AWS Billing
User Guide
Version 2.0
AWS Billing: User Guide
Copyright © 2023 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 AWS Billing? ................................................................. 1
- Features of AWS Billing console ............................................. 1
- Related services ........................................................................ 2

### Getting started ................................................................. 3
- Step 1: Sign up for AWS and create an IAM user ..................... 3
- Sign up for an AWS account ................................................. 3
- Create an administrative user ............................................... 3
- Step 2: Review your bills and usage ....................................... 4
- Step 3: Download or print your bill ....................................... 4
- Learn more about Billing features ......................................... 4
- What do I do next? ................................................................. 5
- Optimize your spending using AWS Cost Management features . 5
- Using the Billing and Cost Management API .......................... 5
- Learn more ............................................................................. 5
- Get help ................................................................................. 5

### Getting help ........................................................................ 6
- AWS Knowledge Center ....................................................... 6
- Contacting AWS Support ...................................................... 6
- Understanding your charged usage ...................................... 7
- Monitoring your Free Tier usage ......................................... 7
- Avoiding unexpected charges .............................................. 7
- Usage exceeds AWS Free Tier ............................................. 8
- Bill received after account closure ...................................... 8
- Turning off AWS Regions .................................................... 8
- Elastic Beanstalk environments ........................................... 8
- Elastic Load Balancing (ELB) .............................................. 8
- Services started in AWS OpsWorks ..................................... 9
- Amazon EC2 instances ....................................................... 9
- Amazon Elastic Block Store volumes and snapshots .......... 9
- Elastic IP addresses ............................................................ 10
- Services launched by other services .................................. 10
- Storage services ............................................................... 10

### Managing your account .................................................. 11

- Managing an AWS account .................................................. 11
  - Editing your account name, AWS account root user password, and AWS account root user email address .................................................. 12
  - Editing contact information ............................................... 12
  - Adding or updating alternate contacts ................................ 12
  - Adding or editing security challenge questions ................. 13
  - Enabling and disabling AWS Regions ............................... 13
  - Activating IAM access to the AWS Billing console .......... 14
  - Manage account contract information ............................. 15
  - Updating and deleting tax registration numbers .............. 15
  - Turning on tax setting inheritance .................................. 15
  - Managing your US tax exemptions .................................. 16
  - Closing your AWS account ............................................. 17
- Managing an account in India .............................................. 17
  - Determining which company your account is with .......... 17
  - Signing up for Amazon Web Services India Private Limited . 18
  - Managing your AWS India account .................................. 19

### Using the AWS Billing console dashboard .......................... 24

- Understanding your dashboard page .................................. 24
- Monthly billing checklist .................................................... 26
- Check purchase order balance and expiration .................... 26
AWS Cost and Usage Reports ................................................................. 233
AWS CloudTrail .................................................................................. 233
Logging API calls with CloudTrail ......................................................... 234
Compliance validation ........................................................................... 239
Resilience .............................................................................................. 239
Infrastructure security .......................................................................... 240
Quotas and restrictions .......................................................................... 241
Cost categories ....................................................................................... 241
Purchase orders ..................................................................................... 241
Advance Pay ............................................................................................ 242
Cost allocation tags ............................................................................... 242
AWS Price List ....................................................................................... 242
Document history ................................................................................... 243
AWS glossary ......................................................................................... 252
What is AWS Billing?

Welcome to the Billing User Guide.

The AWS Billing console contains features to pay your AWS bills and report your AWS cost and usage. You can also use the AWS Billing console to manage your consolidated billing if you're a part of AWS Organizations. Amazon Web Services automatically charges the credit card that you provided when you sign up for an AWS account. You can view or update your credit card information at any time, including designating a different credit card for AWS to charge. You can do this on the Payment Methods page in the Billing console. For more details on the Billing features available, see Features of AWS Billing console (p. 1).

How to find answers about your AWS bills

For questions about your AWS bills or to appeal any of your charges, contact AWS Support to address your inquiries immediately. For options on how you can get help, see Getting help with AWS Billing (p. 6). To understand your bills page contents, see Using the Bills page to understand your monthly charges and invoice (p. 30).

Key differences between AWS Billing console and AWS Cost Management console features

The Billing console works closely with the AWS Cost Management console. The Billing console contains features to manage your ongoing payments and payment methods registered to your AWS account. The AWS Cost Management console features are useful to optimize your future costs. You can use both for a holistic approach to managing your current and ongoing costs. For information about AWS resources to optimize your costs, see the AWS Cost Management User Guide.

Pricing and marketing materials for AWS Billing features

For more information about individual feature pricing and marketing materials, see the Cloud Financial Management with AWS.

Features of AWS Billing console

With the features in AWS Billing console, you can do the following tasks:

- **Manage your account** (p. 11): Manage your account settings using the AWS Management Console and Billing console. This includes designating your default currency, editing alternate contacts, adding or removing AWS Regions, updating your tax information, and closing your AWS account. The Close your account in the AWS Account Management Reference Guide highlights considerations before you close your AWS account. For example, terminating resources before you close the account so you aren't charged for unused services.

- **View your bill** (p. 29): You can use the AWS Billing console to view your past bill details or your estimated charges for your current month at any time. This section outlines how you can view your bills, download PDF copies of your charges, and set up monthly emails to receive your invoices. It also covers how you can use other resources such as AWS Cost and Usage Reports.

- **Managing your payments** (p. 38): You can view your estimated bills and pay your AWS invoices in your preferred currency by setting a payment currency. AWS converts your bill to your preferred currency after your bill is finalized. Until then, all of the preferred currency amounts shown in the console are estimated in USD. AWS guarantees your exchange rate. This is so that refunds use the same exchange rate as your original transaction.

  **Note**
  - AWS Marketplace invoices aren't eligible for this service and are processed in US dollar.
• This service is available only if your default payment method is Visa or MasterCard.
• The rates change daily. The rate that's applied to your invoice is the current rate at the time when your invoice was created. You can check the current rate on the Billing console.
• Currency conversion is provided by Amazon Services LLC.

• **AWS Purchase Order Management (p. 68):** Manage your AWS purchase orders in a self-service fashion by taking care of multiple purchase orders all in one place. This can help to reduce your overhead costs and increase the accuracy and efficiency in your overall procure-to-pay process. Use the Billing console to manage your purchase orders and configure how it reflects on your invoices. In this section, learn how to add, edit, view details, and set up notifications regarding your purchase orders in the console.

• **AWS Cost Categories (p. 77):** Manage your AWS costs with AWS Cost Categories by mapping your cost and usage into meaningful categories. This section defines terms that are used in the console for supported dimensions, operations, rule types, and status. The section also provides more information on how you can create, edit, delete, and split the charges within cost categories.

• **Payment profile (p. 59):** You can use payment profiles to assign more than one payment method to your automatic payments. If you receive invoices from more than one AWS service provider ("seller of record"), you can use payment profiles to assign a unique payment method for each one. After you create a payment profile for a service provider, your payment profile pays your AWS bills automatically. In this section, learn how to use the Billing console to set up custom payment profile.

• **Consolidate billing for AWS Organizations (p. 146):** Use the consolidated billing feature for AWS Organizations to combine your billing for multiple AWS accounts. This chapter outlines the consolidated billing process, differences for Amazon Web Services India Private Limited accounts, and details for discounts.

---

**Related services**

**AWS Billing Conductor**

AWS Billing Conductor is a custom billing service to group your accounts by financial owner, configure billing parameters, and generate AWS Cost and Usage Reports per group. AWS Billing Conductor is a fully managed service that can support the showback and chargeback workflows of AWS Solution Providers and Enterprise customers.

**IAM**

The Billing service and AWS Cost Management service is closely integrated with AWS Identity and Access Management (IAM). You can use IAM with Billing to ensure that other people who work in your account have as much access as they need to get their jobs done.

You also use IAM to control access to all of your AWS resources, not only your billing information. It's important that you familiarize yourself with the major concepts and best practices of IAM before you get too far along with setting up the structure of your AWS account.

**AWS Organizations (Consolidated Billing)**

You can use AWS products and services to accommodate a company of any size, from small start-ups to enterprises. If your company is large or likely to grow, you might want to set up multiple AWS accounts that reflect your company's specific structure. For example, you can have one account for the entire company and accounts for each employee, or an account for the entire company with IAM users for each employee. You can have an account for the entire company, accounts for each department or team within the company, and accounts for each employee.

If you create multiple accounts, you can use the consolidated billing feature of AWS Organizations to combine all member accounts under a management account. That way, you can receive a single bill for all of your member accounts. For more information, see [Consolidated billing for AWS Organizations (p. 146)](#).
Getting started

This section provides information that you need to get started with using the Billing console.

Topics

• Step 1: Sign up for AWS and create an IAM user (p. 3)
• Step 2: Review your bills and usage (p. 4)
• Step 3: Download or print your bill (p. 4)
• Learn more about Billing features (p. 4)
• What do I do next? (p. 5)

Step 1: Sign up for AWS and create an IAM user

If you’re new to AWS, create an AWS account. For more information, see Getting Started with AWS.

Sign up for an AWS account

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

To sign up for an AWS account

2. Follow the online instructions.

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

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

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

Create an administrative user

After you sign up for an AWS account, create an administrative user so that you don't use the root user for everyday tasks.

Secure your AWS account root user

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

   For help signing in by using root user, see Signing in as the root user in the AWS Sign-In User Guide.

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

   For instructions, see Enable a virtual MFA device for your AWS account root user (console) in the IAM User Guide.
Create an administrative user

- For your daily administrative tasks, grant administrative access to an administrative user in AWS IAM Identity Center.

  For instructions, see Getting started in the AWS IAM Identity Center User Guide.

Sign in as the administrative user

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

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

Step 2: Review your bills and usage

Use features in the Billing console to view your current AWS charges and AWS usage.

To open the Billing console and view your usage and charges

2. Choose Bills to see details about your current charges.
3. Choose Payments to see your historical payment transactions.
4. Choose AWS Cost and Usage Reports to see reports that break down your costs.

For more information about setting up and using AWS Cost and Usage Reports, see the AWS Cost and Usage Reports User Guide.

Step 3: Download or print your bill

AWS Billing closes the billing period at midnight on the last day of each month and calculates your bill. Most bills are ready for you to download by the seventh accounting day of the month.

To download or print your bill

2. On the navigation pane, choose Bills.
3. For Date, choose the month of the bill you want to work with.
4. Choose Download CSV to download a comma-separated variable file or choose Print.

Learn more about Billing features

Understand the features available to you in the Billing console.

- Account settings: Managing your account (p. 11)
- AWS Free Tier: Using the AWS Free Tier (p. 98)
What do I do next?

Now that you can view and pay your AWS bill, you're ready to use the features available to you. The rest of this guide helps you navigate your journey using the console.

Optimize your spending using AWS Cost Management features

Use the AWS Cost Management features to budget and forecast costs so you can optimize your AWS spends and reduce your overall AWS bill. Combine and use the Billing console resources to manage your payments, while using AWS Cost Management features to optimize your future costs.

For more information about AWS Cost Management features, see the AWS Cost Management User Guide.

Using the Billing and Cost Management API

Use the AWS Billing and Cost Management API Reference to programmatically use some AWS Cost Management features.

Learn more

You can find more information about Billing features including presentations, virtual workshops, and blog posts on the marketing page Cloud Financial Management with AWS.

You can find virtual workshops by choosing the Services dropdown list and selecting your feature.

Get help

If you have questions about any Billing features, there are many resources available for you. To learn more, see Getting help with AWS Billing (p. 6).
Getting help with AWS Billing

There are many resources available for you if you have any questions about your AWS Billing and Cost Management console tools, your charges, or payment methods.

Topics
- AWS Knowledge Center (p. 6)
- Contacting AWS Support (p. 6)
- Understanding your charged usage (p. 7)
- Monitoring your Free Tier usage (p. 7)
- Avoiding unexpected charges (p. 7)

AWS Knowledge Center

All AWS account owners have access to account and billing support free of charge. You can find answers to your questions quickly by visiting the AWS Knowledge Center.

To find your question or request
1. Open AWS Knowledge Center.
2. Choose Billing Management.
3. Scan the list of topics to locate a question that is similar to yours.

Contacting AWS Support

Contacting AWS Support is the fastest and most direct method for communicating with an AWS associate about your questions. AWS Support does not publish a direct phone number for reaching a support representative. You can use the following process to have an associate contact to you by email or phone instead.

Only personalized technical support requires a support plan. For more information, visit AWS Support.

To open an AWS Support case where you specify Regarding: Account and Billing Support, you must either be signed into AWS as the root account owner, or have IAM permissions to open a support case. For more information, see Accessing AWS Support in the AWS Support User Guide.

If you have closed your AWS account, you can still sign in to AWS Support and view past bills.

To contact AWS Support
1. Sign in and navigate to the AWS Support Center. If prompted, enter the email address and password for your account.
2. Choose Create case.
3. On the Create case page, choose Account and billing support and fill in the required fields on the form.
4. After you complete the form, under Contact options, choose either Web for an email response, or Phone to request a telephone call from an AWS Support representative. Instant messaging support is not available for billing inquiries.
To contact AWS Support when you can't sign in to AWS

1. Recover your password or submit a form at AWS account support.
2. Choose an inquiry type in the Request information section.
3. Fill out the How can we help you? section.
4. Choose Submit.

Understanding your charged usage

If you want to see the usage behind your charged amount, you can check your usage yourself by enabling Cost Explorer. This tool enables you to analyze your costs in depth by providing you with premade reports and graphs.

Cost Explorer is available 24 hours after you activate the feature.

For more information about Cost Explorer, see Analyzing your costs with AWS Cost Explorer.

Monitoring your Free Tier usage

You can track your AWS Free Tier usage to keep you under the Free Tier limits. You can set up alerts on your AWS account when your Free Tier limits reach a threshold, and monitor your usage through the Billing and Cost Management console.

For more information about using these features, see Tracking your AWS Free Tier usage (p. 100).

To see details for usage that was charged beyond your Free Tier limit, see the Understanding your charged usage (p. 7) section.

Avoiding unexpected charges

For questions about your AWS bills or to appeal your charges, contact AWS Support to address your inquiries immediately. To get help, see Getting help with AWS Billing (p. 6). To understand your bills page contents, see Using the Bills page to understand your monthly charges and invoice (p. 30).

When you close resources, some AWS services require specific steps to ensure you aren't charged going forward. The process to close your AWS account also requires some resources to be manually turned off ahead of time so you aren't charged after closing the account. Here are some examples to help you avoid unexpected charges on your bill. This page lists specific features or behaviors within individual services from AWS that can sometimes result in unexpected charges, particularly if you unsubscribe from the service or close your account.

Note
This is not an exhaustive list. For any questions for your specific use case, contact AWS Support by following the process on Getting help with AWS Billing (p. 6).
If you close your account or unsubscribe from a service, make sure that you take the appropriate steps for every AWS Region you've allocated AWS resources.

Topics
Usage exceeds AWS Free Tier

For more information on avoiding unexpected charges related to the AWS Free Tier, see [Avoiding unexpected charges after the AWS Free Tier](p. 99).

Bill received after account closure

Each month's usage is calculated and billed at the beginning of the following month. If you close your account but use opt-in services during the month, you receive a bill for the opt-in service usage at the beginning of the following month.

Turning off AWS Regions

If you turn off an AWS Region that you still have resources in, you continue to incur charges for those resources. There is no charge for turning on an AWS Region. Charges only occur for the resources that you create in a Region. For more information, see [Enabling and disabling AWS Regions](p. 13).

Elastic Beanstalk environments

Elastic Beanstalk is designed to ensure that all the resources that you need are running, which means that it automatically relaunches any services that you stop. To avoid this, you must terminate your Elastic Beanstalk environment before you terminate resources that Elastic Beanstalk has created. For more information, see [Terminating an Environment](in the AWS Elastic Beanstalk Developer Guide).

Elastic Load Balancing (ELB)

Like Elastic Beanstalk environments, ELB load balancers are designed to keep a minimum number of Amazon Elastic Compute Cloud (Amazon EC2) instances running. You must terminate your load balancer before you delete the Amazon EC2 instances that are registered with it. For more information, see [Delete Your Load Balancer](in the Elastic Load Balancing User Guide).

Services started in AWS OpsWorks

If you use the AWS OpsWorks environment to create AWS resources, you must use AWS OpsWorks to terminate those resources or AWS OpsWorks restarts them. For example, if you use AWS OpsWorks to create an Amazon EC2 instance, but then terminate it by using the Amazon EC2 console, the AWS OpsWorks auto healing feature categorizes the instance as failed and restarts it. For more information, see [AWS OpsWorks User Guide].
Amazon EC2 instances

After you remove load balancers and Elastic Load Balancing environments, you can stop or terminate Amazon EC2 instances. Stopping an instance allows you to start it again later, but you might be charged for storage. Terminating an instance permanently deletes it. For more information, see Instance Lifecycle in the Amazon EC2 User Guide for Linux Instances, particularly Stop and Start Your Instance and Terminate Your Instance.

Note
Amazon EC2 instances serve as the foundation for multiple AWS services. They can appear in the Amazon EC2 console Instances list even if they were started by other services. For example, Amazon Relational Database Service (Amazon RDS) instances run on Amazon EC2 instances. If you terminate an underlying Amazon EC2 instance, the service that started it might interpret the termination as a failure and restart the instance. For example, the AWS OpsWorks service has a feature called auto healing that restarts resources when it detects failures. In general, it is a best practice to delete resources through the services that started them.

Additionally, if you create Amazon EC2 instances from an Amazon Machine Image (AMI) that is backed by an instance store, check Amazon S3 for the related bundle. Deregistering an AMI does not delete the bundle. For more information, see Deregistering Your AMI.

Amazon Elastic Block Store volumes and snapshots

Most Amazon EC2 instances are configured so that their associated Amazon EBS volumes are deleted when they are terminated, but it is possible to set up an instance that preserves its volume and the data. Check the Volumes pane in the Amazon EC2 console for volumes that you don’t need anymore. For more information, see Deleting an Amazon EBS Volume in the Amazon EC2 User Guide for Linux Instances.

If you have stored snapshots of your Amazon EBS volumes and no longer need them, you should delete them as well. Deleting a volume does not automatically delete the associated snapshots.

For more information about deleting snapshots, see Deleting an Amazon EBS Snapshot.

Note
Deleting a snapshot might not reduce your organization’s data storage costs. Other snapshots might reference that snapshot’s data, and referenced data is always preserved. For example, when you take the first snapshot of a volume with 10 GiB of data, the size of the snapshot is also 10 GiB. Because snapshots are incremental, the second snapshot that you take of the same volume contains only blocks of data that changed since the first snapshot was taken. The second snapshot also references the data in the first snapshot. That is, if you modify 4 GiB of data and take a second snapshot, the size of the second snapshot is 4 GiB. In addition, the second snapshot references the unchanged 6 GiB in the first snapshot. For more information, see How Incremental Snapshots Work.

The previous example will show two entries in your daily AWS Cost and Usage Reports (AWS CUR). AWS CUR captures the snapshot usage amount for a single day. In this example, the usage is 0.33 GiB (10 GiB/30 days) for snap-A, and 0.133 GiB (4 GiB/30 days) for snap-B. Using the rate of $0.05 per GB month, snap-A costs you 0.33 GiB x $0.05 = $0.0165. Snap-B costs you 0.133 GiB x $0.05 = $0.0066, and you are charged $0.0231 per day for both snapshots. For more information about AWS Cost and Usage Reports, see the AWS Cost and Usage Reports user guide.

<table>
<thead>
<tr>
<th>lineItem/Operation</th>
<th>lineItem/ResourceId</th>
<th>lineItem/UsageAmount</th>
<th>lineItem/UnblendedCost</th>
<th>resourceTags/user:usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateSnapshot</td>
<td>arn:aws:ec2:us-east-1:123:snapshot/snap-A</td>
<td>0.33</td>
<td>0.0165</td>
<td>dev</td>
</tr>
</tbody>
</table>
Elastic IP addresses

Any Elastic IP addresses that are attached to an instance that you terminate are unattached, but they are still allocated to you. If you don’t need that IP address anymore, release it to avoid additional charges. For more information, see Releasing an Elastic IP Address in the Amazon EC2 User Guide for Linux Instances.

Services launched by other services

A number of AWS services can launch resources, so be sure to check for anything that might have launched through any service that you’ve used.

Storage services

When you are minimizing costs for AWS resources, keep in mind that many services might incur storage costs, such as Amazon RDS and Amazon S3.
Managing your account

Use the procedures in this chapter to manage your account settings, your default currency, your alternate contacts, and more.

For information about closing your AWS account, see Close your account in the AWS Account Management Reference Guide.

Topics

• Managing an AWS account (p. 11)
• Managing an account in India (p. 17)

Managing an AWS account

You can use the AWS Billing and Cost Management console to change the following account settings:

• Contact and alternate contact information
• Currency that you pay your bills in
• AWS Regions that you can create resources in
• Tax registration numbers

To sign in to the Account page

Choose one of the following options:

• Sign in to the AWS Management Console, and on the top right-corner, choose your account name, and then choose Account.

Notes:

• Only the AWS account root user can edit some sections on the Account page. If you don’t see the Edit option, switch to the root user.
• For AWS accounts with a billing address in India, see Managing an account in India (p. 17).

Contents

• Editing your account name, AWS account root user password, and AWS account root user email address (p. 12)
• Editing contact information (p. 12)
• Adding or updating alternate contacts (p. 12)
  • Examples for alternate contacts (p. 13)
• Adding or editing security challenge questions (p. 13)
• Enabling and disabling AWS Regions (p. 13)
• Activating IAM access to the AWS Billing console (p. 14)
• Manage account contract information (p. 15)
Editing your account name, AWS account root user password, and AWS account root user email address

You can use the Account page to edit your account name, AWS account root user password, or email address. Email in this case refers to the root user email address. This is the email address that you use to sign in to your account.

**Note**
To perform the following procedure, you must sign in as the root user. The root user doesn't need additional AWS Identity and Access Management (IAM) permissions. You can't complete this procedure with an IAM role.

**To edit your account name, AWS account root user password, or AWS account root user email address**

2. On the Account page, next to Account settings, choose Edit.
3. Enter your updated information and then choose Update.

**Editing contact information**

You can change the contact information associated with your account, including your mailing address, telephone number, and website address.

**To edit your contact information**

2. Under Contact information, choose Edit.
3. Enter your updated information and then choose Update.

**Notes**

- Your phone number must include the country code and can only contain the following characters: 0-9, +, – (hyphen). For example, +1 202-555-0179.
- You can add an email address for billing in the Alternate contacts section to have AWS send a copy of billing-related emails to that email address. For example, AWS sends your Billing contact address an email message when your monthly bill is ready.

**Adding or updating alternate contacts**

Alternate contacts allows AWS to contact another person about issues with your account, even if you're unavailable. The alternate contact doesn't have to be a specific person. You could instead add an email distribution list if you have a team that manages billing, operations and security related issues.
To add or update alternate contacts

2. Under Alternate contacts, choose Edit.
3. Enter your updated information and choose Update.

Examples for alternate contacts

AWS will reach out to each contact type in the following scenarios:

- **Billing** – When your monthly invoice is available, or your payment method needs to be updated. If you enabled Receive PDF Invoice By Email in your Billing preferences, your alternate billing contact also receives the PDF invoices. Notifications can be from AWS Support, or other AWS service teams.
- **Operations** – When your service is, or will be, temporarily unavailable in one of more AWS Regions. Your contacts will also receive any notification related to operations. Notifications can be from AWS Support, or other AWS service teams
- **Security** – When you have notifications from the AWS Security, AWS Trust and Safety, or AWS service teams. These notifications might include security issues or potential abusive or fraudulent activities on your AWS account. Notifications can be from AWS Support, or other AWS service teams concerning security related topics associated with your AWS account usage. Don't include sensitive information in the subject line or full name fields since this might be used in email communications to you.

Adding or editing security challenge questions

You can add another layer of authentication by adding security challenge questions and their answers to your AWS account. When you contact AWS Support, AWS uses this information to help authenticate you as the owner of your account.

To add or edit security challenge questions

3. Change the values in any of the available fields. You can select any of the provided questions, and then enter the appropriate answer.
4. Enter your updated information and choose Update.

Enabling and disabling AWS Regions

Before this feature was available, AWS originally enabled all new Regions by default, which allowed your users to create resources in any Region. Now when AWS adds a Region, the new Region is disabled by default. You can enable a Region so that your users can create resources in that new Region.

Note the following about enabling and disabling Regions:

You can use IAM permissions to control access to Regions

IAM includes permissions that you can use to control which users can enable, disable, and list Regions.

For more information, see the following topics:

- AWS Billing actions (p. 170)
• **AWS:** Allows enabling and disabling AWS Regions in the IAM User Guide
• Managing AWS Regions in the Amazon Web Services General Reference

Enabling a Region is free

There's no charge to enable a Region. You're only charged for resources that you create in the Region.

Disabling a Region removes access to resources in that Region

If you disable a Region that still includes AWS resources, such as Amazon Elastic Compute Cloud (Amazon EC2) instances, you can't access the resources in that Region. For example, you can't use the AWS Management Console or any programmatic method to view or change the configuration of any EC2 instances in that Region.

Charges continue if you disable a Region

If you disable a Region that still includes AWS resources, charges for those resources (if any) continue to accrue at the standard rate.

For example, if you disable a Region that contains Amazon EC2 instances, you still have to pay the charges for those instances even though the instances are inaccessible.

Disabling a Region isn't always immediately visible

If you disable a Region, the change takes time to become visible in all possible endpoints. Disabling a Region can take between a few seconds to minutes to take effect.

Existing Regions are enabled by default

The original Regions (the Regions that existed before we added the ability to enable and disable Regions) are all enabled by default and can't be disabled.

Enabling a Region takes a few minutes for most accounts

Enabling a Region generally takes effect in minutes. However, it can take longer for some accounts. If enabling a Region takes longer than nine hours, sign in to the AWS Support Center Console and create a case with AWS Support.

Follow either procedure to enable or disable a Region:

**To enable or disable a Region**

2. To enable a Region:
   a. Under AWS Regions, select the Region, and then choose Enable.
   b. In the dialog box, choose Enable Region.
3. To disable a Region:
   a. Under AWS Regions, select the Region, and then choose Disable.
   b. In the dialog box, for Disable RegionName, enter disable, and then choose Disable Region.

Activating IAM access to the AWS Billing console

By default, IAM roles within an AWS account can't access the Billing console. This is true even if the IAM user or role has IAM policies that grant access to specific Billing features. The root user can allow IAM users and roles access to Billing console by using the Activate IAM access setting.
For more information about this feature, see About IAM Access to the AWS Billing console (p. 167).

To provide access to the Billing console

2. Under IAM user and role access to Billing information, choose Edit.
3. Select Activate IAM access.
4. Choose Update.

Manage account contract information

If this account is used to service public sector customers, enter the contract details in this section.

To manage the contract information

3. Enter your updated information and choose Update.

Updating and deleting tax registration numbers

Use the following steps to update or delete one or more tax registration numbers.

To update tax registration numbers

2. In the navigation pane, choose Tax settings.
3. Under Tax registrations, select the numbers to edit.
4. For Manage tax registration, choose Edit.
5. Enter your updated registration and choose Update.

You can remove one or more tax registration numbers.

To delete tax registration numbers

2. In the navigation pane, choose Tax settings.
3. Under Tax Registrations, select the tax registration numbers to delete.
4. For Manage tax registration, choose Delete TRN.
5. In the Delete tax registration dialog box, choose Delete.

Turning on tax setting inheritance

You can use your tax registration information with your member accounts by turning on your Tax settings inheritance. After you activate it, your tax registration information is added to your other AWS
Organizations accounts, saving you the effort of registering redundant information. Tax invoices are processed with the consistent tax information, and your usage from member accounts will consolidate to a single tax invoice.

**Notes**

- Tax inheritance settings are only available to accounts after a member account is added.
- If you turn off tax inheritance, the member accounts revert to the account's original TRN setting. If there was no TRN originally set for the account, no TRN will be assigned.

Tax registration information includes:

- Business legal name
- Tax address
- Tax registration number
- Special exemptions (does not apply for US sales tax exemptions)

**To turn on tax setting inheritance**

2. In the navigation pane, choose **Tax settings**.
3. Under **Tax registrations**, select **Enable tax settings inheritance**.
4. In the dialog box, choose **Enable**.

**Managing your US tax exemptions**

If your state is eligible, you can manage your US tax exemptions on the **Tax settings** page. The documents you upload for the exemption are reviewed by AWS Support within 24 hours.

**Note**

You must have IAM permissions to view the **Tax exemptions** tab on the **Tax settings** page in the Billing console.

For an example IAM policy, see [Allow IAM users to view US tax exemptions and create AWS Support cases](p. 194).

**To upload or add your US tax exemption**

2. In the navigation pane, choose **Tax settings**.
3. Choose **Tax exemptions**.
4. Choose all of the accounts to add the tax exemption. Choose **Manage tax exemption** and select **Add tax exemption**.
    a. If you're logged in as a linked account, you can add tax exemptions to only the linked account.
    b. If you're logged in as a payer account, you can add tax exemptions to both payer and linked accounts.
5. Specify your exemption type and jurisdiction.
6. Upload certificate documents.
7. Review your information, and choose **Submit**.
Within 24 hours, AWS Support will notify you through a support case if they need additional information, or if any of your documents weren't valid.

Once the exemption is approved, you can view it under the Tax exemption tab with an Active validity period.

You will be notified through a support case contact if your exemption was rejected.

**Closing your AWS account**

For more information about closing your AWS account, see Close your account in the AWS Account Management Reference Guide.

**Managing an account in India**

If you sign up for a new account and choose India for your contact address, your user agreement is with Amazon Web Services India Private Limited (AWS India), a local AWS seller in India. AWS India manages your billing, and your invoice total is listed in rupees instead of dollars. After you create an account with AWS India, you can't change the country in your contact information.

If you have an existing account with an India address, your account is either with AWS or AWS India, depending on when you opened the account. To learn whether your account is with AWS or AWS India, see the procedure the section called “Determining which company your account is with” (p. 17).

If you're an existing AWS customer, you can continue to use your AWS account. You also can choose to have both an AWS account and an AWS India account, though they can’t be consolidated into the same payment family. For information about managing an AWS account, see Managing an AWS account (p. 11).

If your account is with AWS India, follow the procedures in this chapter to manage your account. This chapter explains how to sign up for an AWS India account, edit information about your AWS India account, and add or edit your Permanent Account Number (PAN).

As part of the credit card verification during signup, AWS India charges your credit card 2 INR. AWS India refunds the 2 INR after verification is done. You might be redirected to your bank as part of the verification process.

**Topics**

- Determining which company your account is with (p. 17)
- Signing up for Amazon Web Services India Private Limited (p. 18)
- Managing your AWS India account (p. 19)

**Determining which company your account is with**

AWS services are provided by both AWS and AWS India. Use this procedure to determine which seller your account is with.

**To determine which company your account is with**

2. In the page footer, look at the copyright notice. If the copyright is for Amazon Web Services, then your account is with AWS. If the copyright is for Amazon Web Services India Private Limited, then your account is with AWS India.
Signing up for Amazon Web Services India Private Limited

AWS India is a local seller of AWS. To sign up for an AWS India account if your contact address is in India, use the following procedure.

**To sign up for an AWS India account**

If your contact address is in India and you want to open an account, sign up with AWS India.

1. Navigate to https://console.aws.amazon.com/, and then choose **Sign In to the Console**.
2. On the **Sign In** page, enter the email address that you want to use.
3. Under your email address, select **I am a new user**, and then choose **Sign in using our secure server**.
4. For each of the login credential fields, enter your information, and then choose **Create account**.
5. For each of the contact information fields, enter your information.

If your contact or billing address is based in India, AWS is required under applicable law to collect and validate your identity information. Confirm the name in your contact or billing information matches the name that appears on the document that you plan to use for customer verification, such as your Permanent Account Number (PAN) or your Corporate Identification Number (CIN).

For a list of accepted document types, see [Accepted India documents for customer verification (p. 20)](.).

6. After you read the customer agreement, select the terms and conditions check box, and then choose **Continue**.
7. On the **Billing information** page, enter the payment method that you want to use. You must provide your CVV as part of the verification process.
8. Under **Do you have a PAN?**, choose **Yes** if you have one, and then enter your **PAN**. If you don't have one or want to add it later, choose **No**.
9. Choose **Verify and continue**. AWS India charges your card 2 INR as part of the verification process and will refund this amount after verification is done.
10. On the **Confirm your identity** page, choose the name that you want to use for customer verification. The names from your billing and contact information will appear for selection if they’re associated with an Indian address. You must pass customer verification to access AWS services.
11. Select the primary purpose of account registration for your account creation. If your account is tied to a business, select one that best applies to your business.
12. Select the ownership type that represents the owner of the account. If you select a company, organization, or partnership, enter the name of the key managerial contact. This can be a director, head of operations, or a person responsible for operations in your business.
13. Depending on the ownership type you selected, choose an accepted India document type to use for verification and enter your information. Confirm that the name on the document type that you chose matches the name that you selected for customer verification. For more information about each document type, see [Manage customer verification (p. 20)](.).

To make changes to the name associated with your billing or contact address, you can do so after you complete account signup.

14. To give your consent to submit your information for verification, select the check box, and then choose **Continue**.

After you complete account signup, you will be notified about the customer verification result by email. You can also check the status if you sign in to your [AWS Health Dashboard](#).

15. To verify your mobile phone number, choose **Text message (SMS)** or **Voice call**.
16. Choose your country and region code, and then enter your mobile phone number.
17. Complete the security check.
18. Choose **Send SMS** or **Call Me Now**. You will receive a four-digit pin in an SMS or an automated call on your mobile phone.
19. On the **Confirm your identity** page, enter the pin that you received, and choose **Continue**.
20. On the **Select a support plan** page, choose your support plan, and then choose **Complete sign up**. After your payment method and customer information is verified, your account is activated, and you will receive an email that confirms your account is activated.

**Note**
If you completed customer verification, and you edited the name, address, or document type previously used to verify your identity, you may need to pass verification again. For more information, see **Editing your customer verification information** (p. 19).

### Managing your AWS India account

Use the **Account Settings** and **Tax Settings** pages of the Billing and Cost Management console to perform the following tasks:

**Topics**
- **Editing your customer verification information** (p. 19)
- **Manage customer verification** (p. 20)
- **Editing your user name, password, or email address** (p. 21)
- **Editing your contact information** (p. 21)
- **Add, update, or removing alternate contacts** (p. 22)
- **Adding or editing a Permanent Account Number** (p. 22)
- **Removing a Permanent Account Number** (p. 22)
- **Editing multiple Permanent Account Numbers** (p. 22)
- **Editing multiple Goods and Services Tax numbers** (p. 23)
- **Viewing a tax invoice** (p. 23)

### Editing your customer verification information

This process is only applicable if you provided all of the following information during your AWS account sign up:

- An India-based billing or contact address
- The primary purpose of account registration
- The ownership type
- The selected name, document type, and document information

You can edit your customer verification information to do the following:

- Change the selected name, document type, or document information to use for verification.
- Update the customer verification information based on recent edits to your billing or contact information.

If you edit the information you previously used for customer verification, such as the name from your billing or contact information, you may need to update and resubmit your customer verification information. You can check your customer verification status on the **Customer verification** page.
To edit your customer verification information

2. On the navigation bar in the upper-right corner, choose your account name (or alias), and choose Account.
3. Under Other settings, choose Customer verification.
   - If the status is Verification required or Verification failed, edit your verification information and submit it again for verification.
4. Choose Edit and then update the information that you want to change.
   - If you choose a different name or document type to use for customer verification, or update your document information, saving the information will restart customer verification.
5. Choose Submit.

Manage customer verification

AWS is required under applicable law to collect and validate your identity information. You must pass a customer verification process to access AWS services. Your identity must be verified using the name from the India billing or contact address that you provided. During verification, AWS will check if the document number is valid and if the name provided by you matches the name associated with the document.

If you need to update your billing name and address, see Managing your AWS payment preferences (p. 63). To update your contact name and address, see Editing your contact information (p. 21).

Accepted India documents for customer verification

The following document types issued by the Indian government are accepted for customer verification.

Note
The following links below are subject to change by the Indian government.

Permanent Account Number (PAN)

This is a unique alphanumeric identifier issued by the Income Tax Department of India to individuals, companies, and entities. A PAN consists of ten characters, including letters and numbers, in the format AAAAA1111A. To check the validity of your PAN, see the official website of the Income Tax Department.

Voter ID/Electors Photo Identity Card (EPIC) number

This is a unique identification number issued by Election Commission of India to eligible voters in India. This ID consists of ten characters, including letters and numbers. To check the validity of your voter ID, see the official website of the Election Commission of India.

Driving license

The India driving license is issued by the Union of India through the Regional Transport Offices (RTOs) or Regional Transport Authorities (RTAs). A driving license number consists of 12-16 characters, including letters, numbers, spaces, and hyphens.

Note
To use a driving license for verification, you must provide your date of birth. Your date of birth will be used for verification, but won't be stored. To check the validity of your driving license, see the Parivahan Sewa website of the Ministry of Road Transport and Highways.
Passport file number

This is a unique alphanumeric identifier associated with an individual's passport issued by the Passport Seva Kendra (PSK). This is different from the passport number. The passport file number can be found in one of the last pages of your India passport. To use a passport file number for verification, you must provide your date of birth. Your date of birth will be used for verification, but won't be stored. A passport file number consists of 15 characters, including letters and numbers. Older versions of the passport file number aren't accepted.

Note
For customer verification, only passports issued in India are accepted. If your passport was issued by an India diplomatic mission in another country, use a different India document for customer verification.

Corporate Identification Number (CIN)

This is a unique alphanumeric identifier assigned to companies registered under the Companies Act, 2013, or earlier under the Companies Act, 1956. The CIN is used to uniquely identify and track companies registered in India. The Ministry of Corporate Affairs (MCA) issues this number and it consists of 21 characters, including letters and numbers. To check the validity of your CIN, see the MCA portal.

Different India document types are accepted for personal and business accounts:

- For personal accounts – Use PAN, voter ID/EPIC number, driving license, or passport file number
- For business accounts – Use PAN or CIN

Editing your user name, password, or email address

You can change the name, password, and email address associated with your AWS India account.

To edit your user name, password, or email address

2. On the navigation bar in the upper-right corner, choose your account name (or alias), and choose Account.
3. Next to Account Settings, choose Edit.
4. Next to the field that you want to update, choose Edit.
5. After you have entered your changes, choose Save changes.
6. After you have made your changes, choose Done.

Editing your contact information

You can change the contact information associated with your AWS India account, including your mailing address, telephone number, and website address. You cannot change your country.

To edit your contact information

2. On the navigation bar in the upper-right corner, choose your account name (or alias), and choose Account.
3. Under Contact Information, choose Edit.
4. For the fields that you want to change, type your updated information, and then choose Update.
**Note**
You can choose to add an email address for billing in the **Alternate Contacts** section to have AWS India send a copy of billing-related emails to that email address. For example, AWS India sends a copy of your monthly bill to your Billing contact address.

**Add, update, or removing alternate contacts**

You can add alternate contacts to your account. Alternate contacts enable AWS India to contact another person about issues with your account. This is even the case if you're unavailable.

**To add, update, or remove alternate contacts**

2. On the navigation bar in the upper-right corner, choose your account name (or alias), and choose **Account**.
3. Scroll down to the **Alternate Contacts** section, and then choose **Edit**.
4. For the fields that you want to change, type your updated information, and then choose **Update**.

**Adding or editing a Permanent Account Number**

You can add your Permanent Account Number (PAN) to your account and edit it.

**To add or edit a PAN**

2. In the navigation pane, choose **Tax Settings**.
3. On the **Tax Settings** navigation bar, choose **Edit**.
4. For **Permanent Account Number (PAN)**, enter your PAN, and then choose **Update**.

**Removing a Permanent Account Number**

You can remove your Permanent Account Number (PAN) in your account.

**To remove a PAN**

2. In the navigation pane, choose **Tax Settings**.
3. Choose the **Account ID** you want to remove the PAN from.
4. Choose **manage tax registration**.
5. Choose **Delete TRN**.

**Editing multiple Permanent Account Numbers**

You can edit multiple Permanent Account Numbers (PANs) in your account.

**To edit multiple PAN numbers**

2. In the navigation pane, choose **Tax Settings**.
3. Under **Manage Tax Registration Numbers**, select the PAN numbers that you want to edit.
4. For **Manage Tax Registration**, choose **Edit**.
5. Update the fields that you want to change, and then choose **Update**.

### Editing multiple Goods and Services Tax numbers

You can edit multiple Goods and Services Tax numbers (GSTs) in your account.

**To edit multiple GST numbers**

2. On the navigation pane, choose **Tax Settings**.
3. Under **Manage Tax Registration Numbers**, select the GST numbers that you want to edit or choose **Edit all**.
4. For **Manage Tax Registration**, choose **Edit**.
5. Update the fields that you want to change and choose **Update**.

### Viewing a tax invoice

You can view your tax invoices in the console.

**To view a tax invoice**

2. On the navigation pane, choose **Bills**.
3. Scroll down and choose the **Invoices** tab.
4. On the **Tax invoices** section, choose an invoice link that is mentioned under **Document ID**.

**Note**
The **Tax invoices** section only appears if there are tax invoices available.
Using the AWS Billing console dashboard

You can use the dashboard page of the AWS Billing console to gain a general view of your AWS spending. You can also use it to identify your highest cost service or Region and view trends in your spending over the past few months. You can use the dashboard page to see various breakdowns of your AWS usage. This is especially useful if you're a Free Tier user. To view more details about your AWS costs and invoices, choose Billing details in the left navigation pane. You can customize your dashboard layout at any time by choosing the gear icon at the top of the page to match your use case.

Viewing your AWS costs in the AWS Billing console dashboard doesn't require turning on Cost Explorer. To turn on Cost Explorer to access additional views of your cost and usage data, see Enabling AWS Cost Explorer.

To open the AWS Billing console and dashboard

- Sign in to the AWS Management Console and open the AWS Billing console at https://console.aws.amazon.com/billing/.

By default, the console shows the AWS Billing Dashboard page.

Understanding your dashboard page

Your AWS Billing console dashboard contains the following sections. To create your preferred layout, drag and drop sections of the Dashboard page. To customize the visible sections and layout, choose the gear icon at the top of the page. These preferences are stored for ongoing visits to the Dashboard page. To temporarily remove sections from your view, choose the x icon for each section. To make all sections visible, choose refresh at the top of the page.

AWS summary

This section is an overview of your AWS costs across all accounts, AWS Regions, service providers, and services, and other KPIs. Total compared to prior period displays your total AWS costs for the most recent closed month. It also provides a comparison to your total forecasted costs for the current month. Choose the gear icon on the card to decide which KPIs you want to display.

Highest cost and usage details

This section shows your top service, account, or AWS Region by estimated month-to-date (MTD) spend. To choose which to view, choose the gear icon on the top right.

Cost trend by top five services

In this section, you can see the cost trend for your top five services for the most recent three to six closed billing periods.

You can choose between chart types and time periods on the top of the section. You can adjust additional preferences using the gear icon.

The columns provide the following information:
- **Average**: The average cost over the trailing three months.
• **Total**: The total for the most recent closed month.
• **Trend**: Compares the **Total** column with the **Average** column.

**Account cost trend**

This section shows the cost trend for your account for the most recent three to six closed billing periods. If you’re a management account of AWS Organizations, the **cost trend by top five section** shows your top five AWS accounts for the most recent three to six closed billing periods. If invoices weren’t already issued, the data isn’t visible in this section.

You can choose between chart types and time periods on the top of the section. Adjust additional preferences using the gear icon.

The columns provide the following information:

• **Average**: The average cost over the trailing three months.
• **Total**: The total for the most recent closed month.
• **Trend**: Compares the **Total** column with the **Average** column.

**Understanding your dashboard (old console)**

On the dashboard, you can view the following graphs:

• **Spend Summary**
• **Month-to-Date Spend by Service**
• **Month-to-Date Top Services by Spend**

**Spend Summary**

The **Spend Summary** graph shows you how much you spent last month, the estimated costs of your AWS usage for the month-to-date, and a forecast for how much you are likely to spend this month. The forecast is an estimate that’s based on your past AWS costs. Therefore, your actual monthly costs might not match the forecast.

**Month-to-Date Spend by Service**

The **Month-to-Date Spend by Service** graph shows the top services that you use most and the proportion of your costs that service contributed to. The **Month-to-Date Spend by Service** graph doesn’t include forecasting.

**Month-to-Date Top Services by Spend**

The **Month-to-Date Top Services by Spend** graph shows the services that you use most, along with the costs incurred for the month to date. The **Month-to-Date Top Services by Spend** graph doesn’t include forecasting.

**Note**

The Billing and Cost Management console has a refresh time of approximately 24 hours to reflect your billing data.
Monthly billing checklist

AWS uses information that you provide in the AWS Billing console to prepare and issue your invoices with proper header information, such as your preferred payment currency, tax settings, business legal name and address.

If this information is missing or inaccurate, AWS might issue inaccurate invoices that you can't use or process.

Follow this 10-minute checklist before the end of the monthly billing period to review your invoice and ensure that your information is up-to-date in your AWS account.

Contents
- Check purchase order balance and expiration (p. 26)
- Review tax settings (p. 26)
- Enable tax setting inheritance (p. 27)
- Update billing contact information (p. 27)
- Review payment currency (p. 28)

Check purchase order balance and expiration

As part of the procure-to-pay process, you can use purchase orders to procure AWS services and approve invoices for payment. To avoid issues with billing and payment, verify that your purchase orders aren't expired or out-of-balance.

To check purchase order balance and expiration

1. Navigate to the Purchase orders page in the AWS Billing console. The purchase order dashboard shows the state of your purchase orders.
2. Choose a purchase order to see the Purchase order details page.
3. Review the purchase order Balance and Expiration fields.

Tip
- You can set up email notifications so that you can proactively take action on expiring or out-of-balance purchase orders. For more information, see Enabling purchase order notifications (p. 75).
- To add a purchase order to use in your invoices, see Adding a purchase order (p. 70).

Review tax settings

To determine your account's location for tax purposes, AWS uses the tax registration number (TRN) and the business legal address associated with your account. A TRN is also known as a value-added tax (VAT) number, VAT ID, VAT registration number, or business registration number.

To review tax settings

2. Under the **Tax registrations** tab, select the account IDs to edit.
3. Under **Manage tax registration**, choose **Edit**.
4. Enter your updated information and then choose **Update**.

For more information, see [Updating and deleting tax registration numbers (p. 15)](#).

## Enable tax setting inheritance

The management account and member accounts that are part of AWS Organizations can have different TRNs or the same TRN. Unless your organization needs to use different TRNs for member accounts, we recommend that you enable tax settings inheritance.

After you enable this setting from the management account, your tax registration information is added to your member accounts in your organization. This saves you time so that you don't need to enter this information for individual accounts. Tax invoices are processed with consistent tax information, and your usage from member accounts will consolidate to a single tax invoice.

**To enable tax settings inheritance**

1. Navigate to the **Tax settings** page in the Billing console.
2. Under **Tax registrations**, select **Enable tax settings inheritance**.
3. In the dialog box, choose **Enable**.

For information about how to manage documents required for US tax exemptions, see [Managing your US tax exemptions (p. 16)](#).

## Update billing contact information

Verify that your billing contact information is correct. AWS uses these contacts to contact you about any billing or payment related communications. You can add additional billing contacts in two ways:

- The **Payment preferences** page
- The **Accounts** page

**To add billing contacts from the Payments preference page**

1. Navigate to the **Payment preferences** page in the Billing console.
2. In the **Default payment preferences** section, review the **Billing contact email** field. AWS uses this contact for any billing or payment related communications.
3. Choose **Edit**.
4. In the **Billing contact email - optional** field, enter the email addresses that you want AWS to send billing related email notifications, payment reminders and payment support notifications to. You can add up to 15 email addresses.
5. Choose **Save changes**.

You can add alternate contacts so that AWS has an alternate email address to contact about issues with your account, even if the AWS account root user contact is unavailable. For the Billing alternate contact, you can specify the email address to receive the invoice. Your alternate contact will be authorized to communicate with AWS for billing, invoice, and payment issues.
The alternate contact doesn't have to be a specific person. For example, you can add an email distribution list if you have a team that manages billing, operations, and security related issues.

**To update alternate contact information from the Accounts page**

1. Navigate to the Accounts page in the Billing console and scroll down to the Alternate contacts section.
2. For the Billing field, review the contact information and confirm the email address where you want your invoices delivered.

For more information about how to use alternate contacts, see *Adding or updating alternate contacts* (p. 12).

**Review payment currency**

The payment currency is the currency that your default payment method will be charged in. This is also the currency displayed on your invoice under your default service provider. Some organizations can't process invoices that are issued in the wrong currency, so it's important to ensure that your payment currency is accurate.

**To review your payment currency**

1. Navigate to Payment preferences in the Billing console.
2. In the Default payment preferences section, choose Edit.
3. In the Payment currency section, ensure that the Default payment currency is correct.

For more information about payment methods, see *Managing credit card and ACH payment methods* (p. 40).
Viewing your bill

For questions about your AWS bills or to appeal your charges, contact AWS Support to address your inquiries immediately. To get help, see Getting help with AWS Billing (p. 6). To understand your bills page contents, see Using the Bills page to understand your monthly charges and invoice (p. 30).

You receive AWS invoices monthly for usage charges and recurring fees. For one-time fees, such as fees for purchasing an All Upfront Reserved Instance, you’re charged immediately.

At any time, you can view estimated charges for the current month and final charges for previous months. This topic describes how to view your monthly bill and past bills, how to receive and read billing reports, and how to download invoices. To make a payment, see Making payments, checking unapplied funds, and viewing your payment history (p. 38).

Topics
- Viewing your monthly charges (p. 29)
- Using the Bills page to understand your monthly charges and invoice (p. 30)
- Downloading a PDF of your invoice (p. 31)
- Getting an invoice emailed to you (p. 32)
- Downloading a monthly report (p. 33)

Viewing your monthly charges

Follow this procedure to view your monthly charges from the Billing console.

To view your monthly charges

2. In the navigation pane, choose Bills.
3. Choose a Billing period (for example, August 2023).
4. View your AWS bill summary.

Viewing your monthly charges (old console)

To view your monthly charges

2. In the navigation pane, choose Bills.
3. For Billing period, choose a month.

The Summary section displays a summary and details of your charges for that month.
Note
The summary isn't an invoice until the month's activity closes and AWS calculates the final charges.

If you use the consolidated billing feature in AWS Organizations, the Bills page lists totals for all accounts on the Charges by account tab. Choose the account ID to see the activity for each account in the organization. For more information about consolidated billing, see Consolidated billing for AWS Organizations (p. 146).

Using the Bills page to understand your monthly charges and invoice

At the end of a monthly billing period, or when you incur a one-time fee, AWS issues an invoice as a PDF file. If you're paying by credit card, AWS also charges the credit card that you have on file at this time.

To download invoices and view your monthly charge details, you can use the Bills page in the AWS Billing console.

Note
IAM users need explicit permission to access some of the pages in the Billing and Cost Management console. For more information, see Overview of managing access permissions (p. 166).

Bills page

You can use the Bills page to see your monthly chargeable costs, along with details of your AWS services and purchases made through AWS Marketplace. Invoices are generated when a monthly billing period closes (the billing status appears as Issued), or when subscriptions or one-time purchases are made. For monthly billing periods that haven't closed (the billing status appears as Pending), this page shows the most recent estimated charges based on your AWS services metered to date.

If you're signed in as the management account of your AWS Organizations, you can see the consolidated charges for your member accounts. You can use the Charges by account to also view account-level details.

Say you're an AWS Billing Conductor user and are signed in as a management account. You can turn on a pro forma view by choosing the gear icon on the top of the page. Choose the month and year to specify your billing period.

To customize the visible sections, choose the gear icon at the top of the page. These preferences are saved for ongoing visits to the Bills page.

AWS bill summary

The AWS bill summary section shows an overview of your monthly charges. The information shows your invoice totals for the closed billing periods (the billing status appears as Issued).

Billing periods that haven't closed have the Pending billing status. The totals show the most recent estimated charges based on your AWS services metered to date. Totals are shown in US dollars (USD). If your invoices are issued in another currency, the total in the other currency is also shown.

Payment information

The Payment information section lists invoices for the selected billing period that AWS received payments for. You can find the service provider, charge types, document types, invoice IDs, payment status, the date AWS received the payments, and the total amount in USD. If your invoices are
issued in another currency, the total in the other currency is also shown. For more information, see Managing Your Payments (p. 38).

Highest cost by service provider

The Highest cost by service provider section identifies your account’s service and AWS Region with the highest cost for the billing period, and shows the month-over-month trends for each. For pending billing periods, the month-over-month trend compares the month-to-date spend in the current billing period with the equivalent portion of the previous billing period.

Charges by service

The Charges by service tab shows your spend in each AWS service. You can sort by service name or amount in USD, and filter by service name and Region. Choose the + icon next to each service to see the charges for that service by Region. Choose a Region to see charge details.

Charges by account

If you use AWS Organizations and signed in to your management account, the Charges by account tab shows the spend of each of your member accounts. You can sort by account ID, account name, or amount in USD, and filter by account ID or account name. Choose the + icon next to each account to see charges for that account by service provider. Choose the + icon next to each line item to see charges by service and Region. Choose a Region to see charge details.

Invoices

The Invoices tab lists the invoices for each service provider that you transacted with during the selected billing period. This includes details such as charge type, invoice date, and total in USD. If your invoices are issued in another currency, the total in the other currency is also shown. To view and download a PDF format for individual invoices, choose the Invoice ID.

Savings

The Savings tab summarizes your savings during the billing period as the outcome of Savings Plans, credits, or other discount programs. These savings are also reflected in the Charges by service, Charges by account, and Invoices tabs. Choose each savings type to see the details by service.

Taxes by service

The Taxes by service tab shows the pre-tax, tax, and post-tax charges for each service that was charged taxes. You can sort by service name, post-tax charge, pre-tax charge, or tax in USD, and filter by service name.

Tax Invoices and Supplemental Documents

The Tax Invoices and Supplemental Documents section lists tax invoices and other supplemental documents for the selected billing period. Not all service providers issue tax invoices. The Invoice ID column shows the associated commercial invoice associated with that tax invoice. To view and download a PDF format for individual invoices, choose the Document ID.

Downloading a PDF of your invoice

Follow this procedure to download a PDF of your monthly invoice.

To download a copy of your charges as a PDF document

2. On the Bills page, select a month for the Billing period.
3. Under the AWS bill summary section, confirm that the Bill status appears as Issued.
4. Choose the Invoices tab.
5. Choose the **Invoice ID** of the document that you want to download.

6. (For service providers other than AWS EMEA SARL) To download a copy of a particular tax invoice, in the **Tax Invoices and Supplemental Documents** section, choose the **Document ID**.

7. (For AWS EMEA SARL) To download a copy of a particular tax invoice, in the **AWS EMEA SARL charges** section, choose the **Document ID**.

### Downloading a copy of your charges as a PDF (old console)

**To download a copy of your charges as a PDF document**

2. On the **Bills** page, select a month from the **Date** list that all activity is closed for.
3. Under **Total**, choose **Amazon Web Services, Inc. - Service Charges**.
4. Choose **Invoice <invoiceID>**.
5. (For entities other than AWS EMEA SARL) To download a copy of a particular tax invoice, choose the **Invoice <invoiceID>** in the **Tax Invoices** section.
6. (For AWS EMEA SARL) To download a copy of a particular tax invoice, choose the **Invoice <invoiceID>** in the **Amazon Web Services EMEA SARL – Service Charges** section.

### Getting an invoice emailed to you

Follow this procedure if you want AWS to send you a PDF copy of your monthly or daily invoice to the email address that's associated with your AWS account.

**Tip**
To view and download your monthly invoices instead, see [Downloading a PDF of your invoice (p. 31)](#).

2. On the navigation pane, choose **Billing preferences**.
3. Under **Invoice delivery preferences**, choose **Edit**.
4. Select **PDF invoices delivered by email**.
5. Choose **Update**.

Depending on the purchase, AWS sends monthly or daily invoices to the following contacts:

- The AWS account root user
- The billing contacts on the **Payment preferences** page
- The alternate billing contacts on the **Account** page

### Additional invoice email

In addition to the PDF invoice email, AWS sends monthly or daily email with your invoice details to the **contact list (p. 32)** in the previous section.

**Note**
If you specify a billing contact on the **Payment preferences** page, the root user won't receive the PDF invoice or the additional invoice by email.
Related information

For more information, see the following topics:

- To edit the root user email address, see Editing your account name, AWS account root user password, and AWS account root user email address (p. 12).
- To update the billing contacts on the Payment preferences page, see Adding additional billing contact email addresses (p. 64).
- To update the alternate billing contact, see Adding or updating alternate contacts (p. 12).

Downloading a monthly report

You can download CSV files for any future billing after you turn on monthly reports. This feature delivers your reports to an Amazon S3 bucket.

**Tip**
We recommend that you use the AWS Cost and Usage Report for the most granular set of cost and usage data available. For more information, see What are AWS Cost and Usage Reports? in the AWS Cost and Usage Reports User Guide.

To download CSV files for a monthly report

2. On the navigation pane, choose Billing preferences.
3. Under Detailed billing reports (legacy), choose Edit, and then select Legacy report delivery to S3.
4. Choose Configure an S3 bucket to activate to specify where your reports are delivered.
5. In the Configure S3 Bucket dialog box, choose one of the following options:
   - To use an existing S3 bucket, choose Use an existing S3 bucket, and then select the S3 bucket.
   - To create a new S3 bucket, choose Create a new S3 bucket, and then for S3 bucket name, enter the name, and then choose the Region.
6. Choose Next.
7. Verify the default IAM policy and then select I have confirmed that this policy is correct.
8. Choose Save.
9. On the Bills page, choose Download all to CSV.
Using the Billing preferences page

You can use the **AWS Billing preferences** page to manage your invoice delivery, alerts, credit sharing, Reserved Instances (RI) and Savings Plans discount sharing, and detailed billing (legacy) reports. For some sections, only the payer account can update them.

You can assign user permissions to view the **Billing preferences** page. For more information, see [Using fine-grained AWS Billing actions](#).

The Billing preferences page contains the following sections.

### Contents
- Invoice delivery preferences (p. 34)
- Alert preferences (p. 34)
- Credit sharing preferences (p. 35)
- Reserved Instances and Savings Plans discount sharing preferences (p. 36)
- Detailed billing reports (legacy) (p. 36)

### Invoice delivery preferences

You can choose to receive a PDF copy of your monthly invoice by email. The monthly invoices are sent to the emails registered as the AWS account root user and the alternate billing contact. For information about updating these email addresses, see [Managing an AWS account](#).

**To opt in or out of receiving monthly PDF invoices by email**

2. In the navigation pane, choose **Billing preferences**.
3. In the Invoice delivery preferences section, choose **Edit**.
4. Select or clear **PDF invoices delivery by email**.
5. Choose **Update**.

### Alert preferences

You can receive email alerts when your AWS service usage is approaching or has exceeded the AWS Free Tier usage limits.

**To opt in or out of receiving AWS Free Tier usage alerts**

2. In the navigation pane, choose **Billing preferences**.
3. In the Alert preferences section, choose **Edit**.
4. Select or clear **Receive AWS Free Tier usage alerts**.
5. (Optional) In the **Additional email address to receive alerts**, enter any email addresses that aren't already registered as a root user or alternate billing contact.

6. Choose **Update**.

You can also use Amazon CloudWatch billing alerts to receive email notifications when your charges reach a specified threshold.

**To receive CloudWatch billing alerts**

2. In the navigation pane, choose **Billing preferences**.
3. In the **Alert preferences** section, choose **Edit**.
4. Select **Receive CloudWatch billing alerts**.
   
   **Important**
   This preference can't be deactivated at a later time.

5. Choose **Update**.

To manage your CloudWatch billing alerts, see your [CloudWatch dashboard](https://console.aws.amazon.com) or view your [AWS Budgets](https://console.aws.amazon.com/budgets/). For more information, see the [Create a billing alarm to monitor your estimated AWS charges](https://docs.aws.amazon.com/CloudWatch/latest/monitoring/alarm-create.html) in the [Amazon CloudWatch User Guide](https://docs.aws.amazon.com/CloudWatch/latest/monitoring/).

---

## Credit sharing preferences

You can use this section to activate sharing credits across member accounts in your billing family. You can select specific accounts or enable sharing for all accounts.

**Note**
This section is only available for the management account (payer account) as part of AWS Organizations.

**To manage credit sharing for member accounts**

2. In the navigation pane, choose **Billing preferences**.
3. In the **Credit sharing preferences** section, choose **Edit**.
4. To activate or deactivate credit sharing for specific accounts, select them from the table and, then choose **Activate** or **Deactivate**.
5. To activate or deactivate credit sharing for all accounts, choose **Actions**, and then choose **Activate All** or **Deactivate All**.
6. Choose **Update**.

**Tip**

- To activate credit sharing for new accounts that join your organization, select **Default sharing for newly created member accounts**.
- To download a history of your credit sharing preferences, choose **Download preference history (CSV)**.

For more information about AWS credits, see [AWS credits (p. 150)](https://docs.aws.amazon.com/aws-cost-management/latest/brguide/aws-credits.html).
Reserved Instances and Savings Plans discount sharing preferences

You can use this section to activate sharing Reserved Instances and Savings Plan discounts across accounts in your billing family. You can select specific accounts or enable sharing for all accounts.

**Note**
This section is only available for the management account (payer account) as part of AWS Organizations.

**To manage Reserved Instances and Savings Plans discount sharing for member accounts**

2. In the navigation pane, choose **Billing preferences**.
3. In the **Reserved Instances and Savings Plans discount sharing preference** section, choose **Edit**.
4. To activate or deactivate discount sharing for specific accounts, select them from the table, and then choose **Activate** or **Deactivate**.
5. To activate or deactivate discount sharing for all accounts, choose **Actions**, and then choose **Activate All** or **Deactivate All**.
6. Choose **Update**.

**Tip**
- To activate credit sharing for new accounts that join your organization, select **Default sharing for newly created member accounts**.
- To download a history of your credit sharing preferences, choose **Download preference history (CSV)**.

Detailed billing reports (legacy)

You can receive legacy billing reports that are offered outside of the AWS Cost and Usage Reports console page. However, we strongly recommend that you use AWS Cost and Usage Reports instead because it provides the most comprehensive billing information. Also, these legacy reporting methods will not be supported at a later date.

For more information about detailed billing reports, see [Detailed Billing Reports](https://aws.amazon.com/documentation/cost-management/user-guide/) in the [AWS Cost and Usage Reports User Guide](https://aws.amazon.com/documentation/cost-management/user-guide/).

For more information about transferring your reports to AWS Cost and Usage Reports, see [Migrating from Detailed Billing Reports to AWS Cost and Usage Reports](https://aws.amazon.com/documentation/cost-management/user-guide/migrate-detailed-billing-reports/).

**Notes**
- This section is only visible if you use AWS Organizations.
- To download a CSV from the **Bills** page, first activate monthly reports.

**To edit your detailed billing reports (legacy) settings**

2. In the navigation pane, choose **Billing preferences**.
3. In the **Detailed billing reports (legacy)** section, choose **Edit**.
4. To set the Amazon S3 bucket for report delivery, select **Legacy report delivery to Amazon S3** and **Configure**.

5. In the **Configure Amazon S3 Bucket** section, select an existing Amazon S3 bucket to receive the AWS Cost and Usage Reports, or create a new bucket.

6. Choose **Update**.

7. To configure the granularity of the reports to show your AWS usage, select the reports to activate.

8. In the **Report activation** section, choose **Activate**.
Managing your payments

To open an AWS account, you must have a valid payment method on file. Use the procedures in this chapter to add, update, or remove payment methods and to make payments.

You can use the Payment preferences page of the AWS Billing console to manage your AWS payment methods.

Note
IAM users need explicit permission to access some of the pages in the Billing console. For more information, see Overview of managing access permissions (p. 166).

For more information about payments or payment methods, see Getting help with AWS Billing (p. 6).

Topics
- Making payments, checking unapplied funds, and viewing your payment history (p. 38)
- Managing credit card and ACH payment methods (p. 40)
- Managing your Advance Pay (p. 43)
- Managing your AWS payments in CNY (p. 45)
- Managing your PIX payment method in Brazil (p. 48)
- Managing your payments in India (p. 49)
- Managing your payments in AWS Europe (p. 51)
- Managing your payment profiles (p. 59)
- Managing your AWS payment preferences (p. 63)

Making payments, checking unapplied funds, and viewing your payment history

You can use the Payments page of the AWS Billing and Cost Management console to perform the following tasks for all payment types:

- Make a payment
- View remaining invoices
- View unapplied funds
- View payment history

Make a payment

AWS charges your default payment method automatically at the beginning of each month. If that charge doesn't process successfully, you can use the console to update your payment method and make a payment.

Note
If you pay by ACH direct debit, AWS provides you with your invoice and initiates the charge to your payment method within 10 days of the start of the month. It can take 3–5 days for your payment to succeed. For more information, see Manage ACH direct debit payment methods (p. 41).

Before making a payment, ensure that the payment method that you want to be automatically charged in the future is set as your default payment method. If you're using a credit card, confirm that your
To make a payment

2. In the navigation pane, choose Payments.
   
   The Payments due table lists all outstanding invoices. If there are no invoices that are listed, you don't need to do anything at this time.
3. If there are outstanding invoices, select the invoice that you want to pay in the Payments due table, and then choose Complete payment.
4. On the Complete a payment page, your default payment method is selected if it's eligible for you to use to pay the invoice. If you want to use a different payment method or choose an eligible payment method, choose Change.
5. Confirm that the summary matches what you want to pay, and choose Verify and pay.

After your bank processes your payment, you're redirected to the Payments page.

Suppose that you pay by ACH direct debit, and you receive an email message from AWS saying that AWS can't charge your bank account and will try again. Then, work with your bank to understand what went wrong.

If you receive an email saying that AWS failed the last attempt to charge your bank account, select the invoice to pay in the Payments due table. Then, choose Complete payment to pay the invoice. If you have questions about issues with charging your bank account or paying an overdue balance, create a case in the Support Center.

If you pay by electronic funds transfer and your account payment is overdue, create a case in the Support Center.

View remaining invoices, unapplied funds, and payment history

You can search and filter the Payments due, Unapplied funds, and Payment history tables described in the following procedures. Choose the gear icon to change the default columns and customize other table settings. Download items individually by choosing the appropriate ID, or choose Download, and then Download CSV to download a CSV file of the table for reporting purposes.

To view remaining invoice payments

2. In the navigation pane, choose Payments.
3. Choose the Payments due tab to view the Payments due table.
   
   The Payments due table lists all your remaining invoice payments. The table shows your total invoice amount and remaining balance.
   
   The table includes the following statuses:
   
   - Due – Outstanding invoices with an approaching due date.
   - Past due – Outstanding invoices with a payment that wasn't made by the due date.
   - Scheduled – Invoices with an upcoming scheduled payment.
   - Processing – Invoices that a payment is currently being scheduled for.
To view unapplied funds
2. In the navigation pane, choose Payments.
3. Choose the Unapplied funds tab to view the Unapplied funds table.
   - The Unapplied funds table lists all unapplied credit memos. The table shows your total invoice amount and remaining balance.
   - If the status is Unapplied, there are available credit memos to be applied to an invoice.
   - If the status is Partially applied, there are credit memos where some amounts have been applied to a previous invoice.

To view payment history
2. In the navigation pane, choose Payments.
3. Choose the Transactions tab to view the Transactions table.
   - The Transactions table lists all completed transactions with AWS.

Managing credit card and ACH payment methods

You can use the Payment preferences page of the AWS Billing console to manage your credit cards and ACH direct debit payment methods.

Topics
- Add a credit card (p. 40)
- Update a credit card (p. 41)
- Confirm credit card information (p. 41)
- Delete a credit card (p. 41)
- Manage ACH direct debit payment methods (p. 41)

Note
If you’re paying with a Chinese yuan credit card, see Use a Chinese yuan credit card (p. 47).

Add a credit card

You can use the Billing console to add a credit card to your account.

To add a credit card to your AWS account
2. In the navigation pane, choose Payment preferences.
3. Choose Add payment method.
4. Enter the credit card information.
5. (Optional) For Set as default payment method, select whether you want this credit card to be your default payment method.
6. Enter your card billing address.
7. Verify your information and then choose Add payment method.

**Update a credit card**

You can update the expiration date, name, address, and phone number that’s associated with your credit card.

**Note**

When you add or update your credit card, AWS charges any unpaid invoices from the previous month to the new card.

**To update a credit card**

2. In the navigation pane, choose Payment preferences. Payment methods associated with your AWS account appear in the Payment methods section.
3. Select the credit card to edit and then choose Edit.
4. Update the information that you want to change.
5. Verify your changes and then choose Save changes.

**Confirm credit card information**

To make a payment, you must have a valid, unexpired credit card on file.

**To confirm that your credit card is up-to-date**

2. In the navigation pane, choose Payment preferences.
3. Ensure that your credit card is valid. If your card expired, update your current card or add a new one.

**Delete a credit card**

Before you delete your credit card, ensure that your AWS account has another valid payment method set as the default.

**To delete a credit card**

2. In the navigation pane, choose Payment preferences. Payment methods associated with your AWS account appear in the Payment method section.
3. Select the payment method and then choose Delete.
4. In the Delete payment method? dialog box, choose Delete.

**Manage ACH direct debit payment methods**

If you meet the eligibility requirements, add a US bank account as an ACH direct debit payment method to your payment methods.

To be eligible, you must be an Amazon Web Services customer and also meet the following requirements:
• You created your AWS account at least 60 days ago
• You paid at least one invoice (in full) in the previous 12 months
• You paid at least $100 (cumulatively) over the previous 12 months
• You set USD as the preferred currency

If you pay by ACH direct debit, AWS provides you with your invoice and initiates the charge to your payment method within 10 days of the start of the month. It can take up to 20 days for the payment to complete successfully, even if the payment shows as Succeeded on the AWS Billing console.

You can use AWS Billing console to add or update a direct debit account.

Contents
• Add a direct debit account (p. 42)
• Update direct debit account (p. 43)

Add a direct debit account

You can use the AWS Billing console to add a direct debit account to your AWS payment methods. You can use any personal or business bank account, provided that the account is located at a branch in the US.

Before you add an ACH direct debit account, have the following information ready:
• A US bank account number
• A US bank account routing number
• The address that’s associated with the bank account
• (For a personal bank account) A US driver’s license number or other state-issued ID number
• (For a business bank account) A Federal tax ID number

To add a direct debit account to your AWS account

2. In the navigation pane, choose Payment preferences.
3. Choose Add payment method.
4. Choose Bank account (ACH).
5. For Account type, choose Personal or Business.
6. For Name on account, enter the name of the principal account holder.
7. For Bank routing number, enter the nine-digit routing number.
   
   Routing numbers are always nine digits long. Some banks list the routing number first on a check. Other banks list the account number first.
8. For Re-enter bank routing number, enter the routing number again.
9. For Checking account number, enter the account number.
   
   Account numbers might be up to 17 digits long. The account must be an ACH-enabled checking account at a bank that’s located in the US.
10. For Re-enter checking account number, enter the bank account number again.
11. For personal bank accounts:
a. For **Driver’s license number or other state-issued ID**, enter the primary account holder’s valid US driver’s license or other state-issued ID number.

b. For **State of ID issued**, enter the name of the state.

12. For business bank accounts, for **Tax ID**, enter the Federal tax ID for the business.

13. (Optional) For **Set as default payment method**, select whether you want this direct debit account to be your default payment method.

14. For **Billing address**, enter the valid US billing address of the primary account holder.

15. Choose **Add payment method** to agree to the **Terms and Conditions** and add your direct debit account.

### Update direct debit account

You can update the name, address, or phone number that’s associated with your direct debit account.

**To update a direct debit account**

2. In the navigation pane, choose **Payment preferences**.
3. Payment methods that are associated with your AWS account are listed in the **Payment method** section.
4. Select the direct debit account that you want to edit and then choose **Edit**.
5. Update the information that you want to change.
6. Verify your changes and then choose **Save changes**.

### Managing your Advance Pay

Advance Pay is in public preview for AWS Billing and Cost Management and is subject to change. This feature is available for a select group of customers. Your use of advance pay is subject to the Betas and Previews terms of the **AWS Service Terms** (Section 2).

Use **Advance Pay** to pay for your AWS usage in advance. AWS uses the funds to pay for your invoices automatically when they’re due.

You can register for Advance Pay in the AWS Billing and Cost Management console. You can add funds to Advance Pay by using electronic fund transfer or by using any personal or business bank account. If you’re adding funds using a bank account, the bank must be a US branch location.

**Notes**

- You can use Advance Pay if your seller of record (SOR) is AWS Inc. and you’re paying in USD. If you don’t see the **Advance Pay** tab, this can be for the following reasons:
  - You have a different SOR for your AWS account. To find your SOR, go to the **Payment preferences** page and under your default payment method, see the name under **Service provider**. You can also find this information in the **Tax settings** page, under the **Seller** column.
  - If you’re a member account that is part of an organization, only the management account (also called the payer account) can use Advance Pay.
  - Advance Pay isn’t available in AWS GovCloud (US).
  - For a full list of service restrictions for Advance Pay, see **Advance Pay (p. 242)**.

**Topics**
Registering your Advance Pay

You can use the AWS Billing and Cost Management console to register for Advance Pay.

To register for Advance Pay

2. In the navigation pane, choose Payments.
3. Choose the Advance Pay tab.
4. Accept the Advance Pay terms and conditions.
5. Choose Register.

Adding funds to your Advance Pay

You can add funds to Advance Pay using electronic funds transfer, or a personal or business bank account.

To add funds to your Advance Pay using electronic funds transfer

2. In the navigation pane, choose Payments.
3. Choose the Advance Pay tab.
4. Choose Add funds.
5. Under Amount, enter the fund amount that you want to add.
   The amount must be entered in US dollars.
6. Under Payment method, choose Choose payment method.
7. Choose Wire transfer.
8. Choose Use this payment method.
9. Review the payment details, and choose Verify.
10. Complete your electronic funds transfer by using the instructions in the Payment summary section.

To use Advance Pay, you must meet eligibility requirements to add a US bank account as an ACH direct debit payment method. For more information, see Manage ACH direct debit payment methods (p. 41).

To add funds to your Advance Pay using a bank account

2. In the navigation pane, choose Payments.
3. Choose the Advance Pay tab.
4. Choose Add funds.
5. Under Amount, enter the fund amount that you want to add.
   The amount must be entered in US dollars.
6. Under Payment method, choose Choose payment method.
7. Choose Bank account.
Managing your AWS payments in CNY

If you're an AWS Inc. customer, you can make payments using the Chinese yuan currency.

### Using the China bank redirect payment method

If you're a customer based in China, you can use the China bank redirect payment method to complete payments. To do this, you must have Chinese yuan payments activated and set as your preferred currency. With the China bank redirect method, you can make payments in Chinese yuan for AWS Inc.

**Topics**

- **Requirements for using China bank redirect payments (p. 45)**
- **Setting up China bank redirect payments (p. 45)**
- **Making payments using China bank redirect (p. 46)**
- **Switching from China bank redirect to Pay by invoice (p. 46)**

### Requirements for using China bank redirect payments

To use China bank redirect as your payment method, you must be an Amazon Web Services, Inc. customer and also meet the following requirements:

- You have Chinese yuan payments activated.
- You set Chinese yuan as your preferred currency.

### Setting up China bank redirect payments

To use China bank redirect as your payment method, activate Chinese yuan payments on the AWS Billing console.

To activate Chinese yuan payments, submit information for identity verification. For a personal account, you need your national ID number for verification. For a business account, you must have the following information:

- Your uniform social credit code or organization code
- Your business license image

After you gathered the required information, follow the following procedure. This procedure outlines how to change your preferred currency to Chinese yuan and to set up China bank redirect payments.

**To activate Chinese yuan payments and set up the China bank redirect payment method**

2. In the navigation pane, choose **Payment methods**.
3. In the **Pay with Chinese yuan** section, choose **Get started** or **Pay in Chinese yuan**.
4. Review the **Terms and Conditions for Chinese Yuan Payments**. Then, select **I have read and agree to the Terms and Conditions for Chinese Yuan Payments**.
5. Choose **Next**.
6. If you have a personal account, do the following:
   - For **Full name**, enter your full name in Chinese.
   - For **Identity card number**, enter your national ID number.

   If you have a business account, do the following:
   - For **Company name**, enter the company name in Chinese.
   - For **Contact name**, enter the contact name in Chinese.
   - For **Contact phone number**, enter the contact phone number for your company.
   - For **Uniform social credit code or organization code**, enter your company’s code.
   - For **Company business license**, upload the image of your company’s business license.

   **Note**
   If applicable to your account, you might be required to add a China UnionPay credit card. For more information, see [Use a Chinese yuan credit card](#).

7. Choose **Next**.
8. Review the identity information that you entered to make sure it’s correct. Then, choose **Submit**.

It can take up to one business day to verify your identity information. After your identity is verified, your default currency automatically changes to Chinese yuan. Additionally, the China bank redirect payment method is made available to you in the **Pay with Chinese yuan** section of the **Payment Methods** console page.

### Making payments using China bank redirect

After setting up the payment method, you can use China bank redirect to make payments on your invoices.

#### To pay invoices using China bank redirect

2. In the navigation pane, choose **Payments**.
3. Select the invoice that you want to pay, and then choose **Complete payment**.
4. For **Select payment option**, choose **China bank redirect**.
5. For payments that are more than $50,000, confirm that you fulfilled the applicable tax and surcharge withholding obligations. To do so, select **I confirm that I fulfilled the Chinese tax and surcharge withholding obligations according to Chinese tax laws and regulations**.
6. Choose **Verify and pay**.
7. To proceed with the redirect, choose **OK**.

After you're redirected, choose your bank from the dropdown menu and complete your payment on your bank’s website. It can take up to 24 hours for your transaction request to process.

### Switching from China bank redirect to Pay by invoice

To change your default payment method to Pay by invoice, follow these steps.
To switch to the Pay by invoice method

2. In the navigation pane, choose Payment methods.
3. In the Pay by invoice section, choose Make default next to the default payment method that you want to use.
4. In the Change your payment method and currency dialog box, choose Yes, I want to proceed.

After you change your payment method, your preferred currency defaults to US dollars. To change your preferred currency back to Chinese yuan, choose Make default next to the China bank redirect payment method. To change your preferred currency to another supported currency, see Changing the currency to pay your bill (p. 64).

Use a Chinese yuan credit card

If you have an account with AWS Inc., are charged in USD, and are based in China, you can use the following sections to add a Chinese yuan (CNY) credit card to your account.

You can use the Payment Methods page of the AWS Billing console to perform the following tasks:

- the section called “Set up a Chinese yuan credit card” (p. 47)
- the section called “Switch from a Chinese yuan credit card to an international credit card” (p. 48)
- the section called “Add a new Chinese yuan credit card” (p. 48)

Set up a Chinese yuan credit card

To change your preferred currency to CNY and add a credit card, you must have the following information:

- National ID number
- Business license number (if applicable)
- Business license image (if applicable)

After you have the required information, you can use the following procedure to change your preferred currency and add your first Chinese credit card.

To add your first Chinese credit card

2. In the navigation pane, choose Payment methods.
3. Choose Pay with Chinese yuan.
4. In the Setting up Chinese yuan payment dialog box, read the Terms and Conditions for Chinese yuan payments, select I’ve already read and agree to the above terms and conditions, and choose Next.
5. For Verify customer identity, provide the following information:
   - National ID name
   - Contact number
   - (Business only) Company Name
   - National ID number
• (Business only) Business License number
• (Business only) Business License image

After you provide the required information, choose Next.

6. For Add a China Union Pay credit card, for the credit card fields, enter the information for the card and bank.
7. Choose Get Code, enter the provided code, and choose Next.
8. Review your information, select I have confirmed that the provided information is accurate and valid, and choose Submit.

It can take up to one business day to verify your customer information. AWS emails you after your information is fully verified.

Switch from a Chinese yuan credit card to an international credit card

To switch from a Chinese yuan credit card to an international credit card, change your preferred currency. You can use the following procedure to change your default payment method and preferred currency at the same time.

To change your default payment methods and currency

2. In the navigation pane, choose Payment methods.
3. Next to the international credit card that you want to use as your default payment method, choose Make Default.
4. In the dialog box, for Select payment currency, choose the currency that you want to use. Then, choose Yes, I want to proceed.

Add a new Chinese yuan credit card

Use the following procedure to add other Chinese yuan credit cards.

To add another Chinese credit card

2. In the navigation pane, choose Payment methods.
3. Choose Add a Chinese yuan credit card.
4. For the credit card boxes, enter the information about the card and bank.
5. Choose Get Code, enter the provided code, and choose Continue.

Managing your PIX payment method in Brazil

If you meet the requirements, you can use your preferred mobile banking app with the PIX feature turned on. You can use this feature to scan the AWS generated QR code and make a payment for your AWS account.

To use PIX, you must be an Amazon Web Services Brazil customer and your AWS account must meet the following requirements:
Your invoices are generated in Brazilian real (BRL), with BRL set as the preferred currency.
You have a credit card set as the default payment.

Registering a credit card is a requirement. However, if your credit card is a valid payment option, PIX isn’t an available payment option. If your credit card payment fails, you can choose PIX as a payment method.

To complete a transaction using PIX

2. In the navigation pane, choose Payments.
3. In the Payments due section, choose an invoice with a Past due status.
5. Choose Change payment method, or Use PIX.
6. Choose Generate QR code.

Note
The PIX QR code is active for 30 minutes. If the transaction time exceeds 30 minutes, complete these steps again to generate a new QR code.
7. In your mobile banking app, open the PIX option and scan the AWS generated QR code to see the details of your transaction. You can also choose Copy PIX code on the AWS Complete a payment page to paste the code into your banking page.
8. Complete any additional steps that are required through your banking app.
9. Confirm your completed transaction in the Payments page.

Note
It takes up to two minutes to receive the payment confirmation from your bank. Your Payments page to reflect the changes as soon as the information is received.

For any questions about your PIX payment, contact AWS Support.

Managing your payments in India

If your account is with AWS India, follow the procedures in this topic to manage your payment methods and make payments, For more information about whether your account is with AWS or AWS India, see Determining which company your account is with (p. 17).

Note
If you have questions about payment methods, see Getting help with AWS Billing (p. 6).

Contents

- Supported payment methods (p. 49)
- Use a credit or debit card to make a payment (p. 50)
- Add a net banking account (p. 50)
- Use a net banking account to make a payment (p. 50)
- Remove a net banking account (p. 51)

Supported payment methods

AWS supports Visa, Mastercard, American Express, and RuPay credit and debit cards for AWS India accounts. You can also use internet banking (net banking) accounts to pay invoices for AWS India.
Use a credit or debit card to make a payment

You can use the Billing console to pay your AWS India bills. Follow this procedure to make a payment with a credit or debit card.

To use a credit or debit card to make a payment

2. In the navigation pane, choose Payments.

   The Payments due table lists all of your remaining invoices. If there aren't any invoices listed, you don't have to do anything.
3. Choose the invoices that you're paying in the Payments due table.
5. On the Complete payment page, enter your card CVV in the Summary section, and then choose Verify and pay.
6. For Visa, Mastercard, and RuPay payment methods, you're redirected to your bank to verify your payment. For American Express payment methods, your bank processes your payment with no action required from you.

   After your payment is verified, you're redirected to the Payments page. Your invoice will remain on the Payments due table until your bank processes your payment.

Add a net banking account

You can use the Billing console to add internet banking (net banking) accounts as your payment method. This payment option is available to all AWS India customers.

To add a net banking account

2. In the navigation pane, choose Payment preferences.
3. Choose Add payment method.
4. Choose Net banking.
5. Under Net banking information, choose your bank name.
6. In the Billing address section, enter your name, billing address, and phone number.
7. Choose Add payment method.

Use a net banking account to make a payment

You can use the Billing console to pay your AWS India bills. Follow this procedure to make a payment with net banking.

   Note
   Because of current AWS India regulations, you're redirected to your bank to authorize the charge with each AWS payment. You can't use net banking for automatic payments.

To use net banking to make a payment

2. In the navigation pane, choose **Payments**.

   The **Payments due** table lists all of your remaining invoices. If there aren't any invoices listed, you don't have to do anything.

3. Choose the invoices that you're paying in the **Payments due** table.

4. Choose **Complete payment**.

5. On the **Complete a payment** page, the net banking account that you previously saved is selected by default. To use another net banking account, choose **Add net banking**.

6. Review the summary and then choose **Verify and pay**.

7. You're redirected to your bank's website to verify your payment. Sign in to your bank's account and follow the prompts to approve the payment.

   After your payment is verified, you're redirected to the **Payments** page. A success message appears at the top of the page.

---

**Remove a net banking account**

You can use the AWS Billing console to remove a net banking account from your AWS account.

**To remove a net banking account**

2. In the navigation pane, choose **Payment preferences**. Payment methods that are associated with your AWS account are listed in the **Payment method** section.
3. Ensure that your AWS account has another valid payment method set as the default.
4. Select the payment method, and then choose **Delete**.
5. In the **Delete payment method** dialog box, choose **Delete**.

---

**Managing your payments in AWS Europe**

If your account is with AWS Europe, follow the procedures in this section to manage your payment methods and payments.

**Topics**

- Managing your AWS Europe payment methods (p. 51)
- Making payments, checking unapplied funds, and viewing your payment history in AWS Europe (p. 52)
- Managing your AWS Europe credit card payment methods (p. 54)
- Managing your AWS Europe credit card payment verifications (p. 55)
- Managing your SEPA direct debit payment method (p. 57)

**Managing your AWS Europe payment methods**

You can use the **Payment preferences** page of the AWS Billing console to perform the following tasks for all payment types:

- **View payment methods associated with your account**
- **Designate a default payment method**
Remove a payment method from your AWS Europe account

In addition, you can use the Payment preferences page of the AWS Billing console to manage your credit cards and direct debit accounts. For more information, see Managing credit card and ACH payment methods (p. 40) and Managing your SEPA direct debit payment method (p. 57).

To view payment methods associated with your AWS account

You can use the console to view the payment methods that are associated with your account.

2. In the navigation pane, choose Payment preferences.

Payment methods that are associated with your AWS account are listed in the Payment method section.

To designate a default payment method

2. In the navigation pane, choose Payment preferences.

Payment methods that are associated with your AWS account are listed in the Payment method section.
3. Select the payment method that you want to use as your default payment method, and choose Set as default.

To remove a payment method from your AWS Europe account

You can use the console to remove a payment method from your account.

2. In the navigation pane, choose Payment preferences.

Payment methods that are associated with your AWS account are listed in the Payment method section.
3. Ensure that your account has another valid payment method set as the default.
4. Select the payment method that you want to remove, and choose Delete.
5. In the Delete payment method dialog box, choose Delete.

Making payments, checking unapplied funds, and viewing your payment history in AWS Europe

You can use the Payments page of the AWS Billing and Cost Management console to perform the following tasks for all payment types:

- Make a payment
- View outstanding invoices
- View unapplied funds
- View payment history
Make a payment

AWS Europe charges your default payment method automatically at the beginning of each month. If that charge doesn't process successfully, you can use the console to update your payment method and make a payment.

Note
If you pay by SEPA direct debit, AWS provides you with your invoice and initiates the charge to your payment method either the following day or the invoice due date, whichever is latest. It can take up to 5 business days for your payment to succeed. For more information, see Managing your SEPA direct debit payment method (p. 57).

Before making a payment, ensure that the payment method that you want automatically charged in the future is set as your default payment method. If you're using a credit card, confirm that your credit card isn't expired. For more information, see Designate a default payment method (p. 52) and Managing your AWS Europe credit card payment methods (p. 54).

To make a payment

2. In the navigation pane, choose Payments.

The Payments due table lists all outstanding invoices. If there aren't any invoices listed, you don't need to do anything at this time.
3. If there are outstanding invoices, select the invoice that you want to pay in the Payments due table, and then choose Complete payment.
4. On the Complete a payment page, your default payment method is selected if it's eligible for you to use to pay the invoice. If you want to use a different payment method or select an eligible payment method, choose Change.
5. Confirm that the summary matches what you want to pay, and choose Verify and pay.

After your bank processes your payment, you're redirected to the Payments page.

Say that you pay by SEPA direct debit, and you receive an email from AWS Europe saying that AWS Europe can't charge your bank account and will try again. Then, work with your bank to understand what went wrong.

Or, suppose that you receive an email saying that AWS Europe failed the last attempt to charge your bank account. Choose Verify and pay on the console to pay your invoice. If you have questions about issues with charging your bank account or paying an overdue balance, create a case in the Support Center.

If you pay by electronic funds transfer and your account payment is overdue, create a case in the Support Center.

View remaining invoices, unapplied funds, and payment history

You can search and filter the Payments due, Unapplied funds, and Payment history tables that are described in the following procedures. Choose the gear icon to change the default columns and customize other table settings. Download items individually by choosing the appropriate ID, or choose Download and then Download CSV to download a CSV file of the table for reporting purposes.

To view remaining invoices

2. In the navigation pane, choose Payments.
3. Choose the **Payments due** tab to view the **Payments due** table.

The **Payments due** table lists all your remaining invoices. The table shows your total invoice amount and remaining balance.

The table includes the following statuses:

- **Due** – Outstanding invoices with an approaching due date.
- **Past due** – Outstanding invoices with a payment that wasn’t made by the due date.
- **Scheduled** – Invoices with an upcoming scheduled payment.
- **Processing** – Invoices that a payment is currently being scheduled for.

**To view unapplied funds**

2. In the navigation pane, choose **Payments**.
3. Choose the **Unapplied funds** tab to view the **Unapplied funds** table.

The **Unapplied funds** table lists all unapplied credit memos. The table shows your total invoice amount and remaining balance.

**To view payment history**

2. In the navigation pane, choose **Payments**.
3. Choose the **Transactions** tab to view the **Transactions** table.

The **Transactions** table lists all completed transactions with AWS.

**Managing your AWS Europe credit card payment methods**

You can use the **Payment preferences** page of the AWS Billing console to perform the following credit card tasks:

- **Add a credit card to your AWS Europe account**
- **Update your credit card**
- **Confirm that your credit card is up to date**

**To add a credit card to your AWS Europe account**

You can use the console to add a credit card to your account.

2. In the navigation pane, choose **Payment Methods**.
3. Choose **Add a card**.
4. For the credit card fields, enter the information and then choose **Continue**.
5. For the credit card information fields, enter your card billing address.
6. Choose **Continue**.
To update your credit card

You can update the name, address, or phone number that’s associated with your credit card.

2. In the navigation pane, choose Payment Methods.
3. Next to the credit card that you want to edit, choose Edit.
4. Update the fields that you want to change.
5. At the bottom on the page, choose Update.

To confirm that your credit card is up to date

You must have a valid, unexpired credit card on file to make a payment.

2. In the navigation pane, choose Payment Methods.
3. Ensure that the Expires On date for your card is in the future. If your card has expired, add a new card or update your current card.

Managing your AWS Europe credit card payment verifications

To comply with the recent EU regulation, your bank might ask you for verification whenever you use a credit card to pay AWS online, add or update a credit card, or register a new AWS account. Banks typically verify by sending unique security codes to credit card holders before online purchases are completed. If your bank needs to verify your payment, you will receive an email from AWS. After verification, you're redirected to the AWS website.

If you prefer not to verify payments, register a bank account as your payment method. For more information about direct debit payment eligibility, see the section called “Manage SEPA direct debit payment method”.

To learn more about the EU regulation, see the European Commission’s website.

- the section called “Best practices for verification”
- the section called “Payment verification”
- the section called “Troubleshooting payment verification”
- the section called “AWS Organizations”
- the section called “Subscription purchases”

Best practices for verification

- Confirm that your credit card information is up to date. Banks send verification codes only to the registered card owner.
- Enter the newest code. If you close the authentication portal or request a new code, you might experience a delay in receiving your newest code.
- Enter the code as prompted. Don't enter the phone number that the code is sent from.
Payment verification

You can use the AWS Billing console to confirm that your payment requires verification or to reattempt any failed payments.

To verify your payment

2. In the navigation pane, choose Orders and invoices.
3. Under Payments due, locate the invoice that you want to pay and choose Verify and pay.
4. On the choose Payment preferences page, select the preferred payment method.
5. Choose Complete payment.
6. If your payment requires verification, you’re redirected to your bank’s website. To complete verification, follow the provided prompts.

After your bank processed our payment, you’re redirected to the Orders and invoices page.

Note
Your invoice appears with a Payment processing status until your bank completes the payment process.

Troubleshooting payment verification

If you can't successfully complete your verification, we recommend that you take any of the following actions:

• Contact your bank to confirm that your contact information is up to date.
• Contact your bank for details about why your verification has failed.
• Clear your cache and cookies or use a different browser.
• Navigate to the Payment preferences page of the AWS Billing console and update your billing contact information.

AWS Organizations

If you're a member account in AWS Organizations, your purchased services that require upfront payments might not activate until the Management account user verifies the payment. If verification is required, AWS notifies the billing contact of the Management account by email.

Establish a communication process between your Management account and member accounts. To change your payment method, see the section called “Manage AWS Europe credit card payment methods”.

Subscription purchases

Suppose that you purchase multiple subscriptions at a time (or in bulk) and your bank requests verification. Then, the bank might ask you to verify each individual purchase.

Subscriptions can include immediate purchases such as Reserved Instances, Business support plan, and Route 53 domains. Subscriptions don't include AWS Marketplace charges.

Make sure to complete validation for all purchases or register a bank account as your payment method. For more information about eligibility for direct debit payment, see the section called “Manage SEPA direct debit payment method”.

Version 2.0
56
Managing your SEPA direct debit payment method

AWS Europe customers can add a bank account to allow SEPA direct debit payments. You can use any personal or business bank account, provided that the account is located at a branch in a SEPA-supported country and payments are in the Euro currency.

If you pay by SEPA direct debit, AWS provides you with your invoice and initiates the charge to your payment method either the following day or the invoice due date, whichever is latest. It can take up to 5 business days for the payment to complete successfully, even if the payment shows as Succeeded in the AWS Billing console.

You can use the Payment preferences page of the AWS Billing console to perform the following SEPA direct debit tasks:

Contents

- Verify and link your bank account to your AWS Europe payment methods (p. 57)
- Manually add a direct debit account to your AWS Europe payment methods (p. 58)
- Update your direct debit account information (p. 59)

Verify and link your bank account to your AWS Europe payment methods

Notes

- This feature is in preview release for Billing and Cost Management and is subject to change.
- To use this feature, you must have a billing address in Germany. To change your billing address, see Update your direct debit account information (p. 59).

You can verify and link a SEPA direct debit account to your AWS account by signing in to your bank account. We ask that you sign in to your bank account, so that we can verify your identity and confirm your ownership of the bank account.

AWS works with TrueLayer to connect to your bank and securely verify ownership of your bank account. Your information is protected with an encrypted end-to-end connection during this one-time validation process. Your personal data won’t be shared or used beyond the purpose of verifying that you're the owner of the connected bank account.

If you don’t have access to the bank account sign in credentials, you can create an IAM entity (such as a user or role) for the bank account owner to provide them access to the Billing console. Then, they can update the AWS account payment method. We recommend that you don’t share sensitive information, including username, password, or payment methods for your account. For more information, see the following topics:

- Overview of managing access permissions (p. 166)
- Best practices to protect your account’s root user in the AWS Account Management Reference Guide

To verify and link your bank account

2. In the navigation pane, choose Payment preferences.
3. Choose Add payment method.
4. Choose Bank account.
5. Choose Sign in to your bank.
6. Choose Link your bank account.
7. Select your bank name.
8. Choose Allow. The information that you share will only be used to confirm your ownership of the bank account and to prevent fraud.
9. Sign in to your bank account. Use the credentials for your bank account, not the credentials for your AWS account. Your connection is encrypted and your credentials are protected. AWS won’t access or store your online banking credentials.

   **Note**
   Your bank might ask that you sign in your account with multi-factor authentication (MFA).

10. For Billing address information, enter the billing address of the primary account owner.
11. Choose Add payment method to agree to the Terms and Conditions and add your direct debit account. Your bank account is now verified and added to your AWS Europe payment methods.

   **Note**
   AWS won’t access or store your online banking credentials. AWS will ask for your explicit consent and will only request the following information from your bank:
   - Name of account holder
   - Account number

Your bank might ask for your consent to share additional information. However, any additional information won’t be shared with AWS. AWS can confirm your ownership of the bank account and charge your bank account after we first collect this information. AWS access to this information will expire based on local regulations and your bank’s policy.

To remove direct debit payments from your account, see Remove a payment method (p. 64). To remove AWS data access to your bank information, see How do I remove my access from TrueLayer? in the TrueLayer documentation.

**Manually add a direct debit account to your AWS Europe payment methods**

To manually add a direct debit account, you must meet the following requirements:

- Paid at least one invoice in full in the previous 12 months
- Paid at least $100 cumulatively over the previous 2 months.

Before you add your payment method, you need the following information:

- Bank Identifier Code (BIC)
- International Bank Account Number (IBAN)
- The address that the bank associates with the account

**To manually add a SEPA direct debit account**

2. In the navigation pane, choose Payment preferences.
3. Choose Add payment method.
4. Choose Bank account.
5. For **Account Holder Name**, enter the name of the principal account holder.
6. For **BIC (Swift Code)**, enter the 8 or 11 digit number. Routing numbers are either 8 or 11 digits long.
7. For **Confirm BIC (Swift Code)**, reenter the BIC. Don't copy and paste.
8. For **IBAN**, enter the digits for the IBAN.
9. For **Reenter IBAN**, reenter the IBAN digits. Don't copy and paste.
10. For **Make Default**, select whether you want this direct debit account to be your default payment method.
11. For **Billing Address information**, enter the billing address of the primary account holder.
12. Choose **Add bank account** to agree to the **Terms and Conditions** and add your direct debit account.

**Update your direct debit account information**

You can update the name, address, or phone number that's associated with your direct debit account.

**To update your direct debit account information**

2. In the navigation pane, choose **Payment preferences**.
   
   Payment methods that are associated with your AWS account are listed in the **Payment method** section.
3. Select the direct debit account that you want to edit, and choose **Edit**.
4. Update the fields that you want to change.
5. At the bottom of the dialog box, choose **Save changes**.

If you have questions about payment methods, see [Getting help with AWS Billing (p. 6)](#).

**Managing your payment profiles**

You can use **payment profiles** to assign payment methods that are different than your default payment method to pay your invoices automatically. If you receive invoices from more than one AWS service provider (“seller of record”), use payment profiles to assign a unique payment method for each one.

After you create a payment profile for a service provider, your payment profile pays your AWS bills automatically by using the payment method that you specified, as long as your payment profile uses the same currency as the invoice and the selected payment method is eligible for automatic payments.

For example, you receive an invoice from AWS Europe for 100 Euro (EUR). If you create a payment profile for AWS Europe and select the EUR currency, your payment profile will automatically pay your bill from AWS Europe by using the payment method selected in your payment profile.

If the currency for a payment profile isn't the same as your invoice, AWS ignores your payment profile and will charge your default payment method instead.

Payment profiles are useful in avoiding situations such as incomplete payments, failed subscription orders, and unprocessed contract renewals despite having a valid default payment method. When you use payment profiles, you can do the following:

- Use different payment methods for different AWS service providers
- Customize your payment preferences for your AWS Organizations member accounts that use different service providers
• Consistently have valid payment methods for your automatic bill payments
• Avoid service interruptions and incomplete balances

Note
Because some country and technological limitations, not all payment methods are available for all providers. If your default payment method isn’t valid for different service providers, create payment profiles by using the payment methods that are accepted by your service provider. For more information, see Creating your payment profiles (p. 60).

Topics
• Creating your payment profiles (p. 60)
• Editing your payment profiles (p. 62)
• Deleting your payment profiles (p. 62)

Creating your payment profiles

You can create new custom profiles using the following steps in the Billing and Cost Management console.

To create payment profiles
2. In the navigation pane under Preferences, choose Payment methods.
3. Under the Payment profiles section, choose Visit payment profiles.
4. Under the Payment profiles section, choose Create payment profiles.
5. Choose a service provider that matches your invoice.
6. Choose a payment currency that matches your invoice from your service provider.
7. (Optional) Enter a name for your payment profiles.
8. Under the Payment method section, choose the payment method to pay your specified service provider and currency with.
   • To add a new payment method
     a. Choose Add a new payment method to open a new tab.
     b. Add a new payment method to your account. For more information, see Managing Your Payments (p. 38).
     c. Return to the Create payment profile tab.
     d. Under the Payment method section, choose the refresh icon.
     e. Choose the new payment method that you created.
9. Choose Create payment profile.

Note
Check that your payment profile currency matches the currency of your invoice for the same service provider.

Example: Creating a payment profile for AWS Inc. bills

This section shows an example of how to create a payment profile for the bills that you receive from the AWS Inc. service provider. In this example, your AWS Organizations management account is with
AWS Europe (shown as "AWS EMEA SARL" as the service provider). Your default payment currency is Euro (EUR).

If you have a valid default payment method on file, you can pay your AWS Europe invoices automatically. Examples of a valid payment method include a credit card and a SEPA direct debit account. For more information, see Managing your payments in AWS Europe (p. 51).

For your AWS Inc. invoices, you can create a payment profile to pay using a EUR currency credit card that's eligible for AWS Inc.

To create a payment profile for this AWS Inc. example

2. In the navigation pane under Preferences, choose Payment methods.
3. Under the Payment profiles section, choose Visit payment profiles.
4. Choose Create payment profiles.
5. For Service provider, choose AWS Inc.
6. For Currency, choose EUR - Euro.
7. (Optional) Enter a name for your payment profiles (for example, My AWS Inc. payment profile).
8. Under the Payment method section, choose the payment method to pay your specified service provider and currency with.
9. Choose Create payment profile.

After this payment profile is created, your AWS Inc. invoices are paid automatically using EUR currency and the payment method that you specified.

Example: Creating a payment profile for AWS Europe bills

This section shows an example of how to create a payment profile for the bills that you receive from the AWS Europe ("AWS EMEA SARL") service provider. In this example, your AWS Organizations management account is with AWS Inc. Your default payment currency is US dollars (USD).

If you have a valid default payment method on file, you can pay your AWS Inc. invoices automatically. Examples of a valid payment method include a credit card and a US bank account for ACH direct debit payments. For more information, see Managing Your Payments (p. 38).

For your AWS Europe invoices, you can create a payment profile to pay using a USD currency credit card that's eligible for AWS Europe.

To create a payment profiles for this AWS Europe example

2. In the navigation pane under Preferences, choose Payment methods.
3. Under the Payment profiles section, choose Visit payment profiles.
4. Choose Create payment profiles.
5. For Service provider, choose AWS EMEA SARL.
6. For Currency, choose USD - US dollar.
7. (Optional) Enter a name for your payment profiles (for example, My AWS Europe payment profile).
8. Under the Payment method section, choose the payment method to pay your specified service provider and currency with.
9. Choose **Create payment profile**.

**Example: Creating a payment profile for AWS Brazil bills**

This section shows an example of how to create a payment profile for the bills that you receive from the AWS Brazil ("Amazon Web Services"/> Serviços Brasil Ltda." service provider. In this example, your AWS Organizations management account is with AWS Inc. Your default payment currency is US dollars (USD).

If you have a valid default payment method on file, you can pay your AWS Inc. invoices automatically. Examples of a valid payment method include a credit card and a US bank account for ACH direct debit payments. For more information, see [Managing Your Payments](p. 38).

For your AWS Brazil invoices, you can create a payment profile to pay using a Brazilian real (BRL) currency credit card that's eligible for AWS Brazil.

**To create payment profiles for this AWS Brazil example**

2. In the navigation pane under **Preferences**, choose **Payment methods**.
3. Under the **Payment profiles** section, choose **Visit payment profiles**.
4. Choose **Create payment profiles**.
5. For **Service provider**, choose Amazon Web Services"/> Serviços Brasil Ltda.
6. For **Currency**, choose BRL - Brazilian real.
7. (Optional) Enter a name for your payment profiles (for example, My AWS Brazil payment profile).
8. Under the **Payment method** section, choose the payment method to pay your specified service provider and currency with.
9. Choose **Create payment profile**.

**Editing your payment profiles**

After you create a payment profile, you can edit the details by using the Billing and Cost Management console at any time.

**To edit a payment profile**

2. In the navigation pane, under **Preferences**, choose **Payment methods**.
3. Under the **Payment profiles** section, choose a payment profile and choose **Edit**.
4. Update your payment profile and choose **Save changes**.

**Deleting your payment profiles**

You can delete your payment profiles by using the Billing and Cost Management console at any time.

**To delete a payment profile**

2. In the navigation pane, under **Preferences**, choose **Payment methods**.
3. Under the **Payment profiles** section, choose **Visit payment profiles**.
4. Choose a payment profile, and then choose **Delete**.
Managing your AWS payment preferences

You can use the Payment preferences page of the AWS Billing console to perform the following tasks for all payment types:

**Topics**
- View your payment methods (p. 63)
- Designate a default payment method (p. 63)
- Remove a payment method (p. 64)
- Changing the currency to pay your bill (p. 64)
- Adding additional billing contact email addresses (p. 64)

**Notes**
- IAM users need explicit permission to access some of the pages in the Billing console. For more information, see Overview of managing access permissions (p. 166).
- You can also use the Payment preferences page to manage your credit cards and direct debit accounts. For more information, see Managing credit card and ACH payment methods (p. 40) and Manage ACH direct debit payment methods (p. 41).

## View your payment methods

You can use the console to view the payment methods that are associated with your account.

### To view payment methods that are associated with your AWS account

2. In the navigation pane, choose Payment preferences.

Payment methods that are associated with your AWS account are listed in the Payment method section.

## Designate a default payment method

You can use the console to designate a default payment method for your AWS account.

### To designate a default payment method

2. In the navigation pane, choose Payment preferences.

Payment methods that are associated with your AWS account are listed in the Payment method section.
3. Next to the payment method that you want to use as your default payment method, choose Set as default.

**Note**

More information or actions might be required, depending on your payment method. Additional actions might include completing your tax registration information or choosing a supported payment currency.
Remove a payment method

You can use the console to remove a payment method from your account.

To remove a payment method from your AWS account

2. In the navigation pane, choose Payment preferences.
3. Ensure that your account has another valid payment method set as the default.
4. Select a payment method to remove, and choose Delete.
5. In the Delete payment method dialog box, choose Delete.

Changing the currency to pay your bill

To change the currency that you use to pay your bill, for example, from Danish kroner to South African rand, perform the following procedure.

To change the local currency that’s associated with your account

2. On the navigation bar in the upper-right corner, choose your account name (or alias), and choose Account.
3. In the navigation pane, choose Payment preferences.
4. In the Default payment preferences section, choose Edit.
5. On the Payment currency section, choose the payment currency you want to use.
6. Choose Save changes.

Adding additional billing contact email addresses

Use additional billing contacts to contact another person about billing related items impacting your AWS accounts. Additional billing contacts will be contacted with the root account contact and alternate billing contact about billing events.

Notes

- If you use credit or debit cards as your payment method, see Adding or updating alternate contacts (p. 12).
- If you have pay by invoice as your payment method, you can use the following procedure to add additional billing contacts to receive emails.

To add additional billing contacts to your account

2. In the navigation pane, choose Payment preferences.
3. In the Default payment preferences section, choose Edit.
4. For Billing contact email, enter the additional billing contact email messages that you want AWS to send billing-related email notifications to.
5. Choose Save changes.
Understanding your customer carbon footprint tool

You can use the customer carbon footprint tool to view estimates of the carbon emissions associated with your AWS products and services.

Topics
- Getting started with customer carbon footprint tool (p. 65)
- Understanding your customer carbon footprint tool overview (p. 66)
- Understanding your carbon emission estimations (p. 66)

Getting started with customer carbon footprint tool

The customer carbon footprint tool is available for all accounts. If a report isn't available for your account, your account might be too new to show data. After each month, you might have a delay of up to three months for AWS to show your carbon emission estimates.

To use the customer carbon footprint tool
2. On the navigation pane, choose Cost & usage reports.

IAM policies

You must have the IAM permission sustainability:GetCarbonFootprintSummary to access the customer carbon footprint tool and data. For more information regarding IAM permissions, see AWS Identity and Access Management for AWS Billing (p. 165).

AWS Organizations users

If you're signed in as a management account of AWS Organizations, the customer carbon footprint tool reports the member account data for the duration that those member accounts were a part of your organization.

If you're a member account, the customer carbon footprint tool reports emission data for all the periods. This is regardless of any changes that might have occurred to your account's associated membership in an organization.
Understanding your customer carbon footprint tool overview

Your customer carbon footprint tool page contains the following sections. This page defines each console section, so you can understand the information provided in depth.

The unit of measurement for carbon emissions is metric tons of carbon dioxide-equivalent (MTCO2e), an industry-standard measure. This measurement considers multiple greenhouse gases, including carbon dioxide, methane, and nitrous oxide. All greenhouse gas emissions are converted to the amount of carbon dioxide that would result in equivalent warming.

Carbon emissions data is available from the last 36 months. New data is available monthly, with a delay of three months as AWS gathers and processes the data that's required to provide your carbon emissions estimates. All values in the customer carbon footprint tool are rounded to the nearest one-tenth ton. If the emissions don't round up to one-tenth ton, the report will display as 0.

Your carbon emissions summary

This section shows your estimated AWS emissions and estimated emissions savings, relative to an equivalent on-premises workload. This is summarized under two categories:

- Emission savings from AWS cloud infrastructure efficiencies
- Emission savings from AWS purchase of renewable energy

Your emissions by geography

This section shows the carbon emissions associated with each applicable geographical region. This information shows high-level geographical groupings such as AMER, EMEA, and not by AWS Regions.

Your emissions by service

This section shows the carbon emissions resulting from your usage of Amazon Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), and any other AWS products and services.

Your carbon emissions statistics

This section shows trends in your carbon emissions over time. You can choose between a monthly, quarterly, or annual view.

Path to 100% renewable energy

This graph shows how your carbon emissions will change over time as AWS moves toward its goal of powering its operations with 100% renewable energy. These figures are based on your current AWS usage profile.

The Path to 100% renewable energy graph isn't impacted by your date range selection.

Understanding your carbon emission estimations

Carbon emissions data in the customer carbon footprint tool adhere to the Greenhouse Gas Protocol and ISO. Carbon footprint estimates for AWS include Scope 1 (emissions from direct operations) and Scope 2 (emissions from electricity production) data. For more information about carbon emissions, see the EPA Scope 1 and Scope 2 Inventory Guidance.

The Scope 2 portion of the estimate is calculated using the GHGP market-based method. This means it factors in Amazon enabled renewable projects on the grids where the customer footprint is being estimated. Because we use the market-based method to calculate Scope 2 emissions, only purchased renewables on the grid where your workloads are running are included in the carbon footprint estimates.
Estimates factor the grid mix of the AWS Regions where you run your workloads, following GHGP guidance. Carbon emission estimates also factor in the AWS power usage effectiveness (PUE) in our data centers.

To estimate your emissions savings compared to on-premises workload equivalent, we use data from 451 Research, which is a part of S&P Global Market Intelligence. This research found that AWS can lower a workload's carbon footprint by 88% for the median surveyed US enterprise data centers, and compared to European data enterprise centers, up to 96% once AWS is powered with 100% renewable energy. This target is on path to meet by the year 2025. For more information, see Reducing carbon by moving to AWS.

Regions, usage, and billing data factors

Electricity grids in different parts of the world use various sources of power. Some use carbon-intense fuels (for example, coal), and some are primarily low-carbon hydro or other renewables. The locations of Amazon's renewable energy projects also play a role, because the energy produces by these projects are accounted against our emissions from Regions on the same grid. As a result, not all AWS Regions have the same carbon intensity.

There are some Regions where high usage result in relatively low emissions. There are others where the low usage results in higher emissions. For carbon reports, EMEA Regions are often shown as under represented in estimates since there are more renewables on the grid. APAC Regions are often shown over represented in estimates. This is because sourcing renewable energy is difficult. Carbon estimates are based on usage only, and one-time charges such as upfront Savings Plan purchases, won't result in similar increases in carbon emissions.

Customer carbon footprint tool and Amazon's carbon footprint report

Amazon's carbon footprint report is a part of our annual sustainability report. This covers Scope 1 through 3 emissions for all Amazon operations, including Amazon Web Services. The customer carbon footprint report provides you with the emissions that attribute to your own AWS usage. For more information, see Amazon Sustainability.
Managing your purchase orders

You can use your Billing and Cost Management console to manage your purchase orders and configure how they reflect on your invoices. You have the option to add multiple purchase orders with multiple line items. Based on your configurations, we select the purchase order that best matches with your invoice. You can manage purchase orders if you’re using a regular AWS account or an AWS Organizations management account. For more information about accessing the feature, see Overview of managing access permissions (p. 166).

Each purchase order can have several line items, and every line item is used for matching with invoices. The following types of line items are available:

- **ALL** – All charges on your AWS account.
- **AWS Monthly Usage** – Your AWS monthly invoice charges.
- **AWS Subscription Purchase** – Your subscription invoice charges; for example, upfront charges for Reserved Instances (RI) and AWS Support charges.
- **AWS Marketplace Transaction** – Your purchase order line item for invoice charges from an AWS Marketplace contract subscription. This is available only for the AWS Inc. and AWS EMEA SARL entity, because all AWS Marketplace invoices are generated from AWS Inc and AWS EMEA SARL. Currently, this line item only supports invoices outside of your normal monthly billing cycle.
- **AWS Marketplace Blanket Usage** – Your default purchase order for AWS Marketplace invoice charges. This is available only for the AWS Inc. and EMEA SARL entity, because all AWS Marketplace invoices are generated from AWS Inc. and AWS EMEA SARL. All invoices with AWS Marketplace subscriptions contain an **AWS Marketplace Blanket Usage** line item, unless the subscription has a transaction-specific purchase order. If the subscription has a transaction-specific purchase order, then your invoice has an **AWS Marketplace Transaction** line item instead.

Many criteria and parameters are used to determine the optimal purchase order for your invoices. You can create up to 100 active purchase orders with up to 100 line items for each regular account or AWS Organizations management account.

When an invoice is generated, all purchase orders that are added to your management account are considered for association. Then, expired or suspended purchase orders are filtered out, leaving only the active purchase orders. Your invoice’s billing entity is matched with the "Bill from" entity in your purchase order, filtering out those that don’t match. For example, if you have a purchase order added for the AWS Inc. entity (PO_1), and another one for the AWS EMEA SARL entity (PO_2). If you purchase a Reserved Instance from AWS Europe, only PO_2 will be considered for invoice association.

Next, we evaluate line item configurations to determine the best fit for your invoice. To be matched with a line item, the invoice's billing period must be within the line item's start and end month, and it must also match the line item type. If multiple line items match, we use the line item with the most specific type for invoice association. For example, if you have an RI invoice, we use the subscription line item instead of ALL if both are configured.

Lastly, the line items with enough balance to cover your invoice amount are selected above the out of balance line items. If line items that belong to multiple purchase orders match all criteria precisely, we use the purchase order that was most recently updated to match the invoice.

**Topics**
- Setting up purchase order configurations (p. 69)
Setting up purchase order configurations

You can use purchase orders and their line item attributes to flexibly define a configuration that best fits your needs. The following are examples of purchase order configuration scenarios that you can use.

You can configure separate purchase orders for different time periods by choosing distinct effective and expiration months.

**Note**
To be matched with a line item, the invoice's billing period must be within the line item's start and end month, and it must also match the line item type.

**Example Example 1**

If you use monthly purchase orders, you can define one purchase order for each month by selecting the same effective and expiration month for each purchase order. The purchase order will only apply to the billing period of the invoices.

Here are a few purchase order configurations that you can use for this setup:

- PO #M1_2021 with the effective month set to Jan 2021 and expiration month Jan 2021.
- PO #M2_2021 with the effective month set to Feb 2021 and expiration month Feb 2021.
- PO #M3_2021 with the effective month set to Mar 2021 and expiration month Mar 2021.

Here is an example of how you can also define a purchase order for a particular quarter, half-year, or the entire year:

- PO #Q4_2021 with the effective month set to Apr 2021 and expiration month Jun 2021.
- PO #2H_2021 with the effective month set to Jul 2021 and expiration month Dec 2021.
- PO #2022Y with the effective month set to Jan 2022 and expiration month as Dec 2022.

**Example Example 2**

You can configure separate purchase orders for different types of invoices through line item configurations.

- PO #Anniversary_Q4_2021 with the effective month set to Apr 2021, and expiration month Jun 2021, Line item type = AWS monthly usage.
- PO #Subscriptions_Q4_2021 with the effective month set to Apr 2021, and expiration month Jun 2021, Line item type = AWS Subscription Purchase.
- PO #Marketplace_Q4_2021 with the effective month set to Apr 2021, and expiration month Jun 2021, Line item type = AWS Marketplace Purchase.
Adding a purchase order

You can track the balance of a given purchase order for different time periods by configuring granular line item start and end months.

**Example Example 3**

Consider PO #Q4_2021 from Example 1 with an effective month of Apr 2021 and an expiration month Jun 2021. You can track this PO's balance on a monthly basis by setting up the following line items:

- Line item #1 with the start month Apr 2021, end month Apr 2021, Line item type = ALL.
- Line item #2 with the start month May 2021, end month May 2021, Line item type = ALL.
- Line item #3 with the start month Jun 2021, end month Jun 2021, Line item type = ALL.

Alternatively, you can track balance for each line item type separately for the same purchase order and time period.

**Example Example 4**

The same PO #Q4_2021 from Example 1 can be set up using the following configuration to track balance of different line item types separately.

- Line item #1 with the start month Apr 2021, end month Jun 2021, Line item type = AWS monthly usage.
- Line item #1.2 with the start month Apr 2021, end month Jun 2021, Line item type = AWS Subscription Purchase.
- Line item #1.3 with the start month Apr 2021, end month Jun 2021, Line item type = AWS Marketplace Purchase.

Continue this configuration for May and June.

**Example Example 5**

You can also combine the previous two configurations to track balances for different time periods and line item types separately.

- Line item #1.1 with the start month Apr 2021, end month Apr 2021, Line item type = AWS monthly usage.
- Line item #1.2 with the start month Apr 2021, end month Apr 2021, Line item type = AWS Subscription Purchase.
- Line item #1.3 with the start month Apr 2021, end month Apr 2021, Line item type = AWS Marketplace Purchase.

Continue this configuration for May and June.

**Adding a purchase order**

You can use the Billing and Cost Management console to add purchase orders to use in your invoices. Adding a purchase order is a two-step process involving purchase orders and line item configurations. First, you enter your purchase order details (for example, purchase order ID, shipping address, effective and expiration month). Then, you define the purchase order line item configurations that are used to match the purchase order with an invoice. If you add multiple purchase orders, we use the purchase order that has the line item best matching the invoice being generated.
To add a purchase order

2. In the navigation pane, choose Purchase orders.
3. Choose Add purchase order.
4. For Purchase order ID, enter a unique identifier for your purchase order ID. Purchase order IDs must be unique within your account. For details about character restrictions for your purchase ID, see Purchase orders (p. 241).
5. (Optional) For Description, describe your purchase order, including any notes for your reference.
6. For Bill from, choose the AWS billing entity that you are invoiced from.

   **Note**
   Remittance details are different for each Bill from location. Be sure to verify your Bill from selection. You must make your payments to the legal entity that you’re billed from. We don’t recommend configuring more than one Bill from location for a purchase order.

7. (Optional) If your purchase order is invoiced from the Amazon Web Services EMEA SARL billing entity: For Tax registration number, select the tax registration numbers that you want to associate with your purchase order. Your purchase order is associated with only the invoices generated for the tax registration numbers that you select.

   **Note**
   The Tax registration number selection is available for only the Amazon Web Services EMEA SARL billing entity. For more information on your tax registration number settings, see Managing your account (p. 11).

8. For Ship to, enter your shipping address.

   (Optional) Select Copy Bill to address to copy and edit the address populated from your Bill to field.

9. For Effective month, choose the month you want your purchase order to start from. Your purchase order is eligible for invoice associations starting from this month.

10. For Expiration month, choose the month you want your purchase order to end. Your purchase order expires at the end of this month, and is not used for invoice associations going forward.

11. (Optional) For Purchase order contacts, enter the contact name, email address, and phone number. You can add up to 20 contacts.

12. (Optional) Enter the tag key and value. You can add up to 50 tags.

13. Choose Configure line items.

14. For Line item number, enter a unique identifier for your line item number.

15. (Optional) For Description, enter a description for your line item.

16. For Line item type, choose your preferred line item type. For a detailed description for each line item type, see Managing your purchase orders (p. 68).

17. For Start month, choose the month you want your line item to start from. This date cannot be earlier than your purchase order Effective month.

18. For End month, choose the month you want your line item to end. This date cannot be later than your purchase order Expiration month.

19. (Optional) Choose Enable balance tracking to track the balance of your line item.

20. For Amount, enter the total amount of your purchase order line item.

21. For Quantity, enter the quantity amount.

22. (Optional) For Tax, enter the tax amount. This can be an absolute value or a percentage of the line item amount.

   For Tax type, choose % of amount to enter a percentage, or amount in $ to enter an absolute tax amount.

23. To add other line items, choose Add new line item. You can add up to 100 line items.
24. Choose **Submit purchase order**.

Some fields are automatically filled and cannot be edited. Here is a list of where the automated fields are referenced from.

- **Bill to** – The Bill to address for your invoice. This field is included as a reference, because your purchase order billing address should match your invoice billing address.
- **Payment terms** – Your negotiated payment terms.
- **Currency** – Your preferred invoice currency.

**Editing your purchase orders**

You can edit your purchase order, line item information, and status using the Billing and Cost Management console. You can't change your purchase order ID in this process.

**To edit a purchase order**

2. In the navigation pane, choose **Purchase orders**.
3. Select the purchase order that you want to edit.
4. Choose **Edit purchase order**.
5. Change any parameter of your choice. Purchase order IDs cannot be changed.
6. Choose **Configure line items**.
7. Choose **Submit purchase order**.

**To update contacts**

2. In the navigation pane, choose **Purchase orders**.
3. Choose the purchase order that you want to edit.
4. Choose **Manage contacts**.
5. Change the contacts information as needed.
6. Choose **Save changes**.

**To change the status of your purchase order**

2. In the navigation pane, choose **Purchase orders**.
3. Choose the purchase order that you want to edit.
4. Choose **Change status**.
5. Choose a status:
   - **Suspended** – Your purchase order will no longer be used for invoice association.
   - **Active** – Your purchase order will be used for invoice association.
6. Choose **Change status**.

**Note**

You can use a suspended purchase order for invoice association when it is past its expiration date and set to **Suspended-Expired** status. To do so, you must change the status to **Expired** and
update the expiration month to make it **Active**. Be sure to update your line item end months accordingly.

**To add a line item**

2. In the navigation pane, choose **Purchase orders**.
3. Choose the purchase order you want to edit.
4. In the **Line items** section, choose **Add line item**.
5. Change the information as needed.
6. Choose **Save line item**.

**To edit a line item**

2. In the navigation pane, choose **Purchase orders**.
3. Choose the purchase order you want to edit.
4. In the **Line items** section, choose **Edit**.
5. Change the line item information as needed.
6. Choose **Save line item**.

**To delete a line item**

2. In the navigation pane, choose **Purchase orders**.
3. Choose the purchase order you want to edit.
4. Select all of the line items to delete in the **Line items** section.
5. Choose **Delete**.
6. Choose **Confirm**.

Use the following procedure to update your tags for your purchase order.

**To update tags for purchase orders**

2. In the navigation pane, choose **Purchase orders**.
3. Choose the purchase order that you want to edit.
4. Choose **Manage tags**.
5. Change your tag information as needed.
6. Choose **Save changes**.

**Deleting your purchase orders**

You can use the Billing and Cost Management console to delete your purchase order at any time, along with all of its notifications and associated contacts. A deleted purchase order can’t be recovered.

**To delete a purchase order**

2. In the navigation pane, choose **Purchase orders**.
3. Select all of the purchase orders that you want to delete.
4. Choose **Delete purchase order**.
5. Choose **Confirm**.

### Viewing your purchase orders

Your purchase order dashboard on the Billing and Cost Management console shows you the state of your purchase orders at a glance. Your purchase orders are listed on the dashboard, along with the following information.

- **Purchase order ID** – The unique identifier for your purchase order.
- **Value** – Your purchase order amount. This is the sum of all line item amounts.
- **Balance** – The sum of all line item balances. This sum is updated whenever an invoice is associated.
- **Effective and Expiration** – The start and end of your purchase order ID.
- **Status** – The current status of your purchase order.
- **Updated on** – The most recent date you updated your purchase order.

### To view your purchase orders

2. In the navigation pane, choose **Purchase orders**.
3. Choose a purchase order to see the **Purchase order details** page.

### Reading your purchase order details page

You can review the contents of your individual purchase orders on the **Purchase order details** page of the Billing and Cost Management console.

To change your purchase order or line items, see [Editing your purchase orders](p. 72).

- **Bill to** – The address reflected on your invoice. To change your billing address, update the information from your **Payment methods**.
- **Ship to** – Your purchase order's shipping address.
- **Bill from** – The AWS legal entity you're billed from.
- **Tax registration numbers** – The tax registration numbers that you selected for your purchase order. Your purchase order is associated with the invoices generated for these tax registration numbers.

  **Note**
  
  The **Tax registration number** selection is available for only the **Amazon Web Services EMEA SARL** billing entity. For more information on your tax registration number settings, see [Managing your account](p. 11).

- **Payment terms** – Your negotiated AWS payment terms.
- **Currency** – Your preferred invoice payment currency.
- **Effective month** – The month your purchase order is effective from. Your purchase order is used for generated invoices starting this month.
- **Expiration month** – The month your purchase order expires. Your purchase order is not used for any invoices that are generated past this month.
• **Contacts** – A list of all contacts for this purchase order. Choose **Manage contacts** to see all listed.

• **Status** – The current status of your purchase order.
  - **Active** – Eligible for invoice association.
  - **Suspended** – Not eligible for invoice association. You can suspend an active or expired purchase order.
  - **Expired** – A purchase order that is past its expiration date, and is no longer eligible for invoice association.
  - **Suspended-expired** – A suspended purchase order that is also past its expiration date.

• **Balance amount** – The balance remaining on your purchase order. This is the total balance amount of all line items configured on your purchase order.

• **Total amount** – The sum of your total values for all line items configured in your purchase order.

• **Line items** – The line item details you used when adding the purchase order.
  - **Number** – The unique identifier for your line item.
  - **Type** – Your line item type.
  - **Start month** – The month that your line is effective from. The line item is eligible for invoice association from this month.
  - **End month** – The month your line item expires. The line item is not eligible for invoice association at the end of this month.
  - **Amount** – The unit price amount.
  - **Quantity** – The number of units.
  - **Tax** – The tax amount.
  - **Total value** – The total value of amount for the particular line item.
  - **Current balance** – The remaining balance after subtracting the total amount of all invoices matched with this line item. To see details for all invoices matching this line item, see the invoices table.

• **Invoices** – All invoices associated with your purchase order.
  - **Date issued** – The date when the invoice was issued.
  - **Type** – The type of invoice. For example, invoice and credit memo.
  - **ID** – The unique identifier of the invoice.
  - **Line item number** – The line item number of your purchase order, associated with the invoice.
  - **Amount** – The invoice amount.
  - **Due date** – Your payment due date for the invoice.

---

**Enabling purchase order notifications**

You can enable email notifications on the Billing and Cost Management console by adding contacts to your purchase orders. You need at least one purchase order contact added to receive notifications.

Notifications are beneficial to proactively take action on your expiring, or out of balance purchase orders. This helps you make payments without delay. To update your contacts information, see **Editing your purchase orders (p. 72)**.

Purchase order notifications are sent to your contacts for the following scenarios:

- **Balance tracking** – When your purchase order's line item balance drops below the 75% threshold. The purchase order balance is tracked at the line item level, and must be enabled at each level.

- **Expiration tracking** – When your purchase order is approaching its expiration. Your contacts receive notifications leading up to your expiration date. If your purchase order expiration is less than one month away, notifications are sent one week prior and on the expiration date. If your expiration date is one to three months away, a notification is sent one month before the expiration date. If the expiration is more than three months away, notifications are sent two months before the expiration date.
Use tags to manage access to purchase orders

You can use attribute-based access control (ABAC) to manage access to your purchase orders. When you create your purchase orders, you can tags with key-value pairs. You can then create IAM policies and specify the tags. For example, if you add the project key and assign it a value of test, your IAM policies can explicitly allow or deny access to any purchase order that has this tag.

To add tags to new purchase orders or update existing ones, see Adding a purchase order (p. 70) and Editing your purchase orders (p. 72).

Example Example: Use tags to allow access

The following policy allows the IAM entity to add, modify, or tag purchase orders that have the project key and a value of test.

```json
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Resource": "arn:aws:purchase-orders::*:purchase-order/*",
      "Condition": {
         "StringEquals": {
            "aws:RequestTag/project": "test"
         },
         "ForAllValues:StringEquals": {
            "aws:TagKeys": "project"
         }
      }
   }]
}
```

Example Example: Use tags to deny access

The following policy denies the IAM entity from completing any purchase order action on purchase orders that have the project key and a value of test.

```json
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Deny",
      "Action": "purchase-orders:*",
      "Resource": "arn:aws:purchase-orders::*:purchase-order/*",
      "Condition": {
         "StringEquals": {
            "aws:ResourceTag/Project": "test"
         }
      }
   }]
}
```

For more information, see the following topics in the IAM User Guide:

- What is ABAC for AWS?
- Controlling access to AWS resources using tags
Managing your costs with AWS Cost Categories

You can use AWS Cost Categories to map your AWS costs and usage into meaningful categories. With cost categories, you can organize your costs using a rule-based engine. The rules that you configure organize your costs into categories. You can then use these categories across multiple products in the AWS Billing and Cost Management console. This includes Cost Explorer, AWS Budgets, AWS Cost and Usage Reports (AWS CUR), and Cost Anomaly Detection.

You can create groupings of costs using cost categories. For example, assume that your business is organized by teams and that each team has multiple accounts within. To build this structure in cost categories, create a cost category named Team. Then, you can map costs to a cost category value that's named Team 1.

Companies commonly have multiple perspectives on their business. These can include projects, cost centers, and applications. You can create cost categories to match these perspectives. Cost category values are groups within cost categories. They're similar to Team 1 or Team 2 from the previous example. By creating cost categories, you can view your business from multiple, corresponding perspectives. Furthermore, you can create multilevel hierarchical relationships among your cost categories to replicate your organizational structure. For example, you can create a cost category named Business Unit that includes groupings of multiple teams. You can then define a cost category value that's named BU1 with Team 1 and Team 2 selected from your Teams cost category and a cost category value BU2 with Team 3 and Team 4 selected from the Teams cost category.

You can start using cost categories by creating a unique category name. Then, map costs to cost category values within the cost categories. In each cost category value, map the type of costs that belong to that value. For example, if your Team 1 consists of multiple accounts, you can write that expression by choosing the accounts dimension (is option) and selecting the applicable accounts. After creating the cost category value, continue to create other teams by adding values.

Note
To create hierarchical relationships among your cost categories, you select the cost category dimension from the parent cost category. This was Business Unit in the previous example. The child cost category is the cost category name. This was Teams in the previous example. You can then select values that belong to the child cost category, such as Team 1 and Team 2, into the parent cost category value. This is BU 1 in the previous example.

After you create the cost categories, they appear in Cost Explorer, AWS Budgets, AWS CUR, and Cost Anomaly Detection. In Cost Explorer and AWS Budgets, a cost category appears as an additional billing dimension. You can use this to filter for the specific cost category value, or group by the cost category. In AWS CUR, the cost category appears as a new column with the cost category value in each row. In Cost Anomaly Detection, you can use cost category as a monitor type to monitor your total costs across specified cost category values.

Note
Cost categories are effective at the start of the current month. If you create or update your cost category in the middle of the month, it retroactively takes effect on cost and usage from the beginning of the month.

This is an administrative feature, and it can only be customized by the management account or regular accounts in AWS Organizations.
Supported dimensions

You can select from a list of billing dimensions to create your cost category rules. These billing dimensions are used to group your data. For example, assume that you wanted to group a set of accounts to form a team. You need to choose the account billing dimension, and then choose the list of accounts that you want to include in the team.

The following billing dimensions are supported.

**Account**

This can be the AWS account name or the account ID, depending on the operation. If you're using an exact match operation (is or is not), account refers to the account ID. If you're using an approximate match operation (starts with, ends with, or contains), account refers to account name.

**Charge type**

The type of charges based on line items details. Also referred to as the RECORD_TYPE in the Cost Explorer API. For more information, see Term comparisons (p. 80).

**Cost category**

A dimension from another cost category. Using cost categories as a dimension helps you organize the levels of categories.

**Region**

The geographic areas where AWS hosts your resources.

**Service**

AWS services, such as Amazon EC2, Amazon RDS, and Amazon S3.

**Tag key**

The cost allocation tag keys that are specified on the resource. For more information, see Using AWS cost allocation tags (p. 87).
Usage Type

Usage types are the units that each service uses to measure the usage of a specific type of resource. For example, the BoxUsage:t2.micro(Hrs) usage type filters by the running hours of Amazon EC2 t2.micro instances.

Supported operations

You can use these operations to create the filter expression when you're creating a cost category rule.

The following operations are supported.

Is

The exact match operation that's used to filter for the exact value specified.

Is not

The exact match operation that's used to filter for the exact value that isn't specified.

Is absent

The exact match operation that's used to exclude the tag key that matches this value.

Contains

The approximate match that's used to filter for a text string containing this value. This value is case sensitive.

Starts with

The approximate match that's used to filter for a text string that starts with this value. This value is case sensitive.

Ends with

The approximate match that's used to filter for a text string that ends with this value. This value is case sensitive.

Supported rule types

Use rule type to define which cost category values to use to categorize your costs.

The following rule types are supported.

Regular Rule

This rule type adds statically defined cost category values that categorize costs based on the defined dimension rules.

Inherited Value

This rule type adds the flexibility of defining a rule that dynamically inherits the cost category value from the dimension value defined. For example, assume that you wanted to dynamically group costs based on the value of a specific tag key. You need to choose the inherited value rule type, then choose the Tag dimension and specify the tag key to use. Optionally, you can use a tag key, teams, to tag your resources. They can tag them with values such as alpha, beta, and gamma. Then, with
an inherited value rule, you can select Tag as the dimension and use teams as the tag key. This generates the dynamic cost category values of alpha, beta, and gamma.

Default value

Optionally, if no rules are matched for the cost category, you can define this value to be used instead.

Status

You can use the console to confirm the status of whether your cost categories completed processing the cost and usage information. After you create or edit a cost category, it can take up to 24 hours before it has categorized your cost and usage information in the AWS Cost and Usage Report, Cost Explorer, and other cost management products.

There are two status states.

Applied

Cost categories completed processing, and the information in AWS Cost and Usage Report, Cost Explorer, and other cost management products is up to date with the new rules.

Processing

The cost category updates are still in progress.

Quotas

For more information about cost categories quotas, see Quotas and restrictions (p. 241).

Term comparisons

CHARGE_TYPE is a dimension supported for cost category expressions. It's the RECORD_TYPE value in the Cost Explorer API. This dimension uses different terms, depending on whether you're using the console or the API/JSON editor. The following table compares the terminology used for both scenarios.

<table>
<thead>
<tr>
<th>Term comparison</th>
<th>Value in API or JSON editor</th>
<th>Name used in the console</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit</td>
<td>Credit</td>
<td>Credit</td>
</tr>
<tr>
<td>DiscountedUsage</td>
<td>Reservation applied usage</td>
<td></td>
</tr>
<tr>
<td>Fee</td>
<td>Fee</td>
<td></td>
</tr>
<tr>
<td>Refund</td>
<td>Refund</td>
<td></td>
</tr>
<tr>
<td>RIFee</td>
<td>Recurring reservation fee</td>
<td></td>
</tr>
<tr>
<td>SavingsPlanCoveredUsage</td>
<td>Savings Plan Covered Usage</td>
<td></td>
</tr>
<tr>
<td>SavingsPlanNegation</td>
<td>Savings Plan Negation</td>
<td></td>
</tr>
</tbody>
</table>
Creating cost categories

You can create cost categories to organize your cost and usage information. Regular accounts and the management account in AWS Organizations have default access to create cost categories. Rules aren't mutually exclusive, and you can control the order that the rules apply in. Allow up to 24 hours after creating a cost category for your usage records to be updated with values.

There are five major steps in creating cost categories.

1. Define a name for your cost category (for example, business units, Teams).
2. (Optional) Add a tag to your cost category. For more information about tags, see Tagging your AWS resources in the AWS Tag Editor User Guide.
3. (Optional) Set the lookback period for your cost category rules. The default will be set to the current month.
   **Tip**
   To request a backfill of your cost data in your AWS Cost and Usage Report, create a support case. In your support case, specify the report name and the billing period that you want backfilled. For more information, see Contacting AWS Support (p. 6).
4. Write the rules to categorize your costs into cost category values (for example, Team-A, Team-B, Team-C).
5. (Optional) Define rules to split charges between your cost category values.
   For more information about split charges, see Splitting charges within cost categories (p. 85).

Use the following procedure to create a cost category.

**To create a cost category**

2. In the navigation pane, choose AWS Cost Categories.
3. At the top of the page, choose Create Cost category.
4. Under Cost category details, enter the name of your cost category. Your cost category name must be unique within your account.
5. (Optional) To add a tag, choose Add new resource tag and enter a key and value.
6. (Optional) To add a lookback period for your cost category rules, choose Apply cost category rules starting any specified month from the previous 12 months, and select the month where you want to retroactively apply the rules.
   **Tip**
   To request a backfill of your cost data in your AWS Cost and Usage Report, create a support case. In your support case, specify the report name and the billing period that you want backfilled. For more information, see Contacting AWS Support (p. 6).
7. Choose Next.
8. Choose Define category values.

Use either the Rule Builder or JSON editor to define your cost categories.

For more information about the JSON request syntax, see the AWS Billing and Cost Management API Reference.

9. For Value, enter the name of the cost category value.
10. Choose a Rule Type, either Regular or Inherited value.
11. Choose a billing Dimension from the list. For a regular rule type, you can choose Accounts, Service, Charge Type (for example, recurring reservation fee), Tag key, Region, Usage Type, or Cost Category. (You can choose Cost Category to create hierarchical relationships among your cost categories.) For an inherited value rule type, you can choose Account or Tag key (Cost Allocation tag key).
12. For a regular rule type, choose Operator from the dropdown list. Your options are Is, Contains, Starts with, and Ends with.

Note
Contains, Starts with, and Ends with are only supported with Accounts and Tag dimensions. If you use these operators with Accounts, the engine evaluates against account name, and not account ID.

Choose a filtered value for your Dimension in the attribute selector.
13. Choose a dimension operator for your rule from the dropdown. You can choose between AND and OR. AND is the default operator. Changing the operator impacts all dimensions in this rule.
14. For an inherited value rule type, choose Account or Tag for Dimension. If Tag is the Dimension, choose the Tag key to inherit the cost category value from.

Note
The Account dimension uses account names, not account IDs for the inherited cost category value.
15. (Optional) Add a default value. It categorizes all unmatched costs to this value.
16. (Optional) To rearrange the rule order, use the arrows or change the number on the top right of each rule.
17. (Optional) To delete a rule, choose Remove on the top right of each rule.
18. (Optional) Under Define split charges, choose Next.

For more information about split charge rules, see Splitting charges within cost categories (p. 85).

a. Choose Add a split charge.

b. Under Source value, choose your cost category value.

Uncategorized cost isn’t an option at this time, but is an available source if you edit your cost category. For more information, see Editing cost categories (p. 84).

c. Under Target values, choose one or more cost category values you wish to allocate split charges to.

d. Under Charge allocation method, choose how you want to allocate your costs. Your choices are proportional, fixed, and even split.

For fixed charge allocation, enter the percentage amount to allocate each target cost category value.

e. Choose Create split charge.

f. Choose Add a split charge and repeat steps to define more split charges.

19. Choose Create cost category.
Tagging cost categories

Tagging cost categories is beneficial to control access to cost categories. For more information, see Controlling access to AWS resources using tags in the IAM User Guide.

You can tag your existing cost categories using the following procedure:

To tag a cost category

2. In the navigation pane, choose AWS Cost Categories.
3. Choose the cost category you want to tag.
5. Choose Manage resource tags.
7. Enter a Key and Value.
8. Once you configure the tags, choose Save changes.

Viewing cost categories

From the cost categories dashboard in AWS Billing and Cost Management, you go to the details page. There comprehensive information about your category details and values is displayed.

Topics
- Navigating to your cost category details page (p. 83)
- Understanding your cost category details page (p. 83)
- Your cost category month-to-date categorizations (p. 84)
- Download your cost category values (p. 84)

Navigating to your cost category details page

You can choose any cost category name in the Billing and Cost Management console to open a details page. The details page is also shown when you add or edit a cost category.

To view your cost category details page

2. In the navigation pane, choose Cost categories.
3. Under the Cost category column, choose a cost category name.

Understanding your cost category details page

Your cost category details page breaks down your month-to-date cost allocations using the Category details and Category values sections.

- Use the month selector on the top right of the page to change the month you’re viewing. You can see a detailed breakdown of cost category value cost allocations within your cost category.
• Under the **Category details** section, you can view your current status (p. 80), default value (p. 80), value count, and your total month-to-date net amortized costs.

• The graph under **Categorized costs** shows the allocation of cost category values in your monthly spend. Any uncategorized costs are shown as **Uncategorized**.

### Your cost category month-to-date categorizations

In the **Category values** section, you can see the month-to-date spend for each configured cost category value. The amounts that are shown are the net amortized costs.

To further explore your costs, open Cost Explorer by choosing **View in AWS Cost Explorer**.

### Download your cost category values

You can download an offline copy of your month-to-date cost category spend.

**To download your cost category details page**

2. In the navigation pane, choose **Cost categories**.
3. Under the **Cost category** column, choose a cost category name.
4. Choose **Download CSV** to download a comma-separated values file.

### Editing cost categories

You can edit your AWS Cost Categories using the following procedure. Cost category names can't be edited. If you're using split charges, you can choose **Uncategorized** cost as your source value at this time.

**To edit a cost category**

2. In the navigation pane, choose **cost categories**.
3. Select the cost category to edit.
4. Choose **Edit cost category**.
5. If you want the changes to retroactively apply from a previous date, choose the month you want the parameter changes to apply from.
6. Make changes to parameters and choose **Confirm cost category**.

### Deleting cost categories

You can delete your cost categories using the following procedure.

**To delete a cost category**

2. In the navigation pane, choose **Cost categories**.
3. Select the cost category to delete.
Splitting charges within cost categories

You can use split charge rules to allocate your charges between your cost category values. Splitting charges is useful when you have costs that aren't directly attributed to a single owner. Therefore, the costs can't be categorized into a single cost category value. For example, your organization has a set of costs shared by multiple teams, business units, and financial owners that incur data transfer costs, enterprise support, and operating costs. You can define split charge rules when you create or edit your cost categories. For more information about these processes, see Creating cost categories (p. 81) and Editing cost categories (p. 84).

This is a list of terms you'll see when configuring your split charges.

**Source**

The group of shared costs you want to split. Sources can be any of your existing cost category values.

**Targets**

The cost category values you want to split your costs across, defined by the source.

**Allocation method**

How you want your source costs split between your targets. You can choose from the following methods:

- **Proportional** - Allocates costs across your targets based on the proportional weighted cost of each target.
- **Fixed** - Allocates costs across your targets based on your defined allocation percentage.
- **Even split** - Allocates costs evenly across all targets.

**Prerequisites**

Before you define your split charge rules, you must categorize your costs into the appropriate cost category values.

**Example Example**

You define a business unit view of your organization, using a Business unit cost category, with values engineering, marketing, and FinOps. Your organization is also operating a shared infrastructure platform that supports engineering and marketing business units.

To allocate costs of this shared infrastructure platform to the target business unit, categorize its costs into a new cost category value, Infrastructure Platform using the appropriate dimensions (p. 78).

We recommend that you move your cost category values containing shared costs to the top of the rule list. Because cost category rules are evaluated in a top-down order, your shared costs are categorized
Understanding split charge best practices

For instructions on how to configure your split charges, see Creating cost categories (p. 81) step 15. After you define split charge rules, you can view the split and allocated costs on the cost categories details page in the console. The details page provides an overview of your costs for each cost category value. This includes the costs for before and after calculating the split charges. You can also download a CSV report from the details page.

Note the following scenarios when configuring your split charges:

- A cost category value can be used as a source only once across all split charge rules. This means that, if a value is used as a source, it can’t be used as a target. If the value is used as a target, it can’t be used as a source. A value can be used as a target in multiple split charge rules.
- If you want to use cost category values as a source or split charge target when the value was created from inherited values (p. 79) rules, you must wait until the cost category status (p. 80) changes to Applied.
- Split charge rules and the total allocated costs are only presented on the cost categories details page. These costs do not appear and don’t impact your AWS Cost and Usage Reports, Cost Explorer, and other AWS Cost Management tools.
- You can define up to 10 split charge rules for a cost category.

For more information about cost category quotas, see Cost categories (p. 241).
Using AWS cost allocation tags

A tag is a label that you or AWS assigns to an AWS resource. Each tag consists of a key and a value. For each resource, each tag key must be unique, and each tag key can have only one value. You can use tags to organize your resources, and cost allocation tags to track your AWS costs on a detailed level. After you activate cost allocation tags, AWS uses the cost allocation tags to organize your resource costs on your cost allocation report, to make it easier for you to categorize and track your AWS costs.

AWS provides two types of cost allocation tags, an AWS-generated tags and user-defined tags.

AWS, or AWS Marketplace ISV defines, creates, and applies the AWS-generated tags for you, and you define, create, and apply user-defined tags. You must activate both types of tags separately before they can appear in Cost Explorer or on a cost allocation report.

The following diagram illustrates the concept. In the example, you've assigned and activated tags on two Amazon EC2 instances, one tag called Cost Center and another tag called Stack. Each of the tags has an associated value. You also activated the AWS-generated tags, createdBy before creating these resources. The createdBy tag tracks who created the resource. The user-defined tags use the user prefix, and the AWS-generated tag uses the aws: prefix.

After you or AWS applies tags to your AWS resources (such as Amazon EC2 instances or Amazon S3 buckets) and you activate the tags in the Billing and Cost Management console, AWS generates a cost allocation report as a comma-separated value (CSV file) with your usage and costs grouped by your active tags. You can apply tags that represent business categories (such as cost centers, application names, or owners) to organize your costs across multiple services.

The cost allocation report includes all of your AWS costs for each billing period. The report includes both tagged and untagged resources, so that you can clearly organize the charges for resources. For example, if you tag resources with an application name, you can track the total cost of a single application that runs on those resources. The following screenshot shows a partial report with columns for each tag.
At the end of the billing cycle, the total charges (tagged and untagged) on the billing report with cost allocation tags reconciles with the total charges on your Bills page total and other billing reports for the same period.

You can also use tags to filter views in Cost Explorer. For more information about Cost Explorer, see Analyzing your costs with AWS Cost Explorer.

For more information about activating the AWS-generated tags, see Activating the AWS generated cost allocation tags (p. 91). For more information about applying and activating user-defined tags, see User-defined cost allocation tags (p. 92). All tags can take up to 24 hours to appear in the Billing and Cost Management console.

Notes

• As a best practice, don't include sensitive information in tags.
• Only the management account in an organization and single accounts that aren't members of an organization have access to the cost allocation tags manager in the Billing console.
• To create and update tags, use AWS Tag Editor. For more information about Tag Editor, see Using Tag Editor in the Tagging AWS Resources User Guide.

Topics

• AWS generated cost allocation tags (p. 88)
• User-defined cost allocation tags (p. 92)
• Monthly cost allocation report (p. 94)
• Understanding dates for cost allocation tags (p. 96)

AWS generated cost allocation tags

The AWS-generated tag createdBy is a tag that AWS defines and applies to supported AWS resources for cost allocation purposes. To use the AWS-generated tag, a management account owner must activate it in the Billing console. When a management account owner activates the tag, the tag is also activated for all member accounts. After the tag is activated, AWS starts applying the tag to resources that are created after the AWS-generated tag is activated. The AWS-generated tag is available only in the Billing console and reports, and doesn't appear anywhere else in the AWS console, including the AWS Tag Editor. The createdBy tag does not count towards your tags per resource quota.

The aws:createdBy tags are populated only in the following AWS Regions:

• ap-northeast-1
• ap-northeast-2
• ap-south-1
• ap-southeast-1
Resources created outside of these AWS Regions will not have this tag auto-populated.

The `createdBy` tag uses the following key-value definition:

```plaintext
key = aws:createdBy

value = account-type:account-ID or access-key:user-name or role session name
```

Not all values include all of the value parameters. For example, the value for a AWS-generated tag for a root account doesn't always have a user name.

Valid values for the `account-type` are Root, IAMUser, AssumedRole, and FederatedUser.

If the tag has an account ID, the `account-id` tracks the account number of the root account or federated user who created the resource. If the tag has an access key, then the `access-key` tracks the IAM access key used and, if applicable, the session role name.

The `user-name` is the user name, if one is available.

Here are some examples of tag values:

- `Root:1234567890`
- `Root: 111122223333 :exampleUser`
- `IAMUser: AIDACKCEVSQ6C2EXAMPLE :exampleUser`
- `AssumedRole: AKIAIOSFODNN7EXAMPLE :exampleRole`
- `FederatedUser:1234567890:exampleUser`

For more information about IAM users, roles, and federation, see the [IAM User Guide](https://docs.aws.amazon.com/IAM/latest/userguide/)

AWS generated cost allocation tags are applied on a best-effort basis. Issues with services that AWS-generated tag depends on, such as CloudTrail, can cause a gap in tagging.

The `createdBy` tag is applied only to the following services and resources after the following events:

<table>
<thead>
<tr>
<th>AWS Product</th>
<th>API or Console Event</th>
<th>Resource Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS CloudFormation (AWS CloudFormation)</td>
<td>CreateStack</td>
<td>Stack</td>
</tr>
<tr>
<td>AWS Data Pipeline (AWS Data Pipeline)</td>
<td>CreatePipeline</td>
<td>Pipeline</td>
</tr>
<tr>
<td>Amazon Elastic Compute Cloud (Amazon EC2)</td>
<td>CreateCustomerGateway</td>
<td>Customer gateway</td>
</tr>
<tr>
<td>AWS Product</td>
<td>API or Console Event</td>
<td>Resource Type</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>----------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>CreateDhcpOptions</td>
<td></td>
<td>DHCP options</td>
</tr>
<tr>
<td>CreateImage</td>
<td></td>
<td>Image</td>
</tr>
<tr>
<td>CreateInternetGateway</td>
<td></td>
<td>Internet gateway</td>
</tr>
<tr>
<td>CreateNetworkAcl</td>
<td></td>
<td>Network ACL</td>
</tr>
<tr>
<td>CreateNetworkInterface</td>
<td></td>
<td>Network interface</td>
</tr>
<tr>
<td>CreateRouteTable</td>
<td></td>
<td>Route table</td>
</tr>
<tr>
<td>CreateSecurityGroup</td>
<td></td>
<td>Security group</td>
</tr>
<tr>
<td>CreateSnapshot</td>
<td></td>
<td>Snapshot</td>
</tr>
<tr>
<td>CreateSubnet</td>
<td></td>
<td>Subnet</td>
</tr>
<tr>
<td>CreateVolume</td>
<td></td>
<td>Volume</td>
</tr>
<tr>
<td>CreateVpc</td>
<td></td>
<td>VPC</td>
</tr>
<tr>
<td>CreateVpcPeeringConnection</td>
<td></td>
<td>VPC peering connection</td>
</tr>
<tr>
<td>CreateVpnConnection</td>
<td></td>
<td>VPN connection</td>
</tr>
<tr>
<td>CreateVpnGateway</td>
<td></td>
<td>VPN gateway</td>
</tr>
<tr>
<td>PurchaseReservedInstancesOffering</td>
<td></td>
<td>Reserved instance</td>
</tr>
<tr>
<td>RequestSpotInstances</td>
<td></td>
<td>Spot-instance-request</td>
</tr>
<tr>
<td>RunInstances</td>
<td></td>
<td>Instance</td>
</tr>
<tr>
<td>Amazon ElastiCache (ElastiCache)</td>
<td>CreateSnapshot</td>
<td>Snapshot</td>
</tr>
<tr>
<td></td>
<td>CreateCacheCluster</td>
<td>Cluster</td>
</tr>
<tr>
<td>AWS Elastic Beanstalk (Elastic Beanstalk)</td>
<td>CreateEnvironment</td>
<td>Environment</td>
</tr>
<tr>
<td></td>
<td>CreateApplication</td>
<td>Application</td>
</tr>
<tr>
<td>Elastic Load Balancing (Elastic Load Balancing)</td>
<td>CreateLoadBalancer</td>
<td>Loadbalancer</td>
</tr>
<tr>
<td>Amazon S3 Glacier (S3 Glacier)</td>
<td>CreateVault</td>
<td>Vault</td>
</tr>
<tr>
<td>Amazon Kinesis (Kinesis)</td>
<td>CreateStream</td>
<td>Stream</td>
</tr>
<tr>
<td>Amazon Relational Database Service (Amazon RDS)</td>
<td>CreateDBInstanceReadReplica</td>
<td>Database</td>
</tr>
<tr>
<td></td>
<td>CreateDBParameterGroup</td>
<td>ParameterGroup</td>
</tr>
<tr>
<td></td>
<td>CreateDBSnapshot</td>
<td>Snapshot</td>
</tr>
<tr>
<td></td>
<td>CreateDBSubnetGroup</td>
<td>SubnetGroup</td>
</tr>
</tbody>
</table>
AWS Marketplace vendor-provided tags

AWS Marketplac vendor-provided tags

Certain AWS Marketplace vendors can create tags and associate them with your software usage. These tags will have the prefix `aws:marketplace:isv:`. To use the tags, a management account owner must activate the tag in the Billing and Cost Management console. When a management account owner activates the tag, the tag is also activated for all member accounts. Similar to `aws:createdBy` tags, these tags appear only in the Billing and Cost Management console and they don't count towards your tags per resource quota. You can find the tag keys that apply to the product on the AWS Marketplace product pages.

Activating the AWS generated cost allocation tags

Management account owners can activate the AWS-generated tags in the Billing and Cost Management console. When a management account owner activates the tag, it's also activated for all member accounts. This tag is visible only in the Billing and Cost Management console and reports.

To activate the AWS-generated tags

You can activate the `createdBy` tag in the Billing and Cost Management console.

2. In the navigation pane, choose Cost allocation tags.
3. Under AWS-generated cost allocation tags, choose the `createdBy` tag.
Deactivating the AWS generated cost allocation tags

Management account owners can deactivate the AWS-generated tags in the Billing and Cost Management console. When a management account owner deactivates the tag, it's also deactivated for all member accounts. After you deactivate the AWS-generated tags, AWS no longer applies the tag to new resources. Previously tagged resources remain tagged.

To deactivate the AWS-generated tags

2. In the navigation pane, choose Cost allocation tags.
3. Under AWS-generated cost allocation tags, choose Deactivate.

It can take up to 24 hours for tags to deactivate.

Restrictions on AWS generated cost allocation tags

The following restrictions apply to the AWS-generated tags:

- Only a management account can activate AWS-generated tags.
- You can't update, edit, or delete AWS-generated tags.
- AWS generated cost allocation tags aren't applied to resources that were created before the tag was activated.
- The maximum active tag keys for Billing and Cost Management reports is 500.
- AWS-generated tags are created using CloudTrail logs. CloudTrail logs over a certain size cause AWS-generated tag creation to fail.
- The reserved prefix is aws:

AWS-generated tag names and values are automatically assigned the aws: prefix, which you can't assign. AWS-generated tag names don't count towards the user-defined resource tag quota of 50. User-defined tag names have the prefix user: in the cost allocation report.

- Null tag values will not appear in Cost Explorer and AWS Budgets. If there is only one tag value that is also null, the tag key will also not appear in Cost Explorer or AWS Budgets.

User-defined cost allocation tags

User-defined tags are tags that you define, create, and apply to resources. After you have created and applied the user-defined tags, you can activate by using the Billing and Cost Management console for cost allocation tracking. Cost allocation tags appear on the console after you've enabled Cost Explorer, Budgets, AWS Cost and Usage Reports, or legacy reports. After you activate the AWS services, they appear on your cost allocation report. You can then use the tags on your cost allocation report to track your AWS costs. Tags are not applied to resources that were created before the tags were created.

Note

- As a best practice, reactivate your cost allocation tags when moving organizations. When an account moves to another organization as a member, previously activated cost allocation
tags for that account lose their "active" status and need to be activated again by the new management account.

- As a best practice, do not include sensitive information in tags.
- Only a management account in an organization and single accounts that aren’t members of an organization have access to the cost allocation tags manager in the Billing and Cost Management console.

### Applying user-defined cost allocation tags

For ease of use and best results, use the AWS Tag Editor to create and apply user-defined tags. The Tag Editor provides a central, unified way to create and manage your user-defined tags. For more information, see [Working with Tag Editor](https://aws.amazon.com/documentation/service/working-with-tag-editor/) in the AWS Resource Groups User Guide.

For supported services, you can also apply tags to resources using the API or the AWS Management Console. Each AWS service has its own implementation of tags. You can work with these implementations individually or use Tag Editor to simplify the process. For a full list of services that support tags, see [Supported Resources for Tag-based Groups](https://aws.amazon.com/documentation/service/supported-resources-for-tag-based-groups/) and [Resource Groups Tagging API Reference](https://aws.amazon.com/documentation/service/resource-groups-tagging-api-reference/).

**Note**
The behavior of cost allocation tags varies across AWS services. To learn more about the cost allocation tag behavior for a supported service, refer to the service’s documentation. For example, to learn more about using cost allocation tags with Amazon ECS, see [Tagging your Amazon ECS resources](https://aws.amazon.com/documentation/service/tagging-your-amazon-ecs-resources/) in the Amazon Elastic Container Service Developer Guide.

After you create and apply user-defined tags, you can activate them (p. 93) for cost allocation. If you activate your tags for cost allocation, it’s a good idea to devise a set of tag keys that represent how you want to organize your costs. Your cost allocation report displays the tag keys as additional columns with the applicable values for each row, so it’s easier to track your costs if you use a consistent set of tag keys.

Some services launch other AWS resources that the service uses, such as Amazon EMR launching an EC2 instance. If the supporting service (EC2) supports tagging, you can tag the supporting resources (such as the associated Amazon EC2 instance) for your report. For a full list of resources that can be tagged, use the Tag Editor to search. For more information about how to search for resources using Tag Editor, see [Searching for Resources to Tag](https://aws.amazon.com/documentation/service/searching-for-resources-to-tag/).

**Note**
AWS Marketplace line items are tagged with the associated Amazon EC2 instance tag.

### Activating user-defined cost allocation tags

For tags to appear on your billing reports, you must activate them. Your user-defined cost allocation tags represent the tag key, which you activate in the Billing console. Once you activate or deactivate the tag key, it will affect all tag values that share the same tag key. A tag key can have multiple tag values.

**Note**
You can also use the UpdateCostAllocationTagsStatus API operation to activate your tags in bulk. For more information, see the [AWS Billing and Cost Management API Reference](https://aws.amazon.com/documentation/service/aws-billing-and-cost-management-api-reference/).

**To activate your tag keys**

2. In the navigation pane, choose **Cost allocation tags**.
3. Select the tag keys that you want to activate.
4. Choose **Activate**.

After you create and apply user-defined tags to your resources, it can take up to 24 hours for the tag keys to appear on your cost allocation tags page for activation. It can then take up to 24 hours for tag keys to activate.

For an example of how tag keys appear in your billing report with cost allocation tags, see Viewing a cost allocation report (p. 95).

### User-defined tag restrictions

For basic tag restrictions, see Tag Restrictions in the Amazon EC2 User Guide.

The following restrictions apply to user-defined tags for Cost Allocation:

- **The reserved prefix is** `aws:`.
  
  AWS-generated tag names and values are automatically assigned the `aws:` prefix, which you can't assign. User-defined tag names have the prefix `user:` in the cost allocation report.

- **Use each key only once for each resource.** If you attempt to use the same key twice on the same resource, your request will be rejected.

- **In some services, you can tag a resource when you create it.** For more information, see the documentation for the service where you want to tag resources.

- **You can't backdate the application of a tag.** This means that tags only start appearing on your cost allocation report after you apply them and don't appear on earlier reports.

- **If you need characters outside of those listed in Tag Restrictions,** you can apply standard base-64 encoding to your tag. Billing and Cost Management does not encode or decode your tag for you.

- **User-defined tags on non-metered services can be activated (for example, Account Tagging).** However, these tags will not populate in the Cost Management suite because these services are not metered.

### Monthly cost allocation report

The monthly cost allocation report lists the AWS usage for your account by product category and linked account user. This report contains the same line items as the detailed AWS Cost and Usage Report and additional columns for your tag keys. We recommend that you use AWS Cost and Usage Report instead.

For more information about the monthly allocation report, see the following topics.

**Topics**

- Setting up a monthly cost allocation report (p. 94)
- Getting an hourly cost allocation report (p. 95)
- Viewing a cost allocation report (p. 95)

### Setting up a monthly cost allocation report

By default, new tag keys that you add using the API or the AWS Management Console are automatically excluded from the cost allocation report. You can add them using the procedures described in this topic.

When you select tag keys to include in your cost allocation report, each key becomes an additional column that lists the value for each corresponding line item. Because you might use tags for more than just your cost allocation report (for example, tags for security or operational reasons), you can include or
exclude individual tag keys for the report. This ensures that you’re seeing meaningful billing information that helps organize your costs. A small number of consistent tag keys makes it easier to track your costs. For more information, see Viewing a cost allocation report (p. 95).

**Note**

AWS stores billing reports in an Amazon S3 bucket that you create and own. You can retrieve these reports from the bucket using the Amazon S3 API, AWS Management Console for Amazon S3, or the AWS Command Line Interface. You can’t download the cost allocation report from the Account Activity page of the Billing and Cost Management console.

**To set up the cost allocation report and activate tags**

2. Under **Detailed billing reports (legacy)**, choose **Edit**, and then select **Legacy report delivery to S3**.
3. Choose **Configure an S3 bucket to activate** to specify where your reports are delivered.
4. In the **Configure S3 Bucket** dialog box, choose one of the following options:
   - To use an existing S3 bucket, choose **Use an existing S3 bucket**, and then select the S3 bucket.
   - To create a new S3 bucket, choose **Create a new S3 bucket**, and then for **S3 bucket name**, enter the name, and then choose the **Region**.
5. Choose Next.
6. Verify the default IAM policy and then select **I have confirmed that this policy is correct**.
7. Choose **Save**.
8. In the **Report** list, select the check box for **Cost allocation report**, and then choose **Activate**.
9. Choose **Manage Report Tags**.

   The page displays a list of tags that you’ve created using either the API or the console for the applicable AWS service. Tag keys that currently appear in the report are selected. Tag keys that are excluded aren’t selected.
10. You can filter tags that are **Inactive** in the dropdown list, and then select the tags that you want to activate for your report.
11. Choose **Activate**.

If you own the management account in an organization, your cost allocation report includes all the usage, costs, and tags for the member accounts. By default, all keys registered by member accounts are available for you to include or exclude from your report. The detailed billing report with resources and tags also includes any cost allocation tag keys that you select using the preceding steps.

**Getting an hourly cost allocation report**

The cost allocation report is one of several reports that AWS publishes to an Amazon S3 bucket several times a day.

**Note**

During the current billing period (monthly), AWS generates an estimated cost allocation report. The current month’s file is overwritten throughout the billing period until a final report is generated at the end of the billing period. Then a new file is created for the next billing period. The reports for the previous months remain in the designated Amazon S3 bucket.

**Viewing a cost allocation report**

The following example tracks the charges for several cost centers and applications. Resources (such as Amazon EC2 instances and Amazon S3 buckets) are assigned tags like "Cost Center"="78925" and "Application"="Widget1". In the cost allocation report, the user-defined tag keys have the prefix user,
such as `user:Cost Center` and `user:Application`. AWS-generated tag keys have the prefix `aws`. The keys are column headings identifying each tagged line item's value, such as "78925".

<table>
<thead>
<tr>
<th>Total Cost</th>
<th>user:Owner</th>
<th>user:Stack</th>
<th>user:Cost Center</th>
<th>user:Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.95</td>
<td>DbAdmin</td>
<td>Test</td>
<td>80432</td>
<td>Widget2</td>
</tr>
<tr>
<td>0.01</td>
<td>DbAdmin</td>
<td>Test</td>
<td>80432</td>
<td>Widget2</td>
</tr>
<tr>
<td>3.84</td>
<td>DbAdmin</td>
<td>Prod</td>
<td>80432</td>
<td>Widget2</td>
</tr>
<tr>
<td>6.00</td>
<td>DbAdmin</td>
<td>Test</td>
<td>78925</td>
<td>Widget1</td>
</tr>
<tr>
<td>234.63</td>
<td>SysEng</td>
<td>Prod</td>
<td>78925</td>
<td>Widget1</td>
</tr>
<tr>
<td>0.73</td>
<td>DbAdmin</td>
<td>Test</td>
<td>78925</td>
<td>Widget1</td>
</tr>
<tr>
<td>0.00</td>
<td>DbAdmin</td>
<td>Prod</td>
<td>80432</td>
<td>Portal</td>
</tr>
<tr>
<td>2.47</td>
<td>DbAdmin</td>
<td>Prod</td>
<td>78925</td>
<td>Portal</td>
</tr>
</tbody>
</table>

Pick your keys carefully so that you have a consistent hierarchy of values. Otherwise, your report won't group costs effectively, and you will have many line items.

**Note**

If you add or change the tags on a resource partway through a billing period, costs are split into two separate lines in your cost allocation report. The first line shows costs before the update, and the second line shows costs after the update.

### Unallocated resources in your report

Any charges that cannot be grouped by tags in your cost allocation report default to the standard billing aggregation (organized by Account/Product/Line Item) and are included in your report. Situations where you can have unallocated costs include:

- You signed up for a cost allocation report mid-month.
- Some resources aren't tagged for part, or all, of the billing period.
- You are using services that currently don't support tagging.
- Subscription-based charges, such as AWS Support and AWS Marketplace monthly fees, can't be allocated.
- One-time fees, such as Amazon EC2 Reserved Instance upfront charges, can't be allocated.

### Unexpected costs associated with tagged resources

You can use cost allocation tags to see what resources are contributing to your usage and costs, but deleting or deactivating the resources doesn't always reduce your costs. For more information on reducing unexpected costs, see [Avoiding unexpected charges](p. 7).

### Understanding dates for cost allocation tags

**Prerequisites**

To view these dates in the Cost allocation tags page of the AWS Billing console, you must have the `ce:ListCostAllocationTags` permission. For more information about updating your AWS Identity and Access Management (IAM) policies, see [Managing access permissions](p. 196).

When you use cost allocation tags, you can determine when the tags were last used or last updated with the following metadata fields:

- **Last updated date** – The last date that the tag key was either activated or deactivated for cost allocation.
For example, suppose that your tag key `lambda:createdby` changed from inactive to active on July 1, 2023. This means that the **Last updated date** column will show July 1, 2023.

- **Last used month** – The last month that the tag key was used on an AWS resource.

For example, suppose that your tag key `lambda:createdby` was last used on April 2023. The **Last used month** column will show April 2023. This means that the tag key hasn't been associated with any resource since that date.

**Notes**

- The **Last updated date** column appears empty for newly created tag keys that haven't been activated.
- The **Last used month** column shows **Before April 2023** for tag keys that were used before April 2023 and that aren't currently associated with any resource.
Using the AWS Free Tier

When you create an AWS account, you can try some AWS services free of charge within certain usage limits.

AWS Free Tier provides three types of offers:

Always free

These free tier offers don't expire and are available to all AWS customers.

12 months free

You can use these offers for 12 months following your initial sign up date to AWS.

Short-term trials

You can use a free tier limit each month for less than 12 months. Most short-term free trial offers start from the date that you activate a particular service.

To find services that offer AWS Free Tier benefits, types, and usage limits

1. Navigate to the AWS Free Tier page.
2. In the Free Tier details section, choose a filter to search for the tier type and product category.

For example, you can choose Always Free and choose Compute to learn about the number of free requests available for AWS Lambda (Lambda).

For more information about AWS Free Tier and on how to avoid charges while you’re eligible, see the following topics:

Topics
- Eligibility for the AWS Free Tier (p. 98)
- Avoiding unexpected charges after the AWS Free Tier (p. 99)
- Tracking your AWS Free Tier usage (p. 100)

Eligibility for the AWS Free Tier

Your AWS usage stays within the AWS Free Tier limits when all of these conditions are met:

• You’re within the active trial period for the AWS Free Tier offering. For example, within 12 months for a 12-month free type of service like Amazon Elastic Compute Cloud (Amazon EC2).
• You use only AWS services that offer AWS Free Tier benefits.
• Your usage stays within the AWS Free Tier limits of those services.

If you use AWS services beyond one or more of these conditions, then you're charged at the standard AWS billing rates for usage that exceeds the Free Tier limits.
To learn more about the AWS Free Tier limits, see AWS Free Tier.

**Note**
For AWS Organizations, the AWS Free Tier eligibility for all member accounts begins on the day that the management account is created. For more information, see the [AWS Organizations User Guide](https://docs.aws.amazon.com/organizations/latest/userguide/userguide.html).

## Avoiding unexpected charges after the AWS Free Tier

Your eligibility for the 12 month free service offering AWS Free Tier expires 12 months after you first activate your AWS account. You can’t extend your Free Tier eligibility after this time.

**Note**
You can continue to use Always Free offers, even after your AWS Free Tier eligibility expires. To learn more about available Always Free offers, see [AWS Free Tier](https://aws.amazon.com/free/).

As the expiration date of your AWS Free Tier eligibility approaches, we recommend that you shut down or delete any resources that you don’t need. After your eligibility expires, you’re charged at the standard AWS billing rates for usage.

For short-term trials, there are no expiration notification for these services. You will receive free tier alerts during the trial period only. To avoid unexpected costs in a short-term trial, you must turn off these resources before the end of the trial period.

Even if you aren’t regularly signing in to your account, you might have active resources running. Use the following procedure to identify your account’s active resources.

### To identify your active resources by using AWS Billing

1. Sign in to the AWS Management Console and open the Billing console at https://console.aws.amazon.com/billing/
2. On the navigation pane, choose Bills.
3. On the Charges by service tab, choose Expand all.
4. Review the list to find the services with active resources and by AWS Region, and the charges for each resource.

### To identify your active resources by using AWS Cost Explorer

2. On the navigation pane, choose Cost Explorer.
3. On the Cost and usage graph, note the services and AWS Regions with resources that you don’t need. For instructions on how to shut down or delete those resources, see the documentation for that service.
4. For example, to terminate an Amazon EC2 Linux instance, see the [Amazon EC2 User Guide for Linux Instances](https://docs.aws.amazon.com/AmazonEC2/latest/UserGuide/).

### Tip
You might decide to close your AWS account. To avoid generating future charges, we recommend that you retrieve the content you want to keep and shut down or delete any remaining resources before you close your account.
Closing your account might not automatically shut down or delete all your active resources and you might continue to incur charges. Review your content and resources across different AWS Regions.

For more information and important considerations, see Close your account in the AWS Account Management Reference Guide.

Tracking your AWS Free Tier usage

You can track your AWS Free Tier usage in the following ways:

- Turn on Free Tier usage alerts in Billing preferences. By default, AWS Free Tier usage alerts automatically notify you over email when you exceed 85 percent of the Free Tier limit for each service. You can also configure AWS Budgets to track your usage to 100 percent of the Free Tier limit by setting a zero spend budget using the template.
- Review your AWS Free Tier usage by using the Free Tier page in the Billing console.

Topics

- Using AWS Free Tier usage alerts (p. 100)
- Top AWS Free Tier services table (p. 101)
- Trackable AWS Free Tier services (p. 101)

Using AWS Free Tier usage alerts

You can use AWS Free Tier usage alerts to track and take action on your cost and usage. For more information about this feature, see Managing your costs with AWS Budgets.

AWS Free Tier usage alerts automatically notify you over email when you exceed 85 percent of your Free Tier limit for each service. For additional tracking, you can configure AWS Budgets to track your usage to 100% of the Free Tier limit by setting a zero spend budget using the template. You can also filter your budget to track individual services.

For example, you can set up a budget to send you an alert when you're forecasted to exceed 100 percent of the Free Tier limit for Amazon Elastic Block Store. To set up a usage budget, see Creating a usage budget.

AWS Free Tier usage alerts cover Free Tier offerings active in the current month, such as the first 25 GB of Amazon DynamoDB storage or the first 10 custom Amazon CloudWatch metrics. It's common to have all three types of AWS Free Tier offerings active within the first 12 months.

For example, you use Amazon EC2, Amazon SageMaker, and Amazon S3. You will see Free Tier usage for those usage types in the AWS Billing console, Free Tier page. After using SageMaker for two months, the short-term trial will end while Amazon EC2 and Amazon S3 continue. After 12 months from account creation, the Amazon EC2 12-month free period expires, but Amazon S3 will continue because the service offers Always free status.

When you exceed the Free Tier limit for a service, AWS sends an email to the email address that you used to create your account (the AWS account root user). To change the email address for AWS Free Tier usage alerts, see the following procedure:

To change the email address for AWS Free Tier usage alerts

2. Under Preferences in the navigation pane, choose Billing preferences.
3. For Alert preferences, choose Edit.
4. Enter the email address to receive the usage alerts.
5. Choose Update.

AWS Budgets usage alerts for 85 percent of the Free Tier limit are automatically activated for all individual AWS accounts, but not for a management account in an AWS Organizations. If you own a management account, you must opt in to get AWS Free Tier usage alerts. Use the following procedure to opt in or out of Free Tier usage alerts.

**To opt in or out of AWS Free Tier usage alerts**

1. Sign in to the AWS Management Console and open the Billing console at https://console.aws.amazon.com/billing/
2. Under Preferences in the navigation pane, choose Billing preferences.
3. For Alert preferences, choose Edit.
4. Select Receive AWS Free Tier alerts to opt in to Free Tier usage alerts. To opt out, clear Receive AWS Free Tier alerts.
5. Choose Update.

**Top AWS Free Tier services table**

If you’re eligible for the AWS Free Tier and you use an AWS Free Tier offering, you can track your usage with the Top AWS Free Tier Services by Usage table on the dashboard of the AWS Billing console. The dashboard shows your account’s top five AWS Free Tier service measurements.

To see more details about your AWS Free Tier usage, including all of your active Free Tier services, choose View all in the Top AWS Free Tier Services by Usage table. The detailed table includes additional information about your forecasted usage for each Free Tier service measurement.

The Top AWS Free Tier Service by Usage table is grouped by service limit. A service might have multiple lines, enabling you to track each AWS Free Tier limit closely. For example, each month you get 2,000 Amazon S3 Put operations and 5 GB of Amazon S3 storage. The AWS Free Tier usage table has two lines, one for S3 - Puts and one for S3 - Storage.

The following conditions might limit whether you see the Free Tier table data:

- You use an AWS service that doesn't offer a AWS Free Tier.
- Your AWS Free Tier has expired.
- You access AWS through an AWS Organizations member account.
- You use an AWS service in the AWS GovCloud (US-West) or AWS GovCloud (US-East) Regions.

**Trackable AWS Free Tier services**

With AWS, you can track how much you used AWS Free Tier services and what service usage types you used. Usage types are the specific type of usage that AWS tracks. For example, the usage type Global-BoxUsage:freetier.micro means that you used an Amazon EC2 micro instance.

The AWS Free Tier usage alerts and the Top AWS Free Tier Services by Usage table cover both expiring and non-expiring AWS Free Tier offerings. You can track the following services and usage types.
<table>
<thead>
<tr>
<th>Service</th>
<th>Usage type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alexa Web Information Service</td>
<td>AlexaWebInfoService::request</td>
</tr>
<tr>
<td></td>
<td>AlexaWebInfoService::Requests</td>
</tr>
<tr>
<td>Amazon API Gateway</td>
<td>Global-ApiGatewayRequest</td>
</tr>
<tr>
<td>Amazon AppStream</td>
<td>Global-stream-hrs:720p:g2</td>
</tr>
<tr>
<td></td>
<td>Global-stream.standard.large-ib</td>
</tr>
<tr>
<td>Amazon Cloud Directory</td>
<td>Global-Requests-Tier1</td>
</tr>
<tr>
<td></td>
<td>Global-Requests-Tier2</td>
</tr>
<tr>
<td></td>
<td>Global-TimedStorage-ByteHrs</td>
</tr>
<tr>
<td>Amazon CloudFront</td>
<td>Global-DataTransfer-Out-Bytes</td>
</tr>
<tr>
<td></td>
<td>Global-Requests-Tier1</td>
</tr>
<tr>
<td></td>
<td>Invalidations</td>
</tr>
<tr>
<td></td>
<td>Execution:Executions-CloudFrontFunctions</td>
</tr>
<tr>
<td>Amazon CloudWatch</td>
<td>Global-CW:Requests</td>
</tr>
<tr>
<td></td>
<td>Global-TimedStorage-ByteHrs</td>
</tr>
<tr>
<td></td>
<td>PutLogEvents:Global-DataProcessing-Bytes</td>
</tr>
<tr>
<td>Amazon Cognito</td>
<td>Global-CognitoUserPoolMAU</td>
</tr>
<tr>
<td>Amazon Cognito Sync</td>
<td>Global-CognitoSyncOperation</td>
</tr>
<tr>
<td></td>
<td>Global-TimedStorage-ByteHrs</td>
</tr>
<tr>
<td>Amazon Connect</td>
<td>USE1-end-customer-mins</td>
</tr>
<tr>
<td>AWS CodeBuild</td>
<td>Global-Build-Min:Linux:g1.small</td>
</tr>
<tr>
<td>Amazon GameLift</td>
<td>Global-BoxUsage:c5.large</td>
</tr>
<tr>
<td>AWS Storage Gateway</td>
<td>Global-Uploaded-Bytes</td>
</tr>
<tr>
<td>Amazon DynamoDB</td>
<td>TimedStorage-ByteHrs</td>
</tr>
<tr>
<td></td>
<td>GetRecords:AFS1-Streams-Requests</td>
</tr>
<tr>
<td>Amazon Elastic Compute Cloud (Amazon EC2)</td>
<td>Global-BoxUsage:freetier.micro</td>
</tr>
<tr>
<td></td>
<td>Global-BoxUsage:freetier.micro</td>
</tr>
<tr>
<td></td>
<td>Global-DataProcessing-Bytes</td>
</tr>
<tr>
<td></td>
<td>Global-EBS:SnapshotUsage</td>
</tr>
<tr>
<td></td>
<td>Global-EBS:VolumeI0Usage</td>
</tr>
<tr>
<td>Service</td>
<td>Usage type</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>Global-EBS:VolumeUsage</td>
<td></td>
</tr>
<tr>
<td>Global-LCUUsage</td>
<td></td>
</tr>
<tr>
<td>Global-LoadBalancerUsage</td>
<td></td>
</tr>
<tr>
<td>Amazon Elastic Container Registry (Amazon ECR)</td>
<td>Global-TimedStorage-ByteHrs</td>
</tr>
<tr>
<td>Amazon Elastic File System</td>
<td>Global-TimedStorage-ByteHrs</td>
</tr>
<tr>
<td>Amazon OpenSearch Service</td>
<td>Global-ES:freetier-Storage</td>
</tr>
<tr>
<td>Amazon OpenSearch Service</td>
<td>Global-ESInstance:freetier.micro</td>
</tr>
<tr>
<td>Amazon Elastic Transcoder</td>
<td>global-ets-audio-success</td>
</tr>
<tr>
<td>Amazon Elastic Transcoder</td>
<td>global-ets-hd-success</td>
</tr>
<tr>
<td>Amazon Elastic Transcoder</td>
<td>global-ets-sd-success</td>
</tr>
<tr>
<td>Amazon Forecast</td>
<td>Global-DataInjection</td>
</tr>
<tr>
<td>Amazon Forecast</td>
<td>Global-TrainingHours</td>
</tr>
<tr>
<td>Amazon Forecast</td>
<td></td>
</tr>
<tr>
<td>Amazon Fraud Detector</td>
<td>Global-BoxUsage:c3.large</td>
</tr>
<tr>
<td>Amazon Fraud Detector</td>
<td>Global-FlexMatchMatchmakingHrs</td>
</tr>
<tr>
<td>Amazon Fraud Detector</td>
<td>Global-FlexMatchPlayerPackages</td>
</tr>
<tr>
<td>Amazon Fraud Detector</td>
<td>Global-DailyActiveUser</td>
</tr>
<tr>
<td>Amazon GameLift</td>
<td>Global-CW:Requests</td>
</tr>
<tr>
<td>Amazon GameLift</td>
<td>Global-DataProcessing-Bytes</td>
</tr>
<tr>
<td>Amazon GameLift</td>
<td>Global-TimedStorage-ByteHrs</td>
</tr>
<tr>
<td>Amazon GameOn</td>
<td>API-Score-Free-Tier</td>
</tr>
<tr>
<td>Amazon GameSparks</td>
<td>Global-ExecutionTime-Code</td>
</tr>
<tr>
<td>Amazon GameSparks</td>
<td>Global-APIScore-Blocks</td>
</tr>
<tr>
<td>Amazon GameSparks</td>
<td>Global-APIScore-Code</td>
</tr>
<tr>
<td>Amazon GameSparks</td>
<td>Global-APIScore-CodeRead</td>
</tr>
<tr>
<td>Amazon GameSparks</td>
<td>Global-APIScore-CodeWrite</td>
</tr>
<tr>
<td>Amazon GameSparks</td>
<td>Global-APIScore-Tune</td>
</tr>
<tr>
<td>Amazon GameSparks</td>
<td>Global-Storage-Code</td>
</tr>
<tr>
<td>Amazon GameSparks</td>
<td>Global-Storage-Content</td>
</tr>
<tr>
<td>Amazon IVS</td>
<td>SUM-Global-Input-Basic-Hours</td>
</tr>
<tr>
<td>Amazon IVS</td>
<td>SUM-Global-Output-SD-Hours</td>
</tr>
<tr>
<td>Service</td>
<td>Usage type</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>Amazon Lex</td>
<td>Lex-Global-Speech-Requests</td>
</tr>
<tr>
<td></td>
<td>Lex-Global-Text-Requests</td>
</tr>
<tr>
<td>Amazon Lookout for Vision</td>
<td>Free-Inference</td>
</tr>
<tr>
<td></td>
<td>Free-Training</td>
</tr>
<tr>
<td>Amazon Macie</td>
<td>SensitiveDataDiscovery</td>
</tr>
<tr>
<td>Amazon MCS</td>
<td>Global-TimedStorage-ByteHrs</td>
</tr>
<tr>
<td></td>
<td>Global-ReadRequestUnits</td>
</tr>
<tr>
<td></td>
<td>Global-WriteRequestUnits</td>
</tr>
<tr>
<td>Amazon Neptune</td>
<td>DataTransfer-Out-Bytes</td>
</tr>
<tr>
<td>Amazon Pinpoint</td>
<td>Domain-Inboxplacement</td>
</tr>
<tr>
<td></td>
<td>MonthlyTargetedAudience</td>
</tr>
<tr>
<td></td>
<td>Predictive-Tests</td>
</tr>
<tr>
<td>Amazon Personalize</td>
<td>Global-DataIngestion</td>
</tr>
<tr>
<td></td>
<td>Global-TPS-hours</td>
</tr>
<tr>
<td></td>
<td>Global-TrainingHour</td>
</tr>
<tr>
<td></td>
<td>Predictive-Tests</td>
</tr>
<tr>
<td></td>
<td>EventsRecorded</td>
</tr>
<tr>
<td>Amazon Polly</td>
<td>Global-SynthesizeSpeech-Chars</td>
</tr>
<tr>
<td>Amazon Relational Database Service</td>
<td>Global-InstanceUsage:db.t1.micro</td>
</tr>
<tr>
<td></td>
<td>Global-RDS:StorageIOUsage</td>
</tr>
<tr>
<td>Amazon Rekognition</td>
<td>Global-FaceVectorsStored</td>
</tr>
<tr>
<td></td>
<td>Global-ImagesProcessed</td>
</tr>
<tr>
<td></td>
<td>Global-inferenceminutes</td>
</tr>
<tr>
<td></td>
<td>Global-MinutesOfVideoProcessed</td>
</tr>
<tr>
<td></td>
<td>Global-minutestrained</td>
</tr>
<tr>
<td>Amazon Route 53</td>
<td>Health-Check-AWS</td>
</tr>
<tr>
<td>Amazon Simple Storage Service (Amazon S3)</td>
<td>Global-Requests-Tier1</td>
</tr>
<tr>
<td></td>
<td>Global-Requests-Tier2</td>
</tr>
<tr>
<td></td>
<td>Global-TimedStorage-ByteHrs</td>
</tr>
</tbody>
</table>
## Trackable AWS Free Tier services

<table>
<thead>
<tr>
<th>Service</th>
<th>Usage type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Simple Email Service (Amazon SES)</td>
<td>Global-Message</td>
</tr>
<tr>
<td></td>
<td>Global-Recipients-MailboxSim-EC2</td>
</tr>
<tr>
<td>Amazon Simple Notification Service (Amazon SNS)</td>
<td>DeliveryAttempts-HTTP</td>
</tr>
<tr>
<td></td>
<td>DeliveryAttempts-SMTP</td>
</tr>
<tr>
<td></td>
<td>Requests-Tier1</td>
</tr>
<tr>
<td></td>
<td>Notifications-Mobile</td>
</tr>
<tr>
<td>Amazon States</td>
<td>Global-StateTransition</td>
</tr>
<tr>
<td>Amazon Simple Workflow Service (Amazon SWF)</td>
<td>Global-AggregateInitiatedActions</td>
</tr>
<tr>
<td></td>
<td>Global-AggregateInitiatedWorkflows</td>
</tr>
<tr>
<td></td>
<td>Global-AggregateWorkflowDays</td>
</tr>
<tr>
<td>Amazon Textract</td>
<td>Global-PagesforAnalyzeDocTables</td>
</tr>
<tr>
<td></td>
<td>Global-PagesforDocumentText</td>
</tr>
<tr>
<td>Amazon WorkLink</td>
<td>WorkLink-MAU</td>
</tr>
<tr>
<td>Amazon TTS</td>
<td>Global-SynthesizeSpeech-Chars</td>
</tr>
<tr>
<td>Amazon WorkSpaces</td>
<td>AutoStop-Usage</td>
</tr>
<tr>
<td></td>
<td>AutoStop-User</td>
</tr>
<tr>
<td>AWS Amplify</td>
<td>Global-BuildDuration</td>
</tr>
<tr>
<td></td>
<td>Global-DataStorage</td>
</tr>
<tr>
<td></td>
<td>Global-DataTransferOut</td>
</tr>
<tr>
<td>AWS Budgets</td>
<td>ActionEnabledBudgetsUsage</td>
</tr>
<tr>
<td>AWS CodeArtifact</td>
<td>Global-Requests</td>
</tr>
<tr>
<td></td>
<td>Global-TimedStorage-ByteHrs</td>
</tr>
<tr>
<td>AWS CodeCommit</td>
<td>User-Month</td>
</tr>
<tr>
<td>AWS CodePipeline</td>
<td>Global-activePipeline</td>
</tr>
<tr>
<td>AWS Database Migration Service</td>
<td>Global-InstanceUsg:dms.t2.micro</td>
</tr>
<tr>
<td></td>
<td>Global-SynthesizeSpeechNeural-Characters</td>
</tr>
<tr>
<td>AWS DataTransfer</td>
<td>Global-DataTransfer-Out-Bytes</td>
</tr>
<tr>
<td>AWS DeepRacer</td>
<td>TimedStorage-GigabyteHrs</td>
</tr>
<tr>
<td>Service</td>
<td>Usage type</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>AWS Glue</td>
<td>Global-Catalog-Request</td>
</tr>
<tr>
<td></td>
<td>Global-Catalog-Storage</td>
</tr>
<tr>
<td>AWS IoT</td>
<td>AWSIoT-messages</td>
</tr>
<tr>
<td>AWS KMS</td>
<td>Global-KMS-Requests</td>
</tr>
<tr>
<td>AWS Lambda</td>
<td>Global-Lambda-GB-Second</td>
</tr>
<tr>
<td></td>
<td>Global-Request</td>
</tr>
<tr>
<td>Amazon SQS</td>
<td>Global-Requests</td>
</tr>
<tr>
<td>AWS X-Ray</td>
<td>Global-XRay-TracesAccessed</td>
</tr>
<tr>
<td></td>
<td>Global-XRay-TracesStored</td>
</tr>
<tr>
<td>AWS Storage Gateway</td>
<td>Global-Uploaded-Bytes</td>
</tr>
<tr>
<td>AWS CodeBuild</td>
<td>Global-Build-Min:Linux:g1.small</td>
</tr>
<tr>
<td>Amazon Comprehend</td>
<td>Global-Comprehend-DC-Custom</td>
</tr>
<tr>
<td></td>
<td>Global-Comprehend</td>
</tr>
<tr>
<td></td>
<td>Global-Comprehend-Syntax</td>
</tr>
<tr>
<td></td>
<td>Global-DetectEvents</td>
</tr>
<tr>
<td></td>
<td>Global-DetectPiiEntities</td>
</tr>
<tr>
<td></td>
<td>Global-DetectTopics</td>
</tr>
<tr>
<td>Amazon Comprehend Medical</td>
<td>Global-CompMed-DetectEntities</td>
</tr>
<tr>
<td></td>
<td>Global-CompMed-DetectPHI</td>
</tr>
<tr>
<td>ContactCenterTelecomm</td>
<td>USE1-US-did-inbound-mins</td>
</tr>
<tr>
<td></td>
<td>USE1-US-outbound-mins</td>
</tr>
<tr>
<td></td>
<td>USE1-US-tollfree-inbound-mins</td>
</tr>
<tr>
<td>ContactLensAmazonConnect</td>
<td>ChatAnalytics:Global-ChatAnalytics</td>
</tr>
<tr>
<td></td>
<td>VoiceAnalytics:Global-VoiceAnalytics</td>
</tr>
<tr>
<td>AWS IoT Device Defender</td>
<td>global-Detect</td>
</tr>
<tr>
<td>AWS IoT Device Management</td>
<td>global-JobExecutions</td>
</tr>
<tr>
<td>Amazon Mobile Analytics</td>
<td>EventsRecorded</td>
</tr>
<tr>
<td>AWS OpsWorks</td>
<td>OpsWorks-Chef-Automate</td>
</tr>
</tbody>
</table>
What is AWS Price List?

To provide feedback about AWS Price List, complete this [short survey](#). Your responses will be anonymous. **Note:** This survey is in English only.

AWS Price List provides a catalog of the products and prices for AWS services that you can purchase on AWS.

This catalog includes always free offers from AWS Free Tier. This catalog doesn't include limited time or fixed usage based Free Tier products. For more information about Free Tier offers, see [Using the AWS Free Tier](#). Also, this catalog doesn't include Amazon Elastic Compute Cloud (Amazon EC2) Spot Instances. For more information about Amazon EC2 Spot Instances, see [Amazon EC2 Spot Instances](#).

To help you use the AWS Price List, the following are its key concepts:

**Service**

An AWS service, such as Amazon EC2 or Savings Plans. For example, a Savings Plan for Amazon EC2 might be `AWSComputeSavingsPlan` and a Savings Plan for machine learning (ML) might be `AWSMachineLearningSavingsPlans`.

**Product**

An entity sold by an AWS service. In the price list file, products are indexed by a unique stock keeping unit (SKU).

**Attribute**

The property associated with a product. This property consists of `AttributeName` and `AttributeValue`. Products can have multiple attributes. Each attribute has one `AttributeName` and a list of applicable `AttributeValue`

You can use the following AWS Price List APIs:

**AWS Price List Query API (p. 108)**

This API provides a centralized and convenient way to programmatically query AWS for services, products, and pricing information.

The Price List Query API uses product attributes and provides prices at the SKU level. Use this API to build cost control and scenario planning tools, reconcile billing data, forecast future spend for budgeting purposes, and provide cost benefit analyses that compare your internal workloads with AWS.

**Note**

The Price List Query API doesn't support Savings Plan prices.

**AWS Price List Bulk API (p. 114)**

This API provides a way to programmatically fetch up-to-date pricing information on current AWS services and products in bulk by using the price list files. The price list files are available in JSON and CSV formats. The price list files are organized by AWS service and AWS Region.
Use the AWS Price List Query API

Note

The Price List Query API and Price List Bulk API provide pricing details for informational purposes only. If there's a difference between the price list file and a service pricing page, AWS charges the prices on the service pricing page. For more information about AWS service pricing, see AWS Pricing.

To call the AWS Price List APIs, we recommend that you use an AWS SDK that supports your preferred programming language. AWS SDKs save you time and simplify the process of signing requests. You can also integrate the AWS SDKs with your development environment and access the related commands.

For more information, see the following topics:

- AWS Billing and Cost Management API Reference
- Language-specific AWS SDKs
- Tools for Amazon Web Services

Using the AWS Price List Query API

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. Note: This survey is in English only.

We recommend that you use the Price List Query API when you want to:

- Find pricing information about a product.
- Search for products and rates that match your filters.
- Quickly find products and prices that you need when you're developing applications that have limited resources, such as front-end environments.

Topics

- IAM permissions (p. 108)
- Endpoints (p. 109)
- Quotas (p. 109)
- Finding services and products (p. 110)

IAM permissions

An AWS Identity and Access Management (IAM) identity, such as a user or role, must have permission to use the Price List Query API. To grant access, use the following IAM policy.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "pricing:DescribeServices",
            "pricing:GetAttributeValues",
            "pricing:GetProducts"
         ],
         "Resource": [
```
Endpoints

The Price List Query API provides the following endpoints:

- https://api.pricing.us-east-1.amazonaws.com
- https://api.pricing.eu-central-1.amazonaws.com
- https://api.pricing.ap-south-1.amazonaws.com

The AWS Region is the API endpoint for the Price List Query API. The endpoints aren't related to product or service attributes.

To call the Price List Query API, see the following examples.

Java

In the following example, specify the \textit{region\_name} and use it to create the PricingClient.

```java
public class Main {
    public static void main(String[] args) {
        // Create pricing client
        PricingClient client = PricingClient.builder()
            .region(Region.US_EAST_1) // or Region.AP_SOUTH_1
            .credentialsProvider(DefaultCredentialsProvider.builder().build())
            .build();
    }
}
```

AWS Command Line Interface

Specify the Region with the following command.

```bash
aws pricing describe-services --region us-east-1
```

Quotas

Some Price List Query API operations are throttled by using a token bucket scheme to maintain service availability. These quotas are per AWS account on a per Region basis. The following table shows the quotas for each API operation.

<table>
<thead>
<tr>
<th>API operation</th>
<th>Token bucket size</th>
<th>Refill rate per second</th>
</tr>
</thead>
<tbody>
<tr>
<td>DescribeServices</td>
<td>10</td>
<td>5</td>
</tr>
</tbody>
</table>
For more information about service quotas (formerly referred to as limits), see AWS service quotas in the AWS General Reference.

Finding services and products

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. Note: This survey is in English only.

To find AWS services, their products, and the product attributes and prices, see the following steps.

Topics
• Step 1: Finding available AWS services (p. 110)
• Step 2: Finding available values for attributes (p. 111)
• Step 3: Finding products from attributes (p. 112)

Step 1: Finding available AWS services

Once you find the service, you can then get its attributes by using the DescribeServices API operation. If you know the service code, you can also use the AWS Price List Query API to get attributes for a service. Then, you can use the service attributes to find the products that meet your requirements based on the attribute values.

Examples: Find services

The following AWS Command Line Interface (AWS CLI) commands show how to find services.

Example Example: Find all services

```bash
aws pricing describe-services --region us-east-1
```

Response

```json
{
    "FormatVersion": "aws_v1",
    "NextToken": "abcdefg123",
    "Services": [
        {
            "AttributeNames": [
                "volumeType",
                "maxIopsVolume",
                "instanceCapacity10xlarge",
            ],
```
Example Example: Find service metadata for Amazon Elastic Compute Cloud (Amazon EC2)

The following command shows how to find service metadata for Amazon EC2.

```
aws pricing describe-services --region us-east-1 --service-code AmazonEC2
```

Response

```
{
  "FormatVersion": "aws_v1",
  "NextToken": "abcdefg123",
  "Services": [
    {
      "AttributeNames": [
        "productFamily",
        "volumeType",
        "engineCode",
        "memory"
      ],
      "ServiceCode": "AmazonEC2"
    }
  ]
}
```

The AWS Region is the API endpoint for the Price List Query API. The endpoints aren't related to product or service attributes.

For more information, see DescribeServices in the AWS Billing and Cost Management API Reference.

**Step 2: Finding available values for attributes**

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. **Note:** This survey is in English only.

In step 1 (p. 110), you retrieved a list of attributes for an AWS service. In this step, you use these attributes to search for products. In step 3, you need the available values for these attributes.

To find the values for an attribute, use the GetAttributeValues API operation. To call the API, specify the AttributeName and ServiceCode parameters.
Example: Get attribute values

The following AWS Command Line Interface (AWS CLI) command shows how to get attribute values for an AWS service.

Example Example: Find attribute values for Amazon Relational Database Service (Amazon RDS)

```bash
aws pricing get-attribute-values --service-code AmazonRDS --attribute-name operation --region us-east-1
```

Response

```
{
  "AttributeValues": [
    {
      "Value": "CreateDBInstance:0002"
    },
    {
      "Value": "CreateDBInstance:0003"
    },
    {
      "Value": "CreateDBInstance:0004"
    },
    {
      "Value": "CreateDBInstance:0005"
    }
  ],
  "NextToken": "abcdefg123"
}
```

The AWS Region is the API endpoint for the Price List Query API. The endpoints aren't related to product or service attributes.

For more information, see GetAttributeValues and language-specific AWS SDKs in the AWS Billing and Cost Management API Reference.

Step 3: Finding products from attributes

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. Note: This survey is in English only.

In this step, you use the information from step 1 (p. 110) and step 2 (p. 111) to find the products and their terms. To get information about products, use the GetProducts API operation. You can specify a list of filters to return the products that you want.

Note

The Price List Query API supports only "AND" matching. The response to your command only contains products that match all specified filters.

Examples: Find products from attributes

The following AWS Command Line Interface (AWS CLI) commands show how to find products by using attributes.

Example Example: Find products with specified filters

The following command shows how you can specify filters for Amazon Relational Database Service (Amazon RDS).
aws pricing get-products --service-code AmazonRDS --region us-east-1 --filters
Type=TERM_MATCH,Field=operation,Value="CreateDBInstance:0002"

Response

```json
{
   "FormatVersion": "aws_v1",
   "PriceList": [
      {
         "product": {
            "productFamily": "Database Instance",
            "attributes": {
               "engineCode": "2",
               "enhancedNetworkingSupported": "Yes",
               "memory": "64 GiB",
               "dedicatedEbsThroughput": "2000 Mbps",
               "vcpu": "16",
               "locationType": "AWS Region",
               "storage": "EBS Only",
               "instanceFamily": "General purpose",
               "regionCode": "us-east-1",
               "operation": "CreateDBInstance:0002",
               ...
            },
            "sku": "22ANV4NNQP3UUCWY",
            "serviceCode": "AmazonRDS",
            "terms": [...]}
      },
   "NextToken": "abcd1234"
}
```

Example Example: Use the filters.json file to specify filters

The following command shows how you can specify a JSON file that contains all filters.

```bash
aws pricing get-products --service-code AmazonRDS --region us-east-1 --filters file://filters.json
```

For example, the filters.json file might include the following filters.

```json
[
   {
      "Type": "TERM_MATCH",
      "Field": "operation",
      "Value": "CreateDBInstance:0002"
   }
]
```

The following example shows how you can specify more than one filter.

```json
[
   {
      "Type": "TERM_MATCH",
      "Field": "AttributeName1",
      "Value": "AttributeValue1"
   },
   {
      "Type": "TERM_MATCH",
      "Field": "AttributeName2",
      "Value": "AttributeValue2"
   }
]
```
Use the AWS Price List Bulk API

Response

```
{
  "FormatVersion": "aws_v1",
  "PriceList": [{
    "product": {
      "productFamily": "Database Instance",
      "attributes": {
        "engineCode": "2",
        "enhancedNetworkingSupported": "Yes",
        "memory": "64 GiB",
        "dedicatedEbsThroughput": "2000 Mbps",
        "vcpu": "16",
        "locationType": "AWS Region",
        "storage": "EBS Only",
        "instanceFamily": "General purpose",
        "regionCode": "us-east-1",
        "operation": "CreateDBInstance:0002",
        ...
      },
      "sku": "22ANV4NNQP3UUCWY",
      "serviceCode": "AmazonRDS",
      "terms": {...}
    },
    "NextToken": "abcd1234"
  }
}
```

For more information, see the following topics:

- [GetProducts](#) and [language-specific AWS SDKs](#) in the [AWS Billing and Cost Management API Reference](#)
- [Reading the service price list files](#)
- [Finding prices in the service price list file](#)

Using the AWS Price List Bulk API

To provide feedback about AWS Price List, complete this [short survey](#). Your responses will be anonymous. **Note:** This survey is in English only.

We recommend that you use the Price List Bulk API when you want to do the following tasks:

- Consume large amounts of product and pricing information for AWS services.
- Consume product and pricing information with a high throughput for an AWS service, such as processing in bulk.

Also, when the Price List Query API doesn't provide sufficient throughput and quotas for your use case, use the Price List Bulk API.

**Topics**

- [IAM permissions](#)
- [Endpoints](#)
- [Quotas](#)
IAM permissions

An AWS Identity and Access Management (IAM) identity, such as a user or role, must have permission to use the Price List Bulk API. To grant access, use the following IAM policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "pricing:DescribeServices",
        "pricing:GetPriceListFileUrl",
        "pricing:ListPriceLists"
      ],
      "Resource": ["*"
      ]
    }
  ]
}
```

**Note**

This policy only grants access to the Price List Bulk API. To also grant access to the Price List Query API, see the example Find products and prices (p. 186) IAM policy.

Endpoints

The Price List Bulk API provides the following endpoints:

- https://api.pricing.us-east-1.amazonaws.com
- https://api.pricing.eu-central-1.amazonaws.com
- https://api.pricing.ap-south-1.amazonaws.com

The AWS Region is the API endpoint for the Price List Bulk API. The endpoints aren't related to product or service attributes.

To call the Price List Bulk API, see the following examples.

Java

In the following example, specify the `region_name` and use it to create the `PricingClient`.

```java
public class Main {
    public static void main(String[] args) {

        // Create pricing client
        PricingClient client = PricingClient.builder()
                .region(Region.US_EAST_1) // or Region.AP_SOUTH_1
                .credentialsProvider(DefaultCredentialsProvider.builder().build())
                .build();
    }
}
```
Quotas

Some Price List Bulk API operations are throttled by using a token bucket scheme to maintain service availability. These quotas are per AWS account on a per Region basis. Quotas for each API operation are shown in the following table.

<table>
<thead>
<tr>
<th>API operation</th>
<th>Token bucket size</th>
<th>Refill rate per second</th>
</tr>
</thead>
<tbody>
<tr>
<td>DescribeServices</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>GetPriceListFileUrl</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>ListPriceLists</td>
<td>10</td>
<td>5</td>
</tr>
</tbody>
</table>

For more information about service quotas (formerly referred to as limits), see AWS service quotas in the AWS General Reference.

Getting price list files

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. Note: This survey is in English only.

We recommend that you use the AWS Price List Bulk API to find and download price list files programmatically.

To get the URL of the price list files, see the following steps:

Topics

- [Step 1: Finding available AWS services](p. 116)
- [Step 2: Finding price list files for an available AWS service](p. 117)
- [Step 3: Getting a specific price list file](p. 119)

If you don't want to use the AWS Price List Bulk API, you can download the price list files manually. For more information, see Getting price list files manually.

Step 1: Finding available AWS services

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. Note: This survey is in English only.
Use the DescribeServices API operation to find all available AWS services that the Price List Bulk API supports. This API operation returns the ServiceCode value from the list of services. You use this value later to find relevant price list files.

**Example Example: Find available services**

The following command shows how to find available AWS services.

```bash
aws pricing describe-services --region us-east-1
```

The AWS Region is the API endpoint for the Price List Bulk API. The endpoints aren't related to product or service attributes.

**Response**

```json
{
    "FormatVersion": "aws_v1",
    "NextToken": "abcdefg123",
    "Services": [
        {
            "AttributeNames": [
                "volumeType",
                "maxIopsvolume",
                "instanceCapacity10xlarge",
                "locationType",
                "operation"
            ],
            "ServiceCode": "AmazonEC2"
        },
        {
            "AttributeNames": [
                "productFamily",
                "volumeType",
                "engineCode",
                "memory"
            ],
            "ServiceCode": "AmazonRDS"
        },
        {...}
    ]
}
```

For more information about this API operation, see [DescribeServices](http://aws.amazon.com/documentation) and [language-specific AWS SDKs](http://aws.amazon.com/documentation) in the [AWS Billing and Cost Management API Reference](http://aws.amazon.com/documentation).

**Step 2: Finding price list files for an available AWS service**

To provide feedback about AWS Price List, complete this [short survey](http://aws.amazon.com/documentation). Your responses will be anonymous. **Note:** This survey is in English only.

Use the ListPriceLists API operation to get a list of price list references that you have permission to view. To filter your results, you can specify the ServiceCode, CurrencyCode, and EffectiveDate parameters.

The AWS Region is the API endpoint for the Price List Bulk API. The endpoints aren't related to product or service attributes.
Examples to find price list files

Example Example: Find price list files for all AWS Regions

If you don't specify the --region-code parameter, the API operation returns price list file references from all available AWS Regions.

```
aws pricing list-price-lists --service-code AmazonRDS --region us-east-1 --currency-code USD --effective-date "2023-04-03 00:00"
```

Response

```
{
   "NextToken": "abcd1234",
   "PriceLists": [
      {
         "CurrencyCode": "USD",
         "FileFormats": [ "json", "csv" ],
         "PriceListArn": "arn:aws:pricing:::price-list/aws/AmazonRDS/USD/20230328234721/us-east-1",
         "RegionCode": "us-east-1"
      },
      {
         "CurrencyCode": "USD",
         "FileFormats": [ "json", "csv" ],
         "PriceListArn": "arn:aws:pricing:::price-list/aws/AmazonRDS/USD/20230328234721/us-east-1",
         "RegionCode": "us-east-1"
      },
      ...
   ]
}
```

Example Example: Find price list files for a specific Region

If you specify the RegionCode parameter, the API operation returns price list file references that are specific to that Region. To find historical price list files, use the EffectiveDate parameter. For example, you can specify a date in the past to find a specific price list file.

From the response, you can then use the PriceListArn value with the GetPriceListFileUrl API operation to get your preferred price list files.

```
aws pricing list-price-lists --service-code AmazonRDS --region us-east-1 --currency-code USD --region-code us-east-1 --effective-date "2023-04-03 00:00"
```

Response

```
{
   "PriceLists": [
      {
         "CurrencyCode": "USD",
         "FileFormats": [ "json", "csv" ],
         "PriceListArn": "arn:aws:pricing:::price-list/aws/AmazonRDS/USD/20230328234721/us-east-1",
         "RegionCode": "us-east-1"
      }
   ]
}
```
For more information about this API operation, see ListPriceLists and language-specific AWS SDKs in the AWS Billing and Cost Management API Reference.

**Step 3: Getting a specific price list file**

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. Note: This survey is in English only.

Use the GetPriceListFileUrl API operation to get a URL for a price list file. This URL is based on the PriceListArn and FileFormats values that you retrieved from the ListPriceLists response in step 1 (p. 116) and step 2 (p. 117)

**Example Example: Get a specific price list file**

The following command gets the URL for a specific price list file for Amazon RDS.

```bash
aws pricing get-price-list-file-url --price-list-arn arn:aws:pricing::price-list/aws/AmazonRDS/USD/20230328234721/us-east-1 --file-format json --region us-east-1
```

**Response**

```json
{
  "Url": "https://pricing.us-east-1.amazonaws.com/offers/v1.0/aws/AmazonRDS/20230328234721/us-east-1/index.json"
}
```

From the response, you can use the URL to download the price list file.

For more information about this API operation, see the following topics:

- GetPriceListFileUrl and language-specific AWS SDKs in the AWS Billing and Cost Management API Reference
- Reading the price list files (p. 123)

**Getting price list files manually**

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. Note: This survey is in English only.

We recommend that you use the AWS Price List Bulk API to find and download price list files programmatically. For more information, see Getting price list files (p. 116).

If you don't want to use the AWS Price List Bulk API, you can download the price list files manually. You can skip to the relevant topics if you already have the information that you need.

**Topics**

- Step 1: Finding available AWS services (p. 120)
- Step 2: Finding available versions for an AWS service (p. 120)
- Step 3: Finding available AWS Regions for a version of an AWS service (p. 121)
- Step 4: Finding available price lists for an AWS Region and version of an AWS service (p. 121)
Step 1: Finding available AWS services

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. Note: This survey is in English only.

You can use the service index file to find available AWS services and Savings Plans that are provided by the AWS Price List Bulk API.

To download the service index file, navigate to the following URL.

https://pricing.us-east-1.amazonaws.com/offers/v1.0/aws/index.json

In the service index file, you can search for the service to find its prices. To download the service-specific price list file, use either the offerCode or serviceCode.

For more information, see the following topics:

• Reading the service index file (p. 124)
• Finding services and products (p. 110)

Step 2: Finding available versions for an AWS service

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. Note: This survey is in English only.

For an AWS service or Savings Plan that you retrieved in step 1 (p. 120), you can find all the historical versions of the price lists by using the service version index file (p. 125).

To download the service version index file, use the serviceCode or savingsPlanCode. To find the values for serviceCode and savingsPlanCode, see Finding services and products (p. 110).

To download the service version index file for an AWS service, navigate to the following URL. Replace <serviceCode> with your own information.

https://pricing.us-east-1.amazonaws.com/offers/v1.0/aws/<serviceCode>/index.json

For example, Amazon Elastic Compute Cloud (Amazon EC2) appears in a URL like the following URL.

https://pricing.us-east-1.amazonaws.com/offers/v1.0/aws/AmazonEC2/index.json

Note
In addition to the versions available in the service version index file, there is another version named current. The current version points to the latest version of the price list files for a specific AWS service.

To download the latest service version index file for Savings Plan, specify savingsPlanCode and current in the URL. Replace <savingsPlanCode> with your own information.

https://pricing.us-east-1.amazonaws.com/savingsPlan/v1.0/aws/<savingsPlanCode>/current/index.json
For example, the current version of AWSComputeSavingsPlan and
AWSMachineLearningSavingsPlans appears like the following URLs.

https://pricing.us-east-1.amazonaws.com/savingsPlan/v1.0/aws/AWSComputeSavingsPlan/current/index.json

https://pricing.us-east-1.amazonaws.com/savingsPlan/v1.0/aws/AWSMachineLearningSavingsPlans/current/index.json

For more information, see Reading the service index file (p. 124).

**Step 3: Finding available AWS Regions for a version of an AWS service**

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. **Note:** This survey is in English only.

For a version of an AWS service or Savings Plan in the previous step (p. 120), you can find all the AWS Regions and edge locations in which an AWS service provides products for purchase.

To download the service Region index file for an AWS service, navigate to the following URL. Replace `<serviceCode>` and `<version>` with your own information.

https://pricing.us-east-1.amazonaws.com/offers/v1.0/aws/<serviceCode>/<version>/region_index.json

For example, the service code for AmazonRDS and its current version has the following URL.

https://pricing.us-east-1.amazonaws.com/offers/v1.0/aws/AmazonRDS/current/region_index.json

To download the service Region index file for Savings Plan, navigate to the following URL. Replace `<savingsPlanCode>` with your own information.

https://pricing.us-east-1.amazonaws.com/savingsPlan/v1.0/aws/<savingsPlanCode>/current/region_index.json

For example, a Savings Plan for AWSComputeSavingsPlan and its current version has the following URL.

https://pricing.us-east-1.amazonaws.com/savingsPlan/v1.0/aws/AWSComputeSavingsPlan/current/region_index.json

For more information, see Reading the service Region index file (p. 128).

**Step 4: Finding available price lists for an AWS Region and version of an AWS service**

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. **Note:** This survey is in English only.
In the previous steps, you retrieved the following information about an AWS service:

- Service code
- Savings Plan code
- Version
- AWS Regions

Next, you can use this information to find the prices in the service price list files. These files are available in JSON and CSV formats.

Contents

- Finding service price list files (p. 122)
- Finding service price list files for Savings Plan (p. 123)

Finding service price list files

The service price list file provides the service related details, such as the following:

- The effective date of the prices in that file
- The version of the service price list
- The list of offered products and their details, along with prices in JSON and CSV formats

In the following URLs, you can change the URL to specify the format that you want (JSON or CSV).

To download the service price list file, navigate to the following URL. Replace each user input placeholder with your own information.

```
https://pricing.us-east-1.amazonaws.com/offers/v1.0/aws/<serviceCode>/<version>/<regionCode>/index.<format>
```

The following examples are for Amazon Relational Database Service (Amazon RDS). This service appears as AmazonRDS in the URL.

**Example Example: Current version of the price list file for Amazon RDS**

To get the current version of the price list file for Amazon RDS in the US East (Ohio) Region, use the following URL.

CSV format

```
https://pricing.us-east-1.amazonaws.com/offers/v1.0/aws/AmazonRDS/current/us-east-2/index.csv
```

JSON format

```
https://pricing.us-east-1.amazonaws.com/offers/v1.0/aws/AmazonRDS/current/us-east-2/index.json
```

**Example Example: Specific version of the price list file for Amazon RDS**

To get the specific version of the price list file for Amazon RDS in the US East (Ohio) Region, use the following URL.
CSV format

https://pricing.us-east-1.amazonaws.com/offers/v1.0/aws/AmazonRDS/20230328234721/us-east-2/index.csv

JSON format

https://pricing.us-east-1.amazonaws.com/offers/v1.0/aws/AmazonRDS/20230328234721/us-east-2/index.json

Finding service price list files for Savings Plan

The service price list file for Savings Plan provides Savings Plan related details, such as the following:

• The effective date of the prices in that file
• The version of the service price list
• The list of offered products and their details, along with prices in JSON and CSV formats

In the following URLs, you can change the URL to specify the format that you want (JSON or CSV).

To download the service price list files for Savings Plan, use the following URL. Replace each user input placeholder with your own information.


Example Example: Service price list file for Amazon SageMaker

To get a specific version (20230509202901) of the price list file for SageMaker (AWSComputeSavingsPlan) in the US East (Ohio) Region, use the following URL.

CSV format


JSON format


For more information, see Reading the service price list files (p. 131).

Reading the price list files

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. Note: This survey is in English only.

To learn more about price list files in detail, see the following topics:

Topics
Reading the service index file

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. Note: This survey is in English only.

After you have the service index file, you can use it to find an service price list file.

The service index file is available as a JSON file. To read the file, you can use a text application or a program that parses the JSON.

The service index file has two main sections:

- Metadata about the service index file
- Either a list of the services that AWS offers (for the service index file) and a list of AWS Regions where a service is offered (for the service Region index file)

The information about the service index file includes the URL where you can download the prices and a URL for the service Region index file for that service.

Contents
- Example: Service index file (p. 124)
- Service index file definitions (p. 125)

Example: Service index file

The service index file looks like the following.

```json
{
  "formatVersion":"The version number for the offer index format",
  "disclaimer":"The disclaimers for this offer index",
  "publicationDate":"The publication date of this offer index",
  "offers":{
    "firstService":{
      "offerCode":"The service that this price list is for",
      "currentVersionUrl":"The URL for this offer file",
      "currentRegionIndexUrl":"The URL for the regional offer index file",
      "savingsPlanVersionIndexUrl":"The URL for the Savings Plan index file (if applicable)"
    },
    "secondService":{
      "offerCode": ...,
      "currentVersionUrl": ...,
      "currentRegionIndexUrl": ...,
      "savingsPlanVersionIndexUrl": ...
    },
    ...
  }
}
```
Service index file definitions

The following list defines the terms that are used in the service index file:

**FormatVersion**

An attribute that tracks which format version the service version index file is in. The formatVersion of the file is updated when the structure is changed. For example, the version will change from v1 to v2.

**Disclaimer**

Any disclaimers that apply to the service version index file.

**PublicationDate**

The date and time in UTC format when a service version index file was published. For example, this might look like 2015-04-09T02:05Z and 2015-09-10T18:21:05Z.

**Offers**

A list of available service price list files.

**Offers:OfferCode**

A unique code for the product of an AWS service. For example, this might be AmazonEC2 or AmazonS3. The OfferCode is used as the lookup key for the index.

**Offers:CurrentVersionUrl**

The URL where you can download the most up-to-date service price list file.

**Offers:currentRegionIndexUrl**

A list of available service price list files by Region.

**Offers:savingsPlanVersionIndexUrl**

The list of applicable Savings Plan offers.

Reading the service version index file

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. **Note:** This survey is in English only.

The service version index file is available in JSON format. To read the file, you can use a text program or an application that parses the JSON.

The service version index file consists of two main sections:

- Metadata about the service version index file
- List of all versions of price list files available for an AWS service

The information about a service version includes the URL that you can use to download the prices for that service for the specified time period.

**Topics**

- Service version index file for an AWS service (p. 126)
• Service version index file for Savings Plan (p. 127)

Service version index file for an AWS service

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. Note: This survey is in English only.

To understand the service version index file, see the following references:

Topics
• Example: Service version index file for a service (p. 126)
• Service version index file definitions (p. 126)

Example: Service version index file for a service

The service version index file looks like the following.

```json
{
  "formatVersion":"The version number for the service version index format",
  "disclaimer":"The disclaimers for this service version index",
  "publicationDate":"The publication date of this service version index",
  "offerCode": "The service code/Savings Plan code",
  "currentVersion": "The latest version of the service"
  "versions":{
    "firstVersion":{
      "versionEffectiveBeginDate":"The date starting which this version is effective",
      "versionEffectiveEndDate":"The date until which this version is effective",
      "offerVersionUrl": "The relative URL for the service price list file of this version"
    },
    "secondVersion":{
      "versionEffectiveBeginDate": ...,
      "versionEffectiveEndDate": ...,
      "offerVersionUrl": ...
    },
    ...
  }
}
```

Service version index file definitions

The following list defines the terms in the service version index file.

**formatVersion**

An attribute that tracks which format version the service version index file is in. The formatVersion of the file is updated when the structure is changed. For example, the version will change from v1 to v2.

**disclaimer**

Any disclaimers that apply to the service version index file.

**publicationDate**

The date and time in UTC format when a service version index file was published. For example, 2023-03-28T23:47:21Z.
offerCode

A unique code for the product of an AWS service. For example, AmazonRDS or AmazonS3.

currentVersion

The latest version number of the AWS service. For example, 20230328234721.

versions

The list of available versions for this AWS service.

versions:version

A unique code for the version of a price list for an AWS service. This is used as the lookup key in the versions list. For example, 20230328234721,

versions:version:versionEffectiveBeginDate

The start date and time in UTC format, which this version is effective. For example, 2023-03-28T23:47:21Z.

versions:version:versionEffectiveEndDate

The end date and time in UTC format, which this version is effective. For example, 2023-03-28T23:47:21Z. If this property isn't set, this means that this version is the currently active version.

versions:version:offerVersionUrl

The relative URL for the service price list files of the version. For example, /offers/v1.0/aws/AmazonRDS/20230328234721/index.json.

Service version index file for Savings Plan

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. Note: This survey is in English only.

To understand the service version index file for Savings Plan, see the following references:

Contents

- Example: Service version index file for Savings Plan (p. 127)
- Service version index definitions (p. 128)

Example: Service version index file for Savings Plan

The service version index file for a Savings Plan looks like the following.

```
{
  "disclaimer":"The disclaimers for this service version index",
  "publicationDate":"The publication date of this service version index",
  "currentOfferVersionUrl":"The relative URL of region index file for latest version number of the service",
  "versions":[
    {
      "publicationDate":"The publication date of this version of service from which this version was effective",
      "offerVersionUrl":"The relative URL for the service region index file of this version"
    }
  ]
}
```
Service version index definitions

The following list defines the terms in the service version index file.

**disclaimer**

Any disclaimers that apply to the service version index file.

**publicationDate**

The date and time in UTC format when a service version index file was published. For example, 2023-03-28T23:47:21Z.

**currentOfferVersionUrl**

The relative URL of the regional index file for latest version number of the service. For example, /savingsPlan/v1.0/aws/AWSComputeSavingsPlan/current/region_index.json.

**versions**

The list of available version for this AWS service.

**versions:version:publicationDate**

The date and time in UTC format when an service version index file was published. For example, 2023-04-07T14:57:05Z.

**versions:version:offerVersionUrl**

The relative URL for the service regional index file of this version. For example, /savingsPlan/v1.0/aws/AWSComputeSavingsPlan/20230407145705/region_index.json.

Reading the service Region index file

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. **Note:** This survey is in English only.

The service Region index file is available in JSON format. To read the file, you can use a text program or an application that parses the JSON.

The service Region index file consists of two main sections:

- Metadata about the service Region index file
- List of all AWS Regions in which AWS services or Savings Plan are available

The information about a service Region includes the URL where you can download the prices for that service for the specified time period and Region.

**Topics**

- [Service Region index file for AWS services](p. 129)
Service Region index file for AWS services

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. Note: This survey is in English only.

To understand the service version index file for AWS services, see the following references:

Contents

- Example: Service Region index file for an AWS service (p. 129)
- Service Region index definitions (p. 129)

Example: Service Region index file for an AWS service

The service Region index file for an AWS service looks like the following.

```
{
    "formatVersion":"The version number for the service region index format",
    "disclaimer":"The disclaimers for this service region index",
    "publicationDate":"The publication date of this service region index",
    "regions":{
        "firstRegion":{
            "regionCode":"A unique identifier that identifies this region",
            "currentVersionUrl":"The relative URL for the service regional price list file of this version"
        },
        "secondRegion":{
            "regionCode": ...,
            "currentVersionUrl": ...,
            ...
        },
        ...
    }
}
```

Service Region index definitions

The following list defines the terms in the service Region index file.

formatVersion

An attribute that tracks which format version the service Region index file is in. The formatVersion of the file is updated when the structure is changed. For example, the version will change from v1 to v2.

disclaimer

Any disclaimers that apply to the service Region index file.

publicationDate

The date and time in UTC format when a service Region index file was published. For example, 2023-03-28T23:47:21Z.

regions

The list of available AWS Region for the AWS service.
regions:regionCode

A unique code for the Region in which this AWS service is offered. This is used as the lookup key in the Regions list. For example, us-east-2 is the US East (Ohio) Region.

regions:regionCode:currentVersionUrl

The relative URL for the service Region index file of this version. For example, /offers/v1.0/aws/AmazonRDS/20230328234721/us-east-2/index.json.

Service Region index file for Savings Plan

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. Note: This survey is in English only.

To understand the service Region index file for Savings Plan, see the following references:

Topics
- Example: Service Region index file for Savings Plan (p. 130)
- Service Region index definitions (p. 130)

Example: Service Region index file for Savings Plan

The service Region index file for Savings Plan looks like the following.

```json
{
    "disclaimer":"The disclaimers for this service version index",
    "publicationDate":"The publication date of this service region index",
    "regions":[
        {
            "regionCode":"A unique identifier that identifies this region",
            "versionUrl":"The relative URL for the service regional price list file of this version"
        },
        {
            "regionCode": ...,  
            "versionUrl": ...
        },
        ...
    ]
}
```

Service Region index definitions

The following list defines the terms in the service Region index file.

**disclaimer**

Any disclaimers that apply to the service Region index file.

**publicationDate**

The date and time in UTC format when a service Region index file was published. For example, 2023-03-28T23:47:21Z.

**regions**

The list of available AWS Region for the AWS service.
regions:regionCode

A unique code for the Region in which this AWS service is offered. This is used as the lookup key in the Regions list. For example, us-east-2 is the (US East (Ohio) Region.

regions:versionUrl

The relative URL for the service Region index file of this version. For example, /savingsPlan/v1.0/aws/AWSComputeSavingsPlan/20230407145705/us-east-2/index.json.

Reading the service price list files

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. Note: This survey is in English only.

The service price list file lists the products and prices for a single AWS service or Savings Plan in all AWS Regions or a single AWS service or Savings Plan in a specific Region.

Service price list files are available in CSV or JSON format.

To read the file, you can use a spreadsheet program to read and sort the CSV file or an application that parses the JSON file.

Note
In the CSV file, the product and pricing details are combined into one section. In the JSON file, the product details and pricing details are in separate sections.

Topics
• Reading the service price list file for an AWS service (p. 131)
• Reading the service price list file for a Savings Plan (p. 135)

Reading the service price list file for an AWS service

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. Note: This survey is in English only.

The service price list files for an AWS service includes the following types of information:

• Service price list file details – Metadata about the service price list files, such as format version and publication date
• Product details – Product metadata that lists the products in a service price list file, along with product information
• Pricing details (terms) – Prices for all products in this service price list file

Contents
• CSV file (p. 132)
• JSON file (p. 132)
• Service price list definitions (p. 133)
• Product details (products) definitions (p. 133)
• Product details (terms) definitions (p. 133)
CSV file

The first five rows of the CSV file contain the metadata for the price list file. The sixth row has the column names for the products and their attributes, such as SKU, OfferTermCode, RateCode, TermType, and more.

The number of columns depends on the service. The first few columns contain the pricing details, and other columns contain the product details for a service.

JSON file

The product details and pricing details are in separate sections. The same product can be offered under multiple terms, and the same term can apply to multiple products.

For example, an Amazon Elastic Compute Cloud (Amazon EC2) instance is available for an Hourly or Reserved term. You can use the SKU of a product to identify the terms that are available for that product.

Example Example: JSON

```json
{
  "formatVersion":"The version of the file format",
  "disclaimer":"The disclaimers for the price list file",
  "offerCode":"The code for the service",
  "version":"The version of the price list file",
  "publicationDate":"The publication date of the price list file",
  "products": {
    "sku": {
      "sku":"The SKU of the product",
      "productFamily":"The product family of the product",
      "attributes": {
        "attributeName":"attributeValue",
      }
    }
  },
  "terms": {
    "termType": {
      "sku": {
        "sku": {
          "offerTermCode":"The term code of the product",
          "sku":"The SKU of the product",
          "effectiveDate":"The effective date of the pricing details",
          "termAttributesType":"The attribute type of the terms",
          "termAttributes": {
            "attributeName":"attributeValue",
          },
          "priceDimensions": {
            "rateCode": {
              "rateCode":"The rate code of the price",
              "description":"The description of the term",
              "unit":"The usage measurement unit for the price",
              "startingRange":"The start range for the term",
              "endingRange":"The end range for the term",
              "pricePerUnit": {
                "currencyCode":"currencyRate",
              }
            }
          }
        }
      }
    }
  }
}
```
Service price list definitions

The following list defines the terms in the service price list files.

**formatVersion**

An attribute that tracks which format version the service price list file is in. The *formatVersion* of the file is updated when the structure is changed. For example, the version will change from v1 to v2.

**disclaimer**

Any disclaimers that apply to the service price list file.

**offerCode**

A unique code for the product of an AWS service. For example, AmazonEC2 for Amazon EC2 or AmazonS3 for Amazon S3.

**version**

An attribute that tracks the version of the service price list file. Each time a new file is published, it contains a new version number. For example, 20150409022205 and 20150910182105.

**publicationDate**

The date and time in UTC format when a service price list file was published. For example, 2015-04-09T02:22:05Z and 2015-09-10T18:21:05Z.

Product details (products) definitions

This section provides information about products in a service price list file for an AWS service. Products are indexed by SKU.

**products:sku**

A unique code for a product. Use the SKU code to correlate product details and pricing.

For example, a product with a SKU of HCNSHiWJAJSVGAAHM is available only for a price that also lists HCNSHiWJAJSVGAAHM as a SKU.

**products:sku:productFamily**

The category for the type of product. For example, compute for Amazon EC2 or storage for Amazon S3.

**products:sku:attributes**

A list of all of the product attributes.

**products:sku:attributes:Attribute Name**

The name of a product attribute. For example, Instance Type, Processor, or OS.

**products:sku:attributes:Attribute Value**

The value of a product attribute. For example, m1.small (instance type), xen (type of processor), or Linux (type of OS).

Product details (terms) definitions

This section provides information about the prices for products in a service price list file for an AWS service.

Prices are indexed first by the terms (onDemand and reserved), and then by SKU.
terms:termType

The specific type of term that a term definition describes. The valid term types are reserved and onDemand.

terms:termType:SKU

A unique code for a product. Use the SKU code to correlate product details and pricing.

For example, a product with a SKU of HCNSHWAJSGVAMHM is available only for a price that also lists HCNSHWAJSGVAMHM as a SKU.

terms:termType:sku:Offer Term Code

A unique code for a specific type of term. For example, KCAKZHGHG.

Product and price combinations are referenced by the SKU code followed by the term code, separated by a period. For example, U7ADXS4BEK5XXHRU.KCAKZHGHG.

terms:termType:sku:Effective Date

The date that an service price list file goes into effect. For example, if a term has an EffectiveDate of November 1, 2017, the price isn't valid before that date.

terms:termType:sku:Term Attributes Type

A unique code for identifying what product and product offering are covered by a term. For example, an EC2-Reserved attribute type means that a term is available for Amazon EC2 reserved hosts.

terms:termType:sku:Term Attributes

A list of all of the attributes that are applicable to a term type. The format appears as attribute-name: attribute-value. For example, this can be the length of term and the type of purchase covered by the term.

terms:termType:sku:Term Attributes:Attribute Name

The name of a TermAttribute. You can use it to look up specific attributes. For example, you can look up terms by length or PurchaseOption.

terms:termType:sku:Term Attributes:Attribute Value

The value of a TermAttribute. For example, terms can have a length of one year and a purchase option of All Upfront.

terms:termType:sku:Price Dimensions

The pricing details for the price list file, such as how usage is measured, the currency that you can use to pay with, and the pricing tier limitations.

terms:termType:sku:Price Dimensions:Rate Code

A unique code for a product, offer, and pricing-tier combination. Product and term combinations can have multiple price dimensions, such as free tier, low use tier, and high use tier.

terms:termType:sku:Price Dimensions:Rate Code:Description

The description for a price or rate.

terms:termType:sku:Price Dimensions:Rate Code:Unit

The type of unit that each service uses to measure usage for billing. For example, Amazon EC2 uses hours, and Amazon S3 uses GB.

terms:termType:sku:Price Dimensions:Rate Code:Starting Range

The lower limit of the price tier covered by this price. For example, 0 GB or 1,001 API operation calls.
terms:termType:sku:Price Dimensions:Rate Code:Ending Range

The upper limit of the price tier covered by this price. For example, 1,000 GB or 10,000 API operation calls.

terms:termType:sku:Price Dimensions:Rate Code:Price Per Unit

A calculation of how much a single measured unit for a service costs.

terms:termType:sku:Price Dimensions:Rate Code:Price Per Unit:Currency Code

A code that indicates the currency for prices for a specific product.

terms:termType:sku:Price Dimensions:Rate Code:Price Per Unit:Currency Rate

The rate for a product in various supported currencies. For example, $1.2536 per unit.

Reading the service price list file for a Savings Plan

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. Note: This survey is in English only.

The service price list files for an AWS service includes the following types of information:

- Service price list file details – Metadata about the service price list file, such as the version, AWS Region, and publication date
- Product details – Product metadata that lists the products in a service price list file along with product information
- Pricing details (terms) – Prices for all products in the service price list file

Contents

- CSV file (p. 135)
- JSON file (p. 135)
- Service price list definitions (p. 136)
- Product details (products) definitions (p. 136)
- Pricing details (terms) definitions (p. 137)

CSV file

The first five rows of the CSV file are the metadata for the price list file. The sixth row has the column names for the products and their attributes, such as SKU, RateCode, and more.

The number of columns varies depends on the Savings Plan. The first few columns contain the pricing details, while other columns contain the product details for a Savings Plan.

JSON file

The product details and pricing details are in separate sections. A JSON service price list file looks like the following example.

```json
{
    "version" : "The version of the price list file",
    "publicationDate" : "The publication date of the price list file",
    "regionCode" : "Region for which price list file is valid for",
...}
```
"products" : [
    {
      "sku" : "The SKU of the product",
      "productFamily" : "The product family of the product",
      "serviceCode" : "Savings plan code",
      "attributes" : {
        "attributeName":"attributeValue",
      }
    },
    ...
  ],
  "terms" : {
    "savingsPlan" : [
      {
        "sku" : "The SKU of the product",
        "description" : "Description of the product",
        "effectiveDate" : "The effective date of the pricing details",
        "leaseContractLength" : {
          "duration" : "Length of the lease contract - it is a number",
          "unit" : "Unit of the duration"
        },
        "rates" : [
          {
            "discountedSku" : "The SKU of the discounted on demand product",
            "discountedUsageType" : "Usage type of the discounted product",
            "discountedOperation" : "Operation of the discounted product",
            "discountedServiceCode" : "Service code of the discounted product",
            "rateCode" : "The rate code of this price detail",
            "unit" : "Unit used to measure usage of the product",
            "discountedRate" : {
              "price" : "Price of the product",
              "currency" : "Currency of the price"
            }
          },
          ...
        ],
      },
      ...
    ],
  }
}

Service price list definitions

The following list defines the terms in the service price list files.

regionCode

The Region code of the Region for which the price list is valid for.

version

An attribute that tracks the version of the price list file. Each time a new file is published, it contains a new version number. For example, 20150409022205 and 20150910182105.

publicationDate

The date and time in UTC format when a service price list file was published. For example, 2015-04-09T02:22:05Z and 2015-09-10T18:21:05Z.

Product details (products) definitions

This section provides information about products in a price list file for a Savings Plan. Products are indexed by SKU.
**products:product:sku**

A unique code for a product. Use the SKU code to correlate product details and pricing.

For example, a product with a SKU of HCNSHWAJSGVAHMH is available only for a price that also lists HCNSHWAJSGVAHMH as a SKU.

**products:product:productFamily**

The category for the type of product. For example, EC2InstanceSavingsPlans for Compute Savings Plans.

**products:product:serviceCode**

The service code of the Savings Plan. For example, ComputeSavingsPlans.

**products:product:attributes**

A list of all product attributes.

**products:product:attributes:attributeName**

The name of a product attribute. For example, Instance Type, Location Type, or Purchase Option.

**products:product:attributes:attributeValue**

The value of a product attribute. For example, m1.small (instance type), AWS Local Zone (type of location), or No Upfront (type of purchase option).

**Pricing details (terms) definitions**

This section provides information about the prices for products in a price list file for a Savings Plan.

Prices are indexed first by the terms (savingsPlan).

**terms:termType**

The specific type of term that a term definition describes. The valid term type is savingsPlan.

**terms:termType:sku**

A unique code for a product. Use the SKU code to correlate product details and pricing.

For example, a product with a SKU of T496KPMD8YQ8RZNC is available only for a price that also lists 496KPMD8YQ8RZNC as a SKU.

**terms:termType:sku:description**

The description of the product.

**terms:termType:sku:effectiveDate**

The date that an service price list file goes into effect. For example, if a term has an EffectiveDate of November 1, 2017, the price isn't valid before that date.

**terms:termType:sku:leaseContractLength:duration**

The length of the lease contract. This value is a number. For example, 1 or 3.

**terms:termType:sku:rates**

A list all of the discounted rates that are applicable to a Savings Plan product. One Savings Plan product is a combination of multiple products from other services and this contains multiple rates for the combination.
**Finding On-Demand prices for services**

The following procedure shows how to find On-Demand prices for AWS services, such as Amazon EC2. 

**Finding On-Demand prices for services (p. 138)**

**Finding tiered prices for services (p. 139)**

**Finding tiered prices for services with Free Tier (p. 139)**

- **Example (p. 140)**

**Finding prices for services with Reserved Instances (p. 140)**

The AWS Billing User Guide

Find prices in the service price list file
To get your CSV or JSON file, follow the steps in Getting price list files (p. 116) or Getting price list files manually (p. 119).

To find an On-Demand price by using the CSV file
1. Download the CSV file for the service.
2. Open the CSV file with your preferred application.
3. Under the TermType column, filter to show OnDemand.
4. Find the usage type and operation that you want.
5. In the PricePerUnit column, see the corresponding price.

To find an On-Demand price by using the JSON file
1. Download the JSON file for the service.
2. Open the JSON file with your preferred application.
3. Under terms and On-Demand, find the SKU that you want.
   - If you don't know the SKU, search under products for the usage type and operation.
4. See the pricePerUnit to find the corresponding On-Demand price for the SKU.

Finding tiered prices for services
The following procedure shows how to find tiered prices for services, such as Amazon Simple Storage Service (Amazon S3).

To find tiered prices for services by using the CSV file
1. Download the CSV file for the service.
2. Open the CSV file with your preferred application.
3. Under the TermType column, filter to show OnDemand.
4. Find the usage type and operation that you want.
5. In the PricePerUnit column, see the corresponding price for each StartingRange and EndingRange.

To find tiered prices for services by using the JSON file
1. Download the JSON file.
2. Open the JSON file with your preferred application.
3. Under terms and On-Demand find the SKU that you want.
   - If you don't know the SKU, search under products for the usage type and operation.
4. Under each beginRange and endRange, see the pricePerUnit to find the corresponding tiered prices.

Finding tiered prices for services with Free Tier
The following procedure shows how to find AWS services that publish Free Tier prices in the AWS Price List Bulk API, such as AWS Lambda.

All Free Tier prices are subject to the terms documented in AWS Free Tier.
To find prices for services with Free Tier by using the CSV file

1. Download the CSV file for the service.
2. Open the CSV file with your preferred application.
3. Under the TermType column, filter to show OnDemand.
4. Under the Location column, filter to show Any.

   Any doesn't represent all AWS Regions in this scenario. It's a subset of Regions defined by other line items in the CSV file, with a RelatedTo column matching the SKU for the location Any entry.
5. To find a list of all eligible locations and products for a specific Free Tier SKU, find the Free Tier SKU under the RelatedTo column.
6. To find the covered usage by Free Tier across all eligible locations, see the StartingRange and EndingRange for the location Any.

Example

This example assumes there are no more entries in the price file where RelatedTo equals to the SKU ABCD.

As shown in the following table, the Free Tier offer with SKU ABCD is valid in the Asia Pacific (Singapore) and US East (Ohio) Regions, but not in AWS GovCloud (US). The covered usage by Free Tier is 400,000 seconds total, used across both eligible Regions.

<table>
<thead>
<tr>
<th>SKU</th>
<th>StartingRange</th>
<th>EndingRange</th>
<th>Unit</th>
<th>RelatedTo</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABCD</td>
<td>0</td>
<td>400000</td>
<td>seconds</td>
<td>Any</td>
<td></td>
</tr>
<tr>
<td>QWER</td>
<td>0</td>
<td>Inf</td>
<td>seconds</td>
<td>ABCD</td>
<td>Asia Pacific (Singapore)</td>
</tr>
<tr>
<td>WERT</td>
<td>0</td>
<td>Inf</td>
<td>seconds</td>
<td>ABCD</td>
<td>US East (Ohio)</td>
</tr>
<tr>
<td>ERTY</td>
<td>0</td>
<td>Inf</td>
<td>seconds</td>
<td></td>
<td>AWS GovCloud (US)</td>
</tr>
</tbody>
</table>

To find tiered prices for services with Free Tier by using the JSON file

1. Download the JSON file for the service.
2. Open the JSON file with your preferred application.
3. Under products, find the usagetype with the Region prefix Global.
4. Take note of the SKU, and look for the same SKU under terms and OnDemand.
5. For the amount of Free Tier usage, see the BeginRange and EndRange.
   
   For a list of products and Regions covered by Free Tier, see appliesTo.

Finding prices for services with Reserved Instances

The following procedure shows how to find prices for services with Reserved Instances, such as Amazon Relational Database Service (Amazon RDS).
To find prices for a Reserved Instance by using the CSV file

1. Download the Amazon EC2 CSV file.
2. Open the CSV file with your preferred application.
3. Under the TermType column, filter to show reserved.
4. Find the usage type and operation that you want.
5. For each LeaseContractLength, PurchaseOption, and OfferingClass, see the PricePerUnit column for the corresponding price.

To find prices for Reserved Instances by using the JSON file

1. Download the JSON file for the service.
2. Open the JSON file with your preferred application.
3. Under terms and Reserved, find the SKU that you want.
   If you don't know the SKU, search under products for the usage type and operation.

You can find prices for LeaseContractLength, PurchaseOption, and OfferingClass for the same product.

### Setting up price update notifications

To provide feedback about AWS Price List, complete this short survey. Your responses will be anonymous. **Note:** This survey is in English only.

Price list files can change anytime. When the price list files are updated, an Amazon Simple Notification Service (Amazon SNS) notification is sent. You can set up to receive notifications when prices change, such as when AWS lowers prices, or when new products and services are launched.

You can get notified every time a price changes or only once a day. If you choose to be notified once a day, the notification includes all price changes applied during the previous day. We recommend that you set up notifications and get the latest files when they change.

### Contents

- Set up Amazon SNS notifications (p. 141)
- Notification structure for AWS services (p. 142)
- Notification structure for Savings Plans (p. 144)

### Set up Amazon SNS notifications

You can use the AWS Management Console to sign up for Amazon SNS notifications.

**To set up Amazon SNS notifications for price list file updates**

2. If you're new to Amazon SNS, choose Get Started.
3. If necessary, change the AWS Region on the navigation bar to **US East (N. Virginia)**.
4. On the navigation pane, choose **Subscriptions**.
5. Choose **Create subscription**.
6. For **Topic ARN**, enter the following as needed:
   - For service pricing:
     - To get notified every time a price changes, enter: `arn:aws:sns:us-east-1:278350005181:price-list-api`
     - To get notified about price changes once a day, enter: `arn:aws:sns:us-east-1:278350005181:daily-aggregated-price-list-api`
7. For **Protocol**, use the default HTTP setting.
8. For **Endpoint**, specify the format that you want to receive the notification, such as Amazon Simple Queue Service (Amazon SQS), AWS Lambda, or email.
9. Choose **Create subscription**.

When a price changes, you will receive a notification from your preferred format that you specified in step 8.

**Important**

If you get an error message Couldn't create subscription. Error code: InvalidParameter - Error message: Invalid parameter: TopicArn, it's likely that you're not using the US East (N. Virginia) Region. The billing metric data is stored in this Region, even for resources in other Regions. Return to step 3 and complete the rest of this procedure.

### Notification structure for AWS services

The pricing update notification has a subject line in the following format.

```
```

**Example Example: Subject line**

A price update notification for Amazon Relational Database Service (Amazon RDS) looks like the following.

```
[Pricing Update] New AmazonRDS offer file available.
```

**Example Example: Notification message**

If you subscribed to AWS services such as Amazon SQS, Lambda, or other services, the structure of the pricing update notification message body looks like the following.

```json
{
  "formatVersion":"v1.0",
  "offerCode":"<serviceCode>",
  "version":"<Version number of this new price list>",
  "timeStamp":"<Publish date of this new price list>",
  "url":{
    "JSON":"
  }
}
```
For example, the notification message for Amazon RDS looks like the following.

```json
{
   "formatVersion": "v1.0",
   "offerCode": "AmazonRDS",
   "version": "20230328234721",
   "timeStamp": "2023-03-28T23:47:21Z",
   "url": {
      "JSON": "https://pricing.us-east-1.amazonaws.com/offers/v1.0/aws/AmazonRDS/current/index.json",
      "CSV": "https://pricing.us-east-1.amazonaws.com/offers/v1.0/aws/AmazonRDS/current/index.csv"
   },
   "regionIndex": "https://pricing.us-east-1.amazonaws.com/offers/v1.0/aws/AmazonRDS/current/region_index.json",
   "operation": "Publish"
}
```

### Example: Email notification

If you subscribed to email, the structure of the pricing update email message body looks like the following.

```
Hello,
You've received this notification because you subscribed to receiving updates from SNS topic arn:aws:sns:us-east-1:278350005181:price-list-api.

We've published a new version of the offer file for Service <serviceCode>. To download the offer file, use the following URLs:
- JSON format : <JSON URL of the current version price list>
- CSV format : <CSV URL of the current version price list>

To download the index for the region-specific offer files, use the following URL:
- RegionIndexUrl : <Region index URL of the current version price list>

To get a daily email that shows all price changes made the previous day, subscribe to the following SNS topic: arn:aws:sns:us-east-1:278350005181:daily-aggregated-price-list-api.

To learn more about offer files and index files, see http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/price-changes.html.

Thank You,
Amazon Web Services Team
```

Am example email message for Amazon RDS looks like the following.

```
Hello,
You've received this notification because you subscribed to receiving updates from SNS topic arn:aws:sns:us-east-1:278350005181:price-list-api.

We've published a new version of the offer file for Service AmazonRDS. To download the offer file, use the following URLs:
- JSON format : https://pricing.us-east-1.amazonaws.com/offers/v1.0/aws/AmazonRDS/current/index.json
- CSV format : https://pricing.us-east-1.amazonaws.com/offers/v1.0/aws/AmazonRDS/current/index.csv

To download the index for the region-specific offer files, use the following URL:
- RegionIndexUrl : https://pricing.us-east-1.amazonaws.com/offers/v1.0/aws/AmazonRDS/current/region_index.json
```
Notification structure for Savings Plans

The pricing update notification has a subject line in the following format.

[ Pricing Update ] New <Savings Plan name> is available.

Example Example: Subject line for Savings Plan

A subject line for Savings Plan looks like the following.

[ Pricing Update ] New AWS Compute Savings Plan is available.

Example Example: Notification message

If you subscribed to AWS services such as Amazon SQS, Lambda, or other services, the structure of the pricing update notification message body looks like the following.

```
{
  "version": "<Version number of this new price list>",
  "offerCode": "<offerCode which can be used as input to API calls>",
  "savingsPlanCode": "<savingsPlan Name>",
  "topicArn": "arn:aws:sns:us-east-1:626627529009:SavingsPlanPublishNotifications",
  "versionIndex": "<version index URL of the version price list>",
  "regionIndex": "<Region index URL of the version price list>
}
```

For example, a notification for ComputeSavingsPlans looks like the following.

```
{
  "version": "20230509202901",
  "offerCode": "AWSComputeSavingsPlan",
  "savingsPlanCode": "ComputeSavingsPlans",
  "topicArn": "arn:aws:sns:us-east-1:626627529009:SavingsPlanPublishNotifications",
  "versionIndex": "https://pricing.us-east-1.amazonaws.com/savingsPlan/v1.0/aws/AWSComputeSavingsPlan/20230509202901/index.json",
  "regionIndex": "https://pricing.us-east-1.amazonaws.com/savingsPlans/v1.0/aws/AWSComputeSavingsPlan/20230509202901/region_index.json"
}
```

Example Example: Email notification

If you subscribed to email, the structure of the pricing update email body looks like the following.

```
Hello,

You’ve received this notification because you subscribed to receiving updates from SNS topic arn:aws:sns:us-east-1:626627529009:SavingsPlanPublishNotifications.
```
We've published a new version of `<Savings Plan name>.

To download the index of current region specific savings plans, use the following URL:
- `<Region index URL of the version price list>`

To download the index of previous versions of savings plans, use the following URL:
- `<version index URL of the version price list>`

To learn more about Savings Plans, see http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/price-changes.html.
To learn about finding Savings Plan prices in an offer file, see https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/sp-offer-file.html

Thank You,
Amazon Web Services Team

For example, an email body for Savings Plan looks like the following.

Hello,

You've received this notification because you subscribed to receiving updates from SNS topic arn:aws:sns:us-east-1:626627529009:SavingsPlanPublishNotifications.

We've published a new version of Compute Savings Plans.

To download the index of current region specific savings plans, use the following URL:
- `https://pricing.us-east-1.amazonaws.com/savingsPlan/v1.0/aws/AWSComputeSavingsPlan/20230509202901/region_index.json`

To download the index of previous versions of savings plans, use the following URL:
- `https://pricing.us-east-1.amazonaws.com/savingsPlan/v1.0/aws/AWSComputeSavingsPlan/20230509202901/index.json`

To learn more about savings plans, see http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/price-changes.html.
To learn about finding Savings Plan prices in an offer file, see https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/sp-offer-file.html

Thank You,
Amazon Web Services Team
Consolidated billing for AWS Organizations

You can use the consolidated billing feature in AWS Organizations to consolidate billing and payment for multiple AWS accounts or multiple Amazon Web Services India Private Limited (AWS India) accounts. Every organization in AWS Organizations has a management account that pays the charges of all member accounts. For more information about organizations, see the AWS Organizations User Guide.

Consolidated billing has the following benefits:

- **One bill** – You get one bill for multiple accounts.
- **Easy tracking** – You can track the charges across multiple accounts and download the combined cost and usage data.
- **Combined usage** – You can combine the usage across all accounts in the organization to share the volume pricing discounts, Reserved Instance discounts, and Savings Plans. This can result in a lower charge for your project, department, or company than with individual standalone accounts. For more information, see Volume discounts (p. 150).
- **No extra fee** – Consolidated billing is offered at no additional cost.

**Note**
The member account bills are for informational purpose only. The management account might reallocate the additional volume discounts, Reserved Instance, or Savings Plans discounts that your account receives.

If you have access to the management account, you can see a combined view of the AWS charges that the member accounts incur. You also can get a cost report for each member account.

AWS and AWS India accounts can't be consolidated together. If your contact address is in India, you can use AWS Organizations to consolidate AWS India accounts within your organization.

**Important**
When a member account leaves an organization, the member account can no longer access Cost Explorer data that was generated when the account was in the organization. The data isn't deleted, and the management account in the organization can still access the data. If the member account rejoins the organization, the member account can access the data again.

Topics

- Consolidated billing process (p. 147)
- Consolidated billing in AWS EMEA (p. 147)
- Consolidated billing in India (p. 149)
- Effective billing date, account activity, and volume discounts (p. 149)
- AWS credits (p. 150)
- Reserved instances (p. 153)
- Understanding Consolidated Bills (p. 156)
- Requesting shorter PDF invoices (p. 162)
Consolidated billing process

AWS Organizations provides consolidated billing so that you can track the combined costs of all the member accounts in your organization. The following steps provide an overview of the process for creating an organization and viewing your consolidated bill.

1. Open the AWS Organizations console or the AWS Billing and Cost Management console. If you open the AWS Billing and Cost Management console, choose Consolidated Billing, and then choose Get started. You are redirected to the AWS Organizations console.
2. Choose Create organization on the AWS Organizations console.
3. Create an organization from the account that you want to be the management account of your new organization. For details, see Creating an Organization. The management account is responsible for paying the charges of all the member accounts.
4. (Optional) Create accounts that are automatically member to the organization. For details, see Creating an AWS account in Your Organization.
5. (Optional) Invite existing accounts to join your organization. For details, see Inviting an AWS account to Join Your Organization.
6. Each month AWS charges your management account for all the member accounts in a consolidated bill.

The management account is billed for all charges of the member accounts. However, unless the organization is changed to support all features in the organization (not consolidated billing features only) and member accounts are explicitly restricted by policies, each member account is otherwise independent from the other member accounts. For example, the owner of a member account can sign up for AWS services, access resources, and use AWS Premium Support unless the management account restricts those actions. Each account owner continues to use their own sign-in credentials, with account permissions assigned independently of other accounts in the organization.

Securing the consolidated billing management account

The owner of the management account in an organization should secure the account by using AWS Multi-Factor Authentication and a strong password that has a minimum of eight characters with both uppercase and lowercase letters, at least one digit, and at least one special character. You can change your password on the AWS Security Credentials page.

Consolidated billing in AWS EMEA

The consolidated daily invoice feature combines your charges, so that you receive fewer invoices each day. You’re automatically opted into this feature if you meet the following requirements:

• Your AWS account is invoiced through the Amazon Web Services EMEA SARL (AWS Europe) entity. For more information, see Managing your payments in AWS Europe (p. 51).
• You’re using the pay by invoice payment method. This feature isn’t available for credit card or direct debit payment methods.

This feature consolidates the following:

• Daily subscriptions and out-of-cycle invoices into one invoice
• Credit memos into one invoice
For example, if you purchase three Reserved Instances and receive two credit memos today, you receive a total of two invoices at the end of the day. One invoice includes your Reserved Instance purchases, and the other includes your credit memos.

**Consolidation period**

AWS processes subscription invoices and refunds between 23:59 to 24:00 midnight UTC. AWS then generates the consolidated invoices and credit memos during the previous 24-hour period. Your consolidated bill is available within minutes.

**Services covered**

Your daily invoice includes AWS service subscriptions, out-of-cycle purchases, and credit memos. This feature doesn't include the following:

- AWS Marketplace purchases
- AWS monthly service and anniversary invoices
- Credit memos issued for different original invoices

For example, suppose that you receive credit memo A for original invoice ID 123, and another credit memo B for original invoice ID 456. Both credit memos aren't consolidated, even if they're issued on the same day. Credit memos are consolidated only if they're issued against the same original invoice ID.

- AWS Support purchases, such as changing AWS Support plans
- Charges for some Amazon Route 53 offerings (for example, purchasing a domain name), AWS Partner Network, AWS Managed Services, and AWS conferences such as re:Invent, and re:Inforce

**Currency and foreign exchange rate**

Credit memos use the same currency and exchange rate as the original invoice.

For subscription invoices, AWS applies the latest currency preference to all one-time fees processed during the previous 24-hour period. For example, if you purchase a Reserved Instance in the morning, and then change your preferred currency in the afternoon, AWS converts the currency for the morning purchase into the new preferred currency. This update appears in the consolidated invoice generated for that day.

**Changes to your AWS Cost and Usage Report**

With consolidated billing, it can take up to 24 hours after AWS processes your one-time charges for them to appear in your AWS Cost and Usage Report (AWS CUR), Cost Explorer, or cost budget alerts set up using AWS Budgets.

You can continue to view your amortized one-time upfront Reserved Instance charges in AWS CUR, Cost Explorer, or Budgets.

**Turn off consolidated billing**

By default, this feature is enabled for your account. If you don't want this feature, use the following procedure.

**To turn off consolidated billing**

1. Sign in to the [AWS Support Center Console](#).
2. Create an **Account & billing** support case.
3. For **Service**, choose **Billing**.
4. For **Category**, choose **Consolidated Billing**.
5. Follow the prompts to create your support case.

**Note**
Repeat this procedure if you want to turn on consolidated billing later.

**Consolidated billing in India**

If you sign up for a new account and choose India for your contact address, your user agreement is with Amazon Web Services India Private Limited (AWS India), a local AWS seller in India. AWS India manages your billing, and your invoice total is listed in rupees instead of in dollars. After you create an account with AWS India, you can't change the country in your contact information.

If you have an existing account with an India address, your account is either with AWS or AWS India, depending on when you opened the account. To learn whether your account is with AWS or AWS India, see the procedure [Determining Which Company Your Account Is With](#). If you’re an existing AWS customer, you can continue to use your AWS account. You can also choose to have both an AWS account and an AWS India account, although they can’t be consolidated into the same organization. (Currently, you can’t migrate an existing account from AWS to AWS India.) If you are in an AWS India organization, the management account can edit the PAN numbers of all member accounts.

If you create an organization from a management account that is with AWS India, you can invite only other AWS India accounts to join your organization. You can’t invite AWS accounts.

If you create an organization from a management account that is with AWS, you can invite only other AWS accounts to join your organization. You can’t invite AWS India accounts.

**Effective billing date, account activity, and volume discounts**

When the member account owner accepts your request to join the organization, you immediately become responsible for the member account’s charges. If the member account joins in the middle of the month, the management account is billed only for the latter part of the month.

For example, if a member account joins an organization on March 10, then AWS bills the management account for the member account’s period of usage starting on March 10. The member account’s original owner is still billed for the first part of the month.

**Billing and account activity**

Each month, AWS charges the management account owner, and not the owners of the member accounts. To see the total usage and charges across all the accounts in an organization, see the **Bills** page of the management account. AWS updates the page multiple times each day. Additionally, AWS makes a downloadable cost report available each day.

Although the owners of the member accounts aren't charged, they can still see their usage and charges by going to their **AWS Bills** pages. They can’t view or obtain data for the management account or any other member accounts on the bill.
Volume discounts

For billing purposes, AWS treats all of the accounts in the organization as if they were one account. Some services, such as AWS Data Transfer and Amazon S3, have volume pricing tiers across certain usage dimensions that give you lower prices the more you use the service. With consolidated billing, AWS combines the usage from all accounts to determine which volume pricing tiers to apply, giving you a lower overall price whenever possible. AWS then allocates each member account a portion of the overall volume discount based on the account's usage.

For example, let's say that Bob's consolidated bill includes both Bob's own account and Susan's account. Bob's account is the management account, so he pays the charges for both himself and Susan.

Bob transfers 8 TB of data during the month and Susan transfers 4 TB.

For the purposes of this example, AWS charges $0.17 per GB for the first 10 TB of data transferred and $0.13 for the next 40 TB. This translates into $174.08 per TB (= .17*1024) for the first 10 TB, and $133.12 per TB (= .13*1024) for the next 40 TB. Remember that 1 TB = 1024 GB.

For the 12 TB that Bob and Susan used, Bob's management account is charged ($174.08 * 10 TB) + ($133.12 * 2 TB) = $1740.80 + $266.24 = $2,007.04.

Without the benefit of tiering across the consolidated bill, AWS would have charged Bob and Susan each $174.08 per TB for their usage, for a total of $2,088.96.

To learn more about pricing, see AWS Pricing.

AWS Free Tier for AWS Organizations

For services such as Amazon EC2 that support a free tier, AWS applies the free tier to the total usage across all accounts in an AWS organization. AWS doesn't apply the free tier to each account individually.

AWS provides budgets that track whether you exceed the free tier limits or are forecasted to go over the free tier limits. Free tier budgets are not enabled for organizations by default. Management account can opt in to free tier usage alerts through the Billing and Cost Management console. Free tier usage alerts aren't available to individual member accounts.

For more information about free tiers, see AWS Free Usage Tier FAQs. For more information about AWS Free Tier usage alerts through AWS Budgets and opting in, see Using AWS Free Tier usage alerts (p. 100).

AWS credits

AWS credits are automatically applied to bills to help cover costs that are associated with eligible services. For more information about eligible services, see Redeem Your AWS Promotional Credit. Credits are applied until they are exhausted or they expire.

For any questions about AWS credits in general or any credits that have already expired, contact AWS Support. For more information about how to contact AWS Support, see Getting help with AWS Billing (p. 6).

Topics

- Step 1: Choosing the credits to apply (p. 151)
- Step 2: Choose where to apply your credits (p. 151)
- Step 3: Applying AWS credits across single and multiple accounts (p. 152)
- Step 4: Sharing AWS credits (p. 152)
Step 1: Choosing the credits to apply

This section explains how AWS credits apply in a single or standalone AWS account. If an AWS account has more than one credit, the available credits apply in the following order:

### The order of how credits apply if an AWS account has more than one credit

1. The soonest to expire amongst the credits
2. The credit with the least number of eligible services
3. The oldest of all credits

For example, Jorge has two credits available to him. Credit one is for 10 dollars, it expires January 2019, and it can be used for either Amazon S3 or Amazon EC2. Credit two is for 5 dollars, it expires December 2019, and it can be used only for Amazon EC2. Jorge has sufficient AWS charges to apply all credits. AWS selects credit one for application first because it expires sooner than credit two.

**Note**

- If you have remaining, eligible usage after credit is consumed, the process will repeat until your credits are consumed or your usage is covered.
- Credit is applied to the largest services charge (for example, Amazon EC2, Amazon S3). Then, the consumption will continue in a descending pattern for the remainder of the service charges.
- Credits don’t require customer selection to apply during the billing process. AWS will automatically apply eligible credits to applicable services.

Step 2: Choose where to apply your credits

This section shows how AWS credits apply in an AWS Organizations when credit sharing is turned on.

### The order of how credits are applied in an AWS Organizations when credit sharing is activated

1. Account that owns the credit is covered for the service charges
2. Credits are applied towards the AWS account with the highest spend
3. Within the linked account, the charges are grouped by specific fields and credits are applied to the group with the highest charges
4. Within this group, credits are applied to the highest charge first

The process repeats until the credit is consumed, or all customer spend is covered.

AWS applies the credit to the largest available charge across all eligible sellers of record. This means that AWS tries to apply your credits before they expire. So they might use a generic credit for a specific service.

For example, Jorge has two credits available to him. Credit one is for 10 dollars, expires January 2019, and can be used for either Amazon S3 or Amazon EC2. Credit two is for 5 dollars, expires December 2019, and can be used only for Amazon EC2. Jorge has two AWS charges: 100 dollars for Amazon EC2 and 50 dollars for Amazon S3. AWS applies credit one, which expires in January, to the Amazon EC2 charge, which leaves him with a 90-dollar Amazon EC2 charge and a 50-dollar Amazon S3 charge. AWS applies credit two to the remaining 90 dollars of Amazon EC2 usage, and Jorge has to pay 85 dollars for Amazon EC2 and 50 dollars for Amazon S3. He has now used all of his credits.
Step 3: Applying AWS credits across single and multiple accounts

The following rules specify how AWS applies credits to bills for single accounts and for organizations by default (Credit sharing turned on):

- The billing cycle begins on the first day of each month.
- Suppose that an AWS account is owned on the first day of the month by an individual who isn't part of an organization. Later in the month, that individual account joins an organization. In this situation, AWS applies that individual's credits to their individual bill for their usage for that month. That is, AWS applies the credit up to the day that the individual joined the organization.

  **Note**
  An individual's account credits don't cover the account usage from the day that the individual joined the organization to the end of that month. For this period, the individual's account credits aren't applied to the bill. However, starting the next month, AWS applies the individual's account credits to the organization.

- If an account is owned by an organization at the start of the month, AWS applies credits redeemed by the payer account or by any linked account to the organization's bill, even if the account leaves the organization in the same month. The start of the month begins one second after 0:00 UTC+0. For example, assume that an account leaves an organization on August 1. AWS still applies the August credits the account redeemed to the organization's bill because the account belonged to the organization during that calendar month.

- If an individual leaves an organization during the month, AWS begins applying credits to the individual's account on the first day of the following month.

- Credits are shared with all accounts that join an organization at any point in the month. However, the organization's shared credit pool consists of only credits from accounts that have been part of the organization since the first day of the month.

For example, assume that Susan owns a single account on the first day of the month and then joins an organization during the month. Also assume that she redeems her credits on any day after she joins the organization. AWS applies her credits to her account for usage she incurred from the first of the month to the day that she joined the organization. However, from the first day of the next month, AWS applies the credits to the organization's bill. If Susan leaves the organization, any credits that she redeems are also applied to the organization's bill until the first of the month after her departure. Starting the month after her departure, AWS applies Susan's credits to her bill instead of the organization's bill.

In another example, assume that Susan owns a single account on January 1 and joins an organization on January 11. If Susan redeems 100 dollars of credits on January 18, AWS applies them to her account for the usage that she incurred for the month of January. From February 1st onwards, Susan's credits are applied to the organization's consolidated bill. If Susan has 50 dollars of credits and leaves the organization on April 16, her credits are applied to the organization's consolidated bill for April. From May onward, Susan's credits are applied to her account.

Step 4: Sharing AWS credits

You can turn off credit sharing on the Billing preferences page on the Billing console. The following rules specify how credits are applied to bills for single accounts and for organizations when credit sharing is turned off:

- The billing cycle begins on the first day of each month.
- Credits are applied to only the account that received the credits.
- Bills are calculated using the credit sharing preference that is active on the last day of the month.
In an organization, only the payer account can turn credit sharing off or on. The payer account user can also select which accounts credits can be shared with.

Credit sharing preferences

You can use this section to activate sharing credits across member accounts in your billing family. You can select specific accounts or enable sharing for all accounts.

**Note**
This section is only available for the management account (payer account) as part of AWS Organizations.

**To manage credit sharing for member accounts**

2. In the navigation pane, choose **Billing preferences**.
3. In the Credit sharing preferences section, choose **Edit**.
4. To activate or deactivate credit sharing for specific accounts, select them from the table, and then choose **Activate** or **Deactivate**.
5. To activate or deactivate credit sharing for all accounts, choose **Actions**, and then choose **Activate All** or **Deactivate All**.
6. Choose **Update**.

**Tip**
- To activate credit sharing for new accounts that join your organization, select **Default sharing for newly created member accounts**.
- To download a history of your credit sharing preferences, choose **Download preference history (CSV)**.

Reserved instances

For billing purposes, the consolidated billing feature of AWS Organizations treats all the accounts in the organization as one account. This means that all accounts in the organization can receive the hourly cost benefit of Reserved Instances that are purchased by any other account.

You can turn off Reserved Instance discount sharing on the **Preferences** page on the Billing and Cost Management console. For more information, see the section called “Reserved Instances and Savings Plans discount sharing” (p. 155).

**Topics**
- Billing examples for specific services (p. 153)
- Reserved Instances and Savings Plans discount sharing (p. 155)

Billing examples for specific services

There are a few other things to know about how consolidated billing works with specific services in AWS.

Amazon EC2 reserved instances
For an Amazon EC2 Reserved Instances example, suppose that Bob and Susan each have an account in an organization. Susan has five Reserved Instances of the same type, and Bob has none. During one particular hour, Susan uses three instances and Bob uses six, for a total of nine instances on the organization's consolidated bill. AWS bills five instances as Reserved Instances, and the remaining four instances as regular instances.

Bob receives the cost benefit from Susan's Reserved Instances only if he launches his instances in the same Availability Zone where Susan purchased her Reserved Instances. For example, if Susan specifies us-west-2a when she purchases her Reserved Instances, Bob must specify us-west-2a when he launches his instances to get the cost benefit on the organization's consolidated bill. However, the actual locations of Availability Zones are independent from one account to another. For example, the us-west-2a Availability Zone for Bob's account might be in a different location than the location for Susan's account.

**Amazon RDS reserved DB instances**

For an Amazon RDS Reserved DB Instances example, suppose that Bob and Susan each have an account in an organization. Susan has five Reserved DB Instances, and Bob has none. During one particular hour, Susan uses three DB Instances and Bob uses six, for a total of nine DB Instances on the consolidated bill. AWS bills five as Reserved DB Instances, and the remaining four as On-Demand DB Instances (for Amazon RDS Reserved DB Instance charges, see the [pricing page](#)). Bob receives the cost benefit from Susan's Reserved DB Instances only if he launches his DB Instances in the same region where Susan purchased her Reserved DB Instances.

Also, all of the relevant attributes of Susan's Reserved DB Instances should match the attributes of the DB Instances launched by Bob as described in [Reserved DB Instances](#). For example, let's say Susan purchased a Reserved DB Instance in us-west-2 with the following attributes:

- DB Engine: Oracle
- DB Instance Class: m1.xlarge
- Deployment Type: Multi-AZ

This means that Bob must launch his DB Instances in us-west-2 with the exact same attributes to get the cost benefit on the organization's consolidated bill.

**Amazon ElastiCache reserved node instances**

For an Amazon ElastiCache Reserved Nodes example, suppose Bob and Susan each have an account in an organization. Susan has five Reserved Nodes, and Bob has none. During one particular hour, Susan uses three nodes and Bob uses six. This makes a total of nine nodes used on the consolidated bill.

AWS bills five as Reserved Nodes. AWS bills the remaining four as On-Demand nodes. (For Amazon ElastiCache Reserved Nodes charges, see [Amazon ElastiCache Pricing](#).) Bob receives the cost benefit from Susan's Reserved Nodes only if he launches his On-Demand nodes in the same region where Susan purchased her Reserved Nodes.

Also, to receive the cost benefit of Susan's Reserved Nodes, all attributes of Bob's nodes must match the attributes of the nodes launched by Susan. For example, let's say Susan purchased Reserved Nodes in us-west-2 with the following attributes:

- Cache engine: Redis
- Node type: cache.r3.large

Bob must launch his ElastiCache nodes in us-west-2 with the same attributes to get the cost benefit on the organization's consolidated bill.
Amazon OpenSearch Service Reserved Instances

For an Amazon OpenSearch Service Reserved Nodes example, suppose Bob and Susan each have an account in an organization. Susan has five Reserved Instances, and Bob has none. During one particular hour, Susan uses three instances and Bob uses six. This makes a total of nine instances used on the consolidated bill.

AWS bills five as Reserved Instances. AWS bills the remaining four as On-Demand instances. (For Amazon OpenSearch Service Reserved Instance charges, see Amazon OpenSearch Service Pricing.) Bob receives the cost benefit from Susan's Reserved Instances only if he launches his On-Demand instances in the same AWS Region where Susan purchased her Reserved Instances.

To receive the cost benefit of Susan's Reserved Instances, Bob also must use the same instance type that Susan reserved. For example, let's say Susan purchased m4.large.elasticsearch instances in us-west-2. Bob must launch his Amazon OpenSearch Service domains in us-west-2 with the same instance type to get the cost benefit on the organization's consolidated bill.

Reserved Instances and Savings Plans discount sharing

The management account of an organization can deactivate Reserved Instance discount and Savings Plans discount sharing for any accounts in that organization, including the management account. This means that Reserved Instances and Savings Plans discounts aren't shared between any accounts that have deactivated sharing.

To share an Reserved Instance or Savings Plans discount with an account, both accounts must have sharing activated. You can change your preference at any time. Each estimated bill is computed by using the last set of preferences. The final bill for the month is calculated based on the preferences set at 23:59:59 UTC time on the last day of the month.

Important
Deactivating Reserved Instance and Savings Plans discount sharing can result in a higher monthly bill.

Topics
- Deactivating shared Reserved Instances and Savings Plans discounts (p. 155)
- Activating shared Reserved Instances and Savings Plans discounts (p. 156)

Deactivating shared Reserved Instances and Savings Plans discounts

You can deactivate sharing discounts for individual member accounts.

To deactivate shared Reserved Instances and Savings Plans discounts

2. In the navigation pane, choose Billing preferences.
3. Under Reserved Instances and Savings Plans discount sharing preference by account, select the accounts that you want to deactivate discount sharing for.
4. Choose Deactivate.
5. In the Deactivate Reserved Instance and Savings Plan sharing dialog box, choose Deactivate.
Tip
You can also choose Actions and then choose Deactivate All to deactivate Reserved Instance and Savings Plans sharing for all accounts.

Activating shared Reserved Instances and Savings Plans discounts

You can use the console to activate Reserved Instance sharing discounts for an account.

You can share Savings Plans with a set of accounts. You can either choose to not share the benefit with other accounts, or to open up line item eligibility for the entire consolidated billing family of accounts.

To activate shared Reserved Instances and Savings Plans discounts

   
   Note
   Ensure that you're signed in to the management account of your AWS Organizations.

2. In the navigation pane, choose Billing preferences.

3. Under Reserved Instances and Savings Plans discount sharing preference by account, select the accounts that you want to activate discount sharing for.

4. Choose Activate.

5. In the Activate Reserved Instance and Savings Plan sharing dialog box, choose Activate.

Tip
You can also choose Actions and then choose Activate All to activate Reserved Instance and Savings Plans sharing for all accounts.

Understanding Consolidated Bills

If you manage an organization in AWS Organizations, you can use consolidated billing to view aggregated usage costs for accounts in the organization. Consolidated billing can also help you reduce those costs. For example, to ensure that you pay the lowest available prices for AWS products and services, AWS offers pricing tiers that reward higher usage with lower prices and discounted rates for purchasing instances in advance (known as reservations or Reserved Instances). Using consolidated billing, you can combine usage from multiple accounts into a single invoice, allowing you to reach the tiers with lower prices faster. You can also apply unused reservations from one account to another account's instance usage.

Topics
- Calculating Consolidated Bills (p. 156)
- Pricing Tiers (p. 157)
- Reserved Instances (p. 159)
- Savings Plans (p. 160)
- Blended Rates and Costs (p. 161)

Calculating Consolidated Bills

In an organization, the management account is responsible for paying all charges that the member accounts incur. If you're an administrator of a management account and you have the appropriate permissions, you can view aggregated usage costs for Reserved Instance discounts and volume tiering...
for all member accounts. You can also view the charges that individual member accounts incur, because AWS creates a separate bill for each member account based on that account’s usage. AWS also includes invoice summaries for each account in the management account invoice. During each billing period, AWS calculates your estimated charges several times each day so that you can track your costs as your organization incurs them. Your bill is not finalized until the beginning of the next month.

Note
Like member accounts, a management account can incur usage charges. However, as a best practice you shouldn't use the management account to run AWS services. An exception is for services and resources that are required to manage the organization itself. For example, as part of managing your consolidated billing you might create an S3 bucket in the management account to store AWS Cost and Usage Reports.

Pricing Tiers

Some AWS services are priced in tiers, which specify unit costs for defined amounts of AWS usage. As your usage increases, your usage crosses thresholds into new pricing tiers that specify lower unit costs for additional usage in a month. Your AWS usage is measured every month. To measure usage, AWS treats all accounts in an organization as a single account. Member accounts don't reach tier thresholds individually. Instead, all usage in the organization is aggregated for each service, which ensures faster access to lower-priced tiers. As each month begins, your service usage is reset to zero.

Each AWS service publishes its pricing information independently. You can access all individual pricing pages from the AWS Pricing page.

Calculating Costs for Amazon S3 Standard Storage

The following table shows an example of pricing tiers (your costs might vary). For more information, see Amazon S3 pricing.

Amazon S3 Pricing Tiers

<table>
<thead>
<tr>
<th>Tier description</th>
<th>Price per GB</th>
<th>Price per TB</th>
</tr>
</thead>
<tbody>
<tr>
<td>First 1 TB/month</td>
<td>$0.10</td>
<td>$100.00</td>
</tr>
<tr>
<td>Next 49 TB/month</td>
<td>$0.08</td>
<td>$80.00</td>
</tr>
<tr>
<td>Next 450 TB/month</td>
<td>$0.06</td>
<td>$60</td>
</tr>
</tbody>
</table>

The following table shows Amazon S3 usage for an organization that includes a management account and three member accounts.

Example S3 Usage Blended Cost

<table>
<thead>
<tr>
<th>Account</th>
<th>Tier</th>
<th>Storage amount (GB)</th>
<th>Storage amount (TB)</th>
<th>Unblended rate (/GB)</th>
<th>Unblended rate (/TB)</th>
<th>Unblended cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management</td>
<td>First TB/month</td>
<td>1,000</td>
<td>1</td>
<td>$0.10</td>
<td>100</td>
<td>$100.00</td>
</tr>
<tr>
<td></td>
<td>Next 49 TB/month</td>
<td>49,000</td>
<td>49</td>
<td>$0.08</td>
<td>80</td>
<td>$3,920.00</td>
</tr>
<tr>
<td></td>
<td>Next 450 TB/month</td>
<td>45,000</td>
<td>45</td>
<td>$0.06</td>
<td>60</td>
<td>$2,700.00</td>
</tr>
</tbody>
</table>
## Pricing Tiers

<table>
<thead>
<tr>
<th>Account</th>
<th>Tier</th>
<th>Storage amount (GB)</th>
<th>Storage amount (TB)</th>
<th>Unblended rate (/GB)</th>
<th>Unblended rate (/TB)</th>
<th>Unblended cost</th>
<th>Blended rate (/GB) = $6,720/95,000</th>
<th>Blended rate (/TB) = $6,720/95</th>
<th>Blended cost = (Blended rate * storage)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td></td>
<td>95,000</td>
<td>95</td>
<td></td>
<td></td>
<td>$6,720.00</td>
<td>0.070737 70.737</td>
<td>0.070737 70.737</td>
<td>$6,720.00</td>
</tr>
</tbody>
</table>

### Member 1

<table>
<thead>
<tr>
<th>Tier</th>
<th>Storage amount (GB)</th>
<th>Storage amount (TB)</th>
<th>Unblended rate (/GB)</th>
<th>Unblended rate (/TB)</th>
<th>Unblended cost</th>
<th>Blended rate (/GB) = $6,720/95,000</th>
<th>Blended rate (/TB) = $6,720/95</th>
<th>Blended cost = (Blended rate * storage)</th>
</tr>
</thead>
<tbody>
<tr>
<td>First TB/month</td>
<td>1,000</td>
<td>1</td>
<td>$0.10</td>
<td>100</td>
<td>$100.00</td>
<td>0.070737 70.737</td>
<td>0.070737 70.737</td>
<td>$70.37</td>
</tr>
<tr>
<td>Next 49 TB/month</td>
<td>14,000</td>
<td>14</td>
<td>$0.08</td>
<td>80</td>
<td>$1,120.00</td>
<td>0.070737 70.737</td>
<td>0.070737 70.737</td>
<td>$990.318</td>
</tr>
<tr>
<td>Next 450 TB/month</td>
<td>15,000</td>
<td>15</td>
<td>$0.06</td>
<td>60</td>
<td>$900.00</td>
<td>0.070737 70.737</td>
<td>0.070737 70.737</td>
<td>$1,061.055</td>
</tr>
</tbody>
</table>

### Member 2

<table>
<thead>
<tr>
<th>Tier</th>
<th>Storage amount (GB)</th>
<th>Storage amount (TB)</th>
<th>Unblended rate (/GB)</th>
<th>Unblended rate (/TB)</th>
<th>Unblended cost</th>
<th>Blended rate (/GB) = $6,720/95,000</th>
<th>Blended rate (/TB) = $6,720/95</th>
<th>Blended cost = (Blended rate * storage)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next 49 TB/month</td>
<td>20,000</td>
<td>20</td>
<td>$0.08</td>
<td>80</td>
<td>$1,600.00</td>
<td>0.070737 70.737</td>
<td>0.070737 70.737</td>
<td>$1,414.74</td>
</tr>
<tr>
<td>Next 450 TB/month</td>
<td>15,000</td>
<td>15</td>
<td>$0.06</td>
<td>60</td>
<td>$900.00</td>
<td>0.070737 70.737</td>
<td>0.070737 70.737</td>
<td>$1,061.55</td>
</tr>
</tbody>
</table>

### Member 3

<table>
<thead>
<tr>
<th>Tier</th>
<th>Storage amount (GB)</th>
<th>Storage amount (TB)</th>
<th>Unblended rate (/GB)</th>
<th>Unblended rate (/TB)</th>
<th>Unblended cost</th>
<th>Blended rate (/GB) = $6,720/95,000</th>
<th>Blended rate (/TB) = $6,720/95</th>
<th>Blended cost = (Blended rate * storage)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next 49 TB/month</td>
<td>15,000</td>
<td>15</td>
<td>$0.08</td>
<td>80</td>
<td>$1,200.00</td>
<td>0.070737 70.737</td>
<td>0.070737 70.737</td>
<td>$1,061.55</td>
</tr>
</tbody>
</table>
Reserved Instances

AWS also offers discounted hourly rates in exchange for an upfront fee and term contract.

Zonal Reserved Instances

A Reserved Instance is a reservation that provides a discounted hourly rate in exchange for an upfront fee and term contract. Services such as Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Relational Database Service (Amazon RDS) use this approach to sell reserved capacity for hourly use of Reserved Instances. It is not a virtual machine. It is a commitment to pay in advance for specific Amazon EC2 or Amazon RDS instances. In return, you get a discounted rate as compared to On-Demand Instance usage. From a technical perspective, there is no difference between a Reserved Instance and an On-Demand Instance. When you launch an instance, AWS checks for qualifying usage across all accounts in an organization that can be applied to an active reservation. For more information, see Reserved Instances in the Amazon EC2 User Guide for Linux Instances and Working with Reserved DB Instances in the Amazon Relational Database Service Developer Guide.

When you reserve capacity with Reserved Instances, your hourly usage is calculated at a discounted rate for instances of the same usage type in the same Availability Zone.
Regional Reserved Instances

Regional Reserved Instances don't reserve capacity. Instead, they provide Availability Zone flexibility and in certain cases instance size flexibility. Availability Zone flexibility allows you to run one or more instances in any Availability Zone in your reserved AWS Region. The Reserved Instance discount is applied to any usage in any Availability Zone. Instance size flexibility provides the Reserved Instance discount to instance usage regardless of size, within that instance family. Instance size flexibility applies to only regional Reserved Instances on the Linux/Unix platform with default tenancy. For more information about regional Reserved Instances, see Reservation Details in the Cost and Usage Reports Guide in this documentation and Applying Reserved Instances in the Amazon Elastic Compute Cloud User Guide for Linux Instances.

Calculating Costs for Amazon EC2 with Reserved Instances

AWS calculates the charges for Amazon EC2 instances by aggregating all the EC2 usage for a specific instance type in a specific AWS Region for an organization.

Calculation Process

AWS calculates blended rates for Amazon EC2 instances using the following logic:

1. AWS aggregates usage for all accounts in an organization for the month or partial month, and calculates costs based on unblended rates such as rates for On-Demand and Reserved Instances. Line items for these costs are created for the management account. This bill computation model attempts to apply the lowest unblended rates that each line item is eligible for. The allocation logic first applies Reserved Instance hours, then free tier hours, and then On-Demand rates to any remaining usage. In the AWS Cost and Usage Reports, you can see line items for these aggregated costs.

2. AWS identifies each Amazon EC2 usage type in each AWS Region and allocates cost from the aggregated management account to the corresponding member account line items for identical usage types in the same region. In the AWS Cost and Usage Reports, the Unblended Rate column shows that rate applied to each line item.

   Note
   When AWS assigns Reserved Instance hours to member accounts, it always starts with the account that purchased the reservation. If there are hours from the capacity reservation left over, AWS applies them to other accounts that operate identical usage types in the same Availability Zone.
   AWS allocates a regional RI by instance size: The RI is applied first to the smallest instance in the instance family, then to the next smallest, and so on. AWS applies an RI or a fraction of an RI based on the normalization factor of the instance. The order in which AWS applies RIs doesn't result in a price difference.

Savings Plans

Savings Plans is a flexible pricing model that can help you reduce your AWS usage bill. Compute Savings Plans enables you to commit to an amount each hour, and receive discounted Amazon EC2, Fargate, and AWS Lambda usage up to that amount.

Calculating Costs with Savings Plans

AWS calculates the charges for Amazon EC2, Fargate, and AWS Lambda by aggregating all usage that's not covered by Reserved Instances, and applying the Savings Plans rates starting with the highest discount.
Blended Rates and Costs

Blended rates are the averaged rates of the Reserved Instances and On-Demand Instances that are used by member accounts in an organization in AWS Organizations. AWS calculates blended costs by multiplying the blended rate for each service with an account's usage of that service.

Note

- AWS shows each member account their charges as unblended costs. AWS continues to apply all of the consolidated billing benefits such as reservations and tiered prices across all member accounts in AWS Organizations.
- Blended rates for Amazon EC2 are calculated at the hourly level.

This section includes examples that show how AWS calculates blended rates for the following services.

- Calculating Blended Rates for Amazon S3 Standard Storage
- Calculating Blended Rates for Amazon EC2

Calculating Blended Rates for Amazon S3 Standard Storage

AWS calculates blended rates for Amazon S3 standard storage by taking the total cost of storage and dividing by the amount of data stored per month.

Using the example from Calculating Consolidated Bills (p. 156) where we calculated a cost of $6,720 for a management account and three member accounts, we calculate the blended rates for the accounts using the following logic:

1. The blended rate in GB is calculated by dividing the total cost ($6,720) by the amount of storage (95,000 GB) to produce a blended rate of $0.070737/GB. The blended rate in TB is calculated by dividing the total cost ($6,720) by the amount of storage (95 TB) to produce a blended rate of $70.737/TB.
2. The blended cost for each member account is allocated by multiplying the blended rate (for GB or TB) by the usage, resulting in the amounts listed in the Blended Cost column. For example, Member 1 uses 14,000 GB of storage priced at the blended rate of $0.070737 (or 14 TB priced at $70.737) for a blended cost of $990.318.

Calculating Blended Rates for Amazon EC2

The consolidated billing logic aggregates Amazon EC2 costs to the management account and then allocates it to the member accounts based on proportional usage.

For this example, all usage is of the same usage type, occurs in the same Availability Zone, and is for the same Reserved Instance term. This example covers Full Upfront and Partial Upfront Reserved Instances.

The following table shows line items that represent the calculation of line items for Amazon EC2 usage for a 720-hour (30-day) month. Each instance is of the same usage type (t2. small) running in the same Availability Zone. The organization has purchased three Reserved Instances for a one-year term. Member Account 1 has three Reserved Instances. Member Account 2 has no Reserved Instances, but uses an On-Demand Instance.
The data in the preceding table shows the following information:

- The organization purchased 1,440 hours of Reserved Instance capacity at a Full Upfront rate (two EC2 instances).
- The organization purchased 720 hours of Reserved Instance capacity at a Partial Upfront rate (one EC2 instance).
- Member account 1 completely uses the two Full Upfront Reserved Instances and the one Partial Upfront Reserved Instance for a total usage of 2,160 hours. Member account 2 uses 720 hours of an On-Demand Instance. Total usage for the organization is 2,880 hours (2160 + 720 = 2,880).
- The unblended rate for the three Reserved Instances is $0.00. The unblended cost of an RI is always $0.00 because RI charges are not included in blended rate calculations.
- The unblended rate for the On-Demand Instance is $0.023. Unblended rates are associated with the current price of the product. They can't be verified from information in the preceding table.
- The blended rate is calculated by dividing the total cost ($16.56) by the total amount of Amazon EC2 usage (2,880 hours). This produces a rate of $0.005750000 dollars per hour.

The AWS PDF invoice contains the AWS service charges for the payer account (management account) and associated member accounts that are part of your AWS Organizations.

This AWS PDF invoice has the following sections:

1. Overall invoice summary
2. AWS service summary for all accounts
3. Summary activity for member accounts
4. Detailed activity for member accounts

When you request this feature for your account, member account details are removed from the PDF invoice, so that you receive fewer pages.
Note
This feature only removes the member account details from the PDF invoice. You can continue to view this information in the AWS Billing console and AWS Cost Explorer.

You can request the following PDF invoice summary options:

Invoice summary option 1
Option 1 contains the following sections:
1. Overall invoice summary
2. AWS service summary for all accounts
3. Summary activity for member accounts

Option 1 excludes the detailed activity for member accounts.

Invoice summary option 2
Option 2 contains the following sections:
1. Overall invoice summary
2. AWS service summary for all accounts

Option 2 excludes the summary activity and the detailed activity for member accounts.

To request either option, see the following procedure.

To request shorter PDF invoices
1. Sign in to the AWS Support Center Console as the payer account.
2. Create an Account & billing support case.
3. For Service, choose Billing.
4. For Category, choose Consolidated Billing.
5. Follow the prompts to create your support case.
6. In the case details, specify which PDF invoice summary that you want for your account: Option 1 or 2.

After the support agent completes your request, your next available invoice is updated to use your requested invoice option. This feature doesn't apply to previously generated invoices.

Note
You can follow the same procedure to change your invoice summary option or request the original PDF invoice summary for member accounts.

AWS Support charges for accounts in an AWS Organizations

AWS calculates AWS Support fees independently for each member account. Typically an AWS Support subscription for a member account does not apply to the entire organization. Each account subscribes independently. Enterprise Support plan customers have the option to include multiple accounts in an aggregated monthly billing. Monthly charges for the Developer, Business, and Enterprise Support plans are based on each month's AWS usage, subject to a monthly minimum. AWS Support fees associated with Reserved Instance and Savings Plan purchases apply to the member accounts that made the purchase. For more information, see AWS Support Plan Pricing.
Security in AWS Billing and Cost Management

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

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

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to AWS Billing and Cost Management, see AWS Services in Scope by Compliance Program.

- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company’s requirements, and applicable laws and regulations.

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

Topics
- Data protection in AWS Billing and Cost Management (p. 164)
- AWS Identity and Access Management for AWS Billing (p. 165)
- Logging and monitoring in AWS Billing and Cost Management (p. 233)
- Compliance validation for AWS Billing and Cost Management (p. 239)
- Resilience in AWS Billing and Cost Management (p. 239)
- Infrastructure security in AWS Billing and Cost Management (p. 240)

Data protection in AWS Billing and Cost Management

The AWS shared responsibility model applies to data protection in AWS Billing and Cost Management. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. This content includes the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the AWS Security Blog.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual users with AWS IAM Identity Center or AWS Identity and Access Management (IAM). That way, each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
• Use SSL/TLS to communicate with AWS resources. We require TLS 1.2 and recommend TLS 1.3.
• Set up API and user activity logging with AWS CloudTrail.
• Use AWS encryption solutions, along with all default security controls within AWS services.
• Use advanced managed security services such as Amazon Macie, which assists in discovering and securing sensitive data that is stored in Amazon S3.
• If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-2.

We strongly recommend that you never put confidential or sensitive information, such as your customers’ email addresses, into tags or free-form text fields such as a Name field. This includes when you work with Billing and Cost Management or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form text fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

AWS Identity and Access Management for AWS Billing

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be authenticated (signed in) and authorized (have permissions) to use Billing resources. IAM is an AWS service that you can use with no additional charge.

To start activating access to the Billing console, see IAM tutorial: grant access to the Billing console in the IAM User Guide.

Topics
• Audience (p. 165)
• Overview of managing access permissions (p. 166)
• Using identity-based policies (IAM policies) for AWS Billing (p. 169)
• AWS Billing policy examples (p. 179)
• Migrating access control for AWS Billing (p. 195)

Audience

How you use IAM differs, depending on the work you do in AWS Billing.

Service user – If you use the AWS Billing service to do your job, your administrator provides you with the credentials and permissions that you need. As you use more Billing and Cost Management features, you might need additional permissions. Understanding how access is managed helps you request the right permissions from your administrator.

Service administrator – If you’re in charge of AWS Billing resources, you probably have full access to AWS Billing. You’re responsible to determine which AWS Billing features and resources employees access. You’re also responsible for submitting requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM.

IAM administrator – If you’re an IAM administrator, you might want to learn more about how you can write policies to manage access to AWS Billing.

This table summarizes the default actions that are permitted in AWS Billing for each type of billing user.
## User types and billing permissions

<table>
<thead>
<tr>
<th>User type</th>
<th>Description</th>
<th>Billing permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account owner</td>
<td>The person or entity that your account is set up under.</td>
<td>• Has full control of all Billing and Cost Management resources.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Receives a monthly invoice of AWS charges.</td>
</tr>
<tr>
<td>IAM user</td>
<td>A person or application that's defined as a user in an account by an account owner or administrative user. Accounts can contain multiple IAM users.</td>
<td>• Has permissions explicitly granted to the user or a group that includes the user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Can be granted permission to view Billing and Cost Management console pages. For more information, see</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Overview of managing access permissions (p. 166).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Can't close accounts.</td>
</tr>
<tr>
<td>Organization management account owner</td>
<td>The person or entity that's associated with an AWS Organizations management account. The management account pays for AWS usage that's incurred by a member account in an organization.</td>
<td>• Has full control of all Billing and Cost Management resources for the management account only.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Receives a monthly invoice of AWS charges for the management account and member accounts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Views the activity of member accounts in the billing reports for the management account.</td>
</tr>
<tr>
<td>Organization member account owner</td>
<td>The person or entity that's associated with an AWS Organizations member account. The management account pays for AWS usage that's incurred by a member account in an organization.</td>
<td>• Doesn't have permission to review any usage reports or account activity except for its own. Doesn't have access to usage reports or account activity for other member accounts in the organization or for the management account.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Doesn't have permission to view billing reports.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Has permission to update account information only for its own account. Can't access other member accounts or the management account.</td>
</tr>
</tbody>
</table>

### Overview of managing access permissions

You can use AWS Identity and Access Management (IAM) to control who in your account or organization has access to specific pages on the AWS Billing console. For example, you can control access to invoices and detailed information about charges and account activity, budgets, payment methods, and credits.
IAM is a feature of your AWS account. You don't need to do anything else to sign up for IAM. You're not charged for using IAM.

Topics
- Granting access to your billing information and tools (p. 167)
- About IAM Access to the AWS Billing console (p. 167)

Granting access to your billing information and tools

When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account **root user** and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see Tasks that require root user credentials in the **IAM User Guide**.

Instead, you should create a special user identity that's called an **IAM user** for anyone who might need access to the account. This approach provides individual sign-in information for each user, and you can grant each user only the permissions that they need.

You can grant some users limited access to your billing information and tools and then grant others complete access. We also recommend that the account owner use an IAM user identity to access the account.

**Important**

By default, IAM users don't have access to the **AWS Billing console**.

To grant IAM entities (such as users or groups) access to the Billing console, complete the following:

- **Activate IAM Access (p. 167)** as the AWS account root user. You only need to complete this action once for your account.
- Create your IAM identities, such as a user, group, or role.
- Use an AWS managed policy or create a customer managed policy that grants permission to specific actions on the Billing console. For more information, see Using identity-based policies (IAM policies) for AWS Billing (p. 169).

For a step-by-step guide, see the **IAM tutorial: Grant access to the Billing console** in the **IAM User Guide**.

**Note**

Permissions for Cost Explorer apply to all accounts and member accounts, regardless of the IAM policies. For more information, see **Controlling access to AWS Cost Explorer**.

About IAM Access to the AWS Billing console

By default, IAM users and roles in an AWS account can't access the Billing console. This is true even if they have IAM policies that grant access to certain Billing features. To grant access, the AWS account root user can use the **Activate IAM Access** setting.

Activate this setting in each account where you want to allow IAM user and role access to the Billing console. If you use AWS Organizations, activate this setting in each management or member account where you want to allow IAM user and role access to the Billing console.

For more information, see **Activating IAM access to the AWS Billing console (p. 14)**.

On the Billing console, the **Activate IAM Access** setting controls access to the following pages:
On the Cost Management console, the **Activate IAM Access** setting controls access to the following pages:

- Home
- Cost Explorer
- Reports
- Rightsizing recommendations
- Savings Plans recommendations
- Savings Plans utilization report
- Savings Plans coverage report
- Reservations overview
- Reservations recommendations
- Reservations utilization report
- Reservations coverage report
- Preferences

**Important**

- The **Activate IAM Access** setting alone doesn't grant IAM users and roles the necessary permissions for these pages. You must also attach the required IAM policies to those users or roles. For more information, see [Using identity-based policies (IAM policies) for AWS Billing](p. 169).
- The **Activate IAM Access** setting isn't available to IAM users with administrator access. This setting is available only to the AWS account root user.

The **Activate IAM Access** setting doesn't control access to the following pages and resources:

- Console pages for AWS Cost Anomaly Detection, Savings Plans overview, Savings Plans inventory, Purchase Savings Plans, Savings Plans cart, and customer verification
- Cost Management view in the AWS Console Mobile Application
- Billing SDK APIs (AWS Cost Explorer, AWS Budgets, and AWS Cost and Usage Reports APIs)
Using identity-based policies (IAM policies) for AWS Billing

Note
The following AWS Identity and Access Management (IAM) actions have reached the end of standard support on July 2023:

- `aws-portal` namespace
- `purchase-orders:ViewPurchaseOrders`
- `purchase-orders:ModifyPurchaseOrders`

If you haven’t migrated the old IAM actions to the new fine-grained actions, you have until December 2023 to do so.
If you’re using AWS Organizations, you can use the bulk policy migrator scripts (p. 205) to update policies from your payer account. You can also use the old to granular action mapping reference (p. 222) to verify the IAM actions that need to be added.
For more information, see the Changes to AWS Billing, AWS Cost Management, and Account Consoles Permission blog.
If you have an AWS account, or are a part of an AWS Organizations created on or after March 6, 2023, 11:00 AM (PDT), the fine-grained actions are already in effect in your organization.

This topic provides examples of several identity-based policies. These policies demonstrate how an account administrator attaches permissions policies to IAM identities (users, groups, and roles) to grant permissions so that they can perform actions on Billing resources.

For more information about your AWS account, IAM identities, and customer managed policies, see the following topics in the IAM User Guide:

- What Is IAM?
- Editing customer managed policies (console)

Important
In addition to IAM policies, you must grant IAM access to the Billing and Cost Management console on the Account Settings console page.
For more information, see the following topics:

- About IAM Access to the AWS Billing console (p. 167)
- IAM tutorial: Grant access to the billing console in the IAM User Guide

Contents

- AWS Billing actions (p. 170)
- AWS managed policies (p. 175)
  - AWSPurchaseOrdersServiceRolePolicy (p. 175)
  - AWSBillingReadOnlyAccess (p. 176)
  - Billing (p. 176)
  - AWSAccountActivityAccess (p. 178)
- Updates to AWS managed policies for AWS Billing (p. 178)
### AWS Billing actions

This table summarizes the permissions that allow or deny IAM users access to your billing information and tools. For examples of policies that use these permissions, see [AWS Billing policy examples](p. 179).

For a list of actions policies for the AWS Cost Management console, see [AWS Cost Management actions policies](p. 179) in the AWS Cost Management User Guide.

<table>
<thead>
<tr>
<th>Permission name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aws-portal:ViewBilling</td>
<td>Allow or deny IAM users permission to view the Billing and Cost Management console pages.</td>
</tr>
<tr>
<td>aws-portal:ModifyBilling</td>
<td>Allow or deny IAM users permission to modify the following Billing and Cost Management console pages:</td>
</tr>
<tr>
<td></td>
<td>• Budgets</td>
</tr>
<tr>
<td></td>
<td>• Consolidated Billing</td>
</tr>
<tr>
<td></td>
<td>• Billing preferences</td>
</tr>
<tr>
<td></td>
<td>• Credits</td>
</tr>
<tr>
<td></td>
<td>• Tax settings</td>
</tr>
<tr>
<td></td>
<td>• Payment methods</td>
</tr>
<tr>
<td></td>
<td>• Purchase orders</td>
</tr>
<tr>
<td></td>
<td>• Cost Allocation Tags</td>
</tr>
<tr>
<td></td>
<td>To allow IAM users to modify these console pages, you must allow both ModifyBilling and ViewBilling. For an example policy, see Allow IAM users to modify billing information (p. 185).</td>
</tr>
<tr>
<td>aws-portal:ViewAccount</td>
<td>Allow or deny IAM users permission to view Account Settings.</td>
</tr>
<tr>
<td>aws-portal:ModifyAccount</td>
<td>Allow or deny IAM users permission to modify Account Settings.</td>
</tr>
<tr>
<td></td>
<td>To allow IAM users to modify account settings, you must allow both ModifyAccount and ViewAccount.</td>
</tr>
<tr>
<td></td>
<td>For an example of a policy that explicitly denies an IAM user access to the Account Settings console page, see Deny access to account settings, but allow full access to all other billing and usage information (p. 185).</td>
</tr>
<tr>
<td>aws-portal:ViewPaymentMethods</td>
<td>Allow or deny IAM users permission to view Payment Methods.</td>
</tr>
<tr>
<td>aws-portal:ModifyPaymentMethods</td>
<td>Allow or deny IAM users permission to modify Payment Methods.</td>
</tr>
<tr>
<td></td>
<td>To allow users to modify payment methods, you must allow both ModifyPaymentMethods and ViewPaymentMethods.</td>
</tr>
<tr>
<td>Permission name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>billing:ListBillingViews</td>
<td>Allow or deny users to get billing information for pro forma billing groups. This is made using AWS Billing Conductor on the Bills page, or AWS Cost and Usage Reports. For more information about viewing your billing group details, see Viewing your billing group details in the AWS Billing Conductor User Guide.</td>
</tr>
<tr>
<td>sustainability:GetCarbonFootprintSummary</td>
<td>Allow or deny IAM users permission to view the AWS customer carbon footprint tool and data. This is accessible from the AWS Cost and Usage Reports page of the Billing and Cost Management console. For an example of a policy, see Allow IAM users to view your billing information and carbon footprint report (p. 182).</td>
</tr>
<tr>
<td>cur:DescribeReportDefinitions</td>
<td>Allow or deny IAM users permission to view AWS Cost and Usage Reports. AWS Cost and Usage Reports permissions apply to all reports that are created using the AWS Cost and Usage Reports Service API and the Billing and Cost Management console. If you create reports using the Billing and Cost Management console, we recommend that you update the permissions for IAM users. Not updating the permissions will result in users losing access to viewing, editing, and removing reports on the console reports page. For an example of a policy, see Allow IAM users to access the reports console page (p. 182).</td>
</tr>
<tr>
<td>cur:PutReportDefinition</td>
<td>Allow or deny IAM users permission to create AWS Cost and Usage Reports. AWS Cost and Usage Reports permissions apply to all reports that are created using the AWS Cost and Usage Reports Service API and the Billing and Cost Management console. If you create reports using the Billing and Cost Management console, we recommend that you update the permissions for IAM users. Not updating the permissions will result in users losing access to viewing, editing, and removing reports on the console reports page. For an example of a policy, see Allow IAM users to access the reports console page (p. 182).</td>
</tr>
<tr>
<td>Permission name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>cur:DeleteReportDefinition</td>
<td>Allow or deny IAM users permission to delete AWS Cost and Usage Reports. AWS Cost and Usage Reports permissions apply to all reports that are created using the AWS Cost and Usage Reports Service API and the Billing and Cost Management console. If you create reports using the Billing and Cost Management console, we recommend that you update the permissions for IAM users. Not updating the permissions will result in users losing access to viewing, editing, and removing reports on the console reports page. For an example of a policy, see Create, view, edit, or delete AWS Cost and Usage Reports (p. 188).</td>
</tr>
<tr>
<td>cur:ModifyReportDefinition</td>
<td>Allow or deny IAM users permission to modify AWS Cost and Usage Reports. AWS Cost and Usage Reports permissions apply to all reports that are created using the AWS Cost and Usage Reports Service API and the Billing and Cost Management console. If you create reports using the Billing and Cost Management console, we recommend that you update the permissions for IAM users. Not updating the permissions will result in users losing access to viewing, editing, and removing reports on the console reports page. For an example of a policy, see Create, view, edit, or delete AWS Cost and Usage Reports (p. 188).</td>
</tr>
<tr>
<td>ce:CreateCostCategoryDefinition</td>
<td>Allow or deny IAM users permissions to create cost categories. For an example policy, see View and manage cost categories.</td>
</tr>
<tr>
<td>ce:DeleteCostCategoryDefinition</td>
<td>Allow or deny IAM users permissions to delete cost categories. For an example policy, see View and manage cost categories.</td>
</tr>
<tr>
<td>ce:DescribeCostCategoryDefinition</td>
<td>Allow or deny IAM users permissions to view cost categories. For an example policy, see View and manage cost categories.</td>
</tr>
<tr>
<td>ce:ListCostCategoryDefinitions</td>
<td>Allow or deny IAM users permissions to list cost categories. For an example policy, see View and manage cost categories.</td>
</tr>
<tr>
<td>Permission name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ce:UpdateCostCategoryDefinition</td>
<td>Allow or deny IAM users permissions to update cost categories.</td>
</tr>
<tr>
<td></td>
<td>For an example policy, see <a href="#">View and manage cost categories</a>.</td>
</tr>
<tr>
<td>aws-portal:ViewUsage</td>
<td>Allow or deny IAM users permission to view AWS usage Reports.</td>
</tr>
<tr>
<td></td>
<td>To allow IAM users to view usage reports, you must allow both ViewUsage and ViewBilling.</td>
</tr>
<tr>
<td></td>
<td>For an example policy, see <a href="#">Allow IAM users to access the reports console page</a>.</td>
</tr>
<tr>
<td>pricing:DescribeServices</td>
<td>Allow or deny IAM users permission to view AWS service products and pricing via the AWS Price List Service API.</td>
</tr>
<tr>
<td></td>
<td>To allow IAM users to use AWS Price List Service API, you must allow DescribeServices, GetAttributeValues, and GetProducts.</td>
</tr>
<tr>
<td></td>
<td>For an example policy, see <a href="#">Find products and prices</a>.</td>
</tr>
<tr>
<td>pricing:GetAttributeValues</td>
<td>Allow or deny IAM users permission to view AWS service products and pricing via the AWS Price List Service API.</td>
</tr>
<tr>
<td></td>
<td>To allow IAM users to use AWS Price List Service API, you must allow DescribeServices, GetAttributeValues, and GetProducts.</td>
</tr>
<tr>
<td></td>
<td>For an example policy, see <a href="#">Find products and prices</a>.</td>
</tr>
<tr>
<td>pricing:GetProducts</td>
<td>Allow or deny IAM users permission to view AWS service products and pricing via the AWS Price List Service API.</td>
</tr>
<tr>
<td></td>
<td>To allow IAM users to use AWS Price List Service API, you must allow DescribeServices, GetAttributeValues, and GetProducts.</td>
</tr>
<tr>
<td></td>
<td>For an example policy, see <a href="#">Find products and prices</a>.</td>
</tr>
<tr>
<td>purchase-orders:ViewPurchaseOrders</td>
<td>Allow or deny IAM users permission to view Purchase Orders (p. 68).</td>
</tr>
<tr>
<td></td>
<td>For an example policy, see <a href="#">View and manage purchase orders</a>.</td>
</tr>
<tr>
<td>Permission name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>purchase-orders:ModifyPurchaseOrders</td>
<td>Allow or deny IAM users permission to modify Purchase Orders (p. 68). For an example policy, see View and manage purchase orders.</td>
</tr>
<tr>
<td>tax:GetExemptions</td>
<td>Allows IAM users read-only access to view exemptions and exemption types by tax console. For an example policy, see Allow IAM users to view US tax exemptions and create AWS Support cases.</td>
</tr>
<tr>
<td>tax:UpdateExemptions</td>
<td>Allows IAM users to upload an exemption to the US tax exemptions console. For an example policy, see Allow IAM users to view US tax exemptions and create AWS Support cases.</td>
</tr>
<tr>
<td>support:CreateCase</td>
<td>Allows IAM users to file support cases, required to upload exemption from tax exemptions console. For an example policy, see Allow IAM users to view US tax exemptions and create AWS Support cases.</td>
</tr>
<tr>
<td>support:AddAttachmentsToSet</td>
<td>Allows IAM users to attach documents to support cases that are required to upload exemption certificates to the tax exemption console. For an example policy, see Allow IAM users to view US tax exemptions and create AWS Support cases.</td>
</tr>
<tr>
<td>customer-verification:GetCustomerVerificationEligibility</td>
<td>(For customers with an India billing or contact address only) Allow or deny IAM users permission to retrieve customer verification eligibility.</td>
</tr>
<tr>
<td>customer-verification:GetCustomerVerificationDetails</td>
<td>(For customers with an India billing or contact address only) Allow or deny IAM users permission to retrieve customer verification data.</td>
</tr>
<tr>
<td>customer-verification:CreateCustomerVerificationDetails</td>
<td>(For customers with an India billing or contact address only) Allow or deny IAM users permission to create customer verification data.</td>
</tr>
<tr>
<td>customer-verification:UpdateCustomerVerificationDetails</td>
<td>(For customers with an India billing or contact address only) Allow or deny IAM users permission to update customer verification data.</td>
</tr>
</tbody>
</table>
AWS managed policies

Managed policies are standalone identity-based policies that you can attach to multiple users, groups, and roles in your AWS account. You can use AWS managed policies to control access in Billing.

An AWS managed policy is a standalone policy that's created and administered by AWS. AWS managed policies are designed to provide permissions for many common use cases. AWS managed policies make it easier for you to assign appropriate permissions to users, groups, and roles than if you had to write the policies yourself.

You can't change the permissions defined in AWS managed policies. AWS occasionally updates the permissions that are defined in an AWS managed policy. When this occurs, the update affects all principal entities (users, groups, and roles) that the policy is attached to.

Billing provides several AWS managed policies for common use cases.

Topics

- AWSPurchaseOrdersServiceRolePolicy (p. 175)
- AWSBillingReadOnlyAccess (p. 176)
- Billing (p. 176)
- AWSAccountActivityAccess (p. 178)

AWSPurchaseOrdersServiceRolePolicy

This managed policy grants full access to the Billing console and to the purchase orders console. The policy allows the user to view, create, update, and delete the account's purchase orders.

```json
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "account:GetAccountInformation",
            "account:GetContactInformation",
            "aws-portal:*Billing",
            "consolidatedbilling:GetAccountBillingRole",
            "invoicing:GetInvoicePDF",
            "payments:GetPaymentInstrument",
            "payments:ListPaymentPreferences",
            "purchase-orders:AddPurchaseOrder",
            "purchase-orders:DeletePurchaseOrder",
            "purchase-orders:GetPurchaseOrder",
            "purchase-orders:ListPurchaseOrderInvoices",
            "purchase-orders:ListPurchaseOrders",
            "purchase-orders:ListTagsForResource",
            "purchase-orders:ModifyPurchaseOrders",
            "purchase-orders:TagResource",
            "purchase-orders:UntagResource",
            "purchase-orders:UpdatePurchaseOrder",
            "tax:ListTaxRegistrations"
         ],
         "Resource":"
      }
   ]
}
```
AWS Billing User Guide
Using IAM policies for Billing

AWSBillingReadOnlyAccess

This managed policy grants users access to view the AWS Billing console.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "account:GetAccountInformation",
        "aws-portal:ViewBilling",
        "billing:GetBillingData",
        "billing:GetBillingDetails",
        "billing:GetBillingNotifications",
        "billing:GetBillingPreferences",
        "billing:GetContractInformation",
        "billing:GetCredits",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:ListBillingViews",
        "ce:ListCostAllocationTags",
        "consolidatedbilling:GetAccountBillingRole",
        "consolidatedbilling:ListLinkedAccounts",
        "cur:GetClassicReport",
        "cur:GetClassicReportPreferences",
        "cur:GetUsageReport",
        "freetier:GetFreeTierAlertPreference",
        "freetier:GetFreeTierUsage",
        "invoicing:GetInvoiceEmailDeliveryPreferences",
        "invoicing:GetInvoicePDF",
        "invoicing:ListInvoiceSummaries",
        "payments:GetPaymentInstrument",
        "payments:GetPaymentStatus",
        "payments:ListPaymentPreferences",
        "purchase-orders:GetPurchaseOrder",
        "purchase-orders:ListPurchaseOrderInvoices",
        "purchase-orders:ListPurchaseOrders",
        "purchase-orders:ListTagsForResource",
        "purchase-orders:ViewPurchaseOrders",
        "tax:GetTaxInheritance",
        "tax:GetTaxRegistrationDocument",
        "tax:ListTaxRegistrations"
      ],
      "Resource": "*"
    }
  ]
}
```

Billing

This managed policy grants users permission to view and edit the Billing console and AWS Cost Management consoles. This includes viewing account usage, modifying budgets and payment methods.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": ["account:GetAccountInformation"
```
Using IAM policies for Billing

"aws-portal:*Billing",
"aws-portal:*PaymentMethods",
"aws-portal:*Usage",
"billing:GetBillingData",
"billing:GetBillingDetails",
"billing:GetBillingNotifications",
"billing:GetBillingPreferences",
"billing:GetContractInformation",
"billing:GetCredits",
"billing:GetIAMAccessPreference",
"billing:GetSellerOfRecord",
"billing:ListBillingViews",
"billing:PutContractInformation",
"billing:RedeemCredits",
"billing:UpdateBillingPreferences",
"billing:UpdateIAMAccessPreference",
"budgets:ModifyBudget",
"budgets:ViewBudget",
"ce:CreateNotificationSubscription",
"ce:CreateReport",
"ce:DeleteNotificationSubscription",
"ce:DeleteReport",
"ce:ListCostAllocationTags",
"ce:UpdateCostAllocationTagsStatus",
"ce:UpdateNotificationSubscription",
"ce:UpdatePreferences",
"ce:UpdateReport",
"consolidatedbilling:GetAccountBillingRole",
"consolidatedbilling:ListLinkedAccounts",
"cur:DeleteReportDefinition",
"cur:DescribeReportDefinitions",
"cur:GetClassicReport",
"cur:GetClassicReportPreferences",
"cur:GetUsageReport",
"cur:ModifyReportDefinition",
"cur:GetReportDefinition",
"cur:GetReportPreferences",
"cur:PutReportDefinition",
"cur:GetFreeTierAlertPreference",
"freetier:GetFreeTierAlertPreference",
"freetier:GetFreeTierUsage",
"invoicing:GetInvoiceEmailDeliveryPreferences",
"invoicing:GetInvoicePDF",
"invoicing:ListInvoiceSummaries",
"invoice:GetInvoiceEmailDeliveryPreferences",
"payments:CreatePaymentInstrument",
"payments:DeletePaymentInstrument",
"payments:GetPaymentInstrument",
"payments:UpdatePaymentPreferences",
"payments:ListPaymentPreferences",
"payments:MakePayment",
"purchase-orders:AddPurchaseOrder",
"purchase-orders:DeletePurchaseOrder",
"purchase-orders:GetPurchaseOrder",
"purchase-orders:GetPurchaseOrderInvoices",
"purchase-orders:ListPurchaseOrders",
"purchase-orders:ListTagsForResource",
"purchase-orders:ModifyPurchaseOrders",
"purchase-orders:TagResource",
"purchase-orders:UntagResource",
"purchase-orders:UpdatePurchaseOrder",
"purchase-orders:UpdatePurchaseOrderStatus",
"purchase-orders:ViewPurchaseOrders",
"tax:BatchPutTaxRegistration",
"tax:DeleteTaxRegistration",

Version 2.0
177
AWS Billing User Guide
Using IAM policies for Billing

AWSAccountActivityAccess
This managed policy grants users permission to view the **Account activity** page.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "account:GetRegionOptStatus",
        "account:GetAccountInformation",
        "account:GetAlternateContact",
        "account:GetChallengeQuestions",
        "account:GetContactInformation",
        "account:GetCountryInformation",
        "account:GetPendingUsageReports",
        "account:GetRegions",
        "aws-portal:ViewBilling",
        "billing:GetIAMAccessPreference",
        "billing:GetSellerOfRecord",
        "billing:GetUsageReports",
        "billing:ListBillingReports",
        "billing:ListPaymentPreferences",
        "billing:ViewAccountBilling",
        "billing:ViewBillingSummary",
        "payments:ListPaymentPreferences"
      ],
      "Resource": "*
    }
  ]
}
```

Updates to AWS managed policies for AWS Billing

View details about updates to AWS managed policies for AWS Billing since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the AWS Billing Document history page.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
</table>
| **Billing (p. 176)** and **AWSBillingReadOnlyAccess (p. 176)** | We added the following cost allocation tag-related permissions to Billing:  
  - ce:ListCostAllocationTags  
  - ce:UpdateCostAllocationTagsStatus | July 26, 2023 |

- Update to existing policies

Version 2.0

178
AWS Billing policy examples

Note
The following AWS Identity and Access Management (IAM) actions have reached the end of standard support on July 2023:

- `aws-portal` namespace
- `purchase-orders:ViewPurchaseOrders`
- `purchase-orders:ModifyPurchaseOrders`

If you haven't migrated the old IAM actions to the new fine-grained actions, you have until December 2023 to do so.
If you're using AWS Organizations, you can use the bulk policy migrator scripts (p. 205) to update policies from your payer account. You can also use the old to granular action mapping reference (p. 222) to verify the IAM actions that need to be added.

For more information, see the Changes to AWS Billing, AWS Cost Management, and Account Consoles Permission blog.

If you have an AWS account, or are a part of an AWS Organizations created on or after March 6, 2023, 11:00 AM (PDT), the fine-grained actions are already in effect in your organization.

This topic contains example policies that you can attach to your IAM user or group to control access to your account’s billing information and tools. The following basic rules apply to IAM policies for Billing and Cost Management:

- **Version** is always 2012-10-17.
- **Effect** is always Allow or Deny.
- **Action** is the name of the action or a wildcard (*).

  The action prefix is budgets for AWS Budgets, cur for AWS Cost and Usage Reports, aws-portal for AWS Billing, or ce for Cost Explorer.

- **Resource** is always * for AWS Billing.

  For actions that are performed on a budget resource, specify the budget Amazon Resource Name (ARN).

- It's possible to have multiple statements in one policy.

For a list of actions policies for the AWS Cost Management console, see AWS Cost Management policy examples in the AWS Cost Management user guide.

**Important**

- These policies require that you activate IAM user access to the Billing and Cost Management console on the Account Settings console page. For more information, see About IAM Access to the AWS Billing console (p. 167).
- To use AWS managed policies, see AWS managed policies (p. 175).

**Topics**

- Allow IAM users to view your billing information (p. 181)
- Allow IAM users to view your billing information and carbon footprint report (p. 182)
- Allow IAM users to access the reports console page (p. 182)
- Deny IAM users access to the Billing and Cost Management consoles (p. 183)
- Deny AWS Console cost and usage widget access for member accounts (p. 183)
- Deny AWS Console cost and usage widget access for specific IAM users and roles (p. 183)
- Allow IAM users to view your billing information, but deny access to carbon footprint report (p. 183)
- Allow IAM users to access carbon footprint reporting, but deny access to billing information (p. 184)
- Allow full access to AWS services but deny IAM users access to the Billing and Cost Management consoles (p. 184)
- Allow IAM users to view the Billing and Cost Management consoles except for account settings (p. 185)
- Allow IAM users to modify billing information (p. 185)
- Deny access to account settings, but allow full access to all other billing and usage information (p. 185)
AWS Billing User Guide
AWS Billing policy examples

- Deposit reports into an Amazon S3 bucket (p. 186)
- Find products and prices (p. 186)
- View costs and usage (p. 187)
- Enable and disable AWS Regions (p. 187)
- View and manage cost categories (p. 187)
- Create, view, edit, or delete AWS Cost and Usage Reports (p. 188)
- View and manage purchase orders (p. 188)
- View and update the Cost Explorer preferences page (p. 188)
- View, create, update, and delete using the Cost Explorer reports page (p. 190)
- View, create, update, and delete reservation and Savings Plans alerts (p. 191)
- Allow read-only access to AWS Cost Anomaly Detection (p. 192)
- Allow AWS Budgets to apply IAM policies and SCPs (p. 192)
- Allow AWS Budgets to apply IAM policies and SCPs and target EC2 and RDS instances (p. 193)
- Allow IAM users to view US tax exemptions and create AWS Support cases (p. 194)
- (For customers with a billing or contact address in India) Allow read-only access to customer verification information (p. 194)
- (For customers with a billing or contact address in India) View, create, and update customer verification information (p. 194)

Allow IAM users to view your billing information

To allow an IAM user to view your billing information without giving the IAM user access to sensitive account information, use a policy similar to the following example policy. Such a policy prevents users from accessing your password and account activity reports. This policy allows IAM users to view the following Billing and Cost Management console pages, without giving them access to the Account Settings or Reports console pages:

- Dashboard
- Cost Explorer
- Bills
- Orders and invoices
- Consolidated Billing
- Preferences
- Credits
- Advance Payment

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "aws-portal:ViewBilling",
      "Resource": "*"
    }
  ]
}
```
Allow IAM users to view your billing information and carbon footprint report

To allow an IAM user to view both billing information and carbon footprint reporting, use a policy similar to the following example. This policy prevents users from accessing your password and account activity reports. This policy allows IAM users to view the following Billing and Cost Management console pages, without giving them access to the Account Settings or Reports console pages:

- Dashboard
- Cost Explorer
- Bills
- Orders and invoices
- Consolidated Billing
- Preferences
- Credits
- Advance Payment
- The AWS customer carbon footprint tool section of the AWS Cost and Usage Reports page

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": "aws-portal:ViewBilling",
         "Resource": "*"
      },
      {
         "Effect": "Allow",
         "Action": "sustainability:GetCarbonFootprintSummary",
         "Resource": "*"
      }
   ]
}
```

Allow IAM users to access the reports console page

To allow an IAM user to access the Reports console page and to view the usage reports that contain account activity information, use a policy similar to this example policy.

For definitions of each action, see AWS Billing actions.

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "aws-portal:ViewUsage",
            "aws-portal:ViewBilling",
            "cur:DescribeReportDefinitions",
            "cur:PutReportDefinition",
            "cur:DeleteReportDefinition",
            "cur:ModifyReportDefinition"
         ],
         "Resource": "*"
      }
   ]
}
```
Deny IAM users access to the Billing and Cost Management consoles

To explicitly deny an IAM user access to the all Billing and Cost Management console pages, use a policy similar to this example policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "aws-portal:*",
      "Resource": "*"
    }
  ]
}
```

Deny AWS Console cost and usage widget access for member accounts

To restrict member (linked) account access to cost and usage data, use your management (payer) account to access the Cost Explorer preferences tab and uncheck **Linked Account Access**. This will deny access to cost and usage data from the Cost Explorer (AWS Cost Management) console, Cost Explorer API, and AWS Console Home page's cost and usage widget regardless of the IAM actions a member account's IAM user or role has.

Deny AWS Console cost and usage widget access for specific IAM users and roles

To deny AWS Console cost and usage widget access for specific IAM users and roles, use the permissions policy below.

**Note**
Adding this policy to an IAM user or role will deny users access to Cost Explorer (AWS Cost Management) console and Cost Explorer APIs as well.

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

Allow IAM users to view your billing information, but deny access to carbon footprint report

To allow an IAM user to both billing information in the Billing and Cost Management consoles, but doesn't allow access to the AWS customer carbon footprint tool. This tool is located in the AWS Cost and Usage Reports page.
Allow IAM users to access carbon footprint reporting, but deny access to billing information

To allow an IAM user to access the AWS customer carbon footprint tool in the AWS Cost and Usage Reports page, but denies access to view billing information in the Billing and Cost Management consoles.

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": "aws-portal:ViewBilling",
         "Resource": "*"
      },
      {
         "Effect": "Allow",
         "Action": "sustainability:GetCarbonFootprintSummary",
         "Resource": "*"
      }
   ]
}
```

Allow full access to AWS services but deny IAM users access to the Billing and Cost Management consoles

To deny IAM users access to everything on the Billing and Cost Management console, use the following policy. Deny user access to AWS Identity and Access Management (IAM) to prevent access to the policies that control access to billing information and tools.

**Important**
This policy doesn't allow any actions. Use this policy in combination with other policies that allow specific actions.

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": [
            "aws-portal:*",
            "iam:*"
         ],
         "Resource": "*"
      }
   ]
}
```
Allow IAM users to view the Billing and Cost Management consoles except for account settings

This policy allows read-only access to all of the Billing and Cost Management console. This includes the Payments Method and Reports console pages. However, this policy denies access to the Account Settings page. This means it protects the account password, contact information, and security questions.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "aws-portal:View*",  
      "Resource": "*"  
    },  
    {  
      "Effect": "Deny",  
      "Action": "aws-portal:*Account",  
      "Resource": "*"  
    }  
  ]
}
```

Allow IAM users to modify billing information

To allow IAM users to modify account billing information in the Billing and Cost Management console, allow IAM users to view your billing information. The following policy example allows an IAM user to modify the Consolidated Billing, Preferences, and Credits console pages. It also allows an IAM user to view the following Billing and Cost Management console pages:

- Dashboard
- Cost Explorer
- Bills
- Orders and invoices
- Advance Payment

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

Deny access to account settings, but allow full access to all other billing and usage information

To protect your account password, contact information, and security questions, deny IAM user access to Account Settings while still enabling full access to the rest of the functionality in the Billing and Cost Management console. The following is an example policy.

```
{
```

Version 2.0
185
Deposit reports into an Amazon S3 bucket

The following policy allows Billing and Cost Management to save your detailed AWS bills to an Amazon S3 bucket if you own both the AWS account and the Amazon S3 bucket. This policy must be applied to the Amazon S3 bucket, rather than an IAM user. This is because it’s a resource-based policy, not a user-based policy. We recommend that you deny IAM user access to the bucket for IAM users who don’t need access to your bills.

Replace **DOC-EXAMPLE-BUCKET1** with the name of your bucket.

For more information, see [Using Bucket Policies and User Policies](#) in the [Amazon Simple Storage Service User Guide](#).

```json
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "billingreports.amazonaws.com"
    },
    "Action": [
      "s3:GetBucketAcl",
      "s3:GetBucketPolicy"
    ],
    "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1"
  },
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "billingreports.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET1/"*
  }
]
```

Find products and prices

To allow an IAM user to use the AWS Price List Service API, use the following policy to grant them access.

This policy grants permission to use both the AWS Price List Bulk API AWS Price List Query API.
View costs and usage

To allow IAM users to use the AWS Cost Explorer API, use the following policy to grant them access.

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

Enable and disable AWS Regions

For an example IAM policy that allows users to enable and disable Regions, see AWS: Allows Enabling and Disabling AWS Regions in the IAM User Guide.

View and manage cost categories

To allow IAM users to use, view, and manage cost categories, use the following policy to grant them access.

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "aws-portal:ViewBilling",
            "ce:GetCostAndUsage",
            "ce:DescribeCostCategoryDefinition",
            "ce:UpdateCostCategoryDefinition",
            "ce:CreateCostCategoryDefinition",
            "ce:DeleteCostCategoryDefinition",
            "pricing:DescribeServices",
            "pricing:GetAttributeValues",
            "pricing:GetProducts",
            "pricing:GetPriceListFileUrl",
            "pricing:ListPriceLists"
         ],
         "Resource": [
            "*"
         ]
      }
   ]
}
```
Create, view, edit, or delete AWS Cost and Usage Reports

This policy allows an IAM user to create, view, edit, or delete sample-report using the API.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ManageSampleReport",
      "Effect": "Allow",
      "Action": [
        "cur:PutReportDefinition",
        "cur:DeleteReportDefinition",
        "cur:ModifyReportDefinition"
      ],
      "Resource": "arn:aws:cur:*:123456789012:definition/sample-report"
    },
    {
      "Sid": "DescribeReportDefs",
      "Effect": "Allow",
      "Action": "cur:DescribeReportDefinitions",
      "Resource": "*"
    }
  ]
}
```

View and manage purchase orders

This policy allows an IAM user to view and manage purchase orders, using the following policy to grant access.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "aws-portal:ViewBilling",
        "purchase-orders:*"
      ],
      "Resource": "*"
    }
  ]
}
```

View and update the Cost Explorer preferences page

This policy allows an IAM user to view and update using the Cost Explorer preferences page.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UpdatePreferences",
      "Effect": "Allow",
      "Action": "ce:UpdatePreferences",
      "Resource": "*"
    }
  ]
}
```
The following policy allows IAM users to view Cost Explorer, but deny permission to view or edit the Preferences page.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewBilling",
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Deny",
            "Action": [
                "ce:GetPreferences",
                "ce:UpdatePreferences"
            ],
            "Resource": "*"
        }
    ]
}
```

The following policy allows IAM users to view Cost Explorer, but deny permission to edit the Preferences page.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewBilling"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Deny",
            "Action": [
                "ce:UpdatePreferences"
            ],
            "Resource": "*"
        }
    ]
}
```

The following policy allows IAM users to view Cost Explorer, but deny permission to view or edit the Preferences page.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewBilling"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Deny",
            "Action": [
                "ce:GetPreferences",
                "ce:UpdatePreferences"
            ],
            "Resource": "*"
        }
    ]
}
```
View, create, update, and delete using the Cost Explorer reports page

This policy allows an IAM user to view, create, update, and delete using the Cost Explorer reports page.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "aws-portal:ViewBilling",
        "ce:CreateReport",
        "ce:UpdateReport",
        "ce:DeleteReport"
      ],
      "Resource": "*"
    }
  ]
}
```

The following policy allows IAM users to view Cost Explorer, but deny permission to view or edit the Reports page.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "aws-portal:ViewBilling"
      ],
      "Resource": "*"
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Deny",
      "Action": [
        "ce:DescribeReport",
        "ce:CreateReport",
        "ce:UpdateReport",
        "ce:DeleteReport"
      ],
      "Resource": "*"
    }
  ]
}
```

The following policy allows IAM users to view Cost Explorer, but deny permission to edit the Reports page.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "aws-portal:ViewBilling"
      ],
      "Resource": "*"
    }
  ]
}
```
View, create, update, and delete reservation and Savings Plans alerts

This policy allows an IAM user to view, create, update, and delete reservation expiration alerts and Savings Plans alerts. To edit reservation expiration alerts or Savings Plans alerts, a user needs all three granular actions: ce:CreateNotificationSubscription, ce:UpdateNotificationSubscription, and ce:DeleteNotificationSubscription.

The following policy allows IAM users to view Cost Explorer, but denies permission to view or edit the Reservation Expiration Alerts and Savings Plans alert pages.

```
[  
  "Version": "2012-10-17",  
  "Statement": [  
    
    
    
],  
]
```

The following policy allows IAM users to view Cost Explorer, but denies permission to view or edit the Reservation Expiration Alerts and Savings Plans alert pages.

```
[  
  "Version": "2012-10-17",  
  "Statement": [  
    
    
    
],  
]
```

The following policy allows IAM users to view Cost Explorer, but denies permission to view or edit the Reservation Expiration Alerts and Savings Plans alert pages.

```
[  
  "Version": "2012-10-17",  
  "Statement": [  
    
    
    
],  
]
```
The following policy allows IAM users to view Cost Explorer, but denies permission to edit the Reservation Expiration Alerts and Savings Plans alert pages.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "aws-portal:ViewBilling"
         ],
         "Resource": "*"
      },
      {
         "Sid": "VisualEditor1",
         "Effect": "Deny",
         "Action": [
            "ce:CreateNotificationSubscription",
            "ce:UpdateNotificationSubscription",
            "ce:DeleteNotificationSubscription"
         ],
         "Resource": "*"
      }
   ]
}
```

**Allow read-only access to AWS Cost Anomaly Detection**

To allow IAM users read-only access to AWS Cost Anomaly Detection, use the following policy to grant them access. `ce:ProvideAnomalyFeedback` is optional as a part of the read-only access.

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

**Allow AWS Budgets to apply IAM policies and SCPs**

This policy allows AWS Budgets to apply IAM policies and service control policies (SCPs) on behalf of the user.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "VisualEditor0",
         "Effect": "Allow",
         "Action": [
            "ce:GetNotificationSubscription",
            "ce:SubscribeToNotificationSubscription",
            "ce:UpdateNotificationSubscription",
            "ce:DeleteNotificationSubscription"
         ],
         "Resource": "*"
      }
   ]
}
```
Allow AWS Budgets to apply IAM policies and SCPs and target EC2 and RDS instances

This policy allows AWS Budgets to apply IAM policies and service control policies (SCPs), and to target Amazon EC2 and Amazon RDS instances on behalf of the user.

Trust policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "budgets.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Permissions policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstanceStatus",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:DetachGroupPolicy",
        "iam:DetachRolePolicy",
        "iam:DetachUserPolicy",
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "rds:DescribeDBInstances",
        "rds:StartDBInstance",
        "rds:StopDBInstance",
        "ssm:StartAutomationExecution"
      ]
    }
  ]
}
```
Allow IAM users to view US tax exemptions and create AWS Support cases

This policy allows an IAM user to view US tax exemptions and create AWS Support cases to upload exemption certificates in the tax exemption console.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "aws-portal:*",
                "tax:GetExemptions",
                "tax:UpdateExemptions",
                "support:CreateCase",
                "support:AddAttachmentsToSet"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow"
        }
    ]
}
```

(For customers with a billing or contact address in India) Allow read-only access to customer verification information

This policy allows IAM users read-only access to customer verification information.

For definitions of each action, see AWS Billing actions (p. 170).

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "customer-verification:GetCustomerVerificationEligibility",
                "customer-verification:GetCustomerVerificationDetails"
            ],
            "Resource": "*"
        }
    ]
}
```

(For customers with a billing or contact address in India) View, create, and update customer verification information

This policy allows IAM users to manage their customer verification information.

For definitions of each action, see AWS Billing actions (p. 170)

```json
{
```

Version 2.0
194
Migrating access control for AWS Billing

Note
The following AWS Identity and Access Management (IAM) actions have reached the end of standard support on July 2023:

- `aws-portal` namespace
- `purchase-orders:ViewPurchaseOrders`
- `purchase-orders:ModifyPurchaseOrders`

If you haven't migrated the old IAM actions to the new fine-grained actions, you have until December 2023 to do so.

If you're using AWS Organizations, you can use the bulk policy migrator scripts (p. 205) to update policies from your payer account. You can also use the old to granular action mapping reference (p. 222) to verify the IAM actions that need to be added.

For more information, see the Changes to AWS Billing, AWS Cost Management, and Account Consoles Permission blog.

You can use fine-grained access controls to provide individuals in your organization access to AWS Billing and Cost Management services. For example, you can provide access to Cost Explorer without providing access to the AWS Billing console.

To use the fine-grained access controls, you'll need to migrate your policies from under `aws-portal` to the new IAM actions.

The following IAM actions in your permission policies or service control policies (SCP) require updating with this migration:

- `aws-portal:ViewAccount`
- `aws-portal:ViewBilling`
- `aws-portal:ViewPaymentMethods`
- `aws-portal:ViewUsage`
- `aws-portal:ModifyAccount`
- `aws-portal:ModifyBilling`
- `aws-portal:ModifyPaymentMethods`
- `purchase-orders:ViewPurchaseOrders`
- `purchase-orders:ModifyPurchaseOrders`

To learn how to use the Affected policies tool to identify your impacted IAM policies, see How to use the affected policies tool (p. 204).
Note
API access to AWS Cost Explorer, AWS Cost and Usage Reports, and AWS Budgets remains unaffected.
About IAM Access to the AWS Billing console (p. 167) remain unchanged.

Topics
- Managing access permissions (p. 196)
- How to use the affected policies tool (p. 204)
- Use scripts to bulk migrate your policies to use fine-grained IAM actions (p. 205)
- Mapping fine-grained IAM actions reference (p. 222)

Managing access permissions

AWS Billing integrates with the AWS Identity and Access Management (IAM) service so that you can control who in your organization can access specific pages on the AWS Billing console. This includes features like Payments, Billing, Credits, Free Tier, Payment preferences, Consolidated billing, Tax settings, and Account pages.

Use the following IAM permissions for granular control for the Billing console.

To provide fine-grained access, replace the aws-portal policy with account, billing, payments, freetier, invoicing, tax, and consolidatedbilling.

Additionally, replace purchase-orders:ViewPurchaseOrders and purchase-orders:ModifyPurchaseOrders with the fine-grained actions under purchase-orders, account, and payments.

Using fine-grained AWS Billing actions

This table summarizes the permissions that allow or deny IAM users and roles access to your billing information. For examples of policies that use these permissions, see AWS Billing policy examples (p. 179).

For a list of actions for the AWS Cost Management console, see AWS Cost Management actions policies in the AWS Cost Management User Guide.

<table>
<thead>
<tr>
<th>Feature name in the Billing console</th>
<th>IAM action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Billing Home</td>
<td>account:GetAccountInformation, billing:Get*, payments:List*, tax:List*</td>
<td>Grants permission to view the Home page. These are read-only permissions. Note These are permissions for the console only. No API access is available for these permissions.</td>
</tr>
<tr>
<td>Bills</td>
<td>account:GetAccountInformation, billing:Get*, consolidatedbilling:Get*, consolidatedbilling:List*</td>
<td>Grants permission to view the Bills page. These are read-only permissions. Note These are permissions for the console only. No</td>
</tr>
<tr>
<td>Feature name in the Billing console</td>
<td>IAM action</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>invoicing:List*</td>
<td>API access is available for these permissions.</td>
<td></td>
</tr>
<tr>
<td>payments:List*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>invoicing:Get*</td>
<td>Grants permission to download invoices from the Bills page.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This is a permission for the console only. No API access is available for this permission.</td>
<td></td>
</tr>
<tr>
<td>cur:Get*</td>
<td>Grants permission to download CSV reports from the Bills page.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This is a permission for the console only. No API access is available for this permission.</td>
<td></td>
</tr>
<tr>
<td>billing:ListBillingViews</td>
<td>Grants permission to view the ARN and description of each AWS Billing Conductor billing group created. This is required to create a report preference for specific groups.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This is a permission for the console only. No API access is available for this permission.</td>
<td></td>
</tr>
<tr>
<td>Payments</td>
<td>account:GetAccountInformation</td>
<td>Grants permission to view the Payments page. These are read-only permissions to the Payments due, Unapplied funds, Transaction, and Advance pay tabs.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>These are permissions for the console only. No API access is available for these permissions.</td>
<td></td>
</tr>
<tr>
<td>invoicing:Get*</td>
<td>Grants permission to download an invoice from the Transactions tab.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This is a permission for the console only. No API access is available for this permission.</td>
<td></td>
</tr>
<tr>
<td>Feature name in the Billing console</td>
<td>IAM action</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>payments:Update*</td>
<td>Grants permission action required to use Advance Pay and set up payment details.</td>
</tr>
<tr>
<td></td>
<td>payments:Make*</td>
<td>Grants permission to generate a funding request document for Advance Pay, and make a payment.</td>
</tr>
<tr>
<td></td>
<td>invoicing:Get*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>billing:Get*</td>
<td>Grants permission to view the <strong>Credits</strong> page.</td>
</tr>
<tr>
<td></td>
<td>account:GetAccountInformation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>billing: RedeemCredits</td>
<td>Grants permission to redeem credits.</td>
</tr>
<tr>
<td><strong>Credits</strong></td>
<td>account:GetAccountInformation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>account:GetContactInformation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>payments:Get*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>payments:List*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>purchase-orders: ListPurchaseOrders</td>
<td></td>
</tr>
<tr>
<td></td>
<td>purchase-orders: ListPurchaseOrderInvoices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>tax: ListTaxRegistrations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>consolidatedbilling: GetAccountBillingRole</td>
<td></td>
</tr>
<tr>
<td></td>
<td>purchase-orders: GetPurchaseOrder</td>
<td>Grants permission to view details of a purchase order.</td>
</tr>
<tr>
<td></td>
<td>purchase-orders: AddPurchaseOrder</td>
<td>Grants permission to add a purchase order.</td>
</tr>
<tr>
<td></td>
<td>purchase-orders: DeletePurchaseOrder</td>
<td>Grants permission to delete a purchase order.</td>
</tr>
<tr>
<td></td>
<td>purchase-orders: UpdatePurchaseOrder</td>
<td>Grants permission to update purchase orders and purchase order status.</td>
</tr>
<tr>
<td></td>
<td>purchase-orders: UpdatePurchaseOrderStatus</td>
<td></td>
</tr>
</tbody>
</table>

Version 2.0
198
<table>
<thead>
<tr>
<th>Feature name in the Billing console</th>
<th>IAM action</th>
<th>Description</th>
</tr>
</thead>
</table>
| **AWS Cost and Usage Reports**     | cur:GetClassic* | Grants permission to view a list of AWS CUR reports on the **[AWS Cost and Usage Reports](https://docs.aws.amazon.com/cost-summary/latest/cur-guide/)** page.  
**Note**  
cur:GetClassic* is a permission for the console only. No API access is available for this permission. |
| **billing:ListBillingViews**       | billing:ListBillingViews | Grants permission to view the ARN and description of each billing group created in AWS Billing Conductor. This is required to create a report preference for specific groups.  
**Note**  
This is a permission for the console only. No API access is available for this permission. |
**Note**  
cur:Validate* is a permission for the console only. No API access is available for these permissions. |
**Note**  
cur:Validate* is a permission for the console only. No API access is available for these permissions. |
<p>| cur:DeleteReportDefinition         | Grants permission to delete AWS CUR reports. |
| cur:GetUsage*                      | Grants permission to download usage reports. |
| sustainability:GetCarbonFootprintSummary | Grants permission to view sustainability data for your AWS account. |</p>
<table>
<thead>
<tr>
<th>Feature name in the Billing console</th>
<th>IAM action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cost categories</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>account:GetAccountInformation</td>
<td>Grants permission to view cost categories.</td>
<td></td>
</tr>
<tr>
<td>ce:ListCostCategoryDefinitions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ce:DescribeCostCategoryDefinition</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ce:GetCostAndUsage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ce:ListTagsForResource</td>
<td></td>
<td></td>
</tr>
<tr>
<td>consolidatedbilling:GetAccountBillingRole</td>
<td></td>
<td></td>
</tr>
<tr>
<td>billing:Get*</td>
<td>Grants permission to create cost categories.</td>
<td></td>
</tr>
<tr>
<td>ce:TagResource</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ce:ListCostAllocationTags</td>
<td></td>
<td></td>
</tr>
<tr>
<td>consolidatedbilling:List*</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ce:CreateCostCategoryDefinition</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pricing:DescribeServices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ce:UpdateCostCategoryDefinition</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ce:UntagResource</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ce:DeleteCostCategoryDefinition</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cost allocation tags</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>account:GetAccountInformation</td>
<td>Grants permission to view cost allocation tags.</td>
<td></td>
</tr>
<tr>
<td>ce:ListCostAllocationTags</td>
<td></td>
<td></td>
</tr>
<tr>
<td>consolidatedbilling:GetAccountBillingRole</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ce:UpdateCostAllocationTags</td>
<td>Grants permission to activate or deactivate cost allocation tags.</td>
<td></td>
</tr>
<tr>
<td><strong>AWS Budgets</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>budgets:ViewBudget</td>
<td>Grants permission to view the budgets page.</td>
<td></td>
</tr>
<tr>
<td>budgets:DescribeBudgetActionsForBudget</td>
<td></td>
<td></td>
</tr>
<tr>
<td>budgets:DescribeBudgetAction</td>
<td></td>
<td></td>
</tr>
<tr>
<td>budgets:DescribeBudgetActionsForAccount</td>
<td></td>
<td></td>
</tr>
<tr>
<td>budgets:DescribeBudgetActionHistories</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature name in the Billing console</td>
<td>IAM action</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>budgets:CreateBudgetAction</td>
<td>Grants permission to create, delete, and modify Budgets and Budgets actions.</td>
</tr>
<tr>
<td></td>
<td>budgets:ExecuteBudgetAction</td>
<td></td>
</tr>
<tr>
<td></td>
<td>budgets:DeleteBudgetAction</td>
<td></td>
</tr>
<tr>
<td></td>
<td>budgets:UpdateBudgetAction</td>
<td></td>
</tr>
<tr>
<td></td>
<td>budgets:ModifyBudget</td>
<td></td>
</tr>
<tr>
<td>Free tier</td>
<td>billing:Get*</td>
<td>Grants permission to view free tier usage limits and month to date usage status.</td>
</tr>
<tr>
<td></td>
<td>freetier:Get*</td>
<td></td>
</tr>
<tr>
<td>Billing preferences</td>
<td>account:GetAccountInformation</td>
<td>Grants permission actions required to view all sections on the Billing preferences page.</td>
</tr>
<tr>
<td></td>
<td>billing:Get*</td>
<td>Note</td>
</tr>
<tr>
<td></td>
<td>consolidatedbilling:Get*</td>
<td>These are permissions for the console only. No API access is available for these permissions.</td>
</tr>
<tr>
<td></td>
<td>consolidatedbilling:List*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cur:GetClassic*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cur:Validate*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>freetier:Get*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>invoicing:Get*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>billing:Update*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>freetier:Put*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cur:PutClassic*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>s3:ListAllMyBuckets</td>
<td></td>
</tr>
<tr>
<td></td>
<td>s3:CreateBucket</td>
<td></td>
</tr>
<tr>
<td></td>
<td>s3:PutBucketPolicy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>s3:GetBucketLocation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>invoicing:Put*</td>
<td>Grants permission to make the following changes in the Billing preferences page:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Turn credit sharing to RI or Savings Plans discount sharing on or off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Set Free Tier Usage Alert preferences</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Set detailed billing reports delivery settings and preferences</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Set or update the PDF invoice by email preferences</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note</td>
</tr>
<tr>
<td></td>
<td>billing:Update*, freetier:Put*, cur:PutClassic*</td>
<td>These are permissions for the console only. No API access is available for these permissions.</td>
</tr>
<tr>
<td>Feature name in the Billing console</td>
<td>IAM action</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Payment preferences</strong></td>
<td>account:GetAccountInformation</td>
<td>Grants permission to view the Payment preferences page. <strong>Note</strong> These are permissions for the console only. No API access is available for these permissions.</td>
</tr>
<tr>
<td></td>
<td>billing:Get*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>payments:GetPaymentInstrument</td>
<td></td>
</tr>
<tr>
<td></td>
<td>payments:List*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>payments:GetPaymentStatus</td>
<td></td>
</tr>
<tr>
<td></td>
<td>payments:Update*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>payments:Make*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>payments:CreatePaymentInstrument</td>
<td></td>
</tr>
<tr>
<td></td>
<td>payments:DeletePaymentInstrument</td>
<td></td>
</tr>
<tr>
<td></td>
<td>tax:PutTaxRegistration</td>
<td>Grants permission to update or delete tax registration numbers.</td>
</tr>
<tr>
<td></td>
<td>tax:Delete*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>payments:UpdatePaymentPreferences</td>
<td></td>
</tr>
<tr>
<td></td>
<td>payments:CreatePaymentInstrument</td>
<td></td>
</tr>
<tr>
<td></td>
<td>payments:Update*</td>
<td></td>
</tr>
<tr>
<td><strong>Tax settings</strong></td>
<td>tax:List*</td>
<td>Grants permission to view tax settings.</td>
</tr>
<tr>
<td></td>
<td>tax:Get*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>tax:BatchPut*</td>
<td>Grants permission action required to update tax settings.</td>
</tr>
<tr>
<td></td>
<td>tax:Put*</td>
<td>Grants permission to set tax inheritance.</td>
</tr>
<tr>
<td></td>
<td>tax:UpdateExemptions</td>
<td>Grants permission to update tax exemption.</td>
</tr>
<tr>
<td></td>
<td>support:CreateCase</td>
<td></td>
</tr>
<tr>
<td></td>
<td>support:AddAttachmentsToSet</td>
<td></td>
</tr>
<tr>
<td>Feature name in the Billing console</td>
<td>IAM action</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Account</strong></td>
<td>account:Get*</td>
<td>Grants permission to view Account settings.</td>
</tr>
<tr>
<td></td>
<td>account:List*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>billing:Get*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>payments:List*</td>
<td></td>
</tr>
<tr>
<td>account:CloseAccount</td>
<td></td>
<td>Grants permission to close AWS accounts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td>account:DisableRegion</td>
<td></td>
<td>Grants permission to turn off an AWS Region on the Account page.</td>
</tr>
<tr>
<td>account:EnableRegion</td>
<td></td>
<td>Grants permission to turn on an AWS Region on the Account page.</td>
</tr>
<tr>
<td>account:PutAlternateContact</td>
<td></td>
<td>Grants permission to write alternate contacts for the account.</td>
</tr>
<tr>
<td>account:PutChallengeQuestions</td>
<td></td>
<td>Grants permission to set security challenge questions for the account.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td>account:PutContactInformation</td>
<td></td>
<td>Grants permission action required to set or write main contact information, including address, for the account.</td>
</tr>
</tbody>
</table>
# Migrating access control

<table>
<thead>
<tr>
<th>Feature name in the Billing console</th>
<th>IAM action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>billing:PutContractInformation</td>
<td></td>
<td>Grants permission to set the account contract information, if the account is used to service public-sector customers. Information that can be pulled includes end user organization names, contract number, and PO numbers.</td>
</tr>
<tr>
<td>billing:Update*</td>
<td></td>
<td>Grants permission action required to turn on or turn off the Activate IAM Access setting on the Account page.</td>
</tr>
<tr>
<td>payments:Update*</td>
<td></td>
<td>Grants permission to set advance pay, currency preference, billing contact details and address, and payment terms and conditions.</td>
</tr>
</tbody>
</table>

## How to use the affected policies tool

**Note**
The following AWS Identity and Access Management (IAM) actions have reached the end of standard support on July 2023:

- `aws-portal` namespace
- `purchase-orders:ViewPurchaseOrders`
- `purchase-orders:ModifyPurchaseOrders`

If you haven't migrated the old IAM actions to the new fine-grained actions, you have until December 2023 to do so.

If you're using AWS Organizations, you can use the bulk policy migrator scripts (p. 205) to update policies from your payer account. You can also use the old to granular action mapping reference (p. 222) to verify the IAM actions that need to be added.

For more information, see the Changes to AWS Billing, AWS Cost Management, and Account Consoles Permission blog.

If you have an AWS account, or are a part of an AWS Organizations created on or after March 6, 2023, 11:00 AM (PDT), the fine-grained actions are already in effect in your organization.

You can use the Affected policies tool in the Billing console to identify IAM policies (excluding SCPs), and reference the IAM actions impacted by this migration. This tool operates within the boundaries of the AWS account you're logged into, and information regarding other AWS Organizations accounts are not disclosed.
To use the Affected policies tool

2. Paste the following URL into your browser to access the Affected policies tool: [https://console.aws.amazon.com/poliden/home?region=us-east-1#/](https://console.aws.amazon.com/poliden/home?region=us-east-1#/).
   
   **Note**
   You must have the `iam:GetAccountAuthorizationDetails` permission to view this page.
3. Review the table that lists the IAM policies impacted. Use the Deprecated IAM actions column to review specific IAM actions referenced in a policy.
4. Choose an IAM policy name you wish to edit.
5. Once you're redirected to the IAM console, update the impacted IAM action with the new action. Don't remove any existing `aws-portal` or `purchase-orders` action if you have any.
   
   For a list of new actions, see Using fine-grained AWS Billing actions (p. 196).
6. Repeat steps 3 to 5 for all listed policies.
7. Once all of the policies are resolved, access the Affected policies tool to confirm there are no policies listed.

Use scripts to bulk migrate your policies to use fine-grained IAM actions

**Note**
The following AWS Identity and Access Management (IAM) actions have reached the end of standard support on July 2023:

- `aws-portal` namespace
- `purchase-orders:ViewPurchaseOrders`
- `purchase-orders:ModifyPurchaseOrders`

If you haven't migrated the old IAM actions to the new fine-grained actions, you have until December 2023 to do so.
If you're using AWS Organizations, you can use the bulk policy migrator scripts (p. 205) to update policies from your payer account. You can also use the old to granular action mapping reference (p. 222) to verify the IAM actions that need to be added.
For more information, see the Changes to AWS Billing, AWS Cost Management, and Account Consoles Permission blog.
If you have an AWS account, or are a part of an AWS Organizations created on or after March 6, 2023, 11:00 AM (PDT), the fine-grained actions are already in effect in your organization.

To help migrate your IAM policies to use new actions, known as fine-grained actions, you can use scripts from the AWS Samples website.

You run these scripts from the payer account of your organization to identify the following affected policies in your organization that use the old IAM actions:

- Customer managed IAM policies
- Role, group, and user IAM inline policies
- Service control policies (SCPs) (applies to the payer account only)
- Permission sets
The scripts generate suggestions for new actions that correspond to existing actions that are used in the policy. You then review the suggestions and use the scripts to add the new actions across all affected policies in your organization. You don't need to update AWS managed policies or AWS managed SCPs (for example, AWS Control Tower and AWS Organizations SCPs).

You use these scripts to:

- Streamline the policy updates to help you manage the affected policies from the payer account.
- Reduce the amount of time that you need to update the policies. You don't need to sign into each member account and manually update the policies.
- Group identical policies from different member accounts together. You can then review and apply the same updates across all identical policies, instead of reviewing them one by one.
- Ensure that user access remains unaffected after AWS retires the old IAM actions on July 6, 2023.

For more information about policies and service control policies (SCPs), see the following topics:

- **Managing IAM policies** in the *IAM User Guide*
- **Service control policies (SCPs)** in the *AWS Organizations User Guide*
- **Custom permissions** in the *IAM Identity Center User Guide*

**Overview**

Follow this topic to complete the following steps:

**Topics**

- Prerequisites (p. 206)
- Step 1: Set up your environment (p. 207)
- Step 2: Create the CloudFormation StackSet (p. 208)
- Step 3: Identify the affected policies (p. 209)
- Step 4: Review the suggested changes (p. 213)
- Step 5: Update the affected policies (p. 214)
- Step 6: Revert your changes (Optional) (p. 216)
- IAM policy examples (p. 217)

**Prerequisites**

To get started, you must do the following:

- Download and install *Python 3*
- Sign in to your payer account and verify that you have an IAM principal that has the following IAM permissions:

  ```
  "iam:GetAccountAuthorizationDetails",
  "iam:GetPolicy",
  "iam:GetPolicyVersion",
  "iam:GetUserPolicy",
  "iam:GetGroupPolicy",
  "iam:GetRole",
  "iam:GetRolePolicy",
  "iam:CreatePolicyVersion",
  "iam:DeletePolicyVersion",
  "iam:ListAttachedRolePolicies",
  "iam:ListPolicyVersions",
  ```
"iam:PutUserPolicy",
"iam:PutGroupPolicy",
"iam:PutRolePolicy",
"iam:SetDefaultPolicyVersion",
"organizations:ListAccounts",
"organizations:ListPolicies",
"organizations:DescribePolicy",
"organizations:UpdatePolicy",
"organizations:DescribeOrganization",
"sso:DescribePermissionSet",
"sso:DescribePermissionSetProvisioningStatus",
"sso:GetInlinePolicyForPermissionSet",
"sso:ListInstances",
"sso:ListPermissionSets",
"sso:ProvisionPermissionSet",
"sso:PutInlinePolicyToPermissionSet",
"sts:AssumeRole"

Tip
To get started, we recommend that you use a subset of an account, such as a test account, to verify that the suggested changes are expected. You can then run the scripts again for remaining accounts in your organization.

Step 1: Set up your environment
To get started, download the required files from the AWS Samples website. You then run commands to set up your environment.

To set up your environment
1. Clone the repository from the AWS Samples website. In a command line window, you can use the following command:

```
git clone https://github.com/aws-samples/bulk-policy-migrator-scripts-for-account-cost-billing-consoles.git
```

2. Navigate to the directory where you downloaded the files. You can use the following command:

```
cd bulk-policy-migrator-scripts-for-account-cost-billing-consoles
```

In the repository, you can find the following scripts and resources:

- billing_console_policy_migrator_role.json – The CloudFormation template that creates the BillingConsolePolicyMigratorRole IAM role in member accounts of your organization. This role allows the scripts to assume the role, and then read and update the affected policies.

- action_mapping_config.json – Contains the one-to-many mapping of the old actions to the new actions. The scripts use this file to suggest the new actions for each affected policy that contains the old actions.

Each old action corresponds to multiple fine-grained actions. The new actions suggested in the file provide users access to the same AWS services before the migration.

- identify_affected_policies.py – Scans and identifies affected policies in your organization. This script generates a affected_policies_and_suggestions.json file that lists the affected policies along with the suggested new actions.

Affected policies that use the same set of old actions are grouped together in the JSON file, so that you can review or update the suggested new actions.
• `update_affected_policies.py` – Updates the affected policies in your organization. The script inputs the `affected_policies_and_suggestions.json` file, and then adds the suggested new actions to the policies.

• `rollback_affected_policies.py` – (Optional) Reverts changes made to the affected policies. This script removes the new fine-grained actions from the affected policies.

3. Run the following commands to set up and activate the virtual environment.

   ```bash
   python3 -m venv venv
   source venv/bin/activate
   ```

4. Run the following command to install the AWS SDK for Python (Boto3) dependency.

   ```bash
   pip install -r requirements.txt
   ```

   **Note**
   You must configure your AWS credentials to use the AWS Command Line Interface (AWS CLI). For more information, see [AWS SDK for Python (Boto3)](https://aws.amazon.com/boto3/).

For more information, see the `README.md` file.

### Step 2: Create the CloudFormation StackSet

Follow this procedure to create a CloudFormation stack set. This stack set then creates the **BillingConsolePolicyMigratorRole** IAM role for all member accounts in your organization.

**Note**
You only need to complete this step once from the management account (payer account).

#### To create the CloudFormation StackSet

1. In a text editor, open the `billing_console_policy_migrator_role.json` file, and replace each instance of `<management_account>` with the account ID of the payer account (for example, `123456789012`).

2. Save the file.

3. Sign in to the AWS Management Console as the payer account.

4. In the CloudFormation console, create a stack set with the `billing_console_policy_migrator_role.json` file that you updated.

   For more information, see [Creating a stack set on the AWS CloudFormation console](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/creating-a-stack-set.html) in the AWS CloudFormation User Guide.

After CloudFormation creates the stack set, each member account in your organization has an **BillingConsolePolicyMigratorRole** IAM role.

The IAM role contains the following permissions:

```json
"iam:GetAccountAuthorizationDetails",
"iam:GetPolicy",
"iam:GetPolicyVersion",
"iam:GetUserPolicy",
"iam:GetGroupPolicy",
"iam:GetRolePolicy",
```

Version 2.0

208
"iam:CreatePolicyVersion",
"iam:DeletePolicyVersion",
"iam:ListPolicyVersions",
"iam:PutUserPolicy",
"iam:PutGroupPolicy",
"iam:PutRolePolicy",
"iam:SetDefaultPolicyVersion"

Notes

- For each member account, the scripts call the AssumeRole API operation to get temporary credentials to assume the BillingConsolePolicyMigratorRole IAM role.
- The scripts call the ListAccounts API operation to get all member accounts.
- The scripts also call IAM API operations to perform the read and write permissions to the policies.

Step 3: Identify the affected policies

After you create the stack set and downloaded the files, run the identify_affected_policies.py script. This script assumes the BillingConsolePolicyMigratorRole IAM role for each member account, and then identifies the affected policies.

To identify the affected policies

1. Navigate to the directory where you downloaded the scripts.
   
   ```
   cd policy_migration_scripts/scripts
   ```

2. Run the identify_affected_policies.py script.

You can use the following input parameters:

- AWS accounts that you want the script to scan. To specify accounts, use the following input parameters:
  - `--all` – Scans all member accounts in your organization.
  - `--accounts` – Scans a subset of member accounts in your organization.
  - `--exclude-accounts` – Excludes specific member accounts in your organization.
  - `--action-mapping-config-file` – (Optional) Specify the path to the action_mapping_config.json file. The script uses this file to generate suggested updates for affected policies. If you don't specify the path, the script uses the action_mapping_config.json file in the folder.

```python
python3 identify_affected_policies.py --all
python3 identify_affected_policies.py --accounts 111122223333, 444455556666, 777788889999
python3 identify_affected_policies.py --all --exclude-accounts 111111111111, 222222222222, 333333333333
python3 identify_affected_policies.py --action-mapping-config-file c:\Users\username\Desktop\Scripts\action_mapping_config.json --all
```
Note
You can't specify organizational units (OUs) with this script.

After you run the script, it creates two JSON files in a Affected_Policies_<Timestamp> folder:

• affected_policies_and_suggestions.json
• detailed_affected_policies.json

affected_policies_and_suggestions.json
Lists the affected policies with the suggested new actions. Affected policies that use the same set of old actions are grouped together in the file.

This file contains the following sections:
• Metadata that provides an overview of the accounts that you specified in the script, including:
  • Accounts scanned and the input parameter used for the identify_affected_policies.py script
  • Number of affected accounts
  • Number of affected policies
  • Number of similar policy groups
• Similar policy groups – Includes the list of accounts and policy details, including the following sections:
  • ImpactedPolicies – Specifies which policies are affected and included in the group
  • ImpactedPolicyStatements – Provides information about the Sid blocks that currently use the old actions in the affected policy. This section includes the old actions and IAM elements, such as Effect, Principal, NotPrincipal, NotAction, and Condition.
  • SuggestedPolicyStatementsToAppend – Provides the suggested new actions that are added as new SID block.

When you update the policies, this block is appended at the end of the policies.

Example Example affected_policies_and_suggestions.json file
This file groups together policies that are similar based on the following criteria:
• Same old actions used – Policies that have the same old actions across all SID blocks.
• Matching details – In addition to affected actions, the policies have identical IAM elements, such as:
  • Effect (Allow/Deny)
  • Principal (who is allowed or denied access)
  • NotAction (what actions are not allowed)
  • NotPrincipal (who is explicitly denied access)
  • Resource (which AWS resources the policy applies to)
  • Condition (any specific conditions under which the policy applies)

Note
For more information, see IAM policy examples (p. 217).

Example Example affected_policies_and_suggestions.json

```json
[
  {
    "AccountsScanned": [ 
      "111111111111",
      "222222222222"
    ],
    "TotalAffectedAccounts": 2,
```
{
  "GroupName": "Group1",
  "ImpactedPolicies": [{
    "Account": "111111111111",
    "PolicyType": "UserInlinePolicy",
    "PolicyName": "Inline-Test-Policy-Allow",
    "PolicyIdentifier": "1111111_1-user:Inline-Test-Policy-Allow"
  },
  {
    "Account": "222222222222",
    "PolicyType": "UserInlinePolicy",
    "PolicyName": "Inline-Test-Policy-Allow",
    "PolicyIdentifier": "222222_1-group:Inline-Test-Policy-Allow"
  }]
},
"ImpactedPolicyStatements": [
  [
    "Sid": "VisualEditor0",
    "Effect": "Allow",
    "Action": [
      "aws-portal:ViewAccounts"
    ],
    "Resource": "*"
  ]
],
"SuggestedPolicyStatementsToAppend": [
  [
    "Sid": "BillingConsolePolicyMigrator0",
    "Effect": "Allow",
    "Action": [
      "account:GetAccountInformation",
      "account:GetAlternateContact",
      "account:GetChallengeQuestions",
      "account:GetContactInformation",
      "billing:GetContractInformation",
      "billing:GetIAMAccessPreference",
      "billing:GetSellerOfRecord",
      "payments:ListPaymentPreferences"
    ],
    "Resource": "*"
  ]
],
"GroupName": "Group2",
"ImpactedPolicies": [{
  "Account": "111111111111",
  "PolicyType": "UserInlinePolicy",
  "PolicyName": "Inline-Test-Policy-deny",
  "PolicyIdentifier": "1111111_2-user:Inline-Test-Policy-deny"
},
  {
    "Account": "222222222222",
    "PolicyType": "UserInlinePolicy",
    "PolicyName": "Inline-Test-Policy-deny",
    "PolicyIdentifier": "222222_2-group:Inline-Test-Policy-deny"
  }]
},
"ImpactedPolicyStatements": [
  [
    "Sid": "VisualEditor0",
    "Effect": "deny",
    "Action": [
      "aws-portal:ModifyAccount"
    ],
    "Resource": "*"
  ]
]
detailed_affected_policies.json

Contains the definition of all affected policies that the identify_affected_policies.py script identified for member accounts.

The file groups similar policies together. You can use this file as reference, so that you can review and manage policy changes without needing to sign in to each member account to review the updates for each policy and account individually.

You can search the file for the policy name (for example, YourCustomerManagedReadOnlyAccessBillingUser) and then review the affected policy definitions.

Example Example: detailed_affected_policies.json

```json
[
  {
    "Account": "111111111111",
    "PolicyType": "CustomerManagedPolicy",
    "PolicyName": "AwsPortalviewAccount",
    "PolicyIdentifier": "arn:aws:iam::111111111111:policy/AwsPortalviewAccount",
    "PolicyDocument": {
      "Version": "2012-10-17",
      "Statement": [{
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": ["aws-portal:ViewAccount"],
        "Resource": "*"
      }]
    }
  },
  {
    "Account": "222222222222",
    "PolicyType": "CustomerManagedPolicy",
    "PolicyName": "AwsPortalviewAccount",
    "PolicyIdentifier": "arn:aws:iam::222222222222:policy/AwsPortalviewAccount",
    "PolicyDocument": {
      "Version": "2012-10-17",
      "Statement": [{
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": ["aws-portal:ViewAccount"],
        "Resource": "*"
      }]
    }
  }
]
```
"Sid": "VisualEditor0",
"Effect": "Allow",
"Action": [
  "aws-portal:ViewAccount"
],
"Resource": "*"
}
}

{  
"Account": "111111111111",
"PolicyType": "CustomerManagedPolicy",
"PolicyName": "AwsPortalModifyAccount",
"PolicyIdentifier": "arn:aws:iam::111111111111:policy/AwsPortalModifyAccount",
"PolicyDocument": {
  
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": [
      "aws-portal:ModifyAccount"
    ],
    "Resource": "*"
  }]
}
}

{  
"Account": "222222222222",
"PolicyType": "CustomerManagedPolicy",
"PolicyName": "AwsPortalModifyAccount",
"PolicyIdentifier": "arn:aws:iam::222222222222:policy/AwsPortalModifyAccount",
"PolicyDocument": {
  
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": [
      "aws-portal:ModifyAccount"
    ],
    "Resource": "*"
  }]
}
}

**Step 4: Review the suggested changes**

After the script creates the affected_policies_and_suggestions.json file, review it and make any changes.

**To review the affected policies**

1. In a text editor, open the affected_policies_and_suggestions.json file.
2. In the AccountsScanned section, verify that the number of similar groups identified across the scanned accounts is expected.
3. Review the suggested fine-grained actions that will be added to the affected policies.
4. Update your file as needed and then save it.

Example 1: Update the `action_mapping_config.json` file

You can update the suggested mappings in the `action_mapping_config.json`. After you update the file, you can rerun the `identify_affected_policies.py` script. This script generates updated suggestions for the affected policies.

You can make multiple versions of the `action_mapping_config.json` file to change the policies for different accounts with different permissions. For example, you might create one file named `action_mapping_config_test.json` to migrate permissions for your test accounts and `action_mapping_config_production.json` for your production accounts.

Example 2: Update the `affected_policies_and_suggestions.json` file

To make changes to the suggested replacements for a specific affected policy group, you can directly edit the suggested replacements section within the `affected_policies_and_suggestions.json` file.

Any changes that you make in this section are applied to all policies within that specific affected policy group.

Example 3: Customize a specific policy

If you find that a policy within an affected policy group that needs different changes than the suggested updates, you can do the following:

- Exclude specific accounts from the `identify_affected_policies.py` script. You can then review those excluded accounts separately.
- Update the affected Sid blocks by removing the affected policies and accounts that need different permissions. Create a JSON block that includes only the specific accounts or excludes them from the current update affected policy run.

When you rerun the `identify_affected_policies.py` script, only the relevant accounts appear in the updated block. You can then refine the suggested replacements for that specific Sid block.

Step 5: Update the affected policies

After you review and refine the suggested replacements, run the `update_affected_policies.py` script. The script takes the `affected_policies_and_suggestions.json` file as input. This script assumes the `BillingConsolePolicyMigratorRole` IAM role to update the affected policies listed in the `affected_policies_and_suggestions.json` file.

To update the affected policies

1. If you haven't already, open a command line window for the AWS CLI.
2. Enter the following command to run the `update_affected_policies.py` script. You can enter the following input parameter:

   - The directory path of the `affected_policies_and_suggestions.json` file that contains a list of the affected policies to be updated. This file is an output of the previous step.

   ```bash
   python3 update_affected_policies.py --affected-policies-directory Affected_Policies_<Timestamp>
   ```

The `update_affected_policies.py` script updates the affected policies within the `affected_policies_and_suggestions.json` file with the suggested new actions. The script adds a
Sid block to the policies, identified as BillingConsolePolicyMigrator#, where # corresponds to an incremental counter (for example, 1, 2, 3).

For example, if there are multiple Sid blocks in the affected policy that use old actions, the script adds multiple Sid blocks that appear as BillingConsolePolicyMigrator# to correspond to each Sid block.

**Important**

- The script doesn't remove old IAM actions from the policies, and or change existing Sid blocks in the policies. Instead, it creates Sid blocks and appends them to the end of the policy. These new Sid blocks have the suggested new actions from the JSON file. This ensures that the permissions of the original policies aren't changed.
- We recommend that you do not change the name of the BillingConsolePolicyMigrator# Sid blocks in case you need to revert your changes.

**Example Example: Policy with appended Sid blocks**

See the appended Sid blocks in the BillingConsolePolicyMigrator1 and BillingConsolePolicyMigrator2 blocks.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [ "ce:*", "aws-portal:ViewAccount" ],
      "Resource": "+",
      "Principal": {
         "AWS": "arn:aws:iam::111111111111:BillingRole"
      },
      "Condition": {
         "BoolIfExists": {
            "aws:MultiFactorAuthPresent": "true"
         }
      }
   },
   { "Sid": "BillingConsolePolicyMigrator1",
   "Effect": "Allow",
   "Action": [ "account:GetAccountInformation",
               "account:GetAlternateContact",
               "account:GetChallengeQuestions",
               "account:GetContactInformation",
               "billing:GetContractInformation",
               "billing:GetIAMAccessPreference",
               "billing:GetSellerOfRecord",
               "payments:ListPaymentPreferences"
            ],
   "Resource": "*",
   "Principal": {
      "AWS": "arn:aws:iam::111111111111:BillingRole"
   },
   "Condition": {
      "BoolIfExists": {
         "aws:MultiFactorAuthPresent": "true"
      }
   }
   }
}  ```
The script generates a status report that contains unsuccessful operations and outputs the JSON file locally.

**Example Example: Status report**

```json
[
  {
    "Account": "111111111111",
    "PolicyType": "Customer Managed Policy",
    "PolicyName": "AwsPortalViewPaymentMethods",
    "PolicyIdentifier": "identifier",
    "Status": "FAILURE", // FAILURE or SKIPPED
    "ErrorMessage": "Error message details"
  }
]
```

**Important**

- If you re-run the `identify_affected_policies.py` and `update_affected_policies.py` scripts, they skip all policies that contain the `BillingConsolePolicyMigratorRole#Sid` block. The scripts assume that those policies were previously scanned and updated, and that they don't require additional updates. This prevents the script from duplicating the same actions in the policy.
- After you update the affected policies, you can use the new IAM by using the affected policies tool. If you identify any issues, you can use the tool to switch back to the previous actions. You can also use a script to revert your policy updates.

For more information, see [How to use the affected policies tool](#) (p. 204) and the [Changes to AWS Billing, Cost Management, and Account Consoles Permissions blog post](#).

- To manage your updates, you can:
  - Run the scripts for each account individually.
  - Run the script in batches for similar accounts, such as testing, QA, and production accounts.
  - Run the script for all accounts.
  - Choose a mix between updating some accounts in batches, and then updating others individually.

**Step 6: Revert your changes (Optional)**

The `rollback_affected_policies.py` script reverts the changes applied to each affected policy for the specified accounts. The script removes all `Sid` blocks that the `update_affected_policies.py` script appended. These `Sid` blocks have the `BillingConsolePolicyMigratorRole#` format.
To revert your changes

1. If you haven't already, open a command line window for the AWS CLI.
2. Enter the following command to run the `rollback_affected_policies.py` script. You can enter the following input parameters:

   - `--accounts`
     - Specifies a comma-separated list of the AWS account IDs that you want to include in the rollback.
     - The following example scans the policies in the specified AWS accounts, and removes any statements with the `BillingConsolePolicyMigrator# Sid` block.

   ```
   python3 rollback_affected_policies.py --accounts 111122223333, 555555555555, 666666666666
   ```

   - `--all`
     - Includes all AWS account IDs in your organization.
     - The following example scans all policies in your organization, and removes any statements with the `BillingConsolePolicyMigratorRole# Sid` block.

   ```
   python3 rollback_affected_policies.py --all
   ```

   - `--exclude-accounts`
     - Specifies a comma-separated list of the AWS account IDs that you want to exclude from the rollback.
     - You can use this parameter only when you also specify the `--all` parameter.
     - The following example scans the policies for all AWS accounts in your organization, except for the specified accounts.

   ```
   python3 rollback_affected_policies.py --all --exclude-accounts 777777777777, 888888888888, 999999999999
   ```

IAM policy examples

Policies are considered similar if they have identical:

- Affected actions across all Sid blocks.
- Details in the following IAM elements:
  - Effect (Allow/Deny)
  - Principal (who is allowed or denied access)
  - NotAction (what actions are not allowed)
  - NotPrincipal (who is explicitly denied access)
  - Resource (which AWS resources the policy applies to)
  - Condition (any specific conditions under which the policy applies)

The following examples show policies which IAM might or might not consider similar based on the differences between them.

**Example Example 1: Policies are considered similar**

Each policy type is different, but both policies contain one Sid block with the same affected Action.
Policy 1: Group inline IAM policy

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "aws-portal:ViewAccount",
            "aws-portal:*Billing"
        ],
        "Resource": "*"
    }]
}
```

Policy 2: Customer managed IAM policy

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "aws-portal:ViewAccount",
            "aws-portal:*Billing"
        ],
        "Resource": "*"
    }]
}
```

Example Example 2: Policies are considered similar

Both policies contain one Sid block with the same affected Action. Policy 2 contains additional actions, but these actions aren't affected.

Policy 1

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "aws-portal:ViewAccount",
            "aws-portal:*Billing"
        ],
        "Resource": "*"
    }]
}
```

Policy 2

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "aws-portal:ViewAccount",
            "aws-portal:*Billing",
            "athena:*"
        ],
        "Resource": "*"
    }]
}
```
Example Example 3: Policies aren't considered similar

Both policies contain one Sid block with the same affected Action. However, policy 2 contains a Condition element that isn't present in policy 1.

Policy 1

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "aws-portal:ViewAccount",
            "aws-portal:*Billing"
        ],
        "Resource": "*"
    }]
}
```

Policy 2

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "aws-portal:ViewAccount",
            "aws-portal:*Billing",
            "athena:*"
        ],
        "Resource": "*",
        "Condition": {
            "BoolIfExists": {
                "aws:MultiFactorAuthPresent": "true"
            }
        }
    }]
}
```

Example Example 4: Policies are considered similar

Policy 1 has a single Sid block with an affected Action. Policy 2 has multiple Sid blocks, but the affected Action appears in only one block.

Policy 1

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "aws-portal:View*
```
Example Example 5: Policies aren't considered similar

Policy 1 has a single Sid block with an affected Action. Policy 2 has multiple Sid blocks, and the affected Action appears in multiple blocks.

Policy 1

```
{  
  "Version": "2012-10-17",
  "Statement": [
    {  
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [  
        "aws-portal:View*
      ],
      "Resource": "*"
    },
    {  
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [  
        "cloudtrail:Get*
      ],
      "Resource": "*"
    }
  ]
}
```

Policy 2

```
{  
  "Version": "2012-10-17",
  "Statement": [
    {  
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [  
        "aws-portal:View*
      ],
      "Resource": "*"
    },
    {  
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [  
        "cloudtrail:Get*
      ],
      "Resource": "*"
    }
  ]
}
```
Example Example 6: Policies are considered similar

Both policies have multiple Sid blocks, with the same affected Action in each Sid block.

Policy 1

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
         "aws-portal:*Account",
         "iam:Get*"
      ],
      "Resource": "**"
   },
   {
      "Sid": "VisualEditor1",
      "Effect": "Deny",
      "Action": [
         "aws-portal:Modify*",
         "iam:Update*"
      ],
      "Resource": "**"
   }
   ]
}
```

Policy 2

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
         "aws-portal:*Account",
         "athena:Get*"
      ],
      "Resource": "**"
   },
   {
      "Sid": "VisualEditor1",
      "Effect": "Deny",
      "Action": [
         "aws-portal:Modify*",
         "athena:Update*"
      ],
      "Resource": "**"
   }
   ]
}
```
Example Example 7

The following two policies aren't considered similar.

Policy 1 has a single Sid block with an affected Action. Policy 2 has a Sid block with the same affected Action. However, policy 2 also contains another Sid block with different actions.

Policy 1

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "aws-portal:*Account",
            "iam:Get*"
        ],
        "Resource": "*"
    },
    {
        "Sid": "VisualEditor1",
        "Effect": "Deny",
        "Action": [
            "aws-portal:Modify*",
            "iam:Update*"
        ],
        "Resource": "*"
    }
}
```

Policy 2

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "VisualEditor0",
        "Effect": "Allow",
        "Action": [
            "aws-portal:*Account",
            "athena:Get*"
        ],
        "Resource": "*"
    },
    {
        "Sid": "VisualEditor1",
        "Effect": "Deny",
        "Action": [
            "aws-portal:*Billing",
            "athena:Update*"
        ],
        "Resource": "*"
    }
}
```

Mapping fine-grained IAM actions reference

**Note**

The following AWS Identity and Access Management (IAM) actions have reached the end of standard support on July 2023:
• `aws-portal` namespace
• `purchase-orders:ViewPurchaseOrders`
• `purchase-orders:ModifyPurchaseOrders`

If you haven't migrated the old IAM actions to the new fine-grained actions, you have until December 2023 to do so.
If you're using AWS Organizations, you can use the bulk policy migrator scripts (p. 205) to update policies from your payer account. You can also use the old to granular action mapping reference (p. 222) to verify the IAM actions that need to be added.
For more information, see the Changes to AWS Billing, AWS Cost Management, and Account Consoles Permission blog.
If you have an AWS account, or are a part of an AWS Organizations created on or after March 6, 2023, 11:00 AM (PDT), the fine-grained actions are already in effect in your organization.

You will need to migrate the following IAM actions in your permission policies or service control policies (SCP):
• `aws-portal:ViewAccount`
• `aws-portal:ViewBilling`
• `aws-portal:ViewPaymentMethods`
• `aws-portal:ViewUsage`
• `aws-portal:ModifyAccount`
• `aws-portal:ModifyBilling`
• `aws-portal:ModifyPaymentMethods`
• `purchase-orders:ViewPurchaseOrders`
• `purchase-orders:ModifyPurchaseOrders`

You can use this topic to view the mapping of the old to new fine-grained actions for each IAM action that we’re retiring.

Overview
1. Review your affected IAM policies in your AWS account. To do so, follow the steps in the Affected policies tool to identify your affected IAM policies. See How to use the affected policies tool (p. 204).
2. Use the IAM console to add the new granular permissions to your policy. For example, if your policy allows the `purchase-orders:ModifyPurchaseOrders` permission, you will need to add each action in the Mapping for `purchase-orders:ModifyPurchaseOrders` (p. 233) table.

Old policy
The following policy allows a user to add, delete, or modify any purchase order in the account.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "purchase-orders:ModifyPurchaseOrders",
      "Resource": "arn:aws:purchase-orders::123456789012:purchase-order/*"
    }
  ]
}
```
New policy

The following policy also allows a user to add, delete, or modify any purchase order in the account. Note that each granular permission appears after the old `purchase-orders:ModifyPurchaseOrders` permission. These permissions give you more control over what actions you want to allow or deny.

**Tip**

We recommend that you keep the old permissions to ensure that you don't lose permissions until this migration is complete.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "purchase-orders:ModifyPurchaseOrders",
        "purchase-orders:AddPurchaseOrder",
        "purchase-orders:DeletePurchaseOrder",
        "purchase-orders:UpdatePurchaseOrder",
        "purchase-orders:UpdatePurchaseOrderStatus"
      ],
      "Resource": "arn:aws:purchase-orders::123456789012:purchase-order/*"
    }
  ]
}
```

3. Save your changes.

**Notes**

- To edit policies manually in the IAM console, see Editing customer managed policies (console) in the IAM User Guide.
- To bulk migrate your IAM policies to use fine-grained actions (new actions), see Use scripts to bulk migrate your policies to use fine-grained IAM actions (p. 205).

**Contents**

- Mapping for aws-portal:ViewAccount (p. 225)
- Mapping for aws-portal:ViewBilling (p. 225)
- Mapping for aws-portal:ViewPaymentMethods (p. 229)
- Mapping for aws-portal:ViewUsage (p. 229)
- Mapping for aws-portal:ModifyAccount (p. 229)
- Mapping for aws-portal:ModifyBilling (p. 230)
- Mapping for aws-portal:ModifyPaymentMethods (p. 232)
- Mapping for purchase-orders:ViewPurchaseOrders (p. 232)
- Mapping for purchase-orders:ModifyPurchaseOrders (p. 233)
## Mapping for aws-portal:ViewAccount

<table>
<thead>
<tr>
<th>New action</th>
<th>Description</th>
<th>Access level</th>
</tr>
</thead>
<tbody>
<tr>
<td>account:GetAccountInformation</td>
<td>Grants permission to retrieve the account information for an account</td>
<td>Read</td>
</tr>
<tr>
<td>account:GetAlternateContact</td>
<td>Grants permission to retrieve the alternate contacts for an account</td>
<td>Read</td>
</tr>
<tr>
<td>account:GetChallengeQuestions</td>
<td>Grants permission to retrieve the challenge questions for an account</td>
<td>Read</td>
</tr>
<tr>
<td>account:GetContactInformation</td>
<td>Grants permission to retrieve the primary contact information for an account</td>
<td>Read</td>
</tr>
<tr>
<td>billing:GetContractInformation</td>
<td>Grants permission to view the account's contract information including the contract number, end-user organization names, purchase order numbers, and if the account is used to service public-sector customers</td>
<td>Read</td>
</tr>
<tr>
<td>billing:GetIAMAccessPreference</td>
<td>Grants permission to retrieve the state of the Allow IAM Access billing preference</td>
<td>Read</td>
</tr>
<tr>
<td>billing:GetSellerOfRecord</td>
<td>Grants permission to retrieve the account's default seller of record</td>
<td>Read</td>
</tr>
<tr>
<td>payments:ListPaymentPreferences</td>
<td>Grants permission to get payment preferences (for example, preferred payment currency, preferred payment method)</td>
<td>Read</td>
</tr>
</tbody>
</table>

## Mapping for aws-portal:ViewBilling

<table>
<thead>
<tr>
<th>New action</th>
<th>Description</th>
<th>Access level</th>
</tr>
</thead>
<tbody>
<tr>
<td>account:GetAccountInformation</td>
<td>Grants permission to retrieve the account information for an account</td>
<td>Read</td>
</tr>
<tr>
<td>billing:GetBillingData</td>
<td>Grants permission to perform queries on billing information</td>
<td>Read</td>
</tr>
<tr>
<td>billing:GetBillingDetails</td>
<td>Grants permission to view detailed line item billing information</td>
<td>Read</td>
</tr>
<tr>
<td>New action</td>
<td>Description</td>
<td>Access level</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>billing:GetBillingNotifications</td>
<td>Grants permission to view notifications sent by AWS related to your accounts billing information</td>
<td>Read</td>
</tr>
<tr>
<td>billing:GetBillingPreferences</td>
<td>Grants permission to view billing preferences such as Reserved Instances, Savings Plans, and credits sharing</td>
<td>Read</td>
</tr>
<tr>
<td>billing:GetContractInformation</td>
<td>Grants permission to view the account’s contract information including the contract number, end-user organization names, purchase order numbers, and if the account is used to service public-sector customers</td>
<td>Read</td>
</tr>
<tr>
<td>billing:GetCredits</td>
<td>Grants permission to view credits that have been redeemed</td>
<td>Read</td>
</tr>
<tr>
<td>billing:GetIAMAccessPreference</td>
<td>Grants permission to retrieve the state of the Allow IAM Access billing preference</td>
<td>Read</td>
</tr>
<tr>
<td>billing:GetSellerOfRecord</td>
<td>Grants permission to retrieve the account’s default seller of record</td>
<td>Read</td>
</tr>
<tr>
<td>billing:ListBillingViews</td>
<td>Grants permission to get billing information for your proforma billing groups</td>
<td>List</td>
</tr>
<tr>
<td>ce:DescribeNotificationSubscription</td>
<td>Grants permission to view reservation expiration alerts</td>
<td>Read</td>
</tr>
<tr>
<td>ce:DescribeReport</td>
<td>Grants permission to view Cost Explorer reports page</td>
<td>Read</td>
</tr>
<tr>
<td>ce:GetAnomalies</td>
<td>Grants permission to retrieve anomalies</td>
<td>Read</td>
</tr>
<tr>
<td>ce:GetAnomalyMonitors</td>
<td>Grants permission to query anomaly monitors</td>
<td>Read</td>
</tr>
<tr>
<td>ce:GetAnomalySubscriptions</td>
<td>Grants permission to query anomaly subscriptions</td>
<td>Read</td>
</tr>
<tr>
<td>ce:GetCostAndUsage</td>
<td>Grants permission to retrieve the cost and usage metrics for your account</td>
<td>Read</td>
</tr>
<tr>
<td>ce:GetCostAndUsageWithResources</td>
<td>Grants permission to retrieve the cost and usage metrics with resources for your account</td>
<td>Read</td>
</tr>
<tr>
<td>ce:GetCostCategories</td>
<td>Grants permission to query cost category names and values for a specified time period</td>
<td>Read</td>
</tr>
<tr>
<td>New action</td>
<td>Description</td>
<td>Access level</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>ce:GetCostForecast</td>
<td>Grants permission to retrieve a cost forecast for a forecast time period</td>
<td>Read</td>
</tr>
<tr>
<td>ce:GetDimensionValues</td>
<td>Grants permission to retrieve all available filter values for a filter for a period of time</td>
<td>Read</td>
</tr>
<tr>
<td>ce:GetPreferences</td>
<td>Grants permission to view the Cost Explorer preferences page</td>
<td>Read</td>
</tr>
<tr>
<td>ce:GetReservationCoverage</td>
<td>Grants permission to retrieve the reservation coverage for your account</td>
<td>Read</td>
</tr>
<tr>
<td>ce:GetReservationPurchaseRecommendation</td>
<td>Grants permission to retrieve the reservation recommendations for your account</td>
<td>Read</td>
</tr>
<tr>
<td>ce:GetReservationUtilization</td>
<td>Grants permission to retrieve the reservation utilization for your account</td>
<td>Read</td>
</tr>
<tr>
<td>ce:GetRightsizingRecommendation</td>
<td>Grants permission to retrieve the rightsizing recommendations for your account</td>
<td>Read</td>
</tr>
<tr>
<td>ce:GetSavingsPlansCoverage</td>
<td>Grants permission to retrieve the Savings Plans coverage for your account</td>
<td>Read</td>
</tr>
<tr>
<td>ce:GetSavingsPlansPurchaseRecommendation</td>
<td>Grants permission to retrieve the Savings Plans recommendations for your account</td>
<td>Read</td>
</tr>
<tr>
<td>ce:GetSavingsPlansUtilization</td>
<td>Grants permission to retrieve the Savings Plans utilization for your account</td>
<td>Read</td>
</tr>
<tr>
<td>ce:GetSavingsPlansUtilizationDetails</td>
<td>Grants permission to retrieve the Savings Plans utilization details for your account</td>
<td>Read</td>
</tr>
<tr>
<td>ce:GetTags</td>
<td>Grants permission to query tags for a specified time period</td>
<td>Read</td>
</tr>
<tr>
<td>ce:GetUsageForecast</td>
<td>Grants permission to retrieve a usage forecast for a forecast time period</td>
<td>Read</td>
</tr>
<tr>
<td>ce:ListCostAllocationTags</td>
<td>Grants permission to list cost allocation tags</td>
<td>List</td>
</tr>
<tr>
<td>ce:ListSavingsPlansPurchaseRecommendation</td>
<td>Grants permission to retrieve a list of your historical recommendation generations</td>
<td>Read</td>
</tr>
<tr>
<td>New action</td>
<td>Description</td>
<td>Access level</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>consolidatedbilling:GetAccountBillingRole</td>
<td>Grants permission to get account role (payer, linked, regular)</td>
<td>Read</td>
</tr>
<tr>
<td>consolidatedbilling:ListLinkedAccounts</td>
<td>Grants permission to get list of member and linked accounts</td>
<td>List</td>
</tr>
<tr>
<td>cur:GetClassicReport</td>
<td>Grants permission to get the CSV report for your bill</td>
<td>Read</td>
</tr>
<tr>
<td>cur:GetClassicReportPreferences</td>
<td>Grants permission to get the classic report enablement status for usage reports</td>
<td>Read</td>
</tr>
<tr>
<td>cur:ValidateReportDestination</td>
<td>Grants permission to validates if the Amazon S3 bucket exists with appropriate permissions for AWS CUR delivery</td>
<td>Read</td>
</tr>
<tr>
<td>freetier:GetFreeTierAlertPreference</td>
<td>Grants permission to get AWS Free Tier alert preference (by email address)</td>
<td>Read</td>
</tr>
<tr>
<td>freetier:GetFreeTierUsage</td>
<td>Grants permission to get AWS Free Tier usage limits and month-to-date (MTD) usage status</td>
<td>Read</td>
</tr>
<tr>
<td>invoicing:GetInvoiceEmailDeliveryPreferences</td>
<td>Grants permission to get invoice email delivery preferences</td>
<td>Read</td>
</tr>
<tr>
<td>invoicing:GetInvoicePDF</td>
<td>Grants permission to get the invoice PDF</td>
<td>Read</td>
</tr>
<tr>
<td>invoicing:ListInvoiceSummaries</td>
<td>Grants permission to get invoice summary information for your account or linked account</td>
<td>List</td>
</tr>
<tr>
<td>payments:GetPaymentInstrument</td>
<td>Grants permission to get information about a payment instrument</td>
<td>Read</td>
</tr>
<tr>
<td>payments:GetPaymentStatus</td>
<td>Grants permission to get payment status of invoices</td>
<td>Read</td>
</tr>
<tr>
<td>payments:ListPaymentPreferences</td>
<td>Grants permission to get payment preferences (for example, preferred payment currency, preferred payment method)</td>
<td>Read</td>
</tr>
<tr>
<td>tax:GetTaxInheritance</td>
<td>Grants permission to view tax inheritance status</td>
<td>Read</td>
</tr>
<tr>
<td>tax:GetTaxRegistrationDocument</td>
<td>Grants permission to download tax registration documents</td>
<td>Read</td>
</tr>
</tbody>
</table>
### Migrating access control

<table>
<thead>
<tr>
<th>New action</th>
<th>Description</th>
<th>Access level</th>
</tr>
</thead>
<tbody>
<tr>
<td>tax:ListTaxRegistrations</td>
<td>Grants permission to view tax registration</td>
<td>Read</td>
</tr>
</tbody>
</table>

### Mapping for aws-portal:ViewPaymentMethods

<table>
<thead>
<tr>
<th>New action</th>
<th>Description</th>
<th>Access level</th>
</tr>
</thead>
<tbody>
<tr>
<td>account:GetAccountInformation</td>
<td>Grants permission to retrieve the account information for an account</td>
<td>Read</td>
</tr>
<tr>
<td>invoicing:GetInvoicePDF</td>
<td>Grants permission to get the invoice PDF</td>
<td>Read</td>
</tr>
<tr>
<td>payments:GetPaymentInstrument</td>
<td>Grants permission to get information about a payment instrument</td>
<td>Read</td>
</tr>
<tr>
<td>payments:GetPaymentStatus</td>
<td>Grants permission to get payment status of invoices</td>
<td>Read</td>
</tr>
<tr>
<td>payments:ListPaymentPreferences</td>
<td>Grants permission to get payment preferences (for example, preferred payment currency, preferred payment method)</td>
<td>List</td>
</tr>
</tbody>
</table>

### Mapping for aws-portal:ViewUsage

<table>
<thead>
<tr>
<th>New action</th>
<th>Description</th>
<th>Access level</th>
</tr>
</thead>
<tbody>
<tr>
<td>cur:GetUsageReport</td>
<td>Grants permission to get a list of AWS services, the usage type and operation for the usage report workflow, and to download usage reports</td>
<td>Read</td>
</tr>
</tbody>
</table>

### Mapping for aws-portal:ModifyAccount

<table>
<thead>
<tr>
<th>New action</th>
<th>Description</th>
<th>Access level</th>
</tr>
</thead>
<tbody>
<tr>
<td>account:CloseAccount</td>
<td>Grants permission to close an account</td>
<td>Write</td>
</tr>
<tr>
<td>account:DeleteAlternateContact</td>
<td>Grants permission to delete the alternate contacts for an account</td>
<td>Write</td>
</tr>
<tr>
<td>account:PutAlternateContact</td>
<td>Grants permission to modify the alternate contacts for an account</td>
<td>Write</td>
</tr>
</tbody>
</table>
## Migrating access control

<table>
<thead>
<tr>
<th>New action</th>
<th>Description</th>
<th>Access level</th>
</tr>
</thead>
<tbody>
<tr>
<td>account:PutChallengeQuestions</td>
<td>Grants permission to modify the challenge questions for an account</td>
<td>Write</td>
</tr>
<tr>
<td>account:PutContactInformation</td>
<td>Grants permission to update the primary contact information for an account</td>
<td>Write</td>
</tr>
<tr>
<td>billing:PutContractInformation</td>
<td>Grants permission to set the account's contract information end-user organization names and if the account is used to service public-sector customers</td>
<td>Write</td>
</tr>
<tr>
<td>billing:UpdateIAMAccessPreference</td>
<td>Grants permission to update the Allow IAM Access billing preference</td>
<td>Write</td>
</tr>
<tr>
<td>payments:UpdatePaymentPreferences</td>
<td>Grants permission to update payment preferences (for example, preferred payment currency, preferred payment method)</td>
<td>Write</td>
</tr>
</tbody>
</table>

### Mapping for aws-portal:ModifyBilling

<table>
<thead>
<tr>
<th>New action</th>
<th>Description</th>
<th>Access level</th>
</tr>
</thead>
<tbody>
<tr>
<td>billing:PutContractInformation</td>
<td>Grants permission to set the account's contract information end-user organization names and if the account is used to service public-sector customers</td>
<td>Write</td>
</tr>
<tr>
<td>billing:RedeemCredits</td>
<td>Grants permission to redeem an AWS credit</td>
<td>Write</td>
</tr>
<tr>
<td>billing:UpdateBillingPreferences</td>
<td>Grants permission to update billing preferences such as Reserved Instances, Savings Plans, and credits sharing</td>
<td>Write</td>
</tr>
<tr>
<td>ce:CreateAnomalyMonitor</td>
<td>Grants permission to create a new anomaly monitor</td>
<td>Write</td>
</tr>
<tr>
<td>ce:CreateAnomalySubscription</td>
<td>Grants permission to create a new anomaly subscription</td>
<td>Write</td>
</tr>
<tr>
<td>ce:CreateNotificationSubscription</td>
<td>Grants permission to create reservation expiration alerts</td>
<td>Write</td>
</tr>
<tr>
<td>ce:CreateReport</td>
<td>Grants permission to create Cost Explorer reports</td>
<td>Write</td>
</tr>
<tr>
<td>New action</td>
<td>Description</td>
<td>Access level</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>ce:DeleteAnomalyMonitor</td>
<td>Grants permission to delete an anomaly monitor</td>
<td>Write</td>
</tr>
<tr>
<td>ce:DeleteAnomalySubscription</td>
<td>Grants permission to delete an anomaly subscription</td>
<td>Write</td>
</tr>
<tr>
<td>ce:DeleteNotificationSubscription</td>
<td>Grants permission to delete reservation expiration alerts</td>
<td>Write</td>
</tr>
<tr>
<td>ce:DeleteReport</td>
<td>Grants permission to delete Cost Explorer reports</td>
<td>Write</td>
</tr>
<tr>
<td>ce:ProvideAnomalyFeedback</td>
<td>Grants permission to provide feedback on detected anomalies</td>
<td>Write</td>
</tr>
<tr>
<td>ce:StartSavingsPlansPurchase</td>
<td>Grants permission to request a Savings Plans recommendation generation</td>
<td>Write</td>
</tr>
<tr>
<td>ce:UpdateAnomalyMonitor</td>
<td>Grants permission to update an existing anomaly monitor</td>
<td>Write</td>
</tr>
<tr>
<td>ce:UpdateAnomalySubscription</td>
<td>Grants permission to update an existing anomaly subscription</td>
<td>Write</td>
</tr>
<tr>
<td>ce:UpdateCostAllocationTags</td>
<td>Grants permission to update existing cost allocation tags status</td>
<td>Write</td>
</tr>
<tr>
<td>ce:UpdateNotificationSubscription</td>
<td>Grants permission to update reservation expiration alerts</td>
<td>Write</td>
</tr>
<tr>
<td>ce:UpdatePreferences</td>
<td>Grants permission to edit the Cost Explorer preferences page</td>
<td>Write</td>
</tr>
<tr>
<td>cur:PutClassicReportPreferences</td>
<td>Grants permission to enable classic reports</td>
<td>Write</td>
</tr>
<tr>
<td>freetier:PutFreeTierAlertPreference</td>
<td>Grants permission to set AWS Free Tier alert preference (by email address)</td>
<td>Write</td>
</tr>
<tr>
<td>invoicing:PutInvoiceEmailDeliveryPreferences</td>
<td>Grants permission to update invoice email delivery preferences</td>
<td>Write</td>
</tr>
<tr>
<td>payments:CreatePaymentInstrument</td>
<td>Grants permission to create a payment instrument</td>
<td>Write</td>
</tr>
<tr>
<td>payments:DeletePaymentInstrument</td>
<td>Grants permission to delete a payment instrument</td>
<td>Write</td>
</tr>
<tr>
<td>payments:MakePayment</td>
<td>Grants permission to make a payment, authenticate a payment, verify a payment method, and generate a funding request document for Advance Pay</td>
<td>Write</td>
</tr>
</tbody>
</table>
### New action

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>Access level</th>
</tr>
</thead>
<tbody>
<tr>
<td>payments:UpdatePaymentPreferences</td>
<td>Grants permission to update payment preferences (for example, preferred payment currency, preferred payment method)</td>
<td>Write</td>
</tr>
<tr>
<td>tax:BatchPutTaxRegistration</td>
<td>Grants permission to batch update tax registrations</td>
<td>Write</td>
</tr>
<tr>
<td>tax:DeleteTaxRegistration</td>
<td>Grants permission to delete tax registration data</td>
<td>Write</td>
</tr>
<tr>
<td>tax:PutTaxInheritance</td>
<td>Grants permission to set tax inheritance</td>
<td>Write</td>
</tr>
</tbody>
</table>

#### Mapping for aws-portal:ModifyPaymentMethods

<table>
<thead>
<tr>
<th>New action</th>
<th>Description</th>
<th>Access level</th>
</tr>
</thead>
<tbody>
<tr>
<td>account:GetAccountInformation</td>
<td>Grants permission to retrieve the account information for an account</td>
<td>Read</td>
</tr>
<tr>
<td>payments:DeletePaymentInstrument</td>
<td>Grants permission to delete a payment instrument</td>
<td>Write</td>
</tr>
<tr>
<td>payments:CreatePaymentInstrument</td>
<td>Grants permission to create a payment instrument</td>
<td>Write</td>
</tr>
<tr>
<td>payments:MakePayment</td>
<td>Grants permission to make a payment, authenticate a payment, verify a payment method, and generate a funding request document for Advance Pay</td>
<td>Write</td>
</tr>
<tr>
<td>payments:UpdatePaymentPreferences</td>
<td>Grants permission to update payment preferences (for example, preferred payment currency, preferred payment method)</td>
<td>Write</td>
</tr>
</tbody>
</table>

#### Mapping for purchase-orders:ViewPurchaseOrders

<table>
<thead>
<tr>
<th>New action</th>
<th>Description</th>
<th>Access level</th>
</tr>
</thead>
<tbody>
<tr>
<td>invoicing:GetInvoicePDF</td>
<td>Grants permission to get invoice PDF</td>
<td>Get</td>
</tr>
<tr>
<td>payments:ListPaymentPreferences</td>
<td>Grants permission to get payment preferences (for example, preferred payment method)</td>
<td>List</td>
</tr>
</tbody>
</table>
# AWS Billing User Guide

## Logging and monitoring

### New action

<table>
<thead>
<tr>
<th>Description</th>
<th>Access level</th>
</tr>
</thead>
<tbody>
<tr>
<td>currency, preferred payment method)</td>
<td></td>
</tr>
<tr>
<td>purchase-orders:GetPurchaseOrder Grants permission to get a purchase order</td>
<td>Read</td>
</tr>
<tr>
<td>purchase-orders:ListPurchaseOrderInvoices Grants permission to view purchase orders and details</td>
<td>List</td>
</tr>
<tr>
<td>purchase-orders:ListPurchaseOrders Grants permission to get all available purchase orders</td>
<td>List</td>
</tr>
</tbody>
</table>

### Mapping for purchase-orders:ModifyPurchaseOrders

<table>
<thead>
<tr>
<th>Description</th>
<th>Access level</th>
</tr>
</thead>
<tbody>
<tr>
<td>purchase-orders:AddPurchaseOrder Grants permission to add a purchase order</td>
<td>Write</td>
</tr>
<tr>
<td>purchase-orders:DeletePurchaseOrder Grants permission to delete a purchase order</td>
<td>Write</td>
</tr>
<tr>
<td>purchase-orders:UpdatePurchaseOrder Grants permission to update an existing purchase order</td>
<td>Write</td>
</tr>
<tr>
<td>purchase-orders:UpdatePurchaseOrderStatus Grants permission to set purchase order status</td>
<td>Write</td>
</tr>
</tbody>
</table>

## Logging and monitoring in AWS Billing and Cost Management

Monitoring is an important part of maintaining the reliability, availability, and performance of your AWS account. There are several tools available to monitor your Billing and Cost Management usage.

### AWS Cost and Usage Reports

AWS Cost and Usage Reports tracks your AWS usage and provides estimated charges associated with your account. Each report contains line items for each unique combination of AWS products, usage type, and operation that you use in your AWS account. You can customize the AWS Cost and Usage Reports to aggregate the information either by the hour or by the day.

For more information about AWS Cost and Usage Reports, see the [Cost and Usage Report Guide](#).

### AWS CloudTrail

Billing and Cost Management is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Billing and Cost Management. CloudTrail captures all write and modify API calls for Billing and Cost Management as events, including calls from the Billing and Cost Management console and from code calls to the Billing and Cost Management APIs.

For more information about AWS CloudTrail, see the [Logging Billing and Cost Management API calls with AWS CloudTrail](#).
Logging Billing and Cost Management API calls with AWS CloudTrail

Billing and Cost Management is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Billing and Cost Management. CloudTrail captures API calls for Billing and Cost Management as events, including calls from the Billing and Cost Management console and from code calls to the Billing and Cost Management APIs. For a full list of CloudTrail events related to Billing, see Billing CloudTrail events (p. 234).

If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Billing and Cost Management. 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 Billing and Cost Management, 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, including how to configure and enable it, see the AWS CloudTrail User Guide.

Billing CloudTrail events

This section shows a full list of the CloudTrail events related to Billing and Cost Management.

Notes

The following CloudTrail events use a different event source instead of billingconsole.amazonaws.com:

- CreateCustomerCase, GetTaxExemptionTypes, and BatchGetTaxExemptions use taxconsole.amazonaws.com.
- CreateCustomerVerificationDetails, GetCustomerVerificationDetails, GetCustomerVerificationEligibility, and UpdateCustomerVerificationDetails use customer-verification.amazonaws.com.

<table>
<thead>
<tr>
<th>Event name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AddPurchaseOrder</td>
<td>Logs the creation of a purchase order.</td>
</tr>
<tr>
<td>AcceptFxPaymentCurrencyTermsAndConditions</td>
<td>Logs the acceptance of the terms and conditions of paying in a currency other than USD.</td>
</tr>
<tr>
<td>BatchGetTaxExemptions</td>
<td>Logs the access to US tax exemptions of an account, and any linked accounts.</td>
</tr>
<tr>
<td>CloseAccount</td>
<td>Logs the closing of an account.</td>
</tr>
<tr>
<td>CreateCustomerCase</td>
<td>Logs the creation of a customer support case to validate US tax exemption for an account.</td>
</tr>
<tr>
<td>CreateCustomerVerificationDetails</td>
<td>Logs the creation of the customer verification details of the account.</td>
</tr>
<tr>
<td>CreateOrigamiReportPreference</td>
<td>Logs the creation of the cost and usage report; management account only.</td>
</tr>
</tbody>
</table>

Version 2.0
234
<table>
<thead>
<tr>
<th>Event name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeletePurchaseOrder</td>
<td>Logs the deletion of a purchase order.</td>
</tr>
<tr>
<td>DeleteOrigamiReportPreferences</td>
<td>Logs the deletion of the cost and usage report; management account only.</td>
</tr>
<tr>
<td>DownloadCommercialInvoice</td>
<td>Logs the download of a commercial invoice.</td>
</tr>
<tr>
<td>DownloadECSVForBillingPeriod</td>
<td>Logs the download of the eCSV file (monthly usage report) for a specific billing period.</td>
</tr>
<tr>
<td>DownloadRegistrationDocument</td>
<td>Logs the download of the tax registration document.</td>
</tr>
<tr>
<td>DownloadTaxInvoice</td>
<td>Logs the download of a tax invoice.</td>
</tr>
<tr>
<td>EnableBillingAlerts</td>
<td>Logs the opt-in of receiving CloudWatch billing alerts for estimated charges.</td>
</tr>
<tr>
<td>FindECSVForBillingPeriod</td>
<td>Logs the retrieval of the ECSV file for a specific billing period.</td>
</tr>
<tr>
<td>GetAccountEDPStatus</td>
<td>Logs the retrieval of the account's EDP status.</td>
</tr>
<tr>
<td>GetAddresses</td>
<td>Logs the access to tax address, billing address, and contact address of an account.</td>
</tr>
<tr>
<td>GetAllAccounts</td>
<td>Logs the access to all member account numbers of the management account.</td>
</tr>
<tr>
<td>GetAllAccountDetails</td>
<td>Logs the access to tax registration details of all member accounts of the management account.</td>
</tr>
<tr>
<td>GetBillsForBillingPeriod</td>
<td>Logs the access of the account's usage and charges for a specific billing period.</td>
</tr>
<tr>
<td>GetBillsForLinkedAccount</td>
<td>Logs the access of a management account retrieving the usage and charges of one of the member accounts in the consolidated billing family for a specific billing period.</td>
</tr>
<tr>
<td>GetCommercialInvoices</td>
<td>Logs the account's commercial invoices metadata for the specific billing period.</td>
</tr>
<tr>
<td>GetConsolidatedBillingFamilySummary</td>
<td>Logs the management account retrieving the summary of the entire consolidated billing family.</td>
</tr>
<tr>
<td>GetCustomerVerificationEligibility</td>
<td>(For customers with an India billing or contact address only) Logs the retrieval of the customer verification eligibility of the account.</td>
</tr>
<tr>
<td>GetCustomerVerificationDetails</td>
<td>(For customers with an India billing or contact address only) Logs the retrieval of the customer verification details of the account.</td>
</tr>
<tr>
<td>GetLinkedAccountNames</td>
<td>Logs the retrieval from a management account of the member account names belonging to its consolidated billing family for a specific billing period.</td>
</tr>
<tr>
<td>GetPurchaseOrder</td>
<td>Logs the retrieval of a purchase order.</td>
</tr>
<tr>
<td>GetSupportedCountryCodes</td>
<td>Logs the access to all country codes supported by tax console.</td>
</tr>
<tr>
<td>GetTaxExemptionTypes</td>
<td>Logs the access to all supported US exemption types by tax console.</td>
</tr>
<tr>
<td>Event name</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>GetTaxInheritance</td>
<td>Logs the access to tax inheritance preference (turning on or off) of an account.</td>
</tr>
<tr>
<td>GetTaxInvoicesMetadata</td>
<td>Logs the retrieval of tax invoices metadata.</td>
</tr>
<tr>
<td>GetTaxRegistration</td>
<td>Logs the access to the tax registration number of an account.</td>
</tr>
<tr>
<td>GetTotal</td>
<td>Logs the retrieval of the account's total charges.</td>
</tr>
<tr>
<td>GetTotalAmountForForecast</td>
<td>Logs the access to the forecasted charges for the specific billing period.</td>
</tr>
<tr>
<td>ListCostAllocationTags</td>
<td>Logs the retrieval and listing of cost allocation tags.</td>
</tr>
<tr>
<td>ListPurchaseOrders</td>
<td>Logs the retrieval and listing of purchase orders.</td>
</tr>
<tr>
<td>ListPurchaseOrderInvoices</td>
<td>Logs of the retrieval and list of invoices associated to a purchase order.</td>
</tr>
<tr>
<td>ListTagsForResource</td>
<td>Lists the tags associated with a resource for a purchase order.</td>
</tr>
<tr>
<td>PreviewTaxRegistrationChange</td>
<td>Logs the preview of tax registration changes before confirmation.</td>
</tr>
<tr>
<td>RedeemPromoCode</td>
<td>Logs the redemption of promotional credits for an account.</td>
</tr>
<tr>
<td>SetAccountContractMetadata</td>
<td>Logs the creation, deletion, or update of the necessary contract information for public sector customers.</td>
</tr>
<tr>
<td>SetAccountPreferences</td>
<td>Logs the updates of the account name, email, and password.</td>
</tr>
<tr>
<td>SetAdditionalContacts</td>
<td>Logs the creation, deletion, or update of the alternate contacts for billing, operations, and security communications.</td>
</tr>
<tr>
<td>SetContactAddress</td>
<td>Logs the creation, deletion, or update of the account owner contact information, including the address and phone number.</td>
</tr>
<tr>
<td>SetCreatedByOptIn</td>
<td>Logs the opt-in of the awscreatedby cost allocation tag preference.</td>
</tr>
<tr>
<td>SetCreditSharing</td>
<td>Logs the history of the credit sharing preference for the management account.</td>
</tr>
<tr>
<td>SetFreetierBudgetsPreference</td>
<td>Logs the preference (opt-in or opt-out) of receiving Free Tier usage alerts.</td>
</tr>
<tr>
<td>SetFxPaymentCurrency</td>
<td>Logs the creation, deletion, or update of the preferred currency used to pay your invoice.</td>
</tr>
<tr>
<td>SetIAMAccessPreference</td>
<td>Logs the creation, deletion, or update of the IAM users ability to access to the billing console. This setting is only for customers with root access.</td>
</tr>
<tr>
<td>SetPANInformation</td>
<td>Logs the creating, deletion, or update of PAN information under AWS India.</td>
</tr>
<tr>
<td>SetPayInformation</td>
<td>Logs the payment method history (invoice or credit/debit card) for the account.</td>
</tr>
<tr>
<td>SetRISharing</td>
<td>Logs the history of the RI/Savings Plans sharing preference for the management account.</td>
</tr>
<tr>
<td>SetSecurityQuestions</td>
<td>Logs the creation, deletion, or update of the security challenge questions to help AWS identify you as the owner of the account.</td>
</tr>
<tr>
<td>SetTagKeysState</td>
<td>Logs the active or inactive state of a particular cost allocation tag.</td>
</tr>
</tbody>
</table>
# Billing and Cost Management information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When supported event activity occurs in Billing and Cost Management, 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 in the AWS CloudTrail User Guide.

For an ongoing record of events in your AWS account, including events for Billing and Cost Management, 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 AWS 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 the following:

- 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

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 in the AWS CloudTrail User Guide.
CloudTrail log entry examples

The following examples are provided for specific Billing and Cost Management CloudTrail log entry scenarios.

Topics
- Billing and Cost Management log file entries (p. 238)
- Tax console (p. 238)

Billing and Cost Management 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 don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the SetContactAddress action.

```json
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "111122223333",
        "accessKeyId": "AIDACKCEVSQ6C2EXAMPLE"
    },
    "eventTime": "2018-05-30T16:44:04Z",
    "eventSource": "billingconsole.amazonaws.com",
    "eventName": "SetContactAddress",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "100.100.10.10",
    "requestParameters": {
        "website": "https://amazon.com",
        "city": "Seattle",
        "postalCode": "98108",
        "fullName": "Jane Doe",
        "districtOrCounty": null,
        "phoneNumber": "206-555-0100",
        "countryCode": "US",
        "addressLine1": "Nowhere Estates",
        "addressLine2": "100 Main Street",
        "addressLine3": "Anytown, USA",
        "state": "Washington",
        "company": "AnyCompany",
        "secondaryPhone": "206-555-0101"
    },
    "responseElements": null,
    "eventID": "5923c499-063e-44ac-80fb-b40example9f",
    "readOnly": false,
    "eventType": "AwsConsoleAction",
    "recipientAccountId": "1111-2222-3333"
}
```

Tax console

The following example shows a CloudTrail log entry that uses the CreateCustomerCase action.

```json
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "111122223333",
        "accessKeyId": "AIDACKCEVSQ6C2EXAMPLE"
    },
    "eventTime": "2018-05-30T16:44:04Z",
    "eventSource": "billingconsole.amazonaws.com",
    "eventName": "CreateCustomerCase",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "100.100.10.10",
    "requestParameters": {
        "productName": "AWS Support"
    },
    "responseElements": null,
    "eventID": "5923c499-063e-44ac-80fb-b40example9f",
    "readOnly": false,
    "eventType": "AwsConsoleAction",
    "recipientAccountId": "1111-2222-3333"
}
```
Compliance validation for AWS Billing and Cost Management

Third-party auditors assess the security and compliance of AWS services as part of multiple AWS compliance programs. Billing and Cost Management is not in scope of any AWS compliance programs.

For a list of AWS services in scope of specific compliance programs, see [AWS Services in Scope by Compliance Program](#). For general information, see [AWS Compliance Programs](#).

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

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

- **Security and Compliance Quick Start Guides** – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- **AWS Compliance Resources** – This collection of workbooks and guides might apply to your industry and location.
- **Evaluating Resources with Rules** in the [AWS Config Developer Guide](#) – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- **AWS Security Hub** – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

Resilience in AWS Billing and Cost Management

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency,
high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

Infrastructure security in AWS Billing and Cost Management

As a managed service, AWS Billing and Cost Management is protected by AWS global network security. For information about AWS security services and how AWS protects infrastructure, see AWS Cloud Security. To design your AWS environment using the best practices for infrastructure security, see Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

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

- Transport Layer Security (TLS). We require TLS 1.2 and recommend TLS 1.3.
- Cipher suites with perfect forward secrecy (PFS) such as DHE (Ephemeral Diffie-Hellman) or ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.
Quotas and restrictions

You can use the following tables to find the current quotas, restrictions, and naming constraints within the AWS Billing console.

Notes

- To learn more about quotas and restrictions for AWS Cost Management, see Quotas and restrictions in the AWS Cost Management User Guide.
- For more information about other AWS service quotas, see AWS service quotas in the AWS General Reference.

Topics

- Cost categories (p. 241)
- Purchase orders (p. 241)
- Advance Pay (p. 242)
- Cost allocation tags (p. 242)
- AWS Price List (p. 242)

Cost categories

<table>
<thead>
<tr>
<th>Description</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>The total number of cost categories for a management account</td>
<td>50</td>
</tr>
<tr>
<td>The number of cost category rules for a cost category (API)</td>
<td>500</td>
</tr>
<tr>
<td>The number of cost category rules for a cost category (UI)</td>
<td>100</td>
</tr>
<tr>
<td>Cost category names</td>
<td></td>
</tr>
<tr>
<td>• Names must be unique</td>
<td></td>
</tr>
<tr>
<td>• Case sensitive</td>
<td></td>
</tr>
<tr>
<td>Cost category value names</td>
<td>Names don't have to be unique</td>
</tr>
<tr>
<td>The type and number of characters allowed in a cost category name and value name</td>
<td></td>
</tr>
<tr>
<td>• Numbers: 0–9</td>
<td></td>
</tr>
<tr>
<td>• Unicode letters</td>
<td></td>
</tr>
<tr>
<td>• Space, if it's not used at the beginning or end of the name</td>
<td></td>
</tr>
<tr>
<td>• The following symbols: underscore (_) or endash (-)</td>
<td></td>
</tr>
<tr>
<td>The number of split charge rules for a cost category</td>
<td>10</td>
</tr>
</tbody>
</table>

Purchase orders

<table>
<thead>
<tr>
<th>Description</th>
<th>Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>The type of characters that you can use in a purchase order ID</td>
<td>A–Z and a–z</td>
</tr>
</tbody>
</table>
The number of characters allowed in a purchase order ID: 100

The number of contacts allowed for a purchase order: 20

The number of tags allowed for a purchase order: 50

The number of line items allowed for a purchase order: 100

**Advance Pay**

<table>
<thead>
<tr>
<th>User entity</th>
<th>AWS Inc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currency</td>
<td>USD</td>
</tr>
</tbody>
</table>

**Fund usage after funds are added to your Advance Pay**

- Funds can only be used to pay for eligible AWS charges. Non-eligible charges (for example, AWS Marketplace invoices) are charged using the default payment method at the time of Advance Pay registration.
- Funds can't be withdrawn, refunded, or transferred.
- Funds can't be converted to other currencies.

**If there are unused funds in your Advance Pay**

- You can't change your seller on record.
- You can't change your preferred currency.
- You can't change your default payment method.

**Cost allocation tags**

You can adjust the maximum number of active cost allocation tag keys from Service Quotas. For more information, see [Requesting a quota increase](#) in the *Service Quotas User Guide*.

<table>
<thead>
<tr>
<th>The maximum number of active cost allocation tag keys for each payer account</th>
<th>500</th>
</tr>
</thead>
<tbody>
<tr>
<td>The number of cost allocation tag that can be activated or deactivated for one request, by using the API or the console.</td>
<td>20</td>
</tr>
</tbody>
</table>

**AWS Price List**

For the AWS Price List Query API, see [Quotas](#).

For the AWS Price List Bulk API, see [Quotas](#).
The following table describes the documentation for this release of the *AWS Billing User Guide*.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updates for Amazon Web Services India Private Limited customer verification</td>
<td>AWS India customers can verify their identity information when signing up for an AWS account.</td>
<td>October 27, 2023</td>
</tr>
<tr>
<td>Updated documentation</td>
<td>You can use the Billing preferences page to activate or deactivate credit sharing, and discount sharing for Reserved Instances and Savings Plans for member accounts in AWS Organizations.</td>
<td>October 19, 2023</td>
</tr>
<tr>
<td>Updated documentation for AWS Price List</td>
<td>Updated documentation, including example AWS CLI commands, definitions, and notifications for the AWS Price List Bulk API and AWS Price List Query API.</td>
<td>October 3, 2023</td>
</tr>
<tr>
<td>Updates to payment methods</td>
<td>For AWS accounts in AWS Europe, you can link and verify your bank account in the Billing console.</td>
<td>September 15, 2023</td>
</tr>
<tr>
<td>Updated documentation</td>
<td>To ensure that your invoices are issued correctly, you can use the monthly billing checklist topic to review your billing information.</td>
<td>September 1, 2023</td>
</tr>
<tr>
<td>Update for cost allocation tags</td>
<td>You can use the Last updated date and Last used month fields to learn when your cost allocation tags were last updated or used.</td>
<td>August 23, 2023</td>
</tr>
<tr>
<td>Update for the AWS Price List Query API</td>
<td>Added endpoint for the Europe (Frankfurt) Region.</td>
<td>August 15, 2023</td>
</tr>
<tr>
<td>Updated AWS managed policies</td>
<td>Billing and AWSBillingReadOnlyAccess – Updated existing policies to add permissions for cost allocation tags.</td>
<td>July 26, 2023</td>
</tr>
<tr>
<td>Updates to the payments documentation</td>
<td>You can use the table on the Payments page to view credit memos that were partially applied.</td>
<td>July 25, 2023</td>
</tr>
<tr>
<td>Update Description</td>
<td>Date</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------------------------------------------</td>
<td>--------------------------</td>
<td></td>
</tr>
<tr>
<td>Updated documentation for AWS managed policies</td>
<td>Updated documentation for AWS managed policies – Updated existing policies to add permissions for purchase order tags.</td>
<td>July 11, 2023</td>
</tr>
<tr>
<td>Updated reference documentation for IAM fine-grained actions</td>
<td>Added documentation so that you can see how the old IAM actions map to the new fine-grained IAM actions.</td>
<td>June 28, 2023</td>
</tr>
<tr>
<td>Updated documentation for the Account page</td>
<td>Updated documentation for the AWS Billing console.</td>
<td>June 22, 2023</td>
</tr>
<tr>
<td>Updated documentation (p. 243)</td>
<td>Added tag support for purchase orders</td>
<td>June 19, 2023</td>
</tr>
<tr>
<td>Use scripts to bulk migrate to IAM fine-grained actions</td>
<td>Added documentation so that you can bulk migrate your policies to the new IAM fine-grained actions.</td>
<td>June 8, 2023</td>
</tr>
<tr>
<td>Updates to payment methods</td>
<td>Added a new feature to manage PIX payment methods in Brazil.</td>
<td>June 6, 2023</td>
</tr>
<tr>
<td>Consolidated billing for AWS EMEA</td>
<td>Added the consolidated billing feature for accounts that are invoiced through the Amazon Web Services EMEA SARL (AWS Europe) entity.</td>
<td>June 6, 2023</td>
</tr>
<tr>
<td>Added support for shorter PDF invoices</td>
<td>Added documentation for how to request shorter PDF invoices.</td>
<td>May 30, 2023</td>
</tr>
<tr>
<td>Added new cost category dimension</td>
<td>Added the Usage Type dimension for AWS Billing.</td>
<td>May 16, 2023</td>
</tr>
<tr>
<td>New and updated managed policies</td>
<td>AWSPurchaseOrdersServiceRolePolicy, Billing, and AWSBillingReadOnlyAccess – Updated existing policies. AWSAccountActivityAccess – New AWS managed policy documented for AWS Billing</td>
<td>March 6, 2023</td>
</tr>
</tbody>
</table>

Version 2.0
244
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>New customer carbon footprint tool</td>
<td>Added a new customer carbon footprint tool feature to view estimates of the carbon emissions associated with your AWS products and services.</td>
<td>February 28, 2022</td>
</tr>
<tr>
<td>New payment profiles</td>
<td>Added a new payment profiles feature to assign automatic payment methods to invoices.</td>
<td>February 17, 2022</td>
</tr>
<tr>
<td>AWSPurchaseOrdersServiceRolePolicy – Update to an existing policy</td>
<td>AWS Billing removed unnecessary permissions.</td>
<td>November 18, 2021</td>
</tr>
<tr>
<td>AWS Billing started tracking changes for AWS managed policies</td>
<td>AWS Billing started tracking changes for its AWS managed policies.</td>
<td>November 18, 2021</td>
</tr>
<tr>
<td>New AWS Cost Management guide</td>
<td>Split the Billing and Cost Management user guide and aligned the feature details into the Billing guide and AWS Cost Management guide to align with the console.</td>
<td>October 20, 2021</td>
</tr>
<tr>
<td>New AWS Cost Anomaly Detection</td>
<td>Added a new AWS Cost Anomaly Detection feature that uses machine learning to continuously monitor your cost and usage to detect unusual spends.</td>
<td>December 16, 2020</td>
</tr>
<tr>
<td>New Purchase Order Management</td>
<td>Added a new purchase order feature to configure how your purchases are reflected on your invoices.</td>
<td>October 15, 2020</td>
</tr>
<tr>
<td>New Budgets Actions</td>
<td>Added a new AWS Budgets actions feature to run an action on your behalf when a budget exceeds a certain cost or usage threshold.</td>
<td>October 15, 2020</td>
</tr>
<tr>
<td>New AWS Cost Categories</td>
<td>Added a new AWS Cost Categories feature to map AWS costs into meaningful categories.</td>
<td>April 20, 2020</td>
</tr>
<tr>
<td>New Heritage Tax feature</td>
<td>Added a new feature that enables you to use your tax registration information with your linked accounts.</td>
<td>March 19, 2020</td>
</tr>
<tr>
<td>New china bank redirect payment method</td>
<td>Added a new payment method that allows China CNY customers using AWS to pay their overdue payments using China Bank Redirect.</td>
<td>February 20, 2020</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>New security chapter</td>
<td>Added a new security chapter that provides information about various security controls. Former &quot;Controlling Access&quot; chapter contents have been migrated here.</td>
<td>February 6, 2020</td>
</tr>
<tr>
<td>New AWS Cost and Usage Reports user guide</td>
<td>Migrated and reorganized all AWS Cost and Usage Reports content to a separate user guide.</td>
<td>January 21, 2020</td>
</tr>
<tr>
<td>New reporting method using AWS Budgets</td>
<td>Added a new reporting functionality using AWS Budgets reports.</td>
<td>June 27, 2019</td>
</tr>
<tr>
<td>Added normalized units to Cost Explorer</td>
<td>Cost Explorer reports now include normalized units.</td>
<td>February 5, 2019</td>
</tr>
<tr>
<td>Credit application changes</td>
<td>AWS changed how they apply credits.</td>
<td>January 17, 2019</td>
</tr>
<tr>
<td>New payment behavior</td>
<td>AWS India customers can now enable the auto-charge ability for their payments.</td>
<td>December 20, 2018</td>
</tr>
<tr>
<td>New AWS Price List Service endpoint</td>
<td>Added a new endpoint for AWS Price List Service.</td>
<td>December 17, 2018</td>
</tr>
<tr>
<td>Updated the Cost Explorer UI</td>
<td>Updated the Cost Explorer UI.</td>
<td>November 15, 2018</td>
</tr>
<tr>
<td>Integrated Amazon Athena into AWS Cost and Usage Reports</td>
<td>Added the ability to upload the data from an AWS Cost and Usage Reports into Athena.</td>
<td>November 15, 2018</td>
</tr>
<tr>
<td>Added Budgets history</td>
<td>Added the ability to see the history of a budget.</td>
<td>November 13, 2018</td>
</tr>
<tr>
<td>Expanded budget services</td>
<td>Expanded RI budgets to Amazon OpenSearch Service.</td>
<td>November 8, 2018</td>
</tr>
<tr>
<td>Added a new payment method</td>
<td>Added the SEPA Direct Debit payment method.</td>
<td>October 25, 2018</td>
</tr>
<tr>
<td>Added On-Demand capacity reservations (p. 243)</td>
<td>Added documentation about AWS Cost and Usage Reports line items that apply to capacity reservations.</td>
<td>October 25, 2018</td>
</tr>
<tr>
<td>Redesigned AWS Budgets experience</td>
<td>Updated the AWS Budgets UI and workflow.</td>
<td>October 23, 2018</td>
</tr>
<tr>
<td>New Reserved Instance recommendation columns</td>
<td>Added new columns to the Cost Explorer RI recommendations.</td>
<td>October 18, 2018</td>
</tr>
<tr>
<td>New AWS CloudTrail actions</td>
<td>More actions added to CloudTrail logging.</td>
<td>October 18, 2018</td>
</tr>
<tr>
<td>Added a new Reserved Instance report</td>
<td>Expanded RI reports to Amazon OpenSearch Service.</td>
<td>October 10, 2018</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>New AWS Cost and Usage Reports columns (p. 243)</td>
<td>New columns added to the AWS Cost and Usage Reports.</td>
<td>September 27, 2018</td>
</tr>
<tr>
<td>Cost Explorer walkthrough</td>
<td>Cost Explorer now provides a walkthrough for the most common functionality.</td>
<td>September 24, 2018</td>
</tr>
<tr>
<td>Added CloudTrail events</td>
<td>Added additional CloudTrail events.</td>
<td>August 13, 2018</td>
</tr>
<tr>
<td>Added a new payment method</td>
<td>Added the ACH Direct Debit payment method.</td>
<td>July 24, 2018</td>
</tr>
<tr>
<td>Updated the AWS free tier widget</td>
<td>Updated the AWS Free Tier Widget.</td>
<td>July 19, 2018</td>
</tr>
<tr>
<td>Added RI purchase recommendations for additional services</td>
<td>Added RI purchase recommendations for additional services in Cost Explorer.</td>
<td>July 11, 2018</td>
</tr>
<tr>
<td>Added RI purchase recommendations for linked accounts</td>
<td>Added RI purchase recommendations for linked accounts in Cost Explorer.</td>
<td>June 27, 2018</td>
</tr>
<tr>
<td>Added support for AWS Cost and Usage Reports data refreshes</td>
<td>AWS Cost and Usage Reports can now update after finalization if AWS applies refunds, credits, or support fees to an account.</td>
<td>June 20, 2018</td>
</tr>
<tr>
<td>Added CloudTrail support</td>
<td>Added support for CloudTrail event logging.</td>
<td>June 7, 2018</td>
</tr>
<tr>
<td>Added AWS CloudFormation for Budgets</td>
<td>Added Budgets templates for AWS CloudFormation.</td>
<td>May 22, 2018</td>
</tr>
<tr>
<td>Updated RI allocation behavior for linked accounts</td>
<td>Updated the RI allocation behavior size-flexible RI for linked accounts.</td>
<td>May 9, 2018</td>
</tr>
<tr>
<td>RI coverage alerts</td>
<td>Added RI coverage alerts.</td>
<td>May 8, 2018</td>
</tr>
<tr>
<td>Unblend linked account bills (p. 243)</td>
<td>Linked account bills no longer show the blended rate for the organization.</td>
<td>May 7, 2018</td>
</tr>
<tr>
<td>Updated AWS tax settings</td>
<td>Added the ability to bulk edit tax settings.</td>
<td>April 25, 2018</td>
</tr>
<tr>
<td>Added Amazon RDS recommendations to Cost Explorer</td>
<td>Added Amazon RDS Recommendations to Cost Explorer.</td>
<td>April 19, 2018</td>
</tr>
<tr>
<td>Added a new Cost Explorer dimension and AWS Cost and Usage Reports line item (p. 243)</td>
<td>Added a new Cost Explorer dimension and AWS Cost and Usage Reports line item.</td>
<td>March 27, 2018</td>
</tr>
<tr>
<td>Added purchase recommendations to the Cost Explorer API</td>
<td>Added access to the Amazon EC2 Reserved Instance (RI) purchase recommendations via the Cost Explorer API.</td>
<td>March 20, 2018</td>
</tr>
<tr>
<td>Added RI coverage for Amazon RDS, Amazon Redshift, and ElastiCache</td>
<td>Reserved Instance (RI) coverage for Amazon RDS, Amazon Redshift, and ElastiCache.</td>
<td>March 13, 2018</td>
</tr>
<tr>
<td>Added RI coverage to the Cost Explorer API</td>
<td>Added GetReservationCoverage to the Cost Explorer API.</td>
<td>February 22, 2018</td>
</tr>
<tr>
<td>Added AWS free tier alerts</td>
<td>Added AWS Free Tier alerts that enable you stay under the free tier limits.</td>
<td>December 13, 2017</td>
</tr>
<tr>
<td>RI recommendations</td>
<td>Added RI recommendations based on previous usage.</td>
<td>November 20, 2017</td>
</tr>
<tr>
<td>Cost Explorer API</td>
<td>Activated API access Cost Explorer.</td>
<td>November 20, 2017</td>
</tr>
<tr>
<td>RI utilization alerts for additional services</td>
<td>Added notifications for additional services.</td>
<td>November 10, 2017</td>
</tr>
<tr>
<td>Added RI reports</td>
<td>Expanded RI reports to Amazon RDS, Redshift, and ElastiCache.</td>
<td>November 10, 2017</td>
</tr>
<tr>
<td>Discount sharing preferences</td>
<td>Updated preferences so that AWS credits and RI discount sharing can be turned off.</td>
<td>November 6, 2017</td>
</tr>
<tr>
<td>New Amazon S3 console (p. 243)</td>
<td>Updated for the new Amazon S3 console.</td>
<td>September 15, 2017</td>
</tr>
<tr>
<td>RI utilization alerts</td>
<td>Added notifications for when RI utilization drops below a preset percentage-based threshold.</td>
<td>August 21, 2017</td>
</tr>
<tr>
<td>Updated Cost Explorer UI</td>
<td>Released a new Cost Explorer UI.</td>
<td>August 16, 2017</td>
</tr>
<tr>
<td>AWS Marketplace data integration (p. 243)</td>
<td>Added AWS Marketplace so that customers can see their data reflected in all billing artifacts, including the Bills page, Cost Explorer, and more.</td>
<td>August 10, 2017</td>
</tr>
<tr>
<td>Consolidated billing with organizations</td>
<td>Updated the consolidated billing with organizations behavior.</td>
<td>June 20, 2017</td>
</tr>
<tr>
<td>Linked account access and usage type groups in AWS Budgets</td>
<td>Added support for creating cost and usage budgets based on specific usage types and usage type groups, and extended budget creation capabilities to all account types.</td>
<td>June 19, 2017</td>
</tr>
<tr>
<td>Regional offer files</td>
<td>The AWS Price List API now offers regional offer files for each service.</td>
<td>April 20, 2017</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Added Cost Explorer advanced options</td>
<td>You can now filter Cost Explorer reports by additional advanced options, such as refunds, credits, RI upfront fees, RI recurring charges, and support charges.</td>
<td>March 22, 2017</td>
</tr>
<tr>
<td>Added a Cost Explorer report</td>
<td>You can now track your Reserved Instance (RI) coverage in Cost Explorer.</td>
<td>March 20, 2017</td>
</tr>
<tr>
<td>Added Cost Explorer filters</td>
<td>You can now filter Cost Explorer reports by tenancy, platform, and the Amazon EC2 Spot and Scheduled Reserved Instance purchase options.</td>
<td>March 20, 2017</td>
</tr>
<tr>
<td>Cost Explorer and Budgets for AWS India</td>
<td>AWS India users can now use Cost Explorer and Budgets.</td>
<td>March 6, 2017</td>
</tr>
<tr>
<td>Added grouping for Cost Explorer usage types</td>
<td>Cost Explorer supports grouping for both cost and usage data, enabling customers to identify their cost drivers by cross-referencing their cost and usage charts.</td>
<td>February 24, 2017</td>
</tr>
<tr>
<td>Added a Cost Explorer report</td>
<td>You can now track your monthly Amazon EC2 Reserved Instance (RI) utilization in Cost Explorer.</td>
<td>December 16, 2016</td>
</tr>
<tr>
<td>Added a Cost Explorer report</td>
<td>You can now track your daily Amazon EC2 Reserved Instance (RI) utilization in Cost Explorer.</td>
<td>December 15, 2016</td>
</tr>
<tr>
<td>Added AWS generated cost allocation tags</td>
<td>You can now activate the AWS generated tag <code>createdBy</code> to track who created an AWS resource.</td>
<td>December 12, 2016</td>
</tr>
<tr>
<td>Added Cost Explorer advanced options</td>
<td>You can now exclude tagged resources from your Cost Explorer reports.</td>
<td>November 18, 2016</td>
</tr>
<tr>
<td>Amazon QuickSight integration for AWS Cost and Usage Reports (p. 243)</td>
<td>AWS Cost and Usage Reports now provide customized queries for uploading your data into Amazon QuickSight.</td>
<td>November 15, 2016</td>
</tr>
<tr>
<td>Expanded AWS Budgets functionality</td>
<td>You can now use AWS Budgets to track usage data.</td>
<td>October 20, 2016</td>
</tr>
<tr>
<td>Expanded Cost Explorer functionality</td>
<td>You can now use Cost Explorer to visualize your costs by usage type groups.</td>
<td>September 15, 2016</td>
</tr>
<tr>
<td>Improved Amazon Redshift integration for AWS Cost and Usage Reports (p. 243)</td>
<td>AWS Cost and Usage Reports now provide customized queries for uploading your data into Amazon Redshift.</td>
<td>August 18, 2016</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td><strong>AWS Cost and Usage Reports</strong></td>
<td>You can now create and download AWS Cost and Usage Reports.</td>
<td>December 16, 2015</td>
</tr>
<tr>
<td><strong>AWS price list API</strong></td>
<td>You can now download offer files that list the products, prices, and restrictions for a single AWS service.</td>
<td>December 9, 2015</td>
</tr>
<tr>
<td><strong>Cost Explorer report manager</strong></td>
<td>You can now save Cost Explorer queries.</td>
<td>November 12, 2015</td>
</tr>
<tr>
<td><strong>AWS free tier tracking</strong></td>
<td>You can now track how much of your free tier limit you've used.</td>
<td>August 12, 2015</td>
</tr>
<tr>
<td><strong>Budgets and forecasting</strong></td>
<td>You can now manage your AWS usage and costs using AWS Budgets and cost forecasts.</td>
<td>June 29, 2015</td>
</tr>
<tr>
<td><strong>Amazon Web Services India Private Limited</strong></td>
<td>You can now manage your account settings and payment methods for an Amazon Web Services India Private Limited (AWS India) account.</td>
<td>June 1, 2015</td>
</tr>
<tr>
<td><strong>Expanded Cost Explorer functionality</strong></td>
<td>You can now use Cost Explorer to visualize your costs by Availability Zone, API operation, purchase option, or multiple cost allocation tags.</td>
<td>February 19, 2015</td>
</tr>
<tr>
<td><strong>Preferred payment currencies</strong></td>
<td>You can now change the currency associated with your credit card.</td>
<td>February 16, 2015</td>
</tr>
<tr>
<td><strong>Expanded Cost Explorer functionality</strong></td>
<td>You can now use Cost Explorer to visualize your costs by Amazon EC2 instance type or region.</td>
<td>January 5, 2015</td>
</tr>
<tr>
<td><strong>Avoiding unexpected charges</strong></td>
<td>Revised and expanded Avoiding Unexpected Charges and Using the Free Tier.</td>
<td>August 19, 2014</td>
</tr>
<tr>
<td><strong>IAM user permissions</strong></td>
<td>You can now enable AWS Identity and Access Management (IAM) users and federated users to access and manage your account settings, view your bills, and perform cost management. For example, you can grant people in your finance department full access to the financial setup and control of your AWS account, without having to give them access to your production AWS environment.</td>
<td>July 7, 2014</td>
</tr>
<tr>
<td><strong>Cost Explorer launched</strong></td>
<td>Cost Explorer provides a visualization of your AWS costs that enables you to analyze your costs in multiple ways.</td>
<td>April 8, 2014</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td><strong>Version 2.0 published (p. 243)</strong></td>
<td>The <em>AWS Billing and Cost Management User Guide</em> has been reorganized and rewritten to use the new Billing and Cost Management console.</td>
<td>October 25, 2013</td>
</tr>
</tbody>
</table>
AWS glossary

For the latest AWS terminology, see the AWS glossary in the AWS Glossary Reference.