Amazon Chime SDK

Administration Guide

Amazon Chime SDK: Administration Guide

Table of Contents

What is the Amazon Chime SDK?

The Amazon Chime SDK is a set of real-time communications components that developers can use to quickly add messaging, audio, video, and screen sharing capabilities to their web or mobile applications. For instance, they can add video to a health application so patients can consult with doctors on health issues remotely, or create customized audio prompts for integration with a public switched telephone network (PSTN). By using the Amazon Chime SDK, developers can help eliminate the cost, complexity, and friction of creating and maintaining their own real-time communication infrastructure and services.

For more information, see Amazon Chime SDK.

Pricing

The Amazon Chime SDK offers pay-for-use pricing with no upfront fees. Developers implementing the SDK can choose to implement some or all of the available media modalities (audio, video, and screen share) for a single rate. Messaging, media pipelines, speech enhancement, and PSTN audio capabilities are also available with pay-for-use pricing. For more information, see Amazon Chime SDK pricing.

Prerequisites

You must have an AWS account to access the Amazon Chime console and create an Amazon Chime administrator account.

Creating an Amazon Web Services account

Before you can create an administrator account for Amazon Chime, you must first create an AWS account.

To create an AWS account

1. Open https://portal.aws.amazon.com/billing/signup.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

For information about how to finish setting up your Amazon Chime administrator account, see Getting started (p. 38).

Security in Amazon Chime SDK

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security *of* the cloud and security *in* the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to the Amazon Chime SDK, see AWS Services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using the Amazon Chime SDK. The following topics show you how to configure the Amazon Chime SDK to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Amazon Chime SDK resources.

Topics

Identity and access management for the Amazon Chime SDK

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use Amazon Chime SDK resources. IAM is an AWS service that you can use with no additional charge.

Topics

Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work that you do in the Amazon Chime SDK.

Service user – If you use the Amazon Chime SDK service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Amazon Chime SDK features to do your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator. If you cannot access a feature in Amazon Chime SDK, see Troubleshooting Amazon Chime SDK identity and access (p. 14).

Service administrator – If you're in charge of Amazon Chime SDK resources at your company, you probably have full access to the Amazon Chime SDK. It's your job to determine which Amazon Chime SDK features and resources your employees should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with the Amazon Chime SDK, see How the Amazon Chime SDK works with IAM (p. 8).

IAM administrator – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to the Amazon Chime SDK. To view example Amazon Chime SDK identity-based policies that you can use in IAM, see Amazon Chime SDK identity-based policy examples (p. 10).

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. For more information about signing in using the AWS Management Console, see Signing in to the AWS Management Console as an IAM user or root user in the *IAM User Guide*.

You must be *authenticated* (signed in to AWS) as the AWS account root user, an IAM user, or by assuming an IAM role. You can also use your company's single sign-on authentication or even sign in using Google or Facebook. In these cases, your administrator previously set up identity federation using IAM roles. When you access AWS using credentials from another company, you are assuming a role indirectly.

To sign in directly to the AWS Management Console, use your password with your root user email address or your IAM user name. You can access AWS programmatically using your root user or IAM users access keys. AWS provides SDK and command line tools to cryptographically sign your request using your credentials. If you don't use AWS tools, you must sign the request yourself. Do this using *Signature Version 4*, a protocol for authenticating inbound API requests. For more information about authenticating requests, see Signature Version 4 signing process in the *AWS General Reference*.

Regardless of the authentication method that you use, you might also be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see Using multi-factor authentication (MFA) in AWS in the *IAM User Guide*.

AWS account root user

When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and

is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the best practice of using the root user only to create your first IAM user. Then securely lock away the root user credentials and use them to perform only a few account and service management tasks.

IAM users and groups

An *IAM user* is an identity within your AWS account that has specific permissions for a single person or application. An IAM user can have long-term credentials such as a user name and password or a set of access keys. To learn how to generate access keys, see Managing access keys for IAM users in the *IAM User Guide*. When you generate access keys for an IAM user, make sure you view and securely save the key pair. You cannot recover the secret access key in the future. Instead, you must generate a new access key pair.

An *IAM group* is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named *IAMAdmins* and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see When to create an IAM user (instead of a role) in the *IAM User Guide*.

IAM roles

An *IAM role* is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. You can temporarily assume an IAM role in the AWS Management Console by switching roles. You can assume a role by calling an AWS CLI or AWS API operation or by using a custom URL. For more information about methods for using roles, see Using IAM roles in the *IAM User Guide*.

IAM roles with temporary credentials are useful in the following situations:

- **Temporary IAM user permissions** – An IAM user can assume an IAM role to temporarily take on different permissions for a specific task.
- **Federated user access** – Instead of creating an IAM user, you can use existing identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as *federated users*. AWS assigns a role to a federated user when access is requested through an identity provider. For more information about federated users, see Federated users and roles in the *IAM User Guide*.
- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see How IAM roles differ from resource-based policies in the *IAM User Guide*.
- **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.
  - **Principal permissions** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. Policies grant permissions to a principal. When you use some services, you might perform an action that then triggers another action in a different service. In this case, you must have permissions to perform both actions. To see whether an action requires additional

dependent actions in a policy, see Actions, resources, and condition keys for Amazon Chime in the *Service Authorization Reference*.

- **Service role** – A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Creating a role to delegate permissions to an AWS service in the *IAM User Guide*.
- **Service-linked role** – A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your IAM account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

- **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see Using an IAM role to grant permissions to applications running on Amazon EC2 instances in the *IAM User Guide*.

To learn whether to use IAM roles or IAM users, see When to create an IAM role (instead of a user) in the *IAM User Guide*.

Managing access using policies

You control access in AWS by creating policies and attaching them to IAM identities or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. You can sign in as the root user or an IAM user, or you can assume an IAM role. When you then make a request, AWS evaluates the related identity-based or resource-based policies. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see Overview of JSON policies in the *IAM User Guide*.

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

Every IAM entity (user or role) starts with no permissions. In other words, by default, users can do nothing, not even change their own password. To give a user permission to do something, an administrator must attach a permissions policy to a user. Or the administrator can add the user to a group that has the intended permissions. When an administrator gives permissions to a group, all users in that group are granted those permissions.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Creating IAM policies in the *IAM User Guide*.

Identity-based policies can be further categorized as *inline policies* or *managed policies*. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see Choosing between managed policies and inline policies in the *IAM User Guide*.

Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

AWS managed policies for the Amazon Chime SDK

To add permissions to users, groups, and roles, it is easier to use AWS managed policies than to write policies yourself. It takes time and expertise to create IAM customer managed policies that provide your team with only the permissions they need. To get started quickly, you can use our AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see AWS managed policies in the *IAM User Guide*.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the **ReadOnlyAccess** AWS managed policy provides read-only access to all AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see AWS managed policies for job functions in the *IAM User Guide*.

Access Control Lists (ACLs)

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs. To learn more about ACLs, see Access control list (ACL) overview in the *Amazon Simple Storage Service Developer Guide*.

Other policy types

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the `Principal` field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see Permissions boundaries for IAM entities in the *IAM User Guide*.
- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all

features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see How SCPs work in the *AWS Organizations User Guide*.

- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see Session policies in the *IAM User Guide*.

Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see Policy evaluation logic in the *IAM User Guide*.

How the Amazon Chime SDK works with IAM

Before you use IAM to manage access to the Amazon Chime SDK, you should understand what IAM features are available to use with the Amazon Chime SDK. To get a high-level view of how the Amazon Chime SDK and other AWS services work with IAM, see AWS services that work with IAM in the *IAM User Guide*.

Topics

Amazon Chime SDK identity-based policies

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. The Amazon Chime SDK supports specific actions, resources, and condition keys. To learn about all of the elements that you use in a JSON policy, see IAM JSON policy elements reference in the *IAM User Guide*.

Actions

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Action` element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Policy actions usually have the same name as the associated AWS API operation. There are some exceptions, such as *permission-only actions* that don't have a matching API operation. There are also some operations that require multiple actions in a policy. These additional actions are called *dependent actions*.

Include actions in a policy to grant permissions to perform the associated operation.

Condition keys

The Amazon Chime SDK does not provide any service-specific condition keys. To see all AWS global condition keys, see AWS Global Condition Context Keys in the *IAM User Guide*.

Resources

The Amazon Chime SDK does not support specifying resource ARNs in a policy.

Examples

To view examples of Amazon Chime SDK identity-based policies, see Amazon Chime SDK identity-based policy examples (p. 10).

Cross-service confused deputy prevention

The confused deputy problem is an information security issue that occurs when an entity without permission to perform an action calls a more-privileged entity to perform the action. This can allow malicious actors to run commands or modify resources they otherwise would not have permission to run or access. For more information, see The confused deputy problem in the *AWS Identity and Access Management User Guide*.

In AWS, cross-service impersonation can lead to a confused deputy scenario. Cross-service impersonation happens when one service (the *calling service*) calls another service (the *called service*). A malicious actor can use the calling service to alter resources in another service by using permissions that they normally would not have.

AWS provides service principals with managed access to resources on your account to help you protect your resources' security. We recommend using the `aws:SourceAccount` global condition context key in your resource policies. These keys limit the permissions that the Amazon Chime SDK gives another service to that resource.

The following example shows an S3 bucket policy that uses the `aws:SourceAccount` global condition context key in the configured `CallDetailRecords` S3 bucket to help prevent the confused deputy problem.

```
{
    "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"
                }
            }
        }
```

```
    ]
}
```

Amazon Chime SDK resource-based policies

The Amazon Chime SDK does not support resource-based policies.

Authorization based on Amazon Chime tags

Amazon Chime does not support tagging resources or controlling access based on tags.

Amazon Chime IAM roles

An IAM role is an entity within your AWS account that has specific permissions.

Using temporary credentials with Amazon Chime

You can use temporary credentials to sign in with federation, assume an IAM role, or to assume a cross-account role. You obtain temporary security credentials by calling AWS STS API operations such as AssumeRole or GetFederationToken.

Amazon Chime supports using temporary credentials.

Service-linked roles

Service-linked roles allow AWS services to access resources in other services that complete actions on your behalf. Service-linked roles appear in your IAM account, and the services own the roles. An IAM administrator can view but not edit the permissions for service-linked roles.

Amazon Chime supports service-linked roles. For details about creating or managing Amazon Chime service-linked roles, see Using service-linked roles for Amazon Chime SDK (p. 16).

Service roles

This feature allows a service to assume a service role on your behalf. This role allows the service to access resources in other services to complete an action on your behalf. Service roles appear in your IAM account and are owned by the account. This means that an IAM administrator can change the permissions for this role. However, doing so might break the functionality of the service.

Amazon Chime does not support service roles.

Amazon Chime SDK identity-based policy examples

By default, IAM users and roles don't have permission to create or modify Amazon Chime SDK resources. They also can't perform tasks using the AWS Management Console, AWS CLI, or AWS API. An IAM

administrator must create IAM policies that grant users and roles permission to perform specific API operations on the specified resources they need. The administrator must then attach those policies to the IAM users or groups that require those permissions.

To learn how to create an IAM identity-based policy using these example JSON policy documents, see Creating policies on the JSON tab in the *IAM User Guide*.

Topics

Policy best practices

Identity-based policies are very powerful. They determine whether someone can create, access, or delete Amazon Chime SDK resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started using AWS managed policies** – To start using the Amazon Chime SDK quickly, use AWS managed policies to give your employees the permissions they need. These policies are already available in your account and are maintained and updated by AWS. For more information, see Get started using permissions with AWS managed policies in the *IAM User Guide*.
- **Grant least privilege** – When you create custom policies, grant only the permissions required to perform a task. Start with a minimum set of permissions and grant additional permissions as necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them later. For more information, see Grant least privilege in the *IAM User Guide*.
- **Enable MFA for sensitive operations** – For extra security, require IAM users to use multi-factor authentication (MFA) to access sensitive resources or API operations. For more information, see Using multi-factor authentication (MFA) in AWS in the *IAM User Guide*.
- **Use policy conditions for extra security** – To the extent that it's practical, define the conditions under which your identity-based policies allow access to a resource. For example, you can write conditions to specify a range of allowable IP addresses that a request must come from. You can also write conditions to allow requests only within a specified date or time range, or to require the use of SSL or MFA. For more information, see IAM JSON policy elements: Condition in the *IAM User Guide*.

Allow users to access Amazon Chime SDK actions

Use the AWS managed **AmazonChimeSDK** policy to grant users access to Amazon Chime SDK actions. For more information, see Example IAM roles in the *Amazon Chime SDK Developer GUide*, and Actions, resources, and condition keys for Amazon Chime in the *Service Authorization Reference*.

```
// Policy ARN: arn:aws:iam::aws:policy/AmazonChimeSDK
// Description: Provides access to Amazon Chime SDK operations
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "chime:CreateMeeting",
                "chime:CreateMeetingWithAttendees",
```

```
                "chime:DeleteMeeting",
                "chime:GetMeeting",
                "chime:ListMeetings",
                "chime:CreateAttendee",
                "chime:BatchCreateAttendee",
                "chime:DeleteAttendee",
                "chime:GetAttendee",
                "chime:ListAttendees",
                "chime:ListAttendeeTags",
                "chime:ListMeetingTags",
                "chime:ListTagsForResource",
                "chime:TagAttendee",
                "chime:TagMeeting",
                "chime:TagResource",
                "chime:UntagAttendee",
                "chime:UntagMeeting",
                "chime:UntagResource",
                "chime:StartMeetingTranscription",
                "chime:StopMeetingTranscription"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS managed policy: AmazonChimeVoiceConnectorServiceLinkedRolePolicy

The `AmazonChimeVoiceConnectorServiceLinkedRolePolicy` enables Amazon Chime Voice Connectors to stream media to Amazon Kinesis Video Streams, provide streaming notifications, and synthesize speech using Amazon Polly. This policy grants the Amazon Chime Voice Connector service permissions to access customer's Amazon Kinesis Video Streams, send notification events to the Amazon Simple Notification Service and Amazon Simple Queue Service, and use Amazon Polly to synthesize speech when using the Amazon Chime SDK Voice Applications `Speak` and `SpeakAndGetDigits` actions. For more information, see Using the Amazon Chime Voice Connector service-linked role (p. 16).

AWS managed policy: AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy

You can't attach `AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy` to your IAM entities. This policy allows Amazon Chime SDK media pipelines to access Amazon Chime SDK meetings on your behalf. For more information, see Using roles with Amazon Chime SDK media pipelines (p. 20) in this guide.

Permissions details

This policy includes the following permissions.

- `chime` – Grants permissions to get meetings, create attendees, and delete attendees.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": [
        "chime:GetMeeting",
        "chime:CreateAttendee",
                "chime:DeleteAttendee"
       ],
      "Resource": "*"
        }
    ]
}
```

Amazon Chime updates to AWS managed policies

The following table lists and describes the updates made to the Amazon Chime IAM policy.

Change	Description	Date
Added the AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy (p. 12) – new managed policy.	The Amazon Chime SDK added a service-linked role that allows you to use media capture pipelines in Amazon Chime SDK meetings.	April 27, 2022
AWS managed policy: AmazonChimeVoiceConnectorServiceLinkedRolePolicy (p. 12) – Update to an existing policy	Amazon Chime Voice Connectors added new permissions to allow you to use Amazon Polly to synthesize speech.These permissions are required to use the `Speak` and `SpeakAndGetDigits` actions in Amazon Chime SDK Voice Applications.	March 15, 2022
`AmazonChimeVoiceConnectorServiceLinkedRolePolicy` – Update to an existing policy	Amazon Chime Voice Connector added new permissions to allow access to Amazon Kinesis Video Streams and send notification events to SNS and SQS. These permissions are required for Amazon Chime Voice Connectors to stream media to Amazon Kinesis Video Streams and provide streaming notifications.	December 20, 2021
Change to existing policy. Creating IAM users or roles with the Chime SDK policy.	Amazon Chime added new actions to support expanded validation. A number of actions were added to allow listing and tagging of attendees and meeting resources, and for starting and stopping meeting transcription.	September 23, 2021
Amazon Chime started tracking changes	Amazon Chime started tracking changes for its AWS managed policies.	September 23, 2021

Troubleshooting Amazon Chime SDK identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with the Amazon Chime SDK and IAM.

Topics

I am not authorized to perform an action in the Amazon Chime SDK

If the Amazon Chime SDK tells you that you're not authorized to perform an action, then you must contact your administrator for assistance. Your administrator is the person that provided you with your user name and password.

The following example error occurs when the `mateojackson` IAM user tries to use the service to view details about a domain but does not have `chime:GetDomain` permissions.

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

In this case, Mateo asks his administrator to update his policies to allow him to access the domain details using the `chime:GetDomain` action.

I am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, then you must contact your administrator for assistance. Your administrator is the person that provided you with your user name and password. Ask that person to update your policies to allow you to pass a role to Amazon Chime SDK.

Some AWS services allow you to pass an existing role to that service, instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named `marymajor` tries to use the service to perform an action in Amazon Chime SDK. However, the action requires the service to have permissions granted by a service role. Mary does not have permissions to pass the role to the service.

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

In this case, Mary asks her administrator to update her policies to allow her to perform the `iam:PassRole` action.

I want to view my access keys

After you create your IAM user access keys, you can view your access key ID at any time. However, you can't view your secret access key again. If you lose your secret key, you must create a new access key pair.

Access keys consist of two parts: an access key ID (for example, `AKIAIOSFODNN7EXAMPLE`) and a secret access key (for example, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. Manage your access keys as securely as you do your user name and password.

> **Important**
> Do not provide your access keys to a third party, even to help find your canonical user ID. By doing this, you might give someone permanent access to your account.

When you create an access key pair, you are prompted to save the access key ID and secret access key in a secure location. The secret access key is available only at the time you create it. If you lose your secret access key, you must add new access keys to your IAM user. You can have a maximum of two access keys. If you already have two, you must delete one key pair before creating a new one. To view instructions, see Managing access keys in the *IAM User Guide*.

I'm an administrator and want to allow others to access the Amazon Chime SDK

To allow others to access Amazon Chime SDK, you must create an IAM entity (user or role) for the person or application that needs access. They will use the credentials for that entity to access AWS. You must then attach a policy to the entity that grants them the correct permissions in Amazon Chime SDK.

To get started right away, see Creating your first IAM delegated user and group in the *IAM User Guide*.

I want to allow people outside of my AWS account to access my Amazon Chime SDK resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Amazon Chime SDK supports these features, see How the Amazon Chime SDK works with IAM (p. 8).
- To learn how to provide access to your resources across AWS accounts that you own, see Providing access to an IAM user in another AWS account that you own in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see Providing access to AWS accounts owned by third parties in the *IAM User Guide*.
- To learn how to provide access through identity federation, see Providing access to externally authenticated users (identity federation) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see How IAM roles differ from resource-based policies in the *IAM User Guide*.

Using service-linked roles for Amazon Chime SDK

The Amazon Chime SDK uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to the Amazon Chime SDK. Service-linked roles are predefined by the Amazon Chime SDK and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up the Amazon Chime SDK more efficient because you aren't required to manually add the necessary permissions. The Amazon Chime SDK defines the permissions of its service-linked roles, and unless defined otherwise, only the Amazon Chime SDK can assume its roles. The defined permissions include the trust policy and the permissions policy. The permissions policy cannot be attached to any other IAM entity.

You can delete a service-linked role only after first deleting their related resources. This protects your Amazon Chime SDK resources because you can't inadvertently remove permission to access the resources.

For information about other services that support service-linked roles, see AWS services that work with IAM. Look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Topics

Using the Amazon Chime Voice Connector service-linked role

The information in the following sections explains how to:

- Use a service-linked role to stream Amazon Chime Voice Connector media to Kinesis
- Synthesize speech with Amazon Polly and the Speak and SpeakAndGetDigits actions.

Topics

Service-linked role permissions for Amazon Chime Voice Connectors

Amazon Chime Voice Connectors use the service-linked role named **AWSServiceRoleForAmazonChimeVoiceConnector** – Allows Amazon Chime SDK Voice Connectors to call AWS services on your behalf. For more information about how to start media streaming for your Amazon Chime Voice Connector, see Streaming Amazon Chime Voice Connector media to Kinesis (p. 66).

The AWSServiceRoleForAmazonChimeVoiceConnector service-linked role trusts the following services to assume the role:

- `voiceconnector.chime.amazonaws.com`

The role permissions policy allows the Amazon Chime SDK to complete the following actions on the specified resources:

- Action: `chime:GetVoiceConnector*` on `all AWS resources`
- Action: `kinesisvideo:*` on `arn:aws:kinesisvideo:us-east-1:111122223333:stream/ChimeVoiceConnector-*`
- Action: `polly:SynthesizeSpeech` on `all AWS resources`

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-Linked Role Permissions in the *IAM User Guide*.

Creating a service-linked role for Amazon Chime Voice Connectors

You don't need to manually create a service-linked role. When you start Kinesis media streaming for your Amazon Chime Voice Connector, or create or update an Amazon Chime SDK SIP media application in the AWS Management Console, the AWS CLI, or the AWS API, Amazon Chime creates the service-linked role for you.

You can also use the IAM console to create a service-linked role with the **Chime Voice Connector** use case. In the AWS CLI or the AWS API, create a service-linked role with the `voiceconnector.chime.amazonaws.com` service name. For more information, see Creating a service-linked role in the *IAM User Guide*. If you delete this service-linked role, you can use this same process to create the role again.

Editing a service-linked role for Amazon Chime Voice Connectors

The Amazon Chime SDK does not allow you to edit the AWSServiceRoleForAmazonChimeVoiceConnector service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role in the *IAM User Guide*.

Deleting a service-linked role for Amazon Chime Voice Connectors

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored or maintained. However, you must clean up your service-linked role before you can manually delete it.

Cleaning up a service-linked role

Before you can use IAM to delete a service-linked role, you must first delete any resources used by the role.

> **Note**
> If the Amazon Chime SDK service is using the role when you try to delete the resources, then the deletion might fail. If that happens, wait for a few minutes and try the operation again.

To delete Amazon Chime SDK resources used by the AWSServiceRoleForAmazonChimeVoiceConnector (console)

- Stop media streaming for all the Amazon Chime Voice Connectors in your Amazon Chime SDK account.

  a. Open the Amazon Chime console at https://chime.aws.amazon.com/.
  b. For **Calling**, choose **Voice connectors**.
  c. Choose the name of the Amazon Chime Voice Connector.
  d. Choose **Streaming**.
  e. For **Send to Kinesis Video Streams**, choose **Stop**.
  f. Choose **Save**.

To delete Amazon Chime SDK resources used by the AWSServiceRoleForAmazonChimeVoiceConnector (AWS CLI)

- Use the **delete-voice-connector-streaming-configuration** command in the AWS CLI to stop media streaming for all Amazon Chime Voice Connectors in your account.

```
aws chime delete-voice-connector-streaming-configuration --voice-connector-
id abcdef1ghij2klmno3pqr4
```

To delete Amazon Chime SDK resources used by the AWSServiceRoleForAmazonChimeVoiceConnector (API)

- Use the **DeleteVoiceConnectorStreamingConfiguration** API operation to stop media streaming for all Amazon Chime Voice Connectors in your account. For more information, see DeleteVoiceConnectorStreamingConfiguration in the *Amazon Chime API Reference*.

Manually delete the service-linked role

Use the IAM console, the AWS CLI, or the AWS API operation to delete the AWSServiceRoleForAmazonChimeVoiceConnector service-linked role. For more information, see Deleting a service-linked role in the *IAM User Guide*.

Supported Regions for Amazon Chime SDK service-linked roles

Amazon Chime SDK supports using service-linked roles in all of the AWS Regions where the service is available. For more information, see Amazon Chime endpoints and quotas.

Using roles with live transcription

The information in the following sections explains how to create and manage a service-linked role for the Amazon Chime SDK live transcription. For more information about the live transcription service, see Using Amazon Chime SDK live transcription.

Topics

- Supported Regions for Amazon Chime Service-Linked Roles (p. 20)

Service-Linked Role Permissions for Amazon Chime SDK Live Transcription

Amazon Chime SDK Live Transcription uses a service-linked role named **AWSServiceRoleForAmazonChimeTranscription – Allows the Amazon Chime SDK to access Amazon Transcribe and Amazon Transcribe Medical on your behalf.**

The AWSServiceRoleForAmazonChimeTranscription service-linked role trusts the following services to assume the role:

- `transcription.chime.amazonaws.com`

The role permissions policy allows the Amazon Chime SDK to complete the following actions on the specified resources:

- Action: `transcribe:StartStreamTranscription` on `all AWS resources`
- Action: `transcribe:StartMedicalStreamTranscription` on `all AWS resources`

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-Linked Role Permissions in the *IAM User Guide*.

Creating a Service-Linked Role for Amazon Chime SDK Live Transcription

You use the IAM console to create a service-linked role with the **Chime Transcription** use case.

> **Note**
> You must have IAM administrative permissions to complete these steps. If you don't, contact a system administrator.

To create the role

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane of the IAM console, choose **Roles**, then choose **Create role**.
3. Choose the **AWS Service** role type, then choose **Chime Transcription**.

   The IAM policy appears.
4. Select the checkbox next to the policy, then choose **Next: Tags**.
5. Choose **Next: Review**.
6. Edit the description as needed, then choose **Create role**.

You can also use the AWS CLI or the AWS API to create a service-linked role named transcription.chime.amazonaws.com.

In the CLI, run this command: `aws iam create-service-linked-role --aws-service-name transcription.chime.amazonaws.com`.

For more information, see Creating a Service-Linked Role in the *IAM User Guide*. If you delete this service-linked role, you can use this same process to create the role again.

Editing a Service-Linked Role for Amazon Chime SDK Live Transcription

The Amazon Chime SDK does not allow you to edit the AWSServiceRoleForAmazonChimeTranscription service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can use IAM to edit the role's description. For more information, see Editing a Service-Linked Role in the *IAM User Guide*.

Deleting a Service-Linked Role for Amazon Chime SDK Live Transcription

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored or maintained.

To manually delete the service-linked role using IAM

Use the IAM console, the AWS CLI, or the AWS API to delete the AWSServiceRoleForAmazonChimeTranscription service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

Supported Regions for Amazon Chime Service-Linked Roles

The Amazon Chime SDK supports using service-linked roles in all of the regions where the service is available. For more information, see Amazon Chime endpoints and quotas, and Using Amazon Chime SDK media Regions.

Using roles with Amazon Chime SDK media pipelines

The information in the following sections explains how to create and manage a service-linked role for Amazon Chime SDK Media Pipelines.

Topics

Service-linked role permissions for Amazon Chime SDK media pipelines

Amazon Chime uses the service-linked role named **AWSServiceRoleForAmazonChimeSDKMediaPipelines** – Allows Amazon Chime SDK media pipelines to access Amazon Chime SDK meetings on your behalf.

The *AWSServiceRoleForAmazonChimeSDKMediaPipelines* service-linked role trusts the following services to assume the role:

- `mediapipelines.chime.amazonaws.com`

The role allows Amazon Chime to complete the following actions on the specified resources:

- Action: `chime:CreateAttendee` on `all AWS resources`
- Action: `chime:DeleteAttendee` on `all AWS resources`
- Action: `chime:GetMeeting` on `all AWS resources`

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-Linked Role Permissions in the *IAM User Guide*.

Creating a service-linked role for Amazon Chime SDK media pipelines

You use the IAM console to create a service-linked role with the **Amazon Chime SDK Media Pipelines** use case.

> **Note**
> You must have IAM administrative permissions to complete these steps. If you don't, contact a system administrator.

To create the role

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane of the IAM console, choose **Roles**, then choose **Create role**.
3. Choose the **AWS Service** role type, then choose **Chime**, then choose **Chime SDK Media Pipelines**.
4. Choose **Next**.
5. Choose **Next**.
6. Edit the description as needed, then choose **Create role**.

You can also use the AWS CLI or the AWS API to create a service-linked role named `mediapipelines.chime.amazonaws.com`.

In the AWS CLI, run this command: `aws iam create-service-linked-role --aws-service-name mediapipelines.chime.amazonaws.com`.

For more information, see Creating a Service-Linked Role in the *IAM User Guide*. If you delete this service-linked role, you can use this same process to create the role again.

Editing a service-linked role for Amazon Chime SDK media pipelines

Amazon Chime doesn't allow you to edit the *AWSServiceRoleForAmazonChimeSDKMediaPipelines* service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a Service-Linked Role in the *IAM User Guide*.

Deleting a service-linked role for Amazon Chime SDK media pipelines

When you don't need to use a feature or service that requires a service-linked role, we recommend deleting that role. That way you don’t have an unused entity that isn't actively monitored or maintained.

To manually delete the service-linked role using IAM

Use the IAM console, the AWS CLI, or the AWS API to delete the *AWSServiceRoleForAmazonChimeSDKMediaPipelines* service-linked role. For more information, see Deleting a Service-Linked Role in the *IAM User Guide*.

Supported Regions for Amazon Chime SDK media pipelines service-linked roles

The Amazon Chime SDK supports using service-linked roles in all of the AWS Regions where the service is available. For more information, see Amazon Chime endpoints and quotas.

Logging and monitoring in the Amazon Chime SDK

Monitoring is an important part of maintaining the reliability, availability, and performance of the Amazon Chime SDK and your other AWS solutions. AWS provides the following tools to monitor the Amazon Chime SDK, report issues, and take automatic actions when appropriate:

- *Amazon CloudWatch* monitors in real time your AWS resources and the applications that you run on AWS. You can collect and track metrics, create customized dashboards, and set alarms that notify you or take actions when a specified metric reaches a threshold that you specify. For example, you can have CloudWatch track CPU usage or other metrics of your Amazon EC2 instances and automatically launch new instances when needed. For more information, see the Amazon CloudWatch User Guide.
- *Amazon EventBridge* delivers a near real-time stream of system events that describe changes in AWS resources. EventBridge enables automated event-driven computing. This lets you write rules that watch for certain events, and trigger automated actions in other AWS services when these events happen. For more information, see the Amazon EventBridge User Guide.
- *Amazon CloudWatch Logs* lets you monitor, store, and access your log files from Amazon EC2 instances, CloudTrail, and other sources. CloudWatch Logs can monitor information in the log files and notify you when certain thresholds are met. You can also archive your log data in highly durable storage. For more information, see the Amazon CloudWatch Logs User Guide.
- *AWS CloudTrail* captures API calls and related events made by or on behalf of your AWS account. It then delivers the log files to an Amazon S3 bucket that you specify. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred. For more information, see the AWS CloudTrail User Guide.

Topics

Monitoring the Amazon Chime SDK with Amazon CloudWatch

You can monitor the Amazon Chime SDK using CloudWatch, which collects raw data and processes it into readable, near real-time metrics. These statistics are kept for 15 months, so that you can access historical information and gain a better perspective about how your web application or service is performing. You can also set alarms that watch for certain thresholds, and send notifications or take actions when those thresholds are met. For more information, see the Amazon CloudWatch User Guide.

CloudWatch metrics for the Amazon Chime SDK

The Amazon Chime SDK sends the following metrics to CloudWatch.

The `AWS/ChimeVoiceConnector` namespace includes the following metrics for phone numbers assigned to your AWS account and to Amazon Chime Voice Connectors.

Metric	Description
`InboundCallAttempts`	The number of inbound calls attempted. Units: Count
`InboundCallFailures`	The number of inbound call failures. Units: Count
`InboundCallsAnswered`	The number of inbound calls that are answered. Units: Count
`InboundCallsActive`	The number of inbound calls that are currently active. Units: Count
`OutboundCallAttempts`	The number of outbound calls attempted. Units: Count
`OutboundCallFailures`	The number of outbound call failures. Units: Count
`OutboundCallsAnswered`	The number of outbound calls that are answered. Units: Count
`OutboundCallsActive`	The number of outbound calls that are currently active. Units: Count
`Throttles`	The number of times your account is throttled when attempting to make a call. Units: Count
`Sip1xxCodes`	The number of SIP messages with 1xx-level status codes. Units: Count
`Sip2xxCodes`	The number of SIP messages with 2xx-level status codes. Units: Count
`Sip3xxCodes`	The number of SIP messages with 3xx-level status codes.

Metric	Description
	Units: Count
`Sip4xxCodes`	The number of SIP messages with 4xx-level status codes. Units: Count
`Sip5xxCodes`	The number of SIP messages with 5xx-level status codes. Units: Count
`Sip6xxCodes`	The number of SIP messages with 6xx-level status codes. Units: Count
`CustomerToVcRtpPackets`	The number of RTP packets sent from the customer to the Amazon Chime Voice Connector infrastructure. Units: Count
`CustomerToVcRtpBytes`	The number of bytes sent from the customer to the Amazon Chime Voice Connector infrastructure in RTP packets. Units: Count
`CustomerToVcRtcpPackets`	The number of RTCP packets sent from the customer to the Amazon Chime Voice Connector infrastructure. Units: Count
`CustomerToVcRtcpBytes`	The number of bytes sent from the customer to the Amazon Chime Voice Connector infrastructure in RTCP packets. Units: Count
`CustomerToVcPacketsLost`	The number of packets lost in transit from the customer to the Amazon Chime Voice Connector infrastructure. Units: Count
`CustomerToVcJitter`	The average jitter for packets sent from the customer to the Amazon Chime Voice Connector infrastructure. Units: Microseconds
`VcToCustomerRtpPackets`	The number of RTP packets sent from the Amazon Chime Voice Connector infrastructure to the customer. Units: Count

Metric	Description
VcToCustomerRtpBytes	The number of bytes sent from the Amazon Chime Voice Connector infrastructure to the customer in RTP packets. Units: Count
VcToCustomerRtcpPackets	The number of RTCP packets sent from the Amazon Chime Voice Connector infrastructure to the customer. Units: Count
VcToCustomerRtcpBytes	The number of bytes sent from the Amazon Chime Voice Connector infrastructure to the customer in RTCP packets. Units: Count
VcToCustomerPacketsLost	The number of packets lost in transit from the Amazon Chime Voice Connector infrastructure to the customer. Units: Count
VcToCustomerJitter	The average jitter for packets sent from the Amazon Chime Voice Connector infrastructure to the customer. Units: Microseconds
RTTBetweenVcAndCustomer	The average round-trip time between the customer and the Amazon Chime Voice Connector infrastructure. Units: Microseconds
MOSBetweenVcAndCustomer	The estimated Mean opinion score (MOS) associated with voice streams between the customer and the Amazon Chime Voice Connector infrastructure. Units: Score between 1.0-4.4. A higher score indicates better perceived audio quality.
RemoteToVcRtpPackets	The number of RTP packets sent from the remote end to the Amazon Chime Voice Connector infrastructure. Units: Count
RemoteToVcRtpBytes	The number of bytes sent from the remote end to the Amazon Chime Voice Connector infrastructure in RTP packets. Units: Count

Metric	Description
RemoteToVcRtcpPackets	The number of RTCP packets sent from the remote end to the Amazon Chime Voice Connector infrastructure. Units: Count
RemoteToVcRtcpBytes	The number of bytes sent from the remote end to the Amazon Chime Voice Connector infrastructure in RTCP packets. Units: Count
RemoteToVcPacketsLost	The number of packets lost in transit from the remote end to the Amazon Chime Voice Connector infrastructure. Units: Count
RemoteToVcJitter	The average jitter for packets sent from the remote end to the Amazon Chime Voice Connector infrastructure. Units: Microseconds
VcToRemoteRtpPackets	The number of RTP packets sent from the Amazon Chime Voice Connector infrastructure to the remote end. Units: Count
VcToRemoteRtpBytes	The number of bytes sent from the Amazon Chime Voice Connector infrastructure to the remote end in RTP packets. Units: Count
VcToRemoteRtcpPackets	The number of RTCP packets sent from the Amazon Chime Voice Connector infrastructure to the remote end. Units: Count
VcToRemoteRtcpBytes	The number of bytes sent from the Amazon Chime Voice Connector infrastructure to the remote end in RTCP packets. Units: Count
VcToRemotePacketsLost	The number of packets lost in transit from the Amazon Chime Voice Connector infrastructure to the remote end. Units: Count

Metric	Description
VcToRemoteJitter	The average jitter for packets sent from the Amazon Chime Voice Connector infrastructure to the remote end. Units: Microseconds
RTTBetweenVcAndRemote	The average round-trip time between the remote end and the Amazon Chime Voice Connector infrastructure. Units: Microseconds
MOSBetweenVcAndRemote	The estimated Mean opinion score (MOS) associated with voice streams between the remote end and the Amazon Chime Voice Connector infrastructure. Units: Units: Score between 1.0-4.4. A higher score indicates better perceived audio quality.

CloudWatch dimensions for the Amazon Chime SDK

The CloudWatch dimensions that you can use with the Amazon Chime SDK are listed as follows.

Dimension	Description
VoiceConnectorId	The identifier of the Amazon Chime Voice Connector to display metrics for.
Region	The AWS Region associated with the event.

CloudWatch logs for the Amazon Chime SDK

You can send Amazon Chime Voice Connector metrics to CloudWatch Logs. For more information, see Editing Amazon Chime Voice Connector settings (p. 61).

Media quality metric logs

You can opt to receive media quality metric logs for your Amazon Chime Voice Connector. When you do, the Amazon Chime SDK sends detailed, per-minute metrics for all of your Amazon Chime Voice Connector calls to a CloudWatch Logs log group that is created for you. The log group name is `/aws/ChimeVoiceConnectorLogs/${VoiceConnectorID}`. The following fields are included in the logs, in JSON format.

Field	Description
voice_connector_id	The Amazon Chime Voice Connector ID carrying the call.
event_timestamp	The time when the metrics are emitted, in number of milliseconds since the UNIX epoch (midnight on January 1, 1970) in UTC.

Field	Description
call_id	Corresponds to the Transaction ID.
from_sip_user	The initiating user for the call.
from_country	The initiating country for the call.
to_sip_user	The receiving user for the call.
to_country	The receiving country for the call.
endpoint_id	An opaque identifier indicating the other endpoint of the call. Use with CloudWatch Logs Insights. For more information, see Analyzing log data with CloudWatch Logs Insights in the *Amazon CloudWatch Logs User Guide*.
aws_region	The AWS Region for the call.
cust2vc_rtp_packets	The number of RTP packets sent from the customer to the Amazon Chime Voice Connector infrastructure.
cust2vc_rtp_bytes	The number of bytes sent from the customer to the Amazon Chime Voice Connector infrastructure in RTP packets.
cust2vc_rtcp_packets	The number of RTCP packets sent from the customer to the Amazon Chime Voice Connector infrastructure.
cust2vc_rtcp_bytes	The number of bytes sent from the customer to the Amazon Chime Voice Connector infrastructure in RTCP packets.
cust2vc_packets_lost	The number of packets lost in transit from the customer to the Amazon Chime Voice Connector infrastructure.
cust2vc_jitter	The average jitter for packets sent from the customer to the Amazon Chime Voice Connector infrastructure.
vc2cust_rtp_packets	The number of RTP packets sent from the Amazon Chime Voice Connector infrastructure to the customer.
vc2cust_rtp_bytes	The number of bytes sent from the Amazon Chime Voice Connector infrastructure to the customer in RTP packets.
vc2cust_rtcp_packets	The number of RTCP packets sent from the Amazon Chime Voice Connector infrastructure to the customer.
vc2cust_rtcp_bytes	The number of bytes sent from the Amazon Chime Voice Connector infrastructure to the customer in RTCP packets.

Field	Description
vc2cust_packets_lost	The number of packets lost in transit from the Amazon Chime Voice Connector infrastructure to the customer.
vc2cust_jitter	The average jitter for packets sent from the Amazon Chime Voice Connector infrastructure to the customer.
rtt_btwn_vc_and_cust	The average round-trip time between the customer and the Amazon Chime Voice Connector infrastructure.
mos_btwn_vc_and_cust	The estimated Mean opinion score (MOS) associated with voice streams between the customer and the Amazon Chime Voice Connector infrastructure.
rem2vc_rtp_packets	The number of RTP packets sent from the remote end to the Amazon Chime Voice Connector infrastructure.
rem2vc_rtp_bytes	The number of bytes sent from the remote end to the Amazon Chime Voice Connector infrastructure in RTP packets.
rem2vc_rtcp_packets	The number of RTCP packets sent from the remote end to the Amazon Chime Voice Connector infrastructure.
rem2vc_rtcp_bytes	The number of bytes sent from the remote end to the Amazon Chime Voice Connector infrastructure in RTCP packets.
rem2vc_packets_lost	The number of packets lost in transit from the remote end to the Amazon Chime Voice Connector infrastructure.
rem2vc_jitter	The average jitter for packets sent from the remote end to the Amazon Chime Voice Connector infrastructure.
vc2rem_rtp_packets	The number of RTP packets sent from the Amazon Chime Voice Connector infrastructure to the remote end.
vc2rem_rtp_bytes	The number of bytes sent from the Amazon Chime Voice Connector infrastructure to the remote end in RTP packets.
vc2rem_rtcp_packets	The number of RTCP packets sent from the Amazon Chime Voice Connector infrastructure to the remote end.
vc2rem_rtcp_bytes	The number of bytes sent from the Amazon Chime Voice Connector infrastructure to the remote end in RTCP packets.

Field	Description
vc2rem_packets_lost	The number of packets lost in transit from the Amazon Chime Voice Connector infrastructure to the remote end.
vc2rem_jitter	The average jitter for packets sent from the Amazon Chime Voice Connector infrastructure to the remote end.
rtt_btwn_vc_and_rem	The average round-trip time between the remote end and the Amazon Chime Voice Connector infrastructure.
mos_btwn_vc_and_rem	The estimated Mean opinion score (MOS) associated with voice streams between the remote end and the Amazon Chime Voice Connector infrastructure.

SIP message logs

You can opt to receive SIP message logs for your Amazon Chime Voice Connector. When you do, the Amazon Chime SDK captures inbound and outbound SIP messages and sends them to a CloudWatch Logs log group that is created for you. The log group name is `/aws/ChimeVoiceConnectorSipMessages/${VoiceConnectorID}`. The following fields are included in the logs, in JSON format.

Field	Description
voice_connector_id	The Amazon Chime Voice Connector ID.
aws_region	The AWS Region associated with the event.
event_timestamp	The time when the message is captured, in number of milliseconds since the UNIX epoch (midnight on January 1, 1970) in UTC.
call_id	The Amazon Chime Voice Connector call ID.
sip_message	The full SIP message that is captured.

Automating the Amazon Chime SDK with EventBridge

Amazon EventBridge lets you automate your AWS services and respond automatically to system events, such as application availability issues or resource changes. For more information about the meeting events, see Meeting events in the *Amazon Chime SDK Developer Guide*.

When the Amazon Chime SDK generates events, it sends them to EventBridge for *best effort delivery*, meaning the Amazon Chime SDK tries to send all events to EventBridge, but in rare cases an event might not be delivered. For more information, refer to Events from AWS services in the *Amazon EventBridge User Guide*.

> **Note**
> If you need to encrypt data, you must use Amazon S3-Managed Keys. We don't support server-side encryption using Customer Master Keys stored in the AWS Key Management Service.

Automating Amazon Chime Voice Connectors with EventBridge

The actions that can be automatically triggered for Amazon Chime Voice Connectors include the following:

- Invoking an AWS Lambda function
- Launching an Amazon Elastic Container Service task
- Relaying the event to Amazon Kinesis Video Streams
- Activating an AWS Step Functions state machine
- Notifying an Amazon SNS topic or an Amazon SQS queue

Some examples of using EventBridge with Amazon Chime Voice Connectors include:

- Activating a Lambda function to download audio for a call after the call is ended.
- Launching an Amazon ECS task to enable real-time transcription after a call is started.

For more information, see the Amazon EventBridge User Guide.

Amazon Chime Voice Connector streaming events

Amazon Chime Voice Connectors support sending events to EventBridge when the events discussed in this section occur.

Amazon Chime Voice Connector streaming starts

Amazon Chime Voice Connectors send this event when media streaming to Kinesis Video Streams starts.

Example Event data

The following is example data for this event.


```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-111122223333",
    "detail-type": "Chime VoiceConnector Streaming Status",
    "source": "aws.chime",
    "account": "111122223333",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "callId": "1112-2222-4333",
        "direction": "Outbound",
        "fromNumber": "+12065550100",
        "inviteHeaders": {
            "from": "\"John\" <sip:+12065550100@10.24.34.0>;tag=abcdefg",
            "to": "<sip:
+13605550199@abcdef1ghij2klmno3pqr4.voiceconnector.chime.aws:5060>",
            "call-id": "1112-2222-4333",
            "cseq": "101 INVITE",
            "contact": "<sip:user@10.24.34.0:6090>;",
            "content-type": "application/sdp",
            "content-length": "246"
        },
        "isCaller": false,
        "mediaType": "audio/L16",
        "sdp": {
            "mediaIndex": 0,
```

```
            "mediaLabel": "1"
        },
        "siprecMetadata": "<&xml version=\"1.0\" encoding=\"UTF-8\"&>;\r\n<recording
 xmlns='urn:ietf:params:xml:ns:recording:1'>",
        "startFragmentNumber": "1234567899444",
        "startTime": "yyyy-mm-ddThh:mm:ssZ",
        "streamArn": "arn:aws:kinesisvideo:us-east-1:123456:stream/ChimeVoiceConnector-
abcdef1ghij2klmno3pqr4-111aaa-22bb-33cc-44dd-111222/111122223333",
        "toNumber": "+13605550199",
        "transactionId": "12345678-1234-1234",
        "voiceConnectorId": "abcdef1ghij2klmno3pqr4",
        "streamingStatus": "STARTED",
        "version": "0"
    }
}
```

Amazon Chime Voice Connector streaming ends

Amazon Chime Voice Connectors send this event when media streaming to Kinesis Video Streams ends.

Example Event data

The following is example data for this event.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-111122223333",
    "detail-type": "Chime VoiceConnector Streaming Status",
    "source": "aws.chime",
    "account": "111122223333",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "streamingStatus": "ENDED",
        "voiceConnectorId": "abcdef1ghij2klmno3pqr4",
        "transactionId": "12345678-1234-1234",
        "callId": "1112-2222-4333",
        "direction": "Inbound",
        "fromNumber": "+12065550100",
        "inviteHeaders": {
            "from": "\"John\" <sip:+12065550100@10.24.34.0>;tag=abcdefg",
            "to": "<sip:
+13605550199@abcdef1ghij2klmno3pqr4.voiceconnector.chime.aws:5060>",
            "call-id": "1112-2222-4333",
            "cseq": "101 INVITE",
            "contact": "<sip:user@10.24.34.0:6090>",
            "content-type": "application/sdp",
            "content-length": "246"
        },
        "isCaller": false,
        "mediaType": "audio/L16",
        "sdp": {
            "mediaIndex": 0,
            "mediaLabel": "1"
        },
        "siprecMetadata": "<&xml version=\"1.0\" encoding=\"UTF-8\"&>\r\n<recording
 xmlns='urn:ietf:params:xml:ns:recording:1'>",
        "startFragmentNumber": "1234567899444",
        "startTime": "yyyy-mm-ddThh:mm:ssZ",
        "endTime": "yyyy-mm-ddThh:mm:ssZ",
        "streamArn": "arn:aws:kinesisvideo:us-east-1:123456:stream/ChimeVoiceConnector-
abcdef1ghij2klmno3pqr4-111aaa-22bb-33cc-44dd-111222/111122223333",
        "toNumber": "+13605550199",
```

```
        "version": "0"
    }
}
```

Amazon Chime Voice Connector streaming updates

Amazon Chime Voice Connectors send this event when media streaming to Kinesis Video Streams is updated.

Example Event data

The following is example data for this event.

```
{
    "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"
    }
}
```

Amazon Chime Voice Connector streaming fails

Amazon Chime Voice Connectors send this event when media streaming to Kinesis Video Streams fails.

Example Event data

The following is example data for this event.

```
{
  "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"
    }
}
```

Logging Amazon Chime SDK API calls with AWS CloudTrail

The Amazon Chime SDK is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in the Amazon Chime SDK. CloudTrail captures all API calls for the Amazon Chime SDK as events, including calls from the Amazon Chime console and from code calls to the Amazon Chime SDK APIs. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for the Amazon Chime SDK. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to the Amazon Chime SDK, the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the AWS CloudTrail User Guide.

Amazon Chime SDK information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When API calls are made from the Amazon Chime administration console, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see Viewing events with CloudTrail event history.

For an ongoing record of events in your AWS account, including events for the Amazon Chime SDK, create a trail. A trail enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the : Event data collected in CloudTrail logs. For more information, see:

- Overview for creating a trail
- CloudTrail supported services and integrations
- Configuring Amazon SNS notifications for CloudTrail
- Receiving CloudTrail log files from multiple Regions and Receiving CloudTrail log files from multiple accounts

All Amazon Chime SDK actions are logged by CloudTrail and are documented in the *Amazon Chime SDK API Reference*. For example, calls to the `CreateAccount`, `InviteUsers` and `ResetPersonalPIN` sections generate entries in the CloudTrail log files. Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or IAM user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity element.

Understanding Amazon Chime SDK log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files are not an ordered stack trace of the public API calls, so they do not appear in any specific order.

Entries for the Amazon Chime SDK are identified by the **chime.amazonaws.com** event source.

If you have configured Active Directory for your Amazon Chime SDK account, see Logging AWS Directory Service API calls using CloudTrail. This describes how to monitor for issues that might affect your Amazon Chime SDK users' ability to sign in.

The following example shows a CloudTrail log entry for Amazon Chime SDK:

```
{"eventVersion":"1.05",
         "userIdentity":{
            "type":"IAMUser",
            "principalId":" AAAAAABBBBBBBBEXAMPLE",
            "arn":"arn:aws:iam::123456789012:user/Alice ",
            "accountId":"0123456789012",
            "accessKeyId":"AAAAAABBBBBBBBEXAMPLE",
            "sessionContext":{
               "attributes":{
                  "mfaAuthenticated":"false",
                  "creationDate":"2017-07-24T17:57:43Z"
               },
               "sessionIssuer":{
                  "type":"Role",
                  "principalId":"AAAAAABBBBBBBBEXAMPLE",
                  "arn":"arn:aws:iam::123456789012:role/Joe",
                  "accountId":"123456789012",
                  "userName":"Joe"
               }
            }
         } ,
         "eventTime":"2017-07-24T17:58:21Z",
         "eventSource":"chime.amazonaws.com",
         "eventName":"AddDomain",
         "awsRegion":"us-east-1",
         "sourceIPAddress":"72.21.198.64",
         "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/59.0.3071.115 Safari/537.36",
         "errorCode":"ConflictException",
         "errorMessage":"Request could not be completed due to a conflict",
         "requestParameters":{
            "domainName":"example.com",
            "accountId":"11aaaaaa1-1a11-1111-1a11-aaadd0a0aa00"
         },
         "responseElements":null,
         "requestID":"be1bee1d-1111-11e1-1eD1-0dc1111f1ac1",
         "eventID":"00fbeee1-123e-111e-93e3-11111bfbfcc1",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
```

Compliance validation for the Amazon Chime SDK

Third-party auditors assess the security and compliance of AWS services as part of multiple AWS compliance programs, such as SOC, PCI, FedRAMP, and HIPAA.

To learn whether or other AWS services are within the scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

Your compliance responsibility when using AWS services is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- Security and Compliance Quick Start Guides – These deployment guides discuss architectural considerations and provide steps for deploying baseline environments on AWS that are security and compliance focused.
- Architecting for HIPAA Security and Compliance on Amazon Web Services – This whitepaper describes how companies can use AWS to create HIPAA-eligible applications.

  Note
  Not all AWS services are HIPAA eligible. For more information, see the HIPAA Eligible Services Reference.
- AWS Compliance Resources – This collection of workbooks and guides might apply to your industry and location.
- Evaluating Resources with Rules in the *AWS Config Developer Guide* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- AWS Security Hub – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.
- AWS Audit Manager – This AWS service helps you continuously audit your AWS usage to simplify how you manage risk and compliance with regulations and industry standards.

Resilience in the Amazon Chime SDK

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

In addition to the AWS global infrastructure, the Amazon Chime SDK offers different features to help support your data resiliency and backup needs. For more information, see Managing Amazon Chime Voice Connector groups (p. 64) and Streaming Amazon Chime Voice Connector media to Kinesis (p. 66).

Infrastructure security in the Amazon Chime SDK

As a managed service, the Amazon Chime SDK is protected by the AWS global network security procedures that are described in the Amazon Web Services: Overview of Security Processes whitepaper.

For an overview of security in the Amazon Chime Software Development Kit (SDK), see Understanding Security in the Amazon Chime Application and SDK blog post. The post includes information on how AWS protects your data, plus the various meeting security features.

You use AWS published API calls to access the Amazon Chime SDK through the network. Clients must support Transport Layer Security (TLS) 1.0 or later. We recommend TLS 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.

Getting started

Setting up phone numbers for your Amazon Chime account

The following phone options are available for Amazon Chime administrative accounts:

Amazon Chime Voice Connector

Provides SIP trunking services for an existing phone system. Port in existing phone numbers or provision new phone numbers in the Amazon Chime console. That includes emergency numbers. For more information, see Managing Amazon Chime Voice Connectors (p. 60).

Amazon Chime SDK SIP media applications

Amazon Chime SDK SIP media applications make it easier and faster for you to create custom signaling and media instructions that you would normally build on your private branch telephone exchange (PBX).

Third-party emergency calling

Managing phone numbers in Amazon Chime SDK

Use the Amazon Chime console to provision phone numbers. Choose from Amazon Chime Voice Connector, or Amazon Chime SDK SIP media application phone numbers.

Amazon Chime Voice Connector

Provides Session Initiation Protocol (SIP) trunking services for existing phone systems. You can port existing phone numbers, or use the Amazon Chime console to provision new phone numbers. Use the Amazon Chime Voice Connector phone numbers for inbound or outbound calling, or both. For more information, see Managing Amazon Chime Voice Connectors (p. 60).

Note
The Amazon Chime SDK doesn't offer emergency calling services outside of the United States. To modify the emergency calling services that the Amazon Chime SDK provides for the United States, you can obtain an emergency call routing number from a third-party emergency service provider, give that number to the Amazon Chime SDK, and complete the configuration with Amazon Chime Voice Connectors. For more information, see Setting up emergency call routing numbers for your Amazon Chime Voice Connector (p. 62).

Amazon Chime SDK SIP media applications

Amazon Chime SDK SIP media applications make it easier and faster for you to create custom signaling and media instructions that you would normally build on your private branch telephone exchange (PBX).

Amazon Chime Voice Connectors, and Amazon Chime SDK SIP media applications have bandwidth requirements. For more information, see Bandwidth requirements (p. 80).

Contents

Provisioning phone numbers

Use the Amazon Chime console to provision phone numbers for your Amazon Chime SDK account. Choose from the following approaches:

- Amazon Chime Voice Connectors – Integrate with an existing phone system. For more information, see Managing Amazon Chime Voice Connectors (p. 60).
- Amazon Chime SDK SIP media applications – Integrate with Amazon Chime SDK meetings. For more information, see Managing SIP media applications and rules.

When provisioning completes, the phone numbers appear in your **Inventory**, and you can assign them to individual users. After you create an Amazon Chime Voice Connector, you can assign phone numbers to it as well. For more information, see Creating an Amazon Chime Voice Connector (p. 61).

To provision phone numbers

Important
You only follow these steps for countries that do not have identification requirements. For information about provisioning phone numbers in countries with identification requirements, see Requesting international phone numbers (p. 40).

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Phone number management**.
3. Choose **Orders**, **Provision phone numbers**.
4. Select **Voice Connector**, or **SIP Media Application Dial-In**, then choose **Next**.
5. Search for available phone numbers by country and other location options. Select the phone numbers that you want, then choose **Provision**.

The phone numbers appear in your **Orders** and **Pending** lists while the provisioning occurs.

Requesting international phone numbers

The steps in this section explain how to request international phone numbers for use with the Amazon Chime SDK. As you go, remember that you can only use international numbers with the SIP Media Application Dial-In product type.

To purchase international numbers, regulations in many countries require you to have:

- A local address
- Proof of your identity, from the Amazon Chime SDK or our carriers

Allow 2-6 weeks for the Amazon Chime SDK to fulfill your request. For more information about the documentation requirements for various countries, see the section called “Country requirements for phone numbers” (p. 41).

To request international phone numbers in countries with identification requirements

1. Do one of the following:
   - Open the Amazon Chime console and choose **Support**, then **Submit request**.
   - If you are an AWS Support customer, open the AWS Support Center page, sign in if necessary, and choose **Create case**, then **Technical support**. For **Service**, choose **Chime**.
2. For **Category**, choose **Other**.
3. For **Subject**, enter **Provisioning international numbers**.
4. For **Issue or Description**, enter the following:
   - Individual or Business
   - Name (Individual Name or Business Name)
   - Type of number (Local or Toll-Free)
   - Country
   - Quantity of phone numbers

5. Do one of the following:

   - If you submit a support request from the Amazon Chime console, for **Email**, enter the email address associated with your Amazon Chime administrator account, then choose **Submit request**.
   - If you create a case in the AWS Support Center, for **Attachments**, select **Choose files** and attach the required documents. For **Contact options**, select a contact method. Optionally, for **Additional contacts**, enter email addresses of people to be notified of case status updates.

   AWS Support responds to your support request to let you know whether the phone numbers can be provisioned. You receive responses from AWS Support in one of the following ways:

   - If you submitted a support request from the Amazon Chime console, AWS Support emails the Operations contact specified under **Alternate Contacts** in the contact information for your AWS account. For more information, see Editing contact information in the AWS Billing and Cost Management User Guide.
   - If you created a case in the AWS Support Center, you receive responses based on your selected contact methods and any email addresses you entered for additional contacts.

   Once the numbers are provisioned, you can view the numbers in the Amazon Chime console under **Calling, Phone number management, Inventory**.
6. Use SIP rules to assign the phone numbers to the appropriate SIP media application.

Country requirements for phone numbers

Outside the US, regulations often require a local address and specific identification documents in order to purchase and use a phone number. The address can be a business or personal address. The following tables list the countries that require identification. When you request international phone numbers (p. 40) or you port existing phone numbers (p. 52), the Amazon Chime SDK support works with you to submit the necessary documents.

> **Note**
> Make sure you provide the identities and addresses of the end-users who use your phone numbers.

Topics

- United Kingdom (p. 51)

Australia

The following tables list and describe the requirements for ordering and porting phone numbers in Australia.

Ordering phone numbers

Supported product types	Number types	ID requirements	Acceptable ID types
Amazon Chime SDK SDK SIP media application dial-in	Local	Yes	• Business address • Proof of location Business addresses must have the same geographic zone as their corresponding phone numbers.
	Toll-free	Yes	• Business address International addresses accepted.

Porting phone numbers

Supported product types	Number types	Required ID
SIP Media Application Dial-In	Local	• Last invoice from current provider • Letter of Authorization
	Toll-free	• Last invoice from current provider • Letter of Authorization

Austria

The following tables list and describe the requirements for ordering and porting phone numbers in Austria.

Ordering phone numbers

Supported product types	Number types	ID requirements	Acceptable ID types
SIP media application dial-in	Local	Yes	• Business address • Proof of telecom services such as

Supported product types	Number types	ID requirements	Acceptable ID types
			an Invoice from a network operator with another phone number in the same area. —OR— An invoice from an internet provider for Internet access with a fixed IP address located in the right area. Business addresses must have the same geographic zone as their corresponding phone numbers.
	National prefixes: +43 720	Yes	• Business address Address must be located in the country.
	Toll-free	Yes	• Business address Foreign address acceptable

Porting phone numbers

Supported product types	Number types	Required ID
SIP Media Application Dial-In	Local	• Last invoice from current provider • Letter of Authorization
	Toll-free	• Last invoice from current provider • Letter of Authorization

Canada

The following tables list and describe the requirements for ordering and porting phone numbers in Canada.

Ordering phone numbers

Supported product types	Number types	ID requirements	Acceptable ID types
SIP Media Application Dial-In	Local	No	N/A
Toll-free	No	N/A	N/A

Porting phone numbers

Supported product types	Number types	Required ID
SIP Media Application Dial-In	Local	• Last invoice from current provider • Letter of Authorization
	Toll-free	• Last invoice from current provider • Letter of Authorization

Denmark

The following tables list and describe the requirements for ordering and porting phone numbers in Denmark.

Ordering phone numbers

Supported product types	Number types	ID requirements	Acceptable ID types
SIP Media Application Dial-In	Local	No	N/A
	Toll-free	No	N/A

Porting phone numbers

Supported product types	Number types	Required ID
SIP Media Application Dial-In	Local	• Last invoice from current provider • Letter of Authorization
	Toll-free	• Last invoice from current provider • Letter of Authorization

Finland

The following tables list and describe the requirements for ordering and porting phone numbers in Finland.

Ordering phone numbers

Supported product types	Number types	ID requirements	Acceptable ID types
SIP Media Application Dial-In	Local	Yes	• Business address • Proof of location Business addresses must be located in the same geographic regions as their corresponding phone numbers.
	National prefixes +358 075	No	N/A
	Toll-free	No	N/A

Porting phone numbers

Supported product types	Number types	Required ID
SIP Media Application Dial-In	Local	• Last invoice from current provider • Letter of Authorization
	Toll-free	• Last invoice from current provider • Letter of Authorization

Germany

The following tables list and describe the requirements for ordering and porting phone numbers in Germany.

Ordering phone numbers

Supported product types	Number types	ID requirements	Acceptable ID types
SIP Media Application Dial-In	Local	Yes	• Business address • A copy of your business registration, or a copy of your ID, if you're an individual • Proof of address, such as a utility bill Business addresses must have the same

Supported product types	Number types	ID requirements	Acceptable ID types
			geographic zone as their corresponding phone numbers.
	National prefixes: +49 32	Yes	• Business address • A copy of your business registration, or a copy of your ID, if you're an individual • Proof of address, such as a utility bill Address must be located in the country.
	Toll-free	Yes	• Business address • Proof of address, such as a utility bill Address must be located in the country. You must first obtain the number directly from the local regulator. Details about the process are provided when you make the request.

Porting phone numbers

Supported product types	Number types	Required ID
SIP Media Application Dial-In	Local	• Last invoice from current provider • Letter of Authorization • Business address • A copy of your business registration • Copy of the company representative's ID Business addresses must have the same geographic zone as their corresponding phone numbers.
	Toll-free	• Last invoice from current provider

Supported product types	Number types	Required ID
		• Letter of Authorization • Number certificate from NRAs You must first obtain the number directly from the local regulator. Details about the process are provided when you make the request

Ireland

The following tables list and describe the requirements for ordering and porting phone numbers in Ireland.

Ordering phone numbers

Supported product types	Number types	ID requirements	Acceptable ID types
SIP Media Application Dial-In	Local	Yes	• Business address Business addresses must be located in the same geographic regions as their corresponding phone numbers.
	Universal access and VOIP prefixes: +353 0818, +353 076	Yes	• Business address Address must be located in the country.
	Toll-free	No	N/A

Porting phone numbers

Supported product types	Number types	Required ID
SIP Media Application Dial-In	Local	• Last invoice from current provider • Letter of Authorization
	Toll-free	• Last invoice from current provider • Letter of Authorization

Italy

The following tables list and describe the requirements for ordering and porting phone numbers in Italy.

Ordering phone numbers

Supported product types	Number types	ID requirements	Acceptable ID types
SIP Media Application Dial-In	Local	Yes	• Business address • Proof of location • Copy of business registration • Passport or end-user ID Business addresses must be located in the same geographic regions as their corresponding phone numbers.
	Toll-free	No	N/A

Porting phone numbers

Supported product types	Number types	Required ID
SIP Media Application Dial-In	Local	• Last invoice from current provider • Letter of Authorization • Copy of the company representative's passport or ID • Copy of the local business registration, or proof of address for an individual
	Toll-free	• Last invoice from current provider • Letter of Authorization

New Zealand

The following tables list and describe the requirements for ordering and porting phone numbers in New Zealand.

Ordering phone numbers

Supported product types	Number types	ID requirements	Acceptable ID types
SIP Media Application Dial-In	Local	No	N/A
	Toll-free	No	N/A

Porting phone numbers

Supported product types	Number types	Required ID
SIP Media Application Dial-In	Local	Not supported
	Toll-free	• Last invoice from current provider • Letter of Authorization

Nigeria

The following tables list and describe the requirements for ordering phone numbers in Nigeria.

Ordering phone numbers

Supported product types	Number types	ID requirements	Acceptable ID types
SIP Media Application Dial-In	Local	Yes	• Business address Foreign address acceptable.

Puerto Rico

The following tables list and describe the requirements for ordering and porting phone numbers in Puerto Rico.

Ordering phone numbers

Supported product types	Number types	ID requirements	Acceptable ID types
Business Calling Voice Connector	Local	No	N/A
Toll-free	No	N/A	N/A

South Korea

The following tables list and describe the requirements for ordering phone numbers in South Korea.

Ordering phone numbers

Supported product types	Number types	ID requirements	Acceptable ID types
SIP Media Application Dial-In	Toll-free	Yes	• Business address • Proof of location Address must be located in the country.

Sweden

The following tables list and describe the requirements for ordering and porting phone numbers in Sweden.

Ordering phone numbers

Supported product types	Number types	ID requirements	Acceptable ID types
SIP Media Application Dial-In	Local	No	N/A
	Toll-free	No	N/A

Porting phone numbers

Supported product types	Number types	Required ID
SIP Media Application Dial-In	Local	• Last invoice from current provider • Letter of Authorization
	Toll-free	• Last invoice from current provider • Letter of Authorization

Switzerland

The following tables list and describe the requirements for ordering and porting phone numbers in Switzerland.

Ordering phone numbers

Supported product types	Number types	ID requirements	Acceptable ID types
SIP Media Application Dial-In	Local	Yes	• Business address • Proof of location • A copy of business registration, or a copy

Supported product types	Number types	ID requirements	Acceptable ID types
			of your ID, if you're an individual Business addresses must have the same geographic zone as their corresponding phone numbers.
	Business number prefixes: +41 051, +41 058	Yes	• Business address Address must be located in the country.
	Toll-free	Yes	• Business address • A copy of business registration, or a copy of your ID, if you're an individual Foreign address acceptable

Porting phone numbers

Supported product types	Number types	Required ID
SIP Media Application Dial-In	Local	• Last invoice from current provider • Letter of Authorization • Business address Foreign addresses acceptable
	Toll-free	• Last invoice from current provider • Letter of Authorization • Business address • Certificate from NRAs Address must be within the country.

United Kingdom

The following tables list and describe the requirements for ordering and porting phone numbers in the United Kingdom.

Ordering phone numbers

Supported product types	Number types	ID requirements	Acceptable ID types
SIP Media Application Dial-In	Local	No	N/A
	Toll-free	No	N/A

Porting phone numbers

Supported product types	Number types	Required ID
SIP Media Application Dial-In	Local	• Last invoice from current provider • Letter of Authorization
	Toll-free	• Last invoice from current provider • Letter of Authorization

Porting existing phone numbers

In addition to provisioning phone numbers, you can also port numbers from your phone carrier into your Amazon Chime SDK inventory. You can use ported numbers with Amazon Chime Voice Connectors, and Amazon Chime SDK SIP media applications.

Before you can port phone numbers for Amazon Chime Voice Connectors, you must create one. For more information, see Creating an Amazon Chime Voice Connector (p. 61).

> **Note**
> You can port toll-free numbers for use with Amazon Chime Voice Connectors, and with Amazon Chime SDK SIP media applications.

Porting phone numbers into the Amazon Chime SDK

You create a support request to port existing phone numbers into the Amazon Chime SDK.

To port existing phone numbers into the Amazon Chime SDK

1. Do one of the following:
   - Open the Amazon Chime console at https://chime.aws.amazon.com/.
   - Choose **Support**, **Submit request**.
   - If you are an AWS Support customer, open the AWS Support Center page, sign in if necessary, and choose **Create case**. Choose **Technical support**. For **Service**, choose **Chime**.
2. For **Category**, choose **Other**.
3. For **Subject**, enter **`Porting phone numbers in`**.
4. For **Issue** or **Description**, enter the following:

   For porting U.S. numbers:

- Existing phone numbers to port in. Indicate the phone number type—**Voice Connector**, or **SIP Media Application Dial-In**.
- Billing Telephone Number (BTN) of the account.
- Authorizing person's name. This is the person in charge of account billing with the current carrier.
- Current carrier, if known.
- Service account number, if this information is present with the current carrier.
- Service PIN, if available.
- Service address and customer name, as they appear in your current carrier contract.
- Requested date and time for the port.
- (Optional) If you want to port your BTN, indicate one of the following options:
  - **I am porting my BTN and I want to replace it with a new BTN that I am providing. I can confirm that this new BTN is on the same account with the current carrier.**
  - **I am porting my BTN and I want to close out my account with my current carrier.**
  - **I am porting my BTN because my account is currently set up so that each phone number is its own BTN.** (Select this option only when your account with the current carrier is set up this way.)
  - After you choose one of the options listed above, download the Letter of Agency (LOA) form and fill it out. If you are porting phone numbers from different carriers, fill out a separate LOA for each carrier.

For porting international numbers:

- You must use the SIP Media Application Dial-In product type for non-US phone numbers.
- Type of number (Local or Toll-Free)
- Existing phone numbers to port in.
- Estimate usage volume
- Country
- You need to fill out the Letter of Agency document provided by AWS Support.
- See Country requirements for phone numbers (p. 41) for information about the documents required for porting in countries that support porting.

5. Do one of the following:

   - If you are submitting a support request from the Amazon Chime console, for **Email**, enter the email address associated with your Amazon Chime administrator account. Choose **Submit request**.
   - If you are creating a case in AWS Support Center **Contact options**, select a contact method. Optionally, for **Additional contacts**, enter email addresses of people to be notified of case status updates.

   AWS Support lets you know whether your phone numbers can be ported from your existing phone carrier. You receive responses from AWS Support in one of the following ways:

   - If you submitted a support request from the Amazon Chime console, AWS Support emails the **Operations** contact specified under **Alternate Contacts** in the **Contact Information** for your AWS account. For more information, see Editing contact information in the *AWS Billing User Guide*.
   - If you created a case in AWS Support Center, you receive responses based on your selected contact methods and any email addresses you entered for additional contacts.

6. To submit required documents please follow the below steps:

   Note
   AWS Support will provide a secure Amazon S3 link to upload all requested documents. Do not proceed until you have received the link.

a. Open the AWS Management Console at https://console.aws.amazon.com/.
b. After you are signed in to your AWS account, open the Amazon S3 upload link generated specifically for your account.

   Note
   The link expires after ten days. It is generated specifically for the account that created the case. The link requires an authorized user from the account to successfully perform the upload action.

c. Choose **Add Files**.
d. Select the identity documents related to your request.
e. Expand the **Permissions** section, and choose **Specify individual ACL permissions**.
f. Choose **Add grantee** at the end of the **Access control list (ACL)** section.
g. Paste the key provided by AWS Support into the **Grantee** text box.
h. Choose the **Read** checkbox under the **Objects** section of the page.
i. Choose **Upload**.

7. After you provide the Letter of Agency (LOA), AWS Support confirms with your existing phone carrier that the information on the LOA is correct. If the information provided on the LOA does not match the information that your phone carrier has on file, AWS Support contacts you to update the information provided on the LOA.
8. (Optional) View the status of your porting request in the Amazon Chime console under **Calling**, **Phone number management**, **Pending**. AWS Support also contacts you with updates and requests for further information, as needed. For more information, see Phone number porting status definitions (p. 55).
9. Assign the ported phone numbers.

   - Assign Amazon Chime Voice Connector numbers to your Voice Connectors.
   - For Amazon Chime SDK SIP Media Application Dial-In numbers, use SIP rules to assign numbers. For more information about SIP rules, refer to Creating SIP rules.

   The phone numbers are not activated for use until after the Firm Order Commit (FOC) date is established, as shown in the following steps. For more information, see Managing phone number inventory (p. 56) and Creating an Amazon Chime Voice Connector (p. 61).
10. After your existing phone carrier confirms that the LOA is correct, they review and approve the requested port. Then they provide AWS Support with a Firm Order Commit (FOC) date and time for the port to occur.
11. AWS Support contacts you with the FOC to confirm that the date and time works for you.

    Note
    The phone numbers cannot place or receive calls until you assign them.

12. On the FOC date, the ported phone numbers are activated for use with the Amazon Chime SDK.

Porting phone numbers out of the Amazon Chime SDK

Note
The ability to port numbers out of the Amazon Chime SDK depends on the receiving carrier's ability to accept those numbers.

To port existing phone numbers out of the Amazon Chime SDK

1. Do one of the following:

- Open the Amazon Chime console at https://chime.aws.amazon.com/.

  Choose **Support**, **Submit request**.
- If you are an AWS Support customer, open the AWS Support Center page, sign in if necessary, and choose **Create case**. Choose **Technical support**. For **Service**, choose **Chime**.

2. For **Category**, choose **Other**.
3. For **Subject**, enter **`Porting phone numbers out`**.
4. For **Issue** or **Description**, enter the phone numbers to port out. Indicate the phone number type **Voice Connector**, or **SIP Media Application Dial-In**.
5. Do one of the following:

   - If you are submitting a support request from the Amazon Chime console, for **Email**, enter the email address associated with your Amazon Chime administrator account. Choose **Submit request**.
   - If you are creating a case in AWS Support Center for **Contact options**, select a contact method. Optionally, for **Additional contacts**, enter email addresses of people to be notified of case status updates.

AWS Support responds with an account ID and PIN to use when requesting the port from your new carrier. You receive responses from AWS Support in one of the following ways:

- If you submitted a support request from the Amazon Chime console, AWS Support emails the **Operations** contact specified under **Alternate Contacts** in the **Contact Information** for your AWS account. For more information, see Editing contact information in the *AWS Billing User Guide*.
- If you created a case in AWS Support Center, you receive responses based on your selected contact methods and any email addresses you entered for additional contacts.

When the porting process is complete and the phone numbers are ported to your new carrier, unassign and delete the phone numbers from your Amazon Chime SDK inventory. For more information, see Managing phone number inventory (p. 56) and Deleting phone numbers (p. 58).

Phone number porting status definitions

After you submit a request to port existing phone numbers into the Amazon Chime SDK, you can view the status of your porting request in the Amazon Chime console under **Calling**, **Phone number management**, **Pending**.

Porting statuses and definitions include the following:

CANCELLED

AWS Support cancelled the porting order because of an issue with the port, such as a cancellation request from the carrier or from you. AWS Support contacts you with details.

CANCEL_REQUESTED

AWS Support is processing a cancellation of the porting order because of an issue with the port, such as a cancellation request from the carrier or from you. AWS Support contacts you with details.

CHANGE_REQUESTED

AWS Support is processing your change request, and the carrier response is pending. Allow for additional processing time.

COMPLETED

Your porting order is completed, and your phone numbers are activated.

EXCEPTION

AWS Support contacts you for additional details needed to complete the port request. Allow for additional processing time.

FOC

The FOC date is confirmed with the carrier. AWS Support contacts you to confirm the date.

PENDING DOCUMENTS

AWS Support contacts you for additional documents needed to complete the port request. Allow for additional processing time.

SUBMITTED

Your porting order is submitted, and the carrier response is pending.

Managing phone number inventory

Use the phone number management **Inventory** page to assign or unassign phone numbers. You can do this with phone numbers for Amazon Chime Voice Connectors or Amazon Chime Voice Connector groups.

Manage Amazon Chime Voice Connector phone numbers on the corresponding **Voice connectors** or **Voice connector groups** page. For more information, see Assigning and unassigning phone numbers for an Amazon Chime Voice Connector group (p. 66).

When you change a user's Amazon Chime Business Calling phone number or phone number permissions, we recommend providing the user with their new phone number or permissions information. Before users can access their new phone number or permissions features, they must sign out of their Amazon Chime account and sign in again.

To assign Amazon Chime Voice Connector phone numbers to an Amazon Chime Voice Connector or Amazon Chime Voice Connector group

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Phone number management**.
3. Choose **Inventory**, and select the phone numbers that you want to assign.
4. For **Assignment type**, choose **Voice connector** or **Voice connector group**.
5. Choose **Assign**.
6. Select the Amazon Chime Voice Connector to assign the phone number to, and choose **Assign**.

You can also choose **Reassign** to reassign phone numbers with the **Voice Connector** product type. This lets you reassign these numbers from one Amazon Chime Voice Connector or Amazon Chime Voice Connector group to another.

To assign an Amazon Chime SDK SIP Media Application Dial-In phone number to a SIP Media Application

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. In the navigation pane, choose **SIP media applications**, locate the SIP application for which you want to create a rule, then copy its phone number. Paste the number into Notepad or a similar program. Keep that program open for later use. This keeps the number available for use later in these steps.
3. In the navigation pane, choose **SIP rules**. The **SIP rules** page appears.
4. Choose **Create**. The **Create a SIP rule** dialog box appears.

5. For **Name**, enter a name for the rule, then create the rule:
   - By default, the **Trigger type** list displays **To phone number**. If it doesn't, open the list and select that value.
   - For **Phone number**, enter a phone number or choose one from the list. If you enter a number, use this format: **+1***ten-digit number*. For example: +15095551212.
6. To use the rule immediately, leave the **Enabled** check box selected. To disable the rule, clear the check box.
7. Choose **Next**, and on the **Step 2** page, open the **SIP media application** list and select the SIP application that you want to use.
8. As needed, choose **Add a SIP media application** to use the rule with multiple applications, then choose **Create**.

A success message appears. If an error message appears, follow its instructions.

The following procedure unassigns phone numbers from Amazon Chime Voice Connectors.

To unassign inventory phone numbers for Amazon Chime Voice Connector

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Phone number management**.
3. Choose I**nventory**, and select the phone number to unassign.
4. Choose **Unassign**.
5. Select the check box, and choose **Unassign**.

To unassign inventory phone numbers for SIP Media Application

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. In the navigation pane, choose **SIP rules**. The **SIP rules** page appears.
3. Choose the option button next to the name of the rule that you want to unassign.
4. Open the **Actions** list and choose **Delete**. The **Delete rule(s)** dialog box appears.
5. Select **I understand that this action cannot be reversed**, then choose **Delete**.

You can also view the details of your inventory phone numbers. For example, you can see which Voice Connector, or Amazon Chime SDK SIP Media Application that a number is assigned to. You can also see if phone calls and text messages are enabled.

To view inventory phone number details

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Phone number management**.
3. Choose **Inventory**, and select the phone number that you want to view.
4. For **Actions**, choose **View details**.

If you have unassigned Amazon Chime Voice Connector, or Amazon Chime SDK SIP media application phone numbers, you can switch them from one product type to another.

> **Note**
> For non-US numbers, you must use the SIP Media Application Dial-In product type.

To edit product types

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.

2. For **Calling**, choose **Phone number management**.
3. Choose **Inventory**, and select the phone number or numbers that you want to change.
4. Select **Business Calling**, **Voice Connector**, or **SIP Media Application Dial-In** and choose **Save**.

Updating outbound calling names

Set a default calling name that appears to recipients of outbound calls made using the phone numbers in your **Inventory**. Default calling names apply to all phone number product types. You can update the names once every seven days.

> **Note**
> When you place a call using an Amazon Chime Voice Connector, the call is routed through the public switched telephone network (PSTN) to a fixed or mobile telephone carrier of the called party. Not all fixed and mobile telephone carriers support Caller ID names (CNAM) or use the same CNAM database as Amazon Chime Voice Connectors. Even though you set your caller ID name in the Amazon Chime console, the called party might see no calling name at all, or they might see a calling name that is different from the value that you set.

To set a default calling name

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Phone number management**.
3. Choose **Inventory**.
4. For **Actions**, choose **Update default calling name**.
5. For **Default calling name**, enter a default calling name of up to 15 characters.
6. Choose **Save**.

Allow 72 hours for the system to update the default calling name.

Set a unique calling name for individual phone numbers on the phone number details screen.

To set a unique calling name

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Phone number management**.
3. Choose **Inventory**.
4. Select the phone number to update.
5. For **Actions**, choose **View details**.
6. On the phone number details screen, for **Actions**, choose **Update unique calling name**.
7. For **Unique calling name**, enter a unique calling name of up to 15 characters.
8. Choose **Save**.

The system updates the unique calling name within 72 hours. After the update finishes, you can update the calling name again.

Deleting phone numbers

You can delete unassigned phone numbers from your phone number management inventory. For more information about unassigning phone numbers, see Managing phone number inventory (p. 56).

To delete unassigned phone numbers

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Phone number management**.
3. Choose **Inventory**, and select the phone number or numbers to delete.
4. For **Actions**, choose **Delete phone number(s)**.
5. Select the check box, and choose **Delete**.

Deleted phone numbers are held in the **Deletion queue** for 7 days before they are deleted permanently.

Restoring deleted phone numbers

You can restore deleted phone numbers from the **Deletion queue** for up to 7 days after they are deleted. Restoring a phone number moves it back into your **Inventory**.

To restore deleted phone numbers

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Phone number management**.
3. Choose **Deletion queue**, and select the phone number or numbers to restore.
4. Choose **Move to inventory**.

Managing Amazon Chime Voice Connectors

What is an Amazon Chime Voice Connector?

An Amazon Chime Voice Connector provides Session Initiation Protocol (SIP) trunking service for your existing phone system. You can manage your Amazon Chime Voice Connector from the Amazon Chime console, and access it over your internet connection or with AWS Direct Connect. For more information, see What is AWS Direct Connect? in the *AWS Direct Connect User Guide*.

Amazon Chime Voice Connector outbound and inbound calling

After you create an Amazon Chime Voice Connector, edit the termination and origination settings to allow outbound or inbound calls, or both. Then, assign phone numbers to the Amazon Chime Voice Connector. You can port in existing phone numbers or provision new phone numbers in the Amazon Chime console. For more information, see Porting existing phone numbers (p. 52), Provisioning phone numbers (p. 39), and Assigning and unassigning Amazon Chime Voice Connector phone numbers (p. 63).

> **Note**
> Amazon Chime Voice Connectors support outbound calling in E.164 format and do not require an international dialing access code, such as 011. You pay a per-minute rate based on the destination country of the call. For a current list of supported countries, and the per-minute rate for each country, see https://aws.amazon.com/chime/voice-connector/pricing/.

Amazon Chime Voice Connector groups

You can also create an Amazon Chime Voice Connector group and add Amazon Chime Voice Connectors to it that are created in different AWS Regions. This creates a fault-tolerant mechanism for fallback if availability events occur. For more information, see Managing Amazon Chime Voice Connector groups (p. 64).

Logging and monitoring Amazon Chime Voice Connector data

Optionally, you can send logs from your Amazon Chime Voice Connector to CloudWatch Logs, and turn on media streaming from your Amazon Chime Voice Connector to Amazon Kinesis. For more information, see CloudWatch logs for the Amazon Chime SDK (p. 27) and Streaming Amazon Chime Voice Connector media to Kinesis (p. 66).

Contents

Before you begin

To use an Amazon Chime Voice Connector, you must have an IP Private Branch Exchange (PBX), Session Border Controller (SBC), or other voice infrastructure with internet access that supports Session Initiation

Protocol (SIP). Make sure that you have enough bandwidth to support peak call volume. For information about bandwidth requirements, see Bandwidth requirements (p. 80).

To ensure security for calls sent from AWS to your on-premises phone system, we recommend configuring an SBC between AWS and your phone system. Allowlist SIP traffic to the SBC from the Amazon Chime Voice Connector signaling and media IP addresses. For more information, see the recommended ports and protocols for Amazon Chime Voice Connector (p. 79).

Amazon Chime Voice Connectors expect phone numbers to be in E.164 format.

Creating an Amazon Chime Voice Connector

Create an Amazon Chime Voice Connector from the Amazon Chime console.

To create an Amazon Chime Voice Connector

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Voice connectors**.
3. Choose **Create new voice connector**.
4. For **Voice connector name**, enter a name for the Amazon Chime Voice Connector.
5. (Optional) For **AWS Region**, choose an AWS Region for your Amazon Chime Voice Connector. The default Region is US East (N. Virginia) (**us-east-1**). Regions cannot be changed after your Amazon Chime Voice Connector is created.
6. For **Encryption**, select **Enabled** or **Disabled**.
7. Choose **Create**.

> **Note**
> Enabling encryption configures your Amazon Chime Voice Connector to use TLS transport for SIP signaling and Secure RTP (SRTP) for media. Inbound calls use TLS transport, and unencrypted outbound calls are blocked.

Editing Amazon Chime Voice Connector settings

To finish setting up your Amazon Chime Voice Connector, edit the settings from the Amazon Chime console. Edit the termination and origination settings to allow outbound or inbound calls, or both.

Termination settings

Termination settings apply to outbound calls from your Amazon Chime Voice Connector. Set up your calling plan and caller ID options here. You can also specify the IP addresses allowed to make outbound calls using your Amazon Chime Voice Connector, and require credentials for making outbound calls to your Amazon Chime Voice Connector. If you don't specify credentials, no authentication is required.

> **Note**
> Your Outbound host name resolves to a set of IP addresses that may change as EC2 instances go in or out of service, so don’t cache records for longer than the DNS Time to Live interval. Caching for longer may result in call failures.

Origination settings

Origination settings apply to inbound calls to your Amazon Chime Voice Connector. Here, configure inbound routes for your SIP hosts to receive inbound calls. Inbound calls are routed to hosts in your SIP

infrastructure by the priority and weight you set for each host. Calls are routed in priority order first, with 1 the highest priority. If hosts are equal in priority, calls are distributed among them based on their relative weight.

Note
Encryption-enabled Voice Connectors use TLS (TCP) protocol for all calls.

To edit Amazon Chime Voice Connector settings

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Voice connectors**.
3. Choose the name of the Amazon Chime Voice Connector to edit.
4. Edit your settings as follows:
    1. (Optional) Choose **General** to update the **Voice connector name**, and enable or disable encryption.
    2. Choose **Termination**, and select **Enabled**.
    3. (Optional) For **Allowlist**, choose **New**, enter the CIDR notations and values to allowlist, and choose **Add**.
    4. For **Calling plan**, select the country or countries to add to your calling plan.
    5. (Optional) For **Credentials**, choose **New**, enter a user name and password, and choose **Save**. Your credentials are updated immediately.
    6. (Optional) For **Caller ID**, choose **Edit**, select a caller ID phone number, and choose **Save**.
    7. Choose **Save** again.
    8. Choose **Origination**, and select **Enabled**.
    9. For **Inbound routes**, choose **New**.
    10. Enter the values for **Host**, **Port**, **Protocol**, **Priority**, and **Weight**.
    11. Choose **Add**.
    12. Choose **Save**.
    13. (Optional) For **Emergency calling**, choose **Add** to add emergency call routing numbers that you have obtained from a third-party emergency service provider. For more information, see Setting up emergency call routing numbers for your Amazon Chime Voice Connector (p. 62).
    14. (Optional) For **Streaming**, choose **Start** to send audio to a Kinesis Video Stream, then choose **Save**.
    15. Choose **Phone numbers**.
    16. Select one or more phone numbers to assign to the Amazon Chime Voice Connector.
    17. Choose **Assign**.
    18. (Optional) For **Logging**, choose **Enabled** to send logs to CloudWatch Logs, then choose **Save**.

For more information about assigning phone numbers to an Amazon Chime Voice Connector, see Assigning and unassigning Amazon Chime Voice Connector phone numbers (p. 63).

Setting up emergency call routing numbers for your Amazon Chime Voice Connector

The Amazon Chime SDK offers emergency calling services for users in the United States.

If you want to modify the emergency calling services offered with Amazon Chime Business Calling for the United States, you can obtain an emergency call routing number from a third-party emergency service provider and provide it to Amazon Chime. After setup, when you place a call to emergency services (such as a 911 call), Amazon Chime will use your emergency call routing number to route your

call to your emergency services provider via the public switched telephone network. Your third-party emergency service provider then routes your call to emergency services.

> **Note**
> Amazon Chime Business Calling supports emergency calling for the United States. You can also use your own provider and set up an Amazon Chime Voice Connector for emergency calls. Your provider should give you a United States emergency number.

Setting up emergency call routing numbers outside the United States requires that you perform the following prerequisites:

- Obtain emergency call routing numbers from a third-party emergency service provider. Ensure they're US numbers.
- Turn on and configure termination and origination settings for an Amazon Chime Voice Connector. For more information, see Editing Amazon Chime Voice Connector settings (p. 61).

To set up emergency call routing numbers for your Amazon Chime Voice Connector

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Voice connectors**.
3. Choose the name of the Amazon Chime Voice Connector.
4. Choose **Emergency calling**.
5. Choose **Add**.
6. For **Call send method**, choose **DNIS** (Dialed Number Identification Service).
7. For **Emergency call routing number for calling emergency services**, enter the third-party phone number for calling emergency services, in E.164 format.
8. For **Test routing number for testing calls to emergency services**, enter the third-party phone number for testing calls to emergency services, in E.164 format.
9. For **Country**, select **United States**.
10. Choose **Add**.

Assigning and unassigning Amazon Chime Voice Connector phone numbers

You can assign phone numbers to an Amazon Chime Voice Connector.

To assign phone numbers to an Amazon Chime Voice Connector

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Voice connectors**.
3. Choose the name of the Amazon Chime Voice Connector.
4. Choose **Phone numbers**.
5. Select one or more phone numbers to assign to the Amazon Chime Voice Connector.
6. Choose **Assign**.

You can also choose **Reassign** to reassign phone numbers with the **Voice Connector** product type from one Amazon Chime Voice Connector or Amazon Chime Voice Connector group to another.

To unassign phone numbers from an Amazon Chime Voice Connector

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Voice connectors**.
3. Choose the name of the Amazon Chime Voice Connector.
4. Choose **Phone numbers**.
5. Select one or more phone numbers to unassign from the Amazon Chime Voice Connector.
6. Select **Unassign**.
7. Select the check box, and choose **Unassign**.

Deleting an Amazon Chime Voice Connector

Before you can delete an Amazon Chime Voice Connector, you must unassign all phone numbers from it. For more information on unassigning phone numbers from an Amazon Chime Voice Connector, see the previous topic.

To delete an Amazon Chime Voice Connector

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Voice connectors**.
3. Choose **Phone numbers**, **Delete voice connector**.
4. Select the check box, and choose **Delete**.

Managing Amazon Chime Voice Connector groups

How an Amazon Chime Voice Connector group works

You can create an Amazon Chime Voice Connector group and add Amazon Chime Voice Connectors to it that are created in different AWS Regions. This allows incoming calls to fail over across Regions, which creates a fault-tolerant mechanism for fallback in case of availability events.

For example, an Amazon Chime Voice Connector group is created with two Amazon Chime Voice Connectors assigned to it. One Amazon Chime Voice Connector is in the US East (N. Virginia) Region, and the other Amazon Chime Voice Connector is in the US West (Oregon) Region.

An incoming call is placed to a phone number associated with the Amazon Chime Voice Connector in the US East (N. Virginia) Region. However, there is a connectivity issue in that Region, so the call is then routed through the US West (Oregon) Region.

Get started with an Amazon Chime Voice Connector group

To get started, first create Amazon Chime Voice Connectors in different AWS Regions. Then, create an Amazon Chime Voice Connector group and assign the Amazon Chime Voice Connectors to it. You can also provision phone numbers for your Amazon Chime Voice Connector group from your Amazon Chime SDK **Phone number management** inventory. For more information, see Provisioning phone numbers (p. 39). For more information about creating Amazon Chime Voice Connectors in different AWS Regions, see Managing Amazon Chime Voice Connectors (p. 60).

Contents

- Assigning and unassigning phone numbers for an Amazon Chime Voice Connector group (p. 66)
- Deleting an Amazon Chime Voice Connector group (p. 66)

Creating an Amazon Chime Voice Connector group

You can create up to three Amazon Chime Voice Connector groups for your account.

To create an Amazon Chime Voice Connector group

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Voice connector groups**.
3. Choose **Create group**.
4. For **Voice connector group name**, enter a name for the group.
5. Choose **Create**.

Editing an Amazon Chime Voice Connector group

After you create an Amazon Chime Voice Connector group, you can add or remove Amazon Chime Voice Connectors for it. You can also edit the priority for the Amazon Chime Voice Connectors in the group.

To add Amazon Chime Voice Connectors to a group

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Voice connector groups**.
3. Choose the name of the Amazon Chime Voice Connector group to edit.
4. For **Actions**, choose **Add**.
5. For **Choose voice connectors**, select the Amazon Chime Voice Connectors to add to the group.
6. Choose **Add**.

To edit Amazon Chime Voice Connector priority in a group

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Voice connector groups**.
3. Choose the name of the Amazon Chime Voice Connector group to edit.
4. For **Actions**, choose **Edit priority**.
5. For **Edit voice connector priority ranking**, enter a different priority ranking for each Amazon Chime Voice Connector. 1 is the highest priority. Higher priority Amazon Chime Voice Connectors are attempted first.
6. Choose **Save**.

To remove Amazon Chime Voice Connectors from a group

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Voice connector groups**.
3. Choose the name of the Amazon Chime Voice Connector group to edit.
4. For **Actions**, choose **Remove**.
5. For **Choose voice connectors**, select the Amazon Chime Voice Connectors to remove.
6. Choose **Remove**.

Assigning and unassigning phone numbers for an Amazon Chime Voice Connector group

You can assign and unassign phone numbers for an Amazon Chime Voice Connector group in the Amazon Chime console.

To assign phone numbers to an Amazon Chime Voice Connector group

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Voice connector groups**.
3. Choose the name of the Amazon Chime Voice Connector group to edit.
4. Choose **Phone numbers**.
5. Choose **Assign from inventory**.
6. Select one or more phone numbers to assign to the Amazon Chime Voice Connector group.
7. Choose **Assign from inventory**.

You can also choose **Reassign** to reassign phone numbers with the **Voice Connector** product type. This lets you reassign these numbers from one Amazon Chime Voice Connector or Amazon Chime Voice Connector group to another.

To unassign phone numbers from an Amazon Chime Voice Connector group

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Voice connector groups**.
3. Choose the name of the Amazon Chime Voice Connector group to edit.
4. Choose **Phone numbers**.
5. Select the phone numbers that you want from the Amazon Chime Voice Connector group, and choose **Unassign**.
6. Choose **Unassign**.

Deleting an Amazon Chime Voice Connector group

Before you can delete an Amazon Chime Voice Connector group, you must unassign all Amazon Chime Voice Connectors and phone numbers from it. For more information, see the previous section.

To delete an Amazon Chime Voice Connector group

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Voice connector groups**.
3. Choose the name of the Amazon Chime Voice Connector group to delete.
4. Choose **Delete group**.
5. Select the check box, and choose **Delete**.

Streaming Amazon Chime Voice Connector media to Kinesis

You can stream phone call audio from Amazon Chime Voice Connectors to Amazon Kinesis Video Streams for analytics, machine learning, and other processing. Developers can store and encrypt audio

data in Kinesis Video Streams, and access the data using the Kinesis Video Streams API operation. For more information, see the *Kinesis Video Streams Developer Guide*.

Use the Amazon Chime console to start media streaming for your Amazon Chime Voice Connector. When media streaming is started, your Amazon Chime Voice Connector uses an AWS Identity and Access Management (IAM) service-linked role to grant permissions to stream media to Kinesis Video Streams. Then, call audio from each Amazon Chime Voice Connector telephone call leg is streamed in real time to separate Kinesis Video Streams.

Use the Kinesis Video Streams Parser Library to download the media streams sent from your Amazon Chime Voice Connector. Filter the streams by the following persistent fragments metadata:

- TransactionId
- VoiceConnectorId

For more information, see Kinesis Video Streams Parser Library and Using streaming metadata with Kinesis Video Streams in the *Amazon Kinesis Video Streams Developer Guide*.

For more information about using IAM service-linked roles with Amazon Chime Voice Connectors, see Using the Amazon Chime Voice Connector service-linked role (p. 16). For more information about using Amazon CloudWatch with the Amazon Chime SDK, see Logging and monitoring in the Amazon Chime SDK (p. 22).

When you enable media streaming for your Amazon Chime Voice Connector, the Amazon Chime SDK creates an IAM service-linked role called AWSServiceRoleForAmazonChimeVoiceConnector. If you have configured call detail record logging for Amazon Chime Voice Connectors in the Amazon Chime console, streaming detail records are sent to your configured Amazon S3 bucket. For more information, see Amazon Chime Voice Connector streaming detail records (p. 77).

Starting media streaming

Start media streaming for your Amazon Chime Voice Connector from the Amazon Chime console.

To start media streaming for your Amazon Chime Voice Connector

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Voice connectors**.
3. Choose the name of the Amazon Chime Voice Connector.
4. Choose **Streaming**.
5. For **Sending to Kinesis Video Streams**, choose **Start**.
6. Select a **Data retention period**.
7. Choose **Save**.

Turn off media streaming from the Amazon Chime console. If you no longer need to use media streaming for any of your Amazon Chime Voice Connectors, we recommend that you also delete the related service-linked role. For more information, see Deleting a service-linked role for Amazon Chime Voice Connectors (p. 17).

To stop media streaming for your Amazon Chime Voice Connector

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Calling**, choose **Voice connectors**.
3. Choose the name of the Amazon Chime Voice Connector.
4. Choose **Streaming**.

5. For **Sending to Kinesis Video Streams**, choose **Stop**.
6. Choose **Save**.

SIP-based media recording (SIPREC) and network-based recording (NBR) compatibility

You can use an Amazon Chime Voice Connector to stream media to Kinesis Video Streams. You can stream from a SIPREC-compatible voice infrastructure or the NBR feature associated with Cisco Unified Border Element (CUBE).

You must have a Private Branch Exchange (PBX), Session Border Controller (SBC), or contact center that supports the SIPREC protocol or NBR feature. The PBX or SBC must be able to send signaling and media to AWS public IP addresses. For more information, see Before you begin (p. 60).

To set up streaming of RTP audio streams forked with SIPREC or NBR

1. Create an Amazon Chime Voice Connector. For more information, see Creating an Amazon Chime Voice Connector (p. 61).
2. Start media streaming for your Amazon Chime Voice Connector. For more information, see Starting media streaming (p. 67).
3. In the Amazon Chime console, under **Voice connectors**, view the **Outbound host name** for your Amazon Chime Voice Connector. For example, *abcdef1ghij2klmno3pqr4*`.voiceconnector.chime.aws`.
4. Do one of the following:

   - **For SIPREC** – Configure your PBX, SBC, or other voice infrastructure to fork RTP streams with SIPREC to the **Outbound host name** of your Amazon Chime Voice Connector.
   - **For NBR** – Configure your PBX, SBC, or other voice infrastructure to fork RTP streams with NBR to the **Outbound host name** of your Amazon Chime Voice Connector. Send an additional header or URI parameter of `X-Voice-Connector-Record-Only` with the value `true` in the `SIP INVITE`.

Managing SIP media applications and rules

You can use the Amazon Chime console to create Session Initiation Protocol (SIP) media applications. SIP media applications make it easier and faster for you to create custom signaling and media instructions that you would normally build on your private branch telephone exchange (PBX).

SIP rules specify how a SIP media application can connect to an Amazon Chime SDK meeting. Calls can go to and from private phone numbers that you own or to and from a Request URI hostname, the name assigned to an Amazon Chime Voice Connector. The Amazon Chime SDK runs the SIP rules when a user places or receives a call.

You must be an AWS Lambda user before you can create SIP media applications. The SIP media applications use Lambda functions for the following reasons:

- You can write complex logic that involves decision-making. For example, a caller can use a touchtone phone to dial in to a meeting. In turn, that phone number triggers Lambda functions that ask for a meeting PIN and route the caller to the correct meeting.
- You can deploy Lambda functions without a server infrastructure.

For more information about AWS Lambda, see Getting started with AWS Lambda.

To create SIP rules, you need private phone numbers or at least one Request URI hostname. For more information about phone numbers, see Managing phone numbers. For more information about Request URI hostnames, see Creating a SIP rule (p. 72).

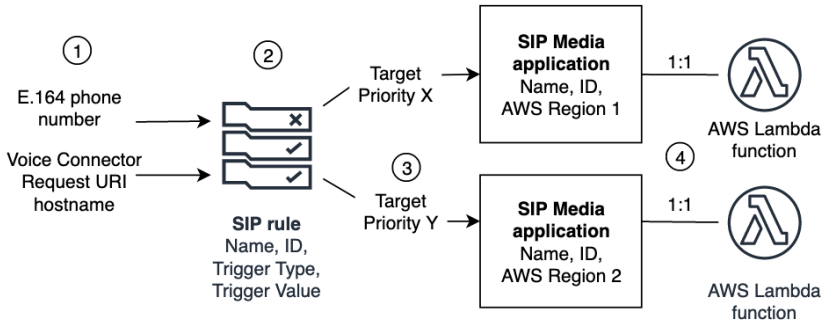
Topics

Understanding SIP rules and applications

To use the Session Initiation Protocol (SIP) with the Amazon Chime SDK, you create SIP rules and SIP media applications. You create both in the Amazon Chime console.

The following diagram shows how the rules and applications work. It shows how SIP rules can route calls from phone numbers and Request URI hostnames to different SIP applications.

Numbers in the image correspond to numbers in the text below the image.



You can only assign phone numbers from your Chime inventory and Amazon Chime Voice Connectors (1) to SIP rules (2). Also, you must provision a phone number or Voice Connector in your PSTN Audio service. Upon receiving a call to a phone number, the SIP rule invokes a SIP media application and its associated Lambda function (4). The Lambda function runs code that invokes actions, such as playing on-hold music or joining a meeting, or muting a call. To provide multi-region resiliency, SIP rules (2) can specify alternate target SIP media applications in different AWS regions (3) by order of priority for failover. If one target fails, the PSTN Audio service tries the next one and so on. Note that each alternate target must reside in a different AWS Region.

Using SIP media applications

A SIP media application is a managed object that passes values from a SIP rule to a target AWS Lambda function. You can create, view, update, and delete SIP media applications. Be aware that you can view the details of any application, and other administrators can view your applications.

> **Note**
> You need an AWS Lambda function before you can create a SIP media application. For more information, see Getting started with AWS Lambda.

Topics

Creating a SIP media application

Create a SIP media application when you need to enable calling to and from a Request URI hostname, Amazon Chime Voice Connector group, or a private phone number.

To create a SIP media application

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. In the Amazon Chime console, in the navigation pane, choose **SIP media applications**.

   The **SIP media application** page appears.
3. Choose **Create**.

   The **Create a SIP media application** page appears.
4. For **Name**, enter a name for your application.

5. For **AWS Regions**, select a Region. Make sure your selection matches the Region in your Lambda function's Amazon Resource Name (ARN). For example, if your function's ARN contains **us-east-1**, choose the list item with that same Region.
6. Copy one of the following values and paste it into the **ARN** box:

   - The ARN of a Lambda function
   - The ARN of the *alias* of a Lambda function
   - The ARN of a *version* of a Lambda function

   Note
   You can create alias and version ARNs when you build a Lambda function, and you must have an alias or version ARN if you want to enable Lambda concurrency. For more information about Lambda function aliases, version aliases, and concurrency, refer to Lambda function aliases, Lambda function versions, and Managing Lambda provisioned concurrency in the *AWS Lambda Developer Guide*.
7. Choose **Create**.

   A success message appears at the top of the **Create a SIP media application** page, and your media application appears in the list of applications. If you see an error message, follow its instructions.

Viewing a SIP media application

Other administrators can view your SIP media applications, including their details, and you can view theirs.

To view a SIP media application

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. In the navigation pane, choose **SIP media applications**.

   The **SIP media application** page appears and displays all the applications in your organization.
3. To view an application's details, choose the application's name.

Updating a SIP media application

You can update the name and Amazon Resource Names (ARNs) of your Lambda function for your SIP media applications. You can't update the AWS Region.

To update a SIP media application

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. In the navigation pane, choose **SIP media applications**.

   The **SIP media application** page appears.
3. Choose the name of the application that you want to update.

   The application appears on its own page.
4. Choose **Edit**.
5. As needed, change the application's name or Lambda ARN, Lambda alias ARN, or Lambda version ARN.

   Note
   You can create alias and version ARNs when you build a Lambda function, and you must have an alias or version ARN if you want to enable Lambda concurrency. For more

information about Lambda function aliases, version aliases, and concurrency, refer to Lambda function aliases, Lambda function versions, and Managing Lambda provisioned concurrency in the *AWS Lambda Developer Guide*.

6. Choose **Save**.

   A success message appears. If you see an error message, follow its instructions.

Deleting a SIP media application

You delete a SIP media application for several reasons, such as the following:

- You stop using a phone number or a Request URI hostname.
- You make a mistake creating a SIP media application.

> **Note**
> As a best practice, check to ensure that deleting the application won't disrupt the call flow. Also, deleting the application does not delete any associated phone numbers or SIP rules.

To delete a SIP media application

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. In the navigation pane, choose **SIP media applications**.

   The **SIP media application** page appears.
3. Choose the option button next to the application name.
4. Choose **Delete**.

   The **Delete** *application name* dialog box appears.
5. Select **I understand that this action cannot be reversed**, then choose **Delete**.

Using SIP rules

A SIP rule associates your SIP media application with a phone number or a Request URI hostname. You can associate a SIP rule with more than one SIP media application. Each application then runs only that rule. The following topics explain how to create and manage SIP rules for your SIP media applications.

Contents

Creating a SIP rule

Before you can create a SIP rule, you need at least one private phone number or Request URI hostname and a SIP media application. For more about SIP applications, see Creating a SIP media application (p. 70). Also, you can use rules created by other administrators.

To create a SIP rule

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. In the navigation pane, choose **SIP media applications**, locate the SIP application for which you want to create a rule, then copy its phone number or **Outbound host name** value. Paste the number or hostname into Notepad or a similar program. Keep that program open for later use. This keeps the number or hostname available for use later in these steps.
3. In the navigation pane, choose **SIP rules**.

   The **SIP rules** page appears.
4. Choose **Create**.

   The **Create a SIP rule** dialog box appears.
5. For **Name**, enter a name for the rule, then do one of the following:

   Create a rule for a phone number

   A. By default, the **Trigger type** list displays **To phone number**. If it doesn't, open the list and select that value.

   B. For **Phone number**, enter a phone number or choose one from the list. If you enter a number, use this format: **+1***ten-digit number*. For example: +15095551212.

   Create a rule for a Request URI hostname

   A. Open the **Trigger type** list and choose **Request URI hostname**.

   B. Paste the hostname that you copied in step 2 into the **Request URI hostname** box.
6. To use the rule immediately, leave the **Enabled** check box selected. To disable the rule—for example, until a voice connector and its hostname become available—clear the check box.
7. Choose **Next**, and on the **Step 2** page, open the **SIP media application** list and select the SIP application that you want to use.
8. As needed, choose **Add a SIP media application** to use the rule with multiple applications.
9. Choose **Create.**

   A success message appears. If an error message appears, follow its instructions.

Viewing a SIP rule

Other administrators can view your SIP rules, including their details, and you can do the same with their rules.

To view a SIP rule

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. In the navigation pane, choose **SIP rules**.

   The **SIP rules** page appears and displays all the rules in your organization.
3. To view a rule's details, choose the rule's name.

Updating a SIP rule

The only update you can make to a SIP rule is to change its name. Typically, you change a rule name to match the name of its corresponding SIP media application.

To update a SIP rule

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. In the navigation pane, choose **SIP rules**.
3. Choose the name of the rule that you want to change.

   The page for that rule appears.
4. Choose **Edit**.
5. For **Name**, enter a new name for the rule, then choose **Save**.

Enabling a SIP rule

You can enable any SIP rule, even rules created by another administrator. As a best practice, view the rule's details before you enable it. For more information, see Viewing a SIP rule (p. 73).

To enable a SIP rule

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. In the navigation pane, choose **SIP rules**.

   The **SIP rules** page appears.
3. As needed, scroll down to the end of the list of rules, then use the horizontal scroll bar to display the **Status** column.

   Disabled rules have a red **Disabled** icon.
4. Do one of the following to enable a rule:

   Use the Actions list

   A. Scroll over and choose the option button next to the rule's name.
   B. Scroll up, open the **Actions** list and choose **Enable**, then go to step 5.

   Use the Enable button

   A. Choose the rule's name.
   B. Choose **Enable**, located next to **Edit**, then go to step 5.
5. When you choose **Enable** using either method described in step 4, the **Enable rule(s)** dialog box appears. Select **I understand that the rule(s) listed here will trigger the SIP media application**, then choose **Enable**.

Disabling a SIP rule

Disable SIP rules when you don't need the connection that the rule provides. Also, you must disable a SIP rule before you delete that rule or an associated SIP media application. You can disable any rule created by any administrator. As a best practice, view the rule's details before you disable it, and check to ensure that disabling the rule won't disrupt a call flow. For more information, see Viewing a SIP rule (p. 73)

To disable a SIP rule

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. In the navigation pane, choose **SIP rules**.

   The **SIP rules** page appears.

3. As needed, scroll down to the end of the list of rules, then use the horizontal scroll bar to display the **Status** column.

   Enabled rules have a green **Enabled** icon.
4. Do one of the following to disable a rule:

   Use the Actions list

   A. Scroll over and choose the option button next to the rule's name.
   B. Scroll up, open the **Actions** list and choose **Disable**.

      The **Disable rule(s)** dialog box appears. Go to step 5.

   Use the Disable button

   A. Scroll over and select the rule's name.
   B. Choose **Disable**, located next to **Edit**.

      The **Disable rule(s)** dialog box appears. Go to step 5.
5. Select **I understand that this action will stop above rules triggering the SIP media application**, then choose **Disable**.

Deleting a SIP rule

Typically, you delete a SIP rule when you don't need the associated Request URI hostname or phone number. Also, you can delete a SIP rule when you make a mistake creating it.

Note
You must disable a rule before you can delete it. For more information about disabling rules, see Disabling a SIP rule (p. 74).

To delete a SIP rule

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. In the navigation pane, choose **SIP rules**.

   The **SIP rules** page appears.
3. Choose the option button next to the rule's name.
4. Open the **Actions** list and choose **Delete**.

   The **Delete rule(s)** dialog box appears.
5. Select **I understand that this action cannot be reversed**, then choose **Delete**.

Managing global settings for the Amazon Chime SDK

Manage call detail record settings for the Amazon Chime SDK.

Configuring call detail records

Before you can configure call detail record settings for your Amazon Chime SDK administrative account, you must first create an Amazon Simple Storage Service bucket. The Amazon S3 bucket is used as the log destination for your call detail records. When you configure your call detail record settings, you grant the Amazon Chime SDK read and write access to the Amazon S3 bucket in order to save and manage your data. For more information about creating an Amazon S3 bucket, see Getting started with Amazon Simple Storage Service in the *Amazon Simple Storage Service User Guide*.

You can configure call detail record settings for Amazon Chime Voice Connectors. For more information about Amazon Chime Voice Connectors, see Managing phone numbers in Amazon Chime SDK (p. 39).

To configure call detail record settings

1. Create an Amazon S3 bucket by following the steps at Getting started with Amazon Simple Storage Service in the *Amazon Simple Storage Service User Guide*.
2. Open the Amazon Chime console at https://chime.aws.amazon.com/.
3. For **Global Settings**, choose **Call detail records**.
4. Choose the **Voice Connector Configuration** configuration. Note that you can also choose **Business Calling Configuration**.
5. For **Log destination**, select the Amazon S3 bucket.
6. Choose **Save**.

You can stop logging call detail records at any time.

To stop logging call detail records

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Global Settings**, choose **Call detail records**.
3. Choose **Disable logging** for the applicable configuration.

Amazon Chime Voice Connector call detail records

When you choose to receive call detail records for your Amazon Chime Voice Connector, they are sent to your Amazon S3 bucket. The following example shows the general format of an Amazon Chime Voice Connector call detail record name.

```
Amazon-Chime-Voice-Connector-CDRs/
json/abcdef1ghij2klmno3pqr4/2019/03/01/17.10.00.020_123abc4d-efg5-6789-h012-j3456789k012
```

The following example shows the data that is represented in the call detail record name.

```
Amazon-Chime-Voice-Connector-CDRs/json/voiceConnectorID/year/month/
day/callStartTime-voiceConnectorTransactionID
```

The following example shows the general format of an Amazon Chime Voice Connector call detail record.

```
{
    "AwsAccountId": "111122223333",
    "TransactionId": "123abc4d-efg5-6789-h012-j3456789k012",
    "CallId": "123a4b567890123c456789012d3456e7@203.0.113.9:8080",
    "VoiceConnectorId": "abcdef1ghij2klmno3pqr4",
    "Status": "Completed",
    "StatusMessage": "OK",
    "SipAuthUser": "XXXX",
    "BillableDurationSeconds": 6,
    "BillableDurationMinutes": 0.1,
    "SchemaVersion": "2.0",
    "SourcePhoneNumber": "+12065550100",
    "SourceCountry": "US",
    "DestinationPhoneNumber": "+12065550101",
    "DestinationCountry": "US",
    "UsageType": "USE1-US-US-outbound-minutes",
    "ServiceCode": "AmazonChimeVoiceConnector",
    "Direction": "Outbound",
    "StartTimeEpochSeconds": 1565399625,
    "EndTimeEpochSeconds": 1565399629,
    "Region": "us-east-1",
    "Streaming": true
}
```

Amazon Chime Voice Connector streaming detail records

When you choose to receive call detail records for your Amazon Chime Voice Connector, and you stream media to Kinesis Video Streams or send SIPREC requests, streaming detail records are sent to your Amazon S3 bucket. For more information, see Streaming Amazon Chime Voice Connector media to Kinesis (p. 66).

The following example shows the general format of a streaming detail record name.

```
Amazon-Chime-Voice-Connector-SDRs/
json/abcdef1ghij2klmno3pqr4/2019/03/01/17.10.00.020_123abc4d-efg5-6789-h012-j3456789k012
```

The following example shows the data that is represented in the streaming detail record name.

```
Amazon-Chime-Voice-Connector-SDRs/json/voiceConnectorID/year/month/
day/callStartTime-voiceConnectorTransactionID
```

The following example shows the general format of a streaming detail record.

```
{
    "SchemaVersion": "1.0",
    "AwsAccountId": "111122223333",
    "TransactionId": "123abc4d-efg5-6789-h012-j3456789k012",
```

```
    "CallId": "123a4b567890123c456789012d3456e7@203.0.113.9:8080",
    "VoiceConnectorId": "abcdef1ghij2klmno3pqr4",
    "StartTimeEpochSeconds": 1565399625,
    "EndTimeEpochSeconds": 1565399629,
    "Status": "Completed",
    "StatusMessage": "Streaming succeeded",
    "ServiceCode": "AmazonChime",
    "UsageType": "USE1-VC-kinesis-audio-streaming",
    "BillableDurationSeconds": 6,
    "Region": "us-east-1"
}
```

Network configuration and bandwidth requirements

The Amazon Chime SDK requires the destinations and ports described in this topic to support various services. If inbound or outbound traffic is blocked, this blockage might affect the ability to use various services, including audio, video, screen sharing, or chat.

The Amazon Chime SDK uses Amazon Elastic Compute Cloud (Amazon EC2) and other AWS services on port TCP/443. If your firewall blocks port TCP/443, you must put `*.amazonaws.com` on an allow list, or put AWS IP address ranges in the *AWS General Reference* for the following services:

- Amazon EC2
- Amazon CloudFront
- Amazon Route 53

Common

The following destinations and ports are required when running the Amazon Chime SDK in your environment.

Destination	Ports
chime.aws	TCP/443
*.chime.aws	TCP/443
*.amazonaws.com	TCP/443
99.77.128.0/18	TCP/443

Amazon Chime Voice Connector

The following destinations and ports are recommended if you use Amazon Chime Voice Connector.

Signaling

AWS Region	Destination	Ports
US East (N. Virginia)	3.80.16.0/23	UDP/5060 TCP/5060 TCP/5061

AWS Region	Destination	Ports
US West (Oregon)	99.77.253.0/24	UDP/5060 TCP/5060 TCP/5061

Media

AWS Region	Destination	Ports
US East (N. Virginia)	3.80.16.0/23	UDP/5000:65000
US East (N. Virginia)	52.55.62.128/25	UDP/1024:65535
US East (N. Virginia)	52.55.63.0/25	UDP/1024:65535
US East (N. Virginia)	34.212.95.128/25	UDP/1024:65535
US East (N. Virginia)	34.223.21.0/25	UDP/1024:65535
US West (Oregon)	99.77.253.0/24	UDP/5000:65000

Bandwidth requirements

The Amazon Chime SDK has the following bandwidth requirements for the media that it provides:

- Audio
  - 1:1 call: 54 kbps up and down
  - Large call: no more than 32 kbps extra down for 50 callers
- Video
  - 1:1 call: 650 kbps up and down
  - HD mode: 1400 kbps up and down
  - 3–4 people: 450 kbps up and (N-1)*400 kbps down
  - 5–16 people: 184 kbps up and (N-1)*134 kbps down
  - Up and down bandwidth adapts lower based on network conditions
- Screen
  - 1.2 mbps up (when presenting) and down (when viewing) for high quality. This adapts as low as 320 kbps based on network conditions.
  - Remote control: 800 kbps fixed

Amazon Chime Voice Connectors have the following bandwidth requirements:

- Audio
  - Call: ~90 kbps up and down. This includes media payload and packet overhead.
- T.38 fax
  - With V.34: ~40 kbps. This includes media payload and packet overhead.
  - Without V.34: ~20 kbps. This includes media payload and packet overhead.

Administrative support for the Amazon Chime SDK

If you are an administrator and need to contact support for the Amazon Chime SDK, choose one of the following options:

- If you have an AWS Support account, go to Support Center and submit a ticket.
- Otherwise, open the AWS Management Console and choose **Amazon Chime**, **Support**, **Submit request**.

It's helpful to provide the following information:

- A detailed description of the issue.
- The time the issue occurred, including your time zone.

Document history for the Amazon Chime SDK

The following table describes important changes to the *Amazon Chime SDK Administration Guide*, beginning in March 2022. Subscribe to an RSS feed for notifications about updates to this documentation.

update-history-change	update-history-description	update-history-date
New service-linked role (p. 82)	A new service-linked role enables developers to use media pipelines in Amazon Chime SDK meetings. For more information, see AWS managed policy: AmazonChimeSDKMediaPipelinesServiceLinkedRolePolicy.	April 26, 2022
Amazon Chime SDK Administration Guide published (p. 82)	The Amazon Chime SDK Administration Guide published. For changes before March 2022, see Document history for Amazon Chime in the *Amazon Chime Administrator Guide*.	March 24, 2022

AWS glossary

For the latest AWS terminology, see the AWS glossary in the *AWS General Reference*.