Amazon Chime

Administration Guide

Amazon Chime: Administration Guide

Table of Contents

What is Amazon Chime?

Amazon Chime is a secure, real-time, unified communications service that helps you run online meetings efficiently. Amazon Chime runs securely on the AWS cloud. The service delivers high-quality audio and video through an application that is easy to use and stays in sync across all of your devices. With Amazon Chime, meetings start on time and a visual roster makes them easy to manage.

Overview

As an administrator, you'll 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.

There are two types of Amazon Chime accounts: team accounts and enterprise accounts. When you create an Amazon Chime account, it is a team account. You can invite users from any email domain to join a team account using the Amazon Chime console. Users receive an invitation email. When users accept your invitation, they are granted an Amazon Chime Plus license. Users can download the Amazon Chime client application at any time, and can be granted an Amazon Chime Pro license from the Amazon Chime console. For more information, see Get Started Using Amazon Chime (p. 2).

If your users are from your organization's email domain, you can convert your team account to an enterprise account. To do this, you send email invitations to your users with instructions to download the Amazon Chime client application. Your users then register for Amazon Chime using their corporate email addresses, which automatically adds them to your Amazon Chime enterprise account. You can also choose to connect your Amazon Chime account with your Active Directory. This enables your Amazon Chime users to log in to Amazon Chime using their directory credentials. For more information, see Manage Users for an Amazon Chime Enterprise Account (p. 8).

Get Started Using Amazon Chime

To get started with Amazon Chime, 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 the Console**, and then choose **Create a new AWS account**.

2. Follow the online instructions.

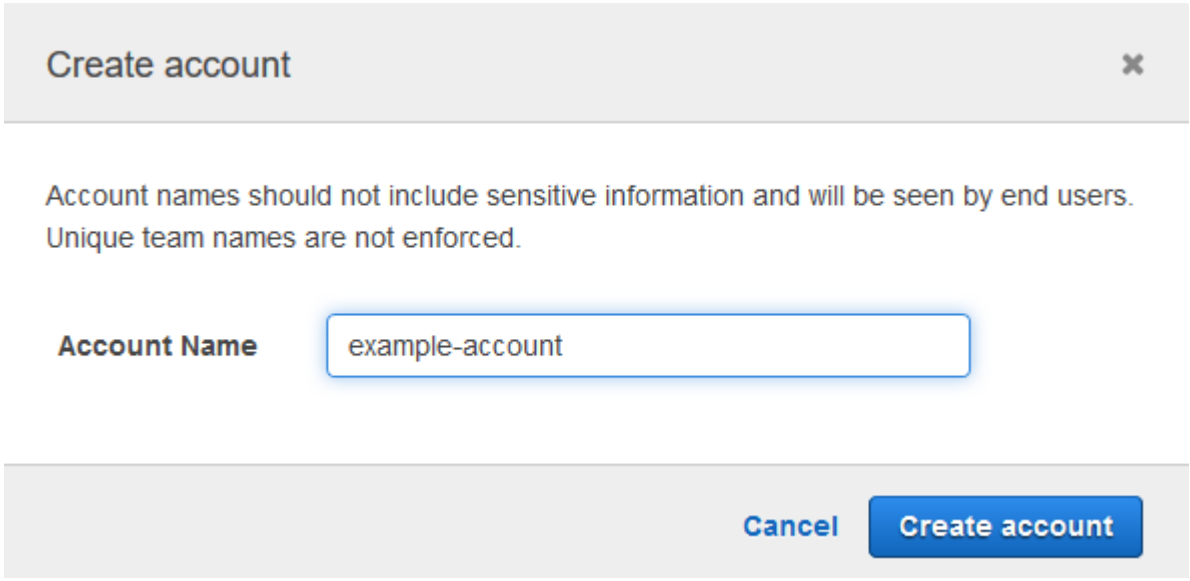
   Part of the sign-up procedure involves receiving a phone call and entering a PIN using the phone keypad.

Step 2: Create an Amazon Chime Account

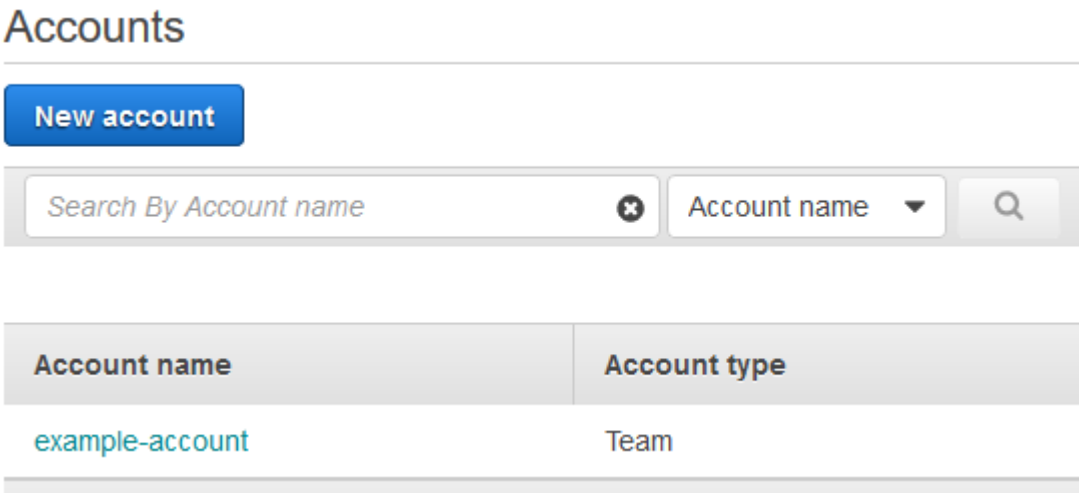
After you've created your AWS account, you can create an Amazon Chime account.

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**.

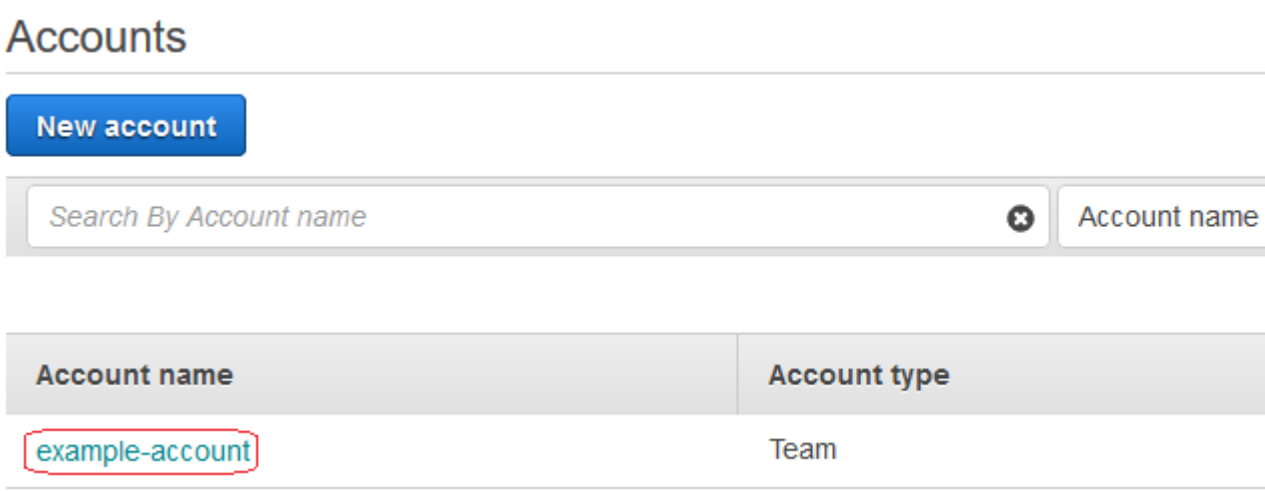


Step 3: Purchase Amazon Chime

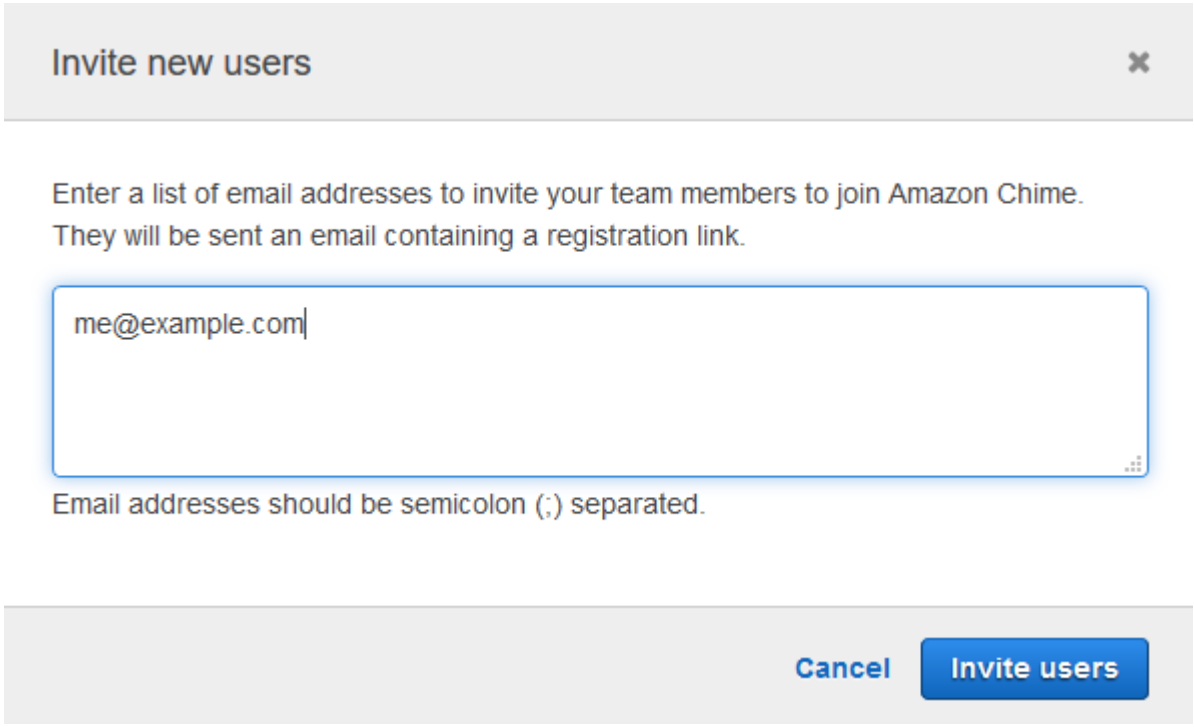
You can purchase Amazon Chime for yourself and for other users and pay a monthly fee per user. What you pay depends on the subscription plan you choose. For more information, see Plans and pricing.

To purchase Amazon Chime

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



3. On the **Users** page, choose **Invite users**.
4. Type the email address that you (or your user) used to sign up for Amazon Chime and choose **Invite users**.



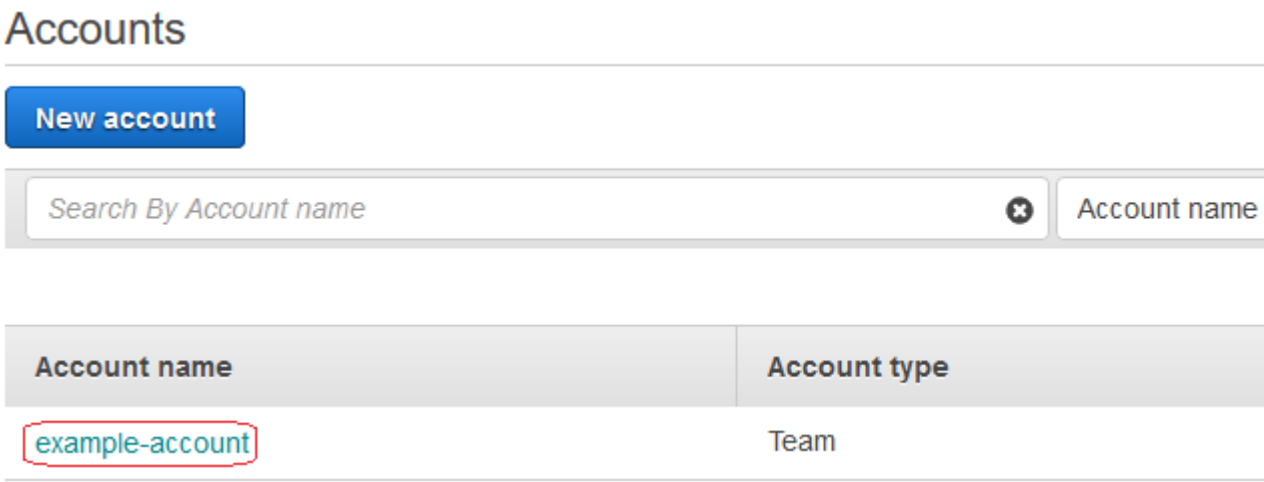
5. You (or your user) receives an email invitation to join the Amazon Chime team that you created. The email recipient chooses **Accept** in the email invitation.
6. After a user chooses **Accept** in the email invitation, they are granted an Amazon Chime Plus license. If the user hasn't already downloaded the Amazon Chime client app (this can be done at any time), they can choose **Download Amazon Chime** to download it and sign in.
7. Repeat this procedure for each additional user that you want to invite.

   If the user has already signed up for an Amazon Chime trial, use the email address that the user used to sign up for Amazon Chime. Otherwise, use the work email address of the user.

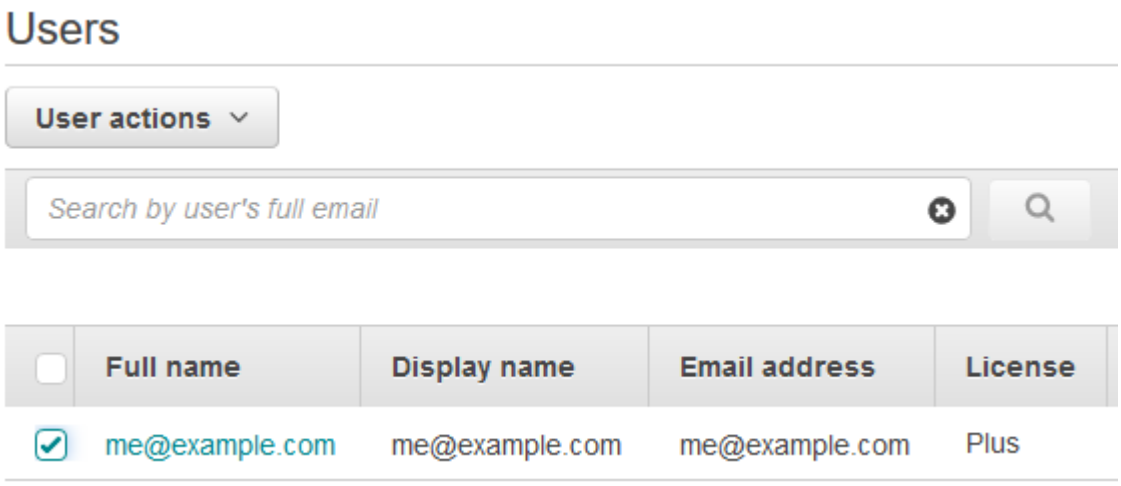
By default, users are granted an Amazon Chime Plus license. Use the following procedure to upgrade from an Amazon Chime Plus license to an Amazon Chime Pro license.

To update from a Plus license to a Pro license

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, select the checkbox next to your email address.



4. Choose **User actions**, **Grant Pro license**.

Manage Users for an Amazon Chime Team Account

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

Alternatively, if the users are from your organization's domain, you can convert your team account to an enterprise account. With an enterprise account, you can send an invitation to the users in your organization and provide them with instructions to create their own Amazon Chime accounts. For more information, see Manage Users for an Amazon Chime Enterprise Account (p. 8).

Contents

Invite Users

Use the following procedure to invite users to join a team account.

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 and then choose **Invite users**.

Remove Users

Use the following procedure to remove users from a team account. This disassociates the 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.

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**.

Manage Users for an Amazon Chime Enterprise Account

After you create an Amazon Chime team account, you can convert it to an enterprise account, connect the account to your Active Directory so that your users can log in to Amazon Chime using their directory credentials, and invite and remove users.

Contents

Invite Users

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*.

> **Note**
> Users must use an email address with the domain that you claimed for your account.

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

Suspend Users

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

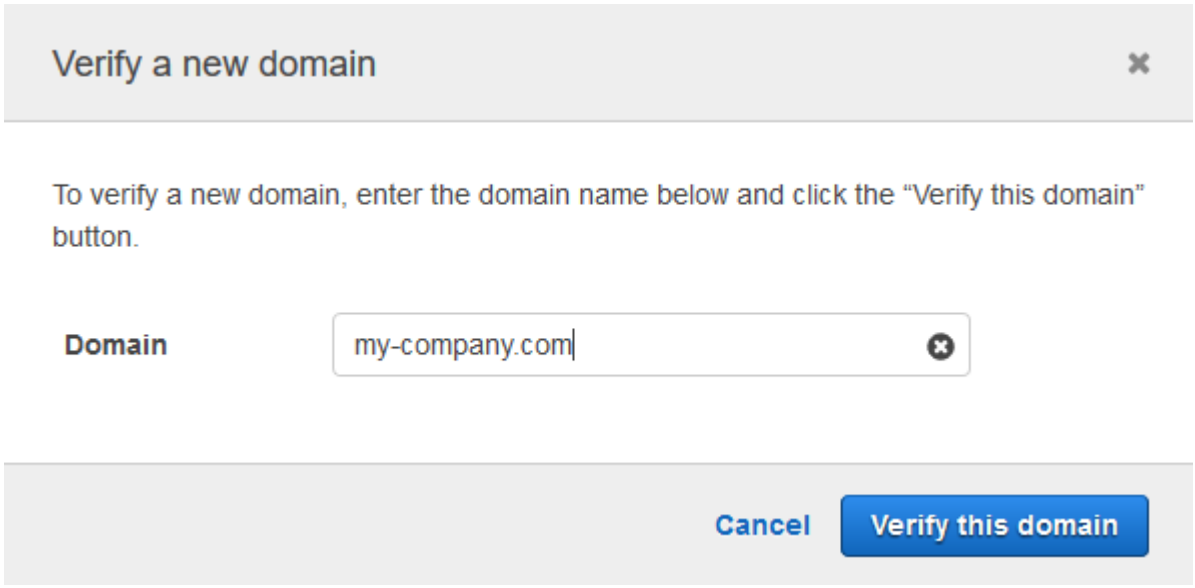
1. Open the Amazon Chime console at https://console.chime.aws.amazon.com/.
2. On the **Accounts** page, select the name of the enterprise account.
3. On the **Users** page, select the users to suspend and choose **User actions**, **Suspend users**.

Convert a Team Account to an Enterprise Account

Use the following steps to convert a team account to an enterprise account.

To convert a team account to 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 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

You can connect your Amazon Chime account with your organization's 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. Note that Amazon Chime can connect using AD Connector or Microsoft AD.
- Set up an Amazon Chime enterprise account. For more information, see Convert a Team Account to an Enterprise Account (p. 9).

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 add a 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.

Manage Amazon Chime Licenses

When a user subscribes to Amazon Chime, they receive a Amazon Chime Plus license or a Amazon Chime Pro license. You can change the license for a user at any time.

To manage Amazon Chime licenses

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. To upgrade users from a Amazon Chime Plus license to a Amazon Chime Pro license, select the checkboxes for the users and then choose **User actions**, **Grant Pro license**.
5. To downgrade users from a Amazon Chime Pro license to a Amazon Chime Plus license, select the checkboxes for the users and then choose **User actions**, **Revoke Pro license**.

Change Amazon Chime Personal Meeting PINs

A personal meeting PIN is a custom ID that makes it easier for a 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.

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. Select the checkbox for the user.
5. Choose **User actions**, **Update Meeting PIN**, **Confirm**.

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.

Amazon Chime Actions

The following is the complete list of Amazon Chime actions.

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:CountUsers`	Counts the users in an Amazon Chime account.
`Chime:GetAccountSettings`	Shows your Amazon Chime account settings.
`Chime:UpdateAccountSettings`	Modifies your Amazon Chime account settings.

Action	Description
`Chime:ListUsers`	Lists the users in an Amazon Chime account.
`Chime:GetUser`	Gets the user details for an Amazon Chime user.
`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.
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.

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 will vary 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 user 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"
      }
```

Contact 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 premium support, 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 OSX, choose **Amazon Chime**, **About Amazon Chime**.
  - In iOS and Android, choose **Settings**, **About**.
- The Log Reference ID. To find this ID:
  - In Windows and OSX, choose **Help**, **Send Diagnostic Logs**.
  - In iOS and Android, choose **Settings**, **Send Diagnostic Logs**.
- If your issue is related to a meeting, the Meeting ID.

Document History for Amazon Chime

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

- **Latest documentation update:** September 27, 2017

Change	Description	Date
Log Amazon Chime administration calls from the console with AWS CloudTrail	Log Amazon Chime Administration Calls with AWS CloudTrail (p. 16)	September 27, 2017
Configure Amazon Chime to interact with your Active Directory	Connect to Your Active Directory (p. 9)	May 5, 2017
Initial release	Initial release	February 14, 2017