aws

管理指南

AWS Wickr

AWS Wickr: 管理指南

Table of Contents

什麼是 AWS Wickr？

AWS Wickr 是一種end-to-end加密服務，可協助組織和政府機構透過one-to-one和群組傳訊、語音和視訊通話、檔案共用、螢幕共用等方式安全地通訊。Wickr 可以協助客戶克服與消費者級訊息應用程式相關的資料保留義務，並安全地促進協作。進階安全和管理控制可協助組織滿足法律和法規要求，並針對資料安全挑戰建置自訂解決方案。

資訊可以記錄到私有、客戶控制的資料存放區，以供保留和稽核之用。使用者對資料具有全面的管理控制，包括設定許可、設定暫時性傳訊選項，以及定義安全群組。Wickr 與其他 服務整合，例如 Active Directory (AD)、單一登入 (SSO) 與 OpenID Connect (OIDC) 等。您可以透過 快速建立和管理 Wickr 網路 AWS 管理主控台，並使用 Wickr 機器人安全地自動化工作流程。若要開始使用，請參閱設定 AWS Wickr。

主題

Wickr 的功能

增強安全性和隱私權

Wickr 會針對每個功能使用 256 位元進階加密標準 (AES) end-to-end加密。通訊會在使用者裝置上於本機加密，在傳送給寄件者和接收者以外的任何人時仍無法解密。每個訊息、呼叫和檔案都會使用新的隨機金鑰加密，而且除了預期收件人之外，沒有人 （ 甚至無法 AWS) 可以解密它們。無論是共用敏感和受管制的資料、討論法律或人力資源事宜，甚至是執行戰術軍事操作，客戶都會使用 Wickr 來傳達安全和隱私權的重要性。

資料保留

彈性的管理功能不僅旨在保護敏感資訊，還是為了保留合規義務、法務保存和稽核目的所需的資料。訊息和檔案可以封存在安全、客戶控制的資料存放區中。

彈性存取

使用者具有多裝置（行動裝置、桌面）存取權，且能夠在低頻寬環境中運作，包括中斷連線和out-of-band通訊。

管理控制項

使用者對資料具有全面的管理控制，包括設定許可、設定負責任的暫時性傳訊選項，以及定義安全群組。

強大的整合和機器人

Wickr 與其他 服務整合，例如 Active Directory、單一登入 (SSO) 與 OpenID Connect (OIDC) 等。客戶可以透過 快速建立和管理 Wickr 網路 AWS 管理主控台，並使用 Wickr Bots 安全地自動化工作流程。

以下是 Wickr 協同合作方案的明細：

- 一對一和群組傳訊：在最多 500 名成員的聊天室中安全地與您的團隊聊天
- 音訊和視訊通話：與最多 70 個人進行電話會議
- 螢幕共用和廣播：最多向 500 名參與者展示
- 檔案共用和儲存：將檔案傳輸到 5GBs並具有無限制的儲存
- 暫時性：控制過期和burn-on-read計時器
- 全球聯合：與網路外的 Wickr 使用者連線

區域可用性

Wickr 在美國東部（維吉尼亞北部）、亞太區域（馬來西亞）、亞太區域（新加坡）、亞太區域（雪梨）、亞太區域（東京）、加拿大（中部）、歐洲（法蘭克福）、歐洲（倫敦）、歐洲（斯德哥爾摩）和歐洲（蘇黎世）提供 AWS 區域。Wickr 也適用於 AWS GovCloud（美國西部）區域。每個區域都包含多個可用區域，它們實際上是分開的，但透過私有、低延遲、高頻寬和備援網路連線來連接。這些可用區域用於提供增強的可用性、容錯能力，並將延遲降至最低。

若要進一步了解 AWS 區域，請參閱 中的指定 AWS 區域 您的帳戶可以使用哪些 AWS 一般參考。如需每個區域中可用區域數量的詳細資訊，請參閱 AWS 全球基礎設施。

存取 Wickr

管理員可在 https：//https://console.aws.amazon.com/wickr/ 存取 AWS 管理主控台 for Wickr。開始使用 Wickr 之前，您應該先完成 設定 AWS Wickr和 AWS Wickr 入門指南。

最終使用者透過 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 適用於個人、小型團隊和大型企業的不同計劃。如需詳細資訊，請參閱 AWS Wickr 定價。

Wickr 最終使用者文件

如果您是 Wickr 用戶端的最終使用者，且需要存取其文件，請參閱 AWS Wickr 使用者指南。

設定 AWS Wickr

註冊 AWS 帳戶

若要開始使用 AWS，您需要 AWS 帳戶。如需建立 的相關資訊 AWS 帳戶，請參閱《 AWS 帳戶管理參考指南》中的 入門 AWS 帳戶。

下一步

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。

AWS Wickr 入門

在本指南中，我們會說明如何透過建立網路、設定網路和建立使用者來開始使用 Wickr。

主題

先決條件

開始之前，如果您尚未完成下列先決條件：

- 註冊 Amazon Web Services (AWS)。如需詳細資訊，請參閱設定 AWS Wickr。
- 請確定您擁有管理 Wickr 所需的許可。如需詳細資訊，請參閱AWS受管政策：AWSWickrFullAccess。
- 請務必允許列出 Wickr 的適當連接埠和網域。如需詳細資訊，請參閱允許 Wickr 網路清單的連接埠和網域。

步驟 1：建立網路

您可以建立 Wickr 網路。

完成下列程序，為您的 帳戶建立 Wickr 網路。

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

   > **Note**
   >
   > 如果您之前尚未建立 Wickr 網路，您會看到 Wickr 服務的資訊頁面。建立一或多個 Wickr 網路後，您會看到 Networks 頁面，其中包含您已建立之所有 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的名稱。選擇組織成員將辨識的名稱，例如貴公司的名稱或團隊的名稱。

4. 選擇計劃。您可以選擇下列其中一個 Wickr 網路計劃：

   - 標準 — 適用於需要管理控制和彈性的小型和大型業務團隊。
   - Premium 或 Premium 免費試用 — 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，最多可供 30 位使用者使用，並持續三個月。For AWS WickrGov 的進階免費試用選項最多允許 50 名使用者，而且也持續三個月。在高級免費試用期內，管理員可以升級或降級為高級或標準計劃。

   如需可用 Wickr 計劃和定價的詳細資訊，請參閱 Wickr 定價頁面。

5. （選用）選擇新增標籤，將標籤新增至您的網路。標籤由索引鍵值對組成。標籤可用來搜尋和篩選資源或追蹤您的 AWS 成本。如需詳細資訊，請參閱網路標籤。

6. 選擇建立網路。

   系統會將您重新導向至 AWS 管理主控台 for Wickr 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 AWS 管理主控台 for Wickr，您可以在其中新增使用者、新增安全群組、設定 SSO、設定資料保留和其他網路設定。

1. 在網路頁面上，選取要導覽至該網路的網路名稱。

   系統會將您重新導向至所選網路的 Wickr 管理員主控台。

2. 下列使用者管理選項可供使用。如需設定這些設定的詳細資訊，請參閱管理您的 AWS Wickr 網路。

   - 安全群組 — 管理安全群組及其設定，例如密碼複雜性政策、訊息偏好設定、呼叫功能、安全功能和外部聯合。如需詳細資訊，請參閱AWS Wickr 的安全群組。
   - 單一登入 (SSO) 組態 — 設定 SSO 並檢視 Wickr 網路的端點地址。Wickr 僅支援使用 OpenID Connect (OIDC) 的 SSO 供應商。不支援使用安全性聲明標記語言 (SAML) 的提供者。如需詳細資訊，請參閱AWS Wickr 的單一登入組態。

步驟 3：建立和邀請使用者

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 Wickr 公司 ID 來邀請使用者。最終使用者使用提供的公司 ID 及其工作電子郵件地址註冊 Wickr。如需詳細資訊，請參閱AWS Wickr 的單一登入組態。
- 邀請 — 您可以在 AWS 管理主控台 for Wickr 的 中手動建立使用者，並將電子郵件邀請傳送給他們。最終使用者可以選擇電子郵件中的連結來註冊 Wickr。

> **Note**
>
> 您也可以為 Wickr 網路啟用訪客使用者。如需詳細資訊，請參閱AWS Wickr 網路中的訪客使用者

完成下列程序以建立或邀請使用者。

> **Note**
>
> 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。

若要建立 Wickr 使用者並使用 SSO 傳送邀請：

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下列資訊：

- 您的 Wickr 公司 ID。您可以在設定 SSO 時指定 Wickr 網路的公司 ID。如需詳細資訊，請參閱在 AWS Wickr 中設定 SSO。
- 他們應該用來註冊的電子郵件地址。
- 下載 Wickr 用戶端的 URL。使用者可以從位於 https：//https://aws.amazon.com/wickr/download/ 的 AWS Wickr 下載頁面下載 Wickr 用戶端。

> **Note**
>
> 如果您已在 AWS GovCloud （美國西部） 中建立 Wickr 網路，請指示使用者下載並安裝 WickrGov 用戶端。對於所有其他 AWS 區域，請指示使用者下載並安裝標準 Wickr 用戶端。

如需 AWS WickrGov 的詳細資訊，請參閱AWS GovCloud (US) 《使用者指南》中的 AWS WickrGov。

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

若要手動建立 Wickr 使用者並傳送邀請：

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台 for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。

   系統會將您重新導向至 Wickr 網路。在 Wickr 網路中，您可以新增使用者、新增安全群組、設定 SSO、設定資料保留，以及調整其他設定。
3. 在導覽窗格中，選擇使用者管理。
4. 在使用者管理頁面的團隊目錄索引標籤下，選擇邀請使用者。

   您也可以選擇邀請使用者旁的下拉式選單箭頭，大量邀請使用者。在大量邀請使用者頁面上，選取下載範本，以下載您可以使用使用者清單編輯和上傳的 CSV 範本。
5. 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需要的欄位。請務必為使用者選擇適當的安全群組。
6. 選擇 Invite (邀請)。

   Wickr 會傳送邀請電子郵件到您為使用者指定的地址。此電子郵件提供 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《AWS Wickr 使用者指南》中的下載 Wickr 應用程式並接受您的邀請。

   當使用者使用電子郵件中的連結註冊 Wickr 時，他們在 Wickr 團隊目錄中的狀態將從待定變更為作用中。

後續步驟

您已完成入門步驟。若要管理 Wickr，請參閱下列內容：

- 管理您的 AWS Wickr 網路
- 在 AWS Wickr 中管理使用者

管理您的 AWS Wickr 網路

在 AWS 管理主控台for Wickr 中，您可以管理 Wickr 網路名稱、安全群組、SSO 組態和資料保留設定。

主題

AWS Wickr 的網路詳細資訊

您可以編輯 Wickr 網路的名稱，並在AWS 管理主控台適用於 Wickr 的網路詳細資訊區段中檢視網路 ID。

主題

在 AWS Wickr 中檢視網路詳細資訊

您可以檢視 Wickr 網路的詳細資訊，包括您的網路名稱和網路 ID。

完成下列程序以檢視您的 Wickr 網路設定檔和網路 ID。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台for Wickr。
2. 在網路頁面上，尋找您要檢視的網路。
3. 在您要檢視的網路右側，選取垂直省略符號圖示（三個點），然後選擇檢視詳細資訊。

   網路首頁會在網路詳細資訊區段中顯示您的 Wickr 網路名稱和網路 ID。您可以使用 網路 ID 來設定聯合。

在 AWS Wickr 中編輯網路名稱

您可以編輯 Wickr 網路的名稱。

完成下列程序以編輯您的 Wickr 網路名稱。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台for Wickr。
2. 在網路頁面上，選取網路名稱以導覽至該網路的 Wickr 管理員主控台。
3. 在網路首頁的網路詳細資訊區段中，選擇編輯。
4. 在網路名稱文字方塊中輸入新的網路名稱。
5. 選擇儲存以儲存您的新網路名稱。

在 AWS Wickr 中刪除網路

您可以刪除 AWS Wickr 網路。

> **Note**
>
> 如果您刪除高級免費試用網路，您將無法建立另一個。

若要在 Networks 首頁刪除您的 Wickr 網路，請完成下列程序。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台for Wickr。
2. 在網路頁面上，尋找您要刪除的網路。
3. 在您要刪除的網路右側，選取垂直省略符號圖示（三個點），然後選擇刪除網路。
4. 在快顯視窗中輸入確認，然後選擇刪除。

網路可能需要幾分鐘的時間才能刪除。

若要在網路中刪除 Wickr 網路，請完成下列程序。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台for Wickr。
2. 在網路頁面上，選取您要刪除的網路。
3. 在網路首頁的右上角附近，選擇刪除網路。
4. 在快顯視窗中輸入確認，然後選擇刪除。

   網路可能需要幾分鐘的時間才能刪除。

> **Note**
>
> 當您刪除網路時，不會刪除資料保留組態保留的資料（如果啟用）。如需詳細資訊，請參閱 AWS Wickr 的資料保留。

AWS Wickr 的安全群組

在 AWS 管理主控台for Wickr 的安全群組區段中，您可以管理安全群組及其設定，例如密碼複雜性政策、訊息偏好設定、呼叫功能、安全功能和網路聯合。

主題

- 在 AWS Wickr 中檢視安全群組
- 在 AWS Wickr 中建立安全群組
- 在 AWS Wickr 中編輯安全群組
- 在 AWS Wickr 中刪除安全群組

在 AWS Wickr 中檢視安全群組

您可以檢視 Wickr 安全群組的詳細資訊。

完成下列程序以檢視安全群組。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。

3. 在導覽窗格中，選擇安全群組。

   安全群組頁面會顯示您目前的 Wickr 安全群組，並提供您建立新群組的選項。

   在安全群組頁面上，選取您要檢視的安全群組。此頁面會顯示該安全群組的目前詳細資訊。

在 AWS Wickr 中建立安全群組

您可以建立新的 Wickr 安全群組。

完成下列程序以建立安全群組。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇安全群組。
4. 在安全群組頁面上，選擇建立安全群組以建立新的安全群組。

   > **Note**
   >
   > 具有預設名稱的新安全群組會自動新增至安全群組清單。

5. 在建立安全群組頁面上，輸入安全群組的名稱。
6. 選擇建立安全群組。

   如需編輯新安全群組的詳細資訊，請參閱 在 AWS Wickr 中編輯安全群組。

在 AWS Wickr 中編輯安全群組

您可以編輯 Wickr 安全群組的詳細資訊。

完成下列程序以編輯安全群組。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇安全群組。
4. 選取您要編輯的安全群組名稱。

   安全群組詳細資訊頁面會在不同的標籤中顯示安全群組的設定。

5. 下列索引標籤和對應的設定可供使用：

   - 安全群組詳細資訊 — 在安全群組詳細資訊區段中選擇編輯以編輯名稱。
   - 訊息 — 管理群組成員的訊息功能。
     - Burn-on-read — 控制使用者可以在 Wickr 用戶端中為burn-on-read計時器設定的最大值。如需詳細資訊，請參閱在 Wickr 用戶端中設定訊息過期和燒錄計時器。
     - 過期計時器 — 控制使用者可以為其 Wickr 用戶端中的訊息過期計時器設定的最大值。如需詳細資訊，請參閱在 Wickr 用戶端中設定訊息過期和燒錄計時器。
     - 訊息轉送 — 控制使用者是否可以在其 Wickr 用戶端轉送訊息。如需詳細資訊，請參閱 Wickr 用戶端中的轉送訊息。
     - 快速回應 — 設定快速回應清單，供使用者回應訊息。
     - 安全碎片強度 — 設定安全碎片控制對使用者執行的頻率。如需詳細資訊，請參閱傳訊。
   - 呼叫 — 管理群組成員的呼叫功能。
     - 啟用音訊呼叫 — 使用者可以起始音訊呼叫。
     - 啟用視訊通話和螢幕共用 — 使用者可以在通話期間開始視訊通話或共用螢幕。
     - TCP 呼叫 — 當組織的 IT 或安全部門不允許標準 VoIP UDP 連接埠時，通常會使用啟用（或強制）TCP 呼叫。如果停用 TCP 呼叫，且 UDP 連接埠無法使用，Wickr 用戶端會先嘗試 UDP 並回復至 TCP。
   - 媒體和連結 — 管理與群組成員的媒體和連結相關的設定。

     檔案下載大小 — 選取最佳品質傳輸，以允許使用者以原始加密格式傳輸檔案和附件。如果您選取低頻寬傳輸，Wickr 中使用者傳送的檔案附件將由 Wickr 檔案傳輸服務壓縮。
   - 位置 — 管理群組成員的位置共用設定。

     位置共用 — 使用者可以使用啟用 GPS 的裝置共用其位置。此功能會根據裝置的作業系統預設值顯示視覺化地圖。使用者可以選擇停用地圖檢視，並改為共用包含其 GPS 座標的連結。
   - 安全 — 設定群組的其他安全功能。
     - 啟用帳戶接管保護 — 當使用者將新裝置新增至其帳戶時，強制執行雙重驗證。若要驗證新裝置，使用者可以從舊裝置產生 Wickr 程式碼，或執行電子郵件驗證。這是額外的安全層，可防止未經授權存取 AWS Wickr 帳戶。
     - 啟用一律重新驗證 — 強制使用者在重新進入應用程式時一律重新驗證。
     - 主復原金鑰 — 建立帳戶時建立主復原金鑰。如果沒有其他裝置可用，使用者可以核准將新裝置新增至其帳戶。

    - 非 SSO 逾時 — 為在絕對期間之後需要在應用程式中重新輸入密碼的非 SSO 使用者設定工作階段逾時，無論使用者活動為何。
  - 通知和可見性 — 設定通知和可見性設定，例如群組成員通知中的訊息預覽。
  - Wickr 開放存取 — 設定群組成員的 Wickr 開放存取設定。
    - 啟用 Wickr 開放存取 — 啟用 Wickr 開放存取會掩飾流量，以保護受限和受監控網路上的資料。根據地理位置，Wickr 開放存取會連接到各種全域代理伺服器，為流量混淆提供最佳路徑和通訊協定。
    - Force Wickr 開放存取 — 自動在所有裝置上啟用和強制執行 Wickr 開放存取。
  - 聯合 — 控制您的使用者與其他 Wickr 網路通訊的能力。
    - 本機聯合 — 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 AWS（中部）區域中有兩個網路已啟用本機聯合，它們將能夠互相通訊。
    - 全球聯合 — 能夠與 Wickr Enterprise 使用者或屬於其他區域的不同網路中的AWS使用者聯合。例如，加拿大（中部）AWS區域 Wickr 網路上的使用者，以及歐洲（倫敦）區域網路AWS中的使用者，將能夠在兩個網路的全域聯合開啟時互相通訊。
    - 限制聯合 — 允許列出使用者可以聯合的特定 AWS Wickr 或 Wickr Enterprise 網路。設定後，使用者只能在允許列出的網路中與外部使用者通訊。兩個網路必須允許彼此列出，才能使用受限制的聯合。

      如需訪客聯合的相關資訊，請參閱啟用或停用 AWS Wickr 網路中的訪客使用者。
  - ATAK 外掛程式組態 — 如需啟用 ATAK 的詳細資訊，請參閱什麼是 ATAK？。
6. 選擇儲存以儲存您對安全群組詳細資訊所做的編輯。

在 AWS Wickr 中刪除安全群組

您可以刪除 Wickr 安全群組。

完成下列程序以刪除安全群組。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇安全群組。
4. 在安全群組頁面上，尋找您要刪除的安全群組。
5. 在您要刪除的安全群組右側，選取垂直省略符號圖示（三個點），然後選擇刪除。
6. 在快顯視窗中輸入確認，然後選擇刪除。

當您刪除已指派使用者的安全群組時，這些使用者會自動新增至預設安全群組。若要修改指派給使用者的安全群組，請參閱 編輯 AWS Wickr 網路中的使用者。

AWS Wickr 的單一登入組態

在 AWS 管理主控台for Wickr 中，您可以將 Wickr 設定為使用單一登入系統進行身分驗證。SSO 與適當的多重要素驗證 (MFA) 系統配對時，可提供額外的安全層。Wickr 僅支援使用 OpenID Connect (OIDC) 的 SSO 供應商。不支援使用安全性聲明標記語言 (SAML) 的提供者。

主題

在 AWS Wickr 中檢視 SSO 詳細資訊

您可以檢視 Wickr 網路和網路端點的單一登入組態詳細資訊。

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。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇使用者管理。

   在使用者管理頁面上，單一登入區段會顯示您的 Wickr 網路端點和目前的 SSO 組態。

在 AWS Wickr 中設定 SSO

為了確保安全存取您的 Wickr 網路，您可以設定目前的單一登入組態。詳細的指南可協助您完成此程序。

Important

- 當您設定 SSO 時，您可以為 Wickr 網路指定公司 ID。請務必記錄此公司 ID。傳送邀請電子郵件時，您必須將其提供給最終使用者。最終使用者註冊 Wickr 網路時，必須指定公司 ID。

- 2025 年 9 月，AWS Wickr 推出了改善且更安全的 SSO 連線系統。若要利用這些安全性增強功能，使用 SSO 的組織必須在 2026 年 3 月 9 日之前遷移至新的重新導向 URI。如需遷移說明，請參閱下列AWS re:Post文章：遷移至 AWS Wickr 的新 SSO 重新導向 URI。

如需設定 SSO 的詳細資訊，請參閱下列指南：

- 使用 Microsoft Entra (Azure AD) 進行 AWS Wickr 單一登入 (SSO) 設定
- 使用 Okta 進行 AWS Wickr 單一登入 (SSO) 設定
- Amazon Cognito 的 AWS Wickr 單一登入 (SSO) 設定

使用 Microsoft Entra (Azure AD) 單一登入設定 AWS Wickr

AWS Wickr 可設定為使用 Microsoft Entra (Azure AD) 做為身分提供者。若要這樣做，請在 Microsoft Entra 和 AWS Wickr 管理員主控台中完成下列程序。

Warning

在網路上啟用 SSO 後，它會將作用中使用者登出 Wickr，並強制他們使用 SSO 供應商重新驗證身分。

步驟 1：在 Microsoft Entra 中將 AWS Wickr 註冊為應用程式

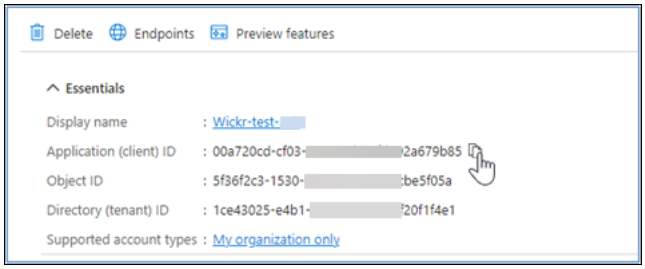
完成下列程序，將 AWS Wickr 註冊為 Microsoft Entra 中的應用程式。

Note

如需詳細的螢幕擷取畫面和疑難排解，請參閱 Microsoft Entra 文件。如需詳細資訊，請參閱使用 Microsoft 身分平台註冊應用程式

1. 在導覽窗格中，選擇應用程式，然後選擇應用程式註冊。
2. 在應用程式註冊頁面上，選擇註冊應用程式，然後輸入應用程式名稱。
3. 僅選取此組織目錄中的帳戶 （僅限預設目錄 - 單一租戶）。
4. 在重新導向 URI 下，選取 Web，然後在 AWS Wickr Admin 主控台的 SSO 組態設定中輸入可用的重新導向 URI

5. 選擇註冊。
6. 註冊後，複製/儲存產生的應用程式（用戶端）ID。

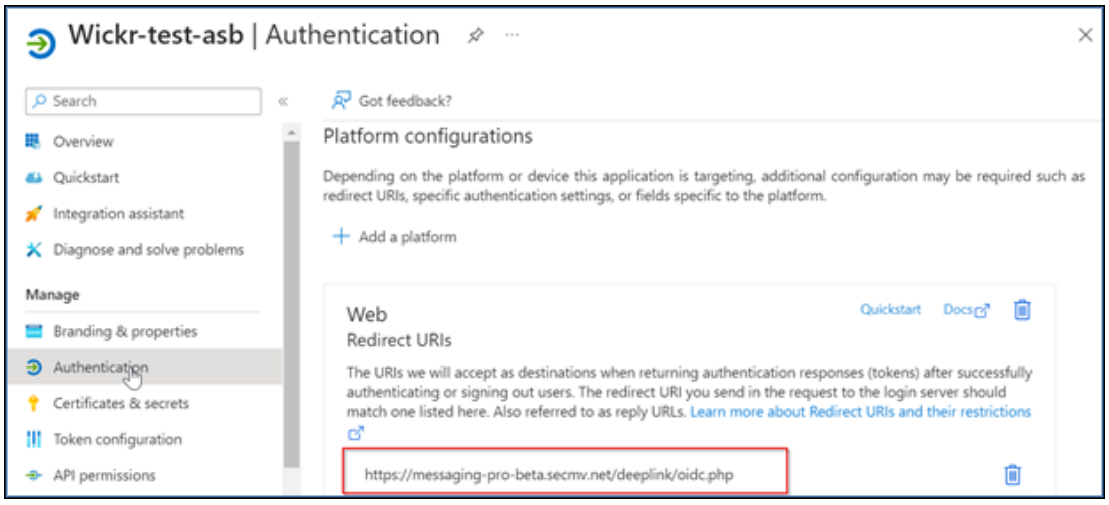


7. 選取端點索引標籤以記下下列項目：
   1. Oauth 2.0 授權端點 (v2)：例如： `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/oauth2/v2.0/authorize`
   2. 編輯此值以移除「oauth2/」和「授權」。例如，固定 URL 如下所示： `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`
   3. 這將參考為 SSO 發行者。

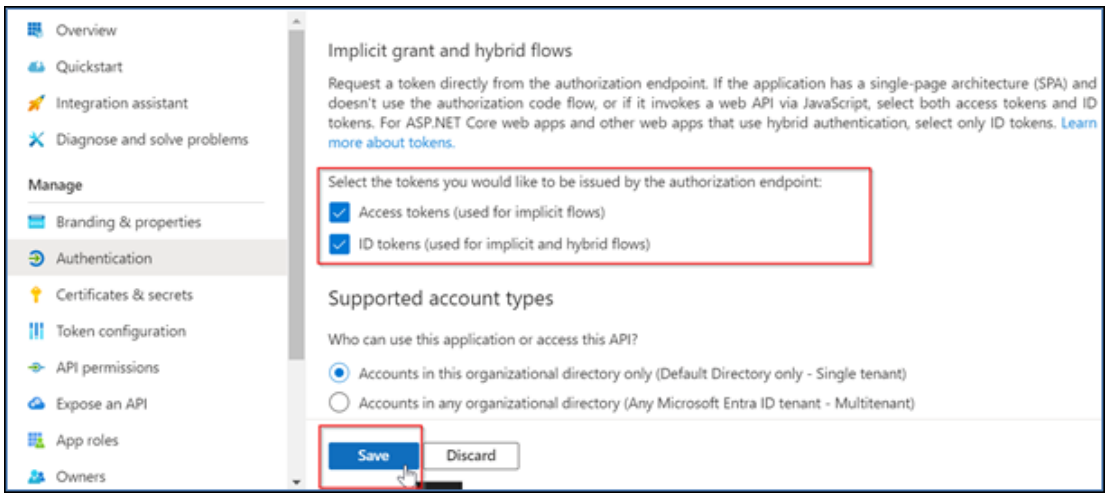
步驟 2：設定身分驗證

完成下列程序以在 Microsoft Entra 中設定身分驗證。

1. 在導覽窗格中，選擇身分驗證。
2. 在身分驗證頁面上，請確定 Web 重新導向 URI 與先前輸入的 URI 相同（在將 AWS Wickr 註冊為應用程式)。



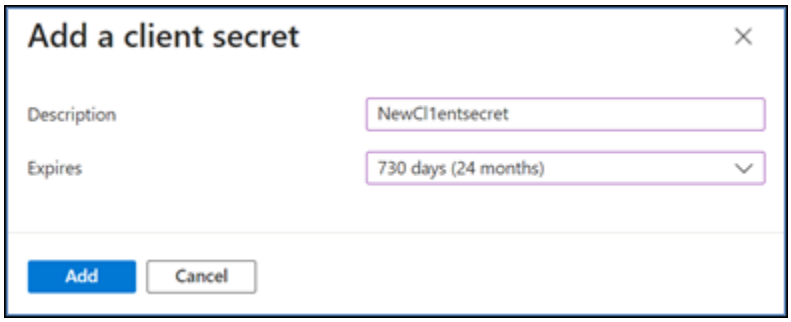
3. 選取用於隱含流程的存取字符，以及用於隱含和混合流程的 ID 字符。
4. 選擇儲存。



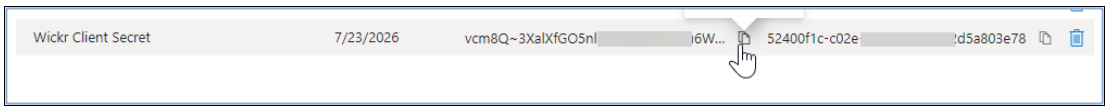
步驟 3：設定憑證和秘密

完成下列程序以在 Microsoft Entra 中設定憑證和秘密。

1. 在導覽窗格中，選擇憑證和秘密。
2. 在憑證與秘密頁面上，選取用戶端秘密索引標籤。
3. 在用戶端秘密索引標籤下，選取新增用戶端秘密。
4. 輸入描述並選取秘密的過期期間。
5. 選擇新增。



6. 建立憑證後，複製用戶端秘密值。

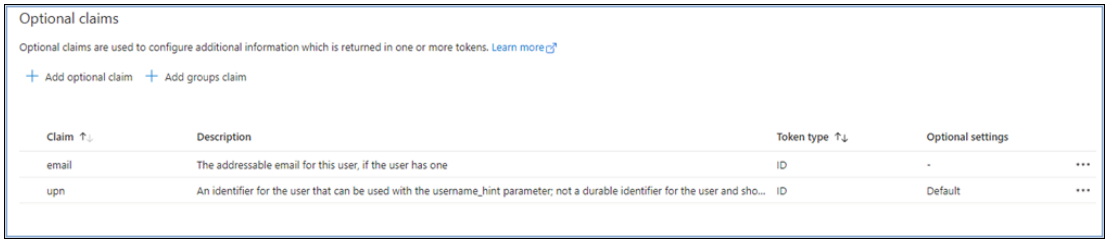


> **Note**
>
> 用戶端應用程式程式碼需要用戶端秘密值 （非秘密 ID)。離開此頁面後，您可能無法檢視或複製秘密值。如果您現在未複製，則必須返回以建立新的用戶端秘密。

步驟 4：設定字符組態

請完成下列程序，以在 Microsoft Entra 中設定權杖組態。

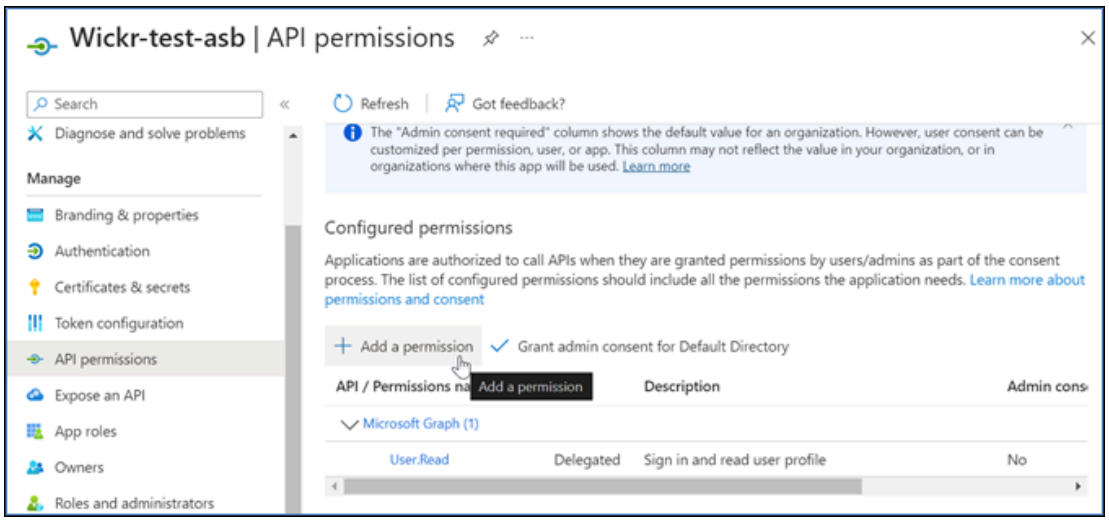
1. 在導覽窗格中，選擇字符組態。
2. 在權杖組態頁面上，選擇新增選用宣告。
3. 在選用宣告下，選取字符類型做為 ID。
4. 選取 ID 之後，在申請下，選取電子郵件並更新。
5. 選擇新增。



步驟 5：設定 API 許可

完成下列程序以在 Microsoft Entra 中設定 API 許可。

1. 在導覽窗格中，選擇 API permissions (API 許可)。
2. 在 API 許可頁面上，選擇新增許可。

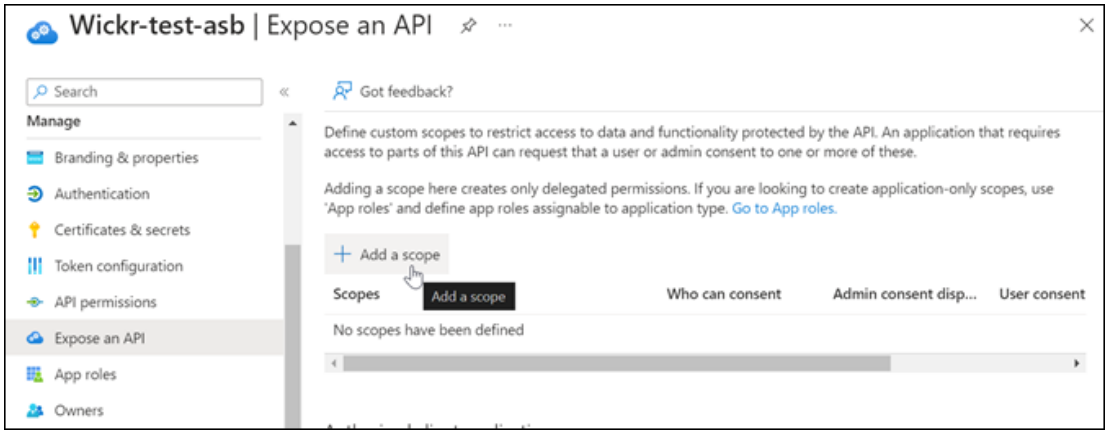


3. 選取 Microsoft Graph，然後選取委派許可 。
4. 選取電子郵件 、離線_存取、Openid、設定檔的核取方塊。
5. 選擇新增許可。

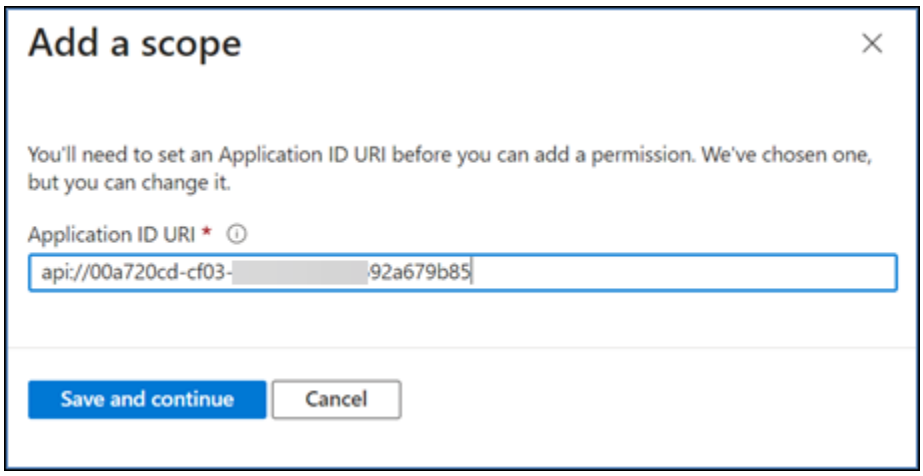
步驟 6：公開 API

請完成下列程序，以公開 Microsoft Entra 中 4 個範圍中的每個範圍的 API。

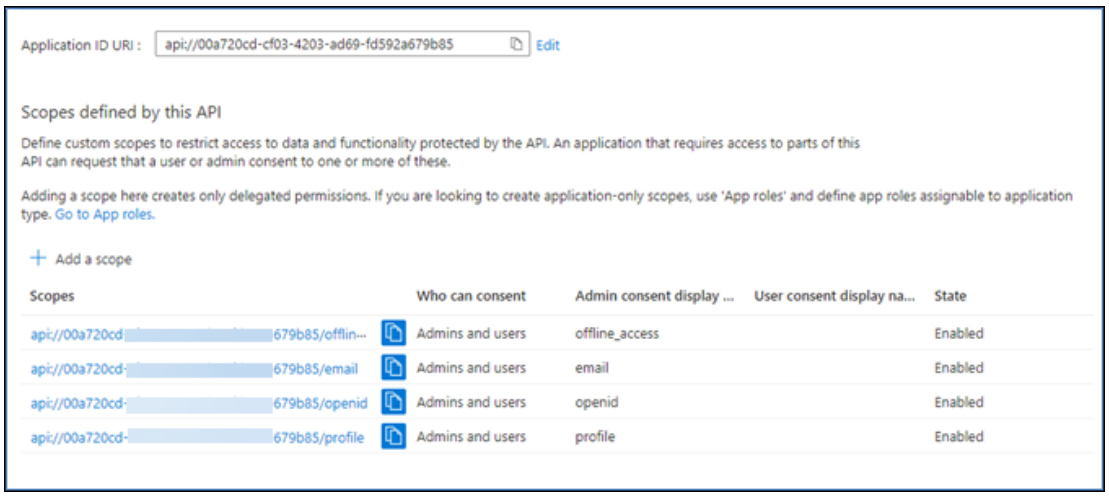
1. 在導覽窗格中，選擇公開 API。
2. 在公開 API 頁面上，選擇新增範圍。



應用程式 ID URI 應自動填入，且 URI 後面的 ID 應符合應用程式 ID （ 在註冊 AWS Wickr 中建立為應用程式)。



3. 選擇儲存並繼續。
4. 選取管理員和使用者標籤，然後將範圍名稱輸入為 offline_access。
5. 選取狀態，然後選取啟用。
6. 選擇新增範圍。
7. 重複本節的步驟 1-6，以新增下列範圍：電子郵件、Openid 和設定檔。



8. 在授權用戶端應用程式下，選擇新增用戶端應用程式。
9. 選取上一個步驟中建立的所有四個範圍。
10. 輸入或驗證應用程式（用戶端）ID。
11. 選擇新增應用程式。

步驟 7：AWS Wickr SSO 組態

在 AWS Wickr 主控台中完成下列組態程序。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台 for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇使用者管理，然後選擇設定 SSO。
4. 輸入下列詳細資訊：

   - 發行者 — 這是先前修改過的端點（例如 `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`）。
   - 用戶端 ID — 這是概觀窗格中的應用程式（用戶端）ID。
   - 用戶端秘密（選用）— 這是憑證和秘密窗格中的用戶端秘密。
   - 範圍 — 這些是公開 API 窗格中公開的範圍名稱。輸入電子郵件、設定檔、離線存取和 openid。
   - 自訂使用者名稱範圍（選用）— 輸入 upn。
   - 公司 ID — 這可以是唯一的文字值，包括英數字元和底線字元。此片語是使用者在新裝置上註冊時將輸入的內容。

   其他欄位為選用。
5. 選擇下一步。
6. 驗證檢閱和儲存頁面中的詳細資訊，然後選擇儲存變更。

SSO 組態已完成。若要驗證，您現在可以在 Microsoft Entra 中將使用者新增至應用程式，並使用 SSO 和公司 ID 與使用者登入。

如需如何邀請和加入使用者的詳細資訊，請參閱建立和邀請使用者。

疑難排解

以下是您可能遇到的常見問題，以及解決這些問題的建議。

- SSO 連線測試失敗或沒有回應：
  - 確定 SSO 發行者設定為預期。
  - 確定 SSO 設定的必填欄位設定為預期。
- 連線測試成功，但使用者無法登入：
  - 確定使用者已新增至您在 Microsoft Entra 中註冊的 Wickr 應用程式。
  - 確定使用者使用正確的公司 ID，包括 字首。例如，UE1-DemoNetworkW_drqtva。

- 用戶端秘密可能無法在 AWS Wickr SSO 組態中正確設定。在 Microsoft Entra 中建立另一個用戶端秘密，並在 Wickr SSO 組態中設定新的用戶端秘密，以重新設定。

權杖重新整理的寬限期

有時，身分提供者可能會遇到暫時或延長中斷，這可能會導致您的使用者因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，您可以建立寬限期，允許使用者保持登入狀態，即使其用戶端重新整理字符在此類中斷期間失敗。

以下是寬限期的可用選項：

- 無寬限期（預設）：使用者將在重新整理字符失敗後立即登出。
- 30 分鐘寬限期：使用者可以在重新整理字符失敗後保持登入長達 30 分鐘。
- 60 分鐘寬限期：使用者可以在重新整理字符失敗後保持登入狀態長達 60 分鐘。

AWS Wickr 的網路標籤

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尋和篩選 Wickr 網路或追蹤您的AWS成本。您可以在 AWS 管理主控台for Wickr 的網路首頁上設定網路標籤。

標籤是套用至資源的鍵/值對，用於保留該資源的中繼資料。每個標籤都是由索引鍵和值組成的標籤。如需標籤的詳細資訊，另請參閱什麼是標籤？ 和 標記使用案例。

主題

- 在 AWS Wickr 中管理網路標籤
- 在 AWS Wickr 中新增網路標籤
- 在 AWS Wickr 中編輯網路標籤
- 在 AWS Wickr 中移除網路標籤

在 AWS Wickr 中管理網路標籤

您可以管理 Wickr 網路的網路標籤。

完成下列程序來管理 Wickr 網路的網路標籤。

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

2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在網路首頁的標籤區段中，選擇管理標籤。
4. 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 — 以金鑰和值對的形式輸入新標籤。選擇新增標籤以新增多個鍵值對。標籤會區分大小寫。如需詳細資訊，請參閱在 AWS Wickr 中新增網路標籤。
   - 編輯現有標籤 — 選取現有標籤的鍵或值文字，然後在文字方塊中輸入修改。如需詳細資訊，請參閱在 AWS Wickr 中編輯網路標籤。
   - 移除現有標籤 — 選擇您要刪除之標籤旁邊的移除按鈕。如需詳細資訊，請參閱在 AWS Wickr 中移除網路標籤。

在 AWS Wickr 中新增網路標籤

您可以將網路標籤新增至 Wickr 網路。

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 在 AWS Wickr 中管理網路標籤。

1. 在網路首頁的標籤區段中，選擇新增標籤。
2. 在管理標籤 頁面上，選擇新增標籤。
3. 在出現的空白索引鍵和值欄位中，輸入新的標籤索引鍵和值。
4. 選擇儲存變更以儲存新標籤。

在 AWS Wickr 中編輯網路標籤

您可以編輯網路標籤到您的 Wickr 網路。

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

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。反之，請移除金鑰和值對，並使用新金鑰新增標籤。

2. 選擇儲存變更以儲存您的編輯。

在 AWS Wickr 中移除網路標籤

您可以移除 Wickr 網路的網路標籤。

完成下列程序，從 Wickr 網路移除標籤。如需管理標籤的詳細資訊，請參閱 在 AWS Wickr 中管理網路標籤。

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。

AWS Wickr 的讀取回條

AWS Wickr 的讀取回條是傳送給寄件者的通知，顯示訊息的讀取時間。這些收據可在one-on-one對話中使用。將針對已傳送的訊息顯示單一核取記號，並針對讀取訊息顯示帶有核取記號的實心圓圈。若要在外部對話期間查看訊息的讀取回條，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讀取回條。此設定將套用至整個網路。

完成下列程序以啟用或停用讀取回條。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇網路政策。
4. 在網路政策頁面的傳訊區段中，選擇編輯。
5. 選取核取方塊以啟用或停用讀取回條。
6. 選擇儲存變更。

管理 AWS Wickr 的網路計劃

在 AWS 管理主控台for Wickr 中，您可以根據您的業務需求管理您的網路計劃。

若要管理您的網路計劃，請完成下列程序。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在網路首頁的網路詳細資訊區段中，選擇編輯。

4. 在編輯網路詳細資訊頁面上，選擇所需的網路計劃。您可以選擇下列其中一項來修改目前的網路計劃：

   - 標準 — 適用於需要管理控制和彈性的小型和大型業務團隊。
   - Premium 或 Premium 免費試用 — 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，最多可供 30 位使用者使用，並持續三個月。對於AWS WickrGov，高級免費試用選項最多允許 50 位使用者，並且持續三個月。這項優惠開放給新的和標準計劃。在高級免費試用期間，管理員可以升級或降級到高級或標準計劃

     > **Note**
     >
     > 若要停止網路的使用和計費，請移除所有使用者，包括網路中暫停的任何使用者。

高級免費試用限制

下列限制適用於 高級免費試用：

- 如果計劃之前已註冊過高級免費試用，則不符合另一項試驗的資格。
- 每個AWS帳戶只能註冊一個網路，才能參加高級免費試用。
- 在高級免費試用期間，無法使用訪客使用者功能。
- 如果標準網路有超過 30 名使用者 (AWSWickrGov 的使用者超過 50 名），將無法升級至高級免費試用。 WickrGov

AWS Wickr 的資料保留

AWS Wickr 資料保留可以保留網路中的所有對話。這包括直接訊息對話，以及網路內（內部）成員與其他團隊（外部）之間的群組或聊天室對話。資料保留僅適用於選擇加入資料保留的 AWS Wickr Premium 計劃使用者和企業客戶。如需 Premium 計劃的詳細資訊，請參閱 Wickr 定價

當網路管理員設定和啟用其網路的資料保留時，其網路中使用者共用的所有訊息和檔案都會封存至指定的位置（例如本機儲存、Amazon S3 儲存貯體），以便視需要檢閱、處理和保留。

> **Note**
>
> AWS無法存取 Wickr end-to-end加密訊息內容。如果您的組織需要存取最終使用者的訊息內容，您必須部署資料保留機器人。

主題

在 AWS Wickr 中檢視資料保留詳細資訊

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

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇網路政策。
4. 網路政策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 AWS Wickr 的資料保留。

> **Note**
>
> 啟用資料保留時，網路中的所有使用者都會看到開啟資料保留訊息，通知他們已啟用保留功能的網路。

設定 AWS Wickr 的資料保留

若要設定 AWS Wickr 網路的資料保留，您必須將資料保留機器人 Docker 映像部署至主機上的容器，例如本機電腦或 Amazon Elastic Compute Cloud (Amazon EC2) 中的執行個體。部署機器人之後，您可以將其設定為在本機或 Amazon Simple Storage Service (Amazon S3) 儲存貯體中存放資

料。您也可以將資料保留機器人設定為使用其他服務， AWS 例如 AWS Secrets Manager (Secrets Manager)、Amazon CloudWatch (CloudWatch)、Amazon Simple Notification Service (Amazon SNS) 和 AWS Key Management Service ()AWS KMS。下列主題說明如何設定和執行 Wickr 網路的資料保留機器人。

對於 Wickr 資料保留 (DR) 機器人的生產部署， AWS 建議使用封存在 Amazon S3 中的訊息部署至 Amazon EC2/Amazon EBS，以及下列執行個體和儲存體大小下限： Amazon S3

- 執行個體類型：m8i.large (8GiB RAM、2vCPUs)
- 儲存：1 TB Amazon EBS 磁碟區
- 部署：每個 Amazon EC2 主機一個 DR 機器人執行個體

如需 Amazon EBS 的詳細資訊，請參閱《Amazon EBS 使用者指南》中的 Amazon EBS 快照生命週期。

主題

設定 AWS Wickr 資料保留的先決條件

這會假設您的 Amazon EC2 執行個體已執行並符合上述最低儲存需求，而且您的 VPC 能夠到達 Wickr 訊息端點：

`com.amazonaws.region.wickr-messaging` — 機器人接收來自 Wickr 訊息服務的訊息。

開始之前，請先完成下列程序，以在 主控台中啟用資料保留。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台 for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。

3. 在導覽窗格中，選擇網路政策。
4. 在網路政策頁面的資料保留區段中，選取編輯。
5. 在編輯資料保留頁面上，遵循步驟 1 和 2。
6. 啟動您的資料保留機器人。如需詳細資訊，請參閱啟動 Wickr 網路的資料保留機器人。
7. 在設定資料保留伺服器區段中，複製使用者名稱和初始密碼。遵循 AWS Wickr 中資料保留機器人的密碼，以使用者名稱和初始密碼設定資料保留機器人。
8. 選取啟用資料保留核取方塊，然後選擇儲存變更。

> **Note**
>
> DR 機器人經過驗證，每小時大約有 11，000 則訊息 (~3 則訊息/秒） 可進行持續處理。對於持續超過此輸送量或預期在單一處理執行中超過 150 萬則訊息的工作負載，應評估額外的擴展策略。

對於災難復原，我們建議在 Amazon EBS 磁碟區 (Amazon S3) 和 Amazon S3 跨區域複寫上使用快照生命週期。若要設定訊息傳送到 Amazon S3 的頻率，您可以設定環境變數 WICKRIO_COMP_FILESIZE 或 WICKRIO_COMP_TIMEROTATE來輪換大小或時間。訊息日誌和檔案附件將交付至相同儲存貯體中的相同字首。如需詳細資訊，請參閱在 AWS Wickr 中設定資料保留機器人的環境變數。

AWS Wickr 中資料保留機器人的密碼

第一次啟動資料保留機器人時，您可以使用下列其中一個選項來指定初始密碼：

- WICKRIO_BOT_PASSWORD 環境變數。本指南稍後的 在 AWS Wickr 中設定資料保留機器人的環境變數一節概述了資料保留機器人環境變數。
- AWS_SECRET_NAME 環境變數在 Secrets Manager 中識別的密碼值。本指南稍後的 AWS Wickr 的 Secrets Manager 值一節概述了資料保留機器人的 Secrets Manager 值。
- 在資料保留機器人提示時輸入密碼。您將需要使用 -ti選項搭配互動式 TTY 存取來執行資料保留機器人。

第一次設定資料保留機器人時，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。您可以輪換產生的密碼。若要輪換產生的密碼，請使用下列各節中提供的指引。

密碼輪換

資料保留機器人（最低版本 6.66.01.00) 可以在啟動時透過設定 WICKRIO_ROTATE_PASSWORD 環境變數，以程式設計方式輪換其 Wickr 帳戶密碼。

Usage

使用 docker 執行啟動機器人時，設定環境變數 WICKRIO_ROTATE_PASSWORD：

```
-e WICKRIO_ROTATE_PASSWORD="new_password"
```

啟動時，機器人成功使用其目前密碼（來自 WICKRIO_BOT_PASSWORD 或 AWS Secrets Manager) 登入後，會執行下列動作：

1. 從程序環境讀取 WICKRIO_ROTATE_PASSWORD。
2. 驗證新密碼（最少 12 個字元，必須與目前的密碼不同）。
3. 呼叫 AWS Wickr 服務來輪換密碼。

輪換成功後，在下次重新啟動之前，將 WICKRIO_BOT_PASSWORD（或 Secrets Manager 中的 AWS 秘密）更新為新密碼。

新產生的密碼會顯示如下範例所示。

> **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。請勿共用此密碼。它可讓您開始 Wickr 網路的資料保留。

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

密碼要求

- 新密碼必須至少為 12 個字元。

- 新密碼必須與目前的密碼不同。
- 機器人必須先能夠使用目前的密碼登入。

AWS Wickr 網路的儲存選項

啟用資料保留並為您的 Wickr 網路設定資料保留機器人後，它會擷取網路內傳送的所有訊息和檔案。訊息會儲存在限制為可使用 環境變數設定之特定大小或時間限制的檔案中。如需詳細資訊，請參閱在 AWS Wickr 中設定資料保留機器人的環境變數。

您可以設定下列其中一個選項來存放此資料：

- 將所有擷取的訊息和檔案儲存在本機。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，並確保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儲存在 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至您指定的 Amazon S3 儲存貯體。擷取的訊息和檔案成功儲存到儲存貯體後，就會從主機機器中移除。
- 將所有擷取的訊息和檔案儲存在 Amazon S3 儲存貯體中加密。資料保留機器人將使用您提供的金鑰重新加密所有擷取的訊息和檔案，並將其儲存至您指定的 Amazon S3 儲存貯體。擷取的訊息和檔案成功重新加密並儲存到儲存貯體後，就會從主機機器中移除。您需要軟體來解密訊息和檔案。

  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

在 AWS Wickr 中設定資料保留機器人的環境變數

您可以使用下列環境變數來設定資料保留機器人。當您執行資料保留機器人 Docker 映像時，您可以使用 `-e`選項來設定這些環境變數。如需詳細資訊，請參閱啟動 Wickr 網路的資料保留機器人。

> **Note**
>
> 除非另有說明，否則這些環境變數為選用。

使用下列環境變數來指定資料保留機器人登入資料：

- `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 AWS Wickr 資料保留的先決條件。 如果您不打算使用密碼提示啟動資料保留機器人，或者不打算使用 Secrets Manager 存放資料保留機器人憑證，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 – 要串流訊息的目錄路徑名稱。預設值為 /tmp/*<botname>*/compliance/messages。
- WICKRIO_COMP_FILEDEST – 要串流檔案的目錄路徑名稱。預設值為 /tmp/*<botname>*/compliance/attachments。
- WICKRIO_COMP_BASENAME – 接收的訊息檔案的基本名稱。預設值為 receivedMessages。
- WICKRIO_COMP_FILESIZE – 所接收訊息檔案的檔案大小上限，以 KB (KiB) 為單位。達到大小上限時，就會啟動新檔案。預設值為 1000000000，如 1024 GiB 所示。
- WICKRIO_COMP_TIMEROTATE – 資料保留機器人將接收訊息放入接收訊息檔案中的時間，以分鐘為單位。預設值為 0，如不輪換。使用 Amazon S3 進行資料保留時，需要此變數。如果不設定此值，訊息檔案永遠不會輪換，因此永遠不會傳送到 Amazon S3。建議的開始值為10分鐘。您可以根據您的訊息量和交付需求調整此值。

使用下列環境變數來定義 AWS 區域 要使用的預設值。

- AWS_DEFAULT_REGION – AWS 區域 用於 Secrets Manager 等 AWS 服務的預設值 （不適用於 Amazon S3 或 AWS KMS)。如果未定義此環境變數，則預設會使用 us-east-1區域。

當您選擇使用 Secrets Manager 來存放資料保留機器人憑證 AWS 和服務資訊時，請使用下列環境變數來指定要使用的 Secrets Manager 秘密。如需您可以在 Secrets Manager 中存放之值的詳細資訊，請參閱 AWS Wickr 的 Secrets Manager 值。

- AWS_SECRET_NAME – Secrets Manager 秘密的名稱，其中包含資料保留機器人所需的登入 AWS 資料和服務資訊。
- AWS_SECRET_REGION – AWS 區域 AWS 秘密所在的 。如果您使用的是 AWS 秘密，但未定義此值，則會使用該AWS_DEFAULT_REGION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，並將這些值存放在該處，則不需要在執行資料保留機器人 Docker 映像時將其指定為環境變數。您只需要指定本指南先前所述的`AWS_SECRET_NAME`環境變數。如需詳細資訊，請參閱AWS Wickr 的 Secrets Manager 值。

當您選擇將訊息和檔案儲存至儲存貯體時，請使用下列環境變數來指定 Amazon S3 儲存貯體。

- `WICKRIO_S3_BUCKET_NAME` – 存放訊息和檔案的 Amazon S3 儲存貯體名稱。
- `WICKRIO_S3_REGION` – 存放訊息和檔案的 Amazon S3 儲存貯體 AWS 區域。
- `WICKRIO_S3_FOLDER_NAME` – Amazon S3 儲存貯體中儲存訊息和檔案的選用資料夾名稱。此資料夾名稱前面會加上 金鑰，用於儲存到 Amazon S3 儲存貯體的訊息和檔案。

當您選擇使用用戶端加密將檔案儲存到 Amazon S3 儲存貯體時，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 Resource Name (ARN)，用於在儲存到 Amazon S3 儲存貯體之前，重新加密資料保留機器人上的訊息檔案和檔案。
- `WICKRIO_KMS_REGION` – 主金鑰所在的 AWS 區域 AWS KMS 。

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來指定 Amazon SNS 詳細資訊。傳送的事件包括啟動、關閉以及錯誤條件。

- `WICKRIO_SNS_TOPIC_ARN` – 您希望資料保留事件傳送到的 Amazon SNS 主題 ARN。

使用下列環境變數將資料保留指標傳送至 CloudWatch。如果指定，則會每 60 秒產生一次指標。

- `WICKRIO_METRICS_TYPE` – 將此環境變數的值設定為 `cloudwatch`，以將指標傳送至 CloudWatch。

AWS Wickr 的 Secrets Manager 值

您可以使用 Secrets Manager 來存放資料保留機器人登入資料 AWS 和服務資訊。如需建立 Secrets Manager 秘密的詳細資訊，請參閱《AWS Secrets Manager Secrets Manager 使用者指南》中的建立秘密。

Secrets Manager 秘密可以有下列值：

- `password` – 資料保留機器人密碼。
- `s3_bucket_name` – 存放訊息和檔案的 Amazon S3 儲存貯體名稱。如果未設定，則會使用預設檔案串流。
- `s3_region` – 存放訊息和檔案的 Amazon S3 儲存貯體 AWS 區域。
- `s3_folder_name` – Amazon S3 儲存貯體中儲存訊息和檔案的選用資料夾名稱。此資料夾名稱前面會加上 金鑰，用於儲存到 Amazon S3 儲存貯體的訊息和檔案。
- `kms_master_key_arn` – AWS KMS 主金鑰的 ARN，用於在儲存到 Amazon S3 儲存貯體之前，重新加密資料保留機器人上的訊息檔案和檔案。
- `kms_region` – AWS KMS 主金鑰所在的 AWS 區域。
- `sns_topic_arn` – 您希望資料保留事件傳送到的 Amazon SNS 主題 ARN。

搭配 AWS 服務使用資料保留的 IAM 政策

如果您計劃 AWS 搭配 Wickr 資料保留機器人使用其他服務，您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、Amazon S3、CloudWatch、Amazon SNS 和 AWS KMS。下列 IAM 政策允許存取這些服務的特定動作。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "secretsmanager:GetSecretValue",
```

```
                "sns:Publish",
                "cloudwatch:PutMetricData",
                "kms:GenerateDataKey"
            ],
            "Resource": "*"
        }
    ]
}
```

您可以透過識別您要允許主機上容器存取之每個服務的特定物件，來建立更嚴格的 IAM 政策。移除您不打算使用之 AWS 服務的動作。例如，如果您打算僅使用 Amazon S3 儲存貯體，請使用下列政策，這會移除 `secretsmanager:GetSecretValue`、`sns:Publish`、 `kms:GenerateDataKey`和 `cloudwatch:PutMetricData`動作。

JSON

```
{
    "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 Wickr 網路的資料保留機器人

執行資料保留機器人之前，您應該先決定設定的方式。如果您計劃在符合下列條件的主機上執行機器人：

- 無法存取 AWS 服務，則您的選項會受到限制。在這種情況下，您將使用預設訊息串流選項。您應該決定要將擷取的訊息檔案大小限制為特定大小或時間間隔。如需詳細資訊，請參閱[在 AWS Wickr 中設定資料保留機器人的環境變數]。

- 將可存取 AWS 服務，然後您應該建立 Secrets Manager 秘密來存放機器人登入 AWS 資料和服務組態詳細資訊。設定 AWS 服務之後，您可以繼續啟動資料保留機器人 Docker 映像。如需可存放在 Secrets Manager 秘密中詳細資訊的詳細資訊，請參閱 AWS Wickr 的 Secrets Manager 值

下列各節顯示執行資料保留機器人 Docker 映像的範例命令。在每個範例命令中，將下列範例值取代為您自己的值：

- *compliance_1234567890_bot* 資料保留機器人的名稱。
- *password* 資料保留機器人的密碼。
- *wickr/data/retention/bot* 包含要與資料保留機器人搭配使用的 Secrets Manager 秘密名稱。
- *bucket-name* 儲存訊息和檔案的 Amazon S3 儲存貯體名稱。
- *folder-name* Amazon S3 儲存貯體中存放訊息和檔案的資料夾名稱。
- *us-east-1* 您指定之資源 AWS 的區域。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 Resource Name (ARN) 來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 命令會啟動資料保留機器人。密碼是使用 WICKRIO_BOT_PASSWORD環境變數來指定。機器人開始使用預設檔案串流，並使用本指南 在 AWS Wickr 中設定資料保留機器人的環境變數區段中定義的預設值。

```
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' \
public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud:latest
```

使用密碼提示啟動機器人（無 AWS 服務）

下列 Docker 命令會啟動資料保留機器人。資料保留機器人提示時，會輸入密碼。它會使用本指南 在 AWS Wickr 中設定資料保留機器人的環境變數區段中定義的預設值，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' \
public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud:latest

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

使用 -ti選項執行機器人，以接收密碼提示。您也應該在啟動 docker 映像後立即執行 docker attach *<container ID or container name>*命令，以取得密碼提示。您應該在指令碼中執行這兩個命令。如果您連接到 Docker 影像，但未看到提示，請按 Enter，您會看到提示。

以 10 分鐘訊息檔案輪換啟動機器人（無 AWS 服務）

下列 Docker 命令會使用環境變數啟動資料保留機器人。它也會將其設定為將接收的訊息檔案輪換為 10 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=10 \
public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud:latest
```

啟動機器人並使用 Secrets Manager 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。啟動資料保留機器人時，您需要設定環境變數，指定存放此資訊的 Secrets Manager。

```
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='wickrpro/alpha/new-3-bot' \
public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud:latest
```

wickrpro/compliance/compliance_1234567890_bot 秘密中的秘密值如下，顯示為純文字。

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

啟動機器人並使用 Secrets Manager 設定 Amazon S3

您可以使用 Secrets Manager 來託管登入資料和 Amazon S3 儲存貯體資訊。啟動資料保留機器人時，您需要設定環境變數，指定存放此資訊的 Secrets Manager。

```
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='wickrpro/alpha/compliance_1234567890_bot' \
 -e WICKRIO_COMP_TIMEROTATE=10 \
public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud:latest
```

wickrpro/compliance/compliance_1234567890_bot 秘密中的秘密值如下，顯示為純文字。

```
{
    "password":"password",
    "s3_bucket_name":"bucket-name",
    "s3_region":"us-east-1",
    "s3_folder_name":"folder-name"
}
```

機器人收到的訊息和檔案會放入名為 的資料夾中的 bot-compliance儲存貯體network1234567890。

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

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。啟動資料保留機器人時，您需要設定環境變數，指定存放此資訊的 Secrets Manager。

```
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='wickrpro/alpha/compliance_1234567890_bot' \
 -e WICKRIO_COMP_TIMEROTATE=10 \
public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud:latest
```

wickrpro/compliance/compliance_1234567890_bot 秘密中的秘密值如下，顯示為純文字。

```
{
    "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"
}
```

機器人收到的訊息和檔案將使用 ARN 值識別的 KMS 金鑰加密，然後放入名為「network1234567890」的資料夾中的「機器人合規」儲存貯體。請確定您已設定適當的 IAM 政策。

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 託管資料保留機器人登入資料，您可以使用下列環境變數啟動資料保留機器人 Docker 映像。您必須使用 WICKRIO_BOT_NAME環境變數來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_COMP_TIMEROTATE=10 \
-e WICKRIO_S3_BUCKET_NAME='bot-compliance' \
-e WICKRIO_S3_FOLDER_NAME='network1234567890' \
-e WICKRIO_S3_REGION='us-east-1' \
public.ecr.aws/x3s2s6k3/wickrio/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 Wickr 網路的資料保留機器人

在資料保留機器人上執行的軟體會擷取SIGTERM訊號並正常關閉。使用 `docker stop <container ID or container name>`命令，如下列範例所示，向資料保留機器人 Docker 映像發出 SIGTERM命令。

```
docker stop compliance_1234567890_bot
```

取得 Wickr 網路的資料保留日誌

在資料保留機器人 Docker 映像上執行的軟體將輸出至 /tmp/<botname>/logs目錄中的日誌檔案。它們最多會輪換 5 個檔案。您可以執行下列命令來取得日誌。

```
docker logs <botname>
```

範例：

```
docker logs compliance_1234567890_bot
```

Wickr 網路的資料保留指標和事件

以下是 AWS Wickr 資料保留機器人 5.116 版目前支援的 Amazon CloudWatch (CloudWatch) 指標和 Amazon Simple Notification Service (Amazon SNS) 事件。

主題

Wickr 網路的 CloudWatch 指標

指標由機器人每隔 1 分鐘產生，並傳輸到與執行資料保留機器人 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	說明
Messages_Rx	收到的訊息。
Messages_Rx_Failed	無法處理收到的訊息。
Messages_Saved	儲存至已接收訊息檔案的訊息。
Messages_Saved_Failed	無法將訊息儲存至接收的訊息檔案。
Files_Saved	收到的檔案。
Files_Saved_Bytes	所接收檔案的位元組數。
Files_Saved_Failed	無法儲存檔案。
登入	登入 （通常每個間隔為 1)。
Login_Failures	登入失敗 （通常每個間隔為 1)。

指標	說明
S3_Post_Errors	將訊息檔案發佈至 Amazon S3 儲存貯體時發生錯誤。
Watchdog_Failures	監視程式失敗。
Watchdog_Warnings	監視程式警告。

產生指標以供 CloudWatch 使用。用於機器人的命名空間為 `WickrIO`。每個指標都有一系列維度。以下是使用上述指標發佈的維度清單。

維度	Value
Id	機器人的使用者名稱。
裝置	特定機器人裝置或執行個體的說明。如果您執行多個機器人裝置或執行個體，則很有用。
產品	機器人的產品。可以是 `WickrPro_` 或 `WickrEnterprise_` 搭配 `Alpha`、 `Beta`或 `Production` 附加。
BotType	機器人類型。標記為合規機器人的合規。
網路	關聯網路的 ID。

Wickr 網路的 Amazon SNS 事件

下列事件會發佈至由使用環境`WICKRIO_SNS_TOPIC_ARN`變數或 `sns_topic_arn` Secrets Manager 秘密值識別的 Amazon Resource Name (ARN) 值定義的 Amazon SNS 主題。如需詳細資訊，請參閱在 AWS Wickr 中設定資料保留機器人的環境變數及AWS Wickr 的 Secrets Manager 值。

資料保留機器人產生的事件會以 JSON 字串傳送。下列值包含在資料保留機器人 5.116 版的事件中。

名稱	值
complianceBot	資料保留機器人的使用者名稱。

名稱	值
dataTime	事件發生的日期和時間。
device	特定機器人裝置或執行個體的描述。如果您執行多個機器人執行個體，則很有用。
dockerImage	與機器人相關聯的 Docker 映像。
dockerTag	Docker 映像的標籤或版本。
message	事件訊息。如需更多資訊，請參閱關鍵事件及正常事件。
notificationType	此值將為 `Bot Event`。
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，系統會傳送電子郵件給您，其中包含類似下列範例的資訊。

```
{
"complianceBot": "compliance_1234567890_bot",
 "dateTime": "2022-10-12T13:05:39",
 "device": "Desktop 1234567890ab",
 "dockerImage": "public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud",
 "dockerTag": "5.116.13.01",
 "message": "Logged in",
 "notificationType": "Bot Event",
 "severity": "normal"
}
```

關鍵事件

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

登入失敗

以下是機器人無法登入時可能產生的事件。每個訊息都會指出登入失敗的原因。

事件類型	事件訊息
失敗登入	登入資料錯誤。檢查密碼。
失敗登入	找不到使用者。
失敗登入	帳戶或裝置已暫停。
佈建中	使用者已結束 命令。
佈建中	`config.wickr` 檔案的密碼不正確。
佈建中	無法讀取`config.wickr` 檔案。
失敗登入	登入所有失敗。
失敗登入	新使用者但資料庫已存在。

更關鍵的事件

事件類型	事件訊息
暫停的帳戶	WickrIOClientMain： ：slotAdminUserSuspend：code(%1)： 原因：%2“
BotDevice 已暫停	裝置已暫停！
WatchDog	SwitchBoard 系統已關閉超過 <*N*> 分鐘
S3 失敗	無法在 S3 儲存貯體上放置檔案 <*file-name* >>。錯誤：<*AWS-error* >
備用金鑰	SERVER SUBMIITED FALLBACK KEY：不是可辨識的用戶端作用中備用金鑰。請將日誌提交至桌面工程。

正常事件

以下是警告您正常操作發生的事件。在特定期間內發生過多這類事件可能會導致疑慮。

裝置已新增至帳戶

當新裝置新增至資料保留機器人帳戶時，就會產生此事件。在某些情況下，這可能表示有人已建立資料保留機器人的執行個體。以下是此事件的訊息。

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

已登入的機器人

此事件會在機器人成功登入時產生。以下是此事件的訊息。

```
Logged in
```

關閉

此事件會在機器人關閉時產生。如果使用者未明確啟動，則可能表示發生問題。以下是此事件的訊息。

```
Shutting down
```

可用的更新

此事件會在資料保留機器人啟動時產生，並識別有較新版本的相關聯 Docker 映像可用。此事件會在機器人啟動時產生，並每天產生。此事件包含陣列versions欄位，可識別可用的新版本。以下是此事件的範例。

```
{
  "complianceBot": "compliance_1234567890_bot",
  "dateTime": "2022-10-12T13:05:55",
  "device": "Desktop 1234567890ab",
  "dockerImage": "public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud",
  "dockerTag": "5.116.13.01",
  "message": "There are updates available",
  "notificationType": "Bot Event",
  "severity": "normal",
  "versions": [
    "5.116.10.01"
  ]
}
```

安全考量

仔細評估部署資料保留機器人的位置和方式。這些機器人會集中收集和解密使用者傳送或接收的所有end-to-end加密訊息，合併先前只能在個別裝置上存取的內容。因此，此元件及其資料儲存體具有極高的安全性值。

如果您部署資料保留機器人，請確保它符合最高安全標準，並與您的組織安全政策保持一致。對於使用 AWS 服務的部署，請遵循 AWS Wickr 和雲端安全共同責任模型的安全最佳實務中的其他指導。AWS

什麼是 ATAK？

Android Team Awareness Kit (ATAK) 或 Android Tactical Assault Kit （也是 ATAK) 供軍事使用，是一種智慧型手機地理空間基礎設施和情境感知應用程式，可實現與地理之間的安全協作。雖然最初設計用於戰鬥區域，但 ATAK 已適應當地、州和聯邦機構的任務。

主題

- 在 Wickr 網路儀表板中啟用 ATAK
- 有關 ATAK 的其他資訊
- 安裝並配對 ATAK 的 Wickr 外掛程式
- 取消配對 ATAK 的 Wickr 外掛程式
- 在 ATAK 中撥號和接聽通話
- 在 ATAK 中傳送檔案
- 在 ATAK 中傳送安全語音訊息 (Push-to-talk)
- ATAK 的 Pinwheel （快速存取）
- ATAK 導覽

在 Wickr 網路儀表板中啟用 ATAK

AWS Wickr 支援許多使用 Android Tactical Assault Kit (ATAK) 的代理程式。不過，到目前為止，使用 Wickr 的 ATAK 運算子必須離開應用程式才能這麼做。為了協助降低中斷和操作風險，Wickr 開發了一個外掛程式，可增強具有安全通訊功能的 ATAK。使用適用於 ATAK 的 Wickr 外掛程式，使用者可以在 ATAK 應用程式內的 Wickr 上傳送訊息、協作和傳輸檔案。這可消除中斷，以及 ATAK 聊天功能的組態複雜性。

在 Wickr 網路儀表板中啟用 ATAK

請完成下列程序，以在 Wickr 網路儀表板中啟用 ATAK。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台 for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇安全群組。
4. 在安全群組頁面上，選取要啟用 ATAK 的所需安全群組。
5. 在整合索引標籤的 ATAK 外掛程式區段中，選擇編輯。
6. 在編輯 ATAK 外掛程式頁面上，選取啟用 ATAK 外掛程式核取方塊。
7. 選擇新增套件
8. 在套件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 最終使用者要在其 Android 裝置上安裝並使用 ATAK 應用程式的一般版本，請在套件文字方塊中輸入此值。
   - `com.atakmap.app.mil` — 如果您的 Wickr 最終使用者要在 Android 裝置上安裝並使用 ATAK 應用程式的軍事版本，請在套件文字方塊中輸入此值。
9. 選擇儲存。

   現在已為選取的 Wickr 網路和選取的安全群組啟用 ATAK。您應該在啟用 ATAK 功能的安全群組中要求 Android 使用者安裝 ATAK 的 Wickr 外掛程式。如需詳細資訊，請參閱安裝和配對 Wickr ATAK 外掛程式。

有關 ATAK 的其他資訊

如需 ATAK 的 Wickr 外掛程式的詳細資訊，請參閱下列內容：

- Wickr ATAK 外掛程式概觀
- 其他 Wickr ATAK 外掛程式資訊

安裝並配對 ATAK 的 Wickr 外掛程式

Android 團隊意識套件 (ATAK) 是美國軍事、州和政府機構使用的 Android 解決方案，需要情境意識功能來執行任務規劃、執行和事件回應。ATAK 具有外掛程式架構，可讓開發人員新增功能。它可讓使用者使用 GPS 和地理空間地圖資料進行導覽，並覆蓋對持續事件的即時情境感知。在本文件中，我們會示範如何在 Android 裝置上安裝適用於 ATAK 的 Wickr 外掛程式，並將其與 Wickr 用戶端配對。這可讓您在 Wickr 上傳送訊息和協同合作，而無需結束 ATAK 應用程式。

安裝 ATAK 的 Wickr 外掛程式

請完成下列程序，以在 Android 裝置上安裝 ATAK 的 Wickr 外掛程式。

1. 前往 Google Play 商店，並安裝 Wickr for ATAK 外掛程式。
2. 在 Android 裝置上開啟 ATAK 應用程式。
3. 在 ATAK 應用程式中，選擇畫面右上角的選單圖示 ()，然後選擇外掛程式。
4. 選擇匯入。
5. 在選取匯入類型快顯視窗上，選擇本機 SD，然後導覽至您儲存 ATAK .apk 檔案的 Wickr 外掛程式的位置。
6. 選擇外掛程式檔案，並依照提示進行安裝。

   > **Note**
   >
   > 如果系統要求您傳送要掃描的外掛程式檔案，請選擇否。

7. ATAK 應用程式將詢問您是否要載入外掛程式。選擇確定。

ATAK 的 Wickr 外掛程式現在已安裝。繼續下列使用 Wickr 配對 ATAK 區段以完成程序。

將 ATAK 與 Wickr 配對

成功完成安裝 ATAK 的 Wickr 外掛程式後，請完成下列程序，將 ATAK 應用程式與 Wickr 配對。

1. 在 ATAK 應用程式中，選擇畫面右上角的選單圖示 ()，然後選擇 Wickr 外掛程式。

2. 選擇配對 Wickr。

   隨即出現通知提示，要求您檢閱 ATAK 的 Wickr 外掛程式許可。如果通知提示未出現，請開啟 Wickr 用戶端並前往設定，然後是連線的應用程式。您應該會在畫面的待定區段下看到外掛程式。
3. 選擇核准以進行配對。
4. 選擇開啟 Wickr ATAK 外掛程式按鈕以返回 ATAK 應用程式。

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

取消配對 ATAK 的 Wickr 外掛程式

您可以取消配對 ATAK 的 Wickr 外掛程式。

請完成下列程序，將 ATAK 外掛程式與 Wickr 取消配對。

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. 在連線的應用程式畫面上，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。

   您現在已成功取消配對 ATAK 的 Wickr 外掛程式。

在 ATAK 中撥號和接聽通話

您可以在 ATAK 的 Wickr 外掛程式中撥打和接聽通話。

完成下列程序以撥打和接聽通話。

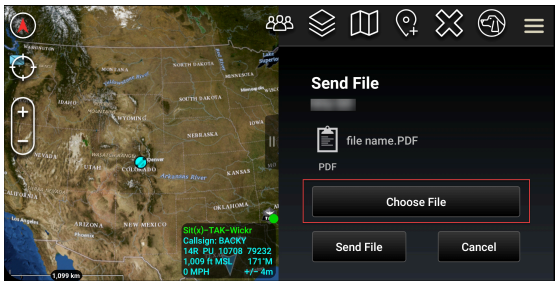
1. 開啟聊天視窗。
2. 在地圖檢視中，選擇您要呼叫之使用者的圖示。
3. 選擇畫面右上角的電話圖示。
4. 連線後，您可以返回 ATAK 外掛程式檢視並接聽通話。

在 ATAK 中傳送檔案

您可以在 ATAK 的 Wickr 外掛程式中傳送檔案。

完成下列程序以傳送檔案。

1. 開啟聊天視窗。
2. 在映射檢視中，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，請選取其名稱。
4. 在傳送檔案畫面上，選取選擇檔案，然後導覽至您要傳送的檔案。



5. 在瀏覽器視窗上，選擇所需的檔案。
6. 在傳送檔案畫面上，選擇傳送檔案。

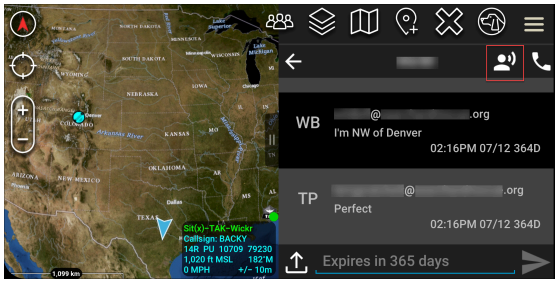
   此時會顯示下載圖示，指出您正在下載選取的檔案。

在 ATAK 中傳送安全語音訊息 (Push-to-talk)

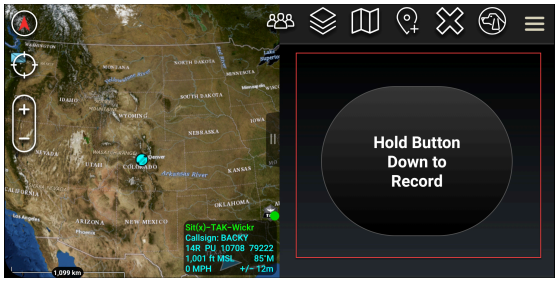
您可以在 ATAK 的 Wickr 外掛程式中傳送安全的語音訊息 (Push-to-talk。

完成下列程序以傳送安全語音訊息。

1. 開啟聊天視窗。
2. 選擇畫面頂端的Push-to-Talk圖示，以說話者的圖示表示。



3. 選取並按住按住按鈕以錄製按鈕。



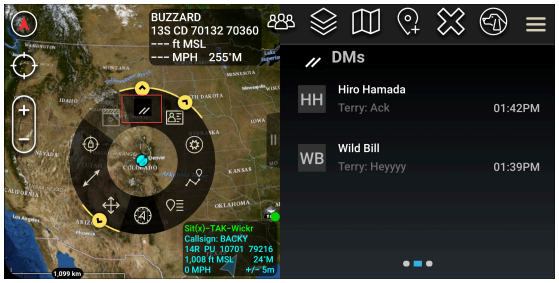
4. 記錄您的訊息。
5. 記錄訊息後，放開要傳送的按鈕。

ATAK 的 Pinwheel （快速存取）

輪轉或快速存取功能用於one-one-one對話或直接訊息。

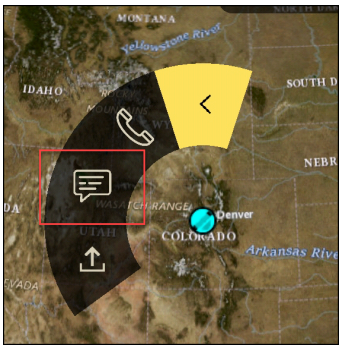
完成下列程序以使用 Pinwheel。

1. 同時開啟 ATAK 映射和 Wickr for ATAK 外掛程式的分割畫面檢視。地圖會在地圖檢視中顯示您的團隊成員或資產。
2. 選擇使用者圖示以開啟腳輪。
3. 選擇 Wickr 圖示，以檢視所選使用者的可用選項。



4. 在齒輪上，選擇下列其中一個圖示：
   - 電話：選擇呼叫。

- 訊息：選擇聊天。



- 檔案傳送：選擇傳送檔案。

ATAK 導覽

外掛程式 UI 包含三個外掛程式檢視，由畫面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。

- 聯絡人檢視：建立直接訊息群組或聊天室對話。
- DMs：建立one-to-one對話。聊天功能的運作方式與 Wickr 原生應用程式相同。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。
- 房間檢視：原生應用程式中的現有房間會移轉。在外掛程式中完成的任何動作都會反映在 Wickr 原生應用程式中。

> **Note**
>
> 某些功能，例如刪除房間，只能在原生應用程式和現場執行，以防止使用者意外修改和現場設備的干擾原因。

允許 Wickr 網路清單的連接埠和網域

允許列出下列連接埠，以確保 Wickr 正常運作：

連接埠

- TCP 連接埠 443（適用於訊息和附件）
- UDP 連接埠 16384-16584（用於呼叫）

要依區域列出之網域和地址

如果您需要允許列出所有可能的呼叫網域和伺服器 IP 地址，請參閱下列依區域列出的潛在 CIDRs 清單。請定期檢查此清單，因為清單可能會有所變更。

> **Note**
>
> 註冊和驗證電子郵件是從 no-reply@amazonaws.com和 傳送donotreply@wickr.email。

美國東部 (維吉尼亞北部)

網域：	• gw-pro-prod.wickr.com • api.messaging.wickr.us-east-1.amazonaws.com • ingress.prod.calling.wickr.com
呼叫 CIDR 地址：	• 44.211.195.0/27 • 44.213.83.32/28
呼叫 IP 地址：	• 44.211.195.0 • 44.211.195.1 • 44.211.195.2 • 44.211.195.3 • 44.211.195.4 • 44.211.195.5

- 44.211.195.6
- 44.211.195.7
- 44.211.195.8
- 44.211.195.9
- 44.211.195.10
- 44.211.195.11
- 44.211.195.12
- 44.211.195.13
- 44.211.195.14
- 44.211.195.15
- 44.211.195.16
- 44.211.195.17
- 44.211.195.18
- 44.211.195.19
- 44.211.195.20
- 44.211.195.21
- 44.211.195.22
- 44.211.195.23
- 44.211.195.24
- 44.211.195.25
- 44.211.195.26
- 44.211.195.27
- 44.211.195.28
- 44.211.195.29
- 44.211.195.30
- 44.211.195.31
- 44.213.83.32
- 44.213.83.33
- 44.213.83.34
- 44.213.83.35

	• 44.213.83.36 • 44.213.83.37 • 44.213.83.38 • 44.213.83.39 • 44.213.83.40 • 44.213.83.41 • 44.213.83.42 • 44.213.83.43 • 44.213.83.44 • 44.213.83.45 • 44.213.83.46 • 44.213.83.47

亞太地區 (馬來西亞)

網域：	• gw-pro-prod.wickr.com • api.messaging.wickr.ap-southeast-5.amazonaws.com • ingress.prod.calling.wickr.ap-southeast-5.amazonaws.com
呼叫 CIDR 地址：	• 43.216.226.160/28
呼叫 IP 地址：	• 43.216.226.160 • 43.216.226.161 • 43.216.226.162 • 43.216.226.163 • 43.216.226.164 • 43.216.226.165 • 43.216.226.166 • 43.216.226.167 • 43.216.226.168

	• 43.216.226.169 • 43.216.226.170 • 43.216.226.171 • 43.216.226.172 • 43.216.226.173 • 43.216.226.174 • 43.216.226.175

亞太地區 (新加坡)

網域：	• gw-pro-prod.wickr.com • api.messaging.wickr.ap-southeast-1.amazonaws.com • ingress.prod.calling.wickr.ap-southeast-1.amazonaws.com
呼叫 CIDR 地址：	• 47.129.23.144/28
呼叫 IP 地址：	• 47.129.23.144 • 47.129.23.145 • 47.129.23.146 • 47.129.23.147 • 47.129.23.148 • 47.129.23.149 • 47.129.23.150 • 47.129.23.151 • 47.129.23.152 • 47.129.23.153 • 47.129.23.154 • 47.129.23.155 • 47.129.23.156 • 47.129.23.157

	• 47.129.23.158 • 47.129.23.159

亞太地區 (悉尼)

網域：	• gw-pro-prod.wickr.com • api.messaging.wickr.ap-southeast-2.amazonaws.com • ingress.prod.calling.wickr.ap-southeast-2.amazonaws.com
呼叫 CIDR 地址：	• 3.27.180.208/28
呼叫 IP 地址：	• 3.27.180.208 • 3.27.180.209 • 3.27.180.210 • 3.27.180.211 • 3.27.180.212 • 3.27.180.213 • 3.27.180.214 • 3.27.180.215 • 3.27.180.216 • 3.27.180.217 • 3.27.180.218 • 3.27.180.219 • 3.27.180.220 • 3.27.180.221 • 3.27.180.222 • 3.27.180.223

亞太地區 (東京)

網域：	• gw-pro-prod.wickr.com • api.messaging.wickr.ap-northeast-1.amazonaws.com • ingress.prod.calling.wickr.ap-northeast-1.amazonaws.com
呼叫 CIDR 地址：	• 57.181.142.240/28
呼叫 IP 地址：	• 57.181.142.240 • 57.181.142.241 • 57.181.142.242 • 57.181.142.243 • 57.181.142.244 • 57.181.142.245 • 57.181.142.246 • 57.181.142.247 • 57.181.142.248 • 57.181.142.249 • 57.181.142.250 • 57.181.142.251 • 57.181.142.252 • 57.181.142.253 • 57.181.142.254 • 57.181.142.255

加拿大 (中部)

網域：	• gw-pro-prod.wickr.com • api.messaging.wickr.ca-central-1.amazonaws.com

	• ingress.prod.calling.wickr.ca-central-1.amazonaws.com
呼叫 CIDR 地址：	• 15.156.152.96/28
呼叫 IP 地址：	• 15.156.152.96 • 15.156.152.97 • 15.156.152.98 • 15.156.152.99 • 15.156.152.100 • 15.156.152.101 • 15.156.152.102 • 15.156.152.103 • 15.156.152.104 • 15.156.152.105 • 15.156.152.106 • 15.156.152.107 • 15.156.152.108 • 15.156.152.109 • 15.156.152.110 • 15.156.152.111

歐洲 (法蘭克福)

網域：	• gw-pro-prod.wickr.com • api.messaging.wickr.eu-central-1.amazonaws.com • ingress.prod.calling.wickr.eu-central-1.amazonaws.com
呼叫 CIDR 地址：	• 3.78.252.32/28
呼叫 IP 地址：	• 3.78.252.32

	• 3.78.252.33 • 3.78.252.34 • 3.78.252.35 • 3.78.252.36 • 3.78.252.37 • 3.78.252.38 • 3.78.252.39 • 3.78.252.40 • 3.78.252.41 • 3.78.252.42 • 3.78.252.43 • 3.78.252.44 • 3.78.252.45 • 3.78.252.46 • 3.78.252.47

訊息 IP 地址：	• 3.163.236.183 • 3.163.238.183 • 3.163.251.183 • 3.163.232.183 • 3.163.241.183 • 3.163.245.183 • 3.163.248.183 • 3.163.234.183 • 3.163.237.183 • 3.163.243.183 • 3.163.247.183 • 3.163.240.183 • 3.163.242.183 • 3.163.244.183 • 3.163.246.183 • 3.163.249.183 • 3.163.252.183 • 3.163.235.183 • 3.163.250.183 • 3.163.239.183 • 3.163.233.183

歐洲 (倫敦)

網域：	• gw-pro-prod.wickr.com • api.messaging.wickr.eu-west-2.amazonaws.com • ingress.prod.calling.wickr.eu-west-2.amazonaws.com
呼叫 CIDR 地址：	• 13.43.91.48/28

呼叫 IP 地址：	• 13.43.91.48 • 13.43.91.49 • 13.43.91.50 • 13.43.91.51 • 13.43.91.52 • 13.43.91.53 • 13.43.91.54 • 13.43.91.55 • 13.43.91.56 • 13.43.91.57 • 13.43.91.58 • 13.43.91.59 • 13.43.91.60 • 13.43.91.61 • 13.43.91.62 • 13.43.91.63

歐洲 (斯德哥爾摩)

網域：	• gw-pro-prod.wickr.com • api.messaging.wickr.eu-north-1.amazonaws.com • ingress.prod.calling.wickr.eu-north-1.amazonaws.com
呼叫 CIDR 地址：	• 13.60.1.64/28
呼叫 IP 地址：	• 13.60.1.64 • 13.60.1.65 • 13.60.1.66 • 13.60.1.67 • 13.60.1.68

	• 13.60.1.69 • 13.60.1.70 • 13.60.1.71 • 13.60.1.72 • 13.60.1.73 • 13.60.1.74 • 13.60.1.75 • 13.60.1.76 • 13.60.1.77 • 13.60.1.78 • 13.60.1.79

歐洲 (蘇黎世)

網域：	• gw-pro-prod.wickr.com • api.messaging.wickr.eu-central-2.amazonaws.com • ingress.prod.calling.wickr.eu-central-2.amazonaws.com
呼叫 CIDR 地址：	• 16.63.106.224/28
呼叫 IP 地址：	• 16.63.106.224 • 16.63.106.225 • 16.63.106.226 • 16.63.106.227 • 16.63.106.228 • 16.63.106.229 • 16.63.106.230 • 16.63.106.231 • 16.63.106.232 • 16.63.106.233

	• 16.63.106.234 • 16.63.106.235 • 16.63.106.236 • 16.63.106.237 • 16.63.106.238 • 16.63.106.239

AWS GovCloud (US-West)

網域：	• gw-pro-prod.wickr.com • api.messaging.wickr.us-gov-west-1.amazonaws.com • ingress-prod-calling.wickr.us-gov-west-1.amazonaws.com • s3.us-gov-west-1.amazonaws.com • s3-fips.us-gov-west-1.amazonaws.com • s3.amazonaws.com • register.wickr.us-gov-west-1.amazonaws.com • admin.wickr.us-gov-west-1.amazonaws.com • admin.messaging.wickr.us-gov-west-1.amazonaws.com • cognito-identity.us-gov-west-1.amazonaws.com • kinesis.us-gov-west-1.amazonaws.com • messaging.wickr.us-gov-west-1.amazonaws.com
呼叫 CIDR 地址：	• 3.30.186.208/28 • 3.31.11.216/29
呼叫 IP 地址：	• 3.30.186.208 • 3.30.186.209

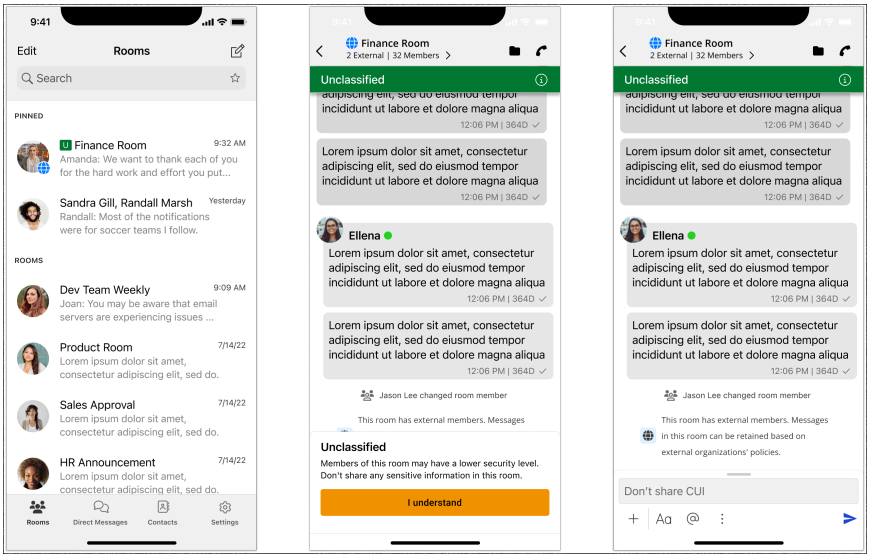
- 3.30.186.210
- 3.30.186.211
- 3.30.186.212
- 3.30.186.213
- 3.30.186.214
- 3.30.186.215
- 3.30.186.216
- 3.30.186.217
- 3.30.186.218
- 3.30.186.219
- 3.30.186.220
- 3.30.186.221
- 3.30.186.222
- 3.30.186.223
- 3.31.11.216
- 3.31.11.217
- 3.31.11.218
- 3.31.11.219
- 3.31.11.220
- 3.31.11.221
- 3.31.11.222
- 3.31.11.223

GovCloud 跨邊界分類和聯合

AWS Wickr 提供專為 GovCloud 使用者量身打造的 WickrGov 用戶端。GovCloud Federation 允許 GovCloud 使用者和商業使用者之間的通訊。跨邊界分類功能可讓 GovCloud 使用者變更對話的使用者介面。身為 GovCloud 使用者，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 (Enterprise、AWS Wickr、訪客使用者） 進行對話時，會顯示下列未分類警告：

- 房間清單中的 U 標籤
- 訊息畫面上的未分類確認

- 對話上方的未分類橫幅



> **Note**
>
> 只有在 GovCloud 使用者與外部使用者進行對話或房間的一部分時，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。GovCloud 使用者之間的對話不會顯示任何警告。

AWS Wickr 的檔案預覽

使用 Wickr Premium 方案（包括 Premium 免費試用版）的組織現在可以在安全群組層級管理檔案下載許可。

在安全群組中預設會啟用檔案下載。管理員可以透過管理員面板啟用或停用檔案下載。此設定會套用至整個 Wickr 網路。

若要啟用或停用檔案下載，請完成下列程序。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇安全群組。
4. 選取您要編輯的安全群組名稱。

   安全群組詳細資訊頁面會在不同的標籤中顯示安全群組的設定。

5. 在傳訊索引標籤下方的媒體和連結區段中，選擇編輯。
6. 在編輯媒體和連結頁面上，勾選或取消勾選檔案下載選項。
7. 選擇儲存變更。

為安全群組啟用檔案下載時，使用者可以下載直接訊息和聊天室中共用的檔案。如果已停用下載，則只能預覽這些檔案並上傳至檔案索引標籤，但無法下載它們。使用者也會受到擷取螢幕擷取畫面的限制；嘗試會導致黑色畫面。

> **Note**
>
> 停用檔案下載時，該安全群組中的所有使用者都需要使用 Wickr 6.54 版及更高版本，才能套用此檔案設定。

> **Note**
>
> 在來自不同網路（由於聯合）和安全群組的使用者存在的房間中，每個使用者預覽或下載檔案的能力取決於其特定的安全群組設定。因此，有些使用者可以下載房間中的檔案，有些則只能預覽檔案。

AWS Wickr 的同意快顯視窗

您可以設定網路的同意快顯視窗，在使用者登入 Wickr 時向他們顯示條款、政策或組織要求。使用者必須先確認快顯視窗，才能存取應用程式。當使用者登出並重新登入，或當快顯內容更新時，快顯會再次顯示。

若要啟用同意快顯視窗，請完成下列程序。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇網路政策。
4. 在網路政策頁面的同意快顯區段中，選擇編輯。
5. 在編輯同意快顯頁面的同意快顯區段中，開啟已啟用。
6. 完成下列欄位：

- 標題 — 輸入顯示在同意快顯視窗頂端的標題。使用 標頭提供呈現給使用者的資訊或動作摘要。
- 內文內容 — 輸入在同意快顯視窗中顯示的主要訊息。使用內文內容來傳達使用者在存取應用程式之前必須檢閱的條款、政策、組織要求或其他資訊。
- 關閉按鈕標籤（選用）— 輸入使用者選擇以確認和關閉同意快顯視窗的按鈕上顯示的文字。例如，您可以使用確認、接受或繼續。

7. 若要預覽同意快顯視窗，請選擇右上角的預覽。在預覽之後，選擇關閉預覽。
8. 選擇儲存變更。

在 AWS Wickr 中管理使用者

在 AWS 管理主控台 for Wickr 的使用者管理區段中，您可以檢視目前的 Wickr 使用者和機器人，並修改其詳細資訊。

主題

AWS Wickr 網路中的團隊目錄

您可以在 AWS 管理主控台 for Wickr 的使用者管理區段中檢視目前的 Wickr 使用者並修改其詳細資訊。

主題

檢視 AWS Wickr 網路中的使用者

您可以檢視已註冊至 Wickr 網路之使用者的詳細資訊。

完成下列程序，以檢視已註冊至 Wickr 網路的使用者。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台 for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇使用者管理。

   團隊目錄索引標籤會顯示已註冊至 Wickr 網路的使用者，包括其名稱、電子郵件地址、指派的安全群組和目前狀態。對於目前使用者，您可以檢視其裝置、編輯其詳細資訊、暫停、刪除和切換到另一個 Wickr 網路。

邀請 AWS Wickr 網路中的使用者

您可以在 Wickr 網路中邀請使用者。

完成下列程序，邀請 Wickr 網路中的使用者。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台 for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇使用者管理。
4. 在團隊目錄索引標籤中，選擇邀請使用者。
5. 在邀請使用者頁面上，輸入使用者的電子郵件地址和安全群組。電子郵件地址和安全群組是唯一需要的欄位。請務必為使用者選擇適當的安全群組。Wickr 會將邀請電子郵件傳送至您為使用者指定的地址。
6. 選擇邀請使用者。

   系統會傳送電子郵件給使用者。此電子郵件提供 Wickr 用戶端應用程式的下載連結，以及註冊 Wickr 的連結。當使用者使用電子郵件中的連結註冊 Wickr 時，他們在 Wickr 團隊目錄中的狀態將從待定變更為作用中。

編輯 AWS Wickr 網路中的使用者

您可以在 Wickr 網路中編輯使用者。

完成下列程序以編輯使用者。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台 for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇使用者管理。
4. 在團隊目錄索引標籤中，選取您要編輯之使用者的垂直省略符號（三個點）圖示。
5. 選擇編輯。
6. 編輯使用者資訊，然後選擇儲存變更。

在 AWS Wickr 網路中刪除使用者

您可以刪除 Wickr 網路中的使用者。

完成下列程序以刪除使用者。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台 for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇使用者管理。
4. 在團隊目錄索引標籤中，選取您要刪除之使用者的垂直省略符號（三個點）圖示。
5. 選擇刪除以刪除使用者。

   當您刪除使用者時，該使用者將無法再登入 Wickr 用戶端中的 Wickr 網路。
6. 在快顯視窗中，選擇刪除。

大量刪除 AWS Wickr 網路中的使用者

您可以在 AWS 管理主控台 for Wickr 的使用者管理區段中大量刪除 Wickr 網路使用者。

> **Note**
>
> 大量刪除使用者的 選項僅適用於未啟用 SSO 的情況。

若要使用 CSV 範本大量刪除 Wickr 網路使用者，請完成下列程序。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台 for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇使用者管理。
4. 團隊目錄索引標籤會顯示已註冊至 Wickr 網路的使用者。
5. 在團隊目錄索引標籤中，選擇管理使用者，然後選擇大量刪除。
6. 在大量刪除使用者頁面上，下載範例 CSV 範本。若要下載範例範本，請選擇下載範本。
7. 新增您要從網路大量刪除之使用者的電子郵件，以完成範本。
8. 上傳完成的 CSV 範本。您可以將檔案拖放到上傳方塊中，或選取選擇檔案。
9. 選取核取方塊，我了解刪除使用者無法還原。
10. 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。已刪除的使用者將無法再登入 Wickr 用戶端中的 Wickr 網路。

若要下載團隊目錄的 CSV 來大量刪除 Wickr 網路使用者，請完成下列程序。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台 for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇使用者管理。
4. 團隊目錄索引標籤會顯示已註冊至 Wickr 網路的使用者。
5. 在團隊目錄索引標籤中，選擇管理使用者，然後選擇下載為 CSV。
6. 下載團隊目錄 CSV 範本之後，請移除不需要刪除的使用者資料列。
7. 在團隊目錄索引標籤中，選擇管理使用者，然後選擇大量刪除。
8. 在大量刪除使用者頁面上，上傳團隊目錄 CSV 範本。您可以將檔案拖放到上傳方塊中，或選取選擇檔案。
9. 選取核取方塊，我了解刪除使用者無法還原。
10. 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。已刪除的使用者將無法再登入 Wickr 用戶端中的 Wickr 網路。

大量暫停 AWS Wickr 網路中的使用者

您可以在 AWS 管理主控台 for Wickr 的使用者管理區段中大量暫停 Wickr 網路使用者。

> **Note**
>
> 大量暫停使用者的 選項僅適用於未啟用 SSO 的情況。

若要大量暫停 Wickr 網路使用者，請完成下列程序。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台 for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇使用者管理。
4. 團隊目錄索引標籤會顯示已註冊至 Wickr 網路的使用者。
5. 在團隊目錄索引標籤中，選擇管理使用者，然後選擇大量暫停。
6. 在大量暫停使用者頁面上，下載範例 CSV 範本。若要下載範例範本，請選擇下載範本。
7. 新增您要從網路大量暫停的使用者電子郵件，以完成範本。
8. 上傳完成的 CSV 範本。您可以將檔案拖放到上傳方塊中，或選取選擇檔案。
9. 選擇暫停使用者。

> **Note**
>
> 此動作會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。

AWS Wickr 網路中的訪客使用者

Wickr 訪客使用者功能允許個別訪客使用者登入 Wickr 用戶端，並與 Wickr 網路使用者協作。Wickr 管理員可以啟用或停用其 Wickr 網路的訪客使用者。

啟用此功能後，邀請到您的 Wickr 網路的訪客使用者可以與 Wickr 網路中的使用者互動。 AWS 帳戶訪客使用者功能的費用會套用至您的 。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

- 在 AWS Wickr 網路中啟用或停用訪客使用者
- 在 AWS Wickr 網路中檢視訪客使用者計數
- 檢視 AWS Wickr 網路中的每月用量
- 在 AWS Wickr 網路中檢視訪客使用者
- 在 AWS Wickr 網路中封鎖訪客使用者

在 AWS Wickr 網路中啟用或停用訪客使用者

您可以在 Wickr 網路中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. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台 for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇安全群組。
4. 選取特定安全群組的名稱。

> **Note**
>
> 您只能為個別安全群組啟用訪客使用者。若要為 Wickr 網路中的所有安全群組啟用訪客使用者，您必須為網路中的每個安全群組啟用 功能。

5. 選擇安全群組中的聯合標籤。
6. 有兩個位置提供啟用訪客使用者的選項：
   - 本機聯合 — 對於美國東部（維吉尼亞北部）的網路，請在頁面的本機聯合區段中選擇編輯。
   - 全域聯合 — 對於其他區域中的所有其他網路，請在頁面的全域聯合區段中選擇編輯。
7. 在編輯聯合頁面上，選取啟用聯合。
8. 選擇儲存變更以儲存變更，並使其對安全群組有效。

   您 Wickr 網路中特定安全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》中的訪客使用者。

在 AWS Wickr 網路中檢視訪客使用者計數

您可以在 Wickr 網路中檢視訪客使用者計數。

完成下列程序，以檢視 Wickr 網路的訪客使用者計數。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台 for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇使用者管理。

   使用者管理頁面會顯示 Wickr 網路中的訪客使用者計數。

檢視 AWS Wickr 網路中的每月用量

您可以檢視網路在計費期間與之通訊的訪客使用者數量。

完成下列程序，以檢視 Wickr 網路的每月用量。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台 for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇使用者管理。
4. 選取訪客使用者索引標籤。

   訪客使用者索引標籤會顯示訪客使用者每月用量。

   > **Note**
   >
   > 訪客帳單資料每 24 小時更新一次。

在 AWS Wickr 網路中檢視訪客使用者

您可以檢視網路使用者在特定計費期間與之通訊的訪客使用者。

完成下列程序，以檢視在特定計費期間與網路使用者通訊的訪客使用者。

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台 for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇使用者管理。
4. 選取訪客使用者索引標籤。

   訪客使用者索引標籤會顯示您網路中的訪客使用者。

在 AWS Wickr 網路中封鎖訪客使用者

您可以在 Wickr 網路中封鎖和解除封鎖訪客使用者。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. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台 for Wickr。

2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇使用者管理。
4. 選取訪客使用者索引標籤。

   訪客使用者索引標籤會顯示您網路中的訪客使用者。
5. 在訪客使用者區段中，尋找您要封鎖的訪客使用者電子郵件。
6. 在訪客使用者名稱的右側，選取三個點，然後選擇封鎖訪客使用者。
7. 在快顯視窗上選擇封鎖。
8. 若要檢視 Wickr 網路中封鎖的使用者清單，請選取狀態下拉式功能表，然後選取封鎖。

解除封鎖訪客使用者

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台 for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 在導覽窗格中，選擇使用者管理。
4. 選取訪客使用者索引標籤。

   訪客使用者索引標籤會顯示您網路中的訪客使用者。
5. 選取狀態下拉式功能表，然後選取封鎖。
6. 在封鎖區段中，尋找您要解除封鎖之訪客使用者的電子郵件。
7. 在訪客使用者名稱的右側，選取三個點，然後選擇解除封鎖使用者。
8. 在快顯視窗上選擇解除封鎖。

AWS Wickr 的安全性

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

安全性是 AWS與您之間的共同責任。共同責任模式將其描述為雲端的安全性，和雲端中的安全性：

- 雲端的安全性 – AWS負責保護在 中執行 AWS服務的基礎設施AWS 雲端。 AWS也為您提供可安全使用的服務。在AWS合規計畫中，第三方稽核人員會定期測試和驗證我們安全的有效性。若要了解適用於 AWS Wickr 的合規計劃，請參閱AWS合規計劃的 服務範圍。
- 雲端的安全性 – 您的責任取決於您使用AWS的服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

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

主題

AWS Wickr 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 的全域基礎設施AWS 雲端。您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。 如需歐洲資料保護的詳細資訊，請參閱一般資料保護規則 (GDPR) 中心。

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

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS資源通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用 設定 API 和使用者活動記錄AWS CloudTrail。如需有關使用 CloudTrail 追蹤擷取AWS活動的資訊，請參閱AWS CloudTrail《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用AWS加密解決方案，以及其中的所有預設安全控制AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果您在AWS透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-3。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用 Wickr 或使用主控台、API AWS CLI或 AWSSDKs的其他AWS 服務 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 Wickr 的身分和存取管理

AWS Identity and Access Management(IAM) 是 AWS 服務，可協助管理員安全地控制對 AWS資源的存取。IAM 管理員可控制誰可以進行身分驗證 （ 登入 ） 和授權 （ 具有許可 ），以使用 Wickr 資源。IAM 是您可以免費使用AWS 服務的 。

主題

AWS Wickr 對象

使用方式 AWS Identity and Access Management(IAM) 會根據您的角色而有所不同：

- 服務使用者 — 若無法存取某些功能，請向管理員申請所需許可 (請參閱 故障診斷 AWS Wickr 身分和存取)
- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 AWS Wickr 如何與 IAM 搭配使用)
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 AWS Wickr 的身分型政策範例)

使用 AWS Wickr 的身分進行身分驗證

身分驗證是您AWS使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者、IAM 使用者或擔任 IAM 角色身分進行身分驗證。

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center(IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的如何登入您的 AWS 帳戶。

對於程式設計存取， AWS提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的 API 請求的 AWS 第 4 版簽署程序。

AWS 帳戶根使用者

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，該身分具有對所有 AWS 服務和 資源的完整存取權。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。

聯合身分

最佳實務是要求人類使用者使用聯合身分提供者，以AWS 服務使用臨時憑證存取 。

聯合身分是您企業目錄、Web 身分提供者的使用者，或使用來自身分來源的AWS 服務憑證存取 Directory Service。聯合身分會擔任角色，而該角色會提供臨時憑證。

若需集中化管理存取權限，建議使用 AWS IAM Identity Center。如需詳細資訊，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https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的要求人類使用者使用聯合身分提供者來AWS使用臨時憑證存取 。

IAM 群組會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html的身分具有特定許可權，其可以提供臨時憑證。您可以透過從使用者切換到 IAM 角色 （主控台） 或呼叫 AWS CLI或 AWSAPI 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

使用 AWS Wickr 的政策管理存取權

您可以透過建立政策並將其連接到身分或資源AWS來控制 AWS中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時AWS， 會評估這些政策。大多數政策會以 JSON 文件AWS的形式存放在 中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的 JSON 政策概觀。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的在受管政策與內嵌政策之間選擇。

資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 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。您必須在資源型政策中指定主體。

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

存取控制清單 (ACL)

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

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

其他政策類型

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

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

多種政策類型

當多種類型的政策適用於請求時，產生的許可會更複雜而無法理解。若要了解如何AWS在涉及多種政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

AWSAWS Wickr 的 受管政策

若要新增許可給使用者、群組和角色，使用 AWS受管政策比自行撰寫政策更容易。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受管政策。您無法變更 AWS受管政策中的許可。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受管政策移除許可，因此政策更新不會破壞您現有的許可。

AWS受管政策：AWSWickrFullAccess

您可將 `AWSWickrFullAccess` 政策連接到 IAM 身分。此政策會將完整的管理許可授予 Wickr 服務，包括 中的 AWS 管理主控台for WickrAWS 管理主控台。如需將政策連接至身分的詳細資訊，請參閱AWS Identity and Access Management《 使用者指南》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 服務完整的管理許可。

JSON

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

AWS受管政策的 Wickr 更新

檢視自此服務開始追蹤這些變更以來，Wickr 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 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 新增了新的政策，將完整的管理許可授予 Wickr 服務，包括 中的 Wickr 管理員主控台AWS 管理主控台。	2022 年 11 月 28 日
Wickr 開始追蹤變更	Wickr 開始追蹤其AWS受管政策的變更。	2022 年 11 月 28 日

AWS Wickr 如何與 IAM 搭配使用

在您使用 IAM 管理 Wickr 的存取權之前，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	Wickr 支援
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

若要全面了解 Wickr 和其他 AWS服務如何與大多數 IAM 功能搭配使用，請參閱《IAM 使用者指南》中的AWS與 IAM 搭配使用的 服務。

Wickr 的身分型政策

支援身分型政策：是

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。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 的身分型政策範例

若要檢視 Wickr 身分型政策的範例，請參閱 AWS Wickr 的身分型政策範例。

Wickr 中的資源型政策

支援資源型政策：否

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

如需啟用跨帳戶存取權，您可以在其他帳戶內指定所有帳戶或 IAM 實體作為資源型政策的主體。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

Wickr 的政策動作

支援政策動作：是

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

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。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字首：

```
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 身分型政策的範例，請參閱 AWS Wickr 的身分型政策範例。

Wickr 的政策資源

支援政策資源：否

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

`Resource` JSON 政策元素可指定要套用動作的物件。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

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

若要查看 Wickr 資源類型及其 ARNs的清單，請參閱服務授權參考中的 AWS Wickr 定義的資源。若要了解您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 身分型政策的範例，請參閱 AWS Wickr 的身分型政策範例。

Wickr 的政策條件索引鍵

支援服務特定政策條件金鑰：否

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

Condition 元素會根據定義的條件，指定陳述式的執行時機。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。若要查看所有AWS全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS全域條件內容索引鍵。

若要查看 Wickr 條件金鑰清單，請參閱服務授權參考中的 AWS Wickr 的條件金鑰。若要了解您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 身分型政策的範例，請參閱 AWS Wickr 的身分型政策範例。

Wickr ACLs

支援 ACL：否

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

ABAC 搭配 Wickr

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，依據稱為標籤的屬性來定義許可。您可以將標籤連接至 IAM 實體AWS和資源，然後設計 ABAC 政策，以便在委託人的標籤符合資源上的標籤時允許操作。

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

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

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的使用 ABAC 授權定義許可。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的使用屬性型存取控制 (ABAC)。

搭配 Wickr 使用臨時登入資料

支援臨時登入資料：否

臨時登入資料提供對 AWS資源的短期存取，並在您使用聯合或切換角色時自動建立。AWS建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的臨時安全憑證與可與 IAM 搭配運作的 AWS 服務。

Wickr 的跨服務主體許可

支援轉寄存取工作階段 (FAS)：否

轉送存取工作階段 (FAS) 使用呼叫 的委託人許可AWS 服務，結合 AWS 服務請求向下游服務提出請求。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。

Wickr 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。

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

Wickr 的服務連結角色

支援服務連結角色：否

服務連結角色是連結至 的一種服務角色AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中AWS 帳戶，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理服務連結角色的詳細資訊，請參閱可搭配 IAM 運作的 AWS 服務。在資料表中尋找服務，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 的身分型政策範例

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 服務的許可。以下顯示許可政策範例。

JSON

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

```
            "Effect": "Allow",
            "Action": [
                "wickr:CreateAdminSession",
                "wickr:ListNetworks"
            ],
            "Resource": "*"
        }
    ]
}
```

此範例政策提供使用者使用 AWS 管理主控台for Wickr 列出 Wickr 網路的許可。若要進一步了解 IAM 政策陳述式中的元素，請參閱 Wickr 的身分型政策。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。

您也可以建立 IAM 政策，以允許使用者存取特定 API 動作。對 API 動作的存取會與 AWS Wickr 主控台分開管理。以下是授予特定 API 動作唯讀存取權的政策範例。如需 API 動作的詳細資訊，請參閱歡迎使用 AWS Wickr API 參考。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "WickrAPIReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "wickr:ListNetworks",
                "wickr:ListUsers",
                "wickr:GetNetworkSettings",
                "wickr:GetNetwork",
                "wickr:GetUser",
                "wickr:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

主題

- 政策最佳實務
- 使用 AWS 管理主控台for Wickr

- 允許使用者檢視他們自己的許可

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、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受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS受管政策。它們可在您的 中使用AWS 帳戶。我們建議您定義特定於使用案例AWS的客戶受管政策，以進一步減少許可。如需更多資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策或任務職能的 AWS 受管政策。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱《IAM 使用者指南》中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。如果透過特定 等使用服務動作AWS服務，您也可以使用條件來授予其存取權CloudFormation。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的透過 MFA 的安全 API 存取。

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

使用 AWS 管理主控台for Wickr

將 `AWSWickrFullAccess`AWS受管政策連接至您的 IAM 身分，以授予他們 Wickr 服務的完整管理許可，包括 中的 Wickr 管理員主控台AWS 管理主控台。如需詳細資訊，請參閱AWS受管政策：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。此政策包含在主控台或使用 或 AWS CLIAWSAPI 以程式設計方式完成此動作的許可。

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

故障診斷 AWS Wickr 身分和存取

如需診斷和修正 IAM 常見問題的說明，請參閱AWS Identity and Access Management《 使用者指南》中的疑難排解 IAM。

法規遵循驗證

如需特定合規計劃範圍內AWS的服務清單，請參閱AWS合規計劃範圍內的服務。如需一般資訊，請參閱 AWSCompliance Programs。

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

您使用 Wickr 時的合規責任取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。AWS 提供下列資源來協助合規：

- 安全與合規快速入門指南 – 這些部署指南討論架構考量，並提供部署以安全與合規為中心之基準環境的步驟AWS。
- AWS 合規資源 – 此工作手冊和指南集合可能適用於您的產業和位置。
- 《 AWS Config開發人員指南》中的使用規則評估資源AWS Config；評估資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub CSPM – AWS此服務提供 內安全狀態的完整檢視AWS，協助您檢查是否符合安全產業標準和最佳實務。

AWS Wickr 中的彈性

AWS全球基礎設施是以 AWS 區域和 可用區域為基礎建置。 AWS 區域提供多個實體隔離和隔離的可用區域，這些可用區域與低延遲、高輸送量和高備援聯網連接。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全球基礎設施。

除了 AWS全球基礎設施之外，Wickr 還提供數種功能，以協助支援您的資料彈性和備份需求。如需詳細資訊，請參閱AWS Wickr 的資料保留。

AWS PrivateLink適用於 AWS Wickr

使用 AWS PrivateLinkfor AWS Wickr，您可以使用界面 VPC 端點，在虛擬私有雲端 (VPC) 與 AWS Wickr 中的端點子集之間建立私有連線。介面 VPC 端點採用一種AWS技術AWS PrivateLink，可讓您AWS使用私有 IP 地址存取在 上執行的服務。

對於行動用戶端或其他內部部署裝置，請使用 VPN 將您的裝置連線至 VPC，以進行端對端私有連線。如需詳細資訊，請參閱 AWS Virtual Private Network 文件。

如需 AWS PrivateLink和 AWSVPC 的詳細資訊，請參閱什麼是AWS PrivateLink？ AWS PrivateLink指南中的 和什麼是 AWSVPC？ Amazon Virtual Private Cloud 使用者指南中的 。

支援的 AWS Wickr 服務

下列 AWS Wickr 服務支援AWS PrivateLink：

服務	端點格式	
AWS Wickr 管理員	`com.amazonaws.` *`your-region`* `.wickr-admin`	
AWS Wickr 訊息	`com.amazonaws.` *`your-region`* `.wickr-messaging`	
AWS Wickr 呼叫	`com.amazonaws.` *`your-region`* `.wickr-calling`	

所有 Wickr VPC 端點目前都需要啟用私有 DNS 名稱。如需詳細資訊，請參閱啟用私有 DNS 名稱。

Wickr VPC 端點在公有 Wickr 端點支援 FIPS 的區域支援 FIPS。如需詳細資訊，請參閱聯邦資訊處理標準。

目前不支援

- 訊息傳送和呼叫端點的 VPC 端點政策
- 訊息傳送和呼叫端點無法在 中使用`us-east-1`。

主題

先決條件

建立 VPC 端點之前，請確定您有下列先決條件：

1. VPC 組態：在多個可用區域中具有子網路的正確設定 VPC
2. 安全群組：允許 HTTPS 流量的適當安全群組 （連接埠 443)
3. DNS 解析：VPC 中啟用的 DNS 主機名稱和 DNS 解析
4. IAM 許可：建立和管理 VPC 端點的必要許可

建立 VPC 端點

您可以為 AWS Wickr Admin、Message 和 Calling 建立 VPC 端點。

完成下列程序，以使用AWS主控台建立 VPC 端點。

步驟 1：導覽至 VPC 主控台

1. 登入 Amazon VPC 主控台。
2. 在左側導覽窗格中選擇 Endpoints (端點)。
3. 選擇建立端點。

步驟 2：設定端點設定

1. 在服務類別下，選取AWS服務。
2. 在服務名稱下，搜尋`wickr`並選擇適當的服務：
    - 對於管理員： `com.amazonaws.`*`your-region`*`.wickr-admin`
    - 對於簡訊： `com.amazonaws.`*`your-region`*`.wickr-messaging`
    - 對於呼叫： `com.amazonaws.`*`your-region`*`.wickr-calling`

步驟 3：網路組態

1. 在 VPC 下，選取您的目標 VPC。
2. 在子網路下，選擇多個可用區域中的子網路以獲得高可用性。
3. 在啟用私有 DNS 名稱下，選取核取方塊。這可讓 支援私有 DNS 名稱。
4. 在安全群組下，選取或建立您要與端點網路介面建立關聯的安全群組。

步驟 4：建立端點

1. 檢閱您的組態。
2. 您可以選擇性地新增或移除標籤。標籤是您用來與端點建立關聯的名稱值對。
3. 選擇建立端點。

完成下列程序，以使用 建立 VPC 端點AWS CLI。

1. 檢查您區域中的服務可用性：

   檢查 Wickr Admin 可用性

   ```
   aws ec2 describe-vpc-endpoint-services --service-names com.amazonaws.your-region.wickr-admin
   ```

   檢查 Wickr Messaging 可用性

   ```
   aws ec2 describe-vpc-endpoint-services --service-names com.amazonaws.your-region.wickr-messaging
   ```

   檢查 Wickr 呼叫可用性

   ```
   aws ec2 describe-vpc-endpoint-services --service-names com.amazonaws.your-region.wickr-calling
   ```

2. 建立 VPC 端點。

   Wickr 管理員端點：

   ```
   aws ec2 create-vpc-endpoint \
     --vpc-endpoint-type Interface \
     --service-name com.amazonaws.your-region.wickr-admin \
     --subnet-ids subnet-12345678 subnet-87654321 subnet-11223344 \
   ```

```
  --vpc-id vpc-12345678 \
  --security-group-ids sg-12345678 \
  --private-dns-enabled \
```

Wickr 訊息端點

```
aws ec2 create-vpc-endpoint \
  --vpc-endpoint-type Interface \
  --service-name com.amazonaws.your-region.wickr-messaging \
  --subnet-ids subnet-12345678 subnet-87654321 subnet-11223344 \
  --vpc-id vpc-12345678 \
  --security-group-ids sg-12345678 \
  --private-dns-enabled \
```

Wickr 呼叫端點

```
aws ec2 create-vpc-endpoint \
  --vpc-endpoint-type Interface \
  --service-name com.amazonaws.your-region.wickr-calling \
  --subnet-ids subnet-12345678 subnet-87654321 subnet-11223344 \
  --vpc-id vpc-12345678 \
  --security-group-ids sg-12345678 \
  --private-dns-enabled \
```

限制

透過 不支援下列功能AWS PrivateLink，且需要網際網路連線：

- Wickr 開放存取 (WOA)
- 用戶端應用程式更新
  - 行動應用程式 (iOS/Android)
    - 來源：App Store/Google Play Store
    - 要求：需要網際網路存取
  - 桌面應用程式
    - Windows/Mac：使用全域 S3 端點 (AWS PrivateLink不相容）

    - Linux：使用 Snap Store （需要網際網路存取）
- 除錯和遙測
    - 損毀報告
    - 偵錯指標
    - 用戶端分析連結
- 行動推播通知

  這些服務需要網際網路連線，且無法使用 AWS PrivateLink：

    - Apple 推播通知
        - 要求：直接網際網路存取
        - 連接埠：443、2195、2196、5223
        - 參考：Apple 支援文件
    - Google/Android 通知
        - 要求：Firebase Cloud Messaging 存取
        - 參考：Firebase 文件
- 私有存取目前不支援 AWS Wickr 主控台。如需詳細資訊，請參閱 Private Access 支援的 AWS 區域服務主控台和功能。

的最低必要用戶端版本AWS PrivateLink

下列用戶端版本已使用 驗證AWS PrivateLink：

- iOS 6.64 （如適用）
- Android 6.60 （如適用）
- 桌面用戶端 6.60
- 機器人 6.60

需要額外組態的功能

Wickr 機器人

- 需求：客戶受管基礎設施
- 動作：設定機器人相依性的網路路徑
- 考量：確保機器人可以透過 VPC 端點存取所需的AWS服務

檔案下載

- S3 連線：檔案操作的必要項目 （ 法蘭克福區域除外 ）
- 解決方案：建立 S3 VPC 閘道端點
- 參考：AWS PrivateLink適用於 Amazon S3

AWS Wickr 中的基礎設施安全

作為受管服務，AWS Wickr 受到 Amazon Web Services：安全程序概觀白皮書中所述的 AWS全球網路安全程序的保護。

AWS Wickr 中的組態和漏洞分析

組態和 IT 控制是客戶AWS與您之間的共同責任。如需詳細資訊，請參閱AWS共同的責任模型。

您有責任根據規格和指導方針設定 Wickr、定期指示使用者下載最新版本的 Wickr 用戶端、確保您執行的是最新版本的 Wickr 資料保留機器人，以及監控使用者使用的 Wickr。

AWS Wickr 的安全最佳實務

Wickr 提供許多安全功能，供您在開發和實作自己的安全政策時考慮。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。

若要防止與您使用 Wickr 相關的潛在安全事件，請遵循下列最佳實務：

- 實作最低權限存取，並建立要用於 Wickr 動作的特定角色。使用 IAM 範本建立角色。如需詳細資訊，請參閱AWSAWS Wickr 的 受管政策。
- 透過驗證AWS 管理主控台第一個 來存取 AWS 管理主控台for Wickr。請勿共用您的個人主控台登入資料。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 Wickr

監控是維護 AWS Wickr 和其他 AWS 解決方案可靠性、可用性和效能的重要部分。 AWS 提供下列監控工具來監看 Wickr、在發生錯誤時回報，並適時採取自動動作：

- AWS CloudTrail 會擷取您 AWS 帳戶或代表您的帳戶發出的 API 呼叫和相關事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。您可以識別呼叫的使用者和帳戶 AWS、進行呼叫的來源 IP 地址，以及呼叫的時間。如需詳細資訊，請參閱「AWS CloudTrail 使用者指南」。如需使用 CloudTrail 記錄 Wickr API 呼叫的詳細資訊，請參閱 使用 記錄 AWS Wickr API 呼叫 AWS CloudTrail。

使用 記錄 AWS Wickr API 呼叫 AWS CloudTrail

AWS Wickr 已與 整合 AWS CloudTrail，此服務提供由使用者、角色或 Wickr 中 AWS 服務所採取之動作的記錄。CloudTrail 會將 Wickr 的所有 API 呼叫擷取為事件。擷取的呼叫包括來自 Wickr AWS 管理主控台 的 呼叫，以及對 Wickr API 操作的程式碼呼叫。如果您建立線索，則可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 Wickr 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。您可以使用 CloudTrail 所收集的資訊，判斷向 Wickr 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。若要進一步了解 CloudTrail，請參閱「AWS CloudTrail 使用者指南」。

CloudTrail 中的 Wickr 資訊

當您建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。當活動在 Wickr 中發生時，該活動會與事件歷史記錄中的其他服務 AWS 事件一起記錄在 CloudTrail 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 事件歷史記錄檢視事件」。

若要持續記錄 中的事件 AWS 帳戶，包括 Wickr 的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案傳送到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案和接收多個帳戶的 CloudTrail 日誌檔案

CloudTrail 會記錄所有 Wickr 動作。例如，對 `CreateAdminSession` 和 `ListNetworks` 動作發出的呼叫會在 CloudTrail 日誌檔案中產生項目。

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

- 是否使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出請求。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

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

了解 Wickr 日誌檔案項目

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

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

```
{
    "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"
}
```

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

```
{
    "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"
}
```

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

```
{
    "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"
}
```

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

```
{
    "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"
}
```


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


```
{
    "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"
}
```


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


```
{
    "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"
}
```

AWS Wickr 中的分析儀表板

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

存取分析儀表板

1. 在 https：//https://console.aws.amazon.com/wickr/ 開啟 AWS 管理主控台 for Wickr。
2. 在網路頁面上，選取要導覽至該網路的網路名稱。
3. 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。

在分析頁面上，您會在每個索引標籤的右上角找到時間範圍篩選條件。此篩選條件適用於整個頁面。此外，在每個索引標籤的右上角，您可以選擇可用的匯出選項，以匯出所選時間範圍的資料點。

> **Note**
>
> 選取的時間以 UTC （國際標準時間） 表示。

下列索引標籤可供使用：

- 概觀顯示：
  - 已註冊 — 已註冊使用者總數，包括所選時間內網路上的作用中和暫停使用者。它不包括待定或受邀的使用者。
  - 待處理 — 在所選時間內網路上的待處理使用者總數。
  - 使用者註冊 — 圖形會顯示所選時間範圍中註冊的使用者總數。
  - 裝置 — 應用程式已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量。

- 成員會顯示：
  - 狀態 — 在所選期間內網路上的作用中使用者。
  - 作用中使用者 —
    - 圖形會顯示作用中使用者隨時間的計數，並可依每日、每週或每月 （在上述選取的時間範圍內） 彙總。

- 作用中的使用者計數可以依平台、用戶端版本或安全群組細分。如果刪除安全群組，總數會顯示為 Deleted#。

- 訊息隨即顯示：
  - 已傳送的訊息 — 在所選期間內，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數量。
  - 檔案 — 網路中使用者傳送的檔案數量（包括語音備註）。
  - 裝置 — 圓餅圖會顯示依作業系統分類的作用中裝置數量。
  - 用戶端版本 — 依用戶端版本分類的作用中裝置數量。

對 AWS Wickr 的問題進行故障診斷

下列程序和秘訣可協助您針對 AWS Wickr 的問題進行疑難排解。

如果您無法使用本指南中的步驟解決問題，請在 AWS Support Center 中開啟支援案例。

主題

故障診斷 AWS Wickr 的一般問題

下列疑難排解秘訣可協助您解決 AWS Wickr 的一般問題。如果本節中的步驟無法解決您的問題，請在AWS 支援中心開啟案例。

主題

開始之前

在故障診斷之前，請先驗證下列項目：

- 您正在為組織使用正確的 Wickr 產品：AWS Wickr、AWS WickrGov (GovCloud) 或 Wickr Enterprise（自我託管）。如果您不確定，請聯絡您的網路管理員。
- 您正在執行支援的用戶端版本。AWS Wickr 支援目前版本和先前的 2-3 版本。若要檢查您的版本，請開啟 Wickr，然後選擇設定、關於。若要更新，請參閱檢查更新。
- 您的組織有正確的身分驗證方法 (SSO 或非 SSO)。
- 您已將使用者密碼和 Wickr 復原金鑰儲存在安全的位置。

- 您的網路允許與必要的 Wickr 網域和連接埠進行通訊。
- 您的裝置符合系統需求。

收集診斷資訊

用戶端日誌

用戶端日誌對於疑難排解大多數 AWS Wickr 問題至關重要。

完成下列程序以收集用戶端日誌。

1. 登入 Wickr 用戶端。
2. 在導覽窗格中，選擇選單（三行或點），然後選擇支援。
3. 選擇支援記錄。
4. 選擇儲存日誌。
5. 請注意儲存日誌的位置。

依平台的日誌位置：

- Windows: `C:\Users\<USERNAME>\AppData\Local\Wickr, LLC\Wickr Pro\logs\`
- macOS：`~/Library/Application Support/Wickr, LLC/Wickr Pro/logs/`
- Linux: `~/.local/share/Wickr, LLC/Wickr Pro/logs/`
- iOS：透過支援記錄功能表匯出
- Android：透過支援記錄功能表匯出

要收集的資訊

疑難排解或聯絡支援時，請收集：

- 裝置資訊：模型、作業系統版本
- 用戶端版本：在關於下的設定中找到
- 網路 ID：在網路設定下的管理員主控台中找到
- 錯誤訊息：確切的文字或螢幕擷取畫面
- 時間戳記：問題發生的時間

- 重製步驟：如何重新建立問題
- 用戶端日誌：從支援記錄功能表

常見錯誤訊息

無法連線至 Wickr 伺服器。

可能原因：

- 網路連線問題
- 防火牆封鎖 Wickr 流量
- VPN 或代理干擾

解決方案

1. 測試行動數據與公司 WiFi 以隔離網路問題。
2. 檢閱網路需求。
3. 請聯絡您的 IT 團隊以允許列出必要的網域和連接埠。

此使用者屬於不同的網路。

可能原因：使用者帳戶存在於不同的 Wickr 網路上

解決方案

1. 確認您使用的是正確的 AWS Wickr 用戶端版本。
2. 請聯絡您的網路管理員。
3. 如果問題仍然存在，請聯絡 AWS Support 並提供使用者電子郵件和網路 ID。

帳戶已暫停

可能原因：多次失敗的登入嘗試或管理員動作

解決方案

1. 請聯絡您的網路管理員以解除潛在的暫停。

2. 如果您是唯一的管理員，請聯絡 AWS Support。

需要電子郵件驗證

可能原因：電子郵件驗證未在註冊期間完成。

解決方案

1. 檢查垃圾郵件/垃圾郵件資料夾是否有驗證電子郵件。
2. 驗證電子郵件地址是否正確。
3. 請與您的 IT 團隊確認電子郵件篩選。
4. 從登入畫面請求新的驗證電子郵件。

對登入和註冊問題進行故障診斷

本節可協助您疑難排解 AWS Wickr 的登入和註冊問題。如果本節中的步驟無法解決您的問題，請在AWS支援中心開啟案例。

主題

開始之前

在對登入或註冊問題進行故障診斷之前，請先驗證下列項目：

- 您為組織使用正確的 Wickr 產品：AWS Wickr、AWSWickrGov (GovCloud) 或 Wickr Enterprise（自我託管）。如果您不確定，請聯絡您的網路管理員。
- 您正在執行支援的用戶端版本。AWS Wickr 支援目前版本和先前的 2-3 版本。若要檢查您的版本，請開啟 Wickr，然後選擇設定、關於。若要更新，請參閱檢查更新。

- 您的組織有正確的身分驗證方法 (SSO 或非 SSO)。
- 您已將使用者密碼和 Wickr 復原金鑰儲存在安全的位置。
- 您的網路允許與必要的 Wickr 網域和連接埠進行通訊。
- 您的裝置符合系統需求。

> **Tip**
>
> 如果您在登入或註冊期間遇到錯誤，請在疑難排解之前擷取錯誤訊息的螢幕擷取畫面。這可協助您的管理員或 AWSSupport 更快診斷問題。

常見的登入問題

當登入失敗時，錯誤訊息會決定故障診斷路徑。從識別您看到的錯誤開始。

「密碼不正確」或登入資料遭拒

1. 確認您輸入正確的密碼。檢查是否有錯別字、額外的空格和大寫鎖定。
2. 如果您使用 SSO (Okta、Microsoft Entra ID、、Amazon Cognito)，請透過身分提供者重設密碼，而不是透過 Wickr。
3. 如果您使用 Wickr 管理的登入資料，請參閱 the section called “密碼重設”。

「無法連線伺服器」或連線錯誤

這表示網路問題，而不是帳戶問題。

1. 確認您的網際網路連線處於作用中狀態。
2. 切換網路 — 嘗試行動數據而非 WiFi，反之亦然。
3. 如果是在公司網路上，請要求 IT 團隊驗證是否允許必要的 Wickr 網域和連接埠。
4. 如果是在 VPN 上，請嘗試暫時中斷連線。
5. 如果問題仍然存在，請收集日誌並聯絡您的網路管理員。

「找不到帳戶」或「找不到使用者」

1. 確認您登入的是正確的 Wickr 產品 (AWS Wickr 與 WickrGov 與 Enterprise)。

2. 確認您的使用者名稱或電子郵件輸入正確。
3. 您的帳戶可能已從網路中移除。請聯絡您的網路管理員。

「帳戶已暫停」

請參閱 the section called “帳戶停用”。

「此使用者屬於不同的網路」

1. 您可能不小心在不同 Wickr 網路上建立帳戶 （ 請參閱 the section called “訪客使用者問題”)。
2. 確認您為組織使用正確的 Wickr 用戶端。
3. 請聯絡您的網路管理員。管理員可能需要聯絡 AWSSupport 並提供您的電子郵件地址和網路 ID 來解決衝突。

在行動裝置上登入失敗，但在桌面上運作

1. 確認您輸入正確的密碼。
2. 測試行動數據 — 停用 WiFi 然後再試一次。如果行動網路正常運作，但 WiFi 無法運作，則問題是您的網路組態。請聯絡您的 IT 團隊。
3. 檢查 Wickr 應用程式是否具有必要的裝置許可。
4. 從應用程式存放區解除安裝和重新安裝 AWS Wickr。

> **Note**
>
> 重新安裝 會刪除本機訊息歷史記錄。

其他登入錯誤

如果您的錯誤未列在上方：

1. 確認您輸入正確的密碼。
2. 擷取錯誤訊息的螢幕擷取畫面。
3. 為您的平台收集日誌。
4. 請聯絡您的網路管理員，並提供螢幕擷取畫面和日誌。

註冊問題

訪客使用者問題

徵狀：註冊後，您會看到「訪客網路」畫面，而且無法在組織的聯絡人中看到其他使用者。

原因：您直接啟動註冊，而不是透過管理員的邀請完成註冊。這會建立訪客使用者帳戶，而不是加入組織的網路。

解決方法：

1. 請聯絡您的網路管理員。
2. 管理員必須刪除訪客使用者帳戶，然後重新邀請您使用正確的網路。
3. 使用來自管理員的邀請連結或程式碼完成註冊。

「此使用者屬於不同的網路」

原因：您不小心在不同 Wickr 網路上建立帳戶，或者您使用錯誤的用戶端。

1. 確認您使用的是正確的用戶端：適用於商用網路的 AWS Wickr、適用於 GovCloud 的 WickrGov 或適用於自我託管的 Wickr Enterprise。
2. 從 AWS Wickr 下載頁面下載正確的用戶端。
3. 請聯絡您的網路管理員。管理員可能需要聯絡 AWSSupport 並提供您的電子郵件地址和網路 ID。

使用者名稱格式錯誤

AWS Wickr 中的使用者名稱有下列需求：

- 使用者名稱是永久的，無法在建立後變更。
- 電子郵件地址是註冊的主要識別符。
- 使用者名稱不得包含不支援的特殊字元。通常支援英數字元、句點、連字號和底線。
- 對於啟用 SSO 的網路，使用者建立是由身分提供者 (IdP) 處理。使用者必須存在於身分端，才能登入 Wickr 用戶端。

未收到電子郵件驗證

1. 檢查您的垃圾郵件資料夾。

2. 驗證您輸入的電子郵件地址是否正確。
3. 請聯絡您的 IT 團隊，以確保來自 AWS Wickr 的電子郵件不會被電子郵件篩選條件封鎖。
4. 返回登入畫面，然後選擇重新傳送驗證電子郵件的選項。

密碼重設

> **Note**
>
> 對於啟用 SSO 的帳戶，密碼重設是透過您的身分提供者 (Microsoft Entra ID、Okta、Amazon Cognito 或) 管理，而不是透過 Wickr。

密碼重設流程 （非 SO) :

> **Important**
>
> 重設 Wickr 密碼是完整的帳戶重設。這會永久刪除所有本機訊息歷史記錄、從所有房間移除使用者，以及清除裝置註冊。使用者必須重新邀請他們之前參與的房間。這無法復原。建議使用者在繼續之前耗盡所有其他選項 （驗證大寫鎖定、檢查已儲存的密碼、嘗試其他裝置）。

1. 在 Wickr 登入畫面上，選擇忘記密碼？
2. 輸入與您的 AWS Wickr 帳戶相關聯的電子郵件地址。
3. 檢查您的收件匣是否有密碼重設電子郵件。如果幾分鐘內未收到，請檢查垃圾郵件資料夾。
4. 選擇電子郵件中的密碼重設連結。密碼重設連結會在 24 小時後過期。
5. 輸入並確認新密碼。您的密碼必須符合網路管理員設定的複雜性要求。

密碼複雜性要求

密碼要求是由管理員在安全群組設定下的管理員主控台中設定。需求可能包括：

- 長度下限 （至少 8 個字元；管理員可以設定較高值）
- 小寫字母的必要計數
- 大寫字母的必要計數

- 所需的數字計數
- 特殊字元的必要計數

從用戶端 6.70 版開始，在 Android 和 iOS 上建立帳戶和變更密碼期間，密碼複雜性要求會內嵌顯示。

帳戶停用

徵狀：您在登入時看到「帳戶暫停」錯誤。

對於一般使用者：

1. 請聯絡您的網路管理員。
2. 管理員可以在管理員主控台 > 團隊目錄 > 尋找使用者 > 取消暫停中取消暫停。

對於單一管理員（沒有其他管理員可取消暫停）：

聯絡 AWSSupport 並提供您的電子郵件地址、網路 ID 和管理員狀態驗證。

由於登入嘗試失敗而導致帳戶鎖定：

- 等待 24 小時以自動解除鎖定，或
- 請聯絡您的網路管理員以手動解鎖您的帳戶，或
- 使用 the section called “密碼重設”流程重設您的登入資料並解鎖您的帳戶。

如果您在解除暫停後無法登入：

聯絡 AWSSupport 並提供您的電子郵件地址、網路 ID、用戶端版本 (Wickr > 設定 > 關於) 和作業系統版本。

收集日誌

日誌收集方法因平台而異。在聯絡管理員或 AWSSupport 之前收集日誌。

桌面

如果您可以存取 Wickr 功能表：

1. 開啟 Wickr，然後選擇漢堡選單 (☰)，然後選擇支援、支援記錄。

2. 開啟允許支援記錄。對於調查，也請啟用延伸記錄詳細資訊。
3. 重現問題。
4. 返回支援並選擇儲存日誌。與您的管理員共用 檔案。

如果您無法存取 Wickr 功能表（例如，用戶端在登入畫面當機），請使用 `-logging`旗標啟動用戶端以產生日誌：

- macOS：開啟終端機並執行：

  ```
  /Applications/AWS\ Wickr.app/Contents/MacOS/AWS\ Wickr -logging
  ```

  日誌會儲存至 `~/Library/Application Support/Wickr, LLC/Wickr Pro/logs/`。
- Windows：開啟 AWS Wickr 捷徑的內容選單，選擇屬性，然後選擇捷徑索引標籤。附加`-logging`至目標路徑（引號外）。啟動捷徑。

  日誌會儲存至 `C:\Users\<USERNAME>\AppData\Local\Wickr, LLC\Wickr Pro\logs\`。
- Linux：從具有 `-logging`旗標的終端機啟動。

  日誌會儲存至 `~/.local/share/Wickr, LLC/Wickr Pro/logs/`。

行動應用程式

1. 開啟 Wickr，然後選擇設定、關於、匯出所有日誌。
2. 與您的管理員共用匯出的日誌檔案。

如果您無法存取設定（例如，您卡在登入畫面）：

- iOS：將您的裝置連接到 Mac、開啟 Console.app、篩選 "Wickr"，然後重現問題。
- Android：啟用 USB 除錯、連接至電腦，然後執行 `adb logcat | grep -i wickr`。

故障診斷 SSO 和身分驗證問題

本節協助管理員疑難排解 AWS Wickr 的單一登入 (SSO) 和身分驗證問題。如果本節中的步驟無法解決您的問題，請在AWS 支援中心開啟案例。

> **Important**
>
> Wickr 僅支援 OpenID Connect (OIDC)。不支援 SAML 型身分提供者。如果您的組織使用僅限 SAML 身分提供者，您必須設定與 OIDC 相容的替代方案或實作 OIDC 橋接器。

主題

開始之前

在故障診斷之前，請先驗證下列項目：

- 您可以讓管理員存取 Wickr 管理員主控台。
- 您可以存取組織的身分提供者 (IdP) 組態。
- 已在 Wickr 網路設定中啟用 SSO。
- 您的身分提供者符合 OIDC 規範。Wickr 不支援 SAML。

常見的 SSO 問題

支援的身分提供者

Wickr 為下列 OIDC 相容身分提供者提供組態指引：

- Microsoft Entra ID （ 先前為 Azure AD)
- Okta
- Amazon Cognito
- AWS Identity and Access Management 身分中心

任何符合 OIDC 的身分提供者都可以與 Wickr 搭配使用。對於上面未列出的提供者，請使用設定 SSO 文件中的一般 OIDC 組態參數。

使用者無法使用 SSO 登入

當使用者回報他們無法使用 SSO 登入時，請執行下列檢查。

驗證 Wickr SSO 組態

1. 在 Wickr Admin 主控台中，選擇網路設定，然後選擇單一登入。
2. 確認 SSO 已啟用。
3. 驗證發行者 URL、用戶端 ID 和用戶端秘密是否符合您的身分提供者組態。
4. 確認身分提供者中的重新導向 URI 符合 Wickr Admin Console 中顯示的值。

常見的 SSO 錯誤

「找不到使用者」

使用者不存在於您的身分提供者中，或尚未指派給 Wickr 應用程式。確認使用者存在於您的 IdP 中，並具有正確的群組指派。

「無效回應」或「設定錯誤」

OIDC 中繼資料或端點設定錯誤。驗證發行者 URL、用戶端 ID 和重新導向 URIs Wickr 和您的身分提供者之間是否相符。

「拒絕存取」

使用者在您的身分提供者中缺少必要的群組成員資格或應用程式指派。檢查 IdP 的應用程式指派設定。

未提示使用者輸入公司 ID

如果在 SSO 註冊期間未提示使用者輸入公司 ID，請確認已在網路設定、Wickr 管理員主控台的網路設定檔中設定公司 ID。

判斷問題是與 Wickr 還是您的身分提供者有關

使用下列問題來判斷問題所在：

- 使用者可以使用相同的 IdP 驗證其他應用程式嗎？ 如果否，問題出在您的身分提供者，而不是 Wickr。
- 是否所有使用者都受到影響，或僅影響特定使用者？ 如果只有特定使用者，請在 IdP 中檢查其群組指派和應用程式存取。

- 您的 IdP 組態最近是否有變更？ 憑證輪換、政策變更或端點更新可能會中斷 OIDC 連線。
- 錯誤是否發生在 Wickr 用戶端或 IdP 登入頁面？ 如果錯誤出現在 IdP 登入頁面上，問題出在您的身分提供者。

其他資源

- 在 AWS Wickr 中設定 SSO
- Microsoft Entra ID SSO 設定（包括 Entra 特定疑難排解）

對身分和存取問題進行故障診斷

本節協助管理員對 AWS Wickr 的身分和存取問題進行疑難排解。如果本節中的步驟無法解決您的問題，請在AWS 支援中心開啟案例。

主題

- 開始之前
- 常見的身分和存取問題

開始之前

故障診斷之前，請先驗證下列項目：

- 您可以讓管理員存取包含 Wickr 網路 AWS 帳戶 的 。
- 您可以存取 IAM 主控台或檢視 IAM 政策的許可。
- 您知道哪些 IAM 使用者或角色遇到存取問題。

常見的身分和存取問題

我無權在 AWS 管理主控台 for Wickr 中執行動作

如果 AWS 管理主控台 for Wickr 告知您無權執行 動作，則必須聯絡管理員尋求協助。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 AWS 管理主控台 for Wickr 來建立、管理或檢視 Wickr 網路，但沒有 `wickr:CreateAdminSession`和 `wickr:ListNetworks`許可時，會發生下列範例錯誤。

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

在此情況下，Mateo 會要求管理員更新其政策，以允許他使用 `wickr:CreateAdminSession`和 `wickr:ListNetworks`動作存取 AWS 管理主控台 for Wickr 的 。如需詳細資訊，請參閱AWS Wickr 的身分型政策範例及AWS受管政策：AWSWickrFullAccess。

故障診斷網路和連線問題

本節協助管理員疑難排解 AWS Wickr 的網路和連線問題。最終使用者報告的大多數連線問題是由企業網路組態（防火牆、代理、VPNs) 封鎖所需的 Wickr 流量所造成。如果本節中的步驟無法解決您的問題，請在AWS支援中心開啟案例。

主題

開始之前

故障診斷之前，請先驗證下列項目：

- 您可以存取組織的網路組態（防火牆規則、代理設定、VPN 組態）。
- 您已檢閱 Wickr 網路需求（必要的網域和連接埠）。
- 您已確認問題是否會影響所有使用者、特定使用者或特定位置。
- 您已確認受影響的使用者是否可以在非企業網路（行動資料或家用 WiFi) 上連線。

> **Important**
>
> 如果使用者可以在行動數據或家用 WiFi 上連線，但不能在公司網路上連線，則問題是您的網路組態，而不是 Wickr 服務。

常見的網路問題

防火牆封鎖 Wickr 流量

這是連線失敗的最常見原因。Wickr 需要存取特定網域和連接埠。

徵狀

使用者無法在公司 WiFi 上連線，但可以在行動數據上連線。相同位置的多個使用者會受到影響。Wickr 先前已運作，但在網路變更後停止。

Resolution

1. 檢閱 Wickr 網路需求中必要網域和連接埠的完整清單。
2. 允許列出防火牆中所有必要的網域。Wickr 需要 HTTPS (TCP 443) 進行簡訊和訊號傳送，以及 UDP 連接埠進行語音和視訊通話。
3. 從公司網路驗證必要網域的 DNS 解析。使用 `nslookup`或 `dig` 確認網域解析。
4. 進行變更後測試連線能力。讓受影響的使用者重新啟動 Wickr 並嘗試連線。

> **Note**
>
> 如果只有語音和視訊通話失敗，但傳訊正常運作，則 UDP 流量可能會遭到封鎖。根據預設，Wickr 會使用 UDP 進行呼叫。請參閱 the section called “UDP 封鎖（呼叫失敗，傳訊運作正常）”。

Proxy 伺服器干擾

公司代理伺服器可能會干擾 Wickr 連線，尤其是不支援 WebSocket 連線的情況。

徵狀

只有在設定代理時才會發生連線問題。Wickr 會在繞過代理時運作。間歇中斷連線。

Resolution

1. 確認您的代理支援 WebSocket 連線 (Wickr 訊息需要）。
2. 為網路需求中列出的 Wickr 網域設定代理繞過 (PAC 檔案例外狀況或直接連線規則）。
3. 檢閱代理日誌是否有與 Wickr 網域的封鎖或失敗連線。

4. 如果您的代理需要身分驗證，請確認 Wickr 流量未因缺少登入資料而遭到拒絕。Wickr 不支援 SaaS 部署上的代理身分驗證。

SSL/TLS 檢查中斷連線

公司 SSL 檢查（也稱為 HTTPS 檢查或 TLS 攔截）會中斷 Wickr 預期的憑證鏈，導致連線失敗。

徵狀

Wickr 中的憑證錯誤。「安全連線失敗」錯誤。Wickr 可在沒有 SSL 檢查的網路上運作。

Resolution

1. 偏好：略過 Wickr 網域的 SSL 檢查。設定您的 SSL 檢查設備以排除網路需求中列出的網域。這會維護 Wickr end-to-end加密。
2. 替代方案：在使用者裝置上安裝組織的根 CA 憑證。這可讓 Wickr 信任攔截的憑證鏈。如需憑證和安裝指示，請聯絡您的 IT 安全團隊。

若要驗證 SSL 檢查是否為原因，請從受影響的裝置執行下列命令，並將憑證發行者與預期的AWS憑證進行比較：

```
openssl s_client -showcerts -connect ingress-prod-calling.wickr.us-
east-1.amazonaws.com:443
```

如果憑證發行者顯示組織的 CA，而不是 AWS或 Amazon 憑證，則 Wickr 流量會啟用 SSL 檢查。

VPN 封鎖 Wickr

VPN 組態通常會封鎖 Wickr 流量，尤其是呼叫所需的 UDP 連接埠。

徵狀

Wickr 在沒有 VPN 的情況下運作，但沒有連接 VPN。VPN 連接時，連線會中斷。呼叫失敗，但傳訊可透過 VPN 運作。

Resolution

1. 設定分割通道，以直接路由網路需求中所列網域的 Wickr 流量（繞過 VPN 通道）。
2. 如果不允許分割通道，請確保 VPN 允許 TCP 443 和網路需求中列出的 UDP 連接埠。
3. 如果只有呼叫透過 VPN 失敗，VPN 可能會封鎖 UDP。請參閱 the section called “UDP 封鎖（呼叫失敗，傳訊運作正常）”。

UDP 封鎖（呼叫失敗，傳訊運作正常）

Wickr 預設會將 UDP 用於語音和視訊通話，並回復為 TCP。如果您的網路封鎖 UDP，呼叫將無法立即連線，且會回復到效能可能降低的 TCP，同時傳訊會繼續正常運作。您可以在 Wickr 網路安全群組中啟用（強制）TCP 呼叫，以完全略過 UDP，強制所有對 TCP 的呼叫。

診斷

要求受影響的使用者啟用 TCP 呼叫做為測試（或透過所有使用者的主控台以管理方式啟用/強制 TCP)：設定、呼叫、啟用 TCP 呼叫。如果啟用 TCP 時呼叫成功，UDP 會遭到封鎖。

Resolution

允許列出防火牆和 VPN 組態中網路需求中列出的 UDP 連接埠。

TCP 呼叫是一種診斷工具，不是永久解決方案。使用 TCP 時，通話品質會降低。

DNS 解析失敗

如果您的 DNS 伺服器無法解析 Wickr 網域，則用戶端無法連線。

診斷

從受影響網路上的裝置，驗證必要 Wickr 網域的 DNS 解析：

```
nslookup gw-pro-prod.wickr.com
```

如果網域未解決，問題是 DNS 組態。

Resolution

1. 確認您的 DNS 伺服器可以解析網路需求中列出的網域。
2. 如果使用 DNS 篩選或 DNS 防火牆，請新增 Wickr 網域的例外狀況。
3. 使用替代 DNS 伺服器（例如 8.8.8.8) 進行測試，以確認問題是否為您的內部 DNS。

判斷問題的範圍

使用下列問題來縮小原因範圍：

- Wickr 是否適用於行動數據或家用 WiFi？ 如果是，問題是您的公司網路組態。

- 所有使用者是否都受到影響，或僅影響特定使用者？ 如果某個位置的所有使用者都受到影響，問題是整個網路。如果只有特定使用者，請檢查其裝置或 VPN 組態。
- 這是否在網路變更後開始？ 防火牆規則更新、代理變更或 VPN 組態變更通常會中斷 Wickr 連線。
- 訊息是否正常運作，但呼叫失敗？ 這表示 UDP 已封鎖。請參閱 the section called “UDP 封鎖（呼叫失敗，傳訊運作正常）”。
- 使用者是否看到憑證錯誤？ 這表示 SSL 檢查正在攔截 Wickr 流量。請參閱 the section called “SSL/TLS 檢查中斷連線”。

其他資源

- AWS Wickr 的網路需求（必要的網域和連接埠）
- 最終使用者網路疑難排解（與受影響的使用者共用）

文件歷史記錄

下表說明 Wickr 的文件版本。

變更	描述	日期
檔案預覽現已推出	Wickr 管理員現在可以啟用或停用檔案下載。如需詳細資訊，請參閱 AWS Wickr 的檔案預覽。	2025 年 5 月 29 日
全新重新設計的 Wickr 管理員主控台現已推出	Wickr 已增強 Wickr 管理員主控台，為管理員提供更好的導覽和改善可存取性。	2025 年 3 月 13 日
Wickr 現已在亞太區域（馬來西亞）提供 AWS 區域	Wickr 現已在亞太區域（馬來西亞）提供 AWS 區域。如需詳細資訊，請參閱區域可用性。	2024 年 11 月 20 日
刪除網路現已可用	Wickr 管理員現在可以刪除 AWS Wickr 網路。如需詳細資訊，請參閱在 AWS Wickr 中刪除網路。	2024 年 10 月 4 日
使用 Microsoft Entra (Azure AD) SSO 設定 AWS Wickr 現已可用	AWS Wickr 可設定為使用 Microsoft Entra (Azure AD) 做為身分提供者。如需詳細資訊，請參閱使用 Microsoft Entra (Azure AD) 單一登入設定 AWS Wickr。	2024 年 9 月 18 日
Wickr 現已在歐洲（蘇黎世）推出 AWS 區域	Wickr 現已在歐洲（蘇黎世）提供 AWS 區域。如需詳細資訊，請參閱區域可用性。	2024 年 8 月 12 日
跨邊界分類和聯合現已推出	跨邊界分類功能可讓 GovCloud 使用者變更對話的使用者介	2024 年 6 月 25 日

	面。如需詳細資訊，請參閱 GovCloud 跨邊界分類和聯合。	
讀取接收功能現已推出	Wickr 管理員現在可以在管理員主控台中啟用或停用讀取接收功能。如需詳細資訊，請參閱讀取回條。	2024 年 4 月 23 日
全球聯合現在支援受限聯合，管理員可以在管理員主控台中檢視用量分析	全球聯合現在支援受限聯合。這適用於其他 中的 Wickr 網路 AWS 區域。如需詳細資訊，請參閱安全群組。此外，管理員現在可以在管理員主控台的分析儀表板上檢視其用量分析。如需詳細資訊，請參閱分析儀表板。	2024 年 3 月 28 日
三個月免費試用 AWS Wickr 的 Premium 計劃現已推出	Wickr 管理員現在可以為最多 30 位使用者選擇三個月免費試用 Premium 計劃。在免費試用期間，所有 Standard 和 Premium 計劃功能皆可使用，包括無限制的管理員控制和資料保留。訪客使用者功能在 Premium 免費試用期間無法使用。如需詳細資訊，請參閱管理計劃。	2024 年 2 月 9 日
訪客使用者功能已全面推出，並已新增更多管理員控制項	Wickr 管理員現在可以存取一系列的新功能，包括訪客使用者清單、大量刪除或暫停使用者的能力，以及封鎖訪客使用者在 Wickr 網路中通訊的選項。如需詳細資訊，請參閱訪客使用者。	2023 年 11 月 8 日

Wickr 現已在歐洲（法蘭克福）推出 AWS 區域	Wickr 現已在歐洲（法蘭克福）提供 AWS 區域。如需詳細資訊，請參閱區域可用性。	2023 年 10 月 26 日
Wickr 網路現在能夠跨 AWS 區域	Wickr 網路現在能夠跨 聯合 AWS 區域。如需詳細資訊，請參閱安全群組。	2023 年 9 月 29 日
Wickr 現已在歐洲（倫敦）推出 AWS 區域	Wickr 現已在歐洲（倫敦）提供 AWS 區域。如需詳細資訊，請參閱區域可用性。	2023 年 8 月 23 日
Wickr 現已在加拿大（中部）推出 AWS 區域	Wickr 現已在加拿大（中部）提供 AWS 區域。如需詳細資訊，請參閱區域可用性。	2023 年 7 月 3 日
訪客使用者功能現在可供預覽	訪客使用者可以登入 Wickr 用戶端並與 Wickr 網路使用者協作。如需詳細資訊，請參閱訪客使用者（預覽）。	2023 年 5 月 31 日
AWS Wickr 現在已與 整合 AWS CloudTrail，現在可在 AWS GovCloud（美國西部）中以 WickrGov 的形式使用	AWS Wickr 現在已與 整合 AWS CloudTrail。如需詳細資訊，請參閱使用 記錄 AWS Wickr API 呼叫 AWS CloudTrail。此外，Wickr 現在以 WickrGov 的形式在 AWS GovCloud（美國西部）提供。如需詳細資訊，請參閱AWS GovCloud (US)《使用者指南》中的 AWS WickrGov。	2023 年 3 月 30 日
標記和建立多個網路	AWS Wickr 現在支援標記。如需詳細資訊，請參閱網路標籤。現在可以在 Wickr 中建立多個網路。如需詳細資訊，請參閱建立網路。	2023 年 3 月 7 日

初始版本	Wickr 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。

2026 年 6 月

- 工作階段逾時 - 管理員現在可以設定閒置逾時，在指定期間後自動鎖定 Wickr 用戶端。系統會提示使用者重新驗證以繼續其工作階段。
- 同意橫幅 - 管理員現在可以設定在登入時向使用者顯示的同意橫幅。使用者必須先確認橫幅，才能存取應用程式。

2026 年 3 月

- 已改善整個管理員主控台的可存取性，包括 ATAK 說明面板的更新、SSO 組態和網路建立流程。

2025 年 12 月

- 裝置暫停和取消暫停動作已從管理員主控台中移除。管理員可以繼續重設使用者裝置。

2025 年 11 月

- 改善網路和安全群組資料表的 UI 和 UX，以及頁面載入和 API 呼叫監控的主控台指標。

2025 年 8 月

- 已更新 AWS Wickr 和AWSWickrGov 的電子郵件範本，以改善使用者加入體驗。寄件者電子郵件地址已從 變更為 `donotreply@wickr.email` `no-reply@amazonaws.com`。

2025 年 5 月

- 檔案預覽現已推出。當管理員在安全群組的管理員主控台中停用檔案下載時，使用者只能在訊息和檔案索引標籤中檢視支援的檔案清單。

2025 年 3 月

- 重新設計的 Wickr 管理員主控台現已可用。

2024 年 10 月

- Wickr 現在支援刪除網路。如需詳細資訊，請參閱在 AWS Wickr 中刪除網路。

2024 年 9 月

- 管理員現在可以使用 Microsoft Entra (Azure AD) 單一登入來設定 AWS Wickr。如需詳細資訊，請參閱使用 Microsoft Entra (Azure AD) 單一登入設定 AWS Wickr。

2024 年 8 月

- 增強功能
  - Wickr 現已在歐洲 （ 蘇黎世 ） 推出AWS 區域。

2024 年 6 月

- GovCloud 使用者現在可以使用跨邊界分類和聯合。如需詳細資訊，請參閱 GovCloud 跨邊界分類和聯合。

2024 年 4 月

- Wickr 現在支援讀取回條。如需詳細資訊，請參閱讀取回條。

2024 年 3 月

- 全球聯合現在支援限制聯合，其中只能針對在限制聯合下新增的所選網路啟用全球聯合。這適用於其他 中的 Wickr 網路AWS 區域。如需詳細資訊，請參閱安全群組。
- 管理員現在可以在管理員主控台的分析儀表板上檢視其用量分析。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 名使用者提供三個月的 Premium 計劃免費試用。變更和限制包括：
  - 所有標準和高級計劃功能，例如無限制的管理員控制和資料保留，現在都可以在高級免費試用中使用。訪客使用者功能在 Premium 免費試用期間無法使用。
  - 先前的免費試用不再可用。如果您尚未使用 Premium 免費試用，您可以將現有的免費試用或標準方案升級至 Premium 免費試用。如需詳細資訊，請參閱管理計劃。

2023 年 11 月

- 訪客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 使用者的濫用。
  - 管理員可以檢視網路已互動的訪客使用者清單，以及每月用量計數。
  - 管理員可以封鎖訪客使用者與其網路通訊。
  - 訪客使用者的附加元件定價。

- 管理員控制增強功能
  - 大量刪除/暫停使用者的能力。
  - 設定字符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）提供AWS 區域。

2023 年 9 月

- 增強功能
  - Wickr 網路現在能夠跨 聯合AWS 區域。如需詳細資訊，請參閱安全群組。

2023 年 8 月

- 增強功能
  - Wickr 現已在歐洲（倫敦）推出AWS 區域。

2023 年 7 月

- 增強功能
  - Wickr 現已在加拿大（中部）提供AWS 區域。

2023 年 5 月

- 增強功能
  - 新增對訪客使用者的支援。如需詳細資訊，請參閱AWS Wickr 網路中的訪客使用者。

2023 年 3 月

- Wickr 現在已與 整合AWS CloudTrail。如需詳細資訊，請參閱使用 記錄 AWS Wickr API 呼叫 AWS CloudTrail。
- Wickr 現在以 WickrGov 的形式在 AWSGovCloud（美國西部）中提供。如需詳細資訊，請參閱AWS GovCloud (US)《使用者指南》中的 AWSWickrGov。
- Wickr 現在支援標記。如需詳細資訊，請參閱AWS Wickr 的網路標籤。現在可以在 Wickr 中建立多個網路。如需詳細資訊，請參閱步驟 1：建立網路。

2023 年 2 月

- Wickr 現在支援 Android 戰術攻擊套件 (ATAK)。如需詳細資訊，請參閱在 Wickr 網路儀表板中啟用 ATAK。

2023 年 1 月

- 所有計劃現在可以設定單一登入 (SSO)，包括免費試用和標準。

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。