

Console

Services

Features

Resources **New**

Documentation

Knowledge articles


Marketplace


Blog posts


Events


Tutorials


Recent


 S3


 EC2


 Light

 Amazon

 Step

 Billing

 AWS

 Secret

Welcome

Getting started with AWS


Open issues


Current month costs


Cost (1)


Services

Show more

 **S3**  
Scalable Storage in the Cloud

 **S3 Glacier**  
Archive Storage in the Cloud

 **AWS Snow Family**  
Large Scale Data Transport

 **Storage Gateway**  
Hybrid Storage Integration

Features

Show more

**Imports from S3**  
■ DynamoDB feature

**Feature spotlight**  
■ S3 feature

out

+ Add widgets

Create application

< 1 >

on | Originati

on.

AWS Region

US East (N. Virginia) us-east-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

mycandy

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.

- ☒ **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 enforced

Bucket owner enforced

## 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, 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 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.

### Turning off block all public access might result in this bucket and the objects within becoming public

AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

# 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, 146.1 KB)**

[Remove](#) [Add files](#) [Add folder](#)

All files and folders in this table will be uploaded.

**1**

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	Screenshot 2025-01-30 at 4.59.10 A...	-	image/png	146.1 KB

**Destination** [Info](#)

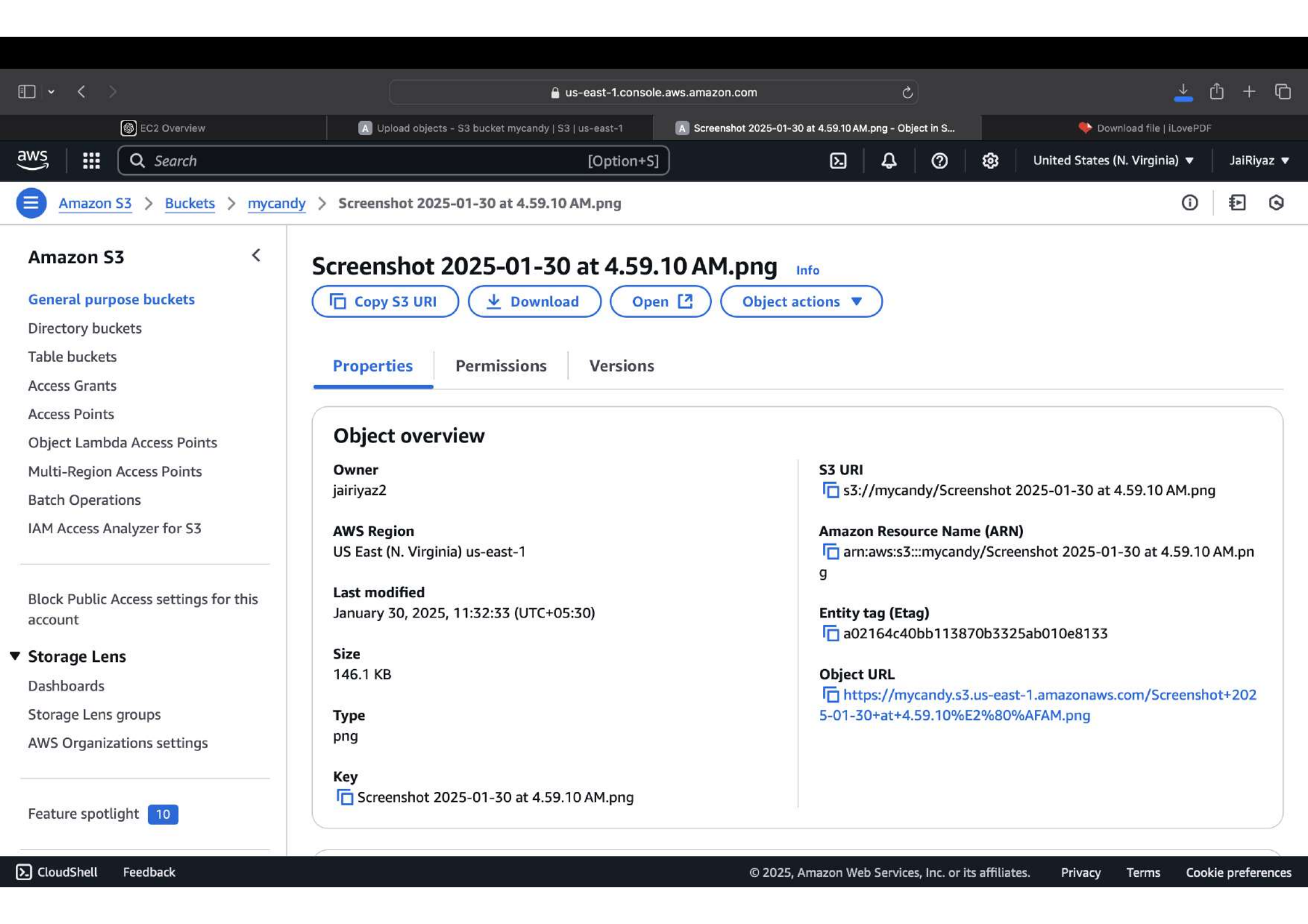
**Destination**  
[s3://mycandy](#)

**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](#)





Policy

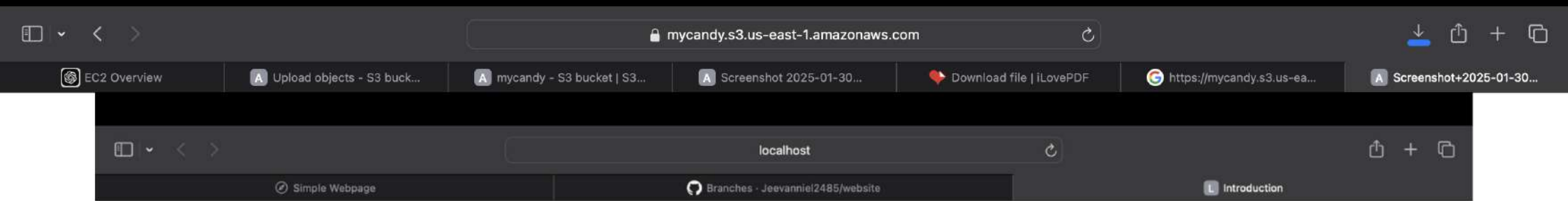
```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": "*",
7       "Action": "s3:GetObject",
8       "Resource": "arn:aws:s3:::mycandy/*"
9     }
10  ]
11 }
```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement



hello everyone i m jeevan