aws

管理指南

AWS 威克爾

AWS 威克爾: 管理指南

Table of Contents

什麼是 AWS 威克爾？

AWS Wickr 是一種 end-to-end 加密服務，可協助組織和政府機構透過群組簡訊、語音 one-to-one 和視訊通話、檔案共用、螢幕共用等方式進行安全通訊。Wickr 可以幫助客戶克服與消費者級消息傳遞應用程序相關的數據保留義務，並安全地促進協作。進階安全性和管理控制可協助組織符合法律和法規要求，並針對資料安全挑戰建置自訂解決方案。

資訊可以記錄到由客戶控制的私人資料存放區，以供保留和稽核之用。使用者對資料具有完整的系統管理控制權，包括設定權限、設定暫時傳訊選項，以及定義安全性群組。威克與其他服務集成，例如活動目錄（AD），單點登錄（SSO）與 OpenID Connect（OIDC）等。您可以通過快速創建和管理 Wickr 網絡 AWS Management Console，並使用 Wickr 機器人安全地自動化工作流程。若要開始使用，請參閱為 AWS 威克爾設定。

主題

威克爾的特點

增強的安全性和隱私

Wickr 對每個功能都使用 256 位進階加密標準 (AES) end-to-end 加密。通信在用戶設備上進行本地加密，並且在傳輸給發送者和接收者以外的任何人都無法解讀。每個消息，呼叫和文件都使用新的隨機密鑰進行加密，除了預定的收件人（甚至 AWS）沒有人可以解密它們。無論他們是共享敏感和受監管的數據，討論法律或人力資源事務，甚至進行戰術軍事行動，客戶都可以在安全和隱私至關重要時使用 Wickr 進行溝通。

資料保留

靈活的管理功能不僅用於保護敏感信息，還可以根據合規義務，法律持有和審計目的保留所需保留數據。訊息和檔案可以封存在安全且由客戶控制的資料存放區中。

靈活存取

使用者可以存取多裝置 (行動裝置、桌上型電腦)，並且能夠在低頻寬環境中運作，包括中斷連線和 out-of-band 通訊。

管理控制

使用者對資料具有完整的系統管理控制權，包括設定權限、設定負責的暫時訊息選項，以及定義安全性群組。

強大的整合和機器人

Wickr 與其他服務集成，例如活動目錄，單點登錄（SSO）與 OpenID Connect（OIDC）等。客戶可以透過 Wickr 機器人快速建立和管理 Wickr 網路 AWS Management Console，並安全地自動化工作流程。

以下是 Wickr 協同合作產品的細分：

- 1 對 1 和群組訊息：在最多 500 名成員的房間內與您的團隊安全聊天
- 音訊和視訊通話：最多可與 70 人進行電話會議
- 屏幕共享和廣播：最多 500 名參與者
- 文件共享和保存：無限存儲空間傳輸高達 5GB 的文件
- 暫時性：控制到期日和計時器 burn-on-read
- 全球聯盟：Connect 您網路外部的 Wickr 使用者連線

> **Note**
>
> AWS GovCloud （美國西部）中的 Wickr 網絡只能與（美國西部）中 AWS GovCloud 的其他 Wickr 網絡聯合。

訪問威克

Wickr 已在美國東部 (維吉尼亞北部)、加拿大 (中部)、歐洲 (倫敦)、亞太區域 (雪梨)、歐洲 (法蘭克福)、歐洲 (斯德哥爾摩)、亞太區域 (新加坡) 和亞太區域 (東京) AWS 區域使用。Wickr 也可作為 WickrGov 在 AWS GovCloud （美國西部）。 AWS 區域

管理員訪問威克爾在 https://console.aws.amazon.com/wickr/。 AWS Management Console 在開始使用 Wickr 之前，您應該完成為 AWS 威克爾設定和開始使用 AWS 威克指南。

> **Note**
>
> Wickr 服務沒有應用程式設計介面 (API)。

終端使用者可透過 Wickr 用戶端存取 Wickr。如需詳細資訊，請參閱 AWS Wickr 使用者指南。

定價

Wickr 針對個人，小型團隊和大型企業提供不同的計劃。如需詳細資訊，請參閱 AWS Wickr 定價。

威克最終用戶文檔

如果您是 Wickr 用戶端的一般使用者，且需要存取其文件，請參閱 AWS Wickr 使用者指南。

為 AWS 威克爾設定

如果您是新 AWS 客戶，請在開始使用 AWS Wickr 之前完成此頁面上列出的設定先決條件。對於這些設定程序，您可以使用 AWS Identity and Access Management (IAM) 服務。如需 IAM 的完整資訊，請參閱《IAM 使用者指南》。

主題

註冊成為 AWS

如果您沒有 AWS 帳戶，請完成以下步驟來建立一個。

若要註冊成為 AWS 帳戶

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

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   當您註冊一個時 AWS 帳戶，將創建AWS 帳戶根使用者一個。根使用者有權存取該帳戶中的所有 AWS 服務 和資源。安全性最佳做法是將管理存取權指派給使用者，並僅使用 root 使用者來執行需要 root 使用者存取權的工作。

建立 IAM 使用者

若要建立管理員使用者，請選擇下列其中一個選項。

選擇一種管理管理員的方式	到	By	您也可以
在 IAM Identity Center (建議)	使用短期憑證存取 AWS。	請遵循 AWS IAM Identity Center 使用	AWS IAM Identity Center在《使用

選擇一種管理管理員的方式	到	By	您也可以
	這與安全性最佳實務一致。有關最佳實務的資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。	者指南的入門中的說明。	AWS Command Line Interface 者指南》中設定 AWS CLI 要使用的，以設定程式設計方式存取。
在 IAM 中 (不建議使用)	使用長期憑證存取 AWS。	請遵循 IAM 使用者指南中建立您的第一個 IAM 管理員使用者和使用者群組的說明。	請參閱 IAM 使用者指南中的管理 IAM 使用者的存取金鑰，設定程式設計存取。

> **Note**
>
> 您也可以指派AWSWickrFullAccess受管理政策，以授與 Wickr 服務的完整管理權限。如需詳細資訊，請參閱 AWS 受管理的策略： AWSWickrFullAccess。

下一步是什麼

您已完成先決條件設定步驟。若要開始設定 Wickr，請參閱開始使用。

開始使用 AWS 威克

在本指南中，我們將向您展示如何通過創建網絡，配置網絡和創建用戶來開始使用 Wickr。

主題

必要條件

開始之前，如果尚未完成下列先決條件：

- 註冊 Amazon Web Services（AWS）。如需詳細資訊，請參閱 為 AWS 威克爾設定。
- 確保您具有管理 Wickr 所需的權限。如需詳細資訊，請參閱 AWS 受管理的策略：AWSWickrFullAccess。
- 確保您允許列出 Wickr 的適當端口和域。如需詳細資訊，請參閱 允許的連接埠和網域清單。

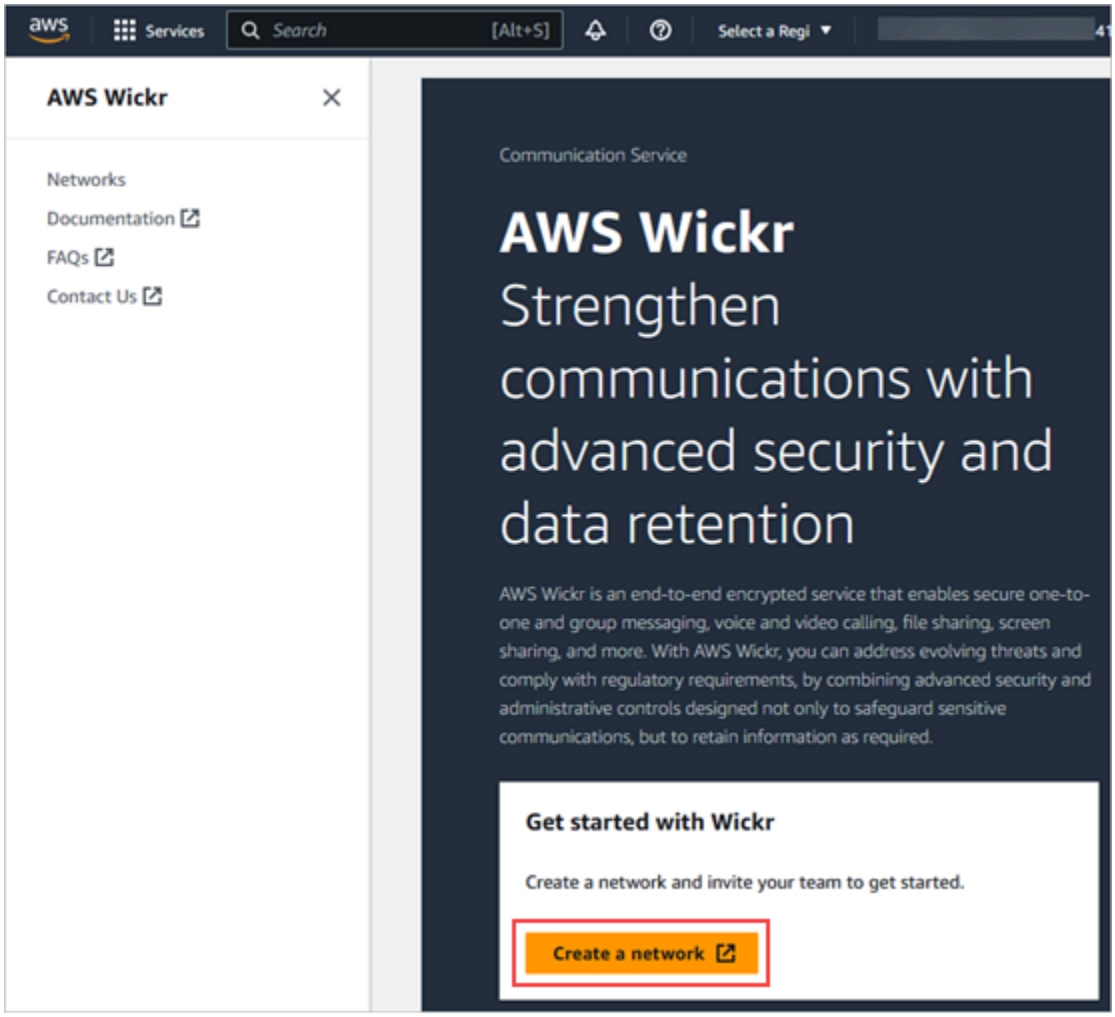
步驟 1：建立網路

請完成下列程序，為您的帳戶建立 Wickr 網路。

1. 打開 AWS Management Console 威克爾在 https://console.aws.amazon.com/wickr/。

   > **Note**
   >
   > 如果您之前尚未建立 Wickr 網路，您將會看到 Wickr 服務的資訊頁面。建立一個或多個 Wickr 網路之後，您會看到「網路」頁面，其中包含您建立的所有 Wickr 網路的清單檢視。

2. 選擇 [建立網路]。



3. 在 [網路名稱] 文字方塊中輸入網路名稱。選擇組織成員可以識別的名稱，例如您的公司名稱或團隊名稱。
4. 選擇一個計劃。您可以選擇以下 Wickr 網絡計劃之一：

   - 標準 — 適用於需要管理控制和彈性的小型和大型企業團隊。
   - 進階版或免費試用版 — 適用於需要最高功能限制、精細管理控制和資料保留的企業。

   管理員可以選擇高級免費試用選項，該選項最多可供 30 個用戶使用，並持續三個月。此優惠適用於新的無法試用和標準計劃。管理員可以在高級免費試用期內升級或降級到高級或標準計劃。

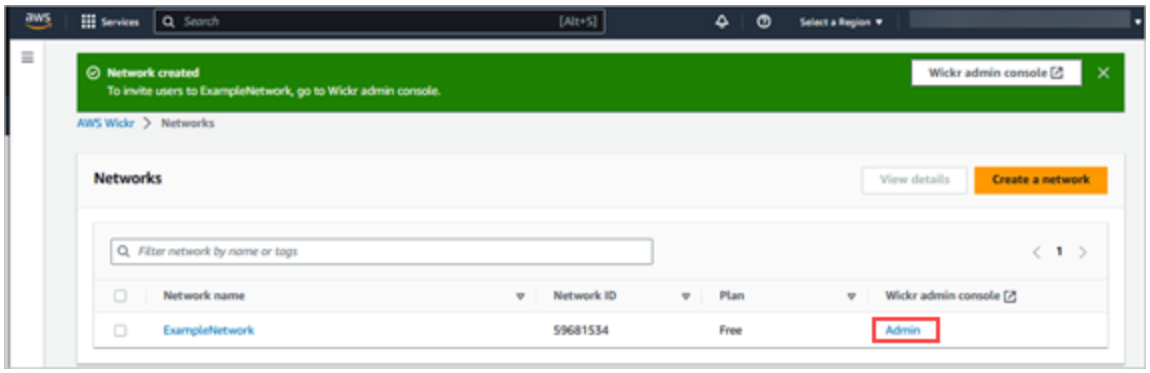
   有關可用 Wickr 計劃和定價的更多信息，請參閱 Wickr 定價頁面。
5. (選擇性) 選擇「新增標籤」，將標籤新增至您的網路。標籤由索引鍵值配對組成。標籤可用於搜尋和篩選資源或追蹤 AWS 成本。如需詳細資訊，請參閱網路標記。
6. 選擇「建立網路」。

系統會將您重新導向至 Wickr AWS Management Console 的「網路」頁面，並在頁面上列出新的網路。

步驟 2：設定您的網路

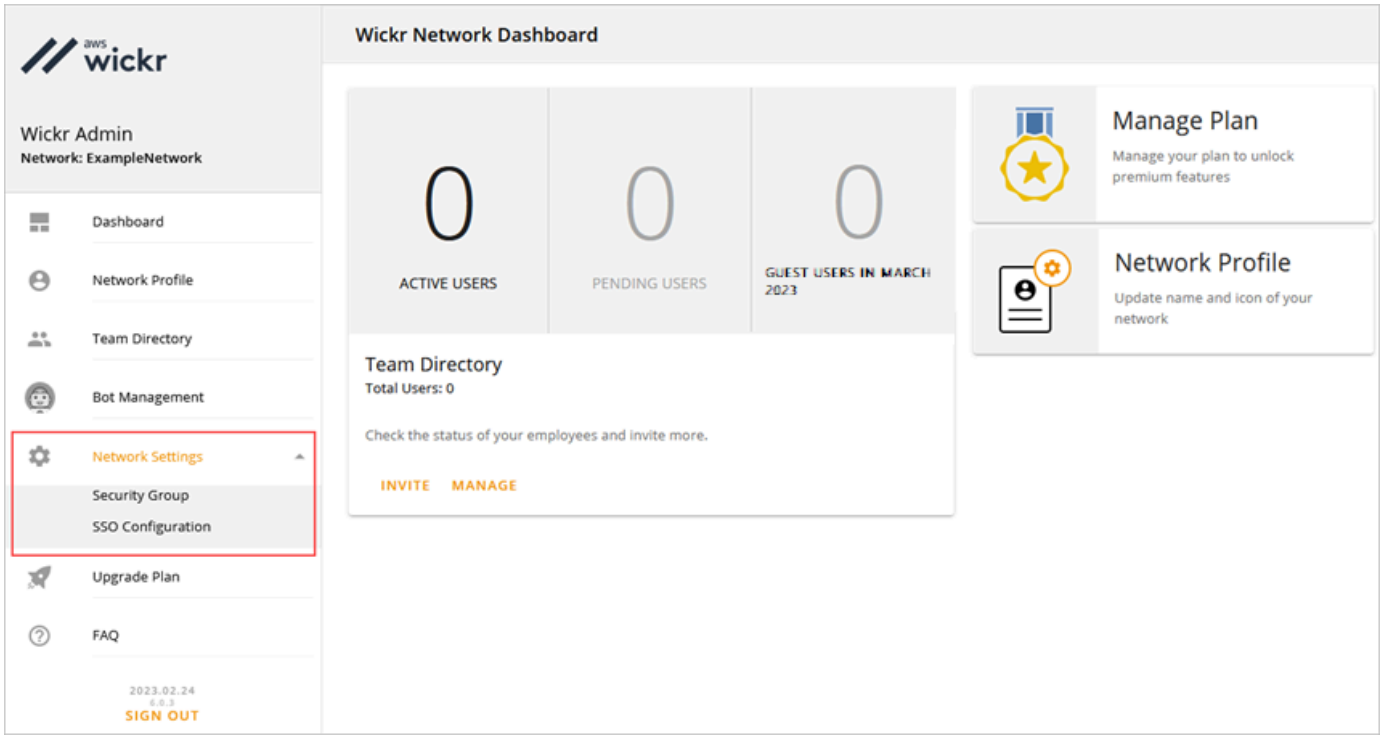
完成下列程序以存取 Wickr Admin Console，您可以在其中新增使用者、新增安全性群組、設定 SSO、設定資料保留和其他網路設定。

1. 在 [網路] 頁面上，選擇 [管理員] 連結，瀏覽至該網路的 Wickr 管理控制台。



系統會將您重新導向至所選網路的 Wickr 管理控制台。

2. 在 Wickr 管理控制台的導覽窗格中，選擇 [網路設定]。



以下是可用的網路設定選項。如需有關進行這些設定的更多資訊，請參閱管理您的 AWS 網路。

- 安全群組 — 管理安全性群組及其設定，例如密碼複雜性原則、訊息偏好設定、通話功能、安全性功能和外部聯合。如需詳細資訊，請參閱 安全群組。
- SSO 組態 — 設定 SSO 並檢視 Wickr 網路的端點位址。威克支持僅使用 OpenID Connect（OIDC）的 SSO 提供商。不支援使用安全性宣告標記語言 (SAML) 的提供者。如需詳細資訊，請參閱 單一登入組態。

步驟 3：建立並邀請使用者

您可以使用下列方法在 Wickr 網路中建立使用者：

- 單一登入 — 如果您設定 SSO，您可以透過共用您的 Wickr 公司 ID 來邀請使用者。最終用戶使用提供的公司 ID 和他們的工作電子郵件地址註冊 Wickr。如需詳細資訊，請參閱 單一登入組態。
- 邀請 — 您可以在 Wickr 中手動建立使用者，並傳送電子郵件邀請給他們。 AWS Management Console 最終用戶可以通過選擇電子郵件中的鏈接註冊 Wickr。

> **Note**
>
> 您也可以為您的 Wickr 網路啟用訪客使用者。訪客使用者功能目前處於預覽狀態。如需更多資訊，請參閱訪客使用者

請完成下列程序來建立或邀請使用者。

> **Note**
>
> 系統管理員也被視為使用者，必須邀請自己加入 SSO 或非 SSO Wickr 網路。

SSO

撰寫並傳送電子郵件給應該註冊 Wickr 的 SSO 使用者。在您的電子郵件中包含以下信息：

- 您的威克公司 ID。您可以在設定 SSO 時指定 Wickr 網路的公司識別碼。如需詳細資訊，請參閱設定 SSO。
- 他們應該用來註冊的電子郵件地址。

- 下載 Wickr 用戶端的網址。使用者可以從 AWS 威克爾下載頁面下載，網址為 https://aws.amazon.com/wickr/download/ 下載威克爾客戶端。

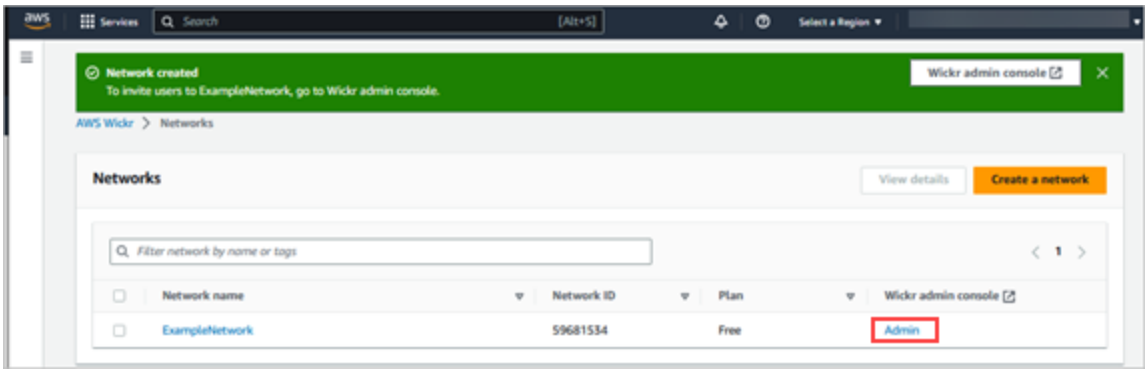
> **Note**
>
> 如果您在 AWS GovCloud (美國西部) 建立 Wickr 網路，請指示您的使用者下載並安裝用戶端。 WickrGov 對於所有其他 AWS 區域，請指示您的使用者下載並安裝標準 Wickr 用戶端。若要取得更多資訊 AWS WickrGov，請參閱《AWS GovCloud (US) 使用指南》AWS WickrGov中的〈〉。

當使用者註冊您的 Wickr 網路時，他們會新增到 Wickr 團隊目錄中，狀態為作用中。

Non-SSO

若要手動建立 Wickr 使用者並傳送邀請：

1. 打開 AWS Management Console 威克爾在 https://console.aws.amazon.com/wickr/。
2. 在 [網路] 頁面上，選擇 [管理員] 連結，瀏覽至該網路的 Wickr 管理控制台。



「網路」頁面。

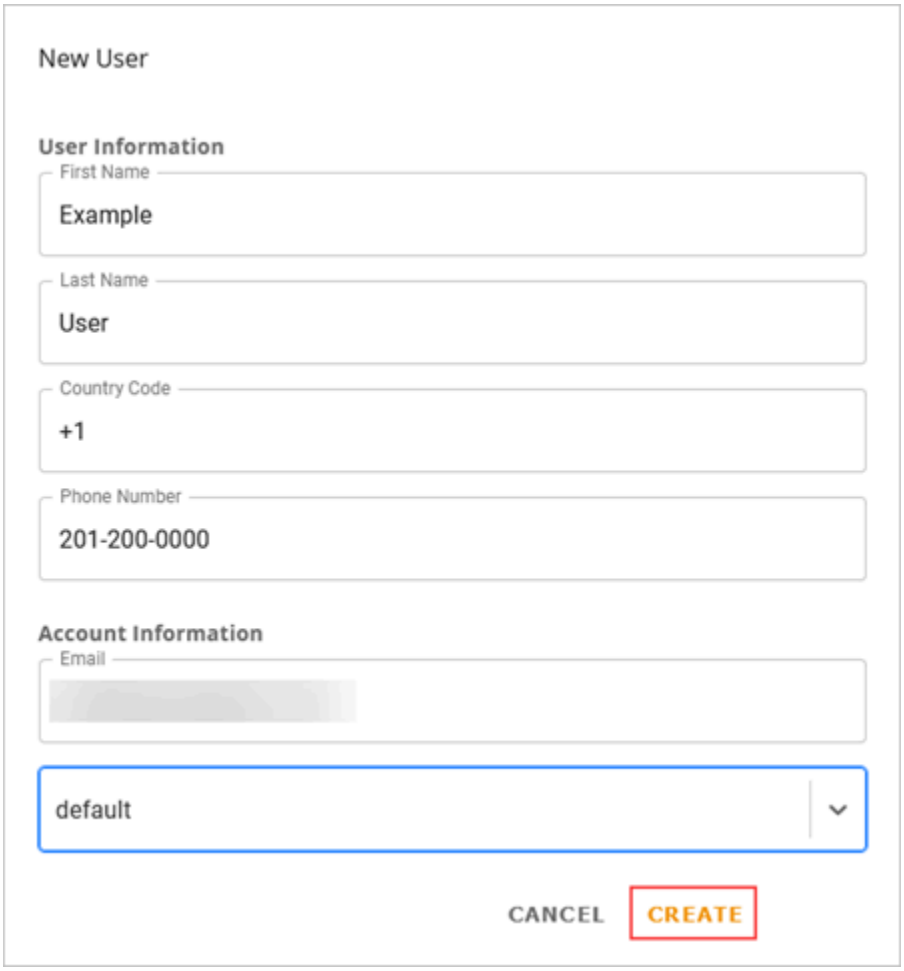
系統會將您重新導向至特定網路的 Wickr 管理控制台。在 Wickr Admin Console 上，您可以為您選取的特定網路新增使用者、新增安全群組、設定 SSO、設定資料保留和其他設定。

3. 在 Wickr 管理控制台的導覽窗格中，選擇 [使用者]，然後選擇 [團隊目錄]。

   在 [使用者] 頁面中，您可以選擇 [建立新使用者] 來新增個別使用者。您也可以選擇頂端導覽窗格中的 [新增使用者] 圖示，以大量新增使用者。選擇「下載 CSV」圖示以下載 CSV 範本，您可以編輯該範本並與使用者清單一起上傳。

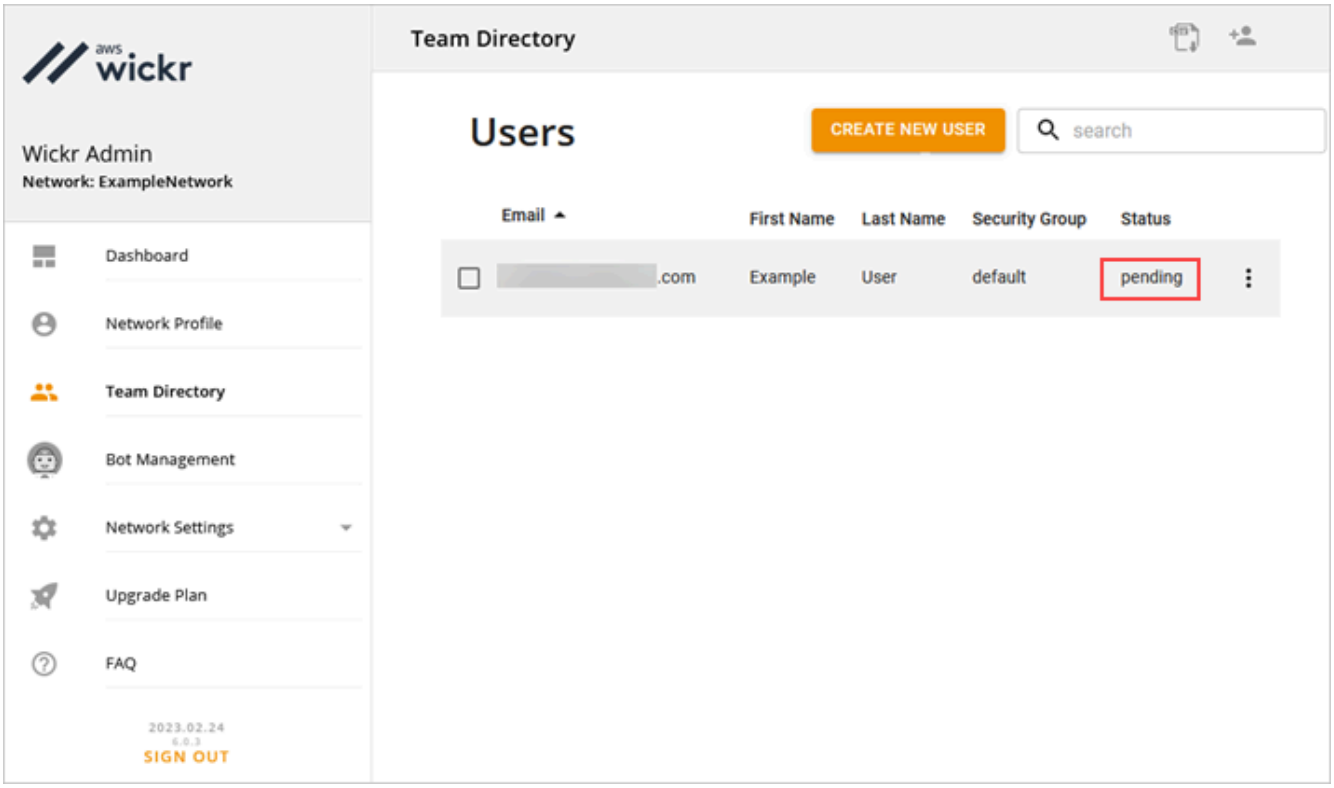
4. 輸入使用者的名字、姓氏、國碼、電話號碼和電子郵件地址。電子郵件地址是唯一必填的欄位。請務必為使用者選擇適當的安全性群組。

5. 選擇建立。



Wickr 會傳送邀請電子郵件至您為使用者指定的地址。電子郵件提供 Wickr 用戶端應用程式的下載連結，以及註冊 Wickr 的連結。如需有關此最終使用者體驗的詳細資訊，請參閱下載 Wickr 應用程式並在 AWS Wickr 使用者指南中接受邀請。

當用戶使用電子郵件中的鏈接註冊 Wickr 時，他們在 Wickr 團隊目錄中的狀態將從「待處理」更改為「活動」。



後續步驟

您已完成開始使用步驟。若要管理 Wickr，請參閱下列指南：

- 管理您的 AWS 網路
- 管理 AWS 中的使用者

將威克爾專業版轉移到 AWS 威克爾

> **Note**
>
> 威克爾臨將於 2024 年 3 月 27 日停產。

在本指南中，我們將向您展示如何從 Wickr Pro 轉移並開始使用 AWS Wickr。

如果您擁有現有的 Wickr Pro 網絡，但 AWS 帳戶 尚未安裝，請按照本指南中的步驟進行操作。如果您需要幫助，請隨時聯繫支持。

如果您的組織已經擁有 AWS 帳戶，請填寫從 Wickr Pro 遷移到 AWS Wickr 表單，AWS Wickr 支援將為您提供協助。

您將需要一個 AWS 帳戶 ID 來管理您的 AWS Wickr 網路。 AWS 服務有關什麼 AWS 帳戶 是以及如何管理帳戶的更多信息，請參閱AWS 帳戶管理參考指南。

主題

步驟 1：創建一個 AWS 帳戶

請完成下列程序以建立 AWS 帳戶。

1. 如果您的組織沒有現有的 AWS 帳戶 ID，您可以先建立獨立 AWS 帳戶 ID。您將需要一些關鍵的東西：

   - 信用卡/借記卡進行計費
   - 群組可存取的電子郵件地址 (建議使用，不需要)
   - 選擇一個 AWS Support 計劃。如需詳細資訊，請參閱變更 AWS Support 計劃。

   > **Note**
   >
   > 當您了解更多有關您的需求時，您可以隨時更改 AWS Support 計劃。

2. 透過 IAM 設定管理存取作為安全性最佳實務 (選用但建議使用)。如需詳細資訊，請參閱 AWS Identity and Access Management。如需有關 AWS Wickr 管理存取的更具體指示，請參閱AWS 受管政策： AWSWickrFullAccess。
3. 完成前面的步驟後，您將可以登錄以在您的帳戶名稱下找 AWS Management Console 到您的 12 位數 AWS 帳戶 ID。

步驟 2：檢索您的威克爾網絡 ID

請完成以下程序以擷取您的 Wickr 網路 ID。

1. 登錄到您當前的 Wickr 管理控制台，然後選擇要遷移的網絡，然後選擇網絡配置文件。
2. 「網路設定檔」頁面會顯示您的網路 ID，而且是 8 位數的數字 ID。

步驟 3：提交請求

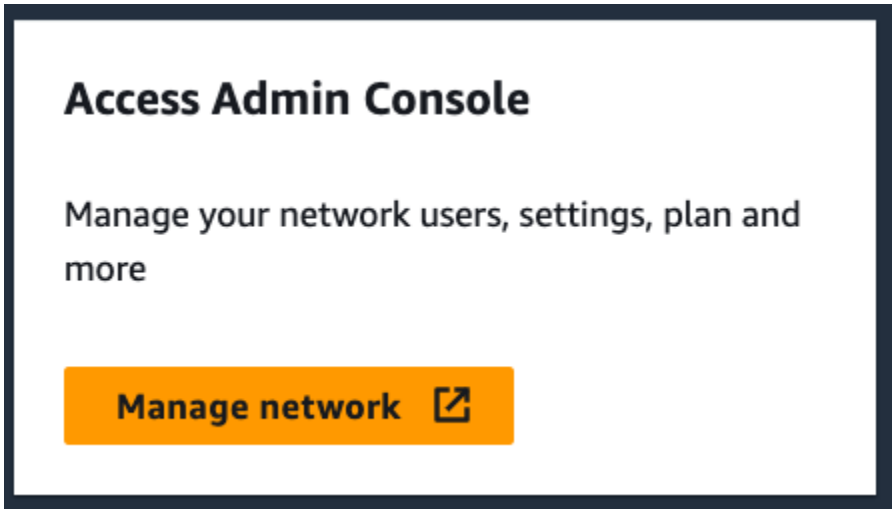
現在您已經擁有您的 AWS 帳戶 ID 和 Wickr 專業版網路 ID，您需要完成從 Wickr Pro 遷移到 AWS Wickr 的表單。

完成後，通常會在 14 天內，AWS Wickr 支援代表會與您聯絡，確認您的 Wickr 網路已新增至您的網路。 AWS 帳戶

步驟 4：登入您的 AWS 主機

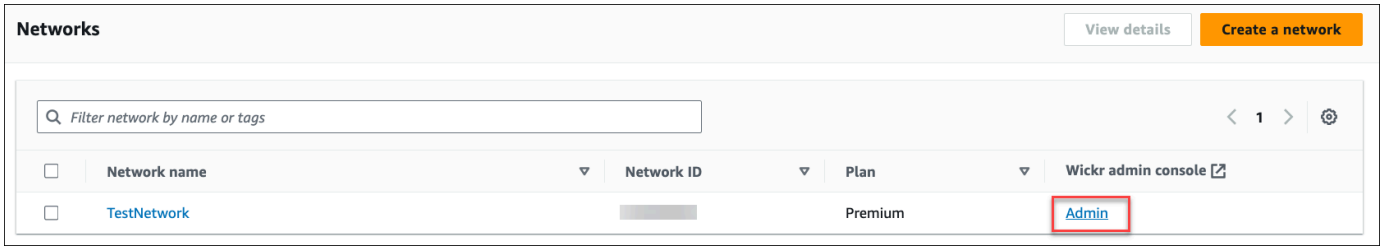
> **Note**
>
> 在收到您的 Wickr Pro 網絡已添加到您的確認後，請按照以下步驟操作 AWS 帳戶。

1. 您可以以根使用者身分登入 AWS 主控台，或使用您先前在 AWS Wickr 的步驟 2 中建立的 IAM 使用者身分登入主控台。
2. 瀏覽至您的 AWS 威克爾服務。您可以從「服務」功能表或在搜尋列中搜尋 AWS Wickr 來執行此操作。
3. 在 AWS Wickr 頁面上，選擇管理網路以存取您的 Wickr 網路清單。



「管理網路」按鈕。

4. 在「網路」頁面的「Wickr 管理控制台」欄下，選取所需網路名稱右側的「管理員」連結。



管理員主控台連結。

5. 轉移現已完成！您將看到您的 Wickr 網絡儀表板。

您網絡的帳單現在將轉移到您的 AWS 帳戶. 最多需要 3 個工作日，以便在確認後與支援人員聯絡。收到您的確認後，您可以通過 AWS 控制台查看和支付賬單。

管理您的 AWS 網路

在 Wickr 的 [網路設定] 區段中，您可以管理您的 Wickr 網路名稱、安全群組、SSO 組態和資料保留設定。 AWS Management Console

主題

網路設定檔

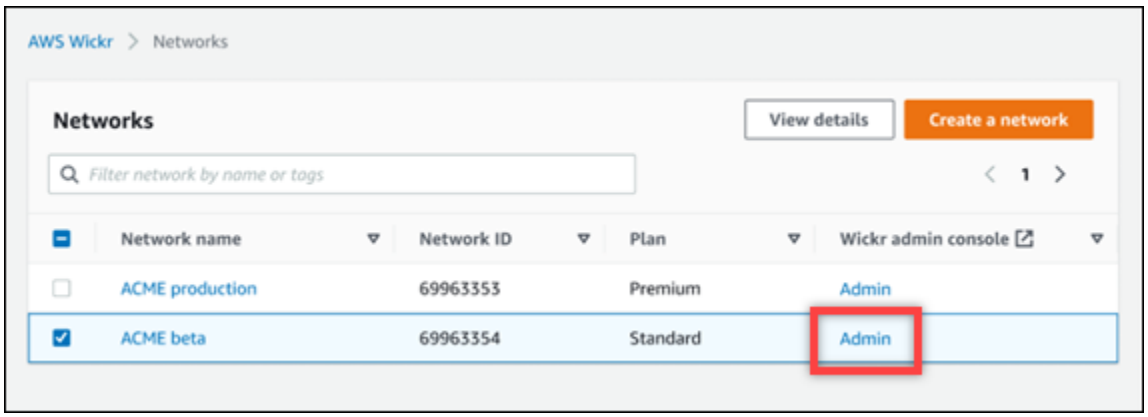
您可以編輯 Wickr 網路名稱，並在 Wickr 的「網路設定檔」區段中檢視您 AWS Management Console 的網路 ID。

主題

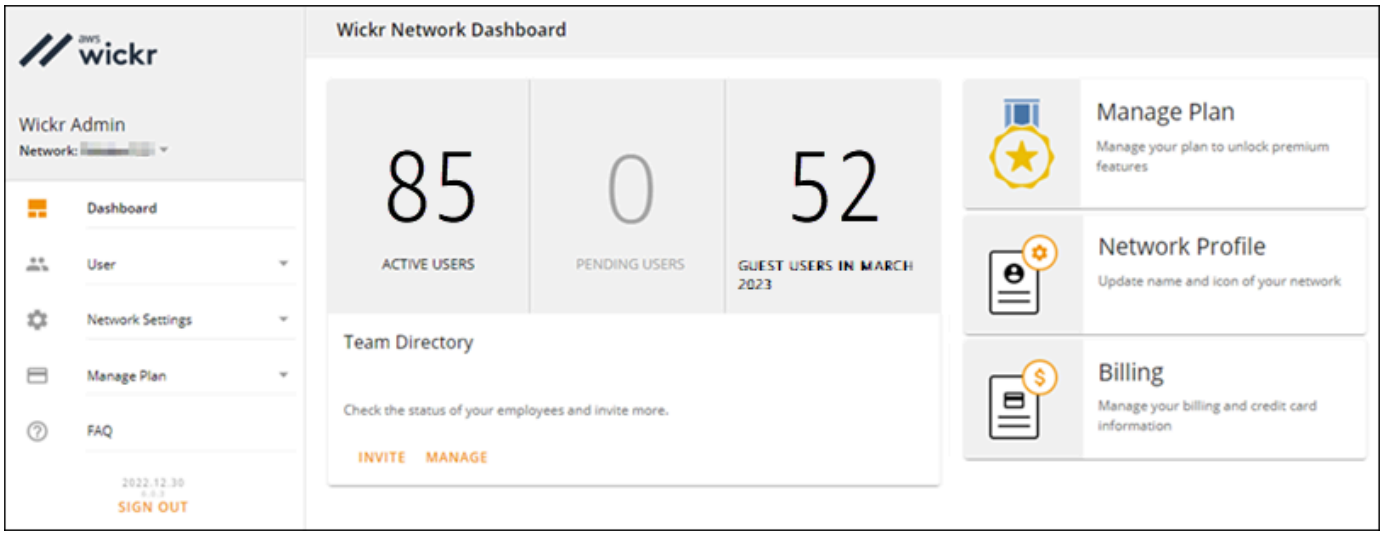
檢視網路設定檔

請完成以下程序以檢視您的 Wickr 網路設定檔和網路 ID。

1. 在以下位置 AWS Management Console 打開威克爾的網址：https://console.aws.amazon.com/wickr/。
2. 在 [網路] 頁面上，選擇 [管理員] 連結，瀏覽至該網路的 Wickr 管理控制台。



系統會將您重新導向至特定網路的 Wickr 管理控制台。



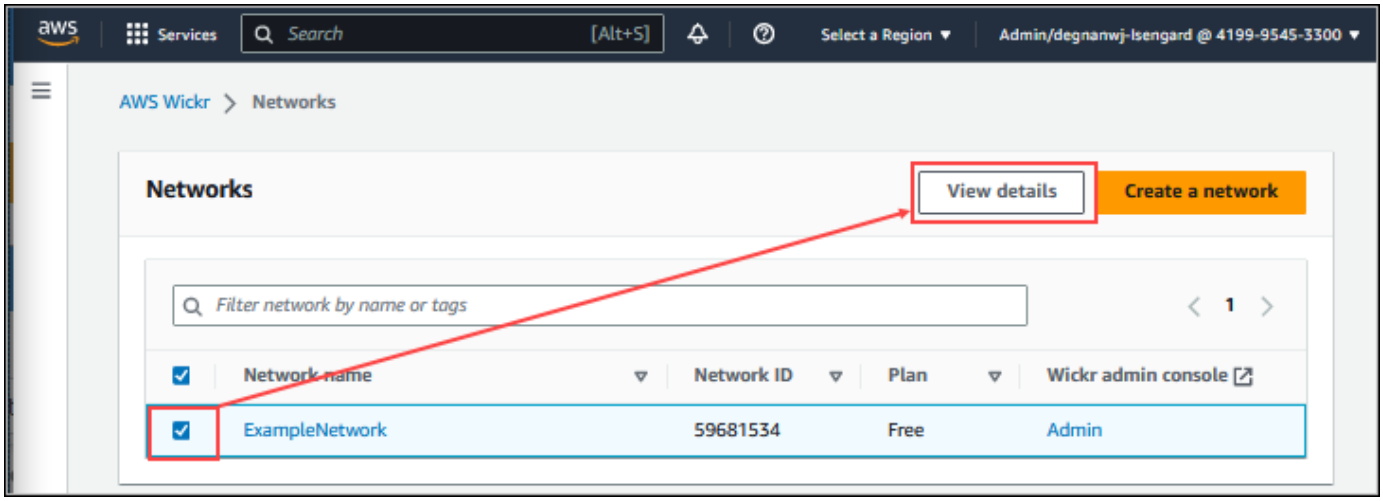
3. 在 Wickr 管理控制台的導覽窗格中，選擇 [網路設定]，然後選擇 [網路設定檔]。

   「網路設定檔」頁面會顯示您的 Wickr 網路名稱和網路 ID。您可以使用網路 ID 來設定同盟。

編輯網路名稱

請完成以下程序以編輯您的 Wickr 網路名稱。

1. 在以下位置 AWS Management Console 打開威克爾的網址：https://console.aws.amazon.com/wickr/。
2. 選擇 [管理網路]。
3. 在 [網路] 頁面上，選取您要編輯之網路名稱旁的核取方塊，然後選擇 [檢視詳細資料]。



4. 在 [網路概觀] 區段中，選擇 [編輯]。
5. 在 [網路名稱] 文字方塊中輸入您的新網路名稱。
6. 選擇 [儲存變更] 以儲存您的新網路名稱。

安全群組

在 AWS Management Console 適用於 Wickr 的 [安全性群組] 區段中，您可以管理安全性群組及其設定，例如密碼複雜性原則、訊息偏好設定、通話功能、安全性功能和網路聯盟。

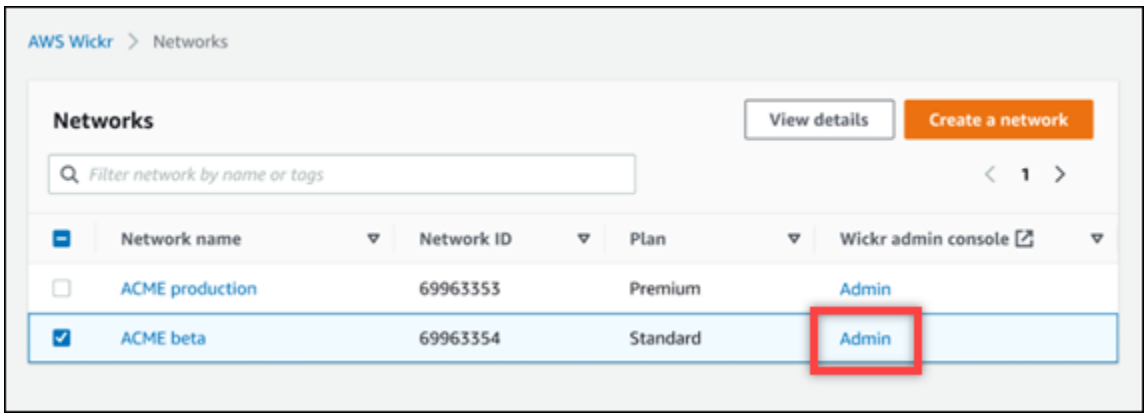
主題

- 檢視安全性群組
- 建立安全群組
- 編輯安全性群組
- 刪除安全群組

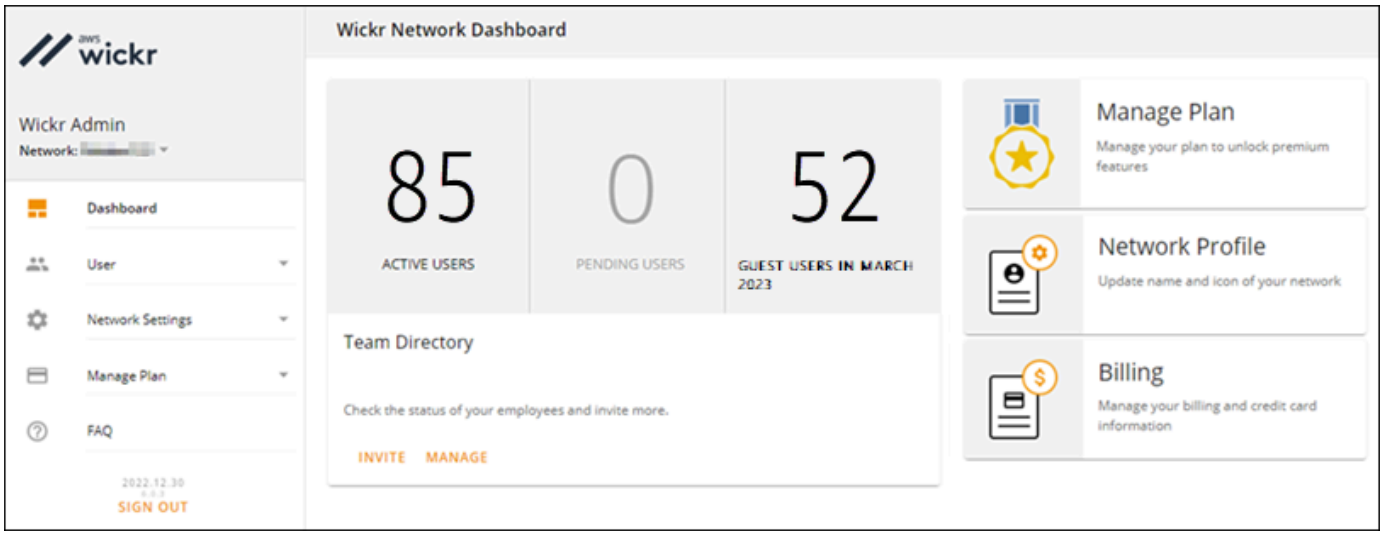
檢視安全性群組

請完成下列程序以檢視安全性群組。

1. 在以下位置 AWS Management Console 打開威克爾的網址：https://console.aws.amazon.com/wickr/。
2. 在 [網路] 頁面上，選擇 [管理員] 連結，瀏覽至該網路的 Wickr 管理控制台。



系統會將您重新導向至特定網路的 Wickr 管理控制台。



3. 在 Wickr 管理控制台的功能窗格中，選擇 [網路設定]，然後選擇 [安全性群組]。

   「安全群組」頁面會顯示您目前的 Wickr 安全性群組，並提供檢視其詳細資料或建立新群組的選項。

建立安全群組

請完成下列程序來建立安全性群組。

1. 在以下位置 AWS Management Console 打開威克爾的網址：https://console.aws.amazon.com/wickr/。
2. 在 [網路] 頁面上，選擇 [管理員] 連結，瀏覽至該網路的 Wickr 管理控制台。

   系統會將您重新導向至特定網路的 Wickr 管理控制台。
3. 在 Wickr 管理控制台的功能窗格中，選擇 [網路設定]，然後選擇 [安全性群組]。

4. 選擇 [新增群組] 以建立新的安全性群組。

   具有預設名稱的新安全性群組會自動新增至安全性群組清單。

   如需編輯新安全性群組的詳細資訊，請參閱編輯安全性群組。

編輯安全性群組

請完成下列程序來編輯安全性群組。

1. 在以下位置 AWS Management Console 打開威克爾的網址：https://console.aws.amazon.com/wickr/。
2. 在 [網路] 頁面上，選擇 [管理員] 連結，瀏覽至該網路的 Wickr 管理控制台。

   系統會將您重新導向至特定網路的 Wickr 管理控制台。
3. 在 Wickr 管理控制台的功能窗格中，選擇 [網路設定]，然後選擇 [安全性群組]。
4. 選擇您要編輯之安全性群組名稱旁邊的 [詳細資料]。

   「安全群組詳細資訊」頁面會在不同標籤中顯示安全性群組的設定。
5. 以下是可用的索引標籤和對應的設定：

   - 安全性群組名稱 — 選擇群組名稱旁邊的鉛筆圖示以編輯名稱。
   - 一般 — 編輯群組的基本配置。
   - 訊息 — 管理群組成員的訊息功能。
   - 呼叫 — 管理群組成員的通話功能。
   - 安全性 — 設定群組的其他安全性功能。
   - 同盟 — 在網路之間進行通訊的能力。您可以在管理控制台中針對安全性群組層級的網路進行設定。AWS Wickr 有兩種聯合類型-本地和全球。
     - 本地聯盟 — 能夠與相同區域內其他網路中的 AWS 使用者聯合。例如，如果加拿大有兩個啟用本機聯盟的網路，它們將能夠彼此通訊。
     - 全域聯合 — 與屬於其他區域的不同網路中的企業 AWS 使用者或使用者聯合的能力。例如，如果加拿大地區的網路中有使用者，在倫敦地區的網路中有使用者，而且兩個網路的全球聯合都已開啟，則他們將能夠彼此通訊。
     - 受限的同盟 — 與屬於不同區域的特定網路 (企業或 AWS) 聯合的能力。管理員可以允許列出其使用者可以聯合的特定網路。限制之後，使用者只能與允許列出的網路中的使用者通訊。

這兩個網路都必須允許從 [同盟] 索引標籤中的安全性群組設定彼此清單，才能使用受限的聯合。

6. 選擇 [儲存] 以儲存您對安全性群組詳細資料所做的編輯。

刪除安全群組

若要刪除安全性群組，請完成下列程序。

1. 在以下位置 AWS Management Console 打開威克爾的網址：https://console.aws.amazon.com/wickr/。
2. 在 [網路] 頁面上，選擇 [管理員] 連結，瀏覽至該網路的 Wickr 管理控制台。

   系統會將您重新導向至特定網路的 Wickr 管理控制台。
3. 在 Wickr 管理控制台的功能窗格中，選擇 [網路設定]，然後選擇 [安全性群組]。
4. 選擇您要刪除之安全性群組名稱旁邊的垂直省略符號圖示。
5. 選擇 [移除] 以刪除安全性群組。

   當您刪除已指派使用者的安全性群組時，這些使用者會自動新增至預設安全性群組。若要修改指派給使用者的安全性群組，請參閱編輯使用者。

單一登入組態

在 Wickr 的 [SSO 組態] 區段中 AWS Management Console ，您可以設定 Wickr 使用單一登入系統進行驗證。SSO 可在與適當的多重要素驗證 (MFA) 系統配對時，提供額外的安全性。威克支持僅使用 OpenID Connect（ OIDC ）的 SSO 提供商。不支援使用安全性宣告標記語言 (SAML) 的提供者。

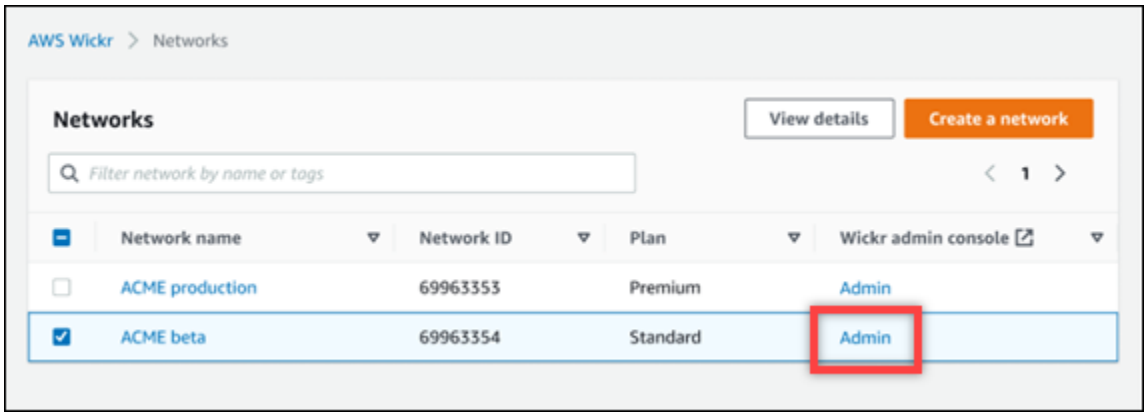
主題

- 檢視 SSO 詳細資料
- 設定 SSO
- 權杖重新整理的寬限期

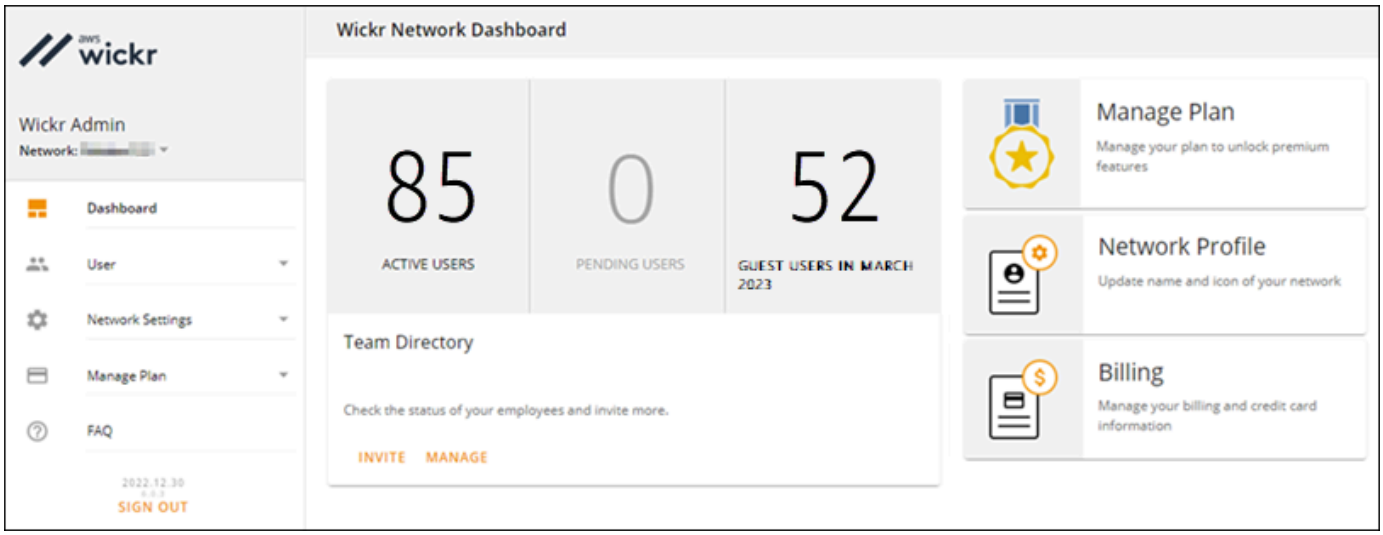
檢視 SSO 詳細資料

完成下列程序以檢視 Wickr 網路目前的單一登入組態 (如果有的話)。您也可以檢視 Wickr 網路的網路端點。

1. 在以下位置 AWS Management Console 打開威克爾的網址：https://console.aws.amazon.com/wickr/。
2. 在 [網路] 頁面上，選擇 [管理員] 連結，瀏覽至該網路的 Wickr 管理控制台。



系統會將您重新導向至特定網路的 Wickr 管理控制台。



3. 在 Wickr 管理控制台的導覽窗格中，選擇 [網路設定]，然後選擇 [SSO 組態]。

「單一登入與 LDAP 組態」頁面會顯示您的 Wickr 網路端點和目前的 SSO 組態。

設定 SSO

如需有關設定 SSO 的詳細資訊，請參閱 Wickr 說明中心中的下列指南：

> **Important**
>
> 設定 SSO 時，您可以指定 Wickr 網路的公司識別碼。請務必記下 Wickr 網路的公司 ID。傳送邀請電子郵件時，您必須將其提供給最終使用者。使用者在註冊您的 Wickr 網路時，必須指定公司 ID。

- 設定 Azure AD 單一登入
- 設定 Okta 單一登入

權杖重新整理的寬限期

有時候，身分識別提供者可能會遇到暫時或延長中斷的情況，這可能導致您的使用者因為其用戶端工作階段的重新整理權杖失敗而意外登出。若要避免此問題發生，您可以建立寬限期，讓使用者保持登入狀態，即使他們的用戶端重新整理權杖在這類中斷期間失敗也是如此。

以下是寬限期的可用選項：

- 無寬限期 (預設)：重新整理權杖失敗後，使用者將立即登出。
- 30 分鐘寬限期：重新整理權杖失敗後，使用者最多可保持登入狀態 30 分鐘。
- 60 分鐘寬限期：重新整理權杖失敗後，使用者最多可保持登入狀態 60 分鐘。

閱讀回條

Wickr 上的讀取回條是發送給發件人的通知，以顯示他們的郵件何時被讀取。這些收據可在 one-on-one 對話中使用。發送的郵件將顯示一個複選標記，並且將出現帶有勾選標記的實心圓圈以供讀取的消息。若要在外部交談期間查看郵件的已讀標記，兩個網路都應啟用讀取回條。

管理員可以在管理員面板中啟用或停用已讀標記。此設定將套用至整個網路。

請完成下列程序，以啟用或停用讀取回條。

1. 在以下位置 AWS Management Console 打開威克爾的網址：https://console.aws.amazon.com/wickr/。
2. 在 Wickr 管理控制台的導覽窗格中，選擇 [網路設定]，然後選擇 [網路設定檔]。
3. 在 [網路設定檔] 頁面的 [讀取回條] 區段中，選擇 [編輯]。
4. 選取啟用或停用。

網路標籤

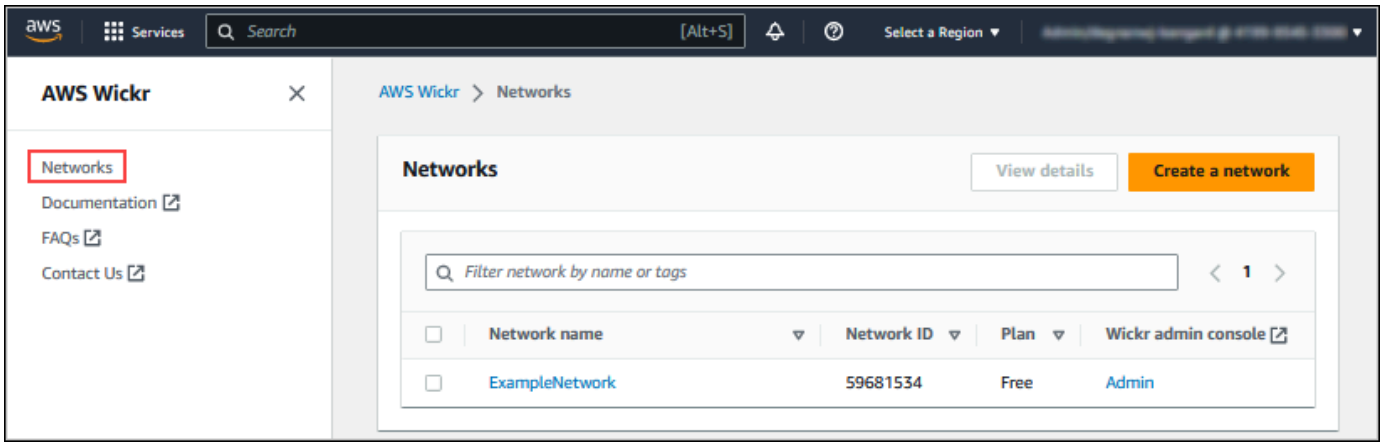
您可以將標籤套用至 Wickr 網路。然後，您可以使用這些標籤來搜索和過濾 Wickr 網絡或跟踪您的 AWS 費用。您可以在 Wickr 的 [網路概觀] 頁面中設定 AWS Management Console 網路標記。

標籤是套用至資源的索引鍵值配對，以保存有關該資源的中繼資料。每個標籤都是由鍵和值組成的標籤。如需有關標籤的詳細資訊，另請參閱什麼是標籤？ 和標記使用案例。

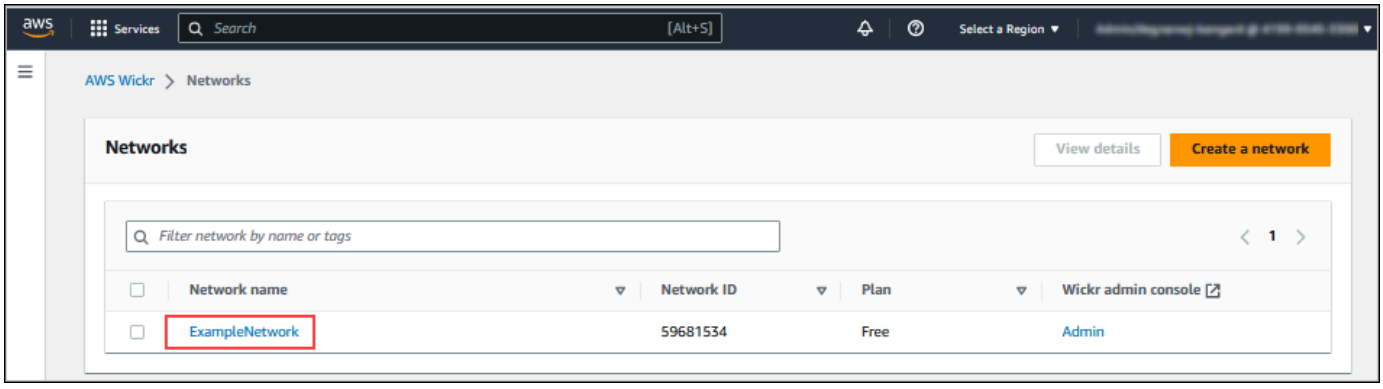
管理網路標籤

請完成下列程序來管理 Wickr 網路的網路標籤。

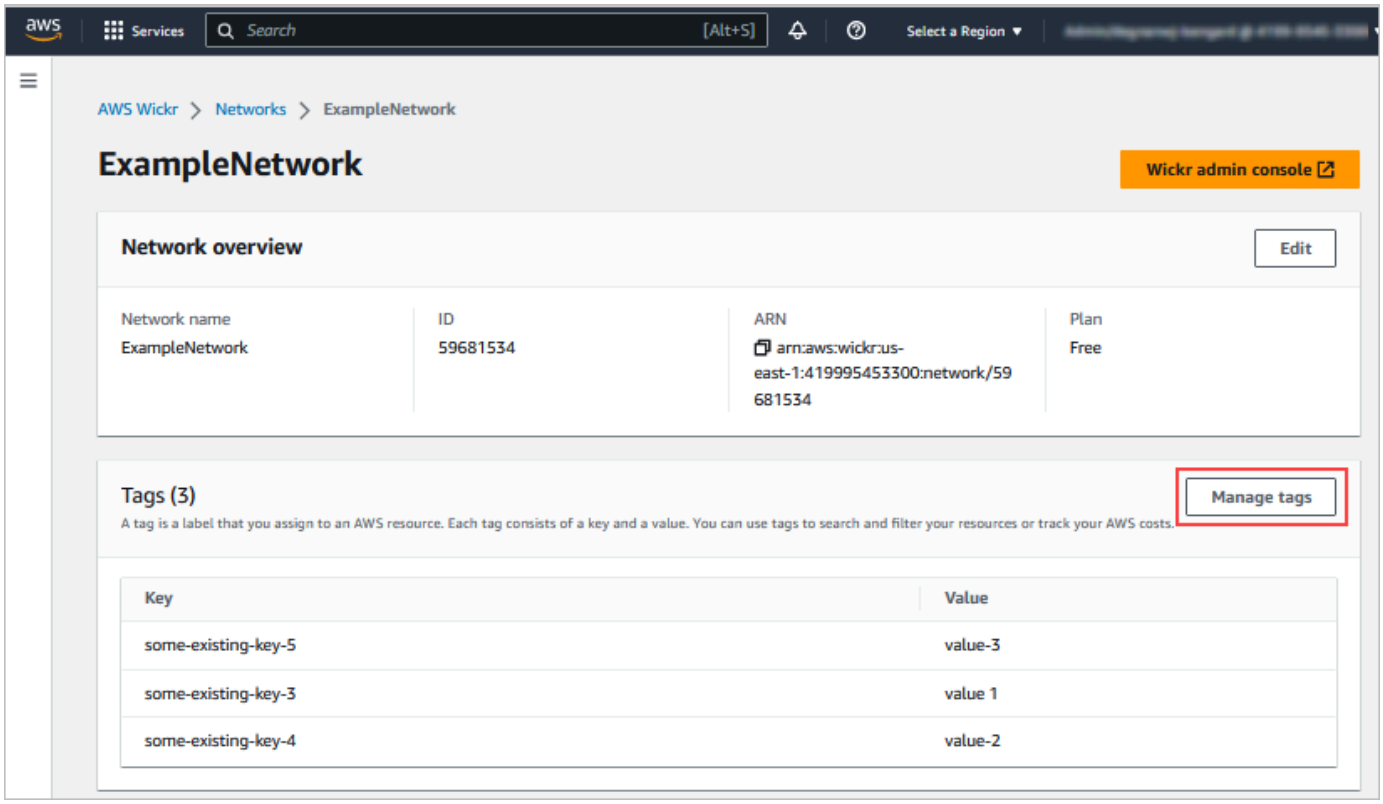
1. 在以下位置 AWS Management Console 打開威克爾的網址：https://console.aws.amazon.com/wickr/。
2. 從的導覽窗格中選取 Wickr AWS Management Console 的「網路」。



3. 在 [網路] 頁面上，選擇您要管理其標記的網路名稱。



4. 在 [網路總覽] 頁面中，選擇 [管理標籤]。



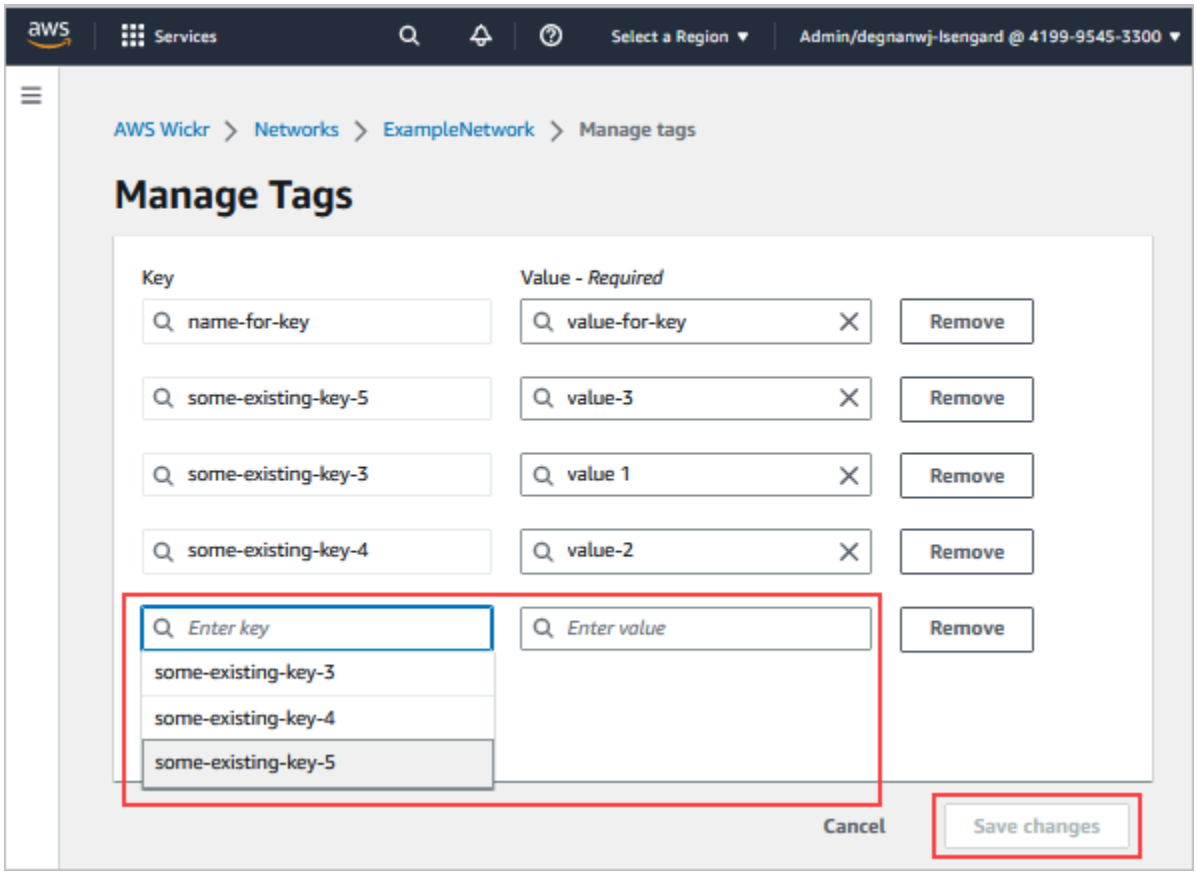
5. 在「管理標籤」頁面上，您可以完成下列其中一個選項：

   - 新增標籤 — 以金鑰和值配對的形式輸入新標籤。選擇 [新增標籤] 以新增多個金鑰值配對。標籤會區分大小寫。如需詳細資訊，請參閱 新增網路標籤。
   - 編輯現有標籤 — 選取現有標籤的金鑰或值文字，然後在文字方塊中輸入修改內容。如需詳細資訊，請參閱 編輯網路標籤。
   - [移除現有的標籤] — 選擇要刪除的標籤旁邊列出的 [移除] 按鈕。如需詳細資訊，請參閱 移除網路標籤。

新增網路標籤

請完成下列程序，將標籤新增至您的 Wickr 網路。如需管理標籤的詳細資訊，請參閱管理網路標籤。

1. 在管理標籤 頁面上，選擇新增標籤。
2. 在出現的空白「關鍵字」和「值」欄位中，輸入新的標籤鍵和值。
3. 選擇 [儲存變更] 以儲存新標籤。

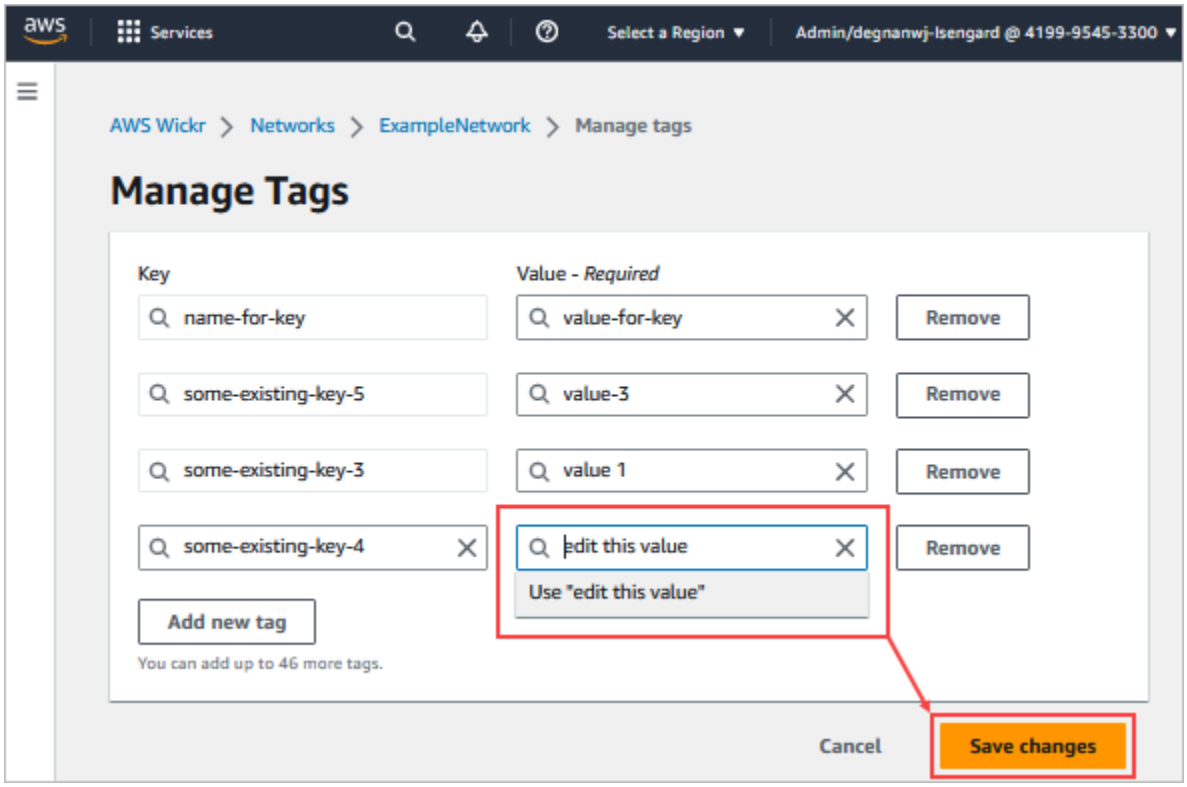


編輯網路標籤

請完成下列程序，以編輯與 Wickr 網路相關聯的標籤。如需管理標籤的詳細資訊，請參閱管理網路標籤。

1. 在「管理標籤」頁面上，編輯標籤的值。

> **Note**
>
> 您無法編輯標籤的金鑰。請改為移除金鑰和值配對，然後使用新金鑰新增標籤。

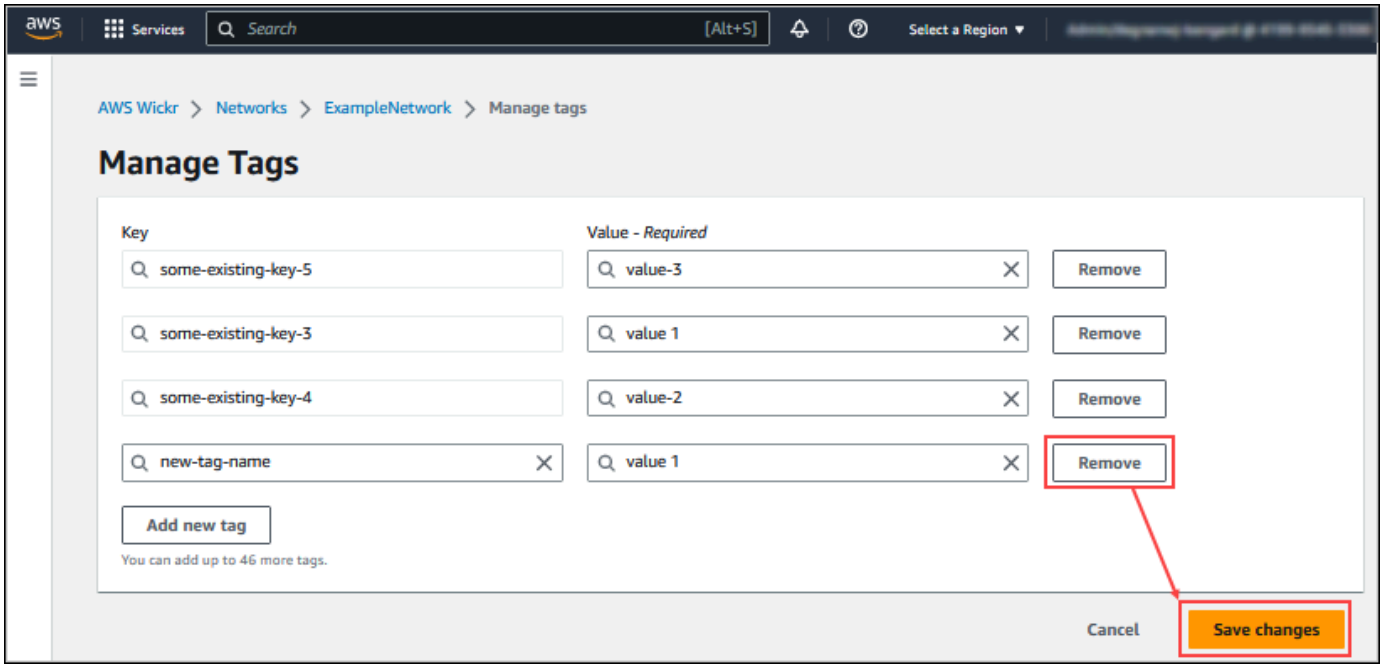


2. 選擇 [儲存變更] 以儲存您的編輯。

移除網路標籤

完成下列程序，即可從 Wickr 網路移除標籤。如需管理標籤的詳細資訊，請參閱管理網路標籤。

1. 在「管理標籤」頁面上，為您要移除的標籤選擇「移除」。



2. 選擇 [儲存變更] 以儲存您的編輯。

管理網絡計劃

在 Wickr 的「管理計劃」區段中，您可以根據您的業務需求來管理您的網路計劃。 AWS Management Console

若要管理您的網路計劃，請完成以下程序。

1. 在以下位置 AWS Management Console 打開威克爾的網址：https://console.aws.amazon.com/wickr/。
2. 在 Wickr 管理控制台的功能窗格中，選擇 [管理方案]，然後選擇 [我的方案]。
3. 在 [我的方案] 頁面上，選擇您想要的網路方案。您可以選擇下列其中一項來修改目前的網路方案：

   - 標準 — 適用於需要管理控制和彈性的小型和大型企業團隊。
   - 進階版或免費試用版 — 適用於需要最高功能限制、精細管理控制和資料保留的企業。

     管理員可以選擇高級免費試用選項，該選項最多可供 30 個用戶使用，並持續三個月。此優惠適用於新的無法試用和標準計劃。管理員可以在高級免費試用期內升級或降級到高級或標準計劃。

> **Note**
>
> 若要停止在您的網路上使用和計費，請移除所有使用者，包括網路中的所有暫停使用者。

高級免費試用版限制

以下限制適用於高級免費試用：

- 如果計劃之前曾經註冊過高級免費試用，則該計劃將不符合再次試用的資格。
- 每個 AWS 帳戶只能註冊一個網絡免費試用。
- 在高級免費試用期間，訪客用戶功能不可用。
- 如果標準網路有超過 30 位使用者，則無法升級為高級免費試用版。

資料保留

AWS Wickr 資料保留可以保留網路中的所有對話。這包括網內（內部）成員和與您的網絡聯盟的其他團隊（外部）之間的「組」或「聊天室」中的直接消息對話和對話。資料保留僅適用於選擇加入資料保留的 AWS Wickr 進階方案使用者和企業客戶。有關高級計劃的更多信息，請參閱 Wickr 定價

當網路管理員設定並啟用其網路的資料保留時，其網路中共用的所有訊息和檔案都會依照組織的合規性原則保留。網路管理員可在外部位置存取這些 .txt 檔案輸出 (例如：本機儲存、Amazon S3 儲存貯體或根據使用者選擇的任何其他儲存)，從中進行分析、清除或傳輸。

> **Note**
>
> Wickr 永遠不會訪問您的消息和文件。因此，您有責任配置數據保留系統。

主題

檢視資料保留詳情

請完成下列程序以檢視 Wickr 網路的資料保留詳細資料。您也可以啟用或停用 Wickr 網路的資料保留。

1. 在以下位置 AWS Management Console 打開威克爾的網址：https://console.aws.amazon.com/wickr/。
2. 選擇 [管理網路]。
3. 在 Wickr 管理控制台的導覽窗格中，選擇 [網路設定]，然後選擇 [資料保留]。

   「資料保留」頁面會顯示設定資料保留的步驟，以及啟用或停用資料保留功能的選項。如需設定資料保留的詳細資訊，請參閱設定資料保留。

> **Note**
>
> 啟動資料保留時，網路中的所有使用者都會看見「開啟資料保留」訊息，通知他們已啟用保留的網路。

設定資料保留

若要為 AWS Wickr 網路設定資料保留，您必須將資料保留機器人 Docker 映像部署到主機上的容器，例如本機電腦或 Amazon Elastic Compute Cloud (Amazon EC2) 中的執行個體。部署機器人後，您可以將其設定為在本機或 Amazon Simple Storage Service (Amazon S3) 貯體中存放資料。您也可以將資料保留機器人設定為使用其他AWS服務，例如 AWS Secrets Manager (Secrets ManagerCloudWatch)、Amazon CloudWatch ()、亞馬遜簡單通知服務 (Amazon SNS) 和 AWS Key Management Service (AWS KMS)。下列主題說明如何設定及執行 Wickr 網路的資料保留機器人。

主題

- 設定資料保留的必要條件
- 密碼
- 儲存選項
- 環境變數
- Secrets Manager 值
- 將資料保留與AWS服務搭配使用的 IAM 政策

- 啟動資料保留機器人
- 停止資料保留機器人

設定資料保留的必要條件

在開始之前，您必須從 Wickr 取得資料保留機器人名稱 (標記為使用者名稱) 和初始密碼。AWS Management Console您必須在第一次啟動資料保留機器人時指定這兩個值。您也必須在主控台中啟用資料保留功能。如需詳細資訊，請參閱 檢視資料保留詳情。

密碼

第一次啟動資料保留機器人時，請使用下列其中一個選項指定初始密碼：

- 環WICKRIO_BOT_PASSWORD境變數。資料保留機器人環境變數概述於本指南後環境變數面的章節中。
- 密碼 Secrets Manager 中由**AWS_SECRET_NAME**環境變數所識別的密碼值。資料保留機器人的「Secrets Manager」值概述於本指南後Secrets Manager 值面的章節中。
- 當資料保留機器人提示時，請輸入密碼。您需要使用該-ti選項以互動式 TTY 存取權來執行資料保留機器人。

當您首次設定資料保留機器人時，系統會產生新密碼。如果您需要重新安裝資料保留機器人，請使用產生的密碼。初始密碼在初始安裝資料保留機器人之後無效。

新生成的密碼將被顯示為顯示在下面的例子。

> **Important**
>
> 將密碼儲存於安全處。如果您遺失密碼，您將無法重新安裝資料保留機器人。不要共享此密碼。它提供了為您的 Wickr 網絡啟動數據保留的功能。

```
************************************************************************
**** GENERATED PASSWORD
**** DO NOT LOSE THIS PASSWORD, YOU WILL NEED TO ENTER IT EVERY TIME
**** TO START THE BOT
 "HuEXAMPLERAW4lGgEXAMPLEn"
 ************************************************************************
```

儲存選項

啟用資料保留功能並為您的 Wickr 網路設定資料保留機器人之後，它會擷取您網路中傳送的所有訊息和檔案。訊息會儲存在限制為特定大小或時間限制的檔案中，這些檔案可以使用環境變數進行配置。如需詳細資訊，請參閱 環境變數。

您可以設定下列其中一個選項來儲存此資料：

- 將所有捕獲的消息和文件存儲在本地。此為預設選項。您有責任將本機檔案移至另一個系統以進行長期儲存，並確定主機磁碟不會耗盡記憶體或空間。
- 將所有擷取的訊息和檔案存放在 Amazon S3 儲存貯體中。資料保留機器人會將所有解密的訊息和檔案儲存到您指定的 Amazon S3 儲存貯體。擷取的訊息和檔案成功儲存至儲存貯體後，會從主機移除這些訊息和檔案。
- 將所有擷取的訊息和加密檔案存放在 Amazon S3 儲存貯體中。資料保留機器人會使用您提供的金鑰重新加密所有擷取的訊息和檔案，並將它們儲存到您指定的 Amazon S3 儲存貯體。擷取的訊息和檔案成功重新加密並儲存至儲存貯體後，會從主機中移除這些訊息和檔案。您將需要軟件來解密消息和文件。

  如需建立 Amazon S3 儲存貯體以搭配資料保留機器人使用的詳細資訊，請參閱 Amazon S3 使用者指南中的建立儲存貯體

環境變數

您可以使用下列環境變數來設定資料保留機器人。您可以在執行資料保留機器人 Docker 映像時使用 -e選項來設定這些環境變數。如需詳細資訊，請參閱 啟動資料保留機器人。

> **Note**
>
> 除非另有指定，否則這些環境變數是選用的

使用下列環境變數來指定資料保留機器人認證：

- `WICKRIO_BOT_NAME`— 資料保留機器人的名稱。當您執行資料保留機器人 Docker 映像時，需要此變數。
- `WICKRIO_BOT_PASSWORD`— 資料保留機器人的初始密碼。如需詳細資訊，請參閱 設定資料保留的必要條件。如果您不打算使用密碼提示啟動資料保留機器人，或者您不打算使用 Secrets Manager 來儲存資料保留機器人認證，則需要此變數。

使用下列環境變數來設定預設資料保留串流功能：

- WICKRIO_COMP_MESGDEST— 將串流訊息之目錄的路徑名稱。預設值為 /tmp/*<botname>*/compliance/messages。
- WICKRIO_COMP_FILEDEST— 將串流處理檔案之目錄的路徑名稱。預設值為 /tmp/*<botname>*/compliance/attachments。
- WICKRIO_COMP_BASENAME— 接收郵件檔案的基本名稱。預設值為 receivedMessages。
- WICKRIO_COMP_FILESIZE— 接收郵件檔案的最大檔案大小 (以 KiB 為單位)。達到最大大小時會啟動新檔案。預設值為1000000000，如 1024 GiB 中所示。
- WICKRIO_COMP_TIMEROTATE— 數據保留機器人將收到的消息放入收到的消息文件中的時間量（以分鐘為單位）。達到時間限制時，會啟動新檔案。您只能使用檔案大小或時間來限制接收郵件檔案的大小。預設值為0，如無限制。

使用下列環境變數來定義要使用AWS 區域的預設值。

- AWS_DEFAULT_REGION— 用於 Secrets Manager 之類的AWS服務的預設值 AWS 區域 (不適用於 Amazon S3 或AWS KMS)。如果未定義此環境變數，則依預設會使用「us-east-1區域」(Region)。

使用下列環境變數來指定當您選擇使用 Secrets Manager 來儲存資料保留機器人認證和AWS服務資訊時要使用的 Secrets Manager 密碼。如需有關您可以儲存在 Secrets Manager 中的值的詳細資訊，請參閱Secrets Manager 值。

- AWS_SECRET_NAME— Secret Manager 密碼的名稱，其中包含資料保留機器人所需的認證和AWS服務資訊。
- AWS_SECRET_REGION— AWS 秘密所在的. AWS 區域 如果您使用的是AWS秘密，並且未定義此AWS_DEFAULT_REGION值，則將使用該值。

> **Note**
>
> 您可以將下列所有環境變數儲存為「Secrets Manager」中的值。如果您選擇使用 Secrets Manager，並將這些值儲存在該處，則在執行資料保留機器人 Docker 映像時，不需要將它們指定為環境變數。您只需要指定本指南前面所述的AWS_SECRET_NAME環境變數。如需詳細資訊，請參閱 Secrets Manager 值。

選擇將訊息和檔案存放到儲存貯體時，請使用下列環境變數指定 Amazon S3 儲存貯體。

- `WICKRIO_S3_BUCKET_NAME`— 將在其中存放訊息和檔案的 Amazon S3 儲存貯體的名稱。
- `WICKRIO_S3_REGION`— 將存放訊息和檔案的 Amazon S3 儲存貯體的AWS區域。
- `WICKRIO_S3_FOLDER_NAME`— Amazon S3 儲存貯體中存放訊息和檔案的選用資料夾名稱。此資料夾名稱前面會加上儲存到 Amazon S3 儲存貯體的訊息和檔案的金鑰。

當您選擇在將檔案儲存到 Amazon S3 儲存貯體時使用用戶端加密來重新加密檔案時，請使用下列環境變數來指定AWS KMS詳細資訊。

- `WICKRIO_KMS_MSTRKEY_ARN`— AWS KMS 主金鑰的 Amazon 資源名稱 (ARN)，用於在資料保留機器人上的訊息檔案和檔案儲存到 Amazon S3 儲存貯體之前，重新加密這些檔案和檔案。
- `WICKRIO_KMS_REGION`— AWS KMS 主金鑰所在的AWS區域。

當您選擇將資料保留事件傳送至 Amazon SNS 主題時，請使用下列環境變數指定 Amazon SNS 詳細資訊。發送的事件包括啟動，關閉以及錯誤條件。

- `WICKRIO_SNS_TOPIC_ARN`— 您希望將資料保留事件傳送至的 Amazon SNS 主題的 ARN。

使用下列環境變數將資料保留指標傳送至 CloudWatch。如果有指定，則每 60 秒會產生一次量度。

- `WICKRIO_METRICS_TYPE`— 將此環境變數的值設定`cloudwatch`為傳送量度 CloudWatch。

Secrets Manager 值

您可以使用 Secrets Manager 來儲存資料保留機器人登入資料和AWS服務資訊。如需有關建立 Secrets Manager 碼的詳細資訊，請參閱《AWS Secrets Manager秘 Sec rets Manager 使用指南》中的建立密碼。

密碼管理員密碼可以具有下列值：

- `password`— 數據保留機器人密碼。
- `s3_bucket_name`— 將在其中存放訊息和檔案的 Amazon S3 儲存貯體的名稱。如果未設定，則會使用預設的檔案串流。
- `s3_region`— 將存放訊息和檔案的 Amazon S3 儲存貯體的AWS區域。

- s3_folder_name— Amazon S3 儲存貯體中存放訊息和檔案的選用資料夾名稱。此資料夾名稱前面會加上儲存到 Amazon S3 儲存貯體的訊息和檔案的金鑰。
- kms_master_key_arn— AWS KMS 主金鑰的 ARN，用來在資料保留機器人上的訊息檔案和檔案儲存至 Amazon S3 儲存貯體之前，重新加密這些檔案和檔案。
- kms_region— AWS KMS 主金鑰所在的AWS區域。
- sns_topic_arn— 您希望將資料保留事件傳送至的 Amazon SNS 主題的 ARN。

將資料保留與AWS服務搭配使用的 IAM 政策

如果您打算搭配 Wickr 資料保留機器人使用其他AWS服務，則必須確保主機具有適當的 AWS Identity and Access Management (IAM) 角色和政策來存取它們。您可以將資料保留機器人設定為使用 Secrets Manager CloudWatch、Amazon S3、Amazon SNS 和AWS KMS. 下列 IAM 政策允許存取這些服務的特定動作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "secretsmanager:GetSecretValue",
                "sns:Publish",
                "cloudwatch:PutMetricData",
                "kms:GenerateDataKey"
            ],
            "Resource": "*"
        }
    ]
}
```

您可以針對每個要允許主機上的容器存取的服務識別特定物件，來建立更嚴格的 IAM 政策。針對您不打算使用的AWS服務移除動作。例如，如果您只想使用 Amazon S3 儲存貯體，請使用下列政策移除secretsmanager:GetSecretValue、sns:Publishkms:GenerateDataKey、和cloudwatch:PutMetricData動作。

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

```
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "*"
        }
    ]
}
```

如果您使用 Amazon Elastic Compute Cloud (Amazon EC2) 執行個體託管資料保留機器人，請使用 Amazon EC2 常見案例建立 IAM 角色，並使用上述政策定義指派政策。

啟動資料保留機器人

在執行資料保留機器人之前，您應該先決定要如何設定資料保留機器人。如果您打算在以下主機上執行機器人：

- 將無法訪問AWS服務，那麼您的選擇是有限的。在這種情況下，您將使用默認消息流選項。您應該決定是否要將捕獲的消息文件的大小限制為特定的大小或時間間隔。如需詳細資訊，請參閱 環境變數。
- 將有權訪問AWS服務，然後您應該創建一個 Secrets Manager 密鑰來存儲機器人憑據和AWS服務配置詳細信息。設定AWS服務後，您可以繼續啟動資料保留機器人 Docker 映像檔。如需有關您可以儲存在 Secret Manager 密碼中的詳細資訊，請參閱 Secrets Manager 值

以下各節顯示用於執行資料保留機器人 Docker 映像的範例命令。在每個範例指令中，以您自己的範例值取代下列範例值：

- *compliance_1234567890_bot*使用您的數據保留機器人的名稱。
- *password*使用您的數據保留機器人的密碼。
- *wickr/data/retention/bot*與您的 Secrets Manager 秘密的名稱與您的數據保留機器人一起使用。
- *bucket-name*使用將存放訊息和檔案的 Amazon S3 儲存貯體的名稱。
- *folder-name*在 Amazon S3 儲存貯體中存放訊息和檔案的資料夾名稱。
- *us-east-1*使用您指定的資源的AWS區域。例如，AWS KMS主金鑰的區域或 Amazon S3 儲存貯體的區域。

- *arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-a617-abababababab*使用AWS KMS主金鑰的 Amazon 資源名稱 (ARN)，用於重新加密訊息檔案和檔案。

使用密碼環境變數啟動機器人 (無AWS服務)

下列 Docker 指令會啟動資料保留機器人。密碼是使用WICKRIO_BOT_PASSWORD環境變數指定的。機器人開始使用預設檔案串流，並使用本指南環境變數章節中定義的預設值。

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
wickr/bot-compliance-cloud:latest
```

使用密碼提示啟動機器人（無AWS服務）

下列 Docker 指令會啟動資料保留機器人。系統會在資料保留機器人提示時輸入密碼。它將使用本指南各環境變數節中定義的預設值開始使用預設檔案串流。

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
wickr/bot-compliance-cloud:latest

docker attach compliance_1234567890_bot
.
.
.
Enter the password:************
Re-enter the password:************
```

使用接收密碼提示的-ti選項運行機器人。您還應該在啟動 docker 映像後立即運行該docker attach *<container ID or container name>*命令，以便獲得密碼提示符。您應該在腳本中運行這兩個命令。如果您附加到 docker 圖像，但沒有看到提示，請按 Enter 鍵，您將看到提示。

以 15 分鐘的消息文件輪替（無AWS服務）啟動機器人

下列 Docker 指令會使用環境變數啟動資料保留機器人。它還將其配置為將收到的消息文件旋轉到 15 分鐘。

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
-e WICKRIO_COMP_TIMEROTATE=15 \
wickr/bot-compliance-cloud:latest
```

啟動機器人並使用密碼管理員指定初始密碼

您可以使用 Secrets Manager 來識別資料保留機器人的密碼。當您啟動資料保留機器人時，您將需要設定環境變數，以指定 Secrets Manager 儲存此資訊的位置。

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e AWS_SECRET_NAME='wickr/data/retention/bot' \
wickr/bot-compliance-cloud:latest
```

該wickrpro/compliance/compliance_1234567890_bot密碼具有以下秘密值，顯示為明文。

```
{
    "password":"password"
}
```

啟動機器人並使用 Secrets Manager 器設定 Amazon S3

您可以使用 Secrets Manager 託管登入資料和 Amazon S3 儲存貯體資訊。當您啟動資料保留機器人時，您將需要設定環境變數，以指定 Secrets Manager 儲存此資訊的位置。

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
 -e AWS_SECRET_NAME='wickr/data/retention/bot' \
wickr/bot-compliance-cloud:latest
```

該wickrpro/compliance/compliance_1234567890_bot密碼具有以下秘密值，顯示為明文。

```
{
    "password":"password",
    "s3_bucket_name":"bucket-name",
```

```
    "s3_region":"us-east-1",
    "s3_folder_name":"folder-name"
}
```

機器人收到的消息和文件將放在名為的文件夾中的bot-compliance存儲桶中network1234567890。

啟動機器人並AWS KMS使用 Secrets Manager 器設定 Amazon S3

您可以使用 Secrets Manager 來託管登入資料、Amazon S3 儲存貯體和AWS KMS主金鑰資訊。當您啟動資料保留機器人時，您將需要設定環境變數，以指定 Secrets Manager 儲存此資訊的位置。

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
 -e AWS_SECRET_NAME='wickr/data/retention/bot' \
wickr/bot-compliance-cloud:latest
```

該wickrpro/compliance/compliance_1234567890_bot密碼具有以下秘密值，顯示為明文。

```
{
    "password":"password",
    "s3_bucket_name":"bucket-name",
    "s3_region":"us-east-1",
    "s3_folder_name":"folder-name",
    "kms_master_key_arn":"arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-
a617-abababababab",
    "kms_region":"us-east-1"
}
```

機器人接收到的訊息和檔案將使用 ARN 值所識別的 KMS 金鑰加密，然後在名為「network1234567890」的資料夾中放入「機器人相容性」值區中。確定您有適當的 IAM 政策設定。

啟動機器人並使用環境變數設定 Amazon S3

如果您不想使用 Secrets Manager 來託管資料保留機器人認證，您可以使用下列環境變數啟動資料保留機器人 Docker 映像檔。您必須使用WICKRIO_BOT_NAME環境變數識別資料保留機器人的名稱。

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
```

```
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
-e WICKRIO_S3_BUCKET_NAME='bucket-name' \
-e WICKRIO_S3_FOLDER_NAME='folder-name' \
-e WICKRIO_S3_REGION='us-east-1' \
wickr/bot-compliance-cloud:latest
```

您可以使用環境值來識別資料保留機器人的登入資料、Amazon S3 儲存貯體的相關資訊，以及預設檔案串流的組態資訊。

停止資料保留機器人

在數據保留機器人上運行的軟件將捕獲SIGTERM信號並正常關閉。使用下列範例所示的`docker stop <container ID or container name>`命令，對資料保留機器人 Docker 映像發出SIGTERM指令。

```
docker stop compliance_1234567890_bot
```

取得資料保留記錄

在資料保留機器人 Docker 映像上執行的軟體將輸出至目錄中的記/tmp/*<botname>*/logs錄檔。他們將旋轉到最多 5 個文件。您可以通過運行以下命令獲取日誌。

```
docker logs <botname>
```

範例：

```
docker logs compliance_1234567890_bot
```

資料保留指標和事件

以下是目前由 5.116 版 AWS Wickr 資料保留機器人所支援的 Amazon () 指標和亞馬遜簡單通知服務 (Amazon SNS) 事件。 CloudWatch CloudWatch

主題

- CloudWatch 度量
- Amazon SNS 事件

CloudWatch 度量

指標由機器人以 1 分鐘的間隔生成，並將其傳輸到與運行數據保留機器人 Docker 映像的帳戶相關聯的 CloudWatch 服務。

以下是資料保留機器人支援的現有指標。

指標	描述
在線留言 _Rx	收到的訊息。
訊息 (_Rx_ 失敗)	無法處理收到的郵件。
訊息已儲存 (_S)	已儲存至接收訊息檔案的訊息。
訊息 (_S) 已儲存 (_ 失敗)	無法將訊息儲存至接收的郵件檔案。
檔案已儲存	收到的文件。
檔案儲存位元組	接收檔案的位元組數。
檔案儲存 (_ 失敗)	無法儲存檔案。
登入	登錄（通常每個間隔都是 1）。
登入失敗	登錄失敗（通常每個間隔都是 1）。
S3_ 後錯誤	將訊息檔案和檔案張貼到 Amazon S3 儲存貯體時發生錯誤。
看門狗故障	看門狗故障。
看門警告	看門狗警告。

指標會產生以供使用 CloudWatch。用於機器人的命名空間是`WickrIO`。每個量度都有一個維度陣列。以下是與上述量度一起公佈的維度清單。

維度	Value
Id	機器人的使用者名稱。

維度	Value
裝置	特定機器人裝置或執行個體的說明。如果您正在執行多個機器人裝置或執行個體，很有用
產品	適用於機器人的產品。可以是`WickrPro_ Alpha`、`Beta`、或`Production` 附加。`WickrEnterprise_`
BotType	機器人類型。標記為合規性機器人的合規性。
網路	關聯網路的識別碼。

Amazon SNS 事件

下列事件會發佈到 Amazon SNS 主題，這些主題是使用`WICKRIO_SNS_TOPIC_ARN`環境變數或機 `sns_topic_arn` Secrets Manager 碼值識別的 Amazon 資源名稱 (ARN) 值所定義。如需詳細資訊，請參閱 環境變數 及 Secrets Manager 值。

資料保留機器人所產生的事件會以 JSON 字串的形式傳送。以下值包含在 5.116 版資料保留機器人的事件中。

名稱	值
合規機器人	資料保留機器人的使用者名稱。
数据时间	事件發生的日期和時間。
裝置	特定機器人裝置或執行個體的說明。如果您正在運行多個 bot 實例，則非常有用。
碼頭映像	與機器人相關聯的泊塢視窗映像檔。
碼頭標籤	泊塢視窗映像檔的標籤或版本。
message	事件訊息。如需更多資訊，請參閱重大事件及正常事件。
notificationType	這個值將是`Bot Event`。

名稱	值
severity	事件的嚴重性。可以是 normal 或 critical。

您必須訂閱 Amazon SNS 主題，才能接收事件。如果您使用電子郵件地址訂閱，將向您發送一封電子郵件，其中包含類似於以下示例的信息。

```
{
"complianceBot": "compliance_1234567890_bot",
 "dateTime": "2022-10-12T13:05:39",
 "device": "Desktop 1234567890ab",
 "dockerImage": "wickr/bot-compliance-cloud",
 "dockerTag": "5.116.13.01",
 "message": "Logged in",
 "notificationType": "Bot Event",
 "severity": "normal"
}
```

重大事件

這些事件將導致機器人停止或重新啟動。重新啟動次數受到限制，以避免造成其他問題。

登入失敗

以下是當機器人無法登錄時可能產生的事件。每個訊息都會指出登入失敗的原因。

事件類型	事件訊息
失敗登錄	憑證錯誤。檢查密碼。
失敗登錄	找不到使用者。
失敗登錄	帳戶或裝置已暫停。
佈建中	使用者結束指令。
佈建中	config.wickr 檔案的密碼錯誤。
佈建中	無法讀取config.wickr 檔案。

事件類型	事件訊息
失敗登錄	全部登入失敗。
失敗登錄	新用戶，但數據庫已經存在。

更多關鍵事件

事件類型	事件訊息
暫停帳戶	slotAdminUser暫停ClientMain：程式碼 (% 1)：原因：% 2
BotDevice 暫停	設備已暫停！
WatchDog	系 SwitchBoard 統停機時間超過 *N* > 分鐘
S3 故障	無法在 S3 儲存貯體上放置檔案 < 檔案*##* ≫。錯誤：< *AWS-##* >
後備鍵	服務器提交後備密鑰：不是可識別的客戶端活動後備密鑰。請將日誌提交到桌面工程。

正常事件

以下是警告您有關正常操作發生的事件。在特定時間段內發生過多的這些類型的事件可能會引起關注。

已新增至帳戶的裝置

當新裝置新增至資料保留機器人帳戶時，會產生此事件。在某些情況下，這可能是有人建立資料保留機器人執行個體的重要指示。以下是此事件的消息。

```
A device has been added to this account!
```

機器人已登入

此事件會在機器人成功登入時產生。以下是此事件的消息。

```
Logged in
```

關閉

此事件會在機器人關閉時產生。如果使用者沒有明確啟動此功能，則可能是問題的指示。以下是此事件的消息。

```
Shutting down
```

可用的更新

此事件會在資料保留機器人啟動時產生，並識別有可用的關聯 Docker 映像檔的較新版本。此事件會在機器人啟動時產生，並且每天都會產生。此事件包括versions陣列欄位，可識別可用的新版本。以下是這個事件的樣子的一個例子。

```
{
  "complianceBot": "compliance_1234567890_bot",
  "dateTime": "2022-10-12T13:05:55",
  "device": "Desktop 1234567890ab",
  "dockerImage": "wickr/bot-compliance-cloud",
  "dockerTag": "5.116.13.01",
  "message": "There are updates available",
  "notificationType": "Bot Event",
  "severity": "normal",
  "versions": [
    "5.116.10.01"
  ]
}
```

什麼是 ATAK？

Android 團隊意識套件（ATAK）-或用於軍事用途的 Android 戰術突擊套件（也是 ATAK）是一款智能手機地理空間基礎架構和情境感知應用程序，可實現在地理位置上的安全協作。雖然它最初設計用於作戰區，但 ATAK 已經過改編以適應當地，州和聯邦機構的任務。

主題

- 在威克爾網路儀表板中啟用 ATAK
- 關於 ATAK 的其他資訊
- 安裝並配對 ATAK 的威克爾插件
- 撥打及接聽電話

- 傳送檔案
- 傳送安全語音訊息 (Push-to-talk)
- 風車（快速訪問）
- Navigation (導覽)

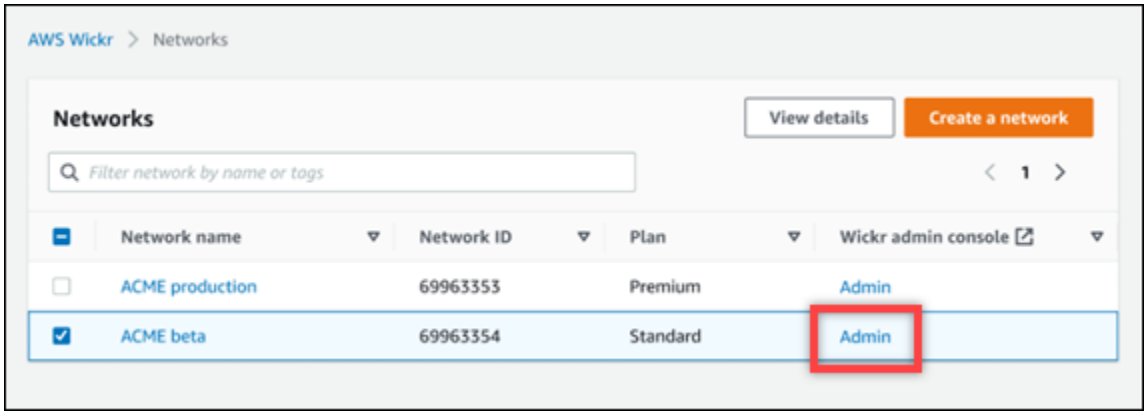
在威克爾網路儀表板中啟用 ATAK

AWS 威克爾支援許多使用安卓戰術突擊套件 (ATAK) 的機構。但是，到目前為止，使用 Wickr 的 ATAK 運營商不得不離開應用程序才能這樣做。為了幫助減少中斷和運營風險，Wickr 開發了一個插件，該插件可通過安全通信功能增強 ATAK。使用適用於 ATAK 的 Wickr 外掛程式，使用者可以在 ATAK 應用程式內傳送訊息、協作和傳輸 Wickr 上的檔案。這消除了中斷和 ATAK 聊天功能配置的複雜性。

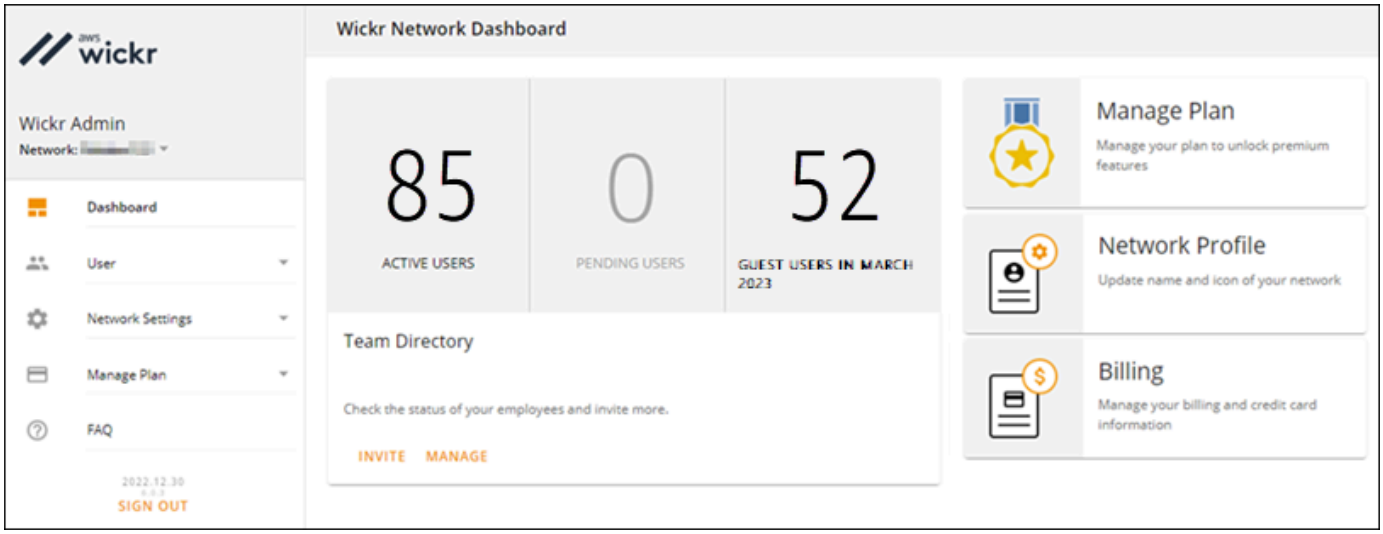
在威克爾網路儀表板中啟用 ATAK

完成下列程序，以在 Wickr 網路儀表板中啟用 ATAK。

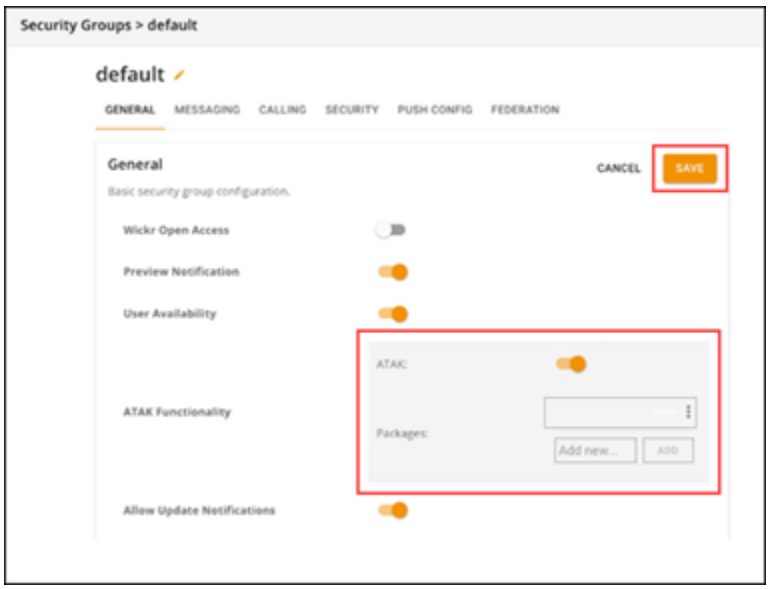
1. 打開AWS Management Console威克爾在 https://console.aws.amazon.com/wickr/。
2. 在 [網路] 頁面上，選擇 [管理員] 連結，瀏覽至該網路的 Wickr 管理控制台。



系統會將您重新導向至特定網路的 Wickr 管理控制台。



3. 在 Wickr 管理控制台的功能窗格中，選擇 [網路設定]，然後選擇 [安全性群組]。
4. 選擇您要啟用 ATAK 之所需安全性群組旁的 [詳細資料]。
5. 在 General (一般) 索引標籤上，選擇 Edit (編輯)。
6. 在 [ATAK 功能] 區段中：
   a. 在「封裝」文字方塊中輸入套件名稱。您可以根據使用者將安裝和使用的 ATAK 版本，輸入下列其中一個值：
      - `com.atakmap.app.civ`— 如果您的 Wickr 最終用戶打算在其 Android 設備上安裝並使用 ATAK 應用程序的民用版本，請在「包」文本框中輸入此值。
      - `com.atakmap.app.mil`— 如果您的 Wickr 最終用戶打算在其 Android 設備上安裝並使用軍事版本的 ATAK 應用程序，請在「包」文本框中輸入此值。
   b. 將 ATAK 切換向右滑動以開啟此功能。
   c. 選擇儲存。



ATAK 現在已為選取的 Wickr 網路和選取的安全性群組啟用。您應該要求您啟用 ATAK 功能的安全性群組中的 Android 使用者，以安裝 ATAK 的 Wickr 外掛程式。如需詳細資訊，請參閱安裝並配對 Wickr ATAK 外掛程式。

關於 ATAK 的其他資訊

如需 ATAK 適用之 Wickr 外掛程式的詳細資訊，請參閱下列內容：

- 威克亞塔克插件概述
- 其他威克 ATAK 插件信息

安裝並配對 ATAK 的威克爾插件

Android 團隊意識工具包（ATAK）是美國軍事，州和政府機構使用的 Android 解決方案，這些機構需要情境感知功能才能進行任務計劃，執行和事件響應。ATAK 有一個插件架構，允許開發人員添加功能。它使用戶能夠使用 GPS 和地理空間地圖數據進行導航，並覆蓋了對正在進行的事件的實時情境感知。在本文檔中，我們將向您展示如何在 Android 設備上安裝 ATAK 的 Wickr 插件並將其與 Wickr 客戶端配對。這使您可以在 Wickr 上發送消息和協作，而無需退出 ATAK 應用程序。

安裝 ATAK 的威克插件

完成下列程序，即可在安卓裝置上安裝 ATAK 的 Wickr 外掛程式。

1. 轉到谷歌播放商店，並安裝威克為 ATAK 插件。
2. 在您的安卓設備上打開 ATAK 應用程序。
3. 在 ATAK 應用程式中，選擇畫面右上角的功能表圖示 ()，然後選擇外掛程式。
4. 選擇匯入。
5. 在 「選擇導入類型」彈出窗口中，選擇「本地 SD」，然後導航到您為 ATAK .apk 文件保存 Wickr 插件的位置。
6. 選擇插件文件，然後按照提示進行安裝。

> **Note**
>
> 如果系統要求您傳送外掛程式檔案進行掃描，請選擇「否」。

7. ATAK 應用程式會詢問您是否要載入外掛程式。選擇 確定。

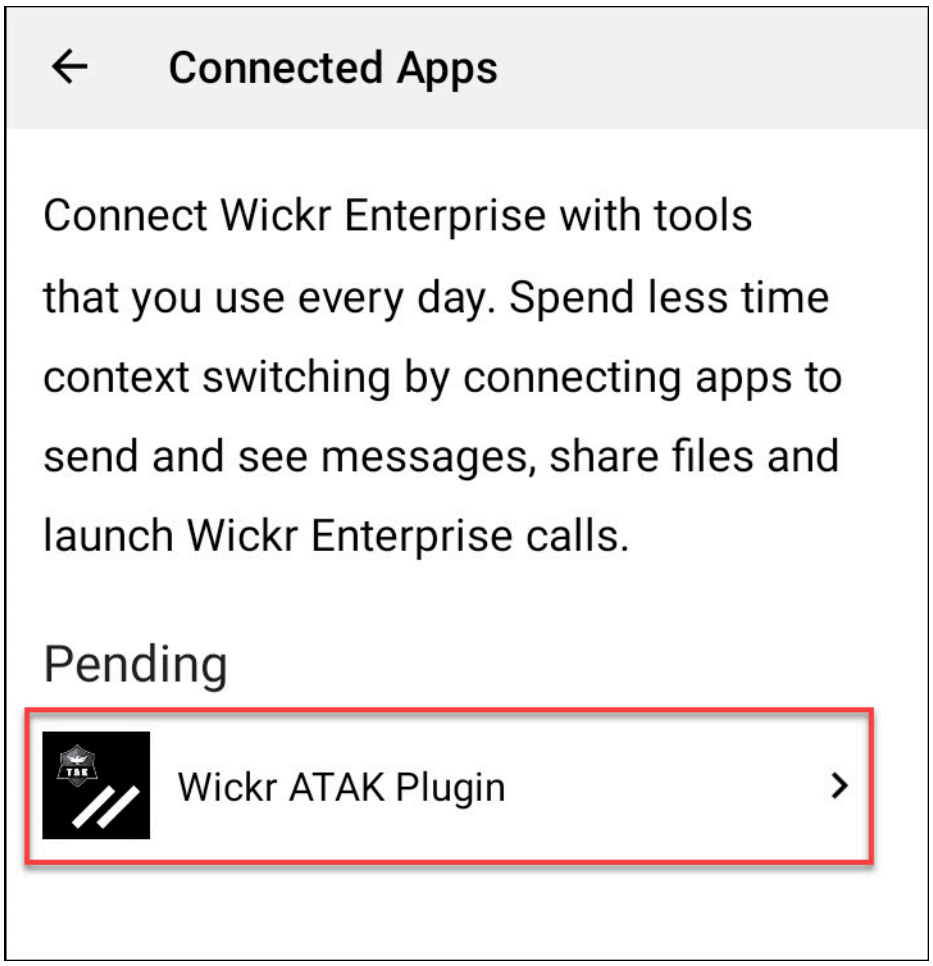
ATAK 的 Wickr 插件現在已安裝。繼續閱讀以下「將 ATAK 與 Wickr 配對」部分，以完成此過程。

將 ATAK 與威克爾配對

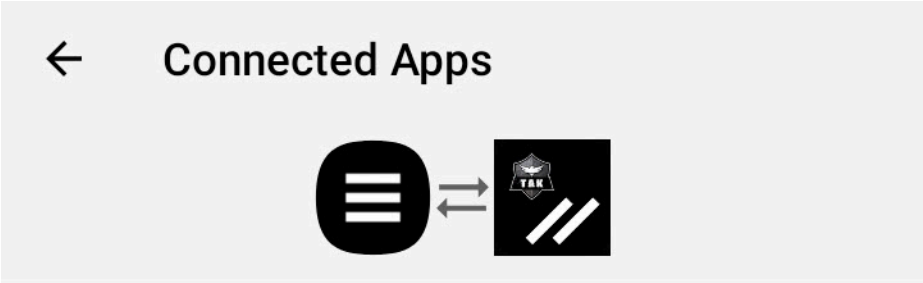
在您成功安裝 ATAK 的 Wickr 外掛程式之後，請完成下列程序，以便將 ATAK 應用程式與 Wickr 配對。

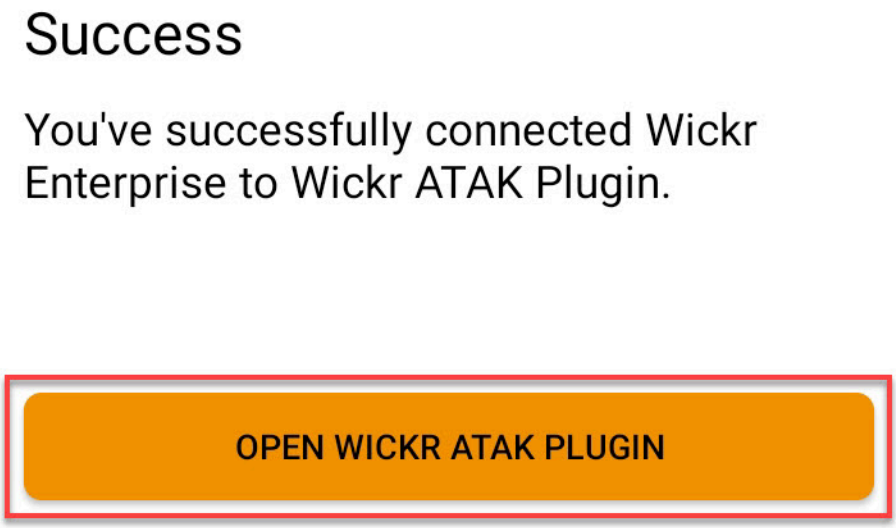
1. 在 ATAK 應用程式中，選擇畫面右上角的功能表圖示 ()，然後選擇 Wickr 外掛程式。
2. 選擇配對柳條。

   此時會出現通知提示，要求您檢閱 ATAK 之 Wickr 外掛程式的權限。如果沒有出現通知提示，請打開 Wickr 客戶端，然後轉到 「設置」，然後轉到「已連接的應用程序」。您應該在屏幕的「待處理」部分下看到該插件。



3. 選擇「核准」以配對。
4. 選擇開啟 Wickr ATAK 外掛程式按鈕返回 ATAK 應用程式。



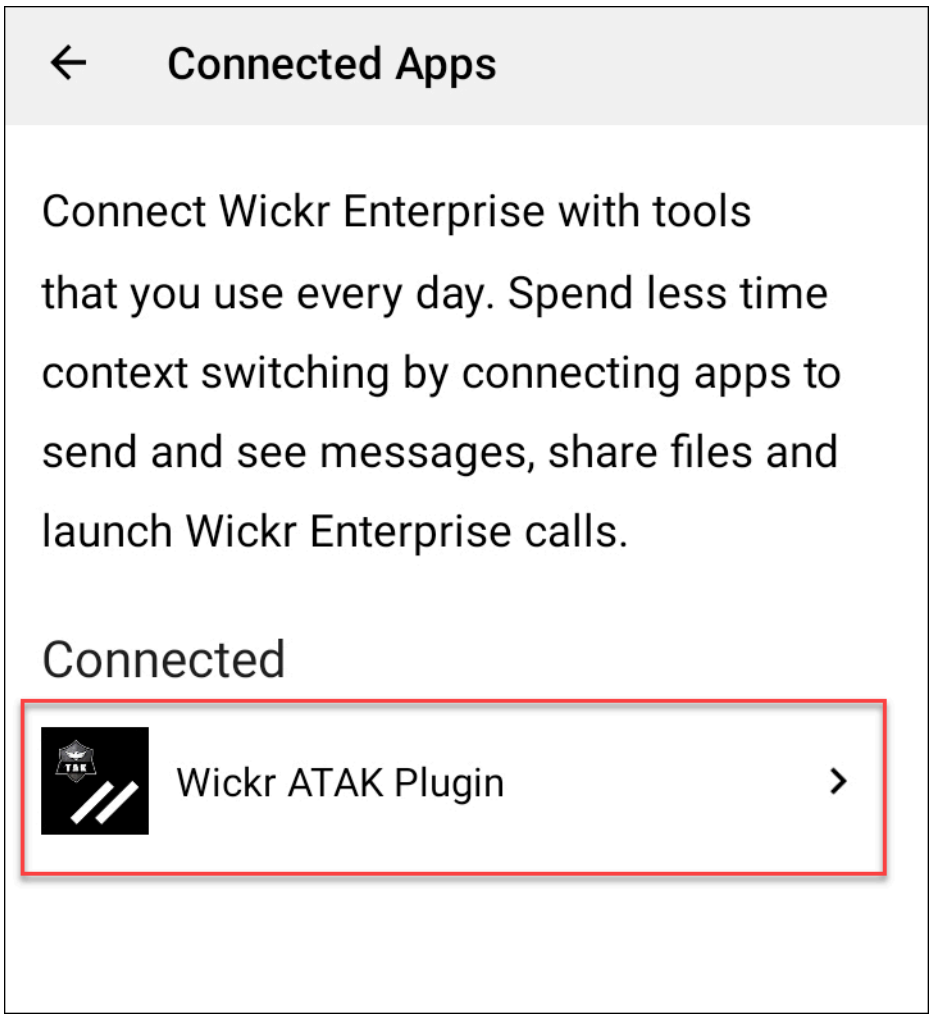


您現在已成功配對 ATAK 外掛程式和 Wickr，並且可以使用該外掛程式傳送訊息並使用 Wickr 進行協作，而無需結束 ATAK 應用程式。

取消 ATAK 與威克爾的配對

請完成下列程序，以取消 ATAK 外掛程式與 Wickr 的配對。

1. 在原生應用程式中，選擇 [設定]，然後選擇 [連線的應用程式]
2. 在「已連接的應用程式」畫面上，選擇 Wickr ATAK 外掛程式。



3. 在 Wickr ATAK 外掛程式畫面上，選擇畫面底部的「移除」。

   確認畫面會顯示您不再使用 API。您現在已成功取消配對 ATAK 外掛程式。

撥打及接聽電話

您可以在 ATAK 的 Wickr 插件中撥打和接聽電話。

完成以下程序以撥打和接聽電話。

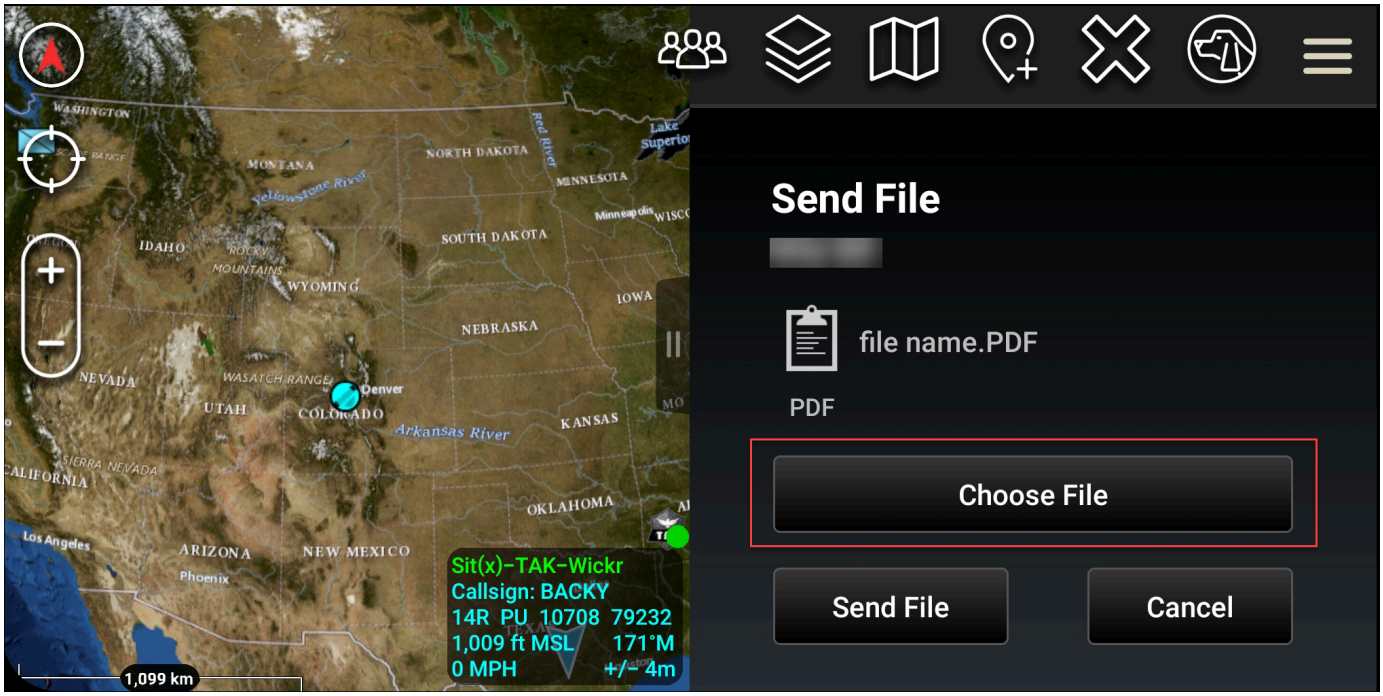
1. 開啟聊天視窗。
2. 在 [地圖] 檢視中，選擇您要呼叫之使用者的圖示。
3. 選擇屏幕右上角的電話圖標。
4. 連接後，您可以返回 ATAK 插件視圖並接聽電話。

傳送檔案

您可以在 ATAK 的 Wickr 插件中發送文件。

請完成下列程序以傳送檔案。

1. 開啟聊天視窗。
2. 在 [地圖] 檢視中，搜尋您要傳送檔案的使用者。
3. 當您找到要傳送檔案的使用者時，請選取他們的名稱。
4. 在「傳送檔案」畫面上，選取「選擇檔案」，然後瀏覽至您要傳送的檔案。



5. 在瀏覽器視窗中，選擇所需的檔案。
6. 在「傳送檔案」畫面上，選擇「傳送檔案」。

   下載圖示隨即顯示，表示正在下載您選取的檔案。

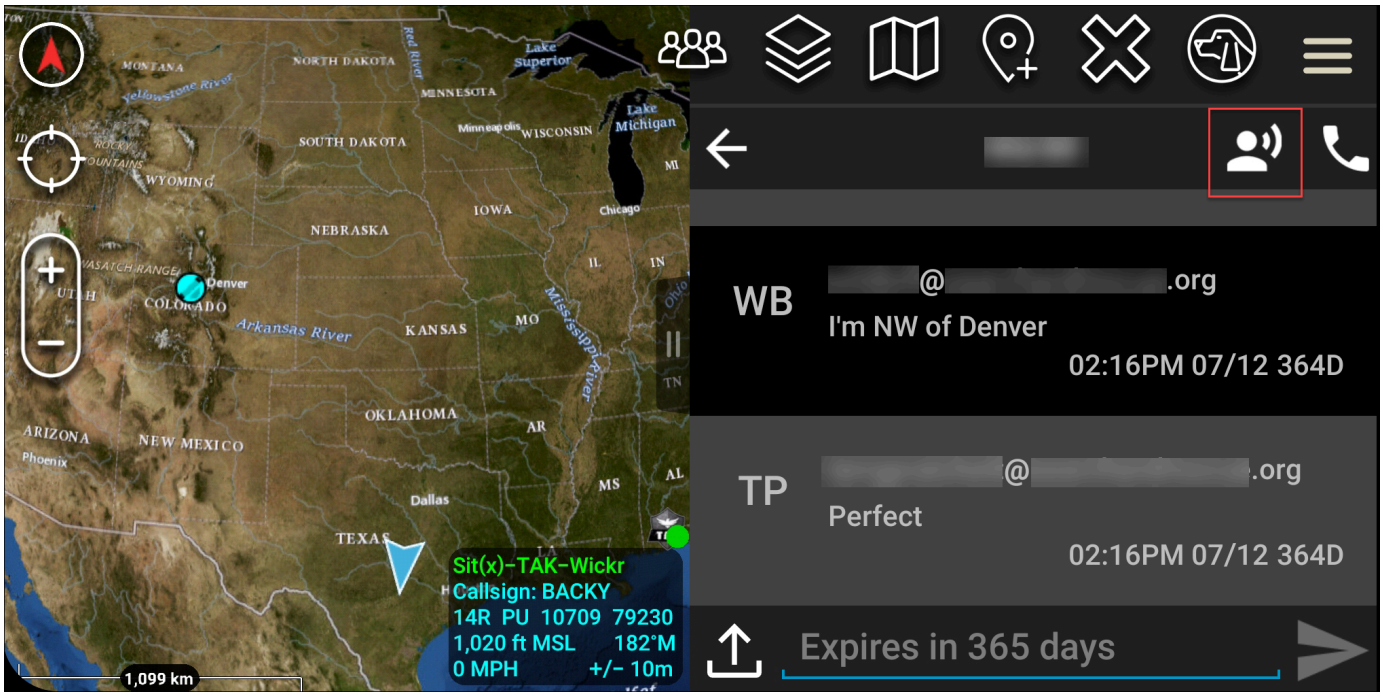
傳送安全語音訊息 (Push-to-talk)

您可以在 ATAK 的 Wickr 外掛程式中傳送安全語音訊息 (Push-to-talk)。

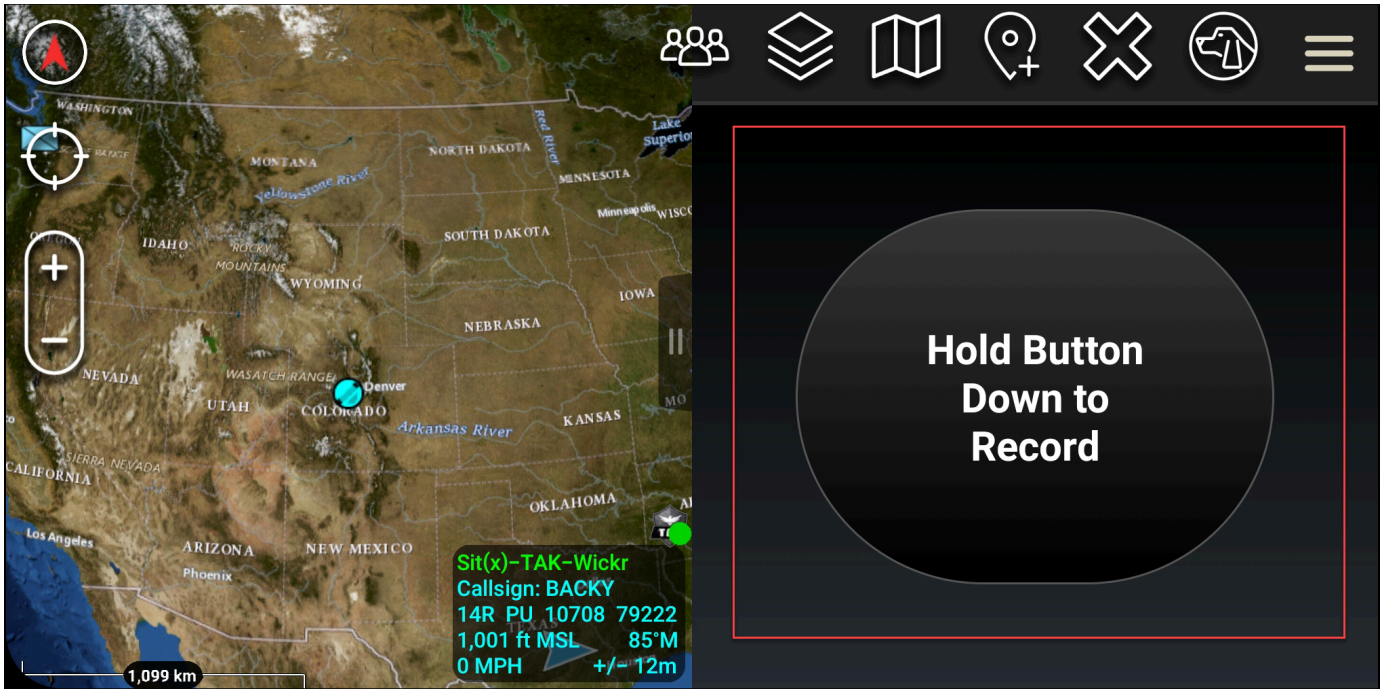
請完成下列程序，以傳送安全的語音訊息。

1. 開啟聊天視窗。

2. 選擇屏幕頂部的「按鍵通話」圖標，該圖標由一個人說話的圖標表示。



3. 選擇並按住按住按鈕下來記錄按鈕。



4. 記錄您的消息。

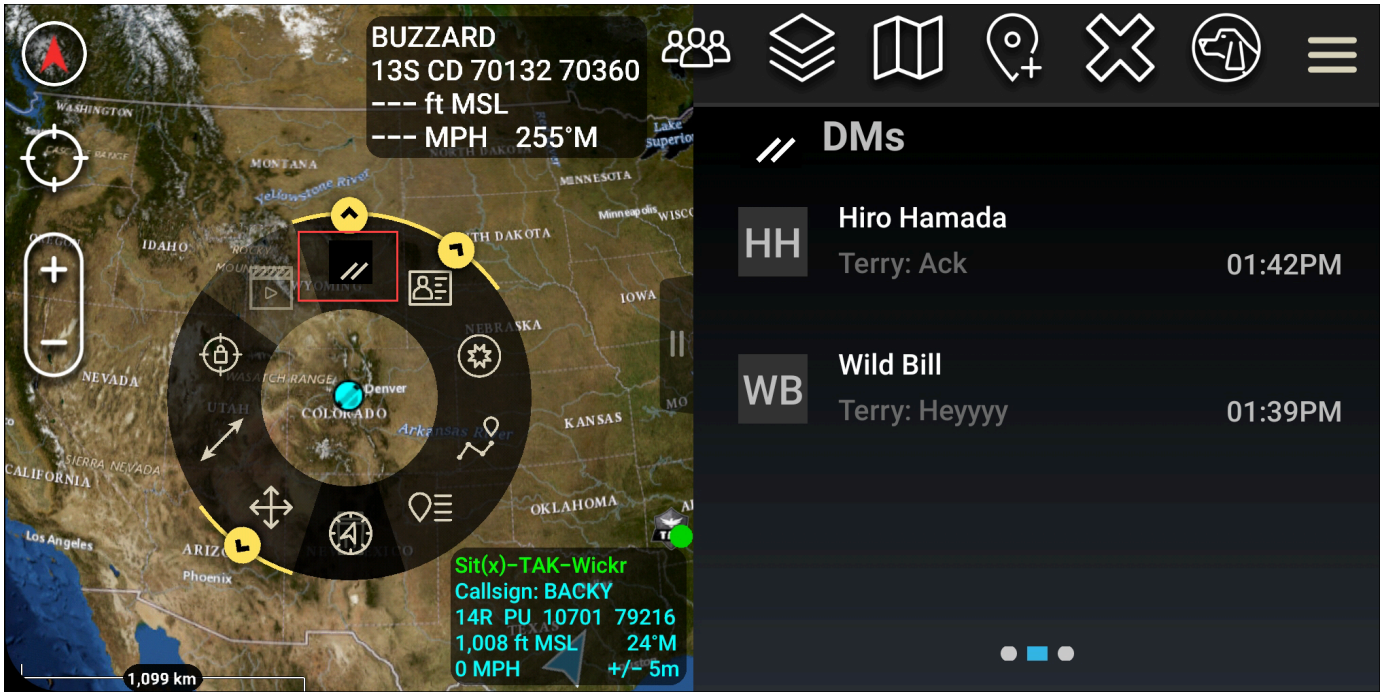
5. 錄製訊息後，放開按鈕即可傳送。

風車（快速訪問）

風車或快速訪問功能用於對 one-one-one 話或直接消息。

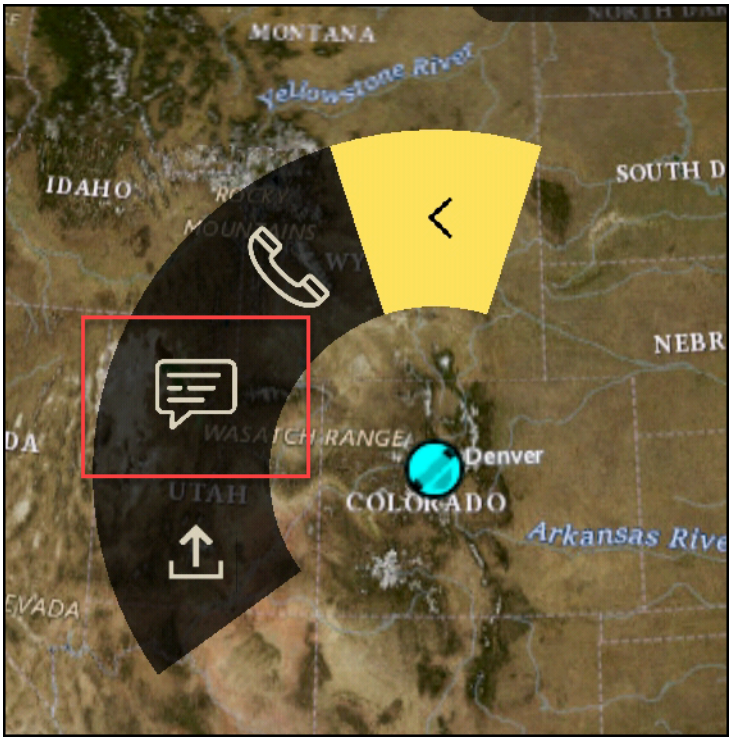
完成下列程序以使用風車。

1. 同時打開 ATAK 地圖的分屏視圖和 ATAK 插件的 Wickr。地圖會在地圖畫面上顯示您的隊友或資產。
2. 選擇使用者圖示以開啟風車。
3. 選擇 Wickr 圖示以檢視所選使用者的可用選項。

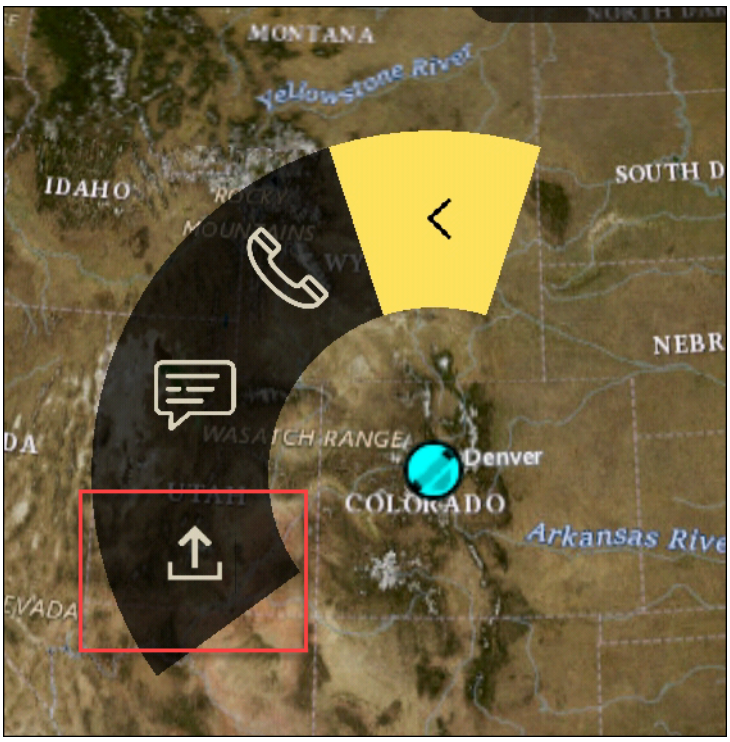


4. 在風車上，選擇下列其中一個圖示：
   - 電話：選擇撥打電話。

- 訊息：選擇聊天。



- 檔案傳送：選擇傳送檔案。



Navigation (導覽)

插件用戶界面包含三個插件視圖，這些視圖由屏幕右下角的藍色和白色形狀表示。向左和向右滑動以在檢視之間導覽。

- 連絡人檢視：建立直接訊息群組或會議室交談。
- DM 檢視：建立 one-to-one 交談。聊天功能與 Wickr 本機應用程序中的工作原理相同。此功能可讓您保留在 [地圖] 檢視中，並與外掛程式上的其他人通訊。
- 會議室視圖：本機應用程序中的現有會議室移植過來。在插件中完成的任何操作都會反映在 Wickr 本機應用程序中。

> **Note**
>
> 某些功能（例如刪除聊天室）只能在本機應用程序中和親自執行，以防止用戶意外修改以及現場設備造成的干擾。

允許的連接埠和網域清單

允許列出以下連接埠和網域，以確保 Wickr 正常運作：

連接埠

- TCP 連接埠 443 (用於訊息和附件)
- UDP 連接埠 (用於呼叫)

區域網域

- 歐洲（法蘭克福）：信息通知歐洲中部
- 美國東部 (維吉尼亞北部) gw-pro-prod:.
- 歐洲（倫敦）：發送信息歐洲西部 2. Amazonaws.com
- 亞太區域 (雪梨)：阿比利時訊息發送給我們的東南部地區 2.amazonaws.com
- 加拿大（中部）：阿馬遜網站
- AWS GovCloud （美國西部）：API 發送消息。 us-gov-west-1. 亞馬遜

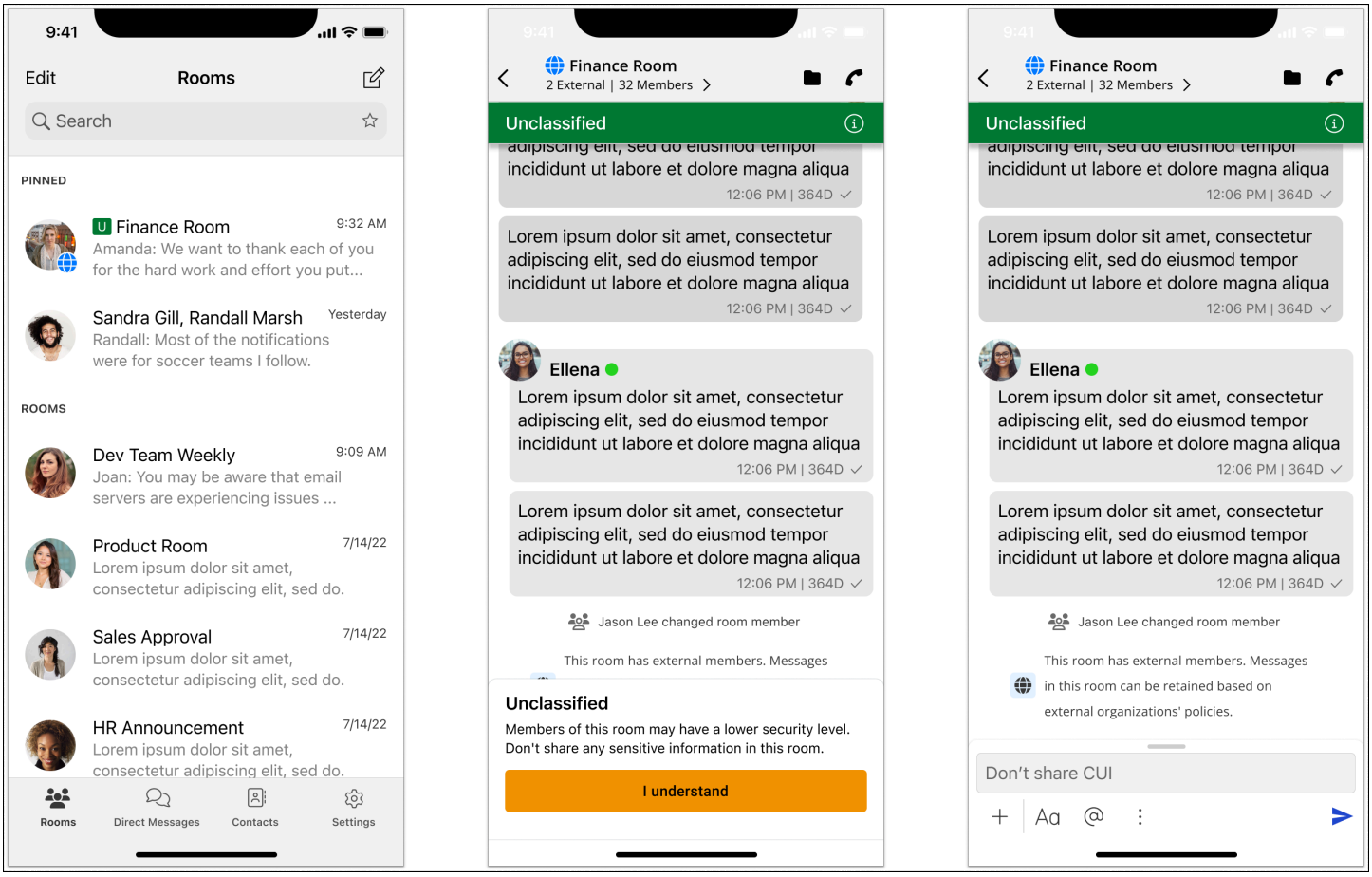
註冊和驗證電子郵件由 donotreply@wickr.email 發送。

如果您需要允許列出所有可能的呼叫服務器 IP 地址，則需要下載可能的 CIDR 的 AllowlistWickr.txt 並定期對其進行檢查，因為它可能會更改。

GovCloud 跨界分類與聯合

AWS Wickr 提供為使用者量身打造的 GovCloud 用 WickrGov 戶端。 GovCloud 同盟允許 GovCloud 使用者與商業使用者之間的通訊。跨界限分類功能可讓使用者變更對話的使 GovCloud 用者介面。作為 GovCloud 用戶，您必須遵守有關政府定義分類的嚴格準則。當 GovCloud 使用者與商業使用者 (企業、AWS Wickr、來賓使用者) 進行對話時，他們會看到顯示下列未分類的警告：

- 房間清單中的 U 標籤
- 訊息畫面上未分類的確認
- 在對話頂部的未分類橫幅



> **Note**
>
> 只有當使用者正在與外部 GovCloud 使用者交談或聊天室的一部分時，才會顯示這些警告。如果外部使用者離開對話，它們將會消失。使用者之間的對話中不會顯示任何警 GovCloud 告。

管理 AWS 中的使用者

在 Wickr 的「使用者」區段中，您可以檢視目前的 Wickr 使用者和機器人，並修改其 AWS Management Console 詳細資訊。

主題

團隊目錄

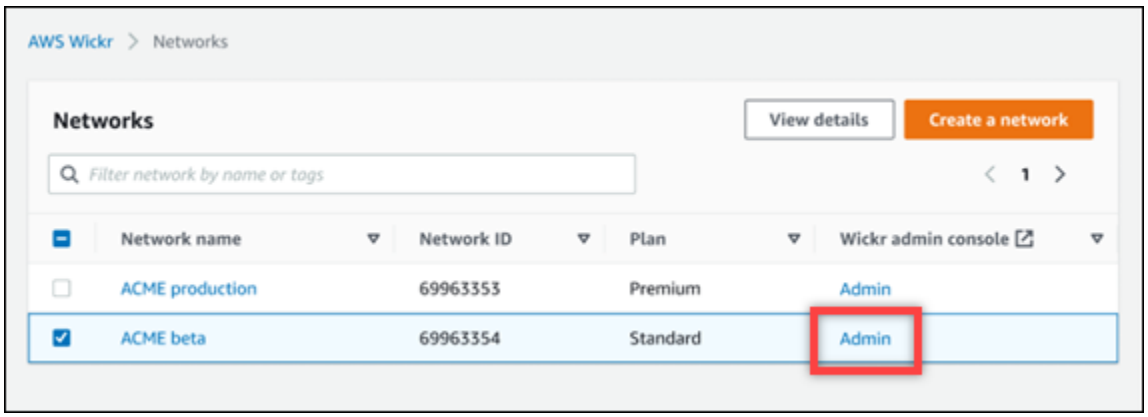
您可以在 Wickr 的「使用者」區段中檢視目前的 Wickr 使用者並修改其詳細資訊。 AWS Management Console

主題

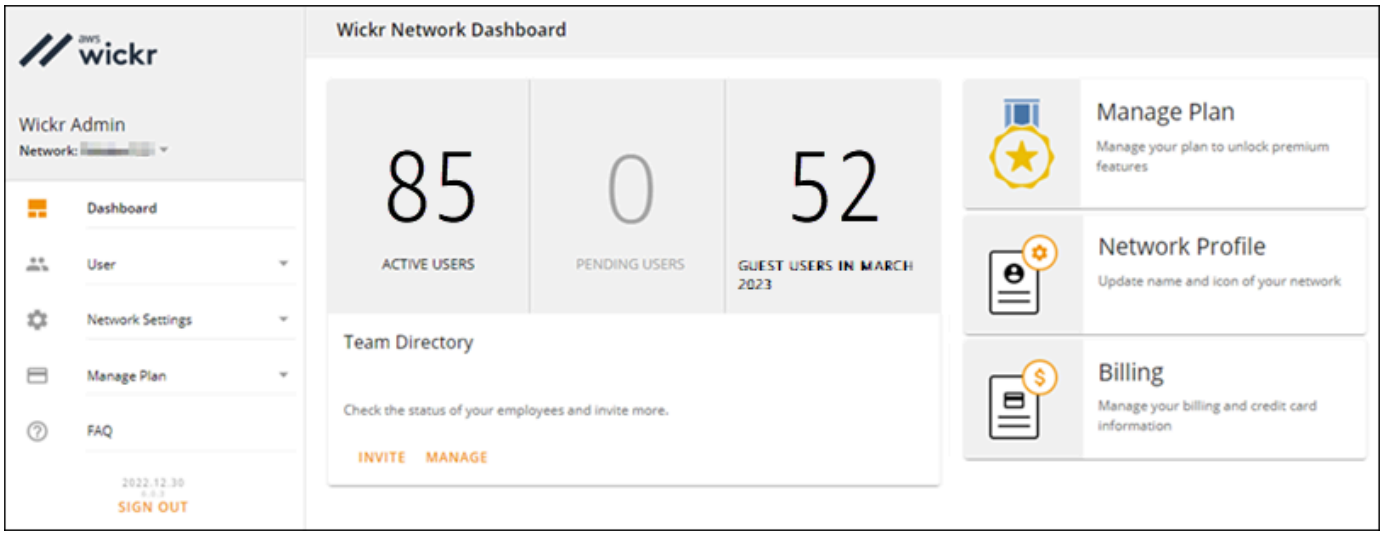
檢視使用者

請完成下列程序以檢視註冊到您的 Wickr 網路的使用者。

1. 打開 AWS Management Console 威克爾在 https://console.aws.amazon.com/wickr/。
2. 在 [網路] 頁面上，選擇 [管理員] 連結，瀏覽至該網路的 Wickr 管理控制台。



系統會將您重新導向至特定網路的 Wickr 管理控制台。



3. 在 Wickr 管理控制台的導覽窗格中，選擇 [使用者]，然後選擇 [團隊目錄]。

   「團隊目錄」頁面會顯示在 Wickr 網路中註冊的使用者，包括他們的姓名、電子郵件地址、指派的安全性群組和目前狀態。對於當前用戶，您可以查看他們的設備，編輯其詳細信息，暫停，刪除並將其切換到另一個 Wickr 網絡。

建立使用者

請完成下列程序來建立使用者。

1. 打開 AWS Management Console 威克爾在 https://console.aws.amazon.com/wickr/。
2. 在 [網路] 頁面上，選擇 [管理員] 連結，瀏覽至該網路的 Wickr 管理控制台。

   系統會將您重新導向至特定網路的 Wickr 管理控制台。
3. 在 Wickr 管理控制台的導覽窗格中，選擇 [使用者]，然後選擇 [團隊目錄]。

4. 選擇 [建立新使用者]。
5. 在顯示的表單中，輸入使用者的名字、姓氏、國家代碼、電話號碼和電子郵件地址。電子郵件地址是唯一必填的欄位。請務必為使用者選擇適當的安全性群組。Wickr 會傳送邀請電子郵件到您為使用者指定的地址。
6. 選擇建立。

   電子郵件會傳送給使用者。電子郵件提供 Wickr 用戶端應用程式的下載連結，以及註冊 Wickr 的連結。當用戶使用電子郵件中的鏈接註冊 Wickr 時，他們在 Wickr 團隊目錄中的狀態將從「待處理」更改為「活動」。

編輯使用者

請完成下列程序來編輯使用者。

1. 打開 AWS Management Console 威克爾在 https://console.aws.amazon.com/wickr/。
2. 在 [網路] 頁面上，選擇 [管理員] 連結，瀏覽至該網路的 Wickr 管理控制台。

   系統會將您重新導向至特定網路的 Wickr 管理控制台。
3. 在 Wickr 管理控制台的導覽窗格中，選擇 [使用者]，然後選擇 [團隊目錄]。
4. 選擇您要刪除之使用者名稱旁邊的垂直省略符號圖示。
5. 您可以選擇以下其中一個選項：

   - 裝置 — 檢視使用者使用 Wickr 用戶端設定的裝置。
   - 編輯 — 編輯使用者詳細資訊，例如其姓名、國家/地區代碼、電話號碼 (選用) 和指派的安全性群組。
   - 暫停 — 暫停使用者，以便他們無法在 Wickr 用戶端中登入您的 Wickr 網路。當您暫停目前在用戶端中登入 Wickr 網路的使用者時，該使用者會自動登出。
   - 刪除 — 從您的 Wickr 網路中刪除使用者。

刪除使用者

請完成下列程序來刪除使用者。

1. 打開 AWS Management Console 威克爾在 https://console.aws.amazon.com/wickr/。
2. 在 [網路] 頁面上，選擇 [管理員] 連結，瀏覽至該網路的 Wickr 管理控制台。

系統會將您重新導向至特定網路的 Wickr 管理控制台。

3. 在 Wickr 管理控制台的導覽窗格中，選擇 [使用者]，然後選擇 [團隊目錄]。
4. 選擇您要刪除之使用者名稱旁邊的垂直省略符號圖示。
5. 選擇刪除以刪除使用者。

   當您刪除使用者時，該使用者將無法再在 Wickr 用戶端中登入您的 Wickr 網路。

大量刪除使用者

您可以在 Wickr 管理控制台的 Wickr 管理控制台的「用戶」部分批量刪除和批量暫停 Wickr 網絡用戶。

> **Note**
>
> 只有在未啟用 SSO 時，才會套用大量刪除使用者的選項。

若要使用 CSV 範本大量刪除 Wickr 網路使用者，請完成以下程序。

1. 打開 AWS Management Console 威克爾在 https://console.aws.amazon.com/wickr/。
2. 在 Wickr 管理控制台的導覽窗格中，選擇 [使用者]，然後選擇 [團隊目錄]。

   「團隊目錄」頁面會顯示在 Wickr 網路中註冊的使用者。
3. 在 [小組目錄] 頁面上，選擇 [管理使用者]。
4. 在「管理使用者」快顯視窗中，選擇「刪除用戶」。
5. 下載範例 CSV 範本。若要下載範例範本，請選擇「下載範本」。
6. 新增您要從網路大量刪除的使用者電子郵件，以完成範本。
7. 上傳完成的 CSV 範本。您可以將文件拖放到上傳框中，或選擇選擇文件。
8. 選中該複選框，我承認刪除用戶是不可逆的。
9. 選擇刪除使用者。

> **Note**
>
> 此動作會立即開始刪除使用者，可能需要幾分鐘的時間。刪除的使用者將無法再在 Wickr 用戶端中登入您的 Wickr 網路。

若要透過下載團隊目錄的 CSV 來批量刪除 Wickr 網路使用者，請完成以下程序。

1. 打開 AWS Management Console 威克爾在 https://console.aws.amazon.com/wickr/。
2. 在 Wickr 管理控制台的導覽窗格中，選擇 [使用者]，然後選擇 [團隊目錄]。

   「團隊目錄」頁面會顯示在 Wickr 網路中註冊的使用者。
3. 選取「團隊目錄」頁面右上角的「下載 CSV」圖示。
4. 下載團隊目錄 CSV 範本之後，請移除不需要刪除的使用者列。
5. 在 [小組目錄] 頁面上，選擇 [管理使用者]。
6. 在「管理使用者」快顯視窗中，選擇「刪除用戶」。
7. 上傳團隊目錄 CSV 範本。您可以將文件拖放到上傳框中，或選擇選擇文件。
8. 選中該複選框，我承認刪除用戶是不可逆的。
9. 選擇刪除使用者。

> **Note**
>
> 此動作會立即開始刪除使用者，可能需要幾分鐘的時間。刪除的使用者將無法再在 Wickr 用戶端中登入您的 Wickr 網路。

大量暫停使用者

您可以在 Wickr 管理控制台的 Wickr 管理控制台的「用戶」部分批量暫停 Wickr 網絡用戶。

> **Note**
>
> 只有在未啟用 SSO 時，才會套用大量暫停使用者的選項。

若要大量停權您的 Wickr 網路使用者，請完成以下程序。

1. 打開 AWS Management Console 威克爾在 https://console.aws.amazon.com/wickr/。
2. 在 Wickr 管理控制台的導覽窗格中，選擇 [使用者]，然後選擇 [團隊目錄]。

   「團隊目錄」頁面會顯示在 Wickr 網路中註冊的使用者。
3. 在 [小組目錄] 頁面上，選擇 [管理使用者]。
4. 在「管理使用者」快顯視窗中，選擇「暫停使用者」

5. 下載範例 CSV 範本。若要下載範例範本，請選擇「下載範本」。
6. 新增您要從網路大量暫停的使用者電子郵件，以完成範本。
7. 上傳完成的 CSV 範本。您可以將文件拖放到上傳框中，或選擇選擇文件。
8. 上傳 CSV 檔案後，請選擇「停用使用者」。

> **Note**
>
> 此動作將立即開始暫停使用者，可能需要幾分鐘的時間。暫停的使用者無法在 Wickr 用戶端中登入您的 Wickr 網路。當您暫停目前在用戶端中登入 Wickr 網路的使用者時，該使用者會自動登出。

訪客使用者

Wickr 來賓使用者功能可讓個別來賓使用者登入 Wickr 用戶端，並與 Wickr 網路使用者合作。Wickr 管理員可以在 Wickr 管理控制台的「安全群組」頁面中啟用或停用其 Wickr 網路的訪客使用者。

啟用此功能後，受邀加入您的 Wickr 網路的訪客使用者可以與您的 Wickr 網路中的使用者互動。訪客使用者功能將收取費用。 AWS 帳戶 如需訪客使用者功能定價的詳細資訊，請參閱定價附加元件下的 Wickr 定價頁面。

主題

啟用或停用訪客使用者

完成下列程序以啟用或停用 Wickr 網路的訪客使用者。

1. 打開 AWS Management Console 威克爾在 https://console.aws.amazon.com/wickr/。
2. 在 [網路] 頁面上，選擇 [管理員] 連結，瀏覽至該網路的 Wickr 管理控制台。

   系統會將您重新導向至特定網路的 Wickr 管理控制台。

3. 在 Wickr 管理控制台的功能窗格中，選擇 [網路設定]，然後選擇 [安全性群組]。
4. 選擇特定安全性群組的 [詳細資料]。

> **Note**
>
> 您只能為個別安全性群組啟用來賓使用者。若要為 Wickr 網路中的所有安全性群組啟用來賓使用者，您必須為網路中的每個安全性群組啟用此功能。

5. 選擇安全性群組詳細資料頁面中的同盟索引標籤。
6. 在兩個位置可以使用允許訪客使用者的切換：
   - 本機同盟 — 對於美國東部 (維吉尼亞北部) 的網路，請選擇頁面之「本機同盟」區段旁的 「編輯」。
   - 全域聯合 — 對於其他區域中的所有其他網路，請選擇頁面之「全域聯盟」段落旁的 「編輯」。
7. 選取「允許訪客使用者啟用安全性群組的來賓使用者」，或取消選取以停用安全性群組。
8. 選擇 [儲存] 儲存變更，並使其對安全性群組有效。

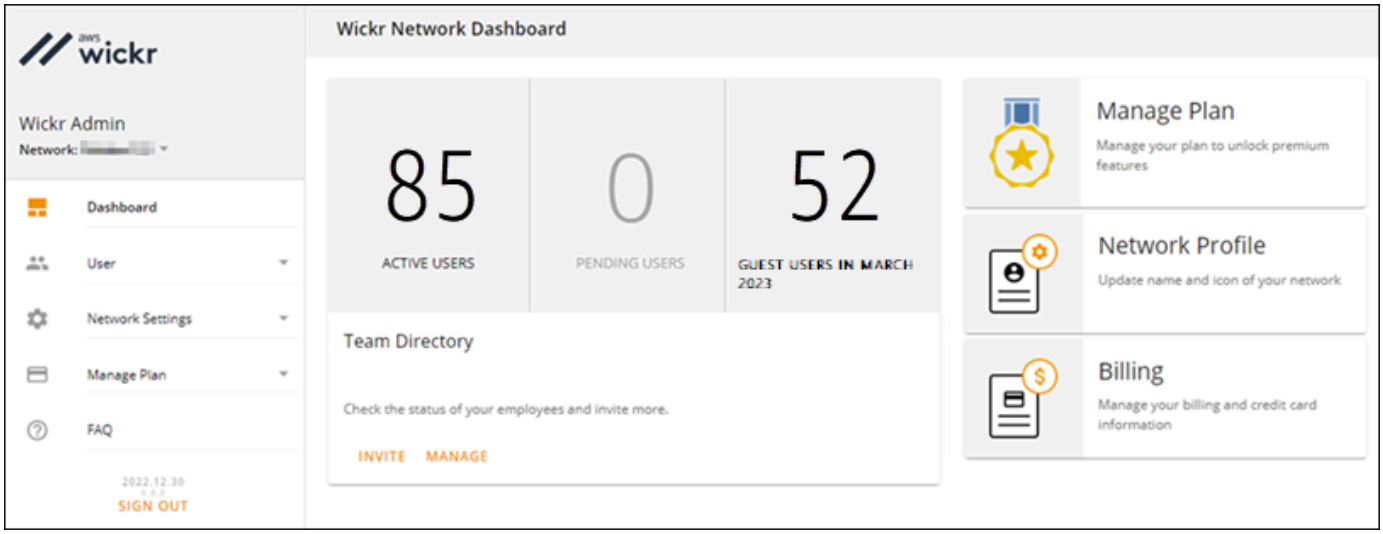
Wickr 網路中特定安全性群組中的註冊使用者現在可以與訪客使用者互動。如需詳細資訊，請參閱 Wickr 使用者指南中的來賓使用者。

檢視訪客使用者計數

請完成下列程序以檢視 Wickr 網路的來賓使用者計數。

1. 打開 AWS Management Console 威克爾在 https://console.aws.amazon.com/wickr/。
2. 在 [網路] 頁面上，選擇 [管理員] 連結，瀏覽至該網路的 Wickr 管理控制台。

系統會將您重新導向至特定網路的 Wickr 管理控制台。「儀表板」頁面會顯示 Wickr 網路中的訪客使用者計數，如下列範例所示。



檢視每月使用量

您可以檢視您的網路在帳單期間與之通訊的訪客使用者數量。若要檢視您的每月用量，請完成以下步驟。

1. 打開 AWS Management Console 威克爾在 https://console.aws.amazon.com/wickr/。
2. 在 [網路] 頁面上，選擇 [管理員] 連結，瀏覽至該網路的 Wickr 管理控制台。
3. 在 Wickr 管理控制台的導覽窗格中，選擇 [使用者]，然後選擇 [訪客使用者]。
4. 在「來賓使用者」頁面上，選擇「每月使用量」區段。

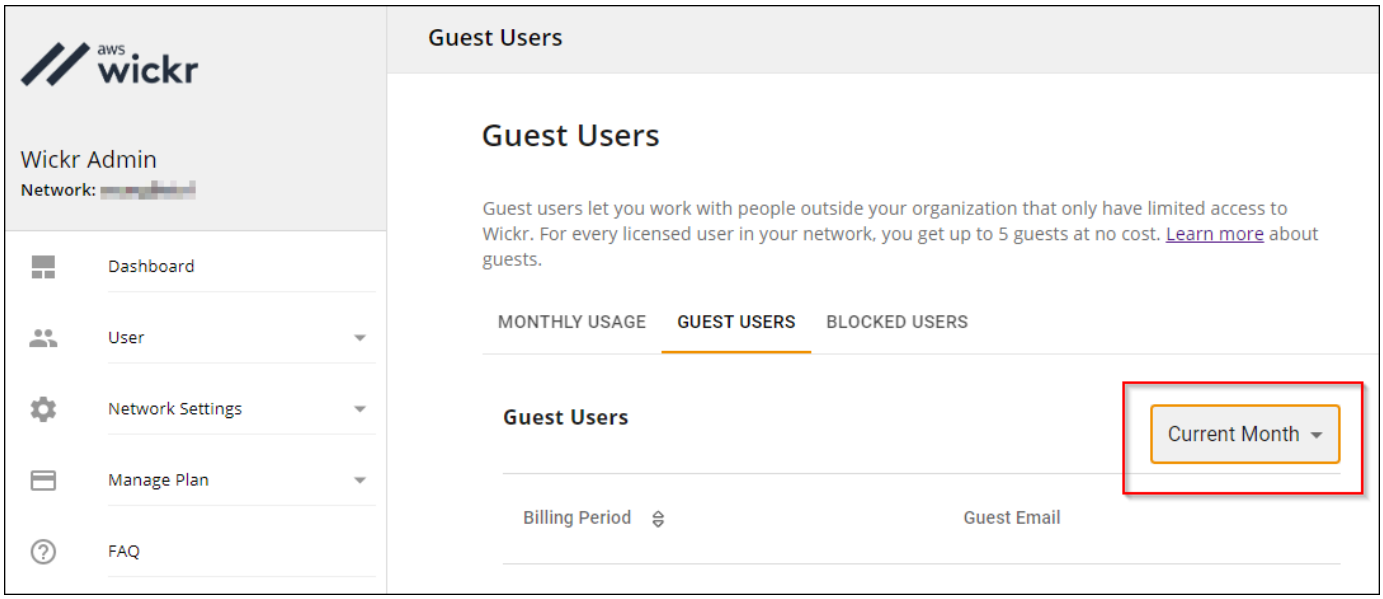
> **Note**
>
> 訪客帳單資料每 24 小時更新一次。

檢視訪客使用者

您可以檢視網路使用者在特定計費週期內與之通訊的訪客使用者清單。若要檢視您的訪客使用者，請完成以下步驟。

1. 打開 AWS Management Console 威克爾在 https://console.aws.amazon.com/wickr/。
2. 在 [網路] 頁面上，選擇 [管理員] 連結，瀏覽至該網路的 Wickr 管理控制台。
3. 在 Wickr 管理控制台的導覽窗格中，選擇 [使用者]，然後選擇 [訪客使用者]。
4. 在「來賓使用者」頁面上，選擇「來賓使用者」區段。

5. 若要檢視特定月份的來賓使用者，請從下拉式功能表中選取對應的月份。



封鎖訪客使用者

封鎖的使用者無法與您網路中的任何人通訊。

封鎖訪客使用者

1. 打開 AWS Management Console 威克爾在 https://console.aws.amazon.com/wickr/。
2. 在 [網路] 頁面上，選擇 [管理員] 連結，瀏覽至該網路的 Wickr 管理控制台。
3. 在 Wickr 管理控制台的導覽窗格中，選擇 [使用者]，然後選擇 [訪客使用者]。
4. 在「來賓使用者」頁面上，選擇「來賓使用者」區段。
5. 「來賓使用者」區段會顯示在您的 Wickr 網路中進行通訊的來賓使用者。
6. 在訪客用戶部分，找到您要阻止的訪客用戶的電子郵件。
7. 在訪客使用者名稱的右側，選取三個點，然後選擇 [封鎖]。
8. 選擇阻止在彈出窗口中。
9. 若要檢視 Wickr 網路中封鎖的使用者清單，請選擇「封鎖的使用者」區段。

解除封鎖訪客使用者

1. 打開 AWS Management Console 威克爾在 https://console.aws.amazon.com/wickr/。
2. 在 [網路] 頁面上，選擇 [管理員] 連結，瀏覽至該網路的 Wickr 管理控制台。

3. 在 Wickr 管理控制台的導覽窗格中，選擇 [使用者]，然後選擇 [訪客使用者]。
4. 在「來賓使用者」頁面上，選擇「封鎖的使用者」區段。
5. 「封鎖的使用者」區段會顯示在您的 Wickr 網路中封鎖的來賓使用者。
6. 在「封鎖的使用者」區段中，找到您要解除封鎖的訪客使用者的電子郵件。
7. 在訪客使用者名稱右側，選取三個點，然後選擇 [解除封鎖]。
8. 選擇取消阻止在彈出窗口中。

AWS 威克爾中的安全性

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。要了解適用於 AWS Wickr 的合規計劃，請參閱AWS 合規計劃的合規計劃AWS。
- 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。

本文件可協助您瞭解如何在使用 Wickr 時套用共同的責任模型。下列主題說明如何設定 Wickr 以符合您的安全性和合規性目標。您還將學習如何使用其他 AWS 服務來幫助您監控和保護 Wickr 資源。

主題

AWS 威克爾中的資料保護

AWS 共同責任模型適用於 AWS Wickr 中的資料保護。如此模型所述， AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

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

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 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。
- 如果透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您 AWS 服務 使用控制台，API 或 AWS SDK 與 Wickr 或其他人 AWS CLI合作時。您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

AWS 威克爾的身分和存取管理

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員控制哪些人可以驗證 (登入) 和授權 (具有權限) 以使用 Wickr 資源。IAM 是您可以使用的 AWS 服務 ，無需額外付費。

主題

物件

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

服務使用者 — 如果您使用 Wickr 服務執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 Wickr 功能來完成工作時，您可能需要其他權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法存取 Wickr 中的功能，請參閱AWS Wickr 身分和存取的疑難排解。

服務管理員 — 如果您負責公司的 Wickr 資源，您可能擁有 Wickr 的完整存取權。決定您的服務使用者應該存取哪些 Wickr 功能和資源是您的工作。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要深入瞭解貴公司如何將 IAM 與 Wickr 搭配使用，請參閱AWS 威克如何與 IAM 搭配使用。

IAM 管理員 — 如果您是 IAM 管理員，您可能想要瞭解如何撰寫政策來管理 Wickr 存取權的詳細資訊。若要檢視可在 IAM 中使用的 Wickr 身分型政策範例，請參閱。AWS Wickr 的基於身份的政策範例

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM 身分中心) 使用者、貴公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料都是聯合身分識別的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使 AWS 用同盟存取時，您會間接擔任角色。

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AWS 登入 使用者指南中的如何登入您 AWS 帳戶的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的簽署 AWS API 請求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。如需更多資訊，請參閱 AWS IAM Identity Center 使用者指南中的多重要素驗證和 IAM 使用者指南中的在 AWS中使用多重要素驗證 (MFA)。

AWS 帳戶 根使用者

建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務 和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱 IAM 使用者指南中的需要根使用者憑證的任務。

聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時認證 AWS 服務 來存取。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需 IAM Identity Center 的詳細資訊，請參閱 AWS IAM Identity Center 使用者指南中的什麼是 IAM Identity Center？。

IAM 使用者和群組

IAM 使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

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

IAM 角色

IAM 角色是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI 或 AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法詳細資訊，請參閱 IAM 使用者指南中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 — 如需向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 IAM 使用者指南中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，

則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。

- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權：您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的主體) 存取您帳戶的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 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）。若要了解跨帳戶存取角色和以資源為基礎的政策之間的差異，請參閱 IAM 使用者指南中的 IAM 中的跨帳戶資源存取。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需詳細資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務服務。
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請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該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需詳細資訊，請參閱 IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

如需了解是否要使用 IAM 角色或 IAM 使用者，請參閱 IAM 使用者指南中的建立 IAM 角色 (而非使用者) 的時機。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 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。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的詳細資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

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

預設情況下，使用者和角色沒有許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或 AWS API 取得角色資訊。

身分型政策

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

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。如需了解如何在受管政策及內嵌政策間選擇，請參閱 IAM 使用者指南中的在受管政策和內嵌政策間選擇。

資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。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。您無法在以資源為基礎的政策中使用 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

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

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

其他政策類型

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

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可界限的詳細資訊，請參閱 IAM 使用者指南中的 IAM 實體許可界限。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需詳細資訊，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

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

AWS 適用於 AWS 威克的受管政策

若要新增使用者、群組和角色的權限，使用 AWS 受管理的原則比自己撰寫原則更容易。建立 IAM 客戶受管政策需要時間和專業知識，而受管政策可為您的團隊提供其所需的許可。若要快速開始使用，您可以使用我們的 AWS 受管政策。這些政策涵蓋常見的使用案例，並可在您的 AWS 帳戶中使用。如需 AWS 受管政策的詳細資訊，請參閱 IAM 使用者指南中的AWS 受管政策。

AWS 服務 維護和更新 AWS 受管理的策略。您無法變更 AWS 受管理原則中的權限。服務偶爾會在 AWS 受管政策中新增其他許可以支援新功能。此類型的更新會影響已連接政策的所有身分識別 (使用者、群組和角色)。當新功能啟動或新操作可用時，服務很可能會更新 AWS 受管政策。服務不會從 AWS 受管理的政策移除權限，因此政策更新不會破壞您現有的權限。

AWS 受管理的策略： AWSWickrFullAccess

您可將 `AWSWickrFullAccess` 政策連接到 IAM 身分。此政策授予 Wickr 服務的完整管理許可，包括在. AWS Management Console AWS Management Console如需將政策附加至身分的詳細資訊，請參閱AWS Identity and Access Management 使用指南中的新增和移除 IAM 身分許可。

許可詳細資訊

此政策包含以下許可。

- `wickr`— 授予 Wickr 服務的完整管理許可。

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

Wickr 對 AWS 受管理政策的更新

檢視 Wickr AWS 受管政策更新的詳細資料，因為此服務開始追蹤這些變更。如需有關此頁面變更的自動警示，請訂閱 Wickr 文件歷史記錄頁面上的 RSS 摘要。

變更	描述	日期
AWSWickrFullAccess – 新政策	Wickr 新增了一項新政策，授與 Wickr 服務的完整管理權限，包括中的 Wickr 管理員主控台。 AWS Management Console	2022 年 11 月 28 日
威克爾開始跟踪更改	Wickr 開始追蹤其 AWS 受管理政策的變更。	2022 年 11 月 28 日

AWS 威克如何與 IAM 搭配使用

在您使用 IAM 管理 Wickr 的存取權限之前，請先了解哪些 IAM 功能可與 Wickr 搭配使用。

您可以搭配 AWS Wickr 使用的 IAM 功能

IAM 功能	威克爾支持
身分型政策	是
資源型政策	否
政策動作	是
政策資源	否
政策條件索引鍵	否
ACL	否
ABAC(政策中的標籤)	否
臨時憑證	否
主體許可	否
服務角色	否
服務連結角色	否

若要深入瞭解 Wickr 和其他 AWS 服務如何搭配大多數 IAM 功能使用，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS 服務。

Wickr 的基於身份識別的政策

支援身分型政策	是

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

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

Wickr 的以身分識別為基礎的政策範例

若要檢視 Wickr 身分型原則的範例，請參閱。AWS Wickr 的基於身份的政策範例

威克爾內基於資源的政策

支援以資源基礎的政策	否

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

如需啟用跨帳戶存取權，您可以指定在其他帳戶內的所有帳戶或 IAM 實體，作為資源型政策的主體。新增跨帳戶主體至資源型政策，只是建立信任關係的一半。當主體和資源位於不同時 AWS 帳戶，受信任帳戶中的 IAM 管理員也必須授與主體實體 (使用者或角色) 權限，才能存取資源。其透過將身分型政策連接到實體來授與許可。不過，如果資源型政策會為相同帳戶中的主體授予存取，這時就不需要額外的身分型政策。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM 中的跨帳戶資源存取。

威克爾的政策行動

支援政策動作	是

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

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 Wickr 動作清單，請參閱服務授權參考中的 AWS Wickr 定義的動作。

Wickr 中的政策動作在動作之前使用以下前綴：

```
wickr
```

若要在單一陳述式中指定多個動作，請用逗號分隔。

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

若要檢視 Wickr 身分型原則的範例，請參閱。AWS Wickr 的基於身份的政策範例

威克爾的政策資源

支援政策資源	否

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

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

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

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

若要查看 Wickr 資源類型及其 ARN 的清單，請參閱服務授權參考資料中的 AWS Wickr 定義的資源。若要了解可以使用哪些動作指定每個資源的 ARN，請參閱 AWS Wickr 定義的動作。

若要檢視 Wickr 身分型原則的範例，請參閱。AWS Wickr 的基於身份的政策範例

Wickr 的政策條件金鑰

支援服務特定政策條件金鑰	否

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

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

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

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

若要查看 Wickr 條件金鑰清單，請參閱服務授權參考資料中的 AWS Wickr 條件金鑰。若要了解可以使用條件金鑰的動作和資源，請參閱 AWS Wickr 定義的動作。

若要檢視 Wickr 身分型原則的範例，請參閱。AWS Wickr 的基於身份的政策範例

在威克爾語中的 ACL

支援 ACL	否

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

阿巴克與威克

支援 ABAC (政策中的標籤)	否

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在中 AWS，這些屬性稱為標籤。您可以將標籤附加到 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

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

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

如需 ABAC 的詳細資訊，請參閱 IAM 使用者指南中的什麼是 ABAC?。如要查看含有設定 ABAC 步驟的教學課程，請參閱 IAM 使用者指南中的使用屬性型存取控制 (ABAC)。

透過 Wickr 使用臨時登入資料

支援臨時憑證	否

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配AWS 服務 使用，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱 IAM 使用者指南中的切換至角色 (主控台)。

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

Wickr 的跨服務主體權限

支援轉寄存取工作階段 (FAS)	否

當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，

才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。

威克爾的服務角色

支援服務角色	否

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

> **Warning**
> 變更服務角色的權限可能會中斷 Wickr 功能。只有在 Wickr 提供指引時才編輯服務角色。

Wickr 的服務連結角色

支援服務連結角色。	否

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

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

AWS Wickr 的基於身份的政策範例

根據預設，全新的 IAM 使用者沒有執行任何動作的許可。IAM 管理員必須建立和指派 IAM 政策，以授予使用者管理 AWS Wickr 服務的權限。以下顯示許可政策範例。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wickr:CreateAdminSession",
```

```
                "wickr:ListNetworks"
            ],
            "Resource": "*"
        }
    ]
}
```

此範例原則授予使用者使用 of Wickr 建立、檢視和管理 Wickr 網路的 AWS Management Console 權限。若要進一步了解 IAM 政策陳述式中的元素，請參閱 Wickr 的基於身份識別的政策。若要了解如何使用這些範例 JSON 政策文件建立 IAM 政策，請參閱《IAM 使用者指南》中的在 JSON 標籤上建立政策。

主題

- 政策最佳實務
- 使用對 AWS Management Console 於威克
- 允許使用者檢視他們自己的許可

政策最佳實務

以身分識別為基礎的政策會決定某人是否可以在您的帳戶中建立、存取或刪除 Wickr 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始將權限授與使用者和工作負載，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定 AWS 服務) 使用 AWS CloudFormation。如需詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。

- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

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

使用對 AWS Management Console 於威克

將AWSWickrFullAccess AWS 受管政策附加到您的 IAM 身分，以授予他們對 Wickr 服務的完整管理權限，包括中的 Wickr 管理員主控台。 AWS Management Console如需詳細資訊，請參閱 AWS 受管理的策略： AWSWickrFullAccess。

允許使用者檢視他們自己的許可

此範例會示範如何建立政策，允許 IAM 使用者檢視附加到他們使用者身分的內嵌及受管政策。此原則包含在主控台上或以程式設計方式使用 AWS CLI 或 AWS API 完成此動作的權限。

```
{
    "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": "*"
        }
    ]
}
```

AWS Wickr 身分和存取的疑難排解

使用下列資訊協助您診斷和修正使用 Wickr 和 IAM 時可能會遇到的常見問題。

主題

- 我沒有授權在 Wickr 中執行管理操作 AWS Management Console

我沒有授權在 Wickr 中執行管理操作 AWS Management Console

如果 of Wickr 告訴您您沒有執行動作的授權，您必須聯絡您的系統管理員尋求協助。 AWS Management Console 您的管理員是為您提供簽署憑證的人員。

當 `mateojackson` IAM 使用者嘗試使用 for Wickr 在 AWS Management Console for Wickr 中建立、管理或檢視 Wickr 網路，但沒有和許可時，就會 AWS Management Console 發生下列範例錯誤。`wickr:CreateAdminSession` `wickr:ListNetworks`

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 wickr:ListNetworks
```

在這種情況下，馬特奧要求管理員更新他的政策，以允許他使用`wickr:CreateAdminSession`和`wickr:ListNetworks`操作訪問 Wickr。 AWS Management Console 如需詳細資訊，請參閱 AWS Wickr 的基於身份的政策範例 及 AWS 受管理的策略：AWSWickrFullAccess。

法規遵循驗證

如需特定規範計劃範圍內的 AWS 服務清單，請參閱合規計劃AWS 服務範圍方案)。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 Wickr 時的合規責任取決於您資料的敏感性、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：

- 安全性與合規快速入門指南 — 這些部署指南討論架構考量，並提供在上部署以安全性和法規遵循為重點的基準環境的步驟。 AWS
- 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。
- 使用AWS Config 開發人員指南中的規則評估資源 — AWS Config；評估您的資源配置如何符合內部實踐，業界準則和法規。
- AWS Security Hub— 此 AWS 服務提供安全狀態的全面檢視，協助您檢查您 AWS 是否符合安全性產業標準和最佳做法。

AWS 威克爾的彈性

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。 AWS 區域 提供多個實體分離和隔離的可用區域，這些區域與低延遲、高輸送量和高冗餘網路相連。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱AWS 全域基礎結構。

除了 AWS 全球基礎設施之外，Wickr 還提供多種功能來支援您的資料恢復能力和備份需求。如需詳細資訊，請參閱 資料保留。

AWS Wickr 中的基礎設施安全

AWS Wickr 是受管服務，受 Amazon Web Services：安 AWS 全程序概觀白皮書中所述的全球網路安全程序保護。

AWS 威克爾中的組態和漏洞分析

配置和 IT 控制是與您（我們的客戶） AWS 之間的共同責任。如需詳細資訊，請參閱 AWS 共用的責任模型。

您有責任根據規格和準則配置 Wickr，定期指示您的用戶下載最新版本的 Wickr 客戶端，以確保您運行的是最新版本的 Wickr 數據保留機器人，並監控您的用戶的 Wickr 使用情況。

AWS 威克的安全最佳實務

Wickr 提供了許多安全性功能，可在您開發和實作自己的安全性原則時考慮。以下最佳實務為一般準則，並不代表完整的安全解決方案。這些最佳實務可能不適用或無法滿足您的環境需求，因此請將其視為實用建議就好，而不要當作是指示。

為了防止與您使用 Wickr 相關的潛在安全事件，請遵循以下最佳做法：

- 實施最低權限訪問並創建用於 Wickr 操作的特定角色。使用 IAM 範本建立角色。如需詳細資訊，請參閱 AWS 適用於 AWS 威克的受管政策。
- 通過 AWS Management Console 對第一個進行身份驗證來訪問威克爾。 AWS Management Console 請勿共用您的個人主機憑證。網際網路上的任何人都可以瀏覽到主控台，但除非他們擁有主控台的有效憑證，否則無法登入或開始工作階段。

監控 AWS 威克

監控是維護 AWS Wickr 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 提供以下監控工具來觀看 Wickr，報告出現錯誤，並在適當時採取自動操作：

- AWS CloudTrail擷取您帳戶或代表您 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。如需使用記錄 Wickr API 呼叫的詳細資訊 CloudTrail，請參閱使用記錄 AWS 威克爾 API 呼叫 AWS CloudTrail。

使用記錄 AWS 威克爾 API 呼叫 AWS CloudTrail

AWS Wickr 整合了這項服務AWS CloudTrail，可提供 Wickr 中使用者、角色或AWS服務所採取的動作記錄。 CloudTrail 捕獲威克爾的所有 API 調用作為事件。捕獲的調AWS Management Console用包括來自 Wickr 和代碼調用 Wickr API 操作的調用。如果您建立追蹤，您可以啟用持續傳遞 CloudTrail 事件到 Amazon S3 儲存貯體，包括 Wickr 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 Wickr 提出的要求、提出要求的 IP 位址、提出要求的人員、提出要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。

威克爾信息 CloudTrail

CloudTrail 在您創建帳戶AWS 帳戶時啟用。當活動在 Wickr 中發生時，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。您可以檢視、搜尋和下載 AWS 帳戶 的最新事件。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄檢視事件。

對於您的事件（包括 Wickr 的AWS 帳戶事件）的持續記錄，請創建一個跟踪。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。該追蹤會記錄來自 AWS 分割區中所有區域的事件，並將日誌檔案交付到您指定的 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 Wickr 動作都由 CloudTrail記錄。例如，呼叫和ListNetworks動作會CreateAdminSession在 CloudTrail 記錄檔中產生項目。

每一筆事件或日誌項目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：

- 該請求是否透過根或 AWS Identity and Access Management (IAM) 使用者憑證來提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 該請求是否由另一項 AWS 服務提出。

如需詳細資訊，請參閱 CloudTrail userIdentity 元素。

瞭解 Wickr 記錄檔項目

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CreateAdminSession動作的 CloudTrail 記錄項目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T07:53:17Z",
                "mfaAuthenticated": "false"
            }
```

```
        }
    },
    "eventTime": "2023-03-10T08:19:24Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "CreateAdminSession",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "networkId": 56019692
    },
    "responseElements": {
        "sessionCookie": "***",
        "sessionNonce": "***"
    },
    "requestID": "39ed0e6f-36e9-460d-8a6e-f24be0ec11c5",
    "eventID": "98ccb633-0e6c-4325-8996-35c3043022ac",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
```

```
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T07:53:17Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-10T07:54:09Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "CreateNetwork",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "networkName": "BOT_Network",
        "accessLevel": "3000"
    },
    "responseElements": null,
    "requestID": "b83c0b6e-73ae-45b6-8c85-9910f64d33a1",
    "eventID": "551277bb-87e0-4e66-b2a0-3cc1eff303f3",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
```

```
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T12:19:39Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-10T12:29:32Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "ListNetworks",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "b9800ba8-541a-43d1-9c8e-efd94d5f2115",
    "eventID": "5fbc83d7-771b-457d-9329-f85163a6a428",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
```

```
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T22:42:15Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-08T22:42:58Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "UpdateNetworkDetails",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "networkName": "CloudTrailTest1",
        "networkId": <network-id>
    },
    "responseElements": null,
    "requestID": "abced980-23c7-4de1-b3e3-56aaf0e1fdbb",
    "eventID": "a4dc3391-bdce-487d-b9b0-6f76cedbb198",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
```

```
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T22:42:15Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-08T23:06:04Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "resource-arn": "<arn>",
        "tags": {
            "some-existing-key-3": "value 1"
        }
    },
    "responseElements": null,
    "requestID": "4ff210e1-f69c-4058-8ac3-633fed546983",
    "eventID": "26147035-8130-4841-b908-4537845fac6a",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
```

```
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<access-key-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T18:50:37Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-08T18:50:37Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "ListTagsForResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "axios/0.27.2",
    "errorCode": "AccessDenied",
    "requestParameters": {
        "resource-arn": "<arn>"
    },
    "responseElements": {
        "message": "User: <arn> is not authorized to perform: wickr:ListTagsForResource
 on resource: <arn> with an explicit deny"
    },
    "requestID": "c7488490-a987-4ca2-a686-b29d06db89ed",
    "eventID": "5699d5de-3c69-4fe8-b353-8ae62f249187",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

分析儀表板

您可以使用分析儀表板來檢視組織如何使用 AWS Wickr。下列程序說明如何使用 AWS Wickr 主控台存取分析儀表板。

若要存取分析儀表板

1. 在以下位置 AWS Management Console 打開威克爾的網址：https://console.aws.amazon.com/wickr/。
2. 在導覽窗格中，選擇分析。

   「分析」頁面會在不同的索引標籤中顯示您網路的指標。

在 Analytics (分析) 頁面上，您會在每個索引標籤的右上角找到一個時間範圍篩選器。此篩選條件適用於整個頁面。此外，在每個選項卡的右上角，您可以通過選擇可用的導出選項來導出所選時間範圍的數據點。

> **Note**
>
> 選擇的時間以 UTC（協調世界時）為單位。

以下是可用的索引標籤：

- 概述顯示：
  - [已註冊] — 已註冊使用者的總數，包括所選時間內網路上的作用中和暫停的使用者。它不包括待處理或受邀的使用者。
  - 擱置中 — 所選時間內網路上擱置的使用者總數。
  - 使用者註冊 — 圖表顯示在所選時間範圍內註冊的使用者總數。
  - 裝置 — 應用程式處於作用中狀態的裝置數量。
  - 用戶端版本 — 依用戶端版本分類的作用中裝置數目。

- 成員顯示：
  - 狀態 — 所選時段內網路上的作用中使用者。
  - 活躍用戶 —

    - 此圖形會顯示一段時間內的作用中使用者計數，並可按每日、每週或每月彙總 (在上述選取的時間範圍內)。
    - 作用中使用者計數可依平台、用戶端版本或安全性群組劃分。如果刪除安全性群組，總計數會顯示為 [已刪除 #]。

- 訊息顯示：
    - 已傳送的訊息 — 所選時段內網路上所有使用者和機器人傳送的唯一訊息計數。
    - 呼叫 — 網路中所有使用者進行的唯一呼叫次數。
    - 檔案 — 網路中使用者傳送的檔案數目 (包括語音備忘)。
    - 裝置 — 圓形圖會依其作業系統分類，顯示作用中裝置的數目。
    - 用戶端版本 — 依用戶端版本分類的作用中裝置數目。

文件歷史記錄

下表說明 Wickr 的文件發行版本。

變更	描述	日期
已讀回條功能現已推出	Wickr 管理員現在可以在管理員控制台中啟用或停用讀取回條功能。如需詳細資訊，請參閱已讀取回條。	2024年4月23 日
全球聯合現在支援受限制的同盟，管理員可以在管理員主控台中檢視使用情	全球同盟現在支援限制的同盟。這適用於其 AWS 區域他的威克爾網絡。如需詳細資訊，請參閱安全性群組。此外，管理員現在可以在管理控制台的 Analytics 儀表板上檢視其使用情況分析。如需詳細資訊，請參閱分析儀表板。	2024年3月28日
AWS Wickr 高級計劃的三個月免費試用現已推出	Wickr 管理員現在可以為最多 30 個用戶選擇三個月的免費試用高級計劃。在免費試用期間，所有標準版和高級方案功能均可使用，包括無限制的管理員控制和資料保留。進階版免費試用期間無法使用訪客使用者功能。如需詳細資訊，請參閱管理計劃。	2024年2月9 日
來賓使用者功能通常可用，而且已新增更多系統管理員控制項	Wickr 管理員現在可以存取一系列新功能，包括訪客使用者清單、批量刪除或暫停使用者的功能，以及阻止訪客使用者在 Wickr 網路中進行通訊的選項。如需詳細資訊，請參閱來賓使用者。	2023 年 11 月 8 日

Wickr 現已在歐洲（法蘭克福）上市 AWS 區域	Wickr 現已在歐洲（法蘭克福）AWS 區域上市。如需詳細資訊，請參閱存取 Wickr。	2023 年 10 月 26 日
Wickr 網絡現在有能力跨越聯盟 AWS 區域	Wickr 網路現在有能力跨越聯盟。 AWS 區域如需詳細資訊，請參閱安全性群組。	2023 年 9 月 29 日
Wickr 現已在歐洲（倫敦）上市 AWS 區域	Wickr 現已在歐洲（倫敦）AWS 區域上市。如需詳細資訊，請參閱存取 Wickr。	2023 年 8 月 23 日
Wickr 現已在加拿大（中部）上市 AWS 區域	Wickr 現已在加拿大（中部）AWS 區域上市。如需詳細資訊，請參閱存取 Wickr。	2023 年 7 月 3 日
來賓使用者功能現在可供預覽	訪客用戶可以登錄到 Wickr 客戶端，並與 Wickr 網絡用戶協作。如需詳細資訊，請參閱來賓使用者 (預覽)。	2023 年 5 月 31 日
AWS Wickr 現已與整合 AWS CloudTrail，現在可在 AWS GovCloud (美國西部) 中使用，如下所示 WickrGov	AWS 威克爾現在已與 AWS CloudTrail. 如需詳細資訊，請參閱使用 AWS CloudTrail. 此外，Wickr 現在可在 AWS GovCloud (美國西部) 作為. WickrGov 若要取得更多資訊，請參閱《AWS GovCloud (US) 使用指南》AWS WickrGov中的。	2023 年 3 月 30 日
標記和多個網絡創建	AWS Wickr 現在支援標記。如需詳細資訊，請參閱網路標記。現在可以在 Wickr 中創建多個網絡。如需詳細資訊，請參閱建立網路。	2023 年 3 月 7 日

初始版本	《威克爾管理指南》的初始版本	2022 年 11 月 28 日

版本備註

為了協助您追蹤 Wickr 的持續更新和改進，我們會發佈說明最近變更的版本通知。

2024 年 3 月

- 全域同盟現在支援限制的同盟，其中只能針對在限制同盟下新增的選取網路啟用全域聯合。這適用於其 AWS 區域他的威克爾網絡。如需詳細資訊，請參閱安全性群組。
- 管理員現在可以在管理控制台的 Analytics 儀表板上檢視其使用情況分析。如需詳細資訊，請參閱分析儀表板。

2024 年 2 月

- AWS Wickr 現在為最多 30 位使用者提供三個月的高級方案免費試用。變更和限制包括：
  - 所有標準版和進階方案功能，例如無限制的管理員控制項和資料保留功能，現在都可在 Premium 免費試用中使用 進階版免費試用期間無法使用訪客使用者功能。
  - 之前的免費試用版已不再可用。如果您尚未使用 Premium 免費試用版，則可以將現有的免費試用或標準方案升級為高級版免費試用版。如需詳細資訊，請參閱管理計劃。

2023 年 11 月

- 來賓使用者功能現已正式推出。變更和新增包括：
  - 能夠報告其他 Wickr 用戶的濫用行為。
  - 管理員可以檢視與網路互動的來賓使用者清單，以及每月使用量計數。
  - 系統管理員可以封鎖訪客使用者與其網路通訊。
  - 訪客使用者的附加價格。

- 管理控制增強
  - 能夠批量刪除/暫停用戶。
  - 用於設定權杖重新整理寬限期的其他 SSO 設定。

2023 年 10 月

- 增強功能
  - Wickr 現已在歐洲（法蘭克福）AWS 區域上市。

2023 年 9 月

- 增強功能
  - Wickr 網路現在有能力跨越聯盟。 AWS 區域如需詳細資訊，請參閱安全性群組。

2023 年八月

- 增強功能
  - Wickr 現已在歐洲（倫敦）AWS 區域上市。

2023 年 7 月

- 增強功能
  - Wickr 現已在加拿大（中部）AWS 區域上市。

2023 年 5 月

- 增強功能
  - 增加了對訪客用戶的支持。如需詳細資訊，請參閱 訪客使用者。

2023 年 3 月

- 威克爾現在與 AWS CloudTrail集成。如需詳細資訊，請參閱 使用記錄 AWS 威克爾 API 呼叫 AWS CloudTrail。
- Wickr 現在可在 AWS GovCloud (美國西部) 作為. WickrGov 若要取得更多資訊，請參閱《AWS GovCloud (US) 使用指南》AWS WickrGov中的。

- 威克現在支持標記。如需詳細資訊，請參閱 網路標籤。現在可以在 Wickr 中創建多個網絡。如需詳細資訊，請參閱 步驟 1：建立網路。

2023 年 2 月

- 威克爾現在支持安卓戰術突擊套件（ATAK）。如需詳細資訊，請參閱 在威克爾網路儀表板中啟用 ATAK。

二零二三年一月

- 單一登入 (SSO) 現在可以在所有方案上設定，包括免費試用和標準版。

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。