



Guia de administração

# Amazon Chime



# Amazon Chime: Guia de administração

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

---

# Table of Contents

.....	viii
O que é o Amazon Chime? .....	1
Visão geral da administração .....	1
Como começar .....	1
Preços .....	2
Recursos .....	2
Guia dos recursos de transição do Amazon Chime .....	3
Recursos de transição para administradores do Amazon Chime .....	3
Relatórios de uso .....	3
Ativar relatórios de uso .....	4
Desativar relatórios de uso .....	5
Conteúdo do relatório .....	6
Chamada comercial - portabilidade de números de telefone .....	7
Gerenciando suas contas de usuário - Contas de equipe .....	7
Gerenciando suas contas de usuário - Contas corporativas .....	8
Recursos de transição para usuários do Amazon Chime .....	10
Usuários Pro - Removendo o Amazon Chime dos seus convites para reuniões .....	10
Administradores da sala de bate-papo - Obtenha uma lista de membros .....	11
Usuários do Amazon Chime - Exporte seus contatos pessoais .....	12
Resumo .....	13
Recursos adicionais .....	13
Pré-requisitos para administradores de sistema .....	15
Como criar uma conta da Amazon Web Services .....	15
Inscreva-se para um Conta da AWS .....	15
Criar um usuário com acesso administrativo .....	16
Conceitos básicos .....	18
Etapa 1: Criar uma conta de administrador do Amazon Chime .....	18
Etapa 2 (opcional): definir configurações da conta .....	19
Etapa 3: adicionar usuários à conta .....	20
(Opcional) Configurar números de telefone da sua conta do Amazon Chime .....	21
Gerenciar suas contas .....	22
Escolher uma conta de equipe ou empresarial .....	23
Reivindicar um domínio .....	24
Converter uma conta de equipe em uma conta empresarial .....	25

Renomear sua conta .....	26
Excluir sua conta .....	26
Gerenciar as configurações da reunião .....	28
Configurações da política da reunião .....	28
Configurações do aplicativo de reunião .....	29
Configurações da região da reunião .....	29
Gerenciar políticas de retenção de bate-papo .....	30
Como as políticas de retenção afetam os usuários do Amazon Chime .....	30
Ativar a retenção de bate-papo .....	33
Restaurando mensagens de bate-papo .....	34
Excluindo mensagens de bate-papo .....	35
Conectar ao Active Directory .....	36
Pré-requisitos .....	36
Conectar ao seu Active Directory no Amazon Chime .....	37
Configurar vários endereços de e-mail .....	37
Conectar ao Okta SSO .....	39
Implantar a extensão para Outlook .....	42
Configurar o aplicativo Amazon Chime Meetings para Slack .....	43
Instalação do aplicativo Amazon Chime Meetings para Slack em uma organização .....	43
Instalação do aplicativo Amazon Chime Meetings para Slack em espaços de trabalho .....	44
Migrar espaços de trabalho para organizações .....	45
Associar espaços de trabalho a contas de equipe do Amazon Chime .....	45
Gerenciamento de usuários .....	48
Adição de usuários .....	48
Visualizar detalhes do usuário .....	49
Gerenciar as permissões e o acesso do usuário .....	51
Gerenciamento de permissões de usuário .....	52
Gerenciar acesso do usuário .....	53
Mudando a reunião pessoal PINs .....	55
Gerenciar avaliações do Pro .....	55
Solicitar anexos de usuários .....	56
Como o Amazon Chime gerencia as atualizações automáticas .....	57
Migrar usuários para outra conta de equipe .....	58
Gerenciar números de telefone .....	59
Provisionar números de telefone .....	60
Transferir números de telefones existentes .....	60

Pré-requisitos para portar números .....	61
Transferindo números de telefone para .....	61
Envio dos documentos necessários .....	63
Visualizando o status da solicitação .....	64
Atribuição de números portados .....	65
Transferindo números de telefone .....	65
Definições de status de transferência de números de telefone .....	67
Atribuição de números de telefone .....	68
Cancelando a atribuição de números de telefone .....	69
Usando nomes de chamadas externas .....	69
Excluir números de telefone .....	70
Restaurar números de telefone excluídos .....	71
Gerenciar configurações globais .....	72
Configurar registros de detalhes de chamadas .....	72
Registros de detalhes de chamadas do Amazon Chime Business Calling .....	73
Configurando relatórios de uso .....	74
Conteúdo do relatório de uso .....	6
Configuração de salas de conferência .....	77
Participar de uma reunião moderada .....	78
Dispositivos VTC compatíveis .....	78
Requisitos de configuração de rede e largura de banda .....	80
Visualizar relatórios .....	84
Estender o cliente de desktop do Amazon Chime .....	85
Gerenciamento de usuários .....	85
Convidar vários usuários .....	85
Fazer download das listas de usuários .....	86
Desconectar vários usuários .....	86
Atualizar dados pessoais do usuário PINs .....	87
Integrando chatbots .....	87
Usar chatbots com o Amazon Chime .....	88
Eventos do Amazon Chime enviados para chatbots .....	97
Criar webhooks .....	99
Solucionar de problemas de erros de webhook .....	101
Suporte administrativo .....	102
Segurança .....	103
Gerenciamento de identidade e acesso .....	104

Público .....	104
Autenticar com identidades .....	105
Gerenciar o acesso usando políticas .....	108
Como o Amazon Chime funciona com o IAM .....	112
Políticas baseadas em identidade do Amazon Chime .....	112
Recursos .....	113
Exemplos .....	113
Prevenção do problema do substituto confuso entre serviços .....	113
Políticas baseadas em recursos do Amazon Chime .....	114
Autorização baseada em tags do Amazon Chime .....	114
Perfis do IAM no Amazon Chime .....	114
Usar credenciais temporárias com o Amazon Chime .....	114
Perfis vinculados ao serviço .....	115
Perfis de serviço .....	115
Exemplos de políticas baseadas em identidade .....	115
Práticas recomendadas de política .....	116
Usar o console do Amazon Chime .....	117
Permita que os usuários tenham acesso total ao Amazon Chime .....	118
Permitir que os usuários visualizem suas próprias permissões .....	119
Permitir que os usuários tenham acesso a ações de gerenciamento de usuário .....	120
AWS política gerenciada: AmazonChimeVoiceConnectorServiceLinkedRolePolicy .....	122
Atualizações do Amazon Chime para AWS políticas gerenciadas .....	122
Solução de problemas .....	123
Não tenho autorização para executar uma ação no Amazon Chime .....	124
Não estou autorizado a realizar iam: PassRole .....	124
Quero permitir que pessoas fora da minha AWS conta acessem meus recursos do Amazon Chime .....	125
Uso de perfis vinculados ao serviço .....	125
Usar funções com dispositivos compartilhados .....	126
Usar perfis com transcrição ao vivo .....	128
Usar perfis com pipeline de mídia .....	131
Registro em log e monitoramento .....	133
Monitoramento com CloudWatch .....	134
Automatizando com EventBridge .....	147
Registrar em log de chamadas de API do serviço .....	152
Validação de conformidade .....	154

---

Resiliência .....	156
Segurança da infraestrutura .....	156
Noções básicas sobre as atualizações automáticas do Amazon Chime .....	157
Histórico de documentos .....	159

Aviso de fim do suporte: em 20 de fevereiro de 2026, AWS encerrará o suporte para o serviço Amazon Chime. Depois de 20 de fevereiro de 2026, você não poderá mais acessar o console do Amazon Chime ou os recursos do aplicativo Amazon Chime. Para obter mais informações, acesse a [postagem do blog](#). Nota: Isso não afeta a disponibilidade do serviço [Amazon Chime SDK](#).

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.

# O que é o Amazon Chime?

O Amazon Chime é um serviço de comunicação que transforma reuniões online com um aplicativo seguro e abrangente. O Amazon Chime funciona perfeitamente em todos os dispositivos, de maneira que você possa se manter conectado. Você pode usar o Amazon Chime em reuniões online, videoconferência, chamadas e chat. Você também pode compartilhar conteúdo, dentro e fora da organização. O Amazon Chime é um serviço totalmente gerenciado que é executado com segurança na AWS nuvem, o que libera a TI da implantação e do gerenciamento de infraestruturas complexas.

Para obter mais informações, consulte [Amazon Chime](#).

## Visão geral da administração

Como administrador, você usa o [console do Amazon Chime](#) para realizar as principais tarefas, como criar contas do Amazon Chime e gerenciar usuários e permissões. Para acessar o console do Amazon Chime e criar uma conta de administrador do Amazon Chime, primeiro crie uma conta. AWS Para obter mais informações, consulte [Pré-requisitos para administradores de sistema do Amazon Chime](#).

## Como começar

Depois de concluir os [Pré-requisitos para administradores de sistema do Amazon Chime](#), você pode criar e configurar sua conta administrativa do Amazon Chime e adicionar usuários a ela. Selecione permissões Basic ou Pro para os usuários.

Você estiver pronto para começar a usar agora, consulte o seguinte tutorial:

- [Conceitos básicos](#)

Para obter mais informações sobre as permissões e o acesso de usuários, consulte [Gerenciar as permissões e o acesso do usuário](#). Para obter mais informações sobre os recursos que os usuários com permissões Pro e Basic podem acessar, consulte [Planos e preços](#).

## Preços

O Amazon Chime fornece preços baseados no uso. Você paga apenas pelos usuários com permissões Pro que organizam reuniões e apenas nos dias em que essas reuniões são realizadas. Os participantes da reunião e os usuários do chat não serão cobrados.

Não há cobrança por usuários com permissões Basic. Os usuários Basic não podem hospedar reuniões, mas podem participar de reuniões e usar o chat. Para obter mais informações sobre a definição de preço e os recursos que os usuários com permissões Pro e Basic podem acessar, consulte [Planos e preços](#).

## Recursos

Para obter mais informações sobre o Amazon Chime, consulte os seguintes recursos:

- [Central de ajuda do Amazon Chime](#)
- [Vídeos de treinamento do Amazon Chime](#)

# Guia dos recursos de transição do Amazon Chime

Após uma análise cuidadosa, decidimos encerrar o suporte para o serviço Amazon Chime, incluindo os recursos de Business Calling, a partir de 20 de fevereiro de 2026. O Amazon Chime não aceitará mais novos clientes a partir de 19 de fevereiro de 2025. Como cliente atual com uma conta Amazon Chime Team ou Enterprise criada antes de 19 de fevereiro de 2025, você pode continuar usando os recursos do Amazon Chime, incluindo chamadas comerciais, agendamento e hospedagem de reuniões, adição e gerenciamento de usuários e outros recursos suportados pelo console administrativo do Amazon Chime. Depois de 20 de fevereiro de 2026, você não poderá mais gerenciar seus usuários, hospedar reuniões do Amazon Chime ou usar qualquer um dos recursos do Business Calling. Entre em contato Suporte se você não conseguir excluir seus dados antes de 20 de fevereiro de 2026.

## Note

Isso não afeta a disponibilidade do serviço [Amazon Chime SDK](#).

Esta página fornece instruções e melhores práticas para administradores e usuários de TI do Amazon Chime fazerem a transição para soluções alternativas de colaboração para atender às suas necessidades comerciais. Isso pode incluir soluções fornecidas por AWS, como [Wickr](#), ou por AWS parceiros, como Slack, Webex e Zoom. Visite o [AWS Marketplace](#) para obter mais informações sobre as soluções de nossos AWS parceiros.

## Recursos de transição para administradores do Amazon Chime

Os seguintes recursos de transição estão disponíveis para administradores do Amazon Chime.

### Relatórios de uso

Antes de fazer a transição para uma nova solução de colaboração, pode ser útil entender quem na sua organização são usuários ativos e quais recursos eles estão usando. Com os relatórios de uso do Amazon Chime, você pode obter informações de contato para alcançar seus usuários ativos, coletar casos de uso e compilar requisitos para uma nova solução.

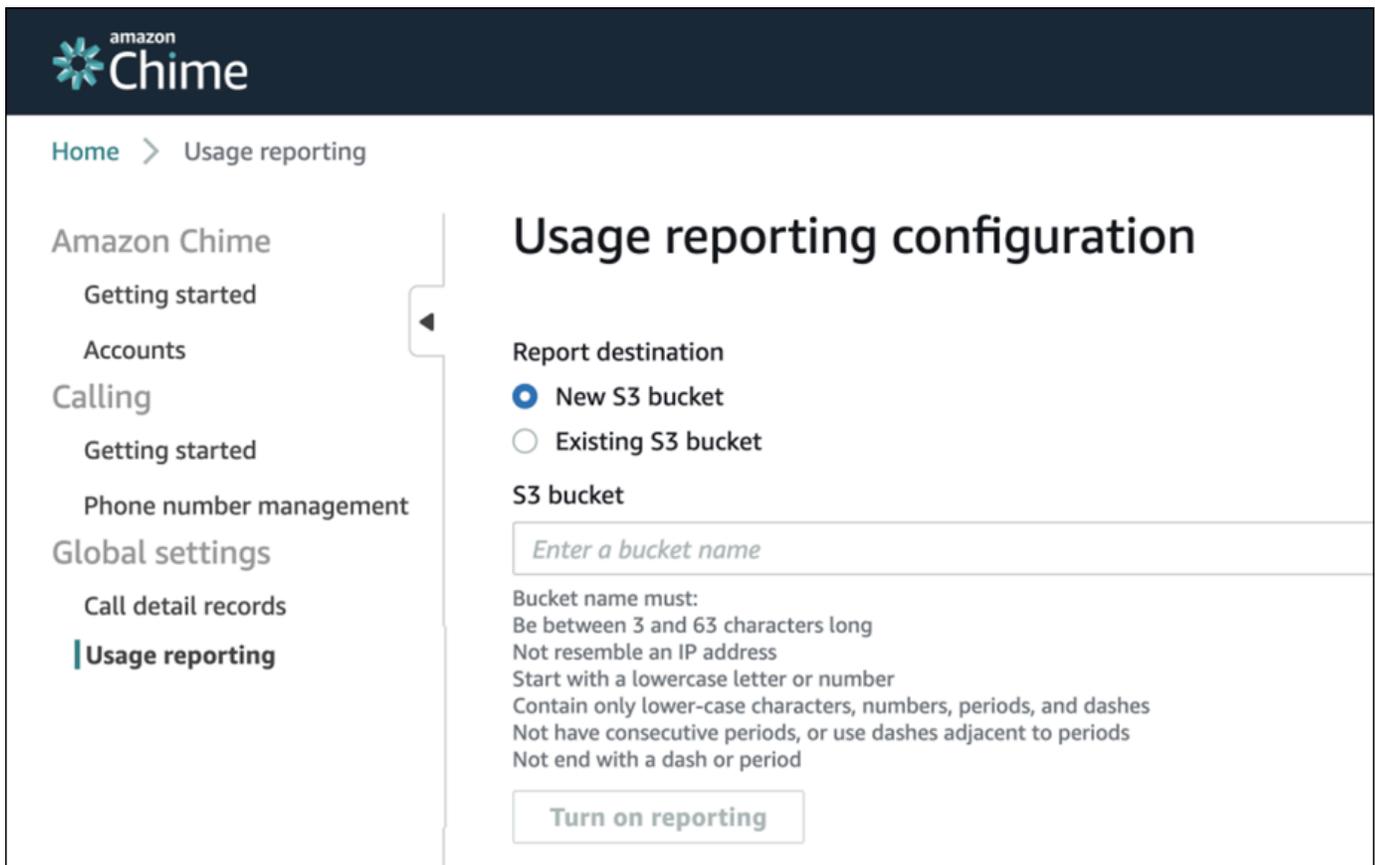
Os relatórios de uso fornecem informações sobre a atividade de cada usuário, incluindo nome, e-mail, status do registro, data de criação da conta do usuário, reuniões atendidas, reuniões

organizadas e mensagens enviadas. Esses dados estão disponíveis semanalmente para cada conta de equipe ou empresa que você criou no console do Amazon Chime. Os relatórios semanais mostrarão o uso por semanas, começando no domingo às 00:00 e terminando no sábado às 23:59. O processamento de dados pode atrasar os relatórios semanais até a segunda-feira da semana seguinte. Todas as datas e horários são apresentados usando o Tempo Universal Coordenado (UTC).

## Ativar relatórios de uso

Um bucket do Amazon Simple Storage Service (Amazon S3) é usado como destino para seus arquivos CSV de relatórios de uso semanais. Siga estas etapas para criar um bucket do Amazon S3 ou selecionar um existente em que o serviço Amazon Chime entregará os relatórios de uso semanais. Para obter mais informações sobre a criação de buckets do Amazon S3 ou sobre como navegar e gerenciar o acesso aos buckets do Amazon S3 existentes, acesse [Conceitos básicos do Amazon S3](#) no Guia do usuário do [Amazon S3](#).

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
2. Selecione Relatórios de uso em Configurações globais.
3. Para ativar os relatórios de uso do Amazon Chime para sua conta do Amazon Chime, primeiro crie ou selecione um bucket do Amazon S3.
  - a. Em Destino do relatório, escolha Novo bucket do S3 para criar um novo bucket e insira um nome seguindo as orientações listadas. Você também pode selecionar Bucket existente do S3 se já tiver um local onde deseja armazenar os arquivos.
  - b. Escolha Salvar para criar o novo bucket do S3 ou selecionar um bucket do S3 existente.
  - c. Os relatórios de uso agora estão ativados.
4. Seus relatórios de uso semanais começarão no domingo seguinte, à meia-noite UTC, e os arquivos serão armazenados no bucket do S3 identificado.

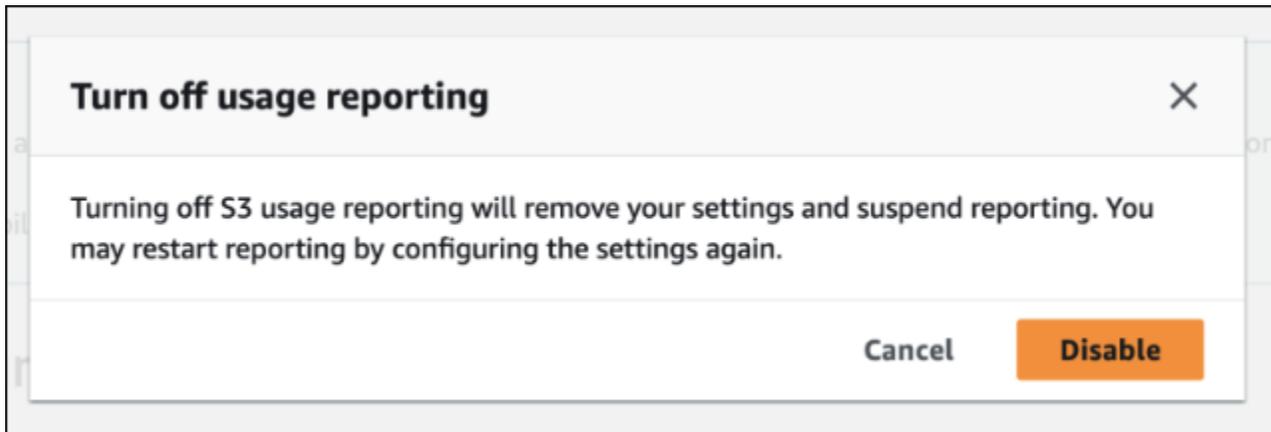


The screenshot shows the Amazon Chime console interface. At the top left is the Amazon Chime logo. Below it, a breadcrumb trail reads "Home > Usage reporting". A left-hand navigation menu lists several categories: "Amazon Chime", "Calling", "Global settings", and "Usage reporting" (which is highlighted with a blue bar). Under "Amazon Chime", there are links for "Getting started" and "Accounts". Under "Calling", there are links for "Getting started" and "Phone number management". Under "Global settings", there are links for "Call detail records" and "Usage reporting". The main content area is titled "Usage reporting configuration". It features a "Report destination" section with two radio buttons: "New S3 bucket" (selected) and "Existing S3 bucket". Below this is an "S3 bucket" section with a text input field containing the placeholder "Enter a bucket name". Underneath the input field, there are several lines of text providing requirements for the bucket name: "Bucket name must:", "Be between 3 and 63 characters long", "Not resemble an IP address", "Start with a lowercase letter or number", "Contain only lower-case characters, numbers, periods, and dashes", "Not have consecutive periods, or use dashes adjacent to periods", and "Not end with a dash or period". At the bottom of the configuration area is a button labeled "Turn on reporting".

## Desativar relatórios de uso

Você pode parar de gerar novos relatórios de uso a qualquer momento.

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/.](https://chime.aws.amazon.com/)
2. Selecione Relatórios de uso em Configurações globais.
3. Escolha Desativar relatórios.
4. Confirme que você deseja que o relatório seja interrompido escolhendo Desativar.



## Conteúdo do relatório

Os relatórios são gerados semanalmente. Conclua as etapas a seguir para visualizar os relatórios de uso.

1. Para visualizar seus dados, navegue até o console do Amazon S3.
2. Localize o nome do bucket.
3. O arquivo do relatório de uso semanal será colocado no seguinte local em seu bucket do S3:

```
Amazon-Chime-User-Activity-Reports/  
csv/<AWSaccountID>/<year>/<month>/<day>/  
<AmazonChimeAccountName>_<AmazonChimeAccountId>_<yyyymmdd>.csv
```

Por exemplo:

```
Amazon-Chime-User-Activity-Reports/csv/123456789012/2024/11/03/  
ExampleSales_12abcdef-34gh-56i7-89jk-01234lmnopq56_20241103.csv
```

4. Os seguintes campos estão incluídos em cada relatório:
  - Nome da conta da equipe ou empresa
  - Data de início da semana
  - Nome de exibição do usuário associado à sua conta do Amazon Chime
  - Endereço de e-mail do usuário
  - Status de registro do usuário
  - Data de criação da conta do usuário

- O número de reuniões que o usuário participou durante a semana
- O número de reuniões que o usuário organizou durante a semana
- O número de mensagens que o usuário enviou (publicações de 1:1, em grupo e na sala de bate-papo) durante a semana

account_name	week_start	display_name	email	registration_status	account_creation_date	last_login	meetings_attended	meetings_hosted	chat_sent
Example Sales	20241103	Alejandro Rosalez	alejandro@example.com	Registered	20170317	2024-10-19T07:04:40.000Z	10	5	14
Example Sales	20241103	Akua Mansa	akua@example.com	Suspended	20190227	2024-02-19T07:04:40.000Z	0	0	0
Example Sales	20241103	Ana Carolina Silva	ana@example.com	Registered	20220708	2024-10-08T20:58:35.000Z	25	11	73
Example Sales	20241103	Arnav Desai	arnav@example.com	Registered	20240901	2024-10-04T18:51:51.000Z	3	2	10
Example Sales	20241103	Carlos Salazar	carlos@example.com	Registered	20191203	2024-10-14T16:53:35.000Z	6	3	6
Example Sales	20241103	Diego Ramirez	diego@example.com	Registered	20190227	2024-10-02T10:23:54.000Z	12	6	291
Example Sales	20241103	Efua Owusu	efua@example.com	Registered	20220708	2024-10-10T23:31:08.000Z	0	0	33
Example Sales	20241103	John Stiles	john@example.com	Registered	20240901	2024-10-15T19:50:27.000Z	13	6	98
Example Sales	20241103	Jorge Souza	jorge@example.com	Registered	20191203	2024-10-10T18:55:08.000Z	2	0	0
Example Sales	20241103	Kwaku Mensah	kwaku@example.com	Registered	20190227	2024-10-28T00:08:20.000Z	1	0	0
Example Sales	20241103	Kwesi Manu	kwesi@example.com	Registered	20191203	2024-10-05T23:46:24.000Z	6	3	7

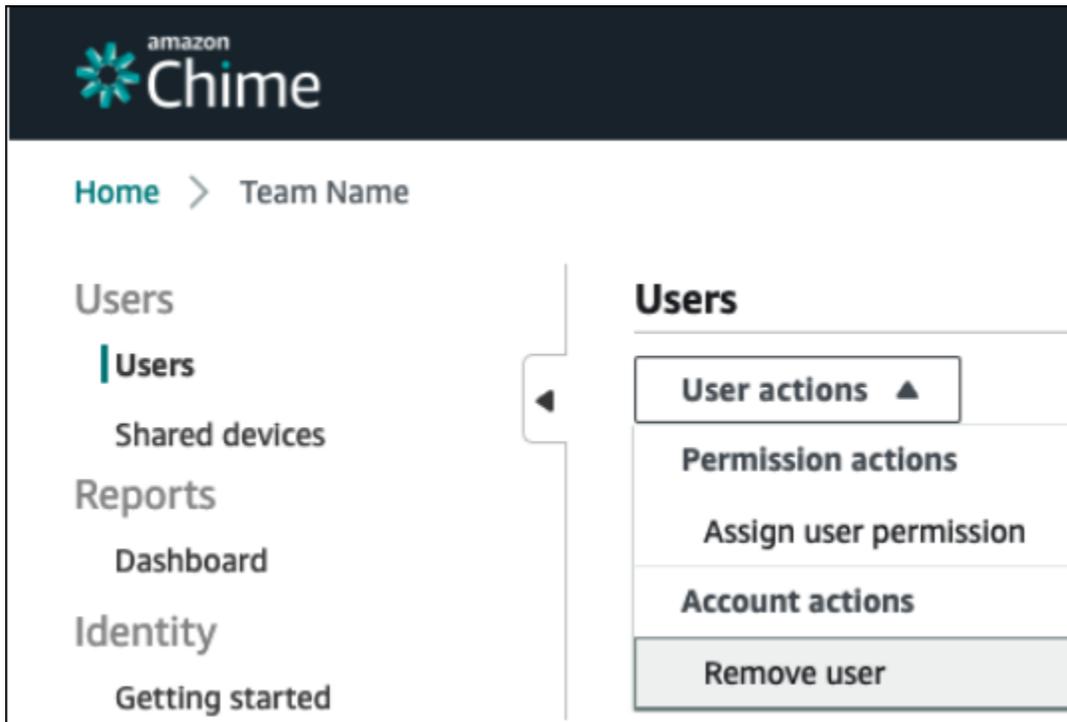
## Chamada comercial - portabilidade de números de telefone

Para ajudar na transição do Amazon Chime Business Calling para voz e SMS, você pode transferir seus números de telefone do Business Calling para outra operadora. Para ter mais informações, consulte [Transferindo números de telefone](#).

## Gerenciando suas contas de usuário - Contas de equipe

Você precisará remover todos os usuários antes de excluir sua conta da equipe. Ao configurar uma conta do Amazon Chime Team, você pode convidar novos usuários, definir seu nível de permissão (Pro ou Básico), definir regiões e outras configurações de conta e pagar para que os usuários organizem reuniões ou usem os recursos do Business Calling. Quando você remove um usuário de uma equipe do Amazon Chime, ele não pode usar recursos pagos, mas pode continuar usando recursos de mensagens e participar de reuniões. Quando você os remove, eles ainda têm acesso à conta de usuário do Amazon Chime e manterão seus contatos, histórico de mensagens individuais e de grupo e associação à sala de bate-papo.

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
2. Clique no nome da equipe abaixo do título Nome da conta.
3. Clique na caixa de seleção Selecionar tudo ou na caixa de seleção ao lado de usuários individuais.
4. Escolha Remover usuário no menu Ações do usuário.



Depois que seus usuários forem removidos, eles ainda poderão entrar e acessar o Amazon Chime, mas não poderão mais organizar reuniões. Se quiserem excluir sua conta do Amazon Chime, podem usar a opção excluir-me usando o Amazon Chime Assistant. Para obter mais informações, consulte [Usando o Amazon Chime Assistant para obter anexos ou solicitar que sua conta seja excluída](#) na Central de Ajuda do Amazon Chime.

## Gerenciando suas contas de usuário - Contas corporativas

Você precisará remover todos os domínios antes de excluir sua conta Enterprise. Você pode fazer o upgrade de uma conta Amazon Chime Team para uma conta Enterprise reivindicando seu domínio. Ao reivindicar seu domínio, você prova que sua empresa é proprietária do domínio e, portanto, possuirá os dados de seus usuários. Todos os usuários registrados do Amazon Chime com endereços de e-mail que correspondam aos seus domínios reivindicados serão inseridos na sua conta corporativa. Você define o nível de permissão (Pro ou Básico), define as configurações da conta, como regiões de reunião suportadas e regras de retenção de bate-papo, e paga para que seus usuários organizem reuniões ou usem os recursos do Business Calling. Você pode liberar todos os usuários escolhendo remover seu (s) domínio (s). Esse processo redefinirá o perfil de cada usuário e excluirá todos os dados, contatos, conversas individuais e em grupo, membros e histórico da sala de bate-papo. Depois que você cancelar a reivindicação de um domínio, os usuários não poderão mais entrar usando o SSO, organizar ou agendar reuniões, e o perfil associado ao endereço

de e-mail será redefinido. Se quiserem continuar usando o Amazon Chime, podem criar uma nova conta seguindo as instruções fornecidas na página de introdução do [Amazon Chime](#). Depois que todos os domínios forem removidos, você poderá excluir sua conta Enterprise.

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
2. Escolha o nome de uma conta corporativa na coluna Nome da conta.
3. Escolha Domínios em Identidade.
4. Escolha Remover.
5. Quando solicitado, analise os resultados da conclusão dessa tarefa e clique na caixa de seleção ao lado de Eu entendo que essa ação não pode ser revertida.
6. Selecione Remover.

### Remove "example.com" domain ✕

You are about to remove this domain from your Amazon Chime account.

The following disruptive actions will occur to the users in this domain:

- will be suspended.
- be immediately be signed out of all devices.
- lose their ability to access Amazon Chime.
- lose their ability to host meetings, including those that have already been scheduled.
- if a user has been assigned a phone number, it will be unassigned and available in your account's phone number management inventory.

After 90 days, users in this domain will be deleted. Learn more about [removing domains](#).

I understand that this action cannot be reversed.

Cancel Remove

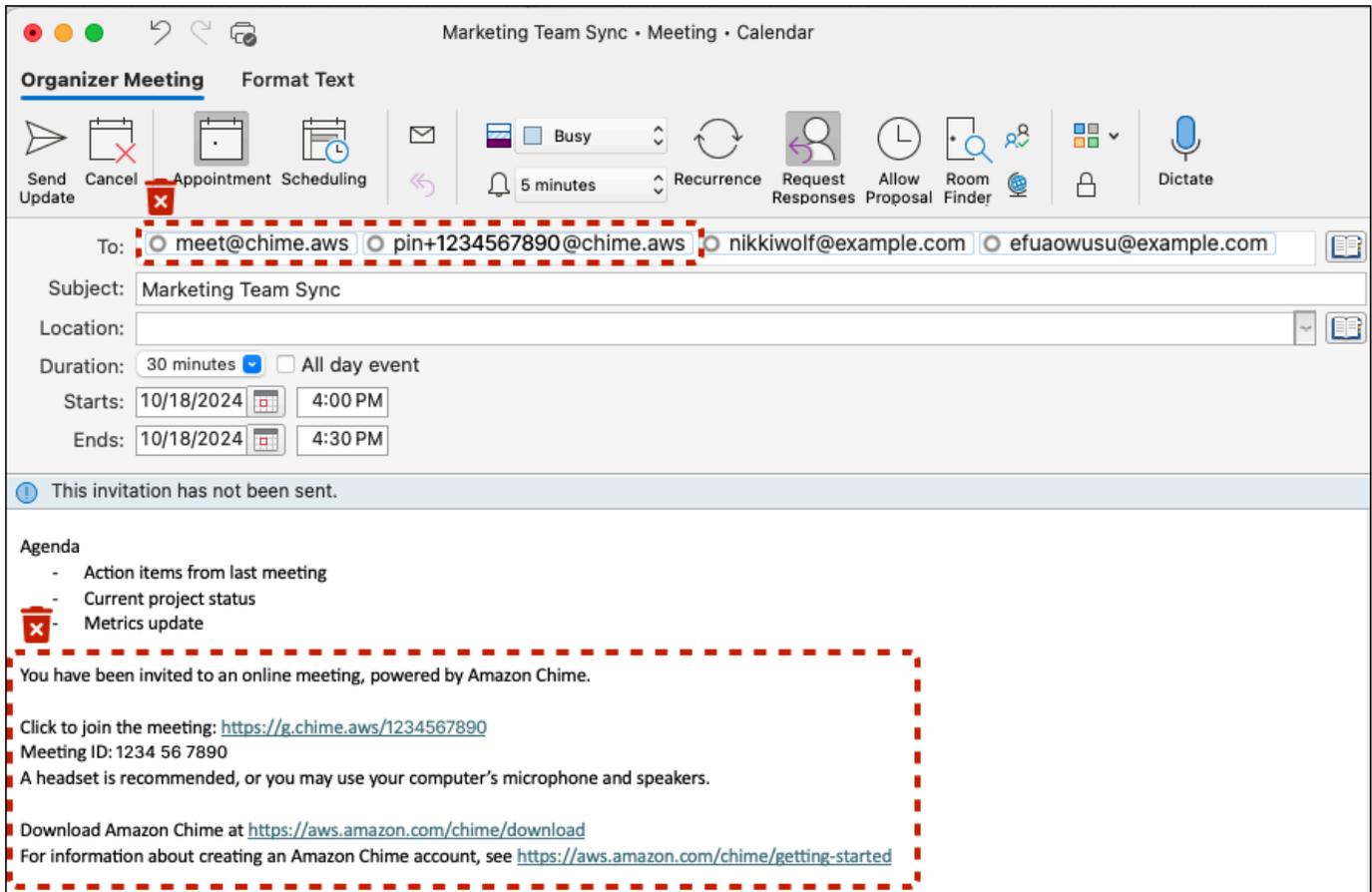
## Recursos de transição para usuários do Amazon Chime

Os seguintes recursos de transição estão disponíveis para administradores do Amazon Chime.

### Usuários Pro - Removendo o Amazon Chime dos seus convites para reuniões

O Amazon Chime liga automaticamente para os participantes da reunião que estão conectados aos seus clientes Amazon Chime quando você tem permissões do Amazon Chime Pro e convida para suas reuniões. `meet@chime.aws` Exclua sua reunião e recrie o convite usando a nova solução ou conclua o procedimento a seguir para remover os detalhes da reunião do Amazon Chime de uma reunião existente em seu calendário.

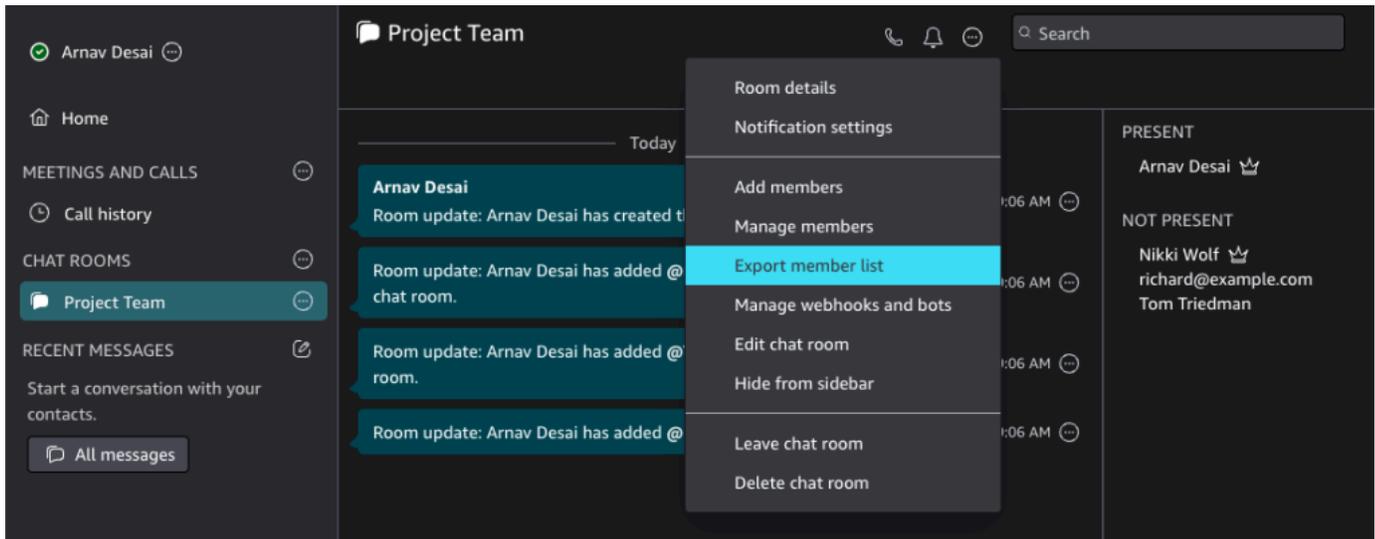
1. Abra seu aplicativo de calendário (não um aplicativo de calendário móvel).
2. Abra uma série recorrente ou uma reunião.
3. Siga as etapas a seguir para remover o Amazon Chime (e a chamada automática) e adicionar as instruções de reunião da nova solução:
  - a. Remova a `meet@chime.aws` e `pin+<meetingid>@chime.aws` do campo Para:.
  - b. Remova as instruções de reunião do Amazon Chime do corpo do convite.
  - c. Se você tiver uma nova solução de reunião, gere novas instruções de reunião e adicione-as ao corpo.
4. Envie o convite e não se esqueça de escolher enviar a atualização para todos.
5. Sua reunião não deve mais aparecer na página inicial do Amazon Chime em Próximas reuniões e não haverá nenhum toque automático do Amazon Chime para seus participantes.



## Administradores da sala de bate-papo - Obtenha uma lista de membros

O Amazon Chime fornece salas de bate-papo para até 10.000 membros. Quando você muda para uma nova solução de mensagens, pode ser útil poder entrar em contato com os membros em sua sala do Amazon Chime para recriar a sala de bate-papo em sua nova solução. Se você for administrador da sala de bate-papo, poderá exportar o nome, o endereço de e-mail e a função de cada membro da sala de bate-papo concluindo o procedimento a seguir.

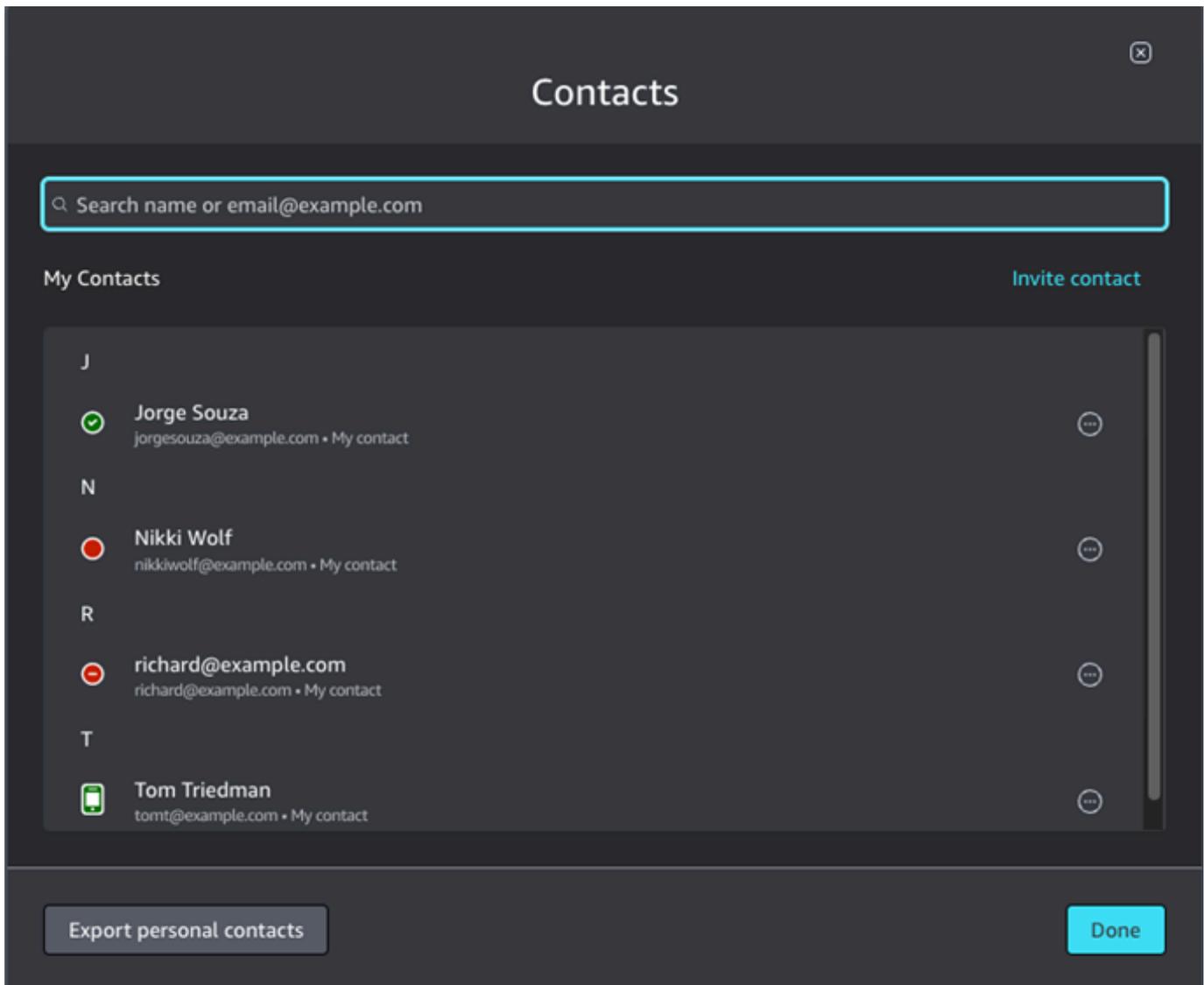
1. [Faça login em um cliente Amazon Chime para Windows, macOS ou web](#). Isso não está disponível usando os clientes móveis.
2. Navegue até uma sala de bate-papo em que você tenha a função de administrador.
3. Em Configurações da sala (o ícone ↓), escolha Exportar lista de membros.
4. Você será solicitado a salvar o arquivo CSV em seu computador se estiver usando o cliente Windows ou macOS. Se você estiver executando essa ação a partir do [cliente web](#), a lista de membros será salva na sua pasta de downloads. O nome do arquivo padrão incluirá o nome da sala.



## Usuários do Amazon Chime - Exporte seus contatos pessoais

O Amazon Chime fornece aos usuários uma lista de contatos pessoais (com até 100 contatos). Você adiciona informações do usuário do Amazon Chime à sua lista de contatos pessoais ao convidá-los ou ao usar a ação Adicionar aos contatos exibida durante as reuniões na lista de contatos, na sua lista de contatos, ou ao escolher a ação Adicionar aos contatos ao lado do nome deles nas listas de Favoritos ou Mensagens recentes. Quando você muda para uma nova solução de mensagens, pode ser útil manter as informações do usuário de pessoas de fora da sua empresa ou de outras pessoas que você adicionou aos seus contatos pessoais. O procedimento a seguir permite que você salve nomes, endereços de e-mail e números de telefone relevantes se você estiver usando o Business Calling.

1. [Faça login em um cliente Amazon Chime para Windows, macOS ou web](#). Isso não está disponível usando os clientes móveis.
2. Navegue até Contatos no menu superior quando estiver usando um cliente Windows ou macOS ou Exibir meus contatos em Ações rápidas no cliente [web](#).
3. Escolha Exportar contatos pessoais.
4. Você será solicitado a salvar o arquivo CSV em seu computador se estiver usando o cliente Windows ou macOS. Se você estiver executando essa ação a partir do [cliente web](#), a lista de membros será salva na sua pasta Downloads.



## Resumo

Organizações com pelo menos uma conta Amazon Chime Team ou Enterprise podem continuar usando os recursos Amazon Chime e Business Calling até 20 de fevereiro de 2026, quando o suporte ao serviço terminará. Os recursos que não serão mais suportados incluem agendamento e hospedagem de reuniões, adição e gerenciamento de usuários e outros recursos disponíveis usando o console do Amazon Chime.

## Recursos adicionais

- [Site do Amazon Chime](#)

- [Guia do usuário do Amazon Chime](#)
- [Central de ajuda do Amazon Chime](#)
- Saiba mais sobre as [soluções AWS Wickre os AWS parceiros](#).
- Se precisar de ajuda ou tiver feedback, entre em contato [Suporte](#).

# Pré-requisitos para administradores de sistema do Amazon Chime

Você deve ter uma AWS conta para acessar o [console do Amazon Chime](#) e criar uma conta de administrador do Amazon Chime.

## Como criar uma conta da Amazon Web Services

Antes de criar uma conta de administrador do Amazon Chime, você deve primeiro criar uma conta da AWS .

Tópicos

- [Inscreva-se para um Conta da AWS](#)
- [Criar um usuário com acesso administrativo](#)

## Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra a <https://portal.aws.amazon.com/billing/inscrição>.
2. Siga as instruções online.

Parte do procedimento de inscrição envolve receber uma ligação ou mensagem de texto e inserir um código de verificação no teclado do telefone.

Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWS é criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar [tarefas que exigem acesso de usuário-raiz](#).

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando <https://aws.amazon.com/e> escolhendo Minha conta.

## Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

### Proteja seu Usuário raiz da conta da AWS

1. Faça login [AWS Management Console](#) como proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira a senha.

Para obter ajuda ao fazer login usando o usuário-raiz, consulte [Fazer login como usuário-raiz](#) no Guia do usuário do Início de Sessão da AWS .

2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

Para obter instruções, consulte [Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz \(console\) no Guia](#) do usuário do IAM.

### Criar um usuário com acesso administrativo

1. Habilita o Centro de Identidade do IAM.

Para obter instruções, consulte [Habilitar o AWS IAM Identity Center](#) no Guia do usuário do AWS IAM Identity Center .

2. No Centro de Identidade do IAM, conceda o acesso administrativo a um usuário.

Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte [Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM](#) no Guia AWS IAM Identity Center do usuário.

### Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com o seu usuário do Centro de Identidade do IAM, use o URL de login enviado ao seu endereço de e-mail quando o usuário do Centro de Identidade do IAM foi criado.

Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte [Como fazer login no portal de AWS acesso](#) no Guia Início de Sessão da AWS do usuário.

## Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

Para obter instruções, consulte [Criar um conjunto de permissões](#) no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

Para obter instruções, consulte [Adicionar grupos](#) no Guia do usuário do AWS IAM Identity Center .

Para obter mais informações sobre como configurar uma conta de administrador do Amazon Chime, consulte [Conceitos básicos](#).

# Conceitos básicos

A maneira mais fácil de os usuários começarem a usar o Amazon Chime é fazer download e usar o Amazon Chime versão Pro gratuitamente por 30 dias. Para obter mais informações, consulte [Fazer download do Amazon Chime](#).

## Comprar o Amazon Chime

Para continuar usando o Amazon Chime versão Pro após o período de avaliação gratuita de 30 dias, você deve criar uma conta de administrador do Amazon Chime e adicionar usuários a ela. Para começar, você deve primeiro preencher o [Pré-requisitos para administradores de sistema do Amazon Chime](#), que inclui a criação de uma AWS conta. Em seguida, você pode criar e configurar uma conta de administrador do Amazon Chime e adicionar usuários a ela concluindo as tarefas a seguir.

## Tarefas

- [Etapa 1: Criar uma conta de administrador do Amazon Chime](#)
- [Etapa 2 \(opcional\): definir configurações da conta](#)
- [Etapa 3: adicionar usuários à conta](#)
- [\(Opcional\) Configurar números de telefone da sua conta do Amazon Chime](#)

## Etapa 1: Criar uma conta de administrador do Amazon Chime

Depois de concluir os [Pré-requisitos para administradores de sistema do Amazon Chime](#), você pode criar uma conta de administrador do Amazon Chime.

### Como criar uma conta de administrador do Amazon Chime

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
2. Na página Accounts (Contas), escolha New account (Nova conta).
3. Em Account Name (Nome da conta), insira um nome para a conta e selecione Create account (Criar conta).
4. (Opcional) Escolha se deseja permitir que o Amazon Chime selecione a AWS região ideal para suas reuniões de todas as regiões disponíveis ou use somente as regiões que você selecionar. Para obter mais informações, consulte [Gerenciar as configurações da reunião](#).

## Etapa 2 (opcional): definir configurações da conta

Por padrão, as novas contas são criadas como contas de equipe. Se você preferir reivindicar um domínio e se conectar ao seu próprio provedor de identidades ou ao Okta SSO, poderá converter para uma conta empresarial. Para obter mais informações sobre os tipos de conta de equipe e empresarial, consulte [Escolher entre uma conta de equipe e uma conta empresarial do Amazon Chime](#).

Converter uma conta da equipe para uma conta corporativa

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
2. Em Contas, escolha o nome da conta.
3. Em Identity (Identidade), selecione Getting Started (Conceitos básicos).
4. Siga as etapas no console para reivindicar o domínio.
5. (Opcional) Siga as etapas no console para configurar o provedor de identidade e configurar o grupo de diretórios.

Para obter mais informações sobre como solicitar domínios, consulte [Reivindicar um domínio](#). Para obter mais informações sobre como configurar provedores de identidade, consulte [Conectar ao seu Active Directory](#) e [Conectar ao Okta SSO](#).

Você também pode iniciar ou interromper a permissão de políticas de conta para as opções, como o controle remoto de telas compartilhadas e o recurso call me do Amazon Chime.

Para configurar as políticas de conta

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
2. Na página Accounts (Contas), selecione o nome da conta para configurar.
3. Em Settings (Configurações), escolha Meetings (Reuniões).
4. Em Policies (Políticas), selecione ou desmarque as opções de políticas da conta que você deseja permitir ou cancelar a permissão.
5. Escolha Alterar.

Para obter mais informações, consulte [Gerenciar as configurações da reunião](#).

## Etapa 3: adicionar usuários à conta

Depois que a conta de equipe do Amazon Chime for criada, convide a si mesmo e seus usuários a participarem. Se você estiver atualizando sua conta para uma conta empresarial, não será necessário convidar os usuários. Em vez disso, atualize para uma conta empresarial e reivindique seu domínio. Para obter mais informações, consulte [Etapa 2 \(opcional\): definir configurações da conta](#).

Como adicionar usuários à conta do Amazon Chime

1. [Abra o console do Amazon Chime em](https://chime.aws.amazon.com/)<https://chime.aws.amazon.com/>.
2. Na página Accounts (Contas), selecione o nome da sua conta.
3. Na página Users, escolha Invite users.
4. Insira os endereços de e-mail dos usuários para convidar, incluindo você mesmo, e selecione Invite users (Convidar usuários).

Os usuários convidados receberão convites por e-mail para ingressar na conta de equipe do Amazon Chime criada por você. Quando eles registrarem suas contas de usuário do Amazon Chime, receberão permissões Pro por padrão, e a avaliação de 30 dias será encerrada. Se eles já tiverem uma conta de usuário do Amazon Chime cadastrada com o endereço de e-mail de trabalho, poderão continuar usando essa conta. Eles também podem baixar o aplicativo cliente Amazon Chime a qualquer momento, escolhendo Baixar Amazon Chime e fazendo login em sua conta de usuário.

Você só será cobrado por um usuário com permissões Pro quando ele hospedar uma reunião. Não há cobrança por usuários com permissões Basic. Os usuários Basic não podem hospedar reuniões, mas podem participar de reuniões e usar o chat. Para obter mais informações sobre a definição de preço e os recursos que os usuários com permissões Pro e Basic podem acessar, consulte [Planos e preços](#).

Para alterar permissões de usuário

1. [Abra o console do Amazon Chime em](https://chime.aws.amazon.com/)<https://chime.aws.amazon.com/>.
2. Na página Accounts (Contas), selecione o nome da sua conta.
3. Na página Users (Usuários), selecione o usuário ou os usuários para os quais alterar as permissões.
4. Selecione User actions (Ações do usuário), Assign user permission (Atribuir permissão do usuário).

5. Em Permissions (Permissões), selecione Pro ou Basic.
6. Selecione Assign (Atribuir).

Você pode fornecer permissões de administrador a outros usuários, além de controlar o acesso deles ao console do Amazon Chime para a sua conta. Para obter mais informações, consulte [Identity and Access Management para o Amazon Chime](#).

## (Opcional) Configurar números de telefone da sua conta do Amazon Chime

As seguintes opções de telefone estão disponíveis para contas administrativas do Amazon Chime:

### Amazon Chime Business Calling

Permite que seus usuários enviem e recebam chamadas telefônicas e mensagens de texto diretamente do Amazon Chime. Provisione seus números de telefone no console do Amazon Chime ou transfira números de telefone existentes. Atribua os números de telefone aos seus usuários do Amazon Chime e conceda a eles permissões para enviar e receber chamadas telefônicas e mensagens de texto usando o Amazon Chime. Para ter mais informações, consulte [Gerenciar números de telefone no Amazon Chime](#) e [Transferir números de telefones existentes](#).

### Amazon Chime Voice Connector

Fornece serviço de entroncamento SIP para um sistema telefônico existente. Transfira números de telefone existentes ou provisione novos números de telefone no console do Amazon Chime. Para obter mais informações, consulte [Managing Amazon Chime Voice Connectors](#) no Guia de administração do SDK do Amazon Chime.

# Gerenciar suas contas do Amazon Chime

Você pode usar o Amazon Chime como um usuário individual ou como um grupo sem administradores. Mas se você quiser adicionar a funcionalidade de administrador ou comprar o Amazon Chime Pro, você deve criar uma conta do Amazon Chime no AWS Management Console. Para saber como criar uma conta de administrador do Amazon Chime ou para obter mais informações sobre a compra do Amazon Chime Pro, consulte [Conceitos básicos](#).

Para obter mais informações sobre os diversos tipos diferentes de contas de administrador do Amazon Chime, consulte [Escolher entre uma conta de equipe e uma conta empresarial do Amazon Chime](#). Para obter mais informações sobre como gerenciar uma conta de administrador existente, consulte os tópicos a seguir.

## Tópicos

- [Escolher entre uma conta de equipe e uma conta empresarial do Amazon Chime](#)
- [Reivindicar um domínio](#)
- [Converter uma conta de equipe em uma conta empresarial](#)
- [Renomear sua conta](#)
- [Excluir sua conta](#)
- [Gerenciar as configurações da reunião](#)
- [Gerenciar políticas de retenção de bate-papo](#)
- [Restaurando mensagens de bate-papo](#)
- [Excluindo mensagens de bate-papo](#)
- [Conectar ao seu Active Directory](#)
- [Conectar ao Okta SSO](#)
- [Implantar a extensão do Amazon Chime para Outlook](#)
- [Configurar o aplicativo Amazon Chime Meetings para Slack](#)

# Escolher entre uma conta de equipe e uma conta empresarial do Amazon Chime

Ao criar uma conta de administrador do Amazon Chime, você escolhe se quer criar uma conta de equipe ou uma conta corporativa. Para obter mais informações sobre como criar uma conta de administrador do Amazon Chime, consulte [Conceitos básicos](#).

## Conta de equipe

Com uma conta de equipe, você pode convidar usuários e conceder a eles permissões do Amazon Chime Pro sem reivindicar um domínio de e-mail. Para obter mais informações sobre as permissões Pro e Basic, consulte [Planos e preços](#).

Você pode convidar usuários de qualquer domínio de e-mail que não tenha sido reivindicado por outra organização. Você paga pelos usuários somente quando eles organizam reuniões. Os usuários da sua conta de equipe podem usar o aplicativo Amazon Chime para pesquisar e entrar em contato com outros usuários do Amazon Chime que estejam registrados na mesma conta. Também recomendamos uma conta de equipe para pagamento para usuários do Pro que não pertencem à sua organização.

## Conta empresarial

Com uma conta empresarial, você tem maior controle sobre os usuários dos domínios da organização. Você pode optar por se conectar ao seu próprio chats ou ao Okta SSO para autenticar e atribuir permissões Pro ou Basic. O Amazon Chime também oferece suporte ao Microsoft Active Directory.

Para criar uma conta empresarial, você deve reivindicar pelo menos um domínio de e-mail. Isso garante que todos os usuários que entrem em Amazon Chime por meio dos domínios reivindicados sejam incluídos na conta do Amazon Chime gerenciada de maneira centralizada. As contas empresariais são necessárias para gerenciar os usuários pode meio de uma integração com o diretório compatível. Para ter mais informações, consulte [Reivindicar um domínio](#) e [Conectar ao seu Active Directory](#).

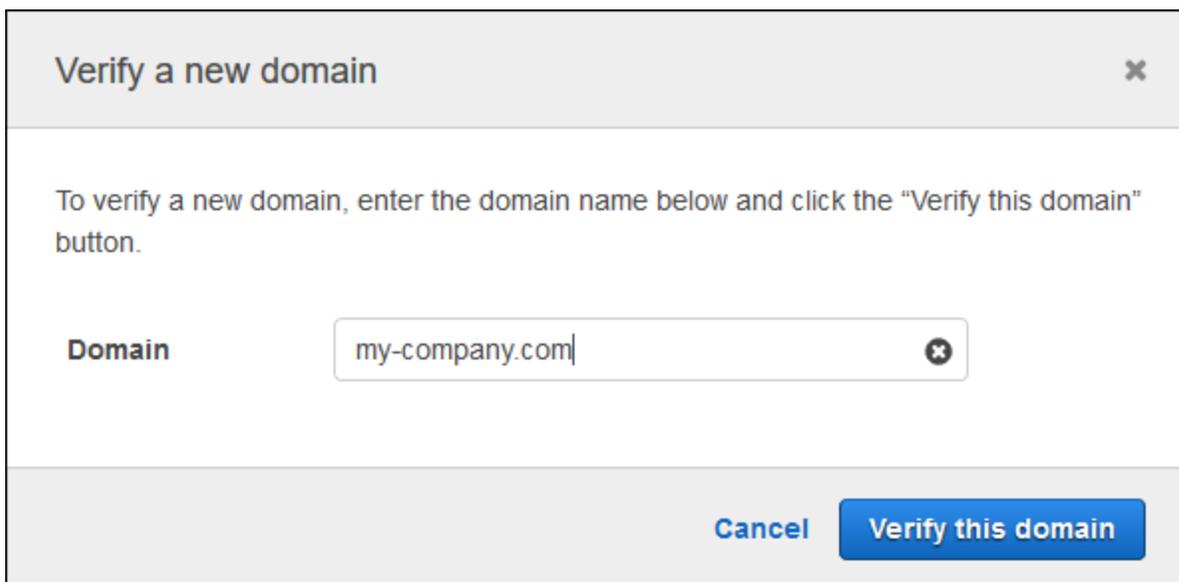
Você também pode gerenciar a ativação e suspensão de usuários da sua conta empresarial. Para obter mais informações, consulte [Gerenciar as permissões e o acesso do usuário](#).

## Reivindicar um domínio

Para criar uma conta empresarial e se beneficiar do maior controle que ela fornece sobre sua conta e seus usuários, você precisa reivindicar pelo menos um domínio de e-mail.

Para solicitar um domínio

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
2. Na página Contas, selecione o nome da conta de equipe.
3. No painel de navegação, escolha Identity (Identidade), Domains (Domínios).
4. Na página Domains (Domínios), escolha Claim a new domain (Solicitar um novo domínio).
5. Em Domain (Domínio), digite o domínio que sua organização usa para endereços de e-mail. Escolha Verify this domain.



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 as instruções na tela para adicionar um registro TXT ao servidor DNS do seu domínio. De modo geral, o processo envolve o login na conta do seu domínio, a localização dos registros de DNS do seu domínio e a adição de um registro TXT com o nome e o valor fornecidos pelo Amazon Chime. Para obter mais informações sobre como atualizar os registros de DNS do seu domínio, consulte a documentação do seu provedor DNS ou registrador de nomes de domínio.

O Amazon Chime verifica a existência desse registro para confirmar se você é o proprietário do domínio. Depois que o domínio é verificado, seu status muda de Pending verification para Verified.

**Note**

A propagação da alteração e da verificação de DNS pelo Amazon Chime pode levar até 24 horas.

7. Se sua organização usa domínios ou subdomínios adicionais para endereços de e-mail, repita este procedimento para cada domínio.

Para obter mais informações sobre a solução de problemas de reivindicações de domínio, consulte [Por que minha solicitação de reivindicação de domínio não está sendo verificada?](#).

## Converter uma conta de equipe em uma conta empresarial

Para converter uma conta de equipe em uma conta empresarial, reivindique um ou mais domínios de e-mail no console do Amazon Chime. Para obter mais informações sobre as diferenças entre as contas de equipe e empresarial, consulte [Escolher entre uma conta de equipe e uma conta empresarial do Amazon Chime](#). Para obter mais informações sobre como solicitar um domínio, consulte [Reivindicar um domínio](#).

Converter uma conta da equipe para uma conta corporativa

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
2. Em Contas, escolha o nome da conta.
3. Em Identity (Identidade), selecione Getting Started (Conceitos básicos).
4. Siga as etapas no console para reivindicar o domínio.
5. (Opcional) Siga as etapas no console para configurar o provedor de identidade e configurar o grupo de diretórios.

Depois que sua conta for convertida em uma conta corporativa, você poderá decidir se deseja conectar uma instância do Active Directory por meio de AWS Directory Service. Conectar-se a uma instância do Active Directory permite que seus usuários entrem no Amazon Chime usando suas credenciais do Active Directory. Para obter mais informações, consulte [Conectar ao seu Active Directory](#).

Se você não se conectar a uma instância do Active Directory, seus usuários farão login por meio do Amazon Chime usando o Login with Amazon (LWA) ou as credenciais de sua conta da Amazon.com.

## Renomear sua conta

As etapas a seguir explicam como renomear a equipe e as contas corporativas do Amazon Chime que você administra. O nome escolhido aparece nos e-mails que convidam os usuários a se juntarem ao Amazon Chime.

Para renomear sua conta

1. [Abra o console do Amazon Chime em](https://chime.aws.amazon.com/)<https://chime.aws.amazon.com/>.

A página Contas aparece por padrão.

2. Na coluna Nome da conta, selecione a conta que você deseja renomear.
3. No painel esquerdo, em Configurações, escolha Conta.

A página de Resumo da conta é exibida.

4. Abra a lista de Ações da conta e escolha Renomear conta.

A caixa de diálogo Renomear conta é exibida.

5. Insira o novo nome da conta e escolha Salvar.

## Excluir sua conta

Se você excluir sua AWS conta no AWS Management Console, suas contas do Amazon Chime serão excluídas automaticamente. Como alternativa, você pode usar o console do Amazon Chime para excluir uma conta de equipe ou empresarial do Amazon Chime.

### Note

Os usuários que não são gerenciados em uma conta empresarial ou de empresa podem solicitar sua exclusão usando o comando "Delete me" do assistente do Amazon Chime. Para obter mais informações, consulte [Using the Amazon Chime Assistant](#).

Como excluir uma conta de equipe

1. [Abra o console do Amazon Chime em](https://chime.aws.amazon.com/)<https://chime.aws.amazon.com/>.
2. Selecione a conta na coluna Account name e, em seguida, Account sob Settings.

3. No painel de navegação, a página Users será exibida.
4. Selecione os usuários e selecione User actions (Ações do usuário), Remove user (Remover usuário).
5. No painel de navegação, escolha Accounts, Account actions e Delete account.
6. Confirme que você deseja excluir sua conta.

Quando você remove usuários de uma conta de equipe, eles continuarão conseguindo entrar, ter acesso aos dados de mensagens e salas de bate-papo e participar de reuniões. Se esses usuários quiserem excluir todos os seus dados e suas contas do Amazon Chime, eles podem optar por solicitar a exclusão usando o comando “Excluir-me” do Amazon Chime Assistant. Para obter mais informações, consulte [Usando o Amazon Chime Assistant no Guia](#) do usuário do Amazon Chime.

Depois de remover todos os seus usuários, você pode excluir sua conta do Amazon Chime Team e excluir todos os dados que não são do usuário. Isso inclui o encerramento de Conta da AWS contas individuais do Amazon Chime ou de usuários não gerenciados do Amazon Chime. Isso exclui dados que não sejam de conteúdos relacionados a contas de usuário e ao uso do Amazon Chime (atributos de serviço abordados no contrato do cliente) que são gerados pelo Amazon Chime.

#### Como excluir uma conta empresarial

1. Remova os domínios.

#### Note

Quando você remove um domínio, ocorre o seguinte:

- Os usuários associados ao domínio são desconectados imediatamente de todos os dispositivos e perdem acesso a todos os contatos, conversas de bate-papo e salas de bate-papo.
- As reuniões agendadas por usuários nesse domínio não são mais iniciadas.
- Os usuários suspensos continuam a ser exibidos com o status Suspended (Suspendido) nas páginas Users (Usuários) e User detail (Detalhes do usuário) e não podem acessar seus dados. Eles podem criar uma nova conta do Amazon Chime com seu endereço de e-mail.
- Os usuários registrados são exibidos como Released (Liberado) nas páginas Users (Usuários) e User detail (Detalhes do usuário) e não podem acessar seus dados. Eles podem criar uma nova conta do Amazon Chime com seu endereço de e-mail.

- Se você possui uma conta do Active Directory e remover um domínio que esteja associado ao endereço de e-mail principal de um usuário, o usuário não pode acessar o Amazon Chime, e seu perfil é excluído. Se você remove um domínio que está associado ao endereço de e-mail secundário de um usuário, ele não pode fazer login com esse endereço de e-mail, mas retém o acesso a seus contatos e dados do Amazon Chime.
- Se você possui uma conta empresarial OpenID connect (OIDC) e remover um domínio que esteja associado ao endereço de e-mail principal de um usuário, o usuário não pode acessar o Amazon Chime, e seu perfil é excluído.

2. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
3. Na página Contas, selecione o nome da conta de equipe.
4. No painel de navegação, selecione Settings, Domains.
5. Na página Domains (Domínios), selecione Remove domain (Remover domínio).
6. No painel de navegação, escolha Accounts, Account actions e Delete account.
7. Confirme que você deseja excluir sua conta.

O Amazon Chime exclui todos os dados de usuário ao excluir sua conta. Isso inclui o encerramento de uma AWS conta, contas individuais do Amazon Chime ou usuários não gerenciados do Amazon Chime. Isso exclui dados que não sejam de conteúdos relacionados a contas de usuário e ao uso do Amazon Chime (atributos de serviço abordados no contrato do cliente) que são gerados pelo Amazon Chime.

Para concluir a exclusão dos dados da sua conta, lembre-se de excluir todos os registros detalhados de chamadas do Business Calling e os relatórios de uso do Amazon Chime que tenham sido publicados no Amazon S3. Para obter mais informações, consulte [Gerenciar configurações globais no Amazon Chime](#).

## Gerenciar as configurações da reunião

Gerencie suas configurações da reunião no console do Amazon Chime.

### Configurações da política da reunião

Gerencie as políticas de conta no console do Amazon Chime, em Configurações, Reuniões. Escolha uma das seguintes opções de política.

## Ativar o controle compartilhado no compartilhamento de tela

Escolha se os usuários da sua organização poderão conceder controle compartilhado dos computadores deles durante as reuniões. Os participantes que solicitarem o controle compartilhado dos computadores de outros usuários receberão uma mensagem de erro indicando que o controle remoto não está disponível.

## Habilitar chamadas de saída para ingressar em reuniões

Ativa o recurso “Ligar para mim” do Amazon Chime. Esse recurso oferece aos participantes da reunião a opção de ingressar em reuniões por meio do recebimento de uma chamada telefônica do Amazon Chime.

## Configurações do aplicativo de reunião

Gerencie o acesso ao aplicativo de reunião em Configurações e Reuniões no console do Amazon Chime. Você pode escolher a seguinte opção:

Permita que os usuários façam login no Amazon Chime usando o aplicativo Amazon Chime Meetings para Slack

Essa opção permite que os usuários da sua organização façam login no Amazon Chime a partir do aplicativo Amazon Chime Meetings para Slack. Para obter mais informações, consulte [Configurar o aplicativo Amazon Chime Meetings para Slack](#).

## Configurações da região da reunião

Para melhorar a qualidade das reuniões e reduzir a latência, o Amazon Chime processa reuniões na região AWS ideal para todos os participantes. Você pode escolher se deseja que o Amazon Chime selecione a região ideal para uma reunião dentre todas as regiões disponíveis ou use somente as regiões selecionadas.

Você pode atualizar essa configuração nas configurações de Meetings (Reuniões) da sua conta a qualquer momento. Nas configurações de Reuniões, você também pode exibir a porcentagem de reuniões do Amazon Chime processadas em cada região.

Como atualizar as configurações da região da reunião

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
2. Na página Accounts (Contas), selecione o nome da conta.

3. No painel de navegação, selecione Settings (Configurações), Meetings (Reuniões).
4. Em Regions (Regiões), escolha uma das seguintes opções:
  - Usar todas as regiões disponíveis para garantir a qualidade da reunião: permite que o Amazon Chime otimize o processamento de reuniões para você.
  - Usar somente as regiões que eu seleciono: permite que você selecione as regiões no menu suspenso.
5. Escolha Salvar.

## Gerenciar políticas de retenção de bate-papo

Se você administra uma ou mais contas empresariais do Amazon Chime, você pode definir políticas de retenção de chat para o seguinte:

- As conversas de chat que incluem apenas membros de sua conta empresarial
- Salas de chat criadas pelos membros da sua conta empresarial

Uma política de retenção exclui automaticamente as mensagens com base no período definido por você. Você pode definir períodos que variam de um dia a 15 anos.

### Note

As contas empresariais do Amazon Chime têm um período de retenção de 90 dias. A política se aplica a conversas envolvendo usuários que pertencem à conta e a usuários que não pertencem à conta.

As políticas de retenção não se aplicam a:

- Conversas de chat que não incluem nenhum membro de conta empresarial do Amazon Chime
- Salas de chat criadas por usuários que não pertencem a uma conta empresarial ou de equipe do Amazon Chime

## Como as políticas de retenção afetam os usuários do Amazon Chime

As políticas de retenção definidas pelos administradores de contas empresariais afetam os usuários do Amazon Chime de forma diferente, dependendo do fato de os usuários fazerem parte da mesma

conta empresarial, de uma conta empresarial diferente, de uma conta de equipe, ou ainda, se os usuários não forem membros de conta alguma.

#### Conversas de bate-papo de membros da empresa

A tabela a seguir mostra como as políticas de retenção afetam as conversas de bate-papo para membros da conta empresarial.

Caso a conversa de bate-papo incluua...	A política de retenção será...
Somente outros membros da conta empresarial do usuário	Definida pelo administrador do usuário
Qualquer pessoa fora da conta empresarial do usuário	Definida automaticamente para 90 dias

#### Salas de bate-papo de membros da empresa

A tabela a seguir mostra como as políticas de retenção afetam as salas de bate-papo para membros da conta empresarial.

Se a sala de bate-papo for criada por...	A política de retenção será...
Um membro da conta empresarial do usuário	Definida pelo administrador do usuário
Outro membro da conta empresarial	Definida pelo administrador da outra conta
Um membro de conta não empresarial	Não aplicável

#### Conversas de bate-papo com membros da equipe

A tabela a seguir mostra como as políticas de retenção afetam as conversas de bate-papo para membros da conta de equipe.

Caso a conversa de bate-papo incluua...	A política de retenção será...
Somente usuários que não são membros de uma conta empresarial	Não aplicável

Caso a conversa de bate-papo incluua...	A política de retenção será...
Ao menos um membro de uma conta empresarial	Definida automaticamente para 90 dias

### Salas de bate-papo de membros da equipe

A tabela a seguir mostra como as políticas de retenção afetam as salas de bate-papo para membros da conta de equipe.

Se a sala de bate-papo for criada por...	A política de retenção será...
Um usuário de conta de equipe	Não aplicável
Qualquer pessoa que não seja membro da conta empresarial	Não aplicável
Um membro de uma conta empresarial	Definida pelo administrador da conta empresarial

Os usuários do Amazon Chime que não são membros de uma conta empresarial ou de equipe estão sujeitos apenas às políticas de retenção de sala de chat em salas de chat criadas por um membro de uma conta empresarial.

Conversas de bate-papo com destinatários que não pertencem a uma conta empresarial ou de equipe

A tabela a seguir mostra como as políticas de retenção afetam as conversas de chat para usuários que não são membros de uma conta de empresa ou de equipe do Amazon Chime.

Caso a conversa de bate-papo incluua...	A política de retenção será...
Somente usuários que não são membros de uma conta empresarial	Não aplicável
Ao menos um membro de uma conta empresarial	Definida automaticamente para 90 dias

Salas de bate-papo criadas por usuários que não pertencem a uma conta empresarial ou de equipe

A tabela a seguir mostra como as políticas de retenção afetam as salas de chat para usuários que não são membros de uma conta de empresa ou de equipe do Amazon Chime.

Se a sala de bate-papo for criada por...	A política de retenção será...
Um usuário que não é membro de uma conta empresarial ou de equipe	Não aplicável
Um usuário de conta de equipe	Não aplicável
Um membro de uma conta empresarial	Definida pelo administrador da conta empresarial

## Ativar a retenção de bate-papo

Os administradores da conta empresarial do Amazon Chime podem usar o console do Amazon Chime para ativar a retenção de chat para conversas de chat e salas de chat em sua conta. Você também pode usar o console para atualizar períodos de retenção de bate-papo ou desativar a retenção de bate-papo a qualquer momento.

Como ativar a retenção de bate-papo

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
2. Na página Contas, selecione o nome da conta.
3. No painel de navegação, em Configurações, escolha Retenção.
4. Na página Retenção, em Retenção de conversas do Chat, mova o controle deslizante para Ativado.
5. Em Período de retenção, insira um número na primeira caixa, abra a lista ao lado da caixa e escolha Dias, Semanas ou Anos.
6. Em Retenção da sala de bate-papo, repita as etapas 4-5. Quando terminar, escolha Salvar.

Dentro de um dia após definir um período de retenção, os usuários em sua conta perdem o acesso às mensagens enviadas fora do período de retenção.

# Restaurando mensagens de bate-papo

## Note

Você deve ser um administrador de conta do Amazon Chime Enterprise para concluir essas etapas.

Você pode restaurar as mensagens de bate-papo em até 30 dias após definir um período de retenção de bate-papo. Ao restaurar mensagens de bate-papo, você restaura todas as mensagens enviadas por todos os usuários em sua conta do Amazon Chime.

Dentro desse período de 30 dias, você pode fazer o seguinte para restaurar as mensagens:

- Use o console do Amazon Chime para desativar a retenção de dados.

—OU—

- Aumente o período de retenção.

Após o período de carência de 30 dias, todas as mensagens de bate-papo que se enquadram no período de retenção são excluídas permanentemente. As novas mensagens de bate-papo são excluídas permanentemente assim que passam do período de retenção.

Para obter informações sobre como definir ou alterar um período de retenção [Ativar a retenção de bate-papo](#), consulte o artigo anterior nesta seção.

As mensagens de bate-papo também são excluídas permanentemente do Amazon Chime quando você ou um membro da conta executa uma das seguintes ações:

- Exclua uma sala de bate-papo do Amazon Chime. Para obter mais informações sobre a exclusão de salas de bate-papo, consulte [Excluir salas de bate-papo](#) no Guia do usuário do Amazon Chime.
- Encerre uma reunião do Amazon Chime na qual as mensagens de bate-papo estejam presentes.

## Note

Conforme necessário, você pode copiar e salvar manualmente as mensagens de bate-papo de uma reunião, mas deve fazer isso antes que a reunião termine. Para obter mais

informações, consulte [Usando o bate-papo em reuniões](#), no Guia do usuário do Amazon Chime.

## Excluindo mensagens de bate-papo

Para cumprir as políticas de retenção de dados, o Amazon Chime retém todas as mensagens de bate-papo e impede que os usuários finais excluam as mensagens que enviam. No entanto, os administradores do sistema Amazon Chime podem usar um par APIs para excluir mensagens individuais de conversas e salas de bate-papo. As mensagens devem residir na conta Amazon Chime do administrador.

Os usuários podem solicitar a exclusão da mensagem enviando a você um ID da mensagem e um ID correspondente da conversa ou da sala de bate-papo. O tópico [Usando recursos de chat](#), no Guia do usuário do Amazon Chime, explica como.

Ao receber uma solicitação de exclusão, você pode escrever código ou usar a AWS CLI para invocar o seguinte. APIs

### Como remover uma mensagem

- Execute um destes procedimentos:
  - Para mensagens de conversação — Use a [RedactConversationMessage](#)API.

Na CLI, execute o seguinte comando:

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

- Para mensagens na sala de bate-papo — Use a [RedactRoomMessage](#)API.

Na CLI, execute o seguinte comando:

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

## Conectar ao seu Active Directory

Ao conectar sua conta administrativa do Amazon Chime a um Active Directory, você pode se beneficiar dos seguintes recursos:

- Seus usuários do Amazon Chime podem fazer login usando suas respectivas credenciais do Active Directory.
- Os administradores do Amazon Chime podem escolher quais recursos de segurança de credenciais adicionar, incluindo mudança de senha, regras de complexidade de senha e autenticação multifator.
- Quando você remove contas de usuário do seu Active Directory, suas contas do Amazon Chime também são removidas.
- Você pode especificar quais grupos do Active Directory recebem permissões do Amazon Chime Pro.
  - Vários grupos podem ser configurados para receber permissões do Basic ou Pro.
  - Os usuários precisam ser membros de um dos grupos para fazer login no Amazon Chime.
  - Usuários em ambos os grupos recebem uma licença do Pro.

Para obter mais informações sobre como gerenciar permissões do usuário, consulte [Gerenciar as permissões e o acesso do usuário](#).

## Pré-requisitos

Antes de se conectar ao Active Directory no Amazon Chime, você precisará concluir os seguintes pré-requisitos:

- Verifique se você tem as AWS Identity and Access Management permissões corretas para configurar domínios, diretórios ativos e grupos de diretórios. Para obter mais informações, consulte [Identity and Access Management para o Amazon Chime](#).
- Crie um diretório AWS Directory Service configurado na região Leste dos EUA (Norte da Virgínia). Para obter mais informações, consulte o [Guia do Administrador do AWS Directory Service](#). O Amazon Chime pode se conectar usando o AD Connector, Microsoft AD ou Simple AD.
- Reivindique um domínio para criar uma conta empresarial do Amazon Chime ou converter sua conta de equipe em uma conta empresarial. Se seus usuários tiverem endereços de e-mail profissionais de mais de um domínio, certifique-se de reivindicar todos esses domínios. Para ter

mais informações, consulte [Reivindicar um domínio](#) e [Converter uma conta de equipe em uma conta empresarial](#).

## Conectar ao seu Active Directory no Amazon Chime

Depois de conectar seu Active Directory ao Amazon Chime, seus usuários serão solicitados a entrar com suas credenciais de diretório quando usarem um endereço de e-mail de um dos domínios que você reivindicou em sua conta empresarial do Amazon Chime.

Como se conectar ao Active Directory no Amazon Chime

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
2. No painel de navegação, escolha Identidade, Active Directory.
3. Em Cloud Directory ID, selecione o AWS Directory Service diretório a ser usado para o Amazon Chime e, em seguida, escolha Connect.

### Note

Você pode encontrar o ID do seu diretório usando o [Console do AWS Directory Service](#).

4. Após a conexão de seu diretório, escolha Adicionar um novo grupo.
5. Em Grupo, insira o nome do grupo. O nome deve corresponder exatamente a um grupo do Active Directory no diretório de destino. As Unidades Organizacionais do Active Directory (OUs) não são suportadas.
6. Para Permissões, escolha Basic ou Pro.
7. Escolha Add Group (Adicionar grupo).
8. (Opcional) Repita este procedimento para criar grupos de diretórios adicionais.

## Configurar vários endereços de e-mail

Depois que você se conectar ao Active Directory no Amazon Chime, os usuários poderão entrar no Amazon Chime usando suas credenciais do Active Directory. Os usuários podem ter vários endereços de e-mail atribuídos no Active Directory. Para permitir que seus usuários façam login no Amazon Chime usando suas credenciais do Active Directory, você deve reivindicar cada domínio de e-mail aplicável em sua conta administrativa do Amazon Chime. Para obter mais informações, consulte [Reivindicar um domínio](#).

**Note**

Se seus usuários tentarem fazer login usando um endereço de e-mail de um domínio não reivindicado, eles serão solicitados a fazer login usando o Log in with Amazon. Eles não conseguem entrar na sua conta administrativa ao usar um endereço de e-mail de um domínio não reivindicado.

Ao visualizar detalhes do usuário no console do Amazon Chime, o Amazon Chime usa o único endereço de e-mail no atributo `EmailAddress` do seu Active Directory como endereço de e-mail principal de cada usuário. Esse é o único endereço de e-mail que você pode ver para o usuário no console do Amazon Chime. No entanto, os usuários podem fazer login com qualquer endereço adicional listado no atributo `ProxyAddress`, desde que você reivindique esses domínios em sua conta do Amazon Chime.

## Exemplo de configuração incorreto

Um usuário com o nome de usuário `shirley.rodriguez` é membro de uma conta do Amazon Chime que reivindicou dois domínios: `example.com` e `example.org`. No Active Directory, este usuário tem os três endereços de e-mail a seguir:

- Endereço de e-mail principal: `shirley.rodriguez@example.com`
- Endereço de e-mail proxy 1: `shirley.rodriguez@example2.com`
- Endereço de e-mail proxy 2: `srodriguez@example.org`

Este usuário pode iniciar uma sessão no Amazon Chime usando `shirley.rodriguez@example.com` ou `srodriguez@anotherdomain.com` e `shirley.rodriguez`. Se eles tentarem fazer login usando `shirley.rodriguez@example2.com`, terão que usar o Login with Amazon e não participarão da sua conta gerenciada. É por isso que é importante reivindicar todos os domínios que seus usuários usam para o e-mail.

Outros usuários do Amazon Chime podem adicioná-los como um contato, convidá-los para reuniões ou adicioná-los como representante usando o endereço de e-mail `shirley.rodriguez@example.com` ou `srodriguez@anotherdomain.org`.

## Exemplo de configuração correto

Um usuário com o nome de usuário shirley.rodriguez é membro de uma conta do Amazon Chime que reivindicou três domínios: example.com, example2.com e example.org. No Active Directory, este usuário tem os três endereços de e-mail a seguir:

- Endereço de e-mail principal: shirley.rodriguez@example.com
- Endereço de e-mail proxy 1: shirley.rodriguez@example2.com
- Endereço de e-mail proxy 2: srodriguez@example.org

Este usuário pode uma iniciar sessão no Amazon Chime usando qualquer um dos seus endereços de e-mail. Outros usuários também podem adicioná-los como um contato, convidá-los para reuniões ou adicioná-los como representante usando qualquer um dos seus endereços de e-mail de trabalho.

## Conectar ao Okta SSO

Caso tenha uma conta empresarial, você pode se conectar ao Okta SSO para se autenticar e atribuir permissões de usuário.

### Note

Caso você precise criar uma conta empresarial, que permite o gerenciamento de todos os usuários em um determinado conjunto de domínios de endereço de e-mail, consulte [Reivindicar um domínio](#).

Conectar o Amazon Chime ao Okta exige a configuração de dois aplicativos no console de administração do Okta. O primeiro aplicativo é configurado manualmente e usa OpenID Connect para autenticar os usuários para o serviço Amazon Chime. O segundo aplicativo está disponível como Amazon Chime SCIM Provisioning na Okta Integration Network (OIN). Ele é configurado para enviar atualizações para o Amazon Chime sobre alterações em usuários e grupos.

Para se conectar ao Okta SSO

1. Crie o aplicativo Amazon Chime (OpenID Connect) no Console de administração do Okta:

1. Faça login no Okta Administration Dashboard e escolha Add Application (Adicionar aplicativo). Na caixa de diálogo Create New Application (Criar novo aplicativo), escolha Web, Next (Avançar).
2. Defina as Application Settings (Configurações do aplicativo):
  - a. Nomeie o aplicativo **Amazon Chime**.
  - b. Em Login Redirect URI (URI de redirecionamento de login), insira o seguinte valor: **https://signin.id.ue1.app.chime.aws/auth/okta/callback**
  - c. Na seção Allowed Grant Types (Tipos de concessão permitidos), selecione todas as opções para habilitá-las.
  - d. No menu suspenso Login initiated by (Login iniciado por), selecione Either (Okta or App) (Okta ou aplicativo) e selecione todas as opções relacionadas.
  - e. Em Initiate Login URI (Iniciar URI de login), insira o seguinte valor: **https://signin.id.ue1.app.chime.aws/auth/okta**
  - f. Escolha Salvar.
  - g. Mantenha essa página aberta porque você precisará do Client ID (ID do cliente), Client secret (Segredo do cliente) e informações do Issuer URI (URI do emissor) para a Etapa 2.
2. No console do Amazon Chime, siga estas etapas:
  1. Na página Okta single-sign on configuration (Configuração de logon único do Okta), na parte superior da página, escolha Set up incoming keys (Configurar chaves recebidas).
  2. Na caixa de diálogo Setup incoming Okta keys (Configurar chaves do Okta recebidas):
    - a. Cole as informações de Client ID (ID do cliente) e Client secret (Segredo do cliente) na página Okta Application Settings (Configurações do aplicativo do Okta).
    - b. Cole o Issuer URI (URI do emissor) na página Okta API. O URI do emissor deve ser um domínio Okta, como `https://example.okta.com`.
3. Configure o aplicativo Amazon Chime SCIM Provisioning no Okta Administration Console para trocar informações de identidade selecionada e associação do grupo com o Amazon Chime:
  1. No Console de administração do Okta, escolha Aplicações, Adicionar aplicação, procure Amazon Chime SCIM Provisioning e adicione a aplicação.

 Important

Durante a configuração inicial, escolha Do not display application to users (Não exibir aplicativo para usuário), Do not display application icon in the Okta Mobile App (Não exibir ícone do aplicativo no Okta Mobile App) e Done (Concluído).

2. Na guia Provisioning (Provisionamento), escolha Configure API Integration (Configurar integração da API) e selecione Enable API Integration (Habilitar integração da API). Mantenha essa página aberta, porque você precisará copiar uma chave de acesso de API para ela na etapa seguinte.
3. No console do Amazon Chime, escolha Criar chave de acesso para criar uma chave de acesso de API. Copie-a para o campo Okta API Token (Token da API do Okta) na caixa de diálogo Configure API Integration (Configurar integração da API), escolha Test the Integration (Testar a integração) e Save (Salvar).
4. Configure as ações e os atributos que o Okta usará para atualizar o Amazon Chime. Na guia Provisioning (Provisionamento), na seção To App (Para aplicativo), escolha Edit (Editar), em Enable Users (Habilitar usuários), Update User Attributes (Atualizar atributos do usuário) e Deactivate Users (Desativar usuários) e Save (Salvar).
5. Na guia Assignments (Atribuições), conceda a usuários permissões para o novo aplicativo SCIM.

 Important

Recomendamos conceder permissões por meio de um grupo que contenha todos os usuários que precisam ter acesso ao Amazon Chime, independentemente da licença. O grupo deve estar no mesmo grupo usado para atribuir o aplicativo OIDC voltado para o usuário na etapa 1 anteriormente. Do contrário, os usuários finais não poderão fazer login.

6. Na guia Enviar grupos, configure quais grupos e associações estão sincronizados com o Amazon Chime. Esses grupos são usados para diferenciar usuários Básicos de Pro.
4. Configure grupos de diretórios no Amazon Chime:
    1. No console do Amazon Chime, acesse a página Configuração de autenticação única do Okta.
    2. Em Directory groups (Grupos de diretórios), escolha Add new groups (Adicionar novos grupos).

3. Insira o nome do grupo de diretórios a ser adicionado ao Amazon Chime. O nome deve ser uma correspondência exata de um dos Push Groups (Grupos de envio) configurados anteriormente na etapa 3-f.
4. Escolha se os usuários desse grupo devem receber recursos de Basic (Básico) ou Pro e Save (Salvar). Repita esse processo para configurar grupos adicionais.

 Note

Se você receber uma mensagem de erro informando que o grupo não foi encontrado, os dois sistemas não terão concluído a sincronização. Aguarde alguns minutos e escolha Add new groups (Adicionar novos grupos) novamente.

Escolher recursos Basic ou Pro para os usuários no grupo de diretórios afeta a licença, os recursos e o custo desses usuários na conta empresarial do Amazon Chime. Para obter mais informações, consulte [Preços do](#).

## Implantar a extensão do Amazon Chime para Outlook

O Amazon Chime fornece duas extensões para o Microsoft Outlook: a extensão do Amazon Chime para Outlook no Windows e extensão do Amazon Chime para Outlook. Essas extensões oferecem os mesmos recursos de programação, mas oferecem suporte a diferentes tipos de usuários. Os assinantes do Microsoft Office 365 e as organizações que usam o Microsoft Exchange 2013 ou posterior no ambiente on-premises podem usar a extensão do Amazon Chime para Outlook. Os usuários do Windows com um servidor Exchange on-premises que executam o Exchange Server 2010 ou anterior e os usuários do Outlook 2010 devem usar o suplemento para o Outlook no Windows do Amazon Chime.

Os usuários do Windows que não têm permissão para instalar a extensão do Amazon Chime para Outlook devem optar pela extensão do Amazon Chime para Outlook no Windows.

Para obter informações sobre qual extensão é a ideal para você e sua organização, consulte [Escolher a extensão certa do Outlook](#).

Se você escolher a extensão do Amazon Chime para Outlook para sua organização, poderá implantá-la aos usuários com a implantação centralizada. Para obter mais informações, consulte o [Guia para administradores de como instalar a extensão do Amazon Chime para Outlook](#).

# Configurar o aplicativo Amazon Chime Meetings para Slack

Se você usa o [Slack Enterprise Grid Organizations](#) e possui ou administra uma organização do Slack, pode configurar o aplicativo Amazon Chime Meetings para Slack para suas organizações. Se você for um administrador do espaço de trabalho do Slack, configure o aplicativo Amazon Chime Meetings para Slack nos seus espaços de trabalho.

As etapas nas seções a seguir explicam como realizar os dois tipos de configurações e como concluir tarefas adicionais, como migrar um espaço de trabalho para uma organização.

## Tópicos

- [Instalação do aplicativo Amazon Chime Meetings para Slack em uma organização](#)
- [Instalação do aplicativo Amazon Chime Meetings para Slack em espaços de trabalho](#)
- [Migrar espaços de trabalho para organizações](#)
- [Associar espaços de trabalho a contas de equipe do Amazon Chime](#)

## Instalação do aplicativo Amazon Chime Meetings para Slack em uma organização

A instalação do aplicativo Amazon Chime Meetings para Slack em uma organização do Slack permite que os usuários iniciem reuniões e chamadas instantâneas com outros usuários nos vários espaços de trabalho dessa organização. Ele também permite que os administradores do espaço de trabalho instalem automaticamente o aplicativo de reuniões Amazon Chime Meetings para Slack em qualquer novo espaço de trabalho. As etapas a seguir explicam como.

### Note

As etapas a seguir pressupõem que você seja proprietário ou administrador da organização e que possa fazer login no console de gerenciamento do Slack.

Como configurar o aplicativo Amazon Chime Meetings para Slack em uma organização

1. No painel esquerdo do console de gerenciamento do Slack, escolha Aplicativos.

A página Aplicativos é exibida e lista os aplicativos instalados pela organização, se houver.

2. Selecione Gerenciar aplicativos, localizado no canto superior direito da página, e selecione Instalar um aplicativo.

A caixa de diálogo Localizar um aplicativo para instalar é exibida.

3. Pesquise sobre **Amazon Chime Meetings** e selecione a opção nos resultados da pesquisa.

A caixa de diálogo Adicionar reuniões do Amazon Chime aos espaços de trabalho é exibida e lista os espaços de trabalho na organização.

4. Escolha o espaço de trabalho ou espaços de trabalho nos quais você deseja instalar o aplicativo Amazon Chime Meetings para Slack.
5. Opcionalmente, escolha Padrão para o futuro espaço de trabalho se quiser instalar automaticamente o aplicativo Amazon Chime Meetings para Slack em todos os novos espaços de trabalho e, em seguida, escolha Próximo.

A caixa de diálogo Revisar as permissões solicitadas deste aplicativo é exibida e exibe as permissões e ações do aplicativo Amazon Chime Meetings para Slack.

6. Escolha Próximo.
7. Se você optar por instalar o aplicativo Amazon Chime Meetings para Slack em novos espaços de trabalho por padrão, escolha Definir esse aplicativo como padrão para futuros espaços de trabalho e selecione Salvar. Caso contrário, selecione Salvar.

#### Note

Você também pode usar OAuth para instalar aplicativos em suas organizações. Para obter mais informações, consulte [Instalando com OAuth](#) na ajuda do Slack.

## Instalação do aplicativo Amazon Chime Meetings para Slack em espaços de trabalho

A instalação do aplicativo Amazon Chime Meetings para Slack em um espaço de trabalho permite que os usuários iniciem reuniões e chamadas instantâneas com outros usuários nesse espaço de trabalho. Os usuários não precisam de um perfil de usuário do Amazon Chime para usar o aplicativo Amazon Chime Meetings para Slack. Eles podem fazer login com seus perfis de usuário do Slack e iniciar chamadas ou reuniões a qualquer momento. Se os usuários precisarem realizar reuniões com mais de uma pessoa, você deverá configurar uma conta de equipe do Amazon Chime

e conceder permissões Pro a esses usuários adicionais. Para obter mais informações sobre como iniciar chamadas e reuniões do Amazon Chime, consulte [Using the Amazon Chime Meetings App for Slack](#) no Guia do usuário do Amazon Chime. Para obter mais informações sobre como configurar uma conta de equipe do Amazon Chime, consulte [Associar espaços de trabalho a contas de equipe do Amazon Chime](#) neste guia.

Para instalar o aplicativo Amazon Chime Meetings para Slack para espaços de trabalho do Slack

1. Navegue até o Diretório de aplicativos do Slack e localize o aplicativo Amazon Chime Meetings.
2. Escolha [Adicionar ao Slack](#) para instalar o Amazon Chime Meetings usando o Diretório de aplicativos do Slack.
3. Defina a configuração de Chamadas do espaço de trabalho do Slack para Habilitar chamadas no Slack, usando o Amazon Chime.

## Migrar espaços de trabalho para organizações

Se você é proprietário de uma organização do Slack, pode migrar espaços de trabalho para essa organização. Para obter mais informações sobre a migração de espaços de trabalho, consulte [Migrate workspaces to Enterprise Grid](#) na ajuda do Slack.

## Associar espaços de trabalho a contas de equipe do Amazon Chime

Associe seu espaço de trabalho a uma conta de equipe do Amazon Chime para gerenciar as permissões dos usuários. É possível atualizar os hosts das reuniões para o Amazon Chime Pro para que eles possam iniciar reuniões com até 250 participantes e 25 blocos de vídeo e incluir números de telefone para discagem por áudio. Atribua aos usuários permissões do Amazon Chime Basic para que eles possam iniciar one-on-one reuniões ou participar de reuniões do Amazon Chime. Para obter mais informações, consulte [Preços do Amazon Chime](#).

### Note

Se você associar uma conta de equipe do Amazon Chime ao seu espaço de trabalho do Slack, os usuários poderão fazer login pelo aplicativo Amazon Chime Meetings para Slack. É possível alterar essa configuração a qualquer momento. Para obter mais informações, consulte [Gerenciar as configurações da reunião](#).

Antes de associar seu espaço de trabalho do Slack a uma conta do Amazon Chime Team, você deve criar uma conta. AWS Para obter mais informações sobre como criar uma AWS conta, consulte [Pré-requisitos para administradores de sistema do Amazon Chime](#).

Para associar seu espaço de trabalho do Slack a uma conta de equipe do Amazon Chime ao instalar o aplicativo Amazon Chime Meetings para Slack

1. Imediatamente depois de instalar o aplicativo Amazon Chime Meetings para Slack no espaço de trabalho do Slack, escolha Atualizar agora.
2. Siga as instruções para fazer login no console do Amazon Chime usando as credenciais da sua conta da AWS .
3. Siga as instruções para criar uma nova conta de equipe do Amazon Chime ou escolha uma existente.
  - Criar uma conta: crie uma conta do Amazon Chime para a qual convidar seus usuários do Slack. Insira um nome de conta, escolha se deseja convidar os usuários do Slack e selecione Create (Criar).
  - Escolher uma conta existente: selecione uma conta existente do Amazon Chime para convidar seus usuários do Slack. Selecione a conta e escolha Invite (Convidar).

Quando você convida seus usuários do Slack para participar do Amazon Chime, eles recebem um convite por e-mail. Ao aceitar o convite, eles são atualizados automaticamente para o Amazon Chime Pro.

Se você não associou seu espaço de trabalho do Slack a uma conta de equipe do Amazon Chime durante a instalação do aplicativo Amazon Chime Meetings para Slack, poderá fazer isso seguindo as instruções abaixo.

Como associar seu espaço de trabalho do Slack a uma conta de equipe do Amazon Chime depois de instalar o aplicativo Amazon Chime Meetings para Slack

1. Faça login na sua AWS conta.
2. Inicie a sessão no seu workspace do Slack como administrador.
3. Acesse [https://signin.id.ue1.app.chime.aws/auth/slack?propósito=app\\_authz](https://signin.id.ue1.app.chime.aws/auth/slack?propósito=app_authz).
4. Siga as instruções para criar uma conta de equipe no Amazon Chime ou escolha uma existente.

- Criar uma conta: crie uma conta do Amazon Chime para a qual convidar seus usuários do Slack. Insira um nome de conta, escolha se deseja convidar os usuários do Slack e selecione Create (Criar).
- Escolher uma conta existente: selecione uma conta existente do Amazon Chime para convidar seus usuários do Slack. Selecione a conta e escolha Invite (Convidar).

# Gerenciamento de usuários

## Note

As etapas desta seção pressupõem que você tenha um conjunto de endereços de e-mail de usuário ou que tenha conectado sua conta de administrador ao Active Directory. Para obter mais informações, consulte [Conectar ao seu Active Directory](#), neste guia.

Você usa o console do Amazon Chime para adicionar e gerenciar usuários. Você adiciona usuários convidando-os. Quando eles aceitam seus convites, eles aparecem em **Usuários**, que lista todos os usuários em sua conta e os detalhes do usuário. Para obter mais informações, consulte [Visualizar detalhes do usuário](#).

Administradores de contas usando o Login with Amazon (LWA) também visualizam opções para gerenciar camadas de permissão e remover usuários de uma conta. Essas ações são gerenciadas por meio do Active Directory ou do Okta, dependendo de qual delas você configura uma conta para usar. Para obter mais informações, consulte [Gerenciar as permissões e o acesso do usuário](#).

## Conteúdo

- [Adição de usuários](#)
- [Visualizar detalhes do usuário](#)
- [Gerenciar as permissões e o acesso do usuário](#)
- [Mudando a reunião pessoal PINs](#)
- [Gerenciar avaliações do Pro](#)
- [Solicitar anexos de usuários](#)
- [Como o Amazon Chime gerencia as atualizações automáticas](#)
- [Migrar usuários para outra conta de equipe](#)

## Adição de usuários

Você adiciona usuários a uma conta do Amazon Chime convidando-os a participar da conta. Você envia convites para usuários em potencial a partir do console do Amazon Chime, e essas etapas explicam como.

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/.](https://chime.aws.amazon.com/)

Uma lista das contas que você administra é exibida.

2. Escolha a conta à qual você deseja adicionar membros e escolha Convidar usuários.

A caixa de diálogo Convidar novos usuários é exibida.

3. Insira os endereços de e-mail dos usuários que você deseja convidar. Separe cada endereço com um ponto e vírgula (;).

4. Escolha Invite users.

Os novos usuários aparecem na lista. Quando você convida usuários para uma conta de equipe, os detalhes deles não aparecerão até que eles aceitem seu convite.

## Visualizar detalhes do usuário

No console do Amazon Chime, em Usuários, você pode visualizar uma lista de todos os usuários em sua conta e ver detalhes dos usuários. Pesquise um usuário específico pelo endereço de e-mail e escolha o nome para ver os detalhes do usuário. Em Detalhes do usuário, você pode ver informações detalhadas sobre o usuário e fazer atualizações em sua conta de usuário.

A tabela a seguir lista os detalhes do usuário que aparecem no console.

### Note

Os detalhes completos do usuário não aparecem para os usuários da conta de equipe até que eles aceitem seus convites.

Campo	Descrição	Exemplo
Nome de exibição	O nome do usuário exibido no Amazon Chime. Para usuários do Login with Amazon (LWA), esse é o nome completo. Para usuários do Active Directory, DISPLAY_NAME_ATTRIBUTE é usado.	Major, Mary

Campo	Descrição	Exemplo
Endereço de e-mail	Para usuários do LWA, o endereço de e-mail usado para registro. Para usuários do Active Directory, o endereço de e-mail principal do Active Directory é exibido.	mary.major@example.com
Registro	O status atual do registro do usuário. Os valores possíveis são diferentes entre contas empresariais, em que os convites não são enviados, e contas de equipe, para as quais os convites são enviados.	Registrada, Não registrada (para a conta de equipe) ou Suspensa (para a conta empresarial)
Permission tier	Definido como Pro por padrão, para permitir que os usuários hospedem reuniões. A opção pode ser alterada para Basic.	Pro, Basic
Invited	Para as contas de equipe, a data em que o usuário foi convidado para a conta.	01/05/2020
Ingressou	A data em que o usuário fez login pela primeira vez no Amazon Chime. Para usuários do Pro Trial, essa também é a data em que o Pro Trial começou.	01/10/2020
Personal PIN	O PIN da reunião pessoal que o usuário pode usar para agendar reuniões.	0123456789

Campo	Descrição	Exemplo
Privacy setting	A configuração de presença que o usuário selecionou.	Public ou Private
Meetings attended	O número de reuniões que um usuário participou.	87
Meetings organized	O número de reuniões que um usuário organizou.	12
Meeting satisfaction	A porcentagem de respostas positivas dadas à end-of-meeting pesquisa.	92%
Last active date	A data em que o usuário esteve ativo pela última vez.	06/12/2020
Chat messages sent	O número de mensagens de chat que o usuário enviou.	1025
Número de telefone	O número de telefone atribuído a um usuário, se houver.	+12065550100

## Gerenciar as permissões e o acesso do usuário

Gerencie quais recursos seus usuários do Amazon Chime podem acessar atribuindo a eles permissões Pro ou Basic. Os usuários com permissões Basic não podem hospedar reuniões, mas podem participar de reuniões e usar o chat. Para obter mais informações sobre os recursos que os usuários com permissões Pro e Basic podem acessar, consulte [Planos e preços](#).

Gerencie quem pode entrar na sua conta administrativa do Amazon Chime convidando ou suspendendo usuários. Os administradores de contas empresariais também podem suspender usuários. Os administradores de contas de equipe podem remover usuários das suas respectivas contas para que eles não paguem mais pelas permissões do usuário. No entanto, eles não podem suspender o usuário para impedi-lo de entrar. Para obter mais informações sobre as diferenças entre as contas de equipe e empresarial, consulte [Gerenciar suas contas do Amazon Chime](#).

## Gerenciamento de permissões de usuário

Como administrador do Amazon Chime, você pode gerenciar as permissões Pro e Basic para os usuários na sua conta do Amazon Chime.

Se o Active Directory ou o Okta estiver configurado na sua conta do Amazon Chime, gerencie as permissões do usuário por meio de associações de grupos. Se você não tiver o Active Directory ou o Okta configurados, gerencie as permissões de usuário no console do Amazon Chime.

### Login with Amazon para contas de equipe e empresariais

Se você administrar uma conta de equipe ou uma conta empresarial de LWA do Amazon Chime, na qual os usuários fazem login com suas contas de Login with Amazon (LWA), você pode gerenciar as permissões Pro e Basic no console do Amazon Chime.

Como gerenciar permissões de usuário para contas de equipe e empresariais de LWA

1. [Abra o console do Amazon Chime em `https://chime.aws.amazon.com/`.](https://chime.aws.amazon.com/)
2. Em Contas, escolha o nome da conta do Amazon Chime.
3. Selecione Usuários.
4. Selecione os usuários e escolha Ações, Atribuir permissões.
5. Escolha uma das seguintes opções:
  - Pro
  - Básico
6. Selecione Assign (Atribuir).

### Contas empresariais do Active Directory ou OpenID Connect (Okta)

Se seus usuários entrarem com as credenciais do Active Directory ou Okta, gerencie suas permissões tornando-os membros de um grupo de diretórios que tenha permissões Pro ou Basic atribuídas a ele.

Para atribuir permissões Pro a um usuário, torne-o membro de um grupo do Active Directory ou Okta ao qual você atribuiu permissões Pro. Para atribuir permissões Basic a um usuário, torne-o membro de um grupo ao qual você atribuiu permissões Basic. Usuários que não têm permissões Pro ou Basic não podem entrar no Amazon Chime.

## Gerenciar acesso do usuário

Se você administrar uma conta do Amazon Chime, poderá convidar usuários para permitir que eles acessem sua conta. Os administradores de contas corporativas podem suspender o acesso do usuário para impedir que eles façam login na conta.

### Convidar e remover usuários da conta de equipe

Com uma conta de equipe, é possível usar o console do Amazon Chime para convidar usuários de qualquer domínio de e-mail.

#### Note

O Pro Trial gratuito de 30 dias de um usuário termina quando ele aceita o convite.

Como convidar usuários para uma conta de equipe

1. [Abra o console do Amazon Chime em](https://chime.aws.amazon.com/)<https://chime.aws.amazon.com/>.
2. Em Contas, escolha o nome da conta da equipe.
3. Escolha Usuários, Convidar usuários.
4. Insira os endereços de e-mail dos usuários a serem convidados, separando vários endereços de e-mail com ponto e vírgula (;).
5. Escolha Invite users.

O procedimento a seguir desassocia os usuários da sua conta de equipe removendo todas as permissões Pro ou Básica atribuídas a eles. Os usuários removidos ainda podem entrar no Amazon Chime, mas não são mais membros pagos da sua conta do Amazon Chime.

Como remover usuários de uma conta de equipe

1. [Abra o console do Amazon Chime em](https://chime.aws.amazon.com/)<https://chime.aws.amazon.com/>.
2. Em Contas, escolha o nome da conta da equipe.
3. Selecione Usuários.
4. Selecione os usuários e escolha Ações, Remover usuário.

Todas as permissões Pro ou Basic atribuídas aos usuários são removidas. Os usuários não podem mais usar o preenchimento automático Contatos para encontrar novos usuários de equipe.

## Convidar e suspender usuários da conta empresarial

Se você administrar uma conta empresarial, todos os usuários que se registrarem no Amazon Chime com um endereço de e-mail dos seus domínios reivindicados serão adicionados automaticamente à sua conta. Se você configurou o Active Directory ou o Okta, os usuários também devem ser membros do grupo de diretórios que você configurou para o Amazon Chime.

### Como convidar usuários para uma conta empresarial

- Envie um e-mail de convite para os usuários na sua organização e instrua-os a seguir as etapas descritas em [Creating an Amazon Chime account](#) no Guia do usuário do Amazon Chime.

Os usuários fazem login com um endereço de e-mail de um dos domínios que você reivindicou para sua conta. Depois que concluírem as etapas para criar as contas de usuário do Amazon Chime, elas serão automaticamente exibidas na página Usuários da conta empresarial no console do Amazon Chime.

O procedimento a seguir suspende os usuários de uma conta corporativa que não tenha o Active Directory ou o Okta configurados. Isso impede que os usuários façam login no Amazon Chime.

### Como suspender usuários de uma conta empresarial

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
2. Em Contas, escolha o nome da conta da empresa.
3. Selecione Usuários.
4. Na página Usuários, selecione os usuários a serem suspensos e escolha Ações, Suspende usuário.
5. Marque a caixa de seleção e escolha Suspende.

Se você possui o Active Directory ou o Okta configurados para sua conta corporativa, use o procedimento a seguir para suspender usuários.

### Como suspender usuários de uma conta empresarial do Active Directory ou OpenID Connect (Okta)

- Execute um destes procedimentos:

- Suspenda ou marque o usuário inativo no painel de administrador do Active Directory ou do Okta.
- Remova o usuário de qualquer grupo do Active Directory que tenha permissões Basic ou Pro atribuídas a ele.

## Mudando a reunião pessoal PINs

Um PIN de reunião pessoal é um ID estático gerado quando o usuário se registra. O PIN facilita o trabalho de um usuário do Amazon Chime para agendar reuniões com outros usuários do Amazon Chime. Usar um PIN de reunião pessoal significa que os organizadores da reunião não precisam se lembrar dos detalhes da reunião para cada nova reunião que eles programam.

Se um usuário achar que seu PIN de reunião pessoal foi comprometido, você poderá redefinir o PIN e gerar um novo ID. Depois de atualizar um PIN de reunião pessoal, o usuário precisará atualizar todas as reuniões que foram agendadas usando o PIN antigo da reunião pessoal.

Para alterar um PIN de reunião pessoal

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/.](https://chime.aws.amazon.com/)
2. Na página Contas, selecione o nome da conta do Amazon Chime.
3. No painel de navegação, escolha Users.
4. Procure o usuário que precisa alterar o PIN.
5. Para abrir a página User detail, escolha o nome do usuário.
6. Escolha User actions, Reset personal PIN, Confirm.

## Gerenciar avaliações do Pro

Quando um usuário aceita um convite de equipe do Amazon Chime ou é adicionado a uma conta empresarial, a avaliação gratuita termina e eles têm permissões do Pro. Isso permite que eles continuem hospedando reuniões agendadas. A alteração do nível de permissão de um usuário para Básico impede que ele atue como o host de uma reunião.

Com a definição de preço do Amazon Chime baseada em uso, você paga somente pelos usuários que hospedam reuniões nos dias em que as hospedam. Os participantes da reunião e os usuários do chat não serão cobrados.

Os usuários são considerados Active Pro se tiverem hospedado uma reunião que tenha terminado em um dia de calendário e que pelo menos um dos eventos a seguir tenha ocorrido:

- A reunião foi programada.
- A reunião incluiu mais de dois participantes.
- A reunião teve pelo menos um evento de gravação.
- A reunião incluiu um participante que discou.
- A reunião incluiu um participante que ingressou com H.323 ou SIP.

Para obter mais informações, consulte [Planos e definição de preço](#).

## Solicitar anexos de usuários

Se você gerencia uma conta empresarial e tem as permissões adequadas, é possível solicitar e receber os anexos que seus usuários carregaram no Amazon Chime. Você pode obter os anexos que os usuários carregaram em conversas individuais e de grupo ou em salas de chat que eles criaram.

### Note

Se você gerencia uma conta de equipe do Amazon Chime, é possível atualizar para uma conta empresarial reivindicando um ou mais domínios. Como alternativa, é possível remover os usuários da conta de equipe, o que permite que os usuários não gerenciados obtenham seus anexos usando o assistente do Amazon Chime.

Como solicitar anexos de usuários

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
2. Na página Contas, selecione o nome da conta do Amazon Chime.
3. Em Settings (Configurações), selecione Account (Conta), Account actions (Ações da conta), Request attachments (Solicitar anexos).
4. Em aproximadamente 24 horas, a página de resumo da conta fornece um link para um arquivo contendo uma lista de preassinados URLs que você usa para acessar cada anexo.
5. Faça download do arquivo .

**Note**

Certifique-se de manter um nível adequado de controle de acesso ao arquivo. Qualquer usuário que obtenha o arquivo pode usar a lista fornecida de URLs para baixar os anexos associados.

Os pré-assinados URLs expiram após 6 dias. Você pode enviar uma solicitação a cada 7 dias.

Para usar políticas AWS Identity and Access Management (IAM) para gerenciar o acesso ao console de administração do Amazon Chime e à ação Solicitar anexos, use uma das políticas gerenciadas do Amazon Chime (, ou). FullAccess UserManagement ReadOnly Como alternativa, você pode atualizar as políticas personalizadas para incluir as ações StartDataExport e RetrieveDataExport. Para obter mais informações, consulte [Actions defined by Amazon Chime](#) no Guia do usuário do IAM.

## Como o Amazon Chime gerencia as atualizações automáticas

O Amazon Chime fornece maneiras diferentes de atualizar seus clientes. O método varia, dependendo se você executa o Amazon Chime em um navegador, em seu desktop ou em um dispositivo móvel.

A aplicação web do Amazon Chime (<https://app.chime.aws>) sempre carrega os recursos e correções de segurança mais recentes.

O cliente de desktop do Amazon Chime verifica se há atualizações sempre que você escolhe Sair ou Desconectar. Isso se aplica a máquinas Windows e macOS. Conforme você executa o cliente, ele verifica se há atualizações a cada três horas. Você também pode verificar se há atualizações escolhendo Verificar atualizações no menu Ajuda do Windows ou no menu Amazon Chime do macOS.

Quando o cliente de desktop detecta uma atualização, o Amazon Chime solicita que o usuário a instale, a menos que esteja em uma reunião em andamento. Eles estão em uma reunião contínua quando:

- Eles participam de uma reunião.
- Eles foram convidados para uma reunião que ainda está em andamento.

O Amazon Chime solicita que eles instalem a versão mais recente e fornece uma contagem regressiva de 15 segundos para que eles possam adiar a instalação. Os usuários escolhem Tentar mais tarde para adiar a atualização.

Se os usuários adiarem uma atualização e não estiverem em uma reunião contínua, o cliente verificará a atualização após três horas e solicitará que eles instalem novamente. A instalação se inicia quando a contagem regressiva termina.

#### Note

Em um computador macOS, os usuários precisam escolher Reiniciar agora para iniciar a atualização.

Em dispositivos móveis: os aplicativos móveis Amazon Chime usam as opções de atualização fornecidas pela App Store e pelo Google Play para fornecer a versão mais recente do cliente Amazon Chime. Você também pode usar o sistema de gerenciamento de dispositivos móveis para implantar atualizações.

## Migrar usuários para outra conta de equipe

Você migra usuários para outras contas de equipe criando e configurando uma conta de destino, se ainda não existir uma. Em seguida, você adiciona usuários à conta de destino. As etapas a seguir levam você às informações sobre como concluir cada parte de uma migração.

Como migrar usuários

1. Se você não tiver uma conta da equipe, crie uma. Para obter mais informações, consulte [Etapa 1: Criar uma conta de administrador do Amazon Chime](#).
2. Conforme necessário, configure a conta. Para obter mais informações, consulte [Etapa 2 \(opcional\): definir configurações da conta](#).
3. Adicione usuários à conta. Para obter mais informações, consulte [Etapa 3: adicionar usuários à conta](#).

# Gerenciar números de telefone no Amazon Chime

Você usa o console do Amazon Chime para provisionar números de telefone. Ao provisionar números, você os solicita de um pool de números gerenciado pelo Amazon Chime. Quando você cancela a atribuição e depois exclui números, eles retornam ao grupo. Ao transferir números, você os transfere para dentro e para fora do Amazon Chime.

## Note

Ao usar o console do Amazon Chime, você só pode provisionar números do Amazon Chime Business Calling. Se você precisar de números internacionais, use os Amazon Chime Voice Connectors e os aplicativos de mídia SIP. Para fazer isso, primeiro você deve criar uma conta administrativa do Amazon Chime SDK. Para obter mais informações, consulte os seguintes tópicos no Guia do administrador do Amazon Chime SDK:

- [Pré-requisitos](#)
- [Gerenciando o inventário de números de telefone](#)
- [Gerenciando conectores de voz](#)
- [Gerenciando aplicativos de mídia SIP](#)

Os tópicos nas seções a seguir explicam como provisionar e gerenciar números de telefone do Amazon Chime.

## Conteúdo

- [Provisionar números de telefone](#)
- [Transferir números de telefones existentes](#)
- [Atribuição de números de telefone do Amazon Chime Business Calling](#)
- [Cancelando a atribuição de números de telefone do Amazon Chime Business Calling](#)
- [Usando nomes de chamadas externas](#)
- [Excluir números de telefone](#)
- [Restaurar números de telefone excluídos](#)

## Provisionar números de telefone

Use o console do Amazon Chime para provisionar números de telefone para a conta do Amazon Chime. Os números vêm de um grupo gerenciado pelo Amazon Chime. Escolha Amazon Chime Business Calling para provisionar e atribuir números de telefone aos seus usuários atuais do Amazon Chime.

Quando o provisionamento estiver concluído, os números de telefone serão exibidos em seu Inventário. Em seguida, você os atribui a usuários individuais.

### Como provisionar números de telefone

1. [Abra o console do Amazon Chime em `https://chime.aws.amazon.com/`.](https://chime.aws.amazon.com/)
2. No painel de navegação, em Chamadas, selecione Gerenciamento de números de telefone.
3. Selecione Orders (Pedidos), Provision phone numbers (Provisionar números de telefone).
4. Selecione Business Calling e escolha Próximo.
5. Procure números de telefone disponíveis. Selecione os números de telefone desejados e escolha Provision (Provisionar).

Os números de telefone aparecem em suas listas Pedidos e Pendente enquanto ocorre o provisionamento.

## Transferir números de telefones existentes

Além de provisionar números de telefone, você também pode transferir números da sua operadora de telefonia para o seu inventário. Isso inclui números gratuitos.

### Note

Se você precisar portar números internacionais, usar o Amazon Chime Voice Connector ou usar aplicativos de mídia SIP, você deve criar uma conta de administrador do Amazon Chime SDK e usar o console do Amazon Chime SDK. Para obter mais informações sobre como fazer isso, consulte [Pré-requisitos](#) no Guia do administrador do Amazon Chime SDK.

As seções a seguir explicam como fazer a portabilidade de números de telefone.

## Tópicos

- [Pré-requisitos para portar números](#)
- [Transferindo números de telefone para](#)
- [Envio dos documentos necessários](#)
- [Visualizando o status da solicitação](#)
- [Atribuição de números portados](#)
- [Transferindo números de telefone](#)
- [Definições de status de transferência de números de telefone](#)

## Pré-requisitos para portar números

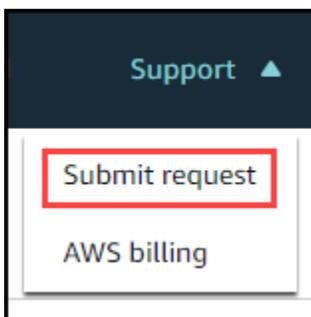
Para portar números, você deve ter uma Carta de Agência (LOA). Você deve ter uma LOA para números de telefone nacionais. Baixe o [formulário da Carta de Agência \(LOA\)](#) e preencha-o. Se você precisar transferir números de telefone de operadoras diferentes, preencha uma LOA separada para cada operadora.

## Transferindo números de telefone para

Você cria uma solicitação de suporte para transferir números de telefone existentes.

Para fazer a portabilidade de números de telefone existentes

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
2. Na barra de comando na parte superior da página, escolha Support e, em seguida, selecione Enviar solicitação.



Isso leva você ao console do AWS Support.

 Note

Você também pode ir diretamente para a página [AWS Support central](#). Se você fizer isso, escolha Criar caso e siga as etapas abaixo.

3. Em Como podemos ajudar, faça o seguinte:

- a. Escolha Conta e faturamento.
- b. Na lista de serviços, escolha Chime SDK (gerenciamento de números).
- c. Na lista de categorias, escolha Número de telefone > Porta de entrada.
- d. Selecione Próxima etapa: informações adicionais.

4. Em Informações adicionais, faça o seguinte

- a. Em Assunto, insira **Porting phone numbers in**.
- b. Em Descrição, insira as seguintes informações:

Para portar números dos EUA:

- Número de telefone de faturamento (BTN) da conta.
- Nome da pessoa para autorização. Essa é a pessoa responsável pelo faturamento da conta com a operadora atual.
- Operadora atual, se conhecida.
- Número da conta de serviço, se essas informações estiverem com a operadora atual.
- PIN de serviço, se disponível.
- Endereço do serviço e nome do cliente, conforme exibidos no contrato da operadora atual.
- Data e hora solicitadas para a porta.
- (Opcional) Se você quiser transferir seu Número de Telefone de Cobrança (BTN), selecione uma das seguintes opções:
  - Estou fazendo a portabilidade do meu BTN e quero substituí-lo por um novo BTN que estou fornecendo. Posso confirmar que este novo BTN está na mesma conta e com a operadora atual.
  - Estou fazendo a portabilidade do meu BTN e quero fechar minha conta com minha operadora atual.

- Estou fazendo a portabilidade do meu BTN porque minha conta está configurada para que cada número de telefone seja seu próprio BTN. (Selecione esta opção somente quando sua conta com a operadora atual estiver configurada desta forma.)
- Depois de escolher uma opção, anexe sua Carta de Agência (LOA) à solicitação.

Para portar números internacionais:

- Você deve usar o tipo de produto SIP Media Application Dial-In para números de telefone fora dos EUA.
  - Tipo de número (local ou gratuito)
  - Números de telefone existentes para fazer a portabilidade.
  - Estime o volume de uso
  - País
- a. Na lista Tipo de número de telefone, selecione Business Calling, SIP Media Application Dial-In ou Voice Connector.
  - b. Em Número de telefone, insira pelo menos um número de telefone, mesmo se você estiver transferindo vários números.
  - c. Em Data de portabilidade, insira a data de portabilidade desejada.
  - d. Em Horário de portabilidade, insira o horário desejado.
  - e. Escolha Próxima etapa: solucione ou entre em contato conosco.
5. Em Resolver agora ou entre em contato conosco, escolha Entre em contato conosco.
  6. Na lista de idiomas de contato preferidos, escolha um idioma
  7. Escolha Web ou Telefone. Se você escolher Telefone, insira seu número de telefone. Ao terminar, escolha Enviar.

AWS Support permite que você saiba se seus números de telefone podem ser transferidos da sua operadora de telefonia existente. Se possível, você precisa enviar todos os documentos necessários. As etapas na próxima seção explicam como enviar esses documentos.

## Envio dos documentos necessários

Depois que o AWS Support disser que você pode transferir números de telefone, você precisará enviar todos os documentos necessários. As etapas a seguir explicam como.

**Note**

AWS O Support fornece um link seguro do Amazon S3 para fazer o upload de todos os documentos solicitados. Não prossiga até receber o link.

Para enviar documentos

1. [Abra o console do Amazon Chime em](https://chime.aws.amazon.com/)<https://chime.aws.amazon.com/>.
2. Faça login na sua AWS conta e abra o link de upload do Amazon S3 gerado especificamente para sua conta.

**Note**

O link expira após dez dias. Ele é gerado especificamente para a conta que criou o caso. O link exige que um usuário autorizado da conta realize o upload.

3. Escolha Adicionar arquivos e selecione os documentos de identidade relacionados à sua solicitação.
4. Expanda a seção Permissões e escolha Especificar permissões individuais de ACL.
5. No final da seção Lista de controle de acesso (ACL), escolha Adicionar favorecido e cole a chave fornecida pelo AWS Support na caixa Favorecido.
6. Em Objetos, escolha a caixa de seleção Ler e, em seguida, escolha Carregar.

Depois de fornecer a Carta de Agência (LOA), Suporte confirme com sua operadora telefônica existente se as informações na LOA estão corretas. Se as informações fornecidas na LOA não corresponderem às informações que a operadora telefônica tiver registrado, o Suporte entrará em contato com você para atualizar as informações fornecidas na LOA.

## Visualizando o status da solicitação

As etapas a seguir explicam como usar o console do Amazon Chime para visualizar o status de suas solicitações de portabilidade.

Para ver o status

1. [Abra o console do Amazon Chime em](https://chime.aws.amazon.com/)<https://chime.aws.amazon.com/>.

2. No painel de navegação, escolha Gerenciamento de números de telefone.
3. Escolha a guia Pedidos.

A coluna Status mostra o status da sua solicitação. Suporte também entra em contato com você com atualizações e solicitações de mais informações, conforme necessário. Para obter mais informações, consulte [Definições de status de transferência de números de telefone](#), mais adiante nesta seção.

## Atribuição de números portados

Depois que sua operadora de telefonia confirmar que a LOA está correta, ela revisa e aprova a porta solicitada. Em seguida, eles Suporte fornecem uma data e hora do Firm Order Commit (FOC) para que a porta ocorra.

Na data do FOC, os números de telefone portados são ativados para uso. Em seguida, você deve atribuir os números aos usuários na conta desejada.

Para atribuir números de telefone

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
2. No painel de navegação, escolha Gerenciamento de números de telefone.
3. Na guia Inventário, marque a caixa de seleção ao lado do número que você deseja atribuir e escolha Atribuir.

### Note

Você só pode escolher um número por vez.

4. Na página Atribuir número de telefone +1 a um perfil de usuário, selecione a conta para o número e escolha Avançar.
5. Selecione o usuário ao qual você deseja atribuir o número e escolha Atribuir.

## Transferindo números de telefone

Você transfere números para fora do Amazon Chime iniciando uma solicitação de portabilidade com sua operadora vencedora. Ao enviar informações para a operadora vencedora, inclua o ID AWS da sua conta como o ID da conta associado ao número de telefone que está sendo transferido.

Quando o processo de transferência terminar e sua transportadora vencedora tiver os números, você deverá cancelar a atribuição e excluir esses números do seu inventário. Para obter mais informações, consulte [Cancelando a atribuição de números de telefone do Amazon Chime Business Calling](#) e [Excluir números de telefone](#) neste guia.

 Important

- A capacidade de transferir números depende da capacidade da operadora vencedora de aceitar esses números.
- Verificar a autenticidade da solicitação de portabilidade da operadora vencedora é fundamental para a segurança do seu número de telefone. Se os detalhes da conta não estiverem corretos (por exemplo, há uma incompatibilidade no ID da conta), sua solicitação de port-out poderá ser rejeitada, causando atrasos e exigindo que você reenvie sua solicitação.

### (Opcional) Como solicitar um PIN para proteger seu número

Para segurança adicional, você pode entrar em contato conosco para aplicar um PIN ao seu número. A operadora vencedora então usa esse PIN. Siga estas etapas:

Para solicitar um PIN

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
2. No painel de navegação, em Fale conosco, escolha Support.

Isso leva você ao console do AWS Support.

 Note

Você também pode ir diretamente para a página [AWS Support central](#). Se você fizer isso, escolha Criar caso e siga as etapas abaixo.

3. Em Como podemos ajudar, faça o seguinte:
  - a. Escolha Conta e faturamento.
  - b. Na lista de serviços, escolha Chime SDK (gerenciamento de números).
  - c. Na lista de categorias, escolha Número de telefone e porta de saída.

- d. Selecione Próxima etapa: informações adicionais.
4. Em Informações adicionais, faça o seguinte
    - a. Em Assunto, insira **Porting phone numbers out**.
    - b. Em Descrição, insira o seguinte.

**I would like to assign a pin to my phone number: Pin: ABCD123 Phone Number: 1234567890**

 Note

Você deve fornecer um PIN alfanumérico de 4 a 10 caracteres.

AWS O Support associa um PIN ao número de telefone. Ao solicitar a porta com a operadora vencedora, forneça o ID AWS da conta e o PIN. Usaremos essas informações para validar todas as solicitações de porta recebidas para seu número.

## Definições de status de transferência de números de telefone

Após o envio de uma solicitação para transferir números de telefones existentes para o Amazon Chime, é possível visualizar o status da solicitação de portabilidade no console do Amazon Chime em Chamadas, Gerenciamento de números de telefone e Pendente.

Os status e as definições de portabilidade incluem o seguinte:

### CANCELADO

Suporte cancelou a ordem de portabilidade devido a um problema com a porta, como uma solicitação de cancelamento da transportadora ou de você. Suporte entra em contato com você com detalhes.

### CANCEL\_REQUESTED

Suporte está processando o cancelamento do pedido de portabilidade devido a um problema com o porto, como uma solicitação de cancelamento da transportadora ou de você. Suporte entra em contato com você com detalhes.

## CHANGE\_REQUESTED

Suporte está processando sua solicitação de alteração e a resposta da transportadora está pendente. Permita um tempo de processamento adicional.

## CONCLUÍDO

Seu pedido de portabilidade está concluído, e seus números de telefone são ativados.

## EXCEPTION

Suporte entra em contato com você para obter detalhes adicionais necessários para concluir a solicitação de porta. Permita um tempo de processamento adicional.

## FOC

A data do FOC é confirmada com a transportadora. Suporte entra em contato com você para confirmar a data.

## DOCUMENTOS PENDENTES

Suporte entra em contato com você para obter documentos adicionais necessários para concluir a solicitação de porta. Permita um tempo de processamento adicional.

## SUBMITTED

Seu pedido de portabilidade é enviado, e a resposta da operadora está pendente.

# Atribuição de números de telefone do Amazon Chime Business Calling

Use a página Inventário de gerenciamento de números de telefone para atribuir números de telefone do Amazon Chime Business Calling a usuários individuais.

Para atribuir números de telefone do Amazon Chime Business Calling

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/.](https://chime.aws.amazon.com/)
2. No painel de navegação, em Chamadas, selecione Gerenciamento de números de telefone.
3. Na guia Inventário, selecione o número de telefone que você deseja atribuir.
4. Selecione Assign (Atribuir).
5. Selecione a conta à qual o usuário pertence e escolha Avançar.
6. Selecione o usuário e escolha Atribuir.

Quando você altera um número de telefone ou as permissões de um número de telefone, recomendamos fornecer ao usuário suas informações novas ou de permissões. Antes de poder acessar os novos recursos de número de telefone ou permissões, os usuários devem sair da conta do Amazon Chime e entrar novamente.

## Cancelando a atribuição de números de telefone do Amazon Chime Business Calling

O procedimento a seguir cancela a atribuição de números de telefone dos usuários do Amazon Chime Business Calling.

Para cancelar a atribuição de números de telefone

1. [Abra o console do Amazon Chime em](https://chime.aws.amazon.com/)<https://chime.aws.amazon.com/>.
2. No painel de navegação, em Chamadas, selecione Gerenciamento de números de telefone.
3. Na guia Inventário, selecione o número de telefone que você deseja cancelar a atribuição.
4. Selecione Unassign (Cancelar a atribuição).
5. Marque a caixa de seleção e selecione Unassign (Cancelar a atribuição).

Você pode ver os detalhes dos números em seu inventário. Por exemplo, você pode ver se as chamadas telefônicas e as mensagens de texto estão habilitadas.

Como visualizar detalhes dos números de telefone do inventário

1. [Abra o console do Amazon Chime em](https://chime.aws.amazon.com/)<https://chime.aws.amazon.com/>.
2. No painel de navegação, em Chamadas, selecione Gerenciamento de números de telefone.
3. Selecione Inventário e escolha o número de telefone que você deseja visualizar.
4. Abra a lista de Ações e escolha Visualizar detalhes.

## Usando nomes de chamadas externas

Os nomes de chamadas externas atuam como IDs chamadores. Você pode definir um nome de chamada padrão para um ou mais números de telefone em seu inventário. Você também pode definir nomes de chamada exclusivos para números de telefone individuais. Os nomes então aparecem para os destinatários das chamadas externas feitas usando esses números de telefone. Os nomes

de chamada se aplicam a todos os tipos de produtos com números de telefone. É possível atualizar os nomes uma vez a cada sete dias.

Por exemplo, você pode definir um nome de chamada padrão de Departamento 5 para todos os números de telefone desse departamento. Você também pode definir um nome exclusivo de Jane Doe para a chefe do departamento.

As etapas a seguir explicam como definir nomes de chamadas de saída padrão e individuais.

Para definir um nome de chamada

1. [Abra o console do Amazon Chime em `https://chime.aws.amazon.com/`.](https://chime.aws.amazon.com/)
2. No painel de navegação, em Chamadas, selecione Gerenciamento de números de telefone.
3. Na guia Inventário, faça o seguinte: marque as caixas de seleção ao lado dos números de telefone que você deseja atualizar.
  - Para definir um nome de chamada padrão para vários números, marque as caixas de seleção ao lado desses números.
  - Para definir um nome de chamada individual, selecione o número desejado.
4. Abra a lista de Ações e escolha Atualizar nome de chamada padrão.
5. Em Nome de chamada padrão, insira um nome com até 15 caracteres.
6. Escolha Salvar.

Aguarde 72 horas para que o sistema atualize o nome de chamada padrão.

## Excluir números de telefone

### Important

Somente os administradores de sistema do Amazon Chime podem concluir essas etapas. Antes de excluir, é necessário cancelar a atribuição de todos os números de telefone.

Ao provisionar um número de telefone, você o solicita a partir de um conjunto de números que o Amazon Chime mantém. A exclusão de um número o move de volta para o grupo. Quando você exclui um número, ele primeiro vai para sua fila de exclusão, onde fica retido por sete dias. Durante esse tempo, você pode mover o número de volta para o seu inventário. Após sete dias, o sistema

exclui automaticamente o número da fila de espera e o desassocia da sua conta. Isso retorna o número para o pool numérico. Se você precisar recuperar um número após o sistema excluí-lo da fila de espera, siga as etapas em [Provisionar números de telefone](#), mas esteja ciente de que o número pode não estar disponível.

Como excluir números de telefone não atribuídos

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
2. No painel de navegação, em Chamadas, selecione Gerenciamento de números de telefone.
3. Selecione Inventário e um ou mais números de telefone que você deseja excluir.
4. Abra a lista Ações e escolha Excluir número(s) de telefone.
5. Marque a caixa de seleção e selecione Excluir.

Os números de telefone excluídos são mantidos na Fila de exclusão por sete dias e depois são excluídos permanentemente.

## Restaurar números de telefone excluídos

Você pode restaurar números de telefone excluídos da Fila de exclusão até sete dias depois de terem sido excluídos. A restauração um número de telefone o move de volta para o Inventory (Inventário).

Como restaurar números de telefone excluídos

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
2. No painel de navegação, em Chamadas, selecione Gerenciamento de números de telefone.
3. Selecione Fila de exclusão e um ou mais números de telefone que você quer restaurar.
4. Selecione Move to inventory (Mover para o inventário).

# Gerenciar configurações globais no Amazon Chime

Você usa o console do Amazon Chime para gerenciar as configurações de registro detalhado da chamada e as configurações do relatório de uso.

## Tópicos

- [Configurar registros de detalhes de chamadas](#)
- [Configurando relatórios de uso](#)

## Configurar registros de detalhes de chamadas

Antes de definir as configurações de registros de detalhes de chamadas para sua conta administrativa do Amazon Chime, você deve criar um bucket do Amazon Simple Storage Service. O bucket do Amazon S3 é usado como o destino de log para seus registros de detalhes de chamadas. Ao definir as configurações de registros de detalhes de chamadas, você concede ao Amazon Chime acesso de leitura e gravação para o bucket do Amazon S3 para salvar e gerenciar seus dados. Para obter informações sobre a criação de um arquivo para um bucket do Amazon S3, consulte [Conceitos básicos do Amazon S3](#), no Guia do usuário do Amazon Simple Storage Service.

Você pode definir as configurações de registro de detalhes da chamada para o Amazon Chime Business Calling. Para obter mais informações sobre Amazon Chime Business Calling, consulte [Gerenciar números de telefone no Amazon Chime](#).

Para definir as configurações de registros de detalhes de chamadas

1. Crie um bucket do Amazon S3 seguindo as etapas em [Conceitos básicos do Amazon S3](#), no Guia do usuário do Amazon Simple Storage Service.
2. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
3. Em Configurações globais, selecione Registros de detalhes de chamadas.
4. Escolha Configuração do Business Calling.
5. Em Destino do log, selecione o bucket do Amazon S3.
6. Escolha Salvar.

Você pode interromper o registro em log dos registros de detalhes de chamada a qualquer momento.

Para interromper o registro em log de registros de detalhes de chamada

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
2. Em Configurações globais, selecione Registros de detalhes de chamadas.
3. Escolha Disable logging (Desativar registro em log) para a configuração aplicável.

## Registros de detalhes de chamadas do Amazon Chime Business Calling

Quando você opta por receber registros de detalhes de chamada para o Amazon Chime Business Calling, eles são enviados ao bucket do Amazon S3. O exemplo a seguir mostra o formato geral de um nome de registro de detalhes de chamada do 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
```

O exemplo a seguir mostra os dados representados no nome de registro de detalhes de chamada.

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

O exemplo a seguir mostra o formato geral de um registro de detalhes de chamada do 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"  
}
```

## Configurando relatórios de uso

Quando você ativa os relatórios de uso, o Amazon Chime gera um arquivo semanal para cada conta de equipe ou empresa gerenciada no console do Amazon Chime.

Antes de definir as configurações do relatório de uso para sua conta administrativa do Amazon Chime, você deve primeiro criar ou escolher um bucket do Amazon S3. O bucket do Amazon S3 é usado como destino do arquivo para seus relatórios de uso. Ao definir as configurações do seu relatório de uso, você concede ao Amazon Chime acesso de leitura e gravação ao bucket do Amazon S3 para salvar e gerenciar seus dados. Para obter mais informações sobre a criação de um bucket do Amazon S3, consulte [Introdução ao Amazon S3](#) no Guia do usuário do Amazon S3 no Guia do usuário do Amazon S3.

Para definir as configurações do relatório de uso

1. Crie ou selecione um bucket do Amazon S3.
  - a. Faça login no seu Conta da AWS e abra o console do [Amazon Chime](#).
  - b. Em Configurações globais, escolha Relatórios de uso.
  - c. Em Destino do relatório, escolha Novo bucket do S3 para criar um novo local e insira um nome seguindo as orientações listadas. Você também pode selecionar Bucket S3 existente se você tiver um bucket Amazon S3 existente onde você deseja armazenar os arquivos.
  - d. Escolha Salvar para criar o novo bucket do Amazon S3 ou selecione um bucket existente do Amazon S3. Isso também ativa os relatórios.
2. Novos relatórios semanais serão colocados no bucket do Amazon S3 e estarão disponíveis na segunda-feira de cada semana para permitir o tempo de processamento.

Você pode desativar os relatórios de uso a qualquer momento.

## Para desativar os relatórios de uso

1. Abra o console do [Amazon Chime](#).
2. Em Configurações globais, escolha Relatórios de uso.
3. Escolha Desativar relatórios para a configuração aplicável.

## Conteúdo do relatório de uso

Os relatórios semanais fornecem dados de atividade do usuário de domingo às 00:00 UTC até sábado às 23:59 UTC. O processamento de dados pode atrasar os relatórios semanais até a segunda-feira da semana.

1. Para visualizar seus dados, volte para a página inicial do AWS console e insira Amazon S3 na pesquisa de serviços.
2. Localize o nome do bucket. Para obter mais informações sobre como criar buckets do Amazon S3, navegar e gerenciar o acesso ao seu bucket do Amazon S3, consulte Introdução ao Amazon S3 no Guia do usuário do [Amazon S3 no Guia do](#) usuário do Amazon S3.
3. O arquivo do relatório de uso semanal será colocado no seguinte local em seu bucket do Amazon S3 (/representa uma pasta).

```
Amazon-Chime-User-Activity-Reports/  
csv/<AWSaccountID>/<year>/<month>/<day>/  
<AmazonChimeAccountName>_<AmazonChimeaccountId>_<yyyymmdd>.csv
```

Por exemplo:

```
Amazon-Chime-User-Activity-Reports/csv/123456789012/2024/11/03/Example  
+Sales_86efea2f-96af-40f7-be75-be057ff52c8c_20241201.csv
```

Os seguintes dados são incluídos em cada relatório para cada usuário em cada conta Team ou Enterprise:

- Nome da conta da equipe ou empresa
- Data de início da semana
- Nome completo do usuário associado à sua conta do Amazon Chime
- Endereço de e-mail do usuário

- Status de registro do usuário
- Data de criação da conta do usuário
- O número de reuniões atendidas durante a semana
- O número de reuniões que o usuário organizou durante a semana
- O número de mensagens enviadas (1:1, publicações em grupo e na sala de bate-papo) durante a semana

# Configuração de salas de conferência

O Amazon Chime pode ser integrado ao hardware de vídeo na sala Cisco, Tandberg, Polycom, Lifesize, Vidyo ou outros quando você usa o protocolo SIP ou H.323.

Para se conectar ao Amazon Chime usando um dispositivo de VTC da sala de conferência compatível com SIP, insira uma das seguintes opções:

- **@meet.chime.in**
- **u@meet.chime.in**
- Um ID da reunião com 10 dígitos, seguido por **@meet.chime.in**

A opção **meet.chime.in** conecta seu dispositivo de sala SIP à região mais próxima do Amazon Chime. Para se conectar a uma região específica, use entradas DNS específicas da região para sistemas de sala SIP. Para obter mais informações, consulte [Sistemas de sala do Session Initiation Protocol \(SIP\)](#).

## Note

Se o seu dispositivo de sala SIP não suportar TLS e precisar de conectividade TCP, entre em contato com o Support. AWS

Se estiver usando um dispositivo compatível apenas com H.323, disque para uma das seguintes opções:

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

Se um firewall estiver filtrando o tráfego entre o dispositivo VTC e o Amazon Chime, abra os intervalos dos protocolos utilizados. Para obter mais informações, consulte [Requisitos de configuração de rede e largura de banda](#).

Na tela inicial do Amazon Chime, insira o ID da reunião com 10 ou 13 dígitos para participar. Você pode encontrar o ID da reunião com 13 dígitos no cliente ou na aplicação web do Amazon Chime, ou escolha a opção Discagem.

## Participar de uma reunião moderada

Se a reunião for moderada e você for o host ou delegado, insira o ID da reunião com 13 dígitos para participar da reunião com essa função. Se você for um moderador, digite a senha do moderador seguida de jogo da velha (#) no teclado de discagem para iniciar a reunião. Se você não for um host, delegado ou moderador, entrará na reunião depois que um moderador iniciá-la.

Os moderadores têm controles de host, o que significa que podem executar mais ações na reunião. Isso inclui interromper a gravação, bloquear e desbloquear a reunião, silenciar todos os outros participantes e encerrar a reunião. Para obter mais informações, consulte [Moderator Actions using phone or in-room video systems](#) no Guia do usuário do Amazon Chime.

### Note

Se você estiver usando o Alexa for Business para participar de reuniões do Amazon Chime, poderá participar como moderador somente se o dispositivo estiver conectado a um sistema de vídeo na sala e você usar o teclado de discagem.

## Dispositivos VTC compatíveis

A tabela a seguir é um subconjunto da lista de dispositivos VTC compatíveis.

Dispositivo	SIP	H.323	Comentário
Cisco SX2 0	Sim	Sim	Audio/Video/ Screen: De e para OK
Cisco DX8 0	Sim	Sim	Audio/Video/ Screen: De e para OK
Lifesize Icon	Sim	Não	Audio/Video/ Screen: De e para OK

Dispositivo	SIP	H.323	Comentário
Polycom Debut	Sim	Sim	Audio/Video/ Screen: De e para OK
Desktop Polycom RealPresence	Não	Sim	Áudio/vídeo: OK, tela: dispositivo de origem OK
Polycom Trio	Sim	Sim	Audio/Video/ Screen: De e para OK
Tandberg C40	Sim	Sim	Audio/Video/ Screen: De e para OK

## Requisitos de configuração de rede e largura de banda

O Amazon Chime requer os destinos e as portas descritos neste tópico para oferecer suporte a vários serviços. Se o tráfego de entrada ou de saída estiver obstruído, isso poderá afetar a possibilidade de usar vários serviços, inclusive áudio, vídeo, compartilhamento de tela ou bate-papo.

O Amazon Chime usa o Amazon Elastic Compute Cloud (Amazon EC2) e outros serviços da AWS na porta TCP/443. Se o firewall bloquear a porta TCP/443, será necessário colocar \*.amazonaws.com em uma lista de permissões ou colocar [intervalos de endereços IP da AWS](#) na Referência geral da AWS para os seguintes serviços:

- Amazon EC2
- Amazon CloudFront
- Amazon Route 53

Expanda as seções a seguir para obter mais informações sobre destinos, portas e largura de banda.

## Destinos e portas necessários

Os seguintes destinos e portas são necessários para executar o Amazon Chime.

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

## Porta de reunião e telefonia

O Amazon Chime usa os destinos e portas a seguir para reuniões e para o Amazon Chime Business Calling.

Destino	Port (Porta)
99.77.128.0/18	UDP/3478

## Sistemas de sala H.323

O Amazon Chime usa os seguintes destinos e portas para sistemas de vídeo na sala H.323.

Destino	Portas
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 do Session Initiation Protocol (SIP)

Os seguintes destinos e portas são recomendados ao executar o Amazon Chime para sistemas de vídeo SIP na sala em seu ambiente.

AWS Região	Destino	Portas
Global (região mais próxima)	99.77.128.0/18	UDP/10000:60000
	34.212.95.128/25	
	34.223.21.0/25	
	52.55.62.128/25	

AWS Região	Destino	Portas
	52.55.63.0/25	
Global	meet.chime.in 13.248.147.139 76.223.18.152	TCP/5061
Leste dos EUA (Norte da Virgínia)	meet.ue1.chime.in	TCP/5061
Oeste dos EUA (Oregon)	meet.uw2.chime.in	TCP/5061
Ásia-Pacífico (Singapura)	meet.as1.chime.in	TCP/5061
Ásia-Pacífico (Sydney)	meet.as2.chime.in	TCP/5061
Ásia-Pacífico (Tóquio)	meet.an1.chime.in	TCP/5061
Europa (Irlanda)	meet.ew1.chime.in	TCP/5061
América do Sul (São Paulo)	meet.se1.chime.in	TCP/5061

## Requisitos de largura de banda

O Amazon Chime tem os seguintes requisitos de largura de banda para áudio, vídeo e compartilhamento de tela:

- **Áudio**
  - Chamada individual: 54 kbps para cima e para baixo
  - Chamada grande: não mais do que 32 kbps extras para baixo em 50 chamadores
- **Vídeo**
  - Chamada individual: 650 kbps para cima e para baixo
  - Modo HD: 1.400 kbps para cima e para baixo
  - De três a quatro pessoas: 450 kbps para cima e  $(N-1)*400$  kbps para baixo
  - De cinco a 16 pessoas: 184 kbps para cima e  $(N-1)*134$  kbps para baixo

- A largura da banda alta ou baixa se adapta para baixo de acordo com as condições de rede
- Compartilhamento de tela
  - 1,2 mbps acima (apresentação) e abaixo (visualização) para alta qualidade. Isso se adapta até o limite mínimo de 320 kbps com base nas condições de rede.
  - Controle remoto: 800 kbps fixos

# Visualizar relatórios

Para tomar decisões mais informadas e aumentar a produtividade da organização, você pode acessar os dados de uso e feedback diretamente pelo console. Os dados do relatório são atualizados diariamente, embora possa haver um atraso de até 48 horas.

Para ver relatórios de uso e feedback

1. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
2. Escolha Reports (Relatórios), Dashboard (Painel).
3. Na página Usage and feedback dashboard report (Relatório do painel de uso e feedback), veja os seguintes dados:

## Note

Para obter mais informações sobre os dados disponíveis, consulte [Painel do relatório do Amazon Chime Report e detalhes de atividades de usuários](#).

- Intervalo de datas (UTC): o intervalo de datas do relatório.
- Usuários registrados: o número de usuários que se cadastraram no Amazon Chime.
- Usuários ativos: o número de usuários que participaram de uma reunião ou enviaram uma mensagem com o Amazon Chime.
- Reuniões realizadas: o número total de reuniões que se encerraram. Você pode selecionar uma determinada reunião para ver detalhes, inclusive o ID da conferência, a hora de início, o tipo, o organizador, a duração e o número de participantes. Escolha um Conference ID (ID de conferência) ou Meeting organizer (Organizador da reunião) específico para ver detalhes adicionais, inclusive participantes, eventos da lista de reuniões, tipo de cliente e feedback da reunião.
- Satisfação com a reunião — A porcentagem de respostas positivas dadas à end-of-meeting pesquisa.
- Mensagens de chat enviadas: o número de mensagens de chat enviadas pelos usuários.

# Estender o cliente de desktop do Amazon Chime

Você pode ampliar os recursos do cliente de desktop Amazon Chime adicionando chatbots, sessões de telefone proxy e webhooks. Os chatbots permitem que os usuários realizem tarefas como consultar sistemas internos em busca de informações. As sessões telefônicas por proxy permitem que os usuários liguem e enviem mensagens de texto sem revelar seus números de telefone. Os webhooks podem enviar mensagens automaticamente para salas de conversa. Por exemplo, um webhook pode enviar lembretes de reunião para uma equipe, junto com um link para a reunião.

## Tópicos

- [Gerenciamento de usuários](#)
- [Integração de chatbots ao cliente de desktop Amazon Chime](#)
- [Criar webhooks para o Amazon Chime](#)

## Gerenciamento de usuários

Os trechos de código a seguir podem ajudar você a gerenciar usuários do Amazon Chime. Todos os exemplos neste tópico usam Java.

## Tópicos

- [Convidar vários usuários](#)
- [Fazer download das listas de usuários](#)
- [Desconectar vários usuários](#)
- [Atualizar dados pessoais do usuário PINs](#)

## Convidar vários usuários

O exemplo a seguir mostra como convidar vários usuários a uma conta Team do 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);
```

## Fazer download das listas de usuários

O exemplo a seguir mostra como baixar uma lista de usuários associados à sua conta administrativa do Amazon Chime em 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();
```

## Desconectar vários usuários

O exemplo a seguir mostra como desconectar vários usuários da conta administrativa do 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);
}
```

## Atualizar dados pessoais do usuário PINs

O exemplo a seguir mostra como redefinir o PIN de reunião pessoal para um usuário especificado do Amazon Chime.

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

ResetPersonalPINResult result = chime.resetPersonalPIN(request);

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

## Integração de chatbots ao cliente de desktop Amazon Chime

Você pode usar o AWS Command Line Interface (AWS CLI), a API do Amazon Chime ou o AWS SDK para integrar chatbots ao Amazon Chime. Os chatbots permitem que você use o poder do Amazon Lex, AWS Lambda, e de outros AWS serviços para simplificar tarefas comuns com interfaces conversacionais inteligentes que são acessíveis aos usuários nas salas de bate-papo do Amazon Chime.

Se você for administrador de conta empresarial do Amazon Chime, poderá usar chatbots para permitir que os usuários realizem tarefas como:

- Consultar seus sistemas internos para obter informações.
- Automatizar tarefas.
- Receber notificações de problemas críticos.

- Criar de tíquetes de suporte.

Para obter mais informações sobre as contas empresariais do Amazon Chime, consulte [Gerenciar suas contas do Amazon Chime](#).

Se administrar uma conta empresarial do Amazon Chime, você poderá criar até dez chatbots para integração com o Amazon Chime. Os chatbots só podem ser usados em salas de chat criadas por membros de sua conta. Somente os administradores de sala de chat podem adicionar chatbots a uma sala de chat. Depois que um chatbot for adicionado a uma sala de chat, os membros da sala poderão interagir com o bot usando comandos fornecidos pelo criador do bot. Para obter mais informações, consulte a próxima seção deste tópico.

Usuários de Linux e macOS podem criar um exemplo de chatbot personalizado. Para obter mais informações, consulte [Criar chatbots personalizados para o Amazon Chime](#).

## Conteúdo

- [Usar chatbots com o Amazon Chime](#)
- [Eventos do Amazon Chime enviados para chatbots](#)

## Usar chatbots com o Amazon Chime

Se administrar uma conta empresarial do Amazon Chime, você poderá criar até dez chatbots para integração com o Amazon Chime. Os chatbots só podem ser usados em salas de chat criadas por membros de sua conta. Somente os administradores de sala de chat podem adicionar chatbots a uma sala de chat. Depois que um chatbot for adicionado a uma sala de chat, os membros da sala poderão interagir com o bot usando comandos fornecidos pelo criador do bot. Para obter mais informações, consulte [Usar chatbots com o Amazon Chime](#) no Guia de administração do Amazon Chime.

Você também pode usar a operação de API do Amazon Chime para habilitar ou interromper chatbots em sua conta do Amazon Chime. Para obter mais informações, consulte [Atualizar os chatbots](#).

### Note

Você não pode excluir chatbots. Para impedir que um chatbot seja usado em sua conta, use a operação da API Amazon [UpdateBot](#)Chime na Amazon Chime API Reference. Quando você interrompe um chatbot, os administradores de sala de chat podem removê-lo de

uma sala de chat, mas eles não podem adicioná-lo a uma sala de chat. Os usuários que @mencionarem um chatbot interrompido em uma sala de chat receberão uma mensagem de erro.

## Pré-requisitos

Antes de iniciar o procedimento para integrar chatbots ao Amazon Chime, complete os seguintes pré-requisitos:

- Crie um chatbot.
- Crie o endpoint de saída para que o Amazon Chime envie eventos ao seu bot. Escolha a partir do ARN de uma função AWS Lambda ou de um endpoint HTTPS. Para obter mais informações sobre o Lambda, consulte o Manual do desenvolvedor do [AWS Lambda](#).

## Práticas Recomendadas de DNS para endpoints HTTPS

Recomendamos as seguintes melhores práticas ao atribuir o DNS ao endpoint HTTPS:

- Use um subdomínio DNS dedicado ao endpoint do bot.
- Use apenas os registros A para apontar para o endpoint do bot.
- Proteja seus servidores DNS e a conta do registrador DNS para impedir o sequestro de domínio.
- Use certificados intermediários TLS válidos publicamente que sejam dedicados ao endpoint do bot.
- Verifique criptograficamente a assinatura da mensagem do bot antes de atuar em uma mensagem de bot.

Depois de criar seu chatbot, use a operação AWS Command Line Interface (AWS CLI) ou a API do Amazon Chime para concluir as tarefas descritas nas seções a seguir.

## Tarefas

- [Etapa 1: Integrar um chatbot ao Amazon Chime](#)
- [Etapa 2: Configurar o endpoint de saída para um chatbot do Amazon Chime](#)
- [Etapa 3: Adicionar o chatbot a uma sala de chat do Amazon Chime](#)
- [Autenticar solicitações do chatbot](#)
- [Atualizar os chatbots](#)

## Etapa 1: Integrar um chatbot ao Amazon Chime

Depois de concluir os [pré-requisitos](#), integre seu chatbot ao Amazon Chime usando a API ou Amazon Chime. AWS CLI

### Note

Esses procedimentos criam um nome e endereço de e-mail para o seu chatbot. Os nomes e endereços de e-mail dos bots não podem ser alterados após a criação.

### AWS CLI

Para integrar um chatbot usando o AWS CLI

1. Para integrar seu chatbot ao Amazon Chime, use o comando `create-bot` na AWS CLI.

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

- a. Insira um nome de exibição do chatbot com até 55 caracteres alfanuméricos ou especiais (por exemplo, +, -, %).
  - b. Insira o nome de domínio registrado para sua conta empresarial do Amazon Chime.
2. O Amazon Chime retorna uma resposta que inclui a ID do 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 e salve o ID e o endereço de e-mail do bot para usar nos procedimentos a seguir.

## API do Amazon Chime

### Como integrar um chatbot usando a API do Amazon Chime

1. Para integrar seu chatbot ao Amazon Chime, use a operação de API na Referência de API [CreateBot](#) do Amazon Chime.
  - a. Insira um nome de exibição do chatbot com até 55 caracteres alfanuméricos ou especiais (por exemplo, +, -, %).
  - b. Insira o nome de domínio registrado para sua conta empresarial do Amazon Chime.
2. O Amazon Chime retorna uma resposta que inclui a ID do bot. Copie e salve o ID do bot e o endereço de e-mail. O endereço de e-mail do bot tem a seguinte aparência: *exampleBot-chimebot@example.com*.

## AWS SDK for Java

O código de exemplo a seguir demonstra como integrar um chatbot usando o AWS SDK for Java.

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

chime.createBot(createBotRequest);
```

O Amazon Chime retorna uma resposta que inclui a ID do bot. Copie e salve o ID do bot e o endereço de e-mail. O endereço de e-mail do bot tem a seguinte aparência: *exampleBot-chimebot@example.com*.

## Etapa 2: Configurar o endpoint de saída para um chatbot do Amazon Chime

Depois de criar uma ID de chatbot para sua conta empresarial do Amazon Chime, configure o endpoint de saída para o Amazon Chime usar para enviar mensagens ao seu bot. [O endpoint de saída pode ser um AWS Lambda ARN de função ou um endpoint HTTPS que você criou como parte dos pré-requisitos](#). Para obter mais informações sobre o Lambda, consulte o Manual do desenvolvedor do [AWS Lambda](#).

**Note**

Se o endpoint HTTPS de saída para seu bot não estiver configurado ou estiver vazio, os administradores de sala de chat não poderão adicionar o bot a uma sala de chat. Além disso, os usuários da sala de chat não podem interagir com o bot.

## AWS CLI

Para configurar um endpoint de saída para seu chatbot, use o comando `put-events-configuration` no AWS CLI. Configure um ARN da função do Lambda ou um endpoint HTTPS de saída.

### 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
```

O Amazon Chime responde com o ID do bot e o endpoint HTTPS.

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

## API do Amazon Chime

Para configurar o endpoint de saída do seu chatbot, use a operação da API Amazon Chime na Amazon Chime [PutEventsConfiguration](#) API Reference. Configure um ARN da função do Lambda ou um endpoint HTTPS de saída.

- Se você configurar um ARN de função do Lambda, o Amazon Chime chama o Lambda para adicionar permissão para permitir que a conta AWS do administrador do Amazon Chime invoque o ARN da função Lambda fornecida. Isso é seguido por uma invocação de simulação para verificar se o Amazon Chime tem permissão para invocar a função. Se houver falha na adição das permissões ou na invocação da simulação, a solicitação PutEventsConfiguration retornará um erro HTTP 4xx.
- Se você configurar um endpoint HTTPS: o Amazon Chime verifica o endpoint enviando uma solicitação HTTP POST com uma carga útil JSON do Challenge para o endpoint HTTPS de saída que você forneceu na etapa anterior. Seu endpoint HTTPS de saída deve responder repetindo o parâmetro do Challenge no formato JSON. Os exemplos a seguir mostram a solicitação e uma resposta válida.

### Request

```
HTTPS POST

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

### Response

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

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

Se houver falha no handshake do Challenge, a solicitação PutEventsConfiguration retornará um erro HTTP 4xx.

## AWS SDK for Java

O código de exemplo a seguir demonstra como configurar um endpoint usando o AWS SDK for 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);
```

### Etapa 3: Adicionar o chatbot a uma sala de chat do Amazon Chime

Somente os administradores de sala de chat podem adicionar chatbot a uma sala de chat. Eles usam o endereço de e-mail do chatbot criado na [Etapa 1](#).

Como adicionar um chatbot a uma sala de bate-papo

1. Abra o cliente de desktop do Amazon Chime ou a aplicação web.
2. Escolha o ícone de engrenagem no canto superior direito e selecione Gerenciar webhooks.
3. Escolha Add bot (Adicionar bot).
4. Para Endereço de e-mail, insira o endereço de e-mail do bot.
5. Escolha Adicionar.

O nome do bot aparecerá na lista de salas de chat. Se houver ações adicionais necessárias para adicionar um chatbot a uma sala de chat, forneça as ações ao administrador da sala de chat.

Depois que o chatbot for adicionado à sala de chat, forneça os comandos do chatbot aos usuários da sala de chat. Uma maneira de fazer isso é programar seu chatbot para enviar a ajuda de comandos para a sala de chat ao receber o convite para a sala de chat. A AWS também recomenda a criação de um comando de ajuda para os usuários de seu chatbot usarem.

### Autenticar solicitações do chatbot

Você pode autenticar solicitações enviadas ao seu chatbot a partir de uma sala de chat do Amazon Chime. Para fazer isso, calcule uma assinatura com base na solicitação. Depois, valide que a

assinatura computada corresponde à do cabeçalho da solicitação. O Amazon Chime usa o SHA256 hash HMAC para gerar a assinatura.

Se o seu chatbot estiver configurado para o Amazon Chime usando um endpoint HTTPS de saída, siga as etapas de autenticação abaixo.

Para validar uma solicitação assinada do Amazon Chime para um chatbot com um endpoint HTTPS de saída configurado

1. Obtenha o cabeçalho Chime-Signature na solicitação HTTP.
2. Obtenha o cabeçalho Chime-Request-Timestamp e o body (corpo) da solicitação. Depois, use uma barra vertical como o delimitador entre os dois elementos para formar uma string.
3. Use a SecurityTokenpartir da CreateBot resposta como a chave inicial de HMAC\_SHA\_256 e faça o hash da string que você criou na etapa 2.
4. Codifique o byte com hash com o codificador Base64 para uma string de assinatura.
5. Compare a assinatura computada com aquela no cabeçalho Chime-Signature.

O exemplo de código a seguir demonstra como gerar uma assinatura usando 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;
    }
}
```

O endpoint HTTPS de saída deve responder à solicitação do Amazon Chime com 200 OK dentro de 2 segundos. Caso contrário, haverá falha na solicitação. Se o endpoint HTTPS de saída ficar indisponível após 2 segundos, possivelmente devido a uma conexão ou tempo limite de leitura, ou se o Amazon Chime receber um código de resposta 5xx, o tentará executar a solicitação duas vezes. A primeira nova tentativa será enviada 200 milissegundos após a falha na solicitação inicial. A segunda nova tentativa será enviada 400 milissegundos após a falha da nova tentativa. Se o endpoint HTTPS de saída ainda estiver indisponível após a segunda nova tentativa, haverá falha na solicitação.

#### Note

O Chime-Request-Timestamp é alterado cada vez que a solicitação é executada novamente.

Se o seu chatbot estiver configurado para que o Amazon Chime use o ARN de uma função do Lambda, siga as etapas de autenticação abaixo.

Como validar uma solicitação assinada do Amazon Chime para um chatbot com o ARN de uma função do Lambda configurada

1. Obtenha o Chime-Signature e o Chime-Request-Timestamp da solicitação Lambda, no formato JSON codificado em Base64. ClientContext

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

2. Obtenha o body (corpo) da solicitação a partir da carga da solicitação.
3. Use a SecurityTokenpartir da CreateBot resposta como a chave inicial de HMAC\_SHA\_256 e faça o hash da string que você criou.
4. Codifique o byte com hash com o codificador Base64 para uma string de assinatura.
5. Compare a assinatura computada com aquela no cabeçalho Chime-Signature.

Se ocorrer uma `com.amazonaws.SdkClientException` durante a invocação do Lambda, o Amazon Chime tentará executar a solicitação duas vezes.

## Atualizar os chatbots

Como administrador da conta do Amazon Chime, você pode usar a API do Amazon Chime com o SDK AWS CLI ou visualizar AWS os detalhes do seu chatbot. Você também pode habilitar ou impedir que seus chatbots sejam usados em sua conta. Você também pode gerar novamente os tokens de segurança para seu chatbot.

Para obter mais informações, consulte os tópicos a seguir na Referência da API do Amazon Chime:

- [GetBot](#)— Obtém os detalhes do seu chatbot, como endereço de e-mail e tipo de bot.
- [UpdateBot](#)— Ativa ou impede que um chatbot seja usado em sua conta.
- [RegenerateSecurityToken](#)— Regenera o token de segurança do seu chatbot.

Você também pode optar por alterar a `PutEventsConfiguration` de seu chatbot. Por exemplo, se o seu chatbot foi configurado inicialmente para usar um endpoint HTTPS de saída, você poderá excluir a configuração de eventos anteriores e inserir uma nova configuração de eventos para o ARN de uma função do Lambda.

Para obter mais informações, consulte os tópicos a seguir na Referência da API do Amazon Chime:

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

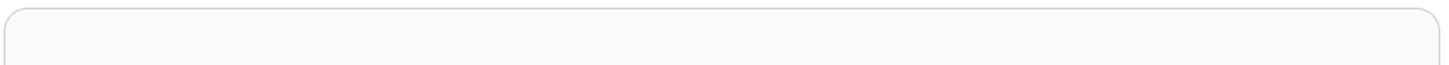
## Eventos do Amazon Chime enviados para chatbots

Os seguintes eventos são enviados para seu chatbot do Amazon Chime:

- Convidar: enviado quando seu chatbot é adicionado a uma sala de chat do Amazon Chime.
- Mencionar: enviado quando um usuário em uma sala de chat @menciona seu chatbot.
- Remover: enviado quando seu chatbot é removido de uma sala de chat do Amazon Chime.

Os exemplos a seguir mostram a carga JSON enviada para o chatbot para cada um desses eventos.

Example : evento Convidar



```

{
  "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=ABCDEFGHIJK1LMnoP2Q3RST4uvwxyZAbC56DeFghIJKLM7N8OP9QRsTuV0WXYZABcdefgHiJ"
  },
  "EventTimestamp": "2019-04-04T21:27:52.736Z"
}

```

### Example : evento Mencionar

```

{
  "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**

O URL `InboundHttpsEndpoint` para um evento Mencionar expira 2 minutos depois de enviado.

Example : evento Remove

```
{
  "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"
}
```

## Criar webhooks para o Amazon Chime

Os webhooks permitem que aplicações web se comuniquem entre si em tempo real. Normalmente, os webhooks enviam notificações quando ocorre uma ação. Por exemplo, digamos que você administra um site de compras on-line. Os webhooks podem notificá-lo quando um cliente adiciona itens a um carrinho de compras, paga por um pedido ou envia um comentário. Os webhooks não precisam de tanta programação quanto os aplicativos tradicionais e não usam tanto poder de processamento. Sem um webhook, um programa precisa pesquisar dados com frequência para obtê-los em tempo real. Com um webhook, o aplicativo de envio publica os dados imediatamente.

Os webhooks de entrada que você cria podem enviar mensagens de forma programática a salas de chat do Amazon Chime. Por exemplo, um webhook pode notificar uma equipe de atendimento ao cliente sobre a criação de um novo tíquete de alta prioridade e adicionar um link ao tíquete na sala de chat.

As mensagens do Webhooks podem ser formatadas com markdown e podem incluir emojis. Links HTTP e endereços de e-mail são renderizados como links ativos. As mensagens também podem

incluir anotações @All e @Present para alertar todos os membros e apresentar os membros de uma sala de bate-papo, respectivamente. Para @mencionar diretamente um participante da sala de bate-papo, use seu alias ou endereço de e-mail completo. Por exemplo, @alias, ou @alias@domain.com.

Os webhooks só podem fazer parte de uma sala de chat e não podem ser compartilhados. Os administradores da sala de chat do Amazon Chime podem adicionar até dez webhooks para cada sala de chat.

Depois de criar um webhook, você poderá integrá-lo a uma sala de chat do Amazon Chime, conforme mostrado no procedimento a seguir.

Para integrar um webhook a uma sala de chat

1. Obtenha o URL do webhook com o administrador da sala de chat. Para obter mais informações, consulte [Adding webhooks to a chat room](#) no Guia do usuário do Amazon Chime.
2. Use o URL do webhook no script ou aplicativo que você criou para enviar mensagens para a sala de chat:
  - a. O URL aceita uma solicitação HTTP POST.
  - b. Os webhooks do Amazon Chime aceitam uma carga útil JSON com uma única chave Content. Veja a seguir um comando curl de amostra com uma carga útil de amostra:

```
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"}'
```

Veja a seguir um exemplo de PowerShell comando para usuários do 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"}'
```

Depois que o programa externo envia o HTTP POST para a URL do webhook, o servidor verifica se o webhook é válido e se há uma sala de bate-papo atribuída a ele. O webhook é exibido na lista de salas de bate-papo com um ícone de webhook ao lado do nome. As mensagens da sala de bate-

papo enviadas pelo webhook são exibidas na sala de bate-papo com o nome do webhook seguido por (Webhook).

 Note

O CORS não está habilitado atualmente para webhooks.

## Solucionar de problemas de erros de webhook

A seguir, uma lista de erros relacionados a webhooks:

- O limite de taxa do webhook recebido para cada um deles é de 1 TPS por sala de bate-papo. O controle de utilização resulta em um erro HTTP 429.
- As mensagens postadas por um webhook devem ter 4 KB ou menos. Um payload de mensagem maior resulta em um erro HTTP 413.
- As mensagens publicadas por um webhook com anotações @Todas e @Presentes funcionam somente em salas de bate-papo com 50 membros ou menos. Mais de 50 membros resultará em um erro HTTP 400.
- Se o URL do webhook for gerado novamente, o uso do URL antigo resultará em um erro HTTP 404.
- Se o webhook em uma sala for excluído, o uso do URL antigo resultará em um erro HTTP 404.
- URLs Resultado de webhook inválido em erros HTTP 403.
- Se o serviço estiver indisponível, o usuário receberá um erro HTTP 503 na resposta.

# Suporte administrativo do Amazon Chime

## Note

Para obter ajuda com sua conta de compras da Amazon, acesse o [Atendimento ao Cliente na amazon.com](#).

Se você precisar entrar em contato com o suporte do Amazon Chime, escolha uma das seguintes opções:

- Se você tiver uma conta do AWS Support, acesse a [Central de Suporte](#) e envie um ticket.
- Caso contrário, abra o [AWS Management Console](#) e selecione Amazon Chime, Suporte e Enviar solicitação.

Forneça o máximo possível das seguintes informações:

- Uma descrição detalhada do problema.
- A hora em que o problema ocorreu, inclusive o fuso horário.
- Sua versão do Amazon Chime. Para encontrar o número da versão:
  - No Windows, escolha Ajuda, Sobre o Amazon Chime.
  - No macOS, escolha Amazon Chime, About Amazon Chime (Sobre o Amazon Chime).
  - Em iOS e Android, selecione Settings (Configurações), About (Sobre).
- O ID de referência do log. Para encontrar esse ID:
  - Em Windows e macOS, escolha Help (Ajuda), Send Diagnostic Logs (Enviar logs de diagnóstico).
  - Em iOS e Android, selecione Settings (Configurações), Send Diagnostic Logs (Enviar logs de diagnóstico).
- Se o problema estiver relacionado a uma reunião, o ID da reunião.

# Segurança no Amazon Chime

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O [modelo de responsabilidade compartilhada](#) descreve isso como segurança da nuvem e segurança na nuvem:

- **Segurança da nuvem** — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de [AWS](#) de . Para saber mais sobre os programas de conformidade que se aplicam ao Amazon Chime, consulte [Serviços da AWS em escopo por programa de conformidade](#).
- **Segurança na nuvem** — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar o Amazon Chime. Os tópicos a seguir mostram como configurar o Amazon Chime para atender aos seus objetivos de segurança e compatibilidade. Você também aprende a usar outros AWS serviços da AWS que ajudam você a monitorar e proteger seus recursos do Amazon Chime.

## Tópicos

- [Identity and Access Management para o Amazon Chime](#)
- [Como o Amazon Chime funciona com o IAM](#)
- [Prevenção do problema do substituto confuso entre serviços](#)
- [Políticas baseadas em recursos do Amazon Chime](#)
- [Autorização baseada em tags do Amazon Chime](#)
- [Perfis do IAM no Amazon Chime](#)
- [Exemplos de políticas baseadas em identidade do Amazon Chime](#)
- [Solucionar problemas de identidade e acesso do Amazon Chime](#)

- [Usar perfis vinculados ao serviço para o Amazon Chime](#)
- [Registrar em log e monitorar no Amazon Chime](#)
- [Validação de conformidade para o Amazon Chime](#)
- [Resiliência no Amazon Chime](#)
- [Segurança de infraestrutura no Amazon Chime](#)
- [Noções básicas sobre as atualizações automáticas do Amazon Chime](#)

## Identity and Access Management para o Amazon Chime

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (ter permissões) para utilizar os recursos do Amazon Chime. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

### Tópicos

- [Público](#)
- [Autenticar com identidades](#)
- [Gerenciar o acesso usando políticas](#)

## Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no Amazon Chime.

Usuário do serviço: se você usar o serviço Amazon Chime para fazer seu trabalho, o administrador fornecerá as credenciais e as permissões necessárias. À medida que mais recursos do Amazon Chime forem usados para realizar o trabalho, talvez sejam necessárias permissões adicionais. Compreenda como o acesso é gerenciado pode ajudar a solicitar as permissões corretas ao administrador. Se você não puder acessar um recurso no Amazon Chime, consulte [Solucionar problemas de identidade e acesso do Amazon Chime](#).

Administrador do serviço: se você for o responsável pelos recursos do Amazon Chime em sua empresa, você provavelmente terá acesso total ao Amazon Chime. Cabe a você determinar quais funcionalidades e recursos do Amazon Chime os usuários do serviço deverão acessar. Envie as

solicitações ao administrador do IAM para alterar as permissões dos usuários de serviço. Revise as informações nesta página para compreender os conceitos básicos do IAM. Para saber mais sobre como a empresa pode usar o IAM com o Amazon Chime, consulte [Como o Amazon Chime funciona com o IAM](#).

Administrador do IAM: se você é um administrador do IAM, talvez queira saber detalhes sobre como pode escrever políticas para gerenciar o acesso ao Amazon Chime. Para visualizar exemplos de políticas baseadas em identidade do Amazon Chime que podem ser usadas no IAM, consulte [Exemplos de políticas baseadas em identidade do Amazon Chime](#).

## Autenticar com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte [Como fazer login Conta da AWS](#) no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para designar solicitações por conta própria, consulte [Versão 4 do AWS Signature para solicitações de API](#) no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser necessário fornecer informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte [Autenticação multifator](#) no Guia do usuário do AWS IAM Identity Center e [Usar a autenticação multifator da AWS no IAM](#) no Guia do usuário do IAM.

## AWS usuário raiz da conta

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário-raiz para tarefas diárias. Proteja as credenciais do usuário-raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário-raiz, consulte [Tarefas que exigem credenciais de usuário-raiz](#) no Guia do Usuário do IAM.

## Usuários e grupos do IAM

Um [usuário do IAM](#) é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, é recomendável contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, é recomendável alternar as chaves de acesso. Para obter mais informações, consulte [Alternar as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo](#) no Guia do Usuário do IAM.

Um [grupo do IAM](#) é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte [Casos de uso para usuários do IAM](#) no Guia do usuário do IAM.

## Perfis do IAM

Uma [função do IAM](#) é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Para assumir temporariamente uma função do IAM no AWS Management Console, você pode [alternar de um usuário para uma função do IAM \(console\)](#). Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para usar perfis, consulte [Métodos para assumir um perfil](#) no Guia do usuário do IAM.

Perfis do IAM com credenciais temporárias são úteis nas seguintes situações:

- **Acesso de usuário federado:** para atribuir permissões a identidades federadas, é possível criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas por ele. Para ter mais informações sobre perfis para federação, consulte [Criar um perfil para um provedor de identidade de terceiros \(federação\)](#) no Guia do usuário do IAM. Se usar o Centro de Identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de Identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte [Conjuntos de Permissões](#) no Guia do Usuário do AWS IAM Identity Center .
- **Permissões temporárias para usuários do IAM:** um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- **Acesso entre contas:** é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.
- **Acesso entre serviços** — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões da entidade principal da chamada, usando um perfil de serviço ou um perfil vinculado ao serviço.
  - **Sessões de acesso direto (FAS)** — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte [Sessões de acesso direto](#).
- **Perfil de serviço:** um perfil de serviço é um [perfil do IAM](#) que um serviço assume para executar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de

serviço do IAM. Para obter mais informações, consulte [Criar um perfil para delegar permissões a um AWS service \(Serviço da AWS\)](#) no Guia do Usuário do IAM.

- **Função vinculada ao serviço** — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS). O serviço pode presumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para perfis vinculados ao serviço.
- **Aplicativos em execução na Amazon EC2** — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo solicitações AWS CLI de AWS API. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que os programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte [Usar uma função do IAM para conceder permissões a aplicativos executados em EC2 instâncias da Amazon](#) no Guia do usuário do IAM.

## Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte [Visão geral das políticas JSON](#) no Guia do usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e perfis não têm permissões. Para conceder permissão aos usuários para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem assumir os perfis.

As políticas do IAM definem permissões para uma ação independentemente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a

ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

## Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte [Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente](#) no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte [Escolher entre políticas gerenciadas e políticas em linha](#) no Guia do usuário do IAM.

## Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o atributo ao qual a política está anexada, a política define quais ações uma entidade principal especificado pode executar nesse atributo e em que condições. Você deve [especificar uma entidade principal](#) em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

## AWS políticas gerenciadas para o Amazon Chime

Para adicionar permissões a usuários, grupos e perfis, é mais fácil usar políticas gerenciadas pela AWS do que gravar políticas por conta própria. É necessário tempo e experiência para [criar políticas gerenciadas pelo cliente do IAM](#) que fornecem à sua equipe apenas as permissões de que precisam. Para começar rapidamente, você pode usar nossas políticas AWS gerenciadas. Essas

políticas abrangem casos de uso comuns e estão disponíveis na sua conta da AWS . Para obter mais informações sobre políticas AWS gerenciadas, consulte [políticas AWS gerenciadas](#) no Guia do usuário do IAM.

AWS os serviços mantêm e atualizam as políticas AWS gerenciadas. Você não pode alterar as permissões nas políticas AWS gerenciadas. Ocasionalmente, os serviços adicionam permissões adicionais a uma política AWS gerenciada para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem uma política AWS gerenciada quando um novo recurso é lançado ou quando novas operações são disponibilizadas. Os serviços não removem as permissões de uma política AWS gerenciada, portanto, as atualizações de políticas não violarão suas permissões existentes.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, a política ReadOnlyAccess AWS gerenciada fornece acesso somente de leitura a todos os AWS serviços e recursos. Quando um serviço inicia um novo atributo, a AWS adiciona permissões somente leitura para novas operações e atributos. Para obter uma lista e descrições das políticas de perfis de trabalho, consulte [Políticas gerenciadas pela AWS para perfis de trabalho](#) no Guia do usuário do IAM.

## Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o AWS WAF Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber mais ACLs, consulte a [visão geral da lista de controle de acesso \(ACL\)](#) no Guia do desenvolvedor do Amazon Simple Storage Service.

## Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma

entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte [Limites de permissões para identidades do IAM](#) no Guia do usuário do IAM.

- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations e SCPs, consulte [Políticas de controle de serviços](#) no Guia AWS Organizations do Usuário.
- Políticas de controle de recursos (RCPs) — RCPs são políticas JSON que você pode usar para definir o máximo de permissões disponíveis para recursos em suas contas sem atualizar as políticas do IAM anexadas a cada recurso que você possui. O RCP limita as permissões para recursos nas contas dos membros e pode afetar as permissões efetivas para identidades, incluindo a Usuário raiz da conta da AWS, independentemente de pertencerem à sua organização. Para obter mais informações sobre Organizations e RCPs, incluindo uma lista Serviços da AWS desse suporte RCPs, consulte [Políticas de controle de recursos \(RCPs\)](#) no Guia AWS Organizations do usuário.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em recursos. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte [Políticas de sessão](#) no Guia do usuário do IAM.

## Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte [Lógica de avaliação de políticas](#) no Guia do usuário do IAM.

# Como o Amazon Chime funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Amazon Chime, você deve entender quais recursos do IAM estão disponíveis para uso com o Amazon Chime. Para ter uma visão de alto nível de como o Amazon Chime e AWS outros serviços funcionam com o IAM, [AWS consulte os serviços que funcionam com o IAM no Guia](#) do usuário do IAM.

## Tópicos

- [Políticas baseadas em identidade do Amazon Chime](#)
- [Recursos](#)
- [Exemplos](#)

## Políticas baseadas em identidade do Amazon Chime

Com as políticas baseadas em identidade do IAM, é possível especificar ações e recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. O Amazon Chime oferece suporte a ações, chaves de condição e recursos específicos. Para saber mais sobre todos os elementos usados em uma política JSON, consulte [Referência de elementos de política JSON do IAM](#) no Guia do usuário do IAM.

## Ações

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

O elemento `Action` de uma política JSON descreve as ações que podem ser usadas para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

## Chaves de condição

O Amazon Chime não oferece chaves de condição específicas ao serviço. Para ver todas as chaves de condição globais da AWS, consulte [Chaves de contexto de condição globais da AWS](#) no Guia do usuário do IAM.

## Recursos

O Amazon Chime não suporta a especificação de recursos ARNs em uma política.

## Exemplos

Para visualizar exemplos de políticas baseadas em identidade do Amazon Chime, consulte [Exemplos de políticas baseadas em identidade do Amazon Chime](#).

## Prevenção do problema do substituto confuso entre serviços

O problema do substituto confuso é um problema de segurança em que uma entidade que não tem permissão para executar uma ação chama uma entidade mais privilegiada a executar a ação. Isso pode permitir que agentes mal-intencionados executem comandos ou modifiquem recursos que, de outra forma, não teriam permissão para executar ou acessar. Para obter mais informações, consulte [O problema de “confused deputy”](#) no Guia do usuário do AWS Identity and Access Management .

Em AWS, a falsificação de identidade entre serviços pode levar a um cenário confuso de delegado. A personificação entre serviços ocorre quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). Um agente mal-intencionado pode usar o serviço de chamada para alterar recursos em outro serviço utilizando permissões que normalmente não teria.

AWS fornece aos diretores de serviços acesso gerenciado aos recursos em sua conta para ajudá-lo a proteger a segurança de seus recursos. Recomendamos usar a chave de contexto de condição global `aws:SourceAccount` em suas políticas de recursos. Essas chaves limitam as permissões que o Amazon Chime concede a outro serviço para este atributo.

O exemplo a seguir mostra uma política de bucket do S3 que usa a chave de contexto de condição global `aws:SourceAccount` no bucket do S3 `CallDetailRecords` configurado para evitar o problema de substituto confuso.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonChimeAclCheck668426",
      "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 baseadas em recursos do Amazon Chime

O Amazon Chime não oferece suporte a políticas baseadas em recursos.

## Autorização baseada em tags do Amazon Chime

O Amazon Chime não é compatível com recursos de marcação ou de controle de acesso com base em tags.

## Perfis do IAM no Amazon Chime

Uma [função do IAM](#) é uma entidade dentro da sua AWS conta que tem permissões específicas.

## Usar credenciais temporárias com o Amazon Chime

É possível usar credenciais temporárias para fazer login com federação, assumir um perfil do IAM ou assumir um perfil entre contas. Você obtém credenciais de segurança temporárias chamando operações de AWS STS API, como [AssumeRole](#) ou [GetFederationToken](#).

A Amazon Chime é compatível com o uso de credenciais temporárias.

## Perfis vinculados ao serviço

[As funções vinculadas ao serviço](#) permitem que AWS os serviços acessem recursos em outros serviços que realizam ações em seu nome. As funções vinculadas ao serviço aparecem em sua conta do IAM e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados a serviço.

O Amazon Chime oferece suporte a funções vinculadas ao serviço. Para obter detalhes sobre como criar ou gerenciar funções vinculadas ao serviço do Amazon Chime, consulte [Usar perfis vinculados ao serviço para o Amazon Chime](#).

## Perfis de serviço

Esse atributo permite que um serviço assumira um [perfil de serviço](#) em seu nome. O perfil permite que o serviço acesse recursos em outros serviços para concluir uma ação em seu nome. Os perfis de serviço aparecem em sua conta do IAM e são de propriedade da conta. Isso significa que um administrador do IAM pode alterar as permissões para esse perfil. Porém, fazer isso pode alterar a funcionalidade do serviço.

O Amazon Chime não é compatível com funções de serviço.

## Exemplos de políticas baseadas em identidade do Amazon Chime

Por padrão, os usuários e os perfis do IAM não têm permissão para criar ou modificar recursos do Amazon Chime. Eles também não podem realizar tarefas usando a AWS API AWS Management Console AWS CLI, ou. Um administrador do IAM deve criar políticas do IAM que concedam aos usuários e perfis permissão para executarem operações de API específicas nos recursos especificados de que precisam. O administrador deve anexar essas políticas aos usuários ou grupos do IAM que exigem essas permissões.

Para saber como criar uma política baseada em identidade do IAM utilizando esses exemplos de documentos de política JSON, consulte [Criar políticas na guia JSON](#) no Guia do usuário do IAM.

### Tópicos

- [Práticas recomendadas de política](#)
- [Usar o console do Amazon Chime](#)

- [Permita que os usuários tenham acesso total ao Amazon Chime](#)
- [Permitir que os usuários visualizem suas próprias permissões](#)
- [Permitir que os usuários tenham acesso a ações de gerenciamento de usuário](#)
- [AWS política gerenciada: AmazonChimeVoiceConnectorServiceLinkedRolePolicy](#)
- [Atualizações do Amazon Chime para AWS políticas gerenciadas](#)

## Práticas recomendadas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Amazon Chime em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e avance para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte [Políticas gerenciadas pela AWS](#) ou [Políticas gerenciadas pela AWS para funções de trabalho](#) no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte [Políticas e permissões no IAM](#) no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte [Elementos da política JSON do IAM: condição](#) no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de cem verificações de política e recomendações práticas para ajudar a

criar políticas seguras e funcionais. Para obter mais informações, consulte [Validação de políticas do IAM Access Analyzer](#) no Guia do Usuário do IAM.

- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte [Configuração de acesso à API protegido por MFA](#) no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte [Práticas recomendadas de segurança no IAM](#) no Guia do usuário do IAM.

## Usar o console do Amazon Chime

Para acessar o console do Amazon Chime, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do Amazon Chime em sua AWS conta. Se você criar uma política baseada em identidade que seja mais restritiva que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis do IAM) com essa política.

Para garantir que essas entidades ainda possam usar o console do Amazon Chime, anexe também a seguinte AmazonChimeReadOnlypolítica AWS gerenciada às entidades. Para obter mais informações, consulte [Adição de permissões a um usuário](#) no Guia do usuário do IAM.

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

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente às ações que corresponderem a operação da API que você estiver tentando executar.

## Permita que os usuários tenham acesso total ao Amazon Chime

A AmazonChimeFullAccess política AWS gerenciada a seguir concede a um usuário do IAM acesso total aos recursos do Amazon Chime. A política concede ao usuário acesso a todas as operações do Amazon Chime e a outras operações de que o Amazon Chime precisa para conseguir executar em seu nome.

```
{
  "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*"
    ]
}
]
}

```

## Permitir que os usuários visualizem suas próprias permissões

Este exemplo mostra como criar uma política que permita que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política inclui permissões para concluir essa ação no console ou programaticamente usando a API AWS CLI ou 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 os usuários tenham acesso a ações de gerenciamento de usuário

Use a `AmazonChimeUserManagement` política AWS gerenciada para conceder aos usuários acesso às ações de gerenciamento de usuários no console do 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": "*"
}
]
```

## AWS política gerenciada:

### AmazonChimeVoiceConnectorServiceLinkedRolePolicy

A `AmazonChimeVoiceConnectorServiceLinkedRolePolicy` permite que os Amazon Chime Voice Connectors transmitam mídia para o Amazon Kinesis Video Streams, forneçam notificações de streaming e sintetizem a fala usando o Amazon Polly. Essa política concede ao serviço Amazon Chime Voice Connector permissões para acessar o Amazon Kinesis Video Streams do cliente, enviar eventos de notificação ao Amazon Simple Notification Service e o Amazon Simple Queue Service e usar o Amazon Polly para sintetizar a fala ao usar as ações `Speak` e `SpeakAndGetDigits` de aplicações de voz do SDK do Amazon Chime. Para obter mais informações, consulte [Exemplos de políticas baseadas em identidade do Amazon Chime](#) no Guia de administração do SDK do Amazon Chime.

## Atualizações do Amazon Chime para AWS políticas gerenciadas

A tabela a seguir lista e descreve as atualizações feitas na política do IAM do Amazon Chime.

Alteração	Descrição	Data
AmazonChimeVoiceConnectorServiceLinkedRolePolicy : atualizar para uma política existente	Os Amazon Chime Voice Connectors adicionaram novas permissões para permitir que você use o Amazon Polly para sintetizar a fala. Essas permissões são necessárias para usar as ações <code>Speak</code> e <code>SpeakAndGetDigits</code> nas aplicações de voz do SDK do Amazon Chime.	15 de março de 2022
AmazonChimeVoiceConnectorServiceLinkedRolePolicy : atualizar para uma política existente	O Amazon Chime Voice Connector adicionou novas permissões para permitir o acesso ao Amazon Kinesis Video Streams e enviar eventos de notificação para	20 de dezembro de 2021

Alteração	Descrição	Data
	o SNS e o SQS. Essas permissões são necessárias para que os Amazon Chime Voice Connectors transmitam mídia para o Amazon Kinesis Video Streams e forneçam notificações de streaming.	
Mudança na política existente . <a href="#">Criar usuários ou perfis do IAM com a política do SDK do Chime.</a>	O Amazon Chime adicionou novas ações para oferecer suporte à validação expandida .  Várias ações foram adicionadas para permitir a listagem e marcação de participantes e recursos da reunião e para iniciar e interromper a transcrição da reunião.	23 de setembro de 2021
O Amazon Chime passou a monitorar alterações	O Amazon Chime começou a monitorar as mudanças em suas políticas AWS gerenciadas.	23 de setembro de 2021

## Solucionar problemas de identidade e acesso do Amazon Chime

Use as informações a seguir para ajudar a diagnosticar e corrigir problemas comuns que você possa encontrar ao trabalhar com o Amazon Chime e o IAM.

### Tópicos

- [Não tenho autorização para executar uma ação no Amazon Chime](#)
- [Não estou autorizado a realizar iam: PassRole](#)
- [Quero permitir que pessoas fora da minha AWS conta acessem meus recursos do Amazon Chime](#)

## Não tenho autorização para executar uma ação no Amazon Chime

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo `my-example-widget` fictício, mas não tem as permissões `chime:GetWidget` fictícias.

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

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso `my-example-widget` usando a ação `chime:GetWidget`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

## Não estou autorizado a realizar iam: PassRole

Se receber uma mensagem de erro informando que você não tem autorização para executar a ação `iam:PassRole`, suas políticas devem ser atualizadas para permitir a transmissão de um perfil ao Amazon Chime.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O erro exemplificado a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta usar o console para executar uma ação no Amazon Chime. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

## Quero permitir que pessoas fora da minha AWS conta acessem meus recursos do Amazon Chime

É possível criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. É possível especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Amazon Chime é compatível com esses recursos, consulte [Como o Amazon Chime funciona com o IAM](#).
- Para saber como fornecer acesso aos seus recursos em todas as Contas da AWS que você possui, consulte Como [fornecer acesso a um usuário do IAM em outra Conta da AWS que você possui](#) no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como [fornecer acesso Contas da AWS a terceiros](#) no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte [Conceder acesso a usuários autenticados externamente \(federação de identidades\)](#) no Guia do usuário do IAM.
- Para conhecer a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.

## Usar perfis vinculados ao serviço para o Amazon Chime

O Amazon Chime usa funções vinculadas a [serviços AWS Identity and Access Management \(IAM\)](#). Perfil vinculado ao serviço é um tipo exclusivo de perfil do IAM vinculado diretamente ao Amazon Chime. As funções vinculadas ao serviço são predefinidas pelo Amazon Chime e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

O perfil vinculado ao serviço facilita a configuração do Amazon Chime, já que não é preciso adicionar as permissões necessárias manualmente. O Amazon Chime define as permissões das funções vinculadas ao serviço e, exceto se definido de outra forma, somente o Amazon Chime pode assumir

suas funções. As permissões definidas incluem a política de confiança e a política de permissões. A política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

Uma função vinculada ao serviço poderá ser excluída somente após excluir seus recursos relacionados. Isso protege seus recursos do Amazon Chime, pois você não pode remover por engano as permissões para acessar os recursos.

Para obter informações sobre outros produtos que oferecem suporte a funções vinculadas aos serviços, consulte [Produtos da AWS que funcionam com o IAM](#). Procure os serviços que têm Sim na coluna Função vinculada ao serviço. Escolha um Sim com um link para visualizar a documentação do perfil vinculado para esse serviço.

### Tópicos

- [Usar funções com dispositivos compartilhados do Alexa for Business](#)
- [Usar perfis com transcrição ao vivo](#)
- [Usar perfis com pipelines de mídia do SDK do Amazon Chime](#)

## Usar funções com dispositivos compartilhados do Alexa for Business

As informações nas seções a seguir explicam como usar funções vinculadas a serviços e conceder ao Amazon Chime acesso aos recursos do Alexa for Business em sua conta. AWS

### Tópicos

- [Permissões de perfil vinculado ao serviço para o Amazon Chime](#)
- [Criar um perfil vinculado ao serviço para o Amazon Chime](#)
- [Editar um perfil vinculado ao serviço do Amazon Chime](#)
- [Excluir um perfil vinculado ao serviço do Amazon Chime](#)
- [Regiões com suporte a perfis vinculados ao serviço do Amazon Chime](#)

## Permissões de perfil vinculado ao serviço para o Amazon Chime

O Amazon Chime usa a função vinculada ao serviço chamada `AWSServiceRoleForAmazonChime`—Permite acesso a AWS serviços e recursos usados ou gerenciados pelo Amazon Chime, como dispositivos compartilhados do Alexa for Business.

A função `AWSServiceRoleForAmazonChime` vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `chime.amazonaws.com`

A política de permissões da função permite que o Amazon Chime conclua as seguintes ações no recurso especificado:

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

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para obter mais informações, consulte [Permissões de perfil vinculado ao serviço](#) no Guia do usuário do IAM.

## Criar um perfil vinculado ao serviço para o Amazon Chime

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você ativa o Alexa for Business para um dispositivo compartilhado no Amazon Chime na, na AWS ou AWS Management Console na API AWS CLI, o Amazon Chime cria a função vinculada ao serviço para você.

Você também pode usar o console do IAM para criar um perfil vinculado ao serviço com o caso de uso do Amazon Chime. Na AWS CLI ou na AWS API, crie uma função vinculada ao serviço com o nome do `chime.amazonaws.com` serviço. Para obter mais informações, consulte [Criar uma função vinculada ao serviço](#) no Manual do usuário do IAM. Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

## Editar um perfil vinculado ao serviço do Amazon Chime

O Amazon Chime não permite que você edite a função vinculada ao `AWSServiceRoleForAmazonChime` serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte [Editar um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

## Excluir um perfil vinculado ao serviço do Amazon Chime

Se você não precisar mais usar um recurso ou um serviço que requer uma função vinculada ao serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida. No entanto, você deve limpar seu perfil vinculado ao serviço para excluí-la manualmente.

## Limpar um perfil vinculado ao serviço

Antes de usar o IAM para excluir um perfil vinculado ao serviço, você deverá excluir qualquer recurso usado pelo perfil.

### Note

Se o Amazon Chime estiver usando a função quando você tenta excluir os recursos, a exclusão poderá falhar. Se isso acontecer, espere alguns minutos e tente a operação novamente.

Para excluir recursos do Amazon Chime usados pelo AWSService RoleForAmazonChime (console)

- Desative o Alexa for Business para todos os dispositivos compartilhados em sua conta do Amazon Chime.
  - a. [Abra o console do Amazon Chime em https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
  - b. Selecione Users (Usuários), Shared devices (Dispositivos compartilhados).
  - c. Selecione um dispositivo.
  - d. Escolha Ações.
  - e. Escolha Desativar o Alexa for Business.

## Excluir manualmente o perfil vinculado ao serviço

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função AWSService RoleForAmazonChime vinculada ao serviço. Para obter mais informações, consulte [Excluir um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

## Regiões com suporte a perfis vinculados ao serviço do Amazon Chime

O Amazon Chime é compatível com perfis vinculados ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte [Endpoints e cotas do Amazon Chime](#).

## Usar perfis com transcrição ao vivo

As informações nas seções a seguir explicam como criar e gerenciar um perfil vinculado ao serviço para transcrição ao vivo do Amazon Chime. Para obter mais informações sobre o serviço de transcrição ao vivo, consulte [Using Amazon Chime SDK live transcription](#).

## Tópicos

- [Permissões de perfil vinculado ao serviço para transcrição ao vivo do Amazon Chime](#)
- [Criar um perfil vinculado ao serviço para transcrição ao vivo do Amazon Chime](#)
- [Editar um perfil vinculado ao serviço para transcrição ao vivo do Amazon Chime](#)
- [Excluir um perfil vinculado ao serviço da transcrição ao vivo do Amazon Chime](#)
- [Regiões com suporte a perfis vinculados ao serviço do Amazon Chime](#)

## Permissões de perfil vinculado ao serviço para transcrição ao vivo do Amazon Chime

O Amazon Chime Live Transcription usa uma função vinculada ao serviço chamada — Permite que o `AWSServiceRoleForAmazonChimeTranscription` acesse o Amazon Transcribe e o Amazon Transcribe Medical em seu nome.

A função `AWSServiceRoleForAmazonChimeTranscription` vinculada ao serviço confia nos seguintes serviços para assumir a função:

- `transcription.chime.amazonaws.com`

A política de permissões da função permite que o Amazon Chime conclua as seguintes ações nos recursos especificados:

- Ação: `transcribe:StartStreamTranscription` em `all AWS resources`
- Ação: `transcribe:StartMedicalStreamTranscription` em `all AWS resources`

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para mais informações, consulte [Permissões de perfil vinculado ao serviço](#) no Guia do usuário do IAM.

## Criar um perfil vinculado ao serviço para transcrição ao vivo do Amazon Chime

Você pode usar o console do IAM para criar um perfil vinculado ao serviço com o caso de uso Transcrição do Chime.

**Note**

Você deve ter permissões administrativas do IAM para concluir essas etapas. Caso contrário, entre em contato com um administrador do sistema.

Para criar a função

1. Faça login no AWS Management Console e abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação do console do IAM, escolha Perfil e Criar perfil.
3. Escolha o tipo de perfil do Serviço da AWS, selecione Chime e escolha Transcrição do Chime.
4. Escolha Próximo.
5. Escolha Próximo.
6. Edite a descrição conforme necessário e escolha Criar perfil.

Você também pode usar a API AWS CLI ou a AWS API para criar uma função vinculada ao serviço chamada `transcription.chime.amazonaws.com`.

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

Para obter mais informações, consulte [Criar uma função vinculada ao serviço](#) no Guia do usuário do IAM. Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

## Editar um perfil vinculado ao serviço para transcrição ao vivo do Amazon Chime

O Amazon Chime não permite que você edite a função vinculada ao `AWSServiceRoleForAmazonChimeTranscription` serviço. Depois de criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, é possível usar o IAM para editar a descrição do perfil. Para mais informações, consulte [Como editar uma função vinculada ao serviço](#) no Guia do usuário do IAM.

## Excluir um perfil vinculado ao serviço da transcrição ao vivo do Amazon Chime

Se você não precisar mais usar um atributo ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função AWSService RoleForAmazonChimeTranscription vinculada ao serviço. Para obter mais informações, consulte [Excluir um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

## Regiões com suporte a perfis vinculados ao serviço do Amazon Chime

O Amazon Chime é compatível com perfis vinculados ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte [Amazon Chime endpoints and quotas](#) e [Using Amazon Chime SDK media Regions](#).

## Usar perfis com pipelines de mídia do SDK do Amazon Chime

As informações nas seções a seguir explicam como criar e gerenciar um perfil vinculado ao serviço para pipelines de mídia do SDK do Amazon Chime.

### Tópicos

- [Permissões de perfil vinculado ao serviço para pipelines de mídia do SDK do Amazon Chime](#)
- [Criar um perfil vinculado ao serviço para pipelines de mídia do SDK do Amazon Chime](#)
- [Editar um perfil vinculado ao serviço para os pipelines de mídia do SDK do Amazon Chime](#)
- [Excluir um perfil vinculado ao serviço para os pipelines de mídia do SDK do Amazon Chime](#)
- [Regiões compatíveis com perfis vinculados ao serviço do SDK do Amazon Chime](#)

## Permissões de perfil vinculado ao serviço para pipelines de mídia do SDK do Amazon Chime

O Amazon Chime usa a função vinculada ao serviço chamada AWSServiceRoleForAmazonChimeSDKMediaPipelines — Permite que os pipelines de mídia do Amazon Chime SDK acessem reuniões do Amazon Chime SDK em seu nome.

A função vinculada ao serviço do AWSService RoleForAmazonChime SDKMedia Pipelines confia nos seguintes serviços para assumir a função:

- `mediapipelines.chime.amazonaws.com`

O perfil permite que o Amazon Chime conclua as seguintes ações nos recursos especificados:

- Ação: `chime:CreateAttendee` em `all AWS resources`
- Ação: `chime>DeleteAttendee` em `all AWS resources`
- Ação: `chime:GetMeeting` em `all AWS resources`

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua um perfil vinculado a serviço. Para mais informações, consulte [Permissões de perfil vinculado ao serviço](#) no Guia do usuário do IAM.

## Criar um perfil vinculado ao serviço para pipelines de mídia do SDK do Amazon Chime

Você pode usar o console do IAM para criar um perfil vinculado ao serviço com o caso de uso do Pipelines de mídia do SDK do Amazon Chime\*.

### Note

Você deve ter permissões administrativas do IAM para concluir essas etapas. Caso contrário, entre em contato com um administrador do sistema.

Para criar a função

1. Faça login no AWS Management Console e abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação do console do IAM, escolha Perfil e Criar perfil.
3. Escolha o tipo de perfil de Serviço da AWS , selecione Chime e escolha Pipelines de mídia do SDK do Chime.
4. Escolha Próximo.
5. Escolha Próximo.
6. Edite a descrição conforme necessário e escolha Criar perfil.

Você também pode usar a API AWS CLI ou a AWS API para criar uma função vinculada ao serviço chamada `mediapipelines.chime.amazonaws.com`.

No AWS CLI, execute este comando:`aws iam create-service-linked-role --aws-service-name mediapipelines.chime.amazonaws.com`.

Para obter mais informações, consulte [Criar uma função vinculada ao serviço](#) no Guia do usuário do IAM. Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

## Editar um perfil vinculado ao serviço para os pipelines de mídia do SDK do Amazon Chime

O Amazon Chime não permite que você edite a função vinculada ao serviço `AWSServiceRoleForAmazonChimeSDKMediaPipelines`. Depois de criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte [Editar uma função vinculada a serviço](#) no Guia do usuário do IAM.

## Excluir um perfil vinculado ao serviço para os pipelines de mídia do SDK do Amazon Chime

Se você não precisar mais usar um atributo ou serviço que requer uma função vinculada a serviço, é recomendável excluí-la. Dessa forma, você não tem uma entidade não utilizada que não seja monitorada ativamente ou mantida.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função vinculada ao serviço do `AWSServiceRoleForAmazonChimeSDKMediaPipelines`. Para obter mais informações, consulte [Excluir um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

## Regiões compatíveis com perfis vinculados ao serviço do SDK do Amazon Chime

O Amazon Chime SDK oferece suporte ao uso de funções vinculadas a serviços em todas as AWS regiões em que o serviço está disponível. Para obter mais informações, consulte [Endpoints e cotas do Amazon Chime](#).

## Registrar em log e monitorar no Amazon Chime

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do Amazon Chime e de suas outras AWS soluções. AWS fornece as seguintes

ferramentas para monitorar o Amazon Chime, relatar problemas e realizar ações automáticas quando apropriado:

- A Amazon CloudWatch monitora em tempo real seus AWS recursos e os aplicativos nos quais você executa AWS. Você pode coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Por exemplo, você pode CloudWatch rastrear o uso da CPU ou outras métricas de suas EC2 instâncias da Amazon e iniciar automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o [Guia CloudWatch do usuário da Amazon](#).
- A Amazon EventBridge fornece um fluxo quase em tempo real de eventos do sistema que descrevem mudanças nos AWS recursos. EventBridge permite a computação automatizada orientada por eventos. Isso permite que você escreva regras que observem determinados eventos e acionem ações automatizadas em outros AWS serviços quando esses eventos acontecem. Para obter mais informações, consulte o [Guia EventBridge do usuário da Amazon](#).
- O Amazon CloudWatch Logs permite monitorar, armazenar e acessar seus arquivos de log de EC2 instâncias da Amazon e de outras fontes. CloudTrail CloudWatch Os registros podem monitorar as informações nos arquivos de log e notificá-lo quando determinados limites forem atingidos. É possível também arquivar seus dados de log em armazenamento resiliente. Para obter mais informações, consulte o [Guia do usuário do Amazon CloudWatch Logs](#).
- AWS CloudTrail captura chamadas de API e eventos relacionados feitos por ou em nome de sua AWS conta. Desse modo, ele fornece os arquivos de log para um bucket do Amazon S3 especificado por você. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte o [Guia do usuário do AWS CloudTrail](#).

## Tópicos

- [Monitorando o Amazon Chime com a Amazon CloudWatch](#)
- [Automatizando o Amazon Chime com EventBridge](#)
- [Registrar chamadas de API do Amazon Chime com o AWS CloudTrail](#)

## Monitorando o Amazon Chime com a Amazon CloudWatch

Você pode monitorar o Amazon Chime usando CloudWatch, que coleta dados brutos e os processa em métricas legíveis, quase em tempo real. Essas estatísticas são mantidas por 15 meses, de maneira que você possa acessar informações históricas e ter uma perspectiva melhor de como

o aplicativo web ou o serviço está se saindo. Você também pode definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte o [Guia CloudWatch do usuário da Amazon](#).

## CloudWatch métricas para Amazon Chime

O Amazon Chime envia as seguintes métricas para CloudWatch

O AWS/ChimeVoiceConnector namespace inclui as seguintes métricas para números de telefone atribuídos à sua AWS conta e aos Amazon Chime Voice Connectors.

Métrica	Descrição
InboundCallAttempts	O número de chamadas de entrada tentadas.  Unidades: contagem
InboundCallFailures	O número de falhas de chamadas de entrada.  Unidades: contagem
InboundCallsAnswered	O número de chamadas de entrada que são atendidas.  Unidades: contagem
InboundCallsActive	O número de chamadas de entrada que estão ativas no momento.  Unidades: contagem
OutboundCallAttempts	O número de chamadas de saída tentadas.  Unidades: contagem
OutboundCallFailures	O número de falhas de chamadas de saída.  Unidades: contagem
OutboundCallsAnswered	O número de chamadas de saída que são atendidas.

Métrica	Descrição
	Unidades: contagem
OutboundCallsActive	O número de chamadas de saída que estão ativas no momento. Unidades: contagem
Throttles	O número de vezes que a conta é limitada ao tentar fazer uma chamada. Unidades: contagem
Sip1xxCodes	O número de mensagens SIP com códigos de status de nível 1xx. Unidades: contagem
Sip2xxCodes	O número de mensagens SIP com códigos de status de nível 2xx. Unidades: contagem
Sip3xxCodes	O número de mensagens SIP com códigos de status de nível 3xx. Unidades: contagem
Sip4xxCodes	O número de mensagens SIP com códigos de status de nível 4xx. Unidades: contagem
Sip5xxCodes	O número de mensagens SIP com códigos de status de nível 5xx. Unidades: contagem

Métrica	Descrição
Sip6xxCodes	<p>O número de mensagens SIP com códigos de status de nível 6xx.</p> <p>Unidades: contagem</p>
CustomerToVcRtpPackets	<p>O número de pacotes RTP enviados do cliente para a infraestrutura do Amazon Chime Voice Connector.</p> <p>Unidades: contagem</p>
CustomerToVcRtpBytes	<p>O número de bytes enviados do cliente para a infraestrutura do Amazon Chime Voice Connector em pacotes RTP.</p> <p>Unidades: contagem</p>
CustomerToVcRtcpPackets	<p>O número de pacotes RTCP enviados do cliente para a infraestrutura do Amazon Chime Voice Connector.</p> <p>Unidades: contagem</p>
CustomerToVcRtcpBytes	<p>O número de bytes enviados do cliente para a infraestrutura do Amazon Chime Voice Connector em pacotes RTCP.</p> <p>Unidades: contagem</p>
CustomerToVcPacketsLost	<p>O número de pacotes perdidos em trânsito do cliente para a infraestrutura do Amazon Chime Voice Connector.</p> <p>Unidades: contagem</p>

Métrica	Descrição
<code>CustomerToVcJitter</code>	<p>A oscilação média para pacotes enviados do cliente para a infraestrutura do Amazon Chime Voice Connector.</p> <p>Unidade: microssegundos</p>
<code>VcToCustomerRtpPackets</code>	<p>O número de pacotes RTP enviados da infraestrutura do Amazon Chime Voice Connector para o cliente.</p> <p>Unidades: contagem</p>
<code>VcToCustomerRtpBytes</code>	<p>O número de bytes enviados da infraestrutura do Amazon Chime Voice Connector para o cliente em pacotes RTP.</p> <p>Unidades: contagem</p>
<code>VcToCustomerRtcpPackets</code>	<p>O número de pacotes RTCP enviados da infraestrutura do Amazon Chime Voice Connector para o cliente.</p> <p>Unidades: contagem</p>
<code>VcToCustomerRtcpBytes</code>	<p>O número de bytes enviados da infraestrutura do Amazon Chime Voice Connector para o cliente em pacotes RTCP.</p> <p>Unidades: contagem</p>
<code>VcToCustomerPacketsLost</code>	<p>O número de pacotes perdidos em trânsito da infraestrutura do Amazon Chime Voice Connector para o cliente.</p> <p>Unidades: contagem</p>

Métrica	Descrição
VcToCustomerJitter	<p>A oscilação média para pacotes enviados da infraestrutura do Amazon Chime Voice Connector para o cliente.</p> <p>Unidade: microssegundos</p>
RTTBetweenVcAndCustomer	<p>O tempo médio de ida e volta entre o cliente e a infraestrutura do Amazon Chime Voice Connector.</p> <p>Unidade: microssegundos</p>
MOSBetweenVcAndCustomer	<p>A pontuação média de opinião (MOS) estimada associada a fluxos de voz entre o cliente e a infraestrutura do Amazon Chime Voice Connector.</p> <p>Unidades: pontuação entre 1,0 e 4,4. Uma pontuação maior indica melhor qualidade de áudio percebida.</p>
RemoteToVcRtpPackets	<p>O número de pacotes RTP enviados da infraestrutura do Amazon Chime Voice Connector para a extremidade remota.</p> <p>Unidades: contagem</p>
RemoteToVcRtpBytes	<p>O número de bytes enviados da extremidade remota para a infraestrutura do Amazon Chime Voice Connector em pacotes RTP.</p> <p>Unidades: contagem</p>
RemoteToVcRtcpPackets	<p>O número de pacotes RTCP enviados da extremidade remota para a infraestrutura do Amazon Chime Voice Connector.</p> <p>Unidades: contagem</p>

Métrica	Descrição
RemoteToVcRtcpBytes	<p>O número de bytes enviados da extremidade remota para a infraestrutura do Amazon Chime Voice Connector em pacotes RTCP.</p> <p>Unidades: contagem</p>
RemoteToVcPacketsLost	<p>O número de pacotes perdidos em trânsito da infraestrutura do Amazon Chime Voice Connector para a extremidade remota.</p> <p>Unidades: contagem</p>
RemoteToVcJitter	<p>A oscilação média para pacotes enviados da infraestrutura do Amazon Chime Voice Connector para a extremidade remota.</p> <p>Unidade: microssegundos</p>
VcToRemoteRtpPackets	<p>O número de pacotes RTP enviados da infraestrutura do Amazon Chime Voice Connector para a extremidade remota.</p> <p>Unidades: contagem</p>
VcToRemoteRtpBytes	<p>O número de bytes enviados da infraestrutura do Amazon Chime Voice Connector para a extremidade remota em pacotes RTP.</p> <p>Unidades: contagem</p>
VcToRemoteRtcpPackets	<p>O número de pacotes RTCP enviados da extremidade remota para a infraestrutura do Amazon Chime Voice Connector.</p> <p>Unidades: contagem</p>

Métrica	Descrição
VcToRemoteRtcpBytes	<p>O número de bytes enviados da infraestrutura do Amazon Chime Voice Connector para a extremidade remota em pacotes RTCP.</p> <p>Unidades: contagem</p>
VcToRemotePacketsLost	<p>O número de pacotes perdidos em trânsito da infraestrutura do Amazon Chime Voice Connector para a extremidade remota.</p> <p>Unidades: contagem</p>
VcToRemoteJitter	<p>A oscilação média para pacotes enviados da infraestrutura do Amazon Chime Voice Connector para a extremidade remota.</p> <p>Unidade: microssegundos</p>
RTTBetweenVcAndRemote	<p>O tempo médio de ida e volta entre a extremidade remota e a infraestrutura do Amazon Chime Voice Connector.</p> <p>Unidade: microssegundos</p>
MOSBetweenVcAndRemote	<p>A pontuação média de opinião (MOS) estimada associada a fluxos de voz entre a extremidade remota e a infraestrutura do Amazon Chime Voice Connector.</p> <p>Unidades: pontuação entre 1,0 e 4,4. Uma pontuação maior indica melhor qualidade de áudio percebida.</p>

## CloudWatch dimensões para Amazon Chime

As CloudWatch dimensões que você pode usar com o Amazon Chime estão listadas a seguir.

Dimensão	Descrição
VoiceConnectorId	O identificador do Amazon Chime Voice Connector para o qual exibir métricas.
Region	A AWS região associada ao evento.

## CloudWatch registros para Amazon Chime

Você pode enviar métricas do Amazon Chime Voice Connector para CloudWatch Logs. Para obter mais informações, consulte [Editing Amazon Chime Voice Connector settings](#) no Guia de administração do SDK do Amazon Chime.

### Logs de métricas de qualidade de mídia

Você pode optar por receber logs de métricas de qualidade de mídia para o Amazon Chime Voice Connector. Ao fazer isso, o Amazon Chime envia métricas detalhadas por minuto para todas as suas chamadas do Amazon Chime Voice Connector para um grupo de registros de CloudWatch registros criado para você. O nome do grupo de logs é `/aws/ChimeVoiceConnectorLogs/${VoiceConnectorID}`. Os campos a seguir estão incluídos nos logs, no formato JSON.

Campo	Descrição
voice_connector_id	O ID do Amazon Chime Voice Connector responsável pela chamada.
event_timestamp	A hora em que as métricas são emitidas, em número de milissegundos desde o UNIX epoch (meia-noite em 1º de janeiro de 1970) em UTC.
call_id	Corresponde ao ID da transação.
from_sip_user	O usuário iniciador da chamada.
from_country	O país iniciador da chamada.
to_sip_user	O usuário receptor da chamada.
to_country	O país receptor da chamada.

Campo	Descrição
endpoint_id	Um identificador opaco indicando o outro endpoint da chamada. Use com o CloudWatch Logs Insights. Para obter mais informações, consulte <a href="#">Análise de dados de log com o CloudWatch Logs Insights</a> no Guia do usuário do Amazon CloudWatch Logs.
aws_region	A AWS região para a chamada.
cust2vc_rtp_packets	O número de pacotes RTP enviados do cliente para a infraestrutura do Amazon Chime Voice Connector.
cust2vc_rtp_bytes	O número de bytes enviados do cliente para a infraestrutura do Amazon Chime Voice Connector em pacotes RTP.
cust2vc_rtcp_packets	O número de pacotes RTCP enviados do cliente para a infraestrutura do Amazon Chime Voice Connector.
cust2vc_rtcp_bytes	O número de bytes enviados do cliente para a infraestrutura do Amazon Chime Voice Connector em pacotes RTCP.
cust2vc_packets_lost	O número de pacotes perdidos em trânsito do cliente para a infraestrutura do Amazon Chime Voice Connector.
cust2vc_jitter	A oscilação média para pacotes enviados do cliente para a infraestrutura do Amazon Chime Voice Connector.
vc2cust_rtp_packets	O número de pacotes RTP enviados da infraestrutura do Amazon Chime Voice Connector para o cliente.

Campo	Descrição
vc2cust_rtp_bytes	O número de bytes enviados da infraestrutura do Amazon Chime Voice Connector para o cliente em pacotes RTP.
vc2cust_rtcp_packets	O número de pacotes RTCP enviados da infraestrutura do Amazon Chime Voice Connector para o cliente.
vc2cust_rtcp_bytes	O número de bytes enviados da infraestrutura do Amazon Chime Voice Connector para o cliente em pacotes RTCP.
vc2cust_packets_lost	O número de pacotes perdidos em trânsito da infraestrutura do Amazon Chime Voice Connector para o cliente.
vc2cust_jitter	A oscilação média para pacotes enviados da infraestrutura do Amazon Chime Voice Connector para o cliente.
rtt_btwn_vc_and_cust	O tempo médio de ida e volta entre o cliente e a infraestrutura do Amazon Chime Voice Connector.
mos_btwn_vc_and_cust	A pontuação média de opinião (MOS) estimada associada a fluxos de voz entre o cliente e a infraestrutura do Amazon Chime Voice Connector.
rem2vc_rtp_packets	O número de pacotes RTP enviados da infraestrutura do Amazon Chime Voice Connector para a extremidade remota.
rem2vc_rtp_bytes	O número de bytes enviados da extremidade remota para a infraestrutura do Amazon Chime Voice Connector em pacotes RTP.

Campo	Descrição
rem2vc_rtcp_packets	O número de pacotes RTCP enviados da extremidade remota para a infraestrutura do Amazon Chime Voice Connector.
rem2vc_rtcp_bytes	O número de bytes enviados da extremidade remota para a infraestrutura do Amazon Chime Voice Connector em pacotes RTCP.
rem2vc_packets_lost	O número de pacotes perdidos em trânsito da infraestrutura do Amazon Chime Voice Connector para a extremidade remota.
rem2vc_jitter	A oscilação média para pacotes enviados da infraestrutura do Amazon Chime Voice Connector para a extremidade remota.
vc2rem_rtp_packets	O número de pacotes RTP enviados da infraestrutura do Amazon Chime Voice Connector para a extremidade remota.
vc2rem_rtp_bytes	O número de bytes enviados da infraestrutura do Amazon Chime Voice Connector para a extremidade remota em pacotes RTP.
vc2rem_rtcp_packets	O número de pacotes RTCP enviados da extremidade remota para a infraestrutura do Amazon Chime Voice Connector.
vc2rem_rtcp_bytes	O número de bytes enviados da infraestrutura do Amazon Chime Voice Connector para a extremidade remota em pacotes RTCP.
vc2rem_packets_lost	O número de pacotes perdidos em trânsito da infraestrutura do Amazon Chime Voice Connector para a extremidade remota.

Campo	Descrição
vc2rem_jitter	A oscilação média para pacotes enviados da infraestrutura do Amazon Chime Voice Connector para a extremidade remota.
rtt_btwn_vc_and_rem	O tempo médio de ida e volta entre a extremidade remota e a infraestrutura do Amazon Chime Voice Connector.
mos_btwn_vc_and_rem	A pontuação média de opinião (MOS) estimada associada a fluxos de voz entre a extremidade remota e a infraestrutura do Amazon Chime Voice Connector.

## Logs de mensagens SIP

É possível optar por receber logs de mensagens SIP para o Amazon Chime Voice Connector. Quando você faz isso, o Amazon Chime captura mensagens SIP de entrada e saída e as envia para um grupo de CloudWatch logs de registros criado para você. O nome do grupo de logs é `/aws/ChimeVoiceConnectorSipMessages/${VoiceConnectorID}`. Os campos a seguir estão incluídos nos logs, no formato JSON.

Campo	Descrição
voice_connector_id	O ID do Amazon Chime Voice Connector.
aws_region	A AWS região associada ao evento.
event_timestamp	A hora em que a mensagem é capturada, em número de milissegundos desde o UNIX epoch (meia-noite em 1º de janeiro de 1970) em UTC.
call_id	O ID de chamada do Amazon Chime Voice Connector.
sip_message	A mensagem SIP completa que é capturada.

## Automatizando o Amazon Chime com EventBridge

A Amazon EventBridge permite que você automatize seus AWS serviços e responda automaticamente a eventos do sistema, como problemas de disponibilidade de aplicativos ou alterações de recursos. Para obter mais informações sobre os eventos da reunião, consulte [Meeting events](#) no Guia do desenvolvedor do Amazon Chime.

Quando o Amazon Chime gera eventos, ele os envia EventBridge para a melhor entrega, o que significa que o Amazon Chime tenta enviar todos os eventos EventBridge para, mas em casos raros, um evento pode não ser entregue. Para obter mais informações, consulte [Eventos de AWS serviços](#) no Guia do EventBridge usuário da Amazon.

### Note

Se você precisar criptografar dados, deverá usar as chaves gerenciadas pelo Amazon S3. Não oferecemos suporte à criptografia do lado do servidor usando chaves mestras do cliente armazenadas no serviço de gerenciamento de AWS chaves.

## Automatizando os conectores de voz do Amazon Chime com EventBridge

As ações que podem ser automaticamente acionadas para os Amazon Chime Voice Connectors incluem as seguintes:

- Invocando uma função AWS Lambda
- Liberar uma tarefa do Amazon Elastic Container Service
- Retransmitir o evento para o Amazon Kinesis Video Streams
- Ativando uma máquina de AWS Step Functions estado
- Notificar um tópico do Amazon SNS ou uma fila do Amazon SQS

Alguns exemplos de uso EventBridge com os conectores de voz do Amazon Chime incluem:

- Ativar uma função do Lambda para fazer download do áudio de uma chamada depois que ela é encerrada.
- Executar uma tarefa do Amazon ECS para habilitar a transcrição em tempo real depois que uma chamada é iniciada.

Para obter mais informações, consulte o [Guia EventBridge do usuário da Amazon](#).

## Eventos de streaming do Amazon Chime Voice Connector

Os Amazon Chime Voice Connectors oferecem suporte ao envio de eventos para EventBridge quando os eventos discutidos nesta seção ocorrerem.

### Início do streaming do Amazon Chime Voice Connector

Os Amazon Chime Voice Connectors enviam esse evento quando o streaming de mídia para o Kinesis Video Streams se inicia.

### Example Dados de eventos

A seguir estão dados de exemplo para esse 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@abcdefghijklmno3pqr4.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-
abcdefghijklmno3pqr4-111aaa-22bb-33cc-44dd-111222/111122223333",
    "toNumber": "+13605550199",
    "transactionId": "12345678-1234-1234",
    "voiceConnectorId": "abcdefghijklmno3pqr4",
    "streamingStatus": "STARTED",
    "version": "0"
}
}

```

O streaming do Amazon Chime Voice Connector termina

Os Amazon Chime Voice Connectors enviam esse evento quando o streaming de mídia para o Kinesis Video Streams termina.

Example Dados de eventos

A seguir estão dados de exemplo para esse 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": "abcdefghijklmno3pqr4",
    "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"
  }
}

```

## Atualizações de streaming do Amazon Chime Voice Connector

Os Amazon Chime Voice Connectors enviam esse evento quando o streaming de mídia para o Kinesis Video Streams é atualizado.

### Exemplo Dados de eventos

A seguir estão dados de exemplo para esse 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"
    }
  }
}

```

## Falha no streaming do Amazon Chime Voice Connector

Os Amazon Chime Voice Connectors enviam esse evento quando o streaming de mídia para o Kinesis Video Streams falha.

### Example Dados de eventos

A seguir estão dados de exemplo para esse 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"
}
}
```

## Registrar chamadas de API do Amazon Chime com o AWS CloudTrail

O Amazon Chime é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço no Amazon Chime. CloudTrail captura todas as chamadas de API para o Amazon Chime como eventos, incluindo chamadas do console do Amazon Chime e de chamadas de código para o Amazon Chime. APIs Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o Amazon Chime. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao Amazon Chime, o endereço IP a partir do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais CloudTrail, consulte o [Guia AWS CloudTrail do usuário](#).

### Informações sobre o Amazon Chime em CloudTrail

CloudTrail é ativado em sua AWS conta quando você cria a conta. Quando as chamadas de API são feitas a partir do console de administração do Amazon Chime, essa atividade é registrada em um CloudTrail evento junto com outros eventos de AWS serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua AWS conta. Para obter mais informações, consulte [Visualização de eventos com histórico de CloudTrail eventos](#).

Para um registro contínuo dos eventos em sua AWS conta, incluindo eventos do Amazon Chime, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando uma trilha é criada no console, a mesma é aplicada a todas as regiões da . A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros AWS serviços para analisar e agir de acordo com: Dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte:

- [Visão geral da criação de uma trilha](#)

- [CloudTrail serviços e integrações suportados](#)
- [Configurando notificações do Amazon SNS para CloudTrail](#)
- [Recebendo arquivos de CloudTrail log de várias regiões](#) e [Recebendo arquivos de CloudTrail log de várias contas](#)

Todas as ações do Amazon Chime são registradas CloudTrail e documentadas na [Amazon Chime API Reference](#). Por exemplo, chamadas para as `ResetPersonalPIN` seções `CreateAccount`, `InviteUsers` e geram entradas nos arquivos de CloudTrail log. Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário-raiz ou usuário do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro AWS serviço.

Para obter mais informações, consulte [Elemento userIdentity do CloudTrail](#).

## Noções básicas sobre entradas de arquivos de log do Amazon Chime

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

As entradas do Amazon Chime são identificadas pela origem de evento `chime.amazonaws.com`.

Se você configurou o Active Directory para sua conta do Amazon Chime, consulte [Registro de chamadas de API do AWS Directory Service usando](#). CloudTrail Isso descreve como monitorar problemas que possam afetar a capacidade dos usuários do Amazon Chime de fazer login.

O exemplo a seguir mostra uma entrada de CloudTrail registro para o 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": "11aaaaa1-1a11-1111-1a11-aaadd0a0aa00"
  },
  "responseElements": null,
  "requestID": "be1bee1d-1111-11e1-1eD1-0dc1111f1ac1",
  "eventID": "00fbee1-123e-111e-93e3-11111bfbfcc1",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}

```

## Validação de conformidade para o Amazon Chime

Audidores terceirizados avaliam a segurança e a conformidade dos AWS serviços como parte de vários programas de AWS conformidade, como SOC, PCI, FedRAMP e HIPAA.

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte [Serviços da AWS Escopo por Programa de Conformidade](#) [Serviços da AWS](#) e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de [AWS conformidade Programas AWS](#) de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte [Baixar relatórios em AWS Artifact](#) .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- [Governança e conformidade de segurança](#): esses guias de implementação de solução abordam considerações sobre a arquitetura e fornecem etapas para implantar recursos de segurança e conformidade.
- [Referência de serviços qualificados para HIPAA](#): lista os serviços qualificados para HIPAA. Nem todos Serviços da AWS são elegíveis para a HIPAA.
- AWS Recursos de <https://aws.amazon.com/compliance/resources/> de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- [AWS Guias de conformidade do cliente](#) — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- [Avaliação de recursos com regras](#) no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- [AWS Security Hub](#)— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a [Referência de controles do Security Hub](#).
- [Amazon GuardDuty](#) — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.

- [AWS Audit Manager](#)— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

## Resiliência no Amazon Chime

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte [Infraestrutura AWS global](#).

Além da infraestrutura AWS global, o Amazon Chime oferece recursos diferentes para ajudar a suportar suas necessidades de resiliência e backup de dados. Para obter mais informações, consulte [Managing Amazon Chime Voice Connector groups](#) e [Streaming Amazon Chime Voice Connector media to Kinesis](#) no Guia de administração do SDK do Amazon Chime.

## Segurança de infraestrutura no Amazon Chime

Como um serviço gerenciado, o Amazon Chime é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte [AWS Cloud Security](#). Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte [Proteção](#) de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar pela rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou é possível usar o [AWS Security Token Service](#) (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

## Noções básicas sobre as atualizações automáticas do Amazon Chime

O Amazon Chime fornece maneiras diferentes de atualizar seus clientes. O método varia, dependendo se seus usuários executam o Amazon Chime em um navegador, em seu desktop ou em um dispositivo móvel.

A aplicação web do Amazon Chime (<https://app.chime.aws>) sempre carrega os recursos e correções de segurança mais recentes.

O cliente de desktop Amazon Chime verifica se há atualizações sempre que um usuário escolhe Sair ou Desconectar. Isso se aplica a máquinas Windows e macOS. Conforme os usuários executam o cliente, ele verifica se há atualizações a cada três horas. Os usuários também podem verificar se há atualizações escolhendo Verificar atualizações no menu Ajuda do Windows ou no menu Amazon Chime do macOS.

Quando o cliente de desktop detecta uma atualização, o Amazon Chime solicita que os usuários a instalem, a menos que estejam em uma reunião contínua. Os usuários estão em uma reunião contínua quando:

- Eles estão participando de uma reunião.
- Eles foram convidados para uma reunião que ainda está em andamento.

O Amazon Chime solicita que eles instalem a versão mais recente e fornece uma contagem regressiva de 15 segundos para que possam adiar a instalação. Escolha Tentar mais tarde para adiar a atualização.

Quando os usuários adiam uma atualização e não estão em uma reunião contínua, o cliente verifica a atualização após três horas e solicita que eles instalem novamente. A instalação se inicia quando a contagem regressiva termina.

 **Note**

Em um computador macOS, os usuários precisam escolher Reiniciar agora para iniciar a atualização.

Em um dispositivo móvel: os aplicativos móveis Amazon Chime usam as opções de atualização fornecidas pela App Store e pelo Google Play para fornecer a versão mais recente do cliente Amazon Chime. Você também pode distribuir atualizações por meio do sistema de gerenciamento de dispositivos móveis. Este tópico pressupõe que você sabe tem conhecimento.

# Histórico da documentação do Amazon Chime

A tabela a seguir descreve alterações importantes no Guia de administração do Amazon Chime, a partir de março de 2018. Para receber notificações sobre atualizações dessa documentação, assine um feed RSS.

Alteração	Descrição	Data
<a href="#">Aviso de fim do suporte</a>	Aviso de fim do suporte: em 20 de fevereiro de 2026, AWS encerrará o suporte para o serviço Amazon Chime. Depois de 20 de fevereiro de 2026, você não poderá mais acessar o console do Amazon Chime ou os recursos do aplicativo Amazon Chime. Para obter mais informações, acesse a <a href="#">postagem do blog</a> . Nota: Isso não afeta a disponibilidade do serviço <a href="#">Amazon Chime SDK</a> .	19 de fevereiro de 2025
<a href="#">Guia de administração do SDK do Amazon Chime publicado</a>	Os tópicos do SDK do Amazon Chime agora estão publicados no Guia de administração do SDK do Amazon Chime. Para obter informações, consulte o <a href="#">Guia de administração do SDK do Amazon Chime</a> .	24 de março de 2022
<a href="#">Atualizações de políticas do IAM</a>	As alterações nas políticas do IAM AWS gerenciadas pelo agora são monitoradas neste guia do administrador. Consulte <a href="#">Exemplos</a>	23 de setembro de 2021

[de políticas baseadas em identidade do Amazon Chime.](#)

[Perfis vinculados a serviço](#)

Agora os administradores podem criar perfis vinculados ao serviço para o Amazon Live Transcription e visualizar mensagens de eventos quando uma operação de transcrição ao vivo do Amazon Chime é iniciada e encerrada. Para obter mais informações, consulte [Uso de funções com transcrição ao vivo](#) e [Automatização do Amazon Chime](#) com eventos. CloudWatch

12 de agosto de 2021

[Aplicações e regras de mídia SIP](#)

Os administradores podem criar aplicativos e regras de mídia SIP para uso com o Amazon Chime Voice Connector e as funções. AWS Lambda Para obter mais informações, consulte [Gerenciamento de aplicativos e regras SIP](#) no Guia do Administrador do Amazon Chime.

18 de novembro de 2020

[Números de roteamento de chamadas de emergência do Amazon Chime Voice Connector](#)

Os administradores do Amazon Chime podem configurar números de roteamento de chamadas de emergência para um Amazon Chime Voice Connector. Para obter mais informações, consulte [Configurar números de roteamento de chamadas de emergência para seu Amazon Chime Voice Connector](#), no Guia do administrador do Amazon Chime.

1.º de julho de 2020

[Amazon Chime em Dolby Voice Huddle](#)

O Amazon Chime oferece uma experiência de reunião nativa ou original no hardware de áudio e de videoconferência do Dolby Voice Huddle. Para obter mais informações, consulte [Configuração do Amazon Chime no hardware Dolby, no](#) Guia do administrador do Amazon Chime.

3 de junho de 2020

[Definir políticas de retenção de bate-papo](#)

Os administradores do Amazon Chime podem definir políticas de retenção de chat para suas contas empresariais. Para obter mais informações, consulte [Gerenciamento de políticas de retenção de bate-papo](#) no Guia do administrador do Amazon Chime.

21 de maio de 2020

[Remover mensagens de chat](#)

Se você tiver a capacidade de programar, poderá usar um par do Amazon Chime APIs para remover mensagens das salas de bate-papo e conversas da sua conta. Para obter mais informações, consulte [Excluir mensagens individuais](#) no Guia do administrador do Amazon Chime.

18 de maio de 2020

[CloudWatch métricas de qualidade de mídia para o Amazon Chime Voice Connector](#)

O Amazon Chime suporta o envio de métricas de qualidade de mídia para seu Amazon Chime Voice Connector para. CloudWatch Para obter mais informações, consulte [Monitoramento do Amazon Chime com CloudWatch](#), no Guia do administrador do Amazon Chime.

23 de janeiro de 2020

[Aplicativo Amazon Chime Meetings para Slack](#)

O Amazon Chime oferece suporte ao aplicativo Amazon Chime Meetings for Slack. Para obter mais informações, consulte [Configuração do aplicativo Amazon Chime Meetings para Slack](#), no Guia do administrador do Amazon Chime.

4 de dezembro de 2019

[Configurações da região da reunião](#)

O Amazon Chime oferece suporte ao processamento de reuniões na AWS região ideal para todos os participantes. Para obter mais informações, consulte [Configurações da região da reunião](#), no Guia do administrador do Amazon Chime.

3 de dezembro de 2019

[Compatibilidade de gravação de mídia baseada em SIP \(SIPREC\)](#)

Os Amazon Chime Voice Connectors comportam streaming de mídia de uma infraestrutura de voz compatível com SIPREC para o Kinesis Video Streams. Para obter mais informações, consulte [Compatibilidade com gravação de mídia baseada em SIP \(SIPREC\)](#) no Guia do administrador do Amazon Chime.

25 de novembro de 2019

## [Amazon Chime em Dolby Voice Room](#)

Se você quiser que os usuários participem de reuniões de maneira conveniente, o Amazon Chime oferece uma experiência de reunião nativa ou original no hardware de áudio e de videoconferência do Dolby Voice Room. Para obter mais informações, consulte [Configuração do Amazon Chime no Dolby Voice Room](#), no Guia do administrador do Amazon Chime.

29 de outubro de 2019

## [Atualizar os nomes das chamadas de saída](#)

Defina um nome de chamada padrão que aparece para os destinatários das chamadas de saída feitas usando números de telefone do inventário do Amazon Chime. Para obter mais informações, consulte [Atualização de nomes de chamadas externas](#) no Amazon Chime Administrator Guide.

24 de outubro de 2019

[Fazer streaming de mídia para o Amazon Kinesis](#)

Faça streaming do áudio de chamadas telefônicas dos Amazon Chime Voice Connectors to Kinesis Video Streams para análises, machine learning e outro processamento. Para obter mais informações, consulte [Streaming de mídia do Amazon Chime Voice Connector para o Kinesis](#) e Uso da [função vinculada ao serviço Amazon Chime Voice Connector](#), no Guia do Administrador do Amazon Chime.

24 de outubro de 2019

[Monitorando o Amazon Chime com a Amazon CloudWatch](#)

Monitore o Amazon Chime usando CloudWatch, que coleta dados brutos e os processa em métricas legíveis, quase em tempo real. Para obter mais informações, consulte [Monitoramento do Amazon Chime com CloudWatch](#), no Guia do administrador do Amazon Chime.

24 de outubro de 2019

## [Grupos do Amazon Chime Voice Connector](#)

Crie um grupo de conectores de voz do Amazon Chime que inclua conectores de voz do Amazon Chime criados em diferentes regiões. AWS Isso permite que chamadas de entrada façam failover entre regiões, o que cria um mecanismo tolerante a falhas para fallback no caso de eventos de disponibilidade. Para obter mais informações, consulte Como [trabalhar com grupos do Amazon Chime Voice Connector](#), no Guia do administrador do Amazon Chime.

24 de outubro de 2019

## [Atualizações de configuração de rede](#)

O Amazon Chime está simplificando seus requisitos de firewall. Para obter mais informações, consulte [Requisitos de configuração de rede e largura de banda](#) no Amazon Chime Administrator Guide.

6 de setembro de 2019

## [Reuniões moderadas](#)

O Amazon Chime oferece suporte a reuniões moderadas. Para obter mais informações, consulte [Participar de uma reunião moderada](#), no Guia do administrador do Amazon Chime.

25 de julho de 2019

[Validação de conformidade para o Amazon Chime](#)

O Amazon Chime é um serviço qualificado pela HIPAA. Para obter mais informações, consulte [Validação de conformidade para o Amazon Chime](#) no Guia de administração do Amazon Chime.

11 de junho de 2019

[Transferir de números de telefone com ligação gratuita](#)

O Amazon Chime oferece suporte à portabilidade de números de telefone gratuitos dos Estados Unidos para uso com os Amazon Chime Voice Connectors. Para obter mais informações, consulte [Como portar números de telefone existentes](#) no Amazon Chime Administrator Guide.

28 de maio de 2019

[Gerenciar números de telefone no Amazon Chime](#)

Use o Amazon Chime Business Calling para provisionar e atribuir números de telefone aos usuários do Amazon Chime. Integre um Amazon Chime Voice Connector a um sistema telefônico existente. Para obter mais informações, consulte [Gerenciamento de números de telefone no Amazon Chime](#) no Guia de administração do Amazon Chime.

18 de março de 2019

### [Suplemento do Amazon Chime para Outlook](#)

O Amazon Chime fornece duas extensões para o Microsoft Outlook: a extensão do Amazon Chime para Outlook no Windows e extensão do Amazon Chime para Outlook. Essas extensões oferecem os mesmos recursos de programação, mas oferecem suporte a diferentes tipos de usuários. Para obter mais informações, consulte [Implantação do complemento para Outlook](#), no Guia do administrador do Amazon Chime.

12 de março de 2019

### [Várias atualizações](#)

Várias atualizações no layout do tópico e na organização.

11 de fevereiro de 2019

### [Recurso “Ligar para mim” do Amazon Chime](#)

Os administradores podem habilitar o recurso “Ligar para mim” do Amazon Chime nas configurações de Reuniões. Para obter mais informações, consulte [Gerenciamento de configurações de reunião](#), no Guia do administrador do Amazon Chime.

22 de agosto de 2018

---

<a href="#">Conectar-se ao Okta SSO</a>	Caso tenha uma conta empresarial, você pode se conectar ao Okta SSO para se autenticar e atribuir permissões de usuário. Para obter mais informações, consulte <a href="#">Connect to Okta SSO</a> , no Amazon Chime Administrator Guide.	1º de agosto de 2018
<a href="#">Solicitar anexos do usuário</a>	Receba anexos que os usuários carregaram no Amazon Chime. Para obter mais informações, consulte <a href="#">Solicitar anexos do usuário</a> , no Guia do administrador do Amazon Chime.	23 de abril de 2018
<a href="#">Visualizar dados de relatório adicionais</a>	Visualize dados de relatório adicionais. Para obter mais informações, consulte <a href="#">Exibir relatórios</a> no Guia do administrador do Amazon Chime.	30 de março de 2018
<a href="#">Atribuir a usuários permissões Pro ou Basic</a>	Atribuir a usuários permissões Pro ou Basic. Para obter mais informações, consulte <a href="#">Gerenciar o acesso e as permissões do usuário</a> no Guia do administrador do Amazon Chime.	29 de março de 2018