Amazon Chime

Administration Guide

Amazon Chime: Administration Guide

Table of Contents

What is Amazon Chime?

Amazon Chime is a communications service that transforms online meetings with an application that is secure and comprehensive. Amazon Chime works across your devices so that you can stay connected. You can use Amazon Chime for online meetings, video conferencing, calls, and chat. You can also share content inside and outside of your organization. Amazon Chime is a fully managed service that runs securely on the AWS cloud, which frees IT from deploying and managing complex infrastructures.

For more information, see Amazon Chime.

Administration overview

As an administrator, you use the Amazon Chime console to perform key tasks, such as creating Amazon Chime accounts and managing users and permissions. To access the Amazon Chime console and create an Amazon Chime administrator account, first create an AWS account. For more information, see Prerequisites (p. 2).

How to get started

After you complete the Prerequisites (p. 2), you can create and configure your Amazon Chime administrative account, then add users to it. Choose Pro or Basic permissions for your users.

If you're ready to get started now, see the following tutorial:

- Getting started (p. 43)

For more information on user access and permissions, see Managing user permissions and access (p. 61). For more information on the features that users with Pro and Basic permissions can access, see Plans and pricing.

Pricing

Amazon Chime provides usage-based pricing. You pay only for the users with Pro permissions that host meetings, and only on the days that those meetings are hosted. Meeting attendees and chat users are not charged.

There is no charge for users with Basic permissions. Basic users cannot host meetings, but they can attend meetings and use chat. For more information on pricing and the features that users with Pro and Basic permissions can access, see Plans and pricing.

Resources

For more information about Amazon Chime, see the following resources:

- Amazon Chime Help Center
- Amazon Chime Training Videos

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. 43).

Security in Amazon Chime

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 Amazon Chime, 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 Amazon Chime. The following topics show you how to configure Amazon Chime 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 resources.

Topics

Identity and access management for Amazon Chime

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 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 you do in Amazon Chime.

Service user – If you use the Amazon Chime service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Amazon Chime 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, see Troubleshooting Amazon Chime identity and access (p. 13).

Service administrator – If you're in charge of Amazon Chime resources at your company, you probably have full access to Amazon Chime. It's your job to determine which Amazon Chime 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 Amazon Chime, see How Amazon Chime works with IAM (p. 7).

IAM administrator – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to Amazon Chime. To view example Amazon Chime identity-based policies that you can use in IAM, see Amazon Chime identity-based policy examples (p. 9).

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 The IAM Console and Sign-in Page 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 or your IAM user name. You can access AWS programmatically using your root user or IAM user 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*.
- **AWS service access** – A service role is an IAM role that a service assumes to perform actions in your account on your behalf. When you set up some AWS service environments, you must define a role for the service to assume. This service role must include all the permissions that are required for the service to access the AWS resources that it needs. Service roles vary from service to service, but many allow you to choose your permissions as long as you meet the documented requirements for that service. Service roles provide access only within your account and cannot be used to grant access to services in other accounts. You can create, modify, and delete a service role from within IAM. For example, you can create a role that allows Amazon Redshift to access an Amazon S3 bucket on your behalf and then load data from that bucket into an Amazon Redshift cluster. For more information, see Creating a Role to Delegate Permissions to an AWS Service in the *IAM User Guide*.

- **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, 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. AWS evaluates these policies when an entity (root user, IAM user, or IAM role) makes a request. 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*.

An IAM administrator can use policies to specify who has access to AWS resources, and what actions they can perform on those resources. 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, role, or group. These policies control what actions that identity 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 such as an Amazon S3 bucket. Service administrators can use these policies to define what actions a specified principal (account member, user, or role) can perform on that resource and under what conditions. Resource-based policies are inline policies. There are no managed resource-based policies.

Access Control Lists (ACLs)

Access control lists (ACLs) are a type of policy that controls 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 Amazon Chime works with IAM

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

Topics

Amazon Chime 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. Amazon Chime 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

The `Action` element of an IAM identity-based policy describes the specific action or actions that will be allowed or denied by the policy. Policy actions usually have the same name as the associated AWS API operation. The action is used in a policy to grant permissions to perform the associated operation.

Policy actions in Amazon Chime use the following prefix before the action: `chime:`. For example, to grant someone permission to access a list of Amazon Chime users in your account with the Amazon Chime `ListUsers` API operation, you include the `chime:ListUsers` action in their policy. Policy statements must include either an `Action` or `NotAction` element. Amazon Chime defines its own set of actions that describe tasks that you can perform with this service.

To specify multiple actions in a single statement, separate them with commas as follows:

```
"Action": [
      "chime:ListUsers",
      "chime:InviteUsers"
```

You can specify multiple actions using wildcards (*). For example, to specify all actions that begin with the word `Get`, include the following action:

```
"Action": "chime:Get*"
```

To see a list of Amazon Chime actions, see Actions defined by Amazon Chime in the *IAM User Guide*.

Resources

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

Condition keys

Amazon Chime 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*.

Examples

To view examples of Amazon Chime identity-based policies, see Amazon Chime identity-based policy examples (p. 9).

Amazon Chime resource-based policies

Amazon Chime 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 to complete 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.

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 (p. 15).

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 identity-based policy examples

By default, IAM users and roles don't have permission to create or modify Amazon Chime 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 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 Amazon Chime 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*.

Using the Amazon Chime console

To access the Amazon Chime console, you must have a minimum set of permissions. These permissions must allow you to list and view details about the Amazon Chime resources in your AWS account. If you create an identity-based policy that is more restrictive than the minimum required permissions, the console won't function as intended for entities (IAM users or roles) with that policy.

To ensure that those entities can still use the Amazon Chime console, also attach the following AWS managed **AmazonChimeReadOnly** policy to the entities. For more information, see Adding permissions to a user in the *IAM User Guide*:

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

You don't need to allow minimum console permissions for users that are making calls only to the AWS CLI or the AWS API. Instead, allow access to only the actions that match the API operation that you're trying to perform.

Allow users full access to Amazon Chime

The following AWS managed **AmazonChimeFullAccess** policy grants an IAM user full access to Amazon Chime resources. The policy gives the user access to all Amazon Chime operations, as well as other operations that Amazon Chime needs to be able to perform on your behalf.

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

```
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketVersioning",
                "s3:GetBucketWebsite"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:GetLogDelivery",
                "logs:ListLogDeliveries",
                "logs:DescribeResourcePolicies",
                "logs:PutResourcePolicy",
                "logs:CreateLogGroup",
                "logs:DescribeLogGroups"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:GetTopicAttributes"
            ],
            "Resource": [
                "arn:aws:sns:*:*:ChimeVoiceConnector-Streaming*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "sqs:GetQueueAttributes",
                "sqs:CreateQueue"
            ],
            "Resource": [
                "arn:aws:sqs:*:*:ChimeVoiceConnector-Streaming*"
            ]
        }
    ]
}
```

Allow users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
```

```
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Allow users to access user management actions

Use the AWS managed **AmazonChimeUserManagement** policy to grant users access to user management actions in the Amazon Chime console.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "chime:ListAccounts",
                "chime:GetAccount",
                "chime:GetAccountSettings",
                "chime:UpdateAccountSettings",
                "chime:ListUsers",
                "chime:GetUser",
                "chime:GetUserByEmail",
                "chime:InviteUsers",
                "chime:InviteUsersFromProvider",
                "chime:SuspendUsers",
                "chime:ActivateUsers",
                "chime:UpdateUserLicenses",
                "chime:ResetPersonalPIN",
                "chime:LogoutUser",
                "chime:ListDomains",
                "chime:GetDomain",
                "chime:ListDirectories",
                "chime:ListGroups",
                "chime:SubmitSupportRequest",
                "chime:ListDelegates",
                "chime:ListAccountUsageReportData",
                "chime:GetMeetingDetail",
                "chime:ListMeetingEvents",
                "chime:ListMeetingsReportData",
                "chime:GetUserActivityReportData",
                "chime:UpdateUser",
                "chime:BatchUpdateUser",
                "chime:BatchSuspendUser",
                "chime:BatchUnsuspendUser",
                "chime:AssociatePhoneNumberWithUser",
                "chime:DisassociatePhoneNumberFromUser",
```

```
                "chime:GetPhoneNumber",
                "chime:ListPhoneNumbers",
                "chime:GetUserSettings",
                "chime:UpdateUserSettings",
                "chime:CreateUser",
                "chime:AssociateSigninDelegateGroupsWithAccount",
                "chime:DisassociateSigninDelegateGroupsFromAccount"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

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 Using the Amazon Chime SDK in the *Amazon Chime Developer Guide*.

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

Troubleshooting Amazon Chime identity and access

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

Topics

- I want to allow people outside of my AWS account to access my Amazon Chime resources (p. 15)

I am not authorized to perform an action in Amazon Chime

If the AWS Management Console 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 console 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.

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 console to perform an action in Amazon Chime. 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 Amazon Chime

To allow others to access Amazon Chime, 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.

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 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 supports these features, see How Amazon Chime works with IAM (p. 7).
- 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

Amazon Chime 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 Amazon Chime. Service-linked roles are predefined by Amazon Chime and include all the permissions that the service requires to call other AWS services on your behalf.

Topics

Using roles to stream Amazon Chime Voice Connector media to Kinesis

Amazon Chime 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 Amazon Chime. Service-linked roles are predefined by Amazon Chime and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Amazon Chime more efficient because you aren't required to manually add the necessary permissions. Amazon Chime defines the permissions of its service-linked

roles, and unless defined otherwise, only Amazon Chime 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 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.

Service-linked role permissions for Amazon Chime Voice Connectors

Amazon Chime Voice Connectors use the service-linked role named **AWSServiceRoleForAmazonChimeVoiceConnector** – Allows Amazon Chime 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. 82).

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

- `voiceconnector.chime.amazonaws.com`

The role permissions policy allows Amazon Chime 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-*`

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 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

Amazon Chime 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 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 resources used by the AWSServiceRoleForAmazonChimeVoiceConnector (console)

- Stop media streaming for all the Amazon Chime Voice Connectors in your Amazon Chime 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 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 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 service-linked roles

Amazon Chime 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 shared Alexa for Business devices

Amazon Chime 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 Amazon Chime. Service-linked roles are predefined by Amazon Chime and include all the permissions that the service requires to call other AWS services on your behalf.

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

Service-linked role permissions for Amazon Chime

Amazon Chime uses the service-linked role named **AWSServiceRoleForAmazonChime** – Allows access to AWS services and resources used or managed by Amazon Chime, such as Alexa for Business shared devices.

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

- `chime.amazonaws.com`

The role permissions policy allows Amazon Chime to complete the following action on the specified resource:

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

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

You don't need to manually create a service-linked role. When you turn on Alexa for Business for a shared device in Amazon Chime 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 **Amazon Chime** use case. In the AWS CLI or the AWS API, create a service-linked role with the `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

Amazon Chime does not allow you to edit the AWSServiceRoleForAmazonChime 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

If you no longer require 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 Amazon Chime 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 resources used by the AWSServiceRoleForAmazonChime (console)

- Turn off Alexa for Business for all shared devices in your Amazon Chime account.

  a. Open the Amazon Chime console at https://chime.aws.amazon.com/.
  b. Choose **Users**, **Shared devices**.
  c. Select a device.
  d. Choose **Actions**.
  e. Choose **Disable Alexa for Business.**

Manually delete the service-linked role

Use the IAM console, the AWS CLI, or the AWS API to delete the AWSServiceRoleForAmazonChime 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

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

Logging and monitoring in Amazon Chime

Monitoring is an important part of maintaining the reliability, availability, and performance of Amazon Chime and your other AWS solutions. AWS provides the following tools to monitor Amazon Chime, 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 Amazon Chime with Amazon CloudWatch

You can monitor Amazon Chime 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 Amazon Chime

Amazon Chime 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.

Metric	Description
	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. 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

Metric	Description
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
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

Metric	Description
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
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

Metric	Description
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
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 Amazon Chime

The CloudWatch dimensions that you can use with Amazon Chime 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 Amazon Chime

You can send Amazon Chime Voice Connector metrics to CloudWatch Logs. For more information, see Editing Amazon Chime Voice Connector settings (p. 77).

Media quality metric logs

You can opt to receive media quality metric logs for your Amazon Chime Voice Connector. When you do, Amazon Chime 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.
call_id	The call 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.

Field	Description
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.
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.

Field	Description
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.
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, Amazon Chime 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.

Field	Description
sip_message	The full SIP message that is captured.

Automating Amazon Chime with EventBridge

Amazon EventBridge lets you automate your AWS services and respond automatically to system events, such as application availability issues or resource changes. Events from AWS services are delivered to EventBridge in near real time. You can write simple rules to specify the events that are of interest to you, and the automated actions to take when any of those events matches a rule.

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"
  }
}
```

Automating the Amazon Chime SDK with EventBridge

Some examples of using EventBridge with the Amazon Chime SDK include:

- Updating metadata when an attendee joins or leaves an Amazon Chime SDK meeting.
- Implementing push notifications or rosters for an Amazon Chime SDK meeting.

For more information, see the Amazon EventBridge User Guide and Using the Amazon Chime SDK in the *Amazon Chime Developer Guide*.

Amazon Chime SDK events

The Amazon Chime SDK supports sending events to EventBridge when the events discussed in this section occur.

Amazon Chime SDK meeting starts

The Amazon Chime SDK sends this event when a new meeting starts.

Example : Event data

The following is example data for this event.

```
{
  "version": "0",
  "source": "aws.chime",
  "account": "111122223333",
  "id": "12345678-1234-1234-1234-111122223333",
  "region": "us-east-1",
  "detail-type": "Chime Meeting State Change",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "resources": []
  "detail": {
    "version": "0",
```

```
    "eventType": "chime:MeetingStarted",
    "timestamp": 12344566754,
    "meetingId": "87654321-4321-4321-1234-111122223333",
  }
}
```

Amazon Chime SDK meeting ends

The Amazon Chime SDK sends this event when an active meeting ends.

Example : Event data

The following is example data for this event.

```
{
  "version": "0",
  "source": "aws.chime",
  "account": "111122223333",
  "id": "12345678-1234-1234-1234-111122223333",
  "region": "us-east-1",
  "detail-type": "Chime Meeting State Change",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "resources": []
  "detail": {
    "version": "0",
    "eventType": "chime:MeetingEnded",
    "timestamp": 12344566754,
    "meetingId": "87654321-4321-4321-1234-111122223333",
  }
}
```

Amazon Chime SDK attendee is added

The Amazon Chime SDK sends this event when a new attendee is added to an active meeting.

Example : Event data

The following is example data for this event.

```
{
  "version": "0",
  "source": "aws.chime",
  "account": "111122223333",
  "id": "12345678-1234-1234-1234-111122223333",
  "region": "us-east-1",
  "detail-type": "Chime Meeting State Change",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "resources": []
  "detail": {
    "version": "0",
    "eventType": "chime:AttendeeAdded",
    "timestamp": 12344566754,
    "meetingId": "87654321-4321-4321-1234-111122223333",
    "attendeeId": "87654321-4321-4321-1234-111122223333",
    "externalUserId": "87654321-4321-4321-1234-111122223333",
  }
}
```

Amazon Chime SDK attendee is removed

The Amazon Chime SDK sends this event when an attendee is removed from an active meeting.

Example : Event data

The following is example data for this event.

```
{
  "version": "0",
  "source": "aws.chime",
  "account": "111122223333",
  "id": "12345678-1234-1234-1234-111122223333",
  "region": "us-east-1",
  "detail-type": "Chime Meeting State Change",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "resources": []
  "detail": {
    "version": "0",
    "eventType": "chime:AttendeeDeleted",
    "timestamp": 12344566754,
    "meetingId": "87654321-4321-4321-1234-111122223333",
    "attendeeId": "87654321-4321-4321-1234-111122223333",
    "externalUserId": "87654321-4321-4321-1234-111122223333",
  }
}
```

Amazon Chime SDK attendee is authorized

The Amazon Chime SDK sends this event when an existing attendee joins a meeting.

Example : Event data

The following is example data for this event.

```
{
  "version": "0",
  "source": "aws.chime",
  "account": "111122223333",
  "id": "12345678-1234-1234-1234-111122223333",
  "region": "us-east-1",
  "detail-type": "Chime Meeting State Change",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "resources": []
  "detail": {
    "version": "0",
    "eventType": "chime:AttendeeAuthorized",
    "timestamp": 12344566754,
    "meetingId": "87654321-4321-4321-1234-111122223333",
    "attendeeId": "87654321-4321-4321-1234-111122223333",
    "externalUserId": "87654321-4321-4321-1234-111122223333"
  }
}
```

Amazon Chime SDK attendee joins a meeting

The Amazon Chime SDK sends this event when an existing attendee joins an Amazon Chime SDK meeting using the specified network transport.

Example : Event data

The following is example data for this event.

```
{
```

```
  "version": "0",
  "source": "aws.chime",
  "account": "111122223333",
  "id": "12345678-1234-1234-1234-111122223333",
  "region": "us-east-1",
  "detail-type": "Chime Meeting State Change",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "resources": []
  "detail": {
    "version": "0",
    "eventType": "chime:AttendeeJoined",
    "timestamp": 12344566754,
    "meetingId": "87654321-4321-4321-1234-111122223333",
    "attendeeId": "87654321-4321-4321-1234-111122223333",
    "externalUserId": "87654321-4321-4321-1234-111122223333"
    "networkType" "Voip"
  }
}
```

Amazon Chime SDK attendee leaves a meeting

The Amazon Chime SDK sends this event when an existing attendee leaves an Amazon Chime SDK meeting using the specified network transport.

Example : Event data

The following is example data for this event.

```
{
  "version": "0",
  "source": "aws.chime",
  "account": "111122223333",
  "id": "12345678-1234-1234-1234-111122223333",
  "region": "us-east-1",
  "detail-type": "Chime Meeting State Change",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "resources": []
  "detail": {
    "version": "0",
    "eventType": "chime:AttendeeLeft",
    "timestamp": 12344566754,
    "meetingId": "87654321-4321-4321-1234-111122223333",
    "attendeeId": "87654321-4321-4321-1234-111122223333",
    "externalUserId": "87654321-4321-4321-1234-111122223333"
    "networkType" "Voip"
  }
}
```

Amazon Chime SDK attendee drops from a meeting

The Amazon Chime SDK sends this event when an existing attendee drops from an Amazon Chime SDK meeting using the specified network transport.

Example : Event data

The following is example data for this event.

```
{
  "version": "0",
  "source": "aws.chime",
  "account": "111122223333",
```

```
  "id": "12345678-1234-1234-1234-111122223333",
  "region": "us-east-1",
  "detail-type": "Chime Meeting State Change",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "resources": []
  "detail": {
    "version": "0",
    "eventType": "chime:AttendeeDropped",
    "timestamp": 12344566754,
    "meetingId": "87654321-4321-4321-1234-111122223333",
    "attendeeId": "87654321-4321-4321-1234-111122223333",
    "externalUserId": "87654321-4321-4321-1234-111122223333"
    "networkType" "Voip"
  }
}
```

Amazon Chime SDK attendee starts streaming video

The Amazon Chime SDK sends this event when an existing attendee starts streaming video.

Example : Event data

The following is example data for this event.

```
{
  "version": "0",
  "source": "aws.chime",
  "account": "111122223333",
  "id": "12345678-1234-1234-1234-111122223333",
  "region": "us-east-1",
  "detail-type": "Chime Meeting State Change",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "resources": []
  "detail": {
    "version": "0",
    "eventType": "chime:AttendeeVideoStarted",
    "timestamp": 12344566754,
    "meetingId": "87654321-4321-4321-1234-111122223333",
    "attendeeId": "87654321-4321-4321-1234-111122223333",
    "externalUserId": "87654321-4321-4321-1234-111122223333"
  }
}
```

Amazon Chime SDK attendee stops streaming video

The Amazon Chime SDK sends this event when an existing attendee stops streaming video.

Example : Event data

The following is example data for this event.

```
{
  "version": "0",
  "source": "aws.chime",
  "account": "111122223333",
  "id": "12345678-1234-1234-1234-111122223333",
  "region": "us-east-1",
  "detail-type": "Chime Meeting State Change",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "resources": []
  "detail": {
    "version": "0",
```

```
    "eventType": "chime:AttendeeVideoStopped",
    "timestamp": 12344566754,
    "meetingId": "87654321-4321-4321-1234-111122223333",
    "attendeeId": "87654321-4321-4321-1234-111122223333",
    "externalUserId": "87654321-4321-4321-1234-111122223333"
  }
}
```

Amazon Chime SDK attendee starts sharing screen

The Amazon Chime SDK sends this event when an existing attendee starts sharing their screen.

Example : Event data

The following is example data for this event.

```
{
  "version": "0",
  "source": "aws.chime",
  "account": "111122223333",
  "id": "12345678-1234-1234-1234-111122223333",
  "region": "us-east-1",
  "detail-type": "Chime Meeting State Change",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "resources": []
  "detail": {
    "version": "0",
    "eventType": "chime:AttendeeScreenShareStarted",
    "timestamp": 12344566754,
    "meetingId": "87654321-4321-4321-1234-111122223333",
    "attendeeId": "87654321-4321-4321-1234-111122223333",
    "externalUserId": "87654321-4321-4321-1234-111122223333"
  }
}
```

Amazon Chime SDK attendee stops sharing screen

The Amazon Chime SDK sends this event when an existing attendee stops sharing their screen.

Example : Event data

The following is example data for this event.

```
{
  "version": "0",
  "source": "aws.chime",
  "account": "111122223333",
  "id": "12345678-1234-1234-1234-111122223333",
  "region": "us-east-1",
  "detail-type": "Chime Meeting State Change",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "resources": []
  "detail": {
    "version": "0",
    "eventType": "chime:AttendeeScreenShareStopped",
    "timestamp": 12344566754,
    "meetingId": "87654321-4321-4321-1234-111122223333",
    "attendeeId": "87654321-4321-4321-1234-111122223333",
    "externalUserId": "87654321-4321-4321-1234-111122223333"
  }
}
```

Amazon Chime SDK attendee content joins a meeting

The Amazon Chime SDK sends this event when a content share joins an Amazon Chime SDK meeting using the specified network transport.

Example : Event data

The following is example data for this event.

```
{
  "version": "0",
  "source": "aws.chime",
  "account": "111122223333",
  "id": "12345678-1234-1234-1234-111122223333",
  "region": "us-east-1",
  "detail-type": "Chime Meeting State Change",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "resources": []
  "detail": {
    "version": "0",
    "eventType": "chime:AttendeeContentJoined",
    "timestamp": 12344566754,
    "meetingId": "87654321-4321-4321-1234-111122223333",
    "attendeeId": "87654321-4321-4321-1234-111122223333",
    "externalUserId": "87654321-4321-4321-1234-111122223333"
    "networkType" "Voip"
  }
}
```

Amazon Chime SDK attendee content leaves a meeting

The Amazon Chime SDK sends this event when a content share leaves an Amazon Chime SDK meeting using the specified network transport.

Example : Event data

The following is example data for this event.

```
{
  "version": "0",
  "source": "aws.chime",
  "account": "111122223333",
  "id": "12345678-1234-1234-1234-111122223333",
  "region": "us-east-1",
  "detail-type": "Chime Meeting State Change",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "resources": []
  "detail": {
    "version": "0",
    "eventType": "chime:AttendeeContentLeft",
    "timestamp": 12344566754,
    "meetingId": "87654321-4321-4321-1234-111122223333",
    "attendeeId": "87654321-4321-4321-1234-111122223333",
    "externalUserId": "87654321-4321-4321-1234-111122223333"
    "networkType" "Voip"
  }
}
```

Amazon Chime SDK attendee content drops from a meeting

The Amazon Chime SDK sends this event when a content share drops from an Amazon Chime SDK meeting using the specified network transport.

Example : Event data

The following is example data for this event.

```
{
  "version": "0",
  "source": "aws.chime",
  "account": "111122223333",
  "id": "12345678-1234-1234-1234-111122223333",
  "region": "us-east-1",
  "detail-type": "Chime Meeting State Change",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "resources": []
  "detail": {
    "version": "0",
    "eventType": "chime:AttendeeContentDropped",
    "timestamp": 12344566754,
    "meetingId": "87654321-4321-4321-1234-111122223333",
    "attendeeId": "87654321-4321-4321-1234-111122223333",
    "externalUserId": "87654321-4321-4321-1234-111122223333"
    "networkType" "Voip"
  }
}
```

Amazon Chime SDK attendee content starts streaming video

The Amazon Chime SDK sends this event when a content share starts streaming video.

Example : Event data

The following is example data for this event.

```
{
  "version": "0",
  "source": "aws.chime",
  "account": "111122223333",
  "id": "12345678-1234-1234-1234-111122223333",
  "region": "us-east-1",
  "detail-type": "Chime Meeting State Change",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "resources": []
  "detail": {
    "version": "0",
    "eventType": "chime:AttendeeContentVideoStarted",
    "timestamp": 12344566754,
    "meetingId": "87654321-4321-4321-1234-111122223333",
    "attendeeId": "87654321-4321-4321-1234-111122223333",
    "externalUserId": "87654321-4321-4321-1234-111122223333"
  }
}
```

Amazon Chime SDK attendee content stops streaming video

The Amazon Chime SDK sends this event when a content share stops streaming video.

Example : Event data

The following is example data for this event.

```
{
```

```
  "version": "0",
  "source": "aws.chime",
  "account": "111122223333",
  "id": "12345678-1234-1234-1234-111122223333",
  "region": "us-east-1",
  "detail-type": "Chime Meeting State Change",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "resources": []
  "detail": {
    "version": "0",
    "eventType": "chime:AttendeeContentVideoStopped",
    "timestamp": 12344566754,
    "meetingId": "87654321-4321-4321-1234-111122223333",
    "attendeeId": "87654321-4321-4321-1234-111122223333",
    "externalUserId": "87654321-4321-4321-1234-111122223333"
  }
}
```

Logging Amazon Chime API calls with AWS CloudTrail

Amazon Chime is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Amazon Chime. CloudTrail captures all API calls for Amazon Chime as events, including calls from the Amazon Chime console and from code calls to the Amazon Chime APIs. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Amazon Chime. 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 Amazon Chime, 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 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 Amazon Chime, 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 actions are logged by CloudTrail and are documented in the *Amazon Chime 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 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 Amazon Chime are identified by the **chime.amazonaws.com** event source.

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

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

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

Compliance validation for Amazon Chime

Third-party auditors assess the security and compliance of Amazon Chime as part of multiple AWS compliance programs. These include ISO and HIPAA.

If you have an executed HIPAA Business Associate Addendum (BAA) with AWS, you can use Amazon Chime for meetings, collaboration, and business calling. For information about getting a BAA with AWS, or about how to run HIPAA-regulated workloads on AWS, see HIPAA.

Amazon Chime's internal communication channels are encrypted during transit and support TLS 1.2. This doesn't include traffic that flows to and from the public telephone network (PSTN) to Amazon Chime's carrier partners. Because the public telephone network (PSTN) is an unencrypted network, there is no end-to-end encryption mechanism for it.

Amazon Chime supports the option for an unencrypted session initiation protocol (SIP) endpoint for video conferencing and PSTN services. This option is for users with equipment that does not support SIP over TLS. For a list of Amazon Chime's public endpoints, see Network configuration and bandwidth requirements (p. 96).

For a list of AWS services that are in scope for 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 Amazon Chime 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 security- and compliance-focused baseline environments on AWS.
- Architecting for HIPAA Security and Compliance Whitepaper – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.
- 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 the compliance of your resource configurations with internal practices, industry guidelines, and regulations.
- AWS Security Hub – This AWS service provides a comprehensive view of your security state within AWS. This helps you check your compliance with security industry standards and best practices.

Resilience in Amazon Chime

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, Amazon Chime offers different features to help support your data resiliency and backup needs. For more information, see Managing Amazon Chime Voice Connector groups (p. 80) and Streaming Amazon Chime Voice Connector media to Kinesis (p. 82).

Infrastructure security in Amazon Chime

As a managed service, Amazon Chime 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 Amazon Chime and 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 Amazon Chime 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.

Understanding Amazon Chime automatic updates

Amazon Chime provides different ways to update its clients. The method varies, depending on whether your users run Amazon Chime in a browser, on your desktop, or on a mobile device.

The Amazon Chime web application – https://app.chime.aws – always loads with the latest features and security fixes.

The Amazon Chime desktop client checks for updates whenever a user chooses **Quit** or **Sign Out**. This applies to Windows and macOS machines. As users run the client, it checks for updates every three hours. Users can also check for updates by choosing **Check for Updates** on the Windows Help menu or on the macOS **Amazon Chime** menu.

When the desktop client detects an update, Amazon Chime prompts users to install it unless they're in an ongoing meeting. Users are in an *ongoing meeting* when:

- They're attending a meeting.
- They were invited to a meeting that is still in progress.

Amazon Chime prompts them to install the latest version, and it gives them a 15-second countdown so they can postpone the installation. Choose **Try Later** to postpone the update.

When users postpone an update, and they aren't in an ongoing meeting, the client checks for the update after three hours and prompts them again to install. The installation begins when the countdown ends.

> **Note**
> On a macOS machine, users need to choose **Restart Now** to begin the update.

On a mobile device – Amazon Chime mobile applications use the update options provided by the App Store and Google Play to deliver the latest version of the Amazon Chime client. You can also distribute updates through your mobile device management system. This topic assumes that you know how.

Getting started

The easiest way for your users to get started with Amazon Chime is to download and use the Amazon Chime Pro version for free for 30 days. For more information, see Download Amazon Chime.

Purchasing Amazon Chime

To continue using the Amazon Chime Pro version after the 30-day free trial period, you must create an Amazon Chime administrator account and add your users to it. To get started, you must first complete the Prerequisites (p. 2), which include creating an AWS account. Then, you can create and configure an Amazon Chime administrator account and add users to it by completing the following tasks.

Tasks

Step 1: Creating an Amazon Chime administrator account

After you complete the Prerequisites (p. 2), you can create an Amazon Chime administrator account.

To create an Amazon Chime administrator account

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. On the **Accounts** page, choose **New account**.
3. For **Account Name**, enter a name for the account and choose **Create account**.
4. (Optional) Choose whether to let Amazon Chime select the optimal AWS Region for your meetings from all available Regions, or to use only the Regions that you select. For more information, see Managing meeting settings (p. 49).

Step 2 (optional): Configuring account settings

By default, new accounts are created as Team accounts. If you prefer to claim a domain and connect to your own identity provider, or Okta SSO, you can convert to an Enterprise account. For more information about Team and Enterprise account types, see Choosing between an Amazon Chime Team account or Enterprise account (p. 46).

To convert a Team account to an Enterprise account

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Accounts**, choose the name of the account.
3. For **Identity**, choose **Getting Started**.
4. Follow the steps in the console to claim your domain.

5. (Optional) Follow the steps in the console to set up your identity provider and configure your directory group.

For more information about claiming domains, see Claiming a domain (p. 53). For more information about setting up identity providers, see Connecting to your Active Directory (p. 54) and Connecting to Okta SSO (p. 56).

You can also allow or stop allowing account policies for options, such as remote control of shared screens and the Amazon Chime call me feature.

To configure account policies

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. On the **Accounts** page, choose the name of the account to configure.
3. For **Settings**, choose **Meetings**.
4. For **Policies**, select or clear the account policy options you want to allow or stop allowing.
5. Choose **Change**.

For more information, see Managing meeting settings (p. 49).

Step 3: Adding users to your account

After your Amazon Chime Team account is created, invite yourself and your users to join it. If you are upgrading your account to an Enterprise account, you do not need to invite your users. Instead, upgrade to an Enterprise account and claim your domain. For more information, see Step 2 (optional): Configuring account settings (p. 43).

To add users to your Amazon Chime account

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. On the **Accounts** page, choose the name of your account.
3. On the **Users** page, choose **Invite users**.
4. Enter the email addresses of the users to invite, including yourself, and choose **Invite users**.

The invited users receive email invitations to join the Amazon Chime Team account that you created. When they register their Amazon Chime user accounts, they receive Pro permissions by default, and their 30-day trial ends. If they have already signed up for an Amazon Chime user account with their work email address, they can continue to use that account. They can also download the Amazon Chime client app at any time by choosing **Download Amazon Chime** and signing in to their user account.

You are only charged for a user with Pro permissions when they host a meeting. There is no charge for users with Basic permissions. Basic users cannot host meetings, but they can attend meetings and use chat. For more information about pricing and the features that users with Pro and Basic permissions can access, see Plans and pricing.

To change user permissions

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. On the **Accounts** page, choose the name of your account.
3. On the **Users** page, select the user or users to change permissions for.
4. Choose **User actions**, **Assign user permission**.

5. For **Permissions**, select **Pro** or **Basic**.
6. Choose **Assign**.

You can provide other users with administrator permissions, and also control their access to the Amazon Chime console for your account. For more information, see Identity and access management for Amazon Chime (p. 3).

(Optional) Setting up phone numbers for your Amazon Chime account

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

Amazon Chime Business Calling

Lets your users send and receive phone calls and text messages directly from Amazon Chime. Provision your phone numbers in the Amazon Chime console or port in existing phone numbers. Assign the phone numbers to your Amazon Chime users and grant them permissions to send and receive phone calls and text messages using Amazon Chime. For more information, see Managing phone numbers in Amazon Chime (p. 68) and Porting existing phone numbers (p. 69).

Amazon Chime Voice Connector

Provides SIP trunking service for an existing phone system. Port in existing phone numbers or provision new phone numbers in the Amazon Chime console. For more information, see Managing Amazon Chime Voice Connectors (p. 76).

(Optional) Configuring your conference rooms to use Amazon Chime

Amazon Chime can integrate with your in-room video conference systems. For more information, see Conference room configuration (p. 94) and Setting up Amazon Chime on Dolby hardware (p. 88).

Managing your Amazon Chime accounts

You can use Amazon Chime as an individual user or as a group with no administrators. But if you want to add administrator functionality or purchase Amazon Chime Pro, you must create an Amazon Chime account in the AWS Management Console. To learn how to create an Amazon Chime administrator account, or for more information about purchasing Amazon Chime Pro, see Getting started (p. 43).

For more information about the different types of Amazon Chime administrator accounts, see Choosing between an Amazon Chime Team account or Enterprise account (p. 46). For more information about managing an existing administrator account, see the following topics.

Contents

Choosing between an Amazon Chime Team account or Enterprise account

When you create an Amazon Chime administrator account, you choose whether to create a Team account or an Enterprise account. For more information about creating an Amazon Chime administrator account, see Getting started (p. 43).

Team account

With a Team account, you can invite users and grant them Amazon Chime Pro permissions without claiming an email domain. For more information about Pro and Basic permissions, see Plans and pricing.

You can invite users from any email domain that hasn't been claimed by another organization. You only pay for users when they host meetings. Users in your Team account can use the Amazon Chime app to search for and contact other Amazon Chime users who are registered to the same account. We also recommend a Team account for paying for Pro users outside of your organization.

Enterprise account

With an Enterprise account, you have more control over the users from your organization's domains. You can choose to connect to your own identity provider or Okta SSO to authenticate and assign Pro or Basic permissions. Amazon Chime also supports Microsoft Active Directory.

To create an Enterprise account, you must claim at least one email domain. This ensures that all users who sign in to Amazon Chime using your claimed domains are included in your centrally managed Amazon Chime account. Enterprise accounts are required for managing your users through a supported directory integration. For more information, see Claiming a domain (p. 53) and Connecting to your Active Directory (p. 54).

You can also manage user activation and suspension from your Enterprise account. For more information, see Managing user permissions and access (p. 61).

Converting a Team account to an Enterprise account

To convert an existing Team account to an Enterprise account, claim one or more email domains in the Amazon Chime console. For more information about the differences between Team and Enterprise accounts, see Choosing between an Amazon Chime Team account or Enterprise account (p. 46). For more information about claiming a domain, see Claiming a domain (p. 53).

To convert a Team account to an Enterprise account

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Accounts**, choose the name of the account.
3. For **Identity**, choose **Getting Started**.
4. Follow the steps in the console to claim your domain.
5. (Optional) Follow the steps in the console to set up your identity provider and configure your directory group.

After your account is converted to an Enterprise account, you can decide whether to connect an Active Directory instance through AWS Directory Service. Connecting to an Active Directory instance allows your users to sign in to Amazon Chime using their Active Directory credentials. For more information, see Connecting to your Active Directory (p. 54).

If you don't connect to an Active Directory instance, your users can continue to sign in to Amazon Chime using Login with Amazon (LWA) or their Amazon.com account credentials.

Renaming your account

Use the following procedure to rename your account. The new name you choose appears in invitation emails sent to users to join your account.

To rename your account

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. Select the account in the **Account name** column. Under **Settings**, choose **Account**.
3. Choose **Account actions**, **Rename account**, enter the new account name, and then choose **Save**.

Deleting your account

If you delete your AWS account in the AWS Management Console, your Amazon Chime accounts are automatically deleted. Alternatively, you can use the Amazon Chime console to delete an Amazon Chime Team or Enterprise account.

> **Note**
> Users who aren't managed on a Team or Enterprise account can request to be deleted using the Amazon Chime Assistant "Delete me" command. For more information, see Using the Amazon Chime Assistant.

To delete a Team account

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. Select the account in the **Account name** column and select **Account** under **Settings**.
3. In the navigation pane, the **Users** page is displayed.
4. Select the users and choose **User actions**, **Remove user**.
5. In the navigation pane, choose **Accounts**, **Account actions**, and **Delete account**.
6. Confirm that you want to delete your account.

Amazon Chime deletes all user data when you delete your account. This includes termination of an AWS account, individual Amazon Chime accounts, or unmanaged Amazon Chime users. This excludes non-content data related to user accounts and Amazon Chime usage (Service Attributes covered under the Customer Agreement) that is generated by Amazon Chime.

To delete an Enterprise account

1. Remove the domains.

   > **Note**
   > When you remove a domain, the following occurs:
   >
   > - Users associated with the domain are immediately signed out of all devices and lose access to all contacts, chat conversations, and chat rooms.
   > - Meetings scheduled by users from this domain no longer start.
   > - Suspended users continue to be displayed as **Suspended** status on the **Users** and **User detail** pages and can't access their data. They can't create new Amazon Chime accounts with their email address.
   > - Registered users are displayed as **Released** on the **Users** and **User detail** pages and can't access their data. They can create a new Amazon Chime account with their email address.
   > - If you have an Active Directory account, and you remove a domain that is associated with a user's primary email address, the user can't access Amazon Chime and their profile is deleted. If you remove a domain that is associated with a user's secondary email address, they can't log in with that email address, but they retain access to their Amazon Chime contacts and data.
   > - If you have an Enterprise OpenID Connect (OIDC) account, and you remove a domain that is associated with a user's primary email address, the user can no longer access Amazon Chime and their profile is deleted.
2. Open the Amazon Chime console at https://chime.aws.amazon.com/.
3. On the **Accounts** page, select the name of the Team account.
4. In the navigation pane, choose **Settings**, **Domains**.
5. On the **Domains** page, choose **Remove domain**.
6. In the navigation pane, choose **Accounts**, **Account actions**, and **Delete account**.

7. Confirm that you want to delete your account.

Amazon Chime deletes all user data when you delete your account. This includes termination of an AWS account, individual Amazon Chime accounts, or unmanaged Amazon Chime users. This excludes non-content data related to user accounts and Amazon Chime usage (Service Attributes covered under the Customer Agreement) that is generated by Amazon Chime.

Managing meeting settings

Manage your meeting settings from the Amazon Chime console.

Meeting policy settings

Manage account policies in the Amazon Chime console under **Settings**, **Meetings**. Choose from the following policy options.

Enable shared control in screen sharing

Choose whether users in your organization can grant shared control of their computers while in meetings. Attendees who request shared control of your users' computers receive an error message indicating that remote control isn't available.

Enable outbound calling to join meetings

Turns on the Amazon Chime call me feature. Provides the option for meeting attendees to join meetings by receiving a phone call from Amazon Chime.

Meeting application settings

Manage meeting application access under **Settings**, **Meetings** in the Amazon Chime console. You can choose the following option:

Allow users to sign in to Amazon Chime using the Amazon Chime Meetings App for Slack

This option lets users in your organization sign in to Amazon Chime from the Amazon Chime Meetings App for Slack. For more information, see Setting up the Amazon Chime Meetings App for Slack (p. 58).

Meeting Region settings

To improve meeting quality and reduce latency, Amazon Chime processes meetings in the optimal AWS Region for all participants. You can choose whether to let Amazon Chime select the optimal Region for a meeting from all available Regions, or to use only the Regions that you select.

You can update this setting from your account **Meetings** settings at any time. From your **Meetings** settings, you can also view the percentage of your Amazon Chime meetings that are being processed in each Region.

To update meeting Region settings

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. On the **Accounts** page, select the name of your account.
3. In the navigation pane, choose **Settings**, **Meetings**.

4. For **Regions**, choose one of the following options:
   - **Use all available Regions to ensure meeting quality** – Allows Amazon Chime to optimize meeting processing for you.
   - **Use only the Regions that I select** – Allows you to select Regions from the dropdown menu.
5. Choose **Save**.

Retention

Manage your retention settings from the Amazon Chime console.

Contents

Managing chat retention policies

Administrators of Amazon Chime Enterprise accounts can choose to set chat retention policies for the following:

- The chat conversations that include only members of their Enterprise account
- The chat rooms that are created by members of their Enterprise account

Messages are automatically deleted based on the time period set by the administrator. You can set time periods lasting from one day to 15 years.

> **Note**
> A retention period of 90 days applies to the chat conversations that include any users who are members of an Amazon Chime Enterprise account and any users who do not belong to the same Enterprise account. The preceding messages are automatically deleted after 90 days.
> Retention policies do not apply to the following:
>
> - The chat conversations that do not include any members of Amazon Chime Enterprise accounts
> - The chat rooms created by users who are not members of an Amazon Chime Enterprise account

How retention policies affect Amazon Chime users

The retention policies that Enterprise account administrators set affect Amazon Chime users differently, depending on whether the users are part of the same Enterprise account, a different Enterprise account, a Team account, or whether the users are not members of any account.

Enterprise member chat conversations

The following table shows how retention policies affect chat conversations for Enterprise account members.

If the chat conversation includes...	The retention policy is...
Only other members of the user's Enterprise account	Set by the user's administrator
Anyone outside of the user's Enterprise account	Automatically set to 90 days

Enterprise member chat rooms

The following table shows how retention policies affect chat rooms for Enterprise account members.

If the chat room is created by...	The retention policy is...
A member of the user's Enterprise account	Set by the user's administrator
Another Enterprise account member	Set by the other account's administrator
A non-Enterprise account member	Not applicable

Team member chat conversations

The following table shows how retention policies affect chat conversations for Team account members.

If the chat conversation includes...	The retention policy is...
Only users who are not members of an Enterprise account	Not applicable
At least one member of an Enterprise account	Automatically set to 90 days

Team member chat rooms

The following table shows how retention policies affect chat rooms for Team account members.

If the chat room is created by ...	The retention policy is...
A Team account user	Not applicable
Anyone who is not an Enterprise account member	Not applicable
A member of an Enterprise account	Set by the Enterprise account's administrator

Amazon Chime users who are not members of an Enterprise or Team account are only subject to chat room retention policies in chat rooms that are created by a member of an Enterprise account.

Chat conversations with recipients who do not belong to an Enterprise or Team account

The following table shows how retention policies affect chat conversations for users who are not members of an Amazon Chime Enterprise or Team account.

If the chat conversation includes...	The retention policy is...
Only users who are not members of an Enterprise account	Not applicable
At least one member of an Enterprise account	Automatically set to 90 days

Chat rooms created by users who do not belong to an Enterprise or Team account

The following table shows how retention policies affect chat rooms for users who are not members of an Amazon Chime Enterprise or Team account.

If the chat room is created by ...	The retention policy is...
A user who is not a member of an Enterprise or Team account	Not applicable
A Team account user	Not applicable
A member of an Enterprise account	Set by the Enterprise account's administrator

Turning on chat retention

Amazon Chime Enterprise account administrators can use the Amazon Chime console to turn chat retention on for chat conversations and chat rooms in their account. You can also use the console to update chat retention periods or turn off chat retention at any time.

To turn on chat retention

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. On the **Accounts** page, select the name of the account.
3. For **Settings**, choose **Retention**.
4. Turn on **Chat conversation retention**.
5. For **Retention period**, select the length of the retention period for chat conversations.
6. Turn on **Chat room retention**.
7. For **Retention period**, select the length of the retention period for chat room messages.

Within one day of setting a chat retention period, users in your account lose access to applicable chat messages that are outside of the chat retention period.

Restoring and deleting chat messages

As an Enterprise account administrator, you can restore chat messages to your users within 30 days of setting or updating a chat retention period. However, after the 30-day grace period, all chat messages that fall under the retention period are permanently deleted, and new chat messages are permanently deleted as soon as they pass the retention period.

> **Note**
> During the 30-day grace period, if you update a chat retention policy with a longer retention period or turn it off, chat messages that haven't passed the new retention period become visible again to users in your account.

Chat messages are also permanently deleted from Amazon Chime when an Enterprise account administrator or a member of your account performs one or more of the following actions:

- Deletes an Amazon Chime chat room
- Ends an Amazon Chime meeting in which chat messages are present

Managing messages

If you have the ability to program, you can use the Amazon Chime API to remove messages from chat rooms and conversations in your account.

Removing messages

Use the Amazon Chime API to remove reported messages from conversations and chat rooms in your organization. You must have the message ID and the conversation ID or chat room ID.

Users can report messages by sending you the message ID information. This includes the conversation ID or chat room ID. Users can choose **Copy message ID** next to a message to copy all of the message ID information to their clipboard. For more information, see Using chat features in the *Amazon Chime User Guide*.

To remove a message

- Do one of the following:
  - **For conversation messages** – Use the RedactConversationMessage API operation in the *Amazon Chime API Reference*.
  - **For chat room messages** – Use the RedactRoomMessage API operation in the *Amazon Chime API Reference*.

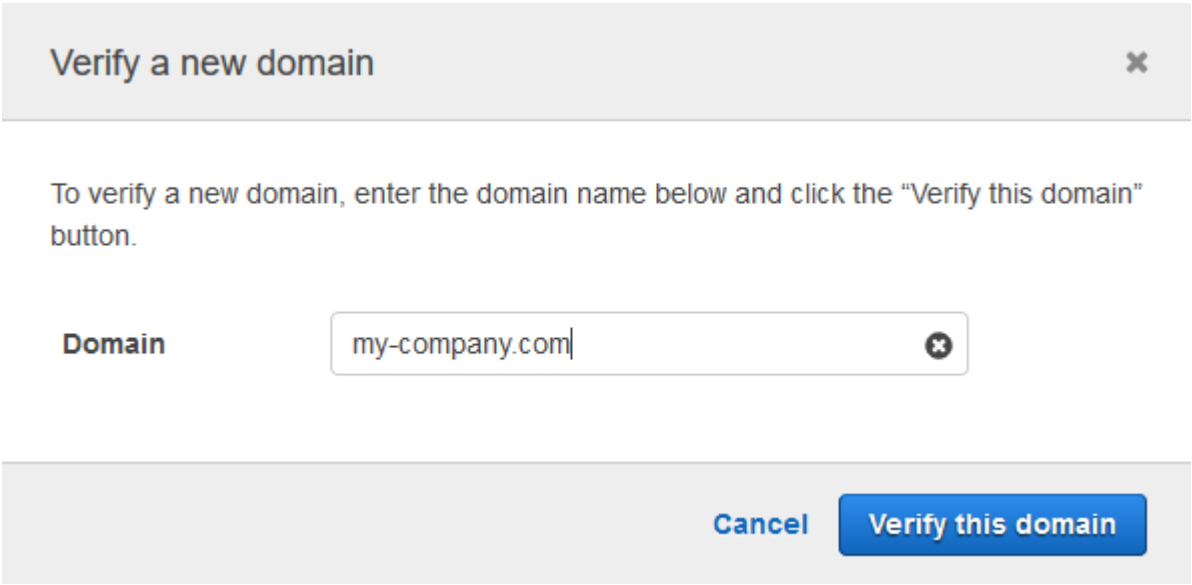
The message is removed from its conversation or chat room and can no longer be viewed.

Claiming a domain

To create an Enterprise account and benefit from the greater control that it provides over your account and users, you must claim at least one email domain.

To claim a domain

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. On the **Accounts** page, select the name of the Team account.
3. In the navigation pane, choose **Identity**, **Domains**.
4. On the **Domains** page, choose **Claim a new domain**.
5. For **Domain**, type the domain that your organization uses for email addresses. Choose **Verify this domain**.



6. Follow the directions on the screen to add a TXT record to the DNS server for your domain. In general, the process involves signing in to your domain's account, finding the DNS records for your domain, and adding a TXT record with the name and value provided by Amazon Chime. For more information about updating the DNS records for your domain, see the documentation for your DNS provider or domain name registrar.

   Amazon Chime checks for the existence of this record to verify that you own the domain. After the domain is verified, its status changes from **Pending verification** to **Verified**.

   Note
   Propagation of the DNS change and verification by Amazon Chime can take up to 24 hours.
7. If your organization uses additional domains or subdomains for email addresses, repeat this procedure for each domain.

For more information about troubleshooting domain claims, see Why isn't my domain claim request getting verified?.

Connecting to your Active Directory

When you connect your Amazon Chime administrative account to an Active Directory, you can benefit from the following capabilities:

- Your Amazon Chime users can sign in with their Active Directory credentials.
- As an Amazon Chime administrator, you choose which credential security features to add, including password rotation, password complexity rules, and multi-factor authentication.
- When you remove user accounts from your Active Directory, their Amazon Chime accounts are also removed.
- You can specify which Active Directory groups receive Amazon Chime Pro permissions.
  - Multiple groups can be configured to receive Basic or Pro permissions.
  - Users must be a member of either group to sign in to Amazon Chime.
  - Users in both groups receive a Pro license.

For more information about managing user permissions, see Managing user permissions and access (p. 61).

Prerequisites

Before you can connect to your Active Directory in Amazon Chime, you must complete the following prerequisites:

- Make sure that you have the correct AWS Identity and Access Management (IAM) permissions to configure domains, active directories, and directory groups. For more information, see Identity and access management for Amazon Chime (p. 3).
- Create a directory with AWS Directory Service that is configured in the US East (N. Virginia) Region. For more information, see the AWS Directory Service Administration Guide. Amazon Chime can connect using AD Connector, Microsoft AD, or Simple AD.
- Claim a domain in order to create an Amazon Chime Enterprise account, or convert your existing Team account to an Enterprise account. If your users have work email addresses from more than one domain, make sure to claim all of those domains. For more information, see Claiming a domain (p. 53) and Converting a Team account to an Enterprise account (p. 47).

Connecting to your Active Directory in Amazon Chime

After you connect your Active Directory to Amazon Chime, your users are prompted to sign in with their directory credentials when they use an email address from one of the domains you claimed in your Amazon Chime Enterprise account.

To connect to your Active Directory in Amazon Chime

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. In the navigation pane, for **Identity**, choose **Active directory**.
3. For **Cloud directory ID**, select the AWS Directory Service directory to use for Amazon Chime, and then choose **Connect**.

   Note
   You can find your directory ID using the AWS Directory Service console.
4. After your directory connects, choose **Add a new group**.
5. For **Group**, enter the group name. The name must exactly match an Active Directory group in the target directory. Active Directory Organization Units (OUs) are not supported.
6. For **Permissions**, choose **Basic** or **Pro**.
7. Choose **Add group**.
8. (Optional) Repeat this procedure to create additional directory groups.

Configuring multiple email addresses

After you connect to your Active Directory in Amazon Chime, users can sign in to Amazon Chime using their Active Directory credentials. Your users can have multiple email addresses assigned to them in your Active Directory. To allow your users to sign in to Amazon Chime using their Active Directory credentials, you must claim each applicable email domain in your Amazon Chime administrative account. For more information, see Claiming a domain (p. 53).

Note
If your users attempt to sign in using an email address from an unclaimed domain, they are prompted to sign in using **Log in with Amazon**. They are not able to sign in to your administrative account when using an email address from an unclaimed domain.

When viewing user details in the Amazon Chime console, Amazon Chime uses the single email address in the `EmailAddress` attribute from your Active Directory as each user's primary email address. This is the only email address that you can see for the user in the Amazon Chime console. However, users can sign in with any additional addresses listed in the `ProxyAddress` attribute, as long as you claim those domains in your Amazon Chime account.

Incorrect configuration example

A user with the **username** shirley.rodriguez is a member of an Amazon Chime account that has claimed two domains: example.com and example.org. In Active Directory, this user has the following three email addresses:

- Primary email address: shirley.rodriguez@example.com
- Proxy email address 1: shirley.rodriguez@example2.com
- Proxy email address 2: srodriguez@example.org

This user can sign into Amazon Chime using shirley.rodriguez@example.com or srodriguez@example.org and her user name shirley.rodriguez. If they attempt to sign in using shirley.rodriguez@example2.com, they are asked to **Log in with Amazon** and they are not part of your managed account. This is why it's important to claim all of the domains your users use for email.

Other Amazon Chime users can add this user as a contact, invite them to meetings, or add them as a delegate using either the shirley.rodriguez@example.com or srodriguez@example.org email address.

Correct configuration example

A user with the **username** shirley.rodriguez is a member of an Amazon Chime account that has claimed three domains: example.com, example2.com, and example.org. In Active Directory, this user has the following three email addresses:

- Primary email address: shirley.rodriguez@example.com
- Proxy email address 1: shirley.rodriguez@example2.com
- Proxy email address 2: srodriguez@example.org

This user can sign into Amazon Chime using any of their work email addresses. Other users can also add them as a contact, invite them to meetings, or add them as a delegate using any of their work email addresses.

Connecting to Okta SSO

If you have an Enterprise account, you can connect to Okta SSO to authenticate and assign user permissions.

> **Note**
> If you need to create an Enterprise account, which allows you to manage all users within a given set of email address domains, see Claiming a domain (p. 53).

Connecting Amazon Chime to Okta requires configuring two applications in the Okta Administration Console. The first application is manually configured, and uses OpenID Connect to authenticate users to the Amazon Chime service. The second application is available as **Amazon Chime SCIM Provisioning** in the Okta Integration Network (OIN). It is configured to push updates to Amazon Chime about changes to users and groups.

To connect to Okta SSO

1. Create the Amazon Chime application (OpenID Connect) in the **Okta Administration Console**:
    1. Sign in to the **Okta Administration Dashboard**, then choose **Add Application**. In the **Create New Application** dialog box, choose **Web**, **Next**.
    2. Configure the **Application Settings**:
        a. Name the application **`Amazon Chime`**.
        b. For **Login Redirect URI**, enter the following value: **`https://signin.id.ue1.app.chime.aws/auth/okta/callback`**
        c. In the **Allowed Grant Types** section, select all of the options to enable them.
        d. On the **Login initiated by** drop-down menu, choose **Either (Okta or App)**, and select all the related options.
        e. For the **Initiate Login URI**, enter the following value: **`https://signin.id.ue1.app.chime.aws/auth/okta`**
        f. Choose **Save**.

g. Keep this page open, because you'll need the **Client ID**, **Client secret**, and **Issuer URI** information for Step 2.

2. In the Amazon Chime console, follow these steps:

   1. On the **Okta single-sign on configuration** page, at the top of the page, choose **Set up incoming keys**.
   2. In the **Setup incoming Okta keys** dialog box:
      a. Paste the **Client ID** and **Client secret** information from the **Okta Application Settings** page.
      b. Paste the appropriate **Issuer URI** from the **Okta API** page. The **Issuer URI** must be an Okta domain, such as `https://example.okta.com`.

3. Set up the **Amazon Chime SCIM Provisioning** application in the **Okta Administration Console** to exchange select identity and group membership information with Amazon Chime:

   1. In the **Okta Administration Console**, choose **Applications**, **Add Application**, search for **Amazon Chime SCIM Provisioning**, and add the application.

      Important
      During the initial setup, choose both **Do not display application to users** and **Do not display application icon in the Okta Mobile App**, then choose **Done**.

   2. On the **Provisioning** tab, choose **Configure API Integration**, and select **Enable API Integration**. Keep this page open, because you'll need to copy an API access key to it for the following step.
   3. In the Amazon Chime console, choose **Create access key** to create an API access key. Copy it to the **Okta API Token** field in the **Configure API Integration** dialog box, choose **Test the Integration**, then choose **Save**.
   4. Configure the actions and attributes that Okta will use to update Amazon Chime. On the **Provisioning** tab, under the **To App** section, choose **Edit**, choose from **Enable Users**, **Update User Attributes**, and **Deactivate Users**, and choose **Save**.
   5. On the **Assignments** tab, grant users permissions to the new SCIM app.

      Important
      We recommend granting permissions through a group that contains all the users who should have access to Amazon Chime, regardless of license. The group must be the same as the group used to assign the user-facing OIDC application in step 1 previously. Otherwise, end users will not be able to sign in.

   6. On the **Push Groups** tab, configure which groups and memberships are synced to Amazon Chime. These groups are used to differentiate between Basic and Pro users.

4. Configure directory groups in Amazon Chime:

   1. In the Amazon Chime console, navigate to the **Okta single-sign on configuration** page.
   2. Under **Directory groups**, choose **Add new groups**.
   3. Type the name of a directory group to add to Amazon Chime. The name must be an exact match of one of the **Push Groups** configured previously in step 3-f.
   4. Choose whether users in this group should receive **Basic** or **Pro** capabilities, and choose **Save**. Repeat this process to configure additional groups.

      Note
      If you receive an error message stating that the group is not found, the two systems might not have completed the sync. Wait for a few minutes, and choose **Add new groups** again.

Choosing **Basic** or **Pro** capabilities for the users in your directory group affects the license, capabilities, and cost of those users in your Amazon Chime Enterprise account. For more information, see Pricing.

Deploying the Amazon Chime Add-In for Outlook

Amazon Chime provides two add-ins for Microsoft Outlook: the Amazon Chime Add-In for Outlook on Windows and the Amazon Chime Add-In for Outlook. These add-ins offer the same scheduling features, but support different types of users. Microsoft Office 365 subscribers and organizations using on-premises Microsoft Exchange 2013 or later can use the Amazon Chime Add-In for Outlook. Windows users with an on-premises Exchange server running Exchange Server 2010 or earlier and Outlook 2010 users must use the Amazon Chime Add-in for Outlook on Windows.

Windows users who do not have permissions to install the Amazon Chime Add-in for Outlook should opt for the Amazon Chime Add-in for Outlook on Windows.

For information about which add-in is right for you and your organization, see Choosing the Right Outlook Add-In.

If you choose the Amazon Chime Add-In for Outlook for your organization, you can deploy it to your users with centralized deployment. For more information, see the Amazon Chime Add-In for Outlook Installation Guide for Administrators.

Setting up the Amazon Chime Meetings App for Slack

If you are a Slack workspace administrator, you can set up the Amazon Chime Meetings App for Slack for your workspace. Your users can use Slack to start instant meetings and calls.

To set up the Amazon Chime Meetings App for Slack for your Slack workspace users

1. Choose **Add to Slack** to install the Amazon Chime Meetings App for Slack from the Slack App Directory.
2. Configure your Slack workspace **Calls** setting to **Enable calling in Slack, using Amazon Chime**.

Your Slack workspace users can now use the Amazon Chime Meetings App for Slack to start instant meetings and calls. For more information about how users can use the Amazon Chime Meetings App for Slack, see Using the Amazon Chime Meetings App for Slack in the *Amazon Chime User Guide*.

Associate your workspace with an Amazon Chime Team account to manage your users' permissions. You can upgrade meeting hosts to Amazon Chime Pro so that they can start meetings with up to 250 attendees and 16 video tiles, and include phone numbers to dial in for audio. Assign users Amazon Chime Basic permissions so they can start one-on-one meetings or join Amazon Chime meetings without being charged for active host days. For more information, see Amazon Chime Pricing.

> **Note**
> If you associate an Amazon Chime Team account with your Slack workspace, users can sign in to Amazon Chime from the Amazon Chime Meetings App for Slack. You can change this setting at any time. For more information, see Managing meeting settings (p. 49).

Before you can associate your Slack workspace with an Amazon Chime Team account, you must create an AWS account. For more information about how to create an AWS account, see Prerequisites (p. 2).

To associate your Slack workspace with an Amazon Chime Team account when installing the Amazon Chime Meetings App for Slack

1. Immediately after installing the Amazon Chime Meetings App for Slack in your Slack workspace, choose **Upgrade now**.

2. Follow the prompts to sign in to the Amazon Chime console using your AWS account credentials.
3. Follow the prompts to create a new Team account in Amazon Chime or choose an existing one.

   - **Create a new account** – Create a new Amazon Chime account to which to invite your Slack users. Enter an account name, choose whether to invite your Slack users, then choose **Create**.
   - **Choose an existing account** – Select an existing Amazon Chime account to invite your Slack users to. Select the account, then choose **Invite**.

When you invite your Slack users to join Amazon Chime, they receive an email invitation. When they accept the invitation, they are automatically upgraded to Amazon Chime Pro.

If you did not associate your Slack workspace with an Amazon Chime Team account when you installed the Amazon Chime Meetings App for Slack, you can do so after the fact by using the following steps.

To associate your Slack workspace with an Amazon Chime Team account after installing the Amazon Chime Meetings App for Slack

1. Sign in to your AWS account.
2. Sign in to your Slack workspace as an administrator.
3. Go to https://signin.id.ue1.app.chime.aws/auth/slack?purpose=app_authz.
4. Follow the prompts to create a new Team account in Amazon Chime or choose an existing one.

   - **Create a new account** – Create a new Amazon Chime account to which to invite your Slack users. Enter an account name, choose whether to invite your Slack users, then choose **Create**.
   - **Choose an existing account** – Select an existing Amazon Chime account to invite your Slack users to. Select the account, then choose **Invite**.

Managing users

In the Amazon Chime console, under **Users**, you can view a list of all the users in your account and see their user details. For more information, see Viewing user details (p. 60).

Administrators of accounts using **Login with Amazon** (LWA) also see options to manage permission tiers and remove users from the account. These actions are managed through Active Directory for accounts where Active Directory is configured and Okta for accounts where Okta is configured. For more information, see Managing user permissions and access (p. 61).

Contents

Viewing user details

In the Amazon Chime console, under **Users**, you can view a list of all the users in your account and see their user details. Search for a specific user by their email address and choose their name to see their user details. Under **User details**, you can see detailed information about the user, and make updates to their user account.

The following table lists the user details that you can view in the console.

> **Note**
> Complete user details don't appear for Team account users until after they accept their invites.

Field	Description	Example
Display name	The user's name that appears in Amazon Chime. For Login with Amazon (LWA) users, this is the full name. For Active Directory users, the DISPLAY_NAME_ATTRIBUTE is used.	Major, Mary
Email address	For LWA users, the email address used for registration. For Active Directory users, the primary email address from Active Directory appears.	mary.major@example.com

Field	Description	Example
Registration	The user's current registration status. The possible values are different between Enterprise accounts, where invitations are not sent, and Team accounts, where invitations are sent.	**Registered**, **Unregistered** (for a Team account), or **Suspended** (for an Enterprise account)
Permission tier	Set to **Pro** by default, to allow users to host meetings. It can be changed to **Basic**.	**Pro**, **Basic**
Invited	For Team accounts, the date when the user was invited to the account.	01/05/2020
Joined	The date when the user first signed into Amazon Chime. For Pro trial users, this is also the date that their Pro trial began.	01/10/2020
Personal PIN	The personal meeting PIN that the user can use to schedule meetings.	0123456789
Privacy setting	The presence setting that the user selected.	**Public** or **Private**
Meetings attended	The number of meetings that a user has attended.	87
Meetings organized	The number of meetings that a user has organized.	12
Meeting satisfaction	The percentage of positive responses given to the end-of-meeting survey.	92%
Last active date	The date when the user was last active.	06/12/2020
Chat messages sent	The number of chat messages the user sent.	1025
Phone number	The phone number assigned to a user, if any.	+12065550100

Managing user permissions and access

Manage which features your Amazon Chime users can access by assigning them Pro or Basic permissions. Users with Basic permissions cannot host meetings, but they can attend meetings and use chat. For more information about the features that users with Pro and Basic permissions can access, see Plans and pricing.

Manage who can sign into your Amazon Chime administrative account by inviting or suspending users. Only Enterprise account administrators can suspend users. Team account administrators can remove users from their accounts so that they are no longer paying for the user's permissions. However, they

can't suspend the user to prevent them from signing in. For more information about the differences between Enterprise and Team accounts, see Managing your Amazon Chime accounts (p. 46).

Managing user permissions

As an Amazon Chime administrator, you can manage Pro and Basic permissions for the users in your Amazon Chime account.

If Active Directory or Okta is configured for your Amazon Chime account, manage user permissions through their directory group membership. If you do not have Active Directory or Okta configured, manage user permissions from the Amazon Chime console.

Team accounts and Enterprise Login with Amazon

If you administer an Amazon Chime Team account or Enterprise LWA account, where users sign in with their Login with Amazon (LWA) accounts, you can manage Pro and Basic permissions in the Amazon Chime console.

To manage user permissions for Team and Enterprise LWA accounts

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Accounts**, choose the name of the Amazon Chime account.
3. Choose **Users**.
4. Select the users and choose **Actions**, **Assign permissions**.
5. Choose one of the following permissions:
   - **Pro**
   - **Basic**
6. Choose **Assign**.

Enterprise Active Directory or Enterprise OpenID Connect (Okta) accounts

If your users sign in with Active Directory or Okta credentials, manage their permissions by making them members of a directory group that has Pro or Basic permissions assigned to it.

To assign Pro permissions to a user, make them a member of an Active Directory or Okta group that you have assigned Pro permissions to. To assign Basic permissions to a user, make them a member of a group that you have assigned Basic permissions to. Users who don't have either Pro or Basic permissions aren't able to sign into Amazon Chime.

Managing user access

If you administer an Amazon Chime account, you can invite users to allow to them to sign in to your account. Enterprise account administrators can suspend user access to prevent them from signing in to the account.

Inviting and removing Team account users

If you administer a Team account, use the Amazon Chime console to invite users from any email domain.

Note
A user's free 30-day Pro trial ends when they accept your invitation.

To invite users to a Team account

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Accounts**, choose the name of the Team account.
3. Choose **Users**, **Invite users**.
4. Enter the email addresses of the users to invite, separating multiple email addresses with a semicolon (**;**).
5. Choose **Invite users**.

The following procedure disassociates users from your Team account by removing any Pro or Basic permissions assigned to them. Removed users can still sign in to Amazon Chime, but they are no longer paid members of your Amazon Chime account.

To remove users from a Team account

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Accounts**, choose the name of the Team account.
3. Choose **Users**.
4. Select the users to remove and choose **Actions**, **Remove user**.

Any Pro or Basic permissions assigned to the users are removed. The users can no longer use autocomplete to find new Team users in their **Contacts**.

Inviting and suspending Enterprise account users

If you administer an Enterprise account, any users that register for Amazon Chime with an email address from your claimed domains are automatically added to your account. If you configured Active Directory or Okta, the users must also be members of the directory group you configured for Amazon Chime.

To invite users to an Enterprise account

- Send an invitation email to the users in your organization and instruct them to follow the steps in Creating an Amazon Chime account in the *Amazon Chime User Guide*.

Users sign in with an email address from one of the domains that you claimed for your account. After they complete the steps to create their Amazon Chime user accounts, they automatically appear under your Enterprise account **Users** in the Amazon Chime console.

The following procedure suspends users from an Enterprise account that does not have Active Directory or Okta configured. This prevents the users from signing in to Amazon Chime.

To suspend users from an Enterprise account

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Accounts**, choose the name of the Enterprise account.
3. Choose **Users**.
4. Select the users to suspend and choose **Actions**, **Suspend user**.
5. Select the check box and choose **Suspend**.

If you have Active Directory or Okta configured for your Enterprise account, use the following procedure to suspend users.

To suspend users from an Enterprise Active Directory or OpenID Connect (Okta) account

- Do one of the following:
  - From your Active Directory or Okta Administrator Dashboard, suspend the user or mark them inactive.
  - Remove the user from any Active Directory group that has Basic or Pro permissions assigned to it.

Managing user phone numbers

You can use the Amazon Chime console to manage phone numbers for your Amazon Chime administrative account. For more information, see Managing phone numbers in Amazon Chime (p. 68).

The following tasks describe how to assign phone numbers to users, unassign phone numbers from users, and change calling and SMS permissions for users from the user profiles in your Amazon Chime administrative account.

> **Note**
> When you change a user's Amazon Chime Business Calling phone number or phone number permissions, we recommend contacting the user with their new phone number or permissions information. Users must also sign out of their Amazon Chime account and sign back in again before they can access their new phone number or permissions features.

Assigning phone numbers to users

Assign a phone number to a user from the Amazon Chime console.

To assign a phone number to a user

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Accounts**, choose the account name that the user belongs to.
3. In the navigation pane, choose **Users**.
4. Choose the full name of the user.
5. On the user details page, for **Actions**, choose **Assign phone number**.
6. Select the phone number to assign to the user.
7. Choose **Assign**.

The phone number is assigned to the user in your account. Calling and SMS permissions are turned off by default. For more information about editing these permissions, see Editing calling and SMS permissions (p. 64).

Editing calling and SMS permissions

Change the calling and SMS permissions for a user from the Amazon Chime console.

To edit a user's calling and SMS permissions

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Accounts**, choose the account name that the user belongs to.
3. In the navigation pane, choose **Users**.
4. Choose the full name of the user.

5. On the user details page, for **Actions**, choose **Edit telephony permissions**.
6. Select the desired calling and SMS permissions for the user, and choose **Save**.

For more information about how users can dial phone numbers and send text messages from Amazon Chime, see Dialing phone numbers with Amazon Chime in the *Amazon Chime User Guide*.

Unassigning phone numbers from users

Unassign a user's phone number using the Amazon Chime console.

To unassign a phone number from a user

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. For **Accounts**, choose the account name that the user belongs to.
3. In the navigation pane, choose **Users**.
4. Choose the full name of the user.
5. On the user details page, for **Actions**, choose **Unassign phone number**.
6. Confirm the check box is selected, and choose **Unassign**.

Changing personal meeting PINs

A personal meeting PIN is a static ID generated when the user registers. The PIN makes it easy for an Amazon Chime user to schedule meetings with other Amazon Chime users. Using a personal meeting PIN means that meeting organizers don't have to remember meeting details for each new meeting that they schedule.

If a user feels that their personal meeting PIN has been compromised, you can reset their PIN and generate a new ID. After you update a personal meeting PIN, the user must update all meetings that were scheduled using the old personal meeting PIN.

To change a personal meeting PIN

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. On the **Accounts** page, select the name of the Amazon Chime account.
3. In the navigation pane, choose **Users**.
4. Search for the user who needs their PIN changed.
5. To open the **User detail** page, choose the name of the user.
6. Choose **User actions**, **Reset personal PIN**, **Confirm**.

Managing Pro trials

When a user accepts an Amazon Chime Team invitation or is added to an Enterprise account, their free trial ends and they have Pro permissions. This enables them to continue to host meetings that are scheduled. Changing a user's permission tier to Basic prevents them from acting as a meeting host.

With Amazon Chime usage-based pricing, you only pay for users that host meetings on the days that they host them. Meeting attendees and chat users are not charged.

Pro users are considered Active Pro if they hosted a meeting that ended on a calendar day and at least one of the following occurred:

- The meeting was scheduled.
- The meeting included more than two attendees.
- The meeting had at least one recording event.
- The meeting included an attendee that dialed in.
- The meeting included an attendee that joined with H.323 or SIP.

For more information, see Plans and Pricing.

Requesting user attachments

If you manage an Enterprise account and have the appropriate permissions, you can request and receive attachments that have been uploaded into Amazon Chime by your users. You can get attachments that users uploaded into 1:1 and group conversations or into chat rooms that they created.

> **Note**
> If you manage an Amazon Chime Team account, you can upgrade to an Enterprise account by claiming one or more domains. Alternatively, you can remove users from the Team account, which enables those unmanaged users to get their attachments using the Amazon Chime Assistant.

To request user attachments

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. On the **Accounts** page, select the name of the Amazon Chime account.
3. Under **Settings**, choose **Account**, **Account actions**, **Request attachments**.
4. Within approximately 24 hours, the **Account summary** page provides a link to a file containing a list of presigned URLs that you use to access each attachment.
5. Download the file.

   > **Note**
   > Be sure to maintain an appropriate level of access control on the file. Any user that obtains the file can use the provided list of URLs to download the associated attachments. Presigned URLs expire after 6 days. You can submit a request one time every 7 days.

To use AWS Identity and Access Management (IAM) policies to manage access to the Amazon Chime administration console and the **Request attachments** action, use one of the Amazon Chime managed policies (FullAccess, UserManagement, or ReadOnly). Alternatively, you can update the custom policies to include the `StartDataExport` action and `RetrieveDataExport` action. For more information about these actions, see Actions defined by Amazon Chime in the *IAM User Guide*.

Managing Amazon Chime automatic updates

Amazon Chime provides different ways to update its clients. The method varies, depending on whether you run Amazon Chime in a browser, on your desktop, or on a mobile device.

The Amazon Chime web application – https://app.chime.aws – always loads with the latest features and security fixes.

The Amazon Chime desktop client checks for updates whenever you choose **Quit** or **Sign Out**. This applies to Windows and macOS machines. As you run the client, it checks for updates every three hours. You can also check for updates by choosing **Check for Updates** on the Windows Help menu or on the macOS **Amazon Chime** menu.

When the desktop client detects an update, Amazon Chime prompts user to install it unless they're in an ongoing meeting. They're in an *ongoing meeting* when:

- They attend a meeting.
- They were invited to a meeting that is still in progress.

Amazon Chime prompts them to install the latest version, and it provides a 15-second countdown so they can postpone the installation. Users choose **Try Later** to postpone the update.

If users postpone an update, and they aren't in an ongoing meeting, the client checks for the update after three hours and prompts them again to install. The installation begins when the countdown ends.

> **Note**
> On a macOS machine, users need to choose **Restart Now** to begin the update.

On mobile devices – Amazon Chime mobile applications use the update options provided by the App Store and Google Play to deliver the latest version of the Amazon Chime client. You can also use mobile device management system to deploy updates.

Managing phone numbers in Amazon Chime

Use the Amazon Chime console to provision phone numbers. Choose from Amazon Chime Business Calling or Amazon Chime Voice Connector phone numbers.

Amazon Chime Business Calling

Lets your users send and receive phone calls and text messages directly from Amazon Chime. Provision your phone numbers in the Amazon Chime console at https://chime.aws.amazon.com/, or port in existing phone numbers. Assign the phone numbers to your Amazon Chime users and grant them permissions to send and receive phone calls and text messages using Amazon Chime.

Note
Text messaging to and from short codes or short numbers is not supported.

Amazon Chime Voice Connector

Provides Session Initiation Protocol (SIP) trunking service for an existing phone system. Port in existing phone numbers or provision new phone numbers in the Amazon Chime console. 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. 76).

Note
Amazon Chime does not offer emergency calling services. If you want to contact emergency calling services in the United States with Amazon Chime, you must obtain an emergency call routing number from a third-party emergency service provider and provide it to Amazon Chime. For more information, see Setting up emergency call routing numbers for your Amazon Chime Voice Connector (p. 78).

There are bandwidth requirements for using Amazon Chime Business Calling and integrating an Amazon Chime Voice Connector. For more information, see Bandwidth requirements (p. 98).

Contents

Provisioning phone numbers

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

- Amazon Chime Business Calling – Provision and assign phone numbers to your existing Amazon Chime users.
- Amazon Chime Voice Connectors – Integrate with an existing phone system. For more information, see Managing Amazon Chime Voice Connectors (p. 76).

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. 77).

To provision phone numbers

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 **Business Calling** or **Voice Connector**, and 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.

To provision Puerto Rican phone numbers

1. Do one of the following:
   - Open the Amazon Chime console at https://chime.aws.amazon.com/ and 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**, **Technical support**, and for **Service**, choose **Chime**.
2. For **Category**, choose **Other**.
3. For **Subject**, enter **`Puerto Rico telephone number request`**.
4. For **Issue** or **Description**, enter the number of phone numbers you want to order and the preferred zone or city. Indicate the phone number type, **Business Calling** or **Voice Connector**.
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 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.

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 sends email messages to 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 AWS Support Center, you receive responses based on your selected contact methods and any email addresses you entered for additional contacts.

If the quantity of numbers that you requested is available, your order takes about a week to complete. If not, your order takes longer, or operations may ask you to choose numbers from a different zone, though that's rare.

Porting existing phone numbers

If you want to turn on Amazon Chime Business Calling for your Amazon Chime users, or if you want to use an Amazon Chime Voice Connector for SIP trunking with an existing phone system, you have the

option to provision new phone numbers in the Amazon Chime console. However, if you want to keep your existing phone numbers, you can port United States phone numbers from your phone carrier. To start the porting process, submit a support request from the Amazon Chime console. Porting can take between 2-4 weeks.

Before you can port phone numbers for Amazon Chime Voice Connectors, you must create an Amazon Chime Voice Connector. For more information, see Creating an Amazon Chime Voice Connector (p. 77).

Note
You can port toll-free numbers for Amazon Chime Voice Connectors. Toll-free numbers are not currently supported for Amazon Chime Business Calling.

Porting phone numbers into Amazon Chime

Create a support request to port existing phone numbers into Amazon Chime.

Before you start porting, download the Letter of Agency (LOA) for Local Telephone Number Porting and fill it out. If you are porting phone numbers from different carriers, fill out a separate LOA for each carrier.

To port existing phone numbers into Amazon Chime

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:
   - Existing phone numbers to port in. Indicate the phone number type, **Business Calling** or **Voice Connector**.
   - 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 are porting 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.)
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 **Attachments**, choose **Choose files**, and attach the LOA. For **Contact options**, select a contact method. Optionally, for **Additional contacts**, enter email addresses of people to be notified of case status updates.

6. AWS Support responds to your support request to let 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 and Cost Management 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.

7. If your phone numbers can be ported, one of the following happens:

   - If you submitted a support request from the Amazon Chime console, AWS Support asks you to provide your completed Letter of Agency (LOA). If you are porting phone numbers from different carriers, fill out a separate LOA for each carrier. This authorizes your existing phone carrier to release your existing phone numbers for porting.
   - If you created a case in AWS Support Center and attached your completed LOA, AWS Support proceeds to step 8.

8. After you provide the 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.
9. (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. 72).
10. Assign the ported phone numbers to individual users as Amazon Chime Business Calling phone numbers, or assign the phone numbers to Amazon Chime Voice Connectors that you create. 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. 73) and Creating an Amazon Chime Voice Connector (p. 77).
11. 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.
12. AWS Support contacts you with the FOC to confirm that the date and time works for you.
13. On the FOC date, the ported phone numbers are activated for use with Amazon Chime.

Porting phone numbers out of Amazon Chime

To port existing phone numbers out of Amazon Chime

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, **Business Calling** or **Voice Connector**.
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 and Cost Management 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 inventory. For more information, see Managing phone number inventory (p. 73) and Deleting phone numbers (p. 75).

Phone number porting status definitions

After you submit a request to port existing phone numbers into Amazon Chime, 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 Amazon Chime Business Calling phone numbers for individual users, or phone numbers for Amazon Chime Voice Connectors or Amazon Chime Voice Connector groups.

Manage Amazon Chime Business Calling phone numbers from within user profiles. Manage Amazon Chime Voice Connector phone numbers on the corresponding **Voice connectors** or **Voice connector groups** page. For more information, see Managing user phone numbers (p. 64), Assigning and unassigning Amazon Chime Voice Connector phone numbers (p. 79), or Assigning and unassigning phone numbers for an Amazon Chime Voice Connector group (p. 81).

To assign an Amazon Chime Business Calling phone number to a user

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 Amazon Chime Business Calling phone number to assign to a user.
4. Choose **Assign**.
5. Select the account that the user belongs to, and choose **Next**.
6. Select the user's full name, and choose **Assign**.

For instructions on how to edit the user's calling and SMS permissions, see Editing calling and SMS permissions (p. 64). 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.

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

To unassign inventory 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 to unassign.
4. Choose **Unassign**.
5. Select the check box, and choose **Unassign**.

You can then view the details about your inventory phone numbers. You can see which user or Amazon Chime Voice Connector 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 to view details for.
4. For **Actions**, choose **View details**.

If you have unassigned Amazon Chime Business Calling and Amazon Chime Voice Connector phone numbers, you can switch them from one product type to another.

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 to change product types for.
4. Select **Business Calling** or **Voice Connector**, 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**.

The default calling name is updated within 72 hours.

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 unique calling name is updated within 72 hours. After the update is complete, you can update the calling name again.

Deleting phone numbers

Delete unassigned phone numbers from your phone number management **Inventory**. For more information about unassigning phone numbers, see Managing phone number inventory (p. 73).

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. 69), Provisioning phone numbers (p. 68), and Assigning and unassigning Amazon Chime Voice Connector phone numbers (p. 79).

> **Note**
> Amazon Chime Voice Connectors don't support international calls. Instead, you use a local number to dial internationally, and you pay a per-minute rate. For a current list of the countries in which Amazon Chime is available, and the call rates for each country, see https://aws.amazon.com/chime/call-me-rates/.

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. 80).

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 Amazon Chime (p. 25) and Streaming Amazon Chime Voice Connector media to Kinesis (p. 82).

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. 98).

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. 97).

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. 78).
    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. 79).

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

Amazon Chime does not offer emergency calling services. If you would like to contact emergency calling services in the United States with Amazon Chime, you must obtain an emergency call routing number from a third-party emergency service provider and provide it to Amazon Chime. When you place a call to emergency services (such as a 911 call), Amazon Chime uses your emergency call routing number to route your call to your emergency services provider via the public switched telephone network (PSTN). Your third-party emergency service provider then routes your call to emergency services.

Note
Amazon Chime is not responsible for routing calls to emergency services.

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

- Obtain emergency call routing numbers from a third-party emergency service provider.
- 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. 77).

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 **Phone number management** inventory. For more information, see Provisioning phone numbers (p. 68). For more information about creating Amazon Chime Voice Connectors in different AWS Regions, see Managing Amazon Chime Voice Connectors (p. 76).

Contents

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 roles to stream Amazon Chime Voice Connector media to Kinesis (p. 15). For more information about using Amazon CloudWatch with Amazon Chime, see Logging and monitoring in Amazon Chime (p. 19).

When you enable media streaming for your Amazon Chime Voice Connector, Amazon Chime 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. 87).

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. 76).

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. 77).
2. Start media streaming for your Amazon Chime Voice Connector. For more information, see Starting media streaming (p. 83).
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 global settings in Amazon Chime

Manage call detail record settings from the Amazon Chime console.

Configuring call detail records

Before you can configure call detail record settings for your Amazon Chime 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 Amazon Chime 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 Getting Started Guide*.

You can configure call detail record settings for Amazon Chime Business Calling and for Amazon Chime Voice Connectors. For more information about Amazon Chime Business Calling and Amazon Chime Voice Connectors, see Managing phone numbers in Amazon Chime (p. 68).

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 Getting Started Guide*.
2. Open the Amazon Chime console at https://chime.aws.amazon.com/.
3. For **Global Settings**, choose **Call detail records**.
4. Choose one or both of the following configurations:
   - **Business Calling Configuration**
   - **Voice Connector 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 Business Calling call detail records

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

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

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

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

The following example shows the general format of an Amazon Chime Business Calling call detail record.

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

    "CallerPhoneNumber": "+12065550100",
    "CallerCountry": "US",

    "DestinationPhoneNumber": "+12065550101",
    "DestinationCountry": "US",

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

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. 82).

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"
}
```

Setting up Amazon Chime on Dolby hardware

If you manage small or medium-size conference rooms and want your users to join meetings conveniently, Amazon Chime offers a native or first-party meeting experience on Dolby Voice Room and Dolby Voice Huddle audio and video conferencing hardware. When Dolby Voice Room or Dolby Voice Huddle is enabled with Amazon Chime, users can join an Amazon Chime meeting quickly from a conference room. In-room calendar integration lets attendees quickly select a meeting with a single tap. When Amazon Chime Business Calling is enabled, you can associate a phone number with the device to use to receive inbound and place outbound calls.

When Alexa for Business is enabled for Dolby Voice Room, meeting attendees can ask Alexa to join a meeting.

To ensure a seamless out-of-box experience, go to http://aws.amazon.com/chime/devices to learn how to order Dolby Voice Room and Dolby Voice Huddle systems from Dolby partners.

Contents

Preparing for setup

There are two ways to set up Amazon Chime on Dolby hardware. If your company has an Enterprise Active Directory account, you can set it up in a shared conference room that many attendees can use. As a shared conference room device, organizers invite the conference room to a meeting. Attendees in the room can join with a single tap. When Alexa for Business is enabled for Dolby Voice Room, attendees can also join with a voice command using Alexa.

Alternately, you can associate Dolby hardware with a single, dedicated user. As a dedicated device, the Dolby Voice Room or Dolby Voice Huddle device is paired with an Amazon Chime profile. This lets the user conveniently select a meeting to join, just like they would using a desktop or mobile client. Dedicated devices can only be paired with registered profiles with either Basic or Pro permission. Make sure that the user is registered before proceeding.

To prepare setup for a shared conference room

1. Create an administrator group to manage the conference room devices called a delegate group:
    1. Create or identify an Active Directory group that consists of administrators who can use their Amazon Chime credentials to set up devices.
    2. Open the Amazon Chime console and choose the Amazon Chime Enterprise Directory account.
    3. Choose **Identity**, **Delegates**, and **Add a new group**.

4. Enter the Active Directory group name that contains the users who have permissions to use their Amazon Chime to set up Dolby devices in conference rooms (for example, IT-AudioVisual-owners).

   Note
   These users must have Basic or Pro permissions to use Amazon Chime and be a part of an Active Directory group. For more information, see the section called "Managing user permissions and access" (p. 61).

2. Create a profile for the conference room:

   1. Make sure that your conference room is set up as a resource in your calendaring system.
   2. Get the email address used when inviting the resource to a meeting.
   3. Open the Amazon Chime console and choose the Amazon Chime Enterprise Directory account.
   4. To create a shared device profile, choose **Users**, **Shared devices**, **Create shared device profile**, enter the email address of the conference room, and choose **Create**.

3. Set up a phone number for the device to use for inbound and outbound calling. To do this, use Amazon Chime Business Calling to provision a phone number and assign a number from the phone number Inventory to the shared device profile. For more information, see *Managing phone numbers* (p. 68).

   Note
   You can also complete this step after pairing the device below.

4. If you want to enable Alexa on a Dolby Voice Room device, first set up Alexa for Business. For information, see the Alexa for Business Administration Guide. Then, follow these steps to enable it:

   Note
   You can also complete this step after pairing the device below.

   1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
   2. Choose **Users**, **Shared devices**, select a device, then choose **Actions** and **Enable Alexa for Business**.

To prepare setup for a single user

1. Set up a phone number for the device to use for inbound and outbound calling. To this, use Amazon Chime Business Calling to provision a phone number and assign a number from the phone number Inventory to the shared device profile. For more information, see *Managing phone numbers* (p. 68).

   Note
   You can also complete this step after pairing the device below.

2. Set up an Amazon Chime user profile to allow it to be associated with a Dolby device. When an Amazon Chime user profile is set up for a Dolby Voice Room device, it can then use Alexa for Business.

   1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
   2. Select the Amazon Chime account.
   3. Using the email address, locate the user's profile to be used for the Dolby device.

      Note
      This user must have a registered Amazon Chime account.

   4. To edit the user's profile, select the account, choose **Users**, select the user to open the user detail page, choose **User actions**, **Edit profile type**, and **Shared device profile**.

3. If you want to enable Alexa on a Dolby Voice Room device, first set up Alexa for Business. For information, see the Alexa for Business Administration Guide. Then, follow these steps to enable it:

   Note
   You can complete this step after device pairing.

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. Choose **Users**, **Shared devices**, select a device, then choose **Actions** and **Enable Alexa for Business**.

Setting up the Dolby hardware

Before you proceed, make sure that you have a physical Ethernet network connection and cables. Confirm that your firewall rules enable your Dolby hardware to connect with Amazon Chime. See *Network configuration and bandwidth requirements* (p. 96) for firewall host, port, and protocol requirements.

Setting up Dolby Voice Room

The Amazon Chime on Dolby Voice Room hardware consists of three components: the hub, conference phone (with a small screen), and camera. Follow these steps to connect them together.

To set up the hardware

1. Connect an Ethernet cable from the hub to a network source.

   Note
   Make sure that you don't connect the Ethernet cable from the phone to the network source. You might not receive the proper version of the device firmware and setup won't work.
2. Connect a second Ethernet cable from the hub to the phone.
3. Use either the short or long USB cable (depending on the distance that you want) to connect the camera to the USB port on the hub (identified by a camera icon).

   Note
   You can perform this step now or at any time.
4. Connect the power cable to the power port in the hub and an electrical outlet.
5. Verify that you see either the Amazon Chime logo on the small screen of the conference phone, or Amazon Chime under **Select your Dolby Voice service provider**. Then select the logo or **Amazon Chime**.
6. Choose the following settings when prompted:

   1. Under **Select time zone**, select the local time zone.
   2. Under **Network setup**, choose **Next**.
7. Confirm that you see the following message on both screens of the device: **Visit app.chime.aws/pair/input to sign in and activate your device**.

Setting up Dolby Voice Huddle

The Amazon Chime on Dolby Voice Huddle hardware consists of two components: the hub (with a built-in camera), and a touch screen. Follow these steps to connect them together.

To set up the hardware

1. Connect an Ethernet cable from the hub to a network source.
2. Connect the touch screen to the USB port on the hub.

   Note
   You can perform this step now or at any time.
3. Connect the power cable to the power port in the hub and an electrical outlet.

4. Choose the following settings when prompted:
    1. Under **Select time zone**, select the local time zone.
    2. Under **Network setup**, choose **Next**.
    3. Under **Provisioning setup**, choose **Amazon Chime**.
5. Confirm that you see the following message on both screens of the device: **Visit app.chime.aws/pair/input to sign in and activate your device**.

Pairing a Dolby device

Depending on whether you are setting up a Dolby device in a shared room or for a single user, perform one of the following procedures.

To pair a Dolby device for a shared conference room

1. Open a browser window on your laptop or phone, then go to https://app.chime.aws/pair/input.
2. On the **Pair device** screen, enter the 8-digit pairing code that appears on the large screen and choose **Next**.

    Note
    The pairing code automatically refreshes after 10 minutes.
3. On the **Sign into Dolby Voice Room?** or **Sign into Dolby Voice Huddle?** screen, choose **Continue**.
4. Enter the email address of an admin user who has permissions to configure the conference room, and choose **Sign in**.
5. When asked to **Allow access to your Amazon Chime profile**, choose **Allow**.
6. Enter the Amazon Chime **Username** and **Password** associated with an admin user who has permissions to set up conference rooms.
7. On the **Select Profile** page, select the room name from the list and choose **Sign in**.
8. If pairing is successful, you receive a **Sign in successful** message.

To pair a Dolby device for a single user

1. Open a browser window on your laptop or phone, then go to https://app.chime.aws/pair/input.
2. On the **Pair device** screen, enter the 8-digit pairing code that appears on the large screen and choose **Next**.

    Note
    The pairing code automatically refreshes after 10 minutes.
3. On the **Sign into Dolby Voice Room?** or **Sign into Dolby Voice Huddle?** screen, choose **Continue**.
4. Enter the user's email address and choose **Sign in**.
5. When asked to **Allow access to your Amazon Chime profile**, choose **Allow**.
6. Complete the sign-in process based on your company's Amazon Chime account settings.
7. If pairing is successful, you receive a **Sign in successful** message.

Setting up a Dolby Voice Room whiteboard

The Dolby Voice Room whiteboard framing feature allows users to share drawings on any surface, such as a dry-erase whiteboard, with meeting participants. This requires a one-time setup process to register the position of the whiteboard with the Dolby Voice Camera.

The whiteboard configuration wizard lets you register the whiteboard position with the Dolby Voice Camera for optimal results. Before you start the setup process, we recommend that you draw something on the whiteboard and clearly mark all four corners. This lets you evaluate the quality of the setup.

To set up a Dolby Voice Room whiteboard

1. On the device, choose **Settings**, **Device Settings**, **Dolby Voice Camera**, and set the mode to **Whiteboard**.
2. Choose **Configure whiteboard** from the list of options.
3. Use the volume up/down button on the device to adjust the zoom and choose the check icon.
4. Use the controls on the device screen to drag the on-screen markers to the corresponding corners of your whiteboard.
5. When the anchor points on the large screen in the room, align to the corners of the whiteboard. Then choose the check icon to preview the frame.
6. Choose **Save** to save the configuration, or **Change** to make additional changes.

Verifying Dolby device settings

You can view and configure settings for your Dolby device at any time.

To verify device settings

- From any Amazon Chime screen on the device, choose **Settings**, and then choose the following:
  - **Meeting and phone information** - View the **Meeting room name**, **Chime meeting ID**, **Business calling number** (if applicable), and **Device phone number** (if applicable).
  - **Device settings** – Configure the following settings for the Dolby device. When you're done, choose the home icon to return to Amazon Chime.
    - **Preferences**
      - **Adjust brightness (Dolby Voice Room only)**
      - **Language (Dolby Voice Huddle only)**
      - **Time zone**
      - **Time format**
      - **Date format**
    - **Dolby Voice Camera (for Dolby Voice Room)**
      - **Change mode**
      - **Adjust image quality**
      - **Position and zoom**
      - **Reset camera settings**
    - **Dolby Voice Camera (for Dolby Voice Huddle)**
      - **Brightness level**
      - **Enable high dynamic range**
      - **Color intensity**
      - **Contrast**
  - **Reboot** – This option reboots the system.
  - **Exit Chime (for Dolby Voice Room only)** - This option takes you to the device home screen to access more device settings. The device remains signed into Amazon Chime. To return to the Amazon Chime screen, choose the Amazon Chime button.
  - **Sign out** – Choose this option if you need to change the room name or dedicated user. Enter the Dolby Video Room or Dolby Video Huddle administrator password when prompted.

Verifying setup of Amazon Chime on Dolby hardware

To make sure that everything is working correctly after you set up Amazon Chime on Dolby hardware, check the following.

To verify setup

1. To make sure that Amazon Chime is working:
    1. Create a scheduled meeting and invite the shared conference room or dedicated user profile to the meeting.
    2. Make sure that you invite meet@chime.aws.
    3. At meeting time, the meeting name appears on the Dolby Voice Room or Dolby Voice Huddle screen.
    4. (Optional) For Dolby Voice Room devices, choose **Share screen** and **Share whiteboard** to test the features.
2. To make sure that Business Calling is working, make an inbound and outbound call by pressing the **Call** button.
3. (Optional) For Dolby Voice Room devices, to make sure that Alexa for Business is enabled, open the Alexa for Business console and choose **Rooms**. Select the room, and verify the Dolby hub serial number under **Shared devices**.

Conference room configuration

Amazon Chime can integrate with your in-room video hardware from Cisco, Tandberg, Polycom, Lifesize, Vidyo, or others when you use the SIP or H.323 protocol.

To connect to Amazon Chime using a conference room VTC device that supports SIP, enter one of the following options:

- **`@meet.chime.in`**
- **`u@meet.chime.in`**
- A 10-digit meeting ID followed by **`@meet.chime.in`**

`meet.chime.in` connects your SIP room device to the nearest Amazon Chime Region. To connect to a specific Region, use Region-specific DNS entries for SIP room systems. For more information, see Session Initiation Protocol (SIP) room systems (p. 97).

> **Note**
> If your SIP room device does not support TLS and requires TCP connectivity, contact AWS Support.

If you are using a device that supports only H.323, you must dial one of the following:

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

If a firewall is filtering traffic between the VTC device and Amazon Chime, open the ranges for the protocols used. For more information, see Network configuration and bandwidth requirements (p. 96).

On the Amazon Chime welcome screen, enter the 10-digit or 13-digit meeting ID to join. You can find the 13-digit meeting ID in the Amazon Chime client or web app, or choose the **Dial-in** option.

Joining a moderated meeting

If the meeting is moderated and you are the host or delegate, enter your 13-digit meeting ID to join the meeting as a moderator. If you are a moderator, enter the moderator passcode in the dialpad followed by the pound sign (#) to join and start the meeting. If you are not a host, delegate, or moderator, you are connected to the meeting after a moderator joins and starts the meeting.

Moderators have host controls, which means that they can perform additional meeting actions. These actions include starting and stopping recording, locking and unlocking the meeting, muting all other attendees, and ending the meeting. For more information, see Moderator Actions using phone or in-room video systems in the *Amazon Chime User Guide*.

> **Note**
> If you are using Alexa for Business to join your Amazon Chime meetings, you can join as a moderator only if your device is connected to an in-room video system and you dial in by using the device's dialpad.

Compatible VTC devices

The following table is a subset of the compatible VTC devices list.

Device	SIP	H.323	Comment
Cisco SX20	Yes	Yes	Audio/Video/Screen: To and From OK
Cisco DX80	Yes	Yes	Audio/Video/Screen: To and From OK
Lifesize Icon	Yes	No	Audio/Video/Screen: To and From OK
Polycom Debut	Yes	Yes	Audio/Video/Screen: To and From OK
Polycom RealPresence Desktop	No	Yes	Audio/Video: OK, Screen: From device is OK
Polycom Trio	Yes	Yes	Audio/Video/Screen: To and From OK
Tandberg C40	Yes	Yes	Audio/Video/Screen: To and From OK

Network configuration and bandwidth requirements

Amazon Chime 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.

Amazon Chime 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 Amazon Chime in your environment.

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

Meetings and Business Calling

Amazon Chime uses the following destination and port for meetings and Amazon Chime Business Calling.

Destination	Ports
99.77.128.0/18	UDP/3478

H.323 room systems

Amazon Chime uses the following destinations and ports for H.323 in-room video systems.

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

Session Initiation Protocol (SIP) room systems

The following destinations and ports are recommended when running Amazon Chime for SIP in-room video systems in your environment.

AWS Region	Destination	Ports
Global (nearest Region)	99.77.128.0/18 34.212.95.128/25 34.223.21.0/25 52.55.62.128/25 52.55.63.0/25	UDP/10000:60000
Global	meet.chime.in 13.248.147.139 76.223.18.152	TCP/5061
US East (N. Virginia)	meet.ue1.chime.in	TCP/5061
US West (Oregon)	meet.uw2.chime.in	TCP/5061
Asia Pacific (Singapore)	meet.as1.chime.in	TCP/5061
Asia Pacific (Sydney)	meet.as2.chime.in	TCP/5061
Asia Pacific (Tokyo)	meet.an1.chime.in	TCP/5061
Europe (Ireland)	meet.ew1.chime.in	TCP/5061
South America (São Paulo)	meet.se1.chime.in	TCP/5061

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
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

Amazon Chime 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.

Viewing reports

To make more informed decisions and increase productivity for your organization, you can access usage and feedback data directly from the console. Report data is updated daily, though there may be a delay of up to 48 hours.

To view usage and feedback reports

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. Choose **Reports**, **Dashboard**.
3. On the **Usage and feedback dashboard report** page, view the following data:

   Note
   For more information about available data, see Amazon Chime Report Dashboard and User Activity details.

   - **Date range (UTC)**—The date range of the report.
   - **Registered users**—The number of users who have signed up for Amazon Chime.
   - **Active users**—The number of users who have either attended a meeting or sent a message with Amazon Chime.
   - **Meetings held**—The total number of meetings that have ended. You can select a specific meeting to view details, including the conference ID, start time, type, organizer, duration, and number of attendees. Choose a specific **Conference ID** or **Meeting organizer** value to view additional details, including attendees, meeting roster events, type of client, and meeting feedback.
   - **Meeting satisfaction**—The percentage of positive responses given to the end-of-meeting survey.
   - **Chat messages sent**—The number of chat messages that users sent.

Administrative support for Amazon Chime

If you are an administrator and need to contact support for Amazon Chime, 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.
- Your Amazon Chime version. To find your version number:
  - In Windows, choose **Help**, **About Amazon Chime**.
  - In macOS, choose **Amazon Chime**, **About Amazon Chime**.
  - In iOS and Android, choose **Settings**, **About**.
- The log reference ID. To find this ID:
  - In Windows and macOS, choose **Help**, **Send Diagnostic Logs**.
  - In iOS and Android, choose **Settings**, **Send Diagnostic Logs**.
- If your issue is related to a meeting, the meeting ID.

Document history for Amazon Chime

The following table describes important changes to the *Amazon Chime Administrator Guide*, beginning in March 2018. For notifications about updates to this documentation, you can subscribe to an RSS feed.

update-history-change	update-history-description	update-history-date
Amazon Chime Voice Connector emergency call routing numbers (p. 102)	Amazon Chime administrators can set up emergency call routing numbers for an Amazon Chime Voice Connector. For more information, see Setting up emergency call routing numbers for your Amazon Chime Voice Connector in the Amazon Chime Administrator Guide.	July 1, 2020
Amazon Chime on Dolby Voice Huddle (p. 102)	Amazon Chime offers a native or first-party meeting experience on Dolby Voice Huddle audio and video conferencing hardware. For more information, see Setting up Amazon Chime on Dolby Hardware in the Amazon Chime Administrator Guide.	June 3, 2020
Setting chat retention policies (p. 102)	Amazon Chime administrators can set chat retention policies for their Enterprise accounts. For more information, see Managing chat retention policies in the Amazon Chime Administrator Guide.	May 21, 2020
Removing chat messages (p. 102)	If you have the ability to program, you can use the Amazon Chime API to remove messages from chat rooms and conversations in your account. For more information, see Managing messages in the Amazon Chime Administrator Guide.	May 18, 2020
CloudWatch media quality metrics for Amazon Chime Voice Connector (p. 102)	Amazon Chime supports sending media quality metrics for your Amazon Chime Voice Connector to CloudWatch. For more information, see Monitoring Amazon Chime with CloudWatch in the Amazon Chime Administrator Guide.	January 23, 2020
Amazon Chime Meetings App for Slack (p. 102)	Amazon Chime supports the Amazon Chime Meetings App for	December 4, 2019

	Slack. For more information, see Setting up the Amazon Chime Meetings App for Slack in the Amazon Chime Administrator Guide.	
Meeting Region settings (p. 102)	Amazon Chime supports processing meetings in the optimal AWS Region for all participants. For more information, see Meeting Region settings in the Amazon Chime Administrator Guide.	December 3, 2019
SIP-based media recording (SIPREC) compatibility (p. 102)	Amazon Chime Voice Connectors support streaming media from a SIPREC-compatible voice infrastructure to Kinesis Video Streams. For more information, see SIP-based media recording (SIPREC) compatibility in the Amazon Chime Administrator Guide.	November 25, 2019
Amazon Chime on Dolby Voice Room (p. 102)	If you want users to join meetings conveniently, Amazon Chime offers a native or first-party meeting experience on Dolby Voice Room audio and video conferencing hardware. For more information, see Setting up Amazon Chime on Dolby Voice Room in the Amazon Chime Administrator Guide.	October 29, 2019
Updating outbound calling names (p. 102)	Set a default calling name that appears to recipients of outbound calls made using phone numbers in your Amazon Chime inventory. For more information, see Updating outbound calling names in the Amazon Chime Administrator Guide.	October 24, 2019
Streaming media to Amazon Kinesis (p. 102)	Stream phone call audio from Amazon Chime Voice Connectors to Kinesis Video Streams for analytics, machine learning, and other processing. For more information, see Streaming Amazon Chime Voice Connector media to Kinesis and Using roles to stream Amazon Chime Voice Connector media to Kinesis in the Amazon Chime Administrator Guide.	October 24, 2019

Monitoring Amazon Chime with Amazon CloudWatch (p. 102)	Monitor Amazon Chime using CloudWatch, which collects raw data and processes it into readable, near real-time metrics. For more information, see Monitoring Amazon Chime with CloudWatch in the Amazon Chime Administrator Guide.	October 24, 2019
Amazon Chime Voice Connector groups (p. 102)	Create an Amazon Chime Voice Connector group that includes Amazon Chime Voice Connectors 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 more information, see Working with Amazon Chime Voice Connector groups in the Amazon Chime Administrator Guide.	October 24, 2019
Network configuration updates (p. 102)	Amazon Chime is simplifying its firewall requirements. For more information, see Network configuration and bandwidth requirements in the Amazon Chime Administrator Guide.	September 6, 2019
Moderated meetings (p. 102)	Amazon Chime supports moderated meetings. For more information, see Joining a moderated meeting in the Amazon Chime Administrator Guide.	July 25, 2019
Compliance validation for Amazon Chime (p. 102)	Amazon Chime is a HIPAA Eligible Service. For more information, see Compliance validation for Amazon Chime in the Amazon Chime Administrator Guide.	June 11, 2019
Porting toll-free phone numbers (p. 102)	Amazon Chime supports porting toll-free United States phone numbers for use with Amazon Chime Voice Connectors. For more information, see Porting existing phone numbers in the Amazon Chime Administrator Guide.	May 28, 2019

Managing phone numbers in Amazon Chime (p. 102)	Use Amazon Chime Business Calling to provision and assign phone numbers to Amazon Chime users. Integrate an Amazon Chime Voice Connector with an existing phone system. For more information, see Managing phone numbers in Amazon Chime in the Amazon Chime Administrator Guide.	March 18, 2019
Amazon Chime Add-In for Outlook (p. 102)	Amazon Chime provides two add-ins for Microsoft Outlook: the Amazon Chime Add-In for Outlook on Windows and the Amazon Chime Add-In for Outlook. These add-ins offer the same scheduling features, but support different types of users. For more information, see Deploying the Add-In for Outlook in the Amazon Chime Administrator Guide.	March 12, 2019
Various updates (p. 102)	Various updates to topic layout and organization.	February 11, 2019
Amazon Chime call me feature (p. 102)	Administrators can enable the Amazon Chime call me feature under their **Meetings** settings. For more information, see Managing meeting settings in the Amazon Chime Administrator Guide.	August 22, 2018
Connect to Okta SSO (p. 102)	If you have an enterprise account, you can connect to Okta SSO to authenticate and assign user permissions. For more information, see Connect to Okta SSO in the Amazon Chime Administrator Guide.	August 1, 2018
Request user attachments (p. 102)	Receive attachments uploaded into Amazon Chime by users. For more information, see Request user attachments in the Amazon Chime Administrator Guide.	April 23, 2018
View additional report data (p. 102)	View additional report data. For more information, see View reports in the Amazon Chime Administrator Guide.	March 30, 2018

Assign users Pro or Basic permissions (p. 102)	Assign users Pro or Basic permissions. For more information, see Manage user access and permissions in the Amazon Chime Administrator Guide.	March 29, 2018

AWS glossary

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