



S3 Connector

Effortless Salesforce-S3 Integration: Streamline Data Management with Ease!

User manual to install app for Salesforce CRM users to integrate Salesforce with AWS S3 to reduce storage costs.

INDEX

About S3 connector	3
How to download the app	4
One time App setup before first use	5
How to configure session settings	5
How to add AWS S3 File Uploader Component to record detail page	6
Create a permission set	8
Profile Settings for giving access to specific profiles:	11
How to Create S3 bucket and configure it	13
How to connect your AWS account with Salesforce	18
Share specific bucket's access to specific user or group of users	24
Upload, view and delete file using File upload component	26
About Advanz101	29

About S3 connector

Introducing the S3 Connector App, a comprehensive solution that seamlessly integrates Salesforce, a leading CRM platform, with AWS S3, a powerful cloud storage service. This app is specifically designed to meet the data management needs of businesses utilizing Salesforce as their CRM platform and AWS S3 for cloud storage.

With the innovative Sync Bucket functionality, users can effortlessly synchronize S3 buckets with Salesforce, enabling smooth and efficient file transfer. It allows for seamless file uploads from Salesforce to S3, ensuring data availability and accessibility across teams. By assigning specific buckets to different teams, such as sales or marketing, organizations can effectively organize and manage their files based on their business needs.

Administrators can exercise granular control over file extensions and maximum upload sizes, ensuring data security and compliance with organizational policies. Moreover, users can conveniently access files through clickable URLs, enabling quick and easy file retrieval. When files are no longer required, they can be promptly deleted from the Salesforce organization, and it gets deleted from S3 bucket as well.

Additionally, the S3 Connector App enhances productivity by streamlining data management workflows across multiple AWS S3 accounts. It provides an intuitive interface that eliminates manual processes, reducing the likelihood of errors and enhancing collaboration among teams. With this app, businesses can optimize their data management practices, resulting in improved efficiency and overall operational performance.

How to download the app

Installation of S3 connector App from Salesforce App Exchange-

1. Connect your salesforce account to your Trailblazer.me profile.
 - 1.1 In a new browser tab, open **AppExchange**.
 - 1.2. Click your avatar to open your Trailblazer.me account menu, and then click **Settings**.
 - 1.3. Under the Salesforce Accounts header in the Connected Accounts section, click **Connect**.
 - 1.4. If you see the Choose a Username page, click **Log in with a Different Username**. If you see a login page, skip to the next step.
 - 1.5. Enter your Salesforce username and password, then click **Log In**.
 - 1.6. Click **Link Account**.

2. Steps to Install Application to Salesforce Org-

- 2.1. In a new browser tab, open **AppExchange**.
- 2.2. Search for **S3 connector**.
- 2.3. Click on **Apply Filters** button and choose Solution type as **Apps** to narrow down search result.
- 2.4. Click on the **S3 connector** App Name.
- 2.5. Now click on the **Get it Now** button.
- 2.6. You will see 2 options **Install in Production** and **Install in Sandbox**.
- 2.7. In Install in Production, you will see all the connected salesforce accounts.
- 2.8. If you can't find the username for the account in which you want to install, then check **Connect Your Salesforce Account to Your Trailblazer.me Profile** i.e. section 1. .
- 2.9. Choose the username and click **Install in Production**.
- 2.10. You will see a page where you can confirm your details.
- 2.11. Select the checkbox **I have read and agree to the terms and conditions** only if you have read and agree to the terms and conditions.
- 2.12. Click on **Confirm and Install**, it will take you to the login screen.
- 2.13. If you want to Install in Sandbox, then click on **Install in Sandbox** button.
- 2.14. You will see a page where you can confirm your details.
- 2.15. Select the checkbox **I have read and agree to the terms and conditions** only if you have read and agreed to the terms and conditions.
- 2.16. Click on **Confirm and Install** it will take you to the login screen.
- 2.17. Provide your login credentials and select for which users you want to install the application.
- 2.18. After that application installation will start.

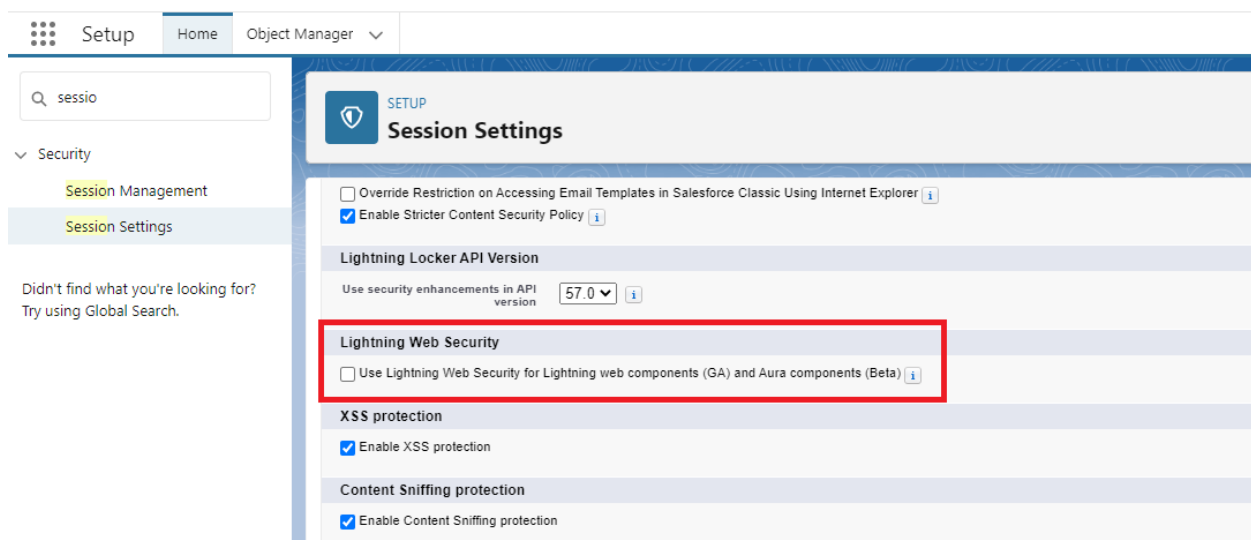
***We strongly recommend not to use any file that you receive from any unauthorized source, or any source not mentioned above.**

One time App setup before first use

Note: Please make sure you are not using Salesforce Classic UI as our App is made to work with Salesforce Lightning Experience.

How to configure session settings

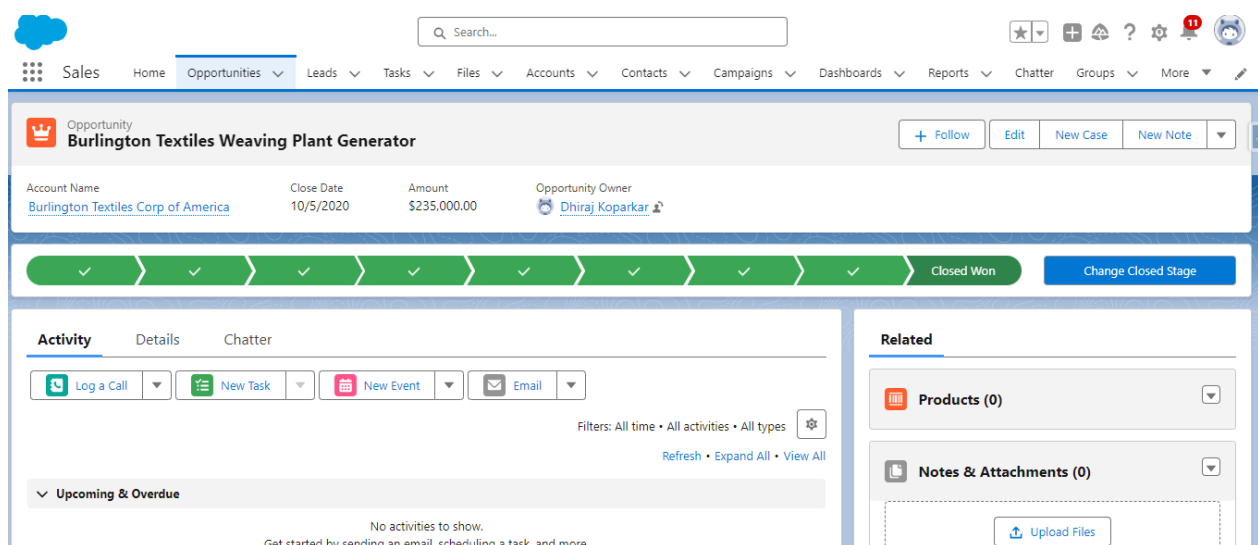
Go to setup and type session settings. In the sessions settings uncheck the checkbox under section Lightning Web Security and click **Save**.



How to add AWS S3 File Uploader Component to record detail page

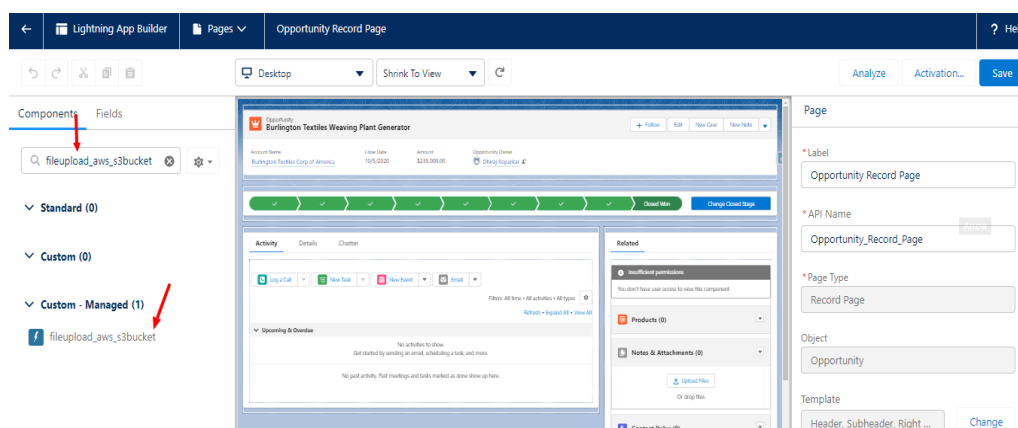
This component is used to upload, view and delete files from any object's record detail page. It is important for the user to add the component to that object's record detail page from where they want to use file upload, view and delete functionalities. Without this component, the app cannot be used. Follow the steps below to set it up.

1. Navigate to any object's record page.



2. Click  and select edit page.

3. Search for **fileupload_aws_s3bucket** component in the Search bar. **fileupload_aws_s3bucket component can be seen on Custom section.**



4. Drag and Drop the Component to the **first row** of Page Layout and Click **Save**.

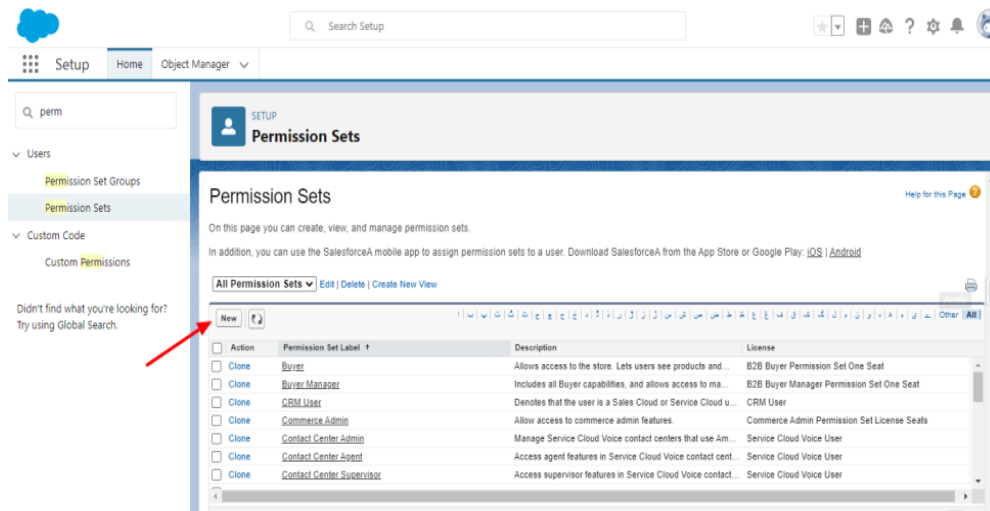
The screenshot shows the Lightning App Builder interface for the 'Opportunity Record Page'. On the left, the 'Components' panel is open, and the 'fileupload_aws_s3bucket' component is selected. In the center, the page layout is being edited, and the component is being dragged to the first row. On the right, the 'Set Component Visibility' panel is visible. The 'Save' button in the top right corner is highlighted with a red arrow.

5. The **Component** can now be seen on related tab

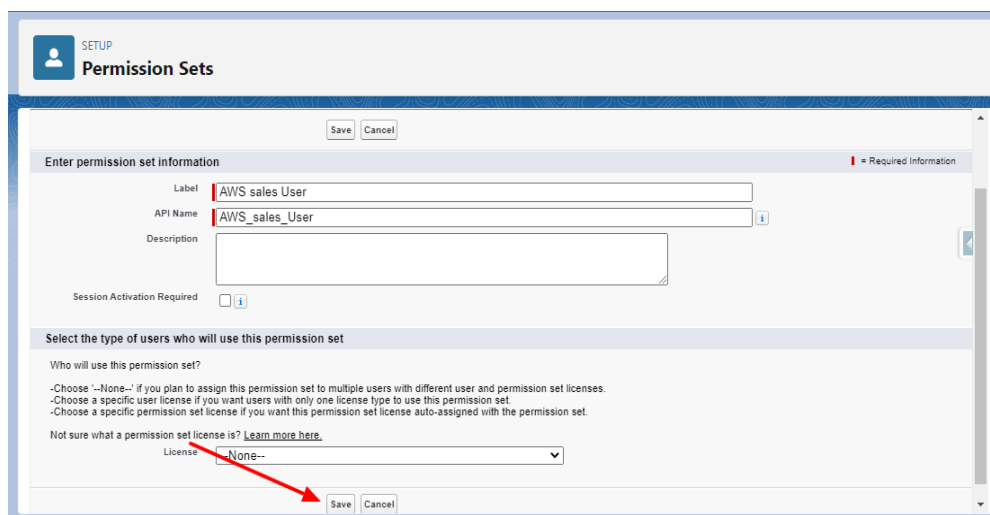
The screenshot shows the Salesforce interface for the 'Burlington Textiles Weaving Plant Generator' record. The 'Related' tab is selected, and the 'AWS S3 File Uploader' component is visible. A red arrow points to the component, indicating its presence on the related tab.

Create a permission set

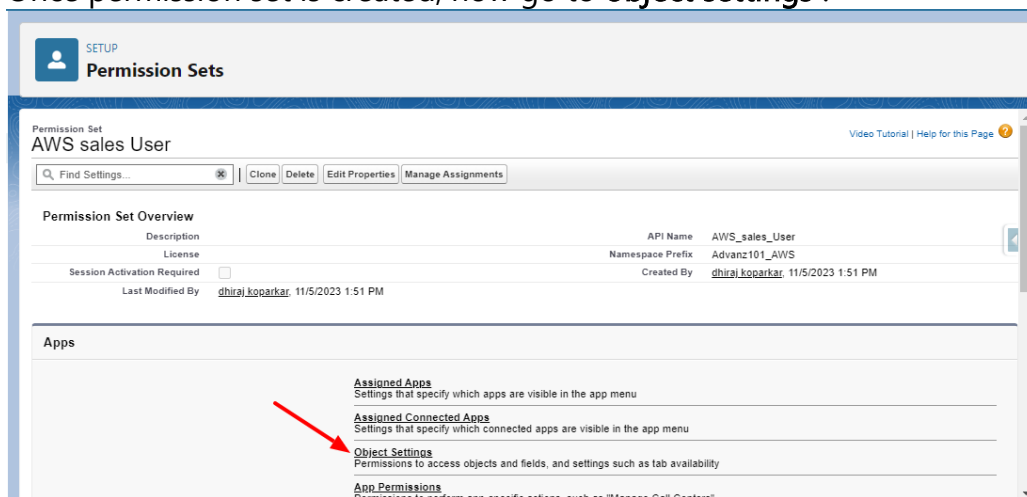
1. Go to setup and click **Permission Sets** and click on **New**



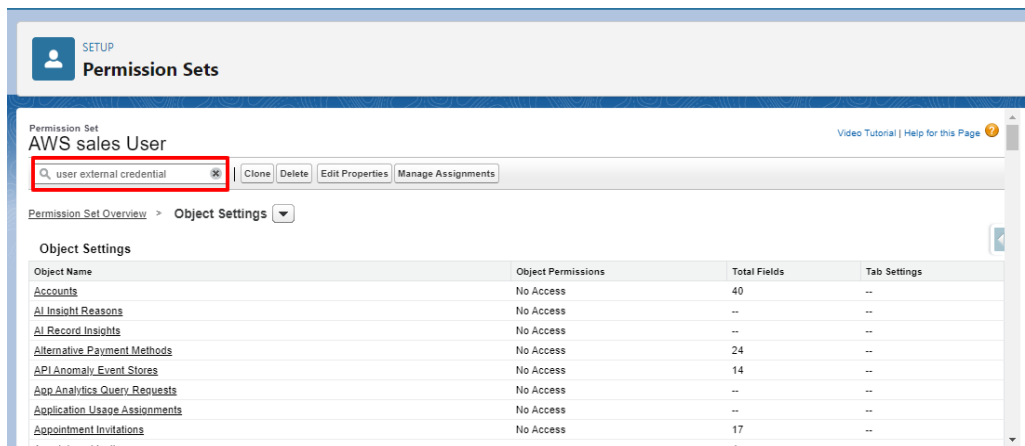
2. Add Label and click **Save**.



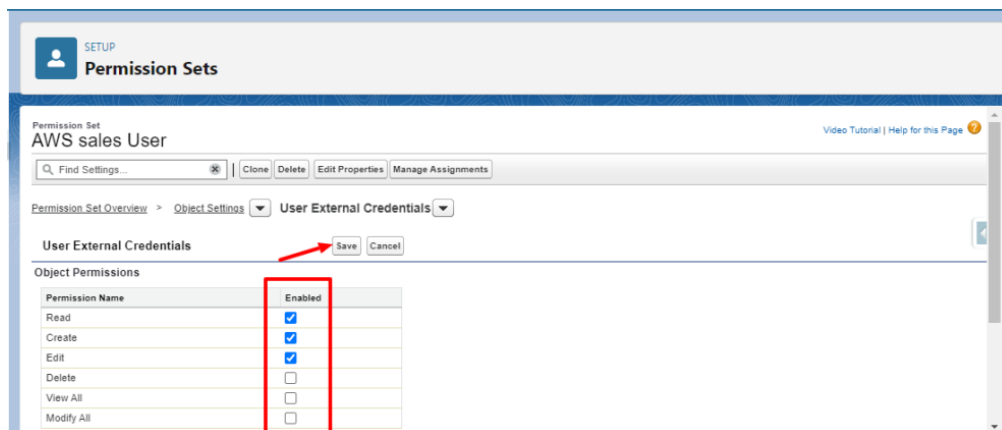
3. Once permission set is created, now go to object settings .



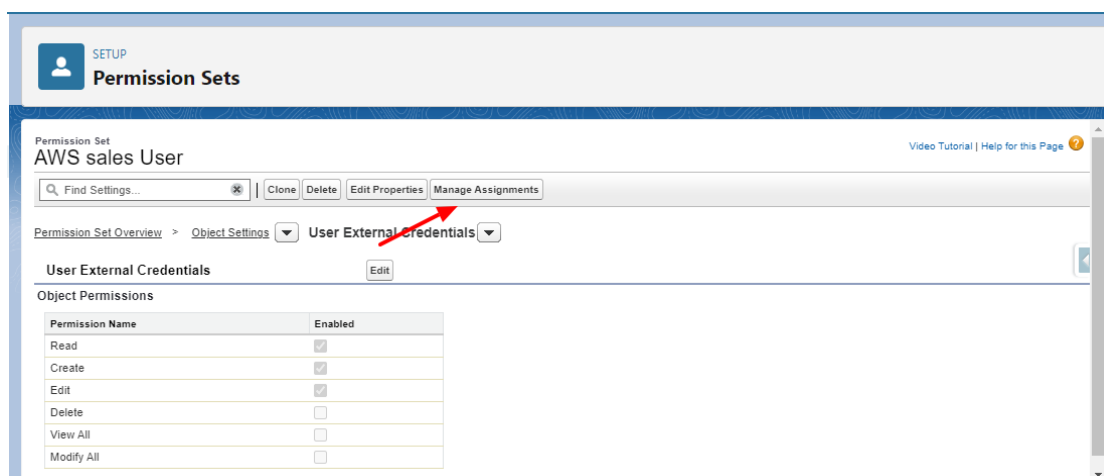
4. Go to User External object.



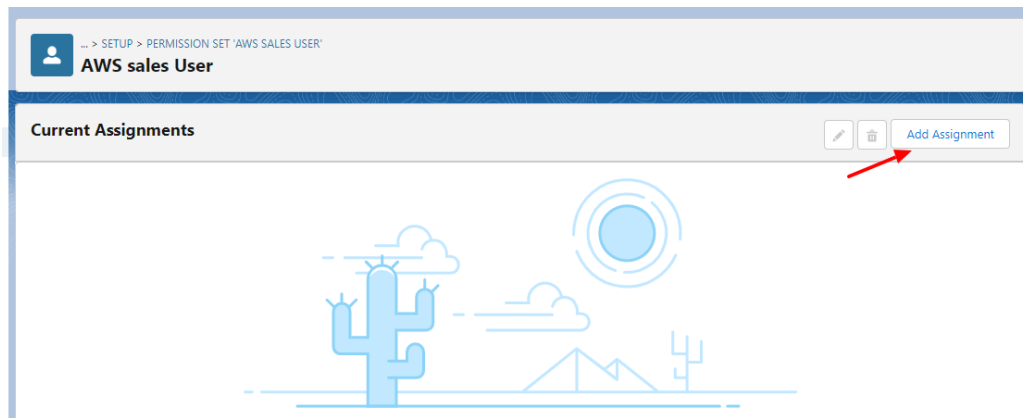
5. Tick the checkbox to give Read, Create and Edit permissions.



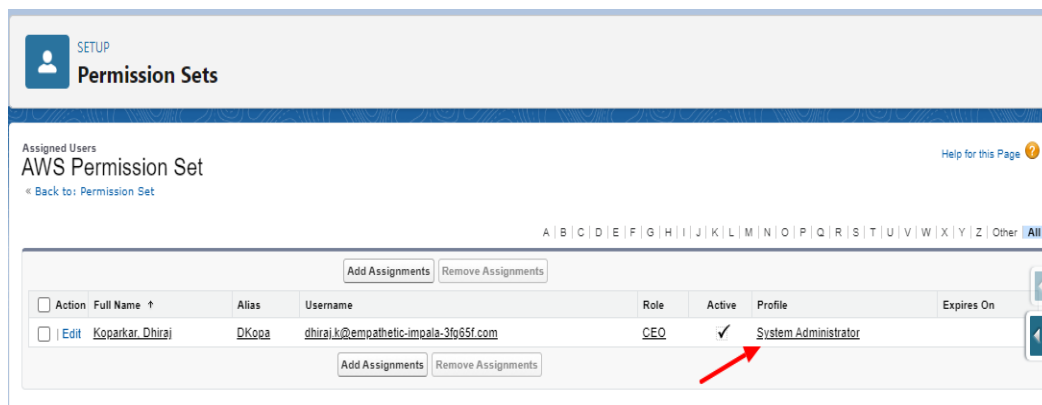
6. Click on manage assignments.



7. Click on **Add Assignment**.



8. Assign permission set to the **System Admin** user.

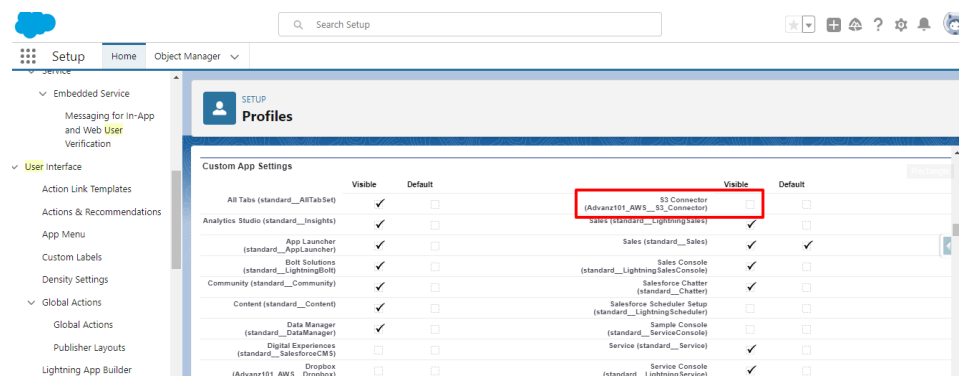


Profile Settings for giving access to specific profiles:

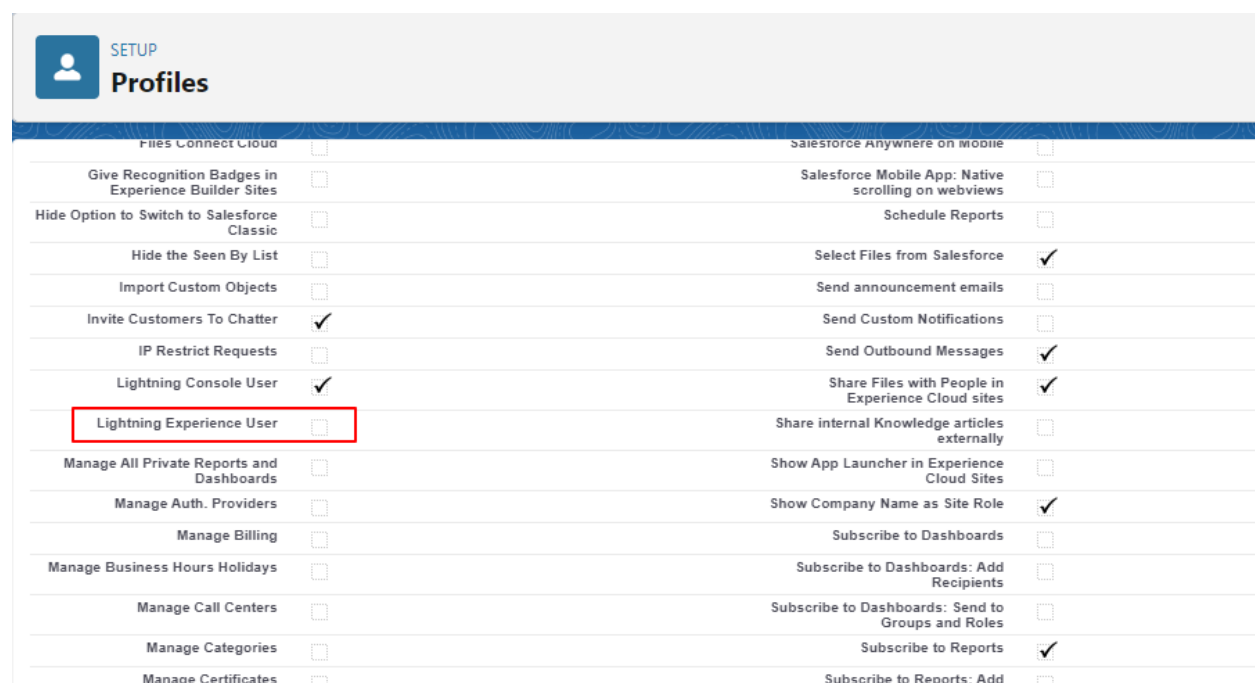
By default S3 Connector app's and objects access are given to all the profiles but it is advisable to keep access for only specific profiles.

Revoke access of S3 Connector app for all the profiles as it is advisable that only System admin have access to the app.

1: Uncheck the S3 Connector app checkbox from custom app settings



2: Give 'Lightning Experience user' access as this component works in Lightning Experience mode.



3: Revoke 'Read, Create, Edit and Delete' access to AWS Key, AWS Buckets and AWS

File object and keep 'Read, Create, Edit and Delete' access to AWS File object only on those profiles through which you want to use file upload functionality.



SETUP
Profiles

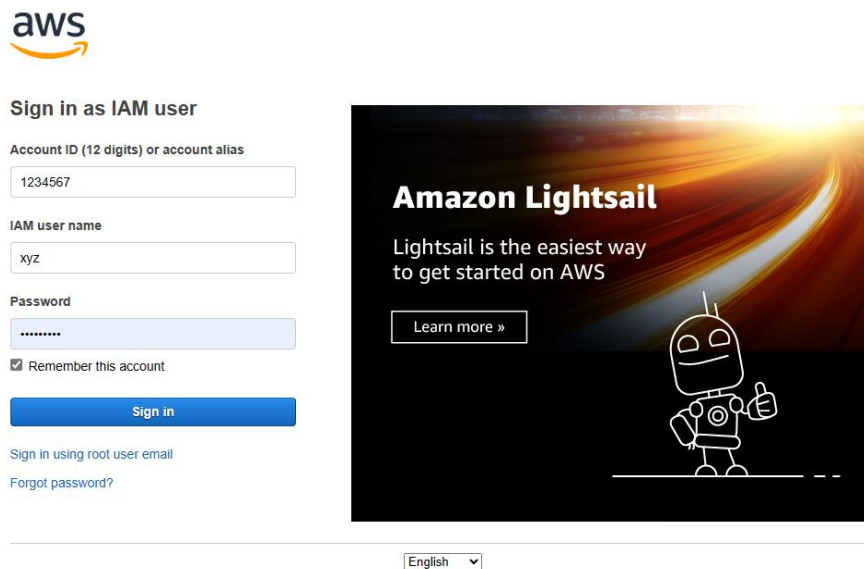
Individuals	☐	☐	☐	☐	☐	☐
Invoices	☐	☐	☐	☐	☐	☐
Leads	☒	☒	☒	☒	☐	☐

Custom Object Permissions

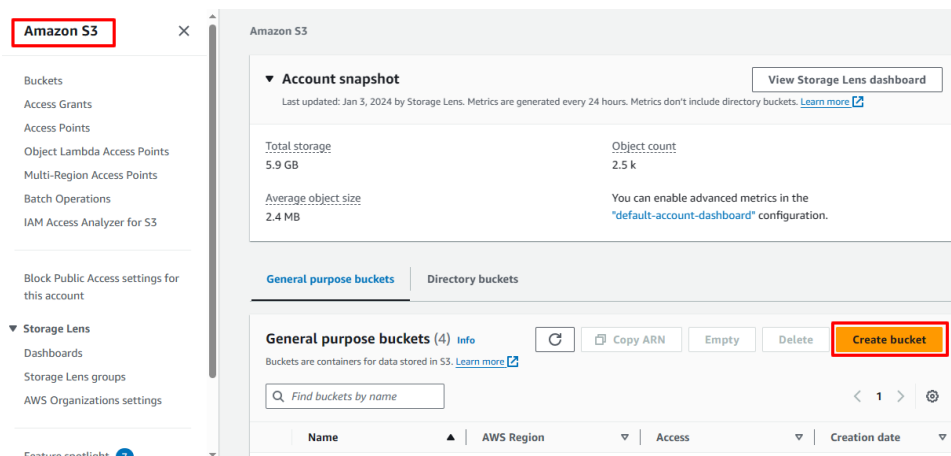
	Basic Access				Data Administration	
	Read	Create	Edit	Delete	View All	Modify All
AWS Files	☒	☒	☒	☒	☐	☐
AWS INFOS	☐	☐	☐	☐	☐	☐
AWS Keys	☐	☐	☐	☐	☐	☐

How to Create S3 bucket and configure it

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



2. In the left navigation pane, choose Buckets.
3. Choose Create bucket.



4. The Create bucket page opens.
5. For bucket name, enter a name for your bucket.
6. For Region, choose the AWS Region where you want the bucket to reside.

Amazon S3 > Buckets > Create bucket

Create bucket [Info](#)

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

AWS Region

Bucket name [Info](#)

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - *optional*
 Only the bucket settings in the following configuration are copied.

Format: s3://bucket/prefix

7. Under Object Ownership, choose ACLs enabled.

Object Ownership [Info](#)

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☐ ACLs disabled (recommended)
 All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

☒ ACLs enabled
 Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

⚠ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.

8. Uncheck Block all public access and check that warning (I acknowledge that the current settings might result in this bucket and the objects within becoming public.)

☐ **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.

⚠ Turning off block all public access might result in this bucket and the objects within becoming public
 AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

☒ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

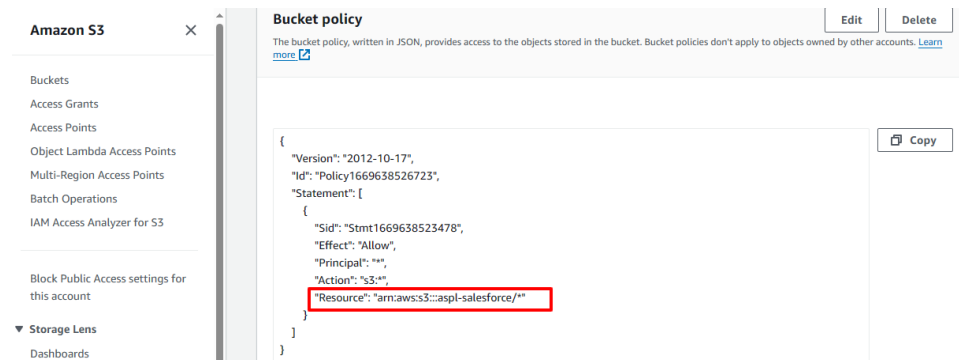
9. Save

After saving navigate to permission section, then add bucket policy and CORS setting

Bucket Policy

Go to bucket policy section, click edit and copy the following code and paste and click Save.

```
{
  "Version": "2012-10-17",
  "Id": "Policy1669638526723",
  "Statement": [
    {
      "Sid": "Stmt1669638523478",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::your Bucket Name/*"
    }
  ]
}
```



Cross-origin resource sharing settings

Go to CORS settings, edit and copy the following code and paste in your CORS section and Save it.

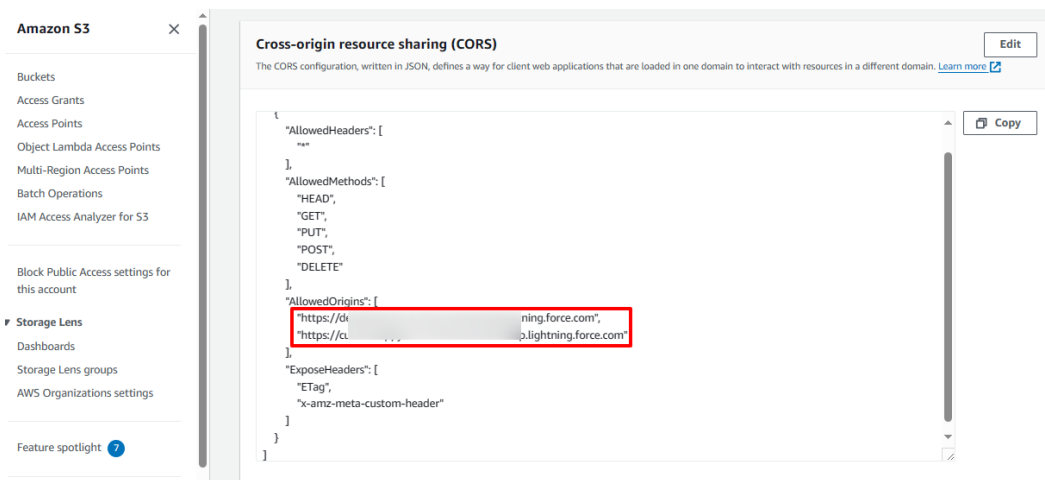
Note: Add your organization URL in AllowedOrigins

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
```

```

    "HEAD",
    "GET",
    "PUT",
    "POST",
    "DELETE"
  ],
  "AllowedOrigins": [
    //Add here your org url
    Ex - "https://sample-dev-ed.lightning.force.com/"
  ],
  "ExposeHeaders": [
    "ETag",
    "x-amz-meta-custom-header"
  ]
}
]

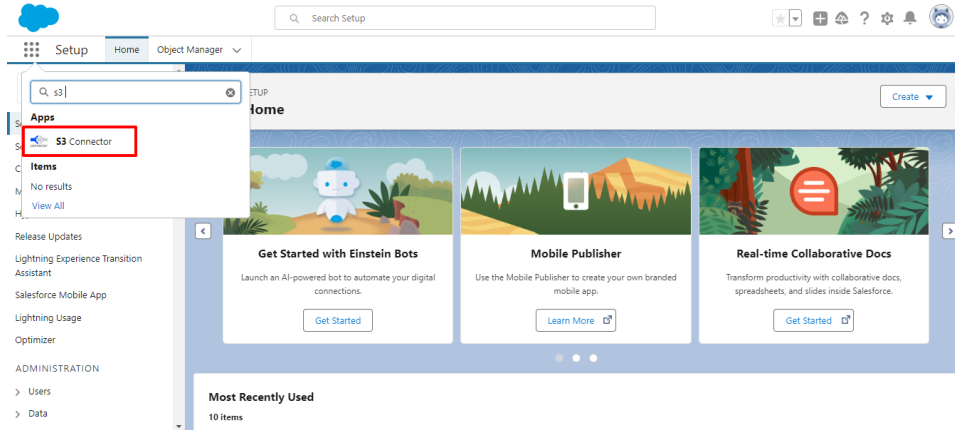
```



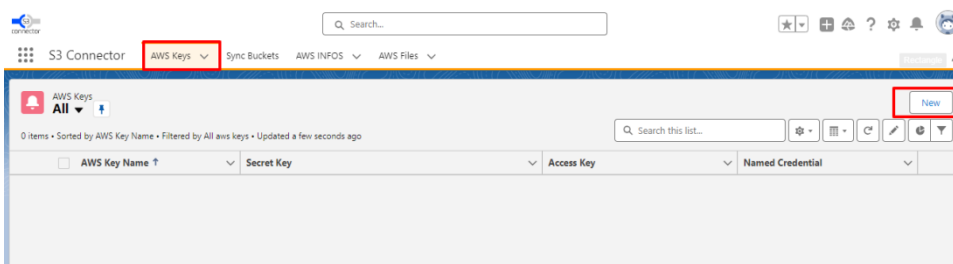
How to connect your AWS account with Salesforce

Step 1: Authenticate using secret key and access key.

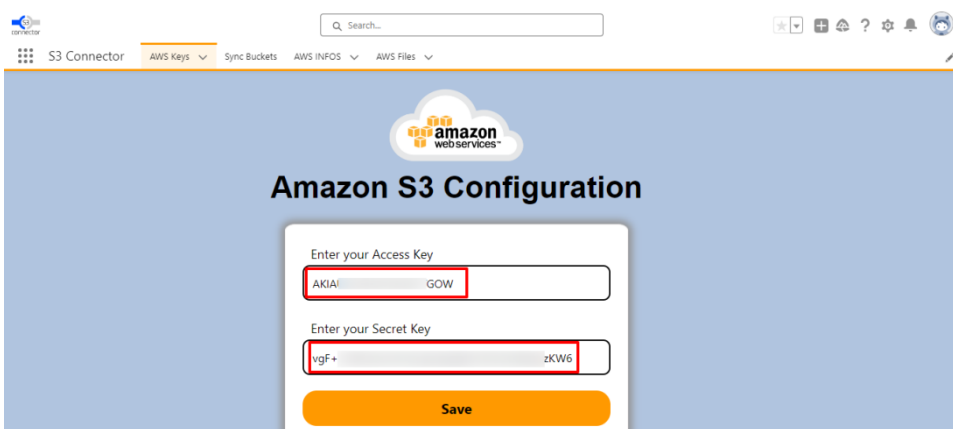
1. Open **S3 Connector** app from App Launcher.



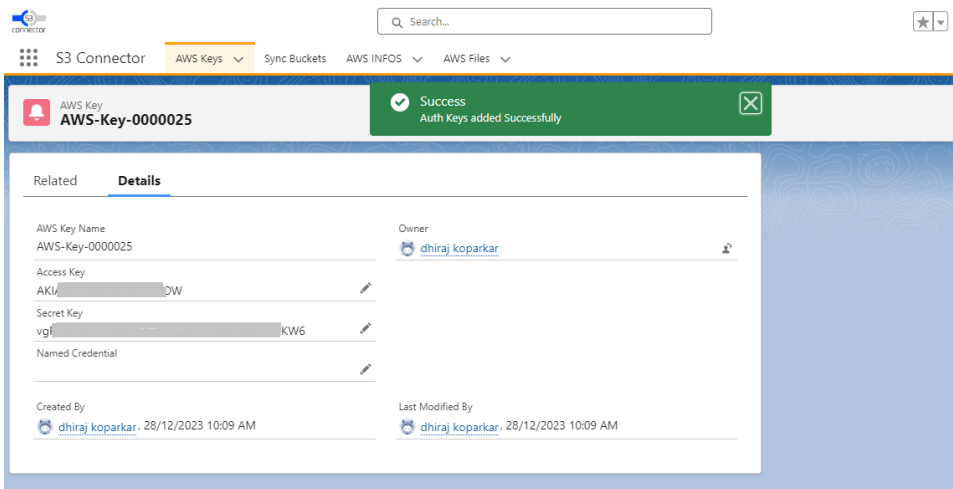
2. Go to **AWS Key** tab and then click **New** button.



3. Enter your Access Key and Secret key and click Save.



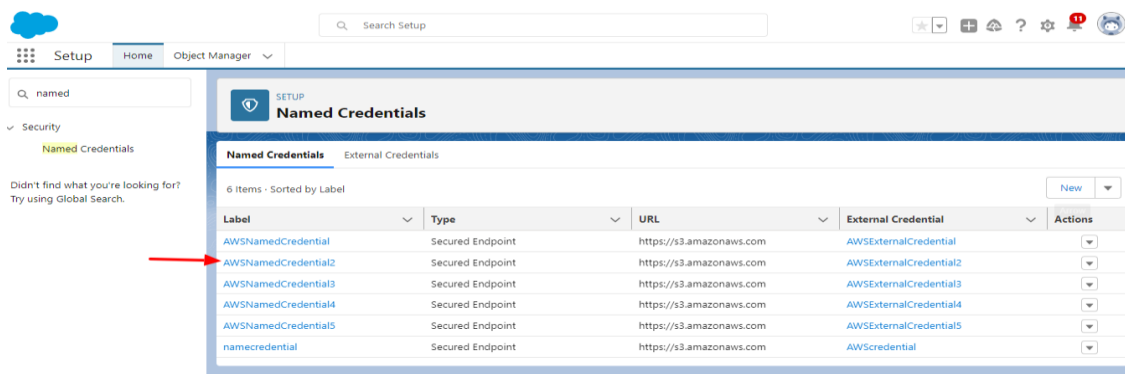
4. After successful authentication you will be redirected to record detail page.



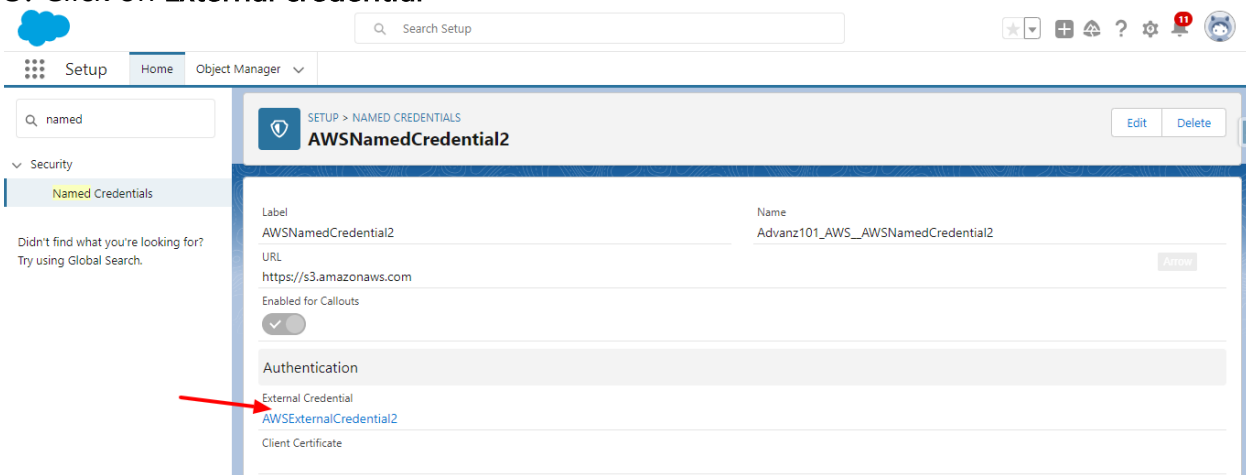
Step 2: Edit External Credential and add Principle

Note: We have provided five Named credentials in this package so you can add up to five AWS accounts.

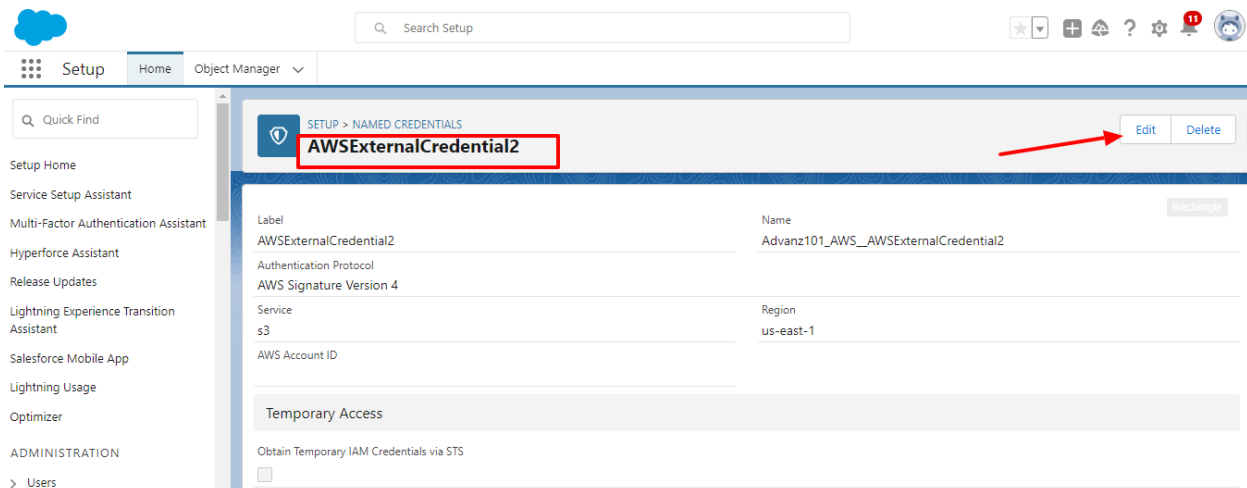
1. From Setup, enter **Named Credentials** in the Quick Find box, then select **Named Credentials**.
2. Click any one **Named Credentials**.



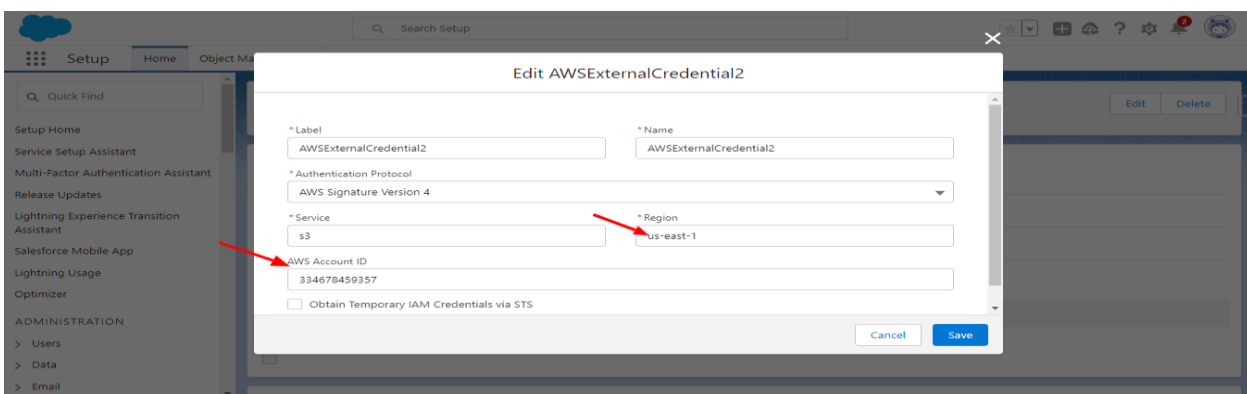
3. Click on External credential



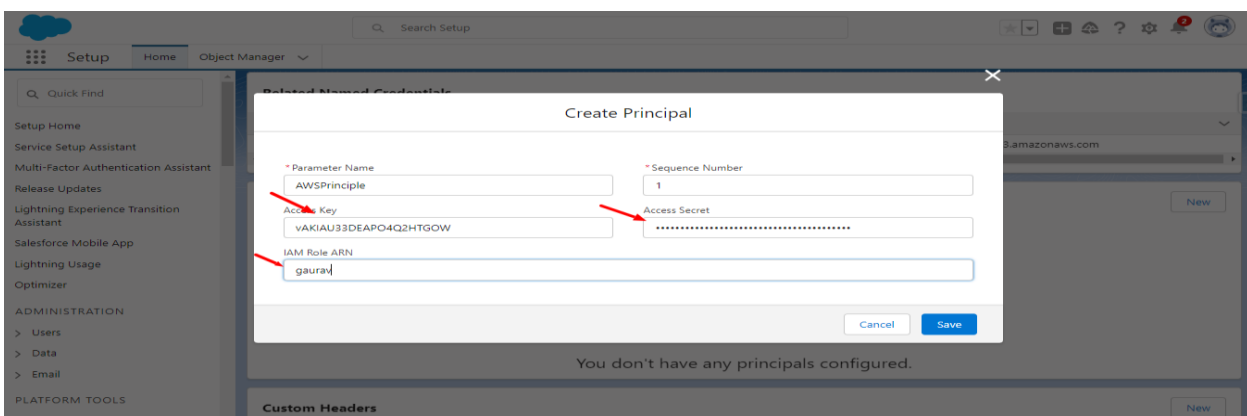
4. Click on Edit



5. Add your Region, AWS Account Id and click Save.

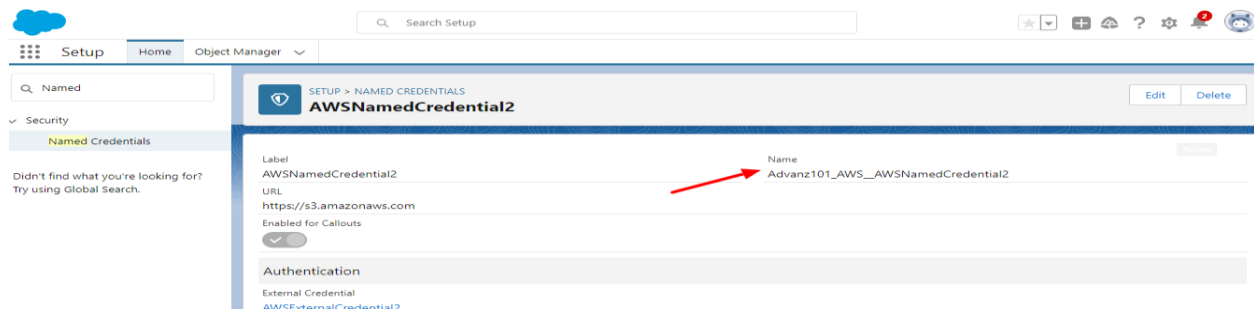


6. Click New on principal, add access key and secret key (through which you have authenticated in first step) and IAM Role IRN and click Save.

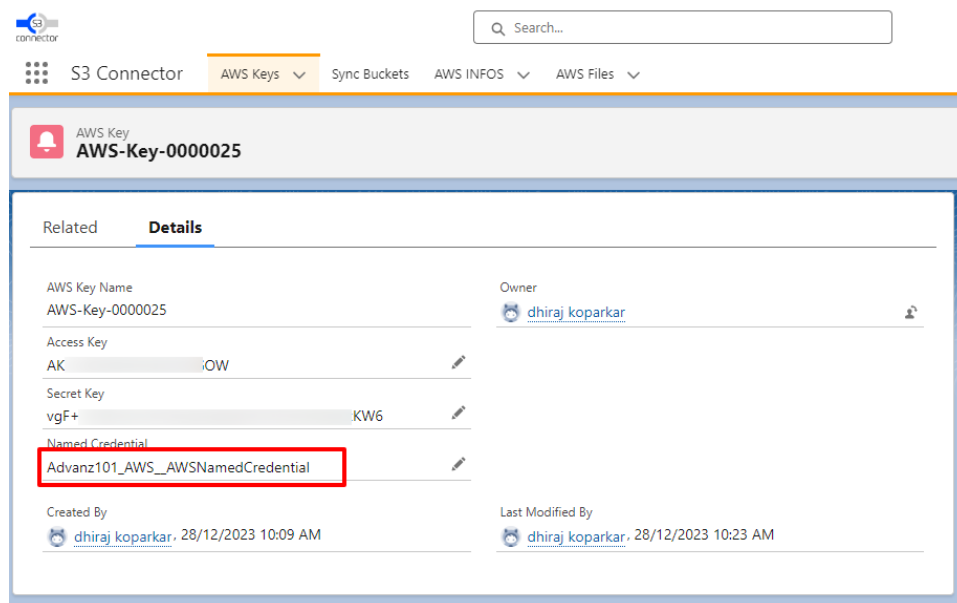


Step3: Add **Named credential** name in AWS Key record

1. Copy the name of the named credential in which you have configured external credential in previous step.

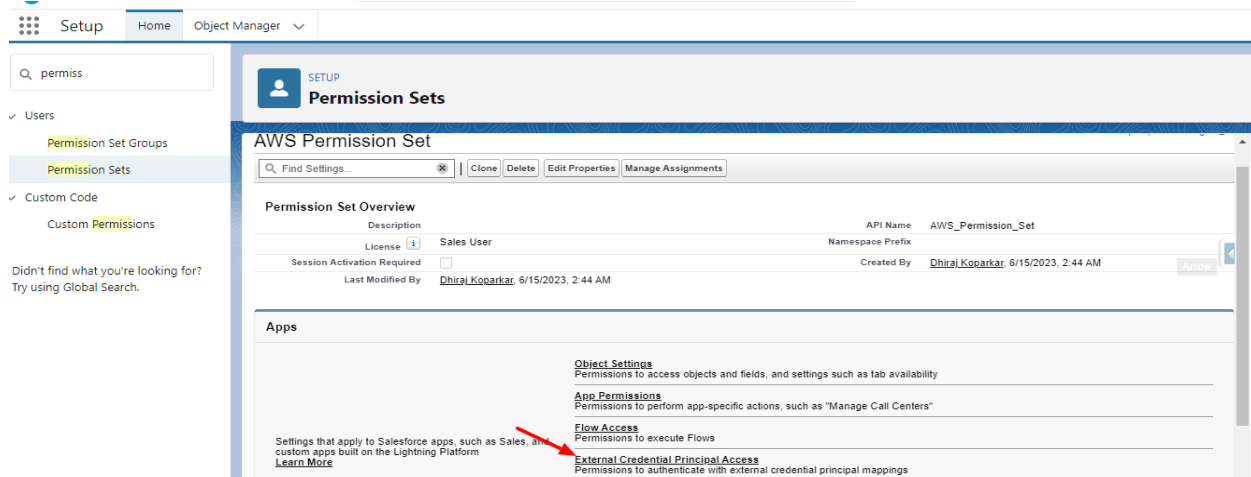


2. Go to AWS Key record created in first step, edit it and paste the name of the Named credential and click Save.

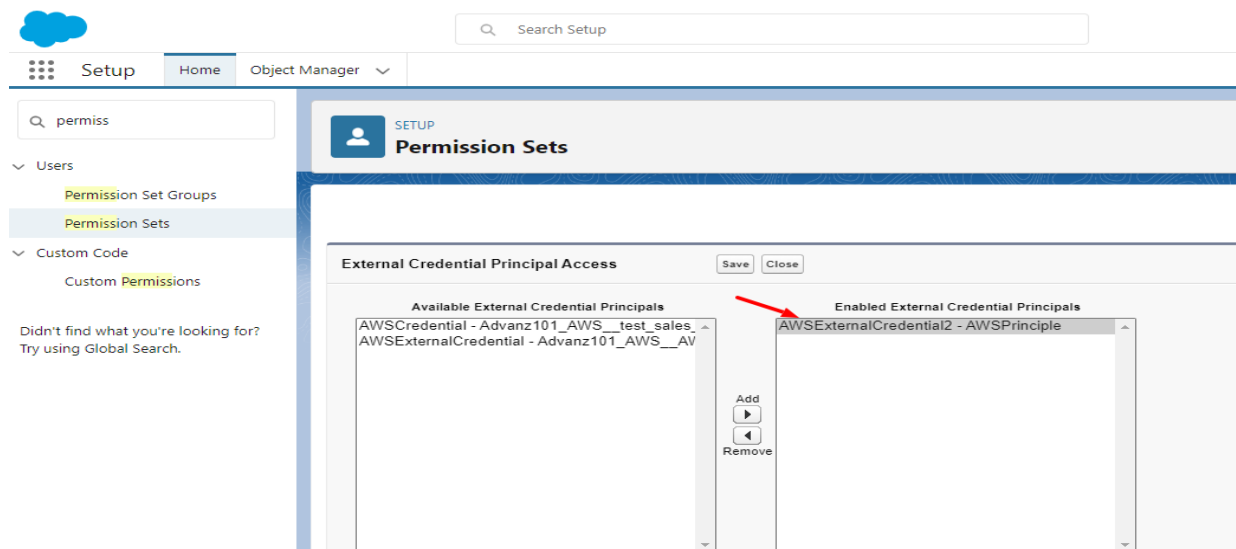


Step 4: Add **External credential Principal** in External Credential Principal Access in Permission Set

1. Go to the permission set you created during one time setup and click on External Credential Principal Access

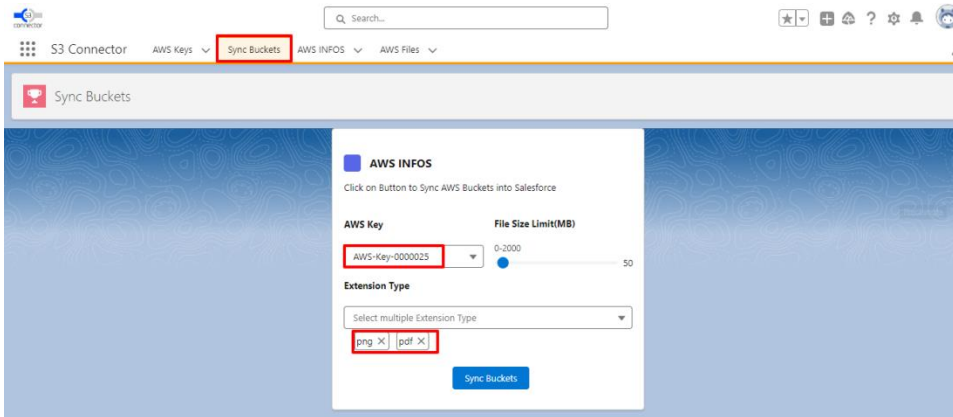


2. Click Edit and add External credential which you configured in step 2 and click Save.



Step 5: Fetch and add buckets in Salesforce using Sync Bucket functionality

1. Go to S3 Connector Application in Salesforce
2. Click on Sync Buckets tab
3. Select AWS Key.
4. Choose the maximum file size limit.
5. Select file extensions you want to allow and click on Sync Buckets.



Sync Buckets

AWS INFOS
Click on Button to Sync AWS Buckets into Salesforce

AWS Key **File Size Limit(MB)**

AWS-Key-0000025 0-2000 50

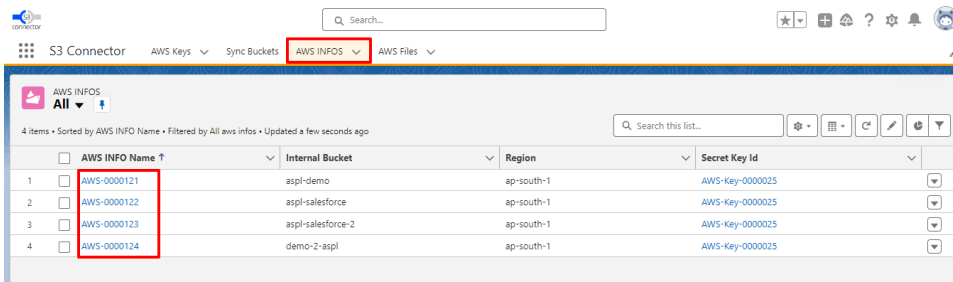
Extension Type

Select multiple Extension Type:

png X pdf X

Sync Buckets

6. After getting the success message click on AWS Info to check whether the buckets present in AWS are added to salesforce or not.



AWS INFOS
All

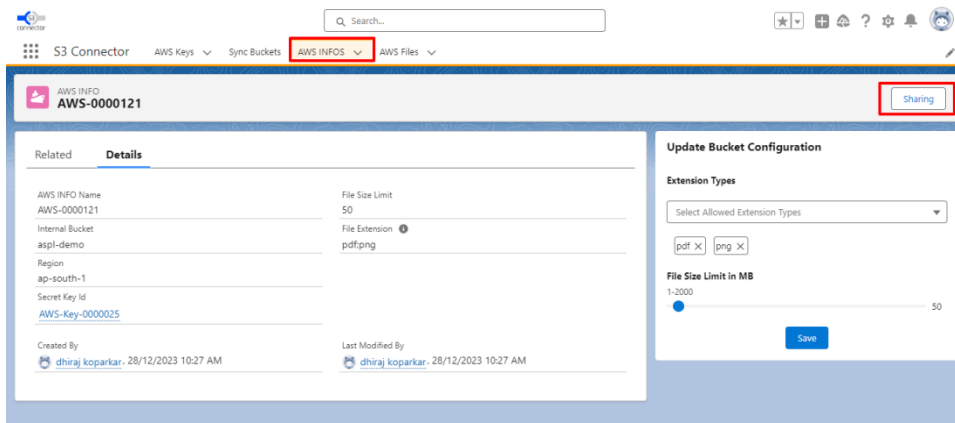
4 items • Sorted by AWS INFO Name • Filtered by All aws infos • Updated a few seconds ago

	AWS INFO Name ↑	Internal Bucket	Region	Secret Key Id
1	AWS-0000121	aspl-demo	ap-south-1	AWS-Key-0000025
2	AWS-0000122	aspl-salesforce	ap-south-1	AWS-Key-0000025
3	AWS-0000123	aspl-salesforce-2	ap-south-1	AWS-Key-0000025
4	AWS-0000124	demo-2-aspl	ap-south-1	AWS-Key-0000025

Share specific bucket's access to specific user or group of users

To use file upload functionality for any user other than System Admin you will need to give 'Read' access of bucket record to a specific role, user or group of users manually.

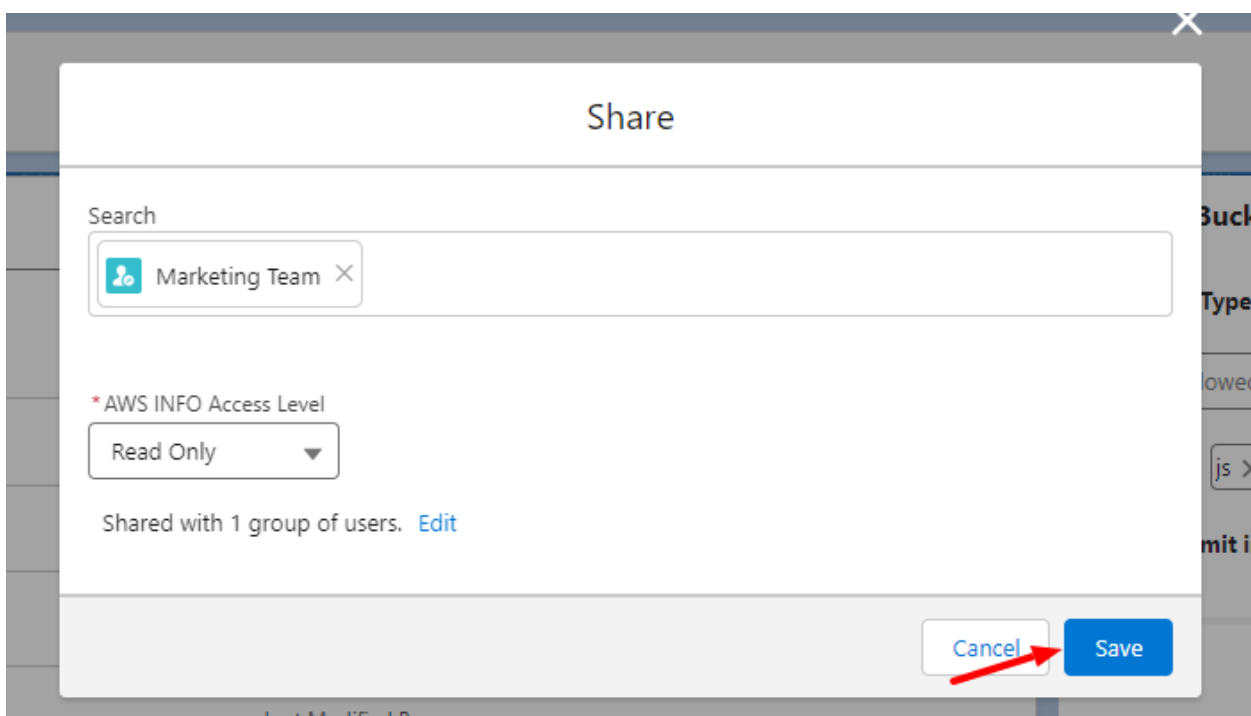
1: Go to the AWS Info tab and select the desired bucket record for sharing and click on the Sharing button.



2: Select the user, role or group of users with whom you want to share access and click on Save.

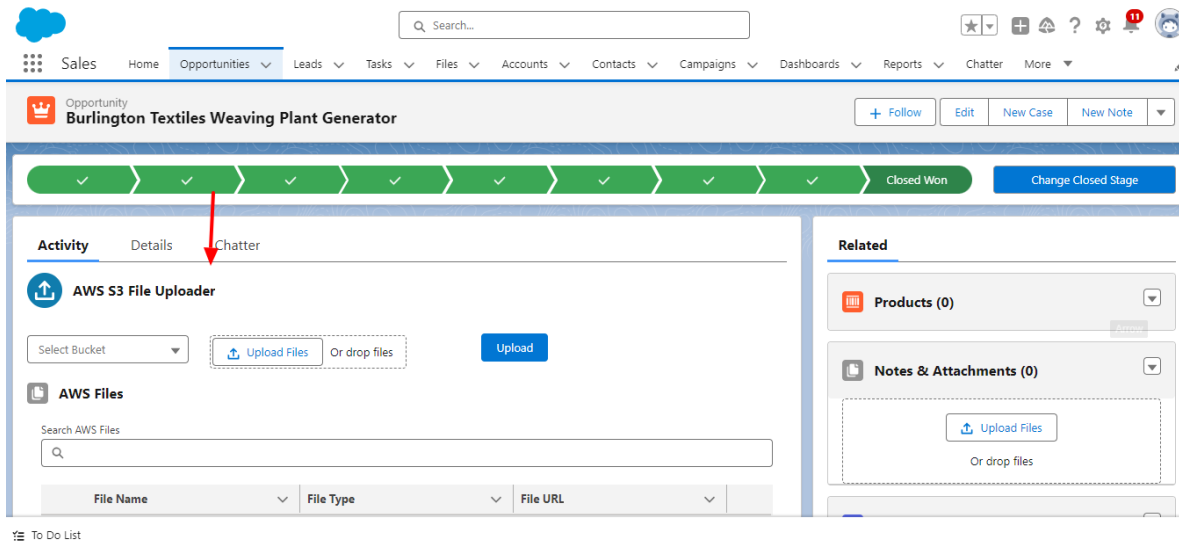
Note: Only give Read access while sharing as it is sufficient and secure.

In the sample image we have selected the Marketing Team role so now all the users having role as Marketing Team will get access to upload file on this specific bucket.



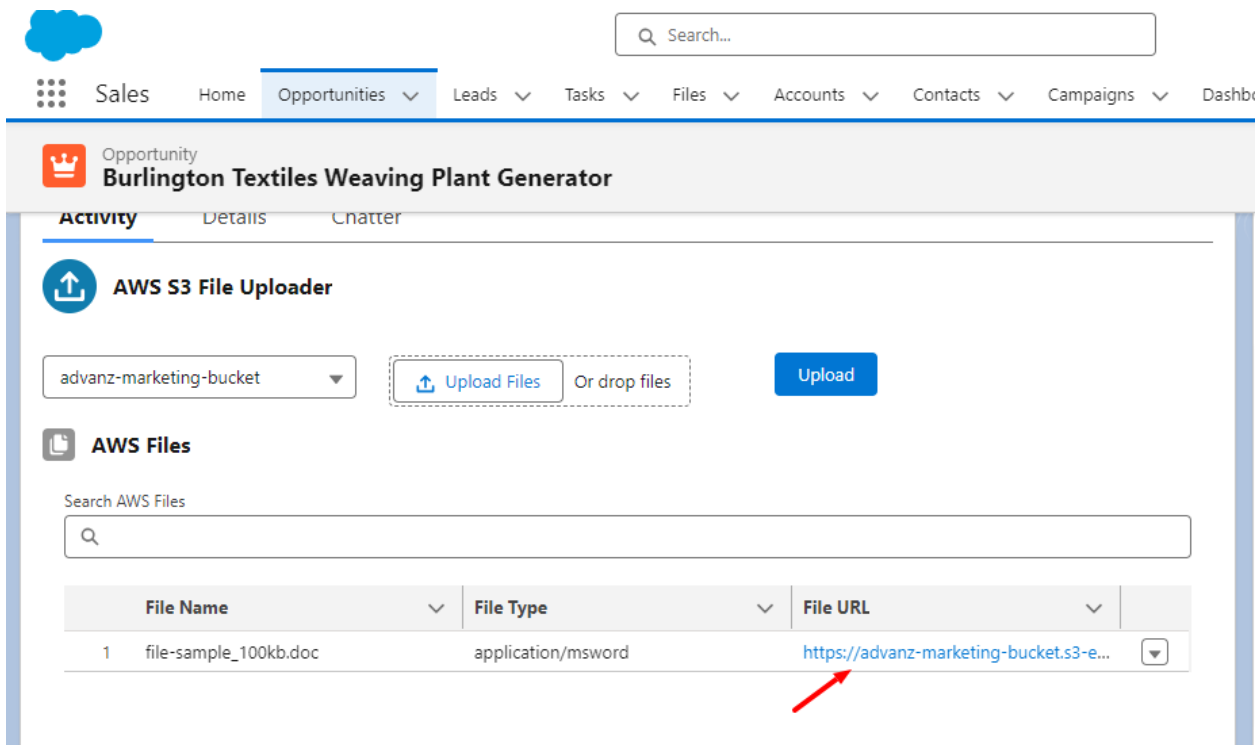
Upload, view and delete file using File upload component

1. Open the record detail page of the object on which you added the file upload component



2. Select the bucket name on which you want to add files and then select a file by clicking on the Upload file icon and click on Upload.

Note: File name should not contain '+' character.



3. The file will be uploaded to S3 bucket as well as a record of that file will be created in Salesforce containing the URL to access that file.

 **AWS S3 File Uploader**

aspl-salesforce

 Upload Files

Or drop files

Upload

 **AWS Files**

Search AWS Files

	File Name	File Type	File URL	
1	apex_assignment.pdf	application/pdf	https://aspl-salesforce.s3-ap-south-1....	

Other Apps by Advanz101

- **MergeEase**
Merge multiple service contracts.
- **PartEase**
User can select Contract Line Items available in Service Contract and Renew only selected Contract Line Items
- **MoveEase**
Transfer asset from one account to another
- **AutoSplit**
Split Service Contract into multiple contracts
- **CaseAutoMail**
Transform Case Communication with CaseAutomail
- **EaseQuotePdf**
Automate Quote PDF Generation on Status
- **Split Ease**
Split Service Contract into multiple contracts manually to avoid large carter errors.

Hope you find our S3 Connector App useful. We would love to hear about our app from you. In case of any query or further clarification please feel free to reach us at info@advanz101.com

Please keep following us as many new apps are under development. Follow us at www.advanz101.com

About Advanz101

ADVANZ101 Business Systems Inc. is a registered Salesforce partner providing best-in class solutions for global business houses and brands. Our team is equipped to meet the SaaS demands of modern enterprises with due diligence in today's business landscape of hybrid IT.

For additional information, please feel free to connect with us at info@advanz101.com