Amazon Chime

Administration Guide

Amazon Chime: Administration Guide

Copyright © 2019 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

What Is Amazon Chime?

Amazon Chime is a communications service that transforms online meetings with a secure, easy-to-use application that you can trust. Amazon Chime works seamlessly 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, both inside and outside your organization. Amazon Chime frees you to work productively from anywhere.

For more information, see the Amazon Chime site.

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

With Amazon Chime, you choose Basic or Pro permissions for your Amazon Chime users. A user's 30-day trial ends when you add them to your Amazon Chime account. For more information, see Plans and pricing.

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.

With Amazon Chime usage-based pricing, you only pay for users that host meetings on the days when meetings are held. Meeting attendees and chat users are not charged. Users with a Pro license are considered Active Pro if they host a meeting that ends on a calendar day and at least one of the following occurs:

- 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.

To begin managing your users and access administrative features, complete the following tasks:

Tasks

Step 1: Create an AWS Account

If you have an AWS account already, skip to the next task. If you don't have an AWS account, use the following procedure to create one.

To create an AWS account

1. Open https://aws.amazon.com/, and then choose **Create an AWS Account**.

   Note
   If you previously signed in to the AWS Management Console using AWS account root user credentials, choose **Sign in to a different account**. If you previously signed in to the console using IAM credentials, choose **Sign-in using root account credentials**. Then choose **Create a new AWS account**.
2. Follow the online instructions.

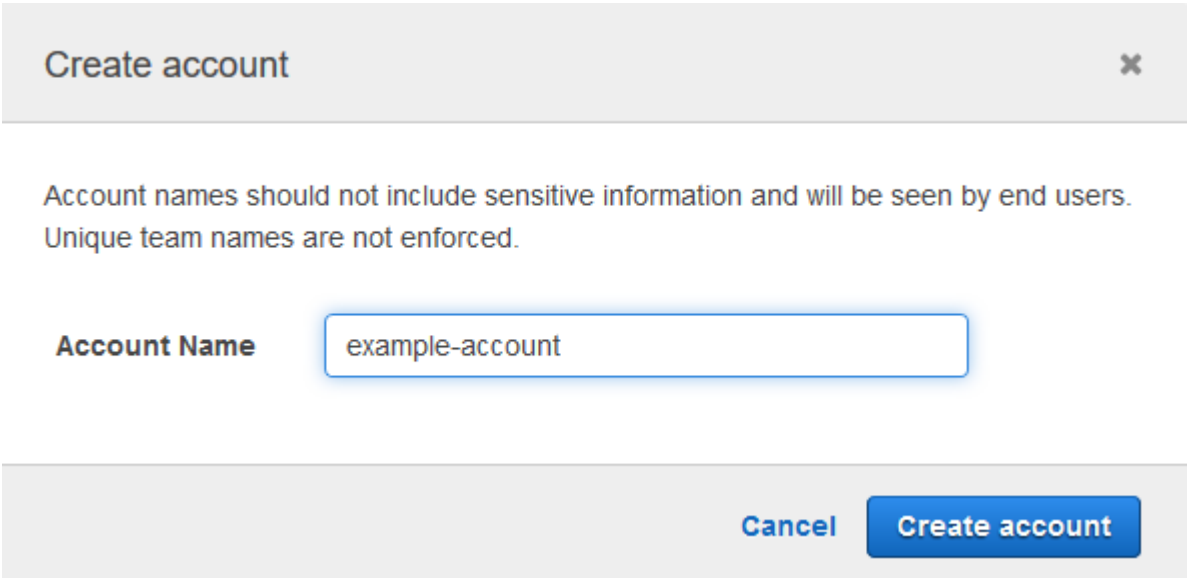
   Part of the sign-up procedure involves receiving a phone call and entering a verification code using the phone keypad.

Step 2: Create an Amazon Chime Account

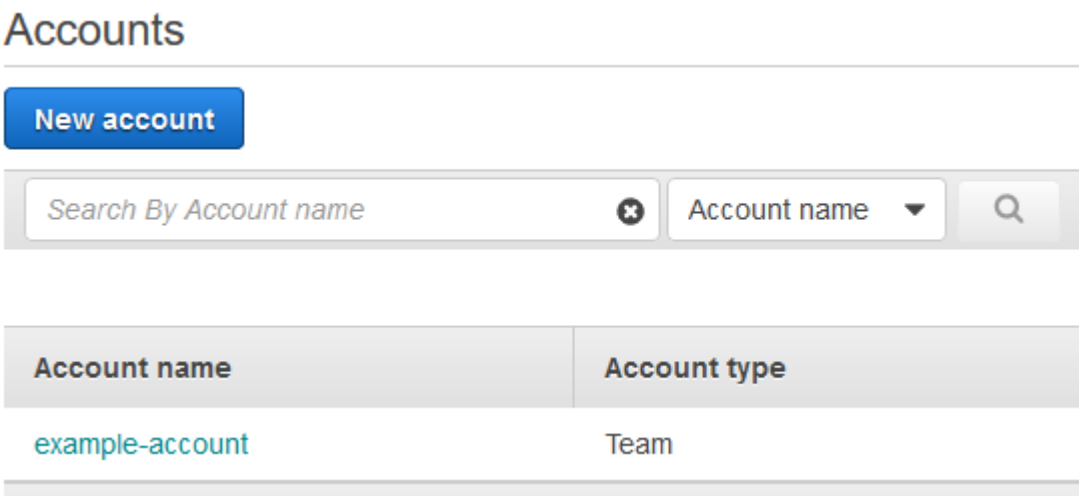
After you've created your AWS account, you can create an Amazon Chime account.

To create an Amazon Chime account

1. Open the Amazon Chime console at https://console.chime.aws.amazon.com/.
2. On the **Accounts** page, choose **New account**.
3. For **Account Name**, type a name for the account and choose **Create account**.



4. The new account has the account type **Team**.



Step 3: Add Users to Your Amazon Chime Account

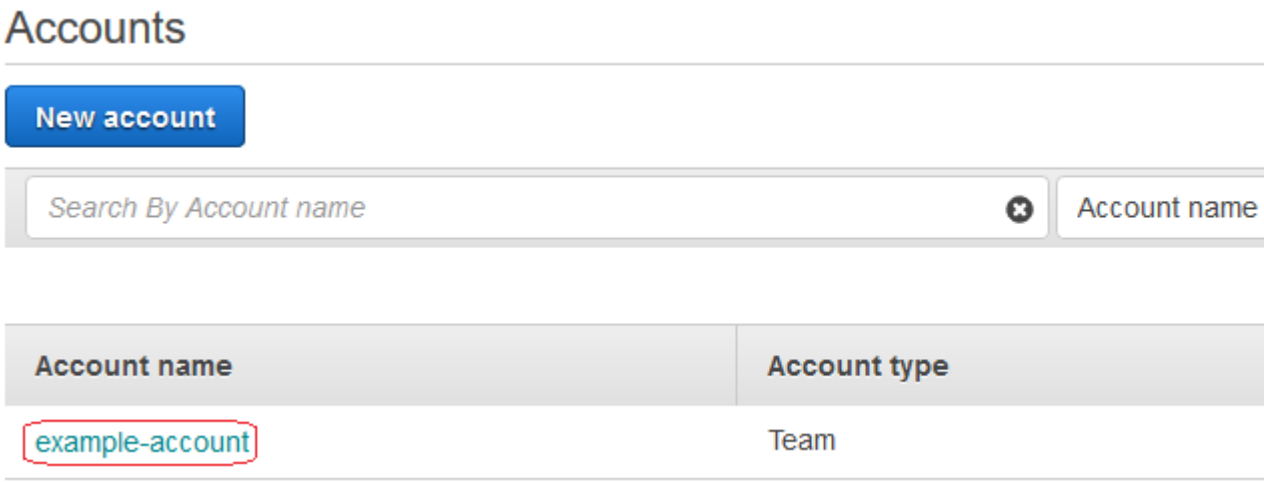
After you create an Amazon Chime account, you can add yourself and other users to the account. You are not charged for invited users. You incur charges after a user accepts an invitation and registers.

Note
When you add a user to your Amazon Chime account, their 30-day trial ends. By default, users have Pro permissions and can host scheduled meetings. To restrict the ability to host meetings, change the user's permission to Basic.
If you plan to upgrade your account to an enterprise account, there is no need to invite users through the administration console. Instead, claim your domains. Any users that register with

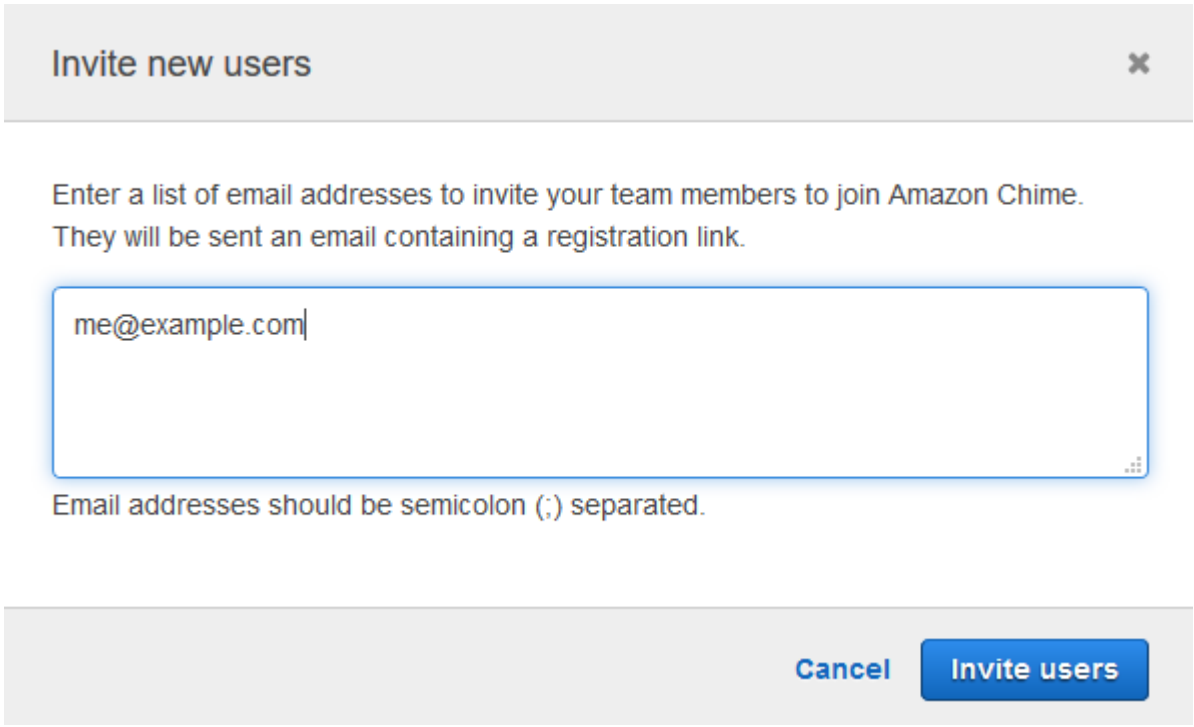
your claimed domain become part of your account. For more information about claiming your first domain and becoming an enterprise account, see Claim a Domain (p. 8).

To add users to your Amazon Chime account

1. Open the Amazon Chime console at https://console.chime.aws.amazon.com/.
2. On the **Accounts** page, select the name of your account.



3. On the **Users** page, enter user email addresses and choose **Invite users**.



4. The user receives an email invitation to join the Amazon Chime team that you created.
5. After a user chooses **Accept** in the email invitation, they are assigned Amazon Chime Pro permissions by default.
   - If the user has already signed up for an Amazon Chime account with their work email address, they are granted the assigned permissions and can continue to use that account.

- If the user hasn't downloaded the Amazon Chime client app (this can be done at any time), they can choose **Download Amazon Chime** to download it and sign in if they have an account. If they don't have an account, they can register to create one. For more information, see Step 2: Create an Amazon Chime Account (p. 2).

6. Repeat steps 1–5 for all users to invite, including yourself.

Managing Your Amazon Chime Accounts

If you are using Amazon Chime as an individual user or as a group with no administrators, and you want to expand your pilot or proof of concept to include administrator functionality or you want to buy Pro, you must create an Amazon Chime account in the AWS Management Console. You can decide whether to create a **team account** or **enterprise account**.

A **team account** is the easiest way to start inviting users to your organization and grant them Pro permissions. You only pay for users when they host meetings. You don't have to claim a domain, and you can invite users from any email domain that hasn't been claimed by another company. Everyone in the same team account is able to search and locate other registered Amazon Chime users in the team. A team account is also the right choice for paying for Pro users outside of your organization.

An **enterprise account** provides more control over your users from your company domains. It includes the ability to connect to your own identity provider or Okta SSO to authenticate and assign user permissions. If you're using your own identity provider, note that Amazon Chime supports Microsoft Active Directory.

Enterprise accounts provide full management of users within your account. This ensures that all users joining Amazon Chime through your claimed domains are included in your centrally managed Amazon Chime account. Enterprise accounts require claiming at least one email domain. Enterprise administrators can suspend and activate users, and use the full administrative capabilities of Amazon Chime, such as preventing specific users from signing in. Enterprise accounts simplify the process of adding users and are required for managing your users through a supported directory integration.

> **Note**
> You can convert your team account to enterprise by claiming one or more email domains. After your account is converted, the ability to connect an Active Directory instance through AWS Directory Service becomes available. You can decide whether to continue to have your users sign in with Login with Amazon, or connect and authenticate via their Active Directory credentials. If you don't connect to an Active Directory, your users sign in with Login with Amazon (or an Amazon.com account). When Active Directory is set up, your users authenticate with their Active Directory credentials.

Contents

Create an Amazon Chime Account

If you haven't created an account, you can create one from the **Accounts** page. For more information, see Step 2: Create an Amazon Chime Account (p. 2).

To immediately upgrade to an enterprise account, after completing Step 2: Create an Amazon Chime Account (p. 2), skip to Claim a Domain (p. 8) to claim at least one domain. For more information about team and enterprise accounts, see Managing Your Amazon Chime Accounts (p. 6).

After you create your account, use the following procedure to see it on the **Accounts** page in the Amazon Chime console. This page provides basic information on the account, including the name and account type. You can also rename or delete your account on this page.

To go to the Accounts page

1. Open the Amazon Chime console at https://console.chime.aws.amazon.com/.
2. Select the account in the **Account name** column. Under **Settings**, choose **Account**.

   Note
   You can search for accounts by account name, or search for specific users across all of your accounts using their email address. In the account detail page, you can manage users and settings.

Rename 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 team account.

To rename your account

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

Delete Your Account

If you delete your AWS account in the AWS 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 Use the Amazon Chime Assistant.

To delete a team account

1. Open the Amazon Chime console at https://console.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://console.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.

Use the Policies Page

The **Policies** page allows you to choose whether users in your organization are able to grant shared control of their computer while in meetings. Attendees who request shared control of your user's computer receive an error message indicating that remote control isn't available.

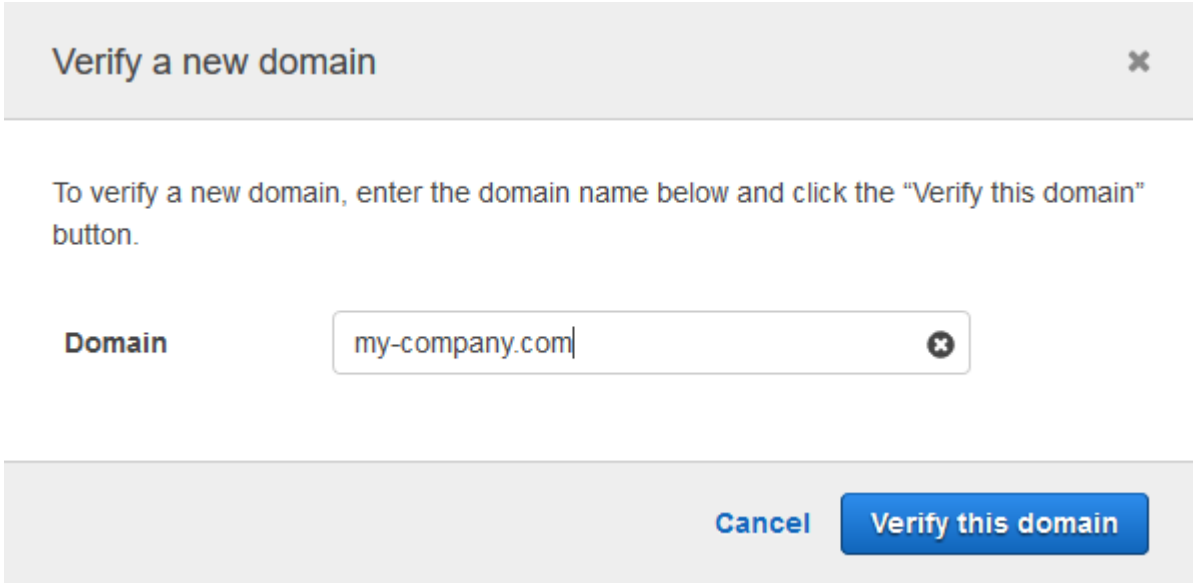
You can also enable the Amazon Chime call me feature on the **Policies** page. This feature provides meeting attendees the option to join meetings by receiving a phone call from Amazon Chime.

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



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

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

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

Connect to Your Active Directory

Benefits

Using your Active Directory has the following benefits:

- Amazon Chime users can sign in with their Active Directory credentials.
- Administrators can choose which credential security features to add, including password rotation, password complexity rules, and multi-factor authorization.
- When users accounts are disabled in your Active Directory, their Amazon Chime accounts are automatically disabled.
- You can specify which Active Directory groups receive Pro permissions.

- Multiple groups can be configured to receive Basic or Pro permissions.
- Users must be a member of either group to sign into Amazon Chime.
- Users in both groups receive a Pro license.

Requirements

Before you can add your Active Directory to Amazon Chime, you must complete the following requirements:

- Make sure that you have appropriate IAM permissions to configure Domains, Active Directory, and Directory Groups.
- Set up 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 or Microsoft AD.
- Set up an Amazon Chime enterprise account. For more information, see Claim a Domain (p. 8).

After you add a directory to Amazon Chime, users are prompted to log in with their directory credentials when they log in using an email address from one of the domains that you added to your Amazon Chime enterprise account.

To connect to your Active Directory

1. Open the Amazon Chime console at https://console.chime.aws.amazon.com/.
2. In the navigation pane, choose **Settings**, **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 has been connected, choose **Add a new group**. For **Group**, type a name for the group. For **Permission tier**, choose **Basic** or **Pro**.
5. Choose **Add Group**.
6. Repeat this procedure to create additional directory groups.

Configure Multiple Email Addresses

After you connect to your Active Directory, users that authenticate with Active Directory can use multiple email addresses. They can use any of their work email addresses with Amazon Chime, as long as the email address is using a domain that has been claimed by your Amazon Chime account, and is associated with their user in Active Directory.

Amazon Chime continues to use the single email address in the EmailAddress attribute in Active Directory as the user's primary email address. This is the only one you can see in the interface. Users can use any additional addresses in the ProxyAddress attribute, as long as the domain is claimed for the account.

Incorrect Configuration Example

Username shirley.rodriguez is a member of an Amazon Chime account that has claimed two domains: example.com and anotherdomain.com. In Active Directory, she has the following three email addresses (one primary and two proxy):

- Primary email address: shirley.rodriguez@example.com

- Proxy email address 1: shirley.rodriguez@example2.com
- Proxy email address 2: srodriguez@anotherdomain.com

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

Other Amazon Chime users can add her as a contact, invite her to meetings, or add her as a delegate using either her shirley.rodriguez@example.com or srodriguez@anotherdomain.com email address.

Correct Configuration Example

Username shirley.rodriguez is a member of an Amazon Chime account that has claimed three domains: example.com, example2.com, and anotherdomain.com. In Active Directory, she 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@anotherdomain.com

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

Connect 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 the section called “Create an Amazon Chime Account” (p. 6).

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. Type the following for the **Login Redirect URI**: **`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)**, select all the related options, and choose **Save**.
        e. 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.

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

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

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

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

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

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

4. Configure directory groups in Amazon Chime:

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

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

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

Manage Users

The **Users** page lists all of the users in your account. You can search for a specific user by searching for their email address, view basic user data, and browse to view more information.

Administrators of accounts using **Login with Amazon** (LWA) also see options to manage permission tiers and remove users from the account. These actions are managed through Active Directory for accounts where Active Directory is configured and Okta for accounts where Okta is configured.

Contents

View User Details

You can use the **User details** page to see detailed information about an individual user, or update a specific user account. The following user information is available on the page.

> **Note**
> If a user hasn't accepted the invitation to a team account, not all information appears on this page.

Field	Description	Example
Display name	The user's name that appears in Amazon Chime. For LWA users, this is the full name. For Active Directory users, the DISPLAY_NAME_ATTRIBUTE is used.	Major, Mary
Email address	For LWA users, the email address used for registration. For Active Directory users, the primary email address from Active Directory appears.	mary.major@example.com
Registration	The user's current registration status. The possible values are different between enterprise accounts, where invitations are not sent, and team accounts, where invitations are sent.	**Registered**, **Unregistered** (for a team account), or **Suspended** (for an enterprise account)
Permission tier	Set to **Pro** by default, to enable users to host meetings. It can be changed to **Basic**.	**Pro**, **Basic**

Field	Description	Example
Invited	For team accounts, the date when the user was invited to the account.	04/05/2017
Joined	The date when the user first signed into Amazon Chime. For ProTrial users, this is also the date that their ProTrial began.	04/10/2017
Personal PIN	The personal meeting PIN that the user can use to schedule meetings.	0123456789
Privacy setting	The presence setting that the user selected.	**Public** or **Private**
Meetings attended	The number of meetings that a user has attended.	87
Meetings organized	The number of meetings that a user has organized.	12
Meeting satisfaction	The percentage of positive responses given to the end-of-meeting survey.	92%
Last active date	The date when the user was last active.	11/12/2017
Chat messages sent	The number of chat messages that users sent.	1025

Manage User Access and Permissions

Access to features within Amazon Chime is determined by the permissions tier assigned to the user. The ability to sign into Amazon Chime is managed by suspending or activating users.

As an Amazon Chime administrator, you can manage the permissions tiers of users in your account. However, the ability to suspend a user account is only available to enterprise team administrators. Administrators of team accounts 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 and prevent them from signing in.

Manage Permissions

How permissions are managed is determined by whether Active Directory or Okta is configured. If you have Active Directory or Okta configured for your account, permissions management is handled through group memberships. If Active Directory or Okta is not configured, permissions are managed through the Amazon Chime console.

Team Accounts and Enterprise Login with Amazon

For administrators of team and enterprise LWA accounts, where users sign in with their Login with Amazon (LwA) accounts, licenses are managed from either the **Users** or **User details** pages.

To manage Amazon Chime licenses for team accounts and enterprise LWA

1. Open the Amazon Chime console at https://console.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. Select the check boxes for the users and then choose **User actions**, **Assign permissions**, **Pro** or **Basic**, and **Assign**.

Enterprise Active Directory or Enterprise OpenID Connect Accounts

The permissions tier for users who sign in with their Active Directory or Okta credentials is determined by directory memberships. If they are a member of an Active Directory or Okta group that has been assigned Pro, they are Pro. If they are a member of an Active Directory or Okta group that has been assigned Basic, they are Basic. Users without Pro or Basic permissions can't sign into Amazon Chime.

Invite and Remove Users

Use the following information to invite and remove users from your Amazon Chime account.

Team Accounts

With a team account, you can use the Amazon Chime console to invite users from any email domain.

> **Note**
> A user's 30-day trial ends when they accept the invitation.

To invite users to a team account

1. Open the Amazon Chime console at https://console.chime.aws.amazon.com/.
2. On the **Accounts** page, select the name of the team account.
3. On the **Users** page, choose **Invite users**.
4. Type the email addresses of the users to invite (separate multiple email addresses with a semicolon **;**) and choose **Invite users**.

Use the following procedure to remove users from a team account. This disassociates the user from the account and removes any permissions that you purchased for them. The user can still access Amazon Chime, but is no longer a paid member of your Amazon Chime account. The user can no longer use autocomplete in **Contacts** to find new team users.

To remove users from a team account

1. Open the Amazon Chime console at https://console.chime.aws.amazon.com/.
2. On the **Accounts** page, select the name of the team account.
3. On the **Users** page, select the users to remove and choose **User actions**, **Remove user**.

Enterprise Accounts

With an enterprise account, any users that register for Amazon Chime with an email address for your claimed domains are automatically added to your account. If you configured Active Directory or Okta, the user must not only have an email address that uses one of your claimed domains, but they must also be members of the directory you configured for Amazon Chime.

To invite users to an enterprise account

1. Send an invitation email to the users in your organization and instruct them to follow the steps in Create an Amazon Chime Account in the *Amazon Chime User Guide*.
2. Users use an email address with the one of the domains that you claimed for your account.

After your users complete the steps to create their Amazon Chime accounts, they automatically appear on the **Users** page for the enterprise account.

Use the following procedure to suspend users from an enterprise account. This prevents users from logging in to Amazon Chime.

To suspend users from an enterprise account

1. Open the Amazon Chime console at https://console.chime.aws.amazon.com/.
2. On the **Accounts** page, select the name of the enterprise account.
3. On the **Users** page, select the users to remove and choose **User actions**, **Suspend user**.

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

- Choose one of the following options:
  - Suspend or mark the user inactive the from your Active Directory or Okta Administrator Dashboard.
  - Make sure that the user is not in an Active Directory group that has Basic or Pro permissions.

Change 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://console.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**.

Manage ProTrials

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.

Users with a Pro license 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.

Request User Attachments

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

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

To request user attachments

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

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

To use IAM policies to manage access to the Amazon Chime administration console and the **Request attachments** action, use one of the Amazon Chime managed policies (FullAccess, UserManagement, or ReadOnly). Alternatively, you can update the custom policies to include the `StartDataExport` action and `RetrieveDataExport` action. For more information about these actions, see Amazon Chime Actions (p. 21).

Configure Conference Rooms

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.

Conference room VTC devices that support SIP must dial "meet.chime.in" or "u@meet.chime.in" to connect to Amazon Chime. Devices that only support H.323 must dial 52.23.133.56 or 52.54.206.237. In both cases, if a firewall is filtering traffic between the VTC device and Amazon Chime, open the ranges for the protocol(s) used. For more information, see Network Configuration and Bandwidth Requirements (p. 27).

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

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

View 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://console.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.

Control Access to the Amazon Chime Console

As an administrator, you must complete the following tasks to allow users in your account to access the Amazon Chime console.

Create an IAM User

Services in AWS, such as Amazon Chime, require that you provide credentials when you access them. This allows the service to determine whether you have permissions to access its resources. We recommend that you avoid accessing AWS with your AWS account root credentials. Instead, use AWS Identity and Access Management (IAM). Create one or more IAM users, add the users to an IAM group, and grant permissions to the group by attaching IAM policies. All of the users in that group inherit the permissions. Your IAM users can then access the AWS and Amazon Chime consoles using their account ID, IAM user name, and password.

For more information about setting up an IAM user, see Creating Your First IAM Admin User and Group. For information about IAM, see What is IAM?

Attach Required IAM User Policies

By default, IAM users don't have permission to access the Amazon Chime console. To provide access, you must create IAM policies that grant IAM users permission to use the specific resources and actions they'll need. You must then attach those policies to IAM users or groups that require those permissions.

When you attach a policy to a user or group, it allows or denies the users permission to perform the specified tasks on the specified resources.

To make creating policies easier, Amazon Chime supports using the following AWS managed policies. AWS managed policies are built for specific use cases and are automatically updated by the Amazon Chime service team when new capabilities are added. When you use these policies, your users have immediate access to the Amazon Chime console without the need to create or maintain your own policies.

AWS Managed Policies for Amazon Chime	Description
AmazonChimeFullAccess (FA)	Full access for Amazon Chime administrators who configure and manage the service
AmazonChimeReadOnly (RO)	Read-only access to the console
AmazonChimeUserManagement (UM)	Full user management capabilities and read-only access to account settings and configuration

To create your own policies, review the Amazon Chime Actions (p. 21) below for a list of all of the actions that you can allow or deny in your policy. For more information about managing and creating IAM policies, see Managing IAM Policies. For information about how to attach managed policies to an IAM user, see Attaching and Detaching IAM Policies .

Read-Only Policy Example

This example policy provides read-only access to the Amazon Chime console. You can use this as a base for any customizations you choose to make.

Note
If you create a custom policy instead of using an AWS managed policy, when Amazon Chime adds new actions, it does not automatically update your policy. Instead, you must review the changes and manually update your policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
          "chime:ListAccounts",
          "chime:GetAccount",
          "chime:GetAccountSettings",
          "chime:ListUsers",
          "chime:GetUser",
          "chime:GetUserByEmail",
          "chime:ListAccountUsageReportData",
          "chime:ListDomains",
          "chime:GetDomain",
          "chime:ListGroups"
          "chime:ListDirectories",
          "chime:GetAccountResource"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Amazon Chime Actions

The following is the complete list of Amazon Chime actions that are available if you create a custom IAM policy for your console users. For more information about creating custom policies, see Creating IAM Policies. For more information about the managed policies for Amazon Chime, seethe section called "Attach Required IAM User Policies" (p. 20).

Note
The following abbreviations are used in the table:

- FA: FullAccess
- UM: UserManagement
- RO: ReadOnly

Action	Description	Managed Policy for Amazon Chime
Accounts		
`chime:CreateAccount`	Creates a new Amazon Chime account.	FA
`chime:RenameAccount`	Modifies the account name for your Amazon Chime enterprise or team account.	FA

Action	Description	Managed Policy for Amazon Chime
`chime:GetAccountSettings`	Shows your Amazon Chime account settings.	FA, UM, RO
`chime:UpdateAccountSettings`	Modifies your Amazon Chime account settings.	FA, UM
`chime:ListAccounts`	Lists the Amazon Chime accounts associated with your AWS account.	FA, UM, RO
`chime:GetAccount`	Gets the account details for an Amazon Chime account.	FA, UM, RO
`chime:DeleteAccount`	Deletes an Amazon Chime account.	FA
Users		
`chime:ListUsers`	Lists the users in an Amazon Chime account.	FA, UM, RO
`chime:GetUser`	Gets the user details for an Amazon Chime user.	FA, UM, RO
`chime:GetUserByEmail`	Gets the user details for an Amazon Chime user based on the email address in an Amazon Chime enterprise or team account.	FA, UM, RO
`chime:InviteUsers`	Invites new users to an Amazon Chime account.	FA, UM
`chime:SuspendUsers`	Suspend users from an Amazon Chime enterprise account.	FA, UM
`chime:ActivateUsers`	Activates users in an Amazon Chime enterprise account.	FA, UM
`chime:UpdateUserLicenses`	Manages the licenses for your Amazon Chime users.	FA, UM
`chime:ResetPersonalPin`	Resets the personal meeting PIN for an Amazon Chime user.	FA, UM
`chime:LogoutUser`	Signs a user out of all their devices.	FA, UM
Reports		
`chime:ListAccountUsageReportData`	Lists Amazon Chime account usage reporting data.	FA, UM, RO
`chime:GetUserActivityReportData`	Shows a summary of user activity on the **User details** page.	FA, UM, RO
`chime:GetMeetingDetail`	Shows attendee, connection, and other details for a meeting.	FA, UM
`chime:ListMeetingEvents`	Lists all events that occurred for a meeting.	FA, UM
`chime:ListMeetingReports`	Lists meetings that ended during the date range.	FA, UM

Action	Description	Managed Policy for Amazon Chime
Domains		
`chime:ListDomains`	Lists domains associated with your Amazon Chime account.	FA, UM, RO
`chime:AddDomain`	Adds a domain to your Amazon Chime account.	FA
`chime:GetDomain`	Shows domain details for a domain associated with your Amazon Chime account.	FA, UM, RO
`chime:DeleteDomain`	Deletes a domain from your Amazon Chime account.	FA
Active Directory		
`chime:AuthorizeDirectory`	Authorizes an Active Directory to associate with your Amazon Chime enterprise account.	FA
`chime:UnauthorizeDirectory`	Unauthorizes an Active Directory from your Amazon Chime enterprise account.	FA
`chime:ListDirectories`	Lists active Microsoft Active Directories hosted in the Directory Service of your AWS account.	FA, UM, RO
`chime:ConnectDirectory`	Connects an Active Directory to your Amazon Chime enterprise account.	FA
`chime:DisconnectDirectory`	Disconnects the Active Directory from your Amazon Chime enterprise account.	FA
Okta		
`chime:ListApiKeys`	Lists the SCIM access keys defined for your Amazon Chime account and Okta configuration.	FA
`chime:CreateApiKey`	Generates a new SCIM access key for your Amazon Chime account and Okta configuration.	FA
`chime:DeleteApiKey`	Deletes the specified SCIM access key associated with your Amazon Chime account and Okta configuration.	FA
`chime:GetAccountWithOpenIdConfig`	Gets the account details and OpenIdConfig attributes for your Amazon Chime account.	FA
`chime:UpdateAccountOpenIdConfig`	Updates the OpenIdConfig attributes for your Amazon Chime account.	FA
`chime:DeleteAccountOpenIdConfig`	Deletes the OpenIdConfig attributes from your Amazon Chime account,	FA
Directory Groups		

Action	Description	Managed Policy for Amazon Chime
`chime:ListGroups`	Lists Active Directory user groups associated with your Amazon Chime enterprise account.	FA, UM, RO
`chime:AddOrUpdateGroups`	Adds new or updated existing Active Directory user groups associated with your Amazon Chime enterprise account.	FA
`chime:DeleteGroups`	Deletes Active Directory user groups from your Amazon Chime enterprise account.	FA
Amazon Chime Support		
`chime:SubmitSupportRequest`	Submits a support ticket from the Amazon Chime console.	FA, UM
AWS Account Delegation		
`chime:AcceptDelegate`	Accepts requests to share management of an Amazon Chime account with another AWS account.	FA
`chime:ValidateDelegate`	Allows process to share the AWS account name and Amazon Chime account name.	FA
`chime:ListDelegates`	Displays shared account management status on the **Account Summary** page.	FA, UM, RO
`chime:DeleteDelegate`	Removes the shared AWS account management.	FA

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. Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

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

For more information, see the CloudTrail userIdentity Element.

Understanding Amazon Chime Log File Entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from

any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files are not an ordered stack trace of the public API calls, so they do not appear in any specific order.

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

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

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

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

Network Configuration and Bandwidth Requirements

Amazon Chime requires the following hosts, ports, and protocols to support various services. If inbound or outbound traffic is blocked, this might affect the ability to use various services, including audio, video, screen sharing, or chat.

Full Solution

The following hosts, ports, and protocols are recommended when running the full Amazon Chime solution in your environment. These recommendations apply to native clients, the web application, and in-room conference systems.

Service	Host	IP Address	Ports
Media (Audio and Video)	N/A	52.54.62.192/26	UDP/7200
	N/A	52.54.63.0/25	UDP/7200
	N/A	52.54.63.128/26	UDP/7200
	N/A	52.55.63.128/25	UDP/7200
	N/A	34.212.67.64/26	UDP/7200
	N/A	34.212.95.0/25	UDP/7200
	haxrp.m1.ue1.app.chime.aws	N/A	TCP/443
	haxrp.m2.ue1.app.chime.aws	N/A	TCP/443
	haxrp.m3.ue1.app.chime.aws	N/A	TCP/443
	haxrp.m1.uw2.app.chime.aws	N/A	TCP/443
	haxrp.m2.uw2.app.chime.aws	N/A	TCP/443
	haxrp.m3.uw2.app.chime.aws	N/A	TCP/443
	N/A	52.54.62.192/26	TCP/443 UDP/16384:17383 UDP/3478
	N/A	52.54.63.0/25	TCP/443 UDP/16384:17383 UDP/3478
	N/A	52.54.63.128/26	TCP/443 UDP/16384:17383 UDP/3478
	N/A	52.55.63.128/25	TCP/443 UDP/16384:17383 UDP/3478
	N/A	34.212.67.64/26	TCP/443 UDP/16384:17383 UDP/3478
	N/A	34.212.95.0/25	TCP/443 UDP/16384:17383 UDP/3478
Screen	chime.aws	N/A	TCP/443
	bitp.m1.ue1.app.chime.aws	N/A	TCP/443
	bitp.m2.ue1.app.chime.aws	N/A	TCP/443
	bitp.m3.ue1.app.chime.aws	N/A	TCP/443
	bitp.m1.uw2.app.chime.aws	N/A	TCP/443
	bitp.m2.uw2.app.chime.aws	N/A	TCP/443
	bitp.m3.uw2.app.chime.aws	N/A	TCP/443
	bitpw.m1.ue1.app.chime.aws	N/A	TCP/443
	bitpw.m2.ue1.app.chime.aws	N/A	TCP/443
	bitpw.m3.ue1.app.chime.aws	N/A	TCP/443
	bitpw.m1.uw2.app.chime.aws	N/A	TCP/443
	bitpw.m2.uw2.app.chime.aws	N/A	TCP/443
	bitpw.m3.uw2.app.chime.aws	N/A	TCP/443
Core	app.chime.aws	N/A	TCP/443
	api.express.ue1.app.chime.aws	N/A	TCP/443
	cognito-identity.us-east-	N/A	TCP/443
	kinesis.us-east-1.amazonaws.com	N/A	TCP/443
	kinesis.web.ue1.app.chime.aws	N/A	TCP/443
	mobileanalytics.us-east-	N/A	TCP/443
	ma.web.ue1.app.chime.aws	N/A	TCP/443
	pinpoint.us-east-1.amazonaws.com	N/A	TCP/443
	pinpoint.web.ue1.app.chime.aws	N/A	TCP/443
H.323	N/A	52.23.133.56	TCP/1720
	N/A	52.54.206.237	TCP/1720
	N/A	52.55.62.128/25	TCP/1024:65535 UDP/1024:65535
	N/A	52.55.63.0/25	TCP/1024:65535 UDP/1024:65535
SIP	meet.chime.in or u@meet.chime.in	0.0.0.0/0	TCP/5061
		52.55.62.128/25	UDP/1024:65535
		52.55.63.0/25	UDP/1024:65535

Web Application Only

The following hosts, ports, and protocols are recommended if you use the Amazon Chime web application only in your environment.

Service	Host	IP Address	Ports
Core	app.chime.aws	N/A	TCP/443
	api.express.ue1.app.chime.aws	N/A	TCP/443
	cognito-identity.us-east-	N/A	TCP/443
	kinesis.us-east-1.amazonaws.com	N/A	TCP/443
	kinesis.web.ue1.app.chime.aws	N/A	TCP/443
	ma.web.ue1.app.chime.aws	N/A	TCP/443
	pinpoint.web.ue1.app.chime.aws	N/A	TCP/443
	bitpw.m1.ue1.app.chime.aws	N/A	TCP/443
	bitpw.m2.ue1.app.chime.aws	N/A	TCP/443
	bitpw.m3.ue1.app.chime.aws	N/A	TCP/443
	bitpw.m1.uw2.app.chime.aws	N/A	TCP/443
	bitpw.m2.uw2.app.chime.aws	N/A	TCP/443
	bitpw.m3.uw2.app.chime.aws	N/A	TCP/443
Media	N/A	52.54.62.192/26	TCP/443
	N/A	52.54.63.0/25	TCP/443
	N/A	52.54.63.128/26	TCP/443
	N/A	52.55.63.128/25	TCP/443
	N/A	34.212.67.64/26	TCP/443
	N/A	34.212.95.0/25	TCP/443
	N/A	52.54.62.192/26	UDP/3478
	N/A	52.54.63.0/25	UDP/3478
	N/A	52.54.63.128/26	UDP/3478
	N/A	52.55.63.128/25	UDP/3478
	N/A	34.212.67.64/26	UDP/3478
	N/A	34.212.95.0/25	UDP/3478

H.323 Only

The following ports and protocols are recommended if you use in-room video systems only via H.323 in your environment.

Service	Host	IP Address	Ports
H.323	N/A	52.23.133.56	TCP/1720
	N/A	52.54.206.237	TCP/1720
	N/A	52.55.62.128/25	TCP/1024:65535 UDP/1024:65535
	N/A	52.55.63.0/25	TCP/1024:65535 UDP/1024:65535

SIP Only

The following ports and protocols are recommended if you use in-room video systems only via SIP in your environment.

Service	Host	IP Address	Ports
SIP	meet.chime.in or u@meet.chime.in	0.0.0.0/0	TCP/5061
		52.55.62.128/25	UDP/1024:65535
		52.55.63.0/25	UDP/1024:65535

Bandwidth Requirements

Amazon Chime has the following bandwidth requirements for media services 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 for network conditions
- Screen
  - 1.2 mbps up (presenting) and down (viewing) for high quality (adapts as low as 320 kbps for network conditions)
  - Remote control: 800 kbps fixed

Purchase Amazon Chime

With Amazon Chime usage-based pricing, you only pay for users that host meetings, on the days that the meetings are hosted. Meeting attendees and chat users are not charged. For more information on pricing and how to upgrade to Pro, see Plans and pricing.

With Pro permissions, users can act as meeting hosts. You are only charged for a user if they host a meeting that meets one or more of the following criteria:

- The meeting is scheduled.
- The meeting includes more than two attendees.
- The meeting is recorded.
- Meeting attendees join using a dial-in or in-room video system.

When a user is assigned Pro permissions, they can access the schedule meeting assistant and start instant meetings from the Amazon Chime **Meetings** menu. They also have access to the Amazon Chime for Outlook add-in for Windows.

In addition to VoIP, attendees can join meetings started by a Pro user using either dial-in or in-room video systems.

Assigning a user Basic permissions prevents them from hosting meetings. Basic users are free, and can attend meetings, receive auto-calls when meetings start, and use all chat and chat room features.

Get 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.

Resources

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

- Amazon Chime Help Center
- Amazon Chime Training Videos

Document History for Amazon Chime

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

update-history-change	update-history-description	update-history-date
Amazon Chime call me feature (p. 34)	Administrators can enable the Amazon Chime call me feature on the **Policies** page. For more information, see Use the Policies Page in the Amazon Chime Administrator Guide.	August 22, 2018
Connect to Okta SSO (p. 34)	If you have an enterprise account, you can connect to Okta SSO to authenticate and assign user permissions. For more information, see Connect to Okta SSO in the Amazon Chime Administrator Guide.	August 1, 2018
Request User Attachments (p. 34)	Receive attachments uploaded into Amazon Chime by users. For more information, see Request User Attachments in the Amazon Chime Administrator Guide.	April 23, 2018
View Additional Report Data (p. 34)	View additional report data. For more information, see View Reports in the Amazon Chime Administrator Guide.	March 30, 2018
Assign Users Pro or Basic Permissions (p. 34)	Assign users Pro or Basic permissions. For more information, see Manage User Access and Permissions in the Amazon Chime Administrator Guide.	March 29, 2018