

Title:: “PutObject” error came when we try to store img or video through postman in s3 bucket.

```
Error executing "PutObject" on "https://frank-transcribe-mediaconvert.s3.amazonaws.com/032420-test-upload.txt"; AWS HTTP error: Client error PUT https://frank-transcribe-mediaconvert.s3.amazonaws.com/032420-test-upload.txt resulted in a 400 Bad Request response: InvalidTokenThe provided token
```

- If you done properly given links steps in “IAM” and “S3” then first **check** following things are correct or not...

<https://www.itsolutionstuff.com/post/laravel-amazon-s3-file-upload-tutorialexample.html>

Check::

- Check in .env file given correct AWS region
- Check you select Aws credential type “Access key – Programmatic access”
- Check in IAM => user, attached policy is AmazonS3FullAccess
- Check in Permission you **uncheck** “Block all public access”.
- Check in Bucket Policy add “s3:GetObject” and “s3:PutObject” in Action.

Cause of Error::

- In Bucket Permissions go to “Object Ownership” and edit it, Select “**ACLs enabled**” change it according to given img and save it, error is solved.

Object Ownership

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.

☐ **ACLs disabled (recommended)**

All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☒ **ACLs enabled**

Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.


Object Ownership

☒ **Bucket owner preferred**

If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.

☐ **Object writer**

The object writer remains the object owner.

 If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. [Learn more](#)

Cancel

Save changes

- In addition check the “Access control list” after above step, if it is in given format then no worries otherwise edit it as given format.





Access control list (ACL)

Grant basic read/write permissions to other AWS accounts. [Learn more](#)

Edit



The console displays combined access grants for duplicate grantees
To see the full list of ACLs, use the Amazon S3 REST API, AWS CLI, or AWS SDKs.

Grantee	Objects	Bucket ACL
Bucket owner (your AWS account) Canonical ID:  abc770be602ba6f454972c217f0a9396d73115e48de4e1785b511abccab655b5	List, Write	Read, Write
Everyone (public access) Group:  http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group:  http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-
S3 log delivery group Group:  http://acs.amazonaws.com/groups/s3/LogDelivery	-	-