Guía de administración

AWS Wickr

AWS Wickr: Guía de administración

Table of Contents

¿Qué es AWS Wickr?

AWSWickr 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 la mensajería grupal, las llamadas de voz y vídeo, el intercambio de archivos, el uso compartido de pantalla y 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 flujos de trabajo de Wickr y automatizarlos de forma segura con los AWS Management Console bots de Wickr. Para empezar, consulte Configuración para AWS Wickr.

Temas

Características de Wickr

Seguridad y privacidad mejoradas

Wickr utiliza el cifrado Advanced Encryption Standard (AES) end-to-end de 256 bits para cada función. Las comunicaciones se cifran localmente en los dispositivos del usuario y permanecen indescifrables 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, el 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 flujos de trabajo de Wickr AWS Management Console Bots 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 hasta 5 archivos GBs 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), Europa (Zúrich), 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 al sitio web de AWS Management Console Wickr en. https://console.aws.amazon.com/wickr/ Antes de empezar a usar Wickr, debe completar las guías Configuración para AWS Wickr y Cómo empezar con 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, consulta 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, consulta los precios de AWSWickr.

Documentación para el usuario final de Wickr

Si eres un usuario final del cliente de Wickr y necesitas acceder a su documentación, consulta la Guía del usuario de AWSWickr.

Configuración para AWS Wickr

Si eres nuevo AWS cliente, complete los requisitos previos de configuración que se enumeran en esta página antes de empezar a usar AWS Wickr. Para estos procedimientos de configuración, utilice el AWS Identity and Access Management (IAM) servicio. Para obtener información completa al respectoIAM, consulte la Guía IAM del usuario.

Temas

Registrarse en AWS

Si no tiene un Cuenta de AWS, complete los pasos siguientes para crear uno.

Para suscribirse a una Cuenta de AWS

1. Abrir https://portal.aws.amazon.com/billing/registro.
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, un Usuario raíz de la cuenta de AWSse crea. El usuario root tiene acceso a todos Servicios de AWS y los recursos de la 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 de 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)	Utilice credenciales de corta duración para acceder AWS. Esto se ajusta a las prácticas recomendadas de seguridad. Para obtener información sobre las prácticas recomendadas, consulte las prácticas recomendadas de seguridad IAM en la Guía del IAM usuario.	Siga las instrucciones de Primeros pasos en la AWS IAM Identity Center Guía del usuario.	Configure el acceso programático mediante la configuración del AWS CLI para usar AWS IAM Identity Center en la AWS Command Line Interface Guía del usuario.
En IAM (No recomendado)	Utilice credenciales de larga duración para acceder AWS.	Siga las instrucciones de Cómo crear su primer usuario IAM administrador y grupo de usuarios en la Guía del IAM usuario.	Configure el acceso mediante programación mediante la administración de las claves de acceso de IAM los usuarios en la Guía del IAM usuario.

> **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.

Cómo empezar con AWS Wickr

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

Temas

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 para 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.

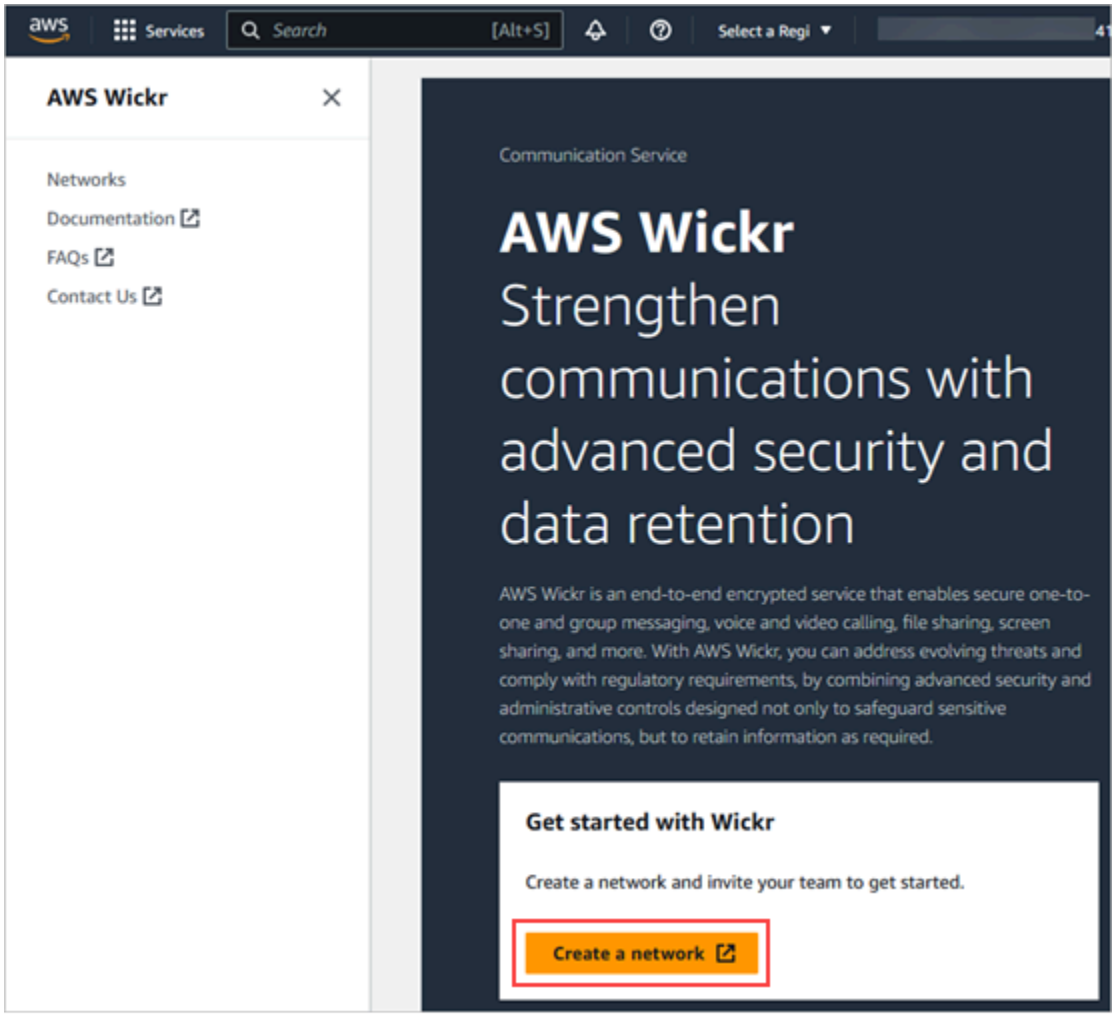
Paso 1: crear una red

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 Cat. 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.

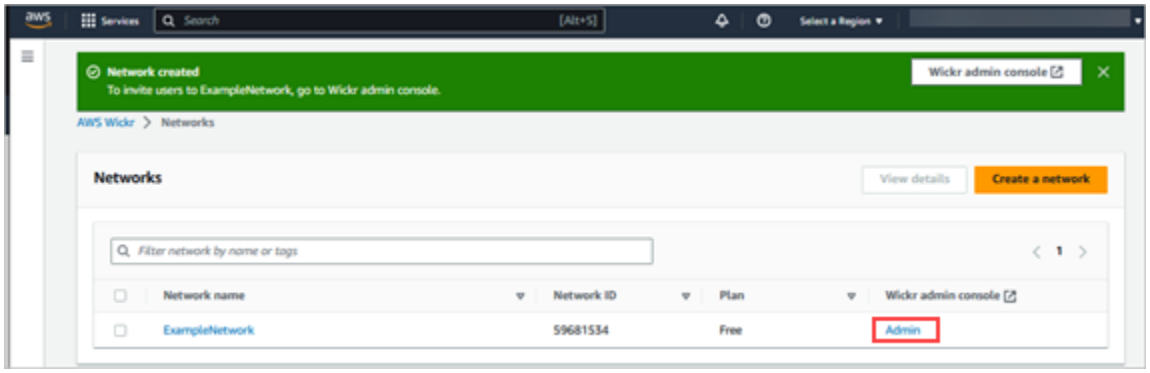
5. (Opcional) Seleccione Agregar nueva etiqueta si desea agregar una etiqueta a su red. Las etiquetas constan de un par clave-valor. Las etiquetas se pueden usar para buscar y filtrar los recursos o para un seguimiento de los costos de AWS . Para obtener más información, consulte Etiquetas de red.
6.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

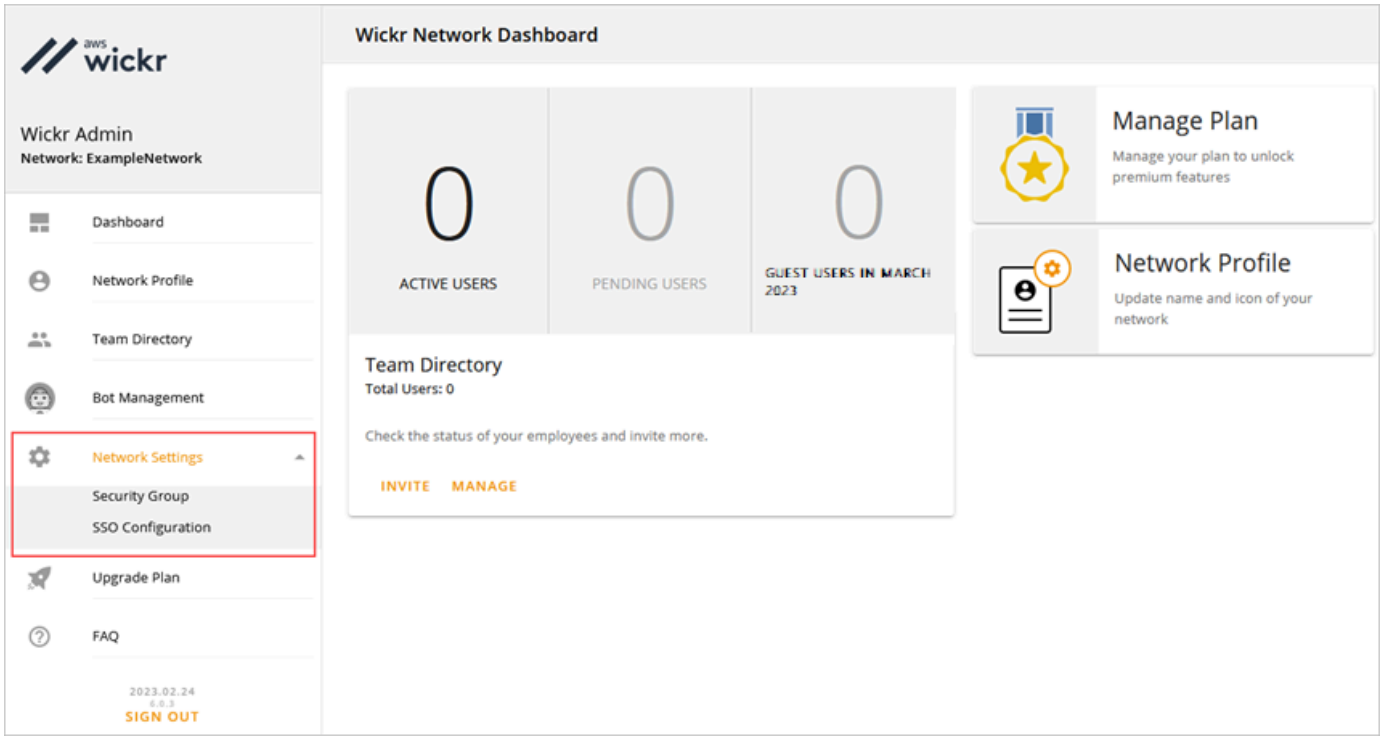
Complete el siguiente procedimiento para acceder a la consola de administración de Wickr, donde puede agregar usuarios, agregar grupos de seguridadSSO, configurar y configurar la retención de datos y otros ajustes de red.

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 Administra tu 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.
- SSOConfiguración: configura SSO y consulta la dirección del punto final de tu red de Wickr. Wickr solo es compatible con SSO los proveedores que utilizan OpenID OIDC Connect (). No se admiten los proveedores que utilizan Security Assertion Markup Language (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: si lo configurasSSO, puedes invitar a usuarios compartiendo el ID de tu 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**
>
> Los administradores también se consideran usuarios y deben invitarse a redes de Wickr SSO o ajenas a ellas. SSO

SSO

Escribe y envía un correo electrónico a los SSO usuarios que deberían registrarse en Wickr. En el mensaje, incluya la información siguiente:

- Su ID de empresa de Wickr. Al configurar, especificas un ID de empresa para tu red de Wickr. SSO Para obtener más información, consulte Configura SSO.
- La dirección de correo electrónico que deben usar para registrarse.
- Luego, URL para descargar el cliente de Wickr. Los usuarios pueden descargar los clientes de Wickr desde la página de descargas de AWS Wickr en download/. https://aws.amazon.com/wickr/

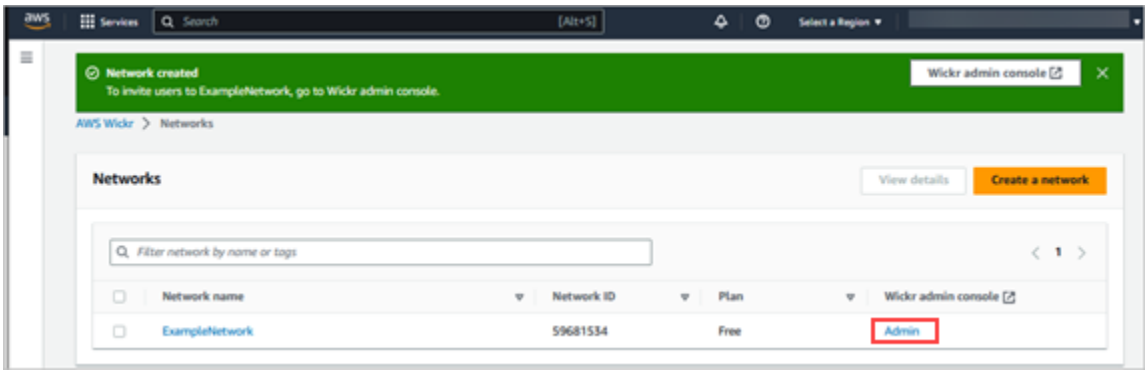
> **Note**
>
> Si has creado tu red Wickr en AWS GovCloud (EE. UU. al oeste), pide a tus usuarios que descarguen e instalen el cliente. WickrGov Para el resto de AWS regiones, pide a tus usuarios que descarguen e instalen el cliente Wickr estándar. Para obtener más información al respecto AWS WickrGov, consulte AWS WickrGovla 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 Wickr Cat 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.

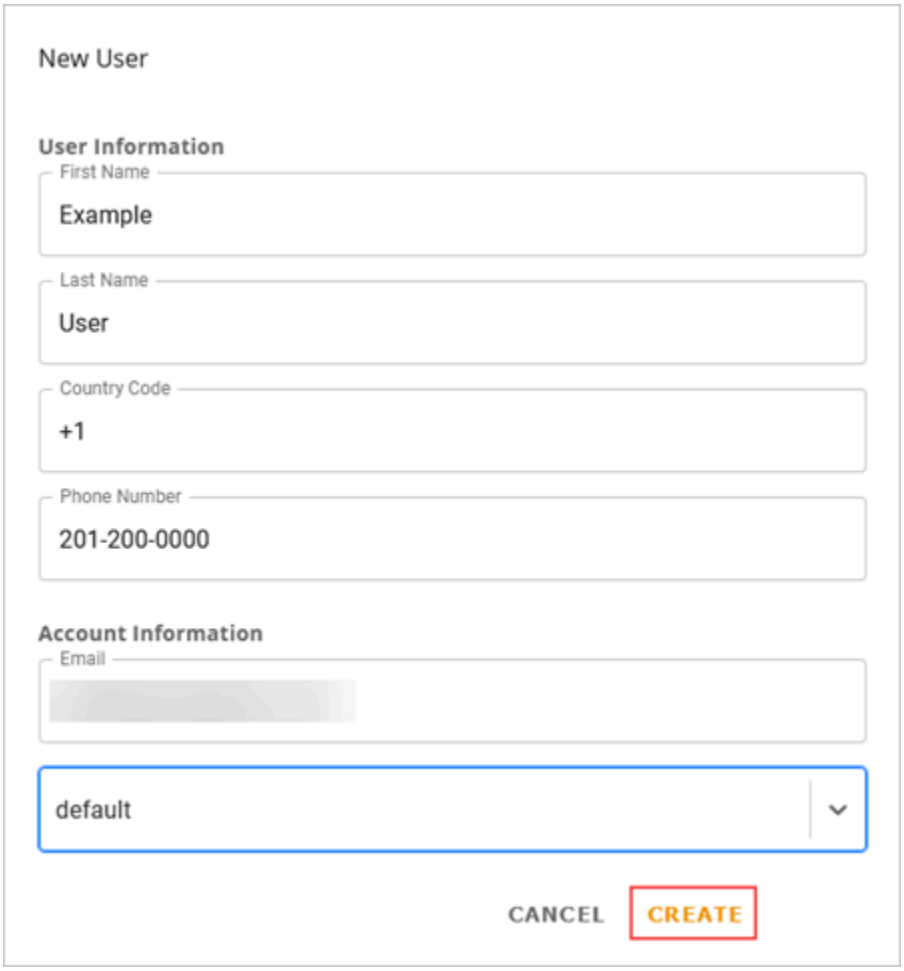


Se le redirigirá a la consola de administración de Wickr de una red específica. En la consola de administración de Wickr, puede agregar usuarios, agregar grupos de seguridad, configurarSSO, configurar la retención de datos y otros ajustes para la red específica que haya seleccionado.

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

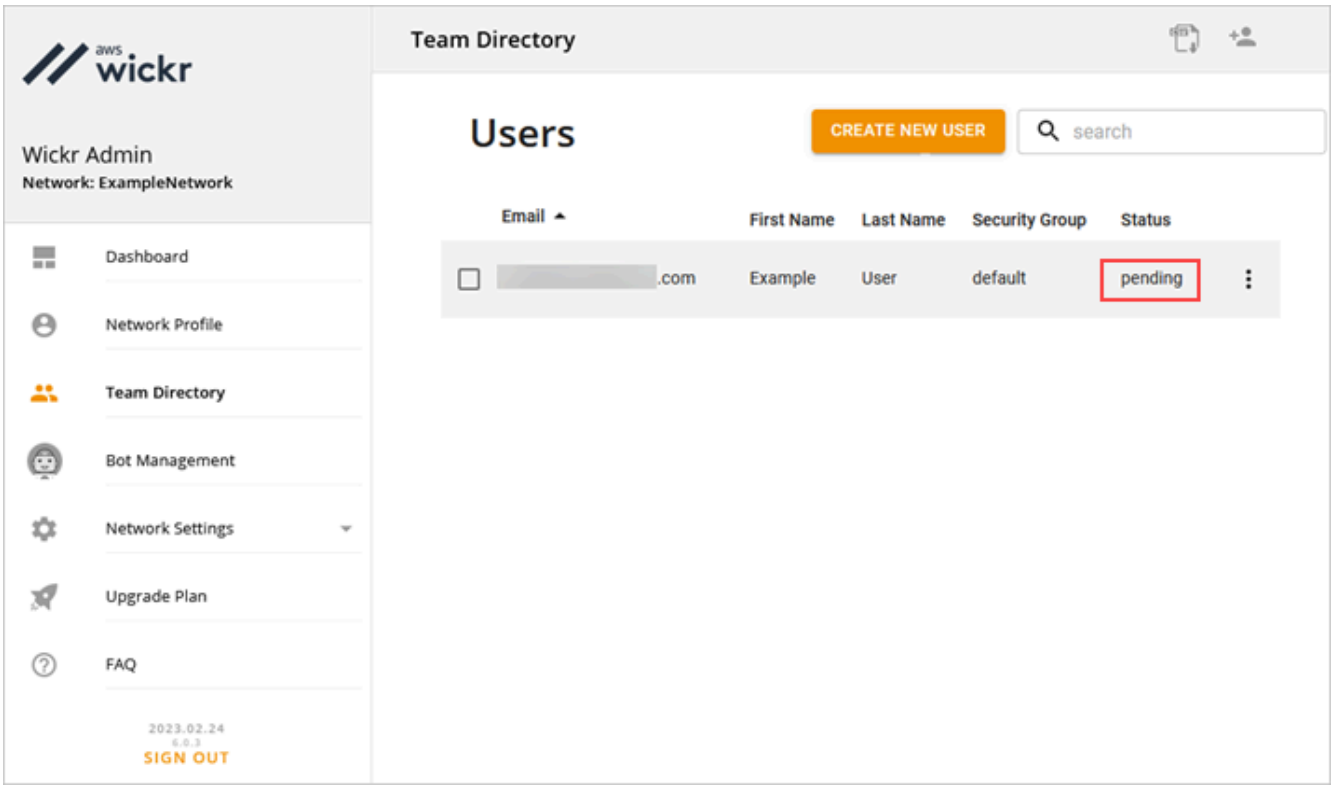
En la página Usuarios puede agregar a usuarios individuales seleccionando Crear nuevo usuario. También puede agregar a usuarios en bloque; para ello, seleccione el icono Añadir usuarios en el panel de navegación superior. Selecciona el CSV ícono de descarga para descargar una CSV plantilla que puedes editar y cargar con tu 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.



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 cómo será la experiencia del usuario final, consulta Descargar la aplicación de 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.



Siguientes pasos

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

- Administra tu red de AWS Wickr
- Cómo gestionar usuarios en AWS Wickr

Transfiere Wickr Pro a Wickr AWS

> **Note**
>
> Wickr Pro ha sido descatalogado. Si has perdido el acceso a Wickr Pro, sigue los pasos de esta guía para pasarte a Wickr. AWS

En esta guía, te mostramos cómo realizar la transferencia desde Wickr Pro y empezar a usar Wickr. AWS

Sigue los pasos de esta guía si ya tienes una red Wickr Pro, pero aún NOT tienes una. Cuenta de AWS No dude en ponerse en contacto con el servicio de asistencia en cualquier momento si necesita ayuda.

Si tu organización ya tiene una AWS cuenta, completa el formulario de migración de Wickr Pro a Wickr y el AWS equipo de soporte de AWS Wickr te ayudará.

Necesitará una Cuenta de AWS identificación 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, consulta la Guía de referencia de administración de AWS cuentas.

Temas

Paso 1: Crea una AWS cuenta

Complete el siguiente procedimiento para crear una AWS cuenta.

1. Si su organización no tiene un ID de AWS cuenta 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)
   - Selecciona 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. Configura el acceso administrativo 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 gestionada: AWSWickrFullAccess.
3. Una vez que complete los pasos anteriores, podrá iniciar sesión AWS Management Console para 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 tienes tu Cuenta de AWS ID y tu ID de red de Wickr Pro, tendrás que completar el formulario Migrar de Wickr Pro a AWS Wickr.

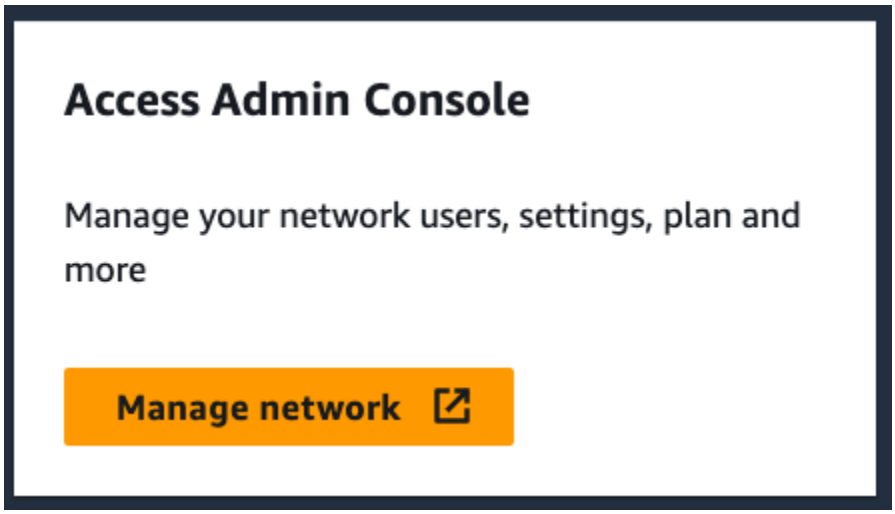
Cuando lo hayas completado, normalmente en un plazo de 14 días, un representante de soporte de AWS Wickr se pondrá en contacto contigo para confirmar que tu red de Wickr se ha añadido a la tuya. Cuenta de AWS

Paso 4: Inicia sesión en tu consola AWS

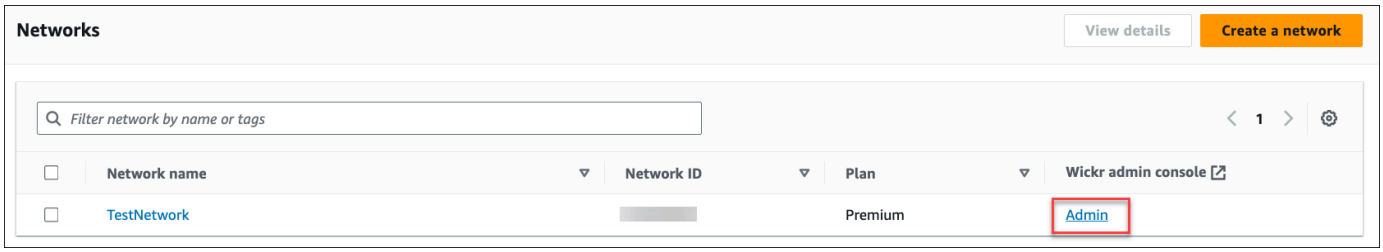
> **Note**
>
> Siga estos pasos para AFTER recibir la confirmación de que su red Wickr Pro se ha agregado a su Cuenta de AWS.

1. Puedes iniciar sesión en la AWS consola como usuario root o con un IAM usuario que hayas creado previamente (como se recomienda) en el paso 2 para AWS Wickr.
2. Navega hasta tu servicio de AWS Wickr. Puedes hacerlo desde el menú Servicios o buscando AWS Wickr en la barra de búsqueda.

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



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.



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, podrás ver y pagar tu factura a través de la AWS consola.

Administra tu red de AWS Wickr

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

Temas

Perfil de red

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

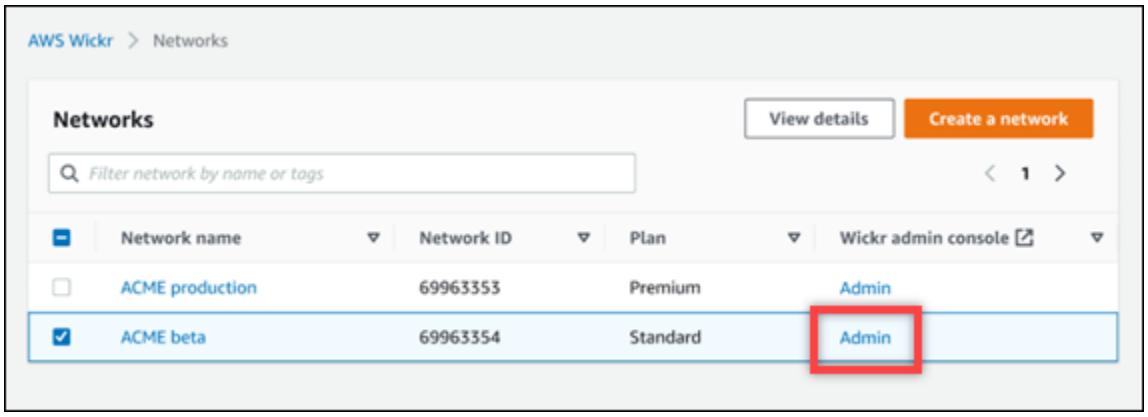
Temas

Cómo consultar el perfil de red

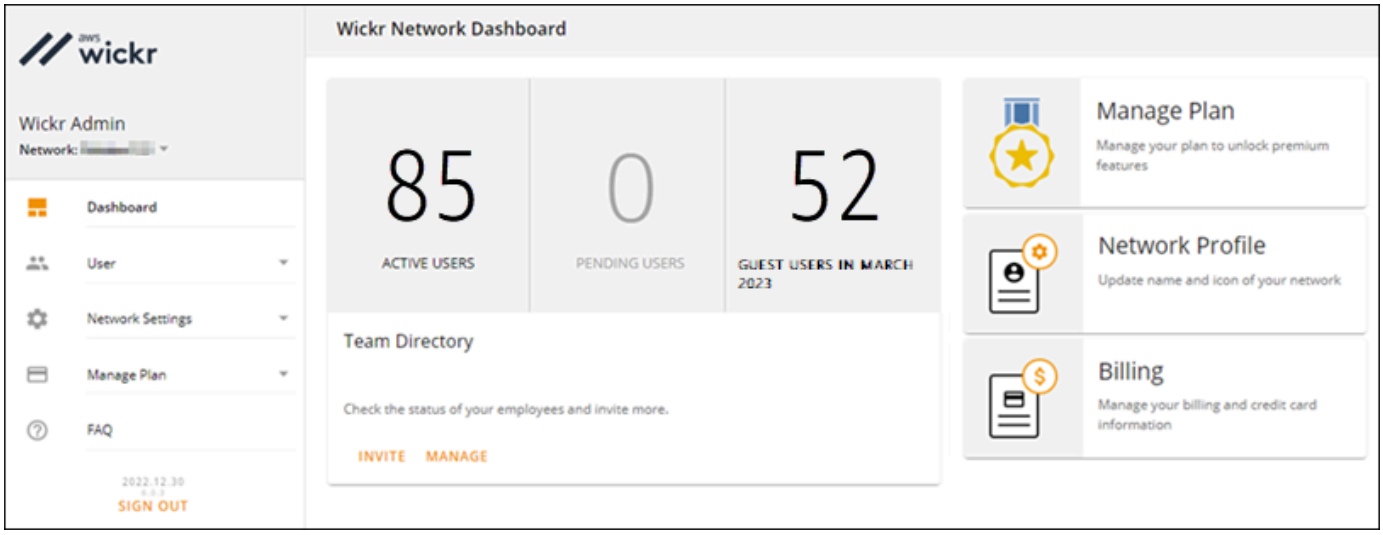
Siga el procedimiento indicado a continuación para ver el perfil de su red de Wickr y el ID de la red.

1. Abra el icono AWS Management Console para Wickr Cat. 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, elija Configuración de red y, a continuación, Perfil de red.

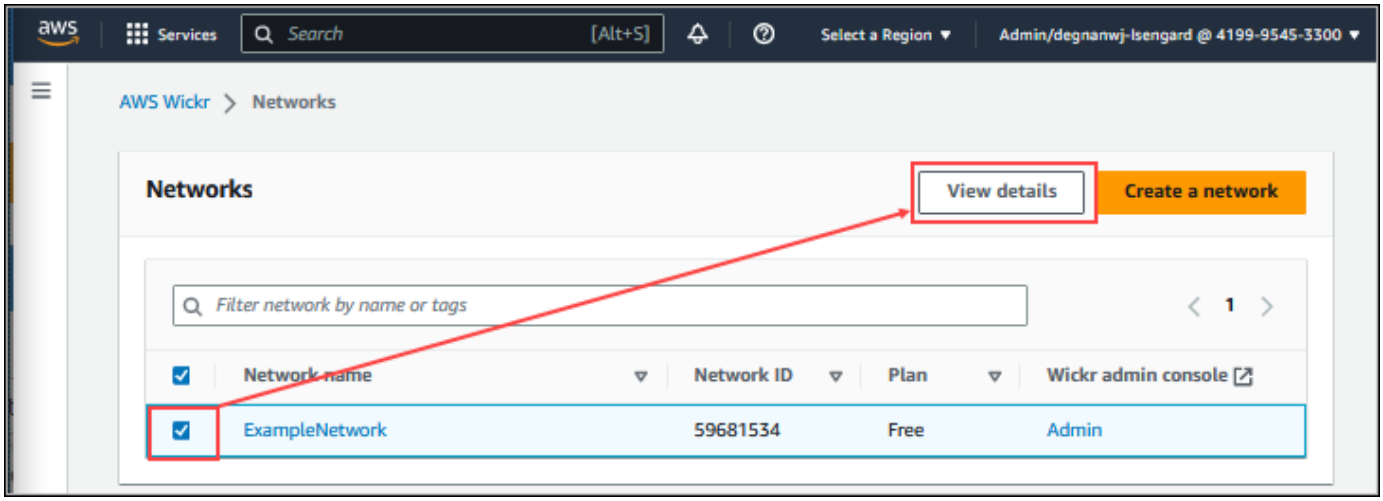
   La página Perfil de red muestra el nombre y el identificador de red de Wickr. Use el ID de red para configurar la federación.

Editar el nombre de la red

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

1. Abra el icono AWS Management Console para Wickr Cat. 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 del AWS Management Console en el caso de Wickr, puedes gestionar los grupos de seguridad y su configuración, como las políticas de complejidad de contraseñas, las preferencias de mensajería, las funciones de llamadas, las funciones de seguridad y la federación de redes.

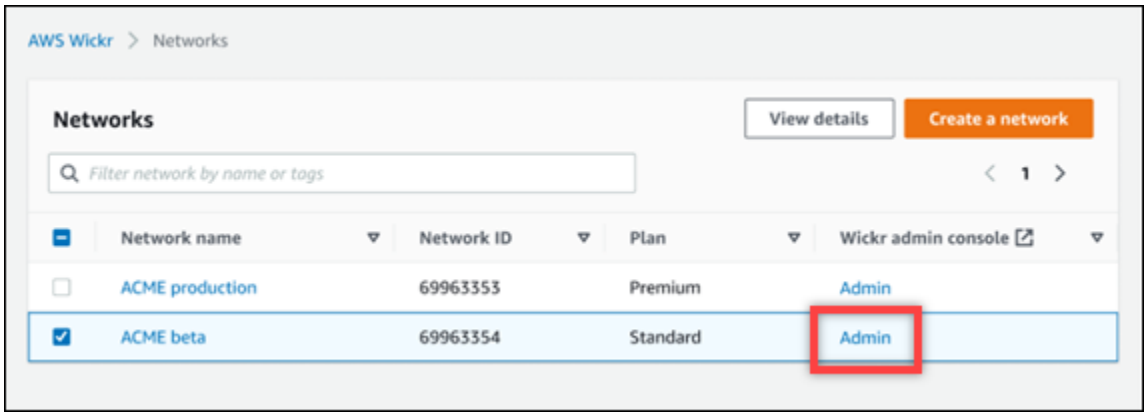
Temas

- Cómo consultar los grupos de seguridad
- Creación de un grupo de seguridad
- Cómo editar un grupo de seguridad
- Eliminación de un grupo de seguridad

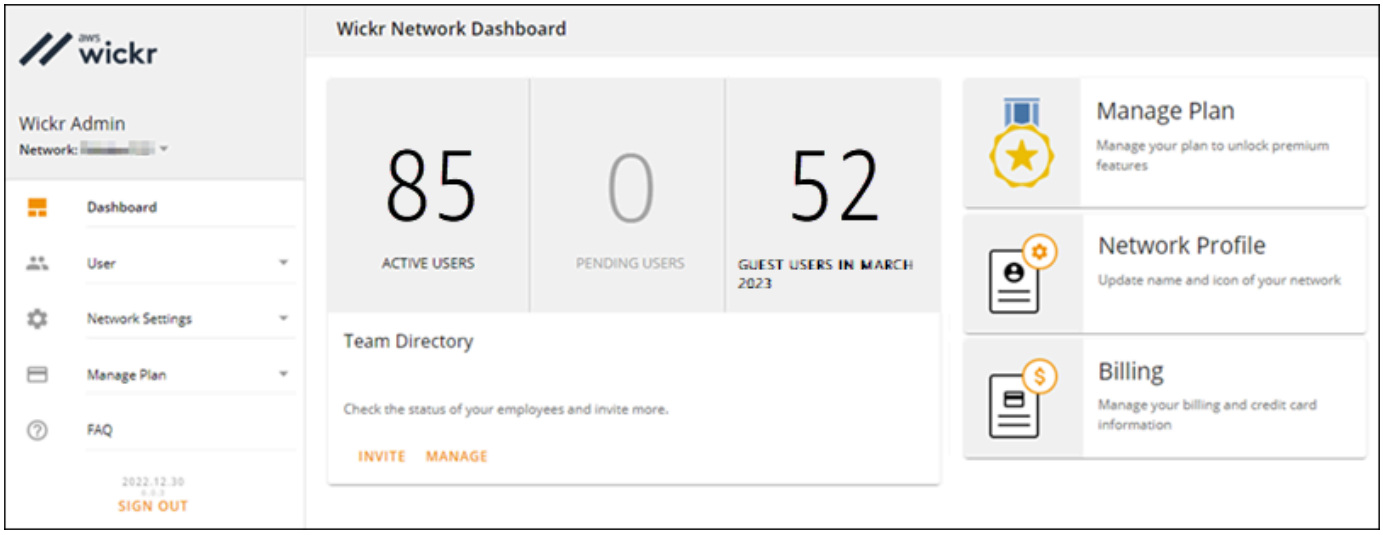
Cómo consultar los grupos de seguridad

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

1. Abra el icono AWS Management Console para Wickr Cat. 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. Abra el icono AWS Management Console para Wickr Cat. 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. Abra el icono AWS Management Console para Wickr Cat. 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. AWSWickr tiene 2 tipos de federación: local y global.
  - Federación local: la capacidad de federarse con AWS usuarios de 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 AWS usuarios de una red diferente que pertenecen 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. Abra el icono AWS Management Console para Wickr Cat. 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 SSOconfiguración del AWS Management Console en el caso de Wickr, puedes configurar Wickr para que utilice un sistema de inicio de sesión único para autenticarse. SSOproporciona un nivel de seguridad adicional cuando se combina con un sistema de autenticación multifactorial () adecuado. MFA Wickr solo es compatible con SSO los proveedores que utilizan OpenID OIDC Connect (). No se admiten los proveedores que utilizan Security Assertion Markup Language (SAML).

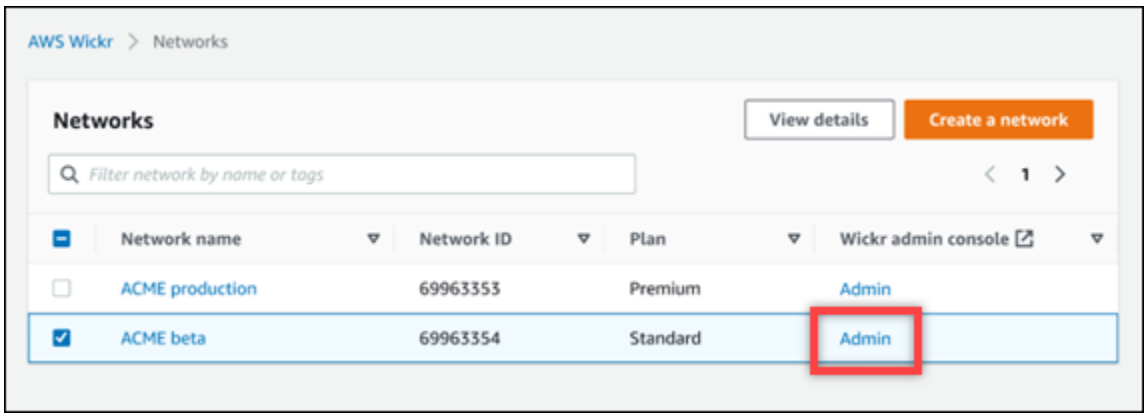
Temas

- Ver detalles SSO
- Configura SSO
- Periodo de gracia para la actualización del token
- Configurar el inicio de sesión único de Microsoft Entra (Azure AD)

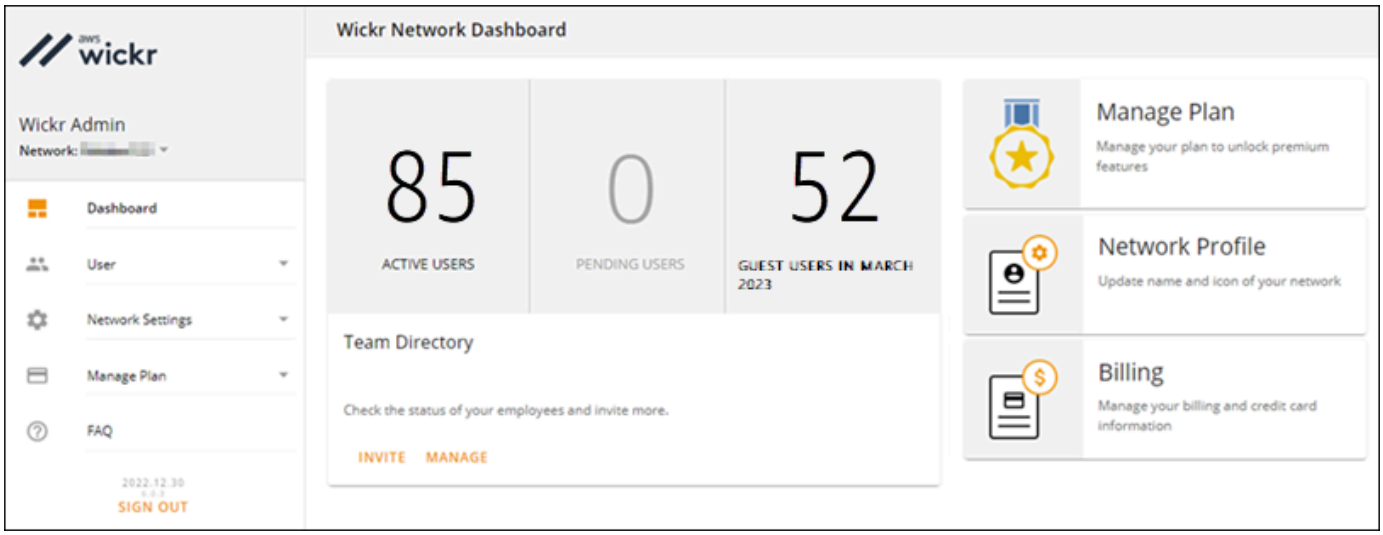
Ver detalles SSO

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. Abra el icono AWS Management Console para Wickr Cat. 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, selecciona Configuración de red y, a continuación, Configuración. SSO

   La página de inicio de sesión y LDAP configuración únicos muestra tu terminal de red de Wickr y la configuración actual. SSO

Configura SSO

Para obtener más información sobre la configuraciónSSO, consulte las siguientes guías:

> **Important**
>
> Cuando configurasSSO, especificas un ID de empresa para tu red 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.

- Configurar el inicio de sesión único de Microsoft Entra (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.

Configurar el inicio de sesión único de Microsoft Entra (Azure AD)

AWSWickr se puede configurar para usar Microsoft Entra (Azure AD) como proveedor de identidades. Para ello, complete los siguientes procedimientos tanto en Microsoft Entra como en la consola de administración de AWS Wickr.

Warning

Una vez SSO activado en una red, cerrará la sesión de los usuarios activos en Wickr y los obligará a volver a autenticarse con el proveedor. SSO

Paso 1: Registra AWS Wickr como una aplicación en Microsoft Entra

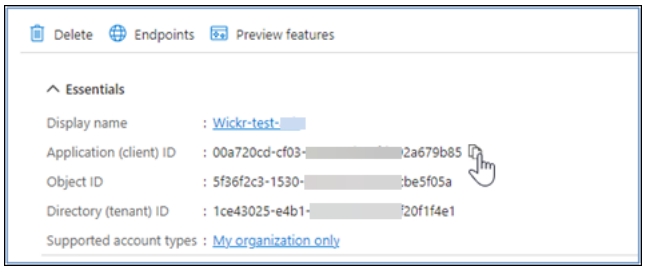
Complete el siguiente procedimiento para registrar AWS Wickr como una aplicación en Microsoft Entra.

> **Note**
>
> Consulte la documentación de Microsoft Entra para obtener capturas de pantalla detalladas y solucionar problemas. Para obtener más información, consulte Registrar una aplicación en la plataforma de identidad de Microsoft

1. En el panel de navegación, elija Aplicaciones y, a continuación, Registros de aplicaciones.
2. En la página de registros de aplicaciones, elija Registrar una aplicación y, a continuación, introduzca el nombre de la aplicación.
3. Seleccione solo las cuentas de este directorio organizativo (solo en el directorio predeterminado: arrendatario único).
4. En Redirigir URI, selecciona Web y, a continuación, introduce la siguiente dirección web:`https://messaging-pro-prod.wickr.com/deeplink/oidc.php`.

   > **Note**
   >
   > El redireccionamiento también se URI puede copiar desde los ajustes de SSO configuración de la consola de administración de AWS Wickr.

5. Elija Registro.
6. Después del registro, copia/guarda el ID de la aplicación (cliente) generado.



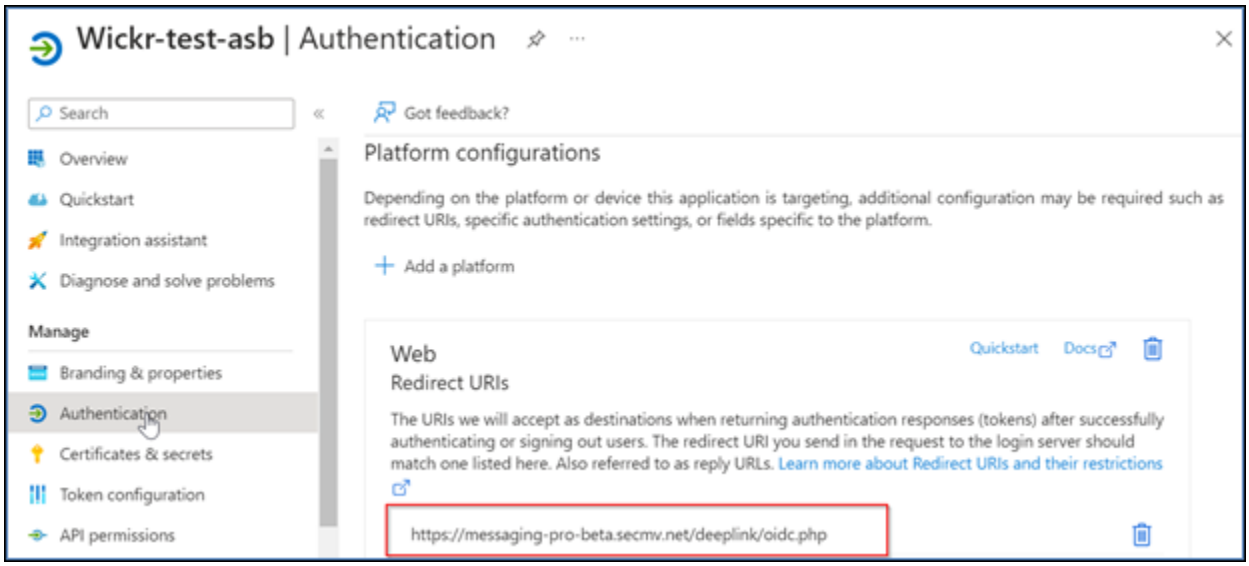
7. Seleccione la pestaña Endpoints para tomar nota de lo siguiente:

1. Punto final de autorización de Oauth 2.0 (v2): Por ejemplo: `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/oauth2/v2.0/authorize`
2. Edita este valor para eliminar «oauth2/» y «autorizar». Por ejemplo, fijo URL tendrá este aspecto: `https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`
3. Se hará referencia a esto como el SSOEmisor.

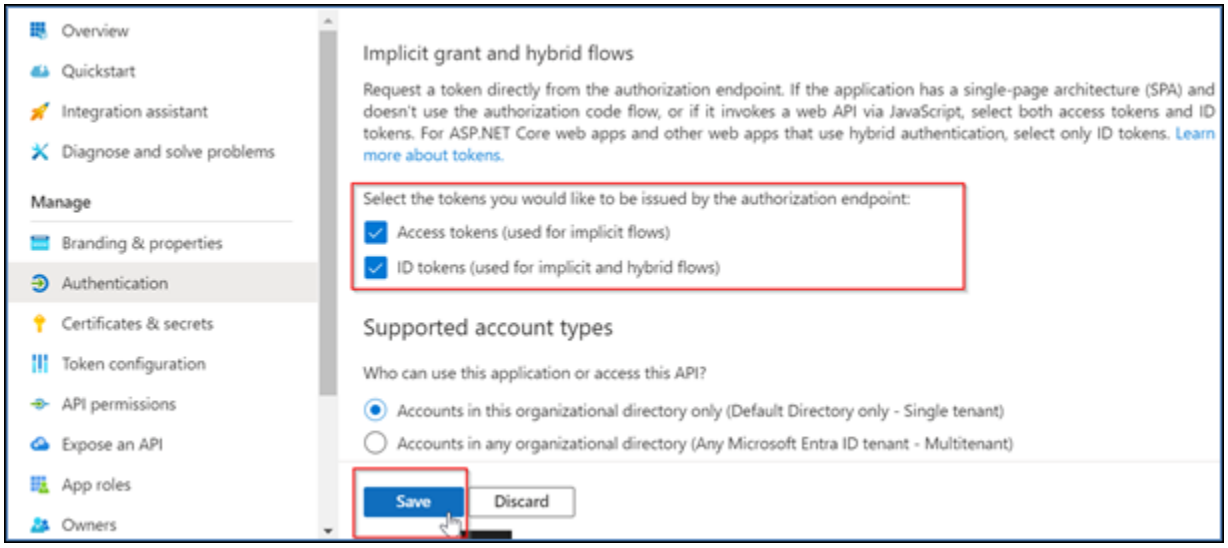
Paso 2: Configurar la autenticación

Complete el siguiente procedimiento para configurar la autenticación en Microsoft Entra.

1. En el panel de navegación, elija Autenticación.
2. En la página de autenticación, asegúrate de que el redireccionamiento web URI sea el mismo que el introducido anteriormente (en Registrar AWS Wickr como aplicación).



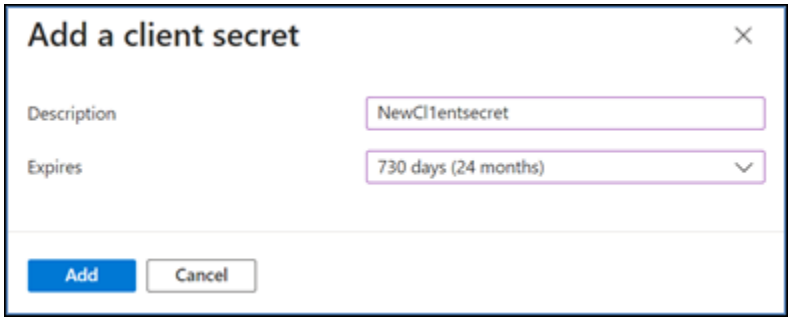
3. Seleccione los tokens de acceso que se utilizan para los flujos implícitos y los tokens de ID que se utilizan para los flujos implícitos e híbridos.
4. Seleccione Guardar.



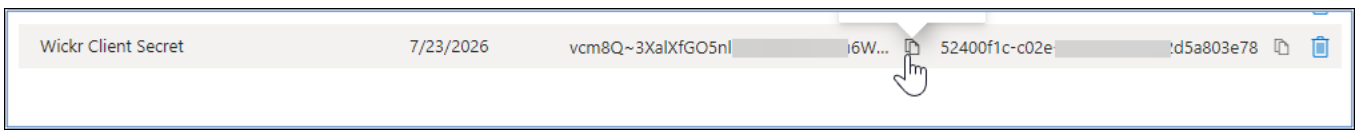
Paso 3: Configurar certificados y secretos

Complete el siguiente procedimiento para configurar los certificados y secretos en Microsoft Entra.

1. En el panel de navegación, elija Certificados y secretos.
2. En la página Certificados y secretos, seleccione la pestaña Secretos del cliente.
3. En la pestaña Secretos del cliente, selecciona Nuevo secreto de cliente.
4. Introduce una descripción y selecciona un período de caducidad para el secreto.
5. Elija Añadir.



6. Una vez creado el certificado, copie el valor secreto del cliente.

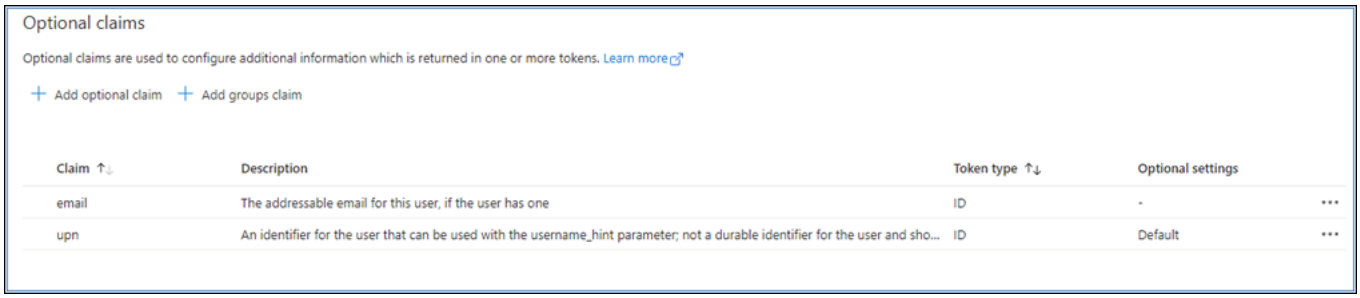


> **Note**
>
> Se necesitará el valor secreto del cliente (no el identificador secreto) para el código de la aplicación cliente. Es posible que no pueda ver ni copiar el valor secreto después de salir de esta página. Si no lo copias ahora, tendrás que volver a crear un nuevo secreto de cliente.

Paso 4: Configurar la configuración del token

Complete el siguiente procedimiento para configurar el token en Microsoft Entra.

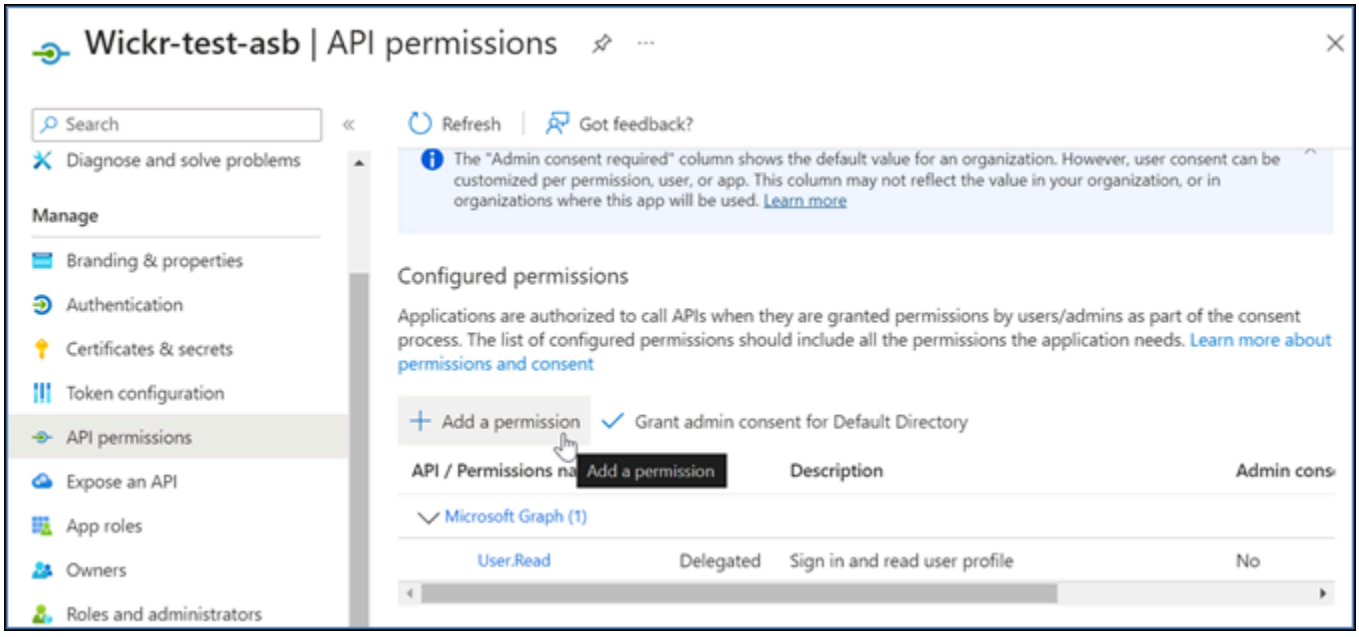
1. En el panel de navegación, elija la configuración del token.
2. En la página de configuración del token, selecciona Añadir reclamación opcional.
3. En Reclamaciones opcionales, selecciona el tipo de token como ID.
4. Después de seleccionar el ID, en Reclamar, selecciona correo electrónico y nombre de usuario.
5. Elija Añadir.



Paso 5: Configurar API los permisos

Complete el siguiente procedimiento para configurar API los permisos en Microsoft Entra.

1. En el panel de navegación, seleccione APIlos permisos.
2. En la página de APIpermisos, elija Añadir un permiso.

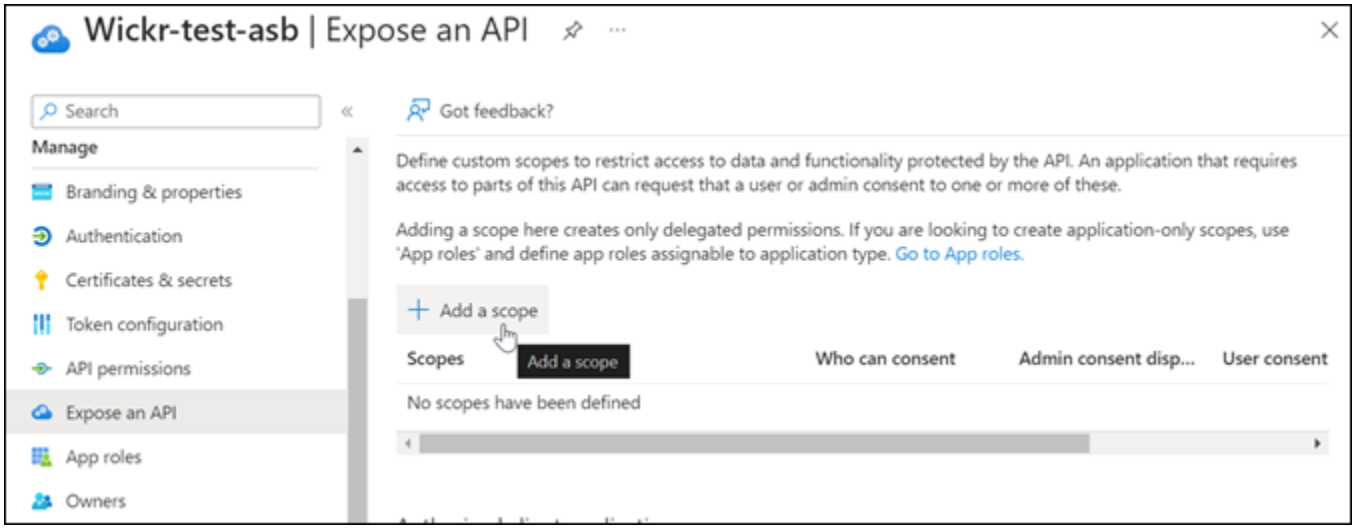


3. Seleccione Microsoft Graph y, a continuación, seleccione Permisos delegados.
4. Selecciona la casilla de verificación de email, offline_access, openid o profile.
5. Elija Añadir permisos.

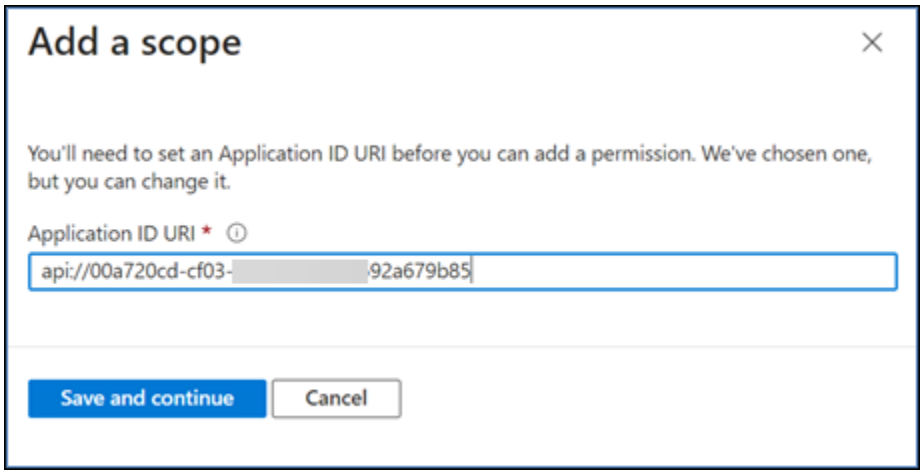
Paso 6: Exponer un API

Complete el siguiente procedimiento para exponer una API para cada uno de los 4 ámbitos de Microsoft Entra.

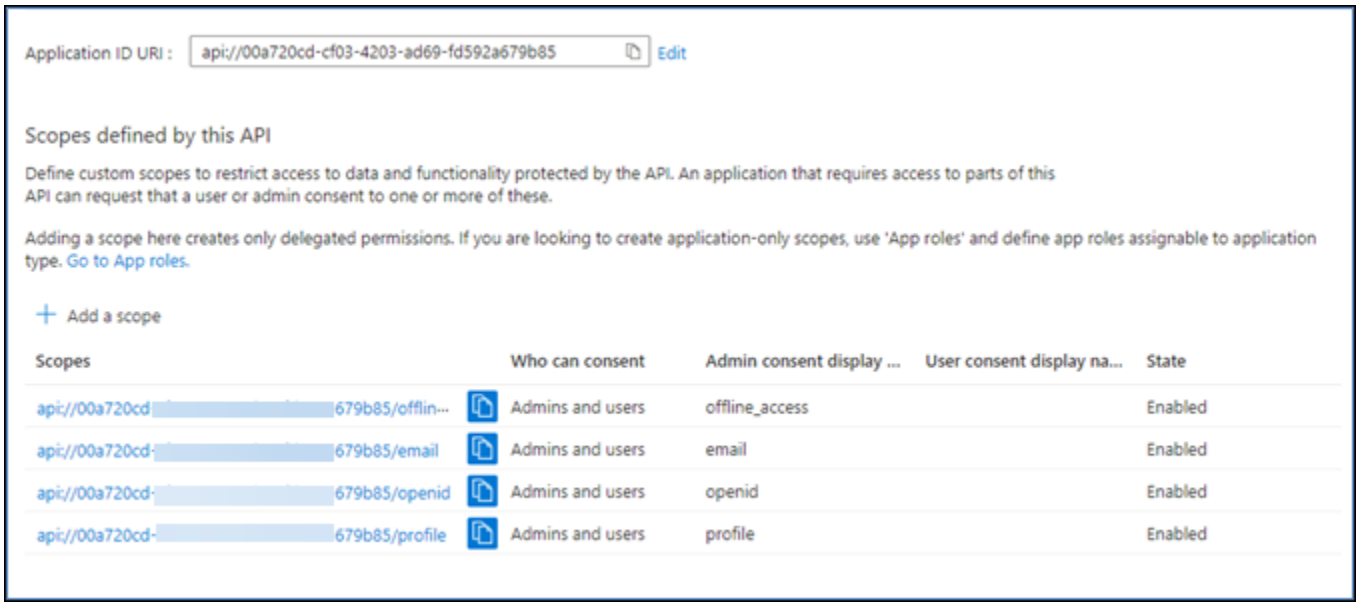
1. En el panel de navegación, elija Exponer un API.
2. En la API página Exponer un ámbito, elija Añadir un ámbito.



El ID de la aplicación URI debe rellenarse automáticamente y el ID que le sigue URI debe coincidir con el ID de la aplicación (creado en Register AWS Wickr como una aplicación).



3. Elija Guardar y continuar.
4. Seleccione la etiqueta Administradores y usuarios y, a continuación, introduzca el nombre del ámbito como offline_access.
5. Selecciona Estado y, a continuación, selecciona Activar.
6. Selecciona Añadir ámbito.
7. Repita los pasos 1 a 6 de esta sección para añadir los siguientes ámbitos: correo electrónico, openid y perfil.



8. En Aplicaciones cliente autorizadas, elija Agregar una aplicación cliente.
9. Seleccione los cuatro ámbitos creados en el paso anterior.

10. Introduzca o verifique el ID de la aplicación (cliente).
11. Elija Agregar aplicación.

Paso 7: Configuración de AWS Wickr SSO

Complete el siguiente procedimiento de configuración en la consola de AWS Wickr.

1. Abra el icono AWS Management Console para Wickr Cat. 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, selecciona Configuración de red y, a continuación, Configuración. SSO
4. En Network Endpoint, asegúrate de que la redirección URI coincida con la siguiente dirección web (que se agregó en el paso 4 en Registrar AWS Wickr como aplicación).

   `https://messaging-pro-prod.wickr.com/deeplink/oidc.php`.
5. En SSOConfiguración, selecciona Iniciar
6. Escriba la información siguiente:

   - SSOEmisor: este es el punto final que se modificó anteriormente (por ejemplo`https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`).
   - SSOID de cliente: es el ID de la aplicación (cliente) del panel de información general.
   - ID de empresa: puede ser un valor de texto único que incluya caracteres alfanuméricos y de subrayado. Esta frase es la que introducirán los usuarios cuando se registren en dispositivos nuevos.
   - Secreto del cliente: es el secreto del cliente que aparece en el panel de certificados y secretos.
   - Ámbitos: son los nombres de los ámbitos que aparecen en el API panel Exponer un objeto. Introduzca el correo electrónico, el perfil, offline_access y openid.
   - Ámbito de nombre de usuario personalizado: introduzca upn.

   Los demás campos son opcionales.
7. Seleccione Probar y guardar.
8. Seleccione Guardar.

SSOla configuración está completa. Para comprobarlo, ahora puede añadir un usuario a la aplicación en Microsoft Entra e iniciar sesión con el usuario con SSO un ID de empresa.

Para obtener más información sobre cómo invitar e incorporar usuarios, consulte Crear e invitar usuarios.

Resolución de problemas

A continuación, se muestran los problemas más comunes que pueden surgir y sugerencias para resolverlos.

- SSOLa prueba de conexión falla o no responde:
  - Asegúrese de que el SSOemisor esté configurado según lo esperado.
  - Asegúrese de que los campos obligatorios de la sección Configurado estén SSOconfigurados como se esperaba.
- La prueba de conexión se ha realizado correctamente, pero el usuario no puede iniciar sesión:
  - Asegúrese de que el usuario esté agregado a la aplicación Wickr que registró en Microsoft Entra.
  - Asegúrese de que el usuario utiliza el identificador de empresa correcto, incluido el prefijo. P.ej. UE1- DemoNetwork w_Drqtva.
  - Es posible que el secreto del cliente no esté configurado correctamente en la configuración de Wickr. AWS SSO Vuelva a configurarlo creando otro secreto de cliente en Microsoft Entra y establezca el nuevo secreto de cliente en la configuración de Wickr. SSO

Lea 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. Abra el icono AWS Management Console para Wickr Cat. 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

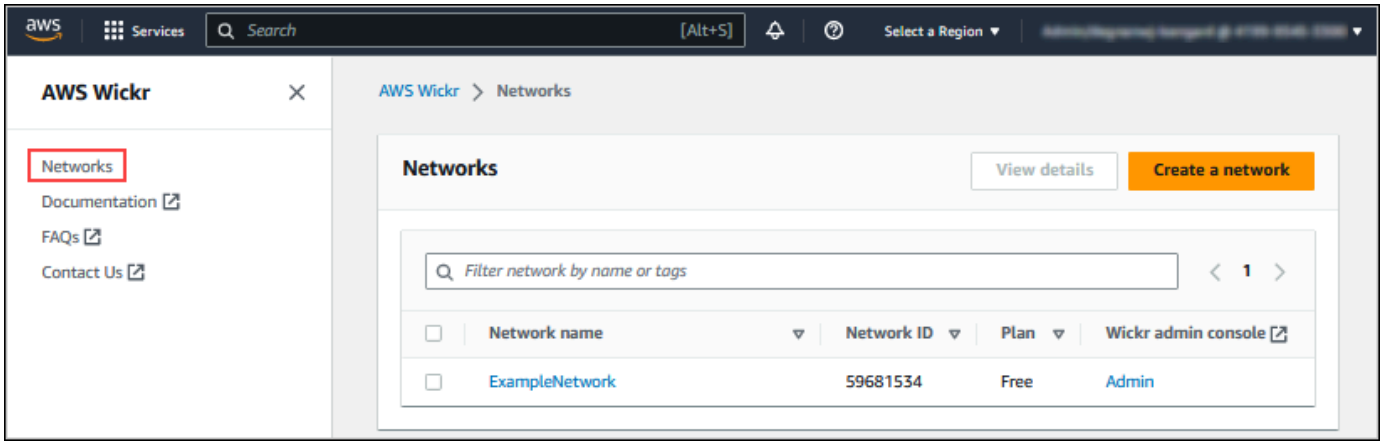
Es posible aplicar etiquetas a las redes de Wickr, Luego puedes usar esas etiquetas para buscar y filtrar tus redes de Wickr o rastrear tus AWS costos. Puede configurar las etiquetas de red en la página de descripción general de la red del AWS Management Console para Wickr.

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.

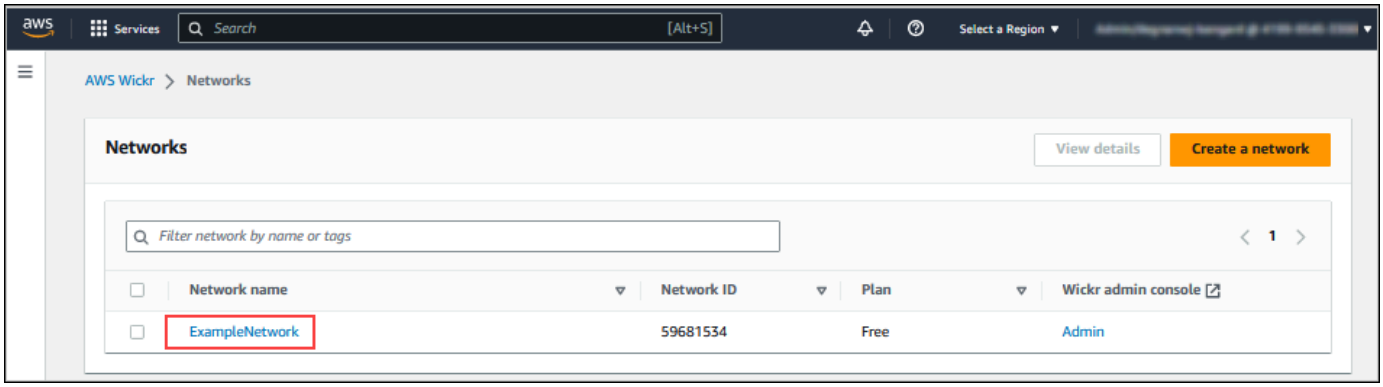
Cómo administrar las etiquetas de red

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

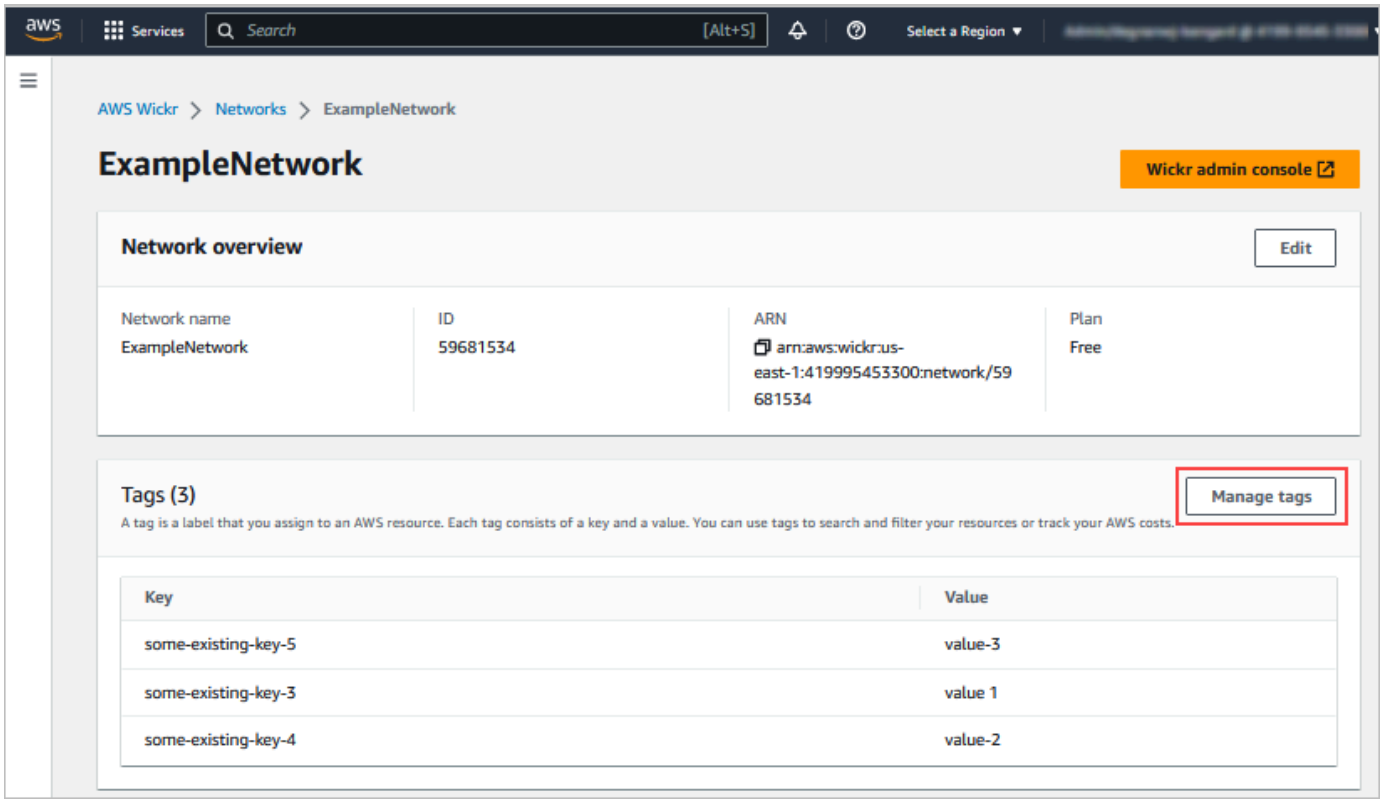
1. Abra el icono AWS Management Console para Wickr Cat. https://console.aws.amazon.com/wickr/
2. Seleccione Redes en el panel de navegación del AWS Management Console para Wickr.



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:

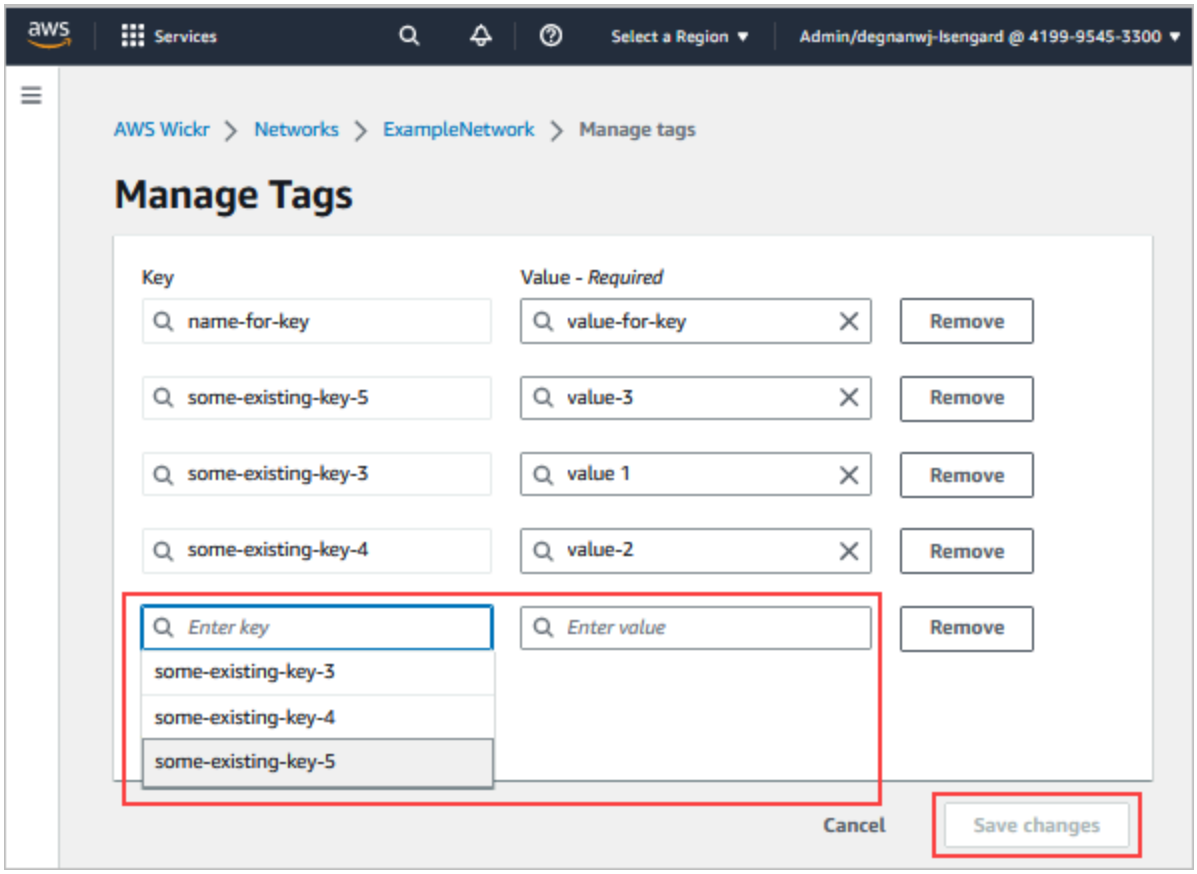
   - Agregar etiquetas nuevas: escriba nuevas etiquetas en forma de pares clave-valor. Seleccione Agregar nueva etiqueta para añadir varios pares clave-valor. Las etiquetas distinguen entre mayúsculas y minúsculas. Para obtener más información, consulte Cómo agregar etiquetas de red.
   - Editar las etiquetas 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.

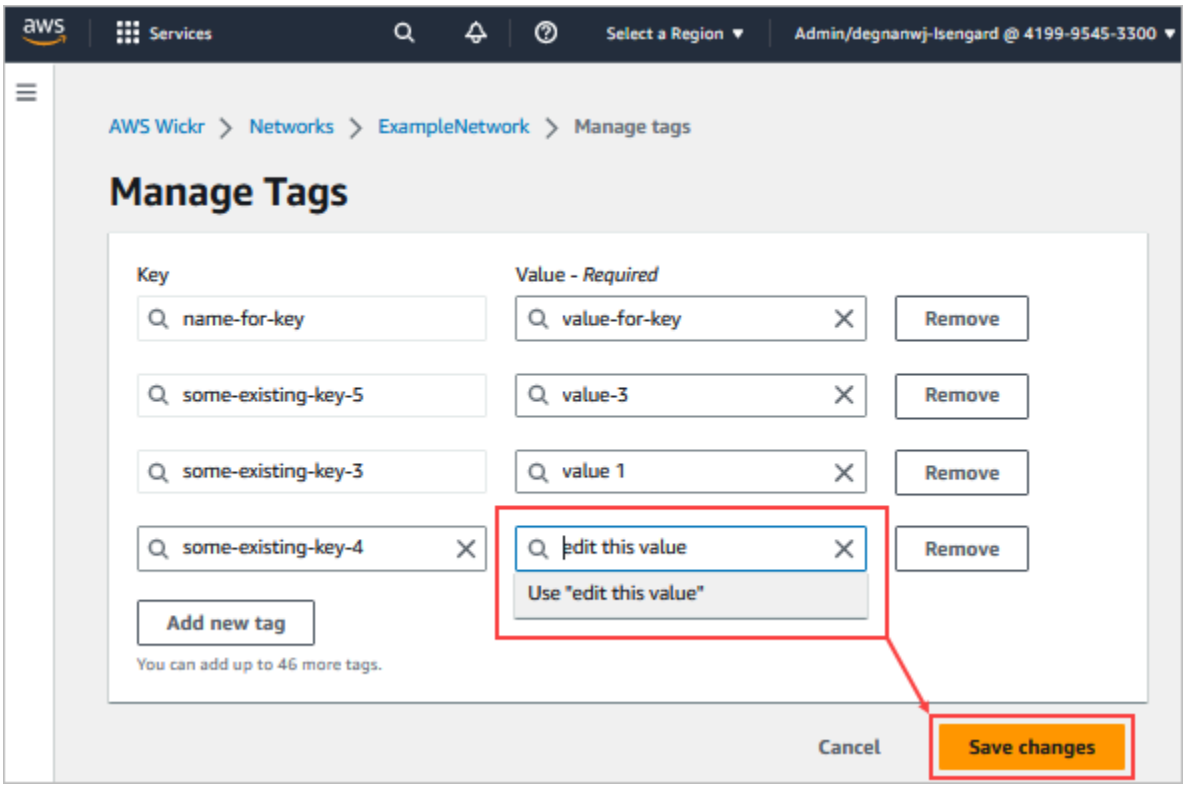


Cómo modificar las etiquetas de red

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.

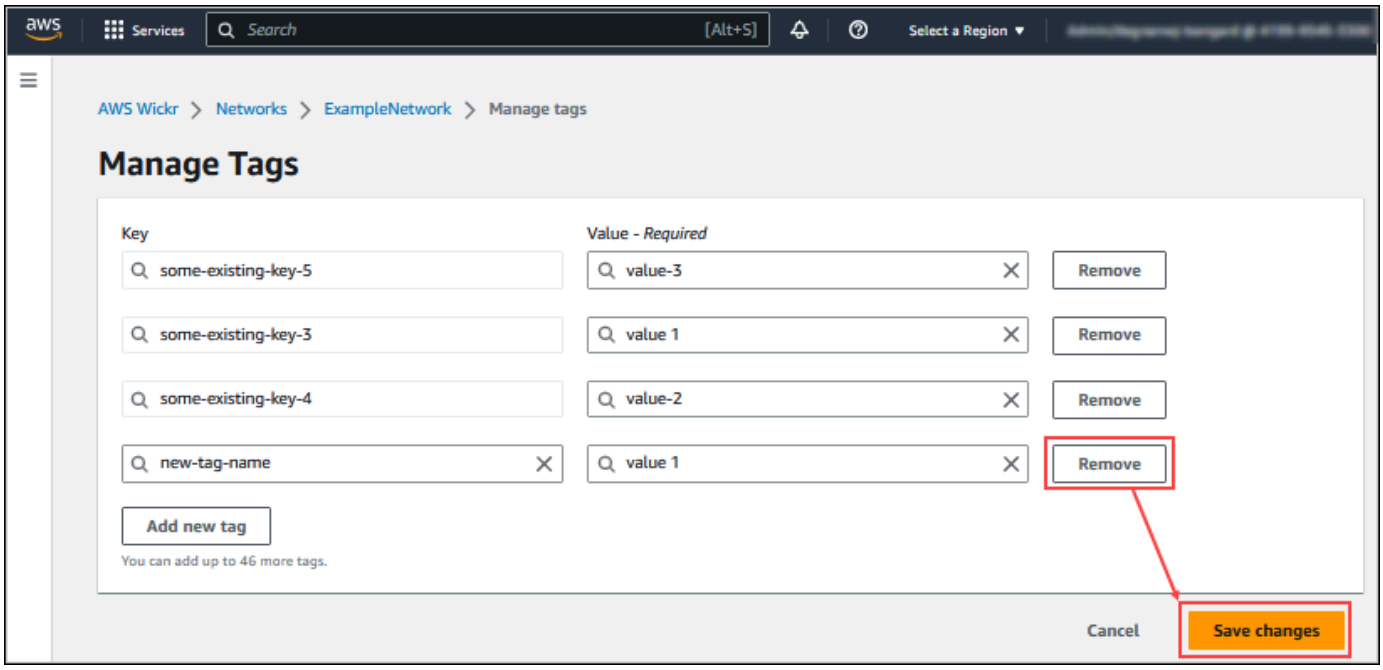


2. Elija Guardar cambios para guardar las modificaciones.

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 plan de la AWS Management Console para Wickr, puede administrar su plan de red en función de las necesidades de su empresa.

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

1. Abra el icono AWS Management Console para Wickr Cat. 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 una red para cada AWS la cuenta se puede inscribir en una versión de 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

AWSLa retención de datos de Wickr puede conservar todas las conversaciones de 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 opten por 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

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 icono AWS Management Console para Wickr Cat. 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

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_MESGDEST`: 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 de Amazon Simple Notification Service (AmazonSNS) que actualmente admite la versión 5.116 del bot de retención de datos de AWS Wickr.

Temas

- CloudWatch métricas
- SNSEventos de Amazon

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

Métrica	Descripción
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.
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.

Dimensión	Valor
Producto	El producto para el bot. Puede ser `WickrPro_` o `WickrEnterprise_` con `Alpha`, `Beta` o `Production` anexado.
BotType	El tipo de bot. Etiquetado como Conformidad para los bots de conformidad.
Network	El ID de la red asociada.

SNSEventos de Amazon

Los siguientes eventos se publican en el SNS tema de Amazon definido por el valor Amazon Resource Name (ARN) identificado mediante la variable de `WICKRIO_SNS_TOPIC_ARN` entorno o el valor secreto de `sns_topic_arn` Secrets Manager. 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 JSON cadenas. En los eventos se incluyen los valores siguientes a partir de la versión 5.116 del bot de retención de datos.

Nombre	Valor
complianceBot	El nombre de usuario del bot de retención de datos.
dataTime	La fecha y hora en que se produjo el evento.
device	La descripción del dispositivo o instancia del bot específico. Es útil si se ejecutan varias instancias de bot.
dockerImage	La imagen de Docker asociada al bot.
dockerTag	La etiqueta o versión de la imagen de Docker.

Nombre	Valor
message	El mensaje del evento. Para obtener más información, consulte Eventos críticos y Eventos normales.
notificationType	Este valor será `Bot Event`.
severity	La gravedad del evento. Puede ser `normal` o `critical`.

Debes suscribirte al SNS tema de Amazon 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 `config.wickr` es incorrecta.
provisioning	No se puede leer el archivo `config.wickr` .
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	W: ickrIOClient Principal: slotAdminUser Suspender: código (%1): motivo: %2»
BotDevice Suspendido	El dispositivo está suspendido.
WatchDog	El SwitchBoard sistema ha estado inactivo durante más de <*N*El sistema ha estado inactivo durante más de unos minutos
Errores de S3	No se pudo colocar el archivo <*file-name* ≫ en un depósito S3. Error: <*AWS-error* >
Clave Fallback (alternativa)	SERVERSUBMIITEDFALLBACKKEY: No es una clave alternativa activa reconocida por

Tipo de evento	Mensajes de los eventos
	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 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

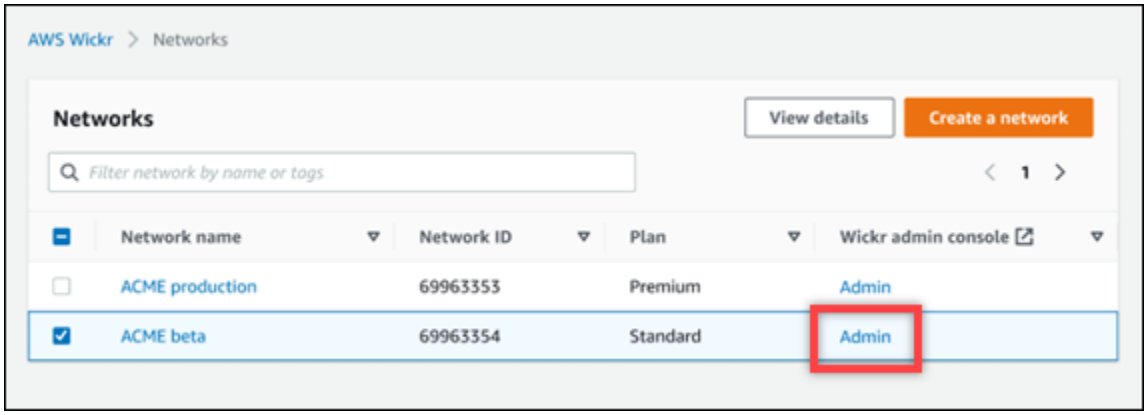
AWS Wickr es compatible con muchas agencias que utilizan Android Tactical Assault Kit (ATAK). Sin embargo, hasta ahora, los operadores de ATAK que utilizan Wickr han tenido que salir de la aplicación para poder hacerlo. Para ayudar a reducir las interrupciones y el riesgo operativo, Wickr ha desarrollado 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.

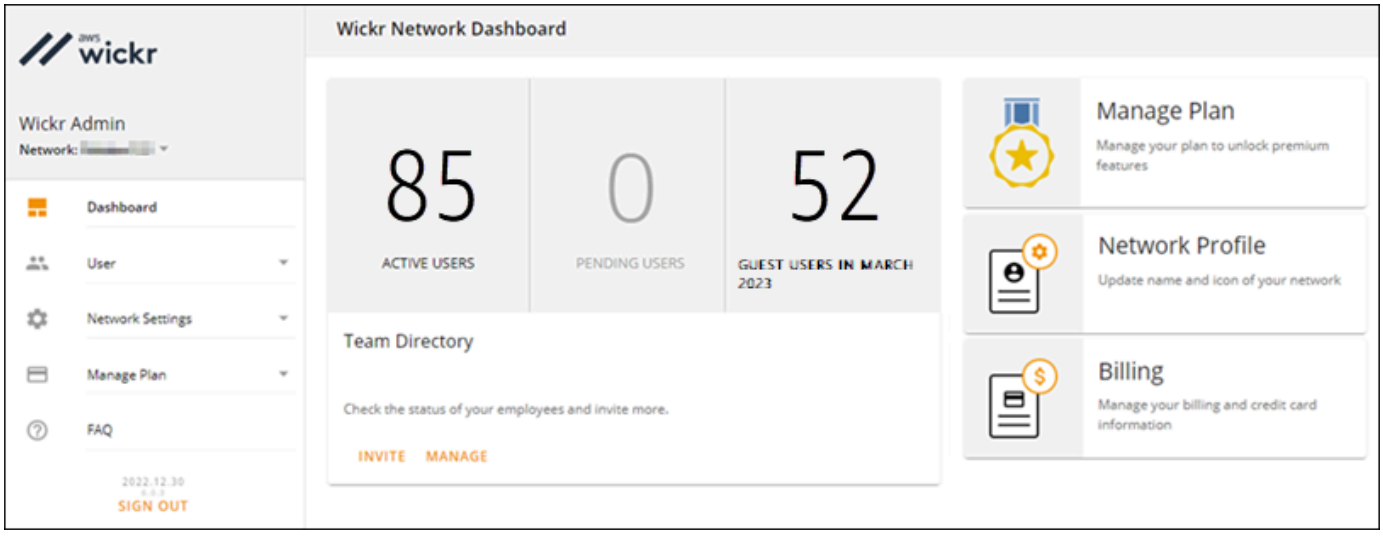
Cómo habilitar ATAK en el panel de la red de Wickr

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.

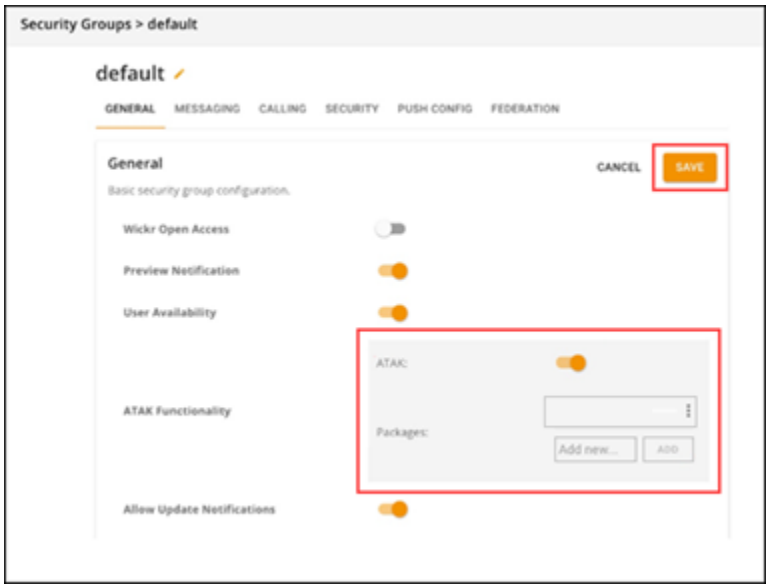
6. En la sección Funcionalidad de ATAK:

   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).

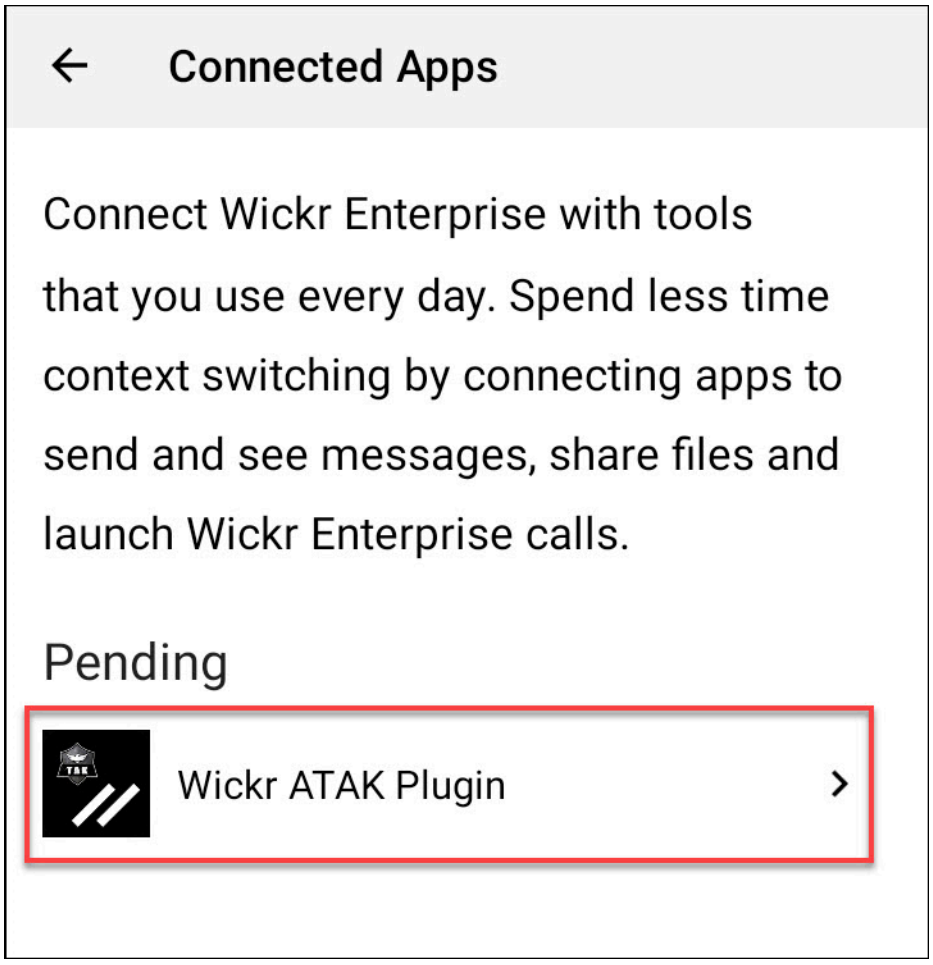
El complemento de Wickr para ATAK ya está instalado. Siga a la sección Emparejar ATAK con Wickr para completar el proceso.

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.

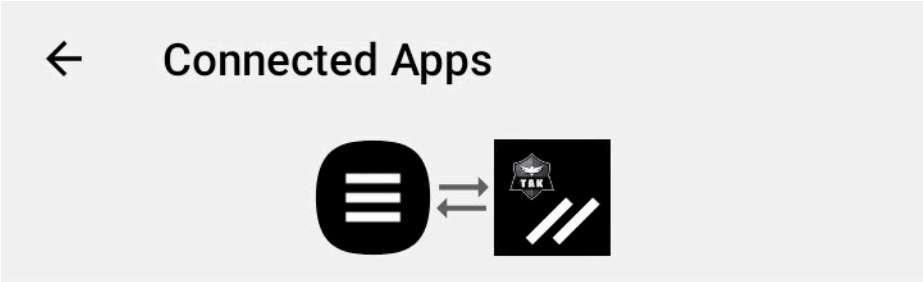
1. En la aplicación ATAK, seleccione el icono de menú () en la parte superior derecha de la pantalla y, a continuación, Complemento de Wickr.
2. Elija Vincular Wickr.

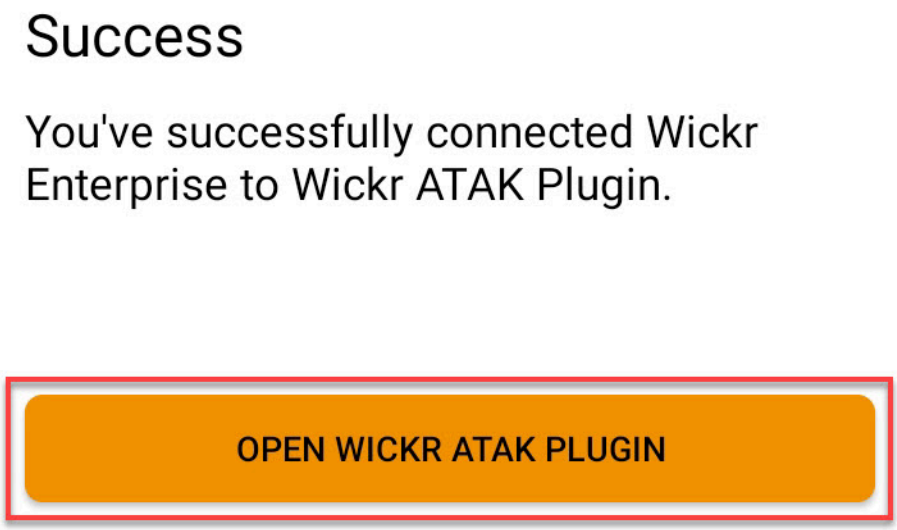
   Aparecerá un mensaje de notificación pidiéndole que revise los permisos del complemento de Wickr para ATAK. En caso contrario, abra el cliente Wickr y vaya a Ajustes y, a continuación, a Aplicaciones conectadas. Debería ver el complemento en la sección Pendiente de la pantalla.



3. Seleccione Aprobar para vincularlo.

4. Selecciona el botón Abrir complemento de Wickr ATAK para volver a la aplicación ATAK.



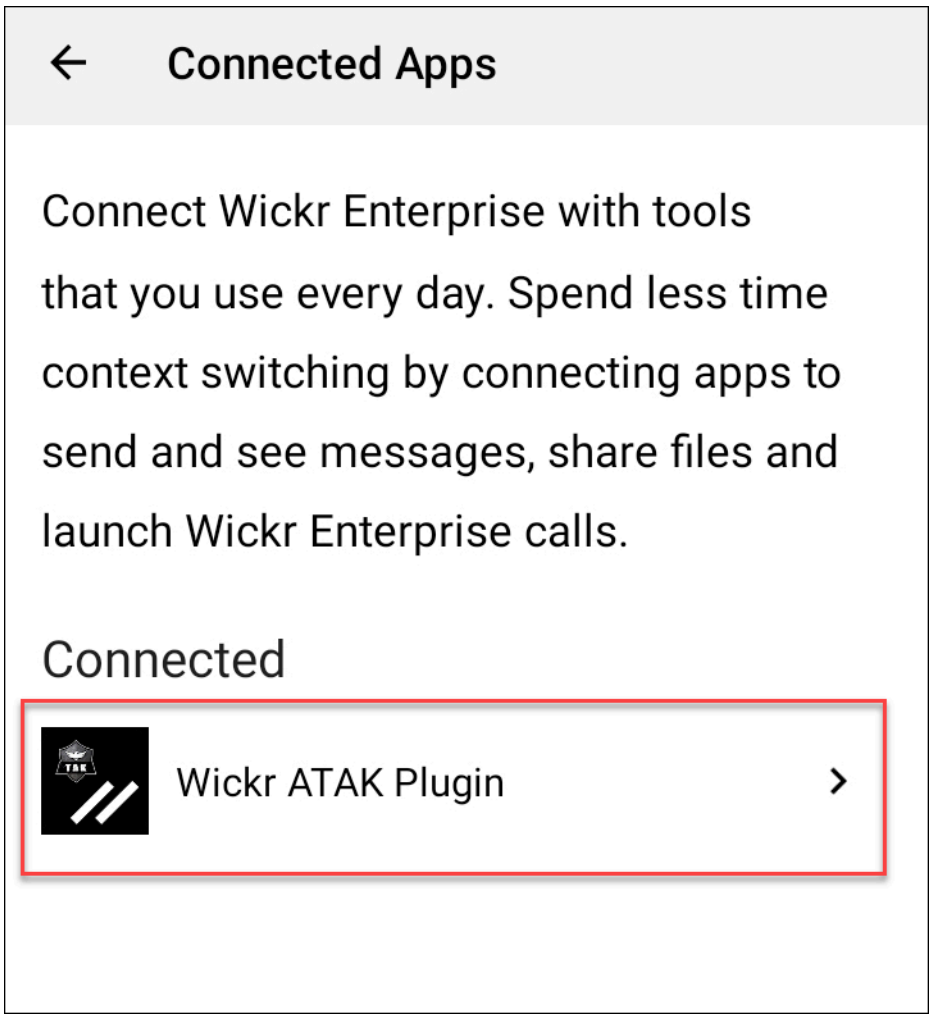


Se ha vinculado correctamente el complemento ATAK y Wickr; ya puede usarlo para enviar mensajes y colaborar con Wickr sin salir de la aplicación ATAK.

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.

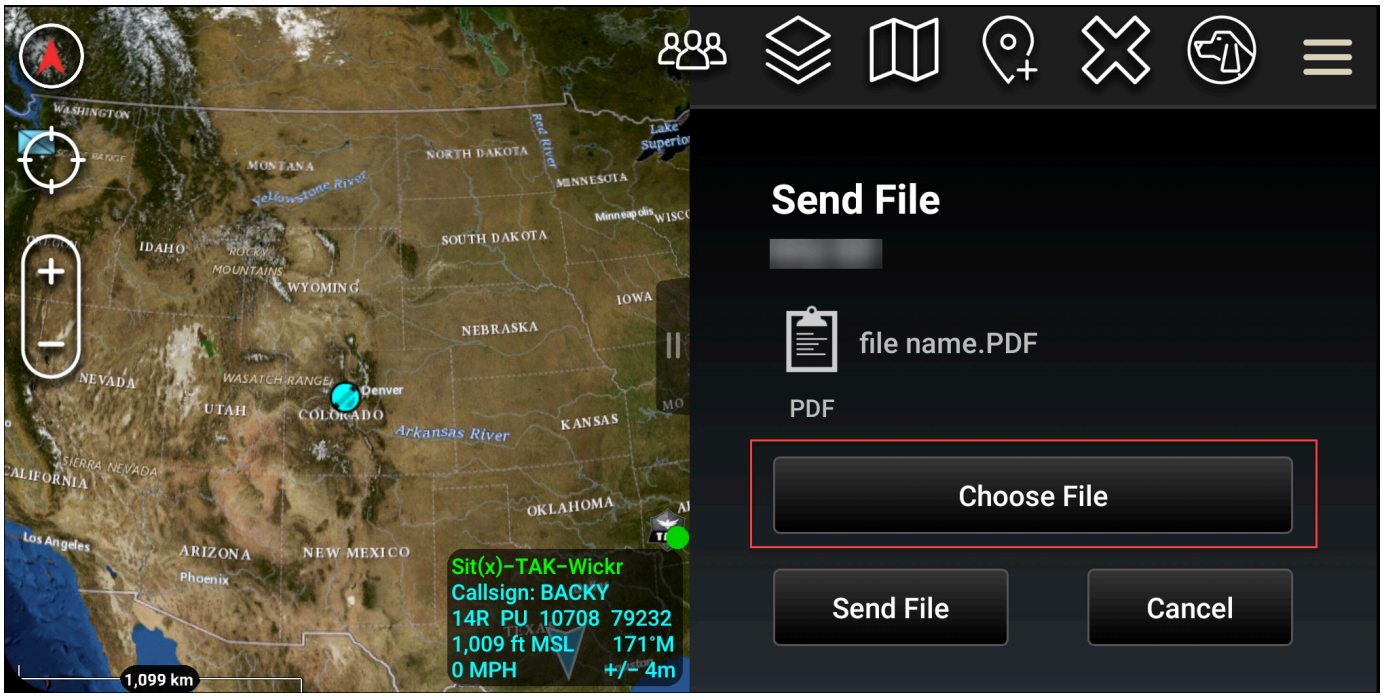
4. Una vez conectado, puede volver a la vista del complemento ATAK y recibir una llamada.

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.

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



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

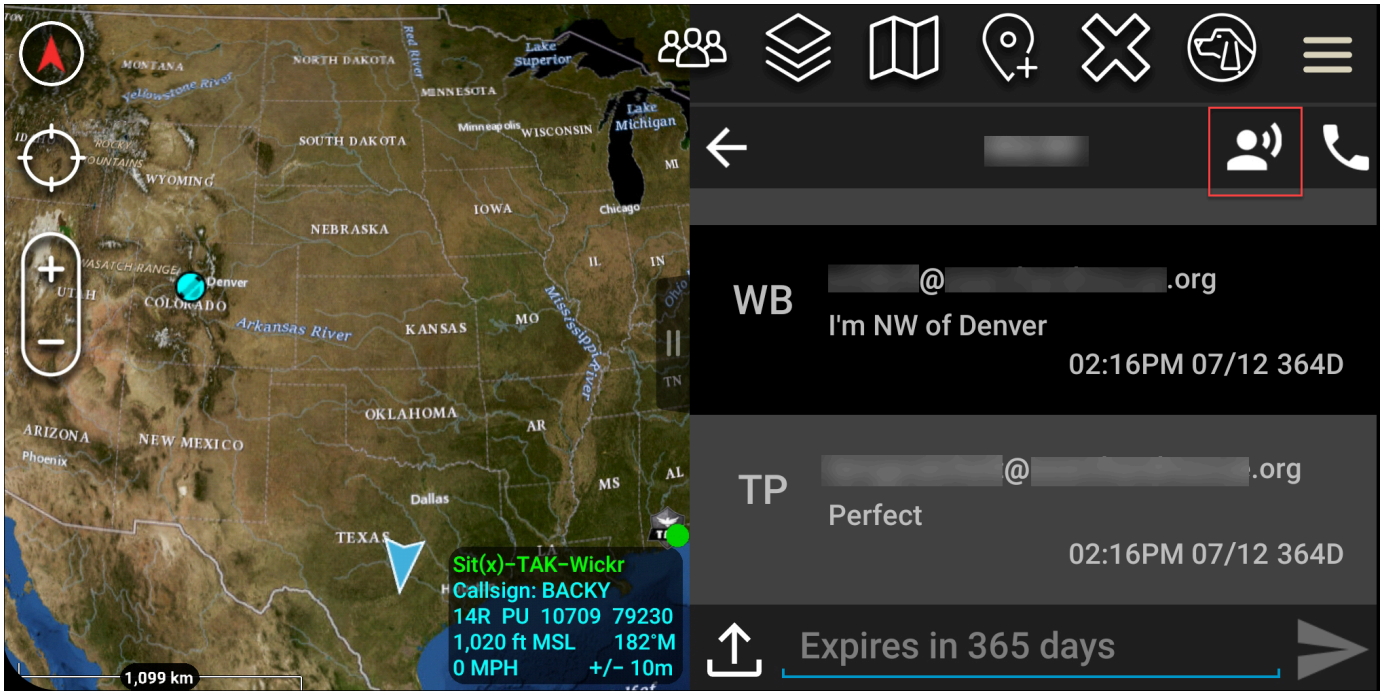
   Aparecerá el icono de descarga, que indica que se está descargando el archivo que ha seleccionado.

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

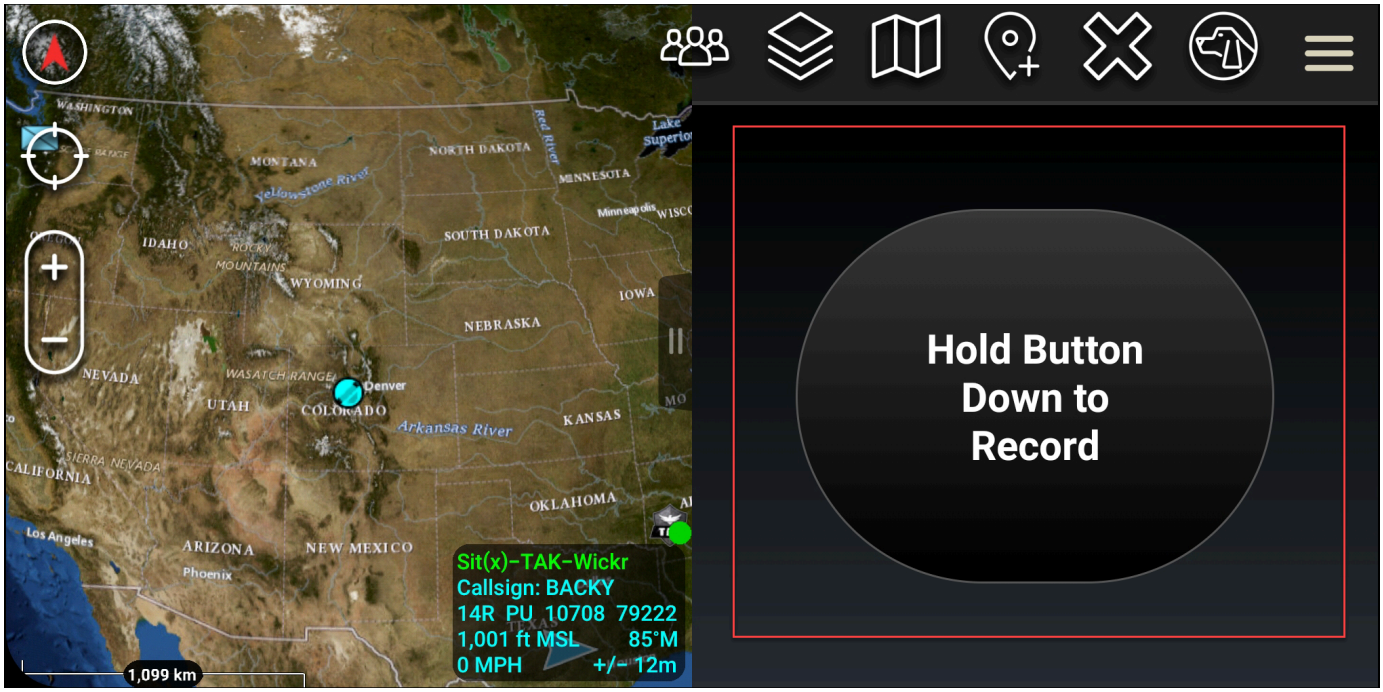
Puedes enviar un mensaje de voz seguro (Push-to-talk) en el complemento Wickr para ATAK.

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.



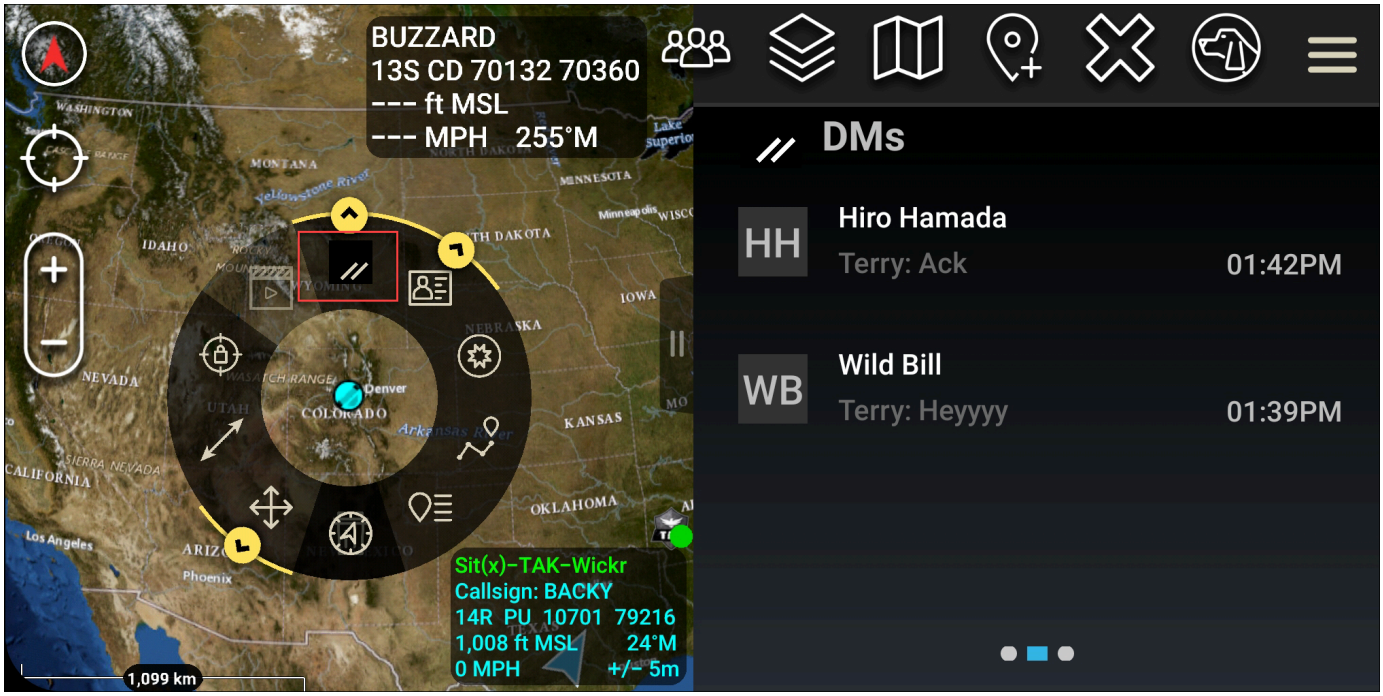
4. Grabe su mensaje.
5. Después de grabar el mensaje, suelte el botón para enviarlo.

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.

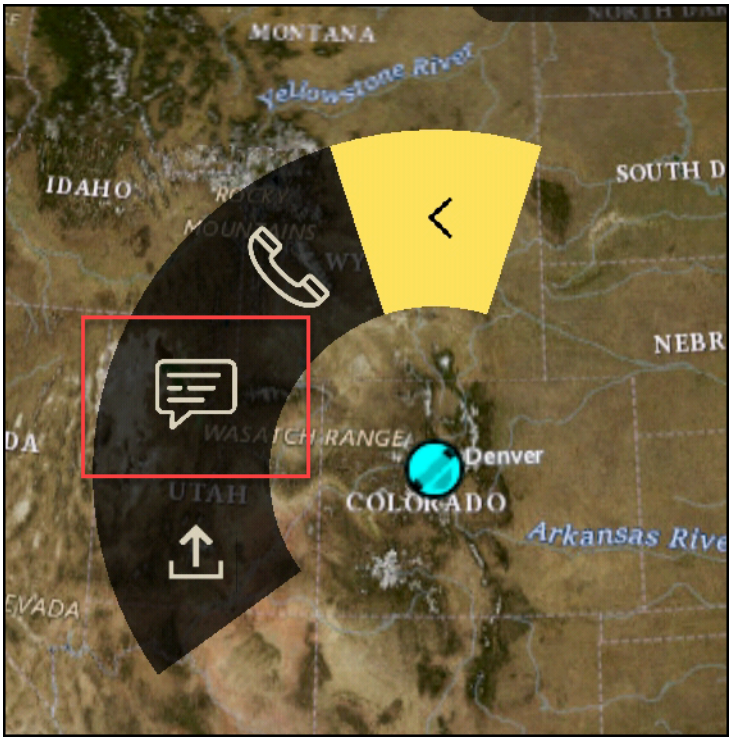
1. Abra la vista en pantalla dividida del mapa de ATAK y del complemento Wickr para ATAK de forma simultánea. El mapa muestra a sus compañeros de equipo o los activos en la vista de mapa.
2. Seleccione el icono de usuario para abrir la rueda de opciones.
3. Seleccione el icono de Wickr para ver las opciones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



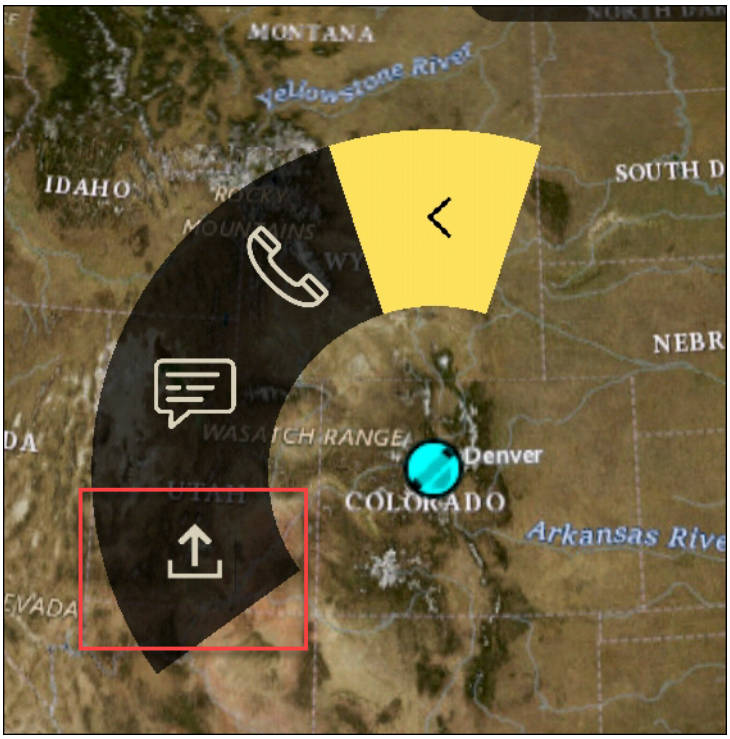
4. En la rueda de opciones, elija uno de los siguientes iconos:

   - 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

Permite enumerar los siguientes puertos para garantizar que Wickr funcione correctamente:

Puertos

- TCPpuerto 443 (para mensajes y archivos adjuntos)
- UDPpuertos 16384-16584 (para llamadas)

Dominios y direcciones que se van a incluir en la lista por región

Si necesitas incluir en una lista todos los dominios de llamadas y direcciones IP de servidores posibles, consulta la siguiente lista de posibles dominios CIDRs por región. Consulte esta lista periódicamente, ya que está sujeta a cambios.

> **Note**
>
> Los correos electrónicos de registro y verificación se envían desde donotreply@wickr.email.

Este de EE. UU. (Norte de Virginia)

Dominios:	• gw-pro-prod.wickr.com • api.messaging. wickr.us-east-1.amazonaws.com
CIDRdirecciones:	• 44.211.195.0/27 • 4421383,32/28
Direcciones IP:	• 44.211.195.0 • 44,211,195,1 • 44,211,195,2 • 44,211,195.3 • 44,211,195,4 • 44,211,195,5 • 44,211,195,6 • 44,211,195,7 • 44,211.195,8 • 44,211.195,9 • 44211195,10 • 44,211.195,11 • 44,211.195,12 • 44,211.195,13 • 44,211.195,14 • 44,211.195,15 • 44,211.195,16 • 44,211.195,17 • 44,211.195,18

- 44,211.195,19
- 44211195,20
- 44,211.195,21
- 44,211.195,22
- 44,211.195,23
- 44,211.195,24
- 44211195,25
- 44,211.195,26
- 44,211.195,27
- 44,211.195,28
- 44211195,29
- 44,211.195,30
- 44,211.195,31
- 4421383,32
- 4421383,33
- 4421383,34
- 4421383,35
- 4421383,36
- 4421383,37
- 4421383,38
- 4421383,39
- 4421383,40
- 4421383,41
- 4421383,42
- 4421383,43
- 4421383,44
- 4421383,45
- 4421383,46
- 4421383,47

Asia-Pacífico (Singapur)

Dominio:	• api.messaging. wickr.ap-southeast-1.amazonaws.com
CIDRdirecciones:	• 47.129.23.144/28
Direcciones IP:	• 47.129.23.144 • 4712923,145 • 4712923,146 • 4712923,147 • 4712923,148 • 4712923,149 • 4712923,150 • 4712923151 • 4712923,152 • 4712923,153 • 4712923,154 • 4712923,155 • 4712923,156 • 4712923,157 • 4712923,158 • 4712923,159

Asia-Pacífico (Sídney)

Dominio:	• api.messaging. wickr.ap-southeast-2.amazonaws.com
CIDRdirecciones:	• 3.27.180.208/28
Direcciones IP:	• 3.27.180.208 • 3,27180,209

	• 3,27,180,210 • 3.27,180,211 • 3.27,180,212 • 3,27,180,213 • 3,27,180,214 • 3.27,180,215 • 3,27,180,216 • 3.27,180,217 • 3.27,180,218 • 3.27180,219 • 3,27180,220 • 3.27180,221 • 3.27180,222 • 3.27180,223

Asia-Pacífico (Tokio)

Dominio:	• api.messaging. wickr.ap-northeast-1.amazonaws.com
CIDRdirecciones:	• 57.181.142.240/28
Direcciones IP:	• 57.181.142.240 • 57,181,142,241 • 57,181,142,242 • 57,181,142,243 • 57,181,142,244 • 57,181,142,245 • 57,181,142,246 • 57,181,142,247 • 57,181,142,248 • 57,181,142,249

	• 57,181,142,250 • 57,181,142251 • 57,181,142,252 • 57,181,142,253 • 57,181,142,254 • 57,181,142,25

Canadá (centro)

Dominio:	• api.messaging. wickr.ca-central-1.amazonaws.com
CIDRdirecciones:	• 15.156.152.96/28
Direcciones IP:	• 15.156.152.96 • 15,156152,97 • 15,156152,98 • 15,156,15,99 • 15,156,152,100 • 15,156,152,101 • 15,156,152,102 • 15,156,152,103 • 15,156,152,104 • 15,156,152,105 • 15,156,152,106 • 15,156,152,107 • 15,156,152,108 • 15,156,152,109 • 15,156,152,110 • 15,156,152,111

Europe (Fráncfort)

Dominio:	• api.messaging. wickr.eu-central-1.amazonaws.com
CIDRdirecciones:	• 3.78.252.32/28
Direcciones IP:	• 3.78.252.32 • 3,78,252,33 • 3,78,252,34 • 3,78,252,35 • 3,78,252,36 • 3,78,252,37 • 3,78,252,38 • 3,78,252,39 • 3,78,252,40 • 3,78,252,41 • 3,78,252,42 • 3,78,252,43 • 3,78,252,44 • 3,78,252,45 • 3,78,252,46 • 3,78,252,47

Europe (Londres)

Dominio:	• api.messaging. wickr.eu-west-2.amazonaws.com
CIDRdirecciones:	• 13.43.91.48/28
Direcciones IP:	• 13.43.91.48 • 13,4391,49

	• 13,4391,50 • 13,4391,51 • 13,4391,52 • 13,4391,53 • 13,4391,54 • 13,4391,55 • 13,4391,56 • 13,4391,57 • 13,4391,58 • 13,4391,59 • 13,4391,60 • 13,4391,61 • 13,4391,62 • 13,4391,63

Europa (Estocolmo)

Dominio:	• api.messaging. wickr.eu-north-1.amazonaws.com
CIDRdirecciones:	• 13.60.1.64/28
Direcciones IP:	• 13.60.1.64 • 13,601,65 • 13,601,66 • 13,601,67 • 13,601,68 • 13,601,69 • 13,601,70 • 13,601,71 • 13,601,72 • 13,601,73

	• 13,601,74 • 13,601,75 • 13,601,76 • 13,601,77 • 13,601,78 • 13,601,79

Europa (Zúrich)

Dominio:	• api.messaging. wickr.eu-central-2.amazonaws.com
CIDRdirecciones:	• 16.63.106.224/28
Direcciones IP:	• 16.63.106.224 • 16,63106,225 • 16,63106226 • 16,63106,227 • 16,63106,228 • 16,63106,229 • 16,63106,230 • 16,63106,231 • 16,63106,232 • 16,63106,233 • 16,63106,234 • 16,63106,235 • 16,63106,236 • 16,63106,237 • 16,63106,238 • 16,63106,239

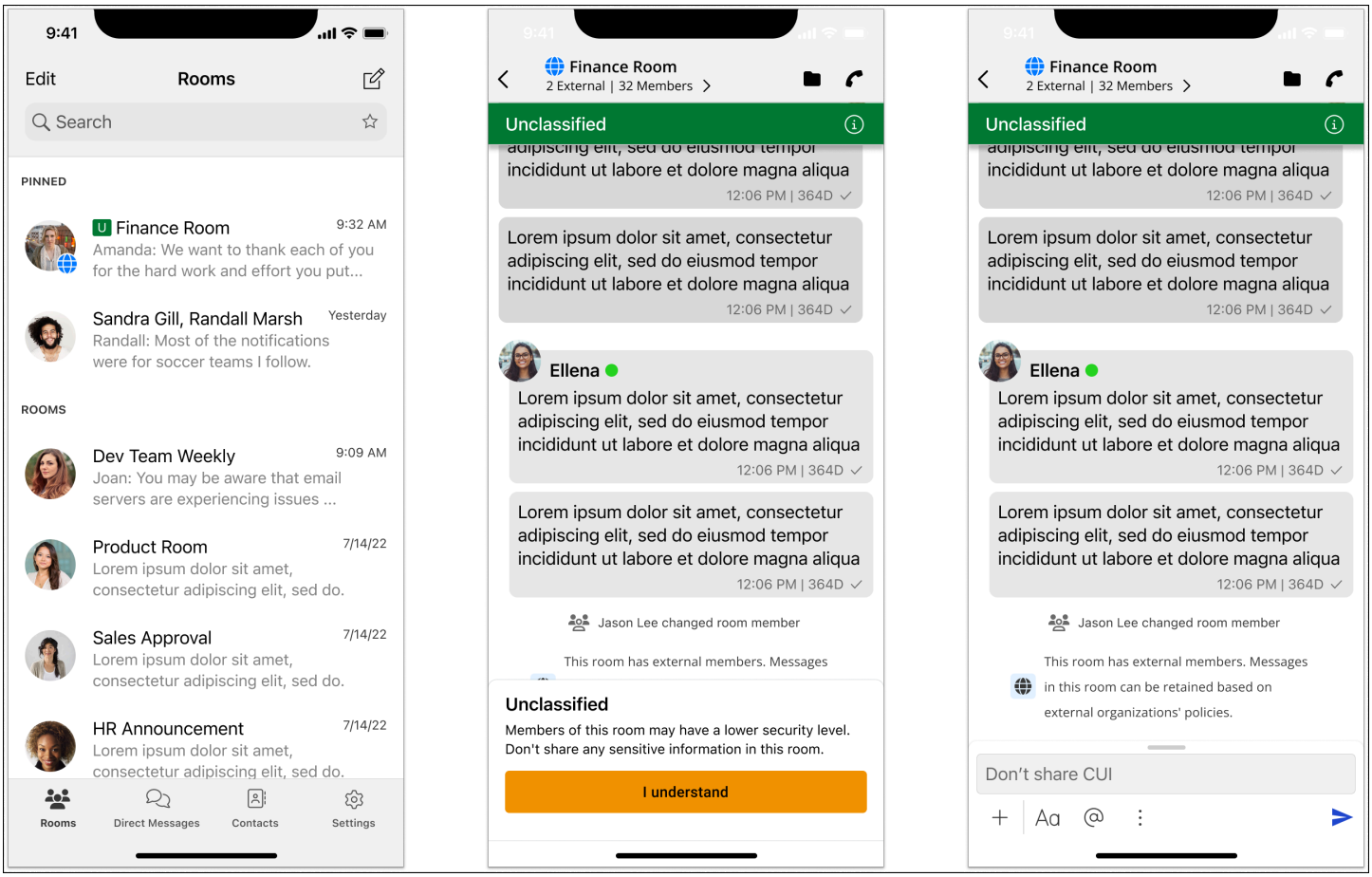
AWS GovCloud (Estados Unidos-Oeste)

Dominio:	• api.messaging.wickr. us-gov-west-1.amazonaws.com
CIDRdirecciones:	• 3.30.186.208/28
Direcciones IP:	• 3.30.186.208 • 3,30186,209 • 3,30186,210 • 3,30186,211 • 3,30186,212 • 3,30186,213 • 3,30186,214 • 3,30186,215 • 3,30186,216 • 3,30186,217 • 3,30186,218 • 3,30186,219 • 3,30186,220 • 3,30186,221 • 3,30186222 • 3,30186,223

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 entablen 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

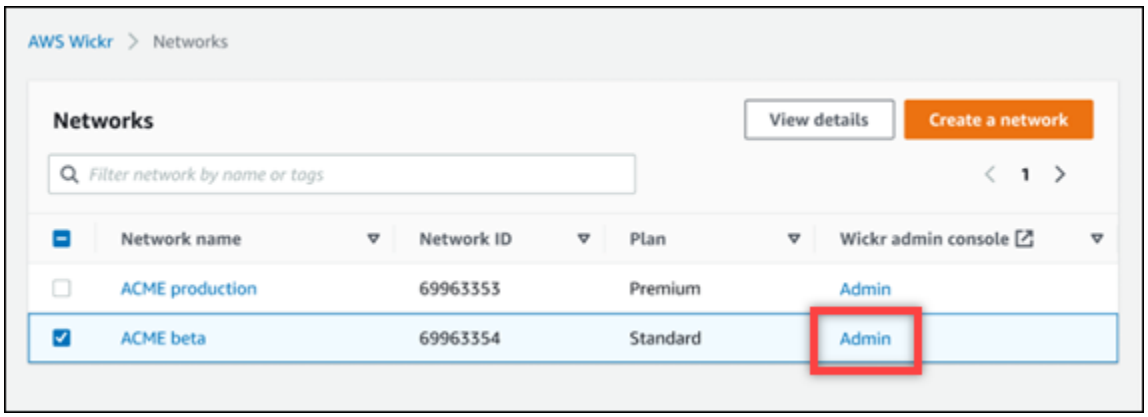
Puedes ver los usuarios actuales de Wickr y modificar sus detalles en la sección Usuario de Wickr. AWS Management Console

Temas

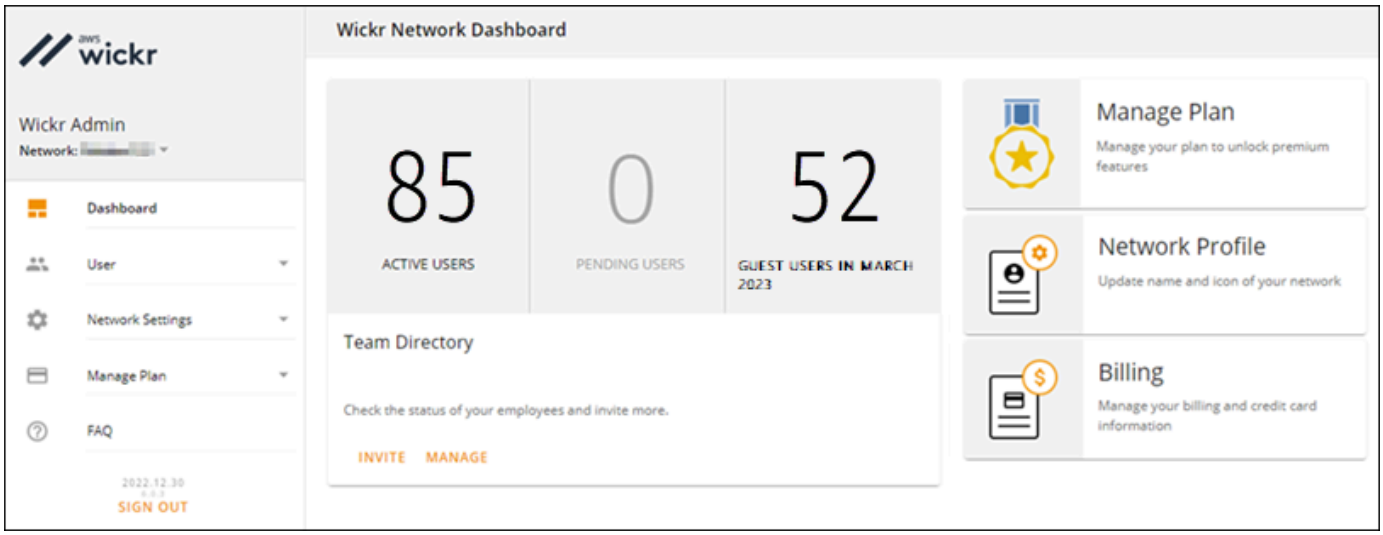
Ver usuarios

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/.
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/.

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. ElijaCrear 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/.
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/.
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/.
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/.
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/.
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. 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.

   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.

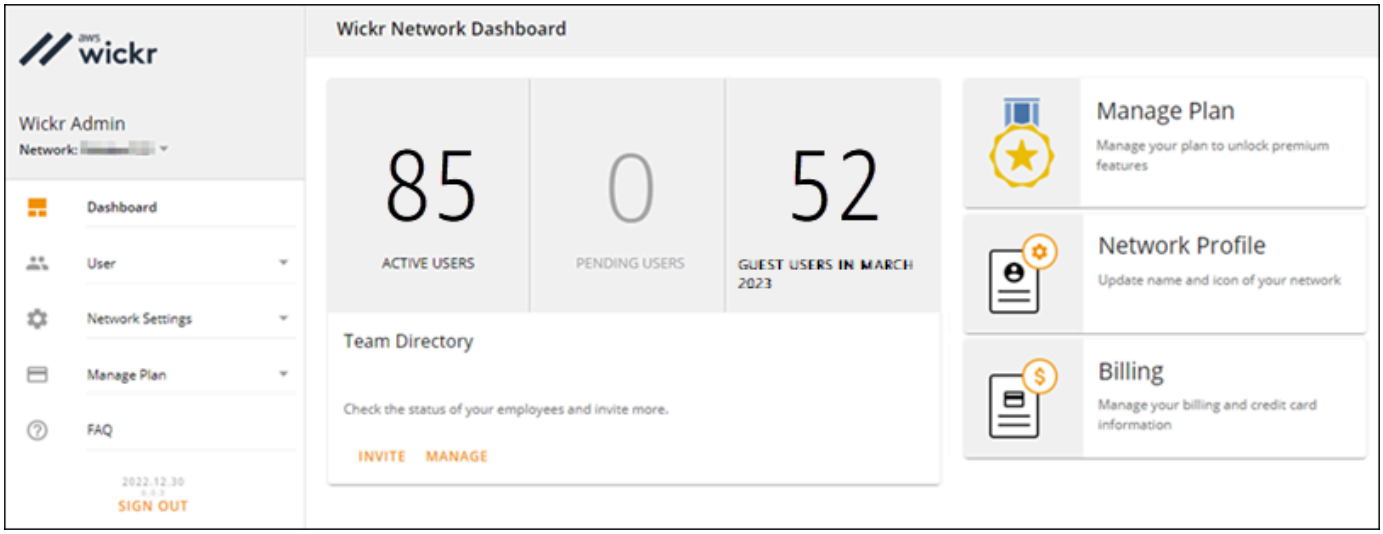
Los usuarios registrados en el grupo de seguridad específico de su red de Wickr ahora pueden interactuar con usuarios invitados. Para obtener más información, consulte Usuarios invitados en la Guía del usuario de Wickr.

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/.
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/.

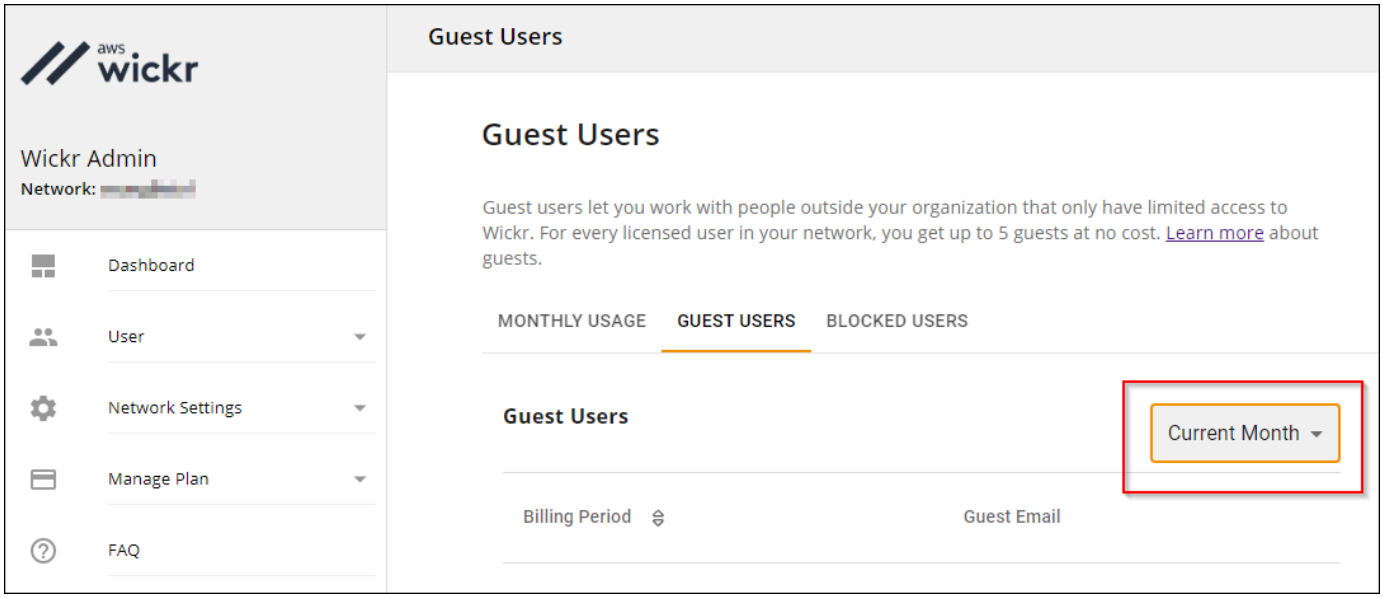
2. En la página Redes, seleccione el enlace Admin para acceder a la consola de administración de Wickr de dicha red.
3. En el panel de navegación de la consola de administración de Wickr, elija Usuario y, luego, Usuarios invitados.
4. En la página Usuarios invitados, seleccione la sección Uso mensual.

> **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/.
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/.
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/.
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 Wickr AWS

Seguridad en la nube en 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 y tú. 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 se ejecuta AWS servicios en el Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte del AWS Programas de cumplimiento . Para obtener más información sobre los programas de cumplimiento que se aplican a AWS Wickr, consulte AWS Servicios incluidos en el ámbito de aplicación del programa de cumplimiento .
- Seguridad en la nube: su responsabilidad viene determinada por la AWS servicio que utiliza. 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 aprendes a usar otros AWS servicios que te ayudan a monitorear y proteger tus recursos de Wickr.

Temas

Protección de datos en Wickr AWS

La AWS modelo de responsabilidad compartida El modelo se aplica a la 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 que está alojado en esta infraestructura. También es responsable de las tareas de configuración y administración de la seguridad del Servicios de AWS que utilizas. Para obtener más información sobre la privacidad de los datos, consulte la sección Privacidad de datos FAQ. Para obtener información sobre la protección de datos en Europa, consulte la AWS Modelo de responsabilidad compartida y entrada de GDPR blog sobre AWS Blog de seguridad.

Para fines de protección de datos, le recomendamos que proteja Cuenta de AWS 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 multifactorial (MFA) con cada cuenta.
- UtiliceSSL/TLSpara comunicarse con AWS recursos. Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Configure API y registre la actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Trabajar con CloudTrail senderos en la AWS CloudTrail Guía del usuario.
- Uso AWS soluciones de 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 entre FIPS 140 y 3 módulos criptográficos validados para acceder AWS a través de una interfaz de línea de comandos oAPI, utilice un FIPS punto final. Para obtener más información sobre los FIPS puntos finales disponibles, consulte la Norma Federal de Procesamiento de Información (FIPS) 140-3.

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 otros Servicios de AWS usando la consola, API AWS CLI, o AWS SDKs. 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, le recomendamos encarecidamente que no incluya información sobre las credenciales URL para validar su solicitud a ese servidor.

Gestión de identidad y acceso para AWS Wickr

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS recursos. IAMlos administradores controlan quién puede autenticarse (iniciar sesión) y quién está autorizado (tiene permisos) para usar los recursos de Wickr. IAMes un Servicio de AWS que puede utilizar sin coste adicional.

Temas

Público

¿Cómo se usa 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 identidad y acceso a 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. A continuación, debes enviar solicitudes a tu IAM administrador para cambiar los permisos de los usuarios del servicio. Revise la información de esta página para comprender los conceptos básicos deIAM. Para obtener más información sobre cómo su empresa puede utilizar IAM Wickr, consulte¿Cómo funciona AWS Wickr con IAM.

IAMadministrador: si eres IAM administrador, quizá te interese obtener más información sobre cómo puedes redactar políticas para administrar el acceso a Wickr. Para ver ejemplos de políticas de Wickr basadas en la identidad que puedes usar, consulta. IAM Ejemplos de políticas basadas en la identidad para Wickr AWS

Autenticación con identidades

La autenticación es la forma de iniciar sesión en AWS utilizando tus credenciales de identidad. Debe estar autenticado (iniciar sesión en AWS) como Usuario raíz de la cuenta de AWS, como IAM usuario o asumiendo un IAM rol.

Puede iniciar sesión en AWS como identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios de (IAMIdentity 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, el administrador configuró previamente la federación de identidades mediante roles. IAM Cuando accedes AWS al usar la federación, está asumiendo un rol de manera indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en AWS Management Console o el AWS portal de acceso. Para obtener más información sobre cómo iniciar sesión en AWS, consulta Cómo iniciar sesión en tu Cuenta de AWS en la AWS Sign-In Guía del usuario.

Si accedes 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 usa AWS herramientas, debe firmar las solicitudes usted mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar AWS APIsolicitudes en la Guía IAM del usuario.

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

Cuenta de AWS usuario raíz

Al crear un Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todas Servicios de AWS y los recursos de la cuenta. Esta identidad se denomina Cuenta de AWS usuario root y se accede a él iniciando sesión con la dirección de correo electrónico y la contraseña que utilizó 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 tareas que requieren que inicie sesión como usuario root, consulte Tareas que requieren credenciales de usuario root en la Guía del IAM usuario.

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, el AWS Directory Service, el directorio del Centro de identidades o cualquier usuario 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 la administración centralizada del acceso, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en IAM Identity Center, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todos sus Cuentas de AWS y aplicaciones. Para obtener información sobre IAM Identity Center, consulte ¿Qué es IAM Identity Center? en el AWS IAM Identity Center Guía del usuario.

Usuarios y grupos de IAM

Un IAMusuario es una identidad dentro de tu Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos utilizar credenciales temporales en lugar de crear IAM usuarios con credenciales de larga duración, como contraseñas y claves de acceso. Sin embargo, si tiene casos de uso específicos que requieren credenciales a largo plazo con IAM los usuarios, le recomendamos que rote las claves de acceso. Para obtener más información, consulte Rotar las claves de acceso con regularidad para los casos de uso que requieran credenciales de larga duración en la Guía del IAM usuario.

Un IAMgrupo es una identidad que especifica un conjunto de IAM usuarios. 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 para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar IAM los recursos.

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 de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Cuándo crear un IAM usuario (en lugar de un rol) en la Guía del IAM usuario.

IAMroles

Un IAMrol es una identidad dentro de tu Cuenta de AWS que tiene permisos específicos. Es similar a un IAM usuario, pero no está asociado a una persona específica. Puede asumir temporalmente un IAM rol en el AWS Management Console cambiando de rol. Puede asumir un rol llamando a un AWS CLI o AWS APIoperación o mediante una operación personalizadaURL. Para obtener más información sobre los métodos de uso de roles, consulte Uso de IAM roles en la Guía del IAM usuario.

IAMlos roles 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 sobre los roles para la federación, consulte Creación de un rol para un proveedor de identidad externo en la Guía del IAM usuario. Si usa IAM Identity Center, configura un conjunto de permisos. Para controlar a qué pueden acceder sus identidades después de autenticarse, IAM Identity Center correlaciona el conjunto de permisos con un rol en. IAM Para obtener información sobre los conjuntos de permisos, consulte los conjuntos de permisos en la AWS IAM Identity Center Guía del usuario.
- Permisos de IAM usuario temporales: un IAM usuario o rol puede asumir un IAM rol para asumir temporalmente diferentes permisos para una tarea específica.
- Acceso multicuenta: puedes usar un IAM rol para permitir que alguien (un responsable de confianza) de una cuenta diferente acceda a los recursos de tu cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunos Servicios de AWS, puede adjuntar una política directamente a un recurso (en lugar de utilizar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso

multicuenta, consulta el tema sobre el acceso a los recursos entre cuentas IAM en la Guía del IAM usuario.

- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual 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 IAM usuario o un rol para realizar acciones en AWS, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos del director que llama a un Servicio de AWS, combinado con la solicitud Servicio de AWS para realizar solicitudes a los servicios intermedios. FASlas solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completar. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre la política a la hora de realizar FAS solicitudes, consulte Reenviar las sesiones de acceso.
  - Función de servicio: una función de servicio es una IAMfunción que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentroIAM. Para obtener más información, consulte Crear un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Función vinculada a un 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 la función de realizar una acción en su nombre. Los roles vinculados al servicio aparecen en su Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver, pero no editar, los permisos de las funciones vinculadas al servicio.
- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un IAM rol para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y se están creando AWS CLI o AWS APIsolicitudes. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS Un rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia que se adjunte a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte Uso de un IAM rol para conceder permisos a aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del IAM usuario.

Para saber si se deben usar IAM roles o IAM usuarios, consulte Cuándo crear un IAM rol (en lugar de un usuario) en la Guía del IAM usuario.

Administración de acceso mediante políticas

Usted controla el acceso en AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto en 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 en AWS como JSON documentos. Para obtener más información sobre la estructura y el contenido de los documentos de JSON políticas, consulte Descripción general de JSON las políticas en la Guía del IAM usuario.

Los administradores pueden utilizar AWS JSONpolíticas 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. Para conceder a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

IAMlas políticas definen los 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 su función en AWS Management Console, el AWS CLI, o el AWS API.

Políticas basadas en identidad

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, 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 información sobre cómo crear una política basada en la identidad, consulte Creación de IAM políticas en la Guía del usuario. 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 funciones de su Cuenta de AWS. Las políticas gestionadas incluyen AWS las políticas gestionadas y las políticas gestionadas por el cliente. Para saber cómo elegir entre una política

gestionada o una política en línea, consulte Elegir entre políticas gestionadas y políticas integradas en la Guía del IAMusuario.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles 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 AWS políticas gestionadas desde una política basada IAM en recursos.

Listas de control de acceso () ACLs

Las listas de control de acceso (ACLs) controlan qué responsables (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLsson similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de JSON políticas.

Amazon S3, AWS WAF, y Amazon VPC son ejemplos de servicios que admitenACLs. Para obtener más informaciónACLs, consulte la descripción general de la 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 función avanzada en la que se establecen los permisos máximos que una política basada en la identidad puede conceder a una IAM entidad (IAMusuario o rol). 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 los límites de los permisos para IAM las entidades en la Guía del IAMusuario.

- 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 obtener más información, consulte las políticas de sesión en la Guía del IAM usuario.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para obtener información sobre cómo AWS determina si se permite una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del IAM usuario.

AWS políticas gestionadas para AWS Wickr

Para añadir permisos a usuarios, grupos y roles, es más fácil de usar AWS administró políticas en lugar de escribir las políticas usted mismo. Crear políticas gestionadas por los IAM clientes que proporcionen a tu equipo solo los permisos que necesita requiere tiempo y experiencia. Para empezar rápidamente, puedes usar nuestra AWS políticas gestionadas. Estas políticas cubren casos de uso comunes y están disponibles en su Cuenta de AWS. Para obtener más información sobre AWS políticas gestionadas, consulte AWS políticas gestionadas en la Guía IAM del usuario.

Servicios de AWS mantener y actualizar AWS políticas gestionadas. No puedes cambiar los permisos en AWS políticas gestionadas. En ocasiones, los servicios añaden permisos adicionales a una AWS política gestionada para admitir nuevas funciones. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Lo más probable es que los servicios actualicen un AWS política gestionada cuando se lanza una nueva función o cuando hay nuevas operaciones disponibles. Los servicios no eliminan los permisos de un AWS política gestionada, para que las actualizaciones de la política no infrinjan los permisos existentes.

AWS política gestionada: AWSWickrFullAccess

Puede adjuntar la `AWSWickrFullAccess` política a sus IAM identidades. Esta política otorga todos los permisos administrativos al servicio de Wickr, incluido el AWS Management Console para Wickr en el AWS Management Console. Para obtener más información sobre cómo adjuntar políticas a

una identidad, consulte Añadir y eliminar permisos de IAM identidad en la AWS Identity and Access Management Guía del usuario.

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 a AWS políticas administradas

Ver detalles sobre las actualizaciones de AWS gestioné las políticas de Wickr desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbete al RSS feed de la página del historial de documentos de Wickr.

Cambio	Descripción	Fecha
AWSWickrFullAccess— Nueva política	Wickr agregó una nueva política que otorga todos los permisos administrativos al servicio de Wickr, incluida la consola de administración de Wickr en AWS Management Console.	28 de noviembre de 2022
Wickr comenzó el seguimiento de los cambios	Wickr comenzó a rastrear los cambios en su AWS políticas gestionadas.	28 de noviembre de 2022

¿Cómo funciona AWS Wickr con IAM

Antes de gestionar el acceso IAM a Wickr, descubre qué IAM funciones están disponibles para su uso con Wickr.

IAMfunciones que puedes usar con Wickr AWS

IAMcaracterística	Compatibilidad de Wickr
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	No
Claves de condición de política	No
ACLs	No
ABAC(etiquetas en las políticas)	No
Credenciales temporales	No
Permisos de entidades principales	No
Roles de servicio	No
Roles vinculados al servicio	No

Para obtener una visión de alto nivel de cómo Wickr y otros AWS los servicios funcionan con la mayoría de las IAM funciones, consulte AWS servicios con los que funcionan IAM en la Guía IAM del usuario.

Políticas basadas en identidades de Wickr

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, 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 información sobre cómo crear una política basada en la identidad, consulte Creación de IAM políticas en la Guía del usuario. IAM

Con las políticas IAM basadas en la identidad, 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 obtener más información sobre todos los elementos que puede utilizar en una JSON política, consulte la referencia sobre los elementos de la IAM JSON política en la Guía del IAMusuario.

Ejemplos de políticas basadas en identidades de Wickr

Para ver ejemplos de políticas basadas en identidad de Wickr, consulte Ejemplos de políticas basadas en la identidad para Wickr AWS.

Políticas basadas en recursos de Wickr

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos JSON de política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles 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.

Para habilitar el acceso entre cuentas, puede especificar una cuenta completa o IAM entidades de otra cuenta como principales en una política basada en 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 IAM administrador de la cuenta de confianza también debe conceder permiso a la entidad principal (usuario o rol) 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 el tema Acceso a recursos entre cuentas IAM en la Guía del IAM usuario.

Acciones de política para Wickr

Compatibilidad con las acciones de política: sí

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

El `Action` elemento de una JSON política describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que las asociadas AWS APIoperación. Hay algunas excepciones, como las acciones que solo permiten permisos y que no tienen una operación coincidente. API 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, consulta las acciones definidas por AWS Wickr en la Referencia de autorización de servicios.

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 la identidad para Wickr AWS.

Recursos de políticas de Wickr

Soporta recursos normativos: No

Los administradores pueden usar AWS JSONpolíticas 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` JSON de política especifica el objeto o los objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso mediante su 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 respectivos tiposARNs, consulta los recursos definidos por AWS Wickr en la referencia de autorización de servicios. Para saber con qué acciones puedes especificar cada recurso, consulta Acciones definidas por AWS Wickr. ARN

Para ver ejemplos de políticas basadas en identidad de Wickr, consulte Ejemplos de políticas basadas en la identidad para Wickr AWS.

Claves de condición de política para Wickr

Admite claves de condición de política específicas del servicio: No

Los administradores pueden usar AWS JSONpolíticas 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 `Condition` elementos en una declaración o varias claves en un solo `Condition` elemento, AWS los evalúa mediante una `AND` operación lógica. Si especifica varios valores para una sola 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 a un IAM usuario permiso para acceder a un recurso solo si está etiquetado con su nombre de IAM usuario. Para obtener más información, consulte los elementos IAM de la política: variables y etiquetas en la Guía del IAM usuario.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas AWS claves de condición globales, consulte AWS claves de contexto de condiciones globales en la Guía IAM del usuario.

Para ver una lista de las claves de condición de Wickr, consulta las claves de condición de AWS Wickr en la Referencia de autorización de servicio. Para saber con qué acciones y recursos 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 la identidad para Wickr AWS.

ACLsen Wickr

SoportesACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLsson similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de JSON políticas.

ABACcon Wickr

Soportes ABAC (etiquetas en las políticas): No

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define los permisos en función de los atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a IAM entidades (usuarios o roles) y a muchas AWS recursos. Etiquetar entidades y recursos es el primer paso deABAC. Luego, diseñe ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso al que está intentando acceder.

ABACes útil en entornos de rápido crecimiento y ayuda en situaciones en las que la administración de políticas se vuelve 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 al respectoABAC, consulte ¿Qué es? ABAC en la Guía IAM del usuario. Para ver un tutorial con los pasos de configuraciónABAC, consulte Usar el control de acceso basado en atributos (ABAC) en la Guía del IAMusuario.

Uso de credenciales temporales con Wickr

Admite credenciales temporales: no

Alguno Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluyendo qué Servicios de AWS trabaje con credenciales temporales, consulte Servicios de AWS que funcionan IAM en la Guía IAM del usuario.

Está utilizando credenciales temporales si inicia sesión en AWS Management Console utilizando 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 su 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 obtener más información sobre el cambio de rol, consulte Cambiar a un rol (consola) en la Guía del IAMusuario.

Puede crear credenciales temporales manualmente mediante el AWS CLI o AWS API. 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 obtener 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 utiliza un IAM usuario o un rol para realizar acciones en AWS, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos del director que llama a un Servicio de AWS, combinado con la solicitud Servicio de AWS para realizar solicitudes a los servicios intermedios. FASlas solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completar. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre la política a la hora de realizar FAS solicitudes, consulte Reenviar las sesiones de acceso.

Roles de servicio de Wickr

Compatible con roles de servicio: No

Una función de servicio es una IAMfunción que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentroIAM. Para obtener más información, consulte Crear 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

Compatibilidad 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 la función de realizar una acción en su nombre. Los roles vinculados al servicio aparecen en su Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver, pero no editar, los permisos de las funciones vinculadas al servicio.

Para obtener más información sobre la creación o la administración de funciones vinculadas a un servicio, consulte AWS servicios con los que funcionan. 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 la identidad para Wickr AWS

De forma predeterminada, un IAM usuario nuevo no tiene permisos para hacer nada. IAMEl administrador debe crear y asignar IAM políticas que den permiso a los usuarios para administrar el servicio de 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 las redes de Wickr mediante AWS Management Console para Wickr. Para obtener más información sobre los elementos de una declaración IAM de política, consultePolíticas basadas en identidades de Wickr. Para obtener información sobre cómo crear una IAM política con estos documentos de JSON política de ejemplo, consulte Creación de políticas en la JSON pestaña de la Guía del IAM usuario.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de 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 suponer costes para su Cuenta de AWS. Al crear o editar políticas basadas en la identidad, siga estas directrices y recomendaciones:

- Comience con AWS políticas gestionadas y avance hacia los permisos con los privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice la AWS políticas gestionadas que conceden permisos para muchos casos de uso habituales. Están disponibles en su Cuenta de AWS. Le recomendamos que reduzca aún más los permisos definiendo AWS políticas gestionadas por el cliente que sean específicas para sus casos de uso. Para obtener más información, consulte AWS políticas gestionadas o AWS políticas gestionadas para las funciones laborales en la Guía IAM del usuario.
- Aplique permisos con privilegios mínimos: cuando establezca permisos con IAM políticas, 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. Para obtener más información sobre cómo IAM aplicar permisos, consulte Políticas y permisos IAM en la IAM Guía del usuario.

- Utilice las condiciones en IAM las políticas para restringir aún más el acceso: puede añadir una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse medianteSSL. También puede utilizar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de un procedimiento específico Servicio de AWS, como, por ejemplo, AWS CloudFormation. Para obtener más información, consulte los elementos IAM JSON de la política: Condición en la Guía del IAM usuario.
- Utilice IAM Access Analyzer para validar sus IAM políticas y garantizar permisos seguros y funcionales: IAM Access Analyzer valida las políticas nuevas y existentes para que se ajusten al lenguaje de las políticas (JSON) y IAM a las IAM mejores prácticas. IAMAccess Analyzer proporciona más de 100 comprobaciones de políticas y recomendaciones prácticas para ayudarle a crear políticas seguras y funcionales. Para obtener más información, consulte la validación de políticas de IAM Access Analyzer en la Guía del IAM usuario.
- Requerir autenticación multifactorial (MFA): si tiene un escenario que requiere IAM usuarios o un usuario raíz en su Cuenta de AWS, actívala MFA para mayor seguridad. Para solicitarlo MFA cuando se cancelen API las operaciones, añada MFA condiciones a sus políticas. Para obtener más información, consulte Configuración del API acceso MFA protegido en la Guía del IAM usuario.

Para obtener más información sobre las prácticas recomendadasIAM, consulte las prácticas recomendadas de seguridad IAM en la Guía del IAM usuario.

Uso de AWS Management Console para Wickr

Adjunte el `AWSWickrFullAccess` AWS administró una política a sus IAM identidades para concederles permisos administrativos completos para el servicio de Wickr, incluida la consola de administrador de Wickr en el AWS Management Console. Para obtener más información, consulteAWS política gestionada: AWSWickrFullAccess.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo se muestra cómo se puede crear una política que permita a IAM los usuarios ver las políticas integradas y administradas asociadas a su identidad de usuario. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante el AWS CLI o AWS API.

```
{
```

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

Solución de problemas de identidad y acceso a AWS Wickr

Usa la siguiente información para ayudarte a diagnosticar y solucionar problemas comunes que puedes encontrar al trabajar con Wickr y. IAM

Temas

- No estoy autorizado a realizar ninguna acción administrativa en el AWS Management Console para Wickr

No estoy autorizado a realizar ninguna acción administrativa en el AWS Management Console para Wickr

Si el archivo de AWS Management Console ya que Wickr le indica que no está autorizado a realizar una acción, debe ponerse en contacto con su 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 `mateojackson` IAM usuario intenta utilizar el AWS Management Console para que Wickr cree, administre o vea las redes de Wickr en AWS Management Console para Wickr, pero no tiene los `wickr:CreateAdminSession` permisos y. `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 permitirle acceder a AWS Management Console para Wickr usando las acciones `wickr:CreateAdminSession` y. `wickr:ListNetworks` Para obtener más información, consulte Ejemplos de políticas basadas en la identidad para Wickr AWS y AWS política gestionada: AWSWickrFullAccess.

Validación de conformidad

Para obtener una lista de AWS servicios en el ámbito de programas de cumplimiento específicos, consulte AWS Servicios incluidos en el ámbito de aplicación del programa de cumplimiento . Para obtener información general, consulte AWS Programas de cumplimiento .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact.

Tu responsabilidad en materia de cumplimiento al utilizar Wickr viene determinada por la confidencialidad de tus datos, los objetivos de cumplimiento de tu empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en la seguridad y el cumplimiento en AWS.
- AWS Recursos de conformidad : esta colección de libros de trabajo y guías puede aplicarse a su sector y ubicación.

- Evaluación de los recursos con las reglas del AWS Config Guía para 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— Esto AWS El servicio proporciona una visión completa del estado de su seguridad interior AWS que le ayuda a comprobar su conformidad con los estándares y las mejores prácticas del sector de la seguridad.

Resiliencia en AWS Wickr

La AWS la infraestructura global se basa en Regiones de AWS y zonas de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas a 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 acerca de Regiones de AWS y zonas de disponibilidad, consulte AWS Infraestructura global.

Además de AWS Wickr, una infraestructura global, ofrece varias funciones que ayudan a respaldar sus necesidades de respaldo y resiliencia de datos. Para obtener más información, consulte Retención de datos.

Infraestructura y seguridad en Wickr AWS

Como servicio gestionado, AWS Wickr está protegido por AWS procedimientos de seguridad de redes globales que se describen en el documento técnico Amazon Web Services: descripción general de los procesos de seguridad.

Análisis de configuración y vulnerabilidad en Wickr AWS

La configuración y los controles de TI son una responsabilidad compartida entre AWS y usted, nuestro cliente. Para obtener más información, consulte la AWS modelo de responsabilidad 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.

Mejores prácticas 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. Usa IAM plantillas para crear un rol. Para obtener más información, consulte AWS políticas gestionadas para AWS Wickr.
- Acceda al AWS Management Console para Wickr autenticándose en el AWS Management Console first. 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 CloudTrailcaptura 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, consulteRegistro 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 y `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": "abced980-23c7-4de1-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
La clasificación y federación transfronterizas ya están disponibles	La función de clasificación transfronteriza permite a los usuarios cambiar las conversaciones de la interfaz de GovCloud usuario. Para obtener más información, consulte Clasificación y federación GovCloud transfronterizas.	25 de junio de 2024
La función de lectura de recibos ya está disponible	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 Leer recibos.	23 de abril de 2024
Global Federation ahora admite la federación restringida y los administradores pueden ver los análisis de uso en la Consola de administración	Global Federation ahora admite la federación restringida. Esto funciona para las redes de Wickr en otras Regiones de AWS. Para obtener más información, consulte Grupos de seguridad. Además, los administradores ahora pueden ver sus análisis de uso en el panel de análisis de la consola de administración. Para obtener más	28 de marzo de 2024

	información, consulte el panel de análisis.	
Ya está disponible una prueba gratuita de tres meses del plan Premium de AWS Wickr	Los administradores de Wickr ahora pueden elegir un plan Premium de prueba gratuito de tres meses para hasta 30 usuarios. Durante la prueba gratuita, están disponibles todas las funciones de los planes 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.	9 de febrero de 2024
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 caracterí sticas, como la lista de usuarios invitados, la posibilid ad 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
Wickr ya está disponible en Europa (Londres) Región de AWS	Wickr ya está disponible en Europa (Londres). Región de AWS Para obtener más información, consulte Acceso a Wickr.	23 de agosto de 2023
Wickr ya está disponible en Canadá (Central) Región de AWS	Wickr ya está disponible en Canadá (Central). Región de AWS Para obtener más información, consulte Acceso a Wickr.	3 de julio de 2023
La característica de usuario invitado está ahora disponible para su vista previa	Los usuarios invitados pueden iniciar sesión en el cliente Wickr y colaborar con usuarios de la red de Wickr. Para más información, consulte Usuarios invitados (vista previa).	31 de mayo de 2023

AWSWickr ahora está integrado y ahora está disponible en AWS GovCloud (EE. UU.-Oeste) como AWS CloudTrail WickrGov	AWSWickr ahora está integrado con. AWS CloudTrail Para obtener más información, consulte Registrar las API llamadas de AWS Wickr mediante. AWS CloudTrail Además, Wickr ya está disponible en EE. UU. AWS GovCloud (oeste de EE. UU.). WickrGov Para obtener más información, consulte la AWS WickrGovGuía del AWS GovCloud (US) usuario.	30 de marzo de 2023
Etiquetado y creación de redes múltiples	AWSWickr ahora admite el etiquetado. Para obtener más información, consulta 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.

Junio de 2024

- La clasificación y federación transfronterizas ya están disponibles para GovCloud los usuarios. Para obtener más información, consulte Clasificación y federación GovCloud transfronterizas.

Abril de 2024

- Wickr ahora admite confirmaciones de lectura. Para obtener más información, consulta Leer recibos.

Marzo de 2024

- La federación global ahora admite la federación restringida, donde la federación global solo se puede habilitar para redes seleccionadas que se agreguen 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

- AWSWickr 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.
  - SSOConfiguración adicional para configurar un período de gracia para la actualización del token.

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 WickrGovGuía 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 ahora es compatible con el kit de asalto táctico de 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 el plan de prueba gratuito y el estándar.

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