aws

管理ガイド

AWS Wickr

AWS Wickr: 管理ガイド

Table of Contents

AWS Wickr とは？

AWS Wickr は、組織や政府機関がグループメッセージング、音声通話、ビデオ通話、ファイル共有、 end-to-end one-to-one 画面共有などを通じて安全に通信できるようにする暗号化されたサービスです。Wickr は、コンシューマーグレードのメッセージングアプリに関連するデータ保持義務を顧客が克服し、コラボレーションを安全に促進できるよう支援します。高度なセキュリティと管理制御により、組織は法的要件や規制要件を満たし、データセキュリティの課題に対応するカスタムソリューションを構築できます。

情報は、保存や監査の目的で、カスタマーが管理するプライベートなデータストアに記録できます。ユーザーは、権限の設定、エフェメラルメッセージングオプションの設定、セキュリティグループの定義など、データを包括的に管理できます。Wickr は、アクティブディレクトリ (AD)、OpenID Connect (OIDC) によるシングルサインオン (SSO) などの追加サービスと統合されます。Wickr ネットワークを経由してすばやく作成して管理し AWS Management Console、Wickr ボットを使用してワークフローを安全に自動化できます。開始するには、 AWS Wickr 用のセットアップ を参照してください。

トピック

Wickr の特徴

セキュリティとプライバシーの強化

Wickrはすべての機能に256ビットの高度暗号化標準 (AES) 暗号化を使用しています。 end-to-end 通信はユーザーデバイス上でローカルに暗号化され、送信者と受信者以外への転送中は解読できません。すべてのメッセージ、通話、ファイルは新しいランダムキーで暗号化され、目的の受信者以外は (AWSましてや) 復号化できません。機密データや規制対象データの共有、法的問題や人事に関する議論、戦術的な軍事作戦の実施など、セキュリティとプライバシーが最優先される場合、カスタマーは Wickr を使用して通信します。

データ保持

柔軟な管理機能は、機密情報を保護するだけでなく、コンプライアンス義務、法的保持、監査目的で必要に応じてデータを保持するように設計されています。メッセージとファイルは、カスタマーが管理する安全なデータストアにアーカイブできます。

柔軟なアクセス

ユーザーはマルチデバイス (モバイル、デスクトップ) でアクセスでき、非接続環境や通信環境など、低帯域幅環境でも機能することができます。 out-of-band

管理コントロール

ユーザーは、権限の設定、責任がありエフェメラルメッセージングオプションの設定、セキュリティグループの定義など、データを包括的に管理できます。

強力なインテグレーションとボット

Wickr は、アクティブディレクトリ、OpenID Connect (OIDC) によるシングルサインオン (SSO) などの追加サービスと統合されます。顧客は、Wickr Bots を使用して Wickr ネットワークを迅速に作成および管理し AWS Management Console、Wickr Bots を使用してワークフローを安全に自動化できます。

Wickr が提供するコラボレーションの内訳は次のとおりです。

- 1 対 1 メッセージとグループメッセージング：最大 500 人のメンバーがいるルームで、チームと安全にチャットできます
- 音声通話とビデオ通話：最大 70 人で電話会議を開催できます
- 画面共有とブロードキャスト：最大 500 人の参加者が参加できます
- ファイル共有と保存：最大 5 GB までファイルを転送でき、ストレージ容量は無制限です
- エフェメラル:有効期限とタイマーを制御 burn-on-read
- グローバルフェデレーション：ネットワーク外の Wickr ユーザーと接続する

> **Note**
>
> (米国西部) の Wickr ネットワークは、 AWS GovCloud (米国西部) の他の Wickr ネットワークとのみフェデレーションできます。 AWS GovCloud

Wickr へのアクセス

Wickrは、米国東部 (バージニア北部)、カナダ (中部)、ヨーロッパ (ロンドン)、アジアパシフィック (シドニー)、ヨーロッパ (フランクフルト)、ヨーロッパ (ストックホルム)、アジアパシフィック (シンガポール)、アジアパシフィック (東京) で利用できます。 AWS リージョン Wickr は (米国西部) と同様にご利用いただけます。 WickrGov AWS GovCloud AWS リージョン

管理者は https://console.aws.amazon.com/wickr/ から AWS Management Console for Wickr にアクセスします。Wickr を使い始める前に、AWS Wickr 用のセットアップ および AWS Wickr の使用開始 ガイドを完成させる必要があります。

> **Note**
>
> Wickr サービスには、アプリケーションプログラミングインターフェイス (API) はありません。

エンドユーザーは Wickr クライアントを通じて Wickr にアクセスします。詳細は、AWS Wickr ユーザーガイドを参照してください。

料金

Wickr は、個人、小規模チーム、大企業向けにさまざまなプランで利用できます。詳細については、「AWS Wickr の料金」を参照してください。

Wickr エンドユーザ向けドキュメント

Wickr クライアントのエンドユーザーで、そのドキュメントにアクセスする必要がある場合は、「AWS Wickr ユーザーガイド」を参照してください。

AWS Wickr 用のセットアップ

新規 AWS 顧客の場合は、AWS Wickr の使用を開始する前に、このページにリストされている セットアップの前提条件を完了してください。セットアップ手順には、AWS Identity and Access Management (IAM) サービスを使用します。IAM の詳細については、「IAM ユーザーガイド」を参照してください。

トピック

AWS へのサインアップ

AWS アカウント をお持ちでない場合は、以下の手順を実行してアカウントを作成してください。

AWS アカウント にサインアップするには

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話のキーパッドを使用して検証コードを入力するように求められます。

   AWS アカウントにサインアップすると、AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS のサービスとリソースへのアクセス権があります。セキュリティのベストプラクティスとして、管理ユーザーに管理アクセスを割り当て、ルートユーザーアクセスが必要なタスクを実行する場合にのみ、ルートユーザーを使用してください。

IAM ユーザーの作成

管理者ユーザーを作成するには、以下のいずれかのオプションを選択します。

管理者を管理する方法を 1 つ選択します	目的	方法	以下の操作も可能
IAM Identity Center 内 (推奨)	短期の認証情報を使用して AWS にアクセスします。 これはセキュリティのベストプラクティスと一致しています。ベストプラクティスの詳細については、IAM ユーザーガイドの「IAM でのセキュリティのベストプラクティス」を参照してください。	AWS IAM Identity Center ユーザーガイドの「開始方法」の手順に従います。	AWS Command Line Interface ユーザーガイドの「AWS IAM Identity Center を使用するための AWS CLI の設定」に従って、プログラムによるアクセスを設定します。
IAM 内 (非推奨)	長期認証情報を使用して AWS にアクセスする。	IAM ユーザーガイドの「最初の IAM 管理者のユーザーおよびグループの作成」の手順に従います。	IAM ユーザーガイドの「IAM ユーザーのアクセスキーの管理」に従って、プログラムによるアクセスを設定します。

> **Note**
>
> `AWSWickrFullAccess` マネージドポリシーを割り当てて、Wickr サービスに完全な管理者権限を付与することもできます。詳細については、「AWS 管理ポリシー: AWSWickrFullAccess」を参照してください。

次のステップ

前提条件となる設定手順が完了しました。Wickr の設定を開始するには、開始 を参照してください。

AWS Wickr の使用開始

このガイドでは、ネットワークの作成、ネットワークの設定、ユーザーの作成など、Wickrを始める方法を紹介します。

トピック

前提条件

始める前に、以下の前提条件を満たしていることを確認してください：

- Amazon Web Services (AWS) にサインアップします。詳細については、「AWS Wickr 用のセットアップ」を参照してください。
- Wickr を管理するために必要なアクセス許可があることを確認してください。詳細については、「AWS 管理ポリシー: AWSWickrFullAccess」を参照してください。
- Wickr の適切なポートとドメインを許可リストに登録していることを確認してください。詳細については、「許可するポートとドメインのリスト」を参照してください。

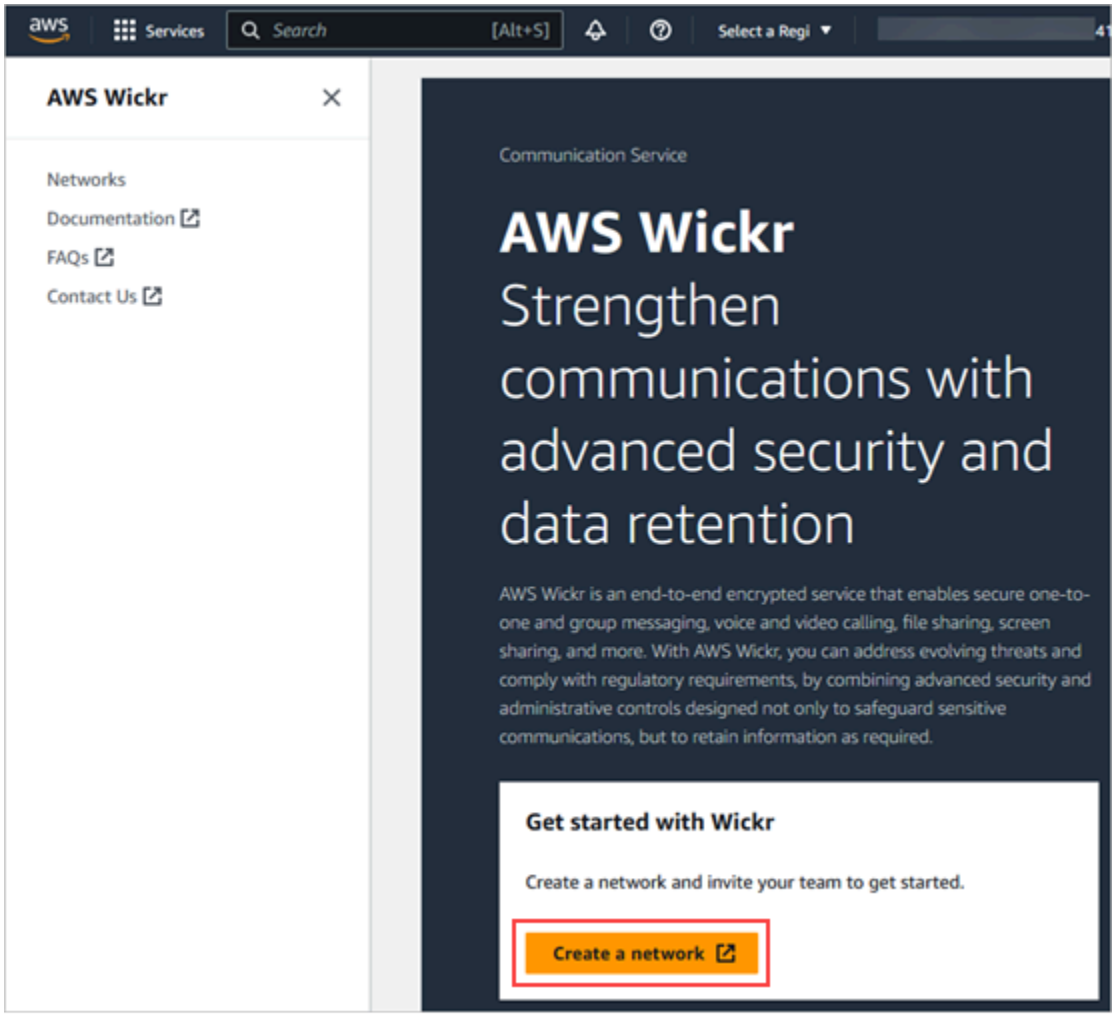
ステップ1：ネットワークの構築

アカウントの Wickr ネットワークを作成には、以下の手順を実行します。

1. https://console.aws.amazon.com/wickr/ で Wickr AWS Management Console の を開きます。

> **Note**
>
> Wickr ネットワークを作成したことがない場合は、Wickr サービスの情報ページが表示されます。1 つ以上の Wickr ネットワークを作成すると、作成したすべての Wickr ネットワークのリストビューを含むネットワークページが表示されます。

2. ネットワークの作成を選択します。



3. ネットワーク名 テキストボックスにネットワークの名前を入力します。会社名やチーム名など、組織のメンバーが認識できる名前を選択します。
4. プランを選択します。次のいずれかの Wickr ネットワークプランを選択できます。

   - 標準 — 管理上の制御と柔軟性を必要とする小規模および大規模なビジネスチーム向け。
   - プレミアムまたはプレミアム無料トライアル — 最高の機能制限、きめ細かな管理コントロール、データ保持を必要とする企業向け。

管理者はプレミアム無料トライアルオプションを選択できます。プレミアム無料トライアルオプションは最大 30 人のユーザーが利用でき、3 か月間使用できます。このオファーは、新しいレガシー無料トライアルおよび標準プランでご利用いただけます。管理者は、プレミアム無料トライアル期間中にプレミアムプランまたはスタンダードプランにアップグレードまたはダウングレードできます。

利用可能な Wickr プランと料金の詳細については、Wickr 料金表 を参照してください。

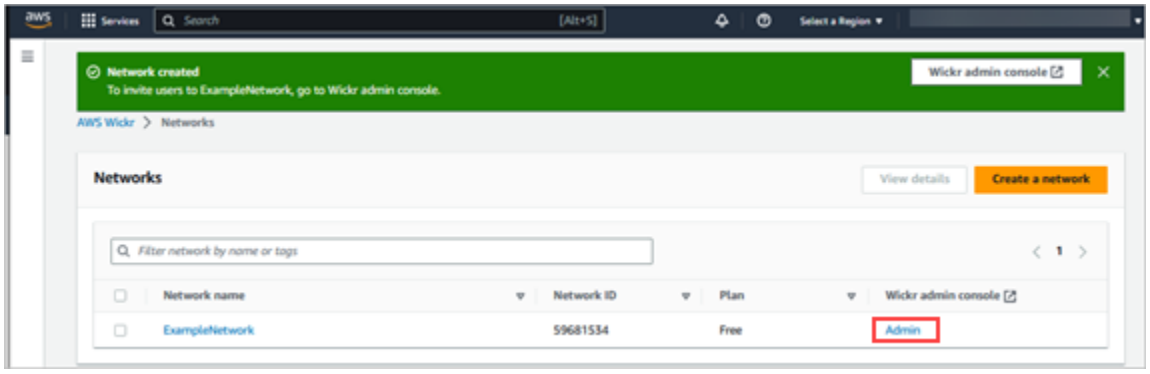
5. （オプション）新しいタグを追加 を選択してネットワークにタグを追加します。タグはキーと値のペアで構成されています。タグは、リソースの検索やフィルタリング、または AWS コストの追跡に使用できます。詳しくはネットワークタグの管理を参照してください。
6. ネットワークの作成を選択します。

   Wickr AWS Management Console の のネットワークページにリダイレクトされ、新しいネットワークがページに表示されます。

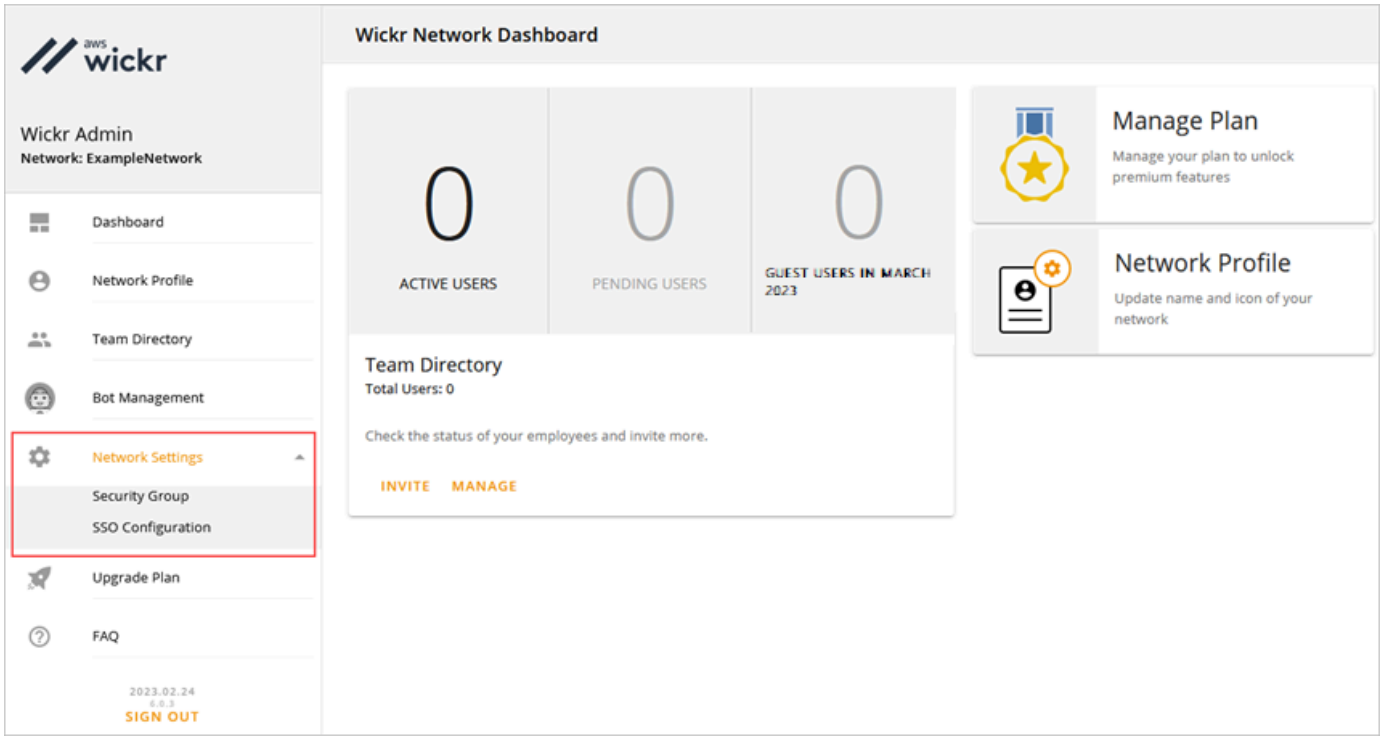
ステップ 2: ネットワークの設定

次の手順を実行して Wickr 管理コンソールにアクセスします。ここでは、ユーザーの追加、セキュリティグループの追加、SSO の設定、データ保持の設定、その他のネットワーク設定を行うことができます。

1. ネットワーク ページで 管理 リンクを選択し、そのネットワークの Wickr 管理コンソールに移動します。



   選択したネットワークの Wickr 管理コンソールにリダイレクトされます。
2. WHM コンソールの左のナビゲーションペインで 設定を微調整する を選択します。



以下のネットワーク設定オプションが利用可能です。これらの設定の実行に関する詳細については、「AWS Wickr ネットワークの管理」を参照してください。

- セキュリティグループ - パスワードの複雑性ポリシー、メッセージ設定、通話機能、セキュリティ機能、外部フェデレーションなどのセキュリティグループとその設定を管理します。詳細については、「セキュリティグループ」を参照してください。
- SSO 設定 - SSO を設定し、Wickr ネットワークのエンドポイントアドレスを表示します。Wickr は、OpenID Connect (OIDC) を使用する SSO プロバイダーのみをサポートしています。Security Assertion Markup Language (SAML) を使用するプロバイダーはサポートされていません。詳細については、「シングルサインオン設定」を参照してください。

ステップ 3：ユーザーを作成して招待する

次の方法を使用して、Wickr ネットワークにユーザーを作成できます。

- シングルサインオン - SSO を設定すると、Wickr 会社 ID を共有してユーザーを招待できます。エンドユーザーは、提供された会社 ID と仕事用の E メールアドレスを使用して Wickr に登録します。詳細については、「シングルサインオン設定」を参照してください。
- 招待 - Wickr AWS Management Console でユーザーを手動で作成し、そのユーザーに招待 E メールを送信できます。エンドユーザーは、E メール内のリンクを選択して Wickr に登録できます。

> **Note**
>
> Wickr ネットワークのゲストユーザーを有効にすることもできます。ゲストユーザー機能は現在プレビュー中です。詳細については、「ゲストユーザー」を参照してください。

ユーザーを作成または招待するには、以下の手順を実行します。

> **Note**
>
> 管理者もユーザーと見なされ、SSO または SSO 以外の Wickr ネットワークに自分自身を招待する必要があります。

SSO

Wickr にサインアップする必要がある SSO ユーザーに E メールを書いて送信します。E メールには、以下の情報を記載してください。

- Wickr の会社 ID。SSO を設定するときに Wickr ネットワークの会社 ID を指定します。詳細については、「SSO の設定」を参照してください。
- サインアップに使用すべき E メールアドレス。
- Wickr クライアントをダウンロードするための URL。ユーザーは https://aws.amazon.com/wickr/download/ の AWS Wickr ダウンロードページから Wickr クライアントをダウンロードできます。

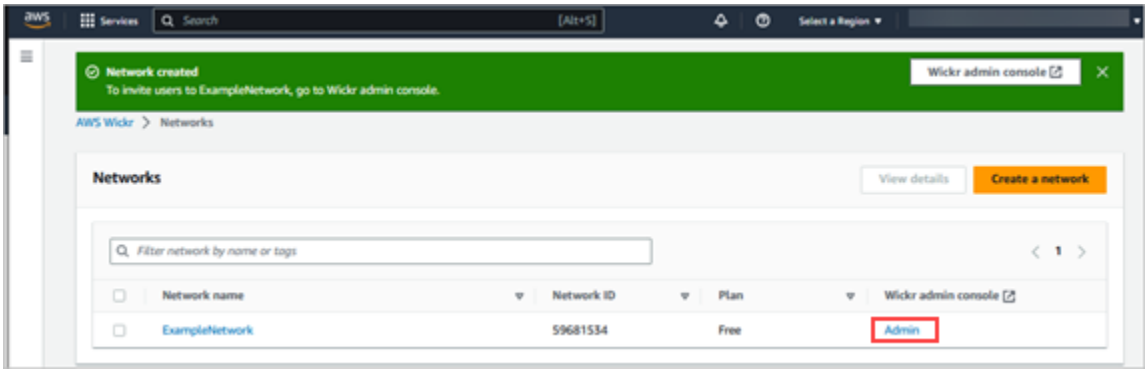
  > **Note**
  >
  > AWS GovCloud （ 米国西部) で Wickr ネットワークを作成した場合は、 WickrGov クライアントをダウンロードしてインストールするようにユーザーに指示します。他のすべての AWS リージョンでは、標準の Wickr クライアントをダウンロードしてインストールするようにユーザーに指示します。の詳細については AWS WickrGov、「 ユーザーガイドAWS WickrGov」のAWS GovCloud (US) 「」を参照してください。

ユーザーが Wickr ネットワークに登録すると、そのユーザーはアクティブのステータスで Wickr チームディレクトリに追加されます。

Non-SSO

Wickr ユーザーを手動で作成して招待状を送信するには

1. https://console.aws.amazon.com/wickr/ で Wickr AWS Management Console の を開きます。
2. ネットワーク ページで 管理 リンクを選択し、そのネットワークの Wickr 管理コンソールに移動します。



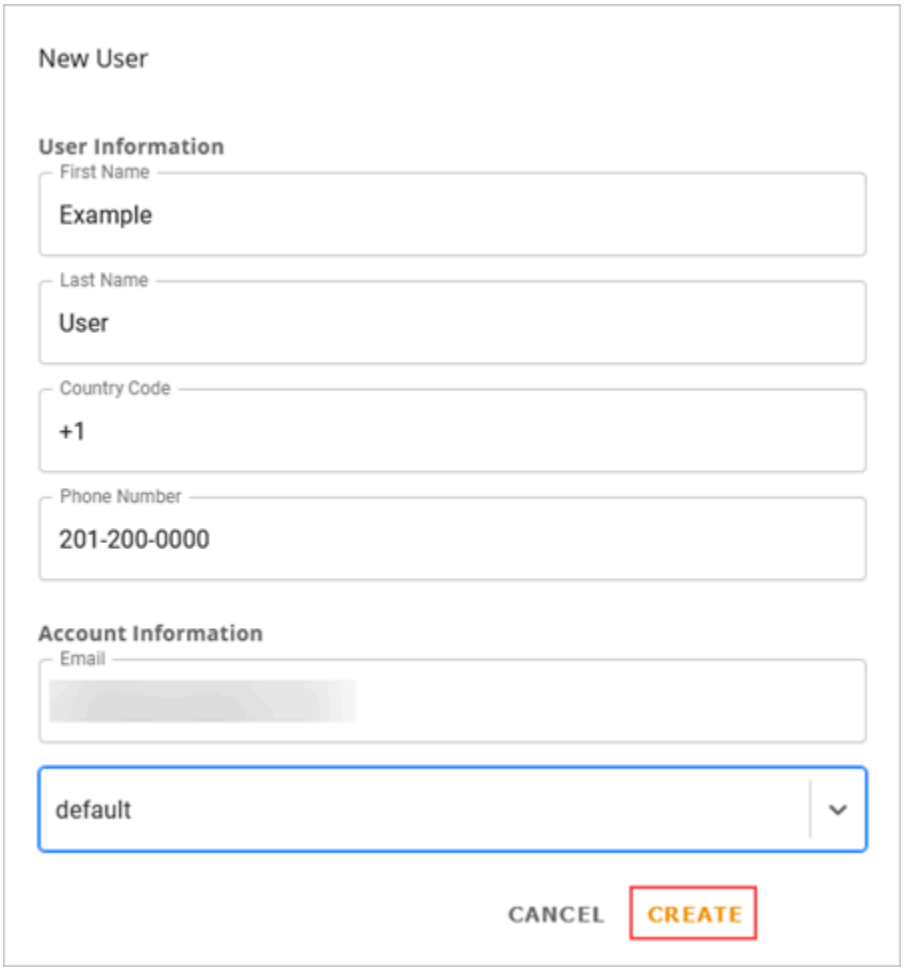
ネットワーク ページ。

特定のネットワークの Wickr 管理コンソールにリダイレクトされます。Wickr 管理コンソールでは、選択した特定のネットワークについて、ユーザーの追加、セキュリティグループの追加、SSO の設定、データ保持の設定、その他の設定を行うことができます。

3. IAM コンソールのナビゲーションペインで、ユーザー、ユーザーの追加 の順に選択します。

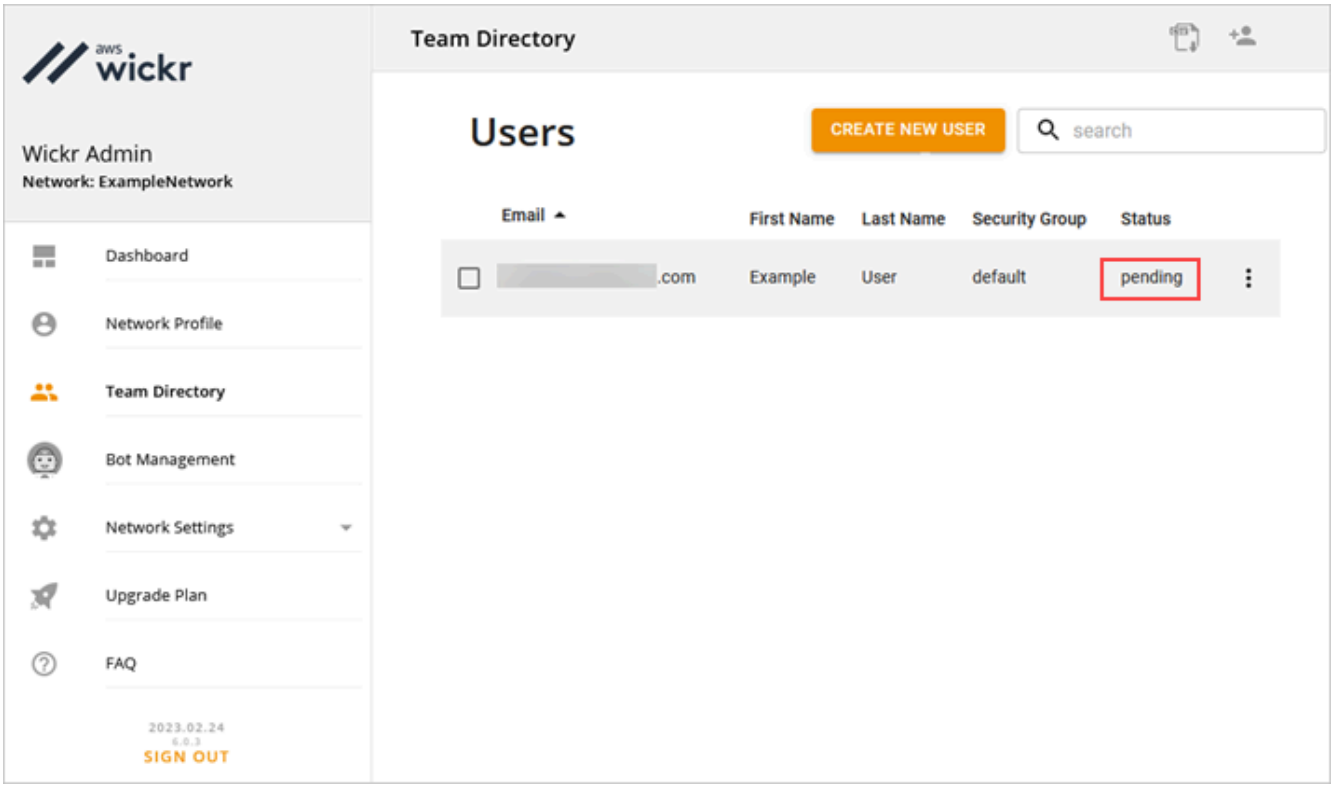
ユーザー ページでは、新規ユーザーを作成 を選択してユーザーを個別に追加できます。上部のナビゲーションペインの ユーザーの追加 アイコンを選択して、ユーザーを一括追加することもできます。CSV のダウンロード アイコンを選択して CSV テンプレートをダウンロードします。このテンプレートを編集して、ユーザーのリストとともにアップロードできます。

4. ユーザーの名、姓、国コード、電話番号、E メールアドレスを入力します。必須のフィールドは E メールアドレスだけです。ユーザーに適したセキュリティグループを必ず選択してください。
5. 作成を選択します。



Wickr は、ユーザーに指定したアドレスに招待 E メールを送信します。この E メールには、Wickr クライアントアプリケーションのダウンロードリンクと Wickr に登録するためのリンクが記載されています。このエンドユーザーエクスペリエンスの詳細については、「AWS Wickr ユーザーガイド」の「Wickr アプリをダウンロードして招待を受ける」を参照してください。

ユーザーが E メール内のリンクを使用して Wickr に登録すると、Wickr チームディレクトリのステータスが 保留中 から アクティブ に変わります。



次のステップ

スタートアップの手順は完了しました。Wickr を管理するには、次のガイドを参照してください。

- AWS Wickr ネットワークの管理
- AWS Wickr でユーザーを管理する

Wickr Pro を AWS Wickr に移行

> **Note**
>
> Wickr Pro は 2024 年 3 月 27 日に廃止されます。

このガイドでは、Wickr Pro から移行して AWS Wickr の使用を開始する方法について説明します。

既存の Wickr Pro ネットワークがあるが、 AWS アカウント まだ持っていない場合は、このガイドの手順に従ってください。サポートが必要な場合は、いつでもサポートに連絡してください。

組織にすでに AWS アカウントがある場合は、「Wickr Pro から AWS Wickr への移行」フォームに記入すると、AWS Wickr サポートがお客様をサポートします。

AWS Wickr ネットワークを として管理するには AWS アカウント ID が必要です AWS のサービス。とは何か、およびアカウントの管理方法の詳細については、 AWS アカウント AWS 「 アカウント管理リファレンスガイド」を参照してください。

トピック

ステップ 1: AWS アカウントを作成する

AWS アカウントを作成するには、以下の手順を実行します。

1. 組織に既存の AWS アカウント ID がない場合は、スタンドアロン AWS アカウント ID を作成することで開始できます。そのために必要になる重要なものがいくつかあります。

   - 請求用のクレジット / デビットカード
   - グループがアクセスできる E メールアドレス (推奨ですが必須ではありません)
   - AWS Support プランを選択します。詳細は変更 AWS Support プランを参照してください。

   > **Note**
   >
   > ニーズの詳細については、いつでも AWS Support プランを変更できます。

2. セキュリティのベストプラクティスとして、IAM を通じて管理アクセスを設定してください (オプションですが推奨)。詳細については、「AWS Identity and Access Management」を参照してください。AWS Wickr 管理アクセスに関する具体的な手順については、「 AWS マネージドポリシー： AWSWickrFullAccess」を参照してください。
3. 前の手順を完了すると、 にログイン AWS Management Console して、アカウント名の下に 12 桁の AWS アカウント ID を見つけることができます。

ステップ 2：Wickr ネットワーク ID を取得する

Wickr ネットワーク ID を取得するには、以下の手順を実行します。

1. 現在の Wickr 管理コンソールにログインし、移行するネットワークを選択し、ネットワークプロファイル を選択します。
2. ネットワークプロファイル ページには、8 桁の数字 ID でネットワーク ID が表示されます。

ステップ 3：リクエストを送信する

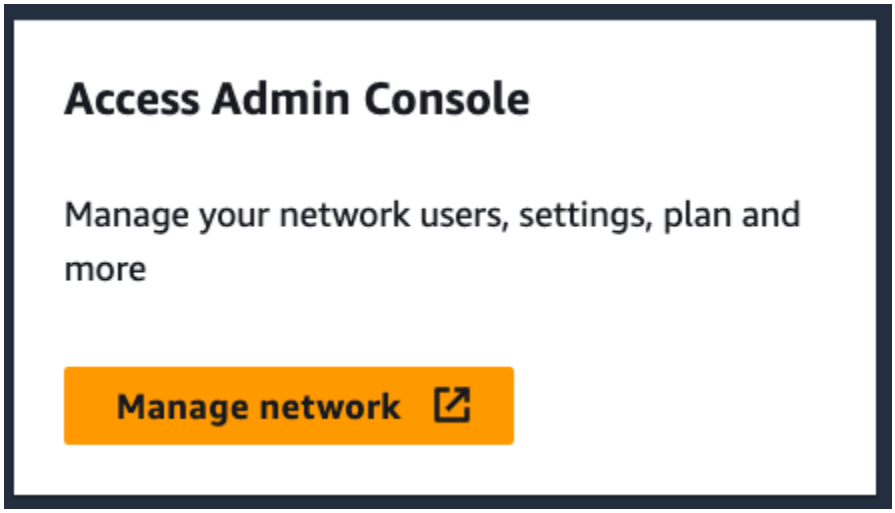
AWS アカウント ID と Wickr Pro ネットワーク ID を取得したので、Wickr Pro から AWS Wickr への移行フォームを完了する必要があります。

完了すると、通常 14 日以内に、AWS Wickr サポート担当者がお客様に連絡し、Wickr ネットワークが AWS アカウントに追加されたことを確認します。

ステップ 4: AWS コンソールにログインする

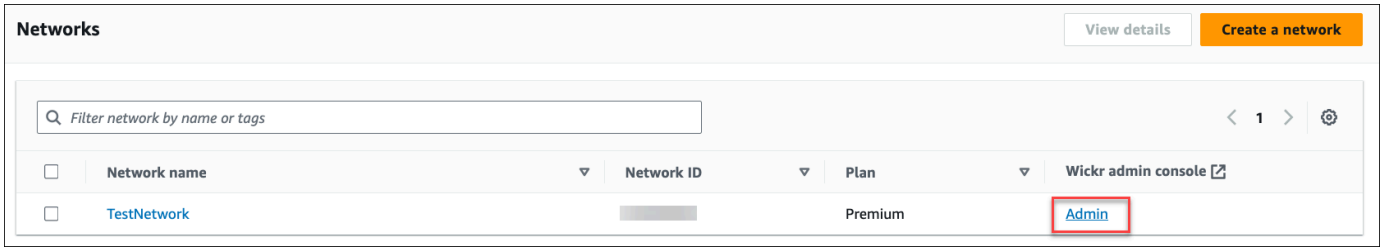
> **Note**
>
> Wickr Pro ネットワークが AWS アカウントに追加されたことを確認したら、次の手順に従います。

1. AWS Wickr のステップ 2 で作成したルートユーザーまたは IAM ユーザー (推奨) を使用して AWS 、コンソールにログインできます。
2. AWS Wickr サービスに移動します。これを行うには、サービス メニューから、または検索バーで AWS Wickr を検索します。
3. AWS Wickr ページで ネットワークの管理 を選択して Wickr ネットワークリストにアクセスします。



ネットワークの管理 ボタン。

4. ネットワーク ページの Wickr 管理コンソール 列で、目的のネットワーク名の右にある管理リンクを選択します。



管理コンソールのリンク。

5. これで、移行は完了です。Wickr ネットワークダッシュボードが表示されます。

これで、ネットワークの請求が AWS アカウントに転送されます。サポートから確認が届くまでに最大 3 営業日かかります。確認を受け取ったら、 AWS コンソールから 請求書を表示して支払いを行うことができます。

AWS Wickr ネットワークの管理

AWS Management Console for Wickrのネットワーク設定セクションでは、Wickrのネットワーク名、セキュリティグループ、SSO設定、およびデータ保持設定を管理できます。

トピック

ネットワークプロファイル

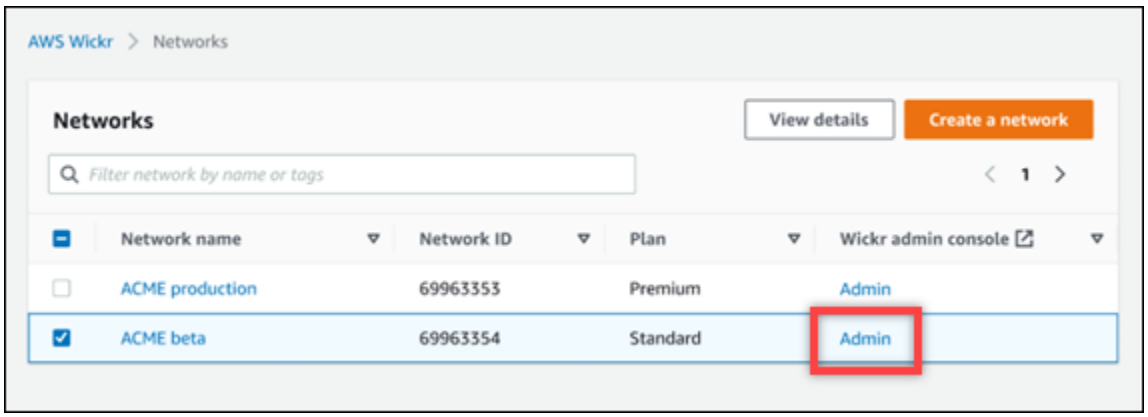
Wickr ネットワークの名前を編集し、for Wickr の「ネットワークプロファイル」セクションでネットワーク ID を表示できます。 AWS Management Console

トピック

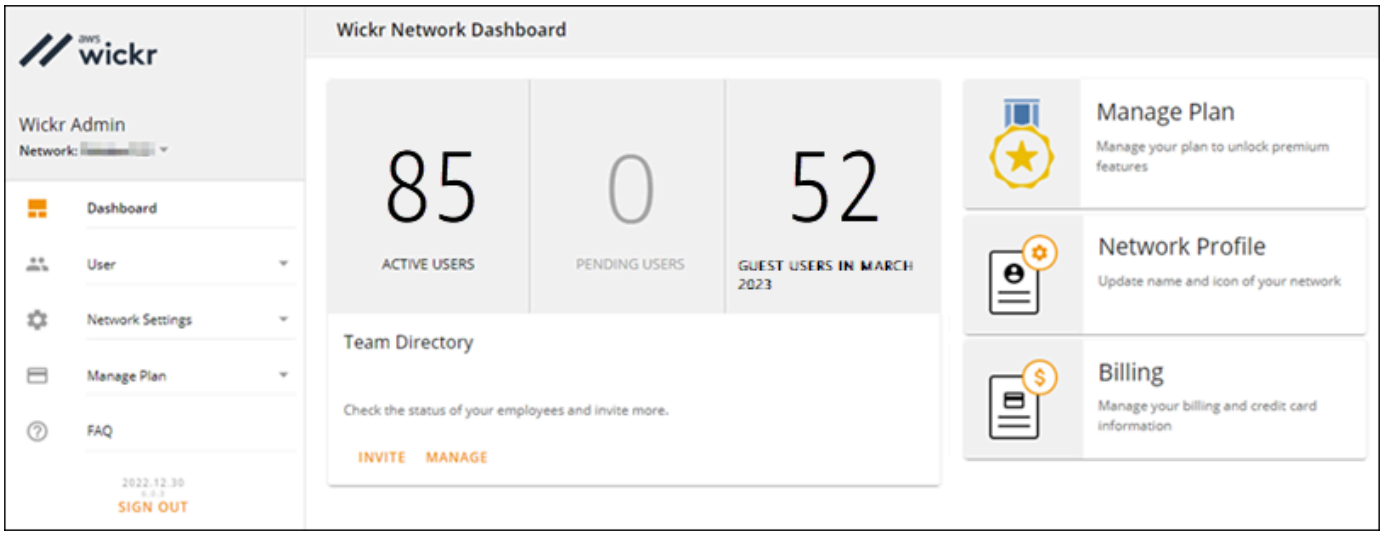
ネットワークプロファイルの表示

Wickr ネットワークプロファイルとネットワーク ID を表示するには、以下の手順を実行します。

1. https://console.aws.amazon.com/wickr/ で For Wickr を開いてください AWS Management Console 。
2. ネットワーク ページで 管理 リンクを選択し、そのネットワークの Wickr 管理コンソールに移動します。



特定のネットワークの Wickr 管理コンソールにリダイレクトされます。



3. Wickr 管理コンソールのナビゲーションペインで ネットワーク設定 を選択し、ネットワークプロファイル を選択します。

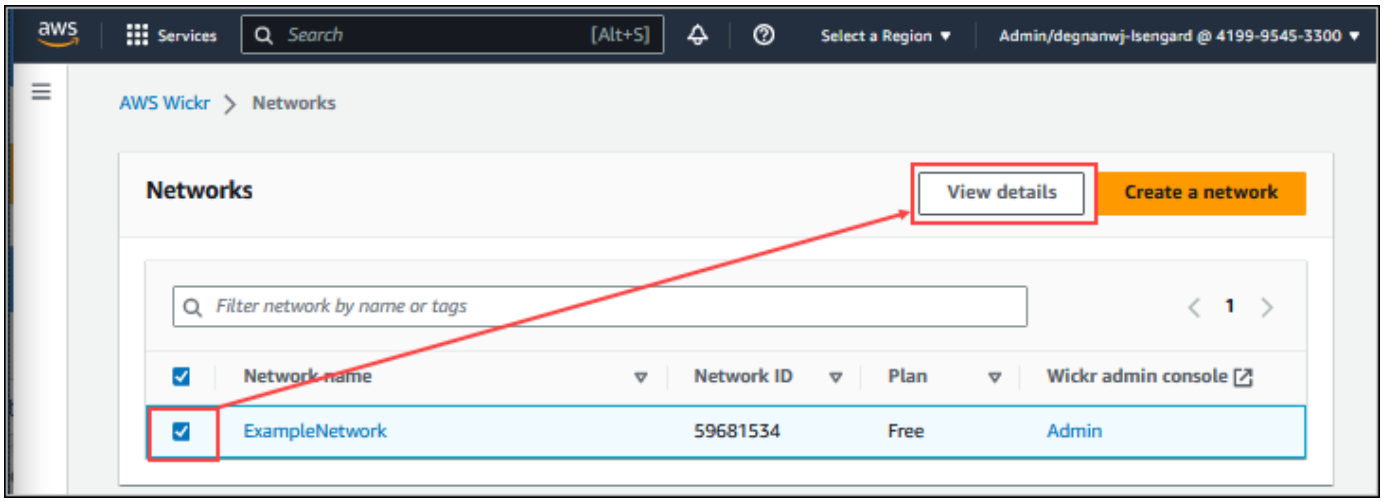
   ネットワークプロファイル ページには、Wickr ネットワーク名とネットワーク ID が表示されます。ネットワーク ID を使用してフェデレーションを設定できます。

ネットワーク名の編集

Wickr ネットワーク名を編集するには、以下の手順を実行します。

1. https://console.aws.amazon.com/wickr/ で AWS Management Console Wickr 用を開いてください。
2. ネットワークの管理 を選択します。

3. [ネットワーク] ページで、編集するネットワーク名の横にあるチェックボックスを選択し、[詳細を表示] を選択します。



4. [ネットワーク概要] セクションで、[編集] を選択します。
5. [ネットワーク名] テキストボックスに新しいネットワーク名を入力します。
6. [変更を保存] を選択して、新しいネットワーク名を保存します。

セキュリティグループ

AWS Management Console for Wickr の「セキュリティグループ」セクションでは、セキュリティグループとその設定 (パスワードの複雑性ポリシー、メッセージ設定、通話機能、セキュリティ機能、ネットワークフェデレーションなど) を管理できます。

トピック

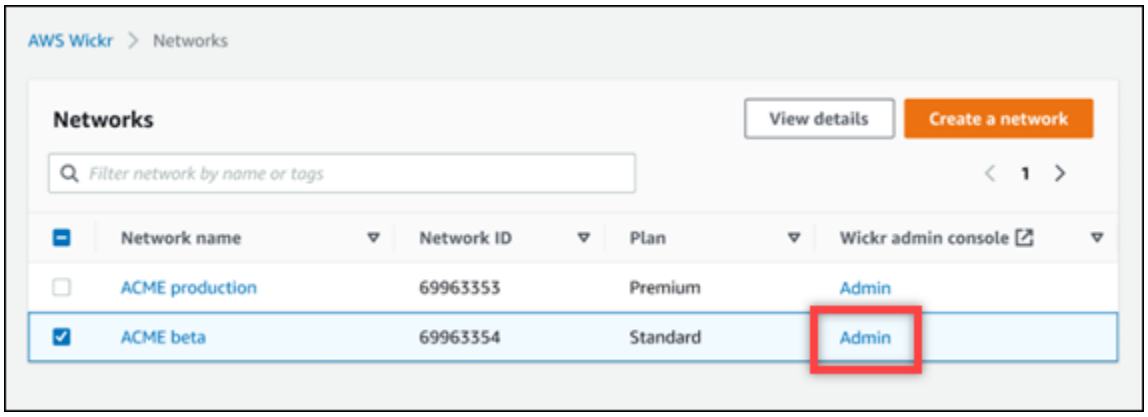
- セキュリティグループの表示
- セキュリティグループの作成
- セキュリティグループを編集する
- セキュリティグループを削除する

セキュリティグループの表示

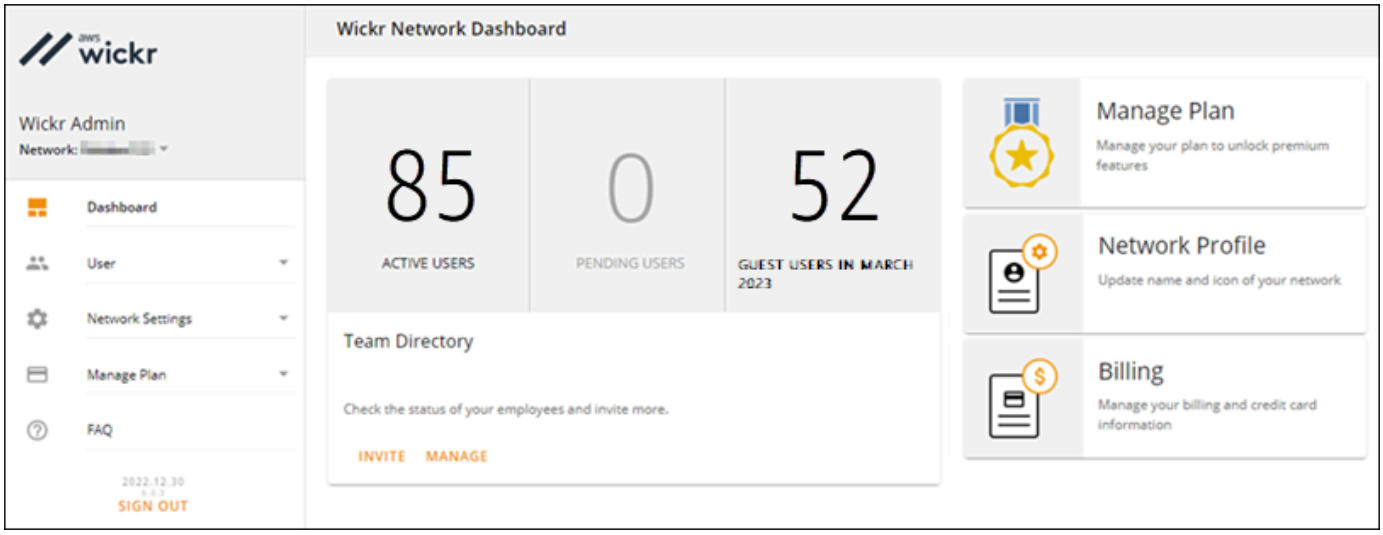
セキュリティグループを表示するには、以下の手順を実行します。

1. https://console.aws.amazon.com/wickr/ で AWS Management Console for Wickr を開いてください。

2. ネットワーク ページで 管理 リンクを選択し、そのネットワークの Wickr 管理コンソールに移動します。



特定のネットワークの Wickr 管理コンソールにリダイレクトされます。



3. Wickr 管理コンソールのナビゲーションペインで ネットワーク設定 を選択し、セキュリティグループ を選択します。

セキュリティグループ ページには現在の Wickr セキュリティグループが表示され、詳細を表示したり、新しいグループを作成したりできます。

セキュリティグループの作成

以下の手順でセキュリティグループを作成します。

1. https://console.aws.amazon.com/wickr/ で AWS Management Console Wickr 用を開いてください。

2. ネットワーク ページで 管理 リンクを選択し、そのネットワークの Wickr 管理コンソールに移動します。

   特定のネットワークの Wickr 管理コンソールにリダイレクトされます。
3. Wickr 管理コンソールのナビゲーションペインで ネットワーク設定 を選択し、セキュリティグループ を選択します。
4. 新しいセキュリティグループを作成するには、新しいグループ を選択します。

   デフォルト名の新しいセキュリティグループがセキュリティグループリストに自動的に追加されます。

   新しいセキュリティグループの編集の詳細については、セキュリティグループを編集するを参照してください。

セキュリティグループを編集する

セキュリティグループを編集するには、以下の手順を実行します。

1. https://console.aws.amazon.com/wickr/ で AWS Management Console Wickr 用を開いてください。
2. ネットワーク ページで 管理 リンクを選択し、そのネットワークの Wickr 管理コンソールに移動します。

   特定のネットワークの Wickr 管理コンソールにリダイレクトされます。
3. Wickr 管理コンソールのナビゲーションペインで ネットワーク設定 を選択し、セキュリティグループ を選択します。
4. 編集するセキュリティグループ名の横にある 詳細 を選択します。

   セキュリティグループの詳細 ページには、セキュリティグループの設定がさまざまなタブに表示されます。
5. 次のタブと対応する設定を使用できます。

   - セキュリティグループ名：グループ名の横にある鉛筆アイコンを選択して名前を編集します。
   - 全般：グループの基本設定を編集します。
   - メッセージング：グループメンバーのメッセージ機能を管理します。
   - 通話：グループメンバーの通話機能を管理します。
   - セキュリティ：グループに追加のセキュリティ機能を設定します。

- フェデレーション：ネットワーク間の通信機能。これはネットワークの管理コンソールでセキュリティグループレベルで設定できます。AWS Wickr には、ローカルとグローバルの 2 種類のフェデレーションがあります。
  - ローカルフェデレーション：同じリージョン内の他のネットワークの AWS ユーザーとフェデレートする機能。たとえば、カナダにローカルフェデレーションが有効になっている 2 つのネットワークがある場合、それらは相互に通信できます。
  - グローバルフェデレーション：Enterprise ユーザーや他の地域に属する別のネットワークの AWS ユーザーとフェデレートする機能。たとえば、カナダ地域のネットワークにユーザーがいて、ロンドン地域のネットワークにユーザーがいて、両方のネットワークでグローバルフェデレーションがオンになっている場合、両者は相互に通信できます。
  - 制限付きフェデレーション — 異なる地域に属する特定のネットワーク (エンタープライズまたは AWS) とフェデレーションできます。管理者は、ユーザーがフェデレーションできる特定のネットワークを許可リストに追加できます。制限後、ユーザーは許可リストに登録されているネットワークのユーザーとのみ通信できます。制限付きフェデレーションを使用するには、両方のネットワークがフェデレーションタブのセキュリティグループ設定から相互に許可リストに登録する必要があります。

6. 保存 を選択すると、セキュリティグループの詳細に加えた編集内容が保存されます。

セキュリティグループを削除する

セキュリティグループを削除するには、以下の手順に従ってください。

1. https://console.aws.amazon.com/wickr/ で AWS Management Console for Wickr を開いてください。
2. ネットワーク ページで 管理 リンクを選択し、そのネットワークの Wickr 管理コンソールに移動します。

   特定のネットワークの Wickr 管理コンソールにリダイレクトされます。
3. Wickr 管理コンソールのナビゲーションペインで ネットワーク設定 を選択し、セキュリティグループ を選択します。
4. 削除するセキュリティグループ名の横にある縦の省略記号アイコンを選択します。
5. 削除 を選択してセキュリティグループを削除します。

ユーザーが割り当てられているセキュリティグループを削除すると、そのユーザーはデフォルトのセキュリティグループに自動的に追加されます。ユーザーに割り当てられたセキュリティグループを変更するには、「ユーザーの編集」を参照してください。

シングルサインオン設定

AWS Management Console for Wickr の SSO 設定セクションでは、シングルサインオンシステムを使用して認証を行うように Wickr を設定できます。SSO は、適切な多要素認証 (MFA) システムと組み合わせると、セキュリティを強化します。Wickr は、OpenID Connect (OIDC) を使用する SSO プロバイダーのみをサポートしています。Security Assertion Markup Language (SAML) を使用するプロバイダーはサポートされていません。

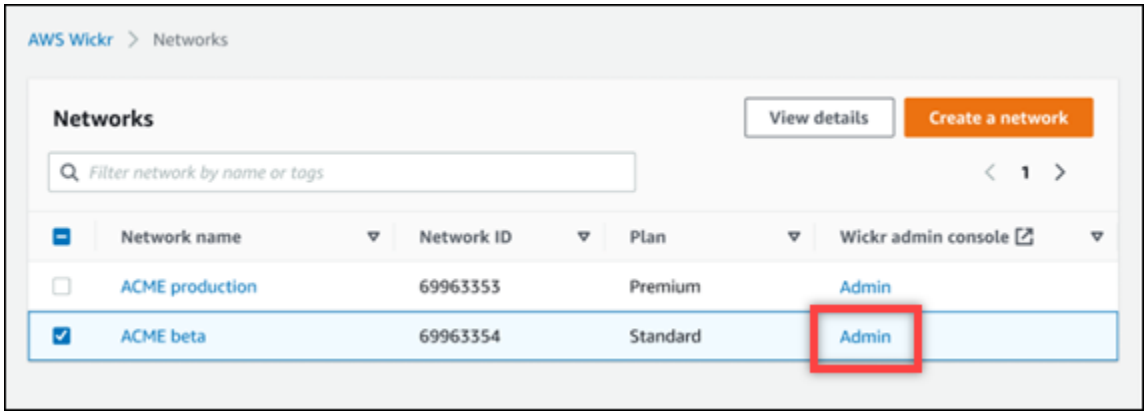
トピック

- SSO の詳細の表示
- SSO の設定
- トークン更新の猶予期間

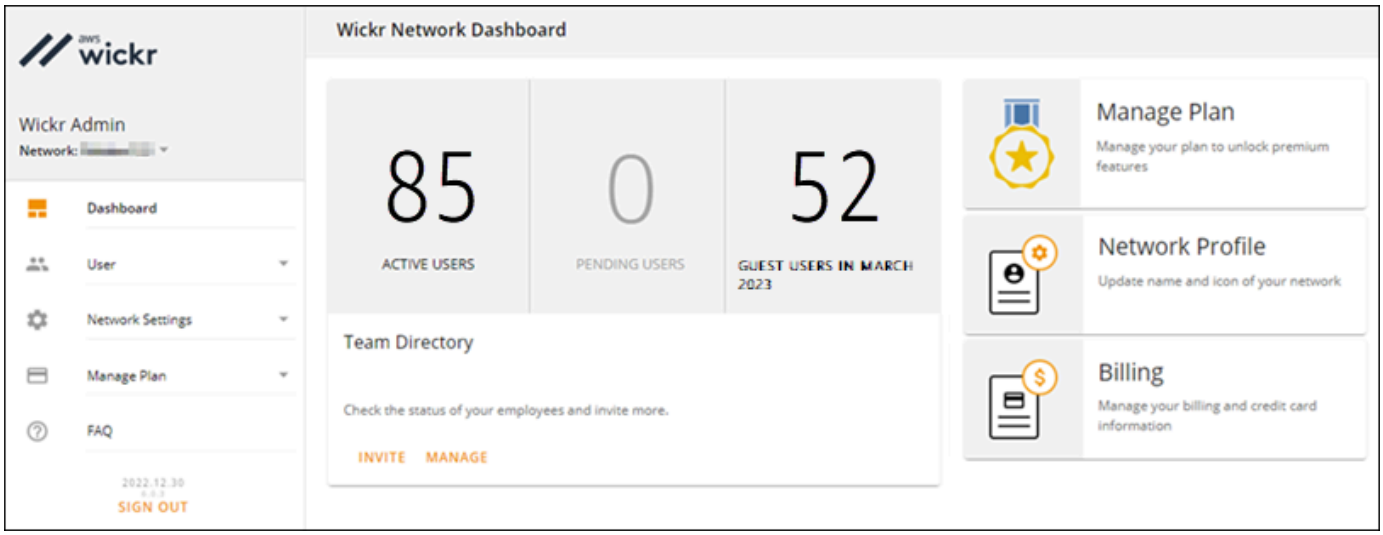
SSO の詳細の表示

Wickr ネットワークの現在のシングルサインオン設定を表示するには、次の手順を実行します。Wickr ネットワークのネットワークエンドポイントを表示することもできます。

1. https://console.aws.amazon.com/wickr/ AWS Management Console で for Wickr を開いてください。
2. ネットワーク ページで 管理 リンクを選択し、そのネットワークの Wickr 管理コンソールに移動します。



特定のネットワークの Wickr 管理コンソールにリダイレクトされます。



3. Wickr 管理コンソールのナビゲーションペインで ネットワーク設定 を選択し、SSO 設定 を選択します。

   シングルサインオンと LDAP 設定 ページには、Wickr ネットワークエンドポイントと現在の SSO 設定が表示されます。

SSO の設定

SSO の設定の詳細については、Wickr ヘルプセンターの次のガイドを参照してください。

> **Important**
>
> SSO を設定するときに Wickr ネットワークの会社 ID を指定します。Wickr ネットワークの会社 ID を必ず書き留めてください。招待 E メールを送信するときは、エンドユーザーに提供する必要があります。エンドユーザーは、Wickr ネットワークに登録する際に会社 ID を指定する必要があります。

- Azure AD シングルサインオンの設定
- Okta シングルサインオンの設定

トークン更新の猶予期間

ID プロバイダーが一時的または長期的に停止し、クライアントセッションの更新トークンが失敗したためにユーザーが予期せずログアウトすることがあります。この問題を防ぐには、停止中にクライアント更新トークンに障害が発生しても、ユーザーがサインインしたままになる猶予期間を設定できます。

猶予期間に使用できるオプションは次のとおりです。

- 猶予期間なし（デフォルト）：更新トークンが失敗すると、ユーザーはすぐにサインアウトされます。
- 30 分の猶予期間：更新トークンが失敗した後も、ユーザーは最大 30 分間サインインしたままになります。
- 60 分の猶予期間：更新トークンが失敗した後も、ユーザーは最大 60 分間サインインしたままになります。

ネットワークタグの管理

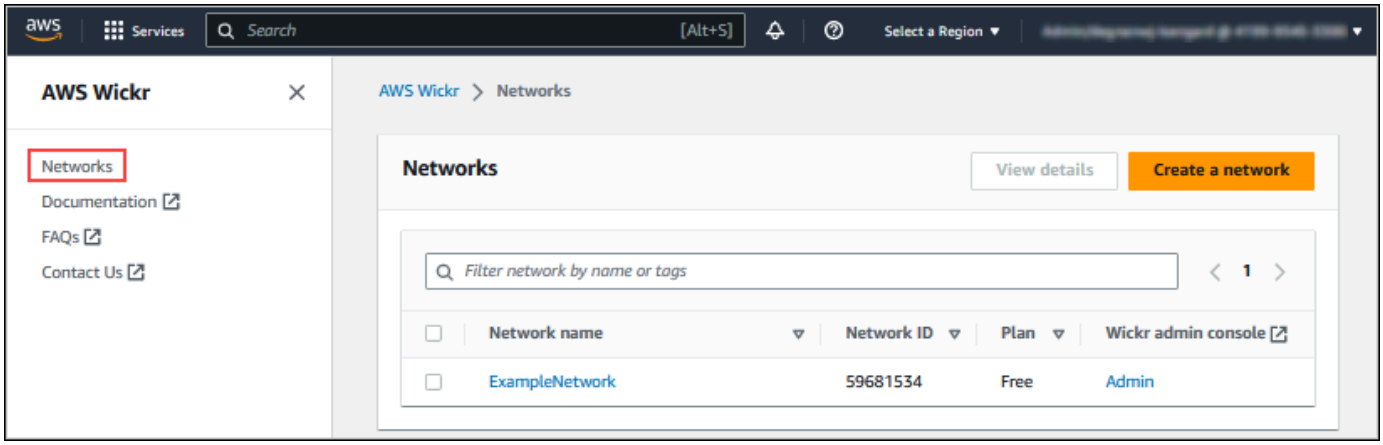
Wickr ネットワークにタグを適用できます。その後、これらのタグを使用して Wickr ネットワークを検索およびフィルタリングしたり、コストを追跡したりできます。 AWS AWS Management Console for Wickr のネットワーク概要ページでネットワークタグを設定できます。

タグはリソースに適用されるキーと値のペアで、そのリソースに関するメタデータを保持します。各タグは、キーと値からなるラベルです。タグの詳細については、「タグとは」および「タグ付けのユースケース」も参照してください。

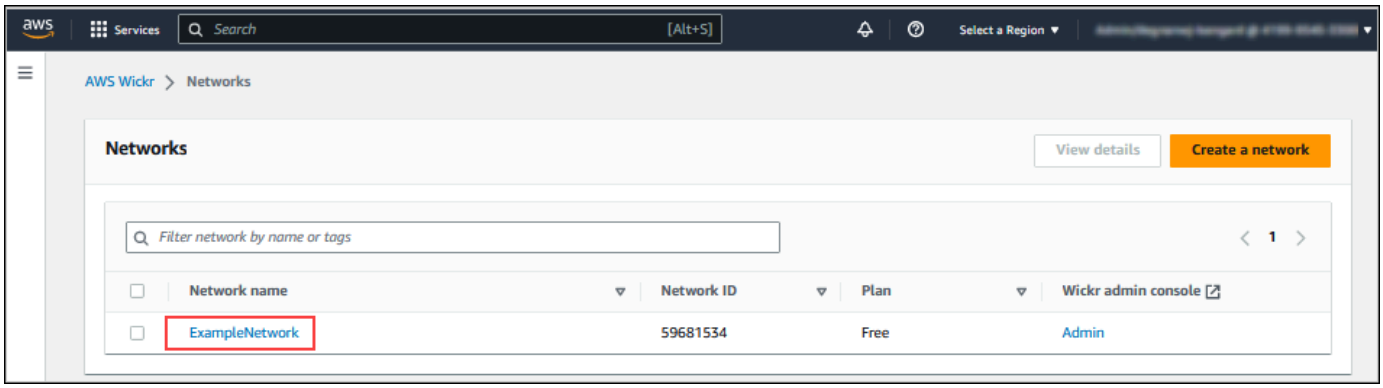
ネットワークタグの管理

Wickr ネットワークのネットワークタグを管理するには、以下の手順を実行します。

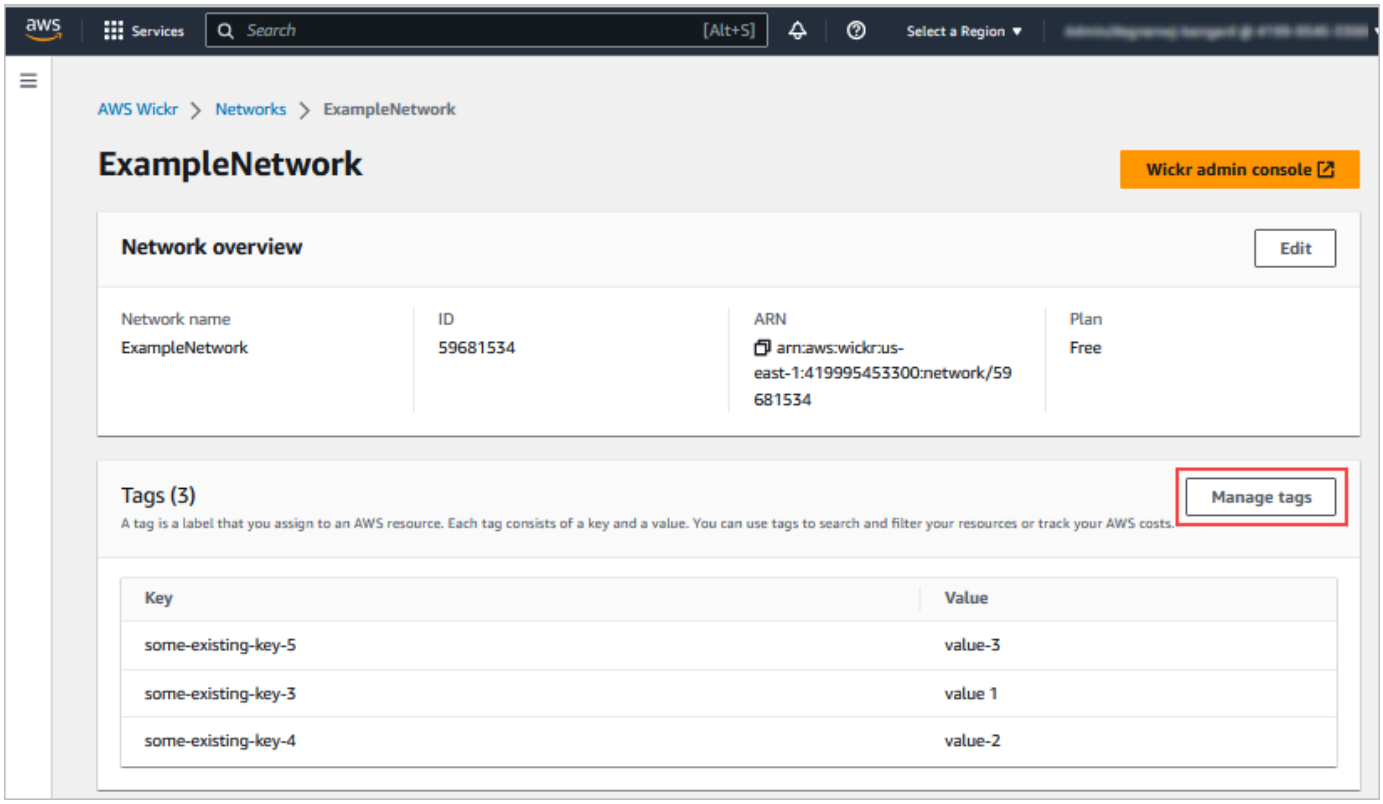
1. https://console.aws.amazon.com/wickr/ で AWS Management Console for Wickr を開きます。
2. Wickr 用 AWS Management Console のナビゲーションペインから ネットワーク を選択します。



3. ネットワーク ページで、タグを管理するネットワークの名前を選択します。



4. ネットワーク概要 ページで、タグの管理 を選択します。



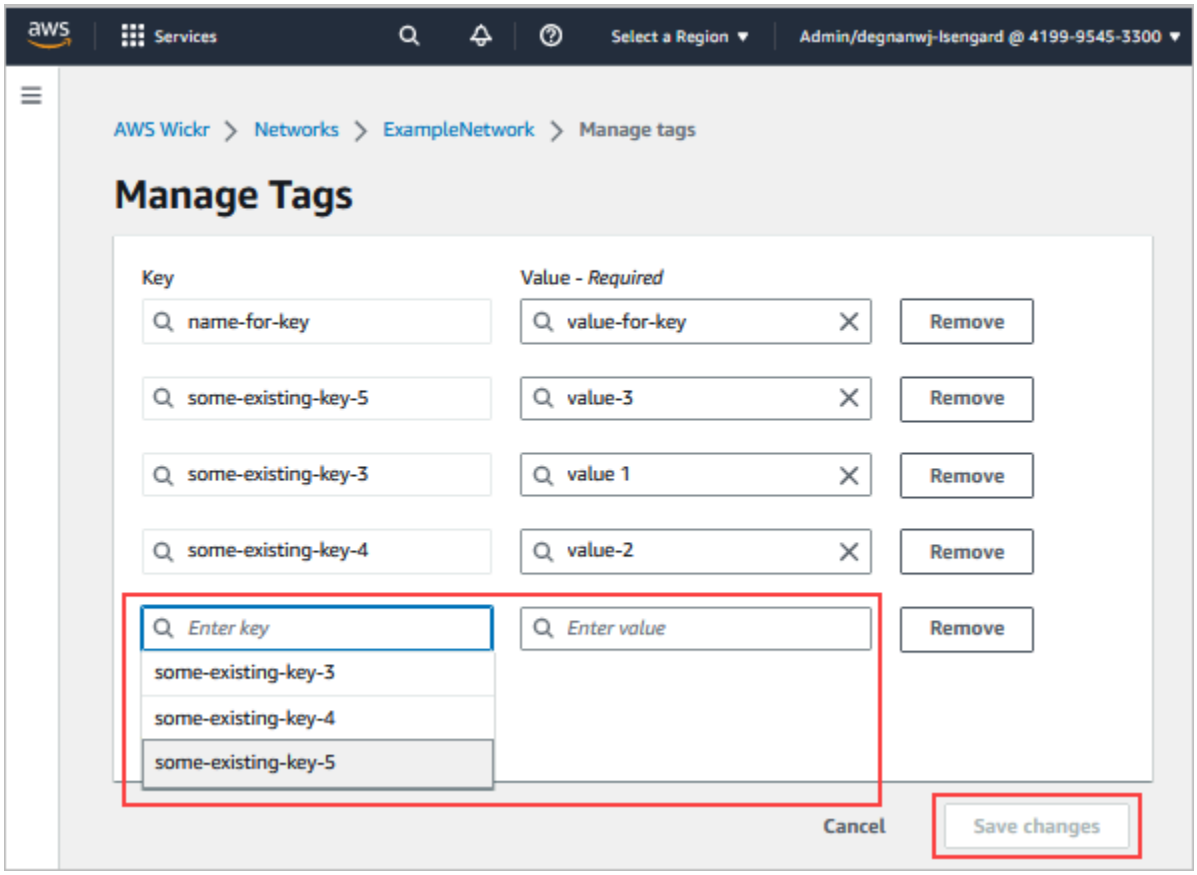
5. タグの管理 ページでは、以下のいずれかのオプションを設定できます。

   - 新しいタグの追加：新しいタグをキーと値のペアの形式で入力します。新しいタグの追加 を選択して、複数のキーと値のペアを追加します。タグは、大文字と小文字が区別します。詳細については、「ネットワークタグの追加」を参照してください。
   - 既存のタグの編集：既存のタグのキーまたは値のテキストを選択し、テキストボックスに変更内容を入力します。詳細については、「ネットワークタグの編集」を参照してください。
   - 既存のタグの削除：削除するタグの横に表示されている 削除 ボタンを選択します。詳細については、「ネットワークタグの削除」を参照してください。

ネットワークタグの追加

Wickr ネットワークにタグを追加するには、以下の手順を実行します。タグの管理の詳細については、「ネットワークタグの管理」を参照してください。

1. タグの管理ページで、タグの追加を選択します。
2. 表示される空の キー フィールドと 値 フィールドに、新しいタグキーと値を入力します。
3. 変更の保存を選択して設定を保存します。

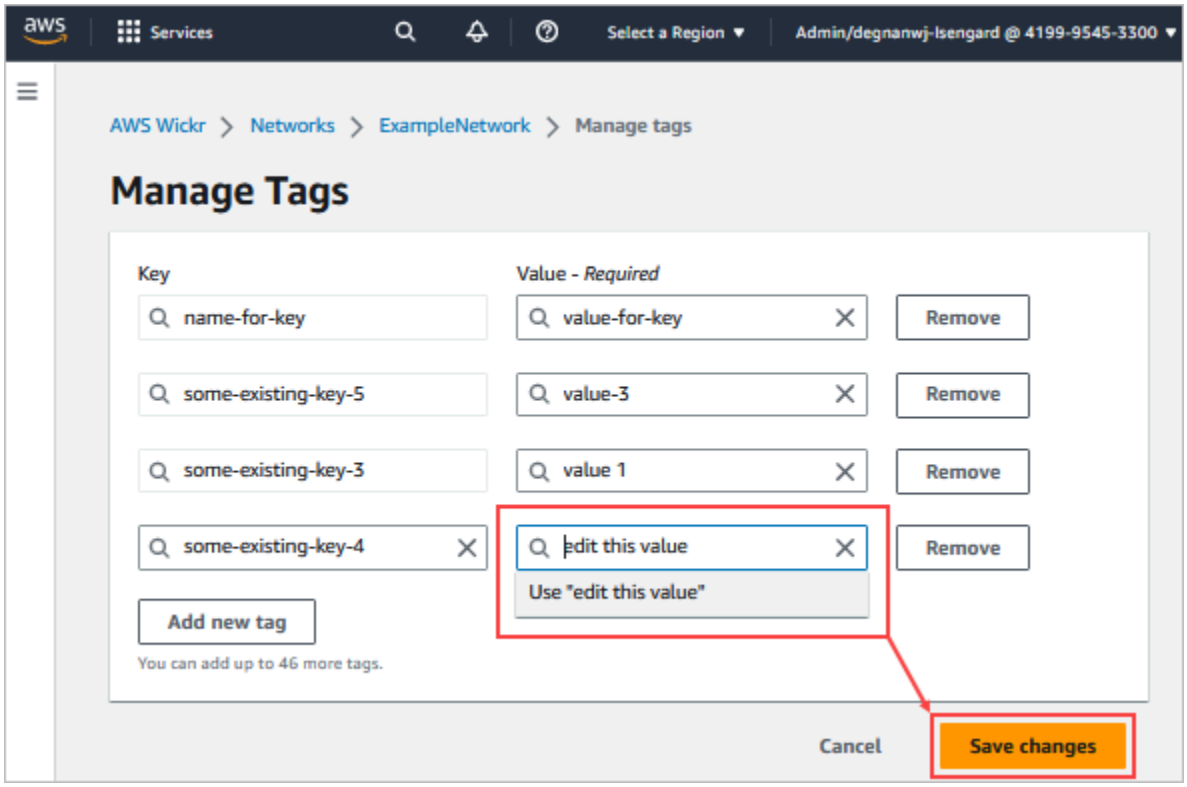


ネットワークタグの編集

Wickr ネットワークに関連付けられたタグをの編集するには、以下の手順を実行します。タグの管理の詳細については、「ネットワークタグの管理」を参照してください。

1. タグの管理 ページで、タグの値を編集します。

> **Note**
>
> タグのキーは編集できません。代わりに、キーと値のペアを削除し、新しいキーを使用して新しいタグを追加してください。

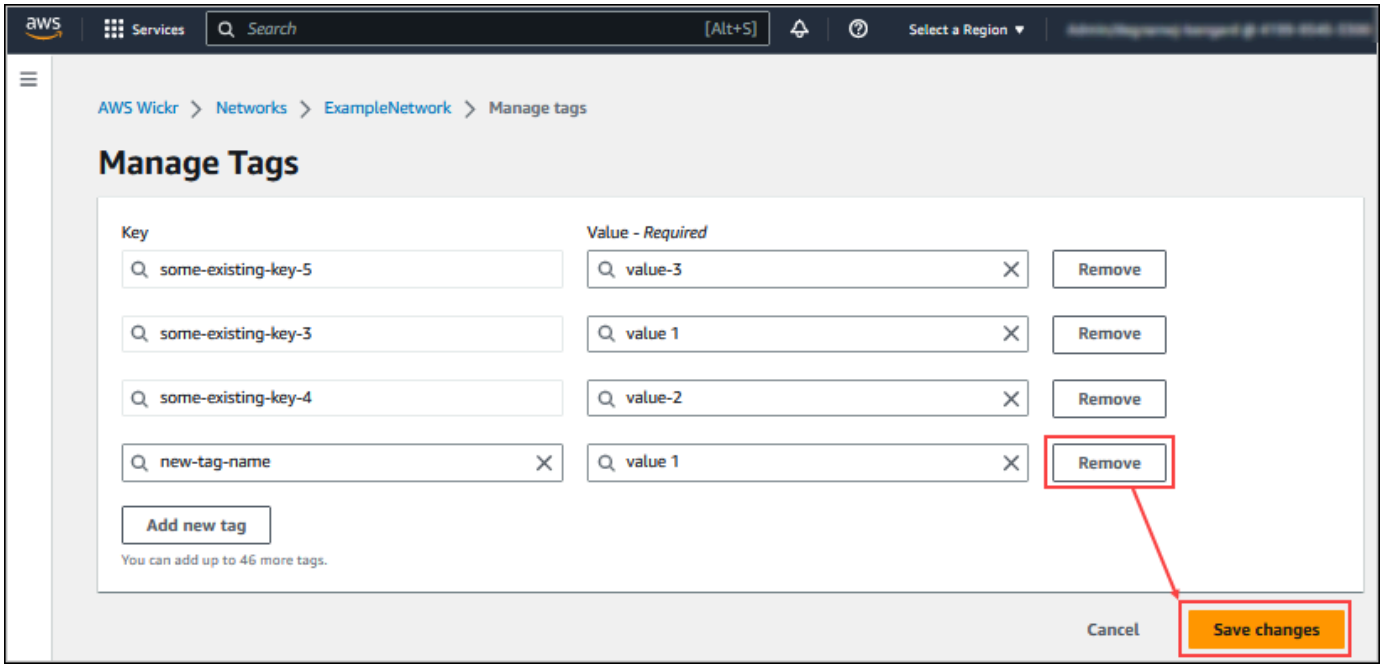


2. 変更の保存 を選択してタグを保存します。

ネットワークタグの削除

Wickr ネットワークにタグを削除するには、以下の手順を実行します。タグの管理の詳細については、「ネットワークタグの管理」を参照してください。

1. タグの管理 ページで、削除する各タグの横にある 削除 を選択します。



2. 変更の保存 を選択してタグを保存します。

ネットワークプランを管理

AWS Management Console for Wickr の「プランの管理」セクションでは、ビジネスニーズに基づいてネットワークプランを管理できます。

ネットワークプランを管理するには、以下の手順を実行してください。

1. https://console.aws.amazon.com/wickr/ で AWS Management Console for Wickr を開きます。
2. Wickr 管理コンソールのナビゲーションペインで、「プランを管理」を選択し、「マイプラン」を選択します。
3. My Plan ページで、ご希望のネットワークプランを選択します。現在のネットワークプランは、次のいずれかを選択して変更できます。

   - 標準 — 管理上の制御と柔軟性を必要とする小規模および大規模の企業チーム向け。
   - プレミアムまたはプレミアムの無料トライアル — 最大限の機能制限、きめ細かな管理制御、データ保持を必要とする企業向け。

     管理者はプレミアム無料トライアルオプションを選択できます。このトライアルは最大 30 ユーザーが利用でき、有効期間は 3 か月です。このオファーは、新しいレガシーフリートライアルプランとスタンダードプランが対象です。管理者は、プレミアム無料トライアル期間中

にプレミアムプランまたはスタンダードプランにアップグレードまたはダウングレードできます。

> **Note**
>
> ネットワークの使用や請求を停止するには、利用停止中のユーザーを含むすべてのユーザーをネットワークから削除します。

プレミアム無料トライアルの制限

プレミアム無料トライアルには以下の制限が適用されます。

- 以前にプレミアム無料トライアルに登録されたことがあるプランは、別のトライアルの対象にはなりません。
- プレミアム無料トライアルには、 AWS アカウントごとに 1 つのネットワークしか登録できません。
- プレミアム無料トライアル中は、ゲストユーザー機能は使用できません。
- 標準ネットワークのユーザー数が 30 人を超える場合、プレミアム無料トライアルにアップグレードすることはできません。

データ保持

AWS Wickr データ保持では、ネットワーク内のすべての会話を保持できます。これには、直接的なメッセージの会話や、ネットワーク内 (内部) のメンバーと、ネットワークが連携している他のチーム (外部) のメンバーとの間でのグループやルームでの会話が含まれます。データ保持は、AWS Wickr Premium プランのユーザーと、データ保持を選択した企業のお客様のみが利用できます。Premium プランの詳細については、「Wickr 料金表」を参照してください。

ネットワーク管理者がネットワークのデータ保持を設定して有効にすると、ネットワーク内で共有するすべてのメッセージとファイルは、組織のコンプライアンスポリシーに従って保持されます。これらの .txt ファイル出力には、外部の場所 (ローカルストレージ、Amazon S3 バケット、またはユーザーが選択したその他のストレージ) からネットワーク管理者がアクセスでき、そこから分析、消去、または転送できます。

> **Note**
>
> Wickr がメッセージやファイルにアクセスすることはありません。したがって、データ保持システムを設定するのはユーザーの責任です。

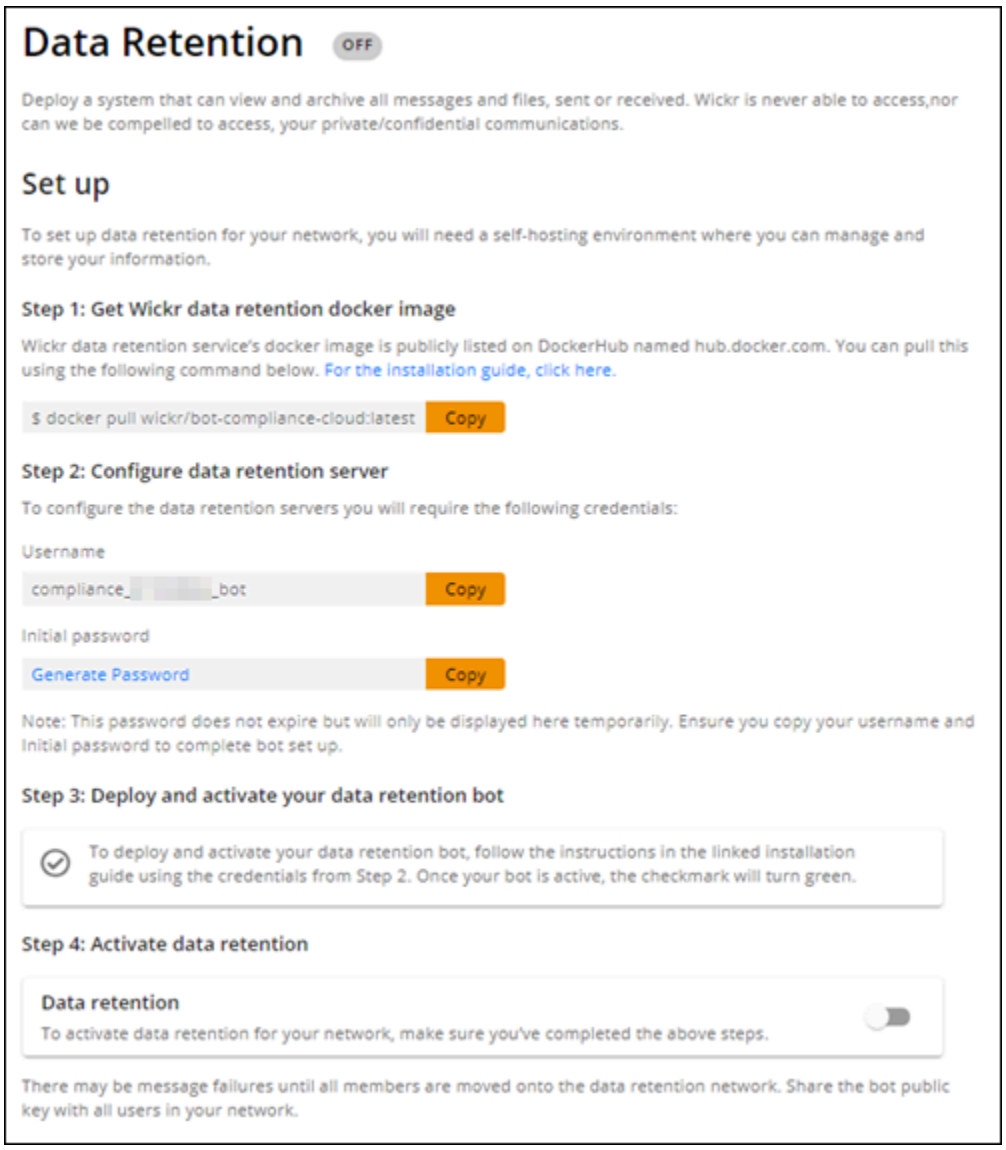
トピック

データ保持の詳細を表示する

Wickr ネットワークのデータ保持の詳細を表示するには、以下の手順を実行します。Wickr ネットワークのデータ保持を有効または無効にすることもできます。

1. https://console.aws.amazon.com/wickr/ で AWS Management Console For Wickr を開いてください。
2. ネットワークの管理 を選択します。
3. Wickr 管理コンソールのナビゲーションペインで ネットワーク設定 を選択し、データ保持 を選択します。

   データ保持 ページには、データ保持の設定手順と、データ保持機能を有効または無効にするオプションが表示されます。データ保持の設定については、データ保持を設定する を参照してください。



> **Note**
>
> データ保持機能を有効にすると、データ保持がオンになっています というメッセージがネットワーク内のすべてのユーザーに表示され、保持が有効なネットワークであることが通知されます。

データ保持を設定する

AWS Wickr ネットワークのデータ保持を設定するには、データ保持ボット Docker イメージを、ローカルコンピュータや Amazon Elastic Compute Cloud (Amazon EC2) 内のインスタンスなどのホ

スト上のコンテナにデプロイする必要があります。ボットをデプロイしたら、データをローカルまたは Amazon Simple Storage Service (Amazon S3) バケットに格納するように設定できます。(Secrets Manager)、Amazon AWS Secrets Manager ()、Amazon Simple Notification Service (Amazon SNS CloudWatch CloudWatch ）、 AWS Key Management Service () などの他の AWSサービスを使用するようにデータ保持ボットを設定することもできますAWS KMS。 Amazon SNS 以下のトピックでは、Wickr ネットワークのデータ保持ボットを設定して実行する方法について説明します。

トピック

データ保持を設定するための前提条件

開始する前に、AWS Management Console Wickr からデータ保持ボット名 (ユーザー名 というラベルが付いている) と初期パスワードを取得する必要があります。データ保持ボットを初めて起動するときは、これらの値の両方を指定する必要があります。また、コンソールでデータ保持を有効にする必要があります。詳細については、「データ保持の詳細を表示する」を参照してください。

パスワード

データ保持ボットを初めて起動するときは、次のいずれかのオプションを使用して初期パスワードを指定します。

- `WICKRIO_BOT_PASSWORD` 環境変数。データ保持ボットの環境変数については、環境変数 本ガイドの後のセクションで概説しています。
- `AWS_SECRET_NAME` 環境変数によって識別される Secrets Manager の パスワード 値。データ保持ボットの Secrets Manager の値については、Secrets Manager の価値観 このガイドの後のセクションで概説されています。
- データ保持ボットのプロンプトが表示されたら、パスワードを入力します。`-ti` オプションを使用してインタラクティブな TTY アクセスでデータ保持ボットを実行する必要があります。

データ保持ボットを初めて設定すると、新しいパスワードが生成されます。データ保持ボットを再インストールする必要がある場合は、生成されたパスワードを使用します。データ保持ボットを初めてインストールした後は、初期パスワードは無効になります。

新しく生成されたパスワードは、次の例のように表示されます。

> **Important**
>
> パスワードを安全な場所に保存します。パスワードを紛失した場合、データ保持ボットを再インストールすることはできません。このパスワードは共有しないでください。Wickr ネットワークのデータ保持を開始できるようになります。

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

ストレージのオプション

データ保持が有効になり、データ保持ボットが Wickr ネットワークに設定されると、ネットワーク内で送信されるすべてのメッセージとファイルがキャプチャされます。メッセージは、環境変数を使用して設定できる特定のサイズまたは時間制限に制限されたファイルに保存されます。詳細については、「環境変数」を参照してください。

このデータを保存するには、次のオプションのいずれかを設定できます。

- キャプチャしたメッセージとファイルをすべてローカルに保存します。これがデフォルトのオプションです。ローカルファイルを別のシステムに移動して長期保存し、ホストディスクのメモリやスペースが不足しないようにするのはユーザーの責任です。
- キャプチャしたすべてのメッセージとファイルを Amazon S3 バケットに格納します。データ保持ボットは、復号されたすべてのメッセージとファイルを、指定した Amazon S3 バケットに保存します。キャプチャされたメッセージとファイルは、バケットに正常に保存されるとホストマシンから削除されます。
- キャプチャしたすべてのメッセージとファイルを Amazon S3 バケットに暗号化して保存します。データ保持ボットは、キャプチャされたすべてのメッセージとファイルを指定したキーを使用して再暗号化し、指定した Amazon S3 バケットに保存します。キャプチャされたメッセージとファイ

ルは、再暗号化に成功してバケットに保存されると、ホストマシンから削除されます。メッセージとファイルを復号化するにはソフトウェアが必要です。

Amazon S3 バケットの作成の詳細については、Amazon S3 ユーザーガイドの「バケットの作成」を参照してください。

環境変数

次の環境変数を使用して、データ保持ボットを構成できます。これらの環境変数は、データ保持ボットの Docker イメージを実行するときの -e オプションを使用して設定します。詳細については、「データ保持ボットを起動する」を参照してください。

> **Note**
>
> これらの環境変数は、特に指定がない限りオプションです。

以下の環境変数を使用して、データ保持ボットの認証情報を指定します。

- WICKRIO_BOT_NAME — データ保持ボットの名前。この変数は、データ保持ボットの Docker イメージを実行する場合に 必要 です。
- WICKRIO_BOT_PASSWORD — データ保持ボットの初期パスワード。詳細については、「データ保持を設定するための前提条件」を参照してください。この変数は、パスワードプロンプトでデータ保持ボットを起動する予定がない場合や、Secrets Manager を使用してデータ保持ボットの認証情報を保存する予定がない場合に 必要 です。

次の環境変数を使用して、デフォルトのデータ保持ストリーミング機能を設定します。

- WICKRIO_COMP_MESGDEST — メッセージがストリーミングされるディレクトリへのパス名。デフォルト値は、/tmp/*<botname>*/compliance/messagesです。
- WICKRIO_COMP_FILEDEST — ファイルがストリーミングされるディレクトリへのパス名。デフォルト値は、/tmp/*<botname>*/compliance/attachmentsです。
- WICKRIO_COMP_BASENAME — 受信したメッセージファイルのベース名。デフォルト値は、receivedMessagesです。
- WICKRIO_COMP_FILESIZE — 受信メッセージファイルの最大ファイルサイズ (KiB)。最大サイズに達すると、新しいファイルが開始されます。デフォルト値は 1000000000 (1024 GiB など) です。

- WICKRIO_COMP_TIMEROTATE — データ保持ボットが受信したメッセージを受信メッセージファイルに保存する時間 (分単位)。制限時間に達すると、新しいファイルが開始されます。受信メッセージファイルのサイズを制限できるのは、ファイルサイズまたは時間だけです。デフォルト値は 0 (制限なし) です。

次の環境変数を使用して、使用するデフォルト AWS リージョン を定義します。

- AWS_DEFAULT_REGION — Secrets Manager などの AWS サービスに使用するデフォルトの AWS リージョン (Amazon S3 や AWS KMS には使用されません)。この環境変数が定義されていない場合、デフォルトでは us-east-1 リージョンが使用されます。

以下の環境変数を使用して、Secrets Manager を使用してデータ保持ボットの認証情報と AWS サービス情報を保存することを選択したときに使用する Secrets Manager シークレットを指定します。Secrets Manager に保存できる値の詳細については、Secrets Manager の価値観 を参照してください。

- AWS_SECRET_NAME— データ保持ボットが必要とする認証情報と AWS サービス情報を含む Secrets Manager シークレットの名前。
- AWS_SECRET_REGION— AWS シークレットが存在する AWS リージョン。AWS シークレットを使用していて、この値が定義されていない場合は、AWS_DEFAULT_REGION 値が使用されます。

> **Note**
>
> 以下の環境変数はすべて、Secrets Manager に値として保存できます。Secrets Manager を使用してこれらの値をそこに保存する場合、データ保持ボットの Dockerイメージを実行するときに、それらを環境変数として指定する必要はありません。指定する必要があるのは、このガイドで前述した AWS_SECRET_NAME 環境変数だけです。詳細については、「Secrets Manager の価値観」を参照してください。

メッセージとファイルをバケットに保存する場合は、以下の環境変数を使用して Amazon S3 バケットを指定します。

- WICKRIO_S3_BUCKET_NAME— メッセージとファイルが保存される Amazon S3 バケットの名前。

- `WICKRIO_S3_REGION`— メッセージとファイルが保存される Amazon S3 バケットの AWS リージョン。
- `WICKRIO_S3_FOLDER_NAME`— メッセージとファイルが保存される Amazon S3 バケットのオプションのフォルダ名。このフォルダ名の前には、Amazon S3 バケットに保存されるメッセージとファイルのキーが先頭に付けられます。

ファイルを Amazon S3 バケットに保存するときに、クライアント側の暗号化を使用してファイルを再暗号化する場合に、次の環境変数を使用して AWS KMS 詳細を指定します。

- `WICKRIO_KMS_MSTRKEY_ARN`— メッセージファイルとデータ保持ボット上のファイルを Amazon S3 バケットに保存する前に再暗号化するために使用される AWS KMS マスターキーの Amazon リソースネーム (ARN)。
- `WICKRIO_KMS_REGION` — AWS KMS マスターキーが置かれている AWS リージョン。

Amazon SNS トピックにデータ保持イベントを送信することを選択した場合、次の環境変数を使用して Amazon SNS の詳細を指定します。送信されるイベントには、スタートアップ、シャットダウン、エラー状態が含まれます。

- `WICKRIO_SNS_TOPIC_ARN`— データ保持イベントの送信先の Amazon SNS トピックの ARN。

次の環境変数を使用して、データ保持メトリクスを に送信します CloudWatch。指定した場合、メトリクスは 60 秒ごとに生成されます。

- `WICKRIO_METRICS_TYPE` - この環境変数の値を に設定`cloudwatch`して、メトリクスを に送信します CloudWatch。

Secrets Manager の価値観

Secrets Manager を使用して、データ保持ボットの認証情報と AWS サービス情報を保存できます。シークレットの作成と保存については、 Secrets Manager ユーザーガイド の「基本的なAWS Secrets Managerシークレットを作成する」を参照してください。

Secrets Manager のシークレットには、次の値を含めることができます。

- `password`— データ保持ボットのパスワード。
- `s3_bucket_name`— メッセージとファイルが保存される Amazon S3 バケットの名前。設定しない場合、デフォルトのファイルストリーミングが使用されます。

- s3_region— メッセージとファイルが保存される Amazon S3 バケットの AWS リージョン。
- s3_folder_name— メッセージとファイルが保存される Amazon S3 バケットのオプションのフォルダ名。このフォルダ名の前には、Amazon S3 バケットに保存されるメッセージとファイルのキーが先頭に付けられます。
- kms_master_key_arn— メッセージファイルとデータ保持ボット上のファイルを Amazon S3 バケットに保存する前に再暗号化するために使用される AWS KMS マスターキーの ARN。
- kms_region — AWS KMS マスターキーが置かれている AWS リージョン。
- sns_topic_arn— データ保持イベントの送信先の Amazon SNS トピックの ARN。

AWS サービスでデータ保持を使用するための IAM ポリシー

Wickr データ保持ボットで他の AWS サービスを使用する予定がある場合は、そのサービスにアクセスするための適切な AWS Identity and Access Management (IAM) ロールとポリシーがホストにあることを確認する必要があります。Secrets Manager、Amazon S3、Amazon SNS CloudWatch、および を使用するようにデータ保持ボットを設定できますAWS KMS。次の IAM ポリシーでは、これらのサービスの特定のアクションへのアクセスを許可します。

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

ホスト上のコンテナにアクセスを許可したい各サービスの特定のオブジェクトを指定することで、より厳密な IAM ポリシーを作成できます。使用しない AWS サービスのアクションを削除します。たとえば、Amazon S3 バケットのみを使用する場合

は、、secretsmanager:GetSecretValue、sns:Publish、kms:GenerateDataKey、および cloudwatch:PutMetricData アクションを削除する次のポリシーを使用してください。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "*"
        }
    ]
}
```

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスを使用してデータ保持ボットをホストする場合は、Amazon EC2 の一般的なケースを使用して IAM ロールを作成し、上記のポリシー定義を使用してポリシーを割り当てます。

データ保持ボットを起動する

データ保持ボットを実行する前に、その設定方法を決定する必要があります。次のようなホストでボットを稼働させる予定がある場合

- AWS サービスにアクセスできなくなると、選択肢が限られます。その場合は、デフォルトのメッセージストリーミングオプションを使用します。キャプチャするメッセージファイルのサイズを特定のサイズに制限するか、時間間隔に制限するかを決定する必要があります。詳細については、「環境変数」を参照してください。
- ボットに、AWS のサービスへのアクセス権がある場合は、Secrets Manager シークレットを作成して、ボットの資格情報と AWS サービス設定の詳細を保存する必要があります。AWS サービスを設定したら、データ保持ボットの Dockerイメージを起動できます。Secrets Manager シークレットに保存できる詳細についての詳細は、Secrets Manager の価値観 を参照してください。

以下のセクションでは、データ保持ボットの Docker イメージを実行するコマンドの例を示します。各コマンド例で、次の例の値を独自の値に置き換えます。

- *compliance_1234567890_bot* をデータ保持ボットの名前に置き換えます。
- *password* にデータ保持ボットのパスワードを入力します。

- *wickr/data/retention/bot* にデータ保持ボットで使用する Secrets Manager シークレットの名前を付けます。
- *bucket-name* にメッセージとファイルが保存される Amazon S3 バケットの名前を指定します。
- *folder-name* にメッセージとファイルが保存される Amazon S3 バケット内のフォルダ名を指定します。
- *us-east-1* は、指定しているリソースの AWS リージョンに置き換えます。たとえば、AWS KMS マスターキーのリージョンや Amazon S3 バケットのリージョンなどです。
- *arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-a617-abababababab* にメッセージファイルおよびファイルの再暗号化に、AWS KMS マスターキーの Amazon リソースネーム (ARN) と入力します。

パスワード環境変数 (AWS サービスなし) を使用してボットを起動します。

次の Docker コマンドはデータ保持ボットを起動します。パスワードは WICKRIO_BOT_PASSWORD 環境変数を使用して指定されます。ボットは、デフォルトのファイルストリーミングと、このガイドの 環境変数 セクションで定義されているデフォルト値の使用を開始します。

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

パスワードプロンプト (AWS サービスなし) でボットを起動します。

次の Docker コマンドはデータ保持ボットを起動します。パスワードは、データ保持ボットによって要求されたときに入力されます。このガイドの 環境変数 セクションで定義されているデフォルト値を使用して、デフォルトのファイルストリーミングを開始します。

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

docker attach compliance_1234567890_bot
.
.
.
```

```
Enter the password:************
Re-enter the password:************
```

パスワードプロンプトを受け取る -ti オプションを使用してボットを実行します。また、docker イメージを起動した直後に docker attach *<container ID or container name>* コマンドを実行して、パスワードプロンプトが表示されるようにする必要があります。これらのコマンドは両方ともスクリプトで実行する必要があります。Docker イメージにアタッチしてもプロンプトが表示されない場合は、Enter キーを押すとプロンプトが表示されます。

15 分間のメッセージファイルローテーション (AWS サービスなし) でボットを起動します。

次の Docker コマンドは、環境変数を使用してデータ保持ボットを起動します。また、受信したメッセージファイルを 15 分にローテーションするように設定しています。

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

ボットを起動し、Secrets Manager で初期パスワードを指定する

Secrets Manager を使用して、データ保持ボットのパスワードを特定できます。データ保持ボットを起動するときは、この情報を保存する Secrets Manager を指定する環境変数を設定する必要があります。

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

wickrpro/compliance/compliance_1234567890_bot シークレットには以下のシークレット値があり、プレーンテキストで表示されます。

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

ボットを起動し、Secrets Manager で Amazon S3 を設定する

Secrets Manager を使用して、認証情報と Amazon S3 バケット情報をホストできます。データ保持ボットを起動するときは、この情報を保存する Secrets Manager を指定する環境変数を設定する必要があります。

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

wickrpro/compliance/compliance_1234567890_bot シークレットには以下のシークレット値があり、プレーンテキストで表示されます。

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

ボットが受信したメッセージとファイルは、network1234567890 という名前のフォルダー内の bot-compliance バケットに格納されます。

ボットを起動し、Secrets Manager を使用して Amazon S3 と AWS KMS を設定する

Secrets Manager を使用して、認証情報、Amazon S3 バケット、AWS KMS マスターキー情報をホストできます。データ保持ボットを起動するときは、この情報を保存する Secrets Manager を指定する環境変数を設定する必要があります。

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

wickrpro/compliance/compliance_1234567890_bot シークレットには以下のシークレット値があり、プレーンテキストで表示されます。

```
{
```

```
    "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"
}
```

ボットが受信したメッセージとファイルは、ARN 値で識別される KMS キーを使用して暗号化され、「network1234567890」という名前のフォルダーの「bot-compliance」バケットに格納されます。適切な IAM ポリシーが設定されていることを確認します。

ボットを起動し、環境変数を使用して Amazon S3 を設定する

Secrets Manager を使用してデータ保持ボットの認証情報をホストしたくない場合は、以下の環境変数を使用してデータ保持ボットの Dockerイメージを起動できます。WICKRIO_BOT_NAME 環境変数を使用してデータ保持ボットの名前を特定する必要があります。

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
-e WICKRIO_S3_BUCKET_NAME='bucket-name' \
-e WICKRIO_S3_FOLDER_NAME='folder-name' \
-e WICKRIO_S3_REGION='us-east-1' \
wickr/bot-compliance-cloud:latest
```

環境値を使用して、データ保持ボットの認証情報、Amazon S3 バケットに関する情報、およびデフォルトのファイルストリーミングの設定情報を識別できます。

データ保持ボットを停止する

データ保持ボットで実行されているソフトウェアが SIGTERM 信号をキャプチャし、正常にシャットダウンします。以下の例に示すように docker stop *<container ID or container name>* コマンドを使用して、データ保持ボットのDockerイメージに SIGTERM コマンドを実行します。

```
docker stop compliance_1234567890_bot
```

データ保持ログの取得

データ保持ボットの Docker イメージで実行されているソフトウェアは、/tmp/*<botname>*/logs ディレクトリ内のログファイルに出力されます。最大 5 つのファイルにローテーションされます。以下のコマンドを実行すれば、ログを取得できる。

```
docker logs <botname>
```

例：

```
docker logs compliance_1234567890_bot
```

データ保持指標とイベント

AWS Wickr データ保持ボットの 5.116 バージョンで現在サポートされている Amazon CloudWatch (CloudWatch) メトリックスと Amazon Simple Notification Service (Amazon SNS) イベントは次のとおりです。

トピック

- CloudWatch メトリックス
- Amazon SNS イベント

CloudWatch メトリックス

メトリクスはボットによって 1 分間隔で生成され、データ保持ボットの Docker CloudWatch イメージが実行されているアカウントに関連付けられているサービスに送信されます。

データ保持ボットがサポートする既存のメトリックスは次のとおりです。

メトリクス	説明
Messages_Rx	メッセージを受信しました。
Messages_Rx_Failed	受信したメッセージを処理できませんでした。
Messages_Saved	メッセージは受信メッセージファイルに保存されます。

メトリクス	説明
Messages_Saved_Failed	受信メッセージファイルへのメッセージの保存に失敗しました。
Files_Saved	ファイルを受信しました。
Files_Saved_Bytes	受信したファイルのバイト数。
Files_Saved_Failed	ファイルの保存に失敗しました。
ログイン	ログイン（通常、各ログイン間隔で 1 回です）。
Login_Failures	ログインに失敗した（通常、各ログイン間隔で 1 回です）。
S3_Post_Errors	メッセージファイルおよびファイルを Amazon S3 バケットに送信中にエラーが発生しました。
Watchdog_Failures	ウォッチドッグの障害。
Watchdog_Warnings	ウォッチドッグの警告。

CloudWatchメトリクスは生成されて消費されます。ボットに使用される名前空間は `WickrIO` です。各メトリクスにはディメンションの配列があります。以下は、上記のメトリクスとともに掲載されるディメンションのリストです。

ディメンション	値
ID	ボットのユーザー名。
デバイス	特定のボットデバイスまたはインスタンスの説明。複数のボットデバイスまたはインスタンスを実行している場合に便利です。
製品	ボット用の製品。`Alpha`、`Beta`、または `Production` を付加した `WickrPro_` また

ディメンション	値
	は WickrEnterprise_ にすることができます。
BotType	ボットタイプ。コンプライアンスボットにはコンプライアンス というラベルが付けられます。
ネットワーク	関連付けられたネットワークの ID。

Amazon SNS イベント

以下のイベントは、WICKRIO_SNS_TOPIC_ARN 環境変数または sns_topic_arn Secrets Manager のシークレット値を使用して識別される Amazon リソースネーム (ARN) 値によって定義された Amazon SNS トピックに投稿されます。詳細については、環境変数およびSecrets Manager の価値観を参照してください。

データ保持ボットによって生成されたイベントは JSON 文字列として送信されます。データ保持ボットの 5.116 バージョンでは、以下の値がイベントに含まれています。

名前	値
complianceBot	データ保持ボットのユーザー名。
dataTime	イベントが発生したときの日時
デバイス	特定のボットデバイスまたはインスタンスの説明。複数のボットインスタンスを実行している場合に便利です。
dockerImage	ボットに関連付けられている Docker イメージ。
dockerTag	Docker イメージのタグまたはバージョン。
message	イベントメッセージ。詳細については、「重要なイベント」および「通常のイベント」を参照してください。

名前	値
notificationType	この値は Bot Event になります。
severity	イベントの重要度。normal または critical のいずれかを設定できます。

イベントを受信するには、Amazon SNS トピックにサブスクライブする必要があります。E メールアドレスを使用してサブスクライブすると、次の例のような情報を含む E メールが送信されます。

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

重要なイベント

これらのイベントにより、ボットは停止または再起動します。他の問題を引き起こさないように、再起動の回数は制限されています。

ログイン失敗

ボットがログインに失敗した場合に発生する可能性のあるイベントは次のとおりです。各メッセージには、ログインに失敗した理由が示されます。

イベントタイプ	イベントメッセージ
failedlogin	不正な認証情報。パスワードを確認してください。
failedlogin	ユーザーが見つかりません。
failedlogin	アカウントまたはデバイスが停止されています。

イベントタイプ	イベントメッセージ
プロビジョニング	ユーザーはコマンドを終了した。
プロビジョニング	`config.wickr` ファイルのパスワードが不正です。
プロビジョニング	`config.wickr` ファイルを読み込めません。
failedlogin	ログインがすべて失敗しました。
failedlogin	新しいユーザーですが、データベースはすでに存在しています。

より重大なイベント

イベントタイプ	イベントメッセージ
停止中のアカウント	WickRioClientMain:: slotAdminUser サスペンド:コード (%1): 理由:%2」
BotDevice 中断されました	デバイスが停止されました。
WatchDog	SwitchBoard システムが < *N* > 分以上ダウンしている
S3 障害	ファイル <*file-name* ≫ を S3 バケットに配置できませんでした。エラー：<*AWS-error* >
フォールバックキー	SERVER SUBMIITED FALLBACK KEY：クライアント側で認識されているアクティブなフォールバックキーではありません。デスクトップエンジニアリングにログを送信してください。

通常のイベント

通常の運用状況について警告するイベントは次のとおりです。特定の期間内にこの種のイベントが多発すると、懸念の原因となることがあります。

デバイスがアカウントに追加されました

このイベントは、データ保持ボットアカウントに新しいデバイスが追加されたときに生成されます。状況によっては、これは誰かがデータ保持ボットのインスタンスを作成したことを示す重要な指標となることがあります。以下は、このイベントのメッセージです。

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

Bot がログインしました

このイベントは、ボットが正常にログインしたときに生成されます。以下は、このイベントのメッセージです。

```
Logged in
```

シャットダウン

このイベントは、ボットのシャットダウン時に生成されます。ユーザーがこれを明示的に開始しなかった場合、問題が発生している可能性があります。以下は、このイベントのメッセージです。

```
Shutting down
```

アップデートがあります

このイベントは、データ保持ボットが起動し、関連する Docker イメージの新しいバージョンが使用可能であることが確認されたときに生成されます。このイベントは、ボットの起動時に毎日生成されます。このイベントには、利用可能な新しいバージョンを識別する versions 配列フィールドが含まれます。以下に示しているのは、イベントの具体的な例です。

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

```
  ]
}
```

ATAK とは

Android チーム認識キット (ATAK) は、軍事用 Android タクティカルアサルトキット (同じく ATAK) とも呼ばれるスマートフォンでの地理空間インフラストラクチャおよび状況認識アプリケーションであり、地理的に離れた場所での安全なコラボレーションを可能にします。ATAK は当初、戦闘地帯での使用を想定して設計されていましたが、地方、州、および連邦機関の任務に合うように適合されています。

トピック

- Wickr ネットワークダッシュボードで ATAK を有効にする
- ATAK に関する追加情報
- ATAK 用 Wickr プラグインをインストールしてペアリングする
- ダイヤル発信と着信
- ファイルの送信
- 安全な音声メッセージを送信する (P ush-to-talk)
- ピンホイール (クイックアクセス)
- ナビゲーション

Wickr ネットワークダッシュボードで ATAK を有効にする

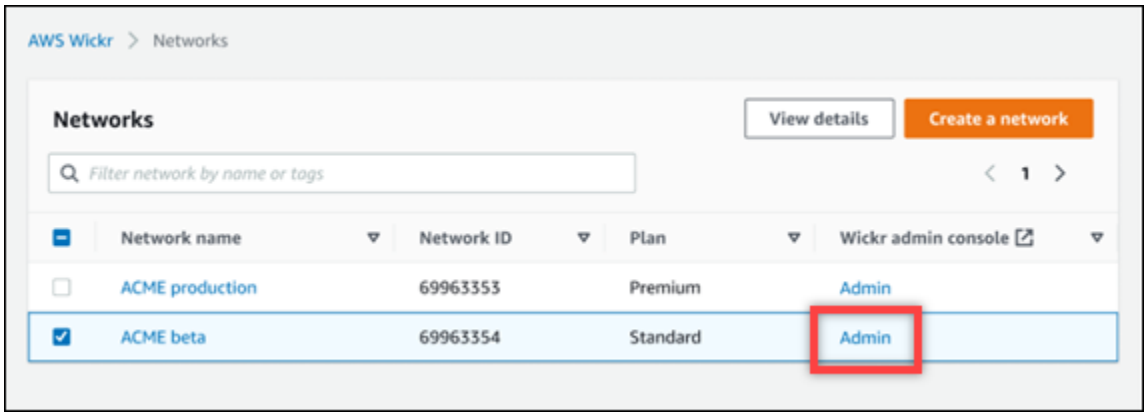
AWS Wickr は Android Tactical Assault Kit (ATAK) を使用する多くの機関をサポートしています。ただし、これまで Wickr を使用する ATAK オペレーターは、そのためにはアプリケーションを終了する必要がありました。中断と運用リスクを軽減するために、Wickr は ATAK を安全な通信機能で強化するプラグインを開発しました。ATAK 用 Wickr プラグインを使用すると、ユーザーは ATAK アプリケーション内で Wickr 上でメッセージを送ったり、共同作業を行ったり、ファイルを転送したりできます。これにより、中断がなくなり、ATAK のチャット機能の設定が複雑になることもなくなります。

Wickr ネットワークダッシュボードで ATAK を有効にする

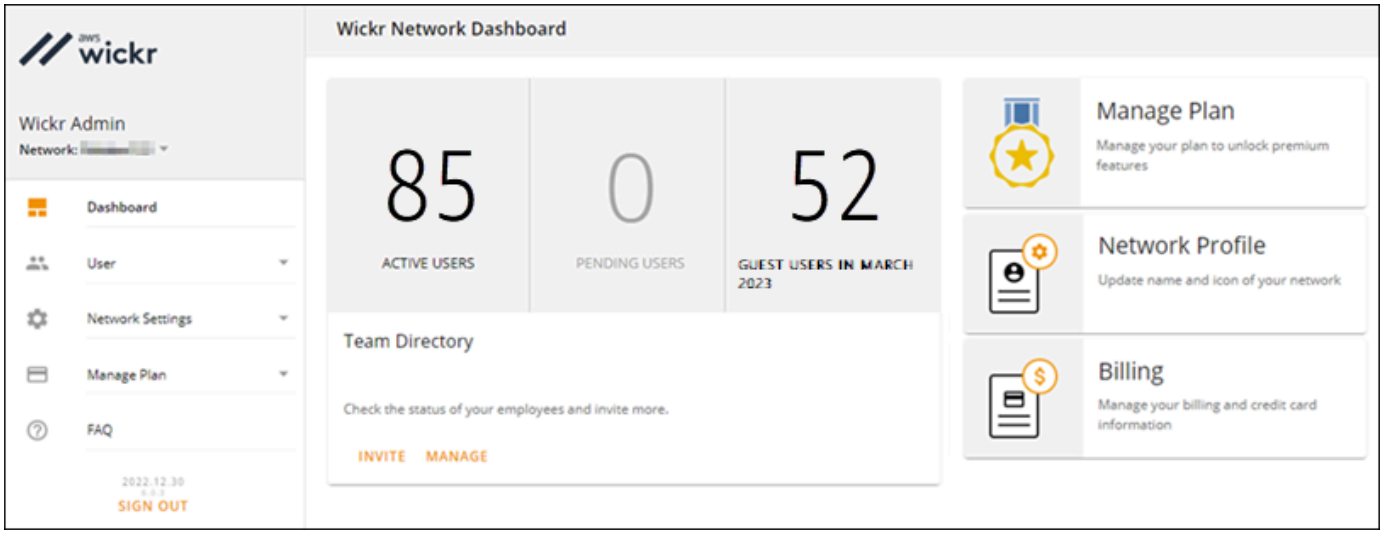
Wickr ネットワークダッシュボードで ATAK を有効にするには、以下の手順を実行します。

1. https://console.aws.amazon.com/wickr/ で Wickr の AWS Management Console を開きます。

2. ネットワーク ページで 管理 リンクを選択し、そのネットワークの Wickr 管理コンソールに移動します。



特定のネットワークの Wickr 管理コンソールにリダイレクトされます。



3. Wickr 管理コンソールのナビゲーションペインで ネットワーク設定 を選択し、セキュリティグループ を選択します。
4. ATAK を有効にするセキュリティグループの横にある 詳細設定 を選択します。
5. 全般タブで、編集 を選択します。
6. ATAK 機能セクションで:

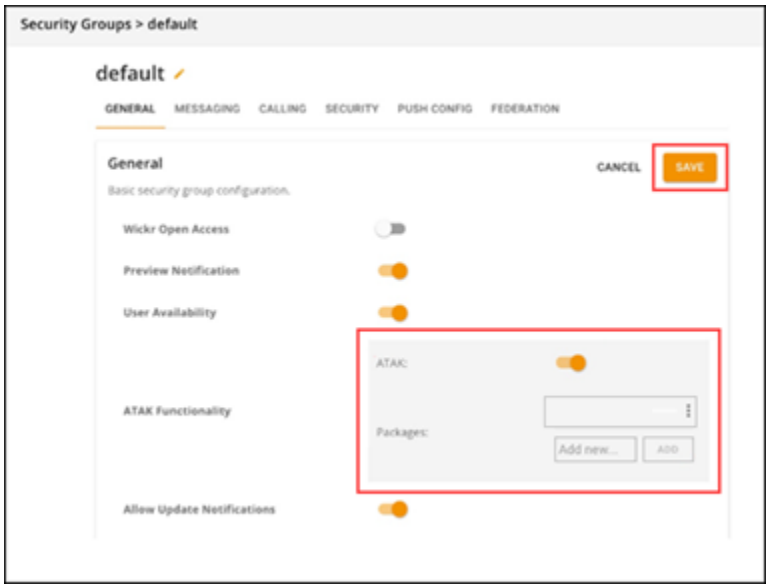
   a. パッケージ テキストボックスにパッケージ名を入力します。ユーザーがインストールおよび使用する ATAK のバージョンに応じて、次のいずれかの値を入力できます。

      - `com.atakmap.app.civ`— Wickr エンドユーザーが Android デバイスに民間版の ATAK アプリケーションをインストールして使用する場合は、この値を「パッケージ」テキストボックスに入力します。

- `com.atakmap.app.mil`— Wickr エンドユーザーが Android デバイスに軍用バージョンの ATAK アプリケーションをインストールして使用する場合は、この値を「パッケージ」テキストボックスに入力します。

b. ATAK トグルを右にスライドさせて機能を有効にします。

c. 保存 を選択します。



これで、選択した Wickr ネットワークと選択したセキュリティグループで ATAK が有効になりました。ATAK 機能を有効にしたセキュリティグループの Android ユーザーに、ATAK 用 Wickr プラグインをインストールするよう依頼してください。詳細については、「Wickr ATAK プラグインのインストールとペア」を参照してください。

ATAK に関する追加情報

ATAK 用 Wickr プラグインの詳細については、以下を参照してください。

- Wickr ATAK プラグインの概要
- Wickr ATAK プラグイン追加情報

ATAK 用 Wickr プラグインをインストールしてペアリングする

Android チーム認識キット (ATAK) は、ミッションの計画、実行、インシデント対応に状況認識機能を必要とする米軍、州、政府機関で使用されている Android ソリューションです。ATAK には、開発者が機能を追加できるプラグインアーキテクチャがあります。これにより、ユーザーは GPS と地理空間マップデータと、進行中のイベントのリアルタイムの状況認識を組み合わせてナビゲートできます。このドキュメントでは、Android デバイスに ATAK 用 Wickr プラグインをインストールし、Wickr クライアントとペアリングする方法を説明します。これにより、ATAK アプリケーションを終了しなくても Wickr でメッセージを送ったり、共同作業を行ったりできます。

ATAK用のWickrプラグインをインストールします。

Android デバイスに ATAK 用 Wickr プラグインをインストールするには、次の手順を実行します。

1. Google Play ストアに移動し、ATAK 用 Wickr プラグインをインストールしてください。
2. Android デバイスで ATAK アプリケーションを開きます。
3. ATAK アプリケーションで、画面の右上にあるメニューアイコン
   ()
   を選択し、[プラグイン] を選択します。
4. Import (インポート) を選択します。
5. [インポートタイプの選択] ポップアップで [ローカル SD] を選択し、ATAK 用 Wickr プラグイン .apk ファイルを保存した場所に移動します。
6. プラグインファイルを選択し、インストールするための指示に従います。

   > **Note**
   >
   > スキャン用にプラグインファイルを送信するように求められた場合は、いいえ を選択します。

7. ATAK アプリケーションから、プラグインをロードするかどうかを尋ねます。OK をクリックします。

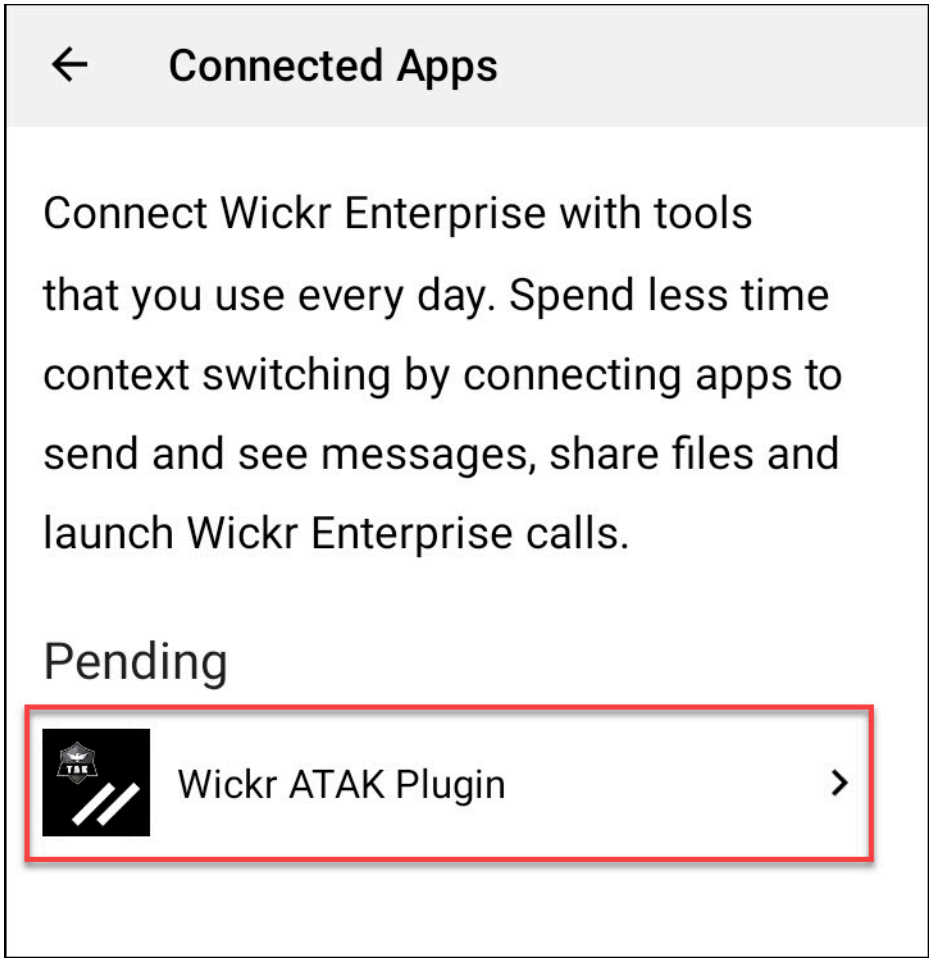
ATAK 用の Wickr プラグインがインストールされました。次の「ATAK と Wickr のペアリング」セクションに進んでプロセスを終了してください。

ATAK と Wickr のペアリング

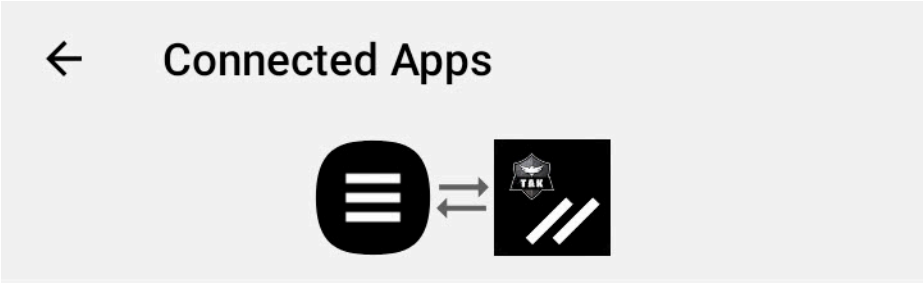
ATAK 用 Wickr プラグインが正常にインストールされたら、次の手順を実行して ATAK アプリケーションと Wickr をペアリングします。

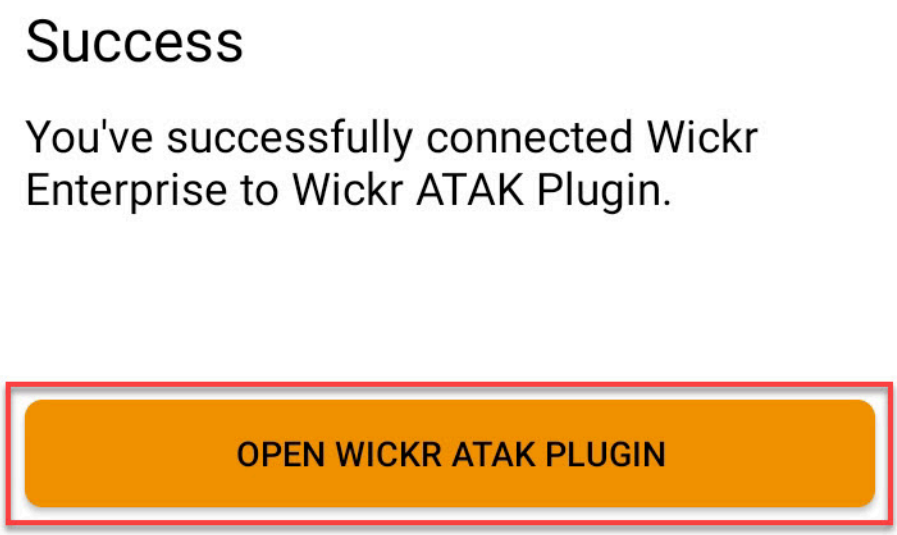
1. ATAK アプリケーションで、画面の右上にあるメニューアイコン
   ( )
   を選択し、次に [Wickr プラグイン] を選択します。
2. Wickr とペアリング を選択します。

   ATAK 用 Wickr プラグインのアクセス許可を確認するように求める通知プロンプトが表示されます。通知プロンプトが表示されない場合は、Wickr クライアントを開いて 設定、接続アプリケーション の順に移動します。画面の [保留中] セクションにプラグインが表示されます。



3. 承認 を選択してペアリングします。
4. Wickr ATAK プラグインを開く ボタンを選択して ATAK アプリケーションに戻ります。



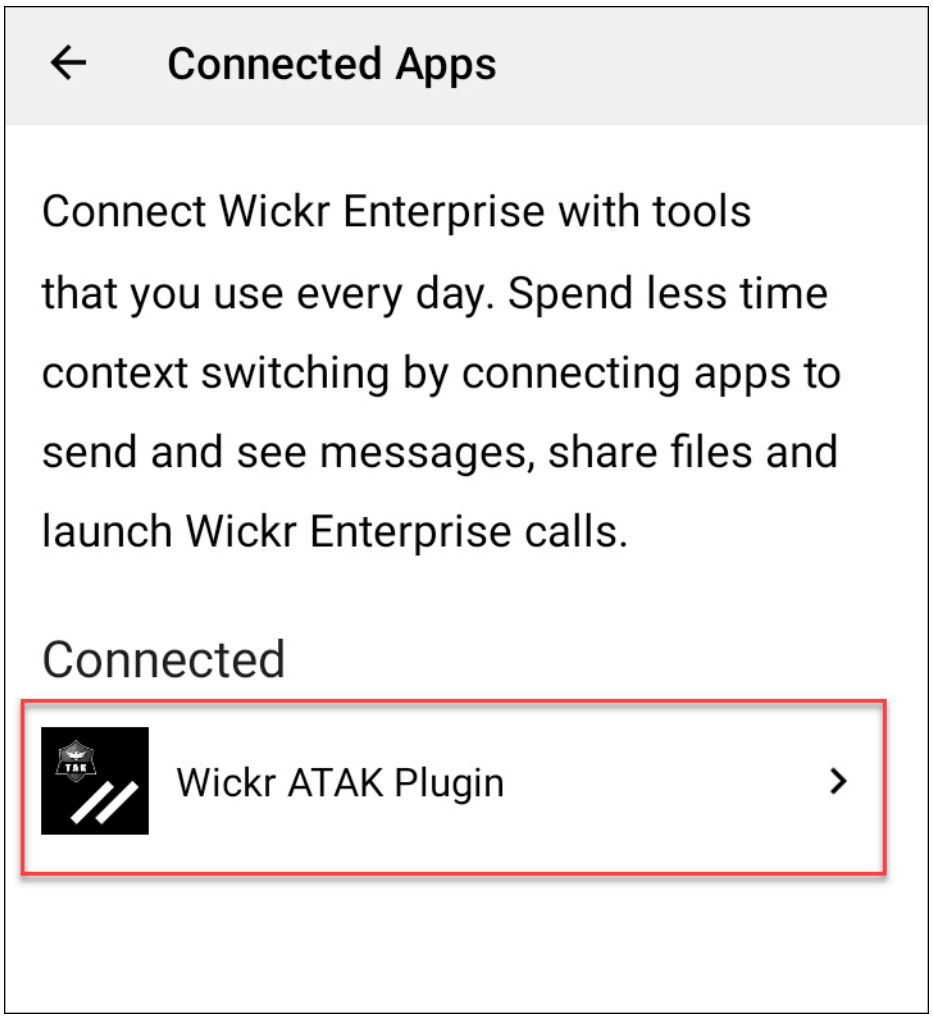


これで ATAK プラグインと Wickr のペアリングが完了しました。ATAK アプリケーションを終了しなくても、プラグインを使用してメッセージを送信したり、Wickr を使用して共同作業を行ったりできます。

ATAK と Wickr のペアリング解除

ATAK プラグインと Wickr のペアリングを解除するには、次の手順を実行します。

1. ネイティブアプリで、[設定]、[接続アプリケーション] の順に選択します。
2. [接続アプリケーション] 画面で、[Wickr ATAK プラグイン] を選択します。



3. [Wickr ATAK プラグイン] 画面で、画面下部の [削除] を選択します。

   API を使用しなくなったことを示す確認画面が表示されます。これで ATAK プラグインのペアリングが正常に解除されました。

ダイヤル発信と着信

ATAK 用 Wickr プラグインではダイヤル発信と着信を行うことができます。

ダイヤル発信と着信を行うには、次の手順を実行します。

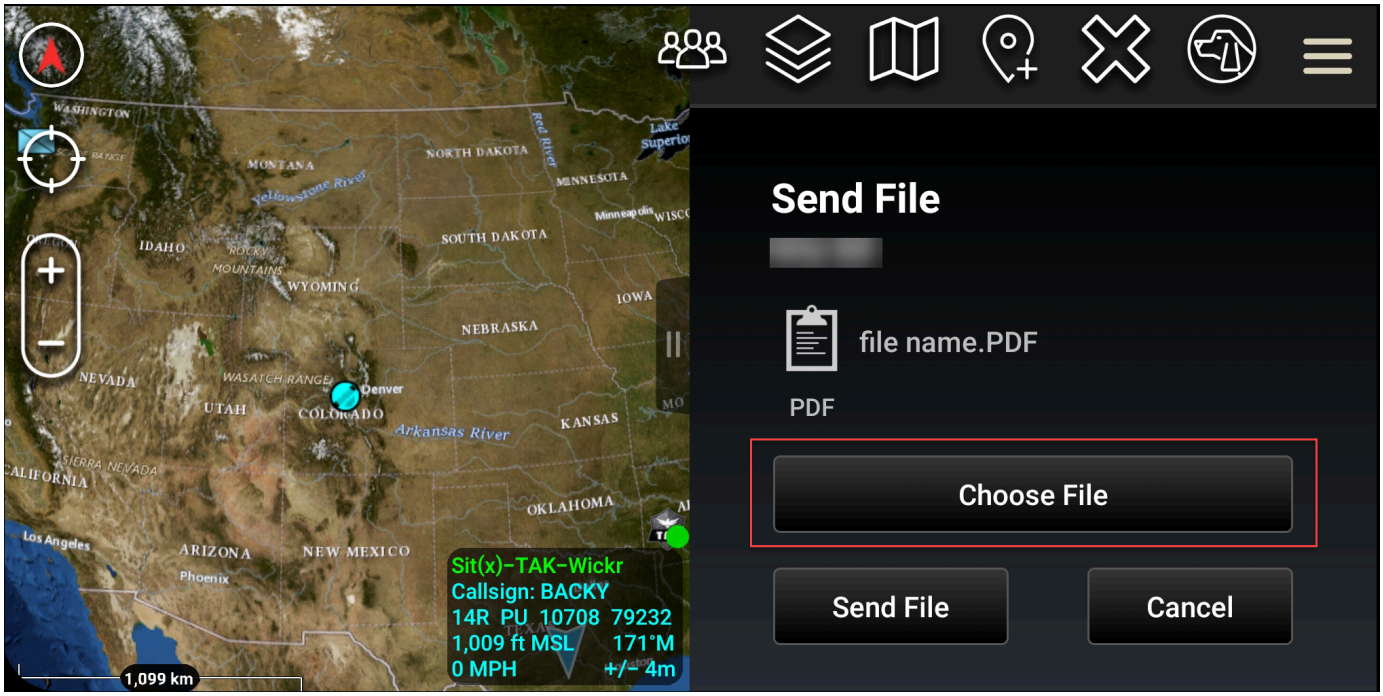
1. チャットウィンドウを開きます。
2. [マップ] ビューで、電話をかけるユーザーのアイコンを選択します。
3. 画面の右上にある電話アイコンを選択します。
4. 接続したら、ATAK プラグインビューに戻って電話を受けることができます。

ファイルの送信

ATAK 用 Wickr プラグインでファイルを送信できます。

ファイルを送信するには、次の手順を実行します。

1. チャットウィンドウを開きます。
2. [マップ] ビューで、ファイルを送信するユーザーを検索します。
3. ファイルを送信するユーザーを見つけたら、その名前を選択します。
4. [ファイルの送信] 画面で [ファイルの選択] を選択し、送信するファイルに移動します。



5. ブラウザウィンドウで、目的のファイルを選択します。
6. [ファイルの送信] 画面で、[ファイルの送信] を選択します。

   選択したファイルがダウンロード中であることを示すダウンロードアイコンが表示されます。

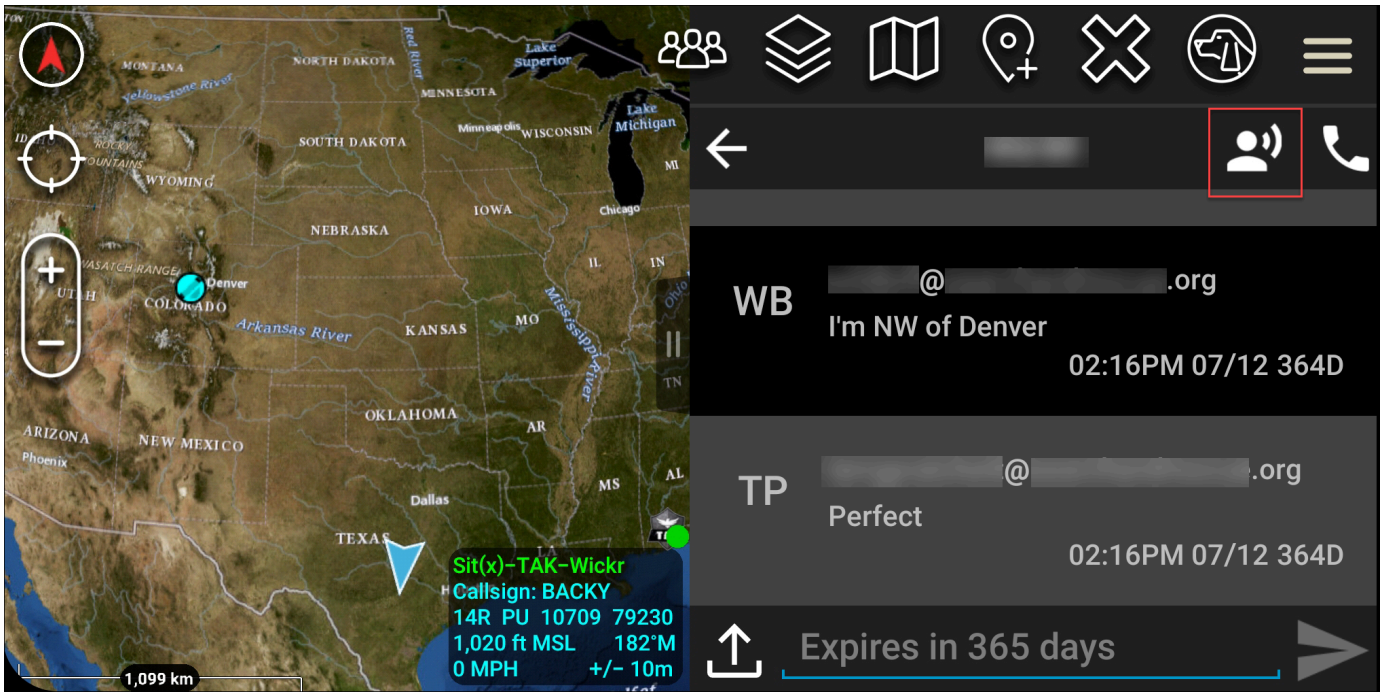
安全な音声メッセージを送信する (P ush-to-talk)

ATAK 用 Wickr プラグインでセキュアボイスメッセージ (P ush-to-talk) を送信できます。

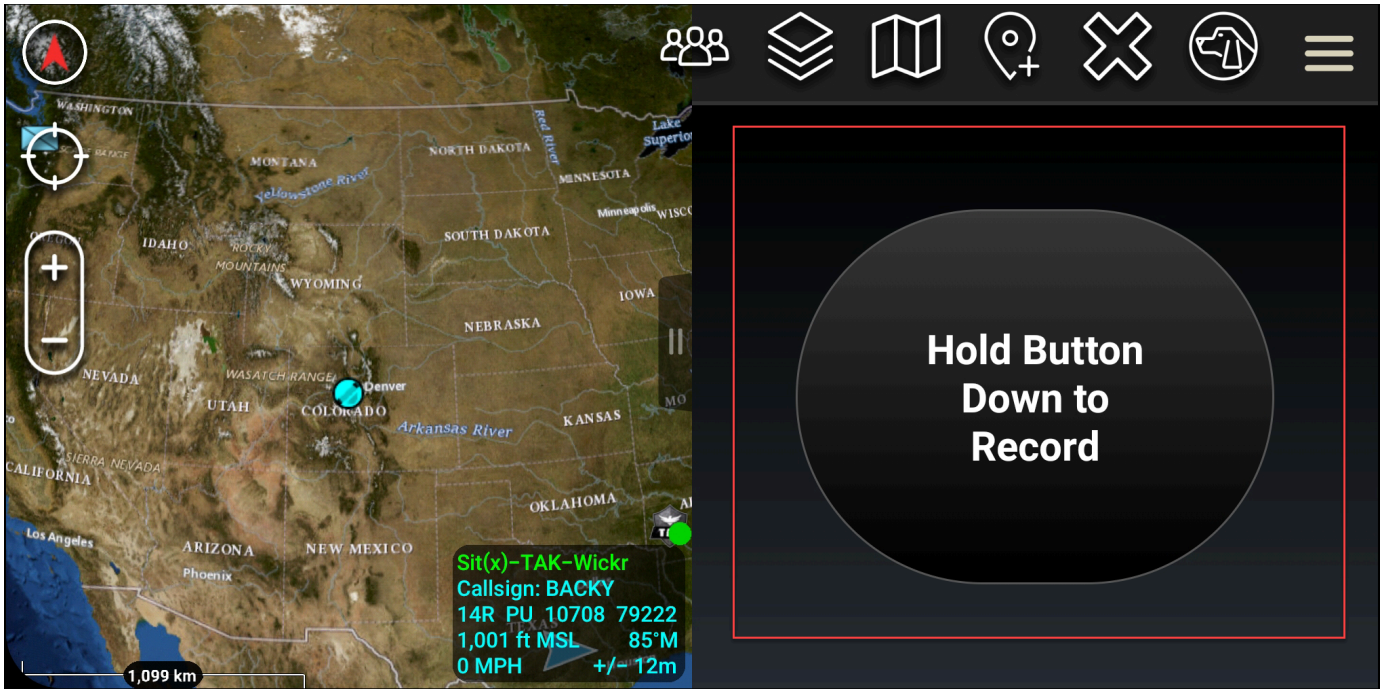
安全な音声メッセージを送信するには、次の手順を実行します。

1. チャットウィンドウを開きます。

2. 画面上部の [プッシュトゥトーク] アイコンを選択します。これは会話している人のアイコンで示されます。



3. [長押しして録音] ボタンを選択し、長押しします。



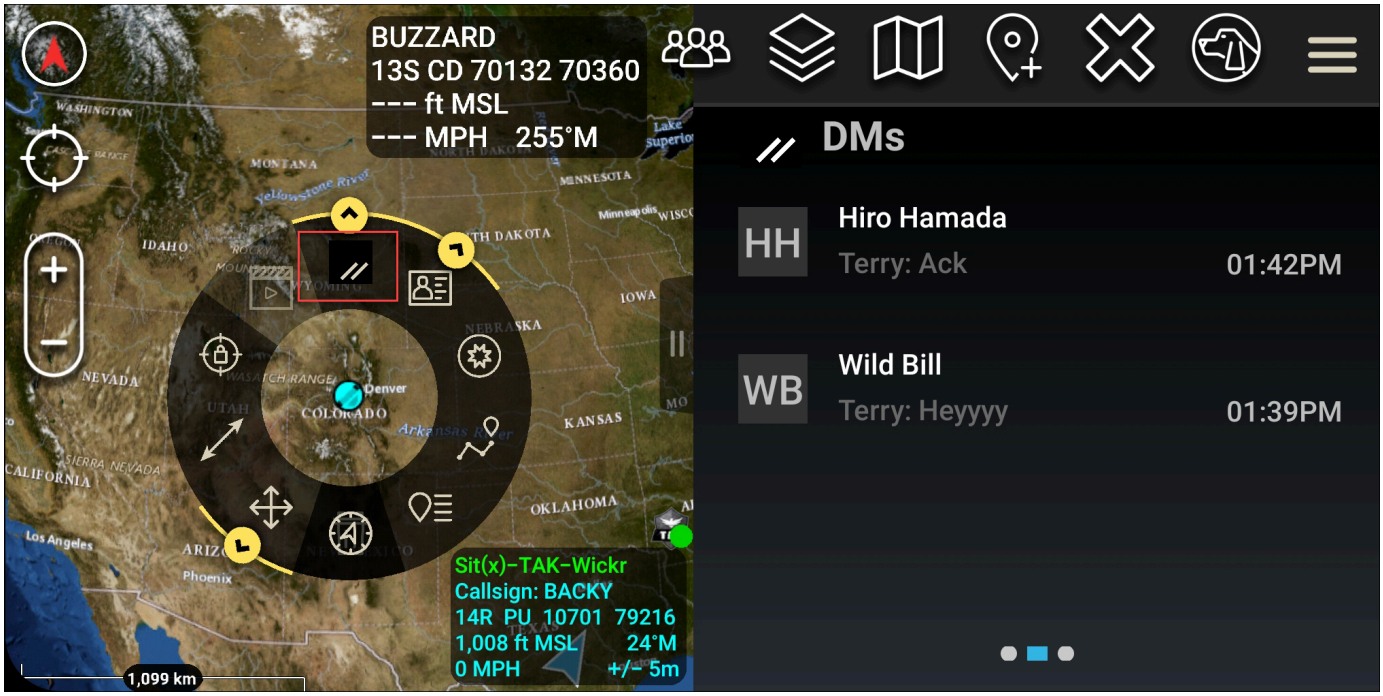
4. メッセージを録音します。
5. メッセージを録音した後、ボタンを離すと送信されます。

ピンホイール (クイックアクセス)

ピンホイールまたはクイックアクセス機能は、 one-one-one 会話や直接メッセージに使用されます。

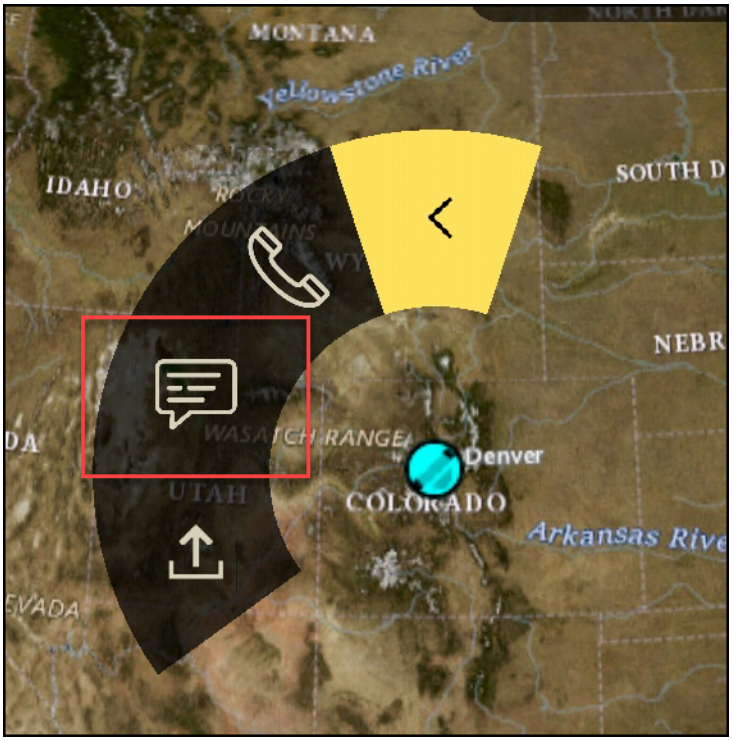
ピンホイールを使用するには、次の手順を実行します。

1. ATAK マップの分割画面ビューと ATAK 用 Wickr プラグインを同時に開きます。マップにはチームメイトやアセットがマップビュー上に表示されます。
2. ユーザーアイコンを選択すると、ピンホイールが開きます。
3. Wickr アイコンを選択すると、選択したユーザーが利用できるオプションが表示されます。

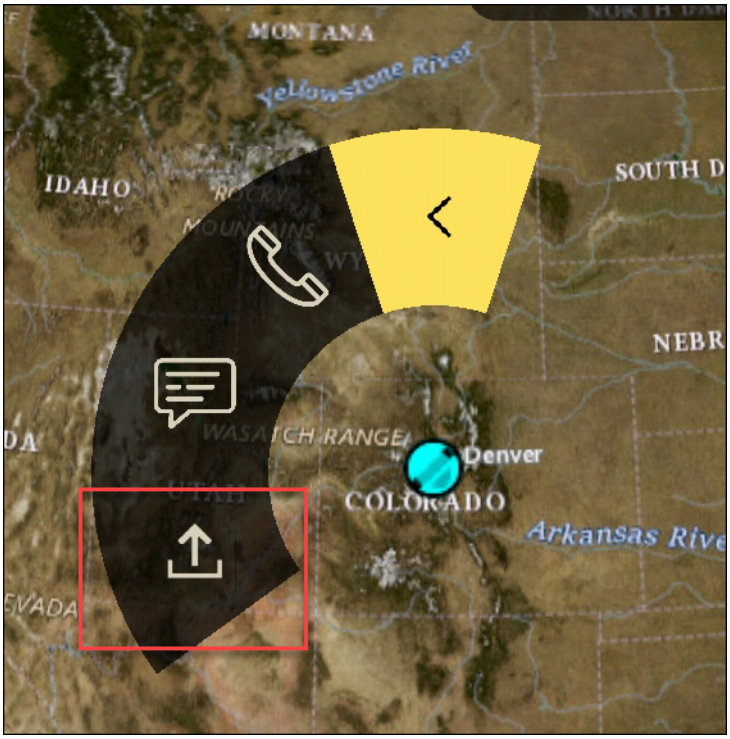


4. ピンホイールで、以下のいずれかのアイコンを選択します。
   - [電話]: 電話をかける場合に選択します。

- [メッセージ]: チャットする場合に選択します。



- [ファイル送信]: ファイルを送信する場合に選択します。



ナビゲーション

プラグイン UI には、画面の右下にある青と白の図形で示される 3 つのプラグインビューがあります。ビュー間を移動するには左右にスワイプします。

- [連絡先ビュー]: ダイレクトメッセージグループまたは会話ルームを作成します。
- DMs view: one-to-one 会話を作成します。チャット機能は Wickr のネイティブアプリと同様に機能します。この機能により、マップビューを開いたまま、プラグイン上で他のユーザーと通信できます。
- [ルームビュー]: ネイティブアプリ内の既存のルームが移植されます。プラグインでの操作はすべて Wickr ネイティブアプリに反映されます。

> **Note**
>
> ルームの削除などの特定の機能は、ユーザーによる意図しない変更や現場の機器による干渉を防ぐために、ネイティブアプリで直接行う場合のみ実行できます。

許可するポートとドメインのリスト

Wickr が正しく機能することを確認するために、以下のポートとドメインを許可リストに登録してください。

ポート

- TCP ポート 443 (メッセージと添付ファイル用)
- UDP ポート 16384-16584 (通話用)

リージョンのドメイン

- 欧州 (フランクフルト): api.messaging.wickr.eu-central-1.amazonaws.com
- 米国東部 (バージニア北部): gw-pro-prod .wickr.com、api.message。 wickr.us-east-1.amazonaws.com
- 欧州 (ロンドン): api.messaging.wickr.eu-west-2.amazonaws.com
- アジアパシフィック (シドニー): api.messaging.wickr.ap-southeast-2.amazonaws.com
- カナダ (中部): api.messaging.wickr.ca-central-1.amazonaws.com
- AWS GovCloud (米国西部): api.messaging.wickr。 us-gov-west-1.amazonaws.com

登録 E メールと確認 E メールは donotreply@wickr.email から送信されます。

呼び出し元サーバーの IP アドレスをすべて一覧表示できるようにする必要がある場合は、使用可能な CIDR AllowlistWickrの.txt をダウンロードし、定期的に確認する必要があります。この情報は変更される可能性があるためです。

AWS Wickr でユーザーを管理する

Wickr AWS Management Console の の Users セクションでは、現在の Wickr ユーザーとボットを表示したり、その詳細を変更したりできます。

トピック

チームディレクトリ

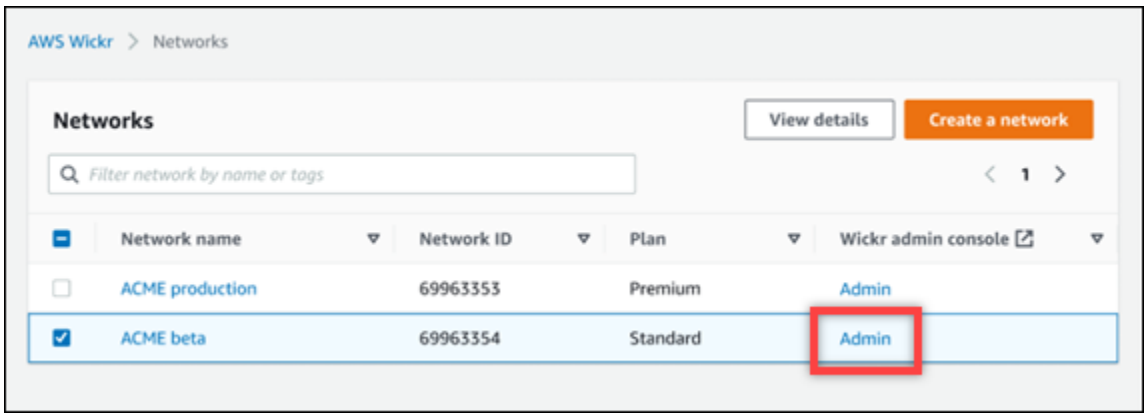
現在の Wickr ユーザーを表示し、Wickr AWS Management Console の のユーザーセクションで詳細を変更できます。

トピック

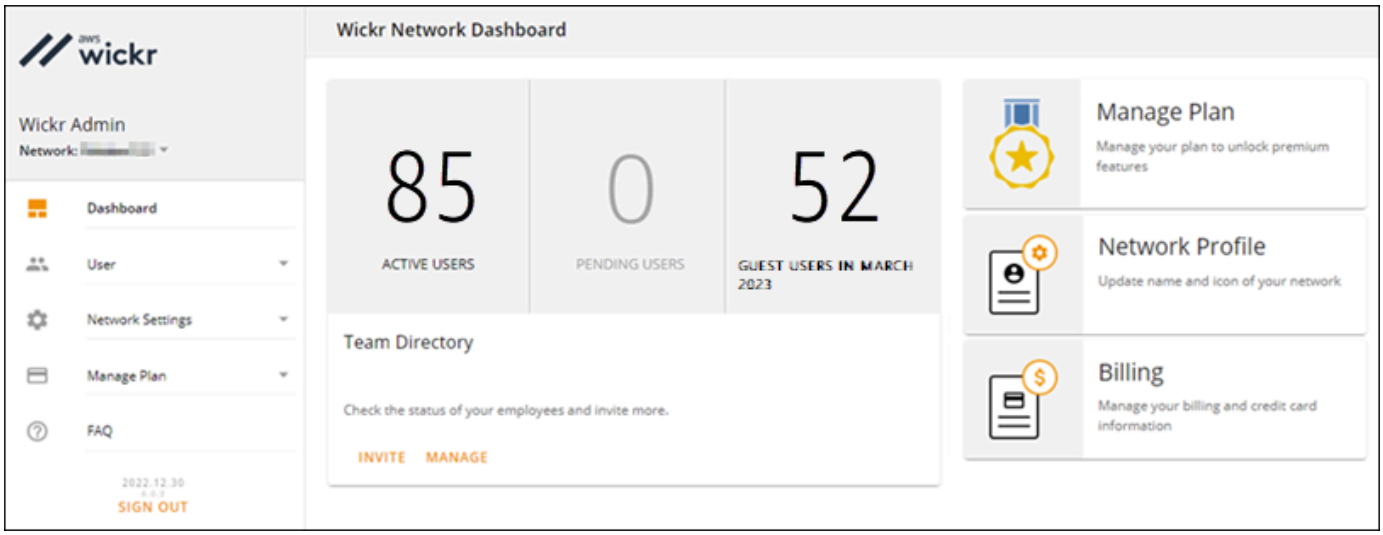
ユーザーを表示する

Wickr ネットワークに登録されているユーザーを表示するには、次の手順を実行します。

1. https://console.aws.amazon.com/wickr/ で Wickr AWS Management Console の を開きます。
2. ネットワーク ページで 管理 リンクを選択し、そのネットワークの Wickr 管理コンソールに移動します。



特定のネットワークの Wickr 管理コンソールにリダイレクトされます。



3. Wickr 管理コンソールのナビゲーションペインで、「ユーザー」を選択し、「チームディレクトリ」を選択します。

   チームディレクトリ ページには、名前、メールアドレス、割り当てられたセキュリティグループ、現在のステータスなど、Wickr ネットワークに登録されているユーザーが表示されます。現在のユーザーについては、デバイスの表示、詳細の編集、一時停止、削除、別の Wickr ネットワークへの切り替えを行うことができます。

ユーザーを作成する

ユーザーを作成するには、次の手順を実行します。

1. https://console.aws.amazon.com/wickr/ で Wickr AWS Management Console の を開きます。

2. ネットワーク ページで 管理 リンクを選択し、そのネットワークの Wickr 管理コンソールに移動します。

   特定のネットワークの Wickr 管理コンソールにリダイレクトされます。

3. Wickr 管理コンソールのナビゲーションペインで、「ユーザー」を選択し、「チームディレクトリ」を選択します。
4. 新しいユーザーの作成 を選択します。
5. 表示されるフォームに、ユーザーの名、姓、国コード、電話番号、メールアドレスを入力します。必須のフィールドは E メールアドレスだけです。ユーザーに適したセキュリティグループを必ず選択してください。Wickr は、ユーザーに指定したアドレスに招待メールを送信します。
6. Create (作成) を選択します。

   メールがユーザーに送信されます。この E メールには、Wickr クライアントアプリケーションのダウンロードリンクと Wickr に登録するためのリンクが記載されています。ユーザーが E メール内のリンクを使用して Wickr に登録すると、Wickr チームディレクトリのステータスが 保留中 から アクティブ に変わります。

ユーザーの編集

ユーザーを編集するには、次の手順を実行します。

1. https://console.aws.amazon.com/wickr/ で Wickr AWS Management Console の を開きます。
2. ネットワーク ページで 管理 リンクを選択し、そのネットワークの Wickr 管理コンソールに移動します。

   特定のネットワークの Wickr 管理コンソールにリダイレクトされます。

3. Wickr 管理コンソールのナビゲーションペインで、「ユーザー」を選択し、「チームディレクトリ」を選択します。
4. 削除するユーザーの名前の横にある縦の省略記号アイコンを選択します。
5. 次のオプションのいずれかを選択します。

   - デバイス — ユーザーが Wickr クライアントで設定したデバイスを表示します。
   - 編集 — 名前、国コード、電話番号 (オプション)、割り当てられたセキュリティグループなどのユーザーの詳細を編集します。

- 一時停止 — Wickr クライアントで Wickr ネットワークにサインインできないように、ユーザーを一時停止します。現在クライアントで Wickr ネットワークにサインインしているユーザーを一時停止すると、そのユーザーは自動的にサインアウトされます。
- 削除 — Wickr ネットワークからユーザーを削除します。

ユーザーの削除

ユーザーを削除するには、次の手順を実行します。

1. https://console.aws.amazon.com/wickr/ で Wickr AWS Management Console の を開きます。
2. ネットワーク ページで 管理 リンクを選択し、そのネットワークの Wickr 管理コンソールに移動します。

   特定のネットワークの Wickr 管理コンソールにリダイレクトされます。
3. Wickr 管理コンソールのナビゲーションペインで、「ユーザー」を選択し、「チームディレクトリ」を選択します。
4. 削除するユーザーの名前の横にある縦の省略記号アイコンを選択します。
5. ユーザーを削除するには、削除を選択します。

   ユーザーを削除すると、そのユーザーは Wickr クライアントで Wickr ネットワークにサインインできなくなります。

ユーザーの一括削除

Wickr 用の Wickr 管理コンソールのユーザーセクションで、Wickr ネットワークユーザーの一括削除と一括停止を行うことができます。

CSV テンプレートを使用して Wickr ネットワークユーザーの一括を削除するには、次の手順を実行します。

1. https://console.aws.amazon.com/wickr/ で Wickr AWS Management Console の を開きます。
2. Wickr 管理コンソールのナビゲーションペインで、「ユーザー」を選択し、「チームディレクトリ」を選択します。

   「チームディレクトリ」ページには、Wickr ネットワークに登録されているユーザーが表示されます。

3. 「チームディレクトリ」ページで、「ユーザーを管理」を選択します。
4. 「ユーザーを管理」ポップアップウィンドウで、「ユーザーを削除」を選択します。
5. サンプル CSV テンプレートをダウンロードします。サンプル テンプレートをダウンロードするには、テンプレートのダウンロード を選択します。
6. ネットワークから一括削除したいユーザーのメールを追加して、テンプレートを完成させます。
7. 完成した CSV テンプレートをアップロードします。ファイルをアップロードボックスにドラッグアンドドロップするか、ファイルを選択 を選択します。
8. チェックボックス、ユーザーの削除は元に戻せないことを認めますを選択します。
9. 「ユーザーの削除」を選択します。

> **Note**
>
> この操作ではただちにユーザーの削除が開始され、数分かかる場合があります。削除したユーザーは、Wickr クライアントで Wickr ネットワークにサインインできなくなります。

チームディレクトリの CSV をダウンロードして Wickr ネットワークユーザーを一括削除するには、次の手順を実行します。

1. https://console.aws.amazon.com/wickr/ で Wickr AWS Management Console の を開きます。
2. Wickr 管理コンソールのナビゲーションペインで、「ユーザー」を選択し、「チームディレクトリ」を選択します。

   「チームディレクトリ」ページには、Wickr ネットワークに登録されているユーザーが表示されます。
3. チームディレクトリ ページの右上隅にある CSV をダウンロード アイコンを選択します。
4. チームディレクトリ CSV テンプレートをダウンロードしたら、削除する必要のないユーザーの行を削除します。
5. 「チームディレクトリ」ページで、「ユーザーを管理」を選択します。
6. 「ユーザーを管理」ポップアップウィンドウで、「ユーザーを削除」を選択します。
7. チームディレクトリ CSV テンプレートをアップロードします。ファイルをアップロードボックスにドラッグアンドドロップするか、ファイルを選択 を選択します。
8. チェックボックス、ユーザーの削除は元に戻せないことを認めますを選択します。
9. 「ユーザーの削除」を選択します。

> **Note**
>
> この操作ではただちにユーザーの削除が開始され、数分かかる場合があります。削除したユーザーは、Wickr クライアントで Wickr ネットワークにサインインできなくなります。

ユーザーの一括停止

Wickr 用の Wickr 管理コンソールのユーザーセクションで、Wickr ネットワークユーザーの一括削除と一括停止を行うことができます。

Wickr ネットワークユーザーの一括利用を停止するには、次の手順を実行します。

1. https://console.aws.amazon.com/wickr/ で Wickr AWS Management Console の を開きます。
2. Wickr 管理コンソールのナビゲーションペインで、「ユーザー」を選択し、「チームディレクトリ」を選択します。

   「チームディレクトリ」ページには、Wickr ネットワークに登録されているユーザーが表示されます。
3. 「チームディレクトリ」ページで、「ユーザーを管理」を選択します。
4. 「ユーザーを管理」ポップアップウィンドウで、「ユーザーを一時停止」を選択します。
5. サンプル CSV テンプレートをダウンロードします。サンプル テンプレートをダウンロードするには、テンプレートのダウンロード を選択します。
6. ネットワークから一括停止したいユーザーのメールアドレスを追加して、テンプレートを完成させます。
7. 完成した CSV テンプレートをアップロードします。ファイルをアップロードボックスにドラッグアンドドロップするか、ファイルを選択 を選択します。
8. CSV ファイルをアップロードしたら、ユーザーを一時停止 を選択します。

> **Note**
>
> この操作を行うと、ただちにユーザーの利用停止が開始され、数分かかる場合があります。利用停止中のユーザーは、Wickr クライアントで Wickr ネットワークにサインイン

できません。現在クライアントで Wickr ネットワークにサインインしているユーザーを一時停止すると、そのユーザーは自動的にサインアウトされます。

ゲストユーザー

Wickr ゲストユーザー機能を使用すると、個々のゲストユーザーが Wickr クライアントにサインインし、Wickr ネットワークユーザーと共同作業を行うことができます。Wickr 管理者は、Wickr 管理コンソールの セキュリティグループ ページで、Wickr ネットワークのゲストユーザーを有効または無効にできます。

この機能を有効にすると、Wickr ネットワークに招待されたゲストユーザーは、Wickr ネットワーク内のユーザーとやり取りできるようになります。ゲストユーザー機能には AWS アカウント に料金がかかります。ゲストユーザー機能の料金について詳しくは、「アドオンの料金設定」の「Wickr 料金ページ」を参照してください。

トピック

ゲストユーザーを有効または無効にする

Wickr ネットワークのゲストユーザーを有効または無効にするには、以下の手順を実行します。

1. https://console.aws.amazon.com/wickr/ で Wickr の AWS Management Console を開きます。
2. ネットワーク ページで 管理 リンクを選択し、そのネットワークの Wickr 管理コンソールに移動します。

   特定のネットワークの Wickr 管理コンソールにリダイレクトされます。
3. Wickr 管理コンソールのナビゲーションペインで ネットワーク設定 を選択し、セキュリティグループ を選択します。
4. 特定のセキュリティグループの 詳細 を選択します。

> **Note**
>
> ゲストユーザーは個々のセキュリティグループでのみ有効にできます。Wickr ネットワーク内のすべてのセキュリティグループでゲストユーザーを有効にするには、ネットワーク内のセキュリティグループごとにこの機能を有効にする必要があります。

5. セキュリティグループの詳細ページで フェデレーション タブを選択します。
6. ゲストユーザーを許可するように切り替えることができる場所は 2 つあります。
   - ローカルフェデレーション：米国東部 (バージニア北部) のネットワークでは、ページの ローカルフェデレーション セクションの横にある 編集 を選択します。
   - グローバルフェデレーション：他の地域の他のすべてのネットワークでは、ページの グローバルフェデレーション セクションの横にある 編集 を選択します。
7. セキュリティグループのゲストユーザーを有効にするには、ゲストユーザーを許可する を選択し、無効にする場合は選択を解除します。
8. 保存 を選択して変更を保存し、セキュリティグループで有効にします。

   これで、Wickr ネットワーク内の特定のセキュリティグループの登録ユーザーがゲストユーザーとやり取りできるようになります。詳細については、「Wickr ユーザーガイド」の「ゲストユーザー」を参照してください。

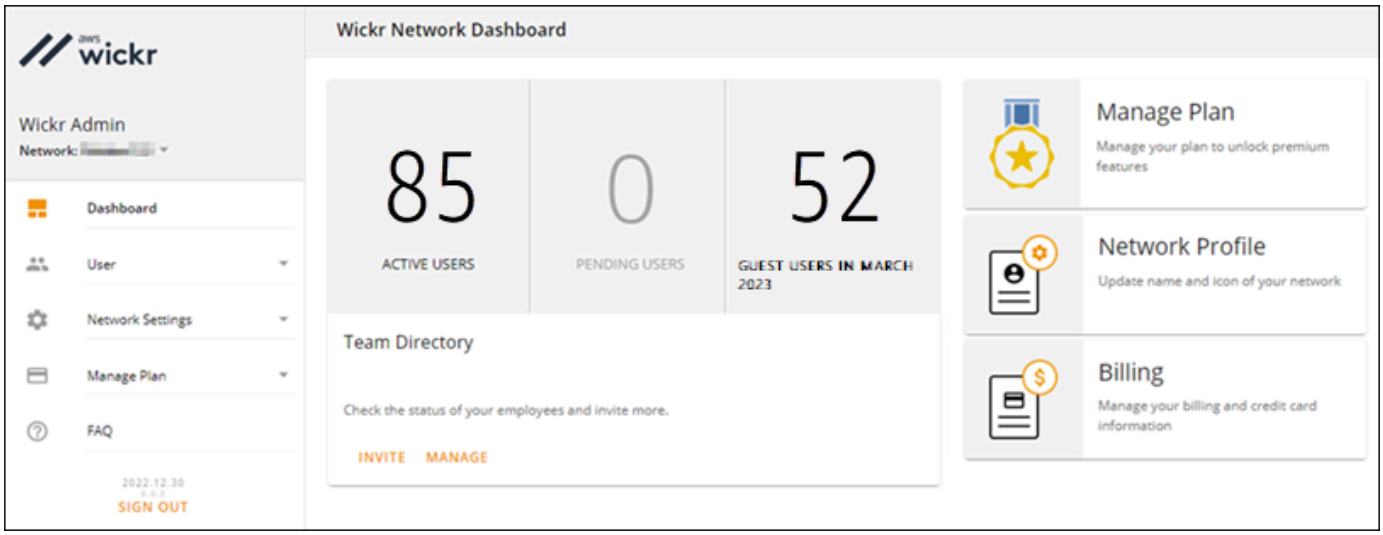
> **Note**
>
> Wickr ゲストユーザー機能は、AWS GovCloud (US)西部 (AWS) では使用できません WickrGov。

ゲストユーザー数の表示

Wickr ネットワークのゲストユーザー数を表示するには、以下の手順を実行します。

1. https://console.aws.amazon.com/wickr/ で Wickr の AWS Management Console を開きます。
2. ネットワーク ページで 管理 リンクを選択し、そのネットワークの Wickr 管理コンソールに移動します。

特定のネットワークの Wickr 管理コンソールにリダイレクトされます。ダッシュボード ページには、次の例のように Wickr ネットワークのゲストユーザー数が表示されます。



毎月の使用状況の表示

請求期間中にネットワークが通信したゲストユーザーの数を表示できます。毎月の使用状況を 確認するには、次のステップを実行します。

1. https://console.aws.amazon.com/wickr/ で Wickr の AWS Management Console を開きます。
2. ネットワーク ページで 管理 リンクを選択し、そのネットワークの Wickr 管理コンソールに移動します。
3. コンソールのナビゲーションペインで、ユーザー、ユーザーの追加 の順に選択します。
4. ゲストユーザー ページで、毎月の使用状況 セクションを選択します。

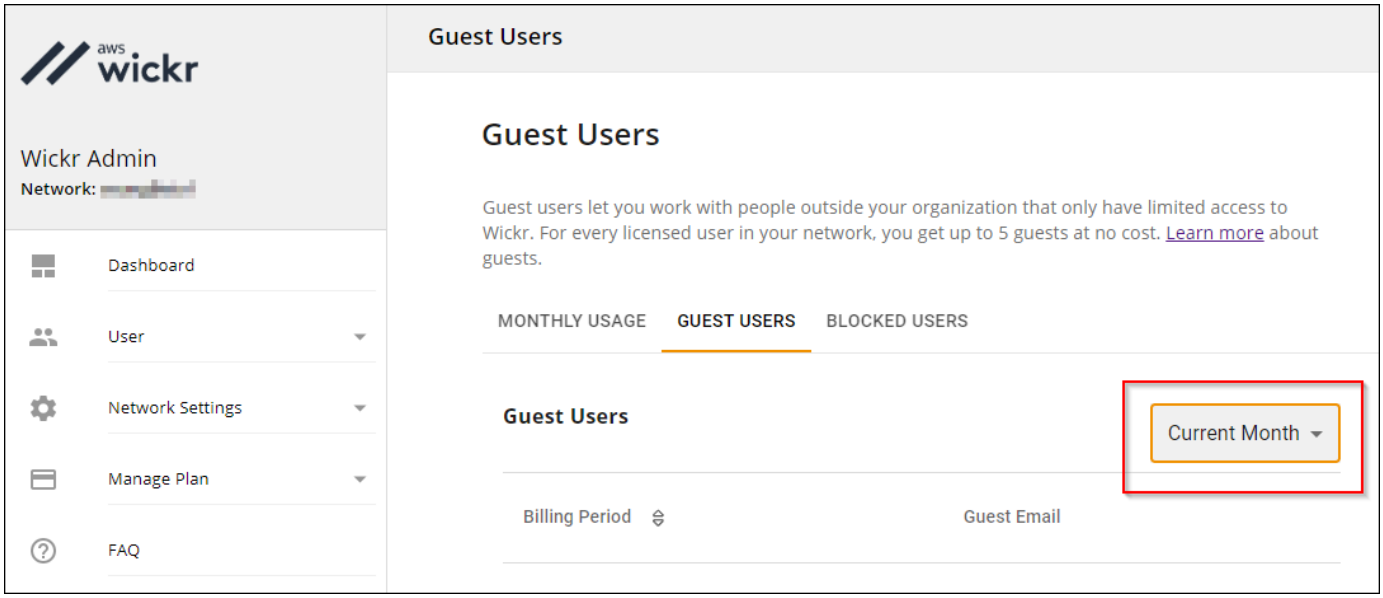
> **Note**
>
> ゲストの請求データは 24 時間ごとに更新されます。

ゲストユーザーの表示

特定の請求期間中にネットワークユーザーが通信したゲストユーザーのリストを表示できます。ゲストユーザーを確認するには、次のステップを実行します。

1. https://console.aws.amazon.com/wickr/ で Wickr の AWS Management Console を開きます。

2. ネットワーク ページで 管理 リンクを選択し、そのネットワークの Wickr 管理コンソールに移動します。
3. コンソールのナビゲーションペインで、ユーザー、ユーザーの追加 の順に選択します。
4. ゲストユーザー ページで、ゲストユーザー セクションを選択します。
5. 特定の月のゲストユーザーを表示するには、ドロップダウンメニューから該当する月を選択します。



ゲストユーザーのブロック

ブロックされたユーザーは、ネットワーク内の誰とも通信できません。

ゲストユーザーをブロックするには

1. https://console.aws.amazon.com/wickr/ で Wickr の AWS Management Console を開きます。
2. ネットワーク ページで 管理 リンクを選択し、そのネットワークの Wickr 管理コンソールに移動します。
3. コンソールのナビゲーションペインで、ユーザー、ユーザーの追加 の順に選択します。
4. ゲストユーザー ページで、ゲストユーザー セクションを選択します。
5. ゲストユーザー セクションには、Wickr ネットワークで通信したゲストユーザーが表示されます。
6. ゲストユーザー セクションで、ブロックしたいゲストユーザーの E メールを探します。
7. ゲストユーザー名の右側にある 3 つのドットを選択し、ブロック を選択します。

8. ポップアップウィンドウで ブロック を選択します。
9. Wickr ネットワーク内のブロックされたユーザーのリストを表示するには、ブロックされたユーザー セクションを選択します。

ゲストユーザーのブロックを解除するには

1. https://console.aws.amazon.com/wickr/ で Wickr の AWS Management Console を開きます。
2. ネットワーク ページで 管理 リンクを選択し、そのネットワークの Wickr 管理コンソールに移動します。
3. コンソールのナビゲーションペインで、ユーザー、ユーザーの追加 の順に選択します。
4. ゲストユーザー ページで、ブロックされたユーザー セクションを選択します。
5. ブロックされたユーザー セクションには、Wickr ネットワークでブロックされているゲストユーザーが表示されます。
6. ブロックされたユーザー セクションで、ブロックを解除したいゲストユーザーの E メールを探します。
7. ゲストユーザー名の右側にある 3 つのドットを選択し、ブロック解除 を選択します。
8. ポップアップウィンドウで ブロック解除 を選択します。

AWS Wickr のセキュリティ

AWS クラウドセキュリティは最優先事項です。 AWS お客様は、最もセキュリティに敏感な組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャの恩恵を受けることができます。

セキュリティは、 AWS お客様とお客様との間で共有される責任です。責任共有モデル では、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ — AWS AWS AWS クラウドクラウド内でサービスを実行するインフラストラクチャを保護する責任があります。 AWS また、安全に使用できるサービスも提供します。第三者監査人は、AWS、当社のセキュリティの有効性を定期的にテストおよび検証しています。AWS Wickr に適用されるコンプライアンスプログラムについては、「AWS コンプライアンスプログラム別の対象サービス」「」を参照してください。
- クラウドのセキュリティ — お客様の責任は、 AWS 使用するサービスによって決まります。また、お客様は、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、Wickr を使用する際に責任共有モデルを適用する方法を理解するのに役立ちます。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成するために Wickr を設定する方法を示します。また、Wickr AWS リソースの監視と保護に役立つ他のサービスの使い方についても学びます。

トピック

AWS Wickr でのデータ保護

AWS https://aws.amazon.com/compliance/shared-responsibility-model/、AWS Wickr のデータ保護に適用されます。このモデルで説明されているように、 AWS はすべてを実行するグローバルインフラストラクチャを保護する責任があります。 AWS クラウドお客様は、このインフラストラクチャでホストされているコンテンツに対する管理を維持する責任があります。また、使用する AWS のサービス のセキュリティ設定と管理タスクもユーザーの責任となります。データプライバシーの詳細については、「データプライバシーのよくある質問」を参照してください。欧州でのデータ保護の詳細については、「AWS セキュリティブログ」に投稿された「AWS 責任共有モデルおよび GDPR」のブログ記事を参照してください。

データ保護の観点から、 AWS アカウント 認証情報を保護し、 AWS IAM Identity Center または AWS Identity and Access Management (IAM) を使用して個々のユーザーを設定することをお勧めします。こうすると、それぞれのジョブを遂行するために必要なアクセス許可のみを各ユーザーに付与できます。また、以下の方法でデータを保護することをお勧めします。

- 各アカウントで多要素認証 (MFA) を使用します。
- SSL/TLS を使用してリソースと通信します。 AWS TLS 1.2、できれば TLS 1.3 が必要です。
- を使用して API とユーザーアクティビティの口ギングを設定します。 AWS CloudTrail
- AWS 暗号化ソリューションと、 AWS のサービスその中に含まれるデフォルトのセキュリティコントロールをすべて使用してください。
- Amazon Macie などの高度なマネージドセキュリティサービスを使用します。これらは、Amazon S3 に保存されている機密データの検出と保護を支援します。
- コマンドラインインターフェイスまたは API AWS を介してアクセスするときに FIPS 140-2 で検証された暗号モジュールが必要な場合は、FIPS エンドポイントを使用してください。利用可能な FIPS エンドポイントの詳細については、「連邦情報処理規格 (FIPS) 140-2」を参照してください。

お客様の E メールアドレスなどの機密情報やセンシティブ情報は、タグや名前フィールドなどの自由形式のフィールドに配置しないことを強くお勧めします。これには、コンソール、API、または SDK を使用して Wickr AWS のサービス などを使用する場合も含まれます。 AWS CLI AWS 名前に使用する自由記述のテキストフィールドやタグに入力したデータは、課金や診断ログに使用される場合があります。外部サーバーへの URL を提供する場合は、そのサーバーへのリクエストを検証するための認証情報を URL に含めないように強くお勧めします。

AWS Wickr の ID とアクセス管理

AWS Identity and Access Management (IAM) は、 AWS のサービス 管理者がリソースへのアクセスを安全に制御できるようにするものです。 AWS IAM 管理者は、Wickr リソースを使用するための認証 (サインイン) および 許可 (アクセス許可を持たせる) を行うことができる人を制御します。IAM AWS のサービス は追加料金なしで使用できるアプリです。

トピック

対象者

使用方法 AWS Identity and Access Management (IAM) は、Wickr で行う作業によって異なります。

サービスユーザー – Wickr サービスを使用してジョブを実行する場合は、必要な認証情報とアクセス許可を管理者が提供します。作業を実行するためにさらに多くの Wickr の機能を使用するとき、追加の許可が必要になる場合があります。アクセスの管理方法を理解しておくと、管理者に適切な許可をリクエストするうえで役立ちます。Wickr の特徴にアクセスできない場合は、「AWS Wickr の ID とアクセスのトラブルシューティング」を参照してください。

サービス管理者 - 社内の Wickr リソースを担当している場合は、通常、Wickr へのフルアクセスがあります。サービスのユーザーがどの Wickr 機能やリソースにアクセスするかを決めるのは管理者の仕事です。その後、IAM 管理者にリクエストを送信して、サービスユーザーの権限を変更する必要があります。このページの情報を点検して、IAM の基本概念を理解してください。貴社で Wickr で IAM を利用する方法の詳細については、AWS Wickr と IAM の連携方法 をご参照ください。

IAM 管理者 - 管理者は、Wickr へのアクセスを管理するポリシーの作成方法の詳細について確認する場合があります。IAM で使用できる Wickr アイデンティティベースのポリシーの例を表示するには、AWS Wickr のアイデンティティベースのポリシーの例 を参照してください。

アイデンティティを使用した認証

認証とは、ID AWS 認証情報を使用してサインインする方法です。IAM ユーザーとして AWS アカウントのルートユーザー、または IAM ロールを引き受けて認証 (サインイン AWS) する必要があります。

ID ソースを通じて提供された認証情報を使用して、フェデレーション ID AWS としてサインインできます。 AWS IAM Identity Center フェデレーテッド ID の例としては、(IAM Identity Center) ユーザー、会社のシングルサインオン認証、Google や Facebook の認証情報などがあります。フェデレーションアイデンティティとしてサインインする場合、IAM ロールを使用して、前もって管理者により ID フェデレーションが設定されています。 AWS フェデレーションを使用してアクセスすると、間接的にロールを引き継ぐことになります。

ユーザーのタイプによっては、 AWS Management Console AWS またはアクセスポータルにサインインできます。へのサインインについて詳しくは AWS、『AWS サインイン ユーザーガイド』の「AWS アカウントにサインインする方法」を参照してください。

AWS プログラムでアクセスする場合は、認証情報を使用してリクエストに暗号署名するためのソフトウェア開発キット (SDK) とコマンドラインインターフェイス (CLI) AWS を提供します。 AWS ツールを使用しない場合は、リクエストに自分で署名する必要があります。推奨方法を使用して自分でリクエストに署名する方法の詳細については、IAM ユーザーガイドの「 AWS API リクエストへの署名」を参照してください。

使用する認証方法を問わず、セキュリティ情報の提供を追加でリクエストされる場合もあります。たとえば、アカウントのセキュリティを強化するために多要素認証 (MFA) AWS を使用することを推奨しています。詳細については、「AWS IAM Identity Center ユーザーガイド」の「多要素認証」および「IAM ユーザーガイド」の「AWSでの多要素認証 (MFA) の使用」を参照してください。

AWS アカウント root ユーザー

を作成するときは AWS アカウント、 AWS のサービス アカウント内のすべてのリソースに完全にアクセスできる 1 つのサインイン ID から始めます。この ID は AWS アカウント root ユーザーと呼ばれ、アカウントの作成に使用したメールアドレスとパスワードでサインインすることでアクセスされます。日常的なタスクには、ルートユーザーを使用しないことを強くお勧めします。ルートユーザーの認証情報を保護し、それらを使用してルートユーザーのみが実行できるタスクを実行してください。ルートユーザーとしてサインインする必要があるタスクの完全なリストについては、「IAM ユーザーガイド」の「ルートユーザー認証情報が必要なタスク」を参照してください。

フェデレーション ID

ベストプラクティスとして、管理者アクセスを必要とするユーザーを含む人間のユーザーに、ID AWS のサービス プロバイダーとのフェデレーションを使用して一時的な認証情報を使用してアクセスするように要求します。

フェデレーテッド ID とは、エンタープライズユーザーディレクトリ、ウェブ ID プロバイダー、Identity Center ディレクトリのユーザー、または ID AWS のサービス ソースを通じて提供された認証情報を使用してアクセスする任意のユーザーです。 AWS Directory Serviceフェデレーテッド ID がアクセスすると AWS アカウント、そのユーザーがロールを引き受け、そのロールが一時的な認証情報を提供します。

アクセスを一元管理する場合は、 AWS IAM Identity Centerを使用することをお勧めします。IAM Identity Center でユーザーとグループを作成したり、独自のアイデンティティソース内のユーザーやグループに接続して同期したりして、すべてのアプリケーションで使用することができます。 AWS アカウント IAM Identity Center の詳細については、「AWS IAM Identity Center ユーザーガイド」の「IAM Identity Center とは？」を参照してください。

IAM ユーザーとグループ

IAM ユーザーは、1 人のユーザーまたはアプリケーションに対して特定の権限を持つ社内の AWS アカウント ID です。可能であれば、パスワードやアクセスキーなどの長期的な認証情報を保有する IAM ユーザーを作成する代わりに、一時的な認証情報を使用することをお勧めします。ただし、IAM ユーザーでの長期的な認証情報が必要な特定のユースケースがある場合は、アクセスキーをローテーションすることをお勧めします。詳細については、IAM ユーザーガイドの「長期的な認証情報を必要とするユースケースのためにアクセスキーを定期的にローテーションする」を参照してください。

IAM グループ は、IAM ユーザーの集団を指定するアイデンティティです。グループとしてサインインすることはできません。グループを使用して、複数のユーザーに対して一度に権限を指定できます。多数のユーザーグループがある場合、グループを使用することで権限の管理が容易になります。例えば、IAMAdmins という名前のグループを設定して、そのグループに IAM リソースを管理する許可を与えることができます。

ユーザーは、ロールとは異なります。ユーザーは 1 人の人または 1 つのアプリケーションに一意に関連付けられますが、ロールはそれを必要とする任意の人が引き受けるようになっています。ユーザーには永続的な長期の認証情報がありますが、ロールでは一時的な認証情報が提供されます。詳細については、「IAM ユーザーガイド」の「IAM ユーザー (ロールではなく) の作成が適している場合」を参照してください。

IAM ロール

IAM ロールは、 AWS アカウント 特定の権限を持つ社内の ID です。これは IAM ユーザーに似ていますが、特定のユーザーには関連付けられていません。 AWS Management Console ロールを切り替えることで、の IAM ロールを一時的に引き受けることができます。 AWS CLI または AWS API オペレーションを呼び出すか、カスタム URL を使用してロールを引き受けることができます。ロールを使用する方法の詳細については、「IAM ユーザーガイド」の「IAM ロールの使用」を参照してください。

一時的な認証情報を持った IAM ロールは、以下の状況で役立ちます。

- フェデレーションユーザーアクセス – フェデレーションアイデンティティに権限を割り当てるには、ロールを作成してそのロールの権限を定義します。フェデレーションアイデンティティが認証されると、そのアイデンティティはロールに関連付けられ、ロールで定義されている権限が付与されます。フェデレーションの詳細については、「IAM ユーザーガイド」の「サードパーティーアイデンティティプロバイダー向けロールの作成」を参照してください。IAM アイデンティティセンターを使用する場合、権限セットを設定します。アイデンティティが認証後にアクセスできるものを制御するため、IAM Identity Center は、権限セットを IAM のロールに関連付けます。アクセス許可セットの詳細については、「AWS IAM Identity Center ユーザーガイド」の「アクセス許可セット」を参照してください。
- 一時的な IAM ユーザー権限 - IAM ユーザーまたはロールは、特定のタスクに対して複数の異なる権限を一時的に IAM ロールで引き受けることができます。
- クロスアカウントアクセス - IAM ロールを使用して、自分のアカウントのリソースにアクセスすることを、別のアカウントの人物 (信頼済みプリンシパル) に許可できます。クロスアカウントアクセス権を付与する主な方法は、ロールを使用することです。ただし、ロールをプロキシとして使用する代わりに AWS のサービス、ポリシーをリソースに直接アタッチできるものもあります。クロスアカウントアクセスにおけるロールとリソースベースのポリシーの違いについては、「IAM ユーザーガイド」の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。
- クロスサービスアクセス — AWS のサービス AWS のサービス他の機能を使用するものもあります。例えば、あるサービスで呼び出しを行うと、通常そのサービスによって Amazon EC2 でアプリケーションが実行されたり、Amazon S3 にオブジェクトが保存されたりします。サービスでは、呼び出し元プリンシパルの許可、サービスロール、またはサービスリンクロールを使用してこれを行う場合があります。
  - 転送アクセスセッション (FAS) — IAM ユーザーまたはロールを使用してアクションを実行する場合 AWS、あなたはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FAS

は、 AWS のサービス を呼び出したプリンシパルの権限をリクエスト元と組み合わせて使用して AWS のサービス、ダウンストリームサービスにリクエストを行います。FASリクエストは、AWS のサービス サービスが他のユーザーとのやりとりやリソースとのやり取りを必要とするリクエストを受信したときにのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

- サービスロール - サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。
- サービスにリンクされたロール — サービスにリンクされたロールは、にリンクされているサービスロールの一種です。 AWS のサービスサービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。 AWS アカウント サービスにリンクされたロールはに表示され、そのサービスが所有します。IAM 管理者は、サービスリンクロールの許可を表示できますが、編集することはできません。

- Amazon EC2 で実行されるアプリケーション — IAM ロールを使用して、EC2 インスタンスで実行され、 AWS API AWS CLI リクエストを行うアプリケーションの一時的な認証情報を管理できます。これは、EC2 インスタンス内でのアクセスキーの保存に推奨されます。EC2 AWS インスタンスにロールを割り当て、そのロールをそのすべてのアプリケーションで使用できるようにするには、インスタンスにアタッチされるインスタンスプロファイルを作成します。インスタンスプロファイルにはロールが含まれ、EC2 インスタンスで実行されるプログラムは一時的な認証情報を取得できます。詳細については、「IAM ユーザーガイド」の「Amazon EC2 インスタンスで実行されるアプリケーションに IAM ロールを使用して許可を付与する」を参照してください。

IAM ロールと IAM ユーザーのどちらを使用するかについては、「IAM ユーザーガイド」の「(IAM ユーザーではなく) IAM ロールをいつ作成したら良いのか」を参照してください。

ポリシーを使用したアクセスの管理

AWS ポリシーを作成して AWS ID またはリソースにアタッチすることで、アクセスを制御します。ポリシーとは、ID またはリソースに関連付けると権限を定義するオブジェクトです。 AWS AWS プリンシパル (ユーザー、ルートユーザー、またはロールセッション) がリクエストを行うと、これらのポリシーを評価します。ポリシーでの権限により、リクエストが許可されるか拒否されるかが決まります。ほとんどのポリシーは JSON AWS ドキュメントとして保存されます。JSON ポリシードキュメントの構造と内容の詳細については、「IAM ユーザーガイド」の「JSON ポリシー概要」を参照してください。

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

デフォルトでは、ユーザーやロールに権限はありません。IAM 管理者は、リソースで必要なアクションを実行するための権限をユーザーに付与する IAM ポリシーを作成できます。その後、管理者はロールに IAM ポリシーを追加し、ユーザーはロールを引き継ぐことができます。

IAM ポリシーは、オペレーションの実行方法を問わず、アクションの権限を定義します。例えば、`iam:GetRole` アクションを許可するポリシーがあるとします。そのポリシーを持つユーザは AWS Management Console、、 AWS CLI、または AWS API からロール情報を取得できます。

アイデンティティベースのポリシー

アイデンティティベースポリシーは、IAM ユーザー、ユーザーグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」を参照してください。

アイデンティティベースのポリシーは、さらに インラインポリシー または マネージドポリシー に分類できます。インラインポリシーは、単一のユーザー、グループ、またはロールに直接埋め込まれています。管理ポリシーは、内の複数のユーザ、グループ、およびロールにアタッチできるスタンドアロンポリシーです。 AWS アカウント管理ポリシーには、 AWS 管理ポリシーと顧客管理ポリシーが含まれます。マネージドポリシーまたはインラインポリシーのいずれかを選択する方法については、「IAM ユーザーガイド」の「マネージドポリシーとインラインポリシーの比較」を参照してください。

リソースベースのポリシー

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーが添付されているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザ、ロール、フェデレーティッドユーザ、またはを含めることができます。 AWS のサービス

リソースベースのポリシーは、そのサービス内にあるインラインポリシーです。IAM AWS の管理ポリシーをリソースベースのポリシーで使用することはできません。

アクセスコントロールリスト (ACL)

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための権限を持つかをコントロールします。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

ACL をサポートするサービスの例としては AWS WAF、Amazon S3、、および Amazon VPC があります。ACL の詳細については、「Amazon Simple Storage Service デベロッパーガイド」の「アクセスコントロールリスト (ACL) の概要」を参照してください。

その他のポリシータイプ

AWS あまり一般的ではないポリシータイプもサポートしています。これらのポリシータイプでは、より一般的なポリシータイプで付与された最大の権限を設定できます。

- アクセス許可の境界 - アクセス許可の境界は、アイデンティティベースのポリシーによって IAM エンティティ (IAM ユーザーまたはロール) に付与できる許可の上限を設定する高度な機能です。エンティティに許可の境界を設定できます。結果として許可される範囲は、エンティティのアイデンティティベースポリシーとその許可の境界の共通部分になります。`Principal` フィールドでユーザーまたはロールを指定するリソースベースのポリシーでは、許可の境界は制限されません。これらのポリシーのいずれかを明示的に拒否した場合、許可は無効になります。アクセス許可の境界の詳細については、「IAM ユーザーガイド」の「IAM エンティティのアクセス許可の境界」を参照してください。
- セッションポリシー - セッションポリシーは、ロールまたはフェデレーティッドユーザーの一時的なセッションをプログラムで作成する際にパラメータとして渡す高度なポリシーです。結果としてセッションの権限される範囲は、ユーザーまたはロールのアイデンティティベースポリシーとセッションポリシーの共通部分になります。また、リソースベースのポリシーから権限が派生する場合もあります。これらのポリシーのいずれかを明示的に拒否した場合、許可は無効になります。詳細については、 IAM ユーザーガイド の「セッションポリシー」を参照してください。

複数のポリシータイプ

1 つのリクエストに複数のタイプのポリシーが適用されると、結果として作成される権限を理解するのがさらに難しくなります。 AWS 複数のポリシータイプが関係している場合にリクエストを許可するかどうかを決定する方法については、IAM ユーザーガイドの「ポリシー評価ロジック」を参照してください。

AWS AWS Wickr のマネージドポリシー

ユーザ、グループ、ロールに権限を追加するには、 AWS 自分でポリシーを作成するよりも管理ポリシーを使用する方が簡単です。チームに必要な許可のみを提供する IAM カスタマーマネージドポリシーを作成するには、時間と専門知識が必要です。すぐに始めるには、 AWS 管理ポリシーをご利用ください。これらのポリシーは、一般的なユースケースをターゲット範囲に含めており、 AWS アカウントで利用できます。 AWS 管理ポリシーの詳細については、IAM ユーザーガイドの「AWS 管理ポリシー」を参照してください。

AWS のサービス AWS 管理ポリシーの保守と更新。 AWS 管理ポリシーの権限は変更できません。サービスでは、新しい機能を利用できるようにするために、 AWS マネージドポリシーに権限が追加されることがあります。この種類の更新は、ポリシーがアタッチされている、すべてのアイデンティティ (ユーザー、グループおよびロール) に影響を与えます。新しい機能が立ち上げられた場合や、新しいオペレーションが使用可能になった場合に、各サービスが AWS マネージドポリシーを更新する可能性が最も高くなります。 AWS サービスは管理ポリシーから権限を削除しないため、ポリシーを更新しても既存の権限が損なわれることはありません。

AWS 管理ポリシー: AWSWickrFullAccess

`AWSWickrFullAccess` ポリシーは IAM ID にアタッチできます。このポリシーは、 AWS Management Console内の Wickr の AWS Management Console を含む、Wickr サービスに対する完全な管理権限を付与します。IAM アイデンティティへのポリシーのアタッチに関する詳細については、「AWS Identity and Access Management IAM ユーザーガイド」の「IAM ID の許可の追加と削除」を参照してください。

アクセス許可の詳細

このポリシーには、以下のアクセス許可が含まれています。

- `wickr`— Wickr サービスに完全な管理者権限を付与します。

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

```
}
```

Wickr AWS による管理ポリシーの更新

このサービスが変更の追跡を開始して以降の Wickr AWS の管理ポリシーの更新に関する詳細を表示します。このページへの変更に関する自動アラートを受信するには、Wickr ドキュメント履歴ページで RSS フィードを購読してください。

変更	説明	日付
AWSWickrFullAccess - 新しいポリシー	Wickr は、 AWS Management Consoleの Wickr 管理者コンソールを含む Wickr サービスに完全な管理者権限を付与する新しいポリシーを追加しました。	2022 年 11 月 28 日
Wickr は変更の追跡を開始しました	Wickr は管理ポリシーの変更の追跡を開始しました。 AWS	2022 年 11 月 28 日

AWS Wickr と IAM の連携方法

IAM を使用して Wickr へのアクセスを管理する前に、Wickr で利用できる IAM の機能について学びます。

AWS Wickr で使用できる IAM 機能

IAM 機能	Wickr サポート
アイデンティティベースのポリシー	Yes
リソースベースのポリシー	いいえ
ポリシーアクション	Yes
ポリシーリソース	いいえ
ポリシー条件キー	いいえ

IAM 機能	Wickr サポート
ACL	No
ABAC (ポリシー内のタグ)	いいえ
一時的な認証情報	いいえ
プリンシパル権限	いいえ
サービスロール	いいえ
サービスリンクロール	No

Wickr AWS やその他のサービスがほとんどの IAM 機能でどのように機能するかを大まかに把握するには、IAM ユーザーガイドの「IAM AWS と連携するサービス」を参照してください。

Wickr のアイデンティティベースのポリシー

アイデンティティベースポリシーをサポートする	Yes

アイデンティティベースポリシーは、IAM ユーザー、ユーザーのグループ、ロールなど、アイデンティティにアタッチできる JSON 許可ポリシードキュメントです。これらのポリシーは、ユーザーとロールが実行できるアクション、リソース、および条件をコントロールします。アイデンティティベースのポリシーを作成する方法については、「IAM ユーザーガイド」の「IAM ポリシーの作成」を参照してください。

IAM アイデンティティベースのポリシーでは、許可または拒否するアクションとリソース、およびアクションを許可または拒否する条件を指定できます。プリンシパルは、それが添付されているユーザーまたはロールに適用されるため、アイデンティティベースのポリシーでは指定できません。JSON ポリシーで使用できるすべての要素について学ぶには、「IAM ユーザーガイド」の「IAM JSON ポリシーの要素のリファレンス」を参照してください。

Wickr のアイデンティティベースのポリシーの例

Wickr のアイデンティティベースのポリシーの例を表示するには、「AWS Wickr のアイデンティティベースのポリシーの例」を参照してください。

Wickr 内のリソースベースのポリシー

リソースベースのポリシーのサポート	なし

リソースベースのポリシーは、リソースに添付する JSON ポリシードキュメントです。リソースベースのポリシーには例として、IAM ロールの信頼ポリシーや Amazon S3 バケットポリシーがあげられます。リソースベースのポリシーをサポートするサービスでは、サービス管理者はポリシーを使用して特定のリソースへのアクセスを制御できます。ポリシーが添付されているリソースの場合、指定されたプリンシパルがそのリソースに対して実行できるアクションと条件は、ポリシーによって定義されます。リソースベースのポリシーでは、プリンシパルを指定する必要があります。プリンシパルには、アカウント、ユーザー、ロール、フェデレーティッドユーザー、またはが含まれます。AWS のサービス

クロスアカウントアクセスを有効にするには、アカウント全体、または別のアカウントの IAM エンティティをリソースベースのポリシーのプリンシパルとして指定します。リソースベースのポリシーにクロスアカウントのプリンシパルを追加しても、信頼関係は半分しか確立されない点に注意してください。プリンシパルとリソースが異なる場合 AWS アカウント、信頼されたアカウントの IAM 管理者は、プリンシパルエンティティ (ユーザーまたはロール) にリソースへのアクセス権限を付与する必要もあります。IAM 管理者は、アイデンティティベースのポリシーをエンティティにアタッチすることで権限を付与します。ただし、リソースベースのポリシーで、同じアカウントのプリンシパルへのアクセス権が付与されている場合は、アイデンティティベースのポリシーを追加する必要はありません。詳細については、「IAM ユーザーガイド」の「IAM ロールとリソースベースのポリシーとの相違点」を参照してください。

Wickr のポリシーアクション

ポリシーアクションに対するサポート	Yes

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

JSON ポリシーの `Action`要素には、ポリシー内のアクセスを許可または拒否するために使用できるアクションが記述されます。ポリシーアクションは通常、関連する AWS API オペレーションと同じ名前です。一致する API オペレーションのない 許可のみのアクション など、いくつかの例外があり

ます。また、ポリシーに複数アクションが必要なオペレーションもあります。これらの追加アクションは、 依存アクション と呼ばれます。

このアクションは、関連付けられたオペレーションを実行するためのアクセス許可を付与するポリシーで使用されます。

Wickr アクションのリストを確認するには、サービス認可リファレンス の「AWS Wickr で定義されるアクション」を参照してください。

Wickr のポリシーアクションは、アクションの前に以下のプレフィックス を使用します。

```
wickr
```

単一のステートメントで複数のアクションを指定するには、アクションをカンマで区切ります。

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

Wickr のアイデンティティベースのポリシーの例を表示するには、「AWS Wickr のアイデンティティベースのポリシーの例」を参照してください。

Wickr のポリシーリソース

ポリシーリソースに対するサポート	No

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかということです。

`Resource` JSON ポリシーの要素は、オブジェクトあるいはアクションが適用されるオブジェクトを指定します。ステートメントには、`Resource` または `NotResource`要素を含める必要があります。ベストプラクティスとしては、Amazon リソースネーム (ARN) を使用してリソースを指定します。これは、 リソースレベルの許可 と呼ばれる特定のリソースタイプをサポートするアクションに対して実行できます。

オペレーションのリスト化など、リソースレベルのアクセス許可をサポートしないアクションの場合は、ステートメントがすべてのリソースに適用されることを示すために、ワイルドカード (*) を使用します。

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

Wickr リソースタイプとその ARN のリストを表示するには、サービス認可リファレンス の「AWS Wickr によって定義されたリソース」を参照してください。どのアクションで各リソースの ARN を指定できるかについては、AWS Wickr で定義されるアクションを参照してください。

Wickr のアイデンティティベースのポリシーの例を表示するには、「AWS Wickr のアイデンティティベースのポリシーの例」を参照してください。

Wickr 向けのポリシー条件キー

サービス固有のポリシー条件キーのサポート	No

管理者は AWS JSON ポリシーを使用して、誰が何にアクセスできるかを指定できます。つまり、どの プリンシパル がどの リソース に対してどのような条件下 で アクション を実行できるかということです。

Condition 要素 (または Condition ブロック) を使用すると、ステートメントが有効な条件を指定できます。Condition 要素はオプションです。イコールや未満などの 条件演算子 を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の Condition要素を指定する場合、または 1 つの Condition要素に複数のキーを指定する場合、 AWS では AND論理演算子を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、 AWS OR論理演算を使用して条件を評価します。ステートメントの権限が付与される前にすべての条件が満たされる必要があります。

条件を指定する際にプレースホルダー変数も使用できます。例えば IAM ユーザーに、IAM ユーザー名がタグ付けされている場合のみリソースにアクセスできる権限を付与することができます。詳細については、 IAM ユーザーガイド の「IAM ポリシーの要素: 変数およびタグ」を参照してください。

AWS グローバル条件キーとサービス固有の条件キーをサポートします。 AWS すべてのグローバル条件キーを確認するには、IAM ユーザーガイドの「AWS グローバル条件コンテキストキー」を参照してください。

Wickr の条件キーのリストを確認するには、「サービス認可リファレンス」の「AWS Wickr の条件キー」を参照してください。どのアクションおよびリソースと条件キーを使用できるかについては、AWS Wickr で定義されるアクションを参照してください。

Wickr のアイデンティティベースのポリシーの例を表示するには、「AWS Wickr のアイデンティティベースのポリシーの例」を参照してください。

Wickr の ACL

ACL のサポート	No

アクセスコントロールリスト (ACL) は、どのプリンシパル (アカウントメンバー、ユーザー、またはロール) がリソースにアクセスするための許可を持つかをコントロールします。ACL はリソースベースのポリシーに似ていますが、JSON ポリシードキュメント形式は使用しません。

Wickr での ABAC

ABAC (ポリシー内のタグ) のサポート	いいえ

属性ベースのアクセス制御 (ABAC) は、属性に基づいて権限を定義する認可戦略です。では AWS、これらの属性はタグと呼ばれます。IAM エンティティ (ユーザーまたはロール) AWS や多くのリソースにタグを付けることができます。エンティティとリソースのタグ付けは、ABAC の最初の手順です。次に、プリンシパルのタグがアクセスを試行するリソースのタグと一致したときにオペレーションを許可するよう、ABAC ポリシーを設計します。

ABAC は、急成長する環境やポリシー管理が煩雑になる状況で役立ちます。

タグに基づいてアクセスを管理するには、`aws:ResourceTag/key-name`、`aws:RequestTag/key-name`、または `aws:TagKeys`の条件キーを使用して、ポリシーの条件要素 でタグ情報を提供します。

サービスがすべてのリソースタイプに対して 3 つの条件キーすべてをサポートする場合、そのサービスの値は Yes です。サービスが一部のリソースタイプに対してのみ 3 つの条件キーすべてをサポートする場合、値は Partial です。

ABAC の詳細については、IAM ユーザーガイドの「ABAC とは？」を参照してください。ABAC をセットアップするステップを説明するチュートリアルについては、「IAM ユーザーガイド」の「属性に基づくアクセスコントロール (ABAC) を使用する」を参照してください。

Wickr での一時的な認証情報の使用

一時的な認証情報のサポート	No

AWS のサービス 一時的な認証情報を使用してサインインすると機能しないものもあります。 AWS のサービス 一時的な認証情報で機能するものなど、追加情報については、『IAM ユーザーガイド』の「IAM と連携する」を参照してくださいAWS のサービス 。

ユーザー名とパスワード以外の方法でにサインインすると、 AWS Management Console 一時的な認証情報が使用されることになります。たとえば、会社のシングルサインオン (SSO) AWS リンクを使用してアクセスすると、そのプロセスによって一時的な認証情報が自動的に作成されます。また、ユーザーとしてコンソールにサインインしてからロールを切り替える場合も、一時的な認証情報が自動的に作成されます。ロールの切り替えに関する詳細については、 IAM ユーザーガイド の「ロールへの切り替え (コンソール)」を参照してください。

または API を使用して一時的な認証情報を手動で作成できます。 AWS CLI AWS その後、その一時的な認証情報を使用してアクセスできます AWS。 AWS 長期アクセスキーを使用する代わりに、一時的な認証情報を動的に生成することをおすすめします。詳細については、「IAM の一時的セキュリティ認証情報」を参照してください。

Wickr のクロスサービスプリンシパル許可

転送アクセスセッション (FAS) をサポート	No

IAM ユーザーまたはロールを使用してアクションを実行する場合 AWS、そのユーザーはプリンシパルと見なされます。一部のサービスを使用する際に、アクションを実行することで、別のサービスの別のアクションがトリガーされることがあります。FASは、を呼び出したプリンシパルの権限と AWS のサービス、 AWS のサービス ダウンストリームサービスにリクエストを行うリクエストを組み合わせて使用します。FASリクエストは、 AWS のサービス サービスが他のユーザーとのやりとりやリソースとのやり取りを必要とするリクエストを受信したときにのみ行われます。この場合、両方のアクションを実行するためのアクセス許可が必要です。FAS リクエストを行う際のポリシーの詳細については、「転送アクセスセッション」を参照してください。

Wickr のサービスロール

サービスロールのサポート	いいえ

サービスロールとは、サービスがユーザーに代わってアクションを実行するために引き受ける IAM ロールです。IAM 管理者は、IAM 内からサービスロールを作成、変更、削除できます。詳細については、「IAM ユーザーガイド」の「AWS のサービスにアクセス許可を委任するロールの作成」を参照してください。

> **Warning**
>
> サービスロールの許可を変更すると、Wickr の機能が破損する可能性があります。 Wickr が指示する場合以外は、サービスロールを編集しないでください。

Wickr のサービスリンクロール

サービスにリンクされたロールのサポート	いいえ

サービスにリンクされたロールは、にリンクされているサービスロールの一種です。 AWS のサービスサービスは、ユーザーに代わってアクションを実行するロールを引き受けることができます。AWS アカウント サービスにリンクされたロールはに表示され、そのサービスが所有します。IAM 管理者は、サービスリンクロールの権限を表示できますが、編集することはできません。

サービスリンクロールの作成または管理の詳細については、「IAM と提携するAWS のサービス」を参照してください。表の中から、サービスにリンクされたロール 列に Yesと記載されたサービスを見つけます。サービスにリンクされたロールに関するドキュメントをサービスで表示するには、Yes (はい) リンクを選択します。

AWS Wickr のアイデンティティベースのポリシーの例

デフォルトで、まったく新しい IAM ユーザーには、何かを実行する許可は一切ありません。IAM 管理者は、AWS Wickr サービスを管理するための許可をユーザーに付与する IAM ポリシーを作成して割り当てる必要があります。以下に示しているのは、アクセス許可ポリシーの例です。

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

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

このサンプルポリシーは、for Wickr を使用して Wickr ネットワークを作成、表示、管理する権限をユーザーに付与します。 AWS Management Console IAM ポリシーステートメント内の要素の詳細については、「Wickr のアイデンティティベースのポリシー」を参照してください。これらの JSON ポリシードキュメント例を使用して IAM ポリシーを作成する方法については、IAM ユーザーガイドの「JSON タブでのポリシーの作成」を参照してください。

トピック

- ポリシーのベストプラクティス
- AWS Management Console を Wickr 用に使用する
- 自分の許可の表示をユーザーに許可する

ポリシーのベストプラクティス

アイデンティティベースのポリシーは、誰かがあなたのアカウントでWickrリソースを作成、アクセス、または削除できるかどうかを決定します。これらのアクションを実行すると、 AWS アカウントに料金が発生する可能性があります。アイデンティティベースのポリシーを作成したり編集したりする際には、以下のガイドラインと推奨事項に従ってください。

- AWS 管理ポリシーから始めて、最小権限の権限に移行する — ユーザーとワークロードへの権限の付与を開始するには、AWS 多くの一般的なユースケースで権限を付与する管理ポリシーを使用してください。これらのポリシーは、で利用できます。 AWS アカウント AWS ユースケースに固有のカスタマー管理ポリシーを定義して、権限をさらに減らすことをお勧めします。詳細については、「IAM ユーザーガイド」の「AWS マネージドポリシー」または「AWS ジョブ機能の管理ポリシー」を参照してください。
- 最小特権を適用する – IAM ポリシーで許可を設定するときは、タスクの実行に必要な許可のみを付与します。これを行うには、特定の条件下で特定のリソースに対して実行できるアクションを定義します。これは、 最小特権アクセス許可 とも呼ばれています。IAM を使用して許可を適用する方法の詳細については、「IAM ユーザーガイド」の「IAM でのポリシーとアクセス許可」を参照してください。
- IAM ポリシーで条件を使用してアクセスをさらに制限する – ポリシーに条件を追加して、アクションやリソースへのアクセスを制限できます。例えば、ポリシー条件を記述して、すべてのリ

クエストを SSL を使用して送信するように指定できます。サービスアクションがなどの特定の用途で使用された場合は AWS のサービス、条件を使用してサービスアクションへのアクセスを許可することもできます AWS CloudFormation。詳細については、「IAM ユーザーガイド」の [IAM JSON policy elements: Condition] (IAM JSON ポリシー要素：条件) を参照してください。

- IAM Access Analyzer を使用して IAM ポリシーを検証し、安全で機能的な権限を確保する - IAM Access Analyzer は、新規および既存のポリシーを検証して、ポリシーが IAM ポリシー言語 (JSON) および IAM のベストプラクティスに準拠するようにします。IAM アクセスアナライザーは 100 を超えるポリシーチェックと実用的な推奨事項を提供し、安全で機能的なポリシーの作成をサポートします。詳細については、「IAM ユーザーガイド」の「IAM Access Analyzer ポリシーの検証」を参照してください。
- 多要素認証 (MFA) が必要 — IAM ユーザーまたは root ユーザーを必要とするシナリオがある場合は AWS アカウント、セキュリティを強化するために MFA をオンにしてください。API オペレーションが呼び出されるときに MFA を必須にするには、ポリシーに MFA 条件を追加します。詳細については、「IAM ユーザーガイド」の「MFA 保護 API アクセスの設定」を参照してください。

IAM でのベストプラクティスの詳細については、「IAM ユーザーガイド」の「IAM でのセキュリティのベストプラクティス」を参照してください。

AWS Management Console を Wickr 用に使用する

`AWSWickrFullAccess` AWS 管理ポリシーを IAM ID にアタッチして、Wickr サービス (の Wickr 管理者コンソールを含む) への完全な管理権限を付与します。 AWS Management Console詳細については、「AWS 管理ポリシー: AWSWickrFullAccess」を参照してください。

自分の許可の表示をユーザーに許可する

この例では、ユーザーアイデンティティに添付されたインラインおよびマネージドポリシーの表示を IAM ユーザーに許可するポリシーを作成する方法を示します。このポリシーには、コンソールで、またはまたは API を使用してこのアクションをプログラムで実行するための権限が含まれています。 AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
```

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

AWS Wickr の ID とアクセスのトラブルシューティング

次の情報は、Wickr と IAM の使用に伴って発生する可能性がある一般的な問題の診断や修復に役立ちます。

トピック

- for Wickr で管理アクションを実行する権限がありません。 AWS Management Console

for Wickr で管理アクションを実行する権限がありません。 AWS Management Console

AWS Management Console for Wickr で、操作を実行する権限がないと表示された場合は、管理者に連絡して支援を求める必要があります。管理者とは、サインイン認証情報を提供した担当者です。

次のエラー例は、mateojackson IAM ユーザーが for Wickr を使用して AWS Management Console for Wickr で Wickr ネットワークを作成、管理、または表示しようとしても、 AWS Management Console およびの権限がない場合に発生します。wickr:CreateAdminSession wickr:ListNetworks

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

この場合、Mateo は管理者に、およびアクションを使用して for Wickr にアクセスできるようにポリシーを更新するように依頼します。 AWS Management Console wickr:CreateAdminSession wickr:ListNetworks詳細については、AWS Wickr のアイデンティティベースのポリシーの例およびAWS 管理ポリシー: AWSWickrFullAccessを参照してください。

コンプライアンス検証

AWS 特定のコンプライアンスプログラムの対象となるサービスの一覧については、「https://aws.amazon.com/compliance/services-in-scope/」を参照してくださいAWS 。一般的な情報については、「AWS」を参照してください。

サードパーティの監査レポートはを使用してダウンロードできます AWS Artifact。詳細については、の「レポートのダウンロード」の「 AWS Artifact」を参照してください AWS Artifact。

Wickr を使用する際のコンプライアンス責任は、データの機密性、貴社のコンプライアンス目標、適用される法律と規制によって決まります。 AWS は、コンプライアンスに役立つ次のリソースを提供します。

- セキュリティとコンプライアンスのクイックスタートガイドセキュリティとコンプライアンスのクイックスタートガイド 、アーキテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスに重点を置いたベースライン環境をに展開する手順について説明します。 AWS
- AWS — この一連のワークブックとガイドは、お客様の業界や地域に適用できる場合があります。
- AWS Config 開発者ガイドのルールによるリソースの評価 — AWS Config; リソース構成が社内慣行、業界ガイドライン、規制にどの程度準拠しているかを評価します。
- AWS Security Hub— AWS このサービスでは、セキュリティの状態を包括的に把握できるため、AWS セキュリティ業界の標準やベストプラクティスに準拠しているかどうかを確認できます。

AWS Wickr の耐障害性

AWS グローバルインフラストラクチャは、アベイラビリティーゾーンを中心に構築されています。AWS リージョン AWS リージョン 物理的に分離された複数のアベイラビリティーゾーンを提供し、低レイテンシー、高スループット、冗長性の高いネットワークで接続します。アベイラビリティーゾーンでは、ゾーン間で中断することなく自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性が高く、フォールトトレラントで、スケーラブルです。

AWS リージョン およびアベイラビリティーゾーンの詳細については、「グローバルインフラストラクチャ」を参照してください。AWS

Wickr には、 AWS グローバルインフラストラクチャに加えて、データの回復力とバックアップのニーズをサポートするいくつかの機能が備わっています。詳細については、「データ保持」を参照してください。

AWS Wickr のインフラストラクチャセキュリティ

マネージドサービスである AWS Wickr は、「Amazon Web Services: セキュリティプロセスの概要」 AWS ホワイトペーパーに記載されているグローバルネットワークセキュリティ手順によって保護されています。

AWS Wickr での設定と脆弱性の分析

設定と IT 管理は、 AWS お客様とお客様との間で共有される責任です。詳細については、「 AWS 責任分担モデル」を参照してください。

仕様とガイドラインに従って Wickr を設定し、定期的に最新バージョンの Wickr クライアントをダウンロードするようにユーザーに指示し、最新バージョンの Wickr データ保持ボットを実行していることを確認し、ユーザーによる Wickr の使用状況を監視するのはお客様の責任です。

AWS Wickr のセキュリティのベストプラクティス

Wickr には、独自のセキュリティポリシーを開発および実装する際に考慮する必要のあるいくつかのセキュリティ機能が用意されています。以下のベストプラクティスは一般的なガイドラインであり、完全なセキュリティソリューションを説明するものではありません。これらのベストプラクティスは

お客様の環境に必ずしも適切または十分でない可能性があるので、処方箋ではなく、あくまで有用な考慮事項とお考えください。

Wickr の使用に関連する潜在的なセキュリティイベントを防ぐには、以下のベストプラクティスに従ってください。

- 最小限の権限アクセスを実装し、Wickr アクションに使用する特定のロールを作成してください。IAM テンプレートを使用してロールを作成します。詳細については、「AWS AWS Wickr のマネージドポリシー」を参照してください。
- AWS Management Console for Wickr にアクセスするには、最初に認証を行います。 AWS Management Console 個人コンソールの認証情報は共有しないでください。インターネット上の誰でもコンソールにアクセスできますが、コンソールへの有効な認証情報がない限り、サインインしたりセッションを開始したりすることはできません。

AWS Wickr のモニタリング

モニタリングは、AWS Wickr AWS やその他のソリューションの信頼性、可用性、パフォーマンスを維持する上で重要な部分です。 AWS には、Wickr を監視し、問題が発生した場合に報告し、必要に応じて自動アクションを実行するための以下のモニタリングツールが用意されています。

- AWS CloudTrailアカウントによって、 AWS またはアカウントに代わって行われた API 呼び出しと関連イベントをキャプチャし、指定した Amazon S3 バケットにログファイルを配信します。どのユーザーとアカウント AWS、呼び出しが行われたソース IP アドレス、呼び出しがいつ発生したかを特定できます。詳細については、『AWS CloudTrail ユーザーガイド』を参照してください。を使用して Wickr API 呼び出しを記録する方法の詳細については CloudTrail、を参照してください。AWS CloudTrail を使用して AWS Wickr API 通話のログ記録

AWS CloudTrail を使用して AWS Wickr API 通話のログ記録

AWS Wickr はAWS CloudTrail、Wickr のユーザー、ロール、または のサービスによって実行されたアクションを記録するAWSサービスである と統合されています。 は、Wickr のすべての API コールをイベントとして CloudTrail キャプチャします。キャプチャされた呼び出すには AWS Management Console for WickrからのコールとWickr APIオペレーションへのコー呼び出すが含まれます。証跡を作成する場合は、Wickr の CloudTrail イベントなど、Amazon S3 バケットへのイベントの継続的な配信を有効にすることができます。証跡を設定しない場合でも、イベント履歴 で CloudTrail コンソールで最新のイベントを表示できます。 で収集された情報を使用して CloudTrail、Wickr に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。の詳細については CloudTrail、「 AWS CloudTrailユーザーガイド」を参照してください。

の Wickr 情報 CloudTrail

CloudTrail アカウントを作成するAWS アカウントと、 は で有効になります。Wickr でアクティビティが発生すると、そのアクティビティは CloudTrail イベント履歴 の他のAWSサービスイベントとともにイベントに記録されます。最近のイベントは、AWS アカウント で表示、検索、ダウンロードできます。詳細については、「イベント履歴 を使用した CloudTrail イベントの表示」を参照してください。

Wickrのイベントも含め、AWS アカウント のイベントを継続的に記録するには、証跡を作成します。証跡により、 はログファイル CloudTrail を Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョン に適用されます。証跡は、AWS パーティションのすべてのリージョンからのイベントをログに記録し、指定した

Amazon S3 バケットにログファイルを配信します。さらに、 CloudTrail ログで収集されたデータをより詳細に分析し、それに基づく対応を行うように他の AWSサービスを設定できます。詳細については、次を参照してください:

- 「証跡作成の概要」
- CloudTrail サポートされているサービスと統合
- の Amazon SNS 通知の設定 CloudTrail
- 複数のリージョンからの CloudTrail ログファイルの受信と複数のアカウントからの CloudTrail ログファイルの受信

すべての Wickr アクションは によってログに記録されます CloudTrail。例えば、、、および ListNetworksアクションを呼び出すとCreateAdminSession、 CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するために役立ちます。

- リクエストが、ルート認証情報と AWS Identity and Access Management (IAM) ユーザー認証情報のどちらを使用して送信されたか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが、別の AWS サービスによって送信されたかどうか。

詳細については、「CloudTrail userIdentity 要素」を参照してください。

Wickrのログファイルエントリーを理解します。

証跡は、指定した Amazon S3 バケットにイベントをログファイルとして配信できるようにする設定です。 CloudTrail ログファイルには、1 つ以上のログエントリが含まれます。イベントは任意の送信元からの単一のリクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどに関する情報が含まれます。 CloudTrail ログファイルは、パブリック API コールの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、 CreateAdminSessionアクションを示す CloudTrail ログエントリを示しています。

```
{
    "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"
}
```

次の例は、 CreateNetworkアクションを示す CloudTrail ログエントリを示しています。


```
{
    "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"
```

```
}
```

次の例は、 ListNetworksアクションを示す CloudTrail ログエントリを示しています。

```
{
    "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"
```

```
}
```

次の例は、 UpdateNetworkdetailsアクションを示す CloudTrail ログエントリを示しています。

```
{
    "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"
}
```

次の例は、 TagResourceアクションを示す CloudTrail ログエントリを示しています。

```
{
    "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"
}
```

次の例は、 ListTagsForResourceアクションを示す CloudTrail ログエントリを示しています。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<access-key-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T18:50:37Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-08T18:50:37Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "ListTagsForResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "axios/0.27.2",
    "errorCode": "AccessDenied",
    "requestParameters": {
```

```
        "resource-arn": "<arn>"
    },
    "responseElements": {
        "message": "User: <arn> is not authorized to perform: wickr:ListTagsForResource
 on resource: <arn> with an explicit deny"
    },
    "requestID": "c7488490-a987-4ca2-a686-b29d06db89ed",
    "eventID": "5699d5de-3c69-4fe8-b353-8ae62f249187",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

分析ダッシュボード

分析ダッシュボードを使用して、組織が AWS Wickr をどのように利用しているかを確認できます。以下の手順では、AWS Wickr コンソールを使用して分析ダッシュボードにアクセスする方法について説明します。

分析ダッシュボードにアクセスするには

1. https://console.aws.amazon.com/wickr/ で AWS Management Console for Wickr を開いてください。
2. ナビゲーションペインで、[Analytics] を選択します。

   Analytics ページには、ネットワークのメトリックがさまざまなタブに表示されます。

Analytics ページでは、各タブの右上隅に時間枠フィルターがあります。このフィルターはページ全体に適用されます。さらに、各タブの右上隅にある [エクスポート] オプションを選択すると、選択した時間範囲のデータポイントをエクスポートできます。

> **Note**
>
> 選択した時間は UTC (世界標準時) です。

以下のタブを使用できます。

- 概要が表示されます。
  - 登録済み — 選択した期間におけるネットワーク上のアクティブユーザーと利用停止ユーザーを含む登録ユーザーの総数。保留中のユーザーや招待されたユーザーは含まれません。
  - 保留中 — 選択した時間におけるネットワーク上の保留中のユーザーの総数。
  - ユーザー登録 — グラフには、選択した時間範囲に登録されたユーザーの総数が表示されます。
  - デバイス — アプリがアクティブだったデバイスの数です。
  - クライアントバージョン — クライアントバージョン別に分類されたアクティブなデバイスの数。

- メンバーには以下が表示されます。
  - ステータス — 選択した期間内のネットワーク上のアクティブユーザー。
  - アクティブユーザー —
    - グラフにはアクティブユーザー数の推移が表示され、日単位、週単位、または月単位 (上記で選択した期間内) に集計できます。
    - アクティブユーザー数は、プラットフォーム、クライアントバージョン、またはセキュリティグループごとに分類できます。セキュリティグループが削除された場合、その合計数は Deleted# と表示されます。

- メッセージには以下が表示されます。
  - 送信されたメッセージ — 選択した期間にネットワーク上のすべてのユーザーとボットが送信したユニークメッセージの数。
  - 通話 — ネットワーク内のすべてのユーザーがかけたユニーク通話の件数。
  - ファイル — ネットワーク内のユーザーが送信したファイルの数 (ボイスメモを含む)。
  - デバイス — 円グラフには、オペレーティングシステム別に分類されたアクティブなデバイスの数が表示されます。
  - クライアントバージョン — クライアントバージョン別に分類されたアクティブデバイスの数。

ドキュメント履歴

以下の表は、Wickrのドキュメントのリリースについて説明したものです。

変更	説明	日付
グローバルフェデレーションは制限付きフェデレーションをサポートするようになり、管理者は管理コンソールで使用状況分析を確認できるようになりました。	グローバルフェデレーションが制限付きフェデレーションをサポートするようになりました。これは他のWickrネットワークでも機能します。AWS リージョン詳しくはセキュリティグループを参照してください。さらに、管理者は管理コンソールの Analytics ダッシュボードで使用状況分析を確認できるようになりました。詳しくは、「Analytics ダッシュボード」を参照してください。	2024 年 3 月 28 日
AWS Wickr のプレミアムプランの 3 か月間の無料トライアルが利用可能になりました	Wickr 管理者は、最大 30 ユーザーまで利用できる 3 か月間の無料トライアル Premium プランを選択できるようになりました。無料トライアル中は、無制限の管理者コントロールやデータ保持など、スタンダードプランとプレミアムプランのすべての機能を利用できます。Premium 無料トライアル中は、ゲストユーザー機能は使用できません。詳しくは、「プランの管理」を参照してください。	2024 年 2 月 9 日

ゲストユーザー機能は一般公開されており、より多くの管理者コントロールが追加されています。	Wickr 管理者は、ゲストユーザーのリスト、ユーザーの一括削除または利用停止、ゲストユーザーの Wickr ネットワーク内での通信をブロックするオプションなど、さまざまな新機能にアクセスできるようになりました。詳細については、ゲストユーザー を参照してください。	2023 年 11 月 8 日
Wickrはヨーロッパ (フランクフルト) でもご利用いただけるようになりました AWS リージョン	Wickrはヨーロッパ (フランクフルト) でもご利用いただけるようになりました。 AWS リージョン詳しくはWickrへのアクセスをご覧ください。	2023 年 10 月 26 日
Wickr ネットワークは、複数のネットワークを統合できるようになりました。 AWS リージョン	Wickr ネットワークが AWS リージョン間でフェデレートできる機能が追加されました。詳しくはセキュリティグループを参照してください。	2023 年 9 月 29 日
Wickr がヨーロッパ (ロンドン) で利用可能になりました AWS リージョン	Wickrはヨーロッパ (ロンドン) でもご利用いただけるようになりました。 AWS リージョン詳しくはWickrへのアクセスをご覧ください。	2022 年 8 月 23 日
Wickr がカナダ (中部) で利用できるようになりました。 AWS リージョン	Wickr がカナダ (中部) で利用できるようになりました。 AWS リージョン詳しくはWickrへのアクセスをご覧ください。	2023 年 7 月 3 日

ゲストユーザー機能をプレビューできるようになりました	ゲストユーザーは、Wickr クライアントにサインインして、Wickr ネットワークユーザーと共同作業できます。詳細については、「ゲストユーザー (プレビュー)」を参照してください。	2023 年 5 月 31 日
AWS Wickr は、現在 AWS GovCloud (米国西部) と統合され AWS CloudTrail、以下で利用できるようになりました。WickrGov	AWS Wickr がと統合されるようになりました。 AWS CloudTrail詳細については、「AWS CloudTrailを使用した AWS Wickr API 呼び出しのログ記録」を参照してください。さらに、Wickr は AWS GovCloud (米国西部) でもご利用いただけるようになりました。 WickrGov詳細については、『ユーザーガイド』AWS WickrGovAWS GovCloud (US) のを参照してください。	2023 年 3 月 30 日
タグ付けと複数のネットワーク作成	タグ付けが AWS Wickr でサポートされるようになりました。詳しくはネットワークタグの管理を参照してください。Wickr で複数のネットワークを作成できるようになりました。詳しくはネットワークの作成を参照してください。	2023 年 3 月 7 日
初回リリース	Wickrアドミニストレーションガイドの初期リリース	2022 年 11 月 28 日

リリースノート

Wickr の継続的な更新と改善を追跡できるように、最近の変更を説明するリリース通知を公開しています。

2024 年 3 月

- グローバルフェデレーションは、制限付きフェデレーションをサポートするようになりました。グローバルフェデレーションは、制限付きフェデレーションの下に追加された特定のネットワークに対してのみ有効にできます。これは他のWickrネットワークでも機能します。 AWS リージョン詳しくはセキュリティグループを参照してください。
- 管理者は管理コンソールの Analytics ダッシュボードで使用状況分析を確認できるようになりました。詳しくは、「Analytics ダッシュボード」を参照してください。

2024 年 2 月

- AWS Wickr は現在、最大 30 ユーザーを対象に Premium プランの 3 か月間の無料トライアルを提供しています。変更点と制限には以下が含まれます。
  - 無制限の管理者コントロールやデータ保持など、スタンダードプランとプレミアムプランのすべての機能が、プレミアム無料トライアルで利用できるようになりました。Premium 無料トライアル中は、ゲストユーザー機能は使用できません。
  - 以前の無料トライアルはご利用いただけなくなります。プレミアム無料トライアルをまだ使用していない場合は、既存の無料トライアルまたはスタンダードプランをプレミアム無料トライアルにアップグレードできます。詳細については、「プランの管理」を参照してください。

2023 年 11 月

- ゲスト ユーザー機能が一般提供されるようになりました。変更と追加には以下が含まれます。
  - 他の Wickr ユーザーによる悪用を報告する機能。
  - 管理者は、ネットワークがやり取りしたゲストユーザーのリストと月間使用回数を表示できます。
  - 管理者はゲストユーザーによるネットワークとの通信をブロックできます。
  - ゲストユーザー向けの価格が追加されました。

- 管理制御の機能強化
  - ユーザーを一括削除/利用停止できます。
  - トークン更新の猶予期間を設定するための SSO 設定の追加。

2023 年 10 月

- 機能強化
  - Wickr は、欧州 (フランクフルト) AWS リージョンで利用可能になりました。

2023 年 9 月

- 機能強化
  - Wickr ネットワークが AWS リージョン間でフェデレートできる機能が追加されました。詳しくはセキュリティグループを参照してください。

2023 年 8 月

- 機能強化
  - Wickr が欧州 (ロンドン) AWS リージョンで利用可能になりました。

2023 年 7 月

- 機能強化
  - Wickr は、カナダ (中部) AWS リージョンで使用可能になりました。

2023 年 5 月

- 機能強化
  - ゲストユーザー向けのサポートが追加されました。詳細については、「ゲストユーザー」を参照してください。

2023 年 3 月

- Wickr がと統合されました。 AWS CloudTrail詳細については、「AWS CloudTrail を使用して AWS Wickr API 通話の口グ記録」を参照してください。
- Wickr は AWS GovCloud (米国西部) でご利用いただけるようになりました。 WickrGov詳細については、『ユーザーガイド』AWS WickrGovAWS GovCloud (US) のを参照してください。
- Wickr がタグ付けをサポートしました。詳細については、「ネットワークタグの管理」を参照してください。Wickr で複数のネットワークを作成できるようになりました。詳細については、「ステップ1：ネットワークの構築」を参照してください。

2023 年 2 月

- Wickr は Android Tactical Assault Kit (ATAK) をサポートできるようになりました。詳細については、「Wickr ネットワークダッシュボードで ATAK を有効にする」を参照してください。

2023 年 1 月

- シングルサインオン (SSO) は、無料トライアルとスタンダードを含むすべてのプランで設定できるようになりました。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。