



Setup S3 & Cloudfront for Laravel/Statamic

Create S3 Bucket

Name it `echo-{clientname}` and leave all settings as is. So if the client name is `quikprint` then the name for the bucket should be `echo-quikprint`. Don't add any permissions to the S3 bucket just yet.

[Amazon S3](#) > [Buckets](#) > Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

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

AWS Region

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Object Ownership [Info](#)

Add a new IAM user for project

Add the user to the IAM using `user-{client name}`. So example would be `user-thebendsportsbar`. Make sure to give it programmatic access.

Specify user details

User details

User name

user-southtown

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☐ Provide user access to the AWS Management Console - *optional*
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel

Next

Attach Role Group

Attach permissions by adding the `EchoWebAssetGroup` to the newly created user. Click on the user and generate the access keys under `Security Credentials`.

Access keys (0)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

Create access key

No access keys

As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. [Learn more](#)

Create access key

SSH public keys for AWS CodeCommit (0)

Credential purpose

Select `Application running outside AWS` for access key practice.

You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

☒ **Application running outside AWS**
You plan to use this access key to enable an application running on an on-premises host, or to use a local AWS client or third-party AWS plugin.

☐ **Other**
Your use case is not listed here.

After you create user be sure the save the `Access ID` and `Secret Key` in a safe place and add it to your `.env` file.

Add CloudFront distribution

Next add the CloudFront distribution and you will see the S3 bucket listed to select from. Select `Origin access control settings (reccomended)` . Then click on `Create control setting (Create New OAC)` button.

The screenshot shows the 'Add origin' form in the AWS CloudFront console. The form is divided into several sections:

- Origin domain:** A text input field containing 'echo-southtown.s3.us-east-2.amazonaws.com' with a search icon on the left and a close icon on the right.
- Origin path - optional:** A text input field with the placeholder 'Enter the origin path'.
- Name:** A text input field containing 'echo-southtown.s3.us-east-2.amazonaws.com'.
- Origin access:** Three radio button options:
 - ☐ Public: Bucket must allow public access.
 - ☒ Origin access control settings (recommended): Bucket can restrict access to only CloudFront.
 - ☐ Legacy access identities: Use a CloudFront origin access identity (OAI) to access the S3 bucket.
- Origin access control:** A section with a dropdown menu showing 'echo-newstride.s3.us-east-2.amazonaws.com' and 'Origin type: S3'. To the right is a button labeled 'Create control setting'.
- Bucket policy:** A section with a radio button option ☒ 'I will manually update the policy'.

At the bottom, there is a red warning icon and the text 'You must update the S3 bucket policy'.

Add Control Setting

Leave default setup and hit create.

Create control setting

Name

echo-revivalwc.s3.us-east-2.amazonaws.com

The name must be unique. Valid characters: letters, numbers and most special characters. Use up to 64 characters.

Description - optional

Enter description

The description can have up to 256 characters.

Signing behavior

☐ Do not sign requests

☒ Sign requests (recommended)

☐ Do not override authorization header

Do not sign if incoming request has authorization header.

Origin type

S3

The origin type must be the same type as origin domain.

Cancel

Create

Firewall Security

Select firewall selection below to enable security protection. Then click on the **Create Distribution** button.

Web Application Firewall (WAF)

☒ Enable security protections

Keep your application secure from the most common web 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 protections from AWS WAF.

☐ Use monitor mode

Count how many of your requests would be blocked by this WAF configuration. When ready, you can disable monitor mode to begin blocking requests.

▼ Included security protections

Allow Cloudfront access to S3

After saved, click on the distribution again to grab the policy needed for the S3 bucket. Go to **Origin**, select the distribution and then click the **Edit** button.

Origin access control

Select an existing origin access control (recommended) or create a new configuration.

echo-newstride.s3.us-east-2.amazonaws.com

Origin type: S3 ▼

Create control setting

Bucket policy

Policy must allow access to CloudFront IAM service principal role.

☒ I will manually update the policy

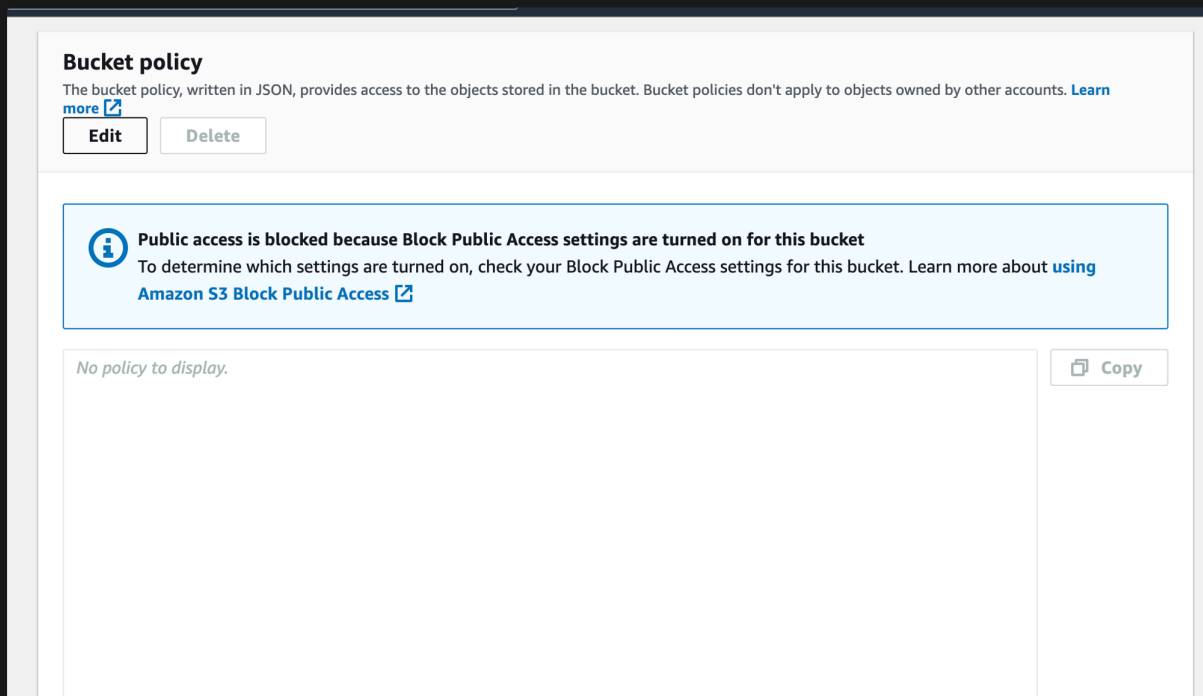
i You must allow access to CloudFront using this policy statement. Learn more about giving CloudFront permission to access the S3 bucket [🔗](#).

📋 Copy policy

🔗 Go to S3 bucket permissions [🔗](#)

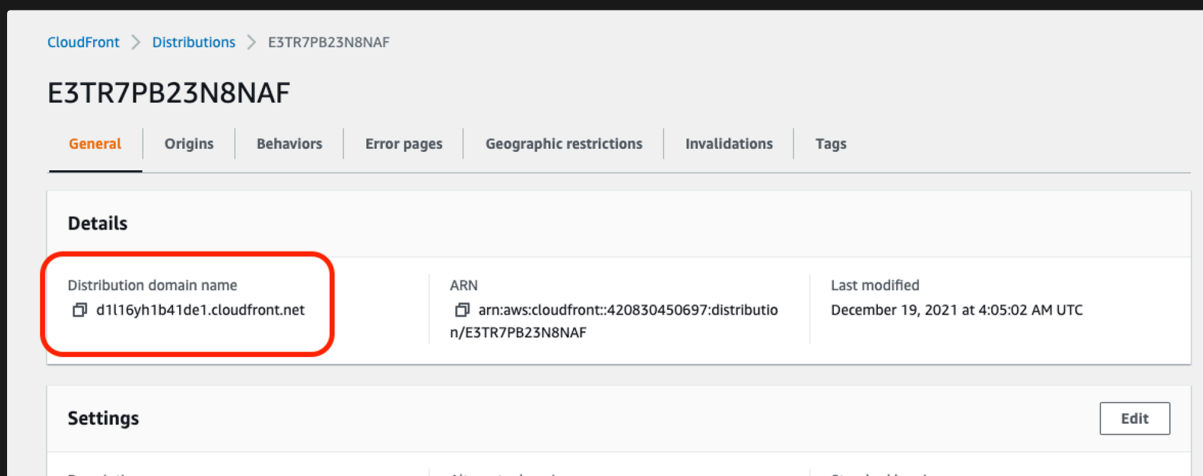
Update S3 bucket policy

Edit the S3 policy and paste the policy from above. Go to the S3 bucket and click on **Permissions**. Attach the policy by editing the bucket policy.



Project ENV Setup

Copy the url from the created distribution for the CloudFront account.



Project Library setup

Be sure to install the filesystem helpers outlined in Laravel docs.

```
composer require league/flysystem-aws-s3-v3 "^3.0" --with-all-dependencies
```

ENV Example Below

```
FILESYSTEM_DISK=s3 AWS_ACCESS_KEY_ID={aws id}
AWS_SECRET_ACCESS_KEY={aws key} AWS_DEFAULT_REGION={input region
name} AWS_BUCKET=echo-{client name} AWS_URL={cloud front url you
copied from previous page}
```

Modify configuration with new change

Now modify the `config > filesystems.php` file and comment out or add `'visibility' => 'private'`.

```
's3' => [ 'driver' => 's3', 'key' => env('AWS_ACCESS_KEY_ID'), 'sec
ret' => env('AWS_SECRET_ACCESS_KEY'), 'region' => env('AWS_DEFAULT_
REGION'), 'bucket' => env('AWS_BUCKET'), 'url' => env('AWS_URL'),
'endpoint' => env('AWS_ENDPOINT'), 'use_path_style_endpoint' => env
('AWS_USE_PATH_STYLE_ENDPOINT', false), 'visibility' => 'private',
// https://statamic.dev/assets#visibility 'throw' => false, ],
```

Change Asset Container Configuration

Select S3 for the Disk.