# Working with S3-compatible credentials

When you want to interact with object storage in Cleura using tools that support an Amazon S3 compatible API (such as `s3cmd`, `rclone`, the `aws` CLI, or the Python `boto3` library), you need an S3-compatible access key ID and secret key.

## Creating credentials

You can create a set of S3-compatible credentials with the following command:

```
openstack ec2 credentials create
```

This will return an `Access` and `Secret` key that you can use to populate the `AWS_ACCESS_KEY_ID` and `AWS_SECRET_ACCESS_KEY` environment variables (or whichever configuration options your application requires).

> Your S3-compatible credentials are always scoped to your Cleura *region* and *project*. You cannot reuse an access and secret key across multiple regions or projects.
>
> Also, your credentials are only "S3-compatible" in the sense that they use the same *format* as AWS S3 does. They are never valid against AWS S3 itself.

## Listing credentials

You can list any previously-created credentials with:

```
openstack ec2 credentials list
```

## Configuring your S3 API client

Once you have obtained your S3-compatible access and secret key, you need to configure your S3 client with it.

How exactly you do that depends on your preferred client:

**aws** **mc** **s3cmd**

Create a new profile, named after your Cleura region:

```
aws configure set \
  --profile <region> \
  aws_access_key_id
<access-key>
aws configure set \
  --profile <region> \

aws_secret_access_key
<secret-key>
```

For the `aws` CLI, you cannot define a region's endpoint in the profile. As such, you must add the `--endpoint-url=https://s3-<region>.citycloud.com:8080` option to each `aws s3api` call.

Create a new alias, named after your Cleura region:

```
mc alias set <region> \
  https://s3-
<region>.citycloud.com:
8080 \
  <access-key> <secret-
key>
```

Once you have configured an alias like this, you are able to run bucket operations with `mc` using the `alias/bucket` syntax.

`s3cmd` does not support configuration profiles, so you need to use a separate configuration

file for each Cleura region you want to use:

```
s3cmd -c ~/.s3cfg-<region> --configure
```

- Set your `Access Key` and `Secret Key` when prompted.
- Leave `Default Region` unchanged.
- Set `S3 Endpoint` to `s3-<region>.citycloud.com:8080`.
- Set `DNS-style bucket+hostname:port template for accessing a bucket` to `s3-<region>.citycloud.com:8080` as well.
- Set `Use HTTPS` default).
- Configure GnuPG encryption and your HTTP proxy server, if needed.
- Test access with your supplied credentials.

On subsequent invocations of the `s3cmd` CLI, always add the `-c ~/.s3cfg-<region>` option.

## Deleting credentials

If at any time you need to delete a set of AWS-compatible credentials, you can do so with the following command:

```
openstack ec2 credentials delete <access-key-id>
```

Deleting a set of S3-compatible credentials will *immediately* revoke access for any applications that were using it.

Last update: 2022-11-07
Created: 2022-09-11
Authors: Florian Haas, Foad Lind