使用者指南

AWS 登入

AWS 登入: 使用者指南

Table of Contents

什麼是 AWS 登入？

本指南可協助您了解登入 Amazon Web Services (AWS) 的不同方式，視您的使用者類型而定。如需有關如何根據您的使用者類型和您要存取 AWS 的資源登入的詳細資訊，請參閱下列其中一個教學課程。

- 登入 AWS 管理主控台
- 登入您的 AWS 存取入口網站
- 以聯合身分身分登入
- 透過 登入 AWS Command Line Interface
- 使用 登入 AWS 建構家 ID

如果您在登入 時遇到問題 AWS 帳戶，請參閱 對 AWS 帳戶 登入問題進行故障診斷。如需 的說明，AWS 建構家 ID 請參閱 對 AWS 建置器 ID 問題進行故障診斷。想要建立 AWS 帳戶？ 註冊。 AWS如需註冊 如何 AWS 協助您或組織的詳細資訊，請參閱聯絡我們。

主題

術語

Amazon Web Services (AWS) 使用常用術語來描述登入程序。我們建議您閱讀並了解這些條款。

管理員

也稱為 AWS 帳戶 管理員或 IAM 管理員。管理員通常是資訊技術 (IT) 人員，是監督 的個人 AWS 帳戶。管理員對 的許可層級 AWS 帳戶 高於其組織的其他成員。管理員會建立和實作 的設定 AWS 帳

戶。他們也會建立 IAM 或 IAM Identity Center 使用者。管理員會提供這些使用者存取憑證和登入 URL 來登入 AWS。

帳戶

標準 AWS 帳戶 包含您的 AWS 資源和可存取這些資源的身分。帳戶與帳戶擁有者的電子郵件地址和密碼相關聯。

憑證

也稱為存取憑證或安全憑證。進行身分驗證和授權時，系統會使用登入資料來識別呼叫發起人，以及是否允許請求的存取。登入資料是使用者提供給 AWS 以登入和存取 AWS 資源的資訊。人類使用者的登入資料可以包含電子郵件地址、使用者名稱、使用者定義的密碼、帳戶 ID 或別名、驗證碼，以及單一使用多重驗證 (MFA) 代碼。對於程式設計存取，您也可以使用存取金鑰。建議盡可能使用短期存取金鑰。

如需登入資料的詳細資訊，請參閱AWS 安全登入資料。

> **Note**
>
> 使用者必須提交的登入資料類型取決於其使用者類型。

公司登入資料

使用者存取其公司網路和資源時提供的登入資料。您的公司管理員可以設定您的 AWS 帳戶 ，以使用您用來存取公司網路和資源的相同登入資料。這些登入資料是由您的管理員或服務台員工提供給您。

設定檔

當您註冊 AWS 建置器 ID 時，您可以建立設定檔。您的設定檔包含您提供的聯絡資訊，以及管理多重要素驗證 (MFA) 裝置和作用中工作階段的能力。您也可以進一步了解隱私權，以及我們在設定檔中處理您的資料的方式。如需 設定檔及其與 關係的詳細資訊 AWS 帳戶，請參閱 AWS 建構家 ID 和其他 AWS 登入資料。

根使用者憑證

根使用者登入資料是用來建立 的電子郵件地址和密碼 AWS 帳戶。我們強烈建議將 MFA 新增至根使用者憑證，以提高安全性。根使用者憑證提供帳戶中所有 AWS 服務和資源的完整存取權。如需根使用者的詳細資訊，請參閱 根使用者。

使用者

使用者是有權對 AWS 產品或存取 AWS 資源進行 API 呼叫的人員或應用程式。每個使用者都有一組不與其他使用者共用的唯一安全登入資料。這些登入資料與 的安全登入資料不同 AWS 帳戶。如需詳細資訊，請參閱判斷您的使用者類型。

驗證碼

驗證碼會在登入程序期間使用多重要素驗證 (MFA) 驗證您的身分。驗證碼的交付方法會有所不同。它們可以透過簡訊或電子郵件傳送。如需詳細資訊，請洽詢您的管理員。

AWS 登入的區域可用性

AWS 登入可在數個常用的 中使用 AWS 區域。此可用性可讓您更輕鬆地存取 AWS 服務和商業應用程式。如需登入支援區域的完整清單，請參閱AWS 登入端點和配額。

登入事件記錄

CloudTrail 會在您的 上自動啟用， AWS 帳戶 並在活動發生時記錄事件。下列資源可協助您進一步了解記錄和監控登入事件。

- CloudTrail 日誌會嘗試登入 AWS 管理主控台。所有 IAM 使用者、根使用者和聯合身分使用者登入事件都會在 CloudTrail 日誌檔案中產生記錄。如需詳細資訊，請參閱《AWS CloudTrail 使用者指南》中的AWS 管理主控台 登入事件。
- 如果您使用區域端點登入 AWS 管理主控台，CloudTrail 會將`ConsoleLogin`事件記錄在端點的適當區域中。如需 AWS 登入端點的詳細資訊，請參閱《 AWS 一般參考指南》中的AWS 登入端點和配額。
- 若要進一步了解 CloudTrail 如何記錄 IAM Identity Center 的登入事件，請參閱《IAM Identity Center 使用者指南》中的了解 IAM Identity Center 登入事件。
- 若要進一步了解 CloudTrail 如何在 IAM 中記錄不同的使用者身分資訊，請參閱《 使用者指南》中的使用 記錄 IAM 和 AWS STS API 呼叫 AWS CloudTrail。 AWS Identity and Access Management

AWS Sign-In 支援以資源為基礎的政策和資源控制政策，可讓您根據網路位置和主體身分來限制主控台存取。對於根使用者，網路位置會在密碼提示出現之前進行驗證。對於所有委託人類型，政策會在驗證前和驗證後進行評估。如需詳細資訊，請參閱使用以資源為基礎的政策和資源控制政策來控制主控台存取。

判斷您的使用者類型

登入的方式取決於您是哪種類型的 AWS 使用者。您可以將 AWS 帳戶 管理為根使用者、IAM 使用者、IAM Identity Center 中的使用者或聯合身分。您可以使用 AWS Builder ID 描述檔來存取特定 AWS 服務和工具。以下列出不同的使用者類型。

主題

根使用者

也稱為帳戶擁有者或帳戶根使用者。身為根使用者，您可以完整存取 中的所有 AWS 服務和資源 AWS 帳戶。第一次建立 時 AWS 帳戶，您會從單一登入身分開始，該身分可完整存取帳戶中的所有 AWS 服務和資源。此身分是 AWS 帳戶根使用者。您可以使用您用來建立帳戶的電子郵件地址和密碼，以根使用者的身分登入。根使用者使用 登入AWS 管理主控台。如需如何登入的逐步說明，請參閱 以根使用者 AWS 管理主控台 身分登入。

> **Important**
>
> 當您建立 時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分可完整存取所有 AWS 服務 和 資源。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，請參閱《IAM 使用者指南》中的需要根使用者憑證的任務。

如需 IAM 身分的詳細資訊，包括根使用者，請參閱 IAM 身分 （使用者、使用者群組和角色）。

IAM 使用者

IAM 使用者是您建立的實體 AWS。此使用者是 內授予特定自訂許可 AWS 帳戶 的身分。您的 IAM 使用者登入資料包含用於登入 的名稱和密碼AWS 管理主控台。如需如何登入的逐步說明，請參閱 以 IAM 使用者 AWS 管理主控台 身分登入。

如需 IAM 身分的詳細資訊，包括 IAM 使用者，請參閱 IAM 身分 （使用者、使用者群組和角色）。

IAM Identity Center 使用者

IAM Identity Center 使用者是 的成員， AWS Organizations 可以透過您的存取入口網站授予對多個 AWS 帳戶 和應用程式的 AWS 存取權。如果其公司已將 Active Directory 或其他身分提供者與 IAM Identity Center 整合，IAM Identity Center 中的使用者可以使用其公司憑證登入。IAM Identity Center 也可以是身分提供者，管理員可以在其中建立使用者。無論身分提供者為何，IAM Identity Center 中的使用者都會使用您的 AWS 存取入口網站登入，這是其組織的特定登入 URL。IAM Identity Center 使用者無法透過 AWS 管理主控台 URL 登入。

IAM Identity Center 中的人類使用者可以從下列任一位置取得您的 AWS 存取入口網站 URL：

- 管理員或服務台員工的訊息
- 來自 的電子郵件， AWS 內含加入 IAM Identity Center 的邀請

> **Tip**
>
> IAM Identity Center 服務傳送的所有電子郵件均來自地址 no-reply@signin.aws 或 no-reply@login.awsapps.com。我們建議您設定電子郵件系統，使其接受來自這些寄件者電子郵件地址的電子郵件，而不會將其視為垃圾郵件或垃圾郵件處理。

如需如何登入的逐步說明，請參閱 登入您的 AWS 存取入口網站。

> **Note**
>
> 我們建議您將組織的特定登入 URL 加入 AWS 您存取入口網站的書籤，以便稍後可以存取。

如需 IAM Identity Center 的詳細資訊，請參閱什麼是 IAM Identity Center？

聯合身分

聯合身分是可以使用知名的外部身分提供者 (IdP) 登入的使用者，例如 Login with Amazon、Facebook、Google 或任何其他與 OpenID Connect (OIDC) 相容的 IdP。使用 Web 聯合身分，您可以接收身分驗證字符，然後將該字符交換為 中的臨時安全登入資料 AWS ，該登入資料對應至具有許可的 IAM 角色，以使用 中的資源 AWS 帳戶。 您不會使用 AWS 管理主控台 或 AWS 存取入口網站登入。反之，使用中的外部身分會決定您的登入方式。

如需詳細資訊，請參閱以聯合身分身分登入。

AWS Builder ID 使用者

身為 AWS 建置器 ID 使用者，您特別登入要存取的服務 AWS 或工具。 AWS Builder ID 使用者會補充 AWS 帳戶 您已擁有或想要建立的任何 。 AWS 建置器 ID 代表您是個人，您可以使用它來存取 AWS 服務和工具，而不需要 AWS 帳戶。您也有一個設定檔，您可以在其中查看和更新您的資訊。如需詳細資訊，請參閱使用 登入 AWS 建構家 ID。

AWS Builder ID 與您的 AWS Skill Builder 訂閱是獨立的線上學習中心，您可以在其中向 AWS 專家學習並線上建置雲端技能。如需 AWS 技能建置器的詳細資訊，請參閱AWS 技能建置器。

判斷您的登入 URL

AWS 根據您的 AWS 使用者類型，使用下列其中一個 URLs來存取 。如需詳細資訊，請參閱判斷您的使用者類型。

主題

- AWS 帳戶 根使用者登入 URL
- AWS 存取入口網站
- IAM 使用者登入 URL
- 聯合身分 URL
- AWS 建置器 ID URL

AWS 帳戶 根使用者登入 URL

根使用者 AWS 管理主控台 從 AWS 登入頁面存取 ：`https://console.aws.amazon.com/` 。

此登入頁面也可以選擇以 IAM 使用者身分登入。

AWS 存取入口網站

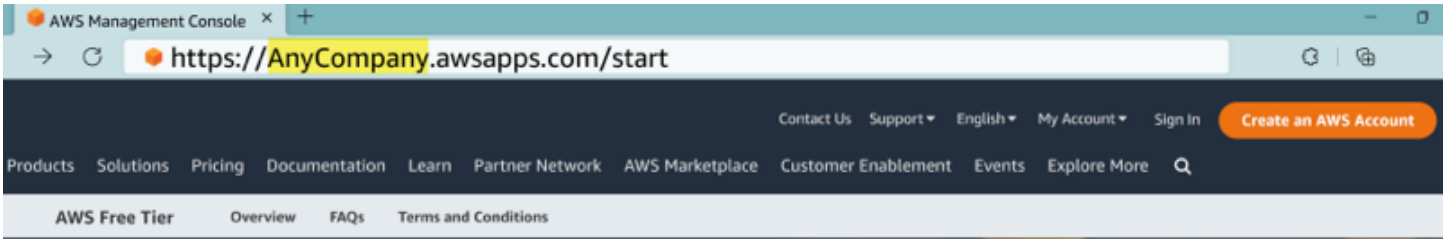
AWS 存取入口網站是 IAM Identity Center 中使用者登入和存取您帳戶的特定登入 URL。當管理員在 IAM Identity Center 中建立使用者時，管理員會選擇使用者是否收到加入 IAM Identity Center 的電子郵件邀請，還是收到來自管理員或服務台員工的訊息，其中包含一次性密碼和 AWS 存取入口網站 URL。特定登入 URL 的格式如下所示：

```
https://d-xxxxxxxxxx.awsapps.com/start
```

或

```
https://your_subdomain.awsapps.com/start
```

特定的登入 URL 會有所不同，因為您的管理員可以自訂。特定的登入 URL 可能以字母 D 開頭，後面接著 10 個隨機號碼和字母。您的子網域也可能用於登入 URL，並可能包含您的公司名稱，如下列範例所示：



> **Note**
>
> 我們建議您將 AWS 存取入口網站的特定登入 URL 加入書籤，以便稍後可以存取。

如需 AWS 存取入口網站的詳細資訊，請參閱使用 AWS 存取入口網站。

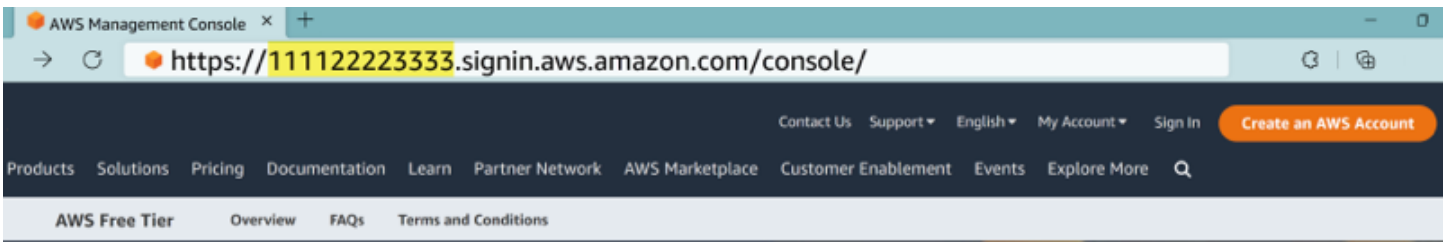
IAM 使用者登入 URL

IAM 使用者可以 AWS 管理主控台 使用特定的 IAM 使用者登入 URL 存取 。IAM 使用者登入 URL 結合了您的 AWS 帳戶 ID 或別名和 `signin.aws.amazon.com/console`

IAM 使用者登入 URL 的外觀範例：

```
https://account_alias_or_id.signin.aws.amazon.com/console/
```

如果您的帳戶 ID 為 111122223333，您的登入 URL 將為：



如果您在 AWS 帳戶 使用 IAM 使用者登入 URL 存取 時遇到問題，請參閱 中的恢復能力 AWS Identity and Access Management以取得更多資訊。

聯合身分 URL

聯合身分的登入 URL 會有所不同。外部身分或外部身分提供者 (IdP) 會決定聯合身分的登入 URL。外部身分可以是 Windows Active Directory、Login with Amazon、Facebook 或 Google。如需如何以聯合身分登入的詳細資訊，請聯絡您的管理員。

如需聯合身分的詳細資訊，請參閱關於 Web 聯合身分。

AWS 建置器 ID URL

AWS 建置器 ID 設定檔的 URL 為 https://profile.aws.amazon.com/。使用您的 AWS 建置器 ID 時，登入 URL 取決於您要存取的服務。例如，若要登入 Amazon CodeCatalyst，請前往 https://codecatalyst.aws/login。

要新增至允許清單的網域

如果您使用新一代防火牆 (NGFW) 或安全 Web Gateway (SWG) 等 Web 內容篩選解決方案來篩選特定 AWS 網域或 URL 端點的存取權，則必須將下列網域或 URL 端點新增至 Web 內容篩選解決方案允許清單。

AWS 要允許清單的登入網域

如果您或您的組織實作 IP 或網域篩選，您可能需要允許列出網域才能使用 AWS 管理主控台。下列網域必須在您嘗試存取 的網路上存取 AWS 管理主控台。

- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

AWS 要允許清單的登入管理網域

如果您使用 CLI AWS 設定主控台存取控制，則必須允許列出 AWS 登入控制平面端點。此端點會處理政策管理，並與上一節中的主控台登入網域不同。

- signin.*[Region]*.api.aws

  將 *#Region#* 取代為您呼叫 AWS 的區域。適用於所有商業區域。範例：signin.us-east-1.api.aws。

AWS 存取入口網站 要允許清單的網域

如果您使用新一代防火牆 (NGFW) 或安全 Web Gateway (SWG) 等 Web 內容篩選解決方案來篩選特定 AWS 網域或 URL 端點的存取權，則必須將下列網域或 URL 端點新增至 Web 內容篩選解決方案允許清單。這樣做可讓您存取 AWS 存取入口網站。

下列清單提供 IPv4 和雙堆疊網域，以及要新增至 Web 內容篩選解決方案允許清單的 URL 端點。如需雙堆疊端點的詳細資訊，請參閱《IAM Identity Center 使用者指南》中的更新防火牆和閘道以允許存取 AWS 存取入口網站 。

IPv4 允許清單

- *[Directory ID or alias]*.awsapps.com
- *[IAM Identity Center instance ID]*.*[Region]*.portal.amazonaws.com
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- *.sso-portal.*[Region]*.amazonaws.com

雙堆疊允許清單

- *[IAM Identity Center instance ID]*.portal.*[Region]*.app.aws
- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.api.aws

- sso.*[Region]*.api.aws
- portal.sso.*[Region]*.api.aws
- *[Region]*.sso.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- cdn.us-east-1.threat-mitigation.aws.amazon.com
- us-east-1.threat-mitigation.aws.amazon.com
- amcs-captcha-prod-us-east-1.s3.dualstack.us-east-1.amazonaws.com

AWS 建構家 ID 要允許清單的網域

如果您或您的組織實作 IP 或網域篩選，您可能需要允許列出網域來建立和使用 AWS 建構家 ID。下列網域必須在您嘗試存取的網路上存取 AWS 建構家 ID。

- view.awsapps.com/start
- *.portal.*.app.aws
- *.aws.dev
- *.api.aws
- *.uis.awsstatic.com
- *.console.aws.a2z.com
- oidc.*.amazonaws.com
- oidc.*.api.aws
- *.sso.amazonaws.com
- *.sso.*.amazonaws.com
- *.sso-portal.*.amazonaws.com
- sso.*.api.aws
- *.signin.aws
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com
- profile.aws.amazon.com

AWS 帳戶 管理員的安全最佳實務

如果您是建立新 的帳戶管理員 AWS 帳戶，我們建議您執行下列步驟，以協助使用者在登入時遵循 AWS 安全最佳實務。

1. 以根使用者身分登入以啟用多重要素驗證 (MFA)，如果您尚未建立AWS 管理使用者，請在 IAM Identity Center 中建立管理使用者。然後，保護您的根憑證，不要將其用於日常任務。
2. 以 AWS 帳戶 管理員身分登入並設定下列身分：
   - 為其他人類建立最低權限的使用者。
   - 設定工作負載的臨時登入資料。
   - 僅針對需要長期憑證的使用案例建立存取金鑰。
3. 新增許可以授予這些身分的存取權。您可以開始使用 AWS 受管政策，並轉向最低權限許可。
   - 將許可集新增至 AWS IAM Identity Center (AWS 單一登入的後續版本) 使用者。
   - 將身分型政策新增至用於工作負載的 IAM 角色。
   - 針對需要長期憑證的使用案例，為 IAM 使用者新增身分型政策。
   - 如需 IAM 使用者的詳細資訊，請參閱 IAM 中的安全最佳實務。
4. 儲存和共用有關 的資訊登入 AWS 管理主控台。視您建立的身分類型而定，此資訊會有所不同。
5. 將您的根使用者電子郵件地址和主要帳戶聯絡電話號碼保持在最新狀態，以確保您可以接收重要的帳戶和安全相關通知。
   - 修改 的帳戶名稱電子郵件地址或密碼 AWS 帳戶根使用者。
   - 存取或更新主要帳戶聯絡人。
6. 檢閱 IAM 中的安全最佳實務，以了解其他身分和存取管理最佳實務。
7. 實作以網路為基礎的存取控制：使用以資源為基礎的登入政策或資源控制政策 (RCPs)，將主控台登入限制為來自已核准 IP 地址範圍或 VPCs請求。對於使用主控台私有存取的環境，請設定 VPC 端點政策，以控制可透過端點存取哪些帳戶 （請參閱主控台私有存取)。登入資源型政策、RCPs 和 VPC 端點政策共同在不同強制執行點提供分層網路控制。對於根使用者，登入政策會在未經授權的網路嘗試存取時完全封鎖登入資料頁面。 AWS 建議設定排除的主體進行復原存取，以防止帳戶鎖定，但這是選用的。如需詳細資訊，請參閱使用以資源為基礎的政策和資源控制政策來控制主控台存取。

登入 AWS 管理主控台

當您 AWS 管理主控台 從主要登入 URL (https://console.aws.amazon.com/) AWS 登入 時，您必須選擇您的使用者類型，根使用者或 IAM 使用者。如果您不確定自己是哪種類型的使用者，請參閱 判斷您的使用者類型。

根使用者具有不受限制的帳戶存取權，並與建立 的人員相關聯 AWS 帳戶。然後，根使用者會建立其他類型的使用者，例如 IAM 使用者和 AWS IAM Identity Center 的使用者，並為其指派存取憑證。

IAM 使用者是 中具有特定自訂許可 AWS 帳戶 的身分。當 IAM 使用者登入時，他們可以使用包含其 AWS 帳戶 或 別名的登入 URL，例如 ，`https://account_alias_or_id.signin.aws.amazon.com/console/`而不是主要 AWS 登入 URL `https://console.aws.amazon.com/` 。

您可以在 的單一瀏覽器中同時登入最多 5 個不同的身分 AWS 管理主控台。這些可以是不同帳戶或相同帳戶中根使用者、IAM 使用者或聯合角色的組合。如需詳細資訊，請參閱 AWS 管理主控台 Getting Started Guide 中的 Signing in to multiple accounts。

教學

- 以根使用者 AWS 管理主控台 身分登入
- 以 IAM 使用者 AWS 管理主控台 身分登入

如果您不確定自己是哪種類型的使用者，請參閱 判斷您的使用者類型。

教學

- 以根使用者 AWS 管理主控台 身分登入
- 以 IAM 使用者 AWS 管理主控台 身分登入

以根使用者 AWS 管理主控台 身分登入

當您第一次建立 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。

> **Important**
>
> 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。

以根使用者身分登入

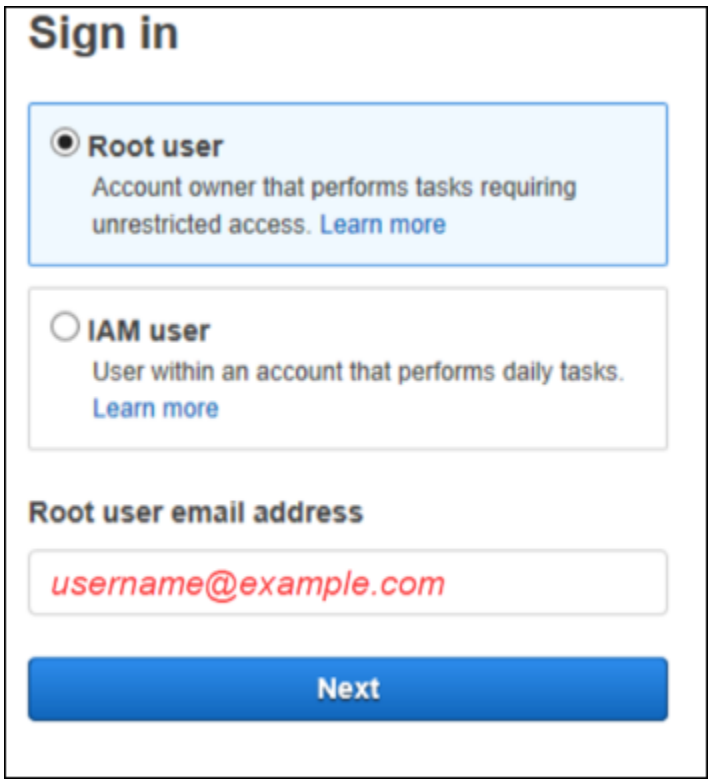
您可以在已登入 中的另一個身分時，以根使用者身分登入 AWS 管理主控台。如需詳細資訊，請參閱 AWS 管理主控台 Getting Started Guide 中的 Signing in to multiple accounts。

AWS 帳戶 使用 管理的 AWS Organizations 可能沒有根使用者憑證，而且您必須聯絡 管理員，在您的成員帳戶中執行根使用者動作。如果您無法以根使用者身分登入，請參閱 對 AWS 帳戶 登入問題進行故障診斷。

1. 在 AWS 管理主控台 開啟 https://console.aws.amazon.com/。

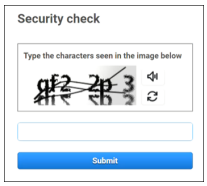
   > **Note**
   >
   > 如果您先前使用此瀏覽器以 IAM 使用者身分登入，您的瀏覽器可能會改為顯示 IAM 使用者登入頁面。選擇使用根使用者電子郵件登入。

2. 選擇根使用者。



3. 在根使用者電子郵件地址下，輸入與您的根使用者相關聯的電子郵件地址。然後，選取下一步。
4. 如果系統提示您完成安全檢查，請輸入提供給您的字元以繼續。如果您無法完成安全檢查，請嘗試聆聽音訊或重新整理一組新字元的安全檢查。

> **Tip**
>
> 依序輸入您看到（或聽到）的英數字元，不含空格。



5. 輸入您的密碼。

6. 使用 MFA 驗證。根據預設，根使用者會強制執行 MFA。對於獨立和成員帳戶的根使用者，您必須手動啟用 MFA，這是強烈建議的。如需詳細資訊，請參閱AWS Identity and Access Management 《使用者指南》中的AWS 帳戶 根使用者的多重驗證。

> **Tip**
>
> 作為安全最佳實務，我們建議您從 AWS 組織中的成員帳戶移除所有根使用者憑證，以協助防止未經授權的使用。如果您選擇此選項，成員帳戶無法以根使用者身分登入、執行密碼復原或設定 MFA。在這種情況下，只有管理帳戶管理員可以執行需要成員帳戶中根使用者憑證的任務。如需詳細資訊，請參閱AWS Identity and Access Management 《使用者指南》中的集中管理成員帳戶的根存取權。

7. 選擇登入。 AWS 管理主控台 隨即出現。

身分驗證後， 會 AWS 管理主控台 開啟主控台首頁。

其他資訊

如果您想要 AWS 帳戶 根使用者的詳細資訊，請參閱下列資源。

- 如需根使用者的概觀，請參閱AWS 帳戶 根使用者。
- 如需使用根使用者的詳細資訊，請參閱使用 AWS 帳戶 根使用者。
- 如需如何重設根使用者密碼的step-by-step說明，請參閱我忘記 的根使用者密碼 AWS 帳戶。

以 IAM 使用者 AWS 管理主控台 身分登入

IAM 使用者是在 中建立的身分 AWS 帳戶 ，具有與 AWS 資源互動的許可。IAM 使用者使用其帳戶 ID 或別名、使用者名稱和密碼登入。IAM 使用者名稱是由您的管理員設定。IAM 使用者名稱可以是易記的名稱，例如 *Zhang*，或電子郵件地址，例如 *zhang@example.com*。IAM 使用者名稱不能包含空格，但可以包含大小寫字母、數字和符號 + = , . @ _ -。

> **Tip**
>
> 如果您的 IAM 使用者已啟用多重要素驗證 (MFA)，您必須能夠存取身分驗證裝置。如需詳細資訊，請參閱搭配 IAM 登入頁面使用 MFA 裝置。

以 IAM 使用者身分登入

您可以在已登入 中的另一個身分時，以 IAM 使用者身分登入 AWS 管理主控台。如需詳細資訊，請參閱 AWS 管理主控台 Getting Started Guide 中的 Signing in to multiple accounts。

1. 在 AWS 管理主控台 開啟 https://console.aws.amazon.com/。
2. 主登入頁面隨即出現。輸入帳戶 ID (12 位數) 或別名、您的 IAM 使用者名稱和密碼。

   > **Note**
   >
   > 如果您先前已使用目前的瀏覽器以 IAM 使用者身分登入，或是使用帳戶登入 URL，則可能不必輸入帳戶 ID 或別名。

3. 選擇登入。
4. 如果您的 IAM 使用者已啟用 MFA， AWS 會要求您向驗證器確認身分。如需詳細資訊，請參閱在中使用多重要素驗證 (MFA) AWS。

身分驗證後， 會 AWS 管理主控台 開啟主控台首頁。

其他資訊

如果您想要 IAM 使用者的詳細資訊，請參閱下列資源。

- 如需 IAM 概觀，請參閱什麼是 Identity and Access Management？
- 如需 AWS 帳戶 IDs的詳細資訊，請參閱AWS 您的帳戶 ID 及其別名。

- 如需如何重設 IAM 使用者密碼step-by-step說明，請參閱我忘記 的 IAM 使用者密碼 AWS 帳戶。

使用以資源為基礎的政策和資源控制政策來控制主控台存取

> **Important**
>
> 主控台登入存取預設為啟用。 AWS 登入最初允許不受限制的主控台存取。若要新增限制，請為您的帳戶或組織啟用主控台授權組態。在您啟用主控台授權之前，您建立的資源許可陳述式不會生效。請參閱 使用資源政策開始使用主控台存取控制。

AWS Sign-In 支援以資源為基礎的政策和資源控制政策 (RCPs)，以控制對 AWS Sign-In 的存取。在身分驗證之前、期間和之後，使用這些政策在整個 AWS 管理主控台 存取過程中驗證使用者身分和網路位置。對於根使用者，這些政策會在憑證收集開始之前驗證網路位置和使用者身分。只有在存取來自預期的網路時，才能輸入登入資料。

AWS 以資源為基礎的登入政策：

- 套用至個別 AWS 帳戶。
- 讓帳戶管理員根據網路參數和主體身分來限制主控台存取。

資源控制政策 RCPs)：

- 透過 AWS Organizations 在整個組織中套用。
- 在所有成員帳戶中提供集中式控管。

這兩種政策類型都會在身分驗證之前驗證存取權。這會封鎖主體從非預期的網路存取登入頁面。

這些政策不會取代持續套用的 IAM 身分型政策。

> **Note**
>
> 如需資源控制政策的完整文件，包括組織層級組態和管理，請參閱《AWS Organizations 使用者指南》中的資源控制政策。本節主要著重於以資源為基礎的 AWS 登入政策。

AWS 以資源為基礎的登入政策和 RCPs 適用於下列身分驗證方法：

- AWS 管理主控台 – 使用主控台登入頁面直接登入。

- AWS IAM Identity Center – 使用 IAM Identity Center 的主控台登入。
- 聯合身分提供者 – 透過 SAML 或 OIDC 聯合登入。
- 與 AWS 登入整合的應用程式 – Amazon Connect、Amazon QuickSight、 AWS Health Dashboard、Amazon AppStream、Amazon Lightsail、AWS IQ。

這些控制項不適用於使用存取金鑰 （以 SigV4 簽署AWS SDKs 或 API 呼叫） 的程式設計存取。SigV4

AWS Sign-In 如何評估以資源為基礎的政策

AWS 登入會在主控台存取期間的兩個時間點評估適用的資源型政策或資源控制政策 (RCPs)：身分驗證前 （身分驗證前階段） 和身分驗證成功後 （身分驗證後階段）。每個評估都會檢查政策中定義的條件索引鍵。可用的金鑰取決於階段和動作。如需詳細資訊，請參閱支援的條件索引鍵。

> **Note**
>
> 對於根使用者登入，在密碼提示出現之前，來自非預期網路的存取嘗試會遭到封鎖。這可防止從非預期的網路提交登入資料。

身分驗證之後，評估也會考慮委託人的身分型政策。拒絕相關登入動作的 IAM 政策可能會阻止授予主控台工作階段，即使符合網路條件也一樣。

支援的動作

AWS 登入資源政策 （以資源為基礎的政策和 RCPs) 支援下列動作：

`signin:Authenticate`

這是在收到登入請求時評估的僅限評估 （不可呼叫） 動作。這是預先驗證檢查，當委託人在登入頁面 （根使用者、IAM 使用者） 輸入登入資料，或使用身分提供者或 AWS STS （聯合使用者、角色） 的登入資料啟動主控台登入時發生。

支援的條件金鑰：`aws:SourceIp`、`aws:SourceVpc`、`aws:SourceVpce`、`aws:VpcSourceIp`、`aws:RequestedR`

委託人型全域條件金鑰 (`aws:PrincipalArn`、`aws:PrincipalAccount`) 不適用於此動作，因為尚未確認使用者的身分。

`signin:AuthorizeOAuth2Access`

用於產生 OAuth 授權碼。身分驗證成功後，系統產生 OAuth 授權碼時會觸發此動作。此時，使用者會經過身分驗證，而且可使用主體型條件金鑰。

支援的條件金鑰：`aws:SourceIp`、`aws:SourceVpc`、`aws:SourceVpce`、`aws:VpcSourceIp`、`aws:RequestedR`

`signin:CreateOAuth2Token`

此驗證後動作用於建立和交換 OAuth 權杖。當兌換存取權杖的授權碼、重新整理權杖或執行權杖交換操作時，會觸發此動作。主體型條件金鑰在此階段期間可用。

支援的條件金鑰：`aws:SourceIp`、`aws:SourceVpc`、`aws:SourceVpce`、`aws:VpcSourceIp`、`aws:RequestedR`

Important

建立 AWS 登入政策（以資源為基礎的政策或 RCPs) 時，請在驗證前陳述`signin:Authenticate`式和驗證後陳述`signin:AuthorizeOAuth2Access``signin:CreateOAuth2Token`式中涵蓋政策中的所有三個動作。主控台登入使用 OAuth 2.0，它會依序流經這三個動作。如果您的政策省略 動作，則不會保護對應的階段。如需包含 的 VPC 端點政策動作`signin:CreateAccount`，請參閱 AWS 管理主控台私有存取。

支援的條件索引鍵

AWS Sign-In 支援資源型政策和資源控制政策 (RCPs中的下列條件索引鍵。使用這些金鑰根據網路位置和主體身分來控制主控台存取：

- 網路型（所有動作）：`aws:SourceIp`、`aws:SourceVpc`、`aws:SourceVpce`、`aws:VpcSourceIp`、`aws:Requested`
- 身分型（身分驗證後動作）：`aws:PrincipalArn`、`aws:PrincipalAccount`。
- 服務特定（僅限預先驗證）：`signin:PrincipalArn`。

如需詳細使用規則、運算子相容性、組合限制和依動作的可用性矩陣，請參閱 AWS 登入條件金鑰參考。

使用資源政策開始使用主控台存取控制

先決條件

- AWS 已安裝並設定 CLI。
- 適當的 IAM 許可 （ 請參閱 AWS 受管政策：AWSSignInResourcePolicyManagement)。
- 已識別的網路周邊 (IP 範圍、VPCs或 VPC 端點 ）。
- 指定保留存取權的排除主體 （ 建議但選用 ）。
- 如果您的網路使用輸出篩選，允許列出 AWS 登入控制平面端點 （ 請參閱 AWS 要允許清單的登入管理網域)。

> **Important**
>
> 在生產環境中啟用主控台授權之前， AWS 建議至少設定一個排除的主體，以維護緊急復原存取權。除非明確排除，否則所有委託人，包括根使用者，都必須遵守政策。排除的主體是選用的，但如果網路條件意外變更，省略它們會增加帳戶鎖定的風險。

`--region us-east-1` 為 AWS 登入政策上的所有寫入操作指定 。 會從此區域全域複 AWS 寫政策。讀取操作可以以任何區域為目標。

步驟 1：建立資源許可陳述式

建立定義存取控制的許可陳述式。所有寫入操作都需要 `--region us-east-1`(AWS Sign-In 服務僅接受此區域中的政策變更 ）。其餘參數 (`--source-vpc`、`--source-ip--requested-region`、、`--excluded-principal`) 定義政策中的條件。例如， 會將限制登入的條件`--requested-region us-west-2`新增至 us-west-2 區域登入端點。

範例 – 限制對公司 VPC 的存取：

```
aws signin put-resource-permission-statement \
  --source-vpc vpc-0abc123def456789 \
  --requested-region us-west-2 \
  --excluded-principal "arn:aws:iam::123456789012:user/EmergencyAdmin" \
  --client-token unique-request-id-12345 \
  --region us-east-1
```

範例 – 限制對特定 IP 範圍的存取：

```
aws signin put-resource-permission-statement \
  --source-ip "IP_ADDRESS" \
  --excluded-principal "arn:aws:iam::123456789012:role/BreakGlassRole" \
  --region us-east-1
```

> **Note**
>
> `--excluded-principal` 參數會指定排除的主體，以略過網路限制，並在網路條件變更時保留緊急存取。

步驟 2：啟用主控台授權組態

下列步驟會在您的帳戶或組織上啟用主控台登入程序的政策強制執行。您可以隨時建立資源許可陳述式，但在啟用主控台授權之前，不會對其進行評估。

> **Warning**
>
> 如果您的網路條件設定錯誤，或者現有服務控制政策 (SCP) 或資源控制政策 (RCP) 拒絕 AWS 登入動作，啟用主控台授權可能會鎖定主體。啟用主控台授權之前，請確認您的許可陳述式正確無誤，並移除或調整任何拒絕 `signin:Authenticate`、 或 的 SCP `signin:AuthorizeOAuth2Access`或 RCP`signin:CreateOAuth2Token`。

對於獨立帳戶：

```
aws signin put-console-authorization-configuration \
  --target-id <your-aws-account-id> \
  --region us-east-1
```

對於 AWS Organizations：

```
aws signin put-console-authorization-configuration \
  --target-id <your-aws-organization-id> \
  --region us-east-1
```

驗證組態：

```
aws signin get-console-authorization-configuration \
```

```
  --target-id <your-target-id> \
  --region <your-region>
```

刪除主控台授權組態：

```
aws signin delete-console-authorization-configuration \
  --target-id <your-target-id> \
  --region us-east-1
```

步驟 3：驗證您的政策

列出所有許可陳述式：

```
aws signin list-resource-permission-statements \
  --max-results 50 \
  --region <your-region>
```

擷取完整的合併政策：

```
aws signin get-resource-policy \
  --region <your-region>
```

`get-resource-policy` 命令會傳回包含所有許可陳述式的完整資源型政策。在測試主控台存取之前，請檢閱此政策以確認其反映您預期的存取控制。

區域可用性

主控台授權 APIs適用於所有 AWS 商業區域。您可以從您操作的任何區域呼叫這些 APIs。

> **Important**
>
> 寫入操作 (`put-console-authorization-configuration`、`put-resource-permission-statement`、`delete-console-authorization-configuration`、`delete-resource-permission-statement`) 必須在 `us-east-1`區域中執行。在 中建立的政策`us-east-1`會自動全域複寫。讀取操作 (`get-console-authorization-configuration`、`list-resource-permission-statements`、`get-resource-policy`) 可以從任何區域執行。

了解政策結構

AWS 登入政策包含兩個陳述式，可保護主控台登入流程的不同階段：

- 驗證前陳述式（動作：**signin:Authenticate**）：在身分驗證完成之前，在收到登入請求時進行評估。全域金鑰在此階段aws:PrincipalArn無法使用，因為主體的身分尚未確認。在此階段中，signin:PrincipalArn可以免除特定主體的網路限制。在此階段中，可以使用網路型條件金鑰進行評估。
- 驗證後陳述式（動作：**signin:AuthorizeOAuth2Access**、**signin:CreateOAuth2Token**）：在 OAuth 權杖交換期間，在驗證後評估。用來aws:PrincipalArn豁免特定委託人。所有網路型和身分型條件金鑰都可以在此階段中進行評估。

這兩個陳述式都是必要的，因為主控台登入使用 OAuth 2.0，它會依序流經所有三個動作。只有一個陳述式的政策會使另一個階段未受保護。 signin:PrincipalArn支援根使用者、IAM 使用者和角色委託人類型。 aws:PrincipalArn支援所有委託人類型（根使用者、IAM 使用者、聯合身分使用者、角色）。

政策範例

範例 1：具有網路周邊和排除主體的 RCP

下列資源控制政策 (RCP) 拒絕從公司網路外部 AWS 管理主控台 跨組織中的所有帳戶登入。指定的排除主體可免除緊急存取。由於 VPC IDs是唯一的，因此政策包含第三個陳述式，將 VPC 型存取鎖定在預期區域內。

EnforceNetworkPerimeterPreAuth 陳述式使用 在預先驗證階段中signin:PrincipalArn排除排除的委託人。EnforceNetworkPerimeterPostAuth 陳述式會在身分驗證後aws:PrincipalArn使用 來排除排除的委託人。EnforceSourceVPCRegion 陳述式可確保請求區域符合 VPC 區域，限制對指定 VPC 之預期區域的存取。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceNetworkPerimeterPreAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["signin:Authenticate"],
      "Resource": "*",
```

```
      "Condition": {
        "ArnNotEquals": {
          "signin:PrincipalArn": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::444455556666:root",
            "arn:aws:iam::777788889999:user/EmergencyUser",
            "arn:aws:iam::777788889999:role/OrgBreakGlassRole"
          ]
        },
        "NotIpAddressIfExists": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringNotEquals": {
          "aws:SourceVpc": "<my-vpc>"
        }
      }
    },
    {
      "Sid": "EnforceNetworkPerimeterPostAuth",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["signin:CreateOAuth2Token", "signin:AuthorizeOAuth2Access"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "aws:PrincipalArn": [
            "arn:aws:iam::111122223333:root",
            "arn:aws:iam::444455556666:root",
            "arn:aws:iam::777788889999:user/EmergencyUser",
            "arn:aws:iam::777788889999:role/OrgBreakGlassRole"
          ]
        },
        "NotIpAddressIfExists": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringNotEquals": {
          "aws:SourceVpc": "<my-vpc>"
        }
      }
    },
    {
      "Sid": "EnforceSourceVPCRegion",
      "Effect": "Deny",
      "Principal": "*",
```

```
      "Action": [
        "signin:Authenticate",
        "signin:CreateOAuth2Token",
        "signin:AuthorizeOAuth2Access"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceVpc": "<my-vpc>"
        },
        "StringNotEqualsIfExists": {
          "aws:RequestedRegion": "<my-vpc-region>"
        }
      }
    }
  ]
}
```

此政策：

- 除非請求來自公司 IP 範圍或公司 VPC，否則拒絕存取登入頁面。排除的根帳戶和 IAM 使用者會透過 `signin:PrincipalArn`（預先驗證）豁免。
- 除非來自公司 IP 範圍或 VPC，否則拒絕 OAuth 權杖交換。排除的根帳戶、IAM 使用者和角色會透過 `aws:PrincipalArn`（身分驗證後全域金鑰）豁免。
- 如果請求來自指定的 VPC，但區域不相符，則會拒絕存取。 AWS VPC IDs是唯一的，而且相同的 VPC ID 可以存在於不同的區域中。
- 設定為 RCP 時，將全域套用至您的 AWS Organization。

範例 2：具有排除委託人之 IP 型存取的資源型政策

下列資源型政策會拒絕主控台存取從指定 IP 範圍之外發出請求的所有委託人，並排除 委託人。政策包含兩個陳述式：使用服務特定`signin:PrincipalArn`金鑰的驗證前陳述式，以及使用全域`aws:PrincipalArn`金鑰的驗證後陳述式。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
```

```
      "Action": ["signin:Authenticate"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "signin:PrincipalArn": "<excluded-principal-arn>"
        },
        "NotIpAddress": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringEquals": {
          "aws:ResourceAccount": "<my-aws-account-id>"
        }
      }
    },
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:CreateOAuth2Token", "signin:AuthorizeOAuth2Access"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "aws:PrincipalArn": "<excluded-principal-arn>"
        },
        "NotIpAddress": {
          "aws:SourceIp": "<my-corporate-cidr>"
        },
        "StringEquals": {
          "aws:ResourceAccount": "<my-aws-account-id>"
        }
      }
    }
  ]
}
```

此政策：

- 拒絕存取所有主體，除非它們從 IP 範圍 連接<my-corporate-cidr>。
- 使用 signin:PrincipalArn（預先驗證） 和 aws:PrincipalArn（驗證後） 將排除的委託人排除在網路限制之外。
- 僅適用於設定資源型政策的特定帳戶 （由 識別<my-aws-account-id>)。

最佳實務

設定排除的主體以進行緊急復原存取

AWS 建議在生產環境中強制執行主控台授權政策之前，設定至少一個排除的使用者。在預先驗證階段，signin:PrincipalArn條件金鑰會豁免根使用者、IAM 使用者和角色主體。在驗證後階段，aws:PrincipalArn條件索引鍵會排除所有委託人類型（根使用者、IAM 使用者、聯合身分使用者、角色）。

排除的主體是選用的，但如果網路條件意外變更或政策設定錯誤，則省略它們會增加帳戶鎖定的風險。

建議的排除主體組態步驟：

1. 建立排除的 IAM 角色（例如 BreakGlassRole)。
2. 對於排除的角色， 在角色信任政策中需要 MFA。
3. 僅授予排除身分緊急復原所需的最低許可。
4. 在驗證前 (signin:PrincipalArn) 和驗證後 (aws:PrincipalArn) 政策陳述式中包含排除的主體 ARN。
5. 記錄復原程序，並將其安全地存放在 外部 AWS。
6. 定期測試排除的主體存取權，以確認其在需要時有效。

維護復原存取路徑

除了上述排除的委託人之外，請確保在主控台授權政策意外封鎖登入時，提供替代的存取方法：

- 角色型程式設計存取：主控台授權政策僅適用於互動式主控台登入。它們不適用於使用 SigV4 簽署的 API 請求。如果您有程式設計存取（例如，現有的存取金鑰、跨帳戶角色），請使用它來呼叫signin:DeleteConsoleAuthorizationConfiguration和移除限制政策。登入資料必須包含signin:DeleteConsoleAuthorizationConfiguration許可（包含在AWSSignInResourcePolicyManagement受管政策中）。 AWS 建議暫時登入資料而非長期 IAM 使用者存取金鑰。對於成員帳戶，管理帳戶管理員可以在成員帳戶 (aws sts assume-role) OrganizationAccountAccessRole中擔任 ，以取得這些臨時登入資料。
- AWS 支援復原：將您的根使用者帳戶電子郵件和電話號碼保持在最新狀態。如果排除主體和程式設計存取都無法使用， AWS Support 可以在身分驗證後提供復原入口網站連結。如需完整復原程序啟用主控台授權後，我的帳戶遭到鎖定，請參閱 。

生產部署前測試

AWS 建議您在未徹底測試政策對帳戶的影響之前，不要將限制性 RCPs 連接到組織的根目錄。反之，請建立 OU，您可以將帳戶一次移入一個，或至少以小數字移動，以確保您不會不小心將使用者鎖定在金鑰帳戶之外。

測試工作流程：

1. 使用主要網路限制建立單一許可陳述式。
2. 在非生產帳戶中啟用主控台授權。
3. 從允許和拒絕的網路測試主控台存取。
4. 檢閱 Amazon CloudTrail 日誌以確認政策評估行為。
5. 使用已排除的主體測試存取權。
6. 逐漸擴展到其他網路和帳戶。
7. 在生產帳戶中強制執行之前進行監控。

深入defense-in-depth的設計

在更廣泛的安全策略中使用 AWS 以登入資源為基礎的政策和資源控制政策作為一層。 AWS 登入政策會根據網路位置和主體身分限制主控台存取。將它們與其他政策類型結合，以建立全面的存取控制：

- AWS 登入政策 （以資源為基礎的政策和 RCPs)：根據驗證之前、期間和之後的網路位置和主體身分來限制主控台存取。
- IAM 政策：控制使用者在登入後可執行的動作。
- 服務控制政策 (SCPs)：在所有主體之間套用整個組織的許可護欄。
- VPC 端點政策：控制可以透過 VPC 端點存取哪些服務和帳戶。

持續監控和稽核

AWS CloudTrail 會自動記錄所有 AWS 登入政策評估和組態變更。在 CloudTrail 事件歷史記錄中檢視這些事件長達 90 天。如需更長的保留期，請透過建立線索將事件交付至 Amazon S3 （請參閱建立線索)。如需即時警示，請建立符合 AWS 登入事件的 Amazon EventBridge 規則、將線索設定為交付至 CloudWatch Logs 日誌群組，以用於指標篩選條件型警示，或將事件轉送至現有的 SIEM 解決方案。

使用案例

網路周邊強制執行

限制主控台存取公司 VPCs或核准的 IP 範圍。針對個別帳戶使用資源型政策，或針對整個組織強制執行使用資源控制政策 (RCPs)，以確保使用者只能從信任的網路位置登入，防止來自公有或不受信任網路的未經授權存取。

範例案例：公司要求所有主控台存取都來自其公司網路或核准的 AWS VPCs。他們會為單一帳戶或整個組織的 RCP 設定資源型政策，拒絕從所有其他網路存取，同時維護緊急管理員的緊急復原存取權。

合規要求

符合網路型存取控制的法規要求。許多合規架構要求組織根據網路位置限制對敏感系統的存取。AWS 登入政策提供可稽核且可執行的控制，以證明符合這些要求。

範例案例：金融服務公司必須遵循僅從核准網路存取主控台的法規。他們使用 RCPs 來強制執行整個組織的網路限制，並維護 AWS CloudTrail 日誌作為合規證據。

多帳戶控管

跨 AWS Organizations 實作一致的主控台存取政策。使用 RCPs 對所有成員帳戶強制執行標準網路限制，確保一致的安全狀態，而無需個別帳戶層級組態。

範例案例：擁有 100 個以上 AWS 帳戶的企業使用 RCPs來強制執行政策，要求所有主控台存取來自其組織內的 VPC 端點，以確認所有帳戶的網路控制一致。

第三方存取控制

將暫時主控台存取權授予特定網路的合作夥伴或承包商。組織可以為外部各方建立限時、網路受限的主控台存取，而不會影響整體安全狀態。

範例案例：公司需要授予諮詢公司臨時主控台存取權。他們建立以資源為基礎的政策，僅允許從諮詢公司的已知 IP 範圍存取，也僅允許指派給顧問的 IAM 角色存取。

限制主控台對特定主體的存取

僅允許一組定義的主體登入 AWS 管理主控台，並拒絕所有其他主體，無論網路位置為何。這對於未使用 VPC 端點且想要身分型主控台限制的客戶非常有用。拒絕主控台登入的主體會保留其程式設計存取； AWS 登入政策只會將主控台登入設為閘道，而且只有您豁免的主體可以登入。

範例案例：公司只想要其管理員使用 主控台。他們會設定 RCP，拒絕管理員主體 ARNs 以外的所有主體的主控台登入。具有有效登入資料的 Amazon EC2 執行個體角色無法登入 主控台，因為它

不是豁免的主體，即使其保留其程式設計許可。這解決了執行個體角色登入資料用於主控台登入的常見案例。

對主控台存取控制進行故障診斷

由於以資源為基礎的登入政策中的網路條件，我無法登入

當 AWS 登入政策拒絕存取時，您可能會看到下列其中一個錯誤訊息：

- 「您的身分驗證資訊不正確。請再試一次。」（以資源為基礎的政策拒絕驗證前）
- 「驗證失敗 無效的請求」(RCP 拒絕驗證前）
- 「驗證失敗：若要存取此帳戶，請從不同的網路登入，或聯絡您的管理員以取得詳細資訊」（驗證後拒絕）

如果您看到任何這些錯誤，且認為應該允許存取，請聯絡您的 AWS 管理員。他們可以檢閱 CloudTrail 日誌中是否有`errorMessage`「因資源型政策而拒絕授權」或「因資源控制政策而拒絕授權」`ConsoleLogin`的事件，以識別哪些政策陳述式拒絕存取。

可能原因：

- 您的來源 IP 地址不在允許的 CIDR 範圍內。
- 您未連線到所需的 VPC 或 VPC 端點。
- 您正在存取的區域登入端點不符合政策中的預期區域。
- 您的委託人 ARN 未正確列在政策的排除委託人中。
- 政策最近已更新，變更尚未全域複寫。

解決方法：

- 確認您已連線至公司網路或 VPN。
- 如果已設定 VPC 端點型限制，請確認您正在透過正確的 VPC 端點存取 。
- 請聯絡您的 AWS 管理員以驗證政策組態，並確認哪些網路已獲授權。
- 如果您設定為排除主體，請確認您的主體 ARN 在排除主體清單中已正確設定。
- 如果最近進行了政策變更，請等待幾分鐘讓全域複寫完成。

對於診斷此問題的管理員：

- 檢閱政策評估事件的 AWS CloudTrail 日誌，以識別哪些政策陳述式拒絕存取。
- 使用 `aws signin get-resource-policy` 來檢閱目前的政策組態。
- 確認使用者的網路位置符合政策中的條件。
- 如果使用者應免於網路限制，請確認已正確設定排除的主體。

啟用主控台授權後，我的帳戶遭到鎖定

如果您已設定主控台授權，且 無法再存取您的帳戶，則在強制執行政策之前，您可能尚未設定排除的委託人。

有多個路徑可以重新取得存取權，具體取決於您的帳戶類型和可用的登入資料。

選項 1：使用程式設計存取 (AWS CLI 或 SDK)

主控台授權政策僅適用於互動式主控台登入。它們不適用於使用 SigV4 簽署的 API 請求。如果您有程式設計存取（例如，現有的存取金鑰、跨帳戶角色），請使用它來呼叫`signin:DeleteConsoleAuthorizationConfiguration`和移除限制政策。您使用的登入資料必須具有呼叫 的許可`signin:DeleteConsoleAuthorizationConfiguration`。AWSSignInResourcePolicyManageme受管政策包含此 permission. AWS recommends temporary credentials over long-term IAM user access key。對於成員帳戶，管理帳戶管理員可以在成員帳戶中擔任`OrganizationAccountAccessRole` ，以取得臨時登入資料。此角色不會在受邀加入組織的帳戶中自動建立。

```
aws signin delete-console-authorization-configuration \
  --target-id <your-aws-account-id> \
  --region us-east-1
```

或刪除特定許可陳述式：

```
# First, list statements to get the statement ID
aws signin list-resource-permission-statements \
  --region us-east-1

# Then delete the problematic statement
aws signin delete-resource-permission-statement \
  --statement-id <statement-id> \
  --region us-east-1
```

選項 2：聯絡 AWS 支援

如果您沒有程式設計存取權，且無法使用 `OrganizationAccountAccessRole` 進行帳戶存取，請聯絡 AWS Support 以啟動鎖定復原程序。

復原程序的運作方式如下：

1. 如果您無法使用上述選項解決問題，請在支援中心開立 AWS 支援案例。 AWS 支援將在檢查您的帳戶之前驗證您的身分。驗證方法可能包括確認根使用者帳戶電子郵件地址、回應電話驗證呼叫，或回答帳戶安全問題。
2. AWS 支援確認主控台存取問題是由資源型政策鎖定所造成。
3. AWS 支援會共用復原入口網站連結。使用此連結，在具有 `signin:DeleteConsoleAuthorizationConfiguration`許可的帳戶中使用 IAM 主體登入。此許可允許主體刪除導致鎖定的主控台授權組態。

> **Important**
>
> 復原入口網站會移除帳戶的整個主控台授權組態，包括所有資源許可陳述式。復原入口網站不允許重新設定以資源為基礎的 AWS 登入政策。

復原入口網站連結會在 AWS Support 共用 72 小時後過期。如果您沒有在該時段內完成復原，請聯絡 AWS Support 以重新啟動程序。

重新取得存取權之後：

- 檢閱並更新您的資源許可陳述式，以包含正確設定的已排除主體。
- 在重新啟用主控台授權之前，從預期的網路測試主控台存取。
- 記錄您的復原程序以供日後參考。

我所做的變更不一定都會立刻生效

政策變更會全域複寫，但複寫可能需要幾分鐘的時間。

解決方法：

- 進行政策變更以完成全域複寫後，請等待幾分鐘。
- 使用 `get-resource-policy`命令驗證您的變更：

```
aws signin get-resource-policy --region <your-region>
```

- 檢查政策評估事件的 AWS CloudTrail 日誌，以確認正在評估新政策。
- 確認您為操作使用正確的區域（寫入操作必須使用 us-east-1)。
- 如果使用 VPC 端點型條件，請確認 VPC 端點政策也已正確設定。

常見的政策複寫問題：

- 快取的登入頁面：瀏覽器可能會快取登入頁面。清除您的瀏覽器快取或使用 incognito 視窗來測試政策變更。
- 衝突陳述式：如果您有多個許可陳述式，請確認它們不會彼此衝突。使用 get-resource-policy來檢閱合併政策。
- VPC 端點政策： AWS 登入政策可與 VPC 端點政策搭配使用。兩者都必須允許所需的存取。

AWS 登入條件金鑰參考

此頁面列出您可以在 AWS 登入資源型政策和資源控制政策 (RCPs) 中使用的條件金鑰，並顯示每個金鑰適用的評估階段和動作。只有 `signin:PrincipalArn` 專屬 AWS 於 Sign-In；其他則是 AWS 全域條件金鑰。如需全域金鑰定義，請參閱AWS 全域條件內容金鑰。

如需服務授權參考中動作和條件索引鍵的完整清單，請參閱 AWS Sign-In 的動作、資源和條件索引鍵。

網路型條件金鑰

這些條件索引鍵會檢查請求的來源。 AWS 登入會針對資源型政策和 RCPs 中的所有 AWS 登入動作 (`signin:Authenticate`、 `signin:AuthorizeOAuth2Access`和 `signin:CreateOAuth2Token`) 進行評估。

網路型條件金鑰

條件鍵	運算子	說明	使用規則
`aws:SourceIp`	`IpAddress` ， `NotIpAddress`	公有 IP 地址或 CIDR 範圍	當請求使用 VPC 端點時不存在。在相同陳述式中與 VPC 型條件結合使用`IfExists`運算子。
`aws:SourceVpc`	`StringEquals` ， `StringNotEquals`	VPC ID (`vpc-xxxxxxxx`)	只有在請求使用 VPC 端點時才會出現。搭配 使用 `aws:RequestedRegion` 以防止跨區域 VPC ID 衝突。
`aws:SourceVpce`	`StringEquals` ， `StringNotEquals`	VPC 端點 ID (`vpce-xxxxxxxx`)	只有在請求使用 VPC 端點時才會出現。
`aws:VpcSourceIp`	`IpAddress` ， `NotIpAddress`	VPC 內的私有 IP	一律使用 `aws:VpcSourceIp` 條件金鑰搭配 `aws:SourceVpc` 或

條件鍵	運算子	說明	使用規則
			aws:SourceVpce 條件金鑰。
aws:RequestedRegion	StringEquals，StringNotEquals	目標 AWS 區域碼	建議在使用時aws:SourceVpc 防止跨區域 VPC ID 衝突。您可以指定多個區域。

> **Important**
>
> 單一請求包含 aws:SourceIp（公有網路）或 aws:SourceVpc(VPC 端點），而非兩者。撰寫涵蓋兩個路徑的拒絕政策時，請使用IfExists運算子（例如 NotIpAddressIfExists) 或建立個別的陳述式。

身分型條件索引鍵

這些條件索引鍵會檢查提出請求的人員。它們僅適用於驗證後動作 (signin:AuthorizeOAuth2Access 和 signin:CreateOAuth2Token)，其中已建立主體身分。

身分型條件索引鍵

條件鍵	運算子	說明	範例
aws:PrincipalArn	ArnEquals，ArnLike, ArnNotEquals，StringEquals，StringLike	已驗證 IAM 主體的 ARN	arn:aws:iam::123456789012:user/alice，arn:aws:iam::123456789012:role/Admin
aws:PrincipalAccount	StringEquals，StringNotEquals	AWS 委託人的帳戶 ID	123456789012

服務特定條件金鑰：signin：PrincipalArn

下列條件金鑰專屬 AWS 於 Sign-In，不是全域 AWS 金鑰。僅在驗證前評估期間可用。在身分驗證完成之前`signin:PrincipalArn`，使用 識別起始登入的委託人。這是 的預先驗證對等項目`aws:PrincipalArn`，在驗證之後才能使用。

運算子

ARN 運算子 (`ArnEquals`、`ArnLike`、`ArnNotEquals`、`ArnNotLike`) 和字串運算子 (`StringEquals`、`StringLike`)。

可用性

AWS 登入會在驗證前階段 (`signin:Authenticate`動作) 的請求內容中包含此金鑰。它不適用於驗證後動作 (`signin:AuthorizeOAuth2Access` 和 `signin:CreateOAuth2Token`)。

資料類型

ARN。使用 ARN 運算子而非字串運算子。

值類型

單一值。

支援於

以資源為基礎的政策和 RCPs。

使用 ARN 運算子來比較值。您可以指定下列委託人類型：

- AWS 帳戶 根使用者 (`arn:aws:iam::123456789012:root`)
- IAM 使用者 (`arn:aws:iam::123456789012:user/`*`user-name`*)
- IAM 角色 (`arn:aws:iam::123456789012:role/`*`role-name`*)

使用案例：將排除的主體身分排除在網路限制之外，防止鎖定，同時仍對所有其他存取嘗試強制執行網路控制。

範例 – 拒絕來自未經授權網路的預先驗證存取，根使用者除外：

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:Authenticate"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "signin:PrincipalArn": "arn:aws:iam::123456789012:root"
        },
        "NotIpAddress": {
          "aws:SourceIp": "203.0.113.0/24"
        },
        "StringEquals": {
          "aws:ResourceAccount": "123456789012"
        }
      }
    },
    {
      "Effect": "Deny",
      "Principal": { "AWS": "*" },
      "Action": ["signin:CreateOAuth2Token", "signin:AuthorizeOAuth2Access"],
      "Resource": "*",
      "Condition": {
        "ArnNotEquals": {
          "aws:PrincipalArn": "arn:aws:iam::123456789012:root"
        },
        "NotIpAddress": {
          "aws:SourceIp": "203.0.113.0/24"
        },
        "StringEquals": {
          "aws:ResourceAccount": "123456789012"
        }
      }
    }
  ]
}
```

此政策拒絕從 203.0.113.0/24 IP 範圍以外的主控台存取，但帳戶根使用者除外。預先驗證陳述式使用 在身分驗證完成之前signin:PrincipalArn豁免根使用者。身分驗證後陳述式會在 OAuth 權杖交換期間，aws:PrincipalArn使用 在身分驗證後豁免相同的委託人。請參閱 政策範例。

依動作的條件索引鍵可用性

依動作的條件索引鍵可用性

條件鍵	Signin：Authenticate	登入：AuthorizeOAuth2Access	signin：CreateOAuth2Token
aws:SourceIp	是	是	是
aws:SourceVpc	是	是	是
aws:SourceVpce	是	是	是
aws:VpcSourceIp	是	是	是
aws:RequestedRegion	是	是	是
aws:PrincipalArn	–	是	是
aws:PrincipalAccount	–	是	是
signin:PrincipalArn	是	–	–

> **Note**
>
> signin:CreateAccount 動作僅用於主控台私有存取的 VPC 端點政策，不適用於資源型政策或 RCPs。沒有與之相關聯的服務特定條件索引鍵。請參閱主控台私有存取。

相關資訊

- 使用以資源為基礎的政策和資源控制政策來控制主控台存取
- AWS 管理主控台 私有存取
- AWS 全域條件內容鍵
- AWS Sign-In 的動作、資源和條件索引鍵

登入您的 AWS 存取入口網站

IAM Identity Center 中的使用者是 的成員 AWS Organizations。IAM Identity Center 中的使用者可以使用特定的登入 URL 登入您的 AWS 存取入口網站，以存取多個 AWS 帳戶 和商業應用程式。如需特定登入 URL 的詳細資訊，請參閱 AWS 存取入口網站。

在 IAM Identity Center 中以使用者 AWS 帳戶 身分登入 之前，請先收集下列必要資訊。

- 公司使用者名稱
- 公司密碼
- 特定登入 URL

> **Note**
>
> 登入後，您的 AWS 存取入口網站工作階段有效期為 8 小時。您必須在 8 小時後再次登入。

登入您的 AWS 存取入口網站

1. 在瀏覽器視窗中，將您透過電子郵件提供的登入 URL 貼上，例如 `https://your_subdomain.awsapps.com/start`或雙堆疊 URL 格式 `https://[IAM Identity Center instance ID].portal.[Region].app.aws`。然後按 Enter 鍵。
2. 使用您的公司登入資料（例如使用者名稱和密碼）登入。

   > **Note**
   >
   > 如果您的管理員向您傳送電子郵件一次性密碼 (OTP)，而這是您第一次登入，請輸入該密碼。登入後，您必須為未來的登入建立新密碼。

3. 如果系統要求您提供驗證碼，請檢查您的電子郵件。然後將程式碼複製並貼到登入頁面。

   > **Note**
   >
   > 驗證碼通常透過電子郵件傳送，但交付方法可能會有所不同。如果您的電子郵件中尚未收到驗證碼，請洽詢您的管理員以取得驗證碼的詳細資訊。

4. 如果已在 IAM Identity Center 中為您的使用者啟用 MFA，您可以使用它進行身分驗證。
5. 身分驗證之後，您可以存取入口網站中出現的任何 AWS 帳戶 和 應用程式。

   a. 若要登入， AWS 管理主控台 請選擇帳戶索引標籤，然後選取要管理的個別帳戶。

      使用者的 角色隨即顯示。選擇帳戶的角色名稱以開啟 AWS 管理主控台。選擇存取金鑰以取得命令列或程式設計存取的登入資料。

   b. 選擇應用程式索引標籤以顯示可用的應用程式，然後選擇您要存取的應用程式圖示。

在 IAM Identity Center 中以使用者身分登入，可為您提供登入資料，以在設定的期間內存取資源，稱為工作階段。根據預設，使用者可以登入 AWS 帳戶 8 小時。IAM Identity Center 管理員可以指定不同的持續時間，從最短 15 分鐘到最長 90 天。工作階段結束後，您可以再次登入。

其他資訊

如果您想要 IAM Identity Center 中使用者的詳細資訊，請參閱下列資源。

- 如需 IAM Identity Center 的概觀，請參閱什麼是 IAM Identity Center？
- 如需 AWS 存取入口網站的詳細資訊，請參閱使用 AWS 存取入口網站。
- 如需 IAM Identity Center 工作階段的詳細資訊，請參閱使用者身分驗證。
- 如需如何重設 IAM Identity Center 使用者密碼step-by-step說明，請參閱 我忘記 的 IAM Identity Center 密碼 AWS 帳戶。
- 如果您或您的組織實作 IP 或網域篩選，您可能需要允許列出網域，以建立和使用您的 AWS 存取入口網站。IAM Identity Center 同時支援 IPv4 和雙堆疊端點。如果您的網路使用 IPv6，請使用雙堆疊端點網域。如需允許列出網域的詳細資訊，請參閱 要新增至允許清單的網域。

透過 登入 AWS Command Line Interface

您必須建立 的 AWS CLI 身分驗證方式 AWS。選擇最適合您工作流程和安全需求的方法。

- 使用主控台登入資料登入 （建議） 如果您使用根帳戶、IAM 使用者或 IAM 聯合 AWS 帳戶存取。
- 使用 IAM Identity Center 登入資料登入 如果您使用 Identity Center 進行 AWS 帳戶存取。

使用主控台登入資料登入 （建議）

此身分驗證方法可讓您將主控台登入資料與 搭配使用 AWS CLI，讓您可以在帳戶設定後的幾分鐘內以 AWS 程式設計方式開始使用 。您可以取得跨本機開發工具無縫運作的臨時登入資料，例如 AWS CLI、 AWS SDKs 和 AWS Tools for PowerShell。

先決條件

- 安裝 AWS CLI。如需詳細資訊，請參閱安裝或更新至最新版本的 AWS CLI。使用 `aws login`命令需要 2.32.0 的最低版本。
- 以 AWS 管理主控台 根使用者、IAM 使用者或透過 IAM 聯合身分登入的存取權。如果您使用 IAM Identity Center，請使用 IAM Identity Center 登入資料登入改為前往 。
- 確保 IAM 身分具有適當的許可。將 SignInLocalDevelopmentAccess 受管政策連接至您的 IAM 使用者、角色或群組。如果您以根使用者身分登入，則不需要額外的許可。

使用主控台登入資料登入

1. 執行下列命令以啟動瀏覽器型身分驗證程序：

```
$ aws login
```

`aws login` 命令支援數個選用參數：

- `aws login --remote` - 在您的裝置不支援瀏覽器時，用於跨裝置身分驗證

> **Note**
>
> 您可以控制對相同裝置 (`aws login`) 和跨裝置 (`aws login --remote`) 身分驗證的存取。在任何相關的 IAM 政策中使用下列資源 ARNs。

    - arn:aws:signin:*region*:*account-id*:oauth2/public-client/localhost — 使用此 ARN 搭配 進行相同的裝置身分驗證aws login。
    - arn:aws:signin:*region*:*account-id*:oauth2/public-client/remote — 使用此 ARN 與 進行跨裝置身分驗證aws login --remote。

  - aws login --profile *profile-name* - 使用特定設定檔進行身分驗證
  - aws login --region *region* - 在特定區域中進行身分驗證

2. 遵循終端機中的提示。命令會自動開啟您的預設瀏覽器，並引導您完成身分驗證程序。身分驗證成功後，您的 AWS CLI 工作階段有效期最長為 12 小時。
3. 若要結束工作階段，請使用：

```
$ aws logout
```

如果您使用 以程式設計方式存取 AWS 服務 AWS Tools for PowerShell，請參閱使用 AWS 驗證適用於 PowerShell 的 AWS 工具。如果您使用的是 AWS SDKs，請參閱使用 AWS SDKs和工具進行身分驗證和存取。

使用 IAM Identity Center 登入資料登入

AWS 存取入口網站可讓 IAM Identity Center 使用者輕鬆選取 ， AWS 帳戶 並取得 的臨時安全登入資料 AWS CLI。如需如何取得這些登入資料的詳細資訊，請參閱 的區域可用性 AWS 建構家 ID。您也可以 AWS CLI 直接將 設定為使用 IAM Identity Center 驗證使用者。

使用 IAM Identity Center 登入資料登入

1. 確認您已完成先決條件。
2. 如果您是第一次登入，請使用aws configure sso精靈設定您的設定檔。
3. 設定設定檔後，請執行下列命令，然後依照終端機中的提示操作：

```
$ aws sso login --profile my-profile
```

其他資訊

如果您想要使用命令列登入的詳細資訊，請參閱下列資源。

- 如需使用主控台登入資料進行 AWS 本機開發的詳細資訊，請參閱 AWS CLI 的身分驗證和存取登入資料。
- 如需 AWS CLI 登入程序的詳細資訊，請參閱使用 的短期憑證進行驗證 AWS CLI。
- 如需 IAM Identity Center 組態的詳細資訊，請參閱設定 AWS CLI 以使用 IAM Identity Center。

以聯合身分身分登入

聯合身分是可以存取具有外部身分之安全 AWS 帳戶 資源的使用者。外部身分可以是來自公司身分存放區 (例如 LDAP 或 Windows Active Directory) 或來自第三方 (例如 Login with Amazon, Facebook, or Google)。聯合身分不會使用 AWS 管理主控台 或 AWS 存取入口網站登入。使用中的外部身分類型決定聯合身分如何登入。

管理員必須建立包含 的自訂 URL`https://signin.aws.amazon.com/federation`。如需詳細資訊，請參閱啟用 的自訂身分代理程式存取權 AWS 管理主控台。

> **Note**
>
> 您的管理員會建立聯合身分。如需如何以聯合身分身分登入的詳細資訊，請聯絡您的管理員。

如需聯合身分的詳細資訊，請參閱關於 Web 聯合身分。

使用 登入 AWS 建構家 ID

AWS 建構家 ID 是個人設定檔，可讓您存取特定工具和服務，包括 Amazon CodeCatalyst、Amazon Q Developer 和 AWS 培訓 和 Certification。 會以個人身分 AWS 建構家 ID 代表您，並與現有 AWS 帳戶中可能擁有的任何登入資料和資料無關。如同其他個人設定檔，隨著您的個人、教育和職業目標的進展， AWS 建構家 ID 會與您一起。

您的 AWS 建構家 ID 補充 AWS 帳戶 您可能已經擁有或想要建立的任何 。雖然 AWS 帳戶 做為您建立 AWS 之資源的容器，並為這些資源提供安全界限，但您的 AWS 建構家 ID 代表您做為個人。如需詳細資訊，請參閱AWS 建構家 ID 和其他 AWS 登入資料。

AWS 建構家 ID 是免費的。您只需為 中消耗 AWS 的資源付費 AWS 帳戶。如需定價的詳細資訊，請參閱 AWS 定價。

如果您或您的組織實作 IP 或網域篩選，您可能需要允許列出網域來建立和使用 AWS 建構家 ID。如需允許列出網域的詳細資訊，請參閱 要新增至允許清單的網域。

> **Note**
>
> AWS Builder ID 與您的 AWS Skill Builder 訂閱是獨立的線上學習中心，您可以在其中向 AWS 專家學習並線上建置雲端技能。如需 AWS 技能建置器的詳細資訊，請參閱AWS 技能建置器。

主題

- AWS 建構家 ID 和其他 AWS 登入資料

使用 登入 AWS 建構家 ID

1. 導覽至您要存取 AWS 的工具或服務AWS 建構家 ID 設定檔或登入頁面。例如，若要存取 Amazon CodeCatalyst，請前往 https://codecatalyst.aws。
2. 選擇如何登入您的 AWS 建構家 ID
   - 我有現有的 帳戶
   - 我有 Google 帳戶
   - 我有 Apple 帳戶
   - 我有 GitHub 帳戶
   - 我有 Amazon 帳戶

我有現有的 帳戶

1. 對於現有帳戶，輸入您用來建立 的電子郵件 AWS 建構家 ID ，然後選擇登入。
2. 輸入您用來建立 的電子郵件 AWS 建構家 ID ，然後選擇登入。
3. 在使用您的 登入 AWS 建構家 ID頁面上，輸入您的密碼。
4. （選用）如果您希望此裝置的未來登入不會提示進行其他驗證，請勾選這是受信任裝置旁的方塊。
5. 選擇繼續。
6. 如果出現其他驗證必要頁面的提示，請依照瀏覽器的指示提供必要的程式碼或安全金鑰。

> **Note**
>
> 為了您的安全，我們會分析您的登入瀏覽器、位置和裝置。如果您告訴我們信任此裝置，則不必在每次登入時提供多重要素驗證 (MFA) 代碼。如需詳細資訊，請參閱信任的裝置。

我有 Google 帳戶

如果您的 Google 帳戶已與 建立關聯 AWS 建構家 ID，您必須使用不同的電子郵件地址來登入應用程式。如需詳細資訊，請參閱我無法使用 Google 登入。

1. 若要使用您的 Google 帳戶登入 AWS 建構家 ID，請選擇使用 Google 繼續。
2. 在使用 Google 登入頁面上，輸入 Google 帳戶登入的資訊。
3. 選擇繼續載入 AWS 應用程式首頁。

我有 Apple 帳戶

如果您的 Apple 帳戶已與 建立關聯 AWS 建構家 ID，您必須使用不同的電子郵件地址來登入應用程式。如需詳細資訊，請參閱我無法使用 Apple 登入。

1. 若要使用您的 Apple 帳戶登入 AWS 建構家 ID，請選擇使用 Apple 繼續。
2. 在使用 Apple 登入頁面上，輸入 Apple 帳戶登入的資訊。
3. 選擇繼續載入 AWS 應用程式首頁。

我有 GitHub 帳戶

如果您的 GitHub 帳戶已與 建立關聯 AWS 建構家 ID，您必須使用不同的電子郵件地址來登入應用程式。如需詳細資訊，請參閱我無法使用 GitHub 登入。

1. 若要使用您的 GitHub 帳戶登入 AWS 建構家 ID，請選擇繼續使用 GitHub。
2. 在使用 GitHub 登入頁面上，輸入 GitHub 帳戶登入的資訊。
3. 選擇繼續以載入 AWS 應用程式首頁。

我有 Amazon 帳戶

如果您的 Amazon 帳戶已與 建立關聯 AWS 建構家 ID，您必須使用不同的電子郵件地址來登入應用程式。如需詳細資訊，請參閱我無法使用 Amazon 登入。

1. 若要使用您的 Amazon 帳戶登入 AWS 建構家 ID，請選擇繼續使用 Amazon。
2. 在使用 Amazon 登入頁面上，輸入 Amazon 帳戶登入的資訊。
3. 選擇繼續載入 AWS 應用程式首頁。

的區域可用性 AWS 建構家 ID

AWS 建構家 ID 在以下提供 AWS 區域。使用 的應用程式 AWS 建構家 ID 可能會在其他 區域中運作。

名稱	Code
美國東部 (維吉尼亞北部)	us-east-1

建立您的 AWS 建構家 ID

您可以在註冊其中一個使用它的 AWS 工具和服務 AWS 建構家 ID 時建立 。使用您的電子郵件地址、名稱和密碼註冊，作為 AWS 工具或服務註冊程序的一部分。

您的密碼必須遵循下列要求：

- 密碼區分大小寫。
- 密碼長度必須介於 8 到 64 個字元之間。
- 密碼必須至少包含以下四個類別中的一個字元：
  - 小寫字母 (a-z)
  - 大寫字母 (A-Z)
  - 數字 (0-9)
  - 非英數字元 (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- 最後三個密碼無法重複使用。
- 無法使用透過從第三方洩露的資料集公開知道的密碼。

> **Note**
>
> 使用 的工具和服務會 AWS 建構家 ID 指示您 AWS 建構家 ID 在需要時建立和使用您的 。

建立您的 AWS 建構家 ID

1. 導覽至您要存取 AWS 的工具或服務AWS 建構家 ID 設定檔或註冊頁面。例如，若要存取 Amazon CodeCatalyst，請前往 https://codecatalyst.aws。
2. 選擇如何建立您的 AWS 建構家 ID
   - 若要使用您的 Google 帳戶，請選擇繼續 Google，然後依照提示完成註冊程序。這會略過下面的步驟 3-8。前往步驟 9。

- 若要使用您的 Apple 帳戶，請選擇繼續 Apple，然後依照提示完成註冊程序。這會略過下面的步驟 3-8。前往步驟 9。

  > **Note**
  >
  > 如果您選擇為使用 Apple 登入啟用 iCloud+「隱藏我的電子郵件」功能， AWS 建構家 ID 則會使用 Apple 帳戶中指定的隱藏我的電子郵件地址來建立您的 ，而不是實際的電子郵件地址。您將無法變更此電子郵件地址，但您的名字和姓氏仍然可以編輯。如果您需要登入 AWS 建構家 ID，您應該使用隱藏我的電子郵件地址。 AWS 建構家 ID 會使用隱藏我的電子郵件地址來傳送電子郵件通訊給您。如需詳細資訊，請參閱如何搭配 Sign in with Apple 使用隱藏我的電子郵件。

- 若要使用您的 GitHub 帳戶，請選擇繼續使用 GitHub，然後依照提示完成註冊程序。這會略過下面的步驟 3-8。前往步驟 9。
- 若要使用您的 Amazon 帳戶，請選擇繼續 Amazon，然後依照提示完成註冊程序。這會略過下面的步驟 3-8。前往步驟 9。
- 若要使用電子郵件和密碼建立 帳戶，請繼續執行下列步驟。

3. 在建立 AWS 建構家 ID頁面上，輸入您的電子郵件地址。我們建議您使用個人電子郵件。
4. 選擇下一步。
5. 輸入您的名稱，然後選擇下一步。
6. 在電子郵件驗證頁面上，輸入我們傳送到您電子郵件地址的驗證碼。選擇 Verify (驗證)。根據您的電子郵件提供者，您可能需要幾分鐘的時間才能收到電子郵件。檢查您的垃圾郵件和垃圾郵件資料夾是否有程式碼。如果您在五分鐘 AWS 後沒有看到來自 的電子郵件，請選擇重新傳送程式碼。
7. 在我們驗證您的電子郵件後，在選擇密碼頁面上，輸入密碼和確認密碼。
8. 如果 Captcha 顯示為額外的安全性，請輸入您看到的字元。
9. 選擇建立 AWS 建構家 ID。

信任的裝置

從登入頁面選取 這是受信任的裝置 選項之後，我們會考慮該裝置上該 Web 瀏覽器的所有未來登入。這表示您不需要在該信任的裝置上提供 MFA 代碼。不過，如果您的瀏覽器、Cookie 或 IP 地址變更，您可能必須使用 MFA 代碼進行其他驗證。

AWS 使用 的工具和服務 AWS 建構家 ID

您可以使用 登入 AWS 建構家 ID ，以存取下列 AWS 工具和服務。存取收費提供的功能或利益需要 AWS 帳戶。

根據預設，當您使用 登入 AWS 工具或服務時 AWS 建構家 ID，工作階段持續時間會持續 30 天，但 Amazon Q Developer 除外，其工作階段持續時間為 90 天。工作階段結束後，您將需要再次登入。

AWS 雲端社群

Community.aws 是 和 的平台，適用於您可以使用 存取的 AWS 建置器社群 AWS 建構家 ID。您可以在這裡探索教育內容、分享您的個人想法和專案、評論其他人的文章，以及追蹤您最愛的建置者。

Amazon CodeCatalyst

當您開始使用 Amazon CodeCatalyst AWS 建構家 ID 時，您將建立 ，並選擇與問題、程式碼遞交和提取請求等活動相關聯的別名。邀請其他人到您的 Amazon CodeCatalyst 空間，該空間包含您團隊建置下一個成功專案所需的工具、基礎設施和環境。您需要 AWS 帳戶 才能將新專案部署至雲端。

AWS Migration Hub

使用 存取 AWS Migration Hub（遷移中樞） AWS 建構家 ID。Migration Hub 提供單一位置來探索現有的伺服器、規劃遷移，以及追蹤每個應用程式遷移的狀態。

Amazon Q Developer

Amazon Q Developer 是採用生成式 AI 技術的對話式助理，可協助您了解、建置、擴展和操作 AWS 應用程式。如需詳細資訊，請參閱《Amazon Q Developer 使用者指南》中的 What is Amazon Q Developer? 部分。

AWS re:Post

AWS re:Post 為您提供專家技術指導，讓您可以使用 AWS 服務更快地創新並提高營運效率。您可以使用 登入 AWS 建構家 ID ，並在 re：Post 上加入社群，無需使用 AWS 帳戶 或 信用卡。

AWS 新創公司

使用 AWS 建構家 ID 加入AWS 新創公司，您可以在其中使用學習內容、工具、資源和支援來擴展您的新創公司 AWS。

AWS 培訓 和 認證

您可以使用 AWS 建構家 ID 存取 AWS 培訓 和 認證，您可以在其中使用 AWS Skill Builder 建置 AWS 雲端 技能、向 AWS 專家學習，以及使用業界認可的憑證驗證您的雲端專業知識。

Kiro

Kiro 是一種代理 IDE，可協助您透過規格驅動的開發，從原型進入生產環境。從簡單到複雜的任務，Kiro 會與您一起將提示轉換為詳細規格，然後轉換為工作程式碼、文件和測試。使用 Kiro，您建置的內容完全是您想要的內容，並且已準備好與您的團隊共用。Kiro 的代理程式可協助您解決具有挑戰性的問題，並自動化產生文件和單元測試等任務。使用 Kiro，您可以建置超越原型的 ，同時在過程中的每個步驟都處於駕駛位置。

網站註冊入口網站 (WRP)

您可以使用 AWS 建構家 ID 做為AWS 行銷網站的持久性客戶身分和註冊設定檔。若要註冊新的網路研討會，以及檢視您已註冊或參加的所有網路研討會，請參閱我的網路研討會。

編輯您的 AWS 建構家 ID 設定檔

您可以隨時變更設定檔資訊。您可以編輯用來建立 的電子郵件地址和名稱 AWS 建構家 ID，以及暱稱。使用 Google 或 Apple 等社交登入時，只能編輯名稱和暱稱。

您的名稱是您在與他人互動時在工具和服務中被提及的方式。您的暱稱指出您希望如何被 AWS、朋友和與您緊密合作的其他人知道。

> **Note**
>
> 使用 的工具和服務會 AWS 建構家 ID 指示您 AWS 建構家 ID 在需要時建立和使用您的 。

編輯您的設定檔資訊

1. 在 登入您的 AWS 建構家 ID 設定檔https://profile.aws.amazon.com。
2. 選擇我的詳細資訊。
3. 在我的詳細資訊頁面上，選擇設定檔旁的編輯按鈕。
4. 在編輯設定檔頁面上，對名稱和暱稱進行任何所需的變更。
5. 選擇儲存變更。頁面頂端會出現綠色確認訊息，讓您知道您已更新設定檔。

> **Note**
>
> 使用我們其中一個其他登入合作夥伴變更您的名稱和暱稱，並不會更新您 的相同設定 AWS 建構家 ID。

若要編輯您的聯絡資訊

1. 在 登入您的 AWS 建構家 ID 設定檔https://profile.aws.amazon.com。
2. 選擇我的詳細資訊。
3. 在我的詳細資訊頁面上，選擇聯絡資訊旁的編輯按鈕。
4. 在編輯聯絡資訊頁面上，變更您的電子郵件地址。
5. 選擇驗證電子郵件。隨即出現對話方塊。
6. 在驗證電子郵件對話方塊中，收到電子郵件中的代碼後，在驗證碼中輸入代碼。選擇 Verify (驗證)。

變更 AWS 建構家 ID 您的密碼

您的密碼必須遵循下列要求：

- 密碼區分大小寫。
- 密碼長度必須介於 8 到 64 個字元之間。
- 密碼必須至少包含以下四個類別中的一個字元：
  - 小寫字母 (a-z)
  - 大寫字母 (A-Z)
  - 數字 (0-9)
  - 非英數字元 (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- 最後三個密碼無法重複使用。

> **Note**
>
> 密碼變更不適用於使用 Google 或 Apple 等社交登入 AWS 建構家 ID 的帳戶。如果您使用社交登入來登入，您可以透過社交登入帳戶來管理您的密碼。若要變更社交登入的密碼：
>
> - 如需 Google 帳戶，請參閱變更或重設您的 (Google) 密碼。

- 對於 Apple 帳戶，請參閱變更您的 Apple 帳戶密碼。
- 如需 GitHub 帳戶，請參閱更新您的 GitHub 存取憑證。
- 對於 Amazon 帳戶，請參閱如何變更 Amazon 密碼。

變更 AWS 建構家 ID 您的密碼

1. 在 登入您的 AWS 建構家 ID 設定檔https://profile.aws.amazon.com。
2. 選擇 Security (安全性)。
3. 在安全頁面上，選擇變更密碼。這會帶您前往新頁面。
4. 在重新輸入密碼頁面的密碼下，輸入您目前的密碼。然後選擇登入。
5. 在變更密碼頁面的新密碼下，輸入您要使用的新密碼。然後在確認密碼下，重新輸入您要使用的新密碼。
6. 選擇變更密碼。系統會將您重新導向至您的 AWS 建構家 ID 設定檔。

刪除您 的所有作用中工作階段 AWS 建構家 ID

在登入裝置下，您可以檢視目前登入的所有裝置。如果您無法辨識裝置，基於安全最佳實務，請先變更您的密碼，然後在任何地方登出。您可以在 安全頁面上刪除所有作用中的工作階段，以登出所有裝置 AWS 建構家 ID。

> **Note**
>
> AWS 建構家 ID 支援 IDE 中 Amazon Q Developer 的 90 天延伸工作階段。對於每個新的 IDE 登入，您可以看到兩個工作階段項目。當您登出 IDE 時，即使 IDE 工作階段不再有效，您也可以繼續查看已登入裝置下列出的 IDE 工作階段。這些工作階段會在 90 天過期後消失。

刪除所有作用中工作階段

1. 在 登入您的 AWS 建構家 ID 設定檔https://profile.aws.amazon.com。
2. 選擇 Security (安全性)。
3. 在安全頁面上，選擇刪除所有作用中的工作階段。
4. 在刪除所有工作階段對話方塊中，輸入全部刪除。透過刪除所有工作階段，您可以登出使用 登入的所有裝置 AWS 建構家 ID，包括不同的瀏覽器。然後選擇刪除所有工作階段。

> **Note**
>
> 使用 Google 或 Apple 等社交登入帳戶時，刪除作用中 AWS 建構家 ID 工作階段不會將您登出社交登入帳戶。

刪除您的 AWS 建構家 ID

下列程序說明如何刪除 AWS 建構家 ID 您的帳戶。

> **Warning**
>
> 刪除您的 AWS 建構家 ID 將導致下列情況：
>
> - 無法存取 – 您無法再存取先前透過 存取的任何 AWS 工具和服務 AWS 建構家 ID。您的 AWS 建構家 ID 與您可能擁有的任何 AWS 帳戶是分開的，刪除您的 AWS 建構家 ID 不會關閉 AWS 您的帳戶。
> - 內容刪除 – AWS 建構家 ID 將刪除僅與您的 相關聯的任何剩餘內容，您將無法再使用 從應用程式存取或復原內容 AWS 建構家 ID。
> - 個人資訊刪除 – 您在建立和管理 時提供的任何個人資訊 AWS 建構家 ID 都會遭到刪除，但 AWS 可能會依法律要求或允許保留個人資訊，例如您刪除請求的記錄，或以無法識別您身分的形式保留資料。
>
>   您可以在 AWS 隱私權聲明中進一步了解我們如何處理您的資訊。您可以前往 AWS Communications Preferences Center 更新您的 AWS 通訊偏好設定或取消訂閱。
> - 社交登入帳戶保持不變 – 如果您使用 Google 或 Apple 等社交登入，刪除 AWS 建構家 ID 不會刪除與您的社交登入帳戶相關的任何內容。請參閱社交登入供應商的文件，了解如何刪除這些帳戶。從社交登入帳戶刪除 AWS 建構家 ID 連線並不會刪除 AWS 建構家 ID 您的帳戶，但您將無法再存取您的 AWS 建構家 ID 設定檔。

刪除您的 AWS 建構家 ID

1. 在 登入您的 AWS 建構家 ID 設定檔https://profile.aws.amazon.com。
2. 選擇隱私權和資料。
3. 在隱私權與資料頁面的刪除 AWS 建構家 ID下，選擇刪除 AWS 建構家 ID。
4. 選取每個免責聲明旁的核取方塊，以確認您已準備好繼續進行。

5. 選擇刪除 AWS 建構家 ID。

管理 AWS 建構家 ID 多重要素驗證 (MFA)

多重要素驗證 (MFA) 是一種簡單且有效的機制，可增強您的安全性。第一個因素：您的密碼，是您記住的秘密，也稱為知識因素。其他因素可以是擁有因素 (您擁有的事物，例如安全金鑰) 或繼承因素 (您自身的事物，例如生物特徵掃描)。我們強烈建議您設定 MFA，為您的 新增額外的 layer AWS 建構家 ID。

您可以註冊內建驗證器，也可以註冊您保存在實體安全位置的安全金鑰。如果您無法使用內建驗證器，則可以使用已註冊的安全金鑰。對於驗證器應用程式，您也可以在這些應用程式中啟用雲端備份或同步功能。如果您遺失或損壞 MFA 裝置，這可協助您避免失去對設定檔的存取權。

重點

- 我們建議您註冊多個 MFA 裝置。如果您無法存取所有已註冊的 MFA 裝置，您將無法復原您的 AWS 建構家 ID。
- 我們建議您定期檢閱已註冊的 MFA 裝置，以確保它們是最新且正常運作的。此外，您應該將這些裝置存放在不使用時實際安全的位置。
- 如果您使用繼續 Google 建立帳戶，您可以透過 Google 帳戶啟用多重驗證。如需詳細資訊，請參閱開啟2-Step驗證。
- 如果您使用 Continue with Apple 建立帳戶，您的 Apple 帳戶中可能已啟用多重驗證。如果沒有，如需如何啟用的詳細資訊，請參閱 Apple 帳戶的雙重驗證。
- 如果您使用繼續 GitHub 建立帳戶，您可以透過 GitHub 帳戶啟用多重驗證。如需詳細資訊，請參閱設定 (GitHub) 雙重驗證。
- 如果您使用 Continue with Amazon 建立帳戶，您可以透過 Amazon 帳戶啟用多重驗證。如需詳細資訊，請參閱什麼是兩步驟驗證？。

的可用 MFA 類型 AWS 建構家 ID

AWS 建構家 ID 支援下列多重要素驗證 (MFA) 裝置類型。

FIDO2 驗證器

FIDO2 是包含 CTAP2 和 WebAuthn 的標準，以公有金鑰密碼編譯為基礎。FIDO 登入資料具有網路釣魚防護，因為它們對建立登入資料的網站是唯一的，例如 AWS。

AWS 支援 FIDO 驗證器的兩種最常見形式因素：內建驗證器和安全金鑰。如需 FIDO 驗證器最常見類型的詳細資訊，請參閱下文。

主題

- 內建驗證器
- 安全金鑰
- 密碼管理器、通行金鑰提供者和其他 FIDO 驗證器

內建驗證器

有些裝置具有內建驗證器，例如 MacBook 上的 TouchID 或 Windows Hello 相容攝影機。如果您的裝置與 FIDO 通訊協定相容，包括 WebAuthn，您可以使用指紋或臉部作為第二個因素。如需詳細資訊，請參閱 FIDO 身分驗證。

安全金鑰

您可以購買與 FIDO2-compatible外部 USB、BLE 或 NFC 連接的安全金鑰。系統提示您輸入 MFA 裝置時，請輕觸金鑰的感應器。YubiKey 或 Feitian 會建立相容的裝置。如需所有相容安全金鑰的清單，請參閱 FIDO 認證產品。

密碼管理器、通行金鑰提供者和其他 FIDO 驗證器

多個第三方供應商支援行動應用程式中的 FIDO 身分驗證，作為密碼管理員、具有 FIDO 模式的智慧卡和其他規格尺寸的功能。這些 FIDO 相容裝置可與 IAM Identity Center 搭配使用，但建議您先自行測試 FIDO 驗證器，再為 MFA 啟用此選項。

> **Note**
>
> 有些 FIDO 驗證器可以建立可探索的 FIDO 登入資料，稱為通行金鑰。通行金鑰可能繫結至建立通行金鑰的裝置，也可能可同步並備份至雲端。例如，您可以在支援的 Macbook 上使用 Apple Touch ID 註冊通行金鑰，然後在 iCloud 中使用 Google Chrome 搭配通行金鑰從 Windows 筆記型電腦登入 網站，方法是遵循登入時的螢幕提示。如需哪些裝置支援作業系統和瀏覽器之間的可同步通行金鑰和目前通行金鑰互通性的詳細資訊，請參閱 passkeys.dev 中的裝置支援，這是 FIDO Alliance and World Wide Web Consortium (W3C) 維護的資源。

驗證器應用程式

驗證器應用程式是一次性密碼 (OTP) 型第三方身分驗證器。您可以使用安裝在行動裝置或平板電腦上的驗證器應用程式，做為授權的 MFA 裝置。第三方驗證器應用程式必須符合 RFC 6238，這是標準型的一次性密碼 (TOTP) 演算法，能夠產生六位數驗證碼。

提示輸入 MFA 時，您必須在顯示的輸入方塊中輸入來自驗證器應用程式的有效代碼。每個指派給使用者的 MFA 裝置都必須是唯一的。您可以為任何指定的使用者註冊兩個驗證器應用程式。

您可以從下列知名的第三方驗證器應用程式進行選擇。不過，任何符合 TOTP 的應用程式都適用於 AWS 建構家 ID MFA。

作業系統	已測試的驗證器應用程式
Android	1Password、Authy、Duo Mobile、Microsoft Authenticator、Google Authenticator
iOS	1Password、Authy、Duo Mobile、Microsoft Authenticator、Google Authenticator

註冊您的 AWS 建構家 ID MFA 裝置

> **Note**
>
> 註冊 MFA、登出，然後在同一個裝置上登入後，可能不會提示您在信任的裝置上輸入 MFA。

使用驗證器應用程式註冊您的 MFA 裝置

1. 在 登入您的 AWS 建構家 ID 設定檔https://profile.aws.amazon.com。
2. 選擇 Security (安全性)。
3. 在安全頁面上，選擇註冊裝置。
4. 在註冊 MFA 裝置頁面上，選擇驗證器應用程式。
5. AWS 建構家 ID 會操作和顯示組態資訊，包括 QR 程式碼圖形。圖形是「秘密組態金鑰」的表示，可在不支援 QR 代碼的驗證器應用程式中手動輸入。
6. 開啟您的驗證器應用程式。如需應用程式清單，請參閱 驗證器應用程式。

如果驗證器應用程式支援多個 MFA 裝置或帳戶，請選擇建立新 MFA 裝置或帳戶的選項。

7. 判斷 MFA 應用程式是否支援 QR 代碼，然後在設定您的驗證器應用程式頁面上執行下列其中一項操作：

   1. 選擇顯示 QR 碼，然後使用應用程式掃描 QR 碼。例如，您可以選擇攝影機圖示或選擇類似於掃描碼的選項。然後使用裝置的相機掃描程式碼。
   2. 選擇顯示私密金鑰，然後在 MFA 應用程式中輸入該私密金鑰。

   完成後，您的驗證器應用程式將產生並顯示一次性密碼。

8. 在驗證器程式碼方塊中，輸入目前出現在驗證器應用程式中的一次性密碼。選擇 Assign MFA (指派 MFA)。

   > **Important**
   >
   > 產生代碼之後立即提交您的請求。如果您產生程式碼，然後等待太久才提交請求，則 MFA 裝置已成功與您的 建立關聯 AWS 建構家 ID，但 MFA 裝置不同步。會發生這種情況是因為定時式的一次性密碼 (TOTP) 在過了一小段時間後就會過期。這種情況下，您可以重新同步裝置。如需詳細資訊，請參閱當我嘗試使用驗證器應用程式註冊或登入時，收到「發生意外錯誤」訊息。

9. 若要在 中為裝置命名易記的名稱 AWS 建構家 ID，請選擇重新命名。此名稱可協助您區分此裝置與您註冊的其他裝置。

MFA 裝置現在可以與 搭配使用 AWS 建構家 ID。

將安全金鑰註冊為您的 AWS 建構家 ID MFA 裝置

使用安全金鑰註冊您的 MFA 裝置

1. 在 登入您的 AWS 建構家 ID 設定檔https://profile.aws.amazon.com。
2. 選擇 Security (安全性)。
3. 在安全頁面上，選擇註冊裝置。
4. 在註冊 MFA 裝置頁面上，選擇安全金鑰。
5. 確保您的安全金鑰已啟用。如果您使用單獨的實體安全金鑰，請將其連接到您的電腦。
6. 遵循畫面上的指示。您的體驗會根據您的作業系統和瀏覽器而有所不同。

7. 若要在 中為裝置命名易記的名稱 AWS 建構家 ID，請選擇重新命名。此名稱可協助您區分此裝置與您註冊的其他裝置。

MFA 裝置現在可以與 搭配使用 AWS 建構家 ID。

重新命名您的 AWS 建構家 ID MFA 裝置

重新命名 MFA 裝置

1. 在 登入您的 AWS 建構家 ID 設定檔https://profile.aws.amazon.com。
2. 選擇 Security (安全性)。當您抵達頁面時，您會看到重新命名呈現灰色。
3. 選取您要變更的 MFA 裝置。這可讓您選擇重新命名。接著會出現對話方塊。
4. 在開啟的提示中，在 MFA 裝置名稱中輸入新名稱，然後選擇重新命名。重新命名的裝置會顯示在多重要素驗證 (MFA) 裝置下。

刪除您的 MFA 裝置

我們建議您保留兩個或多個作用中的 MFA 裝置。移除裝置之前，請參閱 註冊您的 AWS 建構家 ID MFA 裝置 以註冊替代 MFA 裝置。若要停用 的多重要素驗證 AWS 建構家 ID，請從設定檔中移除所有已註冊的 MFA 裝置。

刪除 MFA 裝置

1. 在 登入您的 AWS 建構家 ID 設定檔https://profile.aws.amazon.com。
2. 選擇 Security (安全性)。
3. 選取您要變更的 MFA 裝置，然後選擇刪除。
4. 在刪除 MFA 裝置？模態中，依照指示刪除您的裝置。
5. 選擇 刪除。

刪除的裝置不會再出現在多重要素驗證 (MFA) 裝置下。

中的隱私權和資料 AWS 建構家 ID

AWS 隱私權聲明概述了我們處理您個人資料的方式。如需如何刪除 AWS 建構家 ID 設定檔的資訊，請參閱 刪除您的 AWS 建構家 ID。

請求 AWS 建構家 ID 您的資料

您可以請求和檢視與 相關聯的個人資訊， AWS 建構家 ID 以及您使用 存取 AWS 的應用程式和服務 AWS 建構家 ID。如需行使資料主體權利的詳細資訊，包括與其他 AWS 網站、應用程式、產品、服務、事件和體驗相關的個人資訊，請參閱 https://aws.amazon.com/privacy。

請求您的資料

1. 在 登入您的 AWS 建構家 ID 設定檔https://profile.aws.amazon.com。
2. 選擇我的 AWS 建構家 ID 資料。
3. 在我的 AWS 建構家 ID 資料頁面的刪除 AWS 建構家 ID下，選擇請求您的資料。
4. 綠色確認訊息會出現在我們收到您的請求的頁面頂端，並在 30 天內完成。
5. 當您收到我們的電子郵件，指出請求已處理，請導覽回 AWS 建構家 ID 設定檔的隱私權與資料頁面。選擇使用您的資料下載 ZIP 封存的新可用按鈕。

   當資料請求處於待定狀態時，您將無法刪除您的 AWS 建構家 ID。

AWS 建構家 ID 和其他 AWS 登入資料

您的 AWS 建構家 ID 與任何 AWS 帳戶 或 登入憑證分開。您可以為 AWS 建構家 ID 和 的根使用者電子郵件使用相同的電子郵件 AWS 帳戶。

AWS 建構家 ID：

- 可讓您存取 使用的工具和服務 AWS 建構家 ID。
- 不會影響現有的安全控制，例如您在 AWS 帳戶 或 應用程式中指定的政策和組態。
- 不會取代任何現有的根、IAM Identity Center 或 IAM 使用者、憑證或帳戶。
- 無法取得 IAM AWS 登入資料來存取 AWS 管理主控台、、 AWS CLI AWS SDKs或 AWS Toolkit。

AWS 帳戶 是具有聯絡人和付款資訊的資源容器。它建立了安全界限，在其中操作計費和計量 AWS 服務，例如 S3, EC2 或 Lambda。帳戶擁有者可以在 AWS 帳戶 中登入 AWS 管理主控台。如需詳細資訊，請參閱登入 AWS 管理主控台。

與您現有 IAM Identity Center 身分 AWS 建構家 ID 的關係

身為擁有您管理身分的個人 AWS 建構家 ID。它與您在其他組織可能擁有的任何其他身分無關，例如學校或工作。您可以在 IAM Identity Center 中使用人力資源身分來代表自己的工作，並使用 AWS 建構家 ID 來代表自己的私有身分。這些身分會獨立運作。

IAM Identity Center AWS (AWS 單一登入的後繼者） 中的使用者是由公司 IT 或雲端管理員，或組織身分提供者的管理員管理，例如 Okta、Ping 或 Azure。IAM Identity Center 中的使用者可以跨多個帳戶存取資源 AWS Organizations。

多個 AWS 建構家 ID 設定檔

AWS 建構家 ID 只要每個 ID 使用唯一的電子郵件地址，您就可以建立多個電子郵件地址。不過，使用多個 AWS 建構家 ID 可能會讓您難以回想 AWS 建構家 ID 您用於哪個用途。如果可能，建議您 AWS 建構家 ID 在 AWS 工具和服務中的所有活動中使用單一 。

登出 AWS

登出 的方式 AWS 帳戶 取決於您是哪種類型的 AWS 使用者。您可以是帳戶根使用者、IAM 使用者、IAM Identity Center 中的使用者、聯合身分或 AWS 建置器 ID 使用者。如果您不確定自己是哪種類型的使用者，請參閱 判斷您的使用者類型。

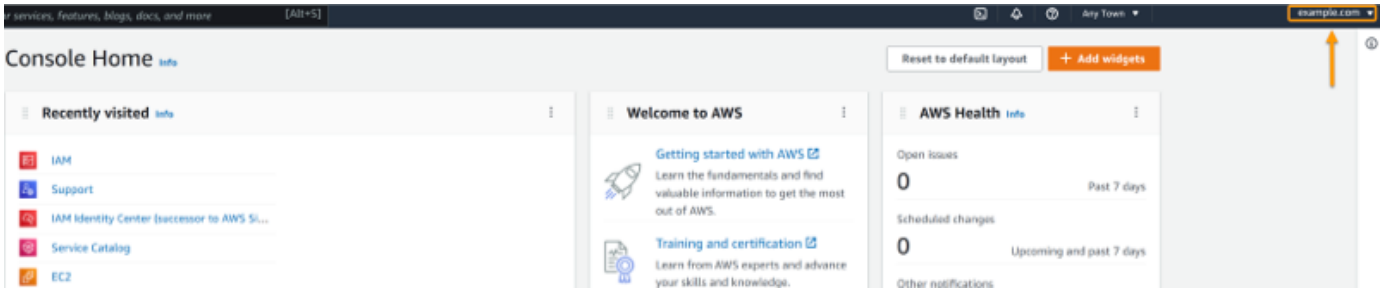
主題

- 登出 AWS 管理主控台
- 登出您的 AWS 存取入口網站
- 登出 AWS Builder ID

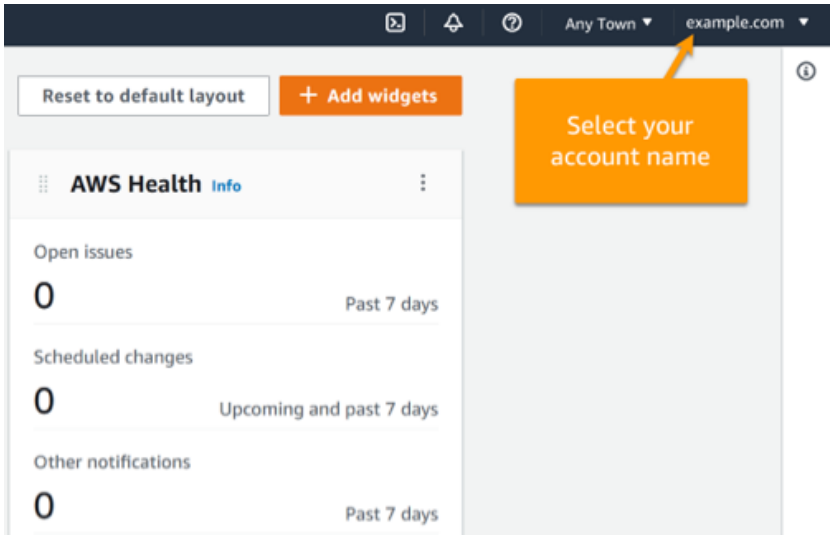
登出 AWS 管理主控台

登出 AWS 管理主控台

1. 登入 後 AWS 管理主控台，您會抵達類似下圖所示的頁面。您的帳戶名稱或 IAM 使用者名稱會顯示在右上角。



2. 在右上角的導覽列中，選擇您的使用者名稱。



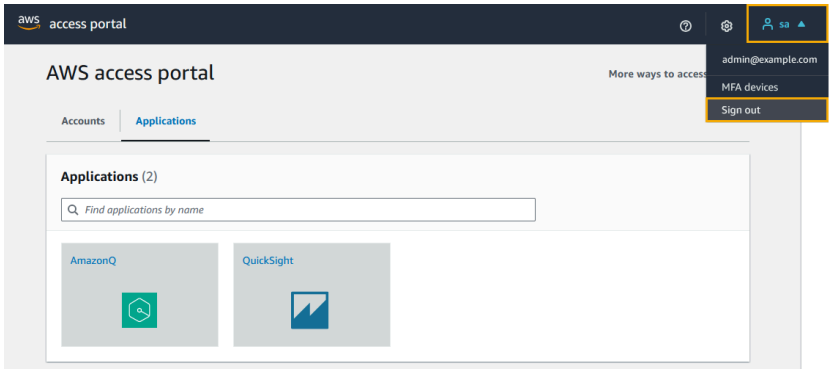
3. 選擇登出選項。按鈕選項會根據您登入的帳戶數量而有所不同。
   - 如果您只登入一個帳戶，請選取登出。
   - 選取登出所有工作階段，以同時登出所有身分。
   - 選取登出目前工作階段以登出您選取的身分。
4. 您將返回 AWS 管理主控台 網頁。

如需登入多個帳戶的詳細資訊，請參閱AWS 管理主控台 《 入門指南》中的登入多個帳戶。

登出您的 AWS 存取入口網站

登出您的 AWS 存取入口網站

1. 在右上角的導覽列中，選擇您的使用者名稱。
2. 選取登出，如下圖所示。



3. 如果您成功登出，您現在會看到您的 AWS 存取入口網站登入頁面。

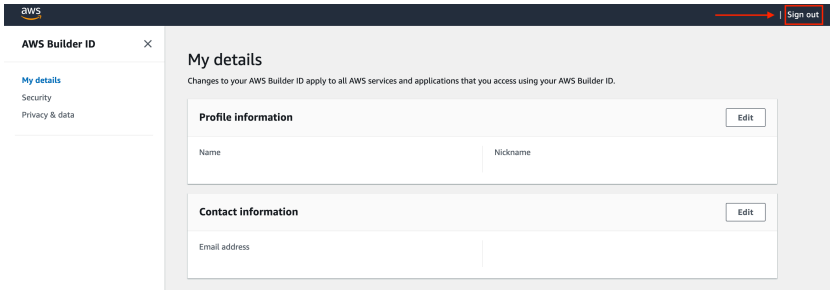
如果您使用外部身分提供者 (IdP) 做為身分來源，當您登出時，不會終止憑證的作用中工作階段。如果您導覽回 AWS 存取入口網站，則可能會自動登入，而無需提供您的登入資料。

登出 AWS Builder ID

若要使用 AWS Builder ID 登出您已存取 AWS 的服務，您必須登出該服務。如果您想要登出 AWS 您的建置器 ID 設定檔，請參閱下列程序。

登出您的 AWS 建置器 ID 設定檔

1. 在 登入 AWS 建置器 ID 設定檔後https://profile.aws.amazon.com/，您會抵達我的詳細資訊。
2. 在 AWS 建置器 ID 設定檔頁面的右上角，選擇登出。



3. 當您不再看到 AWS 您的建置器 ID 設定檔時，系統會將您登出。

對 AWS 帳戶 登入問題進行故障診斷

使用此處的資訊來協助您對登入和其他 AWS 帳戶 問題進行疑難排解。如需登入 step-by-step說明 AWS 帳戶，請參閱 登入 AWS 管理主控台。

如果沒有故障診斷主題可協助您解決登入問題，您可以填寫此表格 支援 來使用 建立案例：我是 AWS 客戶，正在尋找帳單或帳戶支援。作為安全最佳實務， 支援 無法討論您登入帳戶 AWS 帳戶 以外的任何 的詳細資訊。AWS Support 也無法因任何原因變更與帳戶相關聯的登入資料。

> **Note**
>
> 支援 不會發佈直接聯絡支援代表的電話號碼。

如需有關對登入問題進行故障診斷的更多協助，請參閱如果我無法登入或存取我的 該怎麼辦 AWS 帳戶？ 如果您在登入 Amazon.com 時遇到問題，請參閱 Amazon Customer Service 而非此頁面。

主題

- 我的 AWS 管理主控台 登入資料無法運作
- 我的根使用者需要重設密碼
- 我無法存取我的 的電子郵件 AWS 帳戶
- 我的 MFA 裝置遺失或停止運作
- 我無法存取 AWS 管理主控台 登入頁面
- 由於以資源為基礎的登入政策中的網路條件，我無法登入
- 啟用主控台授權後，我的帳戶遭到鎖定
- 我的政策變更未生效
- 如何尋找我的 AWS 帳戶 ID 或別名
- 我需要我的帳戶驗證碼
- 我忘記 的根使用者密碼 AWS 帳戶
- 我忘記 的 IAM 使用者密碼 AWS 帳戶
- 我忘記我的 的聯合身分密碼 AWS 帳戶
- 我無法登入現有的 AWS 帳戶 ，也無法使用 AWS 帳戶 相同的電子郵件地址建立新的
- 我需要重新啟用已暫停的 AWS 帳戶
- 我需要聯絡 支援 以解決登入問題

- 我需要聯絡 AWS Billing 處理帳單問題
- 我有關於零售訂單的問題
- 我需要管理我的 的協助 AWS 帳戶
- 我的 AWS 存取入口網站登入資料無法運作
- 我忘記 的 IAM Identity Center 密碼 AWS 帳戶
- 當我嘗試登入 IAM Identity Center 主控台時，我收到錯誤，指出「這不是您，而是我們」

我的 AWS 管理主控台 登入資料無法運作

如果您記得您的使用者名稱和密碼，但您的登入資料無法運作，您可能會在錯誤頁面。嘗試在其他頁面上登入：

根使用者登入頁面

- 如果您建立或擁有 ， AWS 帳戶 並正在執行需要根使用者登入資料的任務，請在 中輸入您的帳戶電子郵件地址AWS 管理主控台。若要了解如何存取根使用者，請參閱 以根使用者身分登入。如果您忘記根使用者密碼，就無法重設密碼。如需詳細資訊，請參閱我忘記 的根使用者密碼 AWS 帳戶。如果您忘記根使用者電子郵件地址，請檢查您的電子郵件收件匣是否有來自 的電子郵件 AWS。
- 如果您嘗試登入根使用者帳戶並收到錯誤：我的根使用者帳戶的密碼復原已停用，則您沒有根使用者登入資料。您無法以根使用者身分登入，也無法為帳戶的根使用者執行密碼復原。使用 管理 AWS 的成員帳戶 AWS Organizations 可能沒有根使用者密碼、存取金鑰、簽署憑證或作用中的多重要素驗證 (MFA)。

  只有 IAM 的管理帳戶或委派管理員可以在您的成員帳戶中執行根使用者動作。如果需要執行要求根使用者憑證的任務，請聯絡您的管理員。如需詳細資訊，請參閱AWS Identity and Access Management 《 使用者指南》中的集中管理成員帳戶的根存取權。

IAM 使用者登入頁面

- 如果您或其他人在 中建立 IAM 使用者 AWS 帳戶，您必須知道該 AWS 帳戶 ID 或別名才能登入。在 中輸入您的帳戶 ID 或別名、使用者名稱和密碼AWS 管理主控台。若要了解如何存取 IAM 使用者登入頁面，請參閱 以 IAM 使用者身分登入。如果您忘記 IAM 使用者密碼，請參閱 我忘記 的 IAM 使用者密碼 AWS 帳戶 以取得重設 IAM 使用者密碼的相關資訊。如果您忘了帳戶號碼，請搜尋您的電子郵件、瀏覽器我的最愛或瀏覽器歷史記錄中包含 `signin.aws.amazon.com/` 的 URL。您的帳戶 ID 或別名將跟隨 URL 中的 `"account="` 文字。如果您找不到帳戶 ID 或別名，請聯絡您的管理員。支援 無法協助您復原此資訊。在登入之後，您才能看到您的帳戶 ID 或別名。

我的根使用者需要重設密碼

為了保護您的帳戶，當您嘗試登入 時，您可能會收到下列訊息 AWS 管理主控台：

密碼重設是必要的。基於安全性考量，您需要重設密碼。若要保護您的帳戶安全，您必須在下面選擇忘記密碼並重設密碼。

除了此訊息之外， AWS 也會在我們透過與您帳戶相關聯的電子郵件識別潛在問題時通知您。此電子郵件包含需要重設密碼的原因。例如，當我們發現您 的異常登入活動， AWS 帳戶 或與您的 相關聯的登入資料， AWS 帳戶 都可在線上公開取得。

更新您的密碼，以確保您的根使用者登入資料保持安全。若要了解如何重設根使用者密碼，請參閱我忘記我的根使用者密碼 AWS 帳戶。

我無法存取我的 的電子郵件 AWS 帳戶

建立 時 AWS 帳戶，您會提供電子郵件地址和密碼。這些是 AWS 帳戶根使用者的登入資料。如果您不確定與 相關聯的電子郵件地址 AWS 帳戶，請尋找以 @signin.aws 或 @verify.signin.aws 結尾的已儲存通訊到您的組織可能已用於開啟 的任何電子郵件地址 AWS 帳戶。詢問團隊、組織或家人的其他成員。如果您認識的人建立了帳戶，他們可以協助您取得存取權。

如果您知道電子郵件地址，但無法存取該電子郵件，請先嘗試使用以下其中一個選項復原對電子郵件的存取：

- 如果您擁有電子郵件地址的網域，您可以還原刪除的電子郵件地址。或者，您可以為您的電子郵件帳戶設定全部截獲，這會「截獲」所有傳送到已不在郵件伺服器上電子郵件地址的訊息，並將這些訊息重新引導到另一個電子郵件地址。
- 如果帳戶上的電子郵件地址屬於您的公司電子郵件系統，我們建議您與 IT 系統管理員聯絡。這也許有助您重新取得電子郵件的存取許可。

如果您仍然無法登入您的 AWS 帳戶，您可以聯絡 尋找替代支援選項 支援。

我的 MFA 裝置遺失或停止運作

如果您的 MFA 裝置遺失、損壞或無法運作，當您傳送 MFA 驗證請求時，不會收到一次性密碼 (OTP)。

IAM 使用者

您可以使用向相同 IAM 使用者註冊的另一個 MFA 裝置登入。

IAM 使用者必須聯絡管理員，以停用無法運作的 MFA 裝置。如果沒有管理員的協助，這些使用者將無法復原其 MFA 裝置。您的管理員通常是資訊技術 (IT) 人員，擁有 AWS 帳戶 比組織其他成員更高層級的 許可。此個人已建立您的帳戶，並為使用者提供其存取登入資料以登入。

根使用者

若要復原根使用者的存取權，您必須使用向相同根使用者註冊的另一個 MFA 裝置登入。然後，檢閱下列選項以復原或更新 MFA 裝置：

- 如需復原 MFA 裝置的step-by-step說明，請參閱 MFA 裝置遺失或停止運作時該怎麼辦？
- 如需如何更新 MFA 裝置電話號碼step-by-step說明，請參閱如何更新電話號碼以重設遺失的 MFA 裝置？
- 如需啟用 MFA 裝置的step-by-step說明，請參閱為 中的使用者啟用 MFA 裝置 AWS。
- 如果您無法復原 MFA 裝置，請聯絡 支援。

> **Note**
>
> IAM 使用者必須聯絡其管理員，以協助處理 MFA 裝置。 支援 無法協助 IAM 使用者處理 MFA 裝置問題。

我無法存取 AWS 管理主控台 登入頁面

如果您看不到登入頁面，則防火牆可能會封鎖網域。請聯絡您的網路管理員，根據您的使用者類型和登入方式，將下列網域或 URL 端點新增至 Web 內容篩選解決方案允許清單。

根使用者和 IAM 使用者	*.signin.aws.amazon.com
Amazon.com 帳戶登入	www.amazon.com
IAM Identity Center 使用者和第一方應用程式登入	• *.awsapps.com (http://awsapps.com/) • *.signin.aws

由於以資源為基礎的登入政策中的網路條件，我無法登入

如果您看到下列其中一個錯誤訊息，登入資源型政策或資源控制政策 (RCP) 可能會根據您的網路位置限制存取：

- 「您的身分驗證資訊不正確。請再試一次。」
- 「驗證失敗 無效的請求」
- 「驗證失敗：若要存取此帳戶，請從不同的網路登入，或聯絡您的管理員以取得詳細資訊」

如需詳細的故障診斷步驟由於以資源為基礎的登入政策中的網路條件，我無法登入，請聯絡您的管理員或參閱 。

啟用主控台授權後，我的帳戶遭到鎖定

如果您已設定主控台授權，且無法再存取您的帳戶，則可能不會在強制執行政策之前設定已排除的主體或緊急復原存取權。如需包含 AWS CLI 自助服務、 `OrganizationAccountAccessRole`和 AWS 支援選項的解析步驟，請參閱 啟用主控台授權後，我的帳戶遭到鎖定。

我的政策變更未生效

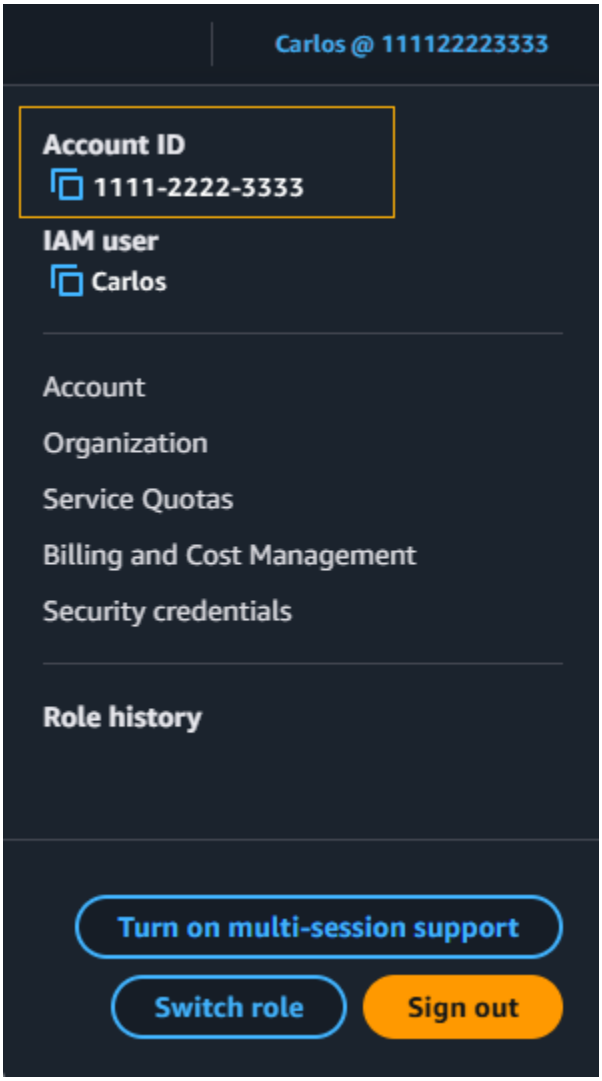
主控台授權組態和資源許可陳述式的變更會全域複寫，可能需要幾分鐘的時間才能生效。如果您的變更在等待後看不到，請參閱 我所做的變更不一定都會立刻生效以取得疑難排解步驟。

如何尋找我的 AWS 帳戶 ID 或別名

如果您是 IAM 使用者且未登入，請向管理員詢問 AWS 帳戶 ID 或別名。您的管理員通常是資訊技術 (IT) 人員，擁有 AWS 帳戶 比組織其他成員更高的 許可層級。此個人已建立您的帳戶，並為使用者提供其存取登入資料以登入。

如果您是可存取 的 IAM 使用者 AWS 管理主控台，您可以在登入 URL 中找到您的帳戶 ID。檢查您的管理員的電子郵件是否有登入 URL。帳戶 ID 是登入 URL 的前十二位數字。例如，在下列 URL 中，`https://111122223333.signin.aws.amazon.com/console`您的 AWS 帳戶 ID 為 111122223333。

登入 後 AWS 管理主控台，您可以在區域旁邊的導覽列中找到您的帳戶資訊。例如，在以下螢幕擷取畫面中，IAM 使用者 Carlos 的 AWS 帳戶 為 1111-2222-3333。



如需 AWS 帳戶 ID 和別名以及如何尋找 ID 的詳細資訊，請參閱您的 AWS 帳戶 ID 及其別名。

我需要我的帳戶驗證碼

如果您提供帳戶電子郵件地址和密碼， AWS 有時會要求您提供一次性驗證碼。若要擷取驗證碼，請檢查與您的 相關聯的電子郵件 AWS 帳戶 ，以取得來自 Amazon Web Services 的訊息。電子郵件地址以 @signin.aws 或 @verify.signin.aws 結尾。請遵循訊息中的指示進行。如果您在帳戶中沒有看到訊息，請檢查您的垃圾郵件資料夾。若您已沒有存取電子郵件的許可，請參閱 我無法存取我的 的電子郵件 AWS 帳戶。

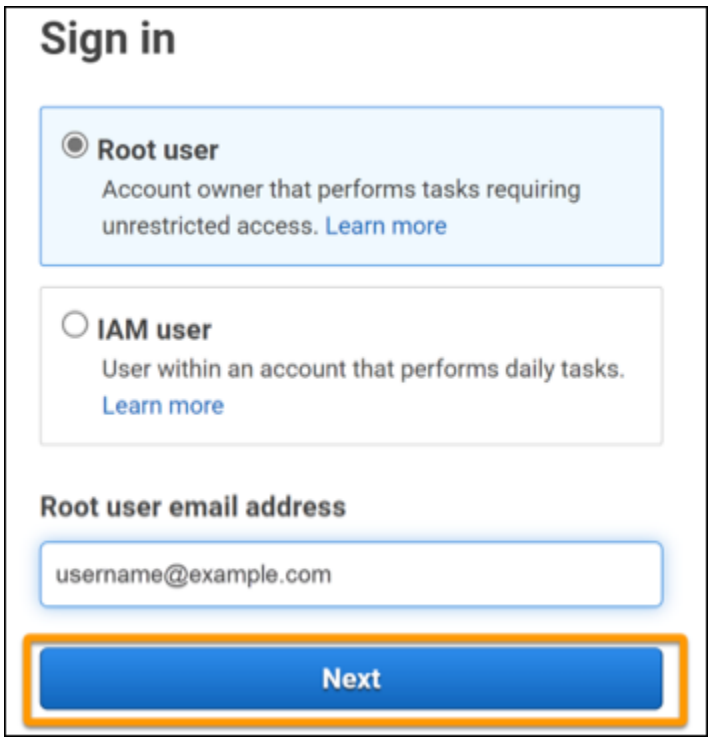
我忘記 的根使用者密碼 AWS 帳戶

如果您是根使用者，而且您遺失或忘記 的密碼 AWS 帳戶，您可以在 中選取「忘記密碼」連結來重設密碼 AWS 管理主控台。您必須知道 AWS 帳戶的電子郵件地址，而且必須能夠存取電子郵件帳戶。在密碼復原程序期間，您會收到重設密碼的連結。連結將傳送到您用來建立 的電子郵件地址 AWS 帳戶。

若要為您使用 AWS Organizations 建立的帳戶重設密碼，請參閱以根使用者身分存取成員帳戶。

若要重設您的根使用者密碼

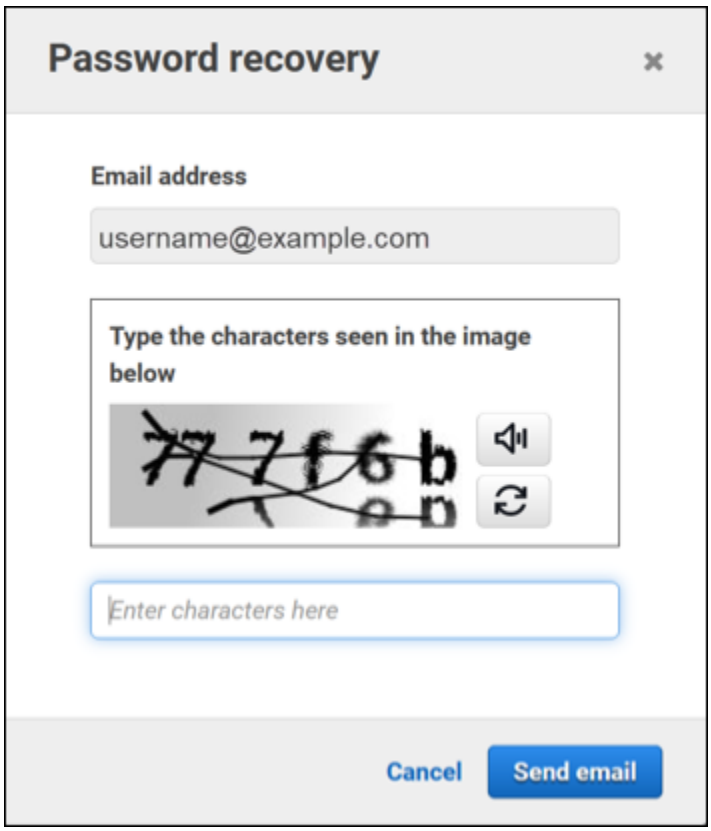
1. 使用 AWS 您的電子郵件地址開始以根使用者的身分登入 AWS 管理主控台。然後選擇下一步。



> **Note**
>
> 如果您AWS 管理主控台使用 IAM 使用者登入資料登入 ，則必須先登出，才能重設根使用者密碼。如果您看到帳戶專屬的 IAM 使用者登入頁面，請選擇頁面底部旁的 Sign-in using root account credentials (使用根帳戶憑證來登入)。如有需要，請提供您的帳戶電子郵件地址，然後選擇 Next (下一步)，以存取 Root user sign in (根使用者登入) 頁面。

2. 選擇忘記密碼？

3. 完成密碼復原步驟。如果您無法完成安全檢查，請嘗試聆聽音訊或重新整理一組新字元的安全檢查。下圖顯示密碼復原頁面的範例。

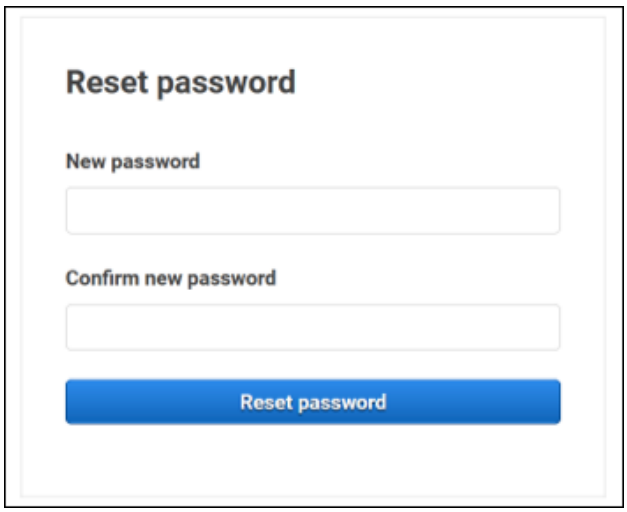


4. 完成密碼復原步驟後，您會收到一則訊息，指示已傳送至與您的 相關聯的電子郵件地址 AWS 帳戶。

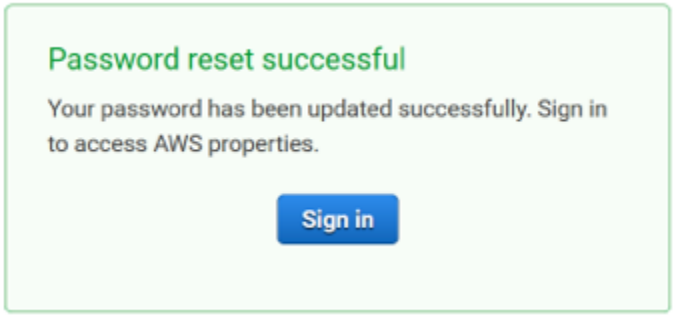
   包含重設密碼連結的電子郵件會傳送至用來建立 的電子郵件 AWS 帳戶。

> **Note**
>
> 電子郵件來自結尾為 @signin.aws 或 @verify.signin.aws 的地址。

5. 選取 AWS 電子郵件中提供的連結以重設您的 AWS 根使用者密碼。
6. 此連結會引導您前往新的網頁，以建立新的根使用者密碼。



您收到密碼重設成功的確認。成功重設密碼會顯示在下圖中。

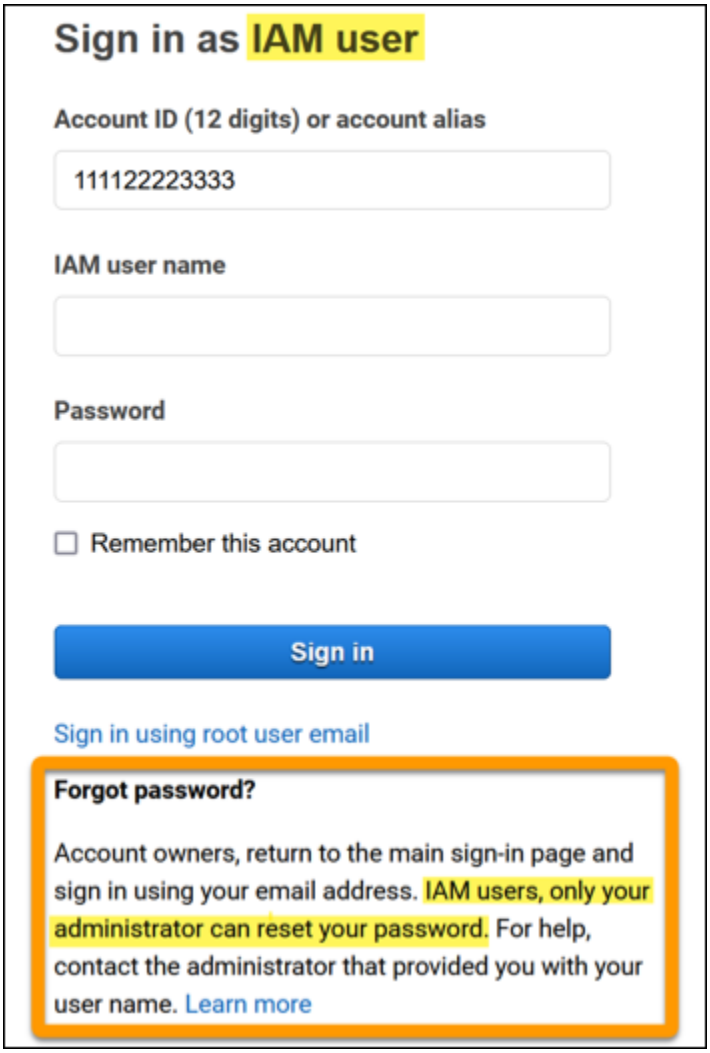


如需重設根使用者密碼的詳細資訊，請參閱如何復原遺失或忘記 AWS 的密碼？

我忘記 的 IAM 使用者密碼 AWS 帳戶

若要變更 IAM 使用者密碼，您必須擁有適當的許可。如需重設 IAM 使用者密碼的詳細資訊，請參閱 IAM 使用者如何變更自己的密碼。

如果您沒有重設密碼的許可，則只有您的 IAM 管理員可以重設 IAM 使用者密碼。IAM 使用者應聯絡其 IAM 管理員以重設密碼。您的管理員通常是資訊技術 (IT) 人員，擁有 AWS 帳戶 比組織其他成員更高層級的 許可。此個人已建立您的帳戶，並為使用者提供其存取登入資料以登入。



基於安全考量， 支援 無法存取、提供或變更您的登入資料。

如需重設 IAM 使用者密碼的詳細資訊，請參閱如何復原遺失或忘記 AWS 的密碼？

若要了解管理員如何管理您的密碼，請參閱管理 IAM 使用者的密碼。

我忘記我的 的聯合身分密碼 AWS 帳戶

聯合身分登入以 AWS 帳戶 使用外部身分存取 。使用中的外部身分類型決定聯合身分如何登入。您的管理員會建立聯合身分。如需如何重設密碼的詳細資訊，請洽詢您的管理員。您的管理員通常是資訊技術 (IT) 人員，擁有 AWS 帳戶 比組織其他成員更高的 許可層級。此個人已建立您的帳戶，並為使用者提供其存取登入資料以登入。

我無法登入現有的 AWS 帳戶 ，也無法使用 AWS 帳戶 相同的電子郵件地址建立新的

您只能將電子郵件地址與電子郵件地址建立關聯 AWS 帳戶根使用者。如果您關閉根使用者帳戶，且該帳戶保持關閉超過 90 天，則無法使用與此帳戶相關聯的 AWS 帳戶 電子郵件地址重新開啟帳戶或建立新帳戶。

若要修正此問題，您可以在註冊新帳戶時，使用在一般電子郵件地址後面新增加號 (+) 的子定址。加號 (+) 後接大寫字母或小寫字母、數字或其他支援簡易郵件傳輸協定 (SMTP) 的字元。例如，您可以使用 email+tag@yourcompany.com email+1@yourcompany.com或您平常的電子郵件是 email@yourcompany.com。這被視為新的地址，即使它與您平常的電子郵件地址連接到相同的收件匣。註冊新帳戶之前，建議您將測試電子郵件傳送至附加的電子郵件地址，以確認您的電子郵件提供者支援子定址。

我需要重新啟用已暫停的 AWS 帳戶

如果您的 AWS 帳戶 已暫停，而您想要將其恢復，請參閱如何重新啟用我的暫停 AWS 帳戶？

我需要聯絡 支援 以解決登入問題

如果您嘗試了一切，您可以透過完成帳單和帳戶支援請求 支援 ，從 取得協助。

我需要聯絡 AWS Billing 處理帳單問題

如果您無法登入您的 ， AWS 帳戶 並想要聯絡 AWS Billing 處理帳單問題，您可以透過帳單和帳戶支援請求來執行此操作。如需 的詳細資訊 AWS 帳單與成本管理，包括您的費用和付款方式，請參閱取得 協助 AWS Billing。

我有關於零售訂單的問題

如果您的 www.amazon.com 帳戶發生問題，或有關於零售訂單的問題，請參閱支援選項和聯絡我們。

我需要管理我的 的協助 AWS 帳戶

如果您需要協助變更信用卡 AWS 帳戶、報告詐騙活動或關閉您的 AWS 帳戶，請參閱疑難排解其他問題 AWS 帳戶。

我的 AWS 存取入口網站登入資料無法運作

當您無法登入 AWS 存取入口網站時，請嘗試記住您之前存取的方式 AWS。

如果您根本不記得使用過密碼

您可能之前 AWS 未使用 AWS 登入資料存取 。這在透過 IAM Identity Center 進行企業單一登入時很常見。以 AWS 這種方式存取意味著您使用公司登入資料來存取 AWS 帳戶或應用程式，而無需輸入您的登入資料。

- AWS 存取入口網站 – 如果管理員允許您從外部使用登入 AWS 資料進行存取 AWS，您需要入口網站的 URL。查看您的電子郵件、瀏覽器我的最愛或瀏覽器歷史記錄中包含 `awsapps.com/start` 或 `signin.aws/platform/login` 的 URL。

  例如，您的自訂 URL 可能包含 ID 或網域，例如 `https://d-1234567890.awsapps.com/start`。如果您找不到入口網站連結，請聯絡您的管理員。 支援 無法協助您復原此資訊。

如果您記得您的使用者名稱和密碼，但您的登入資料無法運作，您可能會在錯誤頁面。查看 Web 瀏覽器中的 URL，如果是 https://signin.aws.amazon.com/，則聯合身分使用者或 IAM Identity Center 使用者無法使用其憑證登入。

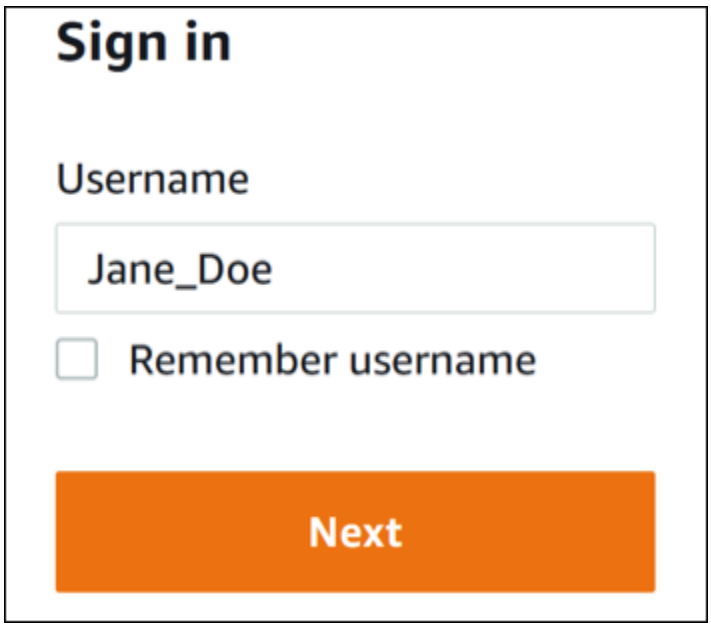
- AWS 存取入口網站 – 如果管理員為 設定 AWS IAM Identity Center (AWS 單一登入的後繼者） 身分來源 AWS，您必須在組織的 AWS 存取入口網站使用您的使用者名稱和密碼登入。若要尋找入口網站的 URL，請檢查您的電子郵件、安全密碼儲存、瀏覽器我的最愛或包含 `awsapps.com/start` 或 的 URL 的瀏覽器歷史記錄`signin.aws/platform/login`。例如，您的自訂 URL 可能包含 ID 或網域，例如`https://d-1234567890.awsapps.com/start`.如果您找不到入口網站連結，請聯絡您的管理員。 支援 無法協助您復原此資訊。

我忘記 的 IAM Identity Center 密碼 AWS 帳戶

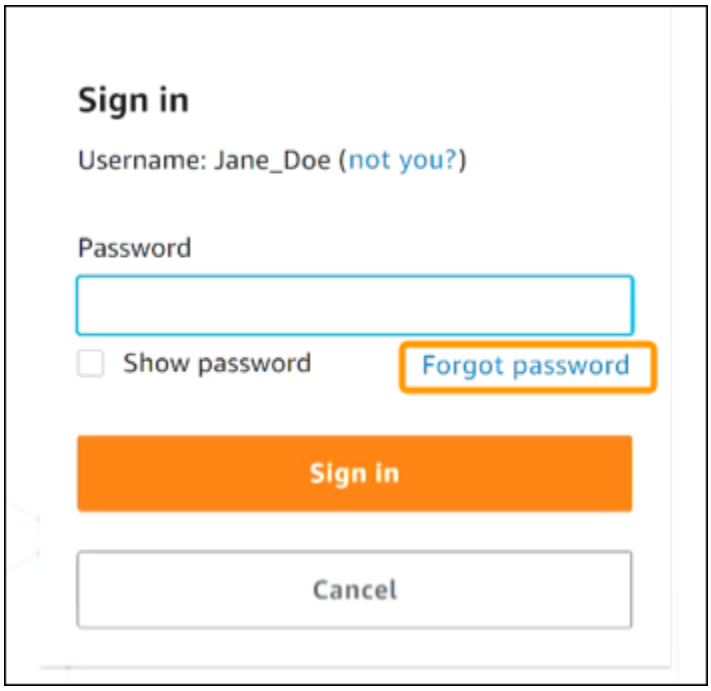
如果您是 IAM Identity Center 的使用者，而且您遺失或忘記 的密碼 AWS 帳戶，您可以重設密碼。您必須知道用於 IAM Identity Center 帳戶的電子郵件地址，並有權存取該帳戶。重設密碼的連結會傳送到您的 AWS 帳戶 電子郵件。

在 IAM Identity Center 密碼中重設您的使用者

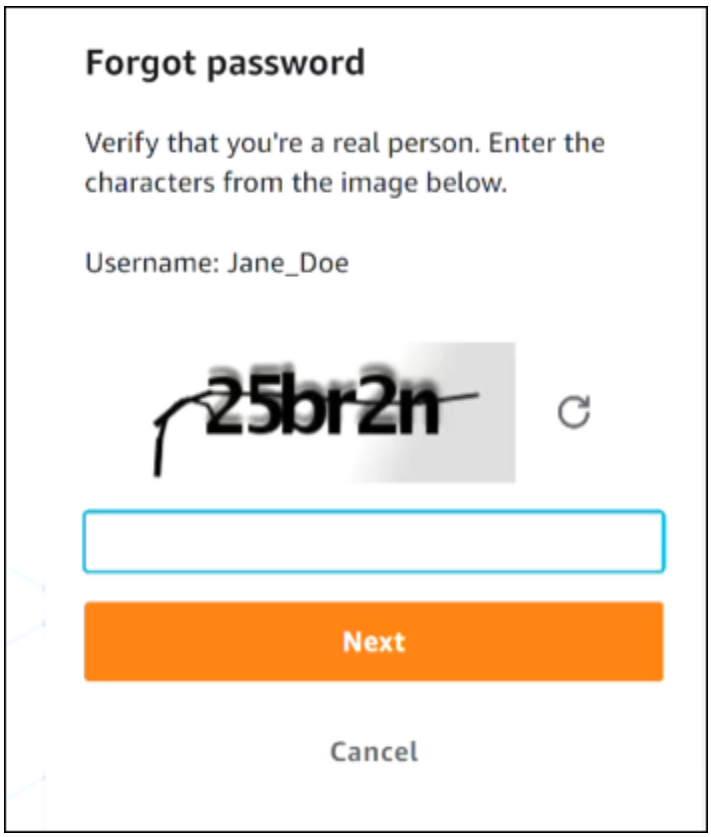
1. 使用您的 AWS 存取入口網站 URL 連結並輸入您的使用者名稱。然後選擇下一步。



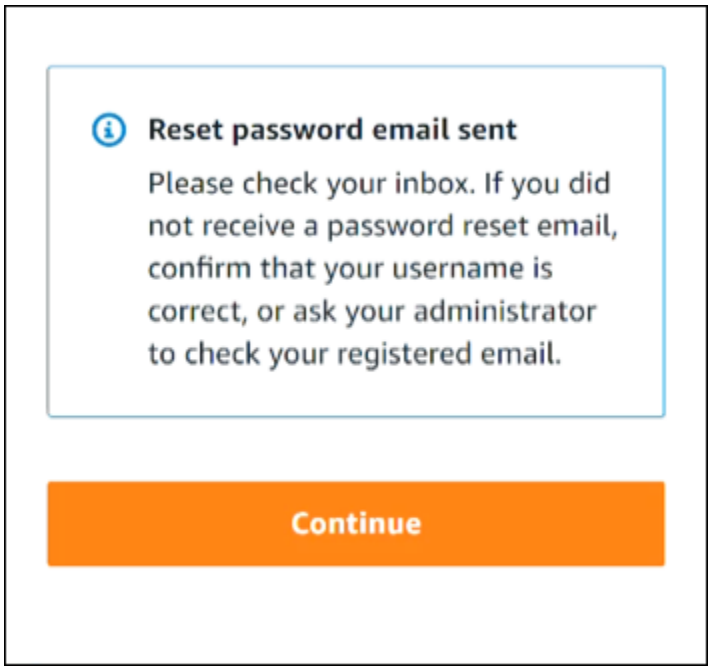
2. 選取忘記密碼，如下圖所示。



3. 完成密碼復原步驟。



4. 完成密碼復原步驟後，您會收到以下訊息，確認您已收到一封電子郵件訊息，可用來重設密碼。



包含重設密碼連結的電子郵件會傳送至與 IAM Identity Center 使用者帳戶相關聯的電子郵件。選取 AWS 電子郵件中提供的連結以重設密碼。該連結會引導您前往新的網頁，以建立新的密碼。建立新密碼後，您會收到密碼重設成功的確認。

如果您未收到重設密碼的電子郵件，請要求管理員確認在 IAM Identity Center 中向使用者註冊的電子郵件。

當我嘗試登入 IAM Identity Center 主控台時，我收到錯誤，指出「這不是您，而是我們」

此錯誤表示您的 IAM Identity Center 執行個體或其用作其身分來源的外部身分提供者 (IdP) 發生設定問題。我們建議您驗證下列項目：

- 驗證您用來登入之裝置上的日期和時間設定。建議您允許自動設定日期和時間。如果無法使用，建議您將日期和時間同步到已知的網路時間通訊協定 (NTP) 伺服器。
- 確認上傳至 IAM Identity Center 的 IdP 憑證與您的身分提供者提供的憑證相同。您可以導覽至設定，從 IAM Identity Center 主控台檢查憑證。在身分來源索引標籤的動作下，選擇管理身分驗證。您可能需要匯入新的憑證。
- 在 IdP 的 SAML 中繼資料檔案中，確保 NameID 格式為 `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`。
- 如果您使用的是 AD Connector，請確認服務帳戶的登入資料正確且尚未過期。如需詳細資訊，請參閱在 中更新您的 AD Connector 服務帳戶登入 Directory Service資料。

對 AWS 建置器 ID 問題進行故障診斷

使用此處的資訊，協助您針對 可能發生的問題進行疑難排解 AWS 建構家 ID。

主題

我的電子郵件已在使用中

如果您輸入的電子郵件已在使用中，且您將其視為自己的電子郵件，則您可能已經註冊 AWS 建置器 ID。請嘗試使用該電子郵件地址登入。如果您不記得密碼，請參閱 我忘記密碼。

我無法完成電子郵件驗證

如果您註冊了 AWS 建置器 ID，但尚未收到驗證電子郵件，請完成下列疑難排解任務。

1. 檢查您的垃圾郵件、垃圾郵件和已刪除項目資料夾。

   > **Note**
   >
   > 此驗證電子郵件來自地址 no-reply@signin.aws 或 no-reply@login.awsapps.com。我們建議您設定郵件系統，使其接受來自這些寄件者電子郵件地址的電子郵件，而不會將其視為垃圾郵件或垃圾郵件處理。

2. 選擇重新傳送程式碼、重新整理收件匣，然後再次檢查您的垃圾郵件、垃圾郵件和已刪除項目資料夾。
3. 如果您仍然看不到驗證電子郵件，請仔細檢查您的 AWS 建置器 ID 電子郵件地址是否有錯字。如果您輸入錯誤的電子郵件地址，請使用您擁有的電子郵件地址再次註冊。

我無法使用 Google 登入

如果您有與 Google 帳戶具有相同電子郵件地址的現有 AWS 建構家 ID 設定檔，請使用 AWS 建構家 ID 您的密碼登入您的帳戶。如果您不記得密碼，請參閱 我忘記密碼。

如需使用 Google 密碼登入的說明，請參閱無法登入您的 Google 帳戶。

我無法使用 Apple 登入

如果您有與 Apple 帳戶具有相同電子郵件地址的現有 AWS 建構家 ID 設定檔，請使用 AWS 建構家 ID 您的密碼登入您的帳戶。如果您不記得密碼，請參閱 我忘記密碼。

如需使用 Apple 密碼登入的說明，請參閱如果您無法登入 Apple 帳戶。

我無法使用 GitHub 登入

如果您有與 GitHub 帳戶具有相同電子郵件地址的現有 AWS 建構家 ID 設定檔，請使用 AWS 建構家 ID 您的密碼登入您的帳戶。如果您不記得密碼，請參閱 我忘記密碼。

如需使用 GitHub 密碼登入的說明，請參閱無法登入 - GitHub Support。

我無法使用 Amazon 登入

如果您有與 Amazon 帳戶具有相同電子郵件地址的現有 AWS 建構家 ID 設定檔，請使用 AWS 建構家 ID 您的密碼登入您的帳戶。如果您不記得密碼，請參閱 我忘記密碼。

如需使用 Amazon 密碼登入的說明，請參閱登入說明。

當我嘗試 AWS 建構家 ID 使用 繼續 Google 註冊 時收到登入錯誤

這表示您使用 AWS 建構家 ID 與 Google 帳戶相同電子郵件地址的現有 ，或與您 Google 帳戶相關聯的電子郵件地址未驗證。在任一情況下，請嘗試再次註冊，輸入您的電子郵件地址並提供密碼。

當我嘗試 AWS 建構家 ID 使用 繼續 Apple 註冊 時，收到登入錯誤

這表示您使用 AWS 建構家 ID 與 Apple 帳戶相同的電子郵件地址，或與您 Apple 帳戶相關聯的電子郵件地址未經您公司透過 Apple Business Manager 進行驗證或管理，或是由您的學校透過 Apple School Manager 進行驗證或管理。在任一情況下，請嘗試再次註冊，輸入您的電子郵件地址並提供密碼。

當我嘗試 AWS 建構家 ID 使用 繼續 GitHub 註冊 時收到登入錯誤

這表示您現有的 AWS 建構家 ID 使用與 GitHub 帳戶相同的電子郵件地址，或者與 GitHub 帳戶相關聯的電子郵件地址未驗證。在任一情況下，請嘗試再次註冊，輸入您的電子郵件地址並提供密碼。

當我嘗試 AWS 建構家 ID 使用 繼續向 Amazon 註冊 時收到登入錯誤

這表示您現有的 AWS 建構家 ID 使用與 Amazon 帳戶相同的電子郵件地址，或與您的 Amazon 帳戶相關聯的電子郵件地址未驗證。在任一情況下，請嘗試再次註冊，輸入您的電子郵件地址並提供密碼。

我收到錯誤，指出「不是您，而是當我嘗試使用 登入時 AWS 建構家 ID

如果您在嘗試登入時收到此錯誤訊息，您的本機設定或電子郵件地址可能會發生問題。

- 驗證您用來登入之裝置上的日期和時間設定。建議您允許自動設定日期和時間。如果無法使用，建議您將日期和時間同步到已知的網路時間通訊協定 (NTP) 伺服器。
- 檢閱您的電子郵件地址是否有格式錯誤。嘗試使用 登入時，下列問題會傳回錯誤 AWS 建構家 ID。
  - 電子郵件地址中的空間
  - 電子郵件地址中的正斜線 (/)
  - 電子郵件地址中的兩個句點 (.)
  - 電子郵件地址中的兩個 ampersands (@)
  - 電子郵件地址結尾的逗號 (,)
  - 電子郵件地址結尾的括號 (】)

我忘記密碼

重設您忘記的密碼

1. 在使用 AWS 建置器 ID 登入頁面上，輸入您在電子郵件地址中用來建立 AWS 建置器 ID 的電子郵件。 選擇下一步。
2. 選擇忘記密碼？。我們會傳送連結到與您的 AWS 建置器 ID 相關聯的電子郵件地址，您可以在其中重設密碼。
3. 請遵循電子郵件中的說明進行。

我無法設定新密碼

為了您的安全，每當您設定或變更密碼時，都必須遵循下列要求：

- 密碼區分大小寫。
- 密碼長度必須介於 8 到 64 個字元之間。
- 密碼必須至少包含下列四個類別中的一個字元：
  - 小寫字母 (a-z)

  - 大寫字母 (A-Z)
  - 數字 (0-9)
  - 非英數字元 (~！@#$%^ 管理入口網站*_-+=`|\(){}【】 ： ；"'<>，.？/)
- 無法重複使用最後三個密碼。
- 無法使用透過從第三方洩露的資料集公開知道的密碼。

我的密碼無法運作

如果您記住密碼，但在使用 AWS 建置器 ID 登入時無法運作，請確定：

- 大寫鎖定已關閉。
- 您未使用較舊的密碼。
- 您使用的是 AWS Builder ID 密碼，而不是 的密碼 AWS 帳戶。

如果您確認密碼是up-to-date且輸入正確，但仍無法運作，請依照 中的指示我忘記密碼重設密碼。

我的密碼無法運作，我無法再存取傳送到 AWS 建置器 ID 電子郵件地址的電子郵件

如果您仍然可以登入 AWS 建置器 ID，請使用設定檔頁面將 AWS 建置器 ID 電子郵件更新為新的電子郵件地址。完成電子郵件驗證後，您就可以登入 ， AWS 並在新的電子郵件地址接收通訊。

如果您使用工作或大學電子郵件地址，且已離開公司或學校，且無法接收傳送到該地址的任何電子郵件，請聯絡該電子郵件系統的管理員。他們可以將您的電子郵件轉送到新的地址、授予您暫時存取權，或從信箱共用內容。

我無法啟用 MFA

若要啟用 MFA，請依照中的步驟，將一或多個 MFA 裝置新增至您的設定檔管理 AWS 建構家 ID 多重要素驗證 (MFA)。

我無法將驗證器應用程式新增為 MFA 裝置

如果您發現無法新增其他 MFA 裝置，可能已達到您可以在該應用程式中註冊的 MFA 裝置限制。請嘗試移除未使用的 MFA 裝置或使用不同的驗證器應用程式。

我無法移除 MFA 裝置

如果您想要停用 MFA，請依照中的步驟繼續移除 MFA 裝置刪除您的 MFA 裝置。不過，如果您想要保持啟用 MFA，您應該先新增另一個 MFA 裝置，再嘗試刪除現有的 MFA 裝置。如需新增其他 MFA 裝置的詳細資訊，請參閱管理 AWS 建構家 ID 多重要素驗證 (MFA)。

當我嘗試使用驗證器應用程式註冊或登入時，收到「發生意外錯誤」訊息

以時間為基礎的一次性密碼 (TOTP) 系統，例如 AWS 建置器 ID 與以程式碼為基礎的驗證器應用程式搭配使用的系統，依賴用戶端和伺服器之間的時間同步。請確定安裝驗證器應用程式的裝置已正確同步至可靠的時間來源，或手動設定裝置上的時間以符合可靠的來源，例如 NIST 或其他本機/區域對等項目。

我收到訊息 '這不是您，而是嘗試登入 AWS 建置器 ID 時

驗證您用來登入之裝置上的日期和時間設定。建議您將日期和時間設定為自動設定。如果無法使用，建議您將日期和時間同步到已知的網路時間通訊協定 (NTP) 伺服器。

登出不會完全登出

系統旨在立即登出，但完全登出最多可能需要一小時。

> **Note**
>
> 使用 Google 或 Apple 等社交登入帳戶時，刪除作用中 AWS 建構家 ID 工作階段不會將您登出社交登入帳戶。

我仍然想要解決我的問題

您可以填寫支援意見回饋表單。在請求資訊區段的 如何協助您，包括您使用 AWS 建置器 ID。盡可能提供詳細資訊，以便我們最有效地處理您的問題。

AWS 的 受管政策 AWS 登入

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。我們建議您定義特定於使用案例的客戶管理政策，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 AWS 管政策中定義的許可，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）。 AWS 服務 當新的 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。

AWS 受管政策：AmazonManagedSignUpServicePolicy

`AmazonManagedSignUpServicePolicy` 政策會授予完成 AWS 帳戶註冊程序所需的許可。

您可以將 `AmazonManagedSignUpServicePolicy` 連接至使用者、群組與角色。

許可詳細資訊

此政策包含以下許可：

- 客戶驗證 - 允許建立、擷取和更新客戶驗證詳細資訊和資格狀態，包括為驗證文件建立上傳 URLs。

若要檢視政策的詳細資訊，包括最新版本的 JSON 政策文件，請參閱《 AWS 受管政策參考指南》中的 AmazonManagedSignUpServicePolicy。

AWS 受管政策：ApplicationProvisioningPolicy

ApplicationProvisioningPolicy 政策授予應用程式佈建和身分管理操作的完整許可，包括 IAM 角色和政策管理、SSO 組態和身分存放區操作。

您可以將 `ApplicationProvisioningPolicy` 連接至使用者、群組與角色。

許可詳細資訊

此政策包含以下許可：

- IAM 管理 - 允許全面的 IAM 操作，包括建立、更新和刪除角色和政策、管理角色連接，以及建立服務連結角色。
- AWS 上的 Research and Engineering Studio - 允許 AWS 上的 Research and Engineering Studio 資源上的所有操作。
- 角色傳遞 - 允許將 IAM 角色傳遞給其他 服務。
- IAM Identity Center - 允許管理 IAM Identity Center 執行個體、應用程式、指派、授予和身分驗證方法。
- Identity Store - 允許從 Identity Store 讀取使用者和群組資訊。
- IAM Identity Center OAuth - 允許透過 IAM Identity Center OAuth 驗證 IAM 工作階段。
- 使用者設定檔和目錄 - 允許管理 IAM Identity Center 連接器、使用者設定檔和目錄組態，包括外部身分提供者設定。
- 使用者訂閱 - 允許列出使用者訂閱。

若要檢視政策的詳細資訊，包括最新版本的 JSON 政策文件，請參閱《 AWS 受管政策參考指南》中的 ApplicationProvisioningPolicy。

AWS 受管政策：SignInLocalDevelopmentAccess

`SignInLocalDevelopmentAccess` 政策會授予許可，以 AWS 使用您的主控台登入資料以程式設計方式存取 。

您可以將 `SignInLocalDevelopmentAccess` 連接至使用者、群組與角色。

許可詳細資訊

此政策包含以下許可：

- 授權 OAuth2 存取 - 准許透過瀏覽器進行身分驗證，並取得憑證交換的 OAuth 2.0 授權碼
- OAuth2 權杖建立 - 准許交換 OAuth 2.0 存取權杖的授權碼和重新整理權杖，可用於從開發人員工具和應用程式存取 AWS 服務

> **Note**
>
> 新增此 AWS 受管政策可讓您同時獲得相同裝置和跨裝置身分驗證的許可。此政策授權對下列資源執行動作：

- arn:aws:signin:*region*:*account-id*:oauth2/public-client/localhost – 用於搭配 的相同裝置身分驗證aws login。
- arn:aws:signin:*region*:*account-id*:oauth2/public-client/remote – 用於搭配 進行跨裝置身分驗證aws login --remote。

若要控制對任一身分驗證方法的存取，您可以建立自己的受管政策或服務控制政策 (SCP)。使用這些資源 ARNs 來允許或拒絕使用您的主控台登入資料對 AWS 進行程式設計存取。

如需詳細資訊，請參閱使用主控台登入資料登入（建議）。若要檢視政策的詳細資訊，包括最新版本的 JSON 政策文件，請參閱《 AWS 受管政策參考指南》中的 SignInLocalDevelopmentAccess。

AWS 受管政策：AWSSignInResourcePolicyManagement

此AWSSignInResourcePolicyManagement政策授予許可，以管理 AWS Sign-In 的主控台授權組態和資源許可陳述式。

您可以將 AWSSignInResourcePolicyManagement 連接至使用者、群組與角色。

許可詳細資訊

此政策包含以下許可：

- signin:PutConsoleAuthorizationConfiguration – 建立或更新主控台授權設定。
- signin:GetConsoleAuthorizationConfiguration – 擷取目前的主控台授權組態。
- signin:DeleteConsoleAuthorizationConfiguration – 移除主控台授權組態。
- signin:PutResourcePermissionStatement – 建立或更新資源許可陳述式。
- signin:DeleteResourcePermissionStatement – 移除資源許可陳述式。
- signin:ListResourcePermissionStatements – 列出帳戶的資源許可陳述式。
- signin:GetResourcePolicy – 擷取合併的資源型政策。

以下是政策 JSON：

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Action": [
                "signin:PutConsoleAuthorizationConfiguration",
                "signin:GetConsoleAuthorizationConfiguration",
                "signin:DeleteConsoleAuthorizationConfiguration",
                "signin:PutResourcePermissionStatement",
                "signin:DeleteResourcePermissionStatement",
                "signin:ListResourcePermissionStatements",
                "signin:GetResourcePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

將此政策連接至管理以資源為基礎的 AWS Sign-In 政策的 IAM 主體（使用者或角色）。這包括負責設定網路型存取控制的安全管理員、需要稽核主控台存取政策的合規主管，以及管理緊急復原存取組態的操作團隊。

> **Important**
>
> 此政策會授予主控台授權控制的管理存取權。在指派此政策時套用最低權限原則。考慮使用 IAM 條件來進一步限制何時以及如何使用這些許可。

若要檢視政策的詳細資訊，包括最新版本的 JSON 政策文件，請參閱《AWS 受管政策參考指南》中的 AWSSignInResourcePolicyManagement。

AWS 登入 AWS 受管政策的更新

檢視自此服務開始追蹤這些變更 AWS 登入 以來， AWS 受管政策更新的詳細資訊。如需此頁面變更的自動提醒，請訂閱 AWS 登入 文件歷史記錄頁面上的 RSS 摘要。

變更	描述	日期
AWSSignInResourcePolicyManagement – 新政策	新增了新的 AWS 受管政策，授予許可來管理 AWS 登入的主控台授權組態和資源許可陳述式。	2026 年 6 月 10 日

變更	描述	日期
SignInLocalDevelopmentAccess – 新政策	新增了新的 AWS 受管政策，授予 AWS 使用您現有主控台登入資料以程式設計方式存取的許可。	2025 年 11 月 19 日
ApplicationProvisioningPolicy – 新政策	新增了新的 AWS 受管政策，授予應用程式佈建和身分管理操作的完整許可，包括 IAM 角色和政策管理、IAM Identity Center 組態和 Identity Store 操作。	2025 年 9 月 30 日
AmazonManagedSignUpServicePolicy – 新政策	新增了新的 AWS 受管政策，授予 AWS 帳戶註冊程序所需的許可，包括客戶驗證和付款設定操作。	2025 年 9 月 30 日
AWS 登入 開始追蹤變更	AWS 登入 開始追蹤其 AWS 受管政策的變更。	2025 年 9 月 30 日

文件歷史記錄

下表說明 AWS 登入文件的重要新增項目。我們也會經常更新文件，以處理您傳送給我們的意見回饋。

- 最新主要文件更新時間：2026 年 6 月 10 日

變更	描述	日期
支援以資源為基礎的登入政策和資源控制政策	新增使用登入資源型政策和資源控制政策 (RCPs)、新條件金鑰參考、`AWSSignInResourcePolicyManagement` 受管政策以及相關故障診斷來控制 AWS 管理主控台 存取的文件。	2026 年 6 月 10 日
支援使用 GitHub 和 Amazon 登入	AWS 登入 現在支援使用 GitHub 登入和使用 Amazon 登入，以便您可以使用 AWS 建構家 ID GitHub 或 Amazon 帳戶建立 。	2026 年 3 月 10 日
支援使用 Apple 登入	AWS 登入 現在支援使用 Apple 登入，因此您可以使用 AWS 建構家 ID Apple 帳戶建立 。AWS 建構家 ID 主題已更新，且新的故障診斷主題已新增至故障診斷 AWS 建構家 ID 問題。	2026 年 2 月 5 日
新的 受管政策	AWS 登入 已發佈新的 受管政策。 `SignInLocalDevelopmentAccess` 授予使用 AWS 現有主控台登入資料的程式設計存取 的許可。如需詳細	2025 年 11 月 19 日

	資訊，請參閱 AWS 登入AWS 受管政策的更新。	
支援使用 Google 登入	AWS 登入 現在支援使用 Google 登入，因此您可以使用 AWS 建構家 ID Google 帳戶建立 。 AWS 建構家 ID 主題已更新，且已將新的故障診斷主題新增至故障診斷 AWS 建構家 ID 問題。	2025 年 9 月 30 日
新受管政策	AWS 登入 已發佈兩個新的 受管政策。 `AmazonManagedSignUpServicePolicy` 授予完成 AWS 帳戶註冊程序所需的許可。 `ApplicationProvisioningPolicy` 授予應用程式佈建和身分管理操作的完整許可。如需詳細資訊，請參閱 AWS 登入AWS 受管政策的更新。	2025 年 9 月 30 日
已更新故障診斷主題	新增了用於登入 AWS 建構家 ID 和 的新故障診斷主題 AWS 管理主控台。	2024 年 2 月 27 日
已更新組織的數個主題	已更新使用者類型、已移除確定使用者類型並將其內容併入使用者類型、如何登入 AWS	2023 年 5 月 15 日
已更新數個主題和頂端橫幅	已更新使用者類型、判斷使用者類型、如何登入 AWS、什麼是 AWS 登入？。也更新了根使用者和 IAM 使用者登入程序。	2023 年 3 月 3 日

更新 AWS 管理主控台 用於登入的簡介段落	已將判斷使用者類型移至頁面頂端，並移除帳戶根使用者中存在的備註。	2023 年 2 月 27 日
已新增 AWS 建構家 ID	已將 AWS 建構家 ID 主題新增至 AWS 登入使用者指南，並將內容整合到現有主題。	2023 年 1 月 31 日
組織更新	根據客戶的意見回饋， 更新了 TOC，以更清楚登入方法。更新登入教學課程。已更新術語和判斷使用者類型。改善交叉連結以定義 IAM 使用者和根使用者等詞彙。	2022 年 12 月 22 日
新的指南	這是 AWS 登入使用者指南的第一個版本。	2022 年 8 月 31 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。