

SharePoint Case Folders for Utilities and Field Service

Case folders created by Flow, attachments and email files moved out of Salesforce storage, and one migration for the backlog

CloudFiles is Document Automation for Salesforce. This guide describes a pattern we see among utilities and field service organizations: automate a SharePoint folder for Cases, move Salesforce Case attachments to SharePoint as they arrive, and migrate the files already sitting in Salesforce. The same Flows can target AWS S3, Google Drive or Azure Blob.

What problem do utilities and field service teams have with Case files?

A utility's service team handles connection requests, meter disputes, outage claims and site visits as Cases in Salesforce. Every Case collects files: photos from the field, customer letters, meter readings, signed forms and a steady stream of email attachments. They pile up in Salesforce file storage. Storage fills, the organization looks at buying more, and the records team still wants the documents in SharePoint where retention and records policies already apply.

Meanwhile, anyone outside the service team who needs a Case document has to be given a Salesforce login or be sent an attachment. Both are poor answers.

Which Salesforce objects are involved?

- **Case:** each Case gets its own folder in SharePoint.
- **EmailMessage:** email-to-case messages and their attachments.
- **Salesforce Files (ContentDocument):** files attached to Cases by agents, portals or integrations.
- **Work Order or custom objects:** field service records can get folders the same way.

How do we automate a SharePoint folder for Cases?

To automate a SharePoint folder for Cases, an admin builds a record-triggered Flow on Case with CloudFiles Flow actions:

1. **Status change.** When a Case moves to a status such as Assigned or In Progress, the Flow calls **Create Folder** in the service team's SharePoint library, named from the Case number and linked to the record.
2. **Subfolders.** The same Flow creates subfolders such as Field Photos, Correspondence and Forms.

3. **Columns. Update Drive Columns** writes Case type, priority and account into SharePoint columns so the records team can search by them in SharePoint.

Starting on status change rather than on creation means Cases closed at first contact never create empty folders. The View Metadata dialog in the CloudFiles Content Library lists the Site Id, Drive Id and Folder Id a Flow needs, each with a copy button.

How do we move Salesforce Case attachments to SharePoint?

To move Salesforce Case attachments to SharePoint as they arrive, a Flow runs when a file is attached to a Case. It calls **Copy Salesforce Files** to place the file in the Case's SharePoint folder, and CloudFiles leaves a link on the record so agents open it in one click.

To take the file out of Salesforce storage as well, use **Move Resource** instead of copying. Move is asynchronous: it returns nothing, and completion arrives later as a CloudFiles event. A second Flow handles that event, and only in that handler is the Salesforce copy removed. That order means a file is never deleted before it exists in SharePoint.

The file-attached event setting ships off. Turn it on for this pattern; for orgs that do not need it, leaving it off reduces API calls.

How do we send email attachments to SharePoint?

Email-to-case brings a large share of the files. To route email attachments to SharePoint, a Flow on EmailMessage copies each attachment into the Case folder and writes the SharePoint link onto the email record, so the agent reading the email thread can open the file where it now lives. The same Flow can file attachments into the Correspondence subfolder.

How do we migrate Salesforce files to SharePoint that are already there?

For the backlog, a scheduled Flow works through existing Cases in batches. For each one it creates the Case folder if missing, then copies or moves the Case's legacy files into it and leaves links on the record. This one-time migration of Salesforce files to SharePoint runs alongside the live Flows, so new files and old files end up in the same place. Files Connect references are supported for SharePoint, so teams moving off Files Connect keep their existing links working.

The goal is simple: reduce Salesforce file storage costs by keeping documents in the SharePoint storage you already pay for, and stop buying extra Salesforce storage for files that belong in your records system.

What do agents and field teams see?

The CloudFiles file browser widget sits on the Case Lightning record page. Agents see the Case's SharePoint folder, preview photos, PDFs and Office files, search across the folder tree and upload new files, all without leaving Salesforce. CloudFiles works on the live SharePoint files through Microsoft's own

API, so there is one copy, in your storage. A records officer who adds a document in SharePoint sees it appear on the Case once the folder is linked.

Customers and contractors can upload into the Case folder through Experience Cloud without having an account in SharePoint, and without being held to Salesforce's own file size limits for portal uploads.

Who has access to the Case folders?

Flow automation runs as a service principal or integration user. The widget runs as each user through their own storage connection. The SharePoint service principal authenticates as the CloudFiles app in your Microsoft tenant, uses no license, and has no password or MFA to break. Your Microsoft 365 admin can limit CloudFiles to only the SharePoint sites you choose.

Update Permissions grants or revokes read or write on a Case folder by email, Salesforce user or group, for example when a Case is escalated to a specialist queue. Permissions go from Salesforce to SharePoint by Flow. External users never need SharePoint access: they receive a share link from **Create Link** with an email wall, password or verification code, an expiry and a view limit, and every view and download is tracked.

Is it 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.

Security documents 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.