



Guía de administración

# AWS Wickr



# AWS Wickr: Guía de administración

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

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

---

# Table of Contents

¿Qué es AWS Wickr? .....	1
Características de Wickr .....	1
Acceso a Wickr .....	3
Precios .....	3
Documentación para el usuario final de Wickr .....	3
Configuración .....	4
Inscríbese en AWS .....	4
Creación un usuario de IAM .....	4
Siguiendo pasos .....	6
Introducción .....	7
Requisitos previos .....	7
Paso 1: crear una red .....	7
Paso 2: configurar su red .....	9
Paso 3: crear e invitar a usuarios .....	11
Siguiendo pasos .....	14
Cómo transferir Wickr Pro a AWS Wickr .....	14
Paso 1: Crea una AWS cuenta .....	15
Paso 2: recuperar su ID de red de Wickr .....	16
Paso 3: enviar una solicitud .....	16
Paso 4: Inicie sesión en su consola AWS .....	16
Cómo administrar la red .....	18
Perfiles de red .....	18
Cómo consultar el perfil de red .....	18
Editar el nombre de la red .....	19
Grupos de seguridad .....	20
Cómo consultar los grupos de seguridad .....	20
Creación de un grupo de seguridad .....	21
Cómo editar un grupo de seguridad .....	22
Eliminación de un grupo de seguridad .....	23
Configuración del SSO .....	24
Cómo ver la información del SSO .....	24
Cómo configurar el SSO .....	25
Periodo de gracia para la actualización del token .....	26
Lee los recibos .....	26

Etiquetas de red .....	27
Cómo administrar las etiquetas de red .....	27
Cómo agregar etiquetas de red .....	29
Cómo modificar las etiquetas de red .....	30
Cómo eliminar las etiquetas de red .....	30
Administre el plan de red .....	31
Limitaciones de la prueba gratuita de Premium .....	32
Retención de datos .....	32
Cómo consultar la información sobre la retención de datos .....	33
Cómo configurar la retención de datos .....	34
Cómo obtener los registros .....	45
Métricas y eventos de retención de datos .....	46
¿Qué es ATAK? .....	51
Cómo habilitar ATAK .....	52
Información adicional sobre ATAK .....	54
Instalar y emparejar .....	54
Marcar y recibir una llamada .....	58
Enviar un archivo .....	59
Enviar un mensaje de voz seguro (Push-to-talk) .....	60
Rueda de opciones .....	61
Navegación .....	64
Lista de puertos y dominios que deben ser permitidos .....	64
GovCloud .....	65
Administración de usuarios .....	67
Directorio de equipos .....	67
Ver usuarios .....	67
Cómo crear usuarios .....	68
Cómo editar usuarios .....	69
Eliminar usuarios .....	70
Cómo eliminar usuarios en bloque .....	70
Suspensión de usuarios en bloque .....	72
Usuarios invitados .....	73
Cómo habilitar o deshabilitar usuarios invitados .....	74
Cómo ver el número de usuarios invitados .....	75
Cómo ver el uso mensual .....	75
Cómo ver los usuarios invitados .....	76

Cómo bloquear a un usuario invitado .....	77
Seguridad .....	79
Protección de datos .....	80
Administración de identidades y accesos .....	81
Público .....	81
Autenticación con identidades .....	82
Administración de acceso mediante políticas .....	86
Políticas administradas por AWS Wickr .....	88
Cómo funciona AWS Wickr con IAM .....	90
Ejemplos de políticas basadas en identidades .....	97
Resolución de problemas .....	101
Validación de conformidad .....	101
Resiliencia .....	102
Seguridad de infraestructuras .....	103
Configuración y análisis de vulnerabilidades .....	103
Prácticas recomendadas de seguridad .....	103
Monitoreo .....	104
CloudTrail registros .....	104
Información sobre Wickr en CloudTrail .....	104
Descripción de las entradas de los archivos de registro de Wickr .....	105
.....	112
Historial de documentos .....	115
Notas de la versión .....	119
Marzo de 2024 .....	119
Febrero de 2024 .....	119
Noviembre de 2023 .....	119
Octubre de 2023 .....	120
Septiembre de 2023 .....	120
Agosto de 2023 .....	120
Julio de 2023 .....	120
Mayo de 2023 .....	120
Marzo de 2023 .....	121
Febrero de 2023 .....	121
Enero de 2023 .....	121
.....	cxxii

# ¿Qué es AWS Wickr?

AWS Wickr es un servicio end-to-end cifrado que ayuda a las organizaciones y agencias gubernamentales a comunicarse de forma segura a través one-to-one de mensajes grupales, llamadas de voz y vídeo, uso compartido de archivos, uso compartido de pantalla y mucho más. Wickr puede ayudar a los clientes a superar las obligaciones de retención de datos asociadas a las aplicaciones de mensajería del consumidor y a facilitar la colaboración de forma segura. Los controles administrativos y de seguridad avanzados ayudan a las organizaciones a cumplir los requisitos legales y reglamentarios y a crear soluciones personalizadas para los desafíos de seguridad de datos.

La información se puede registrar en un almacén de datos privado controlado por el cliente con fines de retención y auditoría. Los usuarios tienen un control administrativo exhaustivo sobre los datos, que incluye la configuración de permisos, la configuración de opciones de mensajería efímera y la definición de grupos de seguridad. Wickr se integra con servicios adicionales como Active Directory (AD), inicio de sesión único (SSO) con OpenID Connect (OIDC) y más. Puede crear y administrar rápidamente una red de Wickr a través de los AWS Management Console bots de Wickr y automatizarlos de forma segura. Para empezar, consulte [Configuración de AWS Wickr](#).

## Temas

- [Características de Wickr](#)
- [Acceso a Wickr](#)
- [Precios](#)
- [Documentación para el usuario final de Wickr](#)

## Características de Wickr

### Seguridad y privacidad mejoradas

Wickr utiliza el cifrado AES (Advanced Encryption Standard) end-to-end de 256 bits para cada función. Las comunicaciones se cifran localmente en los dispositivos del usuario y permanecen indecifrables mientras están en tránsito hacia cualquier persona que no sea el remitente y el receptor. Todos los mensajes, llamadas y archivos se cifran con una nueva clave aleatoria, y solo los destinatarios (ni siquiera AWS) pueden descifrarlos. Ya sea que estén compartiendo datos confidenciales y regulados, discutiendo asuntos legales o de recursos humanos, o incluso llevando a

cabo operaciones militares tácticas, los clientes utilizan Wickr para comunicarse cuando la seguridad y la privacidad son primordiales.

### Retención de datos

Las características administrativas flexibles están diseñadas no solo para proteger la información confidencial, sino también para retener los datos según sea necesario para cumplir con las obligaciones de cumplimiento, la retención legal y los fines de auditoría. Los mensajes y los archivos se pueden archivar en un almacén de datos seguro y controlado por el cliente.

### Acceso flexible

Los usuarios tienen acceso a varios dispositivos (móviles, de escritorio) y pueden funcionar en entornos con poco ancho de banda, incluidos los de desconexión y de comunicación. out-of-band

### Controles administrativos

Los usuarios tienen un control administrativo integral sobre los datos, lo que incluye configuración de permisos, configuración de opciones de mensajería efímera responsable y definición de grupos de seguridad.

### Potentes integraciones y bots

Wickr se integra con servicios adicionales como Active Directory, inicio de sesión único (SSO) con OpenID Connect (OIDC) y más. Los clientes pueden crear y administrar rápidamente una red de Wickr a través de los AWS Management Console robots de Wickr y automatizarlos de forma segura.

A continuación se presenta un desglose de las ofertas de colaboración de Wickr:

- Mensajería individual y grupal: chatee de forma segura con su equipo en salas con hasta 500 miembros
- Llamadas de audio y vídeo: realice conferencias telefónicas con hasta 70 personas
- Transmisión y uso compartido de pantalla: preséntese con hasta 500 participantes
- Compartir y guardar archivos: transfiera archivos de hasta 5 GB con almacenamiento ilimitado
- Efímero: controle la caducidad y los temporizadores burn-on-read
- Federación global: conéctese con usuarios de Wickr fuera de su red

**Note**

Las redes de Wickr en AWS GovCloud (EE. UU. al oeste) solo se pueden federar con otras redes de Wickr en (EE. UU. al oeste). AWS GovCloud

## Acceso a Wickr

Wickr está disponible en EE. UU. Este (Virginia del Norte), Canadá (Centro), Europa (Londres), Asia Pacífico (Sídney), Europa (Fráncfort), Europa (Estocolmo), Asia Pacífico (Singapur) y Asia Pacífico (Tokio). Regiones de AWS Wickr también está disponible WickrGov en Estados Unidos (oeste de EE. UU. AWS GovCloud ). Región de AWS

[Los administradores acceden a AWS Management Console Wickr en https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/). Antes de empezar a usar Wickr, debe completar las guías [Configuración de AWS Wickr](#) y [Introducción a AWS Wickr](#).

**Note**

El servicio Wickr no tiene una interfaz de programación de aplicaciones (API).

Los usuarios finales acceden a Wickr a través del cliente de Wickr. Para obtener más información, consulte la [Guía del usuario de AWS Wickr](#).

## Precios

Wickr está disponible en diferentes planes para individuos, equipos pequeños y grandes empresas. Para obtener más información, consulte [Precios de AWS Wickr](#).

## Documentación para el usuario final de Wickr

Si es un usuario final del cliente de Wickr y necesita acceder a su documentación, consulte la [Guía del usuario de AWS Wickr](#).

# Configuración de AWS Wickr

Si es un AWS cliente nuevo, complete los requisitos previos de configuración que se indican en esta página antes de empezar a usar AWS Wickr. Para estos procedimientos de configuración, utiliza el servicio AWS Identity and Access Management (IAM). Para obtener información completa sobre IAM, consulte la [Guía del usuario de IAM](#).

## Temas

- [Inscríbese en AWS](#)
- [Creación un usuario de IAM](#)
- [Siguietes pasos](#)

## Inscríbese en AWS

Si no tiene una Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abra <https://portal.aws.amazon.com/billing/signup>.
2. Siga las instrucciones que se le indiquen.

Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

Cuando te registras en una Cuenta de AWS, se crea un Usuario raíz de la cuenta de AWS. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar [tareas que requieren acceso de usuario raíz](#).

## Creación un usuario de IAM

Para crear un usuario administrador, elija una de las siguientes opciones.

Elegir una forma de administrar el administrador	Para	Haga esto	También puede
En IAM Identity Center (recomendado)	<p>Usar credenciales a corto plazo para acceder a AWS.</p> <p>Esto se ajusta a las prácticas recomendadas de seguridad. Para obtener información sobre las prácticas recomendadas, consulte <a href="#">Prácticas recomendadas de seguridad en IAM</a> en la Guía del usuario de IAM.</p>	Siga las instrucciones en <a href="#">Introducción</a> en la Guía del usuario de AWS IAM Identity Center .	Configure el acceso programático <a href="#">configurando el AWS CLI que se utilizará AWS IAM Identity Center</a> en la Guía del AWS Command Line Interface usuario.
En IAM (no recomendado)	Usar credenciales a largo plazo para acceder a AWS.	Siga las instrucciones en <a href="#">Creación del primer grupo de usuarios y usuario de administrador de IAM</a> en la Guía del usuario de IAM.	Configure el acceso programático mediante <a href="#">Administración de las claves de acceso de los usuarios de IAM</a> en la Guía del usuario de IAM.

 Note

También puede asignar la política administrada de `AWSWickrFullAccess` para conceder todos los permisos administrativos al servicio Wickr. Para obtener más información, consulte [AWS política gestionada: AWSWickrFullAccess](#).

## Siguientes pasos

Ha completado los pasos de configuración de requisito previo. Para empezar a configurar Wickr, consulte [Introducción](#).

# Introducción a AWS Wickr

En esta guía le mostramos cómo comenzar a utilizar Wickr, crear una red, configurarla y crear usuarios.

## Temas

- [Requisitos previos](#)
- [Paso 1: crear una red](#)
- [Paso 2: configurar su red](#)
- [Paso 3: crear e invitar a usuarios](#)
- [Sigüientes pasos](#)
- [Cómo transferir Wickr Pro a AWS Wickr](#)

## Requisitos previos

Antes de empezar, asegúrese de que cumple los requisitos siguientes si no lo ha hecho todavía:

- Registro en Amazon Web Services (AWS) Para obtener más información, consulte [Configuración de AWS Wickr](#).
- Compruebe que tiene los permisos necesarios para administrar Wickr. Para obtener más información, consulte [AWS política gestionada: AWSWickrFullAccess](#).
- No se olvide de incluir en la lista de puertos y dominios permitidos los apropiados para Wickr. Para obtener más información, consulte [Lista de puertos y dominios que deben ser permitidos](#).

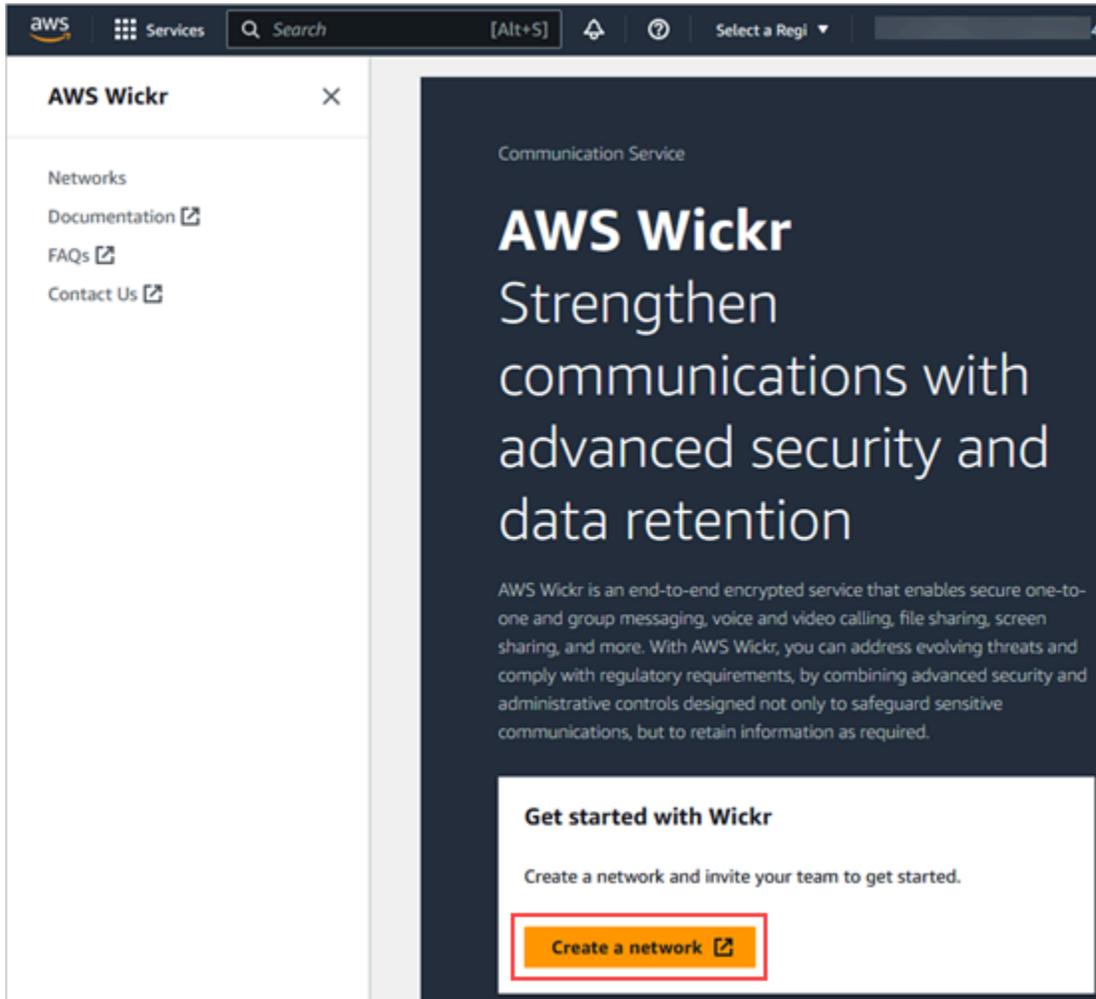
## Paso 1: crear una red

Siga el procedimiento que se indica a continuación para crear una red de Wickr para la cuenta.

1. Abre el formulario AWS Management Console Wickr en <https://console.aws.amazon.com/wickr/>.

**Note**

Si no ha creado una red de Wickr anteriormente, verá la página informativa del servicio de Wickr. Después de crear una o más redes de Wickr, verá la página Redes, con una lista de todas las redes de Wickr que ha creado.

**2. Elija Crear una red.**

3. Introduzca un nombre para la red en el cuadro de texto Nombre de la red. Seleccione un nombre significativo para los miembros de su organización, como el de su empresa o equipo.
4. Elija un plan. Puede elegir uno de los siguientes planes de red de Wickr:
  - Estándar: para equipos de pequeñas y grandes empresas que necesitan flexibilidad y controles administrativos.

- Prueba gratuita Premium o Premium: para empresas que requieren los límites de funciones más altos, controles administrativos detallados y retención de datos.

Los administradores pueden elegir la opción de prueba gratuita premium, que está disponible para un máximo de 30 usuarios y dura tres meses. Esta oferta está abierta a planes nuevos, de prueba gratuita y estándar. Los administradores pueden actualizar o bajar de categoría a los planes Premium o Estándar durante el período de prueba premium gratuito.

Para obtener más información sobre los planes y precios de Wickr disponibles, visite la [página de precios de Wickr](#).

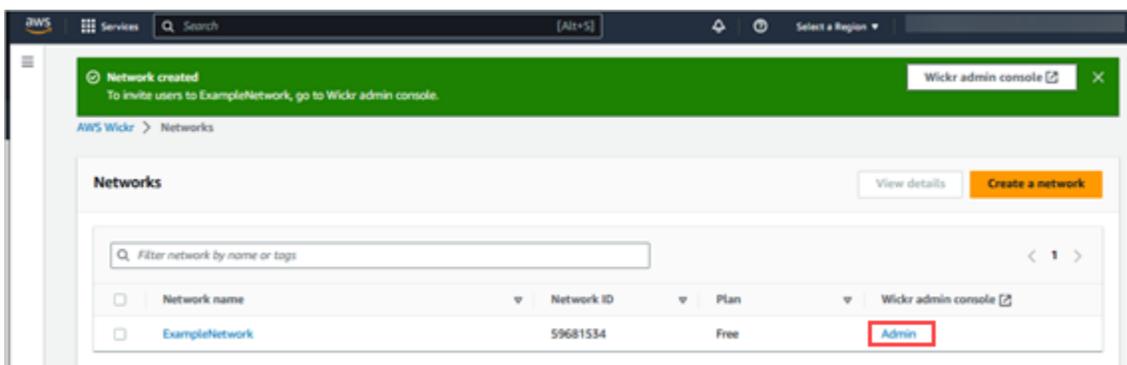
5. (Opcional) Seleccione Agregar nueva etiqueta si desea agregar una etiqueta a su red. Las etiquetas constan de un par clave-valor. Las etiquetas se pueden usar para buscar y filtrar los recursos o para un seguimiento de los costos de AWS . Para obtener más información, consulte [Etiquetas de red](#).
6. Seleccione Crear red.

Se te redirigirá a la página de redes AWS Management Console de Wickr y la nueva red aparecerá en la página.

## Paso 2: configurar su red

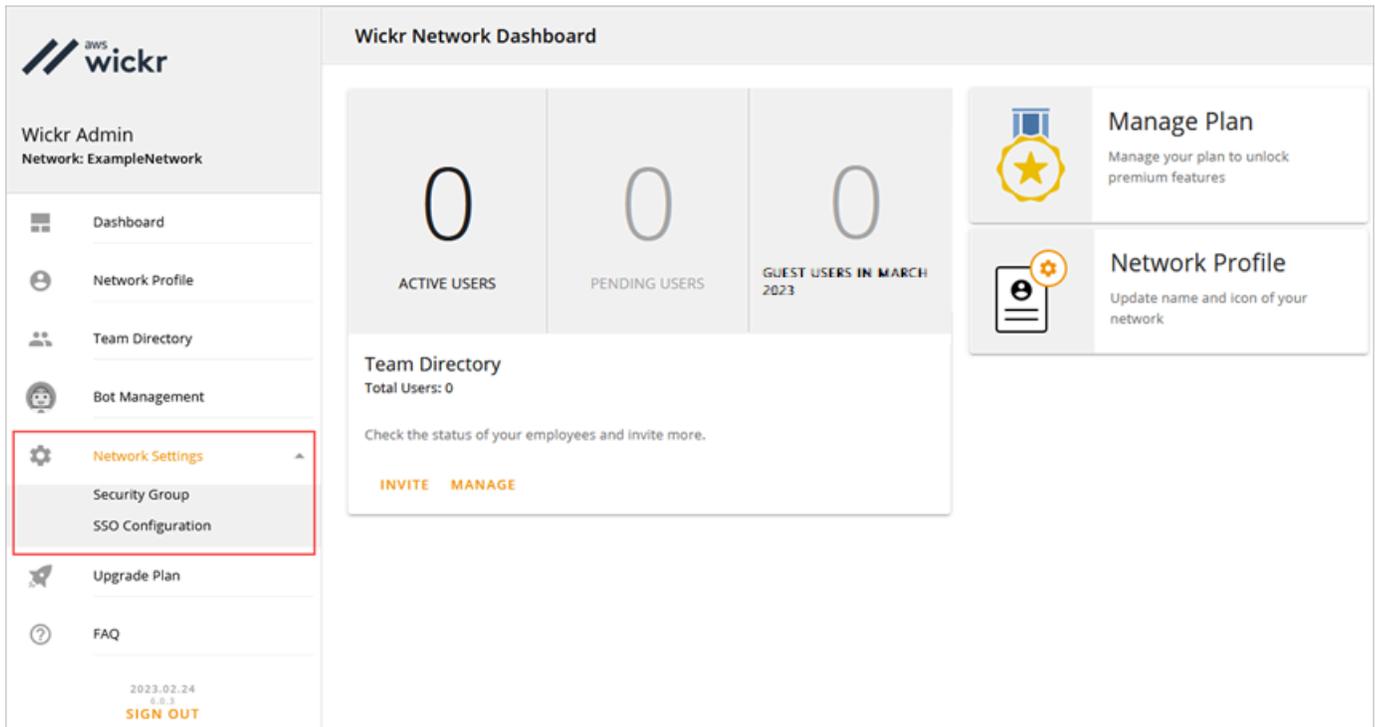
Siga el procedimiento que se indica a continuación para acceder a la consola de administración de Wickr, donde puede agregar usuarios y grupos de seguridad, configurar el SSO y la retención de datos y otros ajustes de la red.

1. En la página Redes, seleccione el enlace Admin para acceder a la consola de administración de Wickr de dicha red.



Se le redirigirá a la consola de administración de Wickr de la red seleccionada.

2. En el panel de navegación izquierdo de la consola de administración de Wickr, seleccione Configuración de red.



Están disponibles varias opciones de configuración, que se detallan a continuación. Para obtener más información sobre la configuración de estos ajustes, consulte [Cómo administrar su red de AWS Wickr](#).

- Grupo de seguridad: administre los grupos de seguridad y su configuración, como las políticas de complejidad de contraseñas, las preferencias de mensajería, las características de llamada, las características de seguridad y la federación externa. Para obtener más información, consulte [Grupos de seguridad](#).
- Configuración del SSO: configure el SSO y consulte la dirección del punto de conexión de su red Wickr. Wickr solo es compatible con los proveedores de SSO que utilizan OpenID Connect (OIDC). No se admiten los proveedores que utilizan lenguaje de marcado para configuraciones de seguridad (SAML). Para obtener más información, consulte [Configuración de inicio de sesión único](#).

## Paso 3: crear e invitar a usuarios

Para crear usuarios en la red de Wickr puede utilizar los métodos siguientes:

- Inicio de sesión único (SSO): si configura el SSO, puede invitar a usuarios compartiendo su ID de empresa de Wickr. Los usuarios finales se registran en Wickr con el ID de empresa proporcionado y su dirección de correo electrónico de empresa. Para obtener más información, consulte [Configuración de inicio de sesión único](#).
- Invitación: puede crear usuarios manualmente en la AWS Management Console de Wickr y enviarles una invitación por correo electrónico. Los usuarios finales pueden registrarse en Wickr con el enlace del correo electrónico.

### Note

También puede habilitar a usuarios invitados para su red de Wickr. Actualmente, la característica de usuario invitado se encuentra en la vista previa. Para obtener más información, consulte [Usuarios invitados](#).

Siga los procedimientos que se indican a continuación para crear usuarios o invitarlos.

### Note

Se considera que los administradores también son usuarios y, por lo tanto, se les debe invitar a las redes de Wickr con SSO o sin SSO.

## SSO

Escriba un correo electrónico y envíelo a los usuarios de SSO para que se registren en Wickr. En el mensaje, incluya la información siguiente:

- Su ID de empresa de Wickr. Al configurar el SSO, se especifica un ID de empresa de la red de Wickr. Para obtener más información, consulte [Cómo configurar el SSO](#).
- La dirección de correo electrónico que deben usar para registrarse.

- La URL para descargar el cliente de Wickr. Los usuarios pueden descargar los clientes de Wickr desde la página de descargas de AWS Wickr en <https://aws.amazon.com/wickr/download/>.

#### Note

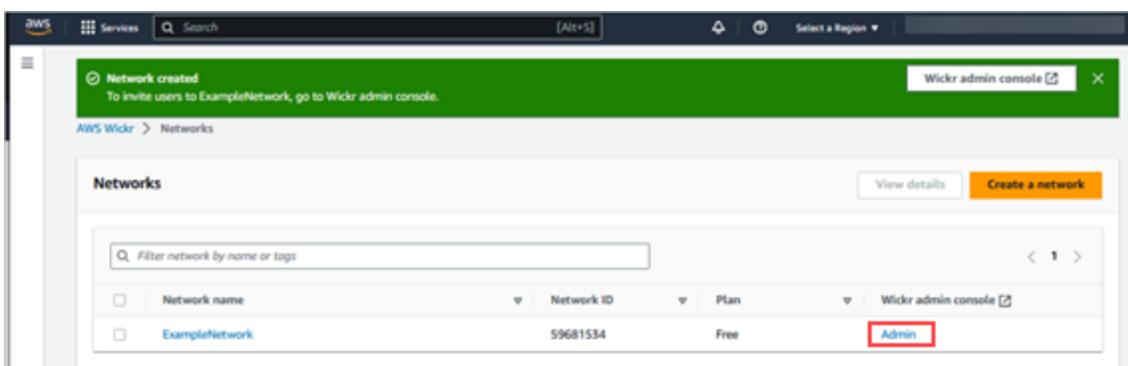
Si has creado tu red Wickr en AWS GovCloud (EE. UU. al oeste), pide a tus usuarios que descarguen e instalen el cliente. WickrGov Para el resto de AWS regiones, pide a tus usuarios que descarguen e instalen el cliente Wickr estándar. Para obtener más información al respecto AWS WickrGov, consulte [AWS WickrGov](#) la Guía del AWS GovCloud (US) usuario.

Los usuarios que se van registrando en su red de Wickr se agregan al directorio del equipo de Wickr con el estado activo.

## Non-SSO

Para crear usuarios de Wickr manualmente y enviar invitaciones, siga estos pasos:

1. Abre el formulario AWS Management Console de Wickr en <https://console.aws.amazon.com/wickr/>.
2. En la página Redes, seleccione el enlace Admin para acceder a la consola de administración de Wickr de dicha red.



La página Redes.

Se le redirigirá a la consola de administración de Wickr de una red específica. En la consola de administración de Wickr puede agregar a usuarios y grupos de seguridad, configurar el SSO y la retención de datos y ajustes adicionales para la red específica que ha seleccionado.

3. En el panel de navegación de la consola de administración de Wickr, elija Usuarios y, luego, Directorio de equipos.

En la página Usuarios puede agregar a usuarios individuales seleccionando Crear nuevo usuario. También puede agregar a usuarios en bloque; para ello, seleccione el icono Añadir usuarios en el panel de navegación superior. Seleccione el icono Descargar CSV para descargar una plantilla CSV que podrá editar y cargar con su lista de usuarios.

4. Especifique el nombre y apellidos, el código de país, el número de teléfono y la dirección de correo electrónico del usuario. El único campo obligatorio es la dirección de correo electrónico. Asegúrese de elegir el grupo de seguridad adecuado para los usuarios.
5. Seleccione Crear.

New User

**User Information**

First Name  
Example

Last Name  
User

Country Code  
+1

Phone Number  
201-200-0000

**Account Information**

Email

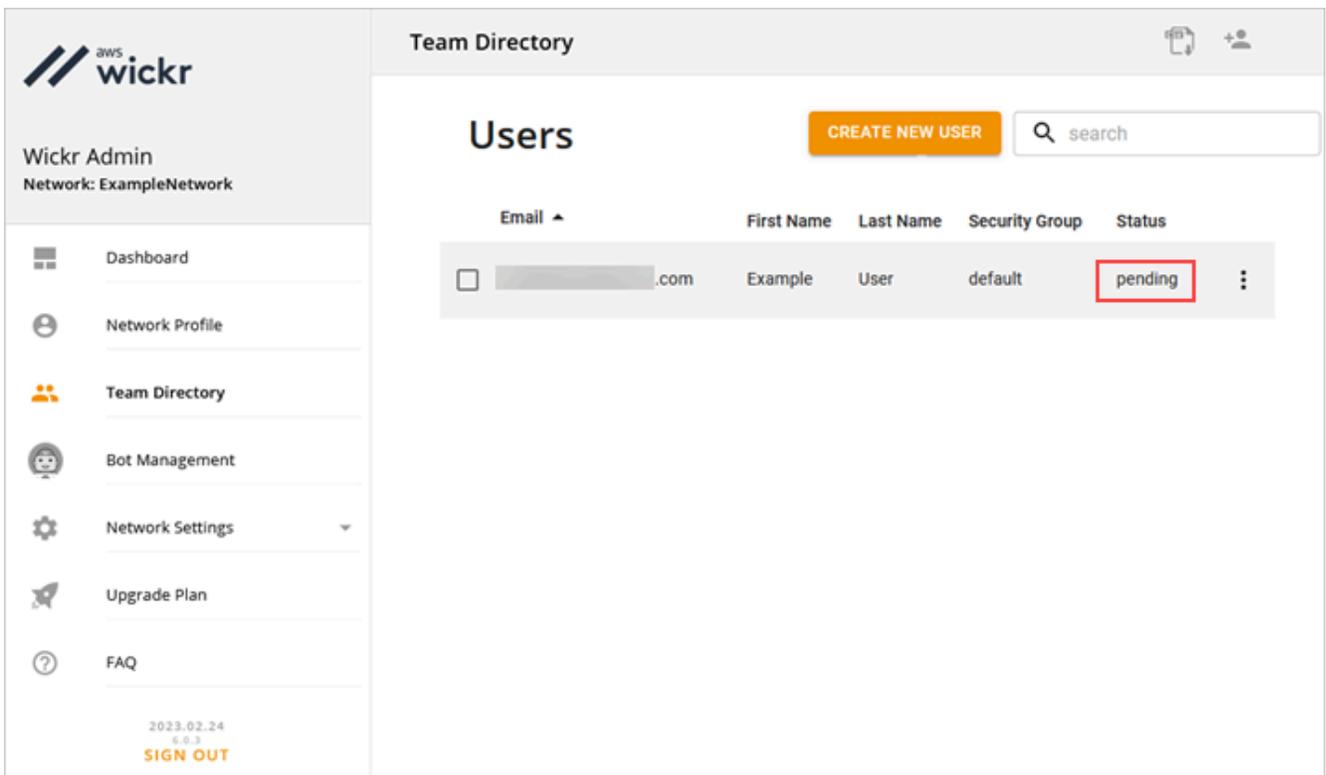
default

CANCEL CREATE

Wickr envía al usuario un correo electrónico de invitación a la dirección que se especifique. El correo electrónico incluye enlaces para descargar las aplicaciones de cliente Wickr y un enlace para registrarse en Wickr. Para obtener más información sobre la experiencia del

usuario final, consulte [\(Descargar la aplicación Wickr y aceptar la invitación\)](#) en la Guía del usuario de AWS Wickr.

A medida que los usuarios se registren en Wickr utilizando su enlace del correo electrónico, su estado en el directorio del equipo de Wickr cambiará de Pendiente a Activo.



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

## Siguientes pasos

Ya ha completado los primeros pasos. Para administrar Wickr, consulte las guías siguientes:

- [Cómo administrar su red de AWS Wickr](#)
- [Cómo gestionar usuarios en AWS Wickr](#)

## Cómo transferir Wickr Pro a AWS Wickr

### Note

Wickr Pro dejará de fabricarse el 27 de marzo de 2024.

En esta guía le mostramos cómo transferir desde Wickr Pro y comenzar a utilizar AWS Wickr.

Sigue los pasos de esta guía si ya tienes una red Wickr Pro, pero AÚN NO la tienes. Cuenta de AWS No dude en ponerse en contacto con el servicio de asistencia en cualquier momento si necesita ayuda.

Si su organización ya tiene una AWS cuenta, complete el formulario [Migrar de Wickr Pro a AWS Wickr](#) y el soporte de AWS Wickr lo ayudará.

Necesitará un Cuenta de AWS ID para administrar su red de AWS Wickr como Servicio de AWS. Para obtener más información sobre qué Cuenta de AWS es una cuenta y cómo administrarla, consulte la [Guía de referencia sobre la administración de AWS cuentas](#).

## Temas

- [Paso 1: Crea una AWS cuenta](#)
- [Paso 2: recuperar su ID de red de Wickr](#)
- [Paso 3: enviar una solicitud](#)
- [Paso 4: Inicie sesión en su consola AWS](#)

## Paso 1: Crea una AWS cuenta

Complete el siguiente procedimiento para crear una AWS cuenta.

1. Si su organización no tiene un ID de cuenta de AWS existente, puede empezar por crear un ID de AWS cuenta independiente. Para ello, necesitará algunos elementos clave:
  - Una tarjeta de crédito o débito para la facturación
  - Una dirección de correo electrónico a la que pueda acceder un grupo (recomendada, no obligatoria)
  - Seleccione un AWS Support plan. Para obtener más información, consulte [Cambio de los planes de AWS Support](#).

### Note

Siempre puede cambiar su AWS Support plan a medida que obtenga más información sobre sus necesidades.

2. Configure el acceso administrativo a través de IAM como práctica recomendada de seguridad (opcional pero recomendable). Para obtener más información, consulte [Administración de identidad y acceso en AWS](#). Para obtener instrucciones más específicas sobre el acceso administrativo de AWS Wickr, consulte la [política AWS administrada: AWSWickrFullAccess](#).
3. Una vez que complete los pasos anteriores, podrá iniciar sesión en el AWS Management Console y encontrar su Cuenta de AWS ID de 12 dígitos debajo del nombre de su cuenta.

## Paso 2: recuperar su ID de red de Wickr

Siga el procedimiento que se detalla a continuación para recuperar el ID de red de Wickr.

1. Inicie sesión en su consola de administración de Wickr actual, seleccione las redes que desea migrar y, a continuación, seleccione Perfil de red.
2. La página Perfil de red muestra su ID de red, que es un ID numérico de 8 dígitos.

## Paso 3: enviar una solicitud

Ahora que tiene su Cuenta de AWS ID y su ID de red de Wickr Pro, tendrá que completar el formulario [Migrar de Wickr Pro a AWS Wickr](#).

Una vez rellenado, normalmente en un plazo máximo de 14 días, un representante de soporte de AWS Wickr se pondrá en contacto con usted para confirmar que su red de Wickr se ha agregado a su Cuenta de AWS.

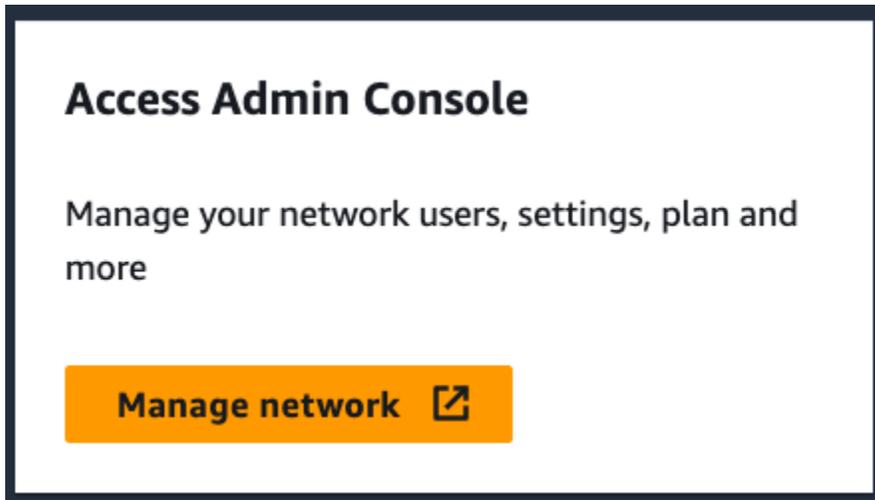
## Paso 4: Inicie sesión en su consola AWS

### Note

Siga estos pasos DESPUÉS de recibir la confirmación de que su red Wickr Pro se ha agregado a su Cuenta de AWS.

1. Puede iniciar sesión en la AWS consola como usuario root O con un usuario de IAM que haya creado previamente (como se recomienda) en el paso 2 para AWS Wickr.
2. Vaya a su servicio AWS Wickr. Puede hacerlo desde el menú Servicios o buscando AWS Wickr en la barra de búsqueda.

3. En la página de AWS Wickr, seleccione Administrar red para acceder a su lista de redes de Wickr.



El botón Administrar red.

4. En la página Redes, en la columna de la consola de administración de Wickr, seleccione el enlace de administrador situado a la derecha del nombre de red deseado.



El enlace de la consola de administración.

5. La transferencia se ha completado con éxito. Verá su panel de control de red de Wickr.

La facturación de su red se transferirá ahora a su Cuenta de AWS. Espere hasta 3 días hábiles para que el equipo de soporte se ponga en contacto con usted y lo confirme. Tras recibir la confirmación, podrá ver y pagar su factura a través de la AWS consola.

# Cómo administrar su red de AWS Wickr

En la sección Configuración de red de Wickr, puede administrar el AWS Management Console nombre de su red de Wickr, los grupos de seguridad, la configuración de SSO y la configuración de retención de datos.

## Temas

- [Perfil de red](#)
- [Grupos de seguridad](#)
- [Configuración de inicio de sesión único](#)
- [Lee los recibos](#)
- [Etiquetas de red](#)
- [Administrar el plan de red](#)
- [Retención de datos](#)
- [¿Qué es ATAК?](#)
- [Lista de puertos y dominios que deben ser permitidos](#)
- [GovCloud clasificación y federación transfronterizas](#)

## Perfil de red

Puedes editar el nombre de tu red de Wickr y ver el ID de la red en la sección Perfil de red de la sección correspondiente a Wickr. AWS Management Console

## Temas

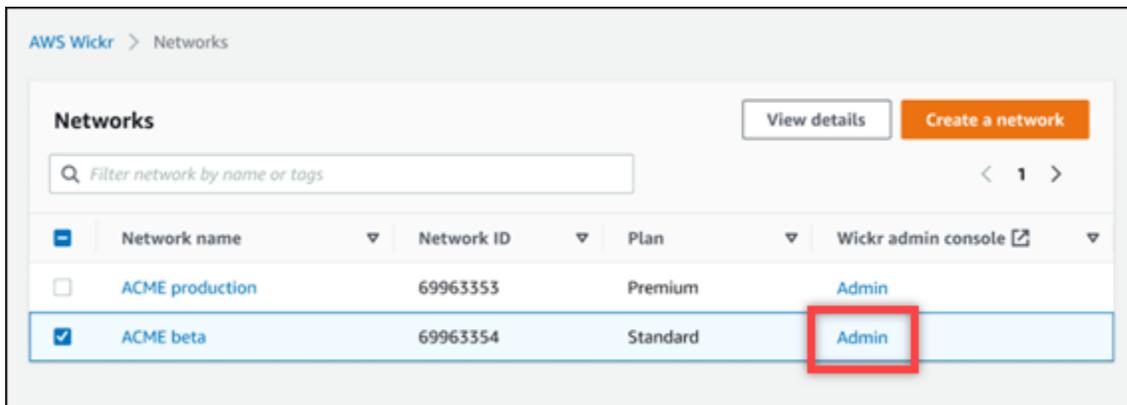
- [Cómo consultar el perfil de red](#)
- [Editar el nombre de la red](#)

## Cómo consultar el perfil de red

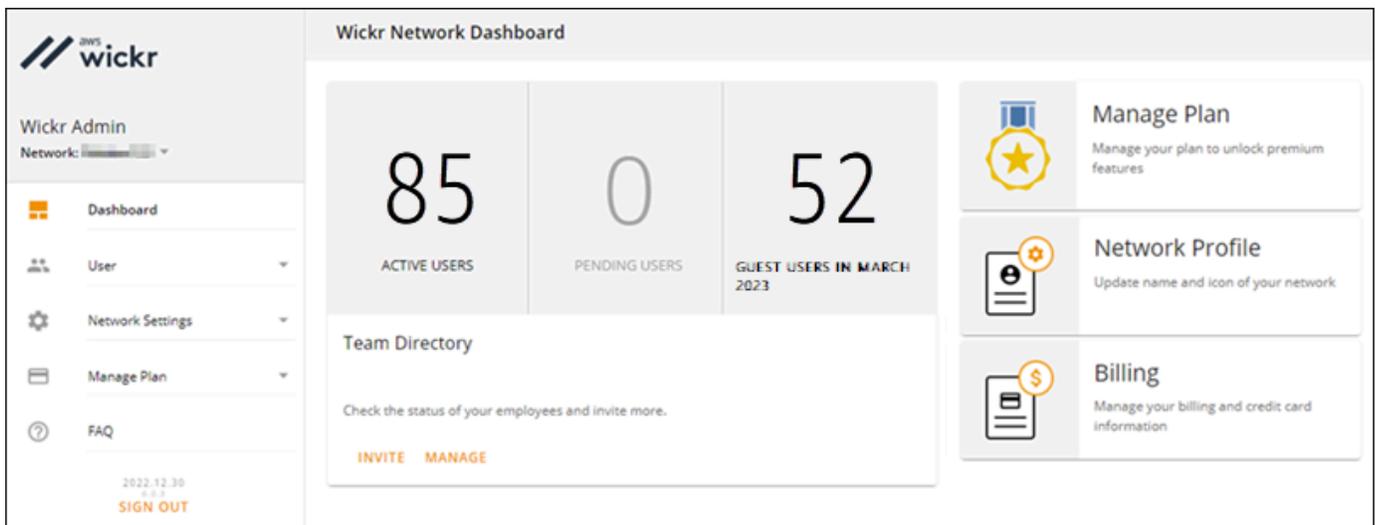
Siga el procedimiento indicado a continuación para ver el perfil de su red de Wickr y el ID de la red.

1. [Abre el formulario de AWS Management Console Wickr en https://console.aws.amazon.com/wickr/.](https://console.aws.amazon.com/wickr/)

- En la página Redes, seleccione el enlace Admin para acceder a la consola de administración de Wickr de dicha red.



Se le redirigirá a la consola de administración de Wickr de una red específica.



- En el panel de navegación de la consola de administración de Wickr, elija Configuración de red y, a continuación, Perfil de red.

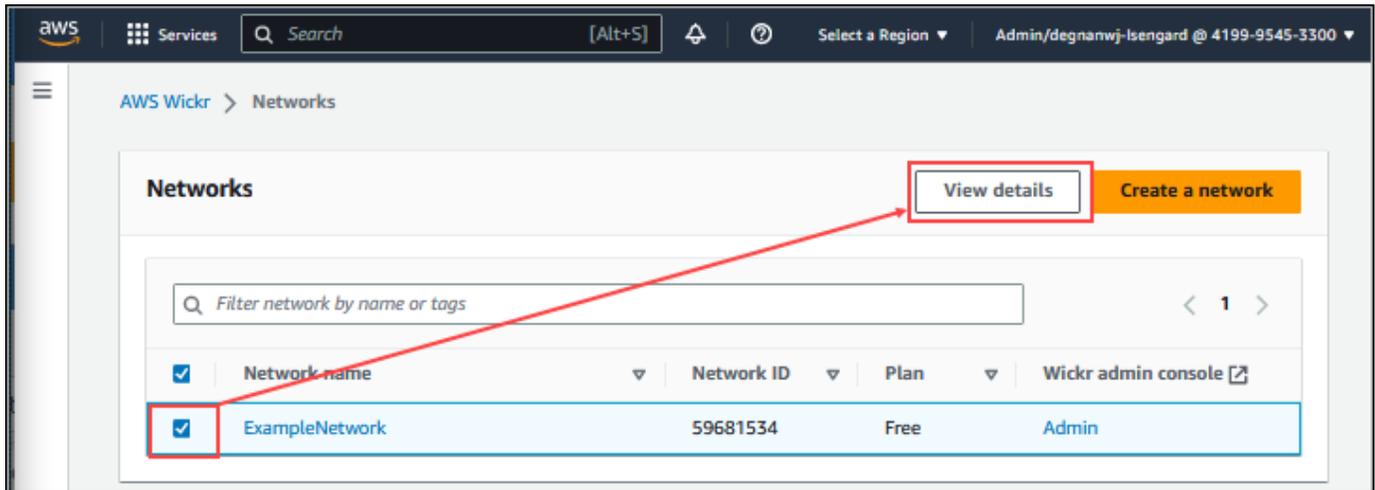
La página Perfil de red muestra el nombre y el identificador de red de Wickr. Use el ID de red para configurar la federación.

## Editar el nombre de la red

Siga el procedimiento que se indica a continuación para editar el nombre de la red de Wickr.

- [Abre el formulario AWS Management Console para Wickr en https://console.aws.amazon.com/wickr/.](https://console.aws.amazon.com/wickr/)

2. Elija Administrar red.
3. En la página Redes, seleccione la casilla de verificación situada junto al nombre de la red que desea editar y, a continuación, seleccione Ver detalles.



4. En la sección Información general de redes, elija Editar.
5. Ingrese un nuevo nombre para la red en el cuadro de texto Nombre de la red.
6. Seleccione Guardar cambios para guardar el nuevo nombre de la red.

## Grupos de seguridad

En la sección Grupos de seguridad de Wickr, puedes administrar los AWS Management Console grupos de seguridad y sus configuraciones, como las políticas de complejidad de contraseñas, las preferencias de mensajería, las funciones de llamadas, las funciones de seguridad y la federación de redes.

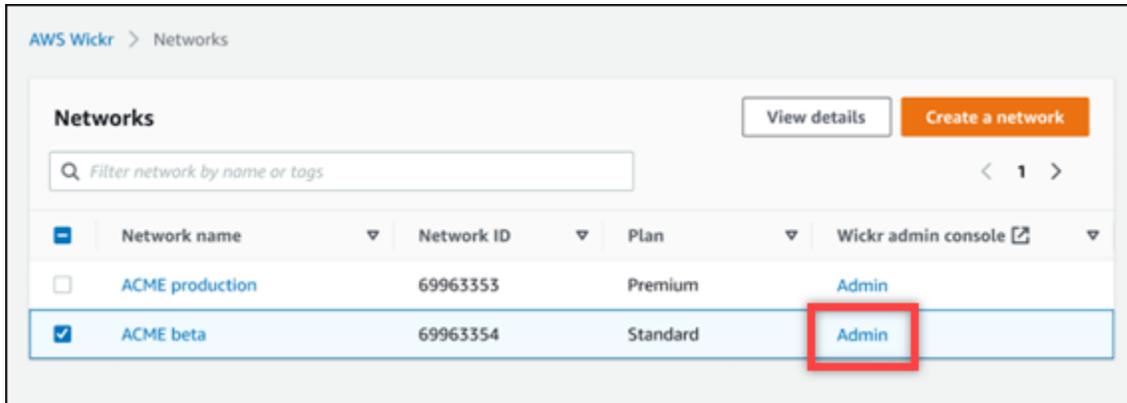
### Temas

- [Cómo consultar los grupos de seguridad](#)
- [Creación de un grupo de seguridad](#)
- [Cómo editar un grupo de seguridad](#)
- [Eliminación de un grupo de seguridad](#)

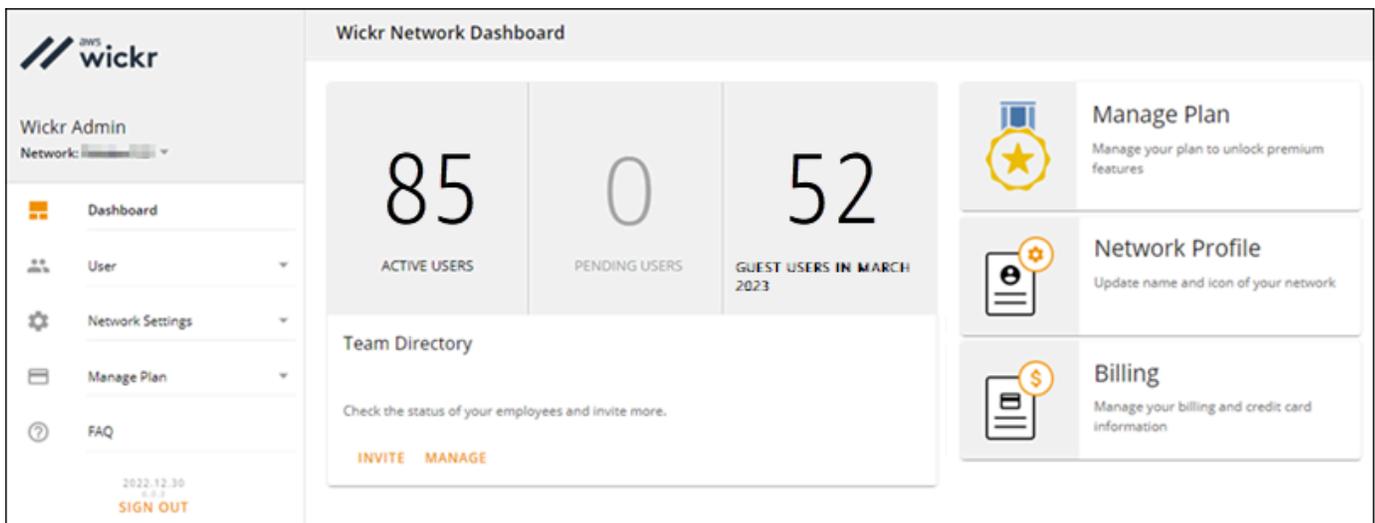
## Cómo consultar los grupos de seguridad

Siga el procedimiento indicado a continuación para ver los grupos de seguridad.

1. [Abre el formulario AWS Management Console para Wickr en https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. En la página Redes, seleccione el enlace Admin para acceder a la consola de administración de Wickr de dicha red.



Se le redirigirá a la consola de administración de Wickr de una red específica.



3. En el panel de navegación de la consola de administración de Wickr, seleccione Configuración de red y, a continuación, Grupo de seguridad.

La página Grupos de seguridad muestra sus grupos de seguridad de Wickr actuales y le permite consultar información detallada o crear un grupo nuevo.

## Creación de un grupo de seguridad

Siga el procedimiento indicado a continuación para crear un grupo de seguridad.

1. [Abre el formulario AWS Management Console para Wickr en https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. En la página Redes, seleccione el enlace Admin para acceder a la consola de administración de Wickr de dicha red.

Se le redirigirá a la consola de administración de Wickr de una red específica.

3. En el panel de navegación de la consola de administración de Wickr, seleccione Configuración de red y, a continuación, Grupo de seguridad.
4. Para crear un nuevo grupo de seguridad, seleccione Grupo nuevo.

Se agrega automáticamente un nuevo grupo de seguridad con un nombre predeterminado a la lista de grupos de seguridad.

Para más información sobre cómo editar el nuevo grupo de seguridad, consulte [Cómo editar un grupo de seguridad](#).

## Cómo editar un grupo de seguridad

Siga el procedimiento indicado a continuación para editar grupos de seguridad.

1. [Abre el formulario AWS Management Console para Wickr en https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. En la página Redes, seleccione el enlace Admin para acceder a la consola de administración de Wickr de dicha red.

Se le redirigirá a la consola de administración de Wickr de una red específica.

3. En el panel de navegación de la consola de administración de Wickr, seleccione Configuración de red y, a continuación, Grupo de seguridad.
4. Seleccione Detalles junto al nombre del grupo de seguridad que desea editar.

La página Detalles del grupo de seguridad muestra la configuración del grupo de seguridad en varias pestañas.

5. Están disponibles las pestañas y la configuración correspondiente siguientes:

- Nombre del grupo de seguridad: haga clic en el icono del lápiz situado junto al nombre del grupo para editarlo.
- General: permite editar la configuración básica del grupo.

- Mensajería: sirve para gestionar las características de mensajería para los miembros del grupo.
  - Llamar: permite gestionar las características de llamada para los miembros del grupo.
  - Seguridad: sirve para configurar las características de seguridad adicionales del grupo.
  - Federación: se refiere a la capacidad de comunicarse entre redes. Puede configurar los parámetros en la consola de administración de las redes en el nivel del grupo de seguridad. AWS Wickr tiene dos tipos de federación: local y global.
    - Federación local: la capacidad de federarse con los usuarios de AWS en otras redes de la misma región. Por ejemplo, si hay dos redes en Canadá, con la federación local habilitada podrán comunicarse entre sí.
    - Federación global: la capacidad de federarse con usuarios empresariales o usuarios de AWS de otra red distinta que pertenezcan a otras regiones. Por ejemplo, si hay un usuario en una red de la región de Canadá y otro en una red de la región de Londres, y la federación global está activada en ambas redes, podrán comunicarse entre sí.
    - Federación restringida: la capacidad de federarse con redes específicas (empresariales o AWS) que pertenecen a diferentes regiones. Los administradores pueden incluir en una lista las redes específicas con las que sus usuarios pueden federarse. Tras la restricción, los usuarios solo pueden comunicarse con los usuarios de las redes de la lista de permitidos. Para usar la federación restringida, ambas redes deben incluirse en la lista de permitidos desde la configuración del grupo de seguridad de la pestaña de federación.
6. Seleccione Guardar para guardar las modificaciones que realice en la información del grupo de seguridad.

## Eliminación de un grupo de seguridad

Siga el procedimiento indicado a continuación para eliminar un grupo de seguridad.

1. [Abre el formulario AWS Management Console de Wickr en https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. En la página Redes, seleccione el enlace Admin para acceder a la consola de administración de Wickr de dicha red.

Se le redirigirá a la consola de administración de Wickr de una red específica.

3. En el panel de navegación de la consola de administración de Wickr, seleccione Configuración de red y, a continuación, Grupo de seguridad.

4. Seleccione el icono de los puntos suspensivos verticales situado junto al nombre del grupo de seguridad que desea eliminar.
5. Seleccione Eliminar para eliminar el grupo de seguridad.

Si se elimina un grupo de seguridad que tiene usuarios asignados, dichos usuarios se agregarán automáticamente al grupo de seguridad predeterminado. Para modificar el grupo de seguridad asignado a los usuarios, consulte [Cómo editar usuarios](#).

## Configuración de inicio de sesión único

En la sección de configuración del SSO de Wickr, puedes configurar Wickr AWS Management Console para que utilice un sistema de inicio de sesión único para autenticarse. El SSO proporciona una capa de seguridad adicional cuando se combina con un sistema de autenticación multifactor (MFA) adecuado. Wickr solo es compatible con los proveedores de SSO que utilizan OpenID Connect (OIDC). No se admiten los proveedores que utilizan lenguaje de marcado para configuraciones de seguridad (SAML).

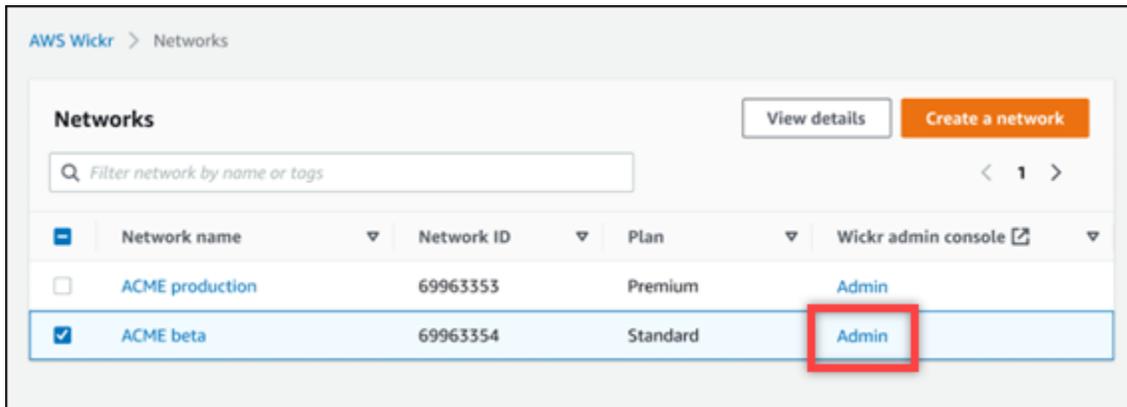
### Temas

- [Cómo ver la información del SSO](#)
- [Cómo configurar el SSO](#)
- [Periodo de gracia para la actualización del token](#)

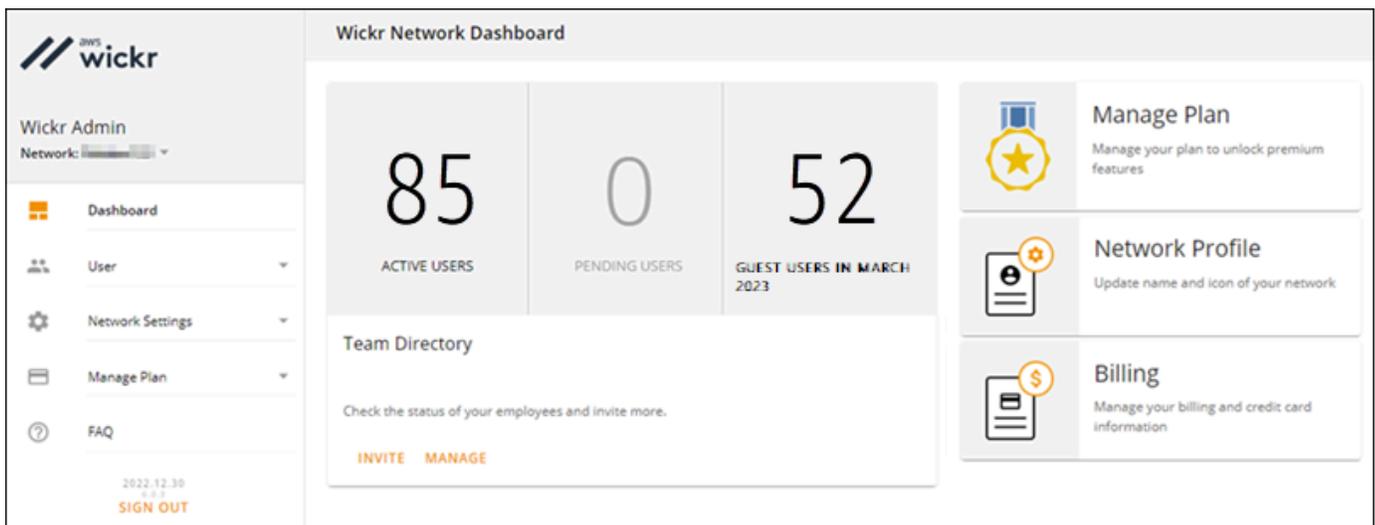
## Cómo ver la información del SSO

Siga el procedimiento indicado a continuación para ver la configuración de inicio de sesión único actual de la red Wickr, si la hay. También puede ver el punto de conexión de red de su red Wickr.

1. [Abre el formulario para Wickr en https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/). [AWS Management Console](#)
2. En la página Redes, seleccione el enlace Admin para acceder a la consola de administración de Wickr de dicha red.



Se le redirigirá a la consola de administración de Wickr de una red específica.



- En el panel de navegación de la consola de administración de Wickr, seleccione Configuración de red y, a continuación Configuración del SSO.

La página Configuración del inicio de sesión único y LDAP muestra su punto de conexión de red Wickr y la configuración del SSO actual.

## Cómo configurar el SSO

Para más información acerca de la configuración del SSO, consulte las siguientes guías en el Centro de ayuda de Wickr:

### **⚠ Important**

Al configurar el SSO, se especifica un ID de empresa para la red de Wickr. Asegúrese de escribir el ID de su empresa de su red de Wickr. Debe proporcionárselo a sus usuarios

finales cuando envíe los correos electrónicos de invitación. Los usuarios finales deben especificar el ID de su empresa cuando se registren en su red de Wickr.

- [Cómo configurar el inicio de sesión único para Azure AD](#)
- [Cómo configurar el inicio de sesión único para Okta](#)

## Periodo de gracia para la actualización del token

Los proveedores de identidad pueden sufrir interrupciones temporales o prolongadas. Como consecuencia de ello, la sesión de los usuarios se puede cerrar de forma inesperada debido a un error en el token de actualización de la sesión de cliente. Para evitar este problema, puede establecer un período de gracia que permita a sus usuarios mantener la sesión iniciada incluso en caso de error del token de actualización del cliente durante dichas interrupciones.

Las opciones disponibles para el período de gracia son las siguientes:

- Sin período de gracia (opción predeterminada): la sesión de los usuarios se cerrará inmediatamente después del error de token de actualización.
- Período de gracia de 30 minutos: los usuarios pueden permanecer conectados hasta 30 minutos después del error de token de actualización.
- Período de gracia de 60 minutos: los usuarios pueden permanecer conectados hasta 60 minutos después del error de token de actualización.

## Lee los recibos

Los recibos de lectura en Wickr son notificaciones que se envían al remitente para mostrar cuándo se ha leído su mensaje. Estos recibos están disponibles en one-on-one las conversaciones. Aparecerá una sola marca de verificación para los mensajes enviados y un círculo continuo con una marca de verificación para los mensajes leídos. Para ver las confirmaciones de lectura de los mensajes durante conversaciones externas, ambas redes deben tener habilitadas las confirmaciones de lectura.

Los administradores pueden activar o desactivar las confirmaciones de lectura en el panel de administración. Esta configuración se aplicará a toda la red.

Complete el siguiente procedimiento para activar o desactivar las confirmaciones de lectura.

1. Abre el formulario AWS Management Console de Wickr en <https://console.aws.amazon.com/wickr/>.
2. En el panel de navegación de la consola de administración de Wickr, elija Configuración de red y, a continuación, Perfil de red.
3. En la página de perfil de la red, en la sección Leer recibos, selecciona Editar.
4. Selecciona Activar o Desactivar.

## Etiquetas de red

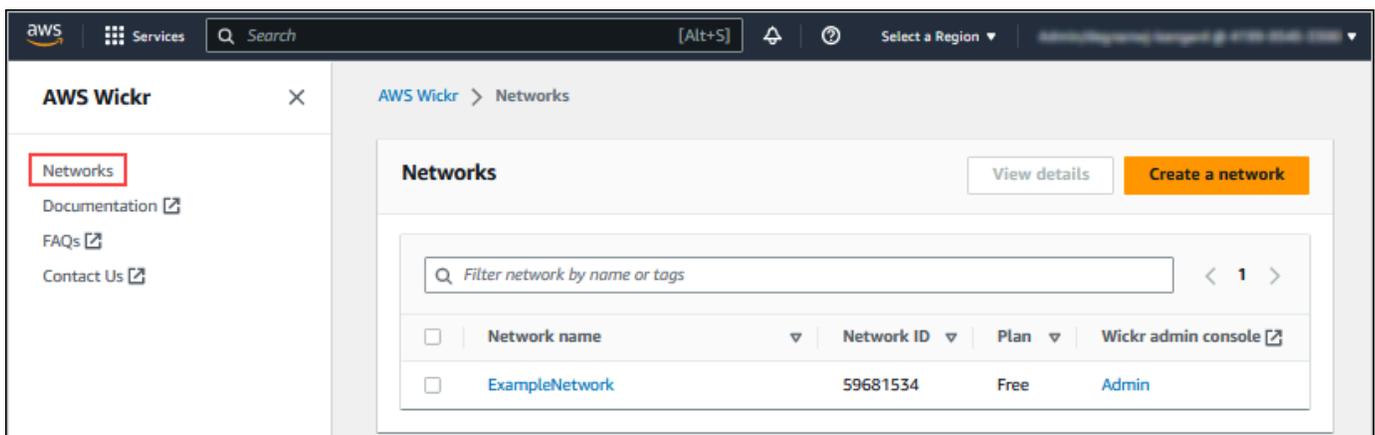
Es posible aplicar etiquetas a las redes de Wickr, Luego puedes usar esas etiquetas para buscar y filtrar tus redes de Wickr o hacer un seguimiento de tus AWS costos. Puedes configurar las etiquetas de red en la página de descripción general de la red de AWS Management Console Wickr.

Una etiqueta es un [par clave-valor](#) que se aplica a un recurso para almacenar metadatos sobre ese recurso. Cada etiqueta consta de una clave y un valor. Para más información sobre las etiquetas, consulte también [¿Qué son las etiquetas?](#) y [Casos de uso de etiquetado](#).

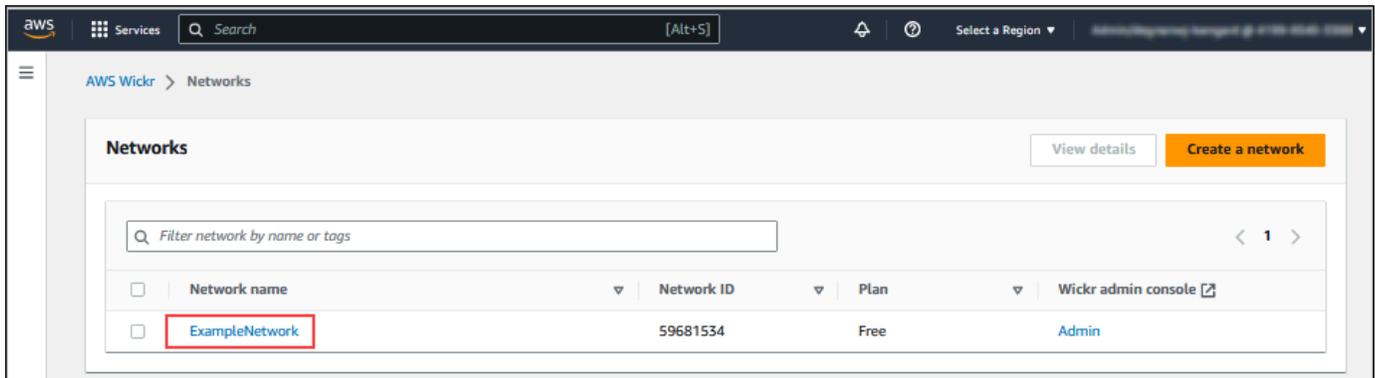
## Cómo administrar las etiquetas de red

Siga el procedimiento indicado a continuación para administrar las etiquetas de red en su red Wickr.

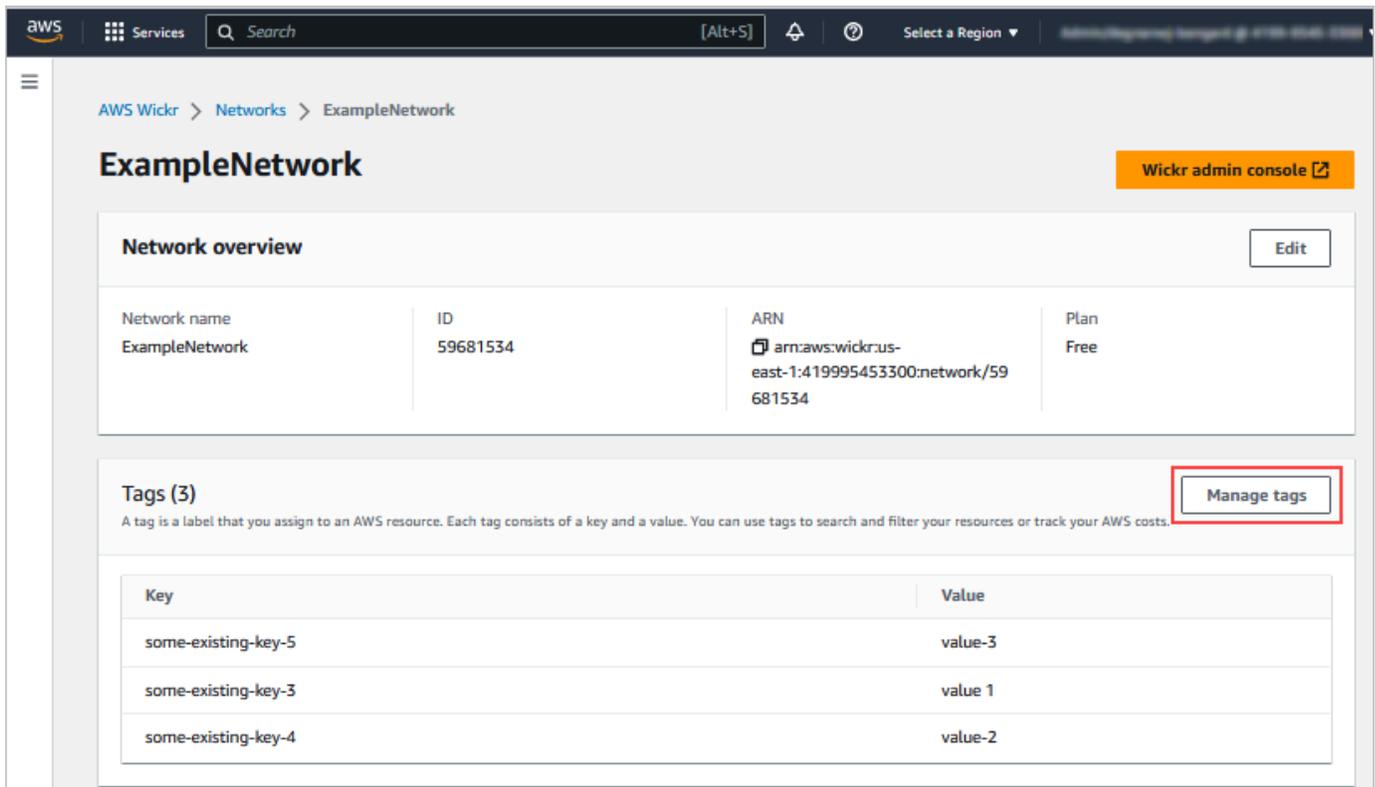
1. [Abre el formulario AWS Management Console para Wickr en https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. Haga clic en Redes, en el panel de navegación de la AWS Management Console de Wickr.



3. En la página Redes, seleccione el nombre de la red para la que desea administrar etiquetas.



4. En la página Información general sobre la red, elija Administrar etiquetas.



5. En la página Administrar etiquetas, puede completar una de las siguientes opciones:

- Agregar etiquetas nuevas: escriba nuevas etiquetas en forma de pares clave-valor. Seleccione Agregar nueva etiqueta para añadir varios pares clave-valor. Las etiquetas distinguen entre mayúsculas y minúsculas. Para obtener más información, consulte [Cómo agregar etiquetas de red](#).
- Editar las etiquetas existentes: seleccione el texto de la clave o el valor de una etiqueta existente y, a continuación, modifique la información necesaria en el cuadro de texto. Para obtener más información, consulte [Cómo modificar las etiquetas de red](#).

- Eliminar etiquetas existentes: haga clic en el botón Eliminar junto a la etiqueta que desee eliminar. Para obtener más información, consulte [Cómo eliminar las etiquetas de red](#).

## Cómo agregar etiquetas de red

Siga el procedimiento que se indica a continuación para agregar etiquetas a la red de Wickr. Para más información sobre la administración de etiquetas, consulte [Cómo administrar las etiquetas de red](#).

1. En la página Administración de etiquetas, seleccione Agregar nueva etiqueta.
2. En los campos Clave y Valor que estén vacíos, indique el nuevo par de clave-valor de la etiqueta.
3. Seleccione Guardar cambios para guardar las nuevas etiquetas.

The screenshot shows the AWS Wickr 'Manage Tags' interface. The breadcrumb navigation is 'AWS Wickr > Networks > ExampleNetwork > Manage tags'. The main heading is 'Manage Tags'. Below this, there is a table with two columns: 'Key' and 'Value - Required'. The table contains five rows 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 the 'Save changes' button is also highlighted with a red box.

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

Cancel Save changes

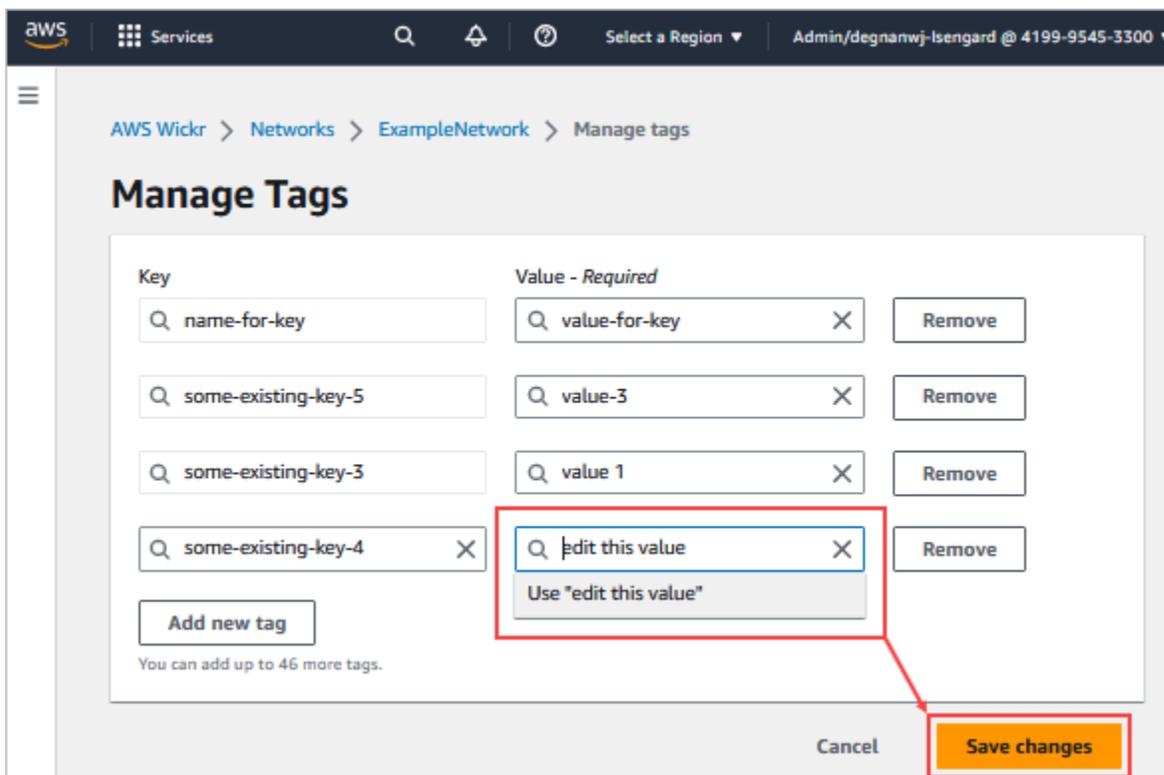
## Cómo modificar las etiquetas de red

Siga el procedimiento indicado a continuación para editar etiquetas asociadas a la red de Wickr. Para más información sobre la administración de etiquetas, consulte [Cómo administrar las etiquetas de red](#).

1. En la página Administrar etiquetas, edite el valor de la etiqueta.

### Note

No es posible editar las claves de las etiquetas. En su lugar, elimine el par de clave-valor y agregue una nueva etiqueta con la nueva clave.

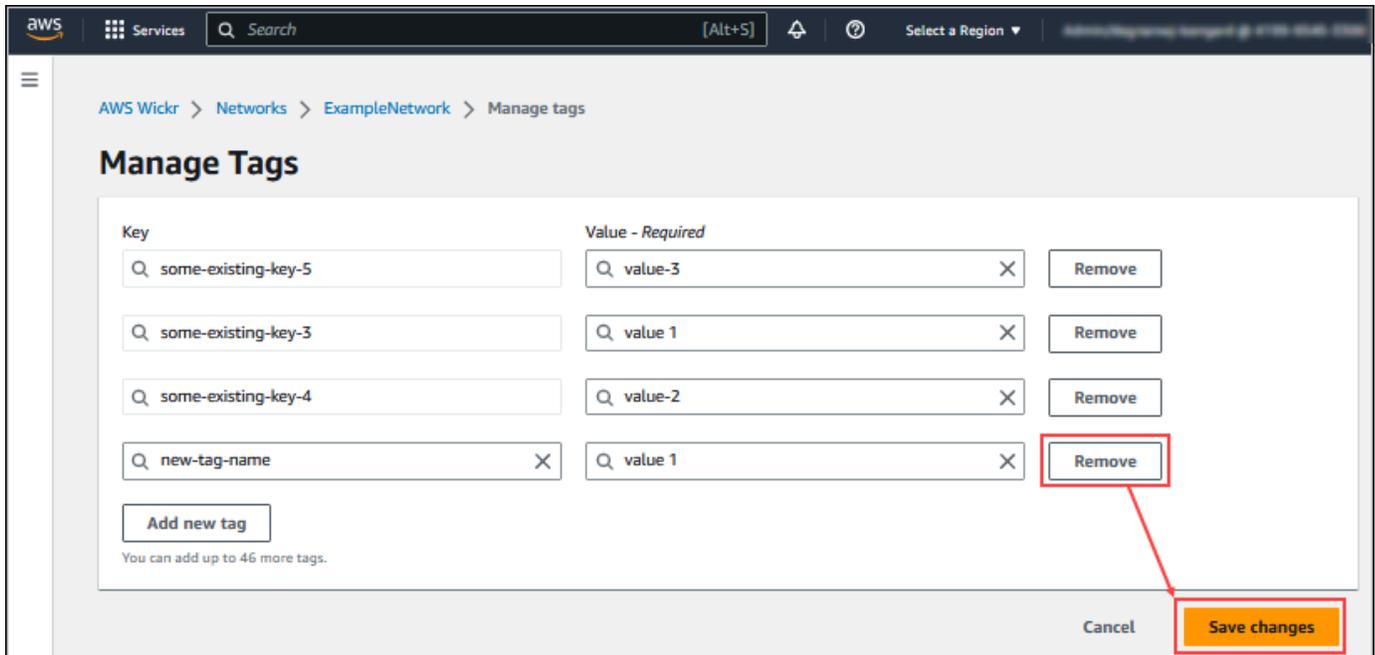


2. Elija Guardar cambios para guardar las modificaciones.

## Cómo eliminar las etiquetas de red

Siga el procedimiento indicado a continuación para eliminar etiquetas de red de Wickr. Para más información sobre la administración de etiquetas, consulte [Cómo administrar las etiquetas de red](#).

1. En la página Administrar etiquetas, elija Eliminar junto a las etiquetas que desee suprimir.



2. Elija Guardar cambios para guardar las modificaciones.

## Administrar el plan de red

En la sección Administrar el AWS Management Console plan de Wickr, puedes administrar tu plan de red en función de las necesidades de tu empresa.

Para administrar su plan de red, complete el siguiente procedimiento.

1. Abre el formulario AWS Management Console de Wickr en <https://console.aws.amazon.com/wickr/>.
2. En el panel de navegación de la consola de administración de Wickr, selecciona Administrar plan y, a continuación, selecciona Mi plan.
3. En la página Mi plan, selecciona el plan de red que desees. Puede modificar su plan de red actual seleccionando una de las siguientes opciones:
  - Estándar: para equipos de pequeñas y grandes empresas que necesitan flexibilidad y controles administrativos.
  - Prueba gratuita Premium o Premium: para empresas que requieren los límites de funciones más altos, controles administrativos detallados y retención de datos.

Los administradores pueden elegir la opción de prueba gratuita premium, que está disponible para un máximo de 30 usuarios y dura tres meses. Esta oferta está abierta a planes nuevos, de prueba gratuita y estándar. Los administradores pueden actualizar o bajar de categoría a los planes Premium o Estándar durante el período de prueba premium gratuito.

 Note

Para detener el uso y la facturación de su red, elimine todos los usuarios de la red, incluidos los usuarios suspendidos.

## Limitaciones de la prueba gratuita de Premium

Se aplican las siguientes limitaciones a la prueba gratuita premium:

- Si un plan ha estado inscrito anteriormente en una versión de prueba gratuita premium, no será elegible para otra prueba.
- Solo se puede inscribir una red para cada AWS cuenta en una prueba gratuita premium.
- La función de usuario invitado no está disponible durante la prueba gratuita premium.
- Si una red estándar tiene más de 30 usuarios, no será posible pasarla a una versión de prueba gratuita premium.

## Retención de datos

Según la retención de datos de AWS Wickr, se pueden conservar todas las conversaciones en la red. Esto incluye las conversaciones a través de mensajería directa y las de grupos o salas entre miembros de la red (internos) y miembros de otros equipos (externos) con los que la red comparta una federación. La retención de datos solo está disponible para los usuarios del plan Premium de AWS Wickr y los clientes empresariales que elijan la retención de datos. Para más información sobre el plan Premium, consulte [Tarifas de Wickr](#).

Cuando un administrador de red configure y active la retención de datos para su red, todos los mensajes y archivos compartidos en su red se conservarán de acuerdo con las políticas de cumplimiento de la organización. El administrador de la red puede acceder a los archivos .txt generados en una ubicación externa (por ejemplo, en almacenamiento local, bucket de Amazon S3 o cualquier otro almacenamiento que elija el usuario); desde allí, se pueden analizar, borrar o transferir.

**Note**

Wickr no accede nunca a sus mensajes y archivos. Por lo tanto, es su responsabilidad configurar un sistema de retención de datos.

**Temas**

- [Cómo consultar la información sobre la retención de datos](#)
- [Cómo configurar la retención de datos](#)
- [Cómo obtener los registros de retención de datos](#)
- [Métricas y eventos de retención de datos](#)

## Cómo consultar la información sobre la retención de datos

Siga el procedimiento indicado a continuación para consultar la información relativa a la retención de datos de su red de Wickr. También puede habilitar o deshabilitar la retención de datos para su red de Wickr.

1. Abra el formulario AWS Management Console para Wickr en <https://console.aws.amazon.com/wickr/>.
2. Elija Administrar red.
3. En el panel de navegación de la consola de administración de Wickr, seleccione Configuración de red y, a continuación, Retención de datos.

La página Retención de datos indica los pasos que hay que seguir para configurar la retención de datos y la opción de activar o desactivar la característica de retención de datos. Para más información sobre cómo configurar la retención de datos, consulte [Cómo configurar la retención de datos](#).

**Note**

Cuando la retención de datos esté activada, se mostrará el mensaje Retención de datos activada a todos los usuarios de la red, notificándoles que la red se ha habilitado para la retención de datos.

## Cómo configurar la retención de datos

Para configurar la retención de datos para su red de AWS Wickr, debe implementar la imagen de Docker del bot de retención de datos en un contenedor de un host, como un ordenador local o una instancia de Amazon Elastic Compute Cloud (Amazon EC2). Una vez que se ha implementado el bot, puede configurarlo para que almacene datos de forma local o en un bucket de Amazon Simple Storage Service (Amazon S3). También puedes configurar el bot de retención de datos para que utilice otros AWS servicios como AWS Secrets Manager (Secrets Manager), Amazon CloudWatch (CloudWatch), Amazon Simple Notification Service (Amazon SNS) y (). AWS Key Management Service AWS KMS Los siguientes temas describen cómo configurar y ejecutar el bot de retención de datos para su red Wickr.

### Temas

- [Requisitos previos para configurar la retención de datos](#)
- [Password](#)
- [Opciones de almacenamiento](#)
- [Variables de entorno](#)
- [Valores de Secrets Manager](#)
- [Política de IAM para utilizar la retención de datos con los servicios de AWS](#)
- [Cómo iniciar el bot de retención de datos](#)
- [Cómo detener el bot de retención de datos](#)

### Requisitos previos para configurar la retención de datos

Antes de empezar, debe obtener el nombre del bot de retención de datos (denominado Nombre de usuario) y la contraseña inicial de la AWS Management Console para Wickr. Debe especificar estos dos valores la primera vez que inicie el bot de retención de datos. También debe habilitar la retención de datos en la consola. Para obtener más información, consulte [Cómo consultar la información sobre la retención de datos](#).

### Password

La primera vez que inicie el bot de retención de datos, especifique la contraseña inicial mediante una de las siguientes opciones:

- La variable de entorno WICKRIO\_BOT\_PASSWORD. Las variables de entorno del bot de retención de datos se describen en la sección [Variables de entorno](#) que aparece más adelante en esta guía.
- El valor de la contraseña de Secrets Manager identificada por la variable de entorno AWS\_SECRET\_NAME. Los valores de Secrets Manager para el bot de retención de datos se describen en la sección [Valores de Secrets Manager](#) que aparece más adelante en esta guía.
- Introduzca la contraseña cuando el bot de retención de datos se lo pida. Deberá ejecutar el bot de retención de datos con acceso TTY interactivo mediante la opción `-ti`.

Cuando configure el bot de retención de datos por primera vez, se generará una nueva contraseña. Si necesita volver a instalar el bot de retención de datos, use la contraseña generada. La contraseña inicial no es válida después de la instalación inicial del bot de retención de datos.

La nueva contraseña generada se mostrará como se indica en el siguiente ejemplo.

#### Important

Guarde la contraseña en un lugar seguro. Si pierde la contraseña, no podrá volver a instalar el bot de retención de datos. No comparta esta contraseña. Ofrece la posibilidad de iniciar la retención de datos para su red Wickr.

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

## Opciones de almacenamiento

Una vez que la retención de datos esté habilitada y el bot de retención de datos esté configurado para su red Wickr, capturará todos los mensajes y archivos enviados dentro de su red. Los mensajes se guardan en archivos que están limitados a un tamaño o límite de tiempo específicos que se pueden configurar mediante una variable de entorno. Para obtener más información, consulte [Variables de entorno](#).

Puede configurar una de las opciones siguientes para almacenar estos datos:

- Almacene todos los mensajes y archivos capturados de forma local. Esta es la opción predeterminada. Es responsabilidad suya desplazar los archivos locales a otro sistema para almacenarlos a largo plazo y asegurarse de que el disco host no se quede sin memoria ni espacio.
- Almacene todos los mensajes y archivos capturados en un bucket de Amazon S3. El bot de retención de datos guardará todos los mensajes y archivos descifrados en el bucket de Amazon S3 que especifique. Los mensajes y archivos capturados se eliminan de la máquina host una vez guardados correctamente en el bucket.
- Almacene todos los mensajes capturados y archivos cifrados en un bucket de Amazon S3. El bot de retención de datos volverá a cifrar todos los mensajes y archivos capturados con una clave que usted proporcione, y los guardará en el bucket de Amazon S3 que especifique. Los mensajes y archivos capturados se eliminan de la máquina host una vez cifrados de nuevo y guardados correctamente en el bucket. Necesitará un software para descifrar los mensajes y archivos.

Para obtener más información acerca de la creación de un bucket para usar su bot de retención de datos de Amazon S3, consulte la sección [Creación de un bucket](#) en la Guía del usuario de Amazon S3

## Variables de entorno

Puede usar las siguientes variables de entorno para configurar el bot de retención de datos. Estas variables de entorno se configuran mediante la opción `-e` cuando se ejecuta la imagen de Docker del bot de retención de datos. Para obtener más información, consulte [Cómo iniciar el bot de retención de datos](#).

### Note

Estas variables de entorno son opcionales a menos que se especifique lo contrario.

Use las siguientes variables de entorno para especificar las credenciales del bot de retención de datos:

- `WICKRIO_BOT_NAME`: el nombre del bot de retención de datos. Esta variable es obligatoria cuando se ejecuta la imagen de Docker del bot de retención de datos.
- `WICKRIO_BOT_PASSWORD`: la contraseña inicial del bot de retención de datos. Para obtener más información, consulte [Requisitos previos para configurar la retención de datos](#). Esta variable es

obligatoria si no planea iniciar el bot de retención de datos con una solicitud de contraseña o si no planea usar Secrets Manager para almacenar las credenciales del bot de retención de datos.

Use las siguientes variables de entorno para configurar las capacidades de transmisión de retención de datos predeterminadas:

- `WICKRIO_COMP_MSGDEST`: el nombre de la ruta al directorio donde se transmitirán los mensajes. El valor predeterminado es `/tmp/<botname>/compliance/messages`.
- `WICKRIO_COMP_FILEDEST`: el nombre de la ruta al directorio donde se transmitirán los archivos. El valor predeterminado es `/tmp/<botname>/compliance/attachments`.
- `WICKRIO_COMP_BASENAME`: el nombre base de los archivos de mensajes recibidos. El valor predeterminado es `receivedMessages`.
- `WICKRIO_COMP_FILESIZE`: el tamaño de archivo máximo de un archivo de mensajes recibidos en kibibyte (KiB). Se inicia un nuevo archivo cuando se alcanza el tamaño máximo. El valor predeterminado es `1000000000`, como en 1024 GiB.
- `WICKRIO_COMP_TIMEROTATE`: el tiempo, en minutos, durante el que el bot de retención de datos colocará los mensajes recibidos en un archivo de mensajes recibidos. Se inicia un nuevo archivo cuando se alcanza el tiempo límite. Solo puede usar el tamaño o el tiempo del archivo para limitar el tamaño del archivo de mensajes recibidos. El valor predeterminado es `0`, como sin límite.

Use la variable de entorno siguiente para definir el valor de Región de AWS por defecto que se va a usar.

- `AWS_DEFAULT_REGION`: la opción predeterminada Región de AWS que se va a usar para servicios AWS como Secrets Manager (no se usa para Amazon S3 ni AWS KMS). Se usa de forma predeterminada la región `us-east-1` si esta variable de entorno no está definida.

Use las siguientes variables de entorno para especificar el secreto de Secrets Manager que se utilizará cuando opte por utilizar Secrets Manager a fin de almacenar las credenciales del bot de retención de datos y la información de servicio de AWS. Para obtener más información sobre los valores que puede almacenar en Secrets Manager, consulte [Valores de Secrets Manager](#).

- `AWS_SECRET_NAME`: el nombre del secreto de Secrets Manager que contiene las credenciales y la información de servicio de AWS que necesita el bot de retención de datos.

- **AWS\_SECRET\_REGION**: el Región de AWS en que se encuentra el secreto de AWS. Si está usando secretos de AWS y este valor no está definido, se usará el valor de **AWS\_DEFAULT\_REGION**.

 Note

Puede almacenar todas las siguientes variables de entorno como valores en Secrets Manager. Si opta por usar Secrets Manager y almacena estos valores allí, no necesitará especificarlos como variables de entorno cuando ejecute la imagen de Docker del bot de retención de datos. Solo tiene que especificar la variable de entorno de **AWS\_SECRET\_NAME** descrita anteriormente en esta guía. Para obtener más información, consulte [Valores de Secrets Manager](#).

Use las siguientes variables de entorno para especificar el bucket de Amazon S3 cuando opte por almacenar mensajes y archivos en un bucket.

- **WICKRIO\_S3\_BUCKET\_NAME**: el nombre del bucket de Amazon S3 donde se almacenarán los mensajes y archivos.
- **WICKRIO\_S3\_REGION**: la región AWS del bucket de Amazon S3 donde se almacenarán los mensajes y archivos.
- **WICKRIO\_S3\_FOLDER\_NAME**: el nombre de carpeta opcional en el bucket de Amazon S3 donde se almacenarán los mensajes y archivos. El nombre de esta carpeta irá precedido de la clave de los mensajes y archivos guardados en el bucket de Amazon S3.

Use las siguientes variables de entorno para especificar los detalles de AWS KMS cuando opte por utilizar el cifrado del cliente para volver a cifrar los archivos al guardarlos en un bucket de Amazon S3.

- **WICKRIO\_KMS\_MSTRKEY\_ARN**: el nombre de recurso de Amazon (ARN) de la clave maestra de AWS KMS utilizada para volver a cifrar los archivos de mensajes y los archivos del bot de retención de datos antes de guardarlos en el bucket de Amazon S3.
- **WICKRIO\_KMS\_REGION**: la región AWS en la que se encuentra la clave maestra de AWS KMS.

Utilice la siguiente variable de entorno para especificar los detalles de Amazon SNS cuando opte por enviar eventos de retención de datos a un tema de Amazon SNS. Los eventos enviados incluyen el inicio, el cierre y las condiciones de error.

- `WICKRIO_SNS_TOPIC_ARN`: el ARN del tema de Amazon SNS al que desea que se envíen los eventos de retención de datos.

Utilice la siguiente variable de entorno para enviar las métricas de retención de datos a CloudWatch. Si se especifica, las métricas se generarán cada 60 segundos.

- `WICKRIO_METRICS_TYPE`— Defina el valor de esta variable de entorno en `cloudwatch` el que enviar las métricas CloudWatch.

## Valores de Secrets Manager

Puede usar Secrets Manager para almacenar las credenciales del bot de retención de datos y la información del servicio de AWS. Para obtener más información acerca de los permisos mínimos, consulte [Creación de un secreto AWS Secrets Manager](#) en la Guía del usuario de Secrets Manager.

El secreto de Secrets Manager puede tener los siguientes valores:

- `password`: la contraseña del bot de retención de datos.
- `s3_bucket_name`: el nombre del bucket de Amazon S3 donde se almacenarán los mensajes y archivos. Si no se establece, se utilizará la transmisión de archivos predeterminada.
- `s3_region`: la región AWS del bucket de Amazon S3 donde se almacenarán los mensajes y archivos.
- `s3_folder_name`: el nombre de carpeta opcional en el bucket de Amazon S3 donde se almacenarán los mensajes y archivos. El nombre de esta carpeta irá precedido de la clave de los mensajes y archivos guardados en el bucket de Amazon S3.
- `kms_master_key_arn`: el ARN de la clave maestra de AWS KMS utilizada para volver a cifrar los archivos de mensajes y los archivos del bot de retención de datos antes de guardarlos en el bucket de Amazon S3.
- `kms_region`: la región AWS en la que se encuentra la clave maestra de AWS KMS.
- `sns_topic_arn`: el ARN del tema de Amazon SNS al que desea que se envíen los eventos de retención de datos.

## Política de IAM para utilizar la retención de datos con los servicios de AWS

Si planea utilizar otros servicios de AWS con el bot de retención de datos de Wickr, debe asegurarse de que el anfitrión tenga el rol (IAM) y la política adecuadas de AWS Identity and Access Management para acceder a ellos. Puede configurar el bot de retención de datos para que utilice Secrets Manager, Amazon S3 CloudWatch, Amazon SNS y AWS KMS. La siguiente política de IAM permite el acceso a acciones específicas para estos servicios.

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

Puede crear una política de IAM más estricta identificando los objetos específicos de cada servicio a los que quiere permitir el acceso de los contenedores de su host. Elimine las acciones de los servicios de AWS que no tiene intención de utilizar. Por ejemplo, si piensa utilizar solo un bucket de Amazon S3, utilice la siguiente política, que elimina las acciones `secretsmanager:GetSecretValue`, `sns:Publish`, `kms:GenerateDataKey` y `cloudwatch:PutMetricData`.

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

```
    }  
  ]  
}
```

Si utiliza una instancia de Amazon Elastic Compute Cloud (Amazon EC2) para alojar su bot de retención de datos, cree un rol de IAM utilizando el caso común de Amazon EC2 y asigne una política según la definición de política anterior.

## Cómo iniciar el bot de retención de datos

Antes de ejecutar el bot de retención de datos, debe determinar cómo quiere configurarlo. Si planea ejecutar el bot en un host que:

- No va a tener acceso a los servicios de AWS, sus opciones serán limitadas. En ese caso, utilizará las opciones de transmisión de mensajes predeterminadas. Debe decidir si desea limitar el tamaño de los archivos de mensajes capturados a un tamaño o intervalo de tiempo específicos. Para obtener más información, consulte [Variables de entorno](#).
- Va a tener acceso a servicios de AWS, debe crear un secreto de Secrets Manager para almacenar las credenciales del bot y los detalles de configuración del servicio de AWS. Una vez configurados los servicios de AWS, puede iniciar la imagen de Docker del bot de retención de datos. Para obtener más información sobre los detalles que puede almacenar en un secreto de Secrets Manager, consulte [Valores de Secrets Manager](#)

En las siguientes secciones se muestran ejemplos de comandos para ejecutar la imagen de Docker del bot de retención de datos. En cada uno de los comandos de ejemplo, sustituya los siguientes valores de ejemplo por los suyos:

- *compliance\_1234567890\_bot* con el nombre de su bot de retención de datos.
- *password* con la contraseña de su bot de retención de datos.
- *wickr/data/retention/bot* con el nombre de su secreto de Secrets Manager para usarlo con su bot de retención de datos.
- *bucket-name* con el nombre del bucket de Amazon S3 donde se almacenarán los mensajes y archivos.
- *folder-name* con el nombre de carpeta en el bucket de Amazon S3 donde se almacenarán los mensajes y archivos.
- *us-east-1* con la región AWS del recurso que está especificando. Por ejemplo, la región de la clave maestra de AWS KMS o la región del bucket de Amazon S3.

- *arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-a617-abababababab* con el nombre de recurso de Amazon (ARN) de la clave maestra de su AWS KMS para volver a cifrar ficheros y archivos de mensajes.

### Cómo iniciar el bot con la variable de entorno de contraseña (sin servicio de AWS)

El siguiente comando de Docker inicia el bot de retención de datos. La contraseña se especifica mediante la variable de entorno de WICKRIO\_BOT\_PASSWORD. El bot comienza a usar la transmisión de archivos predeterminada y a usar los valores predeterminados definidos en la sección [Variables de entorno](#) de esta guía.

```
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
```

### Cómo iniciar el bot con una solicitud de contraseña (sin servicio de AWS)

El siguiente comando de Docker inicia el bot de retención de datos. La contraseña se introduce cuando el bot de retención de datos se lo pida. Comenzará a usar la transmisión de archivos predeterminada mediante los valores predeterminados definidos en la sección [Variables de entorno](#) de esta guía.

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

Ejecute el bot utilizando la opción `-ti` para recibir la solicitud de contraseña. También debe ejecutar el comando `docker attach <container ID or container name>` inmediatamente después de iniciar la imagen de docker para que aparezca la solicitud de contraseña. Debe ejecutar ambos

comandos en un script. Si lo adjunta a la imagen de docker y no ve el mensaje, presione Intro y verá el mensaje.

Cómo iniciar el bot con una rotación del archivo de mensajes de 15 minutos (sin servicio de AWS)

El siguiente comando de Docker inicia el bot de retención de datos mediante variables de entorno. También lo configura para rotar los archivos de mensajes recibidos a 15 minutos.

```
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
```

Cómo iniciar el bot y especificar la contraseña inicial con Secrets Manager

Puede utilizar Secrets Manager para identificar la contraseña del bot de retención de datos. Cuando inicie el bot de retención de datos, necesitará configurar una variable de entorno que especifique al Secrets Manager donde se almacena esta información.

```
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
```

El secreto de wickrpro/compliance/compliance\_1234567890\_bot tiene el siguiente valor secreto, que se muestra como texto sin formato.

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

Cómo iniciar el bot y configurar Amazon S3 con Secrets Manager

Puede usar Secrets Manager para alojar las credenciales y la información del bucket de Amazon S3. Cuando inicie el bot de retención de datos, necesitará configurar una variable de entorno que especifique al Secrets Manager donde se almacena esta información.

```
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
```

El secreto de `wickrpro/compliance/compliance_1234567890_bot` tiene el siguiente valor secreto, que se muestra como texto sin formato.

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

Los mensajes y archivos que reciba el bot se colocarán en el bucket de `bot-compliance` de la carpeta denominada `network1234567890`.

### Cómo iniciar el bot y configurar Amazon S3 y AWS KMS con Secrets Manager

Puede usar Secrets Manager para alojar las credenciales, el bucket de Amazon S3 y la información de la clave maestra de AWS KMS. Cuando inicie el bot de retención de datos, necesitará configurar una variable de entorno que especifique al Secrets Manager donde se almacena esta información.

```
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
```

El secreto de `wickrpro/compliance/compliance_1234567890_bot` tiene el siguiente valor secreto, que se muestra como texto sin formato.

```
{
  "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"
}
```

```
}
```

Los mensajes y archivos recibidos por el bot se cifrarán con la clave KMS identificada por el valor del ARN y, a continuación, se colocarán en el bucket de “conformidad del bot” de la carpeta denominada “network1234567890”. Asegúrese de que tiene la configuración de la política de IAM adecuada.

### Cómo iniciar el bot y configurar Amazon S3 mediante variables de entorno

Si no quiere usar Secrets Manager para alojar las credenciales del bot de retención de datos, puede iniciar la imagen de Docker del bot de retención de datos con las siguientes variables de entorno. Debe identificar el nombre del bot de retención de datos mediante la variable de entorno de 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
```

Puede usar los valores del entorno para identificar las credenciales del bot de retención de datos, la información sobre los buckets de Amazon S3 y la información de configuración para la transmisión de archivos predeterminada.

### Cómo detener el bot de retención de datos

El software que se ejecuta en el robot de retención de datos capturará las señales de SIGTERM y se apagará sin problemas. Utilice el comando `docker stop <container ID or container name>`, como se muestra en el siguiente ejemplo, para enviar el comando SIGTERM a la imagen de Docker del bot de retención de datos.

```
docker stop compliance_1234567890_bot
```

### Cómo obtener los registros de retención de datos

El software que se ejecuta en la imagen de Docker del bot de retención de datos enviará sus resultados a los archivos de registro del directorio `/tmp/<botname>/logs`. Se rotará hasta 5 archivos como máximo. Ejecute el comando siguiente para obtener los registros.

```
docker logs <botname>
```

Ejemplo:

```
docker logs compliance_1234567890_bot
```

## Métricas y eventos de retención de datos

A continuación se muestran las métricas de Amazon CloudWatch (CloudWatch) y los eventos del Amazon Simple Notification Service (Amazon SNS) que actualmente admite la versión 5.116 del bot de retención de datos Wickr de AWS.

Temas

- [CloudWatch métricas](#)
- [Eventos de Amazon SNS](#)

### CloudWatch métricas

El bot genera las métricas en intervalos de 1 minuto y las transmite al CloudWatch servicio asociado a la cuenta en la que se ejecuta la imagen de Docker del bot de retención de datos.

A continuación se muestran las métricas existentes que son compatibles con el bot de retención de datos.

Métrica	Descripción
Messages_Rx	Mensajes recibidos
Messages_Rx_Failed	Errores al procesar los mensajes recibidos.
Messages_Saved	Mensajes guardados en el archivo de mensajes recibidos.
Messages_Saved_Failed	Errores al guardar los mensajes en el archivo de mensajes recibidos.
Files_Saved	Archivos recibidos.

Métrica	Descripción
Files_Saved_Bytes	Número de bytes de los archivos recibidos.
Files_Saved_Failed	Errores al guardar los archivos.
Inicios de sesión	Inicios de sesión (normalmente 1 por intervalo).
Login_Failures	Errores al iniciar sesión (normalmente 1 por intervalo).
S3_Post_Errors	Errores al publicar archivos de mensajes y archivos del bucket de Amazon S3.
Watchdog_Failures	Errores de watchdog.
Watchdog_Warnings	Advertencias de watchdog

Las métricas se generan para que las consuma. CloudWatch El espacio de nombre utilizado para los bots es `WickrIO`. Cada métrica tiene una matriz de dimensiones. La lista siguiente recoge las dimensiones que se publican con las métricas anteriores.

Dimensión	Valor
Id	El nombre de usuario del bot.
Dispositivo	Descripción de una instancia o un dispositivo específico del bot. Es útil si se ejecutan varios dispositivos o instancias de bots.
Producto	El producto para el bot. Puede ser <code>WickrPro_</code> o <code>WickrEnterprise_</code> con <code>Alpha</code> , <code>Beta</code> o <code>Production</code> anexado.
BotType	El tipo de bot. Etiquetado como <code>Conformidad</code> para los bots de conformidad.
Network	El ID de la red asociada.

## Eventos de Amazon SNS

Los eventos siguientes se publican en el tema de Amazon SNS definido por el valor del nombre de recurso de Amazon (ARN) identificado mediante la variable de entorno `WICKRIO_SNS_TOPIC_ARN` o el valor secreto de Secrets Manager `sns_topic_arn`. Para obtener más información, consulte [Variables de entorno](#) y [Valores de Secrets Manager](#).

Los eventos generados por el bot de retención de datos se envían como cadenas JSON. En los eventos se incluyen los valores siguientes a partir de la versión 5.116 del bot de retención de datos.

Nombre	Valor
<code>complianceBot</code>	El nombre de usuario del bot de retención de datos.
<code>dateTime</code>	La fecha y hora en que se produjo el evento.
<code>device</code>	La descripción del dispositivo o instancia del bot específico. Es útil si se ejecutan varias instancias de bot.
<code>dockerImage</code>	La imagen de Docker asociada al bot.
<code>dockerTag</code>	La etiqueta o versión de la imagen de Docker.
<code>message</code>	El mensaje del evento. Para obtener más información, consulte <a href="#">Eventos críticos</a> y <a href="#">Eventos normales</a> .
<code>notificationType</code>	Este valor será <code>Bot Event</code> .
<code>severity</code>	La gravedad del evento. Puede ser <code>normal</code> o <code>critical</code> .

Debe suscribirse al tema de Amazon SNS para poder recibir los eventos. Si se suscribe con una dirección de correo electrónico, se le enviará un correo electrónico con información similar a la del ejemplo siguiente.

```
{
```

```

"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"
}

```

## Eventos críticos

Estos eventos hacen que el bot se detenga o se reinicie. Para evitar otros problemas, el número de reinicios es limitado.

## Errores de inicio de sesión

Los eventos siguientes se pueden generar cuando el bot no consigue iniciar sesión. En cada mensaje se indica el motivo del error de inicio de sesión.

Tipo de evento	Mensaje de evento
failedlogin	Credenciales incorrectas. Compruebe la contraseña.
failedlogin	Usuario no encontrado
failedlogin	La cuenta o el dispositivo están suspendidos.
provisioning	El usuario abandonó el comando.
provisioning	La contraseña del archivo <code>config.wickr</code> es incorrecta.
provisioning	No se puede leer el archivo <code>config.wickr</code> .
failedlogin	Error en todos los inicios de sesión.
failedlogin	Nuevo usuario en una base de datos que ya existe.

## Más eventos críticos

Tipo de evento	Mensajes de los eventos
Cuenta suspendida	WickRioClientMain: slotAdminUser Suspende: código (%1): motivo: %2»
BotDevice Suspendido	El dispositivo está suspendido.
WatchDog	El SwitchBoard sistema ha estado inactivo durante más de < N > minutos
Errores de S3	No se pudo colocar el archivo <file-name >> en el bucket de S3. Error: <AWS-error >
Clave Fallback (alternativa)	EL SERVIDOR ENVIÓ UNA CLAVE FALLBACK (ALTERNATIVA): no es una clave alternativa activa reconocida por el cliente. Envíe los registros al equipo de ingeniería del escritorio.

## Eventos normales

Los eventos siguientes advierten sobre un funcionamiento normal. No obstante, puede ser motivo de preocupación si se producen demasiados eventos de este tipo en un período de tiempo determinado.

### Dispositivo agregado a la cuenta

Este evento se genera cuando se agrega un nuevo dispositivo a la cuenta del bot de retención de datos. En determinadas circunstancias, esto puede ser un indicio importante de que se ha creado una instancia del bot de retención de datos. El mensaje siguiente corresponde a este evento:

A device has been added to this account!

### El bot ha iniciado sesión

Este evento se genera cuando el bot ha iniciado sesión correctamente. El mensaje siguiente corresponde a este evento:

Logged in

## Cerrando

Este evento se genera cuando el bot se cierra. Si el usuario no lo inició de forma explícita, puede indicar que ha habido un problema. El mensaje siguiente corresponde a este evento:

```
Shutting down
```

## Actualizaciones disponibles

Este evento se genera cuando se inicia el bot de retención de datos e identifica que hay disponible una versión más reciente de la imagen de Docker asociada. Este evento se genera cuando se inicia el bot y diariamente. Este evento incluye el campo de la matriz `versions` que identifica las nuevas versiones disponibles. Consulte el ejemplo de este evento a continuación.

```
{
  "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"
  ]
}
```

## ¿Qué es ATAK?

El kit Android Team Awareness Kit (ATAK), o Android Tactical Assault Kit (también conocido como ATAK) para uso militar, es una aplicación de infraestructura geoespacial y conciencia situacional para teléfonos inteligentes que permite una colaboración segura a nivel geográfico. Aunque inicialmente se diseñó para su uso en zonas de combate, ATAK se ha adaptado para adaptarse a los objetivos de agencias locales, estatales y federales.

## Temas

- [Cómo habilitar ATAK en el panel de la red de Wickr](#)
- [Información adicional sobre ATAK](#)
- [Cómo instalar y vincular el complemento de Wickr para ATAK](#)
- [Marcar y recibir una llamada](#)
- [Enviar un archivo](#)
- [Enviar un mensaje de voz seguro \(Push-to-talk\)](#)
- [Rueda de opciones \(acceso rápido\)](#)
- [Navegación](#)

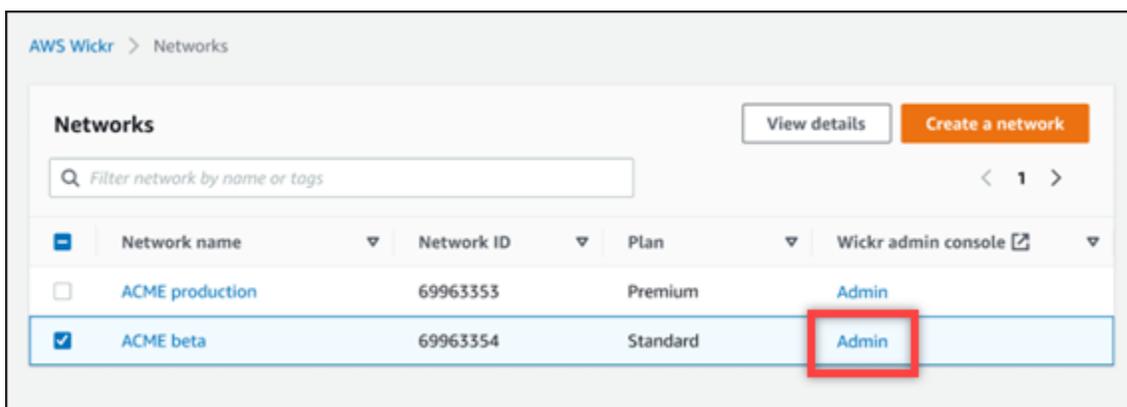
## Cómo habilitar ATAK en el panel de la red de Wickr

AWS Wickr es compatible con muchas agencias que utilizan Android Tactical Assault Kit (ATAK). Sin embargo, hasta ahora, los operadores de ATAK que utilizan Wickr han tenido que salir de la aplicación para poder hacerlo. Para ayudar a reducir las interrupciones y el riesgo operativo, Wickr ha desarrollado un complemento que mejora ATAK con características de comunicación seguras. Con el complemento Wickr para ATAK, los usuarios pueden enviar mensajes, colaborar y transferir archivos en Wickr dentro de la aplicación ATAK. Esto elimina las interrupciones y la complejidad de la configuración con las características de chat de ATAK.

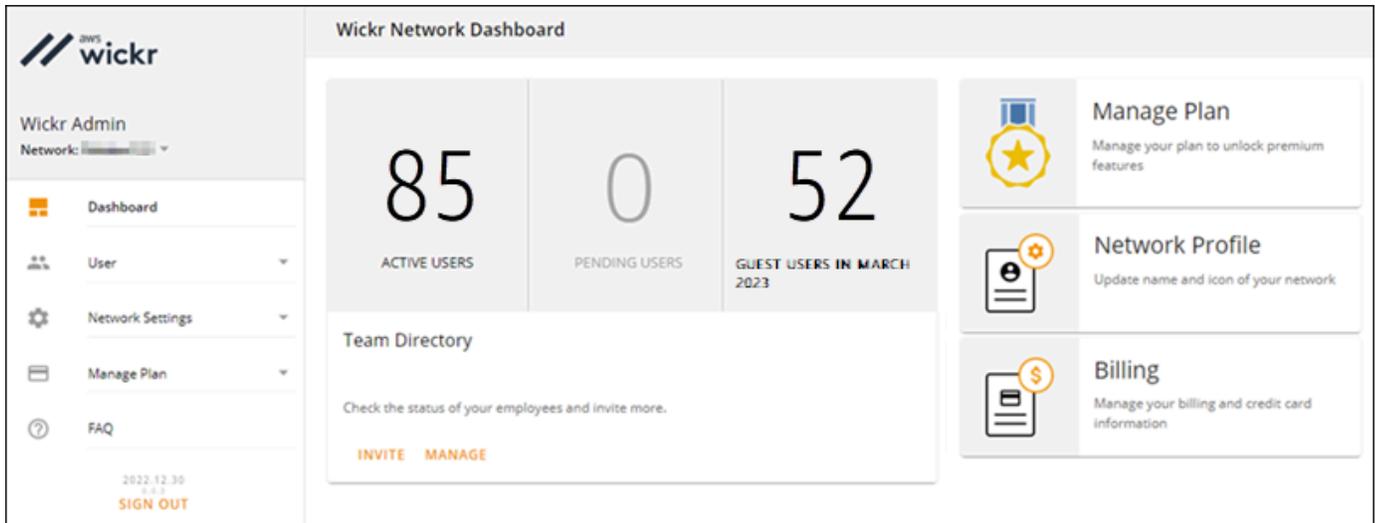
### Cómo habilitar ATAK en el panel de la red de Wickr

Complete el siguiente procedimiento para habilitar ATAK en el panel de la red de Wickr.

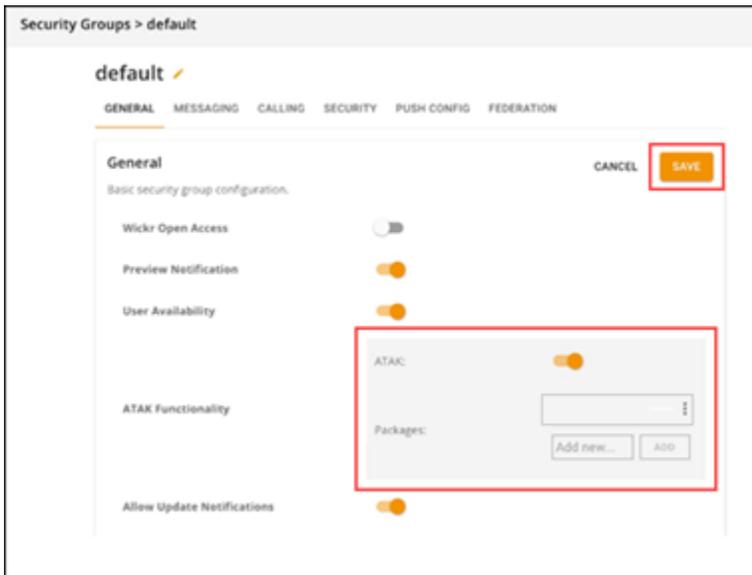
1. Abra la AWS Management Console de Wickr en <https://console.aws.amazon.com/wickr/>.
2. En la página Redes, seleccione el enlace Admin para acceder a la consola de administración de Wickr de dicha red.



Se le redirigirá a la consola de administración de Wickr de una red específica.



3. En el panel de navegación de la consola de administración de Wickr, seleccione Configuración de red y, a continuación, Grupo de seguridad.
4. Elija Detalles junto al grupo de seguridad para el que desea habilitar ATAK.
5. En la pestaña General, seleccione Edit.
6. En la sección Funcionalidad de ATAK:
  - a. Introduzca el nombre del paquete en el cuadro de texto Paquetes. Puede introducir uno de los siguientes valores en función de la versión de ATAK que vayan a instalar y utilizar los usuarios:
    - `com.atakmap.app.civ`: introduzca este valor en el cuadro de texto Paquetes si los usuarios finales de Wickr van a instalar y utilizar la versión civil de la aplicación ATAK en sus dispositivos Android.
    - `com.atakmap.app.mil`: introduzca este valor en el cuadro de texto Paquetes si los usuarios finales de Wickr van a instalar y utilizar la versión militar de la aplicación ATAK en sus dispositivos Android.
  - b. Deslice el botón ATAK hacia la derecha para habilitar la funcionalidad.
  - c. Seleccione Guardar.



Ahora, ATAK está habilitado para la red de Wickr y el grupo de seguridad seleccionados. Debe pedir a los usuarios de Android del grupo de seguridad para el que ha habilitado la funcionalidad de ATAK que instalen el complemento Wickr para ATAK. Para obtener más información, consulte [Instalar y vincular el complemento Wickr para ATAK](#).

## Información adicional sobre ATAK

Para obtener más información sobre el plugin de Wickr para ATA, consulte lo siguiente:

- [Descripción general del complemento Wickr para ATAK](#)
- [Información adicional sobre el complemento Wickr para ATAK](#)

## Cómo instalar y vincular el complemento de Wickr para ATAK

El kit de Android Team Awareness Kit (ATAK) es una solución para Android que utilizan las agencias militares, estatales y gubernamentales de los EE. UU. que requieren capacidades de información situacional para planificar las misiones, ejecutarlas y responder a incidentes. La arquitectura de complementos de ATAK permite a los desarrolladores agregar funcionalidades. Además, los usuarios pueden navegar utilizando datos de mapas geoespaciales y GPS superpuestos con información situacional en tiempo real sobre los eventos en curso. En este documento le mostramos cómo

instalar el complemento de Wickr para ATAK en un dispositivo Android y vincularlo con el cliente Wickr. De este modo podrá enviar mensajes y colaborar en Wickr sin salir de la aplicación ATAK.

## Cómo instalar el complemento de Wickr para ATAK

Siga los pasos que se indican a continuación para instalar el complemento de Wickr para ATAK en un dispositivo Android.

1. Visite la tienda Google Play e instale el complemento de Wickr para ATAK.
2. Abra la aplicación ATAK en su dispositivo Android.
3. En la aplicación ATAK, seleccione el icono de menú  en la parte superior derecha de la pantalla y, a continuación, seleccione Complementos.
4. Seleccione Importar.
5. En la ventana Selección del tipo de importación emergente, elija SD Local y vaya al lugar donde guardó el archivo .apk del complemento Wickr para ATAK.
6. Seleccione el archivo del complemento y siga las instrucciones para instalarlo.

### Note

Si se le pide que envíe el archivo del complemento para escanearlo, seleccione No.

7. La aplicación ATAK le preguntará si desea cargar el complemento. Seleccione OK (Aceptar).

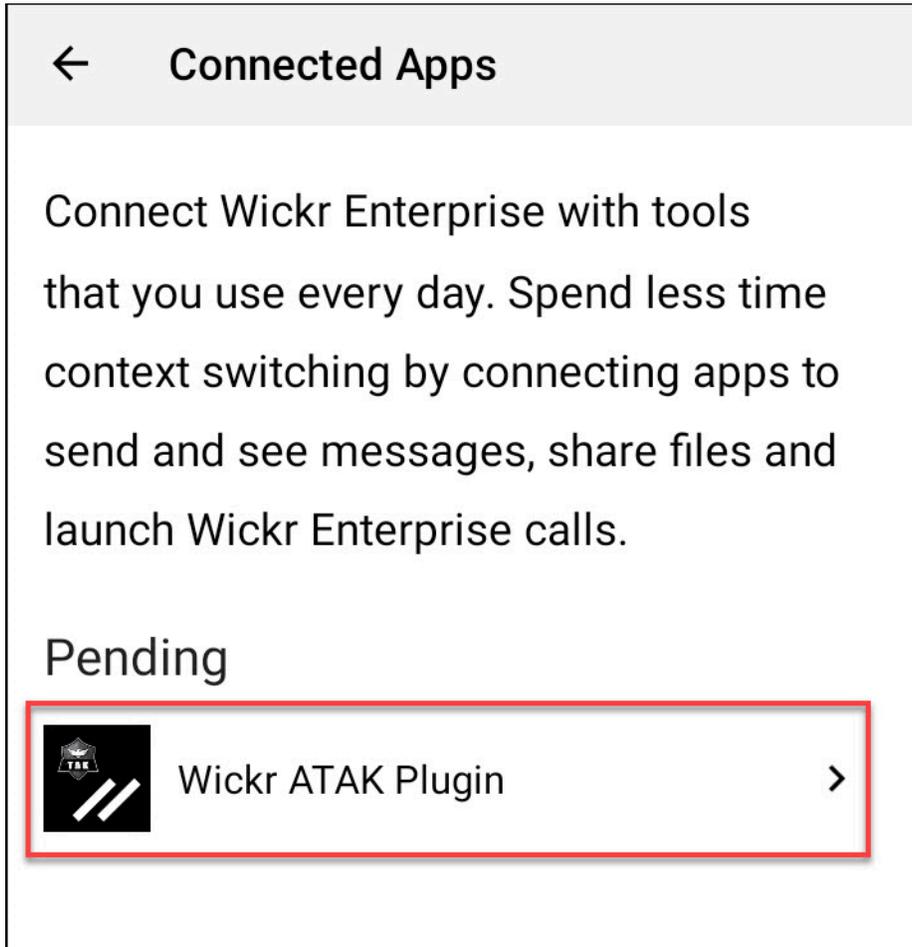
El complemento de Wickr para ATAK ya está instalado. Siga a la sección Emparejar ATAK con Wickr para completar el proceso.

## Cómo vincular ATAK con Wickr

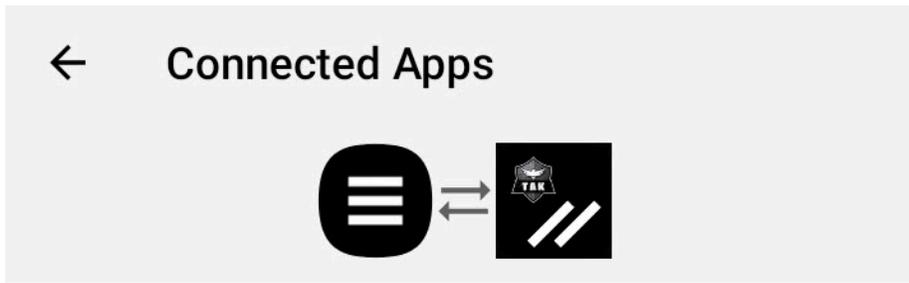
Siga el procedimiento que se indica a continuación para vincular la aplicación ATAK con Wickr una vez instalado correctamente el complemento de Wickr para ATAK.

1. En la aplicación ATAK, seleccione el icono de menú  en la parte superior derecha de la pantalla y, a continuación, Complemento de Wickr.
2. Elija Vincular Wickr.

Aparecerá un mensaje de notificación pidiéndole que revise los permisos del complemento de Wickr para ATAK. En caso contrario, abra el cliente Wickr y vaya a Ajustes y, a continuación, a Aplicaciones conectadas. Debería ver el complemento en la sección Pendiente de la pantalla.



3. Seleccione Aprobar para vincularlo.
4. Selecciona el botón Abrir complemento de Wickr ATAK para volver a la aplicación ATAK.



## Success

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

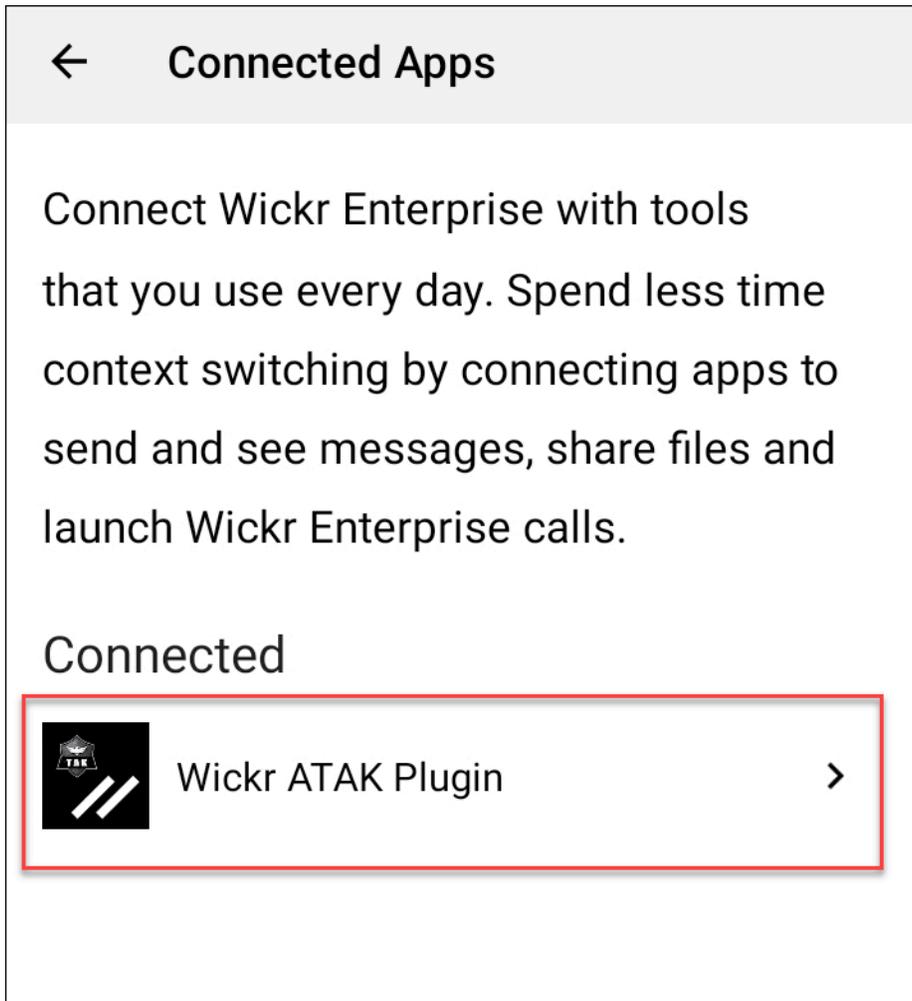


Se ha vinculado correctamente el complemento ATAK y Wickr; ya puede usarlo para enviar mensajes y colaborar con Wickr sin salir de la aplicación ATAK.

## Desvinculación de ATAK de Wickr

Complete el siguiente procedimiento para desvincular el complemento ATAK de Wickr.

1. En la consola, elija Configuración y, a continuación, elija Aplicaciones conectadas.
2. En la pantalla Aplicaciones conectadas, seleccione Complemento Wickr para ATAK.



3. En la pantalla Complemento Wickr para ATAK, seleccione Eliminar en la parte inferior de la pantalla.

Aparece una pantalla de confirmación para indicar que ya no utiliza la API. Ha desvinculado correctamente el complemento ATAK.

## Marcar y recibir una llamada

Puede marcar y recibir una llamada en el complemento Wickr para ATAK.

Complete el siguiente procedimiento para marcar y recibir una llamada.

1. Abra una ventana de chat.
2. En la vista Mapa, seleccione el icono del usuario al que quiere llamar.
3. Elija el icono de teléfono de la parte superior derecha de la pantalla.

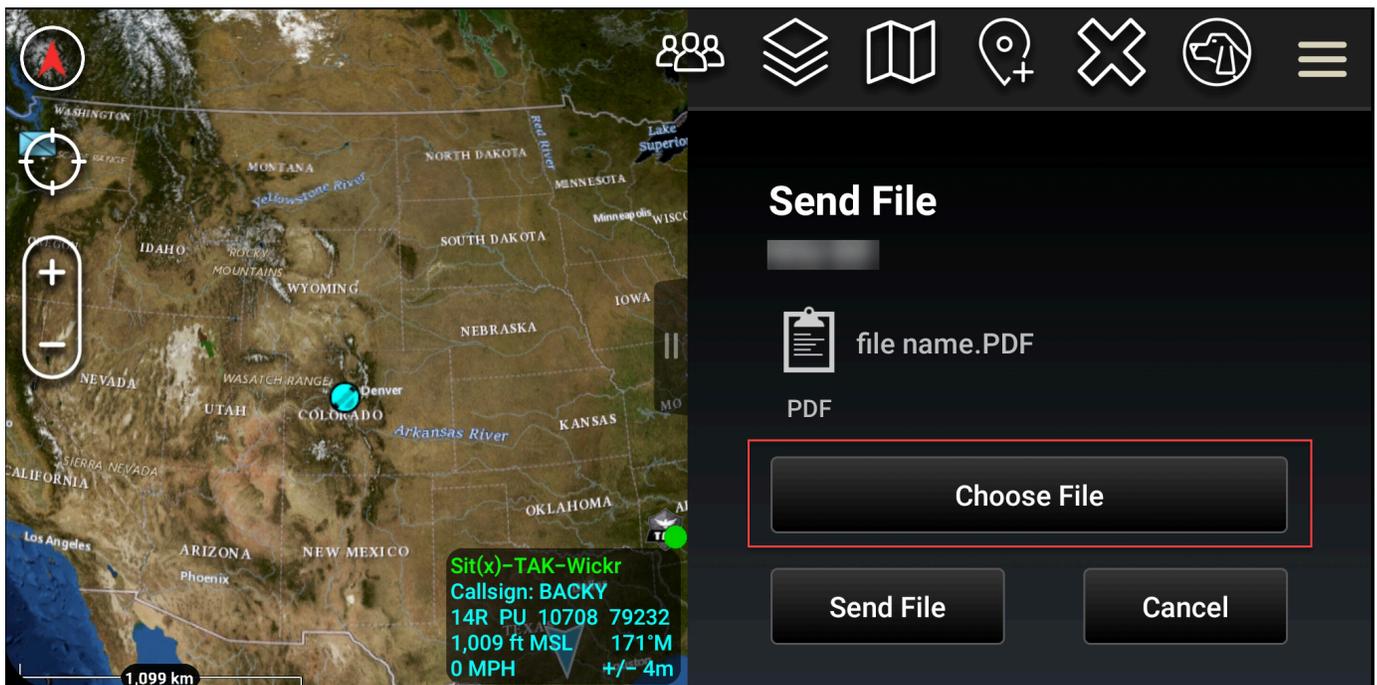
- Una vez conectado, puede volver a la vista del complemento ATAK y recibir una llamada.

## Enviar un archivo

Descubra cómo enviar un archivo en el complemento Wickr para ATAK.

Siga el procedimiento que se indica a continuación para enviar un archivo.

- Abra una ventana de chat.
- En la vista Mapa, busque al usuario al que quiere enviar un archivo.
- Cuando encuentre al usuario al que quiere enviar un archivo, seleccione su nombre.
- En la pantalla Enviar archivo, seleccione Elegir archivo y, a continuación, navegue hasta el archivo que desea enviar.



- En la ventana del navegador, seleccione el archivo deseado.
- En la pantalla Enviar archivo, seleccione Enviar archivo.

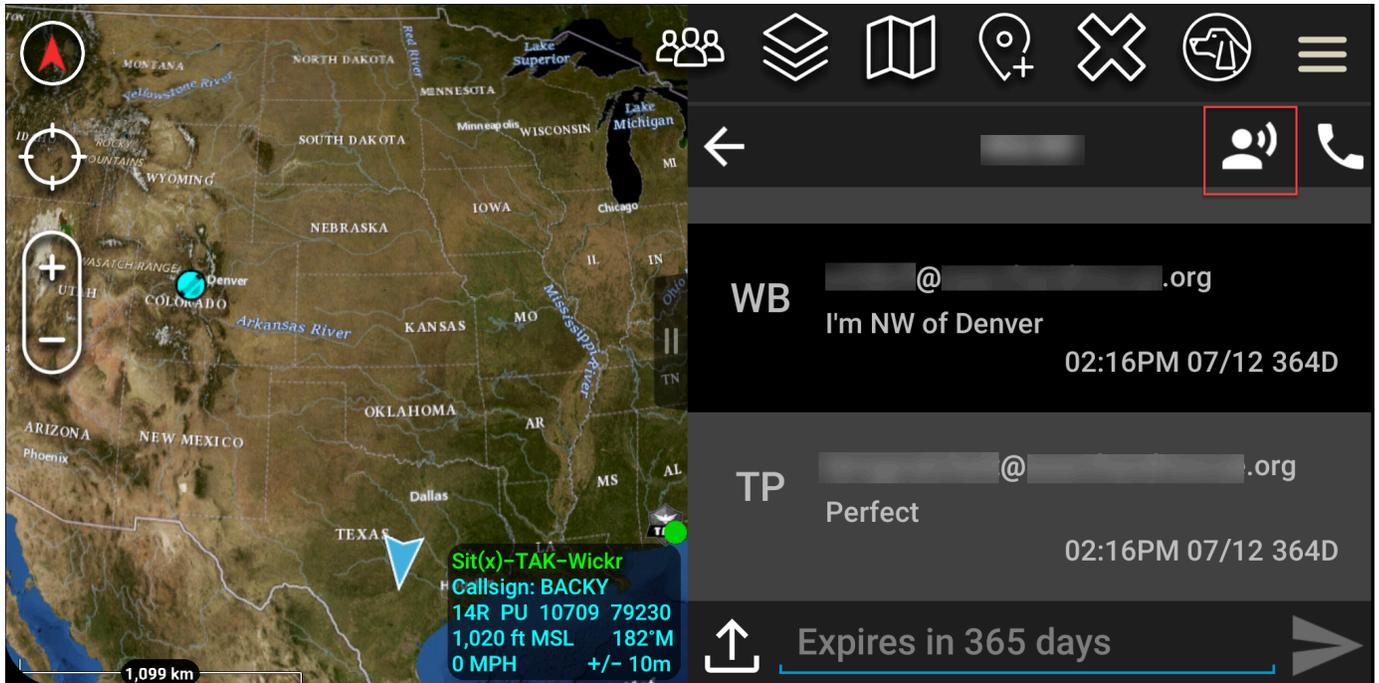
Aparecerá el icono de descarga, que indica que se está descargando el archivo que ha seleccionado.

## Enviar un mensaje de voz seguro (Push-to-talk)

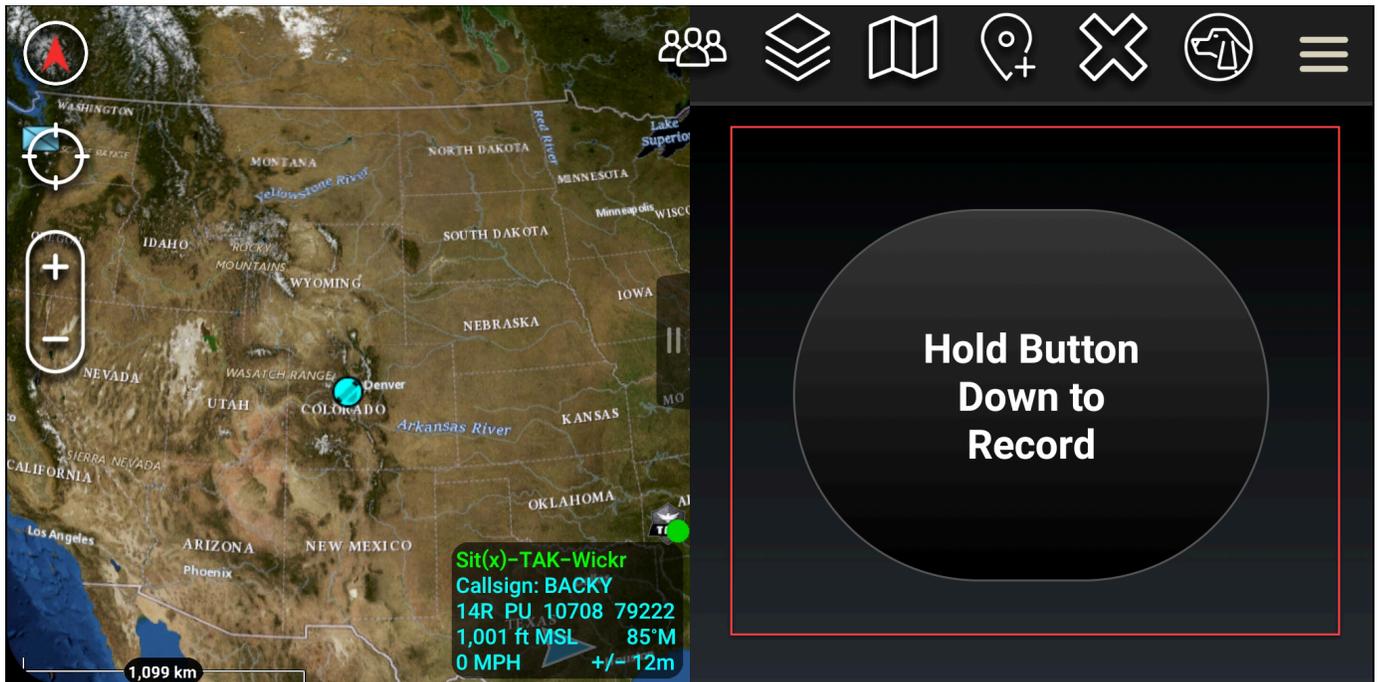
Puedes enviar un mensaje de voz seguro (Push-to-talk) en el complemento Wickr para ATAK.

Complete el siguiente procedimiento para enviar un mensaje de voz de seguro.

1. Abra una ventana de chat.
2. Selecciona el icono de pulsar para hablar en la parte superior de la pantalla, indicado por el icono de una persona hablando.



3. Seleccione y mantenga presionado el botón Presione el botón para grabar.



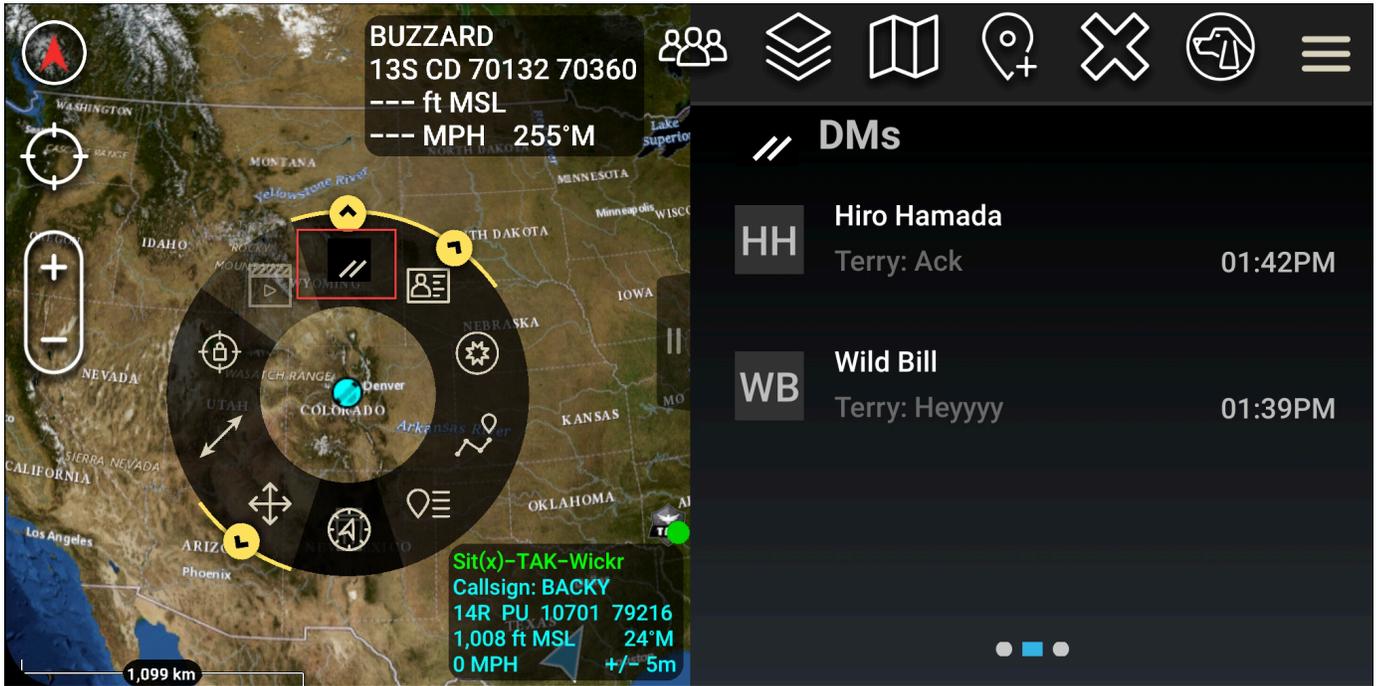
4. Grabe su mensaje.
5. Después de grabar el mensaje, suelte el botón para enviarlo.

## Rueda de opciones (acceso rápido)

La función de molinete o de acceso rápido se utiliza para one-one-one conversaciones o mensajes directos.

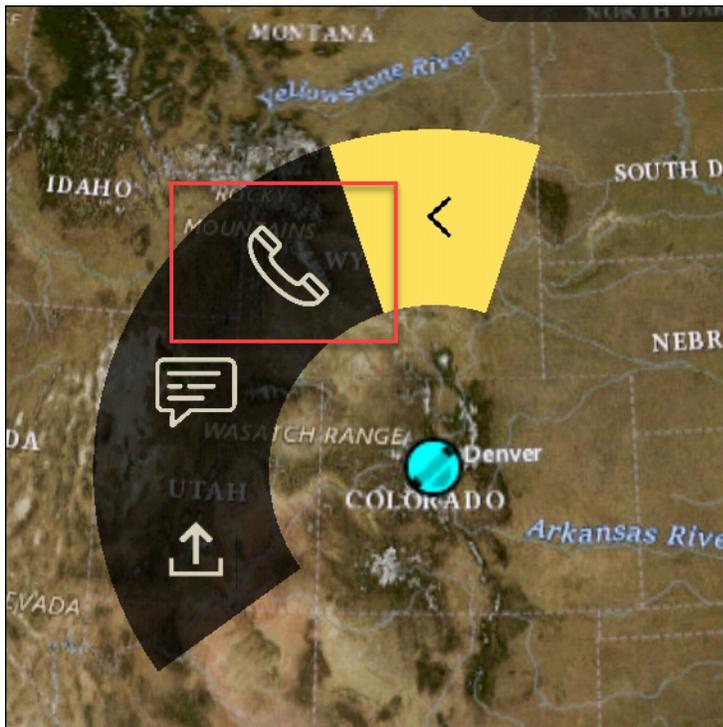
Complete el siguiente procedimiento para usar la rueda de opciones.

1. Abra la vista en pantalla dividida del mapa de ATAK y del complemento Wickr para ATAK de forma simultánea. El mapa muestra a sus compañeros de equipo o los activos en la vista de mapa.
2. Seleccione el icono de usuario para abrir la rueda de opciones.
3. Seleccione el icono de Wickr para ver las opciones disponibles para el usuario seleccionado.



4. En la rueda de opciones, elija uno de los siguientes iconos:

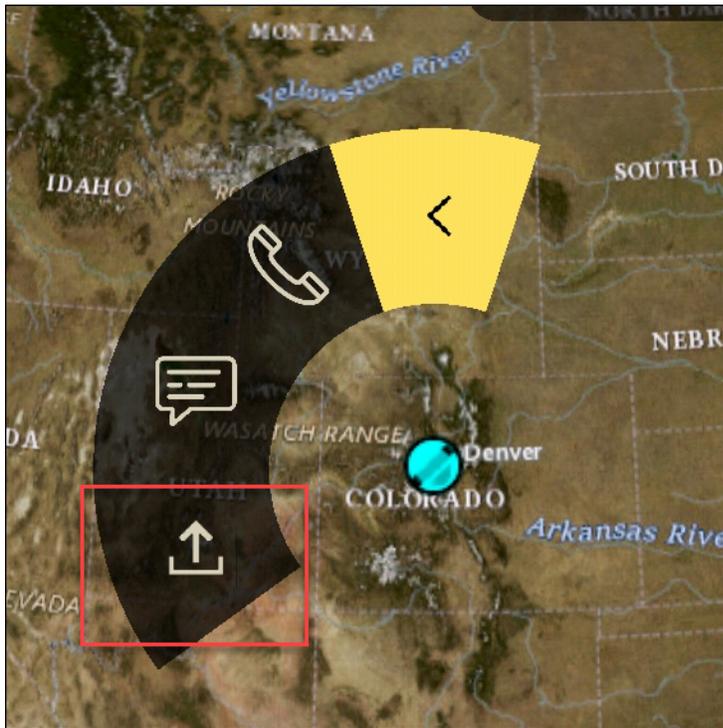
- Teléfono: elija llamar.



- Mensaje: elija participar en un chat.



- Envío de archivos: elija enviar un archivo.



## Navegación

La interfaz de usuario del complemento contiene tres vistas del complemento que se indican mediante las figuras azules y blancas situadas en la parte inferior derecha de la pantalla. Deslice el dedo hacia la izquierda y hacia la derecha para navegar entre las vistas.

- Vista de contactos: cree un grupo de mensajes directos o una conversación de sala.
- Vista de mensajes directos: crea una one-to-one conversación. La funcionalidad de chat funciona igual que en la aplicación nativa de Wickr. Esta funcionalidad le permite permanecer en la vista de mapa y comunicarse con otras personas a través del complemento.
- Vista de salas: las salas existentes en la aplicación nativa se transfieren. Todo lo que se haga en el complemento se reflejará en la aplicación nativa de Wickr.

### Note

Algunas funciones, como la eliminación de una sala, solo se pueden realizar en la aplicación nativa y de forma presencial para evitar modificaciones no deseadas por parte de los usuarios y las interferencias causadas por el equipo de campo.

## Lista de puertos y dominios que deben ser permitidos

Lista de los puertos y dominios permitidos para asegurar que Wickr funcione correctamente:

### Puertos

- Puerto TCP 443 (para mensajes y archivos adjuntos)
- Puertos UDP 16384-16584 (para llamadas)

### Dominios regionales

- Europa (Fráncfort): `api.messaging.wickr.eu-central-1.amazonaws.com`
- EE. UU. Este (Virginia del Norte): `gw-pro-prod .wickr.com`, `api.messaging.wickr.us-east-1.amazonaws.com`
- Europa (Londres): `api.messaging.wickr.eu-west-2.amazonaws.com`
- Asia-Pacífico (Sídney): `api.messaging.wickr.ap-southeast-2.amazonaws.com`

- Canadá (Central): `api.messaging.wickr.ca-central-1.amazonaws.com`
- AWS GovCloud (EEUU-Oeste): `api.messaging.wickr.us-gov-west-1.amazonaws.com`

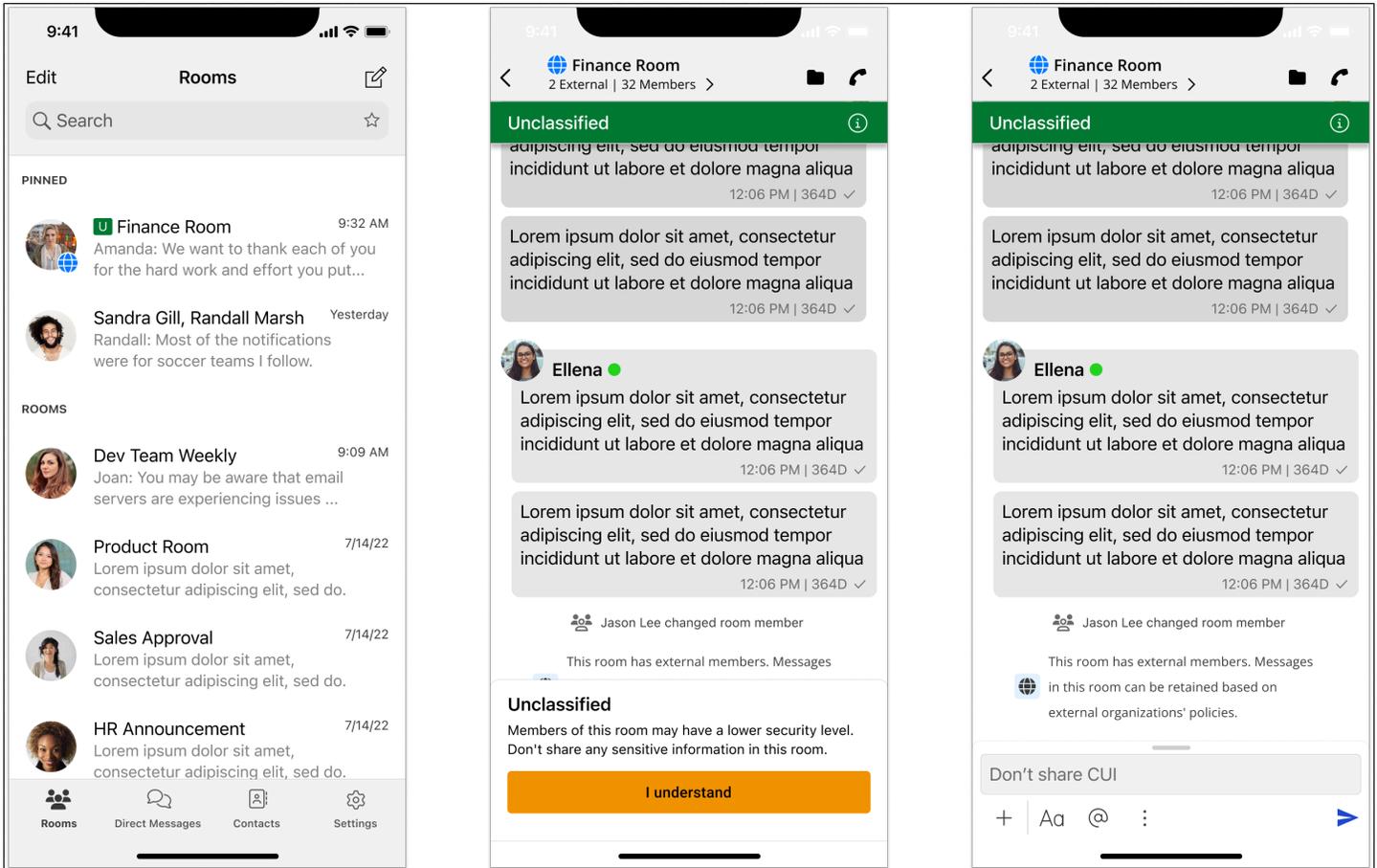
Los correos electrónicos de registro y verificación se envían desde `donotreply@wickr.email`.

Si necesitas permitir enumerar todas las direcciones IP posibles de los servidores de llamadas, tendrás que descargar el [AllowlistWickrarchivo.txt](#) de los posibles CIDR y revisarlo periódicamente, ya que está sujeto a cambios.

## GovCloud clasificación y federación transfronterizas

AWS Wickr ofrece un WickrGov cliente personalizado para GovCloud los usuarios. La GovCloud Federación permite la comunicación entre GovCloud usuarios y usuarios comerciales. La función de clasificación transfronteriza permite a los usuarios modificar la interfaz de usuario en las GovCloud conversaciones. Como GovCloud usuario, debe cumplir con las directrices estrictas relativas a la clasificación definida por el gobierno. Cuando GovCloud los usuarios establezcan conversaciones con usuarios comerciales (Enterprise, AWS Wickr, usuarios invitados), verán las siguientes advertencias no clasificadas:

- Una etiqueta U en la lista de habitaciones
- Un reconocimiento no clasificado en la pantalla de mensajes
- Un banner no clasificado en la parte superior de la conversación



**Note**

Estas advertencias solo se mostrarán cuando un GovCloud usuario esté conversando o formando parte de una sala con usuarios externos. Desaparecerán si los usuarios externos abandonan la conversación. No se mostrará ninguna advertencia en las conversaciones entre GovCloud usuarios.

# Cómo gestionar usuarios en AWS Wickr

En la sección Usuarios de Wickr puedes ver los usuarios y bots actuales de Wickr y modificar sus detalles. AWS Management Console

Temas

- [Directorio de equipos](#)
- [Usuarios invitados](#)

## Directorio de equipos

Puedes ver los usuarios actuales de Wickr y modificar sus detalles en la sección Usuario de Wickr. AWS Management Console

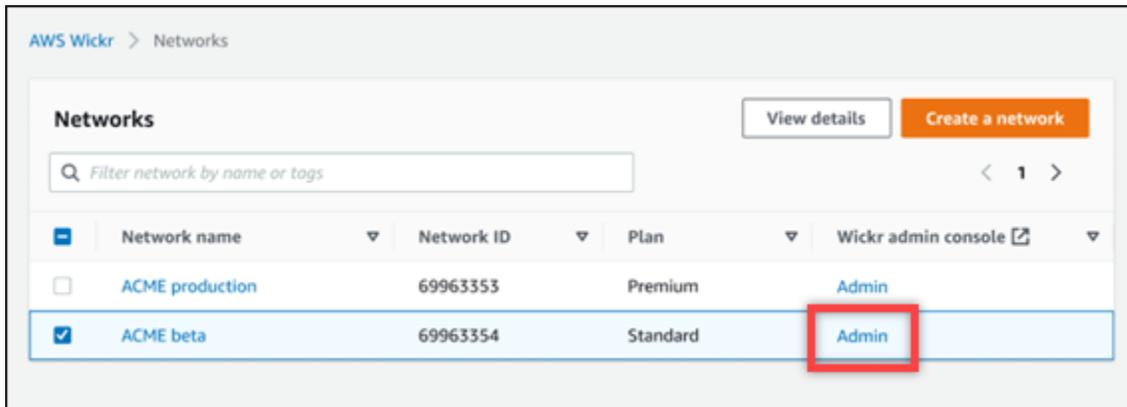
Temas

- [Ver usuarios](#)
- [Cómo crear usuarios](#)
- [Cómo editar usuarios](#)
- [Eliminar usuarios](#)
- [Cómo eliminar usuarios en bloque](#)
- [Suspensión de usuarios en bloque](#)

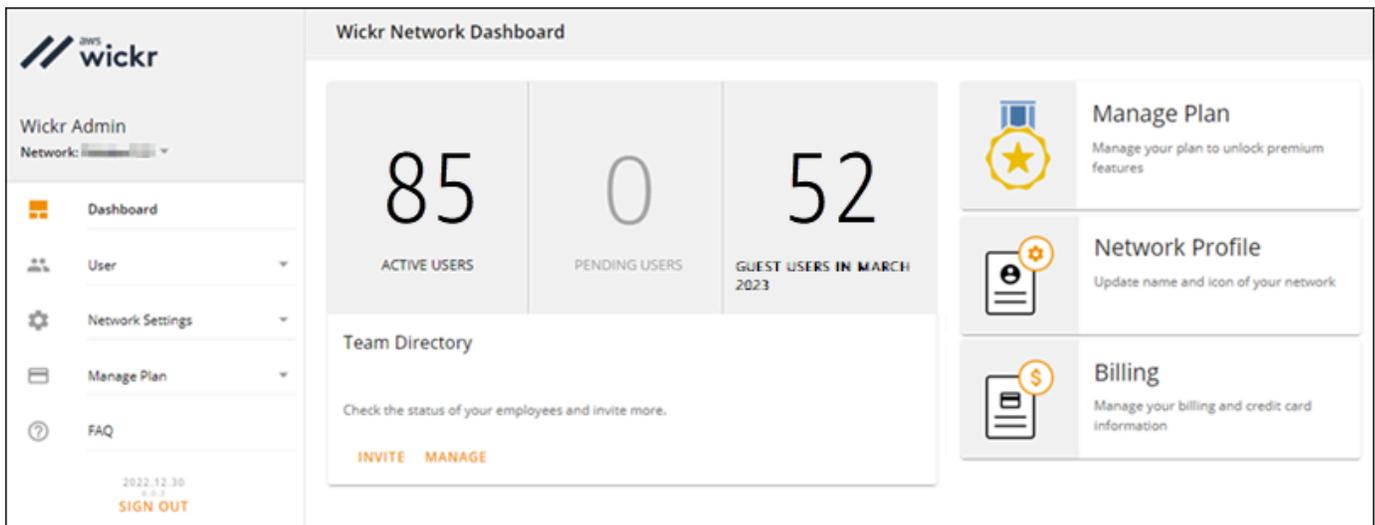
## Ver usuarios

Siga el procedimiento que se indica a continuación para ver los usuarios registrados en su red de Wickr.

1. [Abre el formulario de AWS Management Console Wickr en https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. En la página Redes, seleccione el enlace Admin para acceder a la consola de administración de Wickr de dicha red.



Se le redirigirá a la consola de administración de Wickr de una red específica.



3. En el panel de navegación de la consola de administración de Wickr, seleccione Usuario y, a continuación, Directorio de equipos.

La página Directorio de equipos muestra los usuarios registrados en su red de Wickr, incluida información como su nombre, dirección de correo electrónico, grupo de seguridad asignado y estado actual. En el caso de los usuarios actuales, puede ver sus dispositivos, editar su información, suspenderlos, eliminarlos y cambiarlos a otra red de Wickr.

## Cómo crear usuarios

Siga el procedimiento que se indica a continuación para crear un usuario.

1. [Abre el formulario AWS Management Console para Wickr en https://console.aws.amazon.com/wickr/.](https://console.aws.amazon.com/wickr/)

2. En la página Redes, seleccione el enlace Admin para acceder a la consola de administración de Wickr de dicha red.

Se le redirigirá a la consola de administración de Wickr de una red específica.

3. En el panel de navegación de la consola de administración de Wickr, seleccione Usuario y, a continuación, Directorio de equipos.
4. Elija Crear usuarios.
5. En el formulario que aparecerá a continuación, escriba el nombre y apellidos, el código de país, el número de teléfono y la dirección de correo electrónico de los usuarios. El único campo obligatorio es la dirección de correo electrónico. Asegúrese de elegir el grupo de seguridad adecuado para los usuarios. Wickr les enviará un correo electrónico de invitación a la dirección que se indique.
6. Seleccione Crear.

Se enviará un correo electrónico al usuario. El correo electrónico incluye enlaces para descargar las aplicaciones de cliente Wickr y un enlace para registrarse en Wickr. A medida que los usuarios se registren en Wickr utilizando su enlace del correo electrónico, su estado en el directorio del equipo de Wickr cambiará de Pendiente a Activo.

## Cómo editar usuarios

Siga el procedimiento que se indica a continuación para editar usuarios.

1. [Abre el formulario AWS Management Console para Wickr en https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. En la página Redes, seleccione el enlace Admin para acceder a la consola de administración de Wickr de dicha red.

Se le redirigirá a la consola de administración de Wickr de una red específica.

3. En el panel de navegación de la consola de administración de Wickr, seleccione Usuario y, a continuación, Directorio de equipos.
4. Seleccione el icono de los puntos suspensivos en vertical situado junto al nombre del usuario que desea eliminar.
5. Puede elegir una de las siguientes opciones:

- Dispositivos: muestra los dispositivos que el usuario ha configurado en el cliente Wickr.

- **Editar:** permite editar la información del usuario, como su nombre, código de país, número de teléfono (opcional) y grupo de seguridad asignado.
- **Suspender:** sirve para suspender al usuario para que no pueda iniciar sesión en su red de Wickr del cliente Wickr. Cuando se suspende a un usuario que está conectado a la red de Wickr del cliente, la sesión de dicho usuario se cierra automáticamente.
- **Eliminar:** elimina el usuario de la red de Wickr.

## Eliminar usuarios

Siga el procedimiento que se indica a continuación para eliminar un usuario.

1. [Abre el formulario AWS Management Console para Wickr en https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. En la página Redes, seleccione el enlace Admin para acceder a la consola de administración de Wickr de dicha red.

Se le redirigirá a la consola de administración de Wickr de una red específica.

3. En el panel de navegación de la consola de administración de Wickr, seleccione Usuario y, a continuación, Directorio de equipos.
4. Seleccione el icono de los puntos suspensivos en vertical situado junto al nombre del usuario que desea eliminar.
5. Seleccione Eliminar para eliminarlo.

Cuando se elimina a un usuario, dicho usuario ya no puede iniciar sesión en su red de Wickr del cliente Wickr.

## Cómo eliminar usuarios en bloque

Puede eliminar y suspender en bloque a los usuarios de la red de Wickr en la sección Usuarios de la consola de administración de Wickr.

### Note

La opción de eliminar usuarios de forma masiva solo se aplica cuando el SSO no está activado.

Para eliminar en bloque los usuarios de su red de Wickr mediante una plantilla CSV, siga el procedimiento indicado a continuación.

1. [Abre el formulario AWS Management Console de Wickr en https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. En el panel de navegación de la consola de administración de Wickr, seleccione Usuario y, a continuación, Directorio de equipos.

La página Directorio de equipos muestra los usuarios registrados en su red de Wickr.

3. En la página Directorio de equipos, seleccione Gestión de usuarios.
4. En la ventana emergente de Gestión de usuarios, seleccione Eliminar usuarios.
5. Descargue la plantilla CSV de ejemplo. Para descargar la plantilla de ejemplo, seleccione Descargar plantilla.
6. Rellene la plantilla con el correo electrónico de los usuarios que desee eliminar de su red en bloque.
7. Cargue la plantilla CSV una vez completada. Puede arrastrar y soltar el archivo en el cuadro de carga o seleccionar un archivo.
8. Marque la casilla de verificación Sé que la acción de eliminar usuarios es irreversible.
9. Seleccione Eliminar usuarios.

 Note

Esta acción empezará a eliminar a usuarios inmediatamente y puede tardar varios minutos. Los usuarios eliminados ya no podrán iniciar sesión en su red de Wickr del cliente Wickr.

Para eliminar en bloque a usuarios de su red de Wickr descargando un CSV del directorio de su equipo, siga el procedimiento indicado a continuación.

1. [Abre el formulario AWS Management Console para Wickr en https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. En el panel de navegación de la consola de administración de Wickr, seleccione Usuario y, a continuación, Directorio de equipos.

La página Directorio de equipos muestra los usuarios registrados en su red de Wickr.

3. Seleccione el icono de descarga de CSV situado en la esquina superior derecha de la página del directorio de equipos.
4. Tras descargar la plantilla CSV del directorio del equipo, elimine las filas de usuarios que desee conservar.
5. En la página Directorio de equipos, seleccione Gestión de usuarios.
6. En la ventana emergente de Gestión de usuarios, seleccione Eliminar usuarios.
7. Suba la plantilla CSV del directorio del equipo. Puede arrastrar y soltar el archivo en el cuadro de carga o seleccionar un archivo.
8. Marque la casilla de verificación Sé que la acción de eliminar usuarios es irreversible.
9. Seleccione Eliminar usuarios.

#### Note

Esta acción empezará a eliminar a usuarios inmediatamente y puede tardar varios minutos. Los usuarios eliminados ya no podrán iniciar sesión en su red de Wickr del cliente Wickr.

## Suspensión de usuarios en bloque

Puede suspender en bloque a los usuarios de la red de Wickr en la sección Usuario de la consola de administración de Wickr.

#### Note

La opción de suspender usuarios de forma masiva solo se aplica cuando el SSO no está activado.

Para suspender en bloque a los usuarios de la red de Wickr, siga el procedimiento que se detalla a continuación.

1. [Abre el formulario AWS Management Console para Wickr en https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. En el panel de navegación de la consola de administración de Wickr, seleccione Usuario y, a continuación, Directorio de equipos.

La página Directorio de equipos muestra los usuarios registrados en su red de Wickr.

3. En la página Directorio de equipos, seleccione Gestión de usuarios.
4. En la ventana emergente de Gestión de usuarios, seleccione Eliminar usuarios.
5. Descargue la plantilla CSV de ejemplo. Para descargar la plantilla de ejemplo, seleccione Descargar plantilla.
6. Rellene la plantilla con el correo electrónico de los usuarios que desee suspender en bloque de la red.
7. Cargue la plantilla CSV una vez completada. Puede arrastrar y soltar el archivo en el cuadro de carga o seleccionar un archivo.
8. Después de subir el archivo CSV, elija Suspender usuarios.

#### Note

Esta acción empezará a suspender a los usuarios de forma inmediata y puede tardar varios minutos. Los usuarios suspendidos no podrán iniciar sesión en su red de Wickr del cliente Wickr. Cuando se suspende a un usuario que está conectado a la red de Wickr del cliente, la sesión de dicho usuario se cierra automáticamente.

## Usuarios invitados

La característica de usuario invitado de Wickr permite que usuarios invitados individuales inicien sesión en el cliente Wickr y colaboren con los usuarios de la red de Wickr. Los administradores de Wickr pueden habilitar o deshabilitar los usuarios invitados para sus redes de Wickr en la página Grupo de seguridad de la consola de administración de Wickr.

Una vez habilitada la característica, los usuarios invitados a su red de Wickr pueden interactuar con los usuarios de su red de Wickr. Se le aplicará una tarifa Cuenta de AWS por la función de usuario invitado. Para obtener más información sobre los precios de la característica de usuario invitado, consulta la página de [Precios de Wickr](#) en los complementos Precios.

### Temas

- [Cómo habilitar o deshabilitar usuarios invitados](#)
- [Cómo ver el número de usuarios invitados](#)
- [Cómo ver el uso mensual](#)

- [Cómo ver los usuarios invitados](#)
- [Cómo bloquear a un usuario invitado](#)

## Cómo habilitar o deshabilitar usuarios invitados

Complete el procedimiento siguiente para habilitar o deshabilitar usuarios invitados para su red de Wickr.

1. Abra el formulario AWS Management Console de Wickr en <https://console.aws.amazon.com/wickr/>.
2. En la página Redes, seleccione el enlace Admin para acceder a la consola de administración de Wickr de dicha red.

Se le redirigirá a la consola de administración de Wickr de una red específica.

3. En el panel de navegación de la consola de administración de Wickr, seleccione Configuración de red y, a continuación, Grupo de seguridad.
4. Seleccione Detalles para un grupo de seguridad específico.

### Note

Puede habilitar usuarios invitados únicamente para grupos de seguridad individuales. Para habilitar usuarios invitados en todos los grupos de seguridad de su red de Wickr, debe habilitar la característica para cada grupo de seguridad de su red.

5. En la página de detalles del grupo de seguridad, elija la pestaña Federación.
6. Hay dos ubicaciones en las que estará disponible la opción para permitir usuarios invitados:
  - Federación local: para las redes del Este de EE. UU. (Norte de Virginia), seleccione Editar junto a la sección Federación local de la página.
  - Federación global: para el resto de redes de otras regiones, seleccione Editar junto a la sección Federación global de la página.
7. Seleccione Permitir usuarios invitados para habilitar los usuarios invitados en el grupo de seguridad o anule la selección para deshabilitarlos.
8. Elija Guardar para guardar el cambio y hacerlo efectivo para el grupo de seguridad.

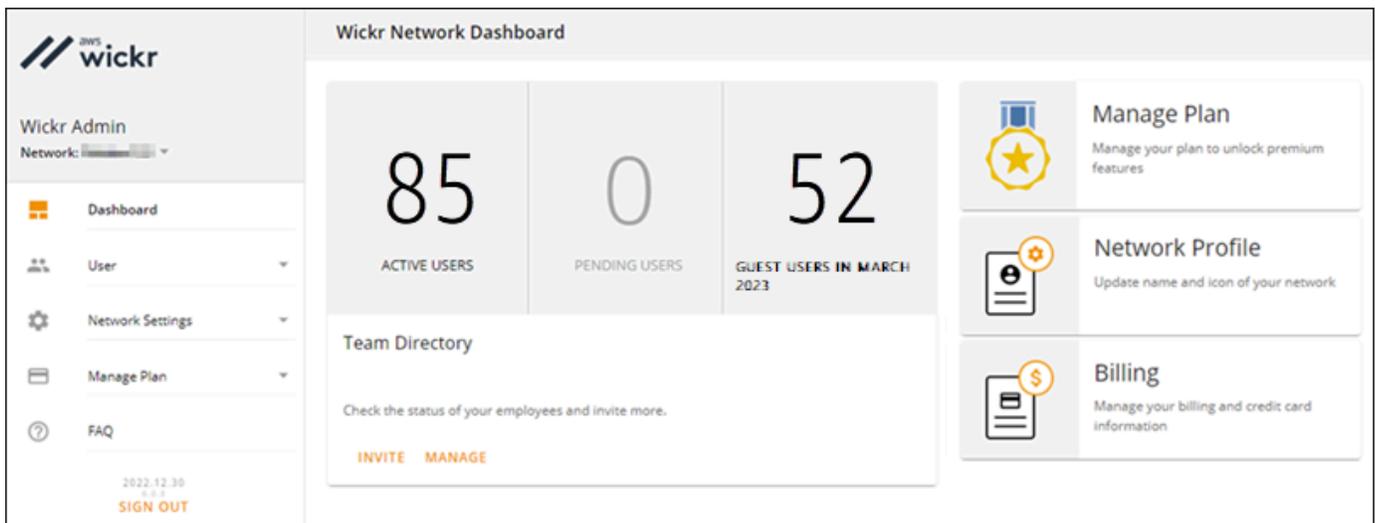
Los usuarios registrados en el grupo de seguridad específico de su red de Wickr ahora pueden interactuar con usuarios invitados. Para obtener más información, consulte [Usuarios invitados](#) en la Guía del usuario de Wickr.

## Cómo ver el número de usuarios invitados

Siga el procedimiento indicado a continuación para ver la cuenta de usuario invitado de su red de Wickr.

1. [Abre el formulario AWS Management Console para Wickr en https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. En la página Redes, seleccione el enlace Admin para acceder a la consola de administración de Wickr de dicha red.

Se le redirigirá a la consola de administración de Wickr de una red específica. La página Panel muestra un recuento de usuarios invitados en su red de Wickr, como se muestra en el siguiente ejemplo.



## Cómo ver el uso mensual

Puede ver el número de usuarios invitados con los que se ha comunicado su red durante un período de facturación. Para ver su uso mensual, siga los pasos que se describen a continuación.

1. [Abre el formulario AWS Management Console para Wickr en https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).

2. En la página Redes, seleccione el enlace Admin para acceder a la consola de administración de Wickr de dicha red.
3. En el panel de navegación de la consola de administración de Wickr, elija Usuario y, luego, Usuarios invitados.
4. En la página Usuarios invitados, seleccione la sección Uso mensual.

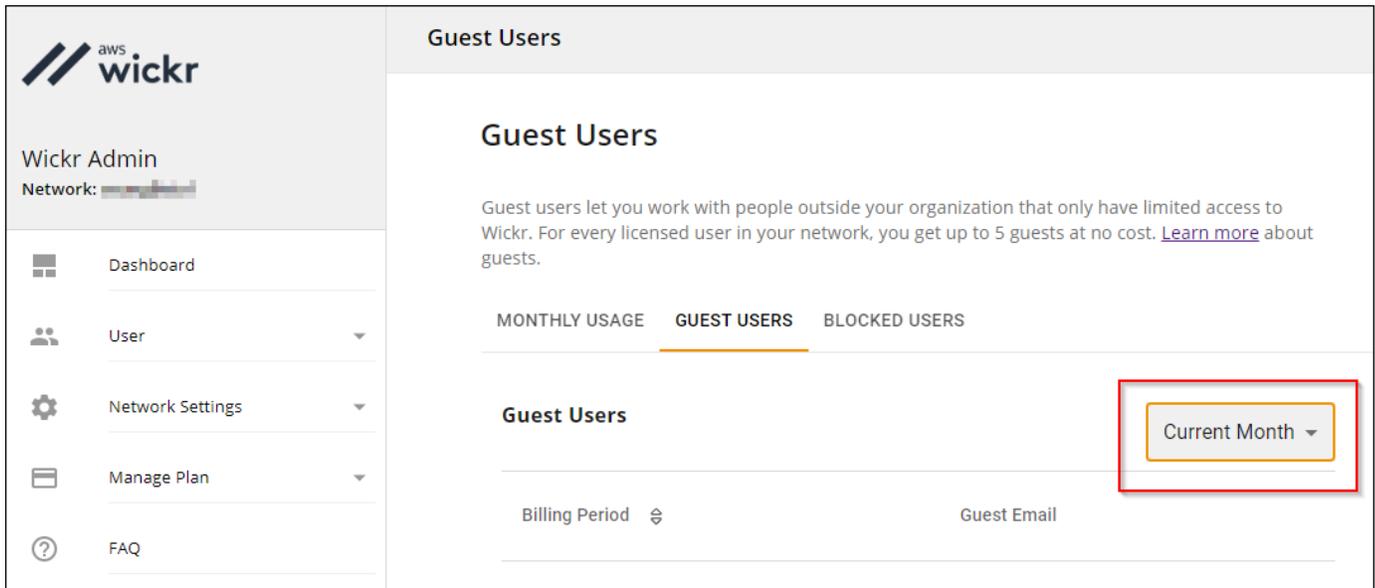
 Note

Los datos de facturación de invitados se actualizan cada 24 horas.

## Cómo ver los usuarios invitados

Puede ver una lista de usuarios invitados con los que se ha comunicado su red durante un período de facturación. Para ver sus usuarios invitados, siga los pasos siguientes.

1. [Abre el formulario AWS Management Console para Wickr en https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. En la página Redes, seleccione el enlace Admin para acceder a la consola de administración de Wickr de dicha red.
3. En el panel de navegación de la consola de administración de Wickr, elija Usuario y, luego, Usuarios invitados.
4. En la página Usuarios invitados, seleccione la sección Usuarios invitados.
5. Para ver los usuarios invitados de un mes específico, seleccione el mes correspondiente en el menú desplegable.



## Cómo bloquear a un usuario invitado

Los usuarios bloqueados no pueden comunicarse con nadie de su red.

Cómo bloquear a un usuario invitado

1. [Abre el formulario AWS Management Console para Wickr en https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. En la página Redes, seleccione el enlace Admin para acceder a la consola de administración de Wickr de dicha red.
3. En el panel de navegación de la consola de administración de Wickr, elija Usuario y, luego, Usuarios invitados.
4. En la página Usuarios invitados, seleccione la sección Usuarios invitados.
5. La sección Usuarios invitados muestra los usuarios invitados que se han comunicado en su red de Wickr.
6. En la sección Usuarios invitados, busque el correo electrónico del usuario invitado que desea bloquear.
7. A la derecha del nombre del usuario invitado, seleccione los tres puntos y elija Bloquear.
8. Seleccione Bloquear en la ventana emergente.
9. Para ver la lista de usuarios bloqueados en su red de Wickr, seleccione la sección Usuarios bloqueados.

## Cómo bloquear a un usuario invitado

1. [Abre el formulario AWS Management Console para Wickr en https://console.aws.amazon.com/wickr/](https://console.aws.amazon.com/wickr/).
2. En la página Redes, seleccione el enlace Admin para acceder a la consola de administración de Wickr de dicha red.
3. En el panel de navegación de la consola de administración de Wickr, elija Usuario y, luego, Usuarios invitados.
4. En la página Usuarios invitados, seleccione la sección Usuarios bloqueados.
5. La sección Usuarios bloqueados muestra los usuarios invitados que están bloqueados en su red de Wickr.
6. En la sección Usuarios bloqueados, busque el correo electrónico del usuario invitado que desea bloquear.
7. A la derecha del nombre del usuario invitado, seleccione los tres puntos y elija Desbloquear.
8. Elija Desbloquear en la ventana emergente.

# Seguridad en AWS Wickr

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El [modelo de responsabilidad compartida](#) la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los [AWS programas](#) de de . Para obtener más información sobre los programas de conformidad que se aplican a AWS Wickr, consulte [AWS Servicios dentro del alcance por programa de conformidad AWS Servicios incluidos](#) .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Wickr. En los siguientes temas, se le mostrará cómo configurar Wickr para satisfacer sus objetivos de seguridad y conformidad. También aprenderás a usar otros AWS servicios que te ayudan a monitorear y proteger tus recursos de Wickr.

## Temas

- [Protección de datos en AWS Wickr](#)
- [Administración de identidades y accesos en alta AWS Wickr](#)
- [Validación de conformidad](#)
- [Resiliencia en AWS Wickr](#)
- [Seguridad de la infraestructura en AWS Wickr](#)
- [Configuración y análisis de vulnerabilidades en AWS Wickr](#)
- [Prácticas recomendadas de seguridad para AWS Wickr](#)

## Protección de datos en AWS Wickr

El [modelo de](#) se aplica a protección de datos en AWS Wickr. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las [Preguntas frecuentes sobre la privacidad de datos](#). Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el [Modelo de responsabilidad compartida de AWS y GDPR](#) en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte [Estándar de procesamiento de la información federal \(FIPS\) 140-2](#).

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabajas con Wickr u otro dispositivo Servicios de AWS mediante la consola, la API o los SDK. AWS CLI AWS Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación

o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

## Administración de identidades y accesos en alta AWS Wickr

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los recursos. AWS Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Wickr. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

### Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración de acceso mediante políticas](#)
- [AWS políticas administradas para AWS Wickr](#)
- [Cómo funciona AWS Wickr con IAM](#)
- [Ejemplos de políticas basadas en identidades de AWS Wickr](#)
- [Solución de problemas de identidades y accesos en AWS Wickr](#)

## Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realices en Wickr.

Usuario de servicio: si utiliza el servicio de Wickr para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Wickr para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en Wickr, consulte [Solución de problemas de identidades y accesos en AWS Wickr](#).

Administrador de servicio: si está a cargo de los recursos de Wickr en su empresa, probablemente tenga acceso completo a Wickr. Su trabajo consiste en determinar a qué características y recursos

de Wickr deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con Wickr, consulte [Cómo funciona AWS Wickr con IAM](#).

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a Wickr. Para consultar ejemplos de políticas basadas en la identidad de Wickr que puede utilizar en IAM, consulte [Ejemplos de políticas basadas en identidades de AWS Wickr](#).

## Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, asumes un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte [Cómo iniciar sesión Cuenta de AWS en su](#) Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte [Firmar las solicitudes de la AWS API](#) en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte [Autenticación multifactor](#) en la Guía del usuario de AWS IAM Identity Center y [Uso de la autenticación multifactor \(MFA\) en AWS](#) en la Guía del usuario de IAM.

## Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte [Tareas que requieren credenciales de usuario raíz](#) en la Guía del usuario de IAM.

## Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulte [¿Qué es el Centro de identidades de IAM?](#) en la Guía del usuario de AWS IAM Identity Center .

## Usuarios y grupos de IAM

Un [usuario de IAM](#) es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte [Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración](#) en la Guía del usuario de IAM.

Un [grupo de IAM](#) es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte [Cuándo crear un usuario de IAM \(en lugar de un rol\)](#) en la Guía del usuario de IAM.

## Roles de IAM

Un [rol de IAM](#) es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console [cambiando](#) de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte [Uso de roles de IAM](#) en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- **Acceso de usuario federado:** para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte [Creación de un rol para un proveedor de identidades de terceros](#) en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte [Conjuntos de permisos](#) en la Guía del usuario de AWS IAM Identity Center .
- **Permisos de usuario de IAM temporales:** un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- **Acceso entre cuentas:** puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener

información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

- **Acceso entre servicios:** algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
- **Sesiones de acceso directo (FAS):** cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte [Reenviar sesiones de acceso](#).
- **Rol de servicio:** un rol de servicio es un [rol de IAM](#) que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte [Creación de un rol para delegar permisos a un Servicio de AWS](#) en la Guía del usuario de IAM.
- **Función vinculada al servicio:** una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- **Aplicaciones que se ejecutan en Amazon EC2:** puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar un AWS rol a una instancia EC2 y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte [Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2](#) en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte [Cuándo crear un rol de IAM \(en lugar de un usuario\)](#) en la Guía del usuario de IAM.

## Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte [Información general de políticas JSON](#) en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

## Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte [Creación de políticas de IAM](#) en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una

política administrada o una política insertada, consulte [Elegir entre políticas administradas y políticas insertadas](#) en la Guía del usuario de IAM.

## Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe [especificar una entidad principal](#) en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

## Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte [Información general de Lista de control de acceso \(ACL\)](#) en la Guía para desarrolladores de Amazon Simple Storage Service.

## Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- **Límites de permisos:** un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una identidad. Los permisos resultantes son la intersección de las políticas basadas en identidad de la entidad y los límites de sus permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites

de los permisos, consulte [Límites de permisos para las entidades de IAM](#) en la Guía del usuario de IAM.

- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte [Políticas de sesión](#) en la Guía del usuario de IAM.

## Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la [lógica de evaluación de políticas](#) en la Guía del usuario de IAM.

## AWS políticas administradas para AWS Wickr

Para añadir permisos a usuarios, grupos y roles, es más fácil usar políticas AWS administradas que escribirlas tú mismo. Se necesita tiempo y experiencia para [crear políticas administradas por el cliente de IAM](#) que proporcionen a su equipo solo los permisos necesarios. Para empezar rápidamente, puedes usar nuestras políticas AWS gestionadas. Estas políticas cubren casos de uso comunes y están disponibles en su Cuenta de AWS. Para obtener más información sobre las políticas AWS administradas, consulte las [políticas AWS administradas](#) en la Guía del usuario de IAM.

Servicios de AWS mantener y actualizar las políticas AWS gestionadas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios agregan permisos adicionales a una política administrada por AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política administrada por AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

## AWS política gestionada: AWSWickrFullAccess

Puede adjuntar la política `AWSWickrFullAccess` a las identidades de IAM. Esta política concede todos los permisos administrativos al servicio Wickr, incluida la AWS Management Console para Wickr en AWS Management Console. Para más información sobre cómo adjuntar políticas a una identidad, consulte [Adición y eliminación de permisos de identidad de IAM](#) en la Guía del usuario de AWS Identity and Access Management .

### Detalles de los permisos

Esta política incluye los siguientes permisos.

- `wickr:` concede todos los permisos administrativos al servicio Wickr.

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

## Wickr actualiza las políticas AWS gestionadas

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas de Wickr desde que este servicio comenzó a rastrear estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbese a la fuente RSS en la página de historial de documentos de Wickr.

Cambio	Descripción	Fecha
<a href="#">AWSWickrFullAccess</a> : política nueva	Wickr agregó una nueva política que otorga todos los permisos administrativos al servicio Wickr, incluida la consola de administrador de	28 de noviembre de 2022

Cambio	Descripción	Fecha
	Wickr en AWS Management Console.	
Wickr comenzó el seguimiento de los cambios	Wickr comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	28 de noviembre de 2022

## Cómo funciona AWS Wickr con IAM

Antes de utilizar IAM para administrar el acceso a Wickr, conozca qué características de IAM se pueden utilizar con Wickr.

Características de IAM que puede utilizar con AWS Wickr

Característica de IAM	Compatibilidad de Wickr
<a href="#">Políticas basadas en identidades</a>	Sí
<a href="#">Políticas basadas en recursos</a>	No
<a href="#">Acciones de políticas</a>	Sí
<a href="#">Recursos de políticas</a>	No
<a href="#">Claves de condición de política</a>	No
<a href="#">ACL</a>	No
<a href="#">ABAC (etiquetas en políticas)</a>	No
<a href="#">Credenciales temporales</a>	No
<a href="#">Permisos de entidades principales</a>	No
<a href="#">Roles de servicio</a>	No

Característica de IAM	Compatibilidad de Wickr
<a href="#">Roles vinculados al servicio</a>	No

Para obtener una visión general de cómo funcionan Wickr y otros AWS servicios con la mayoría de las funciones de IAM, consulta [AWS los servicios que funcionan con IAM en la Guía del usuario de IAM](#).

## Políticas basadas en identidades de Wickr

Compatibilidad con las políticas basadas en identidad	Sí
---	----

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte [Creación de políticas de IAM](#) en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para más información sobre los elementos que puede utilizar en una política de JSON, consulte [Referencia de los elementos de las políticas de JSON de IAM](#) en la Guía del usuario de IAM.

## Ejemplos de políticas basadas en identidades de Wickr

Para ver ejemplos de políticas basadas en identidad de Wickr, consulte [Ejemplos de políticas basadas en identidades de AWS Wickr](#).

## Políticas basadas en recursos de Wickr

Compatibilidad con las políticas basadas en recursos	No
--	----

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe [especificar una entidad principal](#) en una política en función de recursos. Los directores pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

## Acciones de política para Wickr

Admite acciones de política	Sí
-----------------------------	----

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de Wickr, consulte [Acciones definidas por AWS Wickr](#) en la Referencia de autorizaciones de servicio.

Las acciones de políticas de Wickr utilizan el siguiente prefijo antes de la acción:

```
wickr
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

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

Para ver ejemplos de políticas basadas en identidad de Wickr, consulte [Ejemplos de políticas basadas en identidades de AWS Wickr](#).

## Recursos de políticas de Wickr

Admite recursos de políticas

No

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el [Nombre de recurso de Amazon \(ARN\)](#). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (\*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de recursos de Wickr y sus ARN, consulte [Recursos definidos por AWS Wickr](#) en la Referencia de autorizaciones de servicio. Para obtener información sobre las

acciones con las que puede especificar el ARN de cada recursos, consulte [Acciones definidas por AWS Wickr](#).

Para ver ejemplos de políticas basadas en identidad de Wickr, consulte [Ejemplos de políticas basadas en identidades de AWS Wickr](#).

## Claves de condición de política para Wickr

Admite claves de condición de políticas específicas del servicio	No
--	----

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen [operadores de condición](#), tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación AND lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una OR operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte [Elementos de la política de IAM: variables y etiquetas](#) en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de [contexto de condición AWS globales en la Guía](#) del usuario de IAM.

Para ver una lista de las claves de condición de Wickr, consulte [Claves de condición para AWS Wickr](#) en la Referencia de autorizaciones de servicio. Para obtener más información acerca de las acciones y los recursos con los que puede utilizar una clave de condición, consulte [Acciones definidas por AWS Wickr](#).

Para ver ejemplos de políticas basadas en identidad de Wickr, consulte [Ejemplos de políticas basadas en identidades de AWS Wickr](#).

## ACL en Wickr

Admite las ACL

No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

## ABAC con Wickr

Admite ABAC (etiquetas en las políticas)

No

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el [elemento de condición](#) de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte [¿Qué es ABAC?](#) en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte [Uso del control de acceso basado en atributos \(ABAC\)](#) en la Guía del usuario de IAM.

## Uso de credenciales temporales con Wickr

Compatible con el uso de credenciales temporales No

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta Cómo [Servicios de AWS funcionan con IAM](#) en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobre el cambio de roles, consulte [Cambio a un rol \(consola\)](#) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte [Credenciales de seguridad temporales en IAM](#).

## Permisos de entidades principales entre servicios de Wickr

Admite sesiones de acceso directo (FAS) No

Cuando utilizas un usuario o un rol de IAM para realizar acciones en AWSél, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte [Reenviar sesiones de acceso](#).

## Roles de servicio de Wickr

Compatible con roles de servicio	No
----------------------------------	----

Un rol de servicio es un [rol de IAM](#) que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte [Creación de un rol para delegar permisos a un Servicio de AWS](#) en la Guía del usuario de IAM.

### Warning

Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de Wickr. Edite los roles de servicio solo cuando Wickr proporcione orientación para hacerlo.

## Roles vinculados a servicios de Wickr

Compatible con roles vinculados al servicio	No
---	----

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulte [Servicios de AWS que funcionan con IAM](#). Busque un servicio en la tabla que incluya Yes en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

## Ejemplos de políticas basadas en identidades de AWS Wickr

De forma predeterminada, un nuevo usuario de IAM no tiene permisos para realizar ninguna actividad. Un administrador de IAM debe crear y asignar políticas de IAM que concedan permisos a los usuarios para administrar el servicio AWS Wickr. A continuación se muestra un ejemplo de una política de permisos.

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

Este ejemplo de política otorga a los usuarios permisos para crear, ver y administrar redes de Wickr mediante Wickr. AWS Management Console Para obtener más información sobre los elementos de una instrucción de política de IAM, consulte [Políticas basadas en identidades de Wickr](#). Para obtener más información acerca de cómo crear una política de IAM con estos documentos de políticas de JSON de ejemplo, consulte [Creación de políticas en la pestaña JSON](#) en la Guía del usuario de IAM.

## Temas

- [Prácticas recomendadas sobre las políticas](#)
- [Uso de la AWS Management Console para Wickr](#)
- [Cómo permitir a los usuarios consultar sus propios permisos](#)

## Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Wickr de la cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las [políticas administradas por AWS](#) o las [políticas administradas por AWS para funciones de trabajo](#) en la Guía de usuario de IAM.

- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte [Políticas y permisos en IAM](#) en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte [Elementos de la política de JSON de IAM: Condición](#) en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte [Política de validación de Analizador de acceso de IAM](#) en la Guía de usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte [Configuración del acceso a una API protegido por MFA](#) en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las [Prácticas recomendadas de seguridad en IAM](#) en la Guía del usuario de IAM.

## Uso de la AWS Management Console para Wickr

Adjunta la política `AWSWickrFullAccess` AWS gestionada a tus identidades de IAM para concederles todos los permisos administrativos necesarios para acceder al servicio de Wickr, incluida la consola de administrador de Wickr. AWS Management Console Para obtener más información, consulte [AWS política gestionada: AWSWickrFullAccess](#).

## Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API o. AWS CLI AWS

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

## Solución de problemas de identidades y accesos en AWS Wickr

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Wickr e IAM.

### Temas

- [No estoy autorizado a realizar ninguna acción administrativa en nombre de Wickr AWS Management Console](#)

### No estoy autorizado a realizar ninguna acción administrativa en nombre de Wickr AWS Management Console

Si el formulario AWS Management Console de Wickr te indica que no estás autorizado a realizar una acción, debes ponerte en contacto con tu administrador para obtener ayuda. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

El siguiente ejemplo de error se produce cuando el usuario de mateojackson IAM intenta usar AWS Management Console for Wickr para crear, administrar o ver las redes de Wickr en AWS Management Console for Wickr, pero no tiene los permisos `wickr:CreateAdminSession` `wickr:ListNetworks`

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

En este caso, Mateo pide a su administrador que actualice sus políticas para que pueda acceder a las de Wickr mediante AWS Management Console las acciones `wickr:CreateAdminSession` `wickr:ListNetworks`. Para obtener más información, consulte [Ejemplos de políticas basadas en identidades de AWS Wickr](#) y [AWS política gestionada: AWSWickrFullAccess](#).

## Validación de conformidad

Para obtener una lista de AWS los servicios incluidos en el ámbito de los programas de cumplimiento específicos, consulte los [AWS servicios incluidos en el ámbito de aplicación por programa de cumplimiento](#) y . Para obtener información general, consulte Programas de [AWS cumplimiento > Programas AWS](#) .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#) .

Su responsabilidad de conformidad al utilizar Wickr se determina en función de la sensibilidad de los datos, los objetivos de cumplimiento de su empresa y la legislación y los reglamentos correspondientes. AWS proporciona los siguientes recursos para ayudar con la conformidad:

- [Guías de inicio rápido](#) sobre : estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en la seguridad y el cumplimiento. AWS
- [AWS Recursos de](#) de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su sector y ubicación.
- [Evaluación de los recursos con las reglas](#) de la guía para AWS Config desarrolladores: AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- [AWS Security Hub](#)— Este AWS servicio proporciona una visión integral del estado de su seguridad AWS que le ayuda a comprobar el cumplimiento de los estándares y las mejores prácticas del sector de la seguridad.

## Resiliencia en AWS Wickr

La infraestructura AWS global se basa Regiones de AWS en zonas de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

[Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS](#)

Además de la infraestructura AWS global, Wickr ofrece varias funciones para ayudarlo a satisfacer sus necesidades de respaldo y resiliencia de datos. Para obtener más información, consulte [Retención de datos](#).

# Seguridad de la infraestructura en AWS Wickr

Como servicio gestionado, AWS Wickr está protegido por los procedimientos de seguridad de red AWS global que se describen en el documento técnico [Amazon Web Services: Overview of Security Processes](#).

## Configuración y análisis de vulnerabilidades en AWS Wickr

La configuración y los controles de TI son una responsabilidad compartida entre usted AWS y usted, nuestro cliente. Para obtener más información, consulte el [modelo de responsabilidad AWS compartida](#).

Es su responsabilidad configurar Wickr de acuerdo con las especificaciones y las directrices, indicar periódicamente a sus usuarios que descarguen la última versión del cliente Wickr, asegurarse de que está ejecutando la última versión del bot de retención de datos de Wickr y supervisar el uso de Wickr por parte de sus usuarios.

## Prácticas recomendadas de seguridad para AWS Wickr

Wickr proporciona un número de características de seguridad que debe tener en cuenta a la hora de desarrollar e implementar sus propias políticas de seguridad. Las siguientes prácticas recomendadas son directrices generales y no constituyen una solución de seguridad completa. Puesto que es posible que estas prácticas recomendadas no sean adecuadas o suficientes para el entorno, considérelas como consideraciones útiles en lugar de como normas.

Para evitar posibles eventos de seguridad asociados con el uso de Wickr, siga estas prácticas recomendadas:

- Implemente un acceso de privilegio mínimo y cree roles específicos para usarlos en las acciones de Wickr. Use plantillas de IAM para crear un rol. Para obtener más información, consulte [AWS políticas administradas para AWS Wickr](#).
- Acceda al AWS Management Console de Wickr autenticándose con el AWS Management Console primero. No comparta las credenciales de su consola personal. Cualquier usuario de Internet puede navegar hasta la consola, pero no puede iniciar sesión a menos que tenga credenciales válidas para acceder a la consola.

# Supervisión de AWS Wickr

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de AWS Wickr y el resto de sus AWS soluciones. AWS proporciona las siguientes herramientas de supervisión para vigilar Wickr, informar cuando algo va mal y tomar medidas automáticas cuando sea necesario:

- AWS CloudTrail captura las llamadas a la API y los eventos relacionados realizados por su AWS cuenta o en su nombre y entrega los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron las llamadas. Para más información, consulte la [Guía del usuario de AWS CloudTrail](#). Para obtener más información sobre cómo registrar las llamadas a la API de Wickr mediante CloudTrail, consulte [Registro de llamadas a la API de AWS Wickr mediante AWS CloudTrail](#).

## Registro de llamadas a la API de AWS Wickr mediante AWS CloudTrail

AWS Wickr está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Wickr. CloudTrail captura todas las llamadas a la API de Wickr como eventos. Las llamadas capturadas incluyen las llamadas desde AWS Management Console para Wickr y las llamadas de código a las operaciones de la API de Wickr. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Wickr. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puedes determinar la solicitud que se realizó a Wickr, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales. Para obtener más información CloudTrail, consulta la [Guía del AWS CloudTrail usuario](#).

## Información sobre Wickr en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en Wickr, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulta [Cómo ver eventos con el historial de CloudTrail eventos](#).

Para mantener un registro continuo de eventos en la Cuenta de AWS, incluidos los eventos de Wickr, cree un registro de seguimiento. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- [Introducción a la creación de registros de seguimiento](#)
- [CloudTrail servicios e integraciones compatibles](#)
- [Configuración de las notificaciones de Amazon SNS para CloudTrail](#)
- [Recibir archivos de CloudTrail registro de varias regiones](#) y [recibir archivos de CloudTrail registro de varias cuentas](#)

Todas las acciones de Wickr las registra. CloudTrail Por ejemplo, las llamadas a `ListNetworks` las acciones generan entradas en los archivos de CloudTrail registro. `CreateAdminSession`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario AWS Identity and Access Management (IAM) o credenciales de usuario raíz.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte el [elemento `userIdentity` de CloudTrail](#).

## Descripción de las entradas de los archivos de registro de Wickr

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `CreateAdminSession` acción.

```
{
  "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"
}

```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la CreateNetwork acción.

```

{
  "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"
}

```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la ListNetworks acción.

```

{
  "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"
}

```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la UpdateNetworkdetails acción.

```

{
  "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"
}

```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la TagResource acción.

```

{
  "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"
}

```

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la ListTagsForResource acción.

```

{
  "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"
}
```

## Panel de análisis

Puede usar el panel de análisis para ver cómo su organización utiliza AWS Wickr. En el siguiente procedimiento se explica cómo acceder al panel de análisis mediante la consola de AWS Wickr.

Para acceder al panel de análisis

1. Abre el formulario AWS Management Console de Wickr en <https://console.aws.amazon.com/wickr/>.
2. En el panel de navegación, elija Analytics (Análisis).

La página de análisis muestra las métricas de su red en diferentes pestañas.

En la página de análisis, encontrarás un filtro de intervalo de tiempo en la esquina superior derecha de cada pestaña. Este filtro se aplica a toda la página. Además, en la esquina superior derecha de cada pestaña, puede exportar los puntos de datos del intervalo de tiempo seleccionado seleccionando la opción de exportación disponible.

 Note

La hora seleccionada está en UTC (hora universal coordinada).

Están disponibles las siguientes pestañas:

- Muestra la descripción general:
  - Registrados: el número total de usuarios registrados, incluidos los usuarios activos y suspendidos en la red durante el tiempo seleccionado. No incluye los usuarios pendientes ni los invitados.
  - Pendiente: el número total de usuarios pendientes en la red durante el tiempo seleccionado.
  - Registro de usuarios: el gráfico muestra el número total de usuarios registrados en el intervalo de tiempo seleccionado.
  - Dispositivos: el número de dispositivos en los que la aplicación ha estado activa.
  - Versiones de cliente: la cantidad de dispositivos activos clasificados según sus versiones de cliente.
- Los miembros muestran:
  - Estado: usuarios activos en la red durante el período de tiempo seleccionado.
  - Usuarios activos:
    - El gráfico muestra el recuento de usuarios activos a lo largo del tiempo y se puede agregar por día, semana o mes (dentro del intervalo de tiempo seleccionado anteriormente).
    - El recuento de usuarios activos se puede desglosar por plataforma, versión de cliente o grupo de seguridad. Si se eliminó un grupo de seguridad, el recuento total se mostrará como Eliminado#.
- Aparecen los mensajes:
  - Mensajes enviados: el recuento de mensajes únicos enviados por todos los usuarios y bots de la red en el período de tiempo seleccionado.

- Llamadas: número de llamadas únicas realizadas por todos los usuarios de la red.
- Archivos: número de archivos enviados por los usuarios de la red (incluye notas de voz).
- Dispositivos: el gráfico circular muestra la cantidad de dispositivos activos clasificados por su sistema operativo.
- Versiones de cliente: la cantidad de dispositivos activos clasificados según sus versiones de cliente.

# Historial del documento

En la tabla siguiente se detallan las versiones de la documentación de Wickr.

Cambio	Descripción	Fecha
<a href="#">La función de lectura de recibos ya está disponible</a>	Los administradores de Wickr ahora pueden activar o desactivar la función de confirmación de lectura en la Consola de administración. Para obtener más información, consulte <a href="#">Leer recibos</a> .	23 de abril de 2024
<a href="#">Global Federation ahora admite la federación restringida y los administradores pueden ver los análisis de uso en la Consola de administración</a>	Global Federation ahora admite la federación restringida. Esto funciona para las redes de Wickr en otras Regiones de AWS. Para obtener más información, consulte <a href="#">Grupos de seguridad</a> . Además, los administradores ahora pueden ver sus análisis de uso en el panel de análisis de la consola de administración. Para obtener más información, consulte el <a href="#">panel de análisis</a> .	28 de marzo de 2024
<a href="#">Ya está disponible una prueba gratuita de tres meses del plan Premium de AWS Wickr</a>	Los administradores de Wickr ahora pueden elegir un plan Premium de prueba gratuito de tres meses para un máximo de 30 usuarios. Durante la prueba gratuita, están disponibles todas las funciones de los planes	9 de febrero de 2024

Estándar y Premium, incluidos los controles de administración ilimitados y la retención de datos. La función de usuario invitado no está disponible durante la prueba gratuita de Premium. Para obtener más información, consulta [Administrar el plan](#).

[La función de usuario invitado está disponible de forma general y se han agregado más controles de administrador](#)

Los administradores de Wickr pueden ahora acceder a una serie de nuevas características, como la lista de usuarios invitados, la posibilidad de eliminar o suspender usuarios de forma masiva y la opción de impedir que los usuarios invitados se comuniquen en su red de Wickr. Si desea obtener más información, consulte [Usuarios invitados](#).

8 de noviembre de 2023

[Wickr ya está disponible en Europa \(Frankfurt\) Región de AWS](#)

Wickr ya está disponible en Europa (Frankfurt). Región de AWS Para obtener más información, consulte [Acceso a Wickr](#).

26 de octubre de 2023

[Las redes de Wickr ahora tienen la capacidad de federarse en todas Regiones de AWS](#)

Las redes de Wickr tienen ahora la capacidad de federarse en todas Regiones de AWS. Para obtener más información, consulte [Grupos de seguridad](#).

29 de septiembre de 2023

<a href="#">Wickr ya está disponible en Europa (Londres) Región de AWS</a>	Wickr ya está disponible en Europa (Londres). Región de AWS Para obtener más información, consulte <a href="#">Acceso a Wickr</a> .	23 de agosto de 2023
<a href="#">Wickr ya está disponible en Canadá (Central) Región de AWS</a>	Wickr ya está disponible en Canadá (Central). Región de AWS Para obtener más información, consulte <a href="#">Acceso a Wickr</a> .	3 de julio de 2023
<a href="#">La característica de usuario invitado está ahora disponible para su vista previa</a>	Los usuarios invitados pueden iniciar sesión en el cliente Wickr y colaborar con usuarios de la red de Wickr. Para más información, consulte <a href="#">Usuarios invitados (vista previa)</a> .	31 de mayo de 2023
<a href="#">AWS Wickr ahora está integrado y está disponible en AWS GovCloud (EE. UU. Oeste) como AWS CloudTrail WickrGov</a>	AWS Wickr ahora está integrado con AWS CloudTrail. Para obtener más información, consulte <a href="#">Registro de llamadas a la API de AWS Wickr mediante AWS CloudTrail</a> . Además, Wickr ahora está disponible en EE. UU. AWS GovCloud (oeste de EE. UU.). WickrGov Para obtener más información, consulte la <a href="#">AWS WickrGov</a> Guía del AWS GovCloud (US) usuario.	30 de marzo de 2023

[Etiquetado y creación de redes múltiples](#)

AWS Wickr admite ahora el etiquetado. Para obtener más información, consulte [Etiquetas de red](#). Ahora se pueden crear varias redes en Wickr. Para obtener más información, consulte [Creación de una red](#).

7 de marzo de 2023

[Versión inicial](#)

Versión inicial de la Guía de administración de Wickr

28 de noviembre de 2022

# Notas de la versión

Para ayudarle a realizar un seguimiento de las mejoras y de las actualizaciones continuas en Wickr, estamos publicando notificaciones de la versión que describen los cambios recientes.

## Marzo de 2024

- La federación global ahora admite la federación restringida, donde la federación global solo se puede habilitar para las redes seleccionadas que se agregan bajo la federación restringida. Esto funciona para las redes de Wickr en otras Regiones de AWS. Para obtener más información, consulte [Grupos de seguridad](#).
- Los administradores ahora pueden ver sus análisis de uso en el panel de análisis de la consola de administración. Para obtener más información, consulte el [panel de análisis](#).

## Febrero de 2024

- AWS Wickr ofrece ahora una prueba gratuita de tres meses de su plan Premium para un máximo de 30 usuarios. Los cambios y las limitaciones incluyen:
  - Todas las funciones de los planes Estándar y Premium, como los controles administrativos ilimitados y la retención de datos, ahora están disponibles en la versión de prueba gratuita del plan Premium. La función de usuario invitado no está disponible durante la prueba gratuita de Premium.
  - La versión de prueba gratuita anterior ya no está disponible. Puedes actualizar tu versión de prueba gratuita o tu plan Estándar a una versión de prueba gratuita Premium si aún no la has utilizado. Para obtener más información, consulta [Administrar el plan](#).

## Noviembre de 2023

- La característica de usuarios invitados está ahora disponible de forma general. Los cambios y las adiciones incluyen:
  - Posibilidad de denunciar el abuso por parte de otros usuarios de Wickr.
  - Los administradores pueden ver una lista de los usuarios invitados con los que ha interactuado una red y los recuentos de uso mensual.
  - Los administradores pueden impedir que los usuarios invitados se comuniquen con su red.

- Precios de complementos para usuarios invitados.
- Mejoras en el control del administrador
  - Posibilidad de eliminar/suspender usuarios de forma masiva.
  - Configuración de SSO adicional para configurar un periodo de gracia para la actualización de tokens.

## Octubre de 2023

- Mejoras
  - Ahora Wickr está disponible en la Región de AWS de Europa (Fráncfort).

## Septiembre de 2023

- Mejoras
  - Las redes de Wickr tienen ahora la capacidad de federarse en todas Regiones de AWS. Para obtener más información, consulte [Grupos de seguridad](#).

## Agosto de 2023

- Mejoras
  - Ahora Wickr está disponible en la Región de AWS de Europa (Londres).

## Julio de 2023

- Mejoras
  - Ahora Wickr está disponible en la Región de AWS de Canadá (Centro).

## Mayo de 2023

- Mejoras

- Se ha añadido compatibilidad para usuarios invitados. Para obtener más información, consulte [Usuarios invitados](#).

## Marzo de 2023

- Wickr ahora está integrado con AWS CloudTrail. Para obtener más información, consulte [Registro de llamadas a la API de AWS Wickr mediante AWS CloudTrail](#).
- Wickr ahora está disponible en AWS GovCloud (EE. UU.-West) As. WickrGov Para obtener más información, consulte la [AWS WickrGov](#) Guía del AWS GovCloud (US) usuario.
- Wickr ahora admite el etiquetado. Para obtener más información, consulte [Etiquetas de red](#). Ahora se pueden crear varias redes en Wickr. Para obtener más información, consulte [Paso 1: crear una red](#).

## Febrero de 2023

- Wickr es ahora compatible con el Kit de Asalto Táctico Android (ATAK). Para obtener más información, consulte [Cómo habilitar ATAK en el panel de la red de Wickr](#).

## Enero de 2023

- El inicio de sesión único (SSO) ahora se puede configurar en todos los planes, incluidos los de prueba gratuita y estándar.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la versión original de inglés, prevalecerá la versión en inglés.