

Salesforce Document Management Security and Permissions

How CloudFiles keeps SharePoint, AWS S3, Google Drive and Azure Blob access in step with Salesforce, and the evidence behind it

What does secure Salesforce document management require?

CloudFiles is Document Automation for Salesforce. CloudFiles Document Management connects Salesforce to SharePoint, AWS S3, Google Drive and Azure Blob (also OneDrive, Box and Dropbox) and automates folders, file uploads, permissions and secure sharing.

Secure Salesforce document management comes down to three questions a security reviewer will ask. Where do the files live? Who can reach them, and does that change when the Salesforce record changes? What independent evidence backs the vendor's claims? This data sheet answers all three.

Where the files live is the simplest answer. Your files stay in your own storage. CloudFiles transfers them over encrypted connections and does not re-host them. SharePoint and Google Drive files are worked on live through the provider's own API, so there is one copy, in your storage.

How do I sync SharePoint permissions with Salesforce?

Sales, service and project teams change constantly: owners are reassigned, account teams grow, territories are redrawn and deals close. If SharePoint access is managed by hand, it drifts away from Salesforce. CloudFiles lets you sync SharePoint permissions with Salesforce using Salesforce Flow, so the record decides who can open the folder.

The Flow actions for SharePoint permissions in Salesforce are:

- **Update Permissions:** grant or revoke read or write access on a folder or file, by email address or by Salesforce user or group.
- **Create SharePoint Site Group:** create a group for an Account, Opportunity or project.
- **Update SharePoint Site Group Members:** add and remove members as the Salesforce owner, account team or territory changes.

Typical triggers are an owner change, a team change, a territory reassignment, or a status change such as Closed Won, Closed Lost or submitted. For example, an IT services company can create a SharePoint site per Account, keep site-group membership following owner, team and territory, and archive the library when an Opportunity is Closed Lost.

Permissions flow from Salesforce to SharePoint by Flow. Salesforce is the source of truth for who should have access, and SharePoint enforces it.

Users need no SharePoint rights for the widget experience when an admin designs it that way, and external users never need SharePoint access.

Which identities does CloudFiles use?

CloudFiles separates automation from people, which is what makes Salesforce SharePoint security auditable:

- **Automation identity:** Flow automation runs as an integration user or as a service principal.
- **User identity:** the file browser widget and the Content Library run as each user through their own storage connection, so a user sees only what their own storage rights allow.

For SharePoint, the service principal option means CloudFiles authenticates app-only as the CloudFiles app in your own Microsoft tenant. It uses no license, has no password or MFA to break, and shows an "Active for automations" badge when connected.

How is access to SharePoint sites limited?

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 which SharePoint sites users can see from Salesforce.

How is the Salesforce side locked down?

On the Salesforce side, admins assign the Minimum Access Integration permission set to the integration user, which gives CloudFiles automation the permissions it needs and nothing more. Admins also control which objects carry the widget, what each widget allows, and whether print from preview is enabled.

How are AWS S3, Google Drive and Azure Blob connections secured?

- **AWS S3:** you enter the bucket name and deploy a CloudFormation template that creates an IAM role with an External ID.
- **Google Drive:** connected through a Google integration user with OAuth, covering My Drive and Shared Drives. Access can be revoked at any time from the Google admin settings.
- **Azure Blob:** you add the CloudFiles Entra gallery app and assign Storage Blob roles to the CloudFiles service principal. Network access can be restricted by IP allowlist.

In every case the grant lives in your cloud account, under your admin's control, and can be withdrawn by your admin.

Does CloudFiles hold ISO 27001 for Salesforce document management?

Yes. For teams that require ISO 27001 Salesforce document management, CloudFiles is ISO/IEC 27001:2022 certified, with ISO/IEC 27017:2015 and ISO/IEC 27018:2019. CloudFiles is also independently audited for SOC 2 Type II.

Is this HIPAA document storage Salesforce compliance teams can approve?

CloudFiles is compliant with HIPAA (BAA available) and compliant with GDPR. Because files stay in the storage you already run, your existing HIPAA controls in SharePoint, Google Drive, AWS S3 or Azure Blob keep applying. For example, a healthcare organization can automate document and folder creation in Google Drive from Salesforce records while patient files remain in its own Google Workspace.

Where is data hosted and how is it encrypted?

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.

Security controls at a glance

Area	CloudFiles control
File location	Your files stay in your own storage. CloudFiles transfers them over encrypted connections and does not re-host them.
SharePoint tenant access	Service principal or integration user; site-by-site grants by your Microsoft 365 admin
Permission changes	Update Permissions, Create SharePoint Site Group, Update SharePoint Site Group Members in Flow
AWS S3 access	IAM role with External ID via CloudFormation
Azure Blob access	Entra gallery app, Storage Blob roles, IP allowlist
Google Drive access	OAuth integration user, revocable from the Google admin settings
Certifications	ISO/IEC 27001:2022 certified, with ISO/IEC 27017:2015 and ISO/IEC 27018:2019
Audit	Independently audited for SOC 2 Type II
Regulation	Compliant with HIPAA (BAA available). Compliant with GDPR.
Encryption	TLS 1.2 minimum in transit; AES-256 at rest on production data stores

Where can my security team get the documents?

ISO certificates, the SOC 2 Type II report and a penetration test summary are available under NDA from the CloudFiles Trust Center. CloudFiles offers 24x7 support, so a security review question does not wait for business hours in California.

Get started

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

CloudFiles, Document Automation for Salesforce · cloudfiles.io · Install CloudFiles Document Management from AgentExchange