Amazon Chime
Administration Guide
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is Amazon Chime?</td>
<td>vi</td>
</tr>
<tr>
<td>Administration overview</td>
<td>1</td>
</tr>
<tr>
<td>How to get started</td>
<td>1</td>
</tr>
<tr>
<td>Pricing</td>
<td>1</td>
</tr>
<tr>
<td>Resources</td>
<td>1</td>
</tr>
<tr>
<td>Prerequisites for Amazon Chime system administrators</td>
<td>3</td>
</tr>
<tr>
<td>Creating an Amazon Web Services account</td>
<td>3</td>
</tr>
<tr>
<td>Sign up for an AWS account</td>
<td>3</td>
</tr>
<tr>
<td>Create an administrative user</td>
<td>3</td>
</tr>
<tr>
<td>Getting started</td>
<td>5</td>
</tr>
<tr>
<td>Step 1: Creating an Amazon Chime administrator account</td>
<td>5</td>
</tr>
<tr>
<td>Step 2 (optional): Configuring account settings</td>
<td>5</td>
</tr>
<tr>
<td>Step 3: Adding users to your account</td>
<td>6</td>
</tr>
<tr>
<td>(Optional) Setting up phone numbers for your Amazon Chime account</td>
<td>7</td>
</tr>
<tr>
<td>Managing your accounts</td>
<td>8</td>
</tr>
<tr>
<td>Choosing a Team or Enterprise account</td>
<td>8</td>
</tr>
<tr>
<td>Converting a Team account to an Enterprise account</td>
<td>9</td>
</tr>
<tr>
<td>Renaming your account</td>
<td>9</td>
</tr>
<tr>
<td>Deleting your account</td>
<td>10</td>
</tr>
<tr>
<td>Managing meeting settings</td>
<td>11</td>
</tr>
<tr>
<td>Meeting policy settings</td>
<td>11</td>
</tr>
<tr>
<td>Meeting application settings</td>
<td>11</td>
</tr>
<tr>
<td>Meeting Region settings</td>
<td>11</td>
</tr>
<tr>
<td>Managing chat retention policies</td>
<td>12</td>
</tr>
<tr>
<td>How retention policies affect Amazon Chime users</td>
<td>12</td>
</tr>
<tr>
<td>Turning on chat retention</td>
<td>14</td>
</tr>
<tr>
<td>Restoring and deleting chat messages</td>
<td>14</td>
</tr>
<tr>
<td>Managing messages</td>
<td>14</td>
</tr>
<tr>
<td>Removing messages</td>
<td>15</td>
</tr>
<tr>
<td>Claiming a domain</td>
<td>15</td>
</tr>
<tr>
<td>Connecting to Active Directory</td>
<td>16</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>16</td>
</tr>
<tr>
<td>Connecting to your Active Directory in Amazon Chime</td>
<td>16</td>
</tr>
<tr>
<td>Configuring multiple email addresses</td>
<td>17</td>
</tr>
<tr>
<td>Connecting to Okta SSO</td>
<td>18</td>
</tr>
<tr>
<td>Deploying the Add-In for Outlook</td>
<td>19</td>
</tr>
<tr>
<td>Setting up the Amazon Chime Meetings App for Slack</td>
<td>20</td>
</tr>
<tr>
<td>Installing the Amazon Chime Meetings App for Slack on an organization</td>
<td>20</td>
</tr>
<tr>
<td>Installing the Amazon Chime Meetings App for Slack on workspaces</td>
<td>21</td>
</tr>
<tr>
<td>Migrating workspaces to organizations</td>
<td>21</td>
</tr>
<tr>
<td>Associating workspaces with Amazon Chime Team accounts</td>
<td>21</td>
</tr>
<tr>
<td>Managing users</td>
<td>23</td>
</tr>
<tr>
<td>Adding users</td>
<td>23</td>
</tr>
<tr>
<td>Viewing user details</td>
<td>23</td>
</tr>
<tr>
<td>Managing user permissions and access</td>
<td>25</td>
</tr>
<tr>
<td>Managing user permissions</td>
<td>25</td>
</tr>
<tr>
<td>Managing user access</td>
<td>26</td>
</tr>
<tr>
<td>Managing user phone numbers</td>
<td>27</td>
</tr>
<tr>
<td>Assigning phone numbers to users</td>
<td>27</td>
</tr>
<tr>
<td>Editing calling and SMS permissions</td>
<td>28</td>
</tr>
<tr>
<td>Unassigning phone numbers from users</td>
<td>28</td>
</tr>
<tr>
<td>Changing personal meeting PINs</td>
<td>28</td>
</tr>
<tr>
<td>Managing Pro trials</td>
<td>29</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Requesting user attachments</td>
<td>29</td>
</tr>
<tr>
<td>How Amazon Chime manages automatic updates</td>
<td>30</td>
</tr>
<tr>
<td>Migrating users to another Team account</td>
<td>30</td>
</tr>
<tr>
<td>Managing phone numbers</td>
<td>32</td>
</tr>
<tr>
<td>Provisioning phone numbers</td>
<td>33</td>
</tr>
<tr>
<td>Requesting international phone numbers</td>
<td>33</td>
</tr>
<tr>
<td>Country requirements for phone numbers</td>
<td>34</td>
</tr>
<tr>
<td>Porting existing phone numbers</td>
<td>45</td>
</tr>
<tr>
<td>- Porting phone numbers into Amazon Chime</td>
<td>45</td>
</tr>
<tr>
<td>- Porting phone numbers out of Amazon Chime</td>
<td>47</td>
</tr>
<tr>
<td>Phone number porting status definitions</td>
<td>48</td>
</tr>
<tr>
<td>Managing phone number inventory</td>
<td>48</td>
</tr>
<tr>
<td>Updating outbound calling names</td>
<td>49</td>
</tr>
<tr>
<td>Deleting phone numbers</td>
<td>50</td>
</tr>
<tr>
<td>Restoring deleted phone numbers</td>
<td>51</td>
</tr>
<tr>
<td>Managing global settings</td>
<td>52</td>
</tr>
<tr>
<td>- Configuring call detail records</td>
<td>52</td>
</tr>
<tr>
<td>- Amazon Chime Business Calling call detail records</td>
<td>52</td>
</tr>
<tr>
<td>Conference room configuration</td>
<td>54</td>
</tr>
<tr>
<td>- Joining a moderated meeting</td>
<td>54</td>
</tr>
<tr>
<td>- Compatible VTC devices</td>
<td>54</td>
</tr>
<tr>
<td>Network configuration and bandwidth requirements</td>
<td>56</td>
</tr>
<tr>
<td>- Common</td>
<td>56</td>
</tr>
<tr>
<td>- Meetings and Business Calling</td>
<td>56</td>
</tr>
<tr>
<td>- H.323 room systems</td>
<td>56</td>
</tr>
<tr>
<td>- Session Initiation Protocol (SIP) room systems</td>
<td>57</td>
</tr>
<tr>
<td>- Bandwidth requirements</td>
<td>57</td>
</tr>
<tr>
<td>Viewing reports</td>
<td>59</td>
</tr>
<tr>
<td>Extending the Amazon Chime desktop client</td>
<td>60</td>
</tr>
<tr>
<td>User management</td>
<td>60</td>
</tr>
<tr>
<td>- Invite multiple users</td>
<td>60</td>
</tr>
<tr>
<td>- Downloading user lists</td>
<td>60</td>
</tr>
<tr>
<td>- Log out multiple users</td>
<td>61</td>
</tr>
<tr>
<td>- Update user personal PINs</td>
<td>61</td>
</tr>
<tr>
<td>Integrating chatbots</td>
<td>61</td>
</tr>
<tr>
<td>- Using chatbots with Amazon Chime</td>
<td>62</td>
</tr>
<tr>
<td>- Amazon Chime events sent to chatbots</td>
<td>68</td>
</tr>
<tr>
<td>Proxy phone sessions</td>
<td>69</td>
</tr>
<tr>
<td>Creating webhooks</td>
<td>70</td>
</tr>
<tr>
<td>- Troubleshooting webhook errors</td>
<td>71</td>
</tr>
<tr>
<td>Administrative support</td>
<td>72</td>
</tr>
<tr>
<td>Security</td>
<td>73</td>
</tr>
<tr>
<td>- Identity and access management</td>
<td>73</td>
</tr>
<tr>
<td>- Audience</td>
<td>74</td>
</tr>
<tr>
<td>- Authenticating with identities</td>
<td>74</td>
</tr>
<tr>
<td>- Managing access using policies</td>
<td>76</td>
</tr>
<tr>
<td>How Amazon Chime works with IAM</td>
<td>78</td>
</tr>
<tr>
<td>- Amazon Chime identity-based policies</td>
<td>78</td>
</tr>
<tr>
<td>- Resources</td>
<td>79</td>
</tr>
<tr>
<td>- Examples</td>
<td>79</td>
</tr>
<tr>
<td>Cross-service confused deputy prevention</td>
<td>79</td>
</tr>
<tr>
<td>Amazon Chime resource-based policies</td>
<td>80</td>
</tr>
<tr>
<td>Authorization based on Amazon Chime tags</td>
<td>80</td>
</tr>
<tr>
<td>Amazon Chime IAM roles</td>
<td>80</td>
</tr>
<tr>
<td>- Using temporary credentials with Amazon Chime</td>
<td>80</td>
</tr>
<tr>
<td>- Service-linked roles</td>
<td>80</td>
</tr>
</tbody>
</table>
Service roles .................................................................................................................. 80
Identity-based policy examples .......................................................................................... 81
Policy best practices .......................................................................................................... 81
Using the Amazon Chime console .................................................................................... 82
Allow users full access to Amazon Chime .......................................................................... 82
Allow users to view their own permissions ......................................................................... 83
Allow users to access user management actions .................................................................. 84
AWS managed policy: AmazonChimeVoiceConnectorServiceLinkedRolePolicy .................. 85
Amazon Chime updates to AWS managed policies .......................................................... 85
Troubleshooting ................................................................................................................ 86
   I am not authorized to perform an action in Amazon Chime .............................................. 86
   I am not authorized to perform iam:PassRole ..................................................................... 86
   I want to allow people outside of my AWS account to access my Amazon Chime resources .. 87
Using service-linked roles ................................................................................................. 87
   Using roles with shared devices ....................................................................................... 87
   Using roles with live transcription .................................................................................... 89
   Using roles with media pipeline ....................................................................................... 91
Logging and monitoring ..................................................................................................... 92
   Monitoring with CloudWatch ........................................................................................... 93
   Automating with EventBridge ......................................................................................... 101
   Logging service API calls .............................................................................................. 104
Compliance validation ....................................................................................................... 106
Resilience .......................................................................................................................... 107
Infrastructure security ....................................................................................................... 107
Understanding Amazon Chime automatic updates .......................................................... 107
Document history .............................................................................................................. 109
AWS glossary .................................................................................................................... 114
You must have the Amazon Chime system administrator role 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 (p. 3).

How to get started

After you complete the Prerequisites for Amazon Chime system administrators (p. 3), you can create and configure your Amazon Chime administrative account, then add users to it. Choose Pro or Basic permissions for your users.

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

• Getting started (p. 5)

For more information on user access and permissions, see Managing user permissions and access (p. 25). 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.

Topics
- Sign up for an AWS account (p. 3)
- Create an administrative user (p. 3)

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

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 an administrative 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 an administrative user

After you sign up for an AWS account, 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 an administrative user

- For your daily administrative tasks, grant administrative access to an administrative user in AWS IAM Identity Center.
  For instructions, see Getting started in the AWS IAM Identity Center User Guide.

Sign in as the administrative user

- 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.

For more information about setting up your Amazon Chime administrator account, see Getting started (p. 5).
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 (p. 3), 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 (p. 5)
- Step 2 (optional): Configuring account settings (p. 5)
- Step 3: Adding users to your account (p. 6)
- (Optional) Setting up phone numbers for your Amazon Chime account (p. 7)

Step 1: Creating an Amazon Chime administrator account

After you complete the Prerequisites for Amazon Chime system administrators (p. 3), you can create an Amazon Chime administrator account.

To create an Amazon Chime administrator account

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. On the Accounts page, choose New account.
3. For Account Name, enter a name for the account and choose Create account.
4. (Optional) Choose whether to let Amazon Chime select the optimal AWS Region for your meetings from all available Regions, or to use only the Regions that you select. For more information, see Managing meeting settings (p. 11).

Step 2 (optional): Configuring account settings

By default, new accounts are created as Team accounts. If you prefer to claim a domain and connect to your own identity provider, or Okta SSO, you can convert to an Enterprise account. For more information about Team and Enterprise account types, see Choosing between an Amazon Chime Team account or Enterprise account (p. 8).

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.
Step 3: Adding users to your account

After your Amazon Chime Team account is created, invite yourself and your users to join it. If you are upgrading your account to an Enterprise account, you do not need to invite your users. Instead, upgrade to an Enterprise account and claim your domain. For more information, see Step 2 (optional): Configuring account settings (p. 5).

To add users to your Amazon Chime account

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

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

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

To change user permissions

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

You can provide other users with administrator permissions, and also control their access to the Amazon Chime console for your account. For more information, see [Identity and access management for Amazon Chime](p. 73).

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

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

**Amazon Chime Business Calling**

Lets your users send and receive phone calls and text messages directly from Amazon Chime. Provision your phone numbers in the Amazon Chime console or port in existing phone numbers. Assign the phone numbers to your Amazon Chime users and grant them permissions to send and receive phone calls and text messages using Amazon Chime. For more information, see [Managing phone numbers in Amazon Chime](p. 32) and [Porting existing phone numbers](p. 45).

**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 (p. 5).

For more information about the different types of Amazon Chime administrator accounts, see Choosing between an Amazon Chime Team account or Enterprise account (p. 8). For more information about managing an existing administrator account, see the following topics.

Topics
- Choosing between an Amazon Chime Team account or Enterprise account (p. 8)
- Converting a Team account to an Enterprise account (p. 9)
- Renaming your account (p. 9)
- Deleting your account (p. 10)
- Managing meeting settings (p. 11)
- Managing chat retention policies (p. 12)
- Managing messages (p. 14)
- Claiming a domain (p. 15)
- Connecting to your Active Directory (p. 16)
- Connecting to Okta SSO (p. 18)
- Deploying the Amazon Chime Add-In for Outlook (p. 19)
- Setting up the Amazon Chime Meetings App for Slack (p. 20)

Choosing between an Amazon Chime Team account or Enterprise account

When you create an Amazon Chime administrator account, you choose whether to create a Team account or an Enterprise account. For more information about creating an Amazon Chime administrator account, see Getting started (p. 5).

Team account

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

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

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

To create an Enterprise account, you must claim at least one email domain. This ensures that all users who sign in to Amazon Chime using your claimed domains are included in your centrally managed Amazon Chime account. Enterprise accounts are required for managing your users through a supported directory integration. For more information, see Claiming a domain (p. 15) and Connecting to your Active Directory (p. 16).

You can also manage user activation and suspension from your Enterprise account. For more information, see Managing user permissions and access (p. 25).

Converting a Team account to an Enterprise account

To convert an existing Team account to an Enterprise account, claim one or more email domains in the Amazon Chime console. For more information about the differences between Team and Enterprise accounts, see Choosing between an Amazon Chime Team account or Enterprise account (p. 8). For more information about claiming a domain, see Claiming a domain (p. 15).

To convert a Team account to an Enterprise account

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

After your account is converted to an Enterprise account, you can decide whether to connect an Active Directory instance through AWS Directory Service. Connecting to an Active Directory instance allows your users to sign in to Amazon Chime using their Active Directory credentials. For more information, see Connecting to your Active Directory (p. 16).

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

Renaming your account

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

To rename your account

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

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

**To delete an Enterprise account**

1. Remove the domains.

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

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

Managing meeting settings

Manage your meeting settings from the Amazon Chime console.

Meeting policy settings

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

Enable shared control in screen sharing

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

Enable outbound calling to join meetings

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

Meeting application settings

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

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

This option lets users in your organization sign in to Amazon Chime from the Amazon Chime Meetings App for Slack. For more information, see Setting up the Amazon Chime Meetings App for Slack (p. 20).

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.

<table>
<thead>
<tr>
<th>If the chat conversation includes...</th>
<th>The retention policy is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only other members of the user’s Enterprise account</td>
<td>Set by the user’s administrator</td>
</tr>
<tr>
<td>Anyone outside of the user’s Enterprise account</td>
<td>Automatically set to 90 days</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>If the chat room is created by...</th>
<th>The retention policy is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>A member of the user’s Enterprise account</td>
<td>Set by the user’s administrator</td>
</tr>
<tr>
<td>Another Enterprise account member</td>
<td>Set by the other account’s administrator</td>
</tr>
<tr>
<td>A non-Enterprise account member</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

**Team member chat conversations**

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

<table>
<thead>
<tr>
<th>If the chat conversation includes...</th>
<th>The retention policy is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only users who are not members of an Enterprise account</td>
<td>Not applicable</td>
</tr>
<tr>
<td>At least one member of an Enterprise account</td>
<td>Automatically set to 90 days</td>
</tr>
</tbody>
</table>

**Team member chat rooms**

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

<table>
<thead>
<tr>
<th>If the chat room is created by ...</th>
<th>The retention policy is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Team account user</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Anyone who is not an Enterprise account member</td>
<td>Not applicable</td>
</tr>
<tr>
<td>A member of an Enterprise account</td>
<td>Set by the Enterprise account's administrator</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>If the chat conversation includes...</th>
<th>The retention policy is...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only users who are not members of an Enterprise account</td>
<td>Not applicable</td>
</tr>
<tr>
<td>At least one member of an Enterprise account</td>
<td>Automatically set to 90 days</td>
</tr>
</tbody>
</table>

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

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

Restoring and deleting chat messages

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

**Note**

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

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

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

Managing messages

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

---

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

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

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

To remove a message

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

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

Claiming a domain

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

To claim a domain

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

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

Amazon Chime checks for the existence of this record to verify that you own the domain. After the domain is verified, its status changes from Pending verification to Verified.
Note
Propagation of the DNS change and verification by Amazon Chime can take up to 24 hours.

7. If your organization uses additional domains or subdomains for email addresses, repeat this procedure for each domain.

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

Connecting to your Active Directory

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

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

For more information about managing user permissions, see Managing user permissions and access (p. 25).

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 (p. 73).
- Create a directory with AWS Directory Service that is configured in the US East (N. Virginia) Region. For more information, see the AWS Directory Service Administration Guide. Amazon Chime can connect using AD Connector, Microsoft AD, or Simple AD.
- Claim a domain in order to create an Amazon Chime Enterprise account, or convert your existing Team account to an Enterprise account. If your users have work email addresses from more than one domain, make sure to claim all of those domains. For more information, see Claiming a domain (p. 15) and Converting a Team account to an Enterprise account (p. 9).

Connecting to your Active Directory in Amazon Chime

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

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. In the navigation pane, for Identity, choose Active directory.
3. For Cloud directory ID, select the AWS Directory Service directory to use for Amazon Chime, and then choose Connect.
   
   **Note**
   
   You can find your directory ID using the AWS Directory Service console.
4. After your directory connects, choose Add a new group.
5. For Group, enter the group name. The name must exactly match an Active Directory group in the target directory. Active Directory Organization Units (OUs) are not supported.
6. For Permissions, choose Basic or Pro.
7. Choose Add group.
8. (Optional) Repeat this procedure to create additional directory groups.

Configuring multiple email addresses

After you connect to your Active Directory in Amazon Chime, users can sign in to Amazon Chime using their Active Directory credentials. Your users can have multiple email addresses assigned to them in your Active Directory. To allow your users to sign in to Amazon Chime using their Active Directory credentials, you must claim each applicable email domain in your Amazon Chime administrative account. For more information, see Claiming a domain (p. 15).

**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 (p. 15)](#).

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 (p. 20)
- Installing the Amazon Chime Meetings App for Slack on workspaces (p. 21)
- Migrating workspaces to organizations (p. 21)
- Associating workspaces with Amazon Chime Team accounts (p. 21)

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 (p. 21)** 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 (p. 11)**.
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 (p. 3).

**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.
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

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 (p. 23).

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 (p. 25).

Contents
- Adding users (p. 23)
- Viewing user details (p. 23)
- Managing user permissions and access (p. 25)
- Managing user phone numbers (p. 27)
- Changing personal meeting PINs (p. 28)
- Managing Pro trials (p. 29)
- Requesting user attachments (p. 29)
- How Amazon Chime manages automatic updates (p. 30)
- Migrating users to another Team account (p. 30)

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. On the Home page of the console, in the left-hand pane, choose Accounts.

   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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>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.</td>
<td>Major, Mary</td>
</tr>
<tr>
<td>Email address</td>
<td>For LWA users, the email address used for registration. For Active Directory users, the primary email address from Active Directory appears.</td>
<td><a href="mailto:mary.major@example.com">mary.major@example.com</a></td>
</tr>
<tr>
<td>Registration</td>
<td>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.</td>
<td>Registered, Unregistered</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(for a Team account), or</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Suspended (for an Enterprise account)</td>
</tr>
<tr>
<td>Permission tier</td>
<td>Set to <strong>Pro</strong> by default, to allow users to host meetings. It can be changed to <strong>Basic</strong>.</td>
<td>Pro, Basic</td>
</tr>
<tr>
<td>Invited</td>
<td>For Team accounts, the date when the user was invited to the account.</td>
<td>01/05/2020</td>
</tr>
<tr>
<td>Joined</td>
<td>The date when the user first signed into Amazon Chime. For Pro trial users, this is also the date that their Pro trial began.</td>
<td>01/10/2020</td>
</tr>
<tr>
<td>Personal PIN</td>
<td>The personal meeting PIN that the user can use to schedule meetings.</td>
<td>0123456789</td>
</tr>
<tr>
<td>Privacy setting</td>
<td>The presence setting that the user selected.</td>
<td>Public or Private</td>
</tr>
<tr>
<td>Meetings attended</td>
<td>The number of meetings that a user has attended.</td>
<td>87</td>
</tr>
<tr>
<td>Meetings organized</td>
<td>The number of meetings that a user has organized.</td>
<td>12</td>
</tr>
<tr>
<td>Meeting satisfaction</td>
<td>The percentage of positive responses given to the end-of-meeting survey.</td>
<td>92%</td>
</tr>
</tbody>
</table>
### 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/](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**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last active date</td>
<td>The date when the user was last active.</td>
<td>06/12/2020</td>
</tr>
<tr>
<td>Chat messages sent</td>
<td>The number of chat messages the user sent.</td>
<td>1025</td>
</tr>
<tr>
<td>Phone number</td>
<td>The phone number assigned to a user, if any.</td>
<td>+12065550100</td>
</tr>
</tbody>
</table>
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 them to sign in to your account. Enterprise account administrators can suspend user access to prevent them from signing in to the account.

Inviting and removing Team account users

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

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

To invite users to a Team account

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

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

To remove users from a Team account

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

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

Inviting and suspending Enterprise account users

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

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

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

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

To suspend users from an Enterprise account

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

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

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

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

Managing user phone numbers

The following sections explain how to use the Amazon Chime console to manage phone numbers for an Amazon Chime administrative account. For more information about , see Managing phone numbers in Amazon Chime (p. 32).

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

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

Assigning phone numbers to users

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

To assign a phone number to a user

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

The phone number is assigned to the user in your account. Calling and SMS permissions are turned off by default. For more information about editing these permissions, see **Editing calling and SMS permissions** (p. 28).

**Editing calling and SMS permissions**

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

To edit a user's calling and SMS permissions

1. Open the Amazon Chime console at [https://chime.aws.amazon.com/](https://chime.aws.amazon.com/).
2. For **Accounts**, choose the account name that the user belongs to.
3. In the navigation pane, choose **Users**.
4. Choose the full name of the user.
5. On the user details page, for **Actions**, choose **Edit telephony permissions**.
6. Select the desired calling and SMS permissions for the user, and choose **Save**.

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

**Unassigning phone numbers from users**

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

To unassign a phone number from a user

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

**Changing personal meeting PINs**

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

If a user feels that their personal meeting PIN has been compromised, you can reset their PIN and generate a new ID. After you update a personal meeting PIN, the user must update all meetings that were scheduled using the old personal meeting PIN.
To change a personal meeting PIN
1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. On the Accounts page, select the name of the Amazon Chime account.
3. In the navigation pane, choose Users.
4. Search for the user who needs their PIN changed.
5. To open the User detail page, choose the name of the user.
6. Choose User actions, Reset personal PIN, Confirm.

Managing Pro trials

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

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

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

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

For more information, see Plans and Pricing.

Requesting user attachments

If you manage an Enterprise account and have the appropriate permissions, you can request and receive 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.
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.
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 (p. 5).
2. As needed, configure the account. For more information, see Step 2 (optional): Configuring account settings (p. 5).

3. Add users to the account. For more information, see Step 3: Adding users to your account (p. 6).
Managing phone numbers in Amazon Chime

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

**Amazon Chime Business Calling**

Lets your users send and receive phone calls and text messages directly from Amazon Chime. You use the Amazon Chime console at [https://chime.aws.amazon.com/](https://chime.aws.amazon.com/) to provision phone numbers and to port in existing phone numbers. You then assign the numbers to your Amazon Chime users and grant them permissions to send and receive phone calls and text messages using.

**Amazon Chime Voice Connector**

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

**Note**

Amazon Chime Business Calling doesn’t offer emergency calling services outside of the United States. To modify the emergency calling services that Amazon Chime provides for the United States, you can obtain an emergency call routing number from a third-party emergency service provider, give that number to Amazon Chime, and complete the configuration with Amazon Chime Voice Connectors. For more information, see [Setting up emergency call routing numbers for your Amazon Chime Voice Connector](#) in the [Amazon Chime SDK Administration Guide](#).

**SIP media applications and rules**

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

Amazon Chime Business Calling has bandwidth requirements. For more information, see [Bandwidth requirements](#).

**Contents**

- Provisioning phone numbers (p. 33)
- Requesting international phone numbers (p. 33)
- Porting existing phone numbers (p. 45)
- Managing phone number inventory (p. 48)
- Updating outbound calling names (p. 49)
- Deleting phone numbers (p. 50)
- Restoring deleted phone numbers (p. 51)
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.

Requesting international phone numbers

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

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

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

Allow 2-6 weeks for Amazon Chime to fulfill your request. For more information about the documentation requirements for various countries, see the section called “Country requirements for phone numbers” (p. 34).

To request international phone numbers in countries with identification requirements

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

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

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

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

Once the numbers are provisioned, you can view the numbers in the Amazon Chime console under Calling, Phone number management, Inventory.

6. Use SIP rules to assign the phone numbers to the appropriate SIP media application.

### Country requirements for phone numbers

Outside the US, regulations often require a local address and specific identification documents in order to purchase and use a phone number. The address can be a business or personal address. The following tables list the countries that require identification. When you request international phone numbers (p. 33) or you port existing phone numbers (p. 45), Amazon Chime support works with you to submit the necessary documents.

**Note**

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

**Topics**

- [Australia](#)
- [Austria](#)
- [Canada](#)
- [Denmark](#)
- [Finland](#)
- [Germany](#)
- [Ireland](#)
- [Italy](#)
- [New Zealand](#)
- [Nigeria](#)
- [Puerto Rico](#)
- [South Korea](#)
- [Sweden](#)
- [Switzerland](#)
• United Kingdom (p. 44)

Australia

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

Ordering phone numbers

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>ID requirements</th>
<th>Acceptable ID types</th>
</tr>
</thead>
</table>
| Amazon Chime SDK SIP media application dial-in | Local         | Yes             | • Business address  
|                          | Toll-free     | Yes             | • Business address  
|                          |               |                 | International addresses accepted. |

Porting phone numbers

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>Required ID</th>
</tr>
</thead>
</table>
| SIP Media Application Dial-In | Local        | • Last invoice from current provider 
|                          | Toll-free    | • Last invoice from current provider | 
|                          |              | • Letter of Authorization |

Austria

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

Ordering phone numbers

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>ID requirements</th>
<th>Acceptable ID types</th>
</tr>
</thead>
</table>
| SIP media application dial-in | Local        | Yes             | • Business address  
|                          |              |                 | • Proof of telecom services such as  |
## Country requirements for phone numbers

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>ID requirements</th>
<th>Acceptable ID types</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>National prefix: +43 720</td>
<td>Yes</td>
<td>• Business address Address must be located in the country.</td>
</tr>
<tr>
<td></td>
<td>Toll-free</td>
<td>Yes</td>
<td>• Business address Foreign address acceptable</td>
</tr>
</tbody>
</table>

### Porting phone numbers

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>Required ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Media Application Dial-In</td>
<td>Local</td>
<td>• Last invoice from current provider • Letter of Authorization</td>
</tr>
<tr>
<td></td>
<td>Toll-free</td>
<td>• Last invoice from current provider • Letter of Authorization</td>
</tr>
</tbody>
</table>

### Canada

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

#### Ordering phone numbers
supported product
types | number types | ID requirements | acceptable ID types
--- | --- | --- | ---
SIP Media Application Dial-In | Local | No | N/A
Toll-free | No | N/A | N/A

Porting phone numbers

<table>
<thead>
<tr>
<th>supported product types</th>
<th>number types</th>
<th>required ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Media Application Dial-In</td>
<td>Local</td>
<td>• Last invoice from current provider • Letter of Authorization</td>
</tr>
<tr>
<td></td>
<td>Toll-free</td>
<td>• Last invoice from current provider • Letter of Authorization</td>
</tr>
</tbody>
</table>

Denmark

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

Ordering phone numbers

<table>
<thead>
<tr>
<th>supported product types</th>
<th>number types</th>
<th>ID requirements</th>
<th>acceptable ID types</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Media Application Dial-In</td>
<td>Local</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Toll-free</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Porting phone numbers

<table>
<thead>
<tr>
<th>supported product types</th>
<th>number types</th>
<th>required ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Media Application Dial-In</td>
<td>Local</td>
<td>• Last invoice from current provider • Letter of Authorization</td>
</tr>
<tr>
<td></td>
<td>Toll-free</td>
<td>• Last invoice from current provider • Letter of Authorization</td>
</tr>
</tbody>
</table>

Finland

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

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>ID requirements</th>
<th>Acceptable ID types</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Media Application</td>
<td>Local</td>
<td>Yes</td>
<td>• Business address</td>
</tr>
<tr>
<td>Dial-In</td>
<td></td>
<td></td>
<td>• Proof of location</td>
</tr>
<tr>
<td></td>
<td>National prefixes +358 075</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Toll-free</td>
<td>No</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Porting phone numbers

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>Required ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Media Application</td>
<td>Local</td>
<td>• Last invoice from current provider</td>
</tr>
<tr>
<td>Dial-In</td>
<td></td>
<td>• Letter of Authorization</td>
</tr>
<tr>
<td></td>
<td>Toll-free</td>
<td>• Last invoice from current provider</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Letter of Authorization</td>
</tr>
</tbody>
</table>

Germany

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

Ordering phone numbers

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>ID requirements</th>
<th>Acceptable ID types</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Media Application</td>
<td>Local</td>
<td>Yes</td>
<td>• Business address</td>
</tr>
<tr>
<td>Dial-In</td>
<td></td>
<td></td>
<td>• A copy of your business registration, or a copy of your ID, if you're an individual</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Proof of address, such as a utility bill</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Business addresses must have the same</td>
</tr>
</tbody>
</table>
Country requirements for phone numbers

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

Porting phone numbers

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>Required ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Media Application Dial-In</td>
<td>Local</td>
<td>• Last invoice from current provider</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Letter of Authorization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Business address</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• A copy of your business registration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Copy of the company representative’s ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Business addresses must have the same geographic zone as their corresponding phone numbers.</td>
</tr>
<tr>
<td>Toll-free</td>
<td></td>
<td>• Last invoice from current provider</td>
</tr>
</tbody>
</table>
Country requirements for phone numbers

### Supported product types | Number types | Required ID
---|---|---
| | | • Letter of Authorization  
| | | • Number certificate from NRAs

You must first obtain the number directly from the local regulator. Details about the process are provided when you make the request.

---

**Ireland**

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

#### Ordering phone numbers

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

#### Porting phone numbers

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>Required ID</th>
<th></th>
</tr>
</thead>
</table>
| SIP Media Application Dial-In | Local | • Last invoice from current provider  
| | | • Letter of Authorization |   |
| | Toll-free | • Last invoice from current provider  
| | | • Letter of Authorization |   |
Italy

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

Ordering phone numbers

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>ID requirements</th>
<th>Acceptable ID types</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Media Application Dial-In</td>
<td>Local</td>
<td>Yes</td>
<td>• Business address&lt;br&gt;• Proof of location&lt;br&gt;• Copy of business registration&lt;br&gt;• Passport or end-user ID&lt;br&gt;Business addresses must be located in the same geographic regions as their corresponding phone numbers.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>Required ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Media Application Dial-In</td>
<td>Local</td>
<td>• Last invoice from current provider&lt;br&gt;• Letter of Authorization&lt;br&gt;• Copy of the company representative's passport or ID&lt;br&gt;• Copy of the local business registration, or proof of address for an individual</td>
</tr>
</tbody>
</table>

Toll-free                  | No            | N/A          |

Porting phone numbers

New Zealand

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

Ordering phone numbers

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>Required ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Media Application Dial-In</td>
<td>Local</td>
<td>• Last invoice from current provider&lt;br&gt;• Letter of Authorization</td>
</tr>
</tbody>
</table>

Toll-free                  |               |             |
Country requirements for phone numbers

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>ID requirements</th>
<th>Acceptable ID types</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Media Application Dial-In</td>
<td>Local</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Toll-free</td>
<td>No</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Porting phone numbers

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>Required ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Media Application Dial-In</td>
<td>Local</td>
<td>Not supported</td>
</tr>
</tbody>
</table>
|                          | Toll-free | • Last invoice from current provider  
|                          |          | • Letter of Authorization |

Nigeria

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

Ordering phone numbers

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>ID requirements</th>
<th>Acceptable ID types</th>
</tr>
</thead>
</table>
| SIP Media Application Dial-In | Local | Yes | • Business address  
|                          |          |                | Foreign address acceptable. |

Puerto Rico

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

Ordering phone numbers

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>ID requirements</th>
<th>Acceptable ID types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Calling</td>
<td>Local</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Voice Connector</td>
<td>Local</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Toll-free</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

South Korea

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

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>ID requirements</th>
<th>Acceptable ID types</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Media Application Dial-In</td>
<td>Toll-free</td>
<td>Yes</td>
<td>• Business address</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Proof of location</td>
</tr>
</tbody>
</table>

Address must be located in the country.

Sweden

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

Ordering phone numbers

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>ID requirements</th>
<th>Acceptable ID types</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Media Application Dial-In</td>
<td>Local</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Toll-free</td>
<td>No</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

Porting phone numbers

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>Required ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Media Application Dial-In</td>
<td>Local</td>
<td>• Last invoice from current provider</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Letter of Authorization</td>
</tr>
<tr>
<td>Toll-free</td>
<td></td>
<td>• Last invoice from current provider</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Letter of Authorization</td>
</tr>
</tbody>
</table>

Switzerland

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

Ordering phone numbers

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>ID requirements</th>
<th>Acceptable ID types</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Media Application Dial-In</td>
<td>Local</td>
<td>Yes</td>
<td>• Business address</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Proof of location</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• A copy of business registration, or a copy</td>
</tr>
</tbody>
</table>
Supported product types | Number types | ID requirements | Acceptable ID types |
---|---|---|---|
| | | | of your ID, if you're an individual |
| | | | Business addresses must have the same geographic zone as their corresponding phone numbers. |
| Business number prefixes: +41 051, +41 058 | Yes | | |
| Toll-free | Yes | | Business address |
| | | | Address must be located in the country. |
| | | | Foreign address acceptable |

Porting phone numbers

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

United Kingdom

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

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>ID requirements</th>
<th>Acceptable ID types</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Media Application Dial-In</td>
<td>Local</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>Toll-free</td>
<td>No</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Porting phone numbers

<table>
<thead>
<tr>
<th>Supported product types</th>
<th>Number types</th>
<th>Required ID</th>
</tr>
</thead>
</table>
| SIP Media Application Dial-In | Local | • Last invoice from current provider  
• Letter of Authorization |
|                         | Toll-free | • Last invoice from current provider  
• Letter of Authorization |

Porting existing phone numbers

In addition to provisioning phone numbers, you can also port numbers from your phone carrier into your Amazon Chime inventory. You can use ported numbers within Amazon Chime Business Calling.

**Note**

You can port toll-free numbers for use with Amazon Chime Voice Connectors, and with Amazon Chime SIP media applications. Amazon Chime Business Calling doesn't support toll-free numbers. For more information, see [Porting existing phone numbers](#) in the [Amazon Chime SDK Administration Guide](#).

Porting phone numbers into Amazon Chime

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

**To port existing phone numbers into Amazon Chime**

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

   **For porting U.S. toll numbers:**
   - Existing phone numbers to port in. Indicate the phone number type—**Business Calling**.
   - Billing Telephone Number (BTN) of the account.
   - Authorizing person’s name. This is the person in charge of account billing with the current carrier.
• Current carrier, if known.
• Service account number, if this information is present with the current carrier.
• Service PIN, if available.
• Service address and customer name, as they appear in your current carrier contract.
• Requested date and time for the port.
• (Optional) If you want to port your BTN, indicate one of the following options:
  • I am porting my BTN and I want to replace it with a new BTN that I am providing. I can confirm that this new BTN is on the same account with the current carrier.
  • I am porting my BTN and I want to close out my account with my current carrier.
  • I am porting my BTN because my account is currently set up so that each phone number is its own BTN. (Select this option only when your account with the current carrier is set up this way.)
  • Download the Letter of Agency (LOA) for Local Telephone Number Porting and fill it out. If you are porting phone numbers from different carriers, fill out a separate LOA for each carrier.

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

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

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

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

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

b. After you are signed in to your AWS account, open the Amazon S3 upload link generated specifically for your account.

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

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

7. After you provide the 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
Porting phone numbers out of Amazon Chime

8. (Optional) View the status of your porting request in the Amazon Chime console under Calling, Phone number management, Pending. AWS Support also contacts you with updates and requests for further information, as needed. For more information, see Phone number porting status definitions (p. 48).

9. Assign Amazon Chime Business Calling phone numbers to individual users.

The phone numbers are not activated for use until after the Firm Order Commit (FOC) date is established, as shown in the following steps. For more information, see Managing phone number inventory (p. 48).

10. After your existing phone carrier confirms that the LOA is correct, they review and approve the requested port. Then they provide AWS Support with a Firm Order Commit (FOC) date and time for the port to occur.

11. AWS Support contacts you with the FOC to confirm that the date and time works for you.

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

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

**Porting phone numbers out of Amazon Chime**

**Note**

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

**To port existing phone numbers out of Amazon Chime**

1. Do one of the following:

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

     Choose Support, Submit request.

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

2. For Category, choose Other.

3. For Subject, enter Porting phone numbers out.

4. For Issue or Description, enter the phone numbers to port out. Indicate the phone number type as Business Calling.

5. Do one of the following:

   • If you are submitting a support request from the Amazon Chime console, for Email, enter the email address associated with your Amazon Chime administrator account. Choose Submit request.

   • If you are creating a case in AWS Support Center, for Contact options, select a contact method. Optionally, for Additional contacts, enter email addresses of people to be notified of case status updates.

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

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

When the porting process is complete and the phone numbers are ported to your new carrier, unassign and delete the phone numbers from your Amazon Chime inventory. For more information, see Managing phone number inventory (p. 48) and Deleting phone numbers (p. 50).

Phone number porting status definitions

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

Porting statuses and definitions include the following:

CANCELLED

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

CANCEL_REQUESTED

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

CHANGE_REQUESTED

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

COMPLETED

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

EXCEPTION

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

FOC

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

PENDING DOCUMENTS

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

SUBMITTED

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

Managing phone number inventory

Use the phone number management Inventory page to assign or unassign phone numbers. You can do this with Amazon Chime Business Calling phone numbers for individual users. Manage Amazon Chime Business Calling phone numbers from within user profiles. For more information, see Managing user phone numbers (p. 27).
To assign an Amazon Chime Business Calling phone number to a user

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

For instructions on how to edit the user’s calling and SMS permissions, see Editing calling and SMS permissions (p. 28). When you change a user’s Amazon Chime Business Calling phone number or phone number permissions, we recommend providing the user with their new phone number or permissions information. Before users can access their new phone number or permissions features, they must sign out of their Amazon Chime account and sign in again.

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

To unassign inventory phone numbers for Amazon Chime Business Calling

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

You can view the details of your inventory phone numbers. For example, you can see which Amazon Chime Business Calling user that a number is assigned to. You can also see if phone calls and text messages are enabled.

To view inventory phone number details

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

Updating outbound calling names

You can set a default calling name for one or more of the phone numbers in your inventory. The name then appears to recipients of outbound calls made using those phone numbers. Default calling names apply to all phone number product types. You can update the names once every seven days.

To set a default 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. Choose the Inventory tab, select the checkboxes next to the phone numbers that you want to update.
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.

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

**To set a unique calling name**

1. Open the Amazon Chime console at https://chime.aws.amazon.com/.
2. In the navigation pane, under Calling, choose Phone number management.
3. Choose the Inventory tab, then select the phone number that you want to name.
4. Open the Actions list and choose View details.
5. On the phone number details screen, for Actions, choose Update unique calling name.
6. For Unique calling name, enter a name of up to 15 characters.
7. Choose Save.

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

**Deleting phone numbers**

**Important**

Only Amazon Chime system administrators can complete these steps. Also, you must unassign phone numbers before you can delete them. Do one of the following:

- If you use a Voice Connector or Voice Connector group, you unassign the number. For more information, refer to [Unassigning phone numbers](#) in the Amazon Chime SDK Administrator Guide.
- If you use a SIP media application, you delete the SIP rule that contains the number. For more information, refer to [Deleting SIP rules](#) in the Amazon Chime SDK Administrator Guide.

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 Amazon Chime SDK 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](#) (p. 33), 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/](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 (p. 32).

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.
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/11112223333/2019/03/01-17.10.00.020_1a234567-89bc-01d2-3456-e78f9g01234h
```

The following example shows the data that is represented in the call detail record name.
The following example shows the general format of an Amazon Chime Business Calling call detail record.

```json
{
  "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 (p. 57).

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

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

- `13.248.147.139`
- `76.223.18.152`

If a firewall is filtering traffic between the VTC device and Amazon Chime, open the ranges for the protocols used. For more information, see Network configuration and bandwidth requirements (p. 56).

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.
## Compatible VTC devices

<table>
<thead>
<tr>
<th>Device</th>
<th>SIP</th>
<th>H.323</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco SX20</td>
<td>Yes</td>
<td>Yes</td>
<td>Audio/Video/Screen: To and From OK</td>
</tr>
<tr>
<td>Cisco DX80</td>
<td>Yes</td>
<td>Yes</td>
<td>Audio/Video/Screen: To and From OK</td>
</tr>
<tr>
<td>Lifesize Icon</td>
<td>Yes</td>
<td>No</td>
<td>Audio/Video/Screen: From device is OK</td>
</tr>
<tr>
<td>Polycom Debut</td>
<td>Yes</td>
<td>Yes</td>
<td>Audio/Video/Screen: To and From OK</td>
</tr>
<tr>
<td>Polycom RealPresence Desktop</td>
<td>No</td>
<td>Yes</td>
<td>Audio/Video: OK, Screen: From device is OK</td>
</tr>
<tr>
<td>Polycom Trio</td>
<td>Yes</td>
<td>Yes</td>
<td>Audio/Video/Screen: To and From OK</td>
</tr>
<tr>
<td>Tandberg C40</td>
<td>Yes</td>
<td>Yes</td>
<td>Audio/Video/Screen: To and From OK</td>
</tr>
</tbody>
</table>
Network configuration and bandwidth requirements

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

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

- Amazon EC2
- Amazon CloudFront
- Amazon Route 53

Common

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

<table>
<thead>
<tr>
<th>Destination</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>chime.aws</td>
<td>TCP/443</td>
</tr>
<tr>
<td>*.chime.aws</td>
<td>TCP/443</td>
</tr>
<tr>
<td>*.amazonaws.com</td>
<td>TCP/443</td>
</tr>
<tr>
<td>99.77.128.0/18</td>
<td>TCP/443</td>
</tr>
</tbody>
</table>

Meetings and Business Calling

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

<table>
<thead>
<tr>
<th>Destination</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>99.77.128.0/18</td>
<td>UDP/3478</td>
</tr>
</tbody>
</table>

H.323 room systems

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

<table>
<thead>
<tr>
<th>Destination</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.248.147.139</td>
<td>TCP/1720</td>
</tr>
</tbody>
</table>
### 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.

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

### Bandwidth requirements

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

- Audio
• 1:1 call: 54 kbps up and down
• Large call: no more than 32 kbps extra down for 50 callers
• Video
  • 1:1 call: 650 kbps up and down
  • HD mode: 1400 kbps up and down
  • 3–4 people: 450 kbps up and (N-1)*400 kbps down
  • 5–16 people: 184 kbps up and (N-1)*134 kbps down
  • Up and down bandwidth adapts lower based on network conditions
• Screen
  • 1.2 mbps up (when presenting) and down (when viewing) for high quality. This adapts as low as 320 kbps based on network conditions.
  • Remote control: 800 kbps fixed
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 (p. 60)
- Integrating chatbots into the Amazon Chime desktop client (p. 61)
- Proxy phone sessions (p. 69)
- Creating webhooks for Amazon Chime (p. 70)

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 (p. 60)
- Downloading user lists (p. 60)
- Log out multiple users (p. 61)
- Update user personal PINs (p. 61)

Invite multiple users

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

```java
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.

```java
BufferedWriter writer = Files.newBufferedWriter(Paths.get("/path/to/csv"));
CSVPrinter printer = new CSVPrinter(writer, CSVFormat.DEFAULT.withHeader("userId", "email"));
ListUsersRequest listUsersRequest = new ListUsersRequest();
```
Log out multiple users

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

```java
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.

```java
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 (p. 8).

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 (p. 62)
- Amazon Chime events sent to chatbots (p. 68)

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 (p. 68).

**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.

   ```json
   "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.

```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 (p. 62). 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**

```bash
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:fulction-name
```
Amazon Chime Administration Guide
Using chatbots with Amazon Chime

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",
    "OutboundEventsHTTPS Endpoint": "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.

```java
PutEventsConfigurationRequest putEventsConfigurationRequest = new
PutEventsConfigurationRequest()
    .withAccountId("chimeAccountId")
    .withBotId("botId")
    .withOutboundEventsHTTPSEndpoint("https://www.example.com")
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 (p. 63).

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.
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**

```json
{
    "Sender": {
        "SenderId": "user@example.com",
        "SenderIdType": "EmailId"
    },
    "Discussion": {
        "DiscussionId": "abcdef12-g34h-56i7-j8kl-mn9opq012st",
        "DiscussionType": "Room"
    },
    "EventType": "Invite",
    "InboundHttpsEndpoint": {
        "EndpointType": "Persistent",
        "Url": "https://hooks.a.chime.aws/incomingwebhooks/a1b2c34d-5678-90e1-f23g-h45i67j8901k?token=ABCDefGHiJKLMn0P2Q3RSTuvwxYZAbC56DeFghIJKLM7N80P9QSnTvV0WXYZAbcdefghi3"
    },
    "EventTimestamp": "2019-04-04T21:27:52.736Z"
}
```
Example: Mention event

```json
{
  "Sender": {
    "SenderId": "user@example.com",
    "SenderIdType": "EmailId"
  },
  "Discussion": {
    "DiscussionId": "abcdef12-g34h-56i7-j8kl-mm9opqr012st",
    "DiscussionType": "Room"
  },
  "EventType": "Mention",
  "InboundHttpsEndpoint": {
    "EndpointType": "ShortLived",
    "Url": "https://hooks.a.chime.aws/incomingwebhooks/a1b2c34d-5678-90e1-f23g-h45i67j8901k?token=ABCDefGHiJK1LMnO92Q5RST4uvwxYZAbC56DeFghI3kLM7N80P9QsTuV0wXYZABcdefgHiJ"
  },
  "EventTimestamp": "2019-04-04T21:30:43.181Z",
  "Message": "@botDisplayName@example.com Hello Chatbot"
}
```

Note
The InboundHttpsEndpoint URL for a Mention event expires 2 minutes after it is sent.

Example: Remove event

```json
{
  "Sender": {
    "SenderId": "user@example.com",
    "SenderIdType": "EmailId"
  },
  "Discussion": {
    "DiscussionId": "abcdef12-g34h-56i7-j8kl-mm9opqr012st",
    "DiscussionType": "Room"
  },
  "EventType": "Remove",
  "EventTimestamp": "2019-04-04T21:26:38.634Z"
}
```

Proxy phone sessions

You can use the AWS Command Line Interface (AWS CLI), Amazon Chime API, or AWS SDK to create proxy phone sessions for use with Amazon Chime Voice Connectors. Proxy phone sessions allow participants to call or send text messages to each other without revealing private phone numbers.

Creating proxy phone sessions requires the following:

- The ability to program.
- An AWS account.
- An AWS Identity and Access Management (IAM) role that grants permission to access the Amazon Chime API actions used to create proxy phone sessions, such as the following:
  - `chime:CreateProxySession`
  - `chime:DeleteProxySession`
The following procedure demonstrates how to create a proxy phone session.

To create a proxy phone session

1. Use the `PutVoiceConnectorProxy` action in the [Amazon Chime API Reference](https://docs.aws.amazon.com/chime/latest/api_reference/) to configure the Amazon Chime Voice Connector for the proxy phone session.
2. Use the `CreateProxySession` action in the [Amazon Chime API Reference](https://docs.aws.amazon.com/chime/latest/api_reference/) to create the proxy phone session.

For more information about the available Amazon Chime API actions for proxy phone sessions, see the [Amazon Chime API Reference](https://docs.aws.amazon.com/chime/latest/api_reference/).

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 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](https://docs.aws.amazon.com/chime/latest/UserGuide/).
2. Use the webhook URL in the script or application that you created to send messages to the chat room:
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

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

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

It’s helpful to provide the following information:

- A detailed description of the issue.
- The time the issue occurred, including your time zone.
- Your Amazon Chime version. To find your version number:
  - In Windows, choose Help, About Amazon Chime.
  - In macOS, choose Amazon Chime, About Amazon Chime.
  - In iOS and Android, choose Settings, About.
- The log reference ID. To find this ID:
  - In Windows and macOS, choose Help, Send Diagnostic Logs.
  - In iOS and Android, choose Settings, Send Diagnostic Logs.
- If your issue is related to a meeting, the meeting ID.
Security in Amazon Chime

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

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

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

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

**Topics**

- Identity and access management for Amazon Chime (p. 73)
- How Amazon Chime works with IAM (p. 78)
- Cross-service confused deputy prevention (p. 79)
- Amazon Chime resource-based policies (p. 80)
- Authorization based on Amazon Chime tags (p. 80)
- Amazon Chime IAM roles (p. 80)
- Amazon Chime identity-based policy examples (p. 81)
- Troubleshooting Amazon Chime identity and access (p. 86)
- Using service-linked roles for Amazon Chime (p. 87)
- Logging and monitoring in Amazon Chime (p. 92)
- Compliance validation for Amazon Chime (p. 106)
- Resilience in Amazon Chime (p. 107)
- Infrastructure security in Amazon Chime (p. 107)
- Understanding Amazon Chime automatic updates (p. 107)

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** (p. 74)
- **Authenticating with identities** (p. 74)
- **Managing access using policies** (p. 76)

### 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** (p. 86).

**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** (p. 78).

**IAM administrator** – If you’re an IAM administrator, you might want to learn details about how you can write policies to manage access to Amazon Chime. To view example Amazon Chime identity-based policies that you can use in IAM, see **Amazon Chime identity-based policy examples** (p. 81).

### 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 How IAM roles differ from resource-based policies in the IAM User Guide.

- **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects
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 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 in the IAM User Guide.

- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see How SCPs work in the AWS Organizations User Guide.

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

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

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

#### Topics
- Amazon Chime identity-based policies (p. 78)
- Resources (p. 79)
- Examples (p. 79)

#### 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


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](https://docs.aws.amazon.com/chime/latest/dv/identity-based-policy-examples.html).

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](https://docs.aws.amazon.com/IAM/latest/UserGuide/id心裡authority-concepts.html) in the [AWS Identity and Access Management User Guide](https://docs.aws.amazon.com/IAM/latest/UserGuide/sso-integrate-account-certificate.html).

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.

```json
{
    "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"
    }
]}
```
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 (p. 87).

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 (p. 81)
- Using the Amazon Chime console (p. 82)
- Allow users full access to Amazon Chime (p. 82)
- Allow users to view their own permissions (p. 83)
- Allow users to access user management actions (p. 84)
- AWS managed policy: AmazonChimeVoiceConnectorServiceLinkedRolePolicy (p. 85)
- Amazon Chime updates to AWS managed policies (p. 85)

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:

```json
{
   "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.

```json
{
   "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": "*"
       }
   ]
}
```
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.

```json
{
    "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": ["logs:CreateLogDelivery",
                        "logs:DeleteLogDelivery",
                        "logs:GetLogDelivery",
                        "logs:ListLogDeliveries",
                        "logs:DescribeResourcePolicies",
                        "logs:PutResourcePolicy",
                        "logs:CreateLogGroup",
                        "logs:DescribeLogGroups"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "ViewSnsTopics",
            "Effect": "Allow",
            "Action": ["sns:CreateTopic",
                        "sns:GetTopicAttributes"
            ],
            "Resource": ["arn:aws:sns::*:*:ChimeVoiceConnector-Streaming*"
            ]
        },
        {
            "Sid": "ViewSqsQueues",
            "Effect": "Allow",
            "Action": ["sqs:GetQueueAttributes",
                        "sqs:CreateQueue"
            ],
            "Resource": ["arn:aws:sqs::*:*:ChimeVoiceConnector-Streaming*"
            ]
        }
    ]
}
```
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.

```json
{
    "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:ListPhoneNumberNumbers",
                "chime:GetUserSettings",
                "chime:UpdateUserSettings",
                "chime:CreateUser",
                "chime: AssociateSigninDelegateGroupsWithAccount",
                "chime: DisassociateSigninDelegateGroupsFromAccount"
            ],
            "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.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>AmazonChimeVoiceConnectorServiceLinkedRolePolicy – Update to an existing policy</td>
<td>Amazon Chime Voice Connectors added new permissions to allow you to use Amazon Polly to synthesize speech. These permissions are required to use the Speak and SpeakAndGetDigits actions in Amazon Chime SDK Voice Applications.</td>
<td>March 15, 2022</td>
</tr>
<tr>
<td>AmazonChimeVoiceConnectorServiceLinkedRolePolicy – Update to an existing policy</td>
<td>Amazon Chime Voice Connectors 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.</td>
<td>December 20, 2021</td>
</tr>
<tr>
<td>Change to existing policy, Creating IAM users or roles with the Chime SDK policy.</td>
<td>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.</td>
<td>September 23, 2021</td>
</tr>
</tbody>
</table>
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 (p. 86)
- I am not authorized to perform iam:PassRole (p. 86)
- I want to allow people outside of my AWS account to access my Amazon Chime resources (p. 87)

**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.

```plaintext
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.

```plaintext
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 (p. 78).
- To learn how to provide access to your resources across AWS accounts that you own, see Providing access to an IAM user in another AWS account that you own in the IAM User Guide.
- To learn how to provide access to your resources to third-party AWS accounts, see Providing access to AWS accounts owned by third parties in the IAM User Guide.
- To learn how to provide access through identity federation, see Providing access to externally authenticated users (identity federation) in the IAM User Guide.
- To learn the difference between using roles and resource-based policies for cross-account access, see How IAM roles differ from resource-based policies in the IAM User Guide.

Using service-linked roles for Amazon Chime

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

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 (p. 87)
- Using roles with live transcription (p. 89)
- Using roles with Amazon Chime SDK media pipelines (p. 91)

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.
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 (p. 89)
- Creating a Service-Linked Role for Amazon Chime Live Transcription (p. 90)
- Editing a Service-Linked Role for Amazon Chime Live Transcription (p. 90)
- Deleting a Service-Linked Role for Amazon Chime Live Transcription (p. 90)
- Supported Regions for Amazon Chime Service-Linked Roles (p. 91)

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 (p. 91)
• Creating a service-linked role for Amazon Chime SDK media pipelines (p. 91)
• Editing a service-linked role for Amazon Chime SDK media pipelines (p. 90)
• Deleting a service-linked role for Amazon Chime SDK media pipelines (p. 90)
• Supported Regions for Amazon Chime SDK media pipelines service-linked roles (p. 92)

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](https://docs.aws.amazon.com/AmazonCloudWatch/latest/UserGuide/Introduction.html).

• **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](https://docs.aws.amazon.com/eventbridge/latest/userguide/).

• **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](https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/).

• **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](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch_CloudTrail.html).

### Topics

- Monitoring Amazon Chime with Amazon CloudWatch (p. 93)
- Automating Amazon Chime with EventBridge (p. 101)
- Logging Amazon Chime API calls with AWS CloudTrail (p. 104)

## 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](https://docs.aws.amazon.com/AmazonCloudWatch/latest/UserGuide/Introduction.html).

### 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.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>InboundCallAttempts</td>
<td>The number of inbound calls attempted.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>InboundCallFailures</td>
<td>The number of inbound call failures.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>InboundCallsAnswered</td>
<td>The number of inbound calls that are answered.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>InboundCallsActive</td>
<td>The number of inbound calls that are currently active.</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OutboundCallAttempts</td>
<td>The number of outbound calls attempted.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>OutboundCallFailures</td>
<td>The number of outbound call failures.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>OutboundCallsAnswered</td>
<td>The number of outbound calls that are answered.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>OutboundCallsActive</td>
<td>The number of outbound calls that are currently active.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>Throttles</td>
<td>The number of times your account is throttled when attempting to make a call.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>Sip1xxCodes</td>
<td>The number of SIP messages with 1xx-level status codes.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>Sip2xxCodes</td>
<td>The number of SIP messages with 2xx-level status codes.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>Sip3xxCodes</td>
<td>The number of SIP messages with 3xx-level status codes.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>Sip4xxCodes</td>
<td>The number of SIP messages with 4xx-level status codes.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>Sip5xxCodes</td>
<td>The number of SIP messages with 5xx-level status codes.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>Sip6xxCodes</td>
<td>The number of SIP messages with 6xx-level status codes.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>CustomerToVcRtpPackets</td>
<td>The number of RTP packets sent from the customer to the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CustomerToVcRtpBytes</td>
<td>The number of bytes sent from the customer to the Amazon Chime Voice Connector infrastructure in RTP packets.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>CustomerToVcRtcpPackets</td>
<td>The number of RTCP packets sent from the customer to the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>CustomerToVcRtcpBytes</td>
<td>The number of bytes sent from the customer to the Amazon Chime Voice Connector infrastructure in RTCP packets.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>CustomerToVcPacketsLost</td>
<td>The number of packets lost in transit from the customer to the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>CustomerToVcJitter</td>
<td>The average jitter for packets sent from the customer to the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td></td>
<td>Units: Microseconds</td>
</tr>
<tr>
<td>VcToCustomerRtpPackets</td>
<td>The number of RTP packets sent from the Amazon Chime Voice Connector infrastructure to the customer.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>VcToCustomerRtpBytes</td>
<td>The number of bytes sent from the Amazon Chime Voice Connector infrastructure to the customer in RTP packets.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>VcToCustomerRtcpPackets</td>
<td>The number of RTCP packets sent from the Amazon Chime Voice Connector infrastructure to the customer.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>VcToCustomerRtcpBytes</td>
<td>The number of bytes sent from the Amazon Chime Voice Connector infrastructure to the customer in RTCP packets.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VcToCustomerPacketsLost</td>
<td>The number of packets lost in transit from the Amazon Chime Voice Connector infrastructure to the customer.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>VcToCustomerJitter</td>
<td>The average jitter for packets sent from the Amazon Chime Voice Connector infrastructure to the customer.</td>
</tr>
<tr>
<td></td>
<td>Units: Microseconds</td>
</tr>
<tr>
<td>RTTBetweenVcAndCustomer</td>
<td>The average round-trip time between the customer and the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td></td>
<td>Units: Microseconds</td>
</tr>
<tr>
<td>MOSBetweenVcAndCustomer</td>
<td>The estimated Mean opinion score (MOS) associated with voice streams between the customer and the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td></td>
<td>Units: Score between 1.0-4.4. A higher score indicates better perceived audio quality.</td>
</tr>
<tr>
<td>RemoteToVcRtpPackets</td>
<td>The number of RTP packets sent from the remote end to the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>RemoteToVcRtpBytes</td>
<td>The number of bytes sent from the remote end to the Amazon Chime Voice Connector infrastructure in RTP packets.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>RemoteToVcRtcpPackets</td>
<td>The number of RTCP packets sent from the remote end to the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>RemoteToVcRtcpBytes</td>
<td>The number of bytes sent from the remote end to the Amazon Chime Voice Connector infrastructure in RTCP packets.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>RemoteToVcPacketsLost</td>
<td>The number of packets lost in transit from the remote end to the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RemoteToVcJitter</td>
<td>The average jitter for packets sent from the remote end to the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td>VcToRemoteRtpPackets</td>
<td>The number of RTP packets sent from the Amazon Chime Voice Connector infrastructure to the remote end.</td>
</tr>
<tr>
<td>VcToRemoteRtpBytes</td>
<td>The number of bytes sent from the Amazon Chime Voice Connector infrastructure to the remote end in RTP packets.</td>
</tr>
<tr>
<td>VcToRemoteRtcpPackets</td>
<td>The number of RTCP packets sent from the Amazon Chime Voice Connector infrastructure to the remote end.</td>
</tr>
<tr>
<td>VcToRemoteRtcpBytes</td>
<td>The number of bytes sent from the Amazon Chime Voice Connector infrastructure to the remote end in RTCP packets.</td>
</tr>
<tr>
<td>VcToRemotePacketsLost</td>
<td>The number of packets lost in transit from the Amazon Chime Voice Connector infrastructure to the remote end.</td>
</tr>
<tr>
<td>VcToRemoteJitter</td>
<td>The average jitter for packets sent from the Amazon Chime Voice Connector infrastructure to the remote end.</td>
</tr>
<tr>
<td>RTTBetweenVcAndRemote</td>
<td>The average round-trip time between the remote end and the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td>MOSBetweenVcAndRemote</td>
<td>The estimated Mean opinion score (MOS) associated with voice streams between the remote end and the Amazon Chime Voice Connector infrastructure.</td>
</tr>
</tbody>
</table>
CloudWatch dimensions for Amazon Chime

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

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoiceConnectorId</td>
<td>The identifier of the Amazon Chime Voice Connector to display metrics for.</td>
</tr>
<tr>
<td>Region</td>
<td>The AWS Region associated with the event.</td>
</tr>
</tbody>
</table>

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](https://docs.aws.amazon.com/chime/latest_sdk行政/AmazonChimeSDK行政Guide.html) in the [Amazon Chime SDK Administration Guide](https://docs.aws.amazon.com/chime/latest_sdk行政/AmazonChimeSDK行政Guide.html).

**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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice_connector_id</td>
<td>The Amazon Chime Voice Connector ID carrying the call.</td>
</tr>
<tr>
<td>event_timestamp</td>
<td>The time when the metrics are emitted, in number of milliseconds since the UNIX epoch (midnight on January 1, 1970) in UTC.</td>
</tr>
<tr>
<td>call_id</td>
<td>Corresponds to the Transaction ID.</td>
</tr>
<tr>
<td>from_sip_user</td>
<td>The initiating user for the call.</td>
</tr>
<tr>
<td>from_country</td>
<td>The initiating country for the call.</td>
</tr>
<tr>
<td>to_sip_user</td>
<td>The receiving user for the call.</td>
</tr>
<tr>
<td>to_country</td>
<td>The receiving country for the call.</td>
</tr>
<tr>
<td>endpoint_id</td>
<td>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.</td>
</tr>
<tr>
<td>aws_region</td>
<td>The AWS Region for the call.</td>
</tr>
<tr>
<td>cust2vc_rtp_packets</td>
<td>The number of RTP packets sent from the customer to the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td>cust2vc_rtp_bytes</td>
<td>The number of bytes sent from the customer to the Amazon Chime Voice Connector infrastructure in RTP packets.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>cust2vc_rtcp_packets</td>
<td>The number of RTCP packets sent from the customer to the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td>cust2vc_rtcp_bytes</td>
<td>The number of bytes sent from the customer to the Amazon Chime Voice Connector infrastructure in RTCP packets.</td>
</tr>
<tr>
<td>cust2vc_packets_lost</td>
<td>The number of packets lost in transit from the customer to the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td>cust2vc_jitter</td>
<td>The average jitter for packets sent from the customer to the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td>vc2cust_rtp_packets</td>
<td>The number of RTP packets sent from the Amazon Chime Voice Connector infrastructure to the customer.</td>
</tr>
<tr>
<td>vc2cust_rtp_bytes</td>
<td>The number of bytes sent from the Amazon Chime Voice Connector infrastructure to the customer in RTP packets.</td>
</tr>
<tr>
<td>vc2cust_rtcp_packets</td>
<td>The number of RTCP packets sent from the Amazon Chime Voice Connector infrastructure to the customer.</td>
</tr>
<tr>
<td>vc2cust_rtcp_bytes</td>
<td>The number of bytes sent from the Amazon Chime Voice Connector infrastructure to the customer in RTCP packets.</td>
</tr>
<tr>
<td>vc2cust_packets_lost</td>
<td>The number of packets lost in transit from the Amazon Chime Voice Connector infrastructure to the customer.</td>
</tr>
<tr>
<td>vc2cust_jitter</td>
<td>The average jitter for packets sent from the Amazon Chime Voice Connector infrastructure to the customer.</td>
</tr>
<tr>
<td>rtt_btwn_vc_and_cust</td>
<td>The average round-trip time between the customer and the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td>mos_btwn_vc_and_cust</td>
<td>The estimated Mean opinion score (MOS) associated with voice streams between the customer and the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td>rem2vc_rtp_packets</td>
<td>The number of RTP packets sent from the remote end to the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td>rem2vc_rtp_bytes</td>
<td>The number of bytes sent from the remote end to the Amazon Chime Voice Connector infrastructure in RTP packets.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rem2vc_rtcp_packets</td>
<td>The number of RTCP packets sent from the remote end to the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td>rem2vc_rtcp_bytes</td>
<td>The number of bytes sent from the remote end to the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td>rem2vc_packets_lost</td>
<td>The number of packets lost in transit from the remote end to the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td>rem2vc_jitter</td>
<td>The average jitter for packets sent from the remote end to the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td>vc2rem_rtp_packets</td>
<td>The number of RTP packets sent from the Amazon Chime Voice Connector infrastructure to the remote end.</td>
</tr>
<tr>
<td>vc2rem_rtp_bytes</td>
<td>The number of bytes sent from the Amazon Chime Voice Connector infrastructure to the remote end.</td>
</tr>
<tr>
<td>vc2rem_rtcp_packets</td>
<td>The number of RTCP packets sent from the Amazon Chime Voice Connector infrastructure to the remote end.</td>
</tr>
<tr>
<td>vc2rem_rtcp_bytes</td>
<td>The number of bytes sent from the Amazon Chime Voice Connector infrastructure to the remote end.</td>
</tr>
<tr>
<td>vc2rem_packets_lost</td>
<td>The number of packets lost in transit from the Amazon Chime Voice Connector infrastructure to the remote end.</td>
</tr>
<tr>
<td>vc2rem_jitter</td>
<td>The average jitter for packets sent from the Amazon Chime Voice Connector infrastructure to the remote end.</td>
</tr>
<tr>
<td>rtt_btwn_vc_and_rem</td>
<td>The average round-trip time between the remote end and the Amazon Chime Voice Connector infrastructure.</td>
</tr>
<tr>
<td>mos_btwn_vc_and_rem</td>
<td>The estimated Mean opinion score (MOS) associated with voice streams between the remote end and the Amazon Chime Voice Connector infrastructure.</td>
</tr>
</tbody>
</table>

### 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.
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": "12345678-1234-1234-11112222333",
  "detail-type": "Chime VoiceConnector Streaming Status",
  "source": "aws.chime",
  "account": "11112222333",
  "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@abcdeghij2klmno3pqr4.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\"?><\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-abcdef1ghij2klmno3pqr4-111aa-22bb-33cc-44dd-11122222333",
    "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": "12345678-1234-1234-11112222333",
  "detail-type": "Chime VoiceConnector Streaming Status",
  "source": "aws.chime",
  "account": "11112222333",
  "time": "yyyy-mm-ddThh:mm:ssZ",
  "region": "us-east-1",
```
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.

```json
{
  "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"
    },
    "isCaller": false,
    "mediaType": "audio/L16",
    "sdp": {"mediaIndex": 0,
      "medialabel": "1"
    },
    "siprecMetadata": 
      "<xml version="1.0" encoding="UTF-8"/>
      <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-111122223333",
      "toNumber": "+13605550199",
      "version": "0"
    }
  }
}
```
Amazon Chime Administration Guide

Logging service API calls

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:

```json
{"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",
```
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.
- **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.
• **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](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.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Chime SDK Administration Guide published (p. 109)</td>
<td>The Amazon Chime SDK topics are now published in the <em>Amazon Chime SDK Administration Guide</em>. For more information, see the Amazon Chime SDK Administration Guide.</td>
<td>March 24, 2022</td>
</tr>
<tr>
<td>IAM policy updates (p. 109)</td>
<td>Changes to IAM policies managed by AWS are now tracked in this administrator's guide. See Amazon Chime identity-based policy examples.</td>
<td>September 23, 2021</td>
</tr>
<tr>
<td>Service-linked roles (p. 109)</td>
<td>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.</td>
<td>August 12, 2021</td>
</tr>
<tr>
<td>SIP media applications and rule (p. 109)</td>
<td>Administrators can create SIP media applications and rules for use with Amazon Chime Voice Connector and AWS Lambda functions. For more information, see Managing SIP applications and rules in the Amazon Chime Administrator Guide.</td>
<td>November 18, 2020</td>
</tr>
<tr>
<td>Amazon Chime Voice Connector emergency call routing numbers (p. 109)</td>
<td>Amazon Chime administrators can set up emergency call routing numbers for an Amazon Chime Voice Connector. For more information, see Setting up emergency call routing numbers for your Amazon Chime Voice Connector in the Amazon Chime Administrator Guide.</td>
<td>July 1, 2020</td>
</tr>
<tr>
<td>Amazon Chime on Dolby Voice Huddle (p. 109)</td>
<td>Amazon Chime offers a native or first-party meeting experience on Dolby Voice Huddle audio and video conferencing.</td>
<td>June 3, 2020</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Setting chat retention policies (p. 109)</td>
<td>Amazon Chime administrators can set chat retention policies for their Enterprise accounts. For more information, see <a href="#">Managing chat retention policies</a> in the Amazon Chime Administrator Guide.</td>
<td>May 21, 2020</td>
</tr>
<tr>
<td>Removing chat messages (p. 109)</td>
<td>If you have the ability to program, you can use the Amazon Chime API to remove messages from chat rooms and conversations in your account. For more information, see <a href="#">Managing messages</a> in the Amazon Chime Administrator Guide.</td>
<td>May 18, 2020</td>
</tr>
<tr>
<td>CloudWatch media quality metrics for Amazon Chime Voice Connector (p. 109)</td>
<td>Amazon Chime supports sending media quality metrics for your Amazon Chime Voice Connector to CloudWatch. For more information, see <a href="#">Monitoring Amazon Chime with CloudWatch</a> in the Amazon Chime Administrator Guide.</td>
<td>January 23, 2020</td>
</tr>
<tr>
<td>Amazon Chime Meetings App for Slack (p. 109)</td>
<td>Amazon Chime supports the Amazon Chime Meetings App for Slack. For more information, see <a href="#">Setting up the Amazon Chime Meetings App for Slack</a> in the Amazon Chime Administrator Guide.</td>
<td>December 4, 2019</td>
</tr>
<tr>
<td>Meeting Region settings (p. 109)</td>
<td>Amazon Chime supports processing meetings in the optimal AWS Region for all participants. For more information, see <a href="#">Meeting Region settings</a> in the Amazon Chime Administrator Guide.</td>
<td>December 3, 2019</td>
</tr>
<tr>
<td>SIP-based media recording (SIPREC) compatibility (p. 109)</td>
<td>Amazon Chime Voice Connectors support streaming media from a SIPREC-compatible voice infrastructure to Kinesis Video Streams. For more information, see <a href="#">SIP-based media recording (SIPREC) compatibility</a> in the Amazon Chime Administrator Guide.</td>
<td>November 25, 2019</td>
</tr>
<tr>
<td><strong>Amazon Chime on Dolby Voice Room (p. 109)</strong></td>
<td>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 <a href="#">Setting up Amazon Chime on Dolby Voice Room</a> in the Amazon Chime Administrator Guide.</td>
<td>October 29, 2019</td>
</tr>
<tr>
<td><strong>Updating outbound calling names (p. 109)</strong></td>
<td>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 <a href="#">Updating outbound calling names</a> in the Amazon Chime Administrator Guide.</td>
<td>October 24, 2019</td>
</tr>
<tr>
<td><strong>Streaming media to Amazon Kinesis (p. 109)</strong></td>
<td>Stream phone call audio from Amazon Chime Voice Connectors to Kinesis Video Streams for analytics, machine learning, and other processing. For more information, see <a href="#">Streaming Amazon Chime Voice Connector media to Kinesis</a> and <a href="#">Using the Amazon Chime Voice Connector service-linked role</a> in the Amazon Chime Administrator Guide.</td>
<td>October 24, 2019</td>
</tr>
<tr>
<td><strong>Monitoring Amazon Chime with Amazon CloudWatch (p. 109)</strong></td>
<td>Monitor Amazon Chime using CloudWatch, which collects raw data and processes it into readable, near real-time metrics. For more information, see <a href="#">Monitoring Amazon Chime with CloudWatch</a> in the Amazon Chime Administrator Guide.</td>
<td>October 24, 2019</td>
</tr>
<tr>
<td><strong>Amazon Chime Voice Connector groups (p. 109)</strong></td>
<td>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 <a href="#">Working with Amazon Chime Voice Connector groups</a> in the Amazon Chime Administrator Guide.</td>
<td>October 24, 2019</td>
</tr>
<tr>
<td>Topic</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td><strong>Network configuration updates (p. 109)</strong></td>
<td>Amazon Chime is simplifying its firewall requirements. For more information, see <a href="#">Network configuration and bandwidth requirements</a> in the Amazon Chime Administrator Guide.</td>
<td>September 6, 2019</td>
</tr>
<tr>
<td><strong>Moderated meetings (p. 109)</strong></td>
<td>Amazon Chime supports moderated meetings. For more information, see <a href="#">Joining a moderated meeting</a> in the Amazon Chime Administrator Guide.</td>
<td>July 25, 2019</td>
</tr>
<tr>
<td><strong>Compliance validation for Amazon Chime (p. 109)</strong></td>
<td>Amazon Chime is a HIPAA Eligible Service. For more information, see <a href="#">Compliance validation for Amazon Chime</a> in the Amazon Chime Administrator Guide.</td>
<td>June 11, 2019</td>
</tr>
<tr>
<td><strong>Porting toll-free phone numbers (p. 109)</strong></td>
<td>Amazon Chime supports porting toll-free United States phone numbers for use with Amazon Chime Voice Connectors. For more information, see <a href="#">Porting existing phone numbers</a> in the Amazon Chime Administrator Guide.</td>
<td>May 28, 2019</td>
</tr>
<tr>
<td><strong>Managing phone numbers in Amazon Chime (p. 109)</strong></td>
<td>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 <a href="#">Managing phone numbers in Amazon Chime</a> in the Amazon Chime Administrator Guide.</td>
<td>March 18, 2019</td>
</tr>
<tr>
<td><strong>Amazon Chime Add-In for Outlook (p. 109)</strong></td>
<td>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 <a href="#">Deploying the Add-In for Outlook</a> in the Amazon Chime Administrator Guide.</td>
<td>March 12, 2019</td>
</tr>
<tr>
<td><strong>Various updates (p. 109)</strong></td>
<td>Various updates to topic layout and organization.</td>
<td>February 11, 2019</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>Amazon Chime call me feature (p. 109)</strong></td>
<td>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.</td>
<td>August 22, 2018</td>
</tr>
<tr>
<td><strong>Connect to Okta SSO (p. 109)</strong></td>
<td>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.</td>
<td>August 1, 2018</td>
</tr>
<tr>
<td><strong>Request user attachments (p. 109)</strong></td>
<td>Receive attachments uploaded into Amazon Chime by users. For more information, see Request user attachments in the Amazon Chime Administrator Guide.</td>
<td>April 23, 2018</td>
</tr>
<tr>
<td><strong>View additional report data (p. 109)</strong></td>
<td>View additional report data. For more information, see View reports in the Amazon Chime Administrator Guide.</td>
<td>March 30, 2018</td>
</tr>
<tr>
<td><strong>Assign users Pro or Basic permissions (p. 109)</strong></td>
<td>Assign users Pro or Basic permissions. For more information, see Manage user access and permissions in the Amazon Chime Administrator Guide.</td>
<td>March 29, 2018</td>
</tr>
</tbody>
</table>
For the latest AWS terminology, see the AWS glossary in the AWS Glossary Reference.