aws

使用者指南

Amazon One Enterprise

Amazon One Enterprise: 使用者指南

Table of Contents

什麼是 Amazon 一個企業？

Amazon One Enterprise 是全新掌上型身分驗證服務，可讓員工安全地存取建築物和企業資產，而無需使用徽章或密碼。PINs

主題

Amazon 一台設備

Amazon One 裝置專為 Amazon One 企業設計，這是一種安全的掌上型身分服務，可用於企業存取控制。請注意下列裝置規格：

- 用戶輸入 — 棕櫚生物識別技術，QR 碼匹配
- 主機介面 — 無線網路 (2.4 GHz 和 5GHz)、乙太網路、2 USB 個 A 型、1 USB 種 B 型
- 用戶反饋-5.5」觸摸屏，打火機，揚聲器，耳機
- 物理訪問控制協議-OSDP 和韋根
- 電源供應器 —POE, 提供 110/220 VAC 輸入交流轉直流變壓器, 30 瓦 @ 15V
- 安全性 — 竄改開關
- 尺寸 (HxWx深毫米) — 86 x 85 x 256

Amazon 企業控制台一

Amazon One 企業版包含一個主控台，可透過下列方式使用：

- IT 或設施管理員使用 Amazon One 企業版來建立和管理網站。該網站類似於團隊在監控和管理 Amazon One 企業裝置和使用者設定檔時執行的任務的實體位置。IT 或設施管理員的工作包括：
  - 建立網站以包含實體位置中的所有 Amazon One 裝置執行個體
  - 添加管理員用戶來管理網站，並添加安裝程序用戶訪問激活 QR 碼
- 管理員使用 Amazon One 企業版建立裝置執行個體和管理 Amazon One 裝置。管理員工作包括：
  - 在網站下建立裝置執行個體
  - 創建要應用於設備實例的配置模板
  - 監控裝置健康狀況並更新裝置設定
  - 取消使用者註冊

- 安裝程式使用 Amazon One 企業版存取啟用 QR 碼以啟用裝置。安裝程式工作包括：
  - 在主機上存取啟用 QR 碼
  - 選擇與要激活的設備實例對應的 QR 碼
  - 在安裝 Amazon One 設備的情況下掃描選定的 QR 碼

購買 Amazon 一個設備

請聯絡我們以進一步了解 Amazon One Enterprise，業務開發團隊成員將與我們聯絡，分享有關我們產品的更多詳細資訊，包括定價，並回答您可能遇到的任何問題。

Amazon 一個企業定價

請聯絡我們以進一步了解 Amazon One 企業版定價。

Amazon One Enterprise 的運作方式

Amazon One Enterprise 是一種雲端生物識別服務，使用 Amazon One 裝置來驗證使用者的手掌生物識別。您可以聯絡我們 來訂購 Amazon One 裝置，而且您可以在 中註冊 Amazon One Enterprise 安全存取服務 AWS Management Console。

安裝 Amazon One Enterprise 後，您可以在 Amazon One Enterprise Console 和身分驗證應用程式 AWS 帳戶 上啟用裝置，並將其註冊至 。從主控台中，您可以檢視已註冊員工的生物特徵描述檔，並取消員工的註冊。當員工離開公司或遺失識別證時，您可以刪除其生物識別資料。

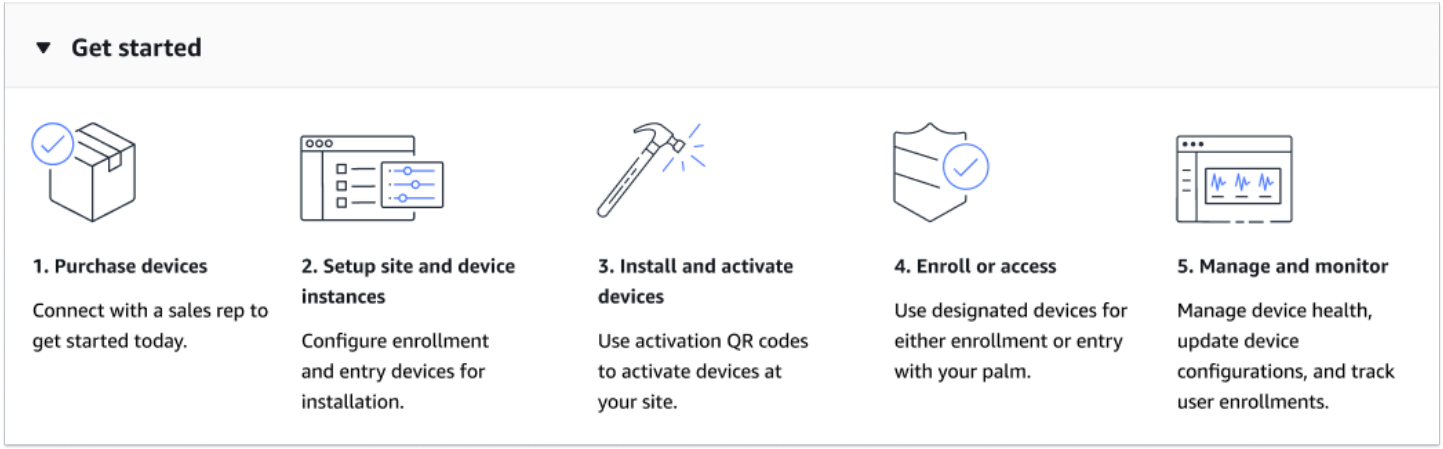
Amazon One Enterprise Console 也可作為管理操作活動的集中位置，例如追蹤已安裝的裝置和檢視每月帳單。

員工可以在現場的受監督註冊站掃描其識別證和手掌來註冊。員工註冊後，可以將手掌放在 Amazon One 裝置上以進入或離開安全位置。

主題

Amazon One Enterprise 工作流程

下圖顯示 Amazon One Enterprise 的基本工作流程。



1. 聯絡我們購買 Amazon One 裝置。
2. 建立網站和裝置執行個體、設定註冊和輸入裝置以進行安裝。
3. 安裝後，請掃描裝置執行個體特有的安全 QR 碼，以啟用 Amazon One 裝置。

4. 要求員工註冊他們的手掌，然後用他們的手掌進行身分驗證以取得存取權。
5. 使用管理和監控功能：確保裝置運作狀態、保持組態為最新狀態，並追蹤使用者註冊以進行全面監督。

Amazon One Enterprise 金鑰術語

以下是 Amazon One Enterprise 的關鍵術語：

- 網站 — 客戶安裝 Amazon One Enterprise 裝置的客戶受管實體建築。網站必須符合 Amazon One Enterprise 裝置的設施、聯網和電源需求。
- 裝置 — 用於身分驗證的 Amazon One Enterprise 掌上掃描生物識別裝置。
- 裝置執行個體 — 具有組態之裝置的邏輯表示法。使用裝置執行個體允許交換 Amazon One 裝置，同時自動繼承先前設定的組態和名稱。裝置執行個體具有使用者定義的名稱（與您的存取控制軟體共用命名慣例）和一組通訊組態。裝置執行個體有三種主要狀態：
  - 需要組態
  - 準備啟用
  - 作用中
- 組態範本 — 套用至裝置執行個體的全包式組態集。

設定 Amazon One Enterprise

本章說明開始使用 Amazon One Enterprise 的基本步驟。

設定網站、裝置執行個體和組態範本 — 請依照下列步驟建立架構，以新增實體位置來存放 Amazon One 裝置，然後使用 Amazon One Enterprise 主控台設定和管理它們。視網站數量、裝置執行個體和組態範本而定，您只會偶爾或甚至只使用一次此程序。

主題

註冊 AWS 帳戶。

如果您沒有 AWS帳戶，請完成下列步驟以建立帳戶。

註冊AWS帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup
2. 請遵循線上指示進行。

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   當您註冊AWS帳戶時，會建立AWS帳戶根使用者。根使用者可存取 帳戶中的所有 AWS 服務和資源。作為安全最佳實務，將管理存取權指派給使用者，並僅使用根使用者來執行需要根使用者存取權的任務

AWS 會在註冊程序完成後傳送確認電子郵件給您。您可以隨時前往 並選擇我的帳戶，以檢視您目前的帳戶活動https://aws.amazon.com/並管理您的帳戶

建立具有管理存取權的使用者

註冊AWS帳戶後，請保護AWS帳戶根使用者的安全、啟用 AWS IAM Identity Center，並建立管理使用者，以免將根使用者用於日常任務。

主題

保護AWS您的帳戶

現在您已登入 Amazon One Enterprise 帳戶，請保護您的帳戶。

保護AWS您的帳戶根使用者

1. 選擇根使用者並輸入AWS您的帳戶電子郵件地址，以帳戶擁有者身分登入 AWS Management Console。
2. 在下一頁中，輸入您的密碼。

   如需使用根使用者登入的協助，請參閱登入使用者指南中的以根使用者AWS身分登入。
3. 為您的根使用者開啟多重要素驗證（MFA）。

   如需指示，請參閱 IAM 使用者指南中的為AWS您的帳戶根使用者（主控台）啟用虛擬MFA裝置。

建立具有管理存取權的使用者

現在您已保護 Amazon One Enterprise 帳戶，請建立具有管理存取權的使用者。

建立具有管理存取權的使用者

1. 啟用IAM身分中心。

   如需指示，請參閱AWSIAM身分中心使用者指南中的啟用AWSIAM身分中心。
2. 在 IAM Identity Center 中，將管理存取權授予使用者。

如需使用 IAM Identity Center 目錄作為身分來源的教學課程，請參閱AWSIAM身分中心使用者指南中的使用預設 IAM Identity Center 目錄設定使用者存取權。

以管理員身分登入

現在您已建立具有管理存取權的使用者，請以管理員身分登入。

以具有管理存取權的使用者身分登入

- 使用您建立 IAM Identity Center URL 使用者時傳送到您電子郵件地址的登入資料，與 IAM Identity Center 使用者登入。

  如需使用 IAM Identity Center 使用者登入的協助，請參閱AWS登入使用者指南中的登入AWS存取入口網站。

將存取權指派給其他使用者

現在您已以管理員身分登入，您可以將存取權指派給其他使用者。

將存取權指派給其他使用者

- 將使用者指派至群組，然後對該群組指派單一登入存取權。

  如需指示，請參閱AWSIAM身分中心使用者指南中的新增群組。

新增 Amazon One Enterprise 使用者

除了管理員使用者之外，您也可以新增缺少管理員許可的使用者。例如，這些使用者可能是僅存取 Amazon One Enterprise 主控台以擷取裝置啟用 QR 碼以啟用 Amazon One 裝置的安裝程式。

新增 Amazon One Enterprise 使用者

1. 請遵循 AWS AWS 登入 使用者指南 中如何登入 中所述，適用於您使用者類型的登入程序。
2. 在導覽窗格中，選取使用者 ，然後選取新增使用者 。
3. 在 指定使用者詳細資訊 頁面 使用者詳細資訊 下方的 使用者名稱 中輸入新使用者的名稱。這是新使用者的 AWS登入名稱。

> **Note**
>
> 中的IAM資源數量和大小 AWS 帳戶 有限。如需詳細資訊，請參閱 IAM和 AWS STS 配額 。使用者名稱最多可包含 64 個字母、數字和下列字元：加號 （ + ）、等於 （ = ）、逗號 （ , ）、句點 （ . ）、符號 （ @ ）、底線 （ _ ） 和連字號 （ - ）。名稱在帳戶中必須是唯一的。它們無法透過大小寫進行區分。例如，您無法建立名為 TESTUSER的兩個使用者和測試使用者 。當使用者名稱用於政策或 的一部分時ARN，名稱會區分大小寫。當主控台中的客戶顯示使用者名稱時 (例如在登入程序期間)，使用者名稱不區分大小寫。

4. 系統會詢問您是否要向使用者提供主控台存取。選取提供使用者存取 - AWS Management Console 選用 。
5. 選取我想要建立IAM使用者 。
6. 在 主控台密碼 中選取下列其中一個選項：
   - 自動產生的密碼 – 使用者會收到符合帳戶密碼政策 的隨機產生的密碼。您可在進入 擷取密碼 頁面時檢視或下載密碼。
   - 自訂密碼 – 系統會將您在欄位中輸入的密碼指派給使用者。
7. （選用） 根據預設，使用者必須在下次登入時建立新密碼 （ 建議），以確保使用者在第一次登入時必須變更密碼。

> **Note**
>
> 如果管理員已啟用 允許使用者變更自己的密碼 帳戶密碼政策設定，則此核取方塊不會執行任何動作。否則，它會自動將名為的 `IAMUserChangePassword` AWS 受管政策連接到新使用者。政策會授予他們變更自己密碼的許可。

8. 選取 下一步。
9. 在設定許可頁面上，選擇直接連接政策。
10. 選取您要附加至使用者的政策。
    - AmazonOneEnterpriseReadOnlyAccess
    - AmazonOneEnterpriseInstallerAccess

> **Note**
>
> AmazonOneEnterpriseInstallerAccess 受管政策只會在 Amazon One Enterprise 主控台中提供使用者啟用 QR 碼的存取權。此政策非常適合雇用第三方安裝 Amazon One 裝置的企業。

11. 選取下一步。
12. (選用) 在 檢閱和建立 頁面的 標籤 下方選擇 新增標籤，透過將標籤做為鍵值對連接，來將中繼資料新增至使用者。如需在 中使用標籤的詳細資訊IAM，請參閱標記IAM資源 。
13. 檢閱您到目前為止所做的所有選擇。準備好繼續時，請選取 建立使用者。
14. 在 擷取密碼 頁面上取得指派給使用者的密碼：
    - 選取密碼旁邊的 顯示 來檢視使用者的密碼，以便手動記錄密碼。
    - 選取下載 .csv，將使用者的登入憑證下載為 .csv 檔案，您可以將其儲存到安全的位置。
15. 選取 電子郵件登入指示。您的本機郵件用戶端會開啟可供您自訂和傳送給使用者的草稿。電子郵件範本包含每位使用者的以下詳細資訊：
    - 使用者名稱
    - URL 帳戶登入頁面。使用以下範例，取代正確的帳戶 ID 號碼或帳戶別名：

      ```
      https://AWS-account-ID or alias.signin.aws.amazon.com/console
      ```

> **Important**
>
> 使用者的密碼不會包含在產生的電子郵件中。您必須以遵循組織安全準則的方式向使用者提供密碼。

建立網站

現在您已登入 AWS Management Console，您可以使用 Amazon One Enterprise 主控台來建立您的網站。

> **Important**
>
> Amazon One Enterprise 僅適用於美國東部（維吉尼亞北部）區域。

建立網站

1. 在 https://console.aws.amazon.com/one-enterprise 開啟 Amazon One Enterprise 主控台。
2. 選擇前往概觀。
3. 在導覽窗格中，選擇 Sites (網站)。
4. 選擇建立網站。
5. 在站台資訊 下，針對站台名稱 輸入站台的名稱。
6. 在實體地址 下，輸入要安裝 Amazon One 裝置的網站地址。
7. （選用）若要將標籤新增至網站，請在標籤 下輸入鍵值對，然後選擇新增標籤。若要在建立網站之前移除此標籤，請選擇移除。
8. 選擇建立網站以建立網站。

建立裝置執行個體

現在您已在AWS管理主控台中建立網站，您可以使用 Amazon One Enterprise 主控台來建立裝置執行個體。

建立裝置執行個體

1. 在 https://console.aws.amazon.com/one-enterprise 開啟 Amazon One Enterprise 主控台。
2. 在導覽窗格中，選擇裝置執行個體。請確定您在未啟用的執行個體索引標籤上。
3. 在執行個體詳細資訊 下，從網站下拉式清單中選擇網站，或選擇建立網站按鈕來建立新網站。
4. 手動輸入每個個別的裝置執行個體名稱。
5. （選用）若要將標籤新增至裝置執行個體，請在標籤 下輸入鍵值對，然後選擇新增標籤。若要在建立裝置執行個體之前移除此標籤，請選擇移除。
6. 選擇建立執行個體以建立裝置執行個體。

> **Note**
>
> 注意：裝置執行個體需要先設定，才能進行安裝。

建立組態範本

現在您已建立裝置執行個體，您可以使用 Amazon One Enterprise 主控台來建立組態範本。

建立組態範本

1. 在 https://console.aws.amazon.com/one-enterprise 開啟 Amazon One Enterprise 主控台。
2. 在導覽窗格中，選擇組態範本 。
3. 選擇建立範本。
4. 在範本資訊 下，針對範本名稱 輸入組態範本的名稱。
5. 在裝置組態 下，選取操作模式 。

   To configure Enrollment operating mode

   1. （選用）在 Wifi 組態 下，提供您的 Wifi 憑證 。
   2. （選用）若要將標籤新增至網站，請在標籤 下輸入鍵值對，然後選擇新增標籤 。若要在建立網站之前移除此標籤，請選擇移除 。
   3. 選擇設定。

   To configure Entry operating mode

   1. 在控制面板設定 下，提供 Amazon One 裝置的通訊設定，以便與您的控制面板通訊。
   2. 在證卡格式設定 下，提供指定公司證卡格式配置的組態設定。
   3. （選用）在 Wifi 組態 下，提供您的 Wifi 憑證 。
   4. （選用）若要將標籤新增至網站，請在標籤 下輸入鍵值對，然後選擇新增標籤 。若要在建立網站之前移除此標籤，請選擇移除 。
   5. 選擇設定。

> **Important**
>
> 您必須設定至少一個 Enrollment 裝置和一個 Entry 裝置，才能啟用 Amazon One Enterprise 的完整功能，以便安全存取。

設定裝置執行個體以啟用

建立裝置執行個體後，您可以使用先前建立的組態範本來設定裝置執行個體（請參閱 建立組態範本），也可以手動新增組態。

設定裝置執行個體以啟用

1. 在 https://console.aws.amazon.com/one-enterprise 開啟 Amazon One Enterprise 主控台。
2. 在導覽窗格中，選擇裝置執行個體 。確保您位於未啟用的執行個體索引標籤上。
3. 選取要設定的一或多個執行個體。
4. 選擇設定。
5. 在裝置組態 下，選取下列兩種輸入方法之一：

   a. 針對使用範本選項，從下拉式清單中選擇範本。檢閱或變更此匯入的組態資訊。

      如需建立範本選項，請參閱 建立組態範本。

   b. 針對手動輸入選項，選取操作模式 。

      To configure Enrollment operating mode

      a. （選用）在 Wifi 組態 下，提供 Wifi 憑證 。
      b. （選用）若要將標籤新增至網站，請在標籤 下輸入鍵值對，然後選擇新增標籤 。若要在建立網站之前移除此標籤，請選擇移除 。
      c. 選擇設定。

      To configure Entry operating mode

      a. 在控制面板設定 下，提供 Amazon One 裝置的通訊設定，以便與您的控制面板通訊。
      b. 在證卡格式設定 下，提供指定公司證卡格式配置的組態設定。
      c. （選用）在 Wifi 組態 下，提供 Wifi 憑證 。

d. （選用）若要將標籤新增至網站，請在標籤 下輸入鍵值對，然後選擇新增標籤 。若要在建立網站之前移除此標籤，請選擇移除 。

e. 選擇設定。

6. 在未啟用執行個體資料表下，執行個體狀態應會顯示

。

7. 驗證啟用 QR 碼是否可供啟用。在導覽窗格中，選擇啟用 QR 碼 。
8. 從選取站台下拉式清單中，選取站台 。
9. 在站台資訊 下，驗證站台地址。
10. 在啟用 QR 碼 下，每個裝置執行個體都有對應的 QR 碼。選擇取得 QR 碼以顯示啟用 QR 碼。

> **Important**
>
> 您必須設定至少一個 Enrollment 裝置和一個 Entry 裝置，才能啟用 Amazon One Enterprise 的完整功能，以便安全存取。

安裝和啟用 Amazon One

設定 Amazon One Enterprise 主控台後，後續步驟是在您的網站上安裝 Amazon One Enterprise 裝置，然後啟用它們。

> **Note**
>
> 本節著重於安裝，並使用行動瀏覽器存取 AWS Management Console 以取得裝置啟用 QR 碼。

主題

了解需求

Amazon One 裝置可以安裝在具有可電氣控制之門的任何公司或商業位置。

控制面板需求

Amazon One 裝置可以作為讀取器連線至大多數標準存取控制面板。Amazon One 裝置支援下列通訊協定：

- OSDP （v1 和 v2）
- Wiegand

網路需求

Amazon One 裝置必須一律連接至網際網路才能正常運作。網際網路連線可由有線乙太網路或 Wi-Fi 提供。所需的最小頻寬為 10 Mbps。

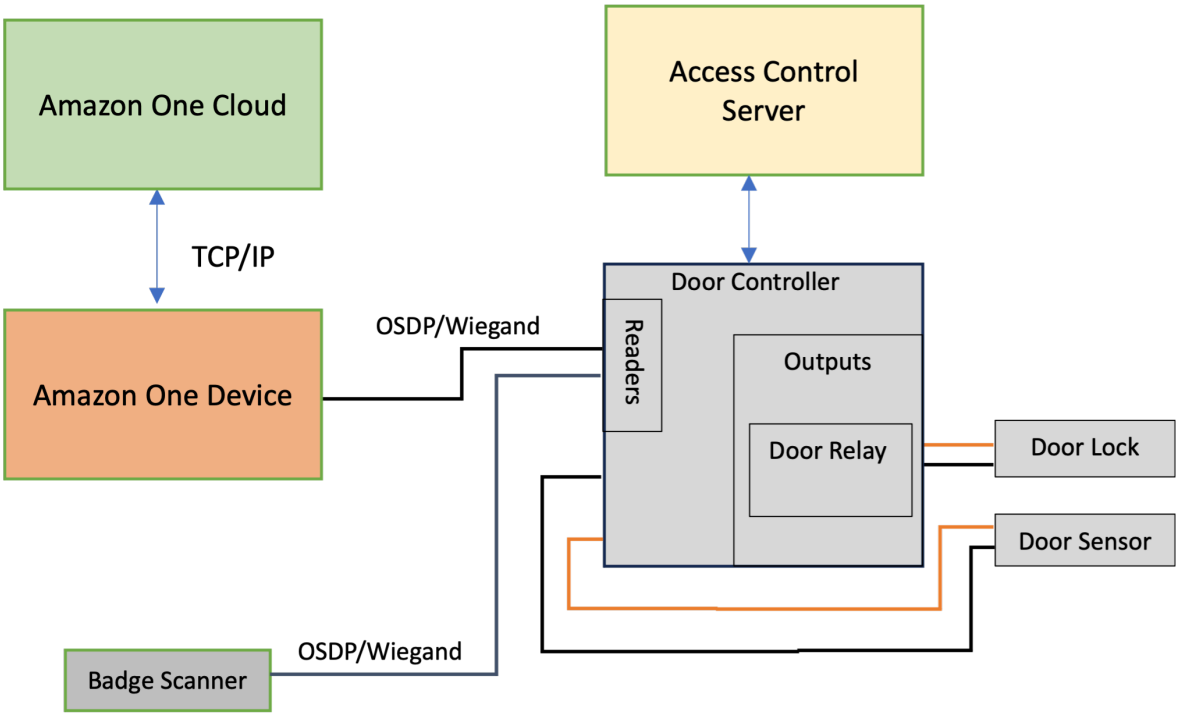
電源需求

Amazon One 裝置可以透過下列兩種方式之一來供電：

- 使用 方塊中提供的 120V 電源轉接器。
- 使用啟用 PoE + 的裝置。

了解安裝概念

為了正確保護建築物存取，Amazon One Enterprise 建議您將裝置安裝為典型存取控制環境的一部分，如下列區塊圖所述。



存取控制環境通常包含下列元件：

- Amazon One 裝置：這是掌上型識別裝置，將執行生物識別身分驗證，以識別嘗試存取建築物安全區域的個人。
- 存取控制伺服器：此元件通常會控制使用者對安全區域的存取權。有權存取該區域的IDs個人徽章通常存放在此伺服器上。此伺服器會快取IDs與適當 門控制器相關的 。
- 門控制器：
  - Amazon One 裝置會透過OSDP介面連線至 門控制器伺服器。
  - 如果需要 Wiegand 介面，則可使用COTS OSDP-to-Wiegand轉換器。

- 成功驗證後，Amazon One 裝置會將使用者的徽章 ID 傳送至門控制器。
- 門控控制器會回應 決策，然後允許 Amazon One 裝置顯示 Access Granted 或 Access Denied 訊息。

- 徽章掃描器：徽章掃描器通常用於掃描RFID徽章，並將徽章號碼傳送至存取控制伺服器。使用 Amazon One Enterprise，徽章掃描器會連線至 Enrollment Amazon One 裝置，以便掃描員工的徽章，並與他們的掌上型設定檔建立關聯。

安裝 Amazon One Enterprise 底座

本節概述安裝 Amazon One Enterprise 底座所需的位置需求和步驟。

開始安裝之前，請確定符合下列先決條件：

- 如果使用 POE+ 為裝置供電，請確保已配置 Cat6 佈線，且 POE+ 注入器或開關可供使用。
- 如果使用 AC 電源（120V）來源，AC AOE 插座應在台的 20 英尺內可用。
- 樓層必須保持水平且乾淨。
- 底座不得封鎖門或通道。
- 所有多餘的纜線應存放在底座內並加以固定。

安裝 Amazon One 裝置底座

1. 從包裝中移除 Amazon One Enterprise 底座。
2. 鬆開兩個 M4 防撥弄螺絲以移除機門。
3. 插入電源線。將纜線穿過底座底板中的孔。
4. 將底座內任何多餘的電源線進行線圈。
5. 將乙太網路纜線（Cat5E 或更高版本）穿過底座的底部板，然後插入乙太網路連接埠。
6. 將乙太網路纜線（Cat5E 或更高版本）穿過底座的底部板，然後插入乙太網路連接埠。
7. 將鐵氧體迴圈安裝在乙太網路纜線上，位於底座底部上方 2 英吋處。
8. 將RS485序列纜線從存取控制面板（或徽章讀取器）饋送至底座，長度超過 1 英尺。
9. 在底座底部上方 2 英吋的RS485電纜上安裝鐵氧體迴圈。
10. 將插座接上電源，並確認 Amazon One 裝置已開啟。
11. 將機門重新連接至底座，然後重新旋緊兩個 M4 防撥弄螺絲以固定。

安裝壁掛式 Amazon One 裝置

本節詳細說明安裝壁掛式 Amazon One 裝置所需的位置需求和步驟。

開始安裝之前，請確定下列事項：

- 壁掛式 Amazon One 裝置僅供室內使用。
- 牆壁是水平的。
- 掛載後，壁掛式的頂端不應高於地面 44-46 英吋。
- 所有多餘的纜線都位於壁掛式後方並固定。
- 對於乙太網路供電（PoE ++）：

確保 IEEE 802.3bt （類型 3） Class 6 POE++ 交換器 （跨度結束） 或注入器 （跨度中） 可供使用，其已列出或認證，並符合 IEC 62368-1。

只能AOE與核准的 PoE ++ 來源搭配使用。

PoE ++ 來源必須位於相同的建築物內。

- 對於 15V DC 電源輸入，您只能將 Amazon One 裝置與 2 NEC類或列出或認證的電源限制核准電源供應器搭配使用。

必要工具：

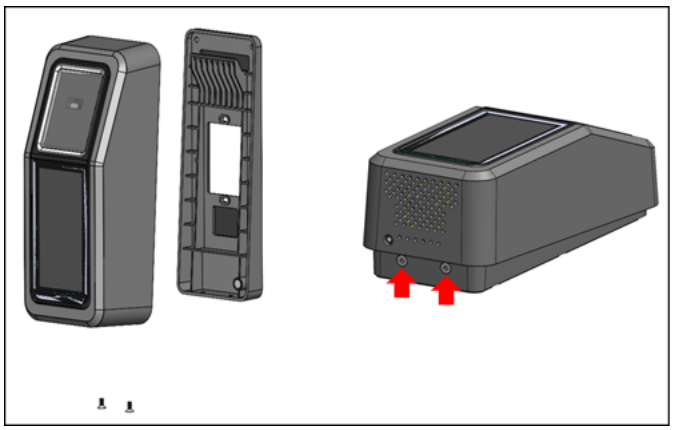
- 如果需要壁錨，請使用 1/4 英吋乾壁或磚工打孔鑽頭
- 剝線器
- 7/64 英吋鑽頭，用於鑽探試驗孔
- #2 Phillips 螺絲起子
- 0.5 公釐 x 2 公釐一字螺絲起子
- T12 安全 Torx 驅動程式
- 鉛筆
- Level

隨附於壁掛式 Amazon One 裝置：

- 6x #8 Drywall 錨點
- 6x #8-32 1in 長螺絲
- 2 個 #6-32 1 英寸機器螺絲
- 2x 6 位置端子台連接器
- 2 個 Torx Security M4x10 平頭螺絲

安裝 Amazon One 裝置的壁掛式板

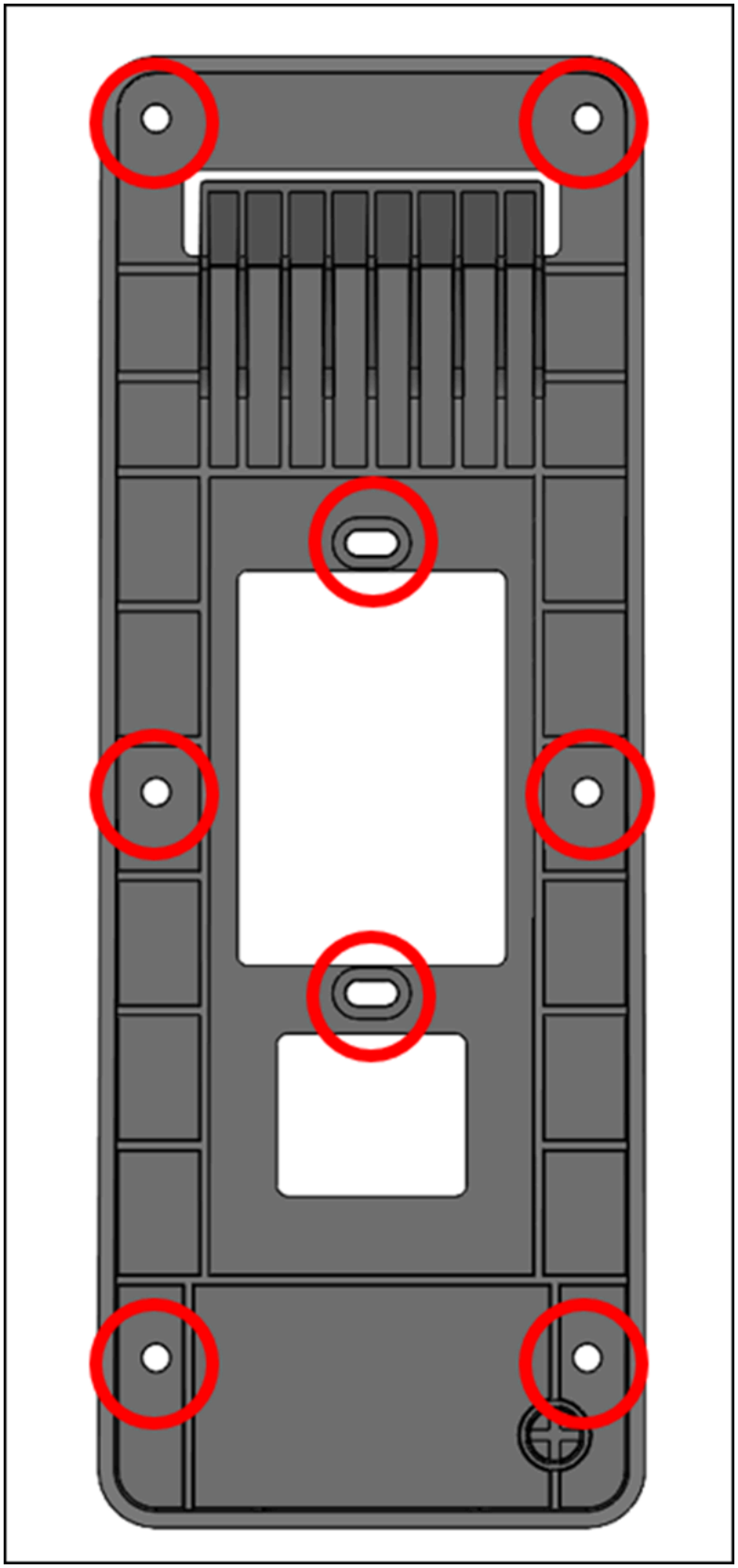
1. 從包裝中移除您的 Amazon One 裝置。
2. 移除兩個底部 Torx 安全螺絲，將掛載板與 Amazon One 裝置分開。



3. 將掛載板放置在所需位置的牆上。使用 括號作為範本，標記外部六個螺絲孔，如下圖所示。

   （選用）如果安裝位置中有單一 Gang 方塊可用，請執行下列動作：

   - 透過將隨附的 #6-32 機器螺絲插入橢圓形孔，將盤鬆散地掛載到 Gang 盒上。
   - 確保掛載板處於水平狀態。
   - 使用掛載板作為範本，使用鉛筆標記六個螺絲位置。您可以使用橢圓形孔和 #6-32 螺絲作為安裝板的額外支援。請勿使用 #6-32 螺絲位置作為掛載牆板的主要方法。



4. 如果安裝到結構、乾燥牆、磚或混凝土表面，請在每個標記的位置鑽 1/4 英吋的孔，然後將它們壓入孔中，直到錨與牆齊平，以安裝壁錨。

   如果掛載到木面上，則不需要錨點，而且標記的位置只需要 7/64 英吋的引導孔。

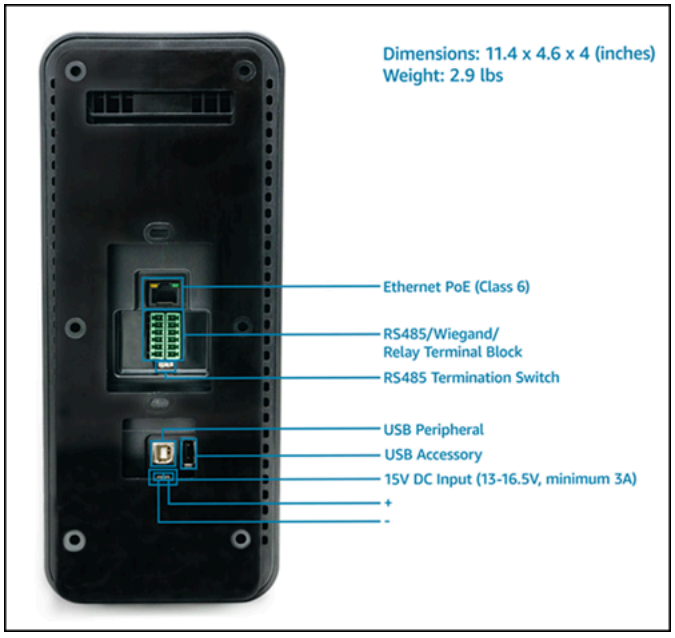
5. 使用錨點位置中的 #8 木螺絲，將牆板鬆散地固定到牆上。
6. 所有緊固件都到位後，請確保掛載板處於水平狀態。
7. 旋緊螺絲以將安裝板固定到牆壁。

連接您的壁掛式 Amazon One 裝置

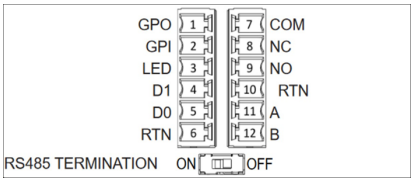
您可以使用 OSDP和 Weigand 存取控制通訊協定來設定 Amazon One 裝置。為了簡化安裝，Amazon One 裝置使用端子台連接器（Mfg P/N：Phoenix Contact 1767694）。您也可以選擇使用內部轉送或一般用途輸入和輸出連線，設定 Amazon One 裝置以直接控制外部裝置。

1. 若要判斷應用程式的適當配線組態，請參閱下圖和連線表。

   如需訊號的詳細電氣特性，請參閱 佈線指示。



連線



Pin	連線	描述	使用	
1	GPO	一般用途輸出	數位輸出訊號 - 選用	
2	GPI	一般用途輸入	數位輸入訊號 – 選用	
3	LED	Wiegand LED	Wiegand LED – 選用	
4	D1	Wiegand D1	Wiegand 資料 1 – 白線	
5	D0	Wiegand D0	Wiegand 資料 0 – 綠線	
6	RTN	訊號傳回	Wiegand Ground – 黑色線	
7	Com	轉送通用	聯絡中繼通用 – 白線	
8	NC	轉送常閉	接觸繼電器常閉 – 橘色電線	
9	NO	轉送常開	接觸繼電器常開 – 黃線	
10	RTN	訊號傳回	OSDP 傳回 – 黑色線	
11	A	RS485_A/D1/ Clock	OSDP D1 – 白線	
12	B	RS485_B/D0/資料	OSDP D0 – 綠線	

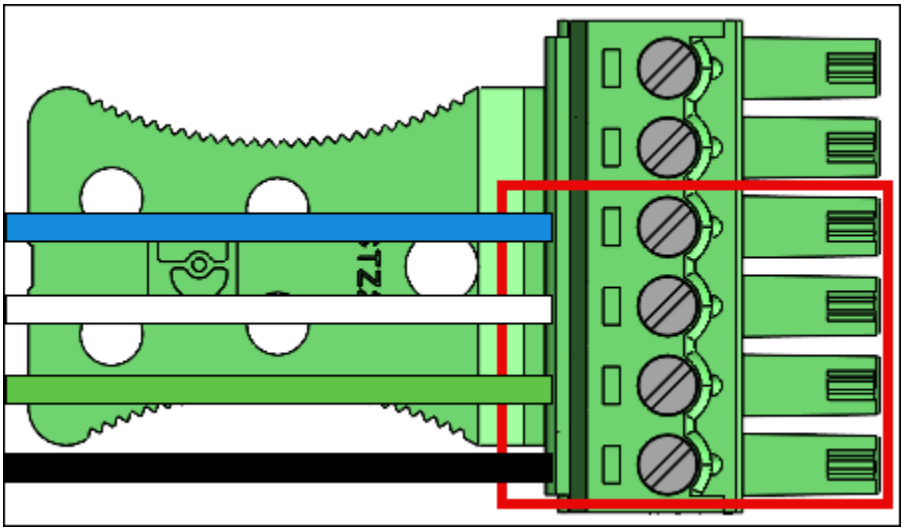
2. 安裝電線時，請將電線的一端剝除 3mm-5mm。
3. 將電線的剝除端插入所需的終端位置。
4. 使用一字螺絲起子，順時針轉動終端機保留螺絲，以夾緊電線，直到緊固為止。請勿過度收緊。
5. 扣上後，輕輕拉動電線，以確保其就位。
6. 進行必要的連線後，請將插頭插入 Amazon One 裝置端子區塊的對應插座。
7. 將 Cat6 乙太網路纜線插入RJ45插孔。
8. 放置 Amazon One 裝置，讓牆板上的掛鉤滑入裝置後方的開口。
9. 確保裝置與掛載板之間沒有卡住纜線，並讓裝置輪轉並就位。
10. 使用兩個 Torx Security M4x10 平頭螺絲，將 Amazon One 裝置固定至掛載板。
11. 手動旋緊螺絲。請勿過度收緊。

連接您的壁掛式 Amazon One 裝置

僅安裝應用程式所需的電線。

Wiegand 連線

- 將藍色電線插入針腳 3 （LED）。
- 將白線插入針腳 4 （D1）。
- 將綠色電線插入針腳 5 （D0）。
- 將黑色電線插入針腳 6 （RTN）。



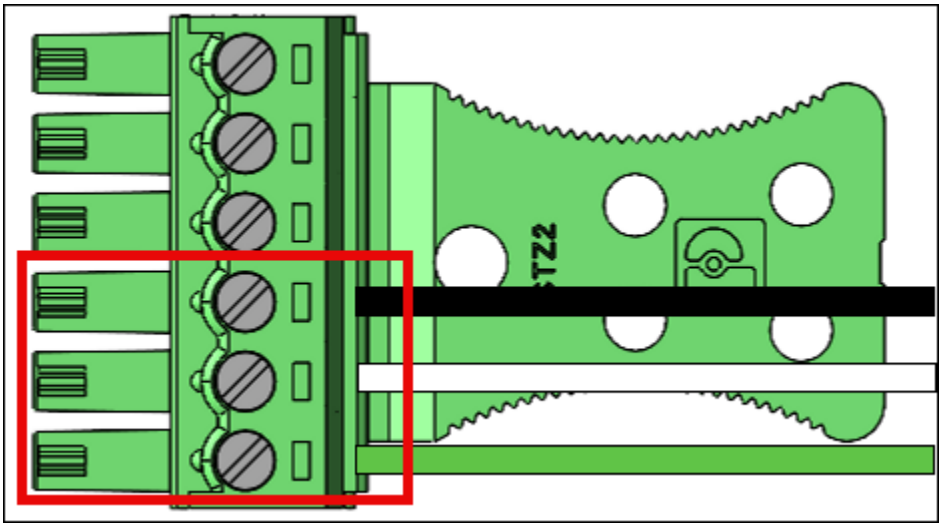
Wiegand 輸出配線

Pin	連線	描述	使用	
3	LED	Wiegand LED	Wiegand LED 輸入 – 選用（5VTTL）	
4	D1	Wiegand D1	Wiegand D1 輸出（5V TTL）	
5	D0	Wiegand D0	Wiegand D0 輸出（5V TTL）	
6	RTN	訊號傳回	Wiegand GND參考	

如果裝置是線路上的最後一個單元，請開啟RS485終止開關。此開關會在線路上啟用 120 Ohms 電阻器終止。

RS485 連線

- 將黑色電線插入 Pin 10（RTN）。
- 將白線插入針腳 11（A）。
- 將綠色電線插入接腳 12（B）。

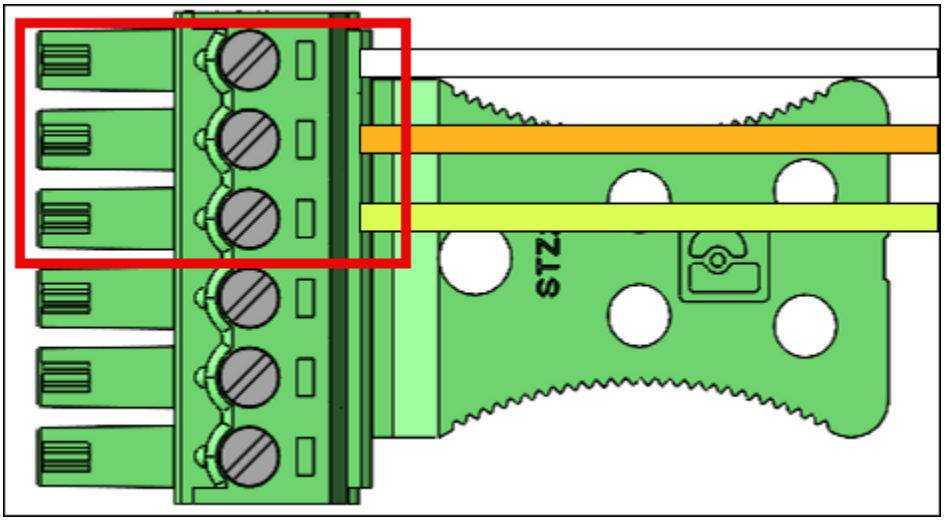


RS485 配線

Pin	連線	描述	使用	
10	RTN	訊號傳回	地面	
11	A	RS485_A/D1/ Clock	RS485 非轉換訊號	
12	B	RS485_B/D0/資料	RS485 反轉訊號	

轉送連線

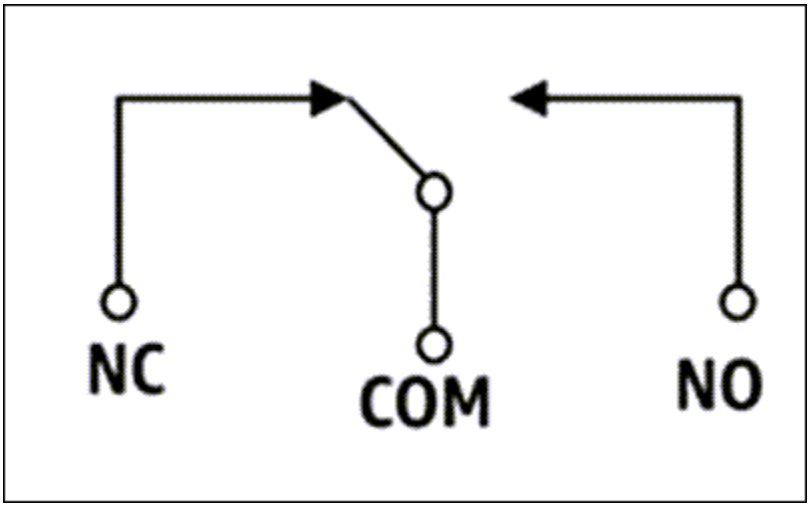
- 將白線插入針腳 7 （COM）。
- 將橘色電線插入 Pin 8 （NC）。
- 將黃色電線插入接腳 9 （NO）。



轉送器配線

Pin	連線	描述	使用	
7	COM	轉送通用	聯絡中繼通用 – 白線	

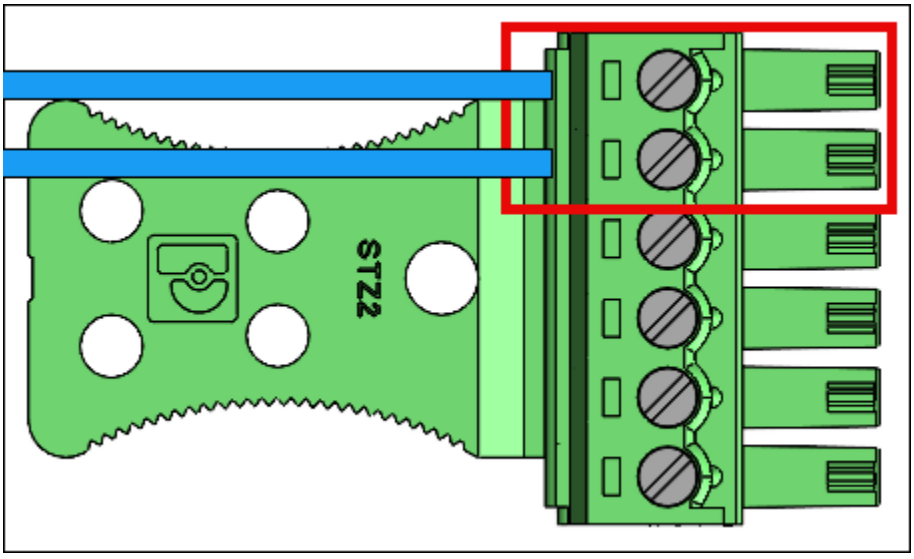
Pin	連線	描述	使用	
8	NC	轉送常閉	接觸繼電器常閉 – 橘色電線	
9	NO	轉送常開	接觸繼電器常開 – 黃線	



轉送器應按照指定的安全額定值 30VAC/60VDC、最大 60W 操作。

數位輸入/輸出連線

- 將藍色電線插入針腳 1（GPO）。
- 將藍色電線插入針腳 2（GPI）。



Pin	連線	描述	使用	
1	GPO	一般用途輸出	數位輸出訊號（5V）	
2	GPI	一般用途輸入	數位輸入訊號（3.6V – 5V）	

- 數位輸入/輸出連線應按所列方式操作。

請參閱 啟用 Amazon One 裝置 以啟用您的 Amazon One 裝置。

安裝 Amazon One 裝置 I/O Hub 以安全存取

本節詳細說明使用 I/O Hub 安裝 Amazon One Enterprise （AOE） 裝置所需的位置需求和步驟。

開始安裝之前，請確定下列事項：

- 具有 I/O Hub 的 Amazon One 裝置僅供室內使用。
- 對於乙太網路供電 （PoE ++）：

  確保 IEEE 802.3bt （第 3 型） Class 6 POE++ 交換器 （跨度結束） 或注入器 （跨度中） 可供使用，其已列出或認證，並符合 IEC 62368-1。

僅使用 Amazon One 裝置搭配核准的 PoE ++ 來源。

PoE ++ 來源必須位於相同的建築物內。

- 對於 15V DC 電源輸入，您只能將 Amazon One 裝置與 2 NEC類或電源限制、已列出或認證的核准電源供應器搭配使用。請參閱下面的選用 DC 區段。

必要工具：

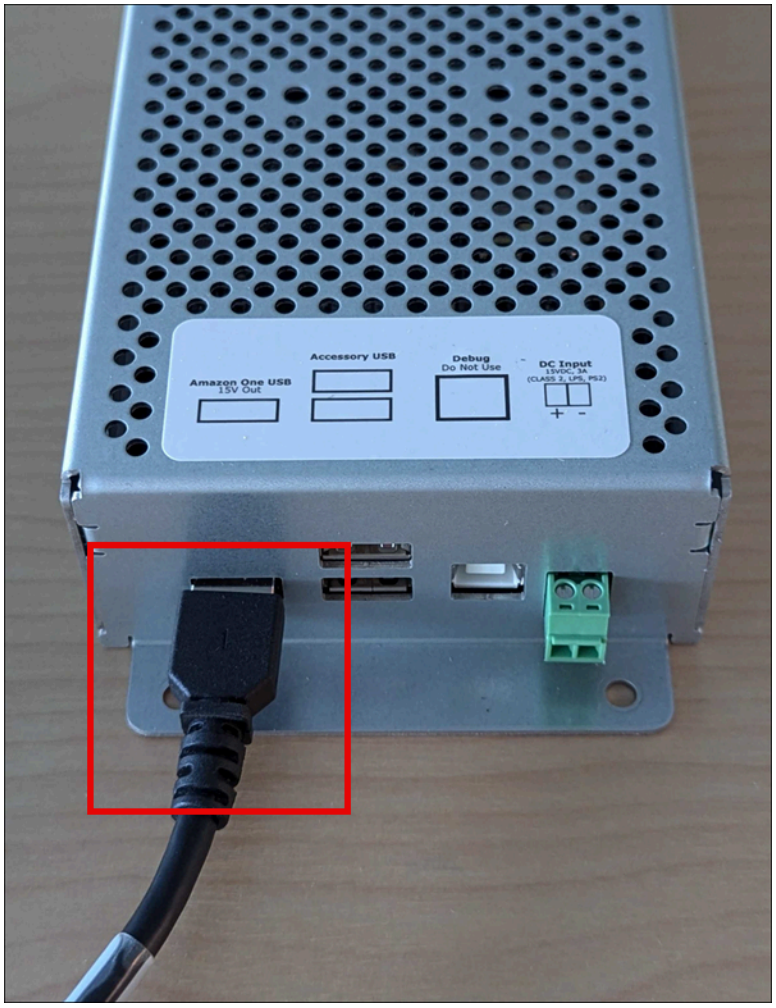
- 剝線器
- #2 Phillips 螺絲起子
- 0.5 公釐 x 2 公釐一字螺絲起子

隨附於具有 I/O Hub 的 Amazon One 裝置：

- 2x 6 位置接線端子連接器
- DC 插頭連接器
- 72 吋電源/資料纜線

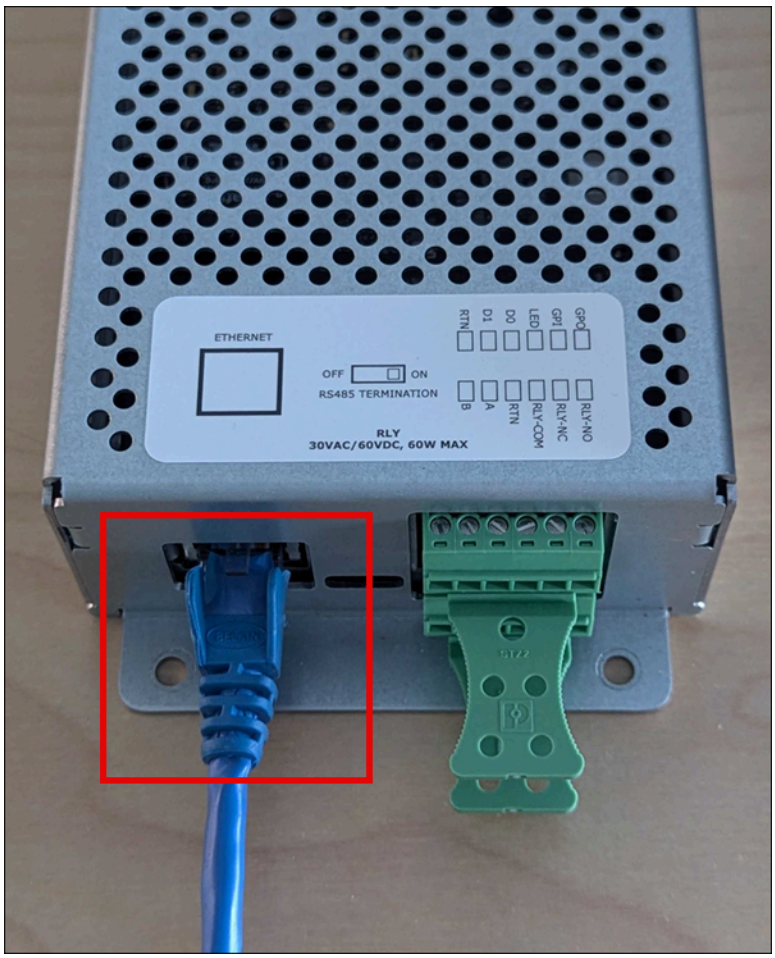
安裝 Amazon One 裝置的 I/O 中樞

1. 從包裝中移除具有 I/O Hub 的 Amazon One 裝置。
2. 將 I/O 集線器固定在所需的位置。
3. 將 Amazon One USB纜線插入 I/O 集線器連接埠。



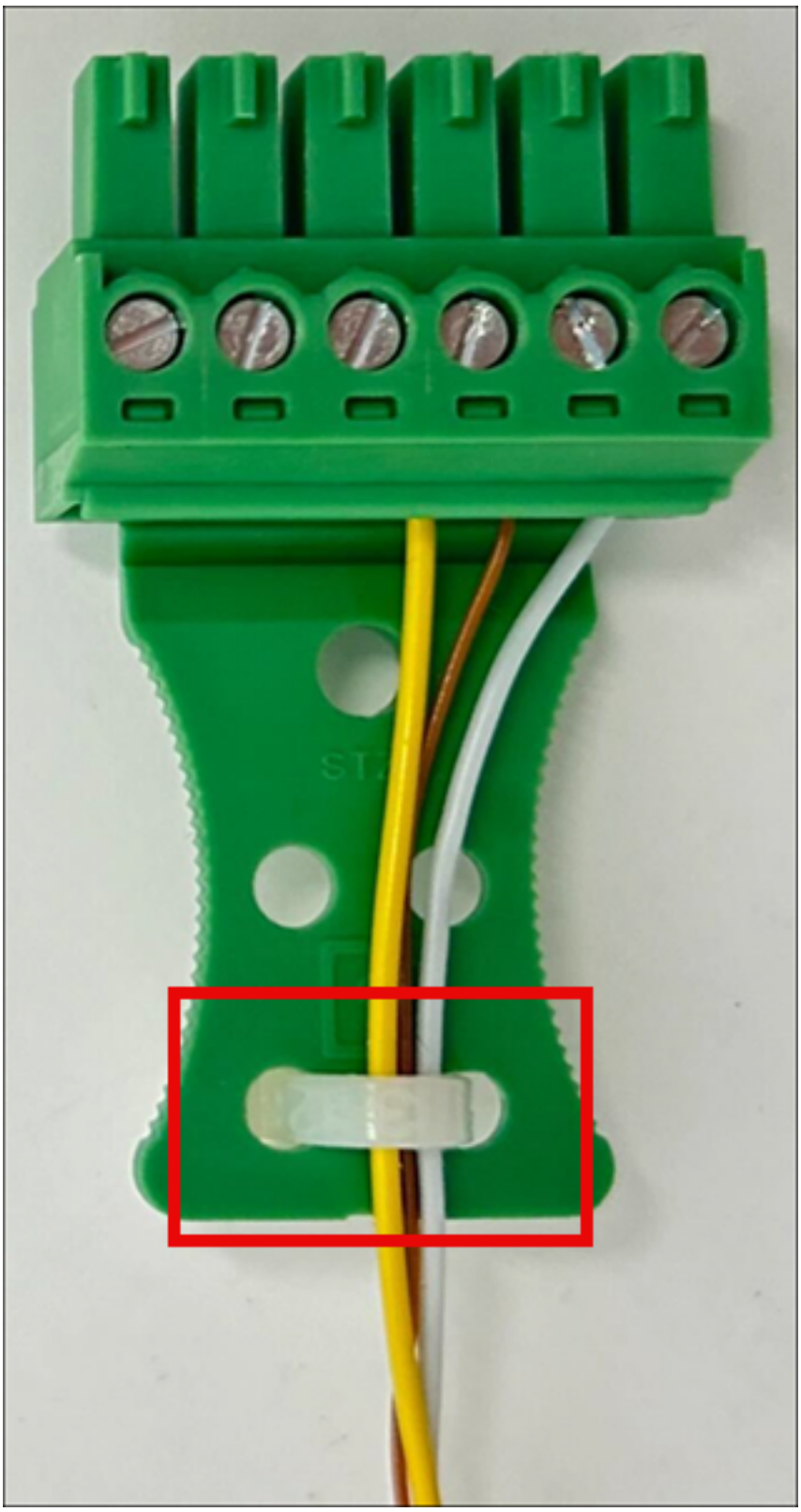
4. 對於 POE++ 電源，請將乙太網路纜線從 POE++ 來源插入 I/O 集線器連接埠。

   選用：如需 DC 電源，請參閱下列安裝 DC 配線一節。

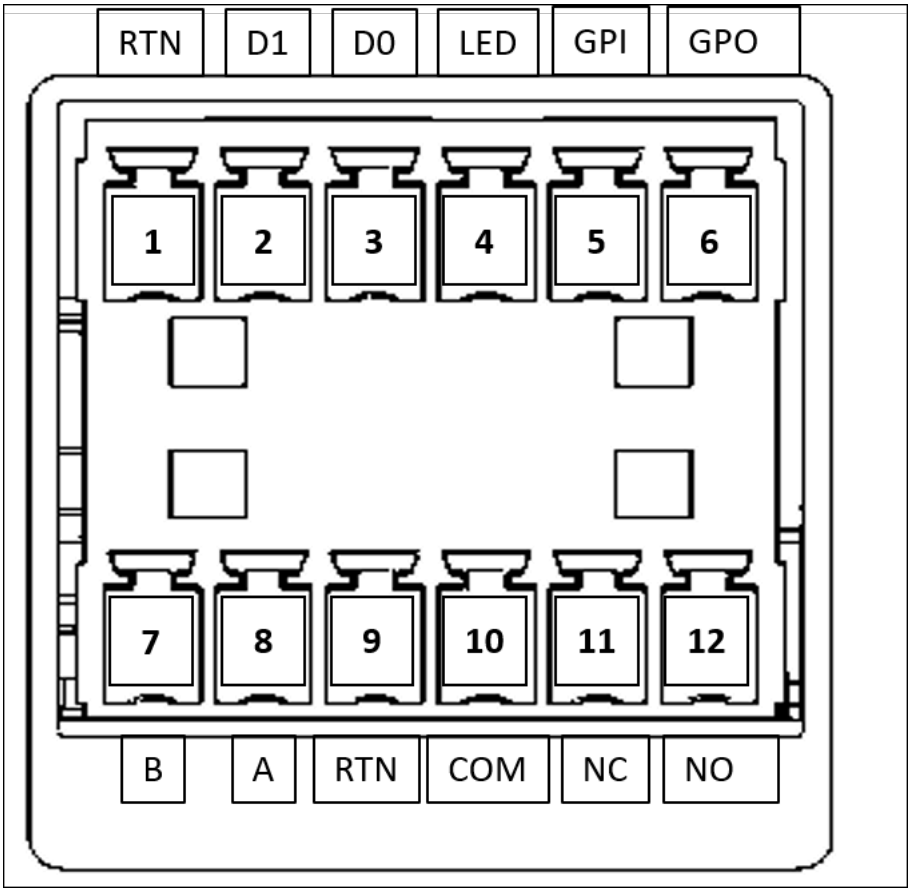


為您的 Amazon One 裝置連接 I/O 集線器

- 安裝滴水迴路，以避免液體意外地向下流過電線並進入 I/O 集線器。
- 連接應力消除夾，以保護電線免受損壞或壓力，如下圖所示。



1. 僅透過端子台插頭插入應用程式所需的電線。請參閱下列配線表和圖表。
2. 將端子台插頭插入 I/O 集線器。

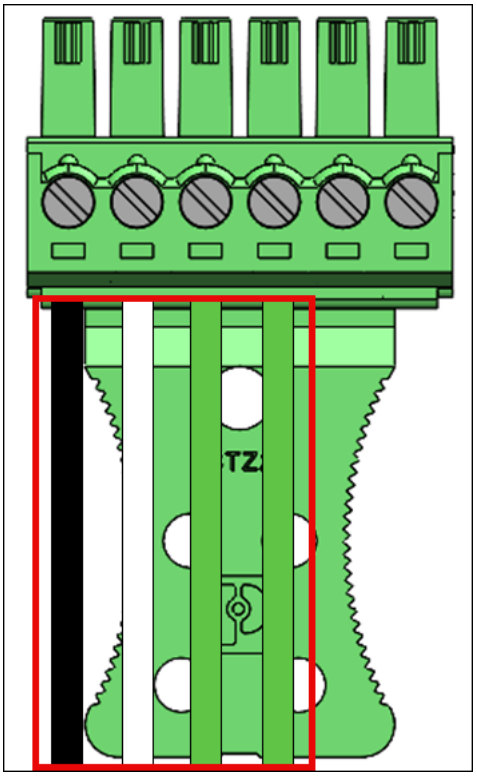


Pin	連線	描述	使用	
1	RTN	訊號傳回	Wiegand 接地 – 黑色線	
2	D1	Wiegand D1	Wiegand 資料 1 – 白線	
3	D0	Wiegand D0	Wiegand 資料 0 – 綠線	
4	LED	Wiegand LED	Wiegand LED – 選用	
5	GPI	一般用途輸入	數位輸入訊號 – 選用	

Pin	連線	描述	使用	
6	GPO	一般用途輸出	數位輸出訊號 - 選用	
7	B	RS485_B/D0/資料	OSDP D0 – 綠線	
8	A	RS485_A/D1/Clock	OSDP D1 – 白線	
9	RTN	訊號傳回	OSDP 傳回 – 黑色線	
10	COM	轉送通用	聯絡中繼通用 – 白線	
11	NC	轉送常閉	接觸繼電器常閉 – 橘色電線	
12	NO	轉送常開	接觸繼電器常開 – 黃線	

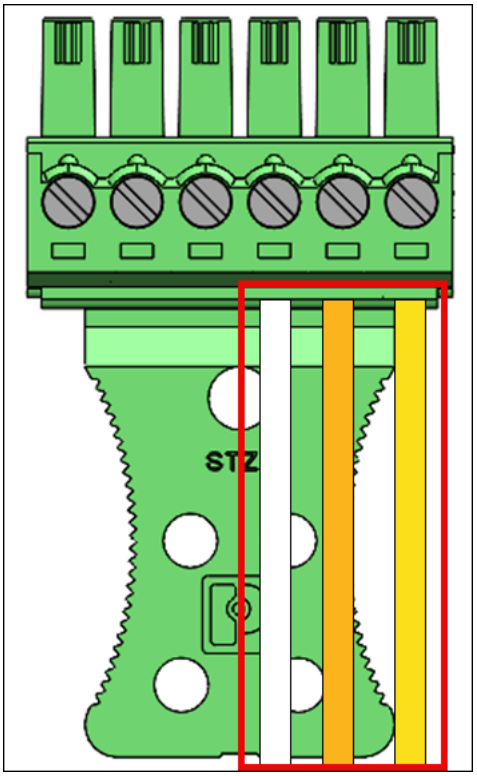
Wiegand 連線

- 將黑色電線插入針腳 1 （RTN）。
- 將白線插入針腳 2 （D1）。
- 將綠色電線插入針腳 3 （D0）。
- 選用：將綠色電線插入針腳 4 （LED）。

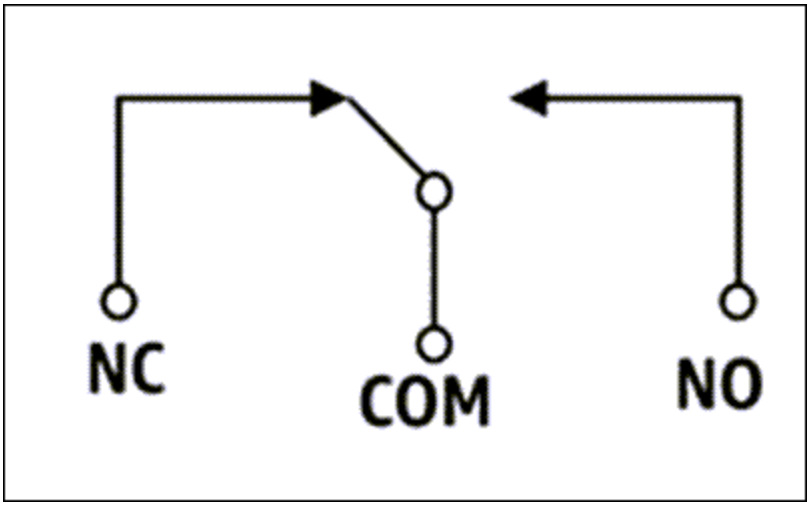


轉送連線

- 將白線插入 Pin 10（COM）。
- 將橘色電線插入 Pin 11（NC）。
- 將黃色電線插入針腳 12（NO）。



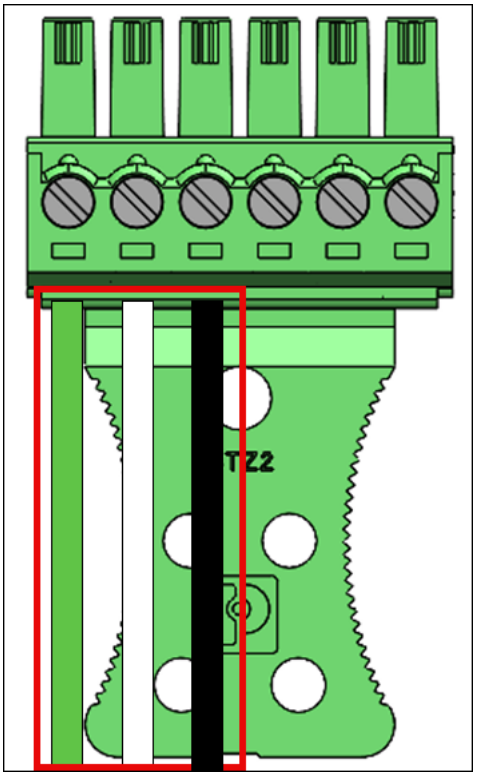
轉送圖



轉送器應按照指定的安全額定值 30VAC/60VDC、最大 60W 操作。

RS485 連線

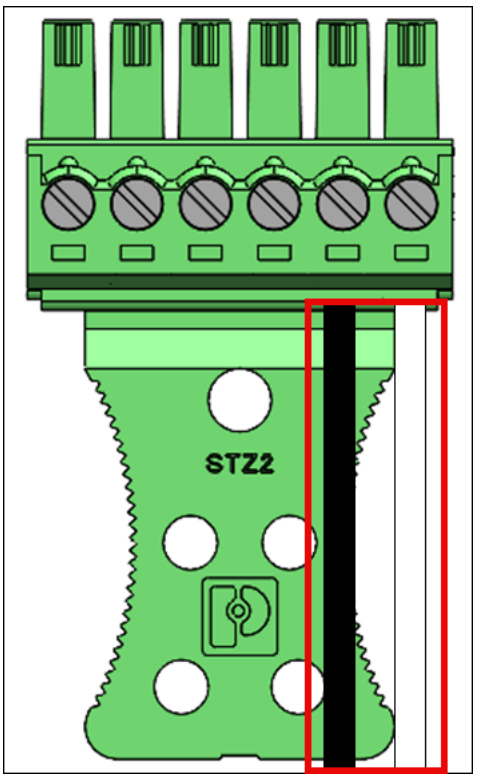
- 將綠色電線插入針腳 7（B）。
- 將白線插入接腳 8（A）。
- 將黑色電線插入針腳 9（RTN）。



如果裝置是線路上的最後一個單元，請開啟RS485終止開關。此開關會在線路上啟用 120 Ohms 電阻器終止。

數位輸入/輸出連線

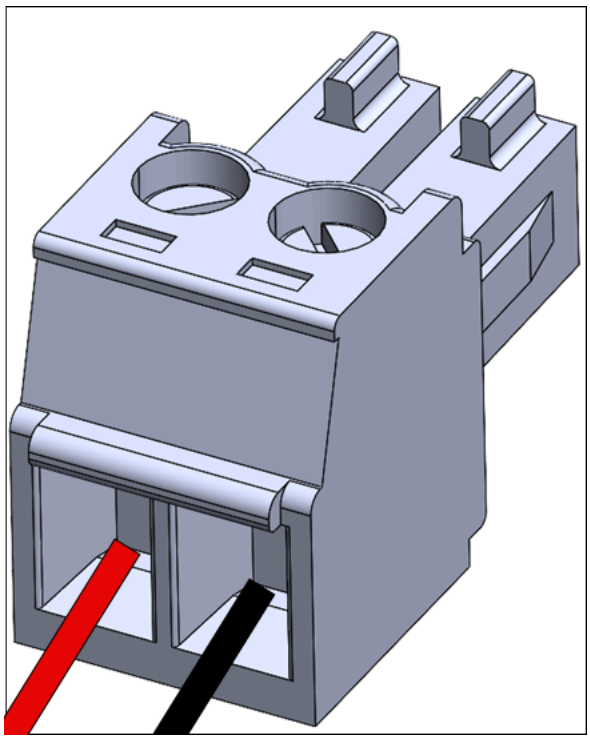
- 將黑色電線插入針腳 5（GPI）。
- 將白線插入針腳 6（GPO）。



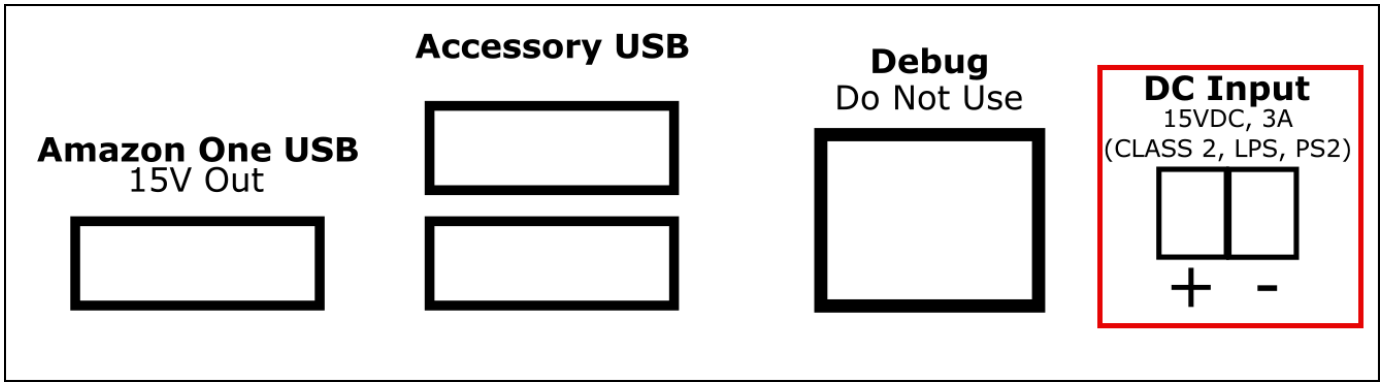
- 數位輸入/輸出連線應按所列方式操作。

選用：安裝 DC 配線

1. 從紅色電線末端剝除 3mm-5mm 的正極 （ + ） 和黑色電線的負極 （ - ）。
2. 將 DC 線的剝除端插入 DC 插頭。



3. 將電線鎖入定位。
4. 將有線 DC 插頭插入 DC 輸入連接埠。



啟用 Amazon One 裝置

安裝並開啟 Amazon One 裝置電源後，即可啟用裝置。

啟用您的 Amazon One 裝置

1. 在 Amazon One 裝置上，點選螢幕即可開始。
2. 選擇乙太網路或 Wifi 以連線至網際網路。

一旦裝置連線到網際網路，就會開始下載最新的軟體套件。

3. 當畫面顯示軟體下載完成！時，選取確定 。
4. 選取 QR 碼 。

   Amazon One 裝置畫面會顯示掃描 QR 碼 。
5. 若要擷取啟用 QR 碼，請開啟位於 https://console.aws.amazon.com/one-enterprise 的 Amazon One Enterprise 主控台。

   > **Note**
   >
   > 強烈建議您授予安裝程式有限的許可，以便他們只能存取 Amazon One Enterprise 主控台中的啟用 QR 碼。請參閱 新增 Amazon One Enterprise 使用者。

6. 在導覽窗格中，選擇啟用 QR 碼 。
7. 從選取網站下拉式清單中，選取安裝 Amazon One 裝置的網站。
8. 在站台資訊 下，確認站台地址。
9. 在啟用 QR 碼 下，尋找您正在啟用的裝置執行個體名稱，然後選取對應的取得 QR 碼以擷取 QR 碼。
10. 使用 Amazon One 裝置掃描 QR 碼。請注意，為了安全起見，QR 碼會定期重新整理，您只能使用 QR 碼一次。
11. 輸入網站郵遞區號，然後在確認顯示正確的網站後，選取確認設定。
12. 當 Amazon One 裝置畫面顯示啟動完成！ 時，表示裝置已準備好可供使用。

註冊和輸入使用者

現在您的 Amazon One 裝置已啟用，您的員工可以開始註冊其手掌，並驗證其手掌以取得存取權。

主題

建立端點政策

使用者必須先完成註冊程序，才能驗證其手掌才能進入。在允許使用者註冊之前，安全人員應一律檢查使用者的身分。

在 Amazon One 裝置上註冊您的手掌

1. 在 Amazon One Enterprise 註冊裝置上，按下開始使用 。
2. 使用連線至 Amazon One Enterprise 註冊裝置的徽章掃描器掃描員工徽章。

   成功掃描徽章時，Amazon One 裝置畫面會顯示已掃描的徽章。
3. 閱讀 使用條款 ，然後按 OK 。
4. 閱讀同意 - 您的 Palm Biometric 資訊，如果您同意，請按下我同意。
5. 請遵循畫面上的指示完成註冊程序。

驗證項目

成功註冊掌上型伺服器之後，您就可以在 Amazon One Enterprise 登入裝置上使用掌上型伺服器進行身分驗證。

驗證 Amazon One 裝置上的登錄檔

- 將掌心放在裝置頂端，並遵循畫面上的指示掃描掌心。

管理使用者

您可以使用註冊使用者管理頁面來追蹤註冊的使用者，以及刪除使用者生物識別特徵。刪除相關聯生物識別的使用者將無法再存取 Amazon One 裝置進行身分驗證。

主題

檢視已註冊的使用者

下列程序詳細說明如何註冊使用者。

檢視已註冊的使用者

1. 在 https://console.aws.amazon.com/one-enterprise 開啟 Amazon One Enterprise 主控台。
2. 在導覽窗格中，選擇註冊使用者管理 。
3. 在註冊使用者 下，您會找到所有註冊的使用者，以及下列詳細資訊：
   - 徽章 ID — 註冊時徽章讀取器擷取的RFID徽章識別符資訊。
   - 註冊來源 — 用於註冊的 Amazon One 裝置的詳細資訊。
   - 註冊日期 — 註冊的日期和時間。

刪除註冊的使用者及其生物識別特徵

下列程序詳細說明如何刪除註冊的使用者及其生物識別特徵。

刪除註冊的使用者及其生物識別特徵

1. 在 https://console.aws.amazon.com/one-enterprise 開啟 Amazon One Enterprise 主控台。
2. 在導覽窗格中，選擇註冊使用者管理 。
3. 在已註冊使用者 下，選取您要刪除其掌上生物識別資料之使用者的徽章 ID。
4. 選擇刪除生物識別技術 。
5. 選擇刪除以確認刪除使用者生物識別資料。

> **Important**
>
> 此動作會導致從 Amazon One Enterprise 永久刪除使用者的掌上生物識別。使用者將需要再次使用 Amazon One Enterprise 註冊裝置註冊，才能使用 Amazon One Enterprise 進行身分驗證。刪除使用者的生物識別也會從 Amazon One Enterprise 永久刪除徽章 ID 等其他設定檔屬性。

管理 Amazon One 裝置

安裝並啟用 Amazon One 裝置後，它會在 Amazon One Enterprise 主控台上開始報告裝置運作狀態。您可以使用 Amazon One Enterprise 主控台來執行裝置管理任務，例如重新啟動裝置或更新組態。

主題

維護和清潔 Amazon One 裝置

維護 Amazon One 裝置可提供最佳的裝置操作環境和裝置體驗。

清潔 Amazon One 裝置之前，請確定下列事項：

- 雖然您不需要啟用或停用 Amazon One，但請確保裝置已連接至電源、具有網路連線，以及任何周邊和搭配裝置（如適用）已連線。
- 如果網路連線無法使用，請向您的管理員呈報問題（如果發生這種情況，Amazon One 裝置會顯示錯誤畫面）、Amazon One 裝置會顯示錯誤畫面，或主控台會顯示裝置連線問題。
- 實體保護裝置，讓未經授權的個人無法篡改裝置。
- 每天目測檢查 Amazon One 裝置，檢查是否有任何未經授權的 Amazon One 裝置連線。
- 檢查裝置的所有端是否有竄改的跡象，包括裝置和外殼的可見螺絲，以確保沒有空隙/開路暴露到任一 Amazon One 裝置的內部元件/電路。
- 如果發生任何錯誤或失敗，請依照 Amazon One 裝置畫面上的指示操作，或參閱故障診斷指南來修復問題。

清除 Amazon One 裝置

清理 Amazon One 裝置會定期清除指紋和手印等任何污點或標記。

> **Note**
>
> 請勿使用本指南所列以外的任何其他清潔產品。建議的清潔排程是每週一到兩次，或每當裝置上出現污物、灰塵或污點時，但每天不得超過一次。

1. 使用異丙醇（IPA）擦拭來擦拭 Amazon One 裝置。僅清潔裝置的觸控表面。除非 Amazon One 指示，否則請勿觸摸光學窗口，或使用任何其他清潔產品。
2. 使用乾的超細纖維布擦除任何條紋。
3. 稍微清除（請勿擦拭）光學視窗中的任何可見污物或碎片。將光學視窗的清潔限制為每天不超過一次）and/or when the window is visually dirty (e.g., finger/hand prints/smudges。裝置的此部分並非旨在接觸，但新客戶可能會無意接觸裝置。
4. 如果適用，請使用KIC智慧卡清潔劑來清潔讀卡器內部。
5. 每週清潔裝置一到兩次，或每當裝置上看見污物、灰塵或污點時。

網站管理

網站代表安裝和操作裝置執行個體集合的實體位置。您可以使用網站來組織共用相同實體地址的 Amazon One 裝置。

主題

變更網站名稱

下列程序詳細說明如何變更裝置的網站名稱。

若要變更網站名稱

1. 在 https://console.aws.amazon.com/one-enterprise 開啟 Amazon One Enterprise 主控台。
2. 在導覽窗格中，選擇站台 。
3. 在站台 下，選取您要編輯名稱的站台。
4. 選擇編輯。
5. 在站台資訊下，輸入所需的站台名稱和站台描述（選用）。
6. 選擇儲存變更以進行更新。

更新網站地址

下列程序詳細說明如何更新裝置的網站地址。

更新網站地址

1. 在 https://console.aws.amazon.com/one-enterprise 開啟 Amazon One Enterprise 主控台。
2. 在導覽窗格中，選擇站台 。
3. 在站台 下，選取您要更新地址的網站。
4. 在裝置執行個體 下，確保啟用的執行個體數目為 0。
5. （選用） 如果啟用的執行個體數目不是 0，請參閱
6. 選擇編輯。
7. 在實體地址下，輸入正確的實體地址。
8. 選擇儲存變更以進行更新。

裝置執行個體管理

裝置執行個體是具有組態之裝置的邏輯表示法。使用裝置執行個體允許交換 Amazon One 裝置，同時自動繼承先前設定的組態和名稱。裝置執行個體具有使用者定義的名稱 （與您的存取控制軟體共用命名慣例） 和一組通訊組態。

主題

檢視裝置執行個體狀態

下列程序詳細說明如何檢視裝置執行個體的狀態。

檢視裝置執行個體狀態

1. 在 https://console.aws.amazon.com/one-enterprise 開啟 Amazon One Enterprise 主控台。
2. 在導覽窗格中，選擇裝置執行個體 。
3. 在已啟用的執行個體 下，您會看到已啟用的 Amazon One 裝置清單。
4. 選擇裝置執行個體名稱以檢視裝置執行個體詳細資訊。

重新啟動 Amazon One 裝置

下列程序詳細說明如何重新啟動 Amazon One 裝置。

若要重新啟動 Amazon One 裝置

1. 在 https://console.aws.amazon.com/one-enterprise 開啟 Amazon One Enterprise 主控台。
2. 在導覽窗格中，選擇裝置執行個體 。
3. 在已啟用的執行個體 下，選擇要重新啟動的裝置執行個體名稱。
4. 選擇重新啟動以重新啟動 Amazon One 裝置。

更新 Amazon One 裝置組態

下列程序詳細說明如何更新 Amazon One 裝置組態。

若要更新 Amazon One 裝置組態

1. 在 https://console.aws.amazon.com/one-enterprise 開啟 Amazon One Enterprise 主控台。
2. 在導覽窗格中，選擇裝置執行個體 。
3. 在已啟用執行個體 下，選擇要更新的裝置的執行個體名稱。
4. 在裝置組態 下，選擇編輯 。

> **Note**
>
> 若要變更 Amazon One 裝置模式，您必須先停用裝置執行個體，然後使用所需的裝置模式進行設定 （請參閱 設定裝置執行個體以啟用 ）。然後，您可以完成裝置啟用程序 （請參閱 啟用 Amazon One 裝置 ）。

5. 完成所需的變更後，請選擇更新裝置組態以確認更新。

更新 Wi-fi 憑證

下列程序詳細說明如何更新 Wi-Fi 憑證。

更新 Wifi 憑證

1. 在 https://console.aws.amazon.com/one-enterprise 開啟 Amazon One Enterprise 主控台。

2. 在導覽窗格中，選擇裝置執行個體 。
3. 在已啟用執行個體 下，選擇要更新的裝置的執行個體名稱。
4. 在網路 下，選擇編輯 。
5. 在 Wi-Fi 組態 下，進行所需的變更。
6. 選擇更新網路以確認更新。

停用裝置執行個體

下列程序詳細說明如何停用裝置執行個體。

若要停用裝置執行個體

1. 在 https://console.aws.amazon.com/one-enterprise 開啟 Amazon One Enterprise 主控台。
2. 在導覽窗格中，選擇裝置執行個體 。
3. 在已啟用執行個體 下，選取您要停用的裝置執行個體名稱。
4. 選擇停用裝置 。
5. 若要確認停用，請在訊息方塊中輸入「停用」，然後選擇停用裝置 。

安全

的雲端安全 AWS 是最高優先順序。作為 AWS 客戶，您受益於資料中心和網路架構，這些架構旨在滿足最安全敏感組織的需求。

安全性是 AWS 和 之間的共同責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端的安全性 – AWS 負責保護在 中執行 AWS 服務的基礎設施 AWS 雲端。 AWS 也提供您可以安全使用的服務。第三方稽核人員會定期測試和驗證我們安全的有效性，這是AWS 合規計畫 的一部分。若要了解適用於 Amazon One Enterprise 的合規計劃，請參閱依AWS 合規計劃在範圍內的合規計劃
- 雲端安全性 – 您的責任取決於您使用 AWS 的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您了解如何在使用 Amazon One Enterprise 時套用共同責任模型。下列主題說明如何設定 Amazon One Enterprise 以符合您的安全和合規目標。您也會了解如何使用 AWS 其他服務來協助您監控和保護 Amazon One Enterprise 資源。

主題

- Amazon One Enterprise 的資料保護
- Amazon One Enterprise 的身分和存取管理
- Amazon One Enterprise 的動作、資源與條件索引鍵
- Amazon 一家企業版的合規驗證

Amazon One Enterprise 的資料保護

AWS 共同責任模型適用於 Amazon One Enterprise 中的資料保護。如本模型所述， AWS 負責保護執行所有 的全域基礎設施 AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權。 FAQ如需歐洲資料保護的相關資訊，請參閱AWS 安全部落格 上的AWS 共同責任模型和GDPR部落格文章。

為了資料保護目的，我們建議您保護 AWS 帳戶 憑證，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management （ ） 設定個別使用者IAM。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 對每個帳戶使用多重要素驗證 （MFA）。

- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 和 建議 TLS 1.3。
- 使用 設定 API 和使用者活動日誌 AWS CloudTrail。如需使用 CloudTrail 線索擷取 AWS 活動的資訊，請參閱 AWS CloudTrail 使用者指南 中的使用 CloudTrail 線索。
- 使用 AWS 加密解決方案，以及 中的所有預設安全控制項 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在 AWS 透過命令列介面或 FIPS 存取 時需要 140-3 個經過驗證的密碼編譯模組API，請使用FIPS端點。如需可用FIPS端點的詳細資訊，請參閱聯邦資訊處理標準（FIPS）140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 Amazon One Enterprise 或其他 AWS 服務 主控台API AWS CLI、 或 時 AWS SDKs。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您將 URL提供給外部伺服器，強烈建議您在 中不要包含憑證資訊，URL以驗證您對該伺服器的請求。

使用靜態資料的預設加密

Amazon One Enterprise 預設提供加密，以使用AWS加密金鑰保護靜態敏感資料。

AWS 擁有的金鑰 — Amazon One Enterprise 預設使用這些金鑰自動加密敏感的最終使用者資料。您無法檢視、管理或使用AWS擁有的金鑰，或稽核其使用。不過，您不需要採取任何動作或變更任何程式，即可保護加密您資料的金鑰。如需詳細資訊，請參閱 AWS Key Management Service 開發人員指南中的AWS擁有金鑰。

管理您自己的客戶金鑰

客戶受管金鑰 — Amazon One Enterprise 支援使用您建立、擁有和管理的對稱客戶金鑰。這會在現有AWS擁有的加密上新增第二層加密。Amazon One Enterprise 支援加密敏感客戶資料，例如使用者資料、裝置組態、Wi-Fi 密碼等。此功能包含新增自我管理安全層的選項，以協助滿足組織的合規和法規要求。如需啟用客戶受管金鑰的詳細資訊，請參閱在 Amazon One Enterprise 中更新加密設定。

您可以完全控制此層加密，因此能執行以下任務：

- 建立和維護金鑰政策
- 建立和維護KMS許可IAM政策
- 依您控制的節奏輪換金鑰密碼編譯材料
- 新增標籤

如需詳細資訊，請參閱 AWS Key Management Service 開發人員指南中的客戶受管金鑰。

> **Note**
>
> 雖然 Amazon One Enterprise 使用AWS自有金鑰自動啟用靜態加密，以免費保護敏感的客戶資料，但使用客戶受管金鑰AWSKMS需付費。如需定價的詳細資訊，請參閱 AWS Key Management Service 定價。如需 AWS 的詳細資訊KMS，請參閱什麼是 AWS Key Management Service？
> 您可以隨時移除服務對客戶受管金鑰的存取權。如果您這樣做，Amazon One Enterprise 將無法存取客戶受管金鑰加密的任何資料，這會影響依賴該資料的操作。例如，如果您嘗試取得加密的使用者、裝置組態 Amazon One Enterprise 無法存取的資料資訊，則操作會傳回 `AccessDeniedException error`。

加密傳輸中的資料

Amazon One Enterprise 使用 Transport Layer Security （ TLS ） 來保護資料，而 Signature 第 4 版可驗證 AWS 服務的所有傳入API請求。預設會啟用此加密。

Amazon One Enterprise 的身分和存取管理

AWS Identity and Access Management （ IAM ） 是一種 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以驗證 （ 登入 ） 和授權 （ 具有許可 ） 使用 Amazon One Enterprise 資源。IAM 是 AWS 服務 您可以免費使用的 。

主題

- 物件
- 使用身分驗證
- 使用政策管理存取權
- Amazon One Enterprise 如何與 搭配使用 IAM
- Amazon One Enterprise 的身分型政策範例
- AWS Amazon 一家企業的受管政策

物件

使用 AWS Identity and Access Management （ IAM ） 的方式會有所不同，具體取決於您在 Amazon One Enterprise 中執行的工作。

服務使用者 – 如果您使用 Amazon One Enterprise 服務來執行您的工作，您的管理員會為您提供所需的憑證和許可。當您使用更多 Amazon One Enterprise 功能來執行工作時，您可能需要額外的許可。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取 Amazon One Enterprise 中的功能，請參閱 對 Amazon One Enterprise 身分和存取權進行疑難排解。

服務管理員 – 如果您在公司負責 Amazon One Enterprise 資源，您可能可以完整存取 Amazon One Enterprise。您的任務是判斷您的服務使用者應存取哪些 Amazon One Enterprise 功能和資源。然後，您必須向IAM管理員提交請求，以變更服務使用者的許可。請檢閱此頁面上的資訊，以了解 的基本概念IAM。若要進一步了解您的公司如何IAM與 Amazon One Enterprise 搭配使用，請參閱 Amazon One Enterprise 如何與 搭配使用 IAM。

IAM 管理員 – 如果您是IAM管理員，您可能想要了解如何撰寫政策以管理 Amazon One Enterprise 存取的詳細資訊。若要檢視您可以在 中使用的 Amazon One Enterprise 身分型政策範例IAM，請參閱 Amazon One Enterprise 的身分型政策範例。

使用身分驗證

驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者身分、IAM使用者身分或擔任IAM角色來驗證 （ 登入 AWS ）。

您可以使用透過身分來源提供的憑證，以聯合身分 AWS 身分登入 。 AWS IAM Identity Center （ IAM Identity Center ） 使用者、您公司的單一登入身分驗證，以及您的 Google 或 Facebook 憑證，都是聯合身分的範例。當您以聯合身分身分登入時，您的管理員先前會使用 IAM角色設定身分聯合。當您 AWS 使用聯合存取 時，您會間接擔任 角色。

您可以登入 AWS Management Console 或 AWS 存取入口網站，視您身分的使用者類型而定。如需登入 的詳細資訊 AWS，請參閱 使用者指南 中的如何登入 AWS 帳戶您的 。 AWS 登入

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 （ SDK ） 和命令列介面 （ CLI ），以使用您的 憑證以密碼編譯方式簽署您的請求。如果您不使用 AWS 工具，則必須自行簽署請求。如需使用建議方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南 中的簽署 AWS API請求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素身分驗證 （ MFA ） 來提高帳戶的安全性。若要進一步了解，請參閱 AWS IAM Identity Center 使用者指南中的多重要素驗證，以及 IAM 使用者指南 中的使用多重要素驗證 （ MFA ） AWS。

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個登入身分開始，該身分可以完全存取 帳戶中的所有 AWS 服務 和資源。此身分稱為 AWS 帳戶 根使用者，透過您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需需要您以根使用者身分登入的任務完整清單，請參閱 IAM 使用者指南 中的需要根使用者憑證的任務。

聯合身分

作為最佳實務， 會要求人類使用者，包括需要管理員存取權的使用者，使用 AWS 服務 臨時憑證來與身分提供者使用聯合來存取 。

聯合身分是來自您的企業使用者目錄、Web 身分提供者、 AWS Directory Service、身分中心目錄，或使用透過身分來源提供的 AWS 服務 憑證存取的任何使用者。當聯合身分存取 時 AWS 帳戶，它們會擔任 角色，而角色會提供臨時憑證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，或者您可以連線並同步到您身分來源中的一組使用者 AWS 帳戶 和群組，以便在所有 和應用程式中使用。如需 IAM Identity Center 的相關資訊，請參閱 AWS IAM Identity Center 使用者指南 中的什麼是 IAM Identity Center？。

IAM 使用者和群組

IAM 使用者是 中具有單一個人或應用程式特定許可 AWS 帳戶 的身分。在可能的情況下，我們建議依賴臨時憑證，而不是建立具有密碼和存取金鑰等長期憑證IAM的使用者。不過，如果您有特定的使用案例需要IAM使用者的長期憑證，建議您輪換存取金鑰。如需詳細資訊，請參閱 IAM 使用者指南 中的定期輪換需要長期憑證的使用案例存取金鑰。

IAM 群組是指定IAM使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有名為 的群組IAMAdmins，並授予該群組管理IAM資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。若要進一步了解，請參閱 IAM 使用者指南 中的何時建立IAM使用者 （ 而非角色 ）。

IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似於IAM使用者，但與特定人員無關。您可以透過 AWS Management Console 切換IAM角色 暫時在 中擔任角色。 https://docs.aws.amazon.com/IAM/

latest/UserGuide/id_roles_use_switch-role-console.html您可以呼叫 AWS CLI 或 AWS API 操作，或使用自訂 來擔任角色URL。如需使用角色方法的詳細資訊，請參閱 IAM 使用者指南 中的擔任角色的方法。

IAM 具有臨時憑證的角色在下列情況下很有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需聯合角色的相關資訊，請參閱 IAM 使用者指南 中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，您可以設定許可集。若要控制身分在身分驗證後可以存取的內容，IAMIdentity Center 會將許可集與 中的角色相關聯IAM。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 臨時IAM使用者許可 – IAM使用者或角色可以擔任IAM角色，暫時接受特定任務的不同許可。
- 跨帳戶存取 – 您可以使用 IAM角色，允許不同帳戶中的某人（受信任的主體）存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。不過，使用某些 AWS 服務，您可以將政策直接連接至資源（而不是使用角色作為代理）。若要了解跨帳戶存取的角色與資源型政策之間的差異，請參閱 IAM 使用者指南 中的跨帳戶資源存取IAM。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在 服務中撥打電話時，該服務通常會在 Amazon 中執行應用程式，EC2或在 Amazon S3 中儲存物件。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉送存取工作階段（FAS）– 當您使用IAM使用者或角色在 中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，並結合請求向下游服務 AWS 服務 提出請求的 。FAS 只有在服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出FAS請求的政策詳細資訊，請參閱轉送存取工作階段 。
  - 服務角色 – 服務角色是服務代表您執行動作時擔任IAM的角色。IAM 管理員可以從 內部建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱 使用者指南 中的建立角色以將許可委派給 AWS 服務 。 IAM
  - 服務連結角色 – 服務連結角色是連結至 的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的 中 AWS 帳戶 ，並由 服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon 上執行的應用程式 EC2 – 您可以使用 IAM角色來管理在EC2執行個體上執行的應用程式的臨時憑證，以及提出 AWS CLI 或 AWS API請求。最好將存取金鑰儲存在EC2執行個體中。若要將 AWS 角色指派給EC2執行個體並將其提供給其所有應用程式，您可以建立連接至執行個體的執行個體設定檔。執行個體設定檔包含 角色，並啟用在EC2執行個體上執行的程式，以取得臨時憑證。

如需詳細資訊，請參閱 IAM 使用者指南 中的使用 IAM角色將許可授予在 Amazon EC2執行個體上執行的應用程式。

若要了解如何使用IAM角色或IAM使用者，請參閱 IAM 使用者指南 中的建立IAM角色（而非使用者）的時機。

使用政策管理存取權

您可以透過建立政策並將其連接至 AWS 身分或資源 AWS 來控制 中的存取。政策是 AWS 其中的物件，當與身分或資源建立關聯時， 會定義其許可。當主體（使用者、根使用者或角色工作階段）發出請求時， 會 AWS 評估這些政策。政策中的許可決定是否允許或拒絕請求。大多數政策都以JSON文件 AWS 形式儲存在 中。如需JSON政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南 中的JSON政策概觀。

管理員可以使用 AWS JSON政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授予使用者對所需資源執行動作的許可，IAM管理員可以建立IAM政策。然後，管理員可以將IAM政策新增至角色，使用者可以擔任角色。

IAM 無論您用來執行操作的方法為何，政策都會定義動作的許可。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該政策的使用者可以從 AWS Management Console、 AWS CLI或 AWS 取得角色資訊API。

身分型政策

身分型政策是JSON許可政策文件，您可以附加到身分，例如IAM使用者、使用者群組或角色。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分型政策，請參閱 IAM 使用者指南 中的建立IAM政策。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管政策是獨立的政策，您可以連接到 中的多個使用者、群組和角色 AWS 帳戶。受管政策包括 AWS 受管政策和客戶受管政策。若要了解如何在受管政策或內嵌政策之間進行選擇，請參閱 IAM 使用者指南 中的在受管政策與內嵌政策之間進行選擇。

資源型政策

資源型政策是您連接至資源JSON的政策文件。資源型政策的範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策 。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權

限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主體可以包括帳戶、使用者、角色、聯合使用者或 AWS 服務。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策IAM中使用來自 的 AWS 受管政策。

存取控制清單 （ACLs）

存取控制清單 （ACLs） 控制哪些主體 （帳戶成員、使用者或角色） 具有存取 資源的許可。ACLs 類似於資源型政策，雖然它們不使用JSON政策文件格式。

Amazon S3 AWS WAF和 Amazon VPC是支援 的服務範例ACLs。若要進一步了解 ACLs，請參閱 Amazon Simple Storage Service 開發人員指南 中的存取控制清單 （ACL） 概觀。

其他政策類型

AWS 支援其他較不常見的政策類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可界限是一項進階功能，您可以在其中設定身分型政策可授予IAM實體 （IAM使用者或角色） 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南 中的IAM實體許可界限。
- 服務控制政策 （SCPs） – SCPs是在 中指定組織或組織單位 （OU） 最大許可JSON的政策 AWS Organizations。 AWS Organizations 是一項用於分組和集中管理您企業擁有 AWS 帳戶 之多個的服務。如果您啟用組織中的所有功能，則可以將服務控制政策 （SCPs） 套用至任何或所有帳戶。SCP 限制成員帳戶中實體的許可，包括每個 AWS 帳戶根使用者。如需 Organizations 和 的詳細資訊SCPs，請參閱 AWS Organizations 使用者指南 中的服務控制政策。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南 中的工作階段政策。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。若要了解如何 AWS 在涉及多種政策類型時決定是否允許請求，請參閱 IAM 使用者指南 中的政策評估邏輯。

Amazon One Enterprise 如何與 搭配使用 IAM

在您使用 IAM 管理 Amazon One Enterprise 的存取權之前，請先了解哪些IAM功能可與 Amazon One Enterprise 搭配使用。

IAM 您可以與 Amazon One Enterprise 搭配使用的功能

IAM 功能	Amazon One Enterprise 支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵	是
ACLs	否
ABAC （政策中的標籤）	是
暫時性憑證	是
主體許可	是
服務角色	否
服務連結角色	否

若要取得 Amazon One Enterprise 和其他 AWS 服務如何與大多數IAM功能搭配使用的高階檢視，請參閱 IAM 使用者指南 中的 AWS 服務IAM。

Amazon One Enterprise 的身分型政策

支援身分型政策：是

身分型政策是您可以連接到身分的JSON許可政策文件，例如IAM使用者、使用者群組或角色。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分型政策，請參閱 IAM 使用者指南 中的建立IAM政策。

透過身分IAM型政策，您可以指定允許或拒絕的動作和資源，以及允許或拒絕動作的條件。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。若要了解您可以在JSON政策中使用的所有元素，請參閱 IAM 使用者指南 中的IAMJSON政策元素參考。

Amazon One Enterprise 的身分型政策範例

若要檢視 Amazon One Enterprise 身分型政策的範例，請參閱 Amazon One Enterprise 的身分型政策範例。

Amazon One Enterprise 中的資源型政策

支援資源型政策：否

資源型政策是您連接至資源JSON的政策文件。資源型政策的範例包括IAM角色信任政策和 Amazon S3 儲存貯體政策 。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主體可以包括帳戶、使用者、角色、聯合使用者或 AWS 服務。

若要啟用跨帳戶存取，您可以將另一個帳戶中的整個帳戶或IAM實體指定為資源型政策中的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源位於不同的 時 AWS 帳戶，受信任帳戶中的IAM管理員也必須授予主體實體（使用者或角色）存取資源的許可。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱 IAM 使用者指南 中的跨帳戶資源存取權IAM。

Amazon One Enterprise 的政策動作

支援政策動作：是

管理員可以使用 AWS JSON政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action`元素說明您可以用來允許或拒絕政策中存取的動作。政策動作通常具有與相關聯 AWS API操作相同的名稱。有一些例外狀況，例如沒有相符API操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 Amazon One Enterprise 動作清單，請參閱 Amazon One Enterprise 的動作、資源與條件索引鍵。

Amazon One Enterprise 中的政策動作在動作之前使用下列字首：

```
one
```

如需在單一陳述式中指定多個動作，請用逗號分隔。

```
"Action": [
      "one:action1",
      "one:action2"
         ]
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭是 Describe 文字的所有動作，請包含以下動作：

```
"Action": "one:Describe*"
```

若要檢視 Amazon One Enterprise 身分型政策的範例，請參閱 Amazon One Enterprise 的身分型政策範例。

Amazon One Enterprise 的政策資源

支援政策資源：是

管理員可以使用 AWS JSON政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素會指定動作套用的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 Amazon Resource Name （ ARN ） 指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

若要查看 Amazon One Enterprise 資源類型及其 的清單ARNs，並了解您可以使用哪些動作來指定每個資源ARN的 ，請參閱 Amazon One Enterprise 的動作、資源與條件索引鍵。

若要檢視 Amazon One Enterprise 身分型政策的範例，請參閱 Amazon One Enterprise 的身分型政策範例。

Amazon One Enterprise 的政策條件金鑰

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON政策來指定誰可以存取內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值， 會使用邏輯OR操作 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，只有在IAM使用者使用其IAM使用者名稱標記時，您才能授予使用者存取資源的許可。如需詳細資訊，請參閱 IAM 使用者指南 中的IAM政策元素：變數和標籤。

AWS 支援全域條件索引鍵和服務特定條件索引鍵。若要查看所有 AWS 全域條件索引鍵，請參閱 IAM 使用者指南 中的AWS 全域條件內容索引鍵。

若要查看 Amazon One Enterprise 條件索引鍵的清單，並了解您可以使用條件索引鍵執行哪些動作和資源，請參閱 Amazon One Enterprise 的動作、資源與條件索引鍵。

若要檢視 Amazon One Enterprise 身分型政策的範例，請參閱 Amazon One Enterprise 的身分型政策範例。

ACLs 在 Amazon One Enterprise 中

支援ACLs：否

存取控制清單 （ ACLs ） 控制哪些主體 （ 帳戶成員、使用者或角色 ） 具有存取 資源的許可。ACLs 類似於資源型政策，雖然它們不使用JSON政策文件格式。

ABAC 搭配 Amazon One Enterprise

支援 ABAC（政策中的標籤）：是

屬性型存取控制（ABAC）是根據屬性定義許可的授權策略。在 中 AWS，這些屬性稱為標籤 。您可以將標籤連接至IAM實體（使用者或角色）和許多 AWS 資源。標記實體和資源是 的第一步ABAC。然後，您可以設計ABAC政策，以便在主體的標籤與其嘗試存取的資源上的標籤相符時允許操作。

ABAC 有助於快速成長的環境，並有助於處理政策管理變得繁瑣的情況。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 的詳細資訊ABAC，請參閱 使用者指南 中的什麼是 ABAC？。 IAM 若要檢視包含設定 之步驟的教學課程ABAC，請參閱 IAM 使用者指南 中的使用屬性型存取控制（ABAC）。

搭配 Amazon One Enterprise 使用臨時憑證

支援臨時憑證：是

當您使用臨時憑證登入時，有些 AWS 服務 無法使用。如需詳細資訊，包括 AWS 服務 使用哪些臨時憑證，請參閱 使用者指南 中的 AWS 服務 使用 IAM 。 IAM

如果您 AWS Management Console 使用使用者名稱和密碼以外的任何方法登入 ，則表示您正在使用臨時憑證。例如，當您 AWS 使用公司的單一登入（SSO）連結存取 時，該程序會自動建立臨時憑證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱 IAM 使用者指南 中的切換到角色（主控台）。

您可以使用 AWS CLI 或 手動建立臨時憑證 AWS API。然後，您可以使用這些臨時登入資料來存取 AWS. AWS recommends，讓您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱 中的臨時安全憑證IAM。

Amazon One Enterprise 的跨服務主體許可

支援轉送存取工作階段（FAS）：是

當您使用IAM使用者或角色在 中執行動作時 AWS，您會被視為委託人。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 使用呼叫 的委託人許可 AWS 服務，並結合 請

求向下游服務 AWS 服務 提出請求。FAS 只有在服務收到需要與其他 AWS 服務 或 資源互動才能完成的請求時，才會發出請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出FAS請求的政策詳細資訊，請參閱轉送存取工作階段 。

Amazon One Enterprise 的服務角色

支援服務角色：否

服務角色是服務代表您執行動作時擔任IAM的角色。IAM 管理員可以從 內部建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱 使用者指南 中的建立角色以將許可委派給 AWS 服務 。 IAM

> **Warning**
>
> 變更服務角色的許可可能會中斷 Amazon One Enterprise 功能。只有在 Amazon One Enterprise 提供指引時，才能編輯服務角色。

Amazon One Enterprise 的服務連結角色

支援服務連結角色：否

服務連結角色是連結至 的服務角色類型 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理服務連結角色的詳細資訊，請參閱AWS 使用 的服務IAM。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

Amazon One Enterprise 的身分型政策範例

根據預設，使用者和角色沒有建立或修改 Amazon One Enterprise 資源的許可。他們也無法使用 AWS Management Console、 AWS Command Line Interface （ AWS CLI ） 或 來執行任務 AWS API。若要授予使用者對所需資源執行動作的許可，IAM管理員可以建立IAM政策。然後，管理員可以將IAM政策新增至角色，使用者可以擔任角色。

若要了解如何使用這些範例政策文件來建立IAM身分型JSON政策，請參閱 IAM 使用者指南 中的建立IAM政策。

如需 Amazon One Enterprise 定義之動作和資源類型的詳細資訊，包括ARNs每種資源類型的 格式，請參閱服務授權參考 Amazon One Enterprise 的動作、資源與條件索引鍵中的 。

主題

政策最佳實務

身分型政策會決定某人是否可以在帳戶中建立、存取或刪除 Amazon One Enterprise 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用 AWS 受管政策，將許可授予許多常見使用案例。它們可在您的 中使用 AWS 帳戶。建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。如需詳細資訊，請參閱 IAM 使用者指南 中的 AWS 受管政策或 AWS 受管政策。
- 套用最低權限許可 – 當您使用IAM政策設定許可時， 只會授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的詳細資訊，請參閱 IAM 使用者指南 中的政策和許可IAM。
- 使用IAM政策中的條件來進一步限制存取：您可以將條件新增至政策，以限制對動作和資源的存取。例如，您可以撰寫政策條件來指定所有請求都必須使用 傳送SSL。如果透過特定 使用服務動作，例如 AWS 服務，您也可以使用 條件來授予其存取權 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南 中的IAMJSON政策元素：條件。
- 使用 IAM Access Analyzer 驗證您的IAM政策，以確保安全且功能許可 – IAM Access Analyzer 會驗證新的和現有的政策，讓政策遵循IAM政策語言 （JSON） 和IAM最佳實務。IAM Access Analyzer 提供超過 100 個政策檢查和可操作的建議，協助您撰寫安全且實用的政策。如需詳細資訊，請參閱 IAM 使用者指南 中的IAM存取分析器政策驗證。
- 需要多因素身分驗證 （MFA） – 如果您有需要IAM使用者或 根使用者的案例 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫API操作MFA時要求 ，請將MFA條件新增至您的政策。如需詳細資訊，請參閱 IAM 使用者指南 中的設定 MFA受保護的API存取。

如需 中最佳實務的詳細資訊IAM，請參閱 IAM 使用者指南 中的安全最佳實務IAM。

使用 Amazon One Enterprise 主控台

若要存取 Amazon One Enterprise 主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視 中 Amazon One Enterprise 資源的詳細資訊 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

對於僅對 AWS CLI 或 進行呼叫的使用者，您不需要允許最低主控台許可 AWS API。相反地，僅允許存取與其嘗試執行API的操作相符的動作。

為了確保使用者和角色仍然可以使用 Amazon One Enterprise 主控台，也請將 Amazon One Enterprise *ConsoleAccess*或*ReadOnly* AWS 受管政策連接至實體。如需詳細資訊，請參閱 IAM 使用者指南 中的新增許可給使用者。

允許使用者檢視他們自己的許可

此範例示範如何建立政策，允許使用者檢視連接至其IAM使用者身分的內嵌和受管政策。此政策包含在主控台上完成此動作或使用 AWS CLI 或 以程式設計方式完成此動作的許可 AWS API。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
```

```
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon One Enterprise 的唯讀存取權

下列範例顯示 AWS 受管政策，AmazonOneEnterpriseReadOnlyAccess授予 Amazon One Enterprise 唯讀存取權。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "one:Get*",
        "one:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

在政策陳述式中，Effect 元素指定允許或拒絕動作。Action 元素列出允許使用者執行的特定動作。Resource 元素列出使用者得以執行特定動作的 AWS 資源。對於控制 Amazon One Enterprise 動作存取權的政策，Resource元素一律設定為 *，也就是「所有資源」的萬用字元。

Action 元素中的值對應至APIs服務支援的 。動作前面會加上 ，config:表示它們參考的是 Amazon One Enterprise 動作。您可以在 Action 元素中使用 * 萬用字元，如下列範例所示：

- "Action": ["one:*DeviceInstanceConfiguration"]

  這允許以 "DeviceInstance"（GetDeviceInstanceConfiguration、 ）結尾的所有 Amazon One Enterprise 動作CreateDeviceInstanceConfiguration。
- "Action": ["one:*"]

  這允許所有 Amazon One Enterprise 動作，但不允許其他 AWS 服務的動作。

- `"Action": ["*"]`

  這允許所有 AWS 動作。此許可適用於擔任您帳戶 AWS 管理員的使用者。

唯讀政策不會授予使用者動作的許可`CreateDeviceInstance`，例如 `UpdateDeviceInstance`、和 `DeleteDeviceInstance`。具有此政策的使用者不允許建立裝置執行個體、更新裝置執行個體或刪除裝置執行個體。如需 Amazon One Enterprise 動作的清單，請參閱 Amazon One Enterprise 的動作、資源與條件索引鍵。

Amazon One Enterprise 的完整存取權

下列範例顯示授予 Amazon One Enterprise 完整存取權的政策。它授予使用者執行所有 Amazon One Enterprise 動作的許可。

> **Important**
>
> 此政策會授予廣泛許可。授予完整存取之前，請考慮從最少的一組許可開始，然後依需要授予其他許可。這比一開始使用太寬鬆的許可，爾後再嘗試限縮許可更為安全。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "one:*"
            ],
            "Resource": "*"
        },
    ]
}
```

Amazon One Enterprise Rule API動作的支援資源層級許可

資源層級許可能夠讓您指定使用者可執行動作的資源。Amazon One Enterprise 支援特定 Amazon One Enterprise 規則API動作的資源層級許可。這表示對於某些 Amazon One Enterprise 規則動作，您可以控制允許使用者使用這些動作的條件。這些條件可以是必須滿足的動作，也可以是允許使用者使用的特定資源。

下表說明目前支援資源層級許可的 Amazon One Enterprise 規則API動作。它還描述ARNs了每個動作支援的 資源及其 。指定 時ARN，您可以在路徑中使用 * 萬用字元；例如，當您無法或不想指定確切的資源 時IDs。

> **Important**
>
> 如果此表格中未列出 Amazon One Enterprise 規則API動作，則不支援資源層級許可。如果 Amazon One Enterprise 規則動作不支援資源層級許可，您可以授予使用者使用該動作的許可，但必須為政策陳述式的資源元素指定 *。

API 動作	資源
CreateDeviceInstance	裝置執行個體 arn：aws：one：*region:accountID* ：device-instance/*deviceInstanceId*
GetDeviceInstance	裝置執行個體 arn：aws：one：*region:accountID* ：device-instance/*deviceInstanceId*
UpdateDeviceInstance	裝置執行個體 arn：aws：one：*region:accountID* ：device-instance/*deviceInstanceId*
DeleteDeviceInstance	裝置執行個體 arn：aws：one：*region:accountID* ：device-instance/*deviceInstanceId*
CreateDeviceActivationQrCode	裝置執行個體 arn：aws：one：*region:accountID* ：device-instance/*deviceInstanceId*
DeleteAssociatedDevice	裝置執行個體

API 動作	資源
	arn：aws：one：*region:accountID* ：device-instance/*deviceInstanceId*
RebootDevice	裝置執行個體 arn：aws：one：*region:accountID* ：device-instance/*deviceInstanceId*
CreateDeviceInstanceConfiguration	裝置執行個體組態 arn：aws：one：*region:accountID* ：device-instance/*deviceInstanceId* /組態/*version*
GetDeviceInstanceConfiguration	裝置執行個體組態 arn：aws：one：*region:accountID* ：device-instance/*deviceInstanceId* /組態/*version*
CreateSite	Site arn：aws：one：*region:accountID* ：站台/*siteId*
DeleteSite	Site arn：aws：one：*region:accountID* ：站台/*siteId*
GetSiteAddress	Site arn：aws：one：*region:accountID* ：站台/*siteId*
UpdateSite	Site arn：aws：one：*region:accountID* ：站台/*siteId*
UpdateSiteAddress	Site arn：aws：one：*region:accountID* ：站台/*siteId*

API 動作	資源
CreateDeviceConfigurationTemplate	裝置組態範本 arn：aws：one：*region:accountID* :device-configuration-template/*templateId*
DeleteDeviceConfigurationTemplate	裝置組態範本 arn：aws：one：*region:accountID* :device-configuration-template/*templateId*
GetDeviceConfigurationTemplate	裝置組態範本 arn：aws：one：*region:accountID* :device-configuration-template/*templateId*
UpdateDeviceConfigurationTemplate	裝置組態範本 arn：aws：one：*region:accountID* :device-configuration-template/*templateId*

例如，您希望允許特定使用者的讀取存取和拒絕寫入存取特定規則。

在第一個政策中，您可以允許 AWS Config 規則讀取動作，例如在指定的規則`GetSite`上。

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "VisualEditor0",
                "Effect": "Allow",
                "Action": [
                    "one:GetSite",
                    "one:GetSiteAddress"
                ],
                "Resource": [
                    "arn:aws:one:region:accountID:site/siteId"
                ]
            }
        ]
```

```
    }
```

在第二個政策中，您拒絕針對特定規則執行 Amazon One Enterprise 規則寫入動作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "one:DeleteSite",
                "one:UpdateSiteAddress"
               ],
            "Resource": "arn:aws:one:region:accountID:site/siteId"
           }
      ]
   }
```

透過資源層級許可，您可以允許讀取存取並拒絕寫入存取，以對 Amazon One Enterprise 規則動作執行特定API動作。

其他資訊

若要進一步了解建立IAM使用者、群組、政策和許可，請參閱 IAM 使用者指南 中的建立您的第一個IAM使用者和管理員群組和存取管理。

AWS Amazon 一家企業的受管政策

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新 AWS 服務 API作業可供現有服務使用時，最有可能會更新 AWS 受管理的策略。

如需詳細資訊，請參閱IAM使用指南中的AWS 受管理策略。

AmazonOneEnterpriseFullAccess

此政策授予管理許可，允許存取所有 Amazon One 企業資源和操作。

one:*可讓您執行所有 Amazon 單一企業版動作。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "FullAccessStatementID",
   "Effect": "Allow",
   "Action": [
    "one:*"
   ],
   "Resource": "*"
  }
 ]
}
```

AmazonOneEnterpriseReadOnlyAccess

此政策授予所有 Amazon One 企業級資源和操作的唯讀許可。

one:Get*獲取 Amazon 一個企業資源。

one:List*列出 Amazon 一個企業資源。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "ReadOnlyAccessStatementID",
   "Effect": "Allow",
   "Action": [
```

```
    "one:Get*",
    "one:List*"
   ],
   "Resource": "*"
  }
 ]
}
```

AmazonOneEnterpriseInstallerAccess

此政策授予有限的讀取和寫入權限，允許您為任何已配置的設備實例創建激活 QR 碼以在任何站點激活設備。

one:CreateDeviceActivationQrCode讓您創建 QR 碼以激活設備。

one:GetDeviceInstance可讓您擷取有關 Amazon One 裝置執行個體的資訊。

one:GetSite讓您獲取有關 Amazon One 企業網站的信息。

one:GetSiteAddress讓您獲取 Amazon 一個企業網站的物理地址。

one:ListDeviceInstances讓您列出 Amazon 一個設備實例。

one:ListSites讓您列出 Amazon 一個企業網站。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "InstallerAccessStatementID",
   "Effect": "Allow",
   "Action": [
    "one:CreateDeviceActivationQrCode",
    "one:GetDeviceInstance",
    "one:GetSite",
    "one:GetSiteAddress",
    "one:ListDeviceInstances",
    "one:ListSites"
   ],
   "Resource": "*"
  }
 ]
}
```

Amazon 一個企業版更新受 AWS 管政策

檢視自此服務開始追蹤這些變更以來，已針對 Amazon One 企業版進行的 AWS 受管政策更新詳細資料。如需有關此頁面變更的自動警示，請訂閱 Amazon One 企業文件歷史記錄頁面上的RSS摘要。

變更	描述	日期
Amazon 一個企業開始跟踪變化	Amazon One 企業版開始追蹤其 AWS 受管政策的變更。	2023 年 12 月 1 日

Amazon One Enterprise 的動作、資源與條件索引鍵

Amazon One 企業版 (服務前綴：one) 提供下列服務特定資源、動作和條件內容金鑰，可用於IAM許可政策。

主題

- Amazon One Enterprise 定義的動作
- Amazon One Enterprise 定義的資源類型
- Amazon One Enterprise 的條件索引鍵

Amazon One Enterprise 定義的動作

您可以在IAM策略陳述式的`Action`元素中指定下列動作。使用政策來授予在 AWS中執行操作的許可。當您在策略中使用動作時，通常會允許或拒絕存取具有相同名稱的API作業或CLI命令。不過，在某些情況下，單一動作可控制對多個操作的存取。或者，某些操作需要多種不同的動作。

「動作」資料表的資源類型欄會指出每個動作是否支援資源層級的許可。如果此欄沒有值，您必須在政策陳述式的 `Resource` 元素中指定政策適用的所有資源 ("*")。如果資料行包含資源類型，則您可以使用該動作在陳述式中指定該類型ARN的類型。如果動作具有一或多個必要資源，呼叫者必須具有對這些資源使用動作的許可。表格中的必要資源會以星號 (*) 表示。如果您使用策略中的`Resource`元素限制資源存取，IAM則必須針對每個所需資源類型包含ARN或模式。某些動作支援多種資源類型。如果資源類型是選用 (未顯示為必要)，則您可以選擇使用其中一種選用資源類型。

「動作」資料表的條件索引鍵欄包含您可以在政策陳述式的 `Condition` 元素中指定的索引鍵。如需有關與服務資源相關聯之條件索引鍵的詳細資訊，請參閱「資源類型」資料表的條件索引鍵欄。

> **Note**
>
> 資源條件索引鍵會列在資源類型資料表中。您可以在「動作」資料表的資源類型 (*必填) 欄中找到適用於動作的資源類型連結。「資源類型」資料表中的資源類型包括條件索引鍵欄，其中包含套用至「動作」資料表中動作的資源條件索引鍵。

如需下表各欄的詳細資訊，請參閱動作資料表。

動作	描述	存取層級	資源類型 (*必填項目)	條件索引鍵	相依動作
CreateDeviceInstance	授予創建設備實例的權限	寫入		aws:RequestTag/${TagKey} aws:TagKeys	
GetDeviceInstance	授予權限以獲取有關設備實例的信息	讀取	裝置執行個體 *		
ListDeviceInstances	授予列出設備實例的權限	讀取			
UpdateDeviceInstance	授予更新設備實例的權限	寫入	裝置執行個體 *		
DeleteDeviceInstance	授予刪除設備實例的權限	寫入	裝置執行個體 *		
CreateDeviceActivationQrCode	授予創建 QR 碼以在設備實例激活設備的權限	寫入	裝置執行個體 *		
DeleteAssociatedDevice	授予刪除設備和設備實例之間關聯的權限	寫入	裝置執行個體 *		

動作	描述	存取層級	資源類型 (*必填項目)	條件索引鍵	相依動作
RebootDevice	授予重新啟動設備的權限	寫入	裝置執行個體 *		
CreateDeviceInstanceConfiguration	授予創建設備實例配置的權限	寫入			
GetDeviceInstanceConfiguration	授予權限以獲取有關設備實例配置的信息	讀取	配置 *		
CreateSite	授予建立網站的權限	寫入		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSite	授予刪除設備實例的權限	寫入	網站 *		
GetSite	授予獲取有關網站信息的權限	讀取	網站 *		
ListSites	授予列出網站的權限	讀取			
GetSiteAddress	授予獲取有關站點地址信息的權限	讀取	網站 *		
UpdateSite	授予更新網站的權限	寫入	網站 *		
UpdateSiteAddress	授予更新網站地址的權限	寫入	網站 *		

動作	描述	存取層級	資源類型 (*必填項目)	條件索引鍵	相依動作
CreateDeviceConfigurationTemplate	授予創建設備實例的權限	寫入		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDeviceConfigurationTemplate	授予刪除裝置設定範本的權限	寫入	device-configuration-template*		
GetDeviceConfigurationTemplate	授予權限以獲取有關設備配置模板的信息	讀取	device-configuration-template*		
ListDeviceConfigurationTemplates	授予列出設備配置模板的權限	讀取			
UpdateDeviceConfigurationTemplate	授予更新設備配置模板的權限	寫入	device-configuration-template*		
TagResource	准許標記資源	標記	裝置執行個體、網站、device-configuration-template	aws:RequestTag/${TagKey} aws:TagKeys	

動作	描述	存取層級	資源類型 (*必填項目)	條件索引鍵	相依動作
UntagResource	准許取消標記資源	標記	裝置執行個體、網站、device-configuration-template	aws:TagKeys	
ListTagForResources	准許列出資源的標籤	讀取			

Amazon One Enterprise 定義的資源類型

下列資源類型由此服務定義，可用於IAM權限原則陳述式的Resource元素中。動作資料表中的每個動作都會指明可使用該動作指定的資源類型。資源類型也能定義您可以在政策中包含哪些條件索引鍵。這些索引鍵都會顯示在「資源類型」資料表的最後一欄。如需下表各欄的詳細資訊，請參閱資源類型資料表。

資源類型	ARN	條件索引鍵
Device Instance	`arn:aws:one: region:accountID :device-instance/ deviceInstanceId`	aws:ResourceTag/${TagKey}
Device Instance Configuration	`arn:aws:one: region:accountID :device-instance/ deviceInstanceId /configuration/ version`	
Site	`arn:aws:one: region:accountID :site/siteId`	aws:ResourceTag/${TagKey}
Device Configuration Template	`arn:aws:one: region:accountID :device-configuration-template/ templateId`	aws:ResourceTag/${TagKey}

Amazon One Enterprise 的條件索引鍵

Amazon One 企業版定義了下列可用於IAM政策Condition元素的條件金鑰。您可以使用這些索引鍵來縮小套用政策陳述式的條件。如需下表各欄的詳細資訊，請參閱條件索引鍵資料表。

若要檢視所有服務都可使用的全域條件索引鍵，請參閱可用全域條件索引鍵。

條件索引鍵	描述	Type
aws:RequestTag/${TagKey}	按照請求的標籤來篩選存取權	字串
aws:ResourceTag/${TagKey}	依與資源關聯的標籤來篩選存取權	字串
aws:TagKeys	按照請求的標籤金鑰來篩選存取權	ArrayOfString

Amazon 一家企業版的合規驗證

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上進行HIPAA安全與合規架構 — 本白皮書說明公司如何使用建立符合資格的應 AWS 用程HIPAA式。

> **Note**
>
> 並非所有 AWS 服務 人都HIPAA符合資格。如需詳細資訊，請參閱合HIPAA格服務參考。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準 AWS 服務 與技術研究所 (NIST)、支付卡產業安全標準委員會 () 和國際標準化組織 (PCI)) 中保護指引的最佳做法，並將其對應至安全控制。ISO
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您因應各種合規性需求 PCIDSS，例如符合特定合規性架構所要求的入侵偵測需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

監控 Amazon One Enterprise

監控是維護 Amazon One Enterprise 和其他 AWS 解決方案可靠性、可用性和效能的重要部分。 AWS 提供下列監控工具來監看 Amazon One Enterprise、報告錯誤，並在適當時採取自動動作：

- Amazon EventBridge 可用來自動化您的 AWS 服務，並自動回應系統事件，例如應用程式可用性問題或資源變更。來自 AWS 服務的事件會以 EventBridge 近乎即時的方式交付至 。您可編寫簡單的規則，來指示您在意的事件，以及當事件符合規則時所要自動執行的動作。如需詳細資訊，請參閱 Amazon EventBridge 使用者指南 。
- AWS CloudTrail 會擷取由 帳戶或代表 AWS 您的帳戶進行的API呼叫和相關事件，並將日誌檔案傳送到您指定的 Amazon S3 儲存貯體。您可以識別名為 的使用者和帳戶 AWS、進行呼叫的來源 IP 地址，以及呼叫的時間。如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》https://docs.aws.amazon.com/awscloudtrail/latest/userguide/。

監控 Amazon 中的 Amazon One Enterprise 事件 EventBridge

您可以在 中監控 Amazon One Enterprise 事件 EventBridge，該事件可從您自己的應用程式、software-as-a-service （ SaaS ） 應用程式 AWS 和服務提供即時資料串流。 EventBridge 會將該資料路由到目標，例如 AWS Lambda 和 Amazon Simple Notification Service。這些事件提供近乎即時的系統事件串流，描述 AWS 資源的變更。

訂閱 Amazon One Enterprise 事件

Amazon One 裝置和使用者設定檔狀態變更事件會使用 發佈 EventBridge，並且可以透過建立新規則在 EventBridge 主控台中啟用。儘管事件沒有排序，但它們具有時間戳記，可讓您使用資料。事件會盡可能發出。

訂閱 Amazon One Enterprise 事件

1. 在 開啟 EventBridge 主控台https://console.aws.amazon.com/events/。
2. 在導覽窗格中的 Buses 下，選擇規則 。
3. 選擇建立規則。
4. 在預設規則詳細資訊頁面上，為規則指派名稱，選擇具有事件模式 的規則，然後選擇下一個 。
5. 在建立事件模式頁面的事件來源 下，確認已選取AWS 事件或 EventBridge 合作夥伴事件。
6. 在範例事件類型 下，選擇輸入我自己的 。

7. 從其中一個 複製並貼上範例事件。
8. 對於建立方法 ，選擇自訂模式 。在事件模式區段中，將JSON事件來源作為 aws:one和所需詳細資訊類型新增 ，然後選擇下一步。
9. 在選取目標 （ Select target ） 頁面上，選取您選擇的目標，其中包含 Lambda 函數、SQS佇列或SNS主題。如需設定目標的相關資訊，請參閱 Amazon EventBridge 目標。
10. 或者，您可以設定標籤。
11. 在 檢閱和建立 頁面上，選擇 建立規則。如需設定規則的詳細資訊，請參閱 EventBridge 使用者指南中的 EventBridge規則。

裝置狀態變更事件類型

裝置狀態變更事件會在 中產生JSON。對於每個事件類型，blob JSON 會傳送至您選擇的目標，如規則中所設定。下列詳細資訊類型可供使用：

裝置運作狀態已變更為運作狀態

裝置已通過所有運作狀態檢查。

裝置運作狀態已變更為重大

裝置未通過一或多個運作狀態檢查。

裝置連線已變更為離線

裝置未連線至網際網路。

裝置連線已變更為線上

裝置已連線至網際網路。

resources

包含發佈裝置狀態變更事件的 deviceInstance arn 清單。

中繼資料

siteName

- deviceInstance 存在 的網站名稱。

siteArn

- Arn 適用於 deviceInstance 存在 的網站。

資料

currentConnectivity

- 表示 deviceInstance 是否連線至網際網路，還是中斷與網際網路的連線。
- 可能的值：CONNECTED、 DISCONNECTED

previousConnectivity

- 表示事件之前 deviceInstance 是否連線至網際網路或中斷連線。
- 可能的值：CONNECTED、 DISCONNECTED

currentHealthStatus

- 表示 deviceInstance 是否已通過所有運作狀態檢查。
- 可能的值：HEALTHY、 CRITICAL

previousHealthStatus

- 表示上次檢查時是否 deviceInstance 通過所有運作狀態檢查。
- 可能的值：HEALTHY、 CRITICAL

assetTagId

- 與 相關聯的 assetTagId 裝置 。 deviceInstance

deviceInstanceName

- 發佈 deviceInstance 裝置狀態事件的 名稱。

使用者設定檔事件類型

使用者設定檔相關事件詳細資訊類型為：

新的成功註冊

當使用者註冊成功時。

新的成功取消註冊

當使用者成功取消註冊時。

註冊失敗

當使用者無法註冊時。

未成功取消註冊

當使用者無法取消註冊時。

成功辨識

當使用者掃描手掌以成功進行身分驗證時。

辨識失敗

當手掌掃描的識別失敗時。

resources

包含發佈使用者設定檔事件的使用者設定檔清單。

資料

accountId

- 發起請求之裝置的相關 AWS 帳戶。

requestSource

- 這是起始請求的裝置 deviceInstanceId 。

createdTimestamp

- 建立事件的時間。

userStatus

- 使用者的目前狀態。
- 可能的值：ACTIVE、 DELETED

associatedId

- 使用者的關聯 ID，例如徽章 ID。

reason

- 不成功的事件將出現此值。它包含事件失敗的原因。

範例事件

下列範例顯示 Amazon One Enterprise 的事件。

主題

- 裝置運作狀態已變更為運作狀態
- 裝置運作狀態已變更為重大
- 裝置連線已變更為線上
- 裝置連線已變更為離線
- 新的成功註冊

裝置運作狀態已變更為運作狀態

裝置已通過所有運作狀態，且裝置執行個體運作狀態HEALTHY已從CRITICAL運作狀態變更為 。

```
{
    "version": "0",
    "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
    "detail-type": "Device Health Status Changed To Healthy",
    "source": "aws.one",
    "account": "123456789012",
    "time": "2022-10-22T18:43:48Z",
    "region": "us-east-1",
    "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
    "detail": {
    "version": "1.0.0",
    "metadata": {
      "siteName": "Site name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    },
    "data": {
      "currentHealthStatus": "HEALTHY",
      "previousHealthStatus": "CRITICAL",
      "assetTagId": "0000195169",
      "deviceInstanceName": "Device name"
    }
  }
}
```

裝置運作狀態已變更為重大

裝置運作狀態檢查失敗，且裝置執行個體運作狀態CRITICAL從 變更為 HEALTHY。

```
{
  "version": "0",
```

```
  "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
  "detail-type": "Device Health Status Changed To Critical",
  "source": "aws.one",
  "account": "123456789012",
  "time": "2022-10-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
  "detail": {
    "version": "1.0.0",
    "metadata": {
      "siteName": "Site name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    },
    "data": {
      "currentHealthStatus": "CRITICAL",
      "previousHealthStatus": "HEALTHY",
      "assetTagId": "0000195169",
      "deviceInstanceName": "Device name"
    }
  }
}
```

裝置連線已變更為線上

裝置已連線至網際網路，且裝置執行個體的連線狀態CONNECTED已從 變更為 DISCONNECTED。

```
{
  "version": "0",
  "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
  "detail-type": "Device Connectivity Changed To Online",
  "source": "aws.one",
  "account": "123456789012",
  "time": "2022-10-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
  "detail": {
    "version": "1.0.0",
    "metadata": {
      "siteName": "Site name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    },
    "data": {
      "currentConnectivity": "CONNECTED",
```

```
      "previousConnectivity": "DISCONNECTED",
      "assetTagId": "0000195169",
      "deviceInstanceName": "Device name"
    }
  }
}
```

裝置連線已變更為離線

裝置未連線至網際網路，且裝置執行個體的連線狀態DISCONNECTED已從 變更為 CONNECTED。

```
{
  "version": "0",
  "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
  "detail-type": "Device Connectivity Changed To Offline",
  "source": "aws.one",
  "account": "123456789012",
  "time": "2022-10-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
  "detail": {
    "version": "1.0.0",
    "metadata": {
      "siteName": "Site name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    },
    "data": {
      "currentConnectivity": "DISCONNECTED",
      "previousConnectivity": "CONNECTED",
      "assetTagId": "0000195169",
      "deviceInstanceName": "Device name"
    }
  }
}
```

新的成功註冊

使用者已成功註冊的事件。

```
{
    "version": "0",
    "id": "aebc9c86-f20e-75db-caaa-63bf14926f59",
```

```
    "detail-type": "New Successful Enrollment",
    "source": "aws.one",
    "account": "679792848029",
    "time": "2023-11-22T02:55:17Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:one:us-east-1:679792848029:user"
    ],
    "detail": {
        "version": "1.0.0",
        "data": {
            "accountId": "679792848029",
            "enrollmentSource": "QfUuUnFqs5accJ",
            "createdTimestamp": "2023-11-22T02:55:17Z",
            "userStatus": "ACTIVE",
            "associatedIds": "[{\"associatedIdType\":\"badge\",\"associatedIdValue\":
\"1111358294500\"}]",
        }
    }
}
```


使用記錄 Amazon 一個企業API通話 AWS CloudTrail

Amazon One 企業與一項服務整合在一起 AWS CloudTrail，該服務可提供 Amazon One 企業中使用者、角色或 AWS 服務所採取的動作記錄。 CloudTrail 以活動形式擷取 Amazon 單一企業版的所有API呼叫。擷取的呼叫包括來自 Amazon One 企業主控台的呼叫，以及對 Amazon One 企業版API操作的程式碼呼叫。如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括 Amazon One 企業版的事件。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷向 Amazon One Enterprise 提出的請求、提出請求的來源 IP 地址、提出請求的人員、提出請求的時間以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail 用者指南。

Amazon 一個企業信息 CloudTrail

CloudTrail 在您創建帳戶 AWS 帳戶 時啟用。當 Amazon One Enterprise 中發生活動時，該活動會與事件歷史記錄中的其他 AWS 服務 CloudTrail 事件一起記錄在事件中。您可以查看，搜索和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

如需您 AWS 帳戶的事件的持續記錄 (包括 Amazon One 企業的活動)，請建立追蹤。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的

AWS 區域。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌文件並從多個帳戶接收 CloudTrail 日誌文件

所有 Amazon One 企業版動作都會由記錄， CloudTrail 並將記錄在Amazon One Enterprise 的動作、資源與條件索引鍵. 例如，呼叫RebootDevice和DeleteDeviceInstance動作會ListSites在 CloudTrail 記錄檔中產生項目。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 要求是使用 root 或 AWS Identity and Access Management (IAM) 使用者認證提出的。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱CloudTrail userIdentity元素。

了解 Amazon 一個企業日誌文件項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共API調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

下列範例顯示示範CreateSite動作的 CloudTrail 記錄項目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAKDBGOAT6C2EXAMPLE:J_DOE",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin/J_DOE",
        "accountId": "123456789012",
        "accessKeyId": "AKIALAVPULGA71EXAMPLE",
        "sessionContext": {
```

```
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAKDBGOAT6C2EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-10-11T06:28:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-10-11T07:19:09Z",
    "eventSource": "one.amazonaws.com",
    "eventName": "CreateSite",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "XXX.XXX.XXX.XXX",
    "userAgent": "userAgent",
    "requestParameters": {
        "name": "***",
        "description": "***",
        "address": {
            "addressLine1": "***",
            "addressLine2": "***",
            "addressLine3": "***",
            "city": "EXAMPLE_CITY",
            "postalCode": "12345",
            "countryCode": "EXAMPLE_COUNTRY",
            "stateOrRegion": "EXAMPLE_STATE"
        },
        "clientToken": "abc12d34-567e-8910-1112-12fghi0jk13l"
    },
    "responseElements": {
        "stateOrRegion": "EXAMPLE_STATE",
        "createdAtInMillis": 1697008749263,
        "city": "EXAMPLE_CITY",
        "countryCode": "EXAMPLE_COUNTRY",
        "deviceInstanceCount": 0,
        "postalCode": "12345",
        "name": "***",
        "description": "***",
        "siteId": " abCdefG12hijkL",
```

```
        "siteArn": "arn:aws:one:us-east-1:123456789012:site/abCdefG12hijkL",
        "tags": "***"
    },
    "requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
    "eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Amazon One Enterprise 疑難排解

如果您對於 Amazon One 裝置或其中一個 Amazon One 裝置有問題，請使用這些建議來疑難排解問題。然後，如果您仍然遇到問題，請聯絡 AWS 支援。

主題

對 Amazon One Enterprise 身分和存取權進行疑難排解

使用下列資訊來協助您診斷和修正使用 Amazon One Enterprise 和 時可能遇到的常見問題IAM。

主題

我無權在 Amazon One Enterprise 中執行動作

如果您收到錯誤，告知您未獲授權執行動作，您的政策必須更新，允許您執行動作。

當mateojacksonIAM使用者嘗試使用主控台檢視虛構*my-example-widget*資源的詳細資訊，但沒有虛構one:*GetWidget*許可時，會發生下列錯誤範例。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 one:GetWidget on resource: my-example-widget
```

在此情況下，必須更新 mateojackson 使用者的政策，允許使用 one:*GetWidget* 動作存取 *my-example-widget* 資源。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想要允許 以外的人員 AWS 帳戶 存取我的 Amazon One Enterprise 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。對於支援資源型政策或存取控制清單（ACLs）的服務，您可以使用這些政策來授予人員對資源的存取權。

如需進一步了解，請參閱以下內容：

- 若要了解 Amazon One Enterprise 是否支援這些功能，請參閱 Amazon One Enterprise 如何與 搭配使用 IAM。
- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱 IAM 使用者指南 中的在您 AWS 帳戶 擁有的另一個資源中為IAM使用者提供存取權。
- 若要了解如何提供資源存取權給第三方 AWS 帳戶，請參閱 使用者指南 中的提供存取權給第三方 AWS 帳戶 擁有。 IAM
- 若要了解如何透過身分聯合提供存取權，請參閱 IAM 使用者指南 中的為外部驗證的使用者提供存取權（身分聯合）。
- 若要了解跨帳戶存取使用角色和資源型政策之間的差異，請參閱 IAM 使用者指南 中的跨帳戶資源存取IAM。

對 Amazon One 主控台進行故障診斷

如果您對於 Amazon One Console 或其中一個 Amazon One 裝置有問題，請使用這些建議來疑難排解問題。然後，如果您仍然遇到問題，請聯絡 AWS 支援。

主題

我無法建立網站

- 請聯絡您的 Amazon One Console 管理員以提供您存取權。
- 如果問題仍然存在，請聯絡 AWS 支援。

我無法建立裝置執行個體

- 請聯絡您的 Amazon One Console 管理員以提供您存取權。
- 如果問題仍然存在，請聯絡 AWS 支援。

我無法建立組態範本

- 請聯絡您的 Amazon One Console 管理員以提供您存取權。
- 如果問題仍然存在，請聯絡 AWS 支援。

我無法建立啟用 QR 碼

- 請聯絡您的 Amazon One Console 管理員以提供您存取權。
- 如果問題仍然存在，請聯絡 AWS 支援。

Amazon One 裝置疑難排解

如果您對於 Amazon One Console 或其中一個 Amazon One 裝置有問題，請使用這些建議來疑難排解問題。然後，如果您仍然遇到問題，請聯絡 AWS 支援。

主題

- 裝置畫面上的 Amazon 標誌，沒有進一步活動
- 暫時無法使用
- 裝置已鎖定
- 結束時發生問題
- 暫時停止服務
- Amazon One 裝置有實體損壞
- 無法讀取手掌
- 無法辨識 Palm
- 由於長時間閒置而鎖定裝置

空白畫面

當裝置沒有電源或在重新啟動期間卡住時，就會發生這種情況。

執行下列動作來疑難排解此問題：

- 等待一段時間（少於 30 秒），以防裝置重新啟動。
- 如果裝置為空白時燈環正在閃爍，請等待最多 30 秒。
- 檢查電源線是否已同時插入電源插座，以及是否穩固地插入 Amazon One 裝置後方。此外，請檢查電源線是否未損壞。
- 檢查電源。
- 檢查所有纜線是否已正確連接至 Amazon One 和USB中樞。
- 從主控台重新啟動裝置。
- 如果重新啟動裝置無法修正問題，請從電源供應器拔掉 Amazon One USB中樞的電源，然後重新插入。
- 如果問題仍然存在，請聯絡 AWS 支援。

我無法連線至 Wi-Fi 或網路

當裝置失去連線時，就會發生這種情況。

執行下列動作來疑難排解此問題：

- 如果連線至 Wi-Fi，請使用另一個裝置來檢查 Wi-Fi 是否顯示在可用網路中。

- 檢查 Wi-Fi 路由器是否已開啟並在範圍內。
- 網路復原後，裝置會重新連線。
- 如果問題仍然存在，請聯絡 AWS 支援。

系統錯誤

由於內部錯誤，因此會發生這種情況。

執行下列動作來疑難排解此問題：

- 在畫面上選擇重新啟動以重新啟動應用程式。
- 嘗試 2 次後，如果問題未解決，請聯絡 AWS 支援。

無法辨識 QR 碼

這是因為未經授權的 QR 碼或過期的 QR 碼。

執行下列動作來疑難排解此問題：

- 選擇再試一次以導覽回 QR 碼畫面。
- 在AWS主控台上建立新的 QR 碼，然後掃描有效的 QR 碼。

無法讀取 QR 碼

當應用程式無法讀取 QR 碼時，就會發生這種情況。

執行下列動作來疑難排解此問題：

- 選擇重試以導覽回 QR 碼畫面。
- 如果問題仍然存在，請取消啟用工作流程並重新啟動。

偵測到多個 QR 碼

掃描多個 QR 碼時會發生這種情況。

執行下列動作來疑難排解此問題：

- 選擇再試一次以導覽回 QR 碼畫面。

- 一次只掃描一個有效的 QR 碼。

裝置執行個體不存在

當裝置執行個體已刪除或主控台中不存在時，就會發生這種情況AWS。

執行下列動作來疑難排解此問題：

- 選擇重試以導覽回 QR 碼畫面。
- 檢查AWS主控台是否有正確的裝置執行個體。如果裝置執行個體遺失，請聯絡您的管理員。
- 為該裝置執行個體建立新的 QR 碼，然後掃描新的 QR 碼。

找不到網站

當刪除網站或在AWS主控台中不存在時，就會發生這種情況。

執行下列動作來疑難排解此問題：

- 檢查AWS主控台以取得網站資訊。如果網站不存在，請聯絡您的管理員。

ZIP 代碼不相符

當輸入與為裝置設定的程式碼不同的ZIP程式碼時，就會發生這種情況。

執行下列動作來疑難排解此問題：

- 選擇再試一次以導覽回ZIP程式碼畫面。
- 檢查您是否有正確的網站ZIP代碼。
- 如果問題仍然存在，請聯絡您的管理員，以在AWS主控台上檢查網站ZIP代碼。

閘道逾時

當閘道在指定時間內沒有回應時，就會發生這種情況。

執行下列動作來疑難排解此問題：

- 選擇重新啟動以重新啟動應用程式。
- 嘗試兩次後，如果問題未解決，請聯絡 AWS 支援。

我無法設定裝置

當操作無法在裝置磁碟上儲存組態時，就會發生這種情況。

執行下列動作來疑難排解此問題：

- 選擇重新啟動以重新啟動應用程式。
- 嘗試兩次後，如果問題未解決，請聯絡 AWS 支援。

裝置已重新啟動，並顯示錯誤訊息和錯誤碼

執行下列動作來疑難排解此問題：

- 選擇重新啟動 ，並讓裝置復原。
- 如果裝置未復原，請從電源供應器拔掉USB集線器並重新連接。
- 如果問題仍然存在，請聯絡 AWS 支援。

裝置畫面上的 Amazon 標誌，沒有進一步活動

執行下列動作來疑難排解此問題：

- 等待一段時間（少於 30 秒），以防裝置重新啟動。
- 將USB集線器從電源拔除並重新連接。
- 如果問題仍然存在，請聯絡 AWS 支援。

暫時無法使用

執行下列動作來疑難排解此問題：

- 確保與主機裝置/系統的USB連線安全。
- 中斷連線並重新連接所有進入USB集線器的纜線。
- 如果問題仍然存在，請聯絡 AWS 支援。

裝置已鎖定

基於安全考量，Amazon One 裝置將在發生任何竄改事件時鎖定。

執行下列動作來疑難排解此問題：

- 聯絡 AWS 支援

結束時發生問題

當發生內部錯誤時，就會發生這種情況。

執行下列動作來疑難排解此問題：

1. 關閉裝置。
2. 中斷其與電源供應器的連線。
3. 等待 30 秒。
4. 將裝置插回電源。
5. 開啟裝置電源。
6. 如果問題仍然存在，請聯絡 AWS 支援。

暫時停止服務

當 Amazon One 將裝置移出服務時，就會發生這種情況。

執行下列動作來疑難排解此問題：

- 聯絡 AWS 支援

Amazon One 裝置有實體損壞

執行下列動作來疑難排解此問題：

- 如需後續步驟，請聯絡 AWS 支援，並盡可能提供詳細資訊，例如發生了什麼、何時發生，以及發生的原因。

無法讀取手掌

執行下列動作來疑難排解此問題：

- 再次檢查 Amazon One 裝置是否沒有條紋和污點。

- 確保客戶的掌心沒有阻塞，例如繃帶、袖子和明顯的髒污/油漬。
- 如果問題仍然存在，且裝置無法讀取任何手掌，請聯絡AWS支援。

無法辨識 Palm

執行下列動作來疑難排解此問題：

- 請客戶嘗試使用另一個手掌。
- 確保客戶已註冊。如果沒有，請讓他們在線上或在裝置上註冊。
- 如果問題仍然存在，且裝置不會讀取任何手掌聯絡人，請聯絡AWS支援。

由於長時間閒置而鎖定裝置

當裝置懷疑已從啟用網站移動時，它會鎖定使用者。當裝置超過最長離線時間時，就會發生這種情況。

執行下列動作以解除鎖定裝置：

1. 從頁面頂端的錯誤橫幅中，選取修復 。
2. 如果裝置仍位於啟用網站，請選擇是，裝置位於此網站 。
3. 如果裝置位於不同的網站，請選擇否，裝置位於不同的網站 。選擇否會停用裝置。在新站台啟用裝置。

Amazon One Enterprise 使用者指南的文件歷史記錄

下表說明 Amazon One Enterprise 的文件版本。

變更	描述	日期
更新	已新增：案例驅動的內容	2024 年 10 月 10 日
更新	新增主題：Amazon One Enterprise 主控台疑難排解	2024 年 10 月 10 日
更新	新增主題：Amazon One Enterprise 裝置疑難排解	2024 年 10 月 10 日
更新	新增章節：設定 Amazon One Enterprise	2024 年 10 月 10 日
更新	新增主題：維護和清潔 Amazon One Enterprise 裝置	2024 年 10 月 10 日
更新	重新組織的內容	2024 年 10 月 10 日
更新	新增主題：安裝 Amazon One Enterprise 裝置 I/O Hub 以進行安全存取	2024 年 8 月 14 日
更新	新增主題：安裝壁掛式 Amazon One Enterprise 裝置	2024 年 6 月 5 日
初始版本	Amazon One Enterprise 使用者指南的初始版本	2023 年 11 月 27 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。