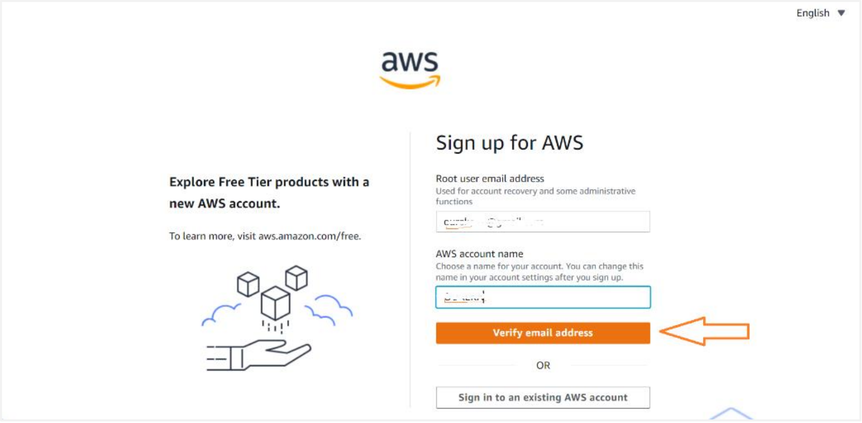
Software Team

Amazon AWS Setup

Follow these steps to create S3 Bucket: (First We will create an AWS account)

1. Create an AWS Account. **Click**: https://aws.amazon.com/s3/

2. Sign Up and Verify email address



Explore Free Tier products with a new AWS account.

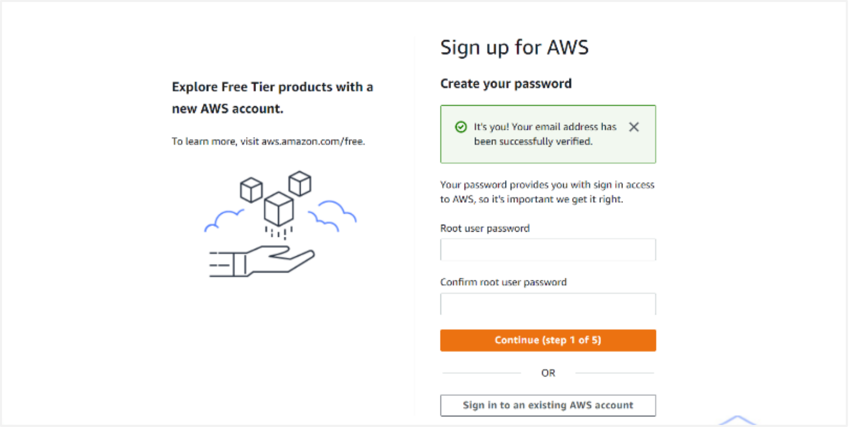
To learn more, visit aws.amazon.com/free.

Sign up for AWS

Root user email address
Used for account recovery and some administrative functions
[redacted]

AWS account name
Choose a name for your account. You can change this name in your account settings after you sign up.
[redacted]

3. Step-1: Set a root user password.



Sign up for AWS

Create your password

It's you! Your email address has been successfully verified.

Your password provides you with sign in access to AWS, so it's important we get it right.

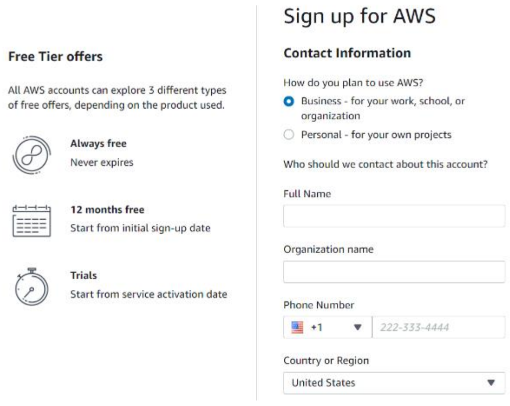
Root user password

Confirm root user password

Explore Free Tier products with a new AWS account.

To learn more, visit aws.amazon.com/free.

4. Step-2: Provide your contact information.



Free Tier offers

All AWS accounts can explore 3 different types of free offers, depending on the product used.

Always free
Never expires

12 months free
Start from initial sign-up date

Trials
Start from service activation date

Sign up for AWS

Contact Information

How do you plan to use AWS?

● Business - for your work, school, or organization

○ Personal - for your own projects

Who should we contact about this account?

Full Name

Organization name

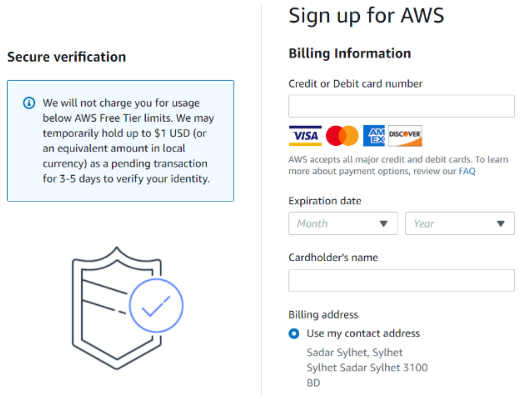
Phone Number

+1 ▼ 222-333-4444

Country or Region

United States ▼

5. Step-3: Provide your billing Information.



Secure verification

We will not charge you for usage below AWS Free Tier limits. We may temporarily hold up to $1 USD (or an equivalent amount in local currency) as a pending transaction for 3-5 days to verify your identity.

Sign up for AWS

Billing Information

Credit or Debit card number

AWS accepts all major credit and debit cards. To learn more about payment options, review our FAQ

Expiration date

Month ▼ Year ▼

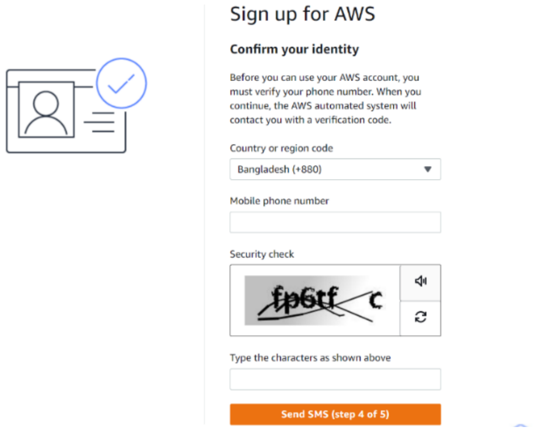
Cardholder's name

Billing address

● Use my contact address

Sadar Sylhet, Sylhet
Sylhet Sadar Sylhet 3100
BD

6. Step-4: Confirm your identity through mobile phone number verification.



Sign up for AWS

Confirm your identity

Before you can use your AWS account, you must verify your phone number. When you continue, the AWS automated system will contact you with a verification code.

Country or region code

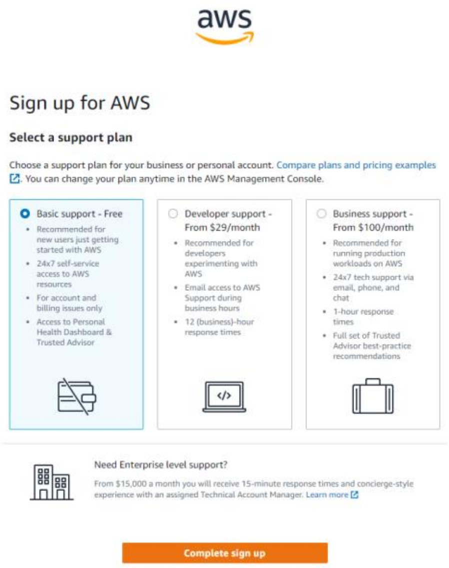
Bangladesh (+880) ▼

Mobile phone number

Security check

Type the characters as shown above

7. Select a support plan (I select Basic support – free) and click to complete sign up.



Sign up for AWS

Select a support plan

Choose a support plan for your business or personal account. Compare plans and pricing examples. You can change your plan anytime in the AWS Management Console.

● Basic support - Free
- Recommended for new users just getting started with AWS
- 24x7 self-service access to AWS resources
- For account and billing issues only
- Access to Personal Health Dashboard & Trusted Advisor

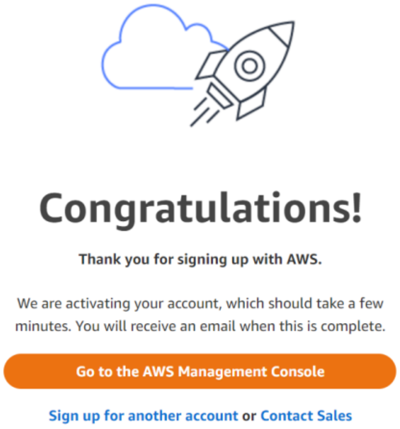
○ Developer support - From $29/month
- Recommended for developers experimenting with AWS
- Email access to AWS Support during business hours
- 12 (business)-hour response times

○ Business support - From $100/month
- Recommended for running production workloads on AWS
- 24x7 tech support via email, phone, and chat
- 1-hour response times
- Full set of Trusted Advisor best-practice recommendations

Need Enterprise level support?

From $15,000 a month you will receive 15-minute response times and concierge-style experience with an assigned Technical Account Manager. Learn more

8. Done!!!



Congratulations!

Thank you for signing up with AWS.

We are activating your account, which should take a few minutes. You will receive an email when this is complete.

Go to the AWS Management Console
Sign up for another account or Contact Sales

Finally, we created an AWS Account. Now move on the next step to create some AWS SDK Credentials.

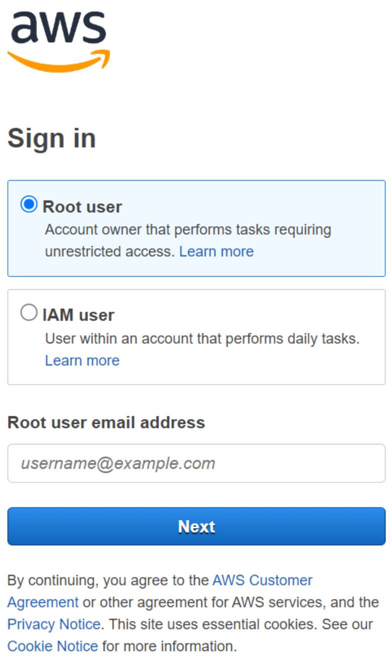
Create an IAM user

When we create an AWS account, the account is provided with root credentials. Those credentials consist of two access keys (Through creating IAM users) :

- Access key ID
- Secret access key

Note: we need access keys to make programmatic calls to AWS. (Will need to connect Raspberry Pi)

To sign in as a root user: Sign in through root user. (Where You need the email address and password of your AWS account.)



aws

Sign in

● Root user
Account owner that performs tasks requiring unrestricted access. Learn more

○ IAM user
User within an account that performs daily tasks. Learn more

Root user email address

username@example.com

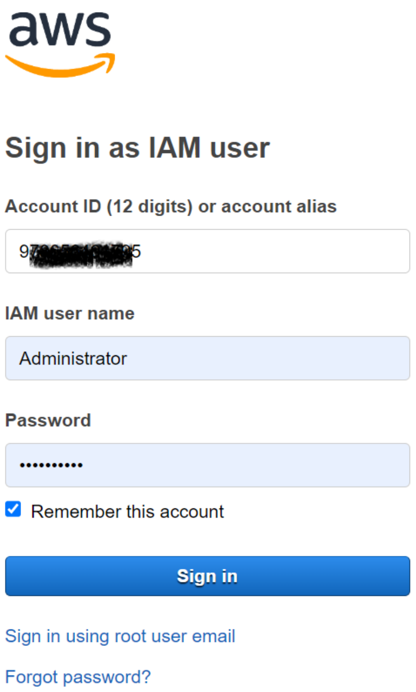
Next

By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.

To sign in as an IAM user: The account owner provides you with the account ID or alias, your user's name, and your password.

Now, 1. Choose **IAM user**, enter the account ID (12 digits) or alias, and choose **Next**.

2. Enter your IAM user name and password and choose **Sign in**.



Sign in as IAM user

Account ID (12 digits) or account alias: [redacted]

IAM user name: Administrator

Password: ••••••••••

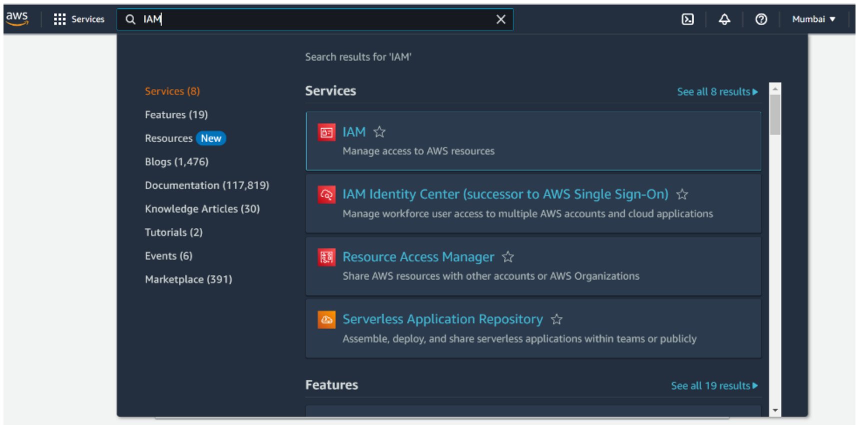
☑ Remember this account

Gather the following information before you sign in. If you do not have this information, contact the administrator of the AWS account owner.

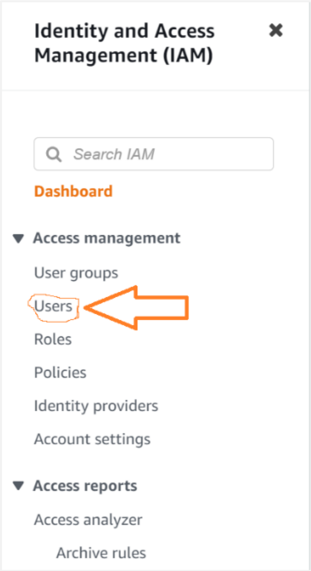
- The 12-digit AWS account ID or the account alias
- The user's name or email address for your IAM user
  - The IAM user name is created by the account administrator
- The password for your IAM user

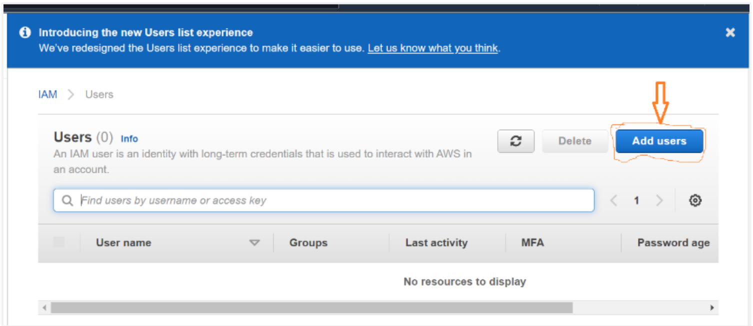
Creating IAM users (console)

1) Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/


aws
Services
IAM
Mumbai ▾
Search results for 'IAM'
Services (8)
Features (19)
Resources New
Blogs (1,476)
Documentation (117,819)
Knowledge Articles (30)
Tutorials (2)
Events (6)
Marketplace (391)
Services
See all 8 results ▸
IAM ☆
Manage access to AWS resources
IAM Identity Center (successor to AWS Single Sign-On) ☆
Manage workforce user access to multiple AWS accounts and cloud applications
Resource Access Manager ☆
Share AWS resources with other accounts or AWS Organizations
Serverless Application Repository ☆
Assemble, deploy, and share serverless applications within teams or publicly
Features
See all 19 results ▸

2) In the navigation penal, choose **Users** and then choose **Add users**.





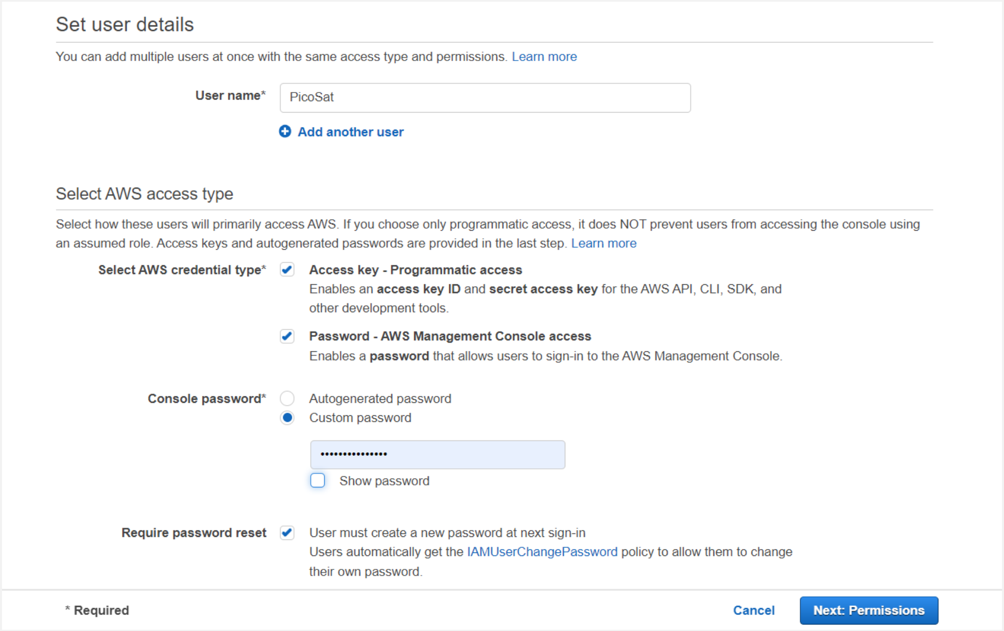
Introducing the new Users list experience

We've redesigned the Users list experience to make it easier to use. Let us know what you think.

Users (0) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

3) Type the user name for the new user. Select programmatic access, access to the AWS Management Console. Provide a **Custom password.** Choose **Next: Permissions**.



Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* PicoSat

Add another user

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. Learn more

Select AWS credential type* ☑ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☑ **Password - AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ○ Autogenerated password
● Custom password

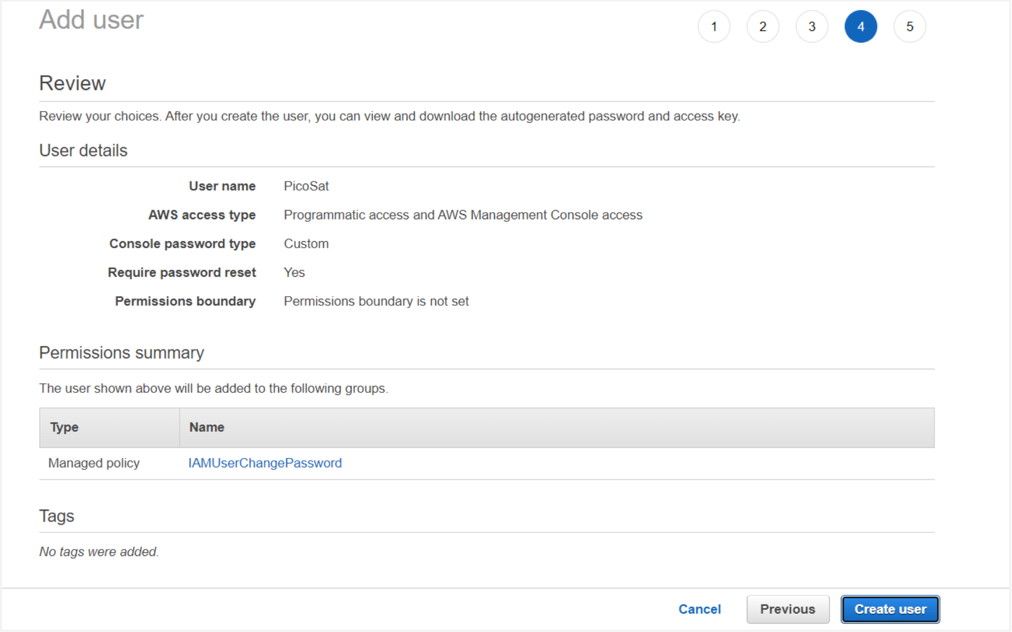
•••••••••••••••

□ Show password

Require password reset ☑ User must create a new password at next sign-in
Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

* Required

4) Choose **Next: Tags**. Choose **Next: Review** and finally choose **Create user.**



Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	PicoSat
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

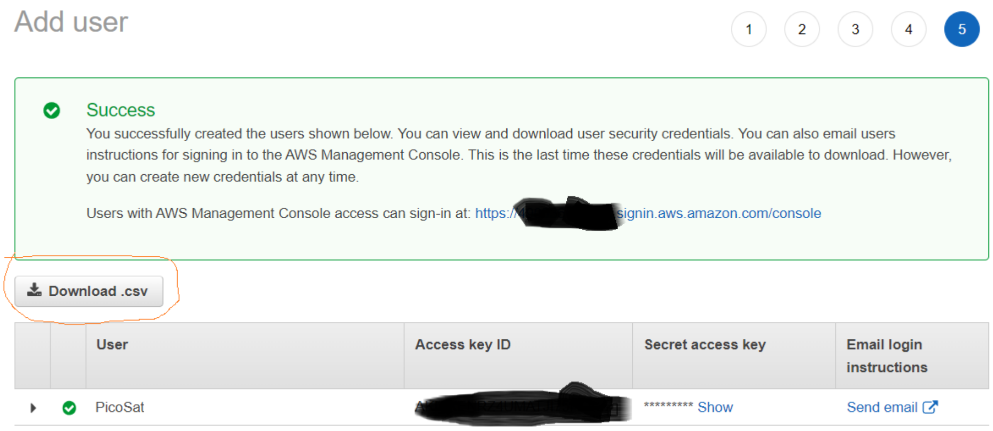
The user shown above will be added to the following groups.

Type	Name
Managed policy	IAMUserChangePassword

Tags

No tags were added.

5) To save the access keys, choose **Download .csv** and then save the file to a safe location.



Add user

1 2 3 4 5

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://[redacted]signin.aws.amazon.com/console

Download .csv

		User	Access key ID	Secret access key	Email login instructions
▸	✓	PicoSat	[redacted]	********* Show	Send email

6) From The top drop-down item My security credentials and download the credentials and save them. These need to be included in the ~/.aws/credentials file of the Linux machine.

```
[default]
aws_access_key_id = YOUR_ACCESS_KEY_ID
aws_secret_access_key = YOUR_SECRET_ACCESS_KEY
```

7) Also set the default region where your S3 bucket will reside in ~/.aws/config. For example:

```
[default]
output = json
region = ap-south-1
```

8) Details information provided in this link. Visit and enjoy: https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users_create.html.

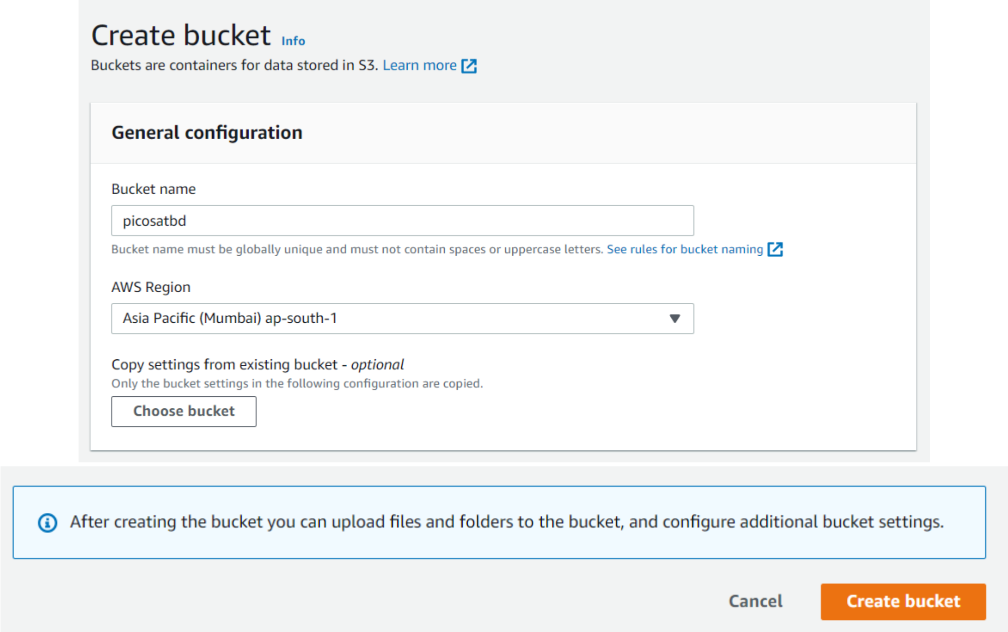
Create an S3 Bucket

Now create an S3 bucket for public website hosting of weather ground station BSMRAAU. Configuring a static website on Amazon S3 follow these steps:

Step 1: Create a bucket

Sign in to the AWS Management Console and open the Amazon S3 console at https://console.aws.amazon.com/s3/.

1) Choose **Create bucket**.
2) Enter the Bucket name (for example, picosatbd). Choose the Region where you want to create the bucket. (Asia Pacific (Mumbai) ap-south-1) and then choose **Create**.



Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name: picosatbd

Bucket name must be globally unique and must not contain spaces or uppercase letters. See rules for bucket naming

AWS Region: Asia Pacific (Mumbai) ap-south-1

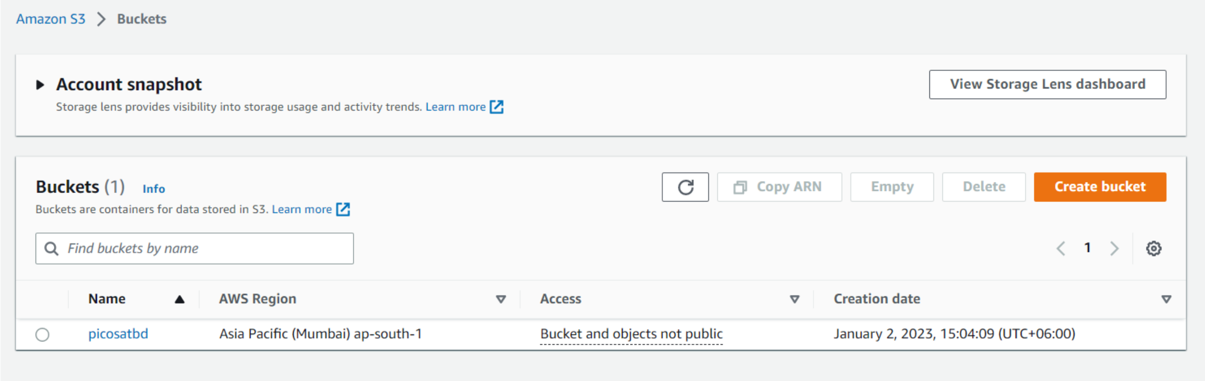
Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

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

Step 2: Enable static website hosting

1) choose the **bucket** and Choose **Properties**.



Amazon S3 > Buckets

Account snapshot

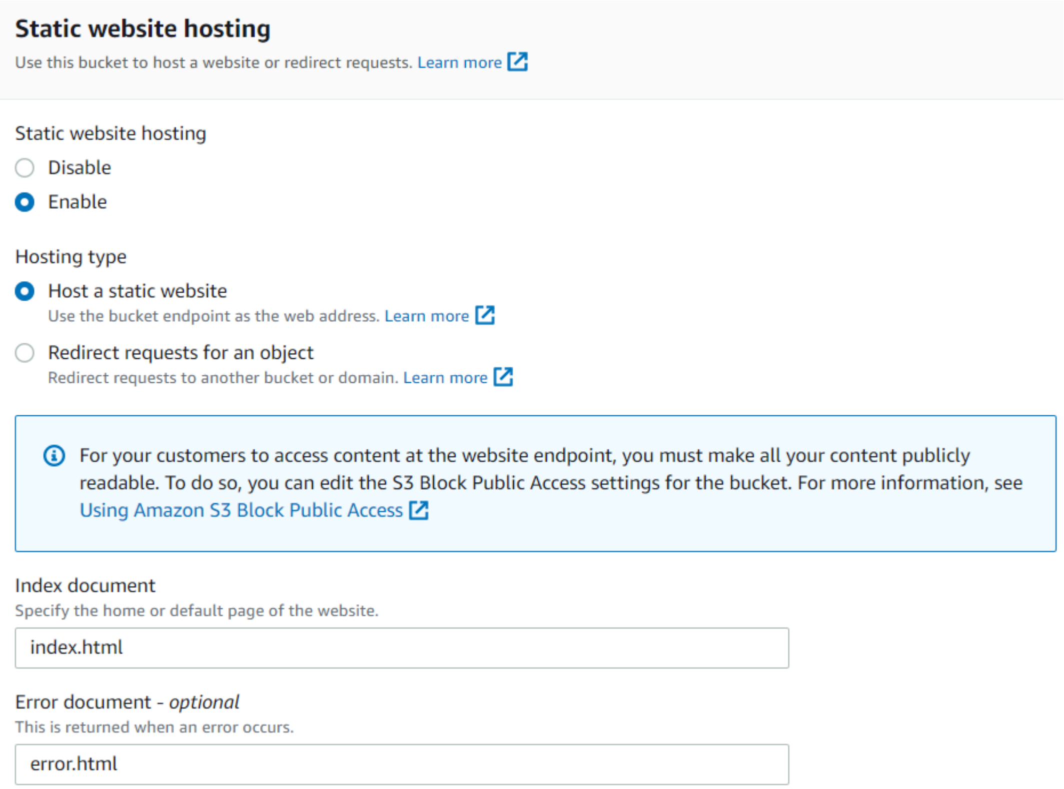
Storage lens provides visibility into storage usage and activity trends. Learn more

Buckets (1) Info

Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	picosatbd	Asia Pacific (Mumbai) ap-south-1	Bucket and objects not public	January 2, 2023, 15:04:09 (UTC+06:00)

2) Under **Static website hosting**, choose **Edit**. (Scroll down)
3) Under Static website hosting, choose **Enable**.
4) In Index document, enter the file name of the index document, typically index.html.



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.

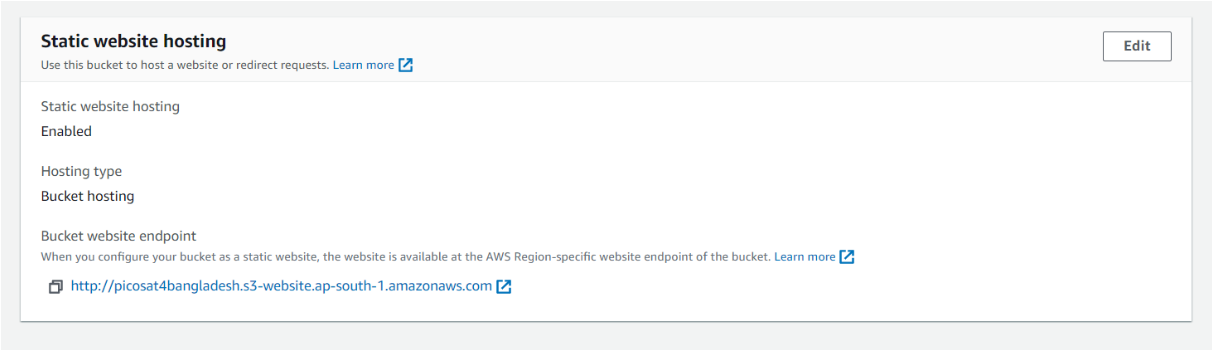
index.html

Error document - *optional*

This is returned when an error occurs.

error.html

5) Choose **Save changes**. (Scroll down)
6) Under **Static website hosting**, note the **Endpoint**.



Static website hosting

Use this bucket to host a website or redirect requests. Learn more

Static website hosting

Enabled

Hosting type

Bucket hosting

Bucket website endpoint

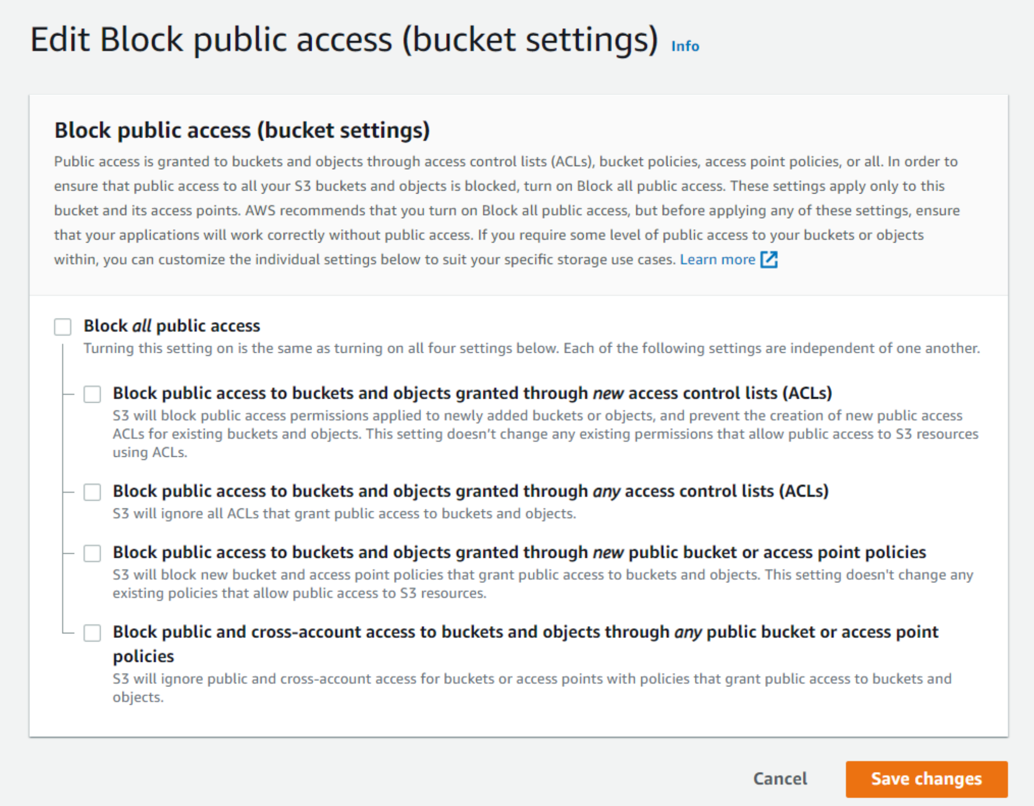
When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. Learn more

http://picosat4bangladesh.s3-website.ap-south-1.amazonaws.com

Step 3: Edit Block Public Access settings

1) Choose the **bucket**.
2) Choose **Permissions.**
3) Under **Block public access (bucket settings)**, choose **Edit**.

4) Clear **Block *all* public access**, and choose **Save changes**.



Edit Block public access (bucket settings) Info

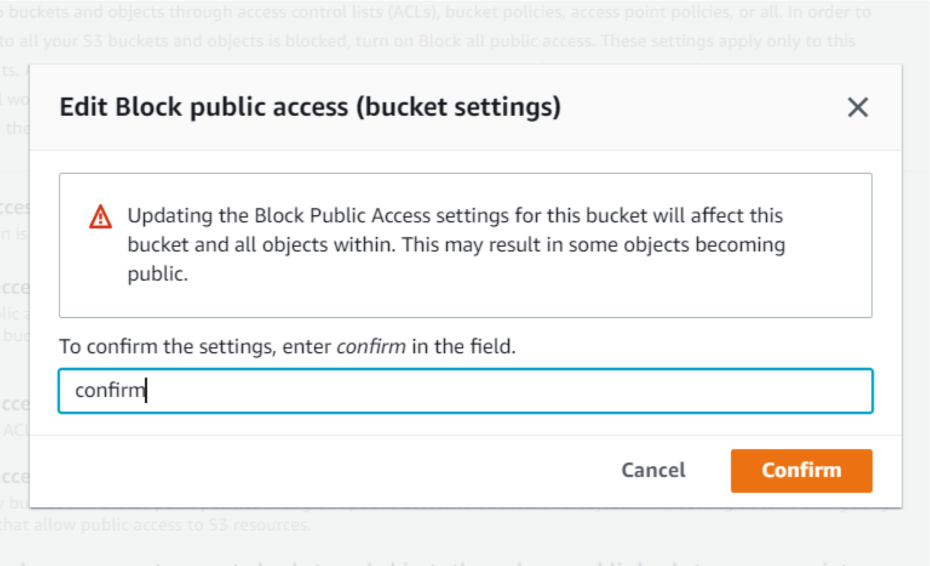
Block public access (bucket settings)

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

□ 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.

5) Type confirm and Click Confirm.



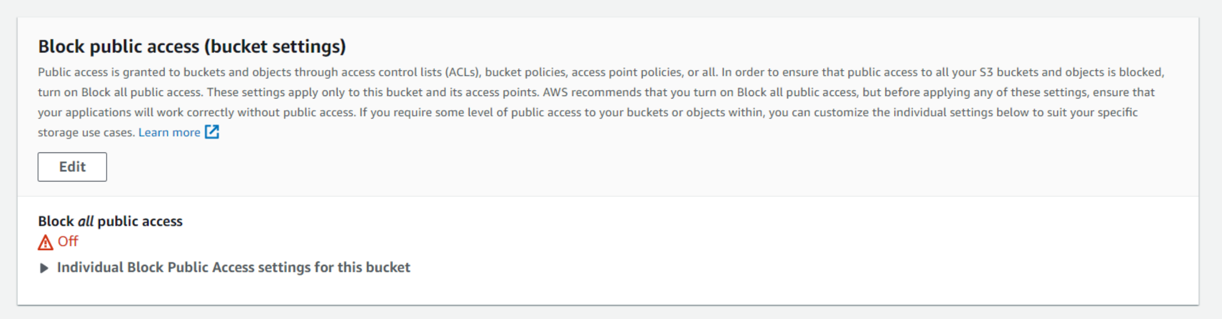
Edit Block public access (bucket settings)

⚠ Updating the Block Public Access settings for this bucket will affect this bucket and all objects within. This may result in some objects becoming public.

To confirm the settings, enter *confirm* in the field.

confirm

6) Block public access no off.



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

Block *all* public access

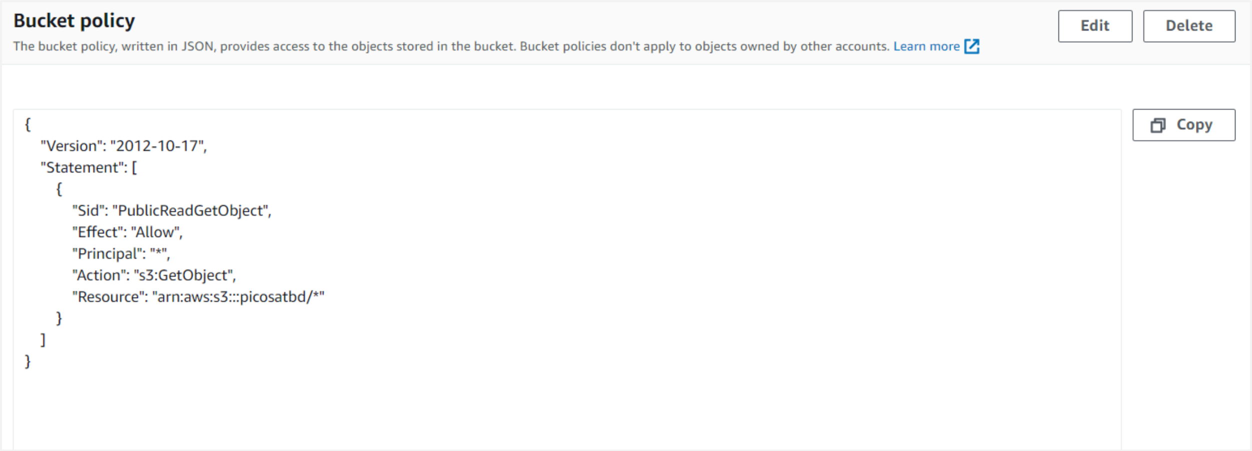
⚠ Off

Step 4: Add a bucket policy that makes your bucket content publicly available

1) Choose the 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:::bucket_name/*"
      }
   ]
}
```

5) Choose **Save changes**.



Bucket policy

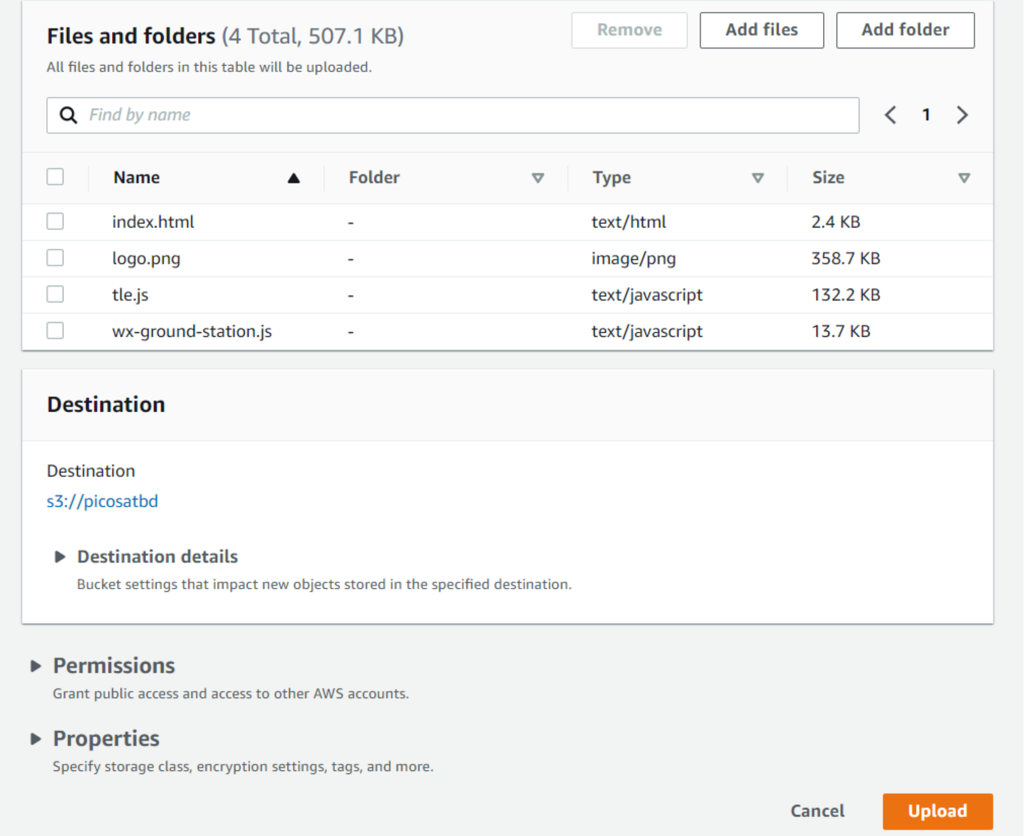
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::picosatbd/*"
        }
    ]
}
```

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

Step 5: Configure an index document

1) Create an index.html file.
2) Save the index file locally.
3) Choose the bucket.
4) To upload the index document to the bucket, do one of the following: (a) Drag and drop the index file into the console bucket listing. (b) Choose Upload, and follow the prompts to choose and upload the index file.



Files and folders (4 Total, 507.1 KB)

All files and folders in this table will be uploaded.

□	Name	Folder	Type	Size
□	index.html	-	text/html	2.4 KB
□	logo.png	-	image/png	358.7 KB
□	tle.js	-	text/javascript	132.2 KB
□	wx-ground-station.js	-	text/javascript	13.7 KB

Destination

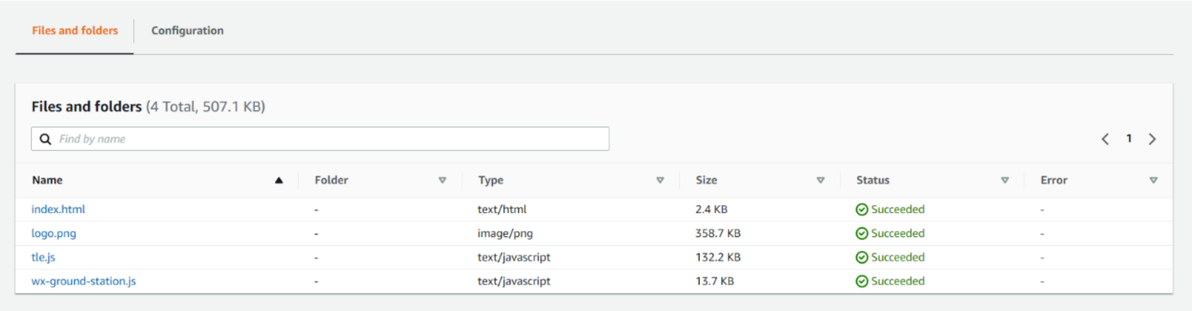
Destination
s3://picosatbd

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

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

▶ **Properties**
Specify storage class, encryption settings, tags, and more.

5) Click Upload.



Files and folders (4 Total, 507.1 KB)

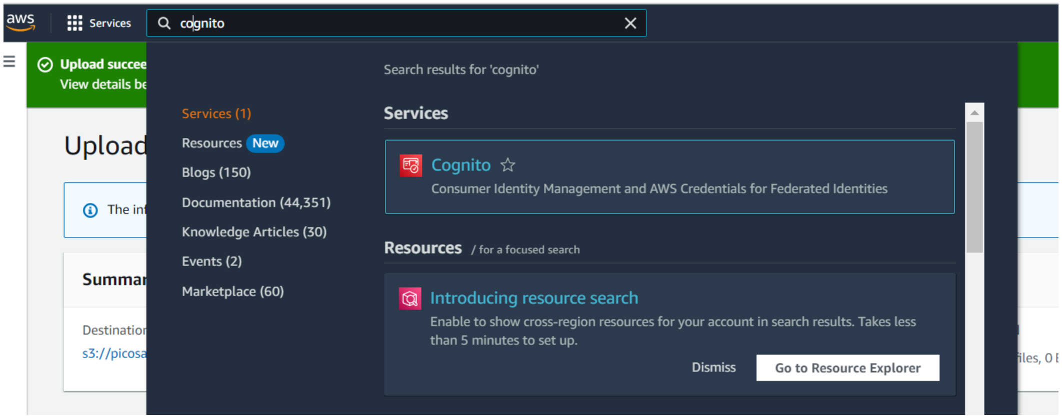
Name	Folder	Type	Size	Status	Error
index.html	-	text/html	2.4 KB	✓ Succeeded	-
logo.png	-	image/png	358.7 KB	✓ Succeeded	-
tle.js	-	text/javascript	132.2 KB	✓ Succeeded	-
wx-ground-station.js	-	text/javascript	13.7 KB	✓ Succeeded	-

6) Go and Check endpoint: http://picosat4bangladesh.s3-website.ap-south-1.amazonaws.com

Create an Identity Pool in Cognito:

To give public users the ability to access we need to set up an identity pool and create a policy allowing them read access to our bucket.

Step-1: From the AWS console, select Cognito.



Search results for 'cognito'

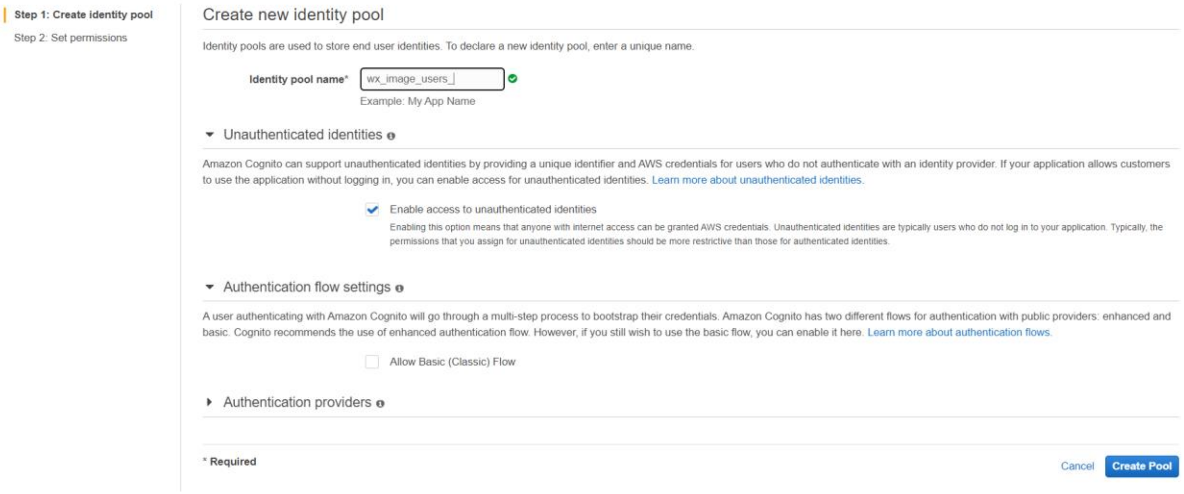
Services

Cognito ☆
Consumer Identity Management and AWS Credentials for Federated Identities

Resources / for a focused search

Introducing resource search
Enable to show cross-region resources for your account in search results. Takes less than 5 minutes to set up.

Step-2: Choose Manage Identity Pools, Create new identity pool, give it a name, say wx_image_users and Choose Enable access to unauthenticated identities (Be sure to select the region in the upper right of the page that matches the region where your S3 bucket was created!) Choose Create Pool.



Create new identity pool

Identity pools are used to store end user identities. To declare a new identity pool, enter a unique name.

Identity pool name* wx_image_users_
Example: My App Name

Unauthenticated identities

Amazon Cognito can support unauthenticated identities by providing a unique identifier and AWS credentials for users who do not authenticate with an identity provider. If your application allows customers to use the application without logging in, you can enable access for unauthenticated identities. Learn more about unauthenticated identities.

☑ Enable access to unauthenticated identities
Enabling this option means that anyone with internet access can be granted AWS credentials. Unauthenticated identities are typically users who do not log in to your application. Typically, the permissions that you assign for unauthenticated identities should be more restrictive than those for authenticated identities.

Authentication flow settings

A user authenticating with Amazon Cognito will go through a multi-step process to bootstrap their credentials. Amazon Cognito has two different flows for authentication with public providers: enhanced and basic. Cognito recommends the use of enhanced authentication flow. However, if you still wish to use the basic flow, you can enable it here. Learn more about authentication flows.

□ Allow Basic (Classic) Flow

Authentication providers

* Required

Step-3: Click View Details and click Allow. On the Sample code page, select JavaScript, copy the code underneath Get AWS Credentials and save it some place. This will be added in the website/wx-ground-station.js script later.

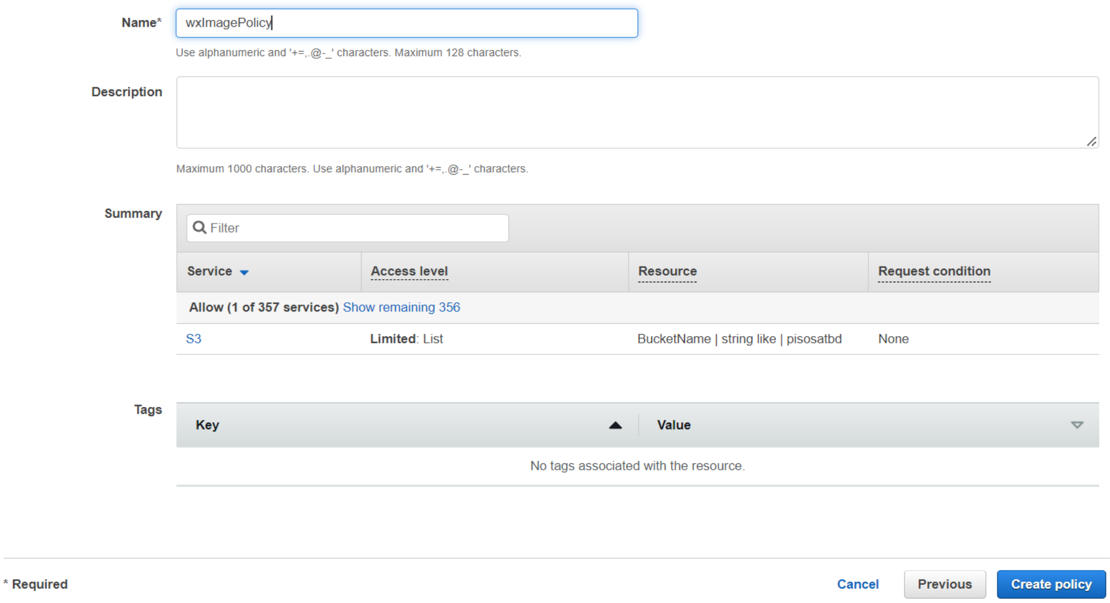
```
         // Initialize the Amazon Cognito credentials provider

AWS.config.region = 'ap-south-1'; // Region
AWS.config.credentials = new AWS.CognitoIdentityCredentials({
   IdentityPoolId: 'ap-south-1:d9c7009a-4005-4572-b65b-4f0fa7ff116b',
                            });
```

Step-4: Add a Policy to the Created IAM Role. In IAM console, choose Policies. Click Create Policy, then click the JSON tab and add this, substituting BUCKET_NAME with your bucket name.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "s3:ListBucket"
         ],
         "Resource": [
            "arn:aws:s3:::bucket_name"
         ]
      }
   ]
}
```

Click Review policy and give your policy a name, like wxImagePolicy and Click Create policy.



Name* wxImagePolicy

Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

Filter

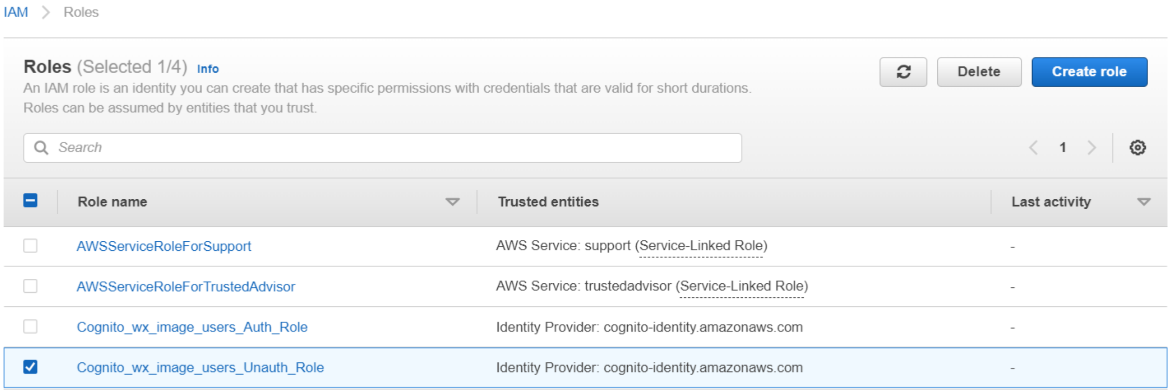
Service	Access level	Resource	Request condition
Allow (1 of 357 services) Show remaining 356			
S3	**Limited**: List	BucketName | string like | pisosatbd	None

Tags

Key	Value
No tags associated with the resource.	

* Required

In IAM console, click Roles, then choose the unauthenticated user role previously created when the identity pool was created (e.g. wxImagePolicy).



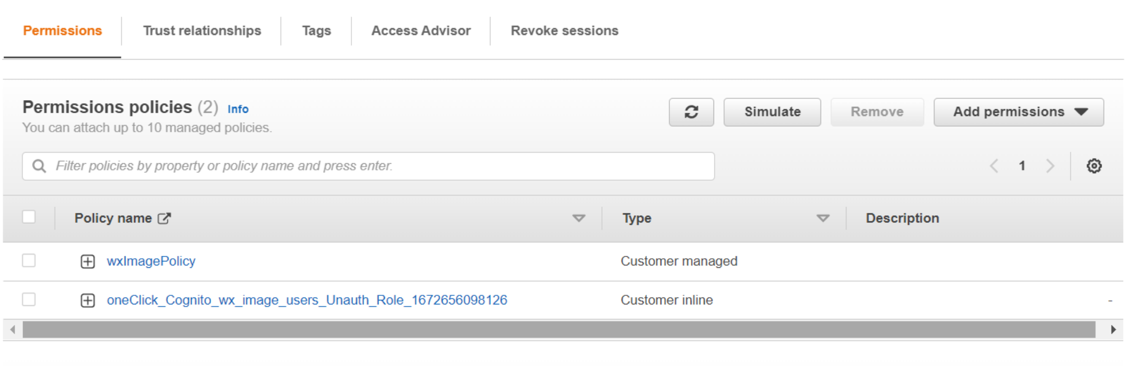
IAM > Roles

Roles (Selected 1/4) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

	Role name	Trusted entities	Last activity
□	AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
□	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
□	Cognito_wx_image_users_Auth_Role	Identity Provider: cognito-identity.amazonaws.com	-
☑	Cognito_wx_image_users_Unauth_Role	Identity Provider: cognito-identity.amazonaws.com	-

Click **Add Permissions**. Choose wxImagePolicy. Click **Attach Policies**.



Permissions policies (2)

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter.

□	Policy name	Type	Description
□	wxImagePolicy	Customer managed	
□	oneClick_Cognito_wx_image_users_Unauth_Role_1672656098126	Customer inline	-

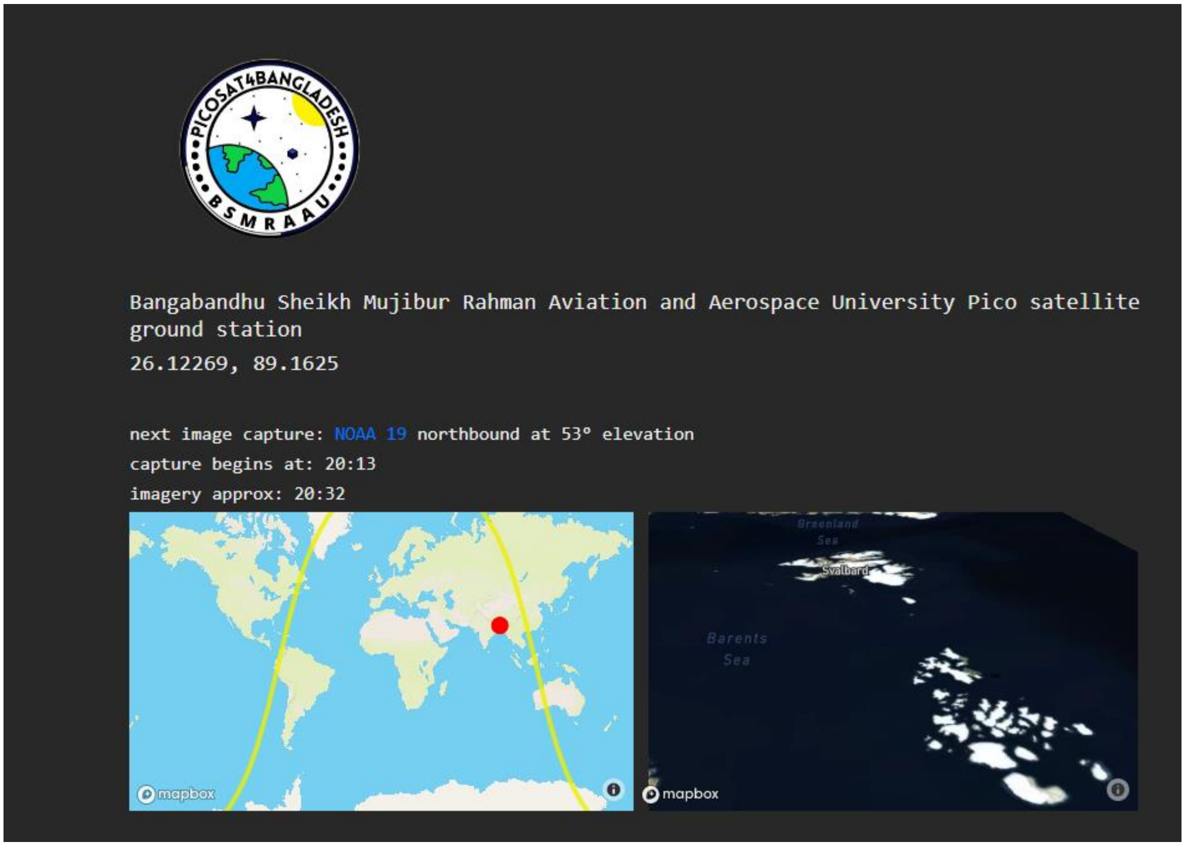
Step-5: Set CORS configuration on the S3 bucket. Select the bucket. Go to the permissions. select CORS configuration and past the following lines:

```
[
    {
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "POST",
            "GET",
            "PUT"
        ],
        "AllowedOrigins": [
            "*"
        ],
        "ExposeHeaders": []
    }
]
```

Click **Save**. S3 bucket configuration is Done.

PicoSat4Bangladesh

Link: http://picosat4bangladesh.s3-website.ap-south-1.amazonaws.com



Bangabandhu Sheikh Mujibur Rahman Aviation and Aerospace University Pico satellite ground station

26.12269, 89.1625

next image capture: NOAA 19 northbound at 53° elevation

capture begins at: 20:13

imagery approx: 20:32

Prepared By,
Jolok Banarjee ASE-02
ID: 21014026, BSMRAAU
Software Team
PicoSAT4Bangladesh Project

02-01-2023