Amazon Chime

Administration Guide

Amazon Chime: Administration Guide

Table of Contents

What Is Amazon Chime?

Amazon Chime is a communications service that transforms online meetings with 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, chat, and to 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, managing Amazon Chime users, and managing Amazon Chime licenses. You must have an AWS account to access the Amazon Chime console.

With Amazon Chime, you choose a subscription plan for your Amazon Chime users: Amazon Chime Plus or Amazon Chime Pro. Pricing is per user per month, and if you change plans within a month, plans are prorated daily. You can try Amazon Chime Pro for 30 days for free. You can change or cancel a subscription at any time. For more information, see Plans and pricing.

Getting Started

The easiest way 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.

If you have installed Amazon Chime and want to expand your pilot or proof of concept to include administrator functionality, 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
   This might be unavailable in your browser if you previously signed into the AWS Management Console. In that case, choose **Sign in to a different account**, and then choose **Create a new AWS account**.

2. Follow the online instructions.

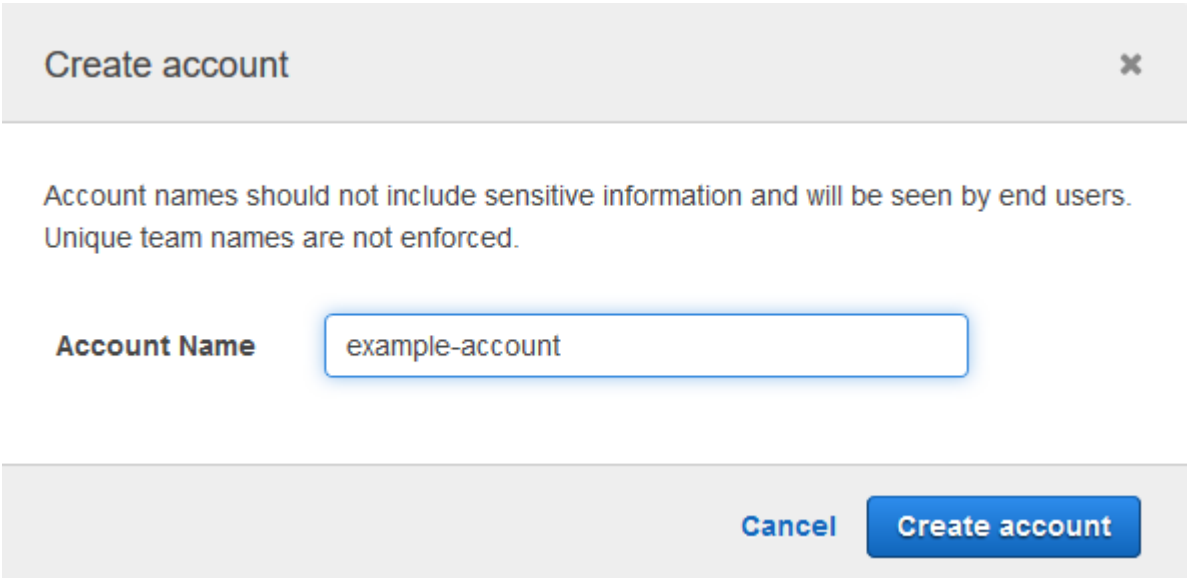
   Part of the sign-up procedure involves receiving a phone call and entering a PIN using the phone keypad.

Step 2: Create an Amazon Chime Account

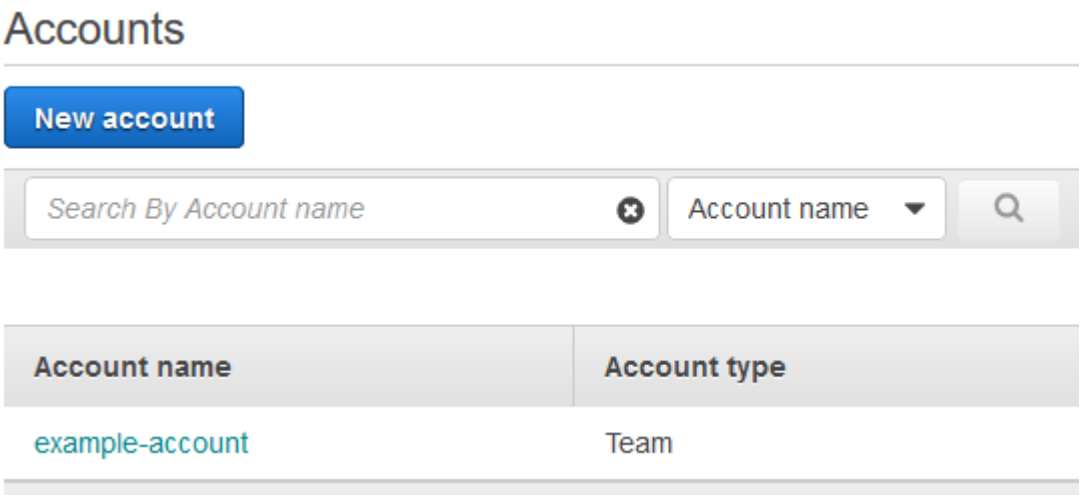
After you've created your AWS account, you can create an Amazon Chime account.

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 then choose **Create account**.



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



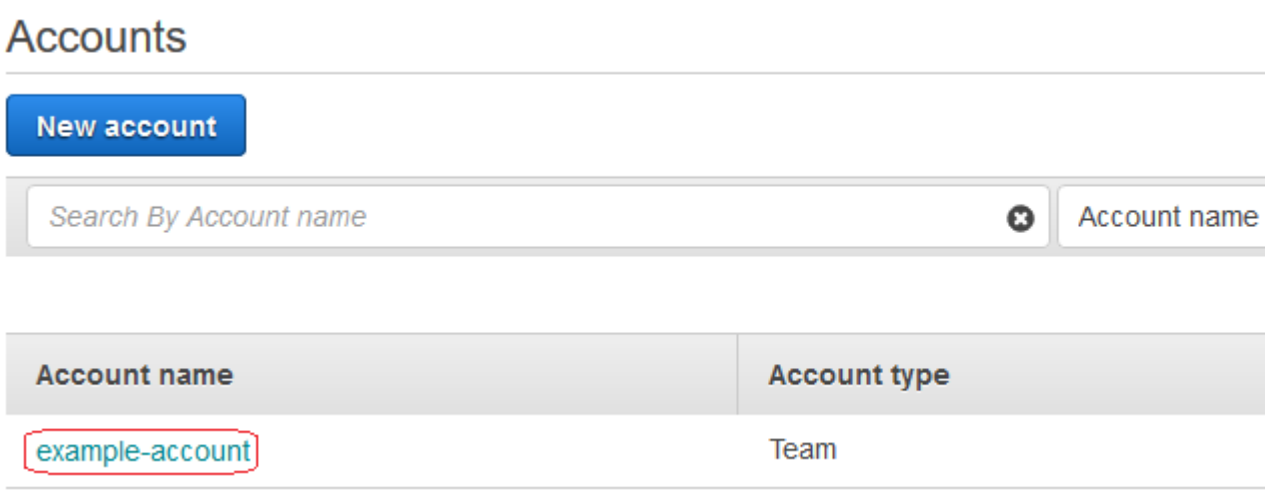
Step 3: Add Users to Your Amazon Chime Account

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

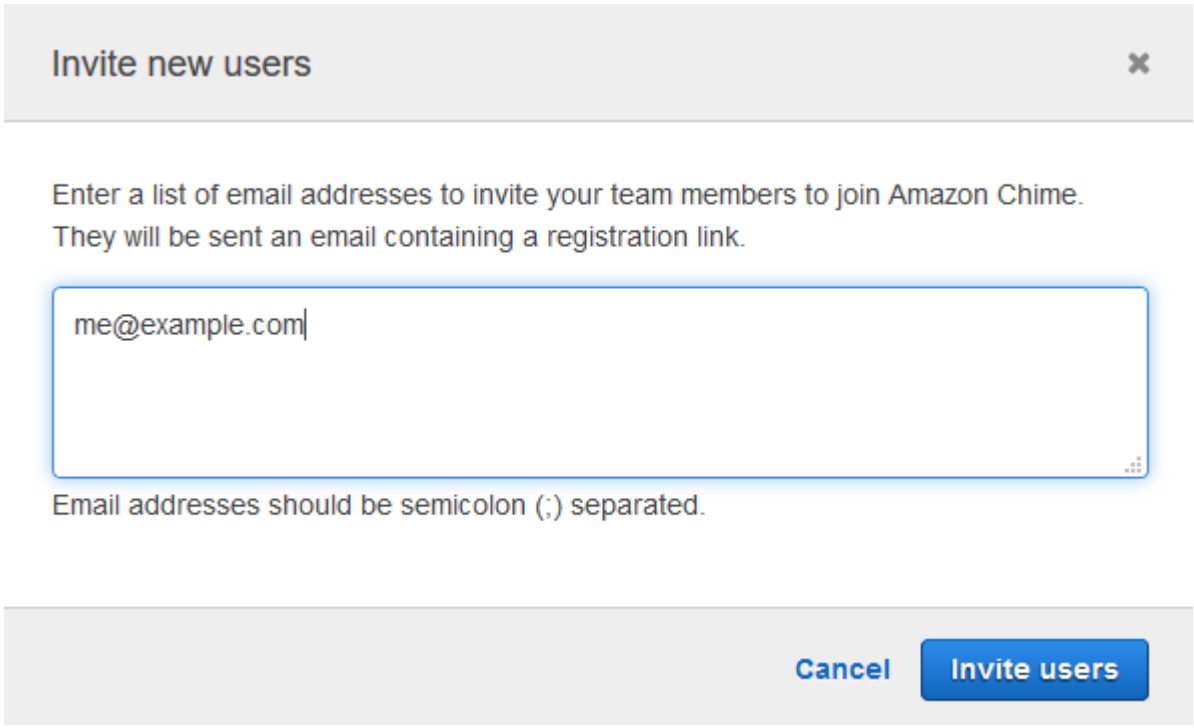
> **Note**
> If you plan to upgrade your account to an enterprise account, there is no need to invite users through the administration console. Instead, you claim your domain(s), and any users that register with your claimed domain become part of your account. For more information about claiming your first domain and becoming an enterprise account, see Claim a Domain (p. 7).

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, choose **Invite users**.



4. You (or your user) receives an email invitation to join the Amazon Chime team that you created. The email recipient chooses **Accept** in the email invitation.
5. After a user chooses **Accept** in the email invitation, they are assigned an Amazon Chime Plus license by default. To upgrade them to an Amazon Chime license Pro, see Manage User Access and Licenses (p. 11).

   - If the user has already signed up for an Amazon Chime, they can use the work email address that they used to sign up for Amazon Chime.
   - 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 that you want 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. You can decide whether you want to create a **team account** or **enterprise account**.

A **team account** is the easiest way to start inviting users to your organization and pay for their Pro or Plus licenses. You don't have to claim a domain, and you can invite users from any email domain. 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 Plus or Pro users outside of your organization.

An **enterprise account** provides more control over your users from your company domains, and includes the ability to connect to your Microsoft Active Directory for authentication and other capabilities. They are best during a proof-of-concept period or for smaller pilots where you want to try some of the basic administrative abilities available in the Amazon Chime administration console, but don't want to perform the extra step of claiming a domain or connecting to an Active Directory. Enterprise accounts provide full management of users within your account, ensuring that all users that join Amazon Chime using your claimed domains are included in your centrally managed Amazon Chime account. Enterprise administrators also can suspend and activate users. Enterprise accounts require claiming at least one email domain. They are best when you want to use the full administrative capabilities that Amazon Chime has to offer, including the ability to prevent specific users from signing in. Enterprise accounts simplify the process of adding users and are required for the additional benefits of managing your users through Active Directory.

> **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.

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).

If you want to immediately upgrade to an enterprise account, after completing Step 2: Create an Amazon Chime Account (p. 2), skip to Claim a Domain (p. 7) to claim at least one domain. For more information about team and enterprise accounts, see Managing Your Amazon Chime Accounts (p. 5).

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. On the **Accounts** page, select the name of the account.

   Note
   You can search for accounts by account name, or search for specific users across all of your accounts using their email address.
   Selecting an account open's that account's page, where 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. On the **Accounts** page, select the name of the account.
3. Choose **Account actions**, **Rename account**, enter the new account name, and choose **Save**.

Delete Your Account

Use the following steps to delete your account.

To delete your account

1. Open the Amazon Chime console at https://console.chime.aws.amazon.com/.
2. On the **Accounts** page, select the name of the account.
3. In the navigation pane, choose **Users**.
4. Select all of the users, and then choose **User Actions**, **Remove all users**.

   Note
   If you have an enterprise account, you must first delete any claimed domains, which converts your account back to a team account. After all users are removed, can delete your account. For more information about how to submit a ticket to support, see Get Support for Amazon Chime (p. 22).
5. In the navigation pane, choose **Accounts**, **Account actions**, and **Delete account**.
6. Confirm that you want to delete your account.

Use the Policies Page

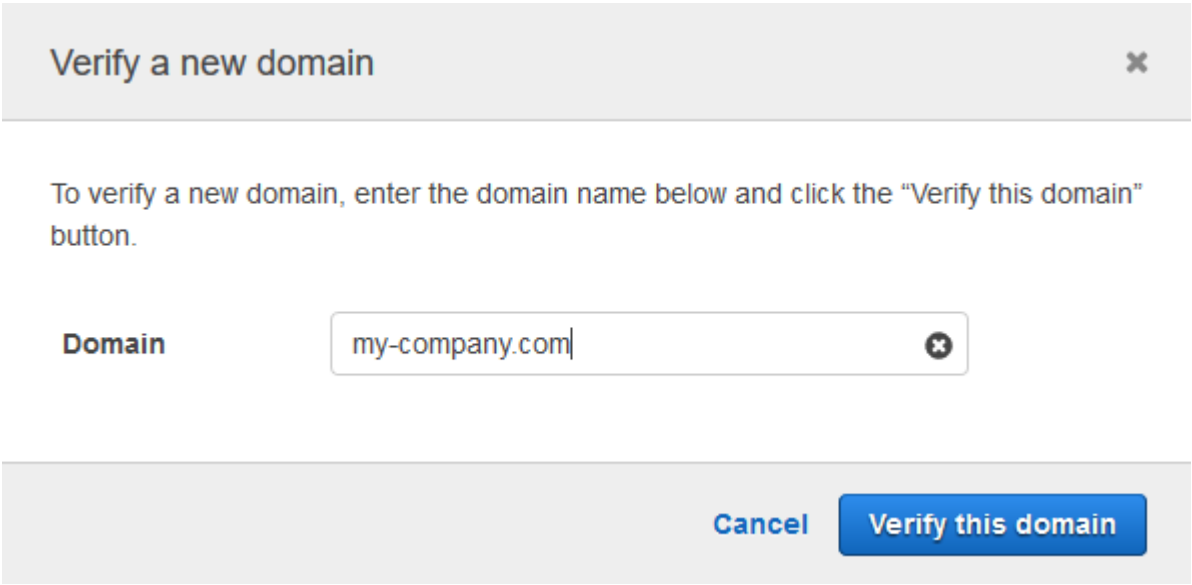
The **Policies** page allows you to choose whether users in your organization are able to share control of their computer while in meetings. Attendees in meetings hosted by your users receives an error message indicating that remote control is not available.

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. Follow these steps to claim your 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**, **Claimed domains**.
4. On the **Claimed 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 Plus or Pro licenses.
  - Multiple groups can be configured to receive Plus or Pro licenses.
  - Users that are not members of either group can't 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:

- 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. 7).

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

To connect to your Active Directory

1. Open the Amazon Chime console at https://console.chime.aws.amazon.com/.
2. In the navigation pane, **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 **License**, select **Plus** or **Pro**. Choose **Add Group**.
5. 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 will be asked to **Log in with Amazon** and won't be 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.

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** also see options to manage user licenses and remove users from the account. These actions are managed through Active Directory for accounts where Active Directory is configured.

Contents

View User Details

You can use the **User details** page to enter 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, this is the email address they used to register. For Active Directory users, the primary email address from Active Directory appears.	mary.major@example.com
Registration	The user's current registration status. Possible values are different for 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)

Field	Description	Example
License	License types for users are **Plus** by default and **Pro** for upgraded users. Users that registered within the past 30 days, and have not had their license type changed, appear as **ProTrial**.	**Pro**, **Plus**, or **ProTrial**
Invited	For team accounts, this is 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	This is the personal meeting PIN that the user can use to schedule meetings.	0123456789
Privacy setting	This is the presence setting that the user selected.	**Public** or **Private**

Manage User Access and Licenses

Access to features within Amazon Chime is determined by the license type 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 license types of users in your account, but 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 they are no longer paying for the user's license, but they can't suspend the user and prevent them from signing in.

Manage Licenses

How license types are managed is determined by whether you have Active Directory configured. If you have Active Directory configured for your account, license management is handled through group memberships. If Active Directory is not configured, license types 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 user license**, **Pro** or **Plus**, and **Assign**.

Enterprise Active Directory Accounts

The license type for users that sign in with their Active Directory credentials is determined by group memberships. If they are a member of an Active Directory group that has been assigned Pro, they are Pro. If they are a member of a group that has been assigned Plus, then they have Plus status. Users not in any of the groups with Pro or Plus license tiers can't sign into Amazon Chime.

Invite and Remove Users

Team Accounts

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

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 then choose **Invite users**.

Use the following procedure to remove users from a team account. This disassociates the user from the account and removes any license 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, the user must not only have an email address that uses one of your claimed domains, but they must also be members of the group 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.
3. 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 them 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**.

Change Personal Meeting PINs

A personal meeting PIN is a static ID generated when the user registers that 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. Choose the name of the user to open the **User detail** page.
6. Choose **User actions**, **Update Meeting PIN**, **Confirm**.

Manage ProTrials

Users are eligible for a 30-day free trial and are given ProTrial status when they first register for Amazon Chime. This gives them the same access to features within Amazon Chime as Pro users, but with a limited set of dial-in numbers. A ProTrial ends when the 30-day period expires, or if the user's administrator changes the user's license type tier from the console.

To allow your users to keep their ProTrial status for the full 30 days before deciding whether to assign them Pro, don't change their license type.

If you configured Active Directory for your account, users only have the 30-day ProTrial period if they are in the Active Directory group that you assigned to Amazon Chime Plus.

Control Access to the Amazon Chime Console

Access to the Amazon Chime console is managed through IAM. By default, IAM users in your AWS account have access to manage your Amazon Chime accounts. To restrict the access IAM users have to Amazon Chime, create IAM policies that grant permissions to perform specific actions, such as changing license types, then attach those policies to the IAM users or groups that require those permissions.

For more information about IAM policies, see Access Management. For more information about managing and creating custom IAM policies, see Working with Policies.

The easiest way to manage access for your users is to use one of the following AWS managed policies.

AWS Managed Policies for Amazon Chime	Description
AmazonChimeFullAccess	Access for administrators
AmazonChimeReadOnly	Read only access to the console
AmazonChimeUserManagement	Full user management capabilities and read only access to account settings and configuration

Amazon Chime Actions

The following is the complete list of Amazon Chime actions that can be used if you want to create a custom policy for your console users.

Action	Description
Accounts	
`chime:CreateAccount`	Creates a new Amazon Chime account.
`chime:RenameAccount`	Modifies the account name for your Amazon Chime enterprise or team account.
`chime:ListAccounts`	Lists the Amazon Chime accounts associated with your AWS account.
`chime:GetAccount`	Gets the account details for an Amazon Chime account.
`chime:DeleteAccount`	Deletes an Amazon Chime account.
Users	
`chime:GetAccountSettings`	Shows your Amazon Chime account settings.
`chime:UpdateAccountSettings`	Modifies your Amazon Chime account settings.
`chime:ListUsers`	Lists the users in an Amazon Chime account.
`chime:GetUser`	Gets the user details for an Amazon Chime user.

Action	Description
chime:GetUserByEmail	Gets user details for an Amazon Chime user based on the email address in an Amazon Chime enterprise or team account.
chime:InviteUsers	Invites new users to an Amazon Chime account.
chime:SuspendUsers	Suspend users from an Amazon Chime enterprise account.
chime:ActivateUsers	Activates users in an Amazon Chime enterprise account.
chime:UpdateUserLicenses	Manages the licenses for your Amazon Chime users.
chime:ResetPersonalPin	Resets the personal meeting PIN for an Amazon Chime user.
Domains	
chime:ListDomains	Lists domains associated with your Amazon Chime account.
chime:AddDomain	Adds a domain to your Amazon Chime account.
chime:GetDomain	Shows domain details for a domain associated with your Amazon Chime account.
chime:DeleteDomain	Deletes a domain from your Amazon Chime account.
Amazon Chime Support	
chime:SubmitSupportRequest	Submits a support ticket from the Amazon Chime console.
Directories	
chime:ListDirectories	Lists active Active Directories hosted in the Directory Service of your AWS account.
chime:ConnectDirectory	Connects an Active Directory to your Amazon Chime enterprise account.
chime:DisconnectDirectory	Disconnects the Active Directory from your Amazon Chime enterprise account.
chime:ListGroups	Lists Active Directory user groups associated with your Amazon Chime enterprise account.
chime:AddOrUpdateGroups	Adds new or updates existing Active Directory user groups associated with your Amazon Chime enterprise account.
chime:DeleteGroups	Deletes Active Directory user groups from your Amazon Chime enterprise account.
AWS Account Delegation	
chime:AcceptDelegate	Accepts request(s) to share management of an Amazon Chime account with another AWS account.
chime:ValidateDelegate	Allows process to share the AWS account name and Amazon Chime account name.
chime:ListDelegates	Displays shared account management status on the **Account Summary** page.
chime:DeleteDelegate	Removes the shared AWS account management.

Example: Full Console Access

The following policy statement grants an IAM user full access to the Amazon Chime console.

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

Example: Read-only Console Access

The following policy statement grants IAM users read-only access to the Amazon Chime console. They can see all of the users, their current status, and their personal meeting PINs, but not make any changes.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
          "Chime:ListAccounts",
          "Chime:GetAccount",
          "Chime:GetAccountSettings",
          "Chime:ListUsers",
          "Chime:GetUser",
          "Chime:GetUserByEmail",
          "Chime:ListDomains",
          "Chime:GetDomain",
          "Chime:ListGroups"

          ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Log Amazon Chime Administration Calls with AWS CloudTrail

The Amazon Chime administration console is integrated with AWS CloudTrail. CloudTrail is a service that captures API calls made by or on behalf of Amazon Chime in your AWS account and delivers the log files to an Amazon S3 bucket that you specify. CloudTrail captures all API calls from the Amazon Chime administration console and logs the responses from mutating calls. For example, listDomain is read-only and you only see the request in CloudTrail. However, with addDomain, you see both the request and the response. Using the information collected by CloudTrail, you can determine which requests were made, the source IP address for the request, who made the request, and when it was made. For more information, including how to configure and enable CloudTrail, see the AWS CloudTrail User Guide.

When CloudTrail logging is enabled in your AWS account, API calls made from the Amazon Chime administration console on your behalf are tracked in log files. These records are written together with other AWS service records in a log file. CloudTrail determines when to create and write to a new file based on time period and file size. All actions taken in the administration console use API calls and are logged by CloudTrail. You can store your log files in your bucket for as long as you want, or you can define Amazon S3 lifecycle rules to archive or delete log files automatically. By default, your log files are encrypted using Amazon S3 server-side encryption (SSE). To take quick action upon log file delivery, you can choose to have CloudTrail publish Amazon SNS notifications when new log files are delivered. For more information, see Configuring Amazon SNS Notifications for CloudTrail. You can also aggregate AWS Directory Service log files from multiple AWS Regions and AWS accounts into a single S3 bucket. For more information, see Receiving CloudTrail Log Files from Multiple Regions.

CloudTrail log files can contain one or more log entries, with each entry comprised of multiple JSON-formatted events. A log entry represents a single request and contains information about the action taken, who generated the request, where they were when they made the request, system information, and information that varies depending on the type of request. For example, the addDomain call includes information on the domain the user is adding. Every log entry also contains information about who generated the request. The identity information in the log helps you determine whether the request was made with root or IAM user credentials, with temporary security credentials for a role or federated user, or by another AWS service. For more information, see the **userIdentity** field in the CloudTrail Log Event Reference.

Log entries are not in any particular order and are not an ordered stack trace of the public API calls. Entries for Amazon Chime are identified by the **chime.amazonaws.com** event source. Sensitive information, such as passwords, authentication tokens, file comments, and file contents, are redacted in log entries.

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 is an example of 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 inability to use various services, including audio, video, screen sharing, or chat.

Service	Host	IP Address	Ports
Audio (App)	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
	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
Screen (App)	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
Screen (Web)	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
Video (App)	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
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

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 kbps 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

You can purchase Amazon Chime for yourself and for other users and pay a monthly fee per user. Billing starts after users have been added and are registered. What you pay depends on the subscription plan that you choose. For more information, see Plans and pricing.

To purchase Amazon Chime

1. Open the Amazon Chime console at https://console.chime.aws.amazon.com/.
2. Complete the steps in Step 2: Create an Amazon Chime Account (p. 2).
3. Complete the steps in Step 3: Add Users to Your Amazon Chime Account (p. 3).

   Note
   Be sure to add yourself to the account.

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

To learn more about Amazon Chime, see the following resources:

- Amazon Chime Help Center
- Amazon Chime Training Videos

Document History for Amazon Chime

The following table describes the documentation for this release of Amazon Chime.

- **Latest documentation update:** December 15, 2017

Change	Description	Date
Reorganization of content	Structural changes throughout	December 15, 2017
Log Amazon Chime administration calls from the console with AWS CloudTrail	Log Amazon Chime Administration Calls with AWS CloudTrail (p. 17)	September 27, 2017
Configure Amazon Chime to interact with your Active Directory	Connect to Your Active Directory (p. 7)	May 5, 2017
Initial release	Initial release	February 14, 2017