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、エンドツーエンドの暗号化サービスです。これにより組織や政府機関は、1 対 1 およびグループでのメッセージング、音声およびビデオ通話、ファイル共有、画面共有、その他を通じての通信を安全に行えるようになります。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。を使用して Wickr ネットワークをすばやく作成および管理し AWS マネジメントコンソール、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 ビット高度暗号化標準 (AES) のエンドツーエンド暗号化を使用しています。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、呼び出し、ファイルは新しいランダムキーで暗号化され、意図した受信者以外 (偶数ではない AWS) は復号できません。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) にアクセスでき、非接続通信や帯域外通信などの低帯域幅環境でも機能することができます。

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。お客様は、 を介して Wickr ネットワークをすばやく作成および管理し AWS マネジメントコンソール、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Burn-on-Read (BOR) タイマーの制御
- 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

リージョナルな可用性

Wickr は、米国東部 (バージニア北部)、アジアパシフィック (マレーシア)、アジアパシフィック (シンガポール)、アジアパシフィック (シドニー)、アジアパシフィック (東京)、カナダ (中部)、欧州 (フランクフルト)、欧州 (ロンドン)、欧州 (ストックホルム)、欧州 (チューリッヒ) で利用できます AWS リージョン。Wickr は AWS GovCloud (米国西部) リージョンでも利用できます。各リージョンには複数のアベイラビリティーゾーンがあり、物理的に分離されていますが、プラ

イベート、低レイテンシー、高帯域幅、冗長ネットワーク接続で接続されています。これらのアベイラビリティーゾーンは、可用性の向上、耐障害性、レイテンシーの最小化に使用されます。

詳細については AWS リージョン、「」のAWS リージョン 「アカウントで使用できる を指定する」を参照してくださいAWS 全般のリファレンス。各リージョンで使用できるアベイラビリティーゾーンの数の詳細については、AWS 「 グローバルインフラストラクチャ」を参照してください。

Wickr へのアクセス

管理者は、https://console.aws.amazon.com/wickr/ で Wickr AWS マネジメントコンソール の 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。

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

新規の AWS お客様は、AWS Wickr の使用を開始する前に、このページに記載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。これらのセットアップ手順では、 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

にサインアップする AWS

がない場合は AWS アカウント、次の手順を実行して作成します。

にサインアップするには AWS アカウント

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、電話またはテキストメッセージを受け取り、電話キーパッドで検証コードを入力します。

   にサインアップすると AWS アカウント、 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。セキュリティベストプラクティスとして、ユーザーに管理アクセス権を割り当て、ルートユーザーアクセスが必要なタスクの実行にはルートユーザーのみを使用するようにしてください。

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 アイデンティティセンター内 (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 アイデンティティセンターユーザーガイドの「開始方法」の手順に従います。	AWS Command Line Interface ユーザーガイドの を使用する AWS CLI ように を設定 AWS IAM アイデンティティセンターして、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 マネージドポリシー: 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、開始方法 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 マネージドポリシー: 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、「Wickr ネットワークのリストを許可するポートとドメイン」を参照してください。

ステップ1: ネットワークの構築

Wickr ネットワークを作成できます。

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. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。

> **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 — 管理統制と柔軟性を必要とする中小企業チーム向け。
   - 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、最大 30 人のユーザーが利用でき、3 か月間有効なプレミアム無料トライアルを選択できます。For AWS WickrGov のプレミアム無料トライアルオプションでは、最大 50 人のユーザーを許可し、3 か月間使用できます。プレミアム無料トライアル期間中、管理者は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。詳細については、「ネットワークタグ」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 マネジメントコンソール 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: ネットワークの構成

Wickr AWS マネジメントコンソール の にアクセスするには、次の手順を実行します。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、ネットワーク名を選択してそのネットワークに移動します。

   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. 次のユーザー管理オプションを使用できます。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、「AWS Wickr のセキュリティグループ」を参照してください。
- シングルサインオン (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、「AWS Wickr の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、「AWS Wickr のシングルサインオン設定」を参照してください。
- 招待 - Wickr AWS マネジメントコンソール 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。詳細については、AWS Wickr ネットワークの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。

Wickr ユーザーを作成し、 SSO を使用して招待を送信するには:

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、「AWS Wickr で SSO を設定する」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。 AWS WickrGov の詳細については、AWS GovCloud (US) 「 ユーザーガイド」のAWS WickrGov」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。

Wickr ユーザーを手動で作成して招待状を送信するには

1. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。

   Wickr ネットワークにリダイレクトされます。Wickr ネットワークでは、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、追加設定の調整を行うことができます。
3. ナビゲーションペインで、ユーザー管理を選択します。
4. ユーザー管理ページのチームディレクトリタブで、ユーザーを招待を選択します。

   招待ユーザーの横にあるドロップダウン矢印を選択して、ユーザーを一括招待することもできます。ユーザーを一括招待ページで、テンプレートのダウンロードを選択して、ユーザーのリストで編集およびアップロードできる CSV テンプレートをダウンロードします。
5. 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。

6. [招待] 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。

次の手順

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、以下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

AWS Wickr ネットワークの管理

Wickr AWS マネジメントコンソール の では、Wickr ネットワーク名、セキュリティグループ、SSO 設定、データ保持設定を管理できます。

トピック

AWS Wickr のネットワークの詳細

Wickr ネットワークの名前を編集し、Wickr AWS マネジメントコンソール の のネットワークの詳細セクションでネットワーク ID を表示できます。

トピック

AWS Wickr でネットワークの詳細を表示する

ネットワーク名やネットワーク ID など、Wickr ネットワークの詳細を表示できます。

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. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、表示するネットワークを見つけます。
3. 表示するネットワークの右側で、縦の省略記号アイコン (3 つのドット) を選択し、詳細の表示を選択します。

   Network ホームページには、Wickr ネットワーク名とネットワーク ID が Network details セクションに表示されます。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。

AWS Wickr でネットワーク名を編集する

Wickr ネットワークの名前を編集できます。

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. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択して、そのネットワークの Wickr 管理コンソールに移動します。
3. Network ホームページの Network details セクションで、Edit を選択します。
4. [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。
5. 保存 を選択して、新しいネットワーク名を保存します。

AWS Wickr でネットワークを削除する

AWS Wickr ネットワークを削除できます。

> **Note**
>
> プレミアム無料トライアルネットワークを削除した場合、別の無料トライアルネットワークを作成することはできません。

ネットワークホームページで Wickr ネットワークを削除するには、次の手順を実行します。

1. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、削除するネットワークを見つけます。
3. 削除するネットワークの右側で、縦の省略記号アイコン (3 つのドット) を選択し、ネットワークの削除を選択します。

4. ポップアップウィンドウで「確認」と入力し、「削除」を選択します。

   ネットワークが削除されるまでに数分かかる場合があります。

ネットワークにいる間に Wickr ネットワークを削除するには、次の手順を実行します。

1. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、削除するネットワークを選択します。
3. Network ホームページの右上隅近くで、Delete network を選択します。
4. ポップアップウィンドウで「確認」と入力し、「削除」を選択します。

   ネットワークが削除されるまでに数分かかる場合があります。

> **Note**
>
> データ保持設定 (有効になっている場合) によって保持されているデータは、ネットワークを削除しても削除されません。詳細については、「AWS Wickr のデータ保持」を参照してください。

AWS Wickr のセキュリティグループ

AWS マネジメントコンソール for Wickr のセキュリティグループセクションでは、パスワードの複雑さに関するポリシー、メッセージング設定、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、セキュリティグループとその設定を管理できます。

トピック

- AWS Wickr でセキュリティグループを表示する
- AWS Wickr でセキュリティグループを作成する
- AWS Wickr でセキュリティグループを編集する
- AWS Wickr でセキュリティグループを削除する

AWS Wickr でセキュリティグループを表示する

Wickr セキュリティグループの詳細を表示できます。

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. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、[Security Groups] (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、新しいグループを作成するオプションが表示されます。

   セキュリティグループページで、表示するセキュリティグループを選択します。このページには、そのセキュリティグループの現在の詳細が表示されます。

AWS Wickr でセキュリティグループを作成する

新しい Wickr セキュリティグループを作成できます。

以下の手順でセキュリティグループを作成します。

1. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、[Security Groups] (セキュリティグループ) を選択します。
4. セキュリティグループページで、セキュリティグループの作成を選択して新しいセキュリティグループを作成します。

   > **Note**
   >
   > 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。

5. セキュリティグループの作成ページで、セキュリティグループの名前を入力します。
6. [セキュリティグループの作成] を選択してください。

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

AWS Wickr でセキュリティグループを編集する

Wickr セキュリティグループの詳細を編集できます。

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. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、[Security Groups] (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の名前を選択します。

   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の詳細 — セキュリティグループの詳細セクションで編集を選択して名前を編集します。
   - 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。
     - Burn-on-read — Wickr クライアントのburn-on-readタイマーにユーザーが設定できる最大値を制御します。詳細については、「Wickr クライアントでメッセージの有効期限とバーンタイマーを設定する」を参照してください。
     - 有効期限タイマー — Wickr クライアントでユーザーがメッセージの有効期限タイマーに設定できる最大値を制御します。詳細については、「Wickr クライアントでメッセージの有効期限とバーンタイマーを設定する」を参照してください。
     - メッセージ転送 — ユーザーが Wickr クライアントでメッセージを転送できるかどうかを制御します。詳細については、「Wickr クライアントのメッセージの転送」を参照してください。
     - クイックレスポンス — ユーザーがメッセージに応答するためのクイックレスポンスのリストを設定します。
     - セキュアシュレッダーの強度 — ユーザーに対してセキュアシュレッダーコントロールを実行する頻度を設定します。詳細については、「メッセージング」を参照してください。
   - 通話: グループメンバーの通話機能を管理します。
     - 音声通話を有効にする — ユーザーは音声通話を開始できます。
     - ビデオ通話と画面共有を有効にする — ユーザーは通話中にビデオ通話を開始したり、画面を共有したりできます。
     - TCP 呼び出し — TCP 呼び出しの有効化 (または強制) は、通常、組織の IT 部門またはセキュリティ部門によって標準の VoIP UDP ポートが許可されていない場合に使用されます。TCP 呼び出しが無効になっており、UDP ポートを使用できない場合、Wickr クライアントは最初に UDP を試し、TCP にフォールバックします。

- メディアとリンク — グループのメンバーのメディアとリンクに関連する設定を管理します。

  ファイルのダウンロードサイズ — 最高品質の転送を選択して、ユーザーが元の暗号化形式でファイルと添付ファイルを転送できるようにします。低帯域幅転送を選択すると、Wickr のユーザーが送信したファイル添付ファイルは Wickr ファイル転送サービスによって圧縮されます。

- Location — グループのメンバーのロケーション共有設定を管理します。

  ロケーション共有 — ユーザーは GPS 対応デバイスを使用してロケーションを共有できます。この機能は、デバイスのオペレーティングシステムのデフォルトに基づいてビジュアルマップを表示します。ユーザーはマップビューを無効にし、代わりに GPS 座標を含むリンクを共有できます。

- 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。
  - アカウント乗っ取り保護を有効にする — ユーザーがアカウントに新しいデバイスを追加するときに、2 要素認証を適用します。新しいデバイスを検証するには、古いデバイスから Wickr コードを生成するか、E メール検証を実行できます。これは、AWS Wickr アカウントへの不正アクセスを防ぐためのセキュリティの追加レイヤーです。
  - 常に再認証を有効にする — アプリケーションに再入力するときに、ユーザーに常に再認証を強制します。
  - マスターリカバリキー — アカウントの作成時にマスターリカバリキーを作成します。他のデバイスが使用できない場合、ユーザーは自分のアカウントへの新しいデバイスの追加を承認できます。
- 通知と可視性 — グループのメンバーへの通知でメッセージプレビューなどの通知と可視性の設定を行います。
- Wickr オープンアクセス — グループのメンバーの Wickr オープンアクセス設定を構成します。
  - Wickr オープンアクセスを有効にする — Wickr オープンアクセスを有効にすると、トラフィックが偽装され、制限および監視対象のネットワーク上のデータが保護されます。地理的位置に基づいて、Wickr オープンアクセスは、トラフィックの難読化に最適なパスとプロトコルを提供するさまざまなグローバルプロキシサーバーに接続します。
  - Force Wickr open access — すべてのデバイスで Wickr open access を自動的に有効化して適用します。
- フェデレーション — ユーザーが他の Wickr ネットワークと通信できるかどうかを制御します。

- 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ションする機能。たとえば、ローカルフェデレーションが有効になっているカナダ (中部) リージョンに AWS 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 — Wickr Enterprise ユーザーまたは他のリージョンに属する別のネットワークの AWS ユーザーとフェデレーションする機能。たとえば、カナダ (中部) リージョンの AWS Wickr ネットワーク上のユーザーと欧州 (ロンドン) リージョンのネットワーク上の AWS ユーザーは、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ときに相互に通信できます。
- 制限付きフェデレーション — ユーザーがフェデレーションできる特定の AWS Wickr または Wickr Enterprise ネットワークのリストを許可します。設定すると、ユーザーは許可リストに登録されたネットワーク内の外部ユーザーとのみ通信できます。どちらのネットワークでも、制限付きフェデレーションを使用するには、相互にリストを許可する必要があります。

  ゲストフェデレーションの詳細については、「AWS Wickr ネットワークでゲストユーザーを有効または無効にする」を参照してください。

- ATAK プラグイン設定 — ATAK の有効化の詳細については、「ATAK とは」を参照してください。

6. 保存 を選択して、セキュリティグループの詳細に加えた編集を保存します。

AWS Wickr でセキュリティグループを削除する

Wickr セキュリティグループを削除できます。

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. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、[Security Groups] (セキュリティグループ) を選択します。
4. セキュリティグループページで、削除するセキュリティグループを見つけます。
5. 削除するセキュリティグループの右側で、縦の省略記号アイコン (3 つのドット) を選択し、削除を選択します。
6. ポップアップウィンドウで「確認」と入力し、「削除」を選択します。

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、「AWS Wickr ネットワークでユーザーを編集する」を参照してください。

AWS Wickr のシングルサインオン設定

Wickr AWS マネジメントコンソール の では、シングルサインオンシステムを使用して認証するように 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

- AWS Wickr で SSO の詳細を表示する
- AWS Wickr で SSO を設定する
- トークン更新の猶予期間

AWS Wickr で SSO の詳細を表示する

Wickr ネットワークとネットワークエンドポイントのシングルサインオン設定の詳細を表示できます。

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。

1. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、ユーザー管理を選択します。

   ユーザー管理ページで、シングルサインオンセクションに 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。

AWS Wickr で SSO を設定する

Wickr ネットワークへの安全なアクセスを確保するために、現在のシングルサインオン設定をセットアップできます。このプロセスに役立つ詳細なガイドが用意されています。

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。この会社 ID を必ず記録してください。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。
- 2025 年 9 月、AWS Wickr は改善されたより安全な SSO 接続システムを導入しました。これらのセキュリティ強化を活用するには、SSO を使用している組織は 2026 年 3 月 9 日までに新しいリダイレクト URI に移行する必要があります。移行手順については、次の AWS re:Post 記事「AWS Wickr の新しい SSO リダイレクト URI への移行」を参照してください。

SSO の設定の詳細については、以下のガイドを参照してください。

- Microsoft Entra (Azure AD) を使用した AWS Wickr シングルサインオン (SSO) のセットアップ
- Okta を使用した AWS Wickr シングルサインオン (SSO) のセットアップ
- Amazon Cognito を使用した AWS Wickr シングルサインオン (SSO) のセットアップ

Microsoft Entra (Azure AD) シングルサインオンで AWS Wickr を設定する

AWS Wickr は、Microsoft Entra (Azure AD) を ID プロバイダーとして使用するように設定できます。そのためには、Microsoft Entra と AWS Wickr 管理コンソールの両方で次の手順を実行します。

Warning

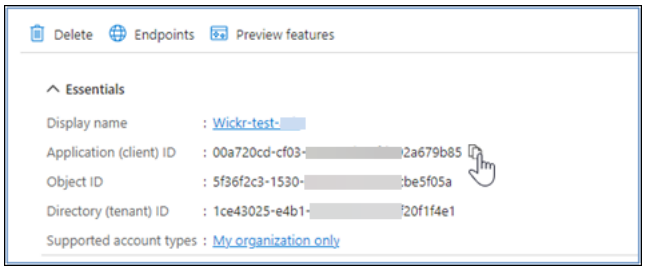
ネットワークで SSO を有効にすると、Wickr からアクティブなユーザーに署名し、SSO プロバイダーを使用して再認証するように強制します。

ステップ 1: Microsoft Entra で AWS Wickr をアプリケーションとして登録する

Microsoft Entra でアプリケーションとして AWS Wickr を登録するには、次の手順を実行します。

> **Note**
>
> 詳細なスクリーンショットとトラブルシューティングについては、Microsoft Entra のドキュメントを参照してください。詳細については、「Microsoft ID プラットフォームでアプリケーションを登録する」を参照してください。

1. ナビゲーションペインで、アプリケーションを選択し、アプリケーション登録を選択します。
2. アプリ登録ページで、アプリケーションの登録を選択し、アプリケーション名を入力します。
3. この組織ディレクトリのアカウントのみを選択します (デフォルトディレクトリのみ - シングルテナント)。
4. Redirect URI で Web を選択し、 AWS Wickr Admin コンソールの SSO 設定で使用できるリダイレクト URI を入力します。
5. [登録] を選択します。
6. 登録後、生成されたアプリケーション (クライアント) ID をコピー/保存します。



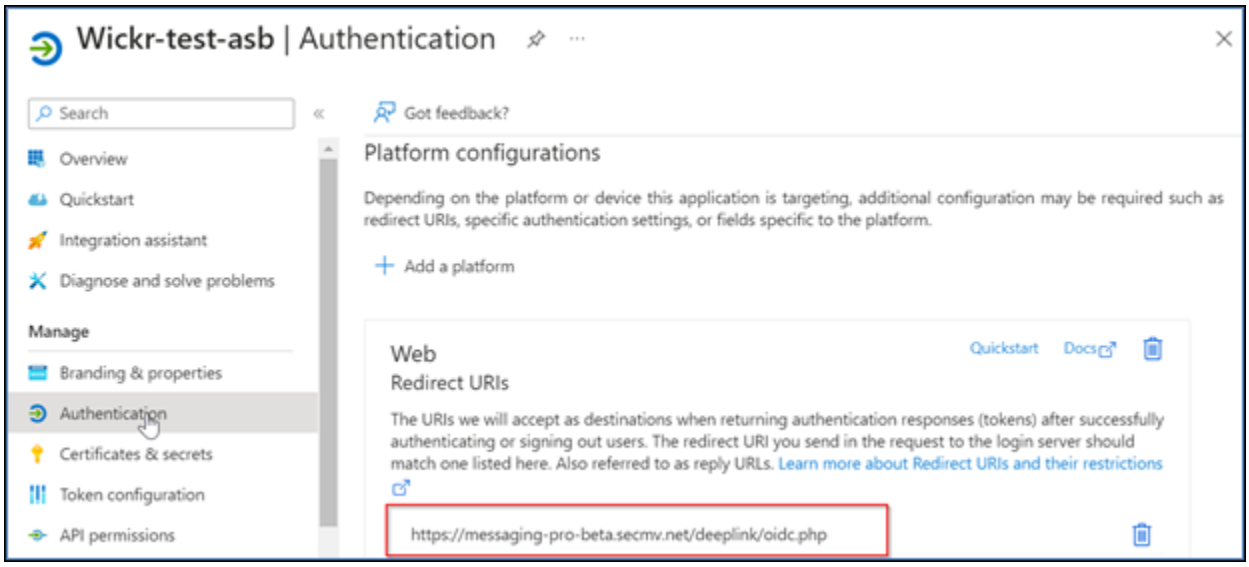
7. エンドポイントタブを選択して、次の点をメモします。
    1. Oauth 2.0 認可エンドポイント (v2): 例: `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/oauth2/v2.0/authorize`
    2. この値を編集して「oauth2/」と「authorize」を削除します。たとえば、固定 URL は次のようになります。 `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`
    3. これは SSO 発行者として参照されます。

ステップ 2: 認証を設定する

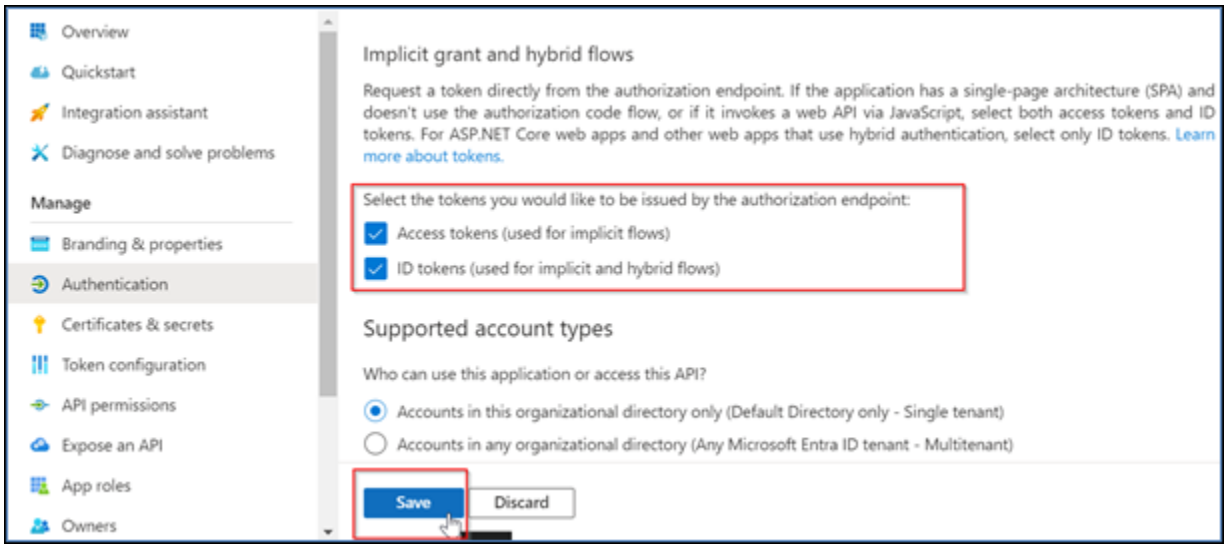
Microsoft Entra で認証を設定するには、次の手順を実行します。

1. ナビゲーションペインで、認証を選択します。

2. 認証ページで、ウェブリダイレクト URI が以前に入力したものと同じであることを確認します (アプリケーションとして AWS Wickr を登録する)。



3. Select 暗黙的なフローに使用されるアクセストークンと、暗黙的なフローとハイブリッドフローに使用される ID トークンを選択します。
4. [保存] を選択します。

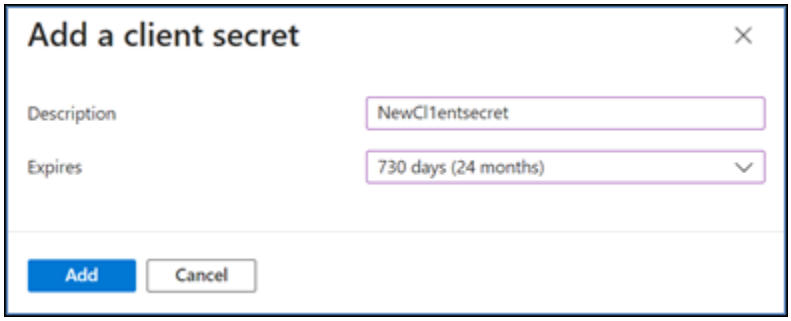


ステップ 3: 証明書とシークレットを設定する

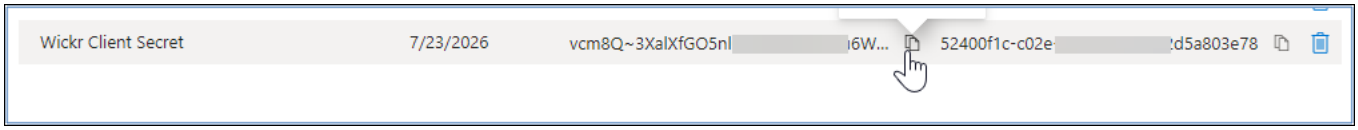
Microsoft Entra で証明書とシークレットを設定するには、次の手順を実行します。

1. ナビゲーションペインで、証明書とシークレットを選択します。
2. 証明書とシークレットページで、クライアントシークレットタブを選択します。

3. クライアントシークレットタブで、新しいクライアントシークレットを選択します。
4. 説明を入力し、シークレットの有効期限を選択します。
5. [Add] (追加) を選択します。



6. 証明書を作成したら、クライアントシークレット値をコピーします。

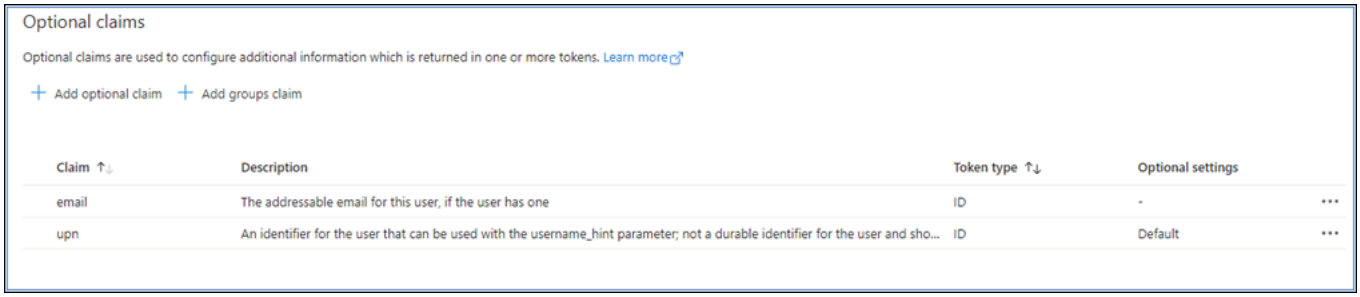


> **Note**
>
> クライアントアプリケーションコードには、クライアントシークレット値 (シークレット ID ではない) が必要です。このページを離れると、シークレット値を表示またはコピーできない場合があります。今すぐコピーしない場合は、戻って新しいクライアントシークレットを作成する必要があります。

ステップ 4: トークン設定をセットアップする

Microsoft Entra でトークン設定をセットアップするには、次の手順を実行します。

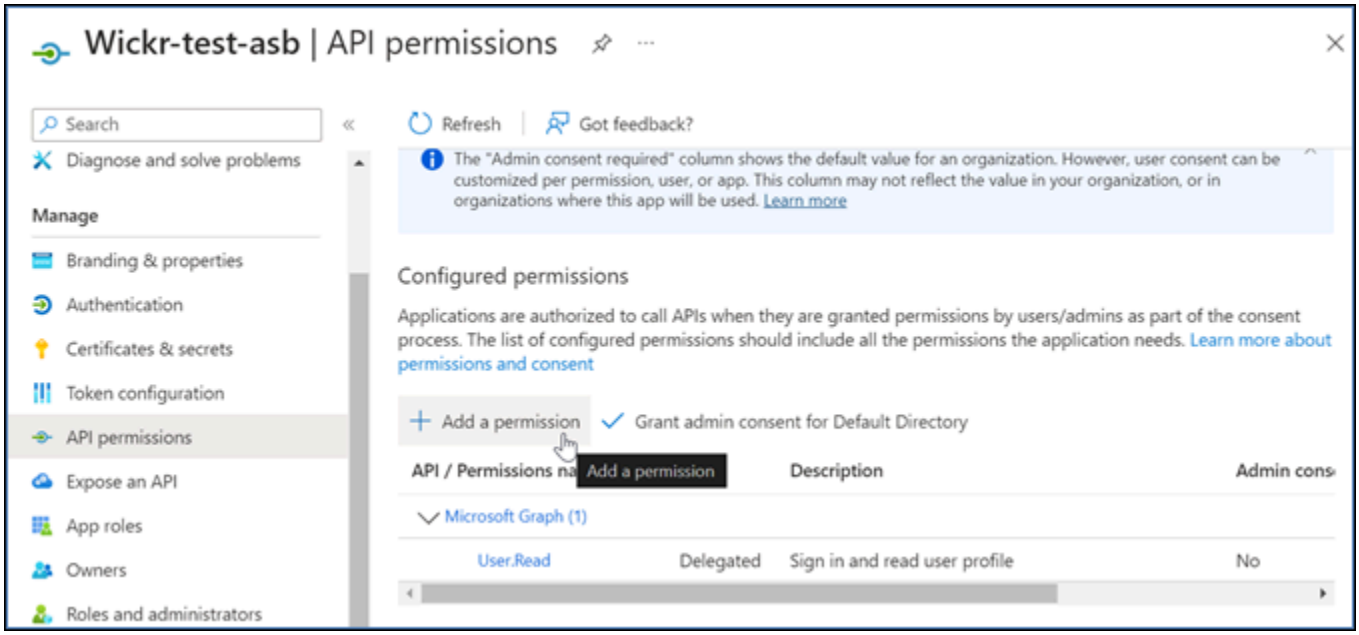
1. ナビゲーションペインで、トークン設定を選択します。
2. トークン設定ページで、オプションのクレームの追加を選択します。
3. オプションのクレームで、トークンタイプを IDとして選択します。
4. ID を選択したら、クレームで E メールを選択して更新します。
5. [Add] (追加) を選択します。



ステップ 5: API アクセス許可を設定する

Microsoft Entra で API アクセス許可を設定するには、次の手順を実行します。

1. ナビゲーションペインで、[API permissions] (API アクセス許可) を選択します。
2. API アクセス許可ページで、アクセス許可の追加を選択します。



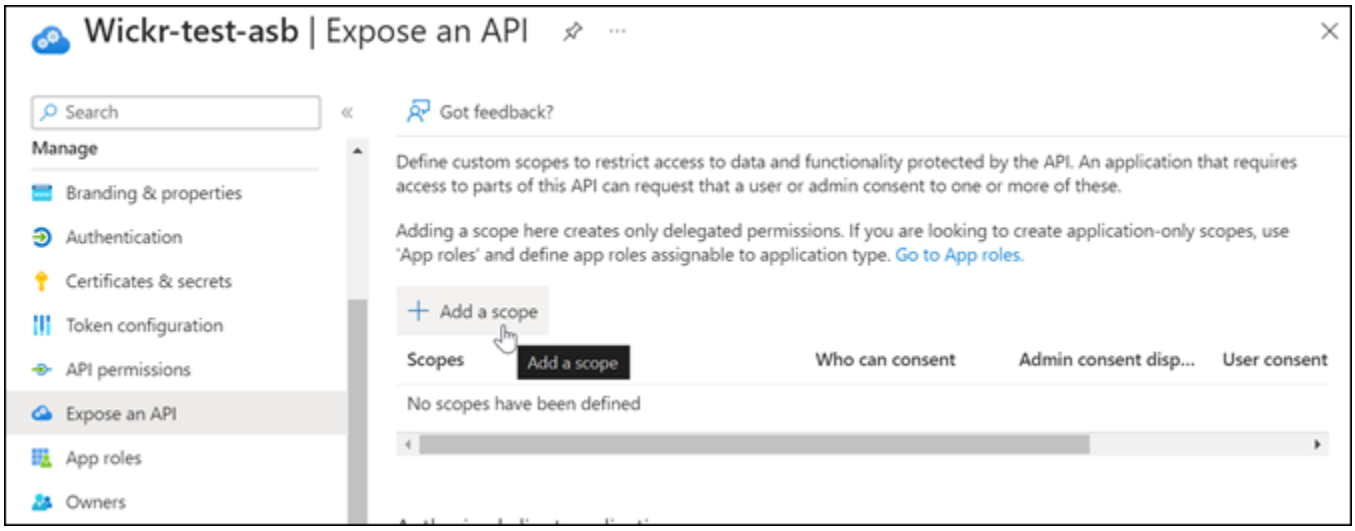
3. Microsoft Graph を選択し、委任されたアクセス許可 を選択します。
4. E メール 、オフラインアクセス、openid、プロファイルのチェックボックスをオンにします。
5. [Add permissions (許可の追加)] を選択します。

ステップ 6: API を公開する

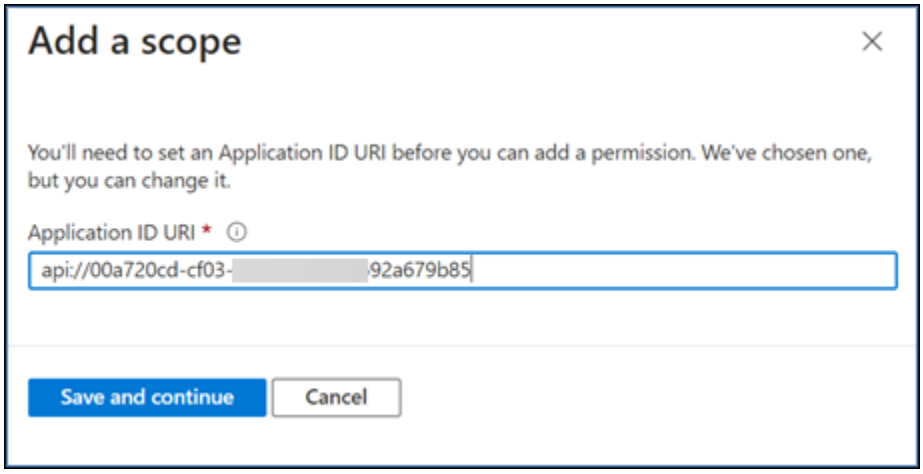
Microsoft Entra の 4 つのスコープごとに API を公開するには、次の手順を実行します。

1. ナビゲーションペインで、API を公開を選択します。

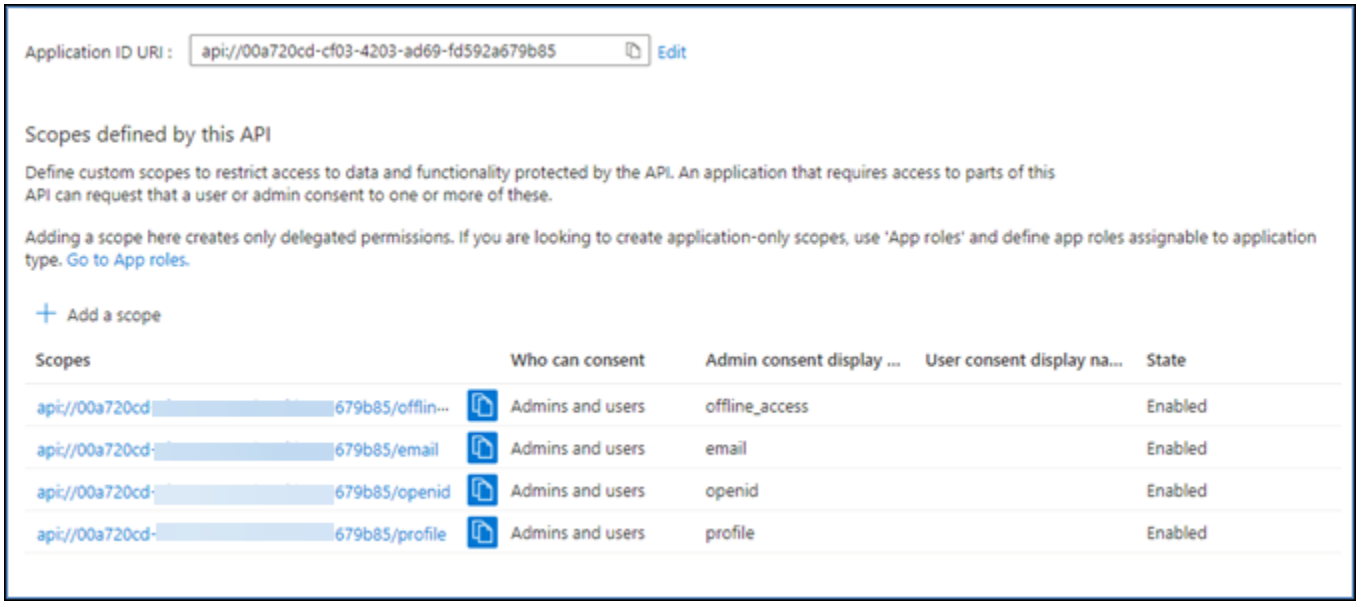
2. API を公開ページで、スコープの追加を選択します。



アプリケーション ID URI は自動的に入力され、URI に続く ID はアプリケーション ID (アプリケーションとして AWS Wickr を登録する で作成) と一致する必要があります。



3. [保存して続行] を選択します。
4. Admins and users タグを選択し、スコープ名を offline_access として入力します。
5. State を選択し、Enable を選択します。
6. スコープの追加 を選択します。
7. このセクションのステップ 1～6 を繰り返して、E メール、openid、プロファイルのスコープを追加します。



8. 「許可されたクライアントアプリケーション」で、「クライアントアプリケーションの追加」を選択します。
9. 前のステップで作成した 4 つのスコープをすべて選択します。
10. アプリケーション (クライアント) ID を入力または検証します。
11. [アプリケーションの追加] を選択します。

ステップ 7: AWS Wickr SSO 設定

AWS Wickr コンソールで次の設定手順を実行します。

1. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、ユーザー管理を選択し、SSO の設定を選択します。
4. 次の詳細情報を入力します。
   - 発行者 — これは以前に変更されたエンドポイントです (例: `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`)。
   - クライアント ID — これは概要ペインのアプリケーション (クライアント) ID です。
   - クライアントシークレット (オプション) — 証明書とシークレットペインのクライアントシークレットです。

- スコープ — API を公開ペインで公開されているスコープ名です。E メール、プロファイル、オフラインアクセス、openid を入力します。
- カスタムユーザー名スコープ (オプション) — upn と入力します。
- 会社 ID — 英数字とアンダースコア文字を含む一意のテキスト値にすることができます。このフレーズは、新しいデバイスに登録するときにユーザーが入力するものです。

その他のフィールドはオプションです。

5. [次へ] を選択します。
6. 確認と保存ページで詳細を確認し、変更の保存を選択します。

SSO 設定が完了しました。確認するために、Microsoft Entra のアプリケーションにユーザーを追加し、SSO と会社 ID を使用してユーザーでログインできるようになりました。

ユーザーを招待およびオンボーディングする方法の詳細については、「ユーザーの作成と招待」を参照してください。

トラブルシューティング

以下は、発生する可能性のある一般的な問題と、それらを解決するための提案です。

- SSO 接続テストが失敗するか、応答しません。
  - SSO 発行者が想定どおりに設定されていることを確認します。
  - SSO Configured の必須フィールドが想定どおりに設定されていることを確認します。
- 接続テストは成功しましたが、ユーザーはログインできません。
  - Microsoft Entra に登録した Wickr アプリケーションにユーザーが追加されていることを確認します。
  - ユーザーが プレフィックスを含む正しい会社 ID を使用していることを確認します。例: UE1-DemoNetworkW_drqtva。
  - AWS Wickr SSO 設定でクライアントシークレットが正しく設定されていない可能性があります。Microsoft Entra で別のクライアントシークレットを作成して再設定し、Wickr SSO 設定で新しいクライアントシークレットを設定します。

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。

AWS Wickr のネットワークタグ

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、 AWS コストを追跡したりできます。 AWS マネジメントコンソール for Wickr の Network ホーム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。

トピック

- AWS Wickr でネットワークタグを管理する
- AWS Wickr でネットワークタグを追加する
- AWS Wickr でネットワークタグを編集する
- AWS Wickr でネットワークタグを削除する

AWS Wickr でネットワークタグを管理する

Wickr ネットワークのネットワークタグを管理できます。

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. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ネットワークのホームページの「タグ」セクションで、「タグの管理」を選択します。
4. タグの管理ページで、次のいずれかのオプションを完了できます。

   - 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、「AWS Wickr でネットワークタグを追加する」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、「AWS Wickr でネットワークタグを編集する」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、「AWS Wickr でネットワークタグを削除する」を参照してください。

AWS Wickr でネットワークタグを追加する

Wickr ネットワークにネットワークタグを追加できます。

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、「AWS Wickr でネットワークタグを管理する」を参照してください。

1. ネットワークのホームページの「タグ」セクションで、「新しいタグの追加」を選択します。
2. [タグの管理]ページで、[タグの追加]を選択します。
3. 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。
4. [変更の保存]を選択して設定を保存します。

AWS Wickr でネットワークタグを編集する

Wickr ネットワークにネットワークタグを編集できます。

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、「AWS Wickr でネットワークタグを管理する」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。

AWS Wickr でネットワークタグを削除する

Wickr ネットワークへのネットワークタグを削除できます。

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、「AWS Wickr でネットワークタグを管理する」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。

AWS Wickr の領収書の読み取り

AWS Wickr の読み取り受信は、メッセージがいつ読み取られたかを示すために送信者に送信される通知です。これらの受信は、one-on-one の会話で利用できます。送信されたメッセージには 1 つのチェックマークが表示され、読み取りメッセージにはチェックマークが付いた実線の円が表示されます。外部との会話中にメッセージの読み取り受信を表示するには、両方のネットワークで読み取り受信が有効になっている必要があります。

管理者は、管理者パネルで読み取り受信を有効または無効にできます。この設定はネットワーク全体に適用されます。

読み取り受信を有効または無効にするには、次の手順を実行します。

1. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、ネットワークポリシーを選択します。
4. ネットワークポリシーページのメッセージングセクションで、編集を選択します。
5. チェックボックスをオンにして、読み取り受信を有効または無効にします。

6. [Save changes] (変更の保存) をクリックします。

AWS Wickr のネットワークプランを管理する

Wickr AWS マネジメントコンソール の 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、次の手順を実行します。

1. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. Network ホームページの Network details セクションで、Edit を選択します。
4. ネットワークの詳細の編集ページで、目的のネットワークプランを選択します。次のいずれかを選択して、現在のネットワークプランを変更できます。

   - 標準 — 管理統制と柔軟性を必要とする中小企業チーム向け。
   - 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、最大 30 人のユーザーが利用でき、3 か月間有効なプレミアム無料トライアルを選択できます。WickrGov AWS の場合、プレミアム無料トライアルオプションでは最大 50 人のユーザーが許可され、3 か月間使用できます。このオファーは、新規および標準プランでご利用いただけます。プレミアム無料トライアル期間中、管理者は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状況と請求を停止するには、ネットワークから中断されたユーザーを含め、すべてのユーザーを削除します。

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、次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登録できるのは、 AWS アカウントごとに 1 つのネットワークのみです。
- ゲストユーザー機能は、プレミアム無料トライアル中は利用できません。
- 標準ネットワークに 30 人を超えるユーザー (WickrGov では AWS 50 人を超えるユーザー) がいる場合、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。

AWS Wickr のデータ保持

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

AWS Wickr で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. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、ネットワークポリシーを選択します。
4. ネットワークポリシーページには、データ保持を設定する手順と、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、「AWS Wickr の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。

AWS Wickr の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 CloudWatch AWS Secrets Manager (CloudWatch)、Amazon Simple Notification Service (Amazon SNS)、 () 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。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

AWS Wickr のデータ保持を設定するための前提条件

開始する前に、Wickr AWS マネジメントコンソール の からデータ保持ボット名 (ユーザー名) 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、「AWS Wickr でデータ保持の詳細を表示する」を参照してください。

AWS Wickr のデータ保持ボットのパスワード

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、AWS Wickr でデータ保持ボットを設定する環境変数 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、AWS Wickr の Secrets Manager 値 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"
```

```
**********************************************************************
```

AWS Wickr ネットワークのストレージオプション

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、「AWS Wickr でデータ保持ボットを設定する環境変数」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。これは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。

  データ保持ボットで使用する 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。

AWS Wickr でデータ保持ボットを設定する環境変数

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、「Wickr ネットワークの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、「AWS Wickr の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、 AWS リージョン 使用するデフォルトを定義します。

- `AWS_DEFAULT_REGION` – Secrets Manager などの AWS サービス AWS リージョン に使用するデフォルト (Amazon S3 や では使用されません AWS KMS)。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。

次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、AWS Wickr の Secrets Manager 値 を参照してください。

- AWS_SECRET_NAME – データ保持ボットに必要な認証情報と 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 AWS リージョン がある 。 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、「AWS Wickr の Secrets Manager 値」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。

クライアント側の暗号化を使用して Amazon S3 バケットに保存するときにファイルを再暗号化する場合は、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 – データ保持ボット上のメッセージファイルとファイルを 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)。 Amazon S3
- WICKRIO_KMS_REGION – マスターキーが AWS KMS 配置されている 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 CloudWatch に送信します。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`— CloudWatch にメトリクスを送信するには、この環境変数の値を `cloudwatch` に設定します。

AWS Wickr の Secrets Manager 値

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。Secrets Manager シークレットの作成の詳細については、Secrets Manager ユーザーガイドの AWS Secrets Manager「シークレットの作成」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` – Amazon S3 バケットに保存される前に、データ保持ボット上のメッセージファイルとファイルを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 マスターキーが配置されている 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 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場合は、ホストがそれらにアクセスするための適切な AWS Identity and Access Management (IAM) ロールとポリシーを持っていることを確認

する必要があります。Secrets Manager、Amazon S3、CloudWatch、Amazon SNS、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。

JSON

```
{
    "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。

JSON

```
{
    "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。

Wickr ネットワークの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いため、オプションは制限されます。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、「AWS Wickr でデータ保持ボットを設定する環境変数」を参照してください。
- AWS サービスにアクセスできるため、Secrets Manager シークレットを作成してボット認証情報と 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、AWS Wickr の Secrets Manager 値 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、指定するリソースの AWS リージョンで指定します。例えば、 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* メッセージファイルとファイルの再暗号化に使用する AWS KMS マスターキーの Amazon リソースネーム (ARN) を使用します。

パスワード環境変数を使用してボットを起動する (AWS サービスなし)

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 AWS Wickr でデータ保持ボットを設定する環境変数 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でボットを起動する (AWS サービスなし)

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 AWS Wickr でデータ保持ボットを設定する環境変数 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でボットを起動する (AWS サービスなし)

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 --
network=host \
-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 --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e AWS_SECRET_NAME='wickrpro/alpha/new-3-bot' \
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 --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
 -e AWS_SECRET_NAME='wickrpro/alpha/compliance_1234567890_bot' \
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。

Secrets Manager AWS KMS を使用してボットを起動し、Amazon S3 と 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 --
network=host \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
 -e AWS_SECRET_NAME='wickrpro/alpha/compliance_1234567890_bot' \
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 --
network=host \
-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='bot-compliance' \
-e WICKRIO_S3_FOLDER_NAME='network1234567890' \
-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。

Wickr ネットワークの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
```

Wickr ネットワークのデータ保持ログを取得する

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
```

Wickr ネットワークのデータ保持メトリクスとイベント

以下は、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) イベントです。

トピック

Wickr ネットワークの CloudWatch メトリクス

メトリクスは 1 分間隔でボットによって生成され、データ保持ボットの Docker イメージが実行されているアカウントに関連付けられた CloudWatch 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。
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。

メトリクス	説明
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。

メトリックスは CloudWatch によって消費されるように生成されます。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。

ディメンション	値
Network	関連付けられたネットワークの ID。

Wickr ネットワークの 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、「AWS Wickr でデータ保持ボットを設定する環境変数」および「AWS Wickr の Secrets Manager 値」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。
メッセージ	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。
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。
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。

イベントタイプ	イベントメッセージ
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::slotAdminUserSuspend: code(%1): reason: %2“
BotDevice Suspended	デバイスが停止されました。
ウォッチドッグ	スイッチボードシステムが <*N*> 分以上停止しています
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
```

更新があります

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

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. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。

3. ナビゲーションペインで、[Security Groups] (セキュリティグループ) を選択します。
4. セキュリティグループページで、ATAK を有効にするセキュリティグループを選択します。
5. 統合タブの ATAK プラグインセクションで、編集を選択します。
6. ATAK プラグインの編集ページで、ATAK プラグインを有効にするチェックボックスをオンにします。
7. 新しいパッケージの追加を選択する
8. 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。
9. [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. [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] を選択してください。

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 用の Wickr プラグインのペアリングを解除する

ATAK 用 Wickr プラグインのペアリングを解除できます。

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。

   これで、ATAK 用 Wickr プラグインのペアリングが正常に解除されました。

ATAK でダイヤルして通話を受信する

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。

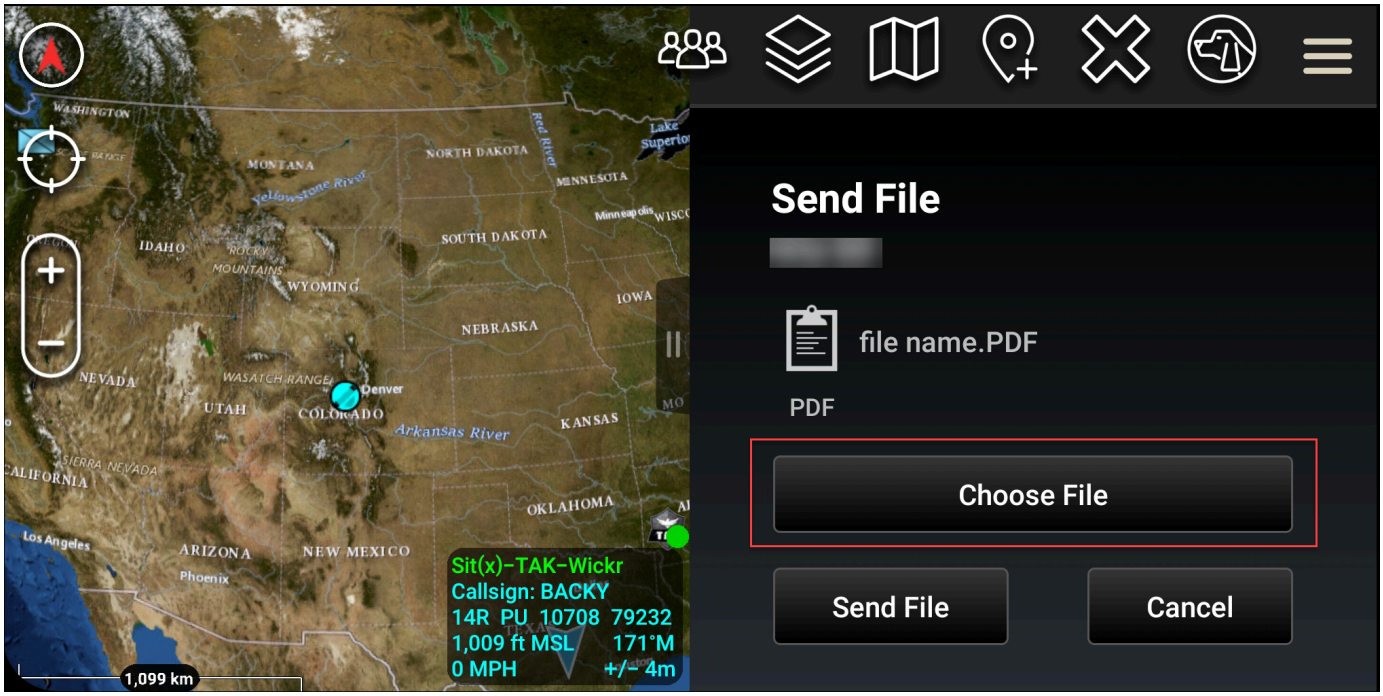
1. チャットウィンドウを開きます。
2. [マップ] ビューで、電話をかけるユーザーのアイコンを選択します。
3. 画面の右上にある電話アイコンを選択します。
4. 接続したら、ATAK プラグインビューに戻って電話を受けることができます。

ATAK でファイルを送信する

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。

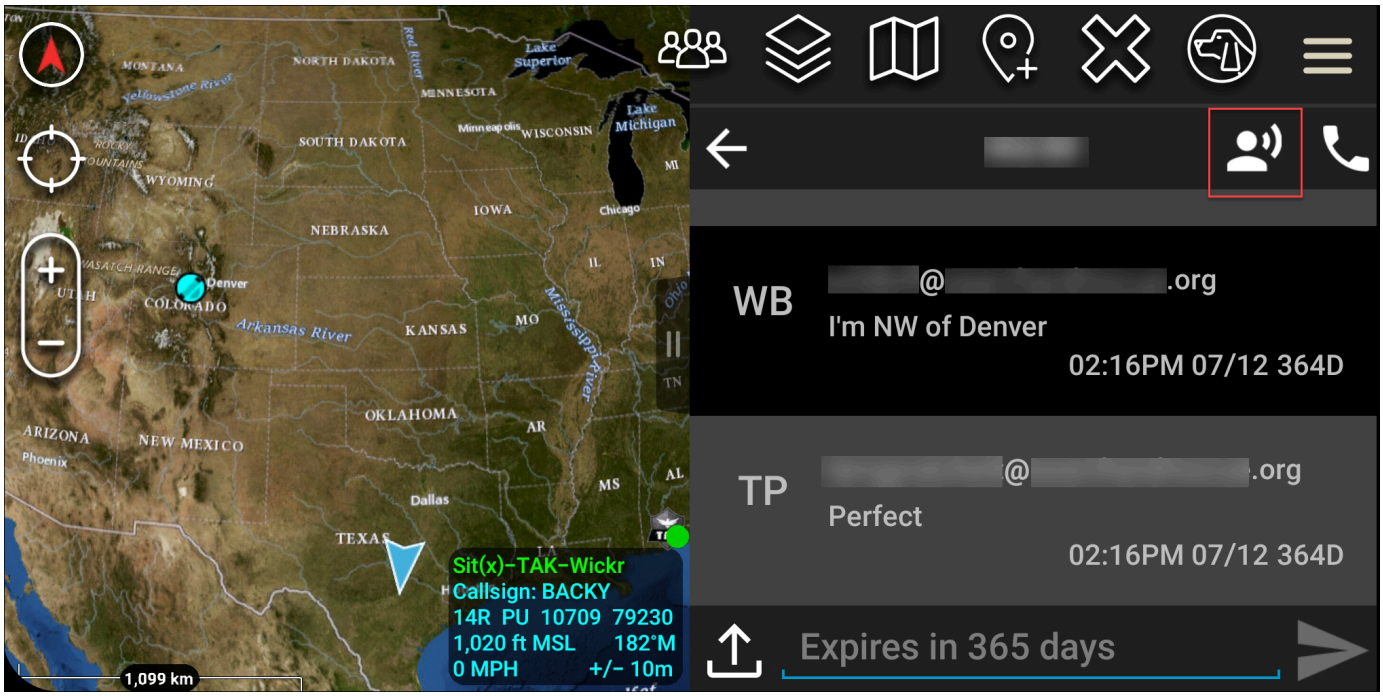
ATAK で安全な音声メッセージ (Push-to-talk) を送信する

ATAK 用 Wickr プラグインで安全な音声メッセージを送信できます (プッシュトゥトーク)。

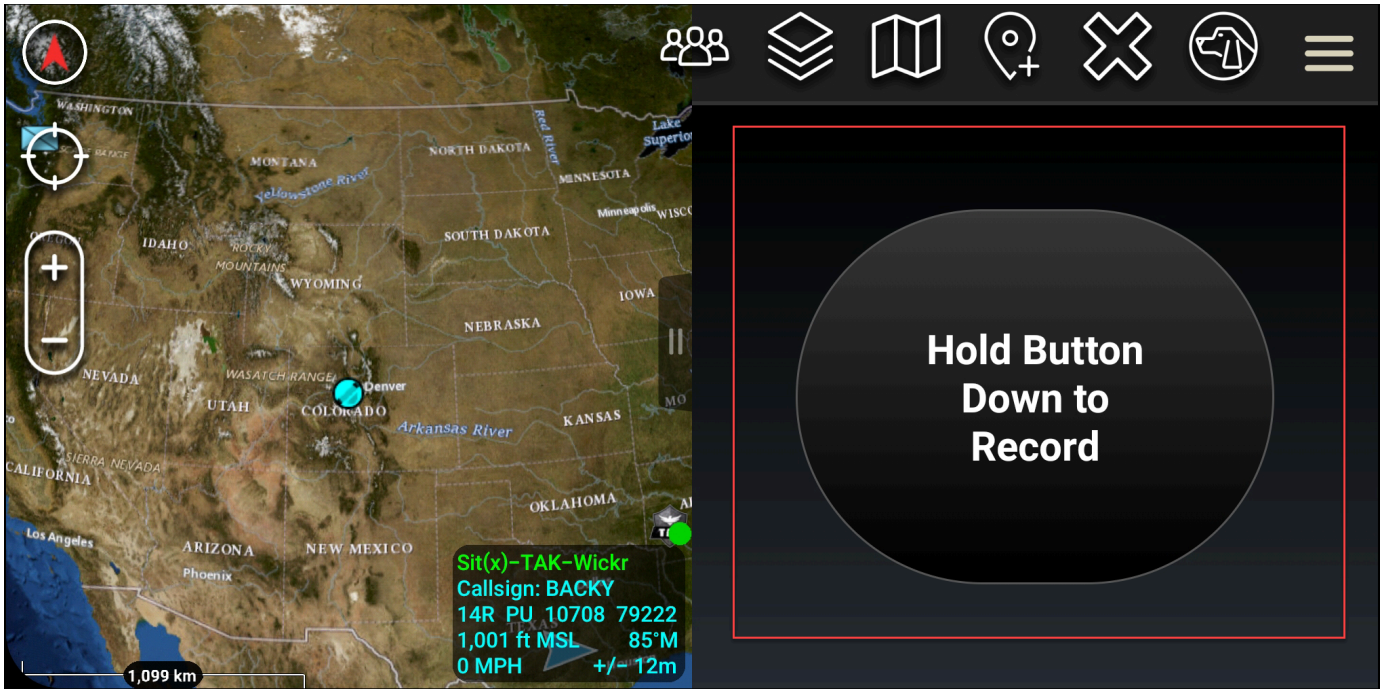
安全な音声メッセージを送信するには、次の手順を実行します。

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。



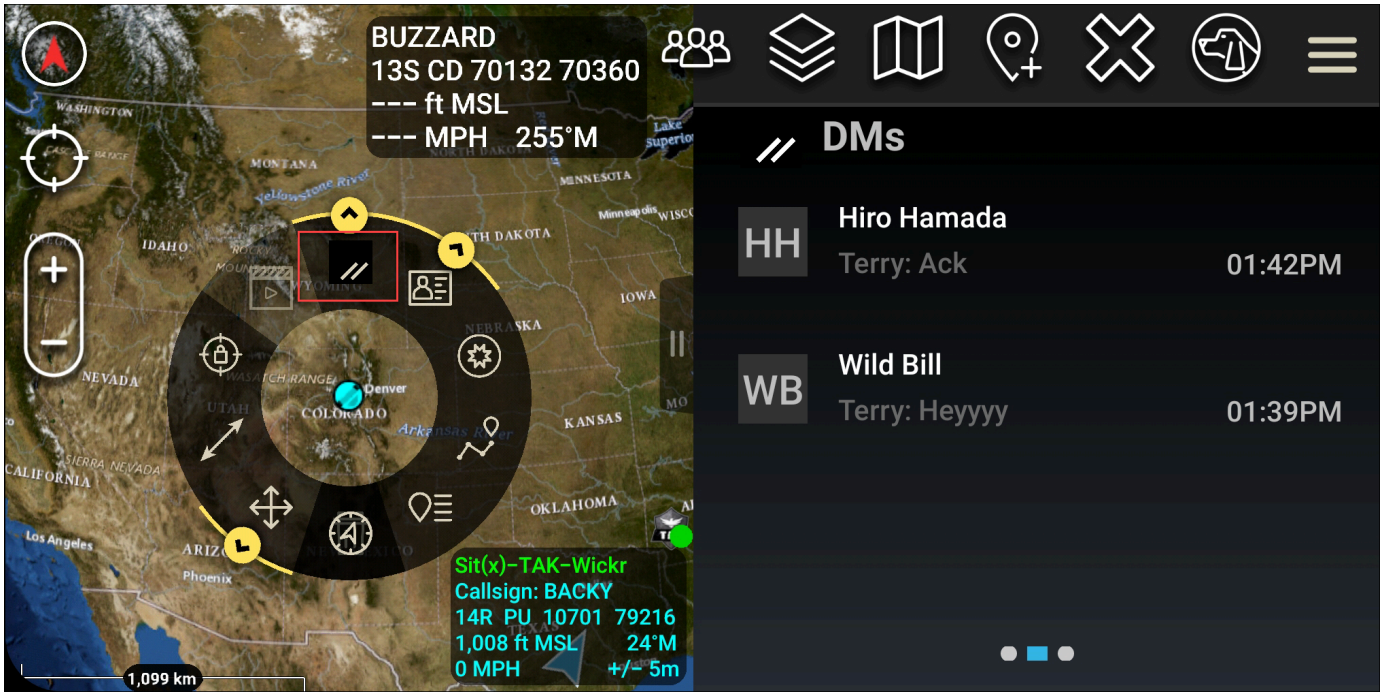
4. メッセージを録音します。
5. メッセージを録音した後、ボタンを離すと送信されます。

ATAK のピンホイール (クイックアクセス)

ピンホイール、別名クイックアクセス機能は、1 対 1 の会話やダイレクトメッセージに使用されます。

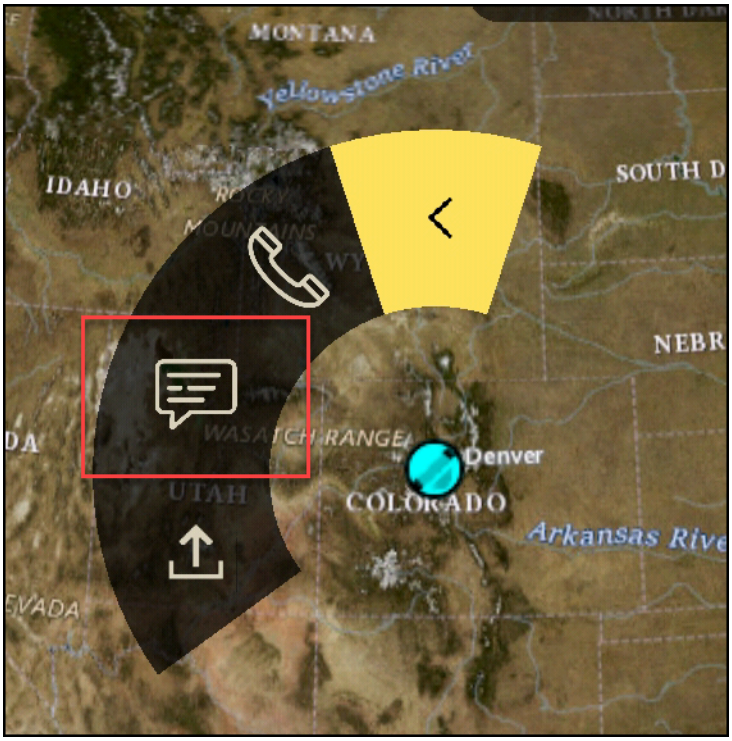
ピンホイールを使用するには、次の手順を実行します。

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。

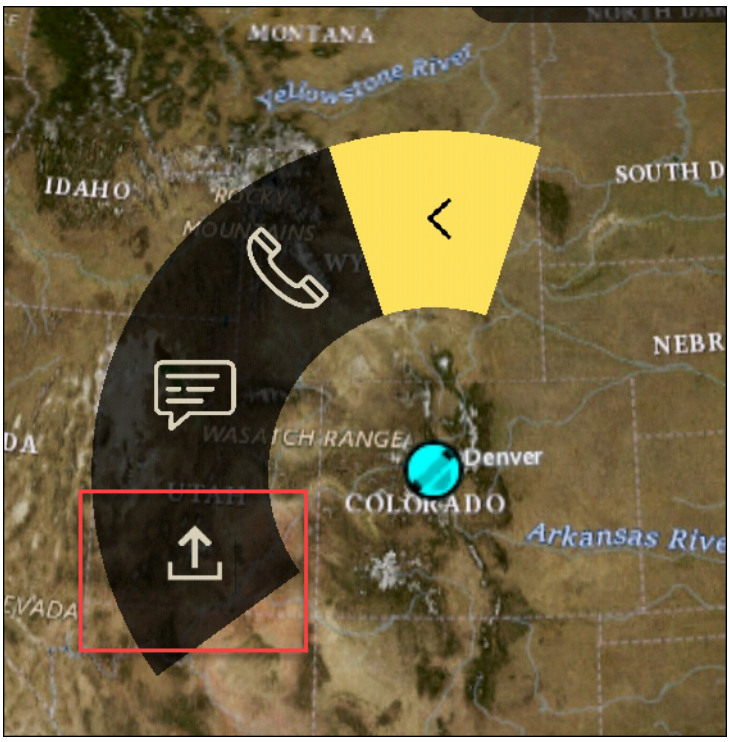


4. ピンホイールで、以下のいずれかのアイコンを選択します。
   - [電話]: 電話をかける場合に選択します。

- [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。



ATAK のナビゲーション

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。
- [DM ビュー]: 1 対 1 の会話を作成します。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。

Wickr ネットワークのリストを許可するポートとドメイン

Wickr が正しく機能するように、次のポートのリストを許可します。

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)

リージョン別の許可リストのドメインとアドレス

可能なすべての呼び出しドメインとサーバー IP アドレスを許可リストに登録する必要がある場合は、リージョン別の潜在的な CIDRs の次のリストを参照してください。このリストは変更される可能性があるため、定期的に確認してください。

> **Note**
>
> 登録と検証の E メールは、 `no-reply@amazonaws.com`と から送信されますdonotreply@wickr.email。

米国東部 (バージニア北部)

ドメイン:	• gw-pro-prod.wickr.com • api.messaging.wickr.us-east-1.amazonaws.com • ingress.prod.calling.wickr.com
CIDR アドレスの呼び出し:	• 44.211.195.0/27 • 44.213.83.32/28
IP アドレスの呼び出し:	• 44.211.195.0 • 44.211.195.1 • 44.211.195.2 • 44.211.195.3 • 44.211.195.4

	• 44.211.195.5 • 44.211.195.6 • 44.211.195.7 • 44.211.195.8 • 44.211.195.9 • 44.211.195.10 • 44.211.195.11 • 44.211.195.12 • 44.211.195.13 • 44.211.195.14 • 44.211.195.15 • 44.211.195.16 • 44.211.195.17 • 44.211.195.18 • 44.211.195.19 • 44.211.195.20 • 44.211.195.21 • 44.211.195.22 • 44.211.195.23 • 44.211.195.24 • 44.211.195.25 • 44.211.195.26 • 44.211.195.27 • 44.211.195.28 • 44.211.195.29 • 44.211.195.30 • 44.211.195.31 • 44.213.83.32 • 44.213.83.33 • 44.213.83.34

	• 44.213.83.35 • 44.213.83.36 • 44.213.83.37 • 44.213.83.38 • 44.213.83.39 • 44.213.83.40 • 44.213.83.41 • 44.213.83.42 • 44.213.83.43 • 44.213.83.44 • 44.213.83.45 • 44.213.83.46 • 44.213.83.47

アジアパシフィック (マレーシア)

ドメイン:	• gw-pro-prod.wickr.com • api.messaging.wickr.ap-southeast-5.amazonaws.com • ingress.prod.calling.wickr.ap-southeast-5.amazonaws.com
CIDR アドレスの呼び出し:	• 43.216.226.160/28
IP アドレスの呼び出し:	• 43.216.226.160 • 43.216.226.161 • 43.216.226.162 • 43.216.226.163 • 43.216.226.164 • 43.216.226.165 • 43.216.226.166 • 43.216.226.167

	• 43.216.226.168 • 43.216.226.169 • 43.216.226.170 • 43.216.226.171 • 43.216.226.172 • 43.216.226.173 • 43.216.226.174 • 43.216.226.175

アジアパシフィック (シンガポール)

ドメイン:	• gw-pro-prod.wickr.com • api.messaging.wickr.ap-southeast-1.amazonaws.com • ingress.prod.calling.wickr.ap-southeast-1.amazonaws.com
CIDR アドレスの呼び出し:	• 47.129.23.144/28
IP アドレスの呼び出し:	• 47.129.23.144 • 47.129.23.145 • 47.129.23.146 • 47.129.23.147 • 47.129.23.148 • 47.129.23.149 • 47.129.23.150 • 47.129.23.151 • 47.129.23.152 • 47.129.23.153 • 47.129.23.154 • 47.129.23.155 • 47.129.23.156

	• 47.129.23.157 • 47.129.23.158 • 47.129.23.159

アジアパシフィック (シドニー)

ドメイン:	• gw-pro-prod.wickr.com • api.messaging.wickr.ap-southeast-2.amazonaws.com • ingress.prod.calling.wickr.ap-southeast-2.amazonaws.com
CIDR アドレスの呼び出し:	• 3.27.180.208/28
IP アドレスの呼び出し:	• 3.27.180.208 • 3.27.180.209 • 3.27.180.210 • 3.27.180.211 • 3.27.180.212 • 3.27.180.213 • 3.27.180.214 • 3.27.180.215 • 3.27.180.216 • 3.27.180.217 • 3.27.180.218 • 3.27.180.219 • 3.27.180.220 • 3.27.180.221 • 3.27.180.222 • 3.27.180.223

アジアパシフィック (東京)

ドメイン:	• gw-pro-prod.wickr.com • api.messaging.wickr.ap-northeast-1.amazonaws.com • ingress.prod.calling.wickr.ap-northeast-1.amazonaws.com
CIDR アドレスの呼び出し:	• 57.181.142.240/28
IP アドレスの呼び出し:	• 57.181.142.240 • 57.181.142.241 • 57.181.142.242 • 57.181.142.243 • 57.181.142.244 • 57.181.142.245 • 57.181.142.246 • 57.181.142.247 • 57.181.142.248 • 57.181.142.249 • 57.181.142.250 • 57.181.142.251 • 57.181.142.252 • 57.181.142.253 • 57.181.142.254 • 57.181.142.255

カナダ (中部)

ドメイン:	• gw-pro-prod.wickr.com • api.messaging.wickr.ca-central-1.amazonaws.com

	• ingress.prod.calling.wickr.ca-central-1.amazonaws.com
CIDR アドレスの呼び出し:	• 15.156.152.96/28
IP アドレスの呼び出し:	• 15.156.152.96 • 15.156.152.97 • 15.156.152.98 • 15.156.152.99 • 15.156.152.100 • 15.156.152.101 • 15.156.152.102 • 15.156.152.103 • 15.156.152.104 • 15.156.152.105 • 15.156.152.106 • 15.156.152.107 • 15.156.152.108 • 15.156.152.109 • 15.156.152.110 • 15.156.152.111

欧州 (フランクフルト)

ドメイン:	• gw-pro-prod.wickr.com • api.messaging.wickr.eu-central-1.amazonaws.com • ingress.prod.calling.wickr.eu-central-1.amazonaws.com
CIDR アドレスの呼び出し:	• 3.78.252.32/28
IP アドレスの呼び出し:	• 3.78.252.32

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

メッセージング IP アドレス:	• 3.163.236.183 • 3.163.238.183 • 3.163.251.183 • 3.163.232.183 • 3.163.241.183 • 3.163.245.183 • 3.163.248.183 • 3.163.234.183 • 3.163.237.183 • 3.163.243.183 • 3.163.247.183 • 3.163.240.183 • 3.163.242.183 • 3.163.244.183 • 3.163.246.183 • 3.163.249.183 • 3.163.252.183 • 3.163.235.183 • 3.163.250.183 • 3.163.239.183 • 3.163.233.183

欧州 (ロンドン)

ドメイン:	• gw-pro-prod.wickr.com • api.messaging.wickr.eu-west-2.amazonaws.com • ingress.prod.calling.wickr.eu-west-2.amazonaws.com
CIDR アドレスの呼び出し:	• 13.43.91.48/28

IP アドレスの呼び出し:	• 13.43.91.48 • 13.43.91.49 • 13.43.91.50 • 13.43.91.51 • 13.43.91.52 • 13.43.91.53 • 13.43.91.54 • 13.43.91.55 • 13.43.91.56 • 13.43.91.57 • 13.43.91.58 • 13.43.91.59 • 13.43.91.60 • 13.43.91.61 • 13.43.91.62 • 13.43.91.63

欧州 (ストックホルム)

ドメイン:	• gw-pro-prod.wickr.com • api.messaging.wickr.eu-north-1.amazonaws.com • ingress.prod.calling.wickr.eu-north-1.amazonaws.com
CIDR アドレスの呼び出し:	• 13.60.1.64/28
IP アドレスの呼び出し:	• 13.60.1.64 • 13.60.1.65 • 13.60.1.66 • 13.60.1.67 • 13.60.1.68

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

欧州 (チューリッヒ)

ドメイン:	• gw-pro-prod.wickr.com • api.messaging.wickr.eu-central-2.amazonaws.com • ingress.prod.calling.wickr.eu-central-2.amazonaws.com
CIDR アドレスの呼び出し:	• 16.63.106.224/28
IP アドレスの呼び出し:	• 16.63.106.224 • 16.63.106.225 • 16.63.106.226 • 16.63.106.227 • 16.63.106.228 • 16.63.106.229 • 16.63.106.230 • 16.63.106.231 • 16.63.106.232 • 16.63.106.233

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

AWS GovCloud (米国西部)

ドメイン:	• gw-pro-prod.wickr.com • api.messaging.wickr.us-gov-west-1.amazonaws.com • ingress-prod-calling.wickr.us-gov-west-1.amazonaws.com • s3.us-gov-west-1.amazonaws.com • s3-fips.us-gov-west-1.amazonaws.com • s3.amazonaws.com • register.wickr.us-gov-west-1.amazonaws.com • admin.wickr.us-gov-west-1.amazonaws.com • admin.messaging.wickr.us-gov-west-1.amazonaws.com • cognito-identity.us-gov-west-1.amazonaws.com • kinesis.us-gov-west-1.amazonaws.com
CIDR アドレスの呼び出し:	• 3.30.186.208/28 • 3.31.11.216/29
IP アドレスの呼び出し:	• 3.30.186.208 • 3.30.186.209 • 3.30.186.210

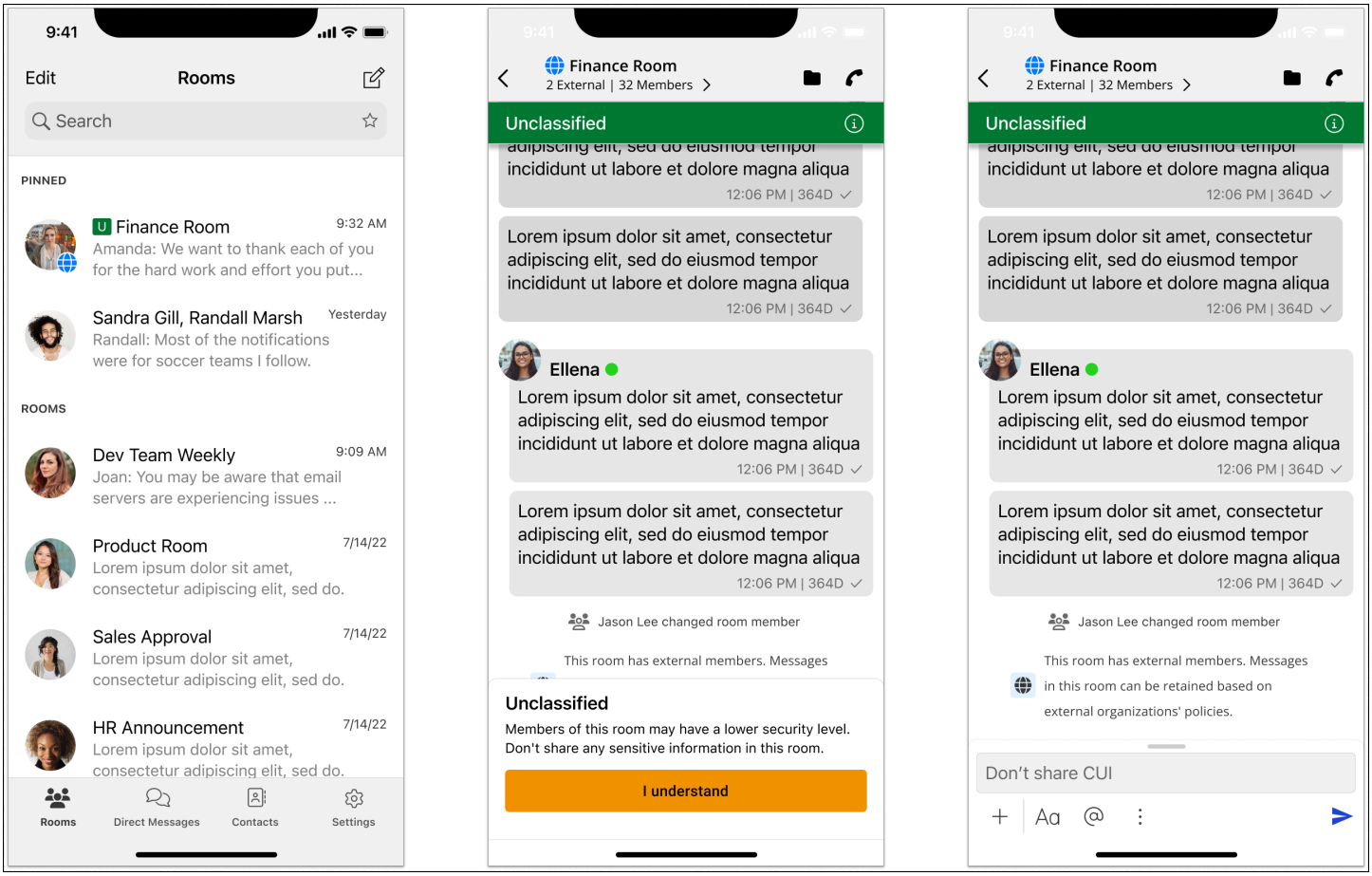
- 3.30.186.211
- 3.30.186.212
- 3.30.186.213
- 3.30.186.214
- 3.30.186.215
- 3.30.186.216
- 3.30.186.217
- 3.30.186.218
- 3.30.186.219
- 3.30.186.220
- 3.30.186.221
- 3.30.186.222
- 3.30.186.223
- 3.31.11.216
- 3.31.11.217
- 3.31.11.218
- 3.31.11.219
- 3.31.11.220
- 3.31.11.221
- 3.31.11.222
- 3.31.11.223

GovCloud クロス境界分類とフェデレーション

AWS Wickr は、GovCloud ユーザー向けにカスタマイズされた WickrGov クライアントを提供します。 GovCloud GovCloud フェデレーションを使用すると、GovCloud ユーザーと商用ユーザー間の通信が可能になります。クロス境界分類機能を使用すると、GovCloud ユーザーの会話に対するユーザーインターフェイスの変更が可能になります。GovCloud ユーザーとして、政府定義の分類に関する厳格なガイドラインに従う必要があります。GovCloud ユーザーが商用ユーザー (エンタープライズ、AWS Wickr、ゲストユーザー) と会話すると、以下の分類されていない警告が表示されます。

- ルームリストの U タグ

- メッセージ画面上の未分類の確認
- 会話の上部にある分類されていないバナー



> **Note**
>
> これらの警告は、GovCloud ユーザーが外部ユーザーと会話しているとき、またはルームの一部である場合にのみ表示されます。外部ユーザーが会話から退出すると、それらは消えます。GovCloud ユーザー間の会話では警告は表示されません。

AWS Wickr のファイルプレビュー

Wickr Premium 階層 (Premium 無料トライアルを含む) を使用している組織は、セキュリティグループレベルでファイルのダウンロード許可を管理できるようになりました。

ファイルのダウンロードは、セキュリティグループでデフォルトで有効になっています。管理者は、管理者パネルを使用してファイルのダウンロードを有効または無効にできます。この設定は Wickr ネットワーク全体に適用されます。

ファイルのダウンロードを有効または無効にするには、次の手順を実行します。

1. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、[Security Groups] (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の名前を選択します。

   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. メッセージングタブの「メディアとリンク」セクションで、編集を選択します。
6. メディアとリンクの編集ページで、ファイルのダウンロードオプションをオンまたはオフにします。
7. [Save changes] (変更の保存) をクリックします。

セキュリティグループでファイルのダウンロードを有効にすると、ユーザーはダイレクトメッセージとルームで共有されているファイルをダウンロードできます。ダウンロードが無効になっている場合、これらのファイルをプレビューしてファイルタブにアップロードすることしかできませんが、ダウンロードすることはできません。ユーザーもスクリーンショットの撮影が制限されます。試行すると黒い画面になります。

> **Note**
>
> ファイルのダウンロードが無効になっている場合、このファイル設定を適用するには、そのセキュリティグループ内のすべてのユーザーが Wickr バージョン 6.54 以降を使用している必要があります。

> **Note**
>
> (フェデレーションによる) さまざまなネットワークとセキュリティグループのユーザーがいる部屋では、各ユーザーがファイルをプレビューまたはダウンロードできるかどうかは、特

定のセキュリティグループ設定に基づきます。その結果、一部のユーザーはルーム内のファイルをダウンロードでき、他のユーザーはプレビューのみできます。

AWS Wickr でユーザーを管理する

Wickr AWS マネジメントコンソール の のユーザー管理セクションでは、現在の Wickr ユーザーとボットを表示し、詳細を変更できます。

トピック

- AWS Wickr ネットワークのチームディレクトリ
- AWS Wickr ネットワークのゲストユーザー

AWS Wickr ネットワークのチームディレクトリ

現在の Wickr ユーザーを表示し、Wickr AWS マネジメントコンソール の のユーザー管理セクションで詳細を変更できます。

トピック

- AWS Wickr ネットワークでユーザーを表示する
- AWS Wickr ネットワークでユーザーを招待する
- AWS Wickr ネットワークでユーザーを編集する
- AWS Wickr ネットワークでユーザーを削除する
- AWS Wickr ネットワークのユーザーを一括削除する
- AWS Wickr ネットワークのユーザーを一括停止する

AWS Wickr ネットワークで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の詳細を表示できます。

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. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、ユーザー管理を選択します。

   チームディレクトリタブには、名前、E 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。

AWS Wickr ネットワークでユーザーを招待する

Wickr ネットワークでユーザーを招待できます。

Wickr ネットワークでユーザーを招待するには、次の手順を実行します。

1. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、ユーザー管理を選択します。
4. チームディレクトリタブで、ユーザーを招待を選択します。
5. ユーザーを招待ページで、ユーザーの E メールアドレスとセキュリティグループを入力します。E メールアドレスとセキュリティグループは、必須のフィールドのみです。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. [Invite user] 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。

AWS Wickr ネットワークでユーザーを編集する

Wickr ネットワークでユーザーを編集できます。

ユーザーを編集するには、次の手順を実行します。

1. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、ユーザー管理を選択します。
4. チームディレクトリタブで、編集するユーザーの縦の省略記号 (3 つのドット) アイコンを選択します。

5. [編集] を選択します。
6. ユーザー情報を編集し、変更の保存を選択します。

AWS Wickr ネットワークでユーザーを削除する

Wickr ネットワーク内のユーザーを削除できます。

ユーザーを削除するには、次の手順を実行します。

1. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、ユーザー管理を選択します。
4. チームディレクトリタブで、削除するユーザーの縦の省略記号 (3 つのドット) 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。
6. ポップアップウィンドウで、[削除] を選択します。

AWS Wickr ネットワークのユーザーを一括削除する

Wickr 用 の「ユーザー管理 AWS マネジメントコンソール 」セクションで Wickr ネットワークユーザーを一括削除できます。

> **Note**
>
> ユーザーを一括削除するオプションは、SSO が有効になっていない場合にのみ適用されます。

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. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。

3. ナビゲーションペインで、ユーザー管理を選択します。
4. チームディレクトリタブには、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。
5. チームディレクトリタブで、ユーザーの管理を選択し、一括削除を選択します。
6. ユーザーを一括削除ページで、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。
7. ネットワークから一括削除するユーザーの E メールを追加して、テンプレートを完了します。
8. 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。
9. チェックボックスをオンにすると、ユーザーの削除は元に戻せないことがわかります。
10. 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. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、ユーザー管理を選択します。
4. チームディレクトリタブには、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。
5. チームディレクトリタブで、ユーザーの管理を選択し、CSV としてダウンロードを選択します。
6. 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。
7. チームディレクトリタブで、ユーザーの管理を選択し、一括削除を選択します。
8. ユーザー一括削除ページで、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。アップロードボックスにファイルをドラッグアンドドロップするか、ファイルの選択を選択します。

9. チェックボックスをオンにすると、ユーザーの削除は元に戻せないことがわかります。
10. 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。

AWS Wickr ネットワークのユーザーを一括停止する

Wickr ネットワークユーザーを一括停止するには、「 for Wickr AWS マネジメントコンソール 」の「ユーザー管理」セクションを参照してください。

> **Note**
>
> ユーザーを一括停止するオプションは、SSO が有効になっていない場合にのみ適用されます。

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. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、ユーザー管理を選択します。
4. チームディレクトリタブには、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。
5. チームディレクトリタブで、ユーザーの管理を選択し、一括停止を選択します。
6. ユーザーを一括停止ページで、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。
7. 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。
8. 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。
9. ユーザーを停止を選択します。

> **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。

AWS Wickr ネットワークのゲストユーザー

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 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。 AWS アカウント ゲストユーザー機能の には料金が適用されます。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

- AWS Wickr ネットワークでゲストユーザーを有効または無効にする
- AWS Wickr ネットワークでゲストユーザー数を表示する
- AWS Wickr ネットワークでの月別使用量の表示
- AWS Wickr ネットワークでゲストユーザーを表示する
- AWS Wickr ネットワークでゲストユーザーをブロックする

AWS Wickr ネットワークでゲストユーザーを有効または無効にする

Wickr ネットワークでゲストユーザーを有効または無効にできます。

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. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、[Security Groups] (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名前を選択します。

> **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. ゲストユーザーを有効にするオプションが利用できる場所は 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) のネットワークの場合は、ページのローカルフェデレーションセクションで編集を選択します。
   - グローバルフェデレーション — 他のリージョンの他のすべてのネットワークについては、ページのグローバルフェデレーションセクションで編集を選択します。
7. フェデレーションの編集ページで、フェデレーションを有効にするを選択します。
8. 変更を保存を選択して変更を保存し、セキュリティグループに対して有効にします。

   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。

AWS Wickr ネットワークでゲストユーザー数を表示する

Wickr ネットワークでゲストユーザー数を表示できます。

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. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、ユーザー管理を選択します。

   ユーザー管理ページには、Wickr ネットワーク内のゲストユーザーの数が表示されます。

AWS Wickr ネットワークでの月別使用量の表示

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。

Wickr ネットワークの毎月の使用状況を表示するには、次の手順を実行します。

1. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、ユーザー管理を選択します。
4. ゲストユーザータブを選択します。

   ゲストユーザータブには、ゲストユーザーの毎月の使用状況が表示されます。

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

AWS Wickr ネットワークでゲストユーザーを表示する

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を表示できます。

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を表示するには、次の手順を実行します。

1. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、ユーザー管理を選択します。
4. ゲストユーザータブを選択します。

   ゲストユーザータブには、ネットワーク内のゲストユーザーが表示されます。

AWS Wickr ネットワークでゲストユーザーをブロックする

Wickr ネットワークでゲストユーザーをブロックまたはブロック解除できます。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. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、ユーザー管理を選択します。

4. ゲストユーザータブを選択します。

   ゲストユーザータブには、ネットワーク内のゲストユーザーが表示されます。
5. [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。
6. ゲストユーザー名の右側で、3 つのドットを選択し、ゲストユーザーをブロックを選択します。
7. ポップアップウィンドウで [ブロック] を選択します。
8. Wickr ネットワークでブロックされたユーザーのリストを表示するには、ステータスドロップダウンメニューを選択し、ブロックを選択します。

ゲストユーザーのブロックを解除するには

1. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、ユーザー管理を選択します。
4. ゲストユーザータブを選択します。

   ゲストユーザータブには、ネットワーク内のゲストユーザーが表示されます。
5. Status ドロップダウンメニューを選択し、Blocked を選択します。
6. ブロック セクションで、ブロックを解除するゲストユーザーの E メールを見つけます。
7. ゲストユーザー名の右側で、3 つのドットを選択し、ユーザーの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

でのクラウドセキュリティが最優先事項 AWS です。お客様は AWS 、セキュリティを最も重視する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からメリットを得られます。

セキュリティは、 AWS お客様とお客様の間の責任共有です。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説明しています。

- クラウドのセキュリティ – AWS は、 で AWS 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を担います AWS クラウド。 は、お客様が安全に使用できるサービス AWS も提供します。サードパーティーの監査者は、AWS コンプライアンスプログラムコンプライアンスプログラムの一環として、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。AWS Wickr に適用されるコンプライアンスプログラムの詳細については、「コンプライアンスプログラムAWS による対象範囲内のサービスコンプライアンスプログラム」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、使用する AWS サービスによって決まります。また、ユーザーは、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 リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

トピック

AWS Wickr でのデータ保護

責任 AWS 共有モデル、AWS Wickr で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 はすべての 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。ユーザーは、このインフラストラクチャでホストされ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に関する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。

データ保護の目的で、認証情報を保護し AWS アカウント 、 AWS IAM アイデンティティセンターまたは 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。この方法により、それぞれのジョブを遂行するために必要な権限のみが各ユーザーに付与されます。また、次の方法でデータを保護することもお勧めします:

- 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 AWS リソースと通信します。TLS 1.2 は必須ですが、TLS 1.3 を推奨します。
- で API とユーザーアクティビティのログ記録を設定します AWS CloudTrail。CloudTrail 証跡を使用して AWS アクティビティをキャプチャする方法については、「 AWS CloudTrail ユーザーガイド」のCloudTrail 証跡の使用」を参照してください。
- AWS 暗号化ソリューションと、その中のすべてのデフォルトのセキュリティコントロールを使用します AWS のサービス。
- Amazon Macie などの高度な管理された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 にアクセスするときに FIPS 140-3 検証済み暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。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) 140-3」を参照してください。

お客様の E メールアドレスなどの極秘または機密情報を、タグ、または [名前] フィールドなどの自由形式のテキストフィールドに含めないことを強くお勧めします。これは、コンソール、API、または SDK を使用して Wickr AWS CLIまたは他の AWS のサービス を使用する場合も同様です。 AWS SDKs タグ、または名前に使用される自由記述のテキストフィールドに入力したデータは、請求または診断ログに使用される場合があります。外部サーバーに URL を提供する場合、そのサーバーへのリクエストを検証できるように、認証情報を URL に含めないことを強くお勧めします。

AWS Wickr の ID とアクセス管理

AWS Identity and Access Management (IAM) は、管理者が AWS リソースへのアクセスを安全に制御 AWS のサービス するのに役立つ です。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 は、追加料金なしで使用できる AWS のサービス です。

トピック

AWS Wickr の対象者

AWS Identity and Access Management (IAM) の使用方法は、ロールによって異なります。

- サービスユーザー - 機能にアクセスできない場合は、管理者にアクセス許可をリクエストします (「AWS Wickr の ID とアクセスのトラブルシューティング」を参照)。
- サービス管理者 - ユーザーアクセスを決定し、アクセス許可リクエストを送信します (「AWS Wickr と IAM の連携方法」を参照)
- IAM 管理者 - アクセスを管理するためのポリシーを作成します (「AWS Wickr のアイデンティティベースのポリシーの例」を参照)

AWS Wickr の ID を使用した認証

認証とは、ID 認証情報 AWS を使用して にサインインする方法です。、IAM ユーザー AWS アカウントのルートユーザー、または IAM ロールを引き受けることで認証される必要があります。

AWS IAM アイデンティティセンター (IAM Identity Center)、シングルサインオン認証、Google/Facebook 認証情報などの ID ソースからの認証情報を使用して、フェデレーティッド ID としてサイ

ンインできます。サインインの詳細については、「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。

プログラムによるアクセスの場合、 は SDK と CLI AWS を提供してリクエストを暗号化して署名します。詳細については、「IAM ユーザーガイド」の「API リクエストに対するAWS 署名バージョン 4」を参照してください。

AWS アカウント ルートユーザー

を作成するときは AWS アカウント、すべての AWS のサービス および リソースへの完全なアクセス権を持つ AWS アカウント ルートユーザーと呼ばれる 1 つのサインインアイデンティティから始めます。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。ルートユーザー認証情報を必要とするタスクについては、「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。

フェデレーテッドアイデンティティ

ベストプラクティスとして、人間のユーザーが一時的な認証情報 AWS のサービス を使用して にアクセスするには、ID プロバイダーとのフェデレーションを使用する必要があります。

フェデレーティッド ID は、エンタープライズディレクトリ、ウェブ ID プロバイダー、または ID Directory Service ソースの認証情報 AWS のサービス を使用して にアクセスするユーザーです。フェデレーテッドアイデンティティは、一時的な認証情報を提供するロールを引き受けます。

アクセスを一元管理する場合は、 AWS IAM アイデンティティセンターをお勧めします。詳細については、「AWS IAM アイデンティティセンター ユーザーガイド」の「IAM アイデンティティセンターとは」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、特定の個人やアプリケーションに対する特定のアクセス許可を持つアイデンティティです。長期認証情報を持つ IAM ユーザーの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。詳細については、IAM ユーザーガイドの「ID プロバイダーとのフェデレーションを使用して にアクセスする必要がある AWS」を参照してください。

IAM グループは、IAM ユーザーの集合を指定し、大量のユーザーに対するアクセス許可の管理を容易にします。詳細については、「IAM ユーザーガイド」の「IAM ユーザーに関するユースケース」を参照してください。

IAM ロール

IAM ロールは、特定のアクセス許可を持つアイデンティであり、一時的な認証情報を提供します。ユーザーから IAM ロール (コンソール) に切り替えるか、 または API オペレーションを呼び出すことで、ロールを引き受けることができます。 AWS CLI AWS 詳細については、「IAM ユーザーガイド」の「ロールを引き受けるための各種方法」を参照してください。

IAM ロールは、フェデレーションユーザーアクセス、一時的な IAM ユーザーのアクセス許可、クロスアカウントアクセス、クロスサービスアクセス、および Amazon EC2 で実行するアプリケーションに役立ちます。詳細については、IAM ユーザーガイド の IAM でのクロスアカウントリソースアクセス を参照してください。

AWS Wickr のポリシーを使用したアクセスの管理

でアクセスを制御する AWS には、ポリシーを作成し、ID AWS またはリソースにアタッチします。ポリシーは、ID またはリソースに関連付けられたときにアクセス許可を定義します。 は、プリンシパルがリクエストを行うときにこれらのポリシー AWS を評価します。ほとんどのポリシーは JSON ドキュメント AWS として に保存されます。JSON ポリシードキュメントの詳細については、「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、ポリシーを使用して、どのプリンシパルがどのリソースに対して、どのような条件でアクションを実行できるかを定義することで、誰が何にアクセスできるかを指定します。

デフォルトでは、ユーザーやロールにアクセス許可はありません。IAM 管理者は IAM ポリシーを作成してロールに追加し、このロールをユーザーが引き受けられるようにします。IAM ポリシーは、オペレーションの実行方法を問わず、アクセス許可を定義します。

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のポリシーは、アイデンティティ (ユーザー、グループ、またはロール) にアタッチできる JSON アクセス許可ポリシードキュメントです。これらのポリシーは、アイデンティティがどのリソースに対してどのような条件下でどのようなアクションを実行できるかを制御します。アイデンティティベースポリシーの作成方法については、IAM ユーザーガイド の カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する 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、インラインポリシー (単一の ID に直接埋め込む) または管理ポリシー (複数の ID にアタッチされたスタンドアロンポリシー) にすることができます。管理ポリシーと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「管理ポリシーとインラインポリシーのいずれかを選択する」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。例としては、IAM ロール信頼ポリシーや Amazon S3 バケットポリシーなどがあります。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。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。

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。リソースベースのポリシーでは、IAM の AWS マネージドポリシーを使用できません。

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アクセス許可を持つかを制御します。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。

Amazon S3、および Amazon VPC は AWS WAF、ACLs。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 は、一般的でない追加のポリシータイプをサポートします。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) に付与できる権限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、権限は無効になります。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ション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、権限は無効になります。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アクセス許可を理解するのがさらに難しくなります。が複数のポリシータイプが関与する場合にリクエストを許可するかどうか AWS 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

ユーザー、グループ、ロールにアクセス許可を追加するには、自分でポリシーを記述するよりも AWS 管理ポリシーを使用する方が簡単です。チームに必要な権限のみを提供する 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。すぐに開始するには、 AWS マネージドポリシーを使用できます。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 管理ポリシーを維持および更新します。 AWS 管理ポリシーのアクセス許可は変更できません。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。サービスは AWS マネージドポリシーからアクセス許可を削除しないため、ポリシーの更新によって既存のアクセス許可が損なわれることはありません。

AWS マネージドポリシー: AWSWickrFullAccess

`AWSWickrFullAccess` ポリシーを IAM アイデンティティにアタッチできます。このポリシーは、AWS マネジメントコンソール内の Wickr の AWS マネジメントコンソール 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。

JSON

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

AWS 管理ポリシーの Wickr 更新

このサービスがこれらの変更の追跡を開始してからの Wickr の AWS マネージド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 マネジメントコンソールの 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、 AWS 管理ポリシーの変更の追跡を開始しました。	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	あり
リソースベースのポリシー	なし
ポリシーアクション	あり
ポリシーリソース	いいえ
ポリシー条件キー	いいえ
ACL	なし
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	いいえ

Wickr およびその他の AWS のサービスがほとんどの IAM 機能と連携する方法の概要については、「IAM ユーザーガイド」のAWS 「IAM と連携する のサービス」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のポリシーのサポート: あり

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ポリシーの作成方法については、「IAM ユーザーガイド」の「カスタマー管理ポリシーでカスタム IAM アクセス許可を定義する」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。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コントロールできます。ポリシーがアタッチ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、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 を含めることができます 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、全体のアカウント、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。詳細については、IAM ユーザーガイドのIAM でのクロスアカウントリソースアクセス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のサポート: あり

管理者は JSON AWS 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。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

ポリシーリソースのサポート: なし

管理者は JSON AWS 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 ポリシー要素はアクションが適用されるオブジェクトを指定します。ベストプラクティスとして、Amazon リソースネーム (ARN) を使用してリソースを指定します。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へのサポート: なし

管理者は JSON AWS 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 要素は、定義された基準に基づいてステートメントが実行される時期を指定します。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して、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。すべての AWS 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: なし

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アクセス許可を持つかを制御します。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: なし

属性ベースのアクセス制御 (ABAC) は、タグと呼ばれる属性に基づいてアクセス許可を定義する認可戦略です。IAM エンティティと AWS リソースにタグをアタッチし、プリンシパルのタグがリソースのタグと一致するときにオペレーションを許可するように ABAC ポリシーを設計できます。

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ありです。サービスが一部のリソースタイプに対してのみ 3 つの条件キーのすべてをサポートする場合、値は「部分的」になります。

ABAC の詳細については、「IAM ユーザーガイド」の「ABAC 認可でアクセス許可を定義する」を参照してください。ABAC をセットアップする手順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「属性ベースの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: なし

一時的な認証情報は、 AWS リソースへの短期的なアクセスを提供し、フェデレーションまたは切り替えロールを使用する場合に自動的に作成されます。 AWS では、長期的な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勧めします。詳細については、「IAM ユーザーガイド」の「IAM の一時的な認証情報」および「AWS のサービス と IAM との連携」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) のサポート: なし

転送アクセスセッション (FAS) は、 を呼び出すプリンシパルのアクセス許可と AWS のサービス、ダウンストリームサービス AWS のサービス へのリクエストをリクエストする を使用します。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: なし

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 のサービスに許可を委任するロールを作成する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: なし

サービスにリンクされたロールは、 にリンクされた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。サービスにリンクされたロールは に表示され AWS アカウント 、サービスによって所有されます。IAM 管理者は、サービスにリンクされたロールのアクセス許可を表示できますが、編集することはできません。

サービスにリンクされた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「サービスリンクロール」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。

JSON

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

このサンプルポリシーは、Wickr AWS マネジメントコンソール の を使用して Wickr ネットワークを一覧表示するアクセス許可をユーザーに付与します。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。

IAM ポリシーを作成して、ユーザーに特定の API アクションへのアクセスを許可することもできます。API アクションへのアクセスは、AWS Wickr コンソールとは別に管理されます。以下は、特定の API アクションへの読み取り専用アクセスを許可するポリシーの例です。API アクションの詳細については、「AWS Wickr API リファレンスへようこそ」を参照してください。

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

トピック

- ポリシーに関するベストプラクティス
- Wickr AWS マネジメントコンソール での の使用
- 自分の権限の表示をユーザーに許可する

ポリシーに関する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では、 AWS アカウントに費用が発生する場合があります。アイデンティティベース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 管理ポリシーを開始し、最小特権のアクセス許可に移行する – ユーザーとワークロードにアクセス許可の付与を開始するには、多くの一般的なユースケースにアクセス許可を付与するAWS 管理ポリシーを使用します。これらは で使用できます AWS アカウント。ユースケースに固有の

AWS カスタマー管理ポリシーを定義することで、アクセス許可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 ジョブ機能のAWS マネージドポリシー を参照してください。

- 最小特権を適用する – IAM ポリシーでアクセス許可を設定する場合は、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。たとえば、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。条件を使用して、サービスアクションが などの特定の を通じて使用されている場合に AWS のサービス、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 CloudFormation。詳細については、IAM ユーザーガイド の IAM JSON ポリシー要素:条件 を参照してください。
- IAM アクセスアナライザー 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 アクセスアナライザー 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 でポリシーを検証する を参照してください。
- 多要素認証 (MFA) を要求する – で IAM ユーザーまたはルート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、MFA をオンにしてセキュリティを強化します。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 を使用した安全な API アクセス 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。

Wickr AWS マネジメントコンソール での の使用

`AWSWickrFullAccess` AWS 管理ポリシーを IAM ID にアタッチして、 の Wickr 管理者コンソールを含む Wickr サービスへの完全な管理アクセス許可を付与します AWS マネジメントコンソール。詳細については、「AWS マネージドポリシー: AWSWickrFullAccess」を参照してください。

自分の権限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アタッチ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の作成方法を示します。このポリシーには、コンソールで、または AWS CLI または AWS API を使用してプログラムでこのアクションを実行するアクセス許可が含まれています。

```
{
    "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

- Wickr AWS マネジメントコンソール の で管理アクションを実行する権限がありません

Wickr AWS マネジメントコンソール の で管理アクションを実行する権限がありません

アクションを実行する権限がないと for AWS マネジメントコンソール Wickr から通知された場合は、管理者に連絡してサポートを依頼する必要があります。管理者とは、サインイン認証情報を提供した担当者です。

次の例のエラーは、IAM `mateojackson` ユーザーが for Wickr を使用して AWS マネジメントコンソール for Wickr で Wickr AWS マネジメントコンソール ネットワークを作成、管理、または表示しようとしても、 `wickr:CreateAdminSession` および アクセス`wickr:ListNetworks`許可がない場合に発生します。

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

この場合、Mateo は管理者にポリシーを更新して、 アクション`wickr:CreateAdminSession`と`wickr:ListNetworks`アクションを使用して Wickr AWS マネジメントコンソール の にアクセスすることを許可するよう依頼します。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 マネージドポリシー: AWSWickrFullAccess」を参照してください。

コンプライアンス検証

特定のコンプライアンスプログラムの対象となる AWS サービスのリストについては、「コンプライアンスAWS プログラムによる対象範囲内のサービスコンプライアンス」を参照してください。一般的な情報については、AWS 「 Compliance ProgramsAssurance」を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細については、「Downloading Reports in AWS Artifact」を参照してください。

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 – これらのデプロイガイドでは、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デプロイする手順について説明します AWS。
- AWS コンプライアンスリソース – このワークブックとガイドのコレクションは、お客様の業界や地域に適用される場合があります。
- 「 デベロッパーガイド」の「ルールによるリソースの評価」 – AWS Configでは、リソース設定が内部プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価します。 AWS Config
- AWS Security Hub CSPM – この AWS サービスは、 内のセキュリティ状態を包括的に把握 AWS し、セキュリティ業界標準とベストプラクティスへの準拠を確認するのに役立ちます。

AWS Wickr の耐障害性

AWS グローバルインフラストラクチャは、 AWS リージョン およびアベイラビリティーゾーンを中心に構築されています。 は、低レイテンシー、高スループット、高度に冗長なネットワークで接続された、物理的に分離および分離された複数のアベイラビリティーゾーン AWS リージョン を提供します。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ー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、フォールトトレランス、および拡張性が優れています。

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、AWS 「 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 グローバルインフラストラクチャに加えて、Wickr はデータの耐障害性とバックアップのニーズをサポートするのに役立ついくつかの機能を提供しています。詳細については、「AWS Wickr のデータ保持」を参照してください。

AWS PrivateLink AWS Wickr の

AWS PrivateLink for AWS Wickr を使用すると、インターフェイス VPC エンドポイントを使用して、仮想プライベートクラウド (VPC) と AWS Wickr のエンドポイントのサブセットとの間にプライベート接続を確立できます。インターフェイス VPC エンドポイントは AWS PrivateLink、プライ

ベート IP アドレス AWS を使用して で実行されているサービスにアクセスするために使用できる AWS テクノロジーである を利用しています。

モバイルクライアントやその他のオンプレミスデバイスの場合は、VPN を使用してデバイスを VPC に接続し、エンドツーエンドのプライベート接続を行います。詳細については、AWS Virtual Private Network ドキュメント を参照してください。

AWS PrivateLink と AWS VPC の詳細については、「 AWS PrivateLink ガイド」の「What is AWS PrivateLink?」と「Amazon Virtual Private Cloud ユーザーガイド」の「What is AWS VPC?」を参照してください。 Amazon Virtual Private Cloud

サポートされている AWS Wickr サービス

次の AWS Wickr サービスがサポートしています AWS PrivateLink。

サービス	エンドポイント形式
AWS Wickr 管理者	`com.amazonaws.` *`your-region`* `.wickr-admin`
AWS Wickr メッセージング	`com.amazonaws.` *`your-region`* `.wickr-messaging`
AWS Wickr 呼び出し	`com.amazonaws.` *`your-region`* `.wickr-calling`

現在、すべての Wickr VPC エンドポイントでは、プライベート DNS 名を有効にする必要があります。詳細については、「プライベート DNS 名を有効にする」を参照してください。

Wickr VPC エンドポイントは、パブリック Wickr エンドポイントが FIPS をサポートするリージョンで FIPS をサポートします。詳細については、「連邦情報処理規格」を参照してください。

現在サポートされていません

- メッセージングエンドポイントと呼び出しエンドポイントの VPC エンドポイントポリシー
- メッセージングエンドポイントと呼び出しエンドポイントは、 では使用できませんus-east-1。

トピック

前提条件

VPC エンドポイントを作成する前に、次の前提条件があることを確認してください。

1. VPC 設定: 複数のアベイラビリティーゾーンにサブネットを持つ適切に設定された VPC
2. セキュリティグループ: HTTPS トラフィックを許可する適切なセキュリティグループ (ポート 443)
3. DNS 解決: VPC で有効になっている DNS ホスト名と DNS 解決
4. IAM アクセス許可: VPC エンドポイントを作成および管理するために必要なアクセス許可

VPC エンドポイントの作成

AWS Wickr 管理者、メッセージング、呼び出し用の VPC エンドポイントを作成できます。

コンソールを使用して AWS VPC エンドポイントを作成するには、次の手順を実行します。

ステップ 1: VPC コンソールに移動する

1. Amazon VPC コンソールにサインインします。
2. 左のナビゲーションペインで [エンドポイント] を選択してください。
3. エンドポイントの作成 を選択します。

ステップ 2: エンドポイント設定を構成する

1. サービスカテゴリで、AWS サービスを選択します。
2. サービス名 で、適切なサービスを検索wickrして選択します。
    - 管理者の場合: `com.amazonaws.`*`your-region`*`.wickr-admin`
    - メッセージングの場合: `com.amazonaws.`*`your-region`*`.wickr-messaging`
    - 呼び出しの場合: `com.amazonaws.`*`your-region`*`.wickr-calling`

ステップ 3: ネットワーク設定

1. VPC で、ターゲット VPC を選択します。
2. サブネットで、高可用性を実現するために複数のアベイラビリティーゾーンのサブネットを選択します。
3. プライベート DNS 名を有効にする で、チェックボックスをオンにします。これにより、プライベート DNS 名がサポートされます。
4. セキュリティグループで、エンドポイントネットワークインターフェイスに関連付けるセキュリティグループを選択または作成します。

ステップ 4: エンドポイントを作成する

1. の設定を確認します。
2. オプションで、タグを追加または削除できます。タグとは名前と値のペアで、エンドポイントに関連付けるために使用します。
3. エンドポイントの作成 を選択します。

を使用して VPC エンドポイントを作成するには、次の手順を実行します AWS CLI。

1. リージョンでのサービスの可用性を確認します。

   Wickr 管理者の可用性を確認する

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

   Wickr Messaging の可用性を確認する

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

   Wickr Calling の可用性を確認する

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

2. VPC エンドポイントを作成します。

   Wickr 管理エンドポイント:

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

Wickr メッセージングエンドポイント

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

Wickr 呼び出しエンドポイント

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

制限事項

以下の機能は ではサポートされていない AWS PrivateLink ため、インターネット接続が必要です。

- Wickr Open Access (WOA)
- クライアントアプリケーションの更新
  - モバイルアプリ (iOS/Android)

    - ソース: App Store/Google Play Store
    - 要件: インターネットアクセスが必要
  - デスクトップアプリケーション
    - Windows/Mac: グローバル S3 エンドポイントを使用する (AWS PrivateLink 互換性なし)
    - Linux: Snap Store を使用する (インターネットアクセスが必要)
- デバッグとテレメトリ
  - クラッシュレポート
  - デバッグメトリクス
  - クライアント側の分析リンク
- モバイルプッシュ通知

  これらのサービスにはインターネット接続が必要であり、 を使用することはできません AWS PrivateLink。

  - Apple プッシュ通知
    - 要件: 直接インターネットアクセス
    - ポート: 443、2195、2196、5223
    - リファレンス: Apple サポートドキュメント
  - Google/Android 通知
    - 要件: Firebase Cloud Messaging アクセス
    - リファレンス: Firebase ドキュメント
- AWS Wickr コンソールは現在、プライベートアクセスではサポートされていません。詳細については、「 プライベートアクセスのサポート対象 AWS リージョン、サービスコンソール、および機能」を参照してください。

に必要な最小クライアントバージョン AWS PrivateLink

次のクライアントバージョンは で検証されています AWS PrivateLink。

- iOS 6.64 (該当する場合)
- Android 6.60 (該当する場合)
- デスクトップクライアント 6.60
- ボット 6.60

追加設定が必要な機能

Wickr ボット

- 要件: カスタマーマネージドインフラストラクチャ
- アクション: ボットの依存関係のネットワークパスを設定する
- 考慮事項: ボットが VPC エンドポイントを介して必要な AWS サービスにアクセスできることを確認する

ファイルのダウンロード

- S3 接続: ファイルオペレーションに必要です (フランクフルトリージョンを除く)
- 解決策: S3 VPC ゲートウェイエンドポイントを作成する
- リファレンス: AWS PrivateLink for Amazon S3

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、ホワイトペーパー「Amazon Web Services: セキュリティプロセスの概要」に記載されている AWS グローバルネットワークセキュリティ手順で保護されています。

AWS Wickr での設定と脆弱性の分析

設定と IT コントロールは、 AWS とお客様の間の責任共有です。詳細については、 AWS 「 責任共有モデル」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

お客様の環境に適切ではないか、十分ではない場合があるため、これらは指示ではなく、有用な考慮事項と見なしてください。

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 マネジメントコンソール を最初に認証して、 AWS マネジメントコンソール for Wickr にアクセスします。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 およびその他の AWS 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。 には、Wickr をモニタリングし、問題が発生したときに報告し、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 AWS が用意されています。

- AWS CloudTrail は、 AWS アカウントによって、またはアカウントに代わって行われた API コールおよび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。呼び出し元のユーザーとアカウント AWS、呼び出し元の送信元 IP アドレス、呼び出しの発生日時を特定できます。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。CloudTrail を使用した Wickr API 呼び出しのログ記録の詳細については、「 を使用した AWS Wickr API コールのログ記録 AWS CloudTrail」を参照してください。

を使用した AWS Wickr API コールのログ記録 AWS CloudTrail

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。CloudTrailはWickrのすべてのAPI コールをイベントとしてキャプチャします。キャプチャされた呼び出しには、Wickr AWS マネジメントコンソール の からの呼び出しと、Wickr API オペレーションへのコード呼び出しが含まれます。トレイルを作成すると、CloudTrailイベントをAmazon S3バケットに継続的に配信できるようになります。追跡を設定しない場合でも、CloudTrail コンソールの Event history (イベント履歴) で最新のイベントを表示できます。CloudTrailによって収集された情報を使用することで、Wickrに対して行われたリクエスト、リクエストが行われたIPアドレス、リクエストを行った人、リクエストが行われた日時、その他の詳細を特定することができます。CloudTrail の詳細については、「AWS CloudTrail ユーザーガイド」を参照してください。

CloudTrailのWickr情報

CloudTrail は、アカウントの作成 AWS アカウント 時に 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イベント履歴の他の AWS サービスイベントとともに CloudTrail 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、 CloudTrail イベント履歴でのイベントの表示を参照してください。

Wickr のイベントなど AWS アカウント、 のイベントの継続的な記録については、証跡を作成します。証跡により、CloudTrail はログファイルを 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 パーティション内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 ログで収集したイベントデータをより詳細に分析し、それに基づいて対応するため、他の AWS サービスを構成できます。詳細については、次を参照してください:

- 追跡を作成するための概要
- CloudTrail がサポートされているサービスと統合
- 「CloudTrail の Amazon SNS 通知の設定」
- 「複数のリージョンから CloudTrail ログファイルを受け取る」および「複数のアカウントから CloudTrail ログファイルを受け取る」

WickrのすべてのアクションはCloudTrailによって記録されます。例えば、`CreateAdminSession` と `ListNetworks` の各アクションを呼び出すと、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、以下を判別するのに役立ちます。

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか。
- 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 サービスによって行われたかどうか。

詳細については、「CloudTrail userIdentity エレメント」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。

「トレイル」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するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは、任意の出典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。

以下の例は、`CreateAdminSession` アクションを示す CloudTrail ログエントリです。

```
{
    "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"
}
```

以下の例は、CreateNetwork アクションを示す CloudTrail ログエントリです。

```
{
    "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"
}
```

以下の例は、ListNetworks アクションを示す CloudTrail ログエントリです。

```
{
    "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"
}
```

以下の例は、UpdateNetworkdetails アクションを示す CloudTrail ログエントリです。

```
{
    "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"
}
```

以下の例は、TagResource アクションを示す CloudTrail ログエントリです。

```
{
    "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"
}
```

以下の例は、ListTagsForResource アクションを示す CloudTrail ログエントリです。

```
{
    "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"
}
```

AWS Wickr の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 をどのように活用しているかを確認できます。次の手順では、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. Wickr AWS マネジメントコンソール の を https://console.aws.amazon.com/wickr/ で開きます。
2. ネットワークページで、ネットワーク名を選択してそのネットワークに移動します。
3. ナビゲーションペインで、[Analytics] を選択します。

   分析ページには、ネットワークのメトリクスがさまざまなタブに表示されます。

分析ページには、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、各タブの右上隅で、使用可能なエクスポートオプションを選択して、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**
>
> 選択した時刻は UTC (協定世界時) です。

以下のタブが利用可能です。

- 概要には以下が表示されます。
  - 登録済み — 選択した時間内のネットワーク上のアクティブユーザーと停止ユーザーを含む、登録済みユーザーの総数。保留中または招待されたユーザーは含まれません。
  - 保留中 — 選択した時間内のネットワーク上の保留中ユーザーの総数。
  - 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になっているデバイスの数。
  - クライアントバージョン — クライアントバージョンによって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 — 選択した期間内にネットワーク上のアクティブなユーザー。
  - アクティブなユーザー —
    - グラフには、時間の経過に伴うアクティブなユーザーの数が表示され、日単位、週単位、または月単位 (上記の選択した時間範囲内) で集計できます。
    - アクティブなユーザー数は、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別に分類できます。セキュリティグループが削除された場合、合計数は Deleted# と表示されます。

- メッセージは以下を表示します。
  - 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によって送信された一意のメッセージの数。
  - 呼び出し — ネットワーク内のすべてのユーザーが行った一意の呼び出しの数。
  - 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 (音声メモを含む) 。
  - 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によって分類されたアクティブなデバイスの数。

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
ファイルプレビューが利用可能になりました	Wickr 管理者は、ファイルのダウンロードを有効または無効にできるようになりました。詳細については、「AWS Wickr のファイルプレビュー」を参照してください。	2025 年 5 月 29 日
新しく再設計された Wickr 管理者コンソールが利用可能になりました	Wickr は、Wickr 管理者コンソールを拡張して、管理者のナビゲーションとアクセシビリティを向上させました。	2025 年 3 月 13 日
Wickr がアジアパシフィック (マレーシア) で利用可能になりました AWS リージョン	Wickr がアジアパシフィック (マレーシア) で利用可能になりました AWS リージョン。詳細については、「リージョナルな可用性」を参照してください。	2024 年 11 月 20 日
削除ネットワークが利用可能になりました	Wickr 管理者は、AWS Wickr ネットワークを削除できるようになりました。詳細については、「AWS Wickr でネットワークを削除する」を参照してください。	2024 年 10 月 4 日
Microsoft Entra (Azure AD) SSO を使用した AWS Wickr の設定が利用可能になりました	AWS Wickr は、Microsoft Entra (Azure AD) を ID プロバイダーとして使用するように設定できます。詳細については、「Configure AWS Wickr	2024 年 9 月 18 日

	with Microsoft Entra (Azure AD) single sign-on」を参照してください。	
Wickr が欧州 (チューリッヒ) で利用可能に AWS リージョン	Wickr が欧州 (チューリッヒ) で利用可能になりました AWS リージョン。詳細については、「リージョナルな可用性」を参照してください。	2024 年 8 月 12 日
クロス境界分類とフェデレーションが利用可能になりました	クロス境界分類機能を使用すると、GovCloud ユーザーの会話に対するユーザーインターフェイスの変更が可能になります。詳細については、GovCloud クロス境界分類とフェデレーション」を参照してください。	2024 年 6 月 25 日
読み取り受信機能が使用可能になりました	Wickr 管理者は、管理者コンソールで読み取り受信機能を有効または無効にできるようになりました。詳細については、「受信の読み取り」を参照してください。	2024 年 4 月 23 日

グローバルフェデレーションで制限付きフェデレーションがサポートされ、管理者は管理者コンソールで使用状況分析を表示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表示できるようになりました。詳細については、「分析ダッシュボード」を参照してください。	2024 年 3 月 28 日
AWS Wickr の Premium 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 人のユーザーに対して 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。ゲストユーザー機能は、プレミアム無料トライアル中は利用できません。詳細については、「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が一般公開され、より多くの管理者コントロールが追加されました。	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 が欧州 (フランクフルト) で利用可能に AWS リージョン	Wickr が欧州 (フランクフルト) で利用可能になりました AWS リージョン。詳細については、「リージョナルな可用性」を参照してください。	2023 年 10 月 26 日
Wickr ネットワークが 間でフェデレーション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 が欧州 (ロンドン) で利用可能になりました AWS リージョン	Wickr が欧州 (ロンドン) で利用可能になりました AWS リージョン。詳細については、「リージョナルな可用性」を参照してください。	2023 年 8 月 23 日
Wickr がカナダ (中部) で利用可能になりました AWS リージョン	Wickr がカナダ (中部) で利用可能になりました AWS リージョン。詳細については、「リージョナルな可用性」を参照してください。	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 が と統合され AWS CloudTrail、WickrGov として AWS GovCloud (米国西部) で利用可能になりました	AWS Wickr が と統合されました AWS CloudTrail。詳細については、「AWS CloudTrail を使用した AWS Wickr API 呼び出しの口グ記録」を参照してください。さらに、Wickr は WickrGov として AWS GovCloud (米国西部) で利用できます。詳細については、AWS GovCloud (US) ユーザーガイド の「AWS WickrGov」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。詳細については、「ネットワークタグ」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。

2025 年 8 月

- AWS Wickr と AWS WickrGov の E メールテンプレートが更新され、ユーザーのオンボーディングエクスペリエンスが向上しました。送信者の E メールアドレスが から donotreply@wickr.emailに変更されましたno-reply@amazonaws.com。

2025 年 5 月

- ファイルプレビューが利用可能になりました。セキュリティグループの管理者コンソールで管理者によってファイルのダウンロードが無効になっている場合、ユーザーはメッセージングタブとファイルタブでのみサポートされているファイルのリストを表示できます。

2025 年 3 月

- 再設計された Wickr 管理者コンソールが利用可能になりました。

2024 年 10 月

- Wickr がネットワークの削除をサポートするようになりました。詳細については、「AWS Wickr でネットワークを削除する」を参照してください。

2024 年 9 月

- 管理者は、Microsoft Entra (Azure AD) シングルサインオンで AWS Wickr を設定できるようになりました。詳細については、「Configure AWS Wickr with Microsoft Entra (Azure AD) single sign-on」を参照してください。

2024 年 8 月

- 機能強化
  - Wickr が欧州 (チューリッヒ) で利用可能になりました AWS リージョン。

2024 年 6 月

- GovCloud ユーザーがクロス境界分類とフェデレーションを使用できるようになりました。詳細については、GovCloud クロス境界分類とフェデレーション」を参照してください。

2024 年 4 月

- Wickr が読み取り受信をサポートするようになりました。詳細については、「受信の読み取り」を参照してください。

2024 年 3 月

- 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。ここで、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で追加された選択したネットワークでのみ有効にできます。これは、他の Wickr ネットワークで機能します 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、 管理者コンソールの Analytics ダッシュボードで使用状況分析を表示できるようになりました。詳細については、「分析ダッシュボード」を参照してください。

2024 年 2 月

- AWS Wickr では、最大 30 人のユーザーに Premium プランの 3 か月間の無料トライアルが提供されるようになりました。変更と制限には以下が含まれます。
  - 無制限の管理コントロールやデータ保持など、すべての Standard および Premium プラン機能が Premium 無料トライアルで利用可能になりました。ゲストユーザー機能は、プレミアム無料トライアル中は利用できません。
  - 以前の無料トライアルは利用できなくなりました。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、「AWS Wickr ネットワークのゲストユーザー」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、「を使用した AWS Wickr API コールのログ記録 AWS CloudTrail」を参照してください。
- Wickr が WickrGov AWS として GovCloud (米国西部) で利用可能になりました。詳細については、AWS GovCloud (US) ユーザーガイド の「AWS WickrGov」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、「AWS Wickr のネットワークタグ」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。