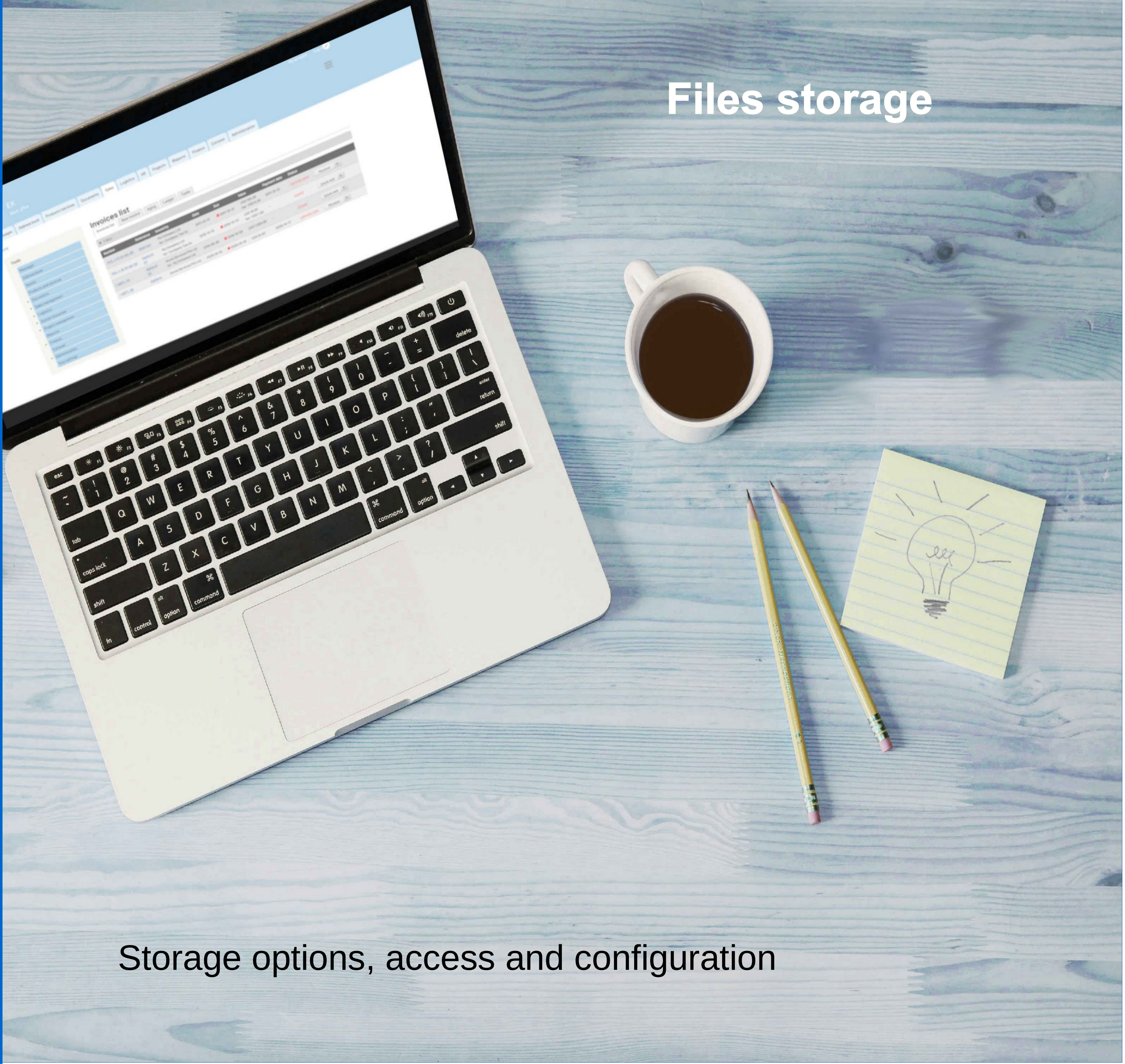
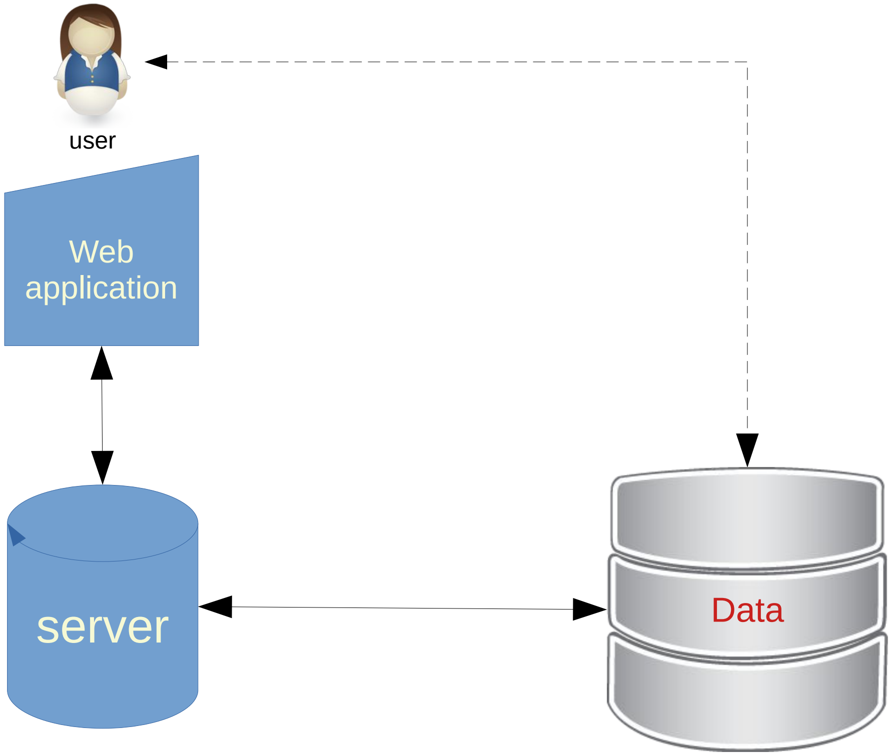
Files storage



Storage options, access and configuration

How files are stored

Definitions:
- Data: any files, document, uploaded by the system via application
- Remote: on a different server, IP address or host from the application host
- AWS S3: **A**mazon **w**eb **s**ervice **s**imple **s**torage **s**ervice
- Bucket: a folder with unique name that store Data



Top ↑

How files are stored

The EK application uses AWS S3 as remote data storage solution.

Files are store in personal dedicated directory called buckets

Buckets are accessed :

1) during upload of data via web application
2) during download of data via web application
3) directly by user having access to the data server with password and login

Data are **not stored** on the application server.

Advantages:

- save space on server;
- increase security, take advantage of AWS S3 data durability, redundency;
- enable access to data storage via personal login and password;
- possibility to own and control your own storage service;
- possibility to use compatible AWS S3 storage services;

Important:

- there is no backup of remote storage to another remote storage;
- if you need a backup of standard remote data provided with the service, you have to setup your own backup;

Top ↑

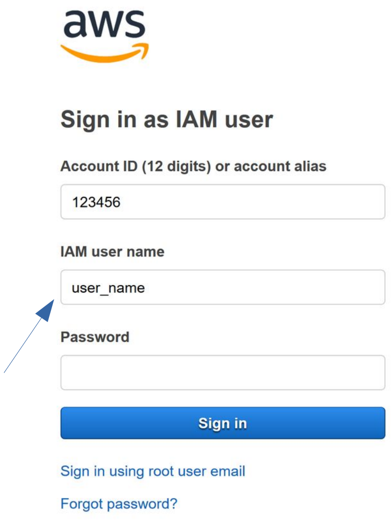
How to access storage for authorized users

With a login and password, Remote data can be access directly by authorized users.
With this access, you can browse, read and download any data.

Login page is:

https://[123456789].signin.aws.amazon.com/console

This is account number provided by vendor or your own account



Sign in as IAM user

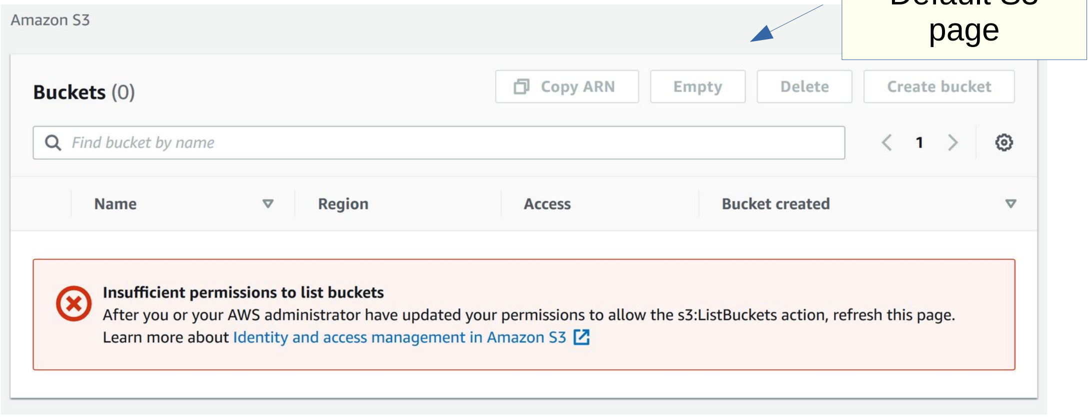
Account ID (12 digits) or account alias: 123456

IAM user name: user_name

Password:

User name and password are provided by vendor created from your own account

Default S3 page



Amazon S3

Buckets (0)

	Name	Region	Access	Bucket created

Insufficient permissions to list buckets
After you or your AWS administrator have updated your permissions to allow the s3:ListBuckets action, refresh this page.
Learn more about Identity and access management in Amazon S3

Top ↑

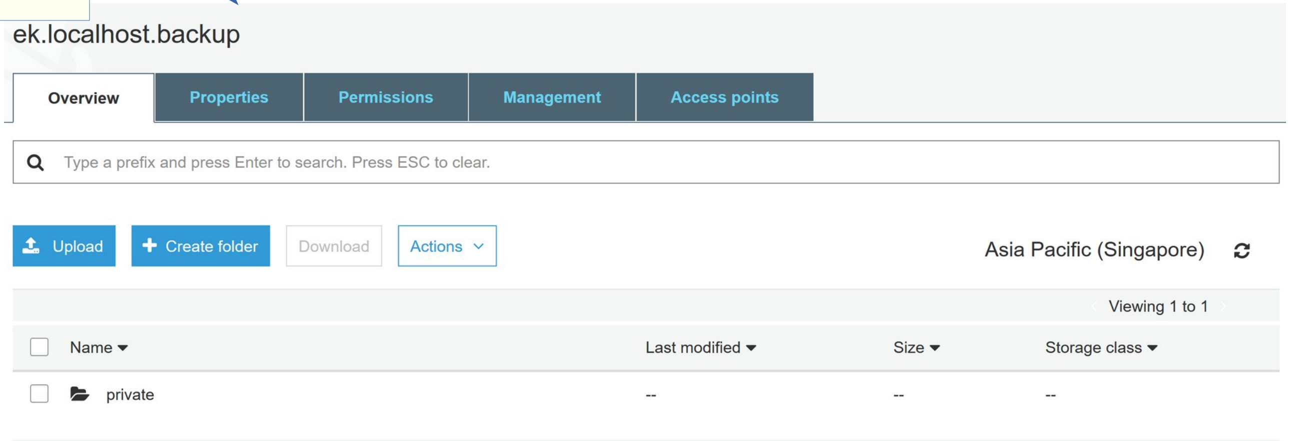
How to access storage for authorized users

You can go to your bucket via link:

https://s3.console.aws.amazon.com/s3/**buckets**/[bucket_name]/?region=ap-southeast-1&tab=overview

This is bucket name or directory provided by vendor or your own account

Sample view with bucket name: ek.localhost.backup



ek.localhost.backup

Asia Pacific (Singapore)

Viewing 1 to 1

□	Name	Last modified	Size	Storage class
□	private	--	--	--

Top ↑

Set-up you own AWS S3 account

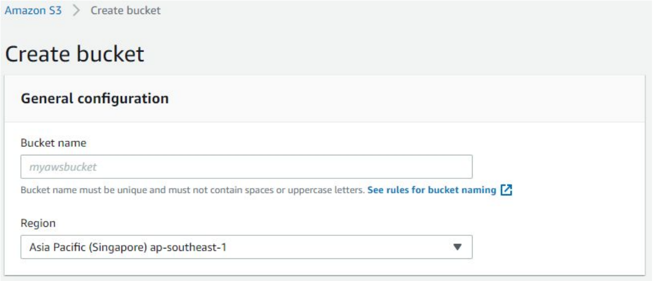
You can setup your own AWS S3 account if you want full control on access.

To register an account : https://portal.aws.amazon.com/billing/signup#/

First 12 months of usage are free with AWS.

Once account is created you have to follow the steps for S3 setup:

- Go to S3 service page;
- Create a bucket;



Create bucket

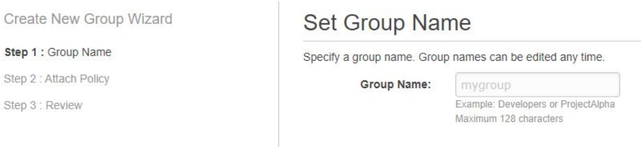
General configuration

Bucket name: myawsbucket

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

Region: Asia Pacific (Singapore) ap-southeast-1

- Go to IAM service page;
- Create an access group to the above bucket with access rights;



Set Group Name

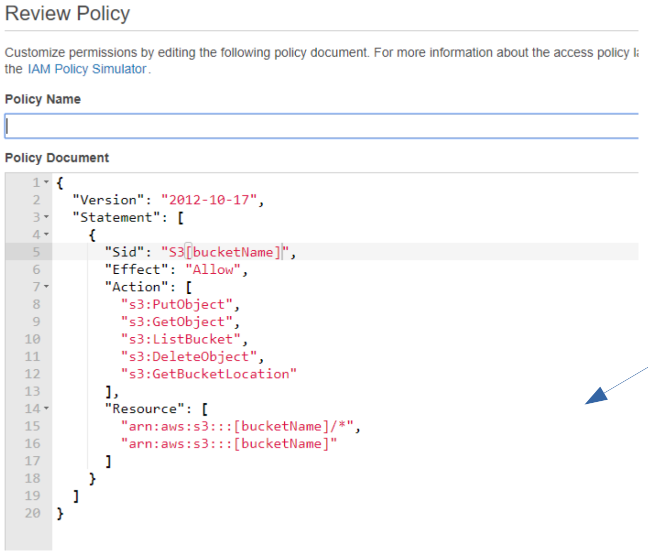
Specify a group name. Group names can be edited any time.

Group Name: mygroup

Example: Developers or ProjectAlpha
Maximum 128 characters

Top ↑

Set-up you own AWS S3 account



Review Policy

Customize permissions by editing the following policy document. For more information about the access policy l
the IAM Policy Simulator.

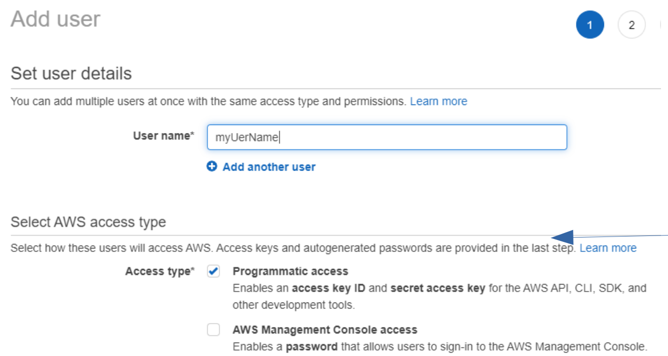
Policy Name

Policy Document

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3[bucketName]",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:DeleteObject",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::[bucketName]/*",
        "arn:aws:s3:::[bucketName]"
      ]
    }
  ]
}
```

Group access policy for read and write specific to your bucket

- Create a user and assign the above group to it;



Add user

Set user details

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

User name* myUerName

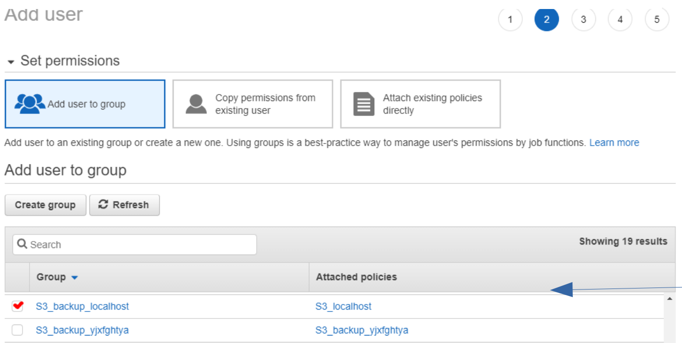
Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. Learn more

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

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

Create



Add user

Set permissions

Add user to group
Copy permissions from existing user
Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Add user to group

Create group
Refresh
Search

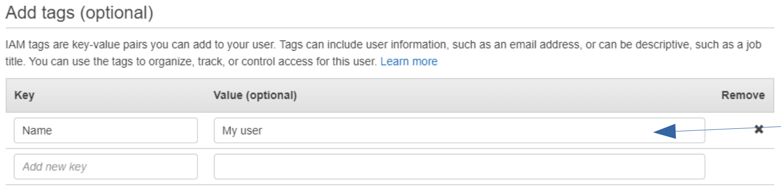
Showing 19 results

	Group	Attached policies
✓	S3_backup_localhost	S3_localhost
☐	S3_backup_yjxfghtya	S3_backup_yjxfghtya

Connect to group

Top ↑

Set-up you own AWS S3 account



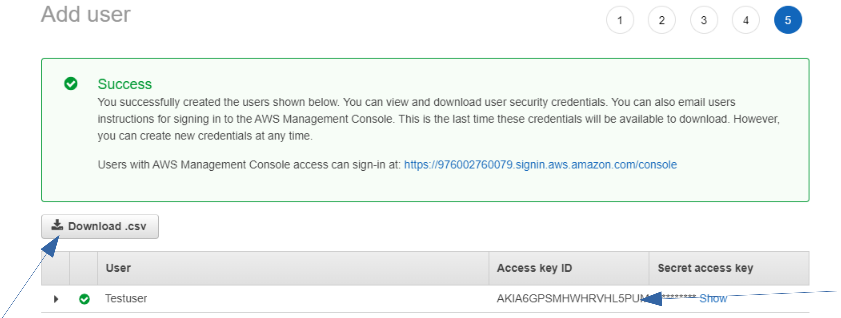
Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. Learn more

Key	Value (optional)	Remove
Name	My user	✖
Add new key		

Option

- Download and keep **public and private access** keys for that user (Keys can only be downloaded or view once!).



Add user

✔ 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://976002760079.signin.aws.amazon.com/console

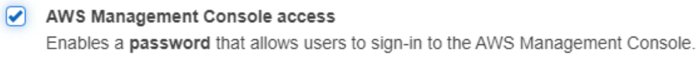
		User	Access key ID	Secret access key
▸	✔	Testuser	AKIA6GPSMHWHRVHL5PUM	******** Show

View/copy Keys

Download Keys (store in safe place)

We need the private and public keys to connect the application to your own AWS S3 storage.

You can create as many users with access group as you need. You can create user *access via console* to be able to access files directly from web browser



☑ AWS Management Console access

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

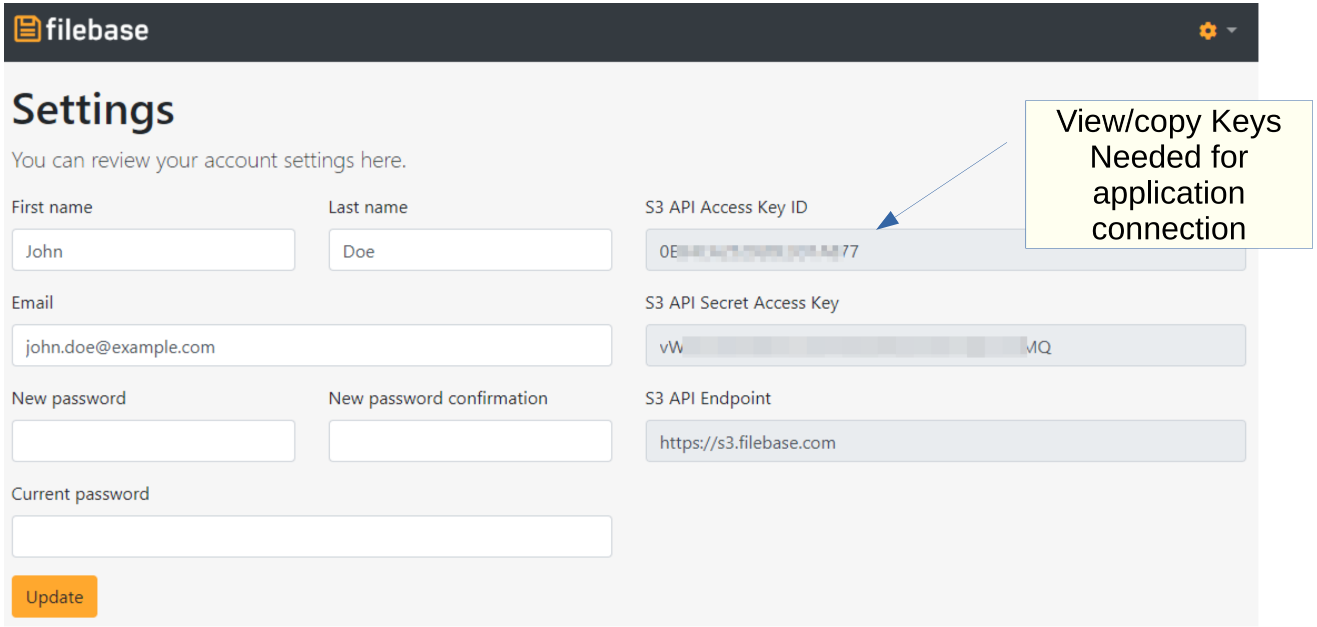
If you use compatible storage services different from AWS S3, we also need the access keys.

Top ↑

AWS compatible storage

https://filebase.com/

Filebase is compatible with AWS S3 that can be used has an alternative for AWS.
You can create your personal account to store files managed by EK application.
Basic account has free storage .



Settings

You can review your account settings here.

First name: John

Last name: Doe

S3 API Access Key ID: 0E[redacted]77

Email: john.doe@example.com

S3 API Secret Access Key: vW[redacted]MQ

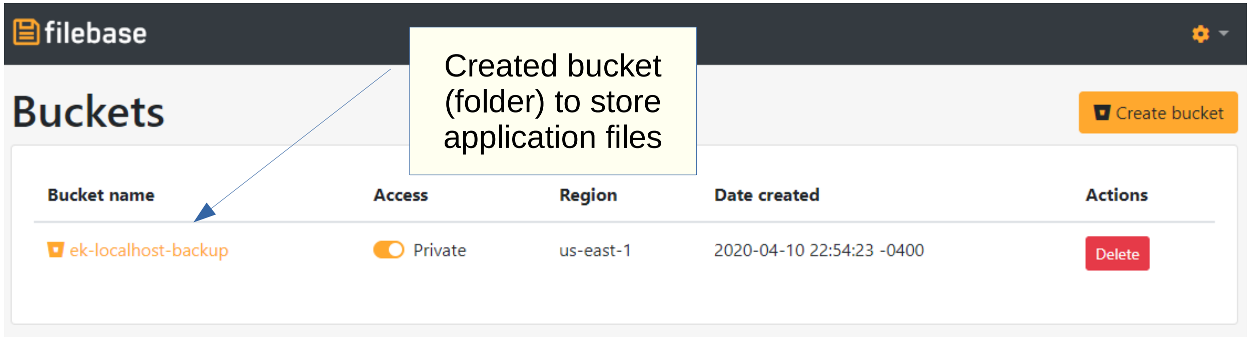
New password:

New password confirmation:

S3 API Endpoint: https://s3.filebase.com

Current password:

View/copy Keys Needed for application connection



Buckets

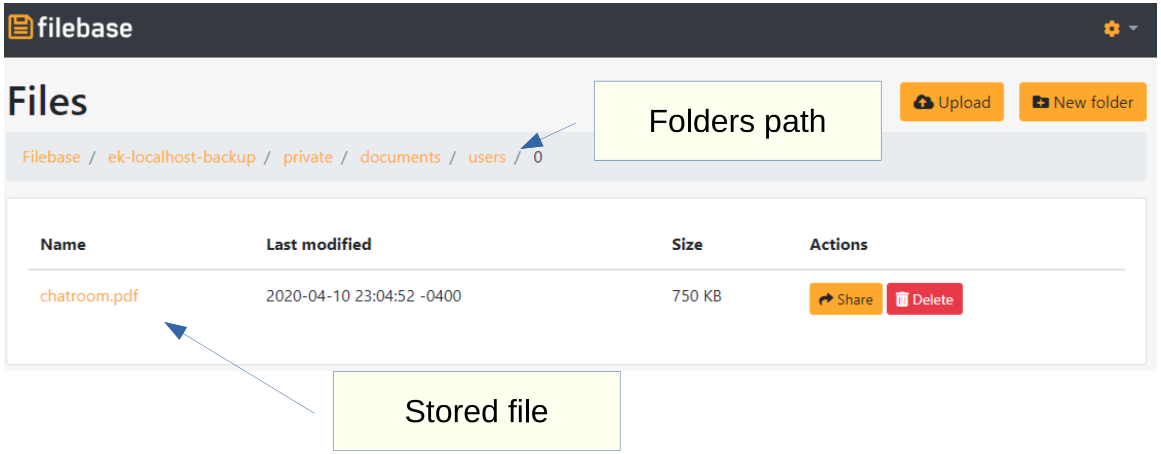
Bucket name	Access	Region	Date created	Actions
ek-localhost-backup	Private	us-east-1	2020-04-10 22:54:23 -0400	Delete

Created bucket (folder) to store application files

Top ↑

AWS compatible storage

Example of bucket and data storage directly managed by EK application



Files

Filebase / ek-localhost-backup / private / documents / users / 0

Name	Last modified	Size	Actions
chatroom.pdf	2020-04-10 23:04:52 -0400	750 KB	Share Delete

Folders path

Stored file

Top ↑

ARREA
Systems

EK