
Amazon Simple Storage Service

Console User Guide



Amazon Simple Storage Service: Console User Guide

Copyright © 2020 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

Welcome to the Amazon S3 Console User Guide	1
Changing the console language	2
Creating and configuring a bucket	3
Creating a bucket	3
More info	4
Deleting a bucket	5
More info	5
Emptying a bucket	6
Viewing bucket properties	6
Enabling or disabling versioning	7
Enabling default encryption	7
More info	9
Enabling server access logging	9
Enabling object-level logging	10
More info	11
Configuring static website hosting	11
Step 1: Configuring a bucket for static website hosting	11
Step 2: Editing S3 Block Public Access settings	12
Step 3: Adding a bucket policy	13
Step 4: Testing your website endpoint	14
Redirecting website requests	14
Advanced settings	15
Setting a destination for event notifications	15
Enabling and configuring event notifications	17
Enabling transfer acceleration	19
Access points	20
Creating an Amazon S3 access point	20
Managing and using Amazon S3 access points	21
Navigating to an access point detail page	21
Managing and using a single access point	21
Uploading, downloading, and managing objects	23
Uploading S3 objects	24
Uploading Files and Folders by Using Drag and Drop	25
Uploading Files by Pointing and Clicking	26
More Info	26
Copying objects	27
Moving objects	27
Downloading S3 objects	28
Related topics	29
Deleting objects	29
Undeleting objects	29
More info	30
Restoring archived S3 objects	30
Archive Retrieval Options	30
Restoring an Archived S3 Object	31
Upgrade an In-Progress Restore	31
Checking Archive Restore Status and Expiration Date	32
Locking Amazon S3 objects	32
More info	33
Viewing an overview of an object	33
More info	33
Viewing object versions	33
More info	34
Viewing object properties	34

Adding encryption to an object	35
More info	36
Editing object metadata	36
Editing system-defined metadata	37
Editing user-defined metadata	38
Editing object tags	38
Using folders	39
Creating a folder	40
Deleting folders	40
Making folders public	41
S3 Batch Operations	42
Creating an S3 Batch Operations job	42
More info	42
Managing S3 Batch Operations jobs	43
More info	43
Storage management	44
Creating a lifecycle rule	44
Creating replication rules	46
Adding a replication rule	47
Grant the source bucket owner permission to encrypt using the AWS KMS CMK	49
More info	50
Managing replication rules	50
More info	51
Configuring Storage Class Analysis	51
Configuring Amazon S3 Inventory	52
Destination Bucket Policy	53
Granting Amazon S3 Permission to Use Your AWS KMS CMK for Encryption	54
Creating a request metrics filter for a bucket	55
Creating a request metrics filter using object tags or prefixes	55
Deleting a request metrics filter	56
Viewing replication metrics	57
Setting permissions	58
Blocking public access	59
Access status	59
More info	59
Editing bucket public access settings	60
Editing public access settings for an S3 bucket	60
More info	60
Editing account public access settings	60
More info	61
Setting object permissions	61
More Info	62
Setting ACL bucket permissions	62
More info	64
Adding a bucket policy	64
More info	65
Adding cross-domain resource sharing with CORS	65
More info	66
Setting Object Ownership to bucket owner preferred	66
How do I ensure that I take ownership of new objects?	66
Using Access Analyzer for S3	66
What information does Access Analyzer for S3 provide?	67
Enabling Access Analyzer for S3	68
Blocking all public access	68
Reviewing and changing bucket access	69
Archiving bucket findings	69
Activating an archived bucket finding	70

Viewing finding details	70
Downloading an Access Analyzer for S3 report	71
Document history	72
Earlier updates	72
AWS glossary	75

Welcome to the Amazon S3 Console User Guide

Welcome to the *Amazon Simple Storage Service Console User Guide* for the Amazon Simple Storage Service (Amazon S3) console.

Amazon S3 provides virtually limitless storage on the internet. This guide explains how you can manage buckets, objects, and folders in Amazon S3 by using the AWS Management Console, a browser-based graphical user interface for interacting with AWS services.

For detailed conceptual information about how Amazon S3 works, see [What Is Amazon S3?](#) in the *Amazon Simple Storage Service Developer Guide*. The developer guide also has detailed information about Amazon S3 features and code examples to support those features.

Topics

- [Creating and configuring an S3 bucket \(p. 3\)](#)
- [Uploading, downloading, and managing objects \(p. 23\)](#)
- [Storage management \(p. 44\)](#)
- [Setting bucket and object access permissions \(p. 58\)](#)

How do I change the language of the AWS Management Console?

You can change the display language of the AWS Management Console. Several languages are supported.

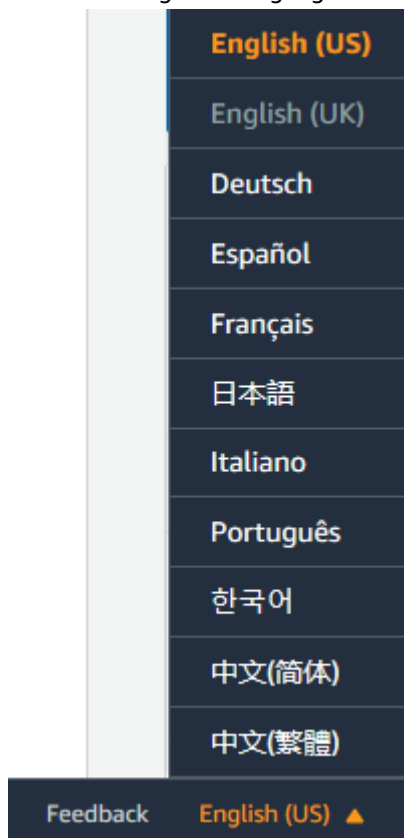
To change the console language

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. On the left-side of the bottom navigation bar, choose the language menu.



3. From the language menu, choose the language that you want.

This will change the language for the entire AWS Management Console.



Creating and configuring an S3 bucket

To upload your data (photos, videos, documents etc.) to Amazon S3, you must first create an S3 bucket in one of the AWS Regions. You can then upload your data objects to the bucket.

Every object you store in Amazon S3 resides in a bucket. You can use buckets to group related objects in the same way that you use a directory to group files in a file system.

Amazon S3 creates buckets in the AWS Region that you specify. You can choose any AWS Region that is geographically close to you to optimize latency, minimize costs, or address regulatory requirements. For example, if you reside in Europe, you might find it advantageous to create buckets in the Europe (Ireland) or Europe (Frankfurt) regions. For a list of Amazon S3 AWS Regions, see [Regions and Endpoints](#) in the *Amazon Web Services General Reference*.

You are not charged for creating a bucket. You are only charged for storing objects in the bucket and for transferring objects out of the bucket. For more information about pricing, see [Amazon Simple Storage Service \(S3\) FAQs](#).

Amazon S3 bucket names are globally unique, regardless of the AWS Region in which you create the bucket. You specify the name at the time you create the bucket. For bucket naming guidelines, see [Bucket Restrictions and Limitations](#) in the *Amazon Simple Storage Service Developer Guide*.

The following topics explain how to use the Amazon S3 console to create, delete, and manage buckets.

Topics

- [How do I create an S3 Bucket? \(p. 3\)](#)
- [How do I delete an S3 Bucket? \(p. 5\)](#)
- [How do I empty an S3 Bucket? \(p. 6\)](#)
- [How do I view the properties for an S3 bucket? \(p. 6\)](#)
- [How do I enable or suspend versioning for an S3 bucket? \(p. 7\)](#)
- [How do I enable default encryption for an Amazon S3 bucket? \(p. 7\)](#)
- [How do I enable server access logging for an S3 bucket? \(p. 9\)](#)
- [How do I enable object-level logging for an S3 bucket with AWS CloudTrail data events? \(p. 10\)](#)
- [How do I configure an S3 bucket for static website hosting? \(p. 11\)](#)
- [How do I redirect requests to an S3 bucket hosted website to another host? \(p. 14\)](#)
- [Advanced settings for S3 bucket properties \(p. 15\)](#)

How do I create an S3 Bucket?

Before you can upload data to Amazon S3, you must create a bucket in one of the AWS Regions to store your data. After you create a bucket, you can upload an unlimited number of data objects to the bucket.

The AWS account that creates the bucket owns it. By default, you can create up to 100 buckets in each of your AWS accounts. If you need additional buckets, you can increase your account bucket quota to a maximum of 1,000 buckets by submitting a service quota increase. For information about how to increase your bucket quota, see [AWS Service Quotas](#) in the *AWS General Reference*.

Buckets have configuration properties, including geographical Region, access settings for the objects in the bucket, and other metadata.

To create a bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Choose **Create bucket**.
3. In **Bucket name**, enter a DNS-compliant name for your bucket.

The bucket name must:

- Be unique across all of Amazon S3.
- Be between 3 and 63 characters long.
- Not contain uppercase characters.
- Start with a lowercase letter or number.

After you create the bucket, you can't change its name. For information about naming buckets, see [Rules for bucket naming](#) in the *Amazon Simple Storage Service Developer Guide*.

Important

Avoid including sensitive information, such as account numbers, in the bucket name. The bucket name is visible in the URLs that point to the objects in the bucket.

4. In **Region**, choose the AWS Region where you want the bucket to reside.

Choose a Region close to you to minimize latency and costs and address regulatory requirements. Objects stored in a Region never leave that Region unless you explicitly transfer them to another Region. For a list of Amazon S3 AWS Regions, see [AWS service endpoints](#) in the *Amazon Web Services General Reference*.

5. In **Bucket settings for Block Public Access**, choose the Block Public Access settings that you want to apply to the bucket.

We recommend that you leave all settings enabled unless you know you need to turn one or more of them off for your use case, such as to host a public website. Block public access settings that you enable for the bucket will also be enabled for all access points that you create on the bucket. For more information about blocking public access, see [Using Amazon S3 Block Public Access](#) in the *Amazon Simple Storage Service Developer Guide*.

6. (Optional) If you want to enable S3 Object Lock:

- a. Choose **Advanced settings**, and read the message that appears.

Important

You can only enable S3 Object Lock for a bucket when you create it. If you enable Object Lock for the bucket, you can't disable it later. Enabling Object Lock also enables versioning for the bucket. After you enable Object Lock for the bucket, you must configure the Object Lock settings before any objects in the bucket will be protected. For more information about configuring protection for objects, see [How do I lock an Amazon S3 object? \(p. 32\)](#).

- b. If you want to enable Object Lock, enter *enable* in the text box and choose **Confirm**.

For more information about the S3 Object Lock feature, see [Locking Objects Using Amazon S3 Object Lock](#) in the *Amazon Simple Storage Service Developer Guide*.

7. Choose **Create bucket**.

More info

- [How do I delete an S3 Bucket? \(p. 5\)](#)

- [How do I set ACL bucket permissions? \(p. 62\)](#)

How do I delete an S3 Bucket?

You can delete an empty bucket, and when you're using the AWS Management Console, you can delete a bucket that contains objects. If you delete a bucket that contains objects, all the objects in the bucket are permanently deleted.

When you delete a bucket with versioning enabled, all versions of all the objects in the bucket are permanently deleted. For more information about versioning, see [Managing Objects in a Versioning-Enabled Bucket](#) in the *Amazon Simple Storage Service Developer Guide*.

Before deleting a bucket, consider the following:

- Bucket names are unique. If you delete a bucket, another AWS user can use the name.
- When you delete a bucket that contains objects, all the objects in the bucket are permanently deleted, including objects that transitioned to the S3 Glacier storage class.
- If the bucket hosts a static website, and you created and configured an Amazon Route 53 hosted zone as described in [Create and Configure Amazon Route 53 Hosted Zone](#): You must clean up the Route 53 hosted zone settings that are related to the bucket as described in [Delete the Route 53 Hosted Zone](#).
- If the bucket receives log data from Elastic Load Balancing (ELB): We recommend that you stop the delivery of ELB logs to the bucket before deleting it. After you delete the bucket, if another user creates a bucket using the same name, your log data could potentially be delivered to that bucket. For information about ELB access logs, see [Access Logs](#) in the *User Guide for Classic Load Balancers* and [Access Logs](#) in the *User Guide for Application Load Balancers*.

Important

If you want to continue to use the same bucket name, don't delete the bucket. We recommend that you empty the bucket and keep it. After a bucket is deleted, the name becomes available to reuse, but the name might not be available for you to reuse for various reasons. For example, it might take some time before the name can be reused, and some other account could create a bucket with that name before you do.

To delete an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, select the option next to the name of the bucket that you want to delete, and then choose **Delete** at the top of the page.
3. On the **Delete bucket** page, confirm that you want to delete the bucket by entering the bucket name into the text field, and then choose **Delete bucket**.

Note

If the bucket contains any objects, empty the bucket before deleting it by selecting the *empty bucket configuration* link in the **This bucket is not empty** error alert and following the instructions on the **Empty bucket** page. Then return to the **Delete bucket** page and delete the bucket.

More info

- [How do I empty an S3 Bucket? \(p. 6\)](#)
- [Deleting objects \(p. 29\)](#)

How do I empty an S3 Bucket?

You can empty a bucket, which deletes all of the objects in the bucket without deleting the bucket. When you empty a bucket with versioning enabled, all versions of all the objects in the bucket are deleted. For more information, see [Managing Objects in a Versioning-Enabled Bucket](#) and [Deleting/Emptying a Bucket](#) in the *Amazon Simple Storage Service Developer Guide*.

To empty an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, select the option next to the name of the bucket that you want to empty, and then choose **Empty**.
3. On the **Empty bucket** page, confirm that you want to empty the bucket by entering **permanently delete** in the text field, and then choose **Empty**.
4. (Optional) Monitor the progress of the bucket emptying process on the **Empty bucket: Status** page.

Warning

This action deletes all objects in the bucket. Wait for the empty bucket action to finish before adding new objects. New objects might be deleted if they are added while the empty bucket action is in progress.

How do I view the properties for an S3 bucket?

You can view and configure the properties for an Amazon S3 bucket, including settings for versioning, tags, default encryption, logging, notifications, and more.

To view the properties for an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want to view the properties for.
3. Choose **Properties**.
4. On the **Properties** page, you can configure the following properties for the bucket.
 - **Bucket Versioning** – Keep multiple versions of an object in one bucket by using versioning. By default, versioning is disabled for a new bucket. For information about enabling versioning, see [How do I enable or suspend versioning for an S3 bucket?](#)
 - **Tags** – With AWS cost allocation, you can use bucket tags to annotate billing for your use of a bucket. A tag is a key-value pair that represents a label that you assign to a bucket. To add tags, choose **Tags**, and then choose **Add tag**. For more information, see [Using cost allocation S3 bucket tags](#).
 - **Default encryption** – Enabling default encryption provides you with automatic server-side encryption. Amazon S3 encrypts an object before saving it to a disk and decrypts the object when you download it. For more information, see [Amazon S3 default encryption for S3 buckets](#).
 - **Server access logging** – Get detailed records for the requests that are made to your bucket with server access logging. By default, Amazon S3 doesn't collect server access logs. For information about enabling server access logging, see [How do I enable server access logging for an S3 bucket? \(p. 9\)](#)
 - **AWS CloudTrail data events** – Use CloudTrail to log data events. By default, trails don't log data events. Additional charges apply for data events. For more information, see [Logging Data Events for Trails](#) in the *AWS CloudTrail User Guide*.

- **Event notifications** – Enable certain Amazon S3 bucket events to send notification messages to a destination whenever the events occur. To enable events, choose **Create event notification**, and then specify the settings you want to use. For more information, see [Enabling and configuring event notifications for an S3 Bucket](#) (p. 17)
- **Transfer acceleration** – Enable fast, easy, and secure transfers of files over long distances between your client and an S3 bucket. For information about enabling transfer acceleration, see [How do I enable transfer acceleration for an S3 bucket?](#) (p. 19)
- **Object Lock** – Use S3 Object Lock to prevent an object from being deleted or overwritten for a fixed amount of time or indefinitely. For more information, see [Locking objects using S3 Object Lock](#).
- **Requester Pays** – Enable Requester Pays if you want the requester (instead of the bucket owner) to pay for requests and data transfers. For more information, see [Requester Pays buckets](#).
- **Static website hosting** – You can host a static website on Amazon S3. To enable static website hosting, choose **Static website hosting**, and then specify the settings you want to use. For more information, see [How do I configure an S3 bucket for static website hosting?](#) (p. 11)

How do I enable or suspend versioning for an S3 bucket?

Versioning enables you to keep multiple versions of an object in one bucket. This section describes how to enable object versioning on a bucket. For more information about versioning support in Amazon S3, see [Object Versioning](#) and [Using Versioning](#) in the *Amazon Simple Storage Service Developer Guide*.

To enable or disable versioning on an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want to enable versioning for.
3. Choose **Properties**.
4. Under **Bucket Versioning**, choose **Edit**.
5. Choose **Suspend** or **Enable**, and then choose **Save changes**.

Note

You can use AWS Multi-Factor Authentication (MFA) with versioning. When you use MFA with versioning, you must provide your AWS account's access keys and a valid code from the account's MFA device in order to permanently delete an object version or suspend or reactivate versioning. To use MFA with versioning, you enable **MFA Delete**. However, you cannot enable **MFA Delete** using the AWS Management Console. You must use the AWS CLI or API. For more information, see [MFA Delete](#).

How do I enable default encryption for an Amazon S3 bucket?

Amazon S3 default encryption provides a way to set the default encryption behavior for an Amazon S3 bucket. You can set default encryption on a bucket so that all objects are encrypted when they are stored in the bucket. The objects are encrypted using server-side encryption with either Amazon S3-managed keys (SSE-S3) or AWS Key Management Service (AWS KMS) customer master keys (CMKs).

When you use server-side encryption, Amazon S3 encrypts an object before saving it to disk in its data centers and decrypts it when you download the objects. For more information about protecting data using server-side encryption and encryption key management, see [Protecting Data Using Server-Side Encryption](#) in the *Amazon Simple Storage Service Developer Guide*.

Default encryption works with all existing and new Amazon S3 buckets. Without default encryption, to encrypt all objects stored in a bucket, you must include encryption information with every object storage request. You must also set up an Amazon S3 bucket policy to reject storage requests that don't include encryption information.

There are no new charges for using default encryption for S3 buckets. Requests to configure the default encryption feature incur standard Amazon S3 request charges. For information about pricing, see [Amazon S3 Pricing](#). For SSE-KMS CMK storage, AWS KMS charges apply and are listed at [AWS KMS Pricing](#).

To enable default encryption on an Amazon S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want.
3. Choose **Properties**.
4. Under **Default encryption**, choose **Edit**.
5. To enable or disable server-side encryption, choose **Enable** or **Disable**.
6. To enable server-side encryption using an Amazon S3-managed key, under **Encryption key type**, choose **Amazon S3 key (SSE-S3)**.

For more information about using Amazon S3 server-side encryption to encrypt your data, see [Protecting Data with Amazon S3-Managed Encryption Keys](#) in the *Amazon Simple Storage Service Developer Guide*.

Important

You might need to update your bucket policy when enabling default encryption. For more information, see [Moving to Default Encryption from Using Bucket Policies for Encryption Enforcement](#) in the *Amazon Simple Storage Service Developer Guide*.

7. To enable server-side encryption using an AWS KMS CMK, follow these steps:
 - a. Under **Encryption key type**, choose **AWS Key Management Service key (SSE-KMS)**.

Important

If you use the AWS KMS option for your default encryption configuration, you are subject to the RPS (requests per second) limits of AWS KMS. For more information about AWS KMS limits and how to request a limit increase, see [AWS KMS limits](#).

- b. Under **AWS KMS key** choose one of the following:
 - **AWS managed key (aws/s3)**
 - **Choose from your KMS master keys**, and choose your **KMS master key**.
 - **Enter KMS master key ARN**, and enter your AWS KMS key ARN.

Important

You can only use KMS CMKs that are enabled in the same AWS Region as the bucket. When you choose **Choose from your KMS master keys**, the S3 console only lists 100 KMS CMKs per Region. If you have more than 100 CMKs in the same Region, you can only see the first 100 CMKs in the S3 console. To use a KMS CMK that is not listed in the console, choose **Custom KMS ARN**, and enter the KMS CMK ARN.

When you use an AWS KMS CMK for server-side encryption in Amazon S3, you must choose a symmetric CMK. Amazon S3 only supports symmetric CMKs and not

asymmetric CMKs. For more information, see [Using Symmetric and Asymmetric Keys](#) in the *AWS Key Management Service Developer Guide*.

For more information about creating an AWS KMS CMK, see [Creating Keys](#) in the *AWS Key Management Service Developer Guide*. For more information about using AWS KMS with Amazon S3, see [Protecting Data with Keys Stored in AWS KMS](#) in the *Amazon Simple Storage Service Developer Guide*.

8. Choose **Save changes**.

More info

- [Amazon S3 Default Encryption for S3 Buckets](#) in the *Amazon Simple Storage Service Developer Guide*
- [How do I add encryption to an S3 object?](#) (p. 35)

How do I enable server access logging for an S3 bucket?

This topic describes how to enable server access logging for an Amazon S3 bucket using the AWS Management Console. For information about how to enable logging programmatically and details about how logs are delivered, see [Server Access Logging](#) in the *Amazon Simple Storage Service Developer Guide*.

By default, Amazon Simple Storage Service (Amazon S3) doesn't collect server access logs. When you enable logging, Amazon S3 delivers access logs for a source bucket to a target bucket that you choose. The target bucket must be in the same AWS Region as the source bucket and must not have a default retention period configuration.

Server access logging provides detailed records for the requests that are made to an S3 bucket. Server access logs are useful for many applications. For example, access log information can be useful in security and access audits. It can also help you learn about your customer base and understand your Amazon S3 bill.

An access log record contains details about the requests that are made to a bucket. This information can include the request type, the resources that are specified in the request, and the time and date that the request was processed. For more information, see [Server Access Log Format](#) in the *Amazon Simple Storage Service Developer Guide*.

Important

There is no extra charge for enabling server access logging on an Amazon S3 bucket. However, any log files that the system delivers to you will accrue the usual charges for storage. (You can delete the log files at any time.) We do not assess data transfer charges for log file delivery, but we do charge the normal data transfer rate for accessing the log files.

To enable server access logging for an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want to enable server access logging for.
3. Choose **Properties**.
4. In the **Server access logging** section, choose **Edit**.
5. Under **Server access logging**, select **Enable**. For **Target bucket**, enter the name of the bucket that you want to receive the log record objects. The target bucket must be in the same Region as the source bucket and must not have a default retention period configuration.

6. Choose **Save changes**.

You can view the logs in the target bucket. After you enable server access logging, it might take a few hours before the logs are delivered to the target bucket. For more information about how and when logs are delivered, see [Server Access Logging](#) in the *Amazon Simple Storage Service Developer Guide*.

More Info

[How do I view the properties for an S3 bucket? \(p. 6\)](#)

How do I enable object-level logging for an S3 bucket with AWS CloudTrail data events?

This section describes how to enable an AWS CloudTrail trail to log data events for objects in an S3 bucket by using the Amazon S3 console. CloudTrail supports logging Amazon S3 object-level API operations such as `GetObject`, `DeleteObject`, and `PutObject`. These events are called data events. By default, CloudTrail trails don't log data events, but you can configure trails to log data events for S3 buckets that you specify, or to log data events for all the Amazon S3 buckets in your AWS account. For more information, see [Logging Amazon S3 API Calls Using AWS CloudTrail](#). CloudTrail does not populate data events in the CloudTrail event history. Additionally, not all bucket-level actions are populated in the CloudTrail event history. For more information, see [Using Amazon CloudWatch Logs filter patterns and Amazon Athena to query CloudTrail logs](#).

To configure a trail to log data events for an S3 bucket, you can use either the AWS CloudTrail console or the Amazon S3 console. If you are configuring a trail to log data events for all the Amazon S3 buckets in your AWS account, it's easier to use the CloudTrail console. For information about using the CloudTrail console to configure a trail to log S3 data events, see [Data Events](#) in the *AWS CloudTrail User Guide*.

Important

Additional charges apply for data events. For more information, see [AWS CloudTrail Pricing](#).

The following procedure shows how to use the Amazon S3 console to enable a CloudTrail trail to log data events for an S3 bucket.

To enable CloudTrail data events logging for objects in an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket.
3. Choose **Properties**.
4. Under **AWS CloudTrail data events**, choose **Configure in CloudTrail**. For information about how to create trails in the CloudTrail console, see [Creating a Trail with the Console](#) in the *AWS CloudTrail User Guide*.
5. To disable object-level logging for the bucket, you must go to the CloudTrail console and remove the bucket name from the trail's **Data events**.

Note

If you use the CloudTrail console or the Amazon S3 console to configure a trail to log data events for an S3 bucket, the Amazon S3 console shows that object-level logging is enabled for the bucket.

For information about enabling object-level logging when you create an S3 bucket, see [How do I create an S3 Bucket? \(p. 3\)](#).

More info

- [How do I view the properties for an S3 bucket? \(p. 6\)](#)
- [Logging Amazon S3 API Calls By Using AWS CloudTrail](#) in the *Amazon Simple Storage Service Developer Guide*
- [Working with CloudTrail Log Files](#) in the *AWS CloudTrail User Guide*

How do I configure an S3 bucket for static website hosting?

You can host a static website on Amazon S3. On a static website, individual webpages include static content. A static website might also contain client-side scripts. By contrast, a dynamic website relies on server-side processing, including server-side scripts such as PHP, JSP, or ASP.NET. Amazon S3 does not support server-side scripting.

You can use the following quick procedures to configure an S3 bucket for static website hosting in the Amazon S3 console. For more information, see [Hosting a Static Website on Amazon S3](#) in the *Amazon Simple Storage Service Developer Guide*. For information about configuring a static website with a custom domain, see [Configuring a static website using a custom domain registered with Route 53](#) in the *Amazon Simple Storage Service Developer Guide*.

Topics

- [Step 1: Configuring a bucket for static website hosting \(p. 11\)](#)
- [Step 2: Editing S3 Block Public Access settings \(p. 12\)](#)
- [Step 3: Adding a bucket policy \(p. 13\)](#)
- [Step 4: Testing your website endpoint \(p. 14\)](#)

Step 1: Configuring a bucket for static website hosting

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want to use to host a static website.
3. Choose **Properties**.
4. Under **Static website hosting**, choose **Edit**.
5. Choose **Use this bucket to host a website**.
6. Under **Static website hosting**, choose **Enable**.
7. In **Index document**, enter the file name of the index document, typically `index.html`.

The index document name is case sensitive and must exactly match the file name of the HTML index document that you plan to upload to your S3 bucket. When you configure a bucket for website hosting, you must specify an index document. Amazon S3 returns this index document when requests are made to the root domain or any of the subfolders. For more information, see [Configuring an index document](#) in the *Amazon Simple Storage Service Developer Guide*.

8. (Optional) If you want to provide your own custom error document for 4XX class errors, in **Error document**, enter the custom error document file name.

The error document name is case sensitive and must exactly match the file name of the HTML error document that you plan to upload to your S3 bucket. If you don't specify a custom error document and an error occurs, Amazon S3 returns a default HTML error document. For more information, see [Configuring a custom error document](#) in the *Amazon Simple Storage Service Developer Guide*.

9. (Optional) If you want to specify advanced redirection rules, in **Redirection rules**, enter XML to describe the rules.

For example, you can conditionally route requests according to specific object key names or prefixes in the request. For more information, see [Configuring advanced conditional redirects](#) in the *Amazon Simple Storage Service Developer Guide*.

10. Choose **Save changes**.

Amazon S3 enables static website hosting for your bucket. At the bottom of the page, under **Static website hosting**, you see the website endpoint for your bucket.

11. Upload the index document to your bucket.

For step-by-step instructions on uploading an object to an S3 bucket, see [Uploading Files by Pointing and Clicking](#) (p. 26).

12. Upload other files for your website, including optional custom error documents.

In the next section, you set the permissions required to access your bucket as a static website.

Step 2: Editing S3 Block Public Access settings

By default, Amazon S3 blocks public access to your account and buckets. If you want to use a bucket to host a static website, you can use these steps to edit your block public access settings.

Warning


Before you complete this step, review [Using Amazon S3 Block Public Access](#) to ensure that you understand and accept the risks involved with allowing public access. When you turn off block public access settings to make your bucket public, anyone on the internet can access your bucket. We recommend that you block all public access to your buckets.

1. Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Choose the name of the bucket that you have configured as a static website.
3. Choose **Permissions**.
4. Under **Block public access (bucket settings)**, choose **Edit**.
5. Clear **Block all public access**, and choose **Save changes**.

Warning

Before you complete this step, review [Using Amazon S3 Block Public Access](#) to ensure you understand and accept the risks involved with allowing public access. When you turn off block public access settings to make your bucket public, anyone on the internet can access your bucket. We recommend that you block all public access to your buckets.

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#) 



Account settings for Block Public Access are currently turned on

Account settings for Block Public Access that are enabled apply even if they are disabled for this bucket.

☐ **Block *all* public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☐ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☐ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**

S3 will ignore all ACLs that grant public access to buckets and objects.

☐ **Block public access to buckets and objects granted through *new* public bucket or access point policies**

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

☐ **Block public and cross-account access to buckets and objects through *any* public bucket or access point policies**

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Amazon S3 turns off Block Public Access settings for your bucket. To create a public, static website, you might also have to [edit the Block Public Access settings](#) for your account before adding a bucket policy. If account settings for Block Public Access are currently turned on, you see a note under **Block public access (bucket settings)**.

Step 3: Adding a bucket policy

After you edit S3 Block Public Access settings, you can add a bucket policy to grant public read access to your bucket. When you grant public read access, anyone on the internet can access your bucket.

Important

The following policy is an example only and allows full access to the contents of your bucket. Before you proceed with this step, review [How can I secure the files in my Amazon S3 bucket?](#) to ensure that you understand the best practices for securing the files in your S3 bucket and risks involved in granting public access.

1. Under **Buckets**, choose the name of your bucket.
2. Choose **Permissions**.
3. Under **Bucket Policy**, choose **Edit**.
4. To grant public read access for your website, copy the following bucket policy, and paste it in the **Bucket policy editor**.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": "*",
```

```
{
  "Action": [
    "s3:GetObject"
  ],
  "Resource": [
    "arn:aws:s3:::example.com/*"
  ]
}
```

5. Update the Resource to your bucket name.

In the preceding example bucket policy, `example.com` is the bucket name. To use this bucket policy with your own bucket, you must update this name to match your bucket name.

6. Choose **Save changes**.

A message appears indicating that the bucket policy has been successfully added.

If you see an error that says `Policy has invalid resource`, confirm that the bucket name in the bucket policy matches your bucket name. For information about adding a bucket policy, see [How do I add an S3 bucket policy?](#)

If you get an error message and cannot save the bucket policy, check your account and bucket Block Public Access settings to confirm that you allow public access to the bucket.

After you edit S3 Block Public Access settings, you can add a bucket policy to grant public read access to your bucket. When you grant public read access, anyone on the internet can access your bucket.

Important

The following policy is an example only and allows full access to the contents of your bucket. Before you proceed with this step, review [How can I secure the files in my Amazon S3 bucket?](#) to ensure that you understand the best practices for securing the files in your S3 bucket and risks involved in granting public access.

Step 4: Testing your website endpoint

After you configure your bucket as a static website and set permissions, you can access your website through an Amazon S3 website endpoint. For more information, see [Website endpoints](#) in the *Amazon Simple Storage Service Developer Guide*. For a complete list of Amazon S3 website endpoints, see [Amazon S3 Website Endpoints](#) in the *Amazon Web Services General Reference*.

1. Under **Buckets**, choose the name of your bucket.
2. Choose **Properties**.
3. At the bottom of the page, under **Static website hosting**, choose your **Bucket website endpoint**.

Your index document opens in a separate browser window.

How do I redirect requests to an S3 bucket hosted website to another host?

For more detailed information about configuring a redirect in Amazon S3, see [Configuring a webpage redirect](#) in the *Amazon Simple Storage Service Developer Guide*.

You can redirect all requests for a website endpoint for a bucket to another host. If you redirect all requests, any request made to the website endpoint is redirected to the specified host name.

For example, if your root domain is `example.com`, and you want to serve requests for both `http://example.com` and `http://www.example.com`, you can create two buckets named `example.com` and `www.example.com`. Then, maintain the content in the `example.com` bucket, and configure the other `www.example.com` bucket to redirect all requests to the `example.com` bucket. For more information, see [Configuring a Static Website Using a Custom Domain Name](#).

To redirect requests for a bucket website endpoint

1. Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Under **Buckets**, choose the name of the bucket that you want to redirect requests from (for example, `www.example.com`).
3. Choose **Properties**.
4. Under **Static website hosting**, choose **Edit**.
5. Choose **Redirect requests for an object**.
6. In the **Host name** box, enter the website endpoint for your bucket or your custom domain.

For example, if you are redirecting to a root domain address, you would enter `example.com`.

7. For **Protocol**, choose the protocol for the redirected requests (**none**, **http**, or **https**).

If you do not specify a protocol, the default option is **none**.

8. Choose **Save changes**.

Advanced settings for S3 bucket properties

This section describes how to configure advanced S3 bucket property settings for object replication, event notification, and transfer acceleration.

Topics

- [Setting a destination to receive Amazon S3 event notifications \(p. 15\)](#)
- [Enabling and configuring event notifications for an S3 Bucket \(p. 17\)](#)
- [How do I enable transfer acceleration for an S3 bucket? \(p. 19\)](#)

Setting a destination to receive Amazon S3 event notifications

Before you can enable event notifications for your bucket you must set up one of the following destination types.

Destination types

- [Amazon SNS topic \(p. 15\)](#)
- [Amazon SQS queue \(p. 16\)](#)
- [Lambda function \(p. 17\)](#)

Amazon SNS topic

Amazon Simple Notification Service (Amazon SNS) is a web service that coordinates and manages the delivery or sending of messages to subscribing endpoints or clients. You can use the Amazon SNS console to create an Amazon SNS topic that your notifications can be sent to. The Amazon SNS topic must be in the same region as your Amazon S3 bucket. For information about creating an Amazon SNS topic, see [Getting Started](#) in the *Amazon Simple Notification Service Developer Guide* and the [SNS FAQ](#).

Before you can use the Amazon SNS topic that you create as an event notification destination, you need the following:

- The Amazon Resource Name (ARN) for the Amazon SNS topic
- A valid Amazon SNS topic subscription (the topic subscribers are notified when a message is published to your Amazon SNS topic)
- A permissions policy that you set up in the Amazon SNS console (as shown in the following example)

```
{
  "Version": "2012-10-17",
  "Id": "__example_policy_ID",
  "Statement": [
    {
      "Sid": "example-statement-ID",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-number:topic-name",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:s3::bucket-name"
        }
      }
    }
  ]
}
```

Amazon SQS queue

Amazon Simple Queue Service (Amazon SQS) offers reliable and scalable hosted queues for storing messages as they travel between computers. You can use the Amazon SQS console to create an Amazon SQS queue that your notifications can be sent to. The Amazon SQS queue must be in the same region as your Amazon S3 bucket. For information about creating an Amazon SQS queue, see [What is Amazon Simple Queue Service](#) and [Getting Started with Amazon SQS](#) in the *Amazon Simple Queue Service Developer Guide*.

Before you can use the Amazon SQS queue as an event notification destination, you need the following:

- The Amazon Resource Name (ARN) for the Amazon SQS topic
- A permissions policy that you set up in the Amazon SQS console (as shown in the following example)

```
{
  "Version": "2012-10-17",
  "Id": "__example_policy_ID",
  "Statement": [
    {
      "Sid": "example-statement-ID",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "SQS:*",
      "Resource": "arn:aws:sqs:region:account-number:queue-name",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:s3::bucket-name"
        }
      }
    }
  ]
}
```

Lambda function

You can use the AWS Lambda console to create a Lambda function that uses the AWS infrastructure to run the code on your behalf. The Lambda function must be in the same region as your S3 bucket. You must also have the name or the ARN of a Lambda function to set up the Lambda function as a event notification destination.

Warning

If your notification ends up writing to the bucket that triggers the notification, this could cause an execution loop. For example, if the bucket triggers a Lambda function each time an object is uploaded, and the function uploads an object to the bucket, then the function indirectly triggers itself. To avoid this, use two buckets, or configure the trigger to only apply to a prefix used for incoming objects.

For more information and an example of using Amazon S3 notifications with AWS Lambda, see [Using AWS Lambda with Amazon S3](#) in the *AWS Lambda Developer Guide*.

For more information about granting the Amazon S3 the permissions required to publish event notifications to a destination, see [Granting Permissions to Publish Event Notification Messages to a Destination](#) in the *Amazon S3 Developer Guide*.

Enabling and configuring event notifications for an S3 Bucket

You can enable certain Amazon S3 events to send a notification message to a destination whenever the events occur. This section explains how to use the Amazon S3 console to enable event notifications. For information about using event notifications with the AWS SDKs and the Amazon S3 REST APIs, see [Configuring Amazon S3 Event Notifications](#) in the *Amazon Simple Storage Service Developer Guide*.

Topics

- [Event notification types \(p. 17\)](#)
- [Enabling and configuring event notifications \(p. 18\)](#)

Event notification types

When you configure event notifications for a bucket, you must specify the type of events for which you want to receive notifications. For a complete list of event types, see [Supported Event Types](#) section in the *Amazon Simple Storage Service Developer Guide*.

In the Amazon S3 console, you have the following options for configuring event notifications. You can choose a single option or multiple options.

- **Object creation**
 - **All object create events** – Receive a notification when an object is created in your bucket by any of the following object creation actions: **Put**, **Post**, **Copy**, and **Multipart upload completed**.
 - **Put, Post, Copy, and Multipart upload completed** – Receive a notification for one of these specific object creation actions.
- **Object deletion**
 - **All object delete events** – Receive a notification any time an object in your bucket is deleted.
 - **Delete marker created** – Receive a notification when a delete marker is created for a versioned object.
- **Object restoration from S3 Glacier or S3 Glacier Deep Archive storage class**

For information about deleting versioned objects, see [Deleting Object Versions](#). For information about object versioning, see [Object Versioning](#) and [Using Versioning](#).

- **Restore initiated** – Receive a notification for *Initiation* of object restoration.
- **Restore completed** – Receive a notification for *Completion* of object restoration.
- **Reduced Redundancy Storage (RRS) object lost events**
 - **Object in RSS Lost** – Receive a notification that an object of the RRS storage class has been lost
- **Objects eligible for replication using Amazon S3 Replication Time Control**
 - **Replication time missed threshold** – Receive a notification that an object exceeded the 15-minute threshold for replication.
 - **Replication time completed after threshold** – Receive a notification that an object replicated after the 15-minute threshold.
 - **Replication time not tracked** – Receive a notification that an object that was eligible for replication is no longer being tracked by replication metrics.
 - **Replication time failed** – Receive a notification that an object failed to replicate.

Note

When you delete the last object from a folder, Amazon S3 can generate an object creation event. When there are multiple objects with the same prefix with a trailing slash (/) as part of their names, those objects are shown as being part of a folder in the Amazon S3 console. The name of the folder is formed from the characters preceding the trailing slash (/). When you delete all the objects listed under that folder, no actual object is available to represent the empty folder. Under such circumstances, the Amazon S3 console creates a zero-byte object to represent that folder. If you enabled event notification for the creation of objects, the zero-byte object creation action that is taken by the console triggers an object creation event.

The Amazon S3 console displays a folder under the following circumstances:

- When a zero-byte object has a trailing slash (/) in its name. In this case, there is an actual Amazon S3 object of 0 bytes that represents a folder.
- If the object has a slash (/) within its name. In this case, there isn't an actual object representing the folder.

Enabling and configuring event notifications

Before you can enable event notifications for your bucket, you must set up one of the destination types. For more information, see [Setting a destination to receive Amazon S3 event notifications \(p. 15\)](#)

To enable and configure event notifications for an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want to enable events for.
3. Navigate to the **Event Notifications** section and choose **Create event notification**.
4. In the **General configuration** section, specify descriptive event name for your event notification. Optionally, you can also specify a prefix and a suffix to limit the notifications to objects with keys ending in the specified characters.
 - a. Enter a description for the **Event name**.

If you don't enter a name, a Globally Unique Identifier (GUID) will be generated and used for the name.
 - b. To optionally filter event notifications by prefix, enter a **Prefix**.

For example, you can set up a prefix filter so that you receive notifications only when files are added to a specific folder (for example, `images/`).

- c. To optionally filter event notifications by suffix, enter a **Suffix**.

For more information, see [Configuring Notifications with Object Key Name Filtering](#).

5. In the **Event types** section, select one or more event types for which you want to receive notifications.

For a listing of the event types, see [Event notification types \(p. 17\)](#).

6. In the **Destination** section, choose the event notification destination.

Note

Before you can publish event notifications, you must grant the Amazon S3 principal the necessary permissions to call the relevant API to publish notifications to a Lambda function, SNS topic, or SQS queue.

- a. Select the destination type: **Lambda Function**, **SNS Topic**, or **SQS Queue**.
- b. After you choose your destination type, choose a function, topic, or queue from the dropdown list.
- c. Alternatively, if you would prefer to specify an Amazon Resource Name (ARN), select **Enter ARN** and enter the ARN.

For more information, see [Setting a destination to receive Amazon S3 event notifications \(p. 15\)](#).

7. Choose **Save changes** and Amazon S3 sends a test message to the event notification destination.

For more information, see [Configuring Amazon S3 event notifications](#) in the *Amazon Simple Storage Service Developer Guide*.

How do I enable transfer acceleration for an S3 bucket?

Amazon Simple Storage Service (Amazon S3) transfer acceleration enables fast, easy, and secure file transfers between your client and an S3 bucket over long distances. This topic describes how to enable Amazon S3 transfer acceleration for a bucket. For more information, see [Amazon S3 Transfer Acceleration](#) in the *Amazon Simple Storage Service Developer Guide*.

Note

If you want to compare accelerated and non-accelerated upload speeds, open the [Amazon S3 Transfer Acceleration Speed Comparison tool](#).

The Speed Comparison tool uses multipart upload to transfer a file from your browser to various AWS Regions with and without Amazon S3 transfer acceleration. You can compare the upload speed for direct uploads and transfer accelerated uploads by Region.

To enable transfer acceleration for an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want to enable transfer acceleration for.
3. Choose **Properties**.
4. Under **Transfer acceleration**, choose **Edit**.
5. Choose **Enable**, and choose **Save changes**.

Amazon S3 enables transfer acceleration for your bucket and displays the **Properties** tab for your bucket. Under **Transfer acceleration**, **Accelerated endpoint** displays the transfer acceleration endpoint for your bucket. You use this endpoint to access accelerated data transfers to and from your bucket. If you suspend transfer acceleration, the accelerate endpoint no longer works.

Introduction to Amazon S3 access points

You can use Amazon S3 access points to manage access to your S3 objects. Amazon S3 access points are named network endpoints that are attached to buckets that you can use to perform S3 object operations, such as uploading and retrieving objects. A bucket can have up to 1,000 access points attached, and each access point enforces distinct permissions and network controls to give you fine-grained control over access to your S3 objects.

For more information about Amazon S3 Access Points, see [Managing Data Access with Amazon S3 Access Points](#) in the *Amazon Simple Storage Service Developer Guide*.

The following topics explain how to use the S3 Management Console to create, manage, and use Amazon S3 Access Points.

Topics

- [Creating an Amazon S3 access point](#) (p. 20)
- [Managing and using Amazon S3 access points](#) (p. 21)

Creating an Amazon S3 access point

This section explains how to create an Amazon S3 access point using the AWS Management Console. For information about creating access points using the AWS CLI, AWS SDKs, and the Amazon S3 REST APIs, see [Managing Data Access with Amazon S3 Access Points](#) in the *Amazon Simple Storage Service Developer Guide*.

An access point is associated with exactly one Amazon S3 bucket. Before you begin, make sure that you have created a bucket that you want to use with this access point. For more information about creating buckets, see [Creating and configuring an S3 bucket](#) (p. 3).

To create an access point

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the navigation pane on the left side of the console, choose **Access points**.
3. On the access points page, choose **Create access point**.
4. In the **Access point name** field, enter your desired name for the access point. For more information about naming access points, see [Rules for naming Amazon S3 access points](#) in the *Amazon Simple Storage Service Developer Guide*.
5. In the **Bucket name** field, enter the name of a bucket in your account to which you want to attach the access point, for example `DOC-EXAMPLE-BUCKET1`. Optionally, you can choose **Browse S3** to browse and search buckets in your account. If you choose **Browse S3**, select the desired bucket and choose **Choose path** to populate the **Bucket name** field with that bucket's name.
6. (Optional) Choose **View** to view the contents of the specified bucket in a new browser window.
7. Select a **Network origin**. If you choose **Virtual private cloud (VPC)**, enter the **VPC ID** that you want to use with the access point.

For more information about network origins for access points, see [Creating Access Points Restricted to a Virtual Private Cloud](#) in the *Amazon Simple Storage Service Developer Guide*.

8. Under **Access point settings for Block Public Access**, select the block public access settings that you want to apply to the access point. All block public access settings are enabled by default for new access points, and we recommend that you leave all settings enabled unless you know you have a specific need to disable any of them. Amazon S3 currently doesn't support changing an access point's block public access settings after the access point has been created.

For more information about using Amazon S3 Block Public Access with access points, see [Managing Public Access to Access Points](#) in the *Amazon Simple Storage Service Developer Guide*.

9. (Optional) Under **Access point policy - optional**, specify the access point policy. For more information about specifying an access point policy, see [Access point policy examples](#) in the *Amazon Simple Storage Service Developer Guide*.
10. Choose **Create access point**.

Managing and using Amazon S3 access points

This section explains how to manage and use your Amazon S3 access points using the AWS Management Console. Before you begin, navigate to the detail page for the access point you want to manage or use, as described in the following procedure.

Navigating to an access point detail page

Option 1: List all access points for your account

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the navigation pane on the left side of the console, choose **Access points**.
3. On the **Access points** page, under **Access points**, select the AWS Region that contains the access points you want to list.
4. (Optional) Search for access points by name by entering a name into the text field next to the Region dropdown menu.
5. Choose the name of the access point you want to manage or use.

Option 2: List all access points for a single bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the navigation pane on the left side of the console, choose **Buckets**.
3. On the **Buckets** page, select the name of the bucket whose access points you want to list.
4. On the bucket detail page, choose the **Access points** tab.
5. Choose the name of the access point you want to manage or use.

Managing and using a single access point

View an access point's configuration details

1. Navigate to the access point detail page for the access point whose details you want to view, as described in [Navigating to an access point detail page](#) (p. 21).
2. Under **Access point overview**, view configuration details and properties for the selected access point.

Use an access point to access your bucket

1. Navigate to the access point detail page for the access point you want to use, as described in [Navigating to an access point detail page \(p. 21\)](#).
2. Under the **Objects** tab, choose the name of an object or objects that you want to access through the access point. On the object operation pages, the console displays a label above the name of your bucket that shows the access point that you're currently using. While you're using the access point, you can only perform the object operations that are allowed by the access point permissions.

Note

- The console view always shows all objects in the bucket. Using an access point as described in this procedure restricts the operations you can perform on those objects, but not whether you can see that they exist in the bucket.
- The S3 Management Console doesn't support using virtual private cloud (VPC) access points to access bucket resources. To access bucket resources from a VPC access point, use the AWS CLI, AWS SDKs, or Amazon S3 REST APIs.

View an access point's settings for Block Public Access

1. Navigate to the access point detail page for the access point whose settings you want to view, as described in [Navigating to an access point detail page \(p. 21\)](#).
2. Choose **Permissions**.
3. Under **Access point policy**, review the access point's Block Public Access settings.

Note

You can't change the Block Public Access settings for an access point after the access point is created.

Edit an access point policy

1. Navigate to the access point detail page for the access point whose policy you want to edit, as described in [Navigating to an access point detail page \(p. 21\)](#).
2. Choose **Permissions**.
3. Under **Access point policy**, choose **Edit**.
4. Enter the access point policy in the text field. The console automatically displays the Amazon Resource Name (ARN) for the access point, which you can use in the policy.
5. Choose **Save**.

Delete an access point

1. Navigate to the list of access points for your account or for a specific bucket, as described in [Navigating to an access point detail page \(p. 21\)](#).
2. Select the option button next to the name of the access point that you want to delete.
3. Choose **Delete**.
4. Confirm that you want to delete your access point by entering its name in the text field that appears, and choose **Delete**.

Uploading, downloading, and managing objects

To upload your data (photos, videos, documents etc.) to Amazon S3, you must first create an S3 bucket in one of the AWS Regions. You can then upload an unlimited number of data objects to the bucket.

The data that you store in Amazon S3 consists of objects. Every object resides within a bucket that you create in a specific AWS Region. Every object that you store in Amazon S3 resides in a bucket.

Objects stored in a region never leave the region unless you explicitly transfer them to another region. For example, objects stored in the Europe (Ireland) region never leave it. The objects stored in an AWS region physically remain in that region. Amazon S3 does not keep copies of objects or move them to any other region. However, you can access the objects from anywhere, as long as you have necessary permissions to do so.

Before you can upload an object into Amazon S3, you must have write permissions to a bucket.

Objects can be any file type: images, backups, data, movies, etc. You can have an unlimited number of objects in a bucket. The maximum size of file you can upload by using the Amazon S3 console is 160 GB. To upload a file larger than 160 GB, use the AWS CLI, AWS SDK, or Amazon S3 REST API. For more information, see [Uploading Objects](#) in the *Amazon Simple Storage Service Developer Guide*.

The following topics explain how to use the Amazon S3 console to upload, delete, and manage objects.

Note

If you rename an object, or change any of the properties; **Storage Class**, **Encryption**, **Metadata**, a new object is created to replace the old one. If S3 Versioning is enabled, a new version of the object is created, and the existing object becomes an older version. The role that changes the property also becomes the owner of the new object or (object version).

Topics

- [How do I upload files and folders to an S3 bucket? \(p. 24\)](#)
- [Copying objects \(p. 27\)](#)
- [Moving objects \(p. 27\)](#)
- [How do I download an object from an S3 bucket? \(p. 28\)](#)
- [Deleting objects \(p. 29\)](#)
- [How do I undelete a deleted S3 object? \(p. 29\)](#)
- [How do I restore an S3 object that has been archived? \(p. 30\)](#)
- [How do I lock an Amazon S3 object? \(p. 32\)](#)
- [How do I see an overview of an object? \(p. 33\)](#)
- [How do I see the versions of an S3 object? \(p. 33\)](#)
- [How do I view the properties of an object? \(p. 34\)](#)
- [How do I add encryption to an S3 object? \(p. 35\)](#)
- [Editing object metadata \(p. 36\)](#)

- [Editing object tags \(p. 38\)](#)
- [How do I use folders in an S3 bucket? \(p. 39\)](#)

How do I upload files and folders to an S3 bucket?

This topic explains how to use the AWS Management Console to upload one or more files or entire folders to an Amazon S3 bucket. Before you can upload files and folders to an Amazon S3 bucket, you need write permissions for the bucket. For more information about access permissions, see [Setting bucket and object access permissions \(p. 58\)](#). For information about uploading files programmatically, see [Uploading Objects](#) in the *Amazon Simple Storage Service Developer Guide*.

When you upload a file to Amazon S3, it is stored as an S3 object. Objects consist of the file data and metadata that describes the object. You can have an unlimited number of objects in a bucket.

You can upload any file type—images, backups, data, movies, etc.—into an S3 bucket. The maximum size of a file that you can upload by using the Amazon S3 console is 160 GB. To upload a file larger than 160 GB, use the AWS CLI, AWS SDK, or Amazon S3 REST API. For more information, see [Uploading Objects](#) in the *Amazon Simple Storage Service Developer Guide*.

Note

To upload *folders*, you must drag and drop them. To upload *files*, you can drag and drop or point and click. Drag and drop functionality is supported only for Chrome and Firefox browsers.

For information about which Chrome and Firefox browser versions are supported, see [What browsers are supported for use with the AWS Management Console?](#)

When you upload a folder, Amazon S3 uploads all of the files and subfolders from the specified folder to your bucket. It then assigns an object key name that is a combination of the uploaded file name and the folder name. For example, if you upload a folder called `/images` that contains two files, `sample1.jpg` and `sample2.jpg`, Amazon S3 uploads the files and then assigns the corresponding key names, `images/sample1.jpg` and `images/sample2.jpg`. The key names include the folder name as a prefix. The Amazon S3 console displays only the part of the key name that follows the last `/`. For example, within an `images` folder the `images/sample1.jpg` and `images/sample2.jpg` objects are displayed as `sample1.jpg` and a `sample2.jpg`.

If you upload individual files and you have a folder open in the Amazon S3 console, when Amazon S3 uploads the files, it includes the name of the open folder as the prefix of the key names. For example, if you have a folder named `backup` open in the Amazon S3 console and you upload a file named `sample1.jpg`, the key name is `backup/sample1.jpg`. However, the object is displayed in the console as `sample1.jpg` in the `backup` folder.

If you upload individual files and you do not have a folder open in the Amazon S3 console, when Amazon S3 uploads the files, it assigns only the file name as the key name. For example, if you upload a file named `sample1.jpg`, the key name is `sample1.jpg`. For more information on key names, see [Object Key and Metadata](#) in the *Amazon Simple Storage Service Developer Guide*.

If you upload an object with a key name that already exists in a versioning-enabled bucket, Amazon S3 creates another version of the object instead of replacing the existing object. For more information about versioning, see [How do I enable or suspend versioning for an S3 bucket? \(p. 7\)](#).

Topics

- [Uploading Files and Folders by Using Drag and Drop \(p. 25\)](#)
- [Uploading Files by Pointing and Clicking \(p. 26\)](#)
- [More Info \(p. 26\)](#)

Uploading Files and Folders by Using Drag and Drop

If you are using the Chrome or Firefox browsers, you can choose the folders and files to upload, and then drag and drop them into the destination bucket. Dragging and dropping is the *only* way that you can upload folders.

To upload folders and files to an S3 bucket by using drag and drop

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want to upload your folders or files to.
3. In a window other than the console window, select the files and folders that you want to upload. Then drag and drop your selections into the console window that lists the objects in the destination bucket.

The files you chose are listed on the **Upload** page.

4. On the **Upload** page, you can drag and drop more files and folders to the console window that displays the **Upload** page. To add more files, you can also choose **Add files** or **Add folder**.
5. In the **Destination** section, if versioning is not enabled, you must check the box acknowledging that objects with the same name will be overwritten.

To immediately upload the listed files and folders without granting or removing permissions for specific users or setting public permissions for all of the files that you're uploading, choose **Upload** at the bottom of the page. For information about object access permissions, see [How do I set permissions on an object? \(p. 61\)](#).

6. In the **Storage class** section, choose the storage class for the files you're uploading. For more information about storage classes, see [Storage Classes](#) in the *Amazon Simple Storage Service Developer Guide*.
7. Choose the type of encryption for the files that you're uploading. If you don't want to encrypt them, choose **Disable**.
 - a. To encrypt the uploaded files using keys that are managed by Amazon S3, choose **Amazon S3 key**. For more information, see [Protecting Data with Amazon S3-Managed Encryption Keys Classes](#) in the *Amazon Simple Storage Service Developer Guide*.
 - b. To encrypt the uploaded files using the AWS Key Management Service (AWS KMS), choose **AWS Key Management Service key**. Then choose a customer master key (CMK) from the list of AWS KMS CMKs.

Note

To encrypt objects in a bucket, you can use only CMKs that are available in the same AWS Region as the bucket.

You can give an external account the ability to use an object that is protected by an AWS KMS CMK. To do this, select **Custom KMS ARN** from the list and enter the Amazon Resource Name (ARN) for the external account. Administrators of an external account that have usage permissions to an object protected by your AWS KMS CMK can further restrict access by creating a resource-level IAM policy.

For more information about creating an AWS KMS CMK, see [Creating Keys](#) in the *AWS Key Management Service Developer Guide*. For more information about protecting data with AWS KMS, see [Protecting Data Using Keys Stored in AWS KMS \(SSE-KMS\)](#) in the *Amazon Simple Storage Service Developer Guide*.

8. In the **Access control list (ACL)** section, you can change the permissions for the AWS account owner. The *owner* refers to the AWS account root user, and not an AWS Identity and Access Management (IAM) user. For more information about the root user, see [The AWS Account Root User](#).

You can grant read access to your objects to the general public (everyone in the world), for all of the files that you're uploading. Granting public read access is applicable to a small subset of use cases such as when buckets are used for websites. We recommend that you do not change the default setting. You can always make changes to object permissions after you upload the object. For information about object access permissions, see [How do I set permissions on an object? \(p. 61\)](#).

Choose **Add grantee** to grant access to another AWS account. For more information about granting permissions to another AWS account, see [How do I set ACL bucket permissions? \(p. 62\)](#).

9. Object tagging gives you a way to categorize storage. Each tag is a key-value pair. Key and tag values are case sensitive. You can have up to 10 tags per object.

To add tags to all of the objects that you are uploading, choose **Add tag**. Type a tag name in the **Key** field. Type a value for the tag. A tag key can be up to 128 Unicode characters in length and tag values can be up to 255 Unicode characters in length. For more information about object tags, see [Object Tagging](#) in the *Amazon Simple Storage Service Developer Guide*.

10. Metadata for Amazon S3 objects is represented by a name-value (key-value) pair. There are two kinds of metadata: system-defined metadata and user-defined metadata. To add metadata to all the objects you are uploading, choose **Add metadata**.
 - a. If you want to add Amazon S3 system-defined metadata, for **Type**, choose **System Defined**. For **Key**, select a key. You can select common HTTP headers, such as **Content-Type** and **Content-Disposition**. Type a value for the key. For a list of system-defined metadata and information about whether you can add the value, see [System-Defined Metadata](#) in the *Amazon Simple Storage Service Developer Guide*.
 - b. Any metadata starting with prefix `x-amz-meta-` is treated as user-defined metadata. User-defined metadata is stored with the object, and is returned when you download the object.

To add user-defined metadata to all of the objects that you are uploading, for **Type** choose **User Defined**. Type `x-amz-meta-` plus a custom metadata name in the **Key** field. Type a value for the key. Both the keys and their values must conform to US-ASCII standards. User-defined metadata can be as large as 2 KB. For more information about user-defined metadata, see [User-Defined Metadata](#) in the *Amazon Simple Storage Service Developer Guide*.

11. Choose **Upload**.

Uploading Files by Pointing and Clicking

This procedure explains how to upload files into an S3 bucket by choosing **Upload**.

To upload files to an S3 bucket by pointing and clicking

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want to upload your files to.
3. Choose **Upload**.
4. On the **Upload** page, choose **Add files** or **Add folder**.
5. Choose one or more files to upload, and then choose **Open**.
6. After you see the files that you chose listed in the **Upload** dialog box, continue with **Step 5 of Uploading Files and Folders by Using Drag and Drop (p. 25)**.

More Info

- [How do I set permissions on an object? \(p. 61\)](#).

- [How do I download an object from an S3 bucket? \(p. 28\)](#)

Copying objects

In the Amazon S3 console, you can copy objects to a bucket or to an access point within the same AWS Region. For more information, see [Copying objects](#) in the *Amazon Simple Storage Service Developer Guide*.

To copy an object

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Navigate to the Amazon S3 bucket or folder that contains the objects that you want to copy.
3. Select the check box to the left of the names of the objects that you want to copy.
4. Choose **Actions** and choose **Copy** from the list of options that appears.

Alternatively, choose **Copy** from the options in the upper right.

5. Select the destination type and destination account. To specify the destination path, choose **Browse S3**, navigate to the destination, and select the check box to the left of the destination. Choose **Choose destination** in the lower right.

Alternatively, enter the destination path.

6. If you do *not* have bucket versioning enabled, you might be asked to acknowledge that existing objects with the same name are overwritten. If this is OK, select the check box and proceed. If you want to keep all versions of objects in this bucket, select **Enable Bucket Versioning**. You can also update default encryption and Object Lock properties.
7. Choose **Copy** in the bottom right and Amazon S3 moves your objects to the destination.

Note

- This action creates a copy of all specified objects with updated settings, updates the last-modified date in the specified location, and adds a delete marker to the original object.
- When moving folders, wait for the move action to finish before making additional changes in the folders.
- Objects encrypted with customer-provided encryption keys (SSE-C) cannot be copied using the S3 console. To copy objects encrypted with SSE-C, use the AWS CLI, AWS SDK, or the Amazon S3 REST API.
- This action updates metadata for bucket versioning, encryption, Object Lock features, and archived objects.

Moving objects

In the Amazon S3 console, you can move objects to a bucket or a folder.

To move objects

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Navigate to the Amazon S3 bucket or folder that contains the objects that you want to move.
3. Select the check box to the left of the names of the objects that you want to move.
4. Choose **Actions** and choose **Move** from the list of options that appears.

Alternatively, choose **Move** from the options in the upper right.

5. To specify the destination path, choose **Browse S3**, navigate to the destination, and select the check box to the left of the destination. Choose **Choose destination** in the lower right.

Alternatively, enter the destination path.

6. If you do *not* have bucket versioning enabled, you might be asked to acknowledge that existing objects with the same name are overwritten. If this is OK, select the check box and proceed. If you want to keep all versions of objects in this bucket, select **Enable Bucket Versioning**. You can also update default encryption and Object Lock properties.
7. Choose **Move** in the bottom right and Amazon S3 moves your objects to the destination.

Note

- This action creates a copy of all specified objects with updated settings, updates the last-modified date in the specified location, and adds a delete marker to the original object.
- When moving folders, wait for the move action to finish before making additional changes in the folders.
- Objects encrypted with customer-provided encryption keys (SSE-C) cannot be copied using the S3 console. To copy objects encrypted with SSE-C, use the AWS CLI, AWS SDK, or the Amazon S3 REST API.
- This action updates metadata for bucket versioning, encryption, Object Lock features, and archived objects.

How do I download an object from an S3 bucket?

This section explains how to use the Amazon S3 console to download objects from an S3 bucket.

Data transfer fees apply when you download objects. For information about Amazon S3 features, and pricing, see [Amazon S3](#).

Important

- If an object key name consists of a single period (.), or two periods (..), you can't download the object using the Amazon S3 console. To download an object with a key name of "." or "..", you must use the AWS CLI, AWS SDKs, or REST API. For more information about naming objects, see [Object Key Naming Guidelines](#) in the *Amazon Simple Storage Service Developer Guide*.
- You can download a single object per request using the Amazon S3 console. To [download multiple objects, use the AWS CLI, AWS SDKs, or REST API](#).

To download an object from an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want to download an object from.
3. You can download an object from an S3 bucket in any of the following ways:
 - Choose the name of the object that you want to download.

On the **Overview** page, choose **Download**.

- Choose the name of the object that you want to download and then choose **Download** or **Download as** from the **Action** menu.
- Choose the name of the object that you want to download. Choose **Latest version** and then choose the download icon.

Related topics

- [How do I upload files and folders to an S3 bucket? \(p. 24\)](#)

Deleting objects

This section explains how to use the Amazon S3 console to delete objects. Because all objects in your S3 bucket incur storage costs, you should delete objects that you no longer need. If you are collecting log files, for example, it's a good idea to delete them when they're no longer needed. You can set up a lifecycle rule to automatically delete objects such as log files. For more information about lifecycle rules, see [How do I create a lifecycle rule for an S3 bucket? \(p. 44\)](#) in this guide.

For information about Amazon S3 features and pricing, see [Amazon S3](#).

To delete objects

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Navigate to the Amazon S3 bucket or folder that contains the objects that you want to delete.
3. Select the check box to the left of the names of the objects that you want to delete.
4. Choose **Actions** and choose **Delete** from the list of options that appears.

Alternatively, choose **Delete** from the options in the upper right.

5. Enter **delete** if asked to confirm that you want to delete these objects.
6. Choose **Delete objects** in the bottom right and Amazon S3 deletes the specified objects.

Warning

- Deleting the specified objects cannot be undone.
- This action deletes all specified objects. When deleting folders, wait for the delete action to finish before adding new objects to the folder. Otherwise, new objects might be deleted as well.
- Deleting the specified objects cannot be undone.

How do I undelete a deleted S3 object?

This section explains how to use the Amazon S3 console to recover (undelete) deleted objects.

To be able to undelete a deleted object, you must have had versioning enabled on the bucket that contains the object before the object was deleted. For information about enabling versioning, see [How do I enable or suspend versioning for an S3 bucket? \(p. 7\)](#).

When you delete an object in a versioning-enabled bucket, all versions remain in the bucket and Amazon S3 creates a delete marker for the object. To undelete the object, you must delete this delete marker. For more information about versioning and delete markers, see [Object Versioning](#) in the *Amazon Simple Storage Service Developer Guide*.

To recover deleted objects from an S3 bucket

The following steps describe how to recover deleted objects that are not folders from your S3 bucket including objects that are within those folders.

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want.
3. To see a list of the **versions** of the objects in the bucket, select the **List versions** switch. You'll be able to see the delete markers for deleted objects.
4. To undelete an object, you must delete the delete marker. Select the check box next to the **delete marker** of the object to recover, and then choose **Delete**.
5. Confirm the deletion on the **Delete objects** page.
 - a. Enter **permanently delete** under **Permanently delete objects?**
 - b. Choose **Delete objects**.

Note

You can't use the Amazon S3 console to undelete folders. You must use the AWS CLI or SDK. For examples, see [How can I retrieve an Amazon S3 object that was deleted in a versioning-enabled bucket?](#)

More info

- [How do I see the versions of an S3 object? \(p. 33\)](#)
- [How do I enable or suspend versioning for an S3 bucket? \(p. 7\)](#)
- [Using Versioning](#) in the *Amazon Simple Storage Service Developer Guide*

How do I restore an S3 object that has been archived?

This section explains how to use the Amazon S3 console to restore an object that has been archived to the S3 Glacier or S3 Glacier Deep Archive storage classes. Objects stored in the S3 Glacier or S3 Glacier Deep Archive are not immediately accessible. To access an object in this class, you must restore a temporary copy of it to its S3 bucket for the duration (number of days) that you specify. For information about the S3 Glacier or S3 Glacier Deep Archive storage classes, see [Storage Classes](#) in the *Amazon Simple Storage Service Developer Guide*.

When you restore an archive, you pay for both the archive and the restored copy. Because there is a storage cost for the copy, restore objects only for the duration you need them. If you want a permanent copy of the object, create a copy of it in your S3 bucket. For information about Amazon S3 features and pricing, see [Amazon S3](#).

After restoring an object, you can download it from the **Overview** page. For more information, see [How do I see an overview of an object? \(p. 33\)](#).

Topics

- [Archive Retrieval Options \(p. 30\)](#)
- [Restoring an Archived S3 Object \(p. 31\)](#)
- [Upgrade an In-Progress Restore \(p. 31\)](#)
- [Checking Archive Restore Status and Expiration Date \(p. 32\)](#)

Archive Retrieval Options

The following are the available retrieval options when restoring an archived object:

- **Expedited** - Expedited retrievals allow you to quickly access your data stored in the S3 Glacier storage class when occasional urgent requests for a subset of archives are required. For all but the largest archived objects (250 MB+), data accessed using Expedited retrievals is typically made available within 1–5 minutes. Provisioned capacity ensures that retrieval capacity for Expedited retrievals is available when you need it. For more information, see [Provisioned Capacity](#). Expedited retrievals and provisioned capacity are not available for objects stored in the S3 Glacier Deep Archive storage class.
- **Standard** - Standard retrievals allow you to access any of your archived objects within several hours. This is the default option for the S3 Glacier and S3 Glacier Deep Archive retrieval requests that do not specify the retrieval option. Standard retrievals typically finish within 3–5 hours for objects stored in the S3 Glacier storage class. They typically finish within 12 hours for objects stored in the S3 Glacier Deep Archive storage class.
- **Bulk** - Bulk retrievals are the lowest-cost retrieval option in Amazon S3 Glacier, enabling you to retrieve large amounts, even petabytes, of data inexpensively. Bulk retrievals typically finish within 5–12 hours for objects stored in the S3 Glacier storage class. They typically finish within 48 hours for objects stored in the S3 Glacier Deep Archive storage class.

For more information about retrieval options, see [Restoring Archived Objects](#) in the *Amazon Simple Storage Service Developer Guide*.

Restoring an Archived S3 Object

This topic explains how to use the Amazon S3 console to restore an object that has been archived to the S3 Glacier or S3 Glacier Deep Archive storage classes. (The console uses the names Glacier and Glacier Deep Archive for these storage classes.)

To restore archived S3 objects

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that contains the objects that you want to restore.
3. In the **Name** list, select the object or objects that you want to restore, choose **Actions**, and then choose **Initiate restore**.
4. In the **Initiate restore** dialog box, type the number of days that you want your archived data to be accessible.
5. Choose one of the following retrieval options from the **Retrieval options** menu.
 - Choose **Bulk retrieval** or **Standard retrieval**, and then choose **Restore**.
 - Choose **Expedited retrieval** (available only for the Glacier storage class).
6. Provisioned capacity is only available for the Glacier storage class. If you have provisioned capacity, choose **Restore** to start a provisioned retrieval. If you have provisioned capacity, all of your expedited retrievals are served by your provisioned capacity. For more information about provisioned capacity, see [Provisioned Capacity](#).
 - If you don't have provisioned capacity and you don't want to buy it, choose **Restore**.
 - If you don't have provisioned capacity, but you want to buy it, choose **Add capacity unit**, and then choose **Buy**. When you get the **Purchase succeeded** message, choose **Restore** to start provisioned retrieval.

Upgrade an In-Progress Restore

You can upgrade the speed of your restoration while it is in progress.

To upgrade an in-progress restore to a faster tier

1. In the **Name** list, select one or more of the objects that you are restoring, choose **Actions**, and then choose **Restore from Glacier**. For information about checking the restoration status of an object, see [Checking Archive Restore Status and Expiration Date \(p. 32\)](#).
2. Choose the tier that you want to upgrade to and then choose **Restore**. For more information about upgrading to a faster restore tier, see [Restoring Archived Objects](#) in the *Amazon Simple Storage Service Developer Guide*.

Checking Archive Restore Status and Expiration Date

To check the progress of the restoration, see the object overview panel. For information about the overview panel, see [How do I see an overview of an object? \(p. 33\)](#).

The **Overview** section shows that restoration is **In progress**.

When the temporary copy of the object is available, the object's **Overview** section shows the **Restoration expiry date**. This is when Amazon S3 will remove the restored copy of your archive.

Restored objects are stored only for the number of days that you specify. If you want a permanent copy of the object, create a copy of it in your Amazon S3 bucket.

Amazon S3 calculates the expiry date by adding the number of days that you specify to the time you request to restore the object, and then rounding to the next day at midnight UTC. This calculation applies to the initial restoration of the object and to any extensions to availability that you request. For example, if an object was restored on 10/15/2012 10:30 AM UTC and the number of days that you specified is 3, then the object is available until 10/19/2012 00:00 UTC. If, on 10/16/2012 11:00 AM UTC you change the number of days that you want it to be accessible to 1, then Amazon S3 makes the restored object available until 10/18/2012 00:00 UTC.

After restoring an object, you can download it from the **Overview** page. For more information, see [How do I see an overview of an object? \(p. 33\)](#).

More Info

- [Restoring Archived Objects](#) in the Amazon S3 Developer Guide.
- [restore-object](#) in the AWS CLI Command Reference.
- [Identity and Access Management in Amazon S3 Glacier](#) in the S3 Glacier Developer Guide.
- [How do I create a lifecycle rule for an S3 bucket? \(p. 44\)](#)
- [How do I undelete a deleted S3 object? \(p. 29\)](#)

How do I lock an Amazon S3 object?

With S3 Object Lock, you can store objects in Amazon S3 using a *write-once-read-many* (WORM) model. You can use S3 Object Lock to prevent an object from being deleted or overwritten for a fixed amount of time or indefinitely. For information about object locking using the AWS CLI, AWS SDKs, and the Amazon S3 REST APIs, see [Locking Objects Using Object Lock](#) in the *Amazon Simple Storage Service Developer Guide*.

Before you lock any objects, you have to enable a bucket to use S3 Object Lock. You enable Object Lock when you create a bucket. After you enable Object Lock on a bucket, you can lock objects in that bucket. When you create a bucket with Object Lock enabled, you can't disable Object Lock or suspend versioning for that bucket.

For information about creating a bucket with S3 Object Lock enabled, see [How do I create an S3 Bucket? \(p. 3\)](#).

To lock an Amazon S3 object

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want.
3. In the **Objects** list, choose the name of the object that you want to lock.
4. Choose **Properties**.
5. Choose **Object Lock**.
6. Choose a retention mode. You can change the **Retain until date**. You can also choose to enable a **Legal hold**. For more information, see [S3 Object Lock Overview](#) in the *Amazon Simple Storage Service Developer Guide*.
7. Choose **Save**.

More info

- [Setting bucket and object access permissions \(p. 58\)](#)

How do I see an overview of an object?

This section explains how to use the Amazon S3 console to view the object overview panel. This panel provides an overview of all the essential information for an object in one place.

To see the overview panel for an object

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that contains the object.
3. In the **Name** list, select the name of the object for which you want an overview.
4. To download the object, choose **Download** in the object overview panel. To copy the path of the object to the clipboard, choose **Copy Path**.
5. If versioning is enabled on the bucket, choose **Latest versions** to list the versions of the object. You can then choose the download icon to download an object version, or choose the trash can icon to delete an object version.

Important

You can undelete an object only if it was deleted as the latest (current) version. You can't undelete a previous version of an object that was deleted. For more information, see [Object Versioning](#) and [Using Versioning](#) in the *Amazon Simple Storage Service Developer Guide*.

More info

- [How do I see the versions of an S3 object? \(p. 33\)](#)

How do I see the versions of an S3 object?

This section explains how to use the Amazon S3 console to see the different versions of an object.

A versioning-enabled bucket can have many versions of the same object; one current (latest) version and zero or more noncurrent (previous) versions. Amazon S3 assigns each object a unique version ID. For information about enabling versioning, see [How do I enable or suspend versioning for an S3 bucket? \(p. 7\)](#).

If a bucket is versioning-enabled, Amazon S3 creates another version of an object under the following conditions:

- If you upload an object that has the same name as an object that already exists in the bucket, Amazon S3 creates another version of the object instead of replacing the existing object.
- If you update any object properties after you upload the object to the bucket, such as changing the storage details or other metadata, Amazon S3 creates a new object version in the bucket.

For more information about versioning support in Amazon S3, see [Object Versioning](#) and [Using Versioning](#) in the *Amazon Simple Storage Service Developer Guide*.

To see multiple versions of an object

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that contains the object.
3. To see a list of the versions of the objects in the bucket, choose the **List versions** switch.

For each object version, the console shows a unique version ID, the date and time the object version was created, and other properties. (Objects stored in your bucket before you set the versioning state have a version ID of **null**.)

To list the objects without the versions, choose the **List versions** switch.

You also can view, download, and delete object versions in the object overview panel. For more information, see [How do I see an overview of an object? \(p. 33\)](#).

Important

You can undelete an object only if it was deleted as the latest (current) version. You can't undelete a previous version of an object that was deleted. For more information, see [Object Versioning](#) and [Using Versioning](#) in the *Amazon Simple Storage Service Developer Guide*.

More info

- [How do I enable or suspend versioning for an S3 bucket? \(p. 7\)](#)
- [How do I create a lifecycle rule for an S3 bucket? \(p. 44\)](#)

How do I view the properties of an object?

This section explains how to use the console to view the properties of an object.

To view the properties of an object

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that contains the object.
3. In the **Name** list, choose the name of the object you want to view the properties for.
4. Choose **Properties**.

5. On the **Properties** page, you can configure the following properties for the object.

Note

If you change the properties **Storage Class**, **Encryption**, or **Metadata**, a new object is created to replace the old one. If S3 Versioning is enabled, a new version of the object is created, and the existing object becomes an older version. The role that changes the property also becomes the owner of the new object or (object version).

- a. **Storage class** – Each object in Amazon S3 has a storage class associated with it. The storage class that you choose to use depends on how frequently you access the object. The default storage class for S3 objects is STANDARD. You choose which storage class to use when you upload an object. For more information about storage classes, see [Storage Classes](#) in the *Amazon Simple Storage Service Developer Guide*.

To change the storage class after you upload an object, choose **Storage class**. Choose the storage class that you want, and then choose **Save**.

- b. **Encryption** – You can encrypt your S3 objects. For more information, see [How do I add encryption to an S3 object? \(p. 35\)](#).
- c. **Metadata** – Each object in Amazon S3 has a set of name-value pairs that represents its metadata. For information on adding metadata to an S3 object, see [Editing object metadata \(p. 36\)](#).
- d. **Tags** – You can add tags to an S3 object. For more information, see [Editing object tags \(p. 38\)](#).
- e. **Object lock** – You can prevent an object from being deleted.

How do I add encryption to an S3 object?

This topic describes how to set or change the type of encryption an object using the Amazon S3 console.

Note

If you change an object's encryption, a new object is created to replace the old one. If S3 Versioning is enabled, a new version of the object is created, and the existing object becomes an older version. The role that changes the property also becomes the owner of the new object or (object version).

To add or change encryption for an object

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Bucket** list, choose the name of the bucket that contains the object.
3. In the **Name** list, choose the name of the object that you want to add or change encryption for.
4. Choose **Properties**, and then choose **Encryption**.

The **Encryption** dialog box opens, giving you three choices for object encryption:

- **None** – No object encryption.
 - **AES-256** – Server-side encryption with Amazon S3 managed keys (SSE-S3).
 - **AWS-KMS** – Server-side encryption with AWS Key Management Service (AWS KMS) customer master keys (SSE-KMS).
5. If you want to remove encryption from an object that already has encryption settings, choose **None** and then choose **Save**.
 6. If you want to encrypt your object using keys that are managed by Amazon S3, follow these steps:
 - a. Choose **AES-256**.

For more information about using Amazon S3 server-side encryption to encrypt your data, see [Protecting Data with Amazon S3-Managed Encryption Keys Classes](#) in the *Amazon Simple Storage Service Developer Guide*.

- b. Choose **Save**.
7. If you want to encrypt your object using AWS KMS, follow these steps:
 - a. Choose **AWS-KMS**.
 - b. Choose an AWS KMS customer master key (CMK).

The list shows [customer managed CMKs](#) that you have created and your AWS managed CMK for Amazon S3. For more information about creating a customer managed AWS KMS CMK, see [Creating Keys](#) in the *AWS Key Management Service Developer Guide*.

Important

The Amazon S3 console lists only 100 AWS KMS CMKs per AWS Region. If you have more than 100 CMKs in the same Region, you can see only the first 100 CMKs in the S3 console. To use a KMS CMK that is not listed in the console, choose **Custom KMS ARN**, and enter the KMS CMK ARN.

- c. Choose **Save**.

Important

To encrypt objects in the bucket, you can use only CMKs that are enabled in the same AWS Region as the bucket. Amazon S3 only supports symmetric CMKs. Amazon S3 does not support asymmetric CMKs. For more information, see [Using Symmetric and Asymmetric Keys](#).

8. To give an external account the ability to use an object that is protected by an AWS KMS CMK, follow these steps:
 - a. Choose **AWS-KMS**.
 - b. Enter the Amazon Resource Name (ARN) for the external account.
 - c. Choose **Save**.

Administrators of an external account that have usage permissions to an object protected by your AWS KMS CMK can further restrict access by creating a resource-level AWS Identity and Access Management (IAM) policy.

Note

This action applies encryption to all specified objects. When encrypting folders, wait for the save operation to finish before adding new objects to the folder.

More info

- [How do I enable default encryption for an Amazon S3 bucket? \(p. 7\)](#)
- [Amazon S3 default encryption for S3 buckets](#) in the *Amazon Simple Storage Service Developer Guide*
- [How do I view the properties of an object? \(p. 34\)](#)
- [Uploading, downloading, and managing objects \(p. 23\)](#)

Editing object metadata

This section explains how to use the Amazon S3 console to edit metadata of existing S3 objects. Each object in Amazon S3 can have a set of key-value pairs that provides *metadata*, which is additional

information about the object. Some metadata is set by Amazon S3 when you upload the object. For example, `Content-Length` is the *key* (name) and the *value* is the size of the object in bytes.

You can also set some metadata when you upload the object and later edit it as your needs change. For example, you may have a set of objects that you initially store in the `STANDARD` storage class. Over time you may no longer need this data to be highly available and change the storage class to `GLACIER` by editing the value of the `x-amz-storage-class` key from `STANDARD` to `GLACIER`.

There are two kinds of metadata for an S3 object, Amazon S3 *system-defined* metadata and *user-defined* metadata:

- **System-defined metadata**—Within system metadata, there are two categories.
 - Metadata such as the `Last-Modified` date is controlled by the system and only Amazon S3 can modify the value.
 - There is also system metadata that you can modify, for example, the storage class for the object or the encryption type.
- **User-defined metadata**—You can define your own custom metadata, called user-defined metadata, that you assign to an object when you upload the object or after the object has been uploaded. User-defined metadata is stored with the object and is returned when you download the object. Amazon S3 does not process user-defined metadata.

The following topics describe how to edit metadata of an object using the Amazon S3 console.

Topics

- [Editing system-defined metadata \(p. 37\)](#)
- [Editing user-defined metadata \(p. 38\)](#)

Note

- This action creates a *copy* of the object with updated settings and the last-modified date. If S3 Versioning is enabled, a new version of the object is created, and the existing object becomes an older version. The IAM role that changes the property also becomes the owner of the new object or (object version).
- Editing metadata updates values for existing key names.
- Objects encrypted with customer-provided encryption keys (SSE-C) cannot be copied using the console and must use the AWS CLI, AWS SDK, or the Amazon S3 REST API,

Warning

- When editing metadata of folders, wait for the Edit metadata operation to finish before adding new objects to the folder. Otherwise, new objects might be edited as well.
- Objects encrypted with customer-provided encryption keys (SSE-C) cannot be copied using the console and must use the AWS CLI, AWS SDK, or the Amazon S3 REST API,

For more information about object metadata including naming guidelines and limits, see [Object Metadata](#) in the *Amazon Simple Storage Service Developer Guide*.

Editing system-defined metadata

You can configure some, but not all, system metadata for an S3 object. For a list of system-defined metadata and whether you can modify their values, see [System-Defined Metadata](#) in the *Amazon Simple Storage Service Developer Guide*.

To edit system-defined metadata of an object

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Navigate to your Amazon S3 bucket or folder and select the check box to the left of the names of the objects with metadata you want to edit.
3. Open the **Action** menu, go to the **Edit actions** section, and choose **Edit metadata**.
4. Review the objects listed and choose **Add metadata**.
5. For metadata **Type**, select **System-defined**.
6. Specify a unique **Key** and the metadata **Value**.
7. To edit additional metadata, choose **Add metadata**. You can also choose **Remove** to remove a set of Type-Key-Values.
8. When you are done, choose **Save changes** and Amazon S3 edits the metadata of the specified objects.

Editing user-defined metadata

You can edit user-defined metadata of an object by combining the metadata prefix, `x-amz-meta-`, and a name you choose to create a custom key. For example, if you add the custom name `alt-name`, the metadata key would be `x-amz-meta-alt-name`. User-defined metadata can be as large as 2 KB. Both keys and their values must conform to US-ASCII standards. For more information, see [User-Defined Metadata](#) in the *Amazon Simple Storage Service Developer Guide*.

To edit user-defined metadata of an object

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Navigate to your Amazon S3 bucket or folder and select the check box to the left of the names of the objects with metadata you want to edit.
3. Open the **Action** menu, go to the **Edit actions** section, and choose **Edit metadata**.
4. Review the objects listed and choose **Add metadata**.
5. For metadata **Type**, select **User-defined**.
6. Enter a unique, custom **Key** following `x-amz-meta-`. Also enter a metadata **Value**.
7. To add additional metadata, choose **Add metadata**. You can also choose **Remove** to remove a set of Type-Key-Values.
8. When you are done, choose **Save changes** and Amazon S3 edits the metadata of the specified objects.

More info

- [How do I view the properties of an object? \(p. 34\)](#)
- [Uploading, downloading, and managing objects \(p. 23\)](#)

Editing object tags

Object tagging gives you a way to categorize storage. This topic explains how to use the console to add tags to an S3 object after the object has been uploaded. For information about adding tags to an object when the object is being uploaded, see [How do I upload files and folders to an S3 bucket? \(p. 24\)](#).

Each tag is a key-value pair that adheres to the following rules:

- You can associate up to 10 tags with an object. Tags associated with an object must have unique tag keys.
- A tag key can be up to 128 Unicode characters in length and tag values can be up to 256 Unicode characters in length.
- Key and tag values are case sensitive.

For more information about object tags, see [Object Tagging](#) in the *Amazon Simple Storage Service Developer Guide*. For more information about tag restrictions, see [User-Defined Tag Restrictions](#) in the *AWS Billing and Cost Management User Guide*.

To add tags to an object

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Navigate to your Amazon S3 bucket or folder and select the check box to the left of the names of the objects that you want to add tags to.
3. Open the **Action** menu, go to the **Edit actions** section, and choose **Edit Tags**.
4. Review the objects listed and choose **Add tags**.
5. Each object tag is a key-value pair. Enter a **Key** and a **Value**. To add another tag, choose **Add Tag**. When you are done, choose **Save changes** and Amazon S3 adds the tags to the specified objects.

You can enter up to 10 tags for an object.

For more information, see also [How do I view the properties of an object? \(p. 34\)](#) and [Uploading, downloading, and managing objects \(p. 23\)](#) in this guide.

How do I use folders in an S3 bucket?

In Amazon S3, buckets and objects are the primary resources, and objects are stored in buckets. Amazon S3 has a flat structure instead of a hierarchy like you would see in a file system. However, for the sake of organizational simplicity, the Amazon S3 console supports the folder concept as a means of grouping objects. Amazon S3 does this by using a shared name prefix for objects (that is, objects have names that begin with a common string). Object names are also referred to as *key names*.

For example, you can create a folder on the console named `photos` and store an object named `myphoto.jpg` in it. The object is then stored with the key name `photos/myphoto.jpg`, where `photos/` is the prefix.

Here are two more examples:

- If you have three objects in your bucket—`logs/date1.txt`, `logs/date2.txt`, and `logs/date3.txt`—the console will show a folder named `logs`. If you open the folder in the console, you will see three objects: `date1.txt`, `date2.txt`, and `date3.txt`.
- If you have an object named `photos/2017/example.jpg`, the console will show you a folder named `photos` containing the folder `2017` and the object `example.jpg`.

Topics

- [Creating a folder \(p. 40\)](#)
- [How do I delete folders from an S3 bucket? \(p. 40\)](#)

- [Making folders public \(p. 41\)](#)

You can have folders within folders, but not buckets within buckets. You can upload and copy objects directly into a folder. Folders can be created, deleted, and made public, but they cannot be renamed. Objects can be copied from one folder to another.

Important

- The Amazon S3 console implements folder object creation by creating a zero-byte object with the folder *prefix and delimiter* value as the key. These folder objects don't appear in the console. Otherwise they behave like any other objects and can be viewed and manipulated through the REST API, AWS CLI, and AWS SDKs.
- The Amazon S3 console treats all objects that have a forward slash "/" character as the last (trailing) character in the key name as a folder, for example `examplekeyname/`. You can't upload an object that has a key name with a trailing "/" character using the Amazon S3 console. However, you can upload objects that are named with a trailing "/" with the Amazon S3 API by using the AWS CLI, AWS SDKs, or REST API.
- An object that is named with a trailing "/" appears as a folder in the Amazon S3 console. The Amazon S3 console does not display the content and metadata for such an object. When you use the console to copy an object named with a trailing "/", a new folder is created in the destination location, but the object's data and metadata are not copied.

Creating a folder

This section describes how to use the Amazon S3 console to create a folder.

Important

If your bucket policy prevents uploading objects to this bucket without encryption, tags, metadata, or access control list (ACL) grantees, you will not be able to create a folder using this configuration. Instead, upload an empty folder and specify these settings in the upload configuration.

To create a folder

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want to create a folder in.
3. Choose **Create folder**.
4. Enter a name for the folder (for example, `favorite-pics`). Then click **Create folder**.

How do I delete folders from an S3 bucket?

This section explains how to use the Amazon S3 console to delete folders from an S3 bucket.

For information about Amazon S3 features and pricing, see [Amazon S3](#).

To delete folders from an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want to delete folders from.
3. In the **Name** list, select the check box next to the folders and objects that you want to delete, choose **Actions**, and then choose **Delete**.

4. On the **Delete objects** page, verify that the names of the folders you selected for deletion are listed. Enter **delete** in the box provided and click **Delete objects**.

Warning

This action deletes all specified objects. When deleting folders, wait for the delete action to finish before adding new objects to the folder. Otherwise, new objects might be deleted as well.

Related topics

- [Deleting objects \(p. 29\)](#)

Making folders public

Amazon S3 has a flat structure instead of a hierarchy like you would typically see in a file system. However, for the sake of organizational simplicity, the Amazon S3 console supports a folder concept as a way to group objects. In Amazon S3, the folder is a naming prefix for an object or group of objects. For more information, see [How do I use folders in an S3 bucket? \(p. 39\)](#)

We recommend blocking all public access to your Amazon S3 folders and buckets unless you specifically require a public folder or bucket. When you make a folder public, anyone on the internet can view all the objects that are grouped in that folder. In the Amazon S3 console, you can make a folder public. You can also make a folder public by creating a bucket policy that limits access by prefix. For more information, see [Setting bucket and object access permissions \(p. 58\)](#).

Warning

After you make a folder public in the Amazon S3 console, you can't make it private again. Instead, you must set permissions on each individual object in the public folder so that the objects have no public access. For more information, see [How do I set permissions on an object? \(p. 61\)](#)

More info

- [How do I delete folders from an S3 bucket? \(p. 40\)](#)
- [How do I set ACL bucket permissions? \(p. 62\)](#)
- [How do I block public access to S3 buckets? \(p. 59\)](#)

Introduction to S3 Batch Operations

S3 Batch Operations performs large-scale batch operations on Amazon S3 objects. You can use S3 Batch Operations to copy objects, set object tags or access control lists (ACLs), initiate object restores from Amazon S3 Glacier, or invoke an AWS Lambda function to perform custom actions using your objects. You can perform these operations on a custom list of objects, or you can use an Amazon S3 inventory report to make generating even the largest lists of objects easy. S3 Batch Operations use the same Amazon S3 APIs that you already use, so you'll find the interface familiar. For information about performing S3 Batch Operations using the AWS CLI, AWS SDKs, and the Amazon S3 REST APIs, see [Performing S3 Batch Operations](#) in the *Amazon Simple Storage Service Developer Guide*.

The following topics explain how to use the Amazon S3 console to configure and run batch operations.

Topics

- [Creating an S3 Batch Operations job](#) (p. 42)
- [Managing S3 Batch Operations jobs](#) (p. 43)

Creating an S3 Batch Operations job

This section describes how to create a S3 Batch Operations job. For information about performing Batch Operations using the AWS CLI, AWS SDKs, and the Amazon S3 REST APIs, see [Performing S3 Batch Operations](#) in the *Amazon Simple Storage Service Developer Guide*.

To create a batch job

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Choose **Batch Operations** on the navigation pane of the Amazon S3 console.
3. Choose **Create job**.
4. Choose the **Region** where you want to create your job.
5. Under **Manifest format**, choose the type of manifest object to use.
 - If you choose **S3 inventory report**, enter the path to the manifest.json object that Amazon S3 generated as part of the CSV-formatted Inventory report, and optionally the version ID for the manifest object if you want to use a version other than the most recent.
 - If you choose **CSV**, enter the path to a CSV-formatted manifest object. The manifest object must follow the format described in the console. You can optionally include the version ID for the manifest object if you want to use a version other than the most recent.
6. Choose **Next**.
7. Under **Operation**, choose the operation that you want to perform on all objects listed in the manifest. Fill out the information for the operation you chose and then choose **Next**.
8. Fill out the information for **Configure additional options** and then choose **Next**.
9. For **Review**, verify the settings. If you need to make changes, choose **Previous**. Otherwise, choose **Create Job**.

More info

- [The Basics: S3 Batch Operations Jobs](#) in the *Amazon Simple Storage Service Developer Guide*

- [Creating a S3 Batch Operations Job](#) in the *Amazon Simple Storage Service Developer Guide*
- [Operations](#) in the *Amazon Simple Storage Service Developer Guide*

Managing S3 Batch Operations jobs

Amazon S3 provides a set of tools to help you manage your S3 Batch Operations jobs after you create them. For more information about managing S3 Batch Operations, see [Managing S3 Batch Operations Jobs](#) in the *Amazon Simple Storage Service Developer Guide*.

More info

- [The Basics: S3 Batch Operations Jobs](#) in the *Amazon Simple Storage Service Developer Guide*
- [Creating a S3 Batch Operations Job](#) in the *Amazon Simple Storage Service Developer Guide*
- [Operations](#) in the *Amazon Simple Storage Service Developer Guide*

Storage management

This section explains how to configure Amazon S3 storage management tools.

Topics

- [How do I create a lifecycle rule for an S3 bucket? \(p. 44\)](#)
- [How do I add a replication rule to an S3 bucket? \(p. 46\)](#)
- [How do I manage the replication rules for an S3 Bucket? \(p. 50\)](#)
- [How Do I Configure Storage Class Analysis? \(p. 51\)](#)
- [How Do I Configure Amazon S3 Inventory? \(p. 52\)](#)
- [How do I create a request metrics filter for all the objects in my S3 bucket? \(p. 55\)](#)
- [How do I create a request metrics filter that limits scope by object tag or prefix? \(p. 55\)](#)
- [How do I delete a request metrics filter? \(p. 56\)](#)
- [How do I view replication metrics? \(p. 57\)](#)

How do I create a lifecycle rule for an S3 bucket?

You can use lifecycle rules to define actions that you want Amazon S3 to take during an object's lifetime (for example, transition objects to another storage class, archive them, or delete them after a specified period of time).

You can define a lifecycle rules for all objects or a subset of objects in the bucket by using a shared prefix (objects names that begin with a common string) or a tag.

Using a lifecycle rule you can define actions specific to current and non-current object versions. For more information, see [Object Lifecycle Management](#) and [Object Versioning](#) and [Using Versioning](#) in the *Amazon Simple Storage Service Developer Guide*.

To create a lifecycle rule

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want to create a lifecycle rule for.
3. Choose the **Management** tab, and choose **Create lifecycle rule**.
4. In **Lifecycle rule name**, enter a name for your rule.

The name must be unique within the bucket.

5. Choose the scope of the lifecycle rule:
 - To apply this lifecycle rule to *all objects with a specific prefix or tag*, choose **Limit the scope to specific prefixes or tags**.
 - To limit the scope by prefix, in **Prefix**, enter the prefix.
 - To limit the scope by tag, choose **Add tag**, and enter the tag key and value.

For more information about object name prefixes, see [Object Keys](#) in the *Amazon Simple Storage Service Developer Guide*. For more information about object tags, see [Object Tagging](#) in the *Amazon Simple Storage Service Developer Guide*.

- To apply this lifecycle rule to *all objects in the bucket*, choose **This rule applies to all objects in the bucket**, and choose **I acknowledge that this rule applies to all objects in the bucket**.
6. Under **Lifecycle rule actions**, choose the actions that you want your lifecycle rule to perform:

- Transition *current* versions of objects between storage classes
- Transition *previous* versions of objects between storage classes
- Expire *current* versions of objects
- Permanently delete *previous* versions of objects
- Delete expired delete markers or incomplete multipart uploads

Depending on the actions that you choose, different options appear.

7. To transition *current* versions of objects between storage classes, under **Transition current versions of objects between storage classes**:
 - a. In **Storage class transitions**, choose the storage class to transition to:
 - Standard-IA
 - Intelligent-Tiering
 - One Zone-IA
 - Glacier
 - Glacier Deep Archive
 - b. In **Days after object creation**, enter the number of days after creation to transition the object.

For more information about storage classes, see [Storage Classes](#) in the *Amazon Simple Storage Service Developer Guide*. You can define transitions for current or previous object versions or for both current and previous versions. Versioning enables you to keep multiple versions of an object in one bucket. For more information about versioning, see [How do I enable or suspend versioning for an S3 bucket? \(p. 7\)](#).

Important

When you choose the Glacier or Glacier Deep Archive storage class, your objects remain in Amazon S3. You cannot access them directly through the separate Amazon S3 Glacier service. For more information, see [Transitioning Objects Using Amazon S3 Lifecycle](#).

8. To transition *non-current* versions of objects between storage classes, under **Transition non-current versions of objects between storage classes**:
 - a. In **Storage class transitions**, choose the storage class to transition to:
 - Standard-IA
 - Intelligent-Tiering
 - One Zone-IA
 - Glacier
 - Glacier Deep Archive
 - b. In **Days after object becomes non-current**, enter the number of days after creation to transition the object.
9. To expire *current* versions of objects, under **Expire previous versions of objects**, in **Number of days after object creation**, enter the number of days.

Important

In a non-versioned bucket the expiration action results in Amazon S3 permanently removing the object. For more information about lifecycle actions, see [Elements to describe lifecycle actions](#) in the *Amazon Simple Storage Service Developer Guide*.

10. To permanently delete previous versions of objects, under **Permanently delete previous versions of objects**, in **Number of days after objects become previous versions**, enter the number of days.
11. Under **Delete expired delete markers or incomplete multipart uploads**, choose **Delete expired object delete markers** and **Delete incomplete multipart uploads**. Then, enter the number of

days after the multipart upload initiation that you want to end and clean up incomplete multipart uploads.

For more information about multipart uploads, see [Multipart Upload Overview](#) in the Amazon Simple Storage Service Developer Guide.

12. Choose **Create rule**.

If the rule does not contain any errors, Amazon S3 enables it, and you can see it on the **Management** tab under **Lifecycle rules**.

How do I add a replication rule to an S3 bucket?

Replication is the automatic, asynchronous copying of objects across buckets in the same or different AWS Regions. Replication copies newly created objects and object updates from a source bucket to a destination bucket. For more information about replication concepts and how to use replication with the AWS CLI, AWS SDKs, and the Amazon S3 REST APIs, see [Replication](#) in the *Amazon Simple Storage Service Developer Guide*.

Replication requires versioning to be enabled on both the source and destination buckets. To review the full list of requirements, see [Requirements for Replication](#) in the *Amazon Simple Storage Service Developer Guide*. For more information about versioning, see [How do I enable or suspend versioning for an S3 bucket? \(p. 7\)](#)

The object replicas in the destination bucket are exact replicas of the objects in the source bucket. They have the same key names and the same metadata—for example, creation time, owner, user-defined metadata, version ID, access control list (ACL), and storage class. Optionally, you can explicitly specify a different storage class for object replicas. And regardless of who owns the source bucket or the source object, you can choose to change replica ownership to the AWS account that owns the destination bucket. For more information, see [Changing the replica owner](#) in the *Amazon Simple Storage Service Developer Guide*.

You can use S3 Replication Time Control (S3 RTC) to replicate your data in the same AWS Region or across different AWS Regions in a predictable timeframe. S3 RTC replicates 99.99 percent of new objects stored in Amazon S3 within 15 minutes and most objects within seconds. For more information, see [Replicating Objects Using S3 Replication Time Control \(S3 RTC\)](#) in the *Amazon Simple Storage Service Developer Guide*.

Note about replication and lifecycle rules

Metadata for an object remains identical between original objects and replica objects. Lifecycle rules abide by the creation time of the original object, and not by when the replicated object becomes available in the destination bucket. However, lifecycle does not act on objects that are pending replication until replication is complete.

You use the Amazon S3 console to add replication rules to the source bucket. Replication rules define which source bucket objects to replicate and the destination bucket where the replicated objects are stored. You can create a rule to replicate all the objects in a bucket or a subset of objects with a specific key name prefix, one or more object tags, or both. A destination bucket can be in the same AWS account as the source bucket, or it can be in a different account.

If you specify an object version ID to delete, Amazon S3 deletes that object version in the source bucket. But it doesn't replicate the deletion in the destination bucket. In other words, it doesn't delete the same object version from the destination bucket. This protects data from malicious deletions.

If the destination bucket is in a different account from the source bucket, you must add a bucket policy to the destination bucket to grant the owner of the source bucket account permission to replicate objects in the destination bucket. For more information, see [Granting permissions when source and destination buckets are owned by different AWS accounts](#) in the *Amazon Simple Storage Service Developer Guide*.

When you add a replication rule to a bucket, the rule is enabled by default, so it starts working as soon as you save it.

Topics

- [Adding a replication rule \(p. 47\)](#)
- [Grant the source bucket owner permission to encrypt using the AWS KMS CMK \(p. 49\)](#)
- [More info \(p. 50\)](#)

Adding a replication rule

Follow these steps to configure a replication rule when the destination bucket is in the same AWS account as the source bucket.

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want.
3. Choose **Management**, scroll down to **Replication rules**, and then choose **Create replication rule**.
4. Under **Rule name**, enter a name for your rule to help identify the rule later. The name is required and must be unique within the bucket.
5. Set up an AWS Identity and Access Management (IAM) role that Amazon S3 can assume to replicate objects on your behalf.

To set up an IAM role, on the **Replication rule configuration** section, under **IAM role**, do one of the following:

- We highly recommend that you choose **Create new role** to have Amazon S3 create a new IAM role for you. When you save the rule, a new policy is generated for the IAM role that matches the source and destination buckets that you choose. The name of the generated role is based on the bucket names and uses the following naming convention: **replication_role_for_source-bucket_to_destination-bucket**.
- You can choose to use an existing IAM role. If you do, you must choose a role that grants Amazon S3 the necessary permissions for replication. Replication fails if this role does not grant Amazon S3 sufficient permissions to follow your replication rule.

Important

When you add a replication rule to a bucket, you must have the `iam:PassRole` permission to be able to pass the IAM role that grants Amazon S3 replication permissions. For more information, see [Granting a User Permissions to Pass a Role to an AWS Service](#) in the *IAM User Guide*.

6. Under **Status**, see that **Enabled** is selected by default. An enabled rule starts to work as soon as you save it. If you want to enable the rule later, select **Disabled**.
7. If the bucket has existing replication rules, you are instructed to set a priority for the rule. You must set a priority for the rule to avoid conflicts caused by objects that are included in the scope of more than one rule. In the case of overlapping rules, Amazon S3 uses the rule priority to determine which rule to apply. The higher the number, the higher the priority. For more information about rule priority, see [Replication configuration overview](#) in the *Amazon Simple Storage Service Developer Guide*.
8. In the **Replication rule configuration**, under **Source bucket**, you have the following options for setting the replication source:
 - To replicate the whole bucket, choose **This rule applies to all objects in the bucket**.

- To replicate all objects that have the same prefix, choose **Limit the scope of this rule using one or more filters**. This will limit replication to all objects that have names that begin with the string (for example `pictures`). Enter a prefix in the box.

Note

If you enter a prefix that is the name of a folder, you must use `/` (forward slash) as the last character (for example, `pictures/`).

- To replicate all objects with one or more object tags, select **Add tag** and enter the key value pair in the boxes. Repeat the procedure to add another tag. You can combine a prefix and tags. For more information about object tags, see [Object Tagging](#) in the *Amazon Simple Storage Service Developer Guide*.

The new schema supports prefix and tag filtering and the prioritization of rules. For more information about the new schema, see [Replication Configuration Backward Compatibility](#) in the *Amazon Simple Storage Service Developer Guide*. The developer guide describes the XML used with the Amazon S3 API that works behind the user interface. In the developer guide, the new schema is described as *replication configuration XML V2*.

9. Under **Destination**, you have the following options for setting the replication destination:

- To replicate to a bucket in your account, select **Choose a bucket in this account** and type or browse for your the destination bucket.
- To replicate to a bucket in a different AWS account, select **Choose a bucket in another account** and enter the destination bucket account ID and type your destination bucket name.

If the destination bucket is in a different account from the source bucket, you must add a bucket policy to the destination bucket to grant the owner of the source bucket account permission to replicate objects in the destination bucket. For more information, see [Granting permissions when source and destination buckets are owned by different AWS accounts](#) in the *Amazon Simple Storage Service Developer Guide*.

Note

If versioning is not enabled on the destination bucket, you will get a warning that contains an **Enable versioning** button. Choose this button to enable versioning on the bucket.

10. If you want to enable **Object Ownership** to help standardize ownership of new objects in the destination bucket, choose **Change object ownership to the destination bucket owner**. For more information about this option, see [Meet compliance requirements using S3 RTC](#) in the *Amazon Simple Storage Service Developer Guide*.

If you want to replicate your data into a specific storage class in the destination bucket, choose **Change the storage class for the replicated objects**. Then choose the storage class that you want to use for the replicated objects in the destination bucket. If you don't select this option, the storage class for replicated objects is the same class as the original objects.

If you want to enable S3 Replication Time Control (S3 RTC) in your replication configuration, select **S3 Replication Time Control**. For more information about this option, see [Meet compliance requirements using S3 RTC](#) in the *Amazon Simple Storage Service Developer Guide*.

Note

When you use S3 RTC, additional per-GB data transfer fees and CloudWatch metrics fees apply.

11. To replicate objects in the source bucket that are encrypted with AWS Key Management Service (AWS KMS), under **Replication criteria**, select **Replicate objects encrypted with AWS KMS**. Under **AWS KMS key for encrypting destination objects** are the source keys that you allow replication to use. All source CMKs are included by default. You can choose to narrow the CMK selection.

Objects encrypted by AWS KMS CMKs that you do not select are not replicated. A CMK or a group of CMKs is chosen for you, but you can choose the CMKs if you want. For information about using AWS KMS with replication, see [Replicating Objects Created with Server-Side Encryption \(SSE\) Using Encryption Keys Stored in AWS KMS](#) in the *Amazon Simple Storage Service Developer Guide*.

Important

When you replicate objects that are encrypted with AWS KMS, the AWS KMS request rate doubles in the source Region and increases in the destination Region by the same amount. These increased call rates to AWS KMS are due to the way that data is re-encrypted using the customer master key (CMK) that you define for the replication destination Region. AWS KMS has a request rate limit that is per calling account per Region. For information about the limit defaults, see [AWS KMS Limits - Requests per Second: Varies](#) in the *AWS Key Management Service Developer Guide*.

If your current Amazon S3 PUT object request rate during replication is more than half the default AWS KMS rate limit for your account, we recommend that you request an increase to your AWS KMS request rate limit. To request an increase, create a case in the AWS Support Center at [Contact Us](#). For example, suppose that your current PUT object request rate is 1,000 requests per second and you use AWS KMS to encrypt your objects. In this case, we recommend that you ask AWS Support to increase your AWS KMS rate limit to 2,500 requests per second, in both your source and destination Regions (if different), to ensure that there is no throttling by AWS KMS.

To see your PUT object request rate in the source bucket, view `PutRequests` in the Amazon CloudWatch request metrics for Amazon S3. For information about viewing CloudWatch metrics, see [How do I create a request metrics filter for all the objects in my S3 bucket? \(p. 55\)](#)

If you chose to replicate objects encrypted with AWS KMS, enter the Amazon Resource Name (ARN) of the AWS KMS CMK to use to encrypt the replicas in the destination bucket. You can find the ARN for your AWS KMS CMK in the IAM console, under **Encryption keys**. Or, you can choose a CMK name from the drop-down list.

For more information about creating an AWS KMS CMK, see [Creating Keys](#) in the *AWS Key Management Service Developer Guide*.

Important

The Amazon S3 console lists only 100 AWS KMS CMKs per AWS Region. If you have more than 100 CMKs in the same Region, you can see only the first 100 CMKs in the S3 console. To use a KMS CMK that is not listed in the console, choose **Custom KMS ARN**, and enter the KMS CMK ARN.

12. To finish, choose **Save**.
13. After you save your rule, you can edit, enable, disable, or delete your rule by selecting your rule and choosing **Edit rule**.

Grant the source bucket owner permission to encrypt using the AWS KMS CMK

You must grant permissions to the account of the source bucket owner to encrypt using your AWS KMS CMK with a key policy. The following procedure describes how to use the AWS Identity and Access Management (IAM) console to modify the key policy for the AWS KMS CMK that is being used to encrypt the replica objects in the destination bucket.

To grant permissions to encrypt using your AWS KMS CMK

1. Sign in to the AWS Management Console using the AWS account that owns the AWS KMS CMK. Open the AWS KMS console at <https://console.aws.amazon.com/kms>.

2. Choose the alias of the CMK that you want to encrypt with.
3. In the **Key Policy** section of the page, choose **Switch to policy view**.
4. Choose **Edit** to edit **Key Policy**.
5. Using the **Key Policy** editor, insert the key policy provided by Amazon S3 into the existing key policy, and then choose **Save Changes**. You might want to add the policy to the end of the existing policy.

For more information about creating and editing AWS KMS CMKs, see [Getting Started](#) in the *AWS Key Management Service Developer Guide*.

More info

- [How do I manage the replication rules for an S3 Bucket?](#) (p. 50)
- [How do I enable or suspend versioning for an S3 bucket?](#) (p. 7)
- [Replication](#) in the *Amazon Simple Storage Service Developer Guide*

How do I manage the replication rules for an S3 Bucket?

Replication is the automatic, asynchronous copying of objects across buckets in the same or different AWS Regions. It replicates newly created objects and object updates from a source bucket to a specified destination bucket.

You use the Amazon S3 console to add replication rules to the source bucket. Replication rules define the source bucket objects to replicate and the destination bucket where the replicated objects are stored. For more information about replication, see [Replication](#) in the *Amazon Simple Storage Service Developer Guide*.

You can manage replication rules on the **Replication** page. You can add, view, enable, disable, delete, and change the priority of the replication rules. For information about adding replication rules to a bucket, see [How do I add a replication rule to an S3 bucket?](#) (p. 46).

To manage the replication rules for an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want.
3. Choose **Management**, and then scroll down to **Replication rules**.
4. You change the replication rules in the following ways.
 - To enable or disable a replication rule, select the rule, choose **Actions**, and in the drop-down list, choose **Enable rule** or **Disable rule**. You can also disable, enable, or delete all the rules in the bucket from the **Actions** drop-down list.
 - To change the rule priorities, select the rule and choose **Edit**, which starts the Replication wizard to help you make the change. For information about using the wizard, see [How do I add a replication rule to an S3 bucket?](#) (p. 46).

You set rule priorities to avoid conflicts caused by objects that are included in the scope of more than one rule. In the case of overlapping rules, Amazon S3 uses the rule priority to determine which rule to apply. The higher the number, the higher the priority. For more information about rule priority, see [Replication Configuration Overview](#) in the *Amazon Simple Storage Service Developer Guide*.

More info

- [How do I add a replication rule to an S3 bucket? \(p. 46\)](#)
- [Replication](#) in the *Amazon Simple Storage Service Developer Guide*

How Do I Configure Storage Class Analysis?

By using the Amazon S3 analytics storage class analysis tool, you can analyze storage access patterns to help you decide when to transition the right data to the right storage class. Storage class analysis observes data access patterns to help you determine when to transition less frequently accessed STANDARD storage to the STANDARD_IA (IA, for infrequent access) storage class. For more information about STANDARD_IA, see the [Amazon S3 FAQ](#) and [Storage Classes](#) in the *Amazon Simple Storage Service Developer Guide*.

Important

Storage class analysis does not give recommendations for transitions to the ONEZONE_IA or S3 Glacier storage classes.

For more information about analytics, see [Amazon S3 Analytics – Storage Class Analysis](#) in the *Amazon Simple Storage Service Developer Guide*.

To configure storage class analysis

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket for which you want to configure storage class analysis.
3. Choose the **Metrics** tab.
4. Under **Storage Class Analysis**, choose **Create analytics configuration**.
5. Type a name for the filter. If you want to analyze the whole bucket, leave the **Prefix** field empty.
6. In the **Prefix** field, type text for the prefix for the objects that you want to analyze.
7. To add a tag, choose **Add tag**. Enter a key and value for the tag. You can enter one prefix and multiple tags.
8. Optionally, you can choose **Enable** under **Export CSV** to export analysis reports to a comma-separated values (.csv) flat file. Choose a destination bucket where the file can be stored. You can type a prefix for the destination bucket. The destination bucket must be in the same AWS Region as the bucket for which you are setting up the analysis. The destination bucket can be in a different AWS account.
9. Choose **Create Configuration**.

Amazon S3 creates a bucket policy on the destination bucket that grants Amazon S3 write permission. This allows it to write the export data to the bucket.

Note

This action configures storage class analysis for all specified buckets.

If an error occurs when you try to create the bucket policy, you'll be given instructions on how to fix it. For example, if you chose a destination bucket in another AWS account and do not have permissions to read and write to the bucket policy, you'll see the following message. You must have the destination bucket owner add the displayed bucket policy to the destination bucket. If the policy is not added to the destination bucket you won't get the export data because Amazon S3 doesn't have permission to write

to the destination bucket. If the source bucket is owned by a different account than that of the current user, then the correct account ID of the source bucket must be substituted in the policy.

For information about the exported data and how the filter works, see [Amazon S3 Analytics – Storage Class Analysis](#) in the *Amazon Simple Storage Service Developer Guide*.

More Info

[Storage management \(p. 44\)](#)

How Do I Configure Amazon S3 Inventory?

Amazon S3 inventory provides a flat file list of your objects and metadata, which is a scheduled alternative to the Amazon S3 synchronous `List` API operation. Amazon S3 inventory provides comma-separated values (CSV) or [Apache optimized row columnar \(ORC\)](#) or [Apache Parquet \(Parquet\)](#) output files that list your objects and their corresponding metadata on a daily or weekly basis for an S3 bucket or for objects that share a prefix (objects that have names that begin with the same string). For more information, see [Amazon S3 Inventory](#) in the *Amazon Simple Storage Service Developer Guide*.

To configure inventory

Note

It may take up to 48 hours to deliver the first report.

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket for which you want to configure Amazon S3 inventory.
3. Choose **Management**.
4. Under **Inventory configurations**, choose **Create inventory configuration**.
5. In **Inventory configuration name**, enter a name.
6. Set the **Inventory scope**:
 - Enter an optional prefix.
 - Choose object versions: **Current versions only** or **Include all versions**.
7. Under **Report details**, choose the location of the AWS account that you want to save the reports to: **This account** or **A different account**.
8. Under **Destination**, choose the destination bucket where you want reports to be saved.

The destination bucket must be in the same AWS Region as the bucket for which you are setting up the inventory. The destination bucket can be in a different AWS account. Under the **Destination** bucket field, you see the **Destination bucket permission** that is added to the destination bucket policy to allow Amazon S3 to place data in that bucket. For more information, see [Destination Bucket Policy \(p. 53\)](#).
9. Under **Frequency**, choose how often the report will be generated: **Daily** or **Weekly**.
10. Choose the **Output format** for the report:
 - **CSV**
 - **Apache ORC**
 - **Apache Parquet**
11. Under **Status**, choose **Enable** or **Disable**.
12. To use server-side encryption, under **Server-side encryption**, follow these steps:
 - a. Choose **Enable**.

- b. Under **Encryption key type**, choose **Amazon S3 key (SSE-S3)** or **AWS Key Management Service key (SSE-KMS)**.

Amazon S3 server-side encryption uses 256-bit Advanced Encryption Standard (AES-256). For more information, see [Amazon S3-Managed Encryption Keys \(SSE-S3\)](#) in the *Amazon Simple Storage Service Developer Guide*. For more information about SSE-KMS, see [AWS KMS CMKs](#) in the *Amazon Simple Storage Service Developer Guide*.

- c. To use a AWS KMS CMK, choose one of the following:

- **AWS managed key (aws/s3)**
- **Choose from your KMS master keys**, and choose your **KMS master key**.
- **Enter KMS master key ARN**, and enter your AWS KMS key ARN.

Note

To encrypt the inventory list file with SSE-KMS, you must grant Amazon S3 permission to use the AWS KMS CMK. For instructions, see [Grant Amazon S3 Permission to Encrypt Using Your AWS KMS CMK \(p. 54\)](#).

13. For **Additional fields**, select one or more of the following to add to the inventory report:

- **Size** – Object size in bytes.
- **Last modified date** – The object creation date or the last modified date, whichever is the latest.
- **Storage class** – The storage class used for storing the object.
- **ETag** – The entity tag is a hash of the object. The ETag reflects changes only to the contents of an object, and not its metadata. The ETag may or may not be an MD5 digest of the object data. Whether it is depends on how the object was created and how it is encrypted.
- **Multipart upload** – Specifies that the object was uploaded as a multipart upload. For more information, see [Multipart Upload Overview](#) in the *Amazon Simple Storage Service Developer Guide*.
- **Replication status** – The replication status of the object. For more information, see [How do I add a replication rule to an S3 bucket? \(p. 46\)](#).
- **Encryption status** – The server-side encryption used to encrypt the object. For more information, see [Protecting Data Using Server-Side Encryption](#) in the *Amazon Simple Storage Service Developer Guide*.
- **S3 Object Lock configurations** – The Object Lock status of the object, including the following settings:
 - **Retention mode** – The level of protection applied to the object, either *Governance* or *Compliance*.
 - **Retain until date** – The date until which the locked object cannot be deleted.
 - **Legal hold status** – The legal hold status of the locked object.

For information about S3 Object Lock, see [S3 Object Lock Overview](#) in the *Amazon Simple Storage Service Developer Guide*.

For more information about the contents of an inventory report, see [What's Included in an Amazon S3 Inventory?](#) in the *Amazon Simple Storage Service Developer Guide*.

14. Choose **Create**.

Destination Bucket Policy

Amazon S3 creates a bucket policy on the destination bucket that grants Amazon S3 write permission. This allows Amazon S3 to write data for the inventory reports to the bucket.

If an error occurs when you try to create the bucket policy, you are given instructions on how to fix it. For example, if you choose a destination bucket in another AWS account and don't have permissions to read and write to the bucket policy, you see an error message.

In this case, the destination bucket owner must add the displayed bucket policy to the destination bucket. If the policy is not added to the destination bucket, you won't get an inventory report because Amazon S3 doesn't have permission to write to the destination bucket. If the source bucket is owned by a different account than that of the current user, the correct account ID of the source bucket must be substituted in the policy.

For more information, see [Amazon S3 Inventory](#) in the *Amazon Simple Storage Service Developer Guide*.

Granting Amazon S3 Permission to Use Your AWS KMS CMK for Encryption

To grant Amazon S3 permission to encrypt using a customer managed AWS Key Management Service (AWS KMS) customer master key (CMK), you must use a key policy. To update your key policy so that you can use an AWS KMS customer managed CMK to encrypt the inventory file, follow the steps below.

To grant permissions to encrypt using your AWS KMS CMK

1. Using the AWS account that owns the customer managed CMK, sign into the AWS Management Console.
2. Open the AWS KMS console at <https://console.aws.amazon.com/kms>.
3. To change the AWS Region, use the Region selector in the upper-right corner of the page.
4. In the left navigation pane, choose **Customer managed keys**.
5. Under **Customer managed keys**, choose the customer managed CMK that you want to use to encrypt the inventory file.
6. Under **Key policy**, choose **Switch to policy view**.
7. To update the key policy, choose **Edit**.
8. Under **Edit key policy**, add the following key policy to the existing key policy.

```
{
  "Sid": "Allow Amazon S3 use of the CMK",
  "Effect": "Allow",
  "Principal": {
    "Service": "s3.amazonaws.com"
  },
  "Action": [
    "kms:GenerateDataKey"
  ],
  "Resource": "*"
}
```

9. Choose **Save changes**.

For more information about creating customer managed CMKs AWS KMS and using key policies, see the following links in the *AWS Key Management Service Developer Guide*:

- [Getting Started](#)
- [Using Key Policies in AWS KMS](#)

More Info

[Storage management \(p. 44\)](#)

How do I create a request metrics filter for all the objects in my S3 bucket?

There are three types of Amazon CloudWatch metrics for Amazon S3: storage metrics, request metrics, and replication metrics. Storage metrics are reported once per day and are provided to all customers at no additional cost. Request metrics are available at one-minute intervals after some latency to process. Request metrics are billed at the standard CloudWatch rate. You must opt into request metrics by configuring them in the console or using the Amazon S3 API.

For more information about CloudWatch metrics for Amazon S3, see [Monitoring metrics with Amazon CloudWatch](#) in the *Amazon Simple Storage Service Developer Guide*.

To create a request metrics filter

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that contains the objects you want request metrics for.
3. Choose the **Metrics** tab.
4. Under **Bucket metrics**, choose **View additional charts**.
5. Choose the **Request metrics** tab.
6. Choose **Create filter**.
7. In the **Filter name** box, enter your filter name.

Names can only contain letters, numbers, periods, dashes, and underscores. We recommend using the name `EntireBucket` for a filter that applies to all objects.

8. Under **Choose a filter scope**, choose **This filter applies to all objects in the bucket**.

You can also define a filter so that the metrics are only collected and reported on a subset of objects in the bucket. For more information, see [How do I create a request metrics filter that limits scope by object tag or prefix?](#) (p. 55)

9. Choose **Create filter**.
10. On the **Request metrics** tab, under **Filters**, choose the filter that you just created.

After about 15 minutes, CloudWatch begins tracking these request metrics. You can see them on the **Request metrics** tab. You can see graphs for the metrics on the Amazon S3 or CloudWatch console. Request metrics are billed at the standard CloudWatch rate. For more information, see [Amazon CloudWatch pricing](#).

How do I create a request metrics filter that limits scope by object tag or prefix?

There are three types of Amazon CloudWatch metrics for Amazon S3: storage metrics, request metrics, and replication metrics. Storage metrics are reported once per day and are provided to all customers at no additional cost. Request metrics are available at one-minute intervals after some latency to process. Request metrics are billed at the standard CloudWatch rate. You must opt into request metrics by configuring them in the console or using the Amazon S3 API.

For more information about CloudWatch metrics for Amazon S3, see [Monitoring metrics with Amazon CloudWatch](#) in the *Amazon Simple Storage Service Developer Guide*.

To filter request metrics on a subset of objects in a bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that contains the objects you want request metrics for.
3. Choose the **Metrics** tab.
4. Under **Bucket metrics**, choose **View additional charts**.
5. Choose the **Request metrics** tab.
6. Choose **Create filter**.
7. In the **Filter name** box, enter your filter name.

Names can only contain letters, numbers, periods, dashes, and underscores.

8. Under **Choose a filter scope**, choose **Limit the scope of this filter using prefix and tags**.
9. (Optional) In the **Prefix** box, enter a prefix to limit the scope of the filter to a single path.
10. (Optional) Under **Tags**, enter a tag **Key** and **Value**.
11. Choose **Create filter**.

Amazon S3 creates a filter that uses the tags or prefixes you specified.

12. On the **Request metrics** tab, under **Filters**, choose the filter that you just created.

You have now created a filter that limits the request metrics scope by object tags and prefixes. About 15 minutes after CloudWatch begins tracking these request metrics, you can see charts for the metrics on both the Amazon S3 and CloudWatch consoles. Request metrics are billed at the standard CloudWatch rate. For more information, see [Amazon CloudWatch pricing](#).

You can also configure request metrics at the bucket level. For information, see [How do I create a request metrics filter for all the objects in my S3 bucket? \(p. 55\)](#)

How do I delete a request metrics filter?

In the Amazon S3 console, you can delete a request metrics filter. When you delete a filter, you are no longer charged for request metrics that use that *specific filter*. However, you will continue to be charged for any other filter configurations that exist. When you delete a filter, you can no longer use the filter for request metrics. Deleting a filter cannot be undone.

For more information about creating a request metrics filter, see [How do I create a request metrics filter for all the objects in my S3 bucket? \(p. 55\)](#) and [How do I create a request metrics filter that limits scope by object tag or prefix? \(p. 55\)](#)

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose your bucket name.
3. Choose the **Metrics** tab.
4. Under **Bucket metrics**, choose **View additional charts**.
5. Choose the **Request metrics** tab.
6. Choose **Manage filters**.
7. Choose your filter.

Important

Deleting a filter cannot be undone.

8. Choose **Delete**.

Amazon S3 deletes your filter.

How do I view replication metrics?

There are three types of Amazon CloudWatch metrics for Amazon S3: storage metrics, request metrics, and replication metrics. *Replication* metrics are turned on automatically when you enable replication with S3 Replication Time Control (S3 RTC) using the AWS Management Console or the Amazon S3 API. Replication metrics are available 15 minutes after you enable a replication rule with S3 Replication Time Control (S3 RTC).

Replication metrics track the rule IDs of the replication configuration. A replication rule ID can be specific to a prefix, a tag, or a combination of both. For more information about S3 Replication Time Control (S3 RTC), see [Replicating Objects Using S3 Replication Time Control \(S3 RTC\)](#) in the *Amazon Simple Storage Service Developer Guide*.

For more information about CloudWatch metrics for Amazon S3, see [Monitoring Metrics with Amazon CloudWatch](#) in the *Amazon Simple Storage Service Developer Guide*.

Prerequisites

Enable a replication rule that has S3 RTC.

To view replication metrics

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that contains the objects you want replication metrics for.
3. Choose the **Metrics** tab.
4. Under **Replication metrics**, choose **Replication rules**.
5. Choose **Display charts**.

Amazon S3 displays **Replication Latency (in seconds)**, **Operations pending replication** in charts.

6. To view all replication metrics, including **Bytes pending replication**, **Replication Latency (in seconds)**, and **Operations pending replication** together on a separate page, choose **View 1 more chart**.

You can then view the replication metrics **Replication Latency (in seconds)**, **Operations pending replication**, and **Bytes pending replication** for the rules that you selected. Amazon CloudWatch begins reporting replication metrics 15 minutes after you enable S3 RTC on the respective replication rule. You can view replication metrics on the Amazon S3 or CloudWatch console. For information, see [Replication metrics overview](#) in the *Amazon Simple Storage Service Developer Guide*.

Setting bucket and object access permissions

This section explains how to use the Amazon Simple Storage Service (Amazon S3) console to grant access permissions to your buckets and objects. It also explains how to use Amazon S3 block public access to prevent the application of any settings that allow public access to data within S3 buckets.

Buckets and objects are Amazon S3 resources. You grant access permissions to your buckets and objects by using resource-based access policies. You can associate an access policy with a resource. An access policy describes who has access to resources. The resource owner is the AWS account that creates the resource. For more information about resource ownership and access policies, see [Overview of Managing Access](#) in the *Amazon Simple Storage Service Developer Guide*.

Bucket access permissions specify which users are allowed access to the objects in a bucket and which types of access they have. *Object access permissions* specify which users are allowed access to the object and which types of access they have. For example, one user might have only read permission, while another might have read and write permissions.

Bucket and object permissions are independent of each other. An object does not inherit the permissions from its bucket. For example, if you create a bucket and grant write access to a user, you can't access that user's objects unless the user explicitly grants you access. Bucket permissions generally allow a user to list information about a bucket and add and delete objects from a bucket. Object permissions generally allow a user to download, replace or delete objects.

Note

You do not necessarily need to grant bucket permissions in order to grant object permissions, and vice versa. For example, you can use the AWS console to grant a user update permissions on an object without granting that user permissions to the bucket containing that object. However, if you were to grant permissions only to the object, and not the bucket, the grantee would not be able to use the AWS console to access the object. (They would not be able to view the object in the console because they would not be able to view the bucket containing the object.) The grantee instead would have to access the object programmatically, such as with the AWS CLI.

To grant access to your buckets and objects to other AWS accounts and to the general public, you use resource-based access policies known as *access control lists* (ACLs).

A *bucket policy* is a resource-based AWS Identity and Access Management (IAM) policy that grants other AWS accounts or IAM users access to an S3 bucket. Bucket policies supplement, and in many cases, replace ACL-based access policies. For more information about using IAM with Amazon S3, see [Managing Access Permissions to Your Amazon S3 Resources](#) in the *Amazon Simple Storage Service Developer Guide*.

For more in-depth information about managing access permissions, see [Introduction to Managing Access Permissions to Your Amazon S3 Resources](#) in the *Amazon Simple Storage Service Developer Guide*.

This section also explains how to use the Amazon S3 console to add a cross-origin resource sharing (CORS) configuration to an S3 bucket. CORS allows client web applications that are loaded in one domain to interact with resources in another domain.

Topics

- [How do I block public access to S3 buckets? \(p. 59\)](#)
- [How do I edit public access settings for S3 buckets? \(p. 60\)](#)

- [How do I edit public access settings for all the S3 buckets in an AWS account?](#) (p. 60)
- [How do I set permissions on an object?](#) (p. 61)
- [How do I set ACL bucket permissions?](#) (p. 62)
- [How do I add an S3 Bucket policy?](#) (p. 64)
- [How do I add cross-domain resource sharing with CORS?](#) (p. 65)
- [Setting S3 Object Ownership to bucket owner preferred in the AWS Management Console](#) (p. 66)
- [Using Access Analyzer for S3](#) (p. 66)

How do I block public access to S3 buckets?

Amazon S3 block public access prevents the application of any settings that allow public access to data within S3 buckets. You can configure block public access settings for an individual S3 bucket or for all the buckets in your account. For information about blocking public access using the AWS CLI, AWS SDKs, and the Amazon S3 REST APIs, see [Using Amazon S3 Block Public Access](#) in the *Amazon Simple Storage Service Developer Guide*.

The following topics explain how to use the Amazon S3 console to configure block public access settings:

- [How do I edit public access settings for S3 buckets?](#) (p. 60)
- [How do I edit public access settings for all the S3 buckets in an AWS account?](#) (p. 60)

The following sections explain viewing bucket access status and searching by access types.

Viewing access status

The list buckets view shows whether your bucket is publicly accessible. Amazon S3 labels the permissions for a bucket as follows:

- **Public** – Everyone has access to one or more of the following: List objects, Write objects, Read and write permissions.
- **Objects can be public** – The bucket is not public, but anyone with the appropriate permissions can grant public access to objects.
- **Buckets and objects not public** – The bucket and objects do not have any public access.
- **Only authorized users of this account** – Access is isolated to IAM users and roles in this account and AWS service principals because there is a policy that grants public access.

The access column shows the access status of the listed buckets.

You can also filter bucket searches by access type. Choose an access type from the drop-down list that is next to the **Search for buckets** bar.

More info

- [How do I edit public access settings for S3 buckets?](#) (p. 60)
- [How do I edit public access settings for all the S3 buckets in an AWS account?](#) (p. 60)
- [Setting bucket and object access permissions](#) (p. 58)
- [Restricting Access Using an Origin Access Identity](#) in the *Amazon Simple Storage Service Developer Guide*

- [Accessing Private Content in Amazon CloudFront](#) in the *AWS Developer Blog*

How do I edit public access settings for S3 buckets?

Amazon S3 Block Public Access prevents the application of any settings that allow public access to data within S3 buckets. This section describes how to edit Block Public Access settings for one or more S3 buckets. For information about blocking public access using the AWS CLI, AWS SDKs, and the Amazon S3 REST APIs, see [Using Amazon S3 Block Public Access](#) in the *Amazon Simple Storage Service Developer Guide*.

Topics

- [Editing public access settings for an S3 bucket](#) (p. 60)
- [More info](#) (p. 60)

Editing public access settings for an S3 bucket

Follow these steps if you need to change the public access settings for a single S3 bucket.

To edit the Amazon S3 block public access settings for an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want.
3. Choose **Permissions**.
4. Choose **Edit** to change the public access settings for the bucket. For more information about the four Amazon S3 Block Public Access Settings, see [Block Public Access Settings](#) in the *Amazon Simple Storage Service Developer Guide*.
5. Choose the setting that you want to change, and then choose **Save changes**.
6. When you're asked for confirmation, enter **confirm**. Then choose **Confirm** to save your changes.

You can change Amazon S3 Block Public Access settings when you create a bucket. For more information, see [How do I create an S3 Bucket?](#) (p. 3).

More info

- [How do I block public access to S3 buckets?](#) (p. 59)
- [How do I edit public access settings for all the S3 buckets in an AWS account?](#) (p. 60)
- [Setting bucket and object access permissions](#) (p. 58)

How do I edit public access settings for all the S3 buckets in an AWS account?

Amazon S3 block public access prevents the application of any settings that allow public access to data within S3 buckets. This section describes how to edit block public access settings for all the S3 buckets in your AWS account. For information about blocking public using the AWS CLI, AWS SDKs, and the Amazon

S3 REST APIs, see [Using Amazon S3 Block Public Access](#) in the *Amazon Simple Storage Service Developer Guide*.

To edit block public access settings for all the S3 buckets in an AWS account

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. Choose **Account settings for Block Public Access**.
3. Choose **Edit** to change the block public access settings for all the buckets in your AWS account.
4. Choose the settings that you want to change, and then choose **Save changes**.
5. When you're asked for confirmation, enter **confirm**. Then choose **Confirm** to save your changes.

More info

- [How do I block public access to S3 buckets?](#) (p. 59)
- [How do I edit public access settings for S3 buckets?](#) (p. 60)
- [Setting bucket and object access permissions](#) (p. 58)

How do I set permissions on an object?

This section explains how to use the Amazon Simple Storage Service (Amazon S3) console to manage access permissions for an Amazon S3 object by using access control lists (ACLs). ACLs are resource-based access policies that grant access permissions to buckets and objects. For more information about managing access permissions with resource-based policies, see [Overview of Managing Access](#) in the *Amazon Simple Storage Service Developer Guide*.

Bucket and object permissions are independent of each other. An object does not inherit the permissions from its bucket. For example, if you create a bucket and grant write access to a user, you can't access that user's objects unless the user explicitly grants you access.

You can grant permissions to other AWS accounts or predefined groups. The user or group that you grant permissions to is called the *grantee*. By default, the owner, which is the AWS account that created the bucket, has full permissions.

Each permission you grant for a user or a group adds an entry in the ACL that is associated with the object. The ACL lists grants, which identify the grantee and the permission granted. For more information about ACLs, see [Managing Access with ACLs](#) in the *Amazon Simple Storage Service Developer Guide*.

To set permissions for an object

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that contains the objects for which you want to set permissions.
3. Choose the **Permissions** tab that appears in the list of tabs under the **Bucket overview** section.
4. To edit *Block Public Access settings*, choose **Edit** to block or allow public access to this bucket and its access points. For more information, see [Blocking public access](#) (p. 59).
5. To edit *Bucket policy*, choose **Edit** to edit the JSON bucket policy that provides access to objects stored in this bucket. This policy only applies to objects owned by your account.

Alternatively, if you have an existing bucket policy, you can choose **Delete** to delete an existing bucket policy. For more information, see [Adding a bucket policy](#) (p. 64).

6. To edit *Object ownership*, choose **Edit** to assume ownership of new objects uploaded to this bucket. For more information, see [??? \(p. 66\)](#).
7. To edit the *Access control list (ACL)*, choose **Edit** to update permissions (list, read, and write) to grantee groups such as *Bucket owner* (your AWS account), *Everyone*, *Authenticated users* (anyone with an AWS account), or *S3 log delivery group*.
 - a. The *Bucket owner* refers to your AWS account, and not an AWS Identity and Access Management (IAM) user. For more information about the root user, see [AWS Account Root User](#) in the *IAM User Guide*.
 - b. To grant access to your object to *Everyone*, choose **Everyone**. Granting public access permissions means that anyone in the world can access the object.

Warning

- Use caution when granting the **Everyone** group anonymous access to your Amazon S3 objects. When you grant access to this group, anyone in the world can access your object. If you need to grant access to everyone, we highly recommend that you only grant permissions to **Read objects**.
 - We highly recommend that you *do not* grant the **Everyone** group write object permissions. Doing so allows anyone to overwrite the ACL permissions for the object.
- c. To grant permissions to an AWS user from a different AWS account, enter the canonical ID of the AWS user that you want to grant object permissions to. For information about finding a canonical ID, see [AWS Account Identifiers](#) in the *Amazon Web Services General Reference*. You can add as many as 99 users.
 - d. To specify the *S3 log delivery group*, provide the name of the target bucket where you want Amazon S3 to save the access logs as objects.

For more information, see [Setting ACL bucket permissions \(p. 62\)](#) and [How to enable server access logging](#) in the *Amazon Simple Storage Service Developer Guide*.

8. To edit *Cross-origin resource sharing (CORS)*, choose **Edit** to create a CORS configuration, which is an XML document that defines how client web applications that are loaded in one domain interact with resources in a different domain. For more information, see [Adding cross-domain resource sharing with CORS \(p. 65\)](#).
9. After editing any of the settings in the previous steps, choose **Save changes** when you are finished.

Note

This action applies permissions to all specified objects. When applying permissions to folders, wait for the save operation to finish before adding new objects.

You can also set object permissions when you upload objects. For more information about setting permissions when uploading objects, see [Uploading S3 objects \(p. 24\)](#).

More Info

- [Setting bucket and object access permissions \(p. 58\)](#)
- [How do I set ACL bucket permissions? \(p. 62\)](#)

How do I set ACL bucket permissions?

This section explains how to use the Amazon Simple Storage Service (Amazon S3) console to manage access permissions for S3 buckets by using access control lists (ACLs). ACLs are resource-based access policies that grant access permissions to buckets and objects. For more information about managing

access permissions with resource-based policies, see [Overview of Managing Access](#) in the *Amazon Simple Storage Service Developer Guide*.

You can grant permissions to other AWS account users or to predefined groups. The user or group that you are granting permissions to is called the *grantee*. By default, the owner, which is the AWS account that created the bucket, has full permissions.

Each permission you grant for a user or group adds an entry in the ACL that is associated with the bucket. The ACL lists grants, which identify the grantee and the permission granted. For more information about ACLs, see [Managing Access with ACLs](#) in the *Amazon Simple Storage Service Developer Guide*.

Warning

We highly recommend that you avoid granting write access to the **Everyone (public access)** or **Authenticated Users group (all AWS authenticated users)** groups. For more information about the effects of granting write access to these groups, see [Amazon S3 Predefined Groups](#) in the *Amazon Simple Storage Service Developer Guide*.

To set ACL access permissions for an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want to set permissions for.
3. Choose **Permissions**, and then choose **Edit** within **Access Control List (ACL)**.
4. You can manage bucket access permissions for the following:

- a. **Access for your AWS account root user**

The *owner* refers to the AWS account root user, and not an AWS Identity and Access Management (IAM) user. For more information about the root user, see [The AWS Account Root User](#) in the *IAM User Guide*.

To change the owner's bucket access permissions, select the checkboxes for the permissions under **Bucket owner (your AWS account)**.

- b. **Access for other AWS accounts**

To grant permissions to an AWS user from a different AWS account, choose **Add grantee**. In the **Enter a canonical ID** field, enter the canonical ID or email of the AWS user that you want to grant bucket permissions to. For information about finding a canonical ID, see [AWS Account Identifiers](#) in the *Amazon Web Services General Reference*. You can add as many as 99 users.

Select the check boxes next to the permissions that you want to grant to the user, and then choose **Save changes**.

Warning

When you grant other AWS accounts access to your resources, be aware that the AWS accounts can delegate their permissions to users under their accounts. This is known as *cross-account access*. For information about using cross-account access, see [Creating a Role to Delegate Permissions to an IAM User](#) in the *IAM User Guide*.

- c. **Public access**

To grant access to your bucket to the general public (everyone in the world), under **Public access**, choose **Everyone**. Granting public access permissions means that anyone in the world can access the bucket. Select the check boxes for the permissions that you want to grant, and then choose **Save**.

To undo public access to your bucket, under **Public access**, choose **Everyone**. Clear all the permissions check boxes, and then choose **Save**.

Warning

Use caution when granting the **Everyone** group public access to your S3 bucket. When you grant access to this group, anyone in the world can access your bucket. We highly recommend that you never grant any kind of public write access to your S3 bucket.

d. S3 log delivery group

To grant access to Amazon S3 to write server access logs to the bucket, under **S3 log delivery group**, choose **Log Delivery**.

If a bucket is set up as the target bucket to receive access logs, the bucket permissions must allow the **Log Delivery** group write access to the bucket. When you enable server access logging on a bucket, the Amazon S3 console grants write access to the **Log Delivery** group for the target bucket that you choose to receive the logs. For more information about server access logging, see [How do I enable server access logging for an S3 bucket? \(p. 9\)](#).

You can also set bucket permissions when you are creating a bucket. For more information about setting permissions when creating a bucket, see [How do I create an S3 Bucket? \(p. 3\)](#).

More info

- [Setting bucket and object access permissions \(p. 58\)](#)
- [How do I set permissions on an object? \(p. 61\)](#)
- [How do I add an S3 Bucket policy? \(p. 64\)](#)

How do I add an S3 Bucket policy?

This section explains how to use the Amazon Simple Storage Service (Amazon S3) console to add a new bucket policy or edit an existing bucket policy. A bucket policy is a resource-based AWS Identity and Access Management (IAM) policy. You add a bucket policy to a bucket to grant other AWS accounts or IAM users access permissions for the bucket and the objects in it. Object permissions apply only to the objects that the bucket owner creates. For more information about bucket policies, see [Overview of Managing Access](#) in the *Amazon Simple Storage Service Developer Guide*.

For examples of Amazon S3 bucket policies, see [Bucket Policy Examples](#) in the *Amazon Simple Storage Service Developer Guide*.

To create or edit a bucket policy

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want to create a bucket policy for or whose bucket policy you want to edit.
3. Choose **Permissions**.
4. (Optional) Choose **Policy generator** to open the AWS Policy Generator in a new window. On the policy generator page, select **S3 Bucket Policy** from the **Select Type of Policy** dropdown menu. Add one or more statements by populating the fields presented, and then choose **Generate Policy**. Copy the generated policy text and return to the **Edit bucket policy** page in the Amazon S3 console.
5. Under **Bucket policy**, choose **Edit**.
6. In the **Policy** text field, type or copy and paste a new bucket policy, or edit an existing policy. The bucket policy is a JSON file. The text you type in the editor must be valid JSON.

Note

For convenience, the console displays the Amazon Resource Name (ARN) of the current bucket above the **Policy** text field. You can copy this ARN for use in the policy. For more information about ARNs, see [Amazon Resource Names \(ARNs\)](#) and [AWS Service Namespaces](#) in the *Amazon Web Services General Reference*.

7. Choose **Save**.

More info

- [Setting bucket and object access permissions](#) (p. 58)
- [How do I set ACL bucket permissions?](#) (p. 62)

How do I add cross-domain resource sharing with CORS?

This section explains how to use the Amazon S3 console to add a cross-origin resource sharing (CORS) configuration to an S3 bucket. CORS allows client web applications that are loaded in one domain to interact with resources in another domain.

To configure your bucket to allow cross-origin requests, you add CORS configuration to the bucket. A CORS configuration is a document that defines rules that identify the origins that you will allow to access your bucket, the operations (HTTP methods) supported for each origin, and other operation-specific information. In the S3 console, the CORS configuration must be a JSON document. For more information about CORS and examples, see [Cross-Origin Resource Sharing \(CORS\)](#) in the *Amazon Simple Storage Service Developer Guide*.

When you enable CORS on the bucket, the access control lists (ACLs) and other access permission policies continue to apply.

Important

In the new S3 console, the CORS configuration must be JSON.

To add a CORS configuration to an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want to create a bucket policy for.
3. Choose **Permissions**.
4. In the **Cross-origin resource sharing (CORS)** section, choose **Edit**.
5. In the **Cross-origin resource sharing (CORS)** text box, type or copy and paste a new CORS configuration, or edit an existing configuration.

In the S3 console, the CORS configuration is a JSON file. The text that you type in the editor must be valid JSON. For more information and examples, see [How Do I Configure CORS on My Bucket?](#)

6. Choose **Save changes**.

Note

Amazon S3 displays the Amazon Resource Name (ARN) for the bucket next to the **CORS configuration editor** title. For more information about ARNs, see [Amazon Resource Names \(ARNs\)](#) and [AWS Service Namespaces](#) in the *Amazon Web Services General Reference*.

More info

- [Setting bucket and object access permissions](#) (p. 58)
- [How do I set ACL bucket permissions?](#) (p. 62)
- [How do I add an S3 Bucket policy?](#) (p. 64)

Setting S3 Object Ownership to bucket owner preferred in the AWS Management Console

S3 Object Ownership is currently under preview and can be configured through the AWS Management Console, AWS Command Line Interface, AWS SDKs, or Amazon S3 REST APIs. AWS CloudFormation support is planned for general availability.

S3 Object Ownership enables you to take ownership of new objects that other AWS accounts upload to your bucket with the `bucket-owner-full-control` canned access control list (ACL). This section describes how to set Object Ownership using the console.

Setting Object Ownership to bucket owner preferred on an S3 bucket

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the **Buckets** list, choose the name of the bucket that you want to enable S3 Object Ownership for.
3. Choose the **Permissions** tab.
4. Choose **Edit** under **Object Ownership**.
5. Choose **Bucket owner preferred**, and then choose **Save**.

How do I ensure that I take ownership of new objects?

With the above steps Object Ownership will take ownership of any new objects that are written by other accounts with the `bucket-owner-full-control` canned ACL. For more information about enforcing Object Ownership, see [How do I ensure that I take ownership of new objects?](#) in the *Amazon Simple Storage Service Developer Guide*.

Using Access Analyzer for S3

Access Analyzer for S3 alerts you to S3 buckets that are configured to allow access to anyone on the internet or other AWS accounts, including AWS accounts outside of your organization. For each public or shared bucket, you receive findings into the source and level of public or shared access. For example, Access Analyzer for S3 might show that a bucket has read or write access provided through a bucket access control list (ACL), a bucket policy, or an access point policy. Armed with this knowledge, you can take immediate and precise corrective action to restore your bucket access to what you intended.

When reviewing an at-risk bucket in Access Analyzer for S3, you can block all public access to the bucket with a single click. We recommend that you block all access to your buckets unless you require public access to support a specific use case. Before you block all public access, ensure that your applications will continue to work correctly without public access. For more information, see [Using Amazon S3 Block Public Access](#) in the *Amazon Simple Storage Service Developer Guide*.

You can also drill down into bucket-level permission settings to configure granular levels of access. For specific and verified use cases that require public access, such as static website hosting, public downloads, or cross-account sharing, you can acknowledge and record your intent for the bucket to remain public or shared by archiving the findings for the bucket. You can revisit and modify these bucket configurations at any time. You can also download your findings as a CSV report for auditing purposes.

Access Analyzer for S3 is available at no extra cost on the Amazon S3 console. Access Analyzer for S3 is powered by AWS Identity and Access Management (IAM) Access Analyzer. To use Access Analyzer for S3 in the Amazon S3 console, you must visit the IAM console and enable IAM Access Analyzer on a per-Region basis.

For more information about IAM Access Analyzer, see [What is Access Analyzer?](#) in the *IAM User Guide*. For more information about Access Analyzer for S3, review the following sections.

Important

- Access Analyzer for S3 requires an account-level analyzer. To use Access Analyzer for S3, you must visit IAM Access Analyzer and create an analyzer that has an account as the zone of trust. For more information, see [Enabling Access Analyzer](#) in *IAM User Guide*.
- When a bucket policy or bucket ACL is added or modified, Access Analyzer generates and updates findings based on the change within 30 minutes. Findings related to account level block public access settings may not be generated or updated for up to 6 hours after you change the settings.

Topics

- [What information does Access Analyzer for S3 provide? \(p. 67\)](#)
- [Enabling Access Analyzer for S3 \(p. 68\)](#)
- [Blocking all public access \(p. 68\)](#)
- [Reviewing and changing bucket access \(p. 69\)](#)
- [Archiving bucket findings \(p. 69\)](#)
- [Activating an archived bucket finding \(p. 70\)](#)
- [Viewing finding details \(p. 70\)](#)
- [Downloading an Access Analyzer for S3 report \(p. 71\)](#)

What information does Access Analyzer for S3 provide?

Access Analyzer for S3 provides findings for buckets that can be accessed outside your AWS account. Buckets that are listed under **Buckets with public access** can be accessed by anyone on the internet. If Access Analyzer for S3 identifies public buckets, you also see a warning at the top of the page that shows you the number of public buckets in your Region. Buckets listed under **Buckets with access from other AWS accounts — including third-party AWS accounts** are shared conditionally with other AWS accounts, including accounts outside of your organization.

For each bucket, Access Analyzer for S3 provides the following information:

- **Bucket name**
- **Discovered by Access analyzer** - When Access Analyzer for S3 discovered the public or shared bucket access.
- **Shared through** - How the bucket is shared—through a bucket policy, a bucket ACL, or an access point policy. A bucket can be shared through both policies and ACLs. If you want to find and review the source for your bucket access, you can use the information in this column as a starting point for taking immediate and precise corrective action.

- **Status** - The status of the bucket finding. Access Analyzer for S3 displays findings for all public and shared buckets.
 - **Active** - Finding has not been reviewed.
 - **Archived** - Finding has been reviewed and confirmed as intended.
 - **All** - All findings for buckets that are public or shared with other AWS accounts, including AWS accounts outside of your organization.
- **Access level** - Access permissions granted for the bucket:
 - **List** - List resources.
 - **Read** - Read but not edit resource contents and attributes.
 - **Write** - Create, delete, or modify resources.
 - **Permissions** - Grant or modify resource permissions.
 - **Tagging** - Update tags associated with the resource.

Enabling Access Analyzer for S3

To use Access Analyzer for S3, you must complete the following prerequisite steps.

1. Grant the required permissions.

For more information, see [Permissions Required to use Access Analyzer](#) in the *IAM User Guide*.

2. Visit IAM to create an account-level analyzer for each Region where you want to use Access Analyzer.

Access Analyzer for S3 requires an account-level analyzer. To use Access Analyzer for S3, you must create an analyzer that has an account as the zone of trust. For more information, see [Enabling Access Analyzer](#) in *IAM User Guide*.

Blocking all public access

If you want to block all access to a bucket in a single click, you can use the **Block all public access** button in Access Analyzer for S3. When you block all public access to a bucket, no public access is granted. We recommend that you block all public access to your buckets unless you require public access to support a specific and verified use case. Before you block all public access, ensure that your applications will continue to work correctly without public access.

If you don't want to block all public access to your bucket, you can edit your block public access settings on the Amazon S3 console to configure granular levels of access to your buckets. For more information, see [Using Amazon S3 Block Public Access](#) in the *Amazon Simple Storage Service Developer Guide*.

In rare events, Access Analyzer for S3 might report no findings for a bucket that an Amazon S3 block public access evaluation reports as public. This happens because Amazon S3 block public access reviews policies for current actions and any potential actions that might be added in the future, leading to a bucket becoming public. On the other hand, Access Analyzer for S3 only analyzes the current actions specified for the Amazon S3 service in the evaluation of access status.

To block all public access to a bucket using Access Analyzer for S3

1. Sign in to the AWS Management Console and open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the navigation pane on the left, under **Dashboards**, choose **Access analyzer for S3**.
3. In Access Analyzer for S3, choose a bucket.
4. Choose **Block all public access**.

5. To confirm your intent to block all public access to the bucket, in **Block all public access (bucket settings)**, enter **confirm**.

Amazon S3 blocks all public access to your bucket. The status of the bucket finding updates to **resolved**, and the bucket disappears from the Access Analyzer for S3 listing. If you want to review resolved buckets, open IAM Access Analyzer on the IAM console.

Reviewing and changing bucket access

If you did not intend to grant access to the public or other AWS accounts, including accounts outside of your organization, you can modify the bucket ACL, bucket policy, or access point policy to remove the access to the bucket. The **Shared through** column shows all sources of bucket access: bucket policy, bucket ACL, and/or access point policy.

To review and change a bucket policy, a bucket ACL, or an access point policy

1. Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the navigation pane, choose **Access analyzer for S3**.
3. To see whether public access or shared access is granted through a bucket policy, a bucket ACL, or an access point policy, look in the **Shared through** column.
4. Under **Buckets**, choose the name of the bucket with the bucket policy, bucket ACL, or access point policy that you want to change or review.
5. If you want to change or view a bucket ACL:

- a. Choose **Permissions**.
- b. Choose **Access Control List**.
- c. Review your bucket ACL, and make changes as required.

For more information, see [How do I set ACL bucket permissions? \(p. 62\)](#)

6. If you want to change or review a bucket policy:

- a. Choose **Permissions**.
- b. Choose **Bucket Policy**.
- c. Review or change your bucket policy as required.

For more information, see [How do I add an S3 Bucket policy? \(p. 64\)](#)

7. If you want to review or change an access point policy:

- a. Choose **Access points**.
- b. Choose the access point name.
- c. Review or change access as required.

For more information, see [Managing and using Amazon S3 access points \(p. 21\)](#).

If you edit or remove a bucket ACL, a bucket policy, or an access point policy to remove public or shared access, the status for the bucket findings updates to resolved. The resolved bucket findings disappear from the Access Analyzer for S3 listing, but you can view them in IAM Access Analyzer.

Archiving bucket findings

If a bucket grants access to the public or other AWS accounts, including accounts outside of your organization, to support a specific use case (for example, a static website, public downloads, or cross-

account sharing), you can archive the finding for the bucket. When you archive bucket findings, you acknowledge and record your intent for the bucket to remain public or shared. Archived bucket findings remain in your Access Analyzer for S3 listing so that you always know which buckets are public or shared.

To archive bucket findings in Access Analyzer for S3

1. Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the navigation pane, choose **Access analyzer for S3**.
3. In Access Analyzer for S3, choose an active bucket.
4. To acknowledge your intent for this bucket to be accessed by the public or other AWS accounts, including accounts outside of your organization, choose **Archive**.
5. Enter **confirm**, and choose **Archive**.

Archive findings for bucket with public access ✕

By archiving the findings for this bucket, you acknowledge that you intend for anyone in the world to be able to access this bucket. If you do not intend for this bucket to be public, use [block public access](#) to configure secure access to your bucket. Before archiving, review the access granted to this bucket.

To confirm that you intend this bucket to be publicly accessible, enter *confirm* in the box.

Cancel Confirm

Activating an archived bucket finding

After you archive findings, you can always revisit them and change their status back to active, indicating that the bucket requires another review.

To activate an archived bucket finding in Access Analyzer for S3

1. Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the navigation pane, choose **Access analyzer for S3**.
3. Choose the archived bucket findings.
4. Choose **Mark as active**.

Viewing finding details

If you need to see more information about a bucket, you can open the bucket finding details in IAM Access Analyzer on the IAM console.

To view finding details in Access Analyzer for S3

1. Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the navigation pane, choose **Access analyzer for S3**.
3. In Access Analyzer for S3, choose a bucket.
4. Choose **View details**.

The finding details open in IAM Access Analyzer on the IAM console.

Downloading an Access Analyzer for S3 report

You can download your bucket findings as a CSV report that you can use for auditing purposes. The report includes the same information that you see in Access Analyzer for S3 on the Amazon S3 console.

To download a report

1. Open the Amazon S3 console at <https://console.aws.amazon.com/s3/>.
2. In the navigation pane on the left, choose **Access analyzer for S3**.
3. In the Region filter, choose the Region.

Access Analyzer for S3 updates to shows buckets for the chosen Region.

4. Choose **Download report**.

A CSV report is generated and saved to your computer.

Document history

Latest documentation update: March 27, 2019

The following table describes the important changes in each release of the *Amazon Simple Storage Service Console User Guide* from June 19, 2018, onward. For notification about updates to this documentation, you can subscribe to an RSS feed.

update-history-change	update-history-description	update-history-date
New archive storage class (p. 72)	Amazon S3 now offers a new archive storage class, S3 Glacier Deep Archive, for storing rarely accessed objects. For more information, see How Do I Restore an S3 Object That Has Been Archived? and Storage Classes in the <i>Amazon Simple Storage Service Developer Guide</i> .	March 27, 2019
Blocking public access to S3 buckets (p. 72)	Amazon S3 block public access prevents the application of any settings that allow public access to data within S3 buckets. For more information, see Blocking Public Access to S3 Buckets .	November 15, 2018
Filtering enhancements in cross-region replication (CRR) rules (p. 72)	In a CRR rule, you can specify an object filter to choose a subset of objects to apply the rule to. Previously, you could filter only on an object key prefix. In this release, you can filter on an object key prefix, one or more object tags, or both. For more information, see How Do I Add a Replication Rule to an S3 Bucket? .	September 19, 2018
Updates now available over RSS (p. 72)	You can now subscribe to an RSS feed to receive notifications about updates to the Amazon Simple Storage Service Console User Guide guide.	June 19, 2018

Earlier updates

The following table describes the important changes in each release of the *Amazon Simple Storage Service Console User Guide* before June 19, 2018.

Change	Description	Date changed
New storage class	Amazon S3 now offers a new storage class, ONEZONE_IA (IA, for infrequent access) for storing objects. For more information, see Storage Classes in the <i>Amazon Simple Storage Service Developer Guide</i> .	April 4, 2018
Support for ORC-formatted Amazon S3 inventory files	Amazon S3 now supports the Apache optimized row columnar (ORC) format in addition to comma-separated values (CSV) file format for inventory output files. For more information, see How Do I Configure Amazon S3 Inventory? (p. 52).	November 17, 2017
Bucket permissions check	Bucket permissions check in the Amazon S3 console checks bucket policies and bucket access control lists (ACLs) to identify publicly accessible buckets. Bucket permissions check makes it easier to identify S3 buckets that provide public read and write access.	November 06, 2017
Default encryption for S3 buckets	Amazon S3 default encryption provides a way to set the default encryption behavior for an S3 bucket. You can set default encryption on a bucket so that all objects are encrypted when they are stored in the bucket. The objects are encrypted using server-side encryption with either Amazon S3-managed keys (SSE-S3) or AWS KMS-managed keys (SSE-KMS). For more information, see How do I enable default encryption for an Amazon S3 bucket? (p. 7).	November 06, 2017
Encryption status in Amazon S3 inventory	Amazon S3 now supports including encryption status in Amazon S3 inventory so you can see how your objects are encrypted at rest for compliance auditing or other purposes. You can also configure to encrypt Amazon S3 inventory with server-side encryption (SSE) or SSE-KMS so that all inventory files are encrypted accordingly. For more information, see How Do I Configure Amazon S3 Inventory? (p. 52).	November 06, 2017
Cross-region replication enhancements	Cross-region replication now supports the following: <ul style="list-style-type: none"> By default, Amazon S3 does not replicate objects in your source bucket that are created using server-side encryption using AWS KMS-managed keys. You can now configure a replication rule to replicate these objects. For more information, see How do I add a replication rule to an S3 bucket? (p. 46). In a cross-account scenario, you can configure a replication rule to change replica ownership to the AWS account that owns the destination bucket. For more information, see How do I add a replication rule to an S3 bucket? (p. 46). 	November 06, 2017
Added functionality and documentation	The Amazon S3 console now supports enabling object-level logging for an S3 bucket with AWS CloudTrail data events logging. For more information, see How do I enable object-level logging for an S3 bucket with AWS CloudTrail data events? (p. 10).	October 19, 2017
Old Amazon S3 console no longer available	The old version of the Amazon S3 console is no longer available and the old user guide was removed from the Amazon S3 documentation site.	August 31, 2017

Change	Description	Date changed
General availability of New Amazon S3 console	Announced the general availability of the new Amazon S3 console.	May 15, 2017

AWS glossary

For the latest AWS terminology, see the [AWS glossary](#) in the *AWS General Reference*.