



Administratorhandbuch

# AWS Wickr



# AWS Wickr: Administratorhandbuch

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

---

# Table of Contents

Was ist AWS Wickr? .....	1
Funktionen von Wickr .....	1
Auf Wickr zugreifen .....	3
Preisgestaltung .....	3
Wickr-Dokumentation für Endbenutzer .....	3
Einrichtung .....	4
Melden Sie sich an für AWS .....	4
Erstellen eines IAM-Benutzers .....	4
Was kommt als Nächstes .....	6
Erste Schritte .....	7
Voraussetzungen .....	7
Schritt 1: Erstellen Sie ein Netzwerk .....	7
Schritt 2: Konfigurieren Sie Ihr Netzwerk .....	9
Schritt 3: Benutzer erstellen und einladen .....	11
Nächste Schritte .....	14
Wickr Pro auf AWS Wickr übertragen .....	15
Schritt 1: Erstellen Sie ein AWS Konto .....	15
Schritt 2: Rufen Sie Ihre Wickr-Netzwerk-ID ab .....	16
Schritt 3: Senden Sie eine Anfrage .....	16
Schritt 4: Loggen Sie sich in Ihre Konsole ein AWS .....	16
Netzwerk verwalten .....	18
Netzwerkprofil .....	18
Netzwerkprofil anzeigen .....	18
Netzwerknamen bearbeiten .....	19
Sicherheitsgruppen .....	20
Sicherheitsgruppen anzeigen .....	20
Eine Sicherheitsgruppe erstellen .....	21
Bearbeiten Sie eine Sicherheitsgruppe .....	22
Löschen einer Sicherheitsgruppe .....	23
SSO-Konfiguration .....	24
SSO-Details anzeigen .....	24
SSO konfigurieren .....	25
Übergangsfrist für die Token-Aktualisierung .....	26
Quittungen lesen .....	26

Netzwerk-Tags .....	27
Netzwerk-Tags verwalten .....	27
Fügen Sie ein Netzwerk-Tag hinzu .....	29
Bearbeiten Sie ein Netzwerk-Tag .....	30
Entfernen Sie ein Netzwerk-Tag .....	30
Netzwerkplan verwalten .....	31
Einschränkungen der kostenlosen Premium-Testversion .....	32
Datenaufbewahrung .....	32
Einzelheiten zur Datenspeicherung anzeigen .....	33
Konfigurieren der Datenaufbewahrung .....	34
Holen Sie sich die Protokolle .....	46
Kennzahlen und Ereignisse zur Datenspeicherung .....	46
Was ist ATAК? .....	52
Aktivieren von ATAК .....	53
Zusätzliche Informationen zu ATAК .....	55
Installieren und koppeln .....	55
Wählen und Empfangen eines Anrufs .....	59
Senden einer Datei .....	60
Senden einer sicheren Sprachnachricht (Push-to-talk) .....	61
Pinwheel .....	62
Navigation .....	65
Liste der Ports und Domänen, die zugelassen werden sollen .....	65
GovCloud .....	66
Benutzer verwalten .....	68
Team-Verzeichnis .....	68
Anzeigen von Benutzern .....	68
Benutzer erstellen .....	69
Benutzer bearbeiten .....	70
Löschen von Benutzern .....	71
Benutzer auf einmal löschen .....	71
Benutzer massenweise sperren .....	73
Gastnutzer .....	74
Aktivieren oder deaktivieren Sie Gastbenutzer .....	75
Anzahl der Gastbenutzer anzeigen .....	76
Monatliche Nutzung anzeigen .....	77
Gastbenutzer anzeigen .....	77

Blockieren Sie einen Gastbenutzer .....	78
Sicherheit .....	80
Datenschutz .....	81
Identity and Access Management .....	82
Zielgruppe .....	82
Authentifizierung mit Identitäten .....	83
Verwalten des Zugriffs mit Richtlinien .....	87
Von AWS Wickr verwaltete Richtlinien .....	89
So funktioniert AWS Wickr mit IAM .....	91
Beispiele für identitätsbasierte Richtlinien .....	99
Fehlerbehebung .....	102
Compliance-Validierung .....	103
Ausfallsicherheit .....	103
Sicherheit der Infrastruktur .....	104
Konfigurations- und Schwachstellenanalyse .....	104
Bewährte Methoden für die Gewährleistung der Sicherheit .....	104
Überwachen .....	106
CloudTrail Protokolle .....	106
Wickr-Informationen in CloudTrail .....	106
Grundlegendes zu Wickr-Protokolldateieinträgen .....	107
.....	114
Dokumentverlauf .....	117
Versionshinweise .....	121
März 2024 .....	121
Februar 2024 .....	121
November 2023 .....	121
Oktober 2023 .....	122
September 2023 .....	122
August 2023 .....	122
Juli 2023 .....	122
Mai 2023 .....	122
März 2023 .....	123
Februar 2023 .....	123
Januar 2023 .....	123
.....	cxxiv

# 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 Management Console Wickr-Bots sicher automatisieren. Um zu beginnen, sehen Sie sich [Einrichtung für AWS Wickr](#) an.

## Themen

- [Funktionen von Wickr](#)
- [Auf Wickr zugreifen](#)
- [Preisgestaltung](#)
- [Wickr-Dokumentation für Endbenutzer](#)

## 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 Management Console 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 Dateien bis zu 5 GB mit unbegrenztem Speicherplatz
- Kurzlebig: Kontrollieren Sie den Ablauf und die Timer burn-on-read
- Globaler Verband: Connect zu Wickr-Benutzern außerhalb Ihres Netzwerks her

**Note**

Wickr-Netzwerke in AWS GovCloud (US-West) können nur mit anderen Wickr-Netzwerken in (US-West) verbunden werden. AWS GovCloud

## Auf Wickr zugreifen

Wickr ist in den USA Ost (Nord-Virginia), Kanada (Zentral), Europa (London), Asien-Pazifik (Sydney), Europa (Frankfurt), Europa (Stockholm), Asien-Pazifik (Singapur) und Asien-Pazifik (Tokio) verfügbar. AWS-Regionen Wickr ist auch WickrGov in den AWS GovCloud (USA West) erhältlich. AWS-Region

[Administratoren greifen auf das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/ zu](https://console.aws.amazon.com/wickr/). Bevor Sie mit der Verwendung von Wickr beginnen, sollten Sie die Anleitungen [Einrichtung für AWS Wickr](#) und [Erste Schritte mit AWS Wickr](#).

**Note**

Der Wickr-Dienst verfügt nicht über eine Anwendungsprogrammierschnittstelle (API).

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

Wenn Sie ein neuer AWS Kunde sind, müssen Sie die auf dieser Seite aufgeführten Einrichtungsvoraussetzungen erfüllen, bevor Sie AWS Wickr verwenden. Für diese Einrichtungsverfahren verwenden Sie den AWS Identity and Access Management (IAM) -Service. Umfassende Informationen zu IAM finden Sie im [IAM-Benutzerhandbuch](#).

## Themen

- [Melden Sie sich an für AWS](#)
- [Erstellen eines IAM-Benutzers](#)
- [Was kommt als Nächstes](#)

## Melden Sie sich an für AWS

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie <https://portal.aws.amazon.com/billing/signup>.
2. Folgen Sie den Online-Anweisungen.

Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontos wird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um [Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich](#) ist.

## Erstellen eines IAM-Benutzers

Wählen Sie zum Erstellen eines Administratorbenutzers eine der folgenden Optionen aus.

Wählen Sie eine Möglichkeit zur Verwaltung Ihres Administrators aus.	Bis	Von	Sie können auch
<p>Im IAM Identity Center (Empfohlen)</p>	<p>Verwendung von kurzfristigen Anmeldeinformationen für den Zugriff auf AWS.</p> <p>Dies steht im Einklang mit den bewährten Methoden für die Sicherheit. Weitere Informationen zu bewährten Methoden finden Sie unter <a href="#">Bewährte Methoden für die Sicherheit in IAM</a> im IAM-Benutzerhandbuch.</p>	<p>Beachtung der Anweisungen unter <a href="#">Erste Schritte</a> im AWS IAM Identity Center - Benutzerhandbuch.</p>	<p>Konfigurieren Sie den programmatischen Zugriff, indem Sie <a href="#">den AWS IAM Identity Center im AWS Command Line Interface Benutzerhandbuch AWS CLI zu verwendenden konfigurieren</a>.</p>
<p>In IAM (Nicht empfohlen)</p>	<p>Verwendung von langfristigen Anmeldeinformationen für den Zugriff auf AWS.</p>	<p>Beachtung der Anweisungen unter <a href="#">Erstellen Ihres ersten IAM-Administratorbenutzers und Ihrer ersten Benutzergruppe</a> im IAM-Benutzerhandbuch.</p>	<p>Programmgesteuerten Zugriff unter Verwendung der Informationen unter <a href="#">Verwalten der Zugriffsschlüssel für IAM-Benutzer</a> im IAM-Benutzerhandbuch konfigurieren.</p>

 Note

Sie können die `AWSWickrFullAccess` verwaltete Richtlinie auch zuweisen, um dem Wickr-Dienst vollständige Administratorrechte zu gewähren. Weitere Informationen finden Sie unter [AWS verwaltete Richtlinie: AWSWickrFullAccess](#).

## Was kommt als Nächstes

Sie haben die erforderlichen Schritte zur Einrichtung abgeschlossen. Informationen zum Konfigurieren von Wickr finden Sie unter [Erste 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.

## Themen

- [Voraussetzungen](#)
- [Schritt 1: Erstellen Sie ein Netzwerk](#)
- [Schritt 2: Konfigurieren Sie Ihr Netzwerk](#)
- [Schritt 3: Benutzer erstellen und einladen](#)
- [Nächste Schritte](#)
- [Wickr Pro auf AWS Wickr übertragen](#)

## 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 [AWS verwaltete Richtlinie: AWSWickrFullAccess](#).
- Stellen Sie sicher, dass Sie die entsprechenden Ports und Domänen für Wickr zulassen. Weitere Informationen finden Sie unter [Liste der Ports und Domänen, die zugelassen werden sollen](#).

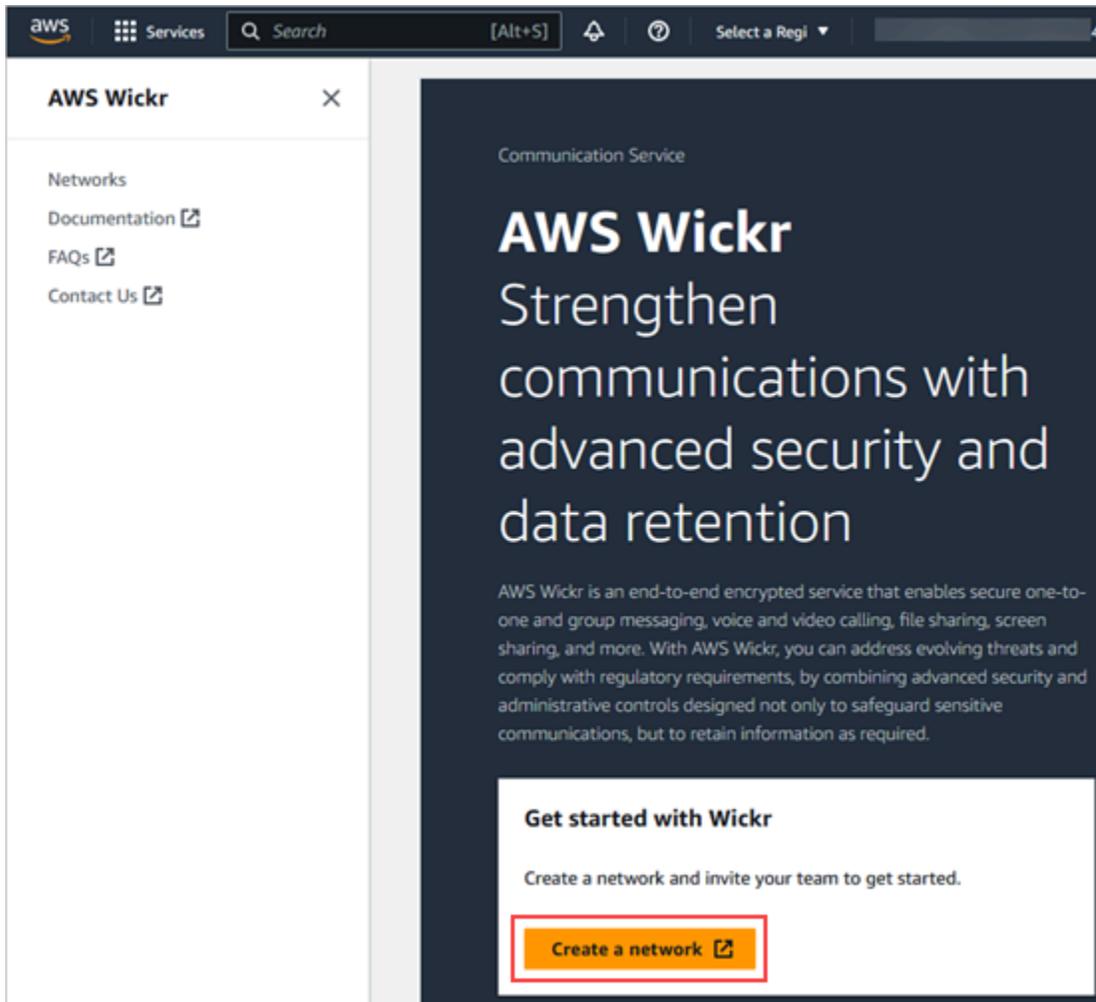
## Schritt 1: Erstellen Sie ein Netzwerk

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

1. [Öffnen Sie das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/](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 können die kostenlose Premium-Testoption wählen, die für bis zu 30 Benutzer verfügbar ist und drei Monate gültig ist. Dieses Angebot gilt für neue, legacy-freie Testversionen und Standardpläne. Administratoren können während der kostenlosen Premium-Testphase 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](#).

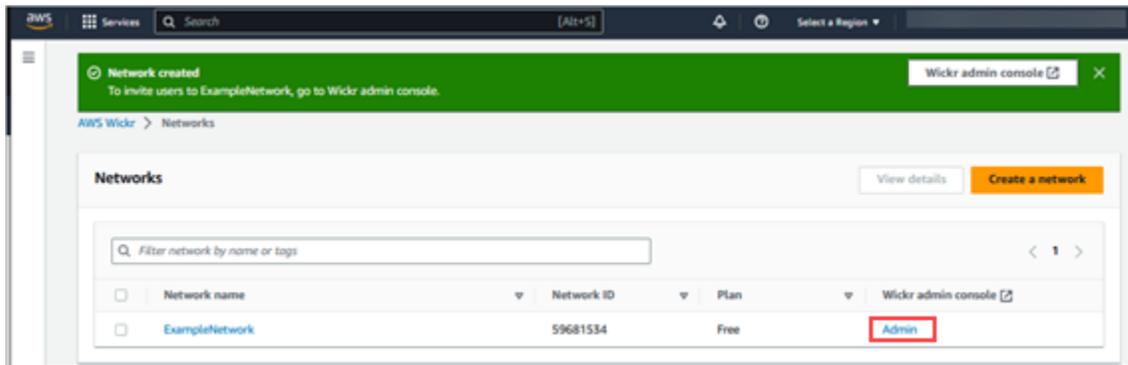
5. (Optional) Wählen Sie Neues Tag hinzufügen, um Ihrem Netzwerk ein Tag hinzuzufügen. Tags bestehen aus einem Schlüssel-Wert-Paar. Tags können verwendet werden, um Ressourcen zu suchen und zu filtern oder Ihre AWS Kosten zu verfolgen. Weitere Informationen finden Sie unter [Netzwerk-Tags](#).
6. Wählen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

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

## Schritt 2: Konfigurieren Sie Ihr Netzwerk

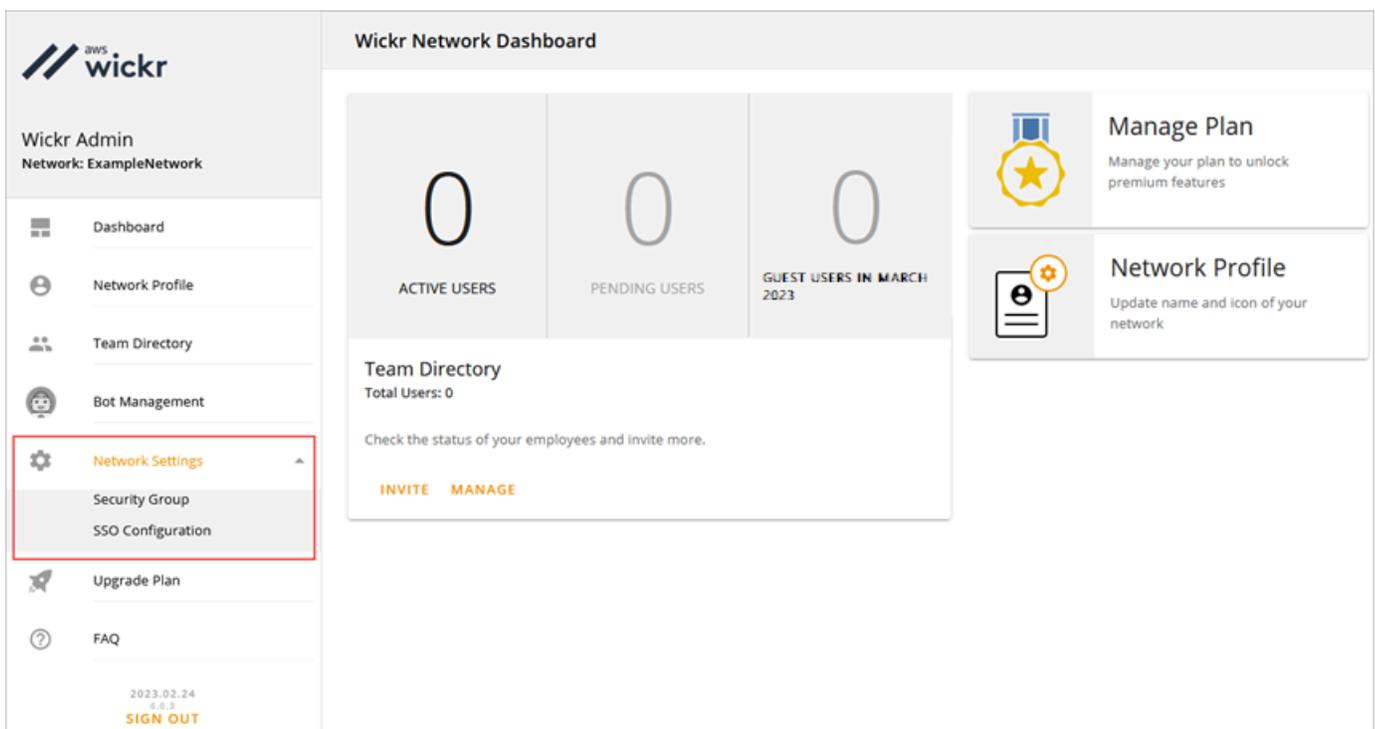
Gehen Sie wie folgt vor, um auf die Wickr Admin Console zuzugreifen, in der Sie Benutzer hinzufügen, Sicherheitsgruppen hinzufügen, SSO konfigurieren, die Datenspeicherung konfigurieren und zusätzliche Netzwerkeinstellungen vornehmen können.

1. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu navigieren.



Sie werden zur Wickr Admin Console für das ausgewählte Netzwerk weitergeleitet.

- Wählen Sie im Navigationsbereich der Wickr Admin Console Netzwerkeinstellungen aus.



Die folgenden Netzwerkeinstellungsoptionen sind verfügbar. Weitere Informationen zur Konfiguration 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](#).
- SSO-Konfiguration — 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 [Konfiguration von Single Sign-On](#).

## 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 [Konfiguration von Single Sign-On](#).
- Einladung — Sie können Benutzer in The AWS Management Console 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. Die Gastbenutzerfunktion befindet sich derzeit in der Vorschauversion. Weitere Informationen finden Sie unter [Gastnutzer](#).

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.

## SSO

Schreiben und senden Sie eine E-Mail an die SSO-Benutzer, die sich für Wickr registrieren sollten. 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 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.](https://aws.amazon.com/wickr/download/)

#### Note

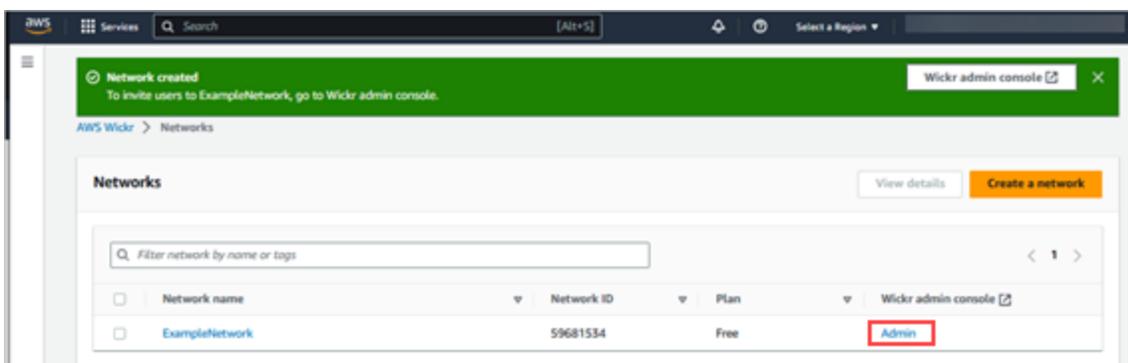
Wenn Sie Ihr Wickr-Netzwerk in AWS GovCloud (US-West) erstellt haben, weisen Sie Ihre Benutzer an, den Client herunterzuladen und zu installieren. WickrGov Weisen Sie Ihre Benutzer für alle anderen AWS Regionen an, den Standard-Wickr-Client herunterzuladen und zu installieren. Weitere Informationen zu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

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

## Non-SSO

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

1. [Öffnen Sie das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/.](https://console.aws.amazon.com/wickr/)
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu navigieren.



Die Seite „Netzwerke“.

Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet. In der Wickr Admin Console können Sie Benutzer hinzufügen, Sicherheitsgruppen hinzufügen, SSO konfigurieren, die Datenspeicherung konfigurieren und zusätzliche Einstellungen für das von Ihnen ausgewählte Netzwerk vornehmen.

3. Wählen Sie im Navigationsbereich der Wickr Admin Console Benutzer und dann Teamverzeichnis aus.

Auf der Seite Benutzer können Sie einzelne Benutzer hinzufügen, indem Sie Neuen Benutzer erstellen wählen. Sie können auch mehrere Benutzer gleichzeitig hinzufügen, indem Sie im oberen Navigationsbereich auf das Symbol Benutzer hinzufügen klicken. Wählen Sie das Symbol CSV herunterladen, um eine CSV-Vorlage herunterzuladen, die Sie bearbeiten und zusammen mit Ihrer Benutzerliste hochladen können.

4. 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.
5. Wählen Sie Erstellen.

**New User**

**User Information**

First Name  
Example

Last Name  
User

Country Code  
+1

Phone Number  
201-200-0000

**Account Information**

Email

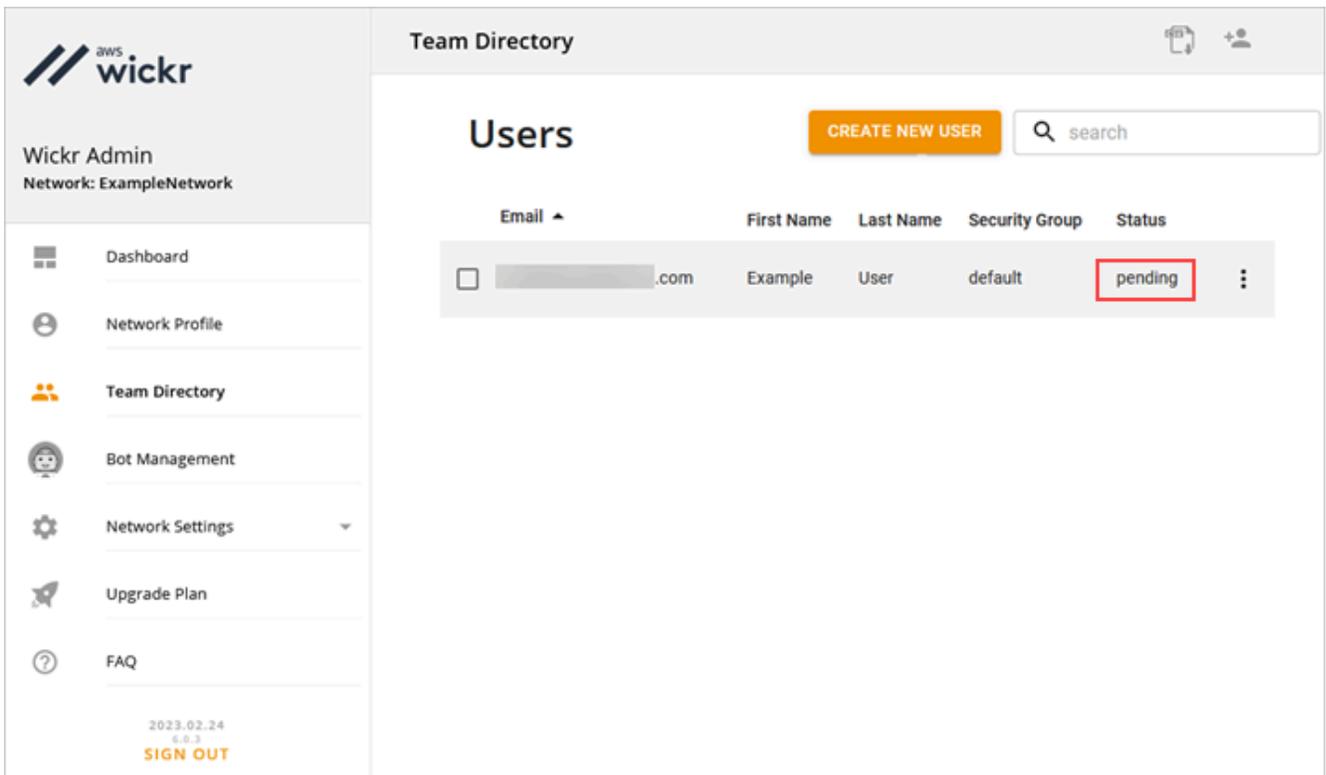
default

CANCEL CREATE

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.



The screenshot shows the AWS Wickr Admin interface. On the left is a navigation sidebar with the Wickr logo and menu items: Dashboard, Network Profile, Team Directory, Bot Management, Network Settings, Upgrade Plan, and FAQ. The main content area is titled 'Team Directory' and 'Users'. It features a 'CREATE NEW USER' button and a search bar. Below is a table with columns: Email, First Name, Last Name, Security Group, and Status. A single user entry is shown with the status 'pending' highlighted in a red box.

Email	First Name	Last Name	Security Group	Status
[redacted].com	Example	User	default	pending

## Nächste Schritte

Sie haben die Schritte „Erste Schritte“ abgeschlossen. Informationen zur Verwaltung von Wickr finden Sie in den folgenden Anleitungen:

- [Verwalten Sie Ihr AWS Wickr-Netzwerk](#)
- [Benutzer in AWS Wickr verwalten](#)

# Wickr Pro auf AWS Wickr übertragen

## Note

Wickr Pro wird am 27. März 2024 eingestellt.

In diesem Handbuch zeigen wir Ihnen, wie Sie von Wickr Pro wechseln und mit der Nutzung von AWS Wickr beginnen.

Folgen Sie den Schritten in diesem Handbuch, wenn Sie bereits ein Wickr Pro-Netzwerk haben, aber noch keines haben. AWS-Konto Bitte wenden Sie sich bei jedem Schritt an den Support, wenn Sie Hilfe benötigen.

Wenn Ihre Organisation bereits über ein AWS Konto verfügt, füllen Sie das Formular „[Migration von Wickr Pro zu AWS Wickr](#)“ aus. Der AWS Wickr-Support hilft Ihnen dann weiter.

Sie benötigen eine AWS-Konto ID, um Ihr AWS Wickr-Netzwerk als AWS-Service zu verwalten. Weitere Informationen darüber, was ein AWS-Konto ist und wie das Konto verwaltet wird, finden Sie im [Referenzhandbuch zur AWS Kontoverwaltung](#).

## Themen

- [Schritt 1: Erstellen Sie ein AWS Konto](#)
- [Schritt 2: Rufen Sie Ihre Wickr-Netzwerk-ID ab](#)
- [Schritt 3: Senden Sie eine Anfrage](#)
- [Schritt 4: Loggen Sie sich in Ihre Konsole ein AWS](#)

## Schritt 1: Erstellen Sie ein AWS Konto

Gehen Sie wie folgt vor, um ein AWS Konto zu erstellen.

1. Wenn Ihre Organisation noch keine AWS-Konto-ID hat, können Sie damit beginnen, eine eigenständige AWS Konto-ID zu erstellen. Ein paar wichtige Dinge, die Sie dafür benötigen:
  - Eine Kredit-/Debitkarte für die Abrechnung
  - Eine E-Mail-Adresse, auf die eine Gruppe zugreifen kann (empfohlen, nicht erforderlich)
  - Wählen Sie einen AWS Support Plan aus. Weitere Informationen finden Sie unter [AWS Support Pläne ändern](#).

**Note**

Sie können Ihren AWS Support Plan jederzeit ändern, wenn Sie mehr über Ihre Bedürfnisse erfahren.

2. Richten Sie als bewährte Sicherheitsmethode den Administratorzugriff über IAM ein (optional, aber empfohlen). Weitere Informationen finden Sie unter [AWS Identity and Access Management](#). Genauere Anweisungen zum administrativen Zugriff auf AWS Wickr finden Sie unter [AWS verwaltete Richtlinie: AWSWickrFullAccess](#).
3. Sobald Sie die vorherigen Schritte abgeschlossen haben, können Sie sich bei der anmelden, um Ihre 12-stellige AWS-Konto ID unter Ihrem Kontonamen AWS Management Console zu finden.

## Schritt 2: Rufen Sie Ihre Wickr-Netzwerk-ID ab

Gehen Sie wie folgt vor, um Ihre Wickr-Netzwerk-ID abzurufen.

1. Melden Sie sich bei Ihrer aktuellen Wickr-Administrationskonsole an und wählen Sie die Netzwerke aus, die Sie migrieren möchten, und wählen Sie dann Netzwerkprofil aus.
2. Auf der Netzwerkprofilseite wird Ihre Netzwerk-ID angezeigt. Dabei handelt es sich um eine 8-stellige numerische ID.

## Schritt 3: Senden Sie eine Anfrage

Nachdem Sie Ihre AWS-Konto ID und Wickr Pro-Netzwerk-ID haben, müssen Sie das Formular „[Von Wickr Pro zu AWS Wickr migrieren](#)“ ausfüllen.

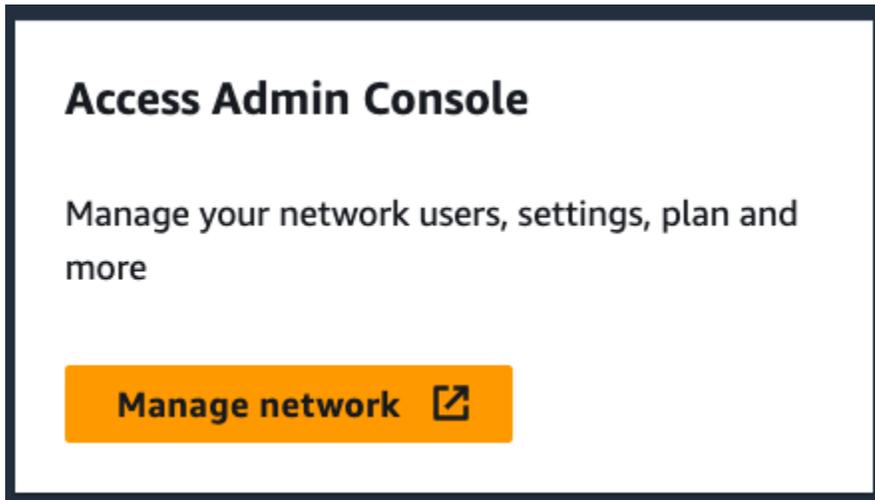
Wenn der Vorgang abgeschlossen ist, normalerweise innerhalb von 14 Tagen, wird sich ein Mitarbeiter des AWS Wickr-Supports mit Ihnen in Verbindung setzen, um zu bestätigen, dass Ihr Wickr-Netzwerk zu Ihrem hinzugefügt wurde. AWS-Konto

## Schritt 4: Loggen Sie sich in Ihre Konsole ein AWS

**Note**

Folgen Sie diesen Schritten, NACHDEM Sie die Bestätigung erhalten haben, dass Ihr Wickr Pro-Netzwerk zu Ihrem AWS-Konto hinzugefügt wurde.

1. Sie können sich bei der AWS Konsole als Root-Benutzer ODER mit einem IAM-Benutzer anmelden, den Sie zuvor (wie empfohlen) in Schritt 2 für AWS Wickr erstellt haben.
2. Navigieren Sie zu Ihrem AWS Wickr-Service. Sie können dies über das Menü Services tun oder indem Sie in der Suchleiste nach AWS Wickr suchen.
3. Wählen Sie auf der Seite AWS Wickr die Option Netzwerk verwalten aus, um auf Ihre Wickr-Netzwerkliste zuzugreifen.



Die Schaltfläche „Netzwerk verwalten“.

4. Wählen Sie auf der Seite Netzwerke in der Spalte Wickr Admin-Konsole den Link Admin rechts neben dem gewünschten Netzwerknamen aus.



Der Link zur Admin-Konsole.

5. Die Übertragung ist jetzt abgeschlossen! Sie werden Ihr Wickr-Netzwerk-Dashboard sehen.

Die Abrechnung für Ihr Netzwerk wird nun auf Ihr AWS-Konto übertragen. Es kann bis zu 3 Werktage dauern, bis sich der Support mit einer Bestätigung bei Ihnen meldet. Nachdem Sie Ihre Bestätigung erhalten haben, können Sie Ihre Rechnung über die AWS Konsole einsehen und bezahlen.

# Verwalten Sie Ihr AWS Wickr-Netzwerk

Im Bereich Netzwerkeinstellungen von AWS Management Console for Wickr können Sie Ihren Wickr-Netzwerknamen, Ihre Sicherheitsgruppen, Ihre SSO-Konfiguration und Ihre Datenaufbewahrungseinstellungen verwalten.

## Themen

- [Netzwerkprofil](#)
- [Sicherheitsgruppen](#)
- [Konfiguration von Single Sign-On](#)
- [Quittungen lesen](#)
- [Netzwerk-Tags](#)
- [Netzwerkplan verwalten](#)
- [Datenaufbewahrung](#)
- [Was ist ATAК?](#)
- [Liste der Ports und Domänen, die zugelassen werden sollen](#)
- [GovCloud Grenzüberschreitende Klassifikation und Föderation](#)

## Netzwerkprofil

Sie können den Namen Ihres Wickr-Netzwerks bearbeiten und Ihre Netzwerk-ID im Bereich Netzwerkprofil von AWS Management Console for Wickr einsehen.

## Themen

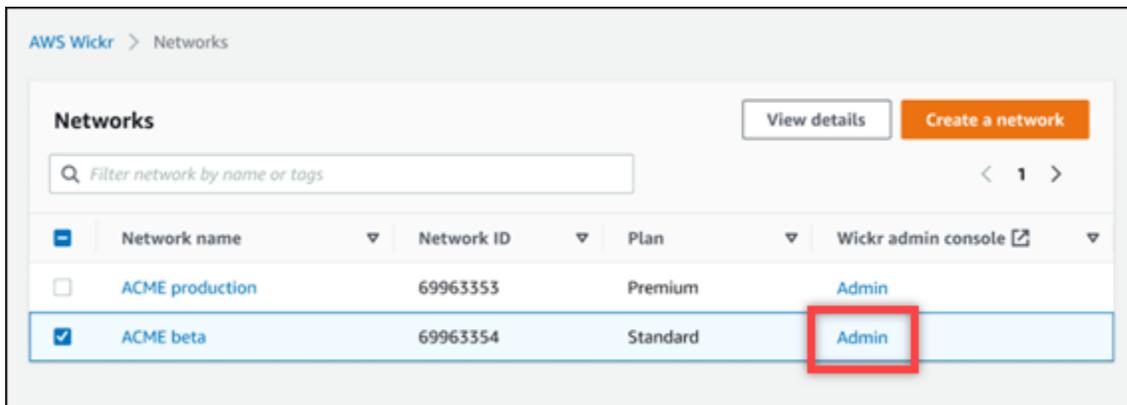
- [Netzwerkprofil anzeigen](#)
- [Netzwerknamen bearbeiten](#)

## Netzwerkprofil anzeigen

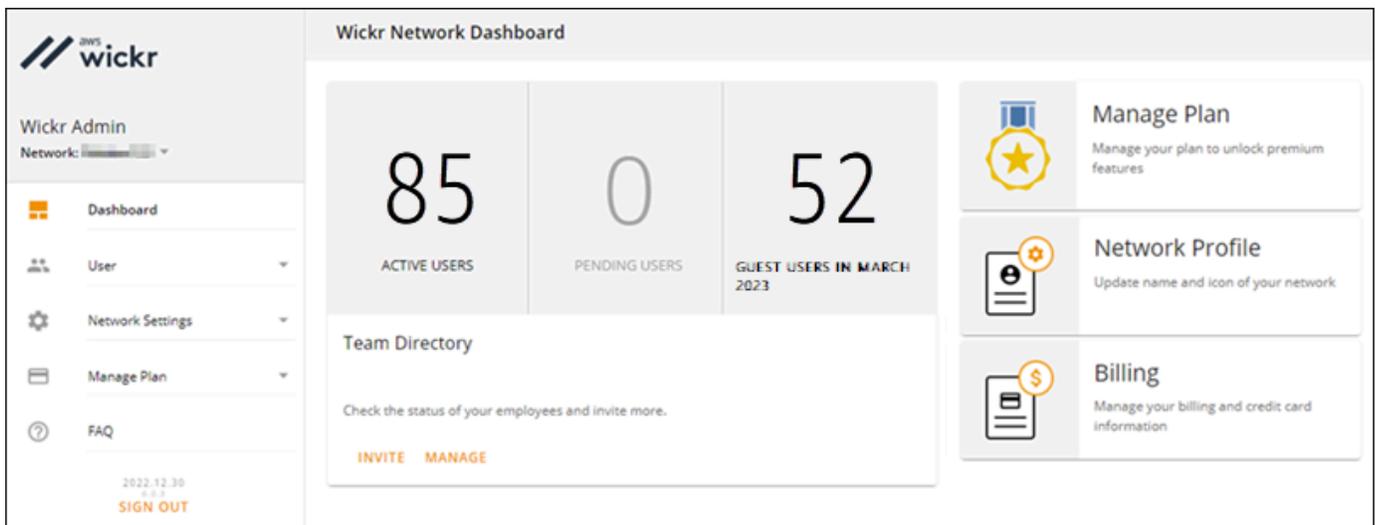
Gehen Sie wie folgt vor, um Ihr Wickr-Netzwerkprofil und Ihre Netzwerk-ID anzuzeigen.

1. [Öffnen Sie das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/.](https://console.aws.amazon.com/wickr/)

- Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu navigieren.



Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.



- Wählen Sie im Navigationsbereich der Wickr Admin Console Netzwerkeinstellungen und dann Netzwerkprofil aus.

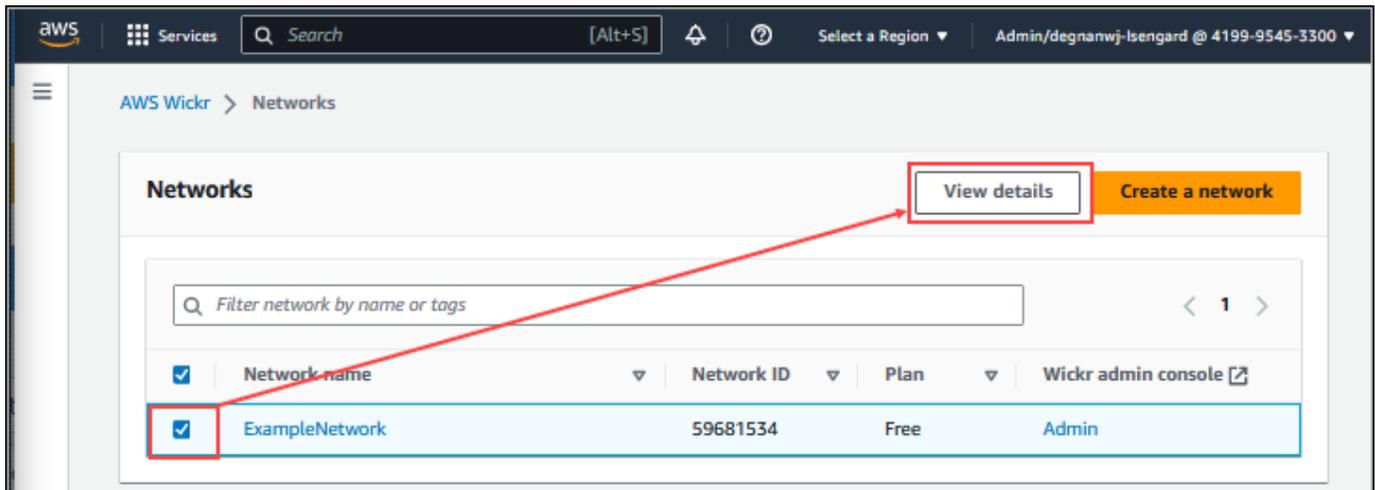
Auf der Netzwerkprofilseite werden Ihr Wickr-Netzwerkname und Ihre Netzwerk-ID angezeigt. Sie können die Netzwerk-ID verwenden, um den Verbund zu konfigurieren.

## Netzwerknamen bearbeiten

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

- [Öffnen Sie den AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/.](https://console.aws.amazon.com/wickr/)

2. Wählen Sie Netzwerk verwalten.
3. Aktivieren Sie auf der Seite Netzwerke das Kontrollkästchen neben dem Netzwerknamen, den Sie bearbeiten möchten, und wählen Sie dann Details anzeigen aus.



4. Wählen Sie im Abschnitt Netzwerkübersicht die Option Bearbeiten aus.
5. Geben Sie Ihren neuen Netzwerknamen in das Textfeld Netzwerkname ein.
6. Wählen Sie Änderungen speichern, um Ihren neuen Netzwerknamen zu speichern.

## Sicherheitsgruppen

Im Bereich Sicherheitsgruppen von AWS Management Console for Wickr können Sie Sicherheitsgruppen und ihre Einstellungen verwalten, z. B. Richtlinien zur Kennwortkomplexität, Nachrichteneinstellungen, Anruhfunktionen, Sicherheitsfunktionen und Netzwerkverbund.

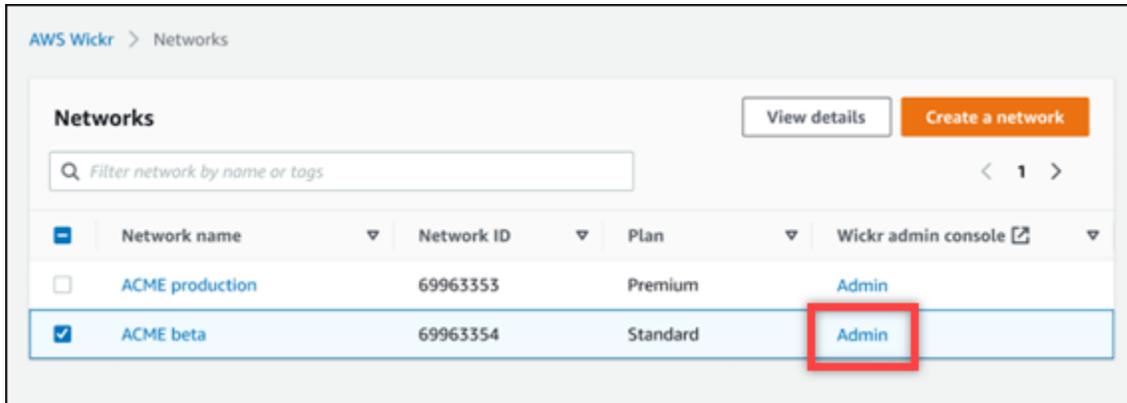
### Themen

- [Sicherheitsgruppen anzeigen](#)
- [Eine Sicherheitsgruppe erstellen](#)
- [Bearbeiten Sie eine Sicherheitsgruppe](#)
- [Löschen einer Sicherheitsgruppe](#)

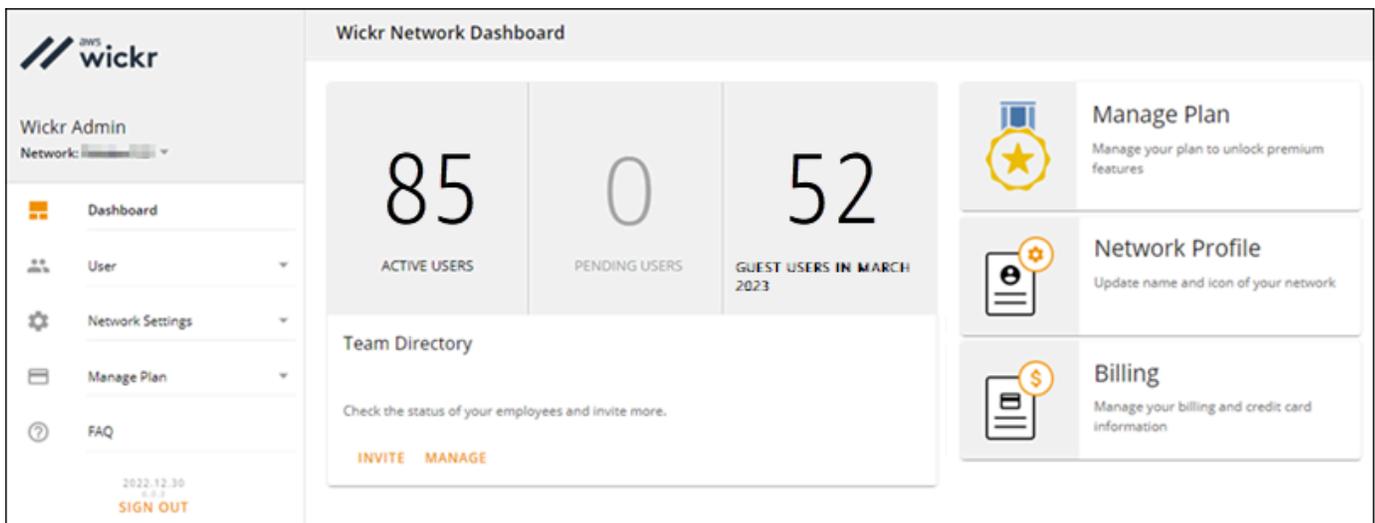
## Sicherheitsgruppen anzeigen

Gehen Sie wie folgt vor, um Sicherheitsgruppen anzuzeigen.

1. Öffnen Sie das AWS Management Console für Wickr unter <https://console.aws.amazon.com/wickr/>.
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu navigieren.



Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.



3. Wählen Sie im Navigationsbereich der Wickr Admin Console Netzwerkeinstellungen und dann Sicherheitsgruppe aus.

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

## Eine Sicherheitsgruppe erstellen

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

1. Öffnen Sie die AWS Management Console für Wickr unter <https://console.aws.amazon.com/wickr/>.
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu navigieren.

Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.

3. Wählen Sie im Navigationsbereich der Wickr Admin Console Netzwerkeinstellungen und dann Sicherheitsgruppe.
4. Wählen Sie Neue Gruppe, um eine neue Sicherheitsgruppe zu erstellen.

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

Weitere Informationen zum Bearbeiten der neuen Sicherheitsgruppe finden Sie unter [Bearbeiten Sie eine Sicherheitsgruppe](#).

## Bearbeiten Sie eine Sicherheitsgruppe

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

1. Öffnen Sie die AWS Management Console für Wickr unter <https://console.aws.amazon.com/wickr/>.
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu navigieren.

Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.

3. Wählen Sie im Navigationsbereich der Wickr Admin Console Netzwerkeinstellungen und dann Sicherheitsgruppe.
4. Wählen Sie Details neben dem Namen der Sicherheitsgruppe, 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:
  - Name der Sicherheitsgruppe — Wählen Sie das Stiftsymbol neben dem Namen der Gruppe, um den Namen zu bearbeiten.
  - Allgemein — Bearbeiten Sie die Grundkonfiguration der Gruppe.

- Messaging — Verwaltet die Nachrichtenfunktionen für Mitglieder der Gruppe.
  - Telefonieren — Verwalten Sie die Anruffunktionen für Mitglieder der Gruppe.
  - Sicherheit — Konfigurieren Sie zusätzliche Sicherheitsfunktionen für die Gruppe.
  - Föderation — Die Fähigkeit, zwischen Netzwerken zu kommunizieren. Dies kann in der Admin-Konsole für ein Netzwerk auf Sicherheitsgruppenebene konfiguriert werden. Bei AWS Wickr gibt es zwei Arten von Verbänden: lokal und global.
    - Lokaler Verbund — Die Möglichkeit, sich mit AWS-Benutzern in anderen Netzwerken innerhalb derselben Region zu verbinden. Wenn es beispielsweise in Kanada zwei Netzwerke gibt, für die der lokale Verbund aktiviert ist, können sie miteinander kommunizieren.
    - Globaler Verbund — Die Möglichkeit, sich entweder mit Enterprise-Benutzern oder AWS Benutzern in einem anderen Netzwerk, die zu anderen Regionen gehören, zu verbünden. Wenn es beispielsweise einen Benutzer in einem Netzwerk in der Region Kanada und einen Benutzer in einem Netzwerk in der Region London gibt und der globale Verbund für beide Netzwerke aktiviert ist, können sie miteinander kommunizieren.
    - Eingeschränkter Verbund — Die Möglichkeit, sich mit bestimmten Netzwerken (Enterprise oder AWS) zu verbinden, die zu verschiedenen Regionen gehören. Administratoren können bestimmte Netzwerke, mit denen sich ihre Benutzer verbinden können, auf eine Zulassungsliste setzen. Nach der Einschränkung können Benutzer nur mit Benutzern in den Netzwerken kommunizieren, die auf der Zulassungsliste stehen. Beide Netzwerke müssen sich in den Sicherheitsgruppeneinstellungen auf der Registerkarte Verbund gegenseitig auf eine Zulassungsliste setzen, um den eingeschränkten Verbund verwenden zu können.
6. Wählen Sie Speichern, um die Änderungen zu speichern, die Sie an den Sicherheitsgruppendetails vornehmen.

## Löschen einer Sicherheitsgruppe

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

1. Öffnen Sie die AWS Management Console für Wickr unter <https://console.aws.amazon.com/wickr/>.
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu navigieren.

Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.

3. Wählen Sie im Navigationsbereich der Wickr Admin Console Netzwerkeinstellungen und dann Sicherheitsgruppe.
4. Wählen Sie das vertikale Ellipsensymbol neben dem Namen der Sicherheitsgruppe, die Sie löschen möchten.
5. Wählen Sie Entfernen, um die Sicherheitsgruppe zu 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 unter [Benutzer bearbeiten](#).

## Konfiguration von Single Sign-On

Im Abschnitt SSO-Konfiguration von AWS Management Console 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.

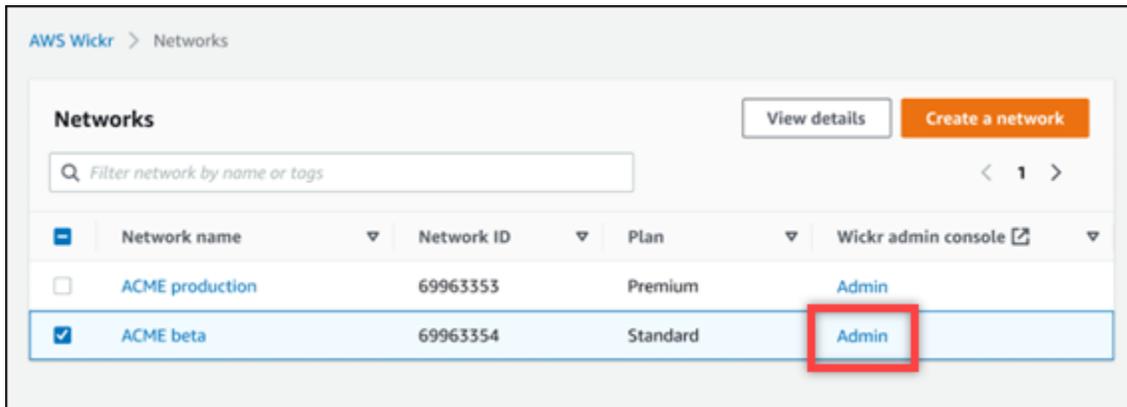
### Themen

- [SSO-Details anzeigen](#)
- [SSO konfigurieren](#)
- [Übergangsfrist für die Token-Aktualisierung](#)

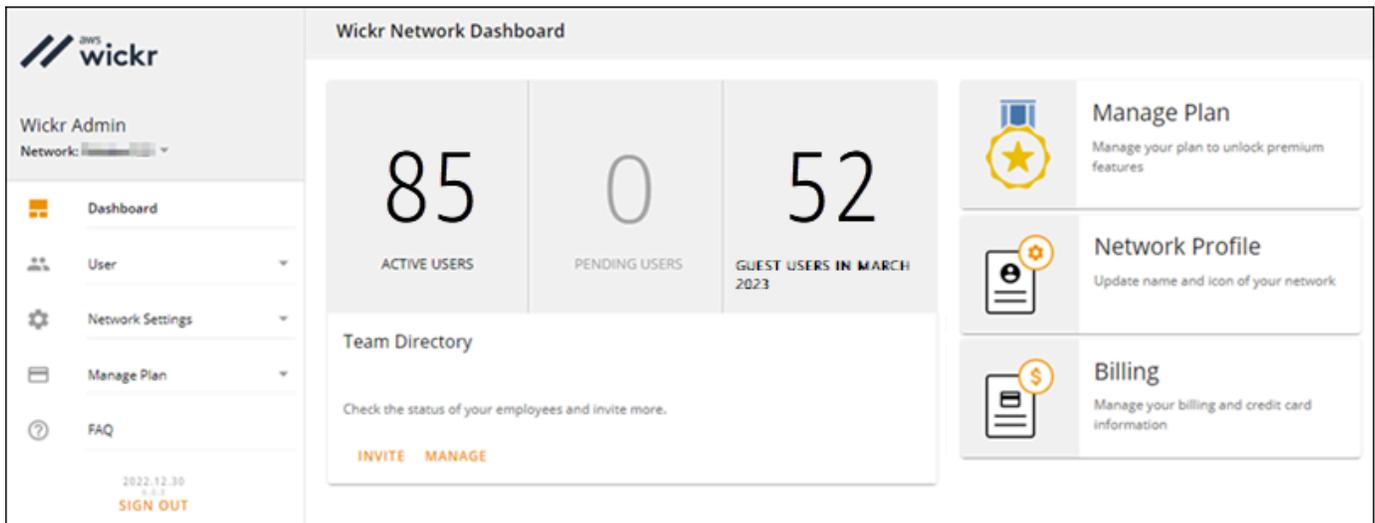
## SSO-Details anzeigen

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

1. [Öffnen Sie den AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu navigieren.



Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.



- Wählen Sie im Navigationsbereich der Wickr Admin Console Netzwerkeinstellungen und dann SSO-Konfiguration.

Auf der Seite Single Sign-On & LDAP-Konfiguration werden Ihr Wickr-Netzwerkendpunkt und die aktuelle SSO-Konfiguration angezeigt.

## SSO konfigurieren

Weitere Informationen zur Konfiguration von SSO finden Sie in den folgenden Anleitungen im Wickr Help Center:

### **⚠ Important**

Wenn Sie SSO konfigurieren, geben Sie eine Unternehmens-ID für Ihr Wickr-Netzwerk an. Notieren Sie sich unbedingt die Firmen-ID für Ihr Wickr-Netzwerk. Sie müssen es 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.

- [Konfigurieren Sie Azure AD Single Sign-On](#)
- [Konfigurieren Sie Okta Single Sign-On](#)

## 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.

## Quittungen lesen

Lesebestätigungen auf Wickr sind Benachrichtigungen, die an den Absender gesendet werden, um anzuzeigen, wann seine Nachricht gelesen wurde. Diese Belege sind in Konversationen verfügbar. one-on-one Für gesendete Nachrichten wird ein einzelnes Häkchen und für gelesene Nachrichten ein durchgezogener Kreis mit einem Häkchen angezeigt. Um Lesebestätigungen in 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 das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. Wählen Sie im Navigationsbereich der Wickr Admin Console Netzwerkeinstellungen und dann Netzwerkprofil aus.
3. Wählen Sie auf der Netzwerkprofilseite im Abschnitt Lesebestätigungen die Option Bearbeiten aus.
4. Wählen Sie Aktivieren oder Deaktivieren aus.

## Netzwerk-Tags

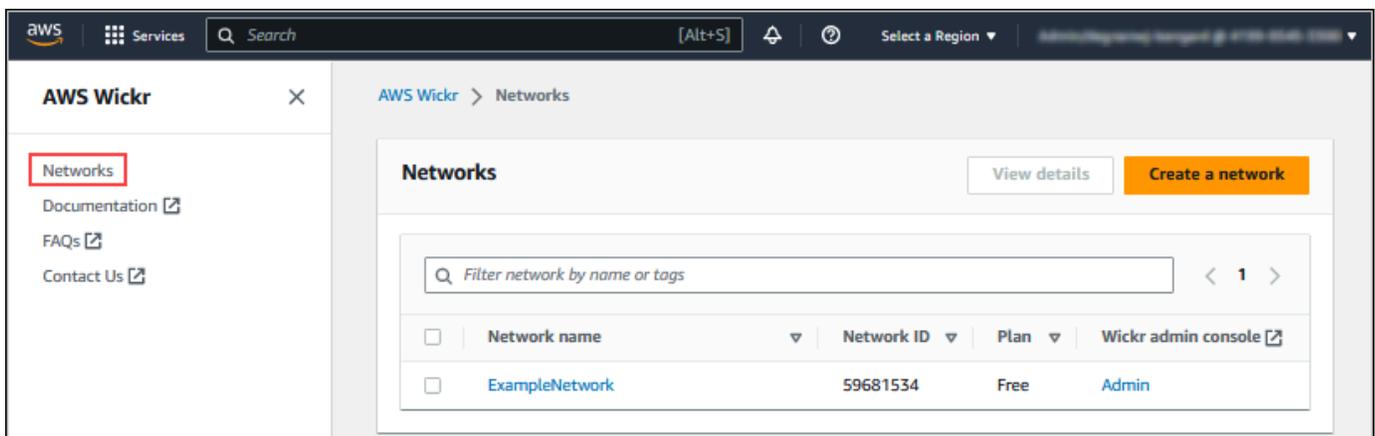
Sie können Tags auf Wickr-Netzwerke anwenden. Sie können diese Tags dann verwenden, um Ihre Wickr-Netzwerke zu durchsuchen und zu filtern oder Ihre AWS Kosten zu verfolgen. Sie können Netzwerk-Tags auf der Netzwerkübersichtsseite von AWS Management Console for Wickr konfigurieren.

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](#).

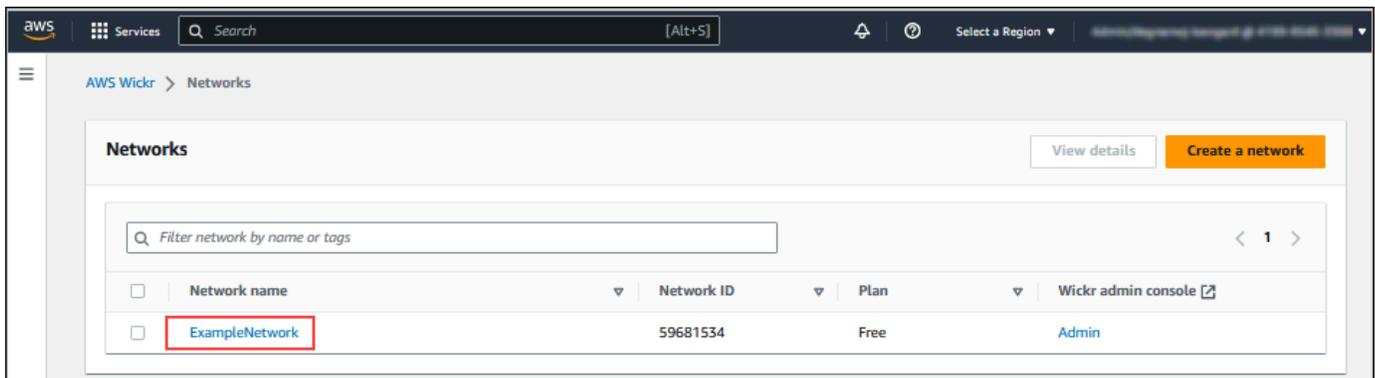
## Netzwerk-Tags verwalten

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

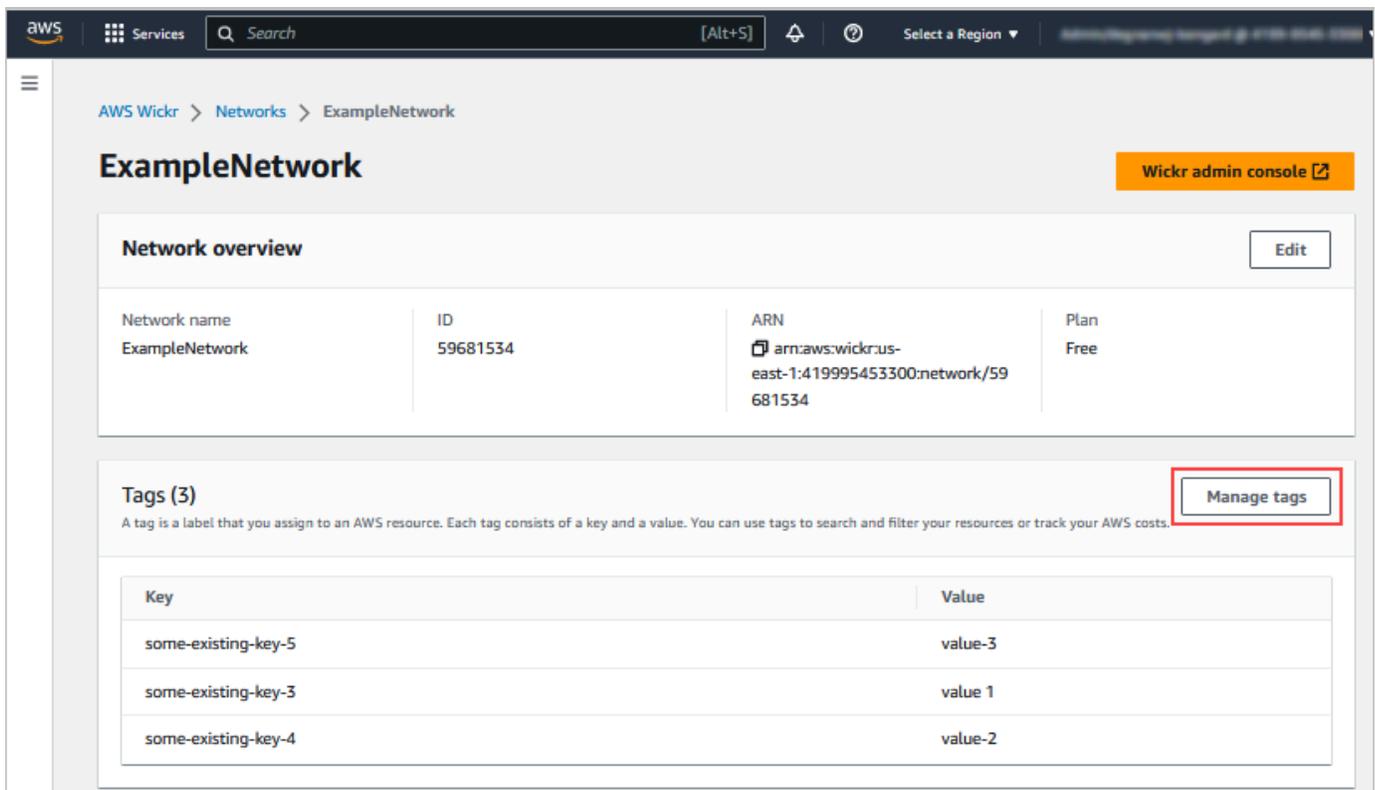
1. [Öffnen Sie das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. Wählen Sie im Navigationsbereich von AWS Management Console for Wickr Netzwerke aus.



- Wählen Sie auf der Seite Netzwerke den Namen des Netzwerks aus, für das Sie Tags verwalten möchten.



- Wählen Sie auf der Netzwerkübersichtsseite die Option Tags verwalten aus.



- 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 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](#).
- 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](#).

## Fügen Sie ein Netzwerk-Tag hinzu

Gehen Sie wie folgt vor, um Ihrem Wickr-Netzwerk ein Tag hinzuzufügen. Weitere Informationen zur Verwaltung von Tags finden Sie unter [Netzwerk-Tags verwalten](#).

1. Wählen Sie auf der Seite Tags verwalten Neuen Tag hinzufügen aus.
2. Geben Sie in die leeren Felder Schlüssel und Wert, die nun angezeigt werden, den Schlüssel und den Wert des neuen Tags ein.
3. Wählen Sie Änderungen speichern, um die neuen Tags zu speichern.

The screenshot displays the 'Manage Tags' page in the AWS Wickr console. The breadcrumb trail is 'AWS Wickr > Networks > ExampleNetwork > Manage tags'. The main heading is 'Manage Tags'. Below this, there is a table with two columns: 'Key' and 'Value - Required'. The table contains five rows, each representing a tag. The first four rows have existing tags, and the fifth row is for a new tag being added. The 'Key' field for the new tag is open, showing a dropdown menu with three options: 'some-existing-key-3', 'some-existing-key-4', and 'some-existing-key-5'. The 'Value - Required' field for the new tag is empty. At the bottom right, there are two buttons: 'Cancel' and 'Save changes', with the 'Save changes' button highlighted by a red box.

Key	Value - Required	
name-for-key	value-for-key	Remove
some-existing-key-5	value-3	Remove
some-existing-key-3	value 1	Remove
some-existing-key-4	value-2	Remove
Enter key some-existing-key-3 some-existing-key-4 some-existing-key-5	Enter value	Remove

Cancel Save changes

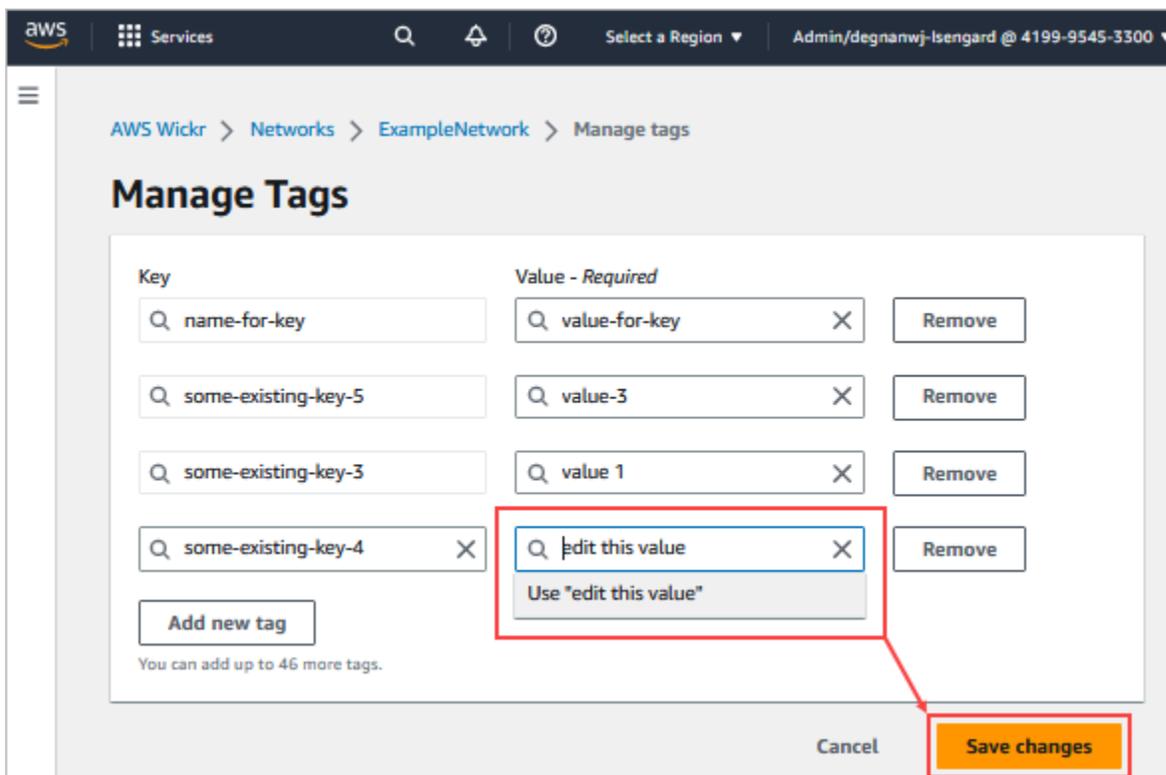
## Bearbeiten Sie ein Netzwerk-Tag

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

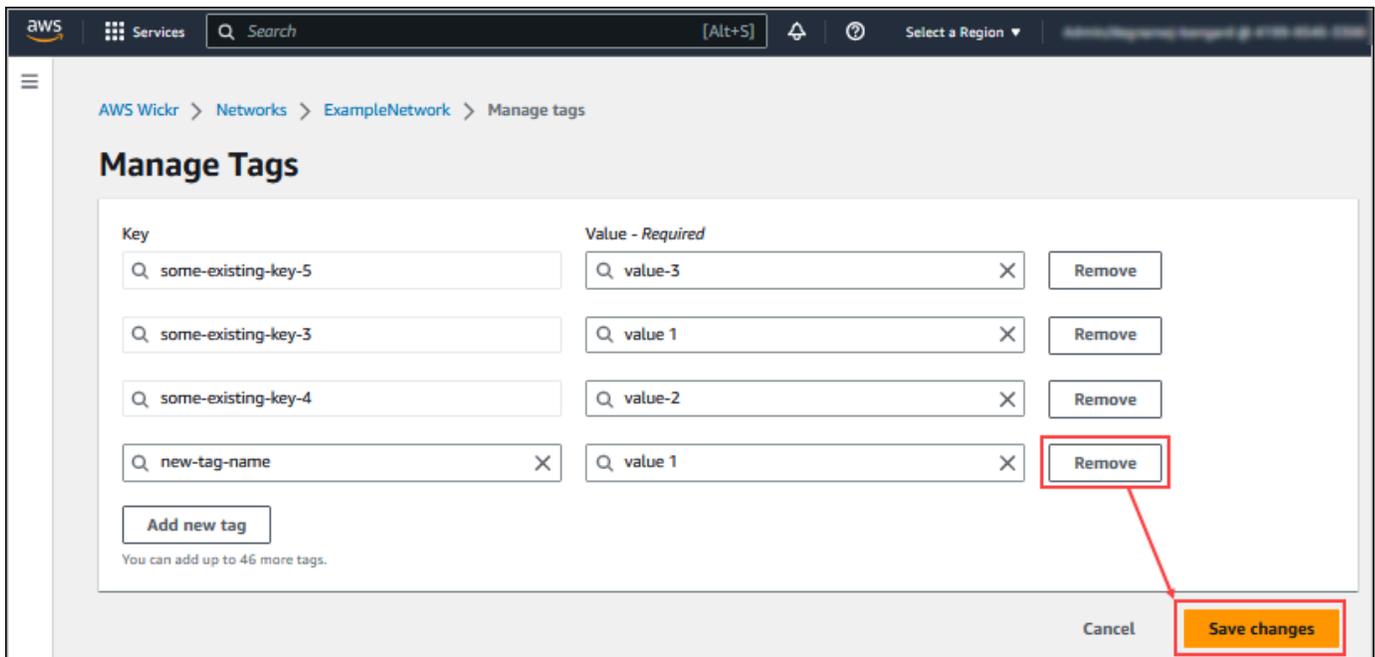


2. Wählen Sie Änderungen speichern, um Ihre Änderungen zu speichern.

## Entfernen Sie ein Netzwerk-Tag

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

## Netzwerkplan verwalten

Im Bereich Plan verwalten von AWS Management Console 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 das AWS Management Console für Wickr unter <https://console.aws.amazon.com/wickr/>.
2. Wählen Sie im Navigationsbereich der Wickr Admin Console die Option Plan verwalten und dann Mein Plan aus.
3. Wählen Sie auf der Seite Mein Plan den gewünschten Netzwerkplan aus. Sie können Ihren aktuellen Netzwerkplan ändern, indem Sie einen 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 können die kostenlose Premium-Testoption wählen, die für bis zu 30 Benutzer verfügbar ist und drei Monate gültig ist. Dieses Angebot gilt für neue, legacy-freie Testversionen und Standardpläne. Administratoren können während der kostenlosen Premium-Testphase 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, ist ein Upgrade auf eine kostenlose Premium-Testversion nicht möglich.

## Datenaufbewahrung

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 in seinem Netzwerk geteilt werden, gemäß den Compliance-Richtlinien des Unternehmens aufbewahrt. Auf diese TXT-Dateiausgaben kann der Netzwerkadministrator an einem externen Ort zugreifen (z. B. lokaler Speicher, Amazon S3 S3-Bucket oder ein anderer Speicher nach Wahl des Benutzers), von wo aus sie analysiert, gelöscht oder übertragen werden können.

#### Note

Wickr greift niemals auf Ihre Nachrichten und Dateien zu. Daher liegt es in Ihrer Verantwortung, ein Datenaufbewahrungssystem zu konfigurieren.

## Themen

- [Einzelheiten zur Datenspeicherung anzeigen](#)
- [Konfigurieren der Datenaufbewahrung](#)
- [Rufen Sie die Datenaufbewahrungsprotokolle ab](#)
- [Metriken und Ereignisse zur Datenspeicherung](#)

## Einzelheiten zur Datenspeicherung 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 Management Console für Wickr unter https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. Wählen Sie Netzwerk verwalten.
3. Wählen Sie im Navigationsbereich der Wickr Admin Console Netzwerkeinstellungen und dann Datenspeicherung.

Auf der Seite zur Datenspeicherung werden Schritte zum Einrichten der Datenspeicherung sowie die Option zum Aktivieren oder Deaktivieren der Datenaufbewahrungsfunktion angezeigt. Weitere Informationen zur Konfiguration der Datenspeicherung finden Sie unter [Konfigurieren der Datenaufbewahrung](#).

**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.

## Konfigurieren der Datenaufbewahrung

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

### Themen

- [Voraussetzungen für die Konfiguration der Datenaufbewahrung](#)
- [Passwort](#)
- [Speicheroptionen](#)
- [Umgebungsvariablen](#)
- [Secrets-Manager-Werte](#)
- [IAM-Richtlinie zur Verwendung der Datenaufbewahrung mit -AWSServices](#)
- [Starten des Bots zur Datenaufbewahrung](#)
- [Stoppen des Bots zur Datenaufbewahrung](#)

## Voraussetzungen für die Konfiguration der Datenaufbewahrung

Bevor Sie beginnen, müssen Sie den Bot-Namen für die Datenaufbewahrung (bezeichnet als Benutzername) und das ursprüngliche Passwort von AWS Management Console für Wickr abrufen. Sie müssen beide Werte angeben, wenn Sie den Bot zur Datenaufbewahrung zum ersten Mal

starten. Sie müssen die Datenaufbewahrung auch in der -Konsole aktivieren. Weitere Informationen finden Sie unter [Einzelheiten zur Datenspeicherung anzeigen](#).

## Passwort

Wenn Sie den Bot zur Datenaufbewahrung zum ersten Mal starten, geben Sie das ursprüngliche Passwort mit einer der folgenden Optionen an:

- Die WICKRIO\_BOT\_PASSWORD Umgebungsvariable. Die Umgebungsvariablen des Datenaufbewahrungs-Bots werden im [Umgebungsvariablen](#) Abschnitt weiter unten in diesem Leitfaden beschrieben.
- Der Passwortwert in Secrets Manager, der durch die AWS\_SECRET\_NAME Umgebungsvariable identifiziert wird. Die Secrets-Manager-Werte für den Datenaufbewahrungs-Bot werden im [Secrets-Manager-Werte](#) Abschnitt weiter unten in diesem Leitfaden beschrieben.
- Geben Sie das Passwort ein, wenn Sie vom Bot zur Datenaufbewahrung 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 Bot zur Datenaufbewahrung neu installieren müssen, verwenden Sie das generierte Passwort. Das ursprüngliche Passwort ist nach der Erstinstallation des Datenaufbewahrungs-Bots nicht gültig.

Das neu generierte Passwort wird angezeigt, wie im folgenden Beispiel gezeigt.

### Important

Bewahren Sie das Passwort an einem sicheren Ort auf. Wenn Sie das Passwort verlieren, können Sie den Bot zur Datenaufbewahrung nicht neu installieren. Geben Sie dieses Passwort nicht weiter. Es bietet die Möglichkeit, die Datenaufbewahrung 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
      "HuEXAMPLERAW41GgEXAMPLEn"
```

\*\*\*\*\*

## Speicheroptionen

Nachdem die Datenaufbewahrung aktiviert und der Bot für die Datenaufbewahrung für Ihr Wickr-Netzwerk konfiguriert ist, 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 beschränkt sind, das mit einer Umgebungsvariablen konfiguriert werden kann. Weitere Informationen finden Sie unter [Umgebungsvariablen](#).

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 für die langfristige Speicherung in ein anderes System zu verschieben und sicherzustellen, dass dem Host-Datenträger nicht der Arbeitsspeicher oder Speicherplatz ausgeht.
- Speichern Sie alle erfassten Nachrichten und Dateien in einem Amazon S3-Bucket. Der Datenaufbewahrungs-Bot speichert alle entschlüsselten Nachrichten und Dateien in dem von Ihnen angegebenen Amazon 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, die in einem Amazon S3-Bucket verschlüsselt sind. Der Datenaufbewahrungs-Bot verschlüsselt alle erfassten Nachrichten und Dateien mit einem von Ihnen bereitgestellten Schlüssel erneut und speichert sie in dem von Ihnen angegebenen Amazon 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 zum Erstellen eines Amazon S3-Buckets zur Verwendung mit Ihrem Datenaufbewahrungs-Bot finden Sie unter [Erstellen eines Buckets](#) im Amazon S3-Benutzerhandbuch.

## Umgebungsvariablen

Sie können die folgenden Umgebungsvariablen verwenden, um den Bot zur Datenaufbewahrung zu konfigurieren. Sie legen diese Umgebungsvariablen mit der `-e` Option fest, wenn Sie das Docker-Image des Datenaufbewahrungs-Bots ausführen. Weitere Informationen finden Sie unter [Starten des Bots zur Datenaufbewahrung](#).

 Note

Diese Umgebungsvariablen sind optional, sofern nicht anders angegeben.

Verwenden Sie die folgenden Umgebungsvariablen, um die Anmeldeinformationen des Datenaufbewahrungs-Bots anzugeben:

- WICKRIO\_BOT\_NAME – Der Name des Bots zur Datenaufbewahrung. Diese Variable ist erforderlich, wenn Sie das Docker-Image des Datenaufbewahrungs-Bots ausführen.
- WICKRIO\_BOT\_PASSWORD – Das ursprüngliche Passwort für den Datenaufbewahrungs-Bot. Weitere Informationen finden Sie unter [Voraussetzungen für die Konfiguration der Datenaufbewahrung](#). Diese Variable ist erforderlich, wenn Sie nicht vorhaben, den Datenaufbewahrungs-Bot mit einer Passwortaufforderung zu starten oder Secrets Manager nicht zum Speichern der Anmeldeinformationen des Datenaufbewahrungs-Bots verwenden möchten.

Verwenden Sie die folgenden Umgebungsvariablen, um die Standard-Streaming-Funktionen für die Datenaufbewahrung zu konfigurieren:

- WICKRIO\_COMP\_MESGDEST – Der Pfadname zu dem Verzeichnis, in das Nachrichten gestreamt werden. Der Standardwert ist `/tmp/<botname>/compliance/messages`.
- WICKRIO\_COMP\_FILEDEST – Der Pfadname zu dem Verzeichnis, in das Dateien gestreamt werden. Der Standardwert ist `/tmp/<botname>/compliance/attachments`.
- WICKRIO\_COMP\_BASENAME – Der Basisname für die empfangenen Nachrichtendateien. Der Standardwert ist `receivedMessages`.
- WICKRIO\_COMP\_FILESIZE – Die maximale Dateigröße für eine empfangene Nachrichtendatei 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 eine Datei mit empfangenen Nachrichten ablegt. Eine neue Datei wird gestartet, wenn das Zeitlimit erreicht ist. Sie können nur die Dateigröße oder `-zeit` verwenden, um die Größe der Datei für empfangene Nachrichten zu begrenzen. Der Standardwert ist `0`, wie bei keinem Limit.

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

- `AWS_DEFAULT_REGION` – Die Standardeinstellung, AWS-Region die für AWS Services wie Secrets Manager verwendet 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-Secret anzugeben, das verwendet werden soll, wenn Sie Secrets Manager zum Speichern der Anmeldeinformationen und AWS Serviceinformationen für den Datenaufbewahrungs-Bot verwenden möchten. Weitere Informationen zu den Werten, die Sie in Secrets Manager speichern können, finden Sie unter [Secrets-Manager-Werte](#).

- `AWS_SECRET_NAME` – Der Name des Secrets-Manager-Geheimnisses, das die Anmeldeinformationen und AWS Serviceinformationen enthält, die der Datenaufbewahrungs-Bot benötigt.
- `AWS_SECRET_REGION` – Die AWS-Region, in der sich das AWS Secret befindet. Wenn Sie AWS Secrets verwenden und dieser Wert nicht definiert ist, wird der `AWS_DEFAULT_REGION` Wert verwendet.

#### Note

Sie können alle der folgenden Umgebungsvariablen als Werte in Secrets Manager speichern. Wenn Sie Secrets Manager verwenden und diese Werte dort speichern, müssen Sie sie nicht als Umgebungsvariablen angeben, wenn Sie das Docker-Image für den Datenaufbewahrungs-Bot ausführen. Sie müssen nur die zuvor in diesem Handbuch beschriebene `AWS_SECRET_NAME` Umgebungsvariable angeben. Weitere Informationen finden Sie unter [Secrets-Manager-Werte](#).

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

- `WICKRIO_S3_BUCKET_NAME` – Der Name des Amazon S3-Buckets, in dem Nachrichten und Dateien gespeichert werden.
- `WICKRIO_S3_REGION` – Die AWS Region des Amazon S3-Buckets, in der Nachrichten und Dateien gespeichert werden.

- `WICKRIO_S3_FOLDER_NAME` – Der optionale Ordnername im Amazon S3-Bucket, in dem Nachrichten und Dateien gespeichert werden. Dem Ordnernamen wird der Schlüssel für Nachrichten und Dateien vorangestellt, die im Amazon S3-Bucket gespeichert sind.

Verwenden Sie die folgenden Umgebungsvariablen, um die AWS KMS Details anzugeben, wenn Sie sich dafür entscheiden, die clientseitige Verschlüsselung zu verwenden, um Dateien beim Speichern in einem Amazon S3-Bucket erneut zu verschlüsseln.

- `WICKRIO_KMS_MSTRKEY_ARN` – Der Amazon-Ressourcenname (ARN) des AWS KMS Masterschlüssels, 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 Masterschlüssel befindet.

Verwenden Sie die folgende Umgebungsvariable, um die Amazon SNS-Details anzugeben, wenn Sie Datenaufbewahrungseignisse an ein Amazon SNS-Thema senden möchten. Zu den gesendeten Ereignissen gehören Startup, Herunterfahren sowie Fehlerbedingungen.

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

Verwenden Sie die folgende Umgebungsvariable, um Datenaufbewahrungsmetriken an zu senden CloudWatch. Wenn angegeben, werden die Metriken alle 60 Sekunden generiert.

- `WICKRIO_METRICS_TYPE` – Legen Sie den Wert dieser Umgebungsvariablen auf `festcloudwatch`, um Metriken an zu senden CloudWatch.

## Secrets-Manager-Werte

Sie können Secrets Manager verwenden, um die Anmeldeinformationen und AWS Serviceinformationen des Datenaufbewahrungsbots zu speichern. Weitere Informationen zum Erstellen eines Secrets-Manager-Secrets finden Sie unter [Erstellen eines AWS Secrets Manager-Secrets](#) im Secrets-Manager-Benutzerhandbuch.

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

- `password` – Das Bot-Passwort für die Datenaufbewahrung.

- `s3_bucket_name` – Der Name des Amazon S3-Buckets, in dem Nachrichten und Dateien gespeichert werden. Wenn nicht festgelegt, wird das Standard-Dateistreaming verwendet.
- `s3_region` – Die AWS Region des Amazon S3-Buckets, in der Nachrichten und Dateien gespeichert werden.
- `s3_folder_name` – Der optionale Ordnername im Amazon S3-Bucket, in dem Nachrichten und Dateien gespeichert werden. Dem Ordnernamen wird der Schlüssel für Nachrichten und Dateien vorangestellt, die im Amazon S3-Bucket gespeichert sind.
- `kms_master_key_arn` – Der ARN des AWS KMS Masterschlüssels, der zum erneuten Verschlüsseln der Nachrichtendateien und Dateien auf dem Datenaufbewahrungs-Bot verwendet wird, bevor sie im Amazon 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-Themas, an das Datenaufbewahrungseignisse gesendet werden sollen.

## IAM-Richtlinie zur Verwendung der Datenaufbewahrung mit -AWSServices

Wenn Sie andere -AWSServices mit dem Wickr-Bot zur Datenaufbewahrung verwenden möchten, müssen Sie sicherstellen, dass der Host über die entsprechende AWS Identity and Access Management (IAM)-Rolle und -Richtlinie verfügt, um darauf zuzugreifen. Sie können den Datenaufbewahrungs-Bot für die Verwendung von Secrets Manager, Amazon S3, CloudWatch Amazon SNS und konfigurieren AWS KMS. Die folgende IAM-Richtlinie erlaubt den Zugriff auf bestimmte Aktionen für diese Services.

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

```
    ]
  }
```

Sie können eine IAM-Richtlinie erstellen, die strenger ist, indem Sie die spezifischen Objekte für jeden Service identifizieren, dem die Container auf Ihrem Host Zugriff gewähren sollen. Entfernen Sie die Aktionen für die AWS Services, die Sie nicht verwenden möchten. Wenn Sie beispielsweise nur einen Amazon S3-Bucket verwenden möchten, verwenden Sie die folgende Richtlinie, die die `cloudwatch:PutMetricData` Aktionen `secretsmanager:GetSecretValue`, `sns:Publish` und `kms:GenerateDataKey` entfernt.

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

Wenn Sie eine Amazon Elastic Compute Cloud (Amazon EC2)-Instance zum Hosten Ihres Datenaufbewahrungs-Bots verwenden, erstellen Sie eine IAM-Rolle mit dem Amazon EC2-Häufigfall und weisen Sie eine Richtlinie mit der oben genannten Richtliniendefinition zu.

## Starten des Bots zur Datenaufbewahrung

Bevor Sie den Bot zur Datenaufbewahrung ausführen, sollten Sie bestimmen, wie Sie ihn konfigurieren möchten. Wenn Sie den Bot auf einem Host ausführen möchten, der:

- Hat keinen Zugriff auf `-AWSServices`, dann sind Ihre Optionen begrenzt. In diesem Fall verwenden Sie die Standard-Streaming-Optionen für Nachrichten. 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](#).
- Hat Zugriff auf `-AWSServices`, dann sollten Sie ein Secrets-Manager-Secret erstellen, um die Bot-Anmeldeinformationen und AWS Service-Konfigurationsdetails zu speichern. Nachdem die AWS Services konfiguriert sind, können Sie mit dem Starten des Docker-Images des Datenaufbewahrungs-Bots fortfahren. Weitere Informationen zu den Details, die Sie in einem Secrets-Manager-Secret speichern können, finden Sie unter [Secrets-Manager-Werte](#)

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

- *compliance\_1234567890\_bot* durch den Namen Ihres Bots zur Datenaufbewahrung.
- *password* mit dem Passwort für Ihren Datenaufbewahrungs-Bot.
- *wickr/data/retention/bot* durch den Namen Ihres Secrets-Manager-Geheimnisses, das mit Ihrem Datenaufbewahrungs-Bot verwendet werden soll.
- *bucket-name* durch den Namen des Amazon S3-Buckets, in dem Nachrichten und Dateien gespeichert werden.
- *folder-name* durch den Ordernamen im Amazon S3-Bucket, in dem Nachrichten und Dateien gespeichert werden.
- *us-east-1* durch die AWS Region der Ressource, die Sie angeben. Zum Beispiel die Region des AWS KMS Masterschlüssels oder die Region des Amazon S3-Buckets.
- *arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-a617-abababababab* durch den Amazon-Ressourcennamen (ARN) Ihres AWS KMS Masterschlüssels, der zum erneuten Verschlüsseln von Nachrichtendateien und Dateien verwendet werden soll.

#### Starten des Bots mit der Passwort-Umgebungsvariable (kein AWS Service)

Der folgende Docker-Befehl startet den Bot zur Datenaufbewahrung. Das Passwort wird mithilfe der `-WICKRIO_BOT_PASSWORD` Umgebungsvariablen angegeben. Der Bot beginnt mit der Verwendung des Standard-Dateistreamings und der Verwendung der im [Umgebungsvariablen](#) 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' \  
wickr/bot-compliance-cloud:latest
```

#### Starten des Bots mit Passwortaufforderung (kein AWS Service)

Der folgende Docker-Befehl startet den Bot zur Datenaufbewahrung. Das Passwort wird eingegeben, wenn der Bot zur Datenaufbewahrung dazu aufgefordert wird. Es verwendet das Standard-Dateistreaming unter Verwendung der im [Umgebungsvariablen](#) 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' \
wickr/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 Passwortaufforderung zu erhalten. Sie sollten den `docker attach <container ID or container name>` Befehl auch unmittelbar nach dem Starten des Docker-Images ausführen, damit Sie die Passwortaufforderung erhalten. Sie sollten beide Befehle in einem Skript ausführen. Wenn Sie an das Docker-Image anhängen und die Eingabeaufforderung nicht angezeigt wird, drücken Sie die Eingabetaste und die Eingabeaufforderung wird angezeigt.

Starten Sie den Bot mit einer 15-minütigen Nachrichtendateirotation (kein AWS Service)

Der folgende Docker-Befehl startet den Bot zur Datenaufbewahrung mithilfe von Umgebungsvariablen. Außerdem wird es so konfiguriert, dass die empfangenen Nachrichtendateien auf 15 Minuten gedreht 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=15 \
wickr/bot-compliance-cloud:latest
```

Starten Sie den Bot und geben Sie das ursprüngliche Passwort 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 sind.

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

```
-e AWS_SECRET_NAME='wickr/data/retention/bot' \  
wickr/bot-compliance-cloud:latest
```

Das `wickrpro/compliance/compliance_1234567890_bot` Secret enthält den folgenden Secret-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-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 sind.

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

Das `wickrpro/compliance/compliance_1234567890_bot` Secret enthält den folgenden Secret-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 in den `bot-compliance` Bucket im Ordner mit dem Namen `eingefügtnetwork1234567890`.

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-Bucket und AWS KMS die Masterschlüsselinformationen zu hosten. Wenn Sie den Datenaufbewahrungs-

Bot starten, müssen Sie eine Umgebungsvariable festlegen, die den Secrets Manager angibt, in dem diese Informationen gespeichert sind.

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

Das wickrpro/compliance/compliance\_1234567890\_bot Secret enthält den folgenden Secret-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"
}
```

Nachrichten und Dateien, die vom Bot empfangen werden, werden mit dem KMS-Schlüssel verschlüsselt, der durch den ARN-Wert identifiziert wird, und dann in den Bucket „bot-compliance“ im Ordner „network1234567890“ eingefügt. Stellen Sie sicher, dass Sie über die entsprechende IAM-Richtlinieneinrichtung verfügen.

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

Wenn Sie Secrets Manager nicht zum Hosten der Anmeldeinformationen des Datenaufbewahrungsbots verwenden möchten, können Sie das Docker-Image des Datenaufbewahrungsbots 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_S3_BUCKET_NAME='bucket-name' \
-e WICKRIO_S3_FOLDER_NAME='folder-name' \
```

```
-e WICKRIO_S3_REGION='us-east-1' \  
wickr/bot-compliance-cloud:latest
```

Sie können Umgebungswerte verwenden, um die Anmeldeinformationen des Datenaufbewahrungs-Bots, Informationen zu Amazon S3-Buckets und Konfigurationsinformationen für das Standard-Dateistreaming zu identifizieren.

## Stoppen des Bots zur Datenaufbewahrung

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 Datenaufbewahrungs-Bots auszugeben.

```
docker stop compliance_1234567890_bot
```

## Rufen Sie die Datenaufbewahrungsprotokolle ab

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

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.

Themen

- [CloudWatch Metriken](#)
- [Amazon SNS SNS-Ereignisse](#)

## CloudWatch Metriken

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	Beschreibung
Messages_Rx	Empfangene Nachrichten.
Messages_Rx_Failed	Fehler bei der Verarbeitung empfangener Nachrichten.
Nachrichten_Gespeichert	Nachrichten, die in der Datei mit empfangenen Nachrichten gespeichert wurden.
Messages_Saved_Failed	Fehler beim Speichern von Nachrichten in der Datei mit empfangenen Nachrichten.
Gespeicherte Dateien	Empfangene Dateien.
Files_Saved_Bytes	Anzahl der Byte für empfangene Dateien.
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-Geräts oder einer bestimmten Instanz. Nützlich, wenn Sie mehrere Bot-Geräte oder -Instanzen ausführen.
Produkt	Das Produkt für den Bot. Kann <code>WickrEnterprise_</code> mit <code>AlphaBeta</code> , <code>WickrPro_</code> oder <code>Production</code> angehängt werden.
BotType	Der Bot-Typ. Für die Compliance-Bots als <code>Compliance</code> gekennzeichnet.
Network (Netzwerk)	Die ID des zugehörigen Netzwerks.

## Amazon SNS SNS-Ereignisse

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 finden Sie unter [Umgebungsvariablen](#) und [Secrets-Manager-Werte](#).

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 Datenaufbewahrungsbots.

Name	Wert
DateTime	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 <a href="#">Kritische Ereignisse</a> und <a href="#">Normale Ereignisse</a> .
notificationType	Dieser Wert wird seinBot 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": "wickr/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	Der Benutzer wurde nicht gefunden.
Anmeldung fehlgeschlagen	Konto oder Gerät ist gesperrt.
Bereitstellung	Der Benutzer hat den Befehl beendet.
Bereitstellung	Falsches Passwort für die <code>config.wickr</code> Datei.
Bereitstellung	Die <code>config.wickr</code> Datei kann nicht gelesen werden.
Anmeldung fehlgeschlagen	Alle Anmeldungen sind fehlgeschlagen.
Anmeldung fehlgeschlagen	Neuer Benutzer, aber die Datenbank ist bereits vorhanden.

### Weitere kritische Ereignisse

Ereignistyp	Ereignismeldungen
Konto gesperrt	WickRIOClientMain:: slotAdminUser Sperren: Code (%1): Grund: %2“
BotDevice Ausgesetzt	Gerät ist gesperrt!

Ereignistyp	Ereignismeldungen
WatchDog	Das SwitchBoard System ist länger als <i>&lt; N &gt;</i> Minuten ausgefallen
S3-Ausfälle	Die Datei <i>&lt; file-name &gt;</i> konnte nicht in den S3-Bucket eingefügt werden. <i>Fehler: &lt;AWS-error &gt;</i>
Ausweichschlüssel	VOM SERVER ÜBERMITTELTEN FALLBACK-SCHLÜSSEL: Ist kein anerkannter aktiver Fallschlüssel 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!

### Hat sich nicht 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": "wickr/bot-compliance-cloud",
  "dockerTag": "5.116.13.01",
  "message": "There are updates available",
  "notificationType": "Bot Event",
  "severity": "normal",
  "versions": [
    "5.116.10.01"
  ]
}
```

## Was ist ATAK?

Das Android Team microSD Kit (ATAK) – oder Android Tactical Assault Kit (auch ATAK) zur Telefonie – ist eine Geodateninfrastruktur und eine Anwendung zur Situationserkennung für Smartphones, die eine sichere Zusammenarbeit anstelle von Geografie ermöglicht. Während es ursprünglich für die Verwendung in Zonen in Telefonie konzipiert wurde, wurde ATAK an die Missionen lokaler, Bundes- und Bundesbehörde angepasst.

### Themen

- [Aktivieren von ATAK im Wickr Network Dashboard](#)
- [Zusätzliche Informationen zu ATAK](#)

- [Installieren und koppeln Sie das Wickr-Plugin für ATAK](#)
- [Wählen und Empfangen eines Anrufs](#)
- [Senden einer Datei](#)
- [Senden einer sicheren Sprachnachricht \(Push-to-talk\)](#)
- [Pinwheel \(Quick Access\)](#)
- [Navigation](#)

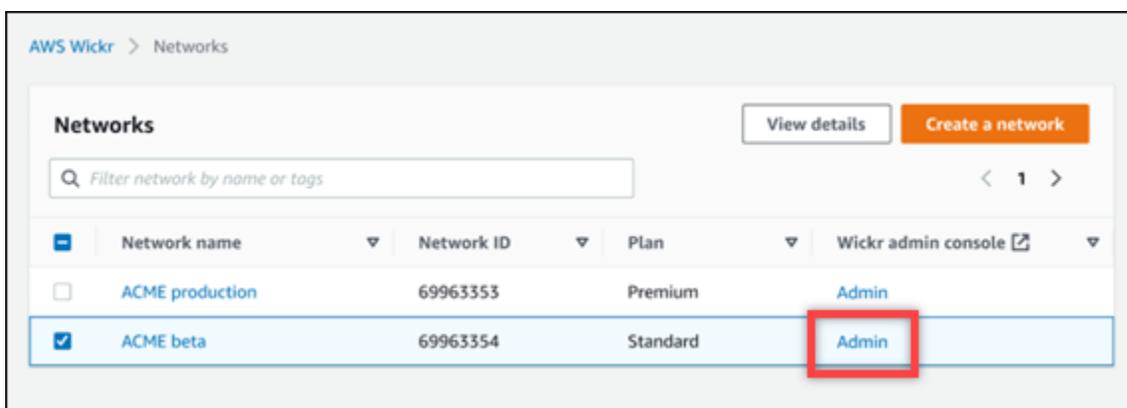
## Aktivieren von ATAK im Wickr Network Dashboard

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

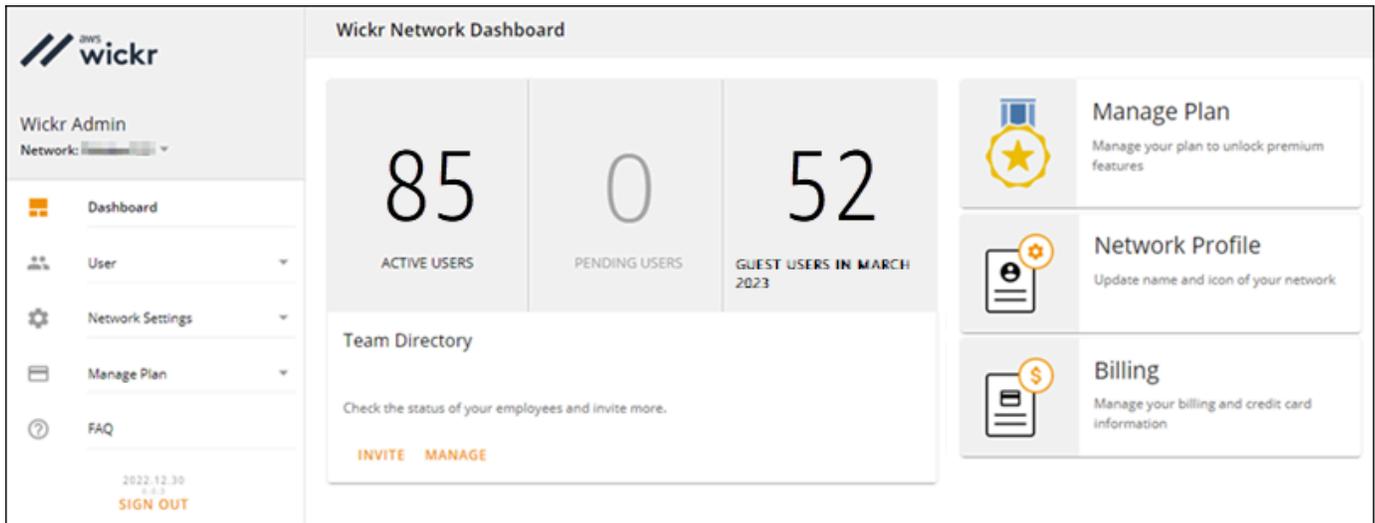
### Aktivieren von ATAK im Wickr Network Dashboard

Führen Sie das folgende Verfahren aus, um ATAK im Wickr Network Dashboard zu aktivieren.

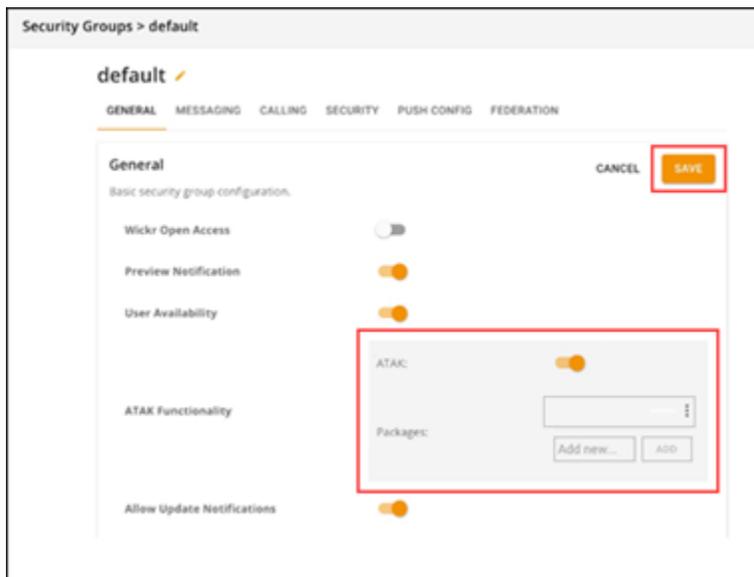
1. Öffnen Sie die AWS Management Console für Wickr unter <https://console.aws.amazon.com/wickr/>.
2. Wählen Sie auf der Seite Netzwerke den Admin-Link aus, um zur Wickr-Admin-Konsole für dieses Netzwerk zu navigieren.



Sie werden für ein bestimmtes Netzwerk zur Wickr-Admin-Konsole umgeleitet.



3. Wählen Sie im Navigationsbereich der Wickr-Admin-Konsole Netzwerkeinstellungen und dann Sicherheitsgruppe aus.
4. Wählen Sie Details neben der gewünschten Sicherheitsgruppe aus, für die Sie ATAK aktivieren möchten.
5. Wählen Sie im Tab General die Option Edit aus.
6. Im Abschnitt ATAK-Funktionalität:
  - a. Geben Sie den Paketnamen in das Textfeld Pakete ein. Sie können je nach Version des ATAK, den Ihre Benutzer installieren und verwenden werden, einen der folgenden Werte eingeben:
    - `com.atakmap.app.civ` – Geben Sie diesen Wert in das Textfeld Pakete ein, wenn Ihre Wickr-Endbenutzer die microSDian-Version der ATAK-Anwendung auf ihren Android-Geräten installieren und verwenden werden.
    - `com.atakmap.app.mil` – Geben Sie diesen Wert in das Textfeld Pakete ein, wenn Ihre Wickr-Endbenutzer die microSD-Version der ATAK-Anwendung auf ihren Android-Geräten installieren und verwenden werden.
  - b. Bewegen Sie den ATAK-Schalter nach rechts, um die Funktionalität zu aktivieren.
  - c. 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-Plugins](#).

## Zusätzliche Informationen zu ATAK

Weitere Informationen zum Wickr-Plugin für ATAK finden Sie hier:

- [Übersicht über das Wickr-ATAK-Plugin](#)
- [Zusätzliche Informationen zum Wickr-ATAK-Plugin](#)

## Installieren und koppeln Sie das Wickr-Plugin für ATAK

Bei dem Android Team microSD Kit (ATAK) handelt es sich um eine Android-Lösung, die von US-Bezirken, US-Bundesstaats- und Arztbehörden verwendet wird, die für die Planung, Ausführung und Reaktion auf Vorfälle Fähigkeiten zur Situationserkennung benötigen. ATAK verfügt über eine Plugin-Architektur, mit der Entwickler Funktionen hinzufügen können. Es ermöglicht Benutzern, mithilfe von GPS- und Geodaten zu navigieren, die mit Echtzeit-Situationserkennung für laufende Ereignisse überlagert sind. In diesem Dokument zeigen wir Ihnen, wie Sie das Wickr-Plugin für ATAK

auf einem Android-Gerät installieren und es mit dem Wickr-Client koppeln. Auf diese Weise können Sie Nachrichten an Wickr senden und zusammenarbeiten, ohne die ATAK-Anwendung zu verlassen.

## Installieren des Wickr-Plugins für ATAK

Führen Sie das folgende Verfahren aus, um das Wickr-Plugin für ATAK auf einem Android-Gerät zu installieren.

1. Gehen Sie zum Google Play Store und installieren Sie das Plugin Wickr für ATAK.
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 dann Plugins aus.
4. Wählen Sie Importieren aus.
5. Wählen Sie im Popup-Fenster Importtyp auswählen die Option Lokale SD aus und navigieren Sie zu der Stelle, an der Sie das Wickr-Plugin 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 aus.

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

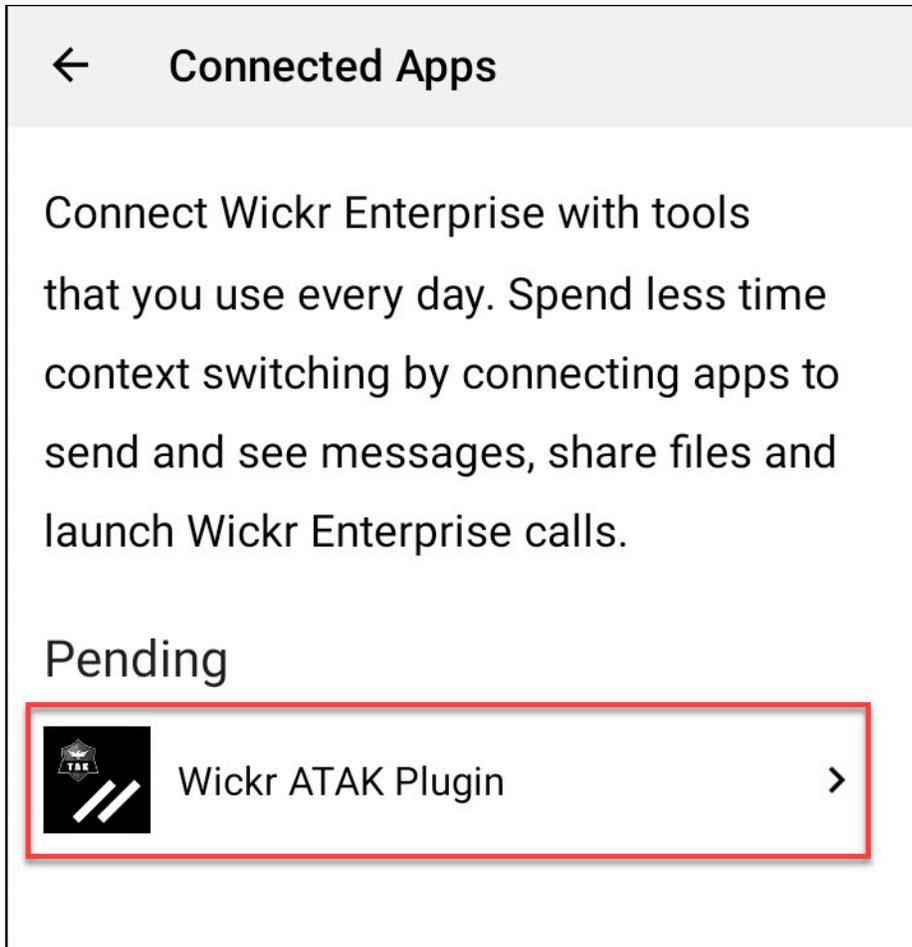
Das Wickr-Plugin für ATAK ist jetzt installiert. Fahren Sie mit dem folgenden Abschnitt ATAK mit Wickr koppeln fort, um den Vorgang abzuschließen.

## ATAK mit Wickr koppeln

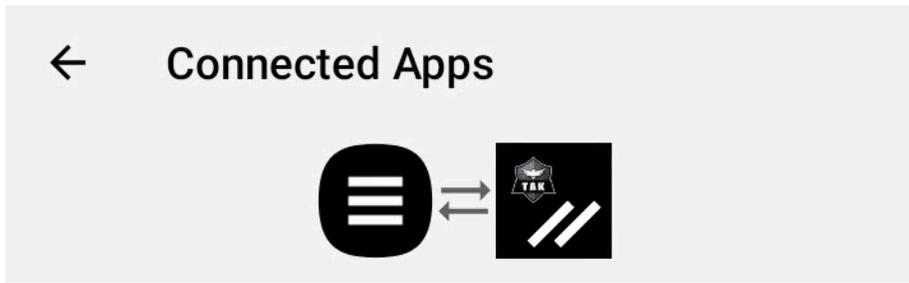
Führen Sie das folgende Verfahren aus, um die ATAK-Anwendung mit Wickr zu koppeln, nachdem Sie das Wickr-Plugin für ATAK erfolgreich installiert haben.

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

Es wird eine Benachrichtigungsaufforderung angezeigt, 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 wechseln Sie zu Einstellungen und dann zu Verbundene Apps. Sie sollten das Plugin im Abschnitt Ausstehend des Bildschirms sehen.



3. Wählen Sie Zu Paar genehmigen aus.
4. Wählen Sie die Schaltfläche Wickr-ATAK-Plugin öffnen, um zur ATAK-Anwendung zurückzukehren.



## Success

You've successfully connected Wickr Enterprise to Wickr ATAK Plugin.

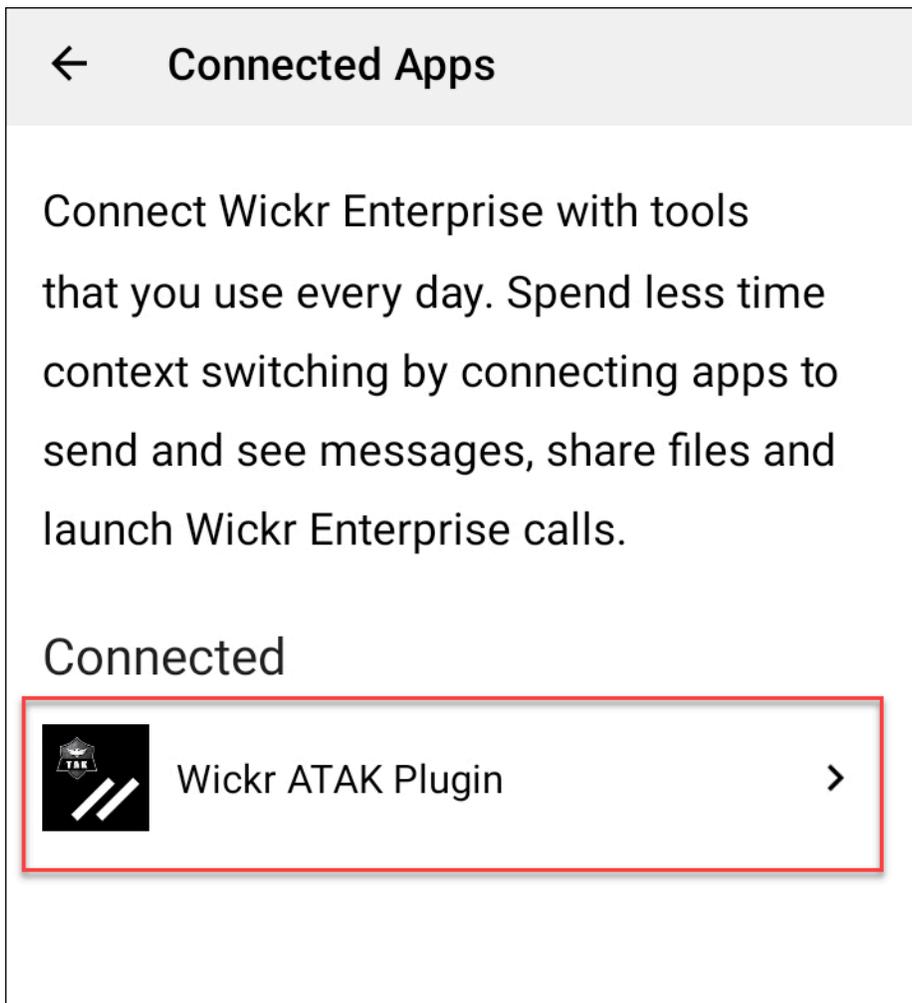


Sie haben jetzt das ATAK-Plugin erfolgreich mit Wickr gekoppelt und können das Plugin verwenden, um Nachrichten zu senden und mit Wickr zu arbeiten, ohne die ATAK-Anwendung zu verlassen.

### ATAK mit Wickr entkoppeln

Führen Sie das folgende Verfahren aus, 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 Connected Apps die Option Wickr-ATAK-Plugin aus.



3. Wählen Sie auf dem Bildschirm Wickr-ATAK-Plugin unten auf dem Bildschirm Entfernen aus.

Auf einem Bestätigungsbildschirm wird angezeigt, dass Sie die API nicht mehr verwenden. Sie haben nun das ATAK-Plugin erfolgreich entkoppelt.

## Wählen und Empfangen eines Anrufs

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

Führen Sie das folgende Verfahren aus, um anzurufen und einen Anruf zu empfangen.

1. Öffnen Sie ein Chat-Fenster.
2. Wählen Sie in der Ansicht Map das Symbol für den Benutzer aus, den Sie aufrufen möchten.
3. Wählen Sie oben rechts auf dem Bildschirm das Telefonsymbol aus.

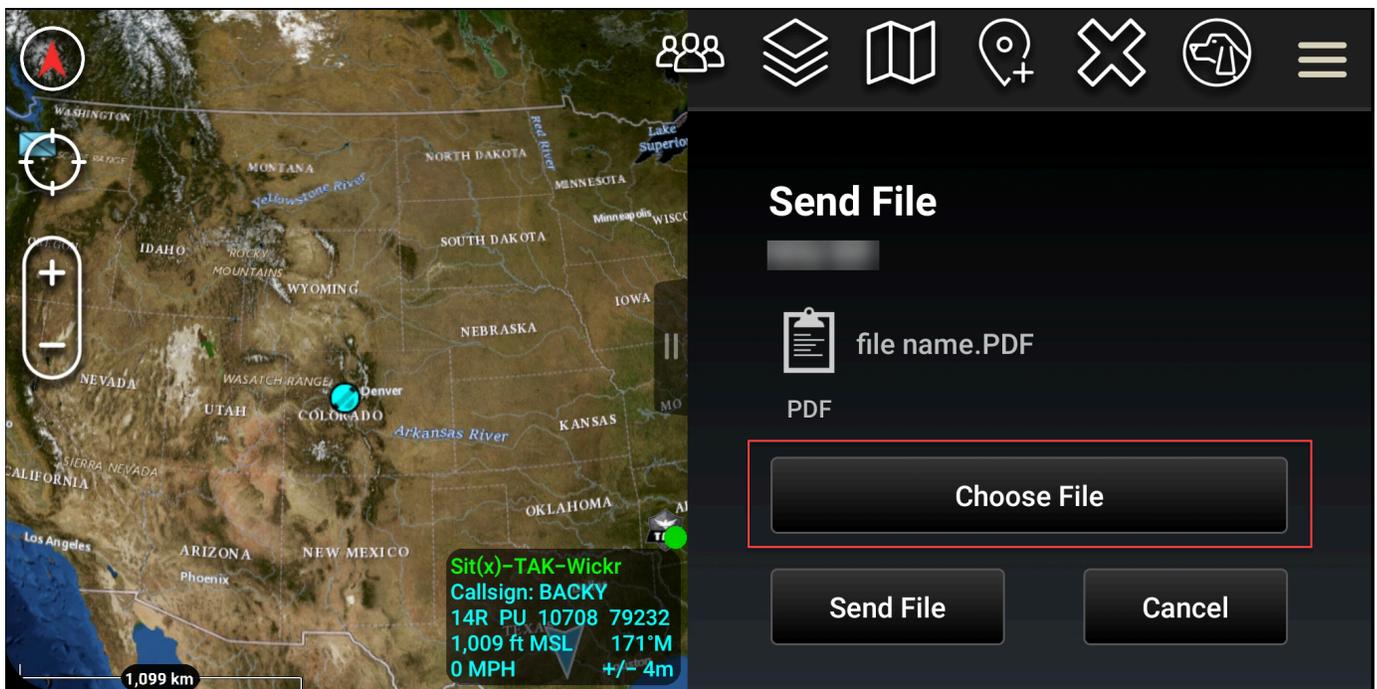
4. Sobald die Verbindung hergestellt ist, können Sie zur Ansicht des ATAK-Plugins zurückkehren und einen -Aufruf erhalten.

## Senden einer Datei

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

Führen Sie das folgende Verfahren aus, um eine Datei zu senden.

1. Öffnen Sie ein Chat-Fenster.
2. Suchen Sie in der Ansicht Map nach dem Benutzer, dem Sie eine Datei senden möchten.
3. Wenn Sie den Benutzer finden, den 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 aus.

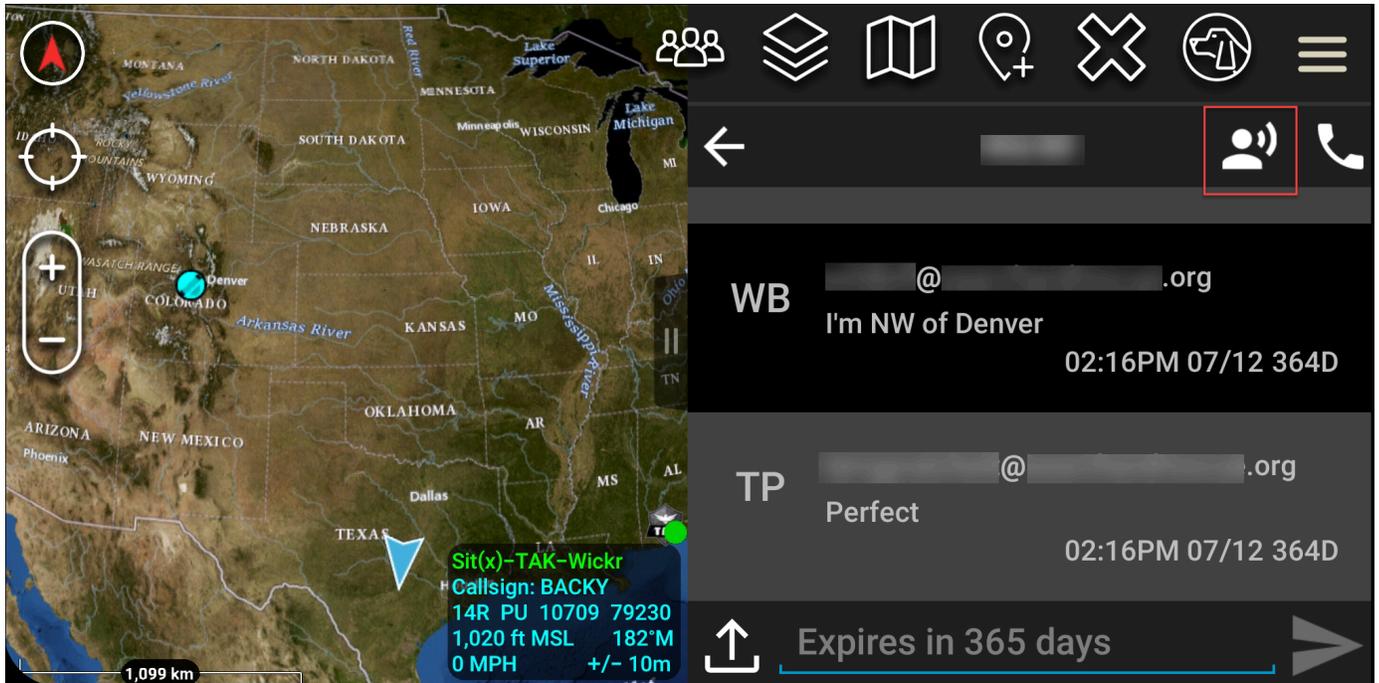
Das Download-Symbol wird angezeigt und zeigt an, dass die ausgewählte Datei heruntergeladen wird.

## Senden einer sicheren Sprachnachricht (Push-to-talk)

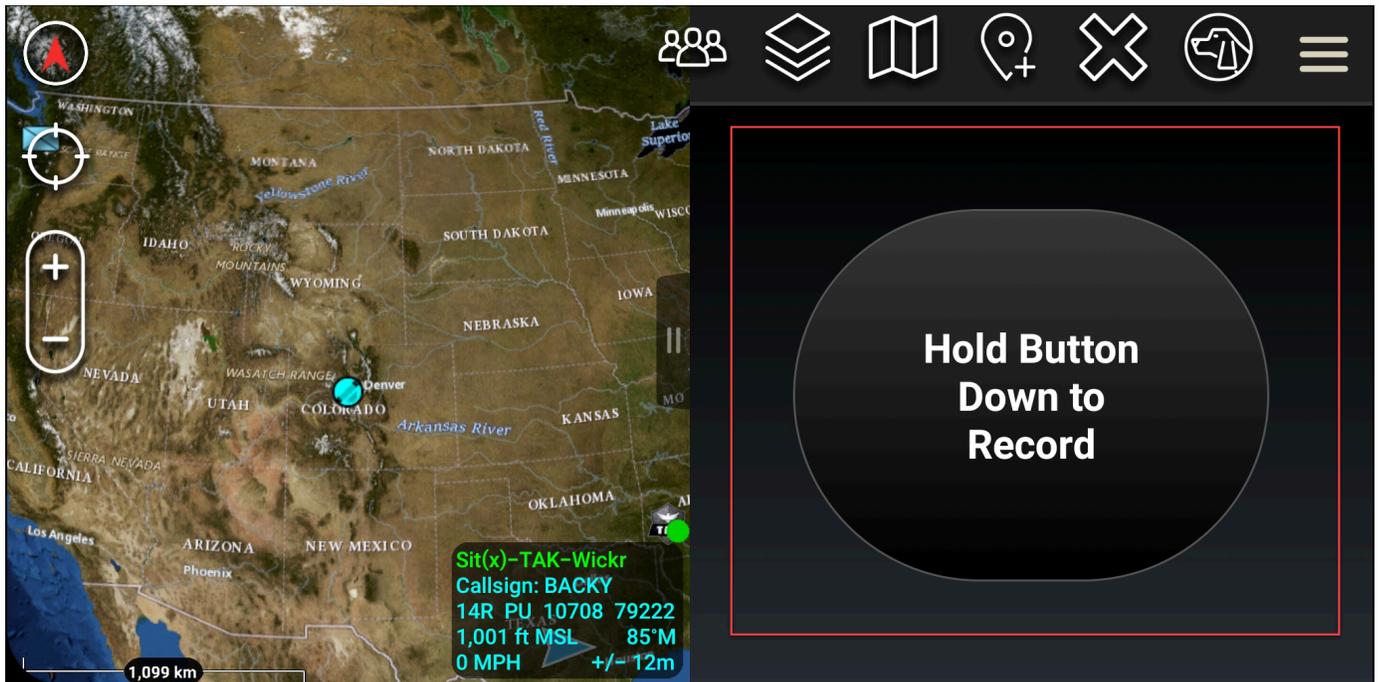
Sie können eine sichere Sprachnachricht (Push-to-talk) im Wickr-Plugin für ATAK senden.

Führen Sie das folgende Verfahren aus, um eine sichere Sprachnachricht zu senden.

1. Öffnen Sie ein Chat-Fenster.
2. Wählen Sie oben auf dem Bildschirm das Push-to-Talk-Symbol aus, das durch ein Symbol einer Person angezeigt wird, die spricht.



3. Wählen und halten Sie die Schaltfläche Halten nach unten zum Aufzeichnen.



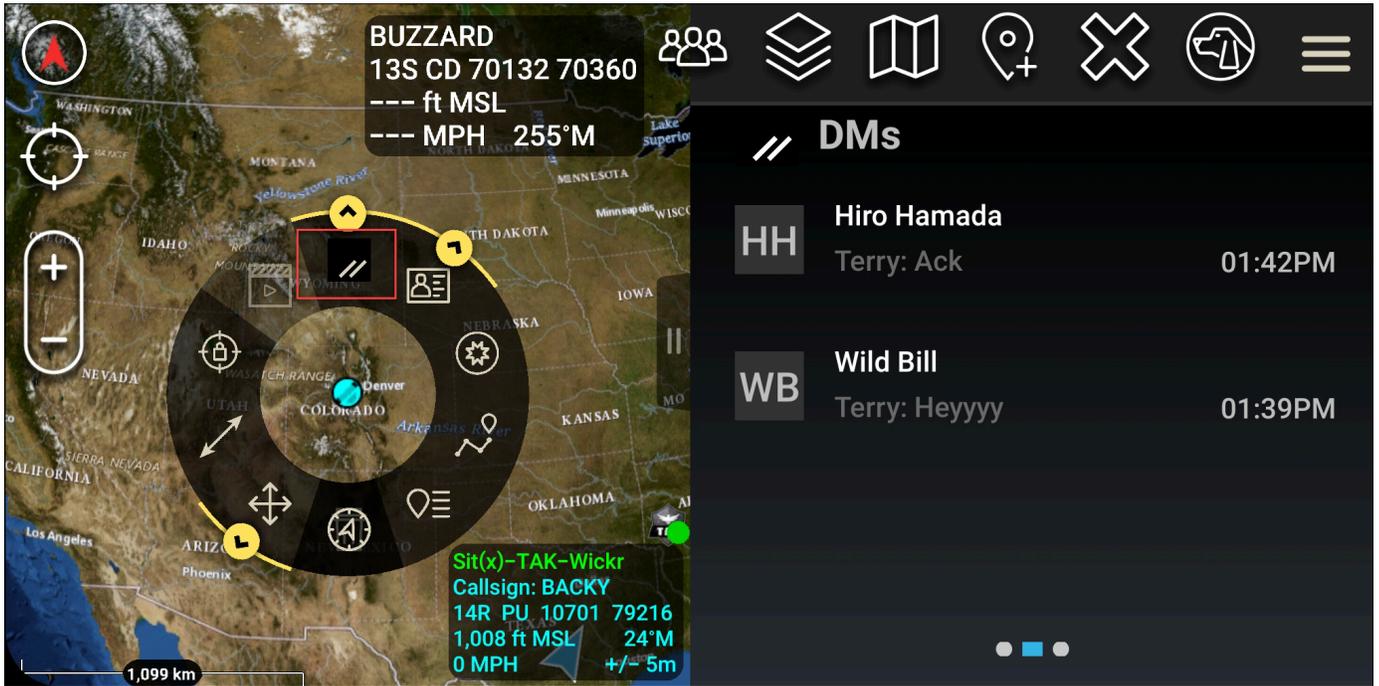
4. Notieren Sie Ihre Nachricht.
5. Nachdem Sie Ihre Nachricht aufgezeichnet haben, lassen Sie die zu sendende Schaltfläche los.

## Pinwheel (Quick Access)

Das Pinwheel- oder Quick-Access-Feature wird für one-one-one Gespräche oder direkte Nachrichten verwendet.

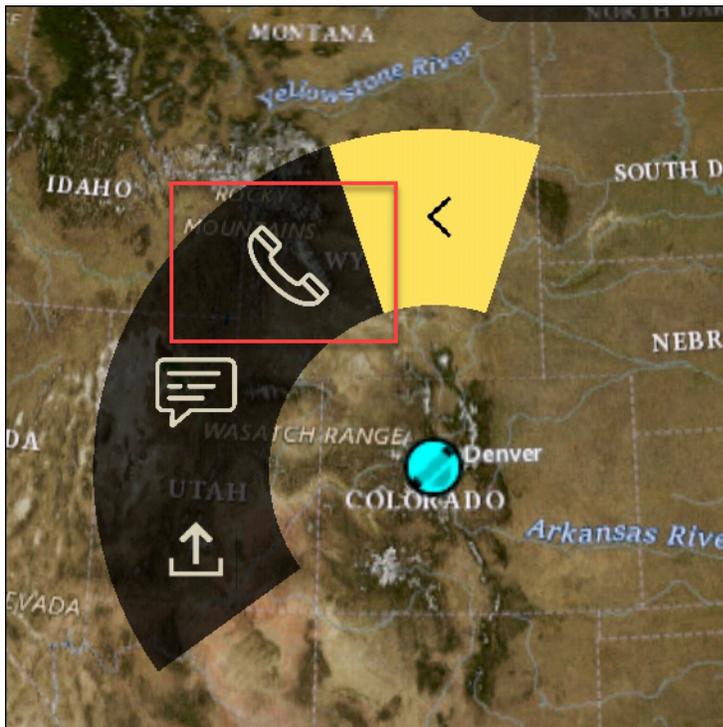
Führen Sie das folgende Verfahren aus, um das Pinwheel zu verwenden.

1. Öffnen Sie gleichzeitig die geteilte Bildschirmansicht der ATAK-Map und des Plugins Wickr für ATAK. Die Karte zeigt Ihre Teammitglieder oder Ressourcen in der Kartenansicht an.
2. Wählen Sie das Benutzersymbol, um das Pinwheel zu öffnen.
3. Wählen Sie das Wickr-Symbol, um die verfügbaren Optionen für den ausgewählten Benutzer anzuzeigen.



4. Wählen Sie auf dem Pinwheel eines der folgenden Symbole aus:

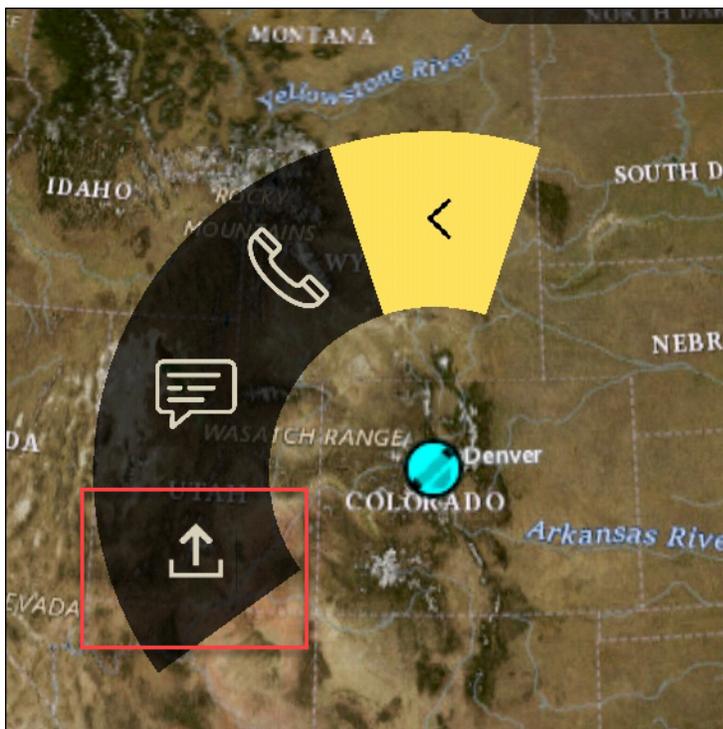
- Telefon : Wählen Sie zum Aufrufen aus.



- Nachricht : Wählen Sie zum Chatten.



- Datei senden: Wählen Sie , um eine Datei zu senden.



## Navigation

Die Plugin-Benutzeroberfläche enthält drei Plugin-Ansichten, die durch die blauen und blauen Formen unten rechts auf dem Bildschirm angezeigt werden. Swipe nach links und rechts, um zwischen den Ansichten zu navigieren.

- Ansicht „Kontakte“: Erstellen einer direkten Nachrichtengruppe oder einer Chatroom-Konversation.
- DMs-Ansicht: Erstellen Sie eine one-to-one Konversation. Die Chat-Funktionalität funktioniert wie in der nativen Wickr-App. Mit dieser Funktion können Sie in der Kartenansicht bleiben und mit anderen im Plugin kommunizieren.
- Raumansicht: Die vorhandenen Räume in der nativen App werden portiert. Alles, was im Plugin gemacht wird, spiegelt 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 Ports und Domänen, die zugelassen werden sollen

Um sicherzustellen, dass Wickr ordnungsgemäß funktioniert, können Sie die folgenden Ports und Domänen auflisten:

### Ports

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

### Regionale Domänen

- Europa (Frankfurt): `api.messaging.wickr.eu-central-1.amazonaws.com`
- USA Ost (Nord-Virginia): `gw-pro-prod.wickr.com`, `api.messaging.wickr.us-east-1.amazonaws.com`
- Europa (London): `api.messaging.wickr.eu-west-2.amazonaws.com`
- Asien-Pazifik (Sydney): `api.messaging.wickr.ap-southeast-2.amazonaws.com`

- Kanada (Zentral): `api.messaging.wickr.ca-central-1.amazonaws.com`
- AWS GovCloud (US-West): `api.messaging.wickr.us-gov-west-1.amazonaws.com`

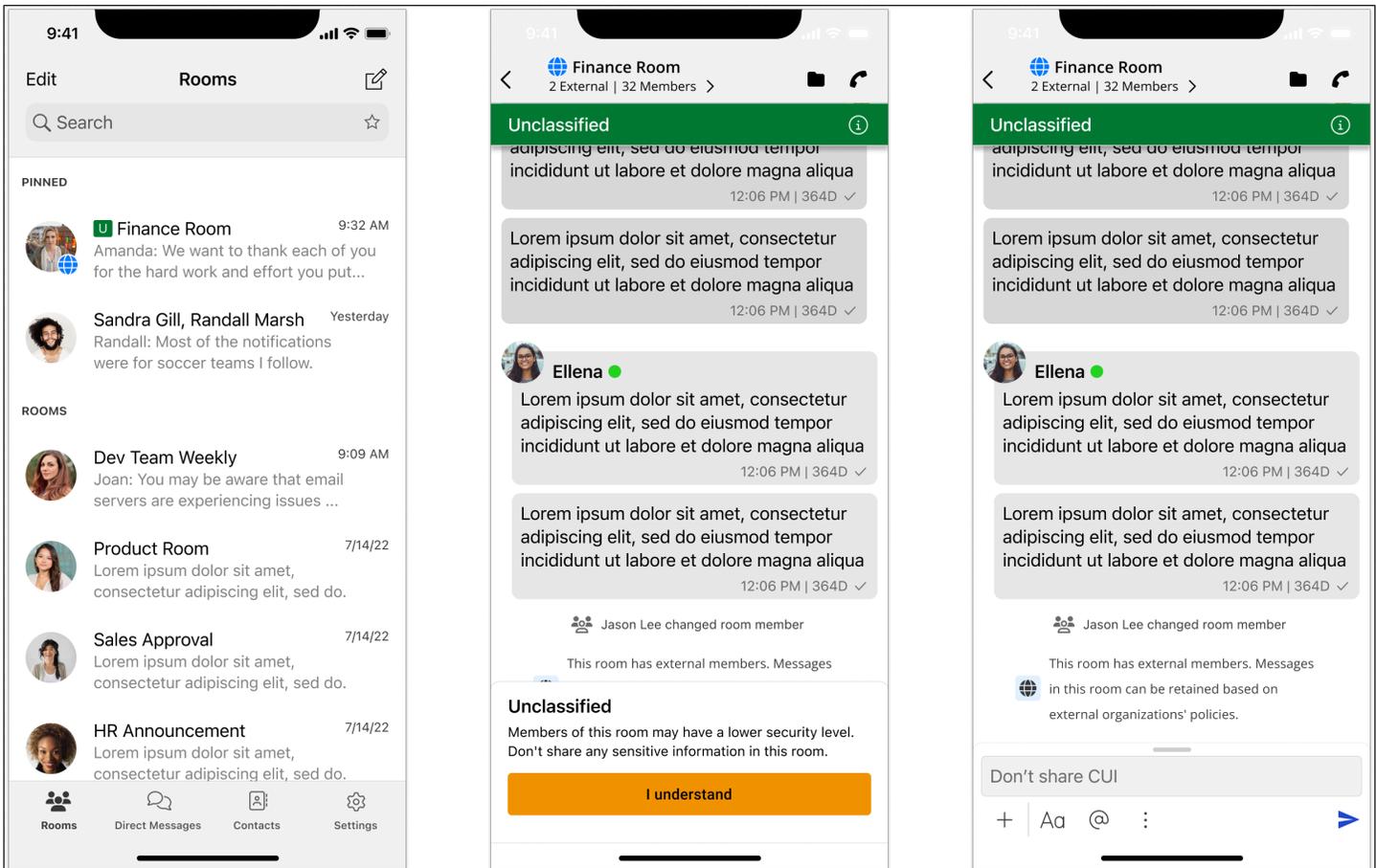
Registrierungs- und Bestätigungs-E-Mails werden von `donotreply@wickr.email` gesendet.

Wenn Sie die Liste aller möglichen IP-Adressen der aufrufenden Server zulassen möchten, müssen Sie die [AllowlistWickr.txt-Datei](#) mit möglichen CIDRs herunterladen und sie regelmäßig überprüfen, da sie sich ändern kann.

## 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 strenge Richtlinien zur behördlich festgelegten Klassifizierung einhalten. 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.

# Benutzer in AWS Wickr verwalten

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

Themen

- [Team-Verzeichnis](#)
- [Gastnutzer](#)

## Team-Verzeichnis

Sie können aktuelle Wickr-Benutzer anzeigen und ihre Details im Benutzerbereich von AWS Management Console for Wickr ändern.

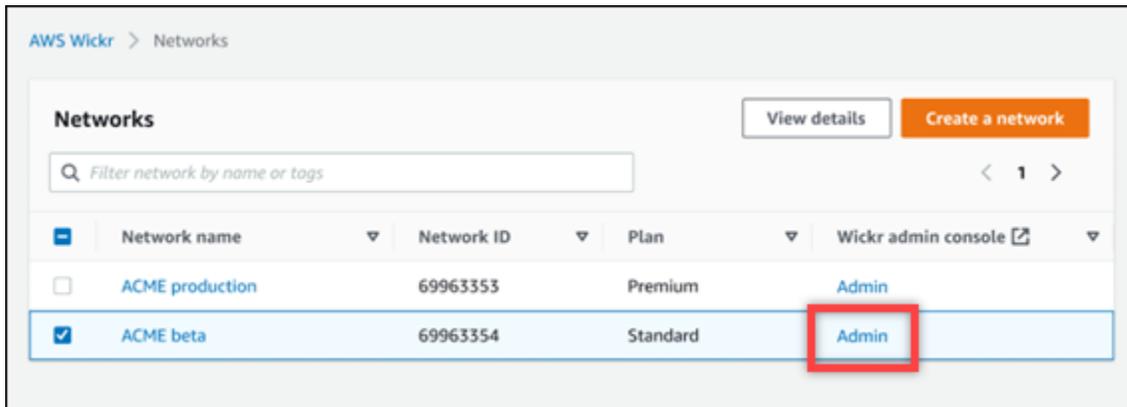
Themen

- [Anzeigen von Benutzern](#)
- [Benutzer erstellen](#)
- [Benutzer bearbeiten](#)
- [Löschen von Benutzern](#)
- [Benutzer auf einmal löschen](#)
- [Benutzer massenweise sperren](#)

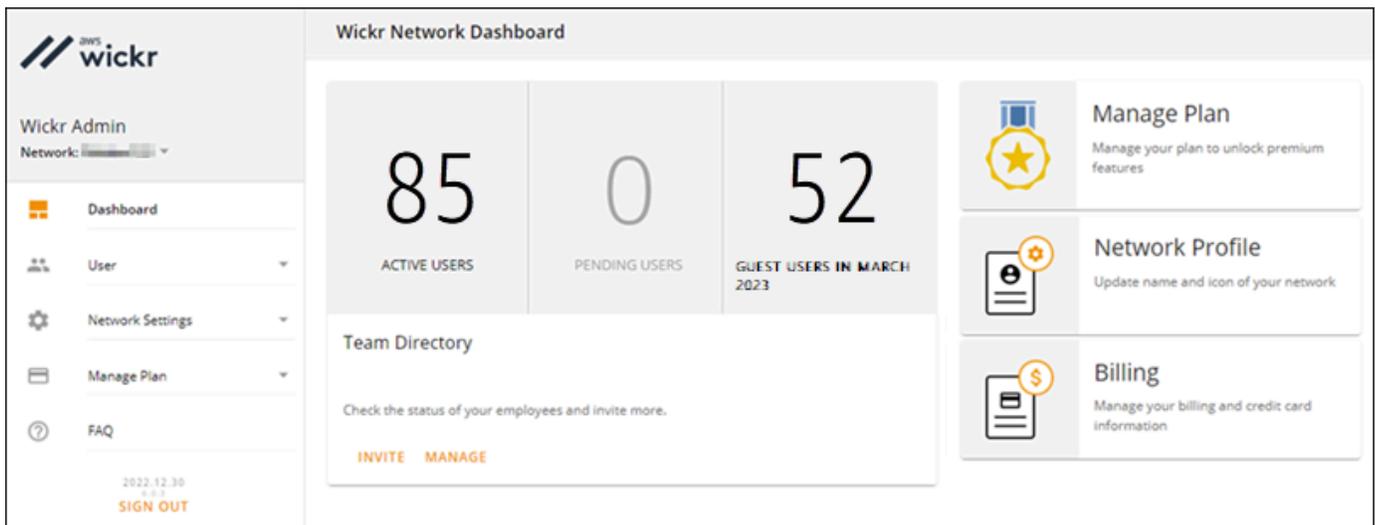
## Anzeigen von Benutzern

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

1. [Öffnen Sie das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/.](https://console.aws.amazon.com/wickr/)
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu navigieren.



Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.



3. Wählen Sie im Navigationsbereich der Wickr Admin Console Benutzer und dann Teamverzeichnis aus.

Auf der Teamverzeichnis-Seite 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.

## Benutzer erstellen

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

1. Öffnen Sie das AWS Management Console für Wickr unter <https://console.aws.amazon.com/wickr/>.

2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu navigieren.

Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.

3. Wählen Sie im Navigationsbereich der Wickr Admin Console Benutzer und dann Teamverzeichnis aus.
4. Wählen Sie Neuen Benutzer erstellen.
5. Geben Sie in dem daraufhin angezeigten Formular den Vor- und 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. Wickr sendet eine Einladungs-E-Mail an die Adresse, die Sie für den Benutzer angegeben haben.
6. Wählen Sie Erstellen.

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 bearbeiten

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

1. Öffnen Sie das AWS Management Console für Wickr unter <https://console.aws.amazon.com/wickr/>.
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu navigieren.  
  
Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.
3. Wählen Sie im Navigationsbereich der Wickr Admin Console Benutzer und dann Teamverzeichnis aus.
4. Wählen Sie das vertikale Ellipsensymbol neben dem Namen des Benutzers, den Sie löschen möchten.
5. Sie können eine der folgenden Optionen wählen:

- Geräte — Sehen Sie sich die Geräte an, die der Benutzer mit dem Wickr-Client konfiguriert hat.
- Bearbeiten — Bearbeiten Sie die Benutzerdetails wie Name, Landesvorwahl, Telefonnummer (optional) und zugewiesene Sicherheitsgruppe.
- Sperren — Sperren Sie den Benutzer, sodass er sich im Wickr-Client nicht bei Ihrem Wickr-Netzwerk anmelden kann. Wenn Sie einen Benutzer sperren, der derzeit im Client in Ihrem Wickr-Netzwerk angemeldet ist, wird dieser Benutzer automatisch abgemeldet.
- Löschen — Löscht den Benutzer aus Ihrem Wickr-Netzwerk.

## Löschen von Benutzern

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

1. Öffnen Sie das AWS Management Console für Wickr unter <https://console.aws.amazon.com/wickr/>.
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu navigieren.

Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.

3. Wählen Sie im Navigationsbereich der Wickr Admin Console Benutzer und dann Teamverzeichnis aus.
4. Wählen Sie das vertikale Ellipsensymbol neben dem Namen des Benutzers, 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.

## Benutzer auf einmal löschen

Sie können Wickr-Netzwerkbenutzer im Benutzerbereich der Wickr Admin-Konsole für Wickr massenweise löschen und sperren.

 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 Management Console für Wickr unter https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. Wählen Sie im Navigationsbereich der Wickr Admin Console die Option Benutzer und dann Teamverzeichnis aus.

Auf der Teamverzeichnis-Seite werden Benutzer angezeigt, die in Ihrem Wickr-Netzwerk registriert sind.

3. Wählen Sie auf der Seite Teamverzeichnis die Option Benutzer verwalten aus.
4. Wählen Sie im Pop-upfenster „Benutzer verwalten“ die Option „Benutzer löschen“.
5. Laden Sie die CSV-Beispielvorlage herunter. Um die Beispielvorlage herunterzuladen, wählen Sie Vorlage herunterladen.
6. Vervollständigen Sie die Vorlage, indem Sie die E-Mail-Adressen der Benutzer hinzufügen, die Sie massenweise aus Ihrem Netzwerk löschen möchten.
7. Laden Sie die fertige CSV-Vorlage hoch. Sie können die Datei per Drag & Drop in das Upload-Feld ziehen oder eine Datei auswählen.
8. Aktivieren Sie das Kontrollkästchen. Ich bestätige, dass das Löschen eines Benutzers nicht rückgängig gemacht werden kann.
9. 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 die AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. Wählen Sie im Navigationsbereich der Wickr Admin Console die Option Benutzer und dann Teamverzeichnis aus.

Auf der Teamverzeichnis-Seite werden Benutzer angezeigt, die in Ihrem Wickr-Netzwerk registriert sind.

3. Wählen Sie in der oberen rechten Ecke der Teamverzeichnis-Seite das CSV-Download-Symbol aus.
4. Nachdem Sie die CSV-Vorlage für das Teamverzeichnis heruntergeladen haben, entfernen Sie die Zeilen mit Benutzern, die nicht gelöscht werden müssen.
5. Wählen Sie auf der Seite Teamverzeichnis die Option Benutzer verwalten aus.
6. Wählen Sie im Pop-up-Fenster „Benutzer verwalten“ die Option „Benutzer löschen“.
7. Laden Sie die CSV-Vorlage für das Teamverzeichnis hoch. Sie können die Datei per Drag & Drop in das Upload-Feld ziehen oder eine Datei auswählen.
8. Aktivieren Sie das Kontrollkästchen. Ich bestätige, dass das Löschen eines Benutzers nicht rückgängig gemacht werden kann.
9. 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 massenweise sperren

Sie können Wickr-Netzwerkbenutzer im Benutzerbereich der Wickr Admin Console für 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 Management Console für Wickr unter https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. Wählen Sie im Navigationsbereich der Wickr Admin Console die Option Benutzer und dann Teamverzeichnis aus.

Auf der Teamverzeichnis-Seite werden Benutzer angezeigt, die in Ihrem Wickr-Netzwerk registriert sind.

3. Wählen Sie auf der Seite Teamverzeichnis die Option Benutzer verwalten aus.
4. Wählen Sie im Popupfenster „Benutzer verwalten“ die Option „Benutzer sperren“.
5. Laden Sie die CSV-Beispielvorlage herunter. Um die Beispielvorlage herunterzuladen, wählen Sie Vorlage herunterladen.
6. Vervollständigen Sie die Vorlage, indem Sie die E-Mail-Adressen der Benutzer hinzufügen, die Sie massenweise von Ihrem Netzwerk sperren möchten.
7. Laden Sie die fertige CSV-Vorlage hoch. Sie können die Datei per Drag & Drop in das Upload-Feld ziehen oder eine Datei auswählen.
8. Nachdem Sie die CSV-Datei hochgeladen haben, 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.

## Gastnutzer

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 auf der Seite Sicherheitsgruppe der Wickr-Administrationskonsole 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

Gastbenutzerfunktion 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](#).

## Themen

- [Aktivieren oder deaktivieren Sie Gastbenutzer](#)
- [Anzahl der Gastbenutzer anzeigen](#)
- [Monatliche Nutzung anzeigen](#)
- [Gastbenutzer anzeigen](#)
- [Blockieren Sie einen Gastbenutzer](#)

## Aktivieren oder deaktivieren Sie Gastbenutzer

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

1. [Öffnen Sie das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu navigieren.

Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet.

3. Wählen Sie im Navigationsbereich der Wickr Admin Console Netzwerkeinstellungen und dann Sicherheitsgruppe.
4. Wählen Sie Details für eine bestimmte Sicherheitsgruppe.

### 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 auf der Seite mit den Sicherheitsgruppendedetails die Registerkarte Federation.
6. Es gibt zwei Bereiche, an denen der Schalter zum Zulassen von Gastbenutzern verfügbar sein wird:
  - Lokaler Verband — Wählen Sie für Netzwerke im Osten der USA (Nord-Virginia) neben dem Abschnitt Lokaler Verband der Seite die Option Bearbeiten aus.

- Globaler Verband — Wählen Sie für alle anderen Netzwerke in anderen Regionen neben dem Bereich Globaler Verband der Seite die Option Bearbeiten aus.
7. Wählen Sie Gastbenutzern erlauben, Gastbenutzer für die Sicherheitsgruppe zu aktivieren, oder deaktivieren Sie die Option, um sie zu deaktivieren.
  8. Wählen Sie Speichern, um die Änderung zu speichern und sie für die Sicherheitsgruppe wirksam zu machen.

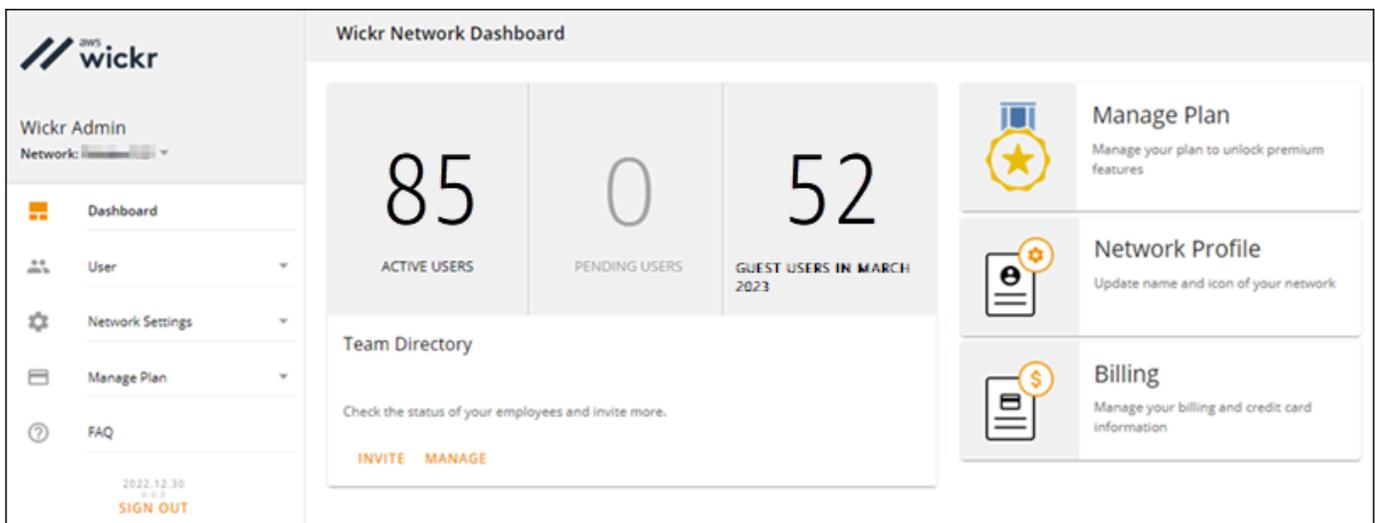
Registrierte Benutzer in der spezifischen Sicherheitsgruppe in Ihrem Wickr-Netzwerk können jetzt mit Gastbenutzern interagieren. Weitere Informationen finden Sie unter [Gastbenutzer](#) im Wickr-Benutzerhandbuch.

## Anzahl der Gastbenutzer anzeigen

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

1. [Öffnen Sie das AWS Management Console für Wickr unter https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu gelangen.

Sie werden zur Wickr Admin Console für ein bestimmtes Netzwerk weitergeleitet. Auf der Dashboard-Seite wird die Anzahl der Gastbenutzer in Ihrem Wickr-Netzwerk angezeigt, wie im folgenden Beispiel gezeigt.



The screenshot displays the 'Wickr Network Dashboard' interface. On the left is a navigation sidebar with the 'Wickr Admin' header and a 'Network:' dropdown. The sidebar menu includes 'Dashboard', 'User', 'Network Settings', 'Manage Plan', and 'FAQ'. At the bottom of the sidebar, it shows the time '2022.12.30 4:13' and a 'SIGN OUT' button. The main dashboard area features three large metric cards: '85 ACTIVE USERS', '0 PENDING USERS', and '52 GUEST USERS IN MARCH 2023'. Below these is a 'Team Directory' section with the text 'Check the status of your employees and invite more.' and 'INVITE' and 'MANAGE' buttons. On the right side, there are three management cards: 'Manage Plan' (with a star icon), 'Network Profile' (with a gear icon), and 'Billing' (with a dollar sign icon).

## Monatliche Nutzung 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 einzusehen.

1. Öffnen Sie das AWS Management Console für Wickr unter <https://console.aws.amazon.com/wickr/>.
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu gelangen.
3. Wählen Sie im Navigationsbereich der Wickr Admin Console Benutzer und dann Gastbenutzer aus.
4. Wählen Sie auf der Seite Gastbenutzer den Abschnitt Monatliche Nutzung aus.

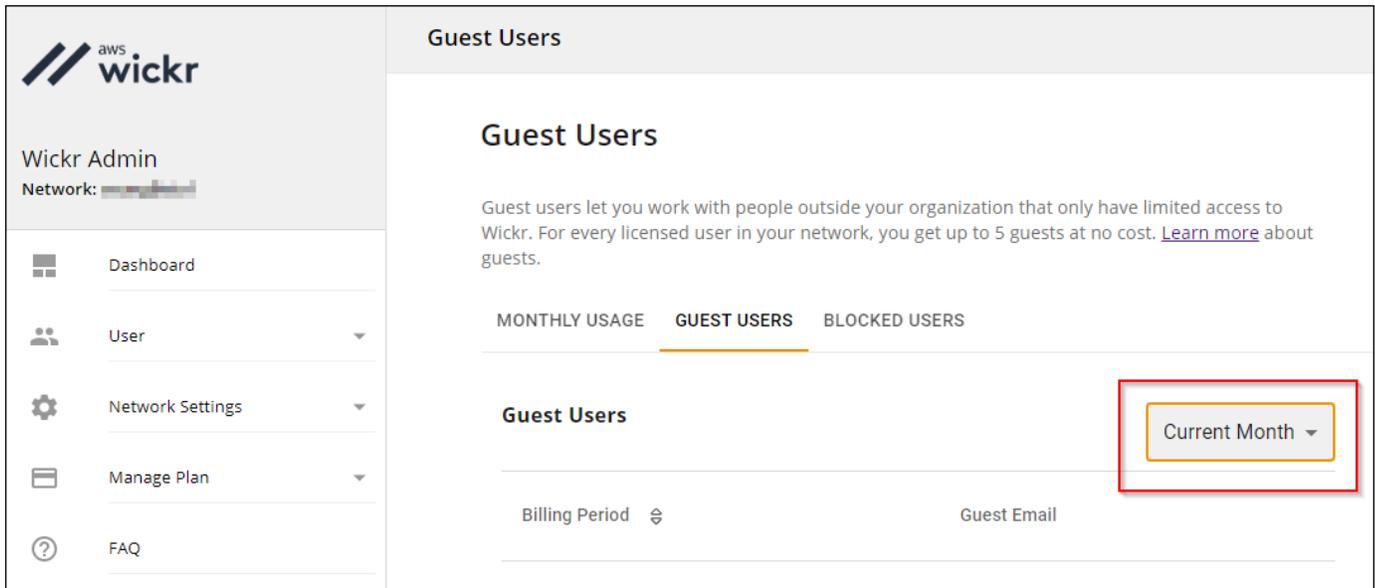
### Note

Die Rechnungsdaten für Gäste werden alle 24 Stunden aktualisiert.

## Gastbenutzer anzeigen

Sie können eine Liste der Gastbenutzer anzeigen, mit denen ein Netzwerkbenutzer während eines bestimmten Abrechnungszeitraums kommuniziert hat. Gehen Sie wie folgt vor, um Ihre Gastbenutzer anzuzeigen.

1. Öffnen Sie das AWS Management Console für Wickr unter <https://console.aws.amazon.com/wickr/>.
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu gelangen.
3. Wählen Sie im Navigationsbereich der Wickr Admin Console Benutzer und dann Gastbenutzer aus.
4. Wählen Sie auf der Seite Gastbenutzer den Abschnitt Gastbenutzer aus.
5. Um Gastbenutzer für einen bestimmten Monat anzuzeigen, wählen Sie den entsprechenden Monat aus dem Drop-down-Menü aus.



## Blockieren Sie einen Gastbenutzer

Blockierte Benutzer können mit niemandem in Ihrem Netzwerk kommunizieren.

Um einen Gastbenutzer zu blockieren

1. Öffnen Sie das AWS Management Console für Wickr unter <https://console.aws.amazon.com/wickr/>.
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu gelangen.
3. Wählen Sie im Navigationsbereich der Wickr Admin Console Benutzer und dann Gastbenutzer aus.
4. Wählen Sie auf der Seite Gastbenutzer den Abschnitt Gastbenutzer aus.
5. Im Bereich Gastbenutzer werden die Gastbenutzer angezeigt, die in Ihrem Wickr-Netzwerk kommuniziert haben.
6. Suchen Sie im Bereich Gastbenutzer nach der E-Mail-Adresse des Gastbenutzers, den Sie blockieren möchten.
7. Wählen Sie auf der rechten Seite neben dem Namen des Gastbenutzers die drei Punkte aus und wählen Sie Blockieren aus.
8. Wählen Sie im Popup-Fenster Blockieren aus.
9. Um die Liste der blockierten Benutzer in Ihrem Wickr-Netzwerk anzuzeigen, wählen Sie den Abschnitt Blockierte Benutzer.

## Um einen Gastbenutzer zu entsperren

1. Öffnen Sie das AWS Management Console für Wickr unter <https://console.aws.amazon.com/wickr/>.
2. Wählen Sie auf der Seite Netzwerke den Link Admin, um zur Wickr Admin Console für dieses Netzwerk zu gelangen.
3. Wählen Sie im Navigationsbereich der Wickr Admin Console Benutzer und dann Gastbenutzer aus.
4. Wählen Sie auf der Seite Gastbenutzer den Abschnitt Blockierte Benutzer aus.
5. Im Abschnitt Blockierte Benutzer werden die Gastbenutzer angezeigt, die in Ihrem Wickr-Netzwerk blockiert sind.
6. Suchen Sie im Abschnitt Blockierte Benutzer 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 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 selbst 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. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe 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 [AWS Services 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. Die folgenden Themen zeigen Ihnen, 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.

## Themen

- [Datenschutz in AWS Wickr](#)
- [Identitäts- und Zugriffsmanagement für AWS Wickr](#)
- [Compliance-Validierung](#)
- [Resilienz in AWS Wickr](#)
- [Infrastruktursicherheit in AWS Wickr](#)
- [Konfiguration und Schwachstellenanalyse in AWS Wickr](#)
- [Bewährte Sicherheitsmethoden für AWS Wickr](#)

# 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](#). Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag [AWS -Modell der geteilten Verantwortung und in der DSGVO](#) im AWS - Sicherheitsblog.

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).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-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 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter [Federal Information Processing Standard \(FIPS\) 140-2](#).

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 Administrator AWS-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 Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

## Themen

- [Zielgruppe](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)
- [AWS verwaltete Richtlinien für AWS Wickr](#)
- [So funktioniert AWS Wickr mit IAM](#)
- [Beispiele für identitätsbasierte Richtlinien für AWS Wickr](#)
- [Fehlerbehebung bei Identität und Zugriff auf AWS Wickr](#)

## Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Wickr ausführen.

**Dienstbenutzer** — Wenn Sie den Wickr-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Wenn Sie für Ihre Arbeit mehr Wickr-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Wenn Sie in Wickr nicht auf eine Funktion zugreifen können, finden Sie weitere Informationen unter [Fehlerbehebung bei Identität und Zugriff auf AWS Wickr](#)

**Serviceadministrator** — Wenn Sie in Ihrem Unternehmen für die Wickr-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Wickr. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen von Wickr Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM

nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit Wickr nutzen kann, finden Sie unter [So funktioniert AWS Wickr mit IAM](#)

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Wickr zu verwalten. Beispiele für identitätsbasierte Wickr-Richtlinien, die Sie in IAM verwenden können, finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Wickr](#)

## Authentifizierung mit Identitäten

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

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter [So melden Sie sich bei Ihrem an AWS-Konto](#) im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu signieren, finden Sie im [IAM-Benutzerhandbuch unter AWS API-Anfragen](#) signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter [Multi-Faktor-Authentifizierung](#) im AWS IAM Identity Center - Benutzerhandbuch und [Verwenden der Multi-Faktor-Authentifizierung \(MFA\) in AWS](#) im IAM-Benutzerhandbuch.

## AWS-Konto Root-Benutzer

Wenn Sie ein AWS-Konto erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter [Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

## Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter [Was ist IAM Identity Center?](#) im AWS IAM Identity Center - Benutzerhandbuch.

## IAM-Benutzer und -Gruppen

Ein [IAM-Benutzer](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto, die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter [Regelmäßiges](#)

[Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Eine [IAM-Gruppe](#) ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter [Erstellen eines IAM-Benutzers \(anstatt einer Rolle\)](#) im IAM-Benutzerhandbuch.

## IAM-Rollen

Eine [IAM-Rolle](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto, die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen [wechseln](#). Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter [Verwenden von IAM-Rollen](#) im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- **Verbundbenutzerzugriff** – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter [Erstellen von Rollen für externe Identitätsanbieter](#) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter [Berechtigungssätze](#) im AWS IAM Identity Center -Benutzerhandbuch.
- **Temporäre IAM-Benutzerberechtigungen** – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.

- **Kontoübergreifender Zugriff** – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zum Unterschied zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch](#).
- **Serviceübergreifender Zugriff** — Einige verwenden Funktionen in anderen. AWS-Services AWS-Services Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
- **Forward Access Sessions (FAS)** — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).
- **Servicerolle** – Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service übernimmt, 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.
- **Dienstbezogene Rolle** — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene 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.
- **Auf Amazon EC2 ausgeführte Anwendungen** — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie

ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter [Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden](#) im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter [Erstellen einer IAM-Rolle \(anstatt eines Benutzers\)](#) im IAM-Benutzerhandbuch.

## Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter [Übersicht über JSON-Richtlinien](#) im IAM-Benutzerhandbuch.

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

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

## Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. 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 [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter [Auswahl zwischen verwalteten und eingebundenen Richtlinien](#) im IAM-Benutzerhandbuch.

## Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. 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

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. 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

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- **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 resultierenden Berechtigungen sind eine Schnittmenge der identitätsbasierten Richtlinien der Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. 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 mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter [Bewertungslogik für Richtlinien](#).

## AWS verwaltete 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 [AWS Verwaltete Richtlinien](#).

AWS-Services verwalten 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.

### AWS verwaltete Richtlinie: AWSWickrFullAccess

Sie können die `AWSWickrFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt dem Wickr-Dienst volle Administratorrechte, einschließlich der AWS Management Console für Wickr in der AWS Management Console. 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.

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

## Wickr aktualisiert verwaltete Richtlinien AWS

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Wickr an, 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.

Änderung	Beschreibung	Datum
<a href="#">AWSWickrFullAccess</a> – Neue Richtlinie.	Wickr hat eine neue Richtlinie hinzugefügt, die dem Wickr-Dienst vollständige Administratorrechte gewährt, einschließlich der Wickr-Administratorkonsole in der. AWS Management Console	28. November 2022
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
<a href="#">Identitätsbasierte Richtlinien</a>	Ja
<a href="#">Ressourcenbasierte Richtlinien</a>	Nein
<a href="#">Richtlinienaktionen</a>	Ja
<a href="#">Richtlinienressourcen</a>	Nein

IAM-Feature	Wickr-Unterstützung
<a href="#">Bedingungsschlüssel für die Richtlinie</a>	Nein
<a href="#">ACLs</a>	Nein
<a href="#">ABAC (Tags in Richtlinien)</a>	Nein
<a href="#">Temporäre Anmeldeinformationen</a>	Nein
<a href="#">Hauptberechtigungen</a>	Nein
<a href="#">Servicerollen</a>	Nein
<a href="#">Serviceverknüpfte Rollen</a>	Nein

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

## Identitätsbasierte Richtlinien für Wickr

Unterstützt Richtlinien auf Identitätsbasis. Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. 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 [Erstellen von IAM-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. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der [IAM-Referenz für JSON-Richtlinienelemente](#) im IAM-Benutzerhandbuch.

## Beispiele für identitätsbasierte Richtlinien für Wickr

Beispiele für identitätsbasierte Wickr-Richtlinien finden Sie unter. [Beispiele für identitätsbasierte Richtlinien für AWS Wickr](#)

## Ressourcenbasierte Richtlinien innerhalb von Wickr

Unterstützt ressourcenbasierte Richtlinien	Nein
--	------

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. 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. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos auch der Prinzipalentsität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter [Kontenübergreifender Ressourcenzugriff in IAM](#) im IAM-Benutzerhandbuch.

## Politische Maßnahmen für Wickr

Unterstützt Richtlinienaktionen	Ja
---------------------------------	----

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

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation 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 [Beispiele für identitätsbasierte Richtlinien für AWS Wickr](#)

## Politische Ressourcen für Wickr

Unterstützt Richtlinienressourcen
-----------------------------------

Nein
------

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

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein `Resource` oder ein `NotResource`-Element enthalten.

Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen [Amazon-Ressourcennamen \(ARN\)](#) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, 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 [Beispiele für identitätsbasierte Richtlinien 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 kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition block`) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. 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.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen AND-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, wertet AWS die Bedingung mithilfe einer logischen OR Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter [IAM-Richtlinienelemente: Variablen und Tags](#) im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und dienstspezifische Bedingungsschlüssel. 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 [Beispiele für identitätsbasierte Richtlinien 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
--	------

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute Tags genannt. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungelement 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 [Was ist ABAC?](#) 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
--	------

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services [funktionieren AWS-Services](#), finden Sie im [IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM](#).

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter [Wechseln zu einer Rolle \(Konsole\)](#) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter [Temporäre Sicherheitsanmeldeinformationen in IAM](#).

## Serviceübergreifende Prinzipalberechtigungen für Wickr

Unterstützt Forward Access Sessions (FAS)	Nein
---	------

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).

## Service rollen für Wickr

Unterstützt Service rollen

Nein

Eine Service rolle ist eine [IAM-Rolle](#), die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Service rolle 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

Das Ändern der Berechtigungen für eine Service rolle kann die Funktionalität von Wickr beeinträchtigen. Bearbeiten Sie Service rollen nur, wenn Wickr Sie dazu anleitet.

## Servicebezogene Rollen für Wickr

Unterstützt serviceverknüpfte Rollen

Nein

Eine dienstbezogene Rolle ist eine Art von Service rolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt 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 Service mit einem Yes in der

Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

## Beispiele für identitätsbasierte Richtlinien 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.

```
{
  "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 zu erstellen, anzuzeigen und zu verwalten. AWS Management Console Weitere Informationen zu den Elementen in einer IAM-Richtlinienanweisung finden Sie unter [Identitätsbasierte 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.

### Themen

- [Bewährte Methoden für Richtlinien](#)
- [Verwenden Sie sie für Wickr AWS Management Console](#)
- [Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer](#)

## Bewährte Methoden für Richtlinien

Identitätsbasierte 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.

Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten 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 [AWS -verwaltete Richtlinien](#) oder [AWS -verwaltete Richtlinien für Auftrags-Funktionen](#) 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 werden AWS-Service, z. AWS 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 [Richtlinienvvalidierung zum 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 erfordert AWS-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 [Konfigurieren eines MFA-geschützten API-Zugriffs](#) im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter [Bewährte Methoden für die Sicherheit in IAM](#) im IAM-Benutzerhandbuch.

## Verwenden Sie sie für Wickr AWS Management Console

Hängen Sie die `AWSWickrFullAccess` AWS verwaltete Richtlinie an Ihre IAM-Identitäten an, um ihnen volle Administratorrechte für den Wickr-Dienst zu gewähren, einschließlich der Wickr-Administratorkonsole in der AWS Management Console. Weitere Informationen finden Sie unter [AWS verwaltete 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:ListGroupsWithUser",
        "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

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Wickr und IAM auftreten können.

### Themen

- [Ich bin nicht berechtigt, eine administrative Aktion in der AWS Management Console für Wickr durchzuführen](#)

### Ich bin nicht berechtigt, eine administrative Aktion in der AWS Management Console für Wickr durchzuführen

Wenn Ihnen das AWS Management Console für Wickr mitteilt, dass Sie nicht berechtigt sind, eine Aktion durchzuführen, 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 Management Console for Wickr Wickr-Netzwerke in for Wickr zu erstellen, zu verwalten oder anzuzeigen, aber nicht über die AWS Management Console 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 Management Console for Wickr zugreifen kann.

wickr:CreateAdminSession wickr:ListNetworks Weitere Informationen finden Sie unter [Beispiele für identitätsbasierte Richtlinien für AWS Wickr](#) und [AWS verwaltete Richtlinie: AWSWickrFullAccess](#).

## Compliance-Validierung

Eine Liste der AWS Services im Rahmen bestimmter Compliance-Programme finden Sie unter [AWS Services im Umfang nach Compliance-Programmen AWS](#). Allgemeine Informationen finden Sie unter [AWS Compliance-Programme AWS](#).

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS 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. AWS bietet die folgenden Ressourcen zur Unterstützung bei der Einhaltung von Vorschriften:

- 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
- [AWS Ressourcen 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 Config Entwicklerhandbuch — AWS Config; bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- [AWS Security Hub](#)— Dieser AWS Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus, sodass Sie überprüfen können AWS, 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-Regionen bieten 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 [AWS Globale 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 [Datenaufbewahrung](#).

## Infrastruktursicherheit in AWS Wickr

Als verwalteter Service ist AWS Wickr durch die AWS globalen Netzwerksicherheitsverfahren geschützt, die im Whitepaper [Amazon Web Services: Sicherheitsprozesse 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 [AWS verwaltete Richtlinien für AWS Wickr](#).
- Greifen Sie auf die AWS Management Console für Wickr zu, indem Sie sich bei der ersten authentifizieren. AWS Management Console 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 CloudTrail erfasst 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, von welcher Quell-IP-Adresse aus die Aufrufe 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 integriert, einem ServiceAWS CloudTrail, der die Aktionen eines Benutzers, einer Rolle oder eines -AWSServices in Wickr. CloudTrail captures aller API-Aufrufe für Wickr als Ereignisse aufzeichnet. Zu den erfassten Aufrufen gehören Aufrufe von AWS Management Console für 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-Bucket aktivieren, einschließlich Ereignissen für Wickr. Wenn Sie keinen Trail konfigurieren, können Sie trotzdem die neuesten Ereignisse in der CloudTrail Konsole unter Ereignisverlauf anzeigen. Anhand der von CloudTrail gesammelten Informationen können Sie die an Wickr gestellte Anfrage, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen. Weitere Informationen zu CloudTrail finden Sie im [AWS CloudTrail - Benutzerhandbuch](#).

## Wickr-Informationen in CloudTrail

CloudTrail wird beim Erstellen des Kontos AWS-Konto auf Ihrem aktiviert. Wenn eine Aktivität in Wickr auftritt, wird diese Aktivität in einem - CloudTrail Ereignis zusammen mit anderen - AWSServiceereignissen im Ereignisverlauf aufgezeichnet. Sie können in Ihrem AWS-Konto die neusten Ereignisse anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter [Anzeigen von Ereignissen mit dem CloudTrail Ereignisverlauf](#) .

Erstellen Sie für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich Ereignissen für Wickr, einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von Protokolldateien an einen Amazon S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon-S3-Bucket bereit. Darüber hinaus können Sie andere -AWSServices konfigurieren, um die in den CloudTrail Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie hier:

- [Übersicht zum Erstellen eines Trails](#)
- [CloudTrail Von unterstützte Services und Integrationen](#)
- [Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail](#)
- [Empfangen von CloudTrail Protokolldateien aus mehreren Regionen](#) und [Empfangen von CloudTrail Protokolldateien aus mehreren Konten](#)

Alle Wickr-Aktionen werden von protokolliert CloudTrail. Aufrufe der ListNetworks Aktionen CreateAdminSession, und erzeugen beispielsweise Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Stammbenutzer- oder AWS Identity and Access Management (IAM)-Benutzeranmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer ausgeführt wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter [CloudTrail -Element userIdentity](#).

## Grundlegendes zu Wickr-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Bereitstellung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon 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, das Datum und die Uhrzeit der

Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

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": "abcd980-23c7-4de1-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

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.

So greifen Sie auf das Analyse-Dashboard zu

1. Öffnen Sie das AWS Management Console für Wickr unter <https://console.aws.amazon.com/wickr/>.
2. 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 — Das Diagramm zeigt die Gesamtzahl der im ausgewählten Zeitraum registrierten Benutzer.
  - 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.

# Dokumentverlauf

In der folgenden Tabelle werden die Dokumentationsversionen für Wickr beschrieben.

Änderung	Beschreibung	Datum
<a href="#">Die Lesebestätigungsfunktion ist jetzt verfügbar</a>	Wickr-Administratoren können jetzt die Lesebestätigungsfunktion in der Administratorkonsole aktivieren oder deaktivieren. Weitere Informationen finden Sie unter <a href="#">Lesebestätigungen</a> .	23. April 2024
<a href="#">Global Federation unterstützt jetzt den eingeschränkten Verbund und Administratoren können Nutzungsanalysen in der Administratorkonsole einsehen</a>	Global Federation unterstützt jetzt den eingeschränkten Verbund. Dies funktioniert für Wickr-Netzwerke in anderen AWS-Regionen. Weitere Informationen finden Sie unter <a href="#">Sicherheitsgruppen</a> . Darüber hinaus können Administratoren ihre Nutzungsanalysen jetzt im Analytics-Dashboard in der Admin Console einsehen. Weitere Informationen finden Sie unter <a href="#">Analytics-Dashboard</a> .	28. März 2024
<a href="#">Eine dreimonatige kostenlose Testversion des Premium-Plans von AWS Wickr ist jetzt verfügbar</a>	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, einschlie	9. Februar 2024

ßlich unbegrenzter Administratorkontrollen und Datenspeicherung. Die Funktion für Gastbenutzer ist während der kostenlosen Premium-Testversion nicht verfügbar. Weitere Informationen finden Sie unter [Abonnement verwalten](#).

[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 [Zugriff auf Wickr](#).

26. Oktober 2023

[Wickr-Netzwerke sind jetzt in der Lage, sich 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

<a href="#">Wickr ist jetzt in Europa (London) erhältlich AWS-Region</a>	Wickr ist jetzt in Europa (London) erhältlich. AWS-Region Weitere Informationen finden Sie unter <a href="#">Zugriff auf Wickr</a> .	23. August 2023
<a href="#">Wickr ist jetzt in Kanada (Zentral) verfügbar AWS-Region</a>	Wickr ist jetzt in Kanada (Zentral) erhältlich. AWS-Region Weitere Informationen finden Sie unter <a href="#">Zugreifen auf Wickr</a> .	03. Juli 2023
<a href="#">Die Gastbenutzerfunktion ist jetzt als Vorschau verfügbar</a>	Gastbenutzer können sich beim Wickr-Client anmelden und mit Wickr-Netzwerkbenutzern zusammenarbeiten. Weitere Informationen finden Sie unter <a href="#">Gastbenutzer (Vorschau)</a> .	31. Mai 2023
<a href="#">AWS Wickr ist jetzt in AWS GovCloud (US-West) integriert und jetzt verfügbar als AWS CloudTrail WickrGov</a>	AWS Wickr ist jetzt in integriert AWS CloudTrail. Weitere Informationen finden Sie unter <a href="#">Protokollieren von AWS Wickr-API-Aufrufen mithilfe von AWS CloudTrail</a> . Darüber hinaus ist Wickr jetzt in AWS GovCloud (US-West) als verfügbar. WickrGov Weitere Informationen finden Sie <a href="#">AWS WickrGov</a> 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.

## 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 anderen AWS-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.
- Zusätzliche Preise für Gastbenutzer.
  
- Verbesserungen der Admin-Steuerung
  - Möglichkeit zum Massenlöschen/Sperren von Benutzern.
  - 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 (Zentral) erhältlich. AWS-Region

## Mai 2023

- Verbesserungen
  - Unterstützung für Gastbenutzer hinzugefügt. Weitere Informationen finden Sie unter [Gastnutzer](#).

## März 2023

- Wickr ist jetzt in integriert AWS 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 [AWS WickrGov](#)im AWS GovCloud (US) Benutzerhandbuch.
- Wickr unterstützt jetzt Tagging. Weitere Informationen finden Sie unter [Netzwerk-Tags](#). 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 von ATAK im Wickr Network Dashboard](#).

## Januar 2023

- Single Sign-On (SSO) kann jetzt für alle Tarife konfiguriert werden, einschließlich der kostenlosen Testversion und der Standardversion.

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.