aws

使用者指南

Amazon One

Amazon One: 使用者指南

Table of Contents

什麼是 Amazon One Enterprise？

Amazon One Enterprise 是一項新的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、PINs或密碼。

主題

Amazon One 裝置

Amazon One 裝置專為 Amazon One Enterprise 所設計，Amazon One Enterprise 是一種安全、以掌上型為基礎的身分服務，可用於企業存取控制。請注意下列裝置規格：

- 使用者輸入 — Palm Biometrics、QR Code 比對
- 主機界面 — Wi-Fi (2.4 GHz 和 5 GHz)、乙太網路、2x USB Type-A、1 個 USB Type-B
- 使用者意見回饋 — 5.5 吋觸控螢幕、Lightring、喇叭、耳機
- 實體存取控制通訊協定 — OSDP 和 Wiegand
- 電源 — POE，提供 110/220 VAC 輸入 AC 至 DC 轉接器，30W @ 15V
- 安全 — 竄改開關
- 維度 (HxWxD mm) — 86 x 85 x 256

Amazon One Enterprise 主控台

Amazon One Enterprise 包含主控台，可用下列方式使用：

- IT 或設施管理員使用 Amazon One Enterprise 來建立和管理網站。網站類似於團隊在監控和管理 Amazon One Enterprise 裝置和使用者設定檔時執行的任務的實體位置。IT 或設施管理員任務包括：
  - 建立網站以包含實體位置中的所有 Amazon One 裝置執行個體
  - 新增管理使用者以管理網站，以及安裝使用者以存取啟用 QR 碼
- 管理員使用 Amazon One Enterprise 來建立裝置執行個體和管理 Amazon One 裝置。管理員任務包括：
  - 在網站下建立裝置執行個體
  - 建立要套用至裝置執行個體的組態範本

  - 監控裝置運作狀態並更新裝置組態
  - 取消使用者註冊

- 安裝程式使用 Amazon One Enterprise 存取啟用 QR 碼來啟用裝置。安裝程式任務包括：
  - 在主控台上存取啟用 QR 碼
  - 選取對應至要啟用之裝置執行個體的 QR 碼
  - 在已安裝 Amazon One 裝置的情況下掃描選取的 QR 碼

購買 Amazon One 裝置

聯絡我們以進一步了解 Amazon One Enterprise，業務開發團隊成員會與您聯絡，分享我們產品的詳細資訊，包括定價，並回答您可能有的任何問題。

Amazon One Enterprise 定價

請聯絡我們，進一步了解 Amazon One Enterprise 定價。

Amazon One 的運作方式

Amazon One 是雲端型生物識別服務，使用 Amazon One 裝置來驗證使用者的掌部生物識別。您可以聯絡我們來訂購 Amazon One 裝置。

安裝 Amazon One 裝置後，您可以在 Amazon One Console 和身分驗證應用程式上啟用並註冊裝置至您的 AWS 帳戶。您可以檢視已註冊的使用者生物識別設定檔。如有需要，您可以取消其註冊並刪除其生物識別資料。

Amazon One Console 可做為管理營運活動的集中中心，例如追蹤裝置和檢視每月帳單。使用者可以在現場受監督的註冊站掃描他們的掌心來註冊。註冊後，使用者可以透過將掌心懸停在已啟用 Amazon One 的裝置上，無縫進入或退出安全位置。

主題

Amazon One 工作流程

以下詳細說明 Amazon One 的基本工作流程：

1. 聯絡我們，購買並安裝 Amazon One 裝置。
2. 安裝裝置後，請啟用 Amazon One。
3. 登入您的 Amazon One 帳戶。
4. 設定使用者註冊和進入裝置。
5. 註冊員工掌心。
6. 使用管理和監控功能來確保裝置運作狀態、讓組態保持在最新狀態，並追蹤使用者註冊以進行全面監督。

Amazon One 關鍵術語

以下是 Amazon One 的重要術語：

- 網站 — 客戶安裝 Amazon One 裝置的客戶受管實體建築物。網站必須符合 Amazon One 裝置的設施、聯網和電源要求。

- 裝置 — 用於身分驗證的 Amazon One Palm 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
  - 準備好啟用
  - 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 主控台

本章說明開始使用 Amazon One 主控台的基本步驟。

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您的 Amazon One 裝置，然後使用 Amazon One Enterprise 主控台來設定和管理它們。視網站數量、裝置執行個體和您的組態範本而定，您只會偶爾或甚至只使用一次此程序。

主題

註冊 AWS 帳戶

如果您還沒有 AWS 帳戶，請完成下列步驟建立新帳戶。

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。

   註冊 AWS 帳戶時，會建立 AWS 帳戶根使用者。根使用者有權存取該帳戶中的所有 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

註冊程序完成後，AWS 會傳送一封確認電子郵件給您。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，請保護您的 AWS 帳戶根使用者、啟用 AWS IAM Identity Center，並建立管理使用者，讓您不會將根使用者用於日常任務。

主題

保護您的 AWS 帳戶

現在您已登入 Amazon One 帳戶，請保護您的帳戶。

保護您的 AWS 帳戶根使用者

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

   如需使用根使用者登入的說明，請參閱《AWS 登入使用者指南》中的以根使用者身分登入。
3. 若要在您的根使用者帳戶上啟用多重要素驗證 (MFA)。

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

建立具有管理存取權的使用者

現在您已保護 Amazon One 帳戶，請建立具有管理存取權的使用者。

若要建立具有管理存取權的使用者

1. 啟用 IAM Identity Center。

   如需說明，請參閱《AWS IAM Identity Center 使用者指南》中的啟用 AWS IAM Identity Center。
2. 在 IAM Identity Center 中，將管理存取權授予使用者。

   如需使用 IAM Identity Center 目錄做為身分來源的教學課程，請參閱《AWS IAM Identity Center 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 使用者時傳送到您電子郵件地址的登入 URL，與您的 IAM Identity Center 使用者登入。

  如需使用 IAM Identity Center 使用者登入的說明，請參閱 AWS Sign-In User Guide (《AWS 登入使用者指南》) 中的 Signing in to the AWS access portal (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。

  如需說明，請參閱《AWS IAM Identity Center 使用者指南》中的新增群組。

新增 Amazon One 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 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 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。使用者名稱最多可組合 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，您不可以建立兩個名為 TESTUSER 和 testuser 的使用者。使用者名稱用在政策中或作為 ARN 的一部分時，名稱區分大小寫。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. 選取您要連接到使用者的政策。

    - AmazonOneEnterpriseReadOnlyAccess
    - AmazonOneEnterpriseInstallerAccess

> **Note**
>
> AmazonOneEnterpriseInstallerAccess 受管政策只會在 Amazon One Enterprise 主控台中讓使用者存取啟用 QR 碼。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 IAM 中使用標籤的詳細資訊，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
    - 帳戶登入頁面的 URL。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 主控台來建立您的網站。

> **Important**
>
> Amazon One 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 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. 在網站資訊下，針對網站名稱輸入網站的名稱。

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 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 主控台。
2. 在導覽窗格中，選擇裝置執行個體。請確定您位於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 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 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 登入資料。
   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，以與您的控制面板進行通訊。
   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 登入資料。
   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註冊裝置和一個 Entry 裝置，以啟用 Amazon One 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 主控台。
2. 在導覽窗格中，選擇裝置執行個體。請確定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 登入資料。
   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 登入資料。
   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. 在未啟用的執行個體資料表下，執行個體狀態應該會顯示

   。

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. 從選取網站下拉式清單中，選取網站。
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註冊裝置和一個 Entry 裝置，以啟用 Amazon One 的完整功能，以便安全存取。

安裝和啟用 Amazon One

成功設定 Amazon One 主控台後，後續步驟涉及在您的站點安裝 Amazon One 裝置，並確保裝置已正確啟用。此程序包括將裝置實際放置在指定區域、將其連接到您的網路，以及完成啟用程序，以啟用無縫的使用者識別和交易功能。啟用後，您的 Amazon One 裝置將準備好為您的客戶或員工提供安全、無接觸的體驗。

> **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 裝置可以安裝在任何公司或商業位置，其門可以電氣控制。

控制面板需求

Amazon One 裝置可以做為讀取器連接到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。

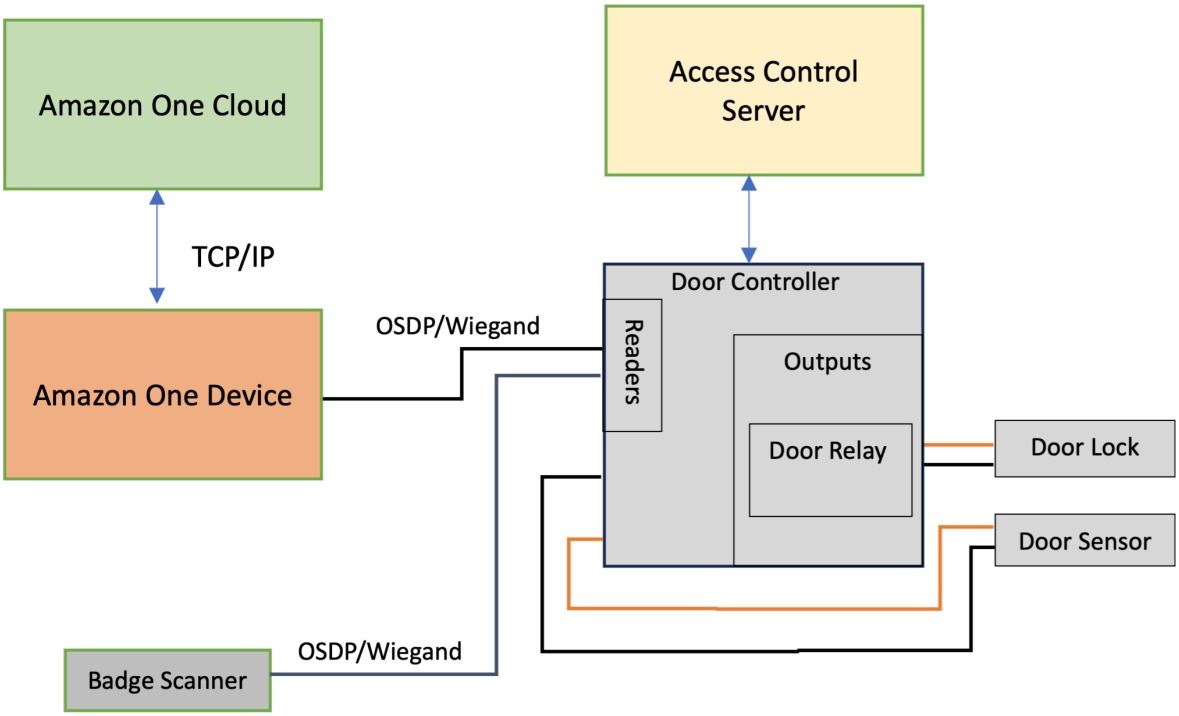
電源需求

Amazon One 裝置可以透過下列兩種方式之一進行供電：

- 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 建議您將裝置安裝為典型存取控制環境的一部分，如以下區塊圖所述。



存取控制環境通常包含下列元件：

- Amazon One 裝置：這是掌上型辨識裝置，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。有權存取該區域的每個人IDs 會存放在此伺服器上。此伺服器會將相關 IDs 快取至適當的門控制器。
- 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 界面，則可以使用 COTS OSDP-to-Wiegand 轉換器。
  - 身分驗證成功後，Amazon One 裝置會將使用者的徽章 ID 傳送至門控制器。
  - 門控制器會回應 決策，然後允許 Amazon One 裝置顯示授予存取或拒絕存取訊息。
- 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，徽章掃描器會連線至 Amazon One 裝置，讓使用者可以掃描其徽章，將他們與其掌上型設定檔建立關聯。

安裝 Amazon One Pedestal

Amazon One Pedestal 是 Amazon One 識別和交易系統的重要元件，旨在為使用者提供無縫、無接觸的體驗。此裝置具有安全的生物識別身分驗證。您可以將其整合到各種位置，以提供無摩擦的存取或付款解決方案。

本節提供安裝 Amazon One Pedestal 的位置需求和step-by-step說明。適當的準備和安裝是確保系統安全且有效率運作的關鍵，為使用者提供順暢、可靠的體驗。

安裝 Amazon One Pedestal 的先決條件和準備

開始安裝之前，請確定符合下列條件，以確保安全、可靠且有效的設定：

- 電源需求：如果您使用 POE+（乙太網路供電）為裝置供電，請確認 Cat6 纜線已安裝，且 POE+ 注入器或交換器可供使用。或者，如果使用 AC 電源 (120V)，請確保可存取的 AC 插座位於台座 20 英呎內。
- 實體設定：地面必須保持水平、乾淨，且無任何碎片，以確保安裝穩定且安全。
- 底座位置：在不會封鎖門、車道或存取點的位置安裝底座，以便輕鬆移動該區域。
- 纜線管理：將所有多餘的纜線路由並固定於底座內，以避免雜亂，並避免在正常使用期間造成任何潛在的損壞。

一旦確認這些先決條件，您就可以繼續安裝程序。

安裝 Amazon One Pedestal

1. 從包裝中移除 Amazon One Pedestal。
2. 轉開兩個 M4 防撥弄螺絲以移除門。
3. 插入電源線。
4. 將纜線穿過底座基底板中的孔。
5. 將底座內任何多餘的電源線進行線圈。
6. 將乙太網路纜線 (Cat5E 或更高版本） 穿過底座的底部板，並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 2 英吋，位於底座底部上方。
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 英呎。
9. 在 RS485 纜線上，於底座底部上方 2 英吋處安裝鐵氧體迴圈。
10. 將插座接上電源，並確認 Amazon One 裝置已開啟。
11. 將門重新連接至底座，並鎖回兩個 M4 防撥弄螺絲以固定。

安裝 Amazon One 裝置後，您就可以啟用裝置。

安裝壁掛式 Amazon One 裝置

壁掛式 Amazon One 裝置是一種多功能、簡潔的生物識別系統，旨在為各種環境中的使用者提供無縫、無接觸的體驗。它使用進階掌上辨識技術進行安全存取或付款，因此非常適合零售空間、辦公室入口等高流量地點。

本節概述安裝壁掛式 Amazon One 裝置的必要位置要求和詳細步驟，以確保最佳效能和安全性。

安裝壁掛式 Amazon One 裝置的先決條件和準備

開始安裝之前，請確定符合下列條件，以確保裝置可有效運作，並在您的空間內正確設定：

- 僅供室內使用：壁掛式 Amazon One 裝置僅供室內使用，因此請確保其安裝在適當的環境中。
- 牆壁要求：牆壁必須保持水平，以確保裝置的適當對齊和功能。
- 掛載高度：安裝後，牆壁掛載的頂端位置不應高於地面 44-46 英吋，以確保使用者易於存取。
- 纜線管理：確保所有多餘的纜線都路由到牆壁掛載後方，並安全地固定以防止損壞或雜亂。

- 乙太網路供電 (PoE++)：如果使用乙太網路供電 (PoE++)，請確認 IEEE 802.3bt （第 3 型） 第 6 類 PoE++ 交換器 （跨度結束） 或注入器 （跨度中） 可用。PoE++ 來源必須列出或經過認證，並符合 IEC 62368-1 標準。重要的是，PoE++ 來源必須位於與裝置相同的建築物內。只能搭配 AOE 裝置使用核准的 PoE++ 來源。
- 15V DC 電源輸入：如果使用 15V DC 電源輸入，請確保僅使用 NEC 第 2 類或電源限制的核准電源供應器。電源必須列出或經過安全與相容性認證。

必要工具

- 如果需要牆錨，則為 1/4 英吋的乾牆或石器鑽頭
- 剝線器
- 7/64 英吋鑽頭，用於鑽探試驗孔
- #2 十字螺絲起子
- 0.5mm x 2mm 一字螺絲起子
- T12 安全 Torx 驅動程式
- 鉛筆
- Level

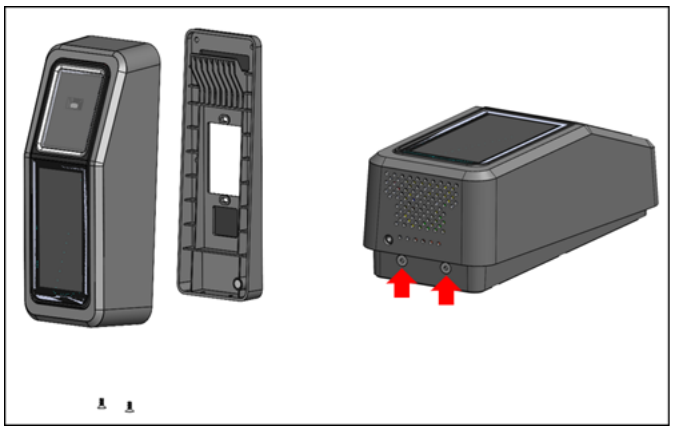
隨附於壁掛式 Amazon One 裝置

- 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 位置接線板連接器
- 2 個 Torx Security M4x10 平頭螺絲

確認這些先決條件後，您可以繼續安裝步驟，以安全地掛載和設定壁掛式 Amazon One 裝置。

安裝 Amazon One 裝置的牆掛式面板

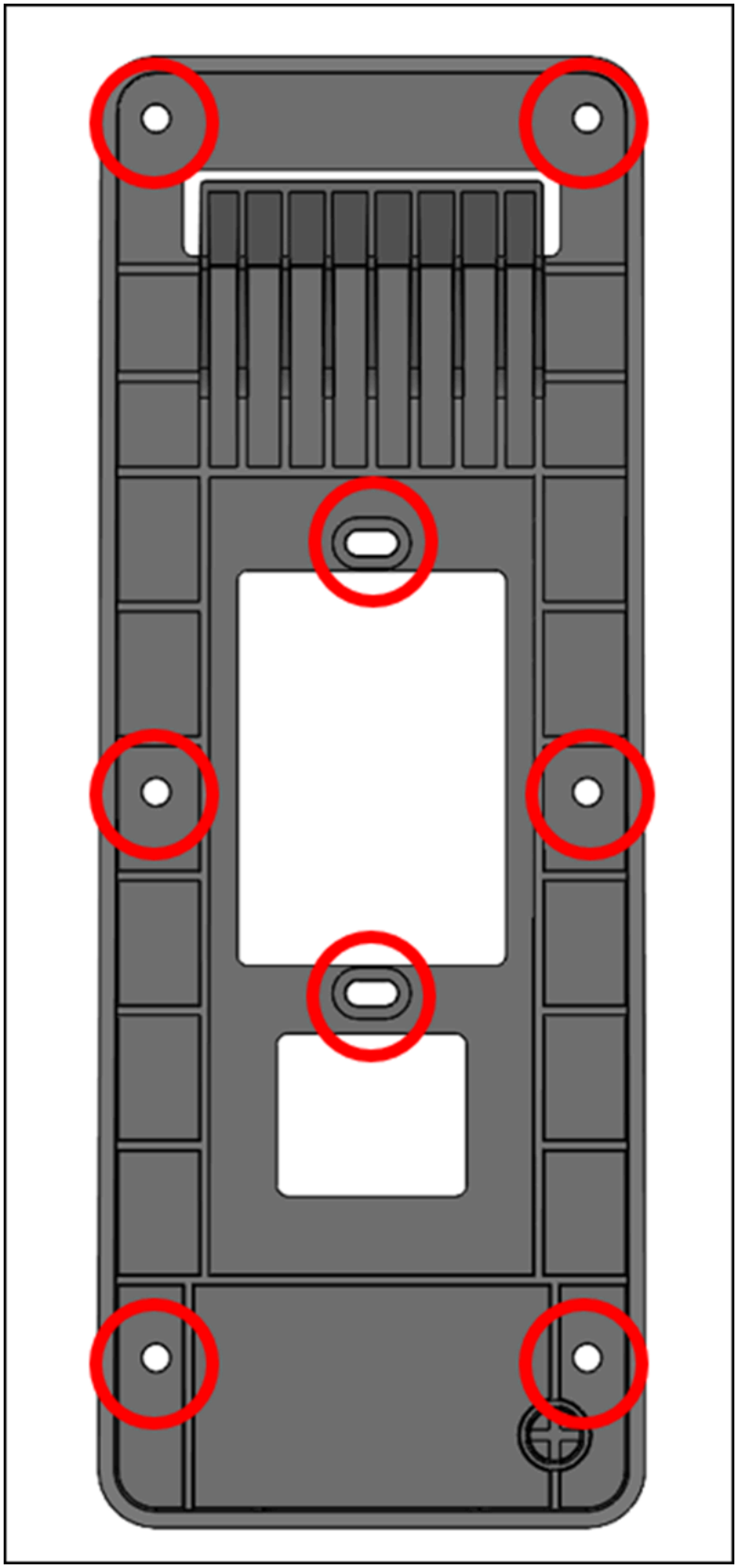
1. 從包裝中移除您的 Amazon One 裝置。
2. 移除兩個底部 Torx 安全螺絲，將掛載板與 Amazon One 裝置分開。



3. 將掛載板放在牆上所需的位置。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：

   - 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。
   - 確定掛載板是水平的。
   - 使用掛載板作為範本，使用鉛筆標記六個螺絲位置。您可以使用長形孔和 #6-32 螺絲作為掛載板的額外支援。請勿使用 #6-32 螺絲位置做為掛載牆板的主要方式。



4. 如果掛載到結構、乾牆、磚塊或混凝土表面，請在每個標記的位置鑽 1/4 英吋的孔，然後將它們壓進孔中，直到錨點與牆壁齊平。

   如果掛載到木面上，則不需要錨點，而且在標記的位置中只需要 7/64 英吋的試驗孔。

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. 所有緊固件都就位後，請確定掛載板是水平的。
7. 旋緊螺絲，將掛載板固定到牆上。

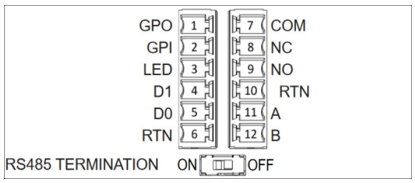
連接您的壁掛式 Amazon One 裝置

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 裝置使用終端機區塊連接器 (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 佈線說明。

   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	資料輸入訊號 – 選用
3	LED	Wiegand LED	Wiegand LED – 選用
4	D1	Wiegand D1	Wiegand 資料 1 – 白線

Pin	連線	描述	使用	
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	聯絡中繼常閉 – 橘色線	
9	NO	轉送常開	聯絡中繼正常開啟 – 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	

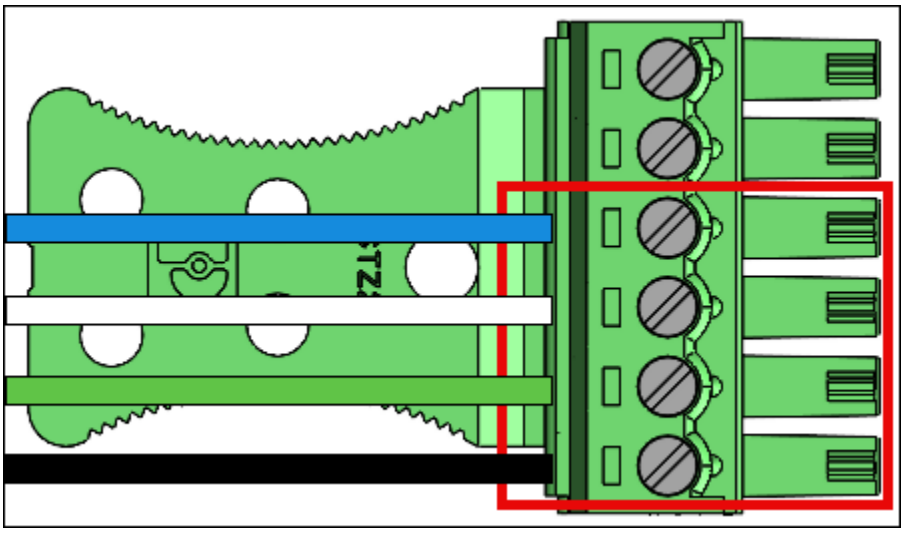
2. 安裝電線時，請將電線末端的 3mm-5mm 剝除。
3. 將剝除的線端插入所需的終端位置。
4. 使用一字螺絲起子，順時針旋轉終端機保留螺絲以夾緊線路，直到緊固為止。請勿過度收緊。
5. 扣上後，輕拉電線，以確保其就位。
6. 進行必要的連線後，請將 插頭插入 Amazon One 裝置終端機區塊的對應插座。
7. 將 Cat6 乙太網路纜線插入 RJ45 插孔。
8. 放置 Amazon One 裝置，讓牆板上的掛鉤滑入裝置背面的開口。
9. 確保纜線不會卡在裝置與掛載板之間，並讓裝置旋轉並就定位。
10. 使用兩個 Torx Security M4x10 平頭螺絲，將 Amazon One 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線路。

Wiegand 連線

- 將藍色線插入接腳 3 (LED)。
- 將白線插入接腳 4 (D1)。
- 將綠色線插入接腳 5 (D0)。
- 將黑色線插入接腳 6 (RTN)。



Wiegand 輸出配線

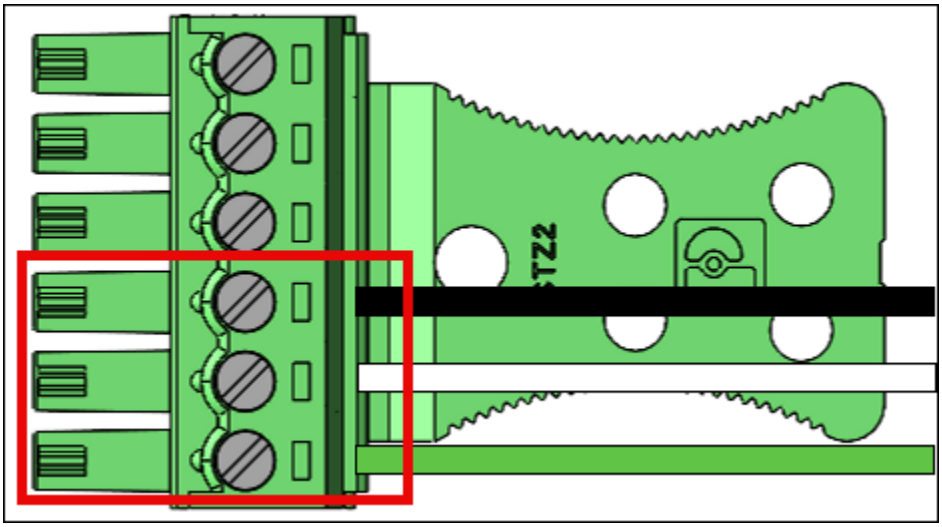
Pin	連線	描述	使用	
3	LED	Wiegand LED	Wiegand LED 輸入 – 選用 (5V TTL)	
4	D1	Wiegand D1	Wiegand D1 輸出 (5V TTL)	
5	D0	Wiegand D0	Wiegand D0 輸出 (5V TTL)	

Pin	連線	描述	使用	
6	RTN	訊號傳回	Wiegand GND 參考	

如果裝置是行上的最後一個單位，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

- 將黑色線插入接腳 10 (RTN)。
- 將白線插入接腳 11 (A)。
- 將綠色線插入接腳 12 (B)。



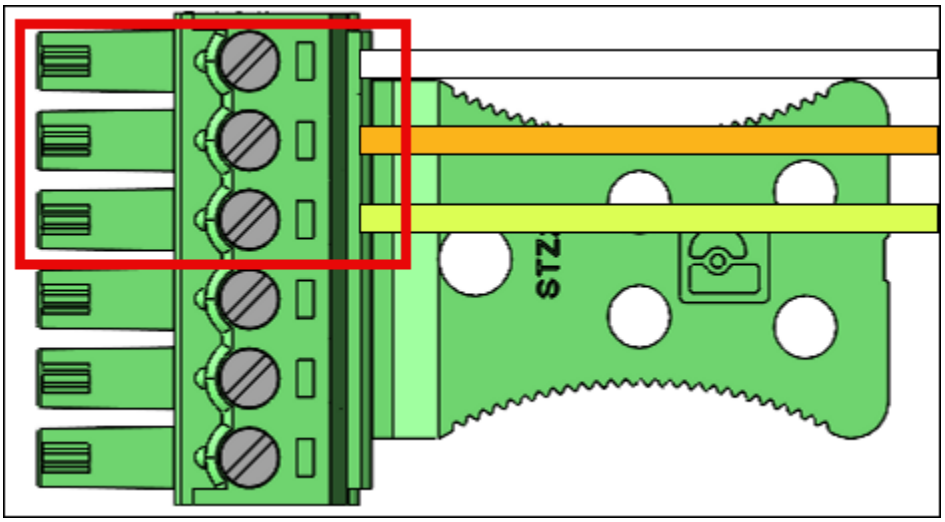
RS485 配線

Pin	連線	描述	使用	
10	RTN	訊號傳回	地面	
11	A	RS485_A/D1/ Clock	RS485 非反轉訊號	

Pin	連線	描述	使用	
12	B	RS485_B/D0/資料	RS485 反轉訊號	

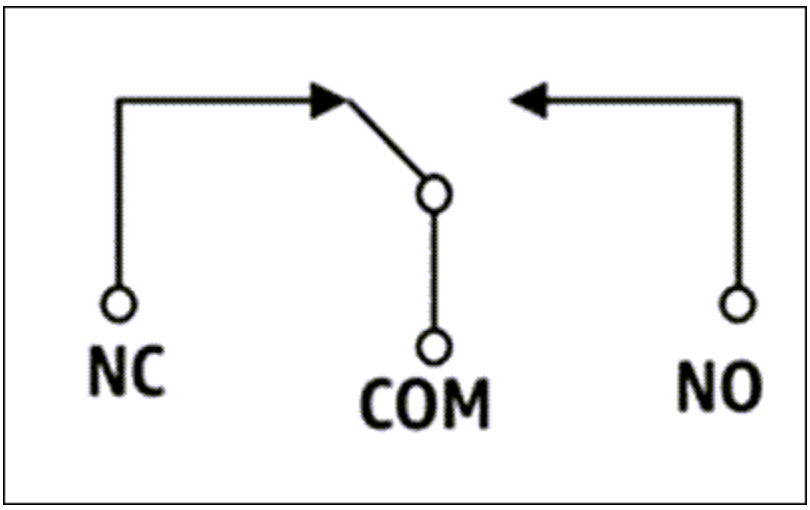
轉送連線

- 將白線插入接腳 7 (COM)。
- 將橘色線插入接腳 8 (NC)。
- 將黃色線插入接腳 9 (NO)。



轉送器佈線

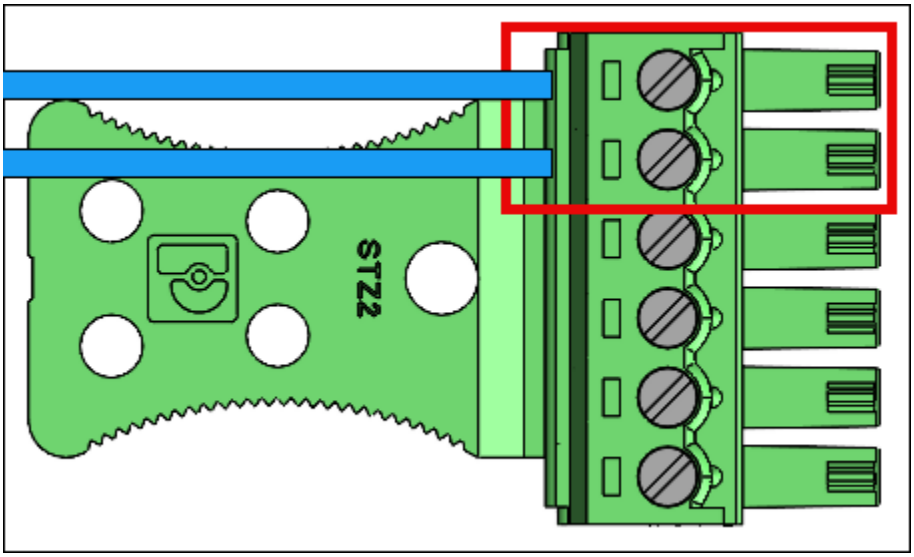
Pin	連線	描述	使用	
7	COM	轉送通用	聯絡中繼通用 – 白線	
8	NC	轉送常閉	聯絡中繼常閉 – 橘色線	
9	NO	轉送常開	聯絡中繼正常開啟 – 黃線	



轉送器應依照指定的安全等級 30VAC/60VDC、最大 60W 操作。

數字輸入/輸出連線

- 將藍色線插入接腳 1 (GPO)。
- 將藍色線插入接腳 2 (GPI)。



輸入/輸出配線

Pin	連線	描述	使用	
1	GPO	一般用途輸出	數位輸出訊號 (5V)	

Pin	連線	描述	使用	
2	GPI	一般用途輸入	資料輸入訊號 (3.6V – 5V)	

- 輸入/輸出連線應如所列操作。

安裝 Amazon One 裝置後，您就可以啟用裝置。

安裝 Amazon One 裝置 I/O Hub 以安全存取

具有 I/O Hub 的 Amazon One 裝置是 Amazon One Enterprise 系統不可或缺的一部分，旨在增強安全性並簡化各種環境的存取控制。裝置利用生物指標掌上辨識功能，為使用者提供安全、無接觸的身分驗證，使其非常適合用於高安全區域，例如辦公大樓、受限入口點或需要無縫存取管理的設施。I/O Hub 可做為裝置與現有安全基礎設施之間的橋樑，啟用與門鎖、警示和其他存取控制系統的通訊。

本節提供使用 I/O Hub 安裝 Amazon One 裝置的位置需求和step-by-step說明。適當的準備和安裝是確保系統安全且有效率運作的關鍵，為使用者提供順暢、可靠的體驗。

安裝 Amazon One Device with I/O Hub 的先決條件和準備

開始安裝之前，請確定符合下列條件，以確保安全、可靠且有效的設定：

- 僅限室內使用：Amazon One 裝置搭配 I/O Hub 僅供室內使用。確保它安裝在適當的環境中。
- 乙太網路供電 (PoE++)：如果使用乙太網路供電 (PoE++)，請確認 IEEE 802.3bt （第 3 型） 第 6 類 PoE++ 交換器 （跨度結束） 或注入器 （跨度中） 可用。PoE++ 來源必須列出或經過認證，並符合 IEC 62368-1 標準。重要的是，PoE++ 來源必須位於與裝置相同的建築物內。只能搭配 AOE 裝置使用核准的 PoE++ 來源。

- 15V DC 電源輸入：如果您使用的是 15V DC 電源輸入，請確保僅使用 NEC 第 2 類或電源限制的核准電源供應器。電源必須列出或經過安全認證。如需更多詳細資訊，請參閱下方的選用 DC 區段。

必要工具

- 剝線器
- #2 十字螺絲起子

- 0.5mm x 2mm 一字螺絲起子

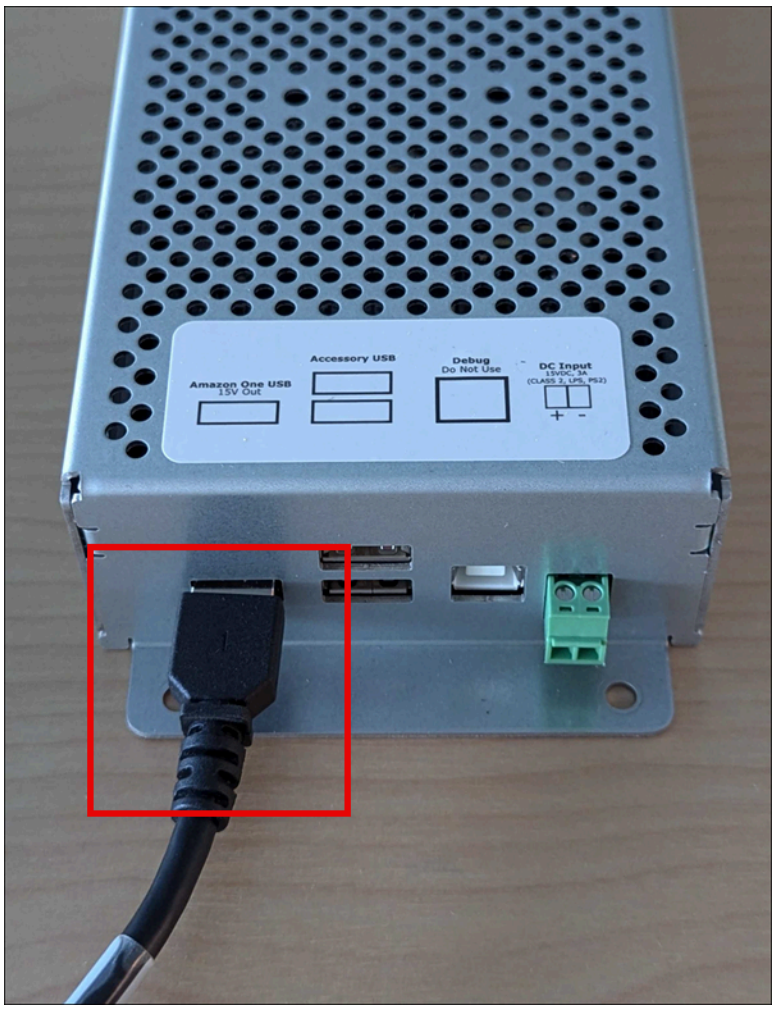
隨附於具有 I/O Hub 的 Amazon One 裝置

- 2x 6 位置終端機區塊連接器
- DC 插頭連接器
- 72" 電源/資料纜線

一旦確認這些先決條件，您就可以繼續進行安裝程序，確保使用 I/O Hub 安全且有效率地設定 Amazon One 裝置。適當的準備將有助於保證裝置功能如預期般運作，並順暢地整合到您的安全存取系統。

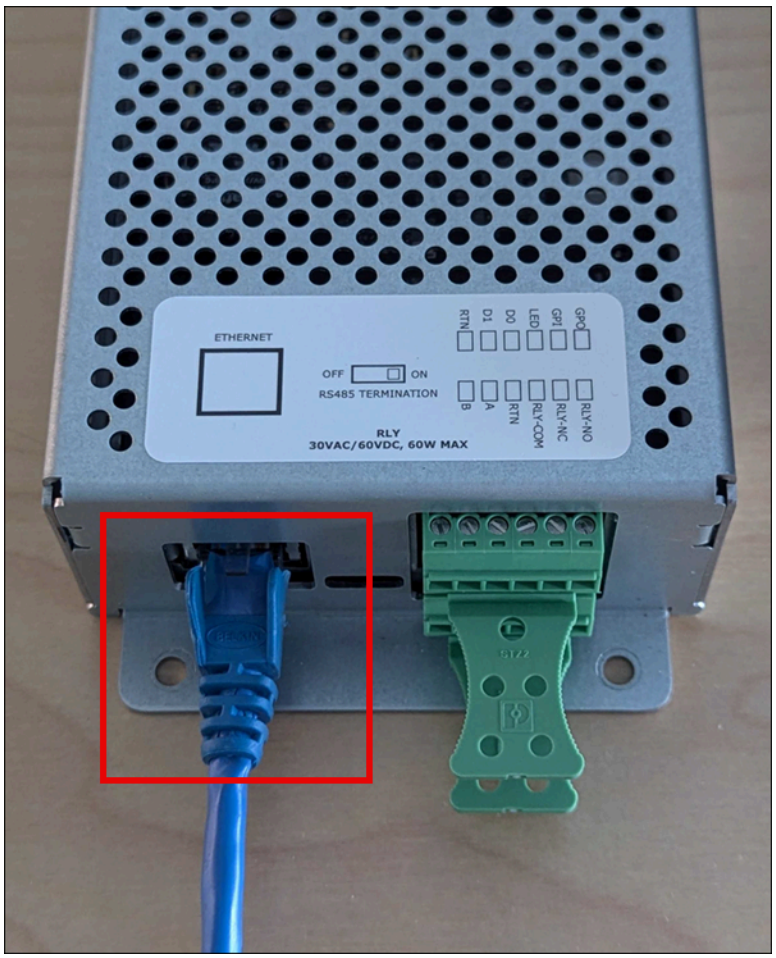
安裝 Amazon One 裝置的 I/O 中樞

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。



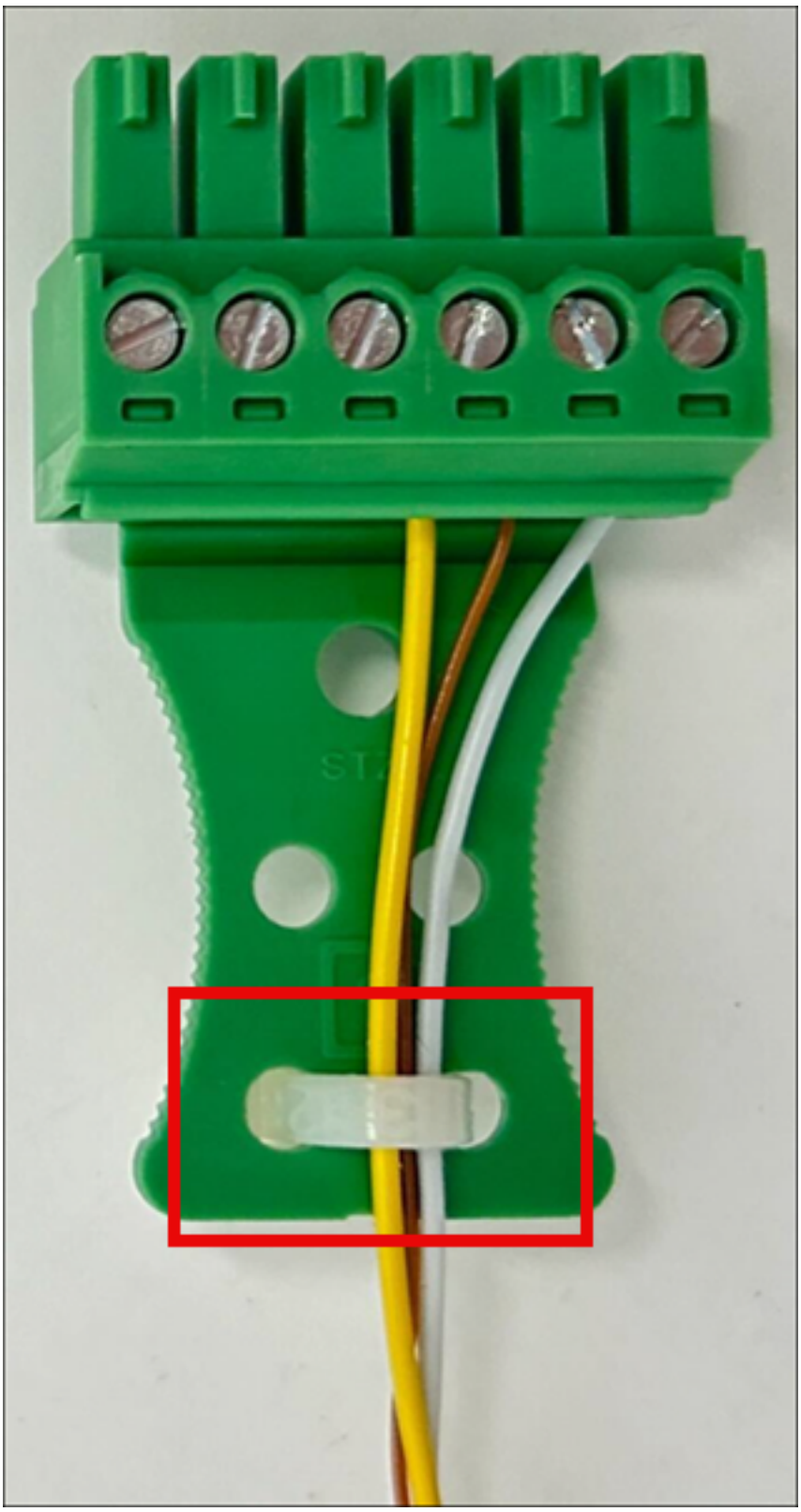
4. 對於 POE++ 電源，將乙太網路纜線從 POE++ 來源插入 I/O 集線器連接埠。

   選用：如需 DC 電源，請參閱下面的安裝 DC 配線一節。



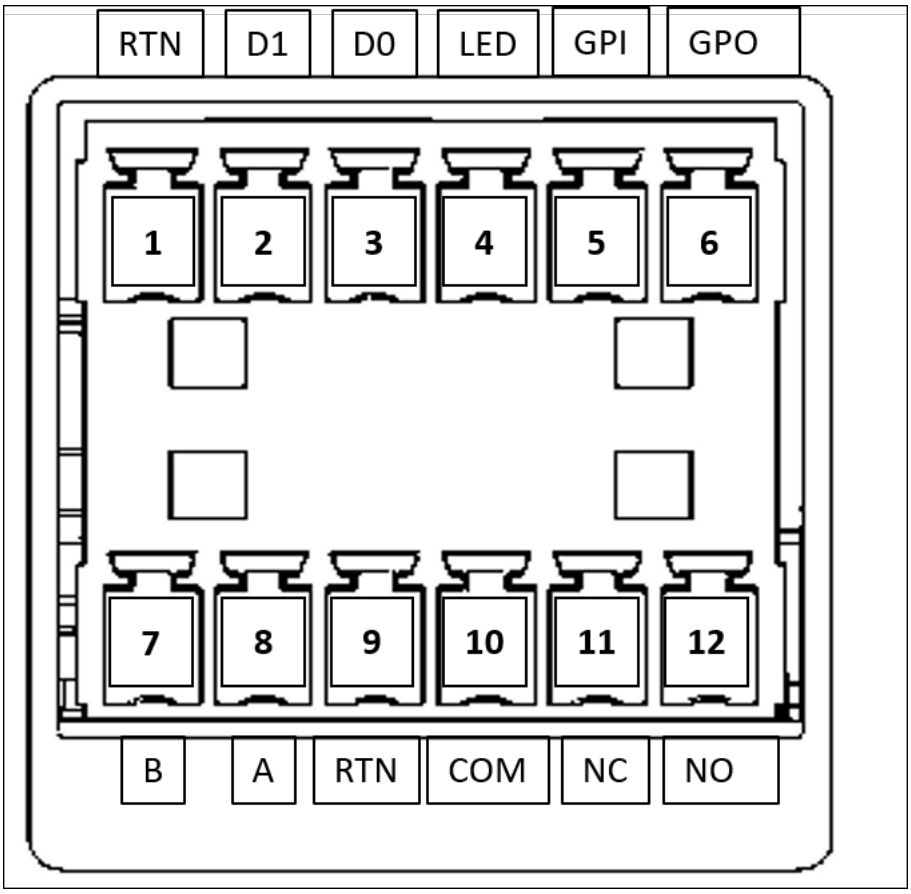
為您的 Amazon One 裝置連接 I/O 集線器

- 安裝滴水迴路，以避免液體意外地向下向下執行並進入 I/O 集線器。
- 連接應變釋放夾，以保護線路免於損壞或壓力，如下圖所示。



1. 將終端機區塊插頭插入 I/O 集線器。
2. 僅透過終端機區塊插頭插入應用程式所需的線路。請參閱下列接線表和圖表。

連線

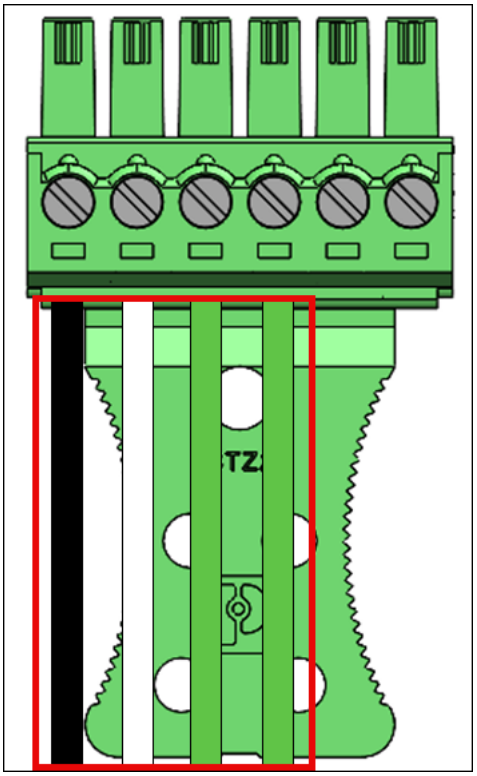


Pin	連線	描述	使用	
1	RTN	訊號傳回	Wiegand 接地 – 黑色線	
2	D1	Wiegand D1	Wiegand 資料 1 – 白線	
3	D0	Wiegand D0	Wiegand 資料 0 – 綠線	
4	LED	Wiegand LED	Wiegand LED – 選用	
5	GPI	一般用途輸入	資料輸入訊號 – 選用	

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	中繼通用	聯絡中繼通用 – 白線	
11	NC	轉送常閉	聯絡中繼常閉 – 橘色線	
12	NO	轉送常開	聯絡中繼正常開啟 – 黃線	

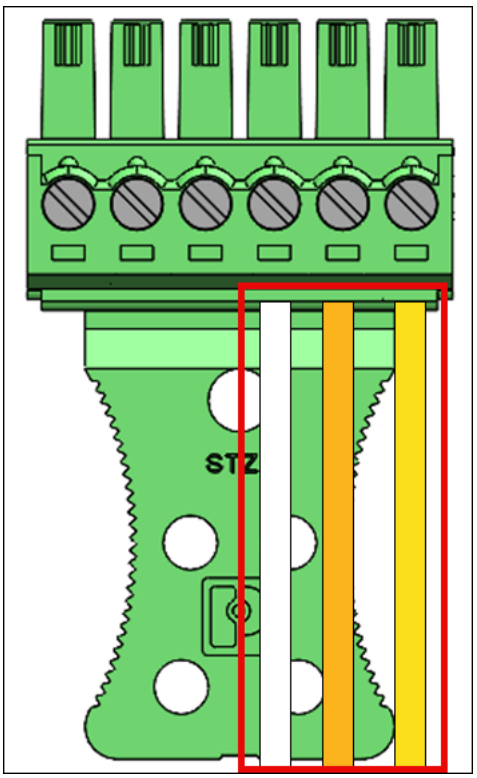
Wiegand 連線

- 將黑色線插入接腳 1 (RTN)。
- 將白線插入接腳 2 (D1)。
- 將綠色線插入接腳 3 (D0)。
- 選用：將綠色線插入接腳 4 (LED)。

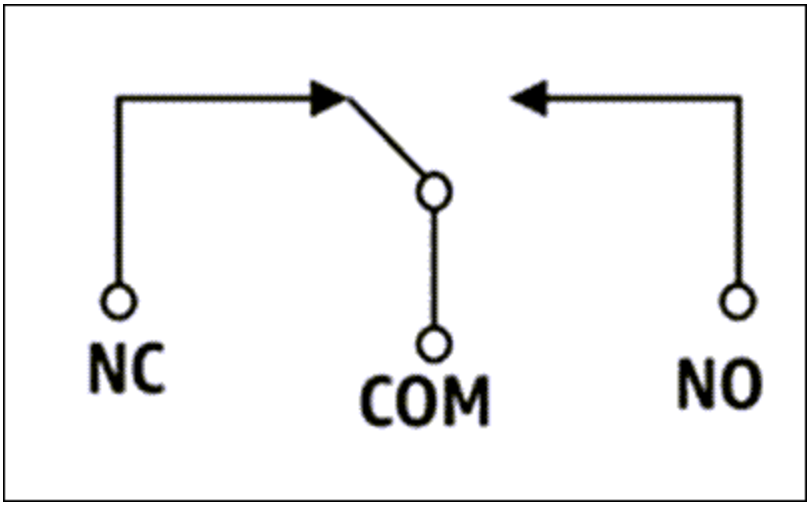


轉送連線

- 將白線插入接腳 10 (COM)。
- 將橘色線插入接腳 11 (NC)。
- 將黃色線插入接腳 12 (NO)。



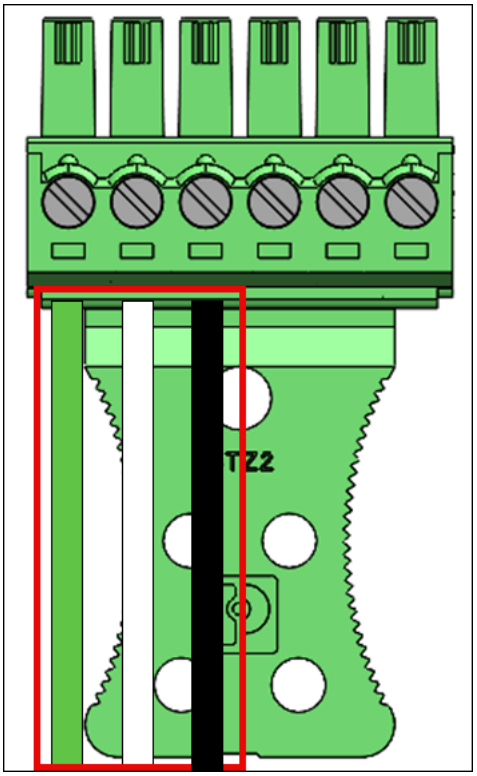
轉送圖



轉送器應該根據指定的安全等級 30VAC/60VDC、最大 60W。

RS485 連線

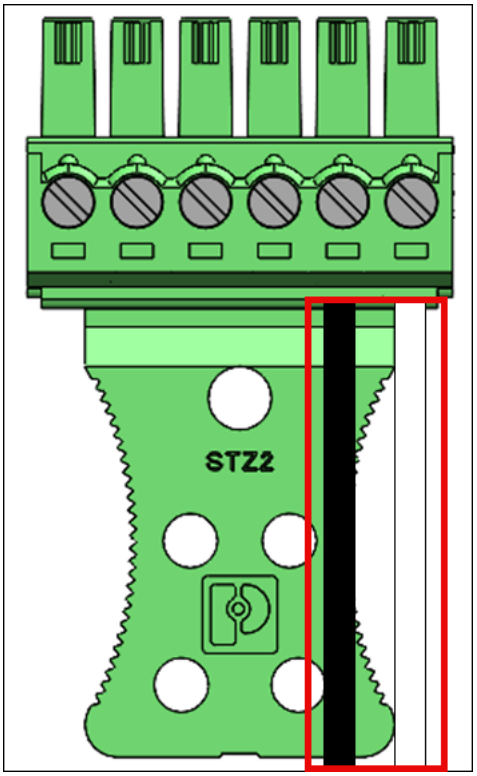
- 將綠色線插入接腳 7 (B)。
- 將白線插入接腳 8 (A)。
- 將黑色線插入接腳 9 (RTN)。



如果裝置是行上的最後一個單位，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。

數字輸入/輸出連線

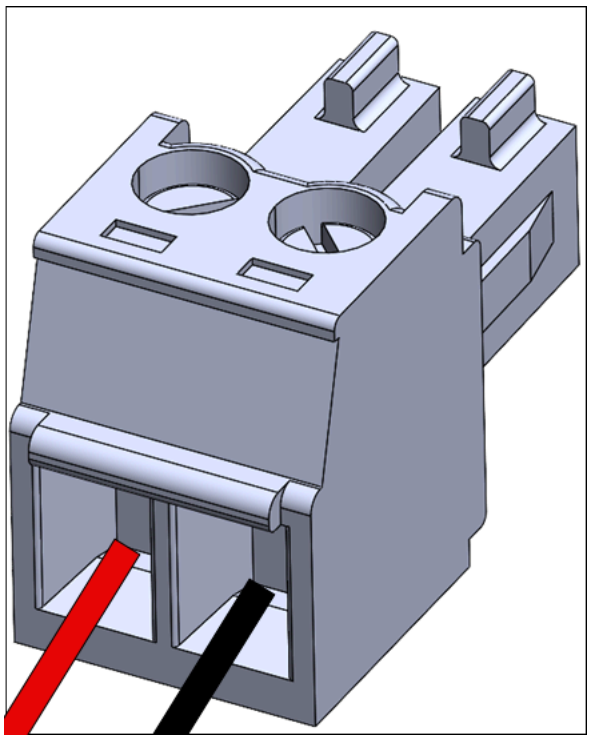
- 將黑色線插入接腳 5 (GPI)。
- 將白線插入接腳 6 (GPO)。



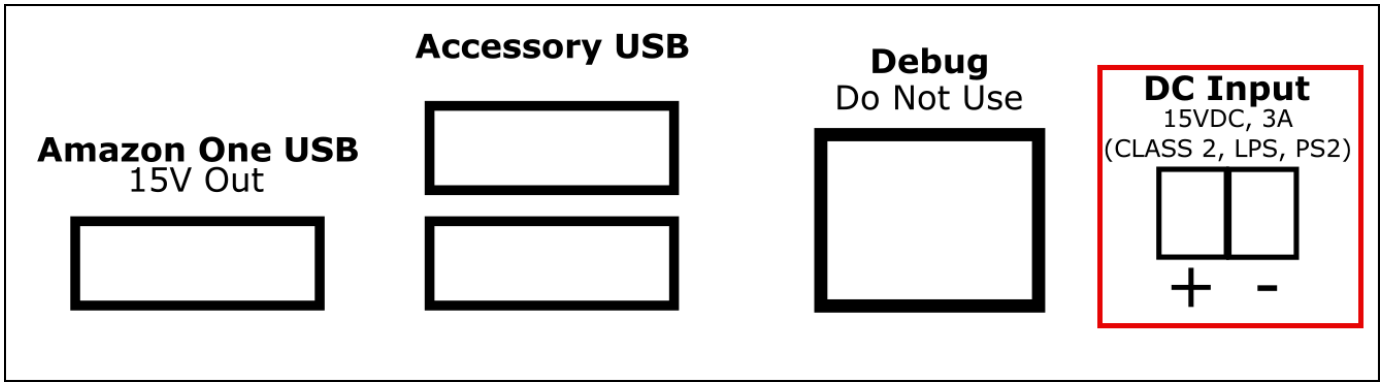
- 輸入/輸出連線應按所列方式操作。

選用：安裝 DC 配線

1. 從紅色線的結尾將 3mm-5mm 的正極 (+) 和黑色線的負極 (-) 剝除。
2. 將 DC 線的分割端插入 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。



安裝 Amazon One 裝置後，您就可以啟用裝置。

啟用 Amazon One 裝置

當您的 Amazon One 裝置安裝並開啟電源時，您就可以啟用它。

啟用您的 Amazon One 裝置

1. 在 Amazon One 裝置上，點選螢幕以開始使用。

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：//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 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！，表示裝置已準備就緒可供使用。

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他們的掌心，並驗證其掌心以取得存取權。

主題

建立端點政策

使用者必須先完成註冊程序，才能驗證他們的掌心才能進入。安全人員在允許使用者註冊之前，應一律檢查使用者的身分。

在 Amazon One 裝置上註冊您的掌心

1. 在 Amazon One Enterprise 註冊裝置上，按下開始使用。
2. 使用連線到您 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，然後按確定。
4. 閱讀同意 - 您的 Palm Biometric 資訊，如果您同意，請按我同意。
5. 依照畫面上的指示完成註冊程序。

驗證項目

成功註冊掌心後，您就可以在 Amazon One Enterprise 進入裝置上使用掌心進行身分驗證。

驗證您的掌上裝置以進入 Amazon One 裝置

- 將掌心懸停在裝置上方，並依照螢幕上的指示掃描掌心。

管理使用者

您可以使用已註冊使用者管理頁面來追蹤已註冊的使用者，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，選擇已註冊的使用者管理。
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，RFID 徽章讀取器擷取的徽章識別符資訊。
   - 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。

刪除已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已註冊的使用者及其生物識別特徵。

刪除已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. 選擇刪除生物辨識。
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

維護和清理 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。

清理 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，以及任何周邊和配套裝置（如適用）已連接。
- 如果網路連線無法使用（如果發生這種情況，Amazon One 裝置會顯示錯誤畫面），則向管理員呈報問題；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，包括裝置的可見螺絲和外殼，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，請遵循 Amazon One 裝置畫面上的指示，或參閱故障診斷指南來修復問題。

清除 Amazon One 裝置

清理您的 Amazon One 裝置會定期移除任何污點或標記，例如指紋和手印。

> **Note**
>
> 請勿使用本指南所列以外的任何其他清潔產品。建議的清理排程是每週一次或兩次，或每當裝置上出現灰塵、污點時，但每天不得超過一次。

1. 使用異丙酒精 (IPA) 抹布來抹除 Amazon One 裝置。僅清理裝置的觸控表面。除非 Amazon One 指示，否則請勿觸碰光學視窗，或使用任何其他清潔產品。
2. 使用乾的超細纖維布料擦除任何條紋。
3. 稍微清除（請勿抹除）光學視窗中的任何可見污物或碎片。將光學窗口的清理限制為每天不超過一次和/或當窗口看起來骯髒時（例如手指/手印/污點）。裝置的此部分並非旨在接觸，但新客戶可能會無意接觸。
4. 如果適用，請使用 KIC Smart Card 清理程式來清理讀卡器內部。
5. 每週清潔裝置一到兩次，或每當裝置上看到灰塵、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。

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，選擇網站。
3. 在網站下，選取您要編輯名稱的網站。
4. 選擇編輯。
5. 在網站資訊下，輸入所需的網站名稱和網站描述（選用）。
6. 選擇儲存變更以更新。

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，選擇網站。
3. 在網站下，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量為 0。
5. （選用）如果啟用的執行個體數量不是 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。

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，選擇您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。

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. 在已啟用的執行個體下，選擇您要更新之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. 在您進行所需的變更之後，請選擇更新裝置組態以確認更新。

更新 Wi-fi 登入資料

下列程序詳細說明如何更新 Wi-Fi 登入資料。

更新 Wifi 登入資料

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，選擇您要更新的裝置執行個體名稱。
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。

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

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構是為了滿足最安全敏感組織的需求而建置。

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 也為您提供可安全使用的服務。第三方稽核人員會定期測試和驗證我們安全的有效性，做為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AWS 合規計劃範圍內的服務。
- 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其他 AWS 服務來協助您監控和保護 Amazon One Enterprise 資源。

主題

- Amazon One Enterprise 中的資料保護
- 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 One Enterprise 的合規驗證

Amazon One Enterprise 中的資料保護

AWS 共同責任模型適用於 Amazon One Enterprise 中的資料保護。如此模型所述， 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，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 設定個別使用者。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：

- 每個帳戶均要使用多重要素驗證 (MFA)。

- 使用 SSL/TLS 與 AWS 資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄 AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 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 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，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 使用 主控台、API AWS CLI或 AWS SDKs時。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。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

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 預設會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，或稽核其使用方式。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 擁有的金鑰。

加密傳輸中的資料

Amazon One Enterprise 使用 Transport Layer Security (TLS) 來保護資料，並使用 Signature 第 4 版來驗證對 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進行身分驗證 （ 登入 ） 和授權 （ 具有許可 ） 來使用 Amazon One Enterprise 資源。IAM 是 AWS 服務 您可以免費使用的 。

主題

目標對象

使用方式 AWS Identity and Access Management (IAM) 會有所不同，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 服務來執行您的任務，您的管理員會為您提供所需的登入資料和許可。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 身分和存取進行故障診斷。

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。您的任務是判斷服務使用者應存取哪些 Amazon One Enterprise 功能和資源。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司如何搭配 Amazon One Enterprise 使用 IAM，請參閱 Amazon One Enterprise 如何與 IAM 搭配使用。

IAM 管理員 – 如果您是 IAM 管理員，建議您了解撰寫政策以管理 Amazon One Enterprise 存取的詳細資訊。若要檢視您可以在 IAM 中使用的 Amazon One Enterprise 身分型政策範例，請參閱 Amazon One Enterprise 的身分型政策範例。

使用身分驗證

身分驗證是您 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 角色身分進行身分驗證 （ 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 身分身分身分登入 。 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 登入資料，都是聯合身分的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使用聯合 AWS 身分存取 時，您會間接擔任角色。

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

如果您以 AWS 程式設計方式存取 ， AWS 會提供軟體開發套件 (SDK) 和命令列界面 (CLI)，以使用您的登入資料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。如需使用建議的方法自行簽署請求的詳細資訊，請參閱《IAM 使用者指南》中的適用於 API 請求的AWS Signature 第 4 版。

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驗證 (MFA) 來提高帳戶的安全性。如需更多資訊，請參閱《AWS IAM Identity Center 使用者指南》中的多重要素驗證和《IAM 使用者指南》中的 IAM 中的AWS 多重要素驗證。

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，該身分可完整存取 帳戶中的所有 AWS 服務 和資源。此身分稱為 AWS 帳戶 Theroot 使用者，可透過使用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。如需這些任務的完整清單，了解需以根使用者登入的任務，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

最佳實務是， 要求人類使用者，包括需要管理員存取權的使用者，使用臨時登入資料 AWS 服務 與身分提供者聯合來存取 。

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 AWS 服務 是透過身分來源提供的登入資料存取的任何使用者。當聯合身分存取時 AWS 帳戶，它們會擔任 角色，而角色會提供臨時登入資料。

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，或者您可以連接並同步到您自己的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 的詳細資訊，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。建議您盡可能依賴臨時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是一種指定 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，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 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，但角色僅提供臨時憑證。如需更多資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色是 中具有特定許可 AWS 帳戶 的身分。它類似 IAM 使用者，但不與特定的人員相關聯。若要在 中暫時擔任 IAM 角色 AWS Management Console，您可以從使用者切換至 IAM 角色（主控台）。您可以透過呼叫 AWS CLI 或 AWS API 操作或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

使用臨時憑證的 IAM 角色在下列情況中非常有用：

- 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。如需有關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 (聯合) 建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。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。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。不過，對於某些 AWS 服務，您可以直接將政策連接到資源（而不是使用角色做為代理）。如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。
- 跨服務存取 – 有些 AWS 服務 使用其他 中的功能 AWS 服務。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。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 AWS 服務 請求向下游服務提出請求。只有當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，才會提出 FAS 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 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。

  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可權給 AWS 服務。
  - 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。
- 在 Amazon EC2 上執行的應用程式 – 您可以使用 IAM 角色來管理在 EC2 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS CLI 或 AWS API 請求。這是在 EC2 執行個體內儲存存取金鑰的較好方式。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描述檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得臨時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色來授予許可權給 Amazon EC2 執行個體上執行的應用程式。

使用政策管理存取權

您可以透過建立政策並將其連接至身分或資源 AWS 來控制 AWS 中的存取。政策是 中的物件， AWS 當與身分或資源相關聯時， 會定義其許可。當委託人（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。大多數政策會以 JSON 文件 AWS 的形式存放在 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。若要授予使用者對其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，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。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 API AWS 取得角色資訊。

身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。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。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

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。如需了解如何在受管政策及內嵌政策之間選擇，請參閱《IAM 使用者指南》中的在受管政策和內嵌政策間選擇。

資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 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。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 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中使用來自 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

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

Amazon S3 AWS WAF和 Amazon VPC 是支援 ACLs的服務範例。如需進一步了解 ACL，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 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 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 JSON 政策，可指定 中組織或組織單位 (OU) 的最大許可 AWS Organizations。 AWS Organizations 是一種用於分組和集中管理您企業擁有 AWS 帳戶 的多個的服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 會限制成員帳戶中實體的許可，包括每個實體 AWS 帳戶根使用者。如需 Organizations 和 SCP 的詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。
- 資源控制政策 (RCP) - RCP 是 JSON 政策，可用來設定您帳戶中資源的可用許可上限，採取這種方式就不需要更新附加至您所擁有的每個資源的 IAM 政策。RCP 會限制成員帳戶中資源的

許可，並可能影響身分的有效許可，包括 AWS 帳戶根使用者，無論它們是否屬於您的組織。如需 Organizations 和 RCPs的詳細資訊，包括支援 RCPs AWS 服務 的 清單，請參閱AWS Organizations 《 使用者指南》中的資源控制政策 RCPs)。

- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過撰寫程式的方式建立角色或聯合使用者的暫時工作階段時，做為參數傳遞。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 IAM 搭配使用

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。

您可以搭配 Amazon One Enterprise 使用的 IAM 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
ACL	否
ABAC (政策中的標籤)	是
暫時性憑證	是
主體許可	是

IAM 功能	Amazon One Enterprise 支援
服務角色	否
服務連結角色	否

若要深入了解 Amazon One Enterprise 和其他 AWS 服務如何與大多數 IAM 功能搭配使用，請參閱《IAM 使用者指南》中的AWS 與 IAM 搭配使用的 服務。

Amazon One Enterprise 的身分型政策

支援身分型政策：是

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。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。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。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。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 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 內的資源型政策

支援資源型政策：否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 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。委託人可以包括帳戶、使用者、角色、聯合身分使用者或 AWS 服務。

如需啟用跨帳戶存取權，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，做為資源型政策的主體。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位置時 AWS 帳戶，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 IAM 中的快帳戶資源存取。

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，哪個主體在什麼条件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述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，例如沒有相符的 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 動作的清單，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 政策元素可指定要套用動作的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。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 ARNs 的清單，並了解您可以使用哪些動作來指定每個資源的 ARN，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，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定的條件金鑰。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，以及了解您可以使用條件索引鍵的動作和資源，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。

Amazon One Enterprise 中的 ACLs

支援 ACL：否

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

Amazon One Enterprise 的 ABAC

支援 ABAC (政策中的標籤)：是

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。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。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

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 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的使用 ABAC 授權定義許可。如要查看含有設定 ABAC 步驟的教學課程，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，包括哪些 AWS 服務 使用臨時登入資料，請參閱《AWS 服務 IAM 使用者指南》中的使用 IAM 的 。

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 ，則會使用臨時登入資料。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登入資料。

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》中的從使用者切換至 IAM 角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議使用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 IAM 中的暫時性安全憑證。

Amazon One Enterprise 的跨服務主體許可

支援轉寄存取工作階段 (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 AWS 服務 請求向下游服務提出請求。只有當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，才會提出 FAS 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 請求時的政策詳細資訊，請參閱轉發存取工作階段。

Amazon One Enterprise 的服務角色

支援服務角色：否

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可權給 AWS 服務。

> **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，請參閱可搭配 IAM 運作的AWS 服務。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 AWS API 來執行任務。若要授予使用者對其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，使用者便能擔任這些角色。

如需了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策 (主控台)。

如需 Amazon One Enterprise 定義的動作和資源類型的詳細資訊，包括每種資源類型的 ARNs 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

以身分為基礎的政策會判斷是否有人可以在您的帳戶中建立、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。我們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。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅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 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。

- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 使用服務動作，您也可以使用條件來授予存取服務動作的權限 AWS 服務，例如 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可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》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA)：如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以增加安全性。如需在呼叫 API 操作時請求 MFA，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》https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_configure-api-require.html中的透過 MFA 的安全 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

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 AWS API 進行呼叫的使用者，您不需要允許最低主控台許可。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

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》中的新增許可到使用者。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此政策包含在 主控台上完成此動作的許可，或使用 AWS CLI 或 AWS API 以程式設計方式完成此動作的許可。

```
{
    "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。對於控制對 Amazon One Enterprise 動作之存取的政策， Resource元素一律設定為 *，也就是「所有資源」的萬用字元。

Action 元素中的值對應至服務所支援的 API。動作前面有 ，config:表示它們參考 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UpdateDeviceInstance，例如 CreateDeviceInstance、和 DeleteDeviceInstance。使用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 動作支援的資源層級許可

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。另說明每個動作支援的資源及其 ARN。指定 ARN 時，您可在路徑中使用 * 萬用字元，例如當您無法或不想明確指定資源 ID 時。

> **Important**
>
> 如果此資料表中未列出 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

API 動作	資源
	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 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* /configuration/*version*
GetDeviceInstanceConfiguration	裝置執行個體組態 arn：aws：one：*region#accountID* ：device-instance/*deviceInstanceId* /configuration/*version*

API 動作	資源
CreateSite	Site arn：aws：one：*region#accountID* ：site/*siteId*
DeleteSite	Site arn：aws：one：*region#accountID* ：site/*siteId*
GetSiteAddress	Site arn：aws：one：*region#accountID* ：site/*siteId*
UpdateSite	Site arn：aws：one：*region#accountID* ：site/*siteId*
UpdateSiteAddress	Site arn：aws：one：*region#accountID* ：site/*siteId*
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，您會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和拒絕寫入存取，以對 Amazon One Enterprise 規則 API 動作執行特定動作。

其他資訊

若要進一步了解如何建立 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 One Enterprise 的 受管政策

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策旨在為許多常見使用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住， AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 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 AWS 受管政策中定義的許可。如果 AWS 更新 受管政策中 AWS 定義的許可，則更新會影響政策連接的所有主體身分（使用者、群組和角色）。當新的 AWS 服務 啟動或新的 API 操作可用於現有 服務時， AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AmazonOneEnterpriseFullAccess

此政策會授予管理許可，以允許存取所有 Amazon One Enterprise 資源和操作。

one:* 可讓您執行所有 Amazon One Enterprise 動作。

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

```
    "Resource": "*"
   }
  ]
}
```

AmazonOneEnterpriseReadOnlyAccess

此政策會授予所有 Amazon One Enterprise 資源和操作的唯讀許可。

one:Get* 取得 Amazon One Enterprise 資源。

one:List* 列出 Amazon One Enterprise 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許可，可讓您為任何已設定的裝置執行個體建立啟用 QR 碼，以在任何站點啟用裝置。

one:CreateDeviceActivationQrCode 可讓您建立 QR 碼以啟用裝置。

one:GetDeviceInstance 可讓您擷取 Amazon One 裝置執行個體的相關資訊。

one:GetSite 可讓您擷取 Amazon One Enterprise 網站的相關資訊。

one:GetSiteAddress 可讓您擷取 Amazon One Enterprise 網站的實體地址。

one:ListDeviceInstances 可讓您列出 Amazon One 裝置執行個體。

one:ListSites 可讓您列出 Amazon One Enterprise 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": "*"
  }
 ]
}
```

受 AWS 管政策的 Amazon One Enterprise 更新

檢視自此服務開始追蹤這些變更以來，Amazon One Enterprise AWS 受管政策的更新詳細資訊。如需此頁面變更的自動提醒，請訂閱 Amazon One Enterprise Document 歷史記錄頁面上的 RSS 摘要。

變更	描述	日期
Amazon One Enterprise 新增了 AmazonOneMetricPublishAccess	名為 AmazonOneMetricPublishAccess 的角色許可政策允許 Amazon One Enterprise 在 CloudWatch Namespace AWS/AmazonOne 上執行 CloudWatch：PutMetricData。 CloudWatch AmazonOne	2025 年 2 月 6 日
Amazon One Enterprise 開始追蹤變更	Amazon One Enterprise 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 Enterprise (服務字首：one) 提供以下服務特有的資源、動作和條件內容索引鍵，可用於 IAM 許可政策。

主題

Amazon One Enterprise 定義的動作

您可在 IAM 政策陳述式的 `Action` 元素中指定以下動作。使用政策來授予在 AWS中執行操作的許可。在政策中使用動作時，通常會允許或拒絕存取相同名稱的 API 操作或 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 ("*")。如果資料欄包含資源類型，則您可以在具有該動作的陳述式中指定該類型的 ARN。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 IAM 政策中的 `Resource` 元素限制資源存取，則每種必要的資源類型必須要有 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	授予建立裝置執行個體的許可	寫入		aws:RequestTag/${TagKey} aws:TagKeys	
GetDeviceInstance	准許取得裝置執行個體的相關資訊	讀取	device-instance*		
ListDeviceInstances	准許列出裝置執行個體	讀取			
UpdateDeviceInstance	授予更新裝置執行個體的許可	寫入	device-instance*		
DeleteDeviceInstance	授予刪除裝置執行個體的許可	寫入	device-instance*		
CreateDeviceActivationQrCode	准許建立 QR 碼以在裝置執行個體中啟用裝置	寫入	device-instance*		
DeleteAssociatedDevice	准許刪除裝置與裝置執行個體之間的關聯	寫入	device-instance*		
RebootDevice	授予重新啟動裝置的許可	寫入	device-instance*		
CreateDeviceInstanceConfiguration	授予建立裝置執行個體組態的許可	寫入			

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
GetDeviceInstanceConfiguration	准許取得裝置執行個體組態的相關資訊	讀取	組態*		
CreateSite	授予許可以建立網站	寫入		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSite	授予刪除裝置執行個體的許可	寫入	網站*		
GetSite	准許取得網站的相關資訊	讀取	網站*		
ListSites	授予許可以列出網站	讀取			
GetSiteAddress	准許取得網站地址的相關資訊	讀取	網站*		
UpdateSite	授予更新網站的許可	寫入	網站*		
UpdateSiteAddress	授予更新網站地址的許可	寫入	網站*		
CreateDeviceConfigurationTemplate	授予建立裝置執行個體的許可	寫入		aws:RequestTag/${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
DeleteDeviceConfigurationTemplate	授予刪除裝置組態範本的許可	寫入	device-configuration-template*		
GetDeviceConfigurationTemplate	准許取得裝置組態範本的相關資訊	讀取	device-configuration-template*		
ListDeviceConfigurationTemplates	准許列出裝置組態範本	讀取			
UpdateDeviceConfigurationTemplate	授予更新裝置組態範本的許可	寫入	device-configuration-template*		
TagResource	准許標記資源	標記	device-instance、Site、device-configuration-template	aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	准許取消標記資源	標記	device-instance、Site、device-configuration-template	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
ListTagForResources	准許列出資源的標籤	讀取			

Amazon One Enterprise 定義的資源類型

此服務會定義下列資源類型，並可用在 IAM 許可政策陳述式的 Resource 元素中。動作表格中的每個動作都代表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 Enterprise 定義下列可在 IAM 政策的 Condition 元素中使用的條件索引鍵。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，請參閱條件索引鍵表。

若要檢視所有服務都可使用的全域條件鍵，請參閱可用全域條件鍵。

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 One Enterprise 的合規驗證

若要了解 是否 AWS 服務 在特定合規計劃的範圍內，請參閱AWS 服務 合規計劃範圍內然後選擇您感興趣的合規計劃。如需一般資訊，請參閱 AWS Compliance Programs。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱在 中下載報告 AWS Artifact。

您在使用 時的合規責任 AWS 服務 取決於資料的敏感度、您公司的合規目標，以及適用的法律和法規。 AWS 提供下列資源以協助合規：

- 安全合規與治理 - 這些解決方案實作指南內容討論了架構考量，並提供部署安全與合規功能的步驟。
- HIPAA 合格服務參考 – 列出 HIPAA 合格服務。並非所有 AWS 服務 都符合 HIPAA 資格。
- AWS 合規資源 – 此工作手冊和指南的集合可能適用於您的產業和位置。
- AWS 客戶合規指南 – 透過合規的角度了解共同的責任模型。本指南摘要說明保護 的最佳實務，AWS 服務 並將指南映射到跨多個架構的安全控制 （ 包括國家標準和技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO))。
- AWS Config 開發人員指南中的使用規則評估資源 – AWS Config 服務會評估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 可讓您全面檢視其中的安全狀態 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 控制參考」。
- Amazon GuardDuty – 這會監控您的環境是否有可疑和惡意活動，藉此 AWS 服務 偵測對您 AWS 帳戶、工作負載、容器和資料的潛在威脅。GuardDuty 可滿足特定合規架構所規定的入侵偵測需求，以協助您因應 PCI DSS 等各種不同的合規需求。

- AWS Audit Manager – 這 AWS 服務 可協助您持續稽核 AWS 用量，以簡化您管理風險的方式，以及符合法規和產業標準的方式。

監控 Amazon One Enterprise

監控是維護 Amazon One Enterprise 及其他 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、在發生錯誤時回報，以及適時採取自動動作：

- 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 服務的事件會以近乎即時的方式交付至 EventBridge。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 AWS 您的帳戶發出或代表您的帳戶發出的 API 呼叫和相關事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。您可以識別呼叫的使用者和帳戶 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」。

在 Amazon EventBridge 中監控 Amazon One Enterprise 事件

您可以在 EventBridge 中監控 Amazon One Enterprise 事件，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 EventBridge 發佈，並且可以透過建立新的規則在 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. 前往 https：//https://console.aws.amazon.com/events/ 登入您的 AWS 主控台。
2. 在 https://console.aws.amazon.com/events/ 開啟 EventBridge 主控台。
3. 在導覽窗格中的匯流排下，選擇規則。
4. 選擇建立規則。
5. 在預設規則詳細資訊頁面上，為規則指派名稱。
6. 選擇 Rule with an event pattern (具有事件模式的規則)，然後選擇 Next (下一步)。
7. 在 建置事件模式 頁面中的 事件來源，選擇 AWS 事件或 EventBridge 合作夥伴事件。

8. 在範例事件類型下，選擇 AWS Events。
9. 針對建立方法，選擇自訂模式。
10. 在事件模式區段中，新增事件來源為 aws:one和必要詳細資訊類型的 JSON：

```
"
source": ["aws.one"],
"detail-type": ["New Successful Enrollment",
"New Successful Un-enrollment",
"Unsuccessful Enrollment",
"Unsuccessful Un-enrollment",
"Successful Recognition",
"Unsuccessful Recognition",
"New Alert(s) Detected",
"Some Alert(s) Cleared"]
}
```

    您可以從上述清單中選擇所需的詳細資訊類型，並移除不需要的詳細資訊類型。
11. 選擇下一步。
12. 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。如需設定目標的資訊，請參閱 Amazon EventBridge 目標。

    例如，若要檢視人員打卡的時間，請選擇「成功辨識」。然後查看事件詳細資訊（在附錄中提供），以查看誰打卡上班。

    若要完成工作流程，您可以執行外部 API 或其他目標。
13. 或者，您可以設定標籤。
14. 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 JSON 中產生。針對每一個事件類型，JSON blob 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：

某些警示（已清除）

裝置已通過一或多個運作狀態檢查。

偵測到新的 Alert (s)

裝置未通過一或多個運作狀態檢查。

resources

包含發佈裝置狀態變更事件的 deviceInstance arn 清單。

資料

clearedAlerts

- 代表 deviceInstance 先前失敗的運作狀態檢查。
- 包含警示類型的 statusCode 和 reportedAt 時間戳記。
- 可能statusCode值：NetworkDisconnected、USBDisconnected

currentAlerts

- 代表 deviceInstance 的目前狀態。
- 包含警示類型的 statusCode 和 reportedAt 時間戳記。
- 可能statusCode值：NetworkDisconnected、USBDisconnected

newAlerts

- 代表 deviceInstance 的新失敗運作狀態檢查。
- 包含警示類型的 statusCode 和 reportedAt 時間戳記。
- 可能statusCode值：NetworkDisconnected、USBDisconnected

currentAlertsCount

- 運作狀態檢查目前因 deviceInstance 失敗的計數。

assetTagId

- 與 deviceInstance 相關聯之裝置的 assetTagId。

deviceInstanceName

- 發佈裝置狀態事件的 deviceInstance 名稱。

siteName

- 存在 deviceInstance 的網站名稱。

siteArn

- Arn 適用於存在 deviceInstance 的網站。

使用者設定檔事件類型

使用者描述檔相關的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 Palm 以成功進行身分驗證時。

辨識失敗

當指紋掃描的辨識失敗時。

resources

包含發佈使用者描述檔事件的使用者描述檔 arn 清單。

資料

accountId

- 啟動請求之裝置的相關 AWS 帳戶。

requestSource

- 這是啟動請求之裝置的 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

- 使用者的相關聯 ID，例如徽章 ID。

reason

- 未成功事件將顯示此值。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正常運作

裝置已通過所有運作狀態檢查。


```
{
        "version": "0",
        "id": "51e022b4-7ce6-34e0-264b-370948fc1123",
        "detail-type": "Some Alert(s) Cleared",
        "source": "aws.one",
        "account": "123456789012",
        "time": "2025-07-17T19:32:42Z",
        "region": "us-east-1",
        "resources":
        [
            "arn:aws:one:us-east-1:123456789012:deviceInstance/F5JRte5Jz21Tqx"
        ],
        "detail":
        {
            "version": "1.0.0",
            "data":
            {
                "clearedAlerts":
                [
```

```
                    {
                        "statusCode": "USBDisconnected",
                        "reportedAt": "Thu Jul 17 19:32:42 UTC 2025"
                    }
                ],
                "currentAlerts":
                [],
                "currentAlertsCount": 0,
                "assetTagId": "0000123456",
                "deviceInstanceName": "device_name",
                "siteName": "site_name",
                "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
            }
        }
    }
```

裝置運作狀態已變更為嚴重

裝置未通過一或多個運作狀態檢查。

```
{
        "version": "0",
        "id": "07af4893-ef9f-965a-d245-3f0c8bd3c123",
        "detail-type": "New Alert(s) Detected",
        "source": "aws.one",
        "account": "123456789012",
        "time": "2025-07-17T19:26:58Z",
        "region": "us-east-1",
        "resources":
        [
            "arn:aws:one:us-east-1:123456789012:deviceInstance/12345678901234"
        ],
        "detail":
        {
            "version": "1.0.0",
            "data":
            {
                "newAlerts":
                [
                    {
                        "statusCode": "USBDisconnected",
                        "reportedAt": "Thu Jul 17 19:26:58 UTC 2025"
                    }
```

```
                ],
                "currentAlerts":
                [
                    {
                        "statusCode": "USBDisconnected",
                        "reportedAt": "Thu Jul 17 19:26:58 UTC 2025"
                    }
                ],
                "currentAlertsCount": 1,
                "assetTagId": "0000123456",
                "deviceInstanceName": "device_name",
                "siteName": "site_name",
                "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
            }
        }
    }
```

裝置連線已變更為線上

裝置現在已連線至網際網路。

```
{
        "version": "0",
        "id": "e6ecea28-dd60-5061-29f8-dfbc902f4123",
        "detail-type": "Some Alert(s) Cleared",
        "source": "aws.one",
        "account": "123456789012",
        "time": "2025-07-17T18:28:23Z",
        "region": "us-east-1",
        "resources":
        [
            "arn:aws:one:us-east-1:123456789012:deviceInstance/12345678901234"
        ],
        "detail":
        {
            "version": "1.0.0",
            "data":
            {
                "clearedAlerts":
                [
                    {
                        "statusCode": "NetworkDisconnected",
                        "reportedAt": "Thu Jul 17 18:28:23 UTC 2025"
```

```
                }
            ],
            "currentAlerts":
            [],
            "currentAlertsCount": 0,
            "assetTagId": "0000123456",
            "deviceInstanceName": "device_name",
            "siteName": "site_name",
            "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
        }
    }
}
```

裝置連線已變更為離線

裝置不再連線至網際網路。

```
{
        "version": "0",
        "id": "e6ecea28-dd60-5061-29f8-dfbc902f4123",
        "detail-type": "New Alert(s) Detected",
        "source": "aws.one",
        "account": "123456789012",
        "time": "2025-07-17T18:28:23Z",
        "region": "us-east-1",
        "resources":
        [
            "arn:aws:one:us-east-1:123456789012:deviceInstance/12345678901234"
        ],
        "detail":
        {
            "version": "1.0.0",
            "data":
            {
                "newAlerts":
                [
                    {
                        "statusCode": "NetworkDisconnected",
                        "reportedAt": "Thu Jul 17 18:28:23 UTC 2025"
                    }
                ],
                "currentAlerts":
                [
```

```
                {
                    "statusCode": "NetworkDisconnected",
                    "reportedAt": "Thu Jul 17 18:28:23 UTC 2025"
                }
            ],
            "currentAlertsCount": 1,
            "assetTagId": "0000123456",
            "deviceInstanceName": "device_name",
            "siteName": "site_name",
            "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
        }
    }
}
```

使用 記錄 Amazon One Enterprise API 呼叫 AWS CloudTrail

Amazon One Enterprise 已與 整合 AWS CloudTrail，此服務提供 Amazon One Enterprise AWS 中使用者、角色或服務所採取動作的記錄。CloudTrail 會將 Amazon One Enterprise 的所有 API 呼叫擷取為事件。擷取的呼叫包括從 Amazon One Enterprise 主控台呼叫，以及對 Amazon One Enterprise API 操作的程式碼呼叫。如果您建立線索，您可以啟用 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 Amazon One Enterprise 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。使用 CloudTrail 收集的資訊，您可以判斷對 Amazon One Enterprise 提出的請求、提出請求的 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「AWS CloudTrail 使用者指南」。

CloudTrail 中的 Amazon One Enterprise 資訊

建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。當活動在 Amazon One Enterprise 中發生時，該活動會記錄於 CloudTrail 事件，以及事件歷史記錄中的其他服務 AWS 事件。您可以在 中檢視、搜尋和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱「使用 CloudTrail 事件歷史記錄檢視事件」。

若要持續記錄 中的事件 AWS 帳戶，包括 Amazon One Enterprise 的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 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。追蹤會記錄 AWS 分割區中所有 區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析 CloudTrail 日誌中收集的事件資料並對其採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合

- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案和接收多個帳戶的 CloudTrail 日誌檔案

CloudTrail 會記錄所有 Amazon One Enterprise 動作，並記錄在 中Amazon One Enterprise 的動作、資源與條件索引鍵。例如，對 `ListSites`、`RebootDevice` 和 `DeleteDeviceInstance` 動作發出的呼叫會在 CloudTrail 記錄檔案中產生專案。

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：

- 請求是使用根還是 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 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 One Enterprise 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

以下範例顯示的是展示 `CreateSite` 動作的 CloudTrail 日誌項目。

```
{
    "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 故障診斷

如果您對於 Amazon One 應用程式或其中一個 Amazon One 裝置發生問題，請使用這些建議來排除問題。然後，如果您仍然遇到問題，請聯絡 AWS Support。

主題

對 Amazon One 身分和存取進行故障診斷

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

主題

我無權在 Amazon One 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。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 one:*GetWidget* 許可時發生。

```
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 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。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

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 IAM 搭配使用。
- 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》中的在您擁有 AWS 帳戶 的另一個 中提供存取權給 IAM 使用者。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有的 。
- 如需了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 如需了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱《IAM 使用者指南》中的 IAM 中的跨帳戶資源存取。

Amazon One Console 故障診斷

如果您對於 Amazon One 應用程式或其中一個 Amazon One 裝置發生問題，請使用這些建議來排除問題。然後，如果您仍然遇到問題，請聯絡 AWS Support。

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。
- 若問題仍持續發生，請聯絡 AWS Support。

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。
- 若問題仍持續發生，請聯絡 AWS Support。

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。
- 若問題仍持續發生，請聯絡 AWS Support。

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。
- 若問題仍持續發生，請聯絡 AWS Support。

Amazon One 裝置故障診斷

如果您對於 Amazon One Console 或其中一個 Amazon One 裝置有問題，請使用這些建議來排除問題。然後，如果您仍然遇到問題，請聯絡 AWS Support。

主題

- 裝置已重新啟動，並顯示錯誤訊息和錯誤碼
- 裝置畫面上沒有進一步活動的 Amazon 標誌
- 暫時無法使用
- 結束發生錯誤
- 暫時停止服務
- Amazon One 裝置有實體損壞
- 無法讀取指紋
- 無法辨識 Palm
- 裝置因長時間閒置而鎖定
- 裝置因竄改事件而鎖定

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：

- 等待幾分鐘（少於 30 秒），以防裝置重新啟動。
- 如果裝置空白時燈環正在脈衝，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到 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此問題，請從電源供應器拔除 Amazon One USB 中樞，然後重新插入。
- 若問題仍持續發生，請聯絡 AWS Support。

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：

- 如果連線到 Wi-Fi，請使用其他裝置來檢查 Wi-Fi 是否顯示在可用的網路中。

- 檢查 Wi-Fi 路由器是否已開啟並在範圍內。
- 一旦網路復原，裝置就會重新連線。
- 如果問題仍然存在，請聯絡 AWS Support。

重新啟動具有作用中提醒的裝置

從主控台請求重新啟動時，操作會等待最多 15 分鐘，讓裝置收到命令並嘗試重新啟動，即使裝置離線或面臨網路問題。

執行下列動作來疑難排解此問題：

- 等待重新啟動完成。
- 如果問題仍然存在，請聯絡 AWS Support。

系統錯誤

這是因為內部錯誤。

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 Support。

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：

- 選擇再試一次以導覽回 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 代碼

掃描多個 QR 代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不存在於 AWS 主控台時，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 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 AWS 主控台中刪除或不存在網站時，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。

郵遞區號不相符

當輸入與裝置設定不同的郵遞區號時，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郵遞區號畫面。

- 檢查您是否有正確的網站郵遞區號。
- 如果問題仍然存在，請聯絡您的管理員，在 AWS 主控台上檢查網站郵遞區號。

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 Support。

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 Support。

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，請從電源供應器拔除 USB 集線器並重新連接。
- 若問題仍持續發生，請聯絡 AWS Support。

裝置畫面上沒有進一步活動的 Amazon 標誌

執行下列動作來疑難排解此問題：

- 等待幾分鐘（少於 30 秒），以防裝置重新啟動。
- 從電源供應器拔除 USB 集線器並重新連接。
- 若問題仍持續發生，請聯絡 AWS Support。

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 連線是安全的。
- 中斷連接並重新連接所有進入 USB 集線器的纜線。
- 若問題仍持續發生，請聯絡 AWS Support。

結束發生錯誤

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. 將其從電源中斷。
3. 等待 30 秒。
4. 將裝置插回其電源。
5. 開啟裝置電源。
6. 若問題仍持續發生，請聯絡 AWS Support。

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：

- 請聯絡 AWS Support。

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 Support，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。

無法讀取指紋

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遮蔽物，例如包布、捲筒和明顯的泥土/油。
- 如果問題仍然存在，且裝置未讀取任何棕櫚樹，請聯絡 AWS Support。

無法辨識 Palm

執行下列動作來疑難排解此問題：

- 讓客戶嘗試使用他們的另一個掌心。
- 確定客戶已註冊。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，且裝置未讀取任何棕櫚樹聯絡人，請聯絡 AWS Support。

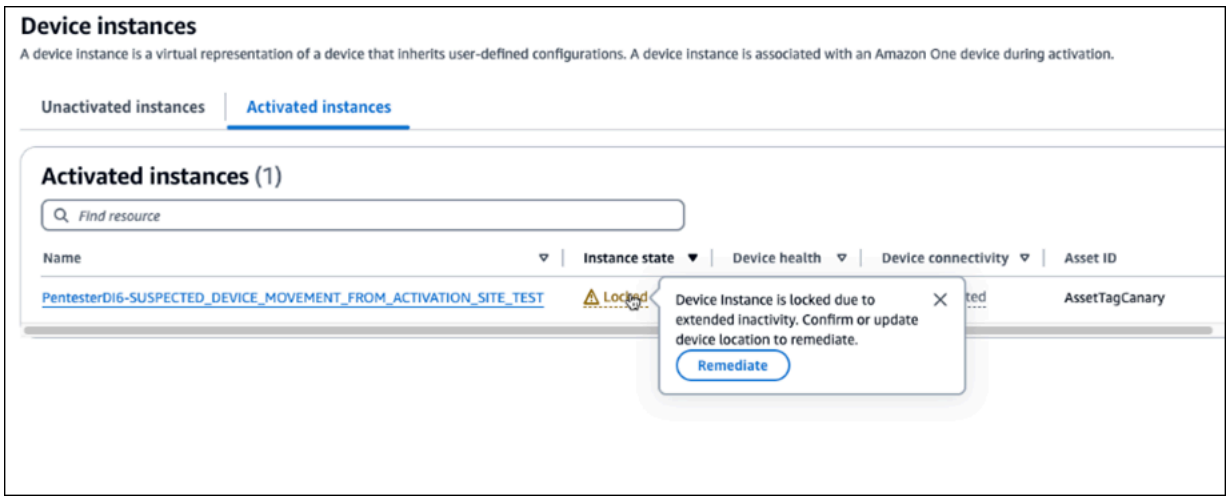
裝置因長時間閒置而鎖定

當裝置懷疑它已從啟用網站移動時，它會鎖定使用者。當裝置超過最長 120 小時的離線時間時，就會發生這種情況。

執行下列動作以解鎖裝置：

1. 登入您的 AWS 主控台，然後選擇裝置執行個體。
2. 從頁面頂端的錯誤橫幅中，選取修復。

   或者：從已啟用的執行個體中，選取鎖定，然後選擇修復。



3. 如果裝置仍在原始啟用網站，請選擇是，裝置就位於此網站。
4. 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。在新站點啟用裝置。

裝置因竄改事件而鎖定

基於安全考量，Amazon One 裝置將在發生任何竄改事件時遭到鎖定。

執行下列動作來疑難排解此問題：

- 請聯絡 AWS Support。

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	已新增服務連結角色區段	2025 年 2 月 4 日
更新	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 裝置故障診斷	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：維護和清理 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。