

Secure External File Sharing from Salesforce and SharePoint

Share Salesforce documents externally, collect portal uploads, and keep every file in SharePoint, AWS S3, Google Drive or Azure Blob

Why does secure external file sharing belong inside Salesforce?

CloudFiles is Document Automation for Salesforce. CloudFiles Document Management connects Salesforce to SharePoint, AWS S3, Google Drive and Azure Blob, and it automates folders, file uploads, permissions and secure sharing from the Salesforce record.

Customers, partners, brokers, applicants and auditors all need documents from you, and they need to send documents back. The usual answers are email attachments, a SharePoint guest invitation, or asking the external party to create an account in yet another system. Each one leaks control: attachments get forwarded, guest access outlives the deal, and nobody on the Salesforce record can see what was shared or opened.

Secure external file sharing works best when it starts where the relationship lives, on the Salesforce record, and when the file itself stays in the storage your IT team already governs. That is the model CloudFiles follows. Your files stay in your own storage. CloudFiles transfers them over encrypted connections and does not re-host them.

How do I share Salesforce documents externally without giving away storage access?

From the CloudFiles file browser widget on any Lightning record page, a user picks a file or folder and creates a share link. The recipient never needs a SharePoint, Google Drive, AWS S3 or Azure Blob account, and your storage permissions stay exactly as they were.

Every share link can carry the controls your security team asks for:

- **Email wall:** the recipient enters an email address before the file opens.
- **Password:** a password set by the sender.
- **Email verification code:** a one-time code sent to the recipient's inbox proves they own that address.
- **Consent step:** the recipient accepts your terms before viewing.
- **Expiry:** the link stops working on the date you choose.
- **View limit:** the link closes after a set number of views.

- **Tracking:** every view is recorded with location, and every download is recorded per file.

Brand and legal teams can set up a white-label custom domain for share links, so recipients see your company's name in the address instead of a vendor's. That matters for recipients who have been trained to distrust unfamiliar links.

When you share Salesforce documents externally this way, the activity sits next to the record. A sales rep can see that the proposal was opened, an account manager can see which files a client downloaded, and a compliance lead can see who accessed a file and from where.

How do I integrate SharePoint for secure external file sharing?

To integrate SharePoint for secure external file sharing, an admin connects CloudFiles to the Microsoft tenant in one of two ways:

- **Service principal (app-only):** CloudFiles authenticates as the CloudFiles app in your own Microsoft tenant. It uses no license and has no password or MFA to break, and the connection shows an "Active for automations" badge.
- **Integration user:** a dedicated Microsoft account that CloudFiles signs in as.

Your Microsoft 365 admin can limit CloudFiles to only the SharePoint sites you choose, granting access site by site. Each new site needs its own grant before CloudFiles can use it. Salesforce admins then register the SharePoint sites that users can see from Salesforce.

Once connected, sharing can be automated with Salesforce Flow. The **Create Link** action generates a share link for a SharePoint, Google Drive, AWS S3 or Azure Blob file or folder, and **Update Link Settings** changes its settings later. A record-triggered Flow can create a link when an Opportunity reaches a stage, write the link onto the record, and send it in the customer email, all without a person opening SharePoint.

How do I share SharePoint files with external users who have no SharePoint account?

This is the most common request we hear from teams that want to share SharePoint files with external users. SharePoint guest access means inviting outsiders into your tenant, managing their identities and remembering to remove them. CloudFiles removes that step. External users never need SharePoint access. They open a controlled share link, or they sign in to your Experience Cloud site and see only the folders you chose to show them.

The file never leaves SharePoint. Versioning, retention and audit in SharePoint keep working, because there is one copy, in your storage. The same holds for AWS S3, Google Drive and Azure Blob.

How does Experience Cloud file sharing work with CloudFiles?

For Experience Cloud file sharing, CloudFiles places its widget on community and portal pages and lets admins decide per widget which folders and files community and portal users see, and whether they can upload. Portal users see folders and files from SharePoint, Google Drive, AWS S3 or Azure Blob as if they were native to the portal.

Three Flow actions keep portal access in step with your process:

- **Share with Community User** grants a portal user access to a folder or file.
- **Remove from Community** takes that access away, for example when a case closes or a contract ends.
- **Get Shared Resources** returns what a given portal user can currently see, which is useful for audits and support.

A pattern we see in rights licensing: back-end systems write files straight into an AWS S3 bucket, event-driven sync indexes them onto the right record, and each portal member sees only their own documents.

What does Salesforce portal document upload look like?

Salesforce portal document upload is where many teams first hit Salesforce's own file size limits and storage limits. With CloudFiles, external users upload into SharePoint, Google Drive, AWS S3 or Azure Blob without having an account in that storage, and the file lands in the folder linked to the right Salesforce record.

- A public sector portal can collect applications into SharePoint and use a Flow to make the folder read-only after submission.
- A support team can accept large log files from a portal straight into a Case folder in Azure Blob.
- An operations team can use the **Create File Request** action to send an upload request tied to a specific folder, so the documents arrive already filed.

Because uploads go to your storage, they do not consume Salesforce file storage, and they arrive where your records management and retention policies already apply.

Which controls cover each sharing scenario?

Scenario	CloudFiles control
One-off document to a customer	Share link with email wall, password, verification code, expiry and view limit
Ongoing access for a partner or client	Experience Cloud widget with Share with Community User and Remove from Community
Collecting documents from outsiders	Portal upload or Create File Request into a record-linked folder
Proving who saw what	View tracking with location and per-file download tracking
Automated sharing at a deal stage	Create Link and Update Link Settings in Salesforce Flow

How is shared content kept secure?

- 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.

ISO certificates, the SOC 2 Type II report and a penetration test summary are available under NDA from the CloudFiles Trust Center.

Why do teams move external sharing to CloudFiles?

Teams tell us they want to stop working in two windows, stop pasting stored SharePoint URLs that break when folders move, and stop asking customers to create accounts just to send a document. Many are replacing Files Connect, Document Extractor or a sync tool that breaks on folder renames. With CloudFiles, secure external file sharing, portal uploads and share-link tracking all run from the Salesforce record, and the files stay in SharePoint, AWS S3, Google Drive or Azure Blob. Support is available 24x7.

Get started

Install CloudFiles Document Management from AgentExchange and start a free 14-day trial, or book a demo at cloudfiles.io.

