

AWS Salesforce Integration

Table of Contents

1. PREREQUISITE	2
1.1.1. Create bucket	
1.1.2. Create IAM User	
2. ASSIGN PERMISSION SET TO USER.....	4
3. CHECK APEX SETTINGS.....	4
4. AS3 CONFIGURATION	4
5. ADD COMPONENT ON OBJECT	5
6. UPLOAD FILES	5
7. SINGLE FILE DOWNLOAD	7
8. FILE PREVIEW	7
9. MULTIPLE FILES DELETE	8
10. SINGLE FILE DELETE.....	9
11. SEARCH S3 FILE	10
12. SEE THE S3 FILE	11

Prerequisite: -

Mandatory Steps: -

1. Users must have an Amazon S3 account with a valid AWS **Access Key Id** and AWS **Secret Key**.
2. A **Bucket** must be **created** on an S3 account with an appropriate **region** to store files.

Before we start configuration for the IAM user, make sure the below steps are complete: -

Steps to Sign Up for Amazon S3

To start with **AS3 Connector**, you must have AWS Key Id and Secret Access Key. For that you need to Sign Up for Amazon. If you already have an Amazon S3 account just ignore it. Otherwise follow the **AS3 Connector** Amazon Sign up Guide document.

Create Bucket

Use:

The S3 bucket is where all the files will be stored.

Process:

Here are the steps to create an S3 bucket-

1. Login in AWS Management Console.
2. Go to Services > S3> Buckets.
3. Click to create Bucket/select existing bucket.
4. Give bucket name, Aws Region.
5. Give the permissions for Block Public Access settings for this bucket click Block *all* public access and select the following policies: -

“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.

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.

6. Click to "Create bucket" button bucket will be created.
7. In bucket Click to "Permissions" and scroll down.
8. Click edit to Cross-origin resource sharing (CORS) and copy this code.

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

Create IAM User

You need to create an IAM user and give them full access for Amazon S3. Here are the configuration steps.

Get IAM User access keys

1. Login in AWS Management Console.
2. Go to Services > IAM > Users
3. Click "Add User". Create individual IAM users (if not created).
4. Open your IAM User from the list.
5. Open "Security Credentials" section. Click "Create Access key"
6. Download csv file for access keys.

Create IAM User Policy to grant access for Single Bucket

If you want to give access to specific buckets, then create this policy for IAM users.

1. Login in AWS Management Console.
2. Go to Services > IAM > Policies > Create Policy
3. Go to JSON and add below JSON in the text area. Here "bucketname" is the bucket name. You have to replace it with your bucket name.

```
{
  "Version": "2012-10-17",
  "Statement": [ { "Sid": "VisualEditor0",
    "Effect": "Allow",
    "Action": [
      "s3: PutObject",
      "s3: GetObject",
      "s3: DeleteObject",
      "s3: PutObjectAcl",
      "s3: GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::bucketname/*"
  },
  {
    "Sid": "VisualEditor1",
    "Effect": "Allow",
    "Action": [
      "s3:ListAllMyBuckets",
      "s3:GetBucketVersioning",
      "s3:GetBucketLocation",
      "s3:PutBucketVersioning"
    ],
    "Resource": "*"
  },
  {
    "Sid": "VisualEditor2",
    "Effect": "Allow",
    "Action": [ "s3: ListBucketVersions", "s3: ListBucket", "s3: PutBucketCORS" ],
    "Resource": "arn:aws:s3:::bucketname"
  } ]
}
```

4. Click "Review Policy"
5. Give name "S3LinkAccessForSingleBucket"
6. Click "Create Policy"

Assign User Policies to IAM Use

Follow the below steps to grant access of single bucket or all buckets to IAM user

1. Login in AWS Management Console.
2. Go to Services > IAM > Users
3. Click "Add User". Create individual IAM users (if not created).
4. Open IAM User detail
5. Click "Add Permissions"
6. Add "AmazonS3FullAccess" permissions to that user if you want to give full access of Amazon S3
7. If you want to give access for specified buckets add "S3LinkAccessForSingleBucket" permission to that use.

Process to Assign Permission set

After installing a package, you need to assign permission set to user which you have logged in.

Steps to Assign Permission set: -

1. Go to setup enter users in Quick find fox.
2. Click to **users**.
3. Click to username which you have logged in.
4. Click on **permission set Assignment**.
5. Click edit Assignment.
6. Select the permission set **AS3 Custom Integration Permission** which is available in Available permission set.
7. Click to add button and click to save button.
8. After these steps user will be able to process following steps.

Check Apex Settings

Follow the steps to check there are correct settings:

1. Go to gear icon, select setup.
2. In Quick Find Box, write Apex Settings.
3. Select Apex Settings.
4. Select "Deploy Metadata from Non-Certified Package Versions via Apex." Option if not already selected and SAVE.

AS3 Configuration process: -

1. From Application Launcher, select AS3 Connector.
2. Click on AS3 **Configuration**.

3. Click on **Authorization**.
4. Set the AWS **Access Key, Secret Key**.
5. Enter Bucket Name you get Amazon S3.
6. Enter Region Name.
7. Click to save button.
8. There is one Functionality for Reset when we click on **Reset** Button all the fields are empty.
9. Click on Configuration tab.
10. Set the **Max Files to delete** Limit.
11. Select the File preview options (Within Salesforce/New Browser Tab).
12. Click to save button.
13. After Completing the AS3 Configuration user will be perform any action.

Add component on object:-

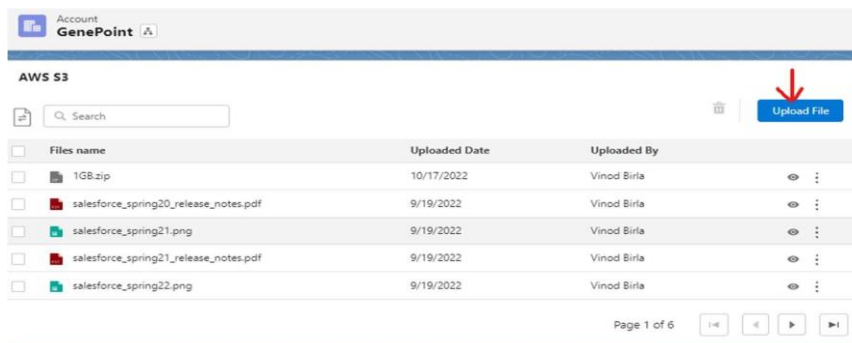
Following are the steps to add component on object:-

1. From Application Launcher, select AS3 Connector.
2. Select any object on which user wants to paste the component.
3. Go on gear icon at the top right corner and select edit page option.
4. Search **s3relatedfiles** custom component in component section.
5. Drag the component and drop anywhere you want on lightning page.

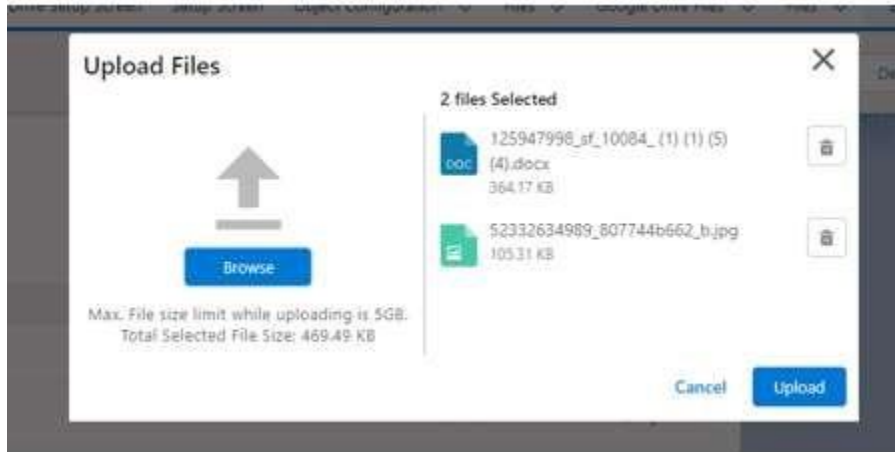
Process to Upload Files

Following are the steps to upload files:-

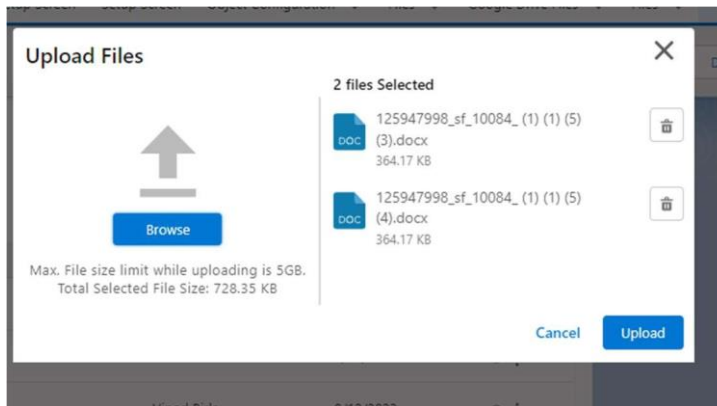
1. Go to Application Launcher, select Account.
2. Open any account record or create new account record.
3. User will see AWS3 Component.
4. Click to **Upload File** Button.



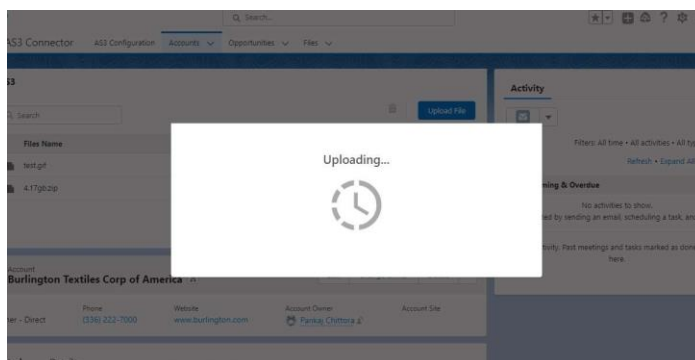
5. Click Browse Files or drop file from Pc (we can select multiple files for upload).



6. User can upload pdfs, .jpg, .png, .jpeg, .exe, .mp4, .mp3, pptx, xlsx, docx, csv, 7z, 3g2, 3gp, xul, xml, xhtml, woff2, woff, webm, weba, wav, vsd, ttf, ts, tiff, tar, swf, sh, rtf, rar, php, otf, opus, ogx, ogv, oga, odt, ods, mpkg, jar, csh, cda, json, midi, jsonld, avi, azw and zip files.
7. There is delete icon for delete any file.



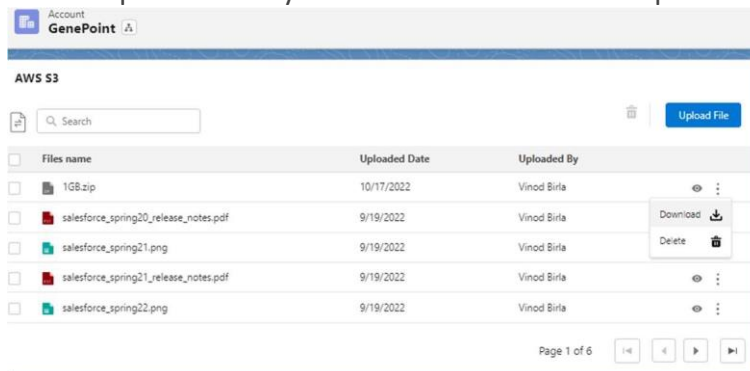
8. Click **Upload** button. And file will be uploaded on particular object and record will be created on **Files** object



Process for Single File Download

Following are the steps to download a file:-

1. Go to Application Launcher, select Account.
2. Open any account record or create new account record.
3. User will see AW S3 Component.
4. Click dropdown of any file and click to **Download** quick action button.

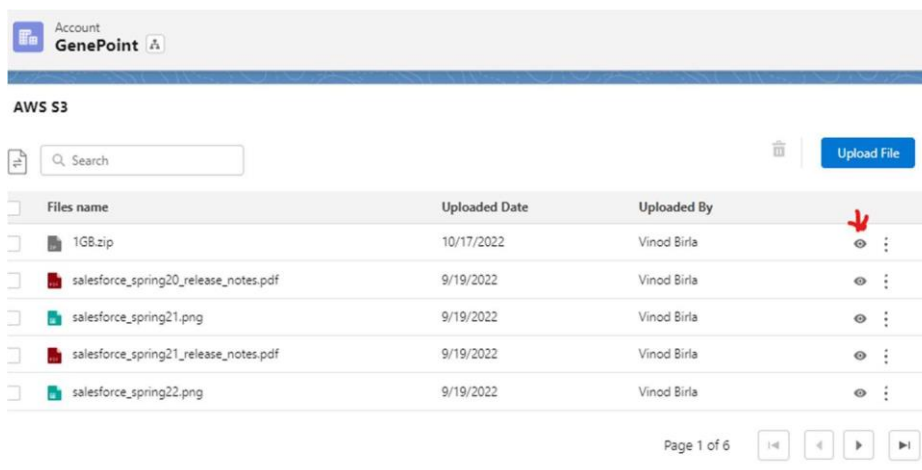


5. And File will be downloaded.

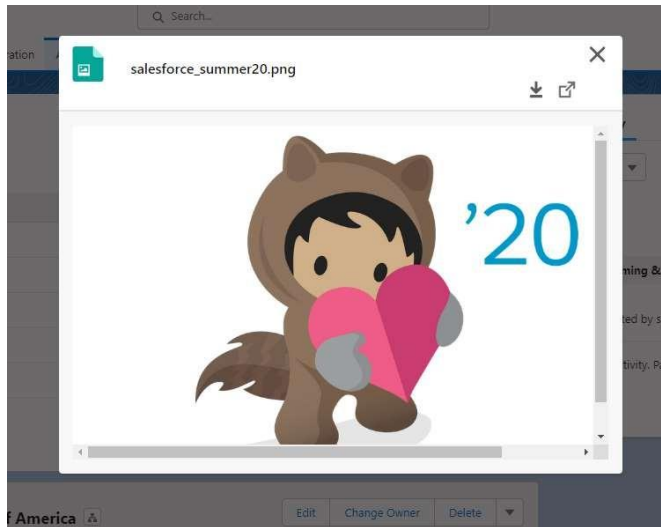
File Preview process

Following are the steps to preview a file:-

1. Go to Application Launcher, select Account.
2. Open any account record or create new account record.
3. User will see AW S3 Component.
4. Click on **Eye Icon** and user will be able to preview the file.



5. Now, user will see the file And There is Download or new window Icon.

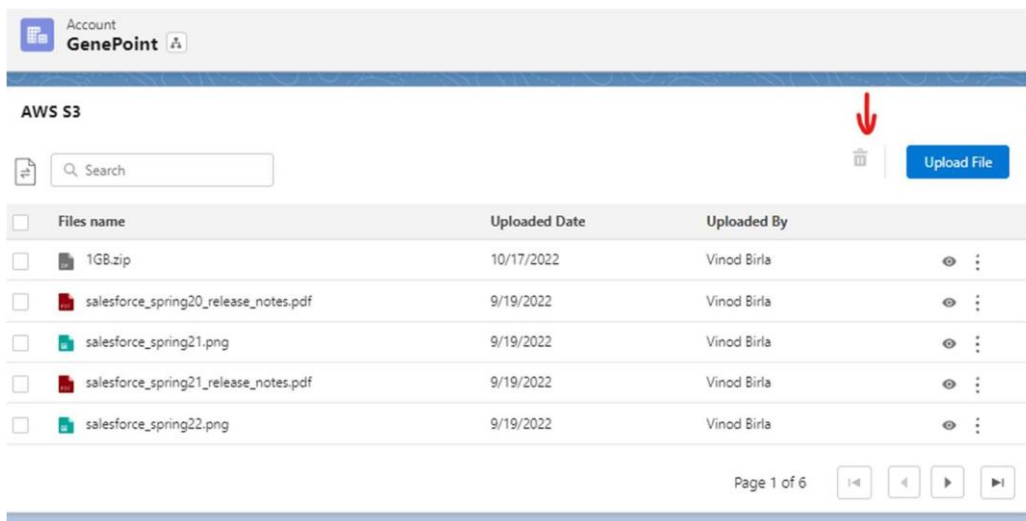


6. User will see the File.

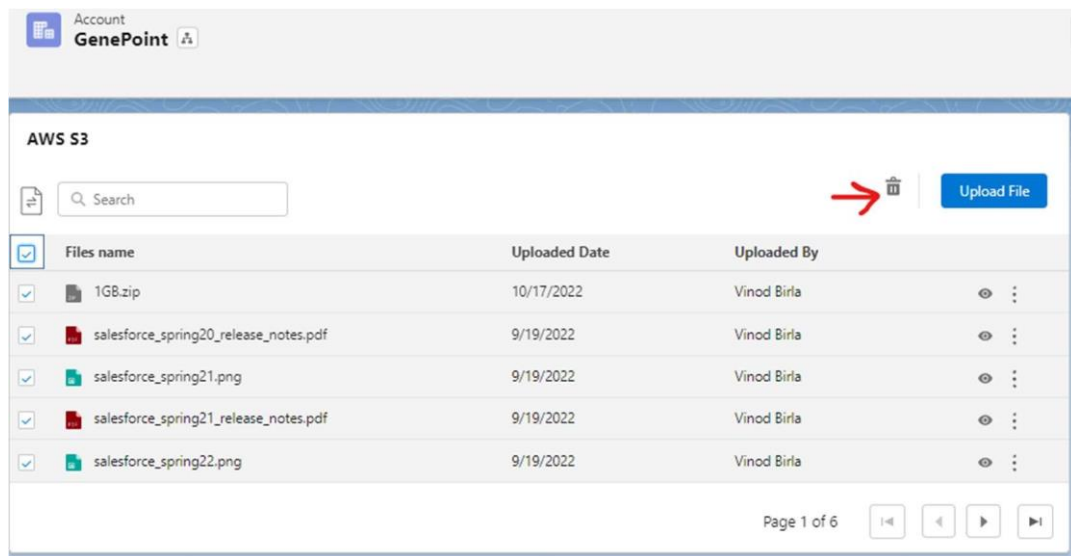
Process for Multiple Files Delete

Following are the steps to delete multiple files simultaneously:-

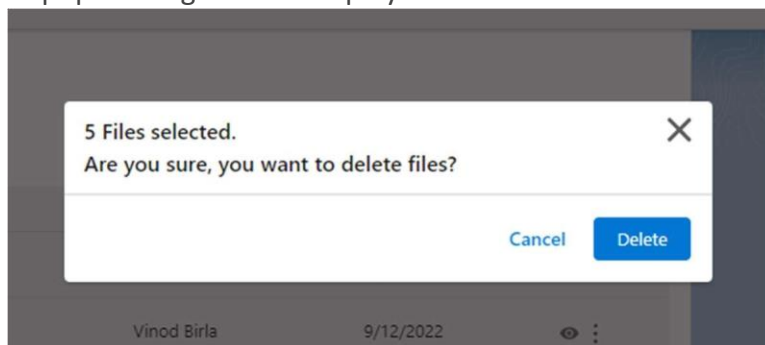
1. Go to Application Launcher, select Account.
2. Open any account record or create new account record.
3. User will see AW S3 Component.



4. User can select file whatever given in **Maximum files to delete** field in configuration tab and **Deleted Icon** Button will be enabled.



5. Click on **Delete Icon** button.
6. Popup message will be display on screen.

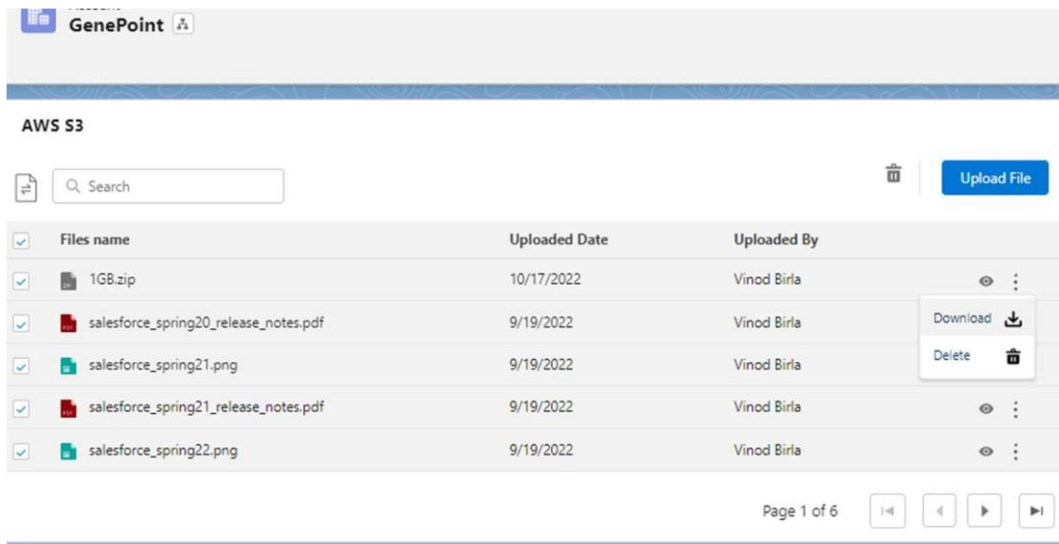


7. Click Yes and Files Will be deleted.

Process for Single File Delete

Following are the steps to delete single file:-

1. Go to Application Launcher, select Account.
2. Open any account record or create new account record.
3. User will see AW S3 Component.
4. Click dropdown of any file and click to **Delete Icon** button.

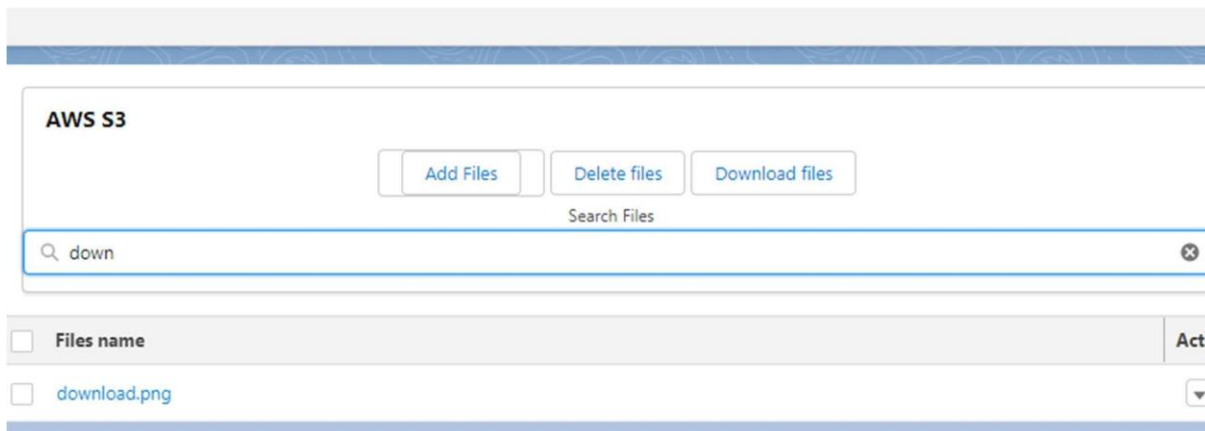


5. Popup message will be display on screen.
6. Click **Yes** and File Will be deleted.

Process to Search S3 Files

Following are the steps to search S3 files:-

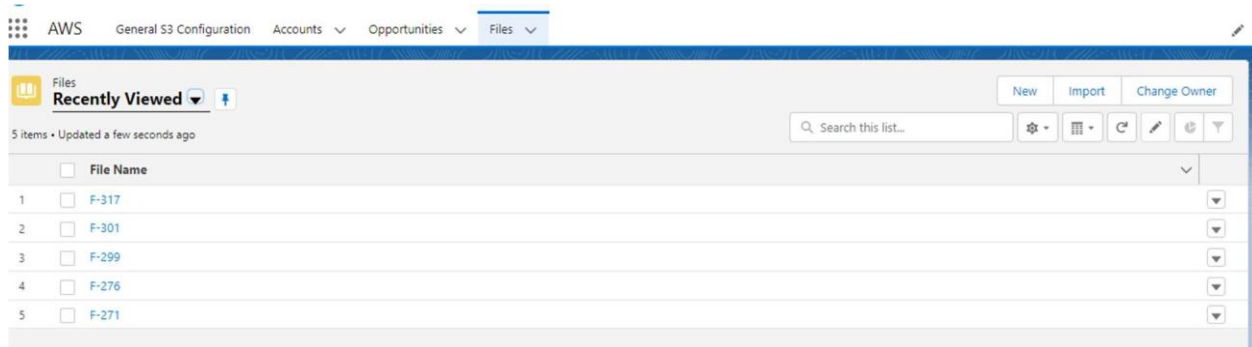
1. Go to Application Launcher, select Account.
2. Open any account record or create new account record.
3. User will see AW S3 Component.
4. user will see **Search** bar.
5. We will search the files by file name.



Process to See the S3 Files

Following are the steps to view all the S3 files:-

1. Go to Application Launcher, Select **Files**.
2. We will see list of Files which we uploaded on S3.



3. Open any file and we will see the details of file.