有的 Prisma Access (Managed by Panorama) 部署）僅支援私人應用程式存取。 |

對於服務連接，您可以將 IPv6 子網路用於靜態或 BGP 路由。對於 BGP 路由，您可以輸入 IPv6 對等位址，並指定 IPv4 和 IPv6 路由選項。

若要設定 IPv6 網路進行服務連線，請完成以下工作。

- Prisma Access (Managed by Strata Cloud Manager)
- Prisma Access (Managed by Panorama)

## 為服務連線啟用 IPv6 網路 (Strata Cloud Manager)

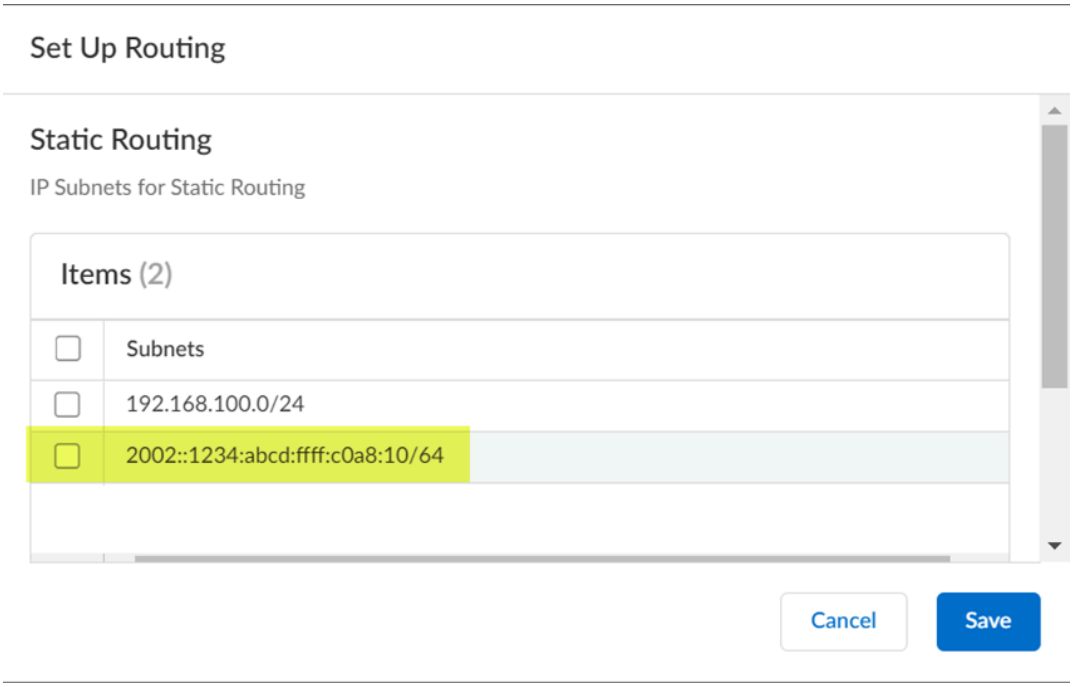
 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** 選取 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Service Connections**（服務連線），並 **Add Service Connection**（新增服務連線）。

**STEP 2 |** 新增服務連線或選取現有服務連線進行編輯。

**STEP 3 |** 為服務連線設定 IPv6 路由。

1. （僅限靜態路由部署）在 **Static Routes**（靜態路由）頁籤中輸入一個或多個 **Corporate Subnets**（企業子網路）。




2. (僅限 BGP 路由部署）指定交換 IPv4 和 IPv6 BGP 路由的方法；然後，輸入 IPv6 **Peer Address**（對等位址）和 **Local Address**（本機位址）。
   - 若要使用單一 IPv4 BGP 工作階段交換 IPv4 和 IPv6 BGP 對等資訊，請選取 **Exchange both IPv4 and IPv6 routes over IPv4 peering**（通過 **IPv4** 對等交換 **IPv4** 和 **IPv6** 路由）。
   - 若要使用 IPv4 BGP 工作階段交換 IPv4 BGP 對等資訊，以及使用 IPv6 工作階段交換 IPv6 BGP 對等資訊，請選取 **Exchange IPv4 routes over IPv4 peering and IPv6**

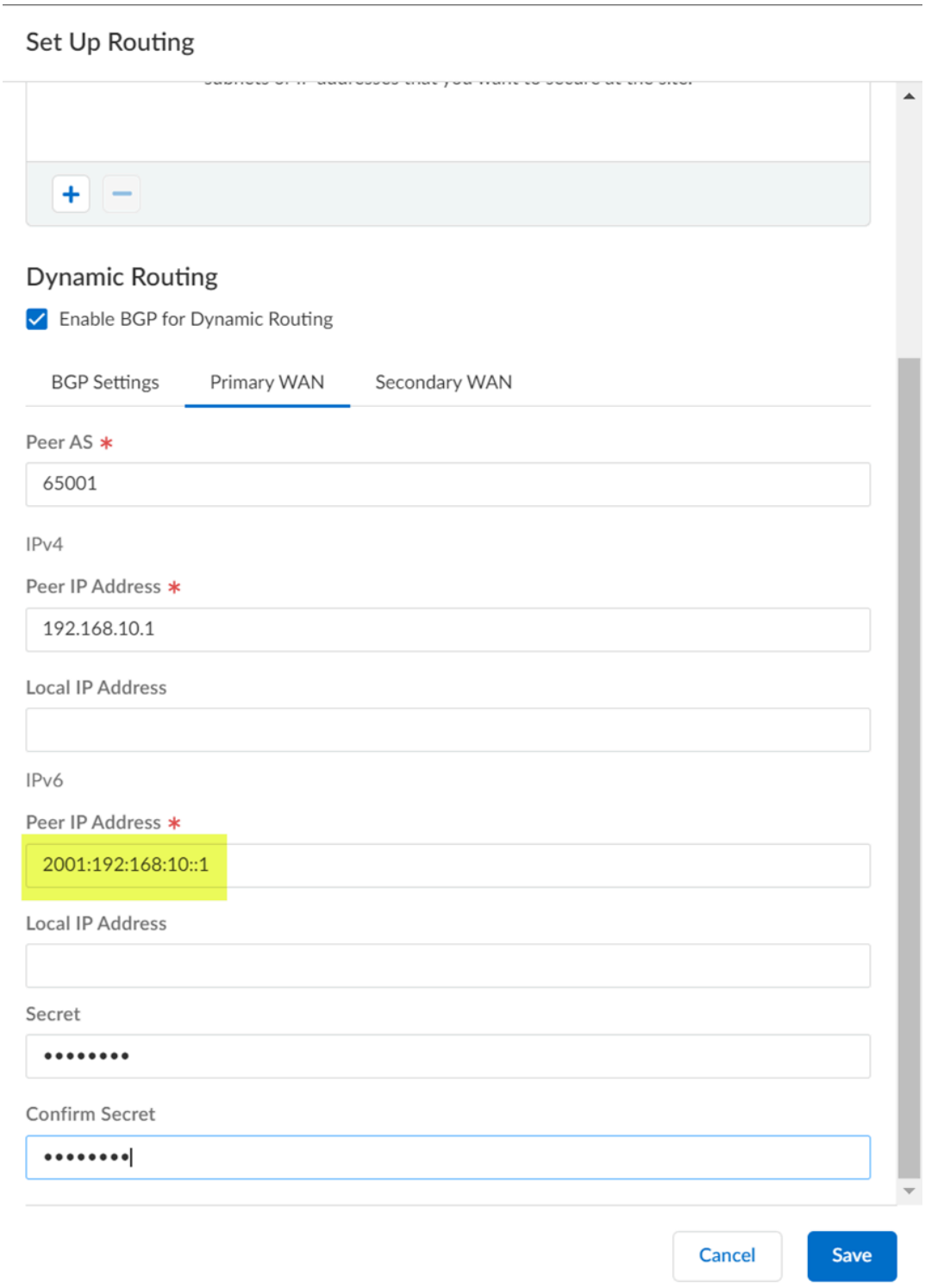
 ©2025 Palo Alto Networks, Inc.

**routes over IPv6 peering**（透過 **IPv4** 對等交換 **IPv4** 路由，以及邊過 **IPv6** 對等交換 **IPv6** 路由）。

- 若要使用單一 IPv6 BGP 工作階段交換 IPv6 BGP 對等資訊，請選取 **Exchange IPv6 routes over IPv6 peering**（透過 **IPv6** 對等交換 **IPv6** 路由）。

3. 如果您的次要 WAN 使用不同的對等或本機位址，請取消選取 **Same as Primary WAN**（與主要 **WAN** 相同），並為次要 WAN 輸入 IPv6 **Peer Address**（對等位址）和 **Local Address**（本機位址）。


©2025 Palo Alto Networks, Inc.




**STEP 4 |** 如果您尚未完成服務連線設定，請立即完成。如需詳細資訊，請參閱在 Prisma Access 中設定服務連線。

服務連線的 *IPv6* 網際網路存取由底層連線啟用，其中 *IPv6* 流量透過 *IPv4* 通道傳遞。


©2025 Palo Alto Networks, Inc.

**STEP 5 |** **Push Config**（推送設定）以將您的變更部署到您的網路。

**STEP 6 |** 如果您尚未完成行動使用者設定，請立即完成。

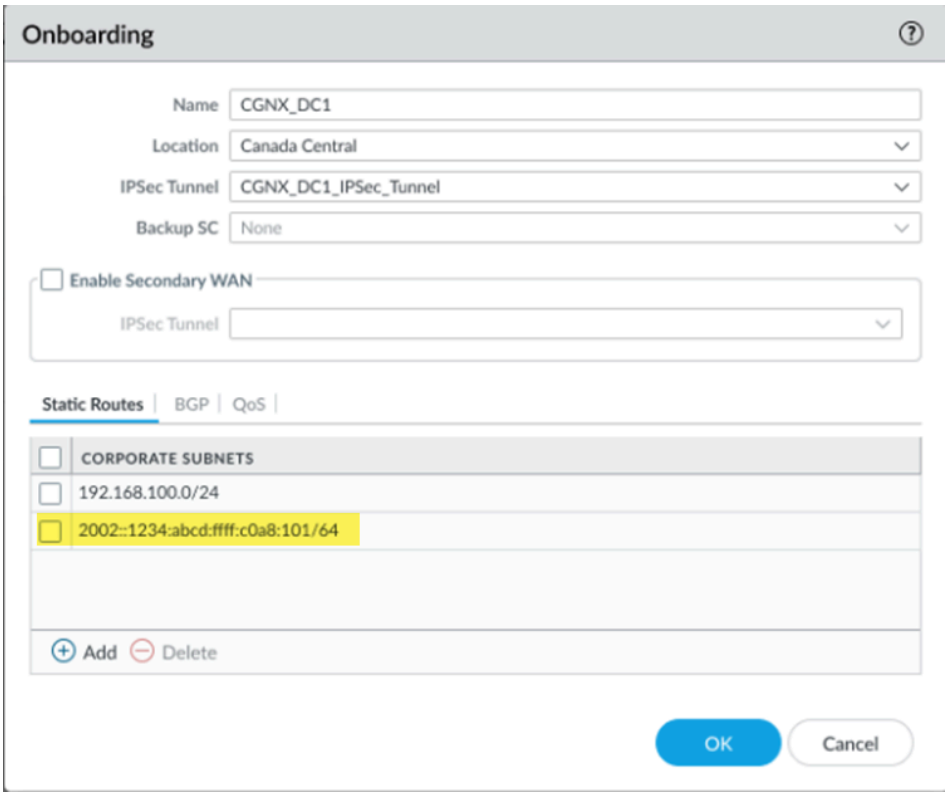
## 為服務連線啟用 IPv6 網路 (Panorama)

**STEP 1 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Connection**（服務連線）。

**STEP 2 |** **Add**（新增）服務連線或選取現有服務連線進行編輯。

**STEP 3 |** 為服務連線設定 IPv6 路由。

1. （僅限靜態路由部署）在 **Static Routes**（靜態路由）頁籤中輸入一個或多個 **Corporate Subnets**（企業子網路）。



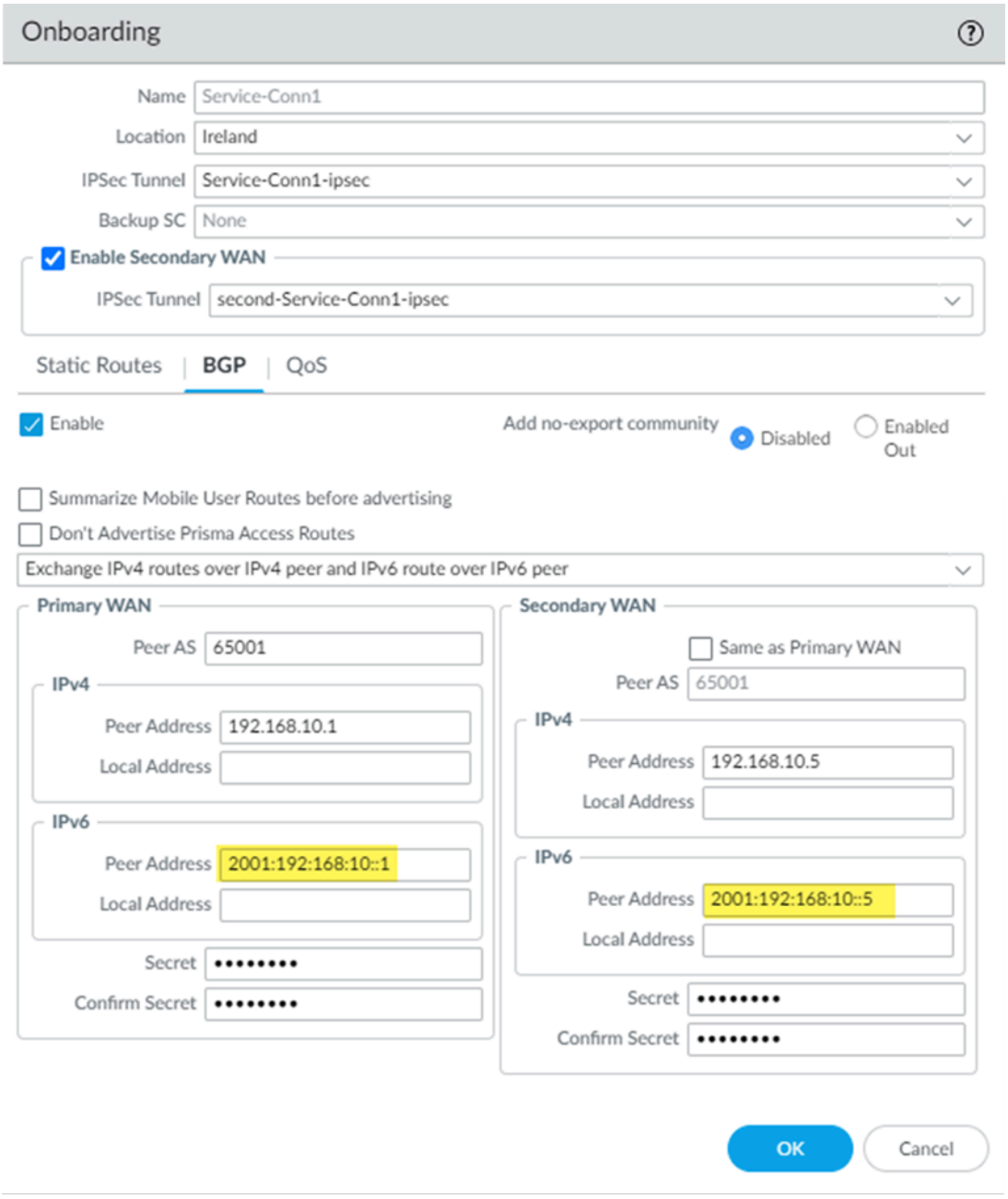

2. (僅限 BGP 路由部署）指定交換 IPv4 和 IPv6 BGP 路由的方法；然後，輸入 IPv6 **Peer Address**（對等位址）和 **Local Address**（本機位址）。
   - 若要使用單一 IPv4 BGP 工作階段交換 IPv4 和 IPv6 BGP 對等資訊，請選取 **Exchange both IPv4 and IPv6 routes over IPv4 peering**（通過 **IPv4** 對等交換 **IPv4** 和 **IPv6** 路由）。
   - 若要使用 IPv4 BGP 工作階段交換 IPv4 BGP 對等資訊，以及使用 IPv6 工作階段交換 IPv6 BGP 對等資訊，請選取 **Exchange IPv4 routes over IPv4 peering and IPv6**

 ©2025 Palo Alto Networks, Inc.

**routes over IPv6 peering**（透過 **IPv4** 對等交換 **IPv4** 路由，以及邊過 **IPv6** 對等交換 **IPv6** 路由）。

- 若要使用單一 IPv6 BGP 工作階段交換 IPv6 BGP 對等資訊，請選取 **Exchange IPv6 routes over IPv6 peering**（透過 **IPv6** 對等交換 **IPv6** 路由）。

3. 如果您的次要 WAN 使用不同的對等或本機位址，請取消選取 **Same as Primary WAN**（與主要 **WAN** 相同），並為次要 WAN 輸入 IPv6 **Peer Address**（對等位址）和 **Local Address**（本機位址）。




**STEP 4 |** 如果您尚未完成服務連線設定，請立即完成。如需詳細資訊，請參閱在 Prisma Access 中設定服務連線。


©2025 Palo Alto Networks, Inc.

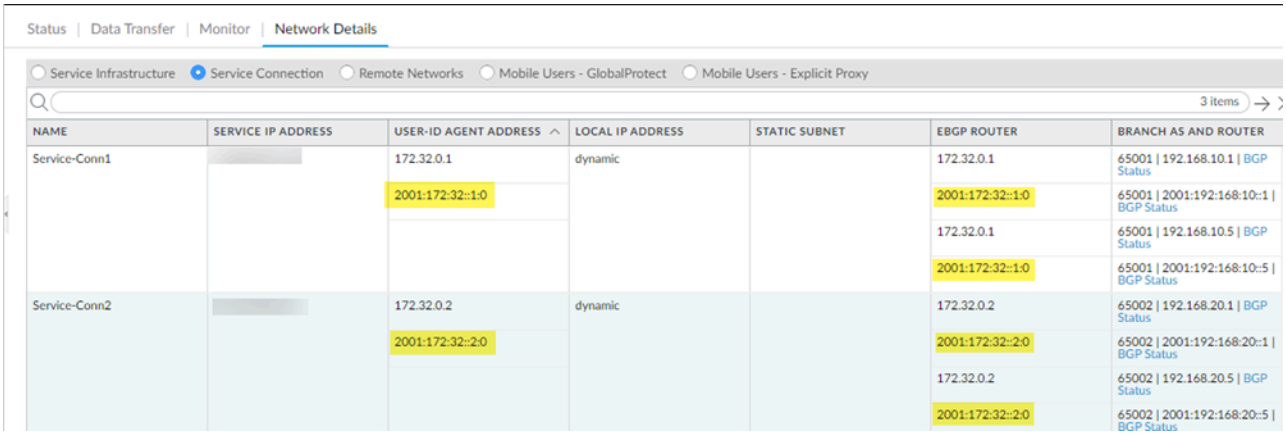
**STEP 5 |** **Commit and Push**（提交並推送）您的變更。

**STEP 6 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資料） > **Service Connection**（服務連線），並記下 IPv6 **User-ID Agent Address**（**User-ID** 代理程式位址）和 **EBGP Router**（**EBGP** 路由器）位址。

在提交您的變更之後，您將具有 IPv6 **User-ID Agent Address**（**User-ID** 代理程式位址）（用於 User-ID 擷取和散佈）和用於服務連線的 **EBGP Router**（**EBGP** 路由器） 位址。

因為用於服務連線的 IPSec 通道使用 IPv4 定址，所以 **Service IP Address**（服務 **IP** 位址）為 IPv4 位址。

服務連線的 IPv6 網際網路存取由底層連線啟用，其中 IPv6 流量透過 IPv4 通道傳遞。




**STEP 7 |** 如果您尚未完成行動使用者設定，請立即完成。

## 為遠端網路啟用 IPv6 網路

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 2.2 版 Preferred 和更新版本<br>❑ 對公用和私人應用程式的原生 IPv6 存取需要以下最低版本：<br>• Prisma Access (Managed by Strata Cloud Manager):2024 年 6 月發行<br>• Prisma Access (Managed by Panorama):Prisma Access 5.1.1 僅適用於新部署。<br>任何其他部署（包括現有的 Prisma Access (Managed by Panorama) 部署）僅支援私人應用程式存取。 |

對於遠端網路連線，您可以將 IPv6 子網路用於靜態路由。對於 BGP 路由，您可以輸入 IPv6 對等位址，並指定 BGP 僅使用 IPv6 路由或同時使用 IPv4 和 IPv6 路由。


©2025 Palo Alto Networks, Inc.

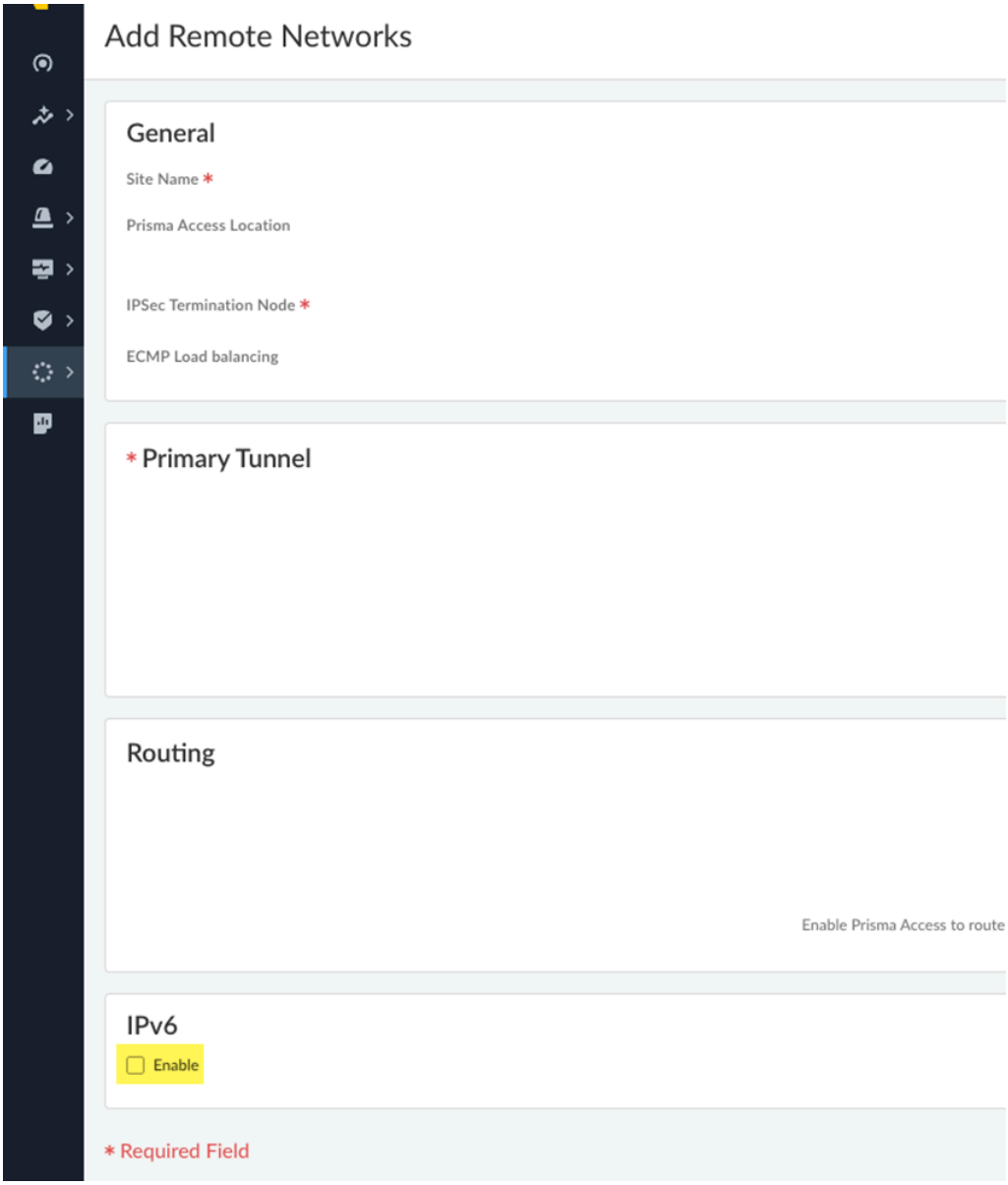
若要設定 IPv6 網路進行遠端網路連線，請完成以下工作。

- Prisma Access (Managed by Strata Cloud Manager)
- Prisma Access (Managed by Panorama)

## 為遠端網路啟用 IPv6 網路 (Strata Cloud Manager)

**STEP 1 |** 選取 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 設定） > **Remote Networks**（遠端網路）和 **Add Remote Networks**（新增遠端網路）。

**STEP 2 |** **Enable**（啟用）IPv6。

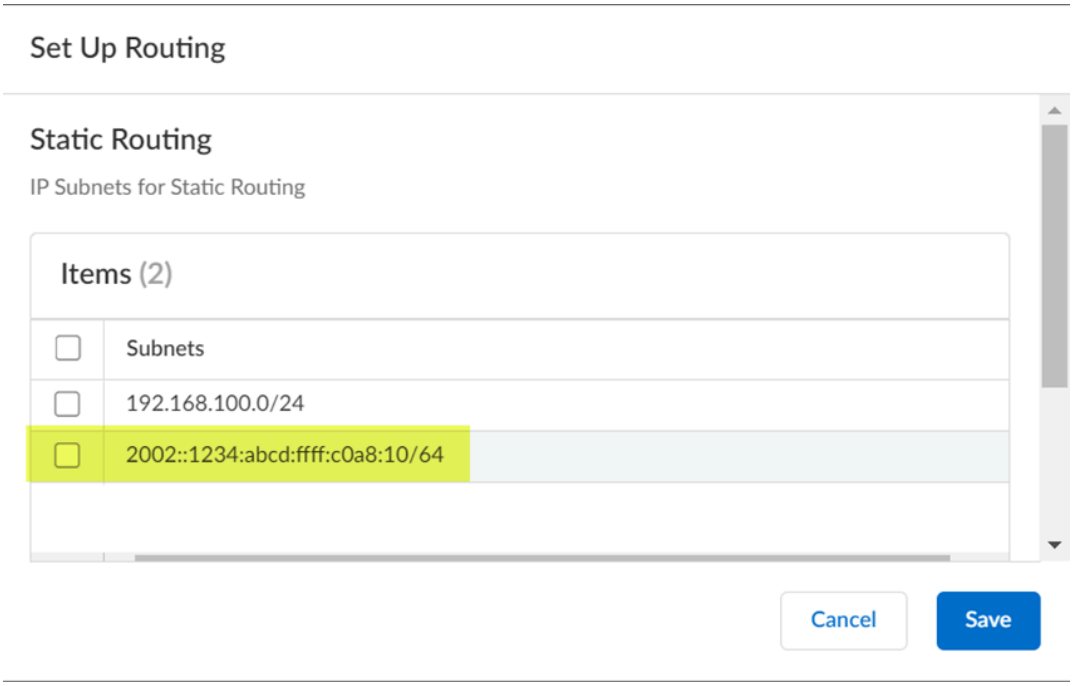



**STEP 3 |** 新增遠端網路連線或選取現有的遠端網路連線進行編輯。

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 為您的遠端網路設定 IPv6 路由。

1. （僅限靜態路由部署）在 **Static Routes**（靜態路由）頁籤中輸入一個或多個 **Corporate Subnets**（企業子網路）。




2. (僅限 BGP 路由部署）指定交換 IPv4 和 IPv6 BGP 路由的方法；然後，輸入 IPv6 **Peer Address**（對等位址）和 **Local Address**（本機位址）。
   - 若要使用單一 IPv4 BGP 工作階段交換 IPv4 和 IPv6 BGP 對等資訊，請選取 **Exchange both IPv4 and IPv6 routes over IPv4 peering**（通過 **IPv4** 對等交換 **IPv4** 和 **IPv6** 路由）。
   - 若要使用 IPv4 BGP 工作階段交換 IPv4 BGP 對等資訊，以及使用 IPv6 工作階段交換 IPv6 BGP 對等資訊，請選取 **Exchange IPv4 routes over IPv4 peering and IPv6**

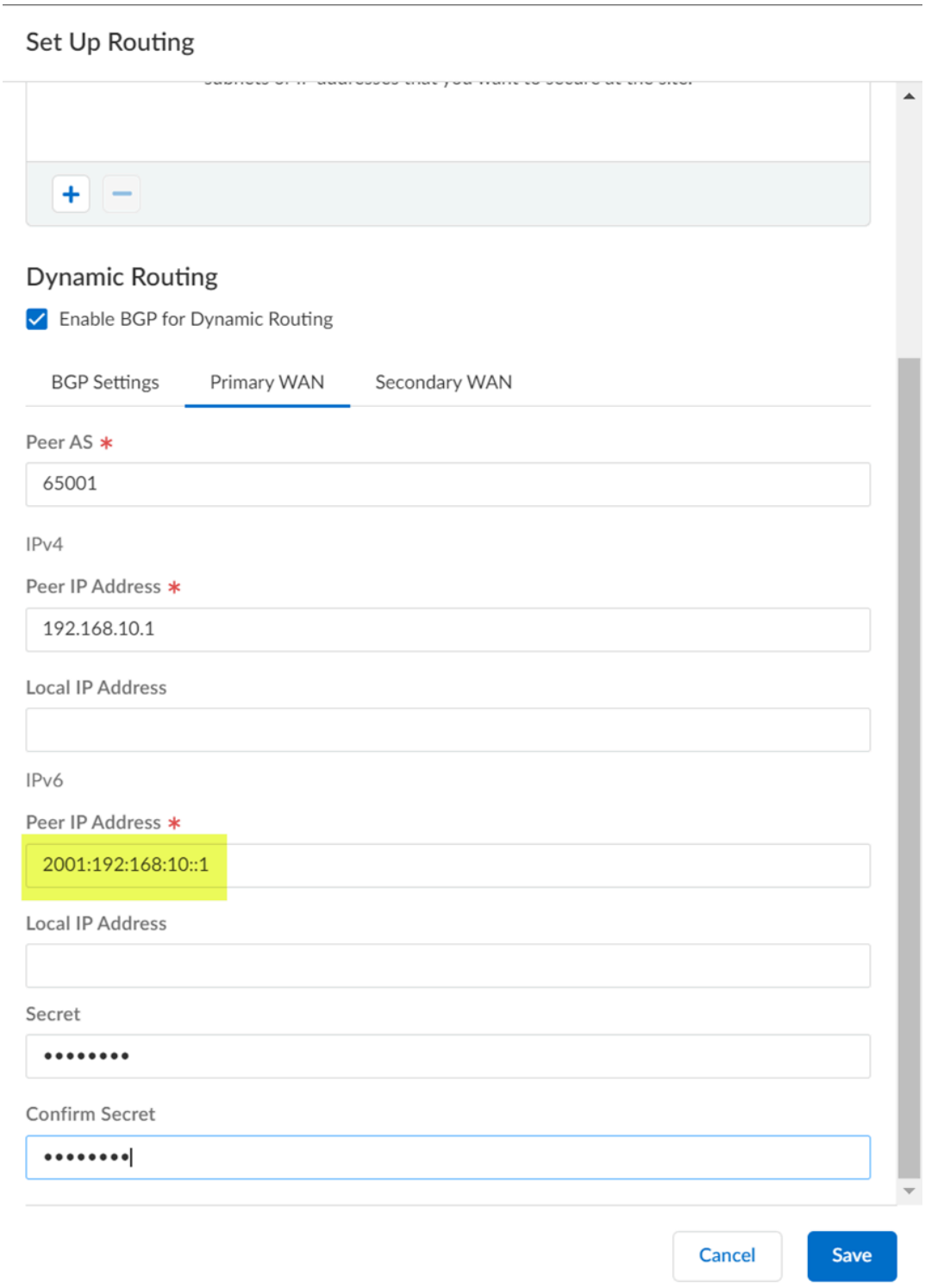
 ©2025 Palo Alto Networks, Inc.

**routes over IPv6 peering**（透過 **IPv4** 對等交換 **IPv4** 路由，以及邊過 **IPv6** 對等交換 **IPv6** 路由）。

- 若要使用單一 IPv6 BGP 工作階段交換 IPv6 BGP 對等資訊，請選取 **Exchange IPv6 routes over IPv6 peering**（透過 **IPv6** 對等交換 **IPv6** 路由）。

3. 如果您的次要 WAN 使用不同的對等或本機位址，請取消選取 **Same as Primary WAN**（與主要 **WAN** 相同），並為次要 WAN 輸入 IPv6 **Peer Address**（對等位址）和 **Local Address**（本機位址）。


©2025 Palo Alto Networks, Inc.




**STEP 5 |** （選用）如果您使用的內部 DNS 伺服器可透過 IPv6 位址連線，請選取 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Remote Networks**（遠端網路） > **Advanced Settings**（進階設定）尋找 **DNS Proxy**、**Add**（新增）規則或指定預設規則，然

 ©2025 Palo Alto Networks, Inc.

後為 **Primary DNS**（主要 **DNS**）和 **Secondary DNS**（次要 **DNS**）伺服器指定 **Custom DNS Server**（自訂 **DNS** 伺服器） IPv6 位址。

Prisma Access 可讓您指定 DNS 伺服器，以解析組織內部網域和外部網域。如果未指定任何設定，則 Prisma Access 不會對遠端網路的 DNS 要求進行 Proxy。您還需要選取一個 **Region**（區域）。

您可以為主要和次要 DNS 伺服器輸入 IPv4 或 IPv6 位址的任意組合。

- *IPv4* 位址使用 *A* 記錄，而 *IPv6* 位址使用 *AAAA* 記錄。有些 *DNS* 伺服器可以透過 *IPv4* 傳輸執行 *AAAA DNS* 查閱；因此，您可能不需要具有 *IPv6 IP* 位址的伺服器。

**STEP 6 |** 如果您尚未完成遠端網路連線設定，請立即完成。

遠端網路連線的 *IPv6* 網際網路存取由底層連線啟用，其中 *IPv6* 流量透過 *IPv4* 通道傳遞。

**STEP 7 |** **Push Config**（推送設定）以將您的變更部署到您的網路。

## 為遠端網路啟用 IPv6 網路 (Panorama)

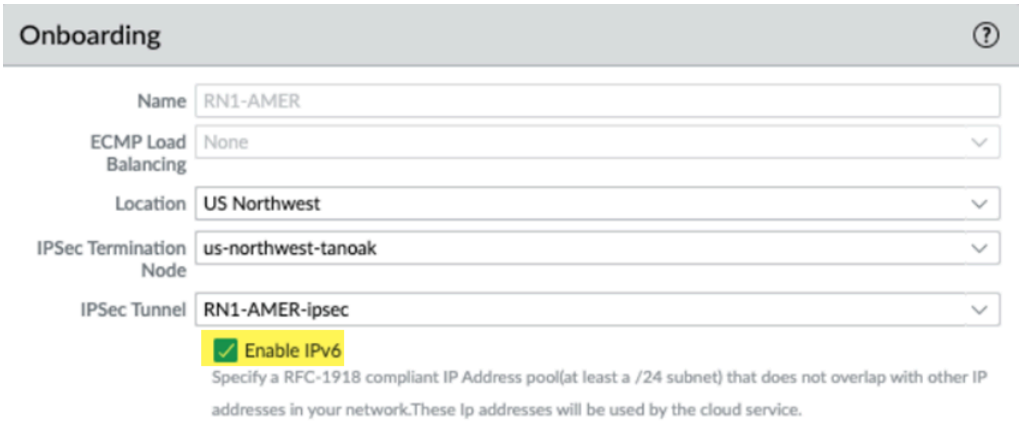
**STEP 1 |** （選用）將 IPv6 位址輸入到您的自訂 DNS 伺服器 Proxy 設定。

1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路），並按一下 **Settings**（設定）區域中的齒輪圖示編輯設定。
2. 在 **DNS Proxy** 區域中，輸入 DNS Proxy 設定的 IPv6 **Custom DNS Server**（自訂 **DNS** 伺服器)位址。

**STEP 2 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路）。

**STEP 3 |** **Add**（新增）遠端網路連線或選取現有的遠端網路連線進行編輯。

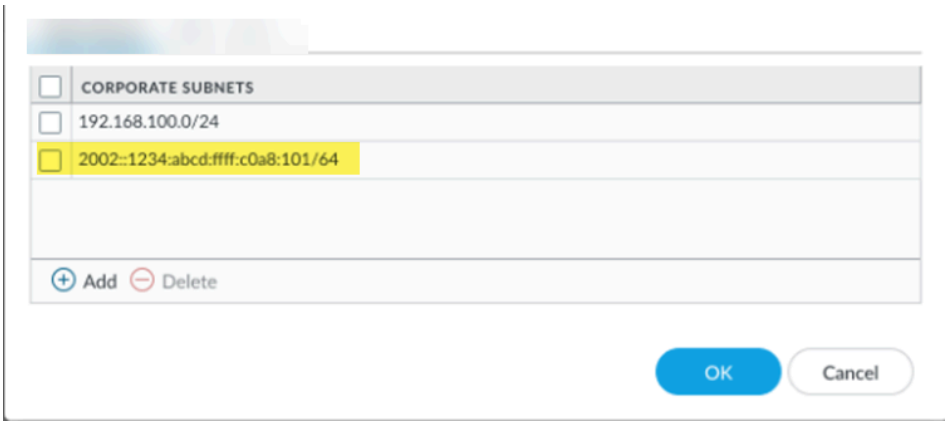
**STEP 4 |** **Enable IPv6**（啟用 **IPv6**）。




 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** 為您的遠端網路設定 IPv6 路由。

1. （僅限靜態路由部署）在 **Static Routes**（靜態路由）頁籤中輸入一個或多個 **Corporate Subnets**（企業子網路）。




2. (僅限 BGP 路由部署）指定交換 IPv4 和 IPv6 BGP 路由的方法；然後，輸入 IPv6 **Peer Address**（對等位址）和 **Local Address**（本機位址）。
   - 若要使用單一 IPv4 BGP 工作階段交換 IPv4 和 IPv6 BGP 對等資訊，請選取 **Exchange both IPv4 and IPv6 routes over IPv4 peering**（通過 **IPv4** 對等交換 **IPv4** 和 **IPv6** 路由）。
   - 若要使用 IPv4 BGP 工作階段交換 IPv4 BGP 對等資訊，以及使用 IPv6 工作階段交換 IPv6 BGP 對等資訊，請選取 **Exchange IPv4 routes over IPv4 peering and IPv6**

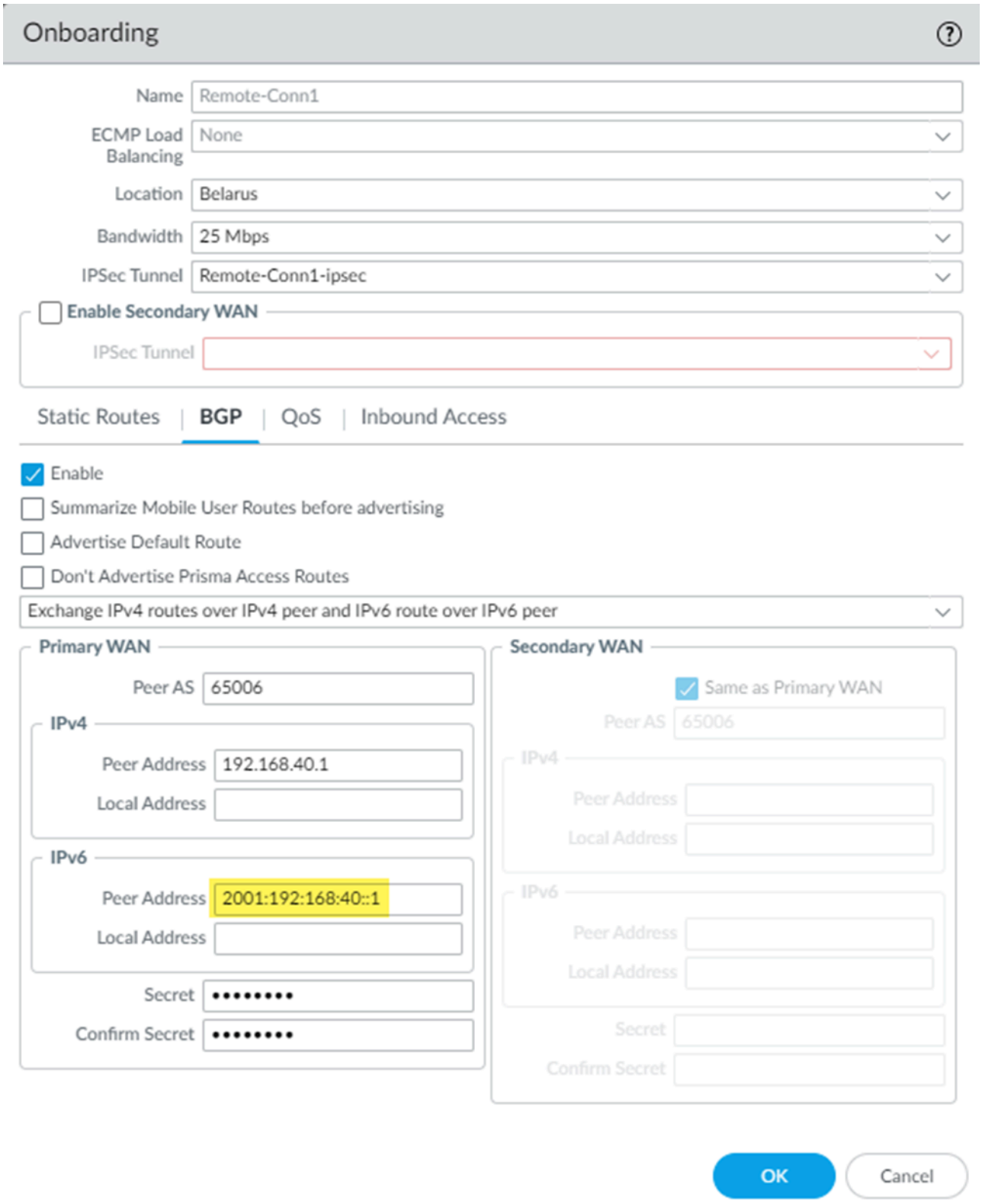
 ©2025 Palo Alto Networks, Inc.

**routes over IPv6 peering**（透過 **IPv4** 對等交換 **IPv4** 路由，以及邊過 **IPv6** 對等交換 **IPv6** 路由）。

- 若要使用單一 IPv6 BGP 工作階段交換 IPv6 BGP 對等資訊，請選取 **Exchange IPv6 routes over IPv6 peering**（透過 **IPv6** 對等交換 **IPv6** 路由）。

3. 如果您的次要 WAN 使用不同的對等或本機位址，請取消選取 **Same as Primary WAN**（與主要 **WAN** 相同），並為次要 WAN 輸入 IPv6 **Peer Address**（對等位址）和 **Local Address**（本機位址）。


©2025 Palo Alto Networks, Inc.




**STEP 6 |** （可選）如果您使用的內部 DNS 伺服器可透過 IPv6 位址存取，請選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Network**（遠端網路） > **Settings**（設定）、按一下齒輪圖示以編輯設定、選取 **DNS Proxy** 頁籤、**Add**（新增）規則

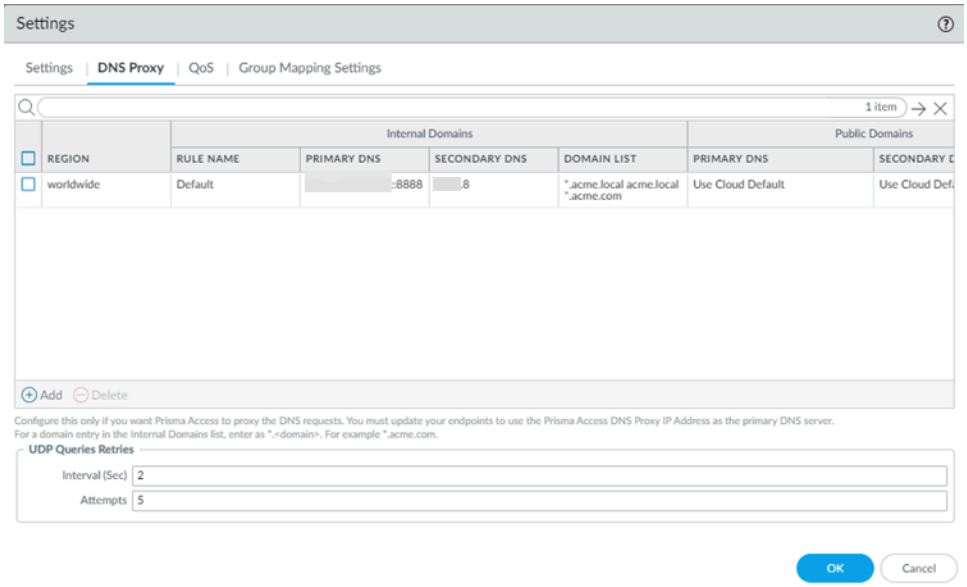
 ©2025 Palo Alto Networks, Inc.

或指定預設規則，然後為 **Primary DNS**（主要 **DNS**）和 **Secondary DNS**（次要 **DNS**）伺服器指定 **Custom DNS Server**（自訂 **DNS** 伺服器）IPv6 位址。

Prisma Access 可讓您指定 DNS 伺服器，以解析組織內部網域和外部網域。如果未指定任何設定，則 Prisma Access 不會對遠端網路的 DNS 要求進行 Proxy。您還需要選取一個 **Region**（區域）。

您可以為主要和次要 DNS 伺服器輸入 IPv4 或 IPv6 位址的任意組合。

*IPv4* 位址使用 *A* 記錄，而 *IPv6* 位址使用 *AAAA* 記錄。有些 *DNS* 伺服器可以透過 *IPv4* 傳輸執行 *AAAA DNS* 查閱；因此，您可能不需要具有 *IPv6 IP* 位址的伺服器。




**STEP 7 |** 如果您尚未完成遠端網路連線設定，請立即完成。

**STEP 8 |** **Commit and Push**（提交並推送）您的變更。

**STEP 9 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資料） > **Remote Networks**（遠端網路），並記下 **EBGP Router**（**EBGP** 路由器）位址。

在提交變更之後，您將具有用於服務連線的 IPv6 **EBGP Router**（**EBGP** 路由器）位址。

因為用於遠端網路連線的 IPSec 通道使用 IPv4 位址，所以 **Service IP Address**（服務 **IP** 位址）仍為 IPv4 位址。

遠端網路連線的 IPv6 網際網路存取由底層連線啟用，其中 IPv6 流量透過 IPv4 通道傳遞。


©2025 Palo Alto Networks, Inc.

# 行動使用者—GlobalProtect 和遠端網路部署的 DNS 解析

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 2.2 版 Preferred 和更新版本<br>❑ 對公用和私人應用程式的原生 IPv6 存取需要以下最低版本：<br>• Prisma Access (Managed by Strata Cloud Manager):2024 年 6 月發行<br>• Prisma Access (Managed by Panorama):Prisma Access 5.1.1 僅適用於新部署。<br>任何其他部署（包括現有的 Prisma Access (Managed by Panorama) 部署）僅支援私人應用程式存取。 |

Prisma Access 可讓您指定 DNS 伺服器，以解析組織內部網域和外部網域。Prisma Access 根據您 DNS 伺服器的設定對 DNS 要求進行 Proxy。下表顯示了內部和外部網域支援的 DNS 解析方法，並指出 Prisma Access 何時對 DNS 要求進行 Proxy。

| 內部 **DNS** 解析方法 | 外部 **DNS** 解析方法 | **Prisma Access** 對 **DNS** 要求進行 **Proxy**（是/否） |
| --- | --- | --- |
| 單一規則，為內部網域設定的 DNS 伺服器 | 雲端預設（適用於 IPv6 的 Google 公用 DNS64） | 是 |
| 單一規則，為內部網域設定的 DNS 伺服器 | 與內部網域相同 | 否。 |
| 單一規則，為內部網域設定的 DNS 伺服器 | 自訂 DNS 伺服器（適用於 IPv6 的 Google 公用 DNS64） | 是 |
| 單一規則，為網域設定的雲端預設 | 雲端預設（適用於 IPv6 的 Google 公用 DNS64） | 是 |
| 單一規則，為網域設定的雲端預設 | 與內部網域相同（適用於 IPv6 的 Google 公用 DNS64） | 是 |
| 單一規則，為網域設定的雲端預設 | 自訂 DNS 伺服器（適用於 IPv6 的 Google 公用 DNS64） | 是 |
| 多個規則，為內部網域設定的 DNS 伺服器 | 雲端預設（適用於 IPv6 的 Google 公用 DNS64） | 是 |

 ©2025 Palo Alto Networks, Inc.

| 內部 DNS 解析方法 | 外部 DNS 解析方法 | Prisma Access 對 DNS 要求進行 Proxy（是/否） |
|---|---|---|
| 多個規則，為內部網域設定的 DNS 伺服器 | 與內部網域相同 | 是 |
| 多個規則，為內部網域設定的 DNS 伺服器 | 自訂 DNS 伺服器（適用於 IPv6 的 Google 公用 DNS64） | 是 |
| 無設定 | 自訂 DNS 伺服器（適用於 IPv6 的 Google 公用 DNS64） | 是 |
| 無設定 | 雲端預設（對於 IPv6，主要 = Google 公有 DNS64，次要 = 雲端預設） | 否。 |
| 無設定 | 無設定 | 否。 |
| 未指定 DNS 解析（存在預設設定，其會使用雲端預設） | 未指定 DNS 解析 | 否。 |
| ZTNA 連接器（無論 *DNS* 解析方法為何） | 無 | 是 |
| 在啟用 ZTNA 連接器之後，Prisma Access 會使用為遠端網路和行動使用者—GlobalProtect 設定的 DNS 規則，對所有 DNS 要求進行 Proxy。 | | |

DNS 要求的來源 IP 位址取決於 Prisma Access 是否對 DNS 要求進行 Proxy。

- 當 Prisma Access 未對 DNS 要求進行 Proxy 時，DNS 要求的來源 IP 位址會變更為要求 DNS 查閱的裝置的 IP 位址。此來源 IP 位址可讓您強制執行來源 IP 位址型 DNS 政策，或識別與惡意網域通訊的端點。此行為適用於行動用使用者和遠端網路部署。
- 當 Prisma Access 對 DNS 要求進行 Proxy 時，DNS 要求的來源 IP 位址會變更為下列位址：
  - 行動使用者部署—DNS 要求的來源 IP 位址是從行動使用者 IP 位址集區取得的 IP 位址（適用於內部要求），以及行動使用者位置的閘道 IP 位址（適用於外部要求）。
  - 遠端網路部署—DNS 要求的來源 IP 位址是 **EBGP Router Address**（**EBGP** 路由器位址）（適用於內部要求）和遠端網路連線的服務 IP 位址（適用於外部要求）。

以下指導方針和限制適用於搭配 Prisma Access 使用 DNS 解析：

- Prisma Access 支援的並行擱置 TCP DNS 要求的數目上限（**Max Pending Requests**（擱置要求數目上限））為 64。
- 對於 UDP 查詢，如果 DNS Proxy 在 2 秒內未收到回應，則會傳送另一個要求，並在嘗試下一部 DNS 伺服器之前最多重試 5 次。
- Prisma Access 快取存留時間 (TTL) 值為 300 秒的 DNS 項目。EDNS 回應也會進行快取。

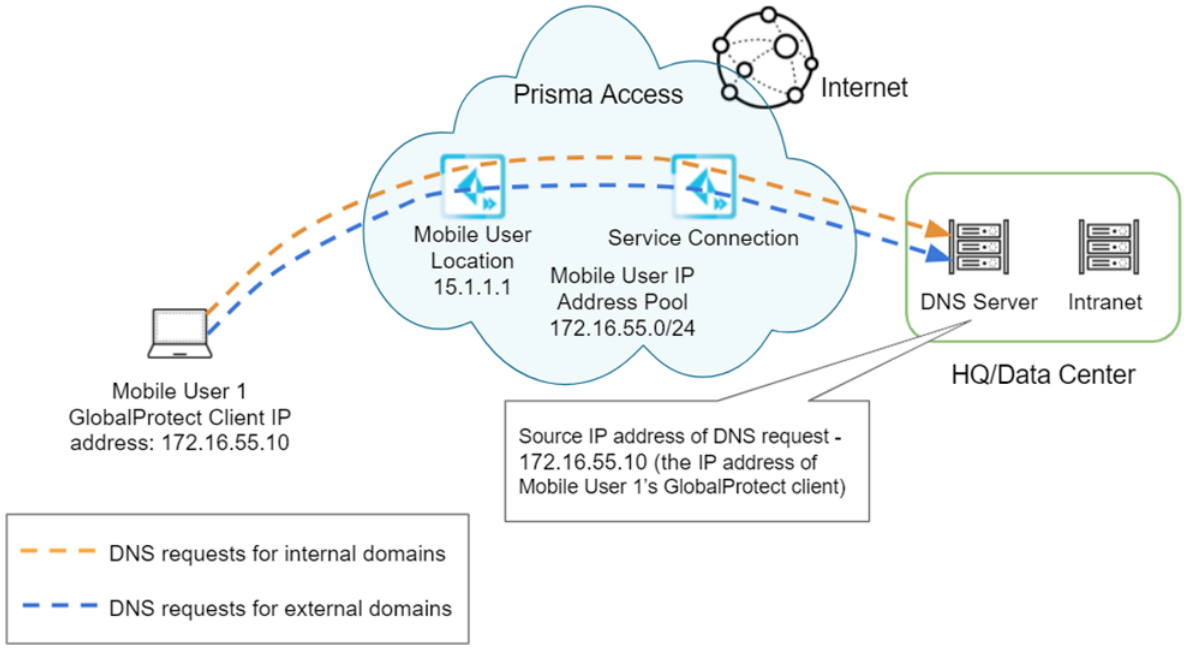

©2025 Palo Alto Networks, Inc.

# 行動使用者—GlobalProtect 部署的 DNS 解析

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Panorama | • Prisma Access 授權 |

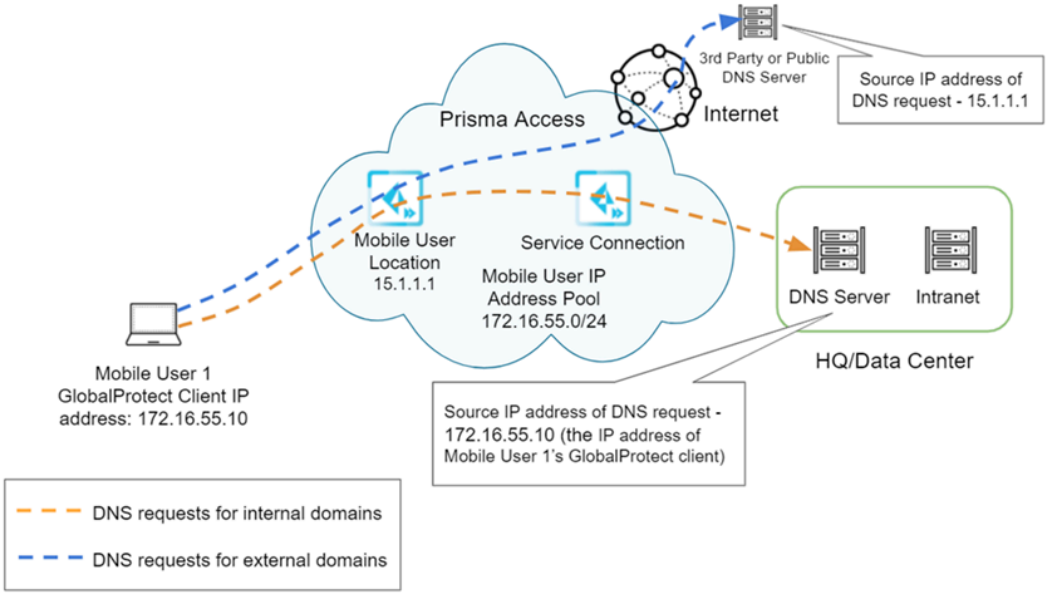
下節提供了幾個範例，展示在您為行動使用者以及為遠端網路設定 DNS 解析之後，Prisma Access 如何處理 DNS 要求的來源 IP 位址。

下圖顯示了一個部署，其中您已指派一部內部 DNS 伺服器來解析內部和外部網域。在此情況下，Prisma Access 不會對 DNS 要求進行 Proxy，並且 DNS 要求來自行動使用者 1 的 GlobalProtect 用戶端 IP 位址。GlobalProtect 用戶端將此 IP 位址指派給行動使用者，而且該位址取自於行動使用者位置的閘道 IP 位址。

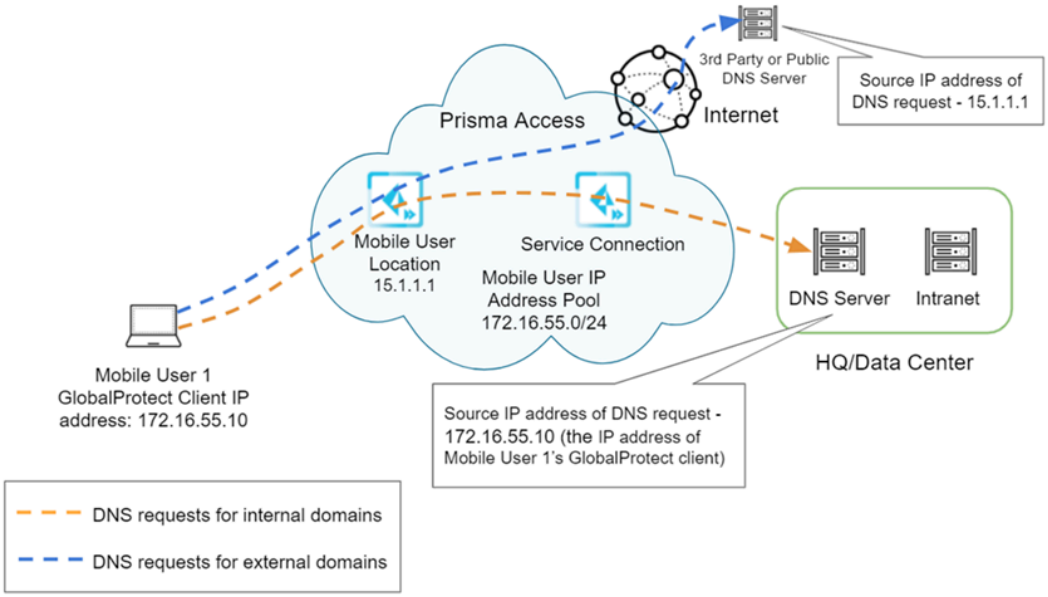



下圖顯示內部網域的 DNS 要求正被總部或資料中心位置的 DNS 伺服器解析，而外部網域的要求由 Prisma Access 雲端預設 DNS 伺服器解析。在此情況下，Prisma Access 會對外部要求進行 Proxy，且來源 IP 位址是 Prisma Access 閘道 IP 位址（在本範例中為 15.1.1.1.1），而內部來源 IP 仍為行動使用者 1 的 GlobalProtect 用戶端 IP 位址。


©2025 Palo Alto Networks, Inc.




下圖顯示了組織將可透過網際網路存取的第三方或公有 DNS 伺服器用於外部網域的要求。Prisma Access 也會對這些要求進行 Proxy。



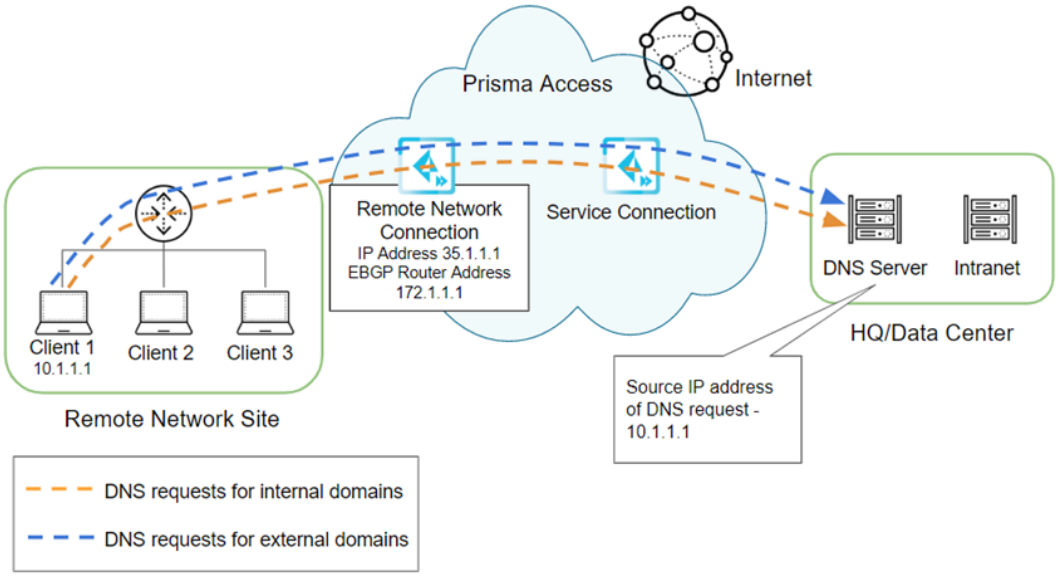

## 遠端網路的 DNS 解析

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Panorama | • Prisma Access 授權 |

如果您有現有的遠端網路部署，則可以繼續使用已準備好的 DNS 解析方法，也可以使用 Prisma Access 對 DNS 要求進行 Proxy。對 DNS 要求進行 Proxy 可讓您將公用網域的 DNS 要求傳送到一部伺服器，並將內部網域的 DNS 要求傳送到另一部伺服器。

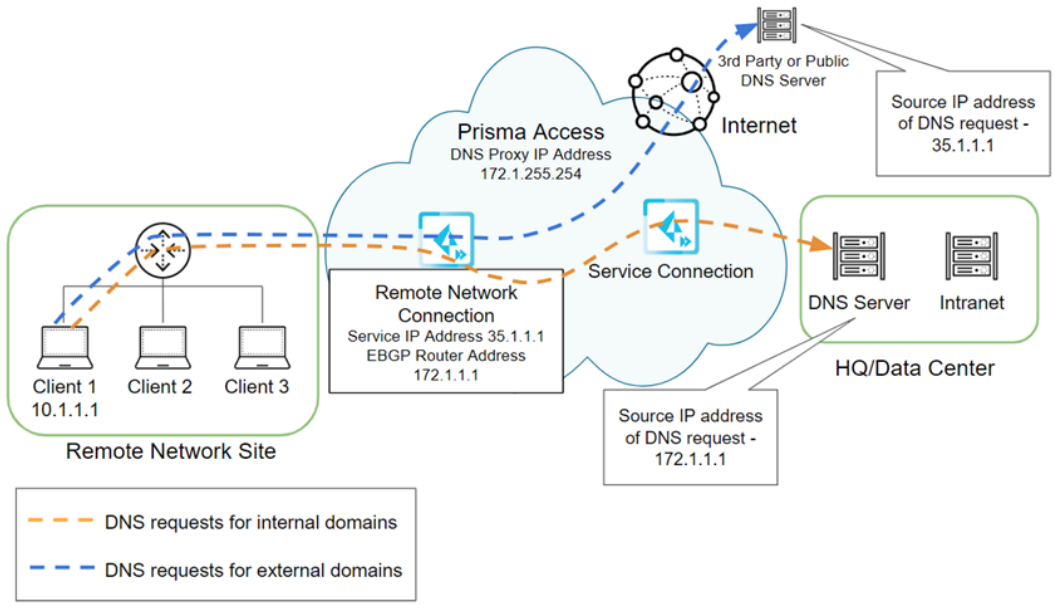
 ©2025 Palo Alto Networks, Inc.

下圖顯示了部署的 DNS 要求，其中內部 DNS 伺服器用來處理內部和外部網域的要求。遠端網路 IP 位址為 35.1.1.1，而 **EBGP Router**（**EBGP** 路由器）IP 位址為 172.1.1.1。在此情況下， Prisma Access 不會對要求進行 Proxy，如果內部 DNS 伺服器不使用 NAT，則 DNS 要求的來源 IP 為 10.1.1.1（遠端網站中用戶端 1 裝置的 IP 位址）。




如果 Prisma Access 對 DNS 要求進行 Proxy，Proxy DNS 要求的來源 IP 位址會變更為 **EBGP Router Address**（**EBGP** 路由器位址）（適用於內部要求），以及遠端網路連線的服務 IP 位址（適用於外部要求），如下圖所示。

當您設定網路中的 *DNS* 位址以用於 *Prisma Access Proxy* 外部要求，請指定 ***Remote Network DNS Proxy IP Address***（遠端網路 ***DNS Proxy IP*** 位址）（***Panorama*** > ***Cloud Services***（雲端服務） > ***Status***（狀態） > ***Service Infrastructure***（服務基礎結構） > ***Remote Network DNS Proxy IP Address***（遠端網路 ***DNS Proxy IP*** 位址））。在下列範例中，您將在網路中為 *DNS* 伺服器指定 *172.1.255.254*。



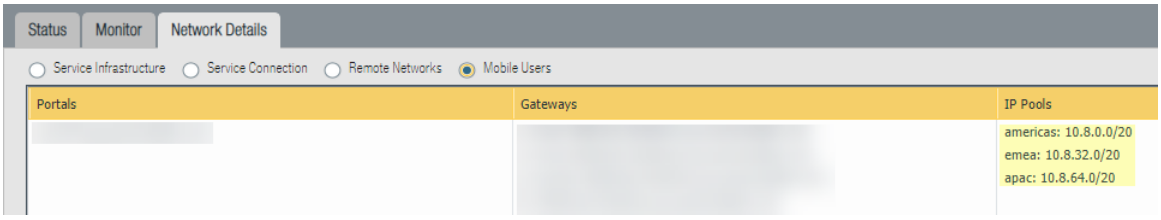

 ©2025 Palo Alto Networks, Inc.

# BGP 如何為服務連線和遠端網路連線公告行動使用者 IP 位址集區

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Panorama | • Prisma Access 授權 |

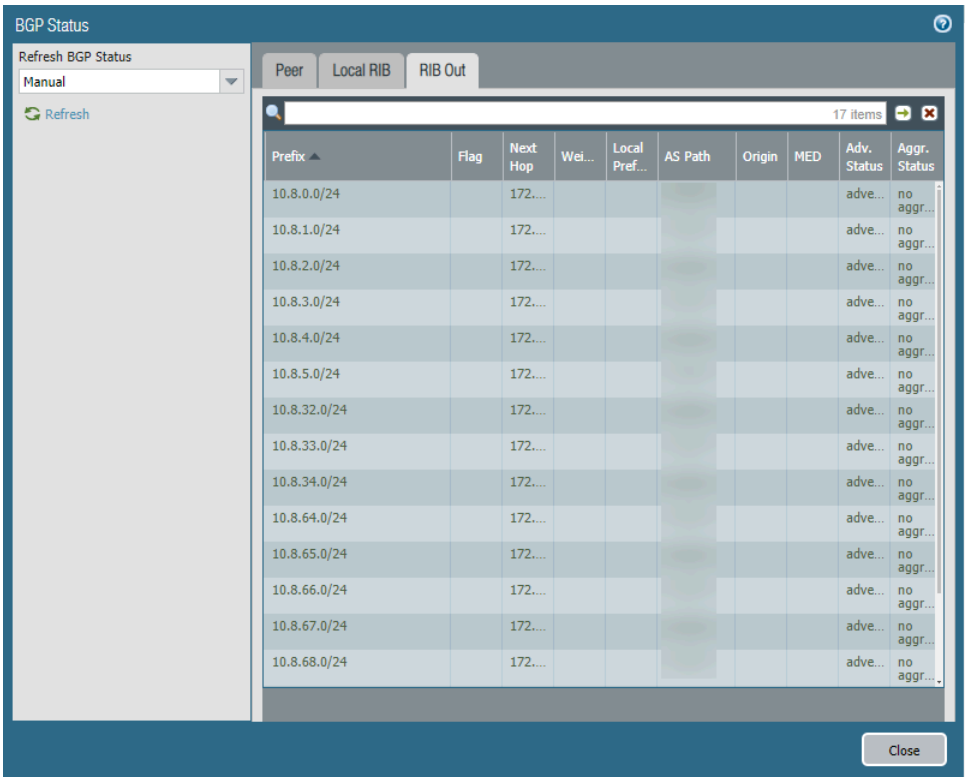
如果您為服務連線或遠端網路連線啟用 BGP，則在 設定 GlobalProtect 行動使用者 (Panorama) 之後，Prisma Access 會使用 C 類 (/24) 位址區塊指派您已指定的行動使用者 IP 位址集區。因此，BGP 會以 /24 區塊的形式公告已配置的行動使用者子網路，而不是與該區域相關聯的整個集區。當 Prisma Access 為 Prisma Access 鬧道新增 /24 子網路時，它會自動傳送 BGP 公告。隨著子網路的新增和刪除，Prisma Access 自動更新其 BGP 公告。此配置方法會在公告 BGP 路由時提供更多的彈性，特別是如果您設定了 **Worldwide**（全球）集區，而不是根據區域配置集區。將 IP 位址池劃分為更小的子網路，允許新增、移除或刪除相同的子網路，然後在配置的位址空間耗盡時於不同的區域中重複使用。

以下螢幕擷取畫面（來自 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Mobile Users**—**GlobalProtect**（行動使用者—**GlobalProtect**）為依區域劃分的行動使用者顯示了三個 /20 IP 集區。




**RIB Out**（**RIB** 輸出）表格（來自 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Service Connection**（服務連線） > **Show BGP Status**（顯示 **BGP** 狀態）（在 **Branch AS and Router**（分支 **AS** 和路由器）區域中））顯示了劃分為 /24 子網路區塊的行動使用者位址集區，用於 BGP 路由公告。請注意，不會公告整個 /20 子網路。


©2025 Palo Alto Networks, Inc.




 ©2025 Palo Alto Networks, Inc.

# Prisma Access 和 Strata Logging Service 的 Proxy 支援

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Panorama | • Prisma Access 授權 |

如果您在 Panorama、Prisma Access 基礎結構和 Strata Logging Service 之間部署 Proxy 伺服器，請參閱下表，以取得預期行為的詳細資訊：

| 功能 | 透過不執行 **SSL** 解密的 **Proxy** 伺服器支援 | 透過執行 **SSL** 解密的 **Proxy** 伺服器支援 |
| --- | --- | --- |
| 初始裝載至 **Strata Logging Service**，使用 **OCSP** 進行憑證撤銷狀態檢查 | 支援 | 僅支援通過 Proxy；不支援任何使用 SSL 解密的 Proxy。 |
| 對 **Strata Logging Service** 進行 **Panorama** 查詢，以取得報告和日誌 | 如果 Proxy 伺服器是 Panorama 上的預設路由，則您無法在 ACC 和 **Monitor**（監控） > **Logs**（日誌）頁面上檢視資料。<br>如果 Panorama 有通往 Strata Logging Service 的替代路由，並且您可以略過 Proxy 伺服器，則您可以在 **Monitor**（監控） > **Logs**（日誌）頁面上檢視資料。 | |


©2025 Palo Alto Networks, Inc.

# 封鎖從特定國家/地區傳入的連線

Prisma Access 可讓您建立安全性政策規則，以封鎖從您指定的國家/地區進行遠端網路、行動使用者—GlobalProtect 和行動使用者—明確 Proxy 部署的登入嘗試。Prisma Access 根據來自用戶端來源 IP 位址的地理位置資訊，封鎖從您指定的國家/地區傳入的連線。

若要封鎖從這些國家/地區傳入的連線，請完成以下工作。

**STEP 1 |** 使用其中一個特定規則名稱建立安全性政策前置規則：

確保您將此規則設定為前置規則。

- 若要封鎖國家/地區進行行動使用者—GlobalProtect 部署，請建立一個名為 **Mobile_User_EMBG_Source_Countries** 的規則。
- 若要封鎖國家/地區進行行動使用者—明確 Proxy 部署，請建立一個名為 **Explicit_Proxy_EMBG_Source_Countries** 的規則。
- 若要封鎖國家/地區進行遠端網路部署，請建立一個名為 **Remote_Network_EMBG_Source_Countries** 的規則。.

**STEP 2 |** 為名稱為 **PA_predefined_embargo_rule** 的規則新增 **Tag**（標籤）。

**STEP 3 |** 在 **Source**（來源）中新增一或多個要封鎖的國家/地區。

**STEP 4 |** 將 **Action**（動作）指定為 **Drop**（丟棄）。


©2025 Palo Alto Networks, Inc.

# 保護來自 AWS WorkSpace 的網際網路流量

組織需要重新思考其方法，以保護透過 Amazon WorkSpace 雲端型虛擬機器存取網際網路的遠端工作人員、承包商、醫院員工和呼叫中心使用者。這些使用者需要能夠安全地存取網際網路，並仍受到保護免於網際網路型威脅，同時組織能夠完全掌握透過這些雲端託管虛擬機器產生的網際網路流量。

在勞動力、資料和雲端應用程式越來越分散的現今複雜和創新經濟中，為遠端工作者和資源設計的傳統網路模式已不堪使用。組織需要雲端服務的彈性和可擴展性，但這些服務需要專為滿足其獨特需求而設計的雲端安全性解決方案。

進一步了解 PRISMA SASE 和 AWS WorkSpace，

使用 Palo Alto Networks Strata Cloud Manager，您可以使用下列方法為 AWS WorkSpace 提供安全的網際網路存取：

- 在 AWS WorkSpace 用戶端上設定 PAC 檔案
- 在 AWS 與 Prisma Access 之間設定站台對站台通道

## 在 AWS WorkSpace 用戶端上設定 PAC 檔案

保護 Amazon WorkSpaces 網際網路流量的一種方法，就是使用 Proxy 自動設定 (PAC) 檔案。PAC 檔案是 JavaScript 程式碼，告訴 Web 瀏覽器如何連線到 Proxy 伺服器。企業環境會採用 PAC 檔案，控制 Web 流量並強制執行安全性政策規則。Web 伺服器通常儲存 PAC 檔案，而 Web 瀏覽器會在啟動時下載 PAC 檔案。

**STEP 1 |** 如果您尚未這樣做，請設定 Prisma SASE 明確 Proxy。

您可以在 Prisma SASE 或 Web 伺服器中託管 PAC 檔案。透過使用 Web 瀏覽器存取 PAC URL，驗證是否可從 WorkSpace 連線 PAC 伺服器。

**STEP 2 |** 自訂 Prisma SASE 明確 Proxy PAC 檔案，以更新 Proxy FQDN 並定義排除項目。

1. 從 Strata Cloud Manager 中，選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Explicit Proxy**（明確 **Proxy**） > **Forwarding Rules**（轉送規則）。
2. 根據 PAC 檔案指導方針編輯 PAC 檔案。

**STEP 3 |** 下載 Prisma SASE 明確 Proxy 根憑證以安裝在 AWS WorkSpace 上。

**STEP 4 |** 在 AWS WorkSpace 用戶端上安裝憑證，以套用使用者型政策規則、流量檢查和報告。

這將允許 WorkSpace 用戶端與 Prisma SASE 明確 Proxy 通訊。

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** 在 AWS WorkSpace 上設定 PAC 檔案。

您執行此動作的方式取決於您使用的瀏覽器。

- Google Chrome：
  1. 開啟 Chrome。
  2. 選取視窗右上角的三個點。
  3. 選取 **Settings**（設定）。
  4. 選取 **Advanced**（進階）。
  5. 在 **System**（系統）下，選取 **Open proxy settings**（開啟 **Proxy** 設定）。
  6. 在 [Local Area Network (LAN) Settings（區域網路 (LAN) 設定）] 視窗中，選取 **Use automatic configuration script**（使用自動設定指令碼）。
  7. 在 **Address**（位址）欄位中，輸入 PAC 檔案的 URL。
  8. 選取 **OK**（確定）來儲存您的變更。
- Firefox
  1. 開啟 Firefox。
  2. 選取視窗右上角的三條線。
  3. 選取 **Options**（選項）。
  4. 選取 **Advanced**（進階）。
  5. 在 **Network**（網路）中選取 **Settings**（設定）。
  6. 在 **Connection Settings**（連線設定）視窗中，選取 **Automatic proxy configuration URL**（自動 **Proxy** 設定 **URL**）。
  7. 在 **URL** 欄位中，輸入 PAC 檔案的 URL。
  8. 然後，選取 **OK**（確定）來儲存您的變更。

當您已套用 PAC 檔案時，Chrome 和 Firefox 將使用它，確定每個網站使用哪個 Proxy 伺服器。

**STEP 6 |** 重新啟動 AWS WorkSpace 瀏覽器。

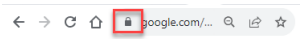
在 WorkSpace 瀏覽器重新啟動之後，它將挑選新的 PAC 檔案，並開始透過 Prisma SASE Proxy 路由流量。

 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** 測試並驗證流量流向。

一旦已將 WorkSpace 用戶端設定為使用 Prisma SASE 明確 Proxy，您就可以透過在瀏覽器中驗證憑證，並在 Prisma Access 上檢視日誌來測試流量流向。

1. 如果使用 Google Chrome，請選取位址列中的掛鎖。




   1. 選取 **Connection is secure**（連線是安全的）。
   2. 選取 **Certificate is valid**（憑證有效）。
   3. 驗證快顯視窗中出現的憑證詳細資訊是否正確。
2. 如果使用 Safari，請選取位址列中的掛鎖圖示。
   1. 選取 **Connection secure**（連線安全）。
   2. 選取 **More information**（詳細資訊）。
   3. 選取 **View Certificate**（檢視憑證）。
   4. 驗證快顯視窗中出現的憑證詳細資訊是否正確。

# 在 AWS 與 Prisma Access 之間設定站台對站台通道

隨著您的業務擴展，並且您有多個 AWS WorkSpace 用戶端執行中，Prisma Access 遠端網路可讓您快速裝載 WorkSpace，並為使用者提供最佳的安全性。它提供了一個方便的選項，可以簡化 WorkSpace 的設定和管理。

組織可以透過在 AWS 與 Prisma Access 之間建立 IPSec 通道，將 AWS WorkSpace 使用者裝載至 Prisma Access。

使用遠端網路的好處是，它可以保護輸出網際網路流量，讓透過 Prisma Access 連線的使用者存取網際網路。

**STEP 1 |** 為您的 Amazon WorkSpace 設定虛擬私人雲端 (VPC) 或為您的 Amazon WorkSpace 使用現有的 VPC。

**STEP 2 |** 將 AWS Transit Gateway 連接到 VPC，以在 AWS 與 Prisma Access 之間設定站台對站台 IPSec 通道。

**STEP 3 |** 在 AWS Transit Gateway 與 Prisma Access 遠端網路之間設定 IPSec VPN。

**STEP 4 |** 在 Prisma Access 遠端網路上，您可以定義安全規則來限制網際網路流量，以保護 AWS WorkSpace 使用者。

 ©2025 Palo Alto Networks, Inc.

# Prisma Access 用於無預設路由網路

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access | ❑ Prisma Access 授權 |

## 什麼是無預設路由網路？

無預設路由網路是未設定預設路由的網路。當網路未設定預設路由時，它會丟棄前往未知目的地的封包。企業通常會使用無預設路由網路來限制其使用者的存取。如果無預設路由網路上的裝置需要存取某個目的地（IP 位址或子網路），管理員將需要為該目的地手動設定路由。企業還需要在無預設路由分支網路上為使用者、伺服器和裝置進行受限且安全的網際網路存取。

有人可能想要設定無預設路由網路的原因有幾個：

- 透過封鎖從網路上受感染端點輸出惡意和 DDoS 流量到隨機目的地來提高安全性，從而防範拒絕服務攻擊和其他惡意流量。
- 透過減少要處理的路由數目來提高路由裝置的效能。
- 透過為特定目的地設定特定路由，實作滿足使用者特定需求的路由政策。

## 無預設路由網路考量

當保護來自無預設網路的網際網路流量時，企業必須清楚地評估分支網路中可能與網際網路交談的使用者、端點、伺服器和裝置。

在無預設路由分支中，可能有裝置具有各種不同的操作系統、多重使用者或共用端點（如 VDI），以及無頭裝置（例如伺服器和 IoT 裝置）。來自所有這些裝置的網際網路流量都需要安全性。具有一個涵蓋所有這些使用案例的解決方案至關重要，該解決方案提供搭配不同連線方法的靈活性，並提供統一的平台來始終如一地保護網際網路存取，無論裝置類型為何。

## 保護無預設路由網路進行網際網路存取的部署建議

如果您有無預設路由網路，以下是我們保護網際網路流量的建議：

| 裝置 | 建議 |
| --- | --- |
| Windows、macOS | Proxy 模式下的 GlobalProtect 代理程式 |
| ChromeOS、VDI | 無代理程式 PAC 檔案 |
| iOS、Android | 無代理程式 PAC 檔案 |
| Linux | 無代理程式 PAC 檔案 |
| 伺服器 | 無代理程式 PAC 檔案 |


©2025 Palo Alto Networks, Inc.

| | |
|---|---|
| IoT 裝置（Proxy 感知） | 無代理程式 PAC 檔案 |
| IoT 裝置（Proxy 未感知） | 遠端網路 (IPSec) |

## 關鍵考量

在無預設路由網路中部署 GlobalProtect 時，請考慮以下幾點：

- 在周邊裝置上新增路由，以將使用者的網際網路流量路由到 Prisma Access 明確 Proxy IP 位址。
- 在內部託管 PAC 檔案，將 IdP URL 和 Prisma Access 入口網站 URL 轉送到明確 Proxy，以允許 GlobalProtect 連線到入口網站和 IdP。
- 新增內部 DNS 記錄以解析明確 Proxy、PAC 檔案和 Prisma Access 入口網站 FQDN（如果無預設路由網路中的 DNS 伺服器無法解析外部 FQDN）。
- 將內部 Prisma Access 明確 Proxy IP 位址和 Prisma Access 入口網站 IP 位址的 DNAT 設定為真正的明確 Proxy IP 位址和入口網站 IP 位址。

對於 *PAC* 型部署，無需將 *Prisma Access* 入口網站 *URL* 轉送到明確 *Proxy*，並將其從 *Prisma Access* 明確 *Proxy* 設定中的驗證設定中排除。


©2025 Palo Alto Networks, Inc.

# Prisma Access 服務連線進階部署

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Panorama | • Prisma Access 授權 |

以下幾節為您展示適用於 Prisma Access 服務連線的進階部署：

- 服務連線多重雲端備援
- 使用流量導向將網際網路繫結流量轉送到服務連線
- 服務連線流量的路由
- 使用多個服務連線建立高頻寬網路

## 服務連線多重雲端備援

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

從 *Prisma Access 3.1 Innovation* 開始，支援服務連線多重雲端備援。

如果你使用 Prisma Access 服務連線，為行動使用者和遠端網站中的使用者提供對總部或資料中心內部資源和應用程式的存取，您可以在不同的雲端提供者中建立作用中和備份服務連線，來確保對這些資源的存取更有彈性。您可以在同一位置或在不同地理區域的不同位置中指定這些作用中和備份服務連線，這樣即使雲端提供者或區域變成不可用，也可讓您透過服務連線存取資源。

您可以在網站中指定作用中和備份服務連線。網站是一個或多個服務連線終止所在的客戶資料中心或總部位置（內部部署或在公有雲端中）。在建立服務連線之後，您可以建立一個網站、將服務連線新增至該網站，然後將您新增的服務連線指定為作用中或備份。

如果雲端提供者或區域停電導致網站中的作用中服務連線中斷，Prisma Access 會使用這些規則重新路由流量，讓您的行動使用者繼續存取該總部或資料中心的資源：

- 如果網站中有一個單一作用中服務連線，Prisma Access 會在該網站中選取備份服務連線來路由流量。
- 如果網站中有多個作用中服務連線，Prisma Access 會選取另一個作用中服務連線來路由流量，而且備份服務連線僅用來在所有作用中服務連線中斷時路由流量。

若要利用在同一國家/地區使用作用中和備份位置的網站，您可以使用國內偏好位置和替代位置裝載服務連線，然後建立網站並將這些國內位置新增至該網站。

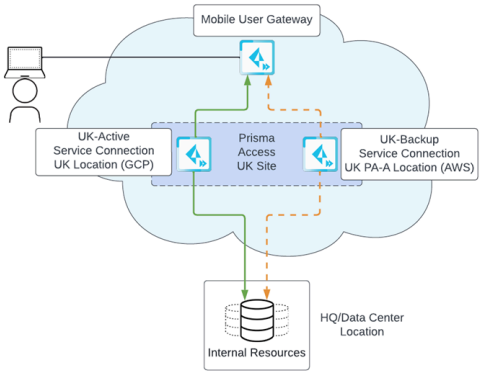
Prisma Access 也為您提供有關您在網站中所裝載服務連線的狀態訊息（例如，如果網站中的所有服務連線都部署在單一區域中）。

以下範例展示如何善加建立網站並將服務連線新增至其中：

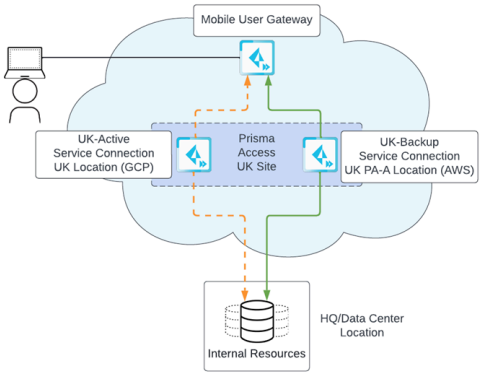

©2025 Palo Alto Networks, Inc.

- 同一地理區域中的不同雲端提供者—如果您是需要在特定國家/地區存取您資料的組織（例如銀行），則可以從該國家/地區選取偏好位置，並從同一國家/地區選取替代位置。以下範例展示英國的一個組織如何在英國裝載其服務連線，以遵得資料位置法規。在此情況下，組織的管理員在英國裝載兩個服務連接，即英國位置中的 UK-Active 和英國 PA-A 位置中的 UK-Backup。英國位置是由英國中的偏好雲端提供者 (GCP) 託管，而英國 PA-A 位置是由該國家/地區中的替代雲端提供者 (AWS) 託管。國內位置清單顯示一個國家的偏好和替代雲端提供者。然後，管理員會建立一個網站，並指定 UK-Active 作為該網站中的作用中位置，以及指定 UK-Backup 作為該網站中的備份位置。

  在正常操作期間，行動使用者會使用 UK-Active 服務連線存取總部或資料中心的內部資源。




  如果 GCP 中斷影響了 UK-Active 服務連線，Prisma Access 會容錯移轉到 AWS 上託管的 UK-Backup 服務連線。這樣，即使在雲端提供者中斷的情況下，Prisma Access 仍允許行動使用者存取資料中心或總部的資源。下圖顯示流量流向。

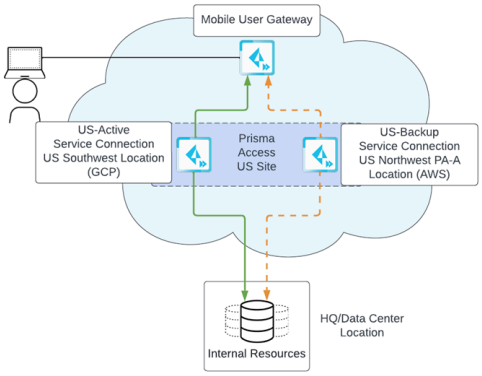



- 不同的地理區域—如果您想要在發生區域中斷時確保備援，則可以在不同的計算位置以及不同的雲端提供者中指定兩個或多個服務連線，從而在某個地理區域發生中斷時為您提供備份存取。在下圖中，管理員已從美國中的位置（美國西南部位置中的 US-Active 和美國西北部 PA-A

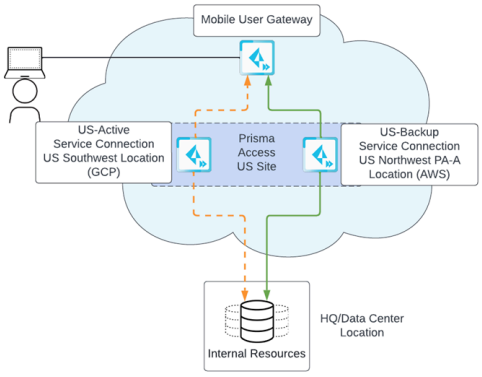
 ©2025 Palo Alto Networks, Inc.

位置中的 US-Backup）裝載服務連線，並建立了一個網站，使 US-Active 成為網站中的作用中服務連線，以及使 US-Backup 成為備份服務連線。

由於您已裝載位於不同計算位置以及不同雲端提供者的服務連線，因此您已設定一個為您同時提供地理和雲端提供者備援的網站。




如果 US-Active 位置失效（因為雲端提供者或區域中斷），服務連線會容錯移轉至 US-Backup 位置，該位置使用與 US-Active 服務連線不同的雲端提供者和計算位置，如下圖所示。

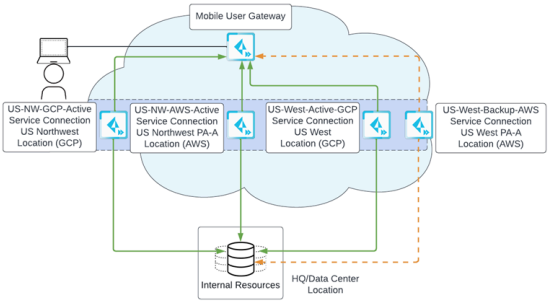




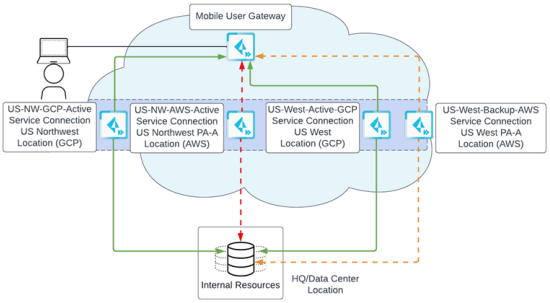
©2025 Palo Alto Networks, Inc.

- 使用多個服務連接的高頻寬連線—如果需要更高頻寬的內部資源連線，您可以建立一個具有多個作用中連線的網站。下圖顯示了四個正在裝載的網站，其中混合使用了 GCP 和 AWS 雲端提供者：
  - US-NW-GCP-Active，使用美國西北部 (GCP) 位置
  - US-NW-AWS-Active，使用美國西北部 PA-A (AWS) 位置
  - US-West-Active-GCP，使用美國西部 (GCP) 位置
  - US-West-Backup-AWS，使用美國西部 PA-A (AWS) 位置

  在網站中，其中三個服務連線被指定為作用中服務連線，第四個服務連線則被指定為備份。與單一服務連線相比，將三個服務連線指定為作用中連線可以有效地為您的內部資源提供三倍頻寬。



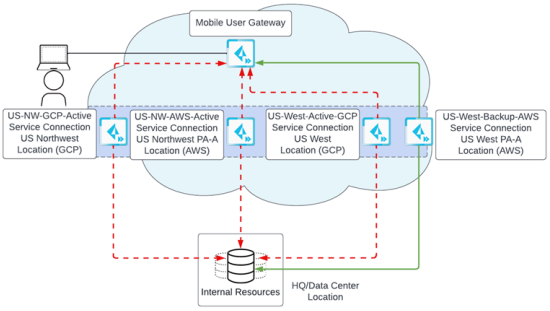

  如果其中一個作用中服務連線失效，則備份連線不會投入使用；反而，Prisma Access 會將流量轉移到剩餘的作用中服務連線，如下圖所示。




  如果所有作用中服務連線都失效，則備份服務連線會投入使用並成為作用中連線。

  如果將多個服務連線設定為備份服務連線，*Prisma Access* 會將所有備份服務連線投入使用，且負載會共用服務連線流量。


©2025 Palo Alto Networks, Inc.




設定備援雲端提供者服務連線時，請使用以下指導方針：

- 您可以使用網站中的偏好或替代位置來新增服務連線。

  Palo Alto Networks 高度建議您使用偏好的雲端提供者作為網站中的作用中服務連線。
- 網站中的所有服務連線都必須指向同一總部或資料中心位置的相同資源。您在網站中不能具有指向不同位置中不同資源的服務連線。
- 您必須在網站中選取至少一個作用中服務連線；不過，您也可以在單一網站中具有多個作用中服務連線。以下網站設定有效：
  - 美國中部（作用中）
  - 美國中部 PA-A（備份）
  - 美國東部（作用中）
  - 美國東部 PA-A（備份）
- 如果您在網站中有多個作用中服務連線，並且有一個作用中服務連線失效，則流量會轉移到另一個作用中服務連線（亦即，只要其中一個作用中服務連線處於啟動狀態，就不會使用備份服務連線）。
- 對於靜態和動態服務連線路由，請使用下列指導方針：
  - 如果您使用靜態路由進行服務連線，請確保您為服務連線指定的子網路指向相同的子網路。

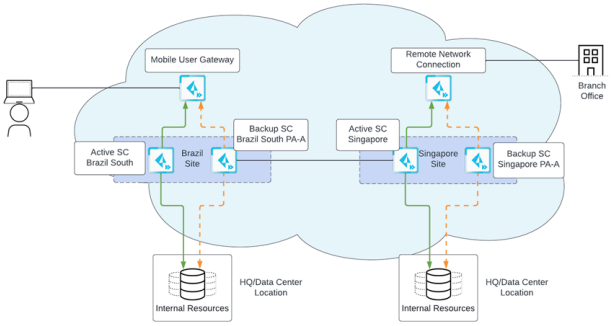
    例如，如果您有一個網站使用 192.168.41.0/24、192.168.44.0/24 和 192.168.47.0/24 作為作用中服務連線的子網路，請確保為備份服務連線指定相同的子網路。
  - 如果您使用動態 (BGP) 路由進行服務連線，請確保所有服務連線將相同的首碼公告至相同的資料中心或總部。
- Prisma Access 使用 BGP 多出口鑑別器 (MED) 值，來區分網站中的作用中和備份服務連線，如下表所示。請注意，作用中服務連線的 MED 值會視您是否已為作用中服務連線啟用次要 IPSec 通道而變更。Prisma Access 會將這些 MED 值公告至 CPE（BGP 對等）。

| 連線類型 | MED 值 |
|---|---|
| 網站中的作用中 **IPSec** 服務連線 | |
| 作用中服務連線，未設定次要 IPSec 通道 | 0 |

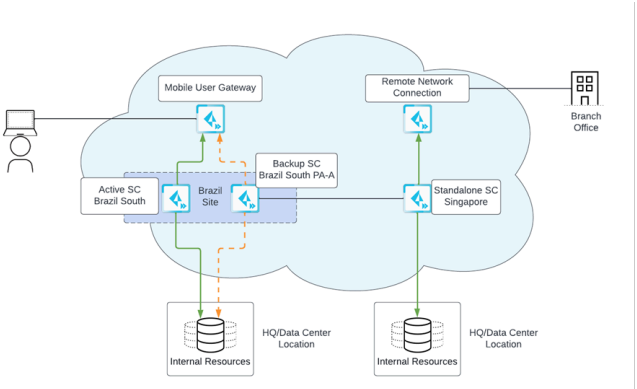

©2025 Palo Alto Networks, Inc.

| 連線類型 | MED 值 |
| --- | --- |
| 作用中服務連線、已設定次要 IPSec 通道、主要通道 | 100 |
| 作用中服務連線、已設定次要 IPSec 通道、次要通道 | 200 |
| 網站中的備份 **IPSec** 服務連線 | |
| 備份服務連線、主要通道（無論是否已設定次要 IPSec 通道） | 500 |
| 備份服務連線、已設定次要 IPSec 通道、次要通道 | 600 |

- 您可以在單一 Prisma Access 部署中新增多個網站，如下圖所示。




- 您仍然可以使用單一的獨立服務連線來存取內部資源。您也可以將獨立服務連線與作用中和備份服務連線混合，如下圖所示。




- 使用熱馬鈴薯路由路由進行服務連線時，不支援服務連線多重雲端備援。
- 請勿使用 CLI 裝載和設定服務連線。如果您需要使用 CLI 來裝載服務連線，請聯繫您的 Palo Alto Networks 團隊。


©2025 Palo Alto Networks, Inc.

# 設定和啟動服務連線雲端提供者備援

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

若要為雲端服務提供者設定多個服務連線，請完成以下步驟。

**STEP 1 |** （僅限現有 Prisma Access 部署）如果您已將外掛程式升級到支援雲端提供者備援的版本，請在升級到支援的外掛程式之後執行 **Commit and Push**（提交並推送）作業。

從 Prisma Access 3.1 Preferred 和 Innovation 開始支援服務連線多雲端備援。在您升級雲端服務外掛程式之後，必須執行 **Commit and Push**（提交並推送），以使雲端備援變更出現在 UI 中。

如果您有新的部署（不是升級），請跳過此步驟。


©2025 Palo Alto Networks, Inc.

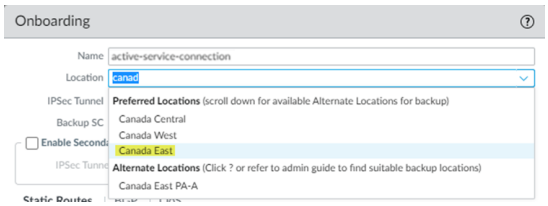
**STEP 2 |** 建立服務連線，用作網站中的作用中和備份服務連線。

在建立慣用和替代位置，且提交並推送您的變更之後，您無法更改這些位置。例如，您無法將慣用位置從加拿大東部變更為加拿大東部 *PA-A*，也無法將替代位置從加拿大東部 *PA-A* 變更為加拿大東部。

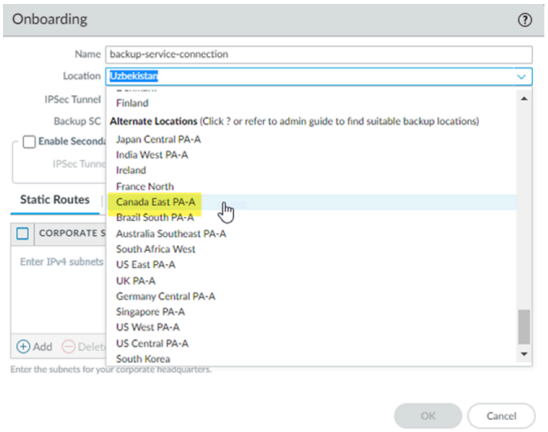
1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Connection**（服務連線）。
2. **Add**（新增）一個服務連線，您會將其指定為網站中的作用中服務連線。

   從慣用或替代位置清單中選取。

   若要搜尋位置，請開始輸入 ***Location***（位置）名稱。




3. **Add**（新增）一個服務連線，您會將其指定為網站中的備份服務連線。



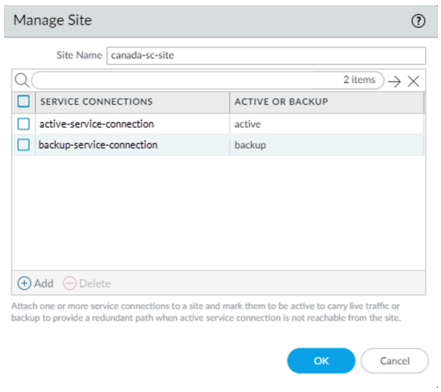

4. （選用）視需要繼續裝載要指定為作用中和備份網站的服務連線。


©2025 Palo Alto Networks, Inc.

**STEP 3 |** 建立一個網站；然後，將您已新增的服務連線指定為網站中的作用中或備份服務連線。

1. 在 **Manage Sites**（管理網站）中，**Add**（新增）一個網站。
2. **Add**（新增）您已裝載的服務連線。
3. 將您已新增的服務位置指定為網站中的 **active**（作用中）和 **backup**（備分）。

   您可以建立多個作用中和備份網站。請指定至少一個網站作為作用中網站。
4. 按一下 **OK**（確定）。
5. （選用）視需要繼續為您的作用中和備份服務連線新增網站。




**STEP 4 |** **Commit and Push**（提交並推送）您的變更。

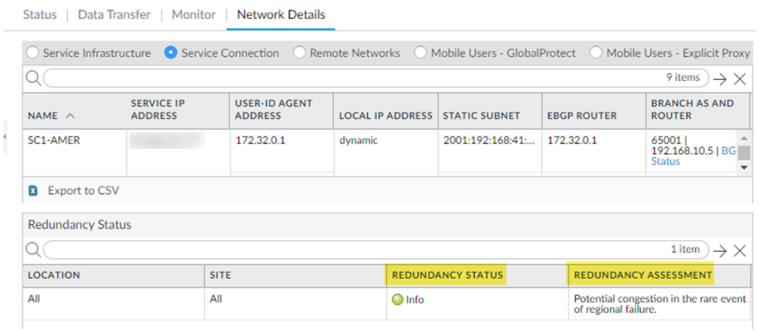
**STEP 5 |** 檢查您網站的狀態。

1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Service Connection**（服務連線） > **Redundancy Status**（備援狀態）。
2. 檢查 **Redundancy Status**（備援狀態）和 **Redundancy Assessment**（備援評估）欄位中的資訊。備援狀態為您提供所部署網站的狀態，而備援評估則為您提供更多有關網站中已部署服務連線的詳細資訊。

| 備援狀態 | 備援評估 |
|---|---|
| 資訊 | 若發生區域故障，您的服務連線可能會遇到擁塞。 |
| 警告 | 所有服務連線都部署在單一區域中。請考慮在附近位置部署。<br>此訊息通知您，您的所有服務連線都部署在單一區域中。 |
| 注意 | 所有連線至網站的服務連線都部署在單一區域中。請考慮在附近位置部署。 |


©2025 Palo Alto Networks, Inc.

| 備援狀態 | 備援評估 |
| --- | --- |
| | 此訊息通知您，所有連線至網站的服務連線都部署在單一區域中。 |




## 支援的國內作用中和備份雲端提供者備援位置

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Panorama | • Prisma Access 授權 |

如果您想要設定作用中位置和備份位置位於同一國家/地區的部署，請從這個國內偏好和替代位置清單中進行選取。

| 偏好位置 | 替代位置 |
| --- | --- |
| 澳大利亞東南部 | 澳大利亞東南部 PA-A |
| 巴林 PA-A | 巴林 |
| 巴西南部 | 巴西南部 PA-A |
| 加拿大東部 | 加拿大東部 PA-A |
| 法國北部 PA-A | 法國北部 |
| 德國中部 | 德國中部 PA-A |
| 印度西部 | 印度西部 PA-A |
| 愛爾蘭 PA-A | 愛爾蘭 |
| 日本中部 | 日本中部 PA-A |
| 新加坡 | 新加坡 PA-A |
| 南非西部 PA-A | 南非西部 |


©2025 Palo Alto Networks, Inc.

| 偏好位置 | 替代位置 |
| --- | --- |
| 韓國 PA-A | 韓國 |
| 英國 | 英國 PA-A |
| 阿拉伯聯合大公國 PA-A | 阿拉伯聯合大陸 |
| 美國中部 | 美國中部 PA-A |
| 美國東部 | 美國東部 PA-A |
| 美國西北部 | 美國西北部 PA-A |
| 美國西部 | 美國西部 PA-A |

# 使用流量導向將網際網路繫結流量轉送到服務連線

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ 若要將憑證撤銷清單 (CRL) 和線上憑證狀態通訊協定 (OCSP) 直接傳送至網際網路，所需的最低 Prisma Access 版本為 5.1.1。 |

Prisma Access 允許您建立流量導向規則，為來自行動使用者和遠端網路連線的網際網路繫結流量指定目標。您可以指定要重新導向至服務連線的流量，然後再將該流量傳送至網際網路，也可以指定要直接輸出至網際網路的流量。此功能稱為流量導向。

或者，您可以設定 Prisma Access 以接受從 CPE 到 Prisma Access 的預設路由，以便 Prisma Access 將網際網路繫結的行動使用者流量轉送到部署中的最佳服務連線。

## 預設路由搭配 Prisma Access 流量導向

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

使用 Prisma Access 中的預設路由功能，接受從 CPE 公告至服務連線的預設路由。您可以使用 BGP 或靜態路由來公告預設路由。Prisma Access 使用 BGP 透過多個服務連線公告這些路由，這允許 Prisma Access 透過給定行動使用者位置的最佳服務連線路由行動使用者流量。若要啟用服務連線接受預設路由，請在 在 Prisma Access 中設定流量導向 時指定 **Accept Default Route over Service Connections**（接受透過服務連線的預設路由）。


©2025 Palo Alto Networks, Inc.

在啟用預設路由之後，您的網際網路繫結流量將被導向至服務連線，而不是從行動使用者位置輸出。如果您想將網際網路繫結流量重新導向至資料中心，此功能會很有用；例如，如果您的資料中心有第三方安全性堆疊，並且您想要該堆疊執行額外的篩選或檢查。

實作預設路由時請使用以下指導方針：

- 預設路由僅適用於行動使用者部署；啟用預設路由時，遠端網路連線運作正常，沒有任何變更。
- 當您允許預設路由時，無需指定目標服務連線或流量導向規則，儘管支援它們與預設路由搭配使用。
- 當您指定 **Accept Default Route over Service Connections**（接受透過服務連線的預設路由）設定時，所有 Prisma Access 服務連線（專用服務連線除外）都接受預設路由，並將在流量導向決策中使用這些路由。
- 在啟用此設定之前，請確保您的資料中心正在傳送預設路由；否則，透過服務連線進行路由將會失敗。
- Palo Alto Networks 建議所有資料中心公告預設路由；當 Prisma Access 接收路由時，它接著可以選取要用於遠端網路位置的最佳服務連線。
- 當您設定服務連線時，僅使用靜態路由或僅使用 BGP 進行連線。Palo Alto Networks 不建議在使用預設路由時將使用 BGP 和靜態路由的服務連線混合。
- （僅限 Prisma Access (Managed by Panorama) 部署）支援使用預設路由搭配多租用戶部署。
- Prisma Access 不會使用預設路由將無用戶端 VPN、入口網站或閘道 SAML 驗證流量轉送至公用識別提供者 (IdP)。

如需透過流量導向實作預設路由的詳細資訊和範例，請參閱 預設路由搭配流量導向範例、預設路由搭配流量導向直接至網際網路範例 和 具有流量導向和專用服務連線的預設路由範例。

## Prisma Access 中的流量導向

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

在標準 Prisma Access 部署中，服務連線會提供對內部網路資源的存取，例如總部或資料中心的驗證服務和私人應用程式。服務連線會處理內部流量，其中不需要網際網路存取。在某些情況下，您可能想要將網際網路繫結流量重新導向到資料中心。流量轉向允許您在將行動使用者或遠端網路流量傳送到網際網路之前將其重新導向到服務連線。

您可以使用流量導向搭配行動使用者部署、遠端網路部署或兩者的組合。使用流量導向，根據多種準則（包括 IP 位址、使用者、URL、自訂 URL 類別、服務類型（HTTP 或 HTTPS）、User-ID、動態位址群組 (DAG)、動態使用者群組 (DUG)和 IP 型外部動態清單 (EDL) 來引導網際網路繫結網路流量。

有兩種流量導向支援的動作類型：

 ©2025 Palo Alto Networks, Inc.

- **Forward to the target**（轉送到目標）—使用流量導向規則中的準則，透過您建立的目標，其中使用一個或多個服務連線，轉送網際網路繫結流量。
- **Forward to the internet**（轉送到網際網路）—使用流量導向規則中的準則，直接將流量從其來源（行動使用者位置或遠端網路連線）轉送到網際網路，而無需轉送至服務連線。

如果轉送到目標，您可以選擇建立兩種類型的目標群組：專用和非專用。

- 僅用於流量導向相關流量的服務連線稱為專用服務連線。若要設定服務連線，以用作專用服務連線，請在您於 Panorama 中在 Prisma Access 中設定流量導向時，選取 **Dedicated for Traffic Steering Only**（僅專用於流量導向）。在 Strata Cloud Manager 中設定流量導向規則時，請選取 **Dedicated for PBF Only**（僅專用於 **PBF**）。

  如果您使用位於您組織內部網路之外的第三方安全性堆疊來處理流量，然後再將其傳送到公用 SaaS 應用程式或網際網路，您可能需要設定專用的服務連接。因為安全性堆疊不是您組織網路的一部分，所以您不想要此服務連線處理任何內部網路流量。
- 用於流量導向和標準服務連線相關流量（例如，前往資料中心驗證伺服器的流量）的服務連線是非專用服務連線。

將服務連線設定為專用服務連線會導致您的部署進行以下變更：

- （僅限 Prisma Access (Managed by Strata Cloud Manager) 部署）服務連線會將來源 NAT 套用至轉送的流量。來源 IP 位址是服務連線的 **EBGP Router**（**EBGP** 路由器）位址，該位址取自基礎結構子網路。
- 與此目標相關聯的所有服務連線的區域會從信任變更為不信任。檢查您的區域對應和 設定區域對應和安全性政策以進行流量導向專用連線，以確保您的網路反映此變更。
- 設定為專用服務連線的服務連線不參與內部或外部的 BGP 路由。
- （僅限 Prisma Access (Managed by Panorama) 部署）如果您的專用服務連線使用 BGP，則在您開啟狀態頁面（**Panorama** > **Cloud Service**（雲端服務） > **Status**（狀態） > **Monitor**（監控） > **Service Connection**（服務連線））、選取一個區域，然後選取 [Status（狀態）] 頁籤時，BGP 狀態顯示為 **Not Enabled**（未啟用）。若要檢查服務連線的 BGP 狀態，請檢查服務連線設定頁面（**Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Connection**（服務連線））。
- （僅限 Prisma Access (Managed by Panorama) 部署）根據預設，服務連線會將來源 NAT 套用至轉送的流量。來源 IP 位址是服務連線的 **User-ID Agent Address**（**User-ID** 代理程式位址）（**Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Service Connection**（服務連線） > **User-ID Agent Address**（**User-ID** 代理程式位址）），該位址取自基礎結構子網路（**Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Service Infrastructure**（服務基礎結構））。

  （僅限 Prisma Access (Managed by Panorama) 部署）您可以停用來源 NAT，並使用您組織的來源 IP 位址進行專用服務連線；若要這樣做，請在 **Target Service Connections for Traffic Steering**（流量導向的目標服務連線）區域中 **Add**（新增）目標時，選取 **Disable Source NAT for Dedicated SC**（停用專用 **SC** 的來源 **NAT**）。


©2025 Palo Alto Networks, Inc.

# 流量導向需求

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

在您的 Prisma Access 部署中實作流量導向之前，請確保您的網路環境具有以下基礎結構需求：

- Prisma Access 必須能夠連線到支援 IPSec 的 CPE（例如路由器或 SD-WAN 裝置），而您的組織將其用來終止服務連線，並且裝置的 IP 位址必須可以從 Prisma Access 連線。

  您可以在堆疊位置與 Prisma Access 之間使用標準 IPSec 和 IKE 密碼設定檔建立服務連線。設定服務連線並使用流量導向時，您可以使用靜態路由、BGP 或結合兩者使用。如果您使用預設路由搭配流量導向，Palo Alto Networks 建議您僅使用 BGP 或僅使用靜態路由。如果您使用靜態路由，請在建立 IKE 閘道時，將組織 CPE 使用的公用 IP 位址指定為 **Peer Address**（對等位址）。
- Prisma Access 可能與來自流量導向規則中 URL 類別的 URL 前幾個封包不符，這意味著網路工作階段的前幾個封包（例如，TCP 交握）可能與規則不符。Palo Alto Networks 建議，對於您在流量導定規則中使用的 URL，建立一個安全性政策規則以允許它們通過不信任區域，以便在新工作階段開始時交握可以完成。
- 如果您是使用此設定搭配安全性堆疊，則必須可以透過標準 IPSec 通道設定從服務連線中連線至堆疊位置。

設定流量導向時請使用以下指導方針：

- 您可以在流量導向設定中指定最多 1000 個 URL（已彙總），包括自訂 URL 類別中的常規和萬用字元 (*.example.com) URL。

  此數目包括手動輸入的 URL、萬用字元 URL，以及在自訂 URL 類別中輸入的 URL。
- 如果您在流量導向規則中使用自訂 URL 類別，則 Prisma Access 會在這些類別中將星號加在 URL 前面。如果對流量導向規則和其他安全性政策規則使用相同的 URL 類別政策，則這些變更將同時套用至流量導向規則和其他安全性政策規則。

  如果您有未在流量導向規則中使用的自訂 URL 類別， Prisma Access 不會變更這些類別中的 URL。
- 在流量轉送規則中輸入 URL 時，以及在自訂 URL 類別中新增 URL 時，請使用全小寫的 URL。
- 您最多可以設定 100 個流量轉送規則。
- 如果您設定了主要和備份通道，則在從主要（作用中）通道容錯移轉至備份通道之後，使用流量導向規則的流量導向將無法運作。預設路由搭配 Prisma Access 流量導向 可在具有主要和備份通道的容錯移轉案例中運作。


©2025 Palo Alto Networks, Inc.

# 預設路由搭配流量導向範例

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

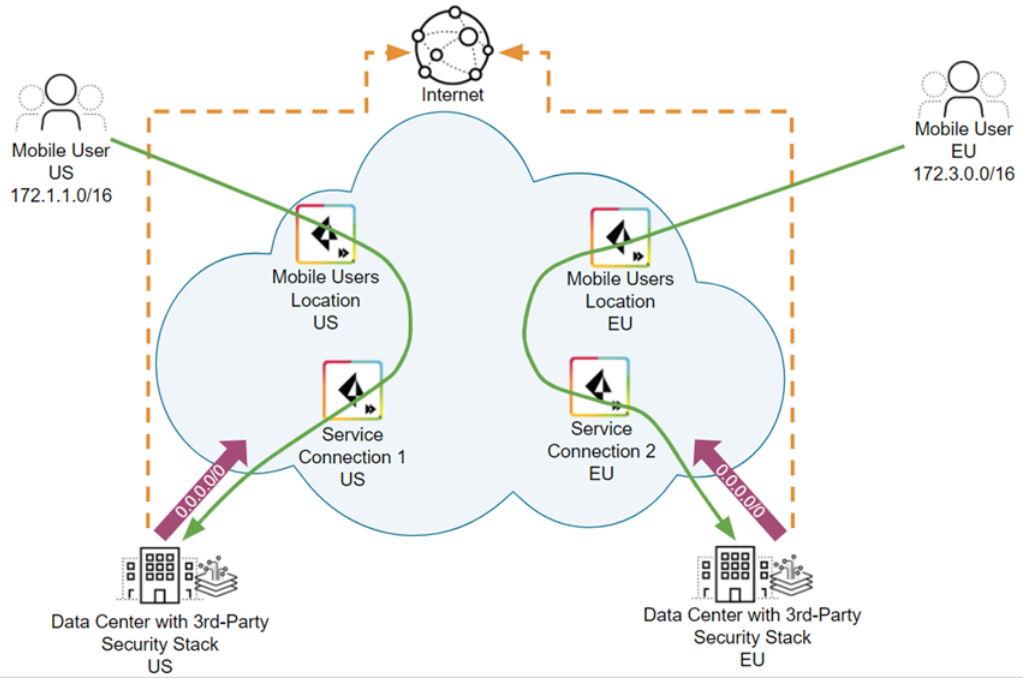
以下範例顯示了一個範例 Prisma Access 部署，元件如下：

- 二個 Prisma Access 行動使用者位置；一個在美國（US），一個在歐盟（EU）。
- 二個 Prisma Access 服務連線；一個在美國、一個在歐盟，這兩個資料中心將預設路由傳送至服務連線（**Accept Default Route over Service Connections**（接受透過服務連線的預設路由）已啟用）。
- 兩個資料中心；一個在美國，一個在歐盟。

  每個資料中心都有一個第三方安全性堆疊；基於此原因，您想要所有網際網路繫結流量在輸出到網路之前都通過資料中心。

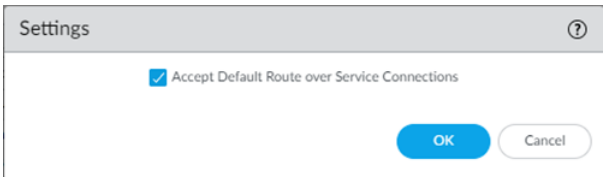
當行動使用者傳送資料中心流量時，Prisma Access 會檢查其路由表，確定最接近的服務連線，並將流量轉送到該服務連線。在下面範例中，Prisma Access 將來自美國行動使用者的資料中心流量傳送到服務連線，並將來自歐盟行動使用者的流量傳送至服務連線 2。

請勿使用 ***Dedicated for Traffic Steering Only***（專用於流量導向）的服務連線搭配預設路由；專用服務連線不參與*BGP*路由，因此無法接收來自總部或資料中心的 *BGP* 公告。




若要啟用預設路由，請在設定流量導向設定時選取 **Accept Default Route over Service Connections**（接受透過服務連線的預設路由）。在進行此設定且提交並推送您的變更之後，Prisma Access 會透過服務連線傳送網際網路繫結流量。

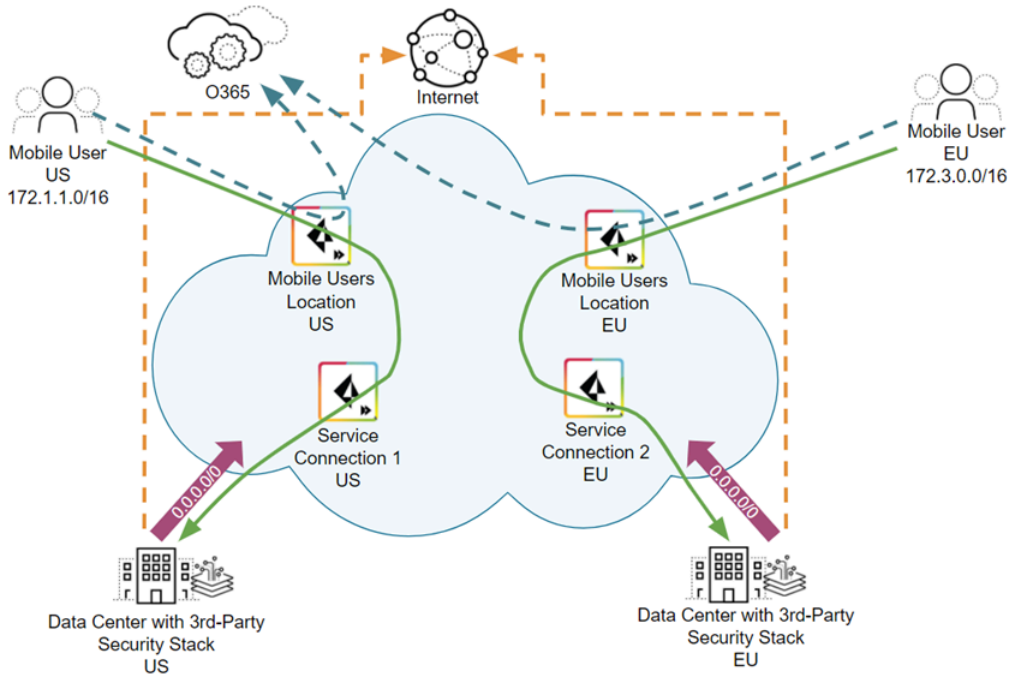

©2025 Palo Alto Networks, Inc.




# 預設路由搭配流量導向直接至網際網路範例

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

以下範例向您展示對外部 SaaS 應用程式繫結流量使用更細微的控制。在此情況下，您想要將 Office 365 流量直接從行動使用者位置輸出至網際網路，而不是將其傳送到資料中心進行進一步處理。對此設定使用流量導向以及預設路由。

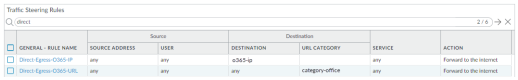



若要允許 Prisma Access 將 Office 365 流量直接路由到網際網路，請執行以下動作：

- 建立一個 EDL（**Object**（物件） > **External Dynamic Lists**（外部動態清單）），其中 IP 位址符合 Office 365 位址。
- 建立一個自訂 URL 類別（**Objects**（物件） > **Custom Objects**（自訂物件） > **URL Category**（**URL** 類別）），其中 URL 符合 Office 365 URL。
- 建立 在 Prisma Access 中設定流量導向 並指定您建立的 EDL 和 URL 類別作為目的地比對規則，**Action**（動作）為 **Forward to the internet**（轉送至網際網路）。

此設定會將 Office 365 流量直接傳送至網際網路，而其他網際網路繫結流量會在輸出至網際網路之前傳送至資料中心，以進行進一步處理。

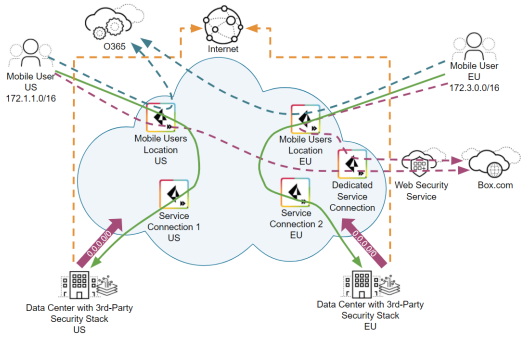

©2025 Palo Alto Networks, Inc.



# 具有流量導向和專用服務連線的預設路由範例

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

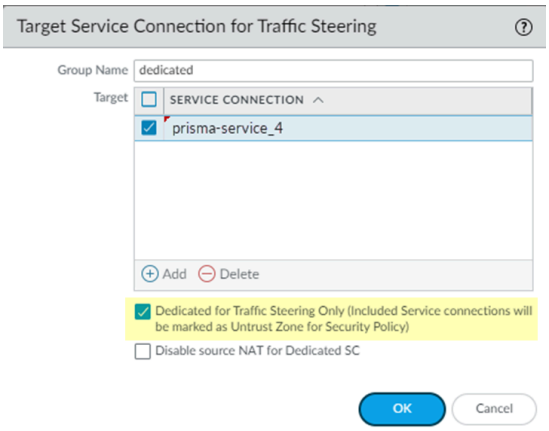
在此範例中，除了先前的設定之外，您還有第三方網際網路安全性服務，並且您想要從 box.com 傳送流量，以在輸出到網際網路之前由安全性服務進行處理。您不想要將任何其他網際網路繫結流量傳送至安全性服務；因此，您為 box.com 流量建立專用服務連線。在您的設定完成之後，Prisma Access 會將 *.box.com 目的地流量傳送至堆疊。




若要啟用此部署，您可以在 [Traffic Steering（流量導向）] 頁籤中執行下列動作：

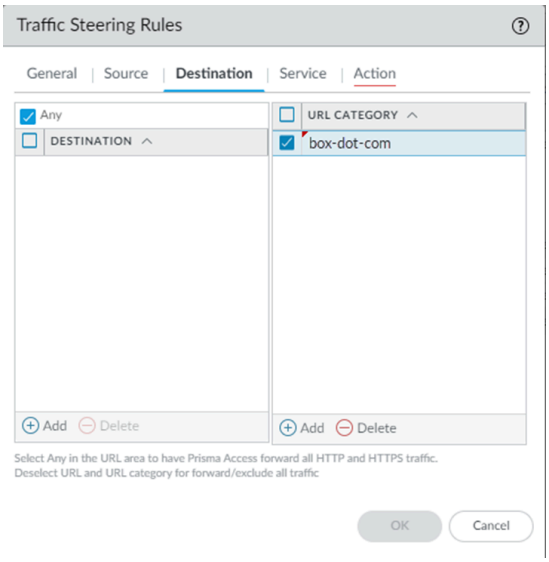
- 建立一個目標服務連線群組，將一個或多個服務連線指派給目標，並選取 **Dedicated for Traffic Steering Only**（僅專用於流量導向），這會使一個或多個目標服務連線成為專用。

  如果您建立一個目標，具有多個服務連線，*Prisma Access* 會選擇最佳服務連線來轉送網際網路繫結流量。

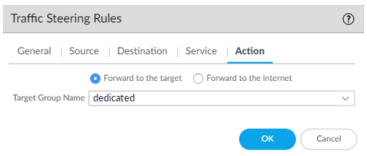



 ©2025 Palo Alto Networks, Inc.

- 建立將流量轉送到 URL 的流量導向規則。以下螢幕擷取畫面顯示了獲指派自訂 URL 類別的流量目的地，該類別包含 URL *.box.com。




- 在 **Forward to the target**（轉送至目標）的流量導向規則中建立一個 **Action**（動作），並指定您建立的目標群組名稱（本案例中的 **dedicated**（專用））。




## Prisma Access 流量導向規則指導方針

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Panorama | • Prisma Access 授權 |

流量導向可以處理各種可能的設定；不過，瞭解 Prisma Access 如何處理規則很重要，以便您可以建立易於維護和管理的規則。若要協助您建立最適合部署的規則，請遵循下列指導方針：

- Prisma Access 會依您建立規則的順序（從上到下）評估這些規則。在頂部指定更具體的規則，在底部指定更一般的規則。
- 建立多個具有較少比對規則的規則，而不是建立更少具有多種準則類型的規則。建立更簡單的規則可加快規則建立速度，同時又能更輕鬆修改規則。
- 由於在建立規則之後，您無法在清單中向上或向下移動該規則，因此在建立規則之前仔細規劃規則順序。
- 不支援指定 **Any**（任何）來源位址和使用者、**Any**（任何）來源目的地和 URL 類別，以及 **Any**（任何）服務的規則。使用更具體的規則；例如，指定具有 **Any**（任何）來源或目的地流量，且服務為 **service-http** 和 **service-https** 的規則。
- 如果您是在 **Source User**（來源使用者）欄位中指定使用者的規則，請確保在本機驗證的使用者與使用 LDAP 驗證的使用者之間共用相同使用者名稱時，Prisma Access 可以區分這些使用


©2025 Palo Alto Networks, Inc.

者，方法是以 `domain/username` 格式驗證 LDAP 使用者，並以 `username` 格式（不含網域名稱）驗證本機使用者。

- 如果您已將內部部署新世代防火牆設定為主要裝置，則可以在流量導向和安全性政策規則中自動填入行動使用者裝置群組的使用者和群組資訊，方法是選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users**（行動使用者）、按一下齒輪圖示來編輯設定，然後在 [Device Group（裝置群組）] 區域中選取 **Master Device**（主要裝置）。雖然這會在每個裝置群組中填入主要裝置，但它只會在安全性政策規則中填入行動使用者的使用者和群組資訊。
- 如果流量導向規則中使用了 EDL（類型 IP 清單），且 EDL 的 EDL 來源 URL 已更新為無法存取的 URL，則 Prisma Access 可能繼續使用上一個 URL 中的快取 IP 清單。
- 如果您針對 TCP 連接埠 80 和 443 使用應用程式覆寫政策，則 Prisma Access 會略過服務類型為 HTTP 或 HTTPS 之規則的流量導向。

  此外，如果您已針對 TCP 連接埠 80 或 443 設定應用程式覆寫政策，則流量導向將不適用於流量導向規則中參考的 URL 類別中的 URL。
- 您可以在相同規則中指定目的地 IP 位址和 URL 類別。如果這樣做，則 Prisma Access 會使用邏輯 OR 來處理規則中的目的地準則，但會根據 TCP 連接埠 80 和 8080（適用於 HTTP）和 TCP 連接埠 443（適用於 HTTPS）處理 URL 和 URL 類別流量。

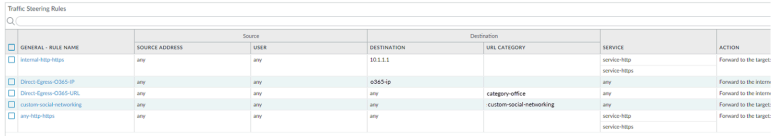
  對於具有 IP 位址和 URL 類別的規則，如果 IP 位址或 URL 類別相符，則流量會比對規則，但僅根據連接埠 80、443 和 8080 處理 URL 類別流量。Palo Alto Networks 建議建立此類型的規則，而是建立更簡單的規則。

例如，您想要對網路流量強制執行下列規則：

- 您在資料中心有一個 IP 位址為 10.1.1.1 的內部 HTTP 伺服器，並且您想要將內部 HTTP 和 HTTPS 流量引導至此伺服器。伺服器的 IP 位址為 10.1.1.1。

  此伺服器的流量不應該流向網際網路，而且應該在內部處理；因此，請為此流量選擇非專用目標，因為此類型的目標會同時處理內部流量和網際網路繫結流量。
- 您想要 office365.com 流量直接路由至網際網路。
- 您想要來自 *.example.com 的流量或自訂 URL 類別 **custom-social-networking** 中定義的任何流量路由到專用連線。
- 您想要任何其他 HTTP 和 HTTPS 流量使用與內部 HTTP 伺服器所使用相同的非專用服務連線目標。

在此範例中，建立最具體到最不具體的規則，如以下螢幕擷取畫所示。請先不要新增允許所有 HTTP 和 HTTPS 流量的規則，否則 Prisma Access 會將所有 HTTP 和 HTTPS 流量引導到非專用連線，而不評估任何其他規則。




 ©2025 Palo Alto Networks, Inc.

# 設定區域對應和安全性政策以進行流量導向專用連線

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

如果您建立一個使用專用服務連線的目標，則專用服務連線的區域會從 **Trust**（信任）變更為 **Untrust**（不信任）（非專用服務連線目標不會變更其區域）。由於您無法為服務連線建立區域或設定區域對應，因此您可以改為對行動使用者和裝置群組的專用服務連線進行區域對應和安全性政策變更。完成以下步驟以設定專用連線的區域對應。

這些步驟會顯示一個範例設定；您可以定制這個範例以適合您的部署。

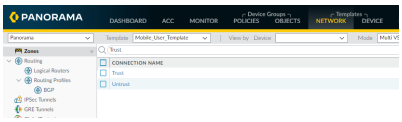
**STEP 1 |** 選取 **Network**（網路） > **Zones**（區域）。

**STEP 2 |** 從下拉式清單中選取正確的 **Template**（範本）（**Mobile_User_Template** 用於行動使用者或 **Remote_Network_Template** 用於遠端網路）。

如果您有行動使用者和遠端網路部署，則需要執行這些步驟兩次；一次在 **Mobile_User_Template** 中，另一次在 **Remote_Network_Template** 中。

**STEP 3 |** 為受信任的區域和不受信任的區域 **Add**（新增）兩個區域。

這個範例建立了兩個區域，分別稱為 **Trust**（信任）和 **Untrust**（不信任）。



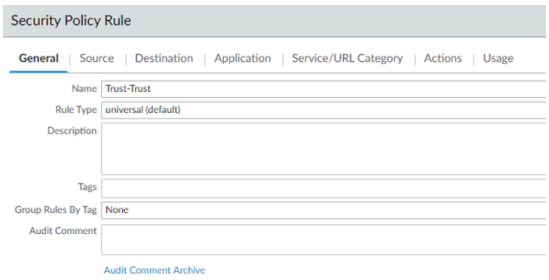

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 為您建立的區域建立預設政策。

1. 選取 **Policies**（政策） > **Security**（安全性） > **Post Rules**（後續規則）。
2. 從下拉式清單中選取正確的 **Device Group**（裝置群組）（**Mobile_User_Device_Group** 用於行動使用者或 **Remote_Network_Device_Group** 用於遠端網路）。

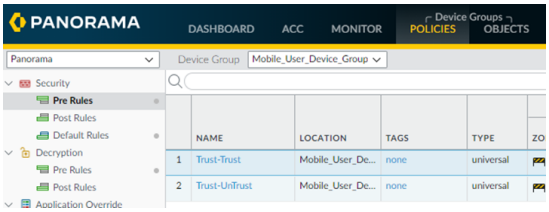
   如果您有行動使用者和遠端網路部署，則需要執行這些步驟兩次；一次在 **Mobile_User_Device_Group** 中，另一次在 **Remote_Network_Device_Group** 中。
3. **Add**（新增）要用於信任區域到信任區域流量的預設政策。

   此政策允許 **Any**（任何）流量，讓所有 **Source**（來源）、**User**（使用者）、**Destination**（目的地）、**Application**（應用程式） 和**Service/URL Category**（服務/**URL** 類別）流量都可傳遞。




4. 使用您用於信任到信任政策的相同參數，**Add**（新增）要用於信任區域到不信任區域流量的預設政策。

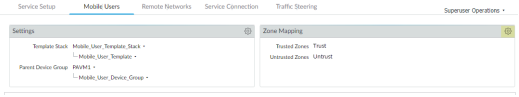
   完成時，您將有兩個安全政策，一個用於信任到信任流量，另一個用於信任到不信任流量。



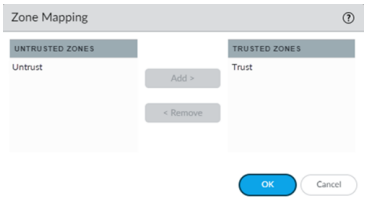

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** 視您部署的需要，為遠端網路、行動使用者或兩者定義區域對應。

1. 為遠端網路、行動使用者或兩者設定區域對應.
   - 對於行動使用者，選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users**（行動使用者）。
   - 對於遠端網路，選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路）。
2. 按一下 **Zone Mapping**（區域對應）旁邊的齒輪圖示以編輯設定。



3. 為您的部署設定 **Zone Mapping**（區域對應），將受信信流量的區域移至 **Trusted Zones**（受信任的區域）、將不受信任流量的區域移至 **Untrusted Zones**（不受信任的區域）；然後，按一下 **OK**（確定）。




## 在 Prisma Access 中設定流量導向

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ 若要將憑證撤銷清單 (CRL) 和線上憑證狀態通訊協定 (OCSP) 直接傳送至網際網路，所需的最低 Prisma Access 版本為 5.1.1。 |

流量導向可讓您設定 Prisma Access 存取，以建立流量導向規則，為來自行動使用者和遠端網路連線的網際網路繫結流量指定目標。您可以指定要重新導向至服務連線的流量，然後再將該流量傳送至網際網路，也可以指定要直接輸出至網際網路的流量。完成下列步驟，為您的 Prisma Access 部署設定流量導向。

- Strata Cloud Manager
- Panorama

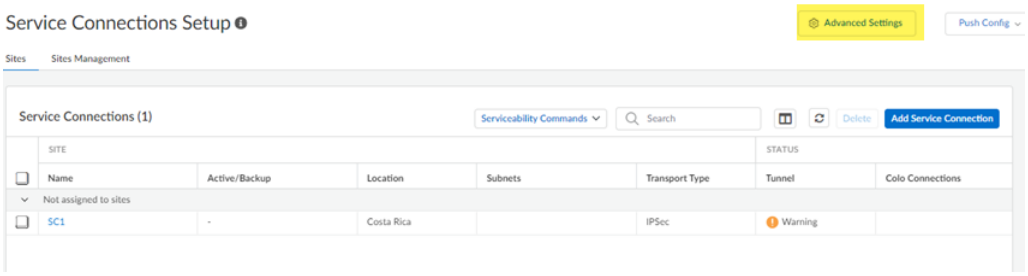
### 在 Prisma Access 中設定流量導向 (Strata Cloud Manager)

在 Prisma Access 部署中，服務連接會提供對內部網路資源的存取，例如總部或資料中心的驗證服務和私人應用程式。服務連線會處理內部流量，其中不需要網際網路存取。在某些情況下，您可能想要將網際網路繫結流量重新導向到資料中心。流量轉向允許您在將行動使用者或遠端網路流量傳送到網際網路之前將其重新導向到服務連線。完成以下步驟，為您的 Prisma Access 部署設定流量導向。

**STEP 1 |** 根據您的部署情況，裝載服務連線、行動使用者和遠端網路。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Service Connection**（服務連線） > **Advanced Settings**（進階設定）。




**STEP 3 |** 設定 **Traffic Steering**（流量導向）規則。

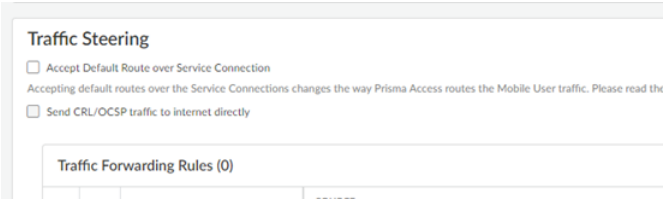
1. （選用，僅限行動使用者部署）允許 Prisma Access 接受並安裝透過 CPE 中一個或多個服務連線公告的預設路由，方法是按一下齒輪圖示開啟設定，並選取 **Accept Default Route over Service Connections**（接受透過服務連線的預設路由）。

   預設路由具有您使用它們時必須遵循的指導方針；例如，僅支援預設路由進行行動使用者部署，但對遠端網路部署無效。在實作具有流量導向的預設路由之前，請務必檢閱這些指導方針。

**STEP 4 |** （選用）允許 Prisma Access 透過選取 **Send CRL/OCSP traffic to internet directly**（直接將 **CRL/OCSP** 流量傳送至網際網路），將憑證撤銷清單 (CRL) 和線上憑證狀態通訊協定 (OCSP) 流量直接傳送到網際網路。

如果您在公用網際網路中有 OCSP 或 CRP 伺服器，並且想要使用不受信任的區域，將該流量直接傳送到網際網路，請選取此選項。如果您未選取此選項，Prisma Access 會將此流量傳送至服務連線。

確定您將 *Prisma Access* 部署升級至最低版本 *5.1.1*，然後再選取 ***Send CRL/OCSP traffic to internet directly***（直接將 ***CRL/OCSP*** 流量傳送到網際網路）。




 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** 為您建立的目標建立規則並將其套用到目標。

1. **Add Rule**（新增規則）。
2. 輸入規則的唯一 **Name**（名稱）。
3. 在 **Source**（來源）區域中：
   - 指定要比對的使用者清單。

     您可以 **Match Any User**（比對任何使用者）、**Match Pre-logon**（比對預先登入）、**Match known-user**（比對 **known-user**）、**Match unknown**（比對未知）或 **Add Users**（新增使用者），並選取要比對的使用者。
   - 選取 **Source Address Entities**（來源位址實體）。您可以選取下列一或多個物件：
     - 一個 IP 位址
     - 一個位址群組
     - 一個使用 IP 位址或 URL 的外部動態清單 (EDL)
4. 在 **Destination**（目的地）區域中，指定下列其中一個 **Destination Address Entities**（目的地位址實體），或選取 **Any**（任何），使流量由 [URL Category（URL 類別）] 欄位中的規則處理：
   - 一個 IP 位址
   - 一個位址群組
   - 一個使用 IP 位址或 URL 的外部動態清單 (EDL)
5. 指定 **URL Category**（**URL** 類別）。

   如果您建立自訂 URL 類別，請輸入全部小寫的 URL。流量導向支援自訂 URL 和預先定義的 URL 類別。您可以使用萬用字元搭配 URL 類別中的 URL。支援以下萬用字元格式：
   - *.example.com
   - *.fqdn.example.com

   不支援以下格式：
   - *
   - *.*
   - *example.com
   - example.com/（與流量導向搭配使用的 URL 類別不支援 URL 中的結尾斜線）
   - example.com/path（僅支援網域名稱）
   - *fqdn.example.com
   - fqdn.example.*

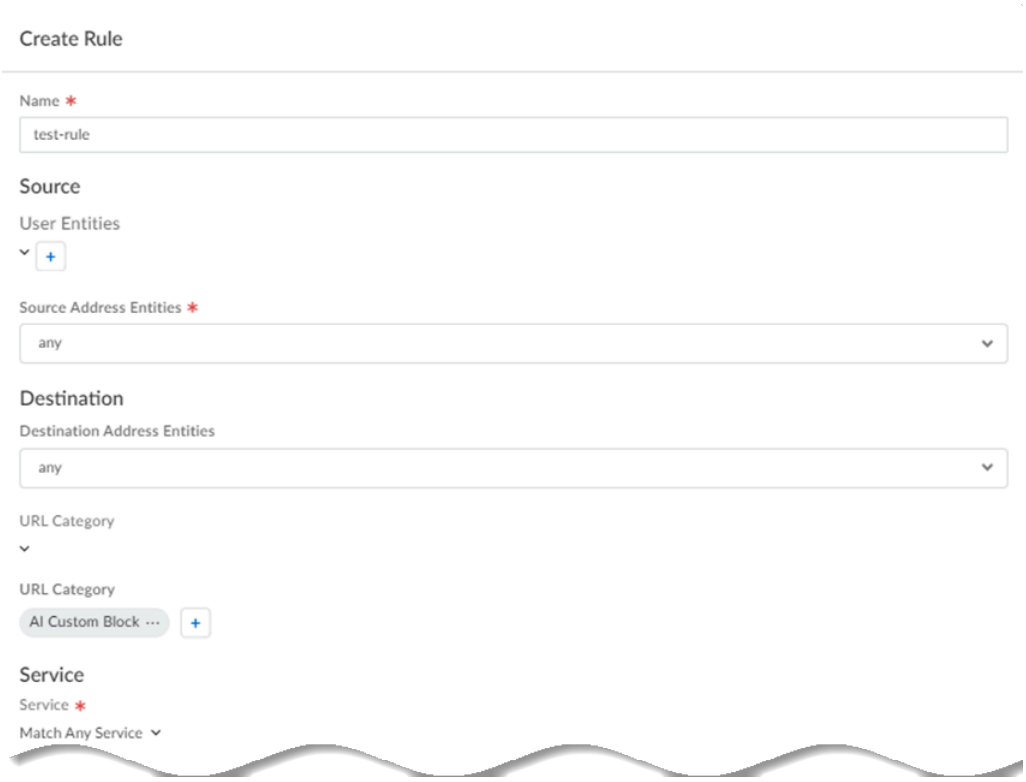
   設定目的地選項時請遵循下列指導方針：
   - 如果指定 URL 類別，即使服務設定為 **[Any**（任何）**]**，Prisma Access 也僅會比對 HTTP 和 HTTPS 流量。
   - 請勿建立類型為 **Category Match**（類別比對）的自訂 URL 類別。

   請勿建立名稱為 **Custom_URL_Category_TFR** 的自訂 URL 類別。

 ©2025 Palo Alto Networks, Inc.

6. 指定 **Service**（服務）類型並 **Add Service**（新增服務）。

   指定 **service-http** 以轉送 HTTP 流量，指定 **service-https** 以指定 HTTPS 流量。選取 **Match Any Service**（比對任何服務），以轉送任何服務類型的流量。




7. 建立服務連線群組並指定 **Action**（動作）。

   1. **Create New**（建立新的）或 **Manage**（管理）群組，並給與它唯一的 **Name**（名稱）。
   2. 指定要與目標搭配使用的 **Service Connection**（服務連線）。

      Palo Alto Networks 不建議在流量導向規則中參考的目標服務連線群組中使用多個服務連線（無論是專用還是非專用）。此外，給定的服務連線只能存在於一個目標中，您無法將單一服務連線新增至兩個不同的目標。
   3. （選用）您可以使用專用服務連線，將流量導向至不在您內部且不需要參與路由的第三方安全性堆疊或雲端。若要設定服務連線，以用作專用服務連線，請選取 **Dedicated for Traffic Steering Only**（僅專用於流量導向）。

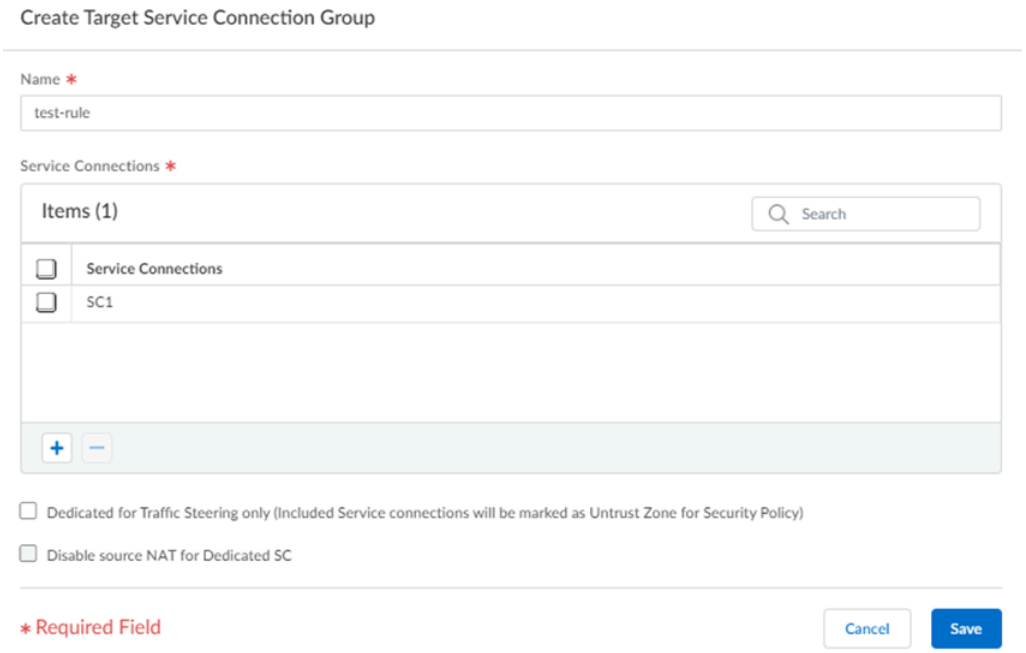
      專用服務連線會變更其區域並標記為安全性政策規則的不受信任區域。

      如果您將透過服務連線傳送正常服務連線相關流量和流量導向流量，請取消選取 **Dedicated for Traffic Steering Only**（僅專用於流量導向）；透過此選擇，服務連線的區域仍為信任。
   4. 選取 **Disable Source NAT for Dedicated SC**（停用專用 **SC** 的來源 **NAT**），來停用專用服務連線的來源 NAT。預設啟用來源 NAT（已取消選取核取方塊）。


©2025 Palo Alto Networks, Inc.

如果停用來源 NAT，Prisma Access 會使用您組織的來源 IP 位址進行專用服務連線。如果啟用來源 NAT，Prisma Access 會使用服務連線的 **EBGP Router**（**EBGP** 路由器）位址（**Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Service Connection**（服務連線） > **EBGP Router**（**EBGP** 路由器））作為來源 IP 位址，即使在流量從專用服務連線輸出之後也是如此。

5. **Save**（儲存）變更。




8. 將流量轉送至指定的服務連線目標，或在不通過服務連線的情況下直接將流量傳送至網際網路。

   - 若要使 Prisma Access 將流量轉送至服務連線目標，請選取 **Forward to the target**（轉送至目標）；然後選取 **Target Service Connection Group**（目標服務連線群組）。

     如果由於 SaaS 應用程式允許清單限制，您需要將流量傳送到現有或舊版環境，或者如果您想要建立流量，以將指定的網際網路流量導回內部部署網路，請指定此選項。

   - 若要使 Prisma Access 將流量直接轉送到網際網路，而不先將其傳送至服務連線，請選取 **Forward to the internet**（轉送至網際網路）。

     如果您是將預設路由傳送到 Prisma Access，並且想要將一些流量直接導向到網際網路，請指定此選項。




 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** **Push Config**（推送設定）以儲存您的變更。

### 在 Prisma Access 中設定流量導向 (Panorama)

**STEP 1 |** 根據您的部署情況，裝載服務連線、行動使用者和遠端網路。

**STEP 2 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Traffic Steering**（流量導向）。

**STEP 3 |** （選用，僅限行動使用者部署）允許 Prisma Access 接受並安裝透過 CPE 中一個或多個服務連線公告的預設路由，方法是按一下齒輪圖示開啟設定，並選取 **Accept Default Route over Service Connections**（接受透過服務連線的預設路由）。

預設路由具有您使用它們時必須遵循的指導方針；例如，僅支援預設路由進行行動使用者部署，但對遠端網路部署無效。在實作具有流量導向的預設路由之前，請務必檢閱這些指導方針。

**STEP 4 |** （選用）允許 Prisma Access 透過選取 **Send CRL/OCSP traffic to internet directly**（直接將 **CRL/OCSP** 流量傳送至網際網路），將憑證撤銷清單 (CRL) 和線上憑證狀態通訊協定 (OCSP) 流量直接傳送到網際網路。

如果您在公用網際網路中有 OCSP 或 CRP 伺服器，並且想要使用不受信任的區域，將該流量直接傳送到網際網路，請選取此選項。如果您未選取此選項，Prisma Access 會將此流量傳送至服務連線。

確定您將 *Prisma Access* 部署升級至最低版本 *5.1.1*，然後再選取 ***Send CRL/OCSP traffic to internet directly***（直接將 ***CRL/OCSP*** 流量傳送到網際網路）。




 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** （選用）建立目標群組並將服務連線指派給它。

1. 在 **Target Service Connections for Traffic Steering**（流量導向的目標服務連線）區域中，**Add**（新增）一個群組，並給與它 **Group Name**（群組名稱）。
2. **Add**（新增）流量的 **Target**（目標），指定與目標搭配使用的 **Service Connection**（服務連線）；然後，按一下 **OK**（確定）。

   Palo Alto Networks 不建議在流量導向規則中參考的目標服務連線群組中使用多個服務連線（無論是專用還是非專用）。此外，給定的服務連線只能存在於一個目標中，您無法將單一服務連線新增至兩個不同的目標。
3. 選擇是否使與此目標相關聯的服務連線成為專用服務連線。
   - 您可以使用專用服務連線，將流量導向至不在您內部且不需要參與路由的第三方安全性堆疊或雲端。若要設定服務連線，以用作專用服務連線，請選取 **Dedicated for Traffic Steering Only**（僅專用於流量導向）。

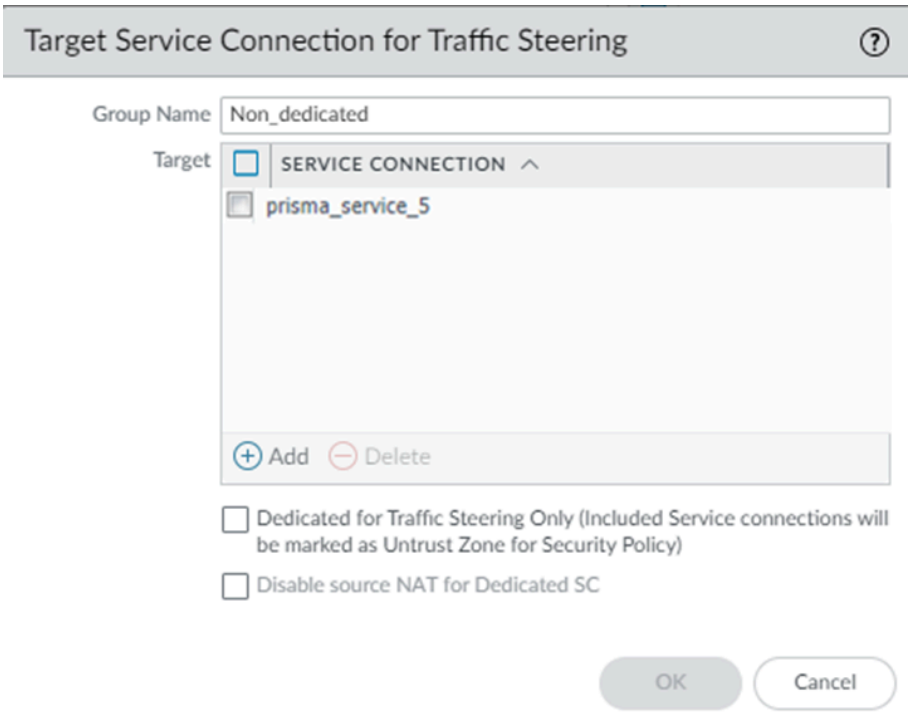
     專用服務連線會變更其區域。
   - 如果您將透過服務連線傳送正常服務連線相關流量和流量導向流量，請取消選取 **Dedicated for Traffic Steering Only**（僅專用於流量導向）；透過此選擇，服務連線的區域仍為信任。
4. 選擇啟用還是停用來源 NAT。

   若要停用專用服務連線的來源 NAT，請選取 **Disable Source NAT for Dedicated SC**（停用專用 **SC** 的來源 **NAT**）。預設啟用來源 NAT（已取消選取核取方塊）。

   如果停用來源 NAT， Prisma Access 會使用您組織的來源 IP 位址進行專用服務連線。如果啟用來源 NAT，Prisma Access 會使用服務連線的 **EBGP Router**（**EBGP** 路由器）位址（**Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路

 ©2025 Palo Alto Networks, Inc.

詳細資訊） > **Service Connection**（服務連線） > **EBGP Router**（**EBGP** 路由器））作為來源 IP 位址，即使在流量從專用服務連線輸出之後也是如此。




 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** 為您建立的目標建立規則並將其套用到目標。

1. 在 **Traffic Steering Rules**（流量導向規則）區域中，**Add**（新增）流量導向規則。
2. 在 **General**（一般）頁籤中，**Name**（命名）流量導向規則。
3. 在 **Source**（來源）頁籤中，指定來源流量的規則。
   - 在 **Source Address**（來源位址）欄位中，指定以下一個或多個物件，或選取 **Any**（任何），使來自任何來源的流量前往此目標：
     - 一個 IP 位址
     - 您在 Panorama 中建立的位址物件（**Objects**（物件） > **Addresses**（位址））
     - 一個動態位址群組 (DAG)
     - 一個使用 IP 位址或 URL 的外部動態清單 (EDL)
   - 在 **Source User**（來源使用者）欄位中，指定來源使用者流量的規則。您可以指定以下使用者資訊：
     - 使用者

       以 *domain/user* 或 *user@domain* 格式輸入使用者。
     - 使用者群組

       輸入使用者群組時使用完整識別名稱 (DN)。
     - 在 Panorama 上設定的使用者（**Device**（裝置） > **Local User Database**（本機使用者資料庫） > **Users**（使用者））
     - 在 Panorama 上設定的使用者群組（**Device**（裝置） > **Local User Database**（本機使用者資料庫） > **User Groups**（使用者群組））

   如果您使用位址物件、DAG、EDL、使用者或使用者群組，請將它們指定為 **Shared**（共用），以與 Prisma Access 中的所有裝置群組共用它們。此外，請勿在位址物件、DAG 或 EDL 中輸入 0.0.0.0/0；相反，直接在規則中輸入 0.0.0.0/0。

   *Prisma Access* 僅會自動填入來自行動使用者裝置群組的使用者。
4. 在 **Destination**（目的地）頁籤中，指定以下值：
   - 在 **Destination**（目的地）區域中，指定下列其中一個條件，或選取 **Any**（任何），使流量由 **URL Category**（**URL** 類別）欄位中的規則處理：
     - 一個 IP 位址或首碼
     - 您在 Panorama 中建立的位址物件（**Objects**（物件） > **Addresses**（位址））
     - 一個動態位址群組 (DAG)
     - 一個 IP 位址型外部動態清單 (EDL)

       請勿在位址物件、*DAG* 或 *EDL* 中輸入 *0.0.0.0/0*；相反，直接在規則中輸入 *0.0.0.0/0*。

     保留選取 **Any**（任何），以傳遞要由 **URL Category**（**URL** 類別）區域中規則處理的所有流量。如果您在 **Destination**（目的地）和 **URL Category**（**URL** 類別）區域中指定規則，Prisma Access 首先處理 **Destination**（目的地）類別中的規則。

 ©2025 Palo Alto Networks, Inc.

- 在 **URL Category**（**URL** 類別）欄位中，輸入自訂 URL 類別（**Objects**（物件） > **Custom Objects**（自訂物件） > **URL Category**（**URL** 類別））建立自訂 URL 類別時，請輸入全部小寫的 URL。流量導向支援自訂 URL 和預先定義的 URL 類別。

  您可以使用萬用字元搭配 URL 類別中的 URL。支援以下萬用字元格式：

  - *.example.com
  - *.fqdn.example.com

  不支援以下格式：

  - *
  - *.*
  - *example.com
  - example.com/（與流量導向搭配使用的 URL 類別不支援 URL 中的結尾斜線）
  - example.com/*path*（僅支援網域名稱）
  - *fqdn.example.com
  - fqdn.example.*

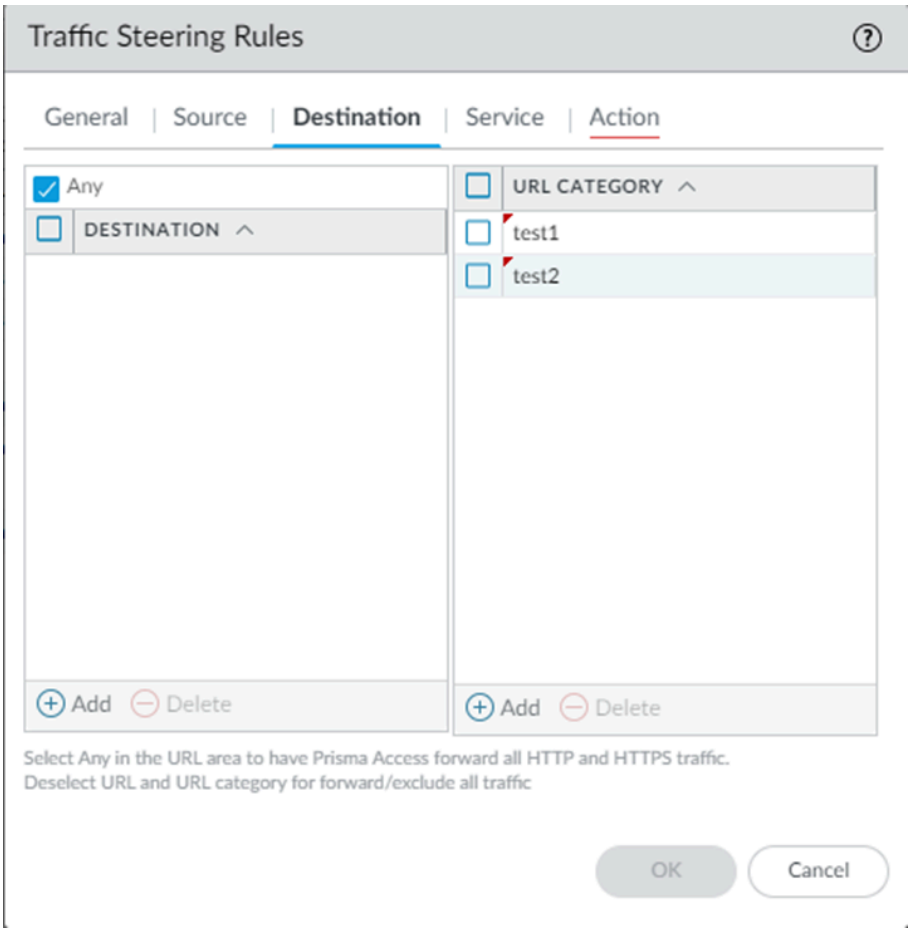
  自訂 URL 類別中的 URL 會使用與新世代防火牆所使用的相同的 URL 模式比對。

設定目的地選項時請遵循下列指導方針：

- 如果指定 URL 類別，即使服務設定為 [Any（任何）]，Prisma Access 也僅會比對 HTTP 和 HTTPS 流量。
- 請勿建立類型為 **Category Match**（類別比對）的自訂 URL 類別。
- 請勿建立名稱為 **Custom_URL_Category_TFR** 的自訂 URL 類別，因為對於從 Prisma Access 1.7 移轉到 2.0 的部署，從 1.7 開始在 URL 區域中輸入的 URL 會移至名稱為

 ©2025 Palo Alto Networks, Inc.

**Custom_URL_Category_TFR***number* 的自訂 URL 類別，其中 *number* 是附加到自訂 URL 類別的數字。




5. 在 **Service**（服務）頁籤中，指定服務類型。

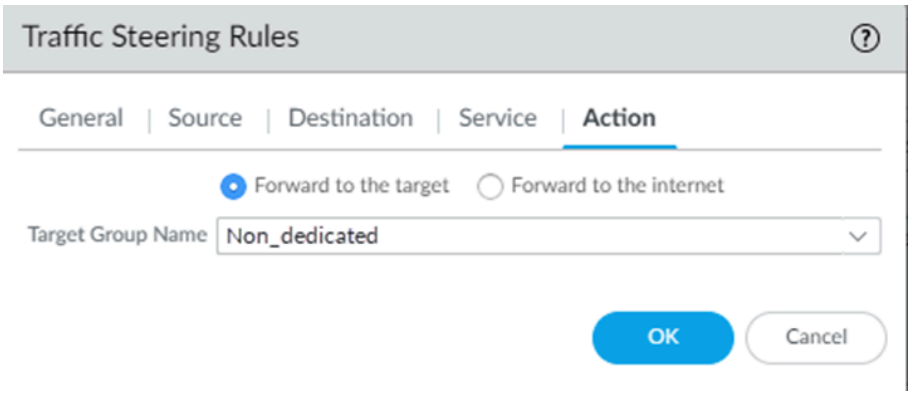
   指定 **service-http** 以轉送 HTTP 流量，指定 **service-https** 以指定 HTTPS 流量。選取 **Any**（任何），以轉送任何服務類型的流量。

6. 在 **Action**（動作）頁籤中，選取要套用至流量導向規則的 **Target Group Name**（目標群組名稱）。

7. 將流量轉送至指定的服務連線目標，或在不通過服務連線的情況下直接將流量傳送至網際網路。

   - 若要使 Prisma Access 將流量轉送至服務連線目標，請選取 **Forward to the target**（轉送至目標）；然後選取 **Target Group Name**（目標群組名稱）。
   - 若要使 Prisma Access 將流量直接轉送到網際網路，而不先將其傳送至服務連線，請選取 **Forward to the internet**（轉送至網際網路）。


©2025 Palo Alto Networks, Inc.



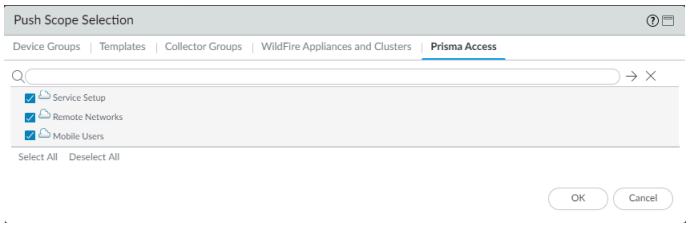

8. 按一下 **OK**（確定）儲存您的變更。

**STEP 7 |** 選用 指定其他流量導向規則。

Prisma Access 會依您建立多個規則的順序（從上到下）處理它們。

**STEP 8 |** 提交並推送您的變更，使其在 Prisma Access 中作用中。

1. 在推送範圍中選取 **Commit**（提交） > **Commit and Push**（提交並推送）和 **Edit Selections**（編輯選取項目）。
2. 選取 **Prisma Access**，然後選取 **Service Setup**（服務設定）、**Remote Networks**（遠端網路）和 **Mobile Users**（行動使用者）。




3. 按一下 **Ok**（確定），以儲存您對 Push Scope（推送範圍）所做的變更。
4. **Commit**（提交）並 **Push**（推送）您的變更。

# 服務連線流量的路由

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

Prisma Access 會使用 BGP 進行動態路由，並使用 BGP 路徑選擇將路由安裝至路由表。當 Prisma Access 使用服務連線，將流量路由至您的到總部或資料中心時，它會使用有效引導該流量的路由方法。Prisma Access 會使用旨在適應大多數網路部署的預設路由模型；不過，並非所有組織的網路都是相同的。為了適應更廣泛的部署，Prisma Access 允許您為服務連線路由選擇另一種模式。

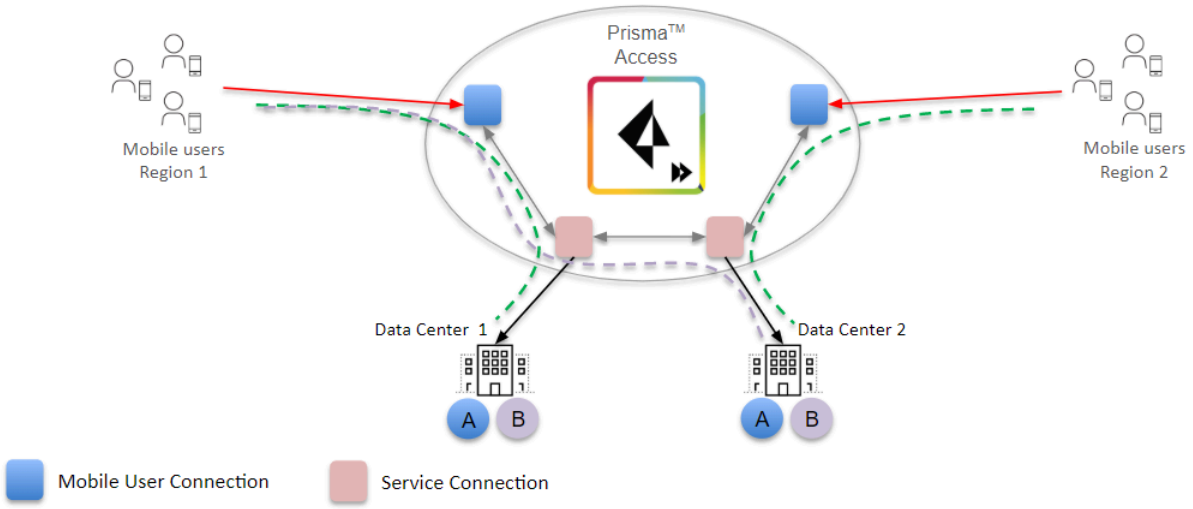
變更 *Prisma Access* 服務連線路由方法需要徹底瞭解組織的拓撲和路由裝置，以及瞭解 *Prisma Access* 的運作方式，如本節所述。在變更預設設定的路由方法之前，請仔細閱讀本節。

 ©2025 Palo Alto Networks, Inc.

Prisma Access 支援靜態路由和使用 BGP 的動態路由，進行服務連線和遠端網路連線。當您使用 BGP 路由進行連線時，您組織的網路會從 Prisma Access 得知 BGP 資訊。

在決定使用哪個服務連線路由之前，您應該瞭解 Prisma Access 如何在行動使用者、遠端網路和服務連線之間路由流量，這是很有用的，因為服務連線之間行動使用者流量和遠端網路流量所使用的路由不同。

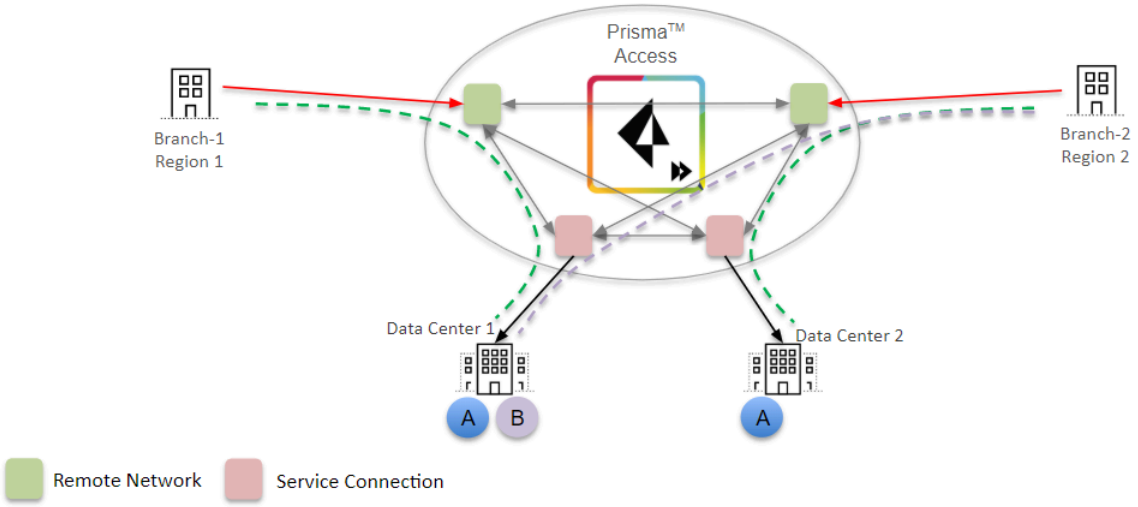
行動使用者服務連線路由—行動使用者連線與最近的服務連線形成 IPSec 通道。Prisma Access 會使用 iBGP 進行內部路由，並使用 eBGP 與資料中心的用戶端周邊設備進行對等。下圖顯示區域 1 和 2 中的行動使用者正在路由到該區域中各自的服務連線。區域 1 中的行動使用者正在存取位於資料中心 1 的應用程式 **A** 和 **B**。如果您組織的網路使用 BGP 路由進行服務連線，且服務連線在資料中心 1 遭遇 ISP 故障，則 Prisma Access 會偵測該故障，並在 BGP 聚合之後將應用程式 **A** 和 **B** 的流量路由到資料中心 2，從而為您網路的資料中心提供備援。




當偵測到故障時，*Prisma Access* 會使用下列計搭配 *BGP*：如果設定 *BGP* 路由並啟用通道監控，則確定安全性參數索引 *(SPI)* 失敗的最短預設保留時間是通道監控，當連續 *15* 秒偵測到通道故障時，通道監控會刪除通往對等方的所有路由。這樣一來，通道監控就可以決定 *BGP* 路由的行為。如果未設定通道監控，保留計時器會決定刪除路由之前通道關閉的時間。*Prisma Access* 會使用 *RFC 4271* 定義的預設 *BGP HoldTime* 值：*90* 秒，這是 *Prisma Access* 刪除非作用 *SPI* 的路由之前的最長等待時間。如果對等 *BGP* 裝置設定的保留時間較短，則 *BGP* 保留計時器會使用較小的值。當次要通道安裝成功後，次要路由會優先採用，直到主要通道恢復正常為止。若主要和次要通道皆正常運作，則優先採用主要路由。

遠端網路服務連線路由—Prisma Access 與其他遠端網路和服務連線建立全網狀網路。與行動使用者一樣，Prisma Access 會使用 iBGP 進行內部路由，並使用 eBGP 與客戶周邊設備對等以交換路由。如果分支 1 中的使用者正在從您組織資料中心的資料中心 1 存取應用程式 **A**，並且分支 1 與資料中心 1 之間的連結失效，則在 BGP 聚合之後，Prisma Access 會將應用程式 **A** 的流量路由到資料中心 2。

 ©2025 Palo Alto Networks, Inc.




在您瞭解 Prisma Access 服務連線路由及其與您網路的關係之後，您可以為服務連線選擇下列其中一個路由模式：

- 預設路由#這是 Prisma Access 使用的預設路由模型。

  如果您想要 Prisma Access 使用 BGP 最佳路徑選擇機制，而不調整任何 BGP 屬性，請使用此路由模式。在此模式下，Prisma Access 將遵守用戶端周邊設備 (CPE) 公告的任何屬性。
- 熱馬鈴薯路由—Prisma Access 會儘快地將流量傳遞至您組織的網路。

  如果您想要組織的網路執行大部分路由決策，請使用此路由方法。

## Prisma Access 預設路由

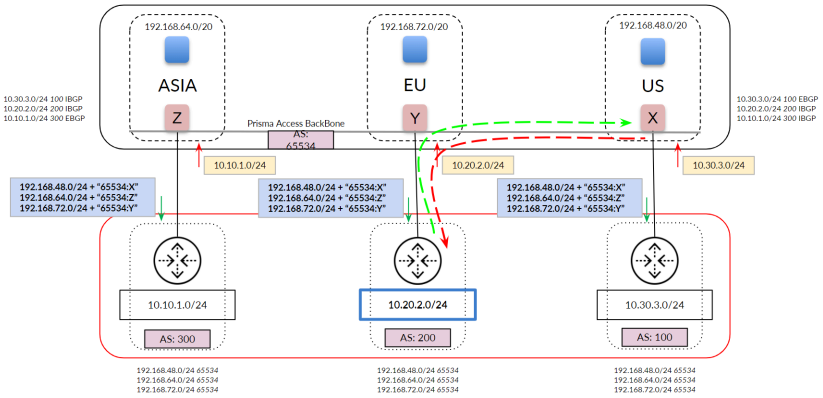
下圖顯示了預設路由模式下 Prisma Access 路由服務連線流量的範例。組織的網路在三個資料中心具有三個獨立的網絡，並且沒有連線網路的骨幹。在預設路由模式下，行動使用者集區平均地公告在三個網路上，如圖片底部所示。

請注意，當 Prisma Access 公告行動使用者路由時，它會在公告子網路之前將這些子網路劃分為 C/24 位址區塊；因此，當閘道使用首碼時，它會以 /24 區塊的形式公告 /20 行動使用者子網路。

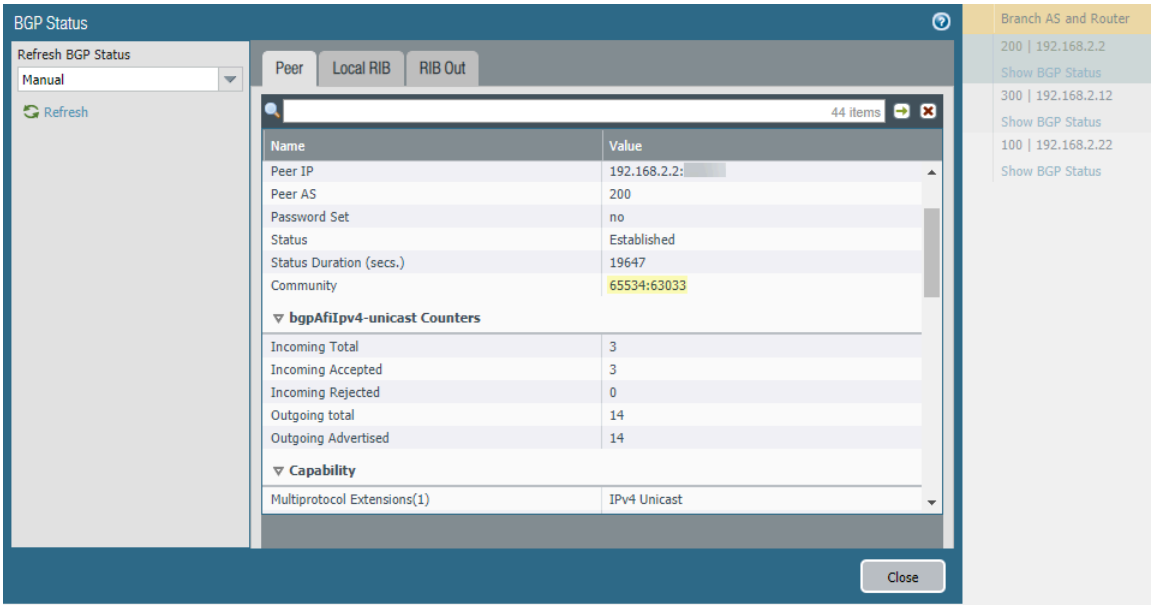
記下 Prisma Access 如何使用 BGP 路由公告：

- Prisma Access 不會調整行動使用者公告路由的預設 BGP 屬性（Prisma Access 會將其 AS 編號新增至路由公告）。
- Prisma Access 會以 /24 子網路區塊的形式公告行動使用者路由，並在其透過服務連線公告的路由中新增 BGP 社群值。下圖顯示一個行動使用者部署，其中具有三個服務連線，以及為行動使用者 IP 位址集區指定的三個不同 IP 位址區塊：`192.168.64.0/20` 用於亞洲、澳洲和日本地區、`192.168.72.0/20` 用於非洲、歐洲和中東地區，而 `192.168.48.0/20` 用於北美和南美洲地區。Prisma Access 會將這些路由劃分為 /24 的區塊，並使用 **AS** 編號 **65534** 公告它們，但也會將 BGP 社群值附加到公告（**Z** 代表亞洲、**Y** 代表歐盟，而 **X** 代表美國）。這些路由顯示在圖片中間。透過這種方式，您可以區分網路中的服務連線，即使 Prisma Access 將相同的 AS 編號指派給它們也一樣。

 ©2025 Palo Alto Networks, Inc.



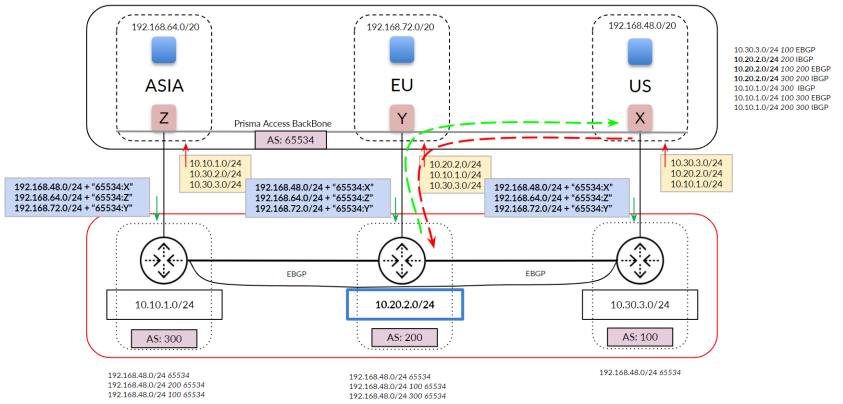

您可以選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Service Connection**（服務連線） > **Show BGP Status**（顯示 **BGP** 狀態），來檢視社群字串，並在 **Peer**（對等）頁籤中尋找 **Community**（社群）欄位。



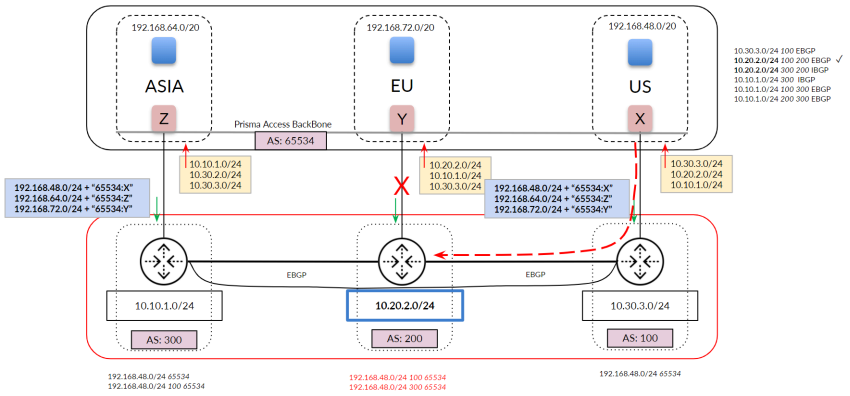

下圖顯示了具有全網狀 eBGP 骨幹的更常見網路。該圖顯示了 Prisma Access 已從右上角組織網路中得知的路由。請注意 Prisma Access 已透過 Prisma Access 骨幹 (iBGP) 和您組織骨幹 (eBGP) 得知的額外路由。

對於 **North America & South America**（北美和南美）地區（圖中的 US）的行動使用者與您組織的**Africa, Europe & Middle East**（非洲、歐洲和中東）地區（圖中的 EU）的資料中心之間的流量，Prisma Access 選擇透過 EU 服務連線的路徑，因為它偏好 AS-PATH 較短的路由。

 ©2025 Palo Alto Networks, Inc.



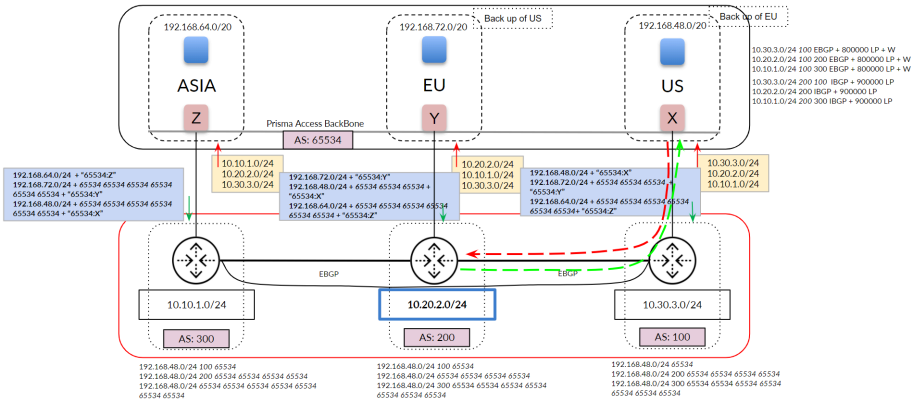

在具有全網狀 eBGP 骨幹的部署中，當 Prisma Access 由於客戶資料中心的 ISP/CPE 失敗而無法連線特定資料中心時，可能引發非對稱。下圖顯示了當 EU 服務連線的連結失效時可能發生的情況。您的網路偵測到連結失敗並為 AS 200 建立新的路由表。從 US 服務連線到 AS 200 的流量使用通過 AS 100 的路徑，因為 AS 200 與 AS 100 之間骨幹的 eBGP 路由優先於服務連線 EU 與 US 之間的 iBGP 路由。不過，不保證傳回流量通過相同路徑，因為內部部署 CPE 可以選擇任一路徑（以紅色顯示）來傳回流量。




前面的範例顯示了一個未彙總路由的網路（亦即，在將 BGP 路由公告傳送至 Prisma Access 之前，您未執行路由彙總）。以下範例顯示了一個網路，其在將路由傳送到 Prisma Access 之前已將該路由彙總為 10.0.0.0/8。如果選取預設路由，此設定可能會造成非對稱路由問題，因為 Prisma Access 無法從匯總路由中確定正確的傳回路徑。

如果你的 *Prisma Access* 部署具有遠端網路，*Palo Alto Networks* 不建議在服務連線上使用路由彙總。服務連線上的路由彙總僅適用於行動使用者部署。


©2025 Palo Alto Networks, Inc.




如果您對行動使用者使用路由彙總，我們強烈建議您啟用熱馬鈴薯路由而不是預設路由，其中 Prisma Access 會儘快將流量移交給您組織的網路；此外，我們建議您依下節所述為每個服務連線選取一個 **Backup SC**（備份 **SC**），以具有確定性的路由行為。

## Prisma Access 熱馬鈴薯路由

當您選取 **Hot Potato Routing**（熱馬鈴薯路由）時,Prisma Access 會儘快從其內部網路輸出繫結至服務連線/資料中心的流量。

透過熱馬鈴薯路由，Prisma Access 會在從閘道傳送的 BGP 首碼公告前面加上 AS 路徑 (AS-PATH)。當這些首碼從服務連線公告至您組織的本機 CPE 時，會在其前面加上此路徑。Prisma Access 會將 AS-PATH 加在前面，以便 CPE 可為主要和次要通道提供正確的優先順序，如此在主要通道失效時，CPE 會選擇次要通道作為備份。

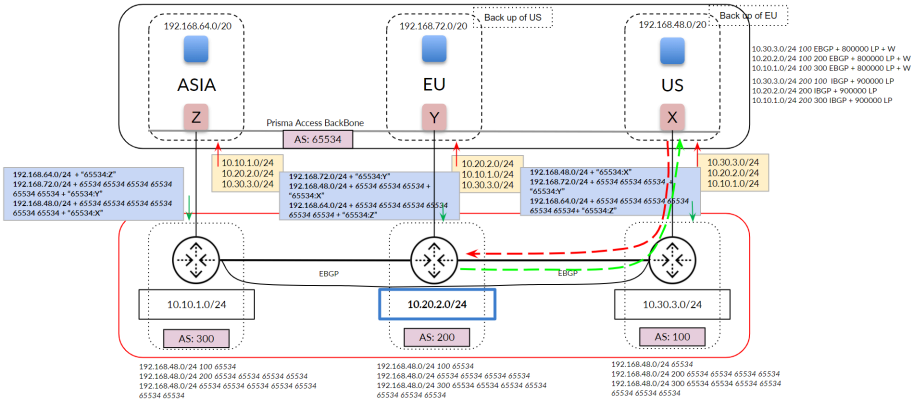
如果您為次要（備份）BGP 對等指定了不同的 IP 位址，則 Prisma Access 根據通道類型新增更多的前置，如下表所示。

| 首碼類型 | 服務連線通道類型 | **As-Path** 前置數目 | 在 **CPE** 上看到的 **AS-PATH** 總數 |
|---|---|---|---|
| 來自主要服務連線的閘道首碼 | 具有相同 BGP 對等 IP 位址的主要或次要通道 | 0 | 1 |
| 來自備份服務連線的閘道首碼 | 具有相同 BGP 對等 IP 位址的主要或次要通道 | 3 | 4 |
| 來自所有其他服務連線的閘道首碼 | 具有相同 BGP 對等 IP 位址的主要或次要通道 | 6 | 7 |
| 來自主要服務連線的閘道首碼 | 具有不同 BGP 對等 IP 位址的次要通道 | 1 | 2 |
| 來自備份服務連線的閘道首碼 | 具有不同 BGP 對等 IP 位址的次要通道 | 4 | 5 |
| 來自所有其他服務連線的閘道首碼 | 具有不同 BGP 對等 IP 位址的次要通道 | 7 | 8 |

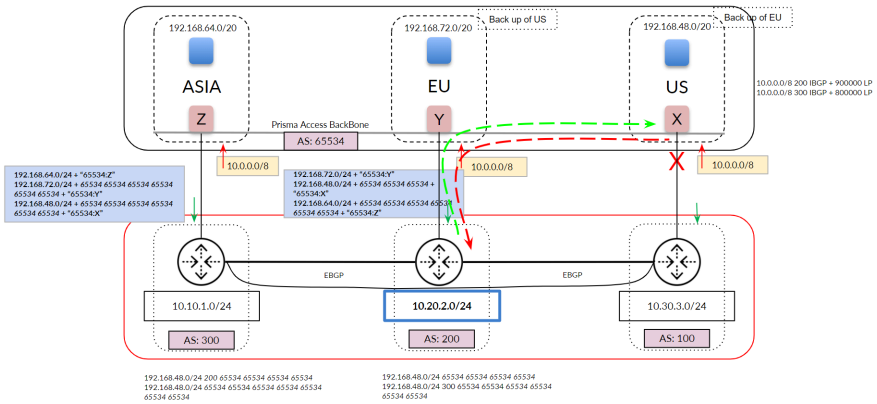
 ©2025 Palo Alto Networks, Inc.

在熱馬鈴薯路由模式下，Prisma Access 允許您在裝載期間指定備份服務連線。指定 **Backup SC**（備份 **SC**）會通知 Prisma Access 在服務連線連結失敗時使用該服務連線作為備份。

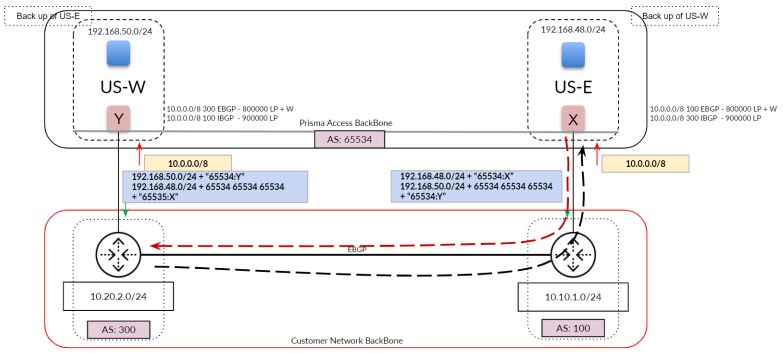
下圖顯示了美國服務連線與 AS 200 之間流量的熱馬鈴薯路由設定，其中歐盟服務連線設定為美國連線的 **Backup SC**（備份 **SC**）。使用熱馬鈴薯路由，Prisma Access 透過美國服務連線從其最近的出口路徑傳送流量。傳回流量採取通過 AS100 的相同路徑，因為此路徑具有對美國位置中行動使用者集區較短的 AS-PATH。Prisma Access 會在其首碼公告前面加上 AS-PATH，取決於通道是主要通道、備份通道，還是不用於主要通道或備份通道。




因為您已設定備份服務連線，所以如果美國服務連線的連結失效，熱馬鈴薯路由會使用其最短的路由透過歐盟服務連線將流量傳送出去。此路由案例也適用於使用路由彙總的網路。




您還可以將備份服務連線用於單一區域中的多個服務連線。下圖顯示了在北美區域具有兩個服務連線的 Prisma Access 部署。在此情況下，您會指定 US-E 的 **Backup SC**（備份 **SC**）進行 US-W 服務連線，反之亦然，以確保對稱路由。




 ©2025 Palo Alto Networks, Inc.

# 設定路由偏好設定

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

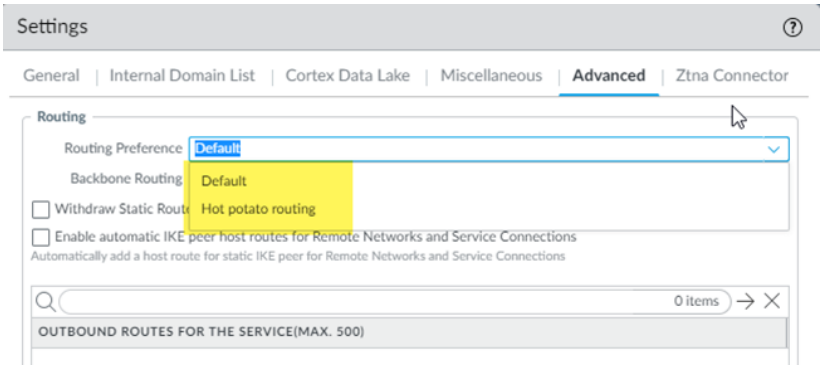
若要啟用路由偏好設定，請完成以下步驟。

若要設定這些路由偏好設定，您必須使用 *BGP* 路由而不是靜態路由進行服務連線。

**STEP 1 |** 設定您的服務連線。

**STEP 2 |** （選用）選取用於服務連線的路由。

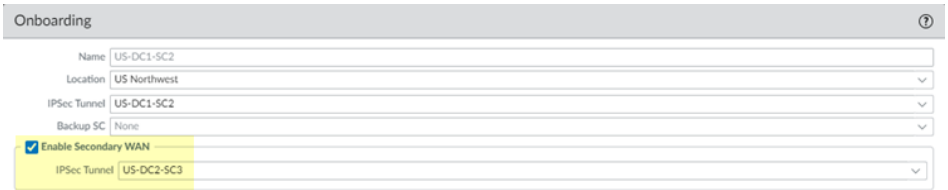
1. 從管理 Prisma Access 的 Panorama 中，前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定），然後按一下齒輪以編輯 **Settings**（設定）。
2. 在 **Advanced**（進階）設定中，選取您的 **Routing Preference**（路由偏好設定）（**Default**（預設值）或 **Hot Potato**（熱馬鈴薯））。




**STEP 3 |** （選用，僅限熱馬鈴薯路由部署）若要指定要在連結失敗時使用的偏好服務連線，請在設定服務連線時設定 **Backup SC**（備份 **SC**）。

您可以選取已新增的任何服務連線。Prisma Access 會使用您選取的 **Backup SC**（備份 **SC**）作為連線失敗時的偏好服務連線。選取備份服務連線可以防止非對稱路由問題（如果您啟用兩個以上的服務連線）。此選擇僅適用於熱馬鈴薯路由模式。

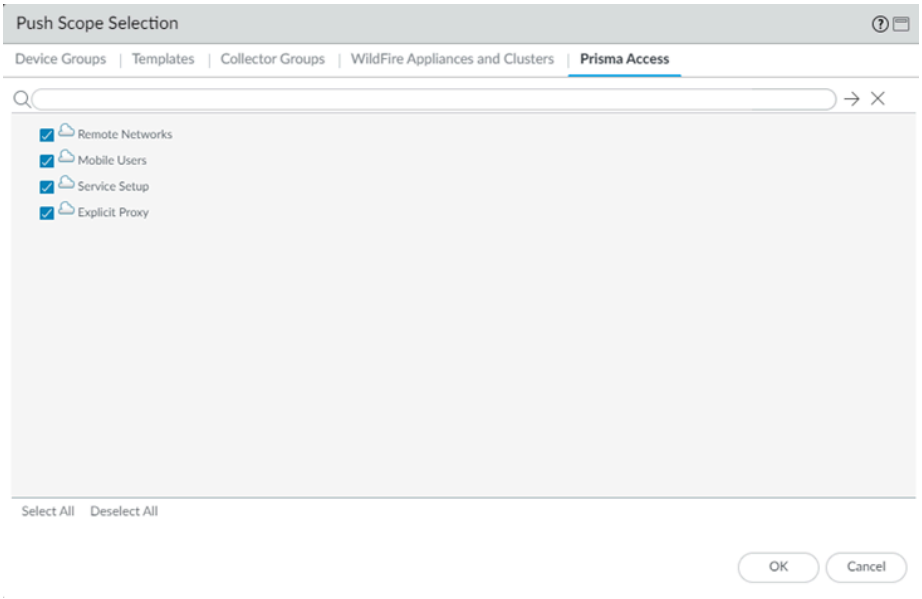
1. 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Connection**（服務連線）
2. 選取要設定的服務連線，或 **Add**（新增）連線。
3. 選取一個服務連線用作偏好備份（**Backup SC**（備份 **SC**））。




 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 將您的變更提交到 Panorama，並將設定變更推送到 Prisma Access。

1. 按一下 **Commit**（提交） > **Commit and Push**（提交並推送）。
2. **Edit Selections**（編輯選取項目），並在 Prisma Access 頁籤中，確保在 **Push Scope**（推送範圍）中選取了 **Service Setup**（服務設定），然後按一下 **OK**（確定）。

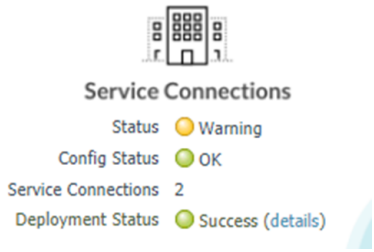



3. 按一下 **Commit and Push**（提交並推送）。


©2025 Palo Alto Networks, Inc.

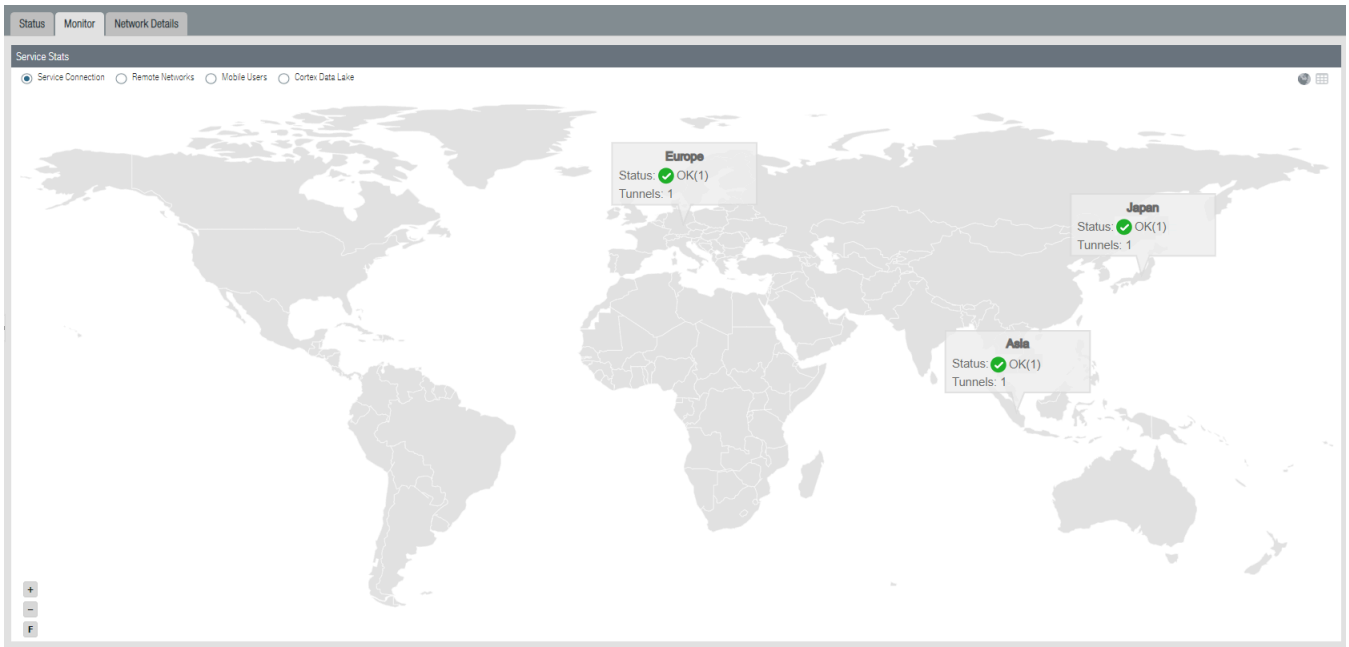
**STEP 5 |** 透過選取 **Panorama > Cloud Services > Status > Status**（**Panorama >** 雲端服務 **>** 狀態 **>** 狀態），並檢查其狀態是否 **OK**（成功），驗證您的服務連線是否已啟動。

**Deployment Status**（部署狀態）區域允許您在完成裝載和部署工作之前檢視其進度，以及查看有關已完成工作狀態的詳細資訊。



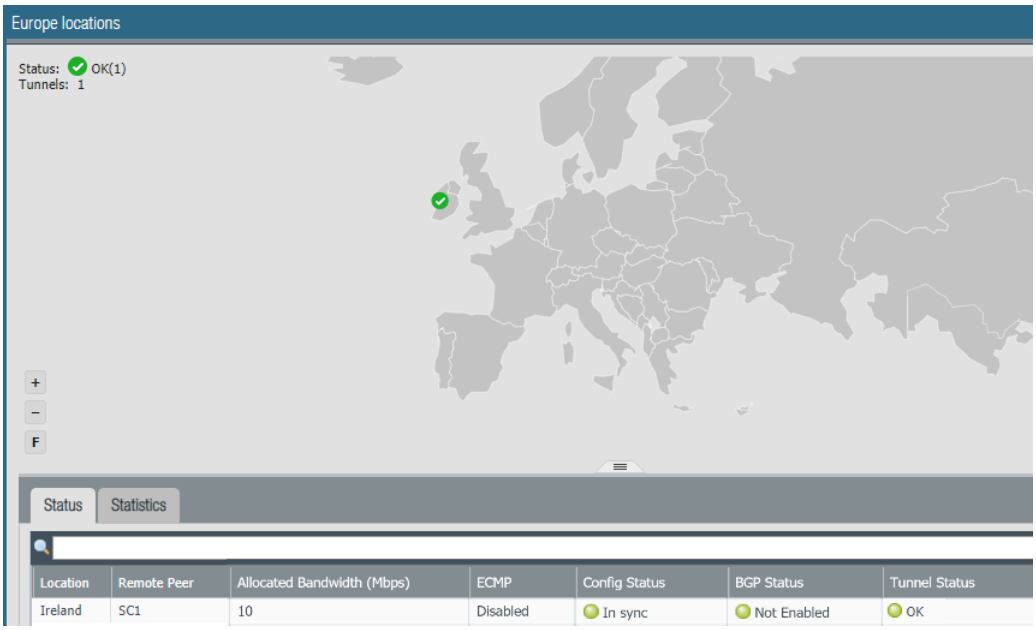

如果狀態不是 **OK**（成功），請將游標暫留在狀態圖示上，以檢視任何錯誤。

若要查看服務連線的圖形表示法，以及狀態詳細資訊，請選取 **Monitor**（監控）頁籤上的 **Service Connection**（服務連線）。




選取一個區域，以取得更多有關該區域的詳細資訊。


©2025 Palo Alto Networks, Inc.




按一下地圖下方的頁籤，以查看有關服務連線的其他資訊。

**Status**（狀態）頁籤：

- **Location**（位置）—服務連線的部署位置。
- **Remote Peer**（遠端對等）—此服務基礎結構設定 IPsec 通道的公司位置。
- **Allocated Bandwidth**（已配置頻寬）—您已配置的服務連線數目乘以 300 Mbps。

  此數目並不會反映可用的服務連線頻寬。

  雖然每個服務連線提供大約 *1 Gbps* 的輸送量，但實際的輸送量取決於幾個因素，包括：

  - 流量混合（例如，框架大小）
  - 服務連線與總部位置或資料中心之間的延遲和封包丟失
  - 服務提供者效能限制
  - 客戶終端裝置效能限制
  - 其他客戶資料中心流量
- **ECMP**—如果您為此服務連線設定了相等成本的多重路徑 (ECMP)。由於 ECMP 不是用於服務連線，因此這個狀態為 **Disabled**（已停用）。
- **Config Status**（設定狀態）—上次推送設定到服務的狀態。如果本機設定和雲端中的設定相符，則設定狀態為 **In sync**（同步）。如果您已在本機進行了變更，但尚未將設定推送到雲端，這可能會顯示狀態 **Out of sync**（不同步）。將游標暫留在狀態指示器上，以取得更

 ©2025 Palo Alto Networks, Inc.

多的詳細資訊。在提交並推送設定到 Prisma Access 之後，設定狀態會變更為 **In sync**（同步）。

- **BGP Status**（**BGP** 狀態）—顯示有關公司/總部位置的防火牆或路由器與服務連線建立所在的 Prisma Access 之間的 BGP 狀態的相關資訊。雖然您可能會通過各種 BGP 狀態（**idle**（閒置）、**active**（作用中）、**open send**（開啟傳送）、**open pend**（開啟擱置）、**open confirm**（開啟確認））暫時看到狀態，但 BGP 狀態最常顯示：
  - **Connect**（連線）—資料中心/總部的路由器正在嘗試與 Prisma Access 建立 BGP 對等關係。


©2025 Palo Alto Networks, Inc.

- **Established**（已建立）—已建立 BGP 對等關係。

此欄位還將顯示 BGP 連線是否處於錯誤狀態：

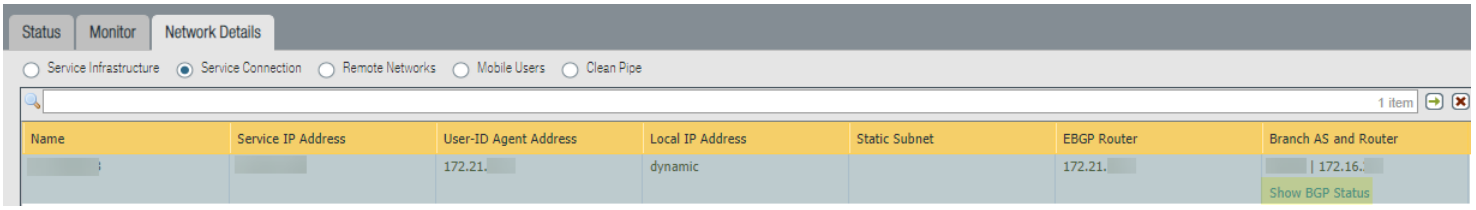
- **Warning**（警告）—超過 8 分鐘未更新 BGP 狀態。這可能表示防火牆中斷。
- **Error**（錯誤）—BGP 狀態未知。

- **Tunnel Status**（通道狀態）—Prisma Access 與服務連線之間連線的操作狀態。

**Statistics**（統計資料）頁籤：

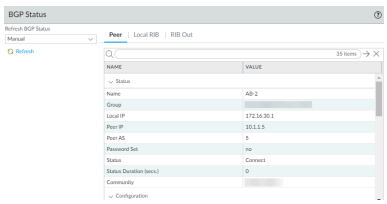
- **Location**（位置）—服務連線的部署位置。
- **Remote Peer**（遠端對等）—服務連線設定 IPsec 通道的公司位置。
- **Ingress Bandwidth (Mbps)**（進入頻寬 **(Mbps)**）—從總部/資料中心位置到 Prisma Access 的頻寬。
- **Ingress Peak Bandwidth (Mbps)**（進入峰值頻寬 **(Mbps)**）—從總部/資料中心位置進入雲端服務的峰值負載。
- **Egress Bandwidth (Mbps)**（輸出頻寬 **(Mbps)**）—從 Prisma Access 進入總部/資料中心位置的頻寬。
- **Egress Peak Bandwidth (Mbps)**（輸出峰值頻寬 **(Mbps)**）—從 Prisma Access 進入總部/資料中心位置的峰值負載。
- **QoS**—選取此按鈕以顯示圖形圖表，其中顯示即時和歷史 QoS 統計資料，包括每個類別丟棄的封包數目。此圖表僅為已啟用 QoS 的服務連線或遠端網路連線顯示。

如果您設定了 BGP，則可以選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Service Connection**（服務連線） > **Show BGP Status**（顯示 **BGP** 狀態）來檢查其狀態。




[BGP Status（BGP 狀態）] 對話方塊隨即顯示。此表格為您提供下列資訊：

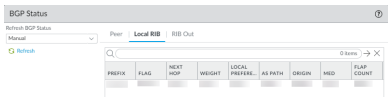
- 對等—BGP 對等的路由資訊，包括狀態、路由總數、設定，以及執行階段統計資料和計數器。路由總數會顯示在 **bgpAfiIpv4-unicast Counters**（**bgpAfiIpv4-unicast** 計數器）區域的 **Incoming Total**（傳入總數）和 **Outgoing Total**（傳出總數）欄位中。



- 本機 **RIB**—Prisma Access 在本機使用的 BGP 路由。Prisma Access 會從 BGP RIB-In 表格（其中儲存了鄰近網路裝置傳送的資訊）中選取此資訊、套用本機 BGP 匯入政策和路由決策，並將本機 RIB 資訊儲存在路由資訊庫 (RIB) 中。

 ©2025 Palo Alto Networks, Inc.

請注意，只會顯示前 256 個項目。若要檢視其他項目，請在 [Filter（篩選器）] 欄位中輸入子網路或 IP 位址，然後按一下 [Apply Filter（套用篩選器）]，檢視最多 256 個路由項目的子集。




- **RIB** 輸出—Prisma Access 透過 BGP 更新訊息公告至其對等的路由資訊。

## 使用多個服務連線建立高頻寬網路

如果您的總部或資料中心位置需要額外的服務連線頻寬，則可以設定該位置的多個服務連線。

每個 Prisma Access 服務連線沒有頻寬上限，但 Palo Alto Networks 預計每個服務連線可以提供大約 1Gbps 的輸送量。雖然此頻寬通常足以存取總部或資料中心位置的內部資源，但您的部署可能需要額外的頻寬；例如，如果您在資料中心託管內部或私人 SaaS 應用程式。

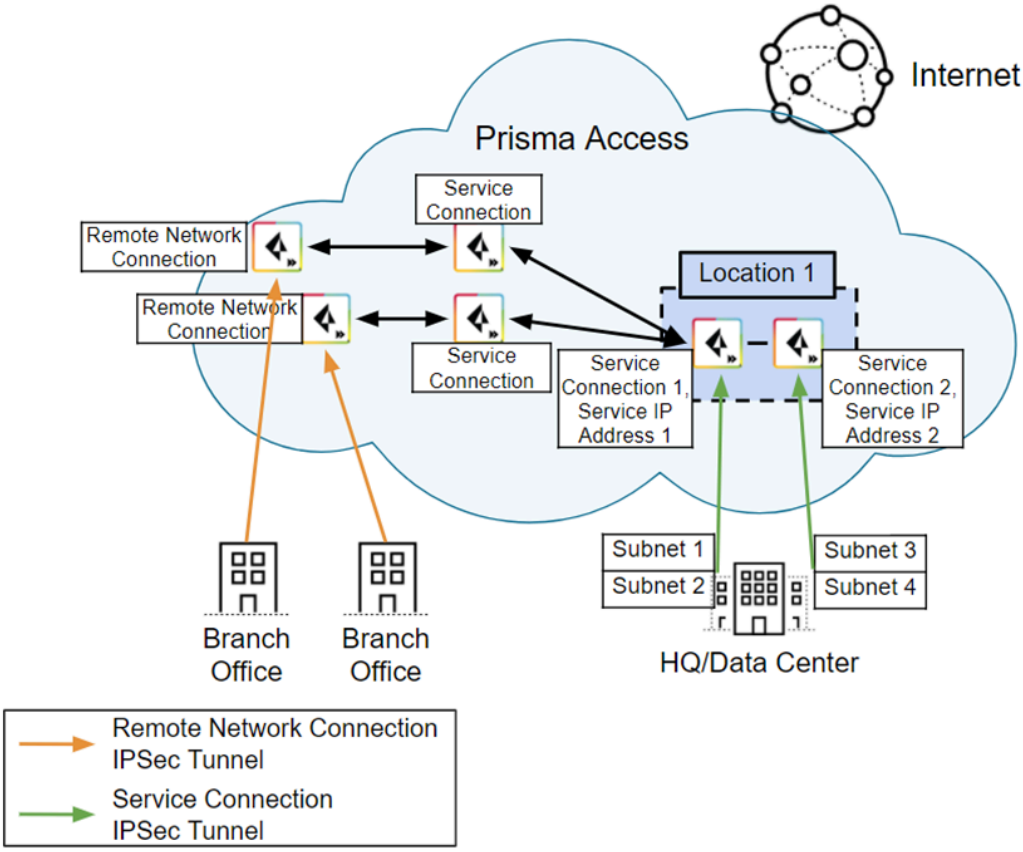
若要建立總部或資料中心網站的高頻寬服務連線，請使用同一 Prisma Access 位置的多個服務連線來裝載該網站。

雖然 *Prisma Access* 不限制您可以裝載到單一總部或資料中心遠端網路位置的服務連線數目上限，但 *Palo Alto Networks* 建議在高頻寬部署中使用的服務連線不要超過四個。如果您需要更多頻寬來存取內部應用程式，請使用 ZTNA 連接器或 Colo-Connect 連接器 而不是多個服務連線。

下圖顯示一個 Prisma Access 遠端網路部署，其中總部或資料中心網站具有來自同一 Prisma Access 網站位置的兩個服務連線，有效地在網站與 Prisma Access 位置之間提供 2 Gbps 頻寬。

除了為高頻寬存取而部署的服務連線之外，該圖還顯示了另一組服務連線。這些服務連線為 Prisma Access 提供正常的路由功能（在此圖中，它們提供遠端網路連線與高頻寬服務連線之間的內部路由存取）。Palo Alto Networks 建議，在部署高頻寬連線時，保留服務連線以提供對總部或資料中心位置中資源的存取，並部署其他服務連接以用於遠端網路、行動使用者和資料中心資源之間的內部路由。


©2025 Palo Alto Networks, Inc.




每個服務連線都是作用中，並且有自己的 **Service IP Address**（服務 **IP** 位址）；您可以使用該位址終止每個服務連線的 IPSec 通道。

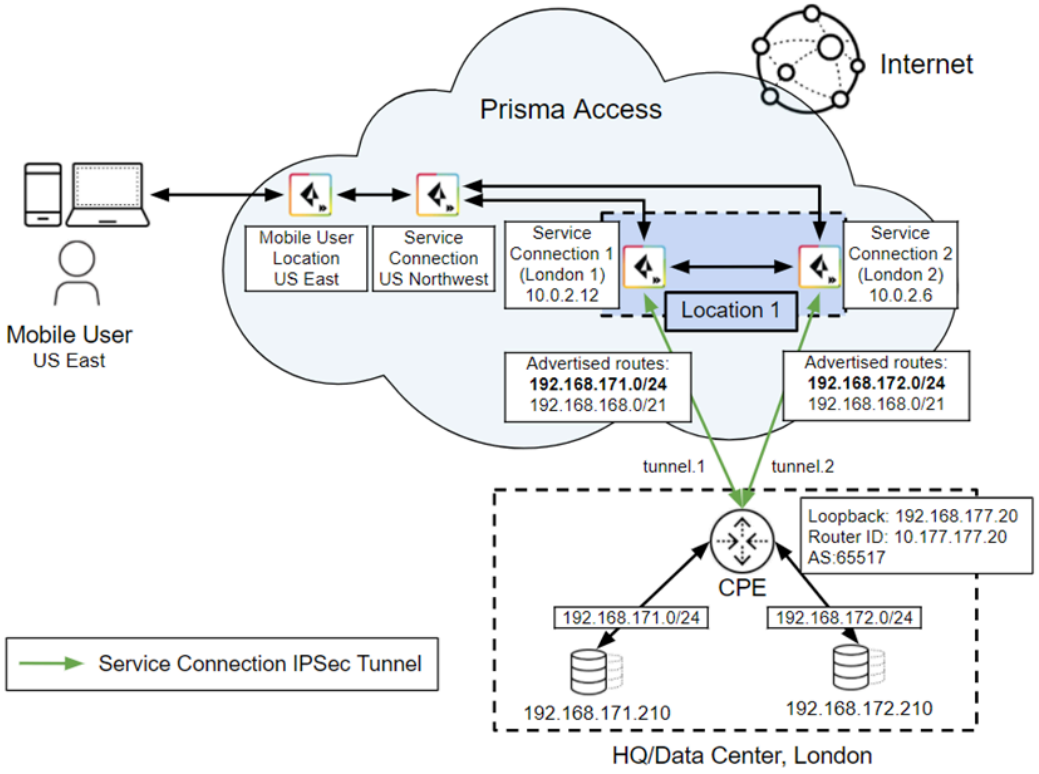
## 建立總部或資料中心位置的高頻寬連線

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

若要設定單一總部或資料中心位置的多個服務連線，請完成下列步驟。

本節中的步驟會使用部署範例，如下圖所示。在此範例中，倫敦總部位置使用兩個不同的 IPsec 通道連線到兩個不同的服務連線（倫敦 1 和倫敦 2），這些通道是在兩個不同的客戶周邊設備 (CPE) 介面（通道 1 和通道 2）上終止。


©2025 Palo Alto Networks, Inc.




此範例和本節中的步驟會使用新世代防火牆，來終止 CPE 上的服務連線；不過，您可以使用支援對稱路由和 PBF 或政策型路由的任何 CPE 作為 CPE。

請使用這些步驟作為指引；每個使用案例可能需要超出本文件範圍的額外設計和計劃。

**STEP 1 |** 在您將多個服務連線從單一 Prisma Access 位置部署至單一網站之前，請確定您的網路具有下列先決條件：

- 您必須在總部或資料中心位置分割子網路，並在每個服務連線上公告唯一的子網路。
- 您的客戶周邊設備 (CPE) 必須支援下列網路功能，且您必須能夠設定這些功能：
  - 政策型轉送 (PBF) 或政策型路由—您的 CPE 必須能夠選擇性地為特定本機來源 IP 位址和子網路挑選特定路徑。
  - 對稱傳回—您必須能夠設定 CPE，以確保流入和流出特定 IP 位址和子網路的流量對稱，並在其中一個通道失效時，為容錯移轉通道設定對稱傳回。

**STEP 2 |** 建立服務連線，並為用於服務連線的 IPsec 通道建立連線。

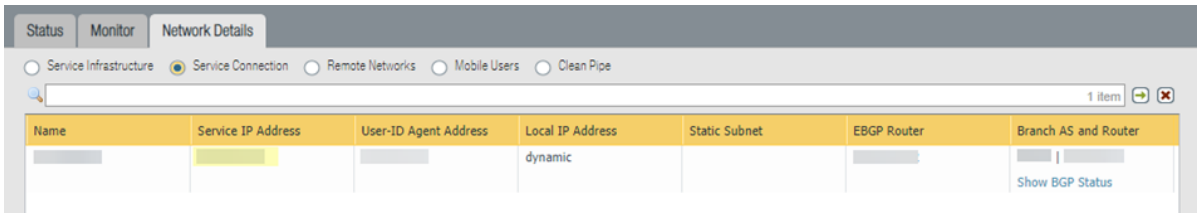
1. 在管理 Prisma Access 的 Panorama 上，設定服務連線，包括建立新的 IPSec 通道設定、IKE 閘道、IPSec 密碼設定檔和通道監控設定。

   *Prisma Access* 提供預先定義的 IPsec 範本，您可以用來簡化 *IPsec* 通道建立程序。

2. 尋找要作為從 CPE 到 Prisma Access 的 IPSec 通道的 IP 位址，方法是選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資

 ©2025 Palo Alto Networks, Inc.

訊）、按一下 **Service Connection**（服務連線）選項按鈕，然後記下網站的 **Service IP Address**（服務 **IP** 位址）。




3. 在您的 CPE 上，建立服務連線的 IPsec 通道

   1. 驗證 IKE 和 IPsec 通道是否使用相同的密碼設定檔，進行對等之間的驗證和加密。
   2. 使用 **Service IP Address**（服務 **IP** 位址）作為通道的對等 IP 位址。

   如果您使用新世代防火牆作為 CPE，請選取 **Network**（網路） > **IPSec Tunnels**（**IPSec** 通道），並為服務連線建立兩個通道（以下螢幕擷取畫面中的 **tunnel.1** 和 **tunnnel.2**）。




**STEP 3 |** 為 CPE 建立虛擬路由器設定。

您可以建立 BGP 路由執行個體，在一個通道上公告一個子網路，而在另一個通道上公告其他子網路，從而確保兩個作用中通道上的負載平衡。

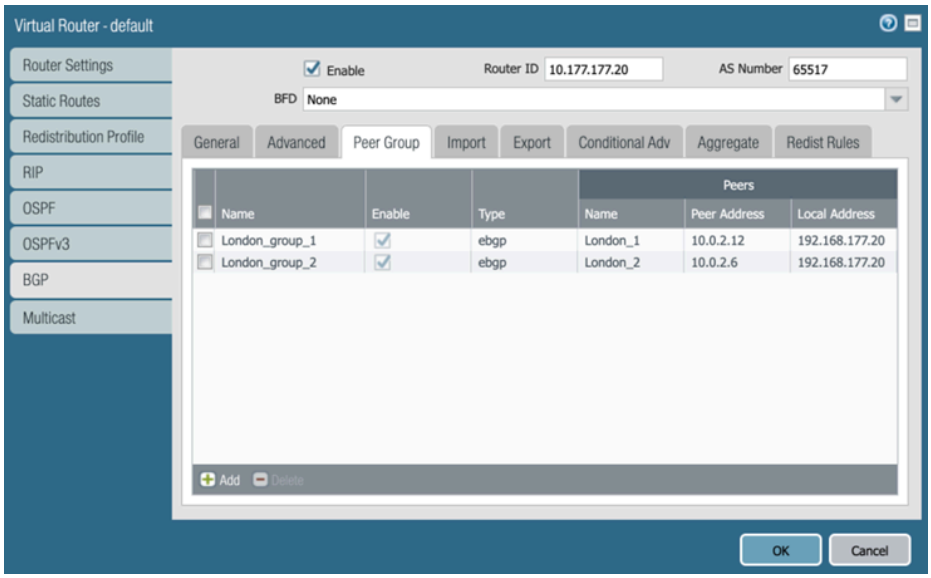
如果您使用新世代防火牆作為 CPE，請選取 **Network**（網路） > **Virtual Routers**（虛擬路由器）、**Add**（新增）虛擬路由器設定，然後為每個通道**Add**（新增）**BGP Peer Group**（對等群組），指定下列設定：

- 指定 CPE 路由器的 **Router ID**（路由器 **ID**）和 **AS Number**（**AS** 編號）（在本範例中，分別為 10.177.177.20 和 65517）。
- 指定服務連線的 **EEBGP Router**（**BGP** 路由器）位址（**Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Service Connection**（服務連

 ©2025 Palo Alto Networks, Inc.

線） > **EBGP Router**（**EBGP** 路由器））作為服務連線的 **Peer Address**（對等位址）（在本範例中，10.0.2.12 用於服務連線 1，10.0.2.6 用於服務連線 2）。

- 對於 **Local Address**（本機位址），您可以指定 CPE 的回送位址（本範例中的 192.168.177.20）。




**STEP 4 |** 為用於兩個通道的 IP 位址建立彙總的子網路。

提供彙總的子網路可確保備援。當兩個通道啟動時，流量會使用最具體的路由來到達其目的地；例如，192.168.171.0/24 使用 Tunnel.1 來到達其目的地。新增涵蓋所有公告子網路的彙總子網路（本範例中的 192.168.168.0/21）確保 192.168.171.0/24 的流量可從 tunnel.2 到

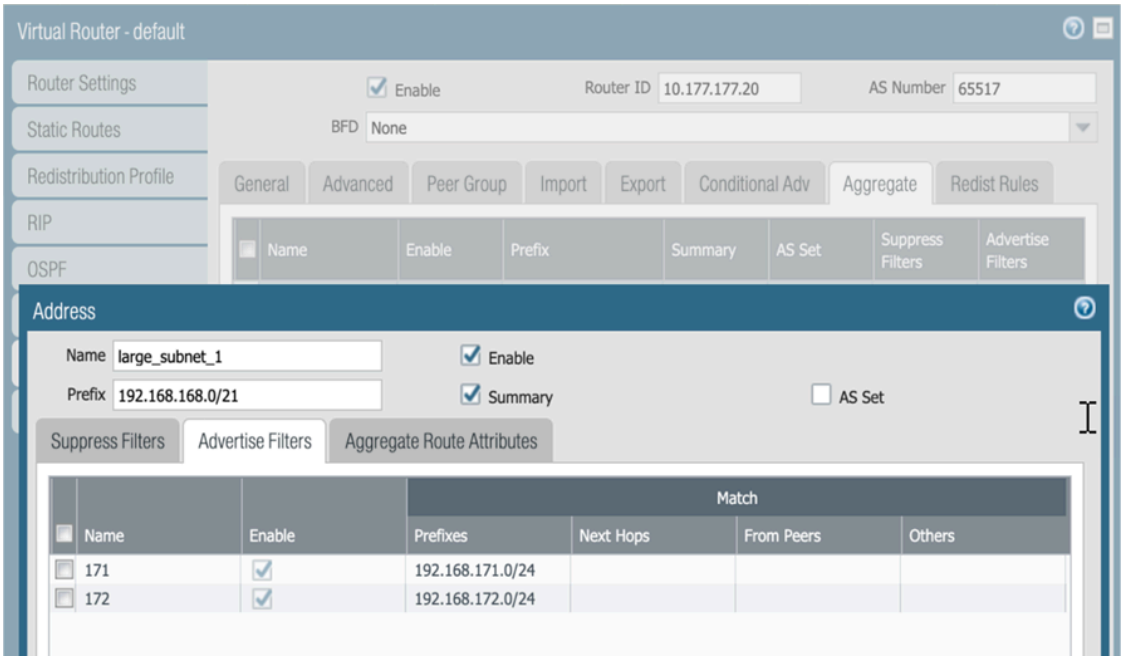
 ©2025 Palo Alto Networks, Inc.

達（如果 tunnel.1 失效），而 192.168.172.0/24 的流量可從 tunnel.1 到達（如果 tunnel.2 失效）。

如果您使用新世代防火牆作為 CPE，請完成下列步驟。

1. 繼續修改虛擬路由器設定檔，並 **Add**（新增）路由彙總參數（**Network**（網路） > **Virtual Routers**（虛擬路由器） > **BGP** > **Aggregate**（彙總））。
2. 為您針對服務連線公告的子網路輸入摘要子網路。

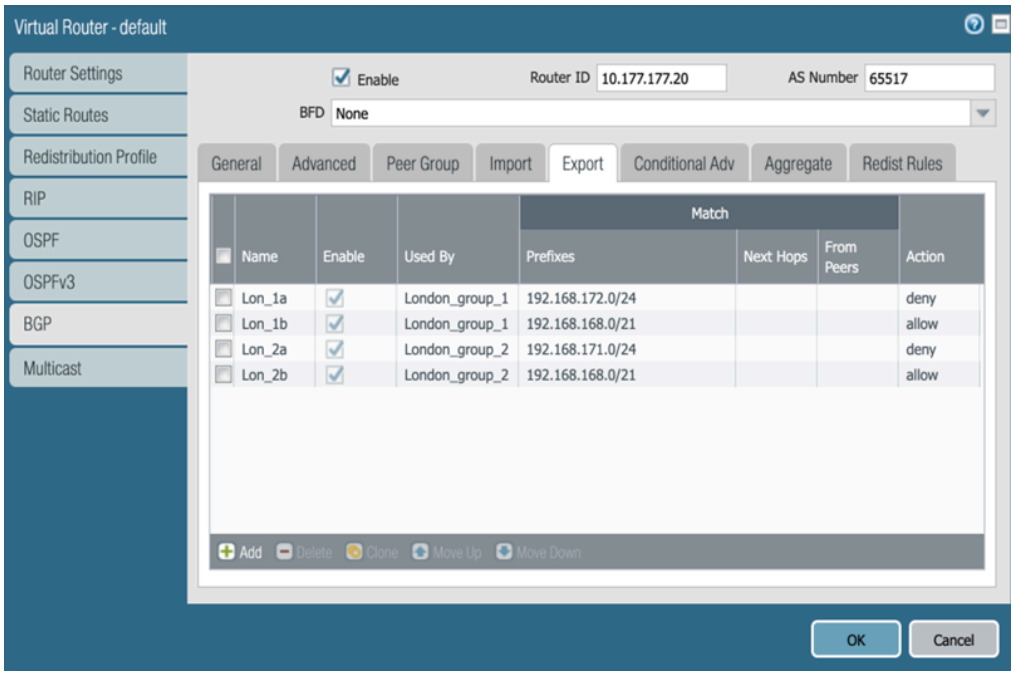
   在此範例中，輸入 **Prefix**（首碼）為 **192.168.168.0/21**，其中彙總了兩個資料中心子網路。




3. 輸入 **Export**（匯出）設定，以確保通道公告正確的子網路。

   在此範例中，您可以指定子網路的 **Action**（動作）為 **deny**（拒絕）和 **allow**（允許），以便第一個子網路 (192.168.171.0/24) 可從 tunnel.1 到達，而第二個子網路 (192.168.172.0/24) 可從以從 tunnel.2 到達。

 ©2025 Palo Alto Networks, Inc.

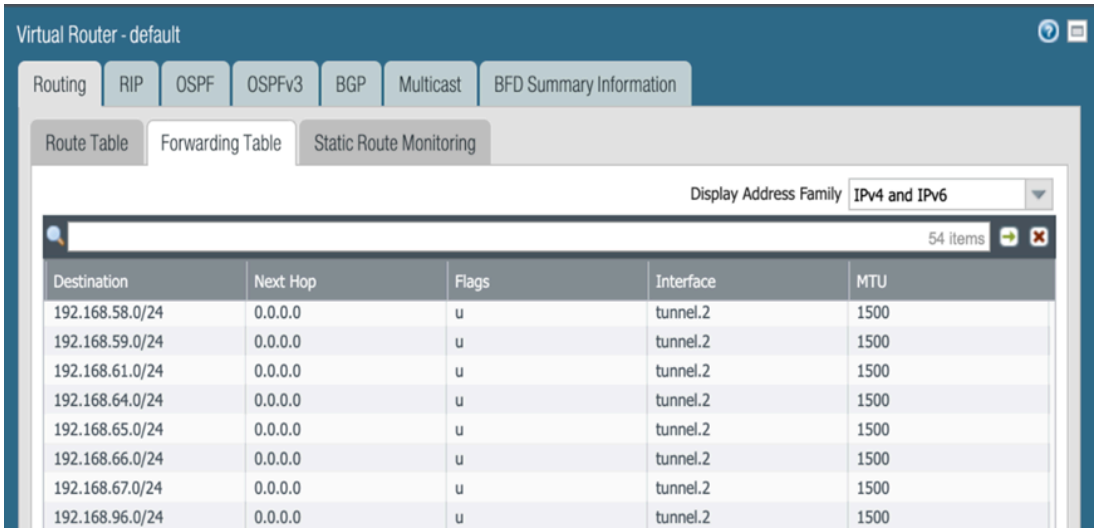



**STEP 5 |** （僅限兩個以上服務連線的部署）如果您需要兩個以上的服務連線，才能將使用者連接至超過 2 Gbps 頻寬的私人資源，請為匯出路由新增 AS-PATH 前置項，以便服務連線在容錯移轉時使用對稱路由進出資料中心。如需詳細資料，請參閱 設定兩個以上與總部或資料中心位置的服務連線。


©2025 Palo Alto Networks, Inc.

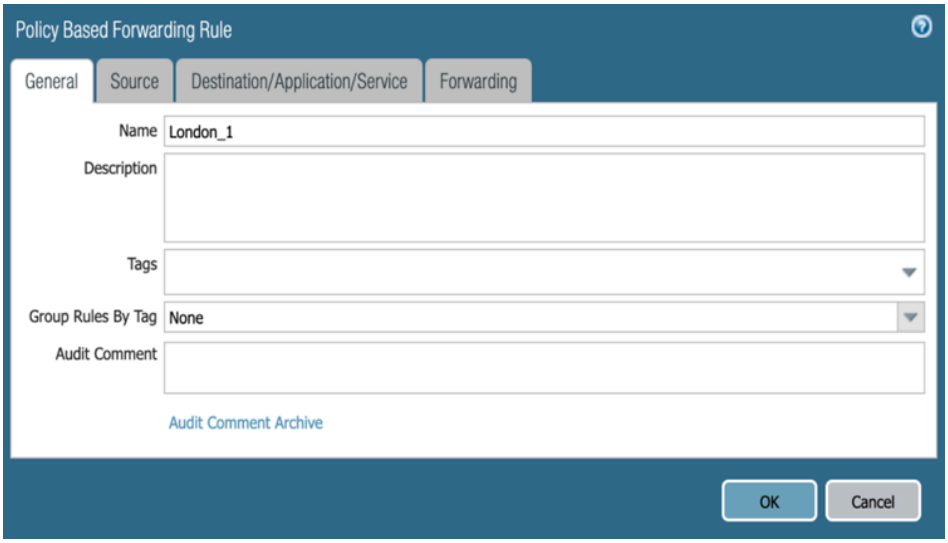
**STEP 6 |** 為了確保對稱傳回（確保 192.168.171.0/24 的流量一律使用 tunnel.1，而 192.168.172.0 的流量一律使用 tunnel.2），請輸入 PBF 或政策型路由規則。

根據預設，無論偏好的通道為何，BGP 都會為所有不同的目的地安裝路由表中的路由。以下螢幕擷取畫面顯示，BGP 公告所有目的地來自 tunnel.2 的 192.168.168.0/21 子網路，這可能會導致 192.168.171.0/24 的流量進行不對稱路由。




若要確保對稱路由，請設定一組 PBF 或路由型轉送規則。如果您使用新世代防火牆作為 CPE，請完成下列步驟。

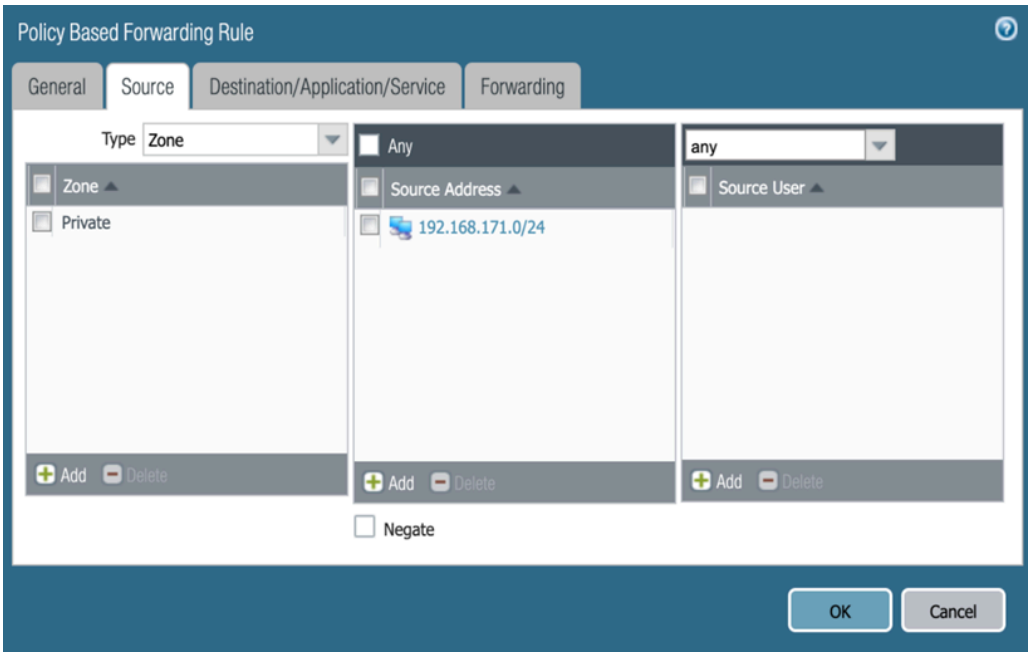
1. 選取 **Policies**（原則） > **Policy Based Forwarding**（基於原則的轉送），然後 **Add**（新增）PBF 原則規則。



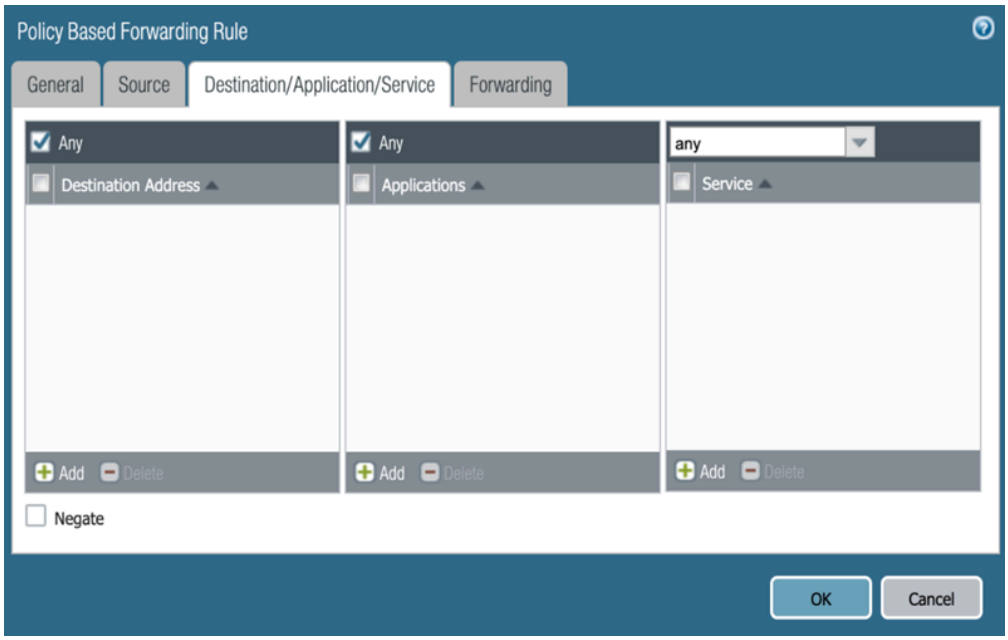

2. 選取 **Source**（來源），並**Add**（新增）要用於 PBF 的 **Source Address**（來源位址）。

   在此情況下，您想要為 tunnel.1 建立一個 PBF，因此您輸入 192.168.171.0/24 子網路。

 ©2025 Palo Alto Networks, Inc.




3. 選取 **Destination/Application/Service**（目的地/應用程式/服務），然後選取 **Any**（任何）目的地位址和 **Any**（任何）應用程式。

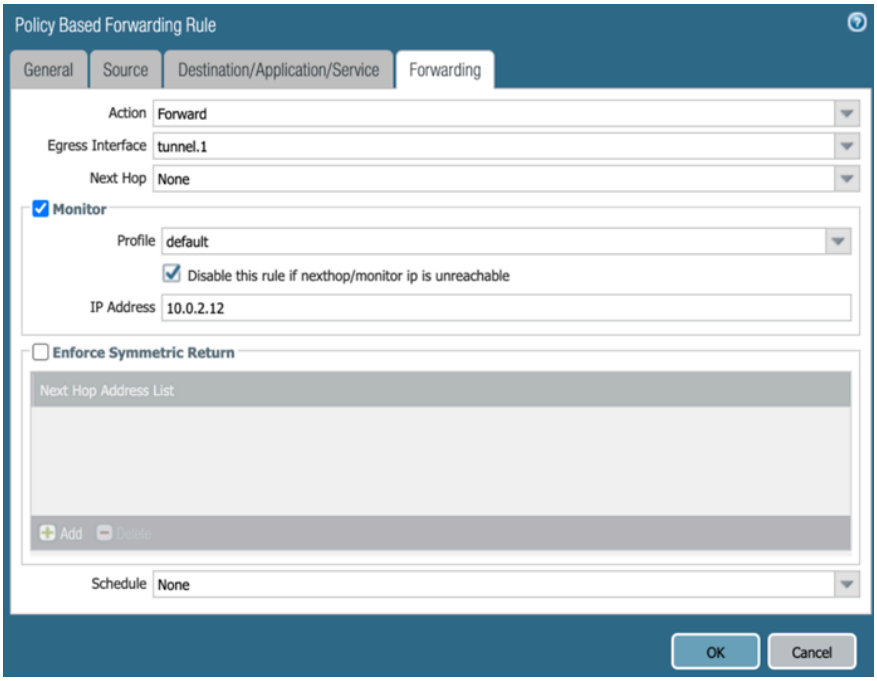



4. 選取 **Forwarding**（轉送）並指定下列參數；然後按一下 **OK**（確定）：
   - 選取 **Action**（動作）為 **Forward**（轉送）。
   - 選取通道的 **Egress Interface**（輸出介面），您想要將 IP 子網路轉送至該通道（本案例中的 **tunnel.1**）。
   - 選取 **Monitor**（監控），然後選取下列監控設定檔：
     - 選取 **Profile**（設定檔）為 **default**（預設值）。


©2025 Palo Alto Networks, Inc.

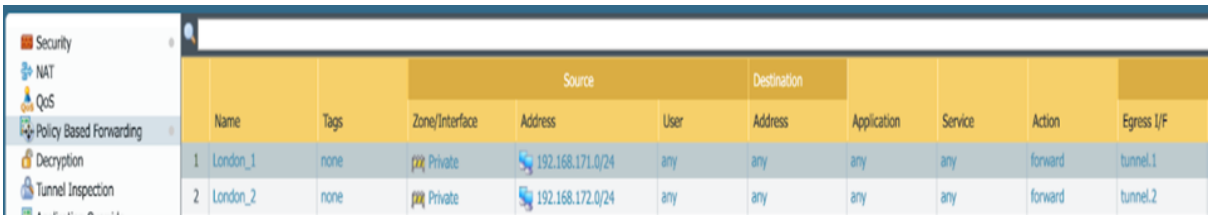
- 選取 **Disable this rule if nexthop/monitor ip is unreachable**（如果無法連線下一個躍點/監控 **ip** 則停用此規則）。
- 指定服務連線 **EBGP Router**（**EBGP** 路由器）位址的 **IP Address**（**IP** 位址）（**Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Service Connection**（服務連線） > **EBGP Router**（**EBGP** 路由器））。

啟用監控並選取服務連線的 EBGP 路由器位址，可確保如果 tunnel.1 失效，防火牆會停用 PBF 政策，並路由仍啟動的通道 (tunnel.2) 上的流量。




5. 重複步驟 6，將服務連線 1 的 **EBGP Router**（**EBGP** 路由器）位址替換為服務連線 2 的 **EBGP Router**（**EBGP** 路由器）位址，而將 tunnel.1 的子網路替換為 tunnel.2 的子網路。

   完成時，您有兩個 PBF 政策，一個用於 tunnel.1，另一個則用於 tunnel.2。

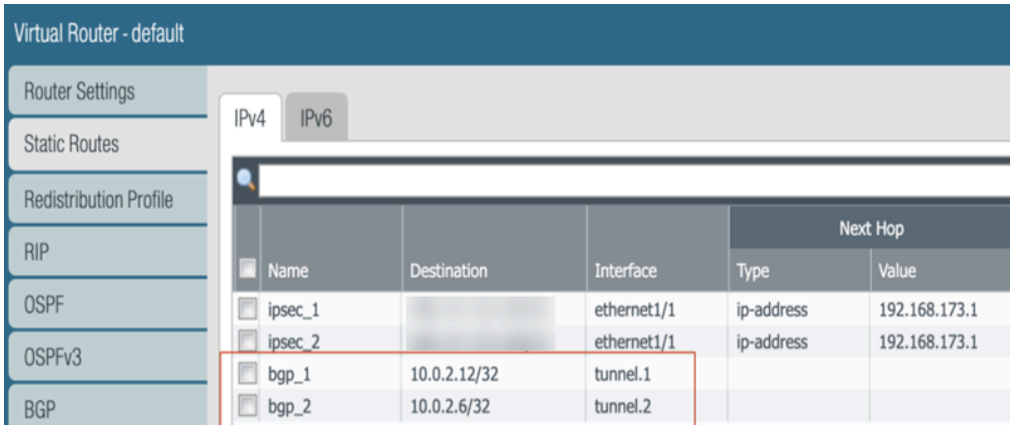



**STEP 7 |** 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器） > **Static Routes**（靜態路由），並將服務連線 1 的 **EBGP Router**（**EBGP** 路由器）位址指派給 **tunnel.1** 的 **Interface**（介面），

 ©2025 Palo Alto Networks, Inc.

然後將服務連線 2 的 **EBGP Router**（**EBGP** 路由器）位址指派給 **tunnel.2** 的 **Interface**（介面）。

為每個路由器 BGP 位址輸入特定的靜態路由，可確保通道監控運作正常，因為服務連線 1 的 EBGP 路由器 IP 位址只能透過 tunnel.1 到達，而服務連線 2 的 EBGP 路由器 IP 位址只能透過 tunnel.2 到達。




## 設定兩個以上與總部或資料中心位置的服務連線

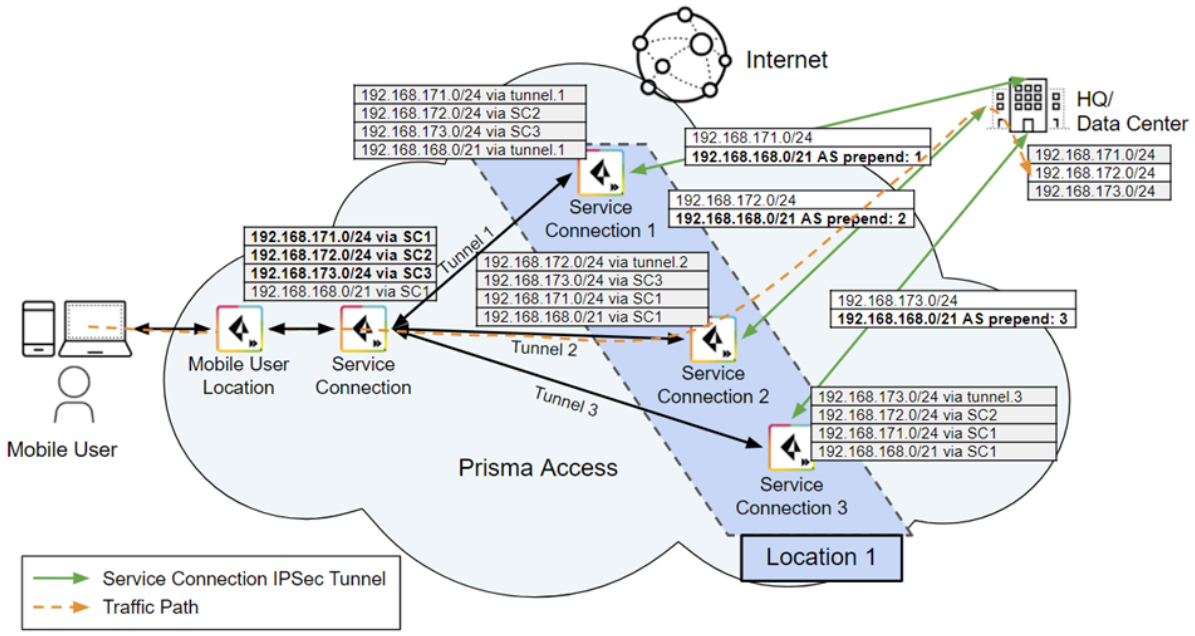
| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

當您使用兩個通道進行高頻寬服務連線時，若通道故障，只留下一個可用的流量路徑，這簡化了容錯移轉路徑的設定。如果您使用兩個以上的連線進行高頻寬連線，則需要執行其他設定，以確保通道容錯移轉的行為一致。

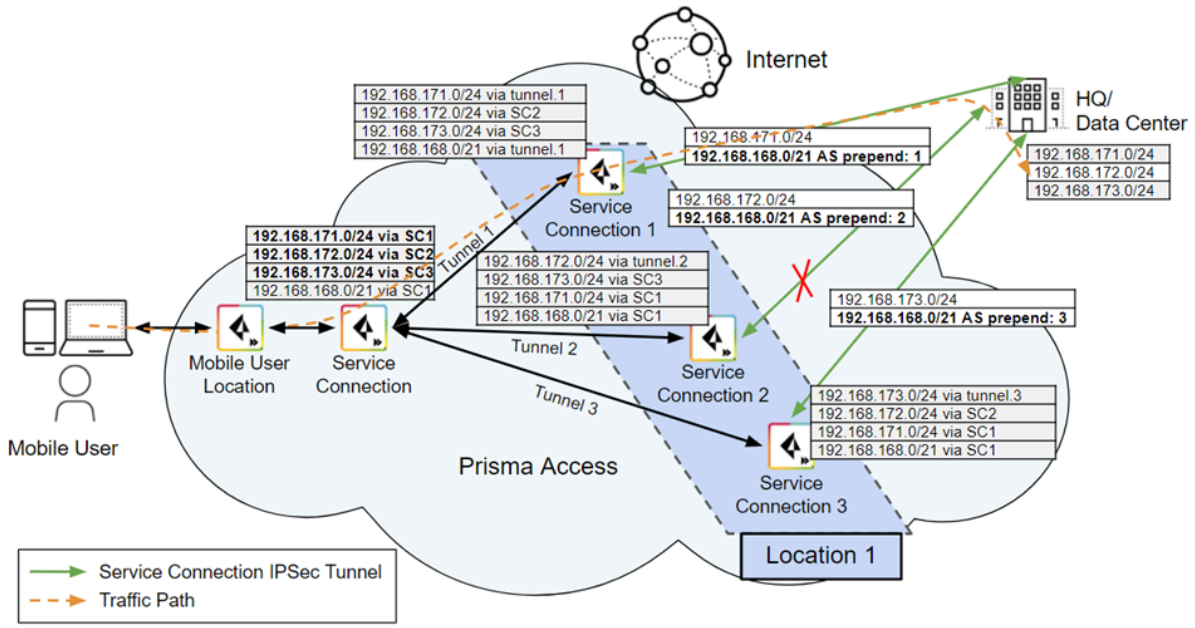
因為您使用彙總的子網路進行通道容錯移轉，所以必須明確指出在發生容錯移轉時要使用的服務連線通道。由於 BGP 路由為路由選擇了最少數目的 AS-PATH，因此您可以在 AS-PATH 前面加上路由，使 BGP 在容錯移轉時偏好通道。

下列範例為使用三個服務連線的高頻寬服務連線顯示路由表。如果所有三個通道都已啟動，Prisma Access 會使用更具體的路由連線到總部或資料中心位置的子網路。由於使用者正在存取 192.168.172.0/24 子網路中的資源，因此最靠近行動使用者的服務連線會檢查其路由表，並選取通道 2 作為資料中心資源的路徑。


©2025 Palo Alto Networks, Inc.




如果通道 2 中斷，則無法使用 192.168.172.0/24 子網路中資源的更具體路由，因此最接近使用者的服務連線會使用彙總的 192.168.168.0/21 子網路。您只為服務連線 1 設定了一個 AS-PATH 前置項；因此，Prisma Access 選擇通道 1 作為容錯移轉路徑，因為它具有較少的 AS-PATH 前置項。

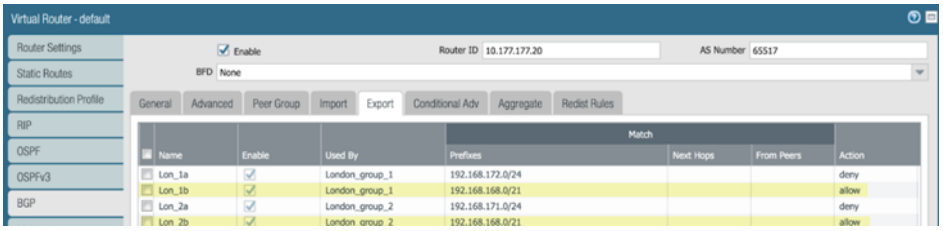



如果您使用新世代防火牆作為 CPE，若要將前置項新增至路由，請完成下列工作。

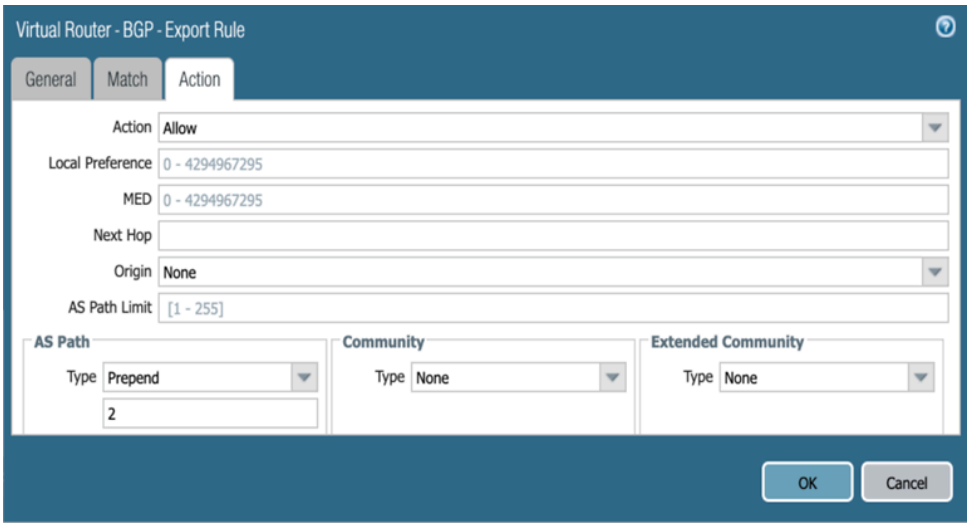
**STEP 1 |** 選取虛擬路由器 BGP 匯出設定檔（**Network**（網路） > **Virtual Routers**（虛擬路由器） > **BGP** > **Export**（匯出））。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 修改您在設定服務連線時建立的匯出規則，其中 **Action**（動作）為 **Allow**（允許）。




**STEP 3 |** 在 AS 路徑區域中，新增 **Prepend**（前置項），然後輸入要新增的 AS-PATH 前置項數目（本範例中 **2** 個）。




**STEP 4 |** 對於 **Action**（動作）為 **Allow**（允許）的每個匯出規則重複步驟 2 和 3，從而新增 AS-PATH 前置項，以符合您為部署規劃的容錯移轉案例。

在本節使用的範例中，您為服務連線 1 資料中心位置的通道新增 AS-PATH 前置項 1 (tunne.1)、為用於服務連線 2 的通道新增 AS-PATH 前置項 2 (tunne.2)，並為用於服務連線 3 的通道新增 AS-PATH 前置項 3 (tunne.3)。

完成後，此範例會在容錯移轉時使用下列通道：

- 如果 tunnel.2 或 tunnel.3 中斷，則對應子網路的流量會容錯移轉 Tunnel.1，該通道具有最短的公告 AS-PATH。
- 如果 tunnel.1 中斷，其子網路 (192.168.171.0/24) 的流量會容錯移轉到 Tunnel.2，該通道具有最短的公告 AS-PATH。

**STEP 5 |** 新增備份 PBF 或政策型路由政策，以在通道失敗時確保對稱傳回流量。

雖然 AS-PATH 前置項可確保從 Prisma Access 到資料中心的流量在容錯移轉時使用特定通道，但您還必須為從資料中心到 Prisma Access 的流量確保對稱傳回路徑。若要確保對稱傳回，請使用 PBF 或政策型路由政策，鏡像您為從資料中心到 Prisma Access 流量所建立的容錯移轉案例。

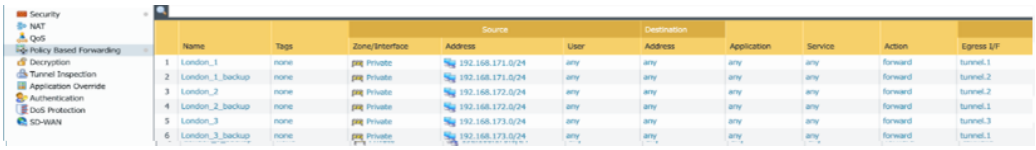
在此範例中，對於來源 IP 為 192.168.171.0/24 的 tunnel.1 流量，您會建立備份 PBF 政策，在發生容錯移轉時強制傳回流量以使用 tunnel.2。如果無法連線到通道監控 IP 位址，第一個 PBF

 ©2025 Palo Alto Networks, Inc.

規則會停用；當發生此容錯移轉時，CPE (本範例中的新世代防火牆) 會評估清單中的下一個規則。




然後，您可以新增更多 PBF 規則，以比對您為從資料中心到 Prisma Access 流量所建立的容錯移轉案例。




# 使用來源 NAT 保留服務連線的 User-ID 與 Device-ID 對應

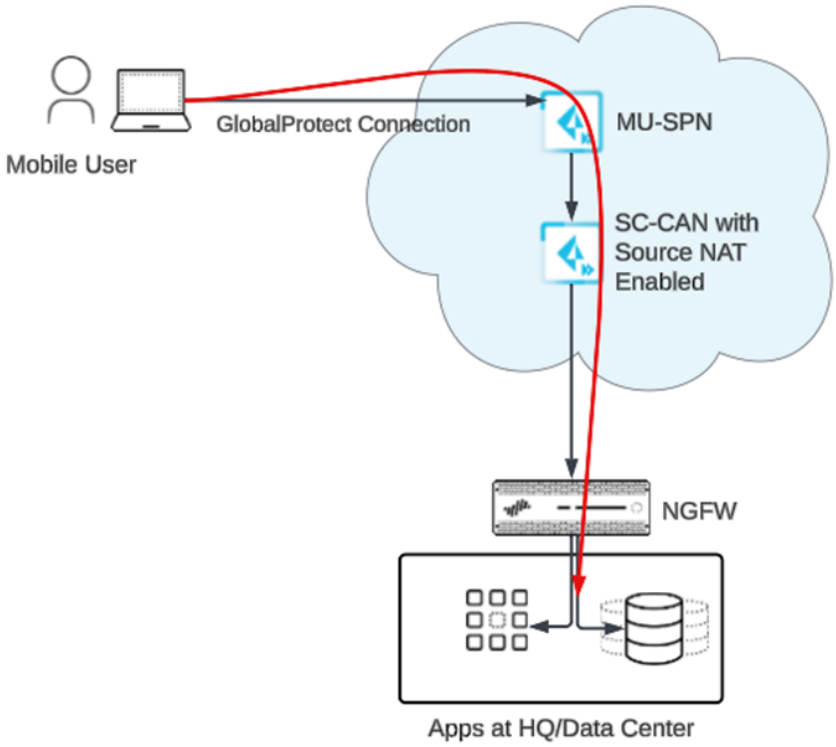
| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ 執行最低 PAN-OS 11.2 版的新世代防火牆 (NGFW)<br>❑ 此功能使用 Geneve 封裝。確保除了執行 PAN-OS 11.2 或更新版本的 NGFW 之外，任何下游防火牆都能夠解除 Geneve 封裝。<br>動態權限存取不支援此功能。 |

您可以在 Prisma Access 中使用服務連線（也稱為服務連線—企業存取節點 (SC-CAN)）來保護私人應用程式。若要根據 User-ID 或 Device-ID 限制對應用程式的存取權，您可以在私人應用程式所在的資料中心或總部位置部署新世代防火牆 (NGFW)；然後，在 NGFW 上根據 User-ID 對應、Device-ID 對應或兩者設定政策規則。

若要使用這些規則，NGFW 必須從 SC-CAN 接收 User-ID 或 Device-ID 對應；但是，如果使用者使用 GlobalProtect 連線到 Prisma Access 且 SC-CAN 啟用了 **Data Traffic source NAT**（資料流量來源 **NAT**），則 NGFW 無法取得此對應。如果在 SC-CAN 上啟用 **Data Traffic source NAT**（資料流量來源 **NAT**），它將在行動使用者 IP 位址集區上執行 NAT，並且不會在資料中心或總部位置公告這些 IP 位址。

在這種情況下，NGFW 無法擷取 GlobalProtect 使用者的 User-ID 或 Device-ID，這表示您無法根據 User-ID 或 Device-ID 強制執行政策。

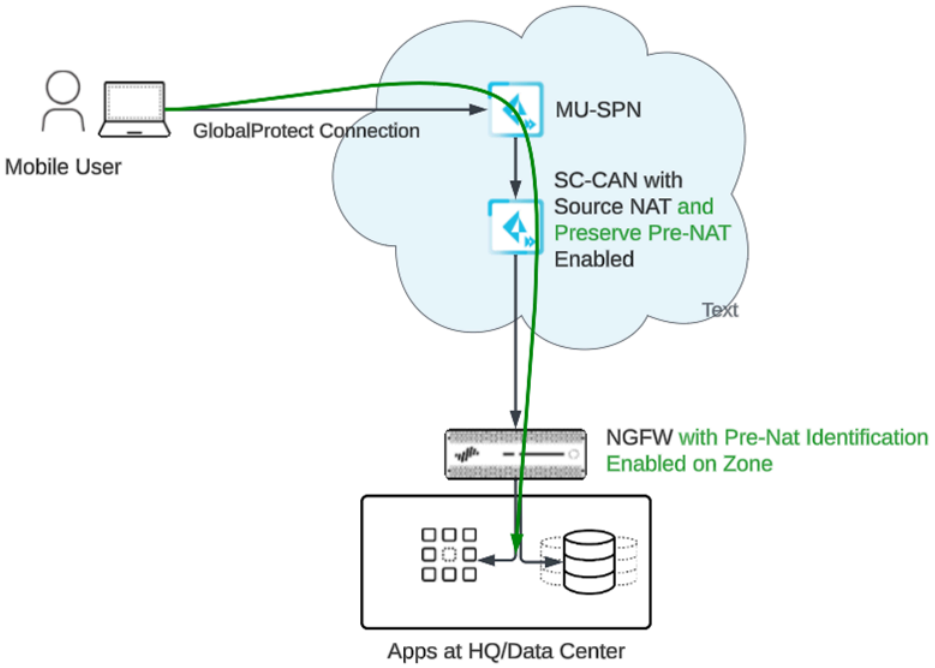
 ©2025 Palo Alto Networks, Inc.




若要確保您的網路將 User-ID 或 Device-ID 對應散佈到總部或資料中心，請完成下列其中一節中列出的參數，允許 NGFW 根據其從 GlobalProtect 得知的 User-ID 對應強制執行安全性政策規則。

需要最低 *PAN-OS* 版本為 *11.2* 的 *NGFW*。服務連線不必在 *NGFW* 上終止，而且只要 *NGFW* 位於服務連線終止位置的下游，就可以在另一台支援 *IPSec* 的裝置上終止。


©2025 Palo Alto Networks, Inc.




- Strata Cloud Manager
- Panorama

## 使用來源 NAT 保留服務連線的使用者與 Device-ID 對應 (Strata Cloud Manager)

若要讓 Prisma Access 將 User-ID 對應從 GlobalProtect 使用者散佈到 Prisma Access (Managed by Strata Cloud Manager) 中總部或資料中心的 NGFW，請完成以下步驟。

此程序假定您已準備好以下網路設定：

- 您已在服務連線上啟用 **Data Traffic source NAT**（資料流量來源 **NAT**）。
- 您已在私人應用程式所在的總部或資料中心部署了 NGFW。
- 您已根據您在 NGFW 中建立的區域為 NGFW 上的 Prisma Access 套用了安全性政策規則。

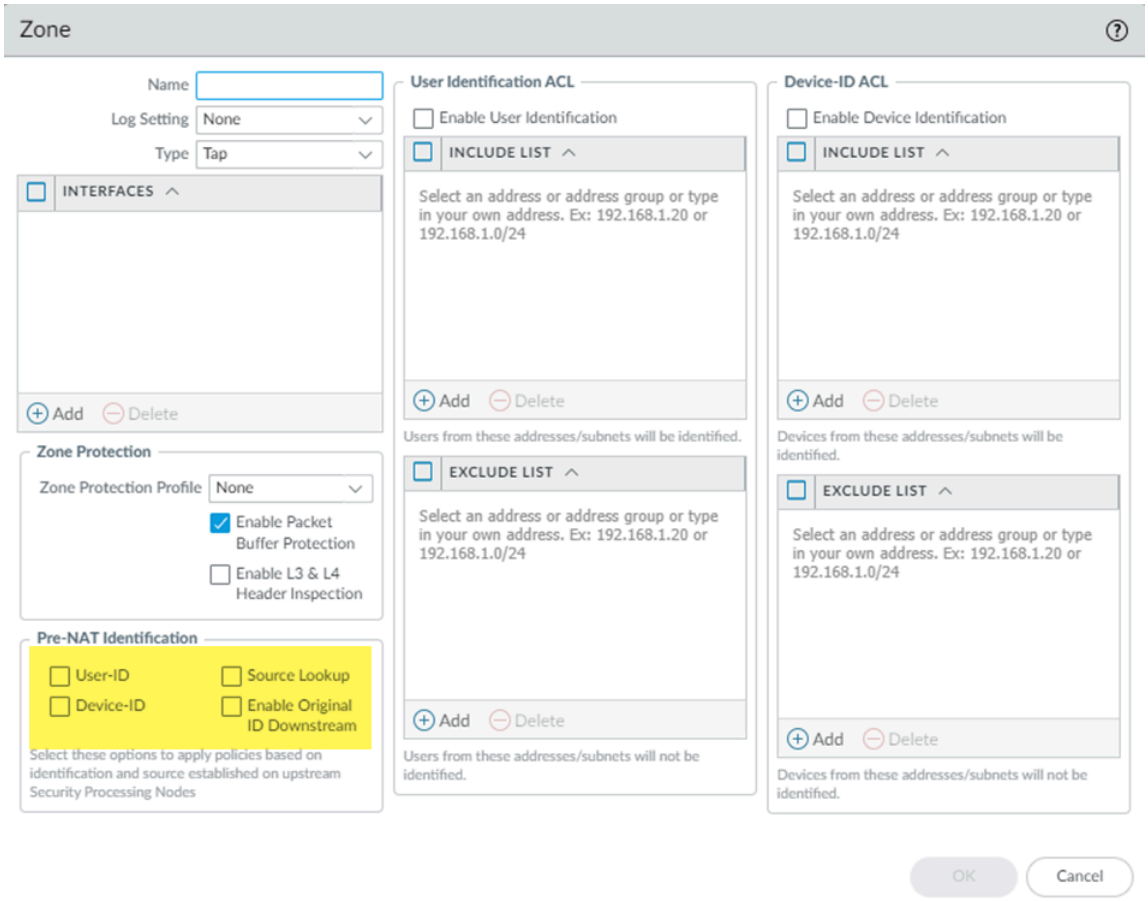
**STEP 1 |** 在 NGFW 上輸入預先 NAT 識別參數。

1. 登入 NGFW，或者登入管理 NGFW 的 SCM 或 Panorama，然後前往 **Network**（網路）> **Zones**（區域）。
2. **Add**（新增）區域或選取現有區域。
3. 選取一個或多個 **Pre-NAT Identification**（預先 **NAT** 識別）參數：
   - **User-ID**—保留 IP 位址進行 NAT 轉換之前所使用的行動使用者 User-ID 對應。如果您在安全性政策規則中使用 User-ID，請啟用此選項。
   - **Device-ID**—保留 IP 位址進行 NAT 轉換之前所使用的行動使用者 Device-ID 對應。如果您在安全性政策規則中使用 Device-ID，請啟用此選項。
   - **Source Lookup**（來源查閱）—使您能夠符合從 GlobalProtect 收到的原始來源 IP 位址。如果您在 QoS 或基於政策的轉送 (PBF) 政策中使用來源查閱，則來源 IP 比較是根據預先 NAT 來源 IP 位址。舉例來說，如果您的安全性政策允許來源 IP 位址為 1.1.1.1

 ©2025 Palo Alto Networks, Inc.

且目的地 IP 位址為「Any（任何）」，則 1.1.1.1 會與封包標頭中預先 NAT 來源 IP 位址進行比較。

- **Enable Original ID Downstream**（啟用原始 **ID** 下游）—如果連續有兩個 NGFW，請指定此選項，以便在第一個 NGFW 檢查流量並對其套用政策後，讓第一個 NGFW 將預先 NAT 資訊傳送給第二個 NGFW。這是 SC-CAN 上的預設設定。




4. 按一下 **OK**（確定）並 **Commit**（交付）變更。

**STEP 2 |** 使用 NGFW 建立命令列介面 (CLI) 工作階段，並在設定模式下輸入以下命令：

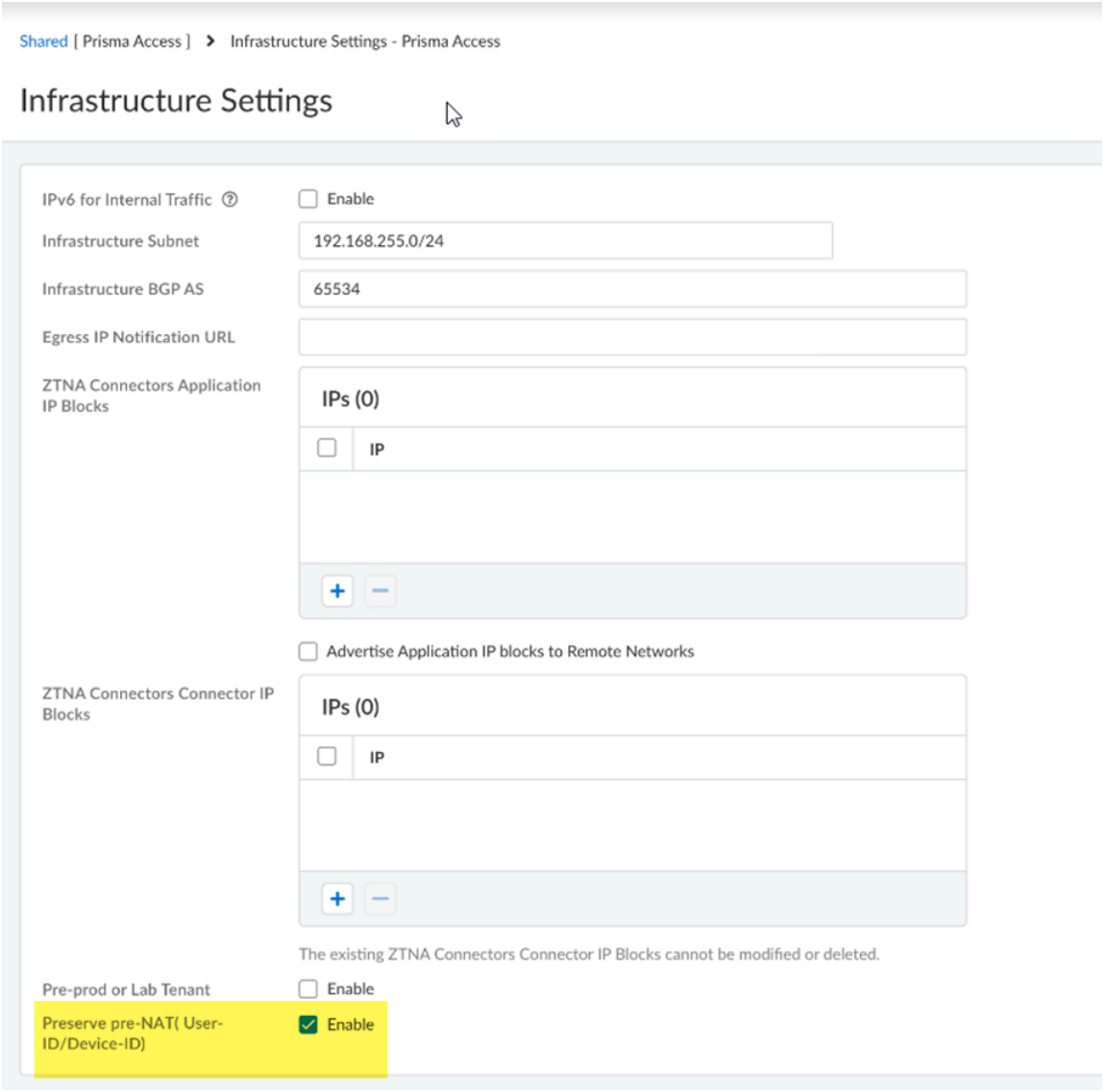
```
set deviceconfig setting preserve-prenat-feature yes
```

如果未來需要停用此功能，請輸入 `set deviceconfig setting preserve-prenat-feature no`。


©2025 Palo Alto Networks, Inc.

**STEP 3 |** 在 Strata Cloud Manager 中啟用預先 NAT 設定。

1. 前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Prisma Access** > **Infrastructure Settings**（基礎結構設定）。
2. **Enable**（啟用）**Preserve pre-NAT (User-ID/Device-ID)**（保留預先 **NAT (User-ID/Device-ID)**）。




3. **Push Config**（推送設定）以儲存您的變更。

## 使用來源 NAT 保留服務連線的使用者與 Device-ID 對應 (Panorama)

若要讓 Prisma Access 將 User-ID 對應從 GlobalProtect 使用者散佈到 Prisma Access (Managed by Panorama) 中總部或資料中心的 NGFW，請完成以下步驟。

此程序假定您已準備好以下網路設定：

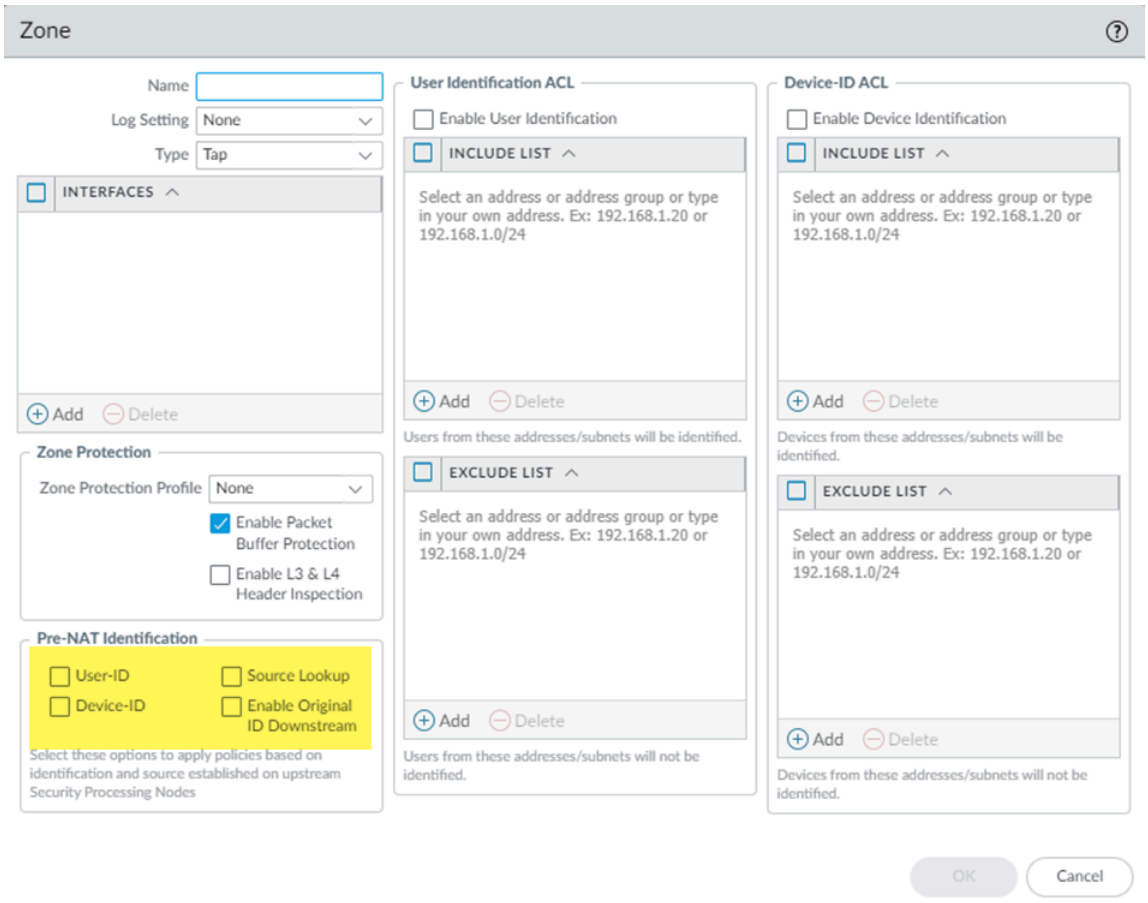
- 您已在服務連線上啟用 **Data Traffic source NAT**（資料流量來源 **NAT**）。
- 您已在私人應用程式所在的總部或資料中心部署了 NGFW。

 ©2025 Palo Alto Networks, Inc.

- 您已根據您在 NGFW 中建立的區域為 NGFW 上的 Prisma Access 套用了安全性政策規則。

**STEP 1 |** 在 NGFW 上輸入預先 NAT 識別參數。

1. 登入 NGFW，或者登入管理 NGFW 的 SCM 或 Panorama，然後前往 **Network**（網路）> **Zones**（區域）。
2. **Add**（新增）區域或選取現有區域。
3. 選取一個或多個 **Pre-NAT Identification**（預先 **NAT** 識別）參數：
   - **User-ID**—保留 IP 位址進行 NAT 轉換之前所使用的行動使用者 User-ID 對應。如果您在安全性政策規則中使用 User-ID，請啟用此選項。
   - **Device-ID**—保留在對 IP 位址進行 NAT 處理之前使用的行動使用者 Device-ID 對應。如果您在安全性政策規則中使用 Device-ID，請啟用此選項。
   - **Source Lookup**（來源查閱）—使您能夠符合從 GlobalProtect 收到的原始來源 IP 位址。如果您在 QoS 或基於政策的轉送 (PBF) 政策中使用來源查閱，則來源 IP 比較是根據預先 NAT 來源 IP 位址。舉例來說，如果您的安全性政策允許來源 IP 位址為 1.1.1.1 且目的地 IP 位址為「Any（任何）」，則 1.1.1.1 會與封包標頭中預先 NAT 來源 IP 位址進行比較。
   - **Enable Original ID Downstream**（啟用原始 **ID** 下游）—如果連續有兩個 NGFW，請指定此選項，以便在第一個 NGFW 檢查流量並對其套用政策後，讓第一個 NGFW 將預先 NAT 資訊傳送給第二個 NGFW。這是 SC-CAN 上的預設設定。




4. 按一下 **OK**（確定）並 **Commit**（交付）變更。

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 使用 NGFW 建立命令列介面 (CLI) 工作階段，並在設定模式下輸入以下命令：

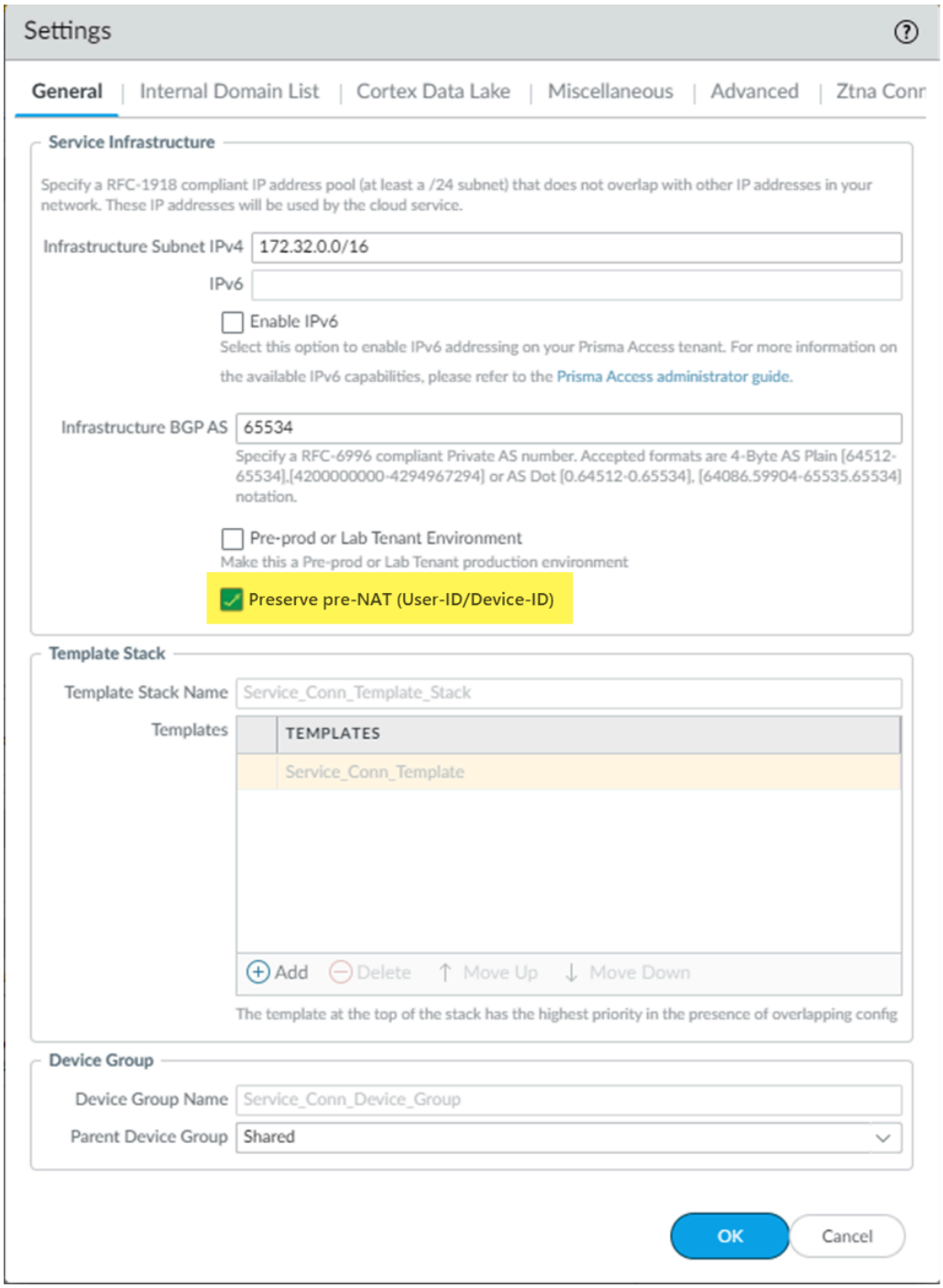
```
set deviceconfig setting preserve-prenat-feature yes
```

如果未來需要停用此功能，請輸入 `set deviceconfig setting preserve-prenat-feature no`。

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 從管理 Prisma Access 的 Panorama 中，啟用預先 NAT 設定。

1. 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定），然後按一下齒輪以編輯 **Settings**（設定）。
2. 選取 **Preserve pre-NAT (User-ID/Device-ID)**（保留預先 **NAT (User-ID/Device-ID)**）。




3. **Commit and Push**（提交並推送）您的變更。


©2025 Palo Alto Networks, Inc.

# Prisma Access 行動使用者—GlobalProtect 進階部署

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

以下幾節為您展示行動使用者—GlobalProtect 部署中可用的進階部署：

- 行動使用者—GlobalProtect 的動態 DNS 註冊支援
- 在 Prisma Access GlobalProtect 部署中識別和隔離遭入侵裝置
- 將行動使用者—GlobalProtect 部署中的 IPv6 流量導向至不同的位置
- 使用 Prisma Access 重新散佈 HIP 資訊
- 檢視 HIP 報告
- 無用戶端 VPN 中 Gzip 編碼的支援
- Prisma Access 中的流量複寫

## 在 Prisma Access 中設定多個入口網站

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ 所需的最低 GlobalProtect 用戶端版本：6.1（僅適用於 Windows 和 macOS） |

您可以根據相同 Prisma Access 租用戶中的連接埠號碼設定兩個入口網站，每個入口網站支援不同的驗證方法。啟用此功能可將行動使用者從一種驗證方法移轉到另一種驗證方法，而無需建立新的 Prisma Access 租用戶。此設定啟用更大的驗證彈性，方法為允許您逐步將使用者移到雲端型驗證，而不需要個別的 Prisma Access 執行個體。

具有 GlobalProtect 多個入口網站的 Prisma Access 會為同一租用戶內的每個入口網站使用不同的連接埠號碼。使用標準連接埠 443 設定第一個 GlobalProtect 入口網站。當您啟用多重入口網站功能時，Prisma Access 會使用替代連接埠 8443 設定第二個 GlobalProtect 入口網站，並允許使用與第一個入口網站相同的 FQDN 連線到第二個入口網站。多重入口網站功能僅支援每個 FQDN 兩個入口網站。

當使用者使用連接埠 443 連線到入口網站時，流量會傳送到第一個驗證入口網站，且 IP 位址不會發生任何變更。若沒有 GlobalProtect 多重入口網站功能，進行設定時此流程保持不變。當使用者使用連接埠 8443 連線時，流量反而會命中目的地 NAT 規則。這會將使用者引導至不同 IP 位址的第二個驗證入口網站。在任一入口網站進行驗證之後，使用者會被轉送到具有驗證覆寫 cookie 的閘道。此功能取決於驗證覆寫 cookie 設定，並且同時針對入口網站和閘道啟用。

下表描述了 GlobalProtect 多重入口網站支援，其中結合了驗證方法，以及在主要入口網站上使用舊版驗證（例如 RADIUS 或LDAP）和在次要入口網站上使用雲端驗證（例如 SAML 或 SAML 搭配 CAS）的憑證。


©2025 Palo Alto Networks, Inc.

| 主要入口網站使用者驗證 | 次要入口網站使用者驗證 | 連線方法選項 |
|---|---|---|
| 舊版，無憑證 | 雲端，無憑證 | 使用者登入（始終開啟、隨選） |
| 舊版、<auth profile selection> 和用戶端憑證<br>註：憑證設定檔必須相同。 | 雲端、<auth profile selection> 和用戶端憑證<br>註：憑證設定檔必須相同。 | 使用者登入（始終開啟、隨選）<br>預先登入（始終開啟、隨選） |
| 舊版，無憑證 | 雲端、<auth profile selection> 或用戶端憑證 | 使用者登入（始終開啟、隨選） |
| 舊版、<auth profile selection> 或用戶端憑證<br>多重入口網站設定不支援用戶端僅使用用戶端憑證進行驗證 | 雲端，無憑證 | 使用者登入（始終開啟、隨選）<br>預先登入（始終開啟、隨選），如果有憑證 |
| 舊版、<auth profile selection> 或用戶端憑證<br>多重入口網站設定不支援用戶端僅使用用戶端憑證進行驗證 | 雲端、<auth profile selection> 或用戶端憑證<br>多重入口網站設定不支援用戶端僅使用用戶端憑證進行驗證 | 使用者登入（始終開啟、隨選）<br>預先登入（始終開啟、隨選），如果有憑證 |

在設定多個入口網站之前，請確保以下事項：

- 兩個入口網站有相同的憑證設定檔件或沒有憑證設定檔
- 與驗證設定檔相關聯的允許清單應該相同
- 當您在入口網站上接受 cookie 進行驗證覆寫時，請確保 cookie 存留時間在入口網站和閘道上相同。
- 多重入口網站設定不支援僅使用用戶端憑證型驗證

在多重入口網站部署中，不支援在次要入口網站上使用無用戶端 VPN；不過，無用戶端 VPN 可以搭配您現有的驗證方法在主要入口網站上運作。

- Strata Cloud Manager
- Panorama

## 在 Prisma Access 中設定多個入口網站 (Strata Cloud Manager)

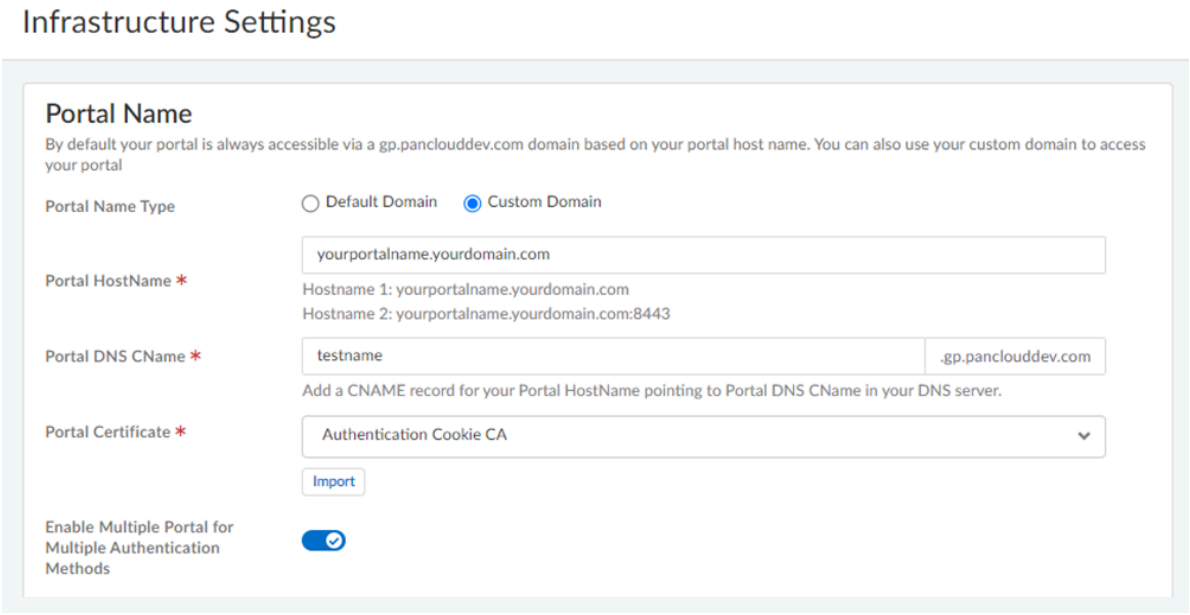
**STEP 1 |** 請聯絡 Palo Alto Networks 支援以啟動此功能。

**STEP 2 |** 為其設定行動使用者和其驗證方法。


©2025 Palo Alto Networks, Inc.

**STEP 3 |** 為同一閘道啟用多個入口網站。

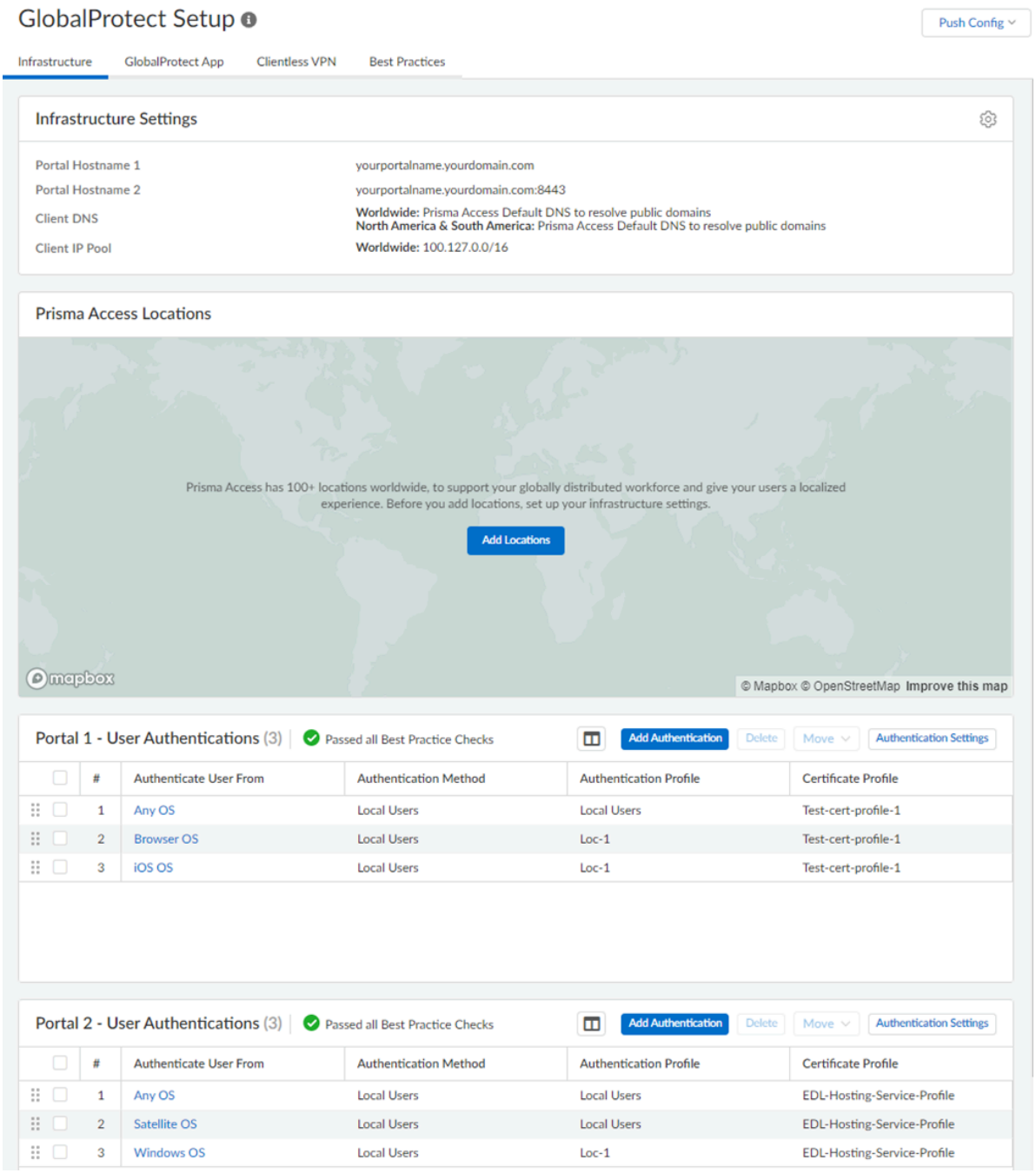
1. 選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **GlobalProtect** > **GlobalProtect Setup**（**GlobalProtect** 設定） > **Infrastructure**（基礎結構）。
2. 編輯 **Infrastructure Settings**（基礎結構設定）。
3. **Enable Multiple Portal for Multiple Authentication Methods**（為多重驗證方法啟用多重入口網站）。




對於同一租用戶的連接埠 8443，會出現新的入口網站。此入口網站繼承了原始連接埠（即連接埠 443）的設定。


©2025 Palo Alto Networks, Inc.

**STEP 4 |** 編輯入口網站設定以更新驗證設定。

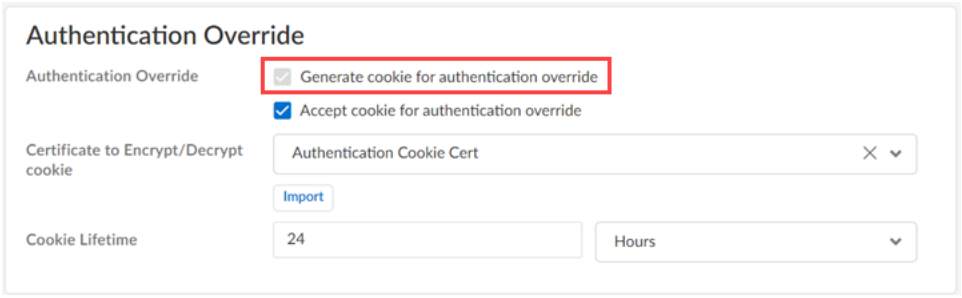



您只能編輯入口網站的 **Authentication Settings**（驗證設定）和 **Certificate Profile**（憑證設定檔）驗證設定。

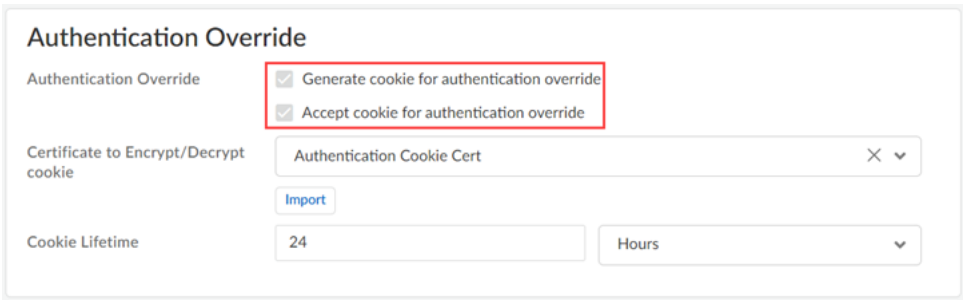
如果您在這兩個入口網站中使用憑證型驗證，請確保這兩個入口網站使用相同的用戶端憑證設定檔進行驗證。

此功能可讓驗證覆寫設定在 GlobalProtect 應用程式設定中為這兩個入口網站產生 cookie。

 ©2025 Palo Alto Networks, Inc.




此功能可讓驗證覆寫設定在通道設定中為這兩個入口網站產生和接受 cookie。




**STEP 5 |** 儲存您的所有變更，並將設定變更 **Push**（推送）到 Prisma Access。

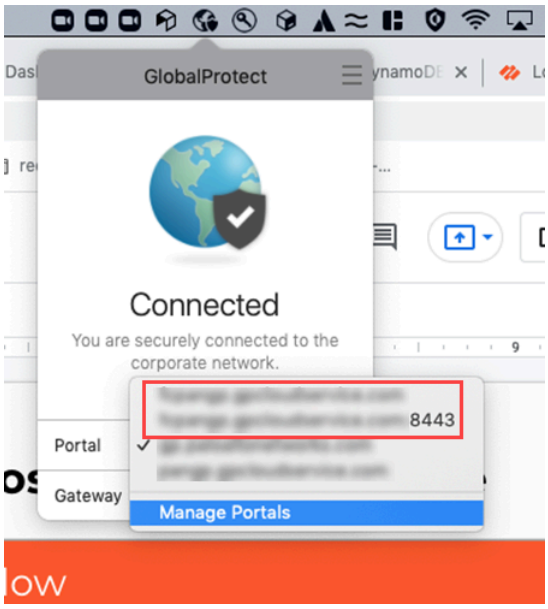
**STEP 6 |** 在 GlobalProtect 應用程式中手動或使用端點管理軟體新增入口網站。

 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** 驗證您是否可以針對閘道使用不同的驗證設定檔連線到這兩個入口網站。

1. 登入您的 Windows 電腦。
2. 在您的 GlobalProtect 應用程式中連線到入口網站。

   當您變更不同驗證方法的入口網站之間的連線，請驗證使用者登入。




如果驗證 *cookie* 在您連線到 *8443* 入口網站並切換到手動閘道時過期，*GlobalProtect* 會連線到 ***Best Available Gateway***（最佳可用閘道）。

如果您的 *GlobalProtect* 應用程式使用快取的入口網站設定，則回復到入口網站將無法運作。

如果您正在為次要入口網站使用 SAML 型驗證，請在整合時依如下方式輸入值：

- ***Single sign on URL***（單一登入 ***URL***）：輸入 ***`https://Portal-FQDN:443/SAML20/SP/ACS`***

  *Portal-FQDN* 是 *Prisma Access* 入口網站的 *FQDN*

  即使您已設定次要入口網站 *(8443)*，也請使用入口網站 ***443***。
- （受眾 ***URI***（***SP*** 實體 ***ID***））：輸入 ***`https://Portal-FQDN:443/SAML20/SP`***

## 在 Prisma Access 中設定多個入口網站 (Panorama)

**STEP 1 |** 請聯絡您的 Palo Alto Networks 客戶代表以啟動此功能。

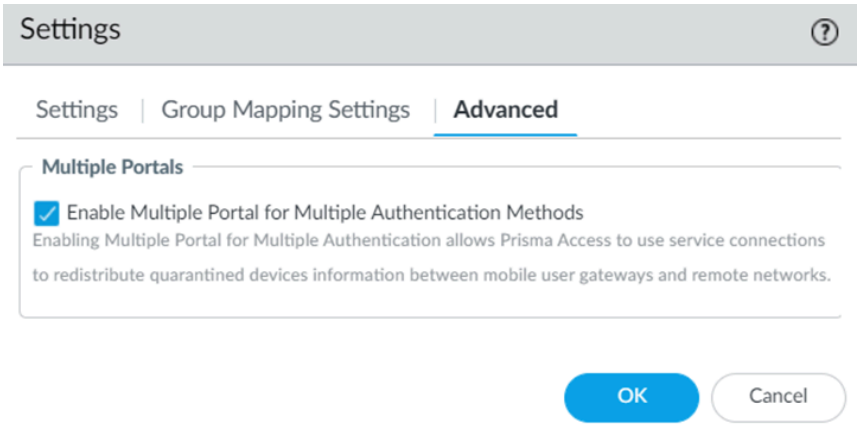
使用流量導向設定多個 *GlobalProtect* 入口網站時，請勿設定 ***Accept Default Routes over Service Connections***（接受服務連線上的預設路由）（***Panorama*** > ***Cloud Services***（雲端服務） > ***Configuration***（設定） > ***Traffic Steering***（流量導向） > ***Settings***（設定） > ***Accept Default Route over Service Connection***（接受服務連線上的預設路由））；如果這樣做，行動使用者無法連線到次要入口網站。

**STEP 2 |** 為其設定行動使用者和其驗證方法。

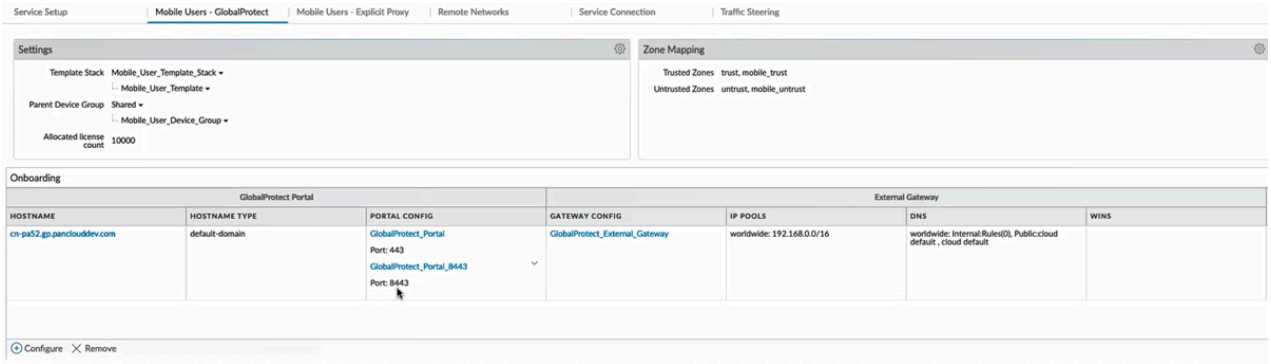

©2025 Palo Alto Networks, Inc.

**STEP 3 |** 選取 **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users—GlobalProtect**（行動使用者—**GlobalProtect**） > **Settings**（設定） > **Advanced**（進階）。

**STEP 4 |** **Enable Multiple Portal for Multiple Authentication Methods**（為多重驗證方法啟用多重入口網站）。




對於同一租用戶的連接埠 8443，會出現新的入口網站。此入口網站繼承了原始連接埠（即連接埠 443）的設定。




 ©2025 Palo Alto Networks, Inc.

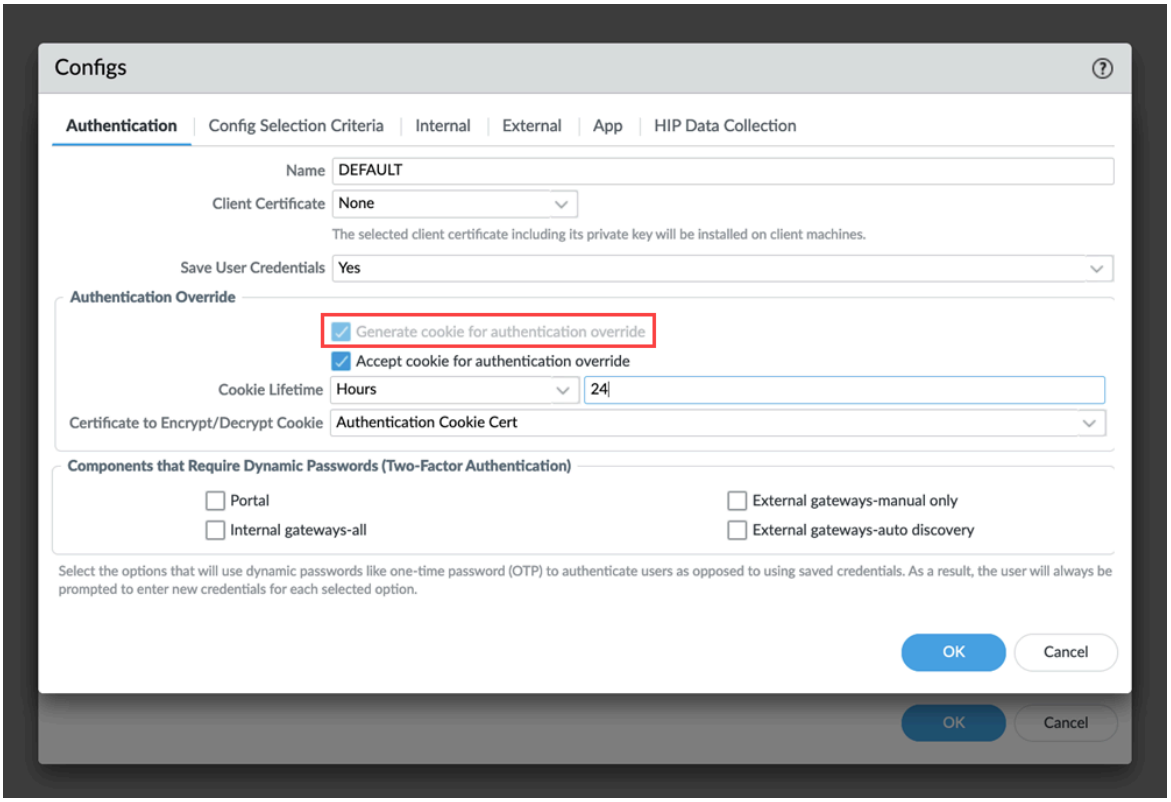
**STEP 5 |** 編輯入口網站設定以更新驗證設定。

1. 按一下入口網站超連結或選取 **Panorama** > **Templates**（範本） > **Network**（網路） > **GlobalProtect** > **Portals**（入口網站），然後按一下入口網站超連結。
2. 在 **Authentication**（驗證）區段中，**Add**（新增）**Client Authentication**（用戶端驗證）與不同的 **Authentication Profile**（驗證設定檔）。

您只能編輯 **Client Authentication**（用戶端驗證）和 **Certificate Profile**（憑證設定檔）驗證設定。

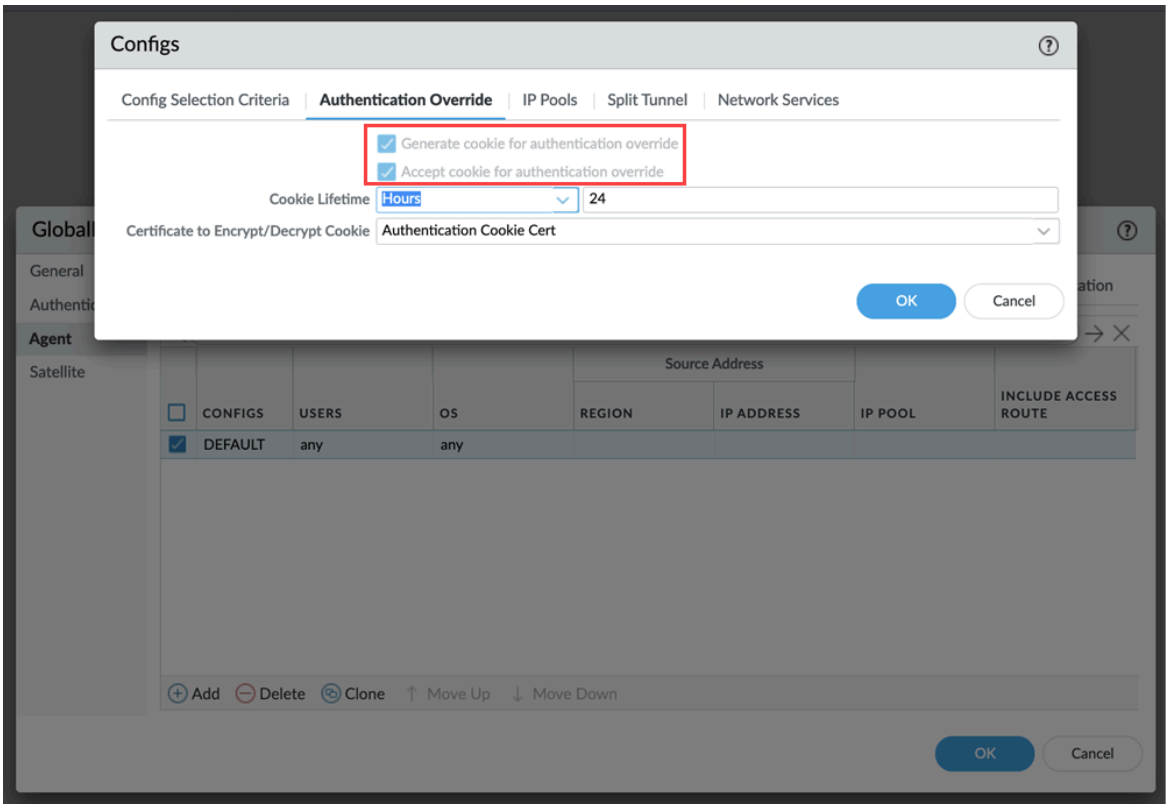
如果您在這兩個入口網站中使用憑證型驗證，請確保閘道沒有憑證型驗證。

此功能可讓驗證覆寫設定在 GlobalProtect 應用程式設定中為這兩個入口網站產生 cookie。



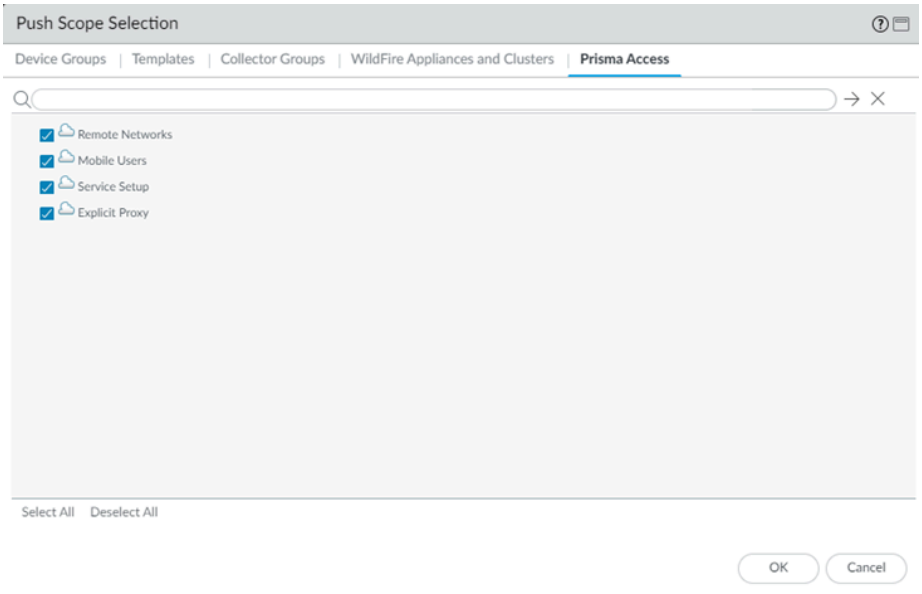

此功能可讓驗證覆寫設定在通道設定中為這兩個入口網站產生和接受 cookie。

 ©2025 Palo Alto Networks, Inc.




**STEP 6 |** 將您的所有變更提交到 Panorama，並將設定變更推送到 Prisma Access。

1. 按一下 **Commit**（提交） > **Commit and Push**（提交並推送）。
2. **Edit Selections**（編輯選取項目），並在 **Prisma Access** 頁籤中，確保在 **Push Scope**（推送範圍）中選取了 **Mobile Users**（行動使用者），然後按一下 **OK**（確定）。




3. 按一下 **Commit and Push**（提交並推送）。

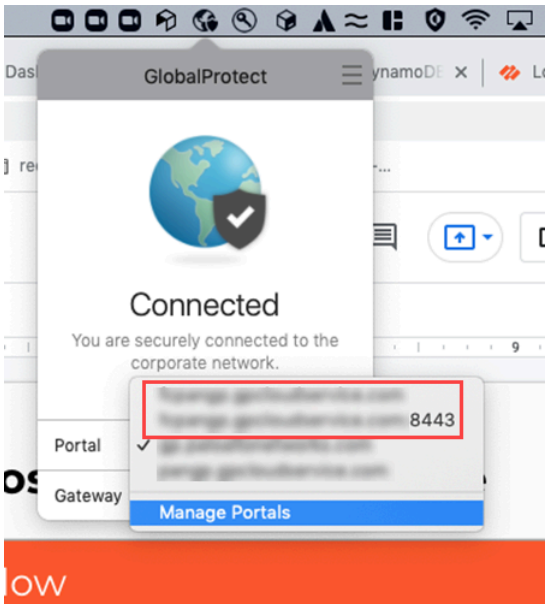
**STEP 7 |** 在 GlobalProtect 應用程式中手動或使用端點管理軟體新增入口網站。

 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** 驗證您是否可以針對閘道使用不同的驗證設定檔連線到這兩個入口網站。

1. 登入您的 Windows 電腦。
2. 在您的 GlobalProtect 應用程式中連線到入口網站。

   當您變更不同驗證方法的入口網站之間的連線，請驗證使用者登入。




   如果驗證 *cookie* 在您連線到 *8443* 入口網站並切換到手動閘道時過期，*GlobalProtect* 會連線到 ***Best Available Gateway***（最佳可用閘道）。

   如果您的 *GlobalProtect* 應用程式使用快取的入口網站設定，則回復到入口網站將無法運作。
3. 在 **Monitor**（監控） > **Logs**（日誌） > **GlobalProtect** 中檢視這兩個入口網站的日誌，以查看入口網站和驗證資訊。

如果您正在為次要入口網站使用 SAML 型驗證，請在整合時依如下方式輸入值：

- ***Single sign on URL***（單一登入 ***URL***）：輸入 ***https://Portal-FQDN:443/SAML20/SP/ACS***

  *Portal-FQDN* 是 *Prisma Access* 入口網站的 *FQDN*

  即使您已設定次要入口網站 *(8443)*，也請使用入口網站 ***443***。
- （受眾 ***URI***（***SP*** 實體 ***ID***））：輸入 ***https://Portal-FQDN:443/SAML20/SP***

## 遠端疑難排解和更新的動態 DNS 支援

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• Prisma Access (Managed by Strata Cloud Manager) | ☐ Prisma Access 授權，包 括行動使用者—GlobalProtect |


©2025 Palo Alto Networks, Inc.

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| | ❑ 最低必要 Prisma Access 版本：5.1 Innovation（至少需要 PAN-OS 資料平面 11.2 版） |

當行動使用者使用 GlobalProtect 代理程式遠端連線到 Prisma Access 時，GlobalProtect 閘道會將 IP 位址和端點 FQDN 指派給使用者。不過，Prisma Access 不會使用此資訊更新企業中的 DNS 伺服器。由於 DNS 伺服器沒有行動使用者獲指派的 IP 位址和 FQDN 資訊，因此您的 IT 管理員和您網路中的應用程式無法使用 FQDN 識別和更新遠端端點。

使用動態 DNS 註冊，您可以整合 Prisma Access 與 IP 位址管理 (IPAM) 廠商，使用 nsupdate 在 DNS 伺服器中動態建立 A 和 PTR 記錄，從而提供以下優勢：

- 與先進的 IPAM 廠商（例如 InfoBlox、BlueCat和 Windows）直接整合。
- DDNS 更新是使用交易特徵碼 (TSIG) 或 Kerberos 作為驗證通訊協定來執行，從而確保對 DNS 資料庫的安全更新。
- 即時 DDNS 更新是根據 GlobalProtect 連線和中斷連線事件，使用批次 nsupdate 呼叫從 Prisma Access 執行到 DNS 伺服器。這些更新會使用行動使用者安全性處理節點 (MU-SPN) 上的 DDNS 服務。

在設定此解決方案之後，您可以執行以下動作：

- 您可以使用 Microsoft Endpoint Configuration Manager (MECM) 等軟體工具，將軟體更新推送到 GlobalProtect 端點。
- IT 和服務台工作人員可以使用裝置的 FQDN 連線並管理 GlobalProtect 端點。
- 您可以實作依賴 DNS 反向查閱的客戶應用程式（例如銀行應用程式），以允許從已核准的 GlobalProtect 端點進行存取。

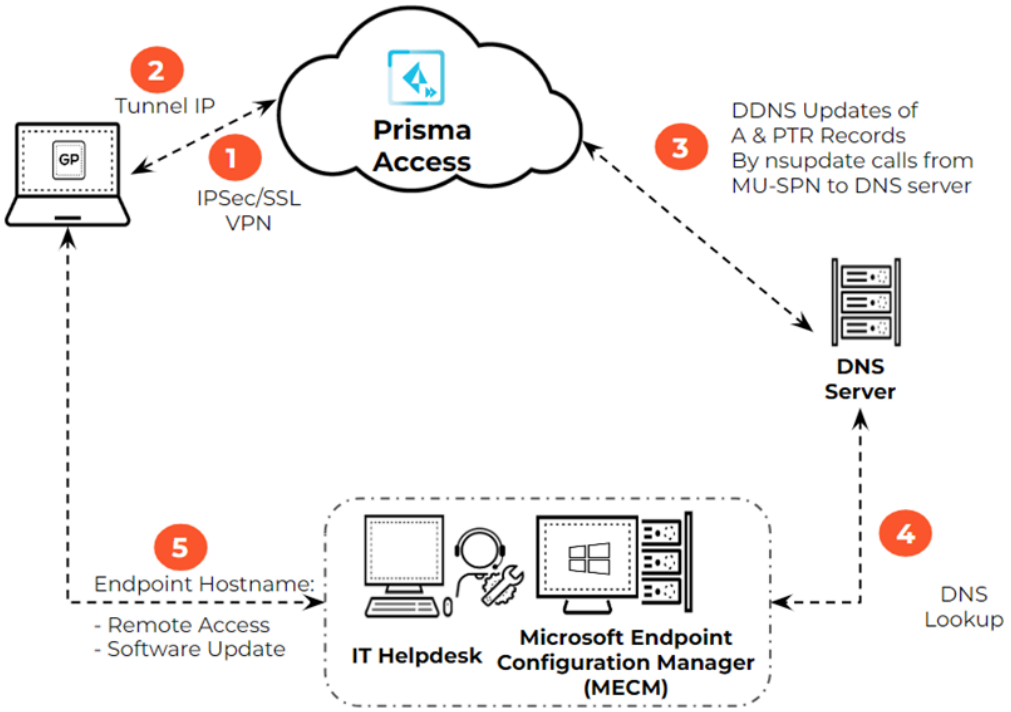
此 *DDNS* 解決方案與使用 *Strata Logging Service* 將 *DDNS* 更新推送到伺服器的行動使用者—GlobalProtect 的動態 DNS 註冊支援不相容。如果您有使用 *Strata Logging Service* 實作的現有解決方案，然後部署此解決方案，則 *Prisma Access* 會使用此解決方案，並使用 *Strata Logging Service* 停用現有的解決方案。

## 動態 DNS 註冊支援使用案例

下圖說明 Prisma Access DDNS 解決方案的典型使用案例。在此範例中，您想要使用 MECM 更新 GlobalProtect 端點，或者想要 IT 技術支援能夠遠端登入 GlobalProtect 端點以進行疑難排解。

1. GlobalProtect 會在 GlobalProtect 端點與 Prisma Access 閘道之間建立 SSL 通道。
2. GlobalProtect 透過通道將行動使用者裝置的主機名稱、網域名稱和通道 IP 位址資訊傳送到內部部署或 Prisma Access 閘道。
3. Prisma Access 會使用 nsupdate 將 A 和 PTR 記錄的 DDNS 更新提供給 DNS 伺服器。Prisma Access 會在處理登入和登出事件時即時提供這些安全更新。
4. IT 管理員或企業軟體透過 DNS 或 RDNS 查閱使用這些記錄，並解析端點名稱或 IP 位址。
5. IT 管理員或端點管理軟體使用此資訊，來管理端點或推送軟體更新。

 ©2025 Palo Alto Networks, Inc.




## 網路連線需求

在實作此解決方案之前，請確保您的網路滿足以下需求：

- 您已新增路由，以確保可從 MU-SPN 和從 Prisma Access 服務連線連線至 DNS 伺服器。

  若要這樣做，請從 Prisma Access 基礎結構子網路（您可以在 **Workflows**（工作流程） > > **Prisma Access Setup**（**Prisma Access** 設定） > **Prisma Access** > **Infrastructure Subnet**（基礎結構子網路）尋找），以及從行動使用者—GlobalProtect IP 位址集區（您可以在 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **GlobalProtect** > **Client IP Pool**（用戶端 **IP** 集區）中尋找）新增路由。
- 您已建立連線，方法是在 Prisma Access 與可連線至 DNS 伺服器的 IPSec 終端裝置（例如，新世代防火牆或路由器）之間建立服務連線。
- 您已確保可以透過服務連線 IPSec 通道存取 DNS 伺服器。
- 您已驗證從 Prisma Access 行動使用者—GlobalProtect 安全性處理節點 (SPN) 傳送的 nsupdate 命令得到允許 並可以連線至 DNS 伺服器。

  為實現此連線而執行的步驟因所使用的 DNS 伺服器的位置和類型而異。例如：

  - 如果 DNS 伺服器位於資料中心，則您可以使用 IPSec 通道設定連線，從行動使用者—GlobalProtect SPN 到服務連線，然後從服務連線到 DNS 伺服器位於其後的閘道路由器（例如，設定為 VM 的新世代防火牆）。
  - 如果 DNS 伺服器位於雲端，您可以使用適當的安全性政策規則，從行動使用者—GlobalProtect SPN 實現與 DNS 伺服器的連線。
- 您已在 DNS 伺服器上設定了正向和反向查閱區域。
- 您已實作支援 nsupdate 的 Infoblox、Bluecat 或 Windows DNS 伺服器。

 ©2025 Palo Alto Networks, Inc.

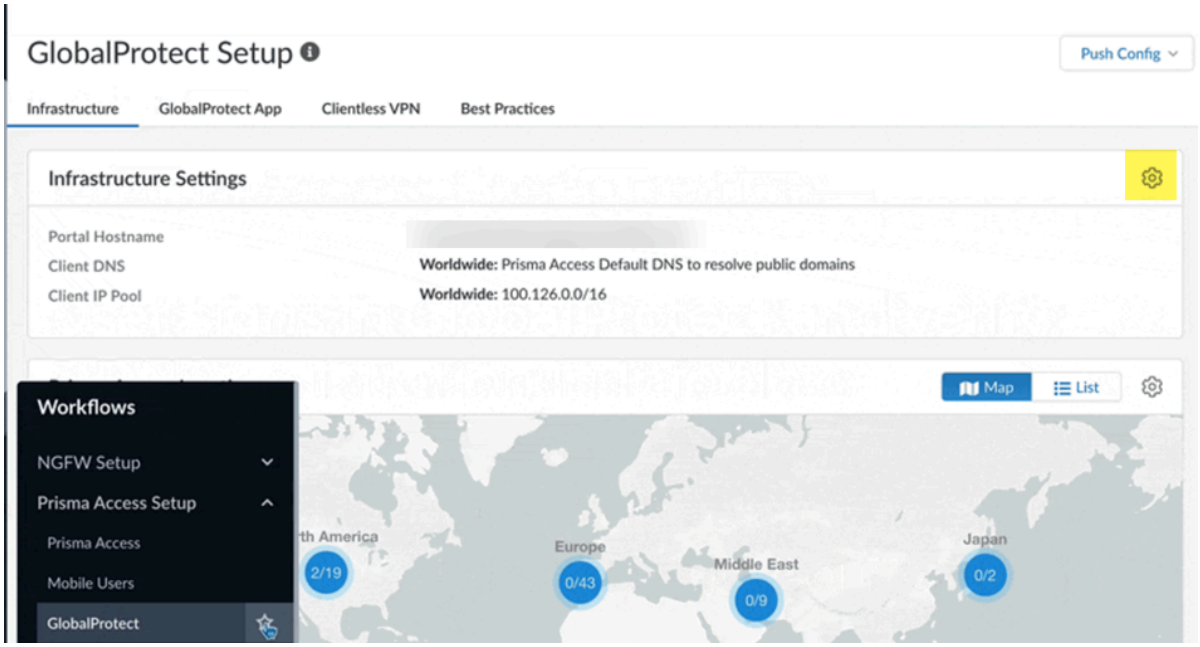
- 如果您個別維護區域的權限，請確保您已建立安全性政策規則，以允許從具有正確 TSIG 或 Kerberos 金鑰的裝置進行 nsupdates。

若要設定此解決方案，請根據您的部署類型使用下列其中一個程序。

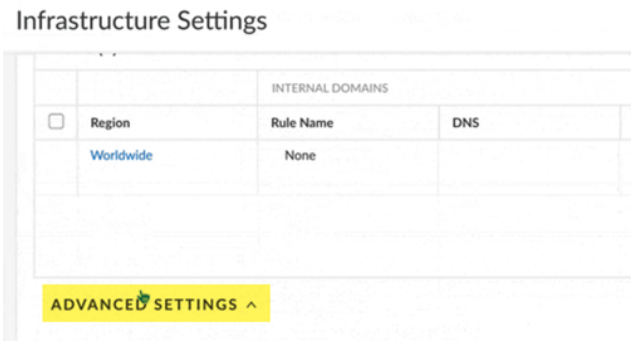
- 雲端管理
- Panorama

## 為 Prisma Access (Managed by Strata Cloud Manager) 設定動態 DNS 更新

**STEP 1 |** 從 Strata Cloud Manager 中，前往 **Workflows**（工作流程） > **GlobalProtect**，然後齒輪以編輯 **Infrastructure Settings**（基礎結構設定）。




**STEP 2 |** 選取 **Advanced Settings**（進階設定）。




**STEP 3 |** 設定 **Dynamic DNS Support**（動態 **DNS** 支援）設定。

1. 選取 **Dynamic DNS Support for GlobalProtect**（**GlobalProtect** 的動態 **DNS** 支援）。
2. 選取 **Domain Type**（網域類型）。
   - **Fallback Domain**（回復網域）—用於 nsupdate 事件的網域會回復到您在 **Fallback Domain**（回復網域）區域中指定的網域。如果 GlobalProtect 用戶端未加入至任何網

 ©2025 Palo Alto Networks, Inc.

域，或者如果它們已加入至 DDNS 服務用來更新 DNS 伺服器上記錄的相同網域，請使用此選項。

如果您選取 **Fallback Domain**（回復網域），並且未連線至網域的使用者登入 GlobalProtect，他們的資訊會新增在 DNS 伺服器上建立的回復網域區域下。

如果登入 GlobalProtect 的 GlobalProtect 用戶端屬於未在 DNS 伺服器上設定的非預期網域，則 nsupdate 可能會失敗；在此情況下，請選取 **Override Domain**（覆寫網域），以 DNS 伺服器已知的網域覆寫未知網域。

- **Override Domain**（覆寫網域）—Prisma Access 僅會使用您指定的網域來更新 DNS 伺服器，並覆寫所有其他網域。如果 GlobalProtect 用戶端登入另一個網域，DDNS 服務會使用您在這裡指定的網域來更新 DNS A 和 PTR 記錄。

3. 在 **Fallback Domain**（回復網域）欄位中，為回復或覆寫網域選取用來更新 PTR 記錄的網域。
4. 選取 **DNS Server IP**（**DNS** 伺服器 **IP**）位址。
5. 選取 **Server Type**（伺服器類型）（**TSIG** 或 **Kerberos**）。
6. （僅限 TSIG 部署）選取要與 TSIG 搭配使用的 **TSIG Key**（**TSIG** 金鑰）。

   確定 TSIG 檔案的格式是正確的，且檔案類型為 .key。

   如果您選擇 Kerberos 驗證類型，請透過 .key 檔案上傳驗證金鑰，該檔案具有從 DNS 伺服器擷取的未編碼 Kerberos 金鑰標籤檔案。

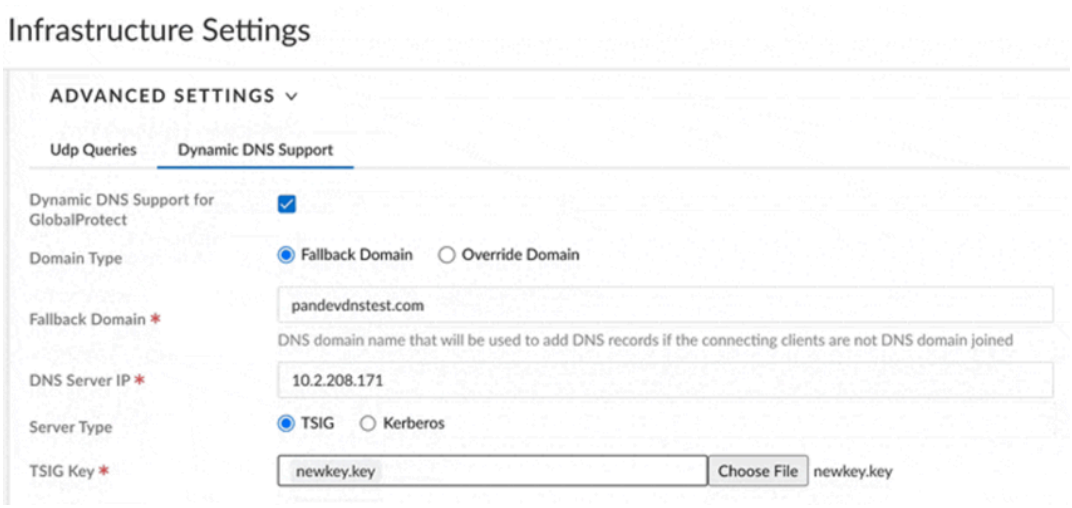
   TSIG 檔案應採用下列格式：

   ```
   key "ddns-gp" { algorithm hmac-sha256; secret
    "aBCDEFGhiJklMNO89PQR+8stUVWX+YZAbcdeFgHI5J="; };
   ```

7. （僅限 Kerberos 部署）指定要使用的 Kerberos 選項。
   - 輸入 **Kerberos Domain Controller**（**Kerberos** 網域控制器）的 IP 位址。
   - 輸入 **Kerberos Admin Server**（**Kerberos** 管理伺服器）的 IP 位址。
   - 輸入 **Kerberos User Name**（**Kerberos** 使用者名稱）。
   - 輸入要使用的 **Kerberos Key**（**Kerberos** 金鑰）（金鑰標籤）。

     請確定 Kerberos 的格式是正確的。

 ©2025 Palo Alto Networks, Inc.



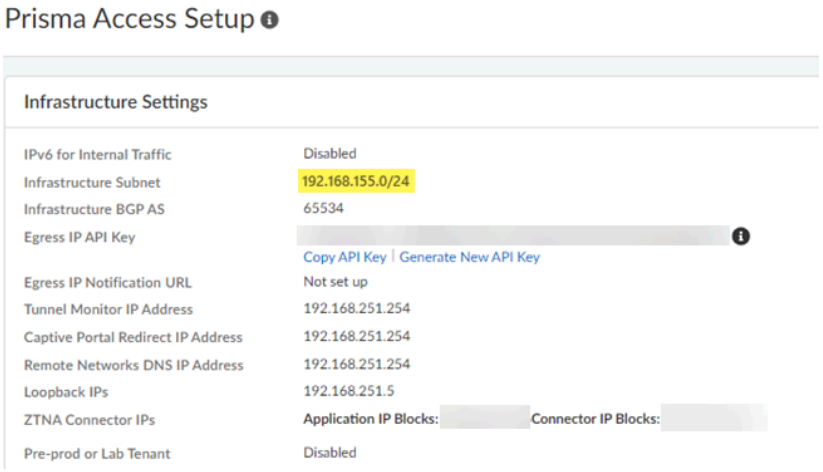

**STEP 4 |** **Save**（儲存）變更。

 ©2025 Palo Alto Networks, Inc.

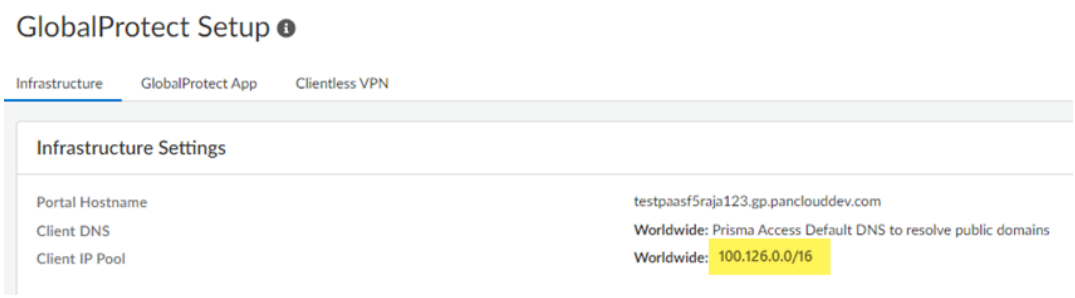
**STEP 5 |** 在 DNS 伺服器上設定正向查閱和反向查閱區域。

請參閱 IPAM 廠商的文件以設定這些區域。此步驟需要您從 Prisma Access 輸入 **Infrastructure Subnet**（基礎結構子網路）和 **Client IP Pool**（用戶端 **IP** 集區）。

- 若要尋找基礎結構子網路，請前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Prisma Access**，並記下 **Infrastructure Subnet**（基礎結構子網路）。



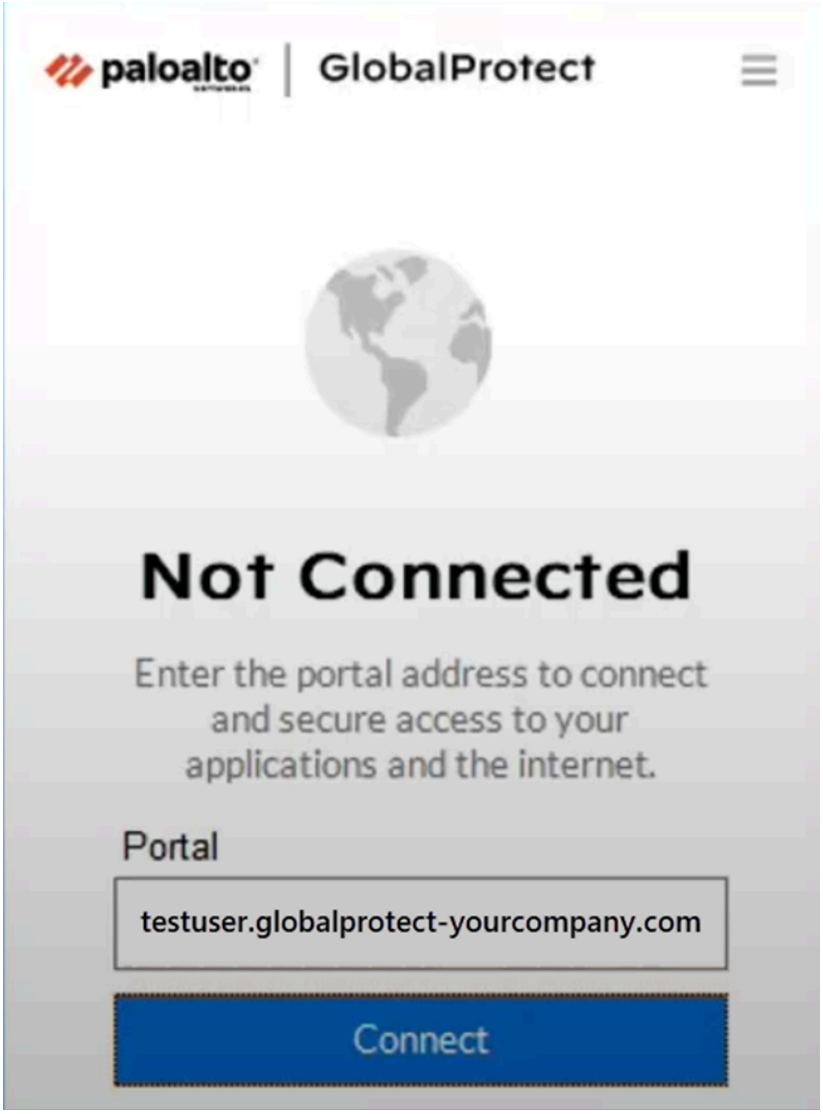

- 若要尋找 GlobalProtect 行動使用者 IP 位址集區，請前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **GlobalProtect**，並記下 **Client IP Pool**（用戶端 **IP** 集區）。




 ©2025 Palo Alto Networks, Inc.

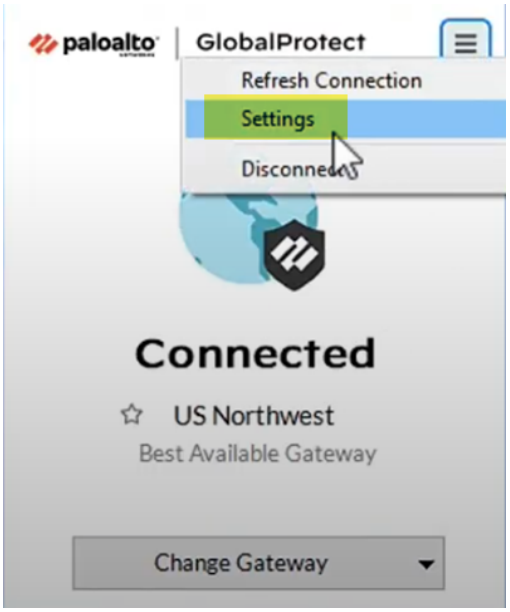
**STEP 6 |** 驗證是否正在 IPAM DNS 伺服器上更新 DNS 記錄。

1. 開啟用戶端電腦並連線至 Prisma Access GlobalProtect 閘道。

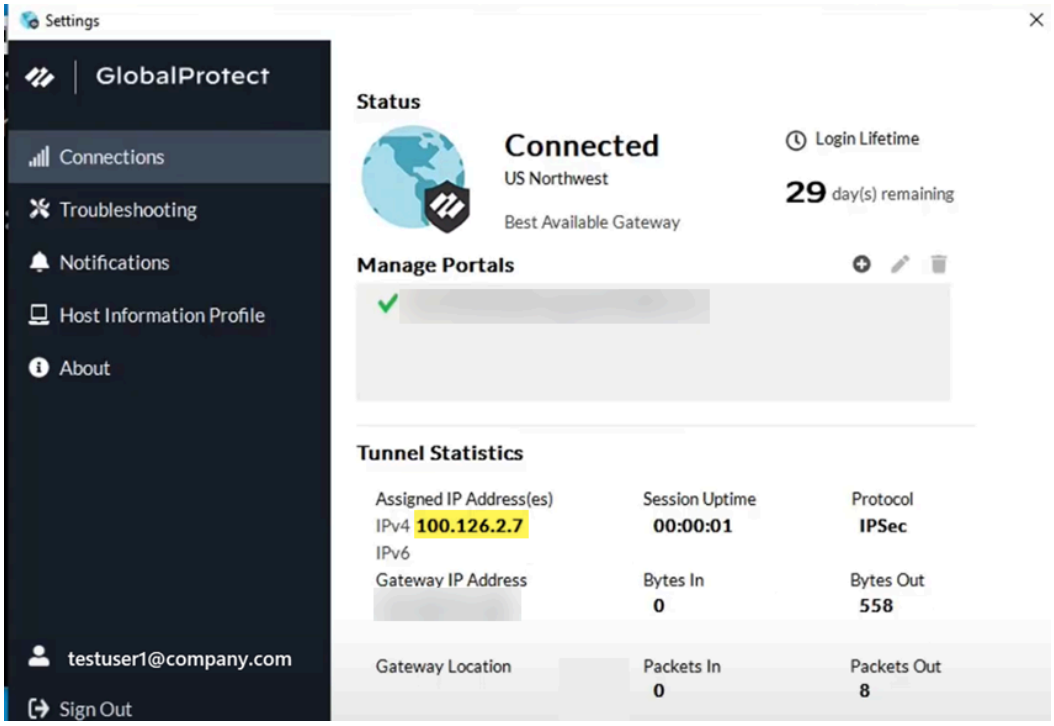



2. 選取 GlobalProtect **Settings**（設定），然後驗證 Prisma Access 指派給使用者的 GlobalProtect IP 位址。

 ©2025 Palo Alto Networks, Inc.

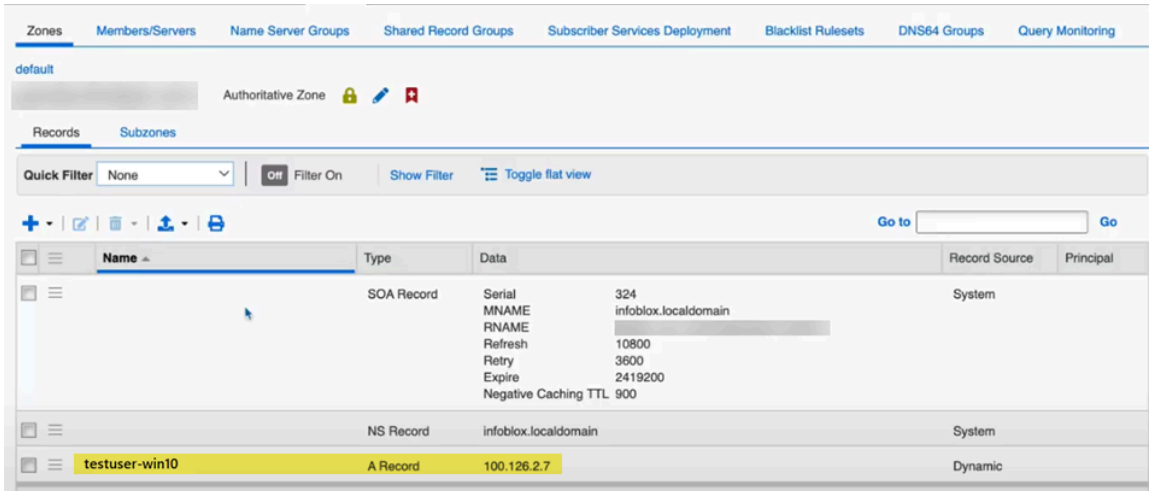



**Assigned IP Address(es)**（指派的 **IP** 位址）(100.126.2.7) 顯示 IP 位址來自 GlobalProtect IP 位址集區 (100.126.0.0/16)。

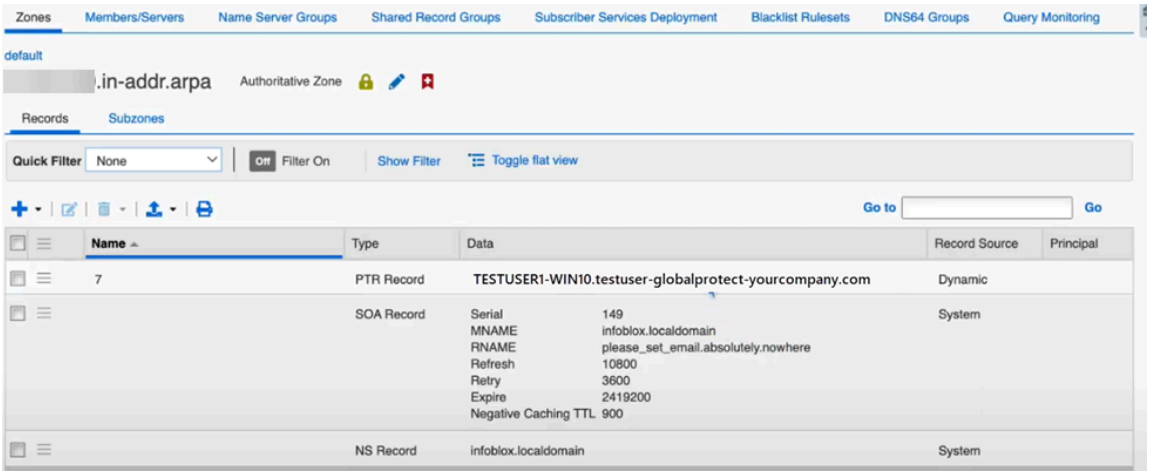



3. 從 IPAM DNS 伺服器檢視使用者的記錄。
   在此範例中，使用者命名為 `testuser1-win10`。


©2025 Palo Alto Networks, Inc.




DNS 反向查閱也會在 PTR 記錄中顯示使用者名稱。




4. 將使用者登出 GlobalProtect 並檢查記錄，以確定 DNS 伺服器已刪除使用者的記錄。

## 為 Prisma Access (Managed by Panorama) 設定動態 DNS 更新

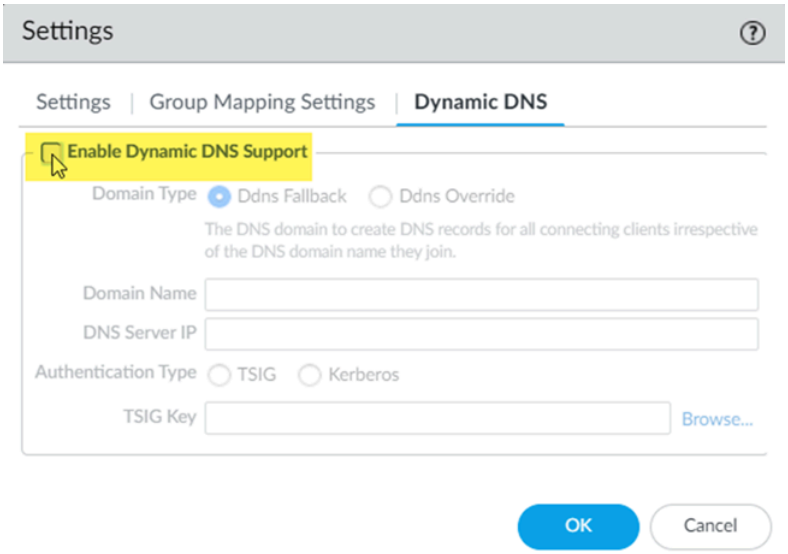
若要為 Prisma Access (Managed by Panorama) 設定動態 DNS 更新，請完成下列步驟。

**STEP 1 |** 從 Panorama 中，前往 **Cloud Services**（雲端服務） > **Configuration**（設定） > **Mobile Users—GlobalProtect**（行動使用者—**GlobalProtect**），然後按一下齒輪以編輯 **Settings**（設定）。

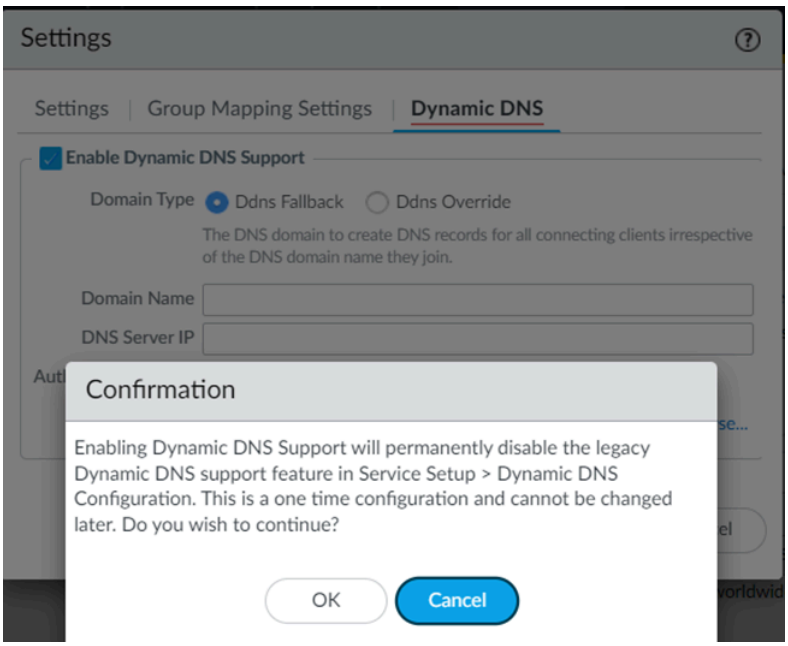
**STEP 2 |** 選取 **Dynamic DNS**（動態 **DNS**）。


©2025 Palo Alto Networks, Inc.

**STEP 3 |** **Enable Dynamic DNS Support**（啟用動態 **DNS** 支援）。




**STEP 4 |** 系統會提示您，如果啟用了舊版動態 DNS 支援，則啟用更新的支援會永久停用舊版支援。按一下 **OK**（確定）繼續。




**STEP 5 |** 設定 **Dynamic DNS**（動態 **DNS**）設定。

1. 選取 **Enable Dynamic DNS Support**（啟用動態 **DNS** 支援）。
2. 選取 **Domain Type**（網域類型）。
   - **Ddns Fallback**（**Ddns** 回復）—用於 nsupdate 事件的網域會回復到您在 **Domain Name**（網域名稱）區域中指定的網域。如果 GlobalProtect 用戶端未加入至任何網


©2025 Palo Alto Networks, Inc.

域，或者如果它們已加入至 DDNS 服務用來更新 DNS 伺服器上記錄的相同網域，請使用此選項。

如果您選取 **Ddns Fallback**（**Ddns** 回復），並且未連線至網域的使用者登入 GlobalProtect，他們的資訊會新增在 DNS 伺服器上建立的 Ddns 回復區域下。

如果登入 GlobalProtect 的 GlobalProtect 用戶端屬於未在 DNS 伺服器上設定的非預期網域，則 nsupdate 可能會失敗；在此情況下，請選取 **Ddns Override**（**Ddns** 覆寫），以 DNS 伺服器已知的網域覆寫未知網域。

- **Ddns Override**（**Ddns** 覆寫）—Prisma Access 僅會使用您指定的網域來更新 DNS 伺服器，並覆寫所有其他網域。如果 GlobalProtect 用戶端登入另一個網域，DDNS 服務會使用您在這裡指定的網域來更新 DNS A 和 PTR 記錄。

3. 在 **Domain Name**（網域名稱）欄位中，為回復或網域名稱選取用來更新 PTR 記錄的網域。
4. 選取 **DNS Server IP**（**DNS** 伺服器 **IP**）位址。
5. 選取 **Authentication Type**（驗證類型）（**TSIG** 或 **Kerberos**）。
6. （僅限 TSIG 部署）選取要與 TSIG 搭配使用的 **TSIG Key**（**TSIG** 金鑰）。

   確保 TSIG 檔案的格式是正確的且檔案類型為 .key。

   - 如果您是執行外掛程式版本為 5.2.0 或更高的 Panorama 受管理部署，並且選擇 Kerberos 驗證類型，請透過 .key 檔案上傳驗證金鑰，該檔案


©2025 Palo Alto Networks, Inc.

具有從 DNS 伺服器擷取的 Kerberos 金鑰的 base64 編碼字串，例如：
"ABCDEFGHIJKLMNOPQRSTUV5WXYZOUy5DT00ADUFabcDluaXN0cmF0b3IAAAABAAAAAAEAE

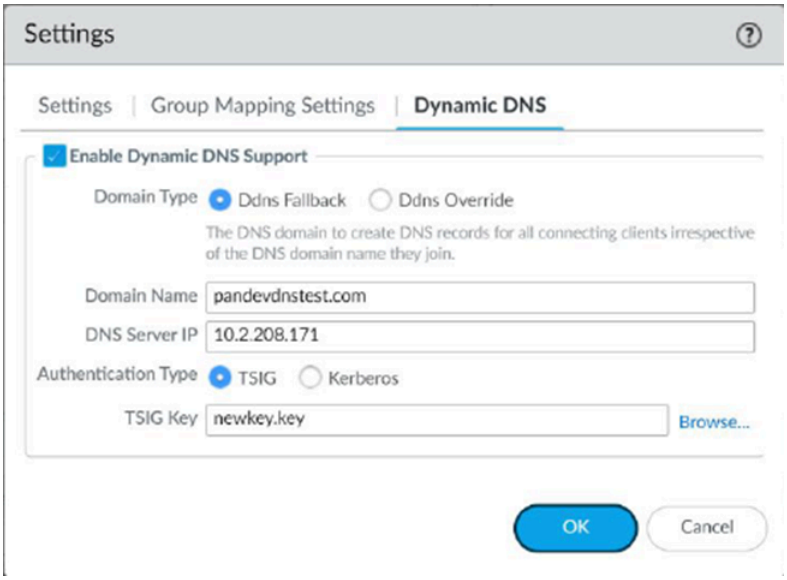
- 如果您是執行外掛程式版本小於 5.1.0 的 Panorama 受管理部署，並且選擇 Kerberos 驗證類型，請透過 .key 檔案上傳驗證金鑰，該檔案具有從 DNS 伺服器擷取的未加密 Kerberos 金鑰標籤檔案。

TSIG 檔案應採用下列格式：

```
key "ddns-gp" { algorithm hmac-sha256; secret
 "aBCDEFGhiJklMNO89PQR+8stUVWX+YZAbcdeFgHI5J="; };
```

7. （僅限 Kerberos 部署）指定要使用的 Kerberos 選項。
   - 輸入 **Kerberos Domain Controller**（**Kerberos** 網域控制器）的 IP 位址。
   - 輸入 **Kerberos Admin Server**（**Kerberos** 管理伺服器）的 IP 位址。
   - 輸入 **Kerberos User Name**（**Kerberos** 使用者名稱）。
   - 輸入要使用的 **Kerberos Key**（**Kerberos** 金鑰）（金鑰標籤）。

     在上傳 Kerberos 金鑰之前，請在其上使用 base64 編碼。



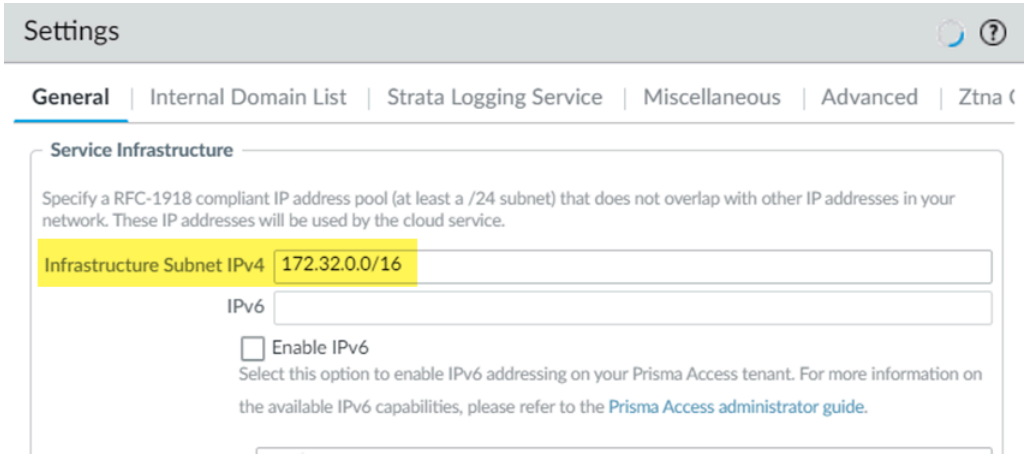

**STEP 6 |** **Save**（儲存）變更。


©2025 Palo Alto Networks, Inc.

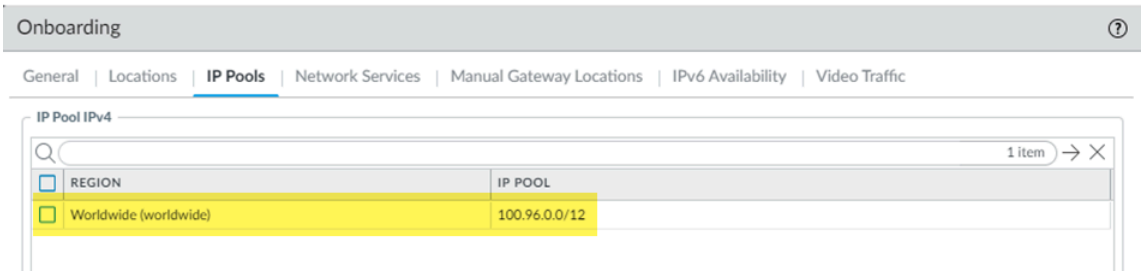
**STEP 7 |** 在 DNS 伺服器上設定正向查閱和反向查閱區域。

請參閱 IPAM 廠商的文件以設定這些區域。此步驟需要您從 Prisma Access 輸入 **Infrastructure Subnet**（基礎結構子網路）和 **Client IP Pool**（用戶端 **IP** 集區）。

- 若要尋找基礎結構子網路，請前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定）、按一下齒輪以編輯 **Settings**（設定），並記下 **Infrastructure Subnet IPv4**（基礎結構子網路 **IPv4**）。



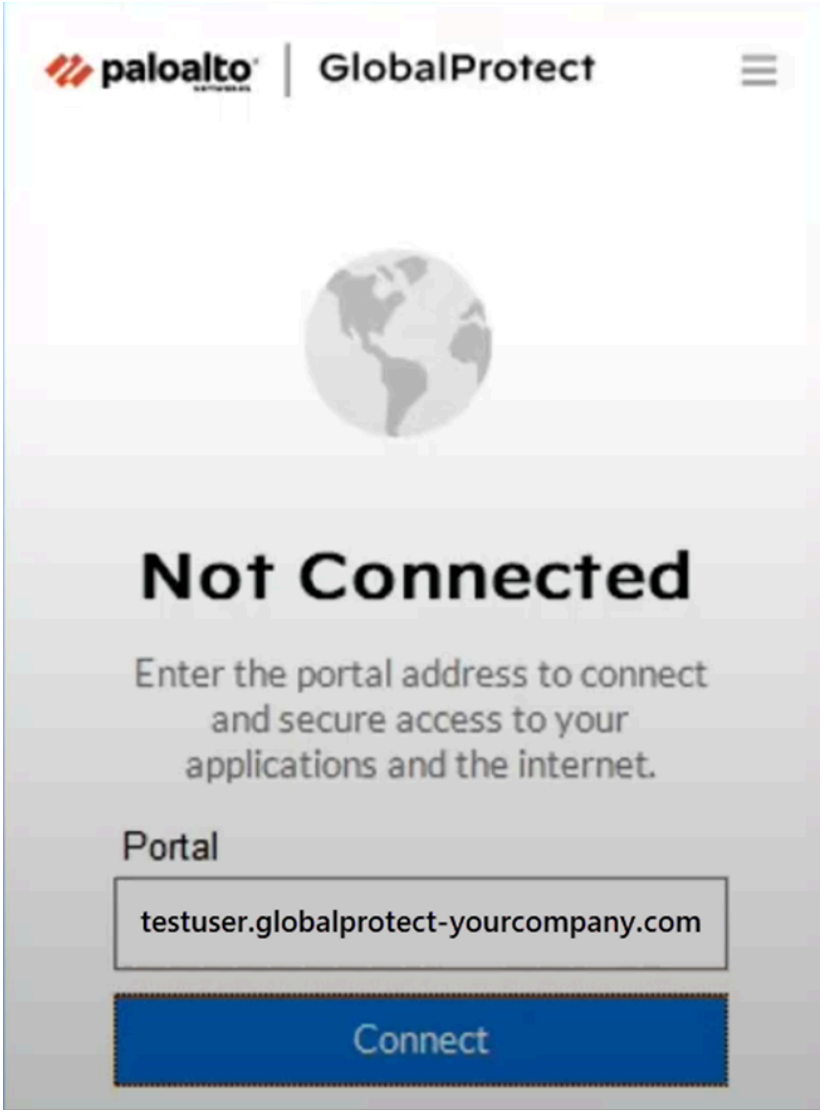

- 若要尋找 GlobalProtect 行動使用者 IP 位址集區，請前往 **Panorama** > **Cloud Services**（雲端服務） > **Mobile Users**—**GlobalProtect**（行動使用者—**GlobalProtect**）、選取 **Hostname**（主機名稱）、選取 **IP Pools**（**IP** 集區），並記下 **IP Pool IPv4**（**IP** 集區 **IPv4**）。




 ©2025 Palo Alto Networks, Inc.

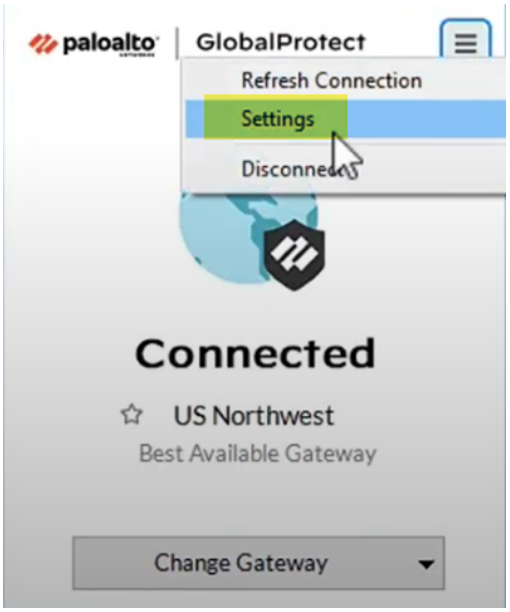
**STEP 8 |** 驗證是否正在 IPAM DNS 伺服器上更新 DNS 記錄。

1. 開啟用戶端電腦並連線至 Prisma Access GlobalProtect 閘道。

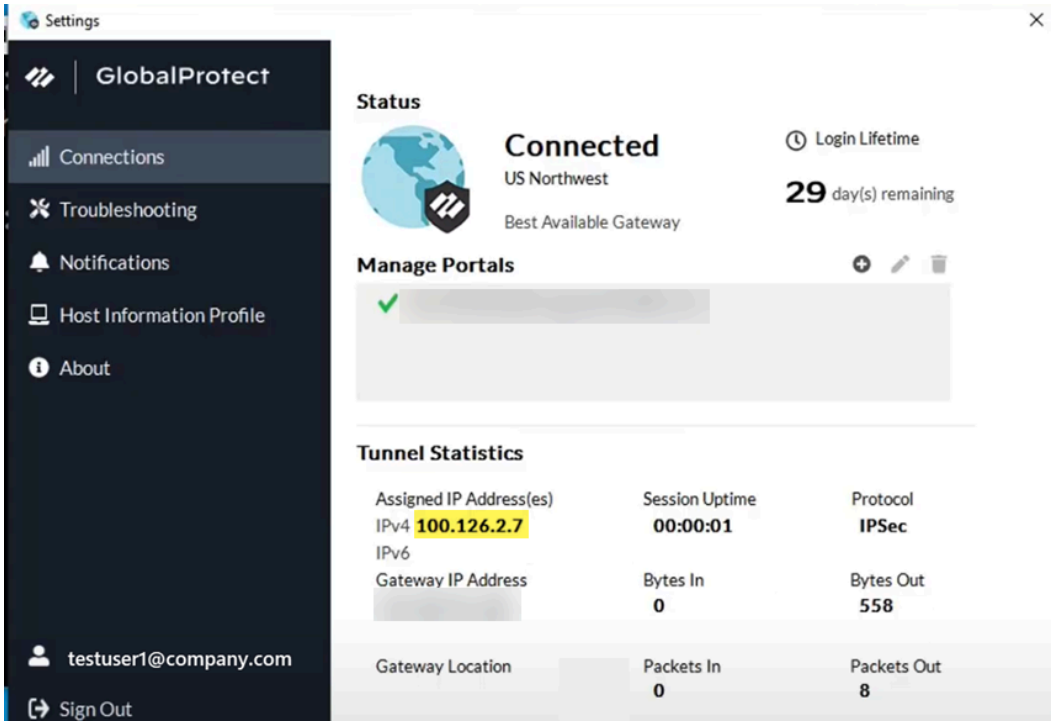



2. 選取 GlobalProtect **Settings**（設定），然後驗證 Prisma Access 指派給使用者的 GlobalProtect IP 位址。


©2025 Palo Alto Networks, Inc.

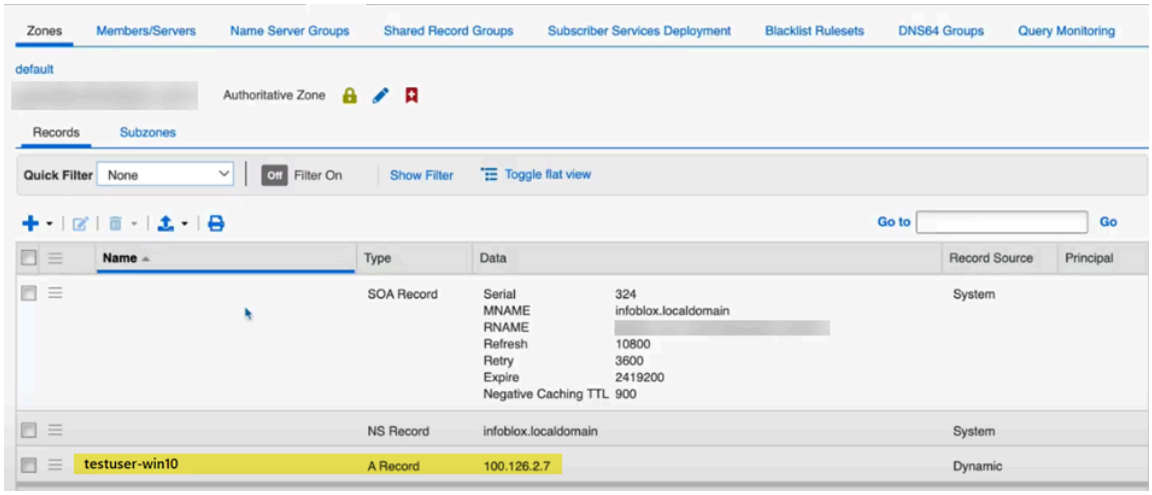



**Assigned IP Address(es)**（指派的 **IP** 位址）(100.126.2.7) 顯示 IP 位址來自 GlobalProtect IP 位址集區 (100.126.0.0/16)。

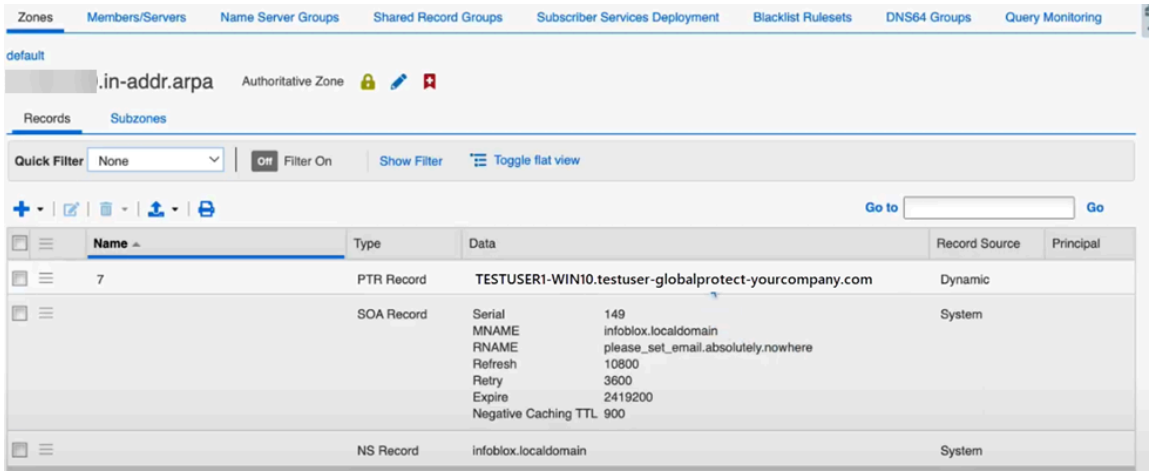



3. 從 IPAM DNS 伺服器檢視使用者的記錄。
   在此範例中，使用者命名為 `testuser1-win10`。

 ©2025 Palo Alto Networks, Inc.




DNS 反向查閱也會在 PTR 記錄中顯示使用者名稱。




4. 將使用者登出 GlobalProtect 並檢查記錄，以確定 DNS 伺服器已刪除使用者的記錄。

# 行動使用者—GlobalProtect 的動態 DNS 註冊支援

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• 由 Panorama 管理的新世代防火牆，具有有效的 Strata Logging Service 授權和雲端服務外掛程式 | ❑ Prisma Access 授權<br>❑ Minimum Required Prisma Access Version：3.1.1 Preferred 或 Innovation<br>❑ 在執行 10.2 和更新版本的 Panoramas 上受支援（在執行 10.1 的 Panoramas 上不受支援）<br>❑ 您的用戶端端點必須加入網域。 |

從 *Prisma Access (Managed by Panorama) 3.1.1* 開始，此功能適用於 *Prisma Access* 部署。

此功能不適用於 *Prisma Access (Managed by Strata Cloud Manager)* 部署。

 ©2025 Palo Alto Networks, Inc.

當行動使用者使用 GlobalProtect 遠端連線到 Prisma Access 時，您企業中的 DNS 伺服器不會使用 GlobalProtect 閘道指派的 IP 位址進行更新。在啟用動態 DNS (DDNS) 之前，沒有通道 IP 位址與端點名稱的對應，這些對應被記錄為位址和指標（A 和 PTR）記錄。因此，您的 IT 管理員或使用者管理軟體無法將遠端端點名稱對應至 IP 位址。

在您於 Prisma Access 上啟用 DDNS 功能之後，Prisma Access 雲端服務外掛程式每 15 分鐘檢查一次 Strata Logging Service 中的 GlobalProtect 事件，以擷取端點主機名稱、網域名稱和通道 IP 位址。它會使用 NSUPDATE 在 DNS 伺服器中動態建立 A 和 PTR 記錄。

行動使用者—**GlobalProtect** 的動態 **DNS** 工作流程

在您啟用 DDNS 之後，並在行動使用者透過 GlobalProtect 應用程式登入時：

閱讀下列章節，以取得 DDNS 運作方式、指導方針與需求，以及如何啟用它的概要。

1. GlobalProtect 會在 GlobalProtect 端點與內部部署或 Prisma Access 閘道之間建立 SSL 通道。
2. GlobalProtect 透過通道將行動使用者裝置的主機名稱、網域名稱和通道 IP 位址資訊傳送到內部部署或 Prisma Access 閘道。
3. 內部部署閘道或 Prisma Access 會將此資訊作為 GlobalProtect 事件轉送至 Strata Logging Service。
4. Prisma Access 雲端服務外掛程式每 15 分鐘探查一次 Strata Logging Service，以更新 DNS 伺服器。

   如果外掛程式未從 Strata Logging Service 收到 GlobalProtect 事件，它最多重試該要求五次。如果重試要求不成功，外掛程式每 15 分鐘重試一次操作，最多重試四次。因此，該外掛程式可以在一小時的時間間隔內接收更新。

   如果您想要更頻繁的更新，可以輸入 `debug plugins cloud_services set-gp-ddns-interval` 命令，將更新間隔變更為五分鐘。A 不需要更新時間間隔。如果您將間隔變更為 5 分鐘，則雲端服務外掛程式最多可以更新 15,000 筆記錄，網路延遲為 50 毫秒，並且可在 20 分鐘的時間間隔內接收更新。

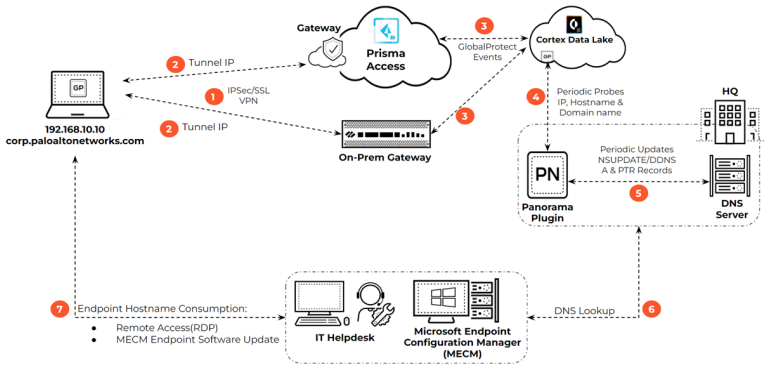
   - 使用該命令變更時間間隔後無需 ***Commit***（提交）。
   - 這些數字來自受控環境，實際操作情況可能會影響這些數字。
5. 在收到來自 Strata Logging Service 的更新之後，雲端服務外掛程式會將 A 和 PTR 記錄封裝為 NSUPDATE，並每 15 分鐘更新一次主要 DNS 伺服器。

   如果您使用 `debug plugins cloud_services set-gp-ddns-interval` 命令將時間間隔變更為五分鐘，則外掛程式每五分鐘更新一次 DNS 伺服器。

   如果外掛程式無法透過 NSUPDATE 更新 DNS 伺服器，則外掛程式最多重試更新操作五次。如果更新不成功，外掛程式每 15 分鐘重試一次更新操作，或者，如果您將間隔變更為五分鐘，則每五分鐘重試一次更新操作，最多四次。因此，外掛程式會嘗試更新記錄的事件，最多一小時（如果您使用 15 分鐘間隔）或 20 分鐘（如果您使用五分鐘間隔），然後重新啟動。
6. 在 DNS 伺服器中提供 GlobalProtect 行動使用者的 A 和 PTR 記錄之後，IT 管理員或企業軟體透過 DNS 或 RDNS 查閱來使用這些記錄，並解析端點名稱或 IP 位址。
7. IT 管理員或端點管理軟體使用此資訊，來管理端點或推送軟體更新。

下圖說明了此工作流程。

 ©2025 Palo Alto Networks, Inc.




若要檢視連線失敗日誌，請為 ***Mobile_User_Device_Group*** 選取 ***Dashboard***（儀表板）***> System Logs***（系統日誌）或 ***Monitor***（監控）***> Logs***（日誌）***> System***（系統）。

動態 **DNS** 指導方針和需求

在啟用 DDNS 之前，請確保您的部署和 DNS 伺服器符合以下指導方針和需求：

- 您的用戶端端點必須加入網域。
- 根據您的作業系統將 GlobalProtect 用戶端更新至下列 GlobalProtect 應用程式版本：
  - Windows：5.2.11 或更新版本
  - Mac：5.2.11 或更新版本
  - Linux：5.3.3 或更新版本
- 啟用 Strata Logging Service，如果您使用的內部部署閘道不是 Prisma Access。
- 需要最低版本為 8.6.1 或更新版本，且支援透過 NSUPDATE 進行 DDNS 更新的 Infoblox DNS 伺服器。
- 多租用戶 Prisma Access 部署不支援 DDNS。
- 以 base64 格式儲存 DNS 伺服器中的驗證金鑰，副檔名為 .key。在 Prisma Access 中，您只能以這種格式上傳金鑰。
- 在您的 DNS 伺服器上啟用 NTP，並確保它與 Prisma Access 的 NTP 相同。
- 在 Infoblox 中為反向 PTR 和正向 A 位址建立區域。

您可以使用新世代防火牆以及 *Prisma Access*，在獨立部署中部署動態 *DNS*。對於防火牆，本節中的所有先決條件都適用，並且您還必須擁有一個有效的 *Strata Logging Service* 授權，並使用 Panorama 中的雲端服務外掛程式進行記錄。

## 為行動使用者—GlobalProtect 啟用 DDNS

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

若要使用 GlobalProtect 行動使用者的 A 和 PTR 記錄更新您的 DNS 伺服器，請完成下列步驟。

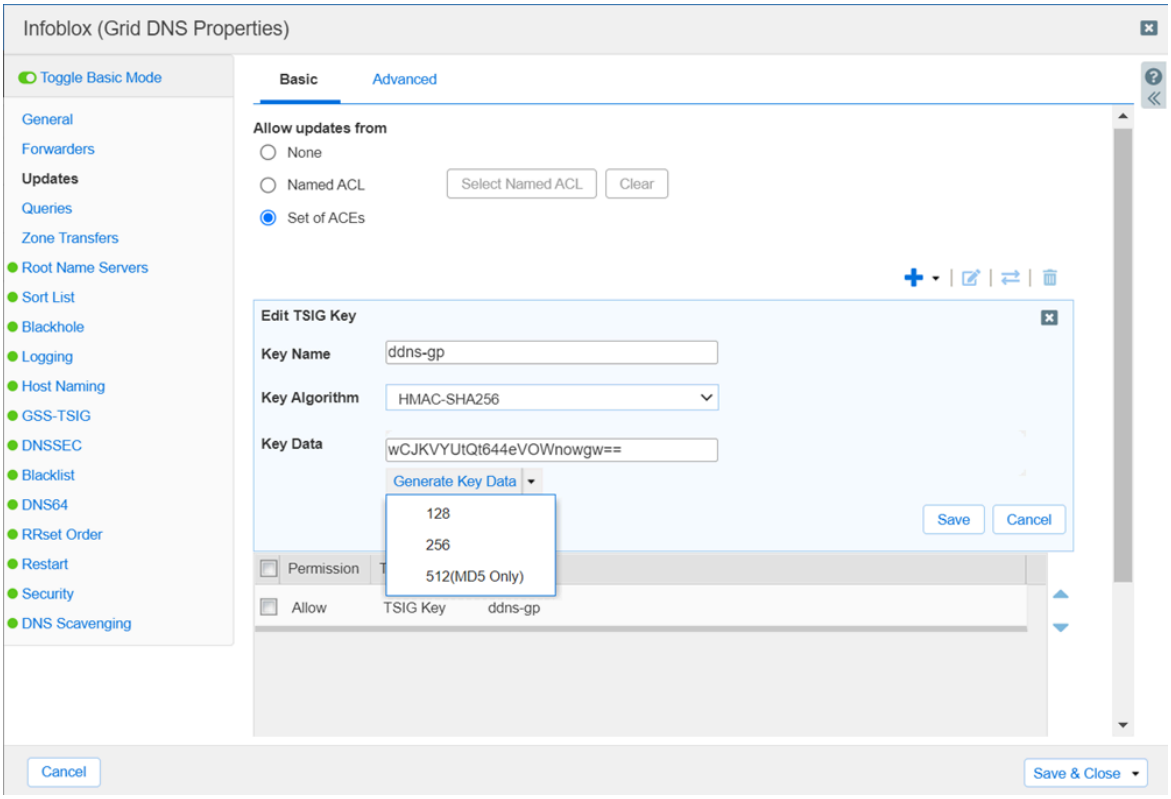

©2025 Palo Alto Networks, Inc.

**STEP 1 |** 在您的 DNS 伺服器中建立驗證金鑰。

此範例使用 Infoblox 作為 *DNS* 伺服器。

1. 登入您的 DNS 伺服器。
2. 選取 **Data Management**（資料管理） > **DNS** > **Grid DNS Properties**（網格 **DNS** 屬性） > **Updates**（更新）。
3. 允許來自 **Set of ACEs**（**ACE** 集）的更新。
4. 填寫詳細資訊後新增 **TSIG Key**（**TSIG** 金鑰）。

   - 選取 ***256*** 金鑰演算法。
   - ***Generate Key Data***（產生金鑰資料）以建立新金鑰。選取 ***256*** 金鑰資料。




5. 以下列格式將金鑰資料複製到檔案，並以 .key 副檔名儲存該檔案。

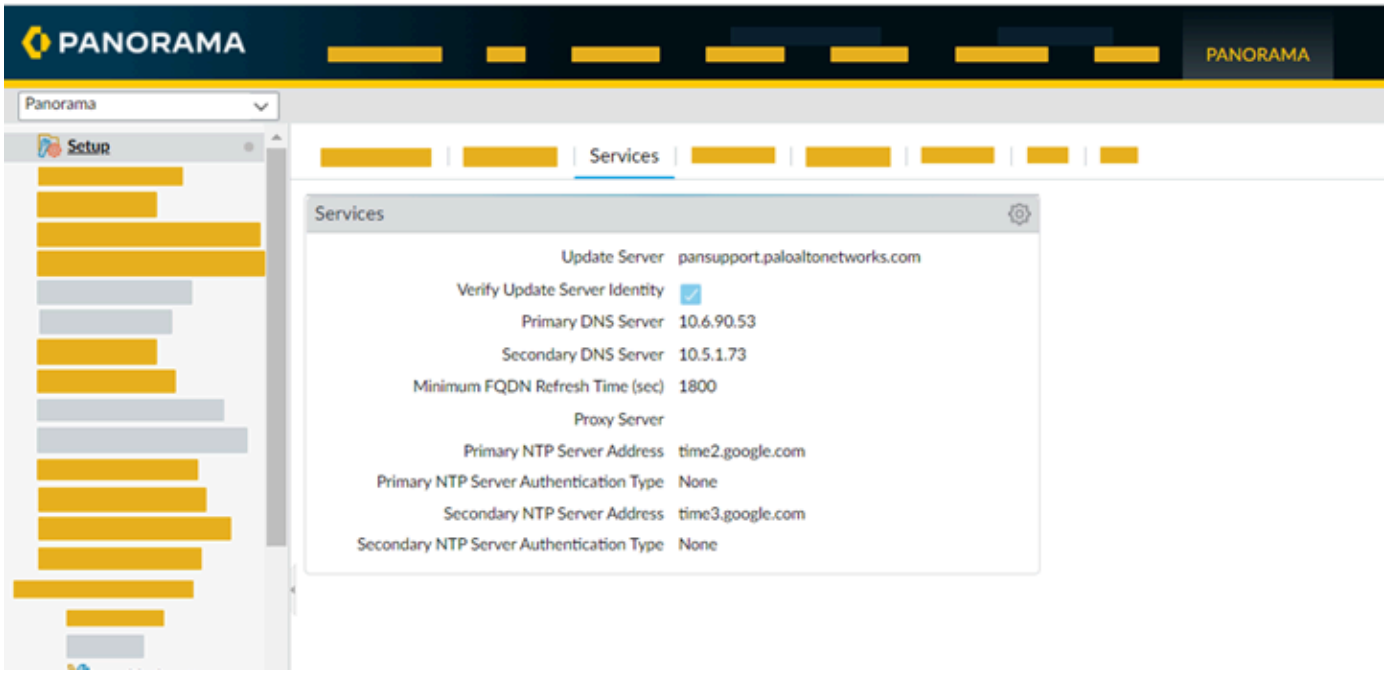
```
key "ddns-gp" { algorithm hmac-sha256; secret
 "wCJKVYUtQt644eVOWnowgw=="; };
```

您會在稍後步驟中將此金鑰上傳到 Prisma Access 雲端服務外掛程式。


©2025 Palo Alto Networks, Inc.

**STEP 2 |** 在您的 Prisma Access 部署時，指定您的 DNS 伺服器作為主要 DNS 伺服器。

1. 選取 **Panorama** > **Setup**（設定） > **Services**（服務）。
2. **Edit**（編輯）設定並更新主要 DNS 伺服器詳細資訊。

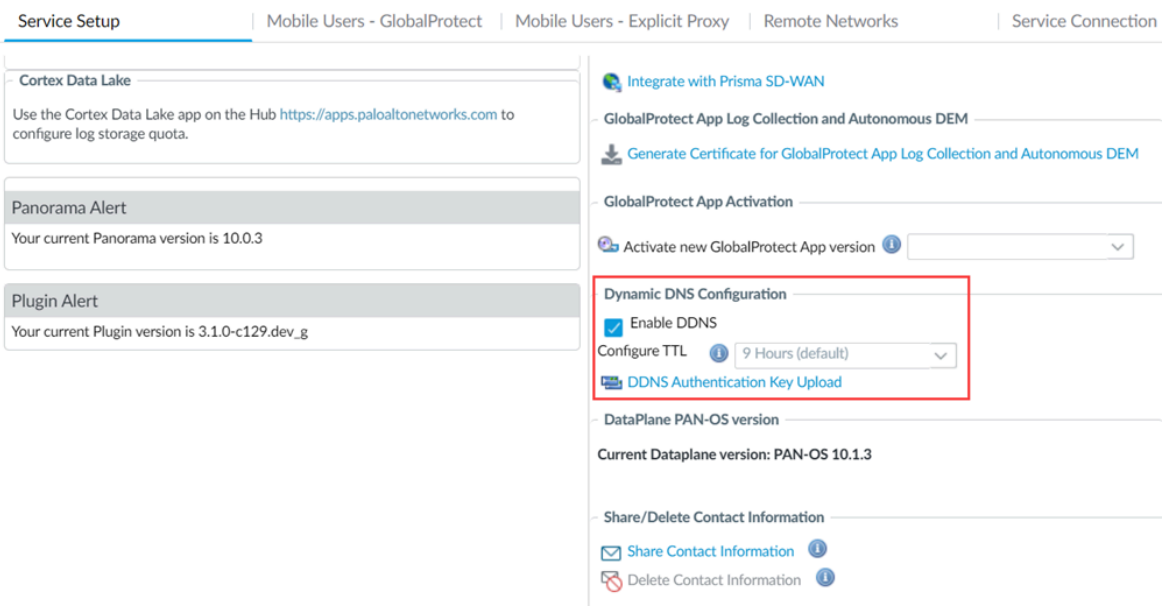



 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 設定 DDNS 設定。

1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定）。
2. 選取 **Service Operations**（服務操作） > **Dynamic DNS Configuration**（動態 **DNS** 設定）並 **Enable DDNS**（啟用 **DDNS**）。
3. （選用）**Configure TTL**（設定 **TTL**）（這是存留時間 (TTL) 值）為您想要 Prisma Access 重新整理其快取中 FDQN 的頻率。

   根據預設，該值設定為 9 小時。




4. 從您的 DNS 伺服器上傳您在步驟 1 中建立的 DDNS 驗證金鑰。

**STEP 4 |** **Commit to Panorama**（提交至 **Panorama**）。

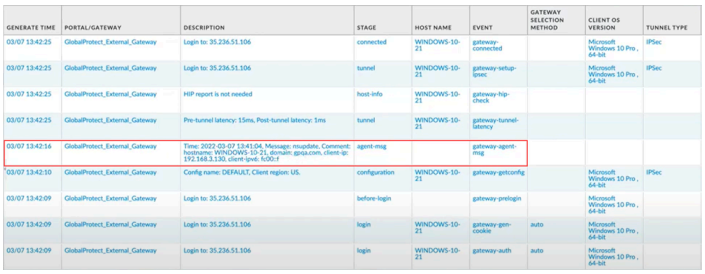
## 驗證動態 DNS 設定

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
|---|---|
| • Panorama | • Prisma Access 授權 |

在啟用了 DNS 之後，請檢查以下 Prisma Access 元件來監控日誌，並針對任何問題進行疑難排解。

選取 **Monitor**（監控） > **Logs**（日誌） > **GlobalProtect**。閘道代理程式包含主機名稱、網域名稱和通道 IP 位址資訊。僅在端點是網域或 AD 的一部分時，GlobalProtect 才會傳送代理程式訊息。


©2025 Palo Alto Networks, Inc.



檢查 Panorama CLI 中的 `gp_ddns_support.log` 命令來檢視其他 DDNS 日誌。

# 在 Prisma Access GlobalProtect 部署中識別和隔離遭入侵裝置

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 授權 |

Prisma Access 允許您識別和隔離與 GlobalProtect 應用程式連線的遭入侵裝置。若要這樣做，請手動或自動將裝置新增至隔離清單。在隔離裝置之後，您可以封鎖隔離的裝置存取網絡，以確保政策一致性。

每個 Prisma Access 行動使用者位置會在管理 Prisma Access 的 Panorama 與其最近的服務連線之間傳送和接收其隔離資訊。如果有新世代防火牆或閘道，您應該讓服務連線將隔離清單資訊重新散佈至 Panorama 和內部部署防火牆或閘道，以及從中重新散佈此資訊。您還應該將來自 Panorama 的隔離清單資訊重新散佈至服務連線，以確保對 Prisma Access 中的所有行動使用者位置（閘道）強制執行一致的政策。

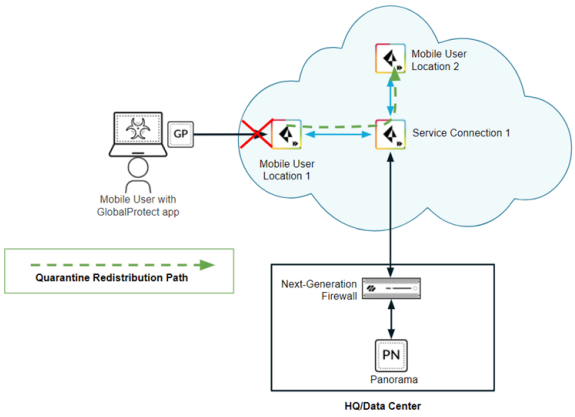
## 隔離清單重新散佈的使用案例

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 授權 |

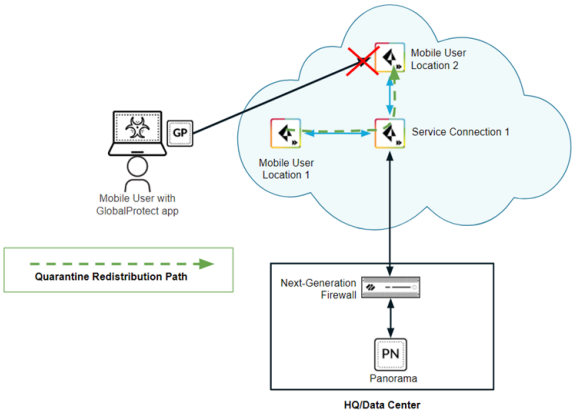
下節描述一些常見的 Prisma Access 部署，其中隔離清單重新散佈有助於對遭入侵裝置進行一致的政策強制執行。

 ©2025 Palo Alto Networks, Inc.

- 連線到相同服務連線的行動使用者位置之間的隔離清單重新散佈—在以下範例中，連線到行動使用者位置 1 的 GlobalProtect 行動使用者遭到入侵並將其自動隔離。Prisma Access 根據政策封鎖或限制隔離裝置。

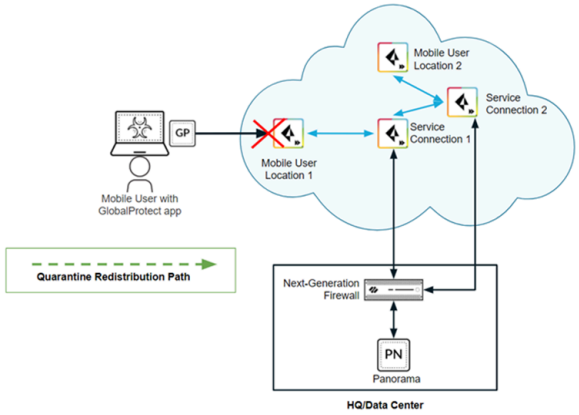



服務連線（本範例中的服務連線 1）在連線其的所有行動使用者位置之間重新散佈隔離清單資訊。由於行動使用者位置 2 藉由服務連線 1 接收重新散佈的隔離清單資訊，因此 GlobalProtect 行動使用者連線到行動使用者位置 2 的嘗試也會遭到封鎖。




 ©2025 Palo Alto Networks, Inc.

- 在連線到不同服務連線的行動使用者位置之間進行隔離清單重新散佈—在以下範例中，有兩個行動使用者位置，但它們連線到兩個不同的服務連線。GlobalProtect 使用者已嘗試連線到行動使用者位置 1。行動使用者位置 1 將 GlobalProtect 使用者端點偵測為遭到入侵並將其隔離。

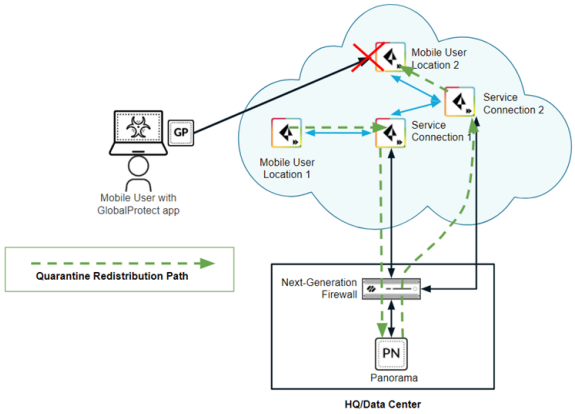



若要將隔離清單資訊從行動使用者位置 1 重新散佈到行動使用者位置 2，請執行下列動作：

- 將隔離清單資訊從服務連線 1 重新散佈到 Panorama。
- 將隔離清單資訊從 Panorama 重新散佈到服務連線 2。

透過此設定，當 GlobalProtect 使用者連線到行動使用者戶位置 1 並遭隔離時，隔離清單資訊會從行動使用者戶位置 1 重新散佈到行動使用者位置 2，並且封鎖對行動使用者位置 2 的任何連線嘗試。

如果 *GlobalProtect* 使用者連線到行動使用者位置 *2* 並遭隔離，此設定還是有效的；隔離清單資訊會從行動使用者位置 *2* 重新散佈到行動使用者位置 *1*。



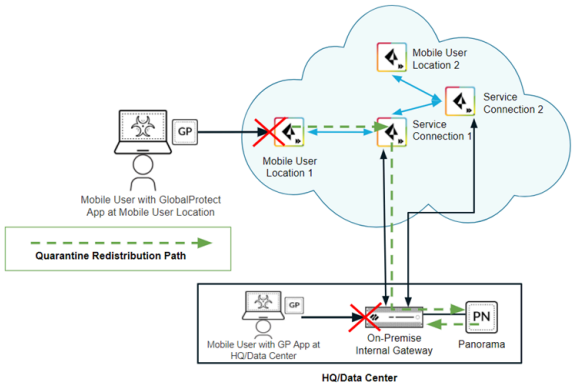

- 在 **Prisma Access** 與新世代防火牆或閘道之間進行隔離清單重新散佈—在以下範例中，GlobalProtect 使用者已嘗試連線到行動使用者位置 1。行動使用者位置 1 將 GlobalProtect

 ©2025 Palo Alto Networks, Inc.

使用者端點偵測為遭到入侵並將其隔離。然後，行動使用者前往公司總部並嘗試再次登入。總部受到使用內部主機偵測設定為 GlobalProtect 閘道的新世代防火牆的保護。

行動使用者位置 1 透過服務連線 1 將隔離清單資訊重新散佈到 Panorama，而 Panorama 將隔離清單資訊重新散佈到內部部署內部閘道。當使用者嘗試從總部位置登入時，GlobalProtect 偵測到內部部署閘道被設定為內部閘道，並在沒有通道的情況下連線到該閘道。

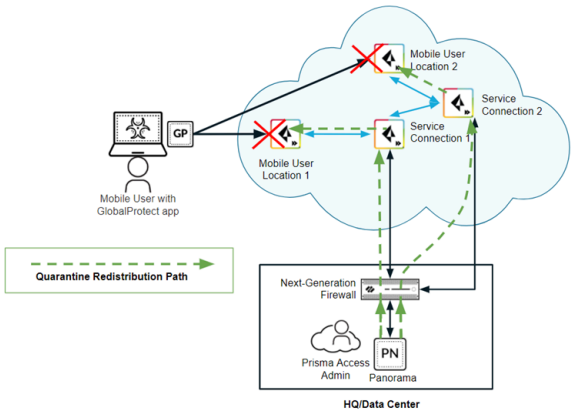
由於隔離清單資訊已重新散佈至內部部署閘道，因此根據設定的使用者政策，使用者在閘道處遭到封鎖。




如果您使用新世代防火牆或閘道搭配 Prisma Access，則應該設定 Panorama，將隔離清單資訊重新散佈到防火牆或閘道、所有服務連線和 Panorama。

- 管理員在 **Panorama** 手動隔離行動使用者—在此範例中，Prisma Access 管理員已在管理 Prisma Access 的 Panorama 設備中手動將行動使用者新增至隔離清單。管理員已在 Panorama、新世代防火牆和服務連線之間設定重新散佈。Panorama 將更新的隔離清單資訊重新散佈到防火牆和服務連線。然後，服務連線將隔離清單資訊重新散佈到行動使用者位置。

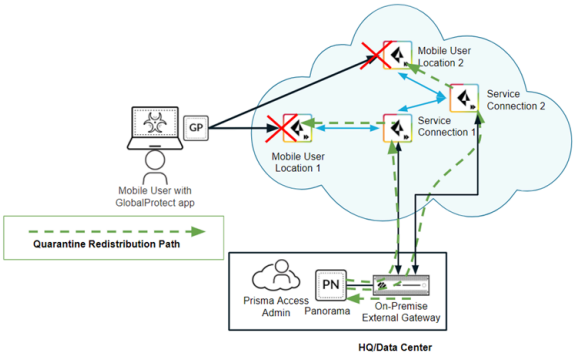
  行動使用者已連接到行動使用者位置 1。在行動使用者位置 1 收到更新的隔離清單資訊之後，使用者連線中斷。如果使用者嘗試連線到行動使用者位置 2，連線將遭封鎖，並且行動使用者會收到隔離通知。




 ©2025 Palo Alto Networks, Inc.

- 行動使用者在內部部署閘道處自動或手動隔離—在此範例中，有一個新世代防火牆已在總部或資料中心位置設定為外部閘道。管理員已在外部閘道手動隔離行動使用者。外部閘道將隔離清單資訊從外部閘道重新散佈到 Panorama。

  在 Panorama 已從外部閘道收到更新的隔離清單資訊之後，其會將該資訊重新散佈到服務連線 1 和 2，然後服務連線將該資訊重新散佈到行動使用者位置 1 和 2。如果行動使用者嘗試連線到行動使用者位置 1 或 2，Prisma Access 會封鎖連線且使用者會收到隔離通知。




## 在 Prisma Access 中設定隔離清單重新散佈

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 授權 |

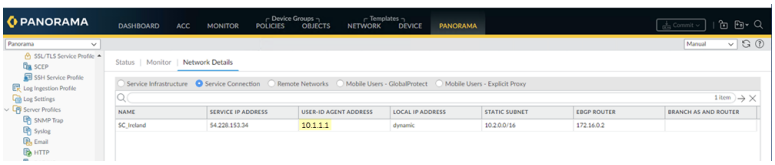
若要將隔離資訊重新散佈至服務連線、管理 Prisma Access 的 Panorama 和新世代防火牆，以及從中重新散佈，請完成以下步驟。


©2025 Palo Alto Networks, Inc.

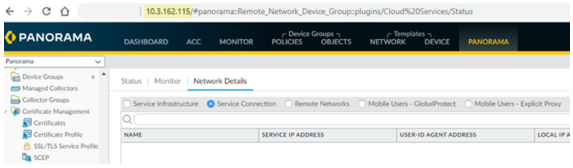
**STEP 1 |** 確保針對您想要將隔離清單資訊重新散佈至其中的所有服務連線，Panorama 管理 IP 位址能夠與其 User-ID 代理程式位址通訊。

服務連線的 User-ID 代理程式位址與 Panorama 的管理 IP 位址之間需要通訊，Prisma Access 才能在 Panorama 與服務連線之間傳送和接收隔離清單資訊。

- 若要尋找 **User-ID Agent Address**（**User-ID** 代理程式位址），請選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Service Connection**（服務連線） > **User-ID Agent Address**（**User-ID** 代理程式位址）。




- 若要尋找管理 Prisma Access 的 Panorama 的管理 IP 位址，請記下當您存取 Panorama 時 Web 瀏覽器中顯示的 IP 位址。




**STEP 2 |** 允許 Prisma Access 重新散佈隔離清單資訊。

1. 在 Panorama 中，選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定）。
2. 按一下齒輪圖示以編輯設定。
3. 在 **Advanced**（進階）頁籤中，選取 **Enable Quarantine List Redistribution**（啟用隔離清單重新散佈）。

   啟用隔離清單重新散佈允許 Prisma Access 將從一個或多個行動使用者位置（閘道）接收的隔離清單資訊重新散佈服務連線。

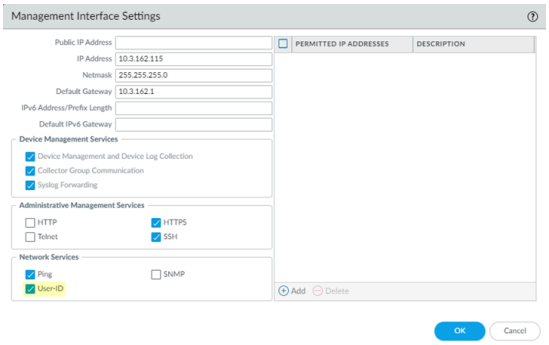



**STEP 3 |** **Commit**（提交）並 **Push**（推送）您的變更。

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 設定管理介面設定，將 Panorama 設定為從 Prisma Access 接收隔離清單資訊。

1. 在管理 Prisma Access 的 Panorama 中，選取 **Panorama** > **Setup**（設定） > **Interfaces**（介面）。
2. 選擇 **Management**（管理）介面。
3. 選取 **User-ID**。




**STEP 5 |** 設定資料重新散佈代理程式，將隔離清單資訊從服務連線重新散佈至 Panorama。

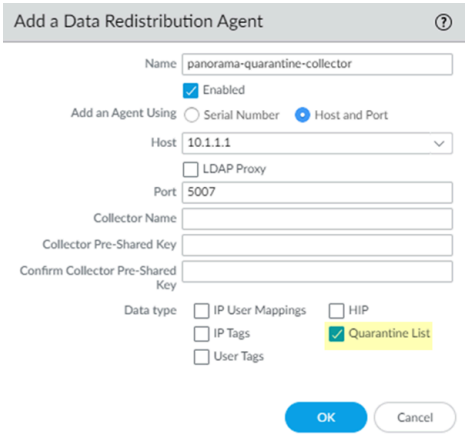
1. 從管理 Prisma Access 的 Panorama 中，選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Service Connection**（服務連線）。
2. 為每個服務連線記下 **User-ID Agent Address**（**User-ID** 代理程式位址）（**Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊）


©2025 Palo Alto Networks, Inc.

> **Service Connection**（服務連線） > **User-ID Agent Address**（**User-ID** 代理程式位址））。

3. 選取 **Panorama** > **Data Redistribution**（資料重新散佈） > **Agents**（代理程式）。
4. **Add**（新增）資料重新散佈代理程式、給與它一個 **Name**（名稱），然後選取 **Enabled**（已啟用）。
5. 輸入服務連線的 **User-ID Agent Address**（**User-ID** 代理程式位址）作為 **Host**（主機），以及輸入 5007 作為 **Port**（連接埠）。

   確保您的網路不會封鎖在 *Panorama* 與 *Prisma Access* 之間對此連接埠的存取。
6. （選用）如果您已將此服務連線設定為收集器（**Device**（裝置） > **Data Redistribution**（資料重新散佈） > **Collector Settings**（收集器設定）），請輸入 **Collector Name**（收集器名稱）和 **Collector Pre-Shared Key**（收集器預先共用金鑰）
7. 選取 **Quarantine List**（隔離清單）；然後，按一下 **OK**（確定）。




8. 針對 Prisma Access 部署中的所有服務連線重複步驟 5。

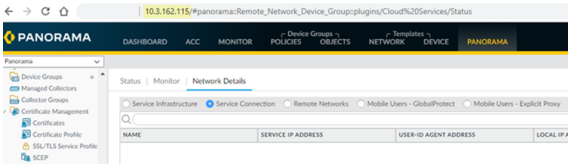
**STEP 6 |** 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**），以在管理 Prisma Access 的 Panorama 上本機儲存您的變更。


©2025 Palo Alto Networks, Inc.

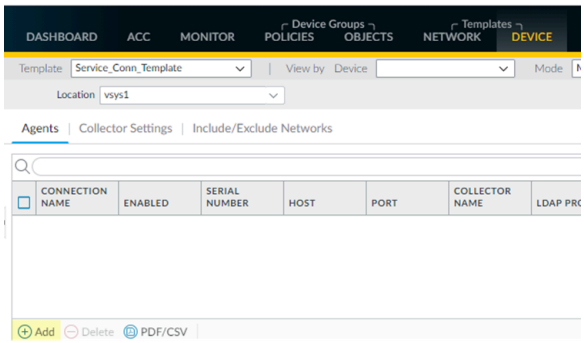
**STEP 7 |** 設定資料重新散佈代理程式，將隔離清單資訊從 Panorama 重新散佈至服務連線。

1. 尋找管理 Prisma Access 的 Panorama 的管理 IP 位址。

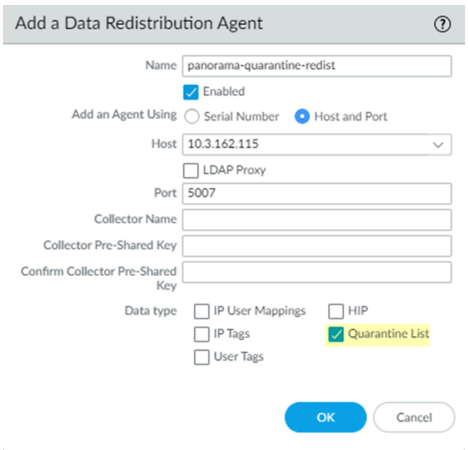
   當您存取 Panorama 時，此位址會顯示在 Web 瀏覽器位址列中。




2. 確保您位於 **Service_Conn_Template** 範本中，然後選取 **Device**（裝置） > **Data Redistribution**（資料重新散佈） > **Agents**（代理程式）。




3. **Add**（新增）資料重新散佈代理程式、給與它一個 **Name**（名稱），然後選取 **Enabled**（已啟用）。
4. 輸入 Panorama 設備的管理 IP 位址作為 **Host**（主機），以及輸入 5007 作為 **Port**（連接埠）。



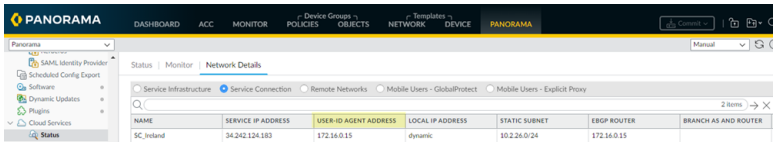

5. 選取 **Quarantine List**（隔離清單）；然後，按一下 **OK**（確定）。

 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** 設定資料重新散佈代理程式，將隔離清單資訊從服務連線重新散佈至行動使用者閘道。

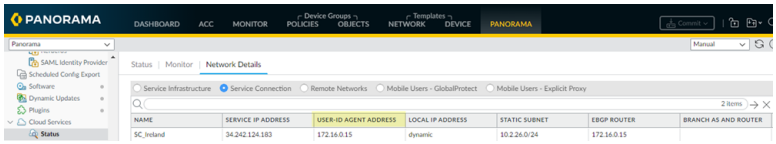
1. 從管理 Prisma Access 的 Panorama 中，選取 **Panorama** > **Cloud Services**（雲端服務）> **Status**（狀態） > **Network Details**（網路詳細資訊） > **Service Connection**（服務連線）。
2. 記下服務連線的 **User-ID Agent Address**（**User-ID** 代理程式位址），您想要從這個服務連線重新散佈隔離清單資訊。

   由於所有服務連線都具有相同的重新散佈隔離清單資訊，因此請選擇任何服務連線。您還可以設定多個服務連線。




3. 確保您位於 **Mobile_User_Template** 範本中，然後選取 **Device**（裝置） > **Data Redistribution**（資料重新散佈） > **Agents**（代理程式）。
4. **Add**（新增）資料重新散佈代理程式、給與它一個 **Name**（名稱），然後選取 **Enabled**（已啟用）。
5. 輸入服務連線的 **User-ID Agent Address**（**User-ID** 代理程式位址）作為主機，以及輸入 **5007** 作為連接埠。

   確保您的網路不會封鎖在 *Panorama* 與 *Prisma Access* 之間對此連接埠的存取。
6. （選用）如果您已將此服務連線設定為收集器（**Device**（裝置） > **Data Redistribution**（資料重新散佈） > **Collector Settings**（收集器設定）），請輸入 **Collector Name**（收集器名稱）和 **Collector Pre-Shared Key**（收集器預先共用金鑰）。
7. 選取 **Quarantine List**（隔離清單）；然後，按一下 **OK**（確定）。




8. **Commit and Push**（提交並推送）您的變更。

**STEP 9 |** 選取 **Panorama** > **Device Quarantine**（裝置隔離），來檢視您的隔離清單資訊。

如需詳細資訊，請參閱 GlobalProtect 管理員指南中的檢視已隔離裝置資訊。

# 將行動使用者—GlobalProtect 部署中的 IPv6 流量導向至不同的位置

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

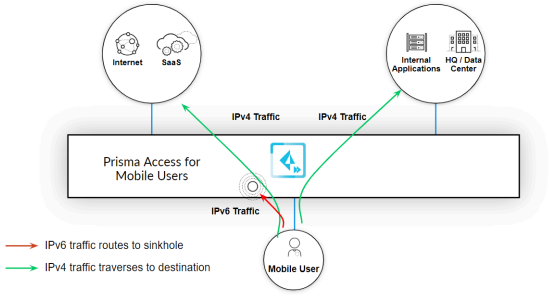

©2025 Palo Alto Networks, Inc.

在可以同時處理 IPv4 和 IPv6 流量的雙堆疊端點中，GlobalProtect 應用程式會將透過 GlobalProtect VPN 通道保護的行動使用者 IPv4 流量傳送至 Prisma Access。不過，行動使用者 IPv6 流量預設不會傳送到 Prisma Access，而是傳送到端點上的本機網路介面卡。為了減少 IPv6 型威脅的攻擊面，Palo Alto Networks 建議您設定 Prisma Access 以將 IPv6 流量導向至不同的位置。因為端點可以自動回復到 IPv4 位址，所以您可以為流向網際網路的行動使用者流量啟用安全且不間斷的使用者體驗。

預設 *IPv6* 路由優先於其他路由。不過，如果實體網路介面存在更具體的 *IPv6* 路由，或者如果您指定實體介面的 *IPv6* 來源位址，則此類流量將傳送至本機網路介面卡。

此外，Palo Alto Networks 建議您將 GlobalProtect 設定為完全停用本機網路介面卡上的網路流量。如果您有內部部署新世代防火牆設定為 GlobalProtect 閘道的混合 Prisma Access 部署，則可以在內部部署 GlobalProtect 閘道上設定 IPv6 Sinkhole 功能。

您可以設定 Prisma Access，以便其可以將所有行動使用者 IPv6 流量導向不同位置。啟用此功能時，除了 IPv4 位址之外，Prisma Access 會將 IPv6 位址指派給連線端點；然後，它會使用內建的安全性政策將 IPv6 流量路由至 Prisma Access 並將其捨棄，如下圖所示。



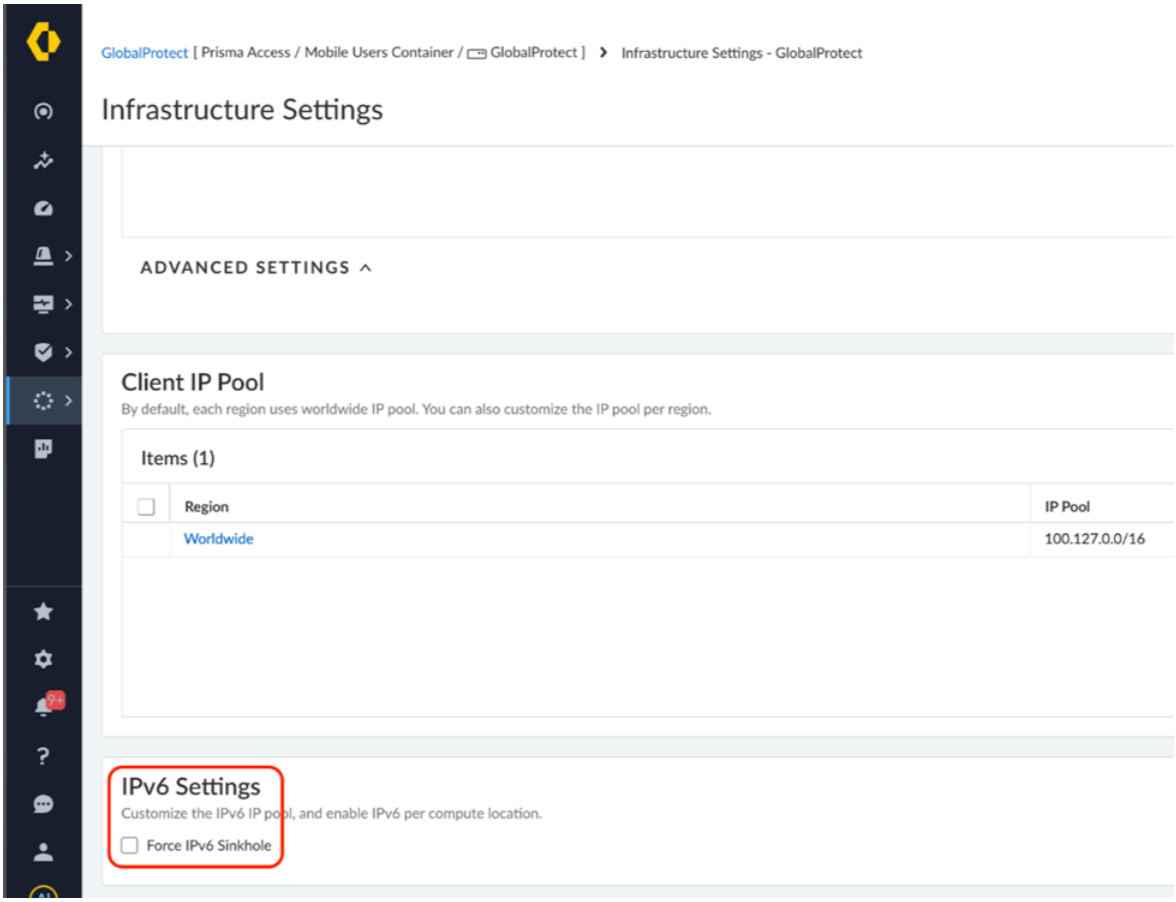

若要設定 Prisma Access，以便其可以將所有行動使用者 IPv6 流量導向不同位置，請完成下列步驟。


©2025 Palo Alto Networks, Inc.

- Prisma Access (Managed by Strata Cloud Manager) 部署：

  前往 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 設定） > **Mobile Users**（行動使用者） > **GlobalProtect Setup**（**GlobalProtect** 設定） > **Advanced Settings**（進階設定）然後選取 **Force IPv6 Sinkhole**（強制執行 **IPv6 Sinkhole**）。

  Prisma Access 會使用 fc00:0:0:0:0:0:0:0/64 作為 Sinkhole 位址。




- Prisma Access (Managed by Panorama) 部署：

  1. 使用您用來登入管理 Prisma Access 之 Panorama 的 IP 位址，開啟具有管理員權限的安全 CLI 工作階段。
  2. 輸入 `configure` 以進入設定模式。
  3. 輸入 **`set plugins cloud_services mobile-users ipv6 yes`** 命令。

     如果您將來需要停用此命令，請輸入 **`set plugins cloud_services mobile-users ipv6 no`**。
  4. 輸入 **`Commit`** 以在本機儲存您的變更。
  5. 輸入 **`exit`** 以結束設定模式。
  6. 輸入 **`commit-all shared-policy include-template yes device-group Mobile_User_Device_Group`**，以提交並推送您的變更，並使其在 Prisma Access 處於作用中狀態。


©2025 Palo Alto Networks, Inc.

# 設定 GlobalProtect 以停用對區域網路的直接存取

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ 在所有 macOS 和 Windows GlobalProtect 端點上都受到支援。在從 GlobalProtect 應用程式版本 6.0.0 開始的 Linux 端點上受到支援。 |

若要確保所有行動使用者流量都傳送到 Prisma Access，您可以完全停用將傳出連線（包括本機子網路流量）傳送到本機介面卡。您可以透過對 GlobalProtect 閘道進行設定變更來停用與本機介面卡的所有傳出連線.

您可以在 Panorama 或在已設定為 GlobalProtect 閘道的本機防火牆上執行以下步驟。

啟用「禁止直接存取本機網路」設定可降低不受信任網路（例如惡意 *Wi-Fi* 存取點）帶來的風險。

**STEP 1 |** 選取 **Network**（網路） > **GlobalProtect** > **Gateways**（閘道）。

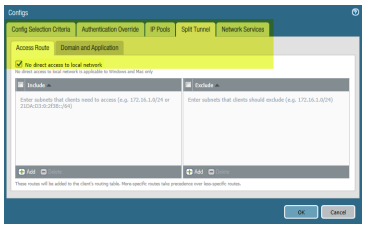
**STEP 2 |** 選取現有的 GlobalProtect 閘道或 **Add**（新增）一個。

**STEP 3 |** 選取 **Agent**（代理程式） > **Client Settings**（用戶端設定）。

**STEP 4 |** 選取 **DEFAULT**（預設）設定或 **Add**（新增）一個。

**STEP 5 |** 選取 **Split Tunnel**（分割通道）；然後，選取 **No direct access to local network**（無法直接存取區域網路）。

停用區域網路存取會導致所有流量（包括 *IPv4* 和 *IPv6* 流量）傳送到本機介面卡。此外，您將無法存取本機子網路上的資源，例如印表機。基於存取路由、目的地網域和應用程式分割通道流量仍按預期工作。




**STEP 6 |** （僅限 Panorama 和 Prisma Access 部署）在本機提交您的變更，使其在 Panorama 作用中。

1. 選取 **Commit**（提交） > **Commit to Panorama**（提交至 **Panorama**）。
2. 確保您的變更是 **Commit Scope**（提交範圍）的一部分。
3. 按一下 **OK**（確定），以儲存您對推送範圍所做的變更。
4. **Commit**（提交）您的變更。


©2025 Palo Alto Networks, Inc.

**STEP 7 |** **Commit**（提交）並 **Push**（推送）您的變更，使其在 Prisma Access 作用中。

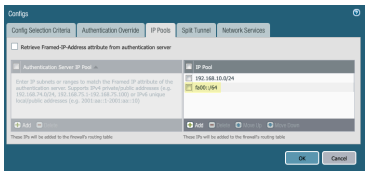
## 在內部部署閘道上設定 IPv6 Sinkhole

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

如果您有一個混合部署，使用設定為閘道的新世代防火牆搭配 Prisma Access，則在內部部署閘道上執行以下工作以丟棄 IPv6 流量。

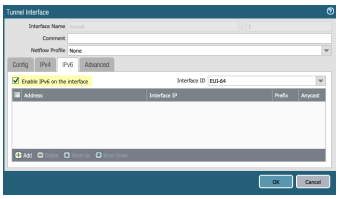
**STEP 1 |** 將 IPv6 IP 集區新增到您的 GlobalProtect 代理程式設定。

1. 選取 **Network**（網路） > **GlobalProtect** > **Gateways**（閘道）。
2. 選取現有的 GlobalProtect 閘道或 **Add**（新增）一個。
3. 選取 **Agent**（代理程式） > **Client Settings**（用戶端設定）。
4. 選取要修改的代理程式設定，或者 **Add**（新增）一個。
5. 選取 **IP Pools**（**IP** 集區）；然後 **Add**（新增）一個要指派給端點上虛擬網路介面卡的 IPv6 集區，而這些端點連線至用於行動網路流量的GlobalProtect 閘道，然後按一下 **OK**（確定）。



**STEP 2 |** 在介面上啟用 IPv6。

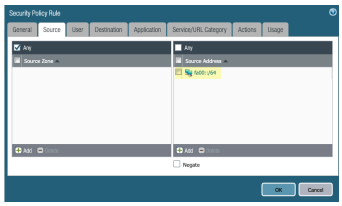
1. 選取 **Device**（裝置） > **Interface**（介面） > **Tunnel**（通道），並選取您用於行動使用者流量的通道 **Interface**（介面）。
2. 選取 **IPv6**，然後選取 **Enable IPv6 on the interface**（在介面上啟用 **IPv6**）。



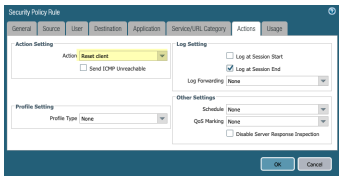
 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 新增安全性政策以設定 TCP 重設動作，其將終止具有 IPv6 來源流量的工作階段，這些流量會比對您在步驟 1 中設定的 IP 集區。

1. 選取 **Policies**（原則） > **Security**（安全性），然後**Add**（新增）一個新的安全性原則。
2. 將規則中的 **Source Address**（來源位址）設定為比對您在步驟 1 中設定的 IP 集區。



3. 選取 **Actions**（動作）；然後，選取 **Action Setting**（動作設定）為 **Reset Client**（重設用戶端），並按一下 **OK**（確定）。



**STEP 4 |** **Commit**（提交）您的變更。

**STEP 5 |** （選用）在您的部署中對所有閘道防火牆上執行此工作。

# 使用 Prisma Access 重新散佈 HIP 資訊

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

若要確保強制執行一致的主機資訊設定檔 (HIP) 政策，並簡化政策管理，您可以將從行動使用者和遠端網路中的使用者（他們使用 GlobalProtect 應用程式）收到的 HIP 資訊從 Prisma Access 重新散佈到您企業中的其他閘道、防火牆和 Panorama 設備，包括管理 Prisma Access 的 Panorama。

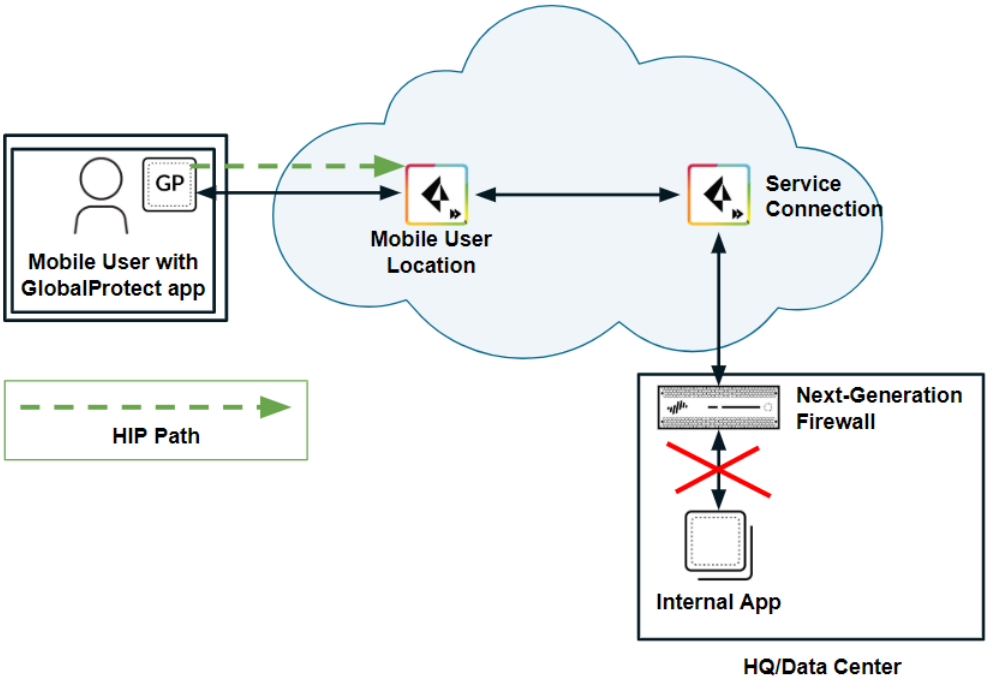
下節描述一些常見的 Prisma Access 部署，其中 HIP 重新散佈對於一致的政策強制執行和 HIP 報告檢視很有用：

- **HIP 從 Prisma Access 重新散佈至新世代防火牆**—如果您在組織的資料中心或總部位置具有新世代防火牆，並且已使用 HIP 型安全性政策設定了該防火牆，則無法對 Prisma Access 行動使用者強制執行這些政策，直到您將 HIP 資訊從 Prisma Access 重新散佈至防火牆。

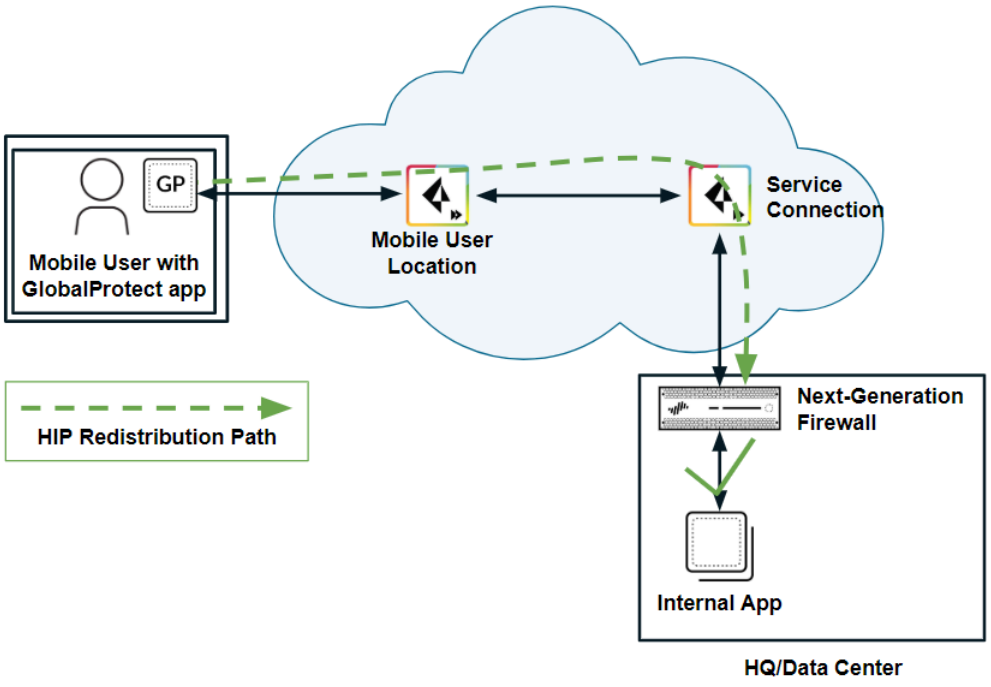
  下圖顯示了一個行動使用者，其端點受 GlobalProtect 應用程式保護。使用者嘗試存取總部/資料中心的內部應用程式，對該應用程式的存取由新世代防火牆透過 HIP 型安全性政策控制。當使用者登入 GlobalProtect 應用程式時，該應用程式會收集 HIP 資訊並將其傳送到 Prisma

 ©2025 Palo Alto Networks, Inc.

Access；不過，Prisma Access 不會將此資訊重新散佈至內部部署防火牆。由於防火牆沒有使用者的 HIP 資訊，因此它會封鎖使用者存取應用程式。



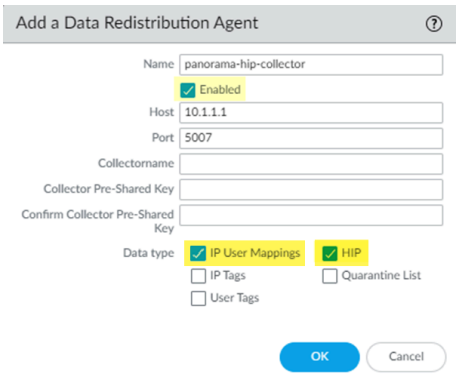

HIP 重新散佈允許您將行動使用者的 HIP 資訊散佈至內部部署防火牆。然後，防火牆可以針對其設定的安全性政策檢查使用者的 HIP 資訊，並授與使用者存取應用程式的權限。



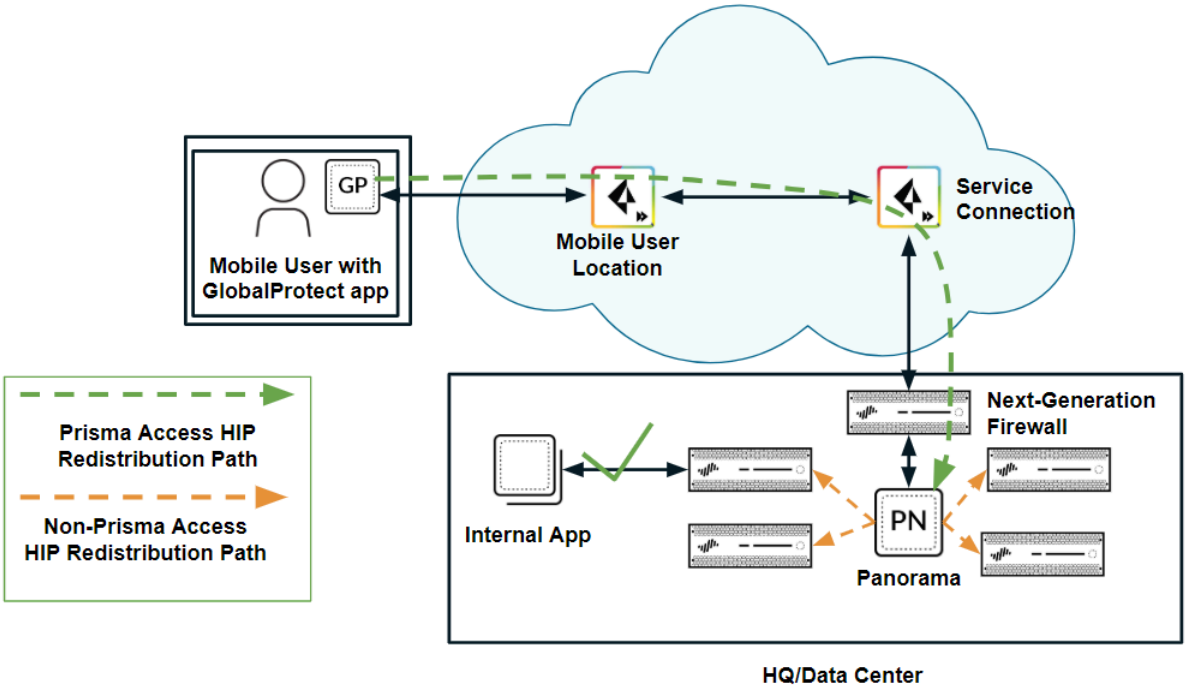

為了將 HIP 資訊從 Prisma Access 重新散佈至防火牆，您允許 Prisma Access 重新散佈 HIP 資訊，然後在防火牆上 **Add**（新增）一個 **User-ID Agent**（**User-ID** 代理程式）（**Panorama** > **User Identification**（使用者識別） > **User-ID Agents**（**User-ID** 代理程式），適用於

 ©2025 Palo Alto Networks, Inc.

9.1.*x* Panorama 設備，或 **Panorama** > **Data Redistribution**（資料重新散佈），適用於 Panorama 10.*x* 設備），並指定 Prisma Access **User-ID Agent Address**（**User-ID** 代理程式位址）（**Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Service Connection**（服務連線） > **User-ID Agent Address**（**User-ID** 代理程式位址））作為 **Host**（主機）（下列範例中的 10.1.1.1），以及指定 **5007** 作為 **Port**（連接埠）。




- **HIP** 從 **Prisma Access** 重新散佈至 **Panorama**—如果您的組織中有多個防火牆或閘道具有 HIP 型安全性政策，則您可以將 HIP 資訊從 Prisma Access 重新散佈至管理 Prisma Access 的 Panorama，方法是在 Panorama 中建立 User-ID 代理程式，並指定 Prisma Access **User-ID Agent Address**（**User-ID** 代理程式位址）作為 User-ID **Host**（主機）。然後，您可以將 HIP 報告從該 Panorama 設備重新散佈至您企業中的其他受管理 Panorama 設備、閘道、防火牆和虛擬系統，方法是使用與您用來將 User-ID 資訊重新散佈至受管理防火牆，並對內部應用程式和資源強制執行一致政策的同一工作流程，如下圖所示。




或者，您可以將企業中的每個內部防火牆或閘道設定為直接從 Prisma Access 收集 HIP 資訊，而不使用 Panorama 作為中心位置，方法是在每個裝置中建立一個 User-ID 代理程式。但請注

 ©2025 Palo Alto Networks, Inc.

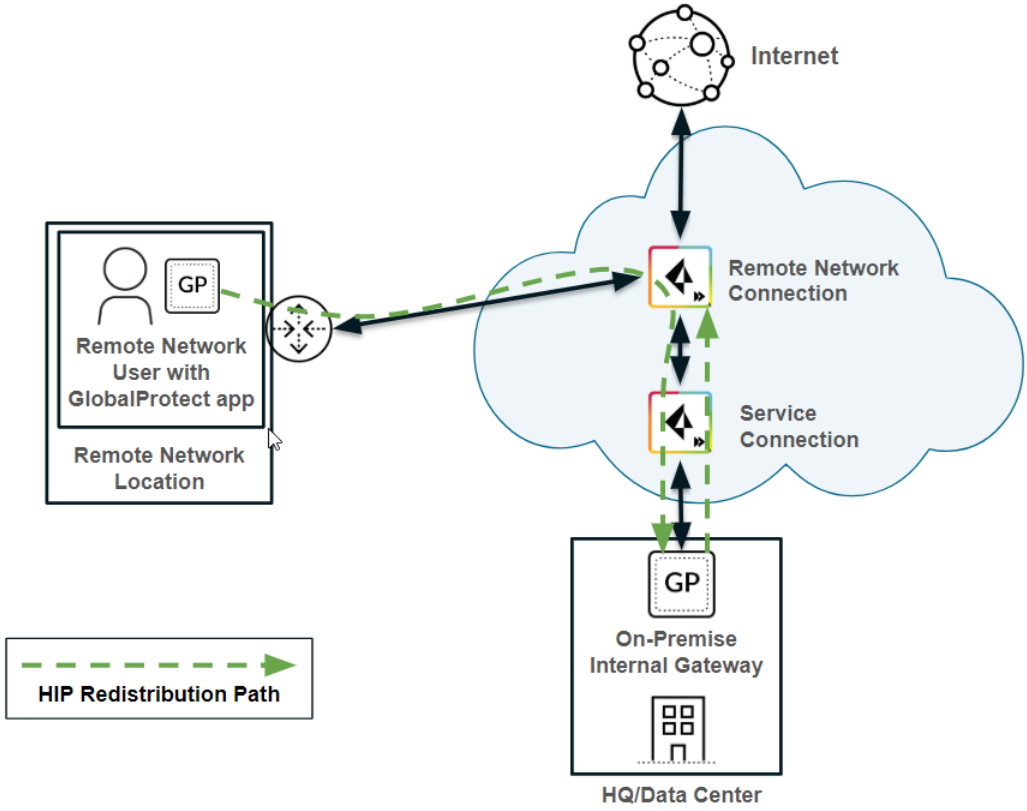
意，Prisma Access 會使用服務連線傳送 HIP 資訊，如果 Prisma Access 傳送大量 HIP 報告，則服務連線頻寬消耗可能會增加。

- **HIP** 從遠端網路中的使用者重新散佈至 **Prisma Access**—前面的使用案例顯示了 Prisma Access 從行動使用者中收集 HIP 資訊。如果想要在 Prisma Access 為遠端網路位置中的使用者套用 HIP 型政策，您需要一種方法，將 HIP 資訊從遠端網路使用者的 GlobalProtect 應用程式散佈至 Prisma Access。

  以下範例顯示了遠端網路位置中的使用者，其網際網路存取位於遠端網路連線上。在 Prisma Access 中，您使用在 **Remote_Network_Device_Group** 或在共用裝置群組中建立的安全性政策控制使用者在遠端網路位置的網際網路存取。若要在遠端網路位置為使用者適當地強制執行政策，您需要設定 Prisma Access，從內部閘道擷取使用者的 HIP 資訊。

  在此範例中，總部/資料中心的 GlobalProtect 閘道使用內部主機偵測設定為內部閘道，其會檢查來自使用者 GlobalProtect 應用程式的使用者 HIP 資訊。內部閘道偵測到使用者位於遠端網路位置內，並從使用者中同時收集 User-ID 和 HIP 資訊。

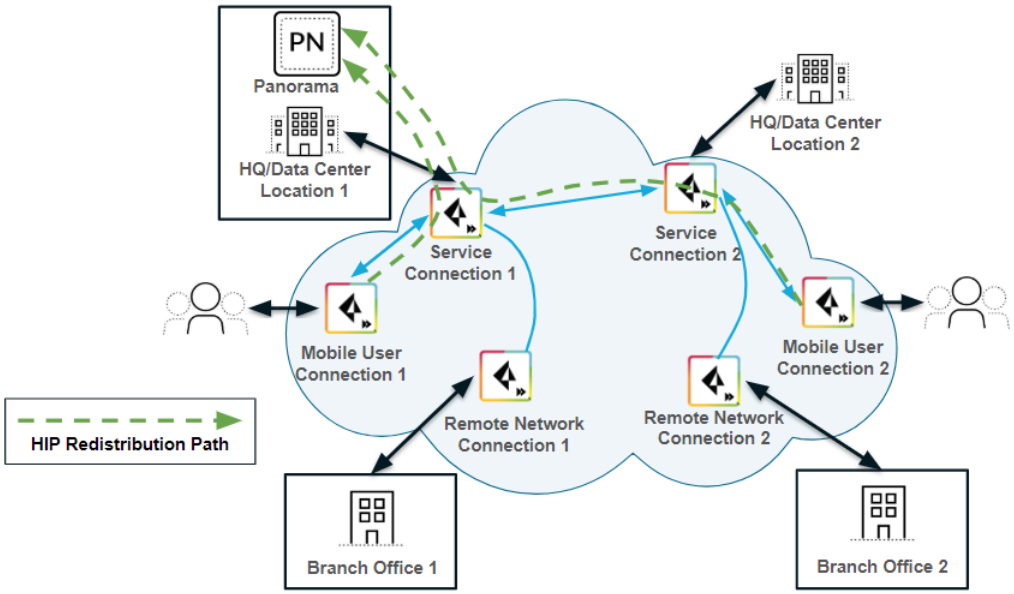
  若要將此 HIP 資訊從內部閘道散佈至 Prisma Access，請在 Panorama 中建立 User-ID 代理程式，並將內部閘道的 IP 位址指定為主機。




- 檢視來自 **Panorama** 的詳細 **HIP** 日誌—當行動使用者使用 GlobalProtect 應用程式登入時，該應用程式會將 HIP 資訊傳送至 Prisma Access。Panorama 會從 Strata Logging Service 擷取結果，以檢視 HIP 比對日誌的結果（**Monitor**（監控） > **Logs**（日誌） > **HIP Match**（**HIP** 比


©2025 Palo Alto Networks, Inc.

對））；不過，您無法檢視詳細的 HIP 報告，直到您設定 Panorama，以將 HIP 報告詳細資訊從 Prisma Access 重新散佈至 Panorama。

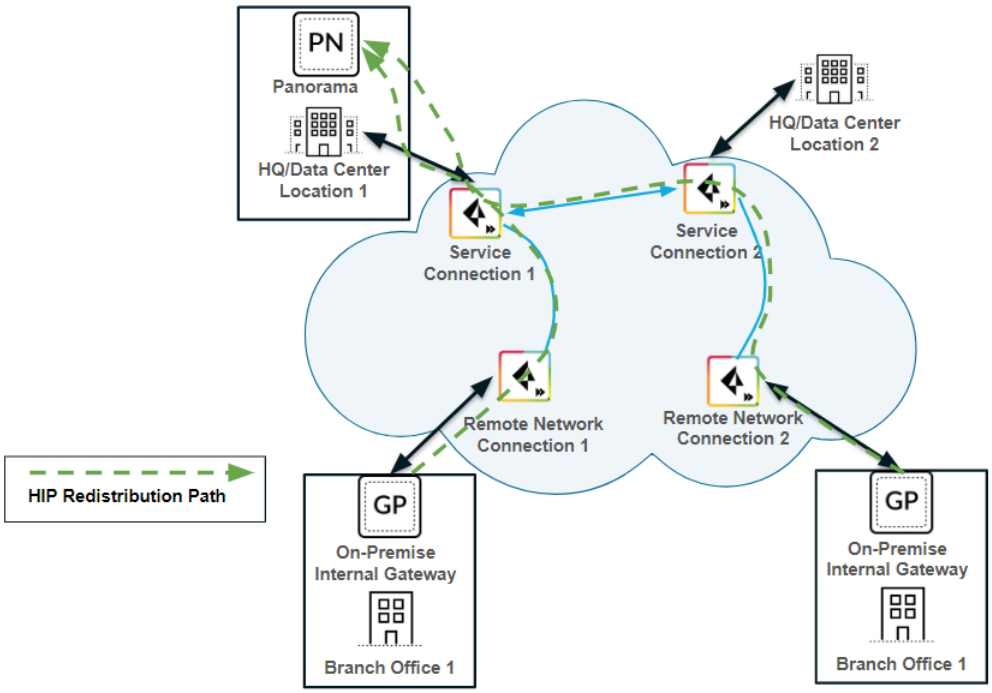



若要將詳細的 HIP 資訊從行動使用者重新散佈至 Panorama，請在 Panorama 中建立 User-ID 代理程式，並指定 **User-ID Agent Address**（**User-ID** 代理程式位址）（**Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Service Connection**（服務連線） > **User-ID Agent Address**（**User-ID** 代理程式位址））作為 User-ID 主機。

如果您已將內部部署閘道設定為遠端使用者位置的內部閘道，則也可以將遠端網路使用者的 HIP 資訊傳送至 Panorama，方法是在 Panorama 中建立 User-ID 代理程式，並指定遠端網路 **EBGP Router**（**EBGP** 路由器）位址（**Panorama** > **Cloud Services**（雲端服務） >


©2025 Palo Alto Networks, Inc.

**Status**（狀態） > **Network Details**（網路詳細資訊） > **Remote Networks**（遠端網路） > **EBGP Router**（**EBGP** 路由器））作為 User-ID 主機。




在 Prisma Access 中啟用和設定 Hip 重新散佈：

- 在 Prisma Access 中設定 HIP 重新散佈

## 在 Prisma Access 中設定 HIP 重新散佈

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

當端點安裝了 GlobalProtect 應用程式的行動使用者連線到 Prisma Access 時，Prisma Access 會從端點的 GlobalProtect 應用程式收集使用者的 HIP 資訊，這使得 HIP 報告可在 Prisma Access 取得。

若要使用 *Hip* 重新散佈，使用者必須在其端點上安裝 *GlobalProtect* 應用程式。儘管 *Prisma Access* 支援 無用戶端 VPN，但您無法為無用戶端 *VPN* 使用者重新散佈 *HIP* 資訊。

Hip 重新散佈適用於行動使用者和遠端網路使用者。不過，對於遠端網路使用者，內部部署閘道必須先使用內部主機偵測來偵測使用者是否位於組織網路的內部，然後內部部署閘道才能將 HIP 資訊傳送到 Prisma Access。

在 *Prisma Access* 中，您可以在設定行動使用者部署時設定內部主機偵測。


©2025 Palo Alto Networks, Inc.

為了確保一致的政策實施，您可以使用 Hip 重新散佈，允許 Prisma Access 將使用者的 HIP 資訊散佈到部署中的其他 Panorama 設備、閘道、防火牆和虛擬系統，以及在某些情況下，將這些裝置中的 HIP 資訊散佈到 Prisma Access。此功能可讓您對使用者流量一致地套用 HIP 型政策實施，其中包括的政策適用於網際網路繫結流量或存取組織總部或資料中心的內部應用程式或資源的流量。將 HIP 資訊重新散佈到 Panorama 設備也可讓您檢視詳細的 HIP 資訊，這是來自該設備的 Prisma Access 使用者的資訊。

請記住，GlobalProtect 內部和外部閘道不支援雙向 Hip 重新散佈。因此，最佳做法是使用 Panorama 設備作為重新散佈點。在此部署中，您將設定內部和外部閘道，以將 HIP 報告傳送至 Panorama，並讓 Panorama 將它們轉送到防火牆，以在整個環境中實施一致的政策。

- Strata Cloud Manager
- Panorama

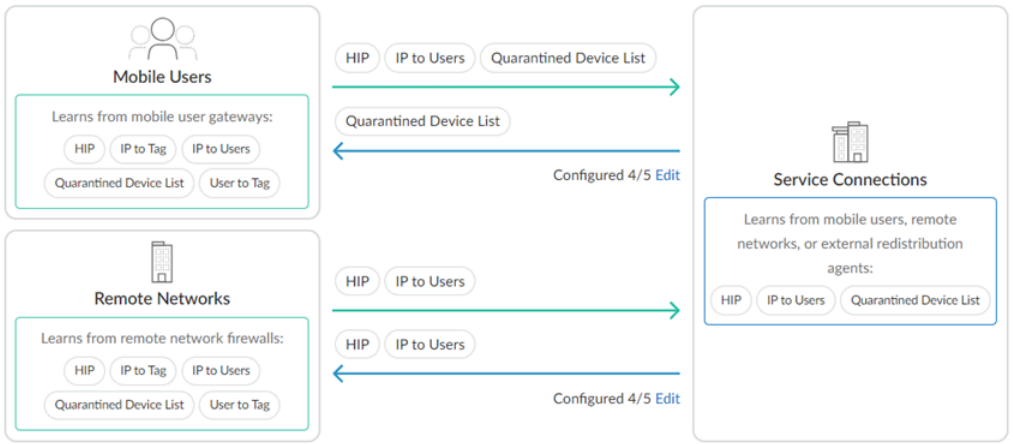
### 在 Prisma Access 中設定 HIP 重新散佈 (Strata Cloud Manager)

根據預設，HIP 報告重新散佈會在 Strata Cloud Manager 中啟用。若要檢視重新散佈詳細資訊或停用重新散佈，請遵循以下步驟。

**STEP 1 |** 在 **Strata Cloud Manager** 中，選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Identify Services**（識別服務） > **Identify Redistribution**（識別重新散佈）。

Prisma Access 識別重新散佈圖會顯示行動使用者與服務連線，以及遠端網路與服務連線之間的預設 HIP 報告重新散佈設定。

Prisma Access Identity Redistribution Diagram




**STEP 2 |** 若要停用在區段之間重新散佈，請按一下 **Edit**（編輯），然後按一下相關來源遠端網路旁邊的 **Edit**（編輯）。

**STEP 3 |** 停用 **HIP**。

### 在 Prisma Access 中設定 HIP 重新散佈 (Panorama)

若要允許 Prisma Access 收集並重新散佈 HIP 資訊，請完成以下工作。


©2025 Palo Alto Networks, Inc.

**STEP 1 |** 允許 Prisma Access 重新散佈 HIP 資訊。

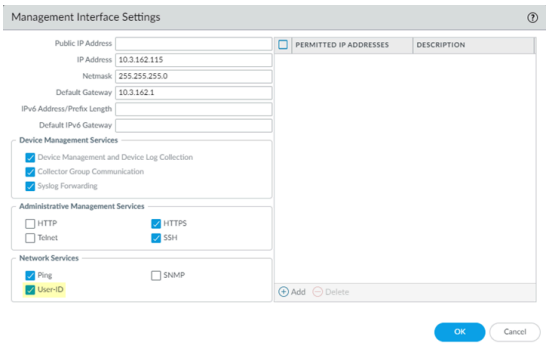
1. 在 Panorama 中，選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Service Setup**（服務設定）。
2. 按一下齒輪圖示以編輯設定。
3. 在 **Advanced**（進階）頁籤中，選取 **Enable HIP Redistribution**（啟用 **HIP** 重新散佈）。

   啟用 HIP 重新散佈可讓 Prisma Access 將從 GlobalProtect 應用程式接收的 HIP 報告重新散佈到內部防火牆和 Panorama。




**STEP 2 |** 設定 Panorama 以從 Prisma Access 接收 HIP 報告。

1. 選取 **Panorama** > **Setup**（設定） > **Interfaces**（介面）。
2. 選擇 **Management**（管理）介面。
3. 選取 **User-ID**。




**STEP 3 |** 設定 Panorama 以從 Prisma Access 收集 User-ID 對應。

1. 從管理 Prisma Access 的 Panorama 中，選取 **Panorama** > **Data Redistribution**（資料重新散佈） > **Agents**（代理程式）（適用於 Panorama 10.*x* 設備）或 **Panorama** > **User Identification**（使用者識別） > **User-ID Agents**（**User-ID** 代理程式）（適用於 9.1.*x* Panorama 設備）。
2. **Add**（新增）一個 User-ID 代理程式並給與它一個 **Name**（名稱）。
3. 在 **Host**（主機）欄位中輸入下列其中一個值，取決於您想要收集的 HIP 資訊類型。
   - 若要收集行使用者的 HIP 資訊，請輸入 **User-ID Agent Address**（**User-ID** 代理程式位址）（**Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Service Connection**（服務連線） > **User-ID Agent Address**（**User-ID** 代理程式位址））。
   - 若要在具有內部閘道的遠端網路位置收集使用者的 HIP 資訊，請輸入內部閘道的 IP 位址。
   - 若要透過遠端網路連線收集使用者的 HIP 資訊，請輸入 **EBGP Router**（**EBGP** 路由器）位址（**Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Remote Networks**（遠端網路） > **EBGP Router**（**EBGP** 路由器）作為 User-ID 主機。

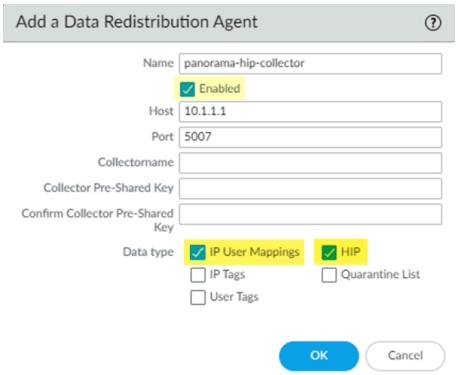
 ©2025 Palo Alto Networks, Inc.

4. 在連接埠欄位中輸入 **5007**。

   根據預設，User-ID 代理程式會使用 5007 連接埠來接聽 HIP 資訊要求。

   確保您的網路不會在 *Prisma Access* 與 *Active Directory* 伺服器或 *User-ID* 代理程式之間封鎖對此連接埠的存取。

5. 選取 **Enabled**（已啟用），讓 Panorama 能夠與 User-ID 代理程式進行通訊。
6. 選取 **IP User Mappings**（**IP** 使用者對應）和 **HIP**，讓 Panorama 能夠從所有行動使用者位置接收 IP 位址至使用者名稱對應和 GlobalProtect HIP 資料。
7. 按一下 **OK**（確定）。




**STEP 4 |** 對於每個您想要設定 HIP 報告收集的服務連線，重複步驟 3。

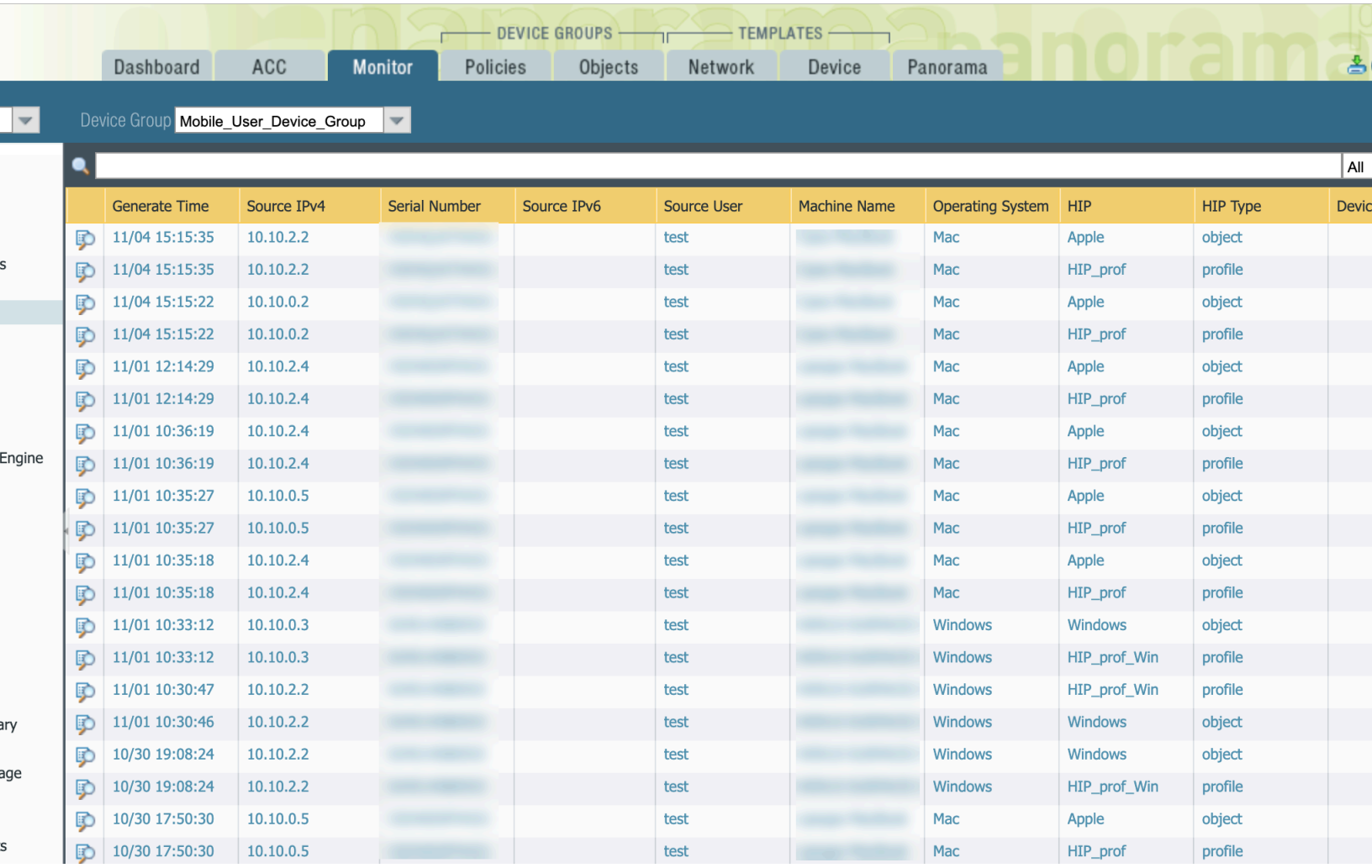
## 檢視 HIP 報告

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

在設定 Prisma Access 以收集 HIP 資訊並將其重新散佈至 Panorama 之後，請使用以下工作流程，在 Panorama 中檢視 HIP 資訊。


©2025 Palo Alto Networks, Inc.

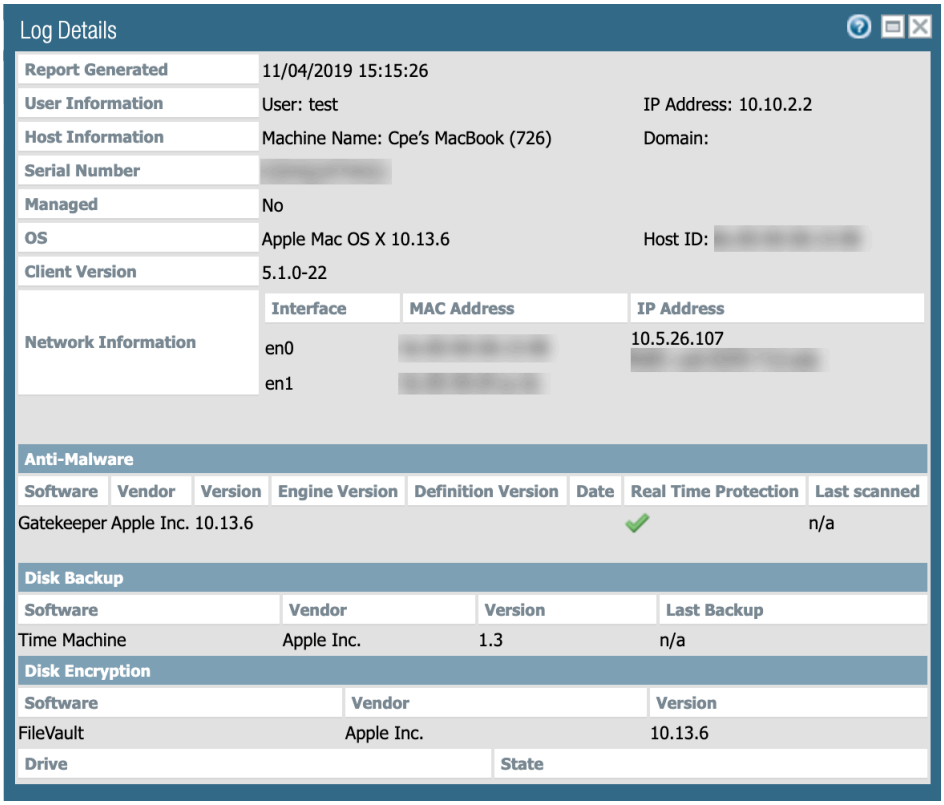
**STEP 1 |** 選取 **Monitor**（監控） > **Logs**（日誌） > **HIP Match**（**HIP** 比對），以檢視 HIP 資訊。




| Generate Time | Source IPv4 | Serial Number | Source IPv6 | Source User | Machine Name | Operating System | HIP | HIP Type | Devic |
|---|---|---|---|---|---|---|---|---|---|
| 11/04 15:15:35 | 10.10.2.2 | | | test | | Mac | Apple | object | |
| 11/04 15:15:35 | 10.10.2.2 | | | test | | Mac | HIP_prof | profile | |
| 11/04 15:15:22 | 10.10.0.2 | | | test | | Mac | Apple | object | |
| 11/04 15:15:22 | 10.10.0.2 | | | test | | Mac | HIP_prof | profile | |
| 11/01 12:14:29 | 10.10.2.4 | | | test | | Mac | Apple | object | |
| 11/01 12:14:29 | 10.10.2.4 | | | test | | Mac | HIP_prof | profile | |
| 11/01 10:36:19 | 10.10.2.4 | | | test | | Mac | Apple | object | |
| 11/01 10:36:19 | 10.10.2.4 | | | test | | Mac | HIP_prof | profile | |
| 11/01 10:35:27 | 10.10.0.5 | | | test | | Mac | Apple | object | |
| 11/01 10:35:27 | 10.10.0.5 | | | test | | Mac | HIP_prof | profile | |
| 11/01 10:35:18 | 10.10.2.4 | | | test | | Mac | Apple | object | |
| 11/01 10:35:18 | 10.10.2.4 | | | test | | Mac | HIP_prof | profile | |
| 11/01 10:33:12 | 10.10.0.3 | | | test | | Windows | Windows | object | |
| 11/01 10:33:12 | 10.10.0.3 | | | test | | Windows | HIP_prof_Win | profile | |
| 11/01 10:30:47 | 10.10.2.2 | | | test | | Windows | HIP_prof_Win | profile | |
| 11/01 10:30:46 | 10.10.2.2 | | | test | | Windows | Windows | object | |
| 10/30 19:08:24 | 10.10.2.2 | | | test | | Windows | Windows | object | |
| 10/30 19:08:24 | 10.10.2.2 | | | test | | Windows | HIP_prof_Win | profile | |
| 10/30 17:50:30 | 10.10.0.5 | | | test | | Mac | Apple | object | |
| 10/30 17:50:30 | 10.10.0.5 | | | test | | Mac | HIP_prof | profile | |


©2025 Palo Alto Networks, Inc.

**STEP 2 |** 按一下記錄左側的圖示以檢視詳細的 HIP 資訊。



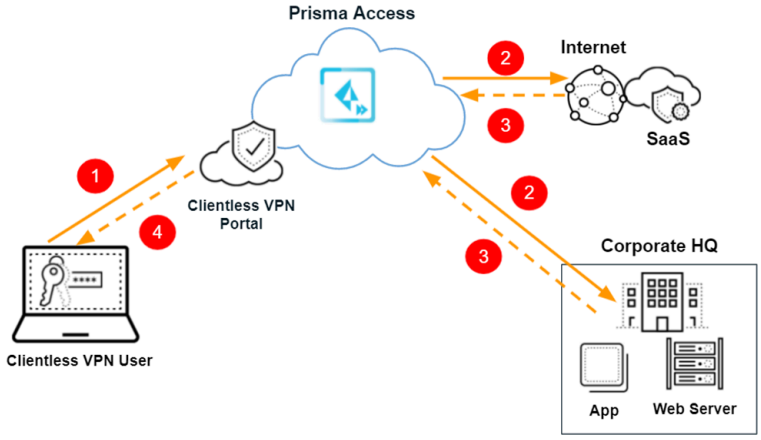

# 無用戶端 VPN 中 Gzip 編碼的支援

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Panorama | • Prisma Access 授權 |

GlobalProtect 無用戶端 VPN 會向常見企業 Web 應用程式提供安全的遠端存取。Prisma Access 無用戶端 VPN 可讓行動使用者存取 Gzip 壓縮的網站，以使用內部和 SaaS 應用程式。對 Gzip 編碼的支援確保了 HTTP 標頭內的 Gzip 編碼要求被無用戶端 VPN 入口網站接受。這確保了透過無用戶端 VPN 入口網站存取時，來自 Gzip 壓縮網頁的內容能夠正確呈現。

以下圖示說明了延伸的支援，允許使用者透過 Prisma Access 中的無用戶端 VPN 存取內部和 SaaS 應用程式。


©2025 Palo Alto Networks, Inc.



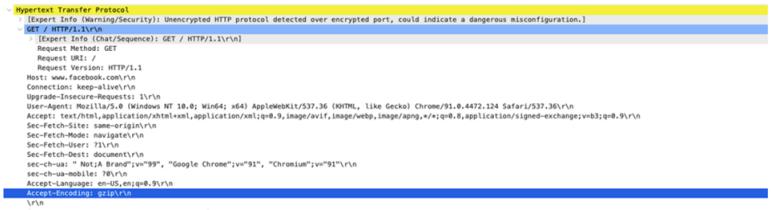

無用戶端 VPN 可以根據來自用戶端的 HTTP 要求和來自應用程式的對應回應，確定是否使用 Gzip 編碼。必須包括 **gzip** 值作為其中一個 Accept-Encoding 標頭值，以便其可被無用戶端 VPN 接受。

例如，考慮無用戶端 VPN 使用 Gzip 編碼時的以下案例：

1. 瀏覽器將 HTTP 要求傳送至網站，其中 Accept-Encoding 標頭值設定為 **gzip**、**deflate** 和 **br**，如以下範例所示。




2. Prisma Access 中的無用戶端 VPN 入口網站解析來自瀏覽器的傳入 HTTP 要求，並將 Accept-Encoding 標頭值設定為 **gzip**，這表示支援 Gzip 編碼，如以下範例所示。

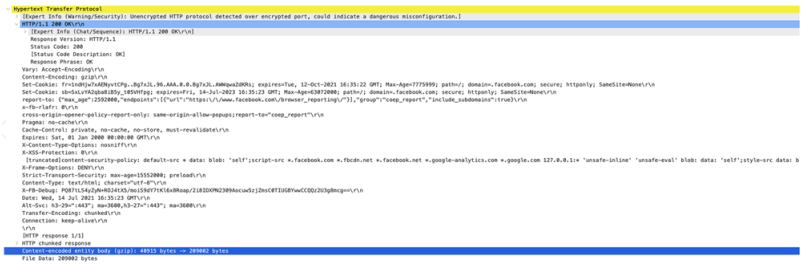



3. 如果網站支援 HTTP 回應中的 Gzip 編碼，則網站會以 **gzip** 形式傳送 Content-Encoding 標頭，這表示內容是以 Gzip 格式呈現，如以下範例所示。




 ©2025 Palo Alto Networks, Inc.

4. 無用戶端 VPN 會將從網站收到的回應以相同格式轉送到 Web 瀏覽器，如以下範例所示。



如果無用戶端 VPN 收到的 HTTP 要求未包括 **gzip** 作為其中一種編碼方法，則無用戶端 VPN 不會接受 Gzip 編碼。

# Prisma Access 中的流量複寫

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權<br>❑ 流量複寫附加授權<br>❑ 對於行動使用者流量，流量複寫至少需要 4.1 Prisma Access 版本。<br>❑ 對於行動使用者和遠端網路流量，流量複寫至少需要5.0 Prisma Access 版本。<br>❑ 遠端網路的 TLS 1.3 支援至少需要 Prisma Access 5.2 版本。<br>❑ PubSub 至少需要 Prisma Access 5.2.1 版本。 |

內部部署網路記錄器一直是組織執行鑑識和違規分析的強大工具。在內部部署拓撲中，實作 Tap 連接埠、Span 連接埠或封包代理程式的平行基礎結構是很常見的，此基礎結構將提供用於此類頻外分析的流量複本。

不過，隨著混合工作和雲端的加速採用，組織正在移轉到 SASE 架構來應對這些挑戰。堅持 SASE 雲端安全性解決方案為這些鑑識分析工具造成了盲點，其中流量再也無法從遠端使用者複製到 SaaS 應用程式。

Prisma Access 流量複寫透過提供正在穿越 Prisma Access 的流量複本，加入了涉及 SASE 架構的鑑識和事後分析的全面可視性。流量複寫發揮作用的一些常見使用案例如下：

- 取證和威脅追蹤分析，其中資料包擷取提供了無可辯駁的攻擊證據和所使用的方法
- 符合特定的法規合規性，其中封包擷取需要儲存一定時間
- 繼續使用您組織投入的任何偏好第三方工具
- 封包層級網路和應用程式效能偵錯

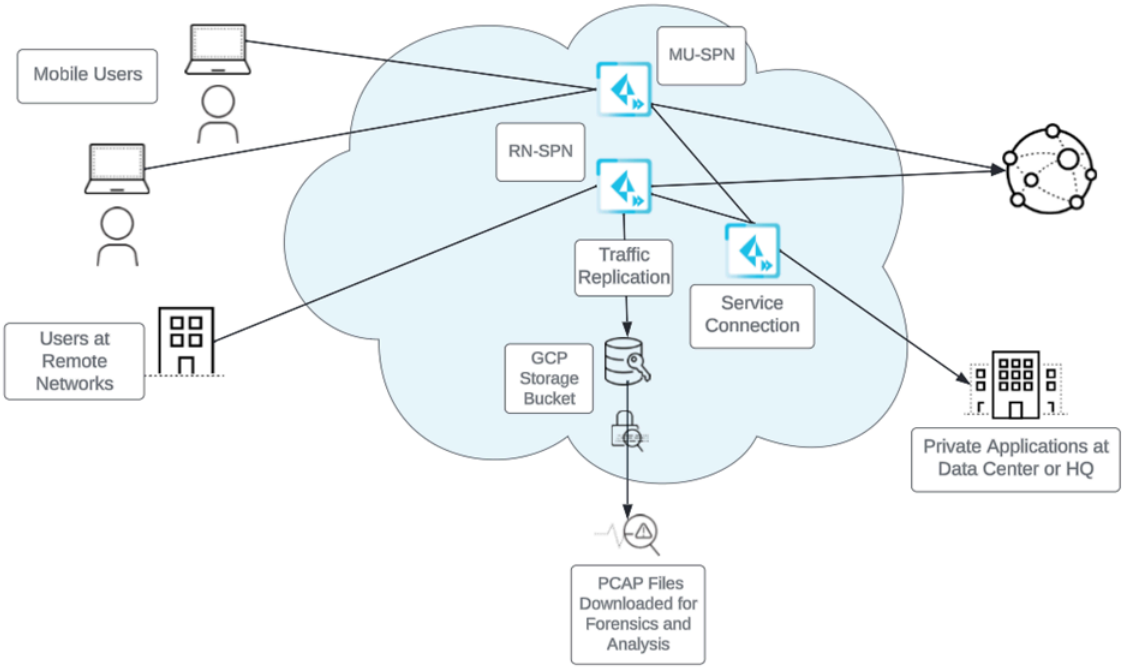
流量複寫提供對使用者真實流量的封包擷取 (pcap) 的存取，從而能夠偵測和修復可能跨越多個工作階段的威脅，或識別並回應異常行為，以降低風險並確保企業安全。

 ©2025 Palo Alto Networks, Inc.

啟用流量複寫時，Prisma Access 會在每個啟用此功能的 Prisma Access 計算位置中建立專用的雲端儲存貯體，並持續儲存 pcap 檔案，其中包含正在穿越 Prisma Access 的流量複本。

若要在新的 pcap 檔案上傳到儲存貯體時收到通知，您可以訂閱 Pub/Sub 通知。為新 pcap 檔案使用 Pub/Sub 通知，就不需要開發在有新資料夾或新檔案新增至貯體時通知您的工具。

您需要提供一個 Google Cloud 服務帳戶，此帳戶將用來共用這些儲存貯體的唯讀權限，從而啟用對 pcap 檔案的安全存取。對靜態 pcap 檔案進行額外加密，涉及透過 Prisma Access 中憑證共用的公開金鑰。只有您有私密金鑰來解密和復原原始 pcap 檔案。




流量複寫的先決條件

在開始設定流量複寫之前，請注意以下先決條件。

- 確保您已在 Google Cloud Platform (GCP) 中建立服務帳戶。
- 確保您已在 **Objects**（物件） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Custom Certificates**（自訂憑證） > **Generate**（產生）頁面中建立透過憑證共用的公開金鑰，以用於 SSL 解密。
- 建議的架構要求從每個儲存貯體讀取 pcap 檔案的計算或服務存在於該貯體正在從中讀取的同一 GCP 區域中。雖然從不同 GCP 區域甚至 GCP 雲端外部讀取儲存貯體中的 pcap 檔案可能行得通，但這些不是支援的部署模型。

流量複寫指導方針

請遵循以下指導方針進行流量複寫：

- **TLS** 支援—行動使用者部署中使用的流量複寫支援 TLS 1.2；遠端網路部署中使用的流量複寫支援 TLS 1.2 和 1.3。
- **IPSec** 通道演算法—流量複寫也支援行動使用者和遠端網路部署支援的所有 IPSec 通道演算法。

瞭解如何設定流量複寫：


©2025 Palo Alto Networks, Inc.

- Strata Cloud Manager
- Panorama

## Prisma Access 中的流量複寫 (Strata Cloud Manager)

若要設定流量複寫並存取封包擷取 (pcap) 檔案，請完成以下步驟。

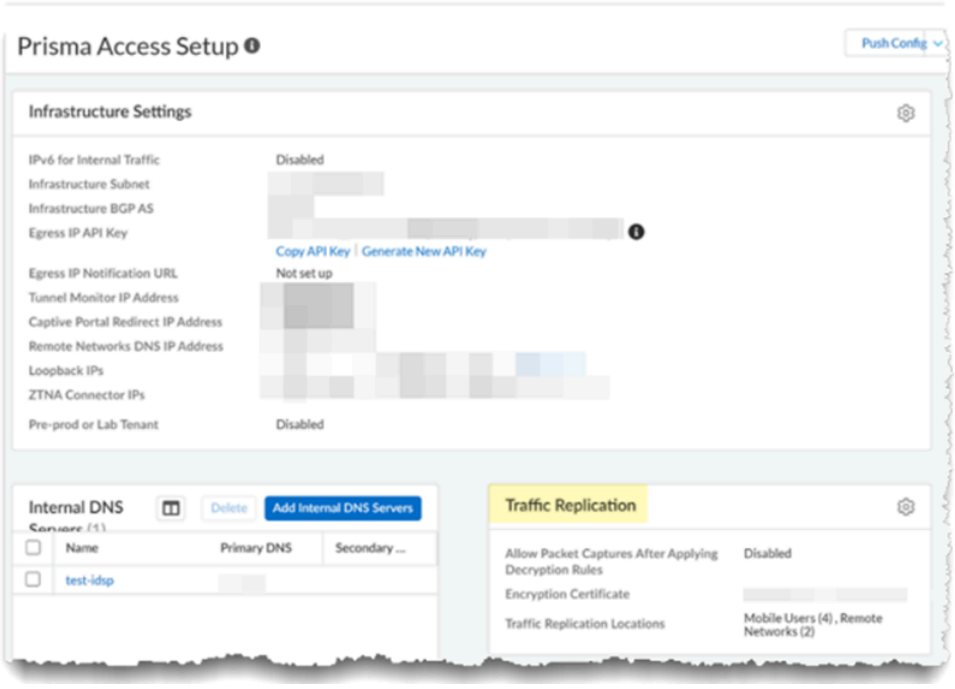
**STEP 1 |** 為您想要啟用流量複寫的位置裝載並設定行動使用者—GlobalProtect，然後 **Commit and Push**（提交並推送）您的變更。

您必須已啟用行動使用者—GlobalProtect 位置，然後才能為這些位置啟用流量複寫。


©2025 Palo Alto Networks, Inc.

**STEP 2 |** （選用）對封包擷取套用 SSL 解密。

1. 前往 Prisma Access (Managed by Strata Cloud Manager) 並選取 **Prisma Access Setup**（設定） > **Prisma Access** > **Traffic Replication**（流量複寫），然後按一下齒輪以編輯 **Settings**（設定）。

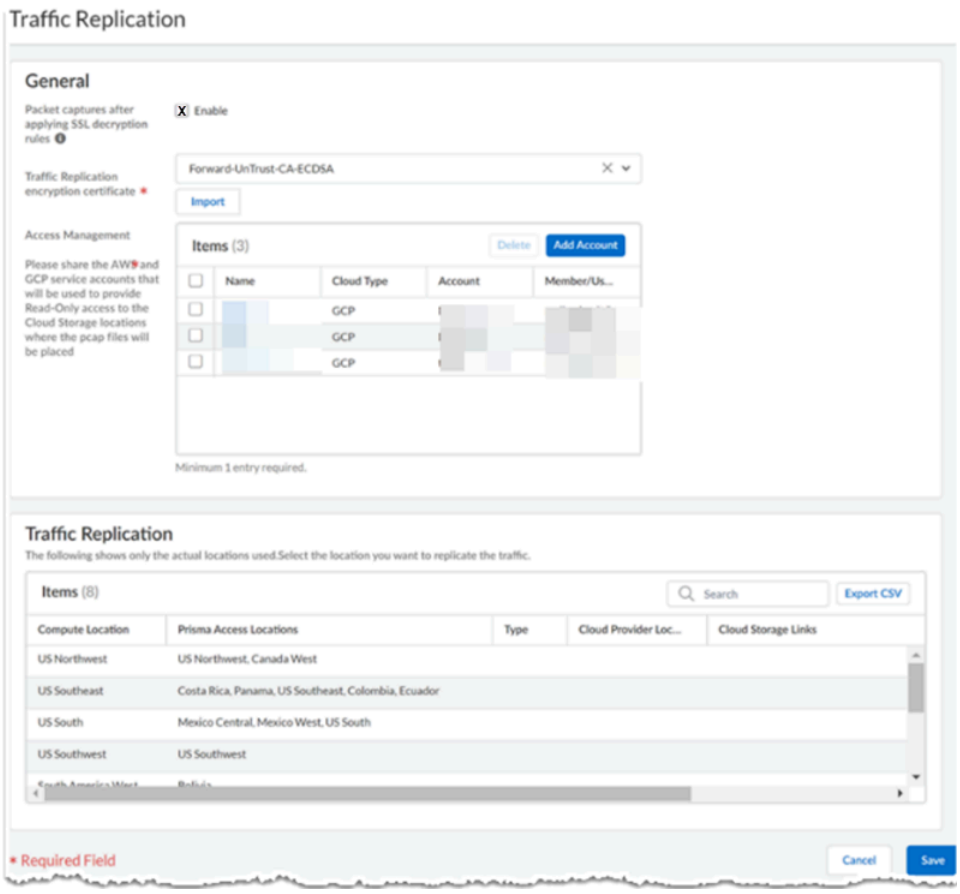



2. 啟用 **Packet captures after applying SSL decryption rules**（在套用 **SSL** 解密規則之後進行封包擷取），以在 pcap 檔案上套用您已設定的 SSL 解密政策。

   只有符合內嵌 SSL 解密政策的流量才會進行解密。

   如果您選取此選項，pcap 檔案將使用您在部署中指定的相同解密規則。如果您取消選取此選項，則不會對 pcap 檔案進行任何解密，無論您設定了哪些解密規則。


©2025 Palo Alto Networks, Inc.




**STEP 3 |** 對於 **Traffic Replication encryption certificate**（流量複寫加密憑證），請選取您已在 **Objects**（物件） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Custom Certificates**（自訂憑證） > **Generate**（產生）頁面中新增的任何憑證，或 **Import**（匯入）憑證，以用於 SSL 解密。

憑證由公開金鑰和私密金鑰組成。上傳 Prisma Access 中的公開金鑰；您保留私密金鑰，並在從儲存貯體下載壓縮的 pcap 檔案時使用該金鑰進行解密。透過這種方式，您保證只有您的組織能夠存取儲存 pcap 檔案的儲存貯體。

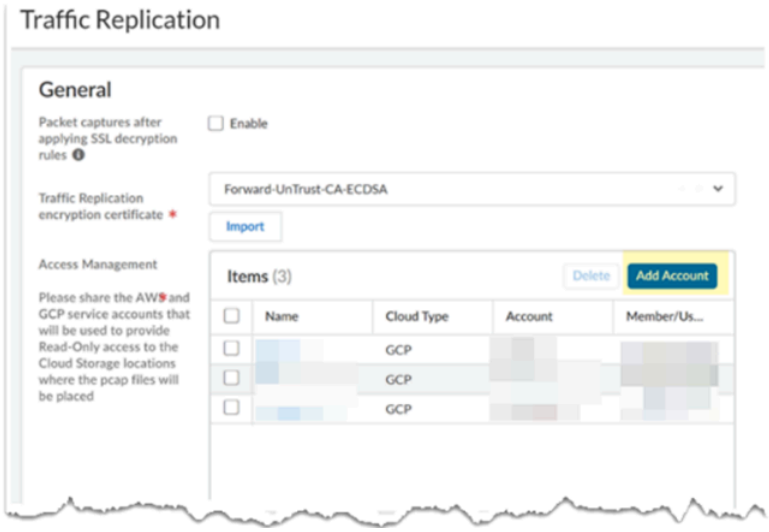
**STEP 4 |** 設定您在步驟 1 中建立的 GCP 服務帳戶。

僅 GCP 帳戶支援流量複寫。此服務帳戶用來在您已啟用流量複寫的位置中共用對 pcap 檔案儲存所在的儲存貯體的唯讀存取。您可以使用正常的 GCP 服務帳戶建立程序，在您的 GCP 帳戶

 ©2025 Palo Alto Networks, Inc.

中建立這些服務帳戶。控制哪些使用者可以存取這些服務帳戶，這是您的責任。任何可以存取 pcap 檔案，也可以存取私密金鑰的使用者都將可以存取 pcap 檔案。

1. 在 **Access Management**（存取管理）區域，**Add Account**（新增帳戶）詳細資訊，以共用對儲存 pcap 檔案之儲存貯體的唯讀存取。




2. 請輸入以下參數：
   - 給與帳戶唯一的 **Account Name**（帳戶名稱）。
   - 指定 **GCP** 作為帳戶的 **Type**（類型）。
   - 指定來自您所建立 GCP 服務帳戶的 **Account**（帳戶）資訊。
   - 為 GCP 服務帳戶輸入 **Member/User**（成員/使用者名稱）。


©2025 Palo Alto Networks, Inc.

**STEP 5 |** （選用）如果您想要新增 Pub/Sub 通知，在新資料夾或新檔案新增到貯體時通知您，請在您的 Google Cloud 服務帳戶中設定 Pub/Sub 通知。

Prisma Access 會為該租用戶中的所有位置建立每個租用戶一個單一的 Pub/Sub 通道。

從 *Prisma Access 5.2* 開始支援 *Pub/Sub* 通知。如果您有現有的帳戶並想要新增 *Pub/Sub* 通知，請升級到 *Prisma Access 5.2*，然後選擇以下其中一個選項，以新增 *Pub/Sub* 通知：

- 修改您已在 *Prisma Access* 中設定的現有 *Google Cloud* 服務帳戶。
- 為現有的服務帳戶新增一個帳戶，並在您的 *Prisma Access* 設定中指定該帳戶。

  如果您新增一個新帳戶，則需要在現有帳戶上停用流量複寫，並在新帳戶上啟用流量複寫。
- 在現有位置上停用和啟用流量複寫。

Prisma Access 會傳送標頭為 `panw-traffic-replication-file-notifications-<tenantid>` 的 Pub/Sub 訊息，其中 *<tenantid>* 是正在傳送通知的租用戶 ID。這些訊息的格式如下：

```
Message { data: b'' ordering_key: '' attributes:
 { "bucketId": "xxxx-xx-xxx-xxxxxxxxx-us-west1",
 "eventTime":"2024-04-24T23:12:59.xxxxxxx",
 "eventType":"OBJECT_FINALIZE", "notificationConfig":
 "projects/_/buckets/xxxx-xx-xxx-xxxxxxxxx-us-west1/
notificationConfigs/1", "objectGeneration": "xxxxxxxxxxxxxxxx",
 "objectId": "instance-group-xxxxxxx/12345678_190000_xxxxx.zip",
 "payloadFormat":"NONE" } }
```

其中：

- `objectGeneration` 是已變更物件的生成編號。
- `objectID` 是已變更物件的名稱。

**STEP 6 |** 為一個或多個行動使用者位置設定流量複寫。

1. 在 **Traffic Replication**（流量複寫）區域中，選取您想要啟用流量複寫的位置，然後選取 **Mobile Users**（行動使用者）。

   您可以選取與 **Prisma Access Locations**（位置）相關聯的 **Compute Location**（計算位置）。即會針對連線到所選位置的所有行動使用者用戶端啟用流量複寫。

**STEP 7 |** **Save**（儲存）設定。

 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** 提交並推送您的變更。

1. 選取 **Manage**（管理） > **Operation**（操作） > **Push Config**（推送設定）。
2. 在 **Push Scope**（推送範圍）中選取 **Mobile Users Container**（行動使用者容器），然後 **Push Config**（推送設定）並 **Push**（推送）您的變更。
3. 檢閱推送目標和推送。

**STEP 9 |** 前往 **Prisma Access Setup**（設定） > **Prisma Access** > **Traffic Replication**（流量複寫）來檢查流量複寫的狀態。

**STEP 10 |** 下載 pcap 檔案。

使用 **Cloud Storage Links**（雲端儲存連結）來存取 GCP 儲存貯體中的 pcap 檔案。

- 這些儲存貯體支援與其他 GCP 儲存貯體相同的常規操作、命令和查詢。
- 您可以最多可有 72 小時下載 pcap 資料。72 小時後，這些檔案將被永久刪除。
- 這些檔案是使用您的公開金鑰進行加密。
- 檔案大小上限為 200 MB 或 5 分鐘的封包擷取，以較小者為準。

1. 在您的服務中列出檔案，方法是輸入 `gsutil ls gs://<storage_bucket_link>/`，其中 *<storage_bucket_link>* 是 GCP 服務帳戶中儲存檔案的儲存連結。
2. 從您的服務帳戶下載檔案，方法是輸入 `gsutil cp gs://<storage_bucket_link>/<file_name> <destination folder>`，其中：
   - *<storage_bucket_link>* 是 GCP 服務帳戶中儲存檔案的儲存連結。
   - *<file_name>* 是 pcap 檔案的名稱。
   - *<destination folder>* 是您想要從中下載 pcap 檔案的資料夾。
3. 解壓縮下載的檔案。
4. 解密下載的檔案。

## Prisma Access 中的流量複寫 (Panorama)

若要設定流量複寫並存取 PCAP 檔案，請完成以下步驟。

**STEP 1 |** 裝載並設定行動使用者—GlobalProtect（如果要為行動使用者設定流量複寫）、遠端網路（如果要為遠端網路設定流量複寫）或兩者（如果要同時為行動使用者和遠端網路設定流量複寫）。

**STEP 2 |** （選用）對封包擷取套用 SSL 解密。

1. 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Traffic Replication**（流量複寫），然後按一下齒輪以編輯 **Settings**（設定）。
2. 選取 **Allow packet captures after applying decryption rules**（在套用解密規則之後允許封包擷取），以在 PCAP 檔案上套用您已設定的 SSL 解密政策。

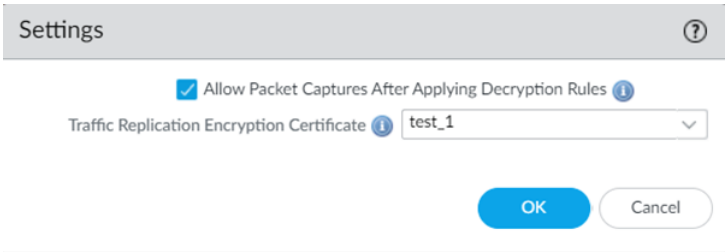
   如果您選取此選項，PCAP 檔案將使用您在部署中指定的相同解密規則。如果您取消選取此選項，則不會對 PCAP 檔案進行任何解密，無論您設定了哪些解密規則。

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 選取先前步驟中您在 **Mobile_User_Template**（適用於行動使用者部署）或 **Remote_Network_Template**（適用於遠端網路部署）建立的 **Traffic Replication Encryption Certificate**（流量複寫加密憑證）（公開金鑰），以用於 SSL 解密。

此步驟是必要的。您可以選取已在 **Mobile_User_Template** 或 **Remote_Network_Template** 的 **Device**（裝置）> **Certificate Management**（憑證管理）> **Certificates**（憑證）> **Device Certificates**（裝置憑證）區域中新增的任何憑證。如果您同時為行動使用者和遠端網路啟用流量複寫，請將憑證同時放入 **Mobile_User_Template** 和 **Remote_Network_Template** 中。

憑證由公開金鑰和私密金鑰組成。上傳 Prisma Access 中的公開金鑰；您保留私密金鑰，並在從儲存貯體下載壓縮的 PCAP 檔案時使用該金鑰進行解密。透過這種方式，您保證只有您的組織能夠存取儲存 PCAP 檔案的儲存貯體。




**STEP 4 |** 為一個或多個行動使用者—GlobalProtect 位置、遠端網路位置或兩者設定流量複寫，方法是在 **Configuration**（設定）區域中選取位置，接著選取要啟用流量複寫的位置，然後選取 **MU-GP**、**RN** 或兩者。

選取與 **Prisma Access Locations**（位置）相關聯的 **Compute Location**（計算位置）。即會針對連線到所選位置的所有行動使用者—GlobalProtect 用戶端、遠端網路使用者或兩者啟用流量複寫。




**STEP 5 |** 新增一個帳戶，讓您可以存取流量複寫封包擷取 (PCAP) 資料。

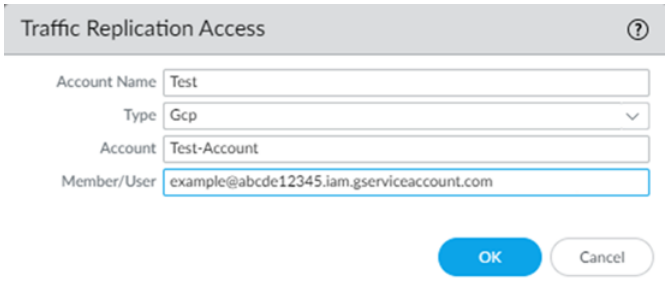
此服務帳戶用來在您已啟用流量複寫的位置中共用對 PACP 檔案儲存所在的儲存貯體的唯讀存取。您可以使用正常的 GCP 服務帳戶建立程序，在您的 GCP 帳戶中建立這些服務帳戶。控制

 ©2025 Palo Alto Networks, Inc.

哪些使用者可以存取這些服務帳戶，這是您的責任。任何可以存取 PCAP 檔案，也可以存取私密金鑰的使用者都將可以存取 PCAP 檔案。

1. 在 **Traffic Replication Access**（流量複寫存取）區域中，**Add**（新增）一個帳戶。
2. 請輸入以下參數：
   - 給與帳戶唯一的 **Account Name**（帳戶名稱）。
   - 指定 **Gcp** 作為帳戶的 **Type**（類型）。

     僅 GCP 帳戶支援流量複寫。
   - 指定來自您所建立 GCP 服務帳戶的 **Account**（帳戶）資訊。
   - 為 GCP 服務帳戶輸入 **Member/User**（成員/使用者名稱）。




**STEP 6 |** （選用）如果您想要新增 Pub/Sub 通知，在新資料夾或新檔案新增到貯體時通知您，請在您的 Google Cloud 服務帳戶中設定 Pub/Sub 通知。

Prisma Access 會為該租用戶中的所有位置建立每個租用戶一個單一的 Pub/Sub 通道。

從 *Prisma Access 5.2* 開始支援 *Pub/Sub* 通知。如果您有現有的帳戶並想要新增 *Pub/Sub* 通知，請升級到 *Prisma Access 5.2*，然後選擇以下其中一個選項，以新增 *Pub/Sub* 通知：

- 修改您已在 *Prisma Access* 中設定的現有 *Google Cloud* 服務帳戶。
- 為現有的服務帳戶新增一個帳戶，並在您的 *Prisma Access* 設定中指定該帳戶。

  如果您新增一個新帳戶，則需要在現有帳戶上停用流量複寫，並在新帳戶上啟用流量複寫。
- 在現有位置上停用和啟用流量複寫。

Prisma Access 會傳送標頭為 `panw-traffic-replication-file-notifications-<tenantid>` 的 Pub/Sub 訊息，其中 *<tenantid>* 是正在傳送通知的租用戶 ID。這些訊息的格式如下：

```
Message { data: b'' ordering_key: '' attributes:
 { "bucketId": "xxxx-xx-xxx-xxxxxxxxx-us-west1",
 "eventTime":"2024-04-24T23:12:59.xxxxxxx",
 "eventType":"OBJECT_FINALIZE", "notificationConfig":
 "projects/_/buckets/xxxx-xx-xxx-xxxxxxxxx-us-west1/
notificationConfigs/1", "objectGeneration": "xxxxxxxxxxxxxxxx",
```

 ©2025 Palo Alto Networks, Inc.

```
"objectId": "instance-group-xxxxxxx/12345678_190000_xxxxx.zip",
"payloadFormat":"NONE" } }
```

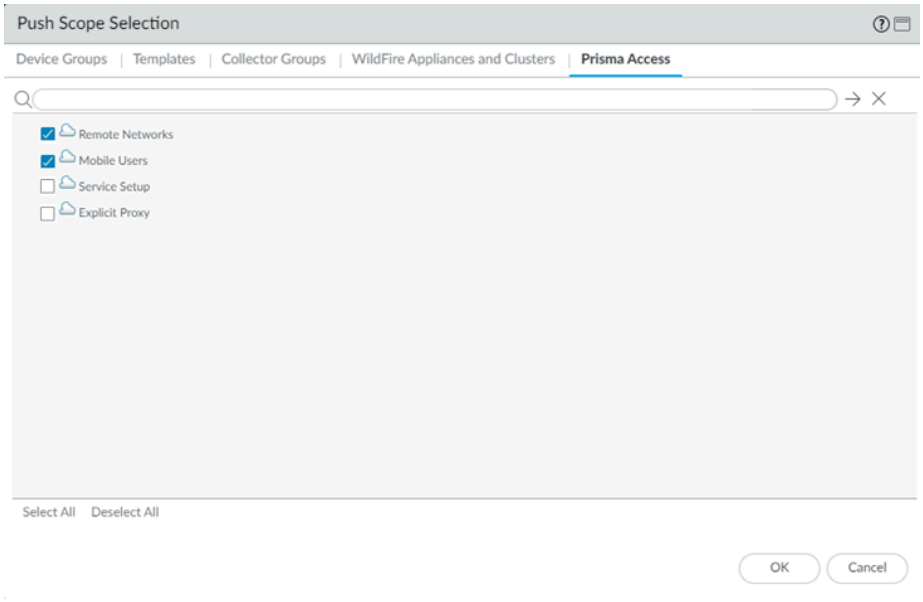
其中：

- `objectGeneration` 是已變更物件的生成編號。
- `objectID` 是已變更物件的名稱。

**STEP 7 |** 提交並推送您的變更，確保在 **Push Scope**（推送範圍）中選取了 **Mobile Users**（行動使用者）（適用於行動使用者部署）、**Remote Networks**（遠端網路）（適用於遠端網路部署）或兩者。

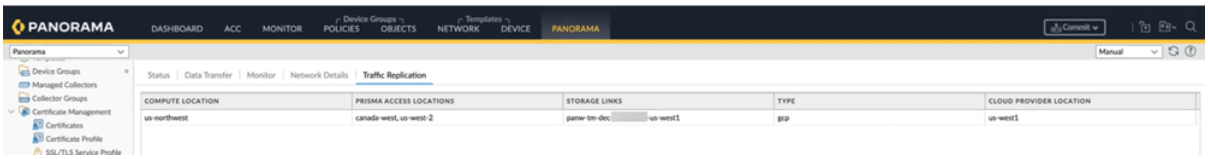
1. 按一下 **Commit**（提交） > **Commit and Push**（提交並推送）。
2. **Edit Selections**（編輯選取項目），並在 **Prisma Access** 頁籤中，確保在 **Push Scope**（推送範圍）中選取了 **Mobile Users**（行動使用者）和 **Remote Networks**（遠端網路），然後按一下 **OK**（確定）。

   **Push Scope**（推送範圍）可能不是自動選取的。




3. 按一下 **Commit and Push**（提交並推送）。

**STEP 8 |** 前往 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Traffic Replication**（流量複寫），檢查流量複寫的狀態。




**Storage Links**（儲存連結）是 GCP 儲存貯體的名稱，您可以在其中存取 PCAP 檔案。**Cloud Provider Location**（雲端提供者位置）是 GCP 執行個體裝載所在的位置。


©2025 Palo Alto Networks, Inc.

**STEP 9 |** 使用只有您擁有的私密金鑰下載 PCAP 檔案。

使用 **Storage Links**（儲存連結）來存取 GCP 儲存貯體中的 PCAP 檔案。

- 這些儲存貯體支援與其他 GCP 儲存貯體相同的常規操作、命令和查詢。
- 您可以最多可有 72 小時下載 PCAP 資料。72 小時後，這些檔案將被永久刪除。
- 這些檔案是使用您的公開金鑰進行加密。
- 檔案大小上限為 200 MB 或 5 分鐘的封包擷取，以較小者為準。

1. 在您的服務中列出檔案，方法是輸入 `gsutil ls gs://<storage_bucket_link>/`，其中 *<storage_bucket_link>* 是 GCP 服務帳戶中儲存檔案的儲存連結。
2. 從您的服務帳戶下載檔案，方法是輸入 `gsutil cp gs://<storage_bucket_link>/<file_name> <destination folder>`，其中：
   - *<storage_bucket_link>* 是 GCP 服務帳戶中儲存檔案的儲存連結。
   - *<file_name>* 是 PCAP 檔案的名稱。
   - *<destination folder>* 是您想要從中下載 PCAP 檔案的資料夾。
3. 解壓縮下載的檔案。
4. 使用只有您擁有的私密金鑰解密下載的檔案。

 ©2025 Palo Alto Networks, Inc.

# Prisma Access 遠端網路進階部署

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

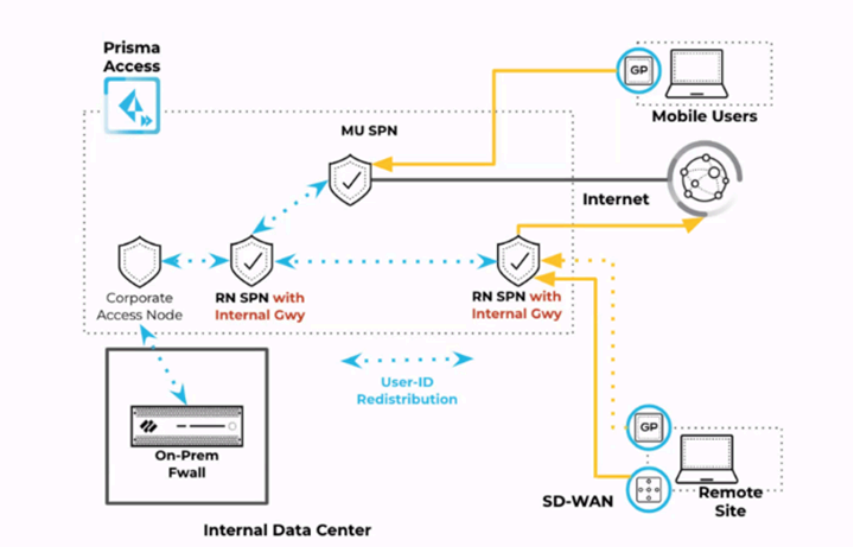
以下幾節為您展示適用於 Prisma Access 遠端網路的進階部署：

- 提供對遠端網路位置的安全輸入存取
- 為遠端網站建立高頻寬網路

## Prisma Access 內部閘道

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 和行動使用者授權<br>❑ Minimum Required Prisma Access Version：5.1<br>❑ Prisma Access (Managed by Panorama) 所需的最低資料平面版本：10.2.4<br>❑ 所需的最低 GlobalProtect 用戶端版本：6.0 |

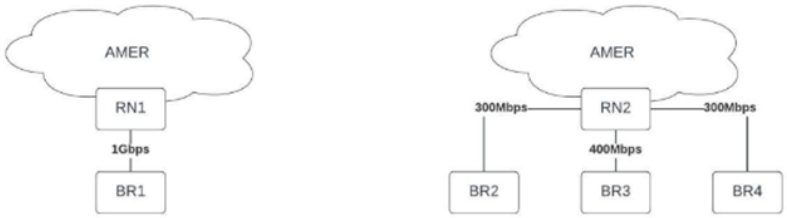
之前，若要為在 Prisma Access 中執行 GlobalProtect 用戶端軟體的主機產生 IP 使用者對應和 HIP，您必須部署一個內部部署 NGFW 作為內部閘道。這個解決方案不是雲端原生的。透過 Prisma Access 雲端原生內部閘道，您可以避免使用內部部署閘道，而且 Prisma Access 內部閘道會在遠端網路中本機產生 IP 使用者對應和 HIP。遠端網路耗用來自本機資料庫的 IP 使用者對應和 HIP 進行態勢檢查，而不是從其他防火牆得知。



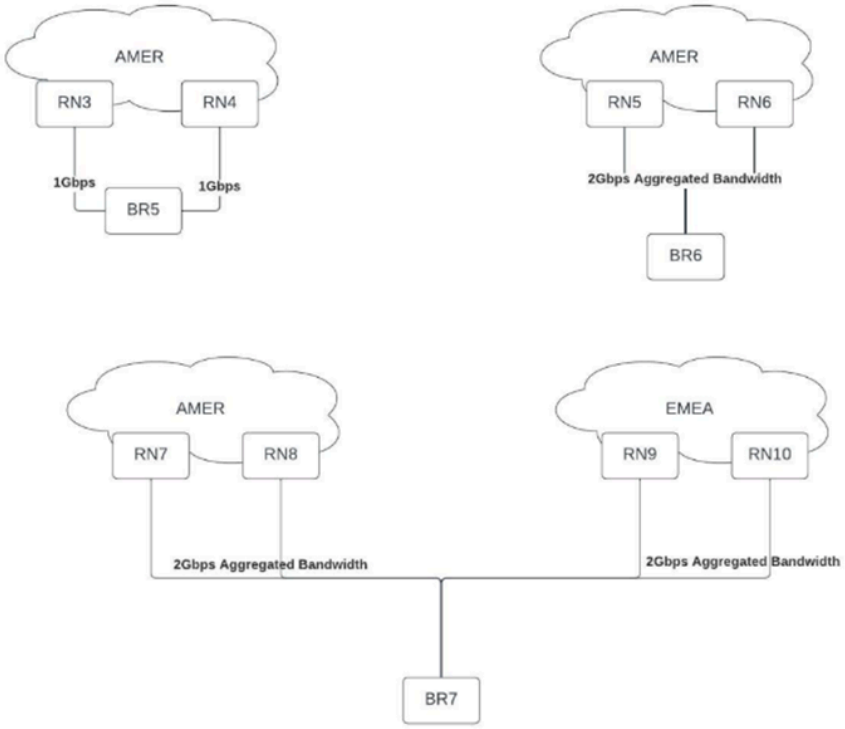


©2025 Palo Alto Networks, Inc.

請注意，當遠端網站有多個 IPsec 通道，通往不同的遠端網站（例如，主動/主動通道）或高頻寬網站時，您無法部署內部閘道。下圖顯示了內部閘道部署的支援環境範例。




下圖提供了不支援內部閘道的部署範例。




在您設定 Prisma Access 內部閘道之前，請先裝載您的行動使用者。

- Strata Cloud Manager
- Panorama

## Prisma Access 內部閘道 (Strata Cloud Manager)

完成以下步驟來設定 Prisma Access 內部閘道。

**STEP 1 |** 在 Strata Cloud Manager 中，設定 GlobalProtect、新增應用程式設定和裝載遠端網路。
請注意，目前沒有內部主機偵測和內部閘道設定。


©2025 Palo Alto Networks, Inc.

**STEP 2 |** 記下 **Remote Networks DNS IP Address**（遠端網路 **DNS IP** 位址），來自 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Prisma Access**。

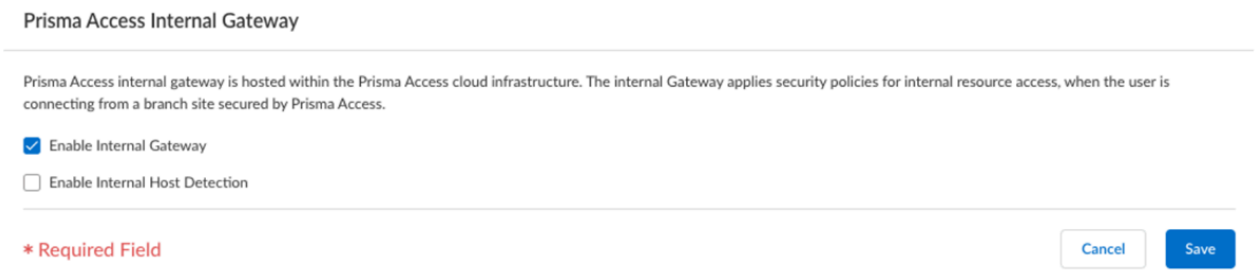
**STEP 3 |** 記下 **Gateway FQDNs**（閘道 **FQDN**），來自 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **GlobalProtect** > **Infrastructure**（基礎結構） > **Infrastructure Settings**（基礎結構設定） > **Gateway FQDNs**（閘道 **FQDN**）。

**STEP 4 |** 選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Remote Networks**（遠端網路） > **Advanced Settings**（進階設定）。

**STEP 5 |** 編輯 **Prisma Access Internal Gateway**（內部閘道）的設定，以啟用內部閘道，並 **Save**（儲存）變更。

（選用）如果您不想要使用自己的 DNS 伺服器，請為 IPv4 **Enable Internal Host Detection**（啟用內部主機偵測）。您可以僅在選取 **Enable Internal Gateway**（啟用內部閘道）之後啟用內部主機偵測。

*Prisma Access* 僅針對 ***Always On***（始終開啟）連線方法支援內部主機偵測。



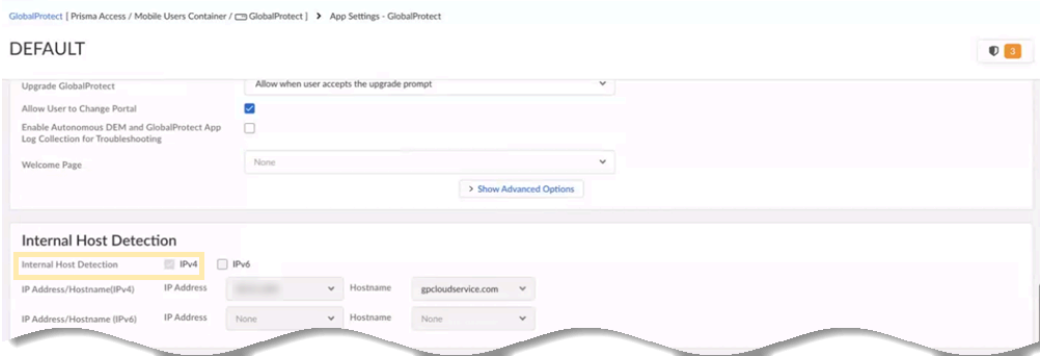

當您啟用內部閘道時，遠端網路執行個體會充當內部閘道。當您啟用內部主機偵測時，Prisma Access 會在遠端網路 DNS Proxy 伺服器上為內部主機偵測程序建立 PTR 記錄。

**STEP 6 |** 選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **GlobalProtect** > **GlobalProtect App**（**GlobalProtect** 應用程式）。

 ©2025 Palo Alto Networks, Inc.

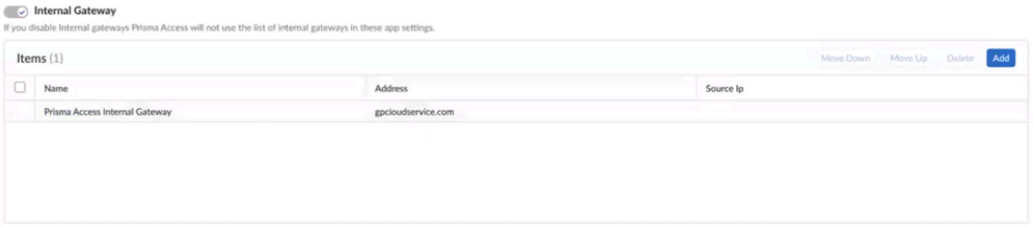
**STEP 7 |** 選取應用程式設定，並檢視內部主機偵測詳細資訊和內部閘道詳細資訊。

當您在步驟 5 中啟用內部閘道和內部主機偵測時，Prisma Access 也會在這裡啟用 IPv4 內部主機偵測和內部閘道。Prisma Access 會填入來自步驟 2 的 **Remote Networks DNS IP Address**（遠端網路 **DNS IP** 位址）值作為 IP 位址。




請注意，不支援 Prisma Access DNS Proxy 上的 IPv6 內部主機偵測。

您無法移除此 **Prisma Access Internal Gateway**（內部閘道）項目。不過，您可以新增自行部署的內部閘道。您可以在內部網路中部署自己的 DNS 伺服器，以進行內部主機偵測，但請確保新增 PTR 記錄，以便可以進行內部主機偵測。Prisma Access 會將來自步驟 3 的 **Gateway FQDNs**（閘道 **FQDN**）值附加到位址。




您可以選取 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Prisma Access**，來檢視 DNS Proxy 伺服器 IP 位址詳細資訊。

如果啟用 **Internal Host Detection**（內部主機偵測），請驗證 DNS 解析是否運作中、執行從內部網路到 DNS Proxy 伺服器 IP 的反向 DNS 查閱，並確保它傳回以 **`any-igw`** 開始的 FQDN。

**STEP 8 |** 將變更同時 **Push**（推送）至行動使用者和遠端網路。

**STEP 9 |** 登入端點。

連線到 GlobalProtect 時，首先使用 GlobalProtect 入口網站進行驗證。內部主機偵測會觸發 GlobalProtect 以連線到內部閘道。然後，當 GlobalProtect 代理程式繼續在非通道模式下操作時，第二個驗證便會出現，並將主機資訊提交到遠端網路上的內部閘道。

## Prisma Access 內部閘道 (Panorama)

**STEP 1 |** 在 Panorama 中，設定 GlobalProtect、新增應用程式設定和裝載遠端網路。

請注意，目前沒有內部主機偵測和內部閘道設定。

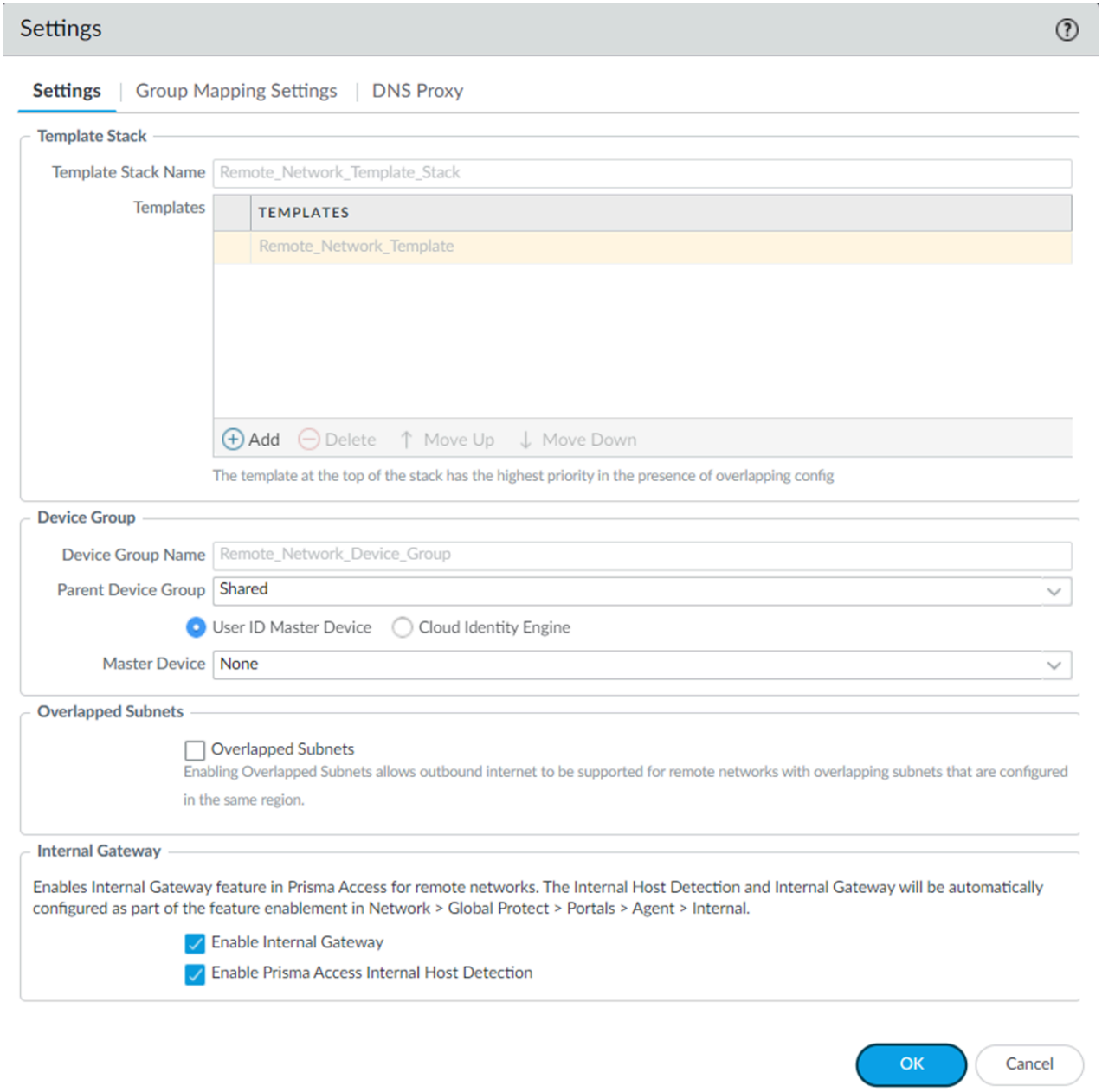
**STEP 2 |** 前往 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路） > **Settings**（設定）。

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** **Enable Internal Gateway**（啟用內部閘道）並保存變更。

（選用）如果您不想要使用自己的 DNS 伺服器，請為 IPv4 **Enable Prisma Access Internal Host Detection**（啟用 **Prisma Access** 內部主機偵測）。您可以僅在選取 **Enable Internal Gateway**（啟用內部閘道）之後啟用內部主機偵測。

*Prisma Access* 僅針對 ***Always On***（始終開啟）連線方法支援內部主機偵測。




當您啟用內部閘道時，遠端網路執行個體會充當內部閘道。當您啟用內部主機偵測時，Prisma Access 會在遠端網路 DNS Proxy 伺服器上為內部主機偵測程序建立 PTR 記錄。

當您啟用內部閘道時，Prisma Access 會在遠端網路範本中建立內部閘道設定。


©2025 Palo Alto Networks, Inc.

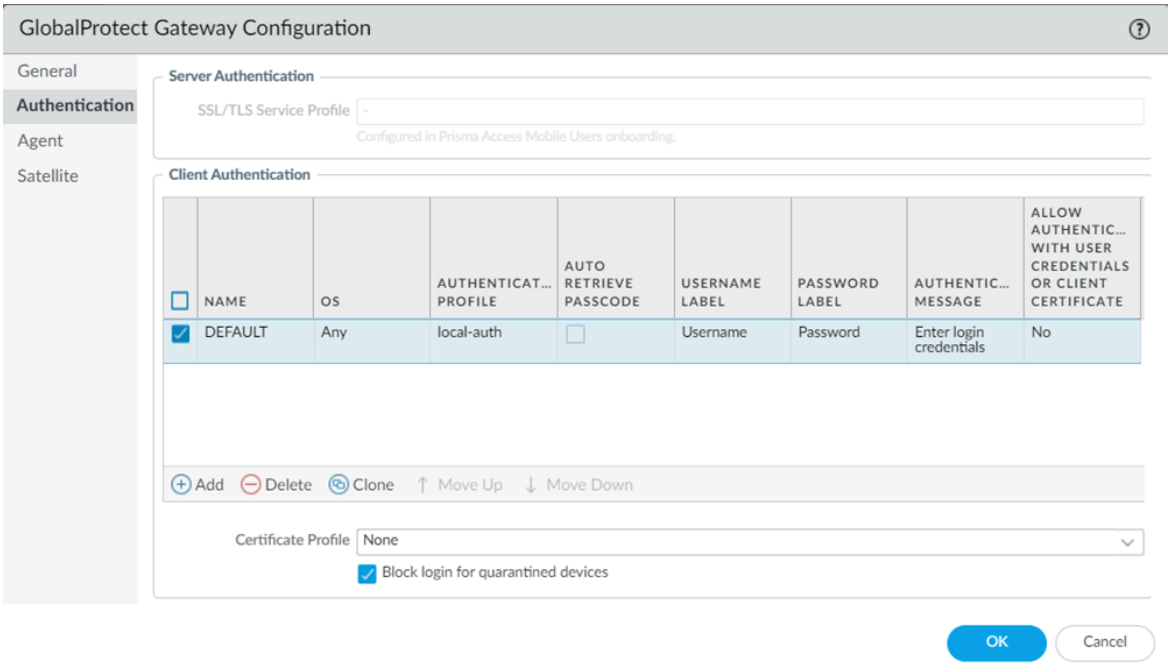
**STEP 4 |** 前往 **Templates**（範本） > **Network**（網路） > **GlobalProtect** > **Gateways**（閘道），並選取 **Remote_Network_Template**。

您將尋找為內部閘道建立的 **GlobalProtect_Internal_Gateway** 範本。

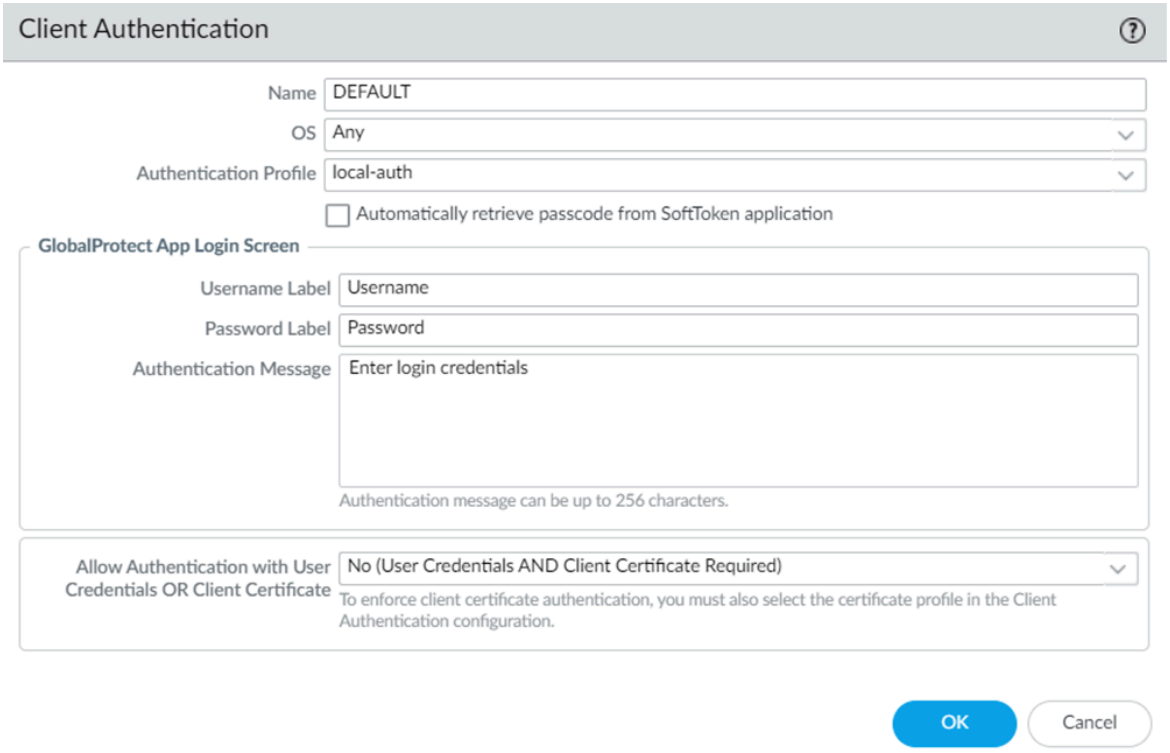

©2025 Palo Alto Networks, Inc.

**STEP 5 |** 為此遠端網路範本建立驗證設定檔，其類似於行動使用者範本中的驗證設定檔。

1. 選取遠端網路範本（**GlobalProtect_Internal_Gateway** 範本）超連結。
2. 前往 **Authentication**（驗證） > **Client Authentication**（用戶端驗證）。



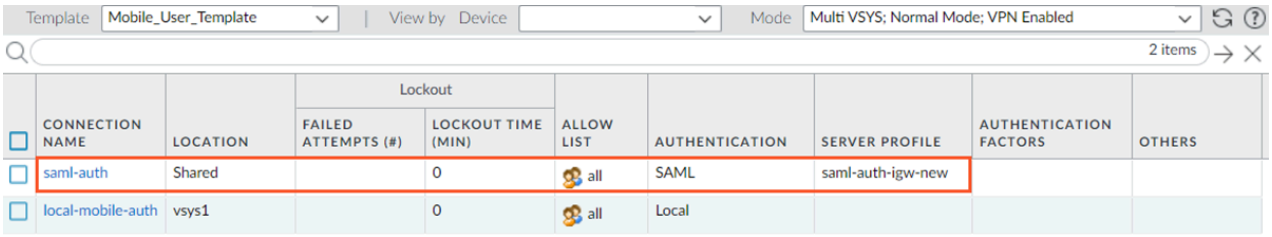

3. 編輯 **DEFAULT**（預設）用戶端驗證的驗證設定檔詳細資訊。



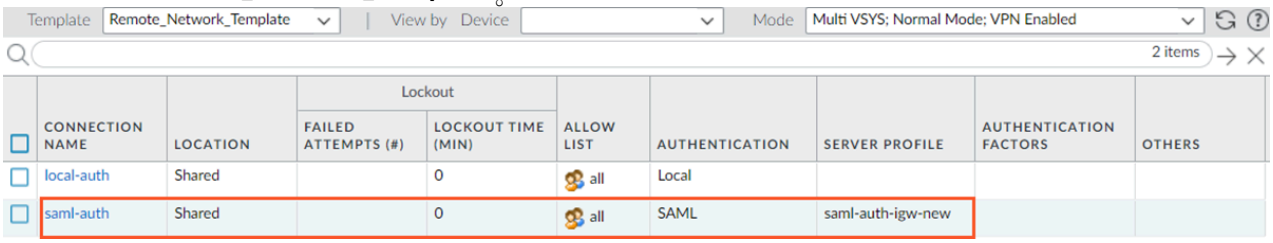


©2025 Palo Alto Networks, Inc.

建立與行動使用者範本中驗證設定檔相同的驗證設定檔。您可以在 **Template**（範本） > **Device**（裝置） > **Authentication Profile**（驗證設定檔）下找到行動使用者範本中使用的驗證設定檔。確保選取 **Mobile_User_Template**。



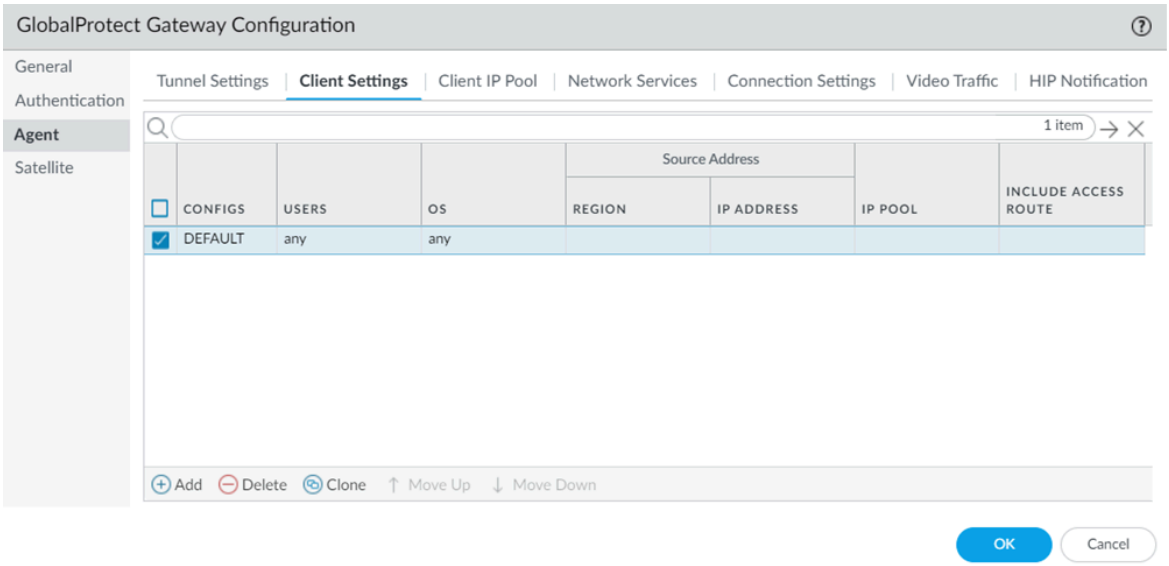

您也可以選取 ***Templates***（範本） ***> Device***（裝置） ***> Authentication Profile***（驗證設定檔），來檢視遠端網路範本的驗證設定檔。選取 ***Remote_Network_Template***。



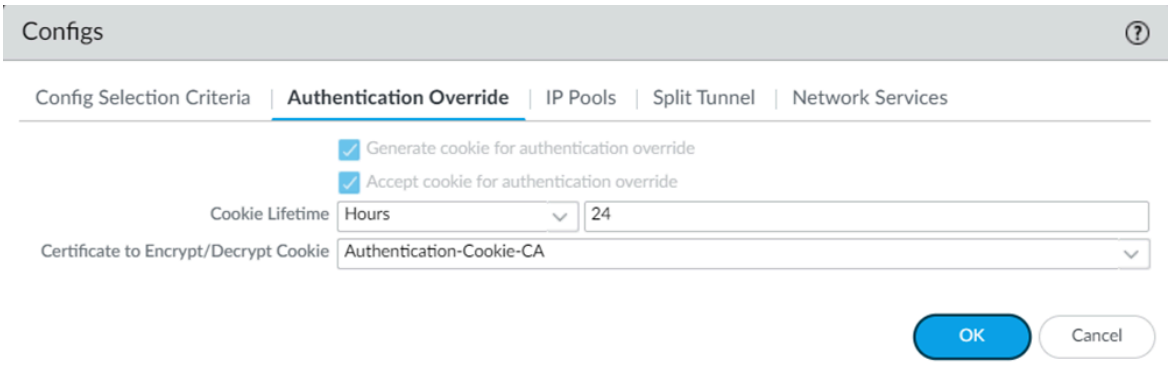

 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** 為遠端網路範本建立裝置憑證，其類似於行動使用者範本中的裝置憑證。

1. 選取遠端網路範本 **(GlobalProtect_Internal_Gateway)** 超連結。
2. 前往 **Agent**（代理程式） > **Client Settings**（用戶端設定）。



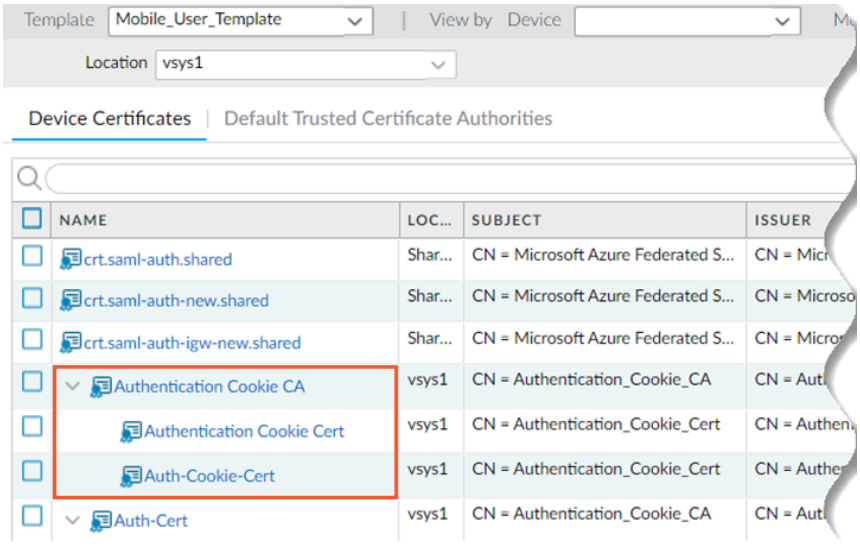

3. 選取 **DEFAULT**（預設）設定，然後前往 **Authentication Override**（驗證覆寫）設定。
4. 編輯 **Certificate to Encrypt/Decrypt Cookie**（要加密/解密 **Cookie** 的憑證）設定，然後建立新的裝置憑證。



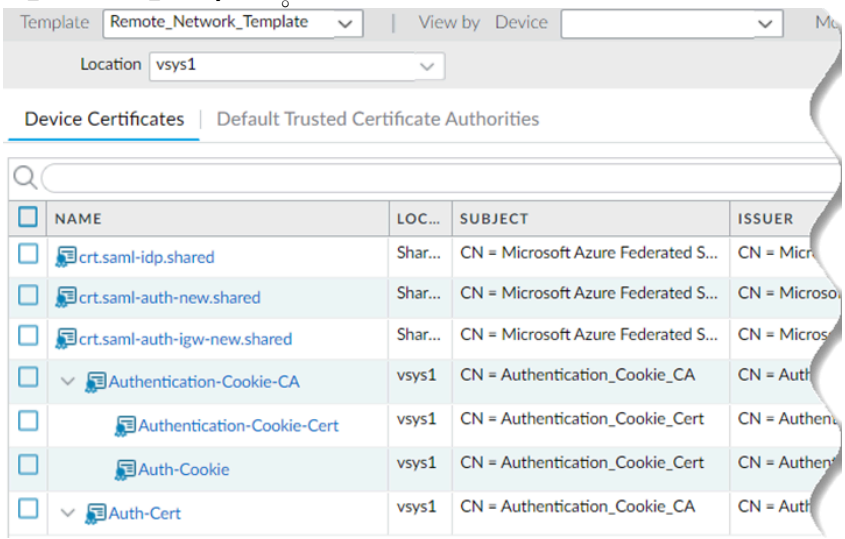

建立與行動使用者範本中裝置憑證相同的裝置憑證。您可以在 **Template**（範本） > **Device**（裝置） > **Certificate Management**（憑證管理） > **Certificates**（憑證） > **Device Certificates**（裝置憑證）下尋找行動使用者範本中使用的裝置憑證。確保選取 **Mobile_User_Template**。**DEFAULT**（預設）設定參考 **Authentication Cookie CA**（驗

 ©2025 Palo Alto Networks, Inc.

證 **Cookie CA**）憑證。遵循與 **Mobile_User_Template** 中階層相同的階層，以成功進行驗證。




您也可以選取 ***Template***（範本）> ***Device***（裝置）> ***Certificate Management***（憑證管理）> ***Certificates***（憑證）> ***Device Certificates***（裝置憑證），來檢視遠端網路範本的裝置憑證。選取 ***Remote_Network_Template***。




**STEP 7 |** 將變更同時 **Push**（推送）至行動使用者和遠端網路。

## 提供對遠端網路位置的安全輸入存取

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權，包括用於站台對站台和使用者對站台存取的網路互連 |


©2025 Palo Alto Networks, Inc.

如果您的組織在遠端網站託管可存取網際網路的應用程式，則提供對這些應用程式的存取會使您的網路暴露於開放網際網路帶來的所有威脅。本節描述 Prisma Access 如何提供一種方法來提供對這些應用程式的安全存取、何時應該實作它，以及如何設定它。

- 遠端網站的安全輸入存取
- 安全輸入存取範例
- 使用安全輸入存取的指導方針
- 為遠端網路網站設定安全輸入存取

## 遠端網站的安全輸入存取

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權，其中包括用於站台對站台和使用者對站台存取的網路互連 |

Prisma Access for Remote Networks 允許對連線網際網路的應用程式的輸出存取。在某些情況下，您的組織可能需要提供對遠端網站上應用程式或網站的輸入存取，並為任何連線網際網路的使用者提供對該應用程式的安全存取—不只是受到 Prisma Access 保護的使用者。例如：

- 您在遠端網站上托管面向公眾的自訂應用程式或入口網站。
- 您有一個實驗室或測試環境，您想要為其提供安全存取。
- 對於不是組織網域成員的使用者，您需要為其提供對應用程式或網站的存取。
- 您有需要存取內部資產管理、追蹤或狀態應用程式的 IoT 裝置。

若要這樣做，請建立一個允許安全輸入存取的遠端網路。如果您需要對遠端網站進行輸出存取以及輸入存取，請在相同位置建立兩個遠端網路（一個用於輸入存取，另一個用於輸出存取）。

雖然這個解決方案可以為每個遠端網路提供最多 *50,000* 個並行輸入工作階段，但 *Palo Alto Networks* 不建議使用這個解決方案，來提供對高容量應用程式或網站的存取。

## 安全輸入存取範例

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權，其中包括用於站台對站台和使用者對站台存取的網路互連 |

本節提供輸入存取範例，以及 Prisma Access 在各種部署中指派的 IP 位址。

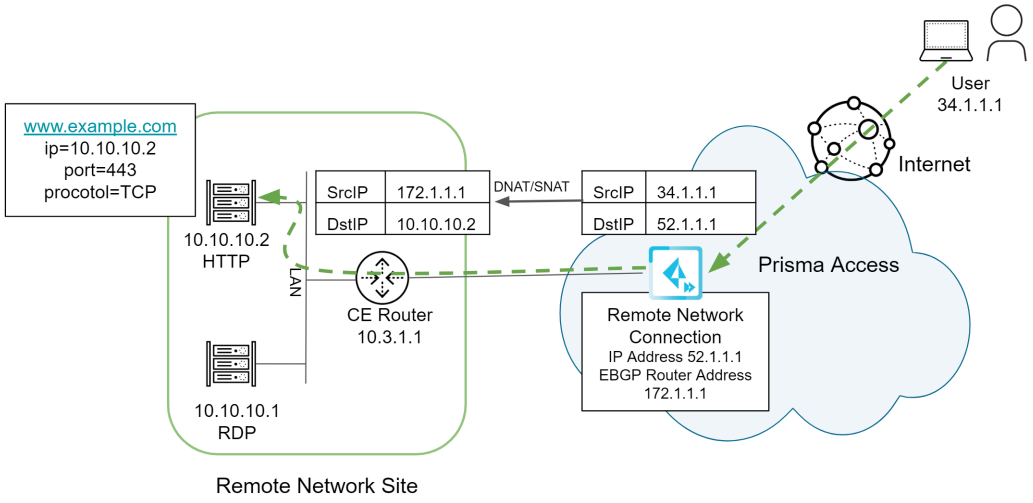
以下範例顯示了一個範例設定，在遠端網站為應用程式 (www.example.com) 啟用輸入存取。您將 IP 位址 10.10.10.2、連接埠 443 和通訊協定 TCP 指派給應用程式。然後，當您設定輸入存取時，

 ©2025 Palo Alto Networks, Inc.

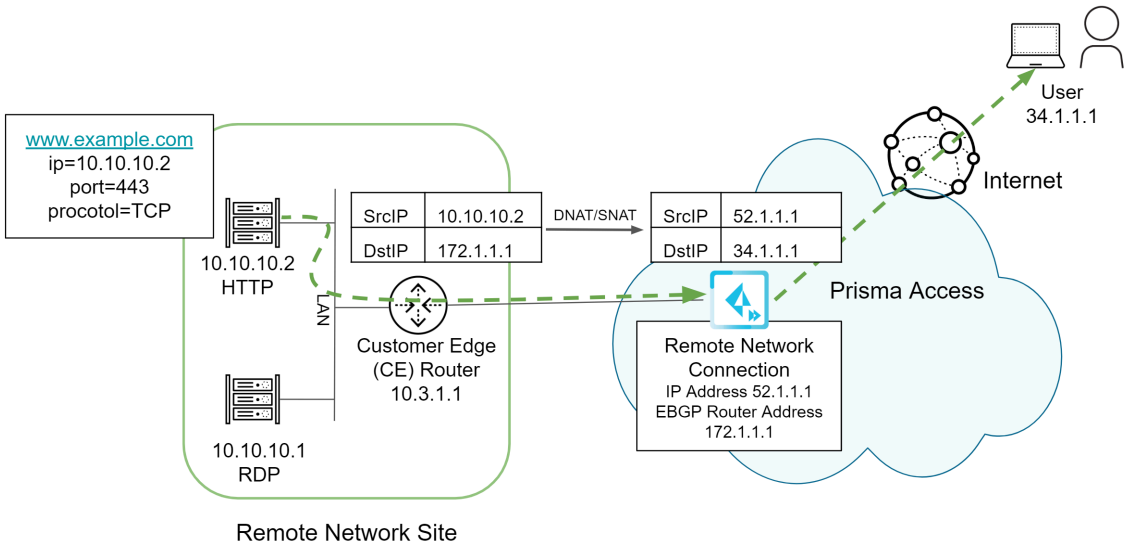
在 Prisma Access 中輸入這些值。在您儲存並提交您的變更之後，Prisma Access 會將公有 IP 位址指派給您定義的應用程式，此案例中的 52.1.1.1.1。

Prisma Access 預設會封包執行來源網路位址轉譯（來源 NAT）。如果遠端網路網站上支援 IPSec 的裝置能夠執行對稱傳回（例如 Palo Alto Networks 新世代防火牆），您可以停用來源 NAT。

下圖顯示了從使用者流向應用程式的流量。由於啟用了來源 NAT，路由表中的來源 IP 位址會從使用者裝置的 IP (34.1.1.1) 變更為遠端網路的 **EBGP Router**（**EBGP** 路由器）位址（**Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Remote Networks**（遠端網路） > **EBGP Router**（**EBGP** 路由器））。(172.1.1.1)。

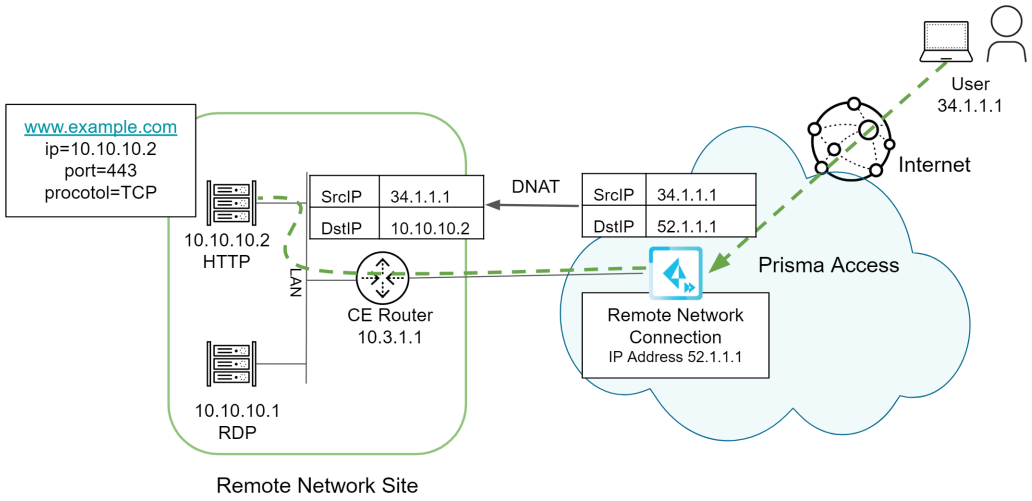



下圖顯示已啟用來源 NAT 的流量的傳回路徑。

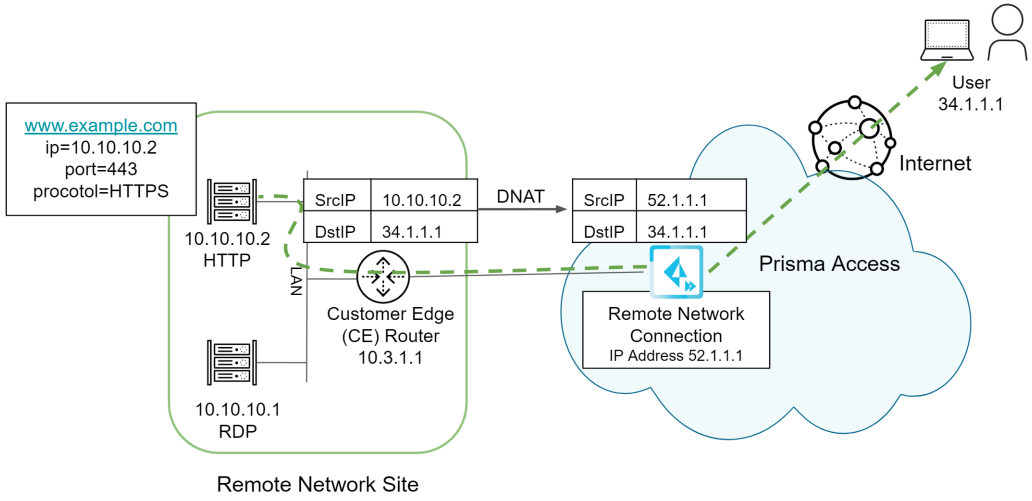



如果您停用來源 NAT，Prisma Access 仍執行目的地 NAT，但要求的來源 IP 位址保持不變。


©2025 Palo Alto Networks, Inc.




對於傳回流量，SNAT 已停用，而且所有路由表的目的地位址都是使用者的 IP 位址 (34.1.1.1)。




如果您有一個資源位於已啟用輸入存取的遠端網路網站，並且您想要非輸入存取網站的使用者可以存取該資源，則您可以在設定非輸入存取遠端網路時，**Allow inbound flows to other Remote Networks over the Prisma Access backbone**（允許輸入流量透過 **Prisma Access** 骨幹流向其他遠端網路）。

如果允許來自其他遠端網路的輸入流量，則必須啟用來源 *NAT*。



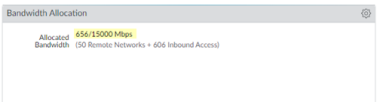

 ©2025 Palo Alto Networks, Inc.

# 使用安全輸入存取的指導方針

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權，其中包括用於站台對站台和使用者對站台存取的網路互連 |

當您將遠端網路設定為使用安全輸入存取時，請使用下列指導方針和限制：

- 設定遠端網路進行輸入存取時，您可以從授權中為配置的 IP 位址新增單位 (Mbps)（5 個 IP 位址為 150 Mbps，而 10 個 IP 位址為 300 Mbps）。基於此原因，在開始之前，請確保您有足夠的剩餘授權頻寬，可裝載輸入存取遠端網路。若要檢查您的可用頻寬，請選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路），然後檢視您的授權 **Bandwidth Allocation**（頻寬配置）。此區域顯示您已配置的頻寬，以及總授權頻寬。



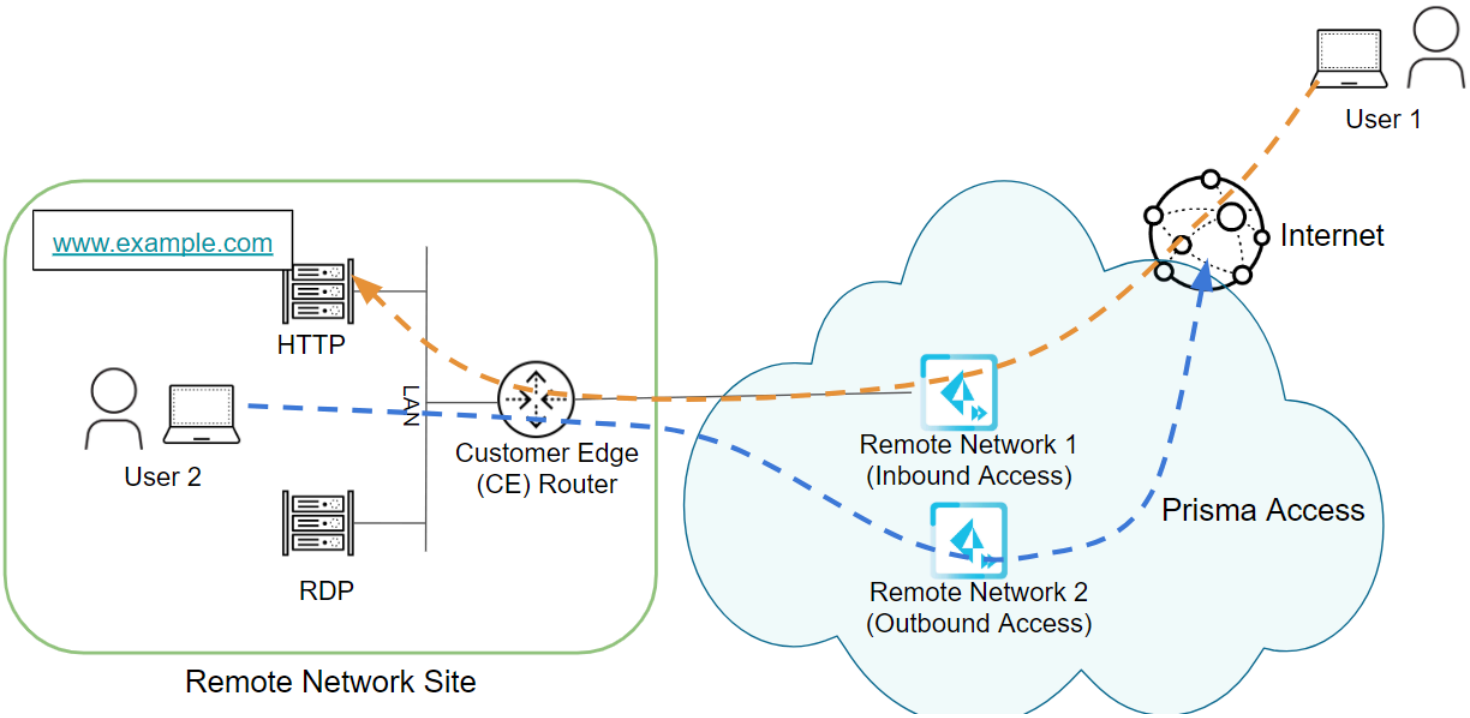

- 安全輸入存取會使用 Prisma Access 位置的子集。
- 您無法修改現有的遠端網路以提供安全輸入存取；而是建立新的遠端網路。
- 輸入存取功能無法在使用 ECMP 負載平衡的遠端網路上使用。
- 不支援應用程式連接埠轉換。
- 裝載遠端網路的大量匯入功能不支援輸入存取。使用 Panorama 來裝載新的輸入存取遠端網路。
- 請勿透過服務連線使用遠端網路輸入存取搭配流量轉送規則。
- 輸入遠端網路不允許源於分支的輸出流量。
- 不支援 User-ID 和應用程式驗證。
- Prisma Access 強制執行下列速率限制閾值以提供爆流保護，並測量每秒連線速率 (CPS)：

| 爆流保護類型 | 以 **CPS** 為單位的警示率 | 以 **CPS** 為單位的啟動率 |
| --- | --- | --- |
| SYN 爆流 | 10000 | 15000 |
| ICMP 爆流 | 20 | 20 |

  如果您需要更好的保護以防範新工作階段爆流，請聯絡您的 Palo Alto Networks 團隊。
- 為安全輸入存取而設定的遠端網路只能用於該目的。如果您需要對遠端網站進行輸出存取以及輸入存取，請在相同位置建立兩個遠端網路網站（一個用於輸入存取，另一個用於輸出存


©2025 Palo Alto Networks, Inc.

取），如下圖所示。在此範例中，使用者 1 使用遠端網路 1 進行對 www.example.com 的輸入存取，而使用者 2 則使用遠端網路 2，從遠端網路位置進行輸出網際網路存取。




- 如果您有已排除其中一個雲端提供者的 Prisma Access 部署，則可能不支援輸入存取；在此情況下，您無法在遠端網路裝載期間選擇位置。
- 評估授權不支援安全輸入存取。

## 為遠端網路網站設定安全輸入存取

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權，其中包括用於站台對站台和使用者對站台存取的網路互連 |

您的部署可能依計算位置裝載頻寬或 依位置進行此操作；支援任一方法設定遠端網路輸入存取。當您為依計算位置配置頻寬的遠端網路設定輸入存取時，您根據每個位置指定頻寬。若要建立一個允許安全輸入存取的遠端網路網站，請完成下列其中一個工作流程：

- 若要為依計算位置配置頻寬的遠端網路部署設定安全輸入存取，請完成下列步驟。
- 若要為依位置配置頻寬的遠端網路部署設定安全輸入存取，請完成下列步驟。


©2025 Palo Alto Networks, Inc.

為遠端網路設定安全輸入存取

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access 授權，其中包括用於站台對站台和使用者對站台存取的網路互連 |

若要使網際網路可存取的應用程式可從遠端網路網站使用，請列出您想要提供存取權的應用程式，並為每個應用程式指派一個私人 IP、連接埠號碼和通訊協定組合。如果您將相同的 IP 位址用於多個應用程式，則每個應用程式的連接埠/通訊協定組合必須是唯一的；如果您將相同的連接埠/通訊協定組合用於多個應用程式，則每個 IP 位址必須是唯一的。

若要開始設定，您可以選擇要為應用程式關聯的公用 IP 位址數目。您可以指定每個遠端網路網站 5 個或 10 個公用 IP 位址。除了您已針對與遠端網路相關聯的計算位置所配置的頻寬之外，每個公用 IP 配置都會從遠端網路授權中取得頻寬 (單位)。5 個 IP 位址從您的遠端網路授權配置中取得 150 Mbps，而 10 個 IP 位址則取得 300 Mbps。

在選擇公用 IP 位址的數目之後，您可以輸入應用程式，以及其相關聯的私人 IP/連接埠號碼/通訊協定組合，您需要其進行安全輸入存取。

您可以決定您想要如何將應用程式對應至公用 IP 位址。根據預設，Prisma Access 會將公用 IP 位址指派給您指定的應用程式，並且多個應用程式可以指派給單一 IP 位址。如果您需要將單一應用程式對應至單一公用 IP 位址，您可以在系統設定期間選取 **Dedicated IP**（專用 **IP**）。您可以為每組佈建的公用 IP 位址（5 或 10 個）最多設定 100 個輸入應用程式。

- Strata Cloud Manager
- Panorama

為遠端網路設定安全輸入存取 *(Strata Cloud Manager)*

以下是如何使所有網際網路連線使用者（不只是 Prisma Access 使用者）可從遠端網路存取應用程式的方式。

**STEP 1 |** 如果您還沒有這樣做，請檢閱輸入存取遠端網路指導方針。

**STEP 2 |** 收集您需要的應用程式詳細資訊以開始使用。

列出您想要提供存取權的應用程式，並為每個應用程式指派一個私人 IP、連接埠號碼和通訊協定組合。如果您將相同的 IP 位址用於多個應用程式，則每個應用程式的連接埠/通訊協定組合必須是唯一的；如果您將相同的連接埠/通訊協定組合用於多個應用程式，則每個 IP 位址必須是唯一的。

**STEP 3 |** 在 Strata Cloud Manager 中，前往 **Workflows**（工作流程） > **Prisma Access Setup**（設定） > **Remote Networks**（遠端網路） > **Inbound Access**（輸入存取） > **Add Inbound Access**（新增輸入存取）。

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** 輸入所需的詳細資訊。

選擇您想要用於應用程式的 **Number of Public IPs**（公用 **IP** 數目），可以是五個或十個。

每個公用 IP 配置都會從您的遠端網路授權中取得帶寬，此外還有遠端網路的授權費用。5 個 IP 位址從您的遠端網路授權配置中取得 150 MB，而 10 個 IP 位址則取得 300 MB。

從 Prisma Access 4.1 版開始，如果您有一個資源位於已啟用輸入存取的遠端網路網站，並且您想要非輸入存取網站的使用者可以存取該資源，則您可以在設定非輸入存取遠端網路時，**Allow inbound flows to other Remote Networks over the Prisma Access backbone**（允許輸入流量透過 **Prisma Access** 骨幹流向其他遠端網路）。

從 Prisma Access 5.0 版開始，當您設定非輸入存取遠端網路時，可以允許透過服務提供者 (SP) 骨幹網路將輸入流程流向其他遠端網路。

*SP* 互連僅支援下列項目：

- *GCP* 區域
- 新的 *Prisma Access* 部署
- 明確 *Proxy* 輸出流量

**STEP 5 |** 新增您想要安全存取的 **Inbound Access Applications**（輸入存取應用程式）。

為應用程式新增相關聯的私人 IP/連接埠號碼/通訊協定組合。

**STEP 6 |** 決定您想要如何將應用程式對應至公用 IP 位址。

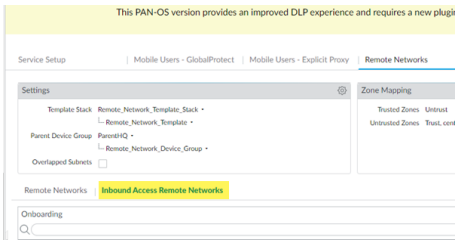
根據預設，Prisma Access 會將公用 IP 位址指派給您指定的應用程式，並且多個應用程式可以指派給單一 IP 位址。如果您需要將單一應用程式對應至單一公用 IP 位址，您可以在系統設定期間 **Assign Dedicated IP**（指派專用 **IP**）。您可以為每組佈建的公用 IP 位址（5 或 10 個）最多設定 100 個輸入應用程式。

**STEP 7 |** 完成設定輸入存取遠端網路，就像設定常規的遠端網路網站一樣。

為遠端網路設定安全輸入存取 *(Panorama)*

如果您有 Prisma Access 部署，依計算位置配置遠端網路頻寬，請完成下列步驟來設定輸入存取。

**STEP 1 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路），然後選取 **Inbound Access Remote Networks**（輸入存取遠端網路）。




**STEP 2 |** **Add**（新增）遠端網路進行輸入存取。

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 指定輸入存取遠端網路連線的設定。

1. 為輸入存取連線輸入一個 **Name**（名稱）。
2. 輸入 **Location**（位置）。

   輸入存取支援位置子集。
3. 指定要用於輸入存取連線的 **Bandwidth**（頻寬）。

   您可以根據每個位置為輸入存取連線配置頻寬。
4. 指定要用於輸入存取連線的 **Number of Public IPs**（公用 **IP** 數目）。

   指定 5 個或 10 個公用 IP 位址。除了您已針對與遠端網路相關聯的計算位置所配置的頻寬之外，每個公用 IP 配置都會從遠端網路授權中取得頻寬 (單位)。
5. 選取要與輸入存取連線搭配使用的 IPsec 通道。
6. 選取您是否想要 **Allow inbound flows to other Remote Networks over the Prisma Access Backbone**（允許輸入流量透過 **Prisma Access** 骨幹流向其他遠端網路）。

   如果您有一個資源位於已啟用輸入存取的遠端網路網站，並且您想要非輸入存取網站的使用者可以存取該資源，則您可以在設定非輸入存取遠端網路時，允許 **Allow Inbound Flows To Other Remote Networks over the Prisma Access Backbone**（允許輸入流量透過 **Prisma Access** 骨幹流向其他遠端網路）。如果允許來自其他遠端網路的輸入流量，則必須啟用來源 NAT。
7. （選用）如果您在此位置有次要 WAN 連結，請選取 **Enable Secondary WAN**（啟用次要 **WAN**），然後提供與主要 IPSec 通道不同的 **IPSec Tunnel**（**IPsec** 通道）。

**STEP 4 |** 為您的部署設定 **Static Routes**（靜態路由）、**BGP** 和 **QoS**。

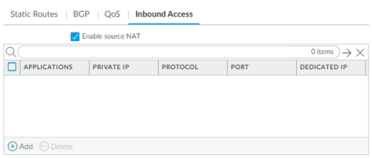
此設定與非輸入存取遠端網路連線相同。

**STEP 5 |** 按一下 **Inbound Access**（輸入存取）頁籤，以設定輸入存取選項。

1. （選用）若要停用來源 NAT，請取消選取 **Enable Source NAT**（啟用 來源 **NAT**）。

   根據預設，來源 NAT 已啟用。如果遠端網路網站上支援 IPsec 的裝置能夠執行對稱傳回（例如 Palo Alto Networks 新世代防火牆），或者如果您尚未選取 **Allow inbound flows to other Remote Networks over the Prisma Access backbone**（允許輸入流量透過 **Prisma Access** 骨幹流向其他遠端網路），請取消選取 **Enable source NAT**（啟用來源 **NAT**）。

   > 如果您選取此核取方塊，則必須在 ***Inbound Access***（輸入存取）頁籤中 ***Enable source NAT***（啟用來源 ***NAT***）。來源 *NAT* 是允許輸入流量流向其他遠端網路的需求。

   
   
2. **Add**（新增）應用程式以提供安全輸入存取。

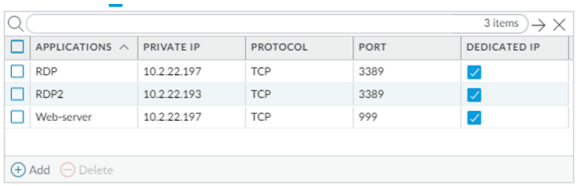
   您可以為每組佈建的公用 IP 位址（5 或 10 個）最多設定 100 個輸入應用程式。為每個應用程式輸入唯一的 **Private IP**（私人 **IP**）位址、**Protocol**（通訊協定）和 **Port**（連接

 ©2025 Palo Alto Networks, Inc.

埠）組合。只要您為一個應用程式選取 **TCP**，為另一個應用程式選取 **UDP**，就可以接受將重複的私人 IP 位址和連接埠用於兩個應用程式。

請提供下列值：

- 指定 **Application**（應用程式）的名稱。
- 指定要與此應用程式搭配使用的 **Private IP**（私人 **IP**）位址。
- 指定要與應用程式搭配使用的 **Protocol**（通訊協定）（**TCP** 或 **UDP**）。
- 指定要與應用程式搭配使用的 **Port**（連接埠）。
- 選擇是否要將單一公用 IP 位址專用於單一應用程式；若要這樣做，請選取 **Dedicated IP**（專用 **IP**）。

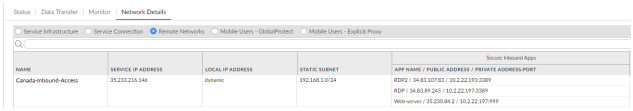



**STEP 6 |** 按一下 **OK**（確定）儲存您的變更。

**STEP 7 |** **Save**（儲存）並 **Commit**（提交）您的變更。

**STEP 8 |** 等待大約 30 分鐘，讓 Prisma Access 產生公用 IP 位址；然後選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Remote Networks**（遠端網路），並記下與您所建立應用程式的 **App Name**（應用程式名稱）相關聯的 **Public Address**（公用位址）。

如果您選取了 **Dedicated IP**（專用 **IP**），請尋找與 **Public Address**（公用位址）相關聯的單一應用程式。



**STEP 9 |** 建立安全性政策，以允許來自輸入網際網路使用者的流量。

由於 Prisma Access 預設安全性政策僅允許不信任至不信任流量，因此您需要設定安全性政策，以允許輸入存取應用程式的不信任至不信任流量。Palo Alto Networks 建議您限制您對輸

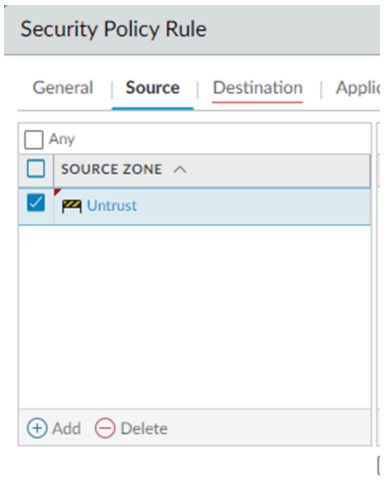
 ©2025 Palo Alto Networks, Inc.

入應用程式允許的存取類型。下列範例提供對 SSH 伺服器、Web 入口網站和 RDP 伺服器的存取。

1. 選取 **Policies**（政策） > **Security**（安全性），並 **Add**（新增）一個政策。

   請務必在 **Remote_Network_Device_Group** 裝置群組下建立此政策。

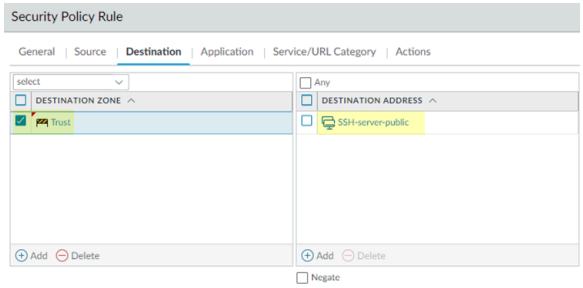
2. 選取 **Source**（來源）流量作為 **Untrust**（不信任）。



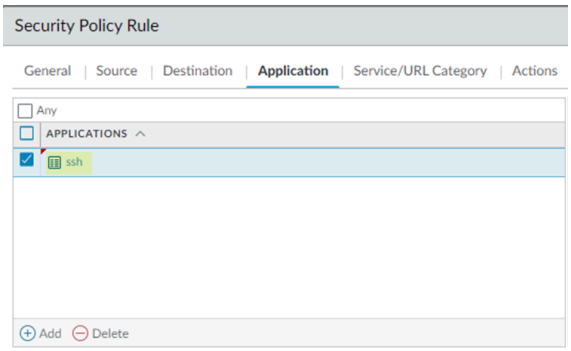

3. 透過選取目的地流量的 **Destination Zone**（目的地區域）作為 **Trust**（信任），並指定 **Destination Address**（目的地位址）為 **SSH-server-public**，來建立一個允許 SSH 伺服器


©2025 Palo Alto Networks, Inc.

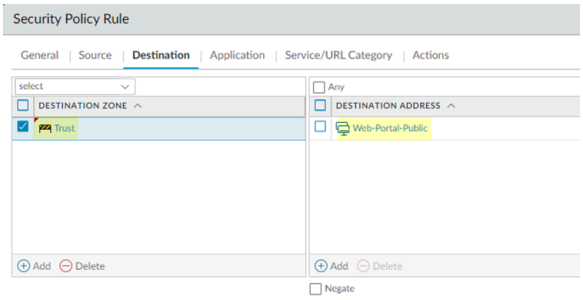
流量的政策。這是您建立的位址或位址群組物件，其中有一個清單，列出用於 SSH 登入的所有公用 IP 位址。




4. 選取 **Application**（應用程式）為 **ssh**。

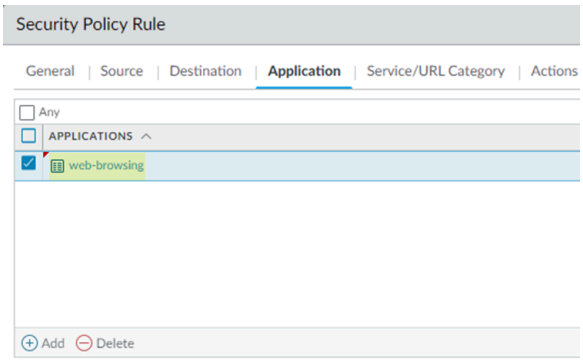



5. 選取 **Service/URL Category**（服務/**URL** 類別）為 **application-default**，以根據 Palo Alto Networks 定義的預設連接埠，允許或拒絕應用程式。
6. 在 **Actions**（動作）中，選取 **Allow**（允許）。
7. 按一下 **OK**（確定）儲存原則。
8. 建立一個政策以允許 Web 入口網站存取，方法是在先前的步驟中建立一個政策，但取代 **Destination**（目的地）和 **Application**（應用程式）頁籤中的下列設定：
   - 選取位址或位址群組的 **Destination Address**（目的地位址）為 **Web-Portal-Public**，其中包含 Web 入口網站的所有公用 IP 位址。



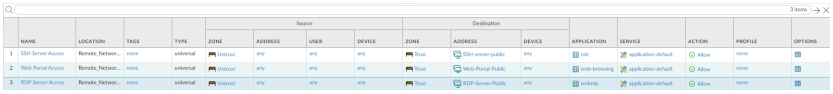

   - 選取 **Application**（應用程式）為 **web-browsing**。


©2025 Palo Alto Networks, Inc.




9. 建立一個安全性政策進行 RDP 伺服器存取，進而使用您對其他政策使用的同一設定，但建立稱為 **RDP-Server-Public**（其中包含 RD P 伺服器的公用 IP 位址） 的位址或位址群組物件作為 **Destination Address**（目的地位址），以及建立 **webrdp** 作為 **Application**（應用程式）。

   完成時，您有三個不同的政策，允許 SSH 伺服器存取、Web 入口網站存取和 RDP 伺服器存取。

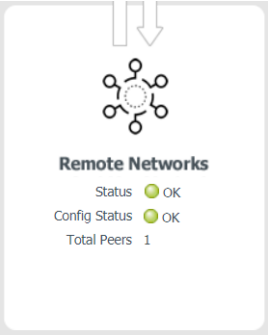


**STEP 10 |** **Save**（儲存）並 **Commit**（提交）您的變更。

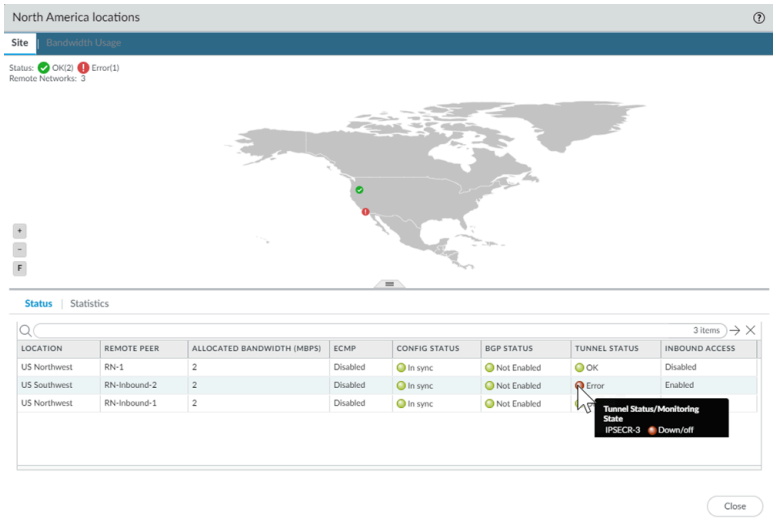
 ©2025 Palo Alto Networks, Inc.

**STEP 11 |** 檢查遠端網路連線是否正常運作，並正確處理輸入流量。

1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > > **Status**（狀態） > **Remote Networks**（遠端網路），然後將游標暫留在 **Status**（狀態）和 **Config Status**（設定狀態）區域上，以查看通道的狀態。




2. 如果發現問題，請選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > > **Monitor**（監控） > **Remote Networks**（遠端網路）、在地圖中選取遠端網路通道的位置，然後將游標暫留在 **Tunnel Status**（通道狀態）區域上，以確定錯誤的原因。




## 為依位置配置頻寬的位置設定遠端網路網站的安全輸入存取

| 這可在何處使用？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | • Prisma Access 授權，其中包括用於站台對站台和使用者對站存取的網路互連 |

如果有 Prisma Access 部署，依位置配置遠端網路頻寬，請完成下列步驟來設定輸入存取。


©2025 Palo Alto Networks, Inc.

**STEP 1 |** 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路）、**Add**（新增）連線並設定遠端網路，包括路由和 IPSec 通道選項。

如需詳細資料，請參閱 Prisma Access 遠端網路。您的部署可能依計算位置或依位置裝載頻寬；支援任一方法進行輸入存取。

確保您選取其中一個支援位置進行輸入存取。

**STEP 2 |** 按一下 **Inbound Access**（輸入存取）頁籤，以設定輸入存取選項。

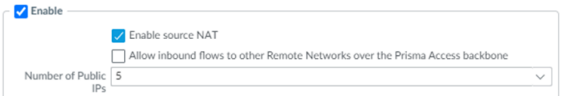
1. 選取 **Enable**（啟用）以啟用遠端網路的輸入存取。

   如果您選取了一個不受支援的位置進行輸入存取，Prisma Access 會提示您選取一個支援的位置。

2. （選用）若要停用來源 NAT，請取消選取 **Enable Source NAT**（啟用 來源 **NAT**）。

   根據預設，來源 NAT 已啟用。如果遠端網路網站上支援 IPsec 的裝置能夠執行對稱傳回（例如 Palo Alto Networks 新世代防火牆），或者如果您尚未選取 **Allow inbound flows to other Remote Networks over the Prisma Access backbone**（允許輸入流量透過 **Prisma Access** 骨幹流向其他遠端網路），請取消選取 **Enable source NAT**（啟用來源 **NAT**）。

   如果您選取此核取方塊，則必須在 ***Inbound Access***（輸入存取）頁籤中 ***Enable source NAT***（啟用來源 ***NAT***）。來源 *NAT* 是允許輸入流量流向其他遠端網路的需求。




**STEP 3 |** **Add**（新增）應用程式以提供安全輸入存取。

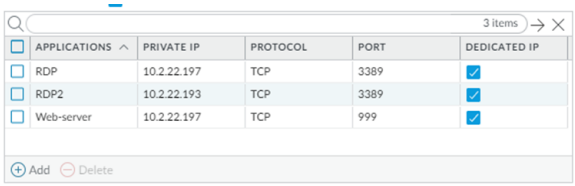
您可以為每組佈建的公用 IP 位址（5 或 10 個）最多設定 100 個輸入應用程式。為每個應用程式輸入唯一的 **Private IP**（私人 **IP**）位址、**Protocol**（通訊協定）和 **Port**（連接埠）組合。只

 ©2025 Palo Alto Networks, Inc.

要您為一個應用程式選取 **TCP**，為另一個應用程式選取 **UDP**，就可以接受將重複的私人 IP 位址和連接埠用於兩個應用程式。

請提供下列值：

- 指定 **Application**（應用程式）的名稱。
- 指定要與此應用程式搭配使用的 **Private IP**（私人 **IP**）位址。
- 指定要與應用程式搭配使用的 **Protocol**（通訊協定）（**TCP** 或 **UDP**）。
- 指定要與應用程式搭配使用的 **Port**（連接埠）。
- 選擇是否要將單一公用 IP 位址專用於單一應用程式；若要這樣做，請選取 **Dedicated IP**（專用 **IP**）。

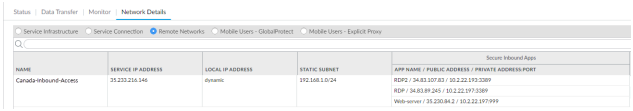



**STEP 4 |** 按一下 **OK**（確定）儲存您的變更。

**STEP 5 |** **Save**（儲存）並 **Commit**（提交）您的變更。

**STEP 6 |** 等待大約 30 分鐘，讓 Prisma Access 產生公用 IP 位址；然後選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Remote Networks**（遠端網路），並記下與您所建立應用程式的 **App Name**（應用程式名稱）相關聯的 **Public Address**（公用位址）。

如果您選取了 **Dedicated IP**（專用 **IP**），請尋找與 **Public Address**（公用位址）相關聯的單一應用程式。



**STEP 7 |** 建立安全性政策，以允許來自輸入網際網路使用者的流量。

由於 Prisma Access 預設安全性政策僅允許不信任至不信任流量，因此您需要設定安全性政策，以允許輸入存取應用程式的不信任至不信任流量。Palo Alto Networks 建議您限制您對輸

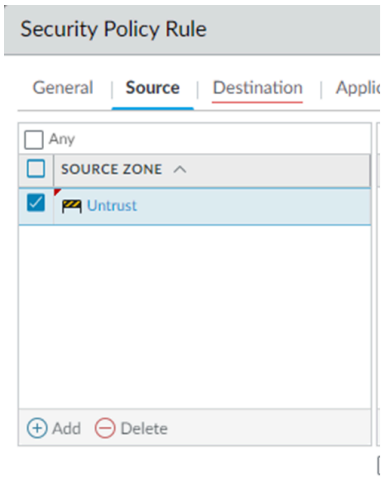
 ©2025 Palo Alto Networks, Inc.

入應用程式允許的存取類型。下列範例提供對 SSH 伺服器、Web 入口網站和 RDP 伺服器的存取。

1. 選取 **Policies**（政策） > **Security**（安全性），並 **Add**（新增）一個政策。

   請務必在 **Remote_Network_Device_Group** 裝置群組下建立此政策。

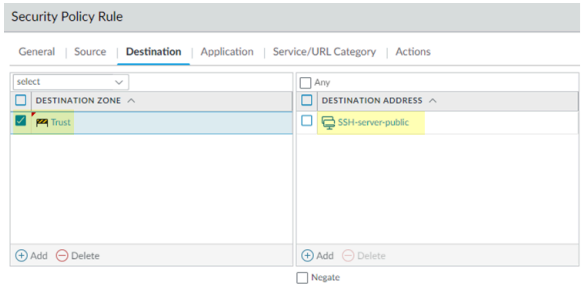
2. 選取 **Source**（來源）流量作為 **Untrust**（不信任）。



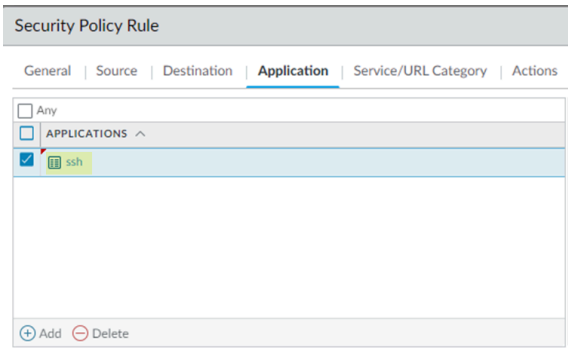

3. 透過選取目的地流量的 **Destination Zone**（目的地區域）作為 **Trust**（信任），並指定 **Destination Address**（目的地位址）為 **SSH-server-public**，來建立一個允許 SSH 伺服器


©2025 Palo Alto Networks, Inc.

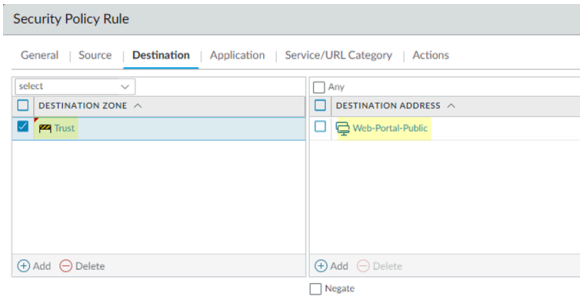
流量的政策。這是您建立的位址或位址群組物件，其中有一個清單，列出用於 SSH 登入的所有公用 IP 位址。




4. 選取 **Application**（應用程式）為 **ssh**。

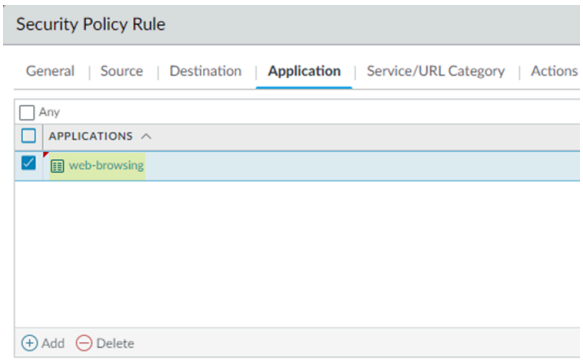



5. 選取 **Service/URL Category**（服務/**URL** 類別）為 **application-default**，以根據 Palo Alto Networks 定義的預設連接埠，允許或拒絕應用程式。
6. 在 **Actions**（動作）中，選取 **Allow**（允許）。
7. 按一下 **OK**（確定）儲存原則。
8. 建立一個政策以允許 Web 入口網站存取，方法是在先前的步驟中建立一個政策，但取代 **Destination**（目的地）和 **Application**（應用程式）頁籤中的下列設定：
   - 選取位址或位址群組的 **Destination Address**（目的地位址）為 **Web-Portal-Public**，其中包含 Web 入口網站的所有公用 IP 位址。



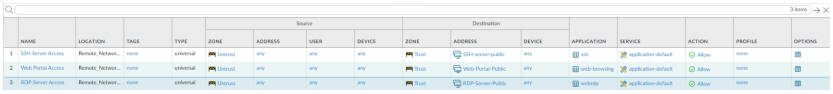

   - 選取 **Application**（應用程式）為 **web-browsing**。


©2025 Palo Alto Networks, Inc.




9. 建立一個安全性政策進行 RDP 伺服器存取，進而使用您對其他政策使用的同一設定，但建立稱為 **RDP-Server-Public**（其中包含 RD P 伺服器的公用 IP 位址） 的位址或位址群組物件作為 **Destination Address**（目的地位址），以及建立 **webrdp** 作為 **Application**（應用程式）。

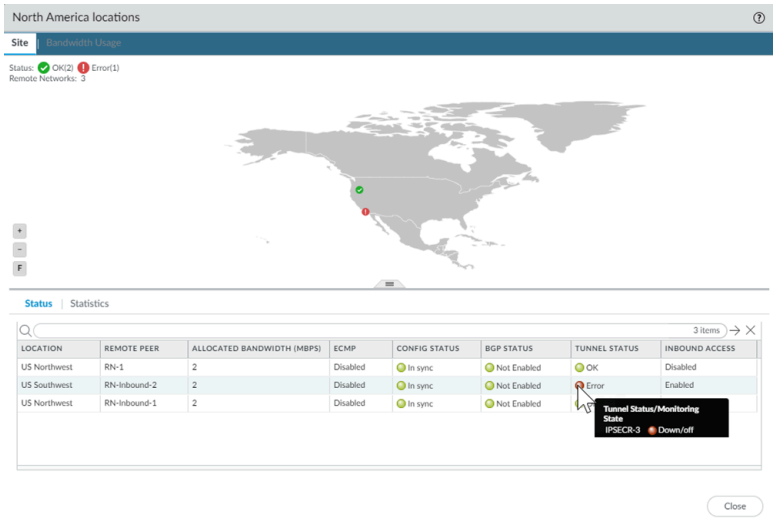
   完成時，您有三個不同的政策，允許 SSH 伺服器存取、Web 入口網站存取和 RDP 伺服器存取。



**STEP 8 |** **Save**（儲存）並 **Commit**（提交）您的變更。

**STEP 9 |** 檢查遠端網路連線是否正常運作，並正確處理輸入流量。

1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > > **Status**（狀態） > **Remote Networks**（遠端網路），然後將游標暫留在 **Status**（狀態）和 **Config Status**（設定狀態）區域上，以查看通道的狀態。
2. 如果發現問題，請選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > > **Monitor**（監控） > **Remote Networks**（遠端網路）、在地圖中選取遠端網路通道的位置，然後將游標暫留在 **Tunnel Status**（通道狀態）區域上，以確定錯誤的原因。




 ©2025 Palo Alto Networks, Inc.

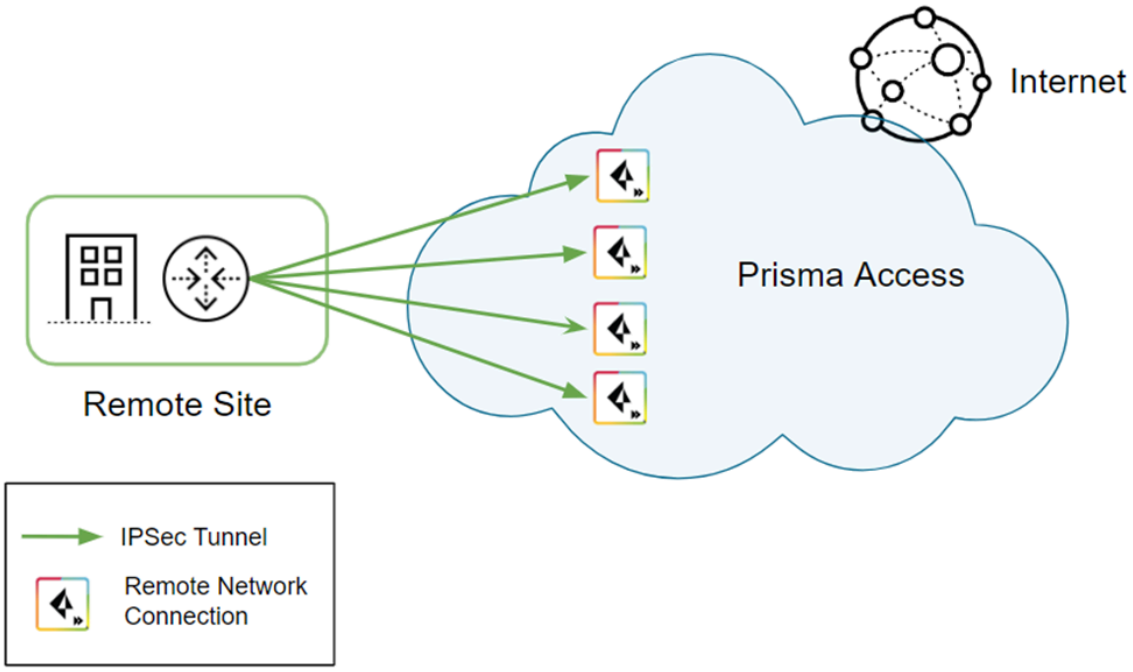
# 為遠端網站建立高頻寬網路

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

如果您想要保護分公司或網站透過 Prisma Access 的高頻寬連線進行輸出網際網路存取，您可以完成本節中的步驟，使用多個 IPSec 通道對來自分公司或網站的流量進行負載平衡。

下圖顯示了使用相同遠端網站的四個遠端網路連線。在裝載之前，將 4 Gbps (4000 Mbps) 指派給計算位置，在本範例中，此計算位置為韓國，對應至遠端網站。4000 Mbps 提供 4 個 IPSec 終止節點，每個 IPSec 終止節點最多提供 1000 Mbps 的頻寬。在裝載過程中為每個遠端網路連線指派自己的 IPSec 終止節點，以利用完整的頻寬。

此範例顯示四個通道。您可以在 *Prisma Access* 用於高頻寬連線的通道數上限基於用戶端周邊設備 *(CPE)* 透過您使用的負載平衡通訊協定支援的 *IPSec* 通道數上限。




在部署此設定之前請考慮以下限制和建議：

- 將 BGP 路由用於 IPSec 通道；不支援靜態路由。
- 僅將此設定用於輸出網際網路存取。
- 請勿在 Prisma Access 或 CPE 上使用通道監控。IPSec 通道的可用性是由 CPE 與 Prisma Access 遠端網路之間的 BGP 對等所決定。如果 IPSec 通道失效且 BGP 連線中斷，則在該通道上透過 BGP 得知的路由會自動從 ECMP 中移除。
- 因為您使用 BGP 來確定通道何時失效，所以請考慮您在 CPE 上設定的 HoldTime 值。保留計時器確定移除路由之前通道失效的時間量。Prisma Access 使用 RFC 4271 定義的預設 BGP HoldTime 值 90 秒。如果為遠端網站中的 BGP CPE 設定較低的保留時間，BGP 會使用較


©2025 Palo Alto Networks, Inc.

低的保留時間值。Palo Alto Networks 建議進行此部署時 CPE 的 KeepAlive 值為 10 秒，其 HoldTime 值為 30 秒。

若要建立高頻寬遠端網路連線，請完成以下工作。


©2025 Palo Alto Networks, Inc.

**STEP 1 |** 在 Panorama 中，設定 Prisma Access 遠端網路通道。

1. （選用）如果您還沒有這樣做，請為您建立的遠端網路連線設定 IKE 閘道、IKE 加密 和 IPSec 密碼設定檔，以及 IPSec 通道。

   記下 IKE 和 IPSec 密碼設定檔；您可以在用來終止遠端網路位置中遠端網路連線的 CPE 上指定相同的設定。

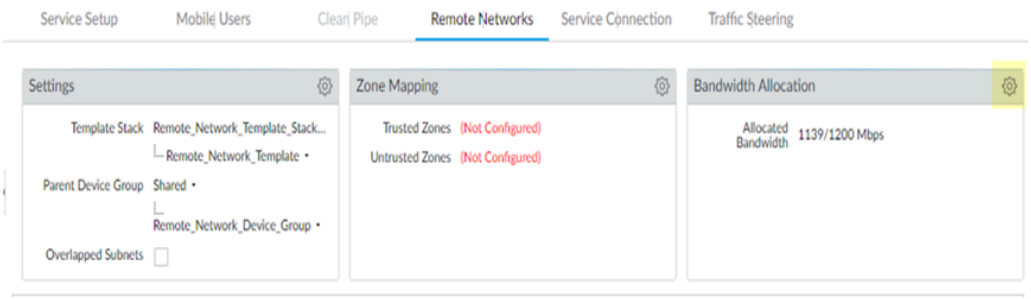
2. 確定您具有的遠端網路部署類型。

   Prisma Access 部署透過根據每個計算位置配置頻寬或依位置配置頻寬來配置頻寬。

3. 裝載遠端網路。

   - 若要裝載依計算位置配置頻寬的遠端網路：

     1. 按一下 **Bandwidth Allocation**（頻寬配置）區域中的齒輪圖示，為您想要裝載的位置配置頻寬。

     2. 為與您要裝載的 **Prisma Access Locations**（位置）相關聯的每個 **Compute Location**（計算位置）輸入您想要的 **Bandwidth Allocation**（頻寬配置）。
     3. 等待頻寬反映在頁面頂部的 **Allocated Total**（已配置總數）欄位中；然後按一下 **OK**（確定）。

   - 若要裝載依位置配置頻寬的遠端網絡，請繼續下一個步驟；您在遠端網路裝載期間配置頻寬。

4. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Remote Networks**（遠端網路），並建立四個遠端網路連線，指定以下設定：

   - 為每個連線選擇相同的 **Location**（位置）。
   - 選取 **IPSec Termination Node**（IPSec 終止節點）。

     為每個遠端網路連線選取個別的 IPSec 終止節點。

     如果您有一個部署，依位置配置頻寬，請選取 ***500 Mbps***的 ***Bandwidth***（頻寬）。

     您選取的頻寬不能超過您已授權的頻寬總量。使用此設定可以定義要配置給此位置的授權頻寬總量。

   - **Enable**（啟用） BGP、**Advertise Default Route**（公告預設路由），且 **Don't Advertise Prisma Access Routes**（不要公告 **Prisma Access** 路由）。
   - 為所有遠端網路連線指定相同的 **Peer AS**（對等 **AS**）。

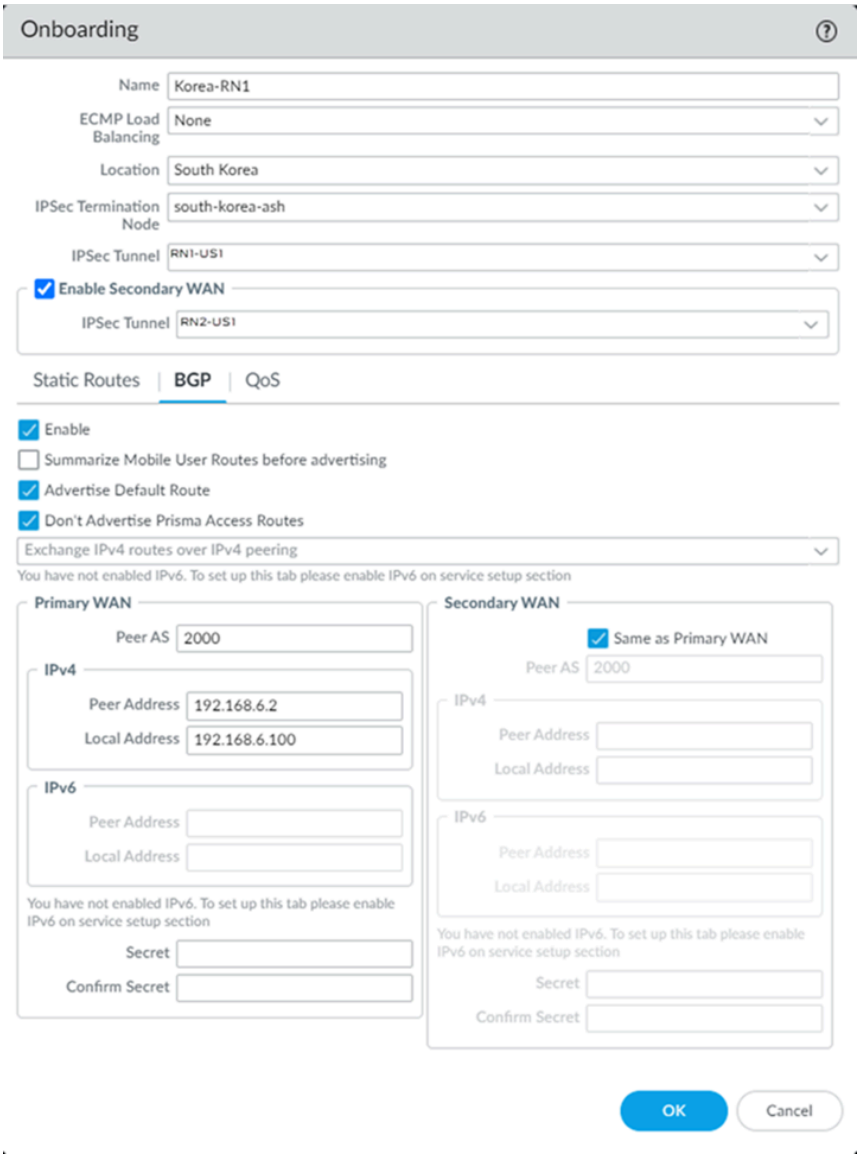

©2025 Palo Alto Networks, Inc.

此範例顯示 **Peer AS**（對等 **AS**）為 2000；在此範例中，您為所有四個連線選取 2000 的 對等 **AS**。

- （選用）如果您想要建立備份遠端網路，請選取 **Enable Secondary WAN**（啟用次要 **WAN**）建立一個；然後，選取您為備份通道建立的 **IPSec Tunnel**（**IPSec** 通道）。

以下部署不支援設定次要 WAN：

- 如果您的次要 WAN 與主要 IPSec 通道設定為主動-主動模式。
- 如果您的用戶端裝置 (CPE) 在具有主要和次要 IPSec 通道的等價多路徑 (ECMP) 設定中設定。

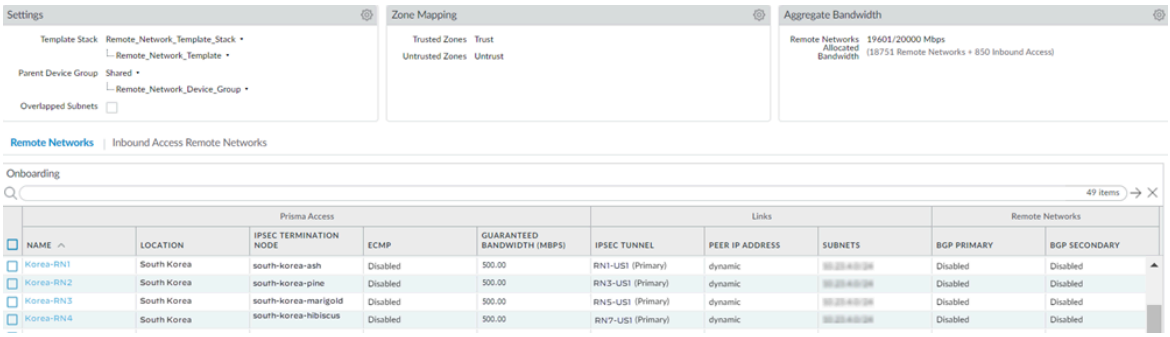



完成時，您會在同一位置具有四個 1000 Mbps 遠端網路連線。

由於依位置配置頻寬的部署最多可有 500 Mbps 的頻寬，因此這個設定將為您提供每個位置 500 Mbps。

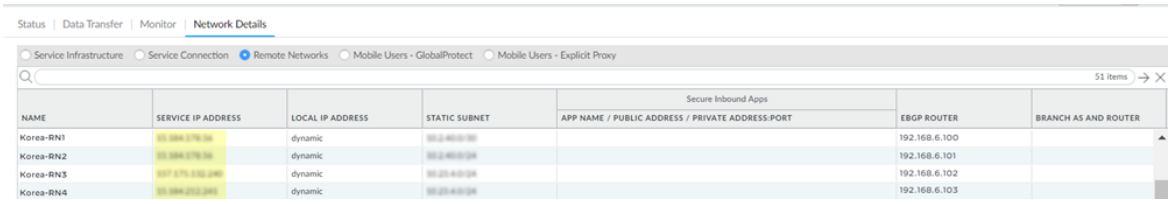
如果您設定了備份通道，則還有四個次要通道用於容錯移轉目的。


©2025 Palo Alto Networks, Inc.




5. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Remote Networks**（網路詳細資料） > **Remote Networks**（遠端網路），並記下 **Service IP Address**（服務 **IP** 位址）和 **EBGP Router**（**EBGP** 路由器）位址。

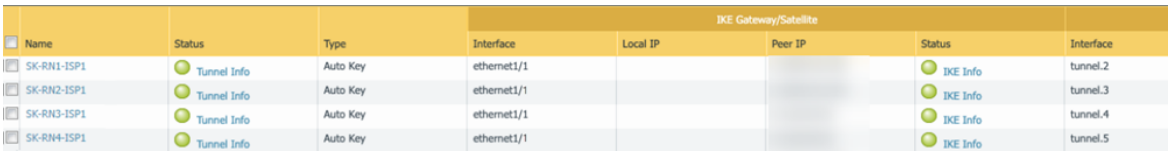
   您會在遠端網站中 CPE 上設定 IPSec 通道時使用 **Service IP Address**（服務 **IP** 位址）作為對等 IP 位址，並在 CPE 上建立靜態路由時使用這些位址和 **EBGP Router**（**EBGP** 路由器）位址。



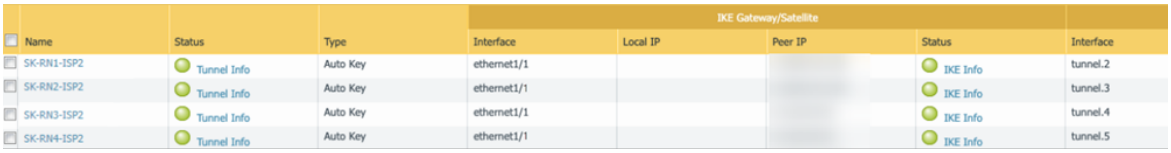

**STEP 2 |** 在遠端網站的 CPE 上，設定遠端網路通道。

- 這些步驟中的設定會使用 *Palo Alto Networks* 新世代防火牆；您可以使用任何支援 *IPSec* 通道和 *ECMP* 的 *CPE* 裝置進行此部署。
- 頻寬平衡取決於 *ECMP* 的 *CPE* 雜湊。不過，*Prisma Access* 確保流量的對稱傳回。

1. 建立四個作用中通道，從作用中 CPE 到四個網路連線的每一個。對於 **Peer IP**（對等 **IP**）位址，輸入您在上一個步驟從 Prisma Access 收到的遠端網路的 **Service IP Address**（服務 **IP** 位址）。



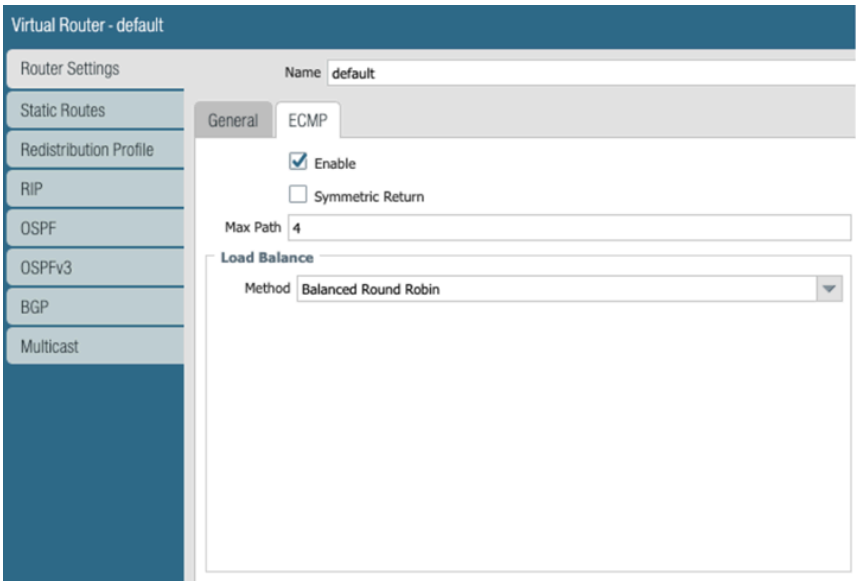

2. （選用）如果您建立備份通道，請建立它們，從作用中 CPE 到四個網路連線的每一個。對於 **Peer IP**（對等 **IP**）位址，輸入您在上一個步驟從 Prisma Access 收到的遠端網路的 **Service IP Address**（服務 **IP** 位址）。




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** 在遠端網站的 CPE 上設定 ECMP。

1. 選取 **Network**（網路） > **Virtual Routers**（虛擬路由器）。
2. 選取 **default**（預設）虛擬路由器，或 **Add**（新增）虛擬路由器。
3. 選取 **Router Settings**（路由器設定） > **Enable**（啟用） > **ECMP**，然後 **Enable**（啟用）ECMP，其中 **Max Path**（最大路徑）為 **4**，而負載平衡 **Method**（方法）為 **Balanced Round Robin**（平衡循環配置資源）。

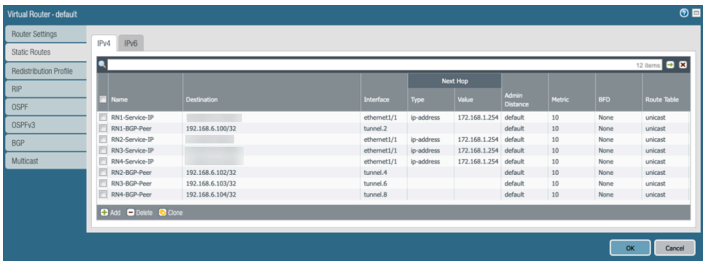



**STEP 4 |** 在遠端網站的 CPE 上，建立 Prisma Access **Service IP Address**（服務 **IP** 位址）的靜態路由，以及您在上一個步驟中擷取的 **EBGP Router**（**EBGP** 路由器）IP 位址。

如前所述，此設定需要使用 BGP 進行動態路由。若要促進 CPE 與 Prisma Access eBGP 路由器之間的 BGP 連線，您需要在 CPE 上為 eBGP 路由器 IP 位址新增靜態路由，而且下一個躍點必須是 CPE 上的通道介面。您必須對剩餘通道上的所有其他遠端網路 eBGP 路由器 IP 位址重複此步驟。

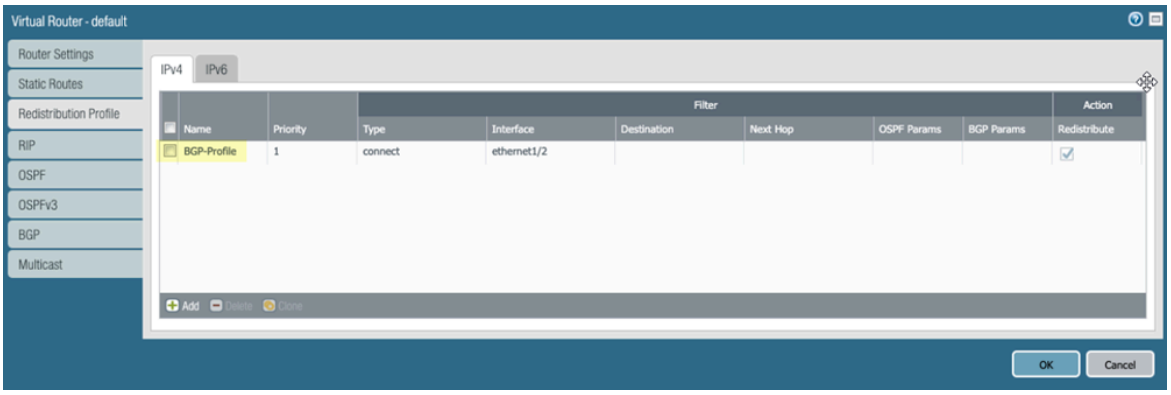
下列範例顯示作用中 CPE 上的路由。如果已在次要 CPE 上建立備份通道，請在次要 CPE 上建立相同的路由。

如果您要設定 Palo Alto Networks 新世代防火牆，請選取 **Static Routes**（靜態路由） > **IPv4** 以新增靜態路由。

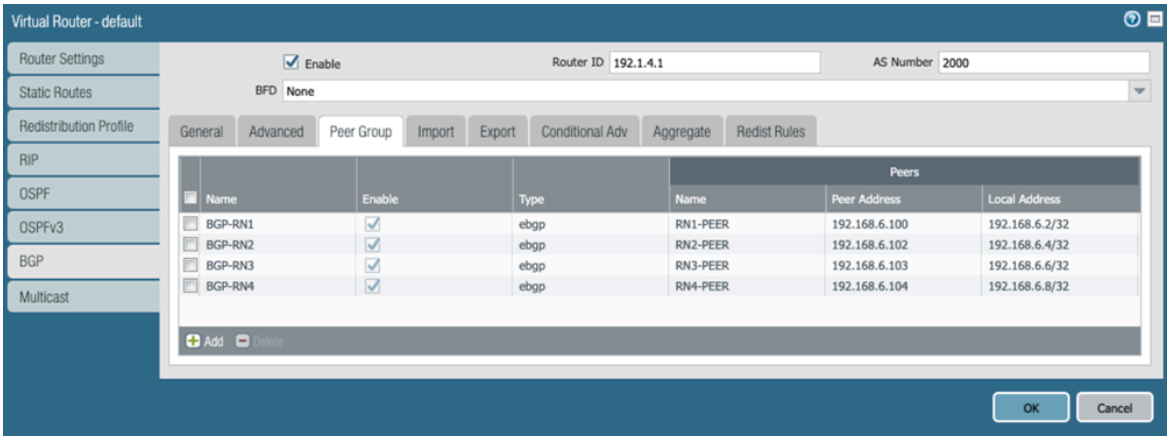


 ©2025 Palo Alto Networks, Inc.

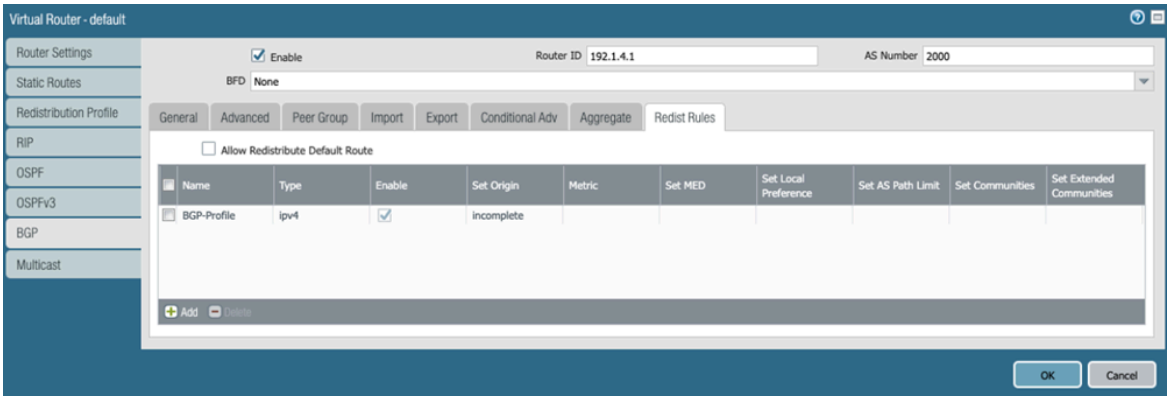
**STEP 5 |** 在 CPE 上啟用 路由重新散佈，方法是選取 **Redistribution Profile**（重新散佈設定檔） > **IPv4**，然後 **Add**（新增）IPv4 路由重新散佈設定檔。




**STEP 6 |** 選取 **BGP** > **Peer Group**（對等群組）、在虛擬路由器執行個體上 **Enable**（啟用）BGP，然後 **Add**（新增）遠端網路 BGP 對等。




**STEP 7 |** 選取 **BGP** > **Redist Rules**（重新散佈規則），然後附加您在上一個步驟中建立的路由重新散佈設定檔。



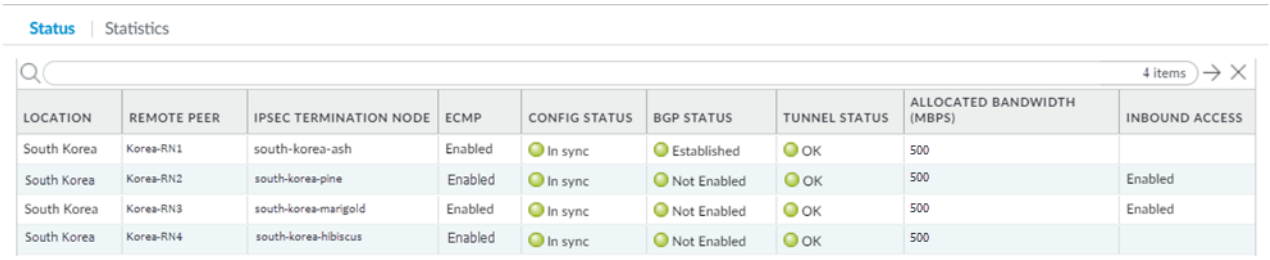

**STEP 8 |** 驗證 CPE 是否正在其所有四個通道上傳遞流量。

 ©2025 Palo Alto Networks, Inc.

**STEP 9 |** 檢查來自 Prisma Access 已啟用 ECMP 的連線狀態。

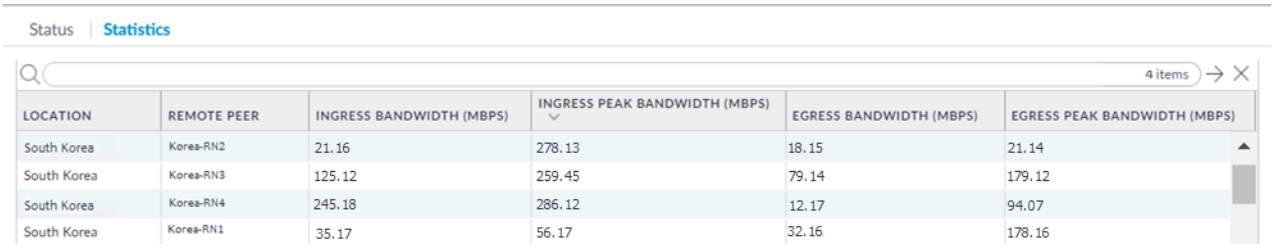
- 選取 **Panorama** > **Cloud Services**（雲端服務） > **Monitor**（監控） > **Remote Networks**（遠端網路）、選取您已部署 ECMP 連線的區域，然後選取 **Status**（狀態）。

  - 在此區域中，***ECMP*** 顯示為 ***No***（否）。這是預期的，因為您沒有設定 *Prisma Access*ECMP 負載平衡功能。
  - *ECMP* 的方向是從 *CPE* 到 *Prisma Access*，且 *Prisma Access* 確保從 *CPE* 對稱傳回流量。




| LOCATION | REMOTE PEER | IPSEC TERMINATION NODE | ECMP | CONFIG STATUS | BGP STATUS | TUNNEL STATUS | ALLOCATED BANDWIDTH (MBPS) | INBOUND ACCESS |
|---|---|---|---|---|---|---|---|---|
| South Korea | Korea-RN1 | south-korea-ash | Enabled | In sync | Established | OK | 500 | |
| South Korea | Korea-RN2 | south-korea-pine | Enabled | In sync | Not Enabled | OK | 500 | Enabled |
| South Korea | Korea-RN3 | south-korea-marigold | Enabled | In sync | Not Enabled | OK | 500 | Enabled |
| South Korea | Korea-RN4 | south-korea-hibiscus | Enabled | In sync | Not Enabled | OK | 500 | |

- 選取 **Statistics**（統計資料），以查看正在通過每個遠端網路通道的流量。




| LOCATION | REMOTE PEER | INGRESS BANDWIDTH (MBPS) | INGRESS PEAK BANDWIDTH (MBPS) | EGRESS BANDWIDTH (MBPS) | EGRESS PEAK BANDWIDTH (MBPS) |
|---|---|---|---|---|---|
| South Korea | Korea-RN2 | 21.16 | 278.13 | 18.15 | 21.14 |
| South Korea | Korea-RN3 | 125.12 | 259.45 | 79.14 | 179.12 |
| South Korea | Korea-RN4 | 245.18 | 286.12 | 12.17 | 94.07 |
| South Korea | Korea-RN1 | 35.17 | 56.17 | 32.16 | 178.16 |

完成此工作流程時，您已為遠端網路建立高頻寬設定。請記住，僅輸出流量支援此解決方案。


©2025 Palo Alto Networks, Inc.

# Prisma Access for Clean Pipe

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

使用 *Prisma Access for Clean Pipe*，以快速且輕鬆地設定全新輸出網際網路連線的多個執行個體。

*Prisma Access (Managed by Strata Cloud Manager)* 不支援這樣做。

# Prisma Access for Clean Pipe 概要

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

為了允許管理其他組織（例如服務提供者、MSSP 或 Telcos）的 IT 基礎結構的組織快速且輕鬆地保護其租用戶的輸出網際網路流量，Palo Alto Networks 提供了 Prisma Access for Clean Pipe。服務提供者、MSSP 或 Telco 可以使用使用合作夥伴互連，將其客戶（設定為租用戶）路由至 Prisma Access for Clean Pipe。在流量跨過合作夥伴互連之後，其將被傳送到租用戶專用的 Clean Pipe 執行個體以確保安全，然後路由到網際網路。

Prisma Access for Clean Pipe 還提供了一個 API，您可以使用它，快速且輕鬆地為租用戶建立 Clean Pipe。

## Clean Pipe 使用案例

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

如果您符合以下所有使用案例，请使用 Prisma Access for Clean Pipe。

- 您管理一個具有大量租用戶的網路部署。

  例如，您是服務提供者、Telco 或 MSSP，管理並維護許多不同組織（高達數萬個）的網路。
- 您想要一種方法，讓部署中的每個租用戶保護其輸出網際網路流量。
- 您需要一種快速且可調整的方法，為您管理其網路的組織裝載 Clean Pipes。
- 除了輸出網際網路安全性外，您沒有額外需求，以保護您所管理網路的行動使用者、總部或分支位置。

  如果您有額外的安全性需求，我們建議在 Prisma Access 中建立多個租用戶，而不是實作 Clean Pipe，這樣可讓您為不同的遠端網路和行動使用者群組建立並強制執行安全性設定檔。

## Clean Pipe 範例

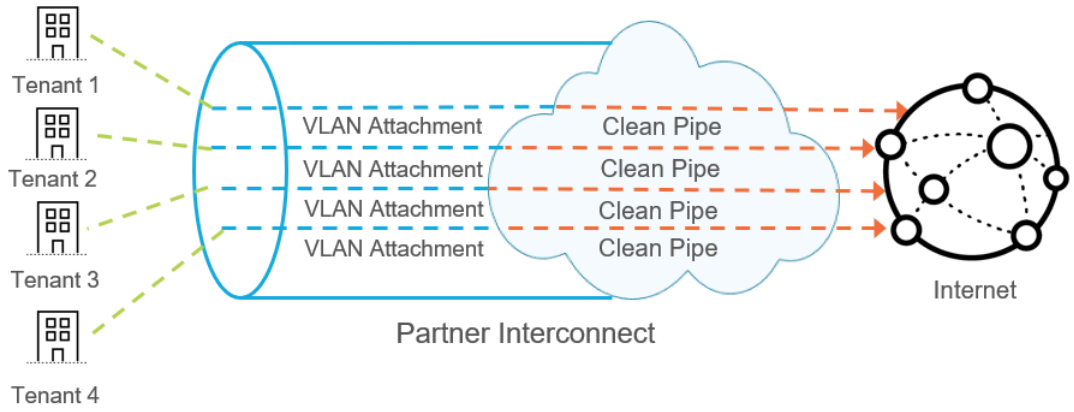
| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

下圖為單一租用戶提供 Clean Pipe 設定的範例，其中租用戶具有多 Clean Pipe 設定。

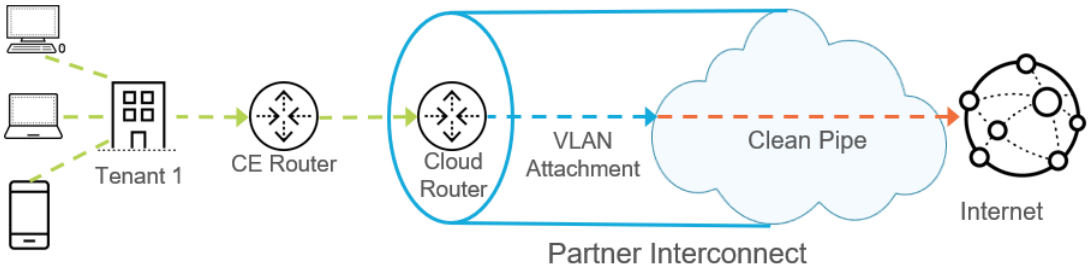
在此範例中，服務提供者管理四個組織的網際網路連線，並想要保護它們免於輸出網際網路存取。服務提供者建立 Google Cloud Platform (GCP) 合作夥伴互連，並為每個租用戶建立 VLAN 連線。服務提供者使用 Panorama 設定 Prisma Access for Clean Pipe，為 VLAN 附件建立安全性。


©2025 Palo Alto Networks, Inc.

此範例顯示每個租用戶都有單一 Clean Pipe。您也可以在單一租用戶中建立多個 Clean Pipe。確保您為租用戶指定的每個 Clean Pipe 使用不同的位置。




下圖為想要全新連線至網際網路的租用戶更詳細地顯示了單一 Clean Pipe。客戶邊緣 (CE) 路由器為租用戶提供 WAN 連線。CE 路由器連線到雲端路由器，而雲端路由器為合作夥伴互連提供連線。服務提供者為租用戶建立 VLAN 連線，並在 Panorama 中設定 Prisma Access for Clean Pipe，為 VLAN 附件提供安全性，從而保護租用戶的網際網路型流量。




## Clean Pipe 和合作夥伴互連需求

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access 授權 |

開始之前，請注意以下 Clean Pipe 部署需求，並注意 Prisma Access for Clean Pipe 與其他 Prisma Access 部署之間的以下差異：

- 您必須具有 Prisma Access for Clean Pipe 授權。

  Prisma Access for Clean Pipe 授權是與其他 Prisma Access 產品分開的授權。不過，購買和安裝 Panorama 與 Strata Logging Service 授權的相同需求也適用於 Clean Pipe。


©2025 Palo Alto Networks, Inc.

- Prisma Access for Clean Pipe 具有以下 GCP 合作夥伴互連需求：
  - 您必須能夠在 GCP 中建立合作夥伴互連。
  - 您必須具備在 GCP 中建立 VLAN 附件的能力。
  - 對於第二層 (L2) 合作夥伴互連，您必須有權存取 MSSP 端上的客戶邊緣 (CE) 路由器，並能夠對其進行設定變更。

  如需 GCP 設定的詳細資訊，請參閱 GCP 文件。
- 請注意 Clean Pipe 部署的最低頻寬需求。

  您可以購買的最低授權為 1000 Mbps。每個 Clean Pipe 租用戶的最低頻寬配置為 100 Mbps。

  在建立租用戶之後，您可以在該租用戶中建立 Clean Pipe。每個 Clean Pipe 必須至少有 100 Mbps。每個 Clean Pipe 共用租用戶的存取網域、範本、範本堆疊和裝置群組。
- 如果為單一租用戶設定多個 Clean Pipe，每個 Clean Pipe 都必須是唯一的位置。如果您想要在作用中/備份設定中為單一 Clean Pipe 位置設定兩個 VLAN 附件，以進行區域內備援，請在新增 Clean Pipe 執行個體時指定e **REDUNDANT**（備援）選項。
- 在 Clean Pipe 租用戶內建立連線時，將頻寬配置與 VLAN 附件的頻寬配置相符。請勿建立頻寬高於或低於連線頻寬的 VLAN 附件。
- 啟用多租用戶後，請勿使用設定區域中的任何其他頁籤設定您的 Clean Pipe 部署，但 **Service Setup**（服務設定）頁籤中的 **Generate API key**（產生 **API** 金鑰）連結除外，該連結可讓您產生 API 金鑰以擷取 Clean Pipe IP 位址。所有設定對於 Prisma Access for Clean Pipe 都是唯一的，並與其他 Prisma Access 部署（例如 Prisma Access for Networks 或 Prisma Access for Users）分開。
- 在提交 Clean Pipe 設定之後，請勿對其進行變更。如果您在提交之後變更 Clean Pipe，則在重新提交時會收到提交錯誤。相反，刪除現有的 Clean Pipe 並新增一個。在系統停機期間排程此變更。如果您已進行變更但尚未提交，則可以透過將 Clean Pipe 設定編輯回其先前的值來還原這些變更。

 ©2025 Palo Alto Networks, Inc.

- 請注意，Clean Pipe 使用的位置與其他 Prisma Access 部署不同。Prisma Access for Clean Pipe 支援以下位置：
  - asia-east1
  - asia-east2
  - asia-northeast1
  - asia-south1
  - asia-southeast1
  - australia-southeast1
  - europe-north1
  - europe-west2
  - europe-west3
  - europe-west4
  - northamerica-northeast1
  - southamerica-east1
  - us-central1
  - us-east1
  - us-east4
  - us-west1
  - us-west2
- 請注意 Clean Pipe 的以下網路限制：
  - 僅在進入時支援 QoS for Clean Pipe（從網際網路到 Clean Pipe 方向）。
  - 不支援 User-ID。
  - Clean Pipe 支援基於來源和目的地 IP 位址的工作階段親和性，並且不可設定。
  - 信任到信任政策對於 Clean Pipe 是無效的，因為流量始終繫結網際網路。僅使用信任到不信任政策。


©2025 Palo Alto Networks, Inc.

# 完成 Clean Pipe 設定

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

若要完成 Prisma Access for Clean Pipe 的設定，您可以在合作夥伴互連和 Panorama 中執行設定。

確保您可以在合作夥伴互連的合作夥伴互連（非 *Prisma Access*）端上存取和設定 *CE* 與雲端路由器。

**STEP 1 |** 在設定的合作夥伴互連端，使用您從 Panorama 擷取的 **Pairing Key**（配對金鑰）建立 VLAN 附件。

如需使用合作夥伴互連建立 VLAN 附件，以及設定客戶邊緣 (CE) 路由器以與雲端路由器通訊的詳細資訊，請參閱 Google Cloud 文件，網址為 https://cloud.google.com/interconnect/docs/

確保您選取的位置和頻寬與您在 Panorama 中指定的 **Location**（位置）相符。您用於合作夥伴互連的服務提供者會使用配對金鑰，以及您要求的連線位置和容量來完成 VLAN 附件的設定。

**STEP 2 |** 在連線啟動之後，返回 Panorama、選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Network Details**（網路詳細資訊） > **Clean Pipe**，並記下 **MSSP CE** 和 **Cloud Router IP**（雲端路由器 **IP**）位址。

在您於 VLAN 附件的另一端上輸入 **Pairing Key**（配對金鑰）時，就會填入這些值。




**STEP 3 |** 登入 CE 路由器並執行以下設定。

1. 輸入 **MSSP CE** 位址作為本機 IP 位址。
2. 輸入 **Cloud Router IP**（雲端路由器 **IP**）位址作為對等 IP 位址。
3. 輸入一個 BGP ASN，與您在 Panorama 時設定 Clean Pipe 時輸入的 **BGP Peer ASN**（**BGP** 對等 **ASN**）相符。

   確保您正確輸入這些值；您無法變更它們。

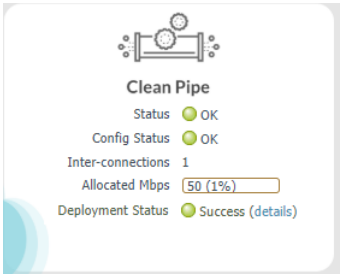

©2025 Palo Alto Networks, Inc.

**STEP 4 |** 檢查 Clean Pipe 狀態。

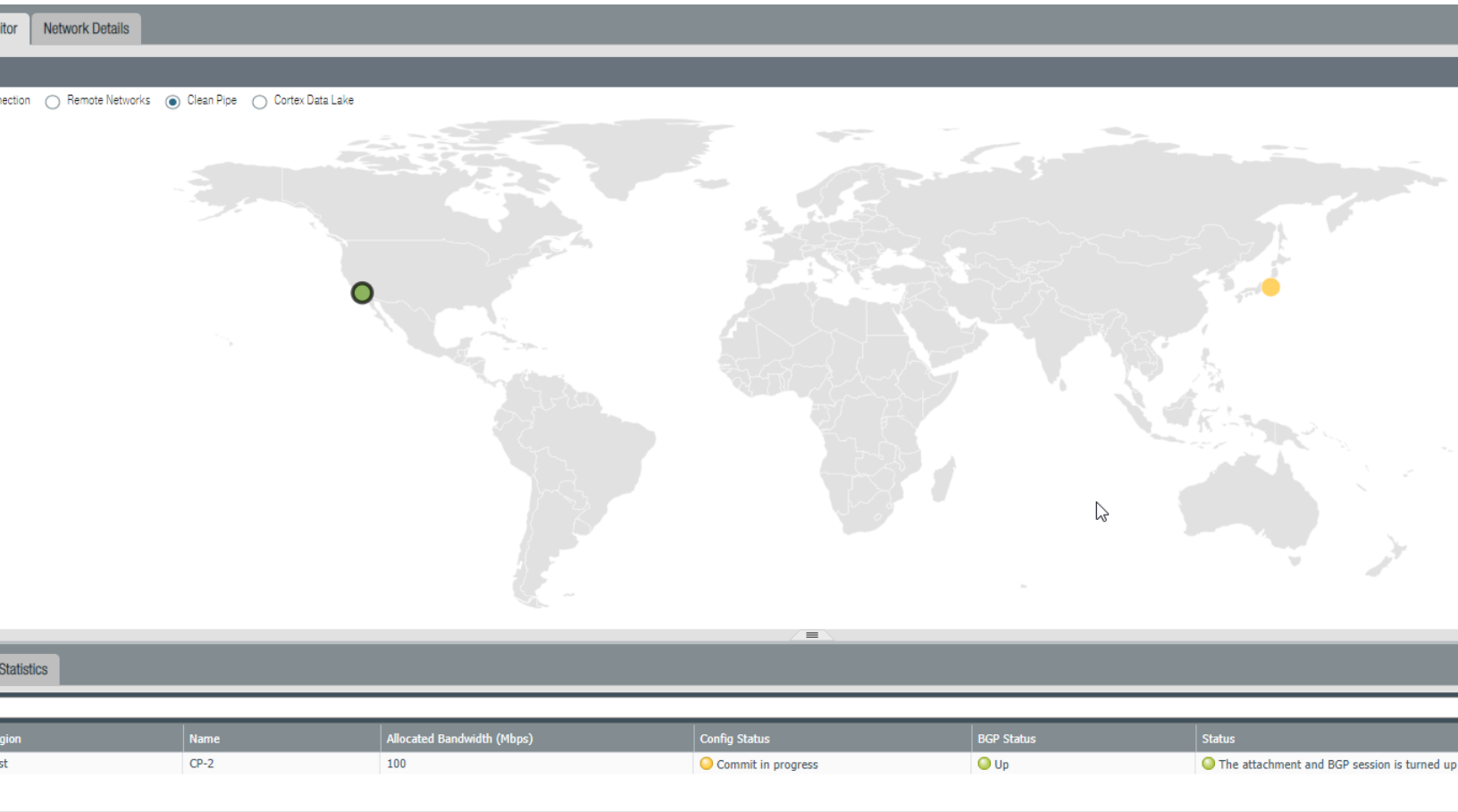
1. 在 Panorama 中，選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態）、從下拉式清單中選取 **Tenant**（租用戶），然後檢查 Clean Pipe 的 **Status**（狀態）。

   請參閱 Prisma Access 位置清單，以取得可接受的值。

   **Deployment Status**（部署狀態）區域允許您在完成裝載和部署工作之前檢視其進度，以及查看有關已完成工作狀態的詳細資訊。如需詳細資訊，請參閱部署進度和狀態。




2. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態） > **Clean Pipe**，然後按一下 **Monitor**（監控）頁籤，以查看與所部署 Clean Pipes 狀態的對應。




按一下對應下方的頁籤，以查看 Clean Pipes 的其他統計資料。

**Status**（狀態）頁籤：

 ©2025 Palo Alto Networks, Inc.

- **Compute Region**（計算區域）—為 Clean Pipe 執行個體部署雲端服務基礎結構的計算區域。
- **Name**（名稱）—Clean Pipe 執行個體的名稱。
- **Allocated Bandwidth (Mbps)**（已配置頻寬 **(Mbps)**）—您為 Clean Pipe 執行個體配置的頻寬量。
- **Config Status**（設定狀態）—上次推送設定到服務的狀態。如果您已在本機進行了變更，但尚未將設定推送至雲端，則狀態會顯示 **Out of sync**（不同步）。將游標暫留在狀態指示器上，以取得更多的詳細資訊。在提交並推送設定至 Prisma Access 之後，設定狀態會變更為 **In sync**（同步）。
- **BGP Status**（**BGP** 狀態）—顯示有關 Clean Pipe 執行個體上防火牆或路由器與 Prisma Access 之間的 BGP 狀態的詳細資訊。雖然您可能會通過各種 BGP 狀態（**idle**（閒置）、**active**（作用中）、**open send**（開啟傳送）、**open pend**（開啟擱置）、**open confirm**（開啟確認））暫時看到狀態，但 BGP 狀態最常顯示：
  - **Connect**（連線）—Clean Pipe 執行個體上的路由器正在嘗試與雲端防火牆建立 BGP 對等關係。


©2025 Palo Alto Networks, Inc.

- **Established**（已建立）—已建立 BGP 對等關係。

  此欄位還將顯示 BGP 連線是否處於錯誤狀態：

- **Warning**（警告）—超過 8 分鐘未更新 BGP 狀態。這可能表示防火牆中斷。
- **Error**（錯誤）—BGP 狀態未知。

- **Status**（狀態）—Prisma Access 與 Clean Pipe 之間連線的操作狀態。

**Statistics**（統計資料）頁籤：

- **Region**（區域）—為 Clean Pipe 執行個體部署雲端服務基礎結構的區域。
- **Name**（名稱）—Clean Pipe 執行個體的名稱。
- **Allocated Bandwidth (Mbps)**（已配置頻寬 **(Mbps)**）—您為遠端網路位置配置的頻寬量。
- **QoS**— 選取 **QoS** 以顯示包含圖形 QoS 統計資料的頁面。
- **Avg Egress Bandwidth 5 Min (Mbps)**（**5** 分鐘平均輸出頻寬 **(Mbps)**）—5 分鐘內平均的 Clean Pipe 輸出頻寬量。
- **Avg Egress Bandwidth 60 Min (Mbps)**（**60** 分鐘平均輸出頻寬 **(Mbps)**）—60 分鐘內平均的 Clean Pipe 輸出頻寬量。
- **Avg Ingress Bandwidth 5 Min (Mbps)**（**5** 分鐘平均進入頻寬 **(Mbps)**）—5 分鐘內平均的 Clean Pipe 進入頻寬量。
- **Avg Ingress Bandwidth 60 Min (Mbps)**（**60** 分鐘平均進入頻寬 **(Mbps)**）—60 分鐘內平均的 Clean Pipe 進入頻寬量。
- **Egress Peak Bandwidth 1 Hour (Mbps)**（**1** 小時輸出峰值頻寬 **(Mbps)**）—過去 1 小時 Clean Pipe 執行個體的峰值輸出頻寬量。
- **Egress Peak Bandwidth 24 Hour (Mbps)**（**24** 小時輸出峰值頻寬 **(Mbps)**）—過去 24 小時 Clean Pipe 執行個體的峰值輸出頻寬量。
- **Egress Peak Bandwidth 7 Days (Mbps)**（**7** 天輸出峰值頻寬 **(Mbps)**）—過去 7 天 Clean Pipe 執行個體的峰值輸出頻寬量。
- **Egress Peak Bandwidth 30 Days (Mbps)**（**30** 天輸出峰值頻寬 **(Mbps)**）—過去 30 天 Clean Pipe 執行個體的峰值輸出頻寬量。
- **Ingress Peak Bandwidth 1 Hour (Mbps)**（**1** 小時進入峰值頻寬 **(Mbps)**）—過去 1 小時 Clean Pipe 執行個體的峰值進入頻寬量。
- **Ingress Peak Bandwidth 24 Hour (Mbps)**（**24** 小時進入峰值頻寬 **(Mbps)**）—過去 24 小時 Clean Pipe 執行個體的峰值進入頻寬量。
- **Ingress Peak Bandwidth 7 Days (Mbps)**（**7** 天進入峰值頻寬 **(Mbps)**）—過去 7 天 Clean Pipe 執行個體的峰值進入頻寬量。
- **Ingress Peak Bandwidth 30 Days (Mbps)**（**30** 天進入峰值頻寬 **(Mbps)**）—過去 30 天 Clean Pipe 執行個體的峰值進入頻寬量。

 ©2025 Palo Alto Networks, Inc.

# 啟用多租用戶並建立租用戶

| 我可以在哪裡使用這個？ | 我需要哪些內容？ |
| --- | --- |
| • Prisma Access (Managed by Panorama) | • Prisma Access 授權 |

若要開始 Clean Pipe 設定，請在 Panorama 中建立多租用戶部署並建立一個或多個租用戶。

**STEP 1 |** 安裝並啟動 Prisma Access for Clean Pipe。

Prisma Access for Clean Pipe 需要個別的授權，而啟動它會在雲端服務外掛程式中建立 Clean Pipe 特定的頁籤。您用來安裝 Prisma Access for Clean Pipe 的程序與您用來啟動並安裝 Prisma Access 授權的程序相同，包括安裝雲端服務外掛程式。

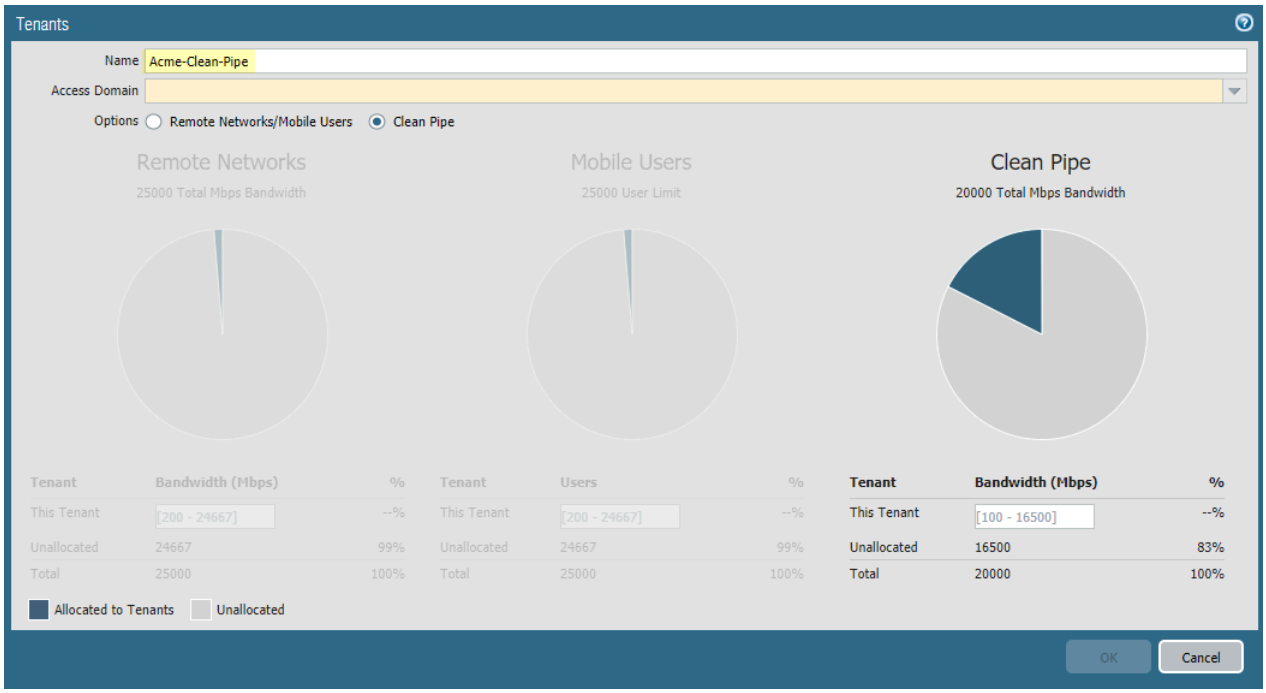
 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** 如果您尚未啟用多租用戶，請將其啟用。

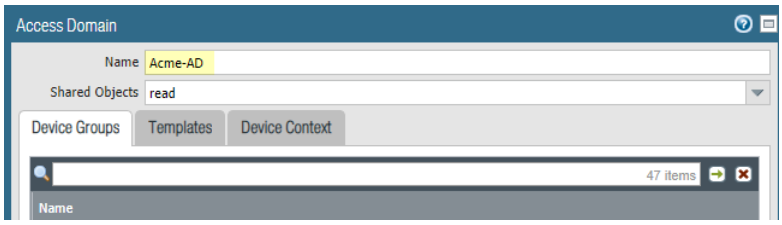
1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定）。
2. 選取 **Enable Multitenancy**（啟用多用租戶）（位於頁面右上角）。
3. 按一下 **OK**（確定）。

   即會顯示 **Tenants**（租用戶）頁面。
4. 在 **Options**（選項）區域中，選取 **Clean Pipe**。

   若要為遠端網路、行動使用者或兩者設定租用戶，請參閱「在 Prisma Access 中管理多個租用戶」。




5. 輸入第一個租用戶的 **Name**（名稱）。
6. 為第一個租用戶建立並設定新的 **Access Domain**（存取網域），然後按一下 **OK**（確定）。




7. 在 **Clean Pipe** 區域中，輸入 **This Tenant**（此租用戶）的 **Bandwidth (Mbps)**（頻寬 **(Mbps)**）。

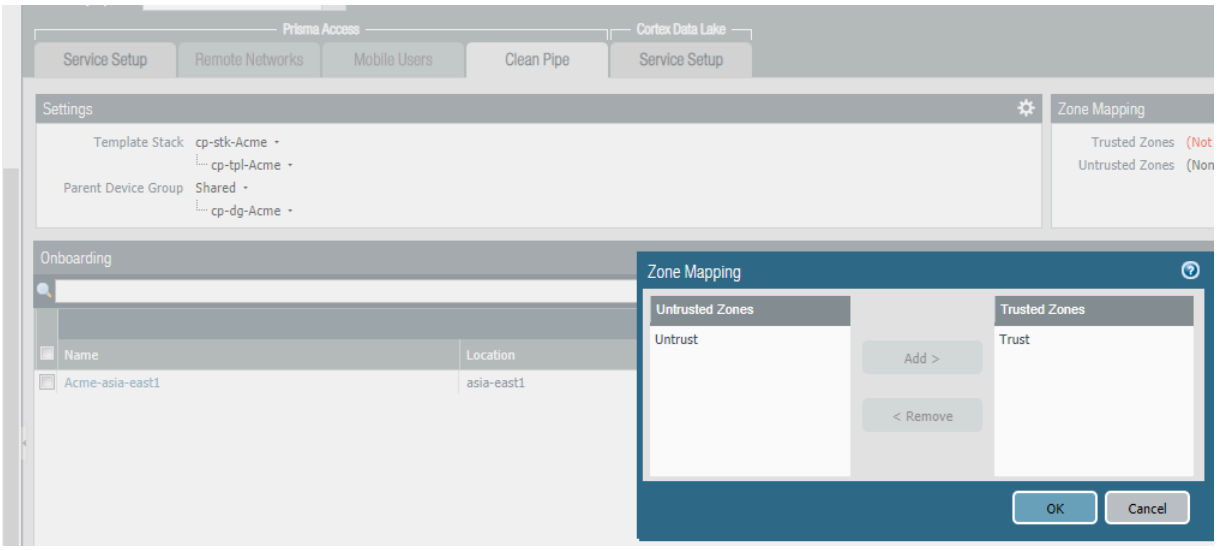
   為您建立的每個租用戶輸入至少 100 Mbps。
8. 按一下 **OK**（確定）。


©2025 Palo Alto Networks, Inc.

**STEP 3 |** 為租戶建立區域並為租用戶對應這些區域。

1. 選取 **Network**（網路） > **Zones**（區域）。

   確保為您建立的租用戶選取了 Clean Pipe **Template**（範本） (**cp-tpl-***tenant*)。
2. 為租用戶建立區域（例如 **Trust**（信任）和 **Untrust**（不信任））。
3. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定），並從下拉式清單中選取 **Tenant**（租用戶）。
4. 選取 **Clean Pipe** 頁籤。
5. 按一下 **Zone Mapping**（區域對應）旁邊的齒輪圖示以編輯設定。
6. **Add**（新增）和 **Remove**（移除）您建立的區域，以將它們對應到受信任和不受信任的區域。




**STEP 4 |** 裝載新的 Clean Pipe。

1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Configuration**（設定） > **Clean Pipe**。
2. 為租用戶 **Add**（新增）Clean Pipe 執行個體，輸入以下資訊：
   - **Name**（名稱）—指定 Clean Pipe 的名稱。
   - **Bandwidth**（頻寬）—選取要為 Clean Pipe 配置的頻寬。

     您可以採取 100 Mbps、200 Mbps、300 Mbps、400 Mbps、500 Mbps、1000 Mbps、2000 Mbps、5000 Mbps 和 10000 Mbps 的增量形式裝載 Clean Pipe 執行個

 ©2025 Palo Alto Networks, Inc.

體實例。您指定的頻寬量必須在授權的頻寬配置內，並且必須與您在合作夥伴互連中建立的 VLAN 附件頻寬相符。

- **Edge Availability Domain**（邊緣可用性網域）—為 Clean Pipe 選取您需要的可用性網域。您可以選擇 **1**、**2**、**ANY** 或 **REDUNDANT**。
  - 為非備援 Clean Pipe 部署指定 **ANY**。

    確保您的雲端提供者支援此選擇；您還必須在合作夥伴互連的雲端提供者端選取 **ANY**。如果該選擇不適用於您的雲端提供者，請做出其他選擇。
  - 若要在相同位置的作用中/備份設定中於相同位置指定兩個 VLAN 附件，請選取 **REDUNDANT**。

    Prisma Access 為 **REDUNDANT** 設定建立兩個配對金鑰（每個可用性區域一個），並為第一個可用性區域將 `zone1` 加在 Clean Pipe 名稱前面，而對於第二個可用性區域，則為 `zone2`。例如，如果您指定 **Name**（名稱）為 **San Francisco**（舊金山），Prisma Access 會建立兩個名為 **San Francisco-zone1** 和 **San Francisco-zone2** 的區域。

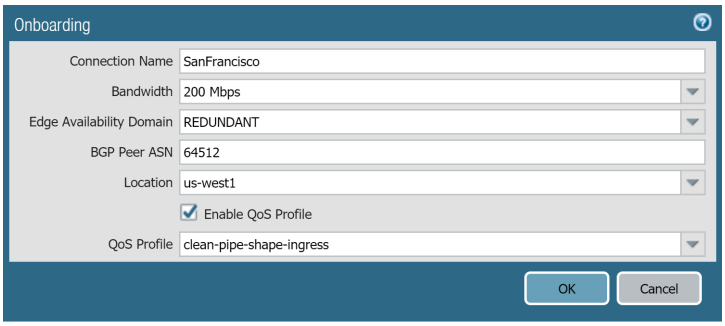
    確保將第一個可用性區域 *(zone1)* 設定為 *CPE* 上的主要區域。

  您還可以在不同位置中為單一租用戶備援建置一對 Clean Pipe；若要這樣做，請為某個位置中的第一個 Clean Pipe 指定 **1**，為不同位置中的第二個 Clean Pipe 指定 **2**。
- **BGP Peer ASN**（**BGP** 對等 **ASN**）—輸入 BGP 自發系統編號 (ASN)。

  您可以指定私人或公用 BGP ASN。

  記下此值；完成 Clean Pipe 設定時，您可以在客戶邊緣 (CE) 路由器上設定它。
- **Location**（位置）—選取位置。

  我們建議您使用為合作夥伴互連建立 VLAN 附件時所使用的同一位置。
- 若要啟用 QoS，請選取 **QoS**，然後選取要與 Clean Pipe 搭配使用的 QoS 設定檔。Clean Pipe QoS 在進入時成形。



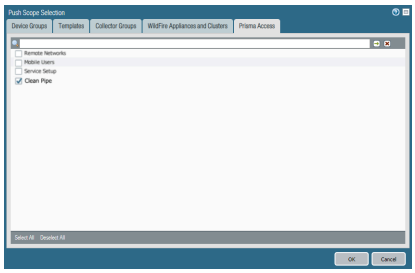

**STEP 5 |** 視需要重複步驟 4 新增更多 Clean Pipe 執行個體。

確保每個額外的 Clean Pipe 使用不同的位置。

 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** 提交並推送您的變更，以使其在 Prisma Access 作用中。

1. 選取 **Commit**（提交） > **Commit and Push**（提交並推送），然後在 Push Scope（推送範圍）中 **Edit Selections**（編輯選擇）。
2. 選取 **Prisma Access**，然後選取 **Clean Pipe**。



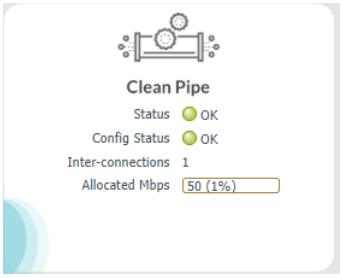
3. 按一下 **Ok**（確定），以儲存您對 Push Scope（推送範圍）所做的變更。
4. **Commit**（提交）並 **Push**（推送）您的變更。

**STEP 7 |** 檢查您的 Clean Pipe 是否已佈建。

1. 選取 **Panorama** > **Cloud Services**（雲端服務） > **Status**（狀態）。
2. 從頁面頂部的下拉式清單中選取 **Tenant**（租用戶）。
3. 按一下 **Status**（狀態）。

   即會顯示 Clean Pipe 狀態。
4. 將游標暫留在 Clean Pipe **Config Status**（設定狀態）上，並等到狀態從 **Provisioning in Progress**（佈建進行中）變更為 **Provisioned**（已佈建）。

   此佈建最多可能需要 30 分鐘。




**STEP 8 |** 按一下 **Network Details**（網路詳細資訊）頁籤、按一下 **Clean Pipe** 選項按鈕，然後記下 **Pairing Key**（配對金鑰）。

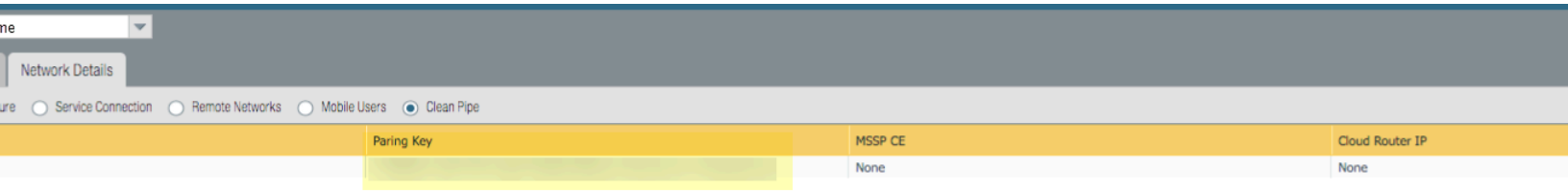
當您開始設定 Clean Pipe 時，**MSSP CE** 和 **Cloud Router IP**（雲端路由器 **IP**）欄位是空的。在完成 Clean Pipe 設定時，這些欄位會在您建立 VLAN 附件之後填入資料。

如果您指定了 **REDUNDANT** 連線，Prisma Access 會建立兩個配對金鑰（每個可用性區域一個），並為第一個可用性區域將 `zone1` 加在 Clean Pipe 名稱前面，而對於第二個可用性區域，則為 `zone2`。以下螢幕擷取畫面顯示了具有備援設定的 **SanFrancisco**（舊金

 ©2025 Palo Alto Networks, Inc.

山）Clean Pipe；Prisma Access 已建立兩個配對金鑰，一個用於 **SanFrancisco-zone1**，一個用於 **SanFrancisco-zone2**。

確保將第一個可用性區域 *(zone1)* 設定為 *CPE* 上的主要區域。




**STEP 9 |** 完成 Clean Pipe 設定。


©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.