使用者指南

AWS Client VPN

AWS Client VPN: 使用者指南

Table of Contents

什麼是 AWS Client VPN？

AWS Client VPN 是一種受管的用戶端型 VPN 服務，可讓您安全地存取 AWS 內部部署網路中的資源和資源。

本指南提供的步驟，可讓您使用裝置上的用戶端應用程式，建立 Client VPN 端點的 VPN 連接。

Client VPN 元件

以下是使用 AWS Client VPN 的關鍵元件。

- Client VPN 端點：您的 Client VPN 管理員會在其中建立和設定 Client VPN 端點 AWS。管理員控制您在建立 VPN 連接時可存取哪些網路和資源。
- VPN 用戶端應用程式 – 您用來連線至 Client VPN 端點並建立安全 VPN 連接的軟體應用程式。
- Client VPN 端點組態檔案 – Client VPN 管理員提供給您的組態檔案。檔案包含 Client VPN 端點的相關資訊，以及建立 VPN 連線所需的憑證。您可以將此檔案載入您選擇的 VPN 用戶端應用程式。AWS 提供的用戶端可讓您連線至五個並行工作階段，每個工作階段都有 Client VPN 管理員提供的專屬組態檔案。如需並行工作階段的詳細資訊，請參閱 支援並行連線。

設定 Client VPN 的其他資源

如果您是 Client VPN 管理員，請參閱AWS Client VPN 管理員指南，以取得建立和設定 Client VPN 端點的詳細資訊。

開始使用 AWS Client VPN

您的 Client VPN 管理員必須建立和設定 Client VPN 端點，您才能建立 VPN 工作階段。您的管理員控制您在建立 VPN 工作階段時可存取哪些網路和資源。接著您可使用以 VPN 用戶端應用程式來連接到 Client VPN 端點，以及建立安全的 VPN 連接。

如果您是需要建立 Client VPN 端點的系統管理員，請參閱《AWS Client VPN 管理員指南》。

主題

使用 Client VPN 的先決條件

若要建立 VPN 連接，您必須有下列各項：

- 存取網際網路
- 支援的裝置
- 支援的 Windows、macOS 或 Linux 版本。
- 對於使用 SAML 型聯合身分驗證 (單一登入) 的 Client VPN 端點，請使用下列其中一個瀏覽器：
  - Apple Safari
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox

步驟 1：取得 VPN 用戶端應用程式

您可以連線到 Client VPN 端點，並使用 AWS 提供的用戶端或其他 OpenVPN 型用戶端應用程式建立 VPN 連接。

您可以透過兩種方法之一下載 Client VPN 應用程式，取決於管理員是否為應用程式建立端點組態檔案：

- 如果您的管理員未設定端點組態檔案，請從 Client AWS VPN 下載下載並安裝用戶端。下載並安裝應用程式後，請繼續the section called “步驟 2：取得 Client VPN 端點組態檔案”從管理員取得端點組態檔案。如果您要連線至多個設定檔，則每個設定檔都需要一個組態檔案。
- 如果您的管理員已預先設定端點組態檔案，您可以從自助式入口網站下載 Client VPN 應用程式以及組態檔案。如需從自助式入口網站下載用戶端和組態檔案的步驟，請參閱 the section called “下載 Client VPN”。下載並安裝應用程式和檔案後，請前往 the section called “步驟 3：連接到 VPN”。

或者，也可以在您要用來建立 VPN 連接的裝置上，下載並安裝 OpenVPN 用戶端應用程式。

步驟 2：取得 Client VPN 端點組態檔案

您可以從管理員取得 Client VPN 端點組態檔案。組態檔案包含有關 Client VPN 端點和建立 VPN 連接所需的憑證的資訊。

或者，如果您的 Client VPN 管理員已設定 Client VPN 端點的自助式入口網站，您可以自行下載 AWS 提供的用戶端最新版本和 Client VPN 端點組態檔案。如需詳細資訊，請參閱AWS Client VPN 從自助式入口網站下載。

步驟 3：連接到 VPN

將 Client VPN 端點組態檔案匯入 AWS 提供的用戶端或 OpenVPN 用戶端應用程式，並連線至 VPN。如需連線至 VPN 的步驟，包括為 AWS 提供的用戶端匯入一或多個端點組態檔案，請參閱下列主題：

- 使用 AWS 提供的用戶端連線至 AWS Client VPN 端點
- 使用 OpenVPN 用戶端連線至 AWS Client VPN 端點

對於使用 Active Directory 身分驗證的 Client VPN 端點，系統會提示您輸入使用者名稱和密碼。如果目錄已啟用 Multi-Factor Authentication (MFA)，系統也會提示您輸入 MFA 代碼。

對於使用 SAML 型聯合身分驗證（單一登入）的 Client VPN 端點， AWS 提供的用戶端會在您的電腦上開啟瀏覽器視窗。系統會提示您輸入公司登入資料，然後才能連線到 Client VPN 端點。

AWS Client VPN 從自助式入口網站下載

自助式入口網站是一種網頁，可讓您下載最新版本的 AWS 用戶端和最新版本的 Client VPN 端點組態檔案。如果您的 Client VPN 端點管理員已預先設定 Client VPN 用戶端的一或多個組態檔案，您可以從此入口網站下載並安裝該 Client VPN 應用程式以及這些組態檔案。

> **Note**
>
> 如果您是管理員且想要設定自助式入口網站，請參閱《 AWS Client VPN 管理員指南》中的 Client VPN 端點。

開始之前，您必須擁有要下載的每個 Client VPN 端點的 ID 您的 Client VPN 端點管理員可以為您提供 ID，或可以為您提供包含 ID 的自助式入口網站 URL。對於多個端點連線，您將需要要連線的每個設定檔的端點 ID。

存取自助式入口網站

1. 移至 https://self-service.clientvpn.amazonaws.com/ 的自助式入口網站，或使用管理員提供給您的 URL。
2. 如有必要，請輸入 Client VPN 端點的 ID，例如 `cvpn-endpoint-0123456abcd123456`。選擇下一步。
3. 輸入您的使用者名稱和密碼，然後選擇 Sign in (登入)。這是您連線到 Client VPN 端點所使用的同一組使用者名稱和密碼。
4. 在自助式入口網站中，您可以執行下列動作：
   - 下載最新版的 Client VPN 端點用戶端組態檔案。如果您想要連線到多個端點，則需要下載每個端點的組態檔案。
   - 為您的平台下載最新版本的 AWS 用戶端。
5. 針對您要為其建立連線設定檔的每個端點組態檔案重複這些步驟。

使用 AWS 提供的用戶端連線至 AWS Client VPN 端點

您可以使用 AWS 提供的用戶端連線至 Client VPN 端點，該用戶端受 Windows、macOS 和 Ubuntu 支援。 AWS 提供的用戶端也支援最多五個並行連線以及 OpenVPN 指令。

主題

安全

安全性是 AWS 所提供用戶端中的最高優先順序。我們會定期發行修補程式，以改善應用程式的安全性狀態。相較於其他 OpenVPN 用戶端，AWS 提供的用戶端包含數個唯一的安全功能，包括 SAML 身分驗證、用戶端路由強制執行和裝置設定監控。

雖然 AWS 提供的用戶端旨在緩解因設定錯誤或洩露的網路環境而產生的威脅，但它不負責修改環境或消除來源的外部威脅。 AWS 提供的用戶端依賴客戶來維護安全且設定良好的環境。其中包含：

- 防止本機使用者未經授權的修改或濫用
- 限制受信任使用者的管理權限
- 維護up-to-date安全修補程式

使用 AWS 提供的用戶端支援並行連線

AWS 提供的用戶端允許 連線到多個並行工作階段。如果您需要跨多個 AWS 環境存取資源，並為這些資源擁有不同的端點，這會很有幫助。例如，您可能需要在與目前連線的端點不同的端點存取環境中的資料庫，但您不想中斷目前的連線。若要讓 AWS 提供的用戶端連線至目前的工作階段，請下載管理員為每個端點建立的組態檔案，然後為每個檔案建立連線設定檔。然後，您可以使用 AWS 提供的用戶端連線到多個工作階段，而不會中斷與目前開啟的任何工作階段的連線。這僅支援 AWS 提供的用戶端。如需連線至並行工作階段的步驟，請參閱下列內容：

- 使用 Windows AWS 提供的用戶端進行連線
- 使用 macOS AWS 提供的用戶端進行連線
- 使用 Linux AWS 提供的用戶端進行連線

連線至多個端點時，Client VPN 會實作檢查，以確保與其他開啟的端點連線沒有衝突，例如，如果兩個工作階段有衝突的 CIDR 區塊或路由政策；或者，如果您已使用完整的通道連線連線。如果檢查發現衝突，在您選擇與開啟的連線不衝突的其他連線，或中斷與造成衝突的開啟工作階段的連線之前，不會建立連線。

允許並行 DNS 連線。其中一個已啟用 DNS 連線的 DNS 伺服器將會套用。視 DNS 伺服器而定，系統可能會在重新連線期間提示您進行身分驗證。

> **Note**
>
> 允許並行工作階段的數量上限為 5 個。

OpenVPN 指令

AWS 提供的用戶端支援下列 OpenVPN 指令。如需這些指令的詳細資訊，請參閱 OpenVPN 網站上的文件。

- auth-federate
- auth-nocache
- auth-retry
- auth-user-pass
- block-outside-dns
- ca
- cert
- cipher
- 用戶端
- connect-retry
- connect-retry-max
- cryptoapicert
- dev
- dev-type
- bb
- dhcp-option

- ifconfig-ipv6
- inactive
- keepalive
- 金鑰
- mssfix
- nobind
- persist-key
- persist-tun
- ping
- ping-exit
- ping-restart
- proto
- pull
- pull-filter
- rcvbuf
- remote
- remote-cert-tls
- remote-random-hostname
- reneg-sec
- resolv-retry
- 路由
- route-ipv6
- server-poll-timeout
- static-challenge
- 點擊休眠
- tun-mtu
- tun-mtu-extra
- verb
- verify-x509-name

AWS Client VPN 適用於 Windows 的

這些章節說明如何使用 Windows x64 和 Windows Arm64 系統 AWS 提供的用戶端建立 VPN 連線。您可以在 AWS Client VPN 下載下載並安裝用戶端。 AWS 提供的用戶端不支援自動更新。

要求

AWS 提供的用戶端同時支援 Windows x64 和 Arm64 系統。每個作業系統都需要下列項目：

Windows Arm64 作業系統

- Windows 11 (64 位元作業系統、Arm64 處理器）
- .NET Framework 4.8.1 或更新版本

> **Note**
>
> 此應用程式包含使用 Arm64 模擬的背景程序。預設在 Windows 11 Arm64 裝置上完全支援並啟用此功能，確保無縫操作，無需任何額外的設定。如需詳細資訊，請參閱模擬如何在 Arm 上運作。

Windows x64 作業系統

- Windows 11 (64 位元作業系統，x64 處理器）
- .NET Framework 4.7.2 或更高版本

> **Note**
>
> 對於 Windows x64 和 Arm64 作業系統，使用 SAML 型聯合身分驗證（單一登入）的 Client VPN 端點，用戶端會在您的電腦上保留 TCP 連接埠 8096-8115。

開始之前，請確認您的 Client VPN 管理員已建立 Client VPN 端點，並已為您提供 Client VPN 端點組態檔案。如果您想要同時連線到多個設定檔，則需要每個設定檔的組態檔案。

主題

- AWS Client VPN 使用 AWS 提供的 Windows 用戶端連線至

- 端點安全軟體相容性
- AWS Client VPN 適用於 Windows 的版本備註

AWS Client VPN 使用 AWS 提供的 Windows 用戶端連線至

開始之前，請務必先詳閱需求。在下列步驟中， AWS 提供的用戶端也稱為 AWS VPN 用戶端。

若要使用 Windows x64 型或 Windows Arm64-based系統 AWS 提供的用戶端進行連線：

1. 開啟 AWS VPN Client 應用程式。
2. 選擇 File (檔案)、Manage Profiles (管理設定檔)。
3. 選擇 Add Profile (新增設定檔)。
4. 對於 Display Name (顯示名稱)，輸入描述檔的名稱。
5. 對於 VPN Configuration File (VPN 組態檔案)，請瀏覽至並選取您從 Client VPN 管理員接收的組態檔案，然後選擇 Add Profile (新增描述檔)。
6. 如果您想要建立多個連線，請針對您要新增的每個組態檔案重複新增設定檔步驟。您可以新增任意數量的設定檔，但最多只能有五個開啟的連線。
7. 在 AWS VPN 用戶端視窗中，選擇您要連線的設定檔，然後選擇連線。如果 Client VPN 端點已設為使用登入資料型的身分驗證，則系統會提示您輸入使用者名稱和密碼。針對您要啟動的每個設定檔連線重複此步驟，最多可連接五個並行端點。

   > **Note**
   >
   > 如果您連線的任何設定檔與目前開啟的工作階段衝突，您將無法進行連線。選擇新的連線，或與造成衝突的工作階段中斷連線。

8. 若要檢視連線的統計資料，請在 AWS VPN 用戶端視窗中選擇連線，選擇顯示詳細資訊，然後選擇您要查看詳細資訊的連線。
9. 若要中斷連線，請在 AWS VPN 用戶端視窗中選擇連線，然後選擇中斷連線。如果您有多個開啟的連線，您必須個別關閉每個連線。或者，選擇 Windows 工作列上的用戶端圖示，然後選擇 Disconnect (中斷連接)。

端點安全軟體相容性

企業端點安全產品，例如主機型防火牆、端點偵測和回應 (EDR) 代理程式和防毒軟體，有時可能會干擾 AWS Client VPN 連線。如果您在使用 Windows AWS 提供的用戶端時遇到連線問題，您可能需要在端點安全軟體中設定排除。

AWS Client VPN 可執行檔路徑

提供的 Windows AWS 用戶端會安裝下列金鑰可執行檔。設定防火牆規則、應用程式允許清單或端點安全政策時，您可能需要這些路徑。

VPN 用戶端應用程式

```
C:\Program Files\Amazon\AWS VPN Client\AWSVPNClient.exe
```

OpenVPN 程序

```
C:\Program Files\Amazon\AWS VPN Client\Resources\openvpn\acvc-openvpn.exe
```

這是建立和維護 VPN 通道連線的核心程序。

Windows 服務

```
C:\Program Files\Amazon\AWS VPN Client\AWSVPNClient.Service.exe
```

網路需求

AWS 提供的用戶端需要對 Client VPN 端點的傳出網路存取權，才能建立 VPN 連線。確保您的防火牆或端點安全軟體允許從`acvc-openvpn.exe`程序到 Client VPN 端點上設定的連接埠和通訊協定的傳出流量。

設定端點安全排除

如果您的端點安全產品干擾 AWS 提供的用戶端連線，請與您的安全管理員檢閱下列排除類別：

以程序為基礎的排除

將 中列出的可執行檔the section called “AWS Client VPN 可執行檔路徑”新增至端點安全產品的程序允許清單或排除清單。

以網路為基礎的排除項目

允許從acvc-openvpn.exe程序到 Client VPN 端點連接埠和通訊協定的傳出流量。

路徑型排除

從即時掃描或行為分析中排除 AWS 提供的用戶端安裝目錄：

```
C:\Program Files\Amazon\AWS VPN Client\
```

Important

由於產品版本和組態的變化，特定第三方端點安全產品的規範性組態指示不在 AWS 文件範圍內。如需設定特定產品排除的詳細說明，請參閱端點安全廠商的文件。

AWS Client VPN 適用於 Windows 的版本備註

下表包含 AWS Client VPN 適用於 Windows x64 型和 Windows Arm64-based系統的 目前和舊版的版本備註和下載連結。

Note

我們會繼續在每個版本中提供可用性和安全性修正。我們強烈建議您為每個平台使用最新版本。舊版可能會受到可用性和/或安全問題的影響。請參閱版本備註取得詳細資訊。

版本	改變	日期	下載連結和 SHA256
5.3.7 (x64 和 Arm64)	• 次要錯誤修正與增強功能	2026 年 6 月 15 日	• 下載 Windows x64 5.3.7 版 sha256：64 ee088e60b 3eab83fba e6b1d1db5 6da1156e8

版本	改變	日期	下載連結和 SHA256
			094ce0b1d 3fdf6e3e2 c285b731 • 下載 Windows Arm64 5.3.7 版 sha256：38 412d18b80 f9a13826e 0a4422f40 3a93fed51 b067f15af feb0727d2 3e76c7d9

版本	改變	日期	下載連結和 SHA256
5.3.6 (x64 和 Arm64)	• 從 5.3.5 轉返變更	2026 年 5 月 28 日	• 下載 Windows x64 5.3.6 版 sha256：a16212bdde30c1547acb33aae45a72b12615dc6e30839eb0b1a36d815279e95b • 下載 Windows Arm64 5.3.6 版 sha256：bc02e64efef9559fc991553e10bbc605bc2742f1d201574adcf4d77d500ee0d7

版本	改變	日期	下載連結和 SHA256
5.3.5 (x64 和 Arm64)	• 次要錯誤修正與增強功能 • 改善安全狀態	2026 年 5 月 27 日	• 下載 Windows x64 5.3.5 版 sha256：8cfc8f5d7de80c5b4673d1c9874b150ecc3133e9628e17208b5a4de30a050608 • 下載 Windows Arm64 5.3.5 版 sha256：1457fe9a8521cc5b4b07539ca57995714efb943265ad7134e464c1cc6698e6d0

版本	改變	日期	下載連結和 SHA256
5.3.4 (x64 和 Arm64)	• 次要錯誤修正與增強功能 • 改善安全狀態	2026 年 3 月 27 日	• 下載 Windows x64 5.3.4 版 sha256：81 a5c510162 4c5f74de8 afdcb816f 03ea8ff9e 8c6a5eaa8 890a95779 a94dbe41 • 下載 Windows Arm64 5.3.4 版 sha256：34 10282ebb0 24e64812a 63668b301 17657d470 ed4c51f05 e96fc812b 8871587d

版本	改變	日期	下載連結和 SHA256
5.3.3 (x64 和 Arm64)	• 修正 5.3.2 版中的連線失敗	2026 年 2 月 28 日	• 下載 Windows x64 5.3.3 版 sha256：bbaebb977b270add6497c941505fed5913b58056e980e3721707337dc051ac86 • 下載 Windows Arm64 5.3.3 版 sha256：c30b6d0121a5070643fdbebc27e7f9569d574a5698631480becb5cb96cac9fde

版本	改變	日期	下載連結和 SHA256
5.3.2 (x64 和 Arm64)	• 次要錯誤修正與增強功能。 • 改善安全狀態。	2026 年 2 月 17 日	• 下載 Windows x64 5.3.2 版 sha256：dd 1e4fb6718 dddbf13a5 aee542175 761bf8ed8 54290c576 a488b9817 3a0ccf92 • 下載 Windows Arm64 5.3.2 版 sha256：d2 d18d91ca9 ef53cc557 434db18ef 5d0002e78 25a998f2d 739eac443 b034af00

版本	改變	日期	下載連結和 SHA256
5.3.1 (x64 和 Arm64)	次要錯誤修正與增強功能。	2025 年 9 月 30 日	• 下載 Windows x64 5.3.1 版 sha256：b71ddbc78230630963acf3ebba7afeb6e52599843091ff589aed6afce4c9eb06 • 下載 Windows Arm64 5.3.1 版 sha256：e691bdb0bdcb55b3da36f4fb2e5198f20f1878dc22a00bf55bc660999698500b

版本	改變	日期	下載連結和 SHA256
5.3.0 (Arm64)	新的 Windows Arm64-based AWS Client VPN 支援。 此版本包含 Windows (x64) 5.3.0 版本的所有更新。	2025 年 8 月 26 日	下載 Windows Arm64 5.3.0 版 sha256：3f 1be6b487a f8307dafb b0f7737cd 597cf71dc 64dcd3177 5aeeebf91 d04b8dce
5.3.0	• 次要增強功能。 • 新增對 IPv6 連線的支援	2025 年 8 月 14 日	下載 Windows x64 5.3.0 版 sha256： e3cf1aff6e1 4d79aa443 78229a3a0 602a9e9c2 a0c6d0d05 5df901440 b6d1454a
5.2.2	改善安全狀態。	2025 年 6 月 2 日	下載 5.2.2 版 sha256：f2 7cb0eed7c 9c5354caa 5d7e37595 eefbb048d 7481bf698 b2e5fb653 b667c190

版本	改變	日期	下載連結和 SHA256
5.2.1	• 新增對 `ping-exit` OpenVPN 旗標的支援。 • 已更新 OpenSSL 程式庫。 • 次要錯誤修正與增強功能。	2025 年 4 月 21 日	不再支援。
5.2.0	• 次要增強功能。 • 新增對用戶端路由強制執行的支援。	2025 年 4 月 8 日	不再支援。
5.1.0	• 修正 5.0.x AWS Client VPN 版在閒置逾時中斷連線後自動重新連線至 VPN 的問題。 • 次要錯誤修正與增強功能。	2025 年 3 月 17 日	不再支援。
5.0.2	• 修正並行連線的 DNS 問題。 • 已修正安裝新 TAP 轉接器時的零星問題。	2025 年 2 月 24 日	不再支援。
5.0.1	修正導致 Windows 用戶端 5.0.0 版上偶發 VPN 連線錯誤的問題。	2025 年 1 月 30 日	不再支援。
5.0.0	• 新增對並行連線的支援。 • 已更新 TAP 驅動程式版本。 • 更新圖形使用者介面。 • 次要錯誤修正與增強功能	2025 年 1 月 21 日	不再支援。
4.1.0	次要錯誤修正與增強功能。	2024 年 11 月 12 日	不再支援。

版本	改變	日期	下載連結和 SHA256
4.0.0	次要增強功能。	2024 年 9 月 25 日	下載 4.0.0 版 sha256：6532f911385ec8fac1494d0847c8f90a999b3bd7380844e2ea4318e9db4a2ebc
3.14.2	新增對 `mssfix` OpenVPN 旗標的支援。	2024 年 9 月 4 日	下載 3.14.2 版 sha256：c171639d7e07e5fd48998cf76f74e6e49e5cbe3356c6264a67b4a9bf473b5f5d
3.14.1	次要錯誤修正與增強功能。	2024 年 8 月 22 日	下載 3.14.1 版 sha256：f743a7b4bc82daa4b803c2994390529997bb57a4bb54d1f5195ab28827283335

版本	改變	日期	下載連結和 SHA256
3.14.0	• 新增對 `tap-sleep` OpenVPN 旗標的支援。 • 已更新 OpenVPN 和 OpenSSL 程式庫。	2024 年 8 月 12 日	下載 3.14.0 版 sha256：812fb2f6d263288c664d598f6bd70e3f601d11dcb89e63b281b0a96b96354516
3.13.0	已更新 OpenVPN 和 OpenSSL 程式庫。	2024 年 7 月 29 日	下載 3.13.0 版 sha256：c9cc896e81a744118409 51e349eed9384507c5 3337fb703c5ec64d52 2c29388b
3.12.1	修正防止 Windows 用戶端 3.12.0 版為某些使用者建立 VPN 連線的問題。	2024 年 7 月 18 日	下載 3.12.1 版 sha256：5ed34aee6c0 3aa281e62 5acdbed27 2896c6704 6364a9e58 46ca697e0 5dbfec08

版本	改變	日期	下載連結和 SHA256
3.12.0	• 區域網路範圍變更時自動重新連線。 • 已移除與 SAML 端點連線時的自動應用程式焦點。	2024 年 5 月 21 日	不再支援
3.11.2	自 123 版以來，已解決以 Chromium 為基礎的瀏覽器的 SAML 身分驗證問題。	2024 年 4 月 11 日	下載 3.11.2 版 sha256：8ba258dd15bea3e861adad108f8a6d6d4bcd8fe42cb9ef8bbc294e72f365c7cc
3.11.1	• 已修正緩衝區溢位動作，可能允許本機演員執行具有更高許可的任意命令。 • 改善安全狀態。	2024 年 2 月 16 日	下載 3.11.1 版 sha256：fb67b60aa8370197958a11ea6f57d5bc0512279560b52a857ae34cb321eaefd0

版本	改變	日期	下載連結和 SHA256
3.11.0	• 已修正 Windows 虛擬機器所造成的連線問題。 • 已修正某些 LAN 組態的連線問題 • 已改善存取性。	2023 年 12 月 6 日	下載 3.11.0 版 sha256：9b 6b7def99d 76c59a97b 067b6a73b dc6ee1c6b 89a206328 6f542e96b 32df5ae9
3.10.0	• 修正用戶端網路中啟用 NAT64 時的連線問題。 • 修正用戶端機器上安裝 Hyper-V 網路介面卡時的連線問題。 • 次要錯誤修正與增強功能。	2023 年 8 月 24 日	下載 3.10.0 版 sha256: d46721aad 40ccb816f 163e406c3 66ff03b11 20abbb43a 20607e06d 3b1fa8667f
3.9.0	改善安全狀態。	2023 年 8 月 3 日	下載 3.9.0 版 sha256：de 9a3800ea2 349155540 bd32bbae4 72404c636 d8d8267a0 e1fb2173a 8aae21ed
3.8.0	改善安全狀態。	2023 年 7 月 15 日	不再支援

版本	改變	日期	下載連結和 SHA256
3.7.0	已復原 3.6.0 版的變更。	2023 年 7 月 15 日	不再支援
3.6.0	改善安全狀態。	2023 年 7 月 14 日	不再支援
3.5.0	次要錯誤修正與增強功能。	2023 年 4 月 3 日	不再支援
3.4.0	已復原 3.3.0 版的變更。	2023 年 3 月 28 日	不再支援
3.3.0	次要錯誤修正與增強功能。	2023 年 3 月 17 日	不再支援
3.2.0	• 新增對「verify-x509-name」OpenVPN 旗標的支援。 • 當用戶端更新版本可用時會自動偵測。 • 加入了新客戶端版本可用時自動安裝的功能。	2023 年 1 月 23 日	不再支援
3.1.0	改善安全狀態。	2022 年 5 月 23 日	不再支援
3.0.0	• 加入了 Windows 11 支援。 • 修復了導致其他驅動程式名稱受到影響的 TAP Windows 驅動程式命名方式。 • 修復了使用聯合身分驗證時橫幅訊息不顯示的問題。 • 修復了較長文字的橫幅文字顯示。 • 增強的安全狀態。	2022 年 3 月 3 日	不再支援
2.0.0	• 加入了建立新連線後對支援橫幅文字的支援。 • 移除了使用 pull-filter (與 echo 相關) 的能力。即 pull-filter * echo • 次要錯誤修正與增強功能。	2022 年 1 月 20 日	不再支援

版本	改變	日期	下載連結和 SHA256
1.3.7	• 已修正在某些情況下的聯合身分驗證連線嘗試。 • 次要錯誤修正與增強功能。	2021 年 11 月 8 日	不再支援
1.3.6	• 新增對 OpenVPN 旗標的支援：connect-retry-max、dev-type、keepalive、ping、ping-restart、pull、rcvbuf、server-poll-timeout。 • 次要錯誤修正與增強功能。	2021 年 9 月 20 日	不再支援
1.3.5	刪除大型視窗日誌的修補程式。	2021 年 8 月 16 日	不再支援
1.3.4	• 已新增對 OpenVPN 旗標的支援：dhcp-option。 • 次要錯誤修正與強化功能。	2021 年 8 月 4 日	不再支援
1.3.3	• 新增對下列 OpenVPN 旗標的支援：inactive、pull-filter、route。 • 修正導致應用程式在中斷連線或結束時當機的問題。 • 修正含反斜線的 Active Directory 使用者名稱相關問題。 • 修正在應用程式外操作設定檔清單時的應用程式當機問題。 • 次要錯誤修正與強化功能。	2021 年 7 月 1 日	不再支援
1.3.2	• 設定時，新增 IPv6 洩漏防護。 • 修正使用 Connection (連線)下的 Show Details (顯示詳細資料) 選項時可能發生的當機問題	2021 年 5 月 12 日	不再支援

版本	改變	日期	下載連結和 SHA256
1.3.1	• 新增了對具有相同主體的多個用戶端憑證的支援。過期的憑證將會被忽略。 • 修正了本機日誌保留，以減少磁碟使用量。 • 新增了對「route-ipv6」OpenVPN 指示詞的支援。 • 次要錯誤修正與強化功能。	2021 年 4 月 5 日	不再支援
1.3.0	新增了支援功能，如錯誤報告、傳送診斷日誌和分析。	2021 年 3 月 8 日	不再支援
1.2.7	• 新增了對 cryptoapicert OpenVPN 指示詞的支援。 • 修正了連線之間的過時路由。 • 次要錯誤修正與強化功能。	2021 年 2 月 25 日	不再支援
1.2.6	次要錯誤修正與強化功能。	2020 年 10 月 26 日	不再支援
1.2.5	• 在 OpenVPN 設定中新增了對註解的支援。 • 新增 TLS 交握錯誤訊息。	2020 年 10 月 8 日	不再支援
1.2.4	次要錯誤修正與強化功能。	2020 年 9 月 1 日	不再支援
1.2.3	轉返在 1.2.2 版本中的變更。	2020 年 8 月 20 日	不再支援
1.2.1	次要錯誤修正與強化功能。	2020 年 7 月 1 日	不再支援
1.2.0	• 已新增對 SAML 2.0 型聯合身分驗證的支援。 • 已取代對 Windows 7 平台的支援。	2020 年 5 月 19 日	不再支援
1.1.1	次要錯誤修正與強化功能。	2020 年 4 月 21 日	不再支援

版本	改變	日期	下載連結和 SHA256
1.1.0	• 新增支援 OpenVPN 靜態挑戰回應功能，可隱藏或顯示使用者界面中顯示的文字。 • 次要錯誤修正與強化功能。	2020 年 3 月 9 日	不再支援
1.0.0	初始版本。	2020 年 2 月 4 日	不再支援

AWS Client VPN for macOS

這些章節說明如何使用 macOS AWS提供的用戶端建立 VPN 連線。您可以在 AWS Client VPN 下載下載並安裝用戶端。AWS提供的用戶端不支援自動更新。

要求

若要將AWS提供的用戶端用於 macOS，需要下列項目：

- macOS Sonoma (14.0)、Sequoia (15.0) 或 Tahoe (26.0)
- 與 x86_64 或 ARM64 處理器相容。
- 對於使用 SAML 型聯合身分驗證（單一登入）的 Client VPN 端點，用戶端會在您的電腦上保留 TCP 連接埠 8096-8115。

主題

AWS Client VPN 使用 macOS AWS 提供的用戶端連線至

開始之前，請確認您的 Client VPN 管理員已建立 Client VPN 端點，並已為您提供 Client VPN 端點組態檔案。如果您想要同時連線到多個設定檔，則需要每個設定檔的組態檔案。

同樣的，請務必先詳閱需求。在下列步驟中， AWS 提供的用戶端也稱為 AWS VPN 用戶端。

使用 macOS AWS 提供的用戶端進行連線

1. 開啟 AWS VPN Client 應用程式。
2. 選擇 File (檔案)、Manage Profiles (管理設定檔)。
3. 選擇 Add Profile (新增設定檔)。
4. 對於 Display Name (顯示名稱)，輸入描述檔的名稱。
5. 對於 VPN Configuration File (VPN 組態檔案)，請瀏覽至並選取您從 Client VPN 管理員接收的組態檔案，然後選擇 Add Profile (新增描述檔)。
6. 如果您想要建立多個連線，請針對您要新增的每個組態檔案重複新增設定檔步驟。您可以新增任意數量的設定檔，但最多只能有五個開啟的連線。
7. 在 AWS VPN 用戶端視窗中，選擇您要連線的設定檔，然後選擇連線。如果 Client VPN 端點已設為使用登入資料型的身分驗證，則系統會提示您輸入使用者名稱和密碼。針對您要啟動的每個設定檔連線重複此步驟，最多可連接五個並行端點。

   > **Note**
   >
   > 如果您連線的任何設定檔與目前開啟的工作階段衝突，您將無法進行連線。選擇新的連線，或與造成衝突的工作階段中斷連線。

8. 若要檢視連線的統計資料，請在 AWS VPN 用戶端視窗中選擇連線，選擇顯示詳細資訊，然後選擇您要查看詳細資訊的連線。
9. 若要中斷連線，請在 AWS VPN 用戶端視窗中選擇連線，然後選擇中斷連線。如果您有多個開啟的連線，您必須個別關閉每個連線。

AWS Client VPN for macOS 版本備註

下表包含 AWS Client VPN 適用於 macOS 的目前和先前版本的版本備註和下載連結。

> **Note**
>
> 我們會繼續在每個版本中提供可用性和安全性修正。我們強烈建議您為每個平台使用最新版本。舊版可能會受到可用性和/或安全問題的影響。請參閱版本備註取得詳細資訊。

版本	改變	日期	下載連結
5.3.5	• 次要錯誤修正與增強功能 • 改善安全狀態 • 在未來的更新中，為 ARM 型 Mac 使用者啟用了原生 ARM64 用戶端的自動升級，無需從在 Rosetta 轉譯層下執行的 Intel 型用戶端手動遷移	2026 年 5 月 14 日	• 下載 macOS ARM64 5.3.5 版 sha256：048c9011b7cea43720cb92d7c2fe064c8d853b391ee499408736cba5d9111652 • 下載 macOS x64 5.3.5 版 sha256：64a84f529a09b2ee9756dd8f5e193b9624b3239bcd76d9f20411a72d1f93887c
5.3.4	• 移除 ARM 機器上的 Intel 相容性層 (Rosetta) 需求 • 次要錯誤修正與增強功能	2026 年 2 月 17 日	不再支援。
5.3.3	• 次要錯誤修正與增強功能。 • 改善安全狀態。	2025 年 12 月 26 日	不再支援。
5.3.2	• 新增 Apple Silicon 架構的原生支援和新的 macOS ARM64 安裝程式。 • 次要錯誤修正與增強功能。	2025 年 10 月 27 日	不再支援。
5.3.1	• 次要錯誤修正與增強功能。	2025 年 9 月 9 日	不再支援。
5.3.0	• 次要增強功能。 • 新增對 IPv6 連線的支援。	2025 年 8 月 14 日	不再支援。
5.2.1	• 新增對 ping-exit OpenVPN 旗標的支援。	2025 年 6 月 18 日	不再支援。

版本	改變	日期	下載連結
	• 已更新 OpenSSL 程式庫。 • 改善安全狀態。 • 次要錯誤修正與增強功能。		
5.2.0	• 次要增強功能。 • 新增對用戶端路由強制執行的支援。	2025 年 4 月 8 日	不再支援。
5.1.0	• 修正 5.0.x AWS Client VPN 版在閒置逾時中斷連線後自動重新連線至 VPN 的問題。 • 已修正 AWS Client VPN 無法為 Windows 樣式行尾的組態檔案建立 VPN 連線的問題。 • 次要錯誤修正與增強功能。	2025 年 3 月 17 日	不再支援。
5.0.3	次要錯誤修正與增強功能。	2025 年 3 月 6 日	不再支援。
5.0.2	修正在選擇 Connect 時導致零星錯誤的問題。	2025 年 2 月 17 日	不再支援。
5.0.1	修正用戶端 5.0.0 版無法為包含空格的設定檔名稱建立 VPN 連線的問題。	2025 年 1 月 22 日	不再支援。
5.0.0	• 新增對並行連線的支援。 • 更新圖形使用者介面。 • 次要錯誤修正與增強功能。	2025 年 1 月 21 日	不再支援。
4.1.0	次要錯誤修正與增強功能。	2024 年 11 月 12 日	不再支援。
4.0.0	次要增強功能。	2024 年 9 月 25 日	不再支援。
3.12.1	新增對 `mssfix` OpenVPN 旗標的支援。	2024 年 9 月 4 日	不再支援。

版本	改變	日期	下載連結
3.12.0	• 新增對 `tap-sleep` OpenVPN 旗標的支援。 • 已更新 OpenVPN 和 OpenSSL 程式庫。	2024 年 8 月 12 日	不再支援。
3.11.0	• 已更新 OpenVPN 和 OpenSSL 程式庫。	2024 年 7 月 29 日	不再支援。
3.10.0	• 區域網路範圍變更時自動重新連線。 • 修正網路切換期間的 DNS 還原問題。 • 已移除與 SAML 端點連線時的自動應用程式焦點。	2024 年 5 月 21 日	不再支援。
3.9.2	• 自 123 版以來，已解決以 Chromium 為基礎的瀏覽器的 SAML 身分驗證問題。 • 新增對 macOS Sonoma 的支援。棄用對 macOS Big Sur 的支援。 • 改善安全狀態。	2024 年 4 月 11 日	不再支援。
3.9.1	• 已修正緩衝區溢位動作，可能允許本機演員執行具有更高許可的任意命令。 • 已修正應用程式更新下載進度列。 • 改善安全狀態。	2024 年 2 月 16 日	不再支援。
3.9.0	• 已修正某些 LAN 組態的連線問題 • 已改善存取性。	2023 年 12 月 6 日	不再支援。
3.8.0	• 修正用戶端網路中啟用 NAT64 時的連線問題。 • 次要錯誤修正與增強功能。	2023 年 8 月 24 日	不再支援。
3.7.0	• 改善安全狀態。	2023 年 8 月 3 日	不再支援。

版本	改變	日期	下載連結
3.6.0	• 改善安全狀態。	2023 年 7 月 15 日	不再支援。
3.5.0	• 已復原 3.4.0 版的變更。	2023 年 7 月 15 日	不再支援。
3.4.0	• 改善安全狀態。	2023 年 7 月 14 日	不再支援。
3.3.0	• 已新增對 macOS Ventura (13.0) 的支援。 • 次要錯誤修正與增強功能。	2023 年 4 月 27 日	不再支援。
3.2.0	• 新增對「verify-x509-name」OpenVPN 旗標的支援。 • 當用戶端更新版本可用時會自動偵測。 • 加入了新客戶端版本可用時自動安裝的功能。	2023 年 1 月 23 日	不再支援。
3.1.0	• 新增對 macOS Monterey 的支援。 • 修復了磁碟機類型偵測的問題。 • 改善安全狀態。	2022 年 5 月 23 日	不再支援。
3.0.0	• 修復了使用聯合身分驗證時橫幅訊息不顯示的問題。 • 修復了較長文字的橫幅文字顯示。 • 增強的安全狀態。	2022 年 3 月 3 日	不再支援。
2.0.0	• 加入了建立新連線後對支援橫幅文字的支援。 • 移除了使用 pull-filter (與 echo 相關) 的能力。即 pull-filter * echo • 次要錯誤修正與增強功能。	2022 年 1 月 20 日	不再支援。

版本	改變	日期	下載連結
1.4.0	• 在連線期間新增 DNS 伺服器監控。如果這些設定不符合 VPN 設定，就會重新設定。 • 已修正在某些情況下的聯合身分驗證連線嘗試。 • 次要錯誤修正與增強功能。	2021 年 11 月 9 日	不再支援。
1.3.5	• 新增對 OpenVPN 旗標的支援：connect-retry-max、dev-type、keepalive、ping、ping-restart、pull、rcvbuf、server-poll-timeout。 • 次要錯誤修正與增強功能。	2021 年 9 月 20 日	不再支援。
1.3.4	• 已新增對 OpenVPN 旗標的支援：dhcp-option。 • 次要錯誤修正與強化功能。	2021 年 8 月 4 日	不再支援。
1.3.3	• 新增對下列 OpenVPN 旗標的支援：inactive、pull-filter、route。 • 修正含空格或 Unicode 的組態檔案名稱相關問題。 • 修正導致應用程式在中斷連線或結束時當機的問題。 • 修正含反斜線的 Active Directory 使用者名稱相關問題。 • 修正在應用程式外操作設定檔清單時的應用程式當機問題。 • 次要錯誤修正與強化功能。	2021 年 7 月 1 日	不再支援。

版本	改變	日期	下載連結
1.3.2	• 設定時，新增 IPv6 洩漏防護。 • 修正使用 Connection (連線)下的 Show Details (顯示詳細資料) 選項時可能發生的當機問題 • 新增 daemon 日誌輪替。	2021 年 5 月 12 日	不再支援。
1.3.1	• 新增了對 macOS Big Sur (10.16) 的支援。 • 修正了移除其他應用程式設定 DNS 設定的問題。 • 修正了使用非有效憑證進行相互驗證導致連線問題的問題。 • 新增了對「route-ipv6」OpenVPN 指示詞的支援。 • 次要錯誤修正與強化功能。	2021 年 4 月 5 日	不再支援。
1.3.0	新增了支援功能，如錯誤報告、傳送診斷日誌和分析。	2021 年 3 月 8 日	不再支援。
1.2.5	次要錯誤修正與強化功能。	2021 年 2 月 25 日	不再支援。
1.2.4	次要錯誤修正與強化功能。	2020 年 10 月 26 日	不再支援。
1.2.3	• 在 OpenVPN 設定中新增了對註解的支援。 • 新增 TLS 交握錯誤訊息。 • 修正了影響部分使用者的解除安裝錯誤。	2020 年 10 月 8 日	不再支援。
1.2.2	次要錯誤修正與強化功能。	2020 年 8 月 12 日	不再支援。

版本	改變	日期	下載連結
1.2.1	• 新增解除安裝應用程式的支援。 • 次要錯誤修正與強化功能。	2020 年 7 月 1 日	不再支援。
1.2.0	• 已新增對 SAML 2.0 型聯合身分驗證的支援。 • 新增了對 macOS Catalina (10.15) 的支援。	2020 年 5 月 19 日	不再支援。
1.1.2	次要錯誤修正與強化功能。	2020 年 4 月 21 日	不再支援。
1.1.1	• 修正 DNS 無法解析的問題。 • 修正因連線較長所造成的應用程式當機問題。 • 修正 MFA 問題。	2020 年 4 月 2 日	不再支援。
1.1.0	• 新增支援 macOS DNS 組態。 • 新增支援 OpenVPN 靜態挑戰回應功能，可隱藏或顯示使用者界面中顯示的文字。 • 次要錯誤修正與強化功能。	2020 年 3 月 9 日	不再支援。
1.0.0	初始版本。	2020 年 2 月 4 日	不再支援。

AWS Client VPN 適用於 Linux

這些章節說明安裝適用於 Linux 的 AWS 用戶端，然後使用 AWS 提供的用戶端建立 VPN 連線。提供的 Linux AWS 用戶端不支援自動更新。如需最新的更新和下載，請參閱 the section called “版本備註”。

使用 Linux AWS 提供的用戶端連線至 Client VPN 的需求

若要使用 Linux AWS 提供的用戶端，需要下列項目：

- Ubuntu 22.04 LTS (AMD64)、Ubuntu 24.04 LTS （僅限 AMD64) 或 Ubuntu 26.04 LTS （僅限 AMD64)

對於使用 SAML 型聯合身分驗證 （單一登入） 的 Client VPN 端點，用戶端會在您的電腦上保留 TCP 連接埠 8096-8115。

開始之前，請確認您的 Client VPN 管理員已建立 Client VPN 端點，並已為您提供 Client VPN 端點組態檔案。如果您想要同時連線到多個設定檔，則需要每個設定檔的組態檔案。

主題

- 安裝 AWS Client VPN 為 Linux 提供的
- 連線至 AWS Client VPN 為 Linux 提供的
- AWS Client VPN 適用於 Linux 的版本備註

安裝 AWS Client VPN 為 Linux 提供的

有多種方法可用來安裝 Linux AWS 提供的用戶端。請使用下列其中一種方法。開始之前，請務必先詳閱需求。

選項 1：透過套件儲存庫安裝

1. 將 AWS VPN 用戶端公有金鑰新增至 Ubuntu 作業系統。

```
wget -qO- https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-
repo/awsvpnclient_public_key.asc | sudo tee /etc/apt/trusted.gpg.d/
awsvpnclient_public_key.asc
```

2. 使用下列命令將儲存庫新增至 Ubuntu 作業系統 (22.04 版及更高版本）：

```
echo "deb [arch=amd64] https://d20adtppz83p9s.cloudfront.net/GTK/latest/debian-repo
 ubuntu main" | sudo tee /etc/apt/sources.list.d/aws-vpn-client.list
```

3. 使用下列命令更新系統上的儲存庫。

```
sudo apt-get update
```

4. 使用下列命令來安裝 Linux AWS 提供的用戶端。

```
sudo apt-get install awsvpnclient
```

選項 2：使用 .deb 套件檔案安裝

1. 從 AWS Client VPN 下載下載 .deb 檔案或使用下列命令。

```
curl https://d20adtppz83p9s.cloudfront.net/GTK/latest/awsvpnclient_amd64.deb -o
 awsvpnclient_amd64.deb
```

2. 使用 dpkg公用程式安裝為 Linux AWS 提供的用戶端。

```
sudo dpkg -i awsvpnclient_amd64.deb
```

選項 3 — 使用 Ubuntu Software Center 安裝 .deb 套件

1. 從 AWS Client VPN 下載下載 .deb 套件檔案。
2. 下載 .deb 套件檔案後，使用 Ubuntu Software Center 安裝套件。遵循使用 Ubuntu Software Center 從獨立 .deb 套件安裝的步驟，如 Ubuntu Wiki 所述。

連線至 AWS Client VPN 為 Linux 提供的

在下列步驟中， AWS 提供的用戶端也稱為 AWS VPN 用戶端。

使用 Linux AWS 提供的用戶端進行連線

1. 開啟 AWS VPN Client 應用程式。
2. 選擇 File (檔案)、Manage Profiles (管理設定檔)。
3. 選擇 Add Profile (新增設定檔)。
4. 對於 Display Name (顯示名稱)，輸入描述檔的名稱。
5. VPN Configuration File (VPN 組態檔案) 請使用您從 Client VPN 管理員收到的組態檔案。選擇 Open (開啟)。
6. 選擇 Add Profile (新增設定檔)。
7. 如果您想要建立多個連線，請針對您要新增的每個組態檔案重複新增設定檔步驟。您可以新增任意數量的設定檔，但最多只能有五個開啟的連線。

8. 在 AWS VPN 用戶端視窗中，選擇您要連線的設定檔，然後選擇連線。如果 Client VPN 端點已設為使用登入資料型的身分驗證，則系統會提示您輸入使用者名稱和密碼。針對您要啟動的每個設定檔連線重複此步驟，最多可連接五個並行端點。

   > **Note**
   >
   > 如果您連線的任何設定檔與目前開啟的工作階段衝突，您將無法進行連線。選擇新的連線，或與造成衝突的工作階段中斷連線。

9. 若要檢視連線的統計資料，請在 AWS VPN 用戶端視窗中選擇連線，選擇顯示詳細資訊，然後選擇您要查看詳細資訊的連線。
10. 若要中斷連線，請在 AWS VPN 用戶端視窗中選擇連線，然後選擇中斷連線。如果您有多個開啟的連線，您必須個別關閉每個連線。

AWS Client VPN 適用於 Linux 的版本備註

下表包含 AWS Client VPN 適用於 Linux 的目前和先前版本的版本備註和下載連結。

> **Note**
>
> 我們會繼續在每個版本中提供可用性和安全性修正。我們強烈建議您為每個平台使用最新版本。舊版可能會受到可用性和/或安全問題的影響。請參閱版本備註取得詳細資訊。

版本	改變	日期	下載連結
5.3.3	• 次要錯誤修正與增強功能 • 改善安全狀態	2026 年 5 月 18 日	下載 5.3.3 版 sha256：d0096c934b36122c245d8c2243d4146cdac67125c7421c4e1e6ad430eb3adfcf

版本	改變	日期	下載連結
5.3.2	• 次要錯誤修正與增強功能。 • 改善安全狀態。	2025 年 12 月 17 日	不再支援。
5.3.1	• 次要增強功能。	2025 年 9 月 25 日	不再支援。
5.3.0	• 次要增強功能。 • 新增對 IPv6 連線的支援。	2025 年 8 月 14 日	不再支援。
5.2.0	• 次要增強功能。 • 新增對用戶端路由強制執行的支援。	2025 年 4 月 8 日	不再支援。
5.1.0	• 修正 5.0.x AWS Client VPN 版在閒置逾時中斷連線後自動重新連線至 VPN 的問題。 • 次要錯誤修正與增強功能。	2025 年 3 月 17 日	不再支援。
5.0.0	• 新增對多個並行連線的支援。 • 更新圖形使用者介面。 • 次要錯誤修正與增強功能。	2025 年 1 月 21 日	不再支援。
4.1.0	• 新增對 Ubuntu 22.04 和 24.04 的支援。 • 錯誤修正。	2024 年 11 月 12 日	不再支援。
4.0.0	次要增強功能。	2024 年 9 月 25 日	不再支援。
3.15.1	新增對 `mssfix` OpenVPN 旗標的支援。	2024 年 9 月 4 日	不再支援。
3.15.0	• 新增對 `tap-sleep` OpenVPN 旗標的支援。 • 已更新 OpenVPN 和 OpenSSL 程式庫。	2024 年 8 月 12 日	不再支援。
3.14.0	• 已更新 OpenVPN 和 OpenSSL 程式庫。	2024 年 7 月 29 日	不再支援。
3.13.0	• 區域網路範圍變更時自動重新連線。	2024 年 5 月 21 日	不再支援。

版本	改變	日期	下載連結
3.12.2	• 自 123 版以來，已解決以 Chromium 為基礎的瀏覽器的 SAML 身分驗證問題。	2024 年 4 月 11 日	不再支援。
3.12.1	• 已修正緩衝區溢位動作，可能允許本機演員執行具有更高許可的任意命令。 • 改善安全狀態。	2024 年 2 月 16 日	不再支援。
3.12.0	• 已修正某些 LAN 組態的連線問題	2023 年 12 月 19 日	不再支援。
3.11.0	• 回復「已修正某些 LAN 組態的連線問題」。 • 已改善存取性。	2023 年 12 月 6 日	不再支援。
3.10.0	• 已修正某些 LAN 組態的連線問題。 • 已改善存取性。	2023 年 12 月 6 日	不再支援。
3.9.0	• 修正用戶端網路中啟用 NAT64 時的連線問題。 • 次要錯誤修正與增強功能。	2023 年 8 月 24 日	不再支援。
3.8.0	• 改善安全狀態。	2023 年 8 月 3 日	不再支援。
3.7.0	• 改善安全狀態。	2023 年 7 月 15 日	不再支援。
3.6.0	• 已復原 3.5.0 版的變更。	2023 年 7 月 15 日	不再支援。
3.5.0	• 改善安全狀態。	2023 年 7 月 14 日	不再支援。
3.4.0	• 新增對「verify-x509-name」OpenVPN 旗標的支援。	2023 年 2 月 14 日	不再支援。
3.1.0	• 修復了磁碟機類型偵測的問題。 • 改善安全狀態。	2022 年 5 月 23 日	不再支援。

版本	改變	日期	下載連結
3.0.0	• 修復了使用聯合身分驗證時橫幅訊息不顯示的問題。 • 修復了較長文字和特定字元序列的橫幅文字顯示問題。 • 增強的安全狀態。	2022 年 3 月 3 日	不再支援。
2.0.0	• 加入了建立新連線後對支援橫幅文字的支援。 • 移除了使用 pull-filter (與 echo 相關) 的能力。即 pull-filter * echo • 次要錯誤修正與增強功能。	2022 年 1 月 20 日	不再支援。
1.0.3	• 已修正在某些情況下的聯合身分驗證連線嘗試。 • 次要錯誤修正與增強功能。	2021 年 11 月 8 日	不再支援。
1.0.2	• 新增對 OpenVPN 旗標的支援：connect-retry-max、dev-type、keepalive、ping、ping-restart、pull、rcvbuf、server-poll-timeout。 • 次要錯誤修正與增強功能。	2021 年 9 月 28 日	不再支援。
1.0.1	• 啟用選項從 Ubuntu 應用程式欄退出。 • 新增對下列 OpenVPN 旗標的支援：inactive、pull-filter、route。 • 次要錯誤修正與強化功能。	2021 年 8 月 4 日	不再支援。
1.0.0	初始版本。	2021 年 6 月 11 日	不再支援。

使用 OpenVPN 用戶端連線至 AWS Client VPN 端點

您可以使用常見的 Open VPN 用戶端應用程式建立與 Client VPN 端點的連線。下列作業系統支援 Client VPN：

- Windows

  使用 Windows Certificate Store 中的憑證和私有金鑰。產生憑證和金鑰後，您可以使用 OpenVPN GUI 用戶端應用程式或 OpenVPN GUI Connect 用戶端建立用戶端 AWS 連線。如需建立憑證和金鑰的步驟，請參閱 在 Windows 上使用憑證建立 VPN 連線。

- macOS

  使用 macOS 型 Tunnelblick 或 AWS Client VPN 的組態檔案建立 VPN 連線。如需詳細資訊，請參閱在 macOS 上建立 VPN 連線。

- Linux

  使用 OpenVPN - Network Manager 介面或 OpenVPN 應用程式在 Linux 上建立 OpenVPN連線。若要使用 OpenVPN - Network Manager 介面，您必須先安裝尚未安裝的網路管理員模組。如需詳細資訊，請參閱在 Linux 上建立 VPN 連線。

- Android 和 iOS

  在 Android 或 iOS 裝置上使用 OpenVPN 用戶端應用程式建立 VPN 連線。如需更多資訊，請參閱Android 和 iOS 上的 Client VPN 連線。

> **Important**
>
> 如果 Client VPN 端點已設定為使用 SAML 型的聯合身分驗證，則您無法使用 OpenVPN 型 VPN 用戶端連線至 Client VPN 端點。這包括任何以 ARM 為基礎的架構。如果您使用具有 ARM 處理器的裝置（例如 Apple Silicon Mac 或 ARM 型 Windows 裝置），則必須搭配 AWS 提供的用戶端而非 OpenVPN 用戶端使用 SAML 型 VPN 端點。

用戶端應用程式

- 使用 Windows 用戶端應用程式連線至 AWS Client VPN 端點
- 使用 macOS 用戶端應用程式連線至 AWS Client VPN 端點
- 使用 OpenVPN 用戶端應用程式連線至 AWS Client VPN 端點

- AWS Client VPN Android 和 iOS 應用程式的 連線

使用 Windows 用戶端應用程式連線至 AWS Client VPN 端點

這些章節說明如何使用 Windows VPN 用戶端建立 VPN 連線。

開始之前，請確認您的 Client VPN 管理員已建立 Client VPN 端點，並已為您提供 Client VPN 端點組態檔案。如果您想要同時連線至多個設定檔，則每個設定檔都需要一個組態檔案。

如需故障診斷資訊，請參閱對使用 Windows 型用戶端的 AWS Client VPN 連線進行故障診斷。

> **Important**
>
> 如果 Client VPN 端點已設定為使用 SAML 型的聯合身分驗證，則您無法使用 OpenVPN 型 VPN 用戶端連線至 Client VPN 端點。這包括任何以 ARM 為基礎的架構。如果您使用具有 ARM 處理器的裝置（例如 Apple Silicon Mac 或 ARM 型 Windows 裝置），則必須搭配 AWS 提供的用戶端而非 OpenVPN 用戶端使用 SAML 型 VPN 端點。

任務

- 使用憑證並在 Windows 上建立 AWS Client VPN 連線

使用憑證並在 Windows 上建立 AWS Client VPN 連線

您可以將 OpenVPN 用戶端設定為使用 Windows 憑證系統存放區中的憑證和私密金鑰。當您使用智慧卡作為 Client VPN 連線的一部分時，此選項很有用。如需 OpenVPN 用戶端 cryptoapicert 選項的詳細資訊，請參閱 OpenVPN 網站上的 OpenVPN 參考手冊。

> **Note**
>
> 憑證必須存放在本機電腦上。

使用憑證並建立連線

1. 建立包含用戶端憑證和私密金鑰的 .pfx 檔案。
2. 將 .pfx 檔案匯入您的本機電腦上的個人憑證存放區。如需詳細資訊，請參閱 Microsoft 網站上的 How to: View certificates with the MMC snap-in。

3. 驗證您的帳戶具有讀取本機電腦憑證的權限。您可以使用 Microsoft 管理主控台來修改權限。如需詳細資訊，請參閱 Microsoft 網站上的查看本機電腦憑證存放區的權限。
4. 更新 OpenVPN 組態檔案，並使用憑證主體或憑證指紋指定憑證。

   以下是使用主體指定憑證的範例。

   ```
   cryptoapicert “SUBJ:Jane Doe”
   ```

   以下是使用指紋指定憑證的範例。您可以使用 Microsoft 管理主控台尋找指紋。如需詳細資訊，請參閱 Microsoft 網站上的如何：擷取憑證的指紋。

   ```
   cryptoapicert “THUMB:a5 42 00 42 01"
   ```

5. 完成組態後，請執行下列其中一項操作，使用 OpenVPN 建立 VPN 連線：

   - 使用 OpenVPN GUI 用戶端應用程式
     1. 啟動 OpenVPN 用戶端應用程式。
     2. 在 Windows 工作列上，選擇顯示/隱藏圖示。在 OpenVPN GUI 上按一下滑鼠右鍵，然後選擇匯入檔案。
     3. 在開啟對話方塊中，選取您從 Client VPN 管理員收到的組態檔案，然後選擇開啟。
     4. 在 Windows 工作列上，選擇顯示/隱藏圖示。在 OpenVPN GUI 上按一下滑鼠右鍵，然後選擇連線。

   - 使用 OpenVPN GUI Connect 用戶端
     1. 啟動 OpenVPN 應用程式，然後選擇匯入、從本機檔案...。
     2. 瀏覽至您從 VPN 管理員收到的組態檔案，然後選擇 Open (開啟)。

使用 macOS 用戶端應用程式連線至 AWS Client VPN 端點

這些章節說明如何使用 macOS 型 VPN 用戶端、Tunnelblick 或 AWS Client VPN 建立 VPN 連線。

開始之前，請確認您的 Client VPN 管理員已建立 Client VPN 端點，並已為您提供 Client VPN 端點組態檔案。如果您想要同時連線至多個設定檔，則每個設定檔都需要一個組態檔案。

如需故障診斷資訊，請參閱對與 macOS 用戶端的 AWS Client VPN 連線進行故障診斷。

> **Important**
>
> 如果 Client VPN 端點已設定為使用 SAML 型的聯合身分驗證，則您無法使用 OpenVPN 型 VPN 用戶端連線至 Client VPN 端點。這包括任何以 ARM 為基礎的架構。如果您使用具有 ARM 處理器的裝置（例如 Apple Silicon Mac 或 ARM 型 Windows 裝置），則必須搭配 AWS 提供的用戶端而非 OpenVPN 用戶端使用 SAML 型 VPN 端點。

主題

在 macOS 上建立 AWS Client VPN 連線

您可以在 macOS 電腦上使用 Tunnelblick 用戶端應用程式建立 VPN 連線。

> **Note**
>
> 如需適用於 macOS 的 Tunnelblick 用戶端應用程式的詳細資訊，請參閱 Tunnelblick 網站上的 Tunnelblick 文件。

使用 Tunnelblick 建立 VPN 連線

1. 啟動 Tunnelblick 用戶端應用程式，然後選擇我有組態檔案。
2. 在組態面板中，拖放您從 VPN 管理員收到的組態檔案。
3. 在組態面板中選取組態檔案，然後選擇連接。

使用 AWS Client VPN 建立 VPN 連線。

1. 啟動 OpenVPN 應用程式並選擇 Import (匯入)、From local file... (從本機檔案...)。
2. 瀏覽至您從 VPN 管理員收到的組態檔案，然後選擇 Open (開啟)。

使用 OpenVPN 用戶端應用程式連線至 AWS Client VPN 端點

這些章節說明如何使用 OpenVPN - Network Manager 或 OpenVPN 建立 VPN 連線。

開始之前，請確認您的 Client VPN 管理員已建立 Client VPN 端點，並已為您提供 Client VPN 端點組態檔案。如果您想要同時連線至多個設定檔，則每個設定檔都需要一個組態檔案。

如需故障診斷資訊，請參閱針對使用 Linux 型用戶端的 AWS Client VPN 連線進行故障診斷。

> **Important**
>
> 如果 Client VPN 端點已設定為使用 SAML 型的聯合身分驗證，則您無法使用 OpenVPN 型 VPN 用戶端連線至 Client VPN 端點。這包括任何以 ARM 為基礎的架構。如果您使用具有 ARM 處理器的裝置（例如 Apple Silicon Mac 或 ARM 型 Windows 裝置），則必須搭配 AWS 提供的用戶端而非 OpenVPN 用戶端使用 SAML 型 VPN 端點。

主題

在 Linux 上建立 AWS Client VPN 連線

使用 Ubuntu 電腦上的 Network Manager GUI 或 OpenVPN 應用程式，使用 建立 VPN 連線。

使用 OpenVPN - Network Manager 建立 VPN 連線

1. 使用以下命令安裝網路管理員模組。

```
sudo apt-get install --reinstall network-manager network-manager-gnome network-manager-openvpn network-manager-openvpn-gnome
```

2. 移至 Settings (設定)、Network (網路)。
3. 選擇 VPN 旁的加號 (+)，然後選擇 Import from file... (從檔案匯入...)。
4. 瀏覽至您從 VPN 管理員收到的組態檔案，然後選擇 Open (開啟)。
5. 在 Add VPN (新增 VPN) 視窗中，選擇 Add (新增)。
6. 啟用您新增之 VPN 設定檔旁邊的切換開關來啟動連線。

使用 OpenVPN 建立 VPN 連線

1. 使用以下命令安裝 OpenVPN。

```
sudo apt-get install openvpn
```

2. 載入您從 VPN 管理員收到的組態檔案，以啟動連接。

```
sudo openvpn --config /path/to/config/file
```

AWS Client VPN Android 和 iOS 應用程式的 連線

> **Important**
>
> 如果 Client VPN 端點已設定為使用 SAML 型的聯合身分驗證，則您無法使用 OpenVPN 型 VPN 用戶端連線至 Client VPN 端點。這包括任何以 ARM 為基礎的架構。如果您使用具有 ARM 處理器的裝置（例如 Apple Silicon Mac 或 ARM 型 Windows 裝置），則必須搭配 AWS 提供的用戶端而非 OpenVPN 用戶端使用 SAML 型 VPN 端點。

下列資訊說明如何在 Android 或 iOS 行動裝置上使用 OpenVPN 用戶端應用程式來建立 VPN 連接。適用於 Android 和 iOS 的步驟相同。

> **Note**
>
> 如需下載和使用適用於 iOS 或 Android 的 OpenVPN 用戶端應用程式的詳細資訊，請參閱 OpenVPN 網站上的 OpenVPN Connect 使用者指南。 OpenVPN

開始之前，請確認您的 Client VPN 管理員已建立 Client VPN 端點，並已為您提供 Client VPN 端點組態檔案。如果您想要同時連線至多個設定檔，則每個設定檔都需要一個組態檔案。

若要建立連線，請啟動 OpenVPN 用戶端應用程式，然後匯入從 Client VPN 管理員收到的檔案。

對 AWS Client VPN 連線進行故障診斷

使用下列主題，針對您使用用戶端應用程式連線到 Client VPN 端點時可能遇到的問題進行故障診斷。

主題

適用於管理員的 Client VPN 端點故障診斷

您可執行本指南中的某些步驟。其他步驟必須由您的 Client VPN 管理員在 Client VPN 端點上執行。下列各節可讓您知道何時需要聯絡系統管理員。

如需針對 Client VPN 端點問題進行故障診斷的其他資訊，請參閱《AWS Client VPN 管理員指南》中的針對 Client VPN 進行故障診斷。

在 AWS 提供的用戶端 AWS 支援 中將診斷日誌傳送至

如果您對 AWS 提供的用戶端有問題，而且需要聯絡 AWS 支援 來協助疑難排解，則 AWS 提供的用戶端可以選擇將診斷日誌傳送到 AWS 支援。此選項可在 Windows、macOS 和 Linux 用戶端應用程式上使用。

傳送檔案之前，您必須同意允許 AWS 支援 存取您的診斷日誌。在您同意之後，我們會提供您可以提供給 的參考號碼， AWS 支援 讓他們可以立即存取檔案。

傳送診斷日誌

在下列步驟中， AWS 提供的用戶端也稱為 AWS VPN 用戶端。

使用 AWS 提供的 Windows 用戶端傳送診斷日誌

1. 開啟 AWS VPN Client 應用程式。

2. 選擇 Help (說明) 和 Send Diagnostic Logs (傳送診斷日誌)。
3. 在 Send Diagnostic Logs (傳送診斷日誌) 視窗中，選擇 Yes (是)。
4. 在 Send Diagnostic Logs (傳送診斷日誌) 視窗中，執行以下其中一個操作：
   - 若要將參考編號複製到剪貼簿，請選擇 Yes (是)，然後選擇 OK (確定)。
   - 若要手動追蹤參考編號，請選擇 No (否)。

   當您聯絡 時 AWS 支援，您需要向他們提供參考號碼。

使用 macOS AWS 提供的用戶端傳送診斷日誌

1. 開啟 AWS VPN Client 應用程式。
2. 選擇 Help (說明) 和 Send Diagnostic Logs (傳送診斷日誌)。
3. 在 Send Diagnostic Logs (傳送診斷日誌) 視窗中，選擇 Yes (是)。
4. 請記下確認視窗中的參考編號，然後選擇 OK (確定)。

   當您聯絡 時 AWS 支援，您需要向他們提供參考號碼。

使用 Ubuntu AWS 提供的用戶端傳送診斷日誌

1. 開啟 AWS VPN Client 應用程式。
2. 選擇 Help (說明) 和 Send Diagnostic Logs (傳送診斷日誌)。
3. 在 Send Diagnostic Logs (傳送診斷日誌) 視窗中，選擇 Send (傳送)。
4. 請記下確認視窗中的參考編號。您可以選擇將資訊複製到剪貼簿。

   當您聯絡 時 AWS 支援，您需要向他們提供參考號碼。

對使用 Windows 型用戶端的 AWS Client VPN 連線進行故障診斷

以下各節針對您在使用 Windows 用戶端連線到 Client VPN 端點時可能會遇到的問題提供了相關資訊。

AWS 提供的用戶端事件日誌

AWS 提供的用戶端會建立事件日誌，並將其存放在您電腦上的下列位置。

```
C:\Users\User\AppData\Roaming\AWSVPNClient\logs
```

以下是可用的日誌類型：

- 應用程式日誌：包含應用程式的相關資訊。這些日誌的字首會加上 'aws_vpn_client_'。
- OpenVPN 日誌：包含 OpenVPN 程序的相關資訊。這些日誌的字首會加上 'ovpn_aws_vpn_client_'。

AWS 提供的用戶端使用 Windows 服務來執行根操作。Windows 服務日誌儲存在電腦的下列位置。

```
C:\Program Files\Amazon\AWS VPN Client\WinServiceLogs\username
```

故障診斷主題

- 用戶端無法連線
- 用戶端無法在出現「沒有 TAP-Windows 介面卡」日誌訊息的情況下連線
- 用戶端卡在重新連接狀態
- VPN 連接程序意外結束
- 應用程式無法啟動
- 用戶端無法建立設定檔
- VPN 與快顯訊息中斷連線
- 在使用 Windows 10 或 11 的 Dell PC 上發生用戶端當機
- OpenVPN GUI
- OpenVPN Connect Client
- 無法解析 DNS
- 遺失 PKI 別名

用戶端無法連線

問題

AWS 提供的用戶端無法連線至 Client VPN 端點。

原因

導致此問題的原因可能為下列其中一項：

- 另一個 OpenVPN 處理程序已在您的電腦上執行，這會阻止用戶端進行連接。
- 您的組態 (.ovpn) 檔案無效。

解決方案

檢查看看您的電腦上有沒有其他 OpenVPN 應用程式正在執行。如果有，請停止或結束這些程序，然後再次嘗試連線到 Client VPN 端點。檢查 OpenVPN 日誌中的錯誤項目，並要求您的 Client VPN 管理員驗證下列資訊：

- 組態檔案包含正確的用戶端金鑰和憑證。如需詳細資訊，請參閱《AWS Client VPN 管理員指南》中的匯出用戶端組態。
- CRL 仍然有效。如需詳細資訊，請參閱《AWS Client VPN 管理員指南》中的用戶端無法連線到 Client VPN 端點。

用戶端無法在出現「沒有 TAP-Windows 介面卡」日誌訊息的情況下連線

問題

AWS 提供的用戶端無法連線至 Client VPN 端點，且應用程式日誌中會顯示下列錯誤訊息：「此系統上沒有 TAP-Windows 轉接器。您可前往「開始 -> 所有程式 -> TAP-Windows -> 公用程式 -> 新增 TAP-Windows 虛擬乙太網路介面卡」，這樣應該就能建立 TAP-Windows 介面卡。

解決方案

您可以採取下列其中一個或多個動作來解決此問題：

- 重新啟動 TAP-Windows 介面卡。
- 重新安裝 TAP-Windows 驅動程式。
- 建立新的 TAP-Windows 介面卡。

用戶端卡在重新連接狀態

問題

AWS 提供的用戶端正在嘗試連線至 Client VPN 端點，但卡在重新連線狀態。

原因

導致此問題的原因可能為下列其中一項：

- 您的電腦未連線到網際網路。
- DNS 主機名稱不會解析為 IP 地址。
- OpenVPN 處理程序正在無限期地嘗試連接到端點。

解決方案

確定您的電腦已連線至網際網路。請您的 Client VPN 管理員驗證組態檔案中的 `remote` 指令可以解析為有效的 IP 地址。您也可以在 VPN 用戶端視窗中選擇中斷連線，然後再次嘗試連線，以中斷 AWS VPN 工作階段的連線。

VPN 連接程序意外結束

問題

連線到 Client VPN 端點時，用戶端意外結束。

原因

TAP-Windows 未安裝在您的電腦上。需要此軟體才能執行用戶端。

解決方案

重新執行 AWS 提供的用戶端安裝程式，以安裝所有必要的相依性。

應用程式無法啟動

問題

在 Windows 7 上， AWS 提供的用戶端不會在您嘗試開啟時啟動。

原因

您的電腦上未安裝 .NET Framework 4.7.2 或更高版本。這是執行用戶端的必要項目。

解決方案

重新執行 AWS 提供的用戶端安裝程式，以安裝所有必要的相依性。

用戶端無法建立設定檔

問題

當您使用 AWS 提供的用戶端嘗試建立描述檔時，發生下列錯誤。

```
The config should have either cert and key or auth-user-pass specified.
```

原因

如果 Client VPN 端點使用交互身分驗證，則組態 (.ovpn) 檔案便不會包含用戶端憑證和金鑰。

解決方案

請確定您的 Client VPN 管理員將用戶端憑證和金鑰新增至組態檔案。如需詳細資訊，請參閱《AWS Client VPN 管理員指南》中的匯出用戶端組態。

VPN 與快顯訊息中斷連線

問題

VPN 會中斷連線，並顯示快顯訊息：「VPN 連線正在終止，因為您裝置連線的本機網路地址空間已變更。請建立新的 VPN 連線。」

原因

TAP-Windows 轉接器不包含必要的描述。

解決方案

如果 `Description` 欄位與下列不相符，請先移除 TAP-Windows 轉接器，然後重新執行 AWS 提供的用戶端安裝程式，以安裝所有必要的相依性。

```
C:\Users\jdoe> ipconfig /all

Ethernet adapter Ethernet 2:

Media State . . . . . . . . . . . : Media disconnected
Connection-specific DNS Suffix  . :
```

```
Description . . . . . . . . . . . : AWS VPN Client TAP-Windows Adapter V9
Physical Address. . . . . . . . . : 00-FF-50-ED-5A-DE
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
```

在使用 Windows 10 或 11 的 Dell PC 上發生用戶端當機

問題

在執行 Windows 10 或 11 的某些 Dell PC (桌上型和筆記型) 上，當您瀏覽檔案系統來匯入 VPN 組態檔案時，可能會發生當機的情況。如果發生此問題，您會在 AWS 提供的用戶端日誌中看到如下的訊息：

```
System.AccessViolationException: Attempted to read or write protected memory. This is
 often an indication that other memory is corrupt.
   at System.Data.SQLite.UnsafeNativeMethods.sqlite3_open_interop(Byte[] utf8Filename,
 Int32 flags, IntPtr& db)
   at System.Data.SQLite.SQLite3.Open(String strFilename, SQLiteConnectionFlags
 connectionFlags, SQLiteOpenFlagsEnum openFlags, Int32 maxPoolSize, Boolean usePool)
   at System.Data.SQLite.SQLiteConnection.Open()
   at
 STCommonShellIntegration.DataShellManagement.CreateNewConnection(SQLiteConnection&
 newConnection)
   at STCommonShellIntegration.DataShellManagement.InitConfiguration(Dictionary`2
 targetSettings)
   at DBROverlayIcon.DBRBackupOverlayIcon.initComponent()
```

原因

Windows 10 和 11 中的 Dell Backup and Recovery 系統可能會導致與 AWS 所提供用戶端的衝突，特別是與下列三個 DLLs的衝突：

- DBRShellExtension.dll
- DBROverlayIconBackuped.dll
- DBROverlayIconNotBackuped.dll

解決方案

為了避免此問題，請先確認您的用戶端是最新版本的 AWS 用戶端。前往 AWS Client VPN 下載，若可取得較新的版本，請升級至最新版。

此外，請執行下列作業：

- 如果您使用的是 Dell Backup and Recovery 應用程式，請務必使用最新版。一篇 Dell 論壇文章聲明此問題已在較新版的應用程式中解決。
- 如果您沒有使用 Dell Backup and Recovery 應用程式，如果您遇到此問題，仍需採取一些動作。如果您不希望升級應用程式，則可以刪除或重新命名 DLL 檔案。但是，請注意，這會使得 Dell Backup and Recovery 應用程式難以順暢運作。

刪除或重新命名 DLL 檔案

1. 前往 Windows 檔案總管並瀏覽到 Dell Backup and Recovery 的安裝位置。此應用程式通常會安裝在下列位置，但您可能需要搜尋才能找出來。

   ```
   C:\Program Files (x86)\Dell Backup and Recovery\Components\Shell
   ```

2. 從安裝目錄手動刪除下列 DLL 檔案，或重新命名這些檔案。任何一項動作皆會使這些檔案無法載入。

   - DBRShellExtension.dll
   - DBROverlayIconBackuped.dll
   - DBROverlayIconNotBackuped.dll

   您可以透過在檔案名稱結尾加上「.bak」來重新命名這些檔案，例如 DBROverlayIconBackuped.dll.bak。

OpenVPN GUI

下列故障診斷資訊已在 Windows 10 家用版 (64 位元) 和 Windows Server 2016 (64 位元) 的 OpenVPN GUI 軟體 11.10.0.0 和 11.11.0.0 版上經過測試。

組態檔案儲存在電腦的下列位置。

```
C:\Users\User\OpenVPN\config
```

連線日誌儲存在電腦的下列位置。

```
C:\Users\User\OpenVPN\log
```

OpenVPN Connect Client

下列故障診斷資訊已在 Windows 10 家用版 (64 位元) 和 Windows Server 2016 (64 位元) 的 OpenVPN Connect Client 軟體 2.6.0.100 和 2.7.1.101 版上經過測試。

組態檔案儲存在電腦的下列位置。

```
C:\Users\User\AppData\Roaming\OpenVPN Connect\profile
```

連線日誌儲存在電腦的下列位置。

```
C:\Users\User\AppData\Roaming\OpenVPN Connect\logs
```

無法解析 DNS

問題

連線失敗，並出現下列錯誤。

```
Transport Error: DNS resolve error on 'cvpn-endpoint-xyz123.prod.clientvpn.us-
east-1.amazonaws.com (http://cvpn-endpoint-xyz123.prod.clientvpn.us-
east-1.amazonaws.com/)' for UDP session: No such host is known.
```

原因

無法解析 DNS 名稱。用戶端必須在 DNS 名稱前面加上隨機字串，以防止 DNS 快取；不過，某些用戶端不會這樣做。

解決方案

請參閱《AWS Client VPN 管理員指南》中無法解析 Client VPN 端點 DNS 名稱的解決方案。

遺失 PKI 別名

問題

與不使用交互身分驗證 Client VPN 端點的連線失敗，並顯示下列錯誤。

```
FATAL:CLIENT_EXCEPTION: connect error: Missing External PKI alias
```

原因

OpenVPN Connect Client 軟體有一個已知的問題，它會嘗試使用交互身分驗證進行驗證。如果組態檔案不包含用戶端金鑰和憑證，身分驗證會失敗。

解決方案

在 Client VPN 組態檔案中指定隨機用戶端金鑰和憑證，然後將新組態匯入 OpenVPN Connect Client 軟體。您也可以使用不同的用戶端，例如 OpenVPN GUI 用戶端 (v11.12.0.0) 或 Viscosity 用戶端 (v.1.7.14)。

對與 macOS 用戶端的 AWS Client VPN 連線進行故障診斷

以下各節針對記錄和您使用 macOS 用戶端時可能遇到的問題提供了相關資訊。請確定您執行的是這些用戶端的最新版本。

AWS 提供的用戶端事件日誌

AWS 提供的用戶端會建立事件日誌，並將其存放在您電腦上的下列位置。

```
/Users/username/.config/AWSVPNClient/logs
```

以下是可用的日誌類型：

- 應用程式日誌：包含應用程式的相關資訊。這些日誌的字首會加上 'aws_vpn_client_'。
- OpenVPN 日誌：包含 OpenVPN 程序的相關資訊。這些日誌的字首會加上 'ovpn_aws_vpn_client_'。

AWS 提供的用戶端使用用戶端協助程式來執行根操作。協助程式日誌儲存在電腦的下列位置。

```
/var/log/AWSVPNClient/AcvcHelperErrLog.txt
/var/log/AWSVPNClient/AcvcHelperOutLog.txt
```

AWS 提供的用戶端會將組態檔案存放在您電腦上的下列位置。

```
/Users/username/.config/AWSVPNClient/OpenVpnConfigs
```

故障診斷主題

- 用戶端無法連線
- 用戶端卡在重新連接狀態
- 用戶端無法建立設定檔
- 協助程式工具為必要錯誤
- Tunnelblick
- 找不到密碼演算法 'AES-256-GCM'
- 連線停止回應並重設
- 擴充金鑰使用方法 (EKU)
- 過期的憑證
- OpenVPN
- 無法解析 DNS

用戶端無法連線

問題

AWS 提供的用戶端無法連線至 Client VPN 端點。

原因

導致此問題的原因可能為下列其中一項：

- 另一個 OpenVPN 處理程序已在您的電腦上執行，這會阻止用戶端進行連接。
- 您的組態 (.ovpn) 檔案無效。

解決方案

檢查看看您的電腦上有沒有其他 OpenVPN 應用程式正在執行。如果有，請停止或結束這些程序，然後再次嘗試連線到 Client VPN 端點。檢查 OpenVPN 日誌中的錯誤項目，並要求您的 Client VPN 管理員驗證下列資訊：

- 組態檔案包含正確的用戶端金鑰和憑證。如需詳細資訊，請參閱《AWS Client VPN 管理員指南》中的匯出用戶端組態。
- CRL 仍然有效。如需詳細資訊，請參閱《AWS Client VPN 管理員指南》中的用戶端無法連線到 Client VPN 端點。

用戶端卡在重新連接狀態

問題

AWS 提供的用戶端正在嘗試連線至 Client VPN 端點，但停滯在重新連線狀態。

原因

導致此問題的原因可能為下列其中一項：

- 您的電腦未連線到網際網路。
- DNS 主機名稱不會解析為 IP 地址。
- OpenVPN 處理程序正在無限期地嘗試連接到端點。

解決方案

確定您的電腦已連線至網際網路。請您的 Client VPN 管理員驗證組態檔案中的 `remote` 指令可以解析為有效的 IP 地址。您也可以在 VPN 用戶端視窗中選擇中斷連線，然後再次嘗試連線，以中斷 AWS VPN 工作階段的連線。

用戶端無法建立設定檔

問題

當您使用 AWS 提供的用戶端嘗試建立描述檔時，發生下列錯誤。

```
The config should have either cert and key or auth-user-pass specified.
```

原因

如果 Client VPN 端點使用交互身分驗證，則組態 (.ovpn) 檔案便不會包含用戶端憑證和金鑰。

解決方案

請確定您的 Client VPN 管理員將用戶端憑證和金鑰新增至組態檔案。如需詳細資訊，請參閱《AWS Client VPN 管理員指南》中的匯出用戶端組態。

協助程式工具為必要錯誤

問題

當您嘗試連接 VPN 時，出現下列錯誤。

```
AWS VPN Client Helper Tool is required to establish the connection.
```

解決方案

請參閱下列有關 AWS re：Post 的文章。AWS VPN 用戶端 - 協助程式工具為必要錯誤

Tunnelblick

下列故障診斷資訊已在 macOS High Sierra 10.13.6 版的 Tunnelblick 軟體 3.7.8 版 (組建 5180) 上經過測試。

私有組態的組態檔案儲存在電腦的下列位置。

```
/Users/username/Library/Application Support/Tunnelblick/Configurations
```

共用組態的組態檔儲存在電腦的下列位置。

```
/Library/Application Support/Tunnelblick/Shared
```

連線日誌儲存在電腦的下列位置。

```
/Library/Application Support/Tunnelblick/Logs
```

若要提高日誌詳細程度，請開啟 Tunnelblick 應用程式、選擇 Settings (設定)，然後調整 VPN log level (VPN 日誌層級) 的值。

找不到密碼演算法 'AES-256-GCM'

問題

連線失敗，並在日誌中傳回下列錯誤。

```
2019-04-11 09:37:14 Cipher algorithm 'AES-256-GCM' not found
2019-04-11 09:37:14 Exiting due to fatal error
```

原因

應用程式使用的是不支援密碼演算法 AES-256-GCM 的 OpenVPN 版本。

解決方案

請執行以下步驟，選擇相容的 OpenVPN 版本：

1. 開啟 Tunnelblick 應用程式。
2. 選擇設定。
3. 對於 OpenVPN version (OpenVPN 版本)，請選擇 2.4.6 - OpenSSL version is v1.0.2q (2.4.6 - OpenSSL 版本是 v1.0.2q)。

連線停止回應並重設

問題

連線失敗，並在日誌中傳回下列錯誤。

```
MANAGEMENT: >STATE:1559117927,WAIT,,,,,,
MANAGEMENT: >STATE:1559117928,AUTH,,,,,,
TLS: Initial packet from [AF_INET]3.217.107.5:443, sid=df19e70f a992cda3
VERIFY OK: depth=1, CN=server-certificate
VERIFY KU OK
Validating certificate extended key usage
Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server
 Authentication
VERIFY EKU OK
VERIFY OK: depth=0, CN=server-cvpn
Connection reset, restarting [0]
SIGUSR1[soft,connection-reset] received, process restarting
```

原因

用戶端憑證已被撤銷。嘗試驗證後，連線會停止回應，並最終從伺服器端重設。

解決方案

向您的 Client VPN 管理員要求新的組態檔案。

擴充金鑰使用方法 (EKU)

問題

連線失敗，並在日誌中傳回下列錯誤。

```
TLS: Initial packet from [AF_INET]50.19.205.135:443, sid=29f2c917 4856ad34
VERIFY OK: depth=2, O=Digital Signature Trust Co., CN=DST Root CA X3
VERIFY OK: depth=1, C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
VERIFY KU OK
Validating certificate extended key usage
 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server
 Authentication
VERIFY EKU OK
VERIFY OK: depth=0, CN=cvpn-lab.myrandomnotes.com (http://cvpn-lab.myrandomnotes.com/)
Connection reset, restarting [0]
SIGUSR1[soft,connection-reset] received, process restarting
MANAGEMENT: >STATE:1559138717,RECONNECTING,connection-reset,,,,,
```

原因

伺服器身分驗證成功。不過，用戶端身分驗證失敗，因為用戶端憑證已啟用伺服器身分驗證的擴充金鑰使用方法 (EKU) 欄位。

解決方案

請確定您使用的是正確的用戶端憑證和金鑰。如有必要，請與您的 Client VPN 管理員驗證。如果您正在使用伺服器憑證，而非用戶端憑證來連線到 Client VPN 端點，便可能發生此錯誤。

過期的憑證

問題

伺服器驗證成功，但用戶端身分驗證失敗，並顯示下列錯誤。

```
WARNING: “Connection reset, restarting [0] , SIGUSR1[soft,connection-reset] received,
 process restarting”
```

原因

用戶端憑證有效性已過期。

解決方案

向您的 Client VPN 管理員要求新的用戶端憑證。

OpenVPN

下列故障診斷資訊已在 macOS High Sierra 10.13.6 的 OpenVPN Connect Client 軟體 2.7.1.100 版上經過測試。

組態檔案儲存在電腦的下列位置。

```
/Library/Application Support/OpenVPN/profile
```

連線日誌儲存在電腦的下列位置。

```
Library/Application Support/OpenVPN/log/connection_name.log
```

無法解析 DNS

問題

連線失敗，並出現下列錯誤。

```
Mon Jul 15 13:07:17 2019 Transport Error: DNS resolve error on 'cvpn-
endpoint-1234.prod.clientvpn.us-east-1.amazonaws.com' for UDP session: Host not found
 (authoritative)
Mon Jul 15 13:07:17 2019 Client terminated, restarting in 2000 ms...
Mon Jul 15 13:07:18 2019 CONNECTION_TIMEOUT [FATAL-ERR]
Mon Jul 15 13:07:18 2019 DISCONNECTED
Mon Jul 15 13:07:18 2019 >FATAL:CONNECTION_TIMEOUT
```

原因

OpenVPN Connect 無法解析 Client VPN DNS 名稱。

解決方案

請參閱《AWS Client VPN 管理員指南》中無法解析 Client VPN 端點 DNS 名稱的解決方案。

針對使用 Linux 型用戶端的 AWS Client VPN 連線進行故障診斷

以下各節針對記錄和您使用 Linux 用戶端時可能遇到的問題提供了相關資訊。請確定您執行的是這些用戶端的最新版本。

主題

AWS 提供的用戶端事件日誌

AWS 提供的用戶端會將日誌檔案和組態檔案存放在系統上的下列位置：

```
/home/username/.config/AWSVPNClient/
```

AWS 提供的用戶端協助程式程序會將日誌檔案存放在您系統的下列位置：

```
/var/log/aws-vpn-client/
```

例如，您可以檢查下列日誌檔，尋找 DNS 上/下指令碼中導致連線失敗的錯誤：

- `/var/log/aws-vpn-client/configure-dns-up.log`
- `/var/log/aws-vpn-client/configure-dns-down.log`

DNS 查詢會移至預設的 nameserver

問題

在某些情況下，建立 VPN 連線之後，DNS 查詢仍會前往預設的系統名稱伺服器，而不是針對 ClientVPN 端點設定的名稱伺服器。

原因

用戶端會與 systemd-resolved 互動，這是 Linux 系統上提供的服務，作為 DNS 管理的中心部分。其用途為設定從 ClientVPN 端點推送的 DNS 伺服器。發生問題的原因在於 systemd-resolved 不會為 ClientVPN 端點所提供的 DNS 伺服器設定最高優先順序。相反地，它會將伺服器附加至本機系統上所設定的現有 DNS 伺服器清單。因此，原始 DNS 伺服器可能仍然具有最高優先順序，而用於解析 DNS 查詢。

解決方案

1. 在 OpenVPN 組態檔第一行新增以下指示詞，確保所有 DNS 查詢都傳送至 VPN 通道。

```
dhcp-option DOMAIN-ROUTE .
```

2. 使用 systemd-resolved 提供的虛設常式解析程式。方法是在系統上執行下列命令，建立 `/etc/resolv.conf` 至 `/run/systemd/resolve/stub-resolv.conf` 的符號連結。

```
sudo ln -sf /run/systemd/resolve/stub-resolv.conf /etc/resolv.conf
```

3. (選用) 如果您不希望 systemd-resolved 代理 DNS 查詢，而是要讓查詢直接傳送至真正的 DNS 名稱伺服器，則建立 `/etc/resolv.conf` 至 `/run/systemd/resolve/resolv.conf` 的符號連結。

```
sudo ln -sf /run/systemd/resolve/resolv.conf /etc/resolv.conf
```

建議您執行此程序，以便針對諸如 DNS 回應快取、個別介面 DNS 設定、DNSec 強制等作業略過 systemd-resolved 組態。當您需要在連線至 VPN 時使用私有記錄覆寫公有 DNS 記錄時，此選項特別有用。例如，您的私有 VPC 中可能有一個私有 DNS 解析程式，其中包含可解析為私有 IP 的 www.example.com 記錄。此選項可用來覆寫可解析為公有 IP 的 www.example.com 公有記錄。

OpenVPN (命令列)

問題

因為 DNS 解析無法運作，所以連線無法正常運作。

原因

未在 Client VPN 端點上設定 DNS 伺服器，或是用戶端軟體未遵守該伺服器。

解決方案

請使用下列步驟來檢查 DNS 伺服器是否已設定且正常運作。

1. 請確定 DNS 伺服器項目存在於日誌中。在以下範例中，最後一行傳回 DNS 伺服器 `192.168.0.2` (於 Client VPN 端點中設定)。

```
Mon Apr 15 21:26:55 2019 us=274574 SENT CONTROL [server]: 'PUSH_REQUEST' (status=1)
```

```
WRRMon Apr 15 21:26:55 2019 us=276082 PUSH: Received control message:
 'PUSH_REPLY,redirect-gateway def1 bypass-dhcp,dhcp-option DNS 192.168.0.2,route-
gateway 10.0.0.97,topology subnet,ping 1,ping-restart 20,auth-token,ifconfig
 10.0.0.98 255.255.255.224,peer-id 0
```

如果未指定任何 DNS 伺服器，請要求您的 Client VPN 管理員修改 Client VPN 端點，確認已為 Client VPN 端點指定 DNS 伺服器 (例如 VPC DNS 伺服器)。如需詳細資訊，請參閱《AWS Client VPN 管理員指南》中的 Client VPN 端點。

2. 請執行下列命令，確定已安裝 `resolvconf` 套件。

```
sudo apt list resolvconf
```

輸出應該會傳回以下內容。

```
Listing... Done
resolvconf/bionic-updates,now 1.79ubuntu10.18.04.3 all [installed]
```

如果未安裝，請使用以下命令安裝它。

```
sudo apt install resolvconf
```

3. 在文字編輯器中開啟 Client VPN 組態檔案 (.ovpn 檔案)，然後新增下列幾行。

```
script-security 2
up /etc/openvpn/update-resolv-conf
down /etc/openvpn/update-resolv-conf
```

檢查日誌以確認 `resolvconf` 指令碼是否已被叫用。日誌應該包含類似下列的行。

```
Mon Apr 15 21:33:52 2019 us=795388 /etc/openvpn/update-resolv-conf tun0 1500 1552
 10.0.0.98 255.255.255.224 init
dhcp-option DNS 192.168.0.2
```

透過網路管理員的 OpenVPN (GUI)

問題

使用網路管理員 OpenVPN 用戶端時，連線失敗，並出現下列錯誤。

```
Apr 15 17:11:07  OpenVPN 2.4.4 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL]
 [PKCS11] [MH/PKTINFO] [AEAD] built on Sep  5 2018
Apr 15 17:11:07  library versions: OpenSSL 1.1.0g  2 Nov 2017, LZO 2.08
Apr 15 17:11:07  RESOLVE: Cannot resolve host address: cvpn-
endpoint-1234.prod.clientvpn.us-east-1.amazonaws.com:443 (Name or service not known)
Apr 15 17:11:07  RESOLVE: Cannot resolve host
Apr 15 17:11:07  Could not determine IPv4/IPv6 protocol
```

原因

`remote-random-hostname` 旗標不會生效，且用戶端無法使用 `network-manager-gnome` 套件進行連線。

解決方案

請參閱《AWS Client VPN 管理員指南》中無法解析 Client VPN 端點 DNS 名稱的解決方案。

疑難排解常見的 AWS Client VPN 問題

以下是您在使用用戶端連線到 Client VPN 端點時，可能會遇到的常見問題。

TLS 金鑰交涉失敗

問題

TLS 交涉失敗，並出現下列錯誤。

```
TLS key negotiation failed to occur within 60 seconds (check your network connectivity)
TLS Error: TLS handshake failed
```

原因

導致此問題的原因可能為下列其中一項：

- 防火牆規則封鎖 UDP 或 TCP 流量。
- 您在組態 (.ovpn) 檔案中使用了不正確的用戶端金鑰和憑證。
- 用戶端憑證撤銷清單 (CRL) 已過期。

解決方案

檢查看看電腦的防火牆規則是否封鎖連接埠 443 或 1194 上的傳入或傳出 TCP 或 UDP 流量。請要求您的 Client VPN 管理員驗證下列資訊：

- Client VPN 端點的防火牆規則未封鎖連接埠 443 或 1194 上的 TCP 或 UDP 流量。
- 組態檔案包含正確的用戶端金鑰和憑證。如需詳細資訊，請參閱《AWS Client VPN 管理員指南》中的匯出用戶端組態。
- CRL 仍然有效。如需詳細資訊，請參閱《AWS Client VPN 管理員指南》中的用戶端無法連線到 Client VPN 端點。

文件歷史記錄

下表說明 AWS Client VPN 使用者指南更新。

變更	描述	日期
AWS 已發行 Windows ARM64 和 x64 的 提供用戶端 (5.3.7)	請參閱版本備註取得詳細資訊。	2026 年 6 月 15 日
AWS 已發行 Windows ARM64 和 x64 的 提供用戶端 (5.3.6)	請參閱版本備註取得詳細資訊。	2026 年 5 月 28 日
AWS 已發行 Windows ARM64 和 x64 的 提供用戶端 (5.3.5)	請參閱版本備註取得詳細資訊。	2026 年 5 月 27 日
AWS 為 Ubuntu 提供的用戶端 (5.3.3) 已發行	請參閱版本備註取得詳細資訊。	2026 年 5 月 18 日
AWS 已發行 macOS ARM64 和 x64 的 提供用戶端 (5.3.5)	請參閱版本備註取得詳細資訊。	2026 年 5 月 14 日
AWS 已發行 Windows ARM64 和 x64 的 提供用戶端 (5.3.4)	請參閱版本備註取得詳細資訊。	2026 年 3 月 26 日
AWS 已發行 Windows ARM64 和 x64 的 提供用戶端 (5.3.3)	請參閱版本備註取得詳細資訊。	2026 年 2 月 28 日
AWS 為 macOS ARM64 和 x64 提供的用戶端 (5.3.4) 已發行	請參閱版本備註取得詳細資訊。	2026 年 2 月 17 日
AWS 已發行 Windows ARM64 和 x64 的 提供用戶端 (5.3.2)	請參閱版本備註取得詳細資訊。	2026 年 2 月 17 日
AWS 為 macOS ARM64 和 x64 提供的用戶端 (5.3.3) 已發行	請參閱版本備註取得詳細資訊。	2025 年 12 月 26 日

AWS 已發行 Ubuntu 的 提供用戶端 (5.3.2)	請參閱版本備註取得詳細資訊。	2025 年 12 月 17 日
AWS 為 macOS x64 提供的用戶端 (5.3.2) 已發行	請參閱版本備註取得詳細資訊。	2025 年 10 月 27 日
AWS 為發行的 macOS ARM64 系統提供用戶端 (5.3.2)	macOS ARM64-based現在已新增支援。這包括專門用於 macOS ARM64 系統的新 5.3.2 AWS Client VPN 版下載。如需詳細資訊，請參閱 Client VPN 以取得 macOS 需求，以及下載連結AWS Client VPN 的 macOS 版本備註。	2025 年 10 月 27 日
AWS 已發行 Windows x64 和 Arm64 的 提供用戶端 (5.3.1)	請參閱版本備註取得詳細資訊。	2025 年 9 月 30 日
AWS 提供的 macOS 用戶端現在支援 Tahoe (26.0)	如需詳細資訊，請參閱需求。	2025 年 9 月 25 日
AWS 已發行 Ubuntu 的 提供用戶端 (5.3.1)	請參閱版本備註取得詳細資訊。	2025 年 9 月 25 日
AWS 為發行的 macOS 提供用戶端 (5.3.1)	請參閱版本備註取得詳細資訊。	2025 年 9 月 9 日
AWS 已發行 Windows Arm64 系統的 提供用戶端 (5.3.0)	現在已新增 Windows Arm64-based的支援。這包括專門針對 Windows Arm64 系統下載的新 AWS Client VPN 版本 5.3.0。如需更多詳細資訊，請參閱 Client VPN for Windows 需求，以及下載連結的 AWS Client VPN for Windows 版本備註。	2025 年 8 月 26 日

AWS 為發行的 macOS 提供用戶端 (5.3.0)	請參閱版本備註取得詳細資訊。	2025 年 8 月 14 日
AWS 針對 Windows 提供的用戶端 (5.3.0) 已發行	請參閱版本備註取得詳細資訊。	2025 年 8 月 14 日
AWS 為 Ubuntu 提供的用戶端 (5.3.0) 已發行	請參閱版本備註取得詳細資訊。	2025 年 8 月 14 日
AWS 針對發行的 macOS 提供用戶端 (5.2.1)	請參閱版本備註取得詳細資訊。	2025 年 6 月 18 日
AWS 針對 Windows 提供的用戶端 (5.2.2) 已發行	請參閱版本備註取得詳細資訊。	2025 年 6 月 2 日
AWS 針對 Windows 提供的用戶端 (5.2.1) 已發行	請參閱版本備註取得詳細資訊。	2025 年 4 月 21 日
AWS 針對發行的 macOS 提供用戶端 (5.2.0)	請參閱版本備註取得詳細資訊。	2025 年 4 月 8 日
AWS 針對 Windows 提供的用戶端 (5.2.0) 已發行	請參閱版本備註取得詳細資訊。	2025 年 4 月 8 日
AWS Ubuntu 提供的用戶端 (5.2.0) 已發行	請參閱版本備註取得詳細資訊。	2025 年 4 月 8 日
AWS 為發行的 macOS 提供用戶端 (5.1.0)	請參閱版本備註取得詳細資訊。	2025 年 3 月 17 日
AWS 已發行 Windows 的 提供用戶端 (5.1.0)	請參閱版本備註取得詳細資訊。	2025 年 3 月 17 日
AWS 已發行 Ubuntu 的 提供用戶端 (5.1.0)	請參閱版本備註取得詳細資訊。	2025 年 3 月 17 日
已移除對 macOS Monterey 的支援，並新增對 macOS Sonoma (14.0) 的支援	如需詳細資訊，請參閱 Client VPN 以取得 macOS 需求。	2025 年 3 月 12 日

已移除對 Ubuntu 18.0.4 (LTS) 和 Ubuntu 20.04 LTS （僅限 AMD64) 的支援	如需詳細資訊，請參閱 Client VPN for Linux 需求。	2025 年 3 月 12 日
AWS 為發行的 macOS 提供用戶端 (5.0.3)	請參閱版本備註取得詳細資訊。	2025 年 3 月 6 日
AWS 針對 Windows 提供的用戶端 (5.0.2) 已發行	請參閱版本備註取得詳細資訊。	2025 年 2 月 24 日
AWS 針對發行的 macOS 提供用戶端 (5.0.2)	請參閱版本備註取得詳細資訊。	2025 年 2 月 17 日
AWS 已發行 Windows 的 提供用戶端 (5.0.1)	請參閱版本備註取得詳細資訊。	2025 年 1 月 30 日
AWS 針對發行的 macOS 提供用戶端 (5.0.1)	請參閱版本備註取得詳細資訊。	2025 年 1 月 22 日
AWS 提供的用戶端現在支援最多五個並行連線	如需詳細資訊，請參閱使用 AWS 提供的用戶端支援並行連線。	2025 年 1 月 21 日
AWS 針對發行的 macOS 提供用戶端 (5.0.0)	請參閱版本備註取得詳細資訊。	2025 年 1 月 21 日
AWS 已發行 Windows 的 提供用戶端 (5.0.0)	請參閱版本備註取得詳細資訊。	2025 年 1 月 21 日
AWS 已發行 Ubuntu 的 提供用戶端 (5.0.0)	請參閱版本備註取得詳細資訊。	2024 年 11 月 12 日
AWS 為發行的 macOS 提供用戶端 (4.1.0)	請參閱版本備註取得詳細資訊。	2024 年 11 月 12 日
AWS 已發行 Windows 的 提供用戶端 (4.1.0)	請參閱版本備註取得詳細資訊。	2024 年 11 月 12 日
AWS Ubuntu 提供的用戶端 (4.1.0) 已發行	請參閱版本備註取得詳細資訊。	2024 年 11 月 12 日

AWS 為發行的 macOS 提供用戶端 (4.0.0)	請參閱版本備註取得詳細資訊。	2024 年 9 月 25 日
AWS 已發行 Windows 的 提供用戶端 (4.0.0)	請參閱版本備註取得詳細資訊。	2024 年 9 月 25 日
AWS Ubuntu 提供的用戶端 (4.0.0) 已發行	請參閱版本備註取得詳細資訊。	2024 年 9 月 25 日
AWS 已發行 Ubuntu 的 提供用戶端 (3.15.1)	請參閱版本備註取得詳細資訊。	2024 年 9 月 4 日
AWS 針對 Windows 提供的用戶端 (3.14.2) 已發行	請參閱版本備註取得詳細資訊。	2024 年 9 月 4 日
AWS 針對發行的 macOS 提供用戶端 (3.12.1)	請參閱版本備註取得詳細資訊。	2024 年 9 月 4 日
AWS 已發行 Windows 的 提供用戶端 (3.14.1)	請參閱版本備註取得詳細資訊。	2024 年 8 月 22 日
AWS 已發行 Ubuntu 的 提供用戶端 (3.15.0)	請參閱版本備註取得詳細資訊。	2024 年 8 月 12 日
AWS 針對 Windows 提供的用戶端 (3.14.0) 已發行	請參閱版本備註取得詳細資訊。	2024 年 8 月 12 日
AWS 為發行的 macOS 提供用戶端 (3.12.0)	請參閱版本備註取得詳細資訊。	2024 年 8 月 12 日
AWS 已發行 Ubuntu 的 提供用戶端 (3.14.0)	請參閱版本備註取得詳細資訊。	2024 年 7 月 29 日
AWS 已發行 Windows 的 提供用戶端 (3.13.0)	請參閱版本備註取得詳細資訊。	2024 年 7 月 29 日
AWS 提供的 macOS 用戶端 (3.11.0) 已發行	請參閱版本備註取得詳細資訊。	2024 年 7 月 29 日

AWS 已發行 Windows 的 提供用戶端 (3.12.1)	請參閱版本備註取得詳細資訊。	2024 年 7 月 18 日
AWS 已發行 Ubuntu 的 提供用戶端 (3.13.0)	請參閱版本備註取得詳細資訊。	2024 年 5 月 21 日
AWS 已發行 Windows 的 提供用戶端 (3.12.0)	請參閱版本備註取得詳細資訊。	2024 年 5 月 21 日
AWS 針對發行的 macOS 提供用戶端 (3.10.0)	請參閱版本備註取得詳細資訊。	2024 年 5 月 21 日
AWS 為發行的 macOS 提供用戶端 (3.9.2)	請參閱版本備註取得詳細資訊。	2024 年 4 月 11 日
AWS 為 Ubuntu 提供的用戶端 (3.12.2) 已發行	請參閱版本備註取得詳細資訊。	2024 年 4 月 11 日
AWS 已發行 Windows 的 提供用戶端 (3.11.2)	請參閱版本備註取得詳細資訊。	2024 年 4 月 11 日
AWS 為發行的 macOS 提供用戶端 (3.9.1)	請參閱版本備註取得詳細資訊。	2024 年 2 月 16 日
AWS 已發行 Ubuntu 的 提供用戶端 (3.12.1)	請參閱版本備註取得詳細資訊。	2024 年 2 月 16 日
AWS 已發行 Windows 的 提供用戶端 (3.11.1)	請參閱版本備註取得詳細資訊。	2024 年 2 月 16 日
AWS 已發行 Ubuntu 的 提供用戶端 (3.12.0)	請參閱版本備註取得詳細資訊。	2023 年 12 月 19 日
AWS 為發行的 macOS 提供用戶端 (3.9.0)	請參閱版本備註取得詳細資訊。	2023 年 12 月 6 日
AWS 已發行 Windows 的 提供用戶端 (3.11.0)	請參閱版本備註取得詳細資訊。	2023 年 12 月 6 日

AWS 已發行 Ubuntu 的 提供用戶端 (3.11.0)	請參閱版本備註取得詳細資訊。	2023 年 12 月 6 日
AWS 已發行 Ubuntu 的 提供用戶端 (3.10.0)	請參閱版本備註取得詳細資訊。	2023 年 12 月 6 日
AWS Ubuntu 提供的用戶端 (3.9.0) 已發行	請參閱版本備註取得詳細資訊。	2023 年 8 月 24 日
AWS 針對發行的 macOS 提供用戶端 (3.8.0)	請參閱版本備註取得詳細資訊。	2023 年 8 月 24 日
AWS 針對 Windows 提供的用戶端 (3.10.0) 已發行	請參閱版本備註取得詳細資訊。	2023 年 8 月 24 日
AWS 已發行 Windows 的 提供用戶端 (3.9.0)	請參閱版本備註取得詳細資訊。	2023 年 8 月 3 日
AWS 已發行 Ubuntu 的 提供用戶端 (3.8.0)	請參閱版本備註取得詳細資訊。	2023 年 8 月 3 日
AWS 為發行的 macOS 提供用戶端 (3.7.0)	請參閱版本備註取得詳細資訊。	2023 年 8 月 3 日
AWS 針對 Windows 提供的用戶端 (3.8.0) 已發行	請參閱版本備註取得詳細資訊。	2023 年 7 月 15 日
AWS 針對 Windows 提供的用戶端 (3.7.0) 已發行	請參閱版本備註取得詳細資訊。	2023 年 7 月 15 日
AWS 已發行 Ubuntu 的 提供用戶端 (3.7.0)	請參閱版本備註取得詳細資訊。	2023 年 7 月 15 日
AWS 為發行的 macOS 提供用戶端 (3.6.0)	請參閱版本備註取得詳細資訊。	2023 年 7 月 15 日
AWS Ubuntu 提供的用戶端 (3.6.0) 已發行	請參閱版本備註取得詳細資訊。	2023 年 7 月 15 日

AWS 針對發行的 macOS 提供用戶端 (3.5.0)	請參閱版本備註取得詳細資訊。	2023 年 7 月 15 日
AWS 已發行 Windows 的 提供用戶端 (3.6.0)	請參閱版本備註取得詳細資訊。	2023 年 7 月 14 日
AWS Ubuntu 提供的用戶端 (3.5.0) 已發行	請參閱版本備註取得詳細資訊。	2023 年 7 月 14 日
AWS 為發行的 macOS 提供用戶端 (3.4.0)	請參閱版本備註取得詳細資訊。	2023 年 7 月 14 日
AWS 為發行的 macOS 提供用戶端 (3.3.0)	請參閱版本備註取得詳細資訊。	2023 年 4 月 27 日
AWS 已發行 Windows 的 提供用戶端 (3.5.0)	請參閱版本備註取得詳細資訊。	2023 年 4 月 3 日
AWS 針對 Windows 提供的用戶端 (3.4.0) 已發行	請參閱版本備註取得詳細資訊。	2023 年 3 月 28 日
AWS 針對 Windows 提供的用戶端 (3.3.0) 已發行	請參閱版本備註取得詳細資訊。	2023 年 3 月 17 日
AWS Ubuntu 提供的用戶端 (3.4.0) 已發行	請參閱版本備註取得詳細資訊。	2023 年 2 月 14 日
AWS 針對發行的 macOS 提供用戶端 (3.2.0)	請參閱版本備註取得詳細資訊。	2023 年 1 月 23 日
AWS 針對 Windows 提供的用戶端 (3.2.0) 已發行	請參閱版本備註取得詳細資訊。	2023 年 1 月 23 日
AWS 為發行的 macOS 提供用戶端 (3.1.0)	請參閱版本備註取得詳細資訊。	2022 年 5 月 23 日
AWS 已發行 Windows 的 提供用戶端 (3.1.0)	請參閱版本備註取得詳細資訊。	2022 年 5 月 23 日

AWS 已發行 Ubuntu 的 提供用戶端 (3.1.0)	請參閱版本備註取得詳細資訊。	2022 年 5 月 23 日
AWS 為發行的 macOS 提供用戶端 (3.0.0)	請參閱版本備註取得詳細資訊。	2022 年 3 月 3 日
AWS 針對 Windows 提供的用戶端 (3.0.0) 已發行	請參閱版本備註取得詳細資訊。	2022 年 3 月 3 日
AWS 已發行 Ubuntu 的 提供用戶端 (3.0.0)	請參閱版本備註取得詳細資訊。	2022 年 3 月 3 日
AWS 為發行的 macOS 提供用戶端 (2.0.0)	請參閱版本備註取得詳細資訊。	2022 年 1 月 20 日
AWS 針對 Windows 提供的用戶端 (2.0.0) 已發行	請參閱版本備註取得詳細資訊。	2022 年 1 月 20 日
AWS 已發行 Ubuntu 的 提供用戶端 (2.0.0)	請參閱版本備註取得詳細資訊。	2022 年 1 月 20 日
AWS 為發行的 macOS 提供用戶端 (1.4.0)	請參閱版本備註取得詳細資訊。	2021 年 11 月 9 日
AWS 提供的 Windows 用戶端 (1.3.7) 已發行	請參閱版本備註取得詳細資訊。	2021 年 11 月 8 日
AWS 已發行 Ubuntu 的 提供用戶端 (1.0.3)	請參閱版本備註取得詳細資訊。	2021 年 11 月 8 日
AWS 已發行 Ubuntu 的 提供用戶端 (1.0.2)	請參閱版本備註取得詳細資訊。	2021 年 9 月 28 日
AWS 針對 Windows (1.3.6) 和 macOS (1.3.5) 提供的用戶端已發行	請參閱版本備註取得詳細資訊。	2021 年 9 月 20 日
AWS 為發行的 Ubuntu 18.04 LTS 和 Ubuntu 20.04 LTS 提供用戶端	您可以在 Ubuntu 18.04 LTS 和 Ubuntu 20.04 LTS 上使用AWS提供的用戶端。	2021 年 6 月 11 日

支援 OpenVPN 使用 Windows 憑證系統存放區中的憑證	您可以透過 Windows 憑證系統存放區中的憑證使用 OpenVPN。	2021 年 2 月 25 日
自助式入口網站	您可以存取自助式入口網站，以取得最新的 AWS 用戶端和組態檔案。	2020 年 10 月 29 日
AWS 提供的用戶端	您可以使用 AWS 提供的用戶端連線到 Client VPN 端點。	2020 年 2 月 4 日
初始版本	此版本推出 AWS Client VPN。	2018 年 12 月 18 日

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。