aws

Administration Guide

Amazon Chime

Amazon Chime: Administration Guide

Table of Contents

You must be an Amazon Chime system administrator to complete the steps in this guide. If you need help with the Amazon Chime desktop client, web app, or mobile app, see Getting support in the *Amazon Chime User Guide*.

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 for Amazon Chime system administrators.

How to get started

After you complete the Prerequisites for Amazon Chime system administrators, 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

For more information on user access and permissions, see Managing user permissions and access. 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 for Amazon Chime system administrators

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. chime

Topics

- [Sign up for an AWS account](#)
- [Create a user with administrative access](#)

Sign up for an AWS account

If you do not have an AWS account, complete the following steps to create one.

To sign up for 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.

   When you sign up for an AWS account, an *AWS account root user* is created. The root user has access to all AWS services and resources in the account. As a security best practice, assign administrative access to a user, and use only the root user to perform [tasks that require root user access](#).

AWS sends you a confirmation email after the sign-up process is complete. At any time, you can view your current account activity and manage your account by going to https://aws.amazon.com/ and choosing **My Account**.

Create a user with administrative access

After you sign up for an AWS account, secure your AWS account root user, enable AWS IAM Identity Center, and create an administrative user so that you don't use the root user for everyday tasks.

Secure your AWS account root user

1. Sign in to the [AWS Management Console](#) as the account owner by choosing **Root user** and entering your AWS account email address. On the next page, enter your password.

   For help signing in by using root user, see [Signing in as the root user](#) in the *AWS Sign-In User Guide*.

2. Turn on multi-factor authentication (MFA) for your root user.

   For instructions, see [Enable a virtual MFA device for your AWS account root user (console)](#) in the *IAM User Guide*.

Create a user with administrative access

1. Enable IAM Identity Center.

   For instructions, see [Enabling AWS IAM Identity Center](#) in the *AWS IAM Identity Center User Guide*.

2. In IAM Identity Center, grant administrative access to a user.

   For a tutorial about using the IAM Identity Center directory as your identity source, see [Configure user access with the default IAM Identity Center directory](#) in the *AWS IAM Identity Center User Guide*.

Sign in as the user with administrative access

- To sign in with your IAM Identity Center user, use the sign-in URL that was sent to your email address when you created the IAM Identity Center user.

  For help signing in using an IAM Identity Center user, see [Signing in to the AWS access portal](#) in the *AWS Sign-In User Guide*.

Assign access to additional users

1. In IAM Identity Center, create a permission set that follows the best practice of applying least-privilege permissions.

    For instructions, see Create a permission set in the *AWS IAM Identity Center User Guide.*

2. Assign users to a group, and then assign single sign-on access to the group.

    For instructions, see Add groups in the *AWS IAM Identity Center User Guide.*

For more information about setting up your Amazon Chime administrator account, see Getting started.

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 for Amazon Chime system administrators, 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
- Step 2 (optional): Configuring account settings
- Step 3: Adding users to your account
- (Optional) Setting up phone numbers for your Amazon Chime account

Step 1: Creating an Amazon Chime administrator account

After you complete the Prerequisites for Amazon Chime system administrators, 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.

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.

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. For more information about setting up identity providers, see Connecting to your Active Directory and Connecting to Okta SSO.

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.

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.

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.

(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 and Porting existing phone numbers.

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 in the *Amazon Chime SDK Administration Guide*.

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.

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

Topics

- Choosing between an Amazon Chime Team account or Enterprise account
- Claiming a domain
- Converting a Team account to an Enterprise account
- Renaming your account
- Deleting your account
- Managing meeting settings
- Managing chat retention policies
- Restoring chat messages
- Deleting chat messages
- Connecting to your Active Directory
- Connecting to Okta SSO
- Deploying the Amazon Chime Add-In for Outlook
- Setting up the Amazon Chime Meetings App for Slack

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.

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](#) and [Connecting to your Active Directory](#).
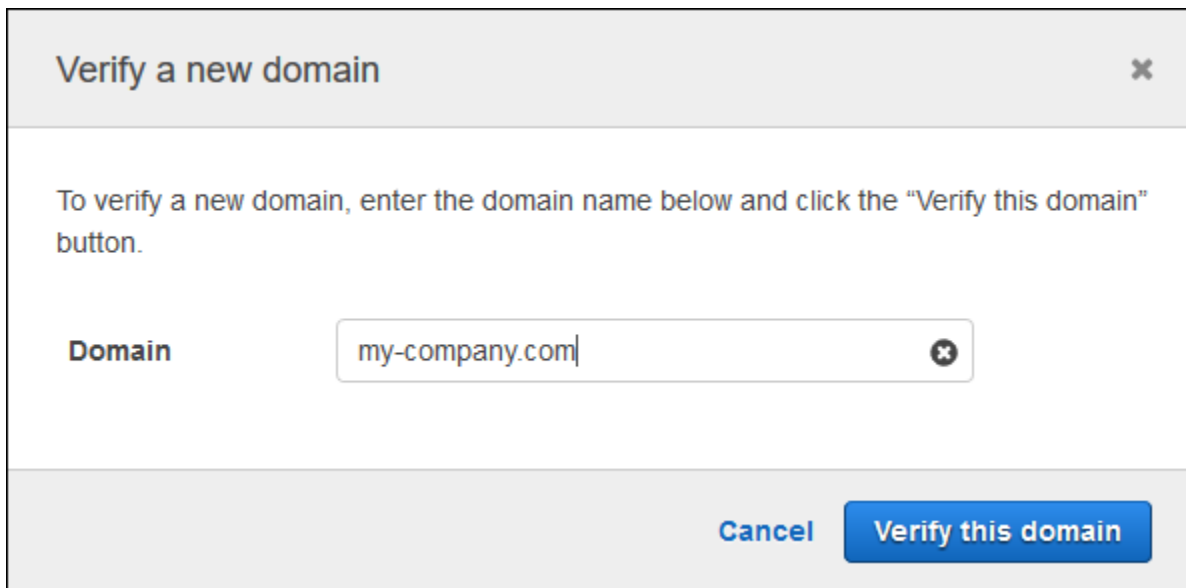
You can also manage user activation and suspension from your Enterprise account. For more information, see [Managing user permissions and access](#).

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?.

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](). For more information about claiming a domain, see [Claiming a domain]().

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]().

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

The following steps explain how to rename the Amazon Chime team and enterprise accounts that you administer. The name you choose appears in the emails that invite users to join Amazon Chime.

To rename your account

1. Open the Amazon Chime console at [https://chime.aws.amazon.com/]().

   The **Accounts** page appears by default.

2. In the **Account name** column, select the account that you want to rename.

3. In the left-hand pane, under **Settings**, choose **Account**.

   The **Account summary** page appears.

4. Open the**Account actions** list and choose **Rename account**.

   The **Rename account** dialog box appears.

5. Enter the new account name and 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.

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**.

Managing chat retention policies

If you administer one or more Amazon Chime Enterprise accounts, you can set chat retention policies for the following:

- Chat conversations that include only members of your Enterprise account.

- Chat rooms created by members of your Enterprise account.

A retention policy automatically deletes messages based on the time period that you set. You can set time periods lasting from one day to 15 years.

> ⓘ **Note**
>
> Amazon Chime Enterprise accounts have a retention period of 90 days. The policy applies to conversations involving users who belong to the account, and to users who don't belong to the account.
> Retention policies do not apply to the following:
>
> - Chat conversations that do not include members of Amazon Chime Enterprise accounts
>
> - Chat rooms created by users who don't belong to 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

If the chat room is created by …	The retention policy is…
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. In the navigation pane, under **Settings**, choose **Retention**.
4. On the **Retention** page, under **Chat conversation retention**, move the slider to **On**.
5. Under **Retention period**, enter a number in the first box, then open the list next to the box and choose **Days**, **Weeks**, or **Years**.
6. Under **Chat room retention**, repeat steps 4-5. When finished, choose **Save**.

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

Restoring chat messages

> ℹ️ **Note**
>
> You must be an Amazon Chime Enterprise account administrator to complete these steps.

You can restore chat messages within 30 days of setting a chat retention period. When you restore chat messages, you restore all the messages sent by all the users in your Amazon Chime account.

Within that 30-day period, you can do either of the following to restore messages:

- Use the Amazon Chime Console to turn off data retention.

  —OR—

- Lengthen the retention period.

After the 30-day grace period, all chat messages that fall under the retention period are permanently deleted. New chat messages are permanently deleted as soon as they pass the retention period.

For information about setting or changing a retention period, see Turning on chat retention, earlier in this section.

Chat messages are also permanently deleted from Amazon Chime when you or an account member perform either of the following actions:

- Delete an Amazon Chime chat room. For more information about deleting chat rooms, see Deleting chat rooms, in the *Amazon Chime User Guide*.
- End an Amazon Chime meeting in which chat messages are present.

> ⓘ **Note**
>
> As needed, you can manually copy and save chat messages from a meeting, but you must do so before the meeting ends. For more information, see Using in-meeting chat, in the *Amazon Chime User Guide*.

Deleting chat messages

To comply with data retention policies, Amazon Chime retains all chat messages, and it prevents end users from deleting the messages that they send. However, Amazon Chime system administrators can use a pair of APIs to delete individual messages from conversations and chat rooms. The messages must reside in the administrator's Amazon Chime account.

Users can request message deletion by sending you a message ID and a corresponding conversation or chat room ID. The topic Using chat features, in the *Amazon Chime User Guide*, explains how.

When you get a deletion request, you can write code or use the AWS CLI to invoke the following APIs.

To remove a message

- Do one of the following:

  - **For conversation messages** – Use the [RedactConversationMessage](#) API.

    In the CLI, run the following command:

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

  - **For chat room messages** – Use the [RedactRoomMessage](#) API.

    In the CLI, run the following command:

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

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](#).

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 permissions to configure domains, active directories, and directory groups. For more information, see Identity and access management for Amazon Chime.

- 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 and Converting a Team account to an Enterprise account.

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**.

   > (i) **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](#).

> ⓘ **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 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 your users' email domains.

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](#).

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. Enter 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 use [Slack Enterprise Grid Organizations](#) , and you own or administer a Slack organization, you can set up the Amazon Chime Meetings App for Slack for your organizations. If you're a Slack workspace administrator, you can set up the Amazon Chime Meetings App for Slack for your workspaces.

The steps in the following sections explain how to perform both types of setups, and how to complete additional tasks such as migrating a workspace to an organization.

Topics

- [Installing the Amazon Chime Meetings App for Slack on an organization](#)
- [Installing the Amazon Chime Meetings App for Slack on workspaces](#)
- [Migrating workspaces to organizations](#)
- [Associating workspaces with Amazon Chime Team accounts](#)

Installing the Amazon Chime Meetings App for Slack on an organization

Installing the Amazon Chime Meetings App for Slack on a Slack organization enables users to start instant meetings and calls with other users in the various workspaces in that organization. It also enables workspace administrators to install the Amazon Chime Meetings App for Slack meetings application automatically on any new workspaces. The following steps explain how.

> **ⓘ Note**
>
> The following steps assume that you are an organization owner or administrator, and that you can log in to the Slack management console.

To set up the Amazon Chime Meetings App for Slack on an organization

1. In the left-hand pane of the Slack management console, choose **Apps**.

   The **Apps** page appears and lists the organization's installed apps, if any.

2. Choose **Manage Apps**, located in the upper-right corner of the page, then choose **Install an app**.

   The **Find an app to install** dialog box appears.

3. Search on `Amazon Chime Meetings`, then select it in the search results.

   The **Add Amazon Chime Meetings to workspaces** dialog box appears and lists the workspaces in the organization.

4. Choose the workspace or workspaces on which you want to install Amazon Chime Meetings App for Slack.

5. Optionally, choose **Default for future workspace** if you want to automatically install the Amazon Chime Meetings App for Slack in all new workspaces, then choose **Next**.

    The **Review this app's requested permissions** dialog box appears and displays the permissions and actions for the Amazon Chime Meetings App for Slack.

6. Choose **Next**.

7. If you chose to install the Amazon Chime Meetings App for Slack on new workspaces by default, choose **I'm ready to set this app as a default for future workspaces**, and then choose **Save**. Otherwise, just choose **Save**.

> ⓘ **Note**
>
> You can also use OAuth to install apps in your organizations. For more information, see Installing with OAuth in the Slack help.

Installing the Amazon Chime Meetings App for Slack on workspaces

Installing the Amazon Chime Meetings App for Slack on a workspace enables users to start instant meetings and calls with other users in that workspace. Users don't need an Amazon Chime user profile to use the Amazon Chime Meetings App for Slack. They can log in with their Slack user profiles and start calls or meetings at any time. If users need to conduct meetings with more than one other person, you must setup an Amazon Chime Team account and grant those additional users Pro permissions. For more information about starting Amazon Chime calls and meetings, see Using the Amazon Chime Meetings App for Slack in the *Amazon Chime User Guide*. For more information about setting up an Amazon Chime Team account, see Associating workspaces with Amazon Chime Team accounts in this guide.

To install the Amazon Chime Meetings App for Slack for Slack workspaces

1. Navigate to the Slack App Directory and locate the Amazon Chime Meetings App.

2. Choose **Add to Slack** to install the Amazon Chime Meetings App for Slack from the Slack App Directory.

3. Configure your Slack workspace **Calls** setting to **Enable calling in Slack, using Amazon Chime**.

Migrating workspaces to organizations

If you own a Slack organization, you can migrate workspaces into that organization. For more information about migrating workspaces, see Migrate workspaces to Enterprise Grid in the Slack help.

Associating workspaces with Amazon Chime Team accounts

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 25 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. 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.

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 for Amazon Chime system administrators.

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 account.

   - **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

> **ⓘ Note**
>
> The steps in this section assume that you have a set of user email addresses, or that you've connected your administrator account to Active Directory. For more information, refer to Connecting to your Active Directory, in this guide.

You use the Amazon Chime console to add and manage users. You add users by inviting them. As they accept your invitations, they appear under **Users**, which lists all the users in your account and their user details. For more information, see Viewing user details.

Administrators of accounts using **Login with Amazon** (LWA) also see options to manage permission tiers and remove users from an account. These actions are managed through Active Directory or Okta, depending on which one of those you configure an account to use. For more information, see Managing user permissions and access.

Contents

- Adding users
- Viewing user details
- Managing user permissions and access
- Changing personal meeting PINs
- Managing Pro trials
- Requesting user attachments
- How Amazon Chime manages automatic updates
- Migrating users to another Team account

Adding users

You add users to an Amazon Chime account by inviting them to join the account. You send invitations to potential users from the Amazon Chime console, and these steps explain how.

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

A list of the accounts that you administer appears.

2. Choose the account to which you want to add members, then choose **Invite users**.

   The **Invite new users** dialog box appears.

3. Enter the email addresses of the users that you want to invite. Separate each address with a semicolon (;).

4. Choose **Invite users**.

The new users appear in the list. When you invite users to a Team account, their details won't appear until they accept your invitation.

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 appear 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

Field	Description	Example
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
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**

Field	Description	Example
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.

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.

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 the attachments that your users upload into Amazon Chime. 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*.

How Amazon Chime manages 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.

Migrating users to another Team account

You migrate users to other Team accounts by creating and configuring a destination account, if one doesn't already exist. Then you add users to the destination account. The following steps take you to information about completing each part of a migration.

To migrate users

1. If you don't have a destination Team account, create one. For more information, see Step 1: Creating an Amazon Chime administrator account.
2. As needed, configure the account. For more information, see Step 2 (optional): Configuring account settings.
3. Add users to the account. For more information, see Step 3: Adding users to your account.

Managing phone numbers in Amazon Chime

You use Use the Amazon Chime console to provision phone numbers. When you provision numbers, you request them from a pool of numbers managed by Amazon Chime. When you unassign and then delete numbers, they return to the pool. When you port numbers, you port them into and out of Amazon Chime.

> ⓘ **Note**
>
> When you use the Amazon Chime console, you can only provision Amazon Chime Business Calling numbers. If you need international numbers, you use Amazon Chime Voice Connectors and SIP media applications. To do that, you must first create an Amazon Chime SDK administrative account. For more information, refer to the following topics in the *Amazon Chime SDK Administrator Guide*:
>
> - Prerequisites
> - Managing phone number inventory
> - Managing Voice Connectors
> - Managing SIP media applications

The topics in the following sections explain how to provision and manage Amazon Chime phone numbers.

Contents

- Provisioning phone numbers
- Porting existing phone numbers
- Assigning Amazon Chime Business Calling phone numbers
- Unassigning Amazon Chime Business Calling phone numbers
- Using outbound calling names
- Deleting phone numbers
- Restoring deleted phone numbers

Provisioning phone numbers

Use the Amazon Chime console to provision phone numbers for your Amazon Chime account. The numbers come from a pool managed by Amazon Chime. Choose Amazon Chime Business Calling to provision and assign phone numbers to your existing Amazon Chime users.

When provisioning completes, the phone numbers appear in your **Inventory**. You then assign them to individual users.

To provision phone numbers

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

2. In the navigation pane, under **Calling**, choose **Phone number management**.

3. Choose **Orders**, **Provision phone numbers**.

4. Select **Business Calling**, then choose **Next**.

5. Search for available phone numbers. Select the phone numbers that you want, then choose **Provision**.

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

Porting existing phone numbers

In addition to provisioning phone numbers, you can also port numbers from your phone carrier into your inventory. This includes toll-free numbers.

> ⓘ **Note**
>
> If you need to port international numbers, use Amazon Chime Voice Connector's, or use SIP media applications, you must create an Amazon Chime SDK administrator account and use the Amazon Chime SDK console. For more information about doing that, refer to [Prerequisites](#), in the *Amazon Chime SDK Administrator Guide*.

The following sections explain how to port phone numbers.

Topics

Prerequisites for porting numbers

To port numbers, you must have a Letter of Agency (LOA). You must have an LOA for domestic phone numbers. Download the Letter of Agency (LOA) form and fill it out. If you need to port phone numbers from different carriers, fill out a separate LOA for each carrier.

Porting phone numbers in

You create a support request to port existing phone numbers in.

To port existing phone numbers

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

2. On the command bar at the top of the page, choose **Support**, then choose **Submit request**.
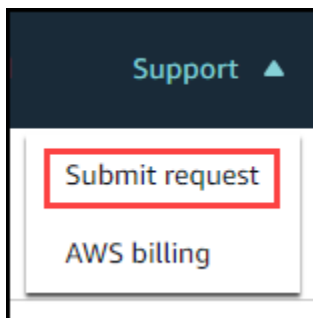
   That takes you to the AWS Support console.

   > **ⓘ Note**
   >
   > You can also go directly to the AWS Support Center page. If you do, choose **Create case**, then follow the steps below.

3. Under **How can we help**, do the following:

   a. Choose **Account and billing**.

   b. From the **Service** list, choose **Chime SDK (Number Management)**.

   c. From the **Category** list, choose **Phone Number Port In**.

   d. Choose **Next step: Additional information**.

4. Under **Additional information**, do the following

   a. Under **Subject**, enter `Porting phone numbers in`.

   b. Under **Description**, enter the following information:

      For porting US numbers:

      - Billing Telephone Number (BTN) of the account.

      - Authorizing person's name. This is the person in charge of account billing with the
        current carrier.

      - Current carrier, if known.

      - Service account number, if this information is present with the current carrier.

      - Service PIN, if available.

      - Service address and customer name, as they appear in your current carrier contract.

      - Requested date and time for the port.

      - (Optional) If you want to port your Billing Telephone Number (BTN), select one of the
        following options:

        - **I am porting my BTN and I want to replace it with a new BTN that I am providing. I
          can confirm that this new BTN is on the same account with the current carrier.**

        - **I am porting my BTN and I want to close out my account with my current carrier.**

        - **I am porting my BTN because my account is currently set up so that each phone
          number is its own BTN.** (Select this option only when your account with the current
          carrier is set up this way.)

        - After you choose an option, attach your Letter of Agency (LOA) to the request.

      For porting international numbers:

      - You must use the SIP Media Application Dial-In product type for non-US phone
        numbers.

- Type of number (Local or Toll-Free)

- Existing phone numbers to port in.

- Estimate usage volume

- Country

c. From the **Phone number type** list, select **Business Calling**, **SIP Media Application Dial-In**, or **Voice Connector**.

d. Under **Phone number**, enter at least one phone number, even if you're porting multiple numbers.

e. Under **Porting Date**, enter the desired porting date.

f. Under **Porting Time**, enter the desired time.

g. Choose **Next step: Solve now or contact us**.

5. Under **Solve now or contact us**, choose **Contact us**.

6. From the **Preferred contact language list**, choose a language

7. Choose **Web** or **Phone**. If you choose **Phone**, enter your phone number. When finished, choose **Submit**.

AWS Support lets you know whether your phone numbers can be ported from your existing phone carrier. If you can, you need to submit any required documents. The steps in the next section explain how to submit those documents.

Submitting required documents

After AWS Support says you can port phone numbers, you need to submit any required documents. The following steps explain how.

> **ⓘ Note**
>
> AWS Support provides a secure Amazon S3 link for uploading all requested documents. Do not proceed until you receive the link.

To submit documents

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

2. Sign in to your AWS account, then open the Amazon S3 upload link generated specifically for your account.

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

3. Choose **Add Files**, then select the identity documents related to your request.

4. Expand the **Permissions** section, and choose **Specify individual ACL permissions**.

5. At the end of the **Access control list (ACL)** section, choose **Add grantee**, then paste the key provided by AWS Support into the **Grantee** box.

6. Under **Objects**, choose the **Read** checkbox, then choose **Upload**.

After you provide the Letter of Agency (LOA), AWS Support confirms with your existing phone carrier that the information on the LOA is correct. If the information provided on the LOA does not match the information that your phone carrier has on file, AWS Support contacts you to update the information provided on the LOA.

Viewing request status

The following steps explain how to use the Amazon Chime console to view the status of your porting requests.

To view the status

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

2. In the navigation pane, choose **Phone number management**.

3. Choose the **Orders** tab.

The **Status** column shows the status of your request. AWS Support also contacts you with updates and requests for further information, as needed. For more information, see Phone number porting status definitions, later in this section.

Assigning ported numbers

After your 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.

On the FOC date, the ported phone numbers are activated for use. You must then assign the numbers to users in the desired account.

To assign phone numbers

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. In the navigation pane, choose **Phone number management**.
3. On the **Inventory** tab, select the checkbox next to the number that you want to assign, then choose **Assign**.

> ⓘ **Note**
>
> You can only choose one number at a time.

4. On the **Assign +1***phone number* **to a user profile** page, select the account for the number, then choose **Next**.
5. Select the user that you want to assign the number to, then choose **Assign**.

Porting phone numbers out

You port numbers out of Amazon Chime by initiating a porting request with your winning carrier. When submitting information to your winning carrier, include your AWS account ID as the account ID associated with the phone number being ported.

When the porting process finishes and your winning carrier has the numbers, you must unassign and delete those numbers from your inventory. For more information, see [Unassigning Amazon Chime Business Calling phone numbers](#) and [Deleting phone numbers](#) in this guide.

> ⚠ **Important**
>
> • The ability to port numbers out depends on the winning carrier's ability to accept those numbers.

- Verifying the authenticity of the winning carrier's port-out request is critical for the security of your phone number. If the account details are not correct (for example, there's an account ID mismatch), your port-out request may be rejected, causing delays and requiring you to resubmit your request.

(Optional) How to request a PIN to protect your number

For additional security, you can contact us to apply a PIN to your number. The winning carrier then uses that PIN. Follow these steps:

To request a PIN

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

2. In the navigation pane, under **Contact Us**, choose **Support**.

   That takes you to the AWS Support console.

   > **ⓘ Note**
   >
   > You can also go directly to the AWS Support Center page. If you do, choose **Create case**, then follow the steps below.

3. Under **How can we help**, do the following:

   a. Choose **Account and billing**.

   b. From the **Service** list, choose **Chime SDK (Number Management)**.

   c. From the **Category** list, choose **Phone Number Port Out**.

   d. Choose **Next step: Additional information**.

4. Under **Additional information**, do the following

   a. Under **Subject**, enter **Porting phone numbers out**.

   b. Under **Description**, enter the following.

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

> ℹ️ **Note**
>
> You must provide an alphanumeric PIN of 4 - 10 characters.

AWS Support associates a PIN with the phone number. When requesting the port with your winning carrier, provide your AWS account ID and PIN. We will use that information to validate any port requests received for your number.

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.

Assigning Amazon Chime Business Calling phone numbers

Use the phone number management **Inventory** page to assign Amazon Chime Business Calling phone numbers to individual users.

To assign Amazon Chime Business Calling phone numbers

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. In the navigation pane, under **Calling**, choose **Phone number management**.
3. On the **Inventory** tab, select the phone number that you want to assign.
4. Choose **Assign**.
5. Select the account that the user belongs to, then choose **Next**.
6. Select the user, then choose **Assign**.

When you change a phone number or phone number permissions, we recommend providing the user with their new 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.

Unassigning Amazon Chime Business Calling phone numbers

The following procedure unassigns phone numbers from Amazon Chime Business Calling users.

To unassign phone numbers

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

2. In the navigation pane, under **Calling**, choose **Phone number management**.

3. On the **Inventory** tab, select the phone number that you want to unassign.

4. Choose **Unassign**.

5. Select the check box, and choose **Unassign**.

You can view the details for the numbers in your inventory. For example, you can 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. In the navigation pane, under **Calling**, choose **Phone number management**.

3. Choose the **Inventory** tab, then select the phone number that you want to view.

4. Open the **Actions** list and choose **View details**.

Using outbound calling names

Outbound calling names act as caller IDs. You can set a default calling name for one or more of the phone numbers in your inventory. You can also set unique calling names for individual phone numbers. The names then appear to recipients of outbound calls made using those phone numbers. Calling names apply to all phone number product types. You can update the names once every seven days.

For example, you can set a default calling name of **Department 5** for all the phone numbers in that department. You can also set a unique name of **Jane Doe** for the department head.

The following steps explain how to set default and individual outbound calling names.

To set a calling name

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

2. In the navigation pane, under **Calling**, choose **Phone number management**.

3. On the **Inventory** tab, do either of the following:select the checkboxes next to the phone numbers that you want to update.

    - To set a default calling name for multiple numbers, select the check boxes next to those numbers.

- To set an individual calling name, select the desired number.

4. Open the **Actions** list and choose **Update default calling name**.

5. In the **Default calling name** box, enter a name of up to 15 characters.

6. Choose **Save**.

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

Deleting phone numbers

> ⚠️ **Important**
>
> Only Amazon Chime system administrators can complete these steps. Also, you must unassign phone numbers before you can delete them.

When you provision a phone number, you order it from a pool of numbers that Amazon Chime maintains. Deleting a number moves it back into the pool. When you delete a number, it first goes to your deletion queue where it's held for 7 days. During that time, you can move the number back to your inventory. After 7 days, the system automatically deletes the number from the holding queue and disassociates it from your account. That returns the number to the number pool. If you need to reclaim a number after the system deletes it from the holding queue, follow the steps in Provisioning phone numbers, but be aware that the number may not be available.

To delete unassigned phone numbers

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

2. In the navigation pane, under **Calling**, choose **Phone number management**.

3. Choose the **Inventory** tab, then select the phone number or numbers that you want to delete.

4. Open the **Actions** list and choose **Delete phone number(s)**.

5. Select the check box, then choose **Delete**.

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

Restoring deleted phone numbers

You can restore deleted phone numbers from the **Deletion queue** for up to 7 days after you delete them. 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. In the navigation pane, under **Calling**, choose **Phone number management**.
3. Choose the **Deletion queue** tab, then select the phone number or numbers that you want to restore.
4. Choose **Move to inventory**.

Managing global settings in Amazon Chime

You use the Amazon Chime console to manage call detail record settings.

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 User Guide*.

You can configure call detail record settings for Amazon Chime Business Calling. For more information about Amazon Chime Business Calling, see Managing phone numbers in Amazon Chime.

To configure call detail record settings

1. Create an Amazon S3 bucket by following the steps at Getting started with Amazon Simple Storage Service in the *Amazon Simple Storage Service User Guide*.

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

3. For **Global Settings**, choose **Call detail records**.

4. Choose **Business Calling Configuration**.

5. For **Log destination**, select the Amazon S3 bucket.

6. Choose **Save**.

You can stop logging call detail records at any time.

To stop logging call detail records

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

2. For **Global Settings**, choose **Call detail records**.

3. Choose **Disable logging** for the applicable configuration.

Amazon Chime 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"
}
```

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.

> ⓘ **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.

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

Device	SIP	H.323	Comment
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

Expand the following sections for more information about destinations, ports, and bandwidth.

Required destinations and ports

The following destinations and ports are required to run Amazon Chime.

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

Meeting and telephony port

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

Destination	Port
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	TCP/5100:6200
34.212.95.128/25	UDP/5100:6200
34.223.21.0/25	
52.55.62.128/25	
52.55.63.0/25	

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	UDP/10000:60000
	34.212.95.128/25	
	34.223.21.0/25	
	52.55.62.128/25	

AWS Region	Destination	Ports
	52.55.63.0/25	
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

Bandwidth requirements

Amazon Chime has the following bandwidth requirements for audio, video, and screen sharing:

- 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 sharing

- 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

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.

Extending the Amazon Chime desktop client

You can extend the capabilities of the Amazon Chime desktop client by adding chat bots, proxy phone sessions, and webhooks. Chat bots enable users to perform tasks such as querying internal systems for information. Proxy phone sessions allow users to call and send texts without revealing their phone numbers. Webhooks can automatically send messages to chat rooms. For example, a webhook can send meeting reminders to a team, along with a link to the meeting.

Topics

- [User management](#)
- [Integrating chatbots into the Amazon Chime desktop client](#)
- [Creating webhooks for Amazon Chime](#)

User management

The following code snippets can help you manage Amazon Chime users. All of the examples in this topic use Java.

Topics

- [Invite multiple users](#)
- [Downloading user lists](#)
- [Log out multiple users](#)
- [Update user personal PINs](#)

Invite multiple users

The following example shows how to invite multiple users to an Amazon Chime Team account.

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

```
chime.inviteUsers(inviteUsersRequest);
```

Downloading user lists

The following example shows how to download a list of users associated with your Amazon Chime administrative account in .csv format.

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

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

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

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

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

printer.close();
```

Log out multiple users

The following example shows how to log out multiple users from your Amazon Chime administrative account.

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

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

    chime.logoutUser(logoutUserRequest);
}
```

Update user personal PINs

The following example shows how to reset the personal meeting PIN for a specified Amazon Chime user.

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

ResetPersonalPINResult result = chime.resetPersonalPIN(request);

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

Integrating chatbots into the Amazon Chime desktop client

You can use the AWS Command Line Interface (AWS CLI), Amazon Chime API, or AWS SDK to integrate chatbots with Amazon Chime. Chatbots let you use the power of Amazon Lex, AWS Lambda, and other AWS services to streamline common tasks with intelligent conversational interfaces that are accessible to users in Amazon Chime chat rooms.

If you're an Amazon Chime Enterprise account administrator, you can use chatbots to allow users to perform such tasks as:

- Querying their internal systems for information.
- Automating tasks.
- Receiving notifications for critical issues.
- Creating support tickets.

For more information about Amazon Chime Enterprise accounts, see Managing your Amazon Chime accounts.

If you administer an Amazon Chime Enterprise account, you can create up to 10 chatbots for integration with Amazon Chime. Chatbots can be used only in chat rooms created by members of your account. Only chat room administrators can add chatbots to a chat room. After a chatbot is added to a chat room, members of the chat room can interact with the bot using commands provided by the bot creator. For more information, see the next section in this topic.

Linux and macOS users can build a sample custom chatbot. For more information, see Build custom chatbots for Amazon Chime.

Content

- Using chatbots with Amazon Chime
- Amazon Chime events sent to chatbots

Using chatbots with Amazon Chime

If you administer an Amazon Chime Enterprise account, you can create up to 10 chatbots for integration with Amazon Chime. Chatbots can only be used in chat rooms created by members of your account. Only chat room administrators can add chatbots to a chat room. After a chatbot is added to a chat room, members of the chat room can interact with the bot using commands provided by the bot creator. For more information, see Using chatbots in the *Amazon Chime User Guide*.

You can also use the Amazon Chime API operation to enable or stop chatbots for your Amazon Chime account. For more information, see Update chatbots.

> ⓘ **Note**
>
> You can't delete chatbots. To stop a chatbot from being used in your account, use the Amazon Chime UpdateBot API operation in the *Amazon Chime API Reference*. When you stop a chatbot, chat room administrators can remove it from a chat room, but they cannot add it to a chat room. Users who @mention a stopped chatbot in a chat room receive an error message.

Prerequisites

Before you start the procedure to integrate chatbots with Amazon Chime, complete the following prerequisites:

- Create a chatbot.

- Create the outbound endpoint for Amazon Chime to send events to your bot. Choose from an AWS Lambda function ARN or an HTTPS endpoint. For more information about Lambda, see the *AWS Lambda Developer Guide*.

DNS best practices for HTTPS endpoints

We recommend the following best practices when assigning DNS for your HTTPS endpoint:

- Use a DNS subdomain that is dedicated to the bot endpoint.

- Use only A-records to point to the bot endpoint.

- Protect your DNS servers and DNS registrar account to prevent domain hijacking.

- Use publicly valid TLS intermediate certificates that are dedicated to the bot endpoint.

- Cryptographically verify the bot message signature before acting on a bot message.

After creating your chatbot, use the AWS Command Line Interface (AWS CLI) or the Amazon Chime API operation to complete the tasks described in the following sections.

Tasks

- Step 1: Integrate a chatbot with Amazon Chime
- Step 2: Configure the outbound endpoint for an Amazon Chime chatbot
- Step 3: Add the chatbot to an Amazon Chime chat room
- Authenticate chatbot requests
- Update chatbots

Step 1: Integrate a chatbot with Amazon Chime

After you complete the prerequisites, integrate your chatbot with Amazon Chime using the AWS CLI or Amazon Chime API.

> **ⓘ Note**
>
> These procedures create a name and email address for your chatbot. Chatbot names and email addresses cannot be changed after creation.

AWS CLI

To integrate a chatbot using the AWS CLI

1. To integrate your chatbot with Amazon Chime, use the **create-bot** command in the AWS CLI.

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

    a. Enter a chatbot display name of up to 55 alphanumeric or special characters (such as +, -, %).

    b. Enter the registered domain name for your Amazon Chime Enterprise account.

2. Amazon Chime returns a response that includes the bot ID.

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

3. Copy and save the bot ID and bot email address to use in the following procedures.

Amazon Chime API

To integrate a chatbot using the Amazon Chime API

1. To integrate your chatbot with Amazon Chime, use the CreateBot API operation in the *Amazon Chime API Reference*.

    a. Enter a chatbot display name of up to 55 alphanumeric or special characters (such as +, -, %).

    b. Enter the registered domain name for your Amazon Chime Enterprise account.

2. Amazon Chime returns a response that includes the bot ID. Copy and save the bot ID and email address. The bot email address looks like this: *exampleBot*-chimebot@*example.com*.

AWS SDK for Java

The following sample code demonstrates how to integrate a chatbot using the AWS SDK for Java.

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

chime.createBot(createBotRequest);
```

Amazon Chime returns a response that includes the bot ID. Copy and save the bot ID and email address. The bot email address looks like this: *exampleBot*-chimebot@*example.com*.

Step 2: Configure the outbound endpoint for an Amazon Chime chatbot

After you create a chatbot ID for your Amazon Chime Enterprise account, configure your outbound endpoint for Amazon Chime to use to send messages to your bot. The outbound endpoint can be an AWS Lambda function ARN or an HTTPS endpoint that you created as part of the prerequisites. For more information about Lambda, see the *AWS Lambda Developer Guide*.

> ⓘ **Note**
>
> If the outbound HTTPS endpoint for your bot is not configured or is empty, chat room administrators cannot add the bot to a chat room. Also, chat room users cannot interact with the bot.

AWS CLI

To configure an outbound endpoint for your chatbot, use the **put-events-configuration** command in the AWS CLI. Configure a Lambda function ARN or an outbound HTTPS endpoint.

Lambda ARN

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

HTTPS endpoint

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

Amazon Chime responds with the bot ID and HTTPS endpoint.

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

Amazon Chime API

To configure the outbound endpoint for your chatbot, use the Amazon Chime
[PutEventsConfiguration](#) API operation in the *Amazon Chime API Reference*. Configure either a
Lambda function ARN or an outbound HTTPS endpoint.

- **If you configure a Lambda function ARN** – Amazon Chime calls Lambda to add permission to
  allow the Amazon Chime administrator's AWS account to invoke the provided Lambda function
  ARN. This is followed by a dry run invocation to verify that Amazon Chime has permission
  to invoke the function. If adding permissions fails, or if the dry run invocation fails, then the
  `PutEventsConfiguration` request returns an HTTP 4xx error.

- **If you configure an outbound HTTPS endpoint** – Amazon Chime verifies your endpoint by
  sending an HTTP Post request with a Challenge JSON payload to the outbound HTTPS endpoint
  that you provided in the previous step. Your outbound HTTPS endpoint must respond by echoing
  back the Challenge parameter in JSON format. The following examples show the request and a
  valid response.

Request

```
HTTPS POST

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

Response

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


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

If the challenge handshake fails, then the `PutEventsConfiguration` request returns an HTTP 4xx error.

AWS SDK for Java

The following sample code demonstrates how to configure an endpoint using the AWS SDK for Java.

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

 chime.putEventsConfiguration(putEventsConfigurationRequest):
```

Step 3: Add the chatbot to an Amazon Chime chat room

Only a chat room administrator can add a chatbot to a chat room. They use the chatbot email address created in [Step 1](#).

To add a chatbot to a chat room

1. Open the Amazon Chime desktop client or web application.

2. Choose the gear icon in the upper-right corner, and choose **Manage webhooks and bots**.

3. Choose **Add bot**.

4. For **Email address**, enter the bot email address.

5. Choose **Add**.

The bot name appears in the chat room roster. If there are additional actions necessary to add a chatbot to a chat room, provide the actions to the chat room administrator.

After the chatbot is added to the chat room, provide the chatbot commands to your chat room users. One way to do this is to program your chatbot to send command help to the chat room when it receives the chat room invite. AWS also recommends creating a help command for your chatbot users to use.

Authenticate chatbot requests

You can authenticate requests sent to your chatbot from an Amazon Chime chat room. To do this, compute a signature based on the request. Then, validate that the computed signature matches the one on the request header. Amazon Chime uses the HMAC SHA256 hash to generate the signature.

If your chatbot is configured for Amazon Chime using an outbound HTTPS endpoint, use the following authentication steps.

To validate a signed request from Amazon Chime for a chatbot with a outbound HTTPS endpoint configured

1. Get the **Chime-Signature** header from the HTTP request.

2. Get the **Chime-Request-Timestamp** header and the **body** of the request. Then, use a vertical bar as the delimiter between the two elements to form a string.

3. Use the **SecurityToken** from the CreateBot response as the initial key of **HMAC_SHA_256**, and hash the string that you created in step 2.

4. Encode the hashed byte with Base64 encoder to a signature string.

5. Compare this computed signature to the one in the **Chime-Signature** header.

The following code sample demonstrates how to generate a signature using Java.

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

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

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

The outbound HTTPS endpoint must respond to the Amazon Chime request with 200 OK within 2 seconds. Otherwise, the request fails. If the outbound HTTPS endpoint is unavailable after 2 seconds, possibly because of a Connection or Read timeout, , or if Amazon Chime receives a 5xx response code, Amazon Chime retries the request two times. The first retry is sent 200 milliseconds after the initial request fails. The second retry is sent 400 milliseconds after the previous retry fails. If the outbound HTTPS endpoint is still unavailable after the second retry, the request fails.

> **ⓘ Note**
>
> The **Chime-Request-Timestamp** changes each time the request is retried.

If your chatbot is configured for Amazon Chime using a Lambda function ARN, use the following authentication steps.

To validate a signed request from Amazon Chime for a chatbot with a Lambda function ARN configured

1. Get the **Chime-Signature** and **Chime-Request-Timestamp** from the Lambda request **ClientContext**, in Base64 encoded JSON format.

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

2. Get the **body** of the request from the request payload.

3. Use the **SecurityToken** from the `CreateBot` response as the initial key of **HMAC_SHA_256**, and hash the string that you created.

4. Encode the hashed byte with Base64 encoder to a signature string.

5. Compare this computed signature to the one in the **Chime-Signature** header.

If a `com.amazonaws.SdkClientException` occurs during the Lambda invocation, Amazon Chime retries the request two times.

Update chatbots

As the Amazon Chime account administrator, you can use the Amazon Chime API with the AWS SDK or AWS CLI to view your chatbot details. You can also enable or stop your chatbots from being used in your account. You can also regenerate security tokens for your chatbot.

For more information, see the following topics in the *Amazon Chime API Reference*:

- GetBot – Gets your chatbot details, such as bot email address and bot type.
- UpdateBot – Enables or stops a chatbot from being used in your account.

- RegenerateSecurityToken – Regenerates the security token for your chatbot.

You can also change the `PutEventsConfiguration` for your chatbot. For example, if your chatbot was initially configured to use an outbound HTTPS endpoint, you can delete the previous events configuration and put a new events configuration for a Lambda function ARN.

For more information, see the following topics in the *Amazon Chime API Reference*:

- DeleteEventsConfiguration
- PutEventsConfiguration

Amazon Chime events sent to chatbots

The following events are sent to your chatbot from Amazon Chime:

- **Invite** – Sent when your chatbot is added to an Amazon Chime chat room
- **Mention** – Sent when a user in a chat room @mentions your chatbot
- **Remove** – Sent when your chatbot is removed from an Amazon Chime chat room

The following examples show the JSON payload sent to your chatbot for each of these events.

Example : Invite event

```
{
  "Sender": {
              "SenderId": "user@example.com",
              "SenderIdType": "EmailId"
          },
  "Discussion": {
              "DiscussionId": "abcdef12-g34h-56i7-j8kl-mn9opqr012st",
              "DiscussionType": "Room"
          },
  "EventType": "Invite",
  "InboundHttpsEndpoint": {
                  "EndpointType": "Persistent",
                  "Url": "https://
hooks.a.chime.aws/incomingwebhooks/a1b2c34d-5678-90e1-f23g-h45i67j8901k?
token=ABCDefGHiJK1LMnoP2Q3RST4uvwxYZAbC56DeFghIJkLM7N8OP9QRsTuV0WXYZABcdefgHiJ"
                  },
```

```
            "EventTimestamp": "2019-04-04T21:27:52.736Z"
        }
```

Example : Mention event

```
        {
            "Sender": {
                    "SenderId": "user@example.com",
                    "SenderIdType": "EmailId"
                },
            "Discussion": {
                    "DiscussionId": "abcdef12-g34h-56i7-j8kl-mn9opqr012st",
                    "DiscussionType": "Room"
                },
            "EventType": "Mention",
            "InboundHttpsEndpoint": {
                                "EndpointType": "ShortLived",
                                "Url": "https://
hooks.a.chime.aws/incomingwebhooks/a1b2c34d-5678-90e1-f23g-h45i67j8901k?
token=ABCDefGHiJK1LMnoP2Q3RST4uvwxYZAbC56DeFghIJkLM7N8OP9QRsTuV0WXYZABcdefgHiJ"
                            },
            "EventTimestamp": "2019-04-04T21:30:43.181Z",
            "Message": "@botDisplayName@example.com Hello Chatbot"
        }
```

> (i) **Note**
>
>   The InboundHttpsEndpoint URL for a Mention event expires 2 minutes after it is sent.

Example : Remove event

```
        {
            "Sender": {
                    "SenderId": "user@example.com",
                    "SenderIdType": "EmailId"
                },
            "Discussion": {
```

```
                                        "DiscussionId": "abcdef12-g34h-56i7-j8kl-mn9opqr012st",
                                        "DiscussionType": "Room"
                                   },
                         "EventType": "Remove",
                         "EventTimestamp": "2019-04-04T21:27:29.626Z"
                    }
```

Creating webhooks for Amazon Chime

Webhooks allow web applications to communicate with each other in real time. Typically, webhooks send notifications when an action occurs. For example, say you run an online shopping site. Webhooks can notify you when a customer adds items to a shopping cart, pays for an order, or sends a comment. Webhooks don't need as much programming as traditional applications, and they don't use as much processing power. Without a webhook, a program has to to poll for data frequently in order to get it in real time. With a webhook, the sending application posts the data immediately.

Incoming webhooks that you create can programmatically send messages to Amazon Chime chat rooms. For example, a webhook can notify a customer service team about the creation of a new high-priority ticket, and add a link to the ticket in the chat room.

Webhooks messages can be formatted with markdown and can include emojis. HTTP links and email addresses render as active links. Messages can also include @All and @Present annotations to alert all members and present members of a chat room, respectively. To directly @mention a chat room participant, use their alias or full email address. For example, @alias or @alias@domain.com.

Webhooks can only be part of a chat room and can't be shared. Amazon Chime chat room administrators can add up to 10 webhooks for each chat room.

After you create a webhook, you can integrate it with an Amazon Chime chat room, as shown in the following procedure.

To integrate a webhook with a chat room

1. Get the webhook URL from the chat room administrator. For more information, see Adding webhooks to a chat room in the *Amazon Chime User Guide*.
2. Use the webhook URL in the script or application that you created to send messages to the chat room:

a. The URL accepts an HTTP POST request.

b. Amazon Chime webhooks accept a JSON payload with a single key **Content**. The following is a sample curl command with a sample payload:

```
curl -X POST "<Insert your webhook URL here>" -H "Content-Type:application/
json" --data '{"Content":"Message Body emoji test: :) :+1: link test: http://
sample.com email test: marymajor@example.com All member callout: @All All
 Present member callout: @Present"}'
```

The following is a sample PowerShell command for Windows users:

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

After the external program sends the HTTP POST to the webhook URL, the server validates that the webhook is valid and has an assigned chat room. The webhook appears in the chat room roster with a webhook icon next to its name. Chat room messages sent by the webhook appear in the chat room under the webhook name followed by **(Webhook)**.

> ⓘ **Note**
>
> CORS is not currently enabled for webhooks.

Troubleshooting webhook errors

The following is a list of webhook-related errors:

- The incoming webhook rate limit for each webhook is 1 TPS per chat room. Throttling results in an HTTP 429 error.

- Messages posted by a webhook must be 4 KB or less. A bigger message payload results in an HTTP 413 error.

- Messages posted by a webhook with @All and @Present annotations work only for chat rooms with 50 or fewer members. More than 50 members results in an HTTP 400 error.

- If the webhook URL is regenerated, using the old URL results in an HTTP 404 error.

- If the webhook in a room is deleted, using the old URL results in an HTTP 404 error.

- Invalid webhook URLs result in HTTP 403 errors.

- If the service is unavailable, the user receives an HTTP 503 error in the response.

Administrative support for Amazon Chime

> **ⓘ Note**
>
> For help with your Amazon shopping account, go to [Customer Service on amazon.com](#).

If you 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**.

Provide as much of the following information as you can:

- 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.

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 AWSAWS services that help you to monitor and secure your Amazon Chime resources.

Topics

- Identity and access management for Amazon Chime
- How Amazon Chime works with IAM
- Cross-service confused deputy prevention
- Amazon Chime resource-based policies
- Authorization based on Amazon Chime tags
- Amazon Chime IAM roles
- Amazon Chime identity-based policy examples
- Troubleshooting Amazon Chime identity and access
- Using service-linked roles for Amazon Chime
- Logging and monitoring in Amazon Chime

- [Compliance validation for Amazon Chime](#)

- [Resilience in Amazon Chime](#)

- [Infrastructure security in Amazon Chime](#)

- [Understanding Amazon Chime automatic updates](#)

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](#)

- [Authenticating with identities](#)

- [Managing access using policies](#)

Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work that 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](#).

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 service users 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](#).

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](#).

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. You must be *authenticated* (signed in to AWS) as the AWS account root user, as an IAM user, or by assuming an IAM role.

You can sign in to AWS as a federated identity by using credentials provided through an identity source. AWS IAM Identity Center (IAM Identity Center) users, your company's single sign-on authentication, and your Google or Facebook credentials are examples of federated identities. When you sign in as a federated identity, your administrator previously set up identity federation using IAM roles. When you access AWS by using federation, you are indirectly assuming a role.

Depending on the type of user you are, you can sign in to the AWS Management Console or the AWS access portal. For more information about signing in to AWS, see [How to sign in to your AWS account](#) in the *AWS Sign-In User Guide*.

If you access AWS programmatically, AWS provides a software development kit (SDK) and a command line interface (CLI) to cryptographically sign your requests by using your credentials. If you don't use AWS tools, you must sign requests yourself. For more information about using the recommended method to sign requests yourself, see [Signing AWS API requests](#) in the *IAM User Guide*.

Regardless of the authentication method that you use, you might 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 [Multi-factor authentication](#) in the *AWS IAM Identity Center User Guide* and [Using multi-factor authentication (MFA) in AWS](#) in the *IAM User Guide*.

AWS account root user

When you create an AWS account, you begin with one 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 don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For

the complete list of tasks that require you to sign in as the root user, see Tasks that require root user credentials in the *IAM User Guide*.

IAM users and groups

An *IAM user* is an identity within your AWS account that has specific permissions for a single person or application. Where possible, we recommend relying on temporary credentials instead of creating IAM users who have long-term credentials such as passwords and access keys. However, if you have specific use cases that require long-term credentials with IAM users, we recommend that you rotate access keys. For more information, see Rotate access keys regularly for use cases that require long-term credentials in the *IAM User Guide*.

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:

- **Federated user access** – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see Creating a role for a third-party Identity Provider in the *IAM User Guide*. If you use IAM Identity Center, you configure a permission set. To control what your identities can access after they authenticate, IAM Identity Center correlates the permission set to a role in IAM. For information about permissions sets, see Permission sets in the *AWS IAM Identity Center User Guide*.

- **Temporary IAM user permissions** – An IAM user or role can assume an IAM role to temporarily take on different permissions for a specific task.

- **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 Cross account resource access in IAM in the *IAM User Guide*.

- **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.

  - **Forward access sessions (FAS)** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. When you use some services, you might perform an action that then initiates another action in a different service. FAS uses the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. FAS requests are only made when a service receives a request that requires interactions with other AWS services or resources to complete. In this case, you must have permissions to perform both actions. For policy details when making FAS requests, see Forward access sessions.

  - **Service role** – A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Creating a role to delegate permissions to an AWS service in the *IAM User Guide*.

  - **Service-linked role** – A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

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

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

Managing access using policies

You control access in AWS by creating policies and attaching them to AWS identities or resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when a principal (user, root user, or role session) 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*.

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

By default, users and roles have no permissions. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

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

Identity-based policies

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

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

Resource-based policies

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

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

AWS managed policies for Amazon Chime

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

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

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

Access Control Lists (ACLs)

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

Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs. To learn more about ACLs, see [Access control list (ACL) overview](link) 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 an 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](link) 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 [Service control policies](link) 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](link) 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](link) 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](#)
- [Resources](#)
- [Examples](#)

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

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

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

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

Condition keys

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*.

Resources

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

Examples

To view examples of Amazon Chime identity-based policies, see [Amazon Chime identity-based policy examples](#).

Cross-service confused deputy prevention

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

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

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

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonChimeAclCheck668426",
            "Effect": "Allow",
            "Principal": {
                "Service": "chime.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::your-cdr-bucket"
        },
        {
            "Sid": "AmazonChimeWrite668426",
```

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

Amazon Chime 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 that complete actions on your behalf. Service-linked roles appear in your IAM account, and the services own the roles. An IAM administrator can view but not edit the permissions for service-linked roles.

Amazon Chime supports service-linked roles. For details about creating or managing Amazon Chime service-linked roles, see [Using service-linked roles for Amazon Chime](#).

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](#)
- [Using the Amazon Chime console](#)
- [Allow users full access to Amazon Chime](#)
- [Allow users to view their own permissions](#)
- [Allow users to access user management actions](#)
- [AWS managed policy: AmazonChimeVoiceConnectorServiceLinkedRolePolicy](#)
- [Amazon Chime updates to AWS managed policies](#)

Policy best practices

Identity-based policies 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 with AWS managed policies and move toward least-privilege permissions** – To
  get started granting permissions to your users and workloads, use the *AWS managed policies*
  that grant permissions for many common use cases. They are available in your AWS account. We
  recommend that you reduce permissions further by defining AWS customer managed policies
  that are specific to your use cases. For more information, see [AWS managed policies](#) or [AWS
  managed policies for job functions](#) in the *IAM User Guide*.

- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the
  permissions required to perform a task. You do this by defining the actions that can be taken on
  specific resources under specific conditions, also known as *least-privilege permissions*. For more
  information about using IAM to apply permissions, see [Policies and permissions in IAM](#) in the
  IAM User Guide.

- **Use conditions in IAM policies to further restrict access** – You can add a condition to your
  policies to limit access to actions and resources. For example, you can write a policy condition to
  specify that all requests must be sent using SSL. You can also use conditions to grant access to
  service actions if they are used through a specific AWS service, such as AWS CloudFormation. For
  more information, see [IAM JSON policy elements: Condition](#) in the *IAM User Guide*.

- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional
  permissions** – IAM Access Analyzer validates new and existing policies so that the policies
  adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides
  more than 100 policy checks and actionable recommendations to help you author secure and
  functional policies. For more information, see [IAM Access Analyzer policy validation](#) in the *IAM
  User Guide*.

- **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users
  or a root user in your AWS account, turn on MFA for additional security. To require MFA when
  API operations are called, add MFA conditions to your policies. For more information, see
  [Configuring MFA-protected API access](#) in the *IAM User Guide*.

For more information about best practices in IAM, see [Security best practices in IAM](#) 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": "*"
        }
    ]
}
```

AWS managed policy: AmazonChimeVoiceConnectorServiceLinkedRolePolicy

The `AmazonChimeVoiceConnectorServiceLinkedRolePolicy` enables Amazon Chime Voice Connectors to stream media to Amazon Kinesis Video Streams, provide streaming notifications, and synthesize speech using Amazon Polly. This policy grants the Amazon Chime Voice Connector service permissions to access customer's Amazon Kinesis Video Streams, send notification events to the Amazon Simple Notification Service and Amazon Simple Queue Service, and use Amazon Polly to synthesize speech when using the Amazon Chime SDK Voice Applications Speak and SpeakAndGetDigits actions. For more information, see Amazon Chime SDK identity-based policy examples in the *Amazon Chime SDK Administrator Guide*.

Amazon Chime updates to AWS managed policies

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

Change	Description	Date
`AmazonChimeVoiceCo nnectorServiceLink edRolePolicy` – Update to an existing policy	Amazon Chime Voice Connectors added new permissions to allow you to use Amazon Polly to synthesiz e speech.These permissions are required to use the Speak and SpeakAndGetDigits	March 15, 2022

Change	Description	Date
	actions in Amazon Chime SDK Voice Applications.	
`AmazonChimeVoiceConnectorServiceLinkedRolePolicy` – Update to an existing policy	Amazon Chime Voice Connector added new permissions to allow access to Amazon Kinesis Video Streams and send notification events to SNS and SQS. These permissions are required for Amazon Chime Voice Connectors to stream media to Amazon Kinesis Video Streams and provide streaming notifications.	December 20, 2021
Change to existing policy. [Creating IAM users or roles with the Chime SDK policy](#).	Amazon Chime added new actions added to support expanded validation. A number of actions were added to allow listing and tagging of attendees and meeting resources, and for starting and stopping meeting transcription.	September 23, 2021
Amazon Chime started tracking changes	Amazon Chime started tracking changes for its AWS managed policies.	September 23, 2021

Troubleshooting Amazon Chime 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 am not authorized to perform an action in Amazon Chime](#)

- [I am not authorized to perform iam:PassRole](#)

- [I want to allow people outside of my AWS account to access my Amazon Chime resources](#)

I am not authorized to perform an action in Amazon Chime

If you receive an error that you're not authorized to perform an action, your policies must be updated to allow you to perform the action.

The following example error occurs when the `mateojackson` IAM user tries to use the console to view details about a fictional *my-example-widget* resource but doesn't have the fictional `chime:`*GetWidget* permissions.

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

In this case, the policy for the `mateojackson` user must be updated to allow access to the *my-example-widget* resource by using the `chime:`*GetWidget* action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

I am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, your policies must be updated 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 that are 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's policies must be updated to allow her to perform the `iam:PassRole` action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

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.
- 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 Cross account resource access in IAM 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.

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.

Topics

- Using roles with shared Alexa for Business devices
- Using roles with live transcription
- Using roles with Amazon Chime SDK media pipelines

Using roles with shared Alexa for Business devices

The information in the following sections explains how to use service-linked roles and grant Amazon Chime access to the Alexa for Business resources in your AWS account.

Topics

- Service-linked role permissions for Amazon Chime
- Creating a service-linked role for Amazon Chime
- Editing a service-linked role for Amazon Chime
- Deleting a service-linked role for Amazon Chime
- Supported Regions for Amazon Chime service-linked roles

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.

Using roles with live transcription

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

Topics

- [Service-Linked Role Permissions for Amazon Chime Live Transcription](#)

- [Creating a Service-Linked Role for Amazon Chime Live Transcription](#)

- [Editing a Service-Linked Role for Amazon Chime Live Transcription](#)

- [Deleting a Service-Linked Role for Amazon Chime Live Transcription](#)

- [Supported Regions for Amazon Chime Service-Linked Roles](#)

Service-Linked Role Permissions for Amazon Chime Live Transcription

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

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

- `transcription.chime.amazonaws.com`

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

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

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

Creating a Service-Linked Role for Amazon Chime Live Transcription

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

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

To create the role

1. Sign in to the AWS Management Console and open the IAM console at https://
    console.aws.amazon.com/iam/.

2. In the navigation pane of the IAM console, choose **Roles**, then choose **Create role**.

3. Choose the **AWS Service** role type, then choose **Chime**, then choose **Chime Transcription**.

4. Choose **Next**.

5. Choose **Next**.

6. Edit the description as needed, then choose **Create role**.

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

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

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

Editing a Service-Linked Role for Amazon Chime Live Transcription

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

Deleting a Service-Linked Role for Amazon Chime Live Transcription

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

To manually delete the service-linked role using IAM

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

Supported Regions for Amazon Chime Service-Linked Roles

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, and Using Amazon Chime SDK media Regions.

Using roles with Amazon Chime SDK media pipelines

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

Topics

- Service-linked role permissions for Amazon Chime SDK media pipelines
- Creating a service-linked role for Amazon Chime SDK media pipelines
- Editing a service-linked role for Amazon Chime SDK media pipelines
- Deleting a service-linked role for Amazon Chime SDK media pipelines
- Supported Regions for Amazon Chime SDK media pipelines service-linked roles

Service-linked role permissions for Amazon Chime SDK media pipelines

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

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

- `mediapipelines.chime.amazonaws.com`

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

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

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

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

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

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

To create the role

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.

2. In the navigation pane of the IAM console, choose **Roles**, then choose **Create role**.

3. Choose the **AWS Service** role type, then choose **Chime**, then choose **Chime SDK Media Pipelines**.

4. Choose **Next**.

5. Choose **Next**.

6. Edit the description as needed, then choose **Create role**.

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

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

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

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

Amazon Chime does not allow you to edit the AWSServiceRoleForAmazonChimeSDKMediaPipelines service-linked role. After you create a service-linked role, you cannot change the name of the role

because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see [Editing a Service-Linked Role](#) in the *IAM User Guide*.

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

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

To manually delete the service-linked role using IAM

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

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

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

Logging and monitoring in 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](#)
- [Automating Amazon Chime with EventBridge](#)
- [Logging Amazon Chime API calls with AWS CloudTrail](#)

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

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

Metric	Description
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

Metric	Description
`CustomerToVcRtcpPackets`	The number of RTCP packets sent from the customer to the Amazon Chime Voice Connector infrastructure. Units: Count
`CustomerToVcRtcpBytes`	The number of bytes sent from the customer to the Amazon Chime Voice Connector infrastructure in RTCP packets. Units: Count
`CustomerToVcPacketsLost`	The number of packets lost in transit from the customer to the Amazon Chime Voice Connector infrastructure. Units: Count
`CustomerToVcJitter`	The average jitter for packets sent from the customer to the Amazon Chime Voice Connector infrastructure. Units: Microseconds
`VcToCustomerRtpPackets`	The number of RTP packets sent from the Amazon Chime Voice Connector infrastructure to the customer. Units: Count
`VcToCustomerRtpBytes`	The number of bytes sent from the Amazon Chime Voice Connector infrastructure to the customer in RTP packets. Units: Count

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

Metric	Description
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

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

Metric	Description
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 in the *Amazon Chime SDK Administration Guide*.

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	Corresponds to the Transaction ID.
from_sip_user	The initiating user for the call.
from_country	The initiating country for the call.
to_sip_user	The receiving user for the call.
to_country	The receiving country for the call.
endpoint_id	An opaque identifier indicating the other endpoint of the call. Use with CloudWatch Logs Insights. For more information, see Analyzing log data with CloudWatch Logs Insights in the *Amazon CloudWatch Logs User Guide*.
aws_region	The AWS Region for the call.
cust2vc_rtp_packets	The number of RTP packets sent from the customer to the Amazon Chime Voice Connector infrastructure.
cust2vc_rtp_bytes	The number of bytes sent from the customer to the Amazon Chime Voice Connector infrastructure in RTP packets.

Field	Description
cust2vc_rtcp_packets	The number of RTCP packets sent from the customer to the Amazon Chime Voice Connector infrastructure.
cust2vc_rtcp_bytes	The number of bytes sent from the customer to the Amazon Chime Voice Connector infrastructure in RTCP packets.
cust2vc_packets_lost	The number of packets lost in transit from the customer to the Amazon Chime Voice Connector infrastructure.
cust2vc_jitter	The average jitter for packets sent from the customer to the Amazon Chime Voice Connector infrastructure.
vc2cust_rtp_packets	The number of RTP packets sent from the Amazon Chime Voice Connector infrastructure to the customer.
vc2cust_rtp_bytes	The number of bytes sent from the Amazon Chime Voice Connector infrastructure to the customer in RTP packets.
vc2cust_rtcp_packets	The number of RTCP packets sent from the Amazon Chime Voice Connector infrastructure to the customer.
vc2cust_rtcp_bytes	The number of bytes sent from the Amazon Chime Voice Connector infrastructure to the customer in RTCP packets.
vc2cust_packets_lost	The number of packets lost in transit from the Amazon Chime Voice Connector infrastructure to the customer.

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

Field	Description
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.
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. For more information about the meeting events, see Meeting events in the *Amazon Chime Developer Guide*.

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

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

Automating Amazon Chime Voice Connectors with EventBridge

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

- Invoking an AWS Lambda function

- Launching an Amazon Elastic Container Service task

- Relaying the event to Amazon Kinesis Video Streams

- Activating an AWS Step Functions state machine

- Notifying an Amazon SNS topic or an Amazon SQS queue

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

- Activating a Lambda function to download audio for a call after the call is ended.

- Launching an Amazon ECS task to enable real-time transcription after a call is started.

For more information, see the Amazon EventBridge User Guide.

Amazon Chime Voice Connector streaming events

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

Amazon Chime Voice Connector streaming starts

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

Example Event data

The following is example data for this event.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-111122223333",
    "detail-type": "Chime VoiceConnector Streaming Status",
    "source": "aws.chime",
    "account": "111122223333",
    "time": "yyyy-mm-ddThh:mm:ssZ",
```

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

Amazon Chime Voice Connector streaming ends

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

Example Event data

The following is example data for this event.

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

Amazon Chime Voice Connector streaming updates

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

Example Event data

The following is example data for this event.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-111122223333",
    "detail-type": "Chime VoiceConnector Streaming Status",
    "source": "aws.chime",
    "account": "111122223333",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "callId": "1112-2222-4333",
        "updateHeaders": {
            "from": "\"John\" <sip:+12065550100@10.24.34.0>;;tag=abcdefg",
            "to": "<sip:
 +13605550199@abcdef1ghij2klmno3pqr4.voiceconnector.chime.aws:5060>",
            "call-id": "1112-2222-4333",
            "cseq": "101 INVITE",
            "contact": "<sip:user@10.24.34.0:6090>",
            "content-type": "application/sdp",
            "content-length": "246"
        },
        "siprecMetadata": "<&xml version=\"1.0\" encoding=\"UTF-8\"&>\r\n<recording
 xmlns='urn:ietf:params:xml:ns:recording:1'>",
        "streamingStatus": "UPDATED",
        "transactionId": "12345678-1234-1234",
        "version": "0",
        "voiceConnectorId": "abcdef1ghij2klmno3pqr4"
    }
}
```

Amazon Chime Voice Connector streaming fails

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

Example Event data

The following is example data for this event.

```
{
  "version": "0",
  "id": "12345678-1234-1234-1234-111122223333",
  "detail-type": "Chime VoiceConnector Streaming Status",
  "source": "aws.chime",
  "account": "111122223333",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
  "resources": [],
  "detail": {
      "streamingStatus":"FAILED",
      "voiceConnectorId":"abcdefghi",
      "transactionId":"12345678-1234-1234",
      "callId":"1112-2222-4333",
      "direction":"Inbound",
      "failTime":"yyyy-mm-ddThh:mm:ssZ",
      "failureReason": "Internal failure",
      "version":"0"
  }
}
```

Logging Amazon Chime 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 a 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 AWS services as part of multiple AWS compliance programs, such as SOC, PCI, FedRAMP, and HIPAA.

To learn whether an AWS service is within the scope of specific compliance programs, see [AWS services in Scope by Compliance Program](#) and choose the compliance program that you are interested in. For general information, see [AWS Compliance Programs](#).

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

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

- [Security and Compliance Quick Start Guides](#) – These deployment guides discuss architectural considerations and provide steps for deploying baseline environments on AWS that are security and compliance focused.

- [Architecting for HIPAA Security and Compliance on Amazon Web Services](#) – This whitepaper describes how companies can use AWS to create HIPAA-eligible applications.

> **ⓘ Note**
>
> Not all AWS services are HIPAA eligible. For more information, see the [HIPAA Eligible Services Reference](#).

- [AWS Compliance Resources](#) – This collection of workbooks and guides might apply to your industry and location.

- **AWS Customer Compliance Guides** – Understand the shared responsibility model through the lens of compliance. The guides summarize the best practices for securing AWS services and map the guidance to security controls across multiple frameworks (including National Institute of Standards and Technology (NIST), Payment Card Industry Security Standards Council (PCI), and International Organization for Standardization (ISO)).

- **Evaluating Resources with Rules** in the *AWS Config Developer Guide* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.

- **AWS Security Hub** – This AWS service provides a comprehensive view of your security state within AWS. Security Hub uses security controls to evaluate your AWS resources and to check your compliance against security industry standards and best practices. For a list of supported services and controls, see **Security Hub controls reference**.

- **Amazon GuardDuty** – This AWS service detects potential threats to your AWS accounts, workloads, containers, and data by monitoring your environment for suspicious and malicious activities. GuardDuty can help you address various compliance requirements, like PCI DSS, by meeting intrusion detection requirements mandated by certain compliance frameworks.

- **AWS Audit Manager** – This AWS service helps you continuously audit your AWS usage to simplify how you manage risk and compliance with regulations and industry standards.

Resilience in 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** and **Streaming Amazon Chime Voice Connector media to Kinesis** in the *Amazon Chime SDK Administration Guide*.

Infrastructure security in Amazon Chime

As a managed service, Amazon Chime is protected by AWS global network security. For information about AWS security services and how AWS protects infrastructure, see [AWS Cloud Security](#). To design your AWS environment using the best practices for infrastructure security, see [Infrastructure Protection](#) in *Security Pillar AWS Well-Architected Framework*.

You use AWS published API calls to access through the network. Clients must support the following:

- Transport Layer Security (TLS). We require TLS 1.2 and recommend TLS 1.3.

- Cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). 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.

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.

Change	Description	Date
[Amazon Chime SDK Administration Guide published](#)	The Amazon Chime SDK topics are now published in the *Amazon Chime SDK Administration Guide*. For for information, see the [Amazon Chime SDK Administration Guide](#).	March 24, 2022
[IAM policy updates](#)	Changes to IAM policies managed by AWS are now tracked in this administrator's guide. See [Amazon Chime identity-based policy examples](#).	September 23, 2021
[Service-linked roles](#)	Administrators can now create service-linked roles for Amazon Live Transcription, and view event messages when an Amazon Chime live transcription operation starts and ends. For more information, see [Using roles with live transcription](#) and [Automating Amazon Chime with CloudWatch events](#).	August 12, 2021
[SIP media applications and rule](#)	Administrators can create SIP media applications and rules	November 18, 2020

for use with Amazon Chime
Voice Connector and AWS
Lambda functions. For more
information, see Managing
SIP applications and rules, in
the Amazon Chime Administr
ator Guide.

Amazon Chime Voice Connector emergency call routing numbers	Amazon Chime administr ators 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	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	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	If you have the ability to program, you can use a pair of Amazon Chime APIs to remove messages from the chat rooms and conversat ions in your account. For more information, see Deleting individual messages, in the Amazon Chime Administrator Guide.	May 18, 2020
CloudWatch media quality metrics for Amazon Chime Voice Connector	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	Amazon Chime supports the Amazon Chime Meetings App for Slack. For more information, see Setting up the Amazon Chime Meetings App for Slack, in the Amazon Chime Administrator Guide.	December 4, 2019
Meeting Region settings	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	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	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	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 | 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 the Amazon Chime Voice Connector service-linked role, in the Amazon Chime Administrator Guide. | October 24, 2019 |
| Monitoring Amazon Chime with Amazon CloudWatch | 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](#)	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 Administr ator Guide.	October 24, 2019
[Network configuration updates](#)	Amazon Chime is simplifyi ng its firewall requirements. For more information, see [Network configuration and bandwidth requirements](#), in the Amazon Chime Administr ator Guide.	September 6, 2019
[Moderated meetings](#)	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](#)	Amazon Chime is a HIPAA Eligible Service. For more information, see [Complianc e validation for Amazon Chime](#) in the Amazon Chime Administrator Guide.	June 11, 2019

Porting toll-free phone numbers	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	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	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	Various updates to topic layout and organization.	February 11, 2019

Amazon Chime call me feature	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	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	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	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	Assign users Pro or Basic permissions. For more information, see Manage user access and permissions, in the Amazon Chime Administrator Guide.	March 29, 2018