



User Guide

# Application Cost Profiler



# Application Cost Profiler: User Guide

Copyright © 2024 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

.....	<b>v</b>
<b>What is AWS Application Cost Profiler?</b> .....	<b>1</b>
<b>Getting started</b> .....	<b>3</b>
Sign up for an AWS account .....	3
Create a user with administrative access .....	4
Grant programmatic access .....	5
Application Cost Profiler specific prerequisites .....	6
Next steps .....	7
Setting up Amazon S3 buckets .....	8
Giving Application Cost Profiler access to your report delivery S3 bucket .....	9
Giving Application Cost Profiler access to your usage data S3 bucket .....	10
Giving Application Cost Profiler access to SSE-KMS encrypted S3 buckets .....	12
<b>Creating your report</b> .....	<b>14</b>
Configure your Application Cost Profiler report .....	14
Reporting tenant usage data from your services .....	15
Step 1: Preparing your resource usage data .....	16
Step 2: Uploading your resource usage .....	19
Step 3: Importing usage data into Application Cost Profiler .....	20
<b>Using reports</b> .....	<b>21</b>
Data available in an Application Cost Profiler report .....	21
<b>Quotas</b> .....	<b>24</b>
Service quotas .....	24
Service endpoints .....	25
<b>Security</b> .....	<b>26</b>
Data protection .....	26
Encryption at rest .....	27
Encryption in transit .....	28
Identity and access management .....	28
Audience .....	28
Authenticating with identities .....	29
Managing access using policies .....	32
How AWS Application Cost Profiler works with IAM .....	34
Identity-based policy examples .....	37
Troubleshooting .....	42

---

Compliance validation .....	44
Resilience .....	45
Infrastructure security .....	45
<b>Monitoring events .....</b>	<b>47</b>
Monitor report generation with EventBridge .....	47
Example of a Report Generated event .....	48
<b>Document history .....</b>	<b>49</b>

AWS Application Cost Profiler will be discontinued by September 30, 2024 and is no longer accepting new customers.

# What is AWS Application Cost Profiler?

AWS Application Cost Profiler helps you separate your AWS billing and costs by the tenants of your service. A *tenant* can be a user, a group of users, or a project.

A *resource* is an entity that users can work with in AWS, such as an Amazon Elastic Compute Cloud (Amazon EC2) instance. Make sure that you can identify your resource usage by the tenant you choose.

Typical AWS resource usage includes shared services that support multiple tenants within your organization. Certain resources use time-based dimensions. To get cost and billing information by tenant rather than by hourly usage for the resource, you can integrate your resources with Application Cost Profiler. With this granular approach, you can understand how AWS resources are consumed across a shared software solution.

The following resources that can use either time-based dimensions or hourly usage are enabled for Application Cost Profiler:

- Amazon EC2 instances (on demand and spot instances only)
- Amazon Simple Queue Service (Amazon SQS) queues
- Amazon Simple Notification Service (Amazon SNS) topics
- Amazon DynamoDB reads and writes

## Note

Amazon SQS, Amazon SNS, and DynamoDB usage is not charged by time, unlike most resources. In their case, the usage during an hour (for example, a number of reads and writes in DynamoDB), is categorized by the percentage of the hour that you allocate to different tenants, regardless of when the reads or writes happened during the hour.

You integrate your services with Application Cost Profiler in three steps:

1. **Enable and configure a report** – This step defines what you want your final output to look like.
2. **Send tenant usage data to Application Cost Profiler** – This step requires code in your service to create usage data that associates tenants with the time they use your resources, and then send that usage data to Application Cost Profiler.

3. **Get reports** – Application Cost Profiler provides reports at the cadence that you specified in your report configuration. The reports show the cost associated with each tenant's usage, giving you a granular view of your billing.

For more information about these steps, see [Getting started](#).

# Getting started with Application Cost Profiler

AWS Application Cost Profiler helps you get cost information about your AWS resources by reporting resource usage by tenant, rather than for the resource as a whole. A *tenant* can be a user, a group of users, or a project. Make sure that you can identify your resource usage by the tenant you choose. To get cost reports about tenant usage, you configure a report and send usage data to Application Cost Profiler. This section discusses the prerequisites that you must complete before you use Application Cost Profiler.

## Topics

- [Sign up for an AWS account](#)
- [Create a user with administrative access](#)
- [Grant programmatic access](#)
- [Application Cost Profiler specific prerequisites](#)
- [Next steps](#)
- [Setting up Amazon S3 buckets for Application Cost Profiler](#)

## 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

1. Open <https://portal.aws.amazon.com/billing/signup>.
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 a 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 a user with administrative access

After you sign up for an AWS account, secure your AWS account root user, enable AWS IAM Identity Center, and 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 a user with administrative access

1. Enable IAM Identity Center.

For instructions, see [Enabling AWS IAM Identity Center](#) in the *AWS IAM Identity Center User Guide*.

2. In IAM Identity Center, grant administrative access to a user.

For a tutorial about using the IAM Identity Center directory as your identity source, see [Configure user access with the default IAM Identity Center directory](#) in the *AWS IAM Identity Center User Guide*.

### Sign in as the user with administrative access

- 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*.

## Assign access to additional users

1. In IAM Identity Center, create a permission set that follows the best practice of applying least-privilege permissions.

For instructions, see [Create a permission set](#) in the *AWS IAM Identity Center User Guide*.

2. Assign users to a group, and then assign single sign-on access to the group.

For instructions, see [Add groups](#) in the *AWS IAM Identity Center User Guide*.

## Grant programmatic access

Users need programmatic access if they want to interact with AWS outside of the AWS Management Console. The way to grant programmatic access depends on the type of user that's accessing AWS.

To grant users programmatic access, choose one of the following options.

Which user needs programmatic access?	To	By
Workforce identity (Users managed in IAM Identity Center)	Use temporary credentials to sign programmatic requests to the AWS CLI, AWS SDKs, or AWS APIs.	<p>Following the instructions for the interface that you want to use.</p> <ul style="list-style-type: none"> <li>• For the AWS CLI, see <a href="#">Configuring the AWS CLI to use AWS IAM Identity Center</a> in the <i>AWS Command Line Interface User Guide</i>.</li> <li>• For AWS SDKs, tools, and AWS APIs, see <a href="#">IAM Identity Center authentication</a> in</li> </ul>

Which user needs programmatic access?	To	By
		the <i>AWS SDKs and Tools Reference Guide</i> .
IAM	Use temporary credentials to sign programmatic requests to the AWS CLI, AWS SDKs, or AWS APIs.	Following the instructions in <a href="#">Using temporary credentials with AWS resources</a> in the <i>IAM User Guide</i> .
IAM	(Not recommended) Use long-term credentials to sign programmatic requests to the AWS CLI, AWS SDKs, or AWS APIs.	Following the instructions for the interface that you want to use. <ul style="list-style-type: none"> <li>• For the AWS CLI, see <a href="#">Authenticating using IAM user credentials</a> in the <i>AWS Command Line Interface User Guide</i>.</li> <li>• For AWS SDKs and tools, see <a href="#">Authenticate using long-term credentials</a> in the <i>AWS SDKs and Tools Reference Guide</i>.</li> <li>• For AWS APIs, see <a href="#">Managing access keys for IAM users</a> in the <i>IAM User Guide</i>.</li> </ul>

## Application Cost Profiler specific prerequisites

Before you get started with Application Cost Profiler, you must complete the following prerequisites:

- **Enable Cost Explorer**

Enable AWS Cost Explorer for your AWS account. Setting up an account with Cost Explorer can take up to 24 hours. You must complete Cost Explorer setup before Application Cost Profiler can generate your daily and monthly reports.

For more information, see [Enabling Cost Explorer](#) in the *AWS Billing and Cost Management User Guide*.

- **Create S3 buckets**

Create at least two Amazon Simple Storage Service (Amazon S3) buckets. Application Cost Profiler uses one S3 bucket to provide reports to you. You use the other S3 bucket to upload usage data to Application Cost Profiler. Typically, you only need one S3 bucket to upload usage data. However, you might want to have more than one S3 bucket so that you can keep usage for different services in separate S3 buckets with different permissions, if needed for your security. You must give Application Cost Profiler permissions to these S3 buckets.

For more information about setting up the Amazon S3 buckets for Application Cost Profiler, see [Setting up Amazon S3 buckets for Application Cost Profiler](#).

- **Enable tags**

To report usage by tag, rather than by resource, you must enable those tags in the AWS Billing and Cost Management console.

For more information about activating AWS generated tags, see [Activating the AWS-Generated Cost Allocation Tags](#) in the *AWS Billing and Cost Management User Guide*. For more information about activating user-defined tags, see [Activating User-Defined Cost Allocation Tags](#) in the *AWS Billing and Cost Management User Guide*.

## Next steps

After you complete these prerequisites, you can:

- Configure your report and send usage data to Application Cost Profiler. For more information, see [Creating your report](#).
- Get and analyze your generated reports. For more information, see [Using Application Cost Profiler reports](#).

# Setting up Amazon S3 buckets for Application Cost Profiler

To send usage data to and receive reports from AWS Application Cost Profiler, you must have at least one Amazon Simple Storage Service (Amazon S3) bucket in your AWS account to store data and one S3 bucket to receive your reports.

## Note

For users of AWS Organizations, the Amazon S3 buckets can be either in the management account or in individual member accounts. The data in S3 buckets owned by the management account can be used to generate reports for the entire organization. In individual member accounts, the data in the S3 buckets can only be used to generate reports for that member account.

The S3 buckets you create are owned by the AWS account that you create them in. The S3 buckets are billed at standard Amazon S3 rates. For more information about how to create an Amazon S3 bucket, see [Creating a bucket](#) in the *Amazon Simple Storage Service User Guide*.

In order for Application Cost Profiler to use the S3 buckets, you must attach a policy to the buckets that gives Application Cost Profiler permissions to read and/or write to the bucket. If you modify the policy after your reports are set up, you may prevent Application Cost Profiler from being able to read your usage data or deliver your reports.

The following topics show how to set up permissions on your Amazon S3 buckets after you have created them. In addition to the ability to read and write objects, if you encrypted the buckets, Application Cost Profiler must have access to the AWS Key Management Service (AWS KMS) key for each bucket.

## Topics

- [Giving Application Cost Profiler access to your report delivery S3 bucket](#)
- [Giving Application Cost Profiler access to your usage data S3 bucket](#)
- [Giving Application Cost Profiler access to SSE-KMS encrypted S3 buckets](#)

## Giving Application Cost Profiler access to your report delivery S3 bucket

The S3 bucket that you configure for Application Cost Profiler to deliver your reports to must have a policy attached that allows Application Cost Profiler to create the report objects. In addition, the S3 bucket must be configured to enable encryption.

### Note

When you create your bucket, you must choose to encrypt it. You may choose to encrypt your bucket with Amazon S3-managed keys (SSE-S3) or with your own key managed by AWS KMS (SSE-KMS). If you have already created your bucket with no encryption, you must edit your bucket to add encryption.

### To give Application Cost Profiler access to your report delivery S3 bucket

1. Go to the [Amazon S3 console](#) and sign in.
2. Select **Buckets** from the left navigation, and then choose your bucket from the list.
3. Choose the **Permissions** tab, then, next to **Bucket policy**, choose **Edit**.
4. In the **Policy** section, insert the following policy. Replace *<bucket\_name>* with the name of your bucket, and *<AWS account>* with the ID of your AWS account.

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "application-cost-profiler.amazonaws.com"
      },
      "Action": [
        "s3:PutObject*",
        "s3:GetEncryptionConfiguration"
      ],
      "Resource": [
        "arn:aws:s3:::<bucket-name>",
        "arn:aws:s3:::<bucket-name>/*"
      ],
    }
  ],
}
```

```
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "<AWS account>"
      },
      "ArnEquals": {
        "aws:SourceArn": "arn:aws:application-cost-profiler:us-east-1:<AWS
account>:*"
      }
    }
  ]
}
```

In this policy you are giving the Application Cost Profiler service principal (`application-cost-profiler.amazonaws.com`) access to deliver reports to the specified bucket. It does this on your behalf, and includes a header with your AWS account and an ARN specific to your report delivery bucket. To ensure that Application Cost Profiler is accessing your bucket only when acting on your behalf, the `Condition` checks for those headers.

5. Choose **Save changes** to save your policy, attached to your bucket.

If you have created your bucket using SSE-S3 encryption, then you are done. If you used SSE-KMS encryption, then the following steps are necessary to give Application Cost Profiler access to your bucket.

6. (Optional) Choose the **Properties** tab for your bucket, and under **Default Encryption**, select the Amazon Resource Name (ARN) for your AWS KMS key. This action displays the AWS Key Management Service console and shows your key.
7. (Optional) Add the policy to give Application Cost Profiler access to the AWS KMS key. For instructions on adding this policy, see [Giving Application Cost Profiler access to SSE-KMS encrypted S3 buckets](#).

## Giving Application Cost Profiler access to your usage data S3 bucket

The S3 bucket that you configure for Application Cost Profiler to read your usage data from must have a policy attached to allow Application Cost Profiler to read the usage data objects.

**Note**

By giving Application Cost Profiler access to your usage data, you agree that we may temporarily copy such usage data objects to the US East (N. Virginia) AWS Region while processing reports. These data objects will be kept in the US East (N. Virginia) Region until the monthly report generation is complete.

**To give Application Cost Profiler access to your usage data S3 bucket**

1. Go to the [Amazon S3 console](#) and sign in.
2. Select **Buckets** from the left navigation, and then choose your bucket from the list.
3. Choose the **Permissions** tab, then, next to **Bucket policy**, choose **Edit**.
4. In the **Policy** section, insert the following policy. Replace *<bucket-name>* with the name of your bucket, and *<AWS account>* with the ID of your AWS account.

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "application-cost-profiler.amazonaws.com"
      },
      "Action": [
        "s3:GetObject*"
      ],
      "Resource": [
        "arn:aws:s3:::<bucket-name>",
        "arn:aws:s3:::<bucket-name>/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "<AWS account>"
        },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:application-cost-profiler:us-east-1:<AWS
account>:*"
        }
      }
    }
  ]
}
```



```
    }  
  ]  
}
```

In this policy you are giving the Application Cost Profiler service principal (`application-cost-profiler.amazonaws.com`) access to get data out of the specified bucket. It does this on your behalf, and includes a header with your AWS account and an ARN specific to your usage bucket. To ensure that Application Cost Profiler is accessing your bucket only when acting on your behalf, the `Condition` checks for those headers.

5. Choose **Save changes** to save your policy, attached to your bucket.

If your bucket is encrypted with AWS KMS managed keys, then you must give Application Cost Profiler access to your bucket by following the procedure in the next section.

## Giving Application Cost Profiler access to SSE-KMS encrypted S3 buckets

If you encrypt the S3 buckets that you configure for Application Cost Profiler (required for report buckets) with keys stored in AWS KMS (SSE-KMS), you must also give permissions to Application Cost Profiler to decrypt them. You do this by giving access to the AWS KMS keys used to encrypt the data.

### Note

If your bucket is encrypted with Amazon S3 managed keys, then you do not need to complete this procedure.

### To give Application Cost Profiler access to AWS KMS for SSE-KMS encrypted S3 buckets

1. Go to the [AWS KMS console](#) and sign in.
2. Select **Customer managed keys** from the left navigation, and then choose the key that is used to encrypt your bucket from the list.
3. Select **Switch to policy view**, then choose **Edit**.
4. In the **Policy** section, insert the following policy statement.

```
{
```

```

    "Effect": "Allow",
    "Principal": {
      "Service": "application-cost-profiler.amazonaws.com"
    },
    "Action": [
      "kms:Decrypt",
      "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "<AWS account>"
      },
      "ArnEquals": {
        "aws:SourceArn": "arn:aws:application-cost-profiler:us-east-1:<AWS
account>:*"
      }
    }
  }
}

```

5. Choose **Save changes** to save your policy, attached to your key.
6. Repeat for each key that encrypts an S3 bucket that Application Cost Profiler needs to access.

#### Note

The data is copied out of your S3 bucket on import into Application Cost Profiler managed buckets (that are encrypted). If you revoke the access to the keys, Application Cost Profiler can't retrieve any new objects from the bucket. However, any data already imported can still be used to generate reports.

# Creating your report

After fulfilling the [prerequisites](#), you're ready to configure the report for your AWS account and send your usage data to AWS Application Cost Profiler. This section describes how to configure the report and how to send the usage data to Application Cost Profiler.

## Configure your Application Cost Profiler report

The following procedure shows how to configure the report that you want to generate based on your usage date. You configure details such as the frequency that the report is generated.

### Note

If your AWS account is part of an AWS organization, you can configure the report using either the management account or an individual member account. Reports configured for individual accounts only contain data for that account. Reports configured using the management account can include data for the entire organization.

The Amazon S3 bucket used for report output must belong to the account creating the report configuration.

### To configure your Application Cost Profiler report

1. Open a web browser and sign in to the [Application Cost Profiler console](#).
2. Choose **Get started now** to configure or modify a report.
3. Enter a **Report Name** and **Report Description** for your report.
4. Enter the name of your S3 bucket in the **Enter S3 bucket name** field and enter the S3 prefix in the **Enter S3 prefix** field. For more information about creating S3 buckets and giving Application Cost Profiler permissions, see [Setting up Amazon S3 buckets for Application Cost Profiler](#).
5. Select the options that you want your report to have:
  - **Time Frequency** – Choose whether the report is generated on a **Daily** or **Monthly** cadence, or **Both**.
  - **Report Output Format** – Choose the type of file to create within your Amazon S3 bucket. If you choose **CSV**, Application Cost Profiler creates a comma-separated values text file with

gzip compression for the reports. If you choose **Parquet**, a Parquet file is generated for the reports.

6. Choose **Configure** to save your report configuration.

**Note**

You can also use the [AWS Application Cost Profiler API](#) to configure reports.

Verify the report settings by choosing **Get started now** to view the current report configuration.

**Note**

You can only have a single report configured. Returning to the configuration page will edit your existing report.

After you have configured your report, data ingestion is enabled. You can integrate your services with Application Cost Profiler to provide usage data for your resources.

## Reporting tenant usage data from your services

After you have configured the report, you are ready to send tenant usage data from the resources or services in your account. You must inform Application Cost Profiler when your resource is being used for a specific tenant. For example, if your service accepts API calls from different tenants, you record a start and end time for each tenant as you start and end an API call from that tenant. Application Cost Profiler uses that data to generate reports about the cost of your service, by the amount of time spent on work for each tenant.

To give Application Cost Profiler the usage data, you do the following:

- **Prepare resource usage data** – Create tables that describe when a resource is used for a specific tenant.
- **Upload usage data** – Upload the tables to an Amazon S3 bucket that you have given Application Cost Profiler permission to access.
- **Import usage data** – Call the `ImportApplicationUsage` API operation to let Application Cost Profiler know the data is ready to be processed.

The following sections describe each of these steps in more detail.

## Topics

- [Step 1: Preparing your resource usage data](#)
- [Step 2: Uploading your resource usage](#)
- [Step 3: Importing usage data into Application Cost Profiler](#)

## Step 1: Preparing your resource usage data

As a resource is being used in your service, you track which tenant is using it. Record this data into a table that you can later upload for Application Cost Profiler to import. Each row in the table describes a resource, the tenant that is using the resource, and the start and end times of that usage. An example of a resource is an Amazon Elastic Compute Cloud (Amazon EC2) instance that is being used.

This step requires that you integrate code into your service to output the correct information about the usage.

The fields that are in a resource usage table are listed in the following table.

Field	Description
<b>ApplicationId</b>	Identifies the application or product in your system that is being used. Defines the scope of the tenant metadata.
<b>TenantId</b>	An identifier in your system for the tenant who is consuming the specified resource. Application Cost Profiler aggregates to this level within the <b>ApplicationId</b> .
<b>TenantDesc</b>	(Optional) Additional data about the tenant for your own additional reporting.
<b>UsageAccountId</b>	The account that the resource runs in (important for accounts that are part of an organization).

Field	Description
<b>StartTime</b>	Timestamp (in milliseconds and microseconds) from Epoch, in UTC. Indicates the start time of the period for the usage by the specified tenant.
<b>EndTime</b>	Timestamp (in milliseconds and microseconds) from Epoch, in UTC. Indicates the end time of the period for the usage by the specified tenant.
<b>ResourceId</b>	Amazon Resource Name (ARN) for resource being used.
<b>Name</b>	(Optional) As an alternative to specifying a <b>ResourceId</b> , you can specify a <b>Name</b> resource tag to attribute costs to a set of resources (the field must include the value you want to use for the <b>Name</b> tag). Resource tags are enabled as part of your Cost and Usage Report. For more information about resource tags, see <a href="#">Resource tags details</a> in the <i>Cost and Usage Report User Guide</i> .

The output must be in a comma-separated values (.csv) file that includes a heading row, as shown in the following example.

```
ApplicationId,TenantId,TenantDesc,UsageAccountId,StartTime,EndTime,ResourceId
MyApp,Tenant1,,123456789012,1613681437032.9001,1613681437041.5312,arn:aws:ec2:us-east-1:123456789012:instance/1234-abcd-example-1234
MyApp,Tenant2,,123456789012,1613681245531.4426,1613681245551.1323,arn:aws:ec2:us-east-1:123456789012:instance/1234-abcd-example-1234
MyApp,Tenant1,,123456789012,1613681904815.3381,1613681904930.0972,arn:aws:ec2:us-east-1:123456789012:instance/1234-abcd-example-1234
MyApp,Tenant2,,123456789012,1613681904765.1956,1613681904946.574,arn:aws:ec2:us-east-1:123456789012:instance/1234-abcd-example-1234
```

Save the data as a file, with a .csv extension (or .csv.gzip if compressed with gzip). When you upload this data to Application Cost Profiler, each time slice is assigned to the associated tenant. In this example, the report includes the time slice of the Amazon EC2 instance cost for that tenant. For Amazon EC2 instances only, slices that are not associated with a specific tenant are added to an *unattributed* tenant. Overlapping time slices are counted multiple times. It's your responsibility to ensure that the data in your usage table is accurate.

**Note**

Your file must represent one hour of time. If a resource is used over multiple hours, end the usage on the hour, and have a new record in the next file that starts at the same time. You must submit a single file containing an entire hour's data. If multiple files are submitted for the same hour's data, Application Cost Profiler only considers the data in the latest file.

For example, the following table shows how Application Cost Profiler calculates usage for three tenants, over an hour (3,600,000 milliseconds), based on provided time slices.

Tenant	Provided time slices	Calculated percent of hourly cost
Tenant1	1,200,000 ms	33.34%
Tenant2	600,000 ms	16.66%
<unattributed>		50.00%

In this example, Tenant1 is assigned one-third of the hour and Tenant2 is assigned one-sixth of the hour. The remaining half-hour (1,800,000 ms) is not attributed to either of the clients, which is 50% of the hour.

Currently, the following resources are enabled for Application Cost Profiler:

- Amazon EC2 instances (on demand and spot instances only)
- Lambda functions (If you are sending data for a Lambda function, you must send the Unqualified Resource ARN as ResourceId.)
- Amazon Elastic Container Service (Amazon ECS) instances

- Amazon Simple Queue Service (Amazon SQS) queues
- Amazon Simple Notification Service (Amazon SNS) topics
- Amazon DynamoDB reads and writes

**Note**

Amazon SQS, Amazon SNS, and DynamoDB usage is not charged by time, unlike most resources. In their case, the usage during an hour (for example, a number of reads and writes in DynamoDB), is categorized by the percentage of the hour that you allocate to different tenants, regardless of when the reads or writes happened during the hour.

## Step 2: Uploading your resource usage

After you have a file of usage by tenant, upload your data file to Amazon S3 and make sure that Application Cost Profiler has permission to access it.

To learn more about creating an S3 bucket, see [Application Cost Profiler specific prerequisites](#).

You must make sure that Application Cost Profiler has access to your S3 bucket. This only needs to be done once per S3 bucket (you can reuse the same bucket for uploading multiple usage files). For information about giving access to the bucket, see [Giving Application Cost Profiler access to your usage data S3 bucket](#). If the bucket is encrypted, see [Giving Application Cost Profiler access to SSE-KMS encrypted S3 buckets](#).

**Note**

It is not required that you encrypt the S3 buckets that you use for usage data.

Upload your data to the S3 bucket as a file, with a .csv extension (or .csv.gz if compressed with gzip), at hourly intervals. After you upload a new file, you must inform Application Cost Profiler that you have uploaded it so that the file can be imported into your report.

**Note**

By giving Application Cost Profiler access to your usage data, you agree that we may temporarily copy such usage data objects to the US East (N. Virginia) AWS Region while



processing reports. These data objects will be kept in the US East (N. Virginia) Region until the monthly report generation is complete.

### Step 3: Importing usage data into Application Cost Profiler

After you have uploaded usage data to an Amazon S3 bucket that Application Cost Profiler has access to, inform Application Cost Profiler that the data exists and to import it into your final report. You do this by using the `ImportApplicationUsage` operation in the Application Cost Profiler API.

For information about the AWS Application Cost Profiler API, including the `ImportApplicationUsage` operation, see the [AWS Application Cost Profiler API Reference](#).

The following example shows how to call `ImportApplicationUsage`. Replace the *input text in brackets* with the values for your S3 bucket and uploaded object.

```
POST /ImportApplicationUsage HTTP/1.1
Content-type: application/json

{
  "sourceS3Location" : {
    "bucket": "<bucket-name>",
    "key": "<object-key>",
    "region": "<region-id>"
  }
}
```

#### Note

The `region` parameter is only required if your bucket is in an AWS Region that is disabled by default. For more information, see [Managing AWS Regions](#) in the *AWS General Reference*.

Application Cost Profiler generates a new report at the frequency that you requested when [configuring your report](#), using the data that you imported with `ImportApplicationUsage`.

After you have configured your report and automated importing your usage data into Application Cost Profiler, you are ready to view your generated reports. For more information about reports, see [Using Application Cost Profiler reports](#).

## Using Application Cost Profiler reports

After you have integrated your usage data with AWS Application Cost Profiler and are sending the data on an hourly basis, Application Cost Profiler automatically generates your report.

Reports are generated either daily or monthly, based on the option you selected when [configuring your report](#). Reports are delivered to the Amazon Simple Storage Service (Amazon S3) bucket that you selected when you configured the report.

Daily reports generated on the first day of the month have the previous month's data.

## Data available in an Application Cost Profiler report

The columns that are created in a usage report are shown in the following table.

Column name	Description
<b>PayerAccountId</b>	The management account ID in an organization, or the account ID if the account is not part of AWS Organizations.
<b>UsageAccountId</b>	The account ID for the account with usage.
<b>LineItemType</b>	The type of record. Always Usage.
<b>UsageStartTime</b>	Timestamp (in milliseconds) from Epoch, in UTC. Indicates the start time of the period for the usage by the specified tenant.
<b>UsageEndTime</b>	Timestamp (in milliseconds) from Epoch, in UTC. Indicates the end time of the period for the usage by the specified tenant.
<b>ApplicationIdentifier</b>	The <b>ApplicationId</b> specified in the usage data sent to Application Cost Profiler.
<b>TenantIdentifier</b>	The <b>TenantId</b> specified in the usage data sent to Application Cost Profiler. Data with

Column name	Description
	no record in the usage data is collected in unattributed .
<b>TenantDescription</b>	The TenantDesc specified in the usage data sent to Application Cost Profiler.
<b>ProductCode</b>	The AWS product being billed (for example, AmazonEC2 ).
<b>UsageType</b>	The type of usage being billed (for example, BoxUsage:c5.large ).
<b>Operation</b>	The operation being billed (for example, RunInstances ).
<b>ResourceId</b>	The resource ID or Amazon Resource Name (ARN) for the resource being billed.
<b>ScaleFactor</b>	If a resource is over-allocated for an hour, for example, the usage data reported is equal to 2 hours instead of 1 hour, a scale factor is applied to make the total equal the actual billed amount (in this case, 0.5). This column reports the scale factor used for the specific resource for that hour. The scale factor is always greater than zero (0) and less than or equal to 1.
<b>TenantAttributionPercent</b>	The percentage of the usage attributed to the specified tenant (between zero (0) and 1).
<b>UsageAmount</b>	The amount of usage attributed to the specified tenant.
<b>CurrencyCode</b>	The currency that the rate and cost are in (for example, USD).

Column name	Description
Rate	The billing rate for the usage, per unit.
TenantCost	The total cost for that resource for the specified tenant.
Region	The AWS Region of the resource.
Name	If you created resource tags for your resources on the Cost and Usage report, or through the resource usage data, the <b>Name</b> tag is shown here. For more information about resource tags, see <a href="#">Resource tags details</a> in the <i>Cost and Usage Report User Guide</i> .

The following is an example of the output report for one resource for two hours.

```
PayerAccountId,UsageAccountId,LineItemType,UsageStartTime,UsageEndTime,ApplicationIdentifier,TenantId,Region,Usage
123456789012,123456789012,Usage,2021-02-01T00:00:00.000Z,2021-02-01T00:30:00.000Z,Canary,unattributed,
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T00:30:00.000Z,2021-02-01T01:00:00.000Z,Canary,Tenant1,
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant2,
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant3,
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant4,
east-1,test-tag
123456789012,123456789012,Usage,2021-02-01T01:00:00.000Z,2021-02-01T02:00:00.000Z,Canary,Tenant1,
east-1,test-tag
```

In this example, the first hour is allocated to Tenant1 for half of the time. A half hour remains as unattributed. In the second hour, four tenants are all allocated the full hour. In this case, the scale factor scales them all down by 0.25, and they are all allocated one-quarter of the hour. You can see the final cost in the TenantCost column.

# AWS Application Cost Profiler quotas and endpoints

Your AWS account has default quotas, formerly referred to as limits, for each AWS service. Unless otherwise noted, each quota is AWS Region-specific. You can request increases for some quotas, and other quotas cannot be increased.

The following tables list the service quotas per account and the AWS Region endpoints for Application Cost Profiler.

## Service quotas

Resource	Default value	Description
Rate of PutReportDefinition requests	5	The maximum number of PutReportDefinition requests per second per account.
Rate of UpdateReportDefinition requests	5	The maximum number of UpdateReportDefinition requests per second per account.
Rate of GetReportDefinition requests	5	The maximum number of GetReportDefinition requests per second per account.
Rate of DeleteReportDefinition requests	5	The maximum number of DeleteReportDefinition requests per second per account.
Rate of ListReportDefinitions requests	5	The maximum number of ListReportDefinitions requests per second per account.

Resource	Default value	Description
Rate of ImportApplicationUsage requests	5	The maximum number of ImportApplicationUsage requests per second per account.
Maximum size of usage data file	10 MB	The maximum size of an hourly usage data file.

## Service endpoints

Application Cost Profiler is a global service. All API calls must be made to the US East (N. Virginia) endpoint.

- US East (N. Virginia) – `application-cost-profiler.us-east-1.amazonaws.com`

# Security in AWS Application Cost Profiler

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 Application Cost Profiler, 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 AWS Application Cost Profiler. It shows you how to configure Application Cost Profiler to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Application Cost Profiler resources.

## Contents

- [Data protection in AWS Application Cost Profiler](#)
- [Identity and access management for AWS Application Cost Profiler](#)
- [Compliance validation for AWS Application Cost Profiler](#)
- [Resilience in AWS Application Cost Profiler](#)
- [Infrastructure security in AWS Application Cost Profiler](#)

## Data protection in AWS Application Cost Profiler

The AWS [shared responsibility model](#) applies to data protection in AWS Application Cost Profiler. 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. You are also responsible for 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. For information about using CloudTrail trails to capture AWS activities, see [Working with CloudTrail trails](#) in the *AWS CloudTrail User Guide*.
- 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 140-3 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 \(FIPS\) 140-3](#).

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 Application Cost Profiler 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.

## Encryption at rest

AWS Application Cost Profiler always encrypts all data stored in the service at rest without requiring any additional configuration. This encryption is automatic when you use Application Cost Profiler.



For Amazon S3 buckets you provide, you must encrypt the report bucket, and can encrypt the usage data bucket and give Application Cost Profiler access. For more information, see [Setting up Amazon S3 buckets for Application Cost Profiler](#).

## Encryption in transit

AWS Application Cost Profiler uses Transport Layer Security (TLS) and client-side encryption for encryption in transit. Communication with Application Cost Profiler is always done over HTTPS so your data is always encrypted in transit. This encryption is configured by default when you use Application Cost Profiler.

## Identity and access management for AWS Application Cost Profiler

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 Application Cost Profiler resources. IAM is an AWS service that you can use with no additional charge.

### Topics

- [Audience](#)
- [Authenticating with identities](#)
- [Managing access using policies](#)
- [How AWS Application Cost Profiler works with IAM](#)
- [AWS Application Cost Profiler identity-based policy examples](#)
- [Troubleshooting AWS Application Cost Profiler identity and access](#)

## Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work that you do in Application Cost Profiler.

**Service user** – If you use the Application Cost Profiler service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Application Cost Profiler features to do your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your

administrator. If you cannot access a feature in Application Cost Profiler, see [Troubleshooting AWS Application Cost Profiler identity and access](#).

**Service administrator** – If you're in charge of Application Cost Profiler resources at your company, you probably have full access to Application Cost Profiler. It's your job to determine which Application Cost Profiler features and resources your service users should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with Application Cost Profiler, see [How AWS Application Cost Profiler works with IAM](#).

**IAM administrator** – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to Application Cost Profiler. To view example Application Cost Profiler identity-based policies that you can use in IAM, see [AWS Application Cost Profiler identity-based policy examples](#).

## Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. You must be *authenticated* (signed in to AWS) as the AWS account root user, as an IAM user, or by assuming an IAM role.

You can sign in to AWS as a federated identity by using credentials provided through an identity source. AWS IAM Identity Center (IAM Identity Center) users, your company's single sign-on authentication, and your Google or Facebook credentials are examples of federated identities. When you sign in as a federated identity, your administrator previously set up identity federation using IAM roles. When you access AWS by using federation, you are indirectly assuming a role.

Depending on the type of user you are, you can sign in to the AWS Management Console or the AWS access portal. For more information about signing in to AWS, see [How to sign in to your AWS account](#) in the *AWS Sign-In User Guide*.

If you access AWS programmatically, AWS provides a software development kit (SDK) and a command line interface (CLI) to cryptographically sign your requests by using your credentials. If you don't use AWS tools, you must sign requests yourself. For more information about using the recommended method to sign requests yourself, see [Signing AWS API requests](#) in the *IAM User Guide*.

Regardless of the authentication method that you use, you might be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication

(MFA) to increase the security of your account. To learn more, see [Multi-factor authentication](#) in the *AWS IAM Identity Center User Guide* and [Using multi-factor authentication \(MFA\) in AWS](#) in the *IAM User Guide*.

## AWS account root user

When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see [Tasks that require root user credentials](#) in the *IAM User Guide*.

## IAM users and groups

An [IAM user](#) is an identity within your AWS account that has specific permissions for a single person or application. Where possible, we recommend relying on temporary credentials instead of creating IAM users who have long-term credentials such as passwords and access keys. However, if you have specific use cases that require long-term credentials with IAM users, we recommend that you rotate access keys. For more information, see [Rotate access keys regularly for use cases that require long-term credentials](#) in the *IAM User Guide*.

An [IAM group](#) is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named *IAMAdmins* and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see [When to create an IAM user \(instead of a role\)](#) in the *IAM User Guide*.

## IAM roles

An [IAM role](#) is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. You can temporarily assume an IAM role in the AWS Management Console by [switching roles](#). You can assume a role by calling an AWS CLI or AWS API operation or by using a custom URL. For more information about methods for using roles, see [Using IAM roles](#) in the *IAM User Guide*.

IAM roles with temporary credentials are useful in the following situations:

- **Federated user access** – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see [Creating a role for a third-party Identity Provider](#) in the *IAM User Guide*. If you use IAM Identity Center, you configure a permission set. To control what your identities can access after they authenticate, IAM Identity Center correlates the permission set to a role in IAM. For information about permission sets, see [Permission sets](#) in the *AWS IAM Identity Center User Guide*.
- **Temporary IAM user permissions** – An IAM user or role can assume an IAM role to temporarily take on different permissions for a specific task.
- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see [Cross account resource access in IAM](#) in the *IAM User Guide*.
- **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.
  - **Forward access sessions (FAS)** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. When you use some services, you might perform an action that then initiates another action in a different service. FAS uses the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. FAS requests are only made when a service receives a request that requires interactions with other AWS services or resources to complete. In this case, you must have permissions to perform both actions. For policy details when making FAS requests, see [Forward access sessions](#).
  - **Service role** – A service role is an [IAM role](#) that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see [Creating a role to delegate permissions to an AWS service](#) in the *IAM User Guide*.
  - **Service-linked role** – A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked

roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

- **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see [Using an IAM role to grant permissions to applications running on Amazon EC2 instances](#) in the *IAM User Guide*.

To learn whether to use IAM roles or IAM users, see [When to create an IAM role \(instead of a user\)](#) in the *IAM User Guide*.

## Managing access using policies

You control access in AWS by creating policies and attaching them to AWS identities or resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when a principal (user, root user, or role session) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see [Overview of JSON policies](#) in the *IAM User Guide*.

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

By default, users and roles have no permissions. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

## Identity-based policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can

perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see [Creating IAM policies](#) in the *IAM User Guide*.

Identity-based policies can be further categorized as *inline policies* or *managed policies*. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see [Choosing between managed policies and inline policies](#) in the *IAM User Guide*.

## Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are *IAM role trust policies* and *Amazon S3 bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must [specify a principal](#) in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

## Access control lists (ACLs)

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs. To learn more about ACLs, see [Access control list \(ACL\) overview](#) in the *Amazon Simple Storage Service Developer Guide*.

## Other policy types

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user

or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of an entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the `Principal` field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see [Permissions boundaries for IAM entities](#) in the *IAM User Guide*.

- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see [Service control policies](#) in the *AWS Organizations User Guide*.
- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see [Session policies](#) in the *IAM User Guide*.

## Multiple policy types

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

## How AWS Application Cost Profiler works with IAM

Before you use IAM to manage access to Application Cost Profiler, you should understand what IAM features are available to use with Application Cost Profiler. To get a high-level view of how Application Cost Profiler and other AWS services work with IAM, see [AWS Services That Work with IAM](#) in the *IAM User Guide*.

### Topics

- [Application Cost Profiler identity-based policies](#)
- [Application Cost Profiler resource-based policies](#)
- [Authorization based on Application Cost Profiler tags](#)
- [Application Cost Profiler IAM roles](#)



## Application Cost Profiler identity-based policies

With IAM identity-based policies, you can specify allowed or denied actions and resources in addition to the conditions under which actions are allowed or denied. Application Cost Profiler supports specific actions. To learn about all of the elements that you use in a JSON policy, see [IAM JSON Policy Elements Reference](#) in the *IAM User Guide*.

### Actions

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Action` element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Policy actions usually have the same name as the associated AWS API operation. There are some exceptions, such as *permission-only actions* that don't have a matching API operation. There are also some operations that require multiple actions in a policy. These additional actions are called *dependent actions*.

Include actions in a policy to grant permissions to perform the associated operation.

Policy actions in Application Cost Profiler use the following prefix before the action: `application-cost-profiler:`. For example, to grant someone permission to view the details of your Application Cost Profiler report definition, you include the `application-cost-profiler:GetReportDefinition` action in their policy. Policy statements must include either an `Action` or `NotAction` element. Application Cost Profiler defines its own set of actions that describe tasks that you can perform with this service.

To specify multiple actions in a single statement, separate them with commas as follows.

```
"Action": [  
    "application-cost-profiler:ListReportDefinitions",  
    "application-cost-profiler:GetReportDefinition"
```

The following are the actions available in Application Cost Profiler. Each allows the API action of the same name. For more information about the Application Cost Profiler API, see [AWS Application Cost Profiler API Reference](#).

- `application-cost-profiler:ListReportDefinitions` – Allows listing the report definition for your AWS account, if any.



- `application-cost-profiler:GetReportDefinition` – Allows getting the details of the report definition for your Application Cost Profiler report.
- `application-cost-profiler:PutReportDefinition` – Allows creating a new report definition.
- `application-cost-profiler:UpdateReportDefinition` – Allows updating a report definition.
- `application-cost-profiler>DeleteReportDefinition` – Allows deleting a report (only available through the Application Cost Profiler API).
- `application-cost-profiler:ImportApplicationUsage` – Allows requesting Application Cost Profiler import usage data from a specified Amazon S3 bucket.

## Resources

Application Cost Profiler does not support specifying resource Amazon Resource Names (ARNs) in a policy.

## Condition keys

Application Cost Profiler does not provide any service-specific condition keys, but it does support using some global condition keys. To see all AWS global condition keys, see [AWS Global Condition Context Keys](#) in the *IAM User Guide*.

## Examples

To view examples of Application Cost Profiler identity-based policies, see [AWS Application Cost Profiler identity-based policy examples](#).

## Application Cost Profiler resource-based policies

Application Cost Profiler does not support resource-based policies.

## Authorization based on Application Cost Profiler tags

Application Cost Profiler does not support tagging resources or controlling access based on tags.

## Application Cost Profiler IAM roles

An [IAM role](#) is an entity within your AWS account that has specific permissions.

## Using temporary credentials with Application Cost Profiler

You can use temporary credentials to sign in with federation, assume an IAM role, or to assume a cross-account role. You obtain temporary security credentials by calling AWS STS API operations such as [AssumeRole](#) or [GetFederationToken](#).

Application Cost Profiler supports using temporary credentials.

### Service-linked roles

[Service-linked roles](#) allow AWS services to access resources in other services to complete an action on your behalf. Service-linked roles appear in your IAM account and are owned by the service. An administrator can view but not edit the permissions for service-linked roles.

Application Cost Profiler does not support service-linked roles.

### Service roles

This feature allows a service to assume a [service role](#) on your behalf. This role allows the service to access resources in other services to complete an action on your behalf. Service roles appear in your IAM account and are owned by the account. This means that an administrator can change the permissions for this role. However, doing so might break the functionality of the service.

Application Cost Profiler does not support service roles.

## AWS Application Cost Profiler identity-based policy examples

By default, IAM users and roles don't have permissions to create or modify AWS Application Cost Profiler resources. They also can't perform tasks using the AWS Management Console, AWS Command Line Interface (AWS CLI), or AWS API. An administrator must create IAM policies that grant users and roles permission to perform the specific API operations that they need. The administrator must then attach those policies to the IAM users or groups that require those permissions.

To learn how to create an IAM identity-based policy using these example JSON policy documents, see [Creating Policies on the JSON Tab](#) in the *IAM User Guide*.

### Topics

- [Policy best practices](#)

- [Using the Application Cost Profiler console](#)
- [Allow users to view their own permissions](#)
- [Accessing one Amazon S3 bucket](#)

## Policy best practices

Identity-based policies determine whether someone can create, access, or delete Application Cost Profiler resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started with AWS managed policies and move toward least-privilege permissions** – To get started granting permissions to your users and workloads, use the *AWS managed policies* that grant permissions for many common use cases. They are available in your AWS account. We recommend that you reduce permissions further by defining AWS customer managed policies that are specific to your use cases. For more information, see [AWS managed policies](#) or [AWS managed policies for job functions](#) in the *IAM User Guide*.
- **Apply least-privilege permissions** – When you set permissions with IAM policies, grant only the permissions required to perform a task. You do this by defining the actions that can be taken on specific resources under specific conditions, also known as *least-privilege permissions*. For more information about using IAM to apply permissions, see [Policies and permissions in IAM](#) in the *IAM User Guide*.
- **Use conditions in IAM policies to further restrict access** – You can add a condition to your policies to limit access to actions and resources. For example, you can write a policy condition to specify that all requests must be sent using SSL. You can also use conditions to grant access to service actions if they are used through a specific AWS service, such as AWS CloudFormation. For more information, see [IAM JSON policy elements: Condition](#) in the *IAM User Guide*.
- **Use IAM Access Analyzer to validate your IAM policies to ensure secure and functional permissions** – IAM Access Analyzer validates new and existing policies so that the policies adhere to the IAM policy language (JSON) and IAM best practices. IAM Access Analyzer provides more than 100 policy checks and actionable recommendations to help you author secure and functional policies. For more information, see [IAM Access Analyzer policy validation](#) in the *IAM User Guide*.
- **Require multi-factor authentication (MFA)** – If you have a scenario that requires IAM users or a root user in your AWS account, turn on MFA for additional security. To require MFA when API operations are called, add MFA conditions to your policies. For more information, see [Configuring MFA-protected API access](#) in the *IAM User Guide*.

For more information about best practices in IAM, see [Security best practices in IAM](#) in the *IAM User Guide*.

## Using the Application Cost Profiler console

To access the AWS Application Cost Profiler console, you must have a minimum set of permissions. These permissions must allow you to list and view details about the Application Cost Profiler resources in your AWS account. If you create an identity-based policy that is more restrictive than the minimum required permissions, the console won't function as intended for entities (IAM users or roles) with that policy.

To ensure that those entities can use the Application Cost Profiler console to view the Application Cost Profiler report definition for your AWS account, attach the following permissions to the entities.

```
application-cost-profiler:ListReportDefinitions
application-cost-profiler:GetReportDefinition
```

For example, you could create the following policy for your read-only users.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "application-cost-profiler:ListReportDefinitions",
        "application-cost-profiler:GetReportDefinition"
      ],
      "Resource": "*"
    }
  ]
}
```

For more information, see [Adding Permissions to a User](#) in the *IAM User Guide*.

You don't need to allow minimum console permissions for users that are making calls only to the AWS CLI or the AWS API. Instead, allow access to only the actions that match the API operation that you're trying to perform.

## Allow users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

## Accessing one Amazon S3 bucket

In this example, you want to grant an IAM user in your AWS account access to one of your Amazon S3 buckets, `examplebucket`. You also want to allow the user to add, update, and delete objects.

In addition to granting the `s3:PutObject`, `s3:GetObject`, and `s3:DeleteObject` permissions to the user, the policy also grants the `s3:ListAllMyBuckets`, `s3:GetBucketLocation`, and `s3:ListBucket` permissions. These are the additional permissions required by the console. Also, the `s3:PutObjectAcl` and the `s3:GetObjectAcl` actions are required to be able to copy, cut, and paste objects in the console. For an example walkthrough that grants permissions to users and tests them using the console, see [An Example Walkthrough: Using user policies to control access to your bucket](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListBucketsInConsole",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets"
      ],
      "Resource": "arn:aws:s3::*:*"
    },
    {
      "Sid": "ViewSpecificBucketInfo",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::examplebucket"
    },
    {
      "Sid": "ManageBucketContents",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:DeleteObject"
      ]
    }
  ]
}
```

```
    ],  
    "Resource": "arn:aws:s3:::examplebucket/*"  
  }  
]  
}
```

## Troubleshooting AWS Application Cost Profiler identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with AWS Application Cost Profiler and AWS Identity and Access Management (IAM).

### Topics

- [I Am Not Authorized to Perform an Action in Application Cost Profiler](#)
- [I Am Not Authorized to Perform iam:PassRole](#)
- [I Want to Allow People Outside of My AWS Account to Access My Application Cost Profiler Resources](#)

### I Am Not Authorized to Perform an Action in Application Cost Profiler

If the AWS Management Console tells you that you're not authorized to perform an action, then you must contact your administrator for assistance. Your administrator is the person that provided you with your sign-in credentials.

The following example error occurs when the mateojackson IAM user tries to use the console to view details about the Application Cost Profiler report but does not have `application-cost-profiler:ListReportDefinitions` permission.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:  
application-cost-profiler:ListReportDefinitions on resource: Report Definition
```

In this case, Mateo asks his administrator to update his policies to allow him to access the report definition resource using the `application-cost-profiler:ListReportDefinitions` action.

### I Am Not Authorized to Perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, your policies must be updated to allow you to pass a role to Application Cost Profiler.

Some AWS services allow you to pass an existing role to that service instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named `marymajor` tries to use the console to perform an action in Application Cost Profiler. However, the action requires the service to have permissions that are granted by a service role. Mary does not have permissions to pass the role to the service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

In this case, Mary's policies must be updated to allow her to perform the `iam:PassRole` action.

If you need help, contact your AWS administrator. Your administrator is the person who provided you with your sign-in credentials.

## I Want to Allow People Outside of My AWS Account to Access My Application Cost Profiler Resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Application Cost Profiler supports these features, see [How AWS Application Cost Profiler works with IAM](#).
- To learn how to provide access to your resources across AWS accounts that you own, see [Providing access to an IAM user in another AWS account that you own](#) in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see [Providing access to AWS accounts owned by third parties](#) in the *IAM User Guide*.
- To learn how to provide access through identity federation, see [Providing access to externally authenticated users \(identity federation\)](#) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see [Cross account resource access in IAM](#) in the *IAM User Guide*.



# Compliance validation for AWS Application Cost Profiler

To learn whether an AWS service is within the scope of specific compliance programs, see [AWS services in Scope by Compliance Program](#) and choose the compliance program that you are interested in. For general information, see [AWS Compliance Programs](#).

You can download third-party audit reports using AWS Artifact. For more information, see [Downloading Reports in AWS Artifact](#).

Your compliance responsibility when using AWS services is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- [Security and Compliance Quick Start Guides](#) – These deployment guides discuss architectural considerations and provide steps for deploying baseline environments on AWS that are security and compliance focused.
- [Architecting for HIPAA Security and Compliance on Amazon Web Services](#) – This whitepaper describes how companies can use AWS to create HIPAA-eligible applications.

## Note

Not all AWS services are HIPAA eligible. For more information, see the [HIPAA Eligible Services Reference](#).

- [AWS Compliance Resources](#) – This collection of workbooks and guides might apply to your industry and location.
- [AWS Customer Compliance Guides](#) – Understand the shared responsibility model through the lens of compliance. The guides summarize the best practices for securing AWS services and map the guidance to security controls across multiple frameworks (including National Institute of Standards and Technology (NIST), Payment Card Industry Security Standards Council (PCI), and International Organization for Standardization (ISO)).
- [Evaluating Resources with Rules](#) in the *AWS Config Developer Guide* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- [AWS Security Hub](#) – This AWS service provides a comprehensive view of your security state within AWS. Security Hub uses security controls to evaluate your AWS resources and to check your

compliance against security industry standards and best practices. For a list of supported services and controls, see [Security Hub controls reference](#).

- [Amazon GuardDuty](#) – This AWS service detects potential threats to your AWS accounts, workloads, containers, and data by monitoring your environment for suspicious and malicious activities. GuardDuty can help you address various compliance requirements, like PCI DSS, by meeting intrusion detection requirements mandated by certain compliance frameworks.
- [AWS Audit Manager](#) – This AWS service helps you continuously audit your AWS usage to simplify how you manage risk and compliance with regulations and industry standards.

## Resilience in AWS Application Cost Profiler

The AWS global infrastructure is built around AWS Regions and Availability Zones. Regions provide multiple physically separated and isolated Availability Zones, which are connected through 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 Application Cost Profiler

As a managed service, AWS Application Cost Profiler 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 Application Cost Profiler 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.

# Monitoring Application Cost Profiler events in EventBridge

You can use Amazon EventBridge to automate your AWS services and respond automatically to system events, such as application availability issues or resource changes. Events from AWS services are delivered to EventBridge in near-real time. You can write simple rules to indicate which events are of interest to you and which automated actions to take when an event matches a rule. For more information, see [Amazon EventBridge User Guide](#).

You can monitor AWS Application Cost Profiler events in EventBridge. EventBridge routes that data to targets such as AWS Lambda and Amazon Simple Notification Service (Amazon SNS). These events are the same as those that appear in Amazon CloudWatch Events, which delivers a near-real-time stream of system events that describe changes in AWS resources.

## Monitor report generation with EventBridge

With EventBridge, you can create rules that define actions to take when Application Cost Profiler sends notification of a report being generated. For example, you can create a rule that sends you an email message each time a report is generated.

### To monitor for report generation

1. Log in to AWS using an account that has permissions to use both EventBridge and Application Cost Profiler.
2. Open the Amazon EventBridge console at <https://console.aws.amazon.com/events/>.
3. Using the following values, create an EventBridge rule that monitors events created when a report is generated:
  - For **Rule type**, choose **Rule with an event pattern**.
  - For **Event source**, choose **Other**.
  - In the **Event pattern** section, choose **Custom patterns (JSON editor)**, and then paste the following event pattern into the text area:

```
{
  "source": ["aws.application-cost-profiler"],
  "detail-type": ["Application Cost Profiler Report Generated"]
}
```

```
}
```

- For **Target types**, choose **AWS service**, and for **Select a target**, choose the AWS service that you want to act when EventBridge detects an event of the selected type. The target is triggered when an event is received that matches the event pattern defined in the rule.

For details about creating rules, see [Creating Amazon EventBridge rules that react to events](#) in the *Amazon EventBridge User Guide*.

## Example of a Report Generated event

This event informs you when a report is generated and ready for you to retrieve. The message field gives you the Amazon Simple Storage Service (Amazon S3) bucket and key for the Amazon S3 object where the report is stored.

```
{
  "version": "0",
  "id": "01234567-EXAMPLE",
  "detail-type": "Application Cost Profiler Report Generated",
  "source": "aws.application-cost-profiler",
  "account": "123456789012",
  "time": "2021-03-31T10:23:43Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "message": "Application Cost Profiler report delivered in bucket: SampleBucket,
key: SampleReport-112233445566"
  }
}
```

## Document history

The following table describes the documentation releases for AWS Application Cost Profiler.

Change	Description	Date
<a href="#">Service deprecation notification</a>	AWS Application Cost Profiler will be discontinued by September 30, 2024 and is no longer accepting new customers.	August 11, 2023
<a href="#">Monitoring events</a>	Due to changes to the EventBridge console, the way that you create rules to monitor Application Cost Profiler events changed. For more information see, <a href="#">Monitoring Application Cost Profiler events in EventBridge</a> .	July 5, 2022
<a href="#">Updates to examples of S3 bucket policies</a>	Documentation-only update to the S3 bucket policy examples. For more information, see <a href="#">Setting up Amazon S3 buckets for Application Cost Profiler</a> .	December 6, 2021
<a href="#">General availability</a>	The initial public release of Application Cost Profiler.	May 13, 2021