

How to - Storage of Medplum

What [↗](#)

i Medplum has by default a storage bucket. This document explains what to do if we manage to upload a file to the bucket but it is not possible to download and view files uploaded via the pre-signed URL process.

How [↗](#)

For pre-signed URLs in Cloudfront to work, it is important to have different configurations set up.

Error of Invalid Key [↗](#)

```
InvalidKeyUnknown Key
This XML file does not appear to have any style information associated with it. The document tree is shown below.
<Error>
  <Code>InvalidKey</Code>
  <Message>Unknown Key</Message>
  ...
</Error>
```

If the error that you see is about the invalid Key, the steps to bypass this error are :

- Find the storagePublicKey in the medplum.env.config.json of the cdk repository
- Go in AWS Cloudfront <https://us-east-1.console.aws.amazon.com/cloudfront/v4/home?region=eu-west-3#/publickey> and verify that the public key is available. If it is not available, then create it.
- Go to the Key groups <https://us-east-1.console.aws.amazon.com/cloudfront/v4/home?region=eu-west-3#/keygrouplist> and verify that the key has been associated to the keygroup linked to the environnement (ie *MedplumUatuseast1StorageStorageKeyGroupF3DXXXX*).
- Validate that the key group is linked to the correct cloudfront distribution (correct s3 bucket).

This should be sufficient to fix this error

Error of access denied [↗](#)

```
1 <Error>
2 <script type="text/javascript" src="chrome-extension://dadeefbkfcpaeacnafgceahcpjlfmmjj/scripts/war.js"/>
3 <Code>AccessDenied</Code>
4 <Message>Access Denied</Message>
5 ...
6 </Error>
```

If you encounter this error, this can come from an issue with the permission policy of the bucket.

Follow these steps :

- Go to the cloudfront distribution <https://us-east-1.console.aws.amazon.com/cloudfront/v4/home?region=eu-west-3#/distributions>
- Go inside of the cloudfront distribution associated to the bucket
- Go to the tab "Origin"
- You should have one Origin line. Check the Origin Access and note the Identifier

Origins							Edit	Delete	Create origin
Filter origins by property or value							< 1 > ⚙		
Origin name	Origin domain	Origin path	Origin type	Origin ...	Origin access				
Medplum	Storage storage.	s3.eu-central-1.amazo...	S3	-	origin-access-identity/cloudfront	EF5CH			

- Go to the left menu Security > Origin Access > Identities
- Find the origin access that has the same id that the previously noted one.
- Copy the Canonical User Id
- Go to the S3 bucket permission policy and verify update the policy so that you have this :

```

},
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access Identity EF5CH3[REDACTED]"
  },
  "Action": [
    "s3:GetObject*",
    "s3:GetBucket*",
    "s3:List*"
  ],
  "Resource": [
    "arn:aws:s3:::storage.uat.apneal.ai",
    "arn:aws:s3:::storage.uat.apneal.ai/*"
  ]
}
]

```

Origin Access previously noted