



Guía de administración

Amazon Chime



Amazon Chime: Guía de administración

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

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

Table of Contents

.....	vii
¿Qué es Amazon Chime?	1
Información general sobre la administración	1
Cómo empezar	1
Precios	2
Recursos	2
Requisitos previos para los administradores del sistema Amazon Chime	3
Creación de una cuenta de Amazon Web Services	3
Registro para obtener una Cuenta de AWS	3
Crear un usuario administrativo	4
Introducción	6
Paso 1: Crear una cuenta de administrador de Amazon Chime	6
Paso 2 (opcional): Configurar los ajustes de la cuenta	7
Paso 3: Agregar usuarios a la cuenta	8
(Opcional) Configuración de los números de teléfono para su cuenta de Amazon Chime	9
Administración de cuentas	10
Elegir una cuenta de equipo o corporativa	10
Para convertir una cuenta de equipo en una cuenta corporativa	11
Cambiar el nombre de una cuenta	12
Eliminar una cuenta	13
Administración de la configuración de la reunión	15
Configuración de la política de la reunión	15
Configuración de la aplicación de reuniones	15
Configuración de la región de la reunión	16
Administración de políticas de retención de chat	16
Cómo afectan las políticas de retención a los usuarios de Amazon Chime	17
Activación de la retención de chat	19
Restaurar los mensajes de chat	20
Eliminar mensajes de chat	21
Solicitar un dominio	22
Conexión con Active Directory	24
Requisitos previos	24
Conexión a Active Directory en Amazon Chime	25
Configuración de varias direcciones de correo electrónico	25

Conexión con Okta SSO	27
Implementación del complemento para Outlook	30
Configuración de la aplicación Amazon Chime Meetings para Slack	31
Instalación de la aplicación Amazon Chime Meetings para Slack en una organización	31
Instalación de la aplicación Amazon Chime Meetings para Slack en los espacios de trabajo	33
Migración de espacios de trabajo a organizaciones	33
Asociación de espacios de trabajo con cuentas de equipo de Amazon Chime	33
Administración de usuarios	36
Añadir usuarios	36
Ver los datos de los usuarios	37
Administración del acceso y los permisos de los usuarios	39
Administración de permisos de usuario	40
Administración del acceso de los usuarios	41
Cambio del PIN personal de las reuniones	43
Administración de versiones de prueba Pro	44
Solicitar archivos adjuntos de los usuarios	44
Cómo gestiona Amazon Chime las actualizaciones automáticas	45
Migración de usuarios a otra cuenta de equipo	46
Administración de números de teléfono	48
Aprovisionamiento de números de teléfono	49
Solicitud de números de teléfono internacionales	50
Requisitos nacionales para los números de teléfono	51
Portabilidad de números de teléfono existentes	70
Requisitos previos para la portabilidad de números	70
Transferencia de números de teléfono al SDK de Amazon Chime	71
Presentación de los documentos requeridos	73
Ver el estado de la solicitud	74
Asignación de números portados	74
Transferencia de números de teléfono del SDK de Amazon Chime	75
Definiciones de estado de portabilidad de números de teléfono	76
Asignación de números de teléfono	77
Anular la asignación de números de teléfono	78
Actualización de nombres de llamadas salientes	78
Eliminación de números de teléfono	80
Restauración de números de teléfono eliminados	81

Administración de la configuración global	82
Configuración de registros de detalles de las llamadas	82
Registros detallados de llamadas de Amazon Chime Business Calling	83
Configuración de salas de conferencias	85
Cómo unirse a una reunión moderada	86
Dispositivos VTC compatibles	86
Requisitos de configuración de red y ancho de banda	88
Visualización de informes	92
Ampliación del cliente de escritorio de Amazon Chime	93
Administración de usuarios	93
Invitar a varios usuarios	93
Descarga de la lista de usuarios	94
Cierre de varias sesiones	94
Actualización de los PIN personales de los usuarios	95
Integración de los chatbots	95
Usar chatbots con Amazon Chime	96
Eventos de Amazon Chime enviados a los chatbots	105
Sesiones de teléfono de proxy	107
Creación de webhooks	108
Solución de errores relacionados con los webhooks	110
Ayuda con la administración	112
Seguridad	113
Administración de identidades y accesos	114
Público	114
Autenticación con identidades	115
Administración de acceso mediante políticas	118
Cómo funciona Amazon Chime con IAM	121
Políticas de Amazon Chime basadas en identidades	122
Recursos	122
Ejemplos	123
Prevención de la sustitución confusa entre servicios	123
Políticas de Amazon Chime basadas en recursos	124
Autorización basada en etiquetas de Amazon Chime	124
Roles de IAM de Amazon Chime	124
Uso de credenciales temporales con Amazon Chime	124
Roles vinculados al servicio	125

Roles de servicio	125
Ejemplos de políticas basadas en identidades	125
Prácticas recomendadas relativas a políticas	126
Uso de la consola Amazon Chime	127
Otorgue a los usuarios acceso completo a Amazon Chime	128
Cómo permitir a los usuarios consultar sus propios permisos	129
Permitir que los usuarios accedan a las acciones de administración de usuarios	130
Política administrada por AWS: AmazonChimeVoiceConnectorServiceLinkedRolePolicy	132
Actualizaciones de Amazon Chime en las políticas administradas por AWS	132
Resolución de problemas	133
No tengo autorización para realizar una acción en Amazon Chime	134
No tengo autorización para realizar la operación iam:PassRole	134
Quiero permitir que personas ajenas a mi cuenta de AWS accedan a mis recursos de Amazon Chime.	135
Uso de roles vinculados a servicios	135
Uso de roles con dispositivos compartidos	136
Uso de roles con transcripción en vivo	139
Uso de roles con canalizaciones de contenido multimedia	141
Registro y monitoreo	144
Monitoreo con CloudWatch	145
Automatizar con EventBridge	158
Registro de llamadas a la API del servicio	163
Validación de conformidad	165
Resiliencia	167
Seguridad de la infraestructura	167
Descripción de las actualizaciones automáticas de Amazon Chime	168
Historial de documentos	170

Debe ser administrador del sistema Amazon Chime para completar los pasos de esta guía. Si necesita ayuda con el cliente de escritorio, la aplicación web o la aplicación móvil de Amazon Chime, consulte [Obtener asistencia](#) en la Guía del usuario de Amazon Chime.

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

¿Qué es Amazon Chime?

Amazon Chime es un servicio de comunicaciones que transforma las reuniones online con una aplicación segura e integral. Amazon Chime funciona perfectamente en todos sus dispositivos para que pueda permanecer conectado. Puede utilizar Amazon Chime para reuniones online, videoconferencias, llamadas y chat. También puede compartir contenido dentro y fuera de la organización. Amazon Chime es un servicio totalmente administrado que se ejecuta de forma segura en la nube de AWS y que libera al equipo de TI de las tareas de implementación y administración de infraestructuras complejas.

Para obtener más información, consulte [Amazon Chime](#).

Información general sobre la administración

Como administrador, utilizará la [consola Amazon Chime](#) para realizar tareas clave, como la creación de cuentas de Amazon Chime y la administración de usuarios y permisos. Debe tener una cuenta de Amazon Chime para obtener acceso a la consola Amazon Chime y crear una cuenta de administrador de AWS. Para obtener más información, consulte [Requisitos previos para los administradores del sistema Amazon Chime](#).

Cómo empezar

Después de completar los [Requisitos previos para los administradores del sistema Amazon Chime](#), puede crear y configurar su cuenta administrativa de Amazon Chime y, a continuación, añadir usuarios a ella. Elija permisos Pro o Basic para sus usuarios.

Si está listo para empezar ahora, consulte el siguiente tutorial:

- [Introducción](#)

Para obtener más información acerca del acceso y los permisos de usuario, consulte [Administración del acceso y los permisos de los usuarios](#). Para obtener más información acerca de las características a las que los usuarios con permisos Pro y Basic tienen acceso, consulte [Planes y precios](#).

Precios

Amazon Chime ofrece precios basados en el uso. Solo se paga por los usuarios con permisos Pro que organizan reuniones y solo en los días en que las organizan. No se cobra por los asistentes a las reuniones ni por los usuarios de chat.

No se le aplicará ningún cargo por los usuarios con permisos Basic. Los usuarios Basic no pueden organizar reuniones, pero pueden asistir a ellas y utilizar el chat. Para obtener más información acerca de los precios y las características a las que los usuarios con permisos Pro y Basic tienen acceso, consulte [Planes y precios](#).

Recursos

Para obtener más información acerca de los permisos de Amazon Chime, consulte los siguientes recursos:

- [Centro de ayuda de Amazon Chime](#)
- [Vídeos de formación sobre Amazon Chime](#)

Requisitos previos para los administradores del sistema Amazon Chime

Debe tener una cuenta de AWS para obtener acceso a la [consola Amazon Chime](#) y crear una cuenta de administrador de Amazon Chime.

Creación de una cuenta de Amazon Web Services

Antes de crear una cuenta de administrador de Amazon Chime, primero debe crear una cuenta de AWS.

Temas

- [Registro para obtener una Cuenta de AWS](#)
- [Crear un usuario administrativo](#)

Registro para obtener una Cuenta de AWS

Si no dispone de una Cuenta de AWS, siga estos pasos para crear una.

Cómo registrarse en una Cuenta de AWS

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

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

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

AWS le enviará un correo electrónico 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 Mi cuenta.

Crear un usuario administrativo

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

Protección de su Usuario raíz de la cuenta de AWS

1. Inicie sesión en la [AWS Management Console](#) como propietario de cuenta, elija Usuario raíz e ingrese el email de su Cuenta de AWS. 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 dispositivo MFA virtual para el usuario raíz de la Cuenta de AWS \(consola\)](#) en la Guía del usuario de IAM.

Creación de un usuario administrativo

1. Activar IAM Identity Center

Para obtener instrucciones, consulte [Enabling 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 administrativo.

Para ver un tutorial sobre cómo utilizar Directorio de IAM Identity Center como origen de identidad, consulte [Configure user access with the default Directorio de IAM Identity Center](#) en la Guía del usuario de AWS IAM Identity Center.

Cómo iniciar sesión como usuario administrativo

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

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

Para obtener más información sobre la configuración de una cuenta de administrador de Amazon Chime, consulte [Introducción](#).

Introducción

La forma más sencilla de que los usuarios comiencen a usar Amazon Chime consiste en descargar y utilizar la versión Pro de Amazon Chime durante 30 días de forma gratuita. Para obtener más información, consulte el tema dónde se describe cómo [descargar Amazon Chime](#).

Comprar Amazon Chime

Para seguir utilizando la versión Pro de Amazon Chime después del período de prueba gratuita de 30 días, debe crear una cuenta de administrador de Amazon Chime y añadir usuarios a ella. Para empezar, primero debe completar los [Requisitos previos para los administradores del sistema Amazon Chime](#), que incluyen la creación de una cuenta de AWS. A continuación, puede crear y configurar una cuenta de administrador de Amazon Chime y añadir usuarios a ella realizando las siguientes tareas.

Tareas

- [Paso 1: Crear una cuenta de administrador de Amazon Chime](#)
- [Paso 2 \(opcional\): Configurar los ajustes de la cuenta](#)
- [Paso 3: Agregar usuarios a la cuenta](#)
- [\(Opcional\) Configuración de los números de teléfono para su cuenta de Amazon Chime](#)

Paso 1: Crear una cuenta de administrador de Amazon Chime

Después de completar los [Requisitos previos para los administradores del sistema Amazon Chime](#), puede crear una cuenta de administrador de Amazon Chime.

Para crear una cuenta de administrador de Amazon Chime

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En la página Accounts (Cuentas), elija New account (Cuenta nueva).
3. En Account Name (Nombre de cuenta), escriba un nombre para la cuenta y elija Create account (Crear cuenta).
4. (Opcional) Decida si desea que Amazon Chime seleccione la región óptima de AWS para sus reuniones entre todas las regiones disponibles o utilice solo las regiones que seleccione. Para obtener más información, consulte [Administración de la configuración de la reunión](#).

Paso 2 (opcional): Configurar los ajustes de la cuenta

De forma predeterminada, las cuentas nuevas se crean como cuentas de equipo. Si prefiere solicitar un dominio y conectarse a su propio proveedor de identidades o a Okta SSO, puede convertir su cuenta a una corporativa. Para obtener más información sobre los tipos de cuentas corporativas y de equipo, consulte [Elegir entre una cuenta de equipo o corporativa de Amazon Chime](#).

Para convertir una cuenta de equipo en una cuenta corporativa

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En Accounts (Cuentas), elija el nombre de la cuenta.
3. En Identity (Identidad), elija Getting Started (Introducción).
4. Siga los pasos de la consola para reclamar su dominio.
5. (Opcional) Siga los pasos de la consola para configurar su proveedor de identidad y configurar su grupo de directorio.

Para obtener más información sobre cómo solicitar dominios, consulte [Solicitar un dominio](#). Para obtener más información sobre cómo configurar proveedores de identidad, consulte [Conectarse a Active Directory](#) y [Conexión con Okta SSO](#).

También puede permitir o prohibir políticas de cuenta para opciones como el control remoto de pantallas compartidas y la característica “Llámame” de Amazon Chime.

Para configurar políticas de cuenta:

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En la página Accounts (Cuentas), seleccione el nombre de la cuenta que desea configurar.
3. En Settings (Configuración), seleccione Meetings (Reuniones).
4. En Políticas (Políticas), seleccione o desactive las opciones de política de cuenta que desea permitir o prohibir.
5. Elija Change.

Para obtener más información, consulte [Administración de la configuración de la reunión](#).

Paso 3: Agregar usuarios a la cuenta

Una vez creada la cuenta de equipo de Amazon Chime, invítese a sí mismo y a sus usuarios para unirse a ella. Si actualiza la cuenta a una cuenta corporativa, no es necesario que invite a los usuarios. En ese caso, actualice a una cuenta corporativa y solicite el dominio. Para obtener más información, consulte [Paso 2 \(opcional\): Configurar los ajustes de la cuenta](#).

Para añadir usuarios a una cuenta de Amazon Chime

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En la página Accounts (Cuentas), elija el nombre de la cuenta.
3. En la página Users (Usuarios), elija Invite users (Invitar a usuarios).
4. Escriba las direcciones de correo electrónico de los usuarios a los que va invitar, incluido usted mismo, y elija Invite users (Invitar a usuarios).

Los usuarios invitados recibirán por correo electrónico invitaciones para unirse a la cuenta de equipo de Amazon Chime que ha creado. Cuando registren sus cuentas de usuario de Amazon Chime, recibirán permisos Pro de forma predeterminada y terminará su versión de evaluación de 30 días. Si ya se han inscrito para obtener una cuenta de usuario de Amazon Chime con su dirección de correo electrónico del trabajo, podrán seguir utilizando esa cuenta. También pueden descargar la aplicación cliente Amazon Chime en cualquier momento seleccionando Descargar Amazon Chime e iniciando sesión en su cuenta de usuario.

Solo se le cobrará por un usuario con permisos Pro cuando ese usuario organice una reunión. No se le aplicará ningún cargo por los usuarios con permisos Basic. Los usuarios Basic no pueden organizar reuniones, pero pueden asistir a ellas y utilizar el chat. Para obtener más información acerca de los precios y las características a las que los usuarios con permisos Pro y Basic tienen acceso, consulte [Planes y precios](#).

Para cambiar los permisos del usuario

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En la página Accounts (Cuentas), elija el nombre de la cuenta.
3. En la página Users (Usuarios), seleccione el usuario o usuarios cuyos permisos desea cambiar.
4. Elija User actions (Acciones de usuario), Assign user permission (Asignar permiso de usuario).
5. En Permissions (Permisos), seleccione Pro o Basic.

6. Elija Assign (Asignar).

Puede proporcionar a otros usuarios permisos de administrador y controlar su acceso a la consola Amazon Chime de la cuenta. Para obtener más información, consulte [Administración de identidades y accesos para Amazon Chime](#).

(Opcional) Configuración de los números de teléfono para su cuenta de Amazon Chime

Las siguientes opciones de teléfono están disponibles para las cuentas administrativas de Amazon Chime:

Amazon Chime Business Calling

Permite a sus usuarios enviar y recibir llamadas telefónicas y mensajes de texto directamente desde Amazon Chime. Aprovechone los números de teléfono en la consola Amazon Chime o transfiera los números de teléfono existentes. Asigne los números de teléfono a sus usuarios de Amazon Chime y concédalos permisos para enviar y recibir llamadas y mensajes de texto con Amazon Chime. Para obtener más información, consulte [Administración de números de teléfono en Amazon Chime](#) y [Portabilidad de números de teléfono existentes](#).

Amazon Chime Voice Connector

Proporciona un servicio de enlace troncal SIP para un sistema telefónico existente. Transfiera los números de teléfono existentes o aprovisiona números de teléfono nuevos en la consola Amazon Chime. Para obtener más información, consulte [Administración de instancias de Amazon Chime Voice Connector](#) en la Guía de administración del SDK de Amazon Chime.

Administración de las cuentas de Amazon Chime

Puede usar Amazon Chime como usuario individual o como grupo sin administradores. Sin embargo, si desea añadir funciones de administrador o comprar Amazon Chime Pro, debe crear una cuenta de Amazon Chime en la AWS Management Console. Para obtener información sobre cómo crear una cuenta de administrador de Amazon Chime o para obtener más información sobre la compra de Amazon Chime Pro, consulte [Introducción](#).

Para obtener más información acerca de los distintos tipos de cuentas de administrador de Amazon Chime, consulte [Elegir entre una cuenta de equipo o corporativa de Amazon Chime](#). Para obtener más información acerca de la administración de una cuenta de administrador existente, consulte los siguientes temas.

Temas

- [Elegir entre una cuenta de equipo o corporativa de Amazon Chime](#)
- [Para convertir una cuenta de equipo en una cuenta corporativa](#)
- [Cambiar el nombre de una cuenta](#)
- [Eliminar una cuenta](#)
- [Administración de la configuración de la reunión](#)
- [Administración de políticas de retención de chat](#)
- [Restaurar los mensajes de chat](#)
- [Eliminar mensajes de chat](#)
- [Solicitar un dominio](#)
- [Conectarse a Active Directory](#)
- [Conexión con Okta SSO](#)
- [Implementación del complemento de Amazon Chime para Outlook](#)
- [Configuración de la aplicación Amazon Chime Meetings para Slack](#)

Elegir entre una cuenta de equipo o corporativa de Amazon Chime

Al crear una cuenta de administrador de Amazon Chime, puede elegir si desea crear una cuenta de equipo o una corporativa. Para obtener más información acerca de cómo crear una cuenta de administrador de Amazon Chime, consulte [Introducción](#).

Cuenta de equipo

Con una cuenta de equipo, puede invitar a usuarios y concederles permisos de Amazon Chime Pro sin solicitar un dominio de correo electrónico. Para obtener más información sobre los permisos Pro y Basic, consulte [Planes y precios](#).

Puede invitar a usuarios de cualquier dominio de correo electrónico que no lo haya reclamado otra organización. Solo se paga por los usuarios cuando estos organizan reuniones. Los usuarios de su cuenta de equipo pueden usar la aplicación Amazon Chime para buscar a otros usuarios de Amazon Chime que estén registrados en la misma cuenta y ponerse en contacto con ellos. Asimismo, recomendamos optar por una cuenta de equipo para pagar por los usuarios Pro que no pertenezcan a la organización.

Cuenta corporativa

Con una cuenta corporativa, tendrá un mayor control sobre los usuarios de los dominios de su organización. Puede elegir conectarse a su propio proveedor de identidad o a Okta SSO para autenticarse y asignar permisos Pro o Basic. Amazon Chime también es compatible con Microsoft Active Directory.

Para crear una cuenta corporativa, debe solicitar al menos un dominio de correo electrónico. Esto garantiza que todos los usuarios que se unan a Amazon Chime a través de sus dominios reclamados estén incluidos en su cuenta de Amazon Chime administrada de forma centralizada. Las cuentas corporativas son necesarias para administrar los usuarios a través de una integración de directorios compatibles. Para más información, consulte [Solicitar un dominio](#) y [Conectarse a Active Directory](#).

También puede gestionar la activación y suspensión de usuarios desde su cuenta corporativa. Para obtener más información, consulte [Administración del acceso y los permisos de los usuarios](#).

Para convertir una cuenta de equipo en una cuenta corporativa

Para convertir una cuenta de equipo existente en una cuenta corporativa, solicite uno o más dominios de correo electrónico en la consola Amazon Chime. Para obtener más información sobre las cuentas de equipo y corporativas, consulte [Elegir entre una cuenta de equipo o corporativa de Amazon Chime](#). Para obtener más información sobre cómo solicitar un dominio, consulte [Solicitar un dominio](#).

Para convertir una cuenta de equipo en una cuenta corporativa

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.

2. En Accounts (Cuentas), elija el nombre de la cuenta.
3. En Identity (Identidad), elija Getting Started (Introducción).
4. Siga los pasos de la consola para reclamar su dominio.
5. (Opcional) Siga los pasos de la consola para configurar su proveedor de identidad y configurar su grupo de directorio.

Después de convertir su cuenta en una cuenta Enterprise, puede decidir si desea conectar una instancia de Active Directory a través de ella AWS Directory Service. La conexión a una instancia de Active Directory permite a los usuarios iniciar sesión en Amazon Chime con sus credenciales de Active Directory. Para obtener más información, consulte [Conectarse a Active Directory](#).

Si no se conecta con una instancia de Active Directory, los usuarios pueden seguir iniciando sesión en Amazon Chime con Login with Amazon (LWA) o las credenciales de una cuenta de Amazon.com.

Cambiar el nombre de una cuenta

Utilice el siguiente procedimiento para cambiar el nombre de una cuenta. El nuevo nombre que elija aparecerá en los correos electrónicos de invitación que se envíen a los usuarios para que se unan a la cuenta.

Para cambiar el nombre de una cuenta

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En la columna Nombre de cuenta, seleccione la cuenta cuyo nombre quiera cambiar.

Aparece la página Usuarios.

3. En el panel izquierdo, en Configuración, seleccione Cuenta.

Aparece la página Resumen de la cuenta.

4. Abra la lista Acciones de la cuenta y seleccione Cambiar nombre de la cuenta.

Se abre el cuadro de diálogo Cambiar nombre de la cuenta.

5. Introduzca el nombre nuevo de la cuenta y seleccione Guardar.

Eliminar una cuenta

Si eliminas tu AWS cuenta en AWS Management Console, tus cuentas de Amazon Chime se eliminarán automáticamente. También puede usar la consola Amazon Chime para eliminar una cuenta corporativa o de equipo de Amazon Chime.

Note

Los usuarios no administrados de una cuenta corporativa o de equipo pueden solicitar la eliminación utilizando el comando “Elimíname” del asistente de Amazon Chime. Para obtener más información, consulte [Uso del asistente de Amazon Chime](#).

Para eliminar una cuenta de equipo

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. Seleccione la cuenta en la columna Account name (Nombre de cuenta) y seleccione Account (Cuenta) en Settings (Configuración).
3. Aparecerá la página Users (Usuarios) en el panel de navegación.
4. Seleccione los usuarios y elija User actions (Acciones del usuario), Remove user (Eliminar un usuario).
5. En el panel de navegación, elija Accounts (Cuentas), Account actions (Acciones de cuenta) y Delete account (Eliminar cuenta).
6. Confirme que desea eliminar la cuenta.

Amazon Chime elimina todos los datos de usuario al eliminar la cuenta. Esto incluye la cancelación de una AWS cuenta, de cuentas individuales de Amazon Chime o de usuarios de Amazon Chime no gestionados. Se excluyen los datos sin contenido relacionados con las cuentas de usuario y el uso de Amazon Chime (los atributos de servicio que se recogen en el Acuerdo de cliente) que genera Amazon Chime.

Para eliminar una cuenta corporativa

1. Elimine los dominios.

 Note

Al eliminar un dominio, ocurre lo siguiente:

- Se cierra inmediatamente la sesión de los usuarios asociados al dominio en todos los dispositivos y pierden el acceso a todos los contactos, conversaciones de chat y salas de chat.
- Las reuniones programadas por los usuarios de este dominio no se iniciarán.
- Los usuarios suspendidos seguirán mostrándose con el estado Suspended (Suspendido) en las páginas Users (Usuarios) y User detail (Datos del usuario) y no podrán obtener acceso a sus datos. Tampoco podrán crear cuentas de Amazon Chime con su dirección de correo electrónico.
- Los usuarios registrados se mostrarán como Released (Publicado) en las páginas Users (Usuarios) y User detail (Datos del usuario) y no podrán obtener acceso a sus datos. Sí podrán crear una cuenta de Amazon Chime con su dirección de correo electrónico.
- Si tiene una cuenta de Active Directory y elimina un dominio asociado a la dirección de correo electrónico principal de un usuario, el usuario no podrá obtener acceso a Amazon Chime y se eliminará su perfil. Si elimina un dominio asociado a la dirección de correo electrónico secundaria de un usuario, el usuario no podrá iniciar sesión con dicha dirección, pero conservará el acceso a sus contactos y datos de Amazon Chime.
- Si tiene una cuenta corporativa de OpenID Connect (OIDC) y elimina un dominio asociado a la dirección de correo electrónico principal de un usuario, el usuario ya no podrá obtener acceso a Amazon Chime y se eliminará su perfil.

2. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
3. En la página Cuentas, seleccione el nombre de la cuenta de equipo.
4. En el panel de navegación, elija Settings (Configuración), Domains (Dominios).
5. En la página Domains (Dominios), elija Remove domain (Eliminar un dominio).
6. En el panel de navegación, elija Accounts (Cuentas), Account actions (Acciones de cuenta) y Delete account (Eliminar cuenta).
7. Confirme que desea eliminar la cuenta.

Amazon Chime elimina todos los datos de usuario al eliminar la cuenta. Esto incluye la cancelación de una AWS cuenta, de cuentas individuales de Amazon Chime o de usuarios de Amazon Chime no gestionados. Se excluyen los datos sin contenido relacionados con las cuentas de usuario y el uso de Amazon Chime (los atributos de servicio que se recogen en el Acuerdo de cliente) que genera Amazon Chime.

Administración de la configuración de la reunión

Administre la configuración de su reunión desde la consola Amazon Chime.

Configuración de la política de la reunión

Administre las políticas de la cuenta en la consola Amazon Chime en Configuración, Reuniones. Elija una de las siguientes opciones de política.

Habilitar el control compartido en el uso compartido de pantalla

Determine si los usuarios de su organización pueden conceder el control compartido de sus equipos durante las reuniones. Los asistentes que soliciten el control compartido de los equipos de sus usuarios recibirán un mensaje de error en el que se indica que el control remoto no está disponible.

Habilitar las llamadas salientes para unirse a reuniones

Activa la característica “Llámame” de Amazon Chime. Ofrece a los asistentes a la reunión la opción de unirse a las reuniones mediante una llamada telefónica desde Amazon Chime.

Configuración de la aplicación de reuniones

Administre el acceso a la aplicación de reuniones en Configuración, Reuniones en la consola Amazon Chime. Puede elegir la siguiente opción:

Permitir a los usuarios iniciar sesión en Amazon Chime mediante la aplicación Amazon Chime Meetings para Slack

Esta opción permite a los usuarios de su organización iniciar sesión en Amazon Chime desde la aplicación Amazon Chime Meetings para Slack. Para obtener más información, consulte [Configuración de la aplicación Amazon Chime Meetings para Slack](#).

Configuración de la región de la reunión

Para mejorar la calidad de las reuniones y reducir la latencia, Amazon Chime procesa las reuniones en la AWS región óptima para todos los participantes. Puede elegir si desea que Amazon Chime seleccione la región óptima para una reunión de todas las regiones disponibles o utilice solo las regiones que seleccione.

Puede actualizar esta configuración desde la configuración de Meetings (Reuniones) de su cuenta en cualquier momento. En la configuración de Reuniones también puede ver el porcentaje de reuniones de Amazon Chime que se están procesando en cada región.

Para actualizar la configuración de la región de la reunión

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En la página Accounts (Cuentas), seleccione el nombre de la cuenta.
3. En el panel de navegación, seleccione Settings (Configuración) y Meetings (Reuniones).
4. En Regions (Regiones), seleccione una de las siguientes opciones:
 - Utilizar todas las regiones disponibles para garantizar la calidad de las reuniones: permite a Amazon Chime optimizar el procesamiento de las reuniones.
 - Utilizar solo las regiones que he seleccionado: le permite seleccionar regiones en el menú desplegable.
5. Seleccione Guardar.

Administración de políticas de retención de chat

Si administra una o más cuentas corporativas de Amazon Chime, puede establecer políticas de retención de chats para lo siguiente:

- Las conversaciones de chat que solo incluyen miembros de la cuenta corporativa
- Las salas de chat creadas por los miembros de la cuenta corporativa

Una política de retención elimina automáticamente los mensajes en función del período de tiempo que establezca. Puede establecer períodos de tiempo comprendidos entre un día y 15 años.

Note

Las cuentas corporativas de Amazon Chime tienen un período de retención de 90 días. La política se aplica a las conversaciones en las que participan usuarios que pertenecen a la cuenta y a usuarios que no pertenecen a la cuenta.

Las políticas de retención no se aplican a lo siguiente:

- Las conversaciones de chat que no incluyen a ningún miembro de las cuentas corporativas de Amazon Chime
- Salas de chat creadas por usuarios que no pertenecen a una cuenta corporativa o de equipo de Amazon Chime

Cómo afectan las políticas de retención a los usuarios de Amazon Chime

Las políticas de retención que establecen los administradores de las cuentas corporativas afectan a los usuarios de Amazon Chime de manera diferente, en función de si los usuarios forman parte de la misma cuenta corporativa, de una cuenta corporativa diferente, de una cuenta de equipo o si no son miembros de ninguna cuenta.

Conversaciones de chat de miembros de cuentas corporativas

En la tabla siguiente, se muestra cómo afectan las políticas de retención a las conversaciones de chat de los miembros de cuentas corporativas.

Si la conversación de chat incluye...	La política de retención...
únicamente a otros miembros de la cuenta corporativa del usuario	la establece el administrador del usuario
a cualquier persona ajena a la cuenta corporativa del usuario	se establece automáticamente en 90 días

Salas de chat para miembros de cuentas corporativas

En la tabla siguiente, se muestra cómo afectan las políticas de retención a las salas de chat de los miembros de las cuentas corporativas.

Si la sala de chat es creada por...	La política de retención...
un miembro de la cuenta corporativa del usuario	la establece el administrador del usuario
un miembro de otra cuenta corporativa	la establece el administrador de la otra cuenta
un miembro de una cuenta que no es corporativa	No aplicable

Conversaciones de chat de miembros de cuentas de equipo

En la tabla siguiente se muestra cómo afectan las políticas de retención a las conversaciones de chat de los miembros de las cuentas de equipo.

Si la conversación de chat incluye...	La política de retención...
únicamente usuarios que no son miembros de una cuenta corporativa	No aplicable
al menos un miembro de una cuenta corporativa	se establece automáticamente en 90 días

Salas de chat para miembros de cuentas de equipo

En la tabla siguiente, se muestra cómo afectan las políticas de retención a las salas de chat de los miembros de las cuentas de equipo.

Si la sala de chat es creada por...	La política de retención...
un usuario de la cuenta de equipo	No aplicable
una persona que no es miembro de ninguna cuenta corporativa	No aplicable
un miembro de una cuenta corporativa	la establece el administrador de la cuenta corporativa

Los usuarios de Amazon Chime que no sean miembros de una cuenta corporativa o de equipo solo están sujetos a las políticas de retención de las salas de chat creadas por un miembro de una cuenta corporativa.

Conversaciones de chat con destinatarios que no pertenecen a una cuenta corporativa o de equipo

En la tabla siguiente, se muestra cómo afectan las políticas de retención a las conversaciones de chat de los usuarios que no sean miembros de una cuenta corporativa o de equipo de Amazon Chime.

Si la conversación de chat incluye...	La política de retención...
únicamente usuarios que no son miembros de una cuenta corporativa	No aplicable
al menos un miembro de una cuenta corporativa	se establece automáticamente en 90 días

Salas de chat creadas por usuarios que no pertenecen a una cuenta corporativa o de equipo

En la tabla siguiente, se muestra cómo afectan las políticas de retención a las salas de chat de los usuarios que no sean miembros de una cuenta corporativa o de equipo de Amazon Chime.

Si la sala de chat es creada por...	La política de retención...
un usuario que no es miembro de una cuenta corporativa o de equipo	No aplicable
un usuario de la cuenta de equipo	No aplicable
un miembro de una cuenta corporativa	la establece el administrador de la cuenta corporativa

Activación de la retención de chat

Los administradores de cuentas corporativas de Amazon Chime pueden usar la consola Amazon Chime para activar la retención de chat en conversaciones y salas de chat de la cuenta. También se

puede usar la consola para actualizar los períodos de retención de chat o desactivar la retención de chat en cualquier momento.

Para activar la retención de chat

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En la página Cuentas, seleccione el nombre de la cuenta.
3. En el panel de navegación, en Configuración, seleccione Retención.
4. En la página Retención, en Retención de conversaciones de chat, mueve el control deslizante a Activado.
5. En Período de retención, introduce un número en el primer cuadro, abre la lista situada junto al cuadro y selecciona Días, Semanas o Años.
6. En Retención de salas de chat, repite los pasos 4 y 5. Cuando termine, elija Guardar.

Al cabo de un día de establecer un período de retención, los usuarios de tu cuenta perderán el acceso a los mensajes enviados fuera del período de retención.

Restaurar los mensajes de chat

Note

Debe ser administrador de una cuenta de Amazon Chime Enterprise para completar estos pasos.

Puede restaurar los mensajes de chat en un plazo de 30 días a partir de haber establecido un período de retención del chat. Al restaurar los mensajes de chat, restaura todos los mensajes enviados por todos los usuarios de su cuenta de Amazon Chime.

Dentro de ese período de 30 días, puede realizar una de las siguientes acciones para restaurar los mensajes:

- Utilice la consola Amazon Chime para desactivar la retención de datos.
- -O BIEN-
- Prolongue el período de retención.

Tras el período de gracia de 30 días, todos los mensajes de chat que estén dentro del período de retención se eliminarán permanentemente. Los mensajes de chat nuevos se eliminan permanentemente en cuanto pasan el período de retención.

Para obtener información sobre cómo configurar o cambiar un período de retención [Activación de la retención de chat](#), consulte la sección anterior.

Los mensajes de chat también se eliminan permanentemente de Amazon Chime cuando usted o un miembro de la cuenta realizan alguna de las siguientes acciones:

- Eliminar una sala de chat de Amazon Chime. Para obtener más información sobre la eliminación de salas de chat, consulte [Eliminar salas de chat](#) en la Guía del usuario de Amazon Chime.
- Finalice una reunión de Amazon Chime en la que haya mensajes de chat.

Note

Si es necesario, puede copiar y guardar manualmente los mensajes de chat de una reunión, pero debe hacerlo antes de que finalice la reunión. Para obtener más información, consulte [Uso del chat durante la reunión](#) en la Guía del usuario de Amazon Chime.

Eliminar mensajes de chat

Para cumplir con las políticas de retención de datos, Amazon Chime conserva todos los mensajes de chat e impide que los usuarios finales eliminen los mensajes que envían. Sin embargo, los administradores del sistema Amazon Chime pueden usar un par de API para eliminar mensajes individuales de las conversaciones y las salas de chat. Los mensajes deben residir en la cuenta Amazon Chime del administrador.

Los usuarios pueden solicitar la eliminación de los mensajes enviándole un identificador de mensaje y el correspondiente identificador de conversación o sala de chat. En el tema [Uso de las funciones de chat](#) de la Guía del usuario de Amazon Chime, se explica cómo hacerlo.

Cuando recibas una solicitud de eliminación, puedes escribir código o usar la AWS CLI para invocar las siguientes API.

Para quitar un mensaje

- Realice una de las acciones siguientes:

- Para los mensajes de conversación: usa la [RedactConversationMessage](#) API.

En la CLI, ejecute el siguiente comando:

```
aws chime redact-conversation-message --conversation-id id_string --message-id id_string
```

- Para los mensajes de la sala de chat: utilice la [RedactRoomMessage](#) API.

En la CLI, ejecute el siguiente comando:

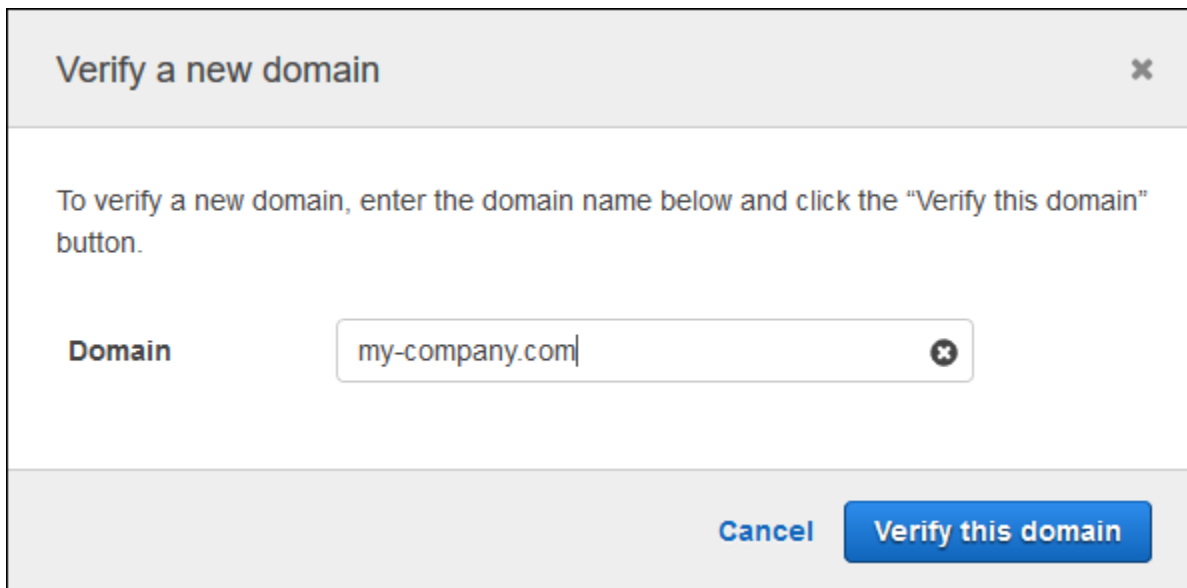
```
aws chime redact-room-message --room-id id_string --message-id id_string
```

Solicitar un dominio

Para crear una cuenta corporativa y beneficiarse del mayor control que esta ofrece sobre su cuenta y sus usuarios, debe reclamar al menos un dominio de correo electrónico.

Para reclamar un dominio

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En la página Cuentas, seleccione el nombre de la cuenta de equipo.
3. En el panel de navegación, seleccione Identity (Identidad), Domains (Dominios).
4. En la página Domains (Dominios), elija Claim a new domain (Reclamar un dominio nuevo).
5. En Domain (Dominio), escriba el nombre del dominio que utiliza su organización para las direcciones de correo electrónico. Elija Verify this domain (Verificar este dominio).



Verify a new domain ✕

To verify a new domain, enter the domain name below and click the "Verify this domain" button.

Domain ✕

Cancel **Verify this domain**

6. Siga las instrucciones de la pantalla para añadir un registro TXT al servidor DNS de su dominio. En general, el proceso implica el inicio de sesión en la cuenta del dominio, la búsqueda de los registros DNS del dominio y la adición de un registro TXT con el nombre y el valor proporcionados por Amazon Chime. Para obtener más información sobre la actualización de los registros DNS del dominio, consulte la documentación de su proveedor de DNS o registrador de nombres de dominio.

Amazon Chime comprueba la existencia de este registro para verificar que usted es el propietario del dominio. Una vez que se ha verificado el dominio, su estado cambia de Pending verification (Verificación pendiente) a Verified (Verificado).

Note

La propagación del cambio de DNS y la verificación por parte de Amazon Chime pueden tardar hasta 24 horas.

7. Si su organización utiliza dominios o subdominios adicionales para las direcciones de correo electrónico, repita este procedimiento para cada dominio.

Para obtener más información sobre cómo solucionar problemas de notificaciones del dominio, consulte la pregunta [¿Por qué no se verifica mi solicitud de notificación del dominio?](#)

Conectarse a Active Directory

Al conectar su cuenta administrativa de Amazon Chime a una instancia de Active Directory, puede beneficiarse de las siguientes funciones:

- Los usuarios de Amazon Chime pueden iniciar sesión con sus credenciales de Active Directory.
- Como administrador de Amazon Chime puede elegir qué características de seguridad de credenciales desean añadir, incluidas la rotación de contraseñas, las reglas de complejidad de las contraseñas y la autenticación multifactor.
- Al eliminar cuentas de usuario de Active Directory, también se eliminan sus cuentas de Amazon Chime.
- Puede especificar qué grupos de Active Directory reciben permisos Pro de Amazon Chime Pro.
 - Se pueden configurar varios grupos para recibir permisos básicos o Pro.
 - Los usuarios deben ser miembros de uno de los grupos para iniciar sesión en Amazon Chime.
 - Los usuarios de ambos grupos reciben una licencia Pro.

Para obtener más información acerca de la administración de permisos de usuario, consulte [Administración del acceso y los permisos de los usuarios](#).

Requisitos previos

Para poder conectarse a Active Directory en Amazon Chime, debe cumplir los siguientes requisitos previos:

- Asegúrese de tener los AWS Identity and Access Management permisos correctos para configurar los dominios, los directorios activos y los grupos de directorios. Para obtener más información, consulte [Administración de identidades y accesos para Amazon Chime](#).
- Cree un directorio AWS Directory Service que esté configurado en la región EE.UU. Este (Norte de Virginia). Para obtener más información, consulte la [Guía de administración de AWS Directory Service](#). Amazon Chime se puede conectar mediante AD Connector, Microsoft AD o Simple AD.
- Reclame un dominio para crear una cuenta corporativa de Amazon Chime o convierta su cuenta de equipo existente en una cuenta corporativa. Si sus usuarios tienen direcciones de correo electrónico de trabajo de más de un dominio, asegúrese de reclamarlos todos. Para más información, consulte [Solicitar un dominio](#) y [Para convertir una cuenta de equipo en una cuenta corporativa](#).

Conexión a Active Directory en Amazon Chime

Después de conectar su instancia de Active Directory a Amazon Chime, se les pedirá a sus usuarios que inicien sesión con sus credenciales de directorio cuando usen una dirección de correo electrónico de uno de los dominios que haya solicitado en su cuenta corporativa de Amazon Chime.

Para conectarse a Active Directory en Amazon Chime

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En el panel de navegación, elija Identidad, Active Directory.
3. En Cloud Directory ID, selecciona el AWS Directory Service directorio que quieres usar para Amazon Chime y, a continuación, selecciona Connect.

Note

Para encontrar el ID del directorio, utilice la [consola de AWS Directory Service](#).

4. Una vez que se haya conectado el directorio, elija Agregar un grupo nuevo.
5. En Grupo, escriba el nombre de grupo. El nombre debe coincidir exactamente con un grupo de Active Directory del directorio de destino. No se admiten las unidades organizativas (OU) de Active Directory.
6. En Permisos, elija Basic o Pro.
7. Elija Añadir grupo.
8. (Opcional) Repita este procedimiento para crear grupos de directorios adicionales.

Configuración de varias direcciones de correo electrónico

Tras conectarse a su instancia de Active Directory en Amazon Chime, los usuarios pueden iniciar sesión en Amazon Chime con sus credenciales de Active Directory. Sus usuarios pueden tener asignadas varias direcciones de correo electrónico en su instancia de Active Directory. Para permitir que sus usuarios inicien sesión en Amazon Chime con sus credenciales de Active Directory, debe reclamar cada dominio de correo electrónico aplicable en su cuenta administrativa de Amazon Chime. Para obtener más información, consulte [Solicitar un dominio](#).

Note

Si sus usuarios intentan iniciar sesión con una dirección de correo electrónico de un dominio no reclamado, se les pedirá que inicien con Iniciar sesión con Amazon. No pueden iniciar sesión en su cuenta administrativa si utilizan una dirección de correo electrónico de un dominio no reclamado.

Al ver los detalles del usuario en la consola Amazon Chime, Amazon Chime utiliza la única dirección de correo electrónico del atributo `EmailAddress` de su instancia de Active Directory como dirección de correo electrónico principal de cada usuario. Esta es la única dirección de correo electrónico del usuario que puede ver en la consola Amazon Chime. Sin embargo, los usuarios pueden iniciar sesión con cualquier dirección adicional que aparezca en el atributo `ProxyAddress`, siempre y cuando solicite esos dominios en su cuenta de Amazon Chime.

Ejemplo de configuración incorrecta

Una usuaria cuyo nombre de usuario es `shirley.rodriguez` es miembro de una cuenta de Amazon Chime que ha reclamado dos dominios: `example.com` y `example.org`. En Active Directory, esta usuaria tiene las tres direcciones de correo electrónico siguientes:

- Dirección de correo electrónico principal: `shirley.rodriguez@example.com`
- Dirección de correo electrónico proxy 1: `shirley.rodriguez@example2.com`
- Dirección de correo electrónico proxy 2: `srodriguez@example.org`

Esta usuaria puede iniciar sesión en Amazon Chime utilizando `shirley.rodriguez@example.com` o `srodriguez@example.org` y `shirley.rodriguez`. Si intenta iniciar sesión con `shirley.rodriguez@example2.com`, se le pedirá Iniciar sesión con Amazon y no formará parte de la cuenta administrada. Por esta razón, es importante reclamar todos los dominios que utilicen los usuarios para el correo electrónico.

Los demás usuarios de Amazon Chime pueden añadirla como contacto, invitarla a reuniones o añadirla como delegado utilizando las direcciones de correo electrónico `shirley.rodriguez@example.com` o `srodriguez@example.org`.

Ejemplo de configuración correcta

Una usuaria cuyo nombre de usuario es shirley.rodriguez es miembro de una cuenta de Amazon Chime que ha reclamado tres dominios: example.com, example2.com y example.org. En Active Directory, esta usuaria tiene las tres direcciones de correo electrónico siguientes:

- Dirección de correo electrónico principal: shirley.rodriguez@example.com
- Dirección de correo electrónico proxy 1: shirley.rodriguez@example2.com
- Dirección de correo electrónico proxy 2: srodriguez@example.org

Esta usuaria puede iniciar sesión en Amazon Chime utilizando cualquiera de sus direcciones de correo electrónico de trabajo. Los demás usuarios también pueden añadirla como contacto, invitarla a reuniones o añadirla como delegado utilizando cualquiera de sus direcciones de correo electrónico de trabajo.

Conexión con Okta SSO

Si tiene una cuenta corporativa, puede conectarse a Okta SSO para autenticarse y asignar permisos de usuario.

Note


Si necesita crear una cuenta corporativa, lo que le permitirá administrar todos los usuarios de un determinado conjunto de dominios de correo electrónico, consulte [Solicitar un dominio](#).

La conexión de Amazon Chime a Okta requiere configurar dos aplicaciones en la consola de administración de Okta. La primera aplicación se configura manualmente y utiliza OpenID Connect para autenticar a los usuarios en el servicio de Amazon Chime. La segunda aplicación está disponible como Amazon Chime SCIM Provisioning en la Okta Integration Network (OIN). Está configurada para insertar las actualizaciones en Amazon Chime sobre los cambios realizados en los usuarios y grupos.

Para conectar con Okta SSO


1. Cree la aplicación de Amazon Chime (OpenID Connect) en la Consola de administración de Okta:

1. Inicie sesión en el panel de administración de Okta y, a continuación, seleccione Add Application (Añadir aplicación). En el cuadro de diálogo Create New Application (Crear nueva aplicación), elija Web, Next (Siguiente).
2. Configure las opciones de Application Settings (Configuración de aplicación):
 - a. Asigne un nombre a la aplicación **Amazon Chime**.
 - b. En Login Redirect URI (URI de redireccionamiento de inicio de sesión), escriba el siguiente valor: **https://signin.id.ue1.app.chime.aws/auth/okta/callback**
 - c. En la sección Allowed Grant Types (Tipos de concesión permitidos), seleccione todas las opciones para habilitarlos.
 - d. En el menú desplegable Login initiated by (Inicio de sesión iniciado por), elija Either (Okta or App) (Cualquiera, Okta o la aplicación) y seleccione todas las opciones relacionadas.
 - e. En Initiate Login URI (Iniciar URI de inicio de sesión), escriba el siguiente valor: **https://signin.id.ue1.app.chime.aws/auth/okta**
 - f. Seleccione Guardar.
 - g. Mantenga esta página abierta, ya que necesitará la información de Client ID (ID de cliente), Client secret (Secreto de cliente) e Issuer URI (URI de emisor) para el paso 2.
2. En la consola Amazon Chime, siga estos pasos:
 1. En la página Okta single-sign on configuration (Configuración del inicio de sesión único de Okta), en la parte superior de la página, elija Set up incoming keys (Configurar las claves entrantes).
 2. En el cuadro de diálogo Setup incoming Okta keys (Configurar las claves entrantes de Okta):
 - a. Pegue la información de Client ID (ID de cliente) y Client secret (Secreto de cliente) de la página Okta Application Settings (Configuración de la aplicación de Okta).
 - b. Pegue los datos apropiados de Issuer URI (URI de emisor) de la página Okta API (API de Okta). El URI del emisor debe ser un dominio de Okta, como **https://example.okta.com**.
3. Configure la aplicación Amazon Chime SCIM Provisioning en la Consola de administración de Okta para intercambiar la información de identidad y de pertenencia a un grupo con Amazon Chime:
 1. En la Consola de administración de Okta, elija Aplicaciones, Añadir aplicación, busque Amazon Chime SCIM Provisioning y añada la aplicación.

 Important

Durante la configuración inicial, elija Do not display application to users (No mostrar la aplicación a los usuarios) y Do not display application icon in the Okta Mobile App (No mostrar el icono de aplicación en la aplicación móvil de Okta); a continuación, elija Done (Listo).

2. En la pestaña Provisioning (Aprovisionamiento), elija Configure API Integration (Configurar la integración de la API) y seleccione Enable API Integration (Habilitar la integración de la API). Mantenga esta página abierta, ya que tendrá que copiar una clave de acceso a la API para ella para el siguiente paso.
3. En la consola Amazon Chime, elija Crear clave de acceso para crear una clave de acceso a la API. Cópiala en el campo Okta API Token (Token de la API de Okta) en el cuadro de diálogo Configure API Integration (Configurar la integración de la API), elija Test the Integration (Probar la integración) y, a continuación, elija Save (Guardar).
4. Configure las acciones y los atributos que Okta usará para actualizar Amazon Chime. En la pestaña Provisioning (Aprovisionamiento), en la sección To App (A la aplicación), elija Edit (Editar), elija en Enable Users (Habilitar usuarios), Update User Attributes (Actualizar atributos de usuario) y Deactivate Users (Desactivar usuarios), y elija Save (Guardar).
5. En la pestaña Assignments (Asignaciones), conceda a los usuarios permisos para la nueva aplicación SCIM.

 Important

Recomendamos conceder permisos a través de un grupo que contenga todos los usuarios que deben tener a Amazon Chime, independientemente de la licencia. El grupo debe ser el mismo que el utilizado para asignar la aplicación OIDC orientada al usuario en el paso 1 anterior. De lo contrario, los usuarios finales no podrán iniciar la sesión.

6. En la pestaña Grupos de inserción, configure qué grupos y miembros se sincronizan con Amazon Chime. Estos grupos se utilizan para diferenciar entre usuarios Basic y Pro.
4. Configurar grupos de directorio en Amazon Chime:
 1. En la consola Amazon Chime, vaya a la página Configuración de inicio de sesión único de Okta.

2. En Directory groups (Grupos de directorios), elija Add new groups (Añadir nuevos grupos).
3. Ingrese el nombre de un grupo de directorio para agregarlo a Amazon Chime. El nombre debe ser una coincidencia exacta de uno de los grupos de inserción configurado anteriormente en el paso 3-f.
4. Elija si los usuarios de este grupo deben recibir capacidades del nivel Basic o Pro y elija Save (Guardar). Repita este proceso para configurar grupos adicionales.

Note

Si recibe un mensaje de error que indica que no se encuentra el grupo, es posible que los dos sistemas no hayan completado la sincronización. Espere unos minutos y vuelva a elegir Add new groups (Añadir nuevos grupos).

Si elige funcionalidades del nivel Basic o Pro para los usuarios del grupo de directorios, la licencia, las funcionalidades y el costo de esos usuarios se verán afectados en su cuenta corporativa de Amazon Chime. Para obtener más información, consulte [Precios](#).

Implementación del complemento de Amazon Chime para Outlook

Amazon Chime proporciona dos complementos para Microsoft Outlook: el complemento de Amazon Chime para Outlook en Windows y el complemento de Amazon Chime para Outlook. Estos complementos ofrecen las mismas características de programación, pero admiten diferentes tipos de usuarios. Los suscriptores y las organizaciones de Microsoft Office 365 que utilizan una instalación local de Microsoft Exchange 2013 o posterior pueden utilizar el complemento de Amazon Chime para Outlook. Los usuarios de Windows con un servidor Exchange instalado localmente que ejecute Exchange Server 2010 o versiones anteriores y los usuarios de Outlook 2010 deben utilizar el complemento de Amazon Chime para Outlook en Windows.

Los usuarios de Windows que no tienen permisos para instalar el complemento de Amazon Chime para Outlook deberían elegir el complemento de Amazon Chime para Outlook en Windows.

Para obtener información sobre qué complemento es el adecuado para usted y su organización, consulte [Selección del complemento de Outlook correcto](#).

Si elige el complemento de Amazon Chime para Outlook para su organización, puede implementarlo en los equipos de los usuarios con una implementación centralizada. Para obtener más

información, consulte la [Guía de instalación del complemento de Amazon Chime para Outlook para administradores](#).

Configuración de la aplicación Amazon Chime Meetings para Slack

Si utiliza [Enterprise Grid Organizations de Slack](#) y eres propietario o administrador de una organización de Slack, puede configurar la aplicación Amazon Chime Meetings para Slack para sus organizaciones. Si es administrador del espacio de trabajo de Slack, puede configurar la aplicación Amazon Chime Meetings para sus espacios de trabajo.

Los pasos de las siguientes secciones explican cómo realizar ambos tipos de configuraciones y cómo completar tareas adicionales, como la migración de un espacio de trabajo a una organización.

Temas

- [Instalación de la aplicación Amazon Chime Meetings para Slack en una organización](#)
- [Instalación de la aplicación Amazon Chime Meetings para Slack en los espacios de trabajo](#)
- [Migración de espacios de trabajo a organizaciones](#)
- [Asociación de espacios de trabajo con cuentas de equipo de Amazon Chime](#)

Instalación de la aplicación Amazon Chime Meetings para Slack en una organización

La instalación de la aplicación Amazon Chime Meetings para Slack en una organización de Slack permite a los usuarios iniciar reuniones y llamadas instantáneas con otros usuarios en los distintos espacios de trabajo de esa organización. También permite a los administradores del espacio de trabajo instalar automáticamente la aplicación Amazon Chime Meetings para reuniones de Slack en cualquier espacio de trabajo nuevo. En los siguientes pasos se explica cómo hacerlo.

Note

En los siguientes pasos se supone que es propietario o administrador de una organización y que puede iniciar sesión en la consola de administración de Slack.

Para configurar la aplicación Amazon Chime Meetings para Slack en una organización

1. En el panel izquierdo de la consola de administración de Slack, seleccione Aplicaciones.

Aparece la página Aplicaciones, donde se muestran las aplicaciones que haya instaladas en la organización.

2. Elija Administrar aplicaciones, en la esquina superior derecha de la página, y, a continuación, elija Instalar una aplicación.

Aparece el cuadro de diálogo Buscar una aplicación para instalar.

3. Busque en **Amazon Chime Meetings** y, a continuación, selecciónela en los resultados de la búsqueda.

Aparece el cuadro de diálogo Añadir Amazon Chime Meetings a los espacios de trabajo, en el que se muestran los espacios de trabajo de la organización.

4. Elija el espacio de trabajo o los espacios de trabajo en los que quiera instalar la aplicación Amazon Chime Meetings para Slack.
5. Si lo desea, seleccione Predeterminado para el espacio de trabajo futuro si quiere instalar automáticamente la aplicación Amazon Chime Meetings para Slack en todos los espacios de trabajo nuevos y, a continuación, seleccione Siguiente.

Aparece el cuadro de diálogo Revisar los permisos solicitados de esta aplicación y muestra los permisos y las acciones de la aplicación Amazon Chime Meetings para Slack.

6. Elija Siguiente.
7. Si ha decidido instalar la aplicación Amazon Chime Meetings para Slack en los nuevos espacios de trabajo de forma predeterminada, seleccione Estoy listo para configurar esta aplicación como predeterminada para los espacios de trabajo futuros y, a continuación, seleccione Guardar. De lo contrario, seleccione Guardar.

Note

También puede usar OAuth para instalar aplicaciones en sus organizaciones. Para obtener más información, consulte [Instalación con OAuth](#) en la ayuda de Slack.

Instalación de la aplicación Amazon Chime Meetings para Slack en los espacios de trabajo

La instalación de la aplicación Amazon Chime Meetings para Slack en un espacio de trabajo permite a los usuarios iniciar reuniones y llamadas instantáneas con otros usuarios de ese espacio de trabajo. Los usuarios no necesitan un perfil de usuario de Amazon Chime para usar la aplicación Amazon Chime Meetings para Slack. Pueden iniciar sesión con sus perfiles de usuario de Slack e iniciar llamadas o reuniones en cualquier momento. Si los usuarios necesitan celebrar reuniones con más de una persona, debe configurar una cuenta de equipo de Amazon Chime y conceder a esos usuarios permisos Pro adicionales. Para obtener más información sobre cómo iniciar llamadas y reuniones con Amazon Chime, consulte [Uso de la aplicación Amazon Chime Meetings para Slack](#) en la Guía del usuario de Amazon Chime. Para obtener más información sobre cómo configurar una cuenta de equipo de Amazon Chime, consulte [Asociación de espacios de trabajo con cuentas de equipo de Amazon Chime](#) en esta guía.

Para instalar la aplicación Amazon Chime Meetings para Slack para los espacios de trabajo de Slack

1. Vaya al directorio de aplicaciones de Slack y busque la aplicación Amazon Chime Meetings.
2. Seleccione [Añadir a Slack](#) para instalar la aplicación Amazon Chime Meetings para Slack desde el directorio de aplicaciones de Slack.
3. Establezca la configuración de Llamadas del espacio de trabajo de Slack para Habilitar las llamadas en Slack mediante Amazon Chime.

Migración de espacios de trabajo a organizaciones

Si es propietario de una organización de Slack, puede migrar los espacios de trabajo a esa organización. Para obtener más información sobre la migración de espacios de trabajo, consulte [Cómo migrar espacios de trabajo a Enterprise Grid](#) en la ayuda de Slack.

Asociación de espacios de trabajo con cuentas de equipo de Amazon Chime

Asocie su espacio de trabajo con una cuenta de equipo de Amazon Chime para administrar los permisos de sus usuarios. Puede promocionar a los organizadores de las reuniones a la categoría Pro de Amazon Chime para que puedan iniciar reuniones con hasta 250 asistentes y 25 mosaicos de vídeo, e incluir números de teléfono a los que pueden marcar para el audio. Asigne a los usuarios

permisos de Amazon Chime Basic para que puedan iniciar one-on-one reuniones o unirse a las reuniones de Amazon Chime. Para obtener más información, consulte [Precios de Amazon Chime](#).

 Note

Si asocia una cuenta de equipo de Amazon Chime a su espacio de trabajo de Slack, los usuarios pueden iniciar sesión en Amazon Chime desde la aplicación Amazon Chime Meetings para Slack. Puede cambiar esta configuración en cualquier momento. Para obtener más información, consulte [Administración de la configuración de la reunión](#).

Para poder asociar tu espacio de trabajo de Slack a una cuenta de equipo de Amazon Chime, debes crear una AWS cuenta. Para obtener más información sobre cómo crear una AWS cuenta, consulta [Requisitos previos para los administradores del sistema Amazon Chime](#)

Para asociar su espacio de trabajo de Slack a una cuenta de equipo de Amazon Chime al instalar la aplicación Amazon Chime Meetings para Slack

1. Inmediatamente después de instalar Amazon Chime en su espacio de trabajo de Slack, seleccione Actualizar ahora.
2. Siga las instrucciones para iniciar sesión en la consola de Amazon Chime con las credenciales de AWS su cuenta.
3. Siga las instrucciones para crear una nueva cuenta de equipo en Amazon Chime o elegir una existente.
 - Crear una cuenta nueva: cree una cuenta nueva de Amazon Chime para invitar a sus usuarios de Slack. Introduzca un nombre de cuenta, decida si desea invitar a sus usuarios de Slack y, a continuación, seleccione Create (Crear).
 - Elegir una cuenta existente: seleccione una cuenta de Amazon Chime existente para invitar a sus usuarios de Slack. Seleccione la cuenta y, a continuación, seleccione Invite (Invitar).

Cuando invita a los usuarios de Slack a unirse a Amazon Chime, reciben una invitación por correo electrónico. Cuando aceptan la invitación, se actualizan automáticamente a Amazon Chime Pro.

Si no asoció su espacio de trabajo de Slack con una cuenta de equipo de Amazon Chime cuando instaló la aplicación Amazon Chime Meetings para Slack, puede hacerlo después siguiendo los pasos siguientes.

Para asociar su espacio de trabajo de Slack a una cuenta de equipo de Amazon Chime después de instalar la aplicación Amazon Chime Meetings para Slack

1. Inicie sesión en su cuenta. AWS
2. Inicie sesión en su espacio de trabajo de Slack como administrador.
3. Visite https://signin.id.ue1.app.chime.aws/auth/slack?purpose=app_authz.
4. Siga las instrucciones para crear una nueva cuenta de equipo en Amazon Chime o elegir una existente.
 - Crear una cuenta nueva: cree una cuenta nueva de Amazon Chime para invitar a sus usuarios de Slack. Introduzca un nombre de cuenta, decida si desea invitar a sus usuarios de Slack y, a continuación, seleccione Create (Crear).
 - Elegir una cuenta existente: seleccione una cuenta de Amazon Chime existente para invitar a sus usuarios de Slack. Seleccione la cuenta y, a continuación, seleccione Invite (Invitar).

Administración de usuarios

La consola Amazon Chime se utiliza para añadir y gestionar usuarios. Para añadir usuarios, debe invitarlos. A medida que acepten sus invitaciones, aparecerán en Usuarios, donde se muestran todos los usuarios de su cuenta y sus detalles de usuario. Para obtener más información, consulte [Ver los datos de los usuarios](#).

Los administradores de las cuentas que utilizan Login with Amazon (LWA) también pueden ver opciones para administrar niveles de permisos y eliminar usuarios de una cuenta. Estas acciones se administran a través de Active Directory u Okta, en función de en cuál de ellas configure una cuenta para usar. Para obtener más información, consulte [Administración del acceso y los permisos de los usuarios](#).

Contenido

- [Añadir usuarios](#)
- [Ver los datos de los usuarios](#)
- [Administración del acceso y los permisos de los usuarios](#)
- [Cambio del PIN personal de las reuniones](#)
- [Administración de versiones de prueba Pro](#)
- [Solicitar archivos adjuntos de los usuarios](#)
- [Cómo gestiona Amazon Chime las actualizaciones automáticas](#)
- [Migración de usuarios a otra cuenta de equipo](#)

Añadir usuarios

Para añadir usuarios a una cuenta de Amazon Chime, debe invitarlos a unirse a la cuenta. Puede enviar invitaciones a usuarios potenciales desde la consola Amazon Chime, y en estos pasos se explica cómo hacerlo.

1. En la página de inicio de la consola, en el panel izquierdo, elija Cuentas.

Aparece una lista de las cuentas que administra.

2. Elija la cuenta a la que desee añadir miembros y elija Invitar a usuarios.

Aparece el cuadro de diálogo Invitar a nuevos usuarios.

3. Escriba la dirección de correo electrónico de los usuarios a los que desee invitar. Separe cada dirección con un punto y coma (;).
4. Elija Invite users.

Los nuevos usuarios aparecen en la lista. Cuando invita a usuarios a una cuenta de equipo, no aparecerán sus detalles hasta que acepten su invitación.

Ver los datos de los usuarios

En la consola Amazon Chime, en Usuarios, puede ver una lista de todos los usuarios de su cuenta y consultar sus detalles. Busque un usuario específico por su dirección de correo electrónico y elija el nombre para ver los detalles del usuario. En Datos del usuario, puede ver información detallada sobre el usuario y actualizar la cuenta.

En la siguiente tabla se muestra una lista de los detalles de usuario que aparecen en la consola.

Note

Los detalles completos de los usuarios de las cuentas de equipo no aparecen hasta que hayan aceptado sus invitaciones.

Campo	Descripción	Ejemplo
Display name (Nombre de visualización)	El nombre del usuario que aparece en Amazon Chime. Para los usuarios de Login with Amazon (LWA), este es el nombre completo. Para los usuarios de Active Directory , se utiliza DISPLAY_NAME_ATTRIBUTE.	Major, Mary
Dirección de correo electrónico	Para los usuarios de LWA, la dirección de correo electrónico que se utilizó para su registro. Para los usuarios de Active	mary.major@example.com

Campo	Descripción	Ejemplo
	Directory, aparece la dirección de correo electrónico principal de Active Directory.	
Registration (Registro)	El estado de registro actual del usuario. Los valores posibles son distintos entre las cuentas corporativas, en las que no se envían invitaciones, y las cuentas de equipo, en las que sí se envían.	Registrado, Sin registrar (en una cuenta de equipo) o Suspendido (en una cuenta corporativa)
Permission tier (Nivel de permisos)	De forma predeterminada, se establece en Pro, lo que permite a los usuarios organizar reuniones. Puede cambiarse a Basic (Básico).	Pro, Basic (Básico)
Invited (Invitado)	En las cuentas de equipo, fecha en la que se invitó al usuario a la cuenta.	01/05/2020
Joined (Se unió)	La fecha en que el usuario inició sesión por primera vez en Amazon Chime. Para los usuarios de prueba Pro, esta es también la fecha en que comenzó dicha prueba.	01/10/2020
Personal PIN (PIN personal)	El número PIN personal para reuniones que el usuario puede utilizar para programar reuniones.	0123456789
Privacy setting (Configuración de privacidad)	La configuración de presencia seleccionada por el usuario.	Public (Público) o Private (Privado)

Campo	Descripción	Ejemplo
Meetings attended (Reuniones a las que se ha asistido)	El número de reuniones a las que ha asistido un usuario.	87
Meetings organized (Reuniones organizadas)	El número de reuniones que ha organizado un usuario.	12
Meeting satisfaction (Satisfacción de los participantes)	El porcentaje de respuestas positivas dadas a la end-of-meeting encuesta.	92%
Last active date (Fecha de la última actividad)	La fecha en la que el usuario estuvo activo por última vez.	12/06/2020
Chat messages sent (Mensajes de chat enviados)	El número de mensajes de chat enviados por el usuario.	1025
Número de teléfono	El número de teléfono asignado a un usuario, si hay alguno.	+12065550100

Administración del acceso y los permisos de los usuarios

Gestione las características a las que pueden acceder sus usuarios de Amazon Chime asignándoles permisos Pro o Basic. Los usuarios Basic no pueden organizar reuniones, pero pueden asistir a ellas y utilizar el chat. Para obtener más información acerca de las características a las que tienen acceso los usuarios con permisos Pro y Basic, consulte [Planes y precios](#).

Administre quién puede iniciar sesión en su cuenta administrativa de Amazon Chime invitando o suspendiendo a los usuarios. Solo los administradores corporativos pueden suspender a los usuarios. Los administradores de las cuentas de equipo pueden eliminar a usuarios de sus cuentas para dejar de pagar por sus permisos. Sin embargo, no pueden suspender al usuario para evitar que inicie sesión. Para obtener más información sobre las diferencias entre las cuentas de equipo y corporativas, consulte [Administración de las cuentas de Amazon Chime](#).

Administración de permisos de usuario

Como administrador de Amazon Chime, puede administrar los permisos Pro y Basic para los usuarios de su cuenta de Amazon Chime.

Si Active Directory u Okta están configurados para la cuenta de Amazon Chime, administre los permisos de usuario a través de la pertenencia a grupos de directorio. Si Active Directory y Okta no están configurados, administre los permisos de usuario desde la consola Amazon Chime.

Cuentas de equipo y cuentas corporativas de Login with Amazon

Si administra una cuenta de equipo de Amazon Chime o una cuenta corporativa de LWA, en la que los usuarios inician sesión con sus cuentas Login with Amazon (LWA), puede administrar los permisos Pro y Basic en la consola Amazon Chime.

Para administrar los permisos de usuario en las cuentas de equipo y las cuentas corporativas de LWA

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En Cuentas, elija el nombre de la cuenta de Amazon Chime.
3. Seleccione Usuarios.
4. Seleccione los usuarios, y elija Acciones y Asignar permisos.
5. Elija uno de los permisos siguientes:
 - Pro
 - Básica
6. Elija Assign (Asignar).

Cuentas empresariales de Active Directory o de OpenID Connect (Okta)

Si los usuarios inician sesión con credenciales de Active Directory u Okta, administre sus permisos haciéndolos miembros de un grupo de directorios que tenga asignados permisos Pro o Basic.

Para asignar permisos Pro a un usuario, conviértalo en miembro de un grupo de Active Directory u Okta al que haya asignado permisos Pro. Para asignar permisos Basic a un usuario, conviértalo en miembro de un grupo al que haya asignado permisos Basic. Los usuarios que no tengan permisos Pro o Basic no pueden iniciar sesión en Amazon Chime.

Administración del acceso de los usuarios

Si administra una cuenta de Amazon Chime, puede invitar a los usuarios para permitir que inicien sesión en su cuenta. Los administradores de cuentas corporativas pueden suspender el acceso de los usuarios para evitar que inicien sesión en la cuenta.

Invitación y eliminación de usuarios de la cuenta de equipo

Si administra una cuenta de equipo, puede utilizar la consola Amazon Chime; para invitar a los usuarios de cualquier dominio de correo electrónico.

Note

La versión de prueba Pro gratuita de 30 días del usuario finaliza cuando acepta la invitación.

Para invitar a los usuarios a una cuenta de equipo

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En Cuentas, elija el nombre de la cuenta de equipo.
3. Seleccione Usuarios e Invitar a usuarios.
4. Introduzca las direcciones de correo electrónico de los usuarios a los que desea invitar y sepárelas mediante signos de punto y coma (;).
5. Elija Invite users.

El siguiente procedimiento desvincula a los usuarios de su cuenta de equipo eliminando cualquier permiso Pro o Basic que se les haya asignado. Los usuarios eliminados pueden seguir iniciando sesión en Amazon Chime, pero ya no son miembros de pago de su cuenta de Amazon Chime.

Para eliminar usuarios de una cuenta de equipo

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En Cuentas, elija el nombre de la cuenta de equipo.
3. Seleccione Usuarios.
4. Seleccione a los usuarios y elija Acciones del usuario y Quitar usuario.

Se eliminan todos los permisos Pro o Basic asignados a los usuarios. Los usuarios ya no podrán utilizar la función de autocompletar para encontrar a nuevos miembros del equipo entre sus Contactos.

Invitación y suspensión de los usuarios de cuentas corporativas

Si administra una cuenta corporativa, cualquier usuario que se registre en Amazon Chime con una dirección de correo electrónico perteneciente a uno de los dominios solicitados se agregará automáticamente a la cuenta. Si ha configurado Active Directory u Okta, los usuarios también deben ser miembros del grupo de directorios que haya configurado para Amazon Chime.

Para invitar a usuarios a una cuenta corporativa

- Envíe un correo electrónico de invitación a los usuarios de su organización con instrucciones para que sigan los pasos que se indican en [Creación de una cuenta de Amazon Chime](#) en la Guía del usuario de Amazon Chime.

Los usuarios inician sesión con una dirección de correo electrónico de uno de los dominios que ha solicitado para la cuenta. Una vez que hayan realizado los pasos necesarios para crear sus cuentas de Amazon Chime, aparecerán automáticamente en Usuarios en la cuenta corporativa de la consola Amazon Chime.

El siguiente procedimiento suspende a los usuarios de una cuenta corporativa que no tenga Active Directory u Okta configurados. Esto impide que los usuarios inicien sesión en Amazon Chime.

Para suspender a los usuarios de una cuenta corporativa

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En Cuentas, elija el nombre de la cuenta corporativa.
3. Seleccione Usuarios.
4. Seleccione los usuarios que desea suspender y elija Acciones, Suspender usuario.
5. Active la casilla y elija Suspender.

Si ha configurado Active Directory u Okta para su cuenta corporativa, utilice el siguiente procedimiento para suspender a usuarios.

Para suspender a los usuarios de una cuenta corporativa de Active Directory u OpenID Connect (Okta)

- Realice una de las acciones siguientes:
 - Desde el panel del administrador de Active Directory u Okta, suspenda al usuario o márkelo como inactivo.
 - Elimine al usuario de cualquier grupo de Active Directory que tenga permisos Basic o Pro asignados.

Cambio del PIN personal de las reuniones

Un número PIN personal para reuniones es un ID estático generado cuando el usuario se registra. El PIN permite a un usuario de Amazon Chime programar reuniones fácilmente con otros usuarios de Amazon Chime. El uso de un número PIN personal para reuniones significa que los organizadores de las reuniones no tienen que recordar los detalles de la reunión para cada reunión nueva que programen.

Si un usuario considera que su número PIN personal para reuniones se ha podido filtrar, es posible restablecer su número PIN y generar un ID nuevo. Después de actualizar un número PIN personal para reuniones, el usuario debe actualizar todas las reuniones que se programaron con el número PIN personal para reuniones antiguo.

Para cambiar un número PIN personal para reuniones

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En la página Cuentas, seleccione el nombre de la cuenta de Amazon Chime.
3. En el panel de navegación, seleccione Usuarios.
4. Busque el usuario cuyo número PIN necesita cambiar.
5. Para abrir la página User detail (Datos del usuario), elija el nombre del usuario.
6. Elija User actions (Acciones del usuario), Reset personal PIN (Restablecer el número PIN personal), Confirm (Confirmar).

Administración de versiones de prueba Pro

Cuando un usuario acepta una invitación para formar parte de un equipo de Amazon Chime, o cuando se le agrega a una cuenta corporativa, finaliza la versión de prueba gratuita y obtiene permisos Pro. Esto le permite continuar siendo el anfitrión de las reuniones que ha programado. Si se cambia el nivel de permisos de un usuario a Basic, este no podrá actuar como anfitrión de una reunión.

Dado que los precios de Amazon Chime se basan en el uso, solo se paga por los usuarios que organizan reuniones los días que las organizan. No se cobra por los asistentes a las reuniones ni por los usuarios de chat.

Los usuarios con una licencia Pro se consideran Active Pro si han organizado una reunión que finalizó en un día natural y se cumple al menos una de las condiciones siguientes:

- La reunión se programó.
- La reunión incluía más de dos los asistentes.
- Durante la reunión se produjo al menos un evento de grabación.
- La reunión contó con la presencia de una persona que llamó por teléfono.
- La reunión contó con la presencia de un asistente que se unió con H.323 o SIP.

Para obtener más información, consulte [Planes y precios](#).

Solicitar archivos adjuntos de los usuarios

Si administra una cuenta corporativa y tiene los permisos adecuados, puede solicitar y recibir archivos adjuntos que los usuarios hayan cargado en Amazon Chime, tanto en conversaciones individuales y de grupo como en salas de chat que hayan creado.

Note

Si administra una cuenta de equipo de Amazon Chime, puede reclamar uno o varios dominios para actualizar a una cuenta corporativa. También puede quitar usuarios de la cuenta de equipo, lo que permite a esos usuarios no administrados obtener sus archivos adjuntos mediante el asistente de Amazon Chime.

Para solicitar archivos adjuntos de los usuarios

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En la página Cuentas, seleccione el nombre de la cuenta de Amazon Chime.
3. En Settings (Configuración), elija Account (Cuenta), Account actions (Acciones de cuenta) y Request attachments (Solicitar archivos adjuntos).
4. En un plazo aproximado de 24 horas, la página Resumen de la cuenta proporcionará un enlace a un archivo que contiene una lista de URL prefirmadas que puede utilizar para obtener acceso a cada uno de los archivos adjuntos.
5. Descargar el archivo.

Note

Asegúrese de mantener un nivel de control de acceso adecuado en el archivo. Todo usuario que obtenga el archivo, puede utilizar la lista de las URL que se proporciona para descargar los archivos adjuntos asociados.

Las URL prefirmadas caducan al cabo de seis días. Puede enviar una solicitud una vez cada siete días.

Para usar políticas AWS Identity and Access Management (IAM) para administrar el acceso a la consola de administración de Amazon Chime y la acción Solicitar archivos adjuntos, use una de las políticas administradas de Amazon Chime FullAccess (UserManagement,, o). ReadOnly Si lo desea, también puede actualizar las políticas personalizadas para incluir las acciones StartDataExport y RetrieveDataExport. Para obtener más información sobre estas acciones, consulte [Acciones definidas por Amazon Chime](#) en la Guía del usuario de IAM.

Cómo gestiona Amazon Chime las actualizaciones automáticas

Amazon Chime ofrece diferentes formas de actualizar sus clientes. El método varía en función de si ejecuta Amazon Chime en un navegador, en el escritorio o en un dispositivo móvil.

La aplicación web de Amazon Chime (<https://app.chime.aws>) siempre se carga con las características y correcciones de seguridad más recientes.

El cliente de escritorio de Amazon Chime comprueba si hay actualizaciones cada vez que seleccione Salir o Cerrar sesión. Esto se aplica a los equipos Windows y macOS. Si se ejecuta el cliente,

este comprueba si hay actualizaciones cada tres horas. También puede buscar actualizaciones seleccionando Buscar actualizaciones en el menú Ayuda de Windows o en el menú Amazon Chime de macOS.

Cuando el cliente de escritorio detecta una actualización, Amazon Chime pide al usuario que la instale, a menos que esté en una reunión en curso. Está en una reunión en curso cuando:

- Asiste a una reunión.
- Los han invitado a una reunión que todavía está en curso.

Amazon Chime le pide que instale la última versión y proporciona una cuenta regresiva de 15 segundos para que pueda posponer la instalación. Los usuarios pueden elegir Probar más tarde para posponer la actualización.

Si los usuarios posponen una actualización y no están en una reunión en curso, el cliente comprueba si existe la actualización al cabo de tres horas y les pide de nuevo que la instalen. La instalación comienza cuando finaliza la cuenta regresiva.

Note

En un equipo macOS, los usuarios deben seleccionar Reiniciar ahora para iniciar la actualización.

En dispositivos móviles: las aplicaciones móviles de Amazon Chime utilizan las opciones de actualización que ofrecen App Store y Google Play para ofrecer la última versión del cliente de Amazon Chime. También puede usar el sistema de administración de dispositivos móviles para implementar actualizaciones.

Migración de usuarios a otra cuenta de equipo

Para migrar usuarios a otras cuentas de equipo, debe crear y configurar una cuenta de destino, si aún no existe ninguna. A continuación, añada los usuarios a la cuenta de destino. Los siguientes pasos le llevan a la información sobre cómo completar cada parte de una migración.

Para migrar usuarios

1. Si no dispone de una cuenta de equipo de destino, cree una. Para obtener más información, consulte [Paso 1: Crear una cuenta de administrador de Amazon Chime](#).

2. Configure la cuenta según sea necesario. Para obtener más información, consulte [Paso 2 \(opcional\): Configurar los ajustes de la cuenta](#).
3. Añada usuarios a la cuenta. Para obtener más información, consulte [Paso 3: Agregar usuarios a la cuenta](#).

Administración de números de teléfono en Amazon Chime

Utilice la consola Amazon Chime para aprovisionar números de teléfono. Cuando aprovisiona números, los solicita desde un grupo de números administrado por el SDK de Amazon Chime. Al anular la asignación de números y, a continuación, eliminarlos, estos vuelven al grupo.

Puede aprovisionar los siguientes tipos de números de teléfono:

Amazon Chime Business Calling

Permite a sus usuarios enviar y recibir llamadas telefónicas y mensajes de texto directamente desde Amazon Chime. Utilice la consola Amazon Chime que se encuentra en <https://chime.aws.amazon.com/> para aprovisionar números de teléfono y transferir los números de teléfono existentes. A continuación, asigne los números a sus usuarios de Amazon Chime y concédales permisos para enviar y recibir llamadas telefónicas y mensajes de texto mediante a través de ellos.

Note

Amazon Chime Business Calling tiene requisitos de ancho de banda. Para obtener más información, consulte [Requisitos de ancho de banda](#).

Amazon Chime Voice Connector

Proporciona servicios de enlace troncal del Protocolo de inicio de sesión (SIP) para los sistemas telefónicos existentes. Puede transferir los números de teléfono existentes o usar la consola Amazon Chime para aprovisionar números de teléfono nuevos. Use los números de teléfono del Amazon Chime Voice Connector para las llamadas entrantes o salientes, o para ambas. Para obtener más información, consulte [Administración de instancias de Amazon Chime Voice Connector](#) en la Guía de administración del SDK de Amazon Chime.

Note

Amazon Chime Business Calling no ofrece servicios de llamadas de emergencia fuera de Estados Unidos. Para modificar los servicios de llamadas de emergencia que proporciona Amazon Chime en Estados Unidos, puede obtener un número de enrutamiento de llamadas de emergencia de un proveedor de servicios de emergencia externo, proporcionar ese número a Amazon Chime y completar la configuración con las

instancias de Amazon Chime Voice Connector. Para obtener más información, consulte [Configuración de los números de enrutamiento de llamadas de emergencia para su instancia de Amazon Chime Voice Connector](#) en la Guía de administración del SDK de Amazon Chime.

Reglas y aplicaciones SIP multimedia

Las aplicaciones multimedia del Protocolo de inicio de sesión (SIP) facilitan y agilizan la creación de instrucciones multimedia y de señalización personalizadas que normalmente se crearían en la central telefónica de conmutación (PBX). Reglas SIP

Contenido

- [Aprovisionamiento de números de teléfono](#)
- [Solicitud de números de teléfono internacionales](#)
- [Portabilidad de números de teléfono existentes](#)
- [Asignación de números de teléfono de Amazon Chime Business Calling](#)
- [Anular la asignación de números de teléfono de Amazon Chime Business Calling](#)
- [Actualización de nombres de llamadas salientes](#)
- [Eliminación de números de teléfono](#)
- [Restauración de números de teléfono eliminados](#)

Aprovisionamiento de números de teléfono

Utilice la consola Amazon Chime para aprovisionar números de teléfono para su cuenta de Amazon Chime. Los números provienen de un grupo administrado por Amazon Chime. Elija Amazon Chime Business Calling para aprovisionar y asignar números de teléfono a sus usuarios actuales de Amazon Chime.

Cuando se complete el aprovisionamiento, los números de teléfono aparecerán en su Inventario. A continuación, puede asignarlos a usuarios individuales.

Para aprovisionar números de teléfono

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En el panel de navegación, en Llamada, elija Administración de números de teléfono.

3. Elija Orders (Pedidos), Provision phone numbers (Aprovisionar números de teléfono).
4. Seleccione Business Calling y, a continuación, seleccione Siguiente.
5. Busque los números de teléfono disponibles. Seleccione los números de teléfono que desee y, a continuación, elija Provision (Aprovisionar).

Los números de teléfono se muestran en las listas Pedidos y Pendiente mientras se realiza el aprovisionamiento.

Solicitud de números de teléfono internacionales

En los pasos de esta sección se explica cómo solicitar números de teléfono internacionales para usarlos con Amazon Chime. Mientras avanza, recuerde que solo puede usar números internacionales con el tipo de producto Llamadas de la aplicación multimedia SIP.

Para comprar números internacionales, la normativa de muchos países exige que dispongas de lo siguiente:

- Dirección local
- Prueba de su identidad, de Amazon Chime o de nuestros transportistas

Espere entre 2 y 6 semanas a que Amazon Chime tramite su solicitud. Para obtener más información acerca de los requisitos de documentación de los distintos países, consulte [the section called "Requisitos nacionales para los números de teléfono"](#).

Para solicitar números de teléfono internacionales en países con requisitos de identificación

1. Realice una de las acciones siguientes:
 - Abra la [consola Amazon Chime](#) y seleccione Soporte y, a continuación, Enviar solicitud.
 - Si es cliente de AWS Support, abra la página del Centro de AWS Support, inicie sesión si es necesario y elija Crear caso y, a continuación, Soporte técnico. En Service (Servicio), elija Chime.
2. En Category (Categoría), elija Other (Otra).
3. En Asunto, introduzca Números internacionales de aprovisionamiento.
4. En Incidencia o Descripción, especifique lo siguiente:
 - Individual o empresarial

- Nombre (nombre individual o nombre comercial)
 - Tipo de número (local o gratuito)
 - País
 - Cantidad de números de teléfono
5. Realice una de las acciones siguientes:
- Si envía una solicitud de soporte desde la consola Amazon Chime, para Correo electrónico, escriba la dirección de correo electrónico asociada a su cuenta de administrador de Amazon Chime y, a continuación, elija Enviar solicitud.
 - Si crea un caso en el [Centro de AWS Support](#), en Archivos adjuntos, seleccione Elegir archivos y adjunte los documentos necesarios. En Contact options (Opciones de contacto), seleccione un método de contacto. Si lo desea, en Additional contacts (Otros contactos), escriba la dirección de correo electrónico de las personas a las que se les van a enviar notificaciones sobre el estado del caso.

AWS Support responde a su solicitud de soporte para informarle si los números de teléfono se pueden aprovisionar. Recibirá respuestas de AWS Support de una de las siguientes maneras:

- Si envió una solicitud de soporte desde la consola de Amazon Chime, AWS Support envía un correo electrónico al contacto de operaciones especificado en Contactos alternativos en la información de contacto de su AWS cuenta. Para obtener más información, consulte [Edición de la información de contacto](#) en la Guía del usuario de AWS Billing and Cost Management.
- Si ha creado un caso en el [Centro de AWS Support](#), recibirá las respuestas con arreglo a los métodos de contacto seleccionados y las direcciones de correo electrónico que haya especificado en los contactos adicionales.

Una vez aprovisionados los números, puede verlos en la consola Amazon Chime, en Llamadas, administración de números de teléfono e inventario.

6. Utilice las reglas SIP para asignar los números de teléfono a la aplicación multimedia SIP correspondiente.

Requisitos nacionales para los números de teléfono

Fuera de EE. UU., las normativas requieren a menudo una dirección local y documentos de identificación específicos para comprar y usar un número de teléfono. La dirección puede ser

una dirección comercial o personal. En las siguientes tablas se indican los países que requieren identificación. Cuando [solicita números de teléfono internacionales](#) o transfiere [números de teléfono existentes](#), el servicio de Support de Amazon Chime le ayuda a enviar los documentos necesarios.

Note

Asegúrese de proporcionar las identidades y direcciones de los usuarios finales que utilizan sus números de teléfono.

Temas

- [Australia](#)
- [Austria](#)
- [Canadá](#)
- [Dinamarca](#)
- [Finlandia](#)
- [Alemania](#)
- [Irlanda](#)
- [Italia](#)
- [Nueva Zelanda](#)
- [Nigeria](#)
- [Puerto Rico](#)
- [Corea del Sur](#)
- [Suecia](#)
- [Suiza](#)
- [Reino Unido](#)

Australia

En las siguientes tablas se indican y describen los requisitos para solicitar y transferir números de teléfono en Australia.

Solicitud de números de teléfono

Tipos de productos admitidos	Tipos de número	Requisitos de ID	Tipos de identificación aceptables
Llamadas de la aplicación multimedia a SIP del SDK de Amazon Chime	Local	Sí	<ul style="list-style-type: none"> Dirección comercial Comprobante de ubicación <p>Las direcciones comerciales deben tener la misma zona geográfica que sus números de teléfono correspondientes.</p>
	Gratuito	Sí	<ul style="list-style-type: none"> Dirección comercial <p>Se aceptan direcciones internacionales.</p>

Portabilidad de números de teléfono

Tipos de productos admitidos	Tipos de número	ID obligatorio
Llamadas de la aplicación multimedia SIP	Local	<ul style="list-style-type: none"> Última factura del proveedor actual Carta de autorización
	Gratuito	<ul style="list-style-type: none"> Última factura del proveedor actual Carta de autorización

Austria

En las siguientes tablas se indican y describen los requisitos para solicitar y transferir números de teléfono en Austria.

Solicitud de números de teléfono

Tipos de productos admitidos	Tipos de número	Requisitos de ID	Tipos de identificación aceptables
Llamadas de la aplicación multimedia SIP	Local	Sí	<ul style="list-style-type: none"> • Dirección comercial • Comprobante de servicios de telecomunicaciones , como una factura de un operador de red con otro número de teléfono en la misma zona. <p style="text-align: center;">-O BIEN-</p> <p>Una factura de un proveedor de Internet por el acceso a Internet con una dirección IP fija ubicada en el área correcta.</p> <p>Las direcciones comerciales deben tener la misma zona geográfica que sus números de teléfono correspondientes.</p>
	Prefijos nacionales: +43 720	Sí	<ul style="list-style-type: none"> • Dirección comercial

Tipos de productos admitidos	Tipos de número	Requisitos de ID	Tipos de identificación aceptables
			La dirección debe estar ubicada en el país.
	Gratuito	Sí	<ul style="list-style-type: none"> Dirección comercial <p>Se acepta una dirección extranjera</p>

Portabilidad de números de teléfono

Tipos de productos admitidos	Tipos de número	ID obligatorio
Llamadas de la aplicación multimedia SIP	Local	<ul style="list-style-type: none"> Última factura del proveedor actual Carta de autorización
	Gratuito	<ul style="list-style-type: none"> Última factura del proveedor actual Carta de autorización

Canadá

En las siguientes tablas se indican y describen los requisitos para solicitar y transferir números de teléfono en Canadá.

Solicitud de números de teléfono

Tipos de productos admitidos	Tipos de número	Requisitos de ID	Tipos de identificación aceptables
Llamadas de la aplicación multimedia SIP	Local	No	N/A
Gratuito	No	N/A	N/A

Portabilidad de números de teléfono

Tipos de productos admitidos	Tipos de número	ID obligatorio
Llamadas de la aplicación multimedia SIP	Local	<ul style="list-style-type: none"> Última factura del proveedor actual Carta de autorización
	Gratuito	<ul style="list-style-type: none"> Última factura del proveedor actual Carta de autorización

Dinamarca

En las siguientes tablas se indican y describen los requisitos para solicitar y transferir números de teléfono en Dinamarca.

Solicitud de números de teléfono

Tipos de productos admitidos	Tipos de número	Requisitos de ID	Tipos de identificación aceptables
Llamadas de la aplicación multimedia SIP	Local	No	N/A
	Gratuito	No	N/A

Portabilidad de números de teléfono

Tipos de productos admitidos	Tipos de número	ID obligatorio
Llamadas de la aplicación multimedia SIP	Local	<ul style="list-style-type: none"> Última factura del proveedor actual Carta de autorización
	Gratuito	<ul style="list-style-type: none"> Última factura del proveedor actual Carta de autorización

Finlandia

En las siguientes tablas se indican y describen los requisitos para solicitar y transferir números de teléfono en Finlandia.

Solicitud de números de teléfono

Tipos de productos admitidos	Tipos de número	Requisitos de ID	Tipos de identificación aceptables
Llamadas de la aplicación multimedia SIP	Local	Sí	<ul style="list-style-type: none"> Dirección comercial Comprobante de ubicación <p>Las direcciones comerciales deben encontrarse en las mismas regiones geográficas que sus números de teléfono correspondientes.</p>
	Prefijos nacionales: +358 075	No	N/A

Tipos de productos admitidos	Tipos de número	Requisitos de ID	Tipos de identificación aceptables
	Gratuito	No	N/A

Portabilidad de números de teléfono

Tipos de productos admitidos	Tipos de número	ID obligatorio
Llamadas de la aplicación multimedia SIP	Local	<ul style="list-style-type: none"> Última factura del proveedor actual Carta de autorización
	Gratuito	<ul style="list-style-type: none"> Última factura del proveedor actual Carta de autorización

Alemania

En las siguientes tablas se indican y describen los requisitos para solicitar y transferir números de teléfono en Alemania.

Solicitud de números de teléfono

Tipos de productos admitidos	Tipos de número	Requisitos de ID	Tipos de identificación aceptables
Llamadas de la aplicación multimedia SIP	Local	Sí	<ul style="list-style-type: none"> Dirección comercial Una copia del registro de la empresa o una copia de su documento de identidad, si es una persona física

Tipos de productos admitidos	Tipos de número	Requisitos de ID	Tipos de identificación aceptables
			<ul style="list-style-type: none"> Comprobante de domicilio, como una factura de servicios públicos <p>Las direcciones comerciales deben tener la misma zona geográfica que sus números de teléfono correspondientes.</p>
	<p>Prefijos nacionales: +49 32</p>	<p>Sí</p>	<ul style="list-style-type: none"> Dirección comercial Una copia del registro de la empresa o una copia de su documento de identidad, si es una persona física Comprobante de domicilio, como una factura de servicios públicos <p>La dirección debe estar ubicada en el país.</p>

Tipos de productos admitidos	Tipos de número	Requisitos de ID	Tipos de identificación aceptables
	Gratuito	Sí	<ul style="list-style-type: none"> • Dirección comercial • Comprobante de domicilio, como una factura de servicios públicos <p>La dirección debe estar ubicada en el país.</p> <p>Debe obtener el número directamente del regulador local. Los detalles sobre el proceso se proporcionan al realizar la solicitud.</p>

Portabilidad de números de teléfono

Tipos de productos admitidos	Tipos de número	ID obligatorio
Llamadas de la aplicación multimedia SIP	Local	<ul style="list-style-type: none"> • Última factura del proveedor actual • Carta de autorización • Dirección comercial • Una copia del registro de la empresa • Copia del documento de identidad del representante de la empresa

Tipos de productos admitidos	Tipos de número	ID obligatorio
	Gratuito	<p>Las direcciones comerciales deben tener la misma zona geográfica que sus números de teléfono correspondientes.</p> <ul style="list-style-type: none"> • Última factura del proveedor actual • Carta de autorización • Certificado numérico de las NRA <p>Debe obtener el número directamente del regulador local. Los detalles sobre el proceso se proporcionan al realizar la solicitud</p>

Irlanda

En las siguientes tablas se indican y describen los requisitos para solicitar y transferir números de teléfono en Irlanda.

Solicitud de números de teléfono

Tipos de productos admitidos	Tipos de número	Requisitos de ID	Tipos de identificación aceptables
Llamadas de la aplicación multimedia SIP	Local	Sí	<ul style="list-style-type: none"> • Dirección comercial <p>Las direcciones comerciales deben encontrarse en las mismas regiones geográficas que sus</p>

Tipos de productos admitidos	Tipos de número	Requisitos de ID	Tipos de identificación aceptables
			números de teléfono correspondientes.
	Acceso universal y prefijos de VOIP: +353 0818, +353 076	Sí	<ul style="list-style-type: none"> Dirección comercial <p>La dirección debe estar ubicada en el país.</p>
	Gratuito	No	N/A

Portabilidad de números de teléfono

Tipos de productos admitidos	Tipos de número	ID obligatorio
Llamadas de la aplicación multimedia SIP	Local	<ul style="list-style-type: none"> Última factura del proveedor actual Carta de autorización
	Gratuito	<ul style="list-style-type: none"> Última factura del proveedor actual Carta de autorización

Italia

En las siguientes tablas se indican y describen los requisitos para solicitar y transferir números de teléfono en Italia.

Solicitud de números de teléfono

Tipos de productos admitidos	Tipos de número	Requisitos de ID	Tipos de identificación aceptables
Llamadas de la aplicación multimedia SIP	Local	Sí	<ul style="list-style-type: none"> • Dirección comercial • Comprobante de ubicación • Copia del registro de la empresa • Pasaporte o documento de identidad del usuario final <p>Las direcciones comerciales deben encontrarse en las mismas regiones geográficas que sus números de teléfono correspondientes.</p>
	Gratuito	No	N/A

Portabilidad de números de teléfono

Tipos de productos admitidos	Tipos de número	ID obligatorio
Llamadas de la aplicación multimedia SIP	Local	<ul style="list-style-type: none"> • Última factura del proveedor actual • Carta de autorización • Copia del pasaporte o documento de identidad del representante de la empresa

Tipos de productos admitidos	Tipos de número	ID obligatorio
		<ul style="list-style-type: none"> Copia del registro de la empresa local o comprobante de domicilio de una persona
	Gratuito	<ul style="list-style-type: none"> Última factura del proveedor actual Carta de autorización

Nueva Zelanda

En las siguientes tablas se indican y describen los requisitos para solicitar y transferir números de teléfono en Nueva Zelanda.

Solicitud de números de teléfono

Tipos de productos admitidos	Tipos de número	Requisitos de ID	Tipos de identificación aceptables
Llamadas de la aplicación multimedia SIP	Local	No	N/A
	Gratuito	No	N/A

Portabilidad de números de teléfono

Tipos de productos admitidos	Tipos de número	ID obligatorio
Llamadas de la aplicación multimedia SIP	Local	No admitido
	Gratuito	<ul style="list-style-type: none"> Última factura del proveedor actual Carta de autorización

Nigeria

En las siguientes tablas se indican y describen los requisitos para solicitar números de teléfono en Nigeria.

Solicitud de números de teléfono

Tipos de productos admitidos	Tipos de número	Requisitos de ID	Tipos de identificación aceptables
Llamadas de la aplicación multimedia SIP	Local	Sí	<ul style="list-style-type: none"> Dirección comercial <p>Se acepta una dirección extranjera.</p>

Puerto Rico

En las siguientes tablas se indican y describen los requisitos para solicitar y transferir números de teléfono en Puerto Rico.

Solicitud de números de teléfono

Tipos de productos admitidos	Tipos de número	Requisitos de ID	Tipos de identificación aceptables
Business Calling	Local	No	N/A
Voice Connector			
Gratuito	No	N/A	N/A

Corea del Sur

En las siguientes tablas se indican y describen los requisitos para solicitar números de teléfono en Corea del Sur.

Solicitud de números de teléfono

Tipos de productos admitidos	Tipos de número	Requisitos de ID	Tipos de identificación aceptables
Llamadas de la aplicación multimedia SIP	Gratuito	Sí	<ul style="list-style-type: none"> Dirección comercial Comprobante de ubicación <p>La dirección debe estar ubicada en el país.</p>

Suecia

En las siguientes tablas se indican y describen los requisitos para solicitar y transferir números de teléfono en Suecia.

Solicitud de números de teléfono

Tipos de productos admitidos	Tipos de número	Requisitos de ID	Tipos de identificación aceptables
Llamadas de la aplicación multimedia SIP	Local	No	N/A
	Gratuito	No	N/A

Portabilidad de números de teléfono

Tipos de productos admitidos	Tipos de número	ID obligatorio
Llamadas de la aplicación multimedia SIP	Local	<ul style="list-style-type: none"> Última factura del proveedor actual Carta de autorización
	Gratuito	<ul style="list-style-type: none"> Última factura del proveedor actual

Tipos de productos admitidos	Tipos de número	ID obligatorio
		<ul style="list-style-type: none"> • Carta de autorización

Suiza

En las siguientes tablas se indican y describen los requisitos para solicitar y transferir números de teléfono en Suiza.

Solicitud de números de teléfono

Tipos de productos admitidos	Tipos de número	Requisitos de ID	Tipos de identificación aceptables
Llamadas de la aplicación multimedia SIP	Local	Sí	<ul style="list-style-type: none"> • Dirección comercial • Comprobante de ubicación • Una copia del registro de la empresa o una copia de su documento de identidad, si es una persona física <p>Las direcciones comerciales deben tener la misma zona geográfica que sus números de teléfono correspondientes.</p>
	Prefijos de números comerciales: +41 051, +41 058	Sí	<ul style="list-style-type: none"> • Dirección comercial

Tipos de productos admitidos	Tipos de número	Requisitos de ID	Tipos de identificación aceptables
			La dirección debe estar ubicada en el país.
	Gratuito	Sí	<ul style="list-style-type: none"> • Dirección comercial • Una copia del registro de la empresa o una copia de su documento de identidad, si es una persona física <p>Se acepta una dirección extranjera</p>

Portabilidad de números de teléfono

Tipos de productos admitidos	Tipos de número	ID obligatorio
Llamadas de la aplicación multimedia SIP	Local	<ul style="list-style-type: none"> • Última factura del proveedor actual • Carta de autorización • Dirección comercial <p>Se aceptan direcciones extranjeras</p>
	Gratuito	<ul style="list-style-type: none"> • Última factura del proveedor actual • Carta de autorización • Dirección comercial

Tipos de productos admitidos	Tipos de número	ID obligatorio
		<ul style="list-style-type: none"> • Certificado de las NRA <p>La dirección debe estar dentro del país.</p>

Reino Unido

En las siguientes tablas se indican y describen los requisitos para solicitar y transferir números de teléfono en el Reino Unido.

Solicitud de números de teléfono

Tipos de productos admitidos	Tipos de número	Requisitos de ID	Tipos de identificación aceptables
Llamadas de la aplicación multimedia SIP	Local	No	N/A
	Gratuito	No	N/A

Portabilidad de números de teléfono

Tipos de productos admitidos	Tipos de número	ID obligatorio
Llamadas de la aplicación multimedia SIP	Local	<ul style="list-style-type: none"> • Última factura del proveedor actual • Carta de autorización
	Gratuito	<ul style="list-style-type: none"> • Última factura del proveedor actual • Carta de autorización

Portabilidad de números de teléfono existentes

Además de aprovisionar números de teléfono, también puede transferir números de su operador de telefonía a su inventario del SDK de Amazon Chime. Esto incluye números gratuitos. Puede usar números transferidos con los conectores de voz de Amazon Chime y las aplicaciones multimedia SIP del SDK de Amazon Chime.

En las siguientes secciones se explica cómo portar números de teléfono.

Temas

- [Requisitos previos para la portabilidad de números](#)
- [Transferencia de números de teléfono al SDK de Amazon Chime](#)
- [Presentación de los documentos requeridos](#)
- [Ver el estado de la solicitud](#)
- [Asignación de números portados](#)
- [Transferencia de números de teléfono del SDK de Amazon Chime](#)
- [Definiciones de estado de portabilidad de números de teléfono](#)

Requisitos previos para la portabilidad de números

Para poder transferir los números, debe disponer de lo siguiente:

- Una carta de agencia (LOA). Debe tener una LOA para los números de teléfono estadounidenses e internacionales. Descarga el [formulario de carta de agencia \(LOA\)](#) y rellénalo. Si va a realizar la portabilidad de números de teléfono de diferentes operadores, rellene una LOA distinta para cada operador.

Note

Varios países tienen requisitos de documentación para la portabilidad de números de teléfono. Para más información, consulte la sección [Requisitos nacionales para los números de teléfono](#) de esta guía.

- Antes de poder portar números de teléfono para los conectores de voz de Amazon Chime, debe crear un conector de voz. Para obtener más información, consulte <https://docs.aws.amazon.com/>

chime-sdk/latest/ag/create-voicecon.html Creación de un conector de voz del SDK de Amazon Chime en la Guía del administrador del SDK de Amazon Chime.

Transferencia de números de teléfono al SDK de Amazon Chime

Crea una solicitud de soporte para transferir los números de teléfono existentes al SDK de Amazon Chime.

Para transferir números de teléfono existentes al SDK de Amazon Chime

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En la barra de comandos de la parte superior de la página, selecciona Support y, a continuación, selecciona Enviar solicitud.

Esto lo lleva a la consola AWS Support.

Note

También puede ir directamente a la página [AWS Support central](#). Si es así, selecciona Crear caso y sigue los pasos que se indican a continuación.

3. En Cómo podemos ayudar, haz lo siguiente:
 - a. Elija Cuenta y facturación.
 - b. En la lista de servicios, selecciona Chime SDK (Number Management).
 - c. En la lista de categorías, selecciona Número de teléfono (Port In).
 - d. Elija Siguiente paso: información adicional.
4. En Información adicional, haga lo siguiente
 - a. En Asunto, introduzca **Porting phone numbers in**.
 - b. En Descripción, introduzca la siguiente información:

Para transferir números estadounidenses:

- Número de teléfono de facturación (BTN) de la cuenta.
- Nombre de la persona que autoriza. Esta es la persona encargada de la facturación de la cuenta con el operador actual.

- Operador actual, si se conoce.
- Número de la cuenta de servicio, si esta información está presente con el operador actual.
- PIN de servicio, si está disponible.
- Dirección de servicio y nombre del cliente, tal y como aparecen en el contrato con su operador actual.
- Fecha y hora solicitadas para la transferencia.
- (Opcional) Si quieres transferir tu número de teléfono de facturación (BTN), selecciona una de las siguientes opciones:
 - Estoy realizando la portabilidad de mi BTN y quiero reemplazarlo por un nuevo BTN que facilito. Puedo confirmar que este nuevo BTN está en la misma cuenta con el operador actual.
 - Estoy realizando la portabilidad de mi BTN y quiero cerrar mi cuenta con mi operador actual.
 - Estoy realizando la portabilidad de mi BTN porque mi cuenta está configurada actualmente para que cada número de teléfono sea su propio BTN. (Seleccione esta opción sólo cuando su cuenta con el operador actual esté configurada de esta manera).
 - Después de elegir una opción, adjunta tu carta de agencia (LOA) a la solicitud.

Para transferir números internacionales:

- Debe utilizar el tipo de producto SIP Media Application Dial-In para números de teléfono no estadounidenses.
 - Tipo de número (local o gratuito)
 - Números de teléfono existentes que se van a transferir.
 - Calcule el volumen de uso
 - País
- c. En la lista de tipos de números de teléfono, selecciona Business Calling, SIP Media Application Dial-In o Voice Connector.
 - d. En Número de teléfono, ingresa al menos un número de teléfono, incluso si vas a transferir varios números.
 - e. En Fecha de portabilidad, ingresa la fecha de portabilidad deseada.
 - f. En Hora de portabilidad, introduzca la hora deseada.

5. En Resolver ahora o contactar con nosotros, selecciona Contactar con nosotros.
6. En la lista de idiomas de contacto preferidos, elige un idioma
7. Elige Internet o Teléfono. Si eliges Teléfono, introduce tu número de teléfono. Cuando termines, selecciona Enviar.

AWS Support le permite saber si sus números de teléfono se pueden transferir desde su proveedor de telefonía actual. Si puedes, debes enviar todos los documentos necesarios. Los pasos de la siguiente sección explican cómo enviar esos documentos.

Presentación de los documentos requeridos

Una vez que AWS Support indique que puedes transferir números de teléfono, tendrás que enviar todos los documentos necesarios. En los siguientes pasos se explica cómo hacerlo.

Note

AWS Support proporciona un enlace seguro a Amazon S3 para cargar todos los documentos solicitados. No continúe hasta que reciba el enlace.

Para enviar documentos

1. [Abra la consola del SDK de Amazon Chime en https://console.aws.amazon.com/chime-sdk/home.](https://console.aws.amazon.com/chime-sdk/home)
2. Inicie sesión en su AWS cuenta y, a continuación, abra el enlace de carga de Amazon S3 generado específicamente para su cuenta.

Note

El enlace caduca a los diez días. Se genera específicamente para la cuenta que creó el caso. El enlace requiere un usuario autorizado de la cuenta para realizar la carga.

3. Selecciona Añadir archivos y, a continuación, selecciona los documentos de identidad relacionados con tu solicitud.
4. Amplíe la sección Permisos y elija Especificar permisos de ACL individuales.
5. Al final de la sección Lista de control de acceso (ACL), elija Agregar concesionario y, a continuación, pegue la clave proporcionada por AWS Support en el cuadro del concesionario.

6. En Objetos, selecciona la casilla Leer y, a continuación, selecciona Cargar.

Después de proporcionar la carta de agencia (LOA), AWS Support confirme con su operador de telefonía actual que la información de la LOA es correcta. Si la información proporcionada en la LOA no coincide con la información que tiene registrada su operador telefónico, AWS Support se pondrá en contacto con usted para actualizar la información facilitada en la LOA.

Ver el estado de la solicitud

Utilizar la consola del SDK de Amazon Chime para ver el estado de las solicitudes de portabilidad.

Para ver el estado

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En el panel de navegación, seleccione Administración de números de teléfono.
3. Seleccione la pestaña Pedidos.

La columna Estado muestra el estado de su solicitud. AWS Support también se pone en contacto contigo con actualizaciones y solicitudes de más información, según sea necesario. Para obtener más información, consulte [Definiciones de estado de portabilidad de números de teléfono](#) más adelante en esta sección.

Asignación de números portados

Una vez que su operador de telefonía confirme que la LOA es correcta, revisará y aprobará el puerto solicitado. Luego, AWS Support proporcionan una fecha y hora de confirmación de pedido en firme (FOC) para que se produzca el puerto.

En la fecha FOC, los números de teléfono transferidos se activan para su uso con el SDK de Amazon Chime. A continuación, debe asignar los números a un conector de voz de Amazon Chime o a una aplicación multimedia SIP para poder realizar y recibir llamadas.

- Para asignar números a los conectores de voz, siga los pasos que se indican en [Asignación y desasignación de números de teléfono del conector de voz del SDK de Amazon Chime, en la Guía del administrador](#) del SDK de Amazon Chime.
- Para los números de acceso telefónico de la aplicación multimedia SIP del SDK de Amazon Chime, utilice las reglas SIP para asignar números. Para obtener más información, consulte [Creación de una regla SIP](#) en la Guía del administrador del SDK de Amazon Chime.

Transferencia de números de teléfono del SDK de Amazon Chime

Note

La capacidad de transferir números fuera del SDK de Amazon Chime depende de la capacidad del transportista receptor para aceptar esos números.

Para transferir números de teléfono existentes al SDK de Amazon Chime

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En el panel de navegación, en Contact Us, selecciona Support.

Esto lo lleva a la consola AWS Support.

Note

También puede ir directamente a la página [AWS Support central](#). Si es así, selecciona Crear caso y sigue los pasos que se indican a continuación.

3. En Cómo podemos ayudar, haz lo siguiente:
 - a. Elija Cuenta y facturación.
 - b. En la lista de servicios, selecciona Chime SDK (Number Management).
 - c. En la lista de categorías, selecciona Puerto de salida de número de teléfono.
 - d. Elija Siguiente paso: información adicional.
4. En Información adicional, haga lo siguiente
 - a. En Asunto, introduzca **Porting phone numbers out**.
 - b. En Descripción, introduzca los datos pertinentes.

AWS Support responde con un identificador de cuenta y un PIN para que los utilices cuando solicites el puerto a tu nuevo operador. Recibirás respuestas en función de los métodos de contacto que hayas seleccionado y de cualquier dirección de correo electrónico que hayas introducido para otros contactos.

Cuando finalice el proceso de transferencia y los números de teléfono se transfieran a su nuevo operador, anule la asignación y elimine los números de teléfono de su inventario del SDK de Amazon Chime. Para más información, consulte [Asignación de números de teléfono de Amazon Chime Business Calling](#) y [Eliminación de números de teléfono](#).

Definiciones de estado de portabilidad de números de teléfono

Tras enviar una solicitud para transferir números de teléfono existentes al SDK de Amazon Chime, puede ver el estado de la solicitud de transferencia en la consola del SDK de Amazon Chime, en Llamadas, administración de números de teléfono, pendiente.

Los estados y las definiciones de portabilidad son los siguientes:

CANCELLED

AWS Support cancelaste la orden de transferencia debido a un problema con el puerto, como una solicitud de cancelación del transportista o tuya. AWS Support se pone en contacto contigo para proporcionarte los detalles.

CANCEL_REQUESTED

AWS Support está procesando la cancelación de la orden de transferencia debido a un problema con el puerto, como una solicitud de cancelación del transportista o suya. AWS Support se pone en contacto con usted con los detalles.

CHANGE_REQUESTED

AWS Support está procesando tu solicitud de cambio y la respuesta del transportista está pendiente. Conceda más tiempo para el procesamiento de la solicitud.

COMPLETED

El pedido de portabilidad se ha completado, y los números de teléfono se han activado.

EXCEPTION

AWS Support se pone en contacto contigo para obtener los detalles adicionales necesarios para completar la solicitud de puerto. Conceda más tiempo para el procesamiento de la solicitud.

FOC

La fecha FOC se confirma con el transportista. AWS Support contacta contigo para confirmar la fecha.

PENDING DOCUMENTS

AWS Support se pone en contacto con usted para solicitar los documentos adicionales necesarios para completar la solicitud de puerto. Conceda más tiempo para el procesamiento de la solicitud.

SUBMITTED

El pedido de portabilidad se ha enviado, y la respuesta del operador está pendiente.

Asignación de números de teléfono de Amazon Chime Business Calling

Utilice la página de inventario de administración de números de teléfono para asignar números de teléfono de Amazon Chime Business Calling a usuarios individuales. Por el contrario, usted administra sus números de teléfono de Amazon Chime Business Calling desde los perfiles de usuario.

Para asignar números de teléfono de Amazon Chime Business Calling

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En el panel de navegación, en Llamada, elija Administración de números de teléfono.
3. Seleccione la pestaña Inventario y, a continuación, seleccione el número de teléfono de Amazon Chime Business Calling para asignárselo a un usuario.
4. Elija Assign (Asignar).
5. Seleccione la cuenta a la que pertenece el usuario y elija Next (Siguiendo).
6. Seleccione el nombre completo del usuario y elija Assign (Asignar).

Cuando cambie el número de teléfono o los permisos de número de teléfono de Amazon Chime de un usuario, le recomendamos que facilite al usuario el nuevo número de teléfono o la información de los permisos. Antes de que los usuarios puedan obtener acceso a sus nuevas características de número de teléfono o permisos, deben cerrar sesión en su cuenta de Amazon Chime e iniciar sesión de nuevo.

Anular la asignación de números de teléfono de Amazon Chime Business Calling

El siguiente procedimiento anula la asignación de los números de teléfono de los usuarios de Amazon Chime Business Calling.

Para anular la asignación de números de teléfono

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En Calling (Llamadas), seleccione Phone number management (Administración de números de teléfono).
3. Elija Inventory (Inventario) y seleccione el número de teléfono cuya asignación desea anular.
4. Elija Unassign (Anular asignación).
5. Active la casilla y elija Unassign (Anular asignación).

Puede ver los detalles de los números de teléfono de su inventario. Por ejemplo, puede ver a qué usuario de Amazon Chime Business Calling está asignado un número. También puede ver si las llamadas telefónicas y los mensajes de texto están habilitados.

Para ver los detalles de los números de teléfono del inventario

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En el panel de navegación, en Llamada, elija Administración de números de teléfono.
3. Elija Inventario y seleccione los números de teléfono que desea ver.
4. Abra la lista Acciones y elija Ver detalles.

Actualización de nombres de llamadas salientes

Puede establecer un nombre de llamada predeterminado para uno o más números de teléfono de su inventario. A continuación, el nombre les aparecerá a los destinatarios de las llamadas salientes realizadas con esos números de teléfono. Los nombres de llamada predeterminados se aplican a todos los tipos de productos de números de teléfono. Puede actualizar los nombres una vez cada siete días.

Para establecer un nombre de llamada predeterminado

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En el panel de navegación, en Llamada, elija Administración de números de teléfono.
3. Elija la pestaña Inventario y seleccione las casillas de verificación situadas al lado de los números de teléfono que desea actualizar.
4. Abra la lista Acciones y seleccione Actualizar el nombre de llamada predeterminado.
5. En Nombre de llamada predeterminado, escriba un nombre de llamada predeterminado de hasta 15 caracteres.
6. Seleccione Guardar.

Espere 72 horas para que el sistema actualice el nombre de llamada predeterminado.

Establezca un nombre de llamada único para números de teléfono individuales en la pantalla de detalles del número de teléfono.

Para establecer un nombre de llamada único

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En el panel de navegación, en Llamada, elija Administración de números de teléfono.
3. Elija Inventario y seleccione los números de teléfono a los que desea actualizarles el nombre.
4. Abra la lista Acciones y elija Ver detalles.
5. En la pantalla de detalles del número de teléfono, para Actions (Acciones), elija Update unique calling name (Actualizar nombre de llamada único).
6. En Nombre de llamada único, escriba un nombre de llamada único de hasta 15 caracteres.
7. Seleccione Guardar.

El sistema actualiza el nombre en un plazo de 72 horas. Una vez terminada la actualización, puede actualizar de nuevo el nombre de la llamada.

Eliminación de números de teléfono

Important

Solo los administradores del sistema Amazon Chime pueden completar estos pasos. Además, debe anular la asignación de los números de teléfono para poder eliminarlos. Realice una de las acciones siguientes:

- Si usa un servicio Voice Connector o un grupo de servicios Voice Connector, anule la asignación del número. Para obtener más información, consulte [Anulación de la asignación de números de teléfono de usuarios](#) en la Guía del administrador del SDK de Amazon Chime.
- Si usa una aplicación multimedia SIP, elimine la regla SIP que contiene el número. Para obtener más información, consulte [Eliminación de reglas SIP](#) en la Guía del administrador del SDK de Amazon Chime.

Cuando se aprovisiona un número de teléfono, se solicita a un grupo de números que Amazon Chime mantiene. Al eliminar un número, se devuelve al grupo. Cuando se elimina un número, primero pasa a la lista de borrados, donde se guarda durante 7 días. Durante ese tiempo, puede volver a mover el número al inventario. Transcurridos los 7 días, el sistema borra automáticamente el número de la lista de espera y lo desvincula de su cuenta. Esto devuelve el número al conjunto de números del SDK de Amazon Chime. Si necesita recuperar un número después de que el sistema lo elimine de la lista de espera, siga los pasos que se indican [Aprovisionamiento de números de teléfono](#), pero tenga en cuenta que es posible que el número no esté disponible.

Para eliminar números de teléfono que ya no están asignados

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En el panel de navegación, en Llamada, elija Administración de números de teléfono.
3. Elija la pestaña Inventario y, después, seleccione el número o los números de teléfono que desea eliminar.
4. Abra la lista Acciones y seleccione Eliminar números de teléfono.
5. Active la casilla y seleccione Eliminar.

Los números de teléfono eliminados se guardan en Cola de eliminación durante 7 días antes de que se eliminen del inventario de manera permanente.

Restauración de números de teléfono eliminados

Puede restaurar los números de teléfono eliminados de la Cola de eliminación en un plazo máximo de 7 días después de eliminarlos. Al restaurar un número de teléfono, este se mueve de nuevo a Inventory (Inventario).

Para restaurar números de teléfono eliminados

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. En el panel de navegación, en Llamada, elija Administración de números de teléfono.
3. Elija la pestaña Cola de eliminación y, después, seleccione el número o los números de teléfono que desea restaurar.
4. Elija Move to inventory (Mover a inventario).

Administración de la configuración global en Amazon Chime

Puede utilizar la consola Amazon Chime para administrar la configuración del registro detallado de las llamadas.

Configuración de registros de detalles de las llamadas

Para poder configurar las opciones de registro de detalles de llamadas para su cuenta administrativa de Amazon Chime, primero debe crear un bucket de Amazon Simple Storage Service. El bucket de Amazon S3 se utiliza como el destino de registro para los registros de detalles de llamadas. Cuando configure las opciones de registro de detalles de llamadas, debe conceder acceso de lectura y escritura en Amazon Chime al bucket de Amazon S3 para poder guardar y administrar sus datos. Para obtener más información acerca de cómo crear un bucket de Amazon S3, consulte [Introducción a Amazon Simple Storage Service](#) en la Guía del usuario de Amazon Simple Storage Service.

Puede configurar los ajustes del registro detallado de llamadas para Amazon Chime Business Calling. Para obtener más información acerca de Amazon Chime Business Calling, consulte [Administración de números de teléfono en Amazon Chime](#).

Para configurar las opciones de registro de detalles de llamadas

1. Para crear un bucket de Amazon S3, siga los pasos que se indican en [Introducción a Amazon Simple Storage Service](#) en la Guía del usuario de Amazon Simple Storage Service.
2. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
3. En Global Settings (Configuración global), elija Call detail records (Registros de detalles de llamadas).
4. Elija Configuración de Business Calling
5. En Destino del registro, seleccione el bucket de Amazon S3.
6. Seleccione Guardar.

Puede detener los registros de detalles de llamadas en cualquier momento.

Para detener los registros de detalles de llamadas

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.

2. En Global Settings (Configuración global), elija Call detail records (Registros de detalles de llamadas).
3. Elija Disable logging (Deshabilitar el registro) para la configuración aplicable.

Registros detallados de llamadas de Amazon Chime Business Calling

Cuando elige recibir registros de detalles de llamadas para Amazon Chime Business Calling, estos se envían a su bucket de Amazon S3. En el ejemplo siguiente se muestra el formato general de un nombre de registro de detalles de llamadas de Amazon Chime Business Calling.

```
Amazon-Chime-Business-Calling-CDRs/json/111122223333/2019/03/01/123a4567-  
b890-1234-5678-cd90efgh1234_2019-03-01-17.10.00.020_1a234567-89bc-01d2-3456-  
e78f9g01234h
```

En el ejemplo siguiente se muestran los datos que se representan en el nombre del registro de detalles de llamadas.

```
Amazon-Chime-Business-Calling-CDRs/json/awsAccountID/year/month/  
day/conferenceID_connectionDate-callStartTime-callDetailRecordID
```

En el ejemplo siguiente se muestra el formato general de un registro de detalles de llamadas de Amazon Chime Business Calling.

```
{  
  "SchemaVersion": "2.0",  
  "CdrId": "1a234567-89bc-01d2-3456-e78f9g01234h",  
  "ServiceCode": "AmazonChimeBusinessCalling",  
  "ChimeAccountId": "12a3456b-7c89-012d-3456-78901e23fg45",  
  "AwsAccountId": "111122223333",  
  "ConferenceId": "123a4567-b890-1234-5678-cd90efgh1234",  
  "ConferencePin": "XXXXXXXXXX",  
  "OrganizerUserId": "1ab2345c-67de-8901-f23g-45h678901j2k",  
  "OrganizerEmail": "jdoe@example.com",  
  
  "CallerPhoneNumber": "+12065550100",  
  "CallerCountry": "US",  
  
  "DestinationPhoneNumber": "+12065550101",
```

```
"DestinationCountry": "US",  
  
"ConferenceStartTimeEpochSeconds": "1556009595",  
"ConferenceEndTimeEpochSeconds": "1556009623",  
"StartTimeEpochSeconds": "1556009611",  
"EndTimeEpochSeconds": "1556009623",  
"BillableDurationSeconds": "24",  
"BillableDurationMinutes": ".4",  
"Direction": "Outbound"  
}
```

Configuración de salas de conferencias

Amazon Chime se puede integrar con el hardware de vídeo de la sala de Cisco, Tandberg, Polycom, Lifesize, Vidyó u otros fabricantes cuando se utiliza el protocolo SIP o H.323.

Para conectarse a Amazon Chime con un dispositivo VTC de la sala de conferencias compatible con SIP, introduzca una de las siguientes opciones:

- **@meet.chime.in**
- **u@meet.chime.in**
- ID de la reunión de 10 dígitos seguido de **@meet.chime.in**

meet.chime.in conecta el dispositivo de sala SIP a la región de Amazon Chime más cercana. Para conectarse a una región específica, utilice entradas DNS específicas de la región para los sistemas de sala SIP. Para obtener más información, consulte [Sistemas de sala SIP \(Protocolo de inicio de sesión\)](#).

Note

Si su dispositivo de sala SIP no admite TLS y requiere conectividad TCP, póngase en contacto con el soporte de AWS.

Si utiliza un dispositivo que solo admite H.323, debe marcar una de las siguientes opciones:

- **13.248.147.139**
- **76.223.18.152**

Si hay un firewall que filtra el tráfico entre el dispositivo VTC y Amazon Chime, abra los rangos para los protocolos que se utilizan. Para obtener más información, consulte [Requisitos de configuración de red y ancho de banda](#).

En la pantalla de bienvenida de Amazon Chime, introduzca el ID de la reunión de 10 o 13 dígitos para acceder. Puede encontrar el ID de la reunión de 13 dígitos en la aplicación web o el cliente de Amazon Chime, o elija la opción Acceso telefónico.

Cómo unirse a una reunión moderada

Si la reunión es moderada y es el organizador o el delegado, introduzca su ID de la reunión de 13 dígitos para unirse a la reunión como moderador. Si es moderador introduzca la clave de acceso de moderador en el teclado seguido de una almohadilla (#) para unirse y comenzar la reunión. Si no es organizador, delegado o moderador, se conecta a la reunión después de que un moderador se una y le dé comienzo.

Los moderadores tienen controles de organizador, lo que significa que pueden llevar a cabo otras acciones de la reunión. Estas acciones incluyen comenzar y detener la grabación, bloquear y desbloquear la reunión, silenciar al resto de asistentes y finalizar la reunión. Para obtener más información, consulte [Acciones del moderador con un sistema de telefonía o vídeo dentro de la sala](#) en la Guía del usuario de Amazon Chime.

Note

Si utiliza Alexa for Business para unirse a sus reuniones de Amazon Chime, puede unirse solo como moderador si su dispositivo está conectado a un sistema de vídeo dentro de la sala y realiza una llamada telefónica utilizando el teclado del dispositivo.

Dispositivos VTC compatibles

La siguiente tabla es un subconjunto de la lista de dispositivos VTC compatibles.

Dispositivo	SIP	H.323	Comentario
Cisco SX20	Sí	Sí	Audio/Vídeo/Pantalla: hacia y desde el dispositivo
Cisco DX80	Sí	Sí	Audio/Vídeo/Pantalla: hacia y desde el dispositivo
Icono Lifesize	Sí	No	Audio/Vídeo/Pantalla: hacia y desde el dispositivo

Dispositivo	SIP	H.323	Comentario
Polycom Debut	Sí	Sí	Audio/Vídeo/Pantalla: hacia y desde el dispositivo
Polycom RealPresence Desktop	No	Sí	Audio/Vídeo: Sí, Pantalla: desde el dispositivo
Polycom Trio	Sí	Sí	Audio/Vídeo/Pantalla: hacia y desde el dispositivo
Tandberg C40	Sí	Sí	Audio/Vídeo/Pantalla: hacia y desde el dispositivo

Requisitos de configuración de red y ancho de banda

Amazon Chime requiere los destinos y puertos que se describen en este tema para admitir varios servicios. Si el tráfico entrante o saliente está bloqueado, este bloqueo podría afectar a la capacidad de utilizar determinados servicios, como audio, vídeo, pantalla compartida o chat.

Amazon Chime utiliza Amazon Elastic Compute Cloud (Amazon EC2) y otros servicios de AWS en el puerto TCP/443. Si el firewall bloquea el puerto TCP/443, debe incluir *.amazonaws.com en una lista de elementos permitidos o incluir los [intervalos de direcciones IP de AWS](#) que se indican en la Referencia general de AWS en los siguientes servicios:

- Amazon EC2
- Amazon CloudFront
- Amazon Route 53

Amplíe las siguientes secciones para obtener más información sobre los destinos, los puertos y el ancho de banda.

Destinos y puertos obligatorios

Los siguientes destinos y puertos son necesarios para ejecutar Amazon Chime.

Destino	Puertos
chime.aws	TCP/443
*.chime.aws	TCP/443
*.amazonaws.com	TCP/443
99.77.128.0/18	TCP/443

Puerto de reuniones y telefonía

Amazon Chime utiliza el siguiente puerto y destino para las reuniones y Amazon Chime Business Calling.

Destino	Puerto
99.77.128.0/18	UDP/3478

Sistemas de sala H.323

Amazon Chime utiliza los siguientes destinos y puertos para los sistemas de vídeo en sala H.323.

Destino	Puertos
13.248.147.139	TCP/1720
76.223.18.152	TCP/1720
99.77.128.0/18	TCP/5100:6200
34.212.95.128/25	UDP/5100:6200
34.223.21.0/25	
52.55.62.128/25	
52.55.63.0/25	

Sistemas de sala SIP (Protocolo de inicio de sesión)

Se recomiendan los siguientes destinos y puertos al ejecutar Amazon Chime para los sistemas de vídeo en sala del SIP en su entorno.

AWS Región	Destino	Puertos
Global (región más cercana)	99.77.128.0/18	UDP/10000:60000
	34.212.95.128/25	
	34.223.21.0/25	
	52.55.62.128/25	

AWS Región	Destino	Puertos
	52.55.63.0/25	
Global	meet.chime.in 13.248.147.139 76.223.18.152	TCP/5061
Este de EE. UU. (Norte de Virginia)	meet.ue1.chime.in	TCP/5061
Oeste de EE. UU. (Oregón)	meet.uw2.chime.in	TCP/5061
Asia-Pacífico (Singapur)	meet.as1.chime.in	TCP/5061
Asia-Pacífico (Sídney)	meet.as2.chime.in	TCP/5061
Asia-Pacífico (Tokio)	meet.an1.chime.in	TCP/5061
Europa (Irlanda)	meet.ew1.chime.in	TCP/5061
América del Sur (São Paulo)	meet.se1.chime.in	TCP/5061

Requisitos de ancho de banda

Amazon Chime tiene los siguientes requisitos de ancho de banda para compartir audio, vídeo y pantalla:

- Audio
 - Llamada 1:1: 54 kbps ascendentes y descendentes
 - Llamada entre varios usuarios: no más de 32 kbps descendentes adicionales para 50 remitentes
- Vídeo
 - Llamada 1:1: 650 kbps ascendentes y descendentes
 - Modo HD: 1 400 kbps ascendentes y descendentes
 - 3–4 personas: 450 kbps ascendentes y $(N-1)*400$ kbps descendentes
 - 5–16 personas: 184 kbps ascendentes y $(N-1)*134$ kbps descendentes

- El ancho de banda ascendente y descendente se reduce en función de las condiciones de red
- Uso compartido de pantalla
 - 1,2 mbps ascendentes (presentación) y descendentes (visualización) para alta calidad. Esto puede reducirse hasta 320 kbps en función de las condiciones de red.
 - Control remoto: 800 kbps fijos

Visualización de informes

Con el fin de tomar decisiones más fundamentadas y aumentar la productividad en la organización, puede tener acceso a datos de uso y de comentarios directamente desde la consola. Los datos de los informes se actualizan a diario, aunque es posible que haya un retraso de hasta 48 horas.

Para ver los informes de uso y de comentarios

1. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
2. Elija Reports (Informes), Dashboard (Panel).
3. En la página Usage and feedback dashboard report (Informe del panel de uso y de comentarios), consulte los siguientes datos:

Note

Para obtener más información acerca de los datos disponibles, consulte el artículo sobre el [panel de informes de Amazon Chime y los detalles de la actividad de los usuarios](#).

- Rango de fechas (UTC): el rango de fechas del informe.
- Usuarios registrados: el número de usuarios que se han inscrito en Amazon Chime.
- Usuarios activos: el número de usuarios que han asistido a una reunión o enviado un mensaje con Amazon Chime.
- Reuniones celebradas: el número total de reuniones que han finalizado. Puede seleccionar una reunión específica para ver más detalles, como el ID de conferencia, la hora de inicio, el tipo, el organizador, la duración y el número de asistentes. Elija unos valores de Conference ID (ID de conferencia) o Meeting organizer (Organizador de la reunión) específicos para ver detalles adicionales, como los asistentes, los eventos de la lista de asistentes de la reunión, el tipo de cliente y los comentarios sobre la reunión.
- Satisfacción de los participantes: el porcentaje de respuestas positivas obtenidas en las encuestas posteriores a las reuniones.
- Mensajes de chat enviados: el número de mensajes de chat enviados por los usuarios.

Ampliación del cliente de escritorio de Amazon Chime

Puede ampliar las capacidades del cliente de escritorio de Amazon Chime añadiendo chatbots, sesiones de teléfono de proxy y webhooks. Los chatbots permiten a los usuarios realizar tareas como consultar información en los sistemas internos. Las sesiones telefónicas de proxy permiten a los usuarios llamar y enviar mensajes de texto sin revelar sus números de teléfono. Los webhooks pueden enviar mensajes automáticamente a salas de chat. Por ejemplo, un webhook puede enviar recordatorios de reuniones a un equipo, junto con un enlace a la reunión.

Temas

- [Administración de usuarios](#)
- [Integración de chatbots en el cliente de escritorio de Amazon Chime](#)
- [Sesiones de teléfono de proxy](#)
- [Creación de webhooks para Amazon Chime](#)

Administración de usuarios

Los siguientes fragmentos de código pueden ayudarle a administrar los usuarios de Amazon Chime. Todos los ejemplos de este tema utilizan Java.

Temas

- [Invitar a varios usuarios](#)
- [Descarga de la lista de usuarios](#)
- [Cierre de varias sesiones](#)
- [Actualización de los PIN personales de los usuarios](#)

Invitar a varios usuarios

El siguiente ejemplo muestra cómo invitar a varios usuarios a una cuenta de Team Amazon Chime.

```
List<String> emails = new ArrayList<>();
emails.add("janedoe@example.com");
emails.add("richardroe@example.net");
InviteUsersRequest inviteUsersRequest = new InviteUsersRequest()
```

```
.withAccountId("chimeAccountId")
.withUserEmailList(emails);

chime.inviteUsers(inviteUsersRequest);
```

Descarga de la lista de usuarios

El siguiente ejemplo muestra cómo descargar una lista de usuarios asociados a su cuenta administrativa de Amazon Chime en formato `.csv`.

```
BufferedWriter writer = Files.newBufferedWriter(Paths.get("/path/to/csv"));
CSVPrinter printer = new CSVPrinter(writer, CSVFormat.DEFAULT.withHeader("userId",
"email"));

ListUsersRequest listUsersRequest = new ListUsersRequest()
    .withAccountId(accountId)
    .withMaxResults(1);

boolean done = false;
while (!done) {
    ListUsersResult listUsersResult = chime.listUsers(listUsersRequest);
    for (User user: listUsersResult.getUsers()) {
        printer.printRecord(user.getUserId(), user.getPrimaryEmail());
    }

    if (listUsersResult.getNextToken() == null) {
        done = true;
    }

    listUsersRequest = new ListUsersRequest()
        .withAccountId(accountId)
        .withNextToken(listUsersResult.getNextToken());
}

printer.close();
```

Cierre de varias sesiones

El siguiente ejemplo muestra cómo la cerrar sesión de varios usuarios de su cuenta administrativa de Amazon Chime.

```
ListUsersRequest listUsersRequest = new ListUsersRequest()
```

```
.withAccountId("chimeAccountId");
ListUsersResult listUsersResult = chime.listUsers(listUsersRequest);

for (User user: listUsersResult.getUsers()) {
    LogoutUserRequest logoutUserRequest = new LogoutUserRequest()
        .withAccountId(user.getAccountId())
        .withUserId(user.getUserId());

    chime.logoutUser(logoutUserRequest);
}
```

Actualización de los PIN personales de los usuarios

El siguiente ejemplo muestra cómo restablecer el PIN de reunión personal de un usuario especificado de Amazon Chime.

```
ResetPersonalPINRequest request = new ResetPersonalPINRequest()
    .withAccountId("chimeAccountId")
    .withUserId("userId");

ResetPersonalPINResult result = chime.resetPersonalPIN(request);

User user = result.getUser();
user.getPersonalPIN()
```

Integración de chatbots en el cliente de escritorio de Amazon Chime

Puede usar AWS Command Line Interface (AWS CLI), la API de Amazon Chime o el SDK de AWS para integrar los chatbots con Amazon Chime. Con los chatbots, puede utilizar la eficacia de Amazon Lex, AWS Lambda y otros servicios de AWS para optimizar tareas comunes con interfaces de conversación inteligentes a las que puedan acceder los usuarios en las salas de chat de Amazon Chime.

Si es administrador de una cuenta corporativa de Amazon Chime, puede usar los chatbots para permitir a los usuarios realizar tareas como:

- Consulta de sistemas internos para obtener información.
- Automatización de tareas.

- Recepción de notificaciones para problemas críticos.
- Creación de tickets de soporte.

Para obtener más información sobre las cuentas corporativas de Amazon Chime, consulte [Administración de las cuentas de Amazon Chime](#).

Si administra una cuenta corporativa de Amazon Chime, puede crear hasta 10 chatbots para integrarlos con Amazon Chime. Los chatbots solo se pueden utilizar en salas de chat creadas por miembros de su cuenta. Solo los administradores de salas de chat pueden añadir chatbots a una sala de chat. Después de añadir un chatbot a una sala de chat, los miembros de la sala de chat pueden interactuar con el bot utilizando comandos proporcionados por el creador del bot. Para obtener más información, consulte la siguiente sección de este tema.

Los usuarios de Linux y macOS pueden crear un chatbot personalizado de muestra. Para obtener más información, consulte [Creación de chatbots personalizados para Amazon Chime](#).

Contenidos

- [Usar chatbots con Amazon Chime](#)
- [Eventos de Amazon Chime enviados a los chatbots](#)

Usar chatbots con Amazon Chime

Si administra una cuenta corporativa de Amazon Chime, puede crear hasta 10 chatbots para integrarlos con Amazon Chime. Los chatbots solo se pueden utilizar en salas de chat creadas por miembros de su cuenta. Solo los administradores de salas de chat pueden añadir chatbots a una sala de chat. Después de añadir un chatbot a una sala de chat, los miembros de la sala de chat pueden interactuar con el bot utilizando comandos proporcionados por el creador del bot. Para obtener más información, consulte [Uso de chatbots](#) en la Guía del usuario de Amazon Chime.

También puede utilizar la API de Amazon Chime para habilitar o detener los chatbots en su cuenta de Amazon Chime. Para obtener más información, consulte [Actualización de los chatbots](#).

Note

No puede eliminar los chatbots. Para detener el uso de un chatbot en su cuenta, utilice la operación de la API [UpdateBot](#) de Amazon Chime en la Referencia de la API de Amazon Chime. Cuando detiene chatbot, los administradores de salas de chat pueden eliminarlo de

una sala de chat, pero no pueden añadirlo a ella. Los usuarios que @mencionan un chatbot detenido en una sala de chat reciben un mensaje de error.

Requisitos previos

Antes de iniciar el procedimiento de integración de los chatbots con Amazon Chime, complete los siguientes requisitos previos:

- Cree un chatbot.
- Cree el punto de conexión saliente para Amazon Chime para enviar eventos al bot. Elija desde un ARN de función de AWS Lambda o un punto de enlace HTTPS. Para obtener más información acerca de Lambda, consulte la [Guía para desarrolladores de AWS Lambda](#).

Prácticas recomendadas de DNS para puntos de conexión HTTPS

Se aconsejan las siguientes prácticas recomendadas al asignar DNS para su punto de enlace HTTPS:

- Utilice un subdominio de DNS que esté dedicado al punto de enlace del bot.
- Utilice únicamente registros A para apuntar al punto de enlace del bot.
- Proteja sus servidores DNS y la cuenta del registrador DNS para evitar la apropiación del dominio.
- Utilice certificados intermedios TLS válidos públicamente dedicados para el punto de enlace del bot.
- Verifique criptográficamente la firma de mensajes del bot antes de actuar en un mensaje de bot.

Tras crear el chatbot, utilice AWS Command Line Interface (AWS CLI) o la operación de la API de Amazon Chime para completar las tareas que se describen en las siguientes secciones.

Tareas

- [Paso 1: Integrar un chatbot con Amazon Chime](#)
- [Paso 2: Configurar el punto de conexión de salida de un chatbot de Amazon Chime](#)
- [Paso 3: Añadir el chatbot a una sala de chat de Amazon Chime](#)
- [Autenticación de solicitudes de chatbots](#)
- [Actualización de los chatbots](#)

Paso 1: Integrar un chatbot con Amazon Chime

Tras completar los [requisitos previos](#), integre el chatbot con Amazon Chime mediante AWS CLI o la API de Amazon Chime.

Note

Estos procedimientos crean un nombre y una dirección de correo electrónico para su chatbot. Los nombres y las direcciones de correo electrónico de los chatbots no se pueden cambiar una vez creados.

AWS CLI

Para integrar un chatbot mediante AWS CLI

1. Para integrar su chatbot con Amazon Chime, utilice el comando `create-bot` de AWS CLI.

```
aws chime create-bot --account-id 12a3456b-7c89-012d-3456-78901e23fg45 --display-name exampleBot --domain example.com
```

- a. Escriba un nombre de visualización para el chatbot de hasta 55 caracteres alfanuméricos o caracteres especiales (como, por ejemplo, +, -, %).
 - b. Escriba el nombre de dominio registrado para su cuenta corporativa de Amazon Chime.
2. Amazon Chime devuelve una respuesta que incluye el ID del bot.

```
"Bot": {  
  "CreatedTimestamp": "timeStamp",  
  "DisplayName": "exampleBot",  
  "Disabled": exampleBotFlag,  
  "UserId": "1ab2345c-67de-8901-f23g-45h678901j2k",  
  "BotId": "botId",  
  "UpdatedTimestamp": "timeStamp",  
  "BotType": "ChatBot",  
  "SecurityToken": "securityToken",  
  "BotEmail": "displayName-chimebot@example.com"  
}
```

3. Copie y guarde el ID y la dirección de correo electrónico del bot para utilizarlos en los siguientes procedimientos.

API de Amazon Chime

Para integrar un chatbot mediante la API de Amazon Chime

1. Para integrar su chatbot con Amazon Chime, utilice la operación de API [CreateBot](#) en la Referencia de la API de Amazon Chime.
 - a. Escriba un nombre de visualización para el chatbot de hasta 55 caracteres alfanuméricos o caracteres especiales (como, por ejemplo, +, -, %).
 - b. Escriba el nombre de dominio registrado para su cuenta corporativa de Amazon Chime.
2. Amazon Chime devuelve una respuesta que incluye el ID del bot. Copie y guarde el ID y la dirección de correo electrónico del bot. La dirección de correo electrónico del bot tiene este formato: *exampleBot-chimebot@example.com*.

SDK de AWS para Java

En el siguiente código de ejemplo, se muestra cómo integrar un chatbot mediante el SDK de AWS para Java.

```
CreateBotRequest createBotRequest = new CreateBotRequest()
    .withAccountId("chimeAccountId")
    .withDisplayName("exampleBot")
    .withDomain("example.com");

chime.createBot(createBotRequest);
```

Amazon Chime devuelve una respuesta que incluye el ID del bot. Copie y guarde el ID y la dirección de correo electrónico del bot. La dirección de correo electrónico del bot tiene este formato: *exampleBot-chimebot@example.com*.

Paso 2: Configurar el punto de conexión de salida de un chatbot de Amazon Chime

Después de crear un ID de chatbot para su cuenta corporativa de Amazon Chime, configure el punto de conexión de salida para que Amazon Chime lo utilice para enviar mensajes a su bot. El punto de conexión de salida puede ser un ARN de función de AWS Lambda o un punto de conexión HTTPS

que haya creado como parte de los [requisitos previos](#). Para obtener más información acerca de Lambda, consulte la [Guía para desarrolladores de AWS Lambda](#).

Note

Si el punto de conexión HTTPS de salida para su bot no está configurado o está vacío, los administradores de salas de chat no pueden añadir el bot a una sala de chat. Además, los usuarios de la sala de chat no pueden interactuar con el bot.

AWS CLI

Para configurar un punto de conexión de salida para su chatbot, utilice el comando `put-events-configuration` de AWS CLI. Configure un ARN de función de Lambda o un punto de conexión HTTPS de salida.

Lambda ARN

```
aws chime put-events-configuration --account-id 12a3456b-7c89-012d-3456-78901e23fg45
--bot-id botId --lambda-function-arn arn:aws:lambda:us-east-1:111122223333:function:function-name
```

HTTPS endpoint

```
aws chime put-events-configuration --account-id 12a3456b-7c89-012d-3456-78901e23fg45
--bot-id botId --outbound-events-https-endpoint https://example.com:8000
```

Amazon Chime responde con el ID del bot y el punto de conexión HTTPS.

```
{
  "EventsConfiguration": {
    "BotId": "BotId",
    "OutboundEventsHTTPEndpoint": "https://example.com:8000"
  }
}
```

API de Amazon Chime

Para configurar el punto de conexión de salida del chatbot, utilice la operación de la API [PutEventsConfiguration](#) de Amazon Chime en la Referencia de la API de Amazon Chime. Configure el ARN de una función de Lambda o un punto de conexión HTTPS de salida.

- Si configura el ARN de una función de Lambda, Amazon Chime llama a Lambda para añadir un permiso que permita a la cuenta de AWS del administrador de Amazon Chime invocar el ARN de función de Lambda proporcionado. Esto va seguido de una invocación de simulacro para verificar que Amazon Chime tenga permiso para invocar la función. Si la adición de permisos o la invocación de simulacro devuelven un error, la solicitud `PutEventsConfiguration` devuelve un error HTTP 4xx.
- Si configura un punto de conexión HTTPS de salida, Amazon Chime verifica su punto de conexión enviando una solicitud HTTP Post con una carga útil Challenge JSON al punto de conexión HTTPS de salida que proporcionó en el paso anterior. El punto de enlace HTTPS saliente debe responder devolviendo el parámetro Challenge en formato JSON. Los siguientes ejemplos muestran la solicitud y una respuesta válida.

Request

```
HTTPS POST

JSON Payload:
{
  "Challenge": "00000000000000000000",
  "EventType" : "HTTPSEndpointVerification"
}
```

Response

```
HTTP/1.1 200 OK
Content-type: application/json

{
  "Challenge": "00000000000000000000"
}
```

Si el enlace por desafío mutuo devuelve un error, entonces la solicitud `PutEventsConfiguration` devuelve un error HTTP 4xx.

SDK de AWS para Java

En el siguiente código de ejemplo, se muestra cómo configurar un punto de conexión mediante el SDK de AWS para Java.

```
PutEventsConfigurationRequest putEventsConfigurationRequest = new
PutEventsConfigurationRequest()
    .withAccountId("chimeAccountId")
    .withBotId("botId")
    .withOutboundEventsHTTPSEndpoint("https://www.example.com")
    .withLambdaFunctionArn("arn:aws:lambda:region:account-id:function:function-name");

chime.putEventsConfiguration(putEventsConfigurationRequest);
```

Paso 3: Añadir el chatbot a una sala de chat de Amazon Chime

Solo un administrador de salas de chat puede añadir un chatbot a una sala de chat. Para ello, usa la dirección de correo electrónico del chatbot creada en el [paso 1](#).

Para agregar un chatbot a una sala de chat

1. Abra su cliente de escritorio o la aplicación web de Amazon Chime.
2. Elija el icono de engranaje de la esquina superior derecha y elija Administrar webhooks y bots.
3. Seleccione Add bot (Añadir bot).
4. En Dirección de correo electrónico, escriba la dirección de correo electrónico del bot.
5. Elija Add (Agregar).

El nombre del bot aparece en la lista de salas de chat. Si es necesario realizar acciones adicionales para añadir un chatbot a una sala de chat, indíquelas al administrador de la sala de chat.

Después de añadir el chatbot a la sala de chat, proporciona los comandos del chatbot a los usuarios de la sala de chat. Una forma de hacerlo es programar el chatbot para enviar ayuda de comandos a la sala de chat donde recibe la invitación de sala de chat. AWS también recomienda la creación de un comando de ayuda para que lo utilicen los usuarios de chatbots.

Autenticación de solicitudes de chatbots

Puede autenticar las solicitudes enviadas a su chatbot desde una sala de chat de Amazon Chime. Para ello, calcule una firma en función de la solicitud. A continuación, valide que la firma calculada coincida con la del encabezado de la solicitud. Amazon Chime utiliza el hash HMAC SHA256 para generar la firma.

Si el chatbot está configurado para Amazon Chime usando un punto de conexión HTTPS de salida, siga los pasos de autenticación que se muestran a continuación.

Para validar una solicitud firmada desde Amazon Chime para un chatbot con un punto de conexión HTTPS de salida configurado

1. Obtenga el encabezado Chime-Signature (Firma de Chime) desde la solicitud HTTP.
2. Obtenga el encabezado Chime-Request-Timestamp (Marca temporal de solicitud de Chime) y el body (cuerpo) de la solicitud. A continuación, utilice una barra vertical como delimitador entre los dos elementos para formar una cadena.
3. Utilice el SecurityToken de la respuesta de CreateBot como clave inicial de HMAC_SHA_256 y aplique hash a la cadena que creó en el paso 2.
4. Cifre el byte con hash con codificador Base64 a una cadena de firma.
5. Compare esta firma calculada con la del encabezado Chime-Signature (Firma de Chime).

El siguiente ejemplo de código muestra cómo generar una firma utilizando Java.

```
private final String DELIMITER = "|";
private final String HMAC_SHA_256 = "HmacSHA256";

private String generateSignature(String securityToken, String requestTime,
String requestBody)
{
    try {
        final Mac mac = Mac.getInstance(HMAC_SHA_256);
        SecretKeySpec key = new SecretKeySpec(securityToken.getBytes(UTF_8),
HMAC_SHA_256);
        mac.init(key);
        String data = requestTime + DELIMITER + requestBody;
        byte[] rawHmac = mac.doFinal(data.getBytes(UTF_8));
```

```
        return Base64.getEncoder().encodeToString(rawHmac);
    }
    catch (Exception e) {
        throw e;
    }
}
```

El punto de conexión HTTPS de salida debe responder a la solicitud de Amazon Chime con 200 OK en el plazo de 2 segundos. De lo contrario, la solicitud devuelve un error. Si el punto de conexión HTTPS de salida no está disponible pasados 2 segundos, debido posiblemente a que se ha agotado el tiempo de espera de lectura o conexión, o si Amazon Chime recibe un código de respuesta 5xx, Amazon Chime reintenta la solicitud 2 veces. El primer reintento se envía 200 milisegundos después de que la solicitud inicial devuelva un error. El segundo reintento se envía 400 milisegundos después de que el reintento anterior devuelva un error. Si el punto de enlace HTTPS saliente sigue sin estar disponible después del segundo reintento, la solicitud devuelve un error.

Note

La Chime-Request-Timestamp (Marca temporal de solicitud de Chime) cambia cada vez que se vuelve a enviar la solicitud.

Si el chatbot se configura para Amazon Chime utilizando un ARN de función de Lambda, siga los pasos de autenticación siguientes.

Para validar una solicitud firmada de Amazon Chime para un chatbot con un ARN de función de Lambda configurado

1. Obtenga Chime-Signature y Chime-Request-Timestamp desde la solicitud ClientContext de Lambda, en formato JSON cifrado en Base64.

```
{
  "Chime-Signature" : "1234567890",
  "Chime-Request-Timestamp" : "2019-04-04T21:30:43.181Z"
}
```

2. Obtenga el body (cuerpo) de la solicitud a partir de la carga de la solicitud.
3. Utilice el SecurityToken de la respuesta de CreateBot como clave inicial de HMAC_SHA_256 y aplique hash a la cadena que ha creado.

4. Cifre el byte con hash con codificador Base64 a una cadena de firma.
5. Compare esta firma calculada con la del encabezado Chime-Signature (Firma de Chime).

Si se produce una `com.amazonaws.SdkClientException` durante la invocación a Lambda, Amazon Chime vuelve a intentar la solicitud dos veces.

Actualización de los chatbots

Como administrador de la cuenta de Amazon Chime, puede usar la API de Amazon Chime con el SDK de AWS o AWS CLI para ver los detalles de su chatbot. También puede activar o impedir el uso de sus chatbots en su cuenta. También tiene la opción de volver a generar tokens de seguridad para su chatbot.

Para obtener más información, consulte los siguientes temas en la Referencia de la API de Amazon Chime:

- [GetBot](#): obtiene los detalles de su chatbot, como la dirección de correo electrónico y el tipo de bot.
- [UpdateBot](#): activa o impide el uso de un chatbot en su cuenta.
- [RegenerateSecurityToken](#): vuelve a generar el token de seguridad de su chatbot.

También puede optar por cambiar `PutEventsConfiguration` para el chatbot. Por ejemplo, si el chatbot se configuró inicialmente para utilizar un punto de conexión HTTPS de salida, puede eliminar la configuración de eventos anterior y colocar una nueva configuración de eventos para un ARN de función de Lambda.

Para obtener más información, consulte los siguientes temas en la Referencia de la API de Amazon Chime:

- [DeleteEventsConfiguration](#)
- [PutEventsConfiguration](#)

Eventos de Amazon Chime enviados a los chatbots

Los eventos siguientes se envían a su chatbot desde Amazon Chime:

- Invitación: se envía cuando se agrega el chatbot a una sala de chat de Amazon Chime.
- Mención: se envía cuando un usuario de una sala de chat @menciona el chatbot.

- Eliminación: se envía cuando se elimina el chatbot de una sala de chat de Amazon Chime.

Los siguientes ejemplos muestran la carga JSON enviada a su chatbot para cada uno de estos eventos.

Example de evento de invitación

```
{
  "Sender": {
    "SenderId": "user@example.com",
    "SenderIdType": "EmailId"
  },
  "Discussion": {
    "DiscussionId": "abcdef12-g34h-56i7-j8kl-mn9opqr012st",
    "DiscussionType": "Room"
  },
  "EventType": "Invite",
  "InboundHttpsEndpoint": {
    "EndpointType": "Persistent",
    "Url": "https://
hooks.a.chime.aws/incomingwebhooks/a1b2c34d-5678-90e1-f23g-h45i67j8901k?
token=ABCDEFGHIJK1LMnoP2Q3RST4uvwxyzYzAbC56DeFghIJKLM7N8OP9QRsTuV0WXYZABcdefghiJ"
  },
  "EventTimestamp": "2019-04-04T21:27:52.736Z"
}
```

Example de evento de mención

```
{
  "Sender": {
    "SenderId": "user@example.com",
    "SenderIdType": "EmailId"
  },
  "Discussion": {
    "DiscussionId": "abcdef12-g34h-56i7-j8kl-mn9opqr012st",
    "DiscussionType": "Room"
  },
  "EventType": "Mention",
  "InboundHttpsEndpoint": {
```

```

        "EndpointType": "ShortLived",
        "Url": "https://
hooks.a.chime.aws/incomingwebhooks/a1b2c34d-5678-90e1-f23g-h45i67j8901k?
token=ABCDefGHiJK1LMnoP2Q3RST4uvwxyZAbC56DeFghIJKLM7N8OP9QRsTuV0WXYZABcdefgHiJ"
    },
    "EventTimestamp": "2019-04-04T21:30:43.181Z",
    "Message": "@botDisplayName@example.com Hello Chatbot"
}

```

Note

La dirección URL `InboundHttpsEndpoint` para un evento `Mention` vence 2 minutos después de enviarse.

Example de evento de eliminación

```

{
  "Sender": {
    "SenderId": "user@example.com",
    "SenderIdType": "EmailId"
  },
  "Discussion": {
    "DiscussionId": "abcdef12-g34h-56i7-j8kl-mn9opqr012st",
    "DiscussionType": "Room"
  },
  "EventType": "Remove",
  "EventTimestamp": "2019-04-04T21:27:29.626Z"
}

```

Sesiones de teléfono de proxy

Puede usar AWS Command Line Interface (AWS CLI), la API de Amazon Chime o el SDK de AWS para crear sesiones de teléfono de proxy para usarlas con las instancias de Amazon Chime Voice Connector. Las sesiones de teléfono de proxy permiten a los participantes llamarse o enviarse mensajes de texto sin revelar números de teléfono privados.

La creación de sesiones telefónicas de proxy requiere lo siguiente:

- La capacidad de programar.
- Una cuenta de AWS.
- Un rol de AWS Identity and Access Management (IAM) que otorga permiso para acceder a las acciones de la API Amazon Chime que se utilizan para crear sesiones de teléfono proxy, como las siguientes:
 - `chime:CreateProxySession`
 - `chime>DeleteProxySession`
 - `chime>DeleteVoiceConnectorProxy`
 - `chime:GetProxySession`
 - `chime:GetVoiceConnectorProxy`
 - `chime:ListProxySessions`
 - `chime:PutVoiceConnectorProxy`
 - `chime:UpdateProxySession`

Para obtener más información, consulte las [políticas basadas en identidad de Amazon Chime](#).

- Una instancia de Amazon Chime Voice Connector creada por un administrador de cuentas de Amazon Chime. Para obtener más información, consulte [Administración de las instancias de Amazon Chime Voice Connector](#).

El siguiente procedimiento demuestra cómo crear una sesión de teléfono de proxy.

Para crear una sesión de teléfono de proxy

1. Utilice la acción [PutVoiceConnectorProxy](#) en la Referencia de la API de Amazon Chime para configurar la instancia de Amazon Chime Voice Connector para la sesión de teléfono de proxy.
2. Utilice la acción [CreateProxySession](#) en la Referencia de la API de Amazon Chime para crear la sesión de teléfono de proxy.

Para obtener más información sobre las acciones de la API de Amazon Chime disponibles para las sesiones de teléfono de proxy, consulte la [Referencia de la API de Amazon Chime](#).

Creación de webhooks para Amazon Chime

Los webhooks permiten que las aplicaciones web se comuniquen entre sí en tiempo real. Por lo general, los webhooks envían notificaciones cuando se produce una acción. Por ejemplo,

supongamos que gestiona un sitio de compras en línea. Webhooks puede avisarle cuando un cliente añada artículos a un carrito de compras, pague un pedido o envíe un comentario. Los webhooks no necesitan tanta programación como las aplicaciones tradicionales y no utilizan tanta potencia de procesamiento. Sin un webhook, un programa tiene que buscar datos con frecuencia para poder obtenerlos en tiempo real. Con un webhook, la aplicación de envío publica los datos inmediatamente.

Los webhooks entrantes que cree pueden enviar mensajes mediante programación a salas de chat de Amazon Chime. Por ejemplo, un webhook puede notificar a un equipo de atención al cliente la creación de una nueva incidencia de alta prioridad y añadir un enlace a la incidencia en la sala de chat.

Puede aplicar formato a los mensajes de los webhooks mediante el marcado e incluir emojis. Los enlaces de HTTP y las direcciones de correo electrónico se representan como enlaces en los que puede hacer clic. Los mensajes también pueden incluir anotaciones @All y @Present para alertar a todos los miembros y a los miembros presentes de una sala de chat, respectivamente. Para @mencionar directamente a un asistente de una sala de chat, use su alias o su dirección de correo electrónico completa. Por ejemplo, @alias o @alias@domain.com.

Los webhooks solo pueden formar parte de una sala de chat y no se pueden compartir. Los administradores de salas de chat de Amazon Chime pueden añadir hasta 10 webhooks para cada sala de chat.

Después de crear un webhook, podrá integrarlo en una sala de chat de Amazon Chime, tal como se muestra en el siguiente procedimiento.

Para integrar un webhook en una sala de chat

1. Obtenga la URL del webhook del administrador de la sala de chat. Para obtener más información, consulte [Añadir webhooks a una sala de chat](#) en la Guía del usuario de Amazon Chime.
2. Use la URL del webhook del script o la aplicación que creó para enviar mensajes a la sala de chat:
 - a. La URL acepta una solicitud HTTP POST.
 - b. Los webhooks de Amazon Chime aceptan una carga JSON con una única clave Contenido. A continuación se muestra un ejemplo de comando Curl con una carga de muestra:

```
curl -X POST "<Insert your webhook URL here>" -H "Content-Type:application/json" --data '{"Content":"Message Body emoji test: :) :+1: link test: http://
```

```
sample.com email test: marymajor@example.com All member callout: @All All  
Present member callout: @Present"}'
```

A continuación, se muestra un comando de PowerShell de ejemplo para usuarios de Windows:

```
Invoke-WebRequest -Uri '<Insert your webhook URL here>' -Method 'Post' -  
ContentType 'application/JSON' -Body '{"Content":"Message Body emoji test: :) :  
+1: link test: http://sample.com email test: marymajor@example.com All member  
callout: @All All Present member callout: @Present"}'
```

Una vez que el programa externo envía la solicitud HTTP POST a la URL del webhook, el servidor confirma que el webhook es válido y que tiene asignada una sala de chat. El webhook aparece en la lista de la sala de chat con un icono de webhook junto a su nombre. Los mensajes de la sala de chat enviados por el webhook aparecen en la sala de chat con el nombre del webhook seguido de (Webhook).

Note

CORS no está habilitado actualmente para los webhooks.

Solución de errores relacionados con los webhooks

A continuación se muestra una lista de los errores relacionados con los webhooks:

- El límite de frecuencia de webhook entrante para cada webhook es de 1 TPS por cada sala de chat. Si se produce una limitación controlada, se genera un error HTTP 429.
- Los mensajes publicadas por un webhook deben ser de 4 KB o menos. Si la carga del mensaje es más grande, se produce un error HTTP 413.
- Los mensajes publicados por un webhook con anotaciones @All y @Present solo funcionan en salas de chat con un máximo de 50 miembros. Si hay más de 50 miembros, se devuelve un error HTTP 400.
- Si la URL del webhook se regenera, cuando se utiliza la URL antigua se produce un error HTTP 404.
- Si se elimina el webhook en una sala, cuando se utiliza la URL antigua se produce un error HTTP 404.

- Las URL de webhook no válidas generan errores HTTP 403.
- Si el servicio no está disponible, el usuario recibe un error HTTP 503 en la respuesta.

Soporte administrativo de Amazon Chime

Note

Para obtener ayuda con tu cuenta de compras de Amazon, visita el [servicio de atención al cliente en amazon.com](#).

Si necesitas ponerte en contacto con el servicio de asistencia de Amazon Chime, elige una de las siguientes opciones:

- Si tiene una cuenta de AWS Support, vaya al [Support Center](#) y envíe un ticket.
- En caso contrario, abra la [AWS Management Console](#) y elija Amazon Chime Support Enviar solicitud.

Proporcione la mayor cantidad posible de la siguiente información:

- Una descripción detallada del problema.
- La hora a la que se produjo, incluida la zona horaria.
- Su versión de Amazon Chime. Cómo averiguar su número de versión:
 - En Windows, elija Ayuda, Acerca de Amazon Chime.
 - En MacOS, elija Amazon Chime, About Amazon Chime (Acerca de Amazon Chime).
 - En iOS y Android, elija Configuración, Acerca de.
- El ID de referencia del log. Cómo encontrar este ID:
 - En Windows y macOS, elija Help (Ayuda), Send Diagnostic Logs (Enviar logs de diagnóstico).
 - En iOS y Android, elija Configuración, Enviar logs de diagnóstico.
- Si el problema está relacionado con una reunión, el ID de la reunión.

Seguridad en Amazon Chime

La seguridad en la nube de AWS es la máxima prioridad. Como cliente de AWS, se beneficia de una arquitectura de red y un centro 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 los servicios de AWS en la nube de AWS. AWS también 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 AWS](#) . Para obtener información sobre los programas de conformidad que se aplican a Amazon Chime, consulte [Servicios de AWS en el ámbito del programa de conformidad](#).
- Seguridad en la nube: su responsabilidad viene determinada por el servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le permite comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Amazon Chime. En los siguientes temas, se mostrará cómo configurar Amazon Chime para satisfacer sus objetivos de seguridad y conformidad. También puede aprender a utilizar otros servicios de AWS que ayudan a monitorear y proteger los recursos de Amazon Chime.

Temas

- [Administración de identidades y accesos para Amazon Chime](#)
- [Cómo funciona Amazon Chime con IAM](#)
- [Prevención de la sustitución confusa entre servicios](#)
- [Políticas de Amazon Chime basadas en recursos](#)
- [Autorización basada en etiquetas de Amazon Chime](#)
- [Roles de IAM de Amazon Chime](#)
- [Ejemplos de políticas de Amazon Chime basadas en identidades](#)
- [Solución de problemas de identidad y acceso de Amazon Chime](#)
- [Uso de roles vinculados a servicios para Amazon Chime](#)

- [Registro y monitoreo en Amazon Chime](#)
- [Validación de la conformidad de Amazon Chime](#)
- [Resiliencia en Amazon Chime](#)
- [Seguridad de la infraestructura en Amazon Chime](#)
- [Descripción de las actualizaciones automáticas de Amazon Chime](#)

Administración de identidades y accesos para Amazon Chime

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los administradores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién se puede autenticar (iniciar sesión) y autorizar (tener permisos) para utilizar los recursos de Amazon Chime. IAM es un servicio de AWS que se puede utilizar sin cargo adicional.

Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración de acceso mediante políticas](#)

Público

La forma en que utilice AWS Identity and Access Management (IAM) varía, en función del trabajo que realice en Amazon Chime.

Usuario de servicio: si utiliza el servicio de Amazon Chime para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Amazon Chime 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 de Amazon Chime, consulte [Solución de problemas de identidad y acceso de Amazon Chime](#).

Administrador de servicio: si está a cargo de los recursos de Amazon Chime de su empresa, probablemente tenga acceso completo a Amazon Chime. El trabajo consiste en determinar a qué características y recursos de Amazon Chime deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM.

Para obtener más información acerca de cómo la empresa puede utilizar IAM con Amazon Chime, consulte [Cómo funciona Amazon Chime con IAM](#).

Administrador de IAM: si es un administrador de IAM, es posible que desee obtener información acerca de cómo escribir políticas para administrar el acceso a Amazon Chime. Para consultar ejemplos de políticas de Amazon Chime basadas en identidades que puede utilizar en IAM, consulte [Ejemplos de políticas de Amazon Chime basadas en identidades](#).

Autenticación con identidades

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

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

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

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

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

AWS Usuario raíz de la cuenta de

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

Usuarios y grupos de IAM

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

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

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

Roles de IAM

Un [rol de IAM](#) es una identidad de tu cuenta de AWS que dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente un rol de IAM en la AWS Management Console [cambiando de roles](#). Puede asumir un

rol llamando a una operación de AWS CLI o de la API de AWS, o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte [Uso de roles de IAM](#) en la Guía del Usuario de IAM.

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

- **Acceso de usuario federado:** para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte [Creación de un rol para un proveedor de identidades de terceros](#) en la Guía del Usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. El IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte [Conjuntos de permisos](#) en la Guía del usuario de AWS IAM Identity Center.
- **Permisos de usuario de IAM temporales:** un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- **Acceso entre cuentas:** puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. No obstante, con algunos Servicios de AWS se puede asociar 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 [Cómo los roles de IAM difieren de las políticas basadas en recursos](#) en la Guía del usuario de IAM.
- **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 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 a servicios.
- **Reenviar sesiones de acceso (FAS):** cuando utiliza un rol o un usuario de IAM 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. FAS utiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS 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 sobre las políticas a la hora de realizar solicitudes de FAS, consulte [Reenviar sesiones de acceso](#).

- Rol de servicio: un rol de servicio es un [rol de IAM](#) que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte [Creación de un rol para delegar permisos a un Servicio de AWS](#) en la Guía del usuario de IAM.
- 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 su Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- Aplicaciones que se ejecutan en Amazon EC2: puede utilizar un rol de IAM que le permita administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia de EC2 y realizan solicitudes a la AWS CLI o a la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar un rol de AWS a una instancia de EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia asociado a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para obtener más información, consulte [Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias de Amazon EC2](#) en la Guía del usuario de IAM.

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

Administración de acceso mediante políticas

Para controlar el acceso en AWS, se crean políticas y se adjuntan a identidades o recursos de AWS. 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 documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte [Información general de las políticas JSON](#) en la Guía del Usuario de IAM.

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

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

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

Políticas basadas en identidades

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

Las políticas basadas en identidad 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 administradas de AWS y las políticas administradas por el cliente. Para obtener más información sobre cómo elegir una política administrada o una política insertada, consulte [Elegir entre políticas administradas y políticas insertadas](#) en la Guía del usuario de IAM.

Políticas basadas en recursos

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

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

Políticas administradas por AWS para Amazon Chime

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

Los servicios de AWS mantienen y actualizan las políticas administradas de AWS. No puede cambiar los permisos en las políticas administradas de AWS. En ocasiones, los servicios agregan permisos adicionales a una política administrada de 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 de AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no quitan los permisos de una política administrada de AWS, por lo tanto, las actualizaciones de las políticas no deteriorarán los permisos existentes.

Además, AWS admite políticas administradas para funciones de trabajo que abarcan varios servicios. Por ejemplo, la política administrada de AWS de ReadOnlyAccess proporciona acceso de solo lectura a todos los servicios y recursos de AWS. 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 descripción de las políticas de funciones de trabajo, consulte [Políticas administradas de AWS para funciones de trabajo](#) en la Guía del usuario de IAM.

Listas de control de acceso (ACL)

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

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

Otros tipos de políticas

AWS admite otros tipos de políticas adicionales 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 en función de identidad puede conceder a una entidad de IAM (usuario o rol de IAM). 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 las entidades de IAM](#) en la Guía del Usuario de IAM.
- **Políticas de control de servicio (SCP):** las SCP son políticas de JSON que especifican los permisos máximos de una organización o una unidad organizativa en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de manera centralizada varias cuentas de AWS que posea su empresa. Si habilita todas las características en una empresa, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Una SCP limita los permisos para las entidades de las cuentas de miembros, incluido cada `rootlong`. Para más información sobre organizaciones y las SCP, consulte [Funcionamiento de las SCP](#) en la Guía del Usuario de AWS Organizations.
- **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 identidad del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte [Políticas de sesión](#) en la Guía del Usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para obtener información sobre cómo AWS decide si permite o no una solicitud cuando hay varios tipos de políticas implicados, consulte [Lógica de evaluación de políticas](#) en la Guía del usuario de IAM.

Cómo funciona Amazon Chime con IAM

Antes de utilizar IAM para administrar el acceso a Amazon Chime, debe conocer qué características de IAM están disponibles con Amazon Chime. Para obtener una perspectiva general sobre cómo

funcionan Amazon Chime y otros servicios de AWS con IAM, consulte [Servicios de AWS que funcionan con IAM](#) en la Guía del usuario de IAM.

Temas

- [Políticas de Amazon Chime basadas en identidades](#)
- [Recursos](#)
- [Ejemplos](#)

Políticas de Amazon Chime basadas en identidades

Con las políticas basadas en identidad de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Amazon Chime admite acciones, claves de condiciones y recursos específicos. Para obtener más información acerca de los elementos que utiliza en una política de JSON, consulte [Referencia de los elementos de las políticas de JSON de IAM](#) en la Guía del usuario de IAM.

Acciones

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

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

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

Claves de condición

Amazon Chime no proporciona ninguna clave de condición específica del servicio. Para ver todas las claves de condición globales de AWS, consulte [Claves de contexto de condición globales de AWS](#) en la Guía del usuario de IAM.

Recursos

Amazon Chime no permite especificar los ARN de los recursos en una política.

Ejemplos

Para ver ejemplos de políticas basadas en identidades de Amazon Chime, consulte [Ejemplos de políticas de Amazon Chime basadas en identidades](#).

Prevención de la sustitución confusa entre servicios

El problema del suplente confuso es un problema de seguridad que se produce cuando una entidad sin permiso para realizar una acción llama a una entidad con más privilegios para que la realice. Esto puede permitir que actores malintencionados ejecuten comandos o modifiquen recursos para los que, de otro modo, no tendrían permiso de ejecución ni acceso. Para obtener más información, consulte [El problema del suplente confuso](#) en la Guía del usuario de AWS Identity and Access Management.

En AWS, la suplantación entre servicios puede dar lugar a un caso de suplente confuso. 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). Un actor malintencionado puede utilizar el servicio de llamadas para alterar los recursos de otro servicio mediante permisos que normalmente no tendría.

AWS proporciona a las entidades principales del servicio acceso gestionado a los recursos de su cuenta para ayudarle a proteger la seguridad de sus recursos. Recomendamos utilizar las claves de contexto de condición global de `aws:SourceAccount` en sus políticas de recursos. Estas claves limitan los permisos que otorga Amazon Chime a otro servicio para el recurso.

En los siguientes ejemplos se muestra una política de buckets de S3 que usa las claves de contexto de condición global de `aws:SourceAccount` en el bucket de S3 de `CallDetailRecords` configurado para evitar el problema del suplente confuso.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonChimeAc1Check668426",
      "Effect": "Allow",
      "Principal": {
        "Service": "chime.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
```

```
    "Resource": "arn:aws:s3:::your-cdr-bucket"
  },
  {
    "Sid": "AmazonChimeWrite668426",
    "Effect": "Allow",
    "Principal": {
      "Service": "chime.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::your-cdr-bucket/*",
    "Condition": {
      "StringEquals": {
        "s3:x-amz-acl": "bucket-owner-full-control",
        "aws:SourceAccount": "112233446677"
      }
    }
  }
]
```

Políticas de Amazon Chime basadas en recursos

Amazon Chime no admite las políticas basadas en recursos.

Autorización basada en etiquetas de Amazon Chime

Amazon Chime no admite el etiquetado de recursos o el control de acceso basado en etiquetas.

Roles de IAM de Amazon Chime

Un [rol de IAM](#) es una entidad de la cuenta de AWS que dispone de permisos específicos.

Uso de credenciales temporales con Amazon Chime

Puede utilizar credenciales temporales para iniciar sesión con federación, asumir un rol de IAM o asumir un rol de acceso entre cuentas. Las credenciales de seguridad temporales se obtienen mediante una llamada a operaciones de la API de AWS STS, como [AssumeRole](#) o [GetFederationToken](#).

Amazon Chime admite el uso de credenciales temporales.

Roles vinculados al servicio

Los [roles vinculados a servicios](#) permiten a los servicios de AWS obtener acceso a los recursos de otros servicios que completan acciones en su nombre. Los roles vinculados a servicios aparecen en la cuenta de IAM y son propiedad de los servicios. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Amazon Chime admite roles vinculados a servicios. Para obtener más información sobre cómo crear o administrar roles vinculados a servicios de Amazon Chime, consulte [Uso de roles vinculados a servicios para Amazon Chime](#).

Roles de servicio

Esta característica permite que un servicio asuma un [rol de servicio](#) en su nombre. Este rol permite que el servicio obtenga acceso a los recursos de otros servicios para completar una acción en su nombre. Los roles de servicio aparecen en su cuenta de IAM y son propiedad de la cuenta. Esto significa que un administrador de IAM puede cambiar los permisos de este rol. Sin embargo, hacerlo podría deteriorar la funcionalidad del servicio.

Amazon Chime no admite roles de servicio.

Ejemplos de políticas de Amazon Chime basadas en identidades

De forma predeterminada, los usuarios y roles de IAM no tienen permiso para crear ni modificar recursos de Amazon Chime. Tampoco pueden realizar tareas mediante la AWS Management Console, la AWS CLI, o la API de AWS. Un administrador de IAM debe crear políticas de IAM que concedan permisos a los usuarios y a los roles para realizar operaciones de la API concretas en los recursos especificados que necesiten. El administrador debe adjuntar esas políticas a los usuarios o grupos de IAM que necesiten esos permisos.

Para obtener más información acerca de cómo crear una política basada en identidad de IAM con estos documentos de políticas de JSON de ejemplo, consulte [Creación de políticas en la pestaña JSON](#) en la Guía del usuario de IAM.

Temas

- [Prácticas recomendadas relativas a políticas](#)
- [Uso de la consola Amazon Chime](#)

- [Otorgue a los usuarios acceso completo a Amazon Chime](#)
- [Cómo permitir a los usuarios consultar sus propios permisos](#)
- [Permitir que los usuarios accedan a las acciones de administración de usuarios](#)
- [Política administrada por AWS: AmazonChimeVoiceConnectorServiceLinkedRolePolicy](#)
- [Actualizaciones de Amazon Chime en las políticas administradas por AWS](#)

Prácticas recomendadas relativas a políticas

Las políticas basadas en identidades determinan si alguien puede crear o eliminar recursos de Amazon Chime de su cuenta, o a acceder a ellos. Estas acciones pueden generar costes adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas administradas de AWS 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 administradas de AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Se recomienda definir políticas administradas por el cliente de AWS específicas para los casos de uso a fin de reducir aún más los permisos. Con el fin de obtener más información, consulte las [políticas administradas por AWS](#) o las [políticas administradas por AWS para funciones de trabajo](#) en la Guía del usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte [Políticas y permisos en IAM](#) en la Guía de usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse utilizando SSL. También puede usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado, como por ejemplo AWS CloudFormation. Para obtener más información, consulte [Elementos de la política de JSON de IAM: Condición](#) en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas

recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte la [Política de validación del analizador de acceso de IAM](#) en la Guía de usuario de IAM.

- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesita usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para obtener más información, consulte [Configuración de acceso a una API protegida por MFA](#) en la Guía del usuario de IAM.

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

Uso de la consola Amazon Chime

Para acceder a la consola Amazon Chime, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle mostrar y consultar los detalles sobre los recursos de Amazon Chime en la cuenta de AWS. Si crea una política basada en identidad que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles de IAM) que tengan esa política.

Para asegurarse de que esas entidades puedan seguir usando la consola Amazon Chime, asocie también la siguiente política AmazonChimeReadOnly administrada por AWS a las entidades. Para obtener más información, consulte [Agregar de permisos a un usuario](#) en la Guía del usuario de IAM:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "chime:List*",
        "chime:Get*",
        "chime:SearchAvailablePhoneNumbers"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

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

Otorgue a los usuarios acceso completo a Amazon Chime

La política AmazonChimeFullAccess administrada por AWS concede a un usuario de IAM acceso completo a los recursos de Amazon Chime. Esta política concede al usuario acceso a todas las operaciones de Amazon Chime, así como a otras operaciones que Amazon Chime necesita poder realizar en su nombre.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "chime:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketLogging",
        "s3:GetBucketVersioning",
        "s3:GetBucketWebsite"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Action": [
        "logs:CreateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs:GetLogDelivery",
        "logs:ListLogDeliveries",
        "logs:DescribeResourcePolicies",
        "logs:PutResourcePolicy",
```

```

        "logs:CreateLogGroup",
        "logs:DescribeLogGroups"
    ],
    "Effect": "Allow",
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "sns:CreateTopic",
        "sns:GetTopicAttributes"
    ],
    "Resource": [
        "arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "sqs:GetQueueAttributes",
        "sqs:CreateQueue"
    ],
    "Resource": [
        "arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"
    ]
}
]
}

```

Cómo permitir a los usuarios consultar sus propios permisos

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

```

{
  "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": "*"
}
]
}

```

Permitir que los usuarios accedan a las acciones de administración de usuarios

Utilice la política AmazonChimeUserManagement administrada por AWS para conceder a los usuarios acceso a las acciones de administración de usuarios en la consola Amazon Chime.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "chime:ListAccounts",
                "chime:GetAccount",
                "chime:GetAccountSettings",
                "chime:UpdateAccountSettings",
                "chime:ListUsers",
            ]
        }
    ]
}

```

```

        "chime:GetUser",
        "chime:GetUserByEmail",
        "chime:InviteUsers",
        "chime:InviteUsersFromProvider",
        "chime:SuspendUsers",
        "chime:ActivateUsers",
        "chime:UpdateUserLicenses",
        "chime:ResetPersonalPIN",
        "chime:LogoutUser",
        "chime:ListDomains",
        "chime:GetDomain",
        "chime:ListDirectories",
        "chime:ListGroup",
        "chime:SubmitSupportRequest",
        "chime:ListDelegates",
        "chime:ListAccountUsageReportData",
        "chime:GetMeetingDetail",
        "chime:ListMeetingEvents",
        "chime:ListMeetingsReportData",
        "chime:GetUserActivityReportData",
        "chime:UpdateUser",
        "chime:BatchUpdateUser",
        "chime:BatchSuspendUser",
        "chime:BatchUnsuspendUser",
        "chime:AssociatePhoneNumberWithUser",
        "chime:DisassociatePhoneNumberFromUser",
        "chime:GetPhoneNumber",
        "chime:ListPhoneNumbers",
        "chime:GetUserSettings",
        "chime:UpdateUserSettings",
        "chime:CreateUser",
        "chime:AssociateSigninDelegateGroupsWithAccount",
        "chime:DisassociateSigninDelegateGroupsFromAccount"
    ],
    "Effect": "Allow",
    "Resource": "*"
}
]
}

```

Política administrada por AWS:

AmazonChimeVoiceConnectorServiceLinkedRolePolicy

AmazonChimeVoiceConnectorServiceLinkedRolePolicy permite a las instancias de Amazon Chime Voice Connector transmitir contenido multimedia a Amazon Kinesis Video Streams, proporcionar notificaciones de streaming y sintetizar voz con Amazon Polly. Esta política concede al servicio Amazon Chime Voice Connector permisos para acceder a Amazon Kinesis Video Streams del cliente, enviar eventos de notificación a Amazon Simple Notification Service y Amazon Simple Queue Service, y utilizar Amazon Polly para sintetizar la voz al utilizar las acciones `Speak` y `SpeakAndGetDigits` de las aplicaciones de voz del SDK de Amazon Chime. Para obtener más información, consulte los [ejemplos de políticas basadas en la identidad del SDK de Amazon Chime](#) en la Guía del administrador del SDK de Amazon Chime.

Actualizaciones de Amazon Chime en las políticas administradas por AWS

En la siguiente tabla se indican y describen las actualizaciones realizadas en la política de IAM de Amazon Chime.

Cambio	Descripción	Fecha
AmazonChimeVoiceConnectorServiceLinkedRolePolicy : actualización de una política actual	Las instancias de Amazon Chime Voice Connector han añadido nuevos permisos que le permiten utilizar Amazon Polly para sintetizar la voz. Estos permisos son necesarios para utilizar las acciones <code>Speak</code> y <code>SpeakAndGetDigits</code> en las aplicaciones de voz del SDK de Amazon Chime.	15 de marzo de 2022
AmazonChimeVoiceConnectorServiceLinkedRolePolicy : actualización de una política actual	Amazon Chime Voice Connector ha añadido nuevos permisos para permitir el acceso a Amazon Kinesis Video Streams y enviar	20 de diciembre de 2021

Cambio	Descripción	Fecha
	eventos de notificación a SNS y SQS. Estos permisos son necesarios para que las instancias de Amazon Chime Voice Connector puedan transmitir contenido multimedia a Amazon Kinesis Video Streams y proporcionar notificaciones de streaming.	
Modificación de la política existente. Crear usuarios o roles de IAM con la política del SDK de Chime.	<p>Amazon Chime ha añadido nuevas acciones para respaldar la validación ampliada.</p> <p>Se han añadido varias acciones para poder enumerar y etiquetar a los asistentes y los recursos de la reunión, y para iniciar y detener la transcripción de las reuniones.</p>	23 de septiembre de 2021
Amazon Chime ha comenzado a hacer un seguimiento de los cambios	Amazon Chime ha comenzado a hacer un seguimiento de los cambios en sus políticas administradas por AWS.	23 de septiembre de 2021

Solución de problemas de identidad y acceso de Amazon Chime

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que es posible que surjan cuando se trabaja con Amazon Chime e IAM.

Temas

- [No tengo autorización para realizar una acción en Amazon Chime](#)
- [No tengo autorización para realizar la operación iam:PassRole](#)

- [Quiero permitir que personas ajenas a mi cuenta de AWS accedan a mis recursos de Amazon Chime.](#)

No tengo autorización para realizar una acción en Amazon Chime

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 usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio `my-example-widget`, pero no tiene los permisos ficticios `chime:GetWidget`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
chime: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 `chime:GetWidget`.

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

No tengo autorización para realizar la operación `iam:PassRole`

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, sus políticas deben actualizarse para permitirle pasar un rol a Amazon Chime.

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 a servicios. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Amazon Chime. Sin embargo, la acción requiere que el servicio cuente con permisos que concede 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 administrador de AWS. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mi cuenta de AWS accedan a mis recursos de Amazon Chime.

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 (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si Amazon Chime admite estas características, consulte [Cómo funciona Amazon Chime con IAM](#).
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte [Cómo proporcionar acceso a un usuario de IAM a otra Cuenta de AWS de la que es propietario](#) en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos a Cuentas de AWS de terceros, consulte [Proporcionar acceso a Cuentas de AWS que son propiedad de terceros](#) en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante federación de identidades, consulte [Proporcionar acceso a usuarios autenticados externamente \(federación de identidades\)](#) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte [Cómo los roles de IAM difieren de las políticas basadas en recursos](#) en la Guía del Usuario de IAM.

Uso de roles vinculados a servicios para Amazon Chime

Amazon Chime utiliza [roles vinculados a servicios](#) de AWS Identity and Access Management (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Amazon Chime. Los roles vinculados a servicios están predefinidos por Amazon Chime e incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS en su nombre.

Un rol vinculado a servicios hace que la configuración de Amazon Chime sea más eficiente, ya que no tendrá que agregar manualmente los permisos necesarios. Amazon Chime define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo Amazon Chime puede asumir sus roles. Los permisos definidos incluyen la política de confianza y la política de permisos. La política de permisos no se puede asociar a ninguna otra entidad de IAM.

Solo puede eliminar una función vinculada a un servicio después de eliminar sus recursos relacionados. De esta forma, se protegen los recursos de Amazon Chime, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener más información sobre otros servicios que admiten los roles vinculados a servicios, consulte [Servicios de AWS que funcionan con IAM](#). Busque los servicios para los que se indique Sí en la columna Roles vinculados a servicios. Seleccione una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Temas

- [Uso de roles con dispositivos Alexa for Business compartidos](#)
- [Uso de roles con transcripción en vivo](#)
- [Uso de roles con canalizaciones de contenido multimedia del SDK de Amazon Chime](#)

Uso de roles con dispositivos Alexa for Business compartidos

La información de las siguientes secciones explica cómo usar las funciones vinculadas a servicios y cómo conceder a Amazon Chime acceso a los recursos de Alexa for Business de su cuenta de AWS.

Temas

- [Permisos de roles vinculados a servicios para Amazon Chime](#)
- [Creación de un rol vinculado a servicios para Amazon Chime](#)
- [Edición de un rol vinculado a un servicio para Amazon Chime](#)
- [Eliminación de un rol vinculado a servicios para Amazon Chime](#)
- [Regiones admitidas para los roles vinculados a servicios de Amazon Chime](#)

Permisos de roles vinculados a servicios para Amazon Chime

Amazon Chime utiliza el rol vinculado a servicios denominado `AWSServiceRoleForAmazonChime`: permite el acceso a los servicios y recursos de AWS de Amazon Chime, como los dispositivos compartidos de Alexa for Business.

El rol vinculado a los servicios `AWSServiceRoleForAmazonChime` depende de los siguientes servicios para asumir el rol:

- `chime.amazonaws.com`

La política de permisos del rol permite que Amazon Chime realice las siguientes acciones en el recurso especificado:

- Acción: `iam:CreateServiceLinkedRole` en `arn:aws:iam::*:role/aws-service-role/chime.amazonaws.com/AWSServiceRoleForAmazonChime`

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte [Permisos de roles vinculados a servicios](#) en la Guía del usuario de IAM.

Creación de un rol vinculado a servicios para Amazon Chime

No necesita crear manualmente un rol vinculado a servicios. Al activar Alexa for Business para un dispositivo compartido en Amazon Chime en la AWS Management Console, AWS CLI o la API de AWS, Amazon Chime crea el rol vinculado a servicios automáticamente.

También puede utilizar la consola de IAM para crear un rol vinculado al servicio con el caso de uso de Amazon Chime. En la AWS CLI o la API de AWS, cree un rol vinculado al servicio con el nombre de servicio `chime.amazonaws.com`. Para obtener más información, consulte [Creación de un rol vinculado a un servicio](#) en la Guía del usuario de IAM. Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

Edición de un rol vinculado a un servicio para Amazon Chime

Amazon Chime no permite editar el rol vinculado a servicios `AWSServiceRoleForAmazonChime`. Después de crear un rol vinculado a servicios, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia al mismo. Sin embargo, puede editar la descripción del rol

mediante IAM. Para obtener más información, consulte [Editar un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Eliminación de un rol vinculado a servicios para Amazon Chime

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe limpiar el rol vinculado a servicios antes de eliminarlo manualmente.

Limpiar un rol vinculado a servicios

Antes de que pueda utilizar IAM para eliminar un rol vinculado a servicios, primero debe eliminar los recursos que utiliza el rol.

Note

Si Amazon Chime está utilizando el rol cuando se intentan eliminar los recursos, es posible que se produzcan errores en la operación de eliminación. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de Amazon Chime utilizados por `AWSServiceRoleForAmazonChime` (consola)

- Desactive Alexa for Business en todos los dispositivos compartidos de su cuenta de Amazon Chime.
 - a. Abra la consola Amazon Chime en <https://chime.aws.amazon.com/>.
 - b. Elija Users (Usuarios), Shared devices (Dispositivos compartidos).
 - c. Seleccione un dispositivo.
 - d. Elija Actions (Acciones).
 - e. Seleccione Desactivar Alexa for Business.

Eliminar manualmente el rol vinculado al servicio

Utilice la consola de IAM, la AWS CLI o la API de AWS para eliminar el rol vinculado a servicios `AWSServiceRoleForAmazonChime`. Para obtener más información, consulte [Eliminar un rol vinculado a un servicio](#) en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a servicios de Amazon Chime

Amazon Chime admite el uso de roles vinculados a servicios en todas las regiones en las que se encuentra disponible el servicio. Para obtener más información, consulte [Cuotas y puntos de conexión de Amazon Chime](#).

Uso de roles con transcripción en vivo

En la información de las secciones siguientes, se explica cómo se crea y administra un rol vinculado a servicios para la transcripción en vivo de Amazon Chime. Para obtener más información sobre el servicio de transcripción en vivo, consulte [Uso de la transcripción en vivo del SDK de Amazon Chime](#).

Temas

- [Permisos del rol vinculado a servicios para la transcripción en vivo de Amazon Chime](#)
- [Creación de un rol vinculado a servicios para la transcripción en vivo de Amazon Chime](#)
- [Edición de un rol vinculado a servicios para la transcripción en vivo de Amazon Chime](#)
- [Eliminación de un rol vinculado a servicios para la transcripción en vivo de Amazon Chime](#)
- [Regiones admitidas para los roles vinculados a servicios de Amazon Chime](#)

Permisos del rol vinculado a servicios para la transcripción en vivo de Amazon Chime

La transcripción en vivo de Amazon Chime utiliza un rol vinculado a servicios denominado `AWSServiceRoleForAmazonChimeTranscription`, que permite a Amazon Chime acceder a Amazon Transcribe y Amazon Transcribe Medical en su nombre.

El rol vinculado a servicios `AWSServiceRoleForAmazonChimeTranscription` confía en que los siguientes servicios asuman el rol:

- `transcription.chime.amazonaws.com`

La política de permisos del rol permite que Amazon Chime realice las siguientes acciones en los recursos especificados:

- Acción: `transcribe:StartStreamTranscription` en `all AWS resources`
- Acción: `transcribe:StartMedicalStreamTranscription` en `all AWS resources`

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte [Permisos de roles vinculados a servicios](#) en la Guía del usuario de IAM.

Creación de un rol vinculado a servicios para la transcripción en vivo de Amazon Chime

Puede utilizar la consola IAM para crear un rol vinculado a servicios con el caso de uso de Transcripción de Chime.

Note

Debe tener permisos administrativos de IAM para completar estos pasos. Si no es el caso, póngase en contacto con un administrador del sistema.

Para crear el rol

1. Inicie sesión en AWS Management Console y abra la consola IAM en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación de la consola de IAM, seleccione Roles y, a continuación, seleccione Crear rol.
3. Elija el tipo de rol del Servicio de AWS, seleccione Chime y, a continuación, Transcripción de Chime.
4. Elija Siguiente.
5. Elija Siguiente.
6. Edite la descripción según sea necesario y, a continuación, elija Crear rol.

También puede utilizar AWS CLI o la API de AWS para crear un rol vinculado a servicios llamado `transcription.chime.amazonaws.com`.

En CLI, ejecute este comando: `aws iam create-service-linked-role --aws-service-name transcription.chime.amazonaws.com`.

Para obtener más información, consulte [Crear un rol vinculado a un servicio](#) en la Guía del usuario de IAM. Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

Edición de un rol vinculado a servicios para la transcripción en vivo de Amazon Chime

Amazon Chime no permite editar el rol vinculado a servicios `AWSServiceRoleForAmazonChimeTranscription`. Después de crear un rol vinculado a servicios, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia al mismo. Sin embargo, puede utilizar IAM para editar la descripción del rol. Para obtener más información, consulte [Editar un rol vinculado a un servicio](#) en la guía del usuario de IAM.

Eliminación de un rol vinculado a servicios para la transcripción en vivo de Amazon Chime

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM, AWS CLI o la API de AWS para eliminar el rol vinculado a servicios `AWSServiceRoleForAmazonChimeTranscription`. Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a servicios de Amazon Chime

Amazon Chime admite el uso de roles vinculados a servicios en todas las regiones en las que se encuentra disponible el servicio. Para obtener más información, consulte [Puntos de conexión y cuotas de Amazon Chime](#) y [Uso de las regiones multimedia del SDK de Amazon Chime](#).

Uso de roles con canalizaciones de contenido multimedia del SDK de Amazon Chime

En la información de las secciones siguientes, se explica cómo se crea y administra un rol vinculado a servicios para las canalizaciones de contenido multimedia del SDK de Amazon Chime.

Temas

- [Permisos de roles vinculados a servicios para las canalizaciones de contenido multimedia del SDK de Amazon Chime](#)
- [Creación de un rol vinculado a servicios para las canalizaciones de contenido multimedia del SDK de Amazon Chime](#)

- [Edición de un rol vinculado a servicios para las canalizaciones de contenido multimedia del SDK de Amazon Chime](#)
- [Eliminación de un rol vinculado a servicios para las canalizaciones de contenido multimedia del SDK de Amazon Chime](#)
- [Regiones que admiten las canalizaciones de contenido multimedia del SDK de Amazon Chime para los roles vinculados a servicios](#)

Permisos de roles vinculados a servicios para las canalizaciones de contenido multimedia del SDK de Amazon Chime

Amazon Chime usa el rol vinculado a servicios denominado `AWSServiceRoleForAmazonChimeSDKMediaPipelines`: permite que las canalizaciones de contenido multimedia del SDK de Amazon Chime accedan a las reuniones del SDK de Amazon Chime en su nombre.

El rol vinculado a servicios `AWSServiceRoleForAmazonChimeSDKMediaPipelines` confía en que los siguientes servicios asuman el rol:

- `mediapipelines.chime.amazonaws.com`

El rol permite que Amazon Chime realice las siguientes acciones en los recursos especificados:

- Acción: `chime:CreateAttendee` en `all AWS resources`
- Acción: `chime>DeleteAttendee` en `all AWS resources`
- Acción: `chime:GetMeeting` en `all AWS resources`

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte [Permisos de roles vinculados a servicios](#) en la Guía del usuario de IAM.

Creación de un rol vinculado a servicios para las canalizaciones de contenido multimedia del SDK de Amazon Chime

Puede utilizar la consola de IAM para crear un rol vinculado a servicios con el caso de uso de Canalizaciones de contenido multimedia del SDK de Amazon Chime*.

Note

Debe tener permisos administrativos de IAM para completar estos pasos. Si no es el caso, póngase en contacto con un administrador del sistema.

Para crear el rol

1. Inicie sesión en AWS Management Console y abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación de la consola de IAM, seleccione Roles y, a continuación, seleccione Crear rol.
3. Elija el tipo de rol Servicio de AWS, seleccione Chime y, a continuación, Canalizaciones de contenido multimedia del SDK de Chime.
4. Elija Siguiente.
5. Elija Siguiente.
6. Edite la descripción según sea necesario y, a continuación, elija Crear rol.

También puede utilizar AWS CLI o la API de AWS para crear un rol vinculado a servicios denominado `mediapipelines.chime.amazonaws.com`.

En AWS CLI, ejecute el comando `aws iam create-service-linked-role --aws-service-name mediapipelines.chime.amazonaws.com`.

Para obtener más información, consulte [Crear un rol vinculado a un servicio](#) en la Guía del usuario de IAM. Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

Edición de un rol vinculado a servicios para las canalizaciones de contenido multimedia del SDK de Amazon Chime

Amazon Chime no permite editar el rol vinculado a servicios `AWSServiceRoleForAmazonChimeSDKMediaPipelines`. Después de crear un rol vinculado a servicios, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia al mismo. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte [Editar un rol vinculado a un servicio](#) en la guía del usuario de IAM.

Eliminación de un rol vinculado a servicios para las canalizaciones de contenido multimedia del SDK de Amazon Chime

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM, AWS CLI o la API de AWS para eliminar el rol vinculado a servicios `AWSServiceRoleForAmazonChimeSDKMediaPipelines`. Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Regiones que admiten las canalizaciones de contenido multimedia del SDK de Amazon Chime para los roles vinculados a servicios

El SDK de Amazon Chime admite el uso de roles vinculados a servicios en todas las regiones de AWS en las que se encuentra disponible el servicio. Para obtener más información, consulte [Cuotas y puntos de conexión de Amazon Chime](#).

Registro y monitoreo en Amazon Chime

El monitoreo es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon Chime y de las demás soluciones de AWS. AWS proporciona las siguientes herramientas para monitorear sus recursos de Amazon Chime, informar de los problemas y tomar acciones automáticas cuando sea necesario:

- Amazon CloudWatch monitorea en tiempo real los recursos de AWS y las aplicaciones que ejecuta en AWS. 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 hacer que CloudWatch haga un seguimiento del uso de la CPU u otras métricas de las instancias de Amazon EC2 y lanzar nuevas instancias automáticamente cuando sea necesario. Para obtener más información, consulte la [Guía del usuario de Amazon CloudWatch](#).
- Amazon EventBridge proporciona una transmisión de secuencia de eventos de sistema casi en tiempo real que describen cambios en los recursos de AWS. Eventbridge habilita una informática basada en eventos automatizada. Puede escribir reglas que vigilan determinados eventos y

activan acciones automatizadas en otros servicios de AWS cuando se producen estos eventos. Para obtener más información, consulte la [Guía del usuario de Amazon EventBridge](#).

- Registros de Amazon CloudWatch le permite supervisar, almacenar y acceder a los archivos de registro desde instancias de Amazon EC2, CloudTrail u otras fuentes. CloudWatch Logs puede monitorear información en los registros y enviarle una notificación cuando se llega a determinados umbrales. También se pueden archivar los datos de los registros en un almacenamiento de larga duración. Para obtener más información, consulte la [Guía del usuario de Amazon CloudWatch Logs](#).
- AWS CloudTrail captura las llamadas a la API y los eventos relacionados realizados por su cuenta de AWS o en su nombre. A continuación, entrega los archivos log al bucket de Amazon S3 que se especifique. También pueden identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen de las llamadas y el momento en que se hicieron. Para obtener más información, consulte la [Guía del usuario de AWS CloudTrail](#).

Temas

- [Supervisión de Amazon Chime con Amazon CloudWatch](#)
- [Automatización de Amazon Chime con EventBridge](#)
- [Registro de llamadas a la API de Amazon Chime con AWS CloudTrail](#)

Supervisión de Amazon Chime con Amazon CloudWatch

Puede supervisar Amazon Chime mediante 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 del usuario de Amazon CloudWatch](#).

Métricas de CloudWatch para Amazon Chime

Amazon Chime envía las siguientes métricas a CloudWatch.

El espacio de nombres de `AWS/ChimeVoiceConnector` incluye las siguientes métricas para los números de teléfono asignados a su cuenta de AWS y a Amazon Chime Voice Connector.

Métrica	Descripción
InboundCallAttempts	Número de llamadas entrantes intentadas. Unidades: recuento
InboundCallFailures	El número de errores de llamadas entrantes. Unidades: recuento
InboundCallsAnswered	El número de llamadas entrantes que se responden. Unidades: recuento
InboundCallsActive	El número de llamadas entrantes que están activas actualmente. Unidades: recuento
OutboundCallAttempts	Número de llamadas salientes intentadas. Unidades: recuento
OutboundCallFailures	Número de errores de llamadas salientes. Unidades: recuento
OutboundCallsAnswered	El número de llamadas salientes que se responden. Unidades: recuento
OutboundCallsActive	El número de llamadas salientes que están activas actualmente. Unidades: recuento
Throttles	El número de veces que su cuenta se limita al intentar realizar una llamada.

Métrica	Descripción
	Unidades: recuento
Sip1xxCodes	El número de mensajes SIP con códigos de estado de 1xx-level. Unidades: recuento
Sip2xxCodes	El número de mensajes SIP con códigos de estado de 2xx-level. Unidades: recuento
Sip3xxCodes	El número de mensajes SIP con códigos de estado de 3xx-level. Unidades: recuento
Sip4xxCodes	El número de mensajes SIP con códigos de estado de 4xx-level. Unidades: recuento
Sip5xxCodes	El número de mensajes SIP con códigos de estado de 5xx-level. Unidades: recuento
Sip6xxCodes	El número de mensajes SIP con códigos de estado de 6xx-level. Unidades: recuento
CustomerToVcRtpPackets	El número de paquetes RTP enviados desde el cliente a la infraestructura de Amazon Chime Voice Connector. Unidades: recuento

Métrica	Descripción
<code>CustomerToVcRtpBytes</code>	<p>El número de bytes enviados desde el cliente a la infraestructura de Amazon Chime Voice Connector en paquetes RTP.</p> <p>Unidades: recuento</p>
<code>CustomerToVcRtcpPackets</code>	<p>El número de paquetes RTCP enviados desde el cliente a la infraestructura de Amazon Chime Voice Connector.</p> <p>Unidades: recuento</p>
<code>CustomerToVcRtcpBytes</code>	<p>El número de bytes enviados desde el cliente a la infraestructura de Amazon Chime Voice Connector en paquetes RTCP.</p> <p>Unidades: recuento</p>
<code>CustomerToVcPacketsLost</code>	<p>El número de paquetes perdidos durante el tránsito desde el cliente a la infraestructura de Amazon Chime Voice Connector.</p> <p>Unidades: recuento</p>
<code>CustomerToVcJitter</code>	<p>La fluctuación media de los paquetes enviados desde el cliente a la infraestructura de Amazon Chime Voice Connector.</p> <p>Unidades: microsegundos</p>
<code>VcToCustomerRtpPackets</code>	<p>El número de paquetes RTP enviados desde la infraestructura de Amazon Chime Voice Connector al cliente.</p> <p>Unidades: recuento</p>

Métrica	Descripción
VcToCustomerRtpBytes	<p>El número de bytes enviados desde la infraestructura de Amazon Chime Voice Connector al cliente en paquetes RTP.</p> <p>Unidades: recuento</p>
VcToCustomerRtcpPackets	<p>El número de paquetes RTCP enviados desde la infraestructura de Amazon Chime Voice Connector al cliente.</p> <p>Unidades: recuento</p>
VcToCustomerRtcpBytes	<p>El número de bytes enviados desde la infraestructura de Amazon Chime Voice Connector al cliente en paquetes RTCP.</p> <p>Unidades: recuento</p>
VcToCustomerPacketsLost	<p>El número de paquetes perdidos durante el tránsito desde la infraestructura de Amazon Chime Voice Connector al cliente.</p> <p>Unidades: recuento</p>
VcToCustomerJitter	<p>La fluctuación media de los paquetes enviados desde la infraestructura de Amazon Chime Voice Connector al cliente.</p> <p>Unidades: microsegundos</p>
RTTBetweenVcAndCustomer	<p>El promedio de tiempo de ida y vuelta entre el cliente y la infraestructura de Amazon Chime Voice Connector.</p> <p>Unidades: microsegundos</p>

Métrica	Descripción
<code>MOSBetweenVcAndCustomer</code>	<p>La puntuación de opinión media (MOS) estimada que se asocia a las transmisiones de voz entre el cliente y la infraestructura de Amazon Chime Voice Connector.</p> <p>Unidades: puntuación entre 1.0 y 4.4. Una puntuación más alta indica una calidad de audio con mejor percepción.</p>
<code>RemoteToVcRtpPackets</code>	<p>El número de paquetes RTP enviados desde el extremo remoto a la infraestructura de Amazon Chime Voice Connector.</p> <p>Unidades: recuento</p>
<code>RemoteToVcRtpBytes</code>	<p>El número de bytes enviados desde el extremo remoto a la infraestructura de Amazon Chime Voice Connector en paquetes RTP.</p> <p>Unidades: recuento</p>
<code>RemoteToVcRtcpPackets</code>	<p>El número de paquetes RTCP enviados desde el extremo remoto a la infraestructura de Amazon Chime Voice Connector.</p> <p>Unidades: recuento</p>
<code>RemoteToVcRtcpBytes</code>	<p>Número de bytes enviados desde el extremo remoto a la infraestructura de Amazon Chime Voice Connector en paquetes RTCP.</p> <p>Unidades: recuento</p>
<code>RemoteToVcPacketsLost</code>	<p>El número de paquetes perdidos durante el tránsito desde el extremo remoto a la infraestructura de Amazon Chime Voice Connector.</p> <p>Unidades: recuento</p>

Métrica	Descripción
RemoteToVcJitter	<p>La fluctuación media de los paquetes enviados desde el extremo remoto a la infraestructura de Amazon Chime Voice Connector.</p> <p>Unidades: microsegundos</p>
VcToRemoteRtpPackets	<p>El número de paquetes RTP enviados desde la infraestructura de Amazon Chime Voice Connector al extremo remoto.</p> <p>Unidades: recuento</p>
VcToRemoteRtpBytes	<p>El número de bytes enviados desde la infraestructura de Amazon Chime Voice Connector al extremo remoto en paquetes RTP.</p> <p>Unidades: recuento</p>
VcToRemoteRtcpPackets	<p>El número de paquetes RTCP enviados desde la infraestructura de Amazon Chime Voice Connector al extremo remoto.</p> <p>Unidades: recuento</p>
VcToRemoteRtcpBytes	<p>Número de bytes enviados desde el extremo remoto a la infraestructura de Amazon Chime Voice Connector en paquetes RTCP.</p> <p>Unidades: recuento</p>
VcToRemotePacketsLost	<p>El número de paquetes perdidos durante el tránsito desde la infraestructura de Amazon Chime Voice Connector al extremo remoto.</p> <p>Unidades: recuento</p>

Métrica	Descripción
VcToRemoteJitter	<p>La fluctuación media de los paquetes enviados desde la infraestructura de Amazon Chime Voice Connector al extremo remoto.</p> <p>Unidades: microsegundos</p>
RTTBetweenVcAndRemote	<p>El promedio de tiempo de ida y vuelta entre el extremo remoto y la infraestructura de Amazon Chime Voice Connector.</p> <p>Unidades: microsegundos</p>
MOSBetweenVcAndRemote	<p>La puntuación de opinión media (MOS) estimada que se asocia a las transmisiones de voz entre el extremo remoto y la infraestructura de Amazon Chime Voice Connector.</p> <p>Unidades: puntuación entre 1.0 y 4.4. Una puntuación más alta indica una calidad de audio con mejor percepción.</p>

Dimensiones de CloudWatch para Amazon Chime

A continuación se indican las dimensiones de CloudWatch que puede utilizar con Amazon Chime.

Dimensión	Descripción
VoiceConnectorId	El identificador de Amazon Chime Voice Connector para mostrar las métricas.
Region	La región de AWS asociada al evento.

Registros de CloudWatch para Amazon Chime

Puede enviar las métricas de Amazon Chime Voice Connector a los Registros de CloudWatch. Para obtener más información, consulte [Edición de la configuración de Amazon Chime Voice Connector](#) en la Guía de administración del SDK de Amazon Chime.

Registros de métricas sobre la calidad de los medios

Puede optar por recibir registros de métricas de calidad de los medios para su instancia de Amazon Chime Voice Connector. Si lo hace, Amazon Chime envía métricas detalladas por minuto de todas las llamadas de Amazon Chime Voice Connector a un grupo de registro de Registros de CloudWatch que se crea automáticamente. El nombre del grupo de registro es `/aws/ChimeVoiceConnectorLogs/${VoiceConnectorID}`. Los siguientes campos se incluyen en los registros, en formato JSON.

Campo	Descripción
<code>voice_connector_id</code>	El identificador de Amazon Chime Voice Connector que contiene la llamada.
<code>event_timestamp</code>	Hora a la que se emiten las métricas, en número de milisegundos desde la fecha de inicio UNIX (medianoche del 1 de enero de 1970) en UTC.
<code>call_id</code>	Corresponde al identificador de la transacción.
<code>from_sip_user</code>	El usuario que inicia la llamada.
<code>from_country</code>	El país de inicio de la llamada.
<code>to_sip_user</code>	El usuario receptor de la llamada.
<code>to_country</code>	El país receptor de la llamada.
<code>endpoint_id</code>	Identificador opaco que indica el otro punto de enlace de la llamada. Úselo con la información de Registros de CloudWatch. Para obtener más información, consulte Análisis de los datos de registro con la información de Registros

Campo	Descripción
	de CloudWatch en la Guía del usuario de Registros de Amazon CloudWatch.
aws_region	La región de AWS para la llamada.
cust2vc_rtp_packets	El número de paquetes RTP enviados desde el cliente a la infraestructura de Amazon Chime Voice Connector.
cust2vc_rtp_bytes	El número de bytes enviados desde el cliente a la infraestructura de Amazon Chime Voice Connector en paquetes RTP.
cust2vc_rtcp_packets	El número de paquetes RTCP enviados desde el cliente a la infraestructura de Amazon Chime Voice Connector.
cust2vc_rtcp_bytes	El número de bytes enviados desde el cliente a la infraestructura de Amazon Chime Voice Connector en paquetes RTCP.
cust2vc_packets_lost	El número de paquetes perdidos durante el tránsito desde el cliente a la infraestructura de Amazon Chime Voice Connector.
cust2vc_jitter	La fluctuación media de los paquetes enviados desde el cliente a la infraestructura de Amazon Chime Voice Connector.
vc2cust_rtp_packets	El número de paquetes RTP enviados desde la infraestructura de Amazon Chime Voice Connector al cliente.
vc2cust_rtp_bytes	El número de bytes enviados desde la infraestructura de Amazon Chime Voice Connector al cliente en paquetes RTP.

Campo	Descripción
vc2cust_rtcp_packets	El número de paquetes RTCP enviados desde la infraestructura de Amazon Chime Voice Connector al cliente.
vc2cust_rtcp_bytes	El número de bytes enviados desde la infraestructura de Amazon Chime Voice Connector al cliente en paquetes RTCP.
vc2cust_packets_lost	El número de paquetes perdidos durante el tránsito desde la infraestructura de Amazon Chime Voice Connector al cliente.
vc2cust_jitter	La fluctuación media de los paquetes enviados desde la infraestructura de Amazon Chime Voice Connector al cliente.
rtt_btwn_vc_and_cust	El promedio de tiempo de ida y vuelta entre el cliente y la infraestructura de Amazon Chime Voice Connector.
mos_btwn_vc_and_cust	La puntuación de opinión media (MOS) estimada que se asocia a las transmisiones de voz entre el cliente y la infraestructura de Amazon Chime Voice Connector.
rem2vc_rtp_packets	El número de paquetes RTP enviados desde el extremo remoto a la infraestructura de Amazon Chime Voice Connector.
rem2vc_rtp_bytes	El número de bytes enviados desde el extremo remoto a la infraestructura de Amazon Chime Voice Connector en paquetes RTP.
rem2vc_rtcp_packets	El número de paquetes RTCP enviados desde el extremo remoto a la infraestructura de Amazon Chime Voice Connector.

Campo	Descripción
rem2vc_rtcp_bytes	Número de bytes enviados desde el extremo remoto a la infraestructura de Amazon Chime Voice Connector en paquetes RTCP.
rem2vc_packets_lost	El número de paquetes perdidos durante el tránsito desde el extremo remoto a la infraestructura de Amazon Chime Voice Connector.
rem2vc_jitter	La fluctuación media de los paquetes enviados desde el extremo remoto a la infraestructura de Amazon Chime Voice Connector.
vc2rem_rtp_packets	El número de paquetes RTP enviados desde la infraestructura de Amazon Chime Voice Connector al extremo remoto.
vc2rem_rtp_bytes	El número de bytes enviados desde la infraestructura de Amazon Chime Voice Connector al extremo remoto en paquetes RTP.
vc2rem_rtcp_packets	El número de paquetes RTCP enviados desde la infraestructura de Amazon Chime Voice Connector al extremo remoto.
vc2rem_rtcp_bytes	Número de bytes enviados desde el extremo remoto a la infraestructura de Amazon Chime Voice Connector en paquetes RTCP.
vc2rem_packets_lost	El número de paquetes perdidos durante el tránsito desde la infraestructura de Amazon Chime Voice Connector al extremo remoto.
vc2rem_jitter	La fluctuación media de los paquetes enviados desde la infraestructura de Amazon Chime Voice Connector al extremo remoto.

Campo	Descripción
rtt_btwn_vc_and_rem	El promedio de tiempo de ida y vuelta entre el extremo remoto y la infraestructura de Amazon Chime Voice Connector.
mos_btwn_vc_and_rem	La puntuación de opinión media (MOS) estimada que se asocia a las transmisiones de voz entre el extremo remoto y la infraestructura de Amazon Chime Voice Connector.

Registros de mensajes SIP

Puede optar por recibir registros de mensajes SIP para su instancia de Amazon Chime Voice Connector. Cuando lo haga, Amazon Chime captura los mensajes SIP entrantes y salientes y los envía a un grupo de registro de Registros de CloudWatch creado automáticamente. El nombre del grupo de registro es `/aws/ChimeVoiceConnectorSipMessages/${VoiceConnectorID}`. Los siguientes campos se incluyen en los registros, en formato JSON.

Campo	Descripción
voice_connector_id	El ID de Amazon Chime Voice Connector.
aws_region	La región de AWS asociada al evento.
event_timestamp	Hora a la que se captura el mensaje, en número de milisegundos desde la fecha de inicio UNIX (medianoche del 1 de enero de 1970) en UTC.
call_id	El identificador de llamada de Amazon Chime Voice Connector.
sip_message	El mensaje SIP completo que se captura.

Automatización de Amazon Chime con EventBridge

Amazon EventBridge le permite automatizar sus servicios de AWS y responder automáticamente a eventos del sistema, como problemas de disponibilidad de aplicaciones o cambios de recursos. Para obtener más información sobre los eventos de la reunión, consulte [Eventos de la reunión](#) en la Guía para desarrolladores de Amazon Chime.

Cuando Amazon Chime genera eventos, los envía a EventBridge para que se entregue el mejor esfuerzo, lo que significa que Amazon Chime intenta enviar todos los eventos a EventBridge, pero en algunos casos raros es posible que no se entregue un evento. Para obtener más información, consulte [Eventos de servicios de AWS](#) en la Guía del usuario de Amazon EventBridge.

Note

Si necesita cifrar datos, debe utilizar claves gestionadas por Amazon S3. No admitimos el cifrado del servidor mediante las claves maestras del cliente almacenadas en el servicio de administración de claves de AWS.

Automatización de las instancias de Amazon Chime Voice Connector con EventBridge

Entre las acciones que se pueden activar automáticamente para las instancias de Amazon Chime Voice Connector se incluyen las siguientes:

- Invocar una función de AWS Lambda
- Lanzamiento de una tarea de Amazon Elastic Container Service
- Desvío del evento a Amazon Kinesis Video Streams
- Activar una máquina de estado de AWS Step Functions
- Notificar un tema de Amazon SNS o una cola de Amazon SQS

Algunos ejemplos del uso de EventBridge con instancias de Amazon Chime Voice Connector son:

- Activación de una función de Lambda para descargar audio de una llamada una vez finalizada la llamada.
- Lanzamiento de una tarea de Amazon ECS para habilitar la transcripción en tiempo real después de iniciar una llamada.

Para obtener más información, consulte la [Guía del usuario de Amazon EventBridge](#).

Eventos de streaming de Amazon Chime Voice Connector

Amazon Chime Voice Connector es compatible con el envío de eventos a EventBridge cuando se producen los eventos descritos en esta sección.

Comienza la transmisión de Amazon Chime Voice Connector

Las instancias de Amazon Chime Voice Connector envían este evento cuando se inicia la transmisión de contenido multimedia a Kinesis Video Streams.

Example Datos de evento

El siguiente es un ejemplo de los datos de este evento.

```
{
  "version": "0",
  "id": "12345678-1234-1234-1234-111122223333",
  "detail-type": "Chime VoiceConnector Streaming Status",
  "source": "aws.chime",
  "account": "111122223333",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "callId": "1112-2222-4333",
    "direction": "Outbound",
    "fromNumber": "+12065550100",
    "inviteHeaders": {
      "from": "\"John\" <sip:+12065550100@10.24.34.0>;tag=abcdefg",
      "to": "<sip:
+13605550199@abcdef1ghij2klmno3pqr4.voiceconnector.chime.aws:5060>",
      "call-id": "1112-2222-4333",
      "cseq": "101 INVITE",
      "contact": "<sip:user@10.24.34.0:6090>",
      "content-type": "application/sdp",
      "content-length": "246"
    },
    "isCaller": false,
    "mediaType": "audio/L16",
    "sdp": {
      "mediaIndex": 0,
      "mediaLabel": "1"
    }
  }
}
```

```

    },
    "siprecMetadata": "<&xml version=\"1.0\" encoding=\"UTF-8\"&>\r\n<recording
xmlns='urn:ietf:params:xml:ns:recording:1'>",
    "startFragmentNumber": "1234567899444",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "streamArn": "arn:aws:kinesisvideo:us-east-1:123456:stream/ChimeVoiceConnector-
abcdef1ghij2klmno3pqr4-111aaa-22bb-33cc-44dd-111222/111122223333",
    "toNumber": "+13605550199",
    "transactionId": "12345678-1234-1234",
    "voiceConnectorId": "abcdef1ghij2klmno3pqr4",
    "streamingStatus": "STARTED",
    "version": "0"
  }
}

```

Finaliza la transmisión de Amazon Chime Voice Connector

Las instancias de Amazon Chime Voice Connector envían este evento cuando finaliza la transmisión multimedia a Kinesis Video Streams.

Example Datos de evento

El siguiente es un ejemplo de los datos de este evento.

```

{
  "version": "0",
  "id": "12345678-1234-1234-1234-111122223333",
  "detail-type": "Chime VoiceConnector Streaming Status",
  "source": "aws.chime",
  "account": "111122223333",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "streamingStatus": "ENDED",
    "voiceConnectorId": "abcdef1ghij2klmno3pqr4",
    "transactionId": "12345678-1234-1234",
    "callId": "1112-2222-4333",
    "direction": "Inbound",
    "fromNumber": "+12065550100",
    "inviteHeaders": {
      "from": "\"John\" <sip:+12065550100@10.24.34.0>;tag=abcdefg",
      "to": "<sip:
+13605550199@abcdef1ghij2klmno3pqr4.voiceconnector.chime.aws:5060>",

```

```

        "call-id": "1112-2222-4333",
        "cseq": "101 INVITE",
        "contact": "<sip:user@10.24.34.0:6090>",
        "content-type": "application/sdp",
        "content-length": "246"
    },
    "isCaller": false,
    "mediaType": "audio/L16",
    "sdp": {
        "mediaIndex": 0,
        "mediaLabel": "1"
    },
    "siprecMetadata": "<&xml version=\"1.0\" encoding=\"UTF-8\">\r\n<recording
xmlns='urn:ietf:params:xml:ns:recording:1'>",
    "startFragmentNumber": "1234567899444",
    "startTime": "yyyy-mm-ddThh:mm:ssZ",
    "endTime": "yyyy-mm-ddThh:mm:ssZ",
    "streamArn": "arn:aws:kinesisvideo:us-east-1:123456:stream/ChimeVoiceConnector-
abcdef1ghij2klmno3pqr4-111aaa-22bb-33cc-44dd-111222/111122223333",
    "toNumber": "+13605550199",
    "version": "0"
}
}

```

Actualizaciones de streaming de Amazon Chime Voice Connector

Las instancias de Amazon Chime Voice Connector envían este evento cuando se actualiza la transmisión multimedia a Kinesis Video Streams.

Example Datos de evento

El siguiente es un ejemplo de los datos de este evento.

```

{
    "version": "0",
    "id": "12345678-1234-1234-1234-111122223333",
    "detail-type": "Chime VoiceConnector Streaming Status",
    "source": "aws.chime",
    "account": "111122223333",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "callId": "1112-2222-4333",

```



```

    "updateHeaders": {
      "from": "\"John\" <sip:+12065550100@10.24.34.0>;tag=abcdefg",
      "to": "<sip:
+13605550199@abcdef1ghij2klmno3pqr4.voiceconnector.chime.aws:5060>",
      "call-id": "1112-2222-4333",
      "cseq": "101 INVITE",
      "contact": "<sip:user@10.24.34.0:6090>",
      "content-type": "application/sdp",
      "content-length": "246"
    },
    "siprecMetadata": "<&xml version=\"1.0\" encoding=\"UTF-8\">\r\n<recording
xmlns='urn:ietf:params:xml:ns:recording:1'>",
    "streamingStatus": "UPDATED",
    "transactionId": "12345678-1234-1234",
    "version": "0",
    "voiceConnectorId": "abcdef1ghij2klmno3pqr4"
  }
}

```

Falla la transmisión de Amazon Chime Voice Connector

Las instancias de Amazon Chime Voice Connector envían este evento cuando se produce un error en la transmisión de contenido multimedia a Kinesis Video Streams.

Example Datos de evento

El siguiente es un ejemplo de los datos de este evento.

```

{
  "version": "0",
  "id": "12345678-1234-1234-1234-111122223333",
  "detail-type": "Chime VoiceConnector Streaming Status",
  "source": "aws.chime",
  "account": "111122223333",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "streamingStatus": "FAILED",
    "voiceConnectorId": "abcdefghi",
    "transactionId": "12345678-1234-1234",
    "callId": "1112-2222-4333",
    "direction": "Inbound",
  }
}

```

```
"failTime": "yyyy-mm-ddThh:mm:ssZ",
"failureReason": "Internal failure",
"version": "0"
}
}
```

Registro de llamadas a la API de Amazon Chime con AWS CloudTrail

Amazon Chime se integra con AWS CloudTrail, un servicio que proporciona un registro de las medidas adoptadas por un usuario, un rol o un servicio de AWS en Amazon Chime. CloudTrail obtiene todas las llamadas a la API para Amazon Chime como eventos, incluidas las llamadas procedentes de la consola Amazon Chime y de las llamadas de código a las API de Amazon Chime. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos de Amazon Chime. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Historial de eventos. Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Amazon Chime, la dirección IP de origen desde la que se realizó, quién la realizó y cuándo, etc.

Para obtener más información acerca de CloudTrail, consulte la [Guía del usuario de AWS CloudTrail](#).

Información de Amazon Chime en CloudTrail

CloudTrail se habilita en su cuenta de AWS cuando la crea. Cuando las llamadas a la API se realizan desde la consola de administración Amazon Chime dicha actividad se registra en un evento de CloudTrail junto con otros eventos de servicio de AWS en el Historial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte [Visualización de eventos con el historial de eventos de CloudTrail](#).

Para mantener un registro continuo de los eventos de la cuenta de AWS, incluidos los eventos de Amazon Chime, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de . El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte:

- [Introducción a la creación de registros de seguimiento](#)

- [Servicios e integraciones compatibles con CloudTrail](#)
- [Configuración de notificaciones de Amazon SNS para CloudTrail](#)
- [Recibir archivos de registro de CloudTrail de varias regiones](#) y [Recibir archivos de registro de CloudTrail de varias cuentas](#)

Todas las acciones de Amazon Chime se registran en CloudTrail y están documentadas en la [Referencia de la API de Amazon Chime](#). Por ejemplo, las llamadas a las secciones `CreateAccount`, `InviteUsers` y `ResetPersonalPIN` generan entradas en los archivos de registro de CloudTrail. Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales raíz o del usuario de IAM de .
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

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

Descripción de las entradas de archivos de registro de Amazon Chime

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que especifique. Los archivos log de CloudTrail pueden contener una o varias entradas de log. Un evento representa una única solicitud de cualquier origen e incluye información acerca de la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etcétera. Los archivos de registro de CloudTrail no son un rastro de pila ordenado de las llamadas a las API públicas, por lo que no aparecen en ningún orden específico.

Las entradas de Amazon Chime se identifican mediante el origen de eventos `chime.amazonaws.com`.

Si ha configurado Active Directory para su cuenta de Amazon Chime, consulte [Registro de llamadas a la API de AWS Directory Service con CloudTrail](#). Allí se describe cómo monitorear los errores que pudieran afectar a la capacidad de los usuarios de Amazon Chime para iniciar sesión.

En el siguiente ejemplo se muestra una entrada de registro de CloudTrail para Amazon Chime:

```
{"eventVersion":"1.05",
  "userIdentity":{"
    "type":"IAMUser",
```

```

    "principalId":" AAAAAABBBBBBBBEXAMPLE",
    "arn":"arn:aws:iam::123456789012:user/Alice ",
    "accountId":"0123456789012",
    "accessKeyId":"AAAAAABBBBBBBBEXAMPLE",
    "sessionContext":{
      "attributes":{
        "mfaAuthenticated":"false",
        "creationDate":"2017-07-24T17:57:43Z"
      },
      "sessionIssuer":{
        "type":"Role",
        "principalId":"AAAAAABBBBBBBBEXAMPLE",
        "arn":"arn:aws:iam::123456789012:role/Joe",
        "accountId":"123456789012",
        "userName":"Joe"
      }
    }
  } ,
  "eventTime":"2017-07-24T17:58:21Z",
  "eventSource":"chime.amazonaws.com",
  "eventName":"AddDomain",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"72.21.198.64",
  "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36",
  "errorCode":"ConflictException",
  "errorMessage":"Request could not be completed due to a conflict",
  "requestParameters":{
    "domainName":"example.com",
    "accountId":"11aaaaaa1-1a11-1111-1a11-aaadd0a0aa00"
  },
  "responseElements":null,
  "requestID":"be1bee1d-1111-11e1-1eD1-0dc1111f1ac1",
  "eventID":"00fbeee1-123e-111e-93e3-11111bfbfcc1",
  "eventType":"AwsApiCall",
  "recipientAccountId":"123456789012"
}

```

Validación de la conformidad de Amazon Chime


Audidores externos evalúan la seguridad y la conformidad de los servicios de AWS como parte de varios programas de conformidad de AWS, como SOC, PCI, FedRAMP e HIPAA.

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](#) y escoja el programa de conformidad que le interese. Para obtener información general, consulte [Programas de conformidad de AWS](#).

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

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

- [Guías de inicio rápido de seguridad y conformidad](#): estas guías de implementación tratan consideraciones sobre arquitectura y ofrecen pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- [Arquitectura para la seguridad y el cumplimiento de la HIPAA en Amazon Web Services](#): en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones aptas para HIPAA.

 Note

No todos los Servicios de AWS son aptos para HIPAA. Para obtener más información, consulte la [Referencia de servicios aptos para HIPAA](#).

- [Recursos de conformidad de AWS](#): este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- [Guías de cumplimiento para clientes de AWS](#): 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, por sus siglas en inglés), el Consejo de Estándares de Seguridad de la Industria de Tarjetas de Pago (PCI, por sus siglas en inglés) y la Organización Internacional de Normalización (ISO, por sus siglas en inglés)).
- [Evaluación de recursos con reglas](#) en la Guía para desarrolladores de AWS Config: el servicio AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.

- [AWS Security Hub](#): este servicio de AWS proporciona una visión completa de su estado de seguridad en 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](#).
- [AWS Audit Manager](#): este Servicio de AWS le ayuda a auditar continuamente el uso de AWS 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 Amazon Chime

La infraestructura global de AWS se compone de regiones y zonas de disponibilidad de AWS. AWS Las regiones 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. Mediante 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 y zonas de disponibilidad de AWS, consulte [Infraestructura global de AWS](#).

Además de la infraestructura global de AWS, Amazon Chime cuenta con diversas características que le ayudan con sus necesidades de resiliencia y copia de seguridad de los datos. Para obtener más información, consulte [Administración de grupos de instancias de Amazon Chime Voice Connector y Transmisión de contenido multimedia de Amazon Chime Voice Connector a Kinesis](#) en la Guía de administración del SDK de Amazon Chime.

Seguridad de la infraestructura en Amazon Chime

Como se trata de un servicio administrado, Amazon Chime se encuentra protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y sobre cómo AWS protege la infraestructura, consulte [Seguridad en la nube de AWS](#). Para diseñar su entorno de AWS conforme a las prácticas recomendadas de seguridad de la infraestructura, consulte [Protección de la infraestructura](#) en Pilar de seguridad del Marco de AWS Well-Architected.

Puede utilizar llamadas a la API publicadas en AWS para acceder a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o 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 principal de IAM. También puede utilizar [AWS Security Token Service](#) (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Descripción de las actualizaciones automáticas de Amazon Chime

Amazon Chime ofrece diferentes formas de actualizar sus clientes. El método varía en función de si los usuarios ejecutan Amazon Chime en un navegador, en el escritorio o en un dispositivo móvil.

La aplicación web de Amazon Chime (<https://app.chime.aws>) siempre se carga con las características y correcciones de seguridad más recientes.


El cliente de escritorio de Amazon Chime comprueba si hay actualizaciones cada vez que un usuario elige Salir o Cerrar sesión. Esto se aplica a los equipos Windows y macOS. Cuando los usuarios ejecutan el cliente, este comprueba si hay actualizaciones cada tres horas. Los usuarios también pueden comprobar si hay actualizaciones seleccionando Buscar actualizaciones en el menú Ayuda de Windows o en el menú Amazon Chime de macOS.

Cuando el cliente de escritorio detecta una actualización, Amazon Chime pide a los usuarios que la instalen, a menos que estén en una reunión en curso. Los usuarios están en una reunión en curso cuando:

- Están asistiendo a una reunión.
- Los han invitado a una reunión que todavía está en curso.

Amazon Chime les pide que instalen la última versión y les da una cuenta regresiva de 15 segundos para que puedan posponer la instalación. Seleccione Probar más tarde para posponer la actualización.

Cuando los usuarios posponen una actualización y no están en una reunión en curso, el cliente comprueba si existe la actualización al cabo de tres horas y les pide de nuevo que la instalen. La instalación comienza cuando finaliza la cuenta regresiva.

 Note

En un equipo macOS, los usuarios deben seleccionar Reiniciar ahora para iniciar la actualización.

En un dispositivo móvil: las aplicaciones móviles de Amazon Chime utilizan las opciones de actualización que ofrecen App Store y Google Play para ofrecer la última versión del cliente Amazon Chime. También puede distribuir las actualizaciones a través del sistema de administración de su dispositivo móvil. En este tema se presupone que sabe hacerlo.

Historial de revisión de Amazon Chime

En la siguiente tabla se describen cambios importantes en la Guía del administrador de Amazon Chime, a partir de marzo de 2018. Para obtener notificaciones sobre las actualizaciones de esta documentación, puede suscribirse a una fuente RSS.

Cambio	Descripción	Fecha
Publicada la guía de administración del SDK de Amazon Chime	Los temas del SDK de Amazon Chime se publican ahora en la Guía de administración del SDK de Amazon Chime. Para obtener más información, consulte la Guía de administración del SDK de Amazon Chime .	24 de marzo de 2022
Actualizaciones de la política de IAM	Los cambios en las políticas de IAM gestionadas por ahora AWS se incluyen en esta guía del administrador. Consulte ejemplos de políticas de Amazon Chime basadas en identidades .	23 de septiembre de 2021
Roles vinculados al servicio	Los administradores ahora pueden crear funciones vinculadas a servicios para la transcripción en vivo de Amazon y ver los mensajes de los eventos cuando se inicia y finaliza una operación de transcripción en vivo de Amazon Chime. Para obtener más información, consulte Uso de roles con transcripciones en directo y Automatización de	12 de agosto de 2021

[Amazon Chime CloudWatch con eventos.](#)

18 de noviembre de 2020

[Reglas y aplicaciones multimedia de SIP](#)

Los administradores pueden crear reglas y aplicaciones multimedia SIP para usarlas con el conector y AWS Lambda las funciones de Amazon Chime Voice. Para obtener más información, consulte [Administración de aplicaciones y reglas de SIP](#) en la Guía del administrador de Amazon Chime.

[Números de enrutamiento de llamadas de emergencia de Amazon Chime Voice Connector](#)

1 de julio de 2020

Los administradores de Amazon Chime pueden configurar números de enrutamiento de llamadas de emergencia para una instancia de Amazon Chime Voice Connector. Para obtener más información, consulte [Configuración de los números de enrutamiento de llamadas de emergencia para su conector de voz de Amazon Chime](#), en la Guía del administrador de Amazon Chime.

[Amazon Chime en Dolby Voice Huddle](#)

Amazon Chime ofrece una experiencia de reunión nativa o propia en hardware de conferencias de audio y vídeo Dolby Voice Huddle. Para obtener más información, consulte [Configuración de Amazon Chime en hardware Dolby, en](#) la Guía del administrador de Amazon Chime.

3 de junio de 2020

[Establecer políticas de retención de chat](#)

Los administradores de Amazon Chime pueden establecer políticas de retención de chat en sus cuentas corporativas. Para obtener más información, consulte [Administrar las políticas de retención de chats](#) en la Guía del administrador de Amazon Chime.

21 de mayo de 2020

[Eliminación de mensajes de chat](#)

Si tiene la capacidad de programar, puede usar un par de API de Amazon Chime para eliminar los mensajes de las salas de chat y las conversaciones de su cuenta. Para obtener más información, consulte [Eliminar mensajes individuales](#) en la Guía del administrador de Amazon Chime.

18 de mayo de 2020

[CloudWatch métricas de calidad multimedia para Amazon Chime Voice Connector](#)

Amazon Chime admite el envío de métricas de calidad multimedia para su conector de voz Amazon Chime a. CloudWatch Para obtener más información, consulte [Monitorear Amazon Chime con CloudWatch](#), en la Guía del administrador de Amazon Chime.

23 de enero de 2020

[Aplicación Amazon Chime Meetings para Slack](#)

Amazon Chime es compatible con la aplicación Amazon Chime Meetings para Slack. Para obtener más información, consulta [Cómo configurar la aplicación Amazon Chime Meetings para Slack](#) en la Guía del administrador de Amazon Chime.

4 de diciembre de 2019

[Configuración de la región de la reunión](#)

Amazon Chime permite procesar las reuniones en la AWS región óptima para todos los participantes. Para obtener más información, consulte [Configuración de la región de reuniones](#) en la Guía del administrador de Amazon Chime.

3 de diciembre de 2019

[Compatibilidad con la grabación de contenido multimedia basada en SIP \(SIPREC\)](#)

Las instancias de Amazon Chime Voice Connector admiten la transmisión de contenido multimedia desde una infraestructura de voz compatible con SIPREC a Kinesis Video Streams. Para obtener más información, consulte [Compatibilidad con la grabación multimedia basada en SIP \(SIPREC\)](#) en la Guía del administrador de Amazon Chime.

25 de noviembre de 2019

[Amazon Chime en Dolby Voice Room](#)

Si desea que los usuarios se unan cómodamente a las reuniones, Amazon Chime ofrece una experiencia de reunión nativa o de primera parte en el dispositivo de audio y videoconferencia Dolby Voice Room. Para obtener más información, consulte [Configuración de Amazon Chime en Dolby Voice Room, en](#) la Guía del administrador de Amazon Chime.

29 de octubre de 2019

[Actualización de nombres de llamadas salientes](#)

Establezca un nombre de llamada predeterminado que aparezca a los destinatarios de las llamadas salientes realizadas con números de teléfono de su inventario de Amazon Chime. Para obtener más información, consulte [Actualización de los nombres de llamadas salientes](#) en la Guía del administrador de Amazon Chime.

24 de octubre de 2019

[Transmisión de contenido multimedia a Amazon Kinesis](#)

Transmita audio de llamadas telefónicas de instancias de Amazon Chime Voice Connector a Kinesis Video Streams para análisis, aprendizaje automático y otros procesos. Para obtener más información, consulte [Transmisión de contenido multimedia de Amazon Chime Voice Connector a Kinesis](#) y Uso de la [función vinculada al servicio Amazon Chime Voice Connector](#), en la Guía del administrador de Amazon Chime.

24 de octubre de 2019

[Supervisión de Amazon Chime con Amazon CloudWatch](#)

Supervise Amazon Chime con Amazon CloudWatch, que recopila datos sin procesar y los procesa para convertirlos en métricas legibles prácticamente en tiempo real. Para obtener más información, consulte [Monitorear Amazon Chime con CloudWatch](#), en la Guía del administrador de Amazon Chime.

24 de octubre de 2019

[Grupos de instancias de Amazon Chime Voice Connector](#)

Cree un grupo de conectores de voz de Amazon Chime que incluya conectores de voz de Amazon Chime creados en distintas regiones. AWS Esto permite que las llamadas entrantes conmuten por error en todas las regiones, lo que crea un mecanismo tolerante a fallos para alternativas en caso de eventos de disponibilidad. Para obtener más información, consulte [Trabajar con grupos de conectores de voz de Amazon Chime](#) en la Guía del administrador de Amazon Chime.

24 de octubre de 2019

[Actualizaciones de la configuración de red](#)

Amazon Chime simplifica sus requisitos de firewall. Para obtener más información, consulte los [requisitos de ancho de banda y configuración de red](#) en la Guía del administrador de Amazon Chime.

6 de septiembre de 2019

[Reuniones moderadas](#)

Amazon Chime admite reuniones moderadas. Para obtener más información, consulte [Unirse a una reunión moderada](#) en la Guía del administrador de Amazon Chime.

25 de julio de 2019

[Validación de la conformidad de Amazon Chime](#)

Amazon Chime es un servicio compatible con HIPAA. Para obtener más información, consulte [Validación de conformidad para Amazon Chime](#) en la Guía del administrador de Amazon Chime.

11 de junio de 2019

[Portabilidad de números de teléfono gratuitos](#)

Amazon Chime admite la portabilidad de números de teléfono gratuitos de Estados Unidos para usarlos con instancias de Amazon Chime Voice Connector. Para obtener más información, consulte [Transferir números de teléfono existentes](#) en la Guía del administrador de Amazon Chime.

28 de mayo de 2019

[Administración de números de teléfono en Amazon Chime](#)

Utilice Amazon Chime Business Calling para aprovisionar y asignar números de teléfono a los usuarios de Amazon Chime. Integre una instancia de Amazon Chime Voice Connector con un sistema de telefonía existente. Para obtener más información, consulte [Administración de números de teléfono en Amazon Chime](#) en la Guía del administrador de Amazon Chime.

18 de marzo de 2019

[Complemento de Amazon Chime para Outlook](#)

Amazon Chime proporciona dos complementos para Microsoft Outlook: el complemento de Amazon Chime para Outlook en Windows y el complemento de Amazon Chime para Outlook. Estos complementos ofrecen las mismas características de programación, pero admiten diferentes tipos de usuarios. Para obtener más información, consulte [Implementación del complemento para Outlook en la Guía del administrador de Amazon Chime](#).

12 de marzo de 2019

[Varias actualizaciones](#)

Varias actualizaciones en el diseño y la organización de los temas.

11 de febrero de 2019

[Característica “Lláname” de Amazon Chime](#)

Los administradores pueden habilitar la característica “Lláname” de Amazon Chime en la configuración de Reuniones. Para obtener más información, consulte [Administrar la configuración de las reuniones](#) en la Guía del administrador de Amazon Chime.

22 de agosto de 2018

[Conexión con Okta SSO](#)

Si tiene una cuenta de empresa, puede conectarse a Okta SSO para autenticar y asignar permisos de usuario. Para obtener más información, consulte [Connect to Okta SSO](#) en la Guía del administrador de Amazon Chime.

1 de agosto de 2018

[Solicitud de archivos adjuntos de los usuarios](#)

Recepción de archivos adjuntos que los usuarios cargan en Amazon Chime. Para obtener más información, consulte [Solicitar archivos adjuntos de usuario](#) en la Guía del administrador de Amazon Chime.

23 de abril de 2018

[Visualización de datos de informe adicionales](#)

Visualización de datos de informe adicionales. Para obtener más información, consulte [Ver informes](#) en la Guía del administrador de Amazon Chime.

30 de marzo de 2018

[Asignación de permisos Basic o Pro a los usuarios](#)

Asignación de permisos Basic o Pro a los usuarios. Para obtener más información, consulte [Administrar el acceso y los permisos de los usuarios](#) en la Guía del administrador de Amazon Chime.

29 de marzo de 2018