Guía del usuario

# AWS Mensajería social para usuarios finales

# AWS Mensajería social para usuarios finales: Guía del usuario

# Table of Contents

# ¿Qué es la mensajería social para usuarios AWS finales?

AWS La mensajería social para el usuario final, también conocida como mensajería social, es un servicio de mensajería que permite a los desarrolladores WhatsApp integrarlo en sus aplicaciones. Proporciona acceso a sus WhatsApp amplias capacidades de mensajería, lo que permite la creación de contenido interactivo y de marca con imágenes, vídeos y botones. Al utilizar este servicio, puede añadir la funcionalidad de WhatsApp mensajería a sus aplicaciones junto con los canales existentes, como SMS las notificaciones automáticas, lo que le permitirá interactuar con los clientes a través de su canal de comunicación preferido.

Para empezar, puedes crear una nueva cuenta WhatsApp empresarial (WABA) mediante el proceso de incorporación autoguiado de la consola social de mensajería para usuarios AWS finales o vincular una cuenta ya existente WABA al servicio.

Temas



## ¿Es la primera vez que AWS usa la mensajería social?

Si es la primera vez que usa AWS End User Messaging Social, le recomendamos que empiece leyendo las siguientes secciones:

- Configuración de mensajería social para usuarios AWS finales
- Cómo empezar a usar AWS End User Messaging Social
- Mejores prácticas para la mensajería social para usuarios AWS finales

## Características de la mensajería AWS social para usuarios finales

AWS End User Messaging Social proporciona las siguientes características y funciones básicas:

- Diseñar mensajes coherentes y reutilizar el contenido de forma más eficaz mediante la creación y el uso de plantillas de mensaje. Una plantilla de mensaje incluye contenido y los ajustes que desea volver a utilizar en los mensajes que envíe.
- Acceda a nuevas y sofisticadas capacidades de mensajería para una experiencia más atractiva. Más allá del texto y los archivos multimedia, puede enviar ubicaciones y mensajes interactivos.
- Reciba mensajes de texto y multimedia de sus clientes.
- Genere confianza entre sus clientes verificando la identidad de su empresa a través de Meta.

## Servicios relacionados

AWS ofrece otros servicios de mensajería que se pueden usar juntos en un flujo de trabajo multicanal:

- Utilice la mensajería del usuario AWS final SMS para enviar SMS mensajes
- Utilice AWS End User Messaging Push para enviar notificaciones push
- Usa Amazon SES para enviar correos electrónicos

# AWS Acceder a las redes sociales de mensajería para usuarios finales

Puede acceder a AWS End User Messaging Social mediante lo siguiente:

AWS Consola social de mensajería para usuarios finales

: La interfaz web donde se crean y administran los recursos.

AWS Command Line Interface

: Interactúa con AWS los servicios de mediante el uso de comandos en el shell de la línea de comandos. La AWS Command Line Interface es compatible con Windows, macOS y Linux. Para obtener más información sobre el AWS CLI, consulte la Guía AWS Command Line Interface del usuario. Puede encontrar los AWS SMS comandos en la Referencia de AWS CLI comandos.

AWS SDKs

: Si es un desarrollador de software que prefiere crear aplicaciones usando un lenguaje en lugar de enviar una solicitud APIs en lugar de enviar una solicitud HTTP o HTTPS si AWS le proporciona

bibliotecas, ejemplos de código, tutoriales y otros recursos. Estas bibliotecas proporcionan funciones básicas que automatizan tareas como la firma criptográfica de las solicitudes, el reintento de las solicitudes o el tratamiento de las respuestas de error. Estas funciones le ayudan a empezar con más eficacia. Para obtener más información, consulte Herramientas para crear en AWS.

# Disponibilidad regional

AWS La mensajería social de usuario final está disponible en varios países de Regiones de AWS en América del Norte, Europa, Asia y Oceanía. En cada región, AWS mantiene varias zonas de disponibilidad. Estas zonas de disponibilidad están físicamente aisladas entre sí, pero están unidas mediante conexiones de red privadas con un alto nivel de rendimiento y redundancia y con baja latencia. Estas zonas de disponibilidad se utilizan para ofrecer niveles sumamente elevados de disponibilidad y redundancia, así como minimizar la latencia.

Para obtener más información Regiones de AWS, consulte Especificar qué Regiones de AWS cuenta puede usar en el Referencia general de Amazon Web Services. Para obtener una lista de todas las regiones en las que la mensajería social para usuarios AWS finales está disponible actualmente y los puntos finales de cada región, consulte los puntos finales y las cuotas de los puntos AWS finales de mensajería social API y de AWS servicio para usuarios finales en la tabla siguiente Referencia general de Amazon Web Serviceso en la siguiente. Para obtener más información sobre la cantidad de zonas de disponibilidad de cada región, consulte Infraestructura global de AWS.

Disponibilidad por región

| Nombres de las regiones | Región | Punto de conexión | WhatsApp APIversión |
|---|---|---|---|
| Este de EE. UU. (Norte de Virginia) | us-east-1 | social-messaging.us-east-1.amazonaws.com<br><br>social-messaging-fips.us-east-1.api.aws<br><br>social-messaging.us-east-1.api.aws | Versión 20 y posteriores |

| Nombres de las regiones | Región | Punto de conexión | WhatsApp APIversión |
|---|---|---|---|
| Este de EE. UU. (Ohio) | us-east-2 | social-messaging.us-east-2.amazonaws.com<br><br>social-messaging-fips.us-east-2.api.aws<br><br>social-messaging.us-east-2.api.aws | Versión 20 y posteriores |
| Oeste de EE. UU. (Oregón) | us-west-2 | social-messaging.us-west-2.amazonaws.com<br><br>social-messaging-fips.us-west-2.api.aws<br><br>social-messaging.us-west-2.api.aws | Versión 20 y posteriores |
| Asia Pacífico (Bombay) | ap-south-1 | social-messaging.ap-south-1.amazonaws.com<br><br>Mensajería social. ap-south-1.api.aws | Versión 20 y posteriores |
| Asia-Pacífico (Singapur) | ap-southeast-1 | social-messaging.ap-southeast-1.amazonaws.com<br><br>social-messaging.ap-southeast-1.api.aws | Versión 20 y posteriores |

| Nombres de las regiones | Región | Punto de conexión | WhatsApp APIversión |
|---|---|---|---|
| Europa (Irlanda) | eu-west-1 | social-messaging.eu-west-1.amazonaws.com<br><br>social-messaging.eu-west-1.api.aws | Versión 20 y posteriores |
| Europa (Londres) | eu-west-2 | social-messaging.eu-west-2.amazonaws.com<br><br>social-messaging.eu-west-1.api.aws | Versión 20 y posteriores |

# Configuración de mensajería social para usuarios AWS finales

Para poder usar AWS End User Messaging Social por primera vez, debe completar los pasos siguientes.

Temas



## Regístrese en Cuenta de AWS

Si no dispone de una Cuenta de AWS, siga los pasos que figuran a continuación para crear una.

Procedimiento para registrarse en 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 un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS le enviará un email de confirmación luego de completar el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/y seleccionando My Account (Mi cuenta).

# Creación de un usuario con acceso administrativo

Después de registrarse para obtener una Cuenta de AWS, proteja su Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no utilizar el usuario raíz en las tareas cotidianas.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un MFA dispositivo virtual para el usuario Cuenta de AWS root (consola) en la Guía del IAM usuario.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .
2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre cómo usar el Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, utilice el inicio de sesión URL que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

Para obtener ayuda para iniciar sesión con un usuario del Centro de IAM identidades de Identity Center, consulte Iniciar sesión en el portal de AWS acceso de en la Guía del AWS Sign-In usuario de.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .
2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

# Siguientes pasos

Ahora que está preparado para trabajar con AWS End User Messaging Social, consulte Cómo empezar a usar AWS End User Messaging Social para crear su cuenta WhatsApp empresarial (WABA) o migrar su cuenta WhatsApp empresarial existente.

# Cómo empezar a usar AWS End User Messaging Social

Estos temas lo guían a través de los pasos para vincular o migrar su cuenta WhatsApp empresarial (WABA) a AWS End User Messaging Social.

Temas



## Registrarse en WhatsApp

Una cuenta WhatsApp empresarial (WABA) permite a su empresa utilizar la plataforma WhatsApp empresarial para enviar mensajes directamente a sus clientes. Todas tus empresas WABAs forman parte de tu cartera empresarial de Meta. A WABA contiene sus activos orientados a los clientes, como el número de teléfono, las plantillas y el perfil de la WhatsApp empresa. Un perfil WhatsApp empresarial contiene la información de contacto de tu empresa que ven los usuarios. Para obtener más información sobre las cuentas WhatsApp empresariales, consulteWhatsApp Cuenta empresarial (WABA) en AWS End User Messaging Social.

Siga los pasos descritos en esta sección para comenzar a utilizar AWS End User Messaging Social. Utilice el proceso de registro integrado para crear una nueva cuenta WhatsApp empresarial (WABA) o migrar una existente WABA a AWS End User Messaging Social.

### Requisitos previos

**Important**

Trabajando con Meta/ WhatsApp

- El uso de la solución WhatsApp empresarial está sujeto a los términos y condiciones de las condiciones del servicio WhatsApp empresarial, las condiciones de la solución WhatsApp empresarial, la política de mensajería WhatsApp empresarial, las directrices de WhatsApp mensajería y todos los demás términos, políticas o directrices que se incluyan en ellas como referencia (ya que cada uno de ellos puede actualizarse periódicamente).
- Meta o WhatsApp puede prohibir en cualquier momento el uso de la solución WhatsApp empresarial.
- Debe crear una cuenta WhatsApp empresarial (» WABA «) con Meta y WhatsApp.

- Debe crear una cuenta de administrador comercial con Meta y vincularla a la suyaWABA.
- Debe proporcionarnos el control de WABA la suya. Si lo solicita, le transferiremos el control de WABA su propiedad de manera razonable y oportuna utilizando los métodos que Meta ponga a nuestra disposición.
- En relación con su uso de la Solución WhatsApp empresarial, no enviará ningún contenido, información o dato que esté sujeto a medidas de protección o a limitaciones de distribución de conformidad con las leyes o reglamentos aplicables.
- WhatsAppLos precios de uso de la solución WhatsApp empresarial se encuentran en los precios basados en conversaciones.

- Para crear una cuenta WhatsApp empresarial (WABA), su empresa necesita una cuenta Meta Business. Compruebe si su empresa ya tiene una cuenta Meta Business. Si aún no cuenta con una cuenta Meta Business, puede crear una durante el proceso de registro.
- Para usar un número de teléfono que ya esté en uso con la aplicación WhatsApp Messenger o la aplicación WhatsApp Business, primero debes eliminarlo.
- Un número de teléfono que pueda recibir una contraseña de un solo uso SMS o una contraseña de voz ()OTP. El número de teléfono utilizado para el registro se asocia a tu WhatsApp cuenta y el número de teléfono se utiliza cuando envías mensajes. El número de teléfono se puede seguir utilizando para SMSMMS, y para la mensajería de voz.
- Si va a importar uno existenteWABA, necesitará el de todos PINs los números de teléfono asociados al importadoWABA. Para restablecer un archivo perdido u olvidadoPIN, siga las instrucciones de la sección Update PIN in the WhatsApp Business Platform Cloud API Reference.

## Regístrese a través de la consola

Sigue estas instrucciones para crear una WhatsApp cuenta nueva, migrar una cuenta existente o añadir un número de teléfono a una existenteWABA. Como parte del proceso de registro, concedes acceso a AWS End User Messaging Social a tu cuenta WhatsApp empresarial. También permites que AWS End User Messaging Social te facture los mensajes. Para obtener más información sobre las cuentas WhatsApp empresariales, consulteDescripción de los tipos de cuentas WhatsApp empresariales.

1. Abra la consola social de mensajería para usuarios AWS finales en https://console.aws.amazon.com/social-messaging/.

2. Seleccione Cuentas empresariales.
3. En la página Vincular una cuenta empresarial, selecciona Iniciar el portal de Facebook. Aparecerá una nueva ventana de inicio de sesión desde Meta.
4. En la ventana de inicio de sesión de Meta, introduce las credenciales de tu cuenta de Facebook.

   En la página de la cuenta WhatsApp empresarial, selecciona Añadir número de WhatsApp teléfono. En la página Añadir número de WhatsApp teléfono, selecciona Iniciar el portal de Facebook. Aparecerá una nueva ventana de inicio de sesión desde Meta.
5. En la ventana de inicio de sesión de Meta, introduce las credenciales de tu cuenta de Facebook.
6. Como parte del proceso de registro, concedes a AWS End User Messaging Social acceso a tu cuenta WhatsApp empresarial (WABA). También permites que AWS End User Messaging Social te facture los mensajes. Elija Continuar.
7. Para la cuenta Meta Business, elige una cuenta Meta Business existente o crea una cuenta Meta Business.

   a. (Opcional) Si necesita crear una cuenta de Meta Business, siga estos pasos:
   b. En Nombre de la empresa, introduce el nombre de tu empresa.
   c. En el caso del sitio web o la página de perfil de la URL empresa, introduce el sitio web de tu empresa o, si tu empresa no tiene un sitio web, introduce el URL de tu página de redes sociales.
   d. En País, selecciona el país en el que se encuentra tu empresa.
   e. (Opcional) Selecciona Añadir dirección e introduce la dirección de tu empresa.
8. Elija Next (Siguiente).
9. En Elige una cuenta WhatsApp empresarial, selecciona una cuenta WhatsApp empresarial existente (WABA) o, si necesitas crear una cuenta, selecciona Crear una cuenta WhatsApp empresarial.

   En Crear o seleccionar un perfil WhatsApp empresarial, elige un perfil WhatsApp empresarial existente o Crea un perfil WhatsApp empresarial nuevo.
10. Elija Next (Siguiente).
11. En Crear un perfil empresarial, introduce la siguiente información:

    - En Nombre de cuenta WhatsApp empresarial, introduzca un nombre para su cuenta. Este campo no está orientado al cliente.

- En el caso del nombre para mostrar en el perfil de WhatsApp empresa, introduce el nombre que se mostrará a tus clientes cuando reciban un mensaje tuyo. Le recomendamos que utilice el nombre de su empresa como nombre para mostrar. Meta revisa el nombre y debe cumplir con las reglas WhatsApp de nombres visibles. Para usar un nombre de marca diferente del nombre de su empresa, debe haber una asociación publicada externamente entre su empresa y la marca. Esta asociación debe mostrarse en su sitio web y en la marca representada por el sitio web del nombre mostrado.

  Una vez que complete el registro, Meta revisará su nombre visible. Meta le envía un correo electrónico informándole si el nombre para mostrar ha sido aprobado o rechazado. Si rechazan tu nombre para mostrar, se reduce tu límite de mensajes por día y es posible que te desconecten de él WhatsApp.

  > **Important**
  >
  > Para cambiar tu nombre visible, tienes que crear un ticket con el soporte de Meta.

- En Timezone, elige la zona horaria en la que se encuentra la empresa.
- En Categoría, elige la categoría que mejor se adapte a tu empresa. Los clientes pueden ver tu categoría como parte de tu información de contacto.
- En Descripción de empresa, introduzca una descripción de su empresa. Los clientes pueden ver la descripción de tu empresa como parte de tu información de contacto.
- En Sitio web, introduce el sitio web de tu empresa. Los clientes pueden ver su sitio web como parte de su información de contacto.
- Elija Next (Siguiente).

12. En Añadir un número de teléfono para WhatsApp, introduce un número de teléfono para registrarte. Este número de teléfono se muestra a tus clientes cuando les envías un mensaje.
13. En Elige cómo quieres verificar tu número, selecciona Mensaje de texto o Llamada telefónica.
    - Cuando estés listo para recibir el código de verificación, selecciona Siguiente.
    - Introduce el código de verificación y, a continuación, selecciona Siguiente.
14. Una vez que se haya verificado tu número, puedes elegir Siguiente para cerrar la ventana desde Meta.
15. En el WhatsApp caso de una cuenta empresarial, expande Etiquetas (opcional) para añadir etiquetas a tu cuenta WhatsApp empresarial.

Las etiquetas son pares de claves y valores que, si lo desea, puede aplicar a AWS los recursos de para controlar el acceso o el uso. Elija Agregar etiqueta de nueva e introduzca un par clave-valor para adjuntarlo.

16. Una cuenta WhatsApp empresarial puede tener un mensaje y un destino de evento para registrar los eventos de la cuenta WhatsApp empresarial y de todos los recursos asociados a la cuenta WhatsApp empresarial. Para habilitar el registro de eventos en AmazonSNS, incluido el registro de la recepción de un mensaje de un cliente, debes activar la publicación de mensajes y eventos. Para obtener más información, consulte Destinos de mensajes y eventos en AWS End User Messaging Social.

> **Important**
>
> Para poder responder a los mensajes de los clientes, debes activar la publicación de mensajes y eventos.

En la sección Detalles del destino de los mensajes y los eventos, activa la publicación de eventos. Para AmazonSNS, elige un tema SNS estándar de New Amazon e introduce un nombre en el nombre del tema, o elige un tema SNS estándar de Amazon existente y elige un tema de la lista desplegable Topic arn.

17. En Números de teléfono:

    Para cada número de teléfono de la sección Números de WhtsApp teléfono:

    a. Para verificar el número de teléfono, ingresa el PIN código existente PIN o ingresa uno nuevo. Para restablecer un archivo perdido u olvidadoPIN, siga las instrucciones de la APIreferencia sobre cómo actualizar PIN en la nube de WhatsApp Business Platform.

    b. Para obtener una configuración adicional:

        i. Para la región de localización de datos (opcional), elige una de las regiones de Meta en la que almacenar tus datos en reposo. Para obtener más información sobre las políticas de privacidad de datos de Meta, consulte Privacidad y seguridad de los datos y Almacenamiento API local en la nube en la APIreferencia sobre la nube de WhatsApp Business Platform.

ii. Las etiquetas son pares de claves y valores que, si lo desea, puede aplicar a AWS los recursos de para controlar el acceso o el uso. Elija Agregar etiqueta de nueva e introduzca un par clave-valor para adjuntarlo.

18. Una cuenta WhatsApp empresarial puede tener un mensaje y un destino de evento para registrar los eventos de la cuenta WhatsApp empresarial y de todos los recursos asociados a la cuenta WhatsApp empresarial. Para habilitar el registro de eventos en AmazonSNS, incluido el registro de la recepción de un mensaje de un cliente, debes activar la publicación de mensajes y eventos. Para obtener más información, consulte Destinos de mensajes y eventos en AWS End User Messaging Social.

> **Important**
>
> Debes activar la publicación de mensajes y eventos para poder responder a los mensajes de los clientes.

En la sección Detalles del destino de los mensajes y del evento, activa la publicación de eventos. Para AmazonSNS, elige un tema SNS estándar de New Amazon e introduce un nombre en el nombre del tema, o elige un tema SNS estándar de Amazon existente y elige un tema de la lista desplegable Topic arn.

19. Para completar la configuración, selecciona Añadir número de teléfono.

## Siguientes pasos

Una vez que haya completado el registro, puede comenzar a enviar mensajes. Cuando esté listo para comenzar a enviar mensajes a gran escala, complete la verificación empresarial. Ahora que su cuenta WhatsApp empresarial y sus cuentas sociales de mensajería para usuarios AWS finales están vinculadas, consulte los siguientes temas:

- Obtén información sobre el destino del evento para registrar eventos y recibir mensajes entrantes.
- Obtén información sobre cómo crear plantillas de mensajes.
- Obtén información sobre cómo enviar un mensaje de texto o multimedia.
- Obtén información sobre cómo recibir un mensaje.
- Obtenga información sobre las cuentas comerciales oficiales para tener una marca de verificación verde junto a su nombre visible y aumentar el rendimiento de sus mensajes.

# WhatsApp Cuenta empresarial (WABA) en AWS End User Messaging Social

Una cuenta WhatsApp empresarial (WABA) permite a su empresa utilizar la plataforma WhatsApp empresarial para enviar mensajes directamente a sus clientes. Todas las tuyas WABAs forman parte de tu cartera de Meta Business. Una cuenta WhatsApp empresarial contiene los activos de cara a sus clientes, como el número de teléfono, las plantillas y la información de contacto empresarial. A solo WABA puede existir en uno Región de AWS. Para obtener más información sobre las cuentas WhatsApp empresariales, consulte la APIreferencia sobre las cuentas WhatsApp empresariales en la nube de WhatsApp Business Platform.

**Important**

Trabajando con Meta/ WhatsApp

- El uso de la solución WhatsApp empresarial está sujeto a los términos y condiciones de las condiciones del servicio WhatsApp empresarial, las condiciones de la solución WhatsApp empresarial, la política de mensajería WhatsApp empresarial, las directrices de WhatsApp mensajería y todos los demás términos, políticas o directrices que se incluyan en ellas como referencia (ya que cada uno de ellos puede actualizarse periódicamente).
- Meta o WhatsApp puede prohibir en cualquier momento el uso de la solución WhatsApp empresarial.
- Debe crear una cuenta WhatsApp empresarial (» WABA «) con Meta y WhatsApp.
- Debe crear una cuenta de administrador comercial con Meta y vincularla a la suyaWABA.
- Debe proporcionarnos el control de WABA la suya. Si lo solicita, le transferiremos el control de WABA su propiedad de manera razonable y oportuna utilizando los métodos que Meta ponga a nuestra disposición.
- En relación con su uso de la Solución WhatsApp empresarial, no enviará ningún contenido, información o dato que esté sujeto a medidas de protección o a limitaciones de distribución de conformidad con las leyes o reglamentos aplicables.
- WhatsAppLos precios de uso de la solución WhatsApp empresarial se encuentran en https://developers.facebook.com/docs/whatsapp/pricing.

Temas



# Vea una cuenta WhatsApp empresarial (WABA) en End User Messaging AWS Social

Sigue estas instrucciones para ver la que WABA está asociada a ti Cuenta de AWS.

1. Abra la consola social de mensajería para usuarios AWS finales en https://console.aws.amazon.com/social-messaging/.
2. En las cuentas comerciales, elija unWABA.
3. En la pestaña Números de teléfono, consulta tu número de teléfono, nombre para mostrar, índice de calidad y el número de conversaciones iniciadas por la empresa que te quedan por el día.

   En la pestaña Destinos del evento, consulta el destino del evento. Para editar el destino de tu evento, sigue las instrucciones que se indicanDestinos de mensajes y eventos en AWS End User Messaging Social.

   En la pestaña Plantillas, selecciona Administrar plantillas de mensajes para editar tus WhatsApp plantillas a través de Meta. Cada una WABA tiene un límite de 250 plantillas.

   En la pestaña Etiquetas, puede administrar las etiquetas WABA de sus recursos.

# Agregue una cuenta WhatsApp empresarial (WABA) en AWS End User Messaging Social

Agrega uno nuevo WABA a tu cuenta si ya tienes un perfil WhatsApp empresarial. Como parte de la creación de un nuevo, WABA debe agregar un número de teléfono alWABA.

- Para añadir uno nuevo WABA a tu cuenta, sigue los pasos que se indican enCómo empezar a usar AWS End User Messaging Social:

- En el paso 8, elige tu perfil WhatsApp empresarial y selecciona Crear una nueva cuenta WhatsApp empresarial.

# Descripción de los tipos de cuentas WhatsApp empresariales

Tu cuenta WhatsApp empresarial determina tu apariencia ante tus clientes. Cuando crees una WhatsApp cuenta, tu cuenta será una cuenta empresarial. WhatsApp tiene dos tipos de cuentas empresariales:

- Cuenta empresarial: WhatsApp verifica la autenticidad de todas las cuentas de la plataforma WhatsApp empresarial. Si una cuenta empresarial ha completado el proceso de verificación empresarial, los usuarios podrán ver el nombre de la empresa aunque no la hayan añadido a su libreta de direcciones. Esta función ayuda a los usuarios a identificar las cuentas empresariales verificadas en WhatsApp.
- Cuenta empresarial oficial: además de las ventajas de una cuenta empresarial, la cuenta empresarial oficial tiene una marca de verificación verde en el perfil y en los encabezados de los hilos de chat.

  La aprobación de una cuenta comercial WhatsApp oficial (OBA) exige acreditar que la empresa es conocida y reconocida por los consumidores, por ejemplo, mediante artículos, publicaciones en blogs o reseñas independientes. La aprobación de una no WhatsApp OBA está garantizada, incluso si la empresa proporciona la documentación requerida. El proceso de aprobación está sujeto a la revisión y aprobación de WhatsApp. WhatsApp no divulga públicamente los criterios específicos que utiliza para evaluar y aprobar las solicitudes de cuentas comerciales oficiales. Las empresas que lo WhatsApp OBA soliciten deben demostrar su reputación y reconocimiento, pero la aprobación final queda a su entera discreción WhatsApp.

Cuando cree una WhatsApp cuenta, su cuenta será una cuenta empresarial. Puedes proporcionar a tus clientes información sobre tu empresa, como el sitio web, la dirección y el horario. En el caso de las empresas que no hayan completado la verificación WhatsApp empresarial, el nombre para mostrar solo aparece en texto pequeño junto al número de teléfono en la vista de contactos, no en la lista de chats ni en el chat individual. Una vez finalizada la verificación de Meta Business, el nombre visible del WhatsApp remitente aparecerá en la lista de chats y en los hilos de chat individuales.

# Recursos adicionales de

- Para obtener más información sobre la cuenta empresarial y la cuenta empresarial oficial, consulte la APIreferencia sobre las cuentas empresariales en la nube de WhatsApp Business Platform.
- Para obtener más información sobre el proceso de verificación empresarial, consulte la APIreferencia sobre la verificación empresarial en la nube de WhatsApp Business Platform.

# Números de teléfono en AWS End User Messaging Social

Todas las cuentas WhatsApp empresariales contienen uno o más números de teléfono que se utilizan para verificar tu identidad WhatsApp y se utilizan como parte de tu identidad de envío. Puedes tener varios números de teléfono asociados a una cuenta WhatsApp empresarial (WABA) y usar cada número de teléfono para una marca diferente.

Temas



## Consideraciones sobre el número de teléfono para su uso con una cuenta WhatsApp empresarial

Al vincular un número de teléfono a tu cuenta WhatsApp empresarial (WABA), debes tener en cuenta lo siguiente:

- Los números de teléfono solo se pueden vincular a uno WABA a la vez.
- El número de teléfono se puede seguir utilizando para SMSMMS, y llamadas de voz.
- Cada número de teléfono tiene una calificación de calidad de Meta.

Puede obtener un número SMS de teléfono compatible mediante la mensajería SMS para el usuario AWS final de la siguiente manera:

1. Asegúrese de que el país o la región del número de teléfono sean compatibles con los dos SMS sentidos.
2. Solicita el número de teléfono. Según el país o la región, es posible que tengas que registrar el número de teléfono.

3. Habilita la SMS mensajería bidireccional para el número de teléfono. Una vez completada la configuración, SMS los mensajes entrantes se envían a un destino del evento.

# Añadir un número de teléfono a una cuenta WhatsApp empresarial (WABA)

Puedes añadir números de teléfono a una cuenta WhatsApp empresarial existente (WABA) o crear una nueva WABA para el número de teléfono.

## Requisitos previos

Antes de comenzar, se debe satisfacer los siguientes requisitos previos siguientes:

- El número de teléfono debe poder recibir un código de acceso de un solo uso SMS o un código de voz (). OTP Este es el número de teléfono que se añade a su. WABA
- El número de teléfono no debe estar asociado con ningún otroWABA.

## Agregar un número de teléfono a un WABA

Cómo añadir un número de teléfono nuevo a su número de teléfono WABA

1. Abra la consola social de mensajería para usuarios AWS finales en https://console.aws.amazon.com/social-messaging/.
2. Seleccione Cuentas empresariales y, a continuación, Añadir número de WhatsApp teléfono.
3. En la página Añadir número de WhatsApp teléfono, selecciona Iniciar el portal de Facebook. Aparecerá una nueva ventana de inicio de sesión desde Meta.
4. En la ventana de inicio de sesión de Meta, introduce las credenciales de tu cuenta de desarrollador de Meta y elige tu cartera de negocios.
5. Elige el WABA perfil WhatsApp empresarial al que quieres añadir el número de teléfono.
6. Elija Next (Siguiente).
7. En Añadir un número de teléfono para WhatsApp, introduce un número de teléfono para registrarte. Este número de teléfono se muestra a tus clientes cuando les envías un mensaje.
8. En Elige cómo quieres verificar tu número, selecciona Mensaje de texto o Llamada telefónica.
9. Cuando estés listo para recibir el código de verificación, selecciona Siguiente

10. Introduce el código de verificación y, a continuación, selecciona Siguiente. Una vez que se haya verificado tu número, puedes elegir Siguiente para cerrar la ventana desde Meta.
11. En Números de WhtsApp teléfono:

    a. Para verificar el número de teléfono, introduce el PIN código existente PIN o introduce uno nuevo. Para restablecer un archivo perdido u olvidadoPIN, siga las instrucciones de la sección Updating PIN in the WhatsApp Business Platform Cloud API Reference.

    b. Para obtener una configuración adicional:

        i. Para la región de localización de datos (opcional), elige una de las regiones de Meta en la que almacenar tus datos en reposo. Para obtener más información sobre las políticas de privacidad de datos de Meta, consulte Privacidad y seguridad de los datos y Almacenamiento API local en la nube en la APIreferencia sobre la nube de WhatsApp Business Platform.

        ii. Las etiquetas son pares de claves y valores que, si lo desea, puede aplicar a AWS los recursos de para controlar el acceso o el uso. Elija Agregar nueva etiqueta e introduzca un par clave-valor para adjuntarlo.

12. Una cuenta WhatsApp empresarial puede tener un mensaje y un destino de evento para registrar los eventos de la cuenta WhatsApp empresarial y de todos los recursos asociados a la cuenta WhatsApp empresarial. Para habilitar el registro de eventos en AmazonSNS, incluido el registro de la recepción de un mensaje de un cliente, activa la publicación de mensajes y eventos. Para obtener más información, consulte Destinos de mensajes y eventos en AWS End User Messaging Social.

    > **Important**
    >
    > Debes activar la publicación de mensajes y eventos para poder responder a los mensajes de los clientes.

    En la sección Detalles del destino de los mensajes y del evento, activa la publicación de eventos. Para AmazonSNS, elige Nuevo tema SNS estándar de Amazon e introduce un nombre en el nombre del tema, o elige Tema SNS estándar de Amazon existente y elige un tema de la lista desplegable Arn del tema.
13. Para completar la configuración, selecciona Añadir número de teléfono.

# Ver el estado de un número de teléfono

Para poder enviar mensajes en AWS End User Messaging Social, el estado del número de teléfono debe ser Activo.

1. Abra la consola social de mensajería para usuarios AWS finales en https://console.aws.amazon.com/social-messaging/.
2. Elija Phone numbers (Números de teléfono).
3. En la sección Números de teléfono, la columna Estado muestra el estado de cada número de teléfono.

> **Note**
>
> Si el estado de un número de teléfono es Configuración incompleta, puedes elegir el número de teléfono y, a continuación, elegir Completar la configuración para terminar de configurar el número de teléfono.

# Ver el identificador de un número de teléfono en AWS End User Messaging Social

Para poder enviar mensajes con el AWS CLI, necesitas el identificador del número de teléfono para identificar el número de teléfono que vas a utilizar al enviarlos.

1. Abra la consola social de mensajería para usuarios AWS finales en https://console.aws.amazon.com/social-messaging/.
2. Elija Phone numbers (Números de teléfono).
3. En la sección Números de teléfono, elija un número de teléfono.
4. La sección de detalles del número de teléfono contiene el identificador del número de teléfono.

# Aumente los límites de las conversaciones de mensajería en WhatsApp

Los límites de mensajería se refieren al número máximo de conversación que un número de teléfono de empresa puede abrir un número de teléfono de empresa en un periodo de 24 horas. Los números

de teléfono comerciales se limitan inicialmente a 250 conversaciones iniciadas por una empresa en un periodo de 24 horas. Meta puede aumentar este límite en función de la calificación de calidad de tus mensajes y del número de mensajes que envíes. Las conversaciones iniciadas por una empresa solo pueden utilizar plantillas de mensajes.

Cuando un cliente te envía un mensaje, se abre una ventana de servicio de 24 horas. Durante este tiempo, puede enviar todo tipo de mensajes.

Puedes aumentar tu límite de mensajes a 1000 mensajes por tu cuenta siguiendo estas pautas:

- El número de teléfono de tu empresa debe tener el estado Activo.
- Si el número de teléfono de tu empresa tiene una calificación de calidad baja, es posible que siga limitándose a 250 conversaciones iniciadas por la empresa por día hasta que su calificación de calidad mejore.
- Solicita la verificación empresarial. Si su empresa está aprobada, se analizará la calidad de los mensajes para determinar si su actividad de mensajería justifica aumentar su límite de mensajes. Según el análisis, Meta aprobará o rechazará tu solicitud de aumento del límite de mensajes.
- Solicita la verificación de identidad. Si completas la verificación de identidad y la confirmas, Meta aprobará un aumento del límite de mensajes.
- Abre 1000 o más conversaciones iniciadas por una empresa en un periodo de mudanza de 30 días utilizando una plantilla con una valoración de alta calidad. Cuando alcances el umbral de 1000 conversaciones, se analizará la calidad de tus mensajes para determinar si tu actividad de mensajería justifica aumentar tu límite de mensajes. El objetivo es enviar mensajes de alta calidad de forma coherente para aumentar el límite de mensajes.

Si has completado la verificación empresarial o la verificación de identidad, o has abierto 1000 o más conversaciones de negocios y todavía tienes un límite de 250 conversaciones iniciadas por empresas, envía una solicitud a Meta para que se amplíe el nivel de mensajes.

Si tu verificación empresarial o de identidad es rechazada, puedes aumentar tus probabilidades de obtener la aprobación enviando mensajes de alta calidad. Al enviar mensajes de alta calidad, conformes y opcionales, es posible que se reevalúen la actividad y la calidad de los mensajes, lo que podría provocar un aumento de las capacidades de mensajería aprobadas.

La puntuación de calidad de los mensajes WhatsApp se calcula en función de los comentarios e interacciones recientes de los usuarios, y se da más importancia a los datos más recientes. Esto ayuda a evaluar la calidad y la fiabilidad generales de tus mensajes en la plataforma.

El nivel de límites de mensajes aumenta

- 1000 conversaciones iniciadas por empresas
- 10 000 conversaciones iniciadas por empresas
- 100 000 conversaciones iniciadas por empresas
- Un número ilimitado de conversaciones iniciadas por la empresa

## Aumente el rendimiento de los mensajes en WhatsApp

El rendimiento de los mensajes es el número de mensajes entrantes y salientes por segundo (MPS) de un número de teléfono. De forma predeterminada, cada número de teléfono tiene un valor MPS de 80. Meta puede aumentar tu valor MPS a 1000 si cumple los siguientes requisitos:

- El número de teléfono debe poder enviar un número ilimitado de conversaciones iniciadas por la empresa
- El número de teléfono debe tener una calificación de calidad media o superior.

## Comprender la calificación de calidad de los números de teléfono en WhatsApp

Meta determina la calidad de tu número de teléfono y de tus mensajes. Tu puntuación de calidad de los mensajes se basa en la forma en que los clientes han recibido tus mensajes durante los últimos 7 días, y los mensajes más recientes tienen más peso. La puntuación de calidad de los mensajes se calcula en función de una combinación de señales de calidad de las conversaciones entre tú y tus WhatsApp usuarios. Estas señales incluyen los comentarios de los usuarios, como los bloqueos, los informes y las razones que los usuarios aducen cuando bloquean una empresa. Meta evalúa la calidad de tus mensajes en función de qué tan bien los reciben tus clientes y se centra en los comentarios e interacciones recientes. WhatsApp

WhatsApp Calificaciones de calidad de los números de teléfono

- Verde: alta calidad
- Amarillo: calidad media
- Rojo: calidad baja

WhatsApp Estado del número de teléfono

- Conectado: puedes enviar mensajes dentro de tu límite de mensajes.
- Marcado: la calidad de tu número de teléfono es baja y debes mejorarla. Si la calidad de tu teléfono no mejora en 7 días, el estado de tu número de teléfono cambiará a Conectado, pero el límite de conversaciones iniciadas por la empresa se reducirá un nivel.
- Restringido: has alcanzado el límite de conversaciones iniciadas por tu empresa durante el período actual de 24 horas, pero aún puedes responder a los mensajes entrantes de los clientes. Una vez transcurrido el período de 24 horas, puedes volver a enviar mensajes.

## Ver la calificación de la calidad de un número de teléfono

Sigue estas instrucciones para ver la calidad de un número de teléfono.

1. Abra la consola social de mensajería para usuarios AWS finales en https://console.aws.amazon.com/social-messaging/.
2. En las cuentas comerciales, elija unWABA.
3. En la pestaña Números de teléfono, consulta tu número de teléfono, nombre para mostrar, índice de calidad y el número de conversaciones iniciadas por la empresa que te quedan por el día.

# Uso de plantillas de mensajes en AWS End User Messaging Social

Puede usar plantillas de mensajes para los tipos de mensajes que usa con frecuencia, como boletines semanales o recordatorios de citas. Los mensajes de plantilla son el único tipo de mensaje que se puede enviar a los clientes que aún no te han enviado ningún mensaje o que no te lo han enviado en las últimas 24 horas.

Meta asigna a cada plantilla una calificación de calidad y un estado. La calificación de calidad afecta al estado de la plantilla y reduce el ritmo o la tasa de envío de la plantilla.

Las plantillas se asocian a tu cuenta WhatsApp empresarial (WABA), se gestionan a través del WhatsApp administrador y son revisadas por WhatsApp él.

Puedes enviar los siguientes tipos de plantillas:

- Basado en texto
- Basado en medios
- Mensaje interactivo
- Basado en la ubicación
- Plantillas de autenticación con botones de contraseña de un solo uso
- Plantillas de mensajes multiproducto

Meta proporciona plantillas de muestra previamente aprobadas. Para obtener más información, consulte Ejemplos de plantillas de mensajes.

Para obtener más información sobre los tipos de plantillas de mensajes, consulte la plantilla de mensajes en la APIreferencia sobre la nube de WhatsApp Business Platform.

## Uso de plantillas de mensajes con WhatsApp Manager

Utilice el WhatsAppAdministrador para crear, modificar o comprobar el estado de una plantilla.

1. Abra la consola social de mensajería para usuarios AWS finales en https://console.aws.amazon.com/social-messaging/.
2. Elija una cuenta empresarial y, a continuación, elija unaWABA.

3. En la pestaña Plantillas de mensajes, selecciona Administrar plantillas de mensajes. El WhatsAppadministrador se abre en una nueva ventana en la que puedes gestionar tus plantillas seleccionando Plantillas de mensajes.

## Siguientes pasos

Una vez que hayas creado o editado una plantilla, debes enviarla para su revisión WhatsApp. La revisión de Meta puede tardar hasta 24 horas. Meta envía un correo electrónico al administrador de tu Business Manager y actualiza el estado de la plantilla en el WhatsApp administrador. Usa el WhatsAppadministrador para comprobar el estado de tu plantilla.

## Entender el ritmo de las plantillas WhatsApp

El ritmo de las plantillas es un método, utilizado por Meta, que permite que los clientes puedan opinar anticipadamente sobre las plantillas nuevas o modificadas. Identifica y detiene las plantillas que reciben poca participación o comentarios, lo que te da tiempo para ajustar el contenido de la plantilla antes de enviarla a demasiados clientes. Esto reduce el riesgo de comentarios negativos de los clientes sobre el negocio. Por ejemplo, si demasiados clientes «bloquean» tu mensaje o si tu plantilla tiene tasas de lectura bajas, es posible que se reduzca la calificación de calidad de la plantilla.

El ritmo de las plantillas afecta a las plantillas recién creadas, a las que no se han pausado y a las que no han obtenido una calificación de alta calidad. El ritmo de las plantillas suele comenzar con un historial previo de plantillas de baja calidad o en pausa. Cuando se sigue el ritmo de una plantilla, los mensajes que utilizan esa plantilla se envían normalmente hasta un cierto umbral determinado por Meta. Después de eso, los mensajes subsiguientes se retienen para dar tiempo a los comentarios de los clientes. Si los comentarios son positivos, se amplía el ritmo de la plantilla. Si los comentarios son negativos, se reduce el ritmo de la plantilla, lo que te permite ajustar el contenido de la plantilla. Para obtener más información, consulte el tema sobre el ritmo de las plantillas en la referencia sobre la nube WhatsApp API de Business Platform.

## Obtenga comentarios sobre el estado reducido de una plantilla con Manager WhatsApp

Meta proporciona información sobre el motivo por el que se ha reducido el estado de una plantilla. Usa los comentarios de Meta para editar la plantilla y enviarla para su reaprobación, usa una plantilla diferente o cambia el comportamiento de tu solicitud. Si editas la plantilla de mensaje y se vuelve a

aprobar, su calificación de calidad mejorará gradualmente siempre y cuando no reciba comentarios negativos frecuentes o índices de lectura bajos.

1. Abre la consola social de mensajería para usuarios AWS finales en https://console.aws.amazon.com/social-messaging/.
2. Elija una cuenta empresarial y, a continuación, elija unaWABA.
3. En la pestaña Plantillas de mensajes, selecciona Administrar plantillas de mensajes. El WhatsAppadministrador se abre en una ventana nueva.
4. Selecciona Plantillas de mensajes y coloca el cursor sobre la plantilla. Debería aparecer una descripción emergente con comentarios sobre los motivos por los que se ha reducido la valoración.

## Entender el estado y la calificación de calidad de una plantilla en WhatsApp

A cada plantilla de mensaje se le asigna una calificación de calidad basada en el uso, los comentarios de los clientes y la participación de los clientes. Solo se puede usar una plantilla si el estado es Activo, pero la calidad determina el ritmo de la plantilla. Si una plantilla de mensaje recibe constantemente valoraciones negativas o tiene un bajo nivel de interacción, se producirá un cambio en el estado de la plantilla.

Meta cambia automáticamente el estado o la calificación de calidad de una plantilla en función de la participación y los comentarios negativos o positivos. Si el estado de tu plantilla cambia, recibirás una notificación del WhatsApp gerente, un correo electrónico y una notificación del evento. Usa el WhatsAppadministrador para comprobar el estado de la plantilla.

Si su plantilla es rechazada por WhatsApp, puede editarla y volver a enviarla para su aprobación o presentar una apelación ante WhatsApp ella. Para obtener más información, consulte la APIreferencia sobre apelaciones en la nube WhatsApp de Business Platform.

| Estado de la plantilla | Calificación de calidad | Significado |
| --- | --- | --- |
| Revisión | | Se está revisando la plantilla del mensaje. Esto puede tardar hasta 24 horas en completarse. |

| Estado de la plantilla | Calificación de calidad | Significado |
| --- | --- | --- |
| Rechazada | | La plantilla del mensaje se ha rechazado y puede presentar una apelación. |
| Activo | Pendiente | La plantilla de mensajes no ha recibido comentarios de calidad ni información sobre la tasa de lectura de los clientes, pero se puede seguir utilizando para enviar mensajes. |
| Activo | Alta | La plantilla de mensajes ha recibido pocos o ningún comentario negativo de los clientes y se puede utilizar para enviar mensajes. |
| Activo | Medio | La plantilla de mensaje ha recibido valoraciones negativas por parte de los clientes o ha registrado bajas tasas de lectura, por lo que es posible que esté en pausa o desactivada. |

| Estado de la plantilla | Calificación de calidad | Significado |
| --- | --- | --- |
| Activo | Baja | La plantilla de mensaje ha recibido comentarios negativos de los clientes o un índice de lectura bajo. Se pueden usar plantillas de mensajes con este estado, pero corren el riesgo de pausarse o deshabilitarse.<br><br>Cuando una plantilla pasa al estado Active-Low, su envío se detiene. La primera pausa dura tres horas, la segunda seis horas y la siguiente desactiva la plantilla. |
| Paused | | La plantilla de mensaje se ha detenido debido a los comentarios negativos recurrentes de los clientes o a las bajas tasas de lectura. |
| Deshabilitad | | La plantilla de mensajes se ha desactivado debido a los comentarios negativos recurrentes de los clientes. |
| Apelación solicitada | | Se ha solicitado una apelación . |

# Motivos por los que se rechaza una plantilla en WhatsApp

Si Meta revisa y rechaza tu plantilla de mensaje, recibirás un correo electrónico explicándote por qué la rechazó. Puedes apelar el rechazo o modificar tu plantilla de mensaje. Estas son algunas de las razones más comunes por las que Meta puede rechazar una plantilla de mensaje:

- Los parámetros variables contienen caracteres especiales, como #, $ o%.
- Faltan parámetros variables, tienen corchetes rizados que no coinciden o no son secuenciales.
- La plantilla del mensaje contiene contenido que infringe la Política WhatsApp comercial o la Política empresarial. WhatsApps

Para obtener más información, consulta la sección sobre los motivos de rechazo más frecuentes en la APIreferencia sobre la nube de WhatsApp Business Platform.

# Destinos de mensajes y eventos en AWS End User Messaging Social

El destino de un evento es un SNS tema de Amazon al que se envían los WhatsApp eventos. Cuando activas la publicación de eventos en un SNS tema de Amazon, todos los eventos de envío y recepción se envían al SNS tema de Amazon. Usa los eventos para monitorear, rastrear y analizar el estado de los mensajes salientes y las comunicaciones entrantes con los clientes.

Cada cuenta WhatsApp empresarial (WABA) puede tener un destino para el evento. Todos los eventos de todos los recursos asociados a la cuenta WhatsApp empresarial se registran en el destino del evento. Por ejemplo, puede tener una cuenta WhatsApp empresarial con tres números de teléfono asociados y todos los eventos de esos números de teléfono se registran en el único destino del evento.

Temas



## Agregue un mensaje y un destino de evento a AWS End User Messaging Social

Al activar la publicación de mensajes y eventos, todos los eventos generados por tu cuenta WhatsApp empresarial (WABA) se envían al SNS tema de Amazon. Esto incluye los eventos de cada número de teléfono asociado a una cuenta WhatsApp empresarial. WABAPuedes tener un SNS tema de Amazon asociado a él.

### Requisitos previos

Antes de comenzar, se deben cumplir los siguientes requisitos previos.

- (Opcional) Para usar un SNS tema de Amazon cifrado con AWS KMS claves, debes conceder permisos a AWS End User Messaging Social para la política de claves existente.

## Añade un mensaje y un destino para el evento

1. Abra la consola social de mensajería para usuarios AWS finales en https://console.aws.amazon.com/social-messaging/.
2. Elija una cuenta empresarial y, a continuación, elija unaWABA.
3. En la pestaña Destino del evento, selecciona Editar destino.
4. Para activar el destino de un evento, selecciona Activar.
5. Para enviar tus eventos a un nuevo SNS destino de Amazon, selecciona Nuevo tema de SNS stand e introduce un nombre en Nombre del tema. El SNS tema de Amazon se crea con permisos para permitir que el usuario AWS final de Messaging Social acceda al tema.

   Para enviar tus eventos a un SNS destino de Amazon existente, selecciona Tema SNS estándar existente y elige un tema del formulario Topic arn. Tienes que aplicar los siguientes permisos al SNS tema de Amazon:

   ```
   {
       "Effect": "Allow",
       "Principal": {
           "Service": [
             "social-messaging.amazonaws.com"
           ]
          },
       "Action": "sns:Publish",
       "Resource": "arn:{PARTITION}:sns:{REGION}:{ACCOUNT}:{TOPIC_NAME}"
   }
   ```

6. Elija Guardar cambios.

## Políticas de SNS temas cifrados de Amazon

Puedes utilizar SNS los temas de Amazon cifrados con AWS KMS claves de para obtener un nivel de seguridad adicional. Esta seguridad adicional puede resultar útil si la aplicación maneja datos privados o confidenciales. Para obtener más información sobre el cifrado de SNS temas de Amazon con AWS KMS claves de, consulte Habilitar la compatibilidad entre los orígenes de eventos de AWS los servicios de y los temas cifrados en la Guía para desarrolladores de Amazon Simple Notification Service.

La instrucción del ejemplo utiliza las `SourceArn` condiciones, opcionales pero recomendadas, `SourceAccount` para evitar el confuso problema de los diputados y solo la cuenta del propietario de AWS End User Messaging Social tiene acceso. Para obtener más información sobre el problema del diputado confuso, consulte El problema del diputado confuso en la guía del IAM usuario.

La clave que utilice debe ser simétrica. Los SNS temas cifrados de Amazon Amazon no admiten AWS KMS claves de asimétricas.

La política de claves se debe modificar para permitir que el usuario AWS final de Messaging Social utilice la clave. Siga las instrucciones de la Guía para AWS Key Management Service desarrolladores sobre cómo cambiar una política clave para añadir los siguientes permisos a la política clave existente:

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "social-messaging.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "{ACCOUNT_ID}"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:{PARTITION}:social-messaging:{REGION}:{ACCOUNT_ID}:*"
        }
     }
}
```

## Siguientes pasos

Una vez que haya configurado su SNS tema de Amazon, debe suscribir un punto de enlace al tema. El punto de enlace comenzará a recibir todos los mensajes publicados en el tema asociado. Para obtener más información sobre la suscripción a un tema, consulta Suscribirse a un SNS tema de Amazon en la Guía para SNSdesarrolladores de Amazon.

# Formato de mensaje y evento en AWS End User Messaging Social

El JSON objeto de un evento contiene el encabezado y la WhatsApp JSON carga útil del AWS evento. Para obtener una lista de la carga útil y los valores de las JSON WhatsApp notificaciones, consulte la referencia de carga útil de notificaciones de Webhooks y el estado de los mensajes en la referencia sobre la nube de WhatsApp Business Platform. API

## AWS Encabezado del evento social de mensajería para usuarios finales

El JSON objeto de un evento contiene el encabezado del AWS evento y WhatsApp JSON. El encabezado contiene los AWS identificadores ARNs de su cuenta WhatsApp empresarial (WABA) y su número de teléfono.

```
{
  "MetaWabaIds": [
    {
      "wabaId": "1234567890abcde",
      "arn": "arn:aws:social-messaging:us-
east-1:123456789012:waba/fb2594b8a7974770b128a409e2example"
    }
  ],
  "MetaPhoneNumberIds": [
    {
      "metaPhoneNumberId": "abcde1234567890",
      "arn": "arn:aws:social-messaging:us-east-1:123456789012:phone-number-
id/976c72a700aac43eaf573ae050example"
    }
  ]
}
{
//WhatsApp notification payload
}
```

En el evento de ejemplo anterior:

- *1234567890abcde* es el WABA identificador de Meta.
- *abcde1234567890* es el identificador del número de teléfono de Meta.
- *fb2594b8a7974770b128a409e2example* es el ID de la cuenta WhatsApp empresarial (WABA).
- *976c72a700aac43eaf573ae050example* es el identificador del número de teléfono.

# Ejemplo WhatsApp JSON de recepción de un mensaje de texto

A continuación se muestra el registro de eventos de un mensaje de texto entrante de WhatsApp. El JSON es generado por WhatsApp. Para obtener una lista de los campos y su significado, consulte la referencia sobre la carga útil de notificaciones de Webhooks en la referencia sobre la nube API de WhatsApp Business Platform.

```
{
//AWS End User Messaging Social header
}
{
  "id": "365731266123456",
  "changes": [
    {
      "value": {
        "messaging_product": "whatsapp",
        "metadata": {
          "display_phone_number": "12065550100",
          "phone_number_id": "321010217760100"
        },
        "contacts": [
          {
            "profile": {
              "name": "Diego"
            },
            "wa_id": "12065550102"
          }
        ],
        "messages": [
          {
            "from": "14255550150",
            "id":
 "wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0RjVGRkexample",
            "timestamp": "1723506035",
            "text": {
              "body": "Hi"
            },
            "type": "text"
          }
        ]
      },
      "field": "messages"
    }
```

```
  ]
}
```

## Ejemplo de recepción WhatsApp JSON de un mensaje multimedia

A continuación se muestra el registro de eventos de un mensaje multimedia entrante. Para recuperar el archivo multimedia, utilice el GetWhatsAppMessageMedia API comando. Para ver una lista de los campos y su significado, consulta la referencia sobre la carga útil de notificaciones de Webhooks

```
{
//AWS End User Messaging Social header
}
{
  "id": "365731266123456",
  "changes": [
    {
      "value": {
        "messaging_product": "whatsapp",
        "metadata": {
          "display_phone_number": "12065550100",
          "phone_number_id": "321010217760100"
        },
        "contacts": [
          {
            "profile": {
              "name": "Diego"
            },
            "wa_id": "12065550102"
          }
        ],
        "messages": [
          {
            "from": "14255550150",
            "id":
 "wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0RjVGRkexample",
            "timestamp": "1723506230",
            "type": "image",
            "image": {
              "mime_type": "image/jpeg",
              "sha256": "BTD0xlqSZ7l02o+/upusiNStlEZhA/urkvKf143Uqjk=",
              "id": "530339869524171"
            }
          }
```

```
        ]
      },
      "field": "messages"
    }
  ]
}
```

# WhatsApp mensaje de estado

Cuando se envía un mensaje, se reciben actualizaciones de estado. Debe activar el registro de eventos para recibir estas notificaciones, consulteDestinos de mensajes y eventos en AWS End User Messaging Social.

## Estados del mensaje de estado

La siguiente tabla contiene los estados de los mensajes de estado

| Nombre del estado | Descripción |
|---|---|
| eliminado | El cliente ha eliminado el mensaje y tú también deberías eliminarlo si se ha descargado en tu servidor. |
| entregado | El mensaje se envió correctamente al cliente. |
| error | No se pudo enviar el mensaje. |
| leer | El cliente leyó el mensaje. Este estado solo se envía si el cliente tiene activada la función de lectura de recibos. |
| enviado | El mensaje se ha enviado pero aún está en tránsito. |
| Advertencia | El mensaje contiene un elemento que no está disponible o que no existe. |

# Recursos adicionales de

Para obtener más información, consulte el artículo sobre el estado del mensaje en la APIreferencia sobre la nube de WhatsApp Business Platform.

# Cargar archivos multimedia para enviarlos con WhatsApp

Al enviar o recibir un archivo multimedia, debe almacenarse en un bucket Amazon S3. El bucket de Amazon S3 debe estar en la misma cuenta de Amazon S3 Cuenta de AWS y debe estar en la Región de AWS misma cuenta de WhatsApp empresa (WABA). Estas instrucciones muestran cómo crear un bucket de Amazon S3, cargar un archivo y URL compilarlo en el archivo. Para obtener más información sobre los comandos de Amazon S3, consulte Usar comandos de alto nivel (s3) con AWS CLI. Para obtener más información sobre la configuración AWS CLI, consulte Configurar el AWS CLI en la Guía del AWS Command Line Interface usuario y Crear un depósito y Cargar objetos en la Guía del usuario de Amazon S3.

También puede crear un archivo multimedia prefirmado URL. Con un prefirmadoURL, puede conceder acceso a los objetos por tiempo limitado y cargarlos sin necesidad de que un tercero tenga credenciales o permisos AWS de seguridad.

Para crear un bucket de Amazon S3, utilice el comando create-bucket AWS CLI . En la línea de comandos, escriba el comando siguiente.

```
aws s3api create-bucket --region 'us-east-1' --bucket BucketName
```

En el comando anterior:

- Reemplazar *us-east-1* con el Región de AWS que WABA está el tuyo.
- Reemplazar *BucketName* por el nombre del nuevo bucket.

Para copiar un archivo en el bucket de Amazon S3, utilice el AWS CLI comando cp. En la línea de comandos, escriba el comando siguiente.

```
aws s3 cp SourceFilePathAndName s3://BucketName/FileName
```

En el comando anterior:

- Reemplazar *SourceFilePathAndName* por la ruta del archivo y el nombre del archivo que desee copiar.
- Reemplazar *BucketName* por el nombre del bucket.
- Reemplazar *FileName* con el nombre que se utilizará para el archivo.

La URL que se debe usar al enviar es:

```
s3://BucketName/FileName
```

Para crear una prefirmada URL, sustituya la *user input placeholders* por su propia información.

```
aws s3 presign s3://amzn-s3-demo-bucket1/mydoc.txt --expires-in 604800 --region af-south-1 --endpoint-url https://s3.af-south-1.amazonaws.com
```

La devolución URL será: `https://amzn-s3-demo-bucket1.s3.af-south-1.amazonaws.com/mydoc.txt?{Headers}`

# Tipos y tamaños de archivos multimedia compatibles en WhatsApp

Al enviar o recibir un mensaje multimedia, el tipo de archivo debe ser compatible y debe tener un tamaño inferior al máximo. Para obtener más información, consulte los tipos de medios compatibles en la APIreferencia sobre la nube de WhatsApp Business Platform.

## Tipos de archivo multimedia

Formatos de audio

| Tipo de audio | Extensión | MIMETipo | Tamaño máximo |
|---|---|---|---|
| AAC | .aac | audio/aac | 16 MB |
| AMR | amr | audio/amr | 16 MB |
| MP3 | .mp3 | audio/mpeg | 16 MB |
| MP4Audio | m4a | audio/mp4 | 16 MB |
| OGGAudio | .ogg | audio/ogg | 16 MB |

## Formatos de documento

| Tipo de documento | Extensión | MIMETipo | Tamaño máximo |
|---|---|---|---|
| Texto | .texto | text/plain | 100 MB |
| Microsoft Excel | .xls, .xlsx | application/vnd.ms-excel, application/vnd.openxmlformats-officedocument.spreadsheetml.sheet | 100 MB |
| Microsoft Word | .doc, .docx | application/msword, application/vnd.openxmlformats-officedocument.wordprocessingml.document | 100 MB |
| Microsoft PowerPoint | .ppt, .pptx | application/vnd.ms-powerpoint, application/vnd.openxmlformats-officedocument.presentationml.presentation | 100 MB |
| PDF | .pdf | application/pdf | 100 MB |

## Formatos de imagen

| Tipo de imagen | Extensión | MIMETipo | Tamaño máximo |
|---|---|---|---|
| JPEG | .jpeg | image/jpeg | 5 MB |
| PNG | .png | image/png | 5 MB |

### Formatos de stickers

| Tipo de pegatina | Extensión | MIMETipo | Tamaño máximo |
|---|---|---|---|
| Pegatina animada | .webp | image/webp | 500 KB |
| Adhesivo estático | .webp | image/webp | 100 KB |

### Formatos de video

| Tipo de video | Extensión | MIMETipo | Tamaño máximo |
|---|---|---|---|
| 3 GPP | .3gp | vídeo/3gp | 16 MB |
| MP4Vídeo | .mp4 | vídeo/mp4 | 16 MB |

# WhatsApp tipos de mensajes

En este tema se enumeran los tipos de mensajes admitidos y una descripción de su uso. Para obtener una lista de los tipos de mensajes, consulte la APIreferencia sobre los mensajes en la nube de WhatsApp Business Platform.

| Tipo de mensaje | Descripción |
|---|---|
| Texto | Envíe un mensaje de texto o URL a su cliente |
| Medios | Envía un archivo de audio, documento, imagen, pegatina o vídeo. También puede enviar enlaces del archivo multimedia. |
| Reaction | Envía un emoji como reacción a un mensaje, como un pulgar hacia arriba |
| Plantilla | Enviar una plantilla de mensajes |
| Ubicación | Enviar una ubicación |
| Contactos | Enviar una tarjeta de contacto |
| Interactivo | Enviar un mensaje interactivo |

## Recursos adicionales de

Para obtener una lista de los objetos de los WhatsApp mensajes, consulte la APIreferencia sobre los mensajes en la nube de WhatsApp Business Platform.

# Envío de mensajes a través WhatsApp de AWS End User Messaging Social

Antes de enviar un mensaje, debe haber completado la configuración WABA y el usuario debe haber optado por recibir sus mensajes, consulte. Obtener permiso

Cuando un usuario le envía un mensaje, se activa o actualiza un temporizador de 24 horas denominado ventana de servicio al cliente. Todos los tipos de mensajes, excepto los mensajes de plantilla, solo se pueden enviar a un usuario cuando hay una ventana de servicio al cliente abierta entre usted y el usuario. Los mensajes de plantilla se pueden enviar a un usuario en cualquier momento, siempre que el usuario haya optado por recibir mensajes tuyos.

Para cada mensaje que envíe o reciba, se generará un estado de mensaje que se enviará al destino del evento. Si su cliente no se ha registrado, se generará WhatsApp un evento con un estado de mensaje `defail`. Debes activar un destino de mensajes y eventos para recibir el estado del mensaje.

> **Important**
>
> Trabajando con Meta/ WhatsApp
>
> - El uso de la solución WhatsApp empresarial está sujeto a los términos y condiciones de las condiciones del servicio WhatsApp empresarial, las condiciones de la solución WhatsApp empresarial, la política de mensajería WhatsApp empresarial, las directrices de WhatsApp mensajería y todos los demás términos, políticas o directrices que se incluyan en ellas como referencia (ya que cada uno de ellos puede actualizarse periódicamente).
> - Meta o WhatsApp puede prohibir en cualquier momento el uso de la solución WhatsApp empresarial.
> - En relación con su uso de la Solución WhatsApp empresarial, no presentará ningún contenido, información o dato que esté sujeto a medidas de protección o a limitaciones de distribución de conformidad con las leyes o reglamentos aplicables.

Temas

# Ejemplo de envío de una plantilla de mensaje en AWS End User Messaging Social

En el siguiente ejemplo se muestra cómo usar una plantilla de para enviar un mensaje al cliente mediante AWS CLI. Para obtener más información sobre cómo configurar el AWS CLI, consulte Configurar el AWS CLI en la Guía del AWS Command Line Interface usuario.

```
aws socialmessaging send-whatsapp-message --message
 '{"messaging_product":"whatsapp","to":"'{PHONE_NUMBER}'","type":"template","template":
{"name":"statement","language":{"code":"en_US"},"components":
[{"type":"body","parameters":[{"type":"text","text":"1000"}]}]}}' --origination-phone-
number-id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version v20.0
```

En el comando anterior, haga lo siguiente.

- Reemplazar *{PHONE_NUMBER}* con el número de teléfono de sus clientes.
- Reemplazar *{ORIGINATION_PHONE_NUMBER_ID}* con el identificador de tu número de teléfono.

# Ejemplo de envío de un mensaje multimedia en AWS End User Messaging Social

En el siguiente ejemplo se muestra cómo enviar un mensaje multimedia a su cliente mediante AWS CLI. Para obtener más información sobre la configuración del AWS CLI, consulte Configurar el AWS CLI en la Guía del AWS Command Line Interface usuario. Para obtener una lista de los tipos de archivos multimedia compatibles, consulteTipos y tamaños de archivos multimedia compatibles en WhatsApp.

1. Cargue el archivo multimedia en un bucket de Amazon S3, consulteCargar archivos multimedia para enviarlos con WhatsApp.
2. Cargue el archivo multimedia WhatsApp mediante el post-whatsapp-message-mediacomando. Al completarlo correctamente, el comando devolverá el *{MEDIA_ID}* que es necesaria para enviar el mensaje multimedia.

   ```
   aws socialmessaging post-whatsapp-message-media --origination-
   phone-number-id {ORIGINATION_PHONE_NUMBER_ID}  --source-s3-file
    bucketName={BUCKET},key={MEDIA_FILE}
   ```

En el comando anterior, haga lo siguiente.

- Reemplazar *{ORIGINATION_PHONE_NUMBER_ID}* con el identificador de tu número de teléfono.
- Reemplazar *{BUCKET}* con el nombre del bucket de Amazon S3.
- Reemplazar *{MEDIA_FILE}* con el nombre del archivo multimedia.

También puede cargarlo mediante una URL prefirmada utilizando `--source-s3-presigned-url` en lugar de`--source-s3-file`. Debe añadirlo `Content-Type` en el campo de encabezados. Si usa ambos, `InvalidParameterException` se devuelve un.

```
--source-s3-presigned-url headers={"Name":"Value"},url=https://BUCKET.s3.REGION/
MEDIA_FILE
```

3. Utilice el send-whatsapp-messagecomando para enviar el mensaje multimedia.

```
aws socialmessaging send-whatsapp-message --message
 '{"messaging_product":"whatsapp","to":"'{PHONE_NUMBER}'","type":"image","image":
{"id":"'{MEDIA_ID}'"}}' --origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID}
 --meta-api-version v20.0
```

En el comando anterior, haga lo siguiente.

- Reemplazar *{PHONE_NUMBER}* con el número de teléfono de sus clientes.
- Reemplazar *{ORIGINATION_PHONE_NUMBER_ID}* con el identificador de tu número de teléfono.
- Reemplazar *{MEDIA_ID}* con el ID de medios que obtuvo en el paso anterior.

4. Cuando ya no necesite el archivo multimedia, puede eliminarlo WhatsApp mediante el delete-whatsapp-message-mediacomando. De este modo solo se elimina el archivo multimedia de WhatsApp su bucket de Amazon S3, no de su bucket.

```
aws socialmessaging delete-whatsapp-message-media --media-id {MEDIA_ID} --
origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID}
```

En el comando anterior, haga lo siguiente.

- Reemplazar *{ORIGINATION_PHONE_NUMBER_ID}* con el identificador de tu número de teléfono.
- Reemplazar *{MEDIA_ID}* con el identificador multimedia.

# Responder a un mensaje recibido en AWS End User Messaging Social

Para poder recibir un mensaje de texto o multimedia, debe haber completado la configuración WABA y configurar el destino del evento. Cuando recibes un mensaje entrante, un evento se guarda en el SNS tema Amazon de destino del evento. Tienes que suscribirte al punto final de SNS temas de Amazon para recibir una notificación.

Para ver un ejemplo de un mensaje multimedia recibido, consulteEjemplo de recepción WhatsApp JSON de un mensaje multimedia. Para obtener más información sobre la configuración del AWS CLI, consulte Configurar el AWS CLI en la Guía del AWS Command Line Interface usuario. Para ver una lista de los tipos de archivos multimedia admitidos, consulteTipos y tamaños de archivos multimedia compatibles en WhatsApp.

> **Important**
>
> Para recibir mensajes entrantes, debe tener habilitados los destinos de los eventosWABA, consulteAgregue un mensaje y un destino de evento a AWS End User Messaging Social.

## Ejemplo de cómo cambiar el estado de un mensaje para que se lea con AWS End User Messaging Social

Puede configurar el estado del mensaje para que muestre `read` al usuario final dos marcas de verificación azules en la pantalla.

```
aws socialmessaging send-whatsapp-message --message
 '{"messaging_product":"whatsapp","message_id":"'{MESSAGE_ID}'","status":"read"}' --
origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version v20.0
```

En el comando anterior, haga lo siguiente.

- Reemplazar *{ORIGINATION_PHONE_NUMBER_ID}* con el identificador de tu número de teléfono.
- Reemplazar *{MESSAGE_ID}* con el identificador único del mensaje. Usa el valor del `id` campo en el objeto de mensaje del SNS tema de Amazon.

# Ejemplo de cómo responder a un mensaje con una reacción en AWS End User Messaging Social

Puedes añadir una reacción al mensaje, como un visto bueno hacia arriba.

```
aws socialmessaging send-whatsapp-message --message
 '{"messaging_product":"whatsapp","recipient_type":"individual","to":"'{PHONE_NUMBER}'","type":
 "reaction","reaction": {"message_id": "'{MESSAGE_ID}'","emoji":"\uD83D\uDC4D"}}' --
origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version v20.0
```

En el comando anterior, haga lo siguiente.

- Reemplazar *{PHONE_NUMBER}* con el número de teléfono de sus clientes.
- Reemplazar *{MESSAGE_ID}* con el identificador único del mensaje. Usa el valor del `id` campo en el objeto de mensaje del SNS tema de Amazon.
- Reemplazar *{ORIGINATION_PHONE_NUMBER_ID}* con el identificador de tu número de teléfono.

# Descargar un archivo multimedia desde WhatsApp Amazon S3

Para recuperar un archivo multimedia y guardarlo en un bucket de Amazon S3, utilice el get-whatsapp-message-mediacomando.

```
aws socialmessaging get-whatsapp-message-media --media-id {MEDIA_ID} --
origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID} --destination-s3-file
 bucketName={BUCKET},key=inbound_
{
    "mimeType": "image/jpeg",
    "fileSize": 78144
}
```

En el comando anterior, haga lo siguiente.

- Reemplazar *{BUCKET}* con el nombre del bucket de Amazon S3.
- Reemplazar *{MEDIA_ID}* con el valor del campo de identificación del evento recibido. Para ver un ejemplo de un evento multimedia entrante, consulteEjemplo de recepción WhatsApp JSON de un mensaje multimedia.
- Reemplazar *{ORIGINATION_PHONE_NUMBER_ID}* con el identificador de su número de teléfono.

Para recuperar el contenido del bucket de Amazon S3, utilice el siguiente comando:

```
aws s3 cp s3://{BUCKET}/inbound_{MEDIA_ID}.jpeg
```

En el comando anterior, haga lo siguiente.

- Reemplazar *{BUCKET}* con el nombre del bucket de Amazon S3.
- Reemplazar *{MEDIA_ID}* con el MEDIA _ID que obtuvo en el paso anterior.

# Ejemplo de respuesta a un mensaje con una lectura y una reacción

En este ejemplo, tu cliente, Diego, te ha enviado un mensaje diciendo «Hola» y tú le respondes con un recibo leído y un emoji con la mano.

## Requisitos previos

Debes haber configurado un SNS tema de Amazon de destino para eventos y suscribirte a uno de los puntos finales del tema para recibir una notificación de que Diego ha enviado un mensaje.

## ¿Respondiendo

1. Cuando se recibe el mensaje de Diego, se publica un evento en los puntos finales del tema. A continuación se muestra un fragmento de lo que se publica en el tema.

   > **Note**
   >
   > El hecho de que Diego haya iniciado la conversación no se descuenta de las conversaciones iniciadas por su empresa.

```
{
  "MetaWabaIds": [
    {
      "wabaId": "1234567890abcde",
      "arn": "arn:aws:social-messaging:us-east-1:123456789012:waba/
fb2594b8a7974770b128a409e2example"
    }
  ],
  "MetaPhoneNumberIds": [
```

```
    {
      "metaPhoneNumberId": "abcde1234567890",
      "arn": "arn:aws:social-messaging:us-east-1:123456789012:phone-number-
id/976c72a700aac43eaf573ae050example"
    }
  ]
}
  {
  "id": "365731266123456",
  "changes": [
    {
      "value": {
        "messaging_product": "whatsapp",
        "metadata": {
          "display_phone_number": "12065550100",
          "phone_number_id": "321010217712345"
        },
        "contacts": [
          {
            "profile": {
              "name": "Diego"
            },
            "wa_id": "12065550102"
          }
        ],
        "messages": [
          {
            "from": "14255550150",
            "id":
 "wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0RjVGRkexample",
            "timestamp": "1723506035",
            "text": {
              "body": "Hi"
            },
            "type": "text"
          }
        ]
      },
      "field": "messages"
    }
  ]
}
```

2. Para mostrarle a Diego que has recibido el mensaje, establece el estado en`read`. Diego verá dos marcas de verificación azules junto al mensaje en su dispositivo.

```
aws socialmessaging send-whatsapp-message --message
 '{"messaging_product":"whatsapp","message_id":"'{MESSAGE_ID}'","status":"read"}'
 --origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version
 v20.0
```

   En el comando anterior, haga lo siguiente.

   - Reemplazar *{ORIGINATION_PHONE_NUMBER_ID}* con el identificador del número de teléfono al que Diego envió su mensaje`phone-number-id-976c72a700aac43eaf573ae050example`.
   - Reemplazar *{MESSAGE_ID}* con el identificador único del mensaje. Es el mismo valor que el identificador del mensaje recibido`wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0RjV`

3. Puedes enviarle a Diego una reacción con la mano.

```
aws socialmessaging send-whatsapp-message --message
 '{"messaging_product":"whatsapp","recipient_type":"individual","to":"'{PHONE_NUMBER}'","ty
 "reaction","reaction": {"message_id": "'{MESSAGE_ID}'","emoji":"\uD83D\uDC4B"}}'
 --origination-phone-number-id {ORIGINATION_PHONE_NUMBER_ID} --meta-api-version
 v20.0
```

   En el comando anterior, haga lo siguiente.

   - Reemplazar *{PHONE_NUMBER}* con el número de teléfono de Diego`14255550150`.
   - Reemplazar *{MESSAGE_ID}* con el identificador único del mensaje. Es el mismo valor que el identificador del mensaje recibido`wamid.HBgLMTQyNTY5ODgzMDIVAgASGCBDNzBDRjM5MDU2ODEwMDkwREY4ODBDRDE0RjV`
   - Reemplazar *{ORIGINATION_PHONE_NUMBER_ID}* con el identificador del número de teléfono al que Diego envió su mensaje`phone-number-id-976c72a700aac43eaf573ae050example`.

## Recursos adicionales de

- Habilite los destinos de eventos para registrar eventos y recibir mensajes entrantes.

- Para obtener una lista de los objetos de los WhatsApp mensajes, consulte la APIreferencia sobre los mensajes en la nube de WhatsApp Business Platform.

# Cómo interpretar los informes WhatsApp de facturación y de uso de AWS End User Messaging Social

El canal social de mensajería para el usuario AWS final genera un tipo de uso que contiene cinco campos con el siguiente formato:*Region code*-*MessagingType*-*ISO*-*FeeDescription*-*FeeType*. Hay dos elementos de facturación posibles para cada WhatsApp conversación: el WhatsApp`ConversationFee`, y el AWS por`MessageFee`.

Cuando inicias una conversación enviando una plantilla de mensaje, se te facturará uno WhatsApp `ConversationFee` y uno AWS por persona. `MessageFee` Esto abre un período de 24 horas en el que cada mensaje que envíes o recibas del mismo cliente se factura de forma individual. AWS `MessageFee`

El tipo de WhatsApp conversación y los detalles de los precios se encuentran en la sección Precios basados en conversaciones de la Guía para desarrolladores de WhatsApp Business Platform.

En la siguiente tabla se muestran los posibles valores y descripciones de los campos del tipo de uso. Para obtener más información sobre los precios de la mensajería social para usuarios AWS finales, consulte los precios de la mensajería para usuarios AWS finales.

| Campo | Opciones | Descripción |
| --- | --- | --- |
| *Region code* | • USE1: región del este de EE. UU. (Norte de Virginia)<br>• USE2: región del este de EE. UU. (Ohio)<br>• USW1: región del oeste de EE. UU. (Oregón)<br>• APS1: región de Asia-Pacífico (Bombay)<br>• APSE1: región de Asia-Pacífico (Singapur)<br>• EUW1: región de Europa (Irlanda) | El Región de AWS prefijo que indica desde dónde se envió o recibió el WhatsApp mensaje. |

| Campo | Opciones | Descripción |
| --- | --- | --- |
| | • EUW2: región de Europa (Londres) | |
| *MessagingType* | `WhatsApp` | En este campo se identifica el tipo de mensaje que se va a enviar. |
| *ISO* | Consulta los países compatibles | El código de ISO país de dos dígitos al que se envió el mensaje. |
| *FeeDescription* | `ConversationFee` , `MessageFee` | En este campo se especifica el WhatsApp `ConversationFee` o el AWS per. `MessageFee` |

| Campo | Opciones | Descripción |
| --- | --- | --- |
| *FeeType* | `Authentication` , `Marketing` , `Service`, `Utility`, `Standard` | Este campo muestra el tipo de conversación que se utilizó o especifica la tarifa estándar por mensaje<br><br>**`ConversationFee`** Categorías iniciadas por empresas<br><br>• `Marketing` — Se utiliza para lograr una amplia gama de objetivos, desde generar conciencia hasta impulsar las ventas y reorientar a los clientes. Algunos ejemplos son los anuncios de nuevos productos, servicios o funciones, promociones u ofertas segmentadas y recordatorios de abandono del carrito de compra.<br>• `Utility`— Se utiliza para hacer un seguimiento de las acciones o solicitudes de los usuarios. Algunos ejemplos son la confirmación de suscripción, la gestión de pedidos y entregas (por ejemplo, una actualización de la entrega), las actualizaciones o alertas de la cuenta (por ejemplo, un recordatorio de pago) o las encuestas de opinión. |

| Campo | Opciones | Descripción |
| --- | --- | --- |
| | | • `Authentication` — Se utilizan para autenticar a los usuarios con códigos de acceso de un solo uso, posiblemente en varios pasos del proceso de inicio de sesión (por ejemplo, la verificación de la cuenta, la recuperación de la cuenta o los problemas de integrida d).<br>• `Service`— Se utiliza para resolver las consultas de los clientes.<br><br>**`Conversat ionFee`** Categorías iniciadas por el usuario<br><br>• `Service`— Se utiliza para resolver las consultas de los clientes.<br><br>Categorías de **`MessageFee`**<br><br>• `Standard`— Tarifa por mensaje enviado o recibido. |

Cuando inicias una conversación enviando una plantilla de mensaje, se te facturará uno `ConversationFee` `MessageFee` y otro. Esto abre un período de 24 horas en el que cada mensaje de plantilla que envíes al mismo cliente se factura de forma individual. `MessageFee` Durante el período de 24 horas, los mensajes de la plantilla deben ser del mismo tipo o se iniciará una nueva conversación.

Por ejemplo, si envías un mensaje de plantilla de marketing a un cliente, se te facturará por el mensaje `ConversationFee` y`MessageFee`.

```
Marketing Template Message 1: APS1-WhatsApp-CA-ConversationFee-Marketing
Marketing Template Message 1: APS1-WhatsApp-CA-MessageFee-Standard
Marketing Template Message 2: APS1-WhatsApp-CA-MessageFee-Standard
```

Si el cliente te envía un mensaje y tú respondes, se te cobrará por abrir una nueva `Service` conversación y un mensaje nuevos.

```
Service Message 1: APS1-WhatsApp-CA-ConversationFee-Service
Service Message 1: APS1-WhatsApp-CA-MessageFee-Standard
Service Message 2: APS1-WhatsApp-CA-MessageFee-Standard
Service Message 3: APS1-WhatsApp-CA-MessageFee-Standard
```

## Ejemplo 1: Envío de un mensaje de plantilla de marketing

Por ejemplo, si envías un mensaje de plantilla de marketing a un cliente, se te facturará uno WhatsApp `ConversationFee` y uno AWS por cada uno. `MessageFee`

```
Marketing Template Message 1: APS1-WhatsApp-CA-ConversationFee-Marketing
Marketing Template Message 1: APS1-WhatsApp-CA-MessageFee-Standard
```

## Ejemplo 2: Abrir una conversación sobre el servicio

Se aplica una tarifa de conversación de servicio cuando una empresa responde a un mensaje entrante de un usuario que no se encuentra dentro de cualquier período de conversación activo de 24 horas iniciado por la empresa. En este escenario, se le facturará uno WhatsApp `ConversationFee` y uno AWS `MessageFee` por cada mensaje entrante y saliente.

```
Service Message 1: APS1-WhatsApp-CA-ConversationFee-Service
Service Message 1: APS1-WhatsApp-CA-MessageFee-Standard
Service Message 2: APS1-WhatsApp-CA-MessageFee-Standard
Service Message 3: APS1-WhatsApp-CA-MessageFee-Standard
```

# AWS Mensajes para usuarios finales: ISO códigos de facturación de redes sociales y WhatsApp mapeo de tarifas de conversación

País

| Código de ISO país de dos dígitos | Country name (Nombre del país) | WhatsApp región de facturación de conversaciones |
|---|---|---|
| AF | Afganistán | Regiones de Asia-Pacífico |
| AX | Islas Aland | Otro |
| AL | Albania | Resto de Europa Central y Oriental |
| DZ | Argelia | África |
| AS | Samoa Americana | Otro |
| CE | Andorra | Otro |
| AO | Angola | África |
| IA | Anguila | Otro |
| AQ | Antártida | Otro |
| AG | Antigua y Barbuda | Otro |
| AR | Argentina | Argentina |
| AM | Armenia | Resto de Europa Central y Oriental |
| AW | Aruba | Otro |
| AC | Isla Ascensión | Otro |
| AU | Australia | Regiones de Asia-Pacífico |
| AT | Austria | Resto de Europa occidental |
| AZ | Azerbaiyán | Resto de Europa Central y Oriental |

| Código de ISO país de dos dígitos | Country name (Nombre del país) | WhatsApp región de facturación de conversaciones |
|---|---|---|
| BS | Bahamas | Otro |
| BH | Bahréin | Oriente Medio |
| BD | Bangladesh | Regiones de Asia-Pacífico |
| BB | Barbados | Otro |
| BY | Belarús | Resto de Europa Central y Oriental |
| BE | Bélgica | Resto de Europa occidental |
| BZ | Belice | Otro |
| BJ | Benín | África |
| BM | Bermudas | Otro |
| BT | Bután | Otro |
| BO | Bolivia | Resto de Latinoamérica |
| BQ | Bonaire | Otro |
| BA | Bosnia y Herzegovina | Otro |
| BW | Botsuana | África |
| BV | Isla Bouvet | Otro |
| BR | Brasil | Brasil |
| E/S | Territorio Británico del Océano Índico | Otro |
| VG | Islas Vírgenes Británicas | Otro |
| BN | Brunéi | Otro |

| Código de ISO país de dos dígitos | Country name (Nombre del país) | WhatsApp región de facturación de conversaciones |
|---|---|---|
| BG | Bulgaria | Resto de Europa Central y Oriental |
| BF | BurkinaFaso | África |
| BI | Burundi | África |
| KH | Camboya | Regiones de Asia-Pacífico |
| CM | Camerún | África |
| CA | Canadá | América del Norte |
| CV | Cabo Verde | Otro |
| KY | Islas Caimán | Otro |
| CF | República Centroafricana | Otro |
| TD | Chad | África |
| CL | Chile | Chile |
| CN | China | Regiones de Asia-Pacífico |
| CX | Isla de Navidad | Otro |
| CC | Islas Cocos | Otro |
| CO | Colombia | Colombia |
| KM | Comoras | Otro |
| CG | Congo | Otro |
| CD | Congo | África |
| CK | Islas Cook | Otro |

| Código de ISO país de dos dígitos | Country name (Nombre del país) | WhatsApp región de facturación de conversaciones |
|---|---|---|
| CR | Costa Rica | Resto de Latinoamérica |
| CI | Costa de Marfil | África |
| HR | Croacia | Resto de Europa Central y Oriental |
| CW | Curazao | Otro |
| CY | Chipre | Otro |
| CZ | República Checa | Resto de Europa Central y Oriental |
| DK | Dinamarca | Resto de Europa occidental |
| DJ | Yibuti | Otro |
| DM | Dominica | Otro |
| DO | República Dominicana | Resto de Latinoamérica |
| EC | Ecuador | Resto de Latinoamérica |
| EG | Egipto | Egipto |
| SV | El Salvador | Resto de Latinoamérica |
| GQ | Guinea Ecuatorial | Otro |
| ER | Eritrea | África |
| EE | Estonia | Otro |
| ET | Etiopía | África |
| FK | Islas Malvinas | Otro |
| FO | Islas Faroe | Otro |

| Código de ISO país de dos dígitos | Country name (Nombre del país) | WhatsApp región de facturación de conversaciones |
|---|---|---|
| FJ | Fiyi | Otro |
| FI | Finlandia | Resto de Europa occidental |
| FR | Francia | Francia |
| GF | Guayana Francesa | Otro |
| PF | Polinesia Francesa | Otro |
| TF | Territorios Australes Franceses | Otro |
| GA | Gabón | África |
| GM | Gambia | África |
| GE | Georgia | Resto de Europa Central y Oriental |
| DE | Alemania | Alemania |
| GH | Ghana | África |
| GI | Gibraltar | Otro |
| GR | Grecia | Resto de Europa Central y Oriental |
| GL | Groenlandia | Otro |
| GD | Granada | Otro |
| GP | Guadalupe | Otro |
| GU | Guam | Otro |
| GT | Guatemala | Resto de Latinoamérica |

| Código de ISO país de dos dígitos | Country name (Nombre del país) | WhatsApp región de facturación de conversaciones |
|---|---|---|
| GG | Guernsey | Otro |
| GN | Guinea | Otro |
| GW | Guinea-Bissau | África |
| GY | Guyana | Otro |
| HT | Haití | Resto de Latinoamérica |
| HM | Heard e McDonald Islands | Otro |
| HN | Honduras | Resto de Latinoamérica |
| HK | Hong Kong | Regiones de Asia-Pacífico |
| HU | Hungría | Resto de Europa Central y Oriental |
| IS | Islandia | Otro |
| IN | India | India |
| IN | India internacional | India internacional |
| ID | Indonesia | Indonesia |
| ID | Internacional de Indonesia | Internacional de Indonesia |
| IQ | Irak | Oriente Medio |
| IE | Irlanda | Resto de Europa occidental |
| IM | Isla de Man | Otro |
| IL | Israel | Israel |
| IT | Italia | Italia |

| Código de ISO país de dos dígitos | Country name (Nombre del país) | WhatsApp región de facturación de conversaciones |
|---|---|---|
| JM | Jamaica | Resto de Latinoamérica |
| JP | Japón | Resto de Asia-Pacífico |
| JE | Jersey | Otro |
| JO | Jordania | Oriente Medio |
| KZ | Kazajistán | Otro |
| KE | Kenia | África |
| KI | Kiribati | Otro |
| XK | Kosovo | Otro |
| KW | Kuwait | Oriente Medio |
| KG | Kirguistán | Otro |
| LA | Lao PDR | Resto de Asia-Pacífico |
| LV | Letonia | Resto de Europa Central y Oriental |
| LB | Líbano | Oriente Medio |
| LS | Lesoto | África |
| LR | Liberia | África |
| LY | Libia | África |
| LI | Liechtenstein | Otro |
| LT | Lituania | Resto de Europa Central y Oriental |
| LU | Luxemburgo | Otro |

| Código de ISO país de dos dígitos | Country name (Nombre del país) | WhatsApp región de facturación de conversaciones |
|---|---|---|
| MO | Macao | Otro |
| MK | Macedonia | Resto de Europa Central y Oriental |
| MG | Madagascar | África |
| MW | Malawi | África |
| MY | Malasia | Malasia |
| MV | Maldivas | Otro |
| ML | Mali | África |
| MT | Malta | Otro |
| MH | Islas Marshall | Otro |
| MQ | Martinica | Otro |
| MR | Mauritania | África |
| MU | Mauricio | Otro |
| YT | Mayotte | Otro |
| MX | México | México |
| FM | Micronesia | Otro |
| MD | Moldavia | Resto de Europa Central y Oriental |
| MC | Mónaco | Otro |
| MN | Mongolia | Resto de Asia-Pacífico |
| ME | Montenegro | Otro |

| Código de ISO país de dos dígitos | Country name (Nombre del país) | WhatsApp región de facturación de conversaciones |
|---|---|---|
| MS | Montserrat | Otro |
| MA | Marruecos | África |
| MZ | Mozambique | África |
| MM | Myanmar | Otro |
| N/D | Namibia | África |
| NR | Nauru | Otro |
| NP | Nepal | Resto de Asia-Pacífico |
| NL | Países Bajos | Países Bajos |
| NC | Nueva Caledonia | Otro |
| NZ | Nueva Zelanda | Resto de Asia-Pacífico |
| NI | Nicaragua | Resto de Latinoamérica |
| NE | Níger | África |
| NG | Nigeria | Nigeria |
| NU | Niue | Otro |
| NF | Isla Norfolk | Otro |
| MP | Islas Marianas del Norte | Otro |
| NO | Noruega | Resto de Europa occidental |
| OM | Omán | Oriente Medio |
| PK | Pakistán | Pakistán |
| PW | Palaos | Otro |

| Código de ISO país de dos dígitos | Country name (Nombre del país) | WhatsApp región de facturación de conversaciones |
|---|---|---|
| PS | Territorio palestino | Otro |
| PA | Panamá | Resto de Latinoamérica |
| PG | Papúa Nueva Guinea | Resto de Asia-Pacífico |
| PY | Paraguay | Resto de Latinoamérica |
| PE | Perú | Perú |
| PH | Filipinas | Resto de Asia-Pacífico |
| PN | Pitcairn | Otro |
| PL | Polonia | Resto de Europa Central y Oriental |
| PT | Portugal | Resto de Europa occidental |
| PR | Puerto Rico | Resto de Latinoamérica |
| QA | Qatar | Oriente Medio |
| RE | Reunión | Otro |
| RO | Rumanía | Resto de Europa Central y Oriental |
| RU | Federación de Rusia | Rusia |
| RW | Ruanda | África |
| SH | Santa Elena | Otro |
| KN | San Cristóbal y Nieves | Otro |
| LC | Santa Lucía | Otro |
| p. m. | San Pedro y Miquelón | Otro |

| Código de ISO país de dos dígitos | Country name (Nombre del país) | WhatsApp región de facturación de conversaciones |
|---|---|---|
| VC | San Vicente y las Granadinas | Otro |
| BL | San Bartolomé | Otro |
| MF | San Martín (Francia) | Otro |
| WS | Samoa | Otro |
| SM | San Marino | Otro |
| ST | Santo Tomé y Príncipe | Otro |
| SA | Arabia Saudí | Arabia Saudí |
| SN | Senegal | África |
| RS | Serbia | Resto de Europa Central y Oriental |
| SC | Seychelles | Otro |
| SL | Sierra Leona | África |
| SG | Singapur | Resto de Asia-Pacífico |
| SX | San Martín (Países Bajos) | Otro |
| SK | Eslovaquia | Resto de Europa Central y Oriental |
| SI | Eslovenia | Resto de Europa Central y Oriental |
| SB | Islas Salomón | Otro |
| SO | Somalia | África |
| ZA | Sudáfrica | Sudáfrica |

| Código de ISO país de dos dígitos | Country name (Nombre del país) | WhatsApp región de facturación de conversaciones |
|---|---|---|
| GS | Islas Georgias del Sur y Sandwich del Sur | Otro |
| KR | Corea del Sur | Otro |
| SS | Sudán del Sur | África |
| ES | España | España |
| LK | Sri Lanka | Resto de Asia-Pacífico |
| SR | Surinam | Otro |
| SJ | Islas Svalbard y Jan Mayen | Otro |
| SZ | Suazilandia | África |
| SE | Suecia | Resto de Europa occidental |
| CH | Suiza | Resto de Europa occidental |
| TW | Taiwán | Resto de Asia-Pacífico |
| TJ | Tayikistán | Resto de Asia-Pacífico |
| TZ | Tanzania | África |
| TH | Tailandia | Resto de Asia-Pacífico |
| TL | Timor Oriental | Otro |
| TG | Togo | África |
| TK | Tokelau | Otro |
| TO | Tonga | Otro |
| TT | Trinidad y Tobago | Otro |

| Código de ISO país de dos dígitos | Country name (Nombre del país) | WhatsApp región de facturación de conversaciones |
|---|---|---|
| TA | Tristán de Acuña | Otro |
| TN | Túnez | África |
| TR | Turquía | Turquía |
| TM | Turkmenistán | Resto de Asia-Pacífico |
| TC | Islas Turcas y Caicos | Otro |
| TV | Tuvalu | Otro |
| UG | Uganda | África |
| UA | Ucrania | Resto de Europa Central y Oriental |
| AE | Emiratos Árabes Unidos | Emiratos Árabes Unidos |
| GB | Reino Unido | Reino Unido |
| EE. UU. | Estados Unidos | América del Norte |
| UY | Uruguay | Resto de Latinoamérica |
| UM | Islas Ultramarinas Menores de EE. UU | Otro |
| UZ | Uzbekistán | Resto de Asia-Pacífico |
| VU | Vanuatu | Otro |
| VA | Ciudad del Vaticano | Otro |
| VE | Venezuela | Resto de Latinoamérica |
| VN | Vietnam | Resto de Asia-Pacífico |
| VI | Islas Vírgenes | Otro |

| Código de ISO país de dos dígitos | Country name (Nombre del país) | WhatsApp región de facturación de conversaciones |
|---|---|---|
| WF | Islas Wallis y Futuna | Otro |
| EH | Sahara Occidental | Otro |
| YE | Yemen | Oriente Medio |
| ZM | Zambia | África |
| ZW | Zimbabue | Otro |

# Supervisión de la mensajería de los usuarios AWS finales en redes sociales

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de AWS End User Messaging Social y de las demás AWS soluciones de. AWSofrece las siguientes herramientas de supervisión para vigilar AWS End User Messaging Social, informar cuando algo no funciona y realizar acciones automáticas cuando proceda:

- Amazon CloudWatch monitorea AWS los recursos de y las aplicaciones que ejecuta en AWS en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique. Por ejemplo, puede CloudWatch hacer que realice un seguimiento de la CPU utilización u otras métricas de las EC2 instancias de Amazon y lanzar nuevas instancias automáticamente cuando sea necesario. Para obtener más información, consulte la Guía de CloudWatch usuario de Amazon.
- Amazon CloudWatch Logs le permite supervisar, almacenar y tener acceso a los archivos de registro desde EC2 instancias de Amazon CloudTrail, u otros orígenes. CloudWatch Los registros pueden supervisar información en los registros y enviarle una notificación cuando se llega a determinados umbrales. También se pueden archivar los datos del registro en un almacenamiento de larga duración. Para obtener más información, consulte la Guía de usuario CloudWatch de Amazon Logs.
- AWS CloudTrailcaptura API llamadas y eventos relacionados efectuados por su AWS cuenta de o en su nombre, y entrega los archivos de registro al bucket de Amazon S3 que se haya especificado. También pueden identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen desde la que se realizaron las llamadas y el momento en que se efectuaron. Para obtener más información, consulte la AWS CloudTrail Guía del usuario de .

## Supervisión de la mensajería social de los usuarios AWS finales con Amazon CloudWatch

También pueden supervisar AWS End User Messaging Social CloudWatch, que recopila y procesa los datos sin procesar y los convierte en métricas legibles y casi en tiempo real. Estas estadísticas se mantienen durante 15 meses, de forma que pueda obtener acceso a información histórica y disponer de una mejor perspectiva sobre el desempeño de su aplicación web o servicio. También

puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se cumplan dichos umbrales. Para obtener más información, consulte la Guía de CloudWatch usuario de Amazon.

En el caso de AWS End User Messaging Social`WhatsAppMessageFeeCount`, puede que te interese observar `WhatsAppConversationFeeCount` y activar una alarma cuando se alcance un límite de gasto.

En las siguientes tablas se muestran las métricas y dimensiones que AWS End User Messaging Social exporta al espacio de `AWS/SocialMessaging` nombres.

| Métrica | Unidad | Descripción |
|---|---|---|
| WhatsAppConversationFeeCount | Recuento | El recuento de las comisiones de conversación WhatsApp |
| WhatsAppMessageFeeCount | Recuento | El recuento de las tarifas por WhatsApp mensajes |

| Dimensión | Descripción |
|---|---|
| MessageFeeType | Los tipos de tarifas válidos son los de servicio, marketing, utilidad y autenticación |
| DestinationCountryCode | El ISO código de dos letras del país |
| WhatsAppPhoneNumberArn | El nombre del número de teléfono |

# Registro de API llamadas sociales de mensajería de usuarios AWS finales mediante AWS CloudTrail

AWS se integra a AWS CloudTrail, un servicio que proporciona un registro de las acciones que realiza un usuario, un rol o un servicio de administración Servicio de AWS. CloudTrail captura todas las API llamadas de AWS End User Messaging Social como eventos. Las llamadas capturadas incluyen las llamadas desde la AWS consola de CloudTrail y las llamadas de código a las API operaciones AWS de la API de CloudTrail. Mediante la información que recopila CloudTrail, se puede

determinar la solicitud que AWS se envió a, la dirección IP desde la que se realizó, cuándo se realizó y detalles adicionales.

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 las credenciales del usuario raíz o del usuario.
- Si la solicitud se realizó en nombre de un usuario de IAM IAM Identity Center.
- 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.

CloudTrail Para obtener más información sobre la Cuenta de AWS cuando usted crea la cuenta y tiene acceso automático al Historial de eventos de administración, ya que usted crea la cuenta y tiene acceso automático al Historial de CloudTrail eventos de administración. El Historial de CloudTrail eventos proporciona un registro visible e inmutable, que se puede buscar y descargar, de los últimos 90 días de eventos de administración registrados en una. Región de AWSPara obtener más información, consulte Uso del historial de CloudTrail eventos en la Guía del usuario.AWS CloudTrail  No se CloudTrail cobran cargos de administración.

Para mantener un registro permanente de los eventos en su Cuenta de AWS más allá de los 90 días, cree un registro de seguimiento o un almacén de datos de seguimiento CloudTrailo un almacén de datos de seguimiento.

CloudTrail senderos

Un registro de seguimiento permite CloudTrail a CloudTrail enviar archivos de registro a un bucket de Amazon S3. Todos los registros de seguimiento que cree con la AWS Management Console son de varias regiones. Puede crear un registro de seguimiento de una sola región o de varias regiones mediante la AWS CLI. Crear un registro de seguimiento de varias regiones es una práctica recomendada, ya que registra actividad Regiones de AWS en todas las de su cuenta. Si crea un registro de seguimiento de una sola región, solo podrá ver los eventos registrados en la Región de AWS del registro de seguimiento. Para obtener más información acerca de los registros de seguimiento, consulte Creación de un registro de seguimiento para su Cuenta de AWS y Creación de un registro de seguimiento para una organización en la Guía del usuario de AWS CloudTrail .

Puede crear un registro de seguimiento para enviar una copia de los eventos de administración en curso en su bucket de Amazon S3 sin costo alguno desde CloudTrail; sin embargo, hay cargos CloudTrail por almacenamiento en Amazon S3. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios. Para obtener información acerca de los precios de Amazon S3, consulte Precios de Amazon S3.

CloudTrail Almacenes de datos de CloudTrail Lake

CloudTrail Lake le permite ejecutar consultas SQL basadas en SQL sobre sus eventos. CloudTrail CloudTrail Lake convierte los eventos existentes en formato JSON basado en filas al JSON formato ORC como eventos de ORC administración. ORCORC es un formato de almacenamiento en columnas optimizado para una recuperación rápida de datos. Los eventos se agregan en almacenes de datos de eventos, que son recopilaciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos avanzados. Los selectores que se aplican a un almacén de datos de eventos controlan los eventos que perduran y están disponibles para la consulta. Para obtener más información acerca de CloudTrail Lake, consulte Cómo trabajar con AWS CloudTrail Lake en la Guía del AWS CloudTrail usuario.

CloudTrail Los almacenes de datos de eventos de Lake y las consultas conllevan cargos. Cuando crea un almacén de datos de eventos, elige la opción de precios que desea utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los eventos, así como el periodo de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios.

## AWS Mensajes de usuario final sobre eventos de datos sociales en CloudTrail

Los eventos de datos proporcionan información sobre las operaciones de recursos realizadas en o dentro de un recurso (por ejemplo, leer o escribir en un objeto de Amazon S3). Se denominan también operaciones del plano de datos. Los eventos de datos suelen ser actividades de gran volumen. De forma predeterminada, CloudTrail los eventos de administración de datos. El Historial de CloudTrail eventos de administración proporciona información sobre los eventos de datos.

Se aplican cargos adicionales a los eventos de datos. Para obtener más información sobre CloudTrail los precios, consulta AWS CloudTrail Precios.

Puede registrar eventos de datos para los tipos de recursos sociales de mensajería para usuarios AWS finales mediante la CloudTrail consola o CloudTrail API las operaciones. AWS CLI Para obtener más información sobre cómo registrar los eventos de datos, consulte Registro de eventos de datos

con la AWS Management Console y Registro de eventos de datos con la AWS Command Line Interface en la Guía del usuario de AWS CloudTrail .

En la siguiente tabla se muestran AWS los tipos de recursos de Amazon S3 para los que puede registrar eventos de datos. La columna Tipo de evento de datos (consola) muestra el valor que se debe elegir en la lista de tipos de eventos de datos ( CloudTrail consola). La columna Tipo de recursos de CloudTrail muestra el **`resources.type`** valor que especificaría al configurar los selectores de eventos avanzados mediante la o las API de CloudTrail. AWS CLI CloudTrail APIs La CloudTrail columna Datos APIs registrados muestra las API llamadas registradas CloudTrail para el tipo de recurso.

| Tipo de evento de datos (consola) | resources.type value | Datos APIs registrados en CloudTrail |
|---|---|---|
| ID del número de teléfono de mensajería social | `AWS::SocialMessaging::PhoneNumberId` | • DeleteWhatsAppMessageMedia<br>• GetWhatsAppMessageMedia<br>• PostWhatsAppMessageMedia<br>• SendWhatsAppMessage |

Puede configurar selectores de eventos avanzados para filtrar según los campos `eventName`, `readOnly` y `resources.ARN` y así registrar solo los eventos que son importantes para usted. Para obtener más información acerca de estos campos, consulte. AdvancedFieldSelectoren la AWS CloudTrail APIReferencia.

## AWS Eventos de administración social de mensajería para usuarios finales en CloudTrail

Los eventos de administración proporcionan información sobre las operaciones de administración que se realizan en los recursos de su cuenta de Cuenta de AWS. Se denominan también operaciones del plano de control. De forma predeterminada, CloudTrail los eventos de administración de forma predeterminada.

AWS Los eventos de administración AWS proporcionan información sobre las operaciones de administración. Para obtener una lista de las operaciones del plano de control de AWS End User

Messaging Social en las que se registra AWS End User Messaging Social CloudTrail, consulte la APIReferencia social de AWS End User Messaging Social.

## AWS Ejemplos de eventos sociales de mensajería para usuarios finales

Un evento representa una única solicitud de cualquier origen e incluye información sobre la API operación solicitada, la fecha y la hora de la operación, los parámetros de la solicitud, los parámetros de la solicitud, etcétera. CloudTrail Los archivos de registro de seguimiento no rastrean el orden en la pila de las API llamadas públicas a la API, por lo que los eventos no aparecen en ningún orden específico.

En el ejemplo que sigue se muestra una CloudTrail entrada de registro de que ilustra la operación.


```
{
        "eventVersion": "1.09",
        "userIdentity": {
            "type": "AssumedRole",
            "principalId": "GR632462JDSBDSHHGS39:session",
            "arn": "arn:aws:sts::123456789101:assumed-role/Role_name/Session_name",
            "accountId": "123456789101",
            "accessKeyId": "12345678901234567890",
            "sessionContext": {
                "sessionIssuer": {
                    "type": "Role",
                    "principalId": "GR632462JDSBDEXAMPLE",
                    "arn": "arn:aws:sts::123456789101:assumed-role/Role_name/
Session_name",
                    "accountId": "123456789101",
                    "userName": "user"
                },
                "attributes": {
                    "creationDate": "2024-10-03T17:25:08Z",
                    "mfaAuthenticated": "false"
                }
            }
        },
        "eventTime": "2024-10-03T17:25:23Z",
        "eventSource": "social-messaging.amazonaws.com",
        "eventName": "SendWhatsAppMessage",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "1.x.x.x",
        "userAgent": "agent",
        "requestParameters": {
```

```
            "originationPhoneNumberId": "phone-number-id-
aa01234567890123456789012345678 9",
            "metaApiVersion": "v20.0",
            "message": "Hi"
        },
        "responseElements": {
            "messageId": "message_id"
        },
        "requestID": "request_id",
        "eventID": "event_id",
        "readOnly": false,
        "resources": [{
            "accountId": "123456789101",
            "type": "AWS::SocialMessaging::PhoneNumberId",
            "ARN": "arn:aws:social-messaging:us-east-1:123456789101:phone-number-id/
phone-number-id-aa01234567890123456789012345678 9"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": false,
        "recipientAccountId": "123456789101",
        "eventCategory": "Data",
        "tlsDetails": {
            "clientProvidedHostHeader": "social-messaging.us-east-1.amazonaws.com"
        }
    }
```


Para obtener información sobre el contenido de los CloudTrail registros, consulte el contenido de los CloudTrail registros en la Guía del AWS CloudTrail usuario.

# Mejores prácticas para la mensajería social para usuarios AWS finales

En esta sección se describen diversas prácticas recomendadas que es posible que le ayuden a mejorar la implicación de los clientes y evitar la suspensión de cuentas. Sin embargo, tenga en cuenta que esta sección no contiene asesoramiento jurídico. Consulte siempre a un abogado para obtener asesoramiento jurídico.

Para ver la lista más reciente de prácticas WhatsApp recomendadas, consulta la Política WhatsApp de mensajería empresarial.

Temas



## Up-to-date perfil empresarial

Mantenga un perfil up-to-date WhatsApp empresarial preciso que incluya información de contacto del servicio de atención al cliente, como una dirección de correo electrónico, una dirección de sitio web o un número de teléfono. Asegúrese de que la información proporcionada sea veraz y no tergiverse ni hacerse pasar por otra empresa.

## Obtener permiso

Nunca envíe mensajes a destinatarios que no hayan pedido de forma explícita recibir los tipos específicos de mensajes que tiene pensado enviar. Solo se admiten las siguientes regiones:

- El proceso de suscripción debe informar claramente a la persona de que está dando su consentimiento para recibir mensajes o llamadas de su empresa. WhatsApp Debes indicar explícitamente el nombre de tu empresa.

- Usted es el único responsable de determinar el método para obtener el consentimiento expreso. Asegúrese de que el proceso de suscripción cumpla con todas las leyes aplicables que rigen sus comunicaciones. Proporcione todos los avisos requeridos y obtenga todos los permisos necesarios en virtud de las leyes pertinentes.

Para obtener más información sobre los requisitos de WhatsApp suscripción, consulte Obtenga la suscripción para WhatsApp

Si los destinatarios pueden inscribirse para recibir sus mensajes mediante un formulario en línea, evite que los scripts automatizados suscriban a las personas sin su conocimiento. También limite el número de veces que un usuario puede enviar un número de teléfono en una sola sesión.

Respeta todas las solicitudes de una persona, ya sean activadas o desactivadas WhatsApp, para bloquear, interrumpir u optar por no recibir comunicaciones, incluida la eliminación de esa persona de tu lista de contactos.

Mantenga registros que incluyan la fecha, la hora y el origen de cada solicitud de alta y confirmación. Esto también puede ayudarte a realizar auditorías rutinarias de tu lista de clientes.

## Contenido de mensajes prohibido

**Important**

Trabajando con Meta/ WhatsApp

- El uso de la solución WhatsApp empresarial está sujeto a los términos y condiciones de las condiciones del servicio WhatsApp empresarial, las condiciones de la solución WhatsApp empresarial, la política de mensajería WhatsApp empresarial, las directrices de WhatsApp mensajería y todos los demás términos, políticas o directrices que se incluyan en ellas como referencia (ya que cada uno de ellos puede actualizarse periódicamente).
- Meta o WhatsApp puede prohibir en cualquier momento el uso de la solución WhatsApp empresarial.
- En relación con su uso de la Solución WhatsApp empresarial, no presentará ningún contenido, información o dato que esté sujeto a medidas de protección o a limitaciones de distribución de conformidad con las leyes o reglamentos aplicables.

Si infringe la WhatsApp política, es posible que se bloquee su cuenta para que no envíe mensajes durante un período de tiempo, que se bloquee hasta que presente una apelación o que se bloquee permanentemente. Meta le informará si alguna de sus cuentas o activos ha infringido la política, por correo electrónico y por medio del gerente WhatsApp comercial. Todas las apelaciones deben presentarse ante Meta. Para ver una infracción de una política o presentar una apelación ante Meta, consulta Ver los detalles de la infracción de la política de tu cuenta WhatsApp empresarial en el Centro de ayuda de Meta Business. Para ver la lista más reciente del contenido prohibido de los mensajes, consulta la Política de mensajería WhatsApp empresarial.

Las siguientes son categorías de contenido prohibido para todos los tipos de mensajes a nivel mundial. Cuando utilice un rol vinculado a un WhatsApp servicio, siga estas pautas:

| Categoría | Ejemplos |
| --- | --- |
| Apuestas | • Casinos<br>• Sorteos<br>• Aplicaciones/sitios web |
| Servicios financieros de alto riesgo | • Préstamos de pago<br>• Préstamos a corto plazo con altos intereses<br>• Préstamos para automóviles<br>• Préstamos hipotecarios<br>• Préstamos escolares<br>• Cobro de deudas<br>• Alertas de stock<br>• Cryptocurrency |
| Condonación de la deuda | • Consolidación de la deuda<br>• Reducción de la deuda<br>• Programas de reparación de créditos |
| Get-rich-quick esquemas | • Work-from-home programas<br>• Oportunidades de inversión de riesgo<br>• Esquemas de marketing pirámide o multinivel |

| Categoría | Ejemplos |
| --- | --- |
| Sustancias ilegales | • Cannabis/CBD CBD |
| Suplantación de identidad o envío de correos electrónicos | • Intenta que los usuarios revelen información personal o información de inicio de sesión en el sitio web. |
| S.H.A.F.T. | • Sexo<br>• Odio<br>• Alcohol<br>• Armas de fuego<br>• Tabaco/vapeo |
| Obtención de clientes potenciales de terceros | • Empresas que compran, venden o comparten información sobre los consumido res |

## Auditar sus listas de clientes

Si envía WhatsApp mensajes recurrentes, audite sus listas de clientes con regularidad. La auditoría de sus listas de clientes ayuda a asegurarse de que los únicos clientes que reciben sus mensajes son los que desean recibirlos.

Al auditar su lista, envíe a cada cliente que ha solicitado el alta un mensaje que les recuerde que ya están suscritos y facilíteles información sobre cómo anular la suscripción.

## Ajustar el envío en función del compromiso

Las prioridades de los clientes pueden cambiar a lo largo del tiempo. Si los clientes dejan de encontrar útiles sus mensajes, podrían darse de baja de sus mensajes o incluso notificar los mensajes como no solicitados. Por estas razones, es importante que ajuste sus prácticas de envío en función del compromiso de los clientes.

Para los clientes que no suelan participar en sus mensajes, debe ajustar la frecuencia de los mismos. Por ejemplo, si envía mensajes semanales a clientes comprometidos, podría crear un resumen mensual independiente para los clientes menos comprometidos.

Por último, elimine de su lista a aquellos clientes que no muestren ningún compromiso. Este paso evita que los clientes se sientan frustrados con sus mensajes. También le ahorra dinero y ayuda a proteger su reputación como remitente.

## Enviar en horarios apropiados

Puede utilizar las políticas administradas de. Si envía mensajes a la hora de la cena o a medianoche, hay muchas probabilidades de que los clientes anulen la suscripción a la lista para evitar que les molesten. Es posible que desees evitar enviar WhatsApp mensajes cuando tus clientes no puedan responderlos de inmediato.

# Seguridad en la mensajería social para usuarios AWS finales

La seguridad en la nube de AWS es la mayor prioridad. Como AWS cliente de, se beneficiará de una arquitectura de red y de centros de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

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

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS servicios de en Nube de AWS. AWS AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los Programas de conformidad de Programas de AWS conformidad de Programas de de de. Para obtener información sobre los programas de conformidad que se aplican a las redes sociales de mensajería para usuarios AWS finales, consulte AWS los Servicios de en el ámbito del programa de conformidad AWS .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio de que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS End User Messaging Social. En los siguientes temas, se le mostrará cómo configurar AWS End User Messaging Social para satisfacer sus objetivos de seguridad y conformidad. También puede aprender a utilizar otros AWS servicios de para supervisar y proteger los recursos sociales de mensajería para usuarios AWS finales de.

Temas

- Prácticas recomendadas de seguridad
- Uso de un rol vinculado a un AWS servicio de

# Protección de datos en AWS End User Messaging Social

El modelo de se aplica a protección de datos en AWS End User Messaging Social. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información acerca de la privacidad de datos, consulte Privacidad de datos FAQ. Para obtener información sobre la protección de datos en Europa, consulte el modelo de responsabilidad AWS compartida y la entrada del GDPR blog sobre AWS seguridad.

A los fines de la protección de datos, recomendamos proteger Cuenta de AWS las credenciales de y configurar cada usuario 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:

- Use los permisos de acceso. MFA
- UseSSL/TLSpara comunicarse con AWS los recursos. Le recomendamos TLS TLS TLS 1.2.
- Configure la API API y el registro de actividad del usuario con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice las soluciones de AWS cifrado de, junto con todos los controles de seguridad predeterminados dentro de los servicios de 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 cuando accede a a AWS través de una interfaz de línea de comandos o unAPI, utilice un FIPS punto de enlace. Para obtener más información sobre los FIPS puntos de enlace disponibles, consulte Estándar de procesamiento de la información federal (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 trabaja con AWS End User Messaging Social u otro tipo Servicios de AWS mediante 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 un URL a un servidor externo, le recomendamos encarecidamente que no incluya información de credenciales en el URL para validar la solicitud para ese servidor.

> **Important**
>
> WhatsApp utiliza el protocolo Signal para garantizar la seguridad de las comunicaciones. Sin embargo, dado que AWS End User Messaging Social es un tercero, WhatsApp no considera que estos mensajes estén end-to-end cifrados. Para obtener más información sobre la protección de WhatsApp datos, consulte el documento técnico sobre privacidad y seguridad de los datos y descripción general del WhatsApp cifrado.

## Cifrado de datos

AWS Los datos sociales de mensajería para usuarios finales se cifran en tránsito y en reposo dentro de los AWS límites. Cuando envía datos a AWS End User Messaging Social, el servicio cifra los datos a medida que los recibe y los almacena. Cuando se recuperan datos de AWS End User Messaging Social, el servicio los transmite mediante los protocolos de seguridad actuales.

### Cifrado en reposo

AWS End User Messaging Social cifra todos los datos que almacena para usted dentro de los AWS límites. Entre estos se incluyen los datos de configuración, los datos de registro y los datos que agrega a AWS End User Messaging Social. Para cifrar los datos, AWS End User Messaging Social utiliza claves internas de AWS Key Management Service (AWS KMS) que el servicio posee y mantiene en su nombre. Para obtener más información acerca de AWS KMS, consulte la Guía para desarrolladores de AWS Key Management Service.

## Cifrado en tránsito

AWS End User Messaging Social utiliza HTTPS la seguridad de la capa de transporte (TLS) 1.2 para comunicarse con los clientes, aplicaciones y Meta para comunicarse con los clientes, aplicaciones y Meta. Para comunicarse con otros AWS servicios, AWS End User Messaging Social utiliza HTTPS y TLS 1.2. Además, al crear y administrar AWS SMS recursos mediante la consola, una o las AWS

SDK AWS Command Line Interface, todas las comunicaciones se protegen mediante HTTPS y TLS 1.2.

## Administración de claves

Para cifrar sus datos, AWS End User Messaging Social utiliza AWS KMS claves internas de que el servicio posee y mantiene en su nombre. Rotamos estas claves periódicamente. No puede aprovisionar ni usar su propia AWS KMS u otras claves para cifrar los datos almacenados en AWS End User Messaging Social.

## Privacidad del tráfico entre redes

La privacidad del tráfico entre redes se refiere a la protección de las conexiones y el tráfico entre AWS End User Messaging Social y los clientes y aplicaciones en las instalaciones, y entre AWS End User Messaging Social y otros AWS recursos de la misma. Región de AWS Las siguientes características y prácticas pueden ayudarle a proteger la privacidad del tráfico entre redes en la red de AWS End User Messaging Social.

### Tráfico entre AWS SMS y aplicaciones y clientes locales

Para establecer una conexión privada entre AWS End User Messaging Social y clientes y aplicaciones en la red en las instalaciones, puede utilizar AWS Direct Connect. Esto le permite vincular su red a una ubicación de AWS Direct Connect mediante un cable de Ethernet de fibra óptica estándar. Un extremo del cable se conecta al enrutador. El otro extremo está conectado a un AWS Direct Connect router. Para obtener más información, consulte ¿Qué es AWS Direct Connect? en la Guía del usuario de AWS Direct Connect .

Para ayudar a proteger el acceso a las redes sociales de mensajería para usuarios AWS finales mediante publicacionesAPIs, le recomendamos que cumpla con los requisitos de las redes sociales de mensajería para usuarios AWS finales en materia de API llamadas. AWS End User Messaging Social requiere que los clientes utilicen Transport Layer Security (TLS) 1.2 o una versión posterior. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS), como Ephemeral Diffie-Hellman () o Elliptic Curve Diffie-Hellman Ephemeral (DHE). ECDHE La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que estén asociados a una entidad principal de AWS Identity and Access

Management (IAM) de la AWS cuenta de. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

# Administración de identidades y accesos de AWS

AWS Identity and Access Management (IAM) es una Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. IAMlos administradores controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de AWS End User Messaging Social. IAMIAM es un Servicio de AWS que se puede utilizar sin cargo adicional.

Temas



## Público

La forma en que utilice AWS Identity and Access Management (IAM) difiere en función del trabajo que realice en AWS End User Messaging Social.

Usuario de servicio: si utiliza el servicio social de mensajería para el usuario AWS final para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características sociales de mensajería para el usuario AWS final 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 AWS End User Messing Social, consulteSolución de problemas de identidad y acceso a la mensajería para usuarios AWS finales en redes sociales.

Administrador de servicio: si está a cargo de los recursos de AWS End User Messaging Social en su empresa, probablemente tenga acceso completo a AWS End User Messaging Social. Su trabajo

consiste en determinar a qué características y recursos de AWS End User Messaging Social deben acceder los usuarios del servicio. A continuación, debe enviar solicitudes a su IAM administrador de para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos deIAM. Para obtener más información sobre cómo su empresa puede utilizar IAM AWS End User Messaging Social, consulteCómo funciona AWS End User Messaging Social con IAM.

IAMadministrador: si es un IAM administrador, es posible que desee obtener más información sobre cómo redactar políticas para administrar el acceso a AWS End User Messaging Social. Para consultar ejemplos de políticas basadas en la identidad social de mensajería de usuario AWS final que puede utilizar enIAM, consulte. Ejemplos de políticas basadas en identidad para la Administración AWS de costos de

## Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales. Debe estar autenticado (con quien haya iniciado sesión AWS) como IAM usuario o asumiendo un IAM rol. Usuario raíz de la cuenta de AWS

Puede iniciar sesión en AWS como una 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 identidad federada, su administrador habrá configurado previamente la federación de identidades mediante IAM roles de. Cuando accede a AWS mediante la federación, está asumiendo un rol vinculado a un servicio.

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

Si accede a AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente las solicitudes con las credenciales. Si no utiliza AWS las herramientas de, debe firmar usted mismo las solicitudes. Para obtener más información sobre el método recomendado para firmar solicitudes, consulte Firma de AWS API solicitudes de en la Guía del IAM usuario de.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda el uso de la autenticación

multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactorial en la Guía del AWS IAM Identity Center usuario y Uso de la autenticación multifactorial (MFA) AWS en la Guía del IAM usuario.

### Cuenta de AWS usuario root

Cuando se crea una Cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los recursos Servicios de AWS y de la cuenta. Esta identidad recibe el nombre de usuario Cuenta de AWS raíz de y se accede a ella 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 obtener la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del IAM usuario de.

### Identidad federada

Como práctica recomendada, solicite que los usuarios humanos, incluidos los que requieren acceso de administrador, utilicen la federación con un proveedor de identidades para acceder a los Servicios de AWS utilizando 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 Identity Center o cualquier usuario que acceda Servicios de AWS a los utilizando credenciales proporcionadas a través de una fuente de identidad. Cuando identidades federadas acceden a Cuentas de AWS, asumen roles y los roles proporcionan credenciales temporales.

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

### Usuarios y grupos de IAM

Un IAMusuario es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear IAM usuarios que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con IAM usuarios, recomendamos rotar las claves de acceso. Para

obtener más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del IAM usuario de.

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, podría asignar un nombre a un grupo IAMAdminsy conceder permisos a dicho grupo para administrar IAM los recursos de.

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 ti Cuenta de AWS que tiene permisos específicos. Es similar a un IAM usuario, pero no está asociado a una determinada persona. Puede asumir temporalmente un IAM rol en AWS Management Console cambiando de roles. Puede asumir un rol llamando a una AWS API operación AWS CLI o o utilizando una operación personalizadaURL. Para obtener más información sobre los métodos de uso de roles, consulte Métodos para asumir un rol en la Guía del IAM usuario.

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

- 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, debe configurar 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 acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos IAM de usuario temporales: un IAM usuario o rol puede asumir un IAM rol para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un IAM rol de para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunos Servicios de AWS se puede adjuntar

una política directamente a un recurso (en lugar de utilizar un rol como representante). Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas IAM en la Guía del IAM usuario de.

- Acceso entre servicios: algunos Servicios de AWS utilizan características de otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon S3 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.
  - Reenviar sesiones de acceso (FAS): cuando utiliza un IAM usuario o un rol para llevar a cabo acciones en AWS, se le considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el solicitante Servicio de AWS para realizar solicitudes a servicios posteriores. FASlas solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre las políticas a la hora de realizar FAS solicitudes, consulte Forward access sessions.
  - Rol de servicio: un rol de servicio es un IAMrol que adopta un servicio para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentro deIAM. Para obtener más información, consulte Crear un rol para delegar permisos Servicio de AWS en un rol en el IAMManual del usuario.
  - Rol vinculado a servicios: un rol vinculado a servicios es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- 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 que realizan AWS CLI o AWS API solicitan. Es preferible hacerlo de este modo a almacenar claves de EC2 acceso. Para asignar un AWS rol de a una EC2 instancia y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia asociado a ella. Un perfil de instancia contiene el rol y permite a los programas que se encuentran en ejecución en la EC2 instancia obtener 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

AWS Para controlar el acceso en, se crean políticas y se asocian a AWS identidades o recursos de. Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando una entidad principal (sesión de rol, usuario o usuario raíz) 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 política, consulte Información general de JSON políticas en la Guía del IAM usuario de.

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

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

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

### Políticas basadas en identidad

Las políticas basadas en identidad son documentos de políticas de JSON permisos que puede asociar 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 asociar a varios usuarios, grupos y roles de su Cuenta de AWS. Las políticas administradas incluyen las políticas AWS administradas por y las políticas administradas por. Para obtener más información acerca

de cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del IAMusuario de.

### Políticas basadas en recursos

Las políticas basadas en recursos son documentos JSON de políticas que se asocian 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. Las entidades principales pueden incluir cuentas, usuarios, usuarios, usuarios federados o servicios de. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No se puede utilizar políticas AWS administradas de desde IAM en una política basada en recursos.

### Listas de acceso (ACLACLs)

Las listas de control de acceso (ACLs) controlan qué entidades principales (miembros de cuentas, 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 JSON de política.

Amazon S3 AWS WAF y Amazon VPC son ejemplos de servicios compatiblesACLs. Para obtener más informaciónACLs, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

### Otros tipos de políticas

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

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

los permisos, consulte Límites de permisos para IAM las entidades de en la Guía del IAM usuario de.

- Políticas de control de servicio (SCPs): SCPs son JSON políticas que especifican los permisos máximos para una organización o unidad organizativa (OU) en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de forma centralizada varias Cuentas de AWS que posee su negocio. Si habilita todas las funciones de una organización, entonces podrá aplicar políticas de control de servicios (SCPs) a una o todas sus cuentas. SCPLimita los permisos para las entidades de las cuentas miembro, incluido cada Usuario raíz de la cuenta de AWS. Para obtener más información sobre OrganizationsSCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.
- 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 acerca de cómo AWS decide si permitir o no una solicitud cuando hay varios tipos de políticas implicados, consulte Lógica de evaluación de políticas en la Guía del IAM usuario de.

## Cómo funciona AWS End User Messaging Social con IAM

Antes de administrar el acceso IAM a AWS End User Messaging Social, conozca qué IAM funciones están disponibles para usar con AWS End User Messaging Social.

IAMfunciones que puede utilizar con AWS End User Messaging Social

| IAMfunción | AWS Soporte social de mensajería para usuarios finales |
| --- | --- |
| Políticas basadas en identidades | Sí |

| IAMfunción | AWS Soporte social de mensajería para usuarios finales |
| --- | --- |
| Políticas basadas en recursos | No |
| Acciones de políticas | Sí |
| Recursos de políticas | Sí |
| Claves de condición de política | Sí |
| ACLs | No |
| ABAC(etiquetas en las políticas) | Parcial |
| Credenciales temporales | Sí |
| Permisos de entidades principales | Sí |
| Roles de servicio | Sí |
| Roles vinculados al servicio | Sí |

Para obtener una visión general de cómo funcionan los servicios sociales de mensajería para el usuario AWS final y otros AWS servicios con la mayoría de IAM las funciones, consulte AWS los servicios con los que funcionan IAM en la Guía del IAM usuario.

## Políticas basadas en identidad para la Administración de AWS costos de

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de JSON permisos que puede asociar 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 identidad, puede especificar las acciones y 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 identidad para la Administración AWS de costos de

Para ver ejemplos de políticas basadas en identidad social para usuarios AWS finales, consulte. Ejemplos de políticas basadas en identidad para la Administración AWS de costos de

## Políticas basadas en AWS recursos de

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos JSON de políticas que se asocian 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. Las entidades principales pueden incluir cuentas, usuarios, usuarios, usuarios federados o servicios de. Servicios de AWS

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

## Acciones políticas para la mensajería social para usuarios AWS finales

Compatibilidad con las acciones de política: sí

Los administradores pueden utilizar AWS JSON las políticas de 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 de la política generalmente tienen el mismo nombre que la AWS API operación de asociada. Hay algunas excepciones, como acciones de solo permiso 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 mensajería social del usuario AWS final, consulte las acciones definidas por el usuario AWS final que envía mensajes a redes sociales en la Referencia de autorización del servicio.

Las acciones de políticas de AWS End User Messing Social utilizan el siguiente prefijo antes de la acción:

```
social-messaging
```

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

```
"Action": [
      "social-messaging:action1",
      "social-messaging:action2"
         ]
```

Para ver ejemplos de políticas basadas en identidad social para usuarios AWS finales, consulte. Ejemplos de políticas basadas en identidad para la Administración AWS de costos de

## Recursos de políticas para la mensajería social para usuarios AWS finales

Compatibilidad con los recursos de políticas: sí

Los administradores pueden utilizar AWS JSON las políticas de 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 la política especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede

hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

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

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

Para ver una lista de los tipos de recursos sociales de mensajería para usuarios AWS finales y sus respectivos recursosARNs, consulte los recursos definidos por AWS End User Messaging Social en la referencia de autorización del servicio. Para obtener información sobre las acciones con las que puede especificar cada recursos, consulte Acciones definidas por AWS End User Messaging Social. ARN

Para ver ejemplos de políticas basadas en identidad social para usuarios AWS finales, consulte. Ejemplos de políticas basadas en identidad para la Administración AWS de costos de

## Claves de condiciones de política AWS para la Administración de costos de

Compatibilidad con claves de condición de políticas específicas del servicio: sí

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

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

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

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de IAM usuario de para acceder a un recurso solo si está etiquetado

con su nombre de IAM usuario de. 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 globales. Para ver todas las claves de condición AWS globales de, consulte Claves de contexto de condición AWS globales de en la Guía del IAM usuario de.

Para ver una lista de las claves de condición de la mensajería social para el usuario AWS final, consulte las claves de condición de la mensajería social para el usuario AWS final en la Referencia de autorización del servicio. Para obtener más información acerca de las acciones y los recursos con los que puede utilizar una clave de condición, consulte Acciones definidas por AWS End User Messaging Social.

Para ver ejemplos de políticas basadas en identidad social para usuarios AWS finales, consulte. Ejemplos de políticas basadas en identidad para la Administración AWS de costos de

## ACLsen AWS End User Messaging Social

SoportesACLs: No

Las listas de control de acceso (ACLs) controlan qué entidades principales (miembros de cuentas, 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 JSON de política.

## ABACcon AWS End User Messaging Social

Soportes ABAC (etiquetas en las políticas): parciales

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

ABACes útil en entornos que están creciendo rápidamente y ayuda con situaciones en las que la administración de políticas resulta engorrosa.

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

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

Para obtener más información 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 AWS

Compatibilidad con credenciales temporales: sí

Algunos Servicios de AWS no funcionan cuando inicia sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta la sección Servicios de AWS Cómo trabajar con credenciales temporales IAM en la Guía del IAM usuario.

Utiliza credenciales temporales si inicia sesión en la AWS Management Console con cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accede a AWS utilizando el enlace de inicio de sesión único (SSO) de la 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 con la tecla 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. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

## Permisos de entidades principales entre servicios de AWS

Admite sesiones de acceso directo (FASFAS):

Cuando utiliza un IAM usuario o un rol para realizar acciones en AWS, se le considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el solicitante Servicio de AWS para realizar solicitudes a servicios posteriores. FASlas solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completarse. En este caso, debe tener

permisos para realizar ambas acciones. Para obtener información detallada sobre las políticas a la hora de realizar FAS solicitudes, consulte Forward access sessions.

### Funciones de servicio de mensajería social para usuarios AWS finales

Compatibilidad con roles de servicio: sí

Un rol de servicio es un IAMrol de que asume un servicio para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentro deIAM. Para obtener más información, consulte Crear un rol para delegar permisos Servicio de AWS en un rol en el IAMManual del usuario.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de AWS End User Messaging Social. Edite los roles de servicio solo cuando AWS End User Messaging Social proporcione orientación para hacerlo.

### Funciones vinculadas al servicio para AWS End User Messaging Social

Admite roles vinculados al servicio: sí

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

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

## Ejemplos de políticas basadas en identidad para la Administración AWS de costos de

De forma predeterminada, los usuarios y roles no tienen permiso para crear ni modificar recursos sociales de AWS End User Messaging. Tampoco pueden realizar tareas con AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS API. Un IAM administrador de puede

crear IAM políticas de para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede agregar las IAM políticas de a los roles y los usuarios pueden asumirlos.

Para obtener información sobre cómo crear una política IAM basada en la identidad mediante estos documentos de JSON política de ejemplo, consulte Creación de IAM políticas en la Guía del IAMusuario.

Para obtener más información sobre las acciones y los tipos de recursos definidos por AWS End User Messaging Social, incluido el formato de ARNs para cada tipo de recurso, consulte Acciones, recursos y claves de condición para AWS End User Messaging Social en la Referencia de autorizaciones de servicio.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola social de mensajería para usuarios AWS finales
- Cómo permitir a los usuarios consultar sus propios permisos

## Prácticas recomendadas sobre las políticas

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

- Comience con las políticas AWS administradas por y continúe con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de trabajo, utilice las políticas AWS administradas por, que conceden permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Se recomienda definir políticas administradas por el AWS cliente específicas para sus casos de uso a fin de reducir aún más los permisos. Para obtener más información, consulte las políticas AWS gestionadas o las políticas AWS gestionadas para las funciones laborales en la Guía del IAM usuario.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con IAM políticas de, 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 condiciones en IAM las políticas de para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse utilizandoSSL. También puede utilizar condiciones para conceder acceso a acciones de servicios si se emplean a través de un determinado como Servicio de AWS, por ejemplo, AWS CloudFormation. Para obtener más información, consulte los elementos IAM JSON de la política: Condición en la Guía del IAM usuario.
- Utilice el analizador de IAM acceso para validar IAM las políticas con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de IAM acceso valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas y IAM las prácticas recomendadas. IAM IAMAccess Analyzer proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar 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.
- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesita IAM usuarios raíz o de usuarios raíz en su Cuenta de AWS, actívela MFA para mayor seguridad. Para solicitar MFA cuando se API invocan las operaciones, agregue 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 recomendadas deIAM, consulte las Prácticas recomendadas de seguridad en en en IAM en la Guía del IAM usuario de.

## Uso de la consola social de mensajería para usuarios AWS finales

Para acceder a la consola social de AWS End User Messaging, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle registrar y consultar los detalles sobre los recursos sociales de mensajería para usuarios AWS finales en su Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a la AWS CLI o a AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la API operación que intenta realizar.

Para asegurarse de que los usuarios y los roles puedan seguir utilizando la AWS consola social de mensajería para usuarios AWS finales, adjunte también a las entidades la política `ReadOnly` AWS

administrada por. *ConsoleAccess* Para obtener más información, consulte Añadir permisos a un usuario en la Guía del IAM usuario.

## Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a IAM los usuarios ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para llevar a cabo esta acción en la consola o mediante programación con la 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": "*"
        }
    ]
}
```

# AWS políticas administradas para AWS End User Messaging Social

Para agregar permisos a usuarios, grupos y roles, es más fácil utilizar las políticas AWS administradas de que escribirlas uno mismo. Se necesita tiempo y experiencia para crear políticas administradas por el IAM cliente de que le proporcionen a su equipo solo los permisos necesarios. Para comenzar a hacerlo con rapidez, puede utilizar nuestras políticas AWS administradas de. Estas políticas cubren casos de uso comunes y están disponibles en su Cuenta de AWS. Para obtener más información sobre las políticas AWS administradas, consulte las políticas AWS administradas en la Guía del IAM usuario.

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

Además, AWS admite políticas administradas para funciones de trabajo que abarcan varios servicios. Por ejemplo, la política ReadOnlyAccess AWS administrada proporciona acceso de solo lectura a todos los AWS servicios y recursos de. Cuando un servicio lanza una nueva característica, AWS agrega permisos de solo lectura para las operaciones y los recursos nuevos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte políticas AWS administradas de para funciones de trabajo en la Guía del IAM usuario de.

## AWS Los usuarios finales envían mensajes sociales a las actualizaciones de las políticas AWS gestionadas

Es posible consultar los detalles sobre las actualizaciones de las políticas AWS administradas por para AWS End User Messaging Social debido a que este servicio comenzó a realizar el seguimiento

de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la RSS fuente en la página Historial de documento social de mensajería para el usuario AWS final de.

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| AWS End User Messaging Social comenzó a registrar los cambios | AWS End User Messaging Social comenzó a realizar un seguimiento de los cambios de las políticas AWS administr adas de. | 26 de septiembre de 2024 |

## Solución de problemas de identidad y acceso a la mensajería para usuarios AWS finales en redes sociales

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con AWS End User Messaging Social yIAM.

Temas

- No tengo autorización para realizar una acción AWS en Amazon.
- No tengo autorización para realizar una acción en PassRole
- Quiero permitir a personas externas a mí el acceso Cuenta de AWS a mis recursos sociales de mensajería para usuarios AWS finales

### No tengo autorización para realizar una acción AWS en Amazon.

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el `mateojackson` IAM usuario intenta utilizar la consola para ver detalles sobre un *`my-example-widget`* recurso ficticio, pero no tiene `social-messaging:`*`GetWidget`* permisos ficticios.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: social-
messaging:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `social-messaging:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador de. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

## No tengo autorización para realizar una acción en PassRole

Si recibe un error que indica que no tiene autorización para realizar la `iam:PassRole` acción, las políticas deben actualizarse a fin de permitirle pasar un rol a AWS End User Messaging Social.

Algunos Servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un IAM usuario denominado `marymajor` intenta utilizar la consola para realizar una acción en AWS End User Messaging Social. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador de. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

## Quiero permitir a personas externas a mí el acceso Cuenta de AWS a mis recursos sociales de mensajería para usuarios AWS finales

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACLs), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si AWS End User Messaging Social admite estas características, consulteCómo funciona AWS End User Messaging Social con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte Proporcionar acceso a un IAM usuario a otra de la Cuenta de AWS que es propietario en la Guía del IAM usuario de.
- Para obtener información sobre cómo proporcionar acceso a los recursos a de terceros Cuentas de AWS, consulte Proporcionar acceso a que Cuentas de AWS son propiedad de terceros en la Guía del IAM usuario de.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticadoPara que su aplicación pueda acceder a s externamente (federación de identidades) en la Guía del IAM usuario de.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas IAM en la Guía del IAM usuario de.

# Validación del cumplimiento de la mensajería social para AWS usuarios finales

Para saber si un Servicio de AWS está incluido en el ámbito de programas de conformidad específicos, consulte Servicios de AWS en el ámbito del programa de conformidad Servicios de AWS y escoja el programa de conformidad que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

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

Su responsabilidad de conformidad al utilizarlos Servicios de AWS se determina en función de la confidencialidad de los datos, los objetivos de conformidad de su empresa, así como de la legislación y los reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con la conformidad:

- Guías de inicio rápido de seguridad y conformidad: estas guías de implementación tratan consideraciones sobre arquitectura y ofrecen pasos para implementar entornos de referencia centrados en AWS la seguridad y la conformidad normativa.

- Architecting for Quick and Compliance on Amazon Web Services (Arquitectura para la HIPAA seguridad y la conformidad en Amazon Web Services): en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear HIPAA aplicaciones aptas para.

  > **Note**
  >
  > No todos son aptos. Servicios de AWS HIPAA Para obtener más información, consulte la Referencia de servicios HIPAA válidos.

- AWS Recursos de de: esta recopilación de manuales y guías podría aplicarse a su sector y ubicación.
- AWS Guías de cumplimiento para clientes de: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad de los Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Estándares de Seguridad de la Industria de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO).
- Evaluación de recursos con reglas en la Guía para AWS Config desarrolladores de: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: este Servicio de AWS detecta posibles amenazas para sus Cuentas de AWS, cargas de trabajo, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a satisfacer varios requisitos de conformidad, por ejemplo PCIDSS, cumpliendo los requisitos de detección de intrusos que exigen determinados marcos de conformidad.
- AWS Audit Manager: este le Servicio de AWS ayuda a auditar continuamente el AWS uso de con el fin de simplificar la forma en que administra el riesgo y la conformidad con las normativas y los estándares del sector.

# Resiliencia en la mensajería social de los usuarios AWS finales

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

Para obtener más información sobre las Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura AWS global de.

Además de la infraestructura AWS global de, AWS End User Messaging Social ofrece varias características que ayudan con sus necesidades de resiliencia y copia de seguridad de los datos.

# La seguridad de la infraestructura en la mensajería AWS social para usuarios finales

Al tratarse de un servicio administrado, AWS End User Messaging Social está protegido por los procedimientos de seguridad de red AWS globales de que se describen en el documento técnico Amazon Web Services: Información general sobre los procesos de seguridad.

Utiliza las API llamadas AWS publicadas para acceder a AWS End User Messaging Social a través de la red. Los clientes deben ser compatibles con Transport Layer Security (TLSTLS) 1.0 o una versión posterior. Le recomendamos TLS TLS 1.2. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como (Ephemeral Diffie-Hellman) o DHE ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad IAM principal de. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

# Prevención de la sustitución confusa entre servicios

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación entre servicios puede dar lugar al problema de la sustitución confusa. La suplantación entre servicios puede producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puede manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que lo ayudan a proteger sus datos para todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta.

Recomendamos usar las claves de contexto de condición `aws:SourceAccount`global `aws:SourceArn`y las claves de contexto en las políticas de recursos para limitar los permisos que Social Messaging otorga a otro servicio al recurso. Utilice `aws:SourceArn` si desea que solo se asocie un recurso al acceso entre servicios. Utilice `aws:SourceAccount` si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.

La forma más eficaz de protegerse contra el problema del suplente confuso es utilizar la clave del contexto ARN de condición `aws:SourceArn` global con todo el recurso. Si no conoce la totalidad ARN del recurso o si está especificando varios recursos, utilice la clave de condición de contexto `aws:SourceArn` global con caracteres comodines (`*`) para las partes desconocidas delARN. Por ejemplo, `arn:aws:social-messaging:*:`*`123456789012`*`:*`.

Si el `aws:SourceArn` valor no contiene el ID de cuenta, como un bucket de Amazon S3ARN, debe utilizar ambas claves de contexto de condición global para limitar los permisos.

El valor `aws:SourceArn` debe ser  ResourceDescription.

El siguiente ejemplo muestra cómo se pueden utilizar las claves contextuales de condición `aws:SourceAccount` global `aws:SourceArn` y global de en Social Messaging para prevenir el problema del suplente confuso.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
```

```
      "Service": "social-messaging.amazonaws.com"
    },
    "Action": "social-messaging:ActionName",
    "Resource": [
      "arn:aws:social-messaging:::ResourceName/*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:social-messaging:*:123456789012:*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

## Prácticas recomendadas de seguridad

AWS End User Messaging Social proporciona una serie 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.

- Cree un usuario individual para cada persona que administre AWS SMS recursos de, incluido usted mismo. No utilice las credenciales AWS raíz AWS SMS de.
- Asigne a cada usuario el conjunto mínimo de permisos requerido para realizar sus tareas.
- IAMUse los permisos de.
- Rote con regularidad sus credenciales de IAM.

## Uso de un rol vinculado a un AWS servicio de

AWS End User Messaging Social utiliza AWS Identity and Access Management (IAM) roles vinculados al servicio. Un rol vinculado a un servicio es un tipo único de IAM rol que está vinculado directamente a AWS End User Messaging Social. Los roles vinculados a servicios los predefine AWS End User Messaging Social e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios de en su nombre.

Un rol vinculado a un servicio simplifica la configuración de AWS End User Messaging Social porque ya no tendrá que añadir manualmente los permisos necesarios. AWS End User Messaging Social define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo AWS End User Messaging Social puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda asociar a ninguna otra IAM entidad de.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. De esta forma, se protegen los recursos sociales de mensajería para el usuario AWS final, ya que se evita que se puedan eliminar de forma accidental permisos de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte AWS Servicios de que funcionan con IAM y busque los servicios que tienen Sí en la columna Roles vinculados a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

## Permisos de un rol vinculado a un AWS servicio de

AWS End User Messaging Social utiliza el rol vinculado al servicio denominado AWSServiceRoleForSocialMessaging: Para publicar métricas y proporcionar información sobre el envío de tus mensajes a redes sociales.

La función AWSServiceRoleForSocialMessaging vinculada al servicio confía en los siguientes servicios para asumir la función:

- `social-messaging.amazonaws.com`

La política de permisos del rol llamada AWSSocialMessagingServiceRolePolicy permite que el usuario AWS final de Messaging Social realice las siguientes acciones en los recursos especificados:

- Acción: `"cloudwatch:PutMetricData"` en `all AWS resources in the AWS/SocialMessaging namespace.`

Debe configurar los permisos para permitir a sus usuarios, grupos o funciones, crear, editar o eliminar la descripción de un rol vinculado al servicio. Para obtener más información, consulte los permisos de roles vinculados a un servicio en la Guía del IAMusuario.

Para ver las actualizaciones de la política, consulte. AWS Los usuarios finales envían mensajes sociales a las actualizaciones de las políticas AWS gestionadas

## Creación de un rol vinculado a un servicio para AWS sin servidor

Puede utilizar la IAM consola de para crear un rol vinculado al servicio con el caso de uso de AWSEndUserMessagingSocial- Metrics. En AWS CLI o en AWS API, cree un rol vinculado a un servicio con el nombre del servicio. `social-messaging.amazonaws.com` Para obtener más información, consulte Creación de un rol vinculado a un servicio en la Guía del usuario. IAM Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

## Edición de un rol vinculado al servicio para AWS sin servidor

AWS End User Messaging Social no le permite editar el rol AWSServiceRoleForSocialMessaging vinculado al servicio. Después de crear un rol vinculado a un servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al mismo. Sin embargo, puede editar la descripción del rol utilizandoIAM. Para obtener más información, consulte Edición de un rol vinculado a un servicio en la Guía del IAMusuario.

## Eliminación de un rol vinculado al servicio para AWS sin servidor

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se monitorice ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

> **Note**
>
> Si el servicio social de mensajería para el usuario AWS final está utilizando el rol cuando intenta eliminar los recursos, la eliminación podría fallar. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos sociales de mensajería para usuarios AWS finales utilizados por AWSServiceRoleForSocialMessaging

1. Llame `list-linked-whatsapp-business-accounts` API para ver los recursos de los que dispone.
2. Para cada cuenta empresarial de whats app vinculada, llama al `disassociate-whatsapp-business-account` API para eliminar el recurso del SocialMessaging servicio.

3. Vuelva a llamar para comprobar que no se `list-linked-whatsapp-business-accounts` API devuelva ningún recurso.

Para eliminar manualmente el rol vinculado al servicio utilizando IAM

Utilice la IAM consola AWS CLI, la o la AWS API para eliminar la función vinculada al AWSServiceRoleForSocialMessaging servicio. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario. IAM

## Regiones admitidas AWS para los roles vinculados a servicios de

AWS End User Messaging Social admite el uso de roles vinculados a servicios en todas las regiones en las que el servicio esté disponible. Para obtener más información, consulte Puntos de conexión y Regiones de AWS.

# Cuotas de mensajería para usuarios AWS finales en redes sociales

La AWS cuenta de incluye cuotas predeterminadas para cada AWS servicios de (estas cuotas se denominaban anteriormente «límites»). A menos que se indique lo contrario, cada cuota es específica de la región de . Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar.

Para ver las cuotas de AWS End User Messaging Social, abra la consola de Service Quotas. En el panel de navegación, elija AWSservicios y seleccione AWS End User Messaging Social.

Para solicitar un aumento de cuota, consulte Solicitud de aumento de cuota en la Guía del usuario de Service Quotas. Si la cuota aún no se encuentra disponible en Service Quotas, utilice el formulario de aumento del límite.

La AWS cuenta de incluye las siguientes cuotas en relación con AWS End User Messaging Social.

| Recurso | Predeterminado |
| --- | --- |
| WhatsApp Cuenta empresarial (WABA) | 25 por región |

AWS End User Messaging Social implementa cuotas que restringen el número de solicitudes que puede realizar a la red social de mensajería para usuarios AWS finales API desde su cuenta Cuenta de AWS.

| Operación | Tarifa |
| --- | --- |
| SendWhatsAppMessage | 1 000 |
| PostWhatsAppMessageMedia | 100 |
| GetWhatsAppMessageMedia | 100 |
| DeleteWhatsAppMessageMedia | 100 |
| DisassociateWhatsAppBusinessAccount | 10 |

| Operación | Tarifa |
| --- | --- |
| ListWhatsAppBusinessAccount | 10 |
| TagResource | 10 |
| UntagResourceRate | 10 |
| ListTagsForResourceRate | 10 |

# Historial de documentos de la Guía del usuario de AWS End User Messaging Social

En la siguiente tabla se describen las versiones de la documentación de la documentación de AWS la documentación de la documentación de archivo.

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| Versión inicial | Versión inicial de la Guía del usuario de AWS End User Messaging Social | 10 de julio de 2024 |

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.