

AWS CLOUDFRONT

GO TO S3 & CREATE A BUCKET

GIVE BUCKET NAME AND KEEP ALL DEFAULTS

The screenshot shows the 'Create bucket' configuration page in the AWS S3 console. The 'General configuration' section is set to 'General purpose'. The bucket name is 'bucketforcloudfront'. Under 'Object Ownership', the 'Bucket owner enforced' option is selected. In the 'Block Public Access settings for this bucket' section, 'Block all public access' is checked. The 'Bucket Versioning' section has 'Enable' selected. There are no tags associated with the bucket. In the 'Default encryption' section, 'Server-side encryption with Amazon S3 managed keys (SSE-S3)' is selected. The 'Bucket Key' section has 'Enable' selected. At the bottom, a note says 'After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.' The 'Create bucket' button is at the bottom right.

Create bucket Info
Buckets are containers for data stored in S3.

General configuration

AWS Region
Europe (Stockholm) eu-north-1

Bucket type Info
 General purpose
Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.
 Directory
Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.

Bucket name Info

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - optional
Only the bucket settings in the following configuration are copied.
[Choose bucket](#)
Format: s3://bucket/prefix

Object Ownership Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

[View bucket details \(recommended\)](#) [CloudShell](#) [Feedback](#) [ACLs](#) © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Block Public Access settings for this bucket
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 this bucket and its 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 this bucket or objects within it, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

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 ignore 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.

Bucket Versioning
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning
 Disable
 Enable

Tags - optional (0)
You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.
[Add tag](#)

Default encryption Info
Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info
 Server-side encryption with Amazon S3 managed keys (SSE-S3)
 Server-side encryption with AWS Key Management Service keys (SSE-KMS)
 Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the [Amazon S3 pricing page](#).

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

Disable
 Enable

Advanced settings

After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

[Cancel](#) [Create bucket](#)

The screenshot shows the AWS S3 Buckets page. At the top, a green banner displays a success message: "Successfully created bucket 'buchetforcloudfront'. To upload files and folders, or to configure additional bucket settings, choose View details." Below this, an "Account snapshot - updated every 24 hours" section provides storage usage and activity trends. The main content area is divided into "General purpose buckets" and "Directory buckets". Under "General purpose buckets", there is a table listing three buckets:

Name	AWS Region	IAM Access Analyzer	Creation date
buchetforcloudfront	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	February 4, 2025, 11:19:17 (UTC+05:30)
fdp-user1-bucket	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	January 31, 2025, 09:42:31 (UTC+05:30)
fdp-user2-bucket	Europe (Stockholm) eu-north-1	View analyzer for eu-north-1	January 31, 2025, 14:33:05 (UTC+05:30)

GO TO BUCKET CREATED

The screenshot shows the AWS S3 Object Details page for the bucket "buchetforcloudfront". The top navigation bar shows the path "Amazon S3 > Buckets > buchetforcloudfront". The main content area is titled "buchetforcloudfront" and includes tabs for Objects, Properties, Permissions, Metrics, Management, and Access Points. The "Objects" tab is selected, showing a table with zero objects. The table has columns for Name, Type, Last modified, Size, and Storage class. A prominent "Upload" button is located at the bottom of the object list.

GO TO PROPERTIES AND HOST STATIC WEBSITE

Edit static website hosting Info

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting

- Disable
- Enable

Hosting type

- Host a static website
Use the bucket endpoint as the web address. [Learn more](#)
- Redirect requests for an object
Redirect requests to another bucket or domain. [Learn more](#)

ⓘ For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see [Using Amazon S3 Block Public Access](#)

Index document

Specify the home or default page of the website.

second.html

Error document - optional

This is returned when an error occurs.

error.html

The screenshot shows the AWS S3 console interface for editing a static website hosting configuration. At the top, there's a navigation bar with the AWS logo, search bar, and various icons. Below it, the breadcrumb navigation shows: Amazon S3 > Buckets > buchettorcloudfront > Edit static website hosting. The main content area contains sections for 'Static website hosting' (with 'Enable' selected), 'Hosting type' (with 'Host a static website' selected), 'Index document' (set to 'second.html'), and 'Error document - optional' (set to 'error.html'). A note about making content publicly readable is displayed in a callout box. At the bottom, there are 'Cancel' and 'Save changes' buttons, along with links for CloudShell, Feedback, and footer links like Privacy, Terms, and Cookie preferences.

SAVE CHANGES

GO TO OBJECT AND UPLOAD A FILE (HTML)

aws Search [Alt+S] Europe (Stockholm) fdponcc

Amazon S3 > Buckets > buchetcforcloudfront > Upload

Upload Info

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose Add files or Add folder.

Files and folders (1 total, 296.0 B)						
All files and folders in this table will be uploaded.						
<input type="text"/> Find by name						
<input type="checkbox"/>	Name	Folder	Type	Size		
<input type="checkbox"/>	second.html	-	text/html	296.0 B	< 1 >	

Destination Info

Destination <s3://buchetcforcloudfront>

▶ Destination details Bucket settings that impact new objects stored in the specified destination.

▶ Permissions Grant public access and access to other AWS accounts.

CloudShell Feedback Properties Specify storage class, encryption settings, tags, and more.

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Storage class Info

Amazon S3 offers a range of storage classes designed for different use cases. [Learn more](#) or see [Amazon S3 pricing](#)

Storage class	Designed for	Bucket type	Availability Zones	Min storage duration	Min billable object size	Monitoring and auto-tiering fees	Retrieval fees
<input checked="" type="radio"/> Standard	Frequently accessed data (more than once a month) with milliseconds access	General purpose	≥ 3	-	-	-	-
<input type="radio"/> Intelligent-Tiering	Data with changing or unknown access patterns	General purpose	≥ 3	-	-	Per-object fees apply for objects ≥ 128 KB	-
<input type="radio"/> Standard-IA	Infrequently accessed data (once a month) with milliseconds access	General purpose	≥ 3	30 days	128 KB	-	Per-GB fees apply
<input type="radio"/> One Zone-IA	Recreatable, infrequently accessed data (once a month) with milliseconds access	General purpose or directory	1	30 days	128 KB	-	Per-GB fees apply
<input type="radio"/> Glacier Instant Retrieval	Long-lived archive data accessed once a quarter with instant retrieval in milliseconds	General purpose	≥ 3	90 days	128 KB	-	Per-GB fees apply
<input type="radio"/> Glacier Flexible Retrieval (formerly Glacier)	Long-lived archive data accessed once a year with retrieval of minutes to hours	General purpose	≥ 3	90 days	-	-	Per-GB fees apply
<input type="radio"/> Glacier Deep Archive	Long-lived archive data accessed less than once a year with retrieval of hours	General purpose	≥ 3	180 days	-	-	Per-GB fees apply
<input type="radio"/> Reduced redundancy	Noncritical, frequently accessed data with milliseconds access (not recommended as S3 Standard is more cost effective)	General purpose	≥ 3	-	-	-	Per-GB fees apply

Server-side encryption Info

Server-side encryption protects data at rest.

Server-side encryption

- Don't specify an encryption key The bucket settings for default encryption are used to encrypt objects when storing them in Amazon S3.
- Specify an encryption key The specified encryption key is used to encrypt objects before storing them in Amazon S3.

⚠ If your bucket policy requires objects to be encrypted with a specific encryption key, you must specify the same encryption key when you upload objects. Otherwise, uploads will fail.

Checksums

Checksums are used for data integrity verification of new objects. [Learn more](#)

Checksum function Checksum functions are used to calculate the checksum value. For objects smaller than 16 MB, only the full object checksum type is supported, for all checksum algorithms.

CRC64NVME (recommended)

Precalculated value - optional When you provide a precalculated value for a single object, S3 compares it to the value it calculates using the selected checksum function. If the values don't match, the upload will fail. [Learn more](#)

Enter value The precalculated value must be a Base64 encoded string. It must not exceed 128 characters, and can contain only letters (a-z, A-Z), numbers (0-9), forward slash (/), plus (+), or equals (=).

Tags - optional

You can use object tags to analyze, manage, and specify permissions for objects. [Learn more](#)

No tags associated with this resource.

Add tag

Metadata - optional

Metadata is optional information provided as a name-value (key-value) pair. [Learn more](#)

No metadata associated with this resource.

Add metadata

Cancel Upload

Upload: status

After you navigate away from this page, the following information is no longer available.

Summary													
Destination s3://buchetforcloudfront	Succeeded 1 file, 296.0 B (100.00%)												
Failed 0 files, 0 B (0%)													
Files and folders Configuration													
Files and folders (1 total, 296.0 B) <table border="1"> <thead> <tr> <th>Name</th> <th>Folder</th> <th>Type</th> <th>Size</th> <th>Status</th> <th>Error</th> </tr> </thead> <tbody> <tr> <td>second.html</td> <td>-</td> <td>text/html</td> <td>296.0 B</td> <td>Succeeded</td> <td>-</td> </tr> </tbody> </table>		Name	Folder	Type	Size	Status	Error	second.html	-	text/html	296.0 B	Succeeded	-
Name	Folder	Type	Size	Status	Error								
second.html	-	text/html	296.0 B	Succeeded	-								

ACCESS URL FROM UR BUCKET - PROPERTIES-> STATIC WEB HOSTING SITE ADDRESS

Amazon S3

General purpose buckets

- Directory buckets
- Table buckets
- Access Grants
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

- Dashboards
- Storage Lens groups
- AWS Organizations settings

Feature spotlight [10](#)

Requester pays

When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](#)

Requester pays

Disabled

Static website hosting

Use this bucket to host a website or redirect requests. [Learn more](#)

We recommend using AWS Amplify Hosting for static website hosting

Deploy a fast, secure, and reliable website quickly with AWS Amplify Hosting. Learn more about [Amplify Hosting](#) or [View your existing Amplify apps](#)

S3 static website hosting

Enabled

Hosting type

Bucket hosting

Bucket website endpoint

When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](#)

<http://buchetforcloudfront.s3-website.eu-north-1.amazonaws.com>

IF YOU TRY TO ACCESS THE URL

403 Forbidden

- Code: AccessDenied
- Message: Access Denied
- RequestId: YAF7TX6H40F421D2
- HostId: lrkdb7hf7HGG4X26oginZ7YKa1+YaRcxnsC5sqqVmyfsrYiuWoKLPMCM9jb9JRYW3Fb019ORyvWQ/P592gPrCw==

STEP 2: CLOUDFRONT

Networking & Content Delivery

Amazon CloudFront

Securely deliver content with low latency and high transfer speeds

Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency and high transfer speeds.

Get started with CloudFront

Enable accelerated, reliable and secure content delivery for Amazon S3 buckets, Application Load Balancers, Amazon API Gateway APIs, and more in 5 minutes or less.

Create a CloudFront distribution

AWS Free Tier

1 TB of data transfer out
10,000,000 HTTP or HTTPS requests

Benefits and features

CREATE A DISTRIBUTION

CloudFront > Distributions > Create

Create distribution

Origin

Origin domain
Choose an AWS origin, or enter your origin's domain name. [Learn more](#)

X

Enter a valid DNS domain name, such as an S3 bucket, HTTP server, or VPC origin ID.

⚠ This S3 bucket has static web hosting enabled. If you plan to use this distribution as a website, we recommend using the S3 website endpoint rather than the bucket endpoint. Use website endpoint

Origin path - optional
Enter a URL path to append to the origin domain name for origin requests.

Name
Enter a name for this origin.

Origin access | [Info](#)

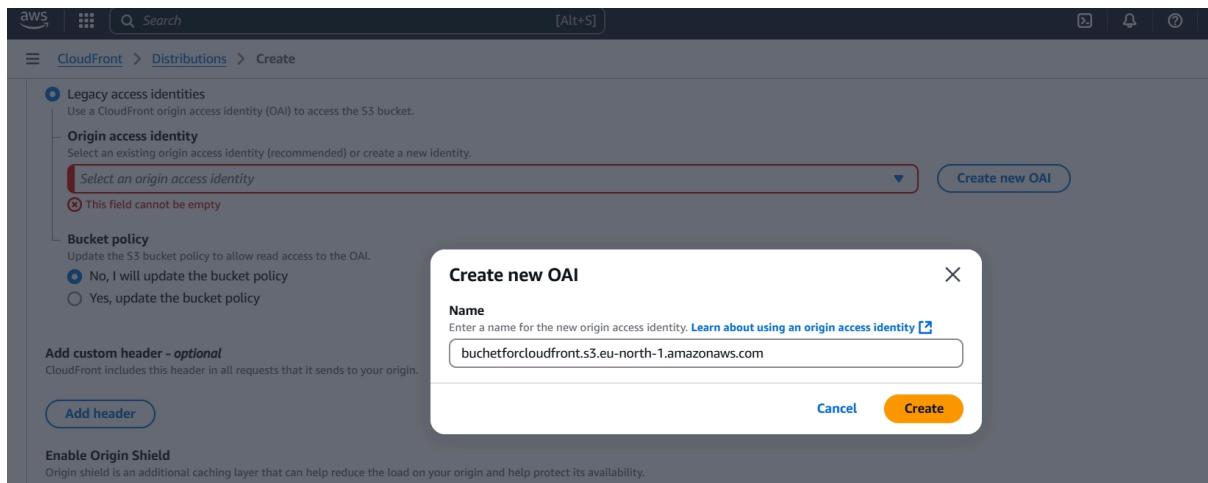
Public
Bucket must allow public access.

Origin access control settings (recommended)
Bucket can restrict access to only CloudFront.

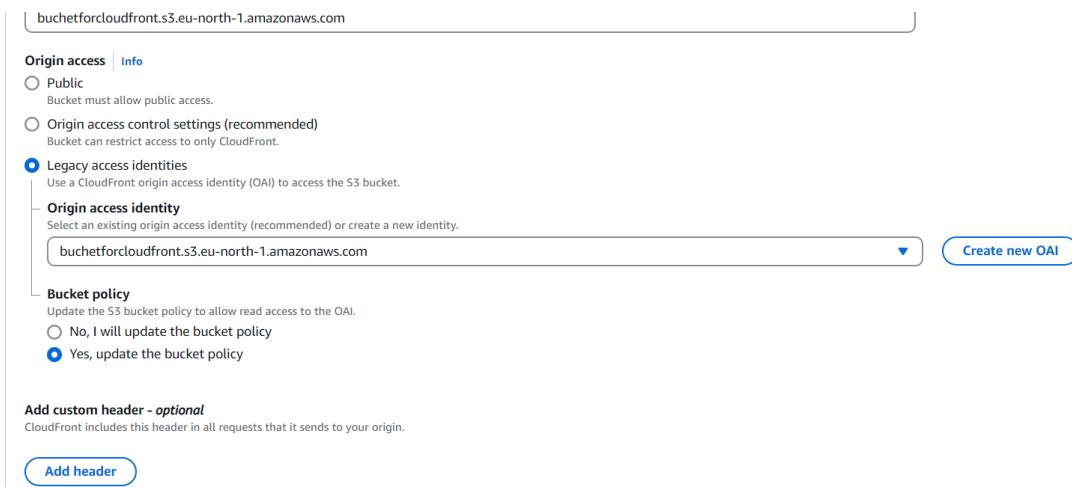
Legacy access identities

CREATE A NEW OAI

Screenshot of the AWS CloudFront 'Create Distribution' wizard, step 2: 'Origin access identities'. The 'Legacy access identities' section is selected. A modal window titled 'Create new OAI' is open, showing a 'Name' field with 'bucchetforcloudfront.s3.eu-north-1.amazonaws.com' and a 'Create' button.



Screenshot of the 'Create new OAI' modal window. The 'Name' field contains 'bucchetforcloudfront.s3.eu-north-1.amazonaws.com'. The 'Create' button is highlighted in orange.



KEEP ALL SETTINGS DEFAULT

Create distribution

Origin

Origin domain
Create an AWS origin, or enter your origin's domain name. Learn more [\[Info\]](#)

Enter a valid DNS domain name, such as an S3 bucket, an HTTP server, or a VPC endpoint ID.

Note: This S3 bucket has static web hosting enabled. If you plan to use this distribution as a website, we recommend using the S3 website endpoint rather than the bucket endpoint.

Use website endpoint

Origin path - optional
Enter a path to redirect to the origin domain name for origin requests.

Name
Enter a name for this origin.

Origin access [\[Info\]](#)

- Public
Bucket must allow public access.
- Origin access identity (recommended)
CloudFront can restrict access to only CloudFront.

Legacy access identities
Selects an existing legacy access identity (OAI) to access the S3 bucket.

Origin access identity
Selects an existing origin access identity (recommended) or creates a new identity.

[Create new OAI](#)

Bucket policy
Update the S3 bucket policy to allow read access to the OAI.

- No, I will update the bucket policy
- Yes, update the bucket policy

Add custom header - optional
CloudFront includes this header in all requests that it sends to your origin.

[Add header](#)

Enable Origin Shield
Origin shield is an additional caching layer that can help reduce the load on your origins and help protect its availability.

- No
- Yes

► Additional settings

Default cache behavior

Path pattern [\[Info\]](#)

Compress objects automatically [\[Info\]](#)
 Yes

Viewer

Viewer protocol policy
 HTTP and HTTPS
 Redirect HTTP to HTTPS
 HTTPS only

Allowed HTTP methods
 GET, HEAD, OPTIONS
 PUT, POST, PATCH, DELETE

Restrict viewer access
Restrict viewer access; viewers must use CloudFront signed URLs or signed cookies to access your content.

- Yes
- No

Cache key and origin requests
We recommend using a cache policy and origin request policy to control the cache key and origin requests.

- Cache policy and origin request policy (recommended)
- Legacy cache settings

Cache policy
Choose an existing cache policy or create a new one.

Enabled. Supports Gzip and Bronto compression. [View policy](#) [\[Info\]](#) Recommended for S3 [Edit](#)

Origin request policy - optional
Choose an existing origin request policy or create a new one.

[View policy](#) [\[Info\]](#) [Edit](#)

Response headers policy - optional
Choose an existing response headers policy or create a new one.

[View policy](#) [\[Info\]](#) [Edit](#)

► Additional settings

Function associations - optional [\[Info\]](#)
Choose an edge function to associate with this cache behavior, and the CloudFront event that invokes the function.

Function type	Function ARN / Name	include body
Viewer request	<input type="text" value="No association"/>	
Viewer response	<input type="text" value="No association"/>	
Origin request	<input type="text" value="No association"/>	
Origin response	<input type="text" value="No association"/>	

Web Application Firewall (WAF) [\[Info\]](#)

Enable security protections
Amazon CloudFront monitors the edge connection for threats and security vulnerabilities using AWS WAF. Blocked requests are stopped before they reach your web servers.

Do not enable security protections
Select this option if your application does not need security protection from AWS WAF.

► Included security protections

- Protect against the most common vulnerabilities found in web applications.
- Protect against malicious attacks detecting suspicious web traffic.
- Block IP addresses from potential threats based on Amazon Internal Threat Intelligence.

Price estimate

This AWS WAF configuration is estimated to cost \$14 for 10 million requests/month

Settings

Anycast static IP list - optional [\[Info\]](#)
Deliver traffic from a small set of IP addresses.
There are no Anycast static IP lists available.

[Create an Anycast static IP list](#) There are no Anycast static IP lists available.

Price class [\[Info\]](#)
The price class associated with the maximum price that you want to pay.

- Use all edge locations (best performance)
- Use only North America and Europe
- Use North America, Europe, Asia, Middle East, and Africa

Alternate domain name (CNAME) - optional
Alternative domain names that you use in URLs for the content served by this distribution.

[Add item](#)

Custom SSL certificate - optional
A certificate that you have in AWS Certificate Manager. This certificate must be in the US East (US Virgin Islands) Region (ca-east-1).

[Choose certificate](#)

Default root object - optional
The object that is used to redirect when a viewer requests the root URL (/) instead of a specific object.

Off
 On

Description - optional

Standard logging [\[Info\]](#)
Additional charges may apply. See Info for more details.

Log delivery
Get logs of viewer requests to CloudWatch, Amazon S3 or Firehose.

- Off
- On

Create distribution

Default root object - optional
The object (file name) to return when a viewer requests the root URL (/) instead of a specific object.

IPv6
 Off
 On

Description - optional

Standard logging [Info](#)
Additional charges may apply. See Info for more details.

Log delivery
Get logs of viewer requests to CloudWatch, Amazon S3 or Firehose
 Off
 On

[Cancel](#) [Create distribution](#)

E10OYDIV9P2N81 [View metrics](#)

[General](#) [Security](#) [Origins](#) [Behaviors](#) [Error pages](#) [Invalidations](#) [Tags](#) [Logging](#)

Details

Distribution domain name <input type="text" value="d21jmagi8xjsj.cloudfront.net"/>	ARN <input type="text" value="arn:aws:cloudfront::699475937818:distribution/E10OYDIV9P2N81"/>	Last modified <input type="text" value="Deploying 1"/>
---	--	---

Settings [Edit](#)

Description -	Alternate domain names -	Standard logging Off	Activate Windows Go to Settings to activate Windows.
------------------	-----------------------------	-------------------------	---

POLICY BEEN CREATED IN S3 BUCKET

Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about [using Amazon S3 Block Public Access](#).

```
[{"Version": "2008-10-17", "Id": "PolicyForCloudFrontPrivateContent", "Statement": [{"Sid": "1", "Effect": "Allow", "Principal": {"AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity E14VD7XXB289B9"}, "Action": "s3:GetObject", "Resource": "arn:aws:s3:::bucetforcloudfront/*"}]}
```

[Copy](#)

GO TO THE LINK (DISTRIBUTION DOMAIN NAME)

The screenshot shows the AWS CloudFront 'Distributions' page. The distribution ID is E1WVDZ5WTBRLXD. The 'General' tab is selected. A success message 'Distribution domain name copied' is displayed next to the domain name d3op513v5bf4mm.cloudfront.net. The ARN is listed as arn:aws:cloudfront::699475937818:distribution/E1WVDZ5WTBRLXD. The last modified date is February 4, 2025 at 6:32:16 AM UTC. The 'Settings' section includes fields for Description (empty), Price class (Use only North America and Europe), and Supported HTTP versions (HTTP/2, HTTP/1.1, HTTP/1.0). The 'Alternate domain names' section is empty. Logging options include Standard logging (Off), Cookie logging (Off), and Default root object (empty). The 'Continuous deployment' section shows a link to activate Windows.

S3 RESULT

The screenshot shows a browser window with multiple tabs. One tab displays a 403 Forbidden error message: '403 ERROR' and 'The request could not be satisfied.' Below this, it says 'Bad request. We can't connect to the server for this app or website at this time. There might be too much traffic or a configuration error. Try again later, or contact the app or website owner. If you provide content to customers through CloudFront, you can find steps to troubleshoot and help prevent this error by reviewing the CloudFront documentation.' At the bottom, it shows 'Generated by cloudfront (CloudFront) Request ID: dtkev29yj119nro201nhUBX8E1vnHkoxBff9UFMLcMsKXs1wbK3A=='.

CLOUD FRONT RESULT