

# AWS S3 Document Management for Insurance and Financial Services on Salesforce

Store Salesforce files and attachments in your own AWS S3 bucket and show them on every policy, claim and account

---

## What problem does this solve for insurance and financial services teams?

CloudFiles is Document Automation for Salesforce. This guide describes a pattern we see in insurance and financial services: Salesforce is where policies, claims, accounts and service requests live, and every one of those records collects documents. Applications, policy schedules, claim photos, statements, identity documents and email attachments pile up as Salesforce Files.

The problems are plain:

- Salesforce file storage fills, and the team is asked to keep buying extra Salesforce storage.
- Documents produced by back-end systems, such as policy administration or statement generation, land in AWS S3 and never reach the Salesforce record.
- Staff work in two windows, one for Salesforce and one for the document store.
- Policyholders and members on a portal need to see their own documents, and only theirs.

CloudFiles Document Management gives these teams AWS S3 document management inside Salesforce. It lets you move Salesforce attachments to S3, store Salesforce files in AWS S3 in your own bucket, and show S3 files on Salesforce records for portal members. The same app connects Salesforce to SharePoint, AWS S3, Google Drive and Azure Blob, so a firm that keeps claims in AWS S3 and underwriting files in SharePoint or Google Drive uses one widget for both.

## Which Salesforce objects are involved?

- **Account** and **Contact** for the insured, member or client.
- **Opportunity** for new business and renewals.
- **Case** for service requests and claims intake.
- Custom objects such as **Policy** and **Claim**.
- **EmailMessage**, whose attachments are often the largest share of Salesforce storage.

CloudFiles works on any standard or custom object. Each record can have its own folder in the S3 bucket, and folder links survive record renames.

## Where are the files stored?

In your own AWS S3 bucket. To connect it, the customer enters the bucket name and deploys a CloudFormation template that creates an IAM role with an External ID. CloudFiles uses that role to work in the bucket.

Event-driven sync is turned on per connection, and CloudFiles sets the bucket notification. A file that arrives in the bucket by any route is indexed and appears on the record. For example, a company can have its statement or policy output system write straight into a Policy's folder in S3, and the file shows up in the CloudFiles widget on that Policy record without anyone uploading it through Salesforce.

## How do we move Salesforce attachments to S3, step by step?

1. **Create folders across objects.** Record-triggered Flows on Account, Policy and Claim create run **Create Folder**, so each record gets its folder in the bucket. **Get Connected Folder** returns the folder for later steps.
2. **Copy files out of Salesforce.** A record-triggered or scheduled Flow runs **Copy Salesforce Files** to copy Salesforce Files and email attachments into the record's S3 folder and leave a link on the record. A scheduled Flow avoids the need for file-attached events; that event setting ships off, and keeping it off reduces API calls.
3. **Remove the Salesforce copy only after completion.** Copying is asynchronous. Completion arrives later as a CloudFiles event, and a platform-event Flow handles it. Remove the Salesforce file in that completion handler and nowhere else, so nothing is deleted before the copy in S3 exists.
4. **Tag the objects.** **Set Resource Property** writes Policy Number, Line of Business or Claim Status onto the file, and **Search by Resource Metadata** finds documents by those values later.
5. **Migrate the backlog.** Legacy files and attachments can be migrated in bulk, so existing records move to S3 as well as new ones.
6. **Share with portal members.** **Share with Community User** shows a member's own Policy or Claim folder in the Experience Cloud portal. Members see their own documents and can upload into AWS S3 without an AWS account.

| Trigger                     | Flow action                            | Result                          |
|-----------------------------|----------------------------------------|---------------------------------|
| Policy or Claim created     | Create Folder                          | Folder in the S3 bucket         |
| Scheduled run or file added | Copy Salesforce Files                  | File in S3, link on the record  |
| Copy completion event       | Delete Records (standard Flow element) | Salesforce storage freed        |
| Member portal enabled       | Share with Community User              | Member sees their own documents |

## How does this reduce Salesforce file storage costs?

Every file copied to S3 and removed from Salesforce is storage you no longer pay Salesforce for. Offloading Salesforce file storage to a bucket you already run means you can stop buying extra Salesforce storage, while users still preview PDF, Office files, images, video and audio from the record, search across the folder tree, and download a file as PDF.

## Who can see the documents?

Inside Salesforce, the CloudFiles widget shows a record's S3 folder to users who can see that record, so Salesforce record access decides who sees which policy or claim documents. Flow automation runs as the integration identity; the widget and Content Library run as each user through their own storage connection. On the AWS side, CloudFiles works only through the IAM role the template created. On the Salesforce side, a least-privilege permission set keeps the integration user to what CloudFiles needs.

For brokers, auditors or outside counsel, **Create Link** issues a share link with an email wall, password, email verification code and consent step. Links can expire and carry a view limit, and every view and download is tracked.

## What are the security and compliance facts?

- ISO/IEC 27001:2022 certified, with ISO/IEC 27017:2015 and ISO/IEC 27018:2019.
- Independently audited for SOC 2 Type II.
- Compliant with HIPAA (BAA available). Compliant with GDPR.
- Hosted on AWS in four regions selected per customer account: United States, EU, United Kingdom and Australia.
- TLS 1.2 minimum in transit; AES-256 at rest on production data stores.
- Your files stay in your own storage. CloudFiles transfers them over encrypted connections and does not re-host them.

Security documents (ISO certificates, SOC 2 Type II report, penetration test summary) are available under NDA from the CloudFiles Trust Center.

## Get started

Install CloudFiles Document Management from AgentExchange and start a free 14-day trial, or book a demo at [cloudfiles.io](https://cloudfiles.io).