



Guide d'administration

# AWS Wickr



# AWS Wickr: Guide d'administration

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

Les marques et la présentation commerciale d'Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n'est pas d'Amazon, d'une manière susceptible de créer une confusion parmi les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

---

# Table of Contents

Qu'est-ce que AWS Wickr ? .....	1
Caractéristiques de Wickr .....	1
Accès à Wickr .....	3
Tarification .....	3
Documentation pour l'utilisateur final de Wickr .....	3
Configuration .....	4
Inscrivez-vous pour AWS .....	4
Création d'un utilisateur IAM .....	4
Quelle est la prochaine étape .....	6
Premiers pas .....	7
Prérequis .....	7
Étape 1 : Création d'un réseau .....	7
Étape 2 : Configuration de votre réseau .....	9
Étape 3 : créer et inviter des utilisateurs .....	11
Étapes suivantes .....	15
Transférer Wickr Pro vers AWS Wickr .....	15
Étape 1 : créer un AWS compte .....	16
Étape 2 : Récupérez votre identifiant réseau Wickr .....	17
Étape 3 : Soumettre une demande .....	17
Étape 4 : connectez-vous à votre AWS console .....	17
Gérer le réseau .....	19
Profil du réseau .....	19
Afficher le profil du réseau .....	19
Modifier le nom du réseau .....	20
Groupes de sécurité .....	21
Afficher les groupes de sécurité .....	21
Création d'un groupe de sécurité .....	22
Modifier un groupe de sécurité .....	23
Supprimer un groupe de sécurité .....	24
SSOconfiguration .....	25
Afficher les SSO détails .....	25
Configurez SSO .....	26
Période de grâce pour l'actualisation des jetons .....	27
Microsoft Entra (Azure AD) .....	27

Lire les reçus .....	35
Balises réseau .....	36
Gérer les balises réseau .....	36
Ajouter un tag réseau .....	38
Modifier un tag réseau .....	39
Supprimer un tag réseau .....	39
Gérer le plan réseau .....	40
Limitations de l'essai gratuit Premium .....	41
Conservation des données .....	41
Afficher les détails relatifs à la conservation des données .....	42
Configuration de la conservation des données .....	43
Obtenir des journaux .....	55
Mesures et événements relatifs à la conservation des données .....	55
Qu'est-ce qu'ATAK ? .....	61
Activer ATAK .....	62
Informations supplémentaires sur ATAK .....	64
Installation et jumelage .....	64
Composez et recevez un appel .....	68
Envoyer un fichier .....	69
Envoyer un message vocal sécurisé (Push-to-talk) .....	69
Moulinet .....	71
Navigation .....	73
Liste des ports et domaines à autoriser .....	74
Liste des domaines et adresses à autoriser par région .....	74
GovCloud .....	83
Gestion des utilisateurs .....	85
Annuaire des équipes .....	85
Afficher les utilisateurs .....	85
Créer des utilisateurs .....	86
Modifier les utilisateurs .....	87
Suppression d'utilisateurs .....	88
Supprimer des utilisateurs en bloc .....	88
Suspension groupée d'utilisateurs .....	90
Utilisateurs invités .....	91
Activer ou désactiver les utilisateurs invités .....	92
Afficher le nombre d'utilisateurs invités .....	93

Afficher l'utilisation mensuelle .....	93
Afficher les utilisateurs invités .....	94
Bloquer un utilisateur invité .....	95
Sécurité .....	97
Protection des données .....	98
Gestion des identités et des accès .....	99
Public ciblé .....	99
Authentification par des identités .....	100
Gestion des accès à l'aide de politiques .....	104
AWSPolitiques gérées par Wickr .....	106
Comment fonctionne AWS Wickr avec IAM .....	108
Exemples de politiques basées sur l'identité .....	115
Résolution des problèmes .....	118
Validation de conformité .....	119
Résilience .....	120
Sécurité de l'infrastructure .....	120
Analyse de la configuration et des vulnérabilités .....	120
Bonnes pratiques de sécurité .....	120
Surveillance .....	122
CloudTrail journaux .....	122
Informations sur Wickr dans CloudTrail .....	122
Comprendre les entrées du fichier journal Wickr .....	123
.....	130
Historique de la documentation .....	133
Notes de mise à jour .....	137
Juin 2024 .....	137
Avril 2024 .....	137
Mars 2024 .....	137
Février 2024 .....	137
Novembre 2023 .....	138
Octobre 2023 .....	138
Septembre 2023 .....	138
août 2023 .....	139
Juillet 2023 .....	139
Mai 2023 .....	139
Mars 2023 .....	139

---

Février 2023 .....	139
janvier 2023 .....	140
.....	cxli

# Qu'est-ce que AWS Wickr ?

AWSWickr est un service end-to-end crypté qui aide les organisations et les agences gouvernementales à communiquer en toute sécurité par le biais one-to-one de la messagerie de groupe, des appels vocaux et vidéo, du partage de fichiers, du partage d'écran, etc. Wickr peut aider les clients à surmonter les obligations de conservation des données associées aux applications de messagerie grand public et à faciliter la collaboration en toute sécurité. Les contrôles de sécurité et administratifs avancés aident les entreprises à répondre aux exigences légales et réglementaires et à créer des solutions personnalisées pour relever les défis liés à la sécurité des données.

Les informations peuvent être enregistrées dans un magasin de données privé contrôlé par le client à des fins de conservation et d'audit. Les utilisateurs disposent d'un contrôle administratif complet sur les données, notamment en définissant des autorisations, en configurant des options de messagerie éphémère et en définissant des groupes de sécurité. Wickr s'intègre à des services supplémentaires tels qu'Active Directory (AD), l'authentification unique (SSO) avec OpenID Connect (OIDC), etc. Vous pouvez créer et gérer rapidement un réseau Wickr via les AWS Management Console robots Wickr et automatiser en toute sécurité les flux de travail. Consultez [Configuration de AWS Wickr](#) pour démarrer.

## Rubriques

- [Caractéristiques de Wickr](#)
- [Accès à Wickr](#)
- [Tarification](#)
- [Documentation pour l'utilisateur final de Wickr](#)

## Caractéristiques de Wickr

### Sécurité et confidentialité renforcées

Wickr utilise un cryptage 256 bits Advanced Encryption Standard (AES) pour end-to-end chaque fonctionnalité. Les communications sont cryptées localement sur les appareils des utilisateurs et restent indéchiffrables en transit pour toute personne autre que l'expéditeur et le destinataire. Chaque message, appel et fichier est chiffré avec une nouvelle clé aléatoire, et personne d'autre que les destinataires prévus (même pas AWS) ne peut les déchiffrer. Qu'il s'agisse de partager des données sensibles et réglementées, de discuter de questions juridiques ou RH, ou même de mener des

opérations militaires tactiques, les clients utilisent Wickr pour communiquer lorsque la sécurité et la confidentialité sont primordiales.

### Conservation des données

Les fonctionnalités administratives flexibles sont conçues non seulement pour protéger les informations sensibles, mais aussi pour conserver les données conformément aux obligations de conformité, à la conservation légale et à des fins d'audit. Les messages et les fichiers peuvent être archivés dans un magasin de données sécurisé contrôlé par le client.

### Accès flexible

Les utilisateurs disposent d'un accès à plusieurs appareils (mobile, ordinateur de bureau) et peuvent fonctionner dans des environnements à faible bande passante, notamment en cas de déconnexion et out-of-band de communication.

### Contrôles administratifs

Les utilisateurs disposent d'un contrôle administratif complet sur les données, notamment en définissant des autorisations, en configurant des options de messagerie éphémère responsables et en définissant des groupes de sécurité.

### Intégrations et robots puissants

Wickr s'intègre à des services supplémentaires tels qu'Active Directory, l'authentification unique (SSO) avec OpenID Connect (OIDC), etc. Les clients peuvent créer et gérer rapidement un réseau Wickr grâce à Wickr AWS Management Console Bots et automatiser en toute sécurité les flux de travail.

Voici un aperçu des offres de collaboration de Wickr :

- Messagerie individuelle et de groupe : discutez en toute sécurité avec votre équipe dans les salles comptant jusqu'à 500 membres
- Appels audio et vidéo : organisez des conférences téléphoniques avec un maximum de 70 personnes
- Partage d'écran et diffusion : présentez devant un maximum de 500 participants
- Partage et sauvegarde de fichiers : transférez jusqu'à 5 fichiers GBs avec un stockage illimité
- Éphémère : contrôlez l'expiration et les délais burn-on-read
- Fédération mondiale : connectez-vous aux utilisateurs de Wickr en dehors de votre réseau

**Note**

Les réseaux Wickr en AWS GovCloud (US-West) peuvent être fédérés uniquement avec d'autres réseaux Wickr en (US-West). AWS GovCloud

## Accès à Wickr

Wickr est disponible dans l'est des États-Unis (Virginie du Nord), au Canada (centre), en Europe (Londres), en Asie-Pacifique (Sydney), en Europe (Francfort), en Europe (Stockholm), en Europe (Zurich), en Asie-Pacifique (Singapour) et en Asie-Pacifique (Tokyo) Régions AWS. Wickr est également disponible aux WickrGov États-Unis AWS GovCloud (ouest des États-Unis). Région AWS

Les administrateurs accèdent au AWS Management Console for Wickr à l'adresse <https://console.aws.amazon.com/wickr/>. Avant de commencer à utiliser Wickr, vous devez suivre les [Commencer à utiliser AWS Wickr](#) guides [Configuration de AWS Wickr](#) et.

**Note**

Le service Wickr ne possède pas d'interface de programmation d'applications (API).

Les utilisateurs finaux accèdent à Wickr via le client Wickr. Pour plus d'informations, consultez le [guide de l'utilisateur de AWS Wickr](#).

## Tarifcation

Wickr est disponible en différents forfaits pour les particuliers, les petites équipes et les grandes entreprises. Pour plus d'informations, consultez la section [Tarifcation de AWS Wickr](#).

## Documentation pour l'utilisateur final de Wickr

Si vous êtes un utilisateur final du client Wickr et que vous avez besoin d'accéder à sa documentation, consultez le guide de l'[utilisateur de AWS Wickr](#).

# Configuration de AWS Wickr

Si vous êtes un nouveau AWS client, remplissez les conditions d'installation répertoriées sur cette page avant de commencer à utiliser AWS Wickr. Pour ces procédures de configuration, vous utilisez AWS Identity and Access Management (IAM) service. Pour obtenir des informations complètes IAM, consultez le [guide de IAM l'utilisateur](#).

## Rubriques

- [Inscrivez-vous pour AWS](#)
- [Création d'un utilisateur IAM](#)
- [Quelle est la prochaine étape](#)

## Inscrivez-vous pour AWS

Si vous n'avez pas de Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez l'<https://portal.aws.amazon.com/billing/inscription>.
2. Suivez les instructions en ligne.

Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWS est créé. L'utilisateur root a accès à tous Services AWS et les ressources du compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les [tâches nécessitant un accès utilisateur racine](#).

## Création d'un utilisateur IAM

Afin de créer un utilisateur administrateur, choisissez l'une des options suivantes :

Choisissez un moyen de gérer votre administrateur	Pour	Par	Vous pouvez également
<p>Dans IAM Identity Center</p> <p>(Recommandé)</p>	<p>Utilisez des informations d'identification à court terme pour accéder AWS.</p> <p>Telles sont les meilleures pratiques en matière de sécurité. Pour plus d'informations sur les meilleures pratiques, consultez <a href="#">la section Bonnes pratiques en matière de sécurité IAM</a> dans le guide de IAM l'utilisateur.</p>	<p>En suivant les instructions de la <a href="#">section Mise en route</a> dans le AWS IAM Identity Center Guide de l'utilisateur.</p>	<p>Configurez l'accès par programmation en <a href="#">configurant le AWS CLI à utiliser AWS IAM Identity Center</a> dans le .AWS Command Line Interface Guide de l'utilisateur.</p>
<p>Dans IAM</p> <p>(Non recommandé)</p>	<p>Utilisez des informations d'identification à long terme pour accéder AWS.</p>	<p>Suivez les instructions de la section <a href="#">Création de votre premier utilisateur IAM administrateur et de votre premier groupe d'utilisateurs</a> dans le guide de IAM l'utilisateur.</p>	<p>Configurez l'accès par programmation en <a href="#">gérant les clés d'accès pour IAM les utilisateurs</a> dans le guide de IAM l'utilisateur.</p>

 Note

Vous pouvez également attribuer la politique `AWSWickrFullAccess` gérée pour accorder une autorisation administrative complète au service Wickr. Pour de plus amples informations, veuillez consulter [AWS politique gérée : AWSWickrFullAccess](#).

## Quelle est la prochaine étape

Vous avez effectué les étapes de configuration préalables. Pour commencer à configurer Wickr, consultez [Premiers pas](#).

# Commencer à utiliser AWS Wickr

Dans ce guide, nous vous montrons comment démarrer avec Wickr en créant un réseau, en configurant votre réseau et en créant des utilisateurs.

## Rubriques

- [Prérequis](#)
- [Étape 1 : Création d'un réseau](#)
- [Étape 2 : Configuration de votre réseau](#)
- [Étape 3 : créer et inviter des utilisateurs](#)
- [Étapes suivantes](#)
- [Transférer Wickr Pro vers AWS Wickr](#)

## Prérequis

Avant de commencer, assurez-vous de remplir les conditions préalables suivantes si ce n'est déjà fait :

- Inscrivez-vous à Amazon Web Services (AWS). Pour de plus amples informations, veuillez consulter [Configuration de AWS Wickr](#).
- Assurez-vous de disposer des autorisations requises pour administrer Wickr. Pour de plus amples informations, veuillez consulter [AWS politique gérée : AWSWickrFullAccess](#).
- Assurez-vous d'autoriser la liste des ports et domaines appropriés pour Wickr. Pour de plus amples informations, veuillez consulter [Liste des ports et domaines à autoriser](#).

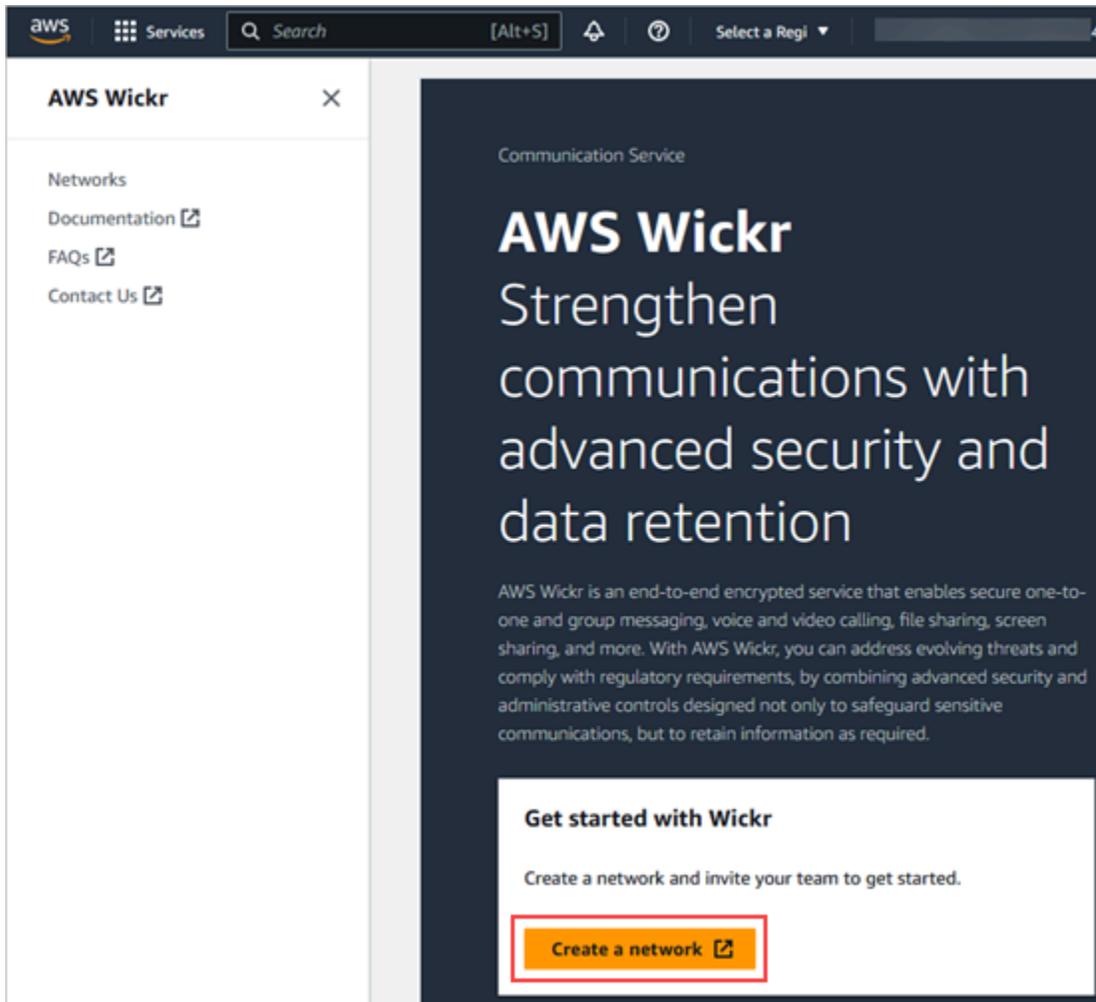
## Étape 1 : Création d'un réseau

Suivez la procédure suivante pour créer un réseau Wickr pour votre compte.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse <https://console.aws.amazon.com/wickr/>.

**Note**

Si vous n'avez jamais créé de réseau Wickr auparavant, vous verrez la page d'information du service Wickr. Après avoir créé un ou plusieurs réseaux Wickr, vous verrez la page Réseaux, qui contient une liste de tous les réseaux Wickr que vous avez créés.

**2. Choisissez Créer un réseau.**

3. Entrez le nom de votre réseau dans la zone de texte Nom du réseau. Choisissez un nom que les membres de votre organisation reconnaîtront, comme le nom de votre entreprise ou le nom de votre équipe.
4. Choisissez un plan. Vous pouvez choisir l'un des plans de réseau Wickr suivants :

- Standard — Pour les équipes des petites et grandes entreprises qui ont besoin de contrôles administratifs et de flexibilité.
- Essai gratuit Premium ou Premium : pour les entreprises qui ont besoin des limites de fonctionnalités les plus élevées, de contrôles administratifs précis et de la conservation des données.

Les administrateurs peuvent choisir l'option d'essai gratuit premium, disponible pour un maximum de 30 utilisateurs et d'une durée de trois mois. Cette offre est ouverte aux nouveaux forfaits d'essai gratuits et aux forfaits standard. Les administrateurs peuvent passer à un forfait Premium ou Standard ou à un abonnement inférieur pendant la période d'essai gratuite Premium.

Pour plus d'informations sur les forfaits et les tarifs Wickr disponibles, consultez la page de [tarification Wickr](#).

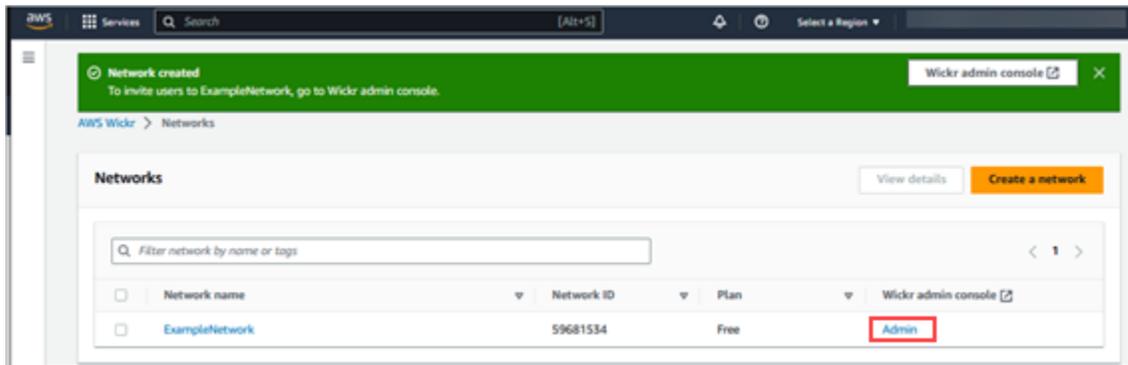
5. (Facultatif) Choisissez Ajouter un nouveau tag pour ajouter un tag à votre réseau. Les balises sont constituées d'une paire clé-valeur. Les tags peuvent être utilisés pour rechercher et filtrer les ressources ou pour suivre vos AWS coûts. Pour plus d'informations, consultez la section [Balises réseau](#).
6. Choisissez Create Network.

Vous êtes redirigé vers la page Réseaux de AWS Management Console for Wickr, et le nouveau réseau est répertorié sur la page.

## Étape 2 : Configuration de votre réseau

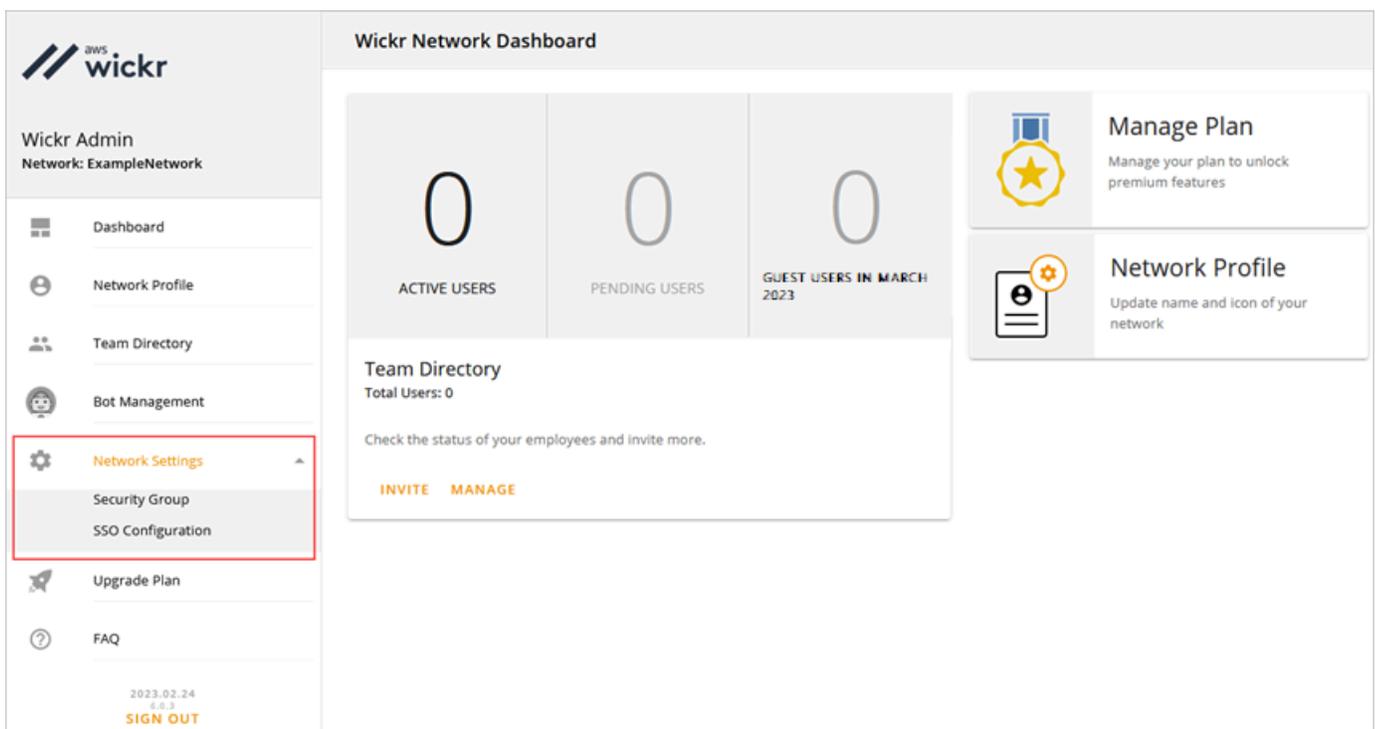
Suivez la procédure suivante pour accéder à la console d'administration Wickr, où vous pouvez ajouter des utilisateurs, ajouter des groupes de sécurité, configurer SSO, configurer la conservation des données et des paramètres réseau supplémentaires.

1. Sur la page Réseaux, choisissez le lien Admin pour accéder à la console d'administration Wickr pour ce réseau.



Vous êtes redirigé vers la console d'administration Wickr pour le réseau sélectionné.

2. Dans le volet de navigation de la console d'administration Wickr, choisissez Paramètres réseau.



Les options de configuration réseau suivantes sont disponibles. Pour plus d'informations sur la configuration de ces paramètres, consultez [Gérez votre réseau AWS Wickr](#).

- Groupe de sécurité : gérez les groupes de sécurité et leurs paramètres, tels que les politiques de complexité des mots de passe, les préférences de messagerie, les fonctionnalités d'appel, les fonctionnalités de sécurité et la fédération externe. Pour de plus amples informations, veuillez consulter [Groupes de sécurité](#).
- SSOConfiguration — Configurez SSO et affichez l'adresse du point de terminaison de votre réseau Wickr. Wickr prend en charge SSO les fournisseurs qui utilisent uniquement OpenID

OIDC Connect (). Les fournisseurs qui utilisent le langage de balisage d'assertions de sécurité (SAML) ne sont pas pris en charge. Pour de plus amples informations, veuillez consulter [Configuration de l'authentification unique](#).

## Étape 3 : créer et inviter des utilisateurs

Vous pouvez créer des utilisateurs dans votre réseau Wickr en utilisant les méthodes suivantes :

- **Authentification unique** — Si vous configurez SSO, vous pouvez inviter des utilisateurs en partageant votre identifiant d'entreprise Wickr. Les utilisateurs finaux s'inscrivent à Wickr en utilisant l'identifiant d'entreprise fourni et leur adresse e-mail professionnelle. Pour de plus amples informations, veuillez consulter [Configuration de l'authentification unique](#).
- **Invitation** — Vous pouvez créer manuellement des utilisateurs dans le AWS Management Console for Wickr et leur faire envoyer une invitation par e-mail. Les utilisateurs finaux peuvent s'inscrire à Wickr en cliquant sur le lien contenu dans l'e-mail.

### Note

Vous pouvez également activer les utilisateurs invités pour votre réseau Wickr. La fonctionnalité utilisateur invité est actuellement en cours de prévisualisation. Pour plus d'informations, consultez [Utilisateurs invités](#).

Suivez les procédures ci-dessous pour créer ou inviter des utilisateurs.

### Note

Les administrateurs sont également considérés comme des utilisateurs et doivent s'inviter à rejoindre SSO ou non les réseaux SSO Wickr.

## SSO

Écrivez et envoyez un e-mail aux SSO utilisateurs qui doivent s'inscrire à Wickr. Incluez les informations suivantes dans votre e-mail :

- Votre identifiant d'entreprise Wickr. Vous spécifiez un identifiant d'entreprise pour votre réseau Wickr lors de la configuration SSO. Pour de plus amples informations, veuillez consulter [Configurez SSO](#).
- L'adresse e-mail qu'ils doivent utiliser pour s'inscrire.
- Ensuite, URL pour télécharger le client Wickr. [Les utilisateurs peuvent télécharger les clients Wickr depuis la page de téléchargement de AWS Wickr sur download/](#). <https://aws.amazon.com/wickr/>

### Note

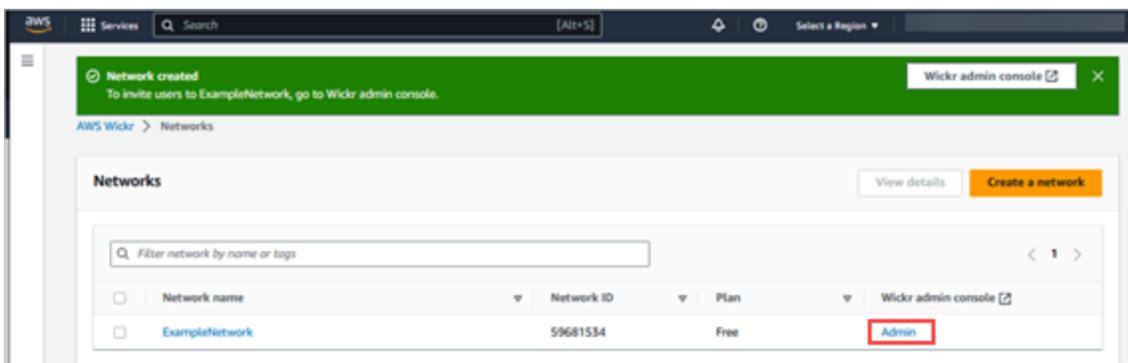
Si vous avez créé votre réseau Wickr dans AWS GovCloud l'ouest des États-Unis, demandez à vos utilisateurs de télécharger et d'installer le client. WickrGov Pour toutes les autres AWS régions, demandez à vos utilisateurs de télécharger et d'installer le client Wickr standard. Pour plus d'informations AWS WickrGov, consultez [AWS WickrGov](#) le guide de l'AWS GovCloud (US) utilisateur.

Lorsque les utilisateurs s'inscrivent sur votre réseau Wickr, ils sont ajoutés au répertoire de l'équipe Wickr avec le statut actif.

## Non-SSO

Pour créer manuellement des utilisateurs Wickr et envoyer des invitations :

1. Ouvrez le AWS Management Console pour Wickr à l'adresse <https://console.aws.amazon.com/wickr/>.
2. Sur la page Réseaux, choisissez le lien Admin pour accéder à la console d'administration Wickr pour ce réseau.



Vous êtes redirigé vers la console d'administration Wickr pour un réseau spécifique. Sur la console d'administration Wickr, vous pouvez ajouter des utilisateurs, ajouter des groupes de sécurité, configurer SSO, configurer la conservation des données et des paramètres supplémentaires pour le réseau spécifique que vous avez sélectionné.

3. Dans le volet de navigation de la console d'administration Wickr, choisissez Users, puis Team Directory.

Sur la page Utilisateurs, vous pouvez ajouter des utilisateurs individuels en choisissant Créer un nouvel utilisateur. Vous pouvez également ajouter des utilisateurs en bloc en choisissant l'icône Ajouter des utilisateurs dans le volet de navigation supérieur. Cliquez sur l'icône Télécharger pour télécharger un CSV modèle que vous pouvez modifier et télécharger avec votre liste d'utilisateurs.

4. Entrez le prénom, le nom de famille, le code du pays, le numéro de téléphone et l'adresse e-mail de l'utilisateur. L'adresse e-mail est le seul champ obligatoire. Assurez-vous de choisir le groupe de sécurité approprié pour l'utilisateur.
5. Sélectionnez Create (Créer).

**New User**

**User Information**

First Name  
Example

Last Name  
User

Country Code  
+1

Phone Number  
201-200-0000

**Account Information**

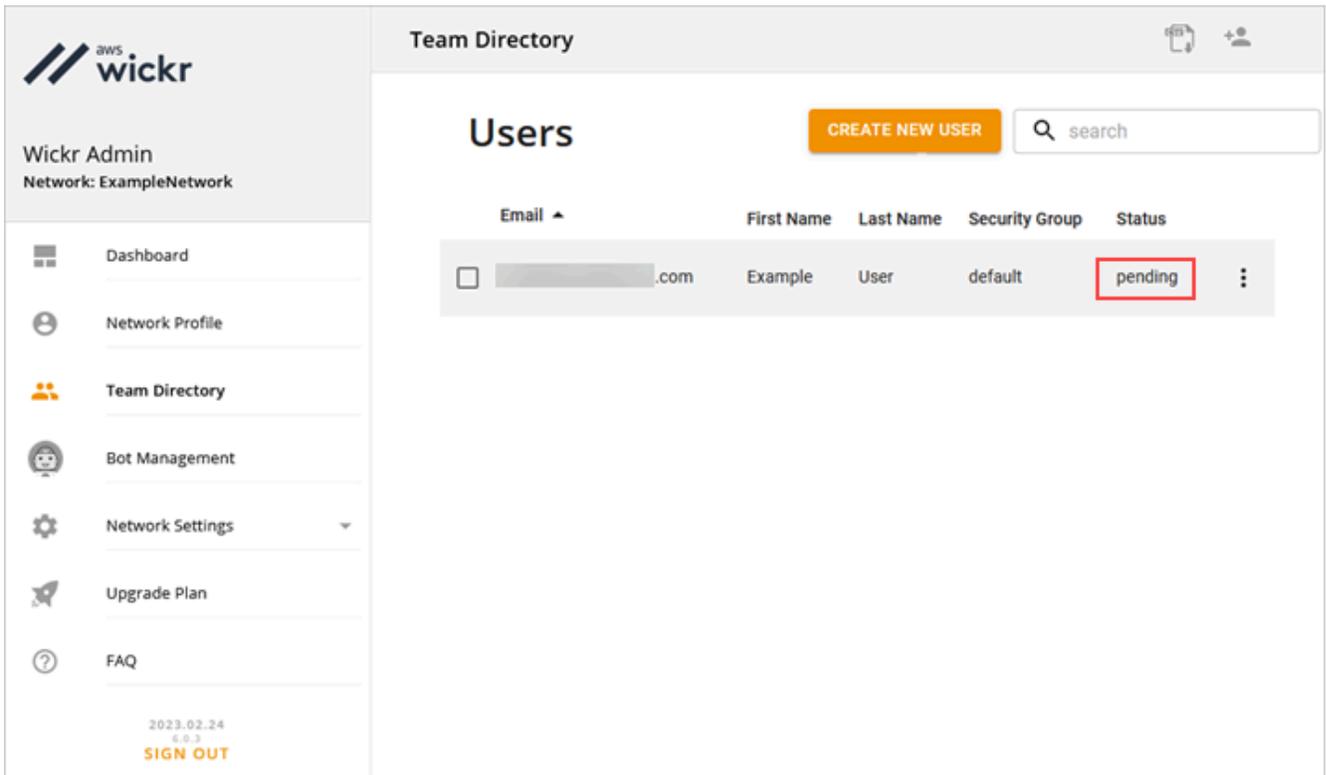
Email  
[blurred]

default

CANCEL CREATE

Wickr envoie un e-mail d'invitation à l'adresse que vous spécifiez pour l'utilisateur. L'e-mail fournit des liens de téléchargement pour les applications clientes Wickr, ainsi qu'un lien pour s'inscrire à Wickr. Pour plus d'informations sur ce à quoi ressemble cette expérience utilisateur final, voir [Télécharger l'application Wickr et accepter votre invitation](#) dans le guide de l'utilisateur de AWS Wickr.

Lorsque les utilisateurs s'inscrivent à Wickr en utilisant le lien contenu dans l'e-mail, leur statut dans le répertoire de l'équipe Wickr passe de En attente à Actif.



The screenshot shows the AWS Wickr interface. On the left is a sidebar with the Wickr Admin logo and navigation menu. The main area is titled 'Team Directory' and 'Users'. It features a 'CREATE NEW USER' button, a search bar, and a table of users. The table has columns for Email, First Name, Last Name, Security Group, and Status. One user is listed with the status 'pending', which is highlighted with a red box.

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

## Étapes suivantes

Vous avez terminé les étapes de démarrage. Pour gérer Wickr, consultez les guides suivants :

- [Gérez votre réseau AWS Wickr](#)
- [Gérer les utilisateurs dans AWS Wickr](#)

## Transférer Wickr Pro vers AWS Wickr

### Note

Wickr Pro n'est plus disponible. Si vous avez perdu l'accès à Wickr Pro, suivez les étapes de ce guide pour passer à AWS Wickr.

Dans ce guide, nous vous montrons comment effectuer un transfert depuis Wickr Pro et commencer à utiliser AWS Wickr.

Suivez les étapes de ce guide si vous possédez déjà un réseau Wickr Pro, mais que vous en NOT avez déjà un Compte AWS . Veuillez contacter l'assistance à tout moment si vous avez besoin d'aide.

Si votre organisation possède déjà un AWS compte, remplissez le formulaire [Migrer de Wickr Pro vers AWS Wickr](#) et le support AWS Wickr vous aidera.

Vous aurez besoin d'un Compte AWS identifiant pour gérer votre réseau AWS Wickr en tant Service AWS que. Pour plus d'informations sur ce qu' Compte AWS est un compte et comment le gérer, consultez le [Guide de référence AWS sur la gestion des comptes](#).

## Rubriques

- [Étape 1 : créer un AWS compte](#)
- [Étape 2 : Récupérez votre identifiant réseau Wickr](#)
- [Étape 3 : Soumettre une demande](#)
- [Étape 4 : connectez-vous à votre AWS console](#)

## Étape 1 : créer un AWS compte

Pour créer un AWS compte, procédez comme suit.

1. Si votre organisation ne possède pas d'identifiant de AWS compte existant, vous pouvez commencer par créer un identifiant de AWS compte autonome. Voici quelques éléments essentiels dont vous aurez besoin pour cela :
  - Une carte de crédit/débit pour la facturation
  - Une adresse e-mail accessible à un groupe (recommandé, non obligatoire)
  - Sélectionnez un AWS Support plan. Pour plus d'informations, consultez la section [Modification AWS Support des plans](#).

### Note

Vous pouvez toujours modifier votre AWS Support forfait au fur et à mesure que vous en apprenez davantage sur vos besoins.

2. Configurez l'accès administratif via IAM en tant que meilleure pratique de sécurité (facultatif mais recommandé). Pour plus d'informations, consultez [AWS Identity and Access Management](#). Pour

des instructions plus spécifiques sur l'accès administratif à AWS Wickr, voir la [politique AWS gérée : AWSWickrFullAccess](#).

3. Une fois les étapes précédentes terminées, vous pourrez vous connecter au pour trouver votre Compte AWS identifiant AWS Management Console à 12 chiffres sous le nom de votre compte.

## Étape 2 : Récupérez votre identifiant réseau Wickr

Effectuez la procédure suivante pour récupérer votre identifiant réseau Wickr.

1. Connectez-vous à votre console d'administration Wickr actuelle, sélectionnez le ou les réseaux que vous souhaitez migrer, puis choisissez Network Profile.
2. La page Profil réseau affiche votre identifiant réseau. Il s'agit d'un identifiant numérique à 8 chiffres.

## Étape 3 : Soumettre une demande

Maintenant que vous avez votre Compte AWS identifiant et votre identifiant réseau Wickr Pro, vous devez remplir le formulaire [de migration de Wickr Pro vers AWS Wickr](#).

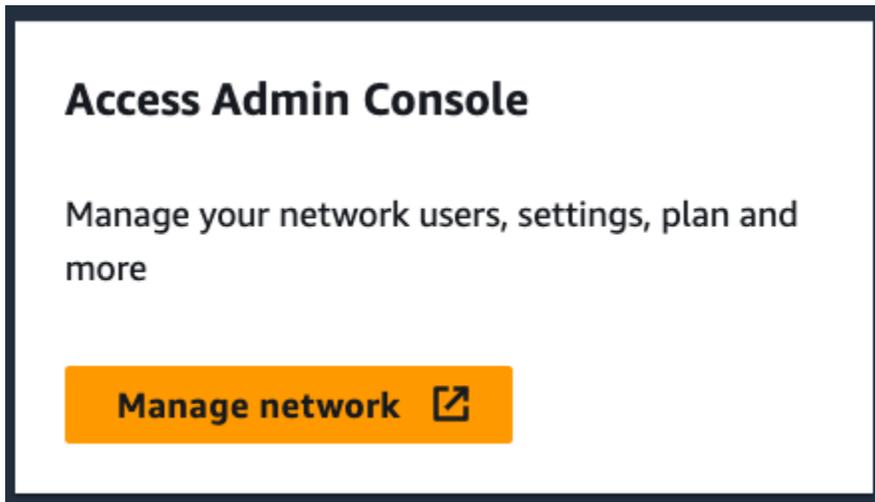
Une fois terminé, généralement dans les 14 jours, un représentant du support AWS Wickr vous contactera pour confirmer que votre réseau Wickr a été ajouté à votre Compte AWS

## Étape 4 : connectez-vous à votre AWS console

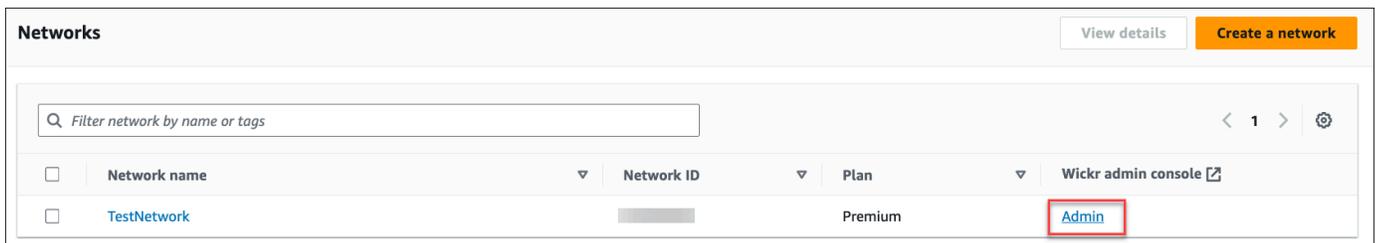
### Note

Suivez ces étapes, AFTER vous recevrez la confirmation que votre réseau Wickr Pro a été ajouté à votre Compte AWS.

1. Vous pouvez vous connecter à la AWS console en tant qu'utilisateur root OU avec un IAM utilisateur que vous avez créé précédemment (comme recommandé) à l'étape 2 pour AWS Wickr.
2. Accédez à votre service AWS Wickr. Vous pouvez le faire depuis le menu Services ou en recherchant AWS Wickr dans la barre de recherche.
3. Sur la page AWS Wickr, choisissez Gérer le réseau pour accéder à votre liste de réseaux Wickr.



4. Sur la page Réseaux, sous la colonne de la console d'administration Wickr, sélectionnez le lien Admin situé à droite du nom du réseau souhaité.



5. Le transfert est maintenant terminé ! Vous verrez le tableau de bord de votre réseau Wickr.

La facturation de votre réseau sera désormais transférée sur votre Compte AWS. Prévoyez jusqu'à 3 jours ouvrables pour que l'assistance vous contacte avec une confirmation. Après avoir reçu votre confirmation, vous pouvez consulter et payer votre facture via la AWS console.

# Gérez votre réseau AWS Wickr

Dans la section Paramètres réseau du AWS Management Console pour Wickr, vous pouvez gérer le nom de votre réseau Wickr, les groupes de sécurité, la SSO configuration et les paramètres de conservation des données.

## Rubriques

- [Profil du réseau](#)
- [Groupes de sécurité](#)
- [Configuration de l'authentification unique](#)
- [Lire les reçus](#)
- [Balises réseau](#)
- [Gérer le plan réseau](#)
- [Conservation des données](#)
- [Qu'est-ce qu'ATAK ?](#)
- [Liste des ports et domaines à autoriser](#)
- [GovCloud classification et fédération transfrontalières](#)

## Profil du réseau

Vous pouvez modifier le nom de votre réseau Wickr et consulter votre identifiant réseau dans la section Profil réseau du AWS Management Console pour Wickr.

## Rubriques

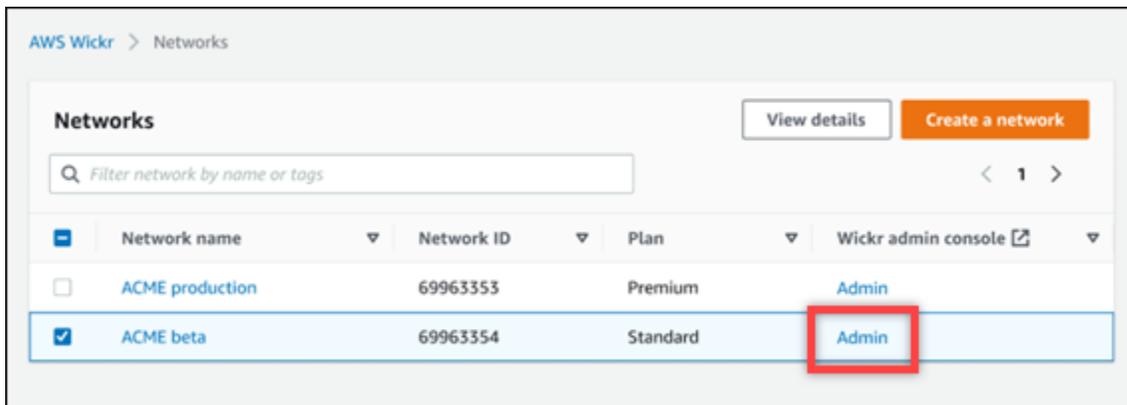
- [Afficher le profil du réseau](#)
- [Modifier le nom du réseau](#)

## Afficher le profil du réseau

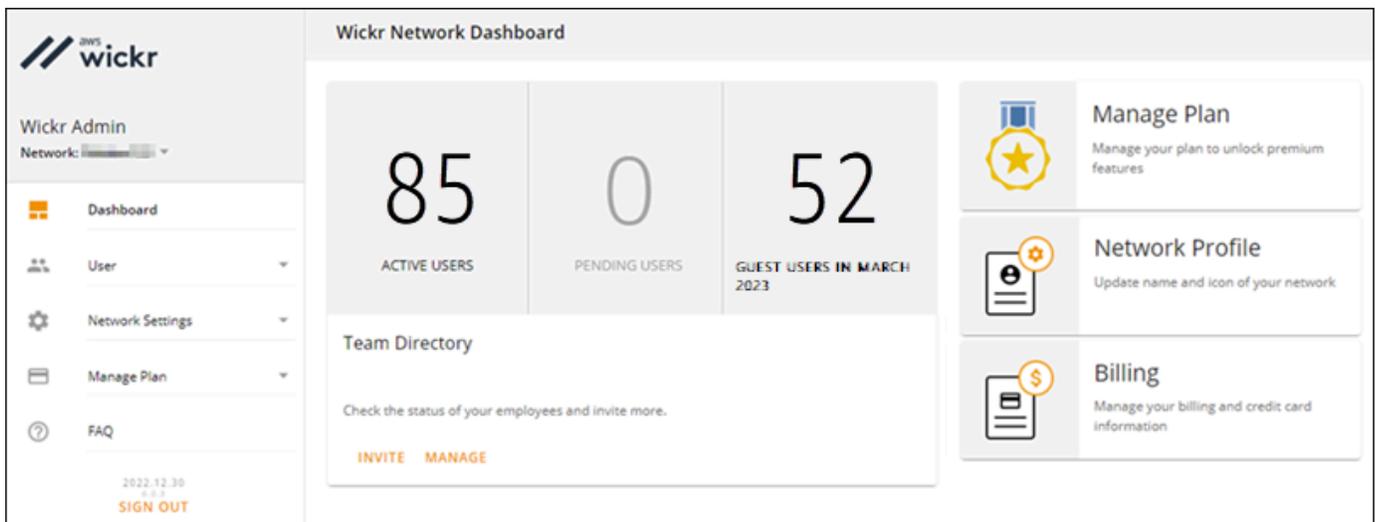
Suivez la procédure suivante pour afficher votre profil réseau Wickr et votre identifiant réseau.

1. Ouvrez le fichier AWS Management Console pour Wickr Cat. <https://console.aws.amazon.com/wickr/>

2. Sur la page Réseaux, choisissez le lien Admin pour accéder à la console d'administration Wickr pour ce réseau.



Vous êtes redirigé vers la console d'administration Wickr pour un réseau spécifique.



3. Dans le volet de navigation de la console d'administration Wickr, choisissez Network Settings, puis Network Profile.

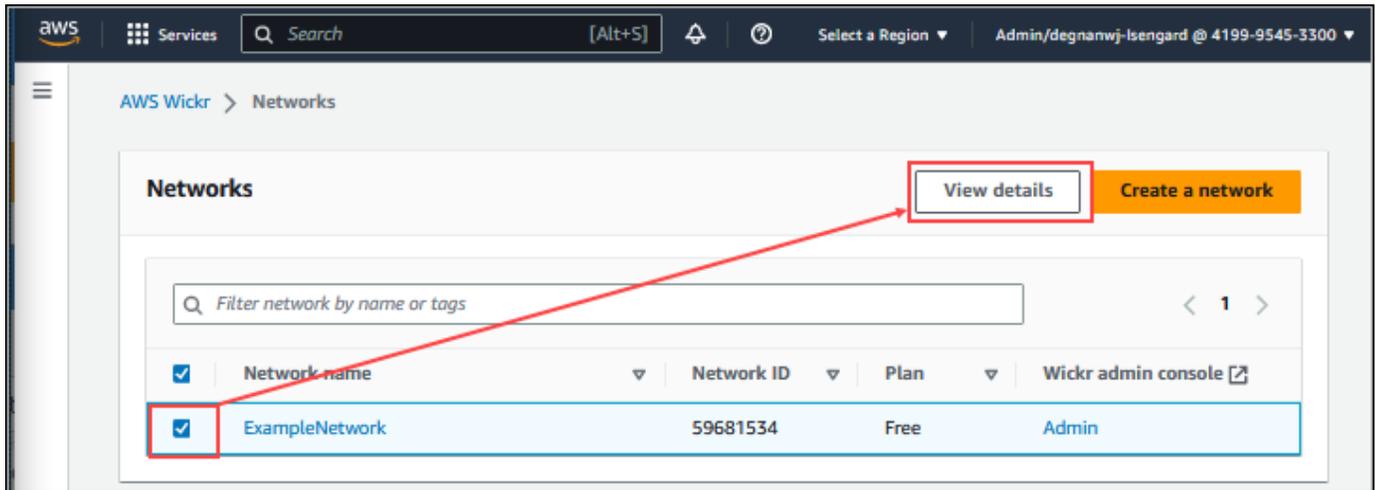
La page de profil réseau affiche le nom et l'identifiant de votre réseau Wickr. Vous pouvez utiliser l'ID réseau pour configurer la fédération.

## Modifier le nom du réseau

Suivez la procédure suivante pour modifier le nom de votre réseau Wickr.

1. Ouvrez le fichier AWS Management Console pour Wickr Cat. <https://console.aws.amazon.com/wickr/>

2. Choisissez Gérer le réseau.
3. Sur la page Réseaux, cochez la case à côté du nom du réseau que vous souhaitez modifier, puis choisissez Afficher les détails.



4. Dans la section Vue d'ensemble du réseau, choisissez Modifier.
5. Entrez le nouveau nom de votre réseau dans la zone de texte Nom du réseau.
6. Choisissez Enregistrer les modifications pour enregistrer le nouveau nom de votre réseau.

## Groupes de sécurité

Dans la section Groupes de sécurité du AWS Management Console pour Wickr, vous pouvez gérer les groupes de sécurité et leurs paramètres, tels que les politiques de complexité des mots de passe, les préférences de messagerie, les fonctionnalités d'appel, les fonctionnalités de sécurité et la fédération réseau.

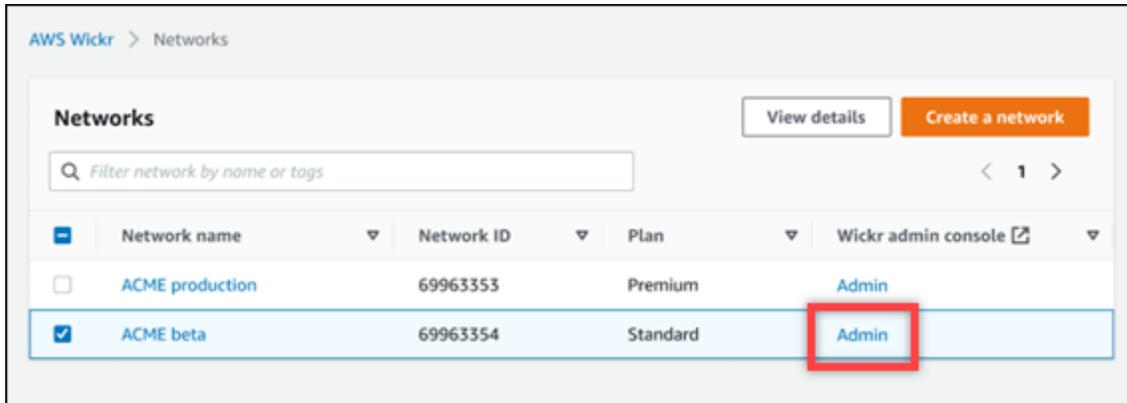
### Rubriques

- [Afficher les groupes de sécurité](#)
- [Création d'un groupe de sécurité](#)
- [Modifier un groupe de sécurité](#)
- [Supprimer un groupe de sécurité](#)

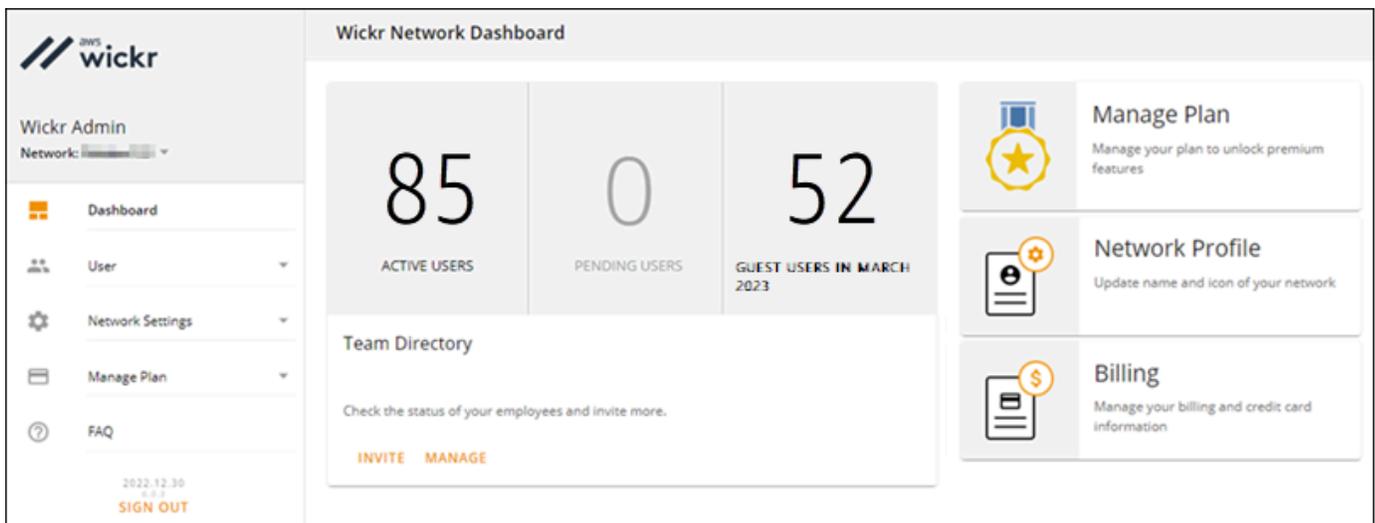
## Afficher les groupes de sécurité

Suivez la procédure ci-dessous pour afficher les groupes de sécurité.

1. Ouvrez le fichier AWS Management Console pour Wickr Cat. <https://console.aws.amazon.com/wickr/>
2. Sur la page Réseaux, choisissez le lien Admin pour accéder à la console d'administration Wickr pour ce réseau.



Vous êtes redirigé vers la console d'administration Wickr pour un réseau spécifique.



3. Dans le volet de navigation de la console d'administration Wickr, choisissez Network Settings, puis Security Group.

La page Groupes de sécurité affiche vos groupes de sécurité Wickr actuels et vous donne la possibilité de consulter leurs détails ou de créer un nouveau groupe.

## Création d'un groupe de sécurité

Suivez la procédure ci-dessous pour créer un groupe de sécurité.

1. Ouvrez le fichier AWS Management Console pour Wickr Cat. <https://console.aws.amazon.com/wickr/>
2. Sur la page Réseaux, choisissez le lien Admin pour accéder à la console d'administration Wickr pour ce réseau.

Vous êtes redirigé vers la console d'administration Wickr pour un réseau spécifique.

3. Dans le volet de navigation de la console d'administration Wickr, choisissez Network Settings, puis Security Group.
4. Choisissez Nouveau groupe pour créer un nouveau groupe de sécurité.

Un nouveau groupe de sécurité portant un nom par défaut est automatiquement ajouté à la liste des groupes de sécurité.

Pour plus d'informations sur la modification du nouveau groupe de sécurité, consultez [Modifier un groupe de sécurité](#).

## Modifier un groupe de sécurité

Suivez la procédure ci-dessous pour modifier un groupe de sécurité.

1. Ouvrez le fichier AWS Management Console pour Wickr Cat. <https://console.aws.amazon.com/wickr/>
2. Sur la page Réseaux, choisissez le lien Admin pour accéder à la console d'administration Wickr pour ce réseau.

Vous êtes redirigé vers la console d'administration Wickr pour un réseau spécifique.

3. Dans le volet de navigation de la console d'administration Wickr, choisissez Network Settings, puis Security Group.
4. Choisissez Détails à côté du nom du groupe de sécurité que vous souhaitez modifier.

La page Détails du groupe de sécurité affiche les paramètres du groupe de sécurité dans différents onglets.

5. Les onglets suivants et les paramètres correspondants sont disponibles :
  - Nom du groupe de sécurité : cliquez sur l'icône en forme de crayon à côté du nom du groupe pour le modifier.
  - Général — Modifiez la configuration de base du groupe.

- Messagerie — Gérez les fonctionnalités de messagerie pour les membres du groupe.
  - Appels — Gérez les fonctionnalités d'appel pour les membres du groupe.
  - Sécurité — Configurez des fonctionnalités de sécurité supplémentaires pour le groupe.
  - Fédération : capacité de communiquer entre les réseaux. Cela peut être configuré dans la console d'administration pour un réseau au niveau du groupe de sécurité. AWSWickr dispose de 2 types de fédération : locale et mondiale.
    - Fédération locale : possibilité de fédérer des AWS utilisateurs d'autres réseaux au sein de la même région. Par exemple, s'il existe deux réseaux au Canada où la fédération locale est activée, ils pourront communiquer entre eux.
    - Fédération mondiale : possibilité de fédérer avec les utilisateurs de l'entreprise ou AWS utilisateurs d'un autre réseau appartenant à d'autres régions. Par exemple, s'il y a un utilisateur dans un réseau de la région du Canada et un utilisateur dans un réseau de la région de Londres, et que la fédération mondiale est activée pour les deux réseaux, ils pourront communiquer entre eux.
    - Fédération restreinte : possibilité de fédérer avec des réseaux spécifiques (Enterprise ou AWS) appartenant à différentes régions. Les administrateurs peuvent autoriser la création de listes de réseaux spécifiques avec lesquels leurs utilisateurs peuvent se fédérer. Après la restriction, les utilisateurs ne peuvent communiquer qu'avec les utilisateurs des réseaux autorisés. Les deux réseaux doivent s'autoriser mutuellement dans les paramètres du groupe de sécurité de l'onglet fédération pour utiliser la fédération restreinte.
6. Choisissez Enregistrer pour enregistrer les modifications que vous apportez aux détails du groupe de sécurité.

## Supprimer un groupe de sécurité

Suivez la procédure ci-dessous pour supprimer un groupe de sécurité.

1. Ouvrez le fichier AWS Management Console pour Wickr Cat. <https://console.aws.amazon.com/wickr/>
2. Sur la page Réseaux, choisissez le lien Admin pour accéder à la console d'administration Wickr pour ce réseau.

Vous êtes redirigé vers la console d'administration Wickr pour un réseau spécifique.

3. Dans le volet de navigation de la console d'administration Wickr, choisissez Network Settings, puis Security Group.

4. Cliquez sur l'icône représentant des points de suspension verticaux à côté du nom du groupe de sécurité que vous souhaitez supprimer.
5. Choisissez Supprimer pour supprimer le groupe de sécurité.

Lorsque vous supprimez un groupe de sécurité auquel des utilisateurs ont été assignés, ceux-ci sont automatiquement ajoutés au groupe de sécurité par défaut. Pour modifier le groupe de sécurité attribué aux utilisateurs, voir [Modifier les utilisateurs](#).

## Configuration de l'authentification unique

Dans la section SSOConfiguration du AWS Management Console pour Wickr, vous pouvez configurer Wickr pour utiliser un système d'authentification unique pour s'authentifier. SSO fournit un niveau de sécurité supplémentaire lorsqu'il est associé à un système d'authentification multifactorielle (MFA) approprié. Wickr prend en charge SSO les fournisseurs qui utilisent uniquement OpenID OIDC Connect (). Les fournisseurs qui utilisent le langage de balisage d'assertions de sécurité (SAML) ne sont pas pris en charge.

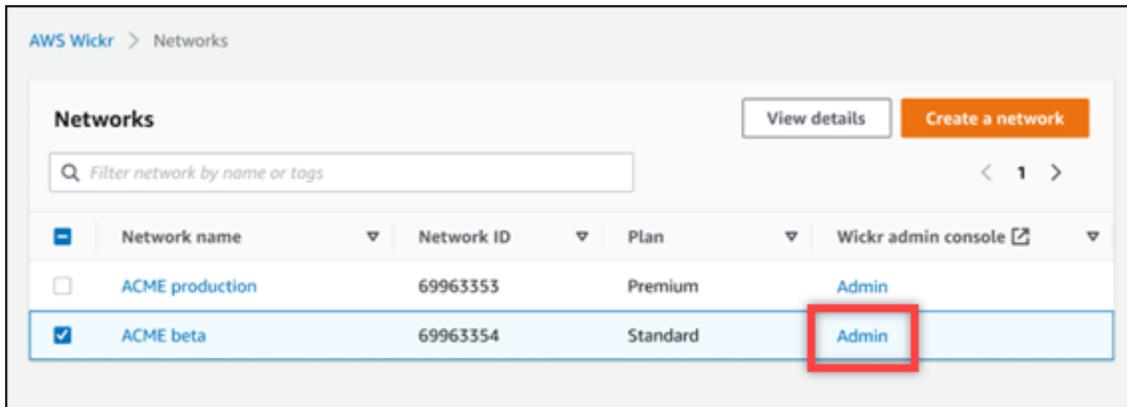
### Rubriques

- [Afficher les SSO détails](#)
- [Configurez SSO](#)
- [Période de grâce pour l'actualisation des jetons](#)
- [Configurer l'authentification unique Microsoft Entra \(Azure AD\)](#)

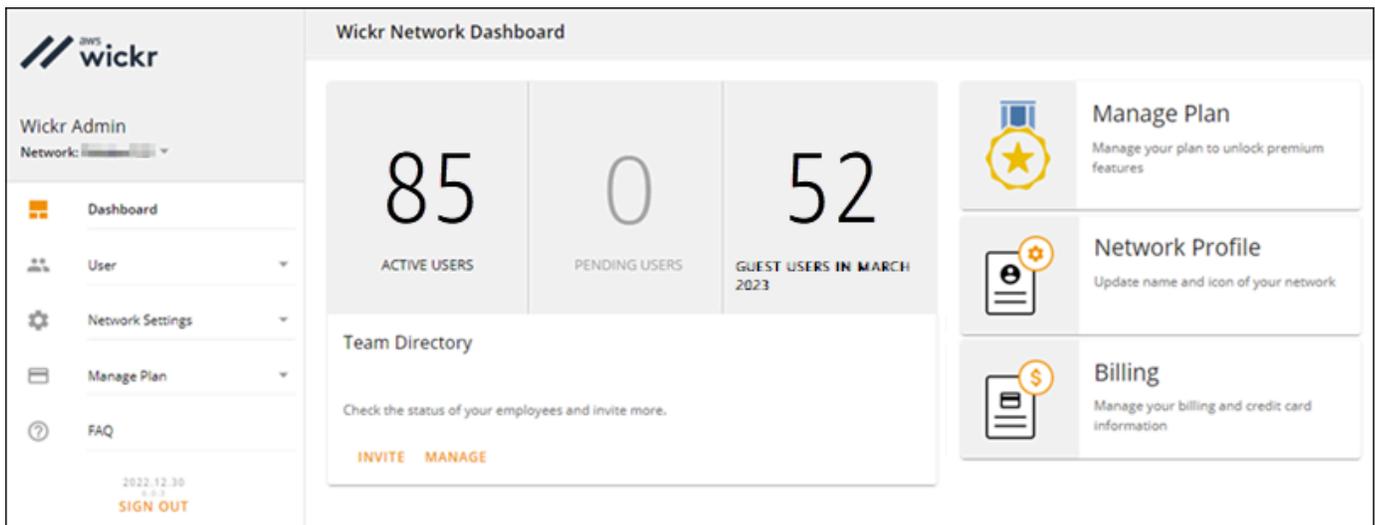
## Afficher les SSO détails

Effectuez la procédure suivante pour afficher la configuration d'authentification unique actuelle pour votre réseau Wickr, le cas échéant. Vous pouvez également afficher le point de terminaison réseau de votre réseau Wickr.

1. Ouvrez le fichier AWS Management Console pour Wickr Cat. <https://console.aws.amazon.com/wickr/>
2. Sur la page Réseaux, choisissez le lien Admin pour accéder à la console d'administration Wickr pour ce réseau.



Vous êtes redirigé vers la console d'administration Wickr pour un réseau spécifique.



3. Dans le volet de navigation de la console d'administration Wickr, choisissez Paramètres réseau, puis SSOConfiguration.

La page d'authentification unique et de LDAP configuration affiche le point de terminaison de votre réseau Wickr et la configuration actuelle SSO.

## Configurez SSO

Pour plus d'informations sur la configuration SSO, consultez les guides suivants :

### ⚠ Important

Lorsque vous configurez SSO, vous spécifiez un identifiant d'entreprise pour votre réseau Wickr. Assurez-vous de noter l'identifiant de l'entreprise pour votre réseau Wickr. Vous devez

le fournir à vos utilisateurs finaux lors de l'envoi d'e-mails d'invitation. Les utilisateurs finaux doivent spécifier l'identifiant de l'entreprise lorsqu'ils s'inscrivent à votre réseau Wickr.

- [Configurer l'authentification unique Microsoft Entra \(Azure AD\)](#)
- [Configurer l'authentification unique Okta](#)

## Période de grâce pour l'actualisation des jetons

Il peut arriver que les fournisseurs d'identité rencontrent des interruptions temporaires ou prolongées, ce qui peut entraîner la déconnexion inattendue de vos utilisateurs en raison de l'échec d'un jeton d'actualisation pour leur session client. Pour éviter ce problème, vous pouvez établir une période de grâce qui permet à vos utilisateurs de rester connectés même si leur jeton d'actualisation client échoue lors de telles pannes.

Voici les options disponibles pour la période de grâce :

- Aucune période de grâce (par défaut) : les utilisateurs seront déconnectés immédiatement après l'échec d'un jeton d'actualisation.
- Période de grâce de 30 minutes : les utilisateurs peuvent rester connectés jusqu'à 30 minutes après l'échec d'un jeton d'actualisation.
- Période de grâce de 60 minutes : les utilisateurs peuvent rester connectés pendant 60 minutes au maximum après l'échec d'un jeton d'actualisation.

## Configurer l'authentification unique Microsoft Entra (Azure AD)

AWSWickr peut être configuré pour utiliser Microsoft Entra (Azure AD) comme fournisseur d'identité. Pour ce faire, suivez les procédures suivantes dans Microsoft Entra et dans la console d'administration AWS Wickr.

### Warning

Une fois SSO activé sur un réseau, les utilisateurs actifs seront déconnectés de Wickr et les obligeront à se réauthentifier en utilisant le fournisseur. SSO

## Étape 1 : enregistrer AWS Wickr en tant qu'application dans Microsoft Entra

Suivez la procédure suivante pour enregistrer AWS Wickr en tant qu'application dans Microsoft Entra.

### Note

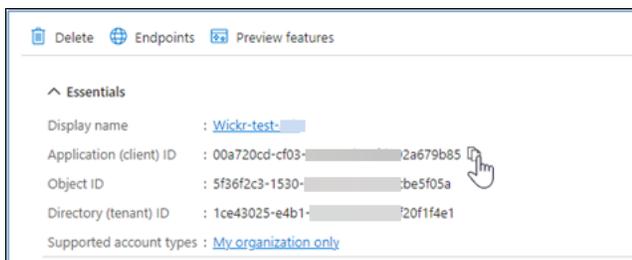
Reportez-vous à la documentation Microsoft Entra pour obtenir des captures d'écran détaillées et un dépannage. Pour plus d'informations, voir [Enregistrer une application auprès de la plateforme d'identité Microsoft](#)

1. Dans le volet de navigation, choisissez Applications, puis cliquez sur Inscriptions d'applications.
2. Sur la page Inscriptions d'applications, choisissez Enregistrer une application, puis entrez un nom d'application.
3. Sélectionnez Comptes uniquement dans ce répertoire d'organisation (répertoire par défaut uniquement - Locataire unique).
4. Sous Redirection URI, sélectionnez Web, puis entrez l'adresse Web suivante : `https://messaging-pro-prod.wickr.com/deeplink/oidc.php`.

### Note

La redirection URI peut également être copiée depuis les paramètres de SSO configuration de la console d'administration AWS Wickr.

5. Choisissez Register (S'inscrire).
6. Après l'enregistrement, copiez/enregistrez l'ID d'application (client) généré.



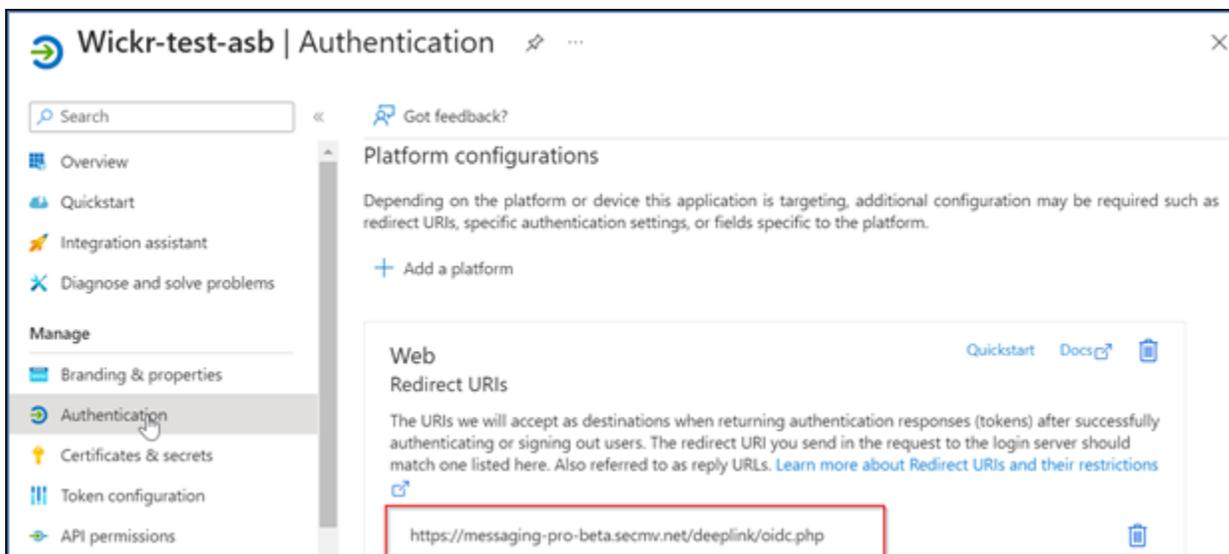
7. Sélectionnez l'onglet Endpoints pour prendre note des points suivants :
  1. Point de terminaison d'autorisation OAuth 2.0 (v2) : Par exemple : `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/oauth2/v2.0/authorize`

2. Modifiez cette valeur pour supprimer « oauth2/ » et « authorize ». Par exemple, URL le correctif ressemblera à ceci : `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`
3. Il sera référencé en tant qu'SSOémetteur.

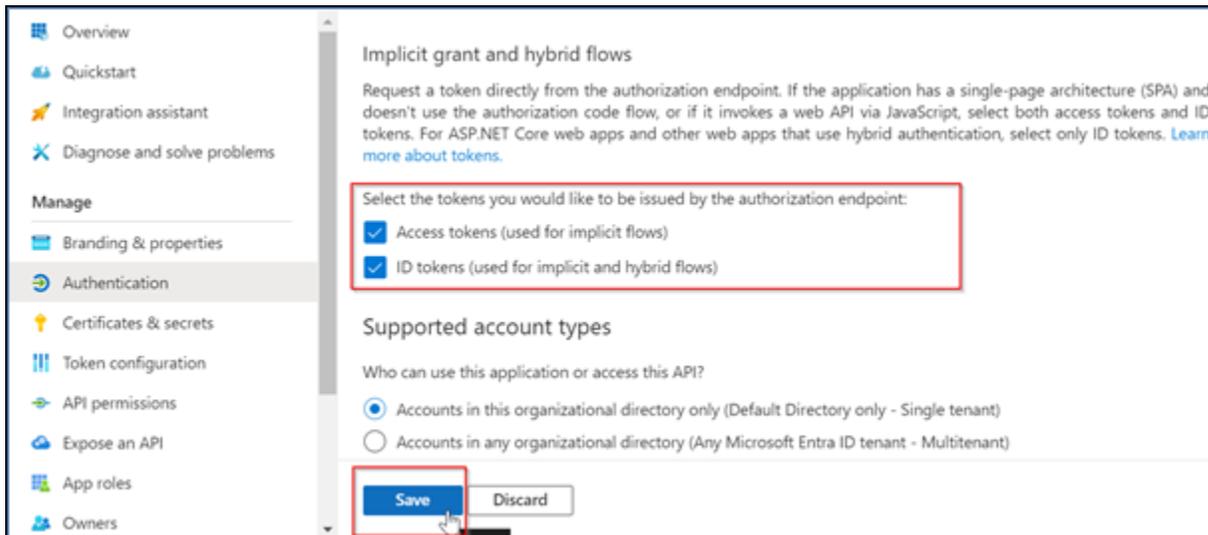
## Étape 2 : Configuration de l'authentification

Suivez la procédure ci-dessous pour configurer l'authentification dans Microsoft Entra.

1. Dans le volet de navigation, choisissez Authentication.
2. Sur la page d'authentification, assurez-vous que la redirection Web URI est la même que celle saisie précédemment (dans Enregistrer AWS Wickr en tant qu'application).



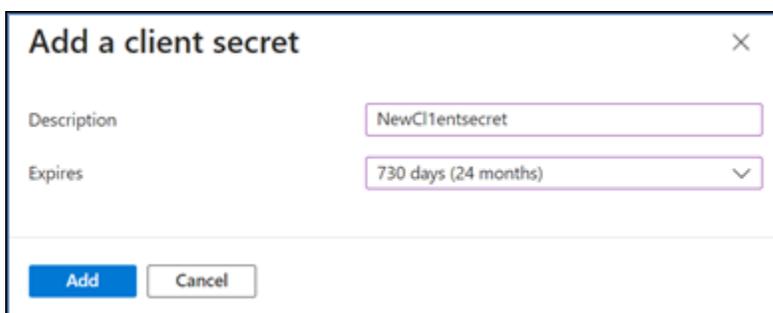
3. Sélectionnez les jetons d'accès utilisés pour les flux implicites et les jetons d'identification utilisés pour les flux implicites et hybrides.
4. Choisissez Save (Enregistrer).



### Étape 3 : Configuration des certificats et des secrets

Suivez la procédure suivante pour configurer les certificats et les secrets dans Microsoft Entra.

1. Dans le volet de navigation, sélectionnez Certificats & secrets.
2. Sur la page Certificats et secrets, sélectionnez l'onglet Secrets clients.
3. Dans l'onglet Secret client, sélectionnez Nouveau secret client.
4. Entrez une description et sélectionnez une période d'expiration pour le secret.
5. Choisissez Ajouter.



6. Une fois le certificat créé, copiez la valeur secrète du client.



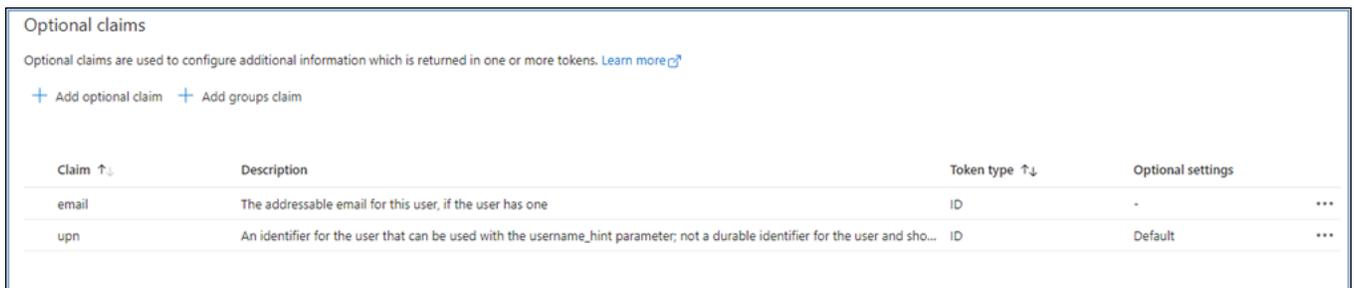
**Note**

La valeur secrète du client (et non l'ID secret) sera requise pour le code de votre application client. Il se peut que vous ne puissiez pas afficher ou copier la valeur secrète après avoir quitté cette page. Si vous ne le copiez pas maintenant, vous devrez y retourner pour créer un nouveau secret client.

**Étape 4 : Configuration de la configuration du jeton**

Suivez la procédure suivante pour configurer la configuration des jetons dans Microsoft Entra.

1. Dans le volet de navigation, choisissez Configuration du jeton.
2. Sur la page de configuration du jeton, choisissez Ajouter une réclamation facultative.
3. Sous Réclamations facultatives, sélectionnez le type de jeton comme identifiant.
4. Après avoir sélectionné l'identifiant, sous Réclamer, sélectionnez e-mail et UPN.
5. Choisissez Ajouter.



Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. [Learn more](#)

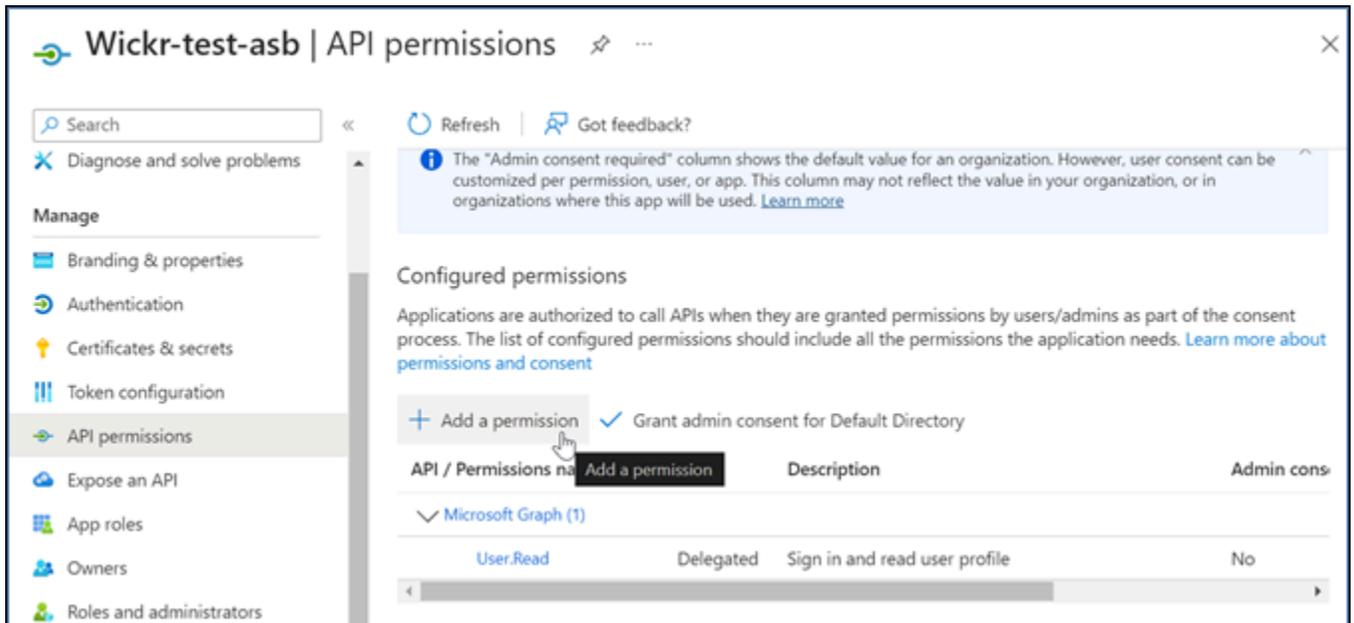
+ Add optional claim + Add groups claim

Claim ↑	Description	Token type ↑↓	Optional settings
email	The addressable email for this user, if the user has one	ID	- ...
upn	An identifier for the user that can be used with the username_hint parameter; not a durable identifier for the user and sho...	ID	Default ...

**Étape 5 : Configuration API des autorisations**

Suivez la procédure ci-dessous pour configurer API les autorisations dans Microsoft Entra.

1. Dans le volet de navigation, choisissez API les autorisations.
2. Sur la page API des autorisations, choisissez Ajouter une autorisation.

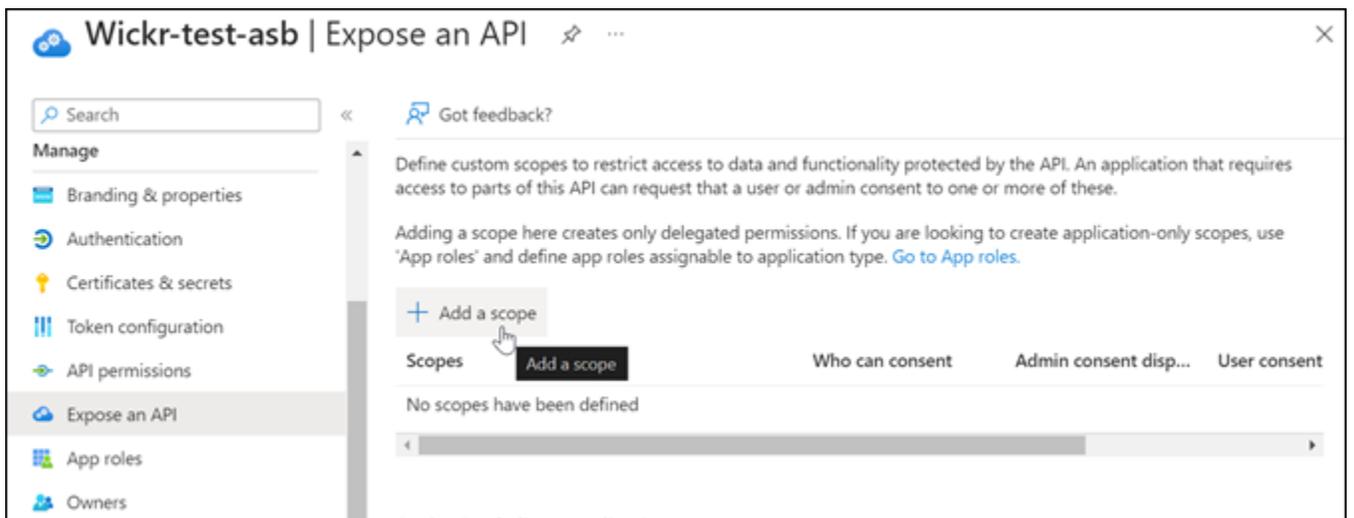


- Sélectionnez Microsoft Graph, puis sélectionnez Autorisations déléguées.
- Cochez la case pour e-mail, offline\_access, openid, profile.
- Choisissez Add permissions (Ajouter des autorisations).

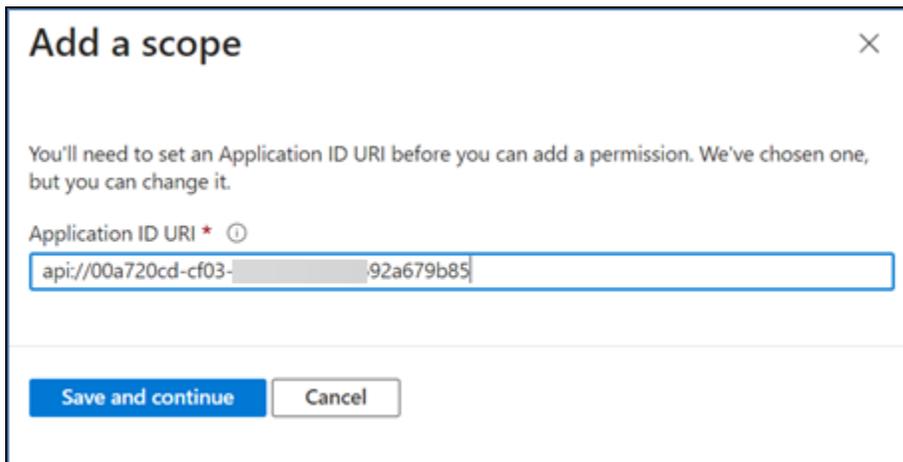
## Étape 6 : Exposer un API

Procédez comme suit pour exposer un API pour chacun des 4 champs d'application dans Microsoft Entra.

- Dans le volet de navigation, choisissez Expose an API.
- Sur la API page Exposer une portée, choisissez Ajouter une étendue.



L'identifiant de l'application URI doit être renseigné automatiquement et l'identifiant qui suit URI doit correspondre à l'identifiant de l'application (créé dans Register AWS Wickr en tant qu'application).



**Add a scope** ✕

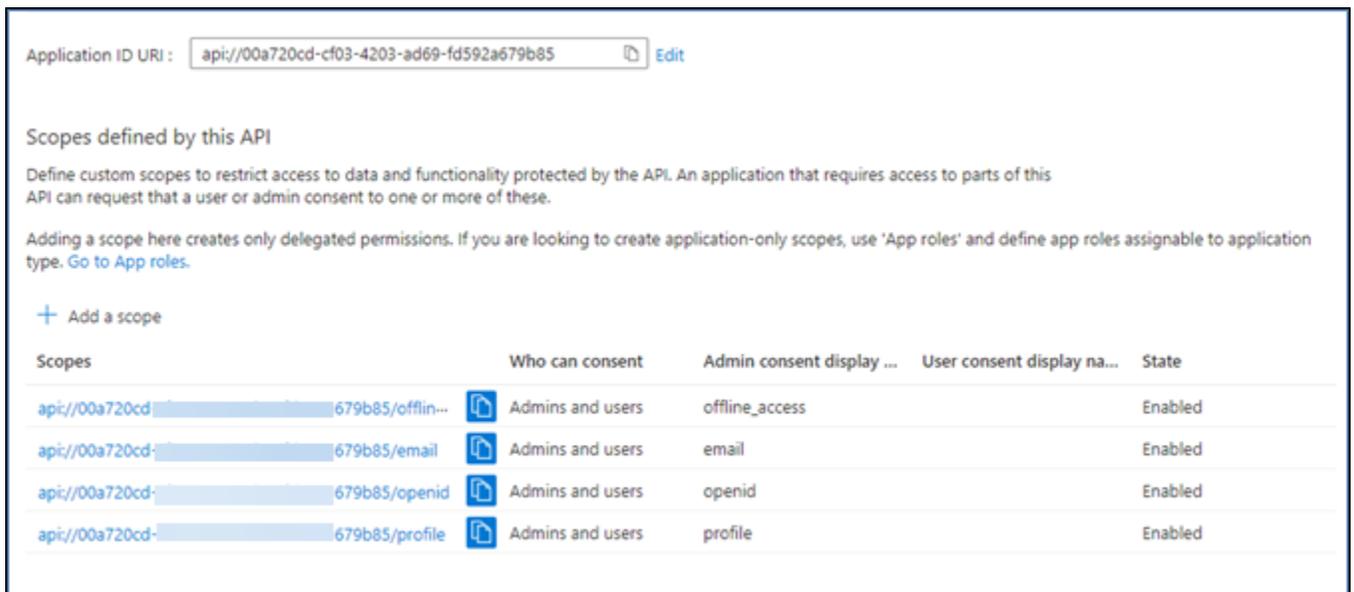
You'll need to set an Application ID URI before you can add a permission. We've chosen one, but you can change it.

Application ID URI \* ⓘ

api://00a720cd-cf03-4203-ad69-fd592a679b85

**Save and continue** **Cancel**

3. Choisissez Save and continue (Enregistrer et continuer).
4. Sélectionnez le tag Admins and users, puis entrez le nom de la portée sous la forme offline\_access.
5. Sélectionnez État, puis sélectionnez Activer.
6. Choisissez Ajouter un champ d'application.
7. Répétez les étapes 1 à 6 de cette section pour ajouter les champs d'application suivants : e-mail, openid et profile.



Application ID URI :  [Edit](#)

**Scopes defined by this API**

Define custom scopes to restrict access to data and functionality protected by the API. An application that requires access to parts of this API can request that a user or admin consent to one or more of these.

Adding a scope here creates only delegated permissions. If you are looking to create application-only scopes, use 'App roles' and define app roles assignable to application type. [Go to App roles.](#)

[+](#) Add a scope

Scopes	Who can consent	Admin consent display ...	User consent display na...	State
api://00a720cd-679b85/offlin...	Admins and users	offline_access		Enabled
api://00a720cd-679b85/email	Admins and users	email		Enabled
api://00a720cd-679b85/openid	Admins and users	openid		Enabled
api://00a720cd-679b85/profile	Admins and users	profile		Enabled

8. Sous Applications clientes autorisées, sélectionnez Ajouter une application client.

9. Sélectionnez les quatre étendues créées à l'étape précédente.
10. Entrez ou vérifiez l'ID de l'application (client).
11. Choisissez Add application (Ajouter une application).

## Étape 7 : Configuration de AWS Wickr SSO

Effectuez la procédure de configuration suivante dans la console AWS Wickr.

1. Ouvrez le fichier AWS Management Console pour Wickr Cat. <https://console.aws.amazon.com/wickr/>
2. Sur la page Réseaux, choisissez le lien Admin pour accéder à la console d'administration Wickr pour ce réseau.
3. Dans le volet de navigation de la console d'administration Wickr, choisissez Paramètres réseau, puis SSOConfiguration.
4. Sous Network Endpoint, assurez-vous que la redirection URI correspond à l'adresse Web suivante (ajoutée à l'étape 4 sous Enregistrer AWS Wickr en tant qu'application).

`https://messaging-pro-prod.wickr.com/deeplink/oidc.php`

5. Sous SSOConfiguration, choisissez Démarrer
6. Entrez les informations suivantes :
  - SSOÉmetteur — Il s'agit du point de terminaison qui a été modifié précédemment (par exemple `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`).
  - SSOID client — Il s'agit de l'ID de l'application (client) indiqué dans le volet Vue d'ensemble.
  - Numéro d'entreprise — Il peut s'agir d'une valeur de texte unique comprenant des caractères alphanumériques et des traits de soulignement. C'est cette phrase que vos utilisateurs saisiront lorsqu'ils s'enregistreront sur de nouveaux appareils.
  - Secret client : il s'agit du secret client indiqué dans le volet Certificats et secrets.
  - Étendue : il s'agit des noms de portée exposés dans le API volet Exposer un. Entrez email, profile, offline\_access et openid.
  - Étendue du nom d'utilisateur personnalisé — Entrez upn.

Les autres champs sont facultatifs.

7. Choisissez Tester et enregistrer.

## 8. Choisissez Save (Enregistrer).

SSO la configuration est terminée. Pour vérifier, vous pouvez désormais ajouter un utilisateur à l'application dans Microsoft Entra et vous connecter avec cet utilisateur à l'aide SSO d'un identifiant d'entreprise.

Pour plus d'informations sur la façon d'inviter et d'intégrer des utilisateurs, voir [Créer et inviter des utilisateurs](#).

### Résolution des problèmes

Vous trouverez ci-dessous les problèmes courants que vous pourriez rencontrer ainsi que des suggestions pour les résoudre.

- SSO Le test de connexion échoue ou ne répond pas :
  - Assurez-vous que l'SSO émetteur est configuré comme prévu.
  - Assurez-vous que les champs obligatoires du champ SSO configuré sont définis comme prévu.
- Le test de connexion est réussi, mais l'utilisateur ne parvient pas à se connecter :
  - Assurez-vous que l'utilisateur est ajouté à l'application Wickr que vous avez enregistrée dans Microsoft Entra.
  - Assurez-vous que l'utilisateur utilise le bon identifiant d'entreprise, y compris le préfixe. Par exemple. UE1- DemoNetwork W\_Draw.
  - Le secret client n'est peut-être pas défini correctement dans la SSO configuration de AWS Wickr. Réinitialisez-le en créant un autre secret client dans Microsoft Entra et définissez le nouveau secret client dans la configuration Wickr. SSO

## Lire les reçus

Les accusés de lecture sur Wickr sont des notifications envoyées à l'expéditeur pour indiquer quand son message a été lu. Ces reçus sont disponibles dans les one-on-one conversations. Une seule coche apparaît pour les messages envoyés, et un cercle plein avec une coche apparaît pour les messages lus. Pour voir les accusés de lecture sur les messages lors de conversations externes, les accusés de lecture doivent être activés sur les deux réseaux.

Les administrateurs peuvent activer ou désactiver les confirmations de lecture dans le panneau de configuration de l'administrateur. Ce paramètre sera appliqué à l'ensemble du réseau.

Procédez comme suit pour activer ou désactiver les confirmations de lecture.

1. Ouvrez le fichier AWS Management Console pour Wickr Cat. <https://console.aws.amazon.com/wickr/>
2. Dans le volet de navigation de la console d'administration Wickr, choisissez Network Settings, puis Network Profile.
3. Sur la page de profil du réseau, dans la section Lire les reçus, choisissez Modifier.
4. Sélectionnez Activer ou Désactiver.

## Balises réseau

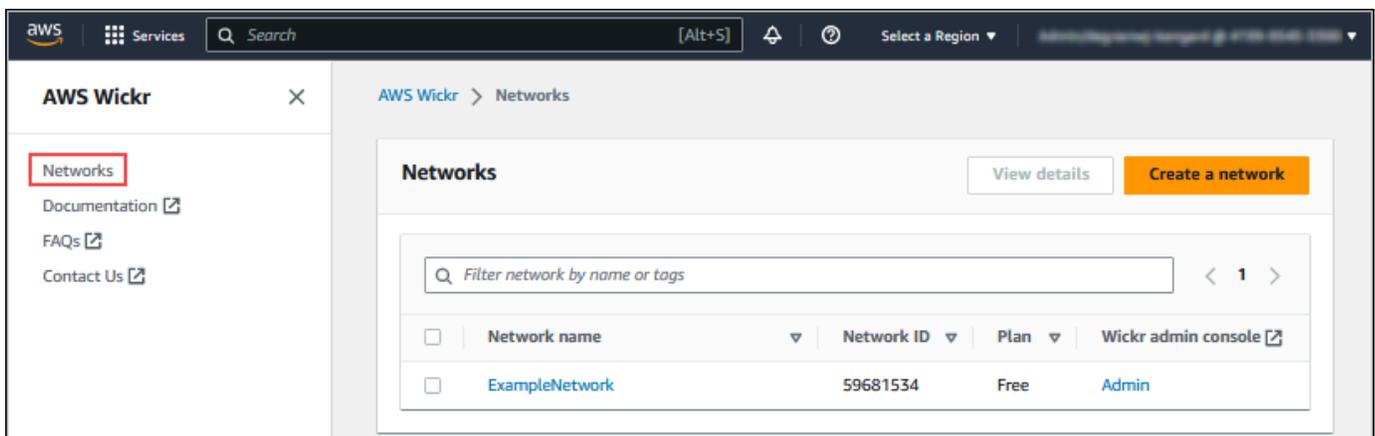
Vous pouvez appliquer des tags aux réseaux Wickr. Vous pouvez ensuite utiliser ces balises pour rechercher et filtrer vos réseaux Wickr ou suivre votre AWS coûts. Vous pouvez configurer les balises réseau sur la page d'aperçu du réseau du AWS Management Console pour Wickr.

Une balise est une [paire clé-valeur](#) appliquée à une ressource pour contenir les métadonnées relatives à cette ressource. Chaque balise est une étiquette composée d'une clé et d'une valeur. Pour plus d'informations sur les balises, voir également [Que sont les balises ?](#) et les [cas d'utilisation du balisage](#).

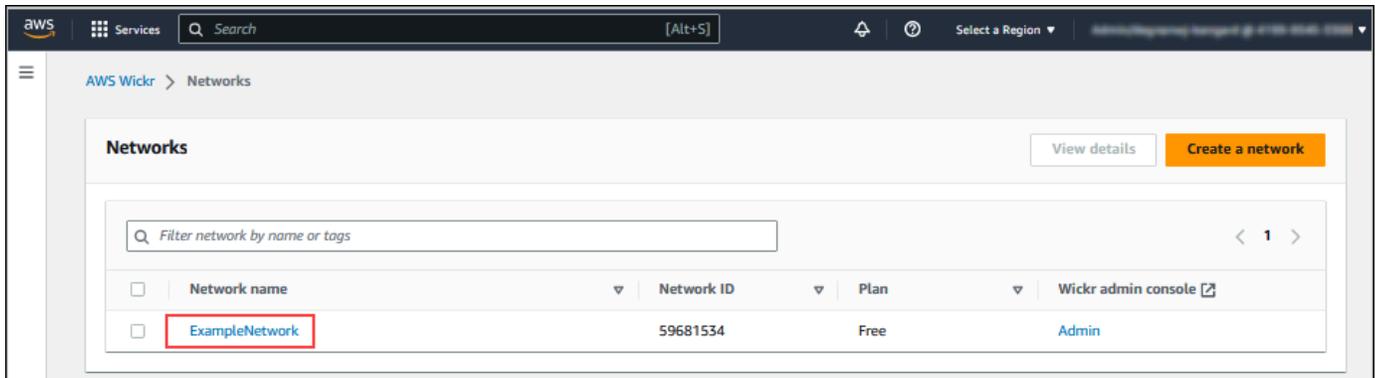
## Gérer les balises réseau

Suivez la procédure suivante pour gérer les balises réseau de votre réseau Wickr.

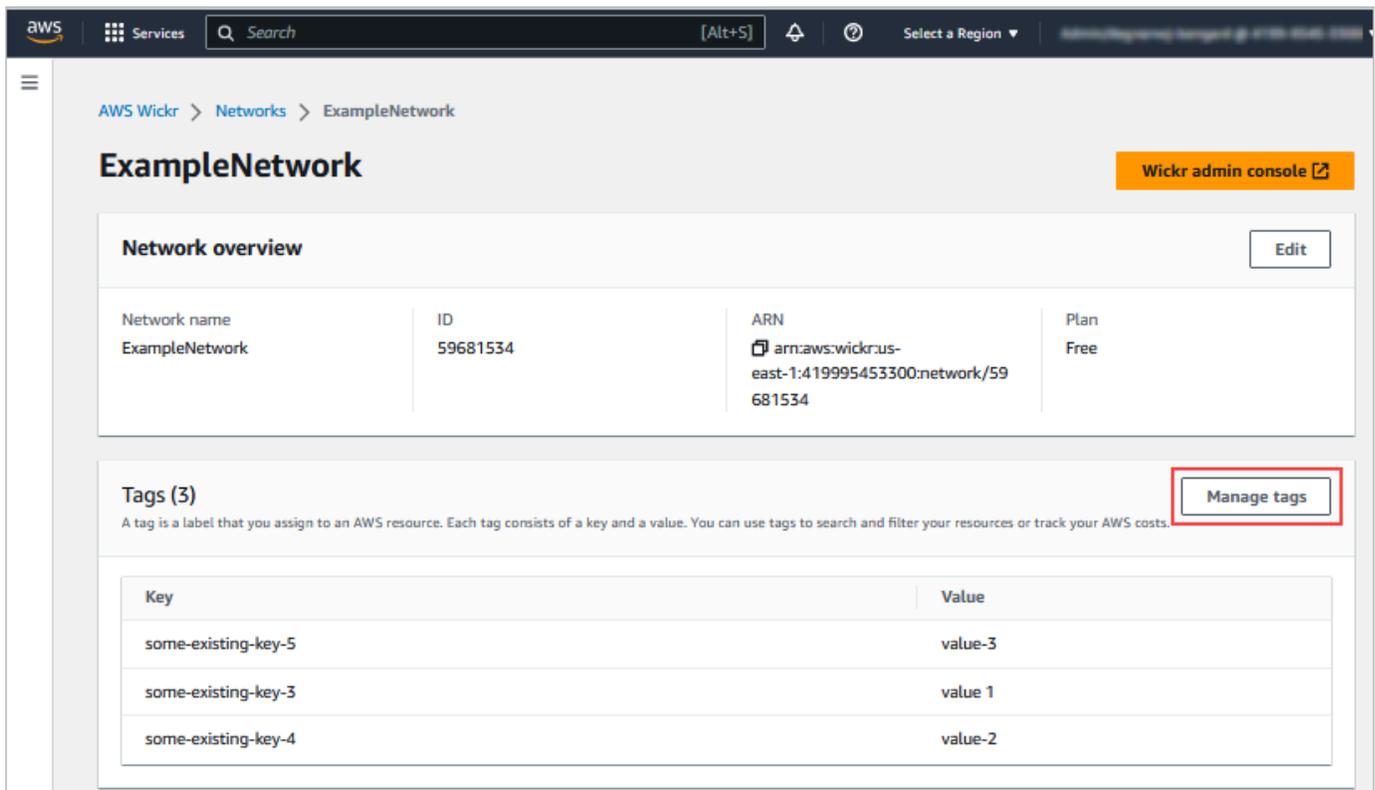
1. Ouvrez le fichier AWS Management Console pour Wickr Cat. <https://console.aws.amazon.com/wickr/>
2. Sélectionnez Réseaux dans le volet de navigation du AWS Management Console pour Wickr.



3. Sur la page Réseaux, choisissez le nom du réseau pour lequel vous souhaitez gérer les balises.



4. Sur la page d'aperçu du réseau, choisissez Gérer les balises.



5. Sur la page Gérer les balises, vous pouvez effectuer l'une des options suivantes :

- Ajouter de nouvelles balises — Entrez de nouvelles balises sous la forme d'une clé et d'une paire de valeurs. Choisissez Ajouter une nouvelle balise pour ajouter plusieurs paires clé-valeur. Les balises sont sensibles à la casse. Pour de plus amples informations, veuillez consulter [Ajouter un tag réseau](#).
- Modifier les balises existantes : sélectionnez le texte de clé ou de valeur d'une balise existante, puis entrez la modification dans la zone de texte. Pour de plus amples informations, veuillez consulter [Modifier un tag réseau](#).

- Supprimer les balises existantes : cliquez sur le bouton Supprimer qui se trouve à côté de la balise que vous souhaitez supprimer. Pour de plus amples informations, veuillez consulter [Supprimer un tag réseau](#).

## Ajouter un tag réseau

Suivez la procédure suivante pour ajouter un tag à votre réseau Wickr. Pour plus d'informations sur la gestion des balises, consultez [Gérer les balises réseau](#).

1. Sur la page Gérer les balises, choisissez Ajouter une nouvelle balise.
2. Dans les champs vides de clé et de valeur qui apparaissent, entrez la nouvelle clé et la nouvelle valeur de balise.
3. Choisissez Enregistrer les modifications pour enregistrer les nouvelles balises.

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

Key	Value - Required	
<input type="text" value="name-for-key"/>	<input type="text" value="value-for-key"/>	<input type="button" value="Remove"/>
<input type="text" value="some-existing-key-5"/>	<input type="text" value="value-3"/>	<input type="button" value="Remove"/>
<input type="text" value="some-existing-key-3"/>	<input type="text" value="value 1"/>	<input type="button" value="Remove"/>
<input type="text" value="some-existing-key-4"/>	<input type="text" value="value-2"/>	<input type="button" value="Remove"/>
<input type="text" value="Enter key"/>	<input type="text" value="Enter value"/>	<input type="button" value="Remove"/>

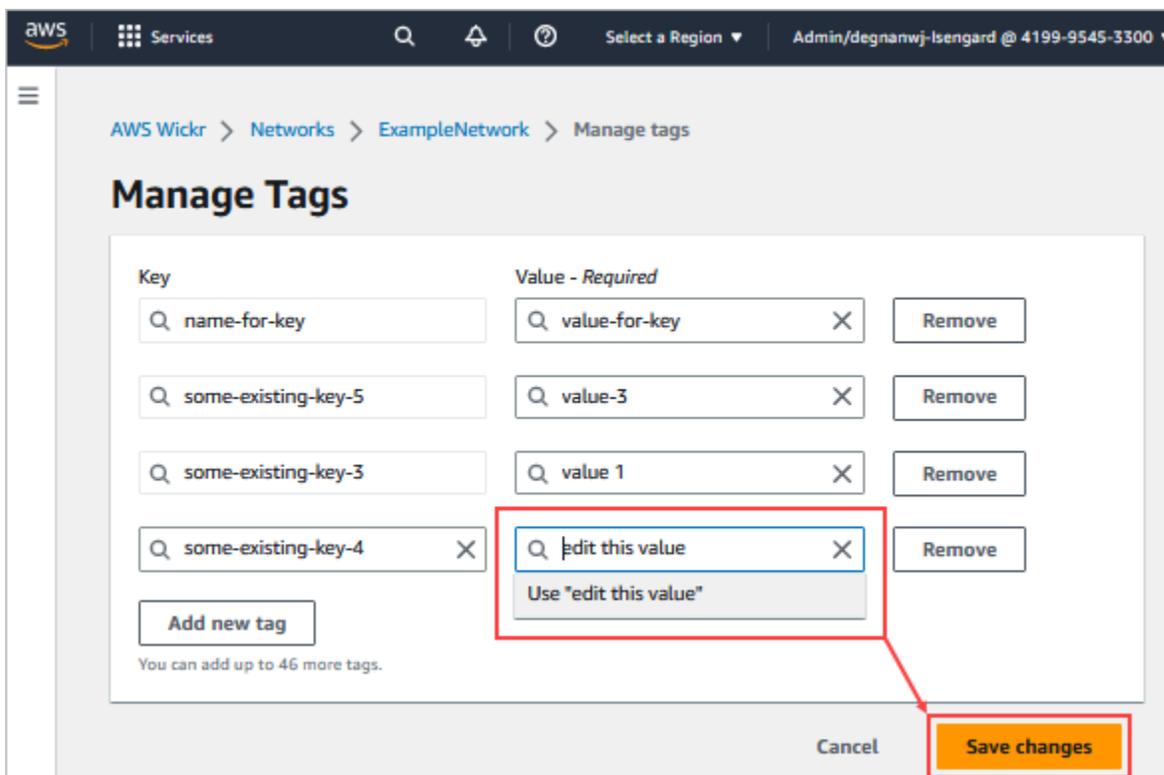
## Modifier un tag réseau

Suivez la procédure suivante pour modifier un tag associé à votre réseau Wickr. Pour plus d'informations sur la gestion des balises, consultez [Gérer les balises réseau](#).

1. Sur la page Gérer les balises, modifiez la valeur d'une balise.

### Note

Vous ne pouvez pas modifier la clé d'un tag. Supprimez plutôt la paire clé/valeur et ajoutez une nouvelle balise à l'aide de la nouvelle clé.

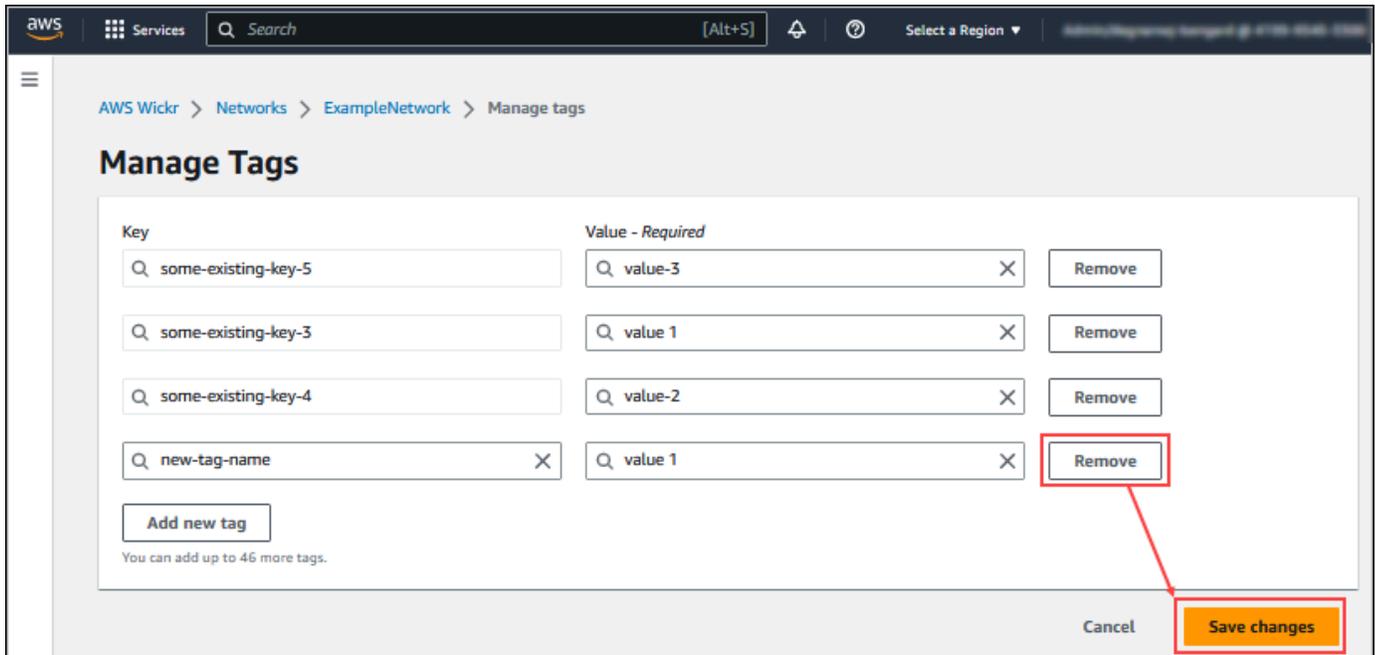


2. Choisissez Enregistrer les modifications pour enregistrer vos modifications.

## Supprimer un tag réseau

Effectuez la procédure suivante pour supprimer un tag de votre réseau Wickr. Pour plus d'informations sur la gestion des balises, consultez [Gérer les balises réseau](#).

1. Sur la page Gérer les balises, choisissez Supprimer pour la balise que vous souhaitez supprimer.



2. Choisissez Enregistrer les modifications pour enregistrer vos modifications.

## Gérer le plan réseau

Dans la section Gérer le plan du AWS Management Console pour Wickr, vous pouvez gérer votre plan réseau en fonction des besoins de votre entreprise.

Pour gérer votre plan réseau, procédez comme suit.

1. Ouvrez le fichier AWS Management Console pour Wickr Cat. <https://console.aws.amazon.com/wickr/>
2. Dans le volet de navigation de la console d'administration Wickr, choisissez Gérer le plan, puis sélectionnez Mon plan.
3. Sur la page Mon forfait, choisissez le forfait réseau de votre choix. Vous pouvez modifier votre plan réseau actuel en choisissant l'une des options suivantes :
  - Standard — Pour les équipes des petites et grandes entreprises qui ont besoin de contrôles administratifs et de flexibilité.

- Essai gratuit Premium ou Premium : pour les entreprises qui ont besoin des limites de fonctionnalités les plus élevées, de contrôles administratifs précis et de la conservation des données.

Les administrateurs peuvent choisir l'option d'essai gratuit premium, disponible pour un maximum de 30 utilisateurs et d'une durée de trois mois. Cette offre est ouverte aux nouveaux forfaits d'essai gratuits et aux forfaits standard. Les administrateurs peuvent passer à un forfait Premium ou Standard ou à un abonnement inférieur pendant la période d'essai gratuite Premium.

#### Note

Pour arrêter l'utilisation et la facturation sur votre réseau, supprimez tous les utilisateurs, y compris les utilisateurs suspendus de votre réseau.

## Limitations de l'essai gratuit Premium

Les restrictions suivantes s'appliquent à l'essai gratuit premium :

- Si un plan a déjà été inscrit à un essai gratuit premium auparavant, il ne sera pas éligible à un autre essai.
- Un seul réseau pour chaque AWS le compte peut être inscrit à un essai gratuit premium.
- La fonctionnalité d'utilisateur invité n'est pas disponible pendant l'essai gratuit Premium.
- Si un réseau standard compte plus de 30 utilisateurs, il ne sera pas possible de passer à un essai gratuit premium.

## Conservation des données

AWS La conservation des données Wickr permet de conserver toutes les conversations sur le réseau. Cela inclut les conversations par message direct et les conversations dans des groupes ou des salles entre les membres du réseau (internes) et ceux avec d'autres équipes (externes) avec lesquelles votre réseau est fédéré. La conservation des données n'est disponible que pour les utilisateurs du plan AWS Wickr Premium et les clients professionnels qui optent pour la conservation des données. Pour plus d'informations sur le plan Premium, consultez les tarifs de [Wickr](#)

Lorsqu'un administrateur réseau configure et active la conservation des données pour son réseau, tous les messages et fichiers partagés sur son réseau sont conservés conformément aux politiques de conformité de l'organisation. Ces sorties de fichiers .txt sont accessibles par l'administrateur réseau depuis un emplacement externe (par exemple : stockage local, compartiment Amazon S3 ou tout autre stockage selon le choix de l'utilisateur), d'où elles peuvent être analysées, effacées ou transférées.

#### Note

Wickr n'accède jamais à vos messages et à vos fichiers. Il est donc de votre responsabilité de configurer un système de conservation des données.

## Rubriques

- [Afficher les détails relatifs à la conservation des données](#)
- [Configuration de la conservation des données](#)
- [Obtenez les journaux de conservation des données](#)
- [Mesures et événements relatifs à la conservation des données](#)

## Afficher les détails relatifs à la conservation des données

Suivez la procédure suivante pour consulter les détails de conservation des données pour votre réseau Wickr. Vous pouvez également activer ou désactiver la conservation des données pour votre réseau Wickr.

1. Ouvrez le fichier AWS Management Console pour Wickr Cat. <https://console.aws.amazon.com/wickr/>
2. Choisissez Gérer le réseau.
3. Dans le volet de navigation de la console d'administration Wickr, choisissez Paramètres réseau, puis choisissez Conservation des données.

La page Conservation des données affiche les étapes de configuration de la conservation des données, ainsi que la possibilité d'activer ou de désactiver la fonctionnalité de conservation des données. Pour plus d'informations sur la configuration de la conservation des données, consultez [Configuration de la conservation des données](#).

**Note**

Lorsque la conservation des données est activée, un message indiquant que la conservation des données est activée sera visible pour tous les utilisateurs de votre réseau pour les informer de l'existence du réseau activé.

## Configuration de la conservation des données

Pour configurer la conservation des données pour votre réseau AWS Wickr, vous devez déployer l'image Docker du bot de conservation des données dans un conteneur sur un hôte, tel qu'un ordinateur local ou une instance dans Amazon Elastic Compute Cloud (Amazon EC2). Une fois le bot déployé, vous pouvez le configurer pour stocker les données localement ou dans un bucket Amazon Simple Storage Service (Amazon S3). Vous pouvez également configurer le bot de conservation des données pour utiliser d'autres AWS services tels que AWS Secrets Manager (Secrets Manager), Amazon CloudWatch (CloudWatch), Amazon Simple Notification Service (Amazon SNS) et (). AWS Key Management Service AWS KMS Les rubriques suivantes décrivent comment configurer et exécuter le bot de conservation des données pour votre réseau Wickr.

### Rubriques

- [Conditions préalables à la configuration de la conservation des données](#)
- [Mot de passe](#)
- [Options de stockage](#)
- [Variables d'environnement](#)
- [Les valeurs de Secrets Manager](#)
- [Politique IAM pour utiliser la conservation des données avec les services AWS](#)
- [Démarrez le bot de conservation des données](#)
- [Arrêtez le bot de conservation des données](#)

### Conditions préalables à la configuration de la conservation des données

Avant de commencer, vous devez obtenir le nom du bot de conservation des données (étiqueté comme nom d'utilisateur) et le mot de passe initial auprès de AWS Management Console for Wickr. Vous devez spécifier ces deux valeurs la première fois que vous démarrez le bot de conservation

des données. Vous devez également activer la conservation des données dans la console. Pour plus d'informations, consultez [Afficher les détails relatifs à la conservation des données](#).

## Mot de passe

La première fois que vous démarrez le bot de conservation des données, vous spécifiez le mot de passe initial à l'aide de l'une des options suivantes :

- La variable d'WICKRIO\_BOT\_PASSWORDenvironnement. Les variables d'environnement du bot de conservation des données sont décrites dans la [Variables d'environnement](#) section suivante de ce guide.
- La valeur du mot de passe dans Secrets Manager identifiée par la variable d'AWS\_SECRET\_NAMEenvironnement. Les valeurs de Secrets Manager pour le bot de conservation des données sont décrites dans la [Les valeurs de Secrets Manager](#) section suivante de ce guide.
- Entrez le mot de passe lorsque le bot de conservation des données vous le demande. Vous devrez exécuter le bot de conservation des données avec un accès TTY interactif à l'aide de l'-t option.

Un nouveau mot de passe sera généré lorsque vous configurerez le bot de conservation des données pour la première fois. Si vous devez réinstaller le bot de conservation des données, vous devez utiliser le mot de passe généré. Le mot de passe initial n'est pas valide après l'installation initiale du bot de conservation des données.

Le nouveau mot de passe généré sera affiché comme indiqué dans l'exemple suivant.

### Important

Conservez le mot de passe en lieu sûr. Si vous perdez le mot de passe, vous ne pourrez pas réinstaller le bot de conservation des données. Ne partagez pas ce mot de passe. Il permet de démarrer la conservation des données pour votre réseau Wickr.

```
*****
**** GENERATED PASSWORD
**** DO NOT LOSE THIS PASSWORD, YOU WILL NEED TO ENTER IT EVERY TIME
**** TO START THE BOT
"HuEXAMPLERAW4lGgEXAMPLen"
*****
```

## Options de stockage

Une fois la conservation des données activée et le bot de conservation des données configuré pour votre réseau Wickr, il capturera tous les messages et fichiers envoyés sur votre réseau. Les messages sont enregistrés dans des fichiers limités à une taille ou à une limite de temps spécifiques qui peuvent être configurées à l'aide d'une variable d'environnement. Pour plus d'informations, consultez [Variables d'environnement](#).

Vous pouvez configurer l'une des options suivantes pour stocker ces données :

- Stockez tous les messages et fichiers capturés localement. Il s'agit de l'option par défaut. Il est de votre responsabilité de déplacer les fichiers locaux vers un autre système pour un stockage à long terme et de vous assurer que le disque hôte ne manque pas de mémoire ou d'espace.
- Stockez tous les messages et fichiers capturés dans un compartiment Amazon S3. Le bot de conservation des données enregistre tous les messages et fichiers déchiffrés dans le compartiment Amazon S3 que vous spécifiez. Les messages et fichiers capturés sont supprimés de la machine hôte une fois qu'ils ont été correctement enregistrés dans le compartiment.
- Stockez tous les messages et fichiers capturés chiffrés dans un compartiment Amazon S3. Le bot de conservation des données chiffre à nouveau tous les messages et fichiers capturés à l'aide d'une clé que vous fournissez et les enregistre dans le compartiment Amazon S3 que vous spécifiez. Les messages et fichiers capturés sont supprimés de la machine hôte une fois qu'ils ont été correctement rechiffrés et enregistrés dans le compartiment. Vous aurez besoin d'un logiciel pour déchiffrer les messages et les fichiers.

Pour plus d'informations sur la création d'un compartiment Amazon S3 à utiliser avec votre bot de conservation des données, consultez la section [Création d'un compartiment](#) dans le guide de l'utilisateur Amazon S3

## Variables d'environnement

Vous pouvez utiliser les variables d'environnement suivantes pour configurer le bot de conservation des données. Vous définissez ces variables d'environnement à l'aide de l'-eoption lorsque vous exécutez l'image Docker du bot de conservation des données. Pour plus d'informations, consultez [Démarrez le bot de conservation des données](#).

 Note

Ces variables d'environnement sont facultatives, sauf indication contraire.

Utilisez les variables d'environnement suivantes pour spécifier les informations d'identification du bot de conservation des données :

- WICKRIO\_BOT\_NAME— Le nom du bot de conservation des données. Cette variable est obligatoire lorsque vous exécutez l'image Docker du bot de conservation des données.
- WICKRIO\_BOT\_PASSWORD— Le mot de passe initial du bot de conservation des données. Pour plus d'informations, consultez [Conditions préalables à la configuration de la conservation des données](#). Cette variable est obligatoire si vous ne prévoyez pas de démarrer le bot de conservation des données en demandant un mot de passe ou si vous ne prévoyez pas d'utiliser Secrets Manager pour stocker les informations d'identification du bot de conservation des données.

Utilisez les variables d'environnement suivantes pour configurer les fonctionnalités de streaming de conservation des données par défaut :

- WICKRIO\_COMP\_MSGDEST— Le nom du chemin d'accès au répertoire dans lequel les messages seront diffusés. La valeur par défaut est `/tmp/<botname>/compliance/messages`.
- WICKRIO\_COMP\_FILEDEST— Le nom du chemin d'accès au répertoire dans lequel les fichiers seront diffusés. La valeur par défaut est `/tmp/<botname>/compliance/attachments`.
- WICKRIO\_COMP\_BASENAME— Le nom de base des fichiers de messages reçus. La valeur par défaut est `receivedMessages`.
- WICKRIO\_COMP\_FILESIZE— La taille maximale d'un fichier de messages reçus en kibioctet (KiB). Un nouveau fichier est lancé lorsque la taille maximale est atteinte. La valeur par défaut est `1000000000`, comme dans 1024 GiB.
- WICKRIO\_COMP\_TIMEROTATE— Durée, en minutes, pendant laquelle le bot de conservation des données insère les messages reçus dans un fichier de messages reçus. Un nouveau fichier est lancé lorsque le délai est atteint. Vous ne pouvez utiliser la taille ou la durée du fichier que pour limiter la taille du fichier des messages reçus. La valeur par défaut est `0`, comme dans aucune limite.

Utilisez la variable d'environnement suivante pour définir la valeur par défaut Région AWS à utiliser.

- **AWS\_DEFAULT\_REGION**— La valeur par défaut Région AWS à utiliser pour AWS des services tels que Secrets Manager (non utilisée pour Amazon S3 ou AWS KMS). La `us-east-1` région est utilisée par défaut si cette variable d'environnement n'est pas définie.

Utilisez les variables d'environnement suivantes pour spécifier le secret Secrets Manager à utiliser lorsque vous choisissez d'utiliser Secrets Manager pour stocker les informations d'identification et les informations de AWS service du bot de conservation des données. Pour plus d'informations sur les valeurs que vous pouvez stocker dans Secrets Manager, consultez [Les valeurs de Secrets Manager](#).

- **AWS\_SECRET\_NAME**— Le nom du secret Secrets Manager qui contient les informations d'identification et AWS de service nécessaires au bot de conservation des données.
- **AWS\_SECRET\_REGION**— L'Région AWS endroit où se trouve le AWS secret. Si vous utilisez des AWS secrets et que cette valeur n'est pas définie, la **AWS\_DEFAULT\_REGION** valeur sera utilisée.

#### Note

Vous pouvez stocker toutes les variables d'environnement suivantes sous forme de valeurs dans Secrets Manager. Si vous choisissez d'utiliser Secrets Manager et que vous y stockez ces valeurs, vous n'avez pas besoin de les spécifier en tant que variables d'environnement lorsque vous exécutez l'image Docker du bot de conservation des données. Il vous suffit de spécifier la variable d'**AWS\_SECRET\_NAME** environnement décrite plus haut dans ce guide. Pour plus d'informations, consultez [Les valeurs de Secrets Manager](#).

Utilisez les variables d'environnement suivantes pour spécifier le compartiment Amazon S3 lorsque vous choisissez de stocker des messages et des fichiers dans un compartiment.

- **WICKRIO\_S3\_BUCKET\_NAME**— Le nom du compartiment Amazon S3 dans lequel les messages et les fichiers seront stockés.
- **WICKRIO\_S3\_REGION**— La AWS région du compartiment Amazon S3 dans laquelle les messages et les fichiers seront stockés.
- **WICKRIO\_S3\_FOLDER\_NAME**— Le nom du dossier facultatif dans le compartiment Amazon S3 où les messages et les fichiers seront stockés. Ce nom de dossier sera précédé de la clé pour les messages et les fichiers enregistrés dans le compartiment Amazon S3.

Utilisez les variables d'environnement suivantes pour spécifier les AWS KMS détails lorsque vous choisissez d'utiliser le chiffrement côté client pour rechiffrer les fichiers lorsque vous les enregistrez dans un compartiment Amazon S3.

- `WICKRIO_KMS_MSTRKEY_ARN`— Le nom de ressource Amazon (ARN) de la clé AWS KMS principale utilisée pour rechiffrer les fichiers de messages et les fichiers sur le bot de conservation des données avant qu'ils ne soient enregistrés dans le compartiment Amazon S3.
- `WICKRIO_KMS_REGION`— La AWS région où se trouve la clé AWS KMS principale.

Utilisez la variable d'environnement suivante pour spécifier les détails d'Amazon SNS lorsque vous choisissez d'envoyer des événements de rétention de données à une rubrique Amazon SNS. Les événements envoyés incluent le démarrage, l'arrêt, ainsi que les conditions d'erreur.

- `WICKRIO_SNS_TOPIC_ARN`— L'ARN de la rubrique Amazon SNS à laquelle vous souhaitez que les événements de conservation des données soient envoyés.

Utilisez la variable d'environnement suivante pour envoyer les métriques de conservation des données à CloudWatch. Si cela est spécifié, les métriques seront générées toutes les 60 secondes.

- `WICKRIO_METRICS_TYPE`— Définissez la valeur de cette variable d'environnement `cloudwatch` à laquelle envoyer les métriques CloudWatch.

## Les valeurs de Secrets Manager

Vous pouvez utiliser Secrets Manager pour stocker les informations d'identification du bot de conservation des données et les informations AWS de service. Pour plus d'informations sur la création d'un secret Secrets Manager, voir [Création d'un AWS Secrets Manager secret](#) dans le Guide de l'utilisateur de Secrets Manager.

Le secret Secrets Manager peut avoir les valeurs suivantes :

- `password`— Le mot de passe du bot de conservation des données.
- `s3_bucket_name`— Le nom du compartiment Amazon S3 dans lequel les messages et les fichiers seront stockés. Si ce n'est pas le cas, le streaming de fichiers par défaut sera utilisé.
- `s3_region`— La AWS région du compartiment Amazon S3 dans laquelle les messages et les fichiers seront stockés.

- `s3_folder_name`— Le nom du dossier facultatif dans le compartiment Amazon S3 où les messages et les fichiers seront stockés. Ce nom de dossier sera précédé de la clé pour les messages et les fichiers enregistrés dans le compartiment Amazon S3.
- `kms_master_key_arn`— L'ARN de la clé AWS KMS principale utilisée pour rechiffrer les fichiers de messages et les fichiers sur le bot de conservation des données avant qu'ils ne soient enregistrés dans le compartiment Amazon S3.
- `kms_region`— La AWS région où se trouve la clé AWS KMS principale.
- `sns_topic_arn`— L'ARN de la rubrique Amazon SNS à laquelle vous souhaitez que les événements de conservation des données soient envoyés.

## Politique IAM pour utiliser la conservation des données avec les services AWS

Si vous envisagez d'utiliser d'autres AWS services avec le bot de conservation des données Wickr, vous devez vous assurer que l'hôte dispose du rôle et de la politique AWS Identity and Access Management (IAM) appropriés pour y accéder. Vous pouvez configurer le bot de conservation des données pour utiliser Secrets Manager, Amazon S3 CloudWatch, Amazon SNS et AWS KMS. La politique IAM suivante permet d'accéder à des actions spécifiques pour ces services.

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

Vous pouvez créer une politique IAM plus stricte en identifiant les objets spécifiques pour chaque service auxquels vous souhaitez autoriser les conteneurs de votre hôte à accéder. Supprimez les actions relatives aux AWS services que vous n'avez pas l'intention d'utiliser. Par exemple, si

vous avez l'intention de n'utiliser qu'un compartiment Amazon S3, appliquez la politique suivante, qui supprime les `cloudwatch:PutMetricData` actions `secretsmanager:GetSecretValue` `sns:Publishkms:GenerateDataKey,,` et.

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

Si vous utilisez une instance Amazon Elastic Compute Cloud (Amazon EC2) pour héberger votre bot de conservation des données, créez un rôle IAM en utilisant le cas courant Amazon EC2 et attribuez une politique en utilisant la définition de politique ci-dessus.

## Démarrez le bot de conservation des données

Avant d'exécuter le bot de conservation des données, vous devez déterminer comment vous souhaitez le configurer. Si vous envisagez d'exécuter le bot sur un hôte qui :

- Vous n'aurez pas accès aux AWS services, vos options sont alors limitées. Dans ce cas, vous utiliserez les options de diffusion de messages par défaut. Vous devez décider si vous souhaitez limiter la taille des fichiers de messages capturés à une taille ou à un intervalle de temps spécifiques. Pour plus d'informations, consultez [Variables d'environnement](#).
- Si vous aurez accès aux AWS services, vous devez créer un secret Secrets Manager pour stocker les informations d'identification du bot et les détails de configuration des AWS services. Une fois les AWS services configurés, vous pouvez démarrer l'image Docker du bot de conservation des données. Pour plus d'informations sur les informations que vous pouvez stocker dans un secret de Secrets Manager, voir [Les valeurs de Secrets Manager](#)

Les sections suivantes présentent des exemples de commandes permettant d'exécuter l'image Docker du bot de conservation des données. Dans chacun des exemples de commandes, remplacez les valeurs d'exemple suivantes par les vôtres :

- `compliance_1234567890_bot` avec le nom de votre robot de conservation des données.
- `password` avec le mot de passe de votre robot de conservation des données.
- `wickr/data/retention/bot` avec le nom de votre secret Secrets Manager à utiliser avec votre bot de conservation des données.
- `bucket-name` avec le nom du compartiment Amazon S3 dans lequel les messages et les fichiers seront stockés.
- `folder-name` avec le nom du dossier dans le compartiment Amazon S3 dans lequel les messages et les fichiers seront stockés.
- `us-east-1` avec la AWS région de la ressource que vous spécifiez. Par exemple, la région de la clé AWS KMS principale ou la région du compartiment Amazon S3.
- `arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-a617-abababababab` avec l'Amazon Resource Name (ARN) de votre clé AWS KMS principale à utiliser pour rechiffrer les fichiers de messages et les fichiers.

Démarrez le bot avec une variable d'environnement de mot de passe (aucun AWS service)

La commande Docker suivante démarre le bot de conservation des données. Le mot de passe est spécifié à l'aide de la variable d'`WICKRIO_BOT_PASSWORD` environnement. Le bot commence à utiliser le streaming de fichiers par défaut et les valeurs par défaut définies dans la [Variables d'environnement](#) section de ce guide.

```
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
```

Démarrez le bot avec une demande de mot de passe (aucun AWS service)

La commande Docker suivante démarre le bot de conservation des données. Le mot de passe est saisi lorsque le bot de conservation des données vous le demande. Il commencera à utiliser le streaming de fichiers par défaut en utilisant les valeurs par défaut définies dans la [Variables d'environnement](#) section de ce guide.

```
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:*****
```

Exécutez le bot à l'aide de l'option `-ti` permettant de recevoir l'invite de mot de passe. Vous devez également exécuter la commande `docker attach <container ID or container name>` immédiatement après le démarrage de l'image docker afin de recevoir l'invite de mot de passe. Vous devez exécuter ces deux commandes dans un script. Si vous joignez l'image du docker et que vous ne voyez pas l'invite, appuyez sur Entrée pour afficher l'invite.

Démarrez le bot avec une rotation des fichiers de messages de 15 minutes (aucun AWS service)

La commande Docker suivante démarre le bot de conservation des données à l'aide de variables d'environnement. Il le configure également pour faire pivoter les fichiers de messages reçus à 15 minutes.

```
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
```

Démarrez le bot et spécifiez le mot de passe initial avec Secrets Manager

Vous pouvez utiliser le Secrets Manager pour identifier le mot de passe du bot de conservation des données. Lorsque vous démarrez le bot de conservation des données, vous devez définir une variable d'environnement qui indique le Secrets Manager dans lequel ces informations sont stockées.

```
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
```

Le `wickrpro/compliance/compliance_1234567890_bot` secret contient la valeur secrète suivante, affichée sous forme de texte brut.

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

Démarrez le bot et configurez Amazon S3 avec Secrets Manager

Vous pouvez utiliser le Secrets Manager pour héberger les informations d'identification et les informations du compartiment Amazon S3. Lorsque vous démarrez le bot de conservation des données, vous devez définir une variable d'environnement qui indique le Secrets Manager dans lequel ces informations sont stockées.

```
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
```

Le `wickrpro/compliance/compliance_1234567890_bot` secret contient la valeur secrète suivante, affichée sous forme de texte brut.

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

Les messages et les fichiers reçus par le bot seront placés dans le `bot-compliance` compartiment du dossier nommé `network1234567890`.

Démarrez le bot et configurez Amazon S3 et AWS KMS avec Secrets Manager

Vous pouvez utiliser le Secrets Manager pour héberger les informations d'identification, le compartiment Amazon S3 et les informations relatives à la clé AWS KMS principale. Lorsque vous démarrez le bot de conservation des données, vous devez définir une variable d'environnement qui indique le Secrets Manager dans lequel ces informations sont stockées.

```
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
```

Le `wickrpro/compliance/compliance_1234567890_bot` secret contient la valeur secrète suivante, affichée sous forme de texte brut.

```
{
  "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"
}
```

Les messages et les fichiers reçus par le bot seront chiffrés à l'aide de la clé KMS identifiée par la valeur ARN, puis placés dans le compartiment « bot-compliance » dans le dossier nommé « network1234567890 ». Assurez-vous de disposer de la configuration de politique IAM appropriée.

Démarrez le bot et configurez Amazon S3 à l'aide de variables d'environnement

Si vous ne souhaitez pas utiliser Secrets Manager pour héberger les informations d'identification du bot de conservation des données, vous pouvez démarrer l'image Docker du bot de conservation des données avec les variables d'environnement suivantes. Vous devez identifier le nom du bot de conservation des données à l'aide de la variable d'environnement `WICKRIO_BOT_NAME`.

```
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
```

Vous pouvez utiliser les valeurs d'environnement pour identifier les informations d'identification du bot de conservation des données, les informations sur les compartiments Amazon S3 et les informations de configuration pour le streaming de fichiers par défaut.

## Arrêtez le bot de conservation des données

Le logiciel exécuté sur le bot de conservation des données capturera les SIGTERM signaux et s'arrêtera harmonieusement. Utilisez la `docker stop <container ID or container name>` commande, comme indiqué dans l'exemple suivant, pour envoyer la SIGTERM commande à l'image Docker du bot de conservation des données.

```
docker stop compliance_1234567890_bot
```

## Obtenez les journaux de conservation des données

Le logiciel exécuté sur l'image Docker du bot de conservation des données sera affiché dans les fichiers journaux du `/tmp/<botname>/logs` répertoire. Ils tourneront jusqu'à un maximum de 5 fichiers. Vous pouvez obtenir les journaux en exécutant la commande suivante.

```
docker logs <botname>
```

Exemple :

```
docker logs compliance_1234567890_bot
```

## Mesures et événements relatifs à la conservation des données

Vous trouverez ci-dessous les métriques Amazon CloudWatch (CloudWatch) et les événements Amazon Simple Notification Service (AmazonSNS) actuellement pris en charge par la version 5.116 du bot de conservation des données AWS Wickr.

Rubriques

- [CloudWatch métriques](#)
- [SNS Événements Amazon](#)

### CloudWatch métriques

Les métriques sont générées par le bot à intervalles d'une minute et transmises au CloudWatch service associé au compte sur lequel l'image Docker du bot de conservation des données est exécutée.

Vous trouverez ci-dessous les mesures existantes prises en charge par le bot de conservation des données.

Métrique	Description
Messages_Rx	Messages reçus.
Messages_Rx_Failed	Échec du traitement des messages reçus.
Messages enregistrés	Messages enregistrés dans le fichier des messages reçus.
Messages_enregistrés_échoués	Impossible d'enregistrer les messages dans le fichier des messages reçus.
Fichiers_enregistrés	Fichiers reçus.
Fichiers_enregistrés_octets	Nombre d'octets pour les fichiers reçus.
Les fichiers enregistrés ont échoué	Échec de l'enregistrement des fichiers.
Connexions	Connexions (normalement, ce sera 1 pour chaque intervalle).
Échecs de connexion	Échec de connexion (normalement, ce sera 1 pour chaque intervalle).
S3_Post_Errors	Erreurs lors de la publication de fichiers de messages et de fichiers dans le compartiment Amazon S3.
Watchdog_Failures	Défaillances de Watchdog.
Watchdog_Warnings	Avertissements de Watchdog.

Les métriques sont générées pour être consommées par CloudWatch. L'espace de noms utilisé pour les robots est `WickrIO`. Chaque métrique possède un ensemble de dimensions. Vous trouverez ci-dessous la liste des dimensions publiées avec les statistiques ci-dessus.

Dimension	Valeur
Id	Le nom d'utilisateur du bot.
Appareil	Description d'un appareil ou d'une instance de bot spécifique. Utile si vous utilisez plusieurs appareils ou instances de bot.
Produit (langue française non garantie)	Le produit pour le bot. Peut être <code>WickrPro_</code> ou <code>WickrEnterprise_</code> avec <code>AlphaBeta</code> , ou <code>Production</code> ajouté.
BotType	Le type de bot. Labellisé Conformité pour les robots de conformité.
Réseau	L'ID du réseau associé.

## SNS Événements Amazon

Les événements suivants sont publiés dans le SNS sujet Amazon défini par la valeur Amazon Resource Name (ARN) identifiée à l'aide de la variable d'`WICKRIO_SNS_TOPIC_ARN` environnement ou de la valeur secrète de `sns_topic_arn` Secrets Manager. Pour plus d'informations, consultez [Variables d'environnement](#) et [Les valeurs de Secrets Manager](#).

Les événements générés par le bot de conservation des données sont envoyés sous forme de JSON chaînes. Les valeurs suivantes sont incluses dans les événements à partir de la version 5.116 du bot de conservation des données.

Nom	Valeur
<code>complianceBot</code>	Le nom d'utilisateur du bot de conservation des données.
<code>dateTime</code>	Date et heure auxquelles l'événement s'est produit.

Nom	Valeur
appareil	Description de l'appareil ou de l'instance de bot spécifique. Utile si vous exécutez plusieurs instances de bot.
dockerImage	L'image Docker associée au bot.
dockerTag	Le tag ou la version de l'image Docker.
message	Le message de l'événement. Pour plus d'informations, consultez <a href="#">Événements critiques</a> et <a href="#">Événements normaux</a> .
notificationType	Cette valeur sera Bot Event.
severity	La gravité de l'événement. Peut être normal ou critical.

Vous devez vous abonner à la SNS rubrique Amazon pour pouvoir recevoir les événements. Si vous vous abonnez à l'aide d'une adresse e-mail, un e-mail contenant des informations similaires à celles de l'exemple suivant vous sera envoyé.

```
{
  "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"
}
```

## Événements critiques

Ces événements provoqueront l'arrêt ou le redémarrage du bot. Le nombre de redémarrages est limité afin d'éviter de provoquer d'autres problèmes.

## Échecs de connexion

Voici les événements possibles qui peuvent être générés lorsque le bot ne parvient pas à se connecter. Chaque message indiquera la raison de l'échec de connexion.

Type d'événement	Message d'événement
échec de connexion	Mauvaises informations d'identification. Vérifiez le mot de passe.
échec de connexion	L'utilisateur est introuvable.
échec de connexion	Le compte ou l'appareil est suspendu.
allocation	L'utilisateur a quitté la commande.
allocation	Mauvais mot de passe pour le <code>config.wickr</code> fichier.
allocation	Impossible de lire le <code>config.wickr</code> fichier.
échec de connexion	Toutes les connexions ont échoué.
échec de connexion	Nouvel utilisateur mais la base de données existe déjà.

### Plus d'événements critiques

Type d'événement	Messages d'événements
Compte suspendu	WickrIOClient Main : : slotAdminUser Suspend : code (%1) : raison : %2 »
BotDevice Suspendu	L'appareil est suspendu !
WatchDog	Le SwitchBoard système est en panne depuis plus de <code>&lt;N&gt;</code> minutes
Défaillances S3	Impossible de mettre le fichier <code>&lt;file-name &gt;&gt;</code> sur le compartiment S3. Erreur : <code>&lt;AWS-error &gt;</code>

Type d'événement	Messages d'événements
Clé de secours	SERVERSUBMITTEDFALLBACKKEY: Il ne s'agit pas d'une clé de secours active reconnue par le client. Veuillez envoyer les journaux à l'ingénierie de bureau.

## Evénements normaux

Vous trouverez ci-dessous les événements qui vous avertissent des événements de fonctionnement normaux. Un trop grand nombre d'événements de ce type au cours d'une période donnée peut être source de préoccupation.

### Appareil ajouté au compte

Cet événement est généré lorsqu'un nouvel appareil est ajouté au compte du bot de conservation des données. Dans certaines circonstances, cela peut être une indication importante que quelqu'un a créé une instance du bot de conservation des données. Voici le message de cet événement.

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

### Bot connecté

Cet événement est généré lorsque le bot s'est connecté avec succès. Voici le message de cet événement.

```
Logged in
```

### Arrêt

Cet événement est généré lorsque le bot s'arrête. Si l'utilisateur ne l'a pas explicitement initié, cela peut être le signe d'un problème. Voici le message de cet événement.

```
Shutting down
```

### Mises à jour disponibles

Cet événement est généré lorsque le bot de conservation des données est démarré et il indique qu'une version plus récente de l'image Docker associée est disponible. Cet événement est généré

au démarrage du bot, et sur une base quotidienne. Cet événement inclut le champ du `versions` tableau qui identifie les nouvelles versions disponibles. Voici un exemple de ce à quoi ressemble cet événement.

```
{
  "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"
  ]
}
```

## Qu'est-ce qu'ATAK ?

L'Android Team Awareness Kit (ATAK), ou Android Tactical Assault Kit (également ATAK) à usage militaire, est une infrastructure géospatiale pour téléphones intelligents et une application de connaissance de la situation qui permettent une collaboration sécurisée sur tout le territoire. Bien qu'il ait été initialement conçu pour être utilisé dans les zones de combat, l'ATAK a été adapté aux missions des agences locales, étatiques et fédérales.

### Rubriques

- [Activez ATAK dans le tableau de bord du réseau Wickr](#)
- [Informations supplémentaires sur ATAK](#)
- [Installez et associez le plugin Wickr pour ATAK](#)
- [Composez et recevez un appel](#)
- [Envoyer un fichier](#)
- [Envoyer un message vocal sécurisé \(Push-to-talk\)](#)
- [Moulinet \(accès rapide\)](#)
- [Navigation](#)

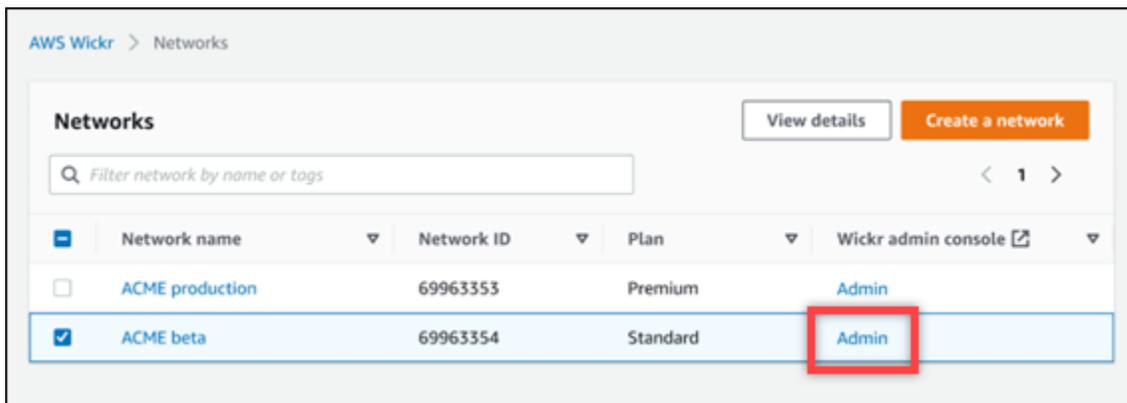
## Activez ATAK dans le tableau de bord du réseau Wickr

AWS Wickr prend en charge de nombreuses agences qui utilisent Android Tactical Assault Kit (ATAK). Cependant, jusqu'à présent, les opérateurs ATAK qui utilisent Wickr devaient quitter l'application pour le faire. Pour aider à réduire les perturbations et les risques opérationnels, Wickr a développé un plugin qui améliore ATAK avec des fonctionnalités de communication sécurisées. Avec le plugin Wickr pour ATAK, les utilisateurs peuvent envoyer des messages, collaborer et transférer des fichiers sur Wickr au sein de l'application ATAK. Cela élimine les interruptions et la complexité de la configuration grâce aux fonctionnalités de chat d'ATAK.

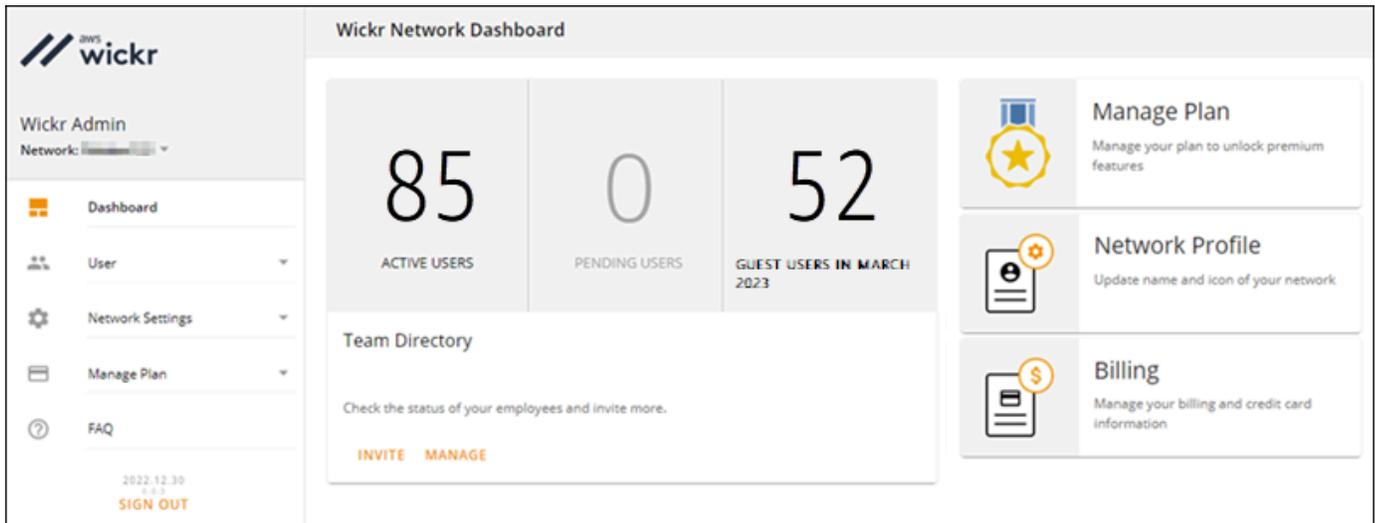
## Activez ATAK dans le tableau de bord du réseau Wickr

Suivez la procédure suivante pour activer ATAK dans le tableau de bord du réseau Wickr.

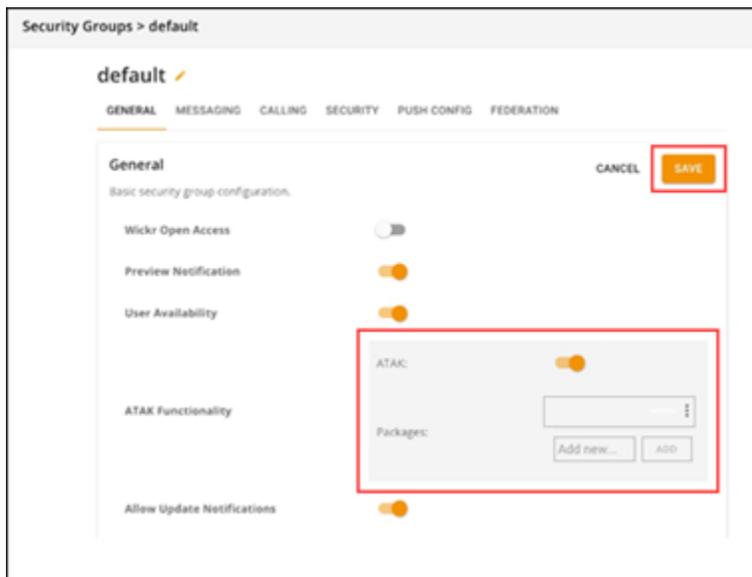
1. Ouvrez le AWS Management Console pour Wickr à l'adresse <https://console.aws.amazon.com/wickr/>.
2. Sur la page Réseaux, choisissez le lien Admin pour accéder à la console d'administration Wickr pour ce réseau.



Vous êtes redirigé vers la console d'administration Wickr pour un réseau spécifique.



3. Dans le volet de navigation de la console d'administration Wickr, choisissez Network Settings, puis Security Group.
4. Choisissez Détails à côté du groupe de sécurité pour lequel vous souhaitez activer ATAK.
5. Sous l'onglet General, choisissez Edit.
6. Dans la section Fonctionnalité ATAK :
  - a. Entrez le nom du package dans la zone de texte Packages. Vous pouvez entrer l'une des valeurs suivantes en fonction de la version de l'ATAK que vos utilisateurs vont installer et utiliser :
    - `com.atakmap.app.civ`— Entrez cette valeur dans la zone de texte Packages si vos utilisateurs finaux de Wickr veulent installer et utiliser la version civile de l'application ATAK sur leurs appareils Android.
    - `com.atakmap.app.mil`— Entrez cette valeur dans la zone de texte Packages si vos utilisateurs finaux de Wickr veulent installer et utiliser la version militaire de l'application ATAK sur leurs appareils Android.
  - b. Faites glisser le bouton ATAK vers la droite pour activer la fonctionnalité.
  - c. Choisissez Enregistrer.



ATAK est désormais activé pour le réseau Wickr sélectionné et le groupe de sécurité sélectionné. Vous devez demander aux utilisateurs Android du groupe de sécurité pour lequel vous avez activé la fonctionnalité ATAK d'installer le plugin Wickr pour ATAK. Pour plus d'informations, consultez [Installer et associer le plugin Wickr ATAK](#).

## Informations supplémentaires sur ATAK

Pour plus d'informations sur le plugin Wickr pour ATAK, consultez ce qui suit :

- [Présentation du plugin Wickr ATAK](#)
- [Informations supplémentaires sur le plugin Wickr ATAK](#)

## Installez et associez le plugin Wickr pour ATAK

L'Android Team Awareness Kit (ATAK) est une solution Android utilisée par les agences militaires, étatiques et gouvernementales américaines qui ont besoin de capacités de connaissance de la situation pour la planification, l'exécution et la réponse aux incidents des missions. ATAK possède une architecture de plugins qui permet aux développeurs d'ajouter des fonctionnalités. Il permet aux utilisateurs de naviguer à l'aide du GPS et de données cartographiques géospatiales superposées à une connaissance situationnelle en temps réel des événements en cours. Dans ce document, nous vous montrons comment installer le plugin Wickr pour ATAK sur un appareil Android et le coupler

avec le client Wickr. Cela vous permet d'envoyer des messages et de collaborer sur Wickr sans quitter l'application ATAK.

## Installez le plugin Wickr pour ATAK

Suivez la procédure ci-dessous pour installer le plugin Wickr pour ATAK sur un appareil Android.

1. Accédez au Google Play Store et installez le plugin Wickr pour ATAK.
2. Ouvrez l'application ATAK sur votre appareil Android.
3. Dans l'application ATAK, choisissez l'icône du menu  en haut à droite de l'écran, puis choisissez Plugins.
4. Choisissez Import (Importer).
5. Dans la fenêtre contextuelle Select Import Type, choisissez Local SD et accédez à l'endroit où vous avez enregistré le plugin Wickr pour le fichier .apk ATAK.
6. Choisissez le fichier du plugin et suivez les instructions pour l'installer.

### Note

Si vous êtes invité à envoyer le fichier du plug-in pour analyse, choisissez Non.

7. L'application ATAK vous demandera si vous souhaitez charger le plugin. Choisissez OK.

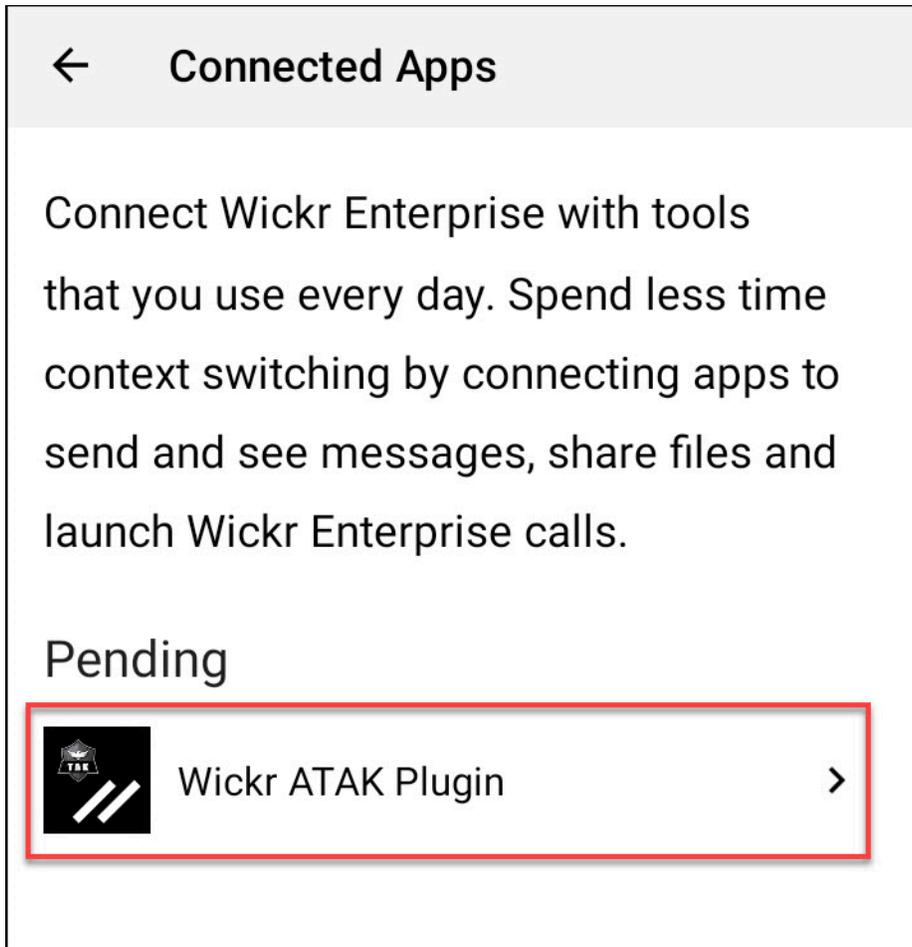
Le plugin Wickr pour ATAK est maintenant installé. Passez à la section suivante Associer ATAK à Wickr pour terminer le processus.

## Associez ATAK à Wickr

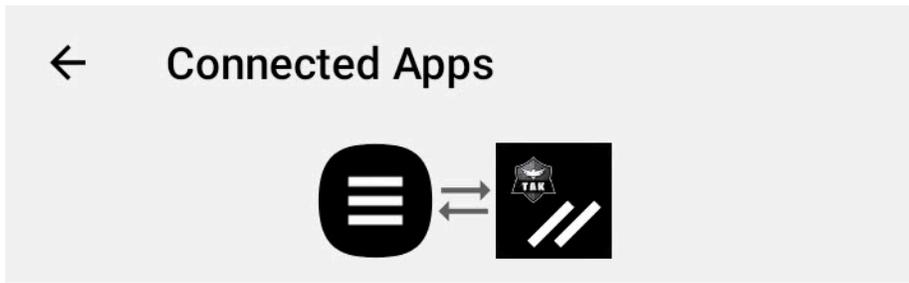
Effectuez la procédure suivante pour associer l'application ATAK à Wickr après avoir correctement installé le plugin Wickr pour ATAK.

1. Dans l'application ATAK, choisissez l'icône du menu  en haut à droite de l'écran, puis choisissez Wickr Plugin.
2. Choisissez Pair Wickr.

Une invite de notification apparaîtra vous demandant de vérifier les autorisations du plugin Wickr pour ATAK. Si l'invite de notification n'apparaît pas, ouvrez le client Wickr et accédez à Paramètres, puis à Applications connectées. Vous devriez voir le plugin dans la section En attente de l'écran.



3. Choisissez Approuver pour jumeler.
4. Choisissez le bouton Open Wickr ATAK Plugin pour revenir à l'application ATAK.



## Success

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

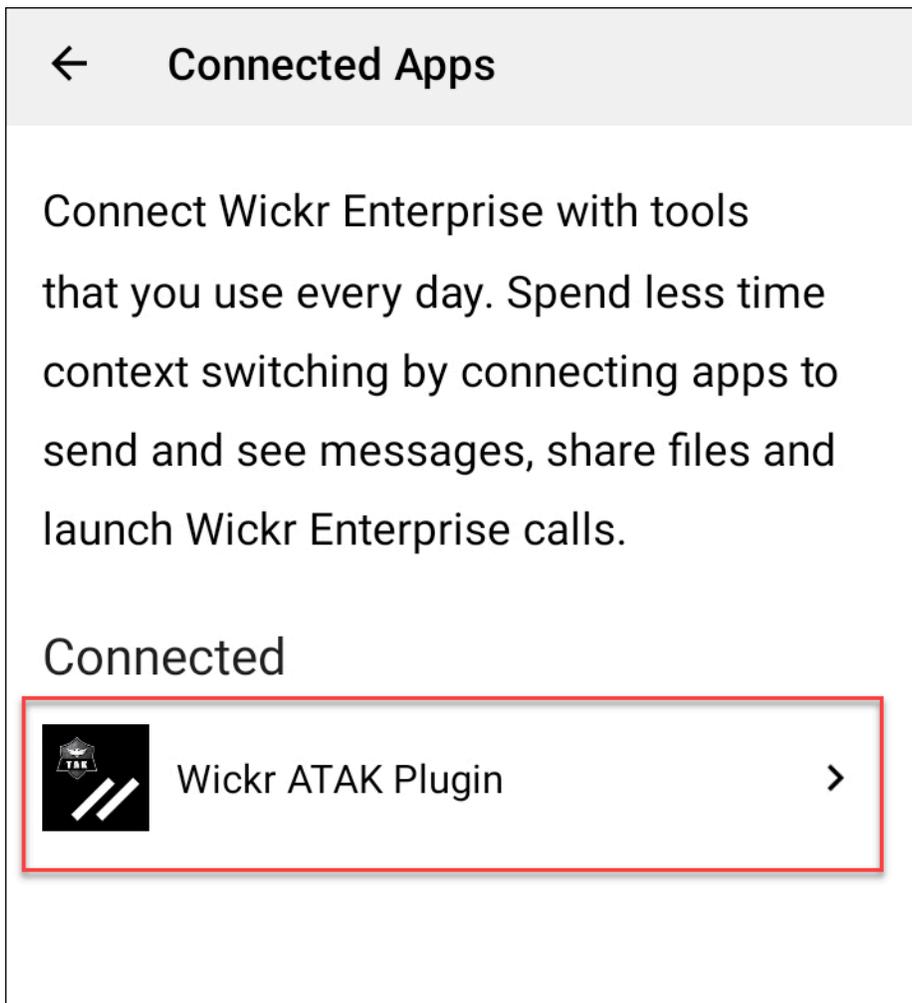


Vous avez maintenant couplé avec succès le plugin ATAK et Wickr, et vous pouvez utiliser le plugin pour envoyer des messages et collaborer à l'aide de Wickr sans quitter l'application ATAK.

## Dissocier ATAK avec Wickr

Effectuez la procédure suivante pour dissocier le plugin ATAK de Wickr.

1. Dans l'application native, choisissez Paramètres, puis Applications connectées.
2. Sur l'écran Connected Apps, choisissez Wickr ATAK Plugin.



3. Sur l'écran du plugin Wickr ATAK, choisissez Supprimer en bas de l'écran.

Un écran de confirmation indique que vous n'utilisez plus l'API. Vous venez de dissocier avec succès le plugin ATAK.

## Composez et recevez un appel

Vous pouvez composer et recevoir un appel dans le plugin Wickr pour ATAK.

Procédez comme suit pour composer un numéro et recevoir un appel.

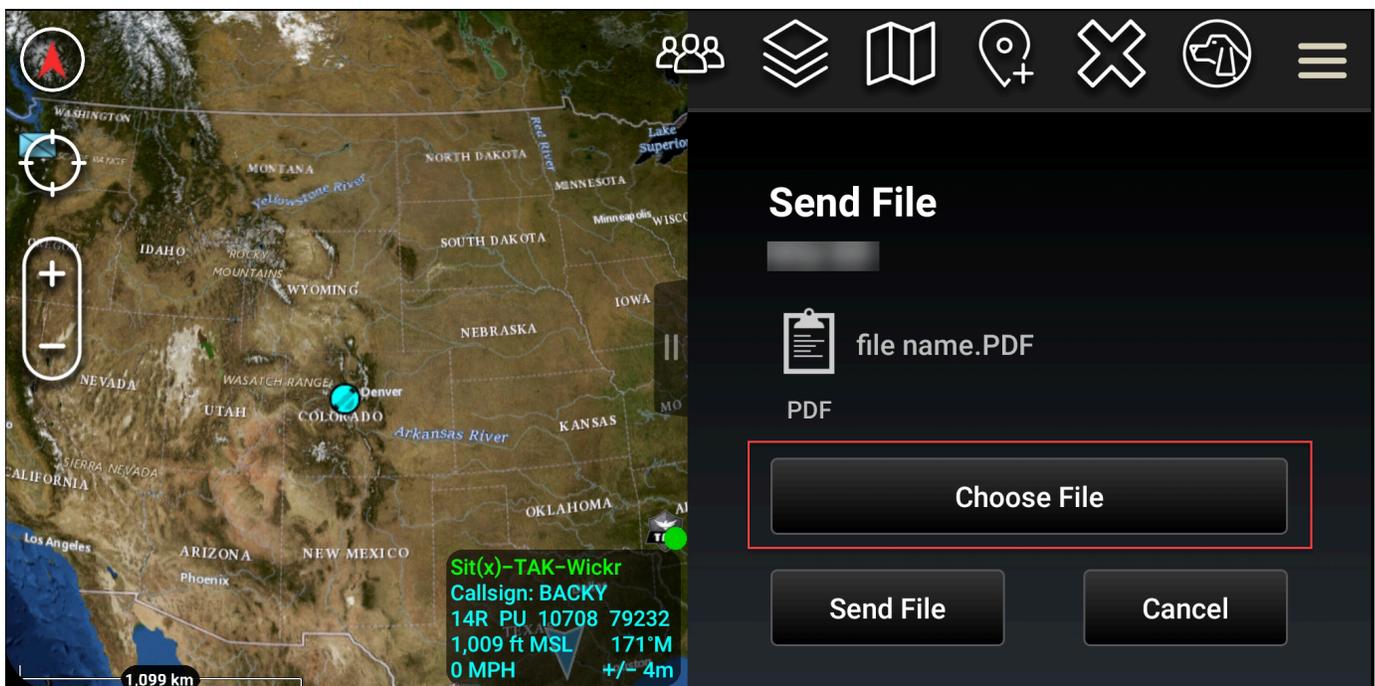
1. Ouvrez une fenêtre de discussion.
2. Dans la vue Carte, choisissez l'icône de l'utilisateur que vous souhaitez appeler.
3. Choisissez l'icône du téléphone en haut à droite de l'écran.
4. Une fois connecté, vous pouvez revenir à la vue du plugin ATAK et recevoir un appel.

## Envoyer un fichier

Vous pouvez envoyer un fichier dans le plugin Wickr pour ATAK.

Pour envoyer un fichier, procédez comme suit.

1. Ouvrez une fenêtre de discussion.
2. Dans la vue Carte, recherchez l'utilisateur auquel vous souhaitez envoyer un fichier.
3. Lorsque vous trouvez l'utilisateur auquel vous souhaitez envoyer un fichier, sélectionnez son nom.
4. Sur l'écran Envoyer un fichier, sélectionnez Choisir un fichier, puis naviguez jusqu'au fichier que vous souhaitez envoyer.



5. Dans la fenêtre du navigateur, sélectionnez le fichier souhaité.
6. Sur l'écran Envoyer un fichier, choisissez Envoyer un fichier.

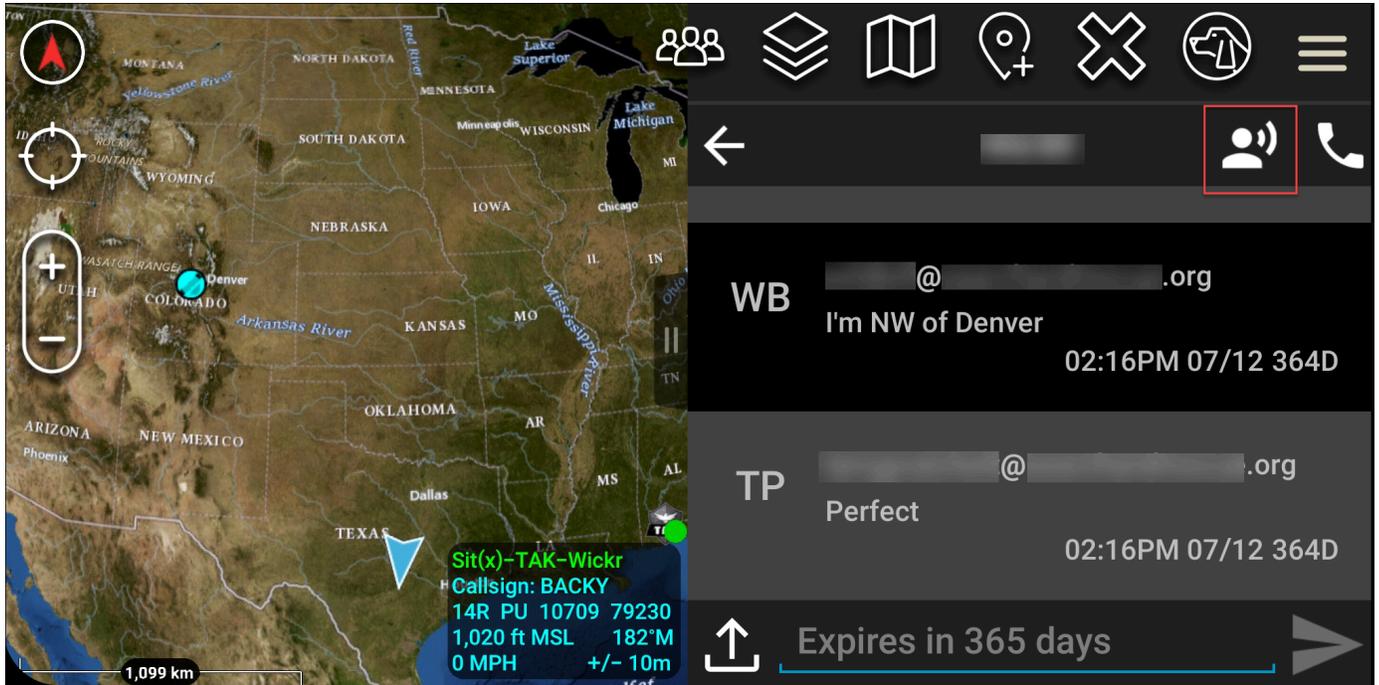
L'icône de téléchargement s'affiche, indiquant que le fichier sélectionné est en cours de téléchargement.

## Envoyer un message vocal sécurisé (Push-to-talk)

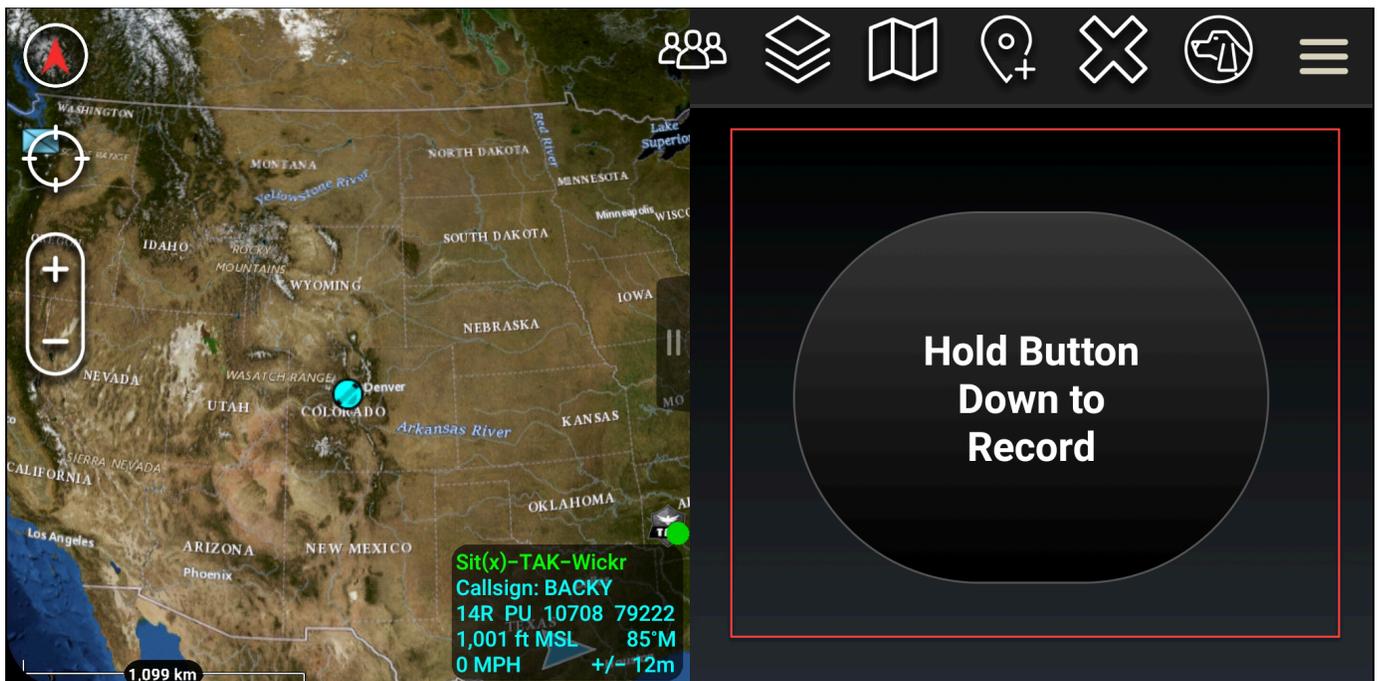
Vous pouvez envoyer un message vocal sécurisé (Push-to-talk) dans le plugin Wickr pour ATAK.

Procédez comme suit pour envoyer un message vocal sécurisé.

1. Ouvrez une fenêtre de discussion.
2. Choisissez l'icône Push-to-Talk en haut de l'écran, indiquée par l'icône représentant une personne en train de parler.



3. Sélectionnez le bouton Maintenir enfoncé pour enregistrer et maintenez-le enfoncé.



4. Enregistrez votre message.

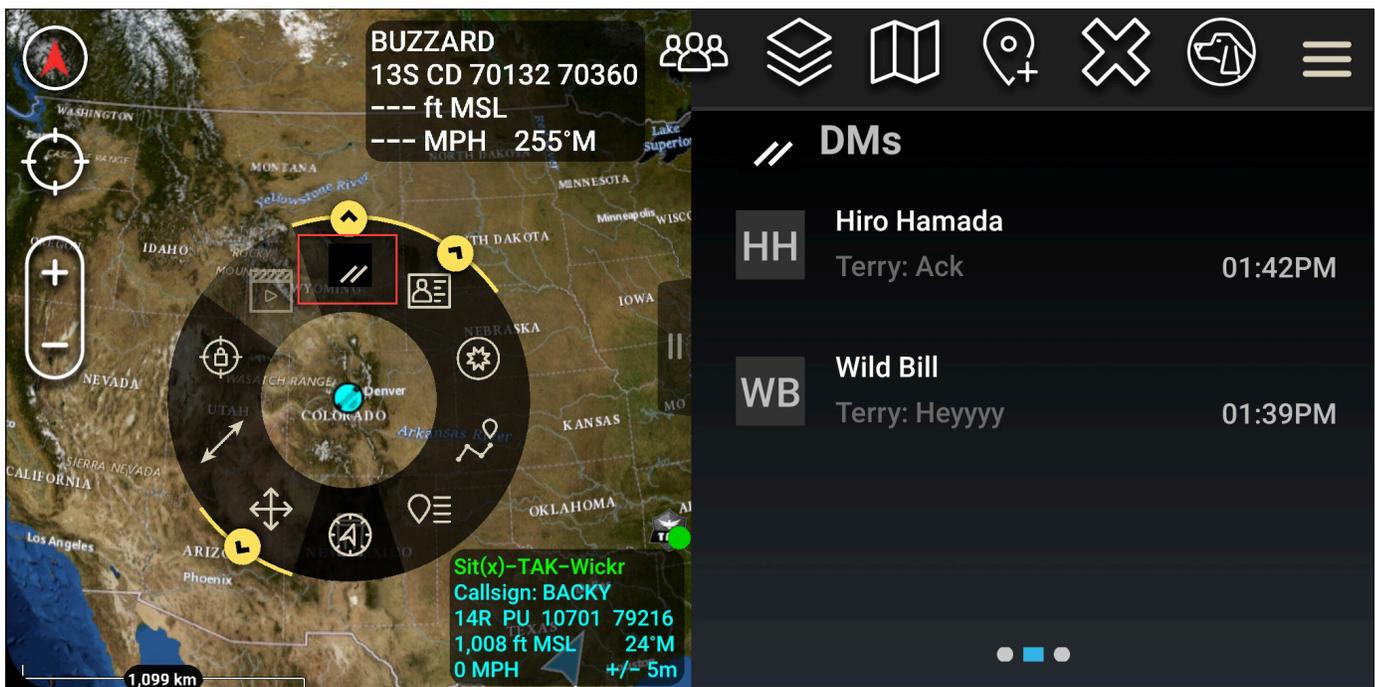
- Après avoir enregistré votre message, relâchez le bouton pour l'envoyer.

## Moulinet (accès rapide)

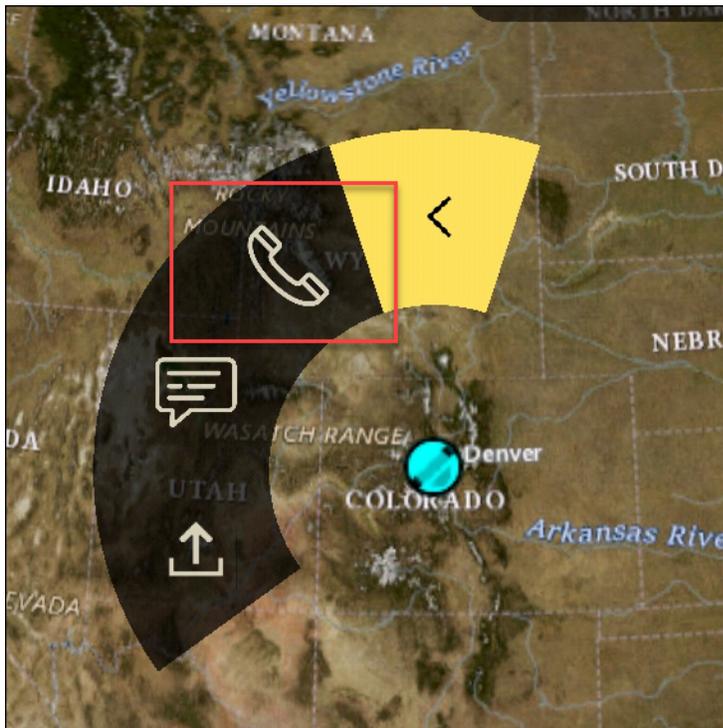
Le moulinet ou fonction d'accès rapide est utilisé pour les one-one-one conversations ou les messages directs.

Pour utiliser le moulinet, procédez comme suit.

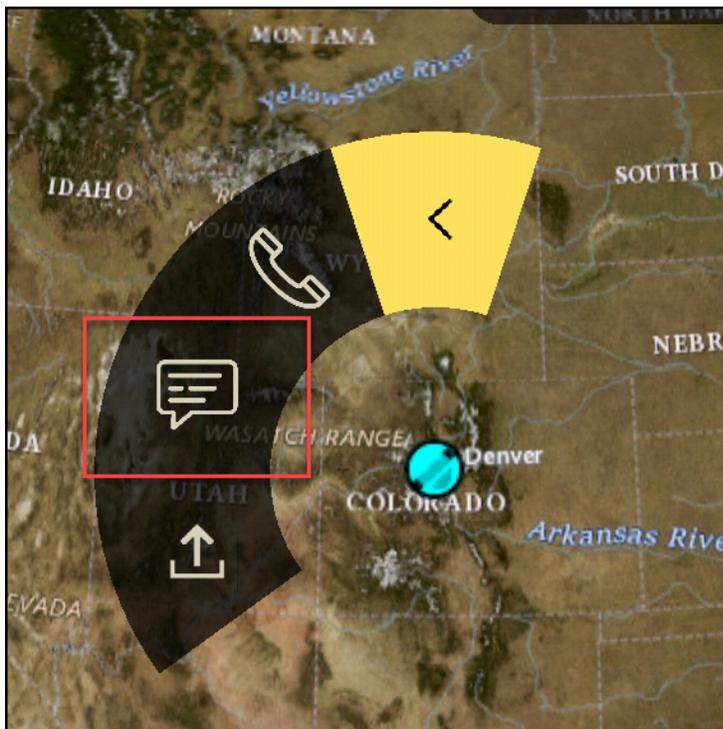
- Ouvrez simultanément la vue en écran partagé de la carte ATAK et du plugin Wickr for ATAK. La carte affiche vos coéquipiers ou vos actifs sur la vue cartographique.
- Cliquez sur l'icône de l'utilisateur pour ouvrir le moulinet.
- Cliquez sur l'icône Wickr pour afficher les options disponibles pour l'utilisateur sélectionné.



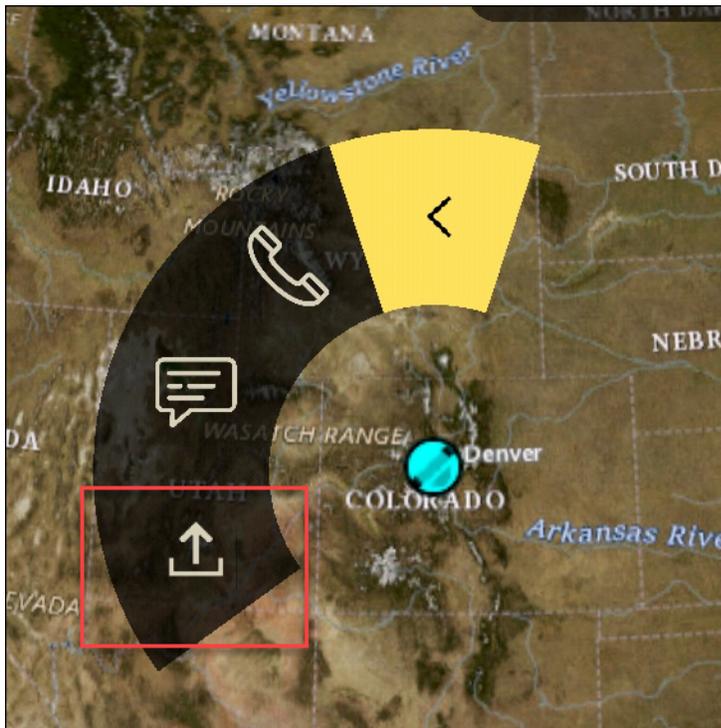
- Sur le moulinet, choisissez l'une des icônes suivantes :
  - Téléphone : Choisissez d'appeler.



- Message : Choisissez de discuter.



- Envoyer un fichier : choisissez d'envoyer un fichier.



## Navigation

L'interface utilisateur du plugin contient trois vues du plugin qui sont indiquées par les formes bleues et blanches en bas à droite de l'écran. Balayez vers la gauche ou vers la droite pour naviguer entre les vues.

- Affichage des contacts : créez un groupe de messages directs ou une conversation de salon.
- Vue DMs : créez une one-to-one conversation. La fonctionnalité de chat fonctionne comme dans l'application native Wickr. Cette fonctionnalité vous permet de rester dans la vue Carte et de communiquer avec les autres utilisateurs du plugin.
- Vue des chambres : les pièces existantes de l'application native sont transférées. Tout ce qui est fait dans le plugin se reflète dans l'application native Wickr.

### Note

Certaines fonctions, telles que la suppression d'une pièce, ne peuvent être exécutées que dans l'application native et en personne afin d'éviter toute modification involontaire par les utilisateurs et les interférences causées par l'équipement de terrain.

## Liste des ports et domaines à autoriser

Autoriser la liste des ports suivants pour garantir le bon fonctionnement de Wickr :

### Ports

- TCPport 443 (pour les messages et les pièces jointes)
- UDPports 16384-16584 (pour les appels)

## Liste des domaines et adresses à autoriser par région

Si vous devez autoriser la liste de tous les domaines d'appel et adresses IP de serveurs possibles, consultez la liste suivante des domaines potentiels CIDRs par région. Consultez régulièrement cette liste, car elle est sujette à modification.

### Note

Les e-mails d'inscription et de vérification sont envoyés par [donotreply@wickr.email](mailto:donotreply@wickr.email).

### USA Est (Virginie du Nord)

Domaines :	<ul style="list-style-type: none"><li>• gw-pro-prod.wickr.com</li><li>• api.messaging.wickr.us-east-1.amazonaws.com</li></ul>
CIDRadresses :	<ul style="list-style-type: none"><li>• 44,211,195,0/27</li><li>• 44,213,83,32/28</li></ul>
Adresses IP :	<ul style="list-style-type: none"><li>• 44,211,195,0</li><li>• 44,211,195,1</li><li>• 44,211,195,2</li><li>• 44,211,195,3</li><li>• 44,211,195,4</li><li>• 44,211,195,5</li><li>• 44,211,195,6</li></ul>

- 44,211,1195,7
- 44,211,195,8
- 44,211,195,9
- 44,211,195,10
- 44,211,195,11
- 44,211,195,12
- 44,211,195,13
- 44,211,195,14
- 44,211,195,15
- 44,211,195,16
- 44,211,195,17
- 44,211,195,18
- 44,211,195,19
- 44,211,195,20
- 44,211,195,21
- 44,211,195,22
- 44,211,195,23
- 44,211,195,24
- 44,211,195,25
- 44,211,195,26
- 44,211,195,27
- 44,211,195,28
- 44,211,195,29
- 44,211,195,30
- 44,211,195,31
- 44,213,83,32
- 44,213,83,33
- 44,213,83,34
- 44,213,83,35
- 44,213,83,36

- 44,213,83,37
- 44,213,83,38
- 44,213,83,39
- 44,213,83,40
- 44,213,83,41
- 44,213,83,42
- 44,213,83,43
- 44,213,83,44
- 44,213,83,45
- 44,213,83,46
- 44,213,83,47

### Asie-Pacifique (Singapour)

Domaine :	<ul style="list-style-type: none"><li>• api.messaging.wickr.ap-southeast-1.amazonaws.com</li></ul>
CIDRaddresses :	<ul style="list-style-type: none"><li>• 47,129,23,144/28</li></ul>
Adresses IP :	<ul style="list-style-type: none"><li>• 47,129,23,144</li><li>• 47,129,23,145</li><li>• 47,129,23,146</li><li>• 47,129,23,147</li><li>• 47,129,23,148</li><li>• 47,129,23,149</li><li>• 47,129,23,150</li><li>• 47,129,23,151</li><li>• 47,129,23,152</li><li>• 47,129,23,153</li><li>• 47,129,23,154</li><li>• 47,129,23,155</li><li>• 47,129,23,156</li></ul>

- 47,129,23,157
- 47,129,23,158
- 47,129,23,159

## Asie-Pacifique (Sydney)

Domaine : 

- api.messaging.wickr.ap-southeast-2.amazonaws.com

CIDRaddresses : 

- 3,27,180,208/28

Adresses IP : 

- 3,27,180,208
- 3,27,180,209
- 3,27,180,210
- 3,27,180,211
- 3,27,180,212
- 3,27,180,213
- 3,27,180,214
- 3,27,180,215
- 3,27,180,216
- 3,27,180,217
- 3,27,180,218
- 3,27,180,219
- 3,27,180,220
- 3,27,180,221
- 3,27,180,222
- 3,27,180,223

## Asie-Pacifique (Tokyo)

Domaine : 

- api.messaging.wickr.ap-northeast-1.amazonaws.com

CIDRaddresses :	<ul style="list-style-type: none"><li>• 57,181,142,240/28</li></ul>
Adresses IP :	<ul style="list-style-type: none"><li>• 57,181,142,240</li><li>• 57,181,142,241</li><li>• 57,181,142,242</li><li>• 57,181,142,243</li><li>• 57,181,142,244</li><li>• 57,181,142,245</li><li>• 57,181,142,246</li><li>• 57,181,142,247</li><li>• 57,181,142,248</li><li>• 57,181,142,249</li><li>• 57,181,142,250</li><li>• 57,181,142,251</li><li>• 57,181,142,252</li><li>• 57,181,142,253</li><li>• 57,181,142,254</li><li>• 57,181,142,255</li></ul>

## Canada (Centre)

Domaine :	<ul style="list-style-type: none"><li>• api.messaging.wickr.ca-central-1.amazonaws.com</li></ul>
CIDRaddresses :	<ul style="list-style-type: none"><li>• 15,156,152,96/28</li></ul>
Adresses IP :	<ul style="list-style-type: none"><li>• 15,156,152,96</li><li>• 15,156,152,97</li><li>• 15,156,152,98</li><li>• 15,156,152,99</li><li>• 15,156,152,100</li><li>• 15,156,152,101</li></ul>

- 15,156,152,102
- 15,156,152,103
- 15,156,152,104
- 15,156,152,105
- 15,156,152,106
- 15,156,152,107
- 15,156,152,108
- 15,156,152,109
- 15,156,152,110
- 15,156,152,111

## Europe (Francfort)

Domaine : 

- api.messaging.wickr.eu-central-1.amazonaws.com

CIDRaddresses : 

- 3,78,252,32/28

Adresses IP : 

- 3,78,252,32
- 3,78,252,33
- 3,78,252,34
- 3,78,252,35
- 3,78,252,36
- 3,78,252,37
- 3,78,252,38
- 3,78,252,39
- 3,78,252,40
- 3,78,252,41
- 3,78,252,42
- 3,78,252,43
- 3,78,252,44
- 3,78,252,45

- 3,78,252,46
- 3,78,252,47

## Europe (Londres)

Domaine : 

- api.messaging. wickr.eu-west-2.amazonaws.com

CIDRaddresses : 

- 13,43,91,48/28

Adresses IP : 

- 13,43,91,48
- 13,43,91,49
- 13,43,91,50
- 13,43,91,51
- 13,43,91,52
- 13,43,91,53
- 13,43,91,54
- 13,43,91,55
- 13,43,91,56
- 13,43,91,57
- 13,43,91,58
- 13,43,91,59
- 13,43,91,60
- 13,43,91,61
- 13,43,91,62
- 13,43,91,63

## Europe (Stockholm)

Domaine : 

- api.messaging. wickr.eu-north-1.amazonaws.com

CIDRaddresses :	<ul style="list-style-type: none"><li>• 13,60,164/28</li></ul>
Adresses IP :	<ul style="list-style-type: none"><li>• 13,60,164</li><li>• 13,601,65</li><li>• 13,601,66</li><li>• 13,601,67</li><li>• 13,601,68</li><li>• 13,601,69</li><li>• 13,601,70</li><li>• 13,601,71</li><li>• 13,60,1,72</li><li>• 13,601,73</li><li>• 13,601,74</li><li>• 13,601,75</li><li>• 13,60,176</li><li>• 13,601,77</li><li>• 13,601,78</li><li>• 13,601,79</li></ul>

## Europe (Zurich)

Domaine :	<ul style="list-style-type: none"><li>• api.messaging.wickr.eu-central-2.amazonaws.com</li></ul>
CIDRaddresses :	<ul style="list-style-type: none"><li>• 16,63.106,224/28</li></ul>
Adresses IP :	<ul style="list-style-type: none"><li>• 16,63.106,224</li><li>• 16,63106,225</li><li>• 16,63.106,226</li><li>• 16,63.106,227</li><li>• 16,63.106,228</li><li>• 16,63106,229</li></ul>

- 16,63,106,230
- 16,63.106,231
- 16,63.106,232
- 16,63.106,233
- 16,63.106,234
- 16,63.106,235
- 16,63.106,236
- 16,63.106,237
- 16,63.106,238
- 16,63.106,239

### AWS GovCloud (US-Ouest)

Domaine : 

- api.messaging.wickr. us-gov-west-1.  
amazonaws.com

CIDRaddresses : 

- 3,30,186,208/28

Adresses IP : 

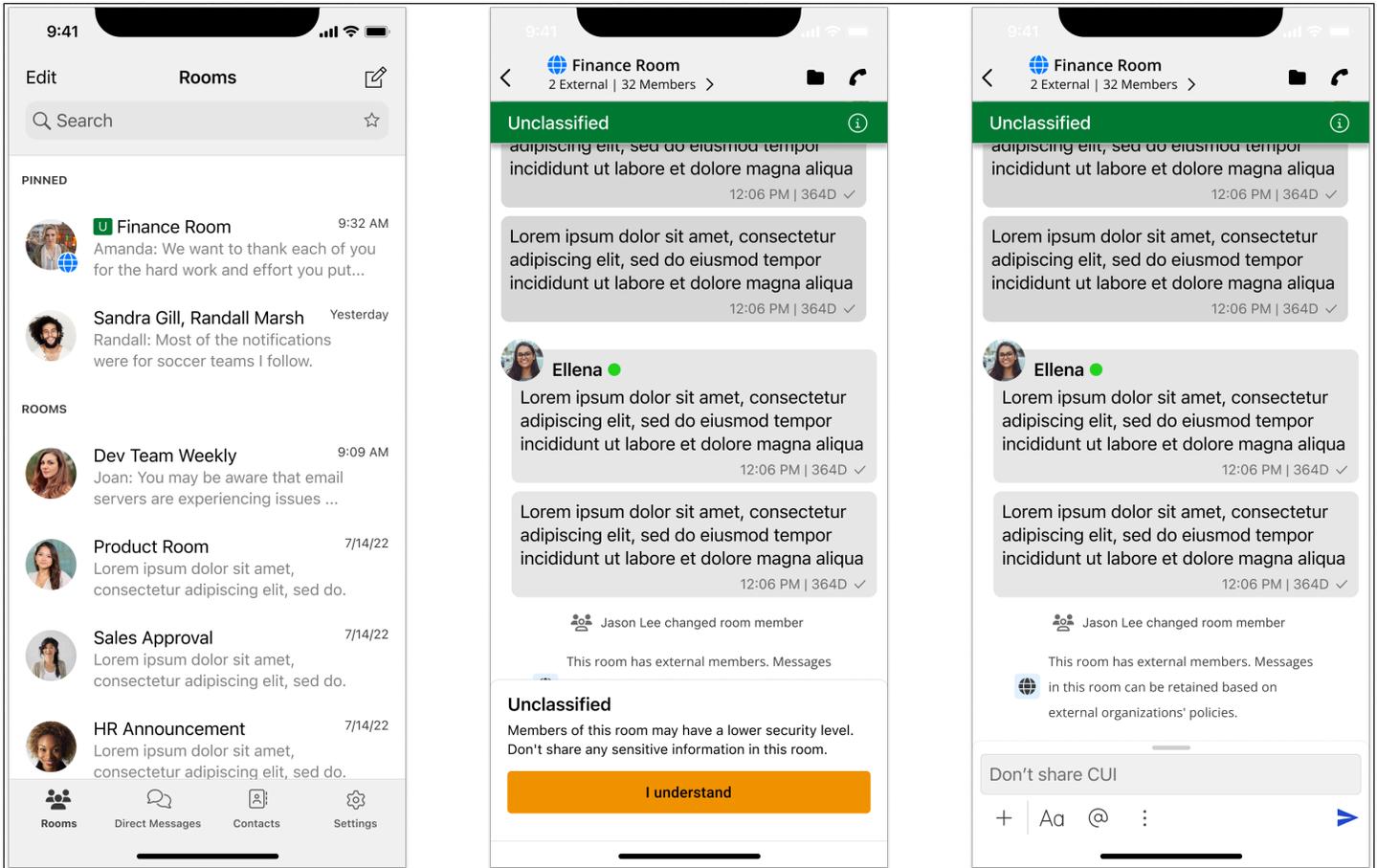
- 3,30,186,208
- 3,30,186,209
- 3,30,186,210
- 3,30,186,211
- 3,30,186,212
- 3,30,186,213
- 3,30,186,214
- 3,30,186,215
- 3,30,186,216
- 3,30,186,217
- 3,30,186,218
- 3,30,186,219
- 3,30,186,220
- 3,30,186,221

- 3,30,186,222
- 3,30,186,223

## GovCloud classification et fédération transfrontalières

AWS Wickr propose un WickrGov client adapté aux GovCloud utilisateurs. La GovCloud Fédération permet la communication entre les GovCloud utilisateurs et les utilisateurs commerciaux. La fonction de classification transfrontalière permet de modifier l'interface utilisateur dans les conversations des GovCloud utilisateurs. En tant qu' GovCloud utilisateur, vous devez respecter des directives strictes concernant la classification définie par le gouvernement. Lorsque GovCloud les utilisateurs engagent des conversations avec des utilisateurs commerciaux (utilisateurs Enterprise, AWS Wickr, utilisateurs invités), les avertissements non classifiés suivants s'affichent :

- Un tag U dans la liste des chambres
- Un accusé de réception non classifié sur l'écran du message
- Une bannière non classifiée au-dessus de la conversation



**Note**

Ces avertissements ne seront affichés que lorsqu'un GovCloud utilisateur est en conversation ou fait partie d'une salle avec des utilisateurs externes. Ils disparaîtront si les utilisateurs externes quittent la conversation. Aucun avertissement ne sera affiché dans les conversations entre GovCloud utilisateurs.

# Gérer les utilisateurs dans AWS Wickr

Dans la section Utilisateurs de AWS Management Console for Wickr, vous pouvez voir les utilisateurs et les robots actuels de Wickr, et modifier leurs informations.

Rubriques

- [Annuaire des équipes](#)
- [Utilisateurs invités](#)

## Annuaire des équipes

Vous pouvez consulter les utilisateurs actuels de Wickr et modifier leurs informations dans la section Utilisateur de AWS Management Console for Wickr.

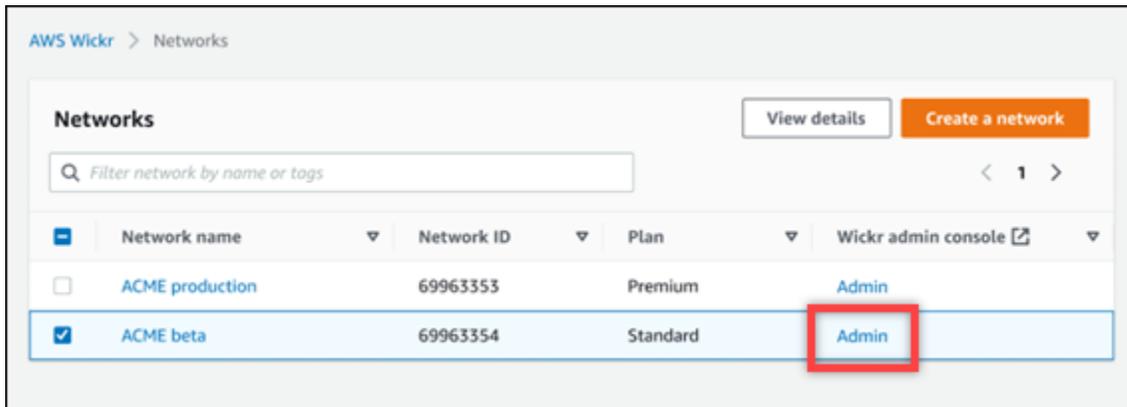
Rubriques

- [Afficher les utilisateurs](#)
- [Créer des utilisateurs](#)
- [Modifier les utilisateurs](#)
- [Suppression d'utilisateurs](#)
- [Supprimer des utilisateurs en bloc](#)
- [Suspension groupée d'utilisateurs](#)

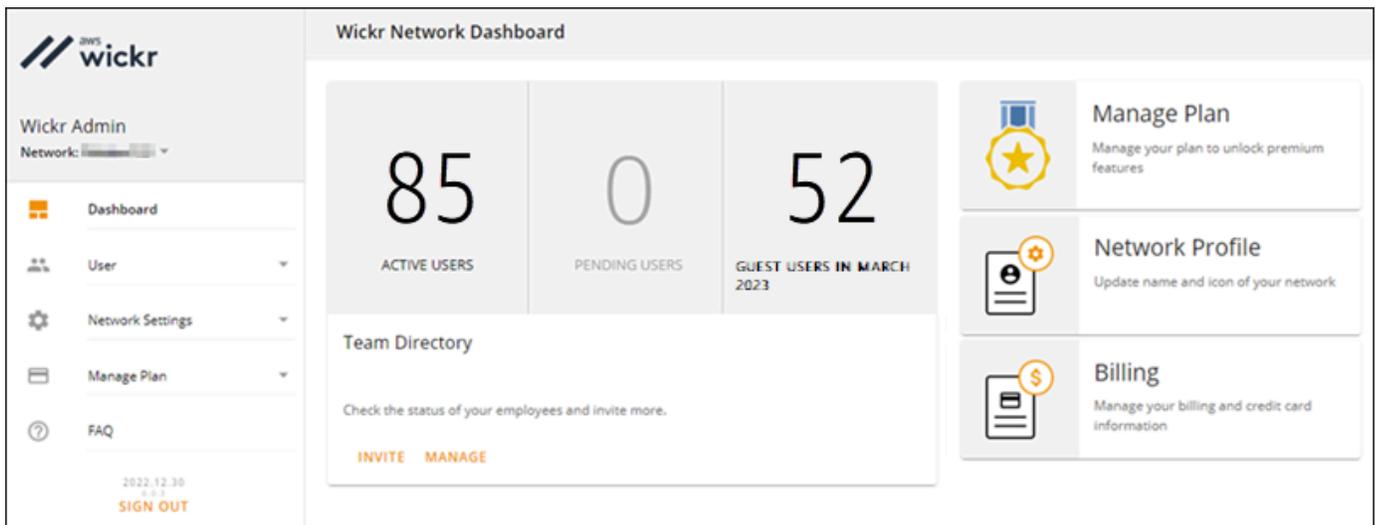
## Afficher les utilisateurs

Suivez la procédure suivante pour voir les utilisateurs enregistrés sur votre réseau Wickr.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse <https://console.aws.amazon.com/wickr/>.
2. Sur la page Réseaux, choisissez le lien Admin pour accéder à la console d'administration Wickr pour ce réseau.



Vous êtes redirigé vers la console d'administration Wickr pour un réseau spécifique.



3. Dans le volet de navigation de la console d'administration Wickr, choisissez User, puis Team Directory.

La page Répertoire des équipes affiche les utilisateurs enregistrés sur votre réseau Wickr, y compris leur nom, leur adresse e-mail, le groupe de sécurité attribué et leur statut actuel. Pour les utilisateurs actuels, vous pouvez consulter leurs appareils, modifier leurs informations, les suspendre, les supprimer et les transférer vers un autre réseau Wickr.

## Créer des utilisateurs

Procédez comme suit pour créer un utilisateur.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse <https://console.aws.amazon.com/wickr/>.

2. Sur la page Réseaux, choisissez le lien Admin pour accéder à la console d'administration Wickr pour ce réseau.

Vous êtes redirigé vers la console d'administration Wickr pour un réseau spécifique.

3. Dans le volet de navigation de la console d'administration Wickr, choisissez User, puis Team Directory.
4. Choisissez Créer un nouvel utilisateur.
5. Dans le formulaire qui apparaît, entrez le prénom, le nom de famille, le code du pays, le numéro de téléphone et l'adresse e-mail de l'utilisateur. L'adresse e-mail est le seul champ obligatoire. Assurez-vous de choisir le groupe de sécurité approprié pour l'utilisateur. Wickr enverra un e-mail d'invitation à l'adresse que vous avez spécifiée pour l'utilisateur.
6. Choisissez Créer.

Un e-mail est envoyé à l'utilisateur. L'e-mail fournit des liens de téléchargement pour les applications clientes Wickr, ainsi qu'un lien pour s'inscrire à Wickr. Lorsque les utilisateurs s'inscrivent à Wickr en utilisant le lien contenu dans l'e-mail, leur statut dans le répertoire de l'équipe Wickr passe de En attente à Actif.

## Modifier les utilisateurs

Pour modifier un utilisateur, procédez comme suit.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse <https://console.aws.amazon.com/wickr/>.
2. Sur la page Réseaux, choisissez le lien Admin pour accéder à la console d'administration Wickr pour ce réseau.

Vous êtes redirigé vers la console d'administration Wickr pour un réseau spécifique.

3. Dans le volet de navigation de la console d'administration Wickr, choisissez User, puis Team Directory.
4. Cliquez sur l'icône représentant des points de suspension verticaux à côté du nom de l'utilisateur que vous souhaitez supprimer.
5. Vous pouvez choisir l'une des options suivantes :
  - Appareils — Affichez les appareils que l'utilisateur a configurés avec le client Wickr.

- **Modifier** : modifiez les informations de l'utilisateur, telles que son nom, son code de pays, son numéro de téléphone (facultatif) et le groupe de sécurité attribué.
- **Suspendre** — Suspendez l'utilisateur afin qu'il ne puisse pas se connecter à votre réseau Wickr dans le client Wickr. Lorsque vous suspendez un utilisateur actuellement connecté à votre réseau Wickr dans le client, cet utilisateur est automatiquement déconnecté.
- **Supprimer** — Supprimez l'utilisateur de votre réseau Wickr.

## Suppression d'utilisateurs

Pour supprimer un utilisateur, procédez comme suit.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse <https://console.aws.amazon.com/wickr/>.
2. Sur la page Réseaux, choisissez le lien Admin pour accéder à la console d'administration Wickr pour ce réseau.

Vous êtes redirigé vers la console d'administration Wickr pour un réseau spécifique.

3. Dans le volet de navigation de la console d'administration Wickr, choisissez User, puis Team Directory.
4. Cliquez sur l'icône représentant des points de suspension verticaux à côté du nom de l'utilisateur que vous souhaitez supprimer.
5. Choisissez Supprimer pour supprimer l'utilisateur.

Lorsque vous supprimez un utilisateur, celui-ci n'est plus en mesure de se connecter à votre réseau Wickr dans le client Wickr.

## Supprimer des utilisateurs en bloc

Vous pouvez supprimer et suspendre en bloc les utilisateurs du réseau Wickr dans la section Utilisateur de la console d'administration Wickr pour Wickr.

### Note

L'option de suppression groupée d'utilisateurs ne s'applique que lorsque l'authentification unique n'est pas activée.

Pour supprimer en bloc les utilisateurs de votre réseau Wickr à l'aide d'un modèle CSV, procédez comme suit.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse <https://console.aws.amazon.com/wickr/>.
2. Dans le volet de navigation de la console d'administration Wickr, choisissez User, puis Team Directory.

La page Répertoire des équipes affiche les utilisateurs enregistrés sur votre réseau Wickr.

3. Sur la page Répertoire de l'équipe, choisissez Gérer les utilisateurs.
4. Dans la fenêtre contextuelle Gérer les utilisateurs, choisissez Supprimer les utilisateurs.
5. Téléchargez l'exemple de modèle CSV. Pour télécharger le modèle d'exemple, choisissez Télécharger le modèle.
6. Complétez le modèle en ajoutant l'adresse e-mail des utilisateurs que vous souhaitez supprimer en bloc de votre réseau.
7. Téléchargez le modèle CSV complété. Vous pouvez glisser-déposer le fichier dans la zone de téléchargement ou sélectionner « Choisir un fichier ».
8. Cochez la case, je reconnais que la suppression d'un utilisateur n'est pas réversible.
9. Choisissez Supprimer les utilisateurs.

 Note

Cette action commencera immédiatement à supprimer des utilisateurs et peut prendre plusieurs minutes. Les utilisateurs supprimés ne pourront plus se connecter à votre réseau Wickr dans le client Wickr.

Pour supprimer en bloc les utilisateurs de votre réseau Wickr en téléchargeant un fichier CSV du répertoire de votre équipe, procédez comme suit.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse <https://console.aws.amazon.com/wickr/>.
2. Dans le volet de navigation de la console d'administration Wickr, choisissez User, puis Team Directory.

La page Répertoire des équipes affiche les utilisateurs enregistrés sur votre réseau Wickr.

3. Sélectionnez l'icône de téléchargement du fichier CSV en haut à droite de la page du répertoire des équipes.
4. Après avoir téléchargé le modèle CSV de répertoire d'équipe, supprimez les lignes d'utilisateurs qui n'ont pas besoin d'être supprimées.
5. Sur la page Répertoire de l'équipe, choisissez Gérer les utilisateurs.
6. Dans la fenêtre contextuelle Gérer les utilisateurs, choisissez Supprimer les utilisateurs.
7. Téléchargez le modèle CSV du répertoire de l'équipe. Vous pouvez glisser-déposer le fichier dans la zone de téléchargement ou sélectionner « Choisir un fichier ».
8. Cochez la case, je reconnais que la suppression d'un utilisateur n'est pas réversible.
9. Choisissez Supprimer les utilisateurs.

#### Note

Cette action commencera immédiatement à supprimer des utilisateurs et peut prendre plusieurs minutes. Les utilisateurs supprimés ne pourront plus se connecter à votre réseau Wickr dans le client Wickr.

## Suspension groupée d'utilisateurs

Vous pouvez suspendre en bloc les utilisateurs du réseau Wickr dans la section Utilisateur de la console d'administration Wickr pour Wickr.

#### Note

L'option de suspension groupée des utilisateurs ne s'applique que lorsque l'authentification unique n'est pas activée.

Pour suspendre en bloc les utilisateurs de votre réseau Wickr, procédez comme suit.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse <https://console.aws.amazon.com/wickr/>.
2. Dans le volet de navigation de la console d'administration Wickr, choisissez User, puis Team Directory.

La page Répertoire des équipes affiche les utilisateurs enregistrés sur votre réseau Wickr.

3. Sur la page Répertoire de l'équipe, choisissez Gérer les utilisateurs.
4. Dans la fenêtre contextuelle Gérer les utilisateurs, choisissez Suspendre les utilisateurs.
5. Téléchargez l'exemple de modèle CSV. Pour télécharger le modèle d'exemple, choisissez Télécharger le modèle.
6. Complétez le modèle en ajoutant l'adresse e-mail des utilisateurs que vous souhaitez suspendre en bloc de votre réseau.
7. Téléchargez le modèle CSV complété. Vous pouvez glisser-déposer le fichier dans la zone de téléchargement ou sélectionner « Choisir un fichier ».
8. Après avoir chargé le fichier CSV, choisissez Suspendre les utilisateurs.

#### Note

Cette action commencera immédiatement à suspendre les utilisateurs et peut prendre plusieurs minutes. Les utilisateurs suspendus ne peuvent pas se connecter à votre réseau Wickr dans le client Wickr. Lorsque vous suspendez un utilisateur actuellement connecté à votre réseau Wickr dans le client, cet utilisateur est automatiquement déconnecté.

## Utilisateurs invités

La fonctionnalité utilisateur invité de Wickr permet aux utilisateurs invités individuels de se connecter au client Wickr et de collaborer avec les utilisateurs du réseau Wickr. Les administrateurs Wickr peuvent activer ou désactiver les utilisateurs invités pour leurs réseaux Wickr sur la page Groupe de sécurité de la console d'administration Wickr.

Une fois la fonctionnalité activée, les utilisateurs invités à rejoindre votre réseau Wickr peuvent interagir avec les utilisateurs de votre réseau Wickr. Des frais vous seront facturés Compte AWS pour la fonctionnalité d'utilisateur invité. Pour plus d'informations sur la tarification de la fonctionnalité utilisateur invité, consultez la page de [tarification de Wickr](#) sous Extensions de tarification.

### Rubriques

- [Activer ou désactiver les utilisateurs invités](#)
- [Afficher le nombre d'utilisateurs invités](#)
- [Afficher l'utilisation mensuelle](#)

- [Afficher les utilisateurs invités](#)
- [Bloquer un utilisateur invité](#)

## Activer ou désactiver les utilisateurs invités

Suivez la procédure suivante pour activer ou désactiver les utilisateurs invités pour votre réseau Wickr.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse <https://console.aws.amazon.com/wickr/>.
2. Sur la page Réseaux, choisissez le lien Admin pour accéder à la console d'administration Wickr pour ce réseau.

Vous êtes redirigé vers la console d'administration Wickr pour un réseau spécifique.

3. Dans le volet de navigation de la console d'administration Wickr, choisissez Network Settings, puis Security Group.
4. Choisissez Détails pour un groupe de sécurité spécifique.

### Note

Vous ne pouvez activer les utilisateurs invités que pour des groupes de sécurité individuels. Pour activer les utilisateurs invités pour tous les groupes de sécurité de votre réseau Wickr, vous devez activer la fonctionnalité pour chaque groupe de sécurité de votre réseau.

5. Choisissez l'onglet Fédération sur la page de détails du groupe de sécurité.
6. L'option permettant d'autoriser les utilisateurs invités sera disponible à deux endroits :
  - Fédération locale : pour les réseaux situés dans l'est des États-Unis (Virginie du Nord), choisissez Modifier à côté de la section Fédération locale de la page.
  - Fédération mondiale : pour tous les autres réseaux des autres régions, choisissez Modifier à côté de la section Fédération mondiale de la page.
7. Sélectionnez Autoriser les utilisateurs invités pour activer les utilisateurs invités pour le groupe de sécurité, ou désélectionnez-le pour le désactiver.
8. Choisissez Enregistrer pour enregistrer la modification et la rendre effective pour le groupe de sécurité.

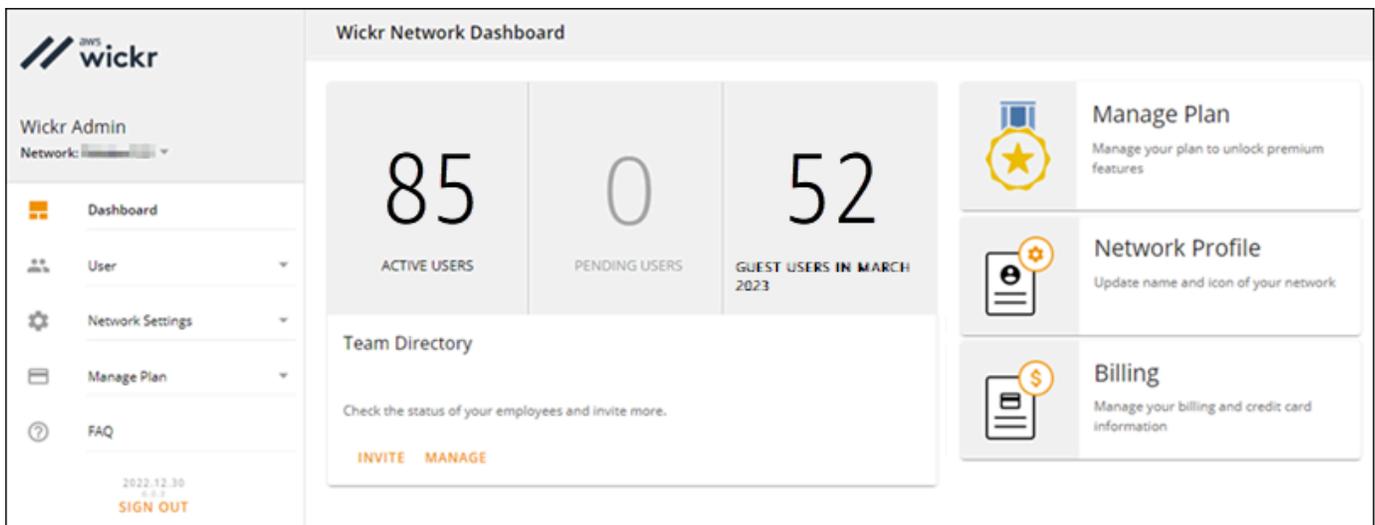
Les utilisateurs enregistrés dans le groupe de sécurité spécifique de votre réseau Wickr peuvent désormais interagir avec les utilisateurs invités. Pour plus d'informations, consultez la section [Utilisateurs invités](#) dans le guide de l'utilisateur de Wickr.

## Afficher le nombre d'utilisateurs invités

Suivez la procédure suivante pour afficher le nombre d'utilisateurs invités pour votre réseau Wickr.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse <https://console.aws.amazon.com/wickr/>.
2. Sur la page Réseaux, choisissez le lien Admin pour accéder à la console d'administration Wickr de ce réseau.

Vous êtes redirigé vers la console d'administration Wickr pour un réseau spécifique. La page Tableau de bord affiche le nombre d'utilisateurs invités de votre réseau Wickr, comme indiqué dans l'exemple suivant.



## Afficher l'utilisation mensuelle

Vous pouvez consulter le nombre d'utilisateurs invités avec lesquels votre réseau a communiqué au cours d'une période de facturation. Pour consulter votre consommation mensuelle, procédez comme suit.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse <https://console.aws.amazon.com/wickr/>.

2. Sur la page Réseaux, choisissez le lien Admin pour accéder à la console d'administration Wickr de ce réseau.
3. Dans le volet de navigation de la console d'administration Wickr, choisissez User, puis Guest Users.
4. Sur la page Utilisateurs invités, choisissez la section Utilisation mensuelle.

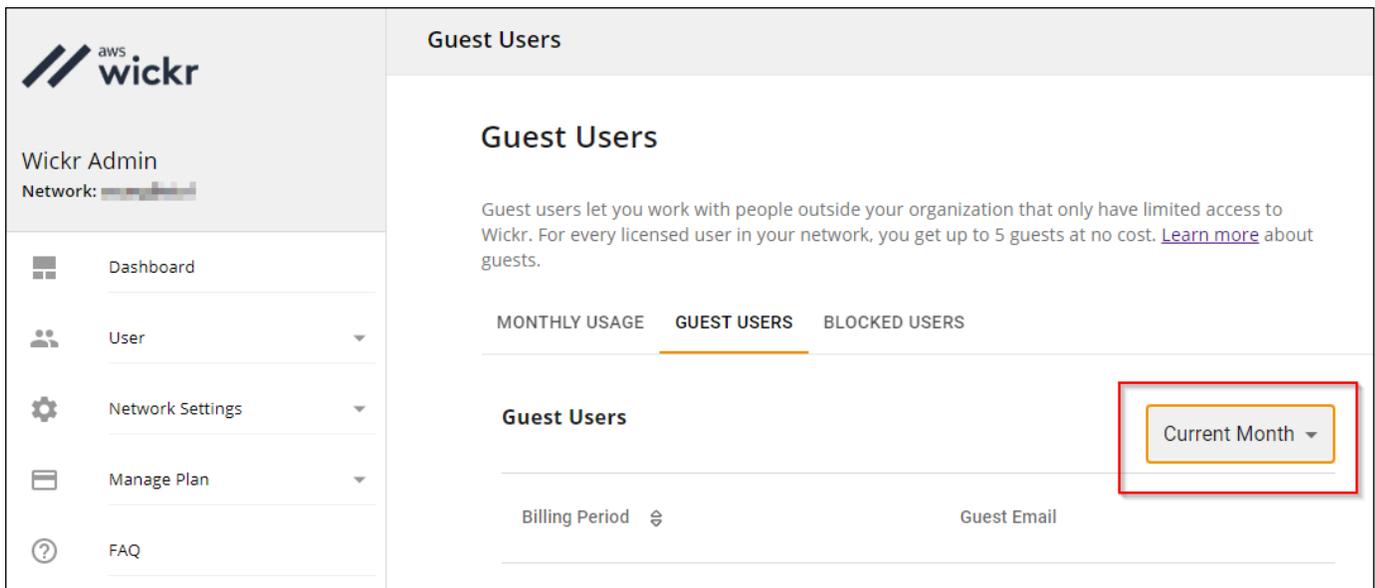
 Note

Les données de facturation des clients sont mises à jour toutes les 24 heures.

## Afficher les utilisateurs invités

Vous pouvez consulter la liste des utilisateurs invités avec lesquels un utilisateur du réseau a communiqué au cours d'une période de facturation spécifique. Pour voir vos utilisateurs invités, procédez comme suit.

1. Ouvrez le AWS Management Console pour Wickr à l'adresse <https://console.aws.amazon.com/wickr/>.
2. Sur la page Réseaux, choisissez le lien Admin pour accéder à la console d'administration Wickr de ce réseau.
3. Dans le volet de navigation de la console d'administration Wickr, choisissez User, puis Guest Users.
4. Sur la page Utilisateurs invités, choisissez la section Utilisateurs invités.
5. Pour afficher les utilisateurs invités pour un mois spécifique, sélectionnez le mois correspondant dans le menu déroulant.



## Bloquer un utilisateur invité

Les utilisateurs bloqués ne peuvent communiquer avec aucun membre de votre réseau.

Pour bloquer un utilisateur invité

1. Ouvrez le AWS Management Console pour Wickr à l'adresse <https://console.aws.amazon.com/wickr/>.
2. Sur la page Réseaux, choisissez le lien Admin pour accéder à la console d'administration Wickr de ce réseau.
3. Dans le volet de navigation de la console d'administration Wickr, choisissez User, puis Guest Users.
4. Sur la page Utilisateurs invités, choisissez la section Utilisateurs invités.
5. La section Utilisateurs invités affiche les utilisateurs invités qui ont communiqué sur votre réseau Wickr.
6. Dans la section Utilisateurs invités, recherchez l'adresse e-mail de l'utilisateur invité que vous souhaitez bloquer.
7. Sur le côté droit du nom de l'utilisateur invité, sélectionnez les trois points, puis choisissez Bloquer.
8. Choisissez Bloquer dans la fenêtre contextuelle.
9. Pour consulter la liste des utilisateurs bloqués sur votre réseau Wickr, choisissez la section Utilisateurs bloqués.

## Pour débloquent un utilisateur invité

1. Ouvrez le AWS Management Console pour Wickr à l'adresse <https://console.aws.amazon.com/wickr/>.
2. Sur la page Réseaux, choisissez le lien Admin pour accéder à la console d'administration Wickr de ce réseau.
3. Dans le volet de navigation de la console d'administration Wickr, choisissez User, puis Guest Users.
4. Sur la page Utilisateurs invités, choisissez la section Utilisateurs bloqués.
5. La section Utilisateurs bloqués affiche les utilisateurs invités bloqués sur votre réseau Wickr.
6. Dans la section Utilisateurs bloqués, recherchez l'e-mail de l'utilisateur invité que vous souhaitez débloquent.
7. Sur le côté droit du nom de l'utilisateur invité, sélectionnez les trois points, puis choisissez Débloquent.
8. Choisissez Débloquent dans la fenêtre contextuelle.

# Sécurité en AWS Wickr

Sécurité du cloud chez AWS est la plus haute priorité. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre AWS et toi. Le [modèle de responsabilité partagée](#) décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud — AWS est chargé de protéger l'infrastructure qui fonctionne AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre du [AWS Programmes de conformité](#) . Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Wickr, voir [AWS Services visés par programme de conformité](#) .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de Wickr. Les rubriques suivantes vous montrent comment configurer Wickr pour répondre à vos objectifs de sécurité et de conformité. Vous apprenez également à utiliser d'autres AWS des services qui vous aident à surveiller et à sécuriser vos ressources Wickr.

## Rubriques

- [Protection des données dans AWS Wickr](#)
- [Gestion des identités et des accès pour AWS Wickr](#)
- [Validation de la conformité](#)
- [La résilience en AWS osier](#)
- [Sécurité des infrastructures dans AWS Wickr](#)
- [Analyse de configuration et de vulnérabilité dans AWS Wickr](#)
- [Bonnes pratiques de sécurité pour AWS Wickr](#)

# Protection des données dans AWS Wickr

Le AWS modèle de [responsabilité partagée modèle](#) de de s'applique à la protection des données dans AWS Wickr. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. Vous êtes responsable du contrôle de votre contenu hébergé sur cette infrastructure. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité pour Services AWS que tu utilises. Pour plus d'informations sur la confidentialité des données, consultez la section [Confidentialité des données FAQ](#). Pour plus d'informations sur la protection des données en Europe, consultez le [AWS Modèle de responsabilité partagée et article de GDPR](#) blog sur le AWS Blog sur la sécurité.

Pour des raisons de protection des données, nous vous recommandons de protéger Compte AWS informations d'identification et configuration des utilisateurs individuels avec AWS IAM Identity Center or AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) pour chaque compte.
- Utilisez SSL/TLS pour communiquer avec AWS ressources. Nous avons besoin de la TLS version 1.2 et recommandons la TLS version 1.3.
- Configuration API et enregistrement des activités des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation CloudTrail des sentiers pour capturer AWS activités, voir [Travailler avec les CloudTrail sentiers](#) dans le AWS CloudTrail Guide de l'utilisateur
- Utiliser AWS solutions de chiffrement, ainsi que tous les contrôles de sécurité par défaut intégrés Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de FIPS 140 à 3 modules cryptographiques validés pour accéder AWS via une interface de ligne de commande ou un API, utilisez un FIPS point de terminaison. Pour plus d'informations sur les FIPS points de terminaison disponibles, voir [Federal Information Processing Standard \(FIPS\) 140-3](#).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Wickr ou un autre Services AWS à l'aide de la console API, AWS CLI, ou AWS SDKs. Toutes les données que vous entrez dans des

balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez un URL à un serveur externe, nous vous recommandons vivement de ne pas inclure d'informations d'identification dans le URL afin de valider votre demande auprès de ce serveur.

## Gestion des identités et des accès pour AWS Wickr

AWS Identity and Access Management (IAM) est un Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès à AWS ressources. IAM les administrateurs contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources Wickr. IAM est un Service AWS que vous pouvez utiliser sans frais supplémentaires.

### Rubriques

- [Public ciblé](#)
- [Authentification par des identités](#)
- [Gestion des accès à l'aide de politiques](#)
- [AWS politiques gérées pour AWS Wickr](#)
- [Comment fonctionne AWS Wickr avec IAM](#)
- [Exemples de politiques basées sur l'identité pour Wickr AWS](#)
- [Résolution des problèmes d'identité et d'AWS accès à Wickr](#)

## Public ciblé

Comment utilisez-vous AWS Identity and Access Management (IAM) diffère en fonction du travail que vous effectuez dans Wickr.

Utilisateur du service — Si vous utilisez le service Wickr pour faire votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités de Wickr pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans Wickr, consultez [Résolution des problèmes d'identité et d'AWS accès à Wickr](#).

Administrateur du service — Si vous êtes responsable des ressources Wickr dans votre entreprise, vous avez probablement un accès complet à Wickr. C'est à vous de déterminer les fonctionnalités

et ressources de Wickr auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite envoyer des demandes à votre IAM administrateur pour modifier les autorisations des utilisateurs de votre service. Consultez les informations de cette page pour comprendre les concepts de base de IAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM Wickr, consultez [Comment fonctionne AWS Wickr avec IAM](#).

**IAM administrateur** — Si vous êtes IAM administrateur, vous voudrez peut-être en savoir plus sur la façon dont vous pouvez rédiger des politiques pour gérer l'accès à Wickr. Pour voir des exemples de politiques basées sur l'identité Wickr que vous pouvez utiliser dans IAM, consultez. [Exemples de politiques basées sur l'identité pour Wickr AWS](#)

## Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS en utilisant vos informations d'identification. Vous devez être authentifié (connecté) à AWS) en tant que Utilisateur racine d'un compte AWS, en tant qu'IAM utilisateur ou en assumant un IAM rôle.

Vous pouvez vous connecter à AWS en tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez en tant qu'identité fédérée, votre administrateur a préalablement configuré la fédération d'identité à l'aide de IAM rôles. Lorsque vous accédez AWS en utilisant la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au AWS Management Console ou le AWS portail d'accès. Pour plus d'informations sur la connexion à AWS, voir [Comment se connecter à votre Compte AWS](#) dans le .Connexion à AWS Guide de l'utilisateur

Si vous accédez AWS programmatiquement, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, voir [Signature AWS API demandes](#) dans le guide de IAM l'utilisateur.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, AWS vous recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez la section [Authentification multifactorielle](#) dans le AWS IAM Identity Center Guide

de l'utilisateur et [utilisation de l'authentification multifactorielle \(MFA\) dans AWS](#) dans le guide de l'utilisateur IAM.

## Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez avec une seule identité de connexion qui donne un accès complet à tous Services AWS et les ressources du compte. Cette identité s'appelle Compte AWS utilisateur root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui nécessitent que vous vous connectiez en tant qu'utilisateur root, consultez la section [Tâches nécessitant des informations d'identification utilisateur root](#) dans le guide de IAM l'utilisateur.

## Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder Services AWS en utilisant des informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, un fournisseur d'identité Web, AWS Directory Service, le répertoire Identity Center ou tout utilisateur accédant Services AWS en utilisant les informations d'identification fournies par le biais d'une source d'identité. Lorsque les identités fédérées accèdent Comptes AWS, ils assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion centralisée des accès, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans tous vos Comptes AWS et applications. Pour plus d'informations sur IAM Identity Center, consultez [Qu'est-ce qu'IAM Identity Center ?](#) dans le AWS IAM Identity Center Guide de l'utilisateur

## Utilisateurs et groupes IAM

Un [IAMutilisateur](#) est une identité au sein de votre Compte AWS qui dispose d'autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des IAM utilisateurs dotés d'informations d'identification à long terme, telles que des mots de

passee et des clés d'accès. Toutefois, si vous avez des cas d'utilisation spécifiques qui nécessitent des informations d'identification à long terme auprès des IAM utilisateurs, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, voir [Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification à long terme](#) dans le Guide de IAM l'utilisateur.

Un [IAMgroupe](#) est une identité qui définit un ensemble d'IAMutilisateurs. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer IAM des ressources.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, voir [Quand créer un IAM utilisateur \(au lieu d'un rôle\)](#) dans le Guide de IAM l'utilisateur.

## IAMrôles

Un [IAMrôle](#) est une identité au sein de votre Compte AWS qui dispose d'autorisations spécifiques. Il est similaire à un IAM utilisateur, mais n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un IAM rôle dans AWS Management Console en [changeant de rôle](#). Vous pouvez assumer un rôle en appelant un AWS CLI or AWS APIopération ou en utilisant une option personnaliséeURL. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez la section [Utilisation IAM des rôles](#) dans le Guide de IAM l'utilisateur.

IAMles rôles dotés d'informations d'identification temporaires sont utiles dans les situations suivantes :

- Accès utilisateur fédéré : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour plus d'informations sur les rôles pour la fédération, voir [Création d'un rôle pour un fournisseur d'identité tiers](#) dans le guide de IAM l'utilisateur. Si vous utilisez IAM Identity Center, vous configurez un ensemble d'autorisations. Pour contrôler les accès auxquels vos identités peuvent accéder après leur authentification, IAM Identity Center met en corrélation l'ensemble d'autorisations avec un rôle dans. IAM Pour plus d'informations sur les ensembles d'autorisations, voir [Ensembles d'autorisations](#) dans le AWS IAM Identity Center Guide de l'utilisateur

- **Autorisations IAM utilisateur temporaires** : un IAM utilisateur ou un rôle peut assumer un IAM rôle afin d'obtenir temporairement différentes autorisations pour une tâche spécifique.
- **Accès entre comptes** : vous pouvez utiliser un IAM rôle pour autoriser une personne (un mandant fiable) d'un autre compte à accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Cependant, avec certains Services AWS, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, voir [Accès aux ressources entre comptes IAM dans le guide](#) de l'IAMutilisateur.
- **Accès multiservices** — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
- **Sessions d'accès transmises (FAS)** : lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions dans AWS, vous êtes considéré comme un directeur. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FASutilise les autorisations du principal appelant un Service AWS, combiné à la demande Service AWS pour adresser des demandes aux services en aval. FASLes demandes ne sont effectuées que lorsqu'un service reçoit une demande nécessitant des interactions avec d'autres Services AWS ou des ressources à compléter. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, voir [Transférer les sessions d'accès](#).
- **Rôle de service** — Un rôle de service est un [IAMrôle](#) qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieurIAM. Pour plus d'informations, voir [Création d'un rôle pour déléguer des autorisations à un Service AWS](#) dans le guide de l'utilisateur IAM.
- **Rôle lié à un service** — Un rôle lié à un service est un type de rôle lié à un service Service AWS. Le service peut assumer le rôle d'effectuer une action en votre nom. Les rôles liés aux services apparaissent dans votre Compte AWS et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.
- **Applications exécutées sur Amazon EC2** : vous pouvez utiliser un IAM rôle pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui créent AWS CLI or AWS API demandes. Cela est préférable au stockage des clés d'accès dans l'EC2instance. Pour attribuer un AWS pour attribuer un rôle à une EC2 instance et le mettre à la disposition de toutes ses applications, vous créez un profil d'instance attaché à l'instance. Un

profil d'instance contient le rôle et permet aux programmes exécutés sur l'EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez la section [Utilisation d'un IAM rôle pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon](#) dans le Guide de IAM l'utilisateur.

Pour savoir s'il faut utiliser IAM des rôles ou des IAM utilisateurs, voir [Quand créer un IAM rôle \(au lieu d'un utilisateur\)](#) dans le guide de IAM l'utilisateur.

## Gestion des accès à l'aide de politiques

Vous contrôlez l'accès dans AWS en créant des politiques et en les associant à AWS identités ou ressources. Une politique est un objet dans AWS qui, lorsqu'elle est associée à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées dans AWS sous forme de JSON documents. Pour plus d'informations sur la structure et le contenu des documents de JSON politique, voir [Présentation des JSON politiques](#) dans le guide de IAM l'utilisateur.

Les administrateurs peuvent utiliser AWS JSON politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour autoriser les utilisateurs à effectuer des actions sur les ressources dont ils ont besoin, un IAM administrateur peut créer des IAM politiques. L'administrateur peut ensuite ajouter les IAM politiques aux rôles, et les utilisateurs peuvent assumer les rôles.

Les politiques définissent les autorisations pour une action, quelle que soit la méthode que vous utilisez pour effectuer l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle auprès du AWS Management Console, le AWS CLI, ou le AWS API.

### Politiques basées sur l'identité

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section [Création de IAM politiques](#) dans le Guide de l'IAM utilisateur.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles dans votre Compte AWS. Les politiques gérées incluent AWS politiques gérées et politiques gérées par le client. Pour savoir comment choisir entre une politique gérée ou une politique intégrée, voir [Choisir entre des politiques gérées et des politiques intégrées dans le Guide](#) de l'IAMutilisateur.

## Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez [spécifier un principal](#) dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou Services AWS.

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser AWS politiques gérées à partir IAM d'une stratégie basée sur les ressources.

## Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

Amazon S3 AWS WAF, et Amazon VPC sont des exemples de services qui prennent en charge ACLs. Pour en savoir plus ACLs, consultez la [présentation de la liste de contrôle d'accès \(ACL\)](#) dans le guide du développeur Amazon Simple Storage Service.

## Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- **Limites d'autorisations** — Une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une IAM entité (IAMutilisateur ou rôle). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations obtenues représentent la combinaison des politiques basées sur l'identité de l'entité et de ses limites d'autorisations. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez la section [Limites d'autorisations pour les IAM entités](#) dans le Guide de IAM l'utilisateur.
- **Politiques de séance** : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez la section [Politiques de session](#) dans le guide de IAM l'utilisateur.

## Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS détermine s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, voir la [logique d'évaluation des politiques](#) dans le guide de IAM l'utilisateur.

## AWS politiques gérées pour AWS Wickr

Pour ajouter des autorisations aux utilisateurs, aux groupes et aux rôles, il est plus facile d'utiliser AWS des politiques gérées plutôt que d'écrire des politiques vous-même. Il faut du temps et de l'expertise pour [créer des politiques gérées par les IAM clients](#) qui fournissent à votre équipe uniquement les autorisations dont elle a besoin. Pour démarrer rapidement, vous pouvez utiliser notre AWS politiques gérées. Ces politiques couvrent les cas d'utilisation courants et sont disponibles dans votre Compte AWS. Pour plus d'informations sur AWS politiques gérées, voir [AWS politiques gérées](#) dans le guide de IAM l'utilisateur.

Services AWS maintenir et mettre à jour AWS politiques gérées. Vous ne pouvez pas modifier les autorisations dans AWS politiques gérées. Les services ajoutent parfois des autorisations supplémentaires à un AWS politique gérée pour prendre en charge les nouvelles fonctionnalités. Ce

type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont les plus susceptibles de mettre à jour un AWS politique gérée lorsqu'une nouvelle fonctionnalité est lancée ou lorsque de nouvelles opérations sont disponibles. Les services ne suppriment pas les autorisations d'un AWS politique gérée, afin que les mises à jour des politiques n'enfreignent pas vos autorisations existantes.

## AWS politique gérée : AWSWickrFullAccess

Vous pouvez associer la `AWSWickrFullAccess` politique à votre IAM identité. Cette politique accorde une autorisation administrative complète au service Wickr, y compris le AWS Management Console pour Wickr in the AWS Management Console. Pour plus d'informations sur l'association de politiques à une identité, voir [Ajouter et supprimer des autorisations IAM d'identité](#) dans le AWS Identity and Access Management Guide de l'utilisateur

### Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `wickr`— Accorde une autorisation administrative complète au service Wickr.

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

## Mises à jour de Wickr vers AWS stratégies gérées

Afficher les détails des mises à jour de AWS politiques gérées pour Wickr depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au RSS flux sur la page d'historique du document Wickr.

Modification	Description	Date
<a href="#">AWSWickrFullAccess</a> – Nouvelle politique	Wickr a ajouté une nouvelle politique qui accorde des autorisations administratives complètes au service Wickr, y compris la console d'administration Wickr dans le AWS Management Console.	28 novembre 2022
Wickr a commencé à suivre les modifications	Wickr a commencé à suivre les modifications apportées à son AWS politiques gérées.	28 novembre 2022

## Comment fonctionne AWS Wickr avec IAM

Avant de commencer IAM à gérer l'accès à Wickr, découvrez quelles IAM fonctionnalités sont disponibles avec Wickr.

IAM fonctionnalités que vous pouvez utiliser avec AWS Wickr

IAM fonctionnalité	Support en osier
<a href="#">Politiques basées sur l'identité</a>	Oui
<a href="#">Politiques basées sur les ressources</a>	Non
<a href="#">Actions de politique</a>	Oui
<a href="#">Ressources de politique</a>	Non
<a href="#">Clés de condition d'une politique</a>	Non
<a href="#">ACLs</a>	Non
<a href="#">ABAC(balises dans les politiques)</a>	Non
<a href="#">Informations d'identification temporaires</a>	Non

IAMfonctionnalité	Support en osier
<a href="#">Autorisations de principaux</a>	Non
<a href="#">Fonctions du service</a>	Non
<a href="#">Rôles liés à un service</a>	Non

Pour avoir une vue d'ensemble de la façon dont Wickr et d'autres AWS les services fonctionnent avec la plupart IAM des fonctionnalités, voir [AWS services compatibles avec IAM](#) le Guide de l'IAMutilisateur.

## Politiques basées sur l'identité pour Wickr

Prend en charge les politiques basées sur l'identité : oui

Les politiques basées sur l'identité sont JSON des documents de politique d'autorisation que vous pouvez joindre à une identité, telle qu'un IAM utilisateur, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour savoir comment créer une politique basée sur l'identité, consultez la section [Création de IAM politiques](#) dans le Guide de l'IAMutilisateur.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier les actions et les ressources autorisées ou refusées ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité, car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour en savoir plus sur tous les éléments que vous pouvez utiliser dans une JSON politique, consultez la [référence aux éléments de IAM JSON politique](#) dans le Guide de IAM l'utilisateur.

Exemples de politiques basées sur l'identité pour Wickr

Pour voir des exemples de politiques basées sur l'identité de Wickr, consultez. [Exemples de politiques basées sur l'identité pour Wickr AWS](#)

## Politiques basées sur les ressources au sein de Wickr

Prend en charge les politiques basées sur les ressources : non

Les politiques basées sur les ressources sont des documents JSON de stratégie que vous attachez à une ressource. Les politiques de confiance dans les IAM rôles et les politiques relatives aux

compartiments Amazon S3 sont des exemples de politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez [spécifier un principal](#) dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou Services AWS.

Pour activer l'accès entre comptes, vous pouvez spécifier un compte entier ou IAM des entités d'un autre compte comme principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un IAM administrateur du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, voir [Accès aux ressources entre comptes IAM dans](#) le Guide de IAM l'utilisateur.

## Actions politiques pour Wickr

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser AWS JSONpolitiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'Actionélément d'une JSON politique décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès dans une politique. Les actions politiques portent généralement le même nom que les actions associées AWS APIopération. Il existe certaines exceptions, telles que les actions avec autorisation uniquement qui n'ont pas d'opération correspondante. API Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour voir la liste des actions Wickr, voir [Actions définies par AWS Wickr](#) dans la référence d'autorisation de service.

Les actions politiques dans Wickr utilisent le préfixe suivant avant l'action :

```
wickr
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

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

Pour voir des exemples de politiques basées sur l'identité de Wickr, consultez [Exemples de politiques basées sur l'identité pour Wickr AWS](#)

## Ressources politiques pour Wickr

Prend en charge les ressources politiques : Non

Les administrateurs peuvent utiliser AWS JSON politiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément Resource JSON de stratégie indique le ou les objets auxquels s'applique l'action. Les instructions doivent inclure un élément Resource ou NotResource. Il est recommandé de spécifier une ressource en utilisant son [Amazon Resource Name \(ARN\)](#). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (\*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

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

Pour voir une liste des types de ressources Wickr et de leurs caractéristiques ARNs, consultez la section [Ressources définies par AWS Wickr](#) dans la référence d'autorisation de service. Pour savoir avec quelles actions vous pouvez spécifier pour chaque ressource, voir [Actions définies par AWS Wickr. ARN](#)

Pour voir des exemples de politiques basées sur l'identité de Wickr, consultez [Exemples de politiques basées sur l'identité pour Wickr AWS](#)

## Clés de conditions de politique pour Wickr

Prend en charge les clés de condition de politique spécifiques au service : Non

Les administrateurs peuvent utiliser AWS JSONpolitiques pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des [opérateurs de condition](#), tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs `Condition` éléments dans une instruction ou plusieurs clés dans un seul `Condition` élément, AWS les évalue à l'aide d'une AND opération logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une OR opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez autoriser un IAM utilisateur à accéder à une ressource uniquement si celle-ci est étiquetée avec son nom IAM d'utilisateur. Pour plus d'informations, consultez [IAM la section Éléments de politique : variables et balises](#) dans le Guide de IAM l'utilisateur.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour tout voir AWS clés de condition globales, voir [AWS clés contextuelles des conditions globales](#) dans le guide de IAM l'utilisateur.

Pour voir la liste des clés de condition Wickr, voir [Clés de condition pour AWS Wickr](#) dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez [Actions définies par AWS Wickr](#).

Pour voir des exemples de politiques basées sur l'identité de Wickr, consultez. [Exemples de politiques basées sur l'identité pour Wickr AWS](#)

## ACLs à Wickr

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format du document JSON de stratégie.

## ABAC avec Wickr

Supports ABAC (balises dans les politiques) : Non

Le contrôle d'accès basé sur les attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs. Entrée AWS, ces attributs sont appelés balises. Vous pouvez associer des tags à IAM des entités (utilisateurs ou rôles) et à de nombreuses AWS ressources. Le balisage des entités et des ressources est la première étape de ABAC. Vous concevez ensuite des ABAC politiques pour autoriser les opérations lorsque le tag du principal correspond à celui de la ressource à laquelle il essaie d'accéder.

ABAC est utile dans les environnements qui se développent rapidement et aide dans les situations où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans [l'élément de condition](#) d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations ABAC, voir [Qu'est-ce que c'est ABAC ?](#) dans le guide de IAM l'utilisateur. Pour consulter un didacticiel présentant les étapes de configuration ABAC, voir [Utiliser le contrôle d'accès basé sur les attributs \(ABAC\)](#) dans le guide de l'IAM utilisateur.

## Utiliser des informations d'identification temporaires avec Wickr

Supporte les informations d'identification temporaires : Non

Momentanée Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris lesquelles Services AWS utilisent des informations d'identification temporaires, voir [Services AWS qui fonctionnent avec IAM](#) le Guide de l'IAM utilisateur.

Vous utilisez des informations d'identification temporaires si vous vous connectez au AWS Management Console en utilisant n'importe quelle méthode, à l'exception du nom d'utilisateur et du mot de passe. Par exemple, lorsque vous accédez AWS à l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification

temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez la section [Passage à un rôle \(console\)](#) dans le guide de IAM l'utilisateur.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide du AWS CLI or AWS API. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez la section Informations [d'identification de sécurité temporaires dans IAM](#).

## Autorisations principales interservices pour Wickr

Prend en charge les sessions d'accès transféré (FAS) : Non

Lorsque vous utilisez un IAM utilisateur ou un rôle pour effectuer des actions dans AWS, vous êtes considéré comme un directeur. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant un Service AWS, combiné à la demande Service AWS pour adresser des demandes aux services en aval. FAS les demandes ne sont effectuées que lorsqu'un service reçoit une demande nécessitant des interactions avec d'autres Services AWS ou des ressources à compléter. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur les politiques relatives FAS aux demandes, voir [Transférer les sessions d'accès](#).

## Rôles de service pour Wickr

Supporte les rôles de service : Non

Un rôle de service est un [IAM rôle](#) qu'un service assume pour effectuer des actions en votre nom. Un IAM administrateur peut créer, modifier et supprimer un rôle de service de l'intérieur IAM. Pour plus d'informations, voir [Création d'un rôle pour déléguer des autorisations à un Service AWS](#) dans le guide de l'utilisateur IAM.

### Warning

La modification des autorisations pour un rôle de service peut perturber les fonctionnalités de Wickr. Modifiez les rôles de service uniquement lorsque Wickr fournit des conseils pour le faire.

## Rôles liés aux services pour Wickr

Prend en charge les rôles liés à un service : non

Un rôle lié à un service est un type de rôle de service lié à un Service AWS. Le service peut assumer le rôle d'effectuer une action en votre nom. Les rôles liés aux services apparaissent dans votre Compte AWS et appartiennent au service. Un IAM administrateur peut consulter, mais pas modifier les autorisations pour les rôles liés à un service.

Pour plus de détails sur la création ou la gestion des rôles liés à un service, voir [AWS services qui fonctionnent avec IAM](#). Recherchez un service dans le tableau qui inclut un Yes dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

## Exemples de politiques basées sur l'identité pour Wickr AWS

Par défaut, un nouvel IAM utilisateur n'est pas autorisé à faire quoi que ce soit. Un IAM administrateur doit créer et attribuer des IAM politiques qui autorisent les utilisateurs à administrer le service AWS Wickr. Un exemple de politique d'autorisation est exposé ci-dessous.

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

Cet exemple de politique autorise les utilisateurs à créer, afficher et gérer les réseaux Wickr à l'aide du AWS Management Console pour Wickr. Pour en savoir plus sur les éléments d'une déclaration IAM de politique, voir [Politiques basées sur l'identité pour Wickr](#). Pour savoir comment créer une IAM politique à l'aide de ces exemples de documents de JSON stratégie, voir [Création de politiques dans l'JSONonglet](#) du Guide de l'IAMutilisateur.

### Rubriques

- [Bonnes pratiques en matière de politiques](#)
- [Utilisation de AWS Management Console pour Wickr](#)
- [Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations](#)

## Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer les ressources Wickr de votre compte. Ces actions peuvent entraîner des coûts pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez les directives et recommandations suivantes :

- Commencez avec AWS politiques gérées et évolution vers des autorisations avec le moindre privilège — Pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez AWS politiques gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant AWS des politiques gérées par le client spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez [.AWS politiques gérées](#) ou [AWS politiques gérées pour les fonctions professionnelles](#) dans le guide de IAM l'utilisateur.
- Appliquer les autorisations du moindre privilège : lorsque vous définissez des autorisations à IAM l'aide de politiques, accordez uniquement les autorisations nécessaires à l'exécution d'une tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation IAM pour appliquer des autorisations, consultez la section [Politiques et autorisations IAM dans](#) le guide de IAM l'utilisateur.
- Utilisez des conditions dans IAM les politiques pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques pour limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez rédiger une condition de politique pour spécifier que toutes les demandes doivent être envoyées en utilisant SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un Service AWS, comme AWS CloudFormation. Pour plus d'informations, voir [Éléments IAM JSON de politique : Condition](#) dans le guide de IAM l'utilisateur.
- Utilisez IAM Access Analyzer pour valider vos IAM politiques afin de garantir des autorisations sécurisées et fonctionnelles. IAM Access Analyzer valide les politiques nouvelles et existantes afin qu'elles soient conformes au langage des IAM politiques (JSON) et IAM aux meilleures pratiques. IAM Access Analyzer fournit plus de 100 vérifications des politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus

d'informations, consultez la section [Validation des politiques d'IAMAccess Analyzer](#) dans le guide de IAM l'utilisateur.

- Exiger une authentification multifactorielle (MFA) — Si vous avez un scénario qui nécessite IAM des utilisateurs ou un utilisateur root dans votre Compte AWS, activez MFA pour plus de sécurité. Pour exiger le MFA moment où les API opérations sont appelées, ajoutez MFA des conditions à vos politiques. Pour plus d'informations, consultez [la section Configuration de l'API accès MFA protégé](#) dans le Guide de l'IAMutilisateur.

Pour plus d'informations sur les meilleures pratiques en matière de [sécurité IAM](#), consultez la section [Bonnes pratiques en matière](#) de sécurité IAM dans le Guide de IAM l'utilisateur.

## Utilisation de AWS Management Console pour Wickr

Joignez le `AWSWickrFullAccess` AWS politique gérée concernant vos IAM identités afin de leur accorder une autorisation administrative complète sur le service Wickr, y compris la console d'administration Wickr dans le AWS Management Console. Pour plus d'informations, consultez [AWS politique gérée : AWSWickrFullAccess](#).

## Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux IAM utilisateurs de consulter les politiques intégrées et gérées associées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide du AWS CLI or AWS API.

```
{
  "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": "*"
    }
  ]
}
```

## Résolution des problèmes d'identité et d'AWSaccès à Wickr

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pourriez rencontrer lorsque vous travaillez avec Wickr etIAM.

### Rubriques

- [Je ne suis pas autorisé à effectuer une action administrative dans le AWS Management Console pour Wickr](#)

### Je ne suis pas autorisé à effectuer une action administrative dans le AWS Management Console pour Wickr

Si l'icône AWS Management Console car Wickr vous indique que vous n'êtes pas autorisé à effectuer une action, vous devez alors contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni vos informations de connexion.

L'exemple d'erreur suivant se produit lorsque l'iam:ListUsers action est effectuée par l'utilisateur IAMUtilisateur qui essaie d'utiliser le AWS Management Console pour que Wickr puisse créer, gérer ou afficher les réseaux Wickr dans le AWS

Management Console pour Wickr mais ne possède pas les `wickr:ListNetworks` autorisations `wickr:CreateAdminSession` et.

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

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder au AWS Management Console pour Wickr en utilisant les `wickr:ListNetworks` actions `wickr:CreateAdminSession` et. Pour plus d'informations, consultez [Exemples de politiques basées sur l'identité pour Wickr AWS](#) et [AWS politique gérée : AWSWickrFullAccess](#).

## Validation de la conformité

Pour une liste des AWS services dans le cadre de programmes de conformité spécifiques, voir [AWS Services visés par programme de conformité](#) . Pour des informations générales, voir [AWS Programmes de conformité](#) .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir [Téléchargement de rapports dans AWS Artifact](#).

Votre responsabilité en matière de conformité lorsque vous utilisez Wickr est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides [de démarrage rapide sur la sécurité et la conformité](#) [Guides](#) sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et fournissent des étapes pour déployer des environnements de base axés sur la sécurité et la conformité sur AWS.
- [AWS Ressources de conformité](#) — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- [Évaluation des ressources à l'aide des règles](#) du AWS Config Guide du développeur — AWS Config; évalue dans quelle mesure vos configurations de ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- [AWS Security Hub](#)— Ceci AWS le service fournit une vue complète de votre état de sécurité au sein de AWS qui vous aide à vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité.

## La résilience en AWS osier

Le AWS l'infrastructure mondiale est construite autour de Régions AWS et zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur Régions AWS et zones de disponibilité, voir [AWS Infrastructure mondiale](#).

En plus du AWS infrastructure mondiale, Wickr propose plusieurs fonctionnalités pour vous aider à répondre à vos besoins en matière de résilience et de sauvegarde des données. Pour de plus amples informations, veuillez consulter [Conservation des données](#).

## Sécurité des infrastructures dans AWS Wickr

En tant que service géré, AWS Wickr est protégé par le AWS les procédures de sécurité du réseau mondial décrites dans le livre blanc [Amazon Web Services : présentation des processus de sécurité](#).

## Analyse de configuration et de vulnérabilité dans AWS Wickr

La configuration et les contrôles informatiques sont une responsabilité partagée entre AWS et vous, notre client. Pour plus d'informations, consultez le AWS [modèle de responsabilité partagée](#).

Il est de votre responsabilité de configurer Wickr conformément aux spécifications et aux directives, de demander périodiquement à vos utilisateurs de télécharger la dernière version du client Wickr, de vous assurer que vous utilisez la dernière version du bot de conservation des données Wickr et de surveiller l'utilisation de Wickr par vos utilisateurs.

## Bonnes pratiques de sécurité pour AWS Wickr

Wickr fournit un certain nombre de fonctionnalités de sécurité à prendre en compte lorsque vous développez et mettez en œuvre vos propres politiques de sécurité. Les bonnes pratiques suivantes doivent être considérées comme des instructions générales et ne représentent pas une solution

de sécurité complète. Étant donné que ces bonnes pratiques peuvent ne pas être appropriées ou suffisantes pour votre environnement, considérez-les comme des remarques utiles plutôt que comme des recommandations.

Pour prévenir les événements de sécurité potentiels associés à votre utilisation de Wickr, suivez les meilleures pratiques suivantes :

- Implémentez l'accès avec le moindre privilège et créez des rôles spécifiques à utiliser pour les actions Wickr. Utilisez IAM des modèles pour créer un rôle. Pour de plus amples informations, veuillez consulter [AWS politiques gérées pour AWS Wickr](#).
- Accédez au AWS Management Console pour Wickr en vous authentifiant auprès du AWS Management Console first. Ne partagez pas vos informations d'identification personnelles sur la console. Tous les utilisateurs d'Internet peuvent accéder à la console, mais ils ne peuvent pas se connecter ou démarrer une session s'ils n'ont pas d'informations d'identification valides pour la console.

# Surveillance d'AWS Wickr

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'AWS Wickr et de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller Wickr, signaler un problème et prendre des mesures automatiques le cas échéant :

- AWS CloudTrail capture les appels d'API et les événements associés effectués par ou pour le compte de votre AWS compte et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour plus d'informations, consultez le [Guide de l'utilisateur AWS CloudTrail](#). Pour plus d'informations sur la journalisation des appels d'API Wickr à l'aide CloudTrail de. [Journalisation des appels d'API AWS Wickr à l'aide de AWS CloudTrail](#)

## Journalisation des appels d'API AWS Wickr à l'aide de AWS CloudTrail

AWS Wickr est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Wickr. CloudTrail capture tous les appels d'API pour Wickr sous forme d'événements. Les appels capturés incluent des appels provenant de AWS Management Console for Wickr et des appels de code vers les opérations de l'API Wickr. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Wickr. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Wickr, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires. Pour en savoir plus CloudTrail, consultez le [guide de AWS CloudTrail l'utilisateur](#).

## Informations sur Wickr dans CloudTrail

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans Wickr, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez afficher,

rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section [Affichage des événements avec l'historique des CloudTrail événements](#).

Pour un enregistrement continu des événements de votre régionCompte AWS, y compris des événements pour Wickr, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal de suivi consigne les événements de toutes les régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour en savoir plus, consultez les ressources suivantes :

- [Présentation de la création d'un journal de suivi](#)
- [CloudTrail services et intégrations pris en charge](#)
- [Configuration des notifications Amazon SNS pour CloudTrail](#)
- [Réception de fichiers CloudTrail journaux de plusieurs régions](#) et [réception de fichiers CloudTrail journaux de plusieurs comptes](#)

Toutes les actions de Wickr sont enregistrées par CloudTrail. Par exemple, les appels au `CreateAdminSession` et les `ListNetworks` actions génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management (IAM).
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été effectuée par un autre service AWS.

Pour de plus amples informations, veuillez consulter l'[élément userIdentity CloudTrail](#) .

## Comprendre les entrées du fichier journal Wickr

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux

contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'CreateAdminSessionaction.

```
{
  "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"
}

```

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'CreateNetworkaction.

```

{
  "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"
}

```

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`ListNetworks` action.

```

{
  "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"
}

```

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'UpdateNetworkdetailsaction.

```

{
  "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"
}

```

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'TagResourceaction.

```

{
  "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"
}

```

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`ListTagsForResource` action.

```

{
  "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"
}
```

## Tableau de bord d'analyse

Vous pouvez utiliser le tableau de bord d'analyse pour voir comment votre organisation utilise AWS Wickr. La procédure suivante explique comment accéder au tableau de bord d'analyse à l'aide de la console AWS Wickr.

Pour accéder au tableau de bord d'analyse

1. Ouvrez le AWS Management Console pour Wickr à l'adresse <https://console.aws.amazon.com/wickr/>.
2. Dans le volet de navigation, sélectionnez Analytics (Analyse).

La page Analytics affiche les statistiques de votre réseau dans différents onglets.

Sur la page Analytics, vous trouverez un filtre de période dans le coin supérieur droit de chaque onglet. Ce filtre s'applique à l'ensemble de la page. En outre, dans le coin supérieur droit de chaque onglet, vous pouvez exporter les points de données pour la plage de temps sélectionnée en choisissant l'option Exporter disponible.

 Note

L'heure sélectionnée est en UTC (temps universel coordonné).

Les onglets suivants sont disponibles :

- La vue d'ensemble s'affiche :
  - Enregistré : nombre total d'utilisateurs enregistrés, y compris les utilisateurs actifs et suspendus sur le réseau pendant la période sélectionnée. Il n'inclut pas les utilisateurs en attente ou invités.
  - En attente : nombre total d'utilisateurs en attente sur le réseau pendant la période sélectionnée.
  - Enregistrement des utilisateurs — Le graphique affiche le nombre total d'utilisateurs enregistrés dans la période sélectionnée.
  - Appareils : nombre d'appareils sur lesquels l'application a été active.
  - Versions clientes : nombre d'appareils actifs classés selon leur version client.
- Les membres affichent :
  - État : utilisateurs actifs sur le réseau pendant la période sélectionnée.
  - Utilisateurs actifs —
    - Le graphique affiche le nombre d'utilisateurs actifs au fil du temps et peut être agrégé par jour, par semaine ou par mois (dans la plage de temps sélectionnée ci-dessus).
    - Le nombre d'utilisateurs actifs peut être ventilé par plate-forme, version du client ou groupe de sécurité. Si un groupe de sécurité a été supprimé, le nombre total sera affiché sous la forme Supprimé#.
- Les messages s'affichent :
  - Messages envoyés : nombre de messages uniques envoyés par tous les utilisateurs et robots du réseau au cours de la période sélectionnée.
  - Appels : nombre d'appels uniques effectués par tous les utilisateurs du réseau.

- Fichiers : nombre de fichiers envoyés par les utilisateurs du réseau (y compris les mémos vocaux).
- Appareils : le graphique circulaire indique le nombre de périphériques actifs classés par système d'exploitation.
- Versions clientes : nombre d'appareils actifs classés selon leur version client.

# Historique du document

Le tableau suivant décrit les versions de documentation de Wickr.

Modification	Description	Date
<a href="#">La classification et la fédération transfrontalières sont désormais disponibles</a>	La fonction de classification transfrontalière permet de modifier l'interface utilisateur dans les conversations des GovCloud utilisateurs. Pour plus d'informations, consultez <a href="#">GovCloud la section Classification transfrontalière et fédération</a> .	25 juin 2024
<a href="#">La fonction de lecture du reçu est désormais disponible</a>	Les administrateurs de Wickr peuvent désormais activer ou désactiver la fonction de confirmation de lecture dans la console d'administration. Pour plus d'informations, consultez la section <a href="#">Lire les reçus</a> .	23 avril 2024
<a href="#">Global Federation prend désormais en charge la fédération restreinte et les administrateurs peuvent consulter les analyses d'utilisation dans la console d'administration</a>	La Fédération mondiale prend désormais en charge la fédération restreinte. Cela fonctionne pour les réseaux Wickr dans d'autres Régions AWS. Pour plus d'informations, consultez <a href="#">la section Groupes de sécurité</a> . En outre, les administrateurs peuvent désormais consulter leurs analyses d'utilisation sur le tableau de bord Analytics de la console d'administration. Pour	28 mars 2024

---

<p><a href="#">Un essai gratuit de trois mois du plan Premium de AWS Wickr est désormais disponible</a></p>	<p>plus d'informations, consultez le <a href="#">tableau de bord Analytics</a>.</p>	<p>9 février 2024</p>
<p><a href="#">La fonctionnalité d'utilisateur invité est généralement disponible et d'autres contrôles d'administrateur ont été ajoutés</a></p>	<p>Les administrateurs de Wickr peuvent désormais choisir un plan Premium d'essai gratuit de trois mois pour un maximum de 30 utilisateurs. Pendant l'essai gratuit, toutes les fonctionnalités des forfaits Standard et Premium sont disponibles, y compris les contrôles d'administration illimités et la conservation des données. La fonctionnalité d'utilisateur invité n'est pas disponible pendant l'essai gratuit Premium. Pour plus d'informations, consultez la section <a href="#">Gérer le plan</a>.</p> <p>Les administrateurs de Wickr peuvent désormais accéder à une série de nouvelles fonctionnalités, notamment la liste des utilisateurs invités, la possibilité de supprimer ou de suspendre des utilisateurs en bloc, et la possibilité d'empêcher les utilisateurs invités de communiquer sur votre réseau Wickr. Pour plus d'informations, consultez la section <a href="#">Utilisateurs invités</a>.</p>	<p>8 novembre 2023</p>

<a href="#">Wickr est désormais disponible en Europe (Francfort) Région AWS</a>	Wickr est désormais disponible en Europe (Francfort). Région AWS Pour plus d'informations, consultez la section <a href="#">Accès à Wickr</a> .	26 octobre 2023
<a href="#">Les réseaux Wickr ont désormais la capacité de se fédérer entre Régions AWS</a>	Les réseaux Wickr ont désormais la capacité de se fédérer entre eux. Régions AWS Pour plus d'informations, consultez <a href="#">la section Groupes de sécurité</a> .	29 septembre 2023
<a href="#">Wickr est désormais disponible en Europe (Londres) Région AWS</a>	Wickr est désormais disponible en Europe (Londres). Région AWS Pour plus d'informations, consultez la section <a href="#">Accès à Wickr</a> .	23 août 2023
<a href="#">Wickr est maintenant disponible au Canada (Centre) Région AWS</a>	Wickr est maintenant disponible au Canada (Centre). Région AWS Pour plus d'informations, consultez la section <a href="#">Accès à Wickr</a> .	3 juillet 2023
<a href="#">La fonctionnalité d'utilisateur invité est désormais disponible en avant-première</a>	Les utilisateurs invités peuvent se connecter au client Wickr et collaborer avec les utilisateurs du réseau Wickr. Pour plus d'informations, consultez la section <a href="#">Utilisateurs invités (version préliminaire)</a> .	31 mai 2023

[AWSWickr est désormais intégré à AWS CloudTrail, et est désormais disponible dans AWS GovCloud \(US-West\) en tant que WickrGov](#)

AWSWickr est désormais intégré à AWS CloudTrail. Pour plus d'informations, consultez la section [Enregistrement des API appels AWS Wickr à l'aide AWS CloudTrail](#) de. De plus, Wickr est désormais disponible en AWS GovCloud (ouest des États-Unis) sous forme de WickrGov. Pour plus d'informations, consultez [AWS WickrGov](#) le guide de AWS GovCloud (US) l'utilisateur.

30 mars 2023

[Balisage et création de réseaux multiples](#)

Le balisage est désormais pris en charge dans AWS Wickr. Pour plus d'informations, consultez la section [Balises réseau](#). Plusieurs réseaux peuvent désormais être créés dans Wickr. Pour plus d'informations, consultez la section [Création d'un réseau](#).

7 mars 2023

[Première version](#)

Publication initiale du guide d'administration de Wickr

28 novembre 2022

# Notes de mise à jour

Pour vous aider à suivre les mises à jour et améliorations continues de Wickr, nous publions des avis de publication décrivant les modifications récentes.

## Juin 2024

- La classification et la fédération transfrontalières sont désormais disponibles pour GovCloud les utilisateurs. Pour plus d'informations, voir [classification GovCloud transfrontalière et fédération](#).

## Avril 2024

- Wickr prend désormais en charge les reçus de lecture. Pour plus d'informations, voir [Lire les reçus](#).

## Mars 2024

- La fédération mondiale prend désormais en charge la fédération restreinte, où la fédération mondiale ne peut être activée que pour certains réseaux ajoutés dans le cadre d'une fédération restreinte. Cela fonctionne pour les réseaux Wickr dans d'autres Régions AWS. Pour plus d'informations, consultez [la section Groupes de sécurité](#).
- Les administrateurs peuvent désormais consulter leurs analyses d'utilisation sur le tableau de bord Analytics de la console d'administration. Pour plus d'informations, consultez le [tableau de bord Analytics](#).

## Février 2024

- AWSWickr propose désormais un essai gratuit de trois mois de son plan Premium pour un maximum de 30 utilisateurs. Les modifications et les limites incluent :
  - Toutes les fonctionnalités des forfaits Standard et Premium, telles que les contrôles administratifs illimités et la conservation des données, sont désormais disponibles dans le cadre de l'essai gratuit Premium. La fonctionnalité d'utilisateur invité n'est pas disponible pendant l'essai gratuit Premium.

- L'essai gratuit précédent n'est plus disponible. Vous pouvez passer de votre essai gratuit ou de votre forfait Standard à un essai gratuit Premium si vous n'avez pas encore utilisé l'essai gratuit Premium. Pour plus d'informations, consultez la section [Gérer le plan](#).

## Novembre 2023

- La fonctionnalité réservée aux utilisateurs invités est désormais disponible pour tous. Les modifications et les ajouts incluent :
  - Possibilité de signaler les abus commis par d'autres utilisateurs de Wickr.
  - Les administrateurs peuvent consulter la liste des utilisateurs invités avec lesquels un réseau a interagi, ainsi que le nombre d'utilisateurs mensuels.
  - Les administrateurs peuvent empêcher les utilisateurs invités de communiquer avec leur réseau.
  - Tarifs supplémentaires pour les utilisateurs invités.
- Améliorations du contrôle administratif
  - Possibilité de supprimer/suspendre des utilisateurs en masse.
  - SSOParamètre supplémentaire pour configurer une période de grâce pour l'actualisation des jetons.

## Octobre 2023

- Améliorations
  - Wickr est désormais disponible en Europe (Francfort). Région AWS

## Septembre 2023

- Améliorations
  - Les réseaux Wickr ont désormais la capacité de se fédérer entre eux. Régions AWS Pour plus d'informations, consultez [la section Groupes de sécurité](#).

## août 2023

- Améliorations
  - Wickr est désormais disponible en Europe (Londres). Région AWS

## Juillet 2023

- Améliorations
  - Wickr est maintenant disponible au Canada (Centre). Région AWS

## Mai 2023

- Améliorations
  - Support supplémentaire pour les utilisateurs invités. Pour plus d'informations, consultez [Utilisateurs invités](#).

## Mars 2023

- Wickr est désormais intégré à AWS CloudTrail. Pour plus d'informations, consultez [Journalisation des appels d'API AWS Wickr à l'aide de AWS CloudTrail](#).
- Wickr est désormais disponible en AWS GovCloud (ouest des États-Unis) sous forme de WickrGov. Pour plus d'informations, consultez [AWS WickrGov](#) le guide de AWS GovCloud (US) l'utilisateur.
- Wickr prend désormais en charge le balisage. Pour plus d'informations, consultez [Balises réseau](#). Plusieurs réseaux peuvent désormais être créés dans Wickr. Pour plus d'informations, consultez [Étape 1 : Création d'un réseau](#).

## Février 2023

- Wickr prend désormais en charge le kit d'assaut tactique Android (ATAK). Pour plus d'informations, consultez [Activez ATAK dans le tableau de bord du réseau Wickr](#).

## janvier 2023

- L'authentification unique (SSO) peut désormais être configurée sur tous les forfaits, y compris l'essai gratuit et le forfait Standard.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.