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 一個企業如何工作

Amazon One 企業版是一種雲端生物識別服務，使用 Amazon One 裝置使用手掌生物識別技術驗證使用者。您可以聯絡我們訂購 Amazon One 裝置，也可以使用註冊 Amazon One 企業安全存取服務 AWS Management Console。

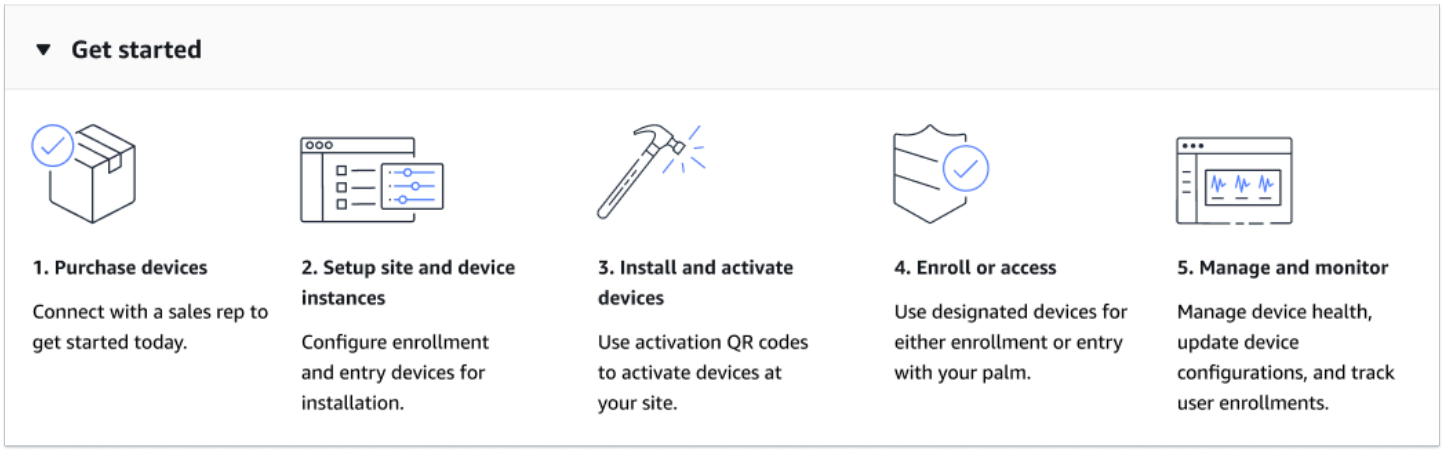
安裝 Amazon One 企業版之後，您可以在 Amazon One 企業主控台 AWS 帳戶 上啟用裝置並註冊裝置，並且可以使用身份驗證應用程式。您也可以檢視已註冊員工的生物識別設定檔，也可以取消員工的註冊。當員工離開公司或遺失徽章時，您可以輕鬆刪除他們的生物特徵識別資料。Amazon One 企業主控台也可做為管理操作活動的集中位置，例如追蹤已安裝的裝置和檢視每月帳單。

員工可以通過在現場受監督的註冊站掃描徽章和手掌進行註冊。員工註冊後，只要將手掌停留在 Amazon One 裝置上，即可進入或離開安全位置。

主題

Amazon 一企業工作流

下圖顯示了 Amazon 一個企業的基本工作流程。



1. 請聯絡我們購買 Amazon One 裝置。
2. 建立網站和裝置執行個體，設定註冊和登入裝置以進行安裝。
3. 安裝後，透過掃描裝置執行個體專用的安全 QR 碼來啟用 Amazon One 裝置。
4. 要求員工註冊他們的手掌，然後用手掌進行身份驗證以獲得訪問權限。

5. 利用管理和監控功能：確保裝置健康狀態、將組態保持在最新狀態，以及追蹤使用者登記，以進行全面監督。

Amazon 一個企業關鍵條款

這些是 Amazon 一個企業的關鍵術語：

- 網站 — 客戶管理的實體建築物，客戶可在其中安裝 Amazon One 企業裝置。網站必須符合您 Amazon One 企業裝置的設施、網路和電源需求。
- 裝置 — 用於身份驗證的 Amazon One 企業掌心掃描生物識別裝置。
- 設備實例 — 具有配置的設備的邏輯表示。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) 以及一組通訊設定。裝置執行個體有三種主要狀態：
  - 需要配置
  - 準備啟動
  - 作用中
- 配置模板 — 在設備實例上應用的一組全包配置。

開始使用

本章介紹了開始使用 Amazon 一個企業的基本步驟：

1. 設定網站、裝置執行個體和組態範本：請按照下列步驟建立框架，用於新增實體位置以容納 Amazon One 裝置，然後對其進行設定和管理。這些步驟使用 Amazon 一個企業控制台。根據您選擇擁有的網站、裝置執行個體和設定範本的數量，您只會偶爾使用或甚至只使用一次此程序。
2. 安裝和啟用裝置 — 在設定開始時，請依照下列步驟操作。裝置啟用需要安裝程式透過行動電話存取 Amazon One 企業主控台，以擷取啟用 QR 碼。
3. 裝置和使用者管理 — 請依照下列步驟操作，以便日常使用 Amazon One 企業主控台。您可以使用這些步驟來監視裝置健康狀況、瞭解使用者參與度指標，以及設定裝置。

要了解有關 Amazon 單一企業的更多信息，您可以訪問 Amazon 一個企業產品詳細信息頁面。

主題

建立 Amazon 一個企業

使用 Amazon One 企業版的第一步是使用 Amazon One 企業主控台設定您的網站、裝置執行個體和組態範本。

主題

步驟 1：建立帳戶和管理員使用者

註冊一個 AWS 帳戶

如果您沒有 AWS 帳戶，請完成下列步驟來建立。

若要註冊成為 AWS 帳戶

1. 打開https://portal.aws.amazon.com/billing/註冊。
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。

   當您註冊一個 AWS 帳戶，一個 AWS 帳戶根使用者已建立。根使用者可以存取所有 AWS 服務 和帳戶中的資源。作為安全最佳實務，請將管理存取權指派給使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

AWS 註冊過程完成後，會向您發送確認電子郵件。您可以隨時前往 https://aws.amazon.com/並選擇「我的帳戶」，檢視目前的帳戶活動並管理您的帳戶。

建立具有管理存取權的使用者

在您註冊一個 AWS 帳戶，保護您的 AWS 帳戶根使用者，啟用 AWS IAM Identity Center，並建立系統管理使用者，這樣您就不會將 root 使用者用於日常工作。

保護您的 AWS 帳戶根使用者

1. 登入 AWS Management Console通過選擇 Root 用戶並輸入您的帳戶所有者 AWS 帳戶 電子郵件地址。在下一頁中，輸入您的密碼。

   如需使用 root 使用者登入的說明，請參閱以 root 使用者身分登入 AWS 登入 使用者指南。
2. 為您的 root 使用者開啟多因素驗證 (MFA)。

   如需指示，請參閱為您的MFA裝置啟用虛擬裝置 AWS 帳戶 使用者指南中的 root IAM 使用者 (主控台)。

建立具有管理存取權的使用者

1. 啟用IAM身分識別中心。

如需指示，請參閱啟用 AWS IAM Identity Center 中的 AWS IAM Identity Center 使用者指南。

2. 在IAM身分識別中心中，將管理存取權授與使用者。

   若要取得有關使用 IAM Identity Center 目錄 做為您的身分識別來源，請參閱以預設值設定使用者存取 IAM Identity Center 目錄 中的 AWS IAM Identity Center 使用者指南。

以具有管理存取權的使用者身分登入

- 若要使用您的 IAM Identity Center 使用者登入URL，請使用建立IAM身分識別中心使用者時傳送至您電子郵件地址的登入資訊。

  如需使用IAM身分識別中心使用者登入的說明，請參閱登入 AWS 存取入口網站 AWS 登入 使用者指南。

指派存取權給其他使用者

1. 在 IAM Identity Center 中，建立遵循套用最低權限權限的最佳作法的權限集。

   如需指示，請參閱 AWS IAM Identity Center 使用者指南。

2. 將使用者指派至群組，然後對該群組指派單一登入存取權。

   如需相關指示，請參閱 AWS IAM Identity Center 使用者指南。

步驟 2：添加 Amazon 一個企業用戶

除了管理員使用者之外，您還可以新增缺少管理員權限的使用者。例如，這些使用者可能是只存取 Amazon One 企業主控台以擷取裝置啟用 QR 碼以啟用 Amazon One 裝置的安裝程式。

要添加 Amazon 一個企業用戶

1. 依照如何登入至中所述，遵循適合您使用者類型的登入程序 AWS 在 AWS 登入 使用者指南。
2. 在功能窗格中，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。這是他們的登入名稱 AWS.

> **Note**
>
> IAM資源的數量和大小 AWS 帳戶 是有限的。如需詳細資訊，請參閱IAM和AWSSTS配額。使用者名稱最多可由 64 個字母、數字和下列字元組成：加號 (+)、等於 (=)、逗號 (,)、句號 (.)、@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，您無法建立兩個名為TESTUSER和 testuser 的使用者。在策略中使用使用者名稱或作為一部分使用者名稱時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 [提供使用者存取權限 — AWS Management Console 可選的。
5. 選取 [我要建立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 — 系統會為使用者提供符合帳號密碼策略的隨機產生密碼。您可在進入 擷取密碼 頁面時檢視或下載密碼。
   - 自訂密碼 — 系統會為使用者指定您在欄位中輸入的密碼。
7. (選用) 根據預設，系統會選取「使用者必須在下次登入時建立新密碼 (建議使用)」，以確保使用者在第一次登入時必須變更其密碼。

> **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，它會自動附加 AWS 為新使用者命名IAMUserChangePassword的受管理策略。政策會授予他們變更自己密碼的許可。

8. 選取 下一步。
9. 在 [設定權限] 頁面上，選擇 [直接附加原則]。
10. 選取您要附加至使用者的策略。
    - AmazonOneEnterpriseReadOnlyAccess
    - AmazonOneEnterpriseInstallerAccess

> **Note**
>
> AmazonOneEnterpriseInstallerAccess 受管政策只能在 Amazon One 企業主控台提供使用者存取啟用 QR 碼的權限。此政策非常適合聘請第三方安裝 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。如需有關在中使用標籤的詳細資訊IAM，請參閱標記IAM資源。
13. 檢閱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]，將使用者的登入認證下載為 .csv 檔案，您可以儲存到安全位置。
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到帳戶登錄頁面。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。

步驟 3：建立網站

現在您已經登入 AWS Management Console，您可以使用 Amazon One 企業主控台建立您的網站。

> **Important**
>
> Amazon One 企業版僅在美國東部 (維吉尼亞北部) 區域提供。

建立網站

1. 在 https://console.aws.amazon.com/一個企業打開 Amazon 一個企業控制台。
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，對於「網站名稱」，輸入網站的名稱。
6. 在「實體位址」下，輸入要安裝 Amazon One 裝置的網站地址。
7. (選擇性) 若要將標籤新增至網站，請在「標籤」下輸入機碼值配對，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。

步驟 4：創建設備實例

若要建立裝置執行個體

1. 在 https://console.aws.amazon.com/一個企業打開 Amazon 一個企業控制台。
2. 在導覽窗格中，選擇 [裝置執行個體]。確定您位於 [未啟動的執行個體] 索引標籤上。
3. 在「執行個體詳細資料」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. 手動輸入每個裝置執行個體名稱。
5. (選擇性) 若要將標籤新增至裝置執行個體，請在標籤下輸入金鑰值配對，然後選擇 [新增標籤]。若要在建立裝置實體之前移除此標籤，請選擇 [移除]。
6. 選擇 [建立執行個體] 建立裝置執行個體。

> **Note**
>
> 注意：裝置執行個體必須先設定，才能進行安裝。

步驟 5：建立設定範本

若要建立組態範本

1. 在 https://console.aws.amazon.com/一個企業打開 Amazon 一個企業控制台。

2. 在瀏覽窗格中，選擇 [組態範本]。
3. 選擇建立範本。
4. 在範本資訊下，對於範本名稱，輸入組態範本的名稱。
5. 在 [裝置組態] 下，選取 [作業模式]。

To configure Enrollment operating mode

1. （可選）在 Wifi 配置下，提供您的 Wifi 憑據。
2. (選擇性) 若要將標籤新增至網站，請在「標籤」下輸入機碼值配對，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 [控制台設定] 下，提供 Amazon One 裝置與控制面板通訊的通訊設定。
2. 在「徽章格式設定」下，提供指定公司徽章格式版面配置的組態設定。
3. （可選）在 Wifi 配置下，提供您的 Wifi 憑據。
4. (選擇性) 若要將標籤新增至網站，請在「標籤」下輸入機碼值配對，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**
>
> 您必須至少設定一個註冊裝置和一個入門裝置，才能啟用 Amazon One 企業版的完整功能，以便安全存取。

步驟 6：設定要啟用的裝置執行個體

建立裝置執行個體之後，您可以使用先前建立的設定範本來設定裝置執行個體 (請參閱步驟 5：建立設定範本)，或者您也可以手動新增設定。

設定要啟用的裝置執行個體

1. 在 https://console.aws.amazon.com/一個企業打開 Amazon 一個企業控制台。
2. 在導覽窗格中，選擇 [裝置執行個體]。確定您位於 [未啟動的執行個體] 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. 對於「使用範本」選項，請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」選項的資訊，請參閱 步驟 5：建立設定範本

   b. 對於手動輸入選項，請選取操作模式。

      To configure Enrollment operating mode

      a. （可選）在 Wifi 配置下，提供 Wifi 憑據。
      b. (選擇性) 若要將標籤新增至網站，請在「標籤」下輸入機碼值配對，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 [控制台設定] 下，提供 Amazon One 裝置與控制面板通訊的通訊設定。
      b. 在「徽章格式設定」下，提供指定公司徽章格式版面配置的組態設定。
      c. （可選）在 Wifi 配置下，提供 Wifi 憑據。
      d. (選擇性) 若要將標籤新增至網站，請在「標籤」下輸入機碼值配對，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「未啟動的例證」表下，「例證」狀態應該會顯示 Ready for activation 出來。
7. 驗證激活 QR 碼是否可用於激活。在功能窗格中，選擇「啟用 QR 碼」。
8. 從 「選取地點」下拉式清單中選取「地點」。
9. 在「網站資訊」下，驗證「網站」位址。
10. 在「啟用 QR 碼」下，每個裝置執行個體都有對應的 QR 碼。選擇「獲取 QR 碼」以顯示激活 QR 碼。

> **Important**
>
> 您必須至少設定一個註冊裝置和一個入門裝置，才能啟用 Amazon One 企業版的完整功能，以便安全存取。

安裝和激活 Amazon 一

設定完 Amazon One 企業主控台之後，接下來的步驟是在您的網站上安裝 Amazon One 企業裝置，然後啟用它們。

> **Note**
>
> 本節重點介紹安裝，並使用移動瀏覽器訪問 AWS Management Console 獲取設備激活 QR 碼。

主題

了解需求

Amazon One 裝置可安裝在任何擁有可電動控制門的公司或商業地點。

控制面板要求

Amazon One 裝置可以作為讀取器連接到大多數標準存取控制面板。Amazon 一個設備支持以下協議：

- OSDP（第 1 和第 2 版）
- 韋根

網路需求

Amazon One 設備必須始終連接到互聯網才能正常運行。互聯網連接可以通過有線以太網或 Wi-Fi 提供。所需的最低頻寬為 10 Mbps。

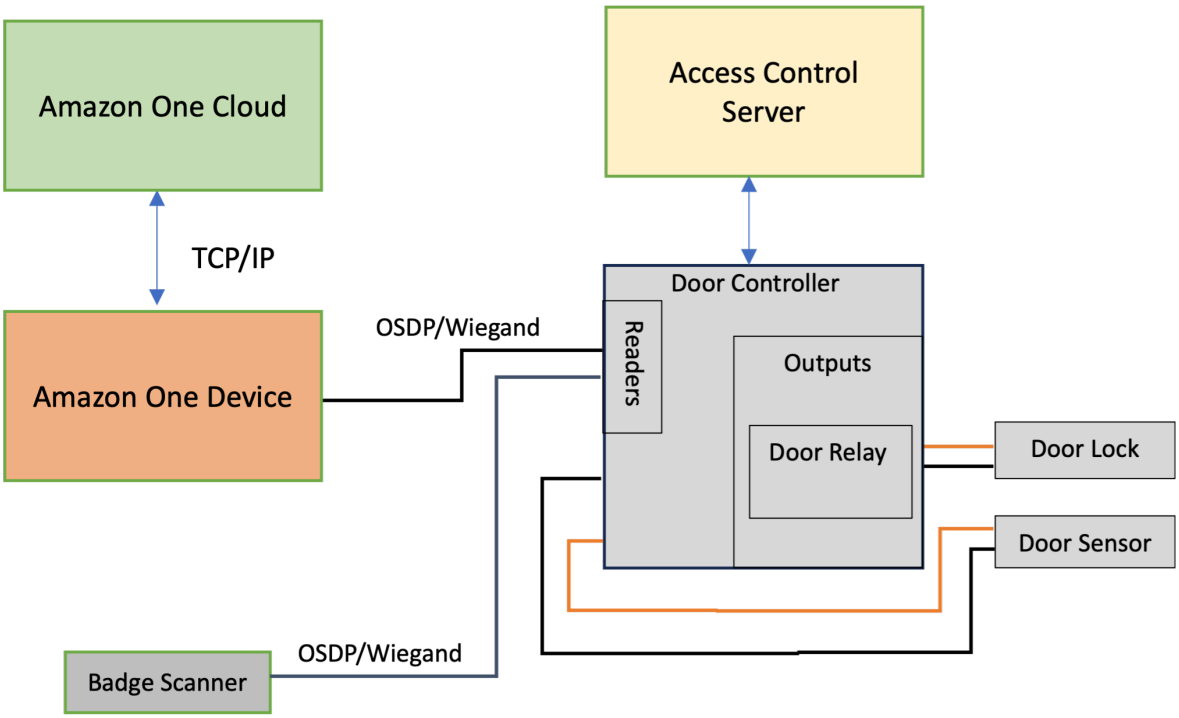
電源需求

Amazon One 裝置可以透過以下兩種方式之一進行供電：

- 通過使用包裝盒中提供的 120V 電源適配器。
- 通過使用啟用 PoE+ 的設備。

瞭解安裝概念

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



存取控制環境通常由下列元件組成：

- Amazon One 裝置：這是掌心辨識裝置，可執行生物特徵驗證，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限。有權訪問該區域IDs的個人的徽章通常存儲在此服務器上。此伺服器會快取與適當IDs的門控制器相關的資訊。
- 門控制器:
  - Amazon One 裝置透過一個OSDP介面連接到門控制器伺服器。
  - 如果需要韋根界面，則可以使用 COTS OSDP Wegand 轉換器。
  - 成功身份驗證後，Amazon One 裝置會將使用者的徽章 ID 傳送到門控制器。
  - 門控制器會回應決定，然後 Amazon One 裝置可顯示「授與存取」或「拒絕存取」訊息。
- 徽章掃描儀：徽章掃描器通常用於掃描RFID徽章並將徽章號碼發送到訪問控制服務器。使用 Amazon One 企業版，徽章掃描器會連接到註冊 Amazon One 裝置，以便掃描員工徽章並與其掌心檔案建立關聯。

安裝 Amazon 一個企業基座

本節概述安裝 Amazon One 企業基座所需的位置要求和步驟。

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，請確定已佈置 Cat6 纜線，並可使用 POE + 注射器或開關。
- 如果使用交流電源 (120V) 電源，交流電插座應在底座 20 英尺範圍內提供。AOE
- 地板必須是水平和乾淨的。
- 底座不得阻塞門或車道。
- 所有多餘的電纜應存放在底座內並固定。

安裝 Amazon 一台設備底座

1. 從包裝中取出 Amazon One 企業基座。

2. 擰下兩個 M4 防篡改螺絲來卸下門。
3. 插入電源線。將纜線穿過底座基板上的孔。
4. 線圈基座內部的任何多餘電源線。
5. 將乙太網路纜線 (Cat5E 或更高版本) 穿過底座底板，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) 穿過底座底板，然後插入乙太網路連接埠。
7. 在基座底座上方 2 英吋處的乙太網路纜線上安裝鐵氧體環。
8. 將RS485序列纜線從存取控制面板 (或徽章讀取器) 送入底座，長度超過 1 英尺。
9. 在基座底座上方 2 英吋處的RS485纜線上安裝鐵氧體環。
10. 將電源插入插座，並確認 Amazon One 裝置已開啟。
11. 將門重新安裝到底座上，然後重新擰緊兩個 M4 防篡改螺絲以固定。

安裝壁掛式 Amazon 一台設備

本節詳細說明安裝可壁掛式 Amazon One 裝置所需的位置需求和步驟。

在開始安裝之前，請確保以下事項：

- 可壁掛式 Amazon 亞馬遜一款裝置僅供室內使用。
- 牆是水平的。
- 安裝後，壁掛安裝的頂部距離地面不應高於 44-46 英寸。
- 所有多餘的電纜都位於牆壁安裝後面並固定。
- 對於乙太網路供電 (PoE++)：

  請確定可使用 IEEE 802.3bt (類型 3) 類別 6 POE ++ 交換器 (端部跨度) 或注射器 (中跨度)，該交換器已列出或認證，並符合 62368-1。IEC

  僅與經核准AOE的 PoE++ 來源搭配使用。

  PoE++ 的源代碼必須位於同一建築物內。

- 對於 15V 直流電源輸入，您只能使用 Amazon One 裝置搭配列出或認證的 NEC Class 2 或電源受限核准的電源供應器。

所需工具：

- 如果需要牆壁錨栓，則為 1/4 英寸乾牆或磚石鑽頭
- 剝線鉗
- 7/64」鑽頭，用於鑽導孔
- #2 十字螺絲起子
- 0.5 公釐 x 2 公釐平頭螺絲起子
- T12 安全星形驅動程序
- 鉛筆
- Level

包括壁掛式 Amazon 一個設備:

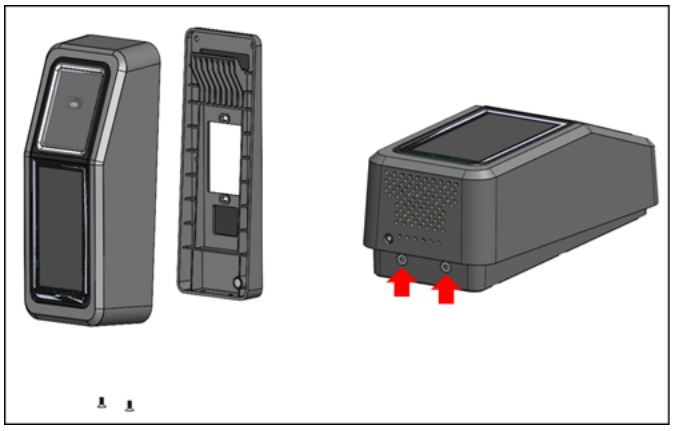
- 6x #8 石膏板錨栓
- 6 個 #8 -32 1 英寸長螺絲
- #6 -32 1 吋機械螺絲
- 2x 6 位置端子台連接器
- 2 個梅花安全 M4x10 平頭螺絲

為您的 Amazon One 裝置安裝壁掛式安裝板

<result>

</result>

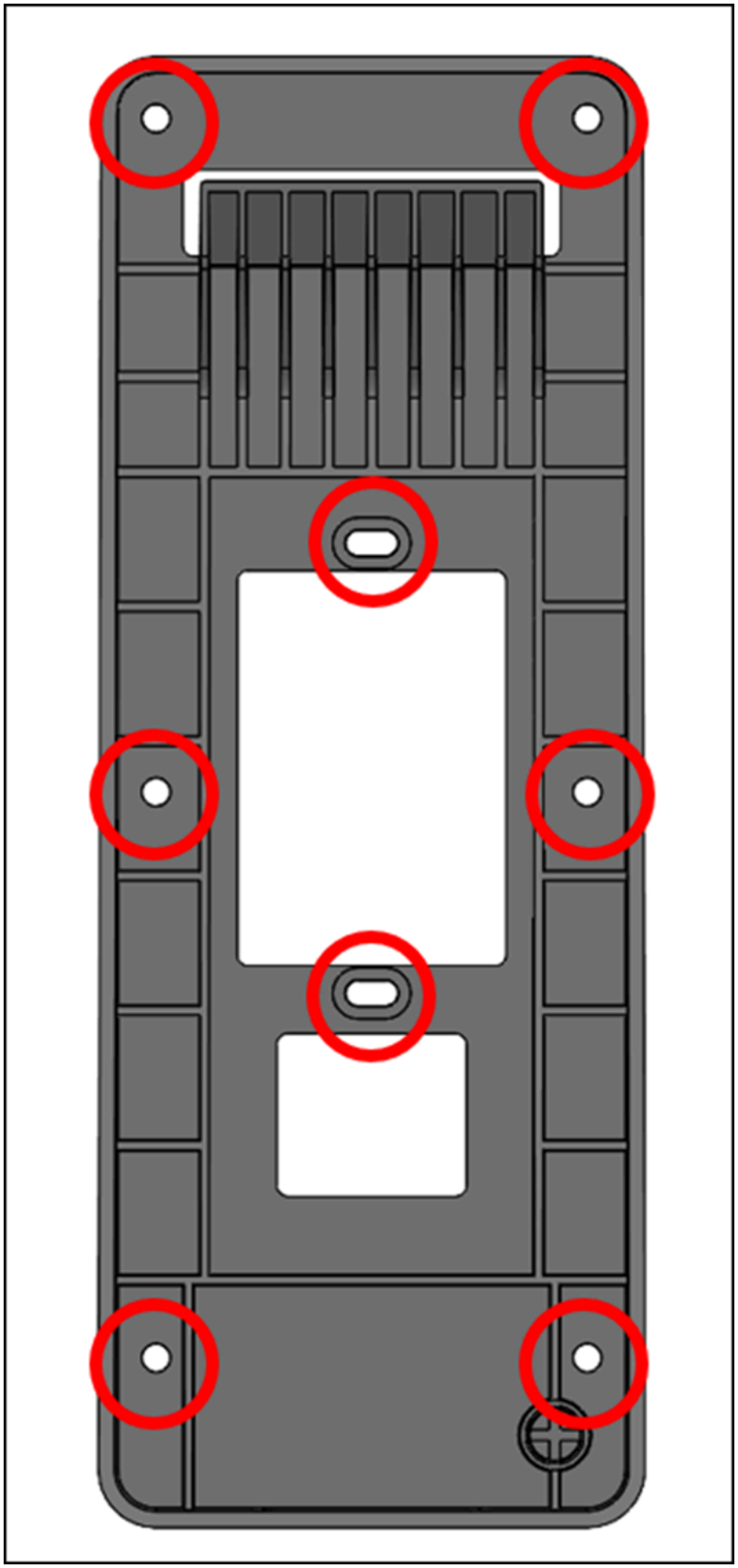
1. 從包裝中取出您的 Amazon One 設備。
2. 移除底部的兩顆 Torx 安全螺絲，將安裝板與您的 Amazon One 裝置分開。



3. 將安裝板放置在牆上的所需位置。使用托架做為樣板來標記外部六個螺絲孔，如下圖所示。

(選擇性) 如果安裝位置有單一幫派方塊，請執行下列動作：

- 通過將隨附的 #6 -32 機器螺釘通過橢圓形孔鬆散地安裝到幫派盒上。
- 確保安裝板處於水平狀態。
- 使用安裝板作為樣板，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撐。請勿使用 #6 -32 螺絲位置作為安裝牆板的主要方法。



4. 如果安裝在灰泥板，石膏板，磚或混凝土表面上，請在每個標記的位置鑽 1/4 英寸的孔，然後通過將其壓入孔中來安裝牆錨，直到錨與牆齊平。

   如果安裝在木質表面上，則不需要錨栓，標記位置只需要 7/64 英寸的導向孔。

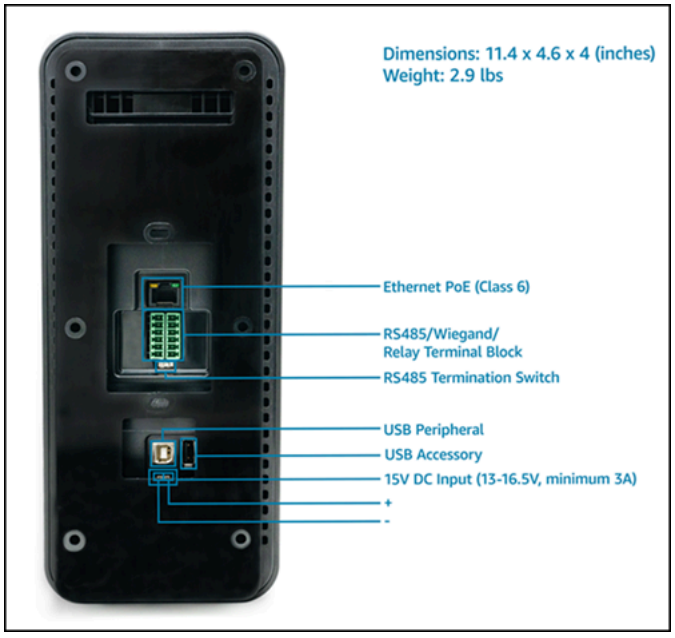
5. 鬆散地將牆板固定在牆壁上使用 #8 在錨定位置的木螺釘。
6. 完成所有緊固件後，請確保安裝板處於水平狀態。
7. 擰緊螺絲以將安裝板固定在牆上。

連接您的壁掛式 Amazon One 設備

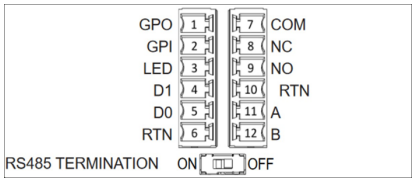
您可以使用OSDP和威格存取控制協定來設定 Amazon One 裝置。為了簡化安裝，Amazon One 裝置使用端子台連接器 (製造商 P/N：鳳凰城聯絡 1767694)。您也可以選擇使用內部轉送或一般用途輸入和輸出連線，將 Amazon One 裝置設定為直接控制外部裝置。

1. 若要為您的應用決定適當的佈線配置，請參閱下圖和連接表。

   有關信號的詳細電氣特性，請參閱接線說明。



連線



Pin	連線	描述	使用	
1	GPO	一般用途輸出	數字輸出信號-可選	
2	GPI	一般用途輸入	數字輸入信號 — 可選	
3	LED	韋根 LED	韋根-可選 LED	
4	D1	韋根 D1	韋根資料 1 — 白線	
5	D0	韋根 D0	韋根資料 0 — 綠色電線	
6	RTN	信號返回	韋根接地 — 黑線	
7	COM	繼電器常見	接點繼電器通用 — 白線	
8	NC	繼電器，常閉	接點繼電器，常閉 — 橙色電線	
9	NO	繼電器常開	接點繼電器，常開 — 黃線	
10	RTN	信號返回	OSDP返回 — 黑線	
11	A	RS485時鐘	OSDPD1 — 白色電線	
12	B	RS485_B/D0/數據	OSDPD0 — 綠色電線	

2. 安裝電線時，從導線末端剝離 3 毫米 -5mm。
3. 將配線的剝離端插入所需的端子位置。

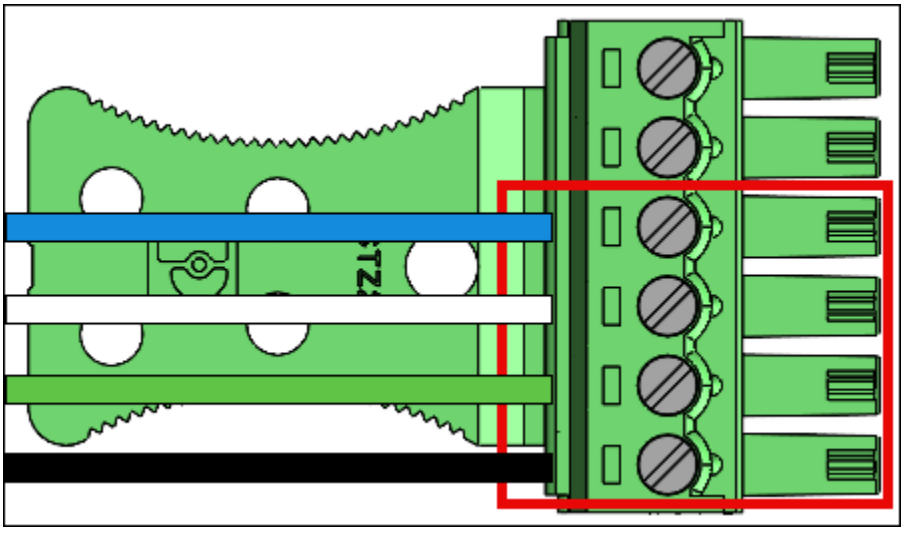
4. 使用平頭螺絲起子，順時針旋轉端子固定螺絲，以夾住電線，直到緊密為止。不要過度擰緊。
5. 固定後，輕輕拉扯電線以確保其就位。
6. 進行必要的連接後，將插頭插入 Amazon One 裝置端子台的對應插座。
7. 將 Cat6 乙太網路纜線插入插RJ45孔。
8. 放置 Amazon One 裝置，使牆板上的掛鉤滑入裝置後方的開口。
9. 確保纜線沒有卡在裝置和安裝板之間，並讓裝置旋轉並安裝到位。
10. 使用兩個 Torx 安全 M4x10 平頭螺絲將您的 Amazon One 裝置固定在安裝板上。
11. 用手擰緊螺絲。不要過度擰緊。

連接您的壁掛式 Amazon One 設備

僅為您的應用安裝所需的電線。

韦根连接

- 在接腳 3 (LED) 中插入藍色線材。
- 在接腳 4 (D1) 中插入白色線材。
- 在接腳 5 (D0) 中插入綠色線材。
- 在接腳 6 (RTN) 中插入黑線。



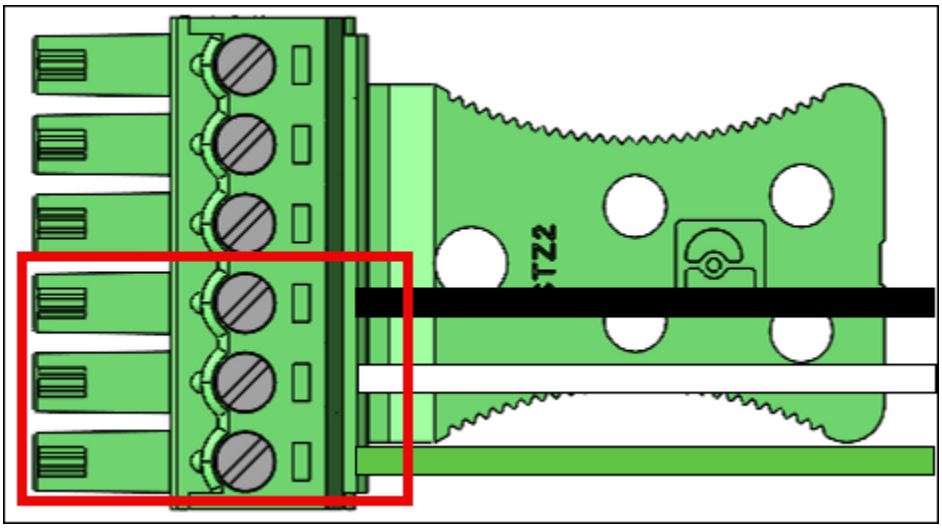
韋根輸出接線

Pin	連線	描述	使用	
3	LED	韋根 LED	韋根LED輸入 — 可選 (5V) TTL	
4	D1	韋根 D1	韋根 D1 輸出（5V）TTL	
5	D0	韋根 D0	韋根 D0 輸出 (5V) TTL	
6	RTN	信號返回	韋根GND參考	

打開RS485終端開關「ON」，如果設備是線路上的最後一個單元。該開關激活 120 歐姆電阻終端在線上。

RS485連接

- 在接腳 10 (RTN) 中插入黑線。
- 在接腳 11 (A) 中插入白色電線。
- 在接腳 12 (B) 中插入綠色電線。

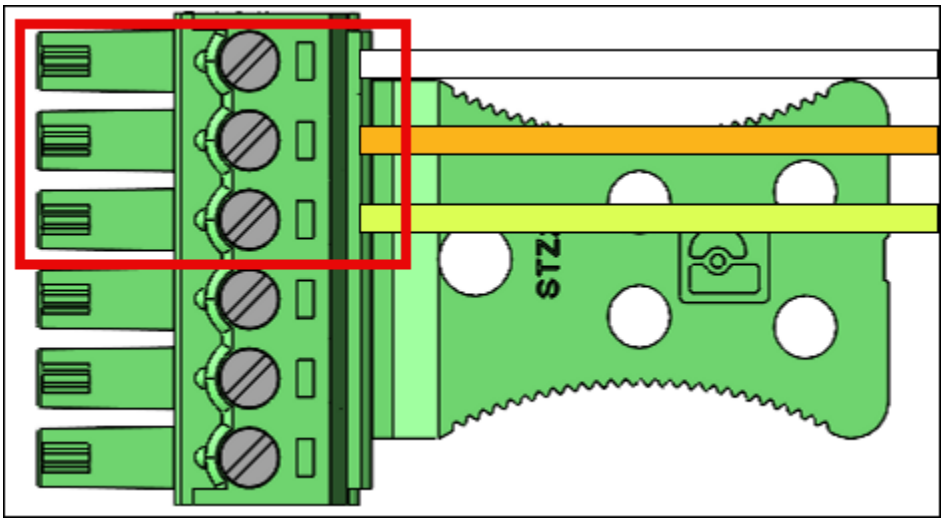


RS485佈線

Pin	連線	描述	使用	
10	RTN	信號返回	地面	
11	A	RS485時鐘	RS485同反相信號	
12	B	RS485_B/D0/數據	RS485反相信號	

繼電器連接

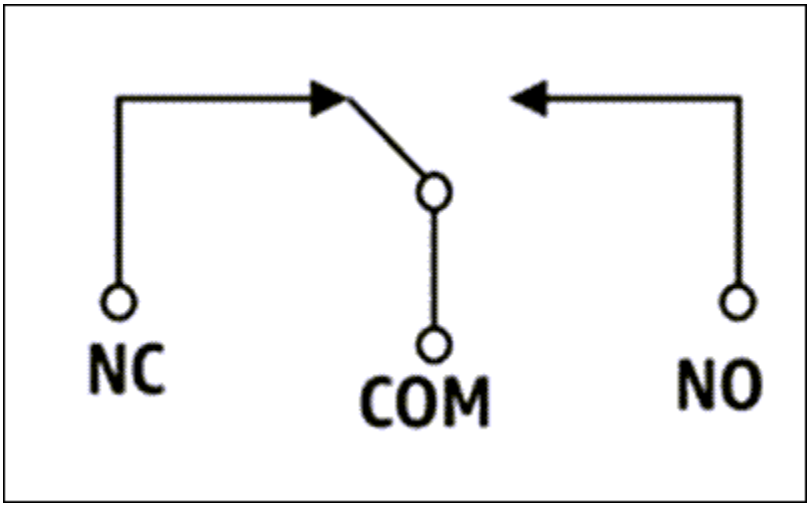
- 在接腳 7 (COM) 中插入白色電線。
- 在接腳 8 (NC) 中插入橘色線材。
- 在接腳 9 (NO) 中插入黃色線材。



繼電器配線

Pin	連線	描述	使用	
7	COM	繼電器常見	觸點繼電器通用 — 白線	

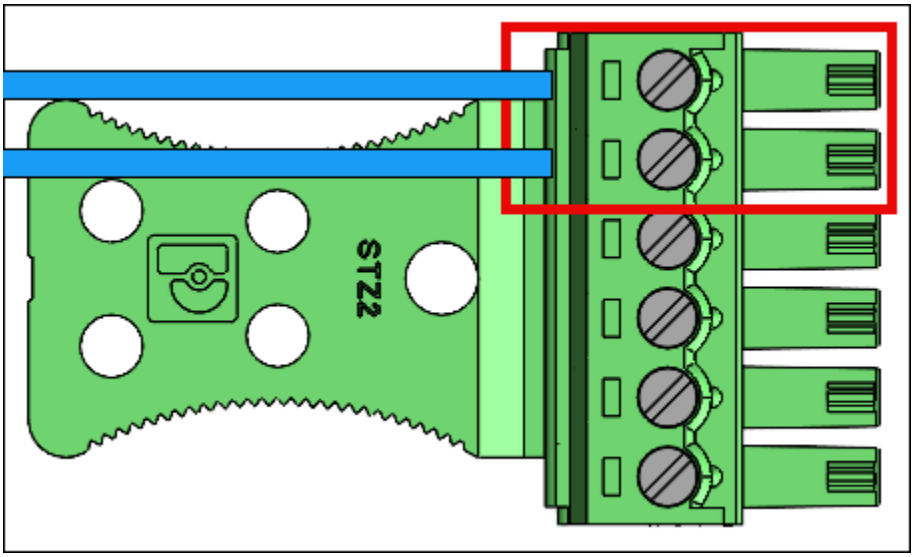
Pin	連線	描述	使用	
8	NC	繼電器，常閉	接點繼電器，常閉 — 橙色電線	
9	NO	繼電器常開	接點繼電器，常開 — 黃線	



繼電器應按照指定的安全額定值 30 VAC /60VDC, 60W Max 進行操作。

數字輸入/輸出連接

- 在接腳 1 (GPO) 中插入藍色線材。
- 在接腳 2 (GPI) 中插入藍色線材。



Pin	連線	描述	使用	
1	GPO	一般用途輸出	數字輸出信號 (5V)	
2	GPI	一般用途輸入	數位輸入訊號 (3.6V — 5V)	

- 數字輸入/輸出連接應按照列出的方式進行操作。

請參閱激活 Amazon 一個設備以激活您的 Amazon 一個設備。

安裝 Amazon One 裝置 I/O 集線器以安全存取

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

在開始安裝之前，請確保以下事項：

- Amazon 一個帶 I/O 集線器的設備僅供室內使用。
- 對於乙太網路供電 (PoE++)：

  請確定可使用 IEEE 802.3bt (類型 3) 類別 6 POE ++ 交換器 (端部跨度) 或注射器 (中跨度)，該交換器已列出或認證，並符合 62368-1。IEC

  只能使用具有核准 PoE++ 來源的 Amazon One 裝置。

PoE++ 的源代碼必須位於同一建築物內。

- 對於 15V 直流電源輸入，您只能使用列出或認證的 NEC Class 2 或功率受限、核准電源供應器的 Amazon One 裝置。請參閱下面的「可選 DC」部分。

所需工具：

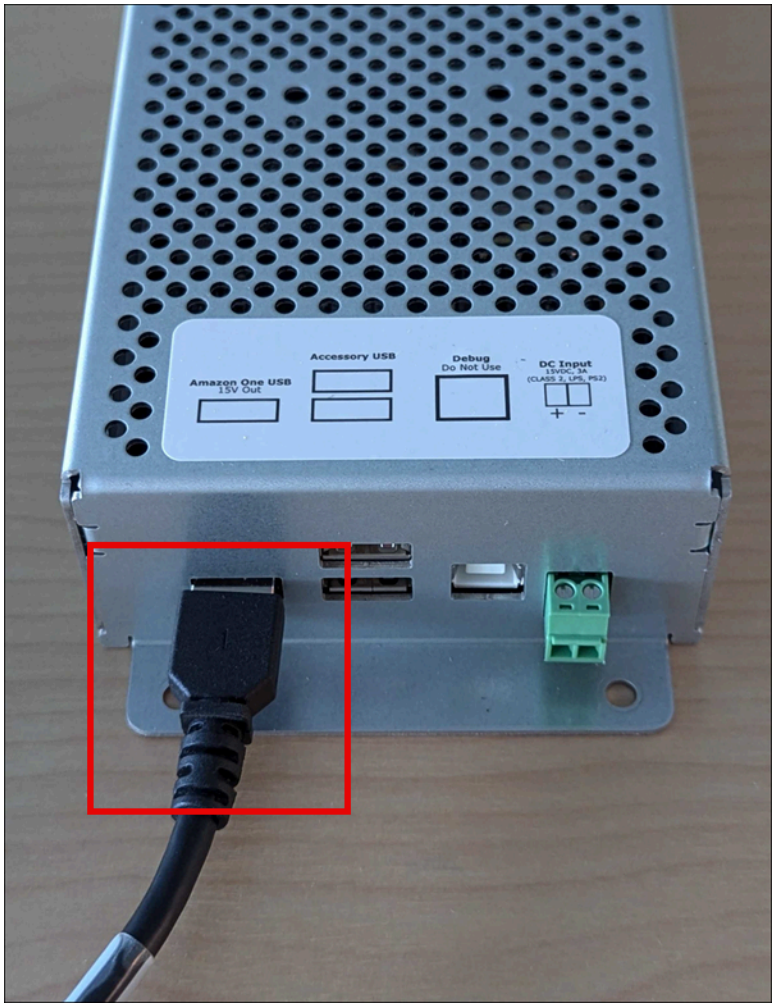
- 剝線鉗
- #2 十字螺絲起子
- 0.5 公釐 x 2 公釐平頭螺絲起子

隨附於具有 I/O 集線器的 Amazon One 設備中：

- 2x 6 位置端子台連接器
- 直流插頭連接器
- 72英寸電源/數據線

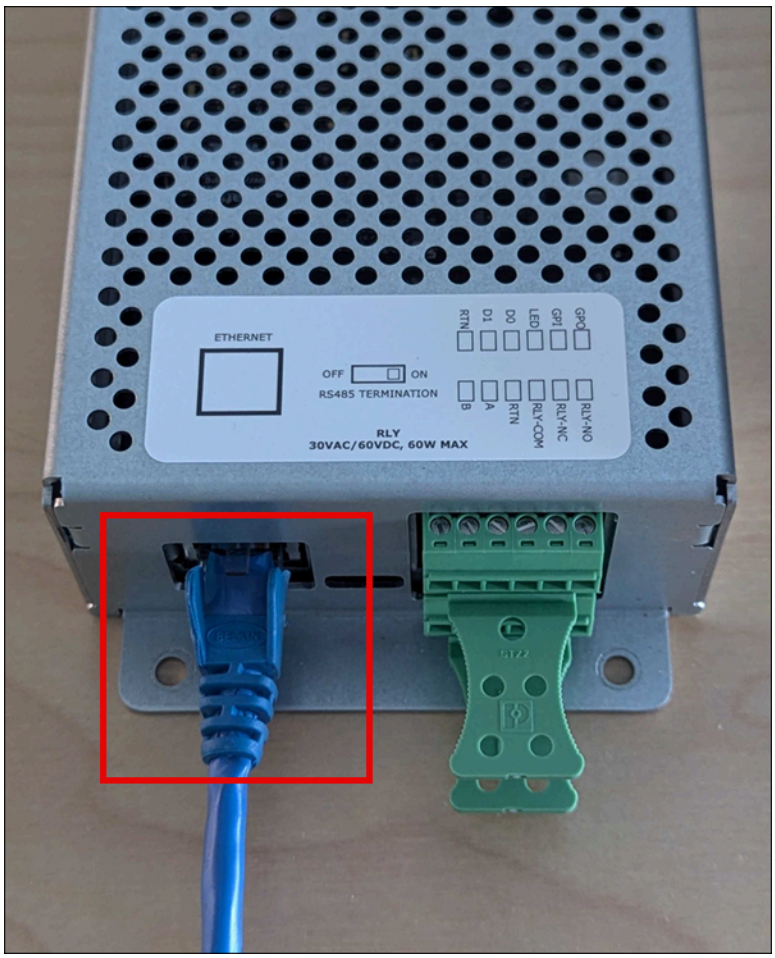
為您的 Amazon 一個設備安裝 I/O 集線器

1. 使用 I/O 集線器從包裝中取出您的 Amazon One 裝置。
2. 將 I/O 集線器固定在所需位置。
3. 將 Amazon One USB 電纜插入 I/O 集線器端口。



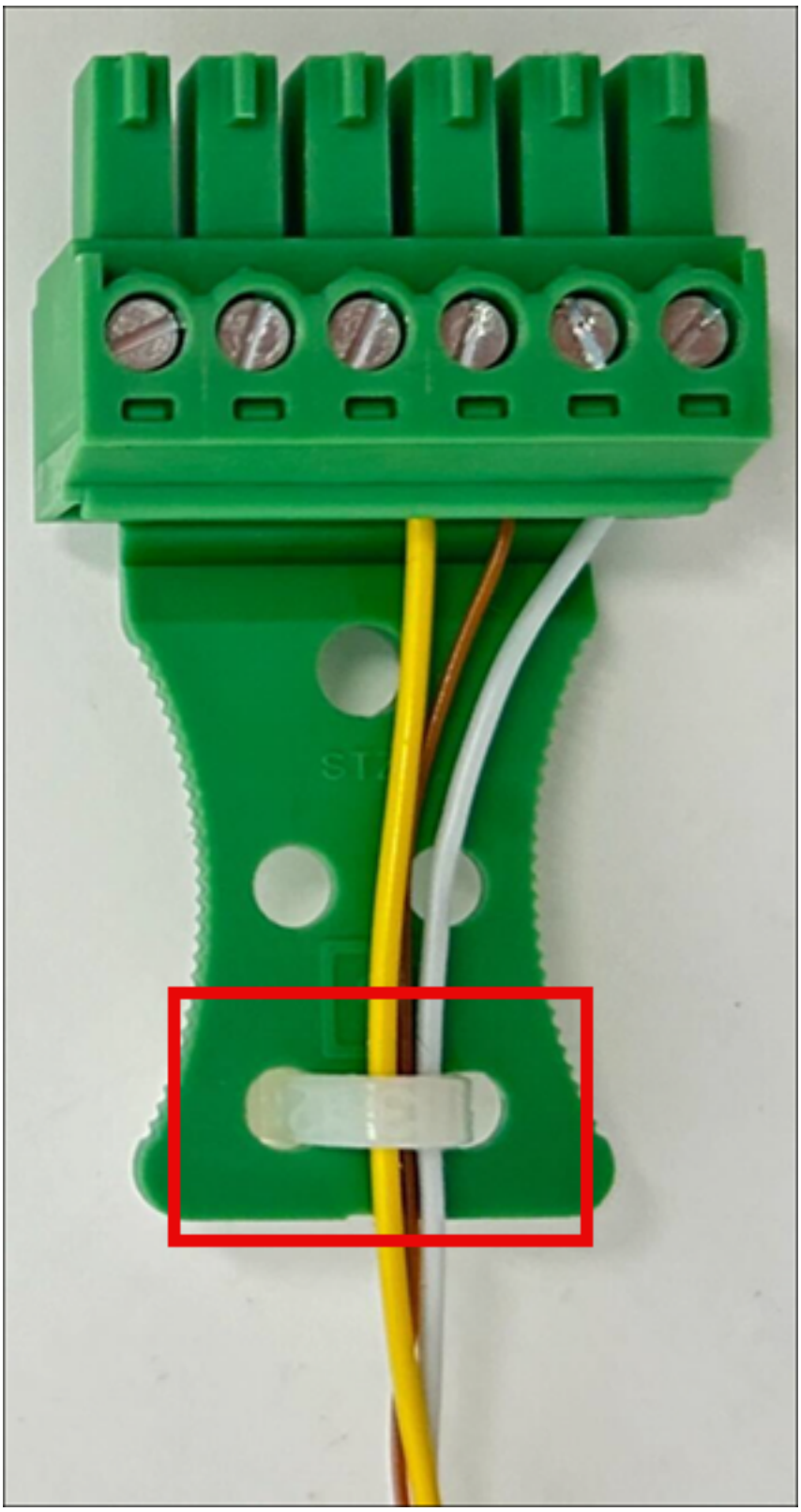
4. 對於 POE ++ 電源，請將以太網電纜從 POE ++ 源插入 I/O 集線器端口。

   可選：對於直流電源，請參閱下面的安裝 DC 接線部分。

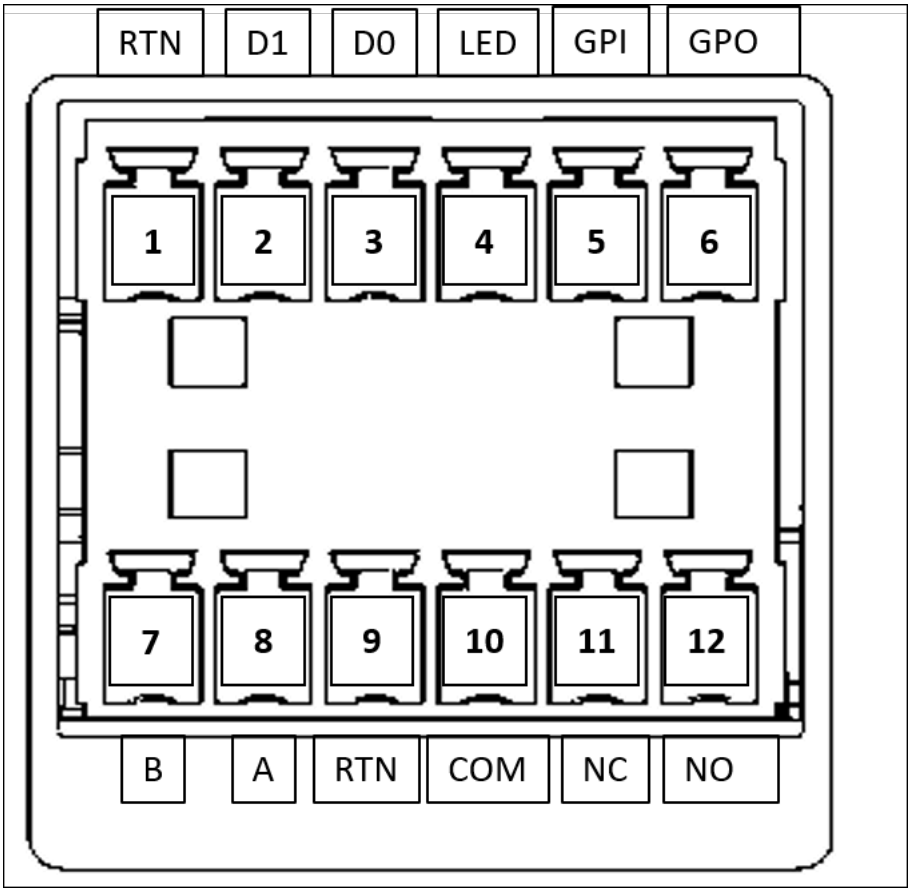


為您的 Amazon 一個設備連接 I/O 集線器

- 安裝滴水環，以避免液體意外地從電源線和 I/O 集線器中流入。
- 如以下影像所示，安裝應變夾鉗以保護電線免受損壞或應 stress。



1. 透過端子台插頭僅插入應用所需的配線。請參閱下面的佈線表格和圖表。
2. 將端子台插頭插入 I/O 集線器。

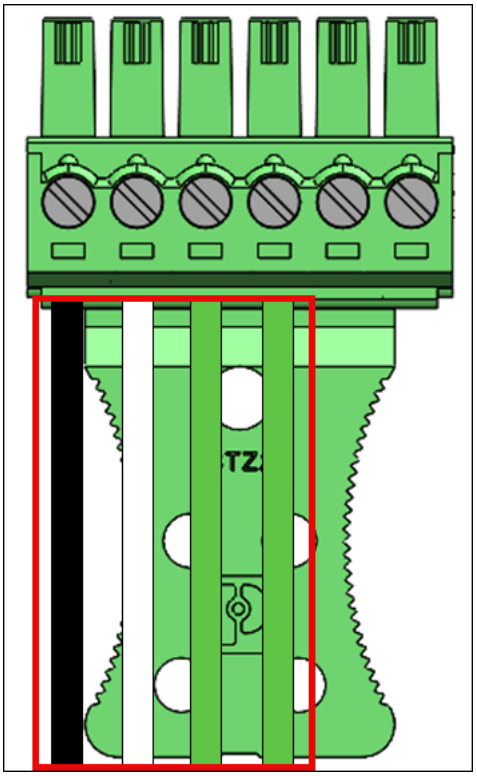


Pin	連線	描述	使用	
1	RTN	信號返回	韋根接地 — 黑線	
2	D1	韋根 D1	韋根資料 1 — 白線	
3	D0	韋根 D0	韋根資料 0 — 綠色電線	
4	LED	韋根 LED	韋根-可選 LED	
5	GPI	一般用途輸入	數字輸入信號 — 可選	
6	GPO	一般用途輸出	數字輸出信號-可選	

Pin	連線	描述	使用	
7	B	RS485_B/D0/數據	OSDPD0 — 綠色電線	
8	A	RS485時鐘	OSDPD1 — 白色電線	
9	RTN	信號返回	OSDP返回 — 黑線	
10	COM	繼電器通用	接點繼電器通用 — 白線	
11	NC	繼電器，常閉	接點繼電器，常閉 — 橙色電線	
12	NO	繼電器，常開	接點繼電器，常開 — 黃線	

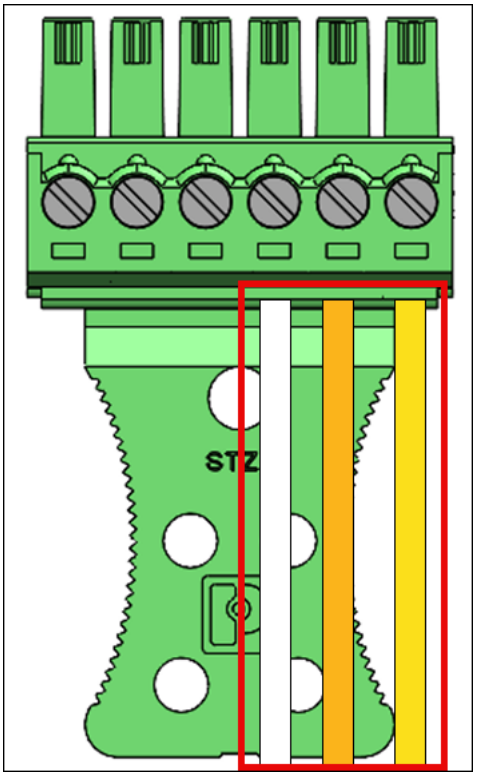
韦根连接

- 在接腳 1 (RTN) 中插入黑線。
- 在接腳 2 (D1) 中插入白色線材。
- 在接腳 3 (D0) 中插入綠色線材。
- 選用性：在接腳 4 (LED) 中插入綠色電線。

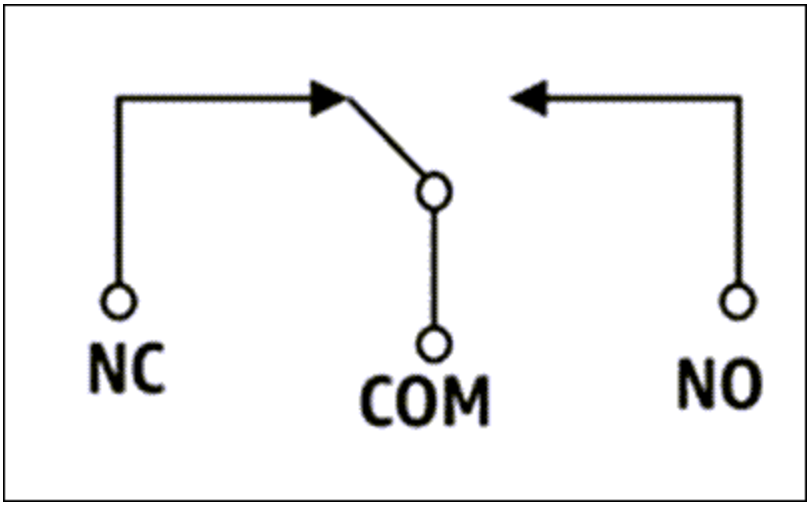


繼電器連接

- 在接腳 10 (COM) 中插入白色電線。
- 在接腳 11 (NC) 中插入橘色電線。
- 在接腳 12 (NO) 中插入黃色線材。



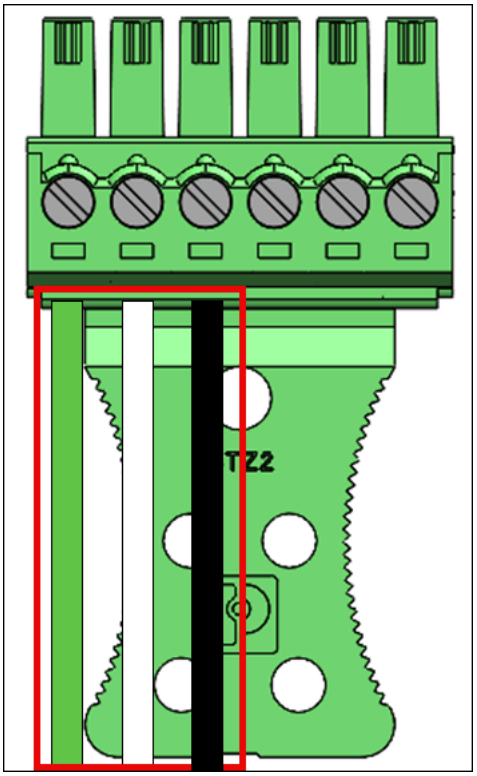
繼電器圖



繼電器應按照指定的安全額定值 30 VAC /60VDC, 60W Max 進行操作。

RS485連接

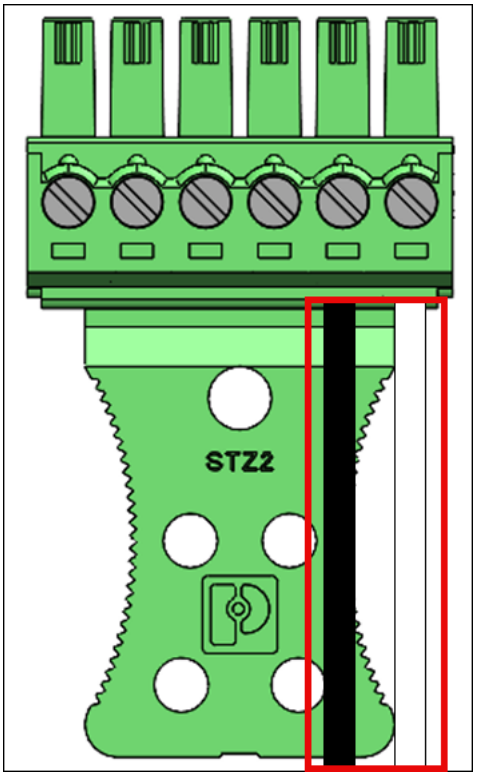
- 在接腳 7 (B) 中插入綠色電線。
- 在接腳 8 (A) 中插入白色電線。
- 在接腳 9 (RTN) 中插入黑線。



打開RS485終端開關「ON」，如果設備是線路上的最後一個單元。該開關激活 120 歐姆電阻終端在線上。

數字輸入/輸出連接

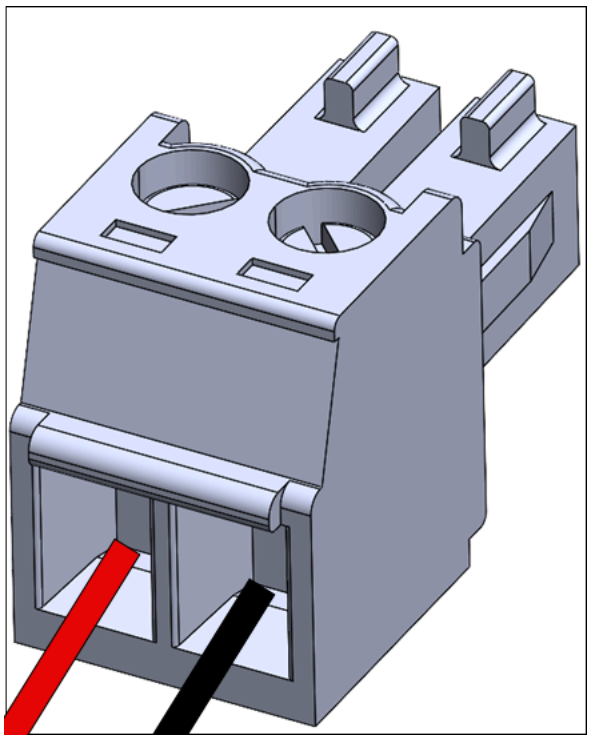
- 在接腳 5 (GPI) 中插入黑線。
- 在接腳 6 (GPO) 中插入白色電線。



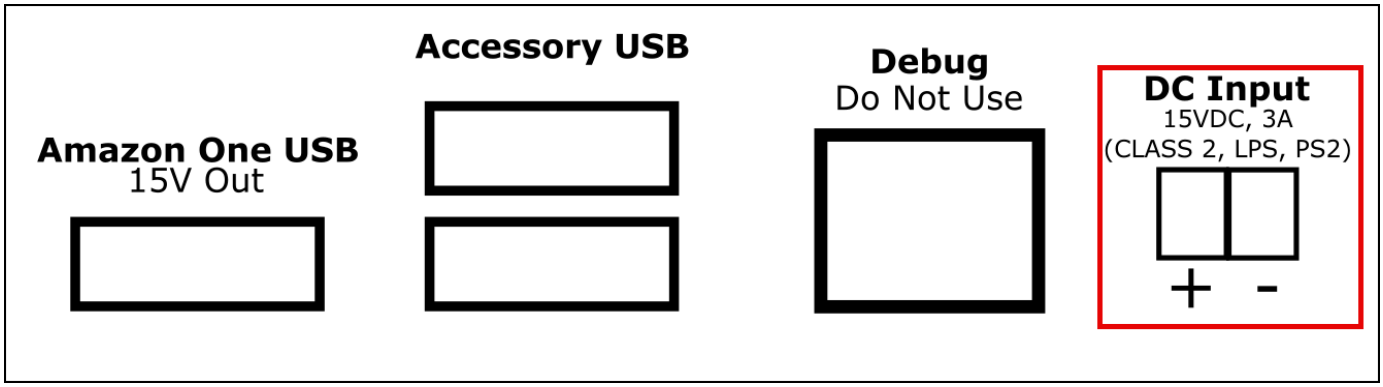
- 數字輸入/輸出連接應按照列出的方式進行操作。

可選：要安裝直流電線

1. 從紅線末端剝離 3mm-5mm 的正極（+），黑線用於負極（-）。
2. 將直流電線剝離的一端插入直流插頭。



3. 將電線擰入適當位置。
4. 將有線 DC 插頭插入直流輸入連接埠。



激活 Amazon 一個設備

當您的 Amazon One 裝置已安裝並開啟電源後，您就可以啟用它了。

激活您的 Amazon 一個設備

1. 在 Amazon One 設備上，點擊屏幕以開始使用。
2. 選擇以太網或 Wifi 連接到互聯網。

   一旦設備連接到互聯網，它將開始下載最新的軟件包。

3. 當屏幕顯示軟件下載完成時！」，選取「確定」。
4. 選擇二維碼。

   Amazon 一個設備屏幕將顯示掃描 QR 碼。
5. 若要擷取啟用二維碼，請在 https://console.aws.amazon.com/one 企業開啟 Amazon One 企業主控台。

   > **Note**
   >
   > 我們強烈建議您授予有限的權限給您的安裝程式，讓他們只能存取 Amazon One 企業主控台中的啟用 QR 碼。請參閱 步驟 2：添加 Amazon 一個企業用戶。
6. 在功能窗格中，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 [網站資訊] 下方，確認 [網站地址]。
9. 在「啟用 QR 碼」下，尋找您要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 一個設備掃描 QR 碼。
11. 當 Amazon One 設備屏幕顯示激活完成時！，裝置已準備就緒，可供使用。

報名及入學

現在您的 Amazon One 裝置已啟用，您的員工可以開始註冊手掌並驗證掌心以取得存取權限。

主題

- 使用者註冊
- 進入驗證

使用者註冊

在用戶可以驗證他們的手掌進入之前，他們將必須經過註冊過程。保安人員在允許用戶註冊之前，應始終檢查用戶的身份。

在 Amazon One 設備上註冊您的手掌

1. 在 Amazon One 企業註冊裝置上，按下開始使用。

2. 使用連接到 Amazon One 企業註冊裝置的徽章掃描器掃描員工徽章。

   成功掃描徽章後，Amazon One 裝置螢幕會顯示已掃描的徽章。
3. 請仔細閱讀使用條款，然後按 「確定」。
4. 閱讀同意-您的 Palm 生物識別信息，如果您同意，請按「我同意」。
5. 依照螢幕上的指示完成註冊程序。

進入驗證

成功註冊掌心後，您就可以在 Amazon One 企業入門裝置上使用掌心進行身份驗證。

在 Amazon One 設備上驗證您的手掌進入

- 將手掌懸停在裝置上方，然後依照螢幕上的指示掃描手掌。

註冊使用者管理

您可以使用「已註冊的使用者管理」頁面來追蹤已註冊的使用者，並刪除使用者生物識別技術。刪除相關生物特徵識別的使用者將無法再存取 Amazon One 裝置進行身份驗證。

若要檢視註冊使用者

1. 在 https://console.aws.amazon.com/一個企業打開 Amazon 一個企業控制台。
2. 在功能窗格中，選擇 [已註冊的使用者管理]。
3. 在 [已註冊的使用者] 底下，您會找到所有已註冊使用者和下列詳細資訊：

   - 徽章 ID — 註冊時由徽RFID章讀取器擷取的徽章識別碼資訊。
   - 註冊來源 — 用於註冊的 Amazon One 裝置的詳細資訊。
   - 報名日期 — 註冊日期和時間。

若要刪除已註冊使用者及其生物特徵識別

1. 在 https://console.aws.amazon.com/一個企業打開 Amazon 一個企業控制台。
2. 在功能窗格中，選擇 [已註冊的使用者管理]。
3. 在「已註冊的使用者」下，選取您要刪除其掌上生物特徵識別資料之使用者的徽章 ID。
4. 選擇刪除生物識別。

5. 選擇刪除以確認刪除使用者生物特徵識別資料。

> **Important**
>
> 此動作會導致從 Amazon One 企業永久刪除使用者的掌心生物特徵識別。使用者必須使用 Amazon One 企業註冊裝置再次註冊，才能使用 Amazon One 企業進行身份驗證。刪除使用者的生物特徵辨識也會永久刪除 Amazon One 企業版中的其他設定檔屬性，例如徽章 ID。

設備管理

安裝並啟用 Amazon One 裝置之後，就會開始在 Amazon One 企業主控台上報告裝置運作狀態。您可以使用 Amazon One 企業主控台執行裝置管理任務，例如重新啟動裝置或更新組態。

主題

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。

若要變更網站名稱

1. 在 https://console.aws.amazon.com/一個企業打開 Amazon 一個企業控制台。
2. 在導覽窗格中，選擇 [網站]。
3. 在「工址」下，選取要編輯其名稱的站台。
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. 選擇儲存變更以進行更新。

若要更新站台位址

1. 在 https://console.aws.amazon.com/一個企業打開 Amazon 一個企業控制台。

2. 在導覽窗格中，選擇 [網站]。
3. 在「站台」下，選取您要更新地址的站台。
4. 在 [裝置執行個體] 下，確定啟動的執行個體數目為 0。
5. (選擇性) 如果啟動的執行個體數目不是 0，請參閱 停用裝置執行個體
6. 選擇編輯。
7. 在 [實體位址] 下，輸入正確的實體位址。
8. 選擇儲存變更以進行更新。

設備實例管理

設備實例是具有配置的設備的邏輯表示。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) 以及一組通訊設定。

檢視裝置執行個體狀態

1. 在 https://console.aws.amazon.com/一個企業打開 Amazon 一個企業控制台。
2. 在瀏覽窗格中，選擇 [裝置執行個體]。
3. 在啟用的執行個體下，您會看到已啟用 Amazon One 裝置的清單。
4. 選擇設備實例名稱以查看設備實例詳細信息。

要重新啟動 Amazon 一個設備

1. 在 https://console.aws.amazon.com/一個企業打開 Amazon 一個企業控制台。
2. 在瀏覽窗格中，選擇 [裝置執行個體]。
3. 在 [已啟動的執行個體] 下方，選擇您要重新開機之裝置的執行個體名稱。
4. 選擇重新啟動以重新啟動 Amazon One 裝置。

若要更新 Amazon 單一裝置組態

1. 在 https://console.aws.amazon.com/一個企業打開 Amazon 一個企業控制台。
2. 在瀏覽窗格中，選擇 [裝置執行個體]。
3. 在「已啟動的執行個體」下，選擇您要更新之裝置的執行個體名稱。

4. 在 [裝置設定] 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 (請參閱步驟 6：設定要啟用的裝置執行個體)。然後，您可以完成設備激活過程（請參閱激活 Amazon 一個設備）。

5. 完成所需的變更後，請選擇 [更新裝置組態] 以確認更新。

若要更新無線上網憑

1. 在 https://console.aws.amazon.com/一個企業打開 Amazon 一個企業控制台。
2. 在瀏覽窗格中，選擇 [裝置執行個體]。
3. 在「已啟動的執行個體」下，選擇您要更新之裝置的執行個體名稱。
4. 在 [網路] 下選擇 [編輯]。
5. 在 Wi-Fi 設定下，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

1. 在 https://console.aws.amazon.com/一個企業打開 Amazon 一個企業控制台。
2. 在瀏覽窗格中，選擇 [裝置執行個體]。
3. 在「已啟動的執行個體」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」。

Amazon 一家企業中的安全

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，這些架構是為了滿足對安全性最敏感的組織的需求而建置的。

安全是 AWS 與您之間共同承擔的責任。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：

- 雲端安全性 — AWS 負責保護中執行 AWS 服務的基礎架構 AWS 雲端。 AWS 還為您提供可以安全使用的服務。若要了解適用於 Amazon One Enterprise 的合規計劃，請參閱合規計劃AWS 服務範圍內的合規計劃AWS的服務。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 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 企業版時套用共同的責任模型。下列主題說明如何設定 Amazon One 企業版，以符合您的安全性和合規目標。您也會學到如何使用其他可 AWS 協助您監控和保護 Amazon One 企業資源的服務。

主題

- Amazon 一家企業中的數據保護
- Amazon 一家企業的身份和訪問管理
- 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 一家企業中的數據保護

所以此 AWS 共同責任模型適用於 Amazon One 企業版的資料保護。如本模型所述， AWS 負責保護運行所有的全球基礎設施 AWS 雲端。 您有責任維持對託管在此基礎結構上的內容的控制權。您也必須負責安全性設定與管理工作 AWS 服務 你使用. 如需有關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 共同責任模型和GDPR博客文章 AWS 安全部落格。

出於數據保護目的，我們建議您進行保護 AWS 帳戶 憑據並設置個別用戶 AWS IAM Identity Center 或 AWS Identity and Access Management (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與之溝通 AWS 的費用。我們需要 TLS 1.2 並推薦 TLS 1.3。
- 設定API和使用者活動記錄 AWS CloudTrail。 如需使用 CloudTrail 軌跡進行擷取的相關資訊 AWS 活動，請參閱使用 CloudTrail 系統線 AWS CloudTrail 用戶指南。
- 使用 AWS 加密解決方案，以及其中的所有默認安全控制 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。
- 如果您在訪問時需要 FIPS 140-3 驗證的加密模塊 AWS 透過指令行介面或API使用FIPS端點。如需有關可用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。這包括當你與 Amazon 一個企業或其他工作 AWS 服務 使用控制台API， AWS CLI，或 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。如果您提供URL給外部伺服器，我們強烈建議您不要在中包含認證資訊，URL以驗證您對該伺服器的要求。

若要使用靜態資料的預設加密

Amazon One 企業版預設提供加密功能，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來自動加密機密的最終使用者資料。您無法檢視、管理或使用AWS擁有的金鑰，也無法稽核其使用情況。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，請參閱金AWS鑰管理服務開發人員指南中的AWS擁有金鑰。

加密傳輸中的資料

Amazon One 企業版使用傳輸層安全性 (TLS) 來保護資料，而簽名版本 4 則用於驗證對AWS服務的所有輸入API請求。此加密預設為啟用。

Amazon 一家企業的身份和訪問管理

AWS Identity and Access Management (IAM) 是一個 AWS 服務 可協助系統管理員安全地控制存取 AWS 的費用。IAM管理員控制誰可以驗證 (登入) 和授權 (有權限) 使用 Amazon One 企業資源。IAM是一個 AWS 服務 您可以使用，無需額外費用。

主題

- 物件

- 使用身分驗證
- 使用政策管理存取權
- Amazon 一個企業如何與 IAM
- Amazon 一個企業版的基於身份的政策示例
- AWS Amazon 一家企業的受管政策
- 疑難排解 Amazon One 企業身分識別和存取

物件

您如何使用 AWS Identity and Access Management （IAM）會有所不同，具體取決於您在 Amazon One 企業中所做的工作。

服務使用者 — 如果您使用 Amazon One 企業版服務執行工作，則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 企業版功能完成工作時，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。如果您無法在 Amazon One 企業版中存取某項功能，請參閱疑難排解 Amazon One 企業身分識別和存取。

服務管理員 — 如果您負責公司的 Amazon One 企業資源，您可能擁有完整的 Amazon One 企業版存取權。您的任務是確定服務使用者應存取哪些 Amazon One 企業版功能和資源。然後，您必須向IAM管理員提交請求，才能變更服務使用者的權限。檢閱此頁面上的資訊，以瞭解的基本概念IAM。若要進一步了解貴公司如何IAM搭配 Amazon One 企業版使用，請參閱Amazon 一個企業如何與 IAM。

IAM管理員 — 如果您是管理IAM員，您可能想要了解如何撰寫政策以管理 Amazon One 企業版存取權的詳細資訊。若要檢視您可以在中使用的 Amazon One 企業身分型政策範例IAM，請參閱。Amazon 一個企業版的基於身份的政策示例

使用身分驗證

驗證是您登入的方式 AWS 使用您的身份證明。您必須經過驗證 (登入 AWS) 作為 AWS 帳戶根使用者，以IAM使用者身分或假定IAM角色。

您可以登入 AWS 使用透過身分識別來源提供的認證做為聯合身分識別。 AWS IAM Identity Center (IAM身分識別中心) 使用者、貴公司的單一登入驗證，以及您的 Google 或 Facebook 認證都是聯合身分識別的範例。當您以同盟身分登入時，您的管理員先前會使用IAM角色設定聯合身分識別。當您存取 AWS 通過使用聯合，您間接擔任一個角色。

根據您的使用者類型，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，請參閱如何登入 AWS 帳戶 中的 AWS 登入 使用者指南。

如果您訪問 AWS 編程方式， AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以密碼編譯方式簽署您的要求。如果你不使用 AWS 工具，您必須自己簽署請求。如需使用建議的方法自行簽署要求的詳細資訊，請參閱簽署 AWS API《IAM用戶指南》中的請求。

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驗證 (MFA) 來增加帳戶的安全性。要了解更多信息，請參閱中的多因素身份驗證 AWS IAM Identity Center 用戶指南和使用多因素身份驗證（MFA）AWS (在 IAM 使用者指南中)

AWS 帳戶 根使用者

當你創建一個 AWS 帳戶時，您會從一個擁有完整存取權限的登入身分開始 AWS 服務 和帳戶中的資源。這個身份被稱為 AWS 帳戶 root 使用者，並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。如需需要您以 root 使用者身分登入的完整工作清單，請參閱《使用指南》中的〈需要 root 使用者認證的IAM工作〉。

聯合身分

最佳作法是要求人類使用者 (包括需要管理員存取權的使用者) 使用與身分識別提供者的同盟來存取 AWS 服務 通過使用臨時憑據。

聯合身分是來自您企業使用者目錄的使用者、Web 身分識別提供者、 AWS Directory Service、身分識別中心目錄或存取的任何使用者 AWS 服務 使用透過身分識別來源提供的認證。同盟身分存取時 AWS 帳戶，他們假定角色，並且角色提供臨時認證。

對於集中式存取管理，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，也可以連線並同步至您自己身分識別來源中的一組使用者和群組，以便在您的所有身分識別來源中使用 AWS 帳戶 和應用程序。如需IAM身分識別中心的相關資訊，請參閱IAM識別中心是什麼？ 在 AWS IAM Identity Center 使用者指南。

IAM 使用者和群組

用IAM戶是您的身份 AWS 帳戶 具有單一人員或應用程式的特定權限。在可能的情況下，我們建議您仰賴臨時登入資料，而不要建立具有長期認證 (例如密碼和存取金鑰) 的IAM使用者。不過，如果您的特定使用案例需要使用IAM者的長期認證，建議您輪換存取金鑰。如需詳細資訊，請參閱《使用指南》中的「IAM定期輪換存取金鑰」以瞭解需要長期認證的使用案例。

IAM群組是指定IAM使用者集合的身分識別。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的群組，IAMAdmins並授與該群組管理IAM資源的權限。

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。要了解更多信息，請參閱《IAM用戶指南》中的創建用戶（而不是角色）的IAM時間。

IAM角色

IAM角色是您的身份 AWS 帳戶 具有特定權限。它類似於用IAM戶，但不與特定人員相關聯。您可以暫時IAM擔任 AWS Management Console 通過切換角色。您可以通過調用一個角色 AWS CLI 或 AWS API操作或通過使用自定義URL。如需有關使用角色方法的詳細資訊，請參閱《使用指南》中的IAM〈使用IAM角色〉。

IAM具有臨時認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《使用指南》中的〈建立第三方身分識別提供IAM者的角色〉。如果您使用IAM身分識別中心，則需要設定權限集。為了控制身分驗證後可以存取的內IAM容，IAMIdentity Center 會將權限集與中的角色相關聯。如需有關權限集的資訊，請參閱 AWS IAM Identity Center 使用者指南。
- 暫時IAM使用者權限 — IAM 使用者或角色可以假定某個IAM角色，暫時取得特定工作的不同權限。
- 跨帳戶存取 — 您可以使用IAM角色允許不同帳戶中的某個人 (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。但是，有一些 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要瞭解跨帳戶存取角色與以資源為基礎的政策之間的差異，請參閱《IAM使用指南》IAM中的〈跨帳號資源存取〉。
- 跨服務訪問 — 一些 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或將物件存放在 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。
  - 轉寄存取工作階段 (FAS) — 當您使用使用IAM者或角色在 AWS，您被視為校長。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使用主體呼叫 AWS 服務，與請求相結合 AWS 服務 向下游服務提出請求。FAS只有當服務收到需要與其他人互動的請求時才會發出請求 AWS 服務 或要完成的資源。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。
  - 服務角色 — 服務角色是指服務代表您執行動作所代表的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱建立角色以將權限委派給 AWS 服務 (在 IAM 使用者指南中)
  - 服務連結角色 — 服務連結角色是連結至 AWS 服務。 服務可以扮演角色代表您執行動作。服務連結角色會出現在 AWS 帳戶 並由服務擁有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。

- 在 Amazon 上執行的應用程式 EC2 — 您可以使用IAM角色來管理在執行個體上EC2執行並製作的應用程式的臨時登入資料 AWS CLI 或 AWS API請求。這比在EC2實例中存儲訪問密鑰更好。若要指派 AWS EC2執行個體的角色並讓它可供其所有應用程式使用，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，可讓執行個體上EC2執行的程式取得臨時登入資料。如需詳細資訊，請參閱使用者指南中的使用IAM角色將許可授與在 Amazon EC2 執行個體上執行的應IAM用程式。

要了解是否使用IAM角色還是用IAM戶，請參閱《用戶指南》中的「IAM創建IAM角色的時機（而不是用戶）」。

使用政策管理存取權

您可以控制存取 AWS 藉由建立原則並將其附加至 AWS 身分識別或資源。原則是中的物件 AWS 當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數策略都儲存在 AWS 作為JSON文件。如需有關JSON原則文件結構和內容的詳細資訊，請參閱《IAM使用指南》中的策略概觀。JSON

管理員可以使用 AWS JSON策略，用於指定誰可以存取什麼內容。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。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

IAM原則會定義動作的權限，不論您用來執行作業的方法為何。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該策略的使用者可以從 AWS Management Console，該 AWS CLI，或 AWS API.

身分型政策

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。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。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

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。受管理的策略是獨立策略，您可以將其附加到您的多個使用者、群組和角色 AWS 帳戶。 受管政策包括 AWS 受管理的政策和客戶管理的政策。若要了解如何在受管策略或內嵌策略之間進行選擇，請參閱《IAM使用手冊》中的「在受管策略和內嵌策略之間進行選擇」。

資源型政策

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括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。主參與者可以包括帳戶、使用者、角色、同盟使用者或 AWS 服務.

資源型政策是位於該服務中的內嵌政策。你不能使用 AWS 在以資源為基礎的策略IAM中受管理的策略。

存取控制清單 (ACLs)

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

Amazon S3， AWS WAF和 Amazon VPC 是支持的服務的例子ACLs。若要進一步了解ACLs，請參閱 Amazon 簡單儲存服務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原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 權限界限 — 權限界限是一項進階功能，您可以在其中設定以身分識別為基礎的原則可授與給IAM實體 (IAM使用者或角色) 的最大權限。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。如需有關權限界限的詳細資訊，請參閱《IAM使用指南》中的IAM實體的權限界限。
- 服務控制策略（SCPs）— SCPs 是指定中組織或組織單位（OU）的最大權限的JSON策略 AWS Organizations. AWS Organizations 是一種用於分組和集中管理多個服務 AWS 帳戶 您的企業擁有。如果您啟用組織中的所有功能，則可以將服務控制策略 (SCPs) 套用至您的任何或所有帳戶。SCP限制成員帳戶中實體的權限，包括每個帳戶 AWS 帳戶根使用者。 如需有關 Organizations 的詳細資訊 SCPs，請參閱 AWS Organizations 使用者指南。
- 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使用指南》中的工作階段原則。

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。若要瞭解如何 AWS 決定當涉及多個原則類型時是否允許要求，請參閱《IAM使用指南》中的「原則評估邏輯」。

Amazon 一個企業如何與 IAM

在您用IAM來管理 Amazon One 企業版的存取權限之前，請先了解哪些IAM功能可用於 Amazon One 企業版。

IAM您可以使用 Amazon 一個企業版的功能

IAM特徵	Amazon 一個企業支持
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(策略中的標籤)	是
暫時性憑證	是
主體許可	是
服務角色	否
服務連結角色	否

為了獲得如何 Amazon 一個企業和其他的高層次視圖 AWS 服務適用於大多數IAM功能，請參閱 AWS《IAM使用者指南》IAM中使用的服務。

Amazon 一個企業版的基於身份的政策

支援身分型政策：是

以身分識別為基礎的原則是您可以附加至身分識別 (例如使用者、使用IAM者群組或角色) 的JSON權限原則文件。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。若要瞭解如何建立以身分識別為基礎的策略，請參閱《IAM使用指南》中的〈建立IAM策略〉。

使用以IAM身分識別為基礎的策略，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。若要瞭解可在JSON策略中使用的所有元素，請參閱《使用IAM者指南》中的IAMJSON策略元素參考資料。

Amazon 一個企業版的基於身份的政策示例

若要檢視 Amazon One 企業版以身分識別為基礎的政策範例，請參閱。Amazon 一個企業版的基於身份的政策示例

Amazon 一家企業內基於資源的政策

支援資源型政策：否

以資源為基礎的JSON策略是您附加至資源的政策文件。以資源為基礎的政策範例包括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。主參與者可以包括帳戶、使用者、角色、同盟使用者或 AWS 服務.

若要啟用跨帳戶存取，您可以在以資源為基礎的策略中指定一個或多個帳戶中的一個或多個帳戶中的IAM實體作為主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主參與者與資源不同時 AWS 帳戶，受信任帳戶中的IAM管理員也必須授與主參與者實體 (使用者或角色) 存取資源的權限。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使用指南》IAM中的〈跨帳號資源存取〉。

Amazon 一個企業的政策行動

支援政策動作：是

管理員可以使用 AWS JSON策略，用於指定誰可以存取什麼內容。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策略Action元素描述了您可以用來允許或拒絕策略中存取的動作。策略動作通常與關聯的名稱相同 AWS API操作。有一些例外情況，例如沒有匹配API操作的僅限權限的操作。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 企業版動作清單，請參閱Amazon One Enterprise 的動作、資源與條件索引鍵。

Amazon One 企業版中的政策動作會在動作前使用下列前置詞：

```
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 企業版以身分識別為基礎的政策範例，請參閱。Amazon 一個企業版的基於身份的政策示例

Amazon 一家企業的政策資源

支援政策資源：是

管理員可以使用 AWS JSON策略，用於指定誰可以存取什麼內容。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。

ResourceJSON原則元素會指定要套用動作的一或多個物件。陳述式必須包含 Resource 或 NotResource 元素。最佳做法是使用其 Amazon 資源名稱 (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 資源類型及其類型的清單ARNs，並了解可以使用哪些動作指定每ARN個資源，請參閱Amazon One Enterprise 的動作、資源與條件索引鍵。

若要檢視 Amazon One 企業版以身分識別為基礎的政策範例，請參閱。Amazon 一個企業版的基於身份的政策示例

Amazon 一個企業的政策條件密鑰

支援服務特定政策條件金鑰：是

管理員可以使用 AWS JSON策略，用於指定誰可以存取什麼內容。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。

如果您在一個語句中指定多個Condition元素，或在單個Condition元素中指定多個鍵， AWS 使用邏輯AND運算來評估它們。如果您為單個條件鍵指定多個值， AWS 使用邏輯OR運算評估條件。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使用者名稱標記資源時，您才可以授與IAM使用者存取資源的權限。如需詳細資訊，請參閱《IAM使用指南》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條件金鑰。若要查看全部 AWS 全域條件索引鍵，請參閱 AWS《IAM使用指南》中的整體條件前後關聯鍵字。

若要查看 Amazon One 企業條件金鑰清單，以及瞭解哪些動作和資源可以搭配使用條件金鑰，請參閱Amazon One Enterprise 的動作、資源與條件索引鍵。

若要檢視 Amazon One 企業版以身分識別為基礎的政策範例，請參閱。Amazon 一個企業版的基於身份的政策示例

ACLs在 Amazon 一家企業

支持ACLs：無

存取控制清單 (ACLs) 控制哪些主參與者 (帳戶成員、使用者或角色) 具有存取資源的權限。ACLs類似於以資源為基礎的策略，雖然它們不使用JSON政策文件格式。

ABAC與 Amazon 一家企業

支援 ABAC (策略中的標籤): 是

以屬性為基礎的存取控制 (ABAC) 是一種授權策略，可根據屬性定義權限。In (入) AWS，這些屬性稱為標籤。您可以將標籤附加到IAM實體 (使用者或角色) 以及許多實體 AWS 的費用。標記實體和資源是的第一步ABAC。然後，您可以設計ABAC策略，以便在主參與者的標籤符合他們嘗試存取的資源上的標籤時允許作業。

ABAC在快速成長的環境中很有幫助，並且有助於原則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。

如需有關的詳細資訊ABAC，請參閱什麼是ABAC？ 在《IAM使用者指南》中。若要檢視包含設定步驟的自學課程ABAC，請參閱《使用指南》中的〈使用以屬性為基礎的存取控制 (ABAC) IAM 〉。

在 Amazon 一個企業中使用臨時登入

支援臨時憑證：是

一些 AWS 服務 使用臨時憑據登錄時不起作用。有關其他信息，包括 AWS 服務 使用臨時登入資料，請參閱 AWS 服務 在《IAM使用者指南》IAM中使用。

如果您登入，您正在使用臨時認證 AWS Management Console 使用除了使用者名稱和密碼之外的任何方法。例如，當您訪問 AWS 使用貴公司的單一登入 (SSO) 連結，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。如需有關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)〉。

您可以使用手動建立臨時認證 AWS CLI 或 AWS API。然後，您可以使用這些臨時登入資料來存取 AWS. AWS 建議您動態產生臨時登入資料，而非使用長期存取金鑰。如需詳細資訊，請參閱IAM。

Amazon 一家企業的跨服務主體許可

支援轉寄存取工作階段 (FAS)：是

當您使用使用IAM者或角色執行動作 AWS，您被視為校長。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使用主體呼叫 AWS 服務，與請求相結合 AWS 服務 向下

游服務提出請求。FAS只有當服務收到需要與其他人互動的請求時才會發出請求 AWS 服務 或要完成的資源。在此情況下，您必須具有執行這兩個動作的許可。有關提出FAS請求時的策略詳細信息，請參閱轉發訪問會話。

Amazon 單一企業版的服務角色

支援服務角色：否

服務角色是服務假定代表您執行動作的IAM角色。IAM管理員可以從中建立、修改和刪除服務角色IAM。如需詳細資訊，請參閱建立角色以將權限委派給 AWS 服務 (在 IAM 使用者指南中)

> **Warning**
>
> 變更服務角色的許可可可可可能會中斷 Amazon One 企業版功能。只有在 Amazon One 企業版提供指導時才編輯服務角色。

Amazon 一家企業版的服務連結角色

支援服務連結角色：否

服務連結角色是連結至服務角色的一種類型 AWS 服務。 服務可以扮演角色代表您執行動作。服務連結角色會出現在 AWS 帳戶 並由服務擁有。IAM管理員可以檢視 (但無法編輯服務連結角色) 的權限。

如需建立或管理服務連結角色的詳細資訊，請參閱 AWS 與之合作的服務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 一個企業版的基於身份的政策示例

依預設，使用者和角色沒有建立或修改 Amazon One 企業資源的權限。他們也無法執行任務使用 AWS Management Console, AWS Command Line Interface (AWS CLI)，或 AWS API。若要授與使用者對所需資源執行動作的權限，IAM管理員可以建立IAM策略。然後，系統管理員可以將IAM原則新增至角色，使用者可以擔任這些角色。

若要瞭解如何使用這些範例原則文件來建立以IAM身分識別為基礎的JSON策略，請參閱使用指南中的IAM建立IAM策略。

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。ARNs

主題

政策最佳實務

以身分識別為基礎的政策決定某人是否可以在您的帳戶中建立、存取或刪除 Amazon One 企業資源。這些動作可能會為您帶來成本 AWS 帳戶。 建立或編輯以身分識別為基礎的原則時，請遵循下列準則和建議：

- 開始使用 AWS 受管原則並朝著最低權限權限移轉 — 若要開始授與使用者和工作負載的權限，請使用 AWS 授與許多常見使用案例權限的受管理策略。他們是可用的 AWS 帳戶。 建議您透過定義進一步減少權限 AWS 針對您的使用案例特定的客戶管理政策。如需詳細資訊，請參閱 AWS 受管理的策略或 AWS 《使用者指南》中針對工作職能的IAM管理策略。
- 套用最低權限權限 — 當您使用原則設定權限時，IAM只授與執行工作所需的權限。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。如需有關使用套用權限IAM的詳細資訊，請參閱《使用指南》IAM中的IAM《策略與權限》。
- 使用IAM策略中的條件進一步限制存取 — 您可以在策略中新增條件，以限制對動作和資源的存取。例如，您可以撰寫政策條件，以指定必須使用傳送所有要求SSL。如果服務動作是透過特定使用條件，您也可以使用條件來授與對服務動作的存取權 AWS 服務，例如， AWS CloudFormation。 如需詳細資訊，請參閱《IAM使用指南》中的IAMJSON策略元素：條件。
- 使用 IAM Access Analyzer 驗證您的原IAM則，以確保安全和功能性的權限 — IAM Access Analyzer會驗證新的和現有的原則，以便原則遵循IAM原則語言 (JSON) 和IAM最佳做法。IAMAccess Analyzer 提供超過 100 項原則檢查和可行的建議，協助您撰寫安全且功能正常的原則。如需詳細資訊，請參閱IAM使IAM用指南中的存取分析器原則驗證。
- 需要多重要素驗證 (MFA) — 如果您的案例需要使IAM用者或 root 使用者 AWS 帳戶，請開啟MFA以獲得額外的安全性。若要在呼叫API作業MFA時需要，請在原則中新增MFA條件。如需詳細資訊，請參閱《IAM使用指南》中的 < 設定MFA受保護的API存取 > 。

如需中最佳作法的詳細資訊IAM，請參閱《IAM使用指南》IAM中的「安全性最佳作法」。

使用 Amazon 一個企業控制台

若要存取 Amazon One 企業主控台，您必須擁有最少一組許可。這些許可必須允許您列出並檢視有關 Amazon One 企業資源的詳細資訊 AWS 帳戶。 如果您建立的以身分識別為基礎的原則比所需的最低權限更嚴格，則控制台將無法如預期用於具有該原則的實體 (使用者或角色) 運作。

您不需要針對只撥打電話的使用者允許最低主控台權限 AWS CLI 或 AWS API。相反地，只允許存取符合他們嘗試執行之API作業的動作。

為了確保用戶和角色仍然可以使用 Amazon One 企業控制台，還可以連接 Amazon 一個企業*ConsoleAccess*或 *ReadOnly* AWS 對實體的管理策略。如需詳細資訊，請參閱《使用指南》中的〈將權限新增至IAM使用者〉。

允許使用者檢視他們自己的許可

此範例顯示如何建立原則，讓使IAM用者檢視附加至其使用者身分識別的內嵌和受管理原則。此原則包含在主控台上完成此動作的權限，或以程式設計方式使用 AWS CLI 或 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": "*"
        }
    ]
}
```

只讀訪問 Amazon 一個企業

下面的例子顯示了 AWS 受管政策AmazonOneEnterpriseReadOnlyAccess，授予 Amazon One 企業版的唯讀存取權。

```
{
  "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。元Resource素會列出 AWS 允許使用者執行這些動作的資源。對於控制存取 Amazon One 企業版動作的政策，Resource元素一律會設定為*，萬用字元表示「所有資源」。

Action元素中的值對應於服務支援的值。APIs這些動作之前會加上config:以表示它們參考 Amazon One 企業版動作。您可以在 Action 元素中使用 * 萬用字元，如下列範例所示：

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

  這允許所有以 "DeviceInstance" (GetDeviceInstanceConfiguration,CreateDeviceInstanceConfiguration) 結尾的 Amazon One 企業動作。
- "Action": ["one:*"]

這允許所有 Amazon One 企業操作，但不允許其他操作 AWS 服務。

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

  這允許所有 AWS 動作。此權限適用於作為 AWS 您帳戶的管理員。

唯讀原則不會授與使用者對動作 (例如`CreateDeviceInstance`、`UpdateDeviceInstance`和) 的權限`DeleteDeviceInstance`。具有此政策的使用者不得建立裝置執行個體、更新裝置執行個體或刪除裝置執行個體。如需 Amazon One 企業版動作的清單，請參閱Amazon One Enterprise 的動作、資源與條件索引鍵。

完全訪問 Amazon 一家企業

下列範例顯示授與 Amazon One 企業版完整存取權的政策。它授予使用者執行所有 Amazon One 企業版動作的權限。

> **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 企業規則動作支援的資源層級許可 API

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 企業版支援特定 Amazon One 企業規則API動作的資源層級許可。這表示對於某些 Amazon One 企業規則動作，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 企業規則API動作。它還描述了支持的資源及其ARNs每個動作。指定時ARN，您可以在路徑中使用 * 萬用字元；例如，當您不能或不想指定確切的資源時IDs。

> **Important**
>
> 如果此表格中未列出 Amazon One 企業規則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，您可以授與使用者使用該動作的權限，但必須為政策陳述式的資源元素指定 *。

API動作	資源
CreateDeviceInstance	設備實例 ARN: AW: 一個:*region:accountID* ：設備實例/*deviceInstanceId*
GetDeviceInstance	設備實例 ARN: AW: 一個:*region:accountID* ：設備實例/*deviceInstanceId*
UpdateDeviceInstance	設備實例 ARN: AW: 一個:*region:accountID* ：設備實例/*deviceInstanceId*
DeleteDeviceInstance	設備實例 ARN: AW: 一個:*region:accountID* ：設備實例/*deviceInstanceId*
CreateDeviceActivationQrCode	設備實例 ARN: AW: 一個:*region:accountID* ：設備實例/*deviceInstanceId*
DeleteAssociatedDevice	設備實例

API動作	資源
	ARN: AW: 一個:*region:accountID* ：設備實例/*deviceInstanceId*
RebootDevice	設備實例 ARN: AW: 一個:*region:accountID* ：設備實例/*deviceInstanceId*
CreateDeviceInstanceConfiguration	設備實例配置 ARN: AW: 一個:*region:accountID* ：設備實例/*deviceInstanceId* /配置/*version*
GetDeviceInstanceConfiguration	設備實例配置 ARN: AW: 一個:*region:accountID* ：設備實例/*deviceInstanceId* /配置/*version*
CreateSite	Site ARN: AW: 一個:*region:accountID* ：網站/*siteId*
DeleteSite	Site ARN: AW: 一個:*region:accountID* ：網站/*siteId*
GetSiteAddress	Site ARN: AW: 一個:*region:accountID* ：網站/*siteId*
UpdateSite	Site ARN: AW: 一個:*region:accountID* ：網站/*siteId*
UpdateSiteAddress	Site ARN: AW: 一個:*region:accountID* ：網站/*siteId*

API動作	資源
CreateDeviceConfigurationTemplate	設備配置模板 ARN: AW: 一個:*region:accountID* :device-configuration-template/*templateId*
DeleteDeviceConfigurationTemplate	設備配置模板 ARN: AW: 一個:*region:accountID* :device-configuration-template/*templateId*
GetDeviceConfigurationTemplate	設備配置模板 ARN: AW: 一個:*region:accountID* :device-configuration-template/*templateId*
UpdateDeviceConfigurationTemplate	設備配置模板 ARN: AW: 一個:*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。

在第一個原則中，您允許 AWS Config 規則讀取動作，例如針GetSite對指定的規則。

```
{
        "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 企業規則的寫入動作。

```
{
    "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權，以便在 Amazon One Enterprise 規則API動作上執行特定動作。

其他資訊

若要深入瞭解如何建立使IAM用者、群組、原則和權限，請參閱《使用指南》中的〈建立您的第一個IAM使用者和管理員群組和存取管理〉。IAM

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

疑難排解 Amazon One 企業身分識別和存取

使用下列資訊來協助您診斷和修正使用 Amazon One 企業版和時可能會遇到的常見問題IAM。

主題

我沒有授權在 Amazon 一個企業執行操作

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。

當使用mateojacksonIAM者嘗試使用主控台來檢視虛構*my-example-widget*資源的詳細資料，但沒有虛構的one:*GetWidget*權限時，就會發生下列範例錯誤。

```
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。

我想讓我以外的人 AWS 帳戶 訪問我的 Amazon 一個企業資源

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。對於支援以資源為基礎的政策或存取控制清單 (ACLs) 的服務，您可以使用這些政策授與人員存取您的資源。

如需進一步了解，請參閱以下內容：

- 若要了解 Amazon One 企業版是否支援這些功能，請參閱Amazon 一個企業如何與 IAM。
- 了解如何提供對您資源的存取權 AWS 帳戶 您擁有的，請參閱為其他IAM使用者提供存取權 AWS 帳戶 您在IAM用戶指南中擁有的。
- 瞭解如何將資源存取權提供給第三方 AWS 帳戶，請參閱提供存取 AWS 帳戶 由IAM用戶指南中的第三方擁有。
- 若要瞭解如何透過身分聯盟提供存取權，請參閱使用指南中的提供對外部驗證使用IAM者的存取權(身分聯合)。
- 若要瞭解針對跨帳號存取使用角色與以資源為基礎的政策之間的差異，請參閱《使用IAM者指南》IAM中的〈跨帳號資源存取〉。

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。

記錄和監控 Amazon 單一企業版

監控是維護 Amazon One 企業和其他 AWS 解決方案的可靠性、可用性和效能的重要組成部分。 AWS 提供下列監控工具來觀看 Amazon One 企業版、在發生錯誤時報告，並在適當時採取自動動作：

- Amazon EventBridge 可用於自動化 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 EventBridge 的方式傳送到。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擷取您帳戶或代表您的 AWS 帳戶發出的API呼叫和相關事件，並將日誌檔傳送到您指定的 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 位址，以及呼叫發生的時間。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南。

在 Amazon 監控 Amazon 一個企業事件 EventBridge

您可以在中監控 Amazon One 企業事件 EventBridge，從您自己的應用程式、 software-as-a-service (SaaS) 應用程式和 AWS 服務提供即時資料串流。 EventBridge將資料路由到目標，例如 AWS Lambda Amazon 簡單通知服務。這些事件提供近乎即時的系統事件串流，用來描述 AWS 資源變更。

訂閱 Amazon 一個企業活動

Amazon One 裝置和使用者設定檔狀態變更事件是使用發佈的 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 一個企業活動

1. 在開啟 EventBridge 主控台https://console.aws.amazon.com/events/。
2. 在導覽窗格的「匯流排」下，選擇「規則」。
3. 選擇建立規則。
4. 在 [預設規則詳細資料] 頁面上，指派規則的名稱，選擇 [具有事件模式的規則]，然後選擇 [下一步]。
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 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，選擇自訂樣式。在 [事件模式] 區段中，將事件來源新增為JSONaws:one與所需詳細資料類型，然後選擇 [下一步]。
9. 在「選取目標」 頁面上，選取您選擇的目標，其中包括 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，您可以配置標籤。
11. 在 檢閱和建立 頁面上，選擇 建立規則。如需有關配置規則的詳細資訊，請參閱《 EventBridge 使用指南》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。針對每個事件類型，會依照規則中的設定，將 JSON blob 傳送至您選擇的目標。可用的詳圖類型如下：

裝置 Health 狀態變更為健全狀況

設備通過所有運行狀態檢查。

裝置 Health 狀態變更為嚴重

裝置一或多項運作狀態檢查失敗。

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

設備已連接到互聯網。

resources

包含針對其發佈「裝置狀態變更」事件的 deviceInstance arn 清單。

中繼資料

siteName

- 存在的網站的 deviceInstance 名稱。

siteArn

- ARN 用於存在的 deviceInstance 網站。

資料

currentConnectivity

- 表示 deviceInstance 是否已連線至網際網路或中斷連線。
- 可能的值：CONNECTED，DISCONNECTED

previousConnectivity

- 表示事件 deviceInstance 發生前是否已連線至網際網路或中斷連線。
- 可能的值：CONNECTED，DISCONNECTED

currentHealthStatus

- 表示是否 deviceInstance 已通過所有健康狀態檢查。
- 可能的值：HEALTHY，CRITICAL

previousHealthStatus

- 表示上次檢查時是否 deviceInstance 通過所有健康狀態檢查。
- 可能的值：HEALTHY，CRITICAL

assetTagId

- 與相關聯 assetTagId 的裝置的deviceInstance。

deviceInstanceName

- 發佈「 deviceInstance 裝置狀態事件」的名稱。

用戶概況事件類型

使用者設定檔相關的事件詳細資料類型為：

新成功報名

使用者註冊成功時。

新成功取消註冊

使用者成功取消註冊時。

註冊失敗

使用者註冊失敗時。

取消註冊失敗

使用者無法取消註冊時。

成功認可

當用戶掃描掌中的身份驗證成功。

辨識不成功

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 arn 清單。

資料

accountId

- 起始要求之裝置的相關 AWS 帳戶。

requestSource

- 這是 deviceInstanceId 發起請求的設備。

createdTimestamp

- 事件被創建的時間。

userStatus

- 使用者的目前狀態。
- 可能的值：ACTIVE，DELETED

associatedId

- 用戶的相關 ID，例如徽章 ID。

reason

- 此值會針對不成功的事件顯示。它包含事件失敗的原因。

範例事件

以下示例顯示了 Amazon 一個企業的事件。

主題

裝置健康狀態變更為健全狀況

設備通過了所有健康狀態，並且設備實例健康狀態更改為HEALTHY從CRITICAL健康狀態。

```
{
    "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"
    }
  }
}
```

裝置健康狀態變更為嚴重

裝置未通過一或多個運作狀態檢查，且裝置執行個體健康狀態變更為「CRITICAL從」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變更為「CONNECTED從」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變更為「DISCONNECTED從」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"
    }
  }
}
```

新成功註冊

使用者成功註冊時的事件。

```
{
    "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 一個企業用戶指南的文檔歷史記錄

下表說明 Amazon One 企業版的文件版本。

變更	描述	日期
更新	添加了新主題：安裝 Amazon 一個設備 I/O 集線器以安全訪問 Amazon 一個企業用戶指南	2024年8月14日
更新	添加了新主題：安裝壁掛式 Amazon 一台設備 Amazon 一個企業用戶指南	2024年6月5 日
初始版本	Amazon 單一企業用戶指南的初始版本	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。