Administratorhandbuch

AWS Wickr

AWS Wickr: Administratorhandbuch

Table of Contents

Was ist AWS Wickr?

AWS Wickr ist ein end-to-end verschlüsselter Service, der Organisationen und Regierungsbehörden dabei hilft, sicher über one-to-one Gruppennachrichten, Sprach- und Videoanrufe, Dateifreigabe, Bildschirmübertragung und mehr zu kommunizieren. Wickr kann Kunden dabei helfen, Datenaufbewahrungspflichten im Zusammenhang mit Messaging-Apps für Privatanwender zu erfüllen und die Zusammenarbeit auf sichere Weise zu erleichtern. Fortschrittliche Sicherheits- und Verwaltungskontrollen helfen Unternehmen dabei, gesetzliche und behördliche Anforderungen zu erfüllen und maßgeschneiderte Lösungen für Herausforderungen im Bereich der Datensicherheit zu entwickeln.

Informationen können zu Aufbewahrungs- und Prüfzwecken in einem privaten, vom Kunden kontrollierten Datenspeicher protokolliert werden. Benutzer haben umfassende administrative Kontrolle über Daten. Dazu gehören das Festlegen von Berechtigungen, das Konfigurieren kurzlebiger Nachrichtenoptionen und das Definieren von Sicherheitsgruppen. Wickr lässt sich in zusätzliche Dienste wie Active Directory (AD), Single Sign-On (SSO) mit OpenID Connect (OIDC) und mehr integrieren. Über die können Sie schnell ein Wickr-Netzwerk erstellen und verwalten und Workflows mithilfe von AWS-Managementkonsole Wickr-Bots sicher automatisieren. Um zu beginnen, sehen Sie sich Einrichtung für AWS Wickr an.

Topics

Funktionen von Wickr

Verbesserte Sicherheit und Datenschutz

Wickr verwendet für jede Funktion die 256-Bit-AES-Verschlüsselung (Advanced end-to-end Encryption Standard). Die Kommunikation wird lokal auf den Benutzergeräten verschlüsselt und bleibt bei der Übertragung an andere Personen als Absender und Empfänger nicht entzifferbar. Jede Nachricht, jeder Anruf und jede Datei wird mit einem neuen zufälligen Schlüssel verschlüsselt,

und niemand außer den vorgesehenen Empfängern (auch nicht AWS) kann sie entschlüsseln. Ganz gleich, ob sie sensible und regulierte Daten teilen, Rechts- oder Personalfragen besprechen oder sogar taktische militärische Operationen durchführen — Kunden nutzen Wickr, um zu kommunizieren, wenn Sicherheit und Datenschutz an erster Stelle stehen.

Datenaufbewahrung

Flexible Verwaltungsfunktionen dienen nicht nur dem Schutz sensibler Informationen, sondern auch der Aufbewahrung von Daten, soweit dies für Compliance-Verpflichtungen, gesetzliche Aufbewahrungsfristen und Prüfungszwecke erforderlich ist. Nachrichten und Dateien können in einem sicheren, vom Kunden kontrollierten Datenspeicher archiviert werden.

Flexibler Zugriff

Benutzer haben Zugriff auf mehrere Geräte (Mobil, Desktop) und können in Umgebungen mit geringer Bandbreite arbeiten, einschließlich Verbindungsabbrüchen und Kommunikation. out-of-band

Administrative Kontrollen

Benutzer haben umfassende administrative Kontrolle über Daten. Dazu gehören das Festlegen von Berechtigungen, das Konfigurieren von Optionen für verantwortungsbewusstes kurzlebiges Messaging und das Definieren von Sicherheitsgruppen.

Leistungsstarke Integrationen und Bots

Wickr lässt sich in zusätzliche Dienste wie Active Directory, Single Sign-On (SSO) mit OpenID Connect (OIDC) und mehr integrieren. Kunden können damit schnell ein Wickr-Netzwerk erstellen und verwalten und Workflows mit Wickr AWS-Managementkonsole Bots sicher automatisieren.

Im Folgenden finden Sie eine Aufschlüsselung der Kooperationsangebote von Wickr:

- Einzel- und Gruppennachrichten: Chatten Sie sicher mit Ihrem Team in Räumen mit bis zu 500 Mitgliedern
- Audio- und Videoanrufe: Halten Sie Telefonkonferenzen mit bis zu 70 Personen ab
- Bildschirmübertragung und Übertragung: Präsentieren Sie mit bis zu 500 Teilnehmern
- Dateien teilen und speichern: Übertragen Sie bis zu 5 Dateien GBs mit unbegrenztem Speicherplatz
- Kurzlebig: Kontrolliere den Ablauf und die Timer burn-on-read
- Globaler Verband: Connect zu Wickr-Benutzern außerhalb Ihres Netzwerks her

Regionale Verfügbarkeit

Wickr ist in den Ländern USA Ost (Nord-Virginia), Asien-Pazifik (Malaysia), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Asien-Pazifik (Tokio), Kanada (Zentral), Europa (Frankfurt), Europa (London), Europa (Stockholm) und Europa (Zürich) AWS-Regionen erhältlich. Wickr ist auch in der Region AWS GovCloud (USA-West) verfügbar. Jede Region enthält mehrere Availability Zones, die physisch getrennt sind, aber über private, redundante Netzwerkverbindungen mit niedriger Latenz und hoher Bandbreite miteinander verbunden sind. Diese Availability Zones werden verwendet, um eine verbesserte Verfügbarkeit, Fehlertoleranz und minimierte Latenz zu gewährleisten.

Weitere Informationen dazu finden Sie unter Geben Sie an AWS-Regionen, was AWS-Regionen Ihr Konto verwenden kann in der. Allgemeine AWS-Referenz Weitere Informationen zur Anzahl der in jeder Region verfügbaren Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zugreifen auf Wickr

Administratoren greifen auf das AWS-Managementkonsole für Wickr unter zu. https://console.aws.amazon.com/wickr/ Bevor Sie mit der Verwendung von Wickr beginnen, sollten Sie die Anleitungen Einrichtung für AWS Wickr undErste Schritte mit AWS Wickr.

Endbenutzer greifen über den Wickr-Client auf Wickr zu. Weitere Informationen finden Sie im AWS Wickr-Benutzerhandbuch.

Preisgestaltung

Wickr ist in verschiedenen Tarifen für Einzelpersonen, kleine Teams und große Unternehmen erhältlich. Weitere Informationen finden Sie unter AWS Wickr — Preise.

Wickr-Dokumentation für Endbenutzer

Wenn Sie ein Endbenutzer des Wickr-Clients sind und auf dessen Dokumentation zugreifen müssen, finden Sie weitere Informationen im AWS Wickr-Benutzerhandbuch.

Einrichtung für AWS Wickr

Melden Sie sich für einen an AWS-Konto

Um loszulegen AWS, benötigen Sie eine AWS-Konto. Informationen zum Erstellen eines AWS-Konto finden Sie unter Erste Schritte mit einem AWS-Konto im AWS -Kontenverwaltung Referenzhandbuch.

Was kommt als Nächstes

Sie haben die erforderlichen Schritte zur Einrichtung abgeschlossen. Informationen zum Konfigurieren von Wickr finden Sie unterErste Schritte.

Erste Schritte mit AWS Wickr

In diesem Handbuch zeigen wir Ihnen, wie Sie mit Wickr beginnen können, indem Sie ein Netzwerk erstellen, Ihr Netzwerk konfigurieren und Benutzer erstellen.

Topics

Voraussetzungen

Bevor Sie beginnen, stellen Sie sicher, dass Sie die folgenden Voraussetzungen erfüllen, falls Sie dies noch nicht getan haben:

- Melden Sie sich für Amazon Web Services an (AWS). Weitere Informationen finden Sie unter Einrichtung für AWS Wickr.
- Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen verfügen, um Wickr zu verwalten. Weitere Informationen finden Sie unter AWSverwaltete Richtlinie: AWSWickrFullAccess.
- Stellen Sie sicher, dass Sie die entsprechenden Ports und Domänen für Wickr zulassen. Weitere Informationen finden Sie unter Liste der zugelassenen Ports und Domänen für Ihr Wickr-Netzwerk.

Schritt 1: Erstellen Sie ein Netzwerk

Sie können ein Wickr-Netzwerk erstellen.

Gehen Sie wie folgt vor, um ein Wickr-Netzwerk für Ihr Konto zu erstellen.

1. Öffnen Sie das AWS-Managementkonsole für Wickr unter. https://console.aws.amazon.com/wickr/

   > **Note**
   >
   > Wenn Sie noch kein Wickr-Netzwerk erstellt haben, wird die Informationsseite für den Wickr-Dienst angezeigt. Nachdem Sie ein oder mehrere Wickr-Netzwerke erstellt haben,

wird die Netzwerkseite angezeigt, die eine Listenansicht aller von Ihnen erstellten Wickr-Netzwerke enthält.

2. Wählen Sie Create a network (Netzwerk erstellen).
3. Geben Sie im Textfeld Netzwerkname einen Namen für Ihr Netzwerk ein. Wählen Sie einen Namen, den die Mitglieder Ihrer Organisation wiedererkennen, z. B. den Namen Ihres Unternehmens oder den Namen Ihres Teams.
4. Wählen Sie einen Plan. Sie können einen der folgenden Wickr-Netzwerkpläne wählen:

   - Standard — Für kleine und große Unternehmensteams, die administrative Kontrollen und Flexibilität benötigen.
   - Premium - oder kostenlose Premium-Testversion — Für Unternehmen, die höchste Funktionseinschränkungen, detaillierte Verwaltungskontrollen und Datenspeicherung benötigen.

   Administratoren haben die Möglichkeit, eine kostenlose Premium-Testversion auszuwählen, die für bis zu 30 Benutzer verfügbar ist und drei Monate gültig ist. Denn AWS WickrGov die kostenlose Premium-Testoption ermöglicht bis zu 50 Benutzer und ist ebenfalls drei Monate gültig. Während der kostenlosen Premium-Testphase können Administratoren ein Upgrade oder Downgrade auf Premium- oder Standard-Tarife durchführen.

   Weitere Informationen zu den verfügbaren Wickr-Plänen und Preisen finden Sie auf der Wickr-Preisseite.
5. (Optional) Wählen Sie Neues Tag hinzufügen, um Ihrem Netzwerk ein Tag hinzuzufügen. Tags bestehen aus einem Schlüssel-Wert-Paar. Tags können verwendet werden, um Ressourcen zu suchen und zu filtern oder Ihre AWS Kosten zu verfolgen. Weitere Informationen finden Sie unter Netzwerk-Tags.
6. Wählen Sie „Netzwerk erstellen“.

   Sie werden auf die Netzwerkseite von AWS-Managementkonsole for Wickr weitergeleitet, und das neue Netzwerk wird auf der Seite aufgeführt.

Schritt 2: Konfigurieren Sie Ihr Netzwerk

Gehen Sie wie folgt vor, um auf AWS-Managementkonsole for Wickr zuzugreifen. Hier können Sie Benutzer hinzufügen, Sicherheitsgruppen hinzufügen, SSO konfigurieren, die Datenspeicherung konfigurieren und zusätzliche Netzwerkeinstellungen einrichten.

1. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.

   Sie werden zur Wickr Admin Console für das ausgewählte Netzwerk weitergeleitet.
2. Die folgenden Benutzerverwaltungsoptionen sind verfügbar. Weitere Informationen zum Konfigurieren dieser Einstellungen finden Sie unter Verwalten Sie Ihr AWS Wickr-Netzwerk.

   - Sicherheitsgruppe — Verwalten Sie Sicherheitsgruppen und ihre Einstellungen, z. B. Richtlinien zur Kennwortkomplexität, Nachrichteneinstellungen, Anruffunktionen, Sicherheitsfunktionen und externen Verbund. Weitere Informationen finden Sie unter Sicherheitsgruppen für AWS Wickr.
   - Konfiguration von Single Sign-On (SSO) — Konfigurieren Sie SSO und sehen Sie sich die Endpunktadresse für Ihr Wickr-Netzwerk an. Wickr unterstützt SSO-Anbieter, die nur OpenID Connect (OIDC) verwenden. Anbieter, die Security Assertion Markup Language (SAML) verwenden, werden nicht unterstützt. Weitere Informationen finden Sie unter Single Sign-On-Konfiguration für AWS Wickr.

Schritt 3: Benutzer erstellen und einladen

Sie können Benutzer in Ihrem Wickr-Netzwerk mit den folgenden Methoden erstellen:

- Single Sign-On — Wenn Sie SSO konfigurieren, können Sie Benutzer einladen, indem Sie Ihre Wickr-Unternehmens-ID teilen. Endbenutzer registrieren sich mit der angegebenen Firmen-ID und ihrer geschäftlichen E-Mail-Adresse für Wickr. Weitere Informationen finden Sie unter Single Sign-On-Konfiguration für AWS Wickr.
- Einladung — Sie können Benutzer in The AWS-Managementkonsole for Wickr manuell erstellen und sich eine E-Mail-Einladung zusenden lassen. Endbenutzer können sich für Wickr registrieren, indem sie den Link in der E-Mail auswählen.

> **Note**
>
> Sie können auch Gastbenutzer für Ihr Wickr-Netzwerk aktivieren. Weitere Informationen finden Sie unter Gastbenutzer im AWS Wickr-Netzwerk.

Gehen Sie wie folgt vor, um Benutzer zu erstellen oder einzuladen.

> **Note**
>
> Administratoren gelten ebenfalls als Benutzer und müssen sich selbst zu Wickr-Netzwerken mit SSO oder ohne SSO einladen.

Um Wickr-Benutzer zu erstellen und Einladungen mit SSO zu versenden:

Schreiben und senden Sie eine E-Mail an die SSO-Benutzer, die sich für Wickr registrieren sollen. Nehmen Sie die folgenden Informationen in Ihre E-Mail auf:

- Ihre Wickr-Firmen-ID. Sie geben eine Unternehmens-ID für Ihr Wickr-Netzwerk an, wenn Sie SSO konfigurieren. Weitere Informationen finden Sie unter SSO in AWS Wickr konfigurieren.
- Die E-Mail-Adresse, die sie für die Anmeldung verwenden sollten.
- Die URL zum Herunterladen des Wickr-Clients. Benutzer können die Wickr-Clients von der AWS Wickr-Downloadseite unter https://aws.amazon.com/wickr/ download/ herunterladen.

  > **Note**
  >
  > Wenn Sie Ihr Wickr-Netzwerk in AWS GovCloud (US-West) erstellt haben, weisen Sie Ihre Benutzer an, den Client herunterzuladen und zu installieren. WickrGov Weisen Sie Ihre Benutzer für alle anderen AWS Regionen an, den Standard-Wickr-Client herunterzuladen und zu installieren. Weitere Informationen zu AWS WickrGov finden Sie AWS WickrGovim AWS GovCloud (US) Benutzerhandbuch.

Wenn sich Benutzer für Ihr Wickr-Netzwerk registrieren, werden sie dem Wickr-Teamverzeichnis mit dem Status Aktiv hinzugefügt.

Um Wickr-Benutzer manuell zu erstellen und Einladungen zu versenden:

1. Öffnen Sie sie AWS-Managementkonsole für Wickr unter. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.

   Sie werden zum Wickr-Netzwerk weitergeleitet. Im Wickr-Netzwerk können Sie Benutzer hinzufügen, Sicherheitsgruppen hinzufügen, SSO konfigurieren, die Datenspeicherung konfigurieren und zusätzliche Einstellungen anpassen.
3. Wählen Sie im Navigationsbereich Benutzerverwaltung aus.
4. Wählen Sie auf der Seite Benutzerverwaltung unter der Registerkarte Teamverzeichnis die Option Benutzer einladen aus.

   Sie können auch mehrere Benutzer gleichzeitig einladen, indem Sie den Dropdown-Pfeil neben Benutzer einladen auswählen. Wählen Sie auf der Seite „Benutzer gleichzeitig einladen“ die Option Vorlage herunterladen aus, um eine CSV-Vorlage herunterzuladen, die Sie bearbeiten und zusammen mit Ihrer Benutzerliste hochladen können.
5. Geben Sie den Vornamen, Nachnamen, die Landesvorwahl, die Telefonnummer und die E-Mail-Adresse des Benutzers ein. Die E-Mail-Adresse ist das einzige Feld, das erforderlich ist. Achten Sie darauf, die passende Sicherheitsgruppe für den Benutzer auszuwählen.
6. Klicken Sie auf Einladen.

   Wickr sendet eine Einladungs-E-Mail an die Adresse, die Sie für den Benutzer angegeben haben. Die E-Mail enthält Download-Links für die Wickr-Client-Anwendungen und einen Link zur Registrierung für Wickr. Weitere Informationen darüber, wie diese Endbenutzererfahrung aussieht, finden Sie im AWS Wickr-Benutzerhandbuch unter Wickr-App herunterladen und Ihre Einladung annehmen.

   Wenn sich Benutzer über den Link in der E-Mail für Wickr registrieren, ändert sich ihr Status im Wickr-Teamverzeichnis von Ausstehend auf Aktiv.

Nächste Schritte

Sie haben die Schritte „Erste Schritte“ abgeschlossen. Informationen zur Verwaltung von Wickr finden Sie im Folgenden:

- Verwalten Sie Ihr AWS Wickr-Netzwerk
- Benutzer in AWS Wickr verwalten

Verwalten Sie Ihr AWS Wickr-Netzwerk

In AWS-Managementkonsole for Wickr können Sie Ihren Wickr-Netzwerknamen, Ihre Sicherheitsgruppen, Ihre SSO-Konfiguration und Ihre Datenaufbewahrungseinstellungen verwalten.

Topics

Netzwerkdetails für AWS Wickr

Sie können den Namen Ihres Wickr-Netzwerks bearbeiten und Ihre Netzwerk-ID im Abschnitt Netzwerkdetails von AWS-Managementkonsole for Wickr einsehen.

Topics

Netzwerkdetails in AWS Wickr anzeigen

Sie können die Details Ihres Wickr-Netzwerks einsehen, einschließlich Ihres Netzwerknamens und Ihrer Netzwerk-ID.

Gehen Sie wie folgt vor, um Ihr Wickr-Netzwerkprofil und Ihre Netzwerk-ID anzuzeigen.

1. Öffnen Sie das AWS-Managementkonsole für Wickr unter. https://console.aws.amazon.com/wickr/
2. Suchen Sie auf der Seite Netzwerke das Netzwerk, das Sie sich ansehen möchten.
3. Wählen Sie auf der rechten Seite des Netzwerks, das Sie anzeigen möchten, das vertikale Ellipsensymbol (drei Punkte) und dann Details anzeigen aus.

   Auf der Netzwerk-Startseite werden Ihr Wickr-Netzwerkname und Ihre Netzwerk-ID im Abschnitt Netzwerkdetails angezeigt. Sie können die Netzwerk-ID verwenden, um den Verbund zu konfigurieren.

Netzwerknamen in AWS Wickr bearbeiten

Sie können den Namen Ihres Wickr-Netzwerks bearbeiten.

Gehen Sie wie folgt vor, um Ihren Wickr-Netzwerknamen zu bearbeiten.

1. Öffnen Sie den AWS-Managementkonsole für Wickr unter. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zur Wickr Admin Console für dieses Netzwerk zu navigieren.
3. Wählen Sie auf der Netzwerk-Startseite im Abschnitt Netzwerkdetails die Option Bearbeiten aus.
4. Geben Sie Ihren neuen Netzwerknamen in das Textfeld Netzwerkname ein.
5. Wählen Sie Speichern, um Ihren neuen Netzwerknamen zu speichern.

Netzwerk in AWS Wickr löschen

Sie können Ihr AWS Wickr-Netzwerk löschen.

> **Note**
>
> Wenn Sie ein kostenloses Premium-Testnetzwerk löschen, können Sie kein weiteres erstellen.

Gehen Sie wie folgt vor, um Ihr Wickr-Netzwerk auf der Networks-Startseite zu löschen.

1. Öffnen Sie das AWS-Managementkonsole für Wickr unter. https://console.aws.amazon.com/wickr/
2. Suchen Sie auf der Seite Netzwerke nach dem Netzwerk, das Sie löschen möchten.
3. Wählen Sie auf der rechten Seite des Netzwerks, das Sie löschen möchten, das vertikale Ellipsensymbol (drei Punkte) und dann Netzwerk löschen aus.
4. Geben Sie in das Popup-Fenster Bestätigen ein und wählen Sie dann Löschen.

   Es kann einige Minuten dauern, bis das Netzwerk gelöscht ist.

Gehen Sie wie folgt vor, um Ihr Wickr-Netzwerk zu löschen, während Sie sich im Netzwerk befinden.

1. Öffnen Sie das AWS-Managementkonsole für Wickr unter. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke das Netzwerk aus, das Sie löschen möchten.
3. Wählen Sie in der oberen rechten Ecke der Netzwerk-Startseite die Option Netzwerk löschen aus.
4. Geben Sie in das Popup-Fenster „Bestätigen“ ein und wählen Sie dann „Löschen“.

   Es kann einige Minuten dauern, bis das Netzwerk gelöscht ist.

> **Note**
>
> Daten, die in Ihrer Datenaufbewahrungskonfiguration gespeichert wurden (falls aktiviert), werden nicht gelöscht, wenn Sie Ihr Netzwerk löschen. Weitere Informationen finden Sie unter Datenspeicherung für AWS Wickr.

Sicherheitsgruppen für AWS Wickr

Im Bereich Sicherheitsgruppen von AWS-Managementkonsole for Wickr können Sie Sicherheitsgruppen und ihre Einstellungen verwalten, z. B. Richtlinien zur Kennwortkomplexität, Nachrichteneinstellungen, Anruffunktionen, Sicherheitsfunktionen und Netzwerkverbund.

Topics

- Bearbeiten Sie eine Sicherheitsgruppe in AWS Wickr
- Löschen Sie eine Sicherheitsgruppe in AWS Wickr

Sicherheitsgruppen in AWS Wickr anzeigen

Sie können die Details Ihrer Wickr-Sicherheitsgruppen einsehen.

Gehen Sie wie folgt vor, um Sicherheitsgruppen anzuzeigen.

1. Öffnen Sie sie AWS-Managementkonsole für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.

   Auf der Seite Sicherheitsgruppen werden Ihre aktuellen Wickr-Sicherheitsgruppen angezeigt und Sie haben die Möglichkeit, eine neue Gruppe zu erstellen.

   Wählen Sie auf der Seite Sicherheitsgruppen die Sicherheitsgruppe aus, die Sie anzeigen möchten. Auf der Seite werden die aktuellen Details für diese Sicherheitsgruppe angezeigt.

Erstellen Sie eine Sicherheitsgruppe in AWS Wickr

Sie können eine neue Wickr-Sicherheitsgruppe erstellen.

Gehen Sie wie folgt vor, um eine Sicherheitsgruppe zu erstellen.

1. Öffnen Sie sie AWS-Managementkonsole für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
4. Wählen Sie auf der Seite Sicherheitsgruppen die Option Sicherheitsgruppe erstellen aus, um eine neue Sicherheitsgruppe zu erstellen.

> **Note**
>
> Eine neue Sicherheitsgruppe mit einem Standardnamen wird automatisch zur Liste der Sicherheitsgruppen hinzugefügt.

5. Geben Sie auf der Seite Sicherheitsgruppe erstellen den Namen Ihrer Sicherheitsgruppe ein.
6. Wählen Sie Sicherheitsgruppe erstellen aus.

   Weitere Informationen zum Bearbeiten der neuen Sicherheitsgruppe finden Sie unterBearbeiten Sie eine Sicherheitsgruppe in AWS Wickr.

Bearbeiten Sie eine Sicherheitsgruppe in AWS Wickr

Sie können die Details Ihrer Wickr-Sicherheitsgruppe bearbeiten.

Gehen Sie wie folgt vor, um eine Sicherheitsgruppe zu bearbeiten.

1. Öffnen Sie sie AWS-Managementkonsole für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
4. Wählen Sie den Namen der Sicherheitsgruppe aus, die Sie bearbeiten möchten.

   Auf der Seite mit den Sicherheitsgruppendetails werden die Einstellungen für die Sicherheitsgruppe auf verschiedenen Registerkarten angezeigt.
5. Die folgenden Registerkarten und die entsprechenden Einstellungen sind verfügbar:

   - Details zur Sicherheitsgruppe — Wählen Sie im Abschnitt Sicherheitsgruppendetails die Option Bearbeiten aus, um den Namen zu bearbeiten.
   - Messaging — Verwaltet die Nachrichtenfunktionen für Mitglieder der Gruppe.
     - Burn-on-read— Steuert den Höchstwert, den Benutzer für ihre Burn-on-Read-Timer in ihren Wickr-Clients festlegen können. Weitere Informationen finden Sie unter Ablaufen- und Brenntimer für Nachrichten im Wickr-Client festlegen.

- Ablauftimer — Steuert den Höchstwert, den Benutzer für ihren Nachrichtenablauftimer in ihren Wickr-Clients festlegen können. Weitere Informationen finden Sie unter Festlegen von Ablaufzeiten und Brenntimern für Nachrichten im Wickr-Client.
- Nachrichtenweiterleitung — Steuert, ob Benutzer Nachrichten in ihren Wickr-Clients weiterleiten können. Weitere Informationen finden Sie unter Nachrichten im Wickr-Client weiterleiten.
- Schnelle Antworten — Legen Sie eine Liste mit Schnellantworten fest, damit Benutzer auf Nachrichten antworten können.
- Intensität des sicheren Aktenvernichters — Konfigurieren Sie, wie oft die sichere Shredder-Steuerung für Benutzer ausgeführt wird. Weitere Informationen finden Sie unter Messaging.

- Telefonieren — Verwalten Sie die Anruffunktionen für Mitglieder der Gruppe.
  - Audioanrufe aktivieren — Benutzer können Audioanrufe einleiten.
  - Videoanrufe und Bildschirmübertragung aktivieren — Benutzer können während des Anrufs Videoanrufe starten oder den Bildschirm teilen.
  - TCP-Anrufe — Das Aktivieren (oder Erzwingen) von TCP-Anrufen wird normalerweise verwendet, wenn Standard-VoIP-UDP-Ports von der IT- oder Sicherheitsabteilung eines Unternehmens nicht zugelassen werden. Wenn TCP-Anrufe deaktiviert sind und UDP-Ports nicht zur Verfügung stehen, versuchen Wickr-Clients zuerst UDP und greifen dann auf TCP zurück.
- Medien und Links — Verwaltet Einstellungen in Bezug auf Medien und Links für Mitglieder der Gruppe.

  Größe des Dateidownloads — Wählen Sie „Übertragung in bester Qualität“ aus, damit Benutzer Dateien und Anlagen in ihrer ursprünglichen verschlüsselten Form übertragen können. Wenn Sie Übertragung mit geringer Bandbreite auswählen, werden Dateianhänge, die von Benutzern in Wickr gesendet werden, vom Wickr-Dateiübertragungsdienst komprimiert.
- Standort — Verwaltet die Einstellungen für die gemeinsame Nutzung von Standorten für Mitglieder der Gruppe.

  Standortfreigabe — Benutzer können ihre Standorte mithilfe von GPS-enabled Geräten teilen. Diese Funktion zeigt eine visuelle Karte an, die auf den Standardeinstellungen des Betriebssystems des Geräts basiert. Benutzer haben die Möglichkeit, die Kartenansicht zu deaktivieren und stattdessen einen Link mit ihren GPS-Koordinaten zu teilen.
- Sicherheit — Konfigurieren Sie zusätzliche Sicherheitsfunktionen für die Gruppe.

- Schutz vor Kontoübernahmen aktivieren — Erzwingen Sie eine Zwei-Faktor-Authentifizierung, wenn ein Benutzer seinem Konto ein neues Gerät hinzufügt. Um ein neues Gerät zu verifizieren, kann der Benutzer auf seinem alten Gerät einen Wickr-Code generieren oder eine E-Mail-Bestätigung durchführen. Dies ist eine zusätzliche Sicherheitsebene, um unbefugten Zugriff auf AWS Wickr-Konten zu verhindern.
- Immer neu authentifizieren aktivieren — Erzwingt Benutzer, sich immer neu zu authentifizieren, wenn sie die Anwendung erneut aufrufen.
- Master-Wiederherstellungsschlüssel — Erstellt einen Master-Wiederherstellungsschlüssel, wenn ein Konto erstellt wird. Benutzer können das Hinzufügen eines neuen Geräts zu ihrem Konto genehmigen, wenn keine anderen Geräte verfügbar sind.
- Timeout ohne SSO — Konfigurieren Sie ein Sitzungs-Timeout für Nicht-SSO-Benutzer, die unabhängig von der Benutzeraktivität nach einem bestimmten Zeitraum erneut ein Passwort in der App eingeben müssen.

- Benachrichtigung und Sichtbarkeit — Konfigurieren Sie Benachrichtigungs- und Sichtbarkeitseinstellungen wie Nachrichtenvorschauen in Benachrichtigungen für Mitglieder der Gruppe.
- Wickr Open Access — Konfigurieren Sie Wickr Open Access-Einstellungen für Mitglieder der Gruppe.
  - Wickr Open Access aktivieren — Durch die Aktivierung von Wickr Open Access wird der Datenverkehr verschleiert, um Daten in eingeschränkten und überwachten Netzwerken zu schützen. Je nach geografischem Standort stellt Wickr Open Access eine Verbindung zu verschiedenen globalen Proxyservern her, die den besten Pfad und die besten Protokolle für die Verschleierung des Datenverkehrs bereitstellen.
  - Wickr Open Access erzwingen — Aktiviert und erzwingt Wickr Open Access automatisch auf allen Geräten.
- Federation — Kontrollieren Sie die Fähigkeit Ihrer Benutzer, mit anderen Wickr-Netzwerken zu kommunizieren.
  - Lokaler Verband — Die Fähigkeit, sich mit AWS Benutzern in anderen Netzwerken innerhalb derselben Region zu verbünden. Wenn es beispielsweise zwei Netzwerke in der Region AWS Kanada (Central) gibt, für die der lokale Verbund aktiviert ist, können sie miteinander kommunizieren.
  - Globaler Verbund — Die Möglichkeit, entweder Wickr Enterprise-Benutzer oder AWS Benutzer in einem anderen Netzwerk, die zu anderen Regionen gehören, zu verbünden. Beispielsweise können ein Benutzer in einem Wickr-Netzwerk in der Region AWS Kanada

(Central) und ein Benutzer in einem Netzwerk in der Region AWS Europa (London) miteinander kommunizieren, wenn der globale Verbund für beide Netzwerke aktiviert ist.

- Eingeschränkter Verbund — Erlaubt die Liste bestimmter AWS Wickr- oder Wickr Enterprise-Netzwerke, mit denen Benutzer sich verbinden können. Wenn konfiguriert, können Benutzer nur mit externen Benutzern in Netzwerken kommunizieren, die auf der Liste der zugelassenen Netzwerke stehen. Beide Netzwerke müssen es zulassen, sich gegenseitig aufzulisten, um den eingeschränkten Verbund verwenden zu können.

  Informationen zum Gastverbund finden Sie unter Aktivieren oder Deaktivieren von Gastbenutzern im AWS Wickr-Netzwerk.

- Konfiguration des ATAK-Plug-ins — Weitere Informationen zur Aktivierung von ATAK finden Sie unter Was ist ATAK? .

6. Wählen Sie Speichern, um die Änderungen zu speichern, die Sie an den Sicherheitsgruppendetails vorgenommen haben.

Löschen Sie eine Sicherheitsgruppe in AWS Wickr

Sie können Ihre Wickr-Sicherheitsgruppe löschen.

Gehen Sie wie folgt vor, um eine Sicherheitsgruppe zu löschen.

1. Öffnen Sie sie AWS-Managementkonsole für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
4. Suchen Sie auf der Seite Sicherheitsgruppen nach der Sicherheitsgruppe, die Sie löschen möchten.
5. Wählen Sie auf der rechten Seite der Sicherheitsgruppe, die Sie löschen möchten, das vertikale Ellipsensymbol (drei Punkte) und dann Löschen aus.
6. Geben Sie in das Popup-Fenster Bestätigen ein und wählen Sie dann Löschen.

   Wenn Sie eine Sicherheitsgruppe löschen, der Benutzer zugewiesen wurden, werden diese Benutzer automatisch der Standardsicherheitsgruppe hinzugefügt. Informationen zum Ändern der den Benutzern zugewiesenen Sicherheitsgruppe finden Sie unterBenutzer im AWS Wickr-Netzwerk bearbeiten.

Single Sign-On-Konfiguration für AWS Wickr

In der AWS-Managementkonsole for Wickr können Sie Wickr so konfigurieren, dass ein Single Sign-On-System zur Authentifizierung verwendet wird. SSO bietet eine zusätzliche Sicherheitsebene, wenn es mit einem geeigneten Multi-Faktor-Authentifizierungssystem (MFA) kombiniert wird. Wickr unterstützt SSO-Anbieter, die nur OpenID Connect (OIDC) verwenden. Anbieter, die Security Assertion Markup Language (SAML) verwenden, werden nicht unterstützt.

Topics

SSO-Details in AWS Wickr anzeigen

Sie können die Details Ihrer Single Sign-On-Konfiguration für Ihr Wickr-Netzwerk und den Netzwerkendpunkt einsehen.

Gehen Sie wie folgt vor, um die aktuelle Single Sign-On-Konfiguration für Ihr Wickr-Netzwerk, falls vorhanden, anzuzeigen.

1. Öffnen Sie das AWS-Managementkonsole für Wickr unter. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Benutzerverwaltung aus.

   Auf der Seite Benutzerverwaltung werden im Sign-on Bereich Single Ihr Wickr-Netzwerkendpunkt und die aktuelle SSO-Konfiguration angezeigt.

SSO in AWS Wickr konfigurieren

Um einen sicheren Zugriff auf Ihr Wickr-Netzwerk zu gewährleisten, können Sie Ihre aktuelle Single Sign-On-Konfiguration einrichten. Detaillierte Anleitungen stehen zur Verfügung, um Sie bei diesem Prozess zu unterstützen.

Important

- Wenn Sie SSO konfigurieren, geben Sie eine Unternehmens-ID für Ihr Wickr-Netzwerk an. Achten Sie darauf, diese Unternehmens-ID aufzuzeichnen. Sie müssen sie Ihren Endbenutzern beim Versenden von Einladungs-E-Mails zur Verfügung stellen. Endbenutzer müssen die Unternehmens-ID angeben, wenn sie sich für Ihr Wickr-Netzwerk registrieren.
- Im September 2025 führte AWS Wickr ein verbessertes, sichereres SSO-Verbindungssystem ein. Um diese Sicherheitsverbesserungen nutzen zu können, müssen Unternehmen, die SSO verwenden, bis zum 09. März 2026 auf eine neue Umleitungs-URI migrieren. Anweisungen zur Migration finden Sie im folgenden AWS re:Post Artikel: Migration zur neuen SSO-Umleitungs-URI für AWS Wickr.

Weitere Informationen zur Konfiguration von SSO finden Sie in den folgenden Anleitungen:

- Einrichtung von AWS Wickr Single Sign-on (SSO) mit Microsoft Entra (Azure AD)
- Einrichtung von AWS Wickr Single Sign-on (SSO) mit Okta
- Einrichtung von AWS Wickr Single Sign-on (SSO) mit Amazon Cognito

Konfigurieren Sie AWS Wickr mit Microsoft Entra (Azure AD) Single Sign-On

AWS Wickr kann so konfiguriert werden, dass Microsoft Entra (Azure AD) als Identitätsanbieter verwendet wird. Führen Sie dazu die folgenden Verfahren sowohl in Microsoft Entra als auch in der AWS Wickr-Administrationskonsole durch.

Warning

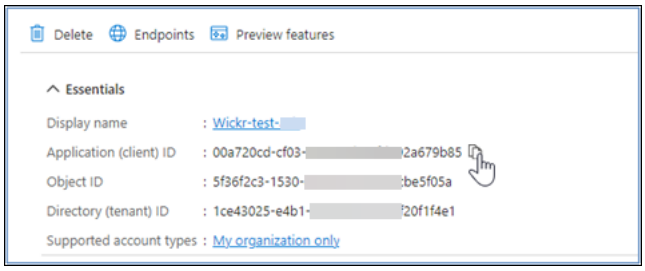
Nachdem SSO in einem Netzwerk aktiviert wurde, werden aktive Benutzer von Wickr abgemeldet und sie werden gezwungen, sich erneut über den SSO-Anbieter zu authentifizieren.

Schritt 1: Registrieren Sie AWS Wickr als Anwendung in Microsoft Entra

Gehen Sie wie folgt vor, um AWS Wickr als Anwendung in Microsoft Entra zu registrieren.

> **Note**
>
> Detaillierte Screenshots und Problemlösungen finden Sie in der Microsoft Entra-Dokumentation. Weitere Informationen finden Sie unter Registrieren einer Anwendung bei der Microsoft Identity Platform

1. Wählen Sie im Navigationsbereich Anwendungen und dann App-Registrierungen aus.
2. Wählen Sie auf der Seite App-Registrierungen die Option Anwendung registrieren aus und geben Sie dann einen Anwendungsnamen ein.
3. Wählen Sie Nur Konten in diesem Organisationsverzeichnis aus (Nur Standardverzeichnis — Einzelmandant).
4. Wählen Sie unter Umleitungs-URI die Option Web aus und geben Sie dann die Umleitungs-URI ein, die in den SSO-Konfigurationseinstellungen in der AWS Wickr Admin-Konsole verfügbar ist
5. Wählen Sie Registrieren aus.
6. Nach der Registrierung wurde copy/save die Anwendungs-ID (Client) generiert.

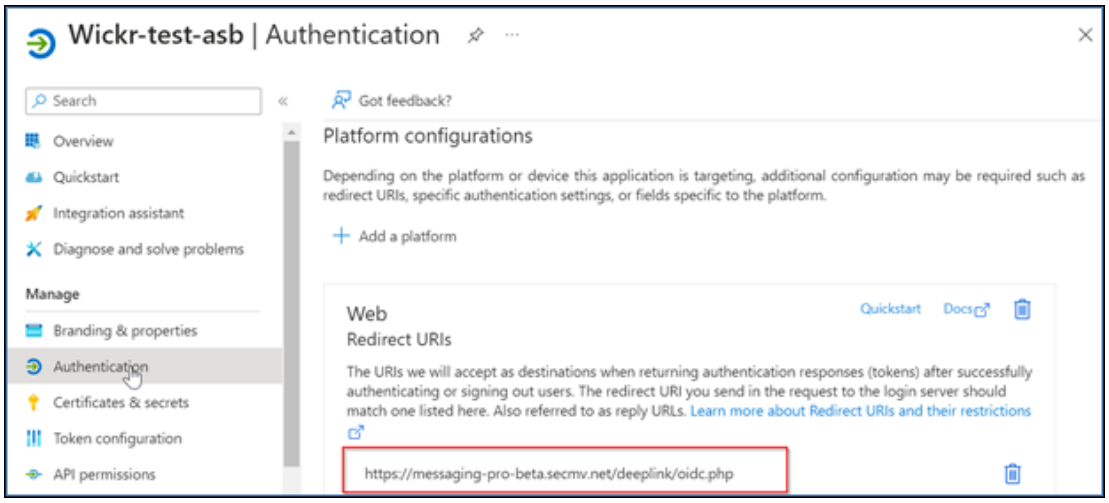


7. Wählen Sie die Registerkarte Endpoints, um sich Folgendes zu notieren:
   1. OAuth 2.0-Autorisierungsendpunkt (v2): z. B.: `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/oauth2/v2.0/authorize`
   2. Bearbeiten Sie diesen Wert, um „oauth2/“ und „authorize“ zu entfernen. Die feste URL sieht zum Beispiel so aus: `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`
   3. Dies wird als SSO-Herausgeber bezeichnet.

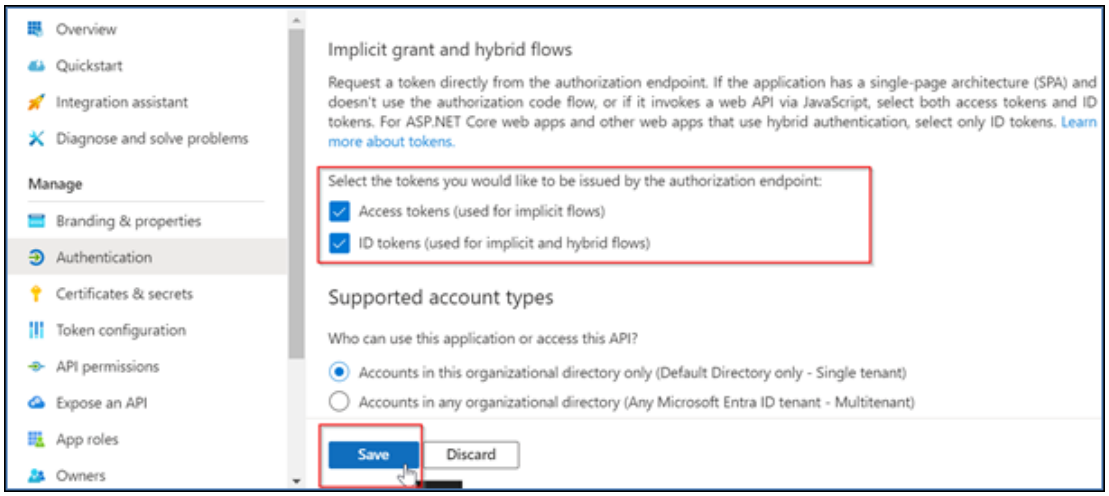
Schritt 2: Authentifizierung einrichten

Gehen Sie wie folgt vor, um die Authentifizierung in Microsoft Entra einzurichten.

1. Wählen Sie im Navigationsbereich Authentifizierung aus.
2. Vergewissern Sie sich auf der Authentifizierungsseite, dass der Webumleitungs-URI derselbe ist, der zuvor eingegeben wurde (unter AWS Wickr als Anwendung registrieren).



3. Wählen Sie Zugriffstoken aus, die für implizite Datenflüsse verwendet werden, und ID-Token, die für implizite und hybride Datenflüsse verwendet werden.
4. Wählen Sie Speichern.

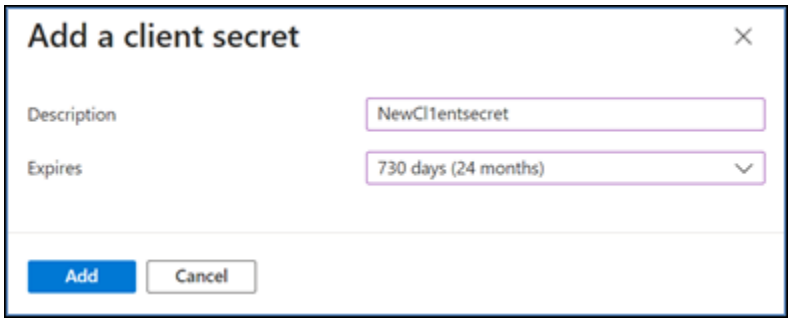


Schritt 3: Zertifikate und Geheimnisse einrichten

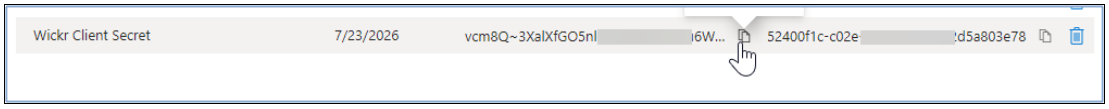
Gehen Sie wie folgt vor, um Zertifikate und Geheimnisse in Microsoft Entra einzurichten.

1. Wählen Sie im Navigationsbereich Certificates & Secrets aus.
2. Wählen Sie auf der Seite Certificates & Secrets die Registerkarte Client Secrets aus.
3. Wählen Sie auf der Registerkarte Client-Geheimnisse die Option Neuer geheimer Client-Schlüssel aus.

4. Geben Sie eine Beschreibung ein und wählen Sie einen Ablaufzeitraum für das Geheimnis aus.
5. Wählen Sie Hinzufügen aus.



6. Kopieren Sie nach der Erstellung des Zertifikats den Wert für den geheimen Clientschlüssel.

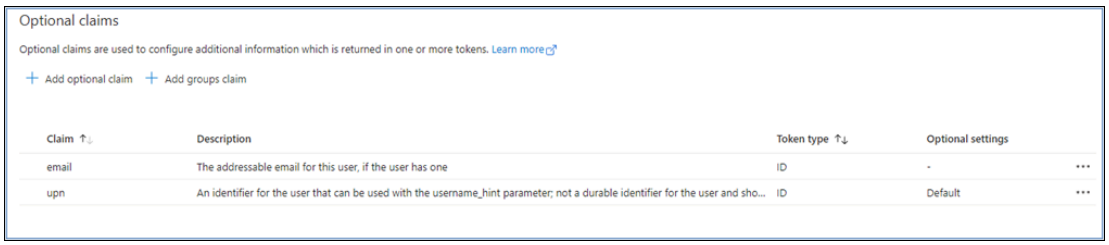


> **Note**
>
> Der geheime Wert des Client (nicht Secret ID) wird für Ihren Client-Anwendungscode benötigt. Möglicherweise können Sie den geheimen Wert nicht anzeigen oder kopieren, nachdem Sie diese Seite verlassen haben. Wenn Sie ihn jetzt nicht kopieren, müssen Sie zurückgehen, um einen neuen geheimen Clientschlüssel zu erstellen.

Schritt 4: Token-Konfiguration einrichten

Gehen Sie wie folgt vor, um die Tokenkonfiguration in Microsoft Entra einzurichten.

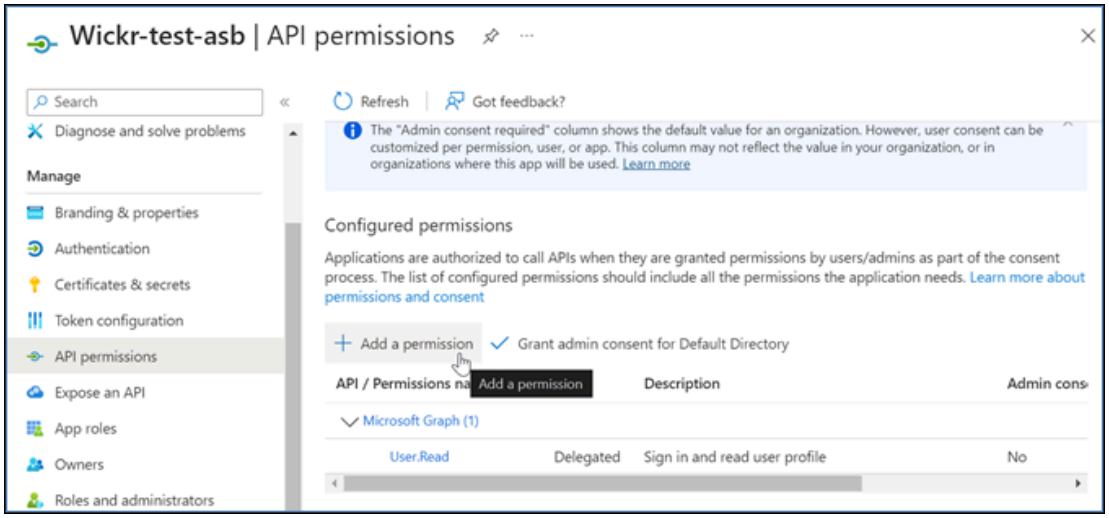
1. Wählen Sie im Navigationsbereich Tokenkonfiguration aus.
2. Wählen Sie auf der Seite Token-Konfiguration die Option Optionalen Anspruch hinzufügen aus.
3. Wählen Sie unter Optionale Ansprüche den Token-Typ als ID aus.
4. Nachdem Sie ID ausgewählt haben, wählen Sie unter Anspruch die Option E-Mail und UPN aus.
5. Wählen Sie Hinzufügen aus.



Schritt 5: API-Berechtigungen einrichten

Gehen Sie wie folgt vor, um API-Berechtigungen in Microsoft Entra einzurichten.

1. Wählen Sie im Navigationsbereich API permissions (API-Berechtigungen) aus.
2. Wählen Sie auf der Seite mit den API-Berechtigungen die Option Berechtigung hinzufügen aus.

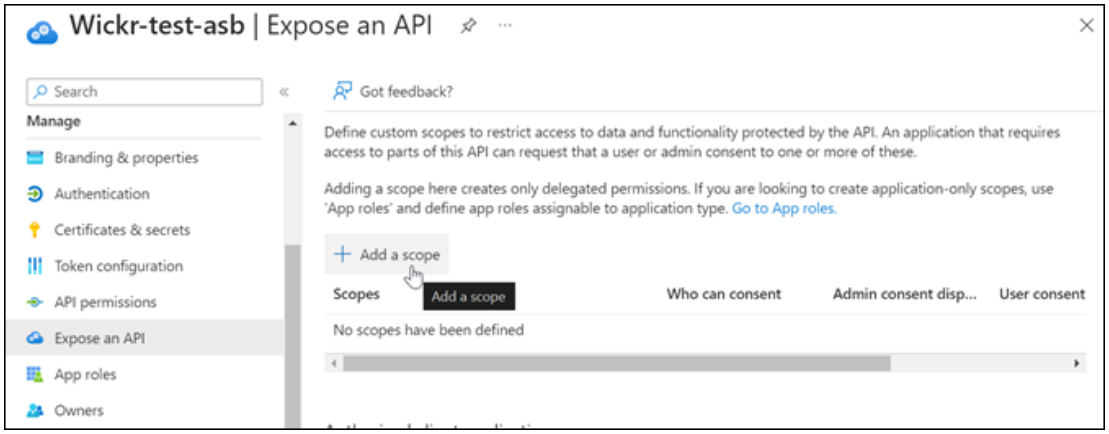


3. Wählen Sie Microsoft Graph und dann Delegierte Berechtigungen aus.
4. Aktivieren Sie das Kontrollkästchen für E-Mail, Offline_Access, OpenID und Profil.
5. Wählen Sie Add permissions (Berechtigungen hinzufügen) aus.

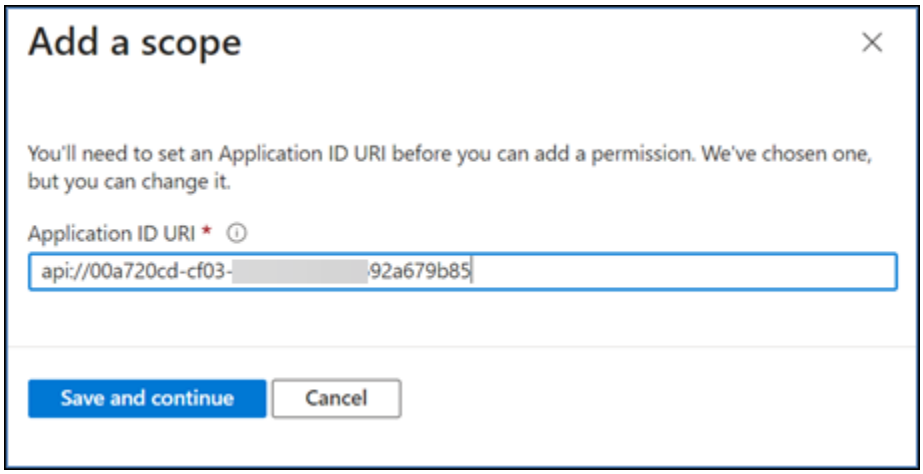
Schritt 6: Machen Sie eine API verfügbar

Gehen Sie wie folgt vor, um eine API für jeden der 4 Bereiche in Microsoft Entra verfügbar zu machen.

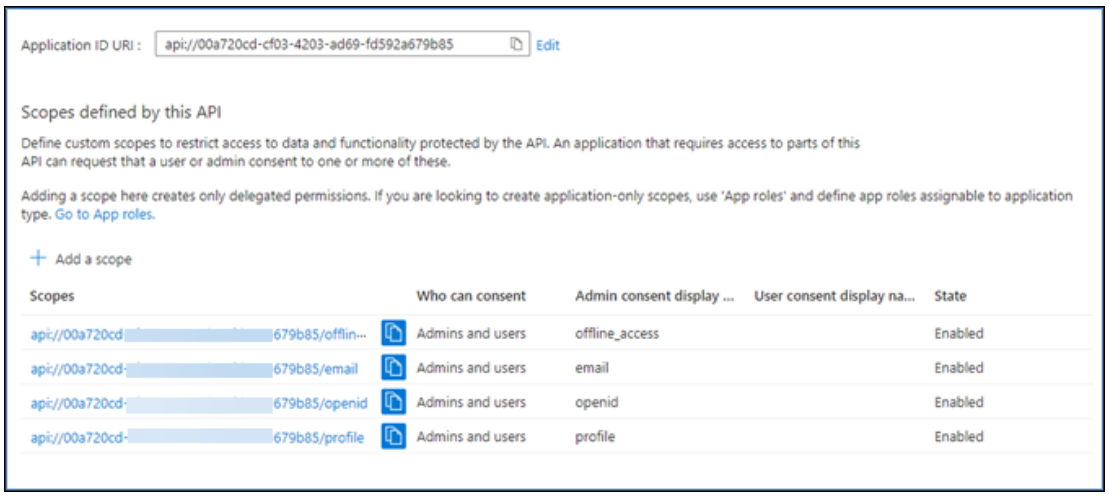
1. Wählen Sie im Navigationsbereich die Option Expose an API aus.
2. Wählen Sie auf der Seite Eine API verfügbar machen die Option Bereich hinzufügen aus.



Die Anwendungs-ID-URI sollte auto aufgefüllt werden, und die ID, die auf den URI folgt, sollte mit der Anwendungs-ID übereinstimmen (erstellt in AWS Wickr als Anwendung registrieren).



3. Wählen Sie Save and continue aus.
4. Wählen Sie das Tag Admins and users aus und geben Sie dann den Bereichsnamen als offline_access ein.
5. Wählen Sie Status und dann Aktivieren aus.
6. Wählen Sie Bereich hinzufügen aus.
7. Wiederholen Sie die Schritte 1—6 dieses Abschnitts, um die folgenden Bereiche hinzuzufügen: E-Mail, OpenID und Profil.



8. Wählen Sie unter Autorisierte Clientanwendungen die Option Clientanwendung hinzufügen aus.
9. Wählen Sie alle vier Bereiche aus, die im vorherigen Schritt erstellt wurden.
10. Geben Sie die Anwendungs-ID (Client) ein oder überprüfen Sie sie.
11. Wählen Sie Anwendung hinzufügen.

Schritt 7: AWS Wickr SSO-Konfiguration

Führen Sie das folgende Konfigurationsverfahren in der AWS Wickr-Konsole durch.

1. Öffnen Sie das AWS-Managementkonsole für Wickr unter. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Benutzerverwaltung und dann SSO konfigurieren aus.
4. Geben Sie folgende Details ein:

   - Aussteller — Dies ist der Endpunkt, der zuvor geändert wurde (z. B.`https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`).
   - Client-ID — Dies ist die Anwendungs-ID (Client) aus dem Übersichtsbereich.
   - Geheimer Client-Schlüssel (optional) — Dies ist der geheime Client-Schlüssel aus dem Bereich Certificates & Secrets.
   - Bereiche — Dies sind die Bereichsnamen, die im Bereich „Eine API verfügbar machen“ angezeigt werden. Geben Sie email, profile, offline_access und openid ein.
   - Gültigkeitsbereich des benutzerdefinierten Benutzernamens (optional) — Geben Sie upn ein.

- Unternehmens-ID — Dies kann ein eindeutiger Textwert sein, der alphanumerische Zeichen und Unterstriche enthält. Dieser Satz wird von Ihren Benutzern eingegeben, wenn sie sich auf neuen Geräten registrieren.

Andere Felder sind optional.

5. Wählen Sie Weiter aus.
6. Überprüfen Sie die Details auf der Seite Überprüfen und speichern und wählen Sie dann Änderungen speichern aus.

Die SSO-Konfiguration ist abgeschlossen. Zur Überprüfung können Sie der Anwendung in Microsoft Entra jetzt einen Benutzer hinzufügen und sich mit dem Benutzer über SSO und Unternehmens-ID anmelden.

Weitere Informationen zum Einladen und Onboarding von Benutzern finden Sie unter Benutzer erstellen und einladen.

Fehlerbehebung

Im Folgenden finden Sie häufig auftretende Probleme und Vorschläge zu deren Lösung.

- Der SSO-Verbindungstest schlägt fehl oder reagiert nicht:
  - Stellen Sie sicher, dass der SSO-Aussteller wie erwartet konfiguriert ist.
  - Stellen Sie sicher, dass die erforderlichen Felder in der SSO-Konfiguration wie erwartet festgelegt sind.
- Der Verbindungstest ist erfolgreich, aber der Benutzer kann sich nicht anmelden:
  - Stellen Sie sicher, dass der Benutzer zu der Wickr-Anwendung hinzugefügt wurde, die Sie in Microsoft Entra registriert haben.
  - Stellen Sie sicher, dass der Benutzer die richtige Unternehmens-ID einschließlich des Präfixes verwendet. Z. B. UE1 - DemoNetwork W_drqtVA.
  - Das Client Secret ist in der AWS Wickr SSO-Konfiguration möglicherweise nicht korrekt festgelegt. Setzen Sie es zurück, indem Sie ein anderes Client-Geheimnis in Microsoft Entra erstellen und das neue Client-Geheimnis in der Wickr SSO-Konfiguration festlegen.

Übergangsfrist für die Token-Aktualisierung

Gelegentlich kann es vorkommen, dass Identitätsanbieter auf vorübergehende oder längere Ausfälle stoßen, was dazu führen kann, dass Ihre Benutzer aufgrund eines fehlgeschlagenen Aktualisierungstokens für ihre Clientsitzung unerwartet abgemeldet werden. Um dieses Problem zu vermeiden, können Sie eine Übergangsfrist einrichten, die es Ihren Benutzern ermöglicht, angemeldet zu bleiben, auch wenn ihr Client-Aktualisierungstoken bei solchen Ausfällen ausfällt.

Hier sind die verfügbaren Optionen für den Kulanzzeitraum:

- Keine Kulanzfrist (Standard): Benutzer werden sofort nach einem Fehler bei einem Aktualisierungstoken abgemeldet.
- Nachfrist von 30 Minuten: Benutzer können bis zu 30 Minuten angemeldet bleiben, nachdem ein Aktualisierungstoken fehlgeschlagen ist.
- Kulanzzeit von 60 Minuten: Benutzer können nach einem Fehler beim Aktualisierungstoken bis zu 60 Minuten angemeldet bleiben.

Netzwerk-Tags für AWS Wickr

Sie können Tags auf Wickr-Netzwerke anwenden. Sie können diese Tags dann verwenden, um Ihre Wickr-Netzwerke zu durchsuchen und zu filtern oder Ihre AWS Kosten zu verfolgen. Sie können Netzwerk-Tags auf der Netzwerk-Startseite von AWS-Managementkonsole for Wickr konfigurieren.

Ein Tag ist ein Schlüssel-Wert-Paar, das auf eine Ressource angewendet wird und Metadaten zu dieser Ressource enthält. Jedes Tag ist eine Bezeichnung, die aus einem Schlüssel und einem Wert besteht. Weitere Informationen zu Tags finden Sie auch unter Was sind Tags? und Anwendungsfälle zum Taggen.

Topics

Netzwerk-Tags in AWS Wickr verwalten

Sie können Netzwerk-Tags für Ihr Wickr-Netzwerk verwalten.

Gehen Sie wie folgt vor, um Netzwerk-Tags für Ihr Wickr-Netzwerk zu verwalten.

1. Öffnen Sie das AWS-Managementkonsole für Wickr unter. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie auf der Netzwerk-Startseite im Abschnitt Tags die Option Tags verwalten aus.
4. Auf der Seite „Tags verwalten“ können Sie eine der folgenden Optionen auswählen:

   - Neue Tags hinzufügen — Geben Sie neue Tags in Form eines Schlüssel- und Wertepaars ein. Wählen Sie Neues Tag hinzufügen, um mehrere Schlüssel-Wert-Paare hinzuzufügen. Bei Tags muss die Groß- und Kleinschreibung beachtet werden. Weitere Informationen finden Sie unter Fügen Sie ein Netzwerk-Tag in AWS Wickr hinzu.
   - Bestehende Tags bearbeiten — Wählen Sie den Schlüssel- oder Werttext für ein vorhandenes Tag aus und geben Sie dann die Änderung in das Textfeld ein. Weitere Informationen finden Sie unter Bearbeiten Sie ein Netzwerk-Tag in AWS Wickr.
   - Bestehende Tags entfernen — Wählen Sie die Schaltfläche Entfernen, die neben dem Tag aufgeführt ist, den Sie löschen möchten. Weitere Informationen finden Sie unter Entfernen Sie ein Netzwerk-Tag in AWS Wickr.

Fügen Sie ein Netzwerk-Tag in AWS Wickr hinzu

Sie können Ihrem Wickr-Netzwerk ein Netzwerk-Tag hinzufügen.

Gehen Sie wie folgt vor, um Ihrem Wickr-Netzwerk ein Tag hinzuzufügen. Weitere Informationen zur Verwaltung von Tags finden Sie unterNetzwerk-Tags in AWS Wickr verwalten.

1. Wählen Sie auf der Netzwerk-Startseite im Abschnitt Tags die Option Neues Tag hinzufügen aus.
2. Wählen Sie auf der Seite Tags verwalten Neuen Tag hinzufügen aus.
3. Geben Sie in den angezeigten leeren Feldern Schlüssel und Wert den Schlüssel und Wert des neuen Tags ein.

4. Wählen Sie Änderungen speichern, um die neuen Tags zu speichern.

Bearbeiten Sie ein Netzwerk-Tag in AWS Wickr

Sie können ein Netzwerk-Tag für Ihr Wickr-Netzwerk bearbeiten.

Gehen Sie wie folgt vor, um ein mit Ihrem Wickr-Netzwerk verknüpftes Tag zu bearbeiten. Weitere Informationen zur Verwaltung von Tags finden Sie unterNetzwerk-Tags in AWS Wickr verwalten.

1. Bearbeiten Sie auf der Seite „Tags verwalten“ den Wert eines Tags.

   > **Note**
   >
   > Sie können den Schlüssel eines Tags nicht bearbeiten. Entfernen Sie stattdessen das Schlüssel- und Wertepaar und fügen Sie mithilfe des neuen Schlüssels ein neues Tag hinzu.

2. Wählen Sie Änderungen speichern, um Ihre Änderungen zu speichern.

Entfernen Sie ein Netzwerk-Tag in AWS Wickr

Sie können ein Netzwerk-Tag aus Ihrem Wickr-Netzwerk entfernen.

Gehen Sie wie folgt vor, um ein Tag aus Ihrem Wickr-Netzwerk zu entfernen. Weitere Informationen zur Verwaltung von Tags finden Sie unterNetzwerk-Tags in AWS Wickr verwalten.

1. Wählen Sie auf der Seite „Stichwörter verwalten“ für das Tag, das Sie entfernen möchten, die Option Entfernen aus.
2. Wählen Sie Änderungen speichern, um Ihre Änderungen zu speichern.

Quittungen für AWS Wickr lesen

Lesebestätigungen für AWS Wickr sind Benachrichtigungen, die an den Absender gesendet werden, um anzuzeigen, dass seine Nachricht gelesen wurde. Diese Belege sind in Einzelgesprächen verfügbar. Für gesendete Nachrichten wird ein einzelnes Häkchen und für gelesene Nachrichten ein durchgezogener Kreis mit einem Häkchen angezeigt. Um Lesebestätigungen für Nachrichten während externer Konversationen zu sehen, sollten Lesebestätigungen in beiden Netzwerken aktiviert sein.

Administratoren können Lesebestätigungen im Administratorbereich aktivieren oder deaktivieren. Diese Einstellung wird auf das gesamte Netzwerk angewendet.

Gehen Sie wie folgt vor, um Lesebestätigungen zu aktivieren oder zu deaktivieren.

1. Öffnen Sie sie AWS-Managementkonsole für Wickr unter. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Netzwerkrichtlinien aus.
4. Wählen Sie auf der Seite Netzwerkrichtlinien im Abschnitt Messaging die Option Bearbeiten aus.
5. Markieren Sie das Kontrollkästchen, um Lesebestätigungen zu aktivieren oder zu deaktivieren.
6. Wählen Sie Änderungen speichern aus.

Netzwerkplan für AWS Wickr verwalten

Im AWS-Managementkonsole for Wickr können Sie Ihren Netzwerkplan auf der Grundlage Ihrer Geschäftsanforderungen verwalten.

Gehen Sie wie folgt vor, um Ihren Netzwerkplan zu verwalten.

1. Öffnen Sie sie AWS-Managementkonsole für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie auf der Netzwerk-Startseite im Abschnitt Netzwerkdetails die Option Bearbeiten aus.
4. Wählen Sie auf der Seite Netzwerkdetails bearbeiten den gewünschten Netzwerkplan aus. Sie können Ihren aktuellen Netzwerkplan ändern, indem Sie eine der folgenden Optionen wählen:

   - Standard — Für kleine und große Unternehmensteams, die administrative Kontrollen und Flexibilität benötigen.
   - Premium - oder kostenlose Premium-Testversion — Für Unternehmen, die höchste Funktionseinschränkungen, detaillierte Verwaltungskontrollen und Datenspeicherung benötigen.

     Administratoren haben die Möglichkeit, eine kostenlose Premium-Testversion auszuwählen, die für bis zu 30 Benutzer verfügbar ist und drei Monate gültig ist. Denn AWS WickrGov

die kostenlose Premium-Testoption ermöglicht bis zu 50 Benutzer und ist ebenfalls drei Monate gültig. Dieses Angebot steht neuen Tarifen und Standardplänen offen. Während der kostenlosen Premium-Testphase können Administratoren ein Upgrade oder Downgrade auf Premium- oder Standard-Tarife durchführen

> **Note**
>
> Um die Nutzung und Abrechnung in Ihrem Netzwerk zu beenden, entfernen Sie alle Benutzer, einschließlich aller gesperrten Benutzer, aus Ihrem Netzwerk.

Einschränkungen der kostenlosen Premium-Testversion

Die folgenden Einschränkungen gelten für die kostenlose Premium-Testversion:

- Wenn ein Plan schon einmal für eine kostenlose Premium-Testversion registriert wurde, ist er nicht für eine weitere Testversion berechtigt.
- Pro AWS Konto kann nur ein Netzwerk für eine kostenlose Premium-Testversion registriert werden.
- Die Gastbenutzerfunktion ist während der kostenlosen Premium-Testversion nicht verfügbar.
- Wenn ein Standardnetzwerk mehr als 30 Benutzer hat (mehr als 50 Benutzer für AWS WickrGov), ist ein Upgrade auf eine kostenlose Premium-Testversion nicht möglich.

Datenspeicherung für AWS Wickr

AWS Wickr Data Retention kann alle Konversationen im Netzwerk speichern. Dazu gehören Direktnachrichtengespräche und Konversationen in Gruppen oder Räumen zwischen (internen) Mitgliedern im Netzwerk und denen mit anderen Teams (extern), mit denen Ihr Netzwerk verbunden ist. Die Datenspeicherung steht nur Benutzern des AWS Wickr Premium-Plans und Unternehmenskunden zur Verfügung, die sich für die Datenspeicherung entscheiden. Weitere Informationen zum Premium-Plan finden Sie unter Wickr-Preise

Wenn ein Netzwerkadministrator die Datenspeicherung für sein Netzwerk konfiguriert und aktiviert, werden alle Nachrichten und Dateien, die von Benutzern in seinem Netzwerk gemeinsam genutzt werden, an einem bestimmten Ort (E.g., lokaler Speicher, Amazon S3 S3-Bucket) archiviert, wo sie nach Bedarf überprüft, verarbeitet und aufbewahrt werden können.

> **Note**
>
> AWSkann nicht auf Ende-zu-Ende verschlüsselte Nachrichteninhalte in Wickr zugreifen. Wenn Ihre Organisation Zugriff auf die Nachrichteninhalte Ihrer Endbenutzer benötigt, müssen Sie einen Datenaufbewahrungsbot einsetzen.

Topics

Details zur Datenspeicherung in AWS Wickr anzeigen

Gehen Sie wie folgt vor, um die Details zur Datenspeicherung für Ihr Wickr-Netzwerk einzusehen. Sie können die Datenspeicherung auch für Ihr Wickr-Netzwerk aktivieren oder deaktivieren.

1. Öffnen Sie das AWS-Managementkonsole für Wickr unter. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Netzwerkrichtlinien aus.
4. Auf der Seite Netzwerkrichtlinien werden Schritte zum Einrichten der Datenspeicherung sowie die Option zum Aktivieren oder Deaktivieren der Datenaufbewahrungsfunktion angezeigt. Weitere Informationen zur Konfiguration der Datenspeicherung finden Sie unterDatenspeicherung für AWS Wickr konfigurieren.

> **Note**
>
> Wenn die Datenspeicherung aktiviert ist, wird allen Benutzern in Ihrem Netzwerk die Meldung „Datenspeicherung aktiviert“ angezeigt, die sie über das Netzwerk mit aktivierter Datenspeicherung informiert.

Datenspeicherung für AWS Wickr konfigurieren

Um die Datenspeicherung für Ihr AWS Wickr-Netzwerk zu konfigurieren, müssen Sie das Docker-Image des Datenaufbewahrungsbots in einem Container auf einem Host bereitstellen, z. B. auf einem lokalen Computer oder einer Instance in Amazon Elastic Compute Cloud (Amazon EC2). Nachdem der Bot bereitgestellt wurde, können Sie ihn so konfigurieren, dass er Daten lokal oder in einem Amazon Simple Storage Service (Amazon S3) -Bucket speichert. Sie können den Datenaufbewahrungs-Bot auch so konfigurieren, dass er andere AWS Dienste wie AWS Secrets Manager (Secrets Manager), Amazon CloudWatch (CloudWatch), Amazon Simple Notification Service (Amazon SNS) und AWS Key Management Service (AWS KMS) verwendet. In den folgenden Themen wird beschrieben, wie Sie den Datenaufbewahrungs-Bot für Ihr Wickr-Netzwerk konfigurieren und ausführen.

Für Produktionsbereitstellungen des Wickr Data Retention (DR) Bot AWS empfiehlt sich die Bereitstellung auf Amazon EC2/Amazon EBS mit in Amazon S3 archivierten Nachrichten und der folgenden Mindestinstanz- und Speichergröße:

- Instance-Typ: m8i.large (8 GiB RAM, 2 vCPUs)
- Speicher: 1 TB Amazon EBS-Volumen
- Bereitstellung: Eine DR-Bot-Instanz pro Amazon EC2 EC2-Host

Weitere Informationen zu Amazon EBS finden Sie unter Amazon EBS-Snapshot-Lebenszyklus im Amazon EBS-Benutzerhandbuch.

Topics

Voraussetzungen für die Konfiguration der Datenspeicherung für AWS Wickr

Dies setzt voraus, dass bereits eine Amazon EC2 EC2-Instance mit den oben aufgeführten Mindestspeicheranforderungen läuft und Ihre VPC den Wickr-Messaging-Endpunkt erreichen kann:

`com.amazonaws.`*`region`*`.wickr-messaging`— Der Bot empfängt Nachrichten vom Wickr-Messaging-Dienst.

Bevor Sie beginnen, führen Sie das folgende Verfahren aus, um die Datenspeicherung in der Konsole zu aktivieren.

1. Öffnen Sie sie AWS-Managementkonsole für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Netzwerkrichtlinien aus.
4. Wählen Sie auf der Seite Netzwerkrichtlinien im Abschnitt Datenspeicherung die Option Bearbeiten aus.
5. Folgen Sie auf der Seite Datenspeicherung bearbeiten den Schritten 1 und 2.
6. Starten Sie Ihren Datenaufbewahrungs-Bot. Weitere Informationen finden Sie unter Starten Sie den Datenaufbewahrungsbot für Ihr Wickr-Netzwerk.
7. Kopieren Sie im Abschnitt Konfigurieren Sie Ihren Datenaufbewahrungsserver den Benutzernamen und das Anfangspasswort. Konfigurieren Sie Ihren Datenaufbewahrungs-Bot mit dem Benutzernamen und dem Anfangspasswort, indem Sie wie folgt vorgehen: Passwort für den Datenaufbewahrungs-Bot in AWS Wickr.
8. Aktivieren Sie das Kontrollkästchen Datenspeicherung aktivieren und wählen Sie dann Änderungen speichern aus.

> **Note**
>
> Der DR-Bot wurde für die kontinuierliche Verarbeitung von etwa 11.000 Nachrichten pro Stunde (~3 messages/second) validiert. Für Workloads, die diesen Durchsatz ständig überschreiten oder voraussichtlich 1,5 Millionen Nachrichten in einem einzigen Verarbeitungslauf überschreiten, sollten zusätzliche Skalierungsstrategien geprüft werden.

Für Disaster Recovery empfehlen wir Snapshot Lifecycles auf den Amazon EBS-Volumes und Amazon S3 Replication. Cross-Region Um zu konfigurieren, wie oft Nachrichten an Amazon S3 gesendet werden, können Sie die Umgebungsvariable WICKRIO_COMP_FILESIZE oder die Rotation `WICKRIO_COMP_TIMEROTATE` nach Größe oder Zeit festlegen. Nachrichtenprotokolle und Dateianhänge werden unter demselben Präfix im selben Bucket zugestellt. Weitere Informationen finden Sie unter Umgebungsvariablen zur Konfiguration des Datenaufbewahrungsbots in AWS Wickr.

Passwort für den Datenaufbewahrungsbot in AWS Wickr

Wenn Sie den Datenaufbewahrungs-Bot zum ersten Mal starten, geben Sie das anfängliche Passwort mit einer der folgenden Optionen an:

- Die `WICKRIO_BOT_PASSWORD`-Umgebungsvariable Die Umgebungsvariablen für den Datenaufbewahrungs-Bot werden im Umgebungsvariablen zur Konfiguration des Datenaufbewahrungsbots in AWS Wickr Abschnitt weiter unten in diesem Handbuch beschrieben.
- Der Passwortwert in Secrets Manager, der durch die `AWS_SECRET_NAME` Umgebungsvariable identifiziert wird. Die Secrets Manager Manager-Werte für den Datenaufbewahrungs-Bot werden im Secrets Manager Manager-Werte für AWS Wickr Abschnitt weiter unten in diesem Handbuch beschrieben.
- Geben Sie das Passwort ein, wenn Sie vom Datenaufbewahrungs-Bot dazu aufgefordert werden. Sie müssen den Datenaufbewahrungs-Bot mit interaktivem TTY-Zugriff mithilfe der `-ti` Option ausführen.

Ein neues Passwort wird generiert, wenn Sie den Datenaufbewahrungs-Bot zum ersten Mal konfigurieren. Wenn Sie den Datenaufbewahrungs-Bot erneut installieren müssen, verwenden Sie das generierte Passwort. Das ursprüngliche Passwort ist nach der Erstinstallation des Datenaufbewahrungsbots nicht gültig. Sie können das generierte Passwort rotieren. Um das generierte Passwort zu rotieren, folgen Sie den Anweisungen in den folgenden Abschnitten.

Rotation des Passworts

Der Datenaufbewahrungs-Bot (Mindestversion 6.66.01.00) kann das Passwort seines Wickr-Kontos beim Start programmgesteuert rotieren, indem er die Umgebungsvariable WICKRIO_ROTATE_PASSWORD setzt.

Usage

Setzen Sie die Umgebungsvariable WICKRIO_ROTATE_PASSWORD, wenn Sie den Bot mit Docker Run starten:

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

Beim Start, nachdem sich der Bot erfolgreich mit seinem aktuellen Passwort (von WICKRIO_BOT_PASSWORD oder AWS Secrets Manager) angemeldet hat, macht er Folgendes:

1. Lesen Sie WICKRIO_ROTATE_PASSWORD aus der Prozessumgebung.
2. Bestätigen Sie das neue Passwort (mindestens 12 Zeichen, muss sich vom aktuellen Passwort unterscheiden).
3. Rufen Sie den AWS Wickr-Service auf, um das Passwort zu wechseln.

Aktualisieren Sie WICKRIO_BOT_PASSWORD (oder das Secret in AWS Secrets Manager) nach einer erfolgreichen Rotation vor dem nächsten Neustart auf das neue Passwort.

Das neu generierte Passwort wird wie im folgenden Beispiel angezeigt.

> **Important**
>
> Bewahren Sie das Passwort an einem sicheren Ort auf. Wenn Sie das Passwort verlieren, können Sie den Datenaufbewahrungsbot nicht erneut installieren. Teilen Sie dieses Passwort nicht mit anderen. Es bietet die Möglichkeit, die Datenspeicherung für Ihr Wickr-Netzwerk zu starten.

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

Passwortanforderungen

- Das neue Passwort muss mindestens 12 Zeichen lang sein.
- Das neue Passwort muss sich vom aktuellen Passwort unterscheiden.
- Der Bot muss sich zuerst mit dem aktuellen Passwort anmelden können.

Speicheroptionen für das AWS Wickr-Netzwerk

Nachdem die Datenspeicherung aktiviert und der Datenaufbewahrungs-Bot für Ihr Wickr-Netzwerk konfiguriert wurde, erfasst er alle Nachrichten und Dateien, die innerhalb Ihres Netzwerks gesendet werden. Nachrichten werden in Dateien gespeichert, die auf eine bestimmte Größe oder ein bestimmtes Zeitlimit begrenzt sind, das mithilfe einer Umgebungsvariablen konfiguriert werden kann. Weitere Informationen finden Sie unter Umgebungsvariablen zur Konfiguration des Datenaufbewahrungsbots in AWS Wickr.

Sie können eine der folgenden Optionen zum Speichern dieser Daten konfigurieren:

- Speichern Sie alle erfassten Nachrichten und Dateien lokal. Dies ist die Standardoption. Es liegt in Ihrer Verantwortung, lokale Dateien zur Langzeitspeicherung auf ein anderes System zu verschieben und sicherzustellen, dass der Hostfestplatte nicht zu wenig Arbeitsspeicher oder Speicherplatz zur Verfügung steht.
- Speichern Sie alle erfassten Nachrichten und Dateien in einem Amazon S3 S3-Bucket. Der Datenaufbewahrungs-Bot speichert alle entschlüsselten Nachrichten und Dateien in dem von Ihnen angegebenen Amazon S3 S3-Bucket. Die erfassten Nachrichten und Dateien werden vom Host-Computer entfernt, nachdem sie erfolgreich im Bucket gespeichert wurden.
- Speichern Sie alle erfassten Nachrichten und Dateien verschlüsselt in einem Amazon S3 S3-Bucket. Der Datenaufbewahrungs-Bot verschlüsselt alle erfassten Nachrichten und Dateien mit einem von Ihnen angegebenen Schlüssel erneut und speichert sie in dem von Ihnen angegebenen Amazon S3 S3-Bucket. Die erfassten Nachrichten und Dateien werden vom Host-Computer entfernt, nachdem sie erfolgreich erneut verschlüsselt und im Bucket gespeichert wurden. Sie benötigen Software, um die Nachrichten und Dateien zu entschlüsseln.

  Weitere Informationen zur Erstellung eines Amazon S3 S3-Buckets zur Verwendung mit Ihrem Datenaufbewahrungs-Bot finden Sie unter Erstellen eines Buckets im Amazon S3 S3-Benutzerhandbuch

Umgebungsvariablen zur Konfiguration des Datenaufbewahrungsbots in AWS Wickr

Sie können die folgenden Umgebungsvariablen verwenden, um den Datenaufbewahrungs-Bot zu konfigurieren. Sie legen diese Umgebungsvariablen mithilfe der `-e` Option fest, wenn Sie das Docker-Image des Datenaufbewahrungs-Bots ausführen. Weitere Informationen finden Sie unter Starten Sie den Datenaufbewahrungs-Bot für Ihr Wickr-Netzwerk.

> **Note**
>
> Diese Umgebungsvariablen sind optional, sofern nicht anders angegeben.

Verwenden Sie die folgenden Umgebungsvariablen, um die Anmeldeinformationen für den Datenaufbewahrungs-Bot anzugeben:

- `WICKRIO_BOT_NAME`— Der Name des Datenaufbewahrungsbots. Diese Variable ist erforderlich, wenn Sie das Docker-Image des Datenaufbewahrungs-Bot ausführen.
- `WICKRIO_BOT_PASSWORD`— Das ursprüngliche Passwort für den Datenaufbewahrungs-Bot. Weitere Informationen finden Sie unter Voraussetzungen für die Konfiguration der Datenspeicherung für AWS Wickr. Diese Variable ist erforderlich, wenn Sie nicht vorhaben, den Datenaufbewahrungs-Bot mit einer Passwortabfrage zu starten, oder wenn Sie nicht beabsichtigen, Secrets Manager zum Speichern der Anmeldeinformationen für den Datenaufbewahrungs-Bot zu verwenden.

Verwenden Sie die folgenden Umgebungsvariablen, um die Standard-Streaming-Funktionen zur Datenspeicherung zu konfigurieren:

- `WICKRIO_COMP_MESGDEST`— Der Pfadname zu dem Verzeichnis, in dem Nachrichten gestreamt werden. Der Standardwert ist `/tmp/<botname>/compliance/messages`.
- `WICKRIO_COMP_FILEDEST`— Der Pfadname zu dem Verzeichnis, in dem Dateien gestreamt werden. Der Standardwert ist `/tmp/<botname>/compliance/attachments`.
- `WICKRIO_COMP_BASENAME`— Der Basisname für die Dateien mit empfangenen Nachrichten. Der Standardwert ist `receivedMessages`.
- `WICKRIO_COMP_FILESIZE`— Die maximale Dateigröße für eine Datei mit empfangenen Nachrichten in Kibibyte (KiB). Eine neue Datei wird gestartet, wenn die maximale Größe erreicht ist. Der Standardwert ist`1000000000`, wie bei 1024 GiB.
- `WICKRIO_COMP_TIMEROTATE`— Die Zeitspanne in Minuten, für die der Datenaufbewahrungs-Bot empfangene Nachrichten in einer Datei mit empfangenen Nachrichten ablegt. Der Standardwert ist `0` „ohne Rotation“. Diese Variable ist erforderlich, wenn Amazon S3 für die Datenspeicherung verwendet wird. Ohne diesen Wert werden Nachrichtendateien niemals rotiert und daher auch nicht an Amazon S3 zugestellt. Ein empfohlener Startwert ist `10` Minuten. Sie können diesen Wert an Ihr Nachrichtenvolumen und Ihre Zustellungsanforderungen anpassen.

Verwenden Sie die folgende Umgebungsvariable, um den zu verwendenden Standard AWS-Region zu definieren.

- `AWS_DEFAULT_REGION`— Die Standardeinstellung AWS-Region für AWS Dienste wie Secrets Manager (wird nicht für Amazon S3 oder verwendet AWS KMS). Die `us-east-1` Region wird standardmäßig verwendet, wenn diese Umgebungsvariable nicht definiert ist.

Verwenden Sie die folgenden Umgebungsvariablen, um das Secrets Manager-Geheimnis anzugeben, das verwendet werden soll, wenn Sie sich dafür entscheiden, Secrets Manager zum Speichern der Anmeldeinformationen und AWS Dienstinformationen für den Datenaufbewahrungs-Bot zu verwenden. Weitere Informationen zu den Werten, die Sie in Secrets Manager speichern können, finden Sie unterSecrets Manager Manager-Werte für AWS Wickr.

- `AWS_SECRET_NAME`— Der Name des Secrets Manager Manager-Geheimnisses, das die Anmeldeinformationen und AWS Serviceinformationen enthält, die der Datenaufbewahrungsbot benötigt.
- `AWS_SECRET_REGION`— Der AWS-Region , in dem sich das AWS Geheimnis befindet. Wenn Sie AWS Geheimnisse verwenden und dieser Wert nicht definiert ist, wird der `AWS_DEFAULT_REGION` Wert verwendet.

> **Note**
>
> Sie können alle folgenden Umgebungsvariablen als Werte in Secrets Manager speichern. Wenn Sie sich für die Verwendung von Secrets Manager entscheiden und diese Werte dort speichern, müssen Sie sie nicht als Umgebungsvariablen angeben, wenn Sie das Docker-Image des Datenaufbewahrungsbots ausführen. Sie müssen nur die zuvor in diesem Handbuch beschriebene `AWS_SECRET_NAME` Umgebungsvariable angeben. Weitere Informationen finden Sie unter Secrets Manager Manager-Werte für AWS Wickr.

Verwenden Sie die folgenden Umgebungsvariablen, um den Amazon S3 S3-Bucket anzugeben, wenn Sie Nachrichten und Dateien in einem Bucket speichern möchten.

- `WICKRIO_S3_BUCKET_NAME`— Der Name des Amazon S3 S3-Buckets, in dem Nachrichten und Dateien gespeichert werden.

- `WICKRIO_S3_REGION`— Die AWS Region des Amazon S3 S3-Buckets, in der Nachrichten und Dateien gespeichert werden.
- `WICKRIO_S3_FOLDER_NAME`— Der optionale Ordnername im Amazon S3 S3-Bucket, in dem Nachrichten und Dateien gespeichert werden. Diesem Ordnernamen wird der Schlüssel für Nachrichten und Dateien vorangestellt, die im Amazon S3 S3-Bucket gespeichert sind.

Verwenden Sie die folgenden Umgebungsvariablen, um die AWS KMS Details anzugeben, wenn Sie sich für die Verwendung der clientseitigen Verschlüsselung entscheiden, um Dateien erneut zu verschlüsseln, wenn Sie sie in einem Amazon S3 S3-Bucket speichern.

- `WICKRIO_KMS_MSTRKEY_ARN`— Der Amazon-Ressourcenname (ARN) des AWS KMS Hauptschlüssels, der zum erneuten Verschlüsseln der Nachrichtendateien und Dateien auf dem Datenaufbewahrungs-Bot verwendet wird, bevor sie im Amazon S3-Bucket gespeichert werden.
- `WICKRIO_KMS_REGION`— Die AWS Region, in der sich der AWS KMS Hauptschlüssel befindet.

Verwenden Sie die folgende Umgebungsvariable, um die Amazon SNS SNS-Details anzugeben, wenn Sie Datenaufbewahrungsereignisse an ein Amazon SNS SNS-Thema senden möchten. Zu den gesendeten Ereignissen gehören Start- und Shutdown-Ereignisse sowie Fehlerbedingungen.

- `WICKRIO_SNS_TOPIC_ARN`— Der ARN des Amazon SNS SNS-Themas, an das Datenaufbewahrungsereignisse gesendet werden sollen.

Verwenden Sie die folgende Umgebungsvariable, um Messdaten zur Datenspeicherung zu CloudWatch senden. Falls angegeben, werden die Metriken alle 60 Sekunden generiert.

- `WICKRIO_METRICS_TYPE`— Legen Sie den Wert dieser Umgebungsvariablen auf fest, `cloudwatch` an die Metriken gesendet CloudWatch werden sollen.

Secrets Manager Manager-Werte für AWS Wickr

Sie können Secrets Manager verwenden, um die Anmeldeinformationen und AWS Serviceinformationen für den Datenaufbewahrungs-Bot zu speichern. Weitere Informationen zum Erstellen eines Secrets Manager Manager-Geheimnisses finden Sie unter Create an AWS Secrets Manager Secret im Secrets Manager Manager-Benutzerhandbuch.

Das Secrets Manager Manager-Geheimnis kann die folgenden Werte haben:

- `password`— Das Passwort für den Datenaufbewahrungs-Bot.
- `s3_bucket_name`— Der Name des Amazon S3 S3-Buckets, in dem Nachrichten und Dateien gespeichert werden. Wenn nicht festgelegt, wird das Standard-Datei-Streaming verwendet.
- `s3_region`— Die AWS Region des Amazon S3 S3-Buckets, in der Nachrichten und Dateien gespeichert werden.
- `s3_folder_name`— Der optionale Ordnername im Amazon S3 S3-Bucket, in dem Nachrichten und Dateien gespeichert werden. Diesem Ordnernamen wird der Schlüssel für Nachrichten und Dateien vorangestellt, die im Amazon S3 S3-Bucket gespeichert sind.
- `kms_master_key_arn`— Der ARN des AWS KMS Hauptschlüssels, der verwendet wird, um die Nachrichtendateien und Dateien auf dem Datenaufbewahrungs-Bot erneut zu verschlüsseln, bevor sie im Amazon S3 S3-Bucket gespeichert werden.
- `kms_region`— Die AWS Region, in der sich der AWS KMS Masterschlüssel befindet.
- `sns_topic_arn`— Der ARN des Amazon SNS SNS-Themas, an das Datenaufbewahrungsereignisse gesendet werden sollen.

IAM-Richtlinie zur Verwendung der Datenspeicherung mit AWS service

Wenn Sie planen, andere AWS Dienste mit dem Wickr-Datenaufbewahrungs-Bot zu verwenden, müssen Sie sicherstellen, dass der Host über die entsprechende AWS Identity and Access Management (IAM-) Rolle und die entsprechende Richtlinie für den Zugriff auf diese Dienste verfügt. Sie können den Datenaufbewahrungs-Bot so konfigurieren, dass er Secrets Manager, Amazon S3 CloudWatch, Amazon SNS und AWS KMS verwendet. Die folgende IAM-Richtlinie ermöglicht den Zugriff auf bestimmte Aktionen für diese Dienste.

JSON

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

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

Sie können eine strengere IAM-Richtlinie erstellen, indem Sie die spezifischen Objekte für jeden Dienst identifizieren, auf die Sie den Containern auf Ihrem Host Zugriff gewähren möchten. Entfernen Sie die Aktionen für die AWS Dienste, die Sie nicht verwenden möchten. Wenn Sie beispielsweise nur einen Amazon S3 S3-Bucket verwenden möchten, verwenden Sie die folgende Richtlinie, mit der die `cloudwatch:PutMetricData` Aktionen`secretsmanager:GetSecretValue`, `sns:Publishkms:GenerateDataKey`, und entfernt werden.

JSON

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

Wenn Sie eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance verwenden, um Ihren Datenaufbewahrungs-Bot zu hosten, erstellen Sie eine IAM-Rolle unter Verwendung des Amazon EC2-Standardfalls und weisen Sie eine Richtlinie mithilfe der Richtliniendefinition von oben zu.

Starten Sie den Datenaufbewahrungs-Bot für Ihr Wickr-Netzwerk

Bevor Sie den Datenaufbewahrungs-Bot ausführen, sollten Sie festlegen, wie Sie ihn konfigurieren möchten. Wenn Sie den Bot auf einem Host ausführen möchten, der:

- Sie werden keinen Zugriff auf AWS Dienste haben, dann sind Ihre Optionen begrenzt. In diesem Fall verwenden Sie die Standardoptionen für das Nachrichtenstreaming. Sie sollten entscheiden,

ob Sie die Größe der erfassten Nachrichtendateien auf eine bestimmte Größe oder ein bestimmtes Zeitintervall beschränken möchten. Weitere Informationen finden Sie unter Umgebungsvariablen zur Konfiguration des Datenaufbewahrungsbots in AWS Wickr.

- Wenn Sie Zugriff auf AWS Dienste haben, sollten Sie ein Secrets Manager Manager-Geheimnis erstellen, um die Bot-Anmeldeinformationen und die AWS Dienstkonfigurationsdetails zu speichern. Nachdem die AWS Dienste konfiguriert wurden, können Sie mit dem Starten des Docker-Images für den Datenaufbewahrungs-Bot fortfahren. Weitere Informationen zu den Details, die Sie in einem Secrets Manager Manager-Secret speichern können, finden Sie unter Secrets Manager Manager-Werte für AWS Wickr

Die folgenden Abschnitte enthalten Beispielbefehle zum Ausführen des Docker-Images des Datenaufbewahrungs-Bot. Ersetzen Sie in jedem der Beispielbefehle die folgenden Beispielwerte durch Ihre eigenen:

- *compliance_1234567890_bot*mit dem Namen Ihres Datenaufbewahrungsbots.
- *password*mit dem Passwort für Ihren Datenaufbewahrungsbot.
- *wickr/data/retention/bot*mit dem Namen Ihres Secrets Manager Manager-Geheimnisses, das Sie mit Ihrem Datenaufbewahrungs-Bot verwenden möchten.
- *bucket-name*mit dem Namen des Amazon S3 S3-Buckets, in dem Nachrichten und Dateien gespeichert werden.
- *folder-name*mit dem Ordnernamen im Amazon S3 S3-Bucket, in dem Nachrichten und Dateien gespeichert werden.
- *us-east-1*mit der AWS Region der Ressource, die Sie angeben. Zum Beispiel die Region des AWS KMS Hauptschlüssels oder die Region des Amazon S3 S3-Buckets.
- *arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-a617-abababababab*mit dem Amazon-Ressourcennamen (ARN) Ihres AWS KMS Hauptschlüssels, der zum erneuten Verschlüsseln von Nachrichtendateien und Dateien verwendet werden soll.

Starten Sie den Bot mit der Umgebungsvariablen Passwort (nein). AWS Dienst)

Der folgende Docker-Befehl startet den Datenaufbewahrungs-Bot. Das Passwort wird mithilfe der `WICKRIO_BOT_PASSWORD` Umgebungsvariablen angegeben. Der Bot verwendet zunächst das Standard-Datei-Streaming und verwendet die im Umgebungsvariablen zur Konfiguration des Datenaufbewahrungsbots in AWS Wickr Abschnitt dieses Handbuchs definierten Standardwerte.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud:latest
```

Starten Sie den Bot mit einer Passwortabfrage (nein). AWS Dienst)

Der folgende Docker-Befehl startet den Datenaufbewahrungs-Bot. Das Passwort wird eingegeben, wenn der Datenaufbewahrungs-Bot dazu auffordert. Es wird zunächst das Standard-Datei-Streaming mit den im Umgebungsvariablen zur Konfiguration des Datenaufbewahrungsbots in AWS Wickr Abschnitt dieses Handbuchs definierten Standardwerten verwendet.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud:latest

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

Führen Sie den Bot mit der `-ti` Option aus, um die Passwortabfrage zu erhalten. Sie sollten den `docker attach <container ID or container name>` Befehl auch unmittelbar nach dem Start des Docker-Images ausführen, damit Sie die Passwortabfrage erhalten. Sie sollten beide Befehle in einem Skript ausführen. Wenn Sie eine Verbindung zum Docker-Image herstellen und die Aufforderung nicht sehen, drücken Sie die Eingabetaste. Die Eingabeaufforderung wird angezeigt.

Starten Sie den Bot mit einer 10-minütigen Rotation der Nachrichtendatei (nein). AWS Dienst)

Der folgende Docker-Befehl startet den Datenaufbewahrungs-Bot mithilfe von Umgebungsvariablen. Es konfiguriert ihn auch so, dass die empfangenen Nachrichtendateien auf 10 Minuten rotiert werden.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
-e WICKRIO_COMP_TIMEROTATE=10 \
```

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

Starten Sie den Bot und geben Sie das Anfangspasswort mit Secrets Manager an

Sie können den Secrets Manager verwenden, um das Passwort des Datenaufbewahrungsbots zu identifizieren. Wenn Sie den Datenaufbewahrungs-Bot starten, müssen Sie eine Umgebungsvariable festlegen, die den Secrets Manager angibt, in dem diese Informationen gespeichert werden.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e AWS_SECRET_NAME='wickrpro/alpha/new-3-bot' \
public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud:latest
```

Das `wickrpro/compliance/compliance_1234567890_bot` Geheimnis enthält den folgenden geheimen Wert, der als Klartext angezeigt wird.

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

Starten Sie den Bot und konfigurieren Sie Amazon S3 mit Secrets Manager

Sie können den Secrets Manager verwenden, um die Anmeldeinformationen und die Amazon S3 S3-Bucket-Informationen zu hosten. Wenn Sie den Datenaufbewahrungs-Bot starten, müssen Sie eine Umgebungsvariable festlegen, die den Secrets Manager angibt, in dem diese Informationen gespeichert werden.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
 -e AWS_SECRET_NAME='wickrpro/alpha/compliance_1234567890_bot' \
 -e WICKRIO_COMP_TIMEROTATE=10 \
public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud:latest
```

Das `wickrpro/compliance/compliance_1234567890_bot` Geheimnis enthält den folgenden geheimen Wert, der als Klartext angezeigt wird.

```
{
```

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

Nachrichten und Dateien, die vom Bot empfangen werden, werden im `bot-compliance` Bucket im angegebenen Ordner abgelegt. `network1234567890`

Starten Sie den Bot und konfigurieren Sie Amazon S3 und AWS KMS mit Secrets Manager

Sie können den Secrets Manager verwenden, um die Anmeldeinformationen, den Amazon S3 S3-Bucket und die AWS KMS Master-Key-Informationen zu hosten. Wenn Sie den Datenaufbewahrungs-Bot starten, müssen Sie eine Umgebungsvariable festlegen, die den Secrets Manager angibt, in dem diese Informationen gespeichert werden.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
 -e AWS_SECRET_NAME='wickrpro/alpha/compliance_1234567890_bot' \
 -e WICKRIO_COMP_TIMEROTATE=10 \
public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud:latest
```

Das `wickrpro/compliance/compliance_1234567890_bot` Geheimnis enthält den folgenden geheimen Wert, der als Klartext angezeigt wird.

```
{
    "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"
}
```

Vom Bot empfangene Nachrichten und Dateien werden mit dem KMS-Schlüssel verschlüsselt, der durch den ARN-Wert identifiziert wird, und dann in den Bucket „bot-compliance“ im Ordner mit dem Namen „network1234567890“ verschoben. Stellen Sie sicher, dass Sie die entsprechende IAM-Richtlinie eingerichtet haben.

Starten Sie den Bot und konfigurieren Sie Amazon S3 mithilfe von Umgebungsvariablen

Wenn Sie Secrets Manager nicht zum Hosten der Anmeldeinformationen für den Datenaufbewahrungs-Bot verwenden möchten, können Sie das Docker-Image für den Datenaufbewahrungs-Bot mit den folgenden Umgebungsvariablen starten. Sie müssen den Namen des Datenaufbewahrungsbots mithilfe der `WICKRIO_BOT_NAME` Umgebungsvariablen identifizieren.

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
-e WICKRIO_COMP_TIMEROTATE=10 \
-e WICKRIO_S3_BUCKET_NAME='bot-compliance' \
-e WICKRIO_S3_FOLDER_NAME='network1234567890' \
-e WICKRIO_S3_REGION='us-east-1' \
public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud:latest
```

Sie können Umgebungswerte verwenden, um die Anmeldeinformationen des Datenaufbewahrungsbots, Informationen zu Amazon S3 S3-Buckets und Konfigurationsinformationen für das Standard-Datei-Streaming zu identifizieren.

Stoppen Sie den Datenaufbewahrungsbot für Ihr Wickr-Netzwerk

Die Software, die auf dem Datenaufbewahrungs-Bot ausgeführt wird, erfasst `SIGTERM` Signale und wird ordnungsgemäß heruntergefahren. Verwenden Sie den `docker stop` *`<container ID or container name>`* Befehl, wie im folgenden Beispiel gezeigt, um den `SIGTERM` Befehl an das Docker-Image des Datenaufbewahrungsbots auszugeben.

```
docker stop compliance_1234567890_bot
```

Holen Sie sich die Datenaufbewahrungsprotokolle für Ihr Wickr-Netzwerk

Die Software, die auf dem Docker-Image des Datenaufbewahrungsbots ausgeführt wird, wird in Protokolldateien im `/tmp/`*`<botname>`*`/logs` Verzeichnis ausgegeben. Sie werden auf maximal 5 Dateien rotiert. Sie können die Protokolle abrufen, indem Sie den folgenden Befehl ausführen.

```
docker logs <botname>
```

Beispiel:

```
docker logs compliance_1234567890_bot
```

Metriken und Ereignisse zur Datenspeicherung für Ihr Wickr-Netzwerk

Im Folgenden finden Sie die Amazon CloudWatch (CloudWatch) -Metriken und Amazon Simple Notification Service (Amazon SNS) -Ereignisse, die derzeit von der Version 5.116 des AWS Wickr-Datenaufbewahrungsbots unterstützt werden.

Topics

CloudWatch Metriken für Ihr Wickr-Netzwerk

Metriken werden vom Bot in Intervallen von 1 Minute generiert und an den CloudWatch Dienst übertragen, der dem Konto zugeordnet ist, auf dem das Docker-Image des Datenaufbewahrungs-Bot läuft.

Im Folgenden sind die vorhandenen Metriken aufgeführt, die vom Datenaufbewahrungs-Bot unterstützt werden.

Metrik	Description
Messages_Rx	Empfangene Nachrichten.
Messages_Rx_Failed	Fehler bei der Verarbeitung empfangener Nachrichten.
Messages_Saved	Nachrichten, die in der Datei mit empfangenen Nachrichten gespeichert wurden.
Messages_Saved_Failed	Fehler beim Speichern von Nachrichten in der Datei mit empfangenen Nachrichten.
Files_Saved	Empfangene Dateien.
Files_Saved_Bytes	Anzahl der Byte für empfangene Dateien.

Metrik	Description
Files_Saved_Failed	Fehler beim Speichern von Dateien.
Anmeldungen	Anmeldungen (normalerweise ist dies 1 für jedes Intervall).
Login_Failures	Fehler bei der Anmeldung (normalerweise ist dies 1 für jedes Intervall).
S3_ Post_Errors	Fehler beim Posten von Nachrichtendateien und Dateien in den Amazon S3 S3-Bucket.
Watchdog_Failures	Watchdog-Fehler.
Watchdog_Warnings	Watchdog-Warnungen.

Metriken werden generiert, um von CloudWatch verwendet zu werden. Der für Bots verwendete Namespace ist`WickrIO`. Jede Metrik hat eine Reihe von Dimensionen. Im Folgenden finden Sie eine Liste der Dimensionen, die zusammen mit den oben genannten Metriken veröffentlicht werden.

Dimension	Wert
Id	Der Benutzername des Bots.
Gerät	Beschreibung eines bestimmten Bot-Gerät s oder einer bestimmten Instanz. Nützlich, wenn Sie mehrere Bot-Geräte oder -Instanzen ausführen.
Produkt	Das Produkt für den Bot. Kann `WickrEnte rprise_` mit `AlphaBeta`, `WickrPro_` oder `Production` angehängt werden.
BotType	Der Bot-Typ. Für die Compliance-Bots als Compliance gekennzeichnet.
Netzwerk	Die ID des zugehörigen Netzwerks.

Amazon SNS SNS-Ereignisse für Ihr Wickr-Netzwerk

Die folgenden Ereignisse werden im Amazon SNS SNS-Thema veröffentlicht, das durch den Amazon Resource Name (ARN) -Wert definiert ist, der mithilfe der `WICKRIO_SNS_TOPIC_ARN` Umgebungsvariablen oder des geheimen `sns_topic_arn` Secrets Manager Manager-Werts identifiziert wurde. Weitere Informationen erhalten Sie unter Umgebungsvariablen zur Konfiguration des Datenaufbewahrungsbots in AWS Wickr und Secrets Manager Manager-Werte für AWS Wickr.

Vom Datenaufbewahrungs-Bot generierte Ereignisse werden als JSON-Zeichenfolgen gesendet. Die folgenden Werte sind ab Version 5.116 des Datenaufbewahrungsbots in den Ereignissen enthalten.

Name	Wert
ComplianceBot	Der Benutzername des Datenaufbewahrungs bots.
DataTime	Das Datum und die Uhrzeit, an dem das Ereignis eingetreten ist.
Gerät	Eine Beschreibung des spezifischen Bot-Geräts oder der jeweiligen Bot-Instanz. Nützlich, wenn Sie mehrere Bot-Instanzen ausführen.
DockerImage	Das mit dem Bot verknüpfte Docker-Image.
DockerTag	Das Tag oder die Version des Docker-Images.
Nachricht	Die Ereignisnachricht. Weitere Informationen finden Sie unter Kritische Ereignisse und Normale Ereignisse.
notificationType	Dieser Wert wird sein`Bot Event`.
severity	Der Schweregrad des Ereignisses. Kann `normal` oder `critical` sein.

Sie müssen das Amazon SNS SNS-Thema abonnieren, damit Sie die Ereignisse erhalten können. Wenn Sie sich mit einer E-Mail-Adresse anmelden, erhalten Sie eine E-Mail mit Informationen, die dem folgenden Beispiel ähneln.

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

Kritische Ereignisse

Diese Ereignisse führen dazu, dass der Bot gestoppt oder neu gestartet wird. Die Anzahl der Neustarts ist begrenzt, um andere Probleme zu vermeiden.

Fehler bei der Anmeldung

Im Folgenden sind die möglichen Ereignisse aufgeführt, die generiert werden können, wenn sich der Bot nicht anmelden kann. In jeder Nachricht wird der Grund für den Anmeldefehler angegeben.

Ereignistyp	Ereignismeldung
Anmeldung fehlgeschlagen	Schlechte Anmeldeinformationen. Überprüfe das Passwort.
Anmeldung fehlgeschlagen	Benutzer wurde nicht gefunden.
Anmeldung fehlgeschlagen	Konto oder Gerät ist gesperrt.
Bereitstellung	Der Benutzer hat den Befehl beendet.
Bereitstellung	Falsches Passwort für die `config.wickr` Datei.
Bereitstellung	Die `config.wickr` Datei kann nicht gelesen werden.
Anmeldung fehlgeschlagen	Alle Anmeldungen sind fehlgeschlagen.

Ereignistyp	Ereignismeldung
Anmeldung fehlgeschlagen	Neuer Benutzer, aber die Datenbank ist bereits vorhanden.

Weitere kritische Ereignisse

Ereignistyp	Ereignismeldungen
Konto gesperrt	WickrIOClientMain: :slotAdminUserSuspend: code (%1): Grund: %2“
BotDevice Suspendiert	Gerät ist gesperrt!
WatchDog	Das SwitchBoard System ist länger als < *N* > Minuten ausgefallen
S3-Ausfälle	Die Datei < *file-name* ≫ konnte nicht in den S3-Bucket gelegt werden. Fehler: < *AWS-error* >
Ausweichschlüssel	VOM SERVER ÜBERMITTELTER FALLBACK-SCHLÜSSEL: Ist kein anerkannter aktiver Fallbackschlüssel für den Client. Bitte senden Sie die Protokolle an Desktop Engineering.

Normale Ereignisse

Im Folgenden sind die Ereignisse aufgeführt, die Sie vor normalen Betriebsereignissen warnen. Zu viele Ereignisse dieser Art innerhalb eines bestimmten Zeitraums können Anlass zur Sorge geben.

Gerät wurde dem Konto hinzugefügt

Dieses Ereignis wird generiert, wenn dem Bot-Konto für die Datenspeicherung ein neues Gerät hinzugefügt wird. Unter bestimmten Umständen kann dies ein wichtiger Hinweis darauf sein, dass jemand eine Instanz des Datenaufbewahrungsbots erstellt hat. Im Folgenden finden Sie die Nachricht zu dieser Veranstaltung.

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

Bot angemeldet

Dieses Ereignis wird generiert, wenn sich der Bot erfolgreich angemeldet hat. Es folgt die Nachricht für dieses Ereignis.

```
Logged in
```

Wird heruntergefahren

Dieses Ereignis wird generiert, wenn der Bot heruntergefahren wird. Wenn der Benutzer dies nicht explizit initiiert hat, könnte dies ein Hinweis auf ein Problem sein. Im Folgenden finden Sie die Nachricht für dieses Ereignis.

```
Shutting down
```

Updates verfügbar

Dieses Ereignis wird generiert, wenn der Datenaufbewahrungs-Bot gestartet wird, und es identifiziert, dass eine neuere Version des zugehörigen Docker-Images verfügbar ist. Dieses Ereignis wird generiert, wenn der Bot gestartet wird, und zwar täglich. Dieses Ereignis umfasst das `versions` Array-Feld, das die neuen verfügbaren Versionen identifiziert. Im Folgenden finden Sie ein Beispiel dafür, wie dieses Ereignis aussieht.

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

Sicherheitsüberlegungen

Prüfen Sie sorgfältig, wo und wie ein Datenaufbewahrungs-Bot eingesetzt werden soll. Diese Bots sammeln und entschlüsseln zentral alle von Benutzern gesendeten oder empfangenen Ende-zu-Ende-verschlüsselten Nachrichten und konsolidieren so Inhalte, auf die zuvor nur auf einzelnen Geräten zugegriffen werden konnte. Daher haben diese Komponente und ihr Datenspeicher einen außergewöhnlich hohen Sicherheitswert.

Wenn Sie einen Bot zur Datenspeicherung einsetzen, stellen Sie sicher, dass er die höchsten Sicherheitsstandards erfüllt und den Sicherheitsrichtlinien Ihres Unternehmens entspricht. Folgen Sie bei Bereitstellungen mithilfe von AWS Services den zusätzlichen Anleitungen in unseren bewährten Sicherheitsmethoden für AWS Wickr und dem Modell der gemeinsamen Verantwortung von AWS Cloud Security.

Was ist ATAK?

Das Android Team Awareness Kit (ATAK) — oder Android Tactical Assault Kit (auch ATAK) für militärische Zwecke — ist eine Smartphone-Anwendung zur Geodateninfrastruktur und Lageerfassung, die eine sichere Zusammenarbeit über geografische Grenzen hinweg ermöglicht. Obwohl es ursprünglich für den Einsatz in Kampfgebieten konzipiert wurde, wurde ATAK an die Aufgaben lokaler, staatlicher und bundesstaatlicher Behörden angepasst.

Topics

Aktivieren Sie ATAK im Wickr Network Dashboard

AWS Wickr unterstützt viele Agenturen, die Android Tactical Assault Kit (ATAK) verwenden. Bisher mussten ATAK-Betreiber, die Wickr verwenden, die Anwendung jedoch verlassen, um dies zu tun. Um Störungen und Betriebsrisiken zu reduzieren, hat Wickr ein Plugin entwickelt, das ATAK um sichere Kommunikationsfunktionen erweitert. Mit dem Wickr-Plugin für ATAK können Benutzer Nachrichten senden, zusammenarbeiten und Dateien auf Wickr innerhalb der ATAK-Anwendung übertragen. Dadurch werden Unterbrechungen und die Komplexität der Konfiguration mit den Chat-Funktionen von ATAK vermieden.

Aktivieren Sie ATAK im Wickr Network Dashboard

Gehen Sie wie folgt vor, um ATAK im Wickr Network Dashboard zu aktivieren.

1. Öffnen Sie das AWS-Managementkonsole für Wickr unter. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
4. Wählen Sie auf der Seite Sicherheitsgruppen die gewünschte Sicherheitsgruppe aus, für die Sie ATAK aktivieren möchten.
5. Wählen Sie auf der Registerkarte Integration im Abschnitt ATAK-Plugin die Option Bearbeiten aus.
6. Aktivieren Sie auf der Seite ATAK-Plugin bearbeiten das Kontrollkästchen ATAK-Plugin aktivieren.
7. Wählen Sie Neues Paket hinzufügen
8. Geben Sie den Paketnamen in das Textfeld Pakete ein. Abhängig von der ATAK-Version, die Ihre Benutzer installieren und verwenden werden, können Sie einen der folgenden Werte eingeben:

   - `com.atakmap.app.civ`— Geben Sie diesen Wert in das Textfeld Pakete ein, wenn Ihre Wickr-Endbenutzer die zivile Version der ATAK-Anwendung auf ihren Android-Geräten installieren und verwenden möchten.
   - `com.atakmap.app.mil`— Geben Sie diesen Wert in das Textfeld Pakete ein, wenn Ihre Wickr-Endbenutzer die militärische Version der ATAK-Anwendung auf ihren Android-Geräten installieren und verwenden möchten.

9. Wählen Sie Speichern.

   ATAK ist jetzt für das ausgewählte Wickr-Netzwerk und die ausgewählte Sicherheitsgruppe aktiviert. Sie sollten die Android-Benutzer in der Sicherheitsgruppe, für die Sie die ATAK-Funktionalität aktiviert haben, bitten, das Wickr-Plugin für ATAK zu installieren. Weitere Informationen finden Sie unter Installieren und Koppeln des Wickr ATAK-Plug-ins.

Zusätzliche Informationen zu ATAK

Weitere Informationen zum Wickr-Plugin für ATAK finden Sie im Folgenden:

- Übersicht über das Wickr ATAK-Plugin
- Zusätzliche Informationen zum Wickr ATAK-Plugin

Installieren und koppeln Sie das Wickr-Plugin für ATAK

Das Android Team Awareness Kit (ATAK) ist eine Android-Lösung, die vom US-Militär, von Bundesstaaten und Regierungsbehörden verwendet wird, die für die Planung, Ausführung und Reaktion auf Zwischenfälle Fähigkeiten zur Situationswahrnehmung benötigen. ATAK verfügt über eine Plugin-Architektur, die es Entwicklern ermöglicht, Funktionen hinzuzufügen. Es ermöglicht Benutzern, mithilfe von GPS- und Geodaten zu navigieren, die mit einem Situationsbewusstsein über aktuelle Ereignisse in Echtzeit überlagert sind. In diesem Dokument zeigen wir Ihnen, wie Sie das Wickr-Plugin für ATAK auf einem Android-Gerät installieren und mit dem Wickr-Client koppeln. Auf diese Weise können Sie Nachrichten senden und auf Wickr zusammenarbeiten, ohne die ATAK-Anwendung zu verlassen.

Installieren Sie das Wickr-Plugin für ATAK

Gehen Sie wie folgt vor, um das Wickr-Plugin für ATAK auf einem Android-Gerät zu installieren.

1. Gehen Sie zum Google Play Store und installieren Sie das Wickr for ATAK-Plugin.
2. Öffnen Sie die ATAK-Anwendung auf Ihrem Android-Gerät.
3. Wählen Sie in der ATAK-Anwendung das Menüsymbol () oben rechts auf dem Bildschirm und wählen Sie dann Plugins.

4. Wählen Sie Importieren aus.
5. Wählen Sie im Popup-Fenster „Importtyp auswählen“ die Option „Local SD“ und navigieren Sie zu dem Speicherort, an dem Sie das Wickr-Plug-In für die ATAK-APK-Datei gespeichert haben.
6. Wählen Sie die Plugin-Datei aus und folgen Sie den Anweisungen, um sie zu installieren.

   > **Note**
   >
   > Wenn Sie aufgefordert werden, die Plugin-Datei zum Scannen zu senden, wählen Sie Nein.

7. Die ATAK-Anwendung fragt Sie, ob Sie das Plugin laden möchten. Wählen Sie OK aus.

Das Wickr-Plugin für ATAK ist jetzt installiert. Fahren Sie mit dem folgenden Abschnitt „ATAK mit Wickr verbinden“ fort, um den Vorgang abzuschließen.

Kombinieren Sie ATAK mit Wickr

Gehen Sie wie folgt vor, um die ATAK-Anwendung mit Wickr zu koppeln, nachdem Sie das Wickr-Plugin für ATAK erfolgreich installiert haben.

1. Wählen Sie in der ATAK-Anwendung das Menüsymbol () oben rechts auf dem Bildschirm und wählen Sie dann Wickr-Plugin.
2. Wählen Sie Pair Wickr.

   Es erscheint eine Benachrichtigung, in der Sie aufgefordert werden, die Berechtigungen für das Wickr-Plugin für ATAK zu überprüfen. Wenn die Benachrichtigungsaufforderung nicht angezeigt wird, öffnen Sie den Wickr-Client und gehen Sie zu Einstellungen und dann zu Verbundene Apps. Sie sollten das Plugin im Bereich Ausstehend auf dem Bildschirm sehen.
3. Wählen Sie „Zum Koppeln genehmigen“.
4. Wählen Sie die Schaltfläche Wickr ATAK-Plugin öffnen, um zur ATAK-Anwendung zurückzukehren.

   Sie haben das ATAK-Plug-In und Wickr nun erfolgreich gepaart und können das Plugin verwenden, um Nachrichten zu senden und mit Wickr zusammenzuarbeiten, ohne die ATAK-Anwendung zu beenden.

Entkoppeln Sie das Wickr-Plugin für ATAK

Sie können das Wickr-Plugin für ATAK entkoppeln.

Gehen Sie wie folgt vor, um das ATAK-Plugin mit Wickr zu entkoppeln.

1. Wählen Sie in der nativen App Einstellungen und dann Verbundene Apps aus.
2. Wählen Sie auf dem Bildschirm Verbundene Apps die Option Wickr ATAK Plugin aus.
3. Wählen Sie auf dem Bildschirm des Wickr ATAK-Plug-ins unten auf dem Bildschirm die Option Entfernen aus.

   Sie haben das Wickr-Plugin für ATAK jetzt erfolgreich entkoppelt.

Wählen und empfangen Sie einen Anruf in ATAK

Im Wickr-Plugin für ATAK können Sie einen Anruf wählen und empfangen.

Gehen Sie wie folgt vor, um einen Anruf zu wählen und anzunehmen.

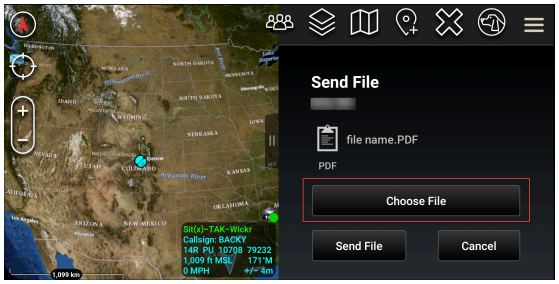
1. Öffnen Sie ein Chat-Fenster.
2. Wählen Sie in der Kartenansicht das Symbol für den Benutzer aus, den Sie anrufen möchten.
3. Wählen Sie das Telefonsymbol oben rechts auf dem Bildschirm.
4. Sobald die Verbindung hergestellt ist, können Sie zur Ansicht des ATAK-Plugins zurückkehren und einen Anruf entgegennehmen.

Senden Sie eine Datei in ATAK

Sie können eine Datei im Wickr-Plugin für ATAK senden.

Gehen Sie wie folgt vor, um eine Datei zu senden.

1. Öffnen Sie ein Chat-Fenster.
2. Suchen Sie in der Kartenansicht nach dem Benutzer, dem Sie eine Datei senden möchten.
3. Wenn Sie den Benutzer gefunden haben, dem Sie eine Datei senden möchten, wählen Sie seinen Namen aus.
4. Wählen Sie auf dem Bildschirm Datei senden die Option Datei auswählen aus, und navigieren Sie dann zu der Datei, die Sie senden möchten.



5. Wählen Sie im Browserfenster die gewünschte Datei aus.
6. Wählen Sie auf dem Bildschirm „Datei senden“ die Option „Datei senden“.

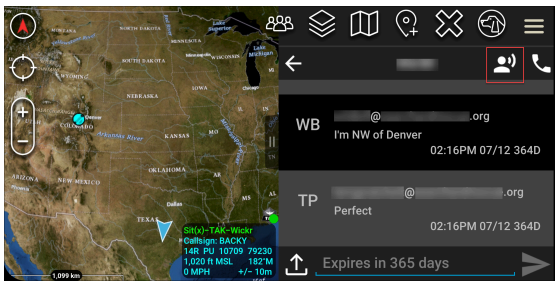
   Das Download-Symbol wird angezeigt, was darauf hinweist, dass die von Ihnen ausgewählte Datei heruntergeladen wird.

Senden Sie eine sichere Sprachnachricht (Push-to-talk) in ATAK

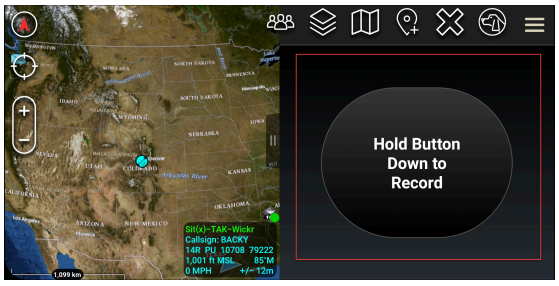
Im Wickr-Plugin für ATAK können Sie eine sichere Sprachnachricht (Push-to-talk) senden.

Gehen Sie wie folgt vor, um eine sichere Sprachnachricht zu senden.

1. Öffnen Sie ein Chat-Fenster.
2. Wählen Sie das Push-to-Talk Symbol oben auf dem Bildschirm, das durch das Symbol einer sprechenden Person gekennzeichnet ist.



3. Wählen Sie die Taste „Zum Aufnehmen gedrückt halten“ und halten Sie sie gedrückt.



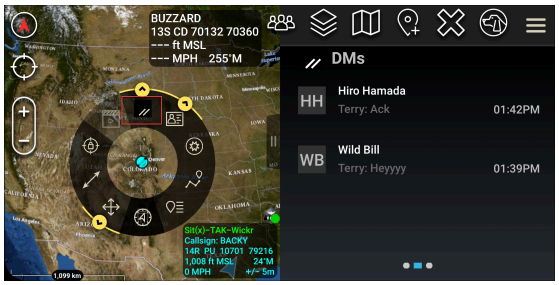
4. Nehmen Sie Ihre Nachricht auf.
5. Nachdem Sie Ihre Nachricht aufgenommen haben, lassen Sie die Taste los, um sie zu senden.

Windrad (Schnellzugriff) für ATAK

Das Windrad oder die Schnellzugriffsfunktion wird für one-one-one Konversationen oder Direktnachrichten verwendet.

Gehen Sie wie folgt vor, um das Windrad zu verwenden.

1. Öffnen Sie gleichzeitig die geteilte Bildschirmansicht der ATAK-Map und des Wickr for ATAK-Plug-ins. Auf der Karte werden deine Teammitglieder oder Ressourcen in der Kartenansicht angezeigt.
2. Wählen Sie das Benutzersymbol, um das Windrad zu öffnen.
3. Wählen Sie das Wickr-Symbol, um die verfügbaren Optionen für den ausgewählten Benutzer anzuzeigen.



4. Wählen Sie auf dem Windrad eines der folgenden Symbole:

   - Telefon: Wählen Sie, ob Sie anrufen möchten.

   - Nachricht: Wählen Sie, ob Sie chatten möchten.

- Datei senden: Wählen Sie, ob Sie eine Datei senden möchten.

Navigation für ATAK

Die Plugin-Benutzeroberfläche enthält drei Plugin-Ansichten, die durch die blauen und weißen Formen unten rechts auf dem Bildschirm gekennzeichnet sind. Wischen Sie nach links und rechts, um zwischen den Ansichten zu navigieren.

- Ansicht „Kontakte“: Erstelle eine Direktnachrichtengruppe oder eine Konversation in einem Chatroom.
- DMs Ansicht: Erstelle eine one-to-one Konversation. Die Chat-Funktionalität funktioniert wie in der nativen Wickr-App. Diese Funktion ermöglicht es dir, in der Kartenansicht zu bleiben und mit anderen Nutzern des Plugins zu kommunizieren.
- Raumansicht: Die vorhandenen Räume in der nativen App werden portiert. Alles, was im Plugin getan wurde, spiegelt sich in der nativen Wickr-App wider.

> **Note**
>
> Bestimmte Funktionen, wie das Löschen eines Raums, können nur in der nativen App und persönlich ausgeführt werden, um unbeabsichtigte Änderungen durch Benutzer und Störungen durch Feldgeräte zu verhindern.

Liste der zugelassenen Ports und Domänen für Ihr Wickr-Netzwerk

Listen Sie die folgenden Ports auf, um sicherzustellen, dass Wickr ordnungsgemäß funktioniert:

Ports

- TCP-Port 443 (für Nachrichten und Anlagen)
- UDP-Ports 16384-16584 (zum Anrufen)

Domänen und Adressen, die nach Regionen zugelassen werden sollen

Wenn Sie alle möglichen aufrufenden Domänen und Server-IP-Adressen auf die Zulassungsliste setzen müssen, sehen Sie sich die folgende Liste potenzieller CIDRs nach Regionen an. Überprüfen Sie diese Liste regelmäßig, da sie sich ändern kann.

> **Note**
>
> Registrierungs- und Bestätigungs-E-Mails werden von `no-reply@amazonaws.com` und gesendetdonotreply@wickr.email.

USA Ost (Nord-Virginia)

Domänen:	• gw-pro-prod.wickr.com • api.messaging. wickr.us-east-1.amazonaws.com • ingress.prod.calling.wickr.com
CIDR-Adressen anrufen:	• 44.211.195. 0/27 • 44,213,83. 32/28
IP-Adressen aufrufen:	• 44.211.195.0 • 44,211,195,1 • 44,211,195,2 • 44,211,159,3 • 44,211,195,4

- 44,211,195,5
- 44,211,159,6
- 44,211,195,7
- 44,211,159,8
- 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

Asien-Pazifik (Malaysia)

Domänen:	• gw-pro-prod.wickr.com • api.messaging. wickr.ap-southeast-5.amazonaws.com • ingress.prod.calling. wickr.ap-southeast-5.amazonaws.com
CIDR-Adressen aufrufen:	• 43.216.226. 160/28
IP-Adressen aufrufen:	• 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

Asien-Pazifik (Singapur)

Domäne:	• gw-pro-prod.wickr.com • api.messaging. wickr.ap-southeast-1.amazonaws.com • ingress.prod.calling. wickr.ap-southeast-1.amazonaws.com
CIDR-Adressen aufrufen:	• 47.129.23. 144/28
IP-Adressen aufrufen:	• 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

Asien-Pazifik (Sydney)

Domäne:	• gw-pro-prod.wickr.com • api.messaging. wickr.ap-southeast-2.amazonaws.com • ingress.prod.calling. wickr.ap-southeast-2.amazonaws.com
CIDR-Adressen aufrufen:	• 3.27.180. 208/28
IP-Adressen aufrufen:	• 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

Asien-Pazifik (Tokio)

Domäne:	• gw-pro-prod.wickr.com • api.messaging. wickr.ap-northeast-1.amazonaws.com • ingress.prod.calling. wickr.ap-northeast-1.amazonaws.com
CIDR-Adressen aufrufen:	• 57.181.142. 240/28
IP-Adressen aufrufen:	• 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 • 57,181142,250 • 57,181142,251 • 57,181142,252 • 57,181,142,253 • 57,181142,254 • 57,181142,255

Kanada (Zentral)

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

	• ingress.prod.calling. wickr.ca-central-1 .amazonaws.com
CIDR-Adressen aufrufen:	• 15.156.152. 96/28
IP-Adressen aufrufen:	• 15.156.152.96 • 15,156,152,97 • 15,156,152,98 • 15,156,152,99 • 15,156,152,100 • 15,156,152,1101 • 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

Europa (Frankfurt)

Domäne:	• gw-pro-prod.wickr.com • api.messaging. wickr.eu-central-1.amazonaw s.com • ingress.prod.calling. wickr.eu-central-1 .amazonaws.com
CIDR-Adressen aufrufen:	• 3.78.252. 32/28
IP-Adressen aufrufen:	• 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

IP-Adressen für Nachrichten:	• 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

Europa (London)

Domäne:	• gw-pro-prod.wickr.com • api.messaging. wickr.eu-west-2.amazonaws.com • ingress.prod.calling. wickr.eu-west-2.amazonaws.com
CIDR-Adressen aufrufen:	• 13.43.91. 48/28

IP-Adressen aufrufen:	• 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

Europa (Stockholm)

Domäne:	• gw-pro-prod.wickr.com • api.messaging. wickr.eu-north-1.amazonaws.com • ingress.prod.calling. wickr.eu-north-1.amazonaws.com
CIDR-Adressen aufrufen:	• 13.60.1. 64/28
IP-Adressen aufrufen:	• 13.60.1.64 • 13,601,65 • 13,601,66 • 13,601,67 • 13,601,68

	• 13,601,69 • 13,601,70 • 13,601,71 • 13,601,72 • 13,601,73 • 13,601,74 • 13,601,75 • 13,601,76 • 13,601,77 • 13,601,78 • 13,601,79

Europa (Zürich)

Domäne:	• gw-pro-prod.wickr.com • api.messaging. wickr.eu-central-2.amazonaws.com • ingress.prod.calling. wickr.eu-central-2 .amazonaws.com
CIDR-Adressen aufrufen:	• 16.63.106. 224/28
IP-Adressen aufrufen:	• 16.63.106.224 • 16,63,106,225 • 16,63,106,226 • 16,63,106,227 • 16,63,106,228 • 16,63,106,229 • 16,63,106,230 • 16,63,106,231 • 16,63,106,232 • 16,63,106,233

	• 16,63,106,234 • 16,63,106,235 • 16,63,106,236 • 16,63,106,237 • 16,63,106,238 • 16,63,106,239

AWS GovCloud (US-West)

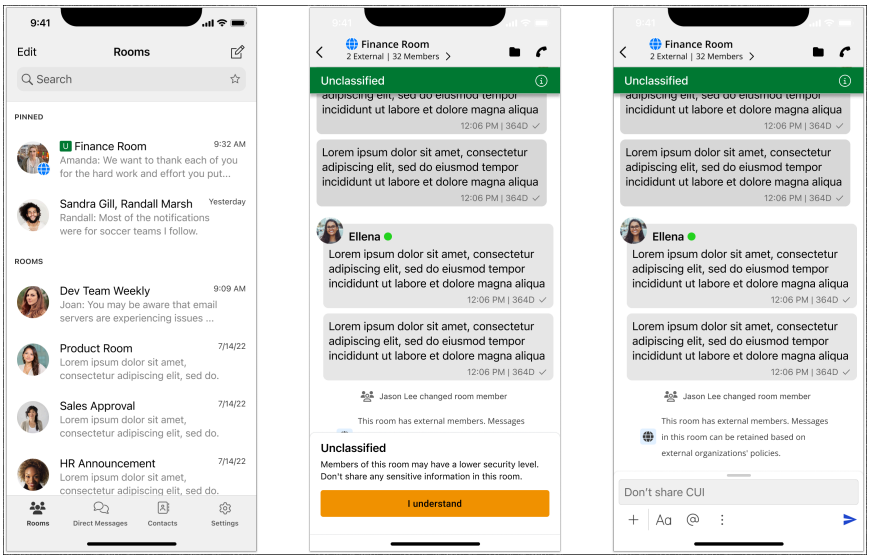
Domäne:	• gw-pro-prod.wickr.com • api.messaging. wickr.us-gov-west-1.amazonaws.com • Ingress-Prod-Calling. wickr.us-gov-west-1.amazonaws.com • s3.us-gov-west-1.amazonaws.com • s3-fips.us-gov-west-1.amazonaws.com • s3.amazonaws.com • registrieren. wickr.us-gov-west-1.amazonaws.com • admin. wickr.us-gov-west-1.amazonaws.com • admin.messaging. wickr.us-gov-west-1.amazonaws.com • cognito-identity.us-gov-west-1.amazonaws.com • kinesis.us-gov-west-1.amazonaws.com • Nachrichtenübermittlung. wickr.us-gov-west-1.amazonaws.com
CIDR-Adressen anrufen:	• 3.30.186. 208/28 • 3,31,11. 216/29
IP-Adressen aufrufen:	• 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
- 3,30,186,1215
- 3,30,186,216
- 3,30,186,1217
- 3,30,186,218
- 3,30,186,1219
- 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 Grenzüberschreitende Klassifikation und Föderation

AWS Wickr bietet einen auf GovCloud Benutzer zugeschnittenen WickrGov Client. Die GovCloud Federation ermöglicht die Kommunikation zwischen GovCloud Benutzern und kommerziellen Benutzern. Die Funktion zur grenzüberschreitenden Klassifizierung ermöglicht es GovCloud Benutzern, Konversationen an der Benutzeroberfläche zu ändern. Als GovCloud Benutzer müssen Sie sich an strenge Richtlinien für die von der Regierung festgelegte Klassifizierung halten. Wenn GovCloud Benutzer Gespräche mit kommerziellen Benutzern (Enterprise, AWS Wickr, Gastbenutzer) führen, werden ihnen die folgenden nicht klassifizierten Warnungen angezeigt:

- Ein U-Tag in der Raumliste
- Eine nicht klassifizierte Bestätigung auf dem Nachrichtenbildschirm
- Ein nicht klassifiziertes Banner über der Konversation



> **Note**
>
> Diese Warnungen werden nur angezeigt, wenn sich ein GovCloud Benutzer mit externen Benutzern unterhält oder Teil eines Raums ist. Sie verschwinden, wenn die externen Benutzer die Konversation verlassen. In Konversationen zwischen GovCloud Benutzern werden keine Warnungen angezeigt.

Dateivorschau für AWS Wickr

Organizations, die die Wickr Premium-Stufe (einschließlich der kostenlosen Premium-Testversion) verwenden, können jetzt die Berechtigungen zum Herunterladen von Dateien auf Sicherheitsgruppenebene verwalten.

Dateidownloads sind in Sicherheitsgruppen standardmäßig aktiviert. Administratoren können das Herunterladen von Dateien über das Administrator-Panel aktivieren oder deaktivieren. Diese Einstellung gilt für das gesamte Wickr-Netzwerk.

Gehen Sie wie folgt vor, um den Dateidownload zu aktivieren oder zu deaktivieren.

1. Öffnen Sie sie AWS-Managementkonsole für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
4. Wählen Sie den Namen der Sicherheitsgruppe aus, die Sie bearbeiten möchten.

   Auf der Seite mit den Sicherheitsgruppendetails werden die Einstellungen für die Sicherheitsgruppe auf verschiedenen Registerkarten angezeigt.
5. Wählen Sie auf der Registerkarte Nachrichten im Abschnitt Medien und Links die Option Bearbeiten aus.
6. Aktivieren oder deaktivieren Sie auf der Seite „Medien und Links bearbeiten“ die Option „Dateidownloads“.
7. Wählen Sie Änderungen speichern aus.

Wenn Dateidownloads für eine Sicherheitsgruppe aktiviert sind, können Benutzer Dateien herunterladen, die in Direktnachrichten und Chatrooms geteilt wurden. Wenn Downloads deaktiviert sind, können sie nur eine Vorschau dieser Dateien anzeigen und sie auf den Tab „Dateien“ hochladen, sie können sie jedoch nicht herunterladen. Benutzern ist es außerdem untersagt, Screenshots zu machen. Versuche führen zu einem schwarzen Bildschirm.

> **Note**
>
> Wenn Dateidownloads deaktiviert sind, müssen alle Benutzer in dieser Sicherheitsgruppe Wickr-Versionen 6.54 und höher verwenden, damit diese Dateieinstellung gilt.

> **Note**
>
> In Räumen, in denen Benutzer aus unterschiedlichen Netzwerken (aufgrund des Verbunds) und Sicherheitsgruppen anwesend sind, hängt die Fähigkeit jedes Benutzers, Dateien in der Vorschau anzuzeigen oder herunterzuladen, von seinen spezifischen Sicherheitsgruppeneinstellungen ab. Daher können einige Benutzer Dateien in einem Raum herunterladen, während andere sie nur in der Vorschau anzeigen können.

Pop-up zur Zustimmung für AWS Wickr

Sie können das Zustimmungs-Popup für Ihr Netzwerk so konfigurieren, dass Benutzern Bedingungen, Richtlinien oder organisatorische Anforderungen angezeigt werden, wenn sie sich bei Wickr anmelden. Benutzer müssen das Pop-up bestätigen, bevor sie auf die Anwendung zugreifen können. Das Pop-up wird erneut angezeigt, wenn sich Benutzer ab- und wieder anmelden oder wenn der Popup-Inhalt aktualisiert wird.

Gehen Sie wie folgt vor, um das Einwilligungs-Popup zu aktivieren.

1. Öffnen Sie sie AWS-Managementkonsole für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Netzwerkrichtlinien aus.
4. Wählen Sie auf der Seite Netzwerkrichtlinien im Popup-Bereich Zustimmung die Option Bearbeiten aus.
5. Aktivieren Sie auf der Popup-Seite „Zustimmung bearbeiten“ im Bereich „Zustimmungs-Popup“ die Option Aktiviert.
6. Füllen Sie die folgenden Felder aus:

   - Kopfzeile — Geben Sie den Titel ein, der oben im Pop-up mit der Zustimmung angezeigt wird. Verwenden Sie die Kopfzeile, um eine Zusammenfassung der Informationen oder Aktionen bereitzustellen, die den Benutzern präsentiert werden.
   - Textinhalt — Geben Sie die Hauptnachricht ein, die im Einwilligungs-Popup angezeigt wird. Verwenden Sie den Textinhalt, um Bedingungen, Richtlinien, organisatorische Anforderungen oder andere Informationen zu kommunizieren, die Benutzer lesen müssen, bevor sie auf die Anwendung zugreifen können.
   - Bezeichnung der Schaltfläche „Schließen“ (optional) — Geben Sie den Text ein, der auf der Schaltfläche angezeigt wird, die Benutzer auswählen, um das Einwilligungs-Popup zu bestätigen und zu schließen. Sie können beispielsweise „Bestätigen“, „Akzeptieren“ oder „Fortfahren“ verwenden.
7. Um eine Vorschau Ihres Einwilligungs-Popups anzuzeigen, wählen Sie in der oberen rechten Ecke „Vorschau“. Wählen Sie nach der Vorschau „Vorschau schließen“.
8. Wählen Sie Änderungen speichern aus.

Benutzer in AWS Wickr verwalten

Im Bereich Benutzerverwaltung von AWS-Managementkonsole for Wickr können Sie aktuelle Wickr-Benutzer und -Bots einsehen und deren Details ändern.

Topics

Teamverzeichnis im AWS Wickr-Netzwerk

Sie können aktuelle Wickr-Benutzer anzeigen und ihre Details im Bereich Benutzerverwaltung von AWS-Managementkonsole for Wickr ändern.

Topics

Benutzer im AWS Wickr-Netzwerk anzeigen

Sie können die Details der Benutzer einsehen, die in Ihrem Wickr-Netzwerk registriert sind.

Gehen Sie wie folgt vor, um die in Ihrem Wickr-Netzwerk registrierten Benutzer anzuzeigen.

1. Öffnen Sie das AWS-Managementkonsole für Wickr unter. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Benutzerverwaltung aus.

Auf der Registerkarte Teamverzeichnis werden Benutzer angezeigt, die in Ihrem Wickr-Netzwerk registriert sind, einschließlich ihres Namens, ihrer E-Mail-Adresse, der zugewiesenen Sicherheitsgruppe und ihres aktuellen Status. Für aktuelle Benutzer können Sie ihre Geräte anzeigen, ihre Daten bearbeiten, sie sperren, löschen und zu einem anderen Wickr-Netzwerk wechseln.

Laden Sie einen Benutzer in das AWS Wickr-Netzwerk ein

Sie können einen Benutzer in Ihr Wickr-Netzwerk einladen.

Gehen Sie wie folgt vor, um einen Benutzer in Ihr Wickr-Netzwerk einzuladen.

1. Öffnen Sie das AWS-Managementkonsole für Wickr unter. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Benutzerverwaltung aus.
4. Wählen Sie auf der Registerkarte Teamverzeichnis die Option Benutzer einladen aus.
5. Geben Sie auf der Seite „Benutzer einladen“ die E-Mail-Adresse und die Sicherheitsgruppe des Benutzers ein. E-Mail-Adresse und Sicherheitsgruppe sind die einzigen Felder, die erforderlich sind. Achten Sie darauf, die passende Sicherheitsgruppe für den Benutzer auszuwählen. Wickr sendet eine Einladungs-E-Mail an die Adresse, die Sie für den Benutzer angegeben haben.
6. Klicken Sie auf Invite user.

   Eine E-Mail wird an den Benutzer gesendet. Die E-Mail enthält Download-Links für die Wickr-Client-Anwendungen und einen Link zur Registrierung für Wickr. Wenn sich Benutzer über den Link in der E-Mail für Wickr registrieren, ändert sich ihr Status im Wickr-Teamverzeichnis von Ausstehend auf Aktiv.

Benutzer im AWS Wickr-Netzwerk bearbeiten

Sie können Benutzer in Ihrem Wickr-Netzwerk bearbeiten.

Gehen Sie wie folgt vor, um einen Benutzer zu bearbeiten.

1. Öffnen Sie das AWS-Managementkonsole für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Benutzerverwaltung aus.
4. Wählen Sie auf der Registerkarte Teamverzeichnis das vertikale Ellipsensymbol (drei Punkte) des Benutzers aus, den Sie bearbeiten möchten.
5. Wählen Sie Bearbeiten aus.
6. Bearbeiten Sie die Benutzerinformationen und wählen Sie dann Änderungen speichern.

Löschen Sie einen Benutzer im AWS Wickr-Netzwerk

Sie können einen Benutzer in Ihrem Wickr-Netzwerk löschen.

Gehen Sie wie folgt vor, um einen Benutzer zu löschen.

1. Öffnen Sie das AWS-Managementkonsole für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Benutzerverwaltung aus.
4. Wählen Sie auf der Registerkarte Teamverzeichnis das vertikale Ellipsensymbol (drei Punkte) des Benutzers aus, den Sie löschen möchten.
5. Wählen Sie Löschen, um den Benutzer zu löschen.

   Wenn Sie einen Benutzer löschen, kann sich dieser Benutzer im Wickr-Client nicht mehr bei Ihrem Wickr-Netzwerk anmelden.
6. Wählen Sie im Popup-Fenster die Option Löschen.

Massenlöschung von Benutzern im AWS Wickr-Netzwerk

Sie können Wickr-Netzwerkbenutzer im Bereich Benutzerverwaltung von AWS-Managementkonsole for Wickr massenweise löschen.

> **Note**
>
> Die Option zum Massenlöschen von Benutzern gilt nur, wenn SSO nicht aktiviert ist.

Gehen Sie wie folgt vor, um Ihre Wickr-Netzwerkbenutzer mithilfe einer CSV-Vorlage massenweise zu löschen.

1. Öffnen Sie das AWS-Managementkonsole für Wickr unter. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Benutzerverwaltung aus.
4. Auf der Registerkarte Teamverzeichnis werden Benutzer angezeigt, die in Ihrem Wickr-Netzwerk registriert sind.
5. Wählen Sie auf der Registerkarte Teamverzeichnis die Option Benutzer verwalten und anschließend Massenlöschung aus.
6. Laden Sie auf der Seite Benutzer gleichzeitig löschen die CSV-Beispielvorlage herunter. Um die Beispielvorlage herunterzuladen, wählen Sie Vorlage herunterladen.
7. Vervollständigen Sie die Vorlage, indem Sie die E-Mail-Adressen der Benutzer hinzufügen, die Sie massenweise aus Ihrem Netzwerk löschen möchten.
8. Laden Sie die fertige CSV-Vorlage hoch. Sie können die Datei per Drag & Drop in das Upload-Feld ziehen oder eine Datei auswählen.
9. Aktivieren Sie das Kontrollkästchen. Ich verstehe, dass das Löschen eines Benutzers nicht rückgängig gemacht werden kann.
10. Wählen Sie Benutzer löschen.

> **Note**
>
> Diese Aktion beginnt sofort mit dem Löschen von Benutzern und kann mehrere Minuten dauern. Gelöschte Benutzer können sich im Wickr-Client nicht mehr bei Ihrem Wickr-Netzwerk anmelden.

Gehen Sie wie folgt vor, um Ihre Wickr-Netzwerkbenutzer massenweise zu löschen, indem Sie eine CSV-Datei Ihres Teamverzeichnisses herunterladen.

1. Öffnen Sie das AWS-Managementkonsole für Wickr unter. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Benutzerverwaltung aus.
4. Auf der Registerkarte Teamverzeichnis werden Benutzer angezeigt, die in Ihrem Wickr-Netzwerk registriert sind.
5. Wählen Sie auf der Registerkarte Teamverzeichnis die Option Benutzer verwalten und dann Als CSV herunterladen aus.
6. Nachdem Sie die CSV-Vorlage für das Teamverzeichnis heruntergeladen haben, entfernen Sie die Zeilen mit Benutzern, die nicht gelöscht werden müssen.
7. Wählen Sie auf der Registerkarte Teamverzeichnis die Option Benutzer verwalten und anschließend Massenlöschung aus.
8. Laden Sie auf der Seite „Benutzer gleichzeitig löschen“ die CSV-Vorlage für das Teamverzeichnis hoch. Sie können die Datei per Drag & Drop in das Upload-Feld ziehen oder Datei auswählen auswählen.
9. Aktivieren Sie das Kontrollkästchen. Ich verstehe, dass das Löschen eines Benutzers nicht rückgängig gemacht werden kann.
10. Wählen Sie Benutzer löschen.

> **Note**
>
> Diese Aktion beginnt sofort mit dem Löschen von Benutzern und kann mehrere Minuten dauern. Gelöschte Benutzer können sich im Wickr-Client nicht mehr bei Ihrem Wickr-Netzwerk anmelden.

Benutzer im AWS Wickr-Netzwerk massenweise sperren

Sie können Wickr-Netzwerkbenutzer im Bereich Benutzerverwaltung von AWS-Managementkonsole for Wickr massenweise sperren.

> **Note**
>
> Die Option zur Massensperrung von Benutzern gilt nur, wenn SSO nicht aktiviert ist.

Gehen Sie wie folgt vor, um Ihre Wickr-Netzwerkbenutzer massenweise zu sperren.

1. Öffnen Sie das AWS-Managementkonsole für Wickr unter. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Benutzerverwaltung aus.
4. Auf der Registerkarte Teamverzeichnis werden Benutzer angezeigt, die in Ihrem Wickr-Netzwerk registriert sind.
5. Wählen Sie auf der Registerkarte Teamverzeichnis die Option Benutzer verwalten und anschließend Bulk sperren aus.
6. Laden Sie auf der Seite „Benutzer gleichzeitig sperren“ die CSV-Beispielvorlage herunter. Um die Beispielvorlage herunterzuladen, wählen Sie Vorlage herunterladen.
7. Vervollständigen Sie die Vorlage, indem Sie die E-Mail-Adressen der Benutzer hinzufügen, die Sie massenweise von Ihrem Netzwerk sperren möchten.
8. Laden Sie die fertige CSV-Vorlage hoch. Sie können die Datei per Drag & Drop in das Upload-Feld ziehen oder eine Datei auswählen.
9. Wählen Sie Benutzer sperren.

> **Note**
>
> Diese Aktion beginnt sofort mit dem Sperren von Benutzern und kann mehrere Minuten dauern. Gesperrte Benutzer können sich im Wickr-Client nicht in Ihrem Wickr-Netzwerk anmelden. Wenn Sie einen Benutzer sperren, der derzeit im Client in Ihrem Wickr-Netzwerk angemeldet ist, wird dieser Benutzer automatisch abgemeldet.

Gastbenutzer im AWS Wickr-Netzwerk

Die Wickr-Gastbenutzerfunktion ermöglicht es einzelnen Gastbenutzern, sich beim Wickr-Client anzumelden und mit Wickr-Netzwerkbenutzern zusammenzuarbeiten. Wickr-Administratoren können Gastbenutzer für ihre Wickr-Netzwerke aktivieren oder deaktivieren.

Nachdem die Funktion aktiviert wurde, können Gastbenutzer, die zu Ihrem Wickr-Netzwerk eingeladen wurden, mit Benutzern in Ihrem Wickr-Netzwerk interagieren. Für die Gastbenutzer-Funktion wird eine Gebühr auf Sie AWS-Konto erhoben. Weitere Informationen zu den Preisen für die Gastbenutzerfunktion finden Sie auf der Preisseite von Wickr unter Preis-Add-ons.

Topics

Gastbenutzer im AWS Wickr-Netzwerk aktivieren oder deaktivieren

Sie können Gastbenutzer in Ihrem Wickr-Netzwerk aktivieren oder deaktivieren.

Gehen Sie wie folgt vor, um Gastbenutzer für Ihr Wickr-Netzwerk zu aktivieren oder zu deaktivieren.

1. Öffnen Sie das AWS-Managementkonsole für Wickr unter. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
4. Wählen Sie den Namen für eine bestimmte Sicherheitsgruppe aus.

> **Note**
>
> Sie können Gastbenutzer nur für einzelne Sicherheitsgruppen aktivieren. Um Gastbenutzer für alle Sicherheitsgruppen in Ihrem Wickr-Netzwerk zu aktivieren, müssen Sie die Funktion für jede Sicherheitsgruppe in Ihrem Netzwerk aktivieren.

5. Wählen Sie in der Sicherheitsgruppe die Registerkarte Federation.
6. Es gibt zwei Standorte, an denen die Option zur Aktivierung von Gastbenutzern verfügbar ist:
   - Lokaler Verbund — Wählen Sie für Netzwerke im Osten der USA (Nord-Virginia) auf der Seite im Bereich Lokaler Verbund die Option Bearbeiten aus.
   - Globaler Verbund — Wählen Sie für alle anderen Netzwerke in anderen Regionen im Bereich Globaler Verbund auf der Seite die Option Bearbeiten aus.
7. Wählen Sie auf der Seite Verbund bearbeiten die Option Verbund aktivieren aus.
8. Wählen Sie Änderungen speichern, um die Änderung zu speichern und für die Sicherheitsgruppe wirksam zu machen.

   Registrierte Benutzer in der spezifischen Sicherheitsgruppe in Ihrem Wickr-Netzwerk können jetzt mit Gastbenutzern interagieren. Weitere Informationen finden Sie unter Gastbenutzer im Wickr-Benutzerhandbuch.

Anzahl der Gastbenutzer im AWS Wickr-Netzwerk anzeigen

Sie können die Anzahl der Gastbenutzer in Ihrem Wickr-Netzwerk einsehen.

Gehen Sie wie folgt vor, um die Anzahl der Gastbenutzer für Ihr Wickr-Netzwerk anzuzeigen.

1. Öffnen Sie das AWS-Managementkonsole für Wickr unter. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Benutzerverwaltung aus.

   Auf der Seite Benutzerverwaltung wird die Anzahl der Gastbenutzer in Ihrem Wickr-Netzwerk angezeigt.

Monatliche Nutzung im AWS Wickr-Netzwerk anzeigen

Sie können die Anzahl der Gastbenutzer einsehen, mit denen Ihr Netzwerk während eines Abrechnungszeitraums kommuniziert hat.

Gehen Sie wie folgt vor, um Ihre monatliche Nutzung für Ihr Wickr-Netzwerk einzusehen.

1. Öffnen Sie das AWS-Managementkonsole für Wickr unter. https://console.aws.amazon.com/wickr/
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Benutzerverwaltung aus.
4. Wählen Sie die Registerkarte Gastbenutzer aus.

   Auf der Registerkarte Gastbenutzer wird die monatliche Nutzung der Gastbenutzer angezeigt.

> **Note**
>
> Die Rechnungsdaten für Gäste werden alle 24 Stunden aktualisiert.

Gastbenutzer im AWS Wickr-Netzwerk anzeigen

Sie können die Gastbenutzer anzeigen, mit denen ein Netzwerkbenutzer während eines bestimmten Abrechnungszeitraums kommuniziert hat.

Gehen Sie wie folgt vor, um Gastbenutzer anzuzeigen, mit denen ein Netzwerkbenutzer während eines bestimmten Abrechnungszeitraums kommuniziert hat.

1. Öffnen Sie sie AWS-Managementkonsole für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Benutzerverwaltung aus.
4. Wählen Sie die Registerkarte Gastbenutzer aus.

   Auf der Registerkarte Gastbenutzer werden die Gastbenutzer in Ihrem Netzwerk angezeigt.

Blockieren Sie einen Gastbenutzer im AWS Wickr-Netzwerk

Sie können einen Gastbenutzer in Ihrem Wickr-Netzwerk blockieren und entsperren. Blockierte Benutzer können mit niemandem in Ihrem Netzwerk kommunizieren.

Um einen Gastbenutzer zu blockieren

1. Öffnen Sie sie AWS-Managementkonsole für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Benutzerverwaltung aus.
4. Wählen Sie die Registerkarte Gastbenutzer aus.

   Auf der Registerkarte Gastbenutzer werden die Gastbenutzer in Ihrem Netzwerk angezeigt.
5. Suchen Sie im Bereich Gastbenutzer nach der E-Mail-Adresse des Gastbenutzers, den Sie blockieren möchten.
6. Wählen Sie auf der rechten Seite neben dem Namen des Gastbenutzers die drei Punkte aus und wählen Sie Gastbenutzer blockieren aus.
7. Wählen Sie im Popup-Fenster Blockieren aus.
8. Um die Liste der blockierten Benutzer in Ihrem Wickr-Netzwerk anzuzeigen, wählen Sie das Dropdownmenü Status und dann Blockiert aus.

Um die Blockierung eines Gastbenutzers zu entsperren

1. Öffnen Sie sie AWS-Managementkonsole für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Benutzerverwaltung aus.
4. Wählen Sie die Registerkarte Gastbenutzer aus.

   Auf der Registerkarte Gastbenutzer werden die Gastbenutzer in Ihrem Netzwerk angezeigt.
5. Wählen Sie das Dropdownmenü Status und dann Blockiert aus.
6. Suchen Sie im Abschnitt Blockiert nach der E-Mail-Adresse des Gastbenutzers, den Sie entsperren möchten.
7. Wählen Sie auf der rechten Seite neben dem Namen des Gastbenutzers die drei Punkte aus und wählen Sie Benutzer entsperren aus.
8. Wählen Sie im Popup-Fenster die Option Entsperren aus.

Sicherheit in AWS Wickr

Cloud-Sicherheit hat AWS höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, auf der AWS Dienste in der ausgeführt AWS Cloud werden. AWSbietet Ihnen auch Dienste, die Sie sicher nutzen können. Third-party Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für AWS Wickr gelten, finden Sie unter AWSServices im Bereich nach Compliance-Programm AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Wickr anwenden können. In den folgenden Themen erfahren Sie, wie Sie Wickr konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Ihnen bei der Überwachung und Sicherung Ihrer Wickr-Ressourcen helfen.

Topics

Datenschutz in AWS Wickr

Das AWS Modell der gilt für den Datenschutz in AWS Wickr. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der AWS Cloud alle Systeme laufen. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz . Weitere Informationen zum Datenschutz in Europa finden Sie im Zentrum für die Datenschutz-Grundverordnung (DSGVO).

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit einAWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrailBenutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen StandardsicherheitskontrollenAWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Wickr oder anderen AWS-Services über die Konsole, API oder SDKs arbeiten. AWS CLI AWS Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen

Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Identitäts- und Zugriffsmanagement für AWS Wickr

AWS Identity and Access Management(IAM) hilft einem AdministratorAWS-Service, den Zugriff auf Ressourcen sicher zu kontrollieren. AWS IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Wickr-Ressourcen zu verwenden. IAM ist ein ProgrammAWS-Service, das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe für AWS Wickr

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von Ihrer Rolle ab:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Features zugreifen können (siehe Fehlerbehebung bei Identität und Zugriff auf AWS Wickr).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe So funktioniert AWS Wickr mit IAM).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe Identity-based Richtlinienbeispiele für AWS Wickr).

Authentifizierung mit Identitäten für AWS Wickr

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen sich als IAM-Benutzer authentifizieren oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung.

AWSBietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter AWS Signature Version 4 for API requests im IAM-Benutzerhandbuch.

AWS-KontoRoot-Benutzer

Wenn Sie einen erstellenAWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem sogenannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Tasks that require root user credentials im IAM-Benutzerhandbuch.

Verbundidentität

Es hat sich bewährt, dass menschliche Benutzer für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter verwenden müssen.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensverzeichnis, Ihrem Directory Service Web-Identitätsanbieter oder der AWS-Services mithilfe von Anmeldeinformationen aus einer Identitätsquelle zugreift. Verbundene Identitäten übernehmen Rollen, die temporäre Anmeldeinformationen bereitstellen.

Für die zentrale Zugriffsverwaltung empfehlen wir AWS IAM Identity Center. Weitere Informationen finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Wir empfehlen die Verwendung temporärer Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erfordern, dass menschliche Benutzer den Verbund mit einem Identitätsanbieter verwenden müssen, um AWS mithilfe temporärer Anmeldeinformationen darauf zugreifen zu können.

Eine IAM-Gruppe spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln AWS CLI oder einen AWS API-Vorgang aufrufen. Weitere Informationen finden Sie unter Methoden, um eine Rolle zu übernehmen im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für den Verbundbenutzer-Zugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, serviceübergreifenden Zugriff und Anwendungen, die auf Amazon EC2 laufen. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwaltung des Zugriffs mithilfe von Richtlinien für AWS Wickr

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie definiert Berechtigungen, wenn sie mit einer Identität oder Ressource verknüpft sind. AWSbewertet diese Richtlinien, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcenund unter welchen Bedingungendurchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identity-based Richtlinien

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität (Benutzer, Gruppe oder Rolle) anhängen. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identity-based Richtlinien können Inline-Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mehreren Identitäten zugeordnet sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter Choose between managed policies and inline policies im IAM-Benutzerhandbuch.

Resource-based Richtlinien

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen und Amazon S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben.

Resource-based Richtlinien sind Inline-Richtlinien, die sich in diesem Dienst befinden. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWSunterstützt zusätzliche, weniger verbreitete Richtlinientypen. Mit diesen Richtlinientypen können Sie die maximalen Berechtigungen festlegen, die Ihnen durch die gängigeren Richtlinientypen gewährt werden.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen stellen die Schnittmenge zwischen den identitätsbasierten Richtlinien der Entität und ihren Berechtigungsgrenzen dar. Resource-based Richtlinien, die den Benutzer oder die Rolle in dem `Principal` Feld angeben, sind nicht durch die Berechtigungsgrenze begrenzt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt

eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.

- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn für eine Anfrage mehrere Arten von Richtlinien gelten, sind die sich daraus ergebenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch.

AWSverwaltete Richtlinien für AWS Wickr

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie im IAM-Benutzerhandbuch unter AWSVerwaltete Richtlinien.

AWS-Servicesverwalten und aktualisieren Sie AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Services fügen einer von AWS verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWSverwaltete Richtlinie: AWSWickrFullAccess

Sie können die `AWSWickrFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt dem Wickr-Dienst volle Administratorrechte, einschließlich der AWS-Managementkonsole für Wickr in der. AWS-Managementkonsole Weitere Informationen zum Anhängen von Richtlinien an eine Identität finden Sie unter Hinzufügen und Entfernen von IAM-Identitätsberechtigungen im Benutzerhandbuch. AWS Identity and Access Management

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `wickr`— Gewährt dem Wickr-Dienst vollständige Administratorrechte.

JSON

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

Wickr aktualisiert aufAWSVerwaltete Richtlinien

Hier finden Sie Informationen zu Aktualisierungen der AWS verwalteten Richtlinien für Wickr, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen. Abonnieren Sie den RSS-Feed auf der Seite mit dem Verlauf der Wickr-Dokumente, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderungen	Beschreibung	Date
AWSWickrFullAccess – Neue Richtlinie	Wickr hat eine neue Richtlini e hinzugefügt, die dem Wickr-	28. November 2022

Änderungen	Beschreibung	Date
	Dienst vollständige Administr atorrechte gewährt, einschlie ßlich der Wickr-Administrato rkonsole in der. AWS-Manag ementkonsole	
Wickr hat begonnen, Änderungen zu verfolgen	Wickr begann, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	28. November 2022

So funktioniert AWS Wickr mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Wickr zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen für Wickr verfügbar sind.

IAM-Funktionen, die Sie mit AWS Wickr verwenden können

IAM-Feature	Wickr-Unterstützung
Identity-based Richtlinien	Ja
Resource-based Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Nein
Bedingungsschlüssel für die Richtlinie	Nein
ACLs	Nein
ABAC (Tags in Richtlinien)	Nein
Temporäre Anmeldeinformationen	Nein
Hauptberechtigungen	Nein

IAM-Feature	Wickr-Unterstützung
Servicerollen	Nein
Service-linked Rollen	Nein

Einen allgemeinen Überblick darüber, wie Wickr und andere AWS Dienste mit den meisten IAM-Funktionen funktionieren, finden Sie im AWSIAM-Benutzerhandbuch unter Dienste, die mit IAM funktionieren.

Identity-based Richtlinien für Wickr

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identity-based Richtlinien sind Richtliniendokumente für JSON-Berechtigungen, die Sie an eine Identität anhängen können, z. B. an einen IAM-Benutzer, eine Benutzergruppe oder eine Rolle. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Identity-based Richtlinienbeispiele für Wickr

Beispiele für identitätsbasierte Wickr-Richtlinien finden Sie unter. Identity-based Richtlinienbeispiele für AWS Wickr

Resource-based Richtlinien innerhalb von Wickr

Unterstützt ressourcenbasierte Richtlinien: Nein

Resource-based Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anhängen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-

S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Richtlinienaktionen für Wickr

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu erteilen.

Eine Liste der Wickr-Aktionen finden Sie unter Von AWS Wickr definierte Aktionen in der Service Authorization Reference.

Bei Richtlinienaktionen in Wickr wird vor der Aktion das folgende Präfix verwendet:

```
wickr
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

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

Beispiele für identitätsbasierte Wickr-Richtlinien finden Sie unter. Identity-based Richtlinienbeispiele für AWS Wickr

Politische Ressourcen für Wickr

Unterstützt Richtlinienressourcen: Nein

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als Best Practice geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

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

Eine Liste der Wickr-Ressourcentypen und ihrer ARNs finden Sie unter Von AWS Wickr definierte Ressourcen in der Service Authorization Reference. Informationen zu den Aktionen, mit denen Sie den ARN jeder Ressource angeben können, finden Sie unter Von AWS Wickr definierte Aktionen.

Beispiele für identitätsbasierte Wickr-Richtlinien finden Sie unter. Identity-based Richtlinienbeispiele für AWS Wickr

Bedingungsschlüssel für Richtlinien für Wickr

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Nein

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der Wickr-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Wickr in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von AWS Wickr definierte Aktionen.

Beispiele für identitätsbasierte Wickr-Richtlinien finden Sie unter. Identity-based Richtlinienbeispiele für AWS Wickr

ACLs in Wickr

Unterstützt ACLs: Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit Wickr

Unterstützt ABAC (Tags in Richtlinien): Nein

Attribute-based Access Control (ABAC) ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Attributen definiert, die als Tags bezeichnet werden. Sie können Tags an IAM-Entitäten und AWS -Ressourcen anhängen und dann ABAC-Richtlinien entwerfen, die Operationen zulassen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit Wickr

Unterstützt temporäre Anmeldeinformationen: Nein

Temporäre Anmeldeinformationen ermöglichen kurzfristigen Zugriff auf AWS Ressourcen und werden automatisch erstellt, wenn Sie einen Verbund verwenden oder die Rollen wechseln. AWSempfiehlt,

temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Anmeldeinformationen in IAM und AWS-Services, die mit IAM funktionieren im IAM-Benutzerhandbuch.

Cross-service Hauptberechtigungen für Wickr

Unterstützt Forward Access Sessions (FAS): Nein

Forward Access Sessions (FAS) verwenden die Berechtigungen des Prinzipals, der einen aufruftAWS-Service, in Kombination mit der Anfrage, Anfragen an nachgeschaltete Dienste AWS-Service zu stellen. Einzelheiten zu den Richtlinien für FAS-Anforderungen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für Wickr

Unterstützt Servicerollen: Nein

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

> **Warning**
>
> Durch das Ändern der Berechtigungen für eine Servicerolle kann die Funktionalität von Wickr beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, wenn Wickr Sie dazu anleitet.

Service-linked Rollen für Wickr

Unterstützt serviceverknüpfte Rollen: Ja

Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer AWS-Service verknüpft ist. Der Dienst kann die Rolle übernehmen, eine Aktion in Ihrem Namen auszuführen. Service-linked Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS-Services, die mit IAM funktionieren. Suchen Sie in der Tabelle nach einem Dienst, der einen `Yes` in der Service-linked Rollenspalte enthält. Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Identity-based Richtlinienbeispiele für AWS Wickr

Standardmäßig besitzt ein völlig neuer IAM-Benutzer überhaupt keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen und zuweisen, die Benutzern die Erlaubnis geben, den AWS Wickr-Service zu verwalten. Dies ist ein Beispiel für eine Berechtigungsrichtlinie.

JSON

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

Diese Beispielrichtlinie gibt Benutzern die Berechtigung, Wickr-Netzwerke mithilfe von for Wickr aufzulisten. AWS-Managementkonsole Weitere Informationen zu den Elementen in einer IAM-Richtlinienanweisung finden Sie unter Identity-based Richtlinien für Wickr. Informationen dazu, wie Sie unter Verwendung dieser Beispiel-JSON-Richtliniendokumente eine IAM-Richtlinie erstellen, finden Sie unter Erstellen von Richtlinien auf der JSON-Registerkarte im IAM-Benutzerhandbuch.

Sie können auch eine IAM-Richtlinie erstellen, um Benutzern den Zugriff auf bestimmte API-Aktionen zu ermöglichen. Der Zugriff auf API-Aktionen wird separat von der AWS Wickr-Konsole verwaltet. Im Folgenden finden Sie ein Beispiel für eine Richtlinie, die nur Lesezugriff auf bestimmte API-Aktionen gewährt. Weitere Informationen zu API-Aktionen finden Sie unter Willkommen bei der AWS Wickr API-Referenz.

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

```
            "Effect": "Allow",
            "Action": [
                "wickr:ListNetworks",
                "wickr:ListUsers",
                "wickr:GetNetworkSettings",
                "wickr:GetNetwork",
                "wickr:GetUser",
                "wickr:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

Themen

- Best Practices für Richtlinien
- Verwendung der AWS-Managementkonsolefür Wickr
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Best Practices für Richtlinien

Identity-based Richtlinien legen fest, ob jemand Wickr-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder diese löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Wenn Sie identitätsbasierte Richtlinien erstellen oder bearbeiten, befolgen Sie diese Richtlinien und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWSverwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien oder Von AWS verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt

als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.

- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werdenAWS-Service, z. CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordertAWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Best Practices für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwendung der AWS-Managementkonsolefür Wickr

Hängen Sie die `AWSWickrFullAccess` AWS verwaltete Richtlinie an Ihre IAM-Identitäten an, um ihnen volle Administratorrechte für den Wickr-Service zu gewähren, einschließlich der Wickr-Administratorkonsole in der. AWS-Managementkonsole Weitere Informationen finden Sie unter AWSverwaltete Richtlinie: AWSWickrFullAccess.

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer

Benutzeridentität angefügt sind. Diese Richtlinie beinhaltet Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der OR-API. AWS CLI AWS

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

Fehlerbehebung bei Identität und Zugriff auf AWS Wickr

Hilfe zur Diagnose und Behebung häufiger Probleme mit IAM finden Sie unter Problembehandlung bei IAM im Benutzerhandbuch. AWS Identity and Access Management

Compliance-Validierung

Eine Liste der AWS Services im Rahmen bestimmter Compliance-Programme finden Sie unter AWSServices im Umfang nach Compliance-Programmen AWS . Allgemeine Informationen finden Sie unter AWSCompliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladenAWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung von Vorschriften bei der Verwendung von Wickr hängt von der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWSstellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung von Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance Schnellstartanleitungen zu — In diesen Bereitstellungshandbüchern werden architektonische Überlegungen erörtert und Schritte für die Implementierung von sicherheits- und Compliance-orientierten Basisumgebungen beschrieben. AWS
- AWSRessourcen zur AWS von Vorschriften — Diese Sammlung von Arbeitsmappen und Leitfäden kann auf Ihre Branche und Ihren Standort zutreffen.
- Bewertung von Ressourcen anhand von Regeln im AWS ConfigEntwicklerhandbuch — AWS Config; bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub CSPM— Dieser AWS Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus, sodass Sie überprüfen könnenAWS, ob Sie die Sicherheitsstandards und Best Practices der Branche einhalten.

Resilienz in AWS Wickr

Die AWS globale Infrastruktur basiert AWS-Regionen auf Availability Zones. AWS-Regionenbieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWSGlobale Infrastruktur.

Zusätzlich zur AWS globalen Infrastruktur bietet Wickr mehrere Funktionen, die Sie bei Ihren Anforderungen an Datenstabilität und Datensicherung unterstützen. Weitere Informationen finden Sie unter Datenspeicherung für AWS Wickr.

AWS PrivateLinkfür AWS Wickr

Mit AWS PrivateLink for AWS Wickr können Sie mithilfe von Schnittstellen-VPC-Endpunkten eine private Verbindung zwischen Ihrer Virtual Private Cloud (VPC) und einer Teilmenge von Endpunkten in AWS Wickr herstellen. Schnittstellen-VPC-Endpoints basieren auf einer AWS TechnologieAWS PrivateLink, mit der Sie mithilfe AWS von privaten IP-Adressen auf Dienste zugreifen können, auf denen sie ausgeführt werden.

Verwenden Sie für mobile Clients oder andere lokale Geräte ein VPN, um Ihr Gerät mit der VPC zu verbinden, um eine private Ende-zu-Ende-Konnektivität zu gewährleisten. Weitere Informationen finden Sie in der AWS Virtual Private NetworkDokumentation.

Weitere Informationen zu AWS PrivateLink und AWS VPC finden Sie unter Was istAWS PrivateLink? im AWS PrivateLinkLeitfaden und Was ist AWS VPC? im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Unterstützte AWS Wickr-Services

Die folgenden AWS Wickr-Services werden unterstütztAWS PrivateLink:

Service	Endpunktformat
AWS Wickr-Administrator	`com.amazonaws.` *`your-region`* `.wickr-admin`
AWS Wickr Nachricht enübermittlung	`com.amazonaws.` *`your-region`* `.wickr-messaging`
AWS Wickr Telefonieren	`com.amazonaws.` *`your-region`* `.wickr-calling`

Für alle Wickr VPC-Endpunkte müssen derzeit private DNS-Namen aktiviert sein. Weitere Informationen finden Sie unter Private DNS-Namen aktivieren.

Wickr VPC Endpoints unterstützt FIPS in Regionen, in denen die öffentlichen Wickr-Endpunkte FIPS unterstützen. Weitere Informationen finden Sie unter Federal Information Processing Standard.

Derzeit nicht unterstützt

- VPC-Endpunktrichtlinien für Messaging- und Calling-Endpunkte
- Endpunkte für Nachrichten und Anrufe sind in nicht verfügbar. `us-east-1`

Topics

Voraussetzungen

Stellen Sie vor dem Erstellen von VPC-Endpoints sicher, dass Sie die folgenden Voraussetzungen erfüllen:

1. VPC-Konfiguration: Eine ordnungsgemäß konfigurierte VPC mit Subnetzen in mehreren Availability Zones
2. Sicherheitsgruppen: Geeignete Sicherheitsgruppen, die HTTPS-Verkehr zulassen (Port 443)
3. DNS-Auflösung: In der VPC aktivierte DNS-Hostnamen und DNS-Auflösungen
4. IAM-Berechtigungen: Erforderliche Berechtigungen zum Erstellen und Verwalten von VPC-Endpoints

Erstellen von VPC-Endpunkten

Sie können einen VPC-Endpunkt für AWS Wickr Admin, Messaging und Calling erstellen.

Gehen Sie wie folgt vor, um mithilfe der AWS Konsole einen VPC-Endpunkt zu erstellen.

Schritt 1: Navigieren Sie zur VPC-Konsole

1. Melden Sie sich bei der Amazon VPC-Konsole an.
2. Wählen Sie im linken Navigationsbereich die Option Endpoints (Endpunkte) aus.
3. Klicken Sie auf Endpunkt erstellen.

Schritt 2: Endpunkteinstellungen konfigurieren

1. Wählen Sie unter Dienstkategorie die Option AWSDienste aus.
2. Suchen Sie unter Dienstname nach dem entsprechenden Dienst `wickr` und wählen Sie ihn aus:
   - Für Admin: `com.amazonaws.`*`your-region`*`.wickr-admin`
   - Für Nachrichten: `com.amazonaws.`*`your-region`*`.wickr-messaging`
   - Zum Anrufen: `com.amazonaws.`*`your-region`*`.wickr-calling`

Schritt 3: Netzwerkkonfiguration

1. Wählen Sie unter VPC Ihre Ziel-VPC aus.
2. Wählen Sie unter Subnetze Subnetze in mehreren Availability Zones für hohe Verfügbarkeit aus.
3. Wählen Sie unter Privaten DNS-Namen aktivieren das Kontrollkästchen aus. Dadurch wird die Unterstützung für private DNS-Namen aktiviert.
4. Wählen oder erstellen Sie unter Sicherheitsgruppen Sicherheitsgruppen, die Sie den Netzwerkschnittstellen der Endpunkte zuordnen möchten.

Schritt 4: Endpunkt erstellen

1. Überprüfen Sie die Sicherheitskonfiguration.
2. Optional können Sie Tags hinzufügen oder entfernen. Tags sind Name-Wert-Paare, die Sie verwenden, um sie Ihrem Endpunkt zuzuordnen.
3. Klicken Sie auf Endpunkt erstellen.

Gehen Sie wie folgt vor, um einen VPC-Endpunkt mit AWS CLI zu erstellen.

1. Überprüfen Sie die Serviceverfügbarkeit in Ihrer Region:

   Überprüfen Sie die Verfügbarkeit von Wickr Admin

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

Überprüfen Sie die Verfügbarkeit von Wickr Messaging

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

Prüfen Sie die Verfügbarkeit von Wickr Calling

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

2. Erstellen Sie VPC-Endpoints.

Wickr Admin-Endpunkt:

```
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 Messaging-Endpunkt

```
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 Calling-Endpunkt

```
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 \
```

Einschränkungen

Die folgenden Funktionen werden nicht unterstützt AWS PrivateLink und erfordern eine Internetverbindung:

- Wickr Open Access (WOA)
- Aktualisierungen der Client-Anwendungen
  - Mobile Apps (iOS/Android)
    - Quelle: App Store/Google Play Store
    - Anforderung: Internetzugang erforderlich
  - Desktopanwendungen
    - Windows/Mac: Verwendet globale S3-Endpunkte (nicht AWS PrivateLink kompatibel)
    - Linux: Verwendet Snap Store (erfordert Internetzugang)
- Debugging und Telemetrie
  - Absturzberichte
  - Metriken debuggen
  - Client-side Links zu Analysen
- Mobile Push-Benachrichtigungen

  Diese Dienste erfordern eine Internetverbindung und können Folgendes nicht verwendenAWS PrivateLink:

  - Apple-Push-Benachrichtigungen
    - Voraussetzung: Direkter Internetzugang
    - Anschlüsse: 443, 2195, 2196, 5223
    - Referenz: Apple-Supportdokumentation

  - Google/Android Benachrichtigungen
    - Anforderung: Firebase Cloud Messaging-Zugriff
    - Referenz: Firebase-Dokumentation
- Die AWS Wickr Console wird derzeit nicht für Private Access unterstützt. Weitere Informationen finden Sie unter UnterstütztAWS-Regionen, Servicekonsolen und Funktionen für Private Access.

Erforderliche Mindestversionen der Clients fürAWS PrivateLink

Die folgenden Client-Versionen wurden mit validiertAWS PrivateLink:

- iOS 6.64 (falls zutreffend)
- Android 6.60 (falls zutreffend)
- Desktop-Clients 6.60
- Bots 6.60

Funktionen, die eine zusätzliche Konfiguration erfordern

Stiefel aus Korbgeflecht

- Anforderung: Infrastruktur Customer-managed
- Aktion: Konfigurieren Sie Netzwerkpfade für Bot-Abhängigkeiten
- Überlegung: Stellen Sie sicher, dass Bots die erforderlichen AWS Dienste über VPC-Endpunkte erreichen können

Downloads von Dateien

- S3-Konnektivität: Für Dateioperationen erforderlich (außer Region Frankfurt)
- Lösung: Erstellen Sie einen S3-VPC-Gateway-Endpunkt
- Referenz: AWS PrivateLinkfür Amazon S3

Infrastruktursicherheit in AWS Wickr

Als verwalteter Service ist AWS Wickr durch die AWS globalen Netzwerksicherheitsverfahren geschützt, die im Whitepaper Amazon Web Services: Security Processes im Überblick beschrieben sind.

Konfiguration und Schwachstellenanalyse in AWS Wickr

Konfiguration und IT-Kontrollen liegen in der gemeinsamen Verantwortung von AWS Ihnen, unserem Kunden. Weitere Informationen finden Sie im Modell der AWS gemeinsamen Verantwortung.

Es liegt in Ihrer Verantwortung, Wickr gemäß den Spezifikationen und Richtlinien zu konfigurieren, Ihre Benutzer regelmäßig anzuweisen, die neueste Version des Wickr-Clients herunterzuladen, sicherzustellen, dass Sie die neueste Version des Wickr-Datenaufbewahrungsbots ausführen, und die Nutzung von Wickr durch Ihre Benutzer zu überwachen.

Bewährte Sicherheitsmethoden für AWS Wickr

Wickr bietet eine Reihe von Sicherheitsfunktionen, die Sie bei der Entwicklung und Implementierung Ihrer eigenen Sicherheitsrichtlinien berücksichtigen sollten. Die folgenden bewährten Methoden sind allgemeine Richtlinien und keine vollständige Sicherheitslösung. Da diese bewährten Methoden für Ihre Umgebung möglicherweise nicht angemessen oder ausreichend sind, sollten Sie sie als hilfreiche Überlegungen und nicht als bindend ansehen.

Um potenzielle Sicherheitsereignisse im Zusammenhang mit Ihrer Nutzung von Wickr zu verhindern, befolgen Sie diese bewährten Methoden:

- Implementieren Sie den Zugriff mit den geringsten Rechten und erstellen Sie spezielle Rollen, die für Wickr-Aktionen verwendet werden sollen. Verwenden Sie IAM-Vorlagen, um eine Rolle zu erstellen. Weitere Informationen finden Sie unter AWSverwaltete Richtlinien für AWS Wickr.
- Greifen Sie auf die AWS-Managementkonsole für Wickr zu, indem Sie sich bei der ersten authentifizieren. AWS-Managementkonsole Geben Sie Ihre persönlichen Konsolenanmeldeinformationen nicht weiter. Jeder Benutzer im Internet kann die Konsole aufrufen, aber er kann sich nur anmelden oder eine Sitzung starten, wenn er über gültige Anmeldeinformationen für die Konsole verfügt.

Überwachung von AWS Wickr

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von AWS Wickr und Ihren anderen AWS Lösungen. AWS bietet die folgenden Überwachungstools, um Wickr zu beobachten, zu melden, wenn etwas nicht stimmt, und gegebenenfalls automatische Maßnahmen zu ergreifen:

- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch. Weitere Informationen zur Protokollierung von Wickr-API-Aufrufen mithilfe von CloudTrail. Protokollieren von AWS Wickr API-Aufrufen mit AWS CloudTrail

Protokollieren von AWS Wickr API-Aufrufen mit AWS CloudTrail

AWS Wickr ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Service in Wickr ausgeführt wurden. CloudTrail erfasst alle API-Aufrufe für Wickr als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von AWS-Managementkonsole for Wickr und Code-Aufrufe der Wickr-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Wickr. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an Wickr gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln. Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Informationen zu Wickr finden Sie unter CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn in Wickr Aktivitäten auftreten, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können in Ihrem AWS-Konto die neusten Ereignisse anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit dem CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem Konto AWS-Konto, einschließlich der Ereignisse für Wickr, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle Wickr-Aktionen werden von CloudTrail protokolliert. Beispielsweise generieren Aufrufe von und `ListNetworks` Aktionen Einträge in den CloudTrail Protokolldateien. `CreateAdminSession`

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlegendes zu den Einträgen in Wickr-Protokolldateien

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `CreateAdminSession` Aktion demonstriert.


```
{
    "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"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `CreateNetwork` Aktion demonstriert.

```
{
    "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"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `ListNetworks` Aktion demonstriert.

```
{
    "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"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `UpdateNetworkdetails` Aktion demonstriert.

```
{
    "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"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `TagResource` Aktion demonstriert.

```
{
    "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"
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `ListTagsForResource` Aktion demonstriert.

```
{
    "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"
}
```


Analyse-Dashboard in AWS Wickr

Sie können das Analyse-Dashboard verwenden, um zu sehen, wie Ihr Unternehmen AWS Wickr verwendet. Das folgende Verfahren erklärt, wie Sie mithilfe der AWS Wickr-Konsole auf das Analyse-Dashboard zugreifen können.

So greifen Sie auf das Analyse-Dashboard zu

1. Öffnen Sie sie AWS-Managementkonsole für Wickr unter https://console.aws.amazon.com/wickr/.
2. Wählen Sie auf der Seite Netzwerke den Netzwerknamen aus, um zu diesem Netzwerk zu navigieren.
3. Wählen Sie im Navigationsbereich Analytics aus.

Auf der Analytics-Seite werden die Metriken für Ihr Netzwerk in verschiedenen Tabs angezeigt.

Auf der Analytics-Seite finden Sie in der oberen rechten Ecke jedes Tabs einen Zeitrahmenfilter. Dieser Filter gilt für die gesamte Seite. Darüber hinaus können Sie in der oberen rechten Ecke jeder Registerkarte die Datenpunkte für den ausgewählten Zeitraum exportieren, indem Sie die verfügbare Exportoption auswählen.

> **Note**
>
> Die gewählte Zeit ist in UTC (Universal Time Coordinated) angegeben.

Die folgenden Tabs sind verfügbar:

- In der Übersicht wird angezeigt:
  - Registriert — Die Gesamtzahl der registrierten Benutzer, einschließlich aktiver und gesperrter Benutzer im Netzwerk in der ausgewählten Zeit. Ausstehende oder eingeladene Benutzer sind nicht enthalten.
  - Ausstehend — Die Gesamtzahl der ausstehenden Benutzer im Netzwerk in der ausgewählten Zeit.
  - Benutzerregistrierung — In der Grafik wird die Gesamtzahl der im ausgewählten Zeitraum registrierten Benutzer angezeigt.
  - Geräte — Die Anzahl der Geräte, auf denen die App aktiv war.
  - Client-Versionen — Die Anzahl der aktiven Geräte, sortiert nach ihren Client-Versionen.

- Mitglieder zeigt an:
  - Status — Aktive Benutzer im Netzwerk innerhalb des ausgewählten Zeitraums.
  - Aktive Benutzer —
    - Das Diagramm zeigt die Anzahl der aktiven Benutzer im Zeitverlauf an und kann nach Tagen, Wochen oder Monaten (innerhalb des oben ausgewählten Zeitraums) aggregiert werden.
    - Die Anzahl der aktiven Benutzer kann nach Plattform, Client-Version oder Sicherheitsgruppe aufgeschlüsselt werden. Wenn eine Sicherheitsgruppe gelöscht wurde, wird die Gesamtzahl als Gelöscht# angezeigt.

- Meldungen werden angezeigt:
  - Gesendete Nachrichten — Die Anzahl der eindeutigen Nachrichten, die von allen Benutzern und Bots im Netzwerk im ausgewählten Zeitraum gesendet wurden.
  - Anrufe — Anzahl der eindeutigen Anrufe, die von allen Benutzern im Netzwerk getätigt wurden.
  - Dateien — Anzahl der von Benutzern im Netzwerk gesendeten Dateien (einschließlich Sprachnotizen).
  - Geräte — Das Kreisdiagramm zeigt die Anzahl der aktiven Geräte, sortiert nach ihrem Betriebssystem.
  - Client-Versionen — Die Anzahl der aktiven Geräte, sortiert nach ihren Client-Versionen.

Probleme mit AWS Wickr beheben

Die folgenden Verfahren und Tipps können Ihnen bei der Behebung von Problemen mit AWS Wickr helfen.

Wenn Sie das Problem mit den Schritten in diesem Handbuch nicht lösen können, öffnen Sie eine Support-Anfrage im AWS Support Center.

Topics

Behebung allgemeiner Probleme mit AWS Wickr

Im Folgenden finden Sie Tipps zur Fehlerbehebung, die Ihnen bei der Lösung allgemeiner Probleme mit AWS Wickr helfen sollen. Wenn die Schritte in diesem Abschnitt Ihr Problem nicht lösen, öffnen Sie einen Fall im AWS Support Center.

Topics

Bevor Sie beginnen

Überprüfen Sie vor der Fehlerbehebung Folgendes:

- Sie verwenden das richtige Wickr-Produkt für Ihre Organisation: AWS Wickr, AWS WickrGov(GovCloud) oder Wickr Enterprise (selbst gehostet). Wenn Sie sich nicht sicher sind, wenden Sie sich an Ihren Netzwerkadministrator.

- Sie verwenden eine unterstützte Client-Version. AWS Wickr unterstützt die aktuelle Version und die vorherigen 2—3 Versionen. Um Ihre Version zu überprüfen, öffnen Sie Wickr und wählen Sie Einstellungen, Über uns. Informationen zum Aktualisieren finden Sie unter Nach Updates suchen.
- Sie haben die richtige Authentifizierungsmethode für Ihre Organisation (SSO oder Nicht-SSO).
- Sie haben Ihr Benutzerpasswort und den Wickr-Wiederherstellungsschlüssel an einem sicheren Ort gespeichert.
- Ihr Netzwerk ermöglicht die Kommunikation mit den erforderlichen Wickr-Domänen und -Ports.
- Ihr Gerät erfüllt die Systemanforderungen.

Sammeln von Diagnoseinformationen

Client-Protokolle

Client-Protokolle sind für die Behebung der meisten Probleme mit AWS Wickr unerlässlich.

Gehen Sie wie folgt vor, um Client-Protokolle zu sammeln.

1. Melden Sie sich beim Wickr-Client an.
2. Wählen Sie im Navigationsbereich das Menü (drei Linien oder Punkte) und dann Support aus.
3. Wählen Sie Support Logging.
4. Wählen Sie Protokolle speichern.
5. Notieren Sie sich den Ort, an dem die Protokolle gespeichert werden.

Speicherorte nach Plattform protokollieren:

- Windows: `C:\Users\<USERNAME>\AppData\Local\Wickr, LLC\Wickr Pro\logs\`
- macOS: `~/Library/Application Support/Wickr, LLC/Wickr Pro/logs/`
- Linux: `~/.local/share/Wickr, LLC/Wickr Pro/logs/`
- iOS: Export über das Support Logging-Menü
- Android: Export über das Support Logging-Menü

Zu sammelnde Informationen

Erfassen Sie bei der Problembehandlung oder bei der Kontaktaufnahme mit dem Support:

- Geräteinformationen: Modell, Betriebssystemversion
- Client-Version: Zu finden in den Einstellungen unter Info
- Netzwerk-ID: In der Admin-Konsole unter Netzwerkeinstellungen zu finden
- Fehlermeldung: Exakter Text oder Screenshot
- Zeitstempel: Wann das Problem aufgetreten ist
- Schritte zur Reproduktion: So stellen Sie das Problem erneut her
- Client-Logs: Aus dem Menü Support Logging

Häufige Fehlermeldungen

Es konnte keine Verbindung zu Wickr-Servern hergestellt werden.

Mögliche Ursachen:

- Problem mit der Netzwerkverbindung
- Firewall blockiert Wickr-Verkehr
- VPN- oder Proxy-Interferenz

Resolution (Auflösung)

1. Testen Sie Mobilfunkdaten im Vergleich WiFi zu Unternehmensdaten, um Netzwerkprobleme zu isolieren.
2. Überprüfen Sie die Netzwerkanforderungen.
3. Wenden Sie sich an Ihr IT-Team, um die erforderlichen Domänen und Ports auf eine Zulassungsliste zu setzen.

Dieser Benutzer gehört zu einem anderen Netzwerk.

Mögliche Ursache: Das Benutzerkonto existiert in einem anderen Wickr-Netzwerk

Resolution (Auflösung)

1. Stellen Sie sicher, dass Sie die richtige AWS Wickr-Client-Version verwenden.
2. Wenden Sie sich an Ihren Netzwerkadministrator.

3. Wenn das Problem weiterhin besteht, wenden Sie sich mit Benutzer-E-Mail und Netzwerk-ID an den AWS Support.

Konto gesperrt

Mögliche Ursache: Mehrere fehlgeschlagene Anmeldeversuche oder Administratoraktion

Resolution (Auflösung)

1. Wenden Sie sich an Ihren Netzwerkadministrator, um eine mögliche Sperre aufzuheben.
2. Wenn Sie der einzige Administrator sind, wenden Sie sich an den AWS Support.

E-Mail-Bestätigung erforderlich

Mögliche Ursache: Die E-Mail-Bestätigung wurde bei der Registrierung nicht abgeschlossen.

Resolution (Auflösung)

1. Suchen Sie in den spam/junk Ordnern nach Bestätigungs-E-Mails.
2. Bestätigen Sie, dass die E-Mail-Adresse korrekt ist.
3. Erkundigen Sie sich bei Ihrem IT-Team nach der E-Mail-Filterung.
4. Fordern Sie vom Anmeldebildschirm aus eine neue Bestätigungs-E-Mail an.

Behebung von Anmelde- und Registrierungsproblemen

Dieser Abschnitt hilft Ihnen bei der Behebung von Anmelde- und Registrierungsproblemen mit AWS Wickr. Wenn die Schritte in diesem Abschnitt Ihr Problem nicht lösen, öffnen Sie einen Fall im AWSSupport Center.

Topics

- Sammeln von Protokollen

Bevor Sie beginnen

Überprüfen Sie Folgendes, bevor Sie Probleme mit der Anmeldung oder Registrierung beheben:

- Sie verwenden das richtige Wickr-Produkt für Ihre Organisation: AWS Wickr, AWSWickrGov(GovCloud) oder Wickr Enterprise (selbst gehostet). Wenn Sie sich nicht sicher sind, wenden Sie sich an Ihren Netzwerkadministrator.
- Sie verwenden eine unterstützte Client-Version. AWS Wickr unterstützt die aktuelle Version und die vorherigen 2—3 Versionen. Um Ihre Version zu überprüfen, öffnen Sie Wickr und wählen Sie Einstellungen, Über uns. Informationen zum Update finden Sie unter Nach Updates suchen.
- Sie haben die richtige Authentifizierungsmethode für Ihre Organisation (SSO oder Nicht-SSO).
- Sie haben Ihr Benutzerpasswort und den Wickr-Wiederherstellungsschlüssel an einem sicheren Ort gespeichert.
- Ihr Netzwerk ermöglicht die Kommunikation mit den erforderlichen Wickr-Domänen und -Ports.
- Ihr Gerät erfüllt die Systemanforderungen.

> **Tip**
>
> Wenn Sie bei der Anmeldung oder Registrierung auf einen Fehler stoßen, machen Sie vor der Fehlerbehebung einen Screenshot der Fehlermeldung. Dies hilft Ihrem Administrator oder AWS Support, das Problem schneller zu diagnostizieren.

Häufige Probleme bei der Anmeldung

Wenn die Anmeldung fehlschlägt, bestimmt die Fehlermeldung den Pfad zur Fehlerbehebung. Identifizieren Sie zunächst, welcher Fehler angezeigt wird.

„Falsches Passwort“ oder Anmeldedaten wurden zurückgewiesen

1. Stellen Sie sicher, dass Sie das richtige Passwort eingeben. Achten Sie auf Tippfehler, zusätzliche Leerzeichen und Feststelltaste.
2. Wenn Sie SSO (Okta, Microsoft Entra ID, Amazon Cognito) verwenden, setzen Sie Ihr Passwort über Ihren Identitätsanbieter zurück — nicht über Wickr.

3. Wenn Sie Anmeldeinformationen verwenden, finden Sie weitere Informationen unter Wickr-managed . the section called “Zurücksetzen des Passworts”

„Server kann nicht erreicht werden“ oder Verbindungsfehler

Dies weist auf ein Netzwerkproblem hin, nicht auf ein Kontoproblem.

1. Stellen Sie sicher, dass Ihre Internetverbindung aktiv ist.
2. Wechseln Sie zwischen Netzwerken — versuchen Sie es stattdessen mit Mobilfunkdaten oder umgekehrt. WiFi
3. Wenn Sie sich in einem Unternehmensnetzwerk befinden, bitten Sie Ihr IT-Team, zu überprüfen, ob die erforderlichen Wickr-Domänen und -Ports zulässig sind.
4. Wenn Sie ein VPN verwenden, versuchen Sie, die Verbindung vorübergehend zu trennen.
5. Wenn das Problem weiterhin besteht, sammeln Sie Protokolle und wenden Sie sich an Ihren Netzwerkadministrator.

„Konto nicht gefunden“ oder „Benutzer nicht gefunden“

1. Stellen Sie sicher, dass Sie sich beim richtigen Wickr-Produkt anmelden (AWS Wickr im WickrGov Vergleich zu Enterprise).
2. Stellen Sie sicher, dass Ihr Benutzername oder Ihre E-Mail-Adresse korrekt eingegeben wurde.
3. Ihr Konto wurde möglicherweise aus dem Netzwerk entfernt. Wenden Sie sich an Ihren Netzwerkadministrator.

„Konto gesperrt“

Siehe the section called “Sperrung des Kontos”.

„Dieser Benutzer gehört zu einem anderen Netzwerk“

1. Möglicherweise haben Sie versehentlich ein Konto in einem anderen Wickr-Netzwerk erstellt (siehethe section called “Problem mit Gastbenutzern”).
2. Stellen Sie sicher, dass Sie den richtigen Wickr-Client für Ihre Organisation verwenden.
3. Wenden Sie sich an Ihren Netzwerkadministrator. Der Administrator muss sich möglicherweise mit Ihrer E-Mail-Adresse und Netzwerk-ID an den AWS Support wenden, um den Konflikt zu lösen.

Die Anmeldung schlägt auf dem Handy fehl, funktioniert aber auf dem Desktop

1. Stellen Sie sicher, dass Sie das richtige Passwort eingeben.
2. Testen Sie mit Mobilfunkdaten — deaktivieren Sie es WiFi und versuchen Sie es erneut. Wenn Mobilfunk funktioniert, aber WiFi nicht, liegt das Problem an Ihrer Netzwerkkonfiguration. Wenden Sie sich an Ihr IT-Team.
3. Vergewissern Sie sich, dass die Wickr-App über die erforderlichen Geräteberechtigungen verfügt.
4. Deinstallieren Sie AWS Wickr aus Ihrem App Store und installieren Sie es erneut.

> **Note**
>
> Durch die Neuinstallation wird der lokale Nachrichtenverlauf gelöscht.

Andere Anmeldefehler

Wenn Ihr Fehler oben nicht aufgeführt ist:

1. Vergewissern Sie sich, dass Sie das richtige Passwort eingeben.
2. Machen Sie einen Screenshot der Fehlermeldung.
3. Erfassen Sie Protokolle für Ihre Plattform.
4. Wenden Sie sich mit dem Screenshot und den Protokollen an Ihren Netzwerkadministrator.

Probleme bei der Registrierung

Problem mit Gastbenutzern

Symptom: Nach der Registrierung wird der Bildschirm „Gastnetzwerk“ angezeigt und Sie können keine anderen Benutzer in den Kontakten Ihrer Organisation sehen.

Ursache: Sie haben die Registrierung direkt initiiert, anstatt die Registrierung über eine Einladung Ihres Administrators abzuschließen. Dadurch wird ein Gastbenutzerkonto erstellt, anstatt dem Netzwerk Ihrer Organisation beizutreten.

Auflösung

1. Wenden Sie sich an Ihren Netzwerkadministrator.

2. Der Administrator muss das Gastbenutzerkonto löschen und Sie dann erneut zum richtigen Netzwerk einladen.
3. Schließen Sie die Registrierung über den Einladungslink oder den Code Ihres Administrators ab.

„Dieser Benutzer gehört zu einem anderen Netzwerk“

Ursache: Sie haben versehentlich ein Konto in einem anderen Wickr-Netzwerk erstellt oder Sie verwenden den falschen Client.

1. Stellen Sie sicher, dass Sie den richtigen Client verwenden: AWS Wickr für kommerzielle Netzwerke GovCloud, WickrGovfür oder Wickr Enterprise für selbst gehostete.
2. Laden Sie den richtigen Client von der AWS Wickr-Downloadseite herunter.
3. Wenden Sie sich an Ihren Netzwerkadministrator. Der Administrator muss sich möglicherweise mit Ihrer E-Mail-Adresse und Netzwerk-ID an den AWS Support wenden.

Fehler beim Format des Benutzernamens

Für Benutzernamen in AWS Wickr gelten die folgenden Anforderungen:

- Benutzernamen sind permanent — sie können nach der Erstellung nicht mehr geändert werden.
- Die E-Mail-Adresse ist die primäre Kennung für die Registrierung.
- Benutzernamen dürfen keine Sonderzeichen enthalten, die nicht unterstützt werden. Alphanumerische Zeichen, Punkte, Bindestriche und Unterstriche werden generell unterstützt.
- Bei SSO-enabled Netzwerken wird die Benutzererstellung vom Identity Provider (IdP) übernommen. Benutzer müssen auf der Identitätsseite existieren, bevor sie sich beim Wickr-Client anmelden können.

E-Mail-Bestätigung nicht erhalten

1. Überprüfe deinen Spam- oder Junk-Ordner.
2. Vergewissern Sie sich, dass die von Ihnen eingegebene E-Mail-Adresse korrekt ist.
3. Wenden Sie sich an Ihr IT-Team, um sicherzustellen, dass E-Mails von AWS Wickr nicht durch E-Mail-Filter blockiert werden.
4. Kehren Sie zum Anmeldebildschirm zurück und wählen Sie die Option, die Bestätigungs-E-Mail erneut zu senden.

Zurücksetzen des Passworts

> **Note**
>
> Bei SSO-enabled Konten erfolgt das Zurücksetzen des Passworts über Ihren Identitätsanbieter (Microsoft Entra ID, Okta, Amazon Cognito oder) — nicht über Wickr.

Ablauf beim Zurücksetzen des Passworts (ohne SSO):

> **Important**
>
> Das Zurücksetzen eines Wickr-Passworts ist ein vollständiges Zurücksetzen des Kontos. Dadurch wird der gesamte lokale Nachrichtenverlauf dauerhaft gelöscht, der Benutzer wird aus allen Räumen entfernt und die Geräteregistrierung wird gelöscht. Der Benutzer muss erneut in Räume eingeladen werden, an denen er zuvor teilgenommen hat. Dies kann nicht rückgängig gemacht werden. Empfehlen Sie den Benutzern, alle anderen Optionen auszuschöpfen (Feststelltaste überprüfen, gespeicherte Passwörter überprüfen, ein anderes Gerät ausprobieren), bevor Sie fortfahren.

1. Wählen Sie auf dem Wickr-Anmeldebildschirm die Option Passwort vergessen?
2. Geben Sie die E-Mail-Adresse ein, die mit Ihrem AWS Wickr-Konto verknüpft ist.
3. Suchen Sie in Ihrem Posteingang nach einer E-Mail zum Zurücksetzen des Passworts. Überprüfen Sie die spam/junk Ordner, wenn Sie sie nicht innerhalb weniger Minuten erhalten haben.
4. Wählen Sie den Link zum Zurücksetzen des Passworts in der E-Mail. Links zum Zurücksetzen des Passworts laufen nach 24 Stunden ab.
5. Geben Sie Ihr neues Passwort ein und bestätigen Sie es. Ihr Passwort muss den von Ihrem Netzwerkadministrator konfigurierten Komplexitätsanforderungen entsprechen.

Anforderungen an die Komplexität von Kennwörtern

Die Kennwortanforderungen werden von Ihrem Administrator in der Admin-Konsole unter Sicherheitsgruppeneinstellungen konfiguriert. Zu den Anforderungen können gehören:

- Mindestlänge (mindestens 8 Zeichen; der Administrator kann eine höhere Länge festlegen)
- Erforderliche Anzahl von Kleinbuchstaben

- Erforderliche Anzahl von Großbuchstaben
- Erforderliche Anzahl von Zahlen
- Erforderliche Anzahl von Sonderzeichen

Ab der Client-Version 6.70 werden die Anforderungen an die Passwortkomplexität bei der Kontoerstellung und bei Passwortänderungen auf Android und iOS inline angezeigt.

Sperrung des Kontos

Symptom: Bei der Anmeldung wird der Fehler „Konto gesperrt“ angezeigt.

Für reguläre Benutzer:

1. Wenden Sie sich an Ihren Netzwerkadministrator.
2. Der Administrator kann die Sperre unter Admin-Konsole > Teamverzeichnis > Benutzer suchen > Sperren aufheben.

Für einen einzelnen Administrator (kein anderer Administrator, der die Sperre aufheben kann):

Wenden Sie sich mit Ihrer E-Mail-Adresse, Netzwerk-ID und Bestätigung des Administratorstatus an den AWS Support.

Kontosperrung aufgrund fehlgeschlagener Anmeldeversuche:

- Warten Sie 24 Stunden auf die automatische Entsperrung, oder
- Wenden Sie sich an Ihren Netzwerkadministrator, um Ihr Konto manuell zu entsperren, oder
- Verwenden Sie den the section called “Zurücksetzen des Passworts” Flow, um Ihre Anmeldeinformationen zurückzusetzen und Ihr Konto zu entsperren.

Wenn du dich nach Aufhebung der Sperre nicht anmelden kannst:

Wenden Sie sich mit Ihrer E-Mail-Adresse, Netzwerk-ID, Client-Version (Wickr > Einstellungen > Info) und Betriebssystemversion an den AWS Support.

Sammeln von Protokollen

Die Methoden zur Erfassung von Protokollen unterscheiden sich je nach Plattform. Sammeln Sie Protokolle, bevor Sie sich an Ihren Administrator oder AWS Support wenden.

Desktop

Wenn Sie auf das Wickr-Menü zugreifen können:

1. Öffnen Sie Wickr und wählen Sie das Hamburger-Menü (☰), dann Support, Support Logging.
2. Aktivieren Sie die Option Support-Protokollierung zulassen. Aktivieren Sie für Untersuchungen auch die Option Extended Logging Detail.
3. Reproduzieren Sie das Problem.
4. Kehren Sie zu Support zurück und wählen Sie Protokolle speichern. Teilen Sie die Datei mit Ihrem Administrator.

Wenn Sie nicht auf das Wickr-Menü zugreifen können (z. B. wenn der Client auf dem Anmeldebildschirm abstürzt), starten Sie den Client mit der `-logging` Flagge, um Protokolle zu generieren:

- macOS: Öffne das Terminal und führe Folgendes aus:

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

  Protokolle werden gespeichert unter`~/Library/Application Support/Wickr, LLC/Wickr Pro/logs/`.
- Windows: Öffnen Sie das Kontextmenü für die AWS Wickr-Verknüpfung, wählen Sie Eigenschaften und dann die Registerkarte Verknüpfung. An den Zielpfad **`-logging`** anhängen (außerhalb der Anführungszeichen). Starten Sie die Verknüpfung.

  Protokolle werden gespeichert unter`C:\Users\<USERNAME>\AppData\Local\Wickr, LLC\Wickr Pro\logs\`.
- Linux: Starten Sie vom Terminal mit der `-logging` Flagge aus.

  Protokolle werden gespeichert unter`~/.local/share/Wickr, LLC/Wickr Pro/logs/`.

Mobil

1. Öffnen Sie Wickr und wählen Sie Einstellungen, Über uns, Alle Protokolle exportieren.
2. Teilen Sie die exportierte Protokolldatei mit Ihrem Administrator.

Wenn Sie nicht auf Einstellungen zugreifen können (z. B. weil Sie auf dem Anmeldebildschirm nicht weiterkommen):

- iOS: Connect dein Gerät mit einem Mac, öffne es Console.app, filtere nach „Wickr“ und reproduziere das Problem.
- Android: Aktivieren Sie das USB-Debugging, stellen Sie eine Verbindung zu einem Computer her und starten Sie es. `adb logcat | grep -i wickr`

SSO- und Authentifizierungsprobleme beheben

Dieser Abschnitt hilft Administratoren bei der Behebung von Single Sign-On (SSO) und Authentifizierungsproblemen mit AWS Wickr. Wenn die Schritte in diesem Abschnitt Ihr Problem nicht lösen, öffnen Sie einen Fall im AWS Support Center.

> **Important**
>
> Wickr unterstützt nur OpenID Connect (OIDC). SAML-based Identitätsanbieter werden nicht unterstützt. Wenn Ihre Organisation einen SAML-only Identitätsanbieter verwendet, müssen Sie eine OIDC-compatible Alternative konfigurieren oder eine OIDC-Bridge implementieren.

Topics

Bevor Sie beginnen

Überprüfen Sie vor der Fehlerbehebung Folgendes:

- Sie haben Administratorzugriff auf die Wickr Admin Console.
- Sie haben Zugriff auf die Identity Provider (IdP) -Konfiguration Ihres Unternehmens.
- SSO ist in Ihren Wickr-Netzwerkeinstellungen aktiviert.
- Ihr Identitätsanbieter ist OIDC-compliant. Wickr unterstützt SAML nicht.

Häufige SSO-Probleme

Unterstützte Identitätsanbieter

Wickr bietet Anleitungen zur Konfiguration der folgenden OIDC-compliant Identitätsanbieter:

- Microsoft Entra ID (früher Azure AD)
- Okta
- Amazon Cognito
- AWS Identity and Access Management Identitätszentrum

Jeder OIDC-compliant Identitätsanbieter kann mit Wickr verwendet werden. Verwenden Sie für Anbieter, die oben nicht aufgeführt sind, die allgemeinen OIDC-Konfigurationsparameter in der Dokumentation Configure SSO.

Benutzer können sich nicht mit SSO anmelden

Wenn Benutzer melden, dass sie sich nicht mit SSO anmelden können, führen Sie die folgenden Prüfungen durch.

Überprüfen Sie die Wickr SSO-Konfiguration

1. Wählen Sie in der Wickr Admin Console Netzwerkeinstellungen und dann Single. Sign-On
2. Bestätigen Sie, dass SSO aktiviert ist.
3. Stellen Sie sicher, dass die Aussteller-URL, die Client-ID und der geheime Clientschlüssel mit Ihrer Identitätsanbieter-Konfiguration übereinstimmen.
4. Stellen Sie sicher, dass die Umleitungs-URI in Ihrem Identitätsanbieter mit dem in der Wickr Admin-Konsole angezeigten Wert übereinstimmt.

Häufige SSO-Fehler

„Benutzer nicht gefunden“

> Der Benutzer ist in Ihrem Identity Provider nicht vorhanden oder wurde der Wickr-Anwendung nicht zugewiesen. Stellen Sie sicher, dass der Benutzer in Ihrem IdP existiert und über die richtigen Gruppenzuweisungen verfügt.

„Ungültige Antwort“ oder „Konfigurationsfehler“

Die OIDC-Metadaten oder Endpunkte sind falsch konfiguriert. Stellen Sie sicher, dass die Aussteller-URL, die Client-ID und die Weiterleitungs-URIs zwischen Wickr und Ihrem Identitätsanbieter übereinstimmen.

„Zugriff verweigert“

Dem Benutzer fehlt die erforderliche Gruppenmitgliedschaft oder Anwendungszuweisung in Ihrem Identity Provider. Überprüfen Sie die Einstellungen für die Anwendungszuweisung Ihres IdP.

Der Benutzer wurde nicht zur Eingabe der Unternehmens-ID aufgefordert

Wenn Benutzer bei der SSO-Registrierung nicht zur Eingabe einer Unternehmens-ID aufgefordert werden, überprüfen Sie, ob die Unternehmens-ID in den Netzwerkeinstellungen, Netzwerkprofil in der Wickr Admin-Konsole konfiguriert ist.

Stellen Sie fest, ob das Problem bei Wickr oder Ihrem Identitätsanbieter liegt

Ermitteln Sie anhand der folgenden Fragen, wo das Problem liegt:

- Können sich Benutzer mit demselben IdP bei anderen Anwendungen authentifizieren? Falls nein, liegt das Problem bei Ihrem Identitätsanbieter, nicht bei Wickr.
- Sind alle Benutzer betroffen oder nur bestimmte Benutzer? Wenn es sich nur um bestimmte Benutzer handelt, überprüfen Sie deren Gruppenzuweisungen und Anwendungszugriff in Ihrem IdP.
- Gab es kürzlich Änderungen an Ihrer IdP-Konfiguration? Zertifikatsrotationen, Richtlinienänderungen oder Endpunktaktualisierungen können die OIDC-Verbindung unterbrechen.
- Tritt der Fehler im Wickr-Client oder auf der IdP-Anmeldeseite auf? Wenn der Fehler auf der IdP-Anmeldeseite erscheint, liegt das Problem bei Ihrem Identitätsanbieter.

Weitere Ressourcen

- SSO in AWS Wickr konfigurieren
- Einrichtung von Microsoft Entra ID SSO (einschließlich Entra-specific Fehlerbehebung)

Behebung von Identitäts- und Zugriffsproblemen

Dieser Abschnitt hilft Administratoren bei der Behebung von Identitäts- und Zugriffsproblemen mit AWS Wickr. Wenn die Schritte in diesem Abschnitt Ihr Problem nicht lösen, öffnen Sie einen Fall im AWS Support Center.

Topics

Bevor Sie beginnen

Überprüfen Sie vor der Fehlerbehebung Folgendes:

- Sie haben Administratorzugriff auf den AWS-Konto , der Ihr Wickr-Netzwerk enthält.
- Sie haben Zugriff auf die IAM-Konsole oder sind berechtigt, IAM-Richtlinien einzusehen.
- Sie wissen, bei welchem IAM-Benutzer oder welcher IAM-Rolle das Zugriffsproblem auftritt.

Häufige Identitäts- und Zugriffsprobleme

Ich bin nicht berechtigt, eine Aktion in der AWS-Managementkonsole für Wickr

Wenn Ihnen das AWS-Managementkonsole für Wickr mitteilt, dass Sie nicht berechtigt sind, eine Aktion auszuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM-Benutzer versucht, mit AWS-Managementkonsole for Wickr Wickr-Netzwerke zu erstellen, zu verwalten oder anzuzeigen, aber nicht über die Berechtigungen und verfügt. `wickr:CreateAdminSession` `wickr:ListNetworks`

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

In diesem Fall bittet Mateo seinen Administrator, seine Richtlinien zu aktualisieren, damit er mithilfe der Aktionen und auf AWS-Managementkonsole for Wickr zugreifen kann. `wickr:CreateAdminSession` `wickr:ListNetworks` Weitere Informationen erhalten

Sie unter Identity-based Richtlinienbeispiele für AWS Wickr und AWSverwaltete Richtlinie: AWSWickrFullAccess.

Behebung von Netzwerk- und Verbindungsproblemen

Dieser Abschnitt hilft Administratoren bei der Behebung von Netzwerk- und Konnektivitätsproblemen mit AWS Wickr. Die meisten von Endbenutzern gemeldeten Verbindungsprobleme werden dadurch verursacht, dass die Unternehmensnetzwerkkonfiguration (Firewalls, Proxys, VPNs) den erforderlichen Wickr-Verkehr blockiert. Wenn die Schritte in diesem Abschnitt Ihr Problem nicht lösen, öffnen Sie einen Fall im AWSSupport Center.

Topics

Bevor Sie beginnen

Überprüfen Sie vor der Fehlerbehebung Folgendes:

- Sie haben Zugriff auf die Netzwerkkonfiguration Ihres Unternehmens (Firewallregeln, Proxyeinstellungen, VPN-Konfiguration).
- Sie haben die Wickr-Netzwerkanforderungen (erforderliche Domänen und Ports) überprüft.
- Sie haben bestätigt, ob das Problem alle Benutzer, bestimmte Benutzer oder bestimmte Standorte betrifft.
- Sie haben bestätigt, ob die betroffenen Benutzer eine Verbindung zu einem unternehmensfremden Netzwerk (Mobilfunknetz oder zu Hause WiFi) herstellen können.

> **Important**
>
> Wenn Benutzer eine Verbindung über mobile Daten oder zu Hause herstellen können, WiFi aber nicht über Ihr Unternehmensnetzwerk, liegt das Problem an Ihrer Netzwerkkonfiguration — nicht am Wickr-Dienst.

Häufige Netzwerkprobleme

Firewall blockiert Wickr-Verkehr

Dies ist die häufigste Ursache für Verbindungsfehler. Wickr benötigt Zugriff auf bestimmte Domänen und Ports.

Symptome

Benutzer können keine Verbindung über Unternehmen herstellen WiFi , können jedoch über Mobilfunkdaten eine Verbindung herstellen. Es sind mehrere Benutzer am selben Standort betroffen. Wickr funktionierte zuvor, wurde aber nach einer Netzwerkänderung eingestellt.

Auflösung

1. Die vollständige Liste der erforderlichen Domänen und Ports finden Sie unter Netzwerkanforderungen für Wickr.
2. Alle erforderlichen Domänen in Ihrer Firewall zulassen. Wickr benötigt HTTPS (TCP 443) für Nachrichten und Signalisierung sowie UDP-Ports für Sprach- und Videoanrufe.
3. Überprüfen Sie die DNS-Auflösung für die erforderlichen Domänen in Ihrem Unternehmensnetzwerk. Verwenden Sie `nslookup` oder`dig`, um die Domänenauflösung zu bestätigen.
4. Testen Sie die Konnektivität, nachdem Sie Änderungen vorgenommen haben. Lassen Sie die betroffenen Benutzer Wickr neu starten und versuchen, eine Verbindung herzustellen.

> **Note**
>
> Wenn nur Sprach- und Videoanrufe fehlschlagen, die Nachrichtenübermittlung jedoch funktioniert, ist der UDP-Verkehr wahrscheinlich blockiert. Wickr verwendet standardmäßig UDP für Anrufe. Siehe the section called “UDP blockiert (Anrufe schlagen fehl, Messaging funktioniert)”.

Interferenz mit dem Proxyserver

Proxyserver von Unternehmen können Wickr-Verbindungen stören, insbesondere wenn sie keine WebSocket Verbindungen unterstützen.

Symptome

Verbindungsprobleme nur, wenn der Proxy konfiguriert ist. Wickr funktioniert, wenn der Proxy umgangen wird. Intermittierende Verbindungsabbrüche.

Auflösung

1. Stellen Sie sicher, dass Ihr Proxy WebSocket Verbindungen unterstützt (erforderlich für Wickr-Messaging).
2. Konfigurieren Sie eine Proxyumgehung (PAC-Dateiausnahme oder Regel für direkte Verbindungen) für Wickr-Domänen, die in den Netzwerkanforderungen aufgeführt sind.
3. Überprüfen Sie die Proxyprotokolle auf blockierte oder fehlgeschlagene Verbindungen zu Wickr-Domänen.
4. Wenn Ihr Proxy eine Authentifizierung erfordert, stellen Sie sicher, dass der Wickr-Verkehr nicht aufgrund fehlender Anmeldeinformationen abgelehnt wird. Wickr unterstützt keine Proxyauthentifizierung in SaaS-Bereitstellungen.

SSL/TLS Inspektion, Verbindungsunterbrechung

Die unternehmensinterne SSL-Inspektion (auch als HTTPS-Inspektion oder TLS-Abfangen bezeichnet) unterbricht die von Wickr erwartete Zertifikatskette, was zu Verbindungsfehlern führt.

Symptome

Zertifikatsfehler in Wickr. Fehler „Sichere Verbindung fehlgeschlagen“. Wickr funktioniert in Netzwerken ohne SSL-Inspektion.

Auflösung

1. Bevorzugt: Umgehen Sie die SSL-Inspektion für Wickr-Domains. Konfigurieren Sie Ihre SSL-Inspektions-Appliance so, dass die in den Netzwerkanforderungen aufgeführten Domänen ausgeschlossen werden. Dadurch wird die Ende-zu-Ende-Verschlüsselung von Wickr beibehalten.
2. Alternative: Installieren Sie das Root-CA-Zertifikat Ihrer Organisation auf Benutzergeräten. Dadurch kann Wickr der abgefangenen Zertifikatskette vertrauen. Wenden Sie sich an Ihr IT-Sicherheitsteam, um das Zertifikat und die Installationsanweisungen zu erhalten.

Um zu überprüfen, ob die SSL-Inspektion die Ursache ist, führen Sie auf einem betroffenen Gerät den folgenden Befehl aus und vergleichen Sie den Zertifikatsaussteller mit dem erwarteten AWS Zertifikat:

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

Wenn der Zertifikatsaussteller die CA Ihrer Organisation anstelle eines AWS oder Amazon-Zertifikats anzeigt, ist die SSL-Inspektion für Wickr-Verkehr aktiv.

VPN blockiert Wickr

VPN-Konfigurationen blockieren häufig den Wickr-Verkehr, insbesondere UDP-Ports, die für Anrufe erforderlich sind.

Symptome

Wickr funktioniert ohne VPN, aber nicht mit verbundenem VPN. Die Verbindung wird unterbrochen, wenn das VPN eine Verbindung herstellt. Anrufe schlagen fehl, aber die Nachrichtenübermittlung funktioniert über VPN.

Auflösung

1. Konfigurieren Sie Split-Tunneling so, dass der Wickr-Verkehr direkt (unter Umgehung des VPN-Tunnels) für die in den Netzwerkanforderungen aufgeführten Domänen weitergeleitet wird.
2. Wenn Split-Tunneling nicht zulässig ist, stellen Sie sicher, dass das VPN sowohl TCP 443 als auch die in den Netzwerkanforderungen aufgeführten UDP-Ports zulässt.
3. Wenn nur Anrufe über VPN fehlschlagen, blockiert das VPN wahrscheinlich UDP. Siehe the section called “UDP blockiert (Anrufe schlagen fehl, Messaging funktioniert)”.

UDP blockiert (Anrufe schlagen fehl, Messaging funktioniert)

Wickr verwendet standardmäßig UDP für Sprach- und Videoanrufe und greift auf TCP zurück. Wenn Ihr Netzwerk UDP blockiert, können Anrufe nicht sofort eine Verbindung herstellen und es wird auf TCP zurückgegriffen, was möglicherweise zu Leistungseinbußen führen kann, während das Messaging weiterhin normal funktioniert. Sie können TCP-Anrufe innerhalb der Wickr Network Security Group aktivieren (erzwingen), um UDP vollständig zu überspringen und alle Aufrufe an TCP zu erzwingen.

Diagnose

Bitten Sie den betroffenen Benutzer, TCP-Anrufe testweise zu aktivieren (oder administrativ enable/force TCP über die Konsole für alle Benutzer): Einstellungen, Anrufen, TCP-Anrufe aktivieren. Wenn Anrufe bei aktiviertem TCP erfolgreich sind, wird UDP blockiert.

Auflösung

Setzen Sie die UDP-Ports, die in den Netzwerkanforderungen in Ihrer Firewall- und VPN-Konfiguration aufgeführt sind, auf die Zulassungsliste.

TCP-Anrufe sind ein Diagnosetool, keine dauerhafte Lösung. Die Anrufqualität wird bei Verwendung von TCP reduziert.

Fehler bei der DNS-Auflösung

Wenn Ihre DNS-Server Wickr-Domänen nicht auflösen können, kann der Client keine Verbindung herstellen.

Diagnose

Überprüfen Sie auf einem Gerät im betroffenen Netzwerk die DNS-Auflösung für eine erforderliche Wickr-Domain:

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

Wenn sich die Domain nicht lösen lässt, liegt das Problem an der DNS-Konfiguration.

Auflösung

1. Stellen Sie sicher, dass Ihre DNS-Server die in den Netzwerkanforderungen aufgeführten Domänen auflösen können.
2. Wenn Sie DNS-Filterung oder eine DNS-Firewall verwenden, fügen Sie Ausnahmen für Wickr-Domänen hinzu.
3. Testen Sie mit einem alternativen DNS-Server (z. B.`8.8.8.8`), um zu überprüfen, ob das Problem Ihr internes DNS ist.

Ermitteln Sie den Umfang des Problems

Verwenden Sie die folgenden Fragen, um die Ursache einzugrenzen:

- Funktioniert Wickr mit Mobilfunkdaten oder zu Hause WiFi? Falls ja, liegt das Problem an Ihrer Unternehmensnetzwerkkonfiguration.
- Sind alle Benutzer betroffen oder nur bestimmte Benutzer? Wenn alle Benutzer an einem Standort betroffen sind, ist das Problem netzwerkweit. Wenn es sich nur um bestimmte Benutzer handelt, überprüfen Sie deren Geräte- oder VPN-Konfiguration.

- Hat das nach einer Netzwerkänderung angefangen? Aktualisierungen von Firewallregeln, Proxyänderungen oder Änderungen der VPN-Konfiguration unterbrechen häufig die Wickr-Konnektivität.
- Funktioniert Messaging, aber Anrufe schlagen fehl? Dies weist darauf hin, dass UDP blockiert ist. Siehe the section called “UDP blockiert (Anrufe schlagen fehl, Messaging funktioniert)”.
- Sehen Benutzer Zertifikatsfehler? Dies deutet darauf hin, dass die SSL-Inspektion den Wickr-Verkehr abfängt. Siehe the section called “SSL/TLS Inspektion, Verbindungsunterbrechung”.

Weitere Ressourcen

- Netzwerkanforderungen für AWS Wickr (erforderliche Domänen und Ports)
- End-user Netzwerk-Fehlerbehebung (mit betroffenen Benutzern teilen)

Dokumentverlauf

In der folgenden Tabelle werden die Dokumentationsversionen für Wickr beschrieben.

Änderung	Beschreibung	Datum
Die Dateivorschau ist jetzt verfügbar	Wickr-Administratoren haben jetzt die Möglichkeit, Dateidownloads zu aktivieren oder zu deaktivieren. Weitere Informationen finden Sie unter Dateivorschau für AWS Wickr.	29. Mai 2025
Die neu gestaltete Wickr-Administratorkonsole ist jetzt verfügbar	Wickr hat die Wickr-Adm inistratorkonsole für eine bessere Navigation und verbesserte Zugänglichkeit für Administratoren erweitert.	13. März 2025
Wickr ist jetzt im asiatisch-pazifischen Raum (Malaysia) erhältlich AWS-Region	Wickr ist jetzt im asiatisch-pazifischen Raum (Malaysia) AWS-Region erhältlich. Weitere Informationen finden Sie unter Regionale Verfügbar keit.	20. November 2024
Netzwerk löschen ist jetzt verfügbar	Wickr-Administratoren haben jetzt die Möglichkeit, ein AWS Wickr-Netzwerk zu löschen. Weitere Informationen finden Sie unter Netzwerk löschen in AWS Wickr.	4. Oktober 2024
Die Konfiguration von AWS Wickr mit Microsoft Entra (Azure AD) SSO ist jetzt verfügbar	AWS Wickr kann so konfiguri ert werden, dass Microsoft Entra (Azure AD) als Identität sanbieter verwendet wird.	18. September 2024

	Weitere Informationen finden Sie unter Konfigurieren von AWS Wickr mit Microsoft Entra (Azure AD) Single Sign-On.	
Wickr ist jetzt in Europa (Zürich) verfügbar AWS-Region	Wickr ist jetzt in Europa (Zürich) erhältlich. AWS-Region Weitere Informationen finden Sie unter Regionale Verfügbarkeit.	12. August 2024
Grenzüberschreitende Klassifikation und Föderation sind jetzt verfügbar	Die Funktion zur grenzüberschreitenden Klassifizierung ermöglicht GovCloud Benutzern Änderungen der Benutzeroberfläche an Konversationen. Weitere Informationen finden Sie unter GovCloud Grenzüberschreitende Klassifizierung und Föderation.	25. Juni 2024
Die Funktion „Lesebestätigung“ ist jetzt verfügbar	Wickr-Administratoren können jetzt die Lesebestätigungsfunktion in der Administratorkonsole aktivieren oder deaktivieren. Weitere Informationen finden Sie unter Lesebestätigungen.	23. April 2024

Global Federation unterstützt jetzt den eingeschränkten Verbund und Administratoren können Nutzungsanalysen in der Administratorkonsole einsehen	Global Federation unterstützt jetzt den eingeschränkten Verbund. Dies funktioniert für Wickr-Netzwerke in anderen AWS-Regionen. Weitere Informationen finden Sie unter Sicherheitsgruppen. Darüber hinaus können Administratoren ihre Nutzungsanalysen jetzt im Analytics-Dashboard in der Admin Console einsehen. Weitere Informationen finden Sie unter Analytics-Dashboard.	28. März 2024
Eine dreimonatige kostenlose Testversion des Premium-Plans von AWS Wickr ist jetzt verfügbar	Wickr-Administratoren können jetzt einen dreimonatigen Premium-Testplan für bis zu 30 Benutzer wählen. Während der kostenlosen Testversion sind alle Funktionen des Standard- und Premium-Plans verfügbar, einschließlich unbegrenzter Administratorkontrollen und Datenspeicherung. Die Funktion für Gastbenutzer ist während der kostenlosen Premium-Testversion nicht verfügbar. Weitere Informationen finden Sie unter Abo verwalten.	9. Februar 2024

Die Gastbenutzerfunktion ist allgemein verfügbar und es wurden weitere Administratorsteuerelemente hinzugefügt	Wickr-Administratoren können jetzt auf eine Reihe neuer Funktionen zugreifen, darunter die Liste von Gastbenutzern, die Möglichkeit, Benutzer massenweise zu löschen oder zu sperren, und die Option, Gastbenutzer daran zu hindern, in Ihrem Wickr-Netzwerk zu kommunizieren. Weitere Informationen finden Sie unter Gastbenutzer.	8. November 2023
Wickr ist jetzt in Europa (Frankfurt) erhältlich AWS-Region	Wickr ist jetzt in Europa (Frankfurt) erhältlich. AWS-Region Weitere Informationen finden Sie unter Regionale Verfügbarkeit.	26. Oktober 2023
Wickr-Netzwerke sind jetzt in der Lage, sich untereinander zu verbünden AWS-Regionen	Wickr-Netzwerke sind jetzt in der Lage, sich untereinander zu verbünden. AWS-Regionen Weitere Informationen finden Sie unter Sicherheitsgruppen.	29. September 2023
Wickr ist jetzt in Europa (London) erhältlich AWS-Region	Wickr ist jetzt in Europa (London) erhältlich. AWS-Region Weitere Informationen finden Sie unter Regionale Verfügbarkeit.	23. August 2023
Wickr ist jetzt in Kanada (Zentral) erhältlich AWS-Region	Wickr ist jetzt in Kanada (Central) AWS-Region erhältlich. Weitere Informationen finden Sie unter Regionale Verfügbarkeit.	03. Juli 2023

Die Gastbenutzerfunktion ist jetzt als Vorschau verfügbar	Gastbenutzer können sich beim Wickr-Client anmelden und mit Wickr-Netzwerkbenutzern zusammenarbeiten. Weitere Informationen finden Sie unter Gastbenutzer (Vorschau).	31. Mai 2023
AWS Wickr ist jetzt in AWS GovCloud (US-West) integriert und jetzt verfügbar als AWS CloudTrail WickrGov	AWS Wickr ist jetzt in integriert AWS CloudTrail. Weitere Informationen finden Sie unter Protokollieren von AWS Wickr-API-Aufrufen mithilfe von AWS CloudTrail. Darüber hinaus ist Wickr jetzt in AWS GovCloud (US-West) als verfügbar. WickrGov Weitere Informationen finden Sie unter AWS WickrGov im AWS GovCloud (US) -Benutzerhandbuch.	30. März 2023
Tagging und Erstellung mehrerer Netzwerke	Tagging wird jetzt in AWS Wickr unterstützt. Weitere Informationen finden Sie unter Netzwerk-Tags. In Wickr können jetzt mehrere Netzwerke erstellt werden. Weitere Informationen finden Sie unter Netzwerk erstellen.	7. März 2023
Erstversion	Erste Version des Wickr Administration Guide	28. November 2022

Versionshinweise

Um Ihnen zu helfen, den Überblick über die laufenden Updates und Verbesserungen von Wickr zu behalten, veröffentlichen wir Versionshinweise, in denen die letzten Änderungen beschrieben werden.

Juni 2026

- Sitzungs-Timeout — Administratoren können jetzt ein Inaktivitäts-Timeout konfigurieren, das den Wickr-Client nach einem bestimmten Zeitraum automatisch sperrt. Benutzer werden aufgefordert, sich erneut zu authentifizieren, um ihre Sitzung fortzusetzen.
- Zustimmungsbanner — Administratoren können jetzt ein Zustimmungsbanner konfigurieren, das Benutzern bei der Anmeldung angezeigt wird. Benutzer müssen das Banner bestätigen, bevor sie auf die Anwendung zugreifen können.

März 2026

- Die Barrierefreiheit wurde in der gesamten Verwaltungskonsole verbessert, einschließlich Aktualisierungen der ATAK-Hilfebereiche, der SSO-Konfiguration und der Abläufe zur Netzwerkerstellung.

Dezember 2025

- Die Aktionen zum Sperren und Entsperren von Geräten wurden aus der Admin-Konsole entfernt. Administratoren können Benutzergeräte weiterhin zurücksetzen.

November 2025

- Verbesserte Benutzeroberfläche und UX für Netzwerk- und Sicherheitsgruppentabellen sowie Konsolenmetriken für das Laden von Seiten und die Überwachung von API-Aufrufen.

August 2025

- E-Mail-Vorlagen für AWS Wickr und AWS WickrGov wurden aktualisiert, um das Onboarding-Erlebnis für Benutzer zu verbessern. Die E-Mail-Adresse des Absenders wurde von `donotreply@wickr.email` zu geändert. `no-reply@amazonaws.com`

Mai 2025

- Die Dateivorschau ist jetzt verfügbar. Wenn Dateidownloads vom Administrator in der Admin-Konsole für eine Sicherheitsgruppe deaktiviert werden, können Benutzer nur eine Liste der unterstützten Dateien auf den Tabs Nachrichten und Dateien einsehen.

März 2025

- Die neu gestaltete Wickr-Administratorkonsole ist jetzt verfügbar.

Oktober 2024

- Wickr unterstützt jetzt das Löschen von Netzwerken. Weitere Informationen finden Sie unter Netzwerk löschen in AWS Wickr.

September 2024

- Administratoren können AWS Wickr jetzt mit Microsoft Entra (Azure AD) Single Sign-On konfigurieren. Weitere Informationen finden Sie unter Konfigurieren von AWS Wickr mit Microsoft Entra (Azure AD) Single Sign-On.

August 2024

- Verbesserungen
  - Wickr ist jetzt in Europa (Zürich) AWS-Region erhältlich.

Juni 2024

- Die grenzüberschreitende Klassifizierung und Föderation ist jetzt für GovCloud Benutzer verfügbar. Weitere Informationen finden Sie unter GovCloud Grenzüberschreitende Klassifizierung und Föderation.

April 2024

- Wickr unterstützt jetzt Lesebestätigungen. Weitere Informationen finden Sie unter Quittungen lesen.

März 2024

- Global Federation unterstützt jetzt den eingeschränkten Verbund, bei dem der globale Verbund nur für ausgewählte Netzwerke aktiviert werden kann, die im Rahmen eines eingeschränkten Verbunds hinzugefügt wurden. Dies funktioniert für Wickr-Netzwerke in anderenAWS-Regionen. Weitere Informationen finden Sie unter Sicherheitsgruppen.
- Administratoren können ihre Nutzungsanalysen jetzt im Analytics-Dashboard in der Admin Console einsehen. Weitere Informationen finden Sie unter Analytics-Dashboard.

Februar 2024

- AWS Wickr bietet jetzt eine dreimonatige kostenlose Testversion seines Premium-Plans für bis zu 30 Benutzer an. Zu den Änderungen und Einschränkungen gehören:
  - Alle Funktionen des Standard- und Premium-Tarifs wie unbegrenzte Administratorrechte und Datenspeicherung sind jetzt in der kostenlosen Premium-Testversion verfügbar. Die Funktion für Gastbenutzer ist während der kostenlosen Premium-Testversion nicht verfügbar.
  - Die vorherige kostenlose Testversion ist nicht mehr verfügbar. Sie können Ihre bestehende kostenlose Testversion oder Ihren Standardplan auf eine kostenlose Premium-Testversion aktualisieren, falls Sie die kostenlose Premium-Testversion noch nicht genutzt haben. Weitere Informationen finden Sie unter Abo verwalten.

November 2023

- Die Funktion für Gastbenutzer ist jetzt allgemein verfügbar. Zu den Änderungen und Ergänzungen gehören:
  - Möglichkeit, Missbrauch durch andere Wickr-Benutzer zu melden.
  - Administratoren können eine Liste der Gastbenutzer, mit denen ein Netzwerk interagiert hat, sowie die monatliche Nutzungszahl einsehen.
  - Administratoren können Gastbenutzer daran hindern, mit ihrem Netzwerk zu kommunizieren.
  - Add-on Preise für Gastbenutzer.

- Verbesserungen der Admin-Steuerung
  - Möglichkeit, mehrere delete/suspend Benutzer gleichzeitig zu verwenden.
  - Zusätzliche SSO-Einstellung zur Konfiguration einer Übergangszeit für die Token-Aktualisierung.

Oktober 2023

- Verbesserungen
  - Wickr ist jetzt in Europa (Frankfurt) AWS-Region erhältlich.

September 2023

- Verbesserungen
  - Wickr-Netzwerke sind jetzt in der Lage, sich untereinander zu verbünden. AWS-Regionen Weitere Informationen finden Sie unter Sicherheitsgruppen.

August 2023

- Verbesserungen
  - Wickr ist jetzt in Europa (London) AWS-Region erhältlich.

Juli 2023

- Verbesserungen
  - Wickr ist jetzt in Kanada (Central) AWS-Region erhältlich.

Mai 2023

- Verbesserungen
  - Unterstützung für Gastbenutzer hinzugefügt. Weitere Informationen finden Sie unter Gastbenutzer im AWS Wickr-Netzwerk.

März 2023

- Wickr ist jetzt in integriertAWS CloudTrail. Weitere Informationen finden Sie unter Protokollieren von AWS Wickr API-Aufrufen mit AWS CloudTrail.
- Wickr ist jetzt in AWS GovCloud (US-West) als verfügbar. WickrGov Weitere Informationen finden Sie unter AWSWickrGov im AWS GovCloud (US)-Benutzerhandbuch.
- Wickr unterstützt jetzt Tagging. Weitere Informationen finden Sie unter Netzwerk-Tags für AWS Wickr. In Wickr können jetzt mehrere Netzwerke erstellt werden. Weitere Informationen finden Sie unter Schritt 1: Erstellen Sie ein Netzwerk.

Februar 2023

- Wickr unterstützt jetzt das Android Tactical Assault Kit (ATAK). Weitere Informationen finden Sie unter Aktivieren Sie ATAK im Wickr Network Dashboard.

Januar 2023

- Single Sign-On (SSO) kann jetzt für alle Tarife konfiguriert werden, einschließlich Free Trial und Standard.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.