UPPER SPIRE | the summit of Salesforce cloud apps

CARTULARIUS

DOCUMENT MANAGEMENT

Getting Started with Cartularius for Admins

Getting Started with Cartularius for Admins

Cartularius Version 3.48

Disclaimer

Upper Spire B.V. (Upper Spire) makes no representation or warranty concerning the adequacy or accuracy of this documentation or the software which it describes. In no event will Upper Spire or its direct or indirect suppliers be liable for any damages whatsoever including, but not limited to, direct, indirect, incidental, or consequential damages of any character including, without limitation, loss of business profits, data, business information, or any other commercial damages or losses, or for any damages.

Upper Spire B.V.

Website: www.upperspire.com
E-mail: support@upperspire.com

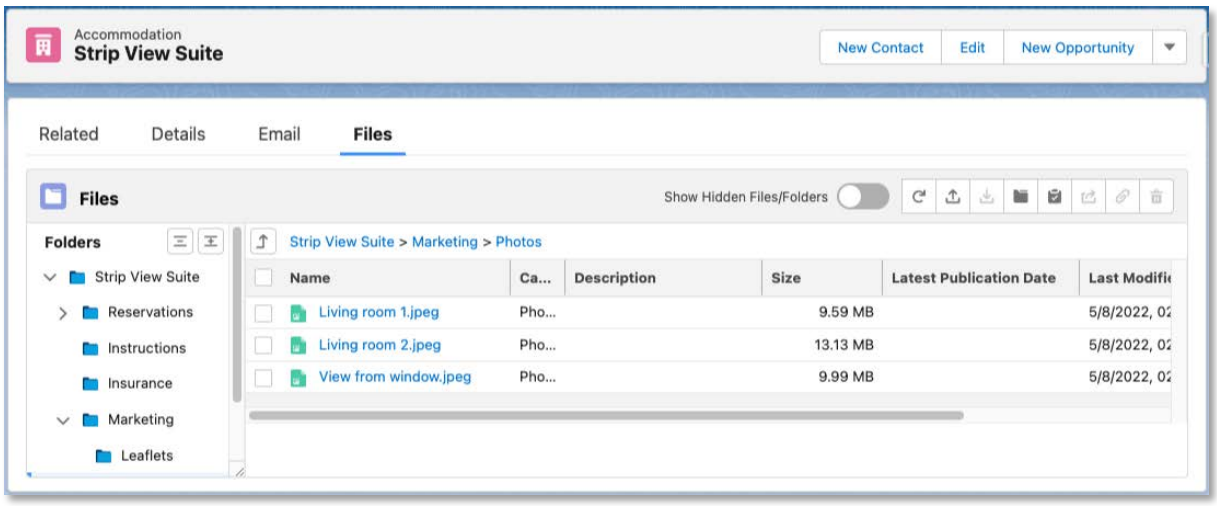
Table of Contents

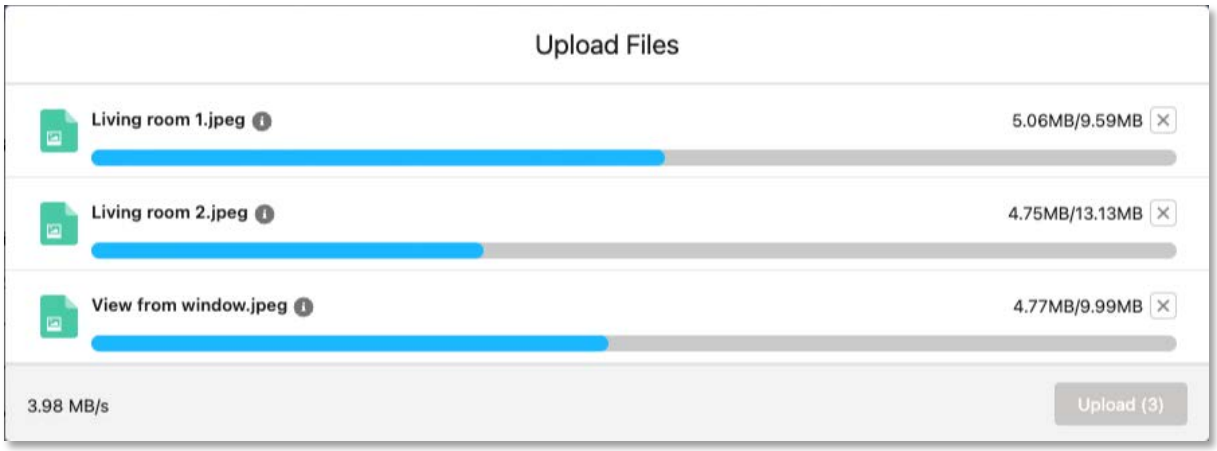
Chapter 1: Introduction

Welcome to the *Getting Started with Cartularius for Admins* guide. This guide is designed to provide documentation for a technical audience, specifically system administrators responsible for performing administrative tasks within the Salesforce ecosystem.

What is Cartularius?

Cartularius (CDM) is an app that can be installed from the Salesforce AppExchange as an add-on to your existing Salesforce organization. CDM is a document management solution that relates your Salesforce object model to an advanced folder hierarchy. The software also functions as an interface between Salesforce and Amazon S3, which is used to securely store your files. CDM is a cost-effective solution that enables you to store gigabytes of files and access them directly from your Salesforce records.

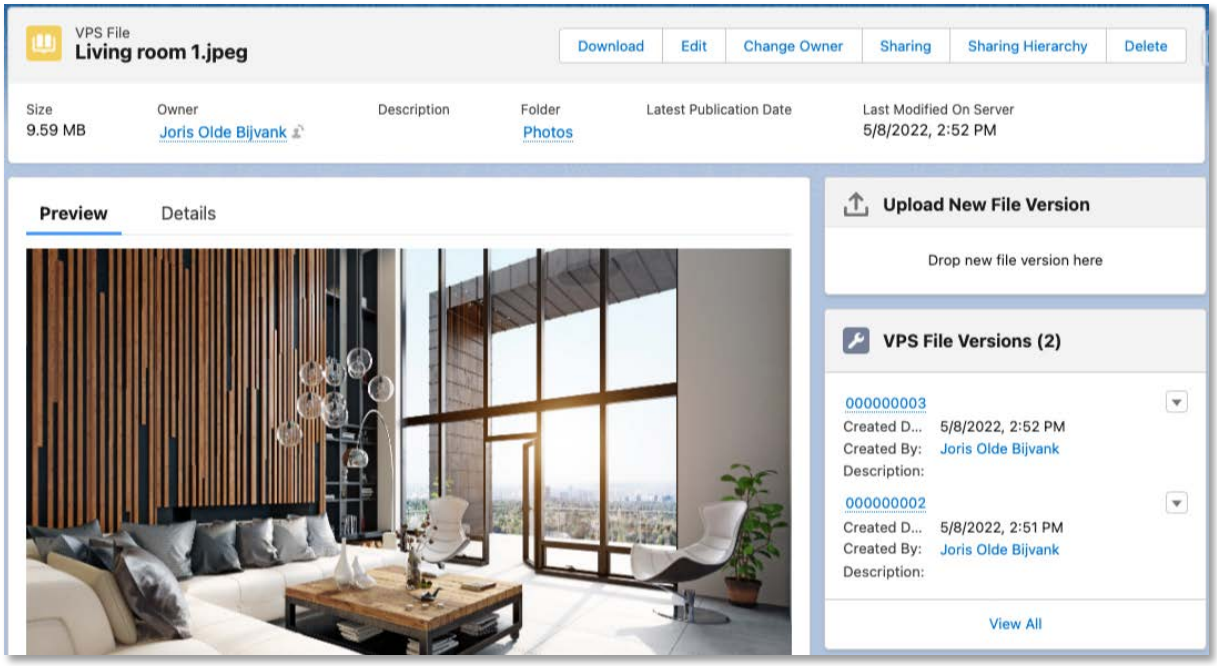




Scope of this document

This document is designed as a getting-started guide that covers the most common topics for starting with CDM from scratch. While it goes into detail on a vast number of topics, it is not designed as an all-inclusive reference manual.

This document only explains the administrative tasks for CDM. Please read the Getting Started with Cartularius for Users guide to learn how to use the software.



Chapter 2: Editions

Cartularius is available in **three editions**: **Core**, **Professional**, and **Enterprise**, each tailored to meet different needs to provide flexibility. All editions share the fundamental capabilities for Salesforce document management, but higher-tier editions include additional functionality for more advanced use cases. This section will help you understand the key differences between the editions and what functionality comes with each.

Cartularius Core Edition (Base Functionality)

Cartularius Core is the base edition, providing all the essential document management features natively within Salesforce. It includes everything you need to manage files and folders in a familiar, Salesforce-integrated interface. With the Core edition, users can organize documents using a hierarchical folder structure (including uploading entire folder hierarchies) and relate those folders to Salesforce records for context. Core supports easy file uploads with **drag-and-drop** simplicity, allowing you to import large files and whole folders in one go. Users can **preview common file types** (like PDFs, images, Word, or Excel documents) directly in Salesforce without downloading, enabling quick access to content. The app leverages **Salesforce Files** (the native file storage in Salesforce) for seamless integration with existing workflows or other AppExchange apps.

Core edition also provides robust organizational features to keep your documents tidy and consistent. It offers **automatic folder creation** based on Salesforce records or object types (so when a new record is created, predefined folders can be generated for it). You can enforce **file category restrictions** on folders – for example, specifying that a folder should only contain files of a certain category – and Cartularius will automatically sort incoming files into the correct folders, reducing manual effort. Additionally, **folder names can be translated** through multi-language support, allowing your end-users to see the folder structure in their preferred language.

To streamline user access to documents, the Core edition displays **related folders** on record pages, allowing users to easily navigate to folders linked to the records they're viewing. For instance, from an Account record, you might quickly access that account's document folder as well as folders of related records (like associated Opportunities or Cases) if configured. Core also enables **exporting files and folders** in bulk for sharing or backup: with a few clicks, you can export an entire folder hierarchy (including files from related records) as a Zip archive, instead of downloading files one by one. These capabilities form the foundation of Cartularius and are included in every edition, giving all users a solid, full-featured document management experience in Salesforce.

Cartularius Professional Edition (Advanced Capabilities)

Cartularius Professional includes *all* the functionality of the Core edition and adds a suite of advanced features tailored for organizations with more demanding document management requirements. The Professional edition is ideal if you need enhanced storage options, larger file support, or additional tools for collaboration, compliance, and productivity beyond the basics.

One of the key enhancements in Professional is integration with **external storage**. In this edition, you can connect Cartularius to an **Amazon S3** bucket to store documents outside of Salesforce. This brings benefits such as offloading file storage from Salesforce (useful if you have very large files or want to save on Salesforce storage costs) and leveraging Amazon's scalable, secure infrastructure for your documents. With S3 integration, Cartularius Professional supports files larger than the standard Salesforce file size limit. You can manage files well over 2GB (in fact, uploads of files up to 5TB are supported). The user experience remains the same, but behind the scenes, your files reside in your own S3 environment, giving you full control and potentially unlimited storage capacity.

In addition to external storage, the Professional edition introduces **document version control and collaboration** enhancements. Users can maintain and retrieve **multiple versions** of a file, helping teams collaborate safely by keeping version history. This goes hand-in-hand with Office integration: Professional supports **Office 365 integration for the web**, allowing your users to open and edit Word, Excel, and PowerPoint files directly from Salesforce in real-time. Colleagues can co-author documents through Office online, and Cartularius will save changes back to Amazon S3, ensuring everyone is always working on the latest version. This real-time editing capability allows teams to enjoy true **live collaboration with version control,** thereby avoiding overlap or lost changes.

Cartularius Professional also adds features to improve communication and oversight. Users can directly **email files (CDM files)** from the Cartularius interface, making it easy to share documents with colleagues or clients without needing to manually download and attach files. An **External Link Bundles** feature allows you to share multiple documents externally via a single secure link. For example, you can generate a single link that provides a client with access to a whole set of files at once, simplifying external sharing while maintaining security. For administrators and compliance needs, the Professional edition provides **comprehensive audit logs** of user actions. Every view, upload, download, edit, or deletion can be tracked, which is vital for auditing and governance. These audit logs help Salesforce Admins ensure that document handling meets company policies and regulatory requirements by keeping a detailed history of all file activity.

Rounding out the Professional feature set, this edition introduces **AI-powered tools** to boost productivity. Using your connected OpenAI account, Cartularius can perform **file content analysis,** such as automatically categorizing files by their content and suggesting the appropriate folder (an AI File Category Analysis). It can also generate **AI-driven summaries of documents**, providing users with a quick overview of a file's content without requiring them to read the entire document. For example, when uploading a lengthy contract or report, Cartularius can provide a concise summary directly in Salesforce. These AI features save time and enable users to find relevant information more quickly. In summary, the Professional edition is designed for organizations that require external storage flexibility, support for large files, advanced collaboration features (including Office 365 integration and version control), enhanced sharing options, thorough auditing, and intelligent document processing, in addition to the core features.

Cartularius Enterprise Edition (Full Integration and Automation)

Cartularius Enterprise is the top-tier edition, offering the most extensive feature set. It includes everything from the Core and Professional editions, and adds specialized capabilities designed for enterprise-scale requirements, complex Salesforce orgs, and advanced automation scenarios. If your implementation demands deep integration of document management into business processes or handling of complex record relationships, the Enterprise edition is optimized for you.

One major addition in Enterprise is the support for **Salesforce Invocable Actions** related to Cartularius. Invocable Actions enable Salesforce admins to seamlessly incorporate Cartularius functionality into **Salesforce Flows and Apex**. In the Enterprise edition, Cartularius provides a set of invocable actions (for example, creating a folder, uploading a file, or linking a document to a record via a Flow). This means you can automate document management tasks as part of your business processes. For instance, you could build a Flow that automatically creates a predefined folder structure and initial documents whenever a new project record is created, or a Flow that sends out a notification when a file with a certain category is uploaded. With invocable actions, Cartularius Enterprise empowers you to extend its capabilities through Salesforce's native automation tools, enabling custom solutions that were not possible with the out-of-the-box features alone.

Another advanced feature exclusive to Enterprise is **Indirect Related Folders**. This functionality builds on the related folders concept from the Core edition, allowing you to handle folder relationships across more complex or indirect record relationships. In practical terms, indirect related folders allow you to surface or link documents that are not directly related to a single record, but are associated through a chain of relationships. For example, if your data model involves multiple levels (such as an Account → Opportunity → Quote hierarchy), the Enterprise edition can be configured so that an Account's document management view includes not only the Account's own files but also relevant folders from related Quotes or other indirectly related records. This provides a more unified view of all pertinent documents in one place, which is particularly useful in complex Salesforce orgs where information is spread across several related objects. It helps users avoid searching through multiple records to find files and ensures that nothing falls through the cracks in a multi-tiered relationship scenario.

In summary, the **Core edition** gives you the robust basics of Salesforce-integrated file and folder management. Stepping up to **Professional** brings in external storage (Amazon S3 support), larger file handling, Office 365 web integration, advanced sharing and audit tools, and AI enhancements. The **Enterprise edition** includes all of that and extends the power of Cartularius into advanced Salesforce automation and complex record scenarios (through invocable actions and indirect folder relationships). When planning your Cartularius implementation, first identify which edition your organization has purchased or plans to use. Each edition is designed to meet the needs of admins and users, from fundamental requirements to cutting-edge document management solutions within Salesforce.

Chapter 3: Install or upgrade the Core Edition from the AppExchange

Cartularius Core is available on the Salesforce AppExchange as a managed package. To install a package, the user must have the "*Download AppExchange packages"* permission.

If you're not interested in the Core Edition and want to start with the Professional or Enterprise Edition immediately, please continue to the next chapter.

Follow the instructions below to install Cartularius into your production instance or sandbox:

1. Go to the AppExchange listing for Cartularius.

2. Click the **Get It Now** button.

3. Log in to AppExchange using your Salesforce production credentials.

4. Choose where you want to install this package
    a. **Install in Production**
    b. **Install in Sandbox**

5. Please complete the on-screen AppExchange Checkout steps if you are installing the package into a production organization.

6. Review and confirm the installation details
    a. Edit your profile if needed
    b. Read and agree to the terms and conditions
    c. Click **Confirm and Install**

7. Log in to the Salesforce instance where you want to install the package.

8. Select *"Install for Admins Only"* from the installation dialog box and click **"Install"** or **"Upgrade"**.

9. Check *'Yes' to grant access to these third-party websites* in the Approve Third-Party Access dialog box, and then click **Continue**.

10. Select **Done** when you see the message "This app is taking a long time to install." You will receive a notification e*mail when the installation is complete.*

For more information on installing a package from the AppExchange, refer to the Application Installation Guide.

Chapter 4: Buying, installing, or upgrading Cartularius Editions

When you install **Cartularius** from the Salesforce AppExchange, you receive the **Core Edition** by default. The Core Edition includes all foundational document management capabilities, providing everything you need to start organizing, uploading, and managing files and folders within Salesforce.

If your organization requires advanced functionality, such as external storage with Amazon S3, Office for the Web integration, AI-powered file categorization, or Salesforce Flow automation, you can **upgrade to the Professional or Enterprise Edition** at any time.

Upgrading unlocks additional functionality without requiring a reinstall or data migration. All your existing configuration and files remain intact.

If you would like to start immediately with the **Professional** or **Enterprise Edition**, or if you're ready to upgrade your existing Core Edition, please don't hesitate to **contact us**. Our team will schedule a brief call to review your requirements and make the necessary arrangements to enable your selected edition.

You can reach us directly through the contact details provided in the package listing or by visiting https://www.cartularius.com.

Chapter 5: Setting up your Amazon AWS account

Note: The features described in this chapter are available only in the **Cartularius Professional** and **Enterprise Editions**. If you are using the **Core Edition** and would like to access these capabilities, please contact us to discuss an upgrade.

Cartularius stores files directly on Amazon S3 using your Amazon AWS account. If you don't have an active AWS account, you can create one on the Amazon Web Services website or by completing the signup form directly.

Please visit the Amazon Web Services website for more information on the AWS Free Tier, which provides access to various free services, including 12 months of complimentary 5GB storage on Amazon S3.

Basic Setup

You need to create an access key before you can connect Amazon S3 and Cartularius. The access key consists of an *access key id* to identify you and a *secret key*, which is used to calculate the signature to authenticate any request. As a security measure, the secret part of the access key will be shown only once. If you lose or forget your *secret key*, it cannot be retrieved again. Instead, you must create a new access key and turn the old one inactive.

Perform the following steps to create a new access key:

1. Go to your AWS Management Console.

2. Open the account menu in the top-right corner of the screen and click **Security credentials**.

3. Open the *Access keys (access key ID and secret access key)* section.

4. Click **Create New Access Key**.

5. Securely store the given *access key id* and the *secret key*, as you need them while setting up Cartularius. You only need the access key once. Ensure that nobody else can use it again (delete the file, shred the paper; if necessary, you can always create a new access key).

Multi-Factor Authentication

One important security measure we would like to highlight is the use of multi-factor authentication (MFA) to enhance the security of your AWS account. Using MFA for your AWS account root user makes hacking into your AWS account much harder. Go to the documentation and follow the steps to enable MFA for your AWS account root user.

For more information and best practices for securing your AWS account, check out Amazon's best practices page.

Chapter 6: Configuring Amazon S3

Note: The features described in this chapter are available only in the **Cartularius Professional** and **Enterprise Editions**. If you are using the **Core Edition** and would like to access these capabilities, please contact us to discuss an upgrade.

After setting up an Amazon AWS account, the next step is to configure Amazon Simple Storage Service (S3). Amazon S3 is an object storage service offering industry-leading scalability, data availability, security, and performance.

Within Amazon S3, a bucket is a resource where objects are stored. With CDM, we use a bucket to store files in a folder hierarchy by assigning each file a uniquely identifiable key that consists of the entire folder path and filename.

Amazon S3 and its related services offer numerous configuration and security options. We will run you through the basics and ensure all necessary settings are set for CDM. Make yourself comfortable with all the options and keep your knowledge up to date, as well as your files secure.

Follow the instructions below to set up a bucket:

1. Go to the AWS management console.
2. Log in to Amazon if you have not done so already.
3. Click **Create bucket**.
4. Choose a unique bucket name.
5. Choose the *AWS Region* for the bucket (you can usually use the region closest to your location).
6. For now, the remainder of the settings can be left to their default values.
7. Click **Create bucket**.

The bucket is created and will be listed in the bucket overview. Click on the bucket name to open it.

By default, the objects tab will be shown. Here, you can browse through all files and folders that are uploaded to this bucket. For now, go to the *properties* tab.

Properties

The *properties* tab contains various configuration options for the selected bucket. Since this is a getting-started guide, we only explain the essential properties for CDM to set up a secure environment.

Bucket Versioning

With bucket versioning enabled, a new version of the document is created every time a document is uploaded with the same key.

If you want to undo a change made to the newest version of a document, you can restore a previous version.

Versioning also provides an extra layer of protection against ransomware attacks. In a ransomware attack, new file versions are encrypted with a key known only to the attacker, rendering the files useless to the owner. However, the encryption of older file versions remains unchanged, allowing for proper file restoration.

Bucket versioning can be enabled or suspended via the AWS management console or by using *CDM Settings* from within Salesforce. We strongly recommend that you enable this feature.

Default Encryption

Default encryption is the method used to encrypt objects stored in the bucket at rest. This provides an extra layer of security against direct attacks on Amazon's servers. Should an attacker successfully infiltrate the Amazon servers and be able to download any data, this data would be useless because it is encrypted.

It is recommended that server-side encryption be enabled with the Amazon S3 key (SSE-S3) type. If you have chosen the SSE-S3 key type, Amazon manages the encryption using a strong 256-bit Advanced Encryption Standard (AES-256) block cipher. There are no additional fees for using SSE-S3.

Permissions

The *permissions* tab contains various configuration options to control access to the selected bucket. While many options are out of the scope of this getting-started guide, we will include the most important ones.

Block Public Access

Make sure you *block all public access* to the bucket unless you know what you are doing and are 100% sure that you cannot provide access in any other way.

Cross-origin Resource Sharing (CORS)

Cross-origin resource sharing allows a web application to interact with resources in a different domain. In the CORS configuration, you define what interactions are allowed.

It is mandatory to create a CORS (Cross-Origin Resource Sharing) configuration to allow Salesforce to interact with resources stored in Amazon S3. This way, we can upload, download, and delete files as part of the Salesforce environment.

Example CORS Configuration

The following is an example of a CORS Configuration used to interact with the Salesforce instance. To make the configuration stricter, you can change the allowed origin to the specific domain of your Salesforce instance, i.e., *https://mycompany.lightning.force.com*.

```
[
  {
    "AllowedHeaders": [
      "*"
    ],
    "AllowedMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE"
    ],
    "AllowedOrigins": [
      "https://*.lightning.force.com",
      "https://*.upperspire.com"
    ],
    "ExposeHeaders": [
      "etag",
      "last-modified",
      "content-length",
      "content-type",
      "x-amz-version-id"
    ]
  }
]
```

Chapter 7: Configuring Cartularius

After the managed package for CDM has been installed and the Amazon S3 bucket is ready, it is time to configure CDM. Configuring CDM is relatively easy. Most of the app's settings are available within the *CDM Settings* tab and include easy-to-understand help text.

Prerequisites

Before we explore the *CDM Settings* tab, permission sets need to be assigned, Apex Class access must be configured, and Apex Managed Sharing can be set optionally.

Permission Sets

Cartularius has three permission sets that you can assign to users:

- Cartularius Admin
- Cartularius User
- Cartularius Base Access

A third permission set is available, but is only used for guest users:

- Cartularius Guest User

Cartularius Admin

The *Cartularius Admin* permission set grants assignees the permission to configure and use CDM. Because *Cartularius Admin* inherits all permissions from *Cartularius User*, there is no need to grant the Cartularius User permission set either.

Cartularius User

Assigning the *Cartularius User* permission set grants assignees the necessary permissions to use CDM. These permissions allow the user to upload, download, and preview files from the *Related Files and Folders* component (CDM's main component).

Cartularius Base Access

The *Cartularius Base Access* permission set grants the minimum Apex Class and object access required for standard Salesforce users who interact indirectly with Cartularius functionality. This ensures that system processes, such as triggers responding to changes on standard Salesforce objects (e.g., Accounts, Contacts, Opportunities), execute successfully even if the user does not hold a Cartularius license.

Note: Assign this permission set to Salesforce users who are not licensed for Cartularius but whose actions may trigger Cartularius automation. It prevents permission-related errors when Cartularius logic executes in the background.

Cartularius Guest User

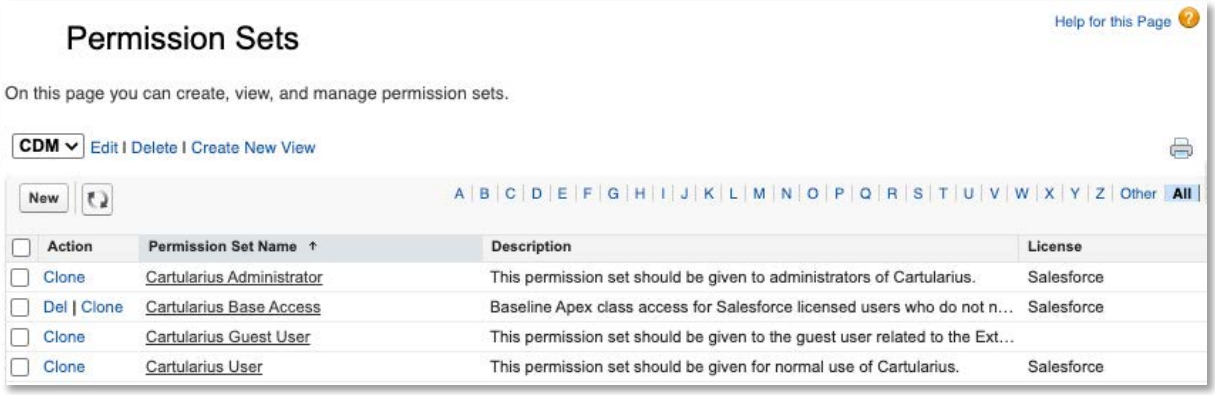
Cartularius Guest User is the permission set exclusively used by external parties to access files that have been shared with them using *External Links.*

Assign Permission Set to Users

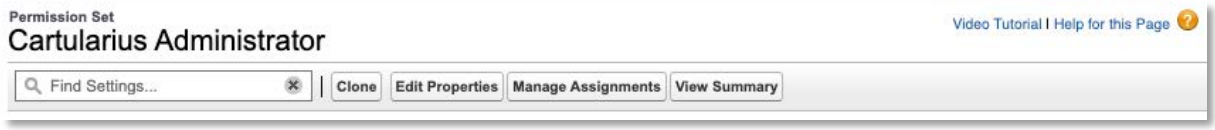
Perform the following steps to assign a permission set to users:

1. From Setup, enter *Permission Sets* in the Quick Find box, then select **Permission Sets**.

2. Open a permission set by clicking its label in the list of permission sets.



3. Click **Manage Assignments**.



4. First, we need to create local versions of the permission sets **Cartularius Admin** and **Cartularius User**.

Note: Those permission sets are used to configure the **External Client App**, and it isn't allowed to use managed permission sets for that. Also, **local permission sets** can be used to fine-tune permissions to match your organization's requirements.

5. Click **Clone**.

6. Fill in the Label and the API Name (i.e., **Cartularius Administrator Local** / **Cartularius_Administrator_Local**)

7. Click **Save**.

8. Click the label of the local permission set.

9. Click **Manage Assignments**.

10. Click **Add Assignment**.

11. Select one or more users by clicking the option box(es).

12. Click **Next**.

13. Click **Assign.**

Repeat the above steps for the **Cartularius User** permission set.

CDM Settings (All Editions)

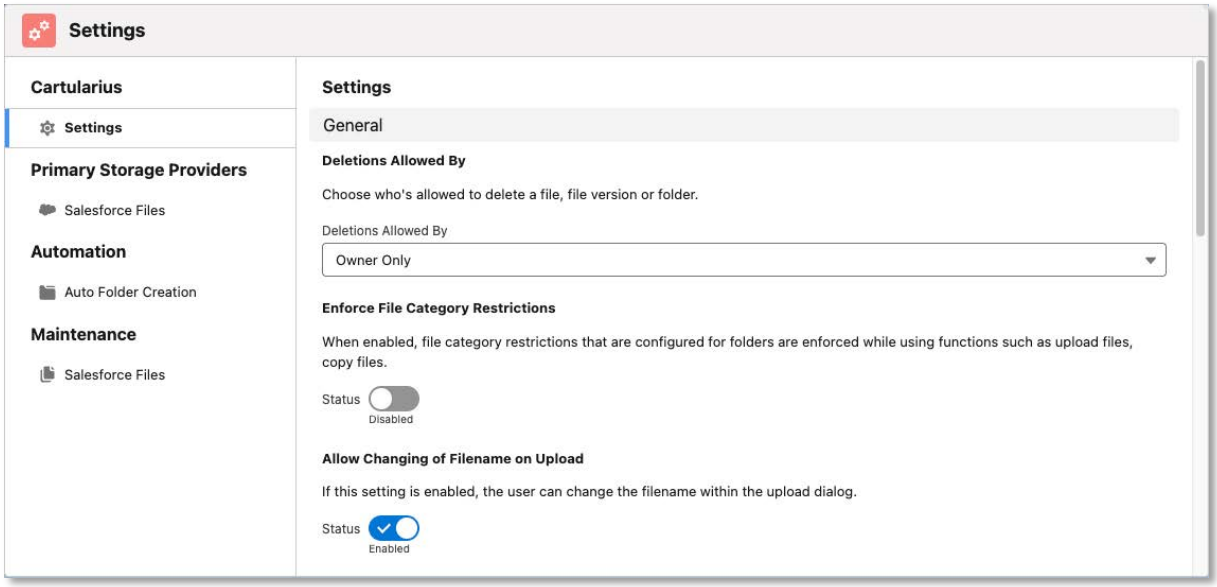
The *CDM Settings* tab is the central hub for configuring CDM. Having a centralized configuration page will make it easier for admins to configure and maintain the application.

The *CDM Settings* tab is available for users assigned to the Cartularius Admin permission set. To open it, click the App Launcher at the top left of the screen and select *CDM Settings* from the *All Items* section.

In this section, we are showing how to configure the settings that are available in all Cartularius Editions, including the Core Edition. In the following sections, we show how to configure settings that are available in the Professional and Enterprise Editions.

Settings

The settings section contains general configuration options on a vast number of subjects.



Deletions Allowed By

Control who can delete files from CDM.

Deletion Allowed By	Description
Owner Only	Only the owner of a file can delete it.
Owner & Admins	The owner of the file and users with the *Cartularius Admin* permission set can delete a file.

Enforce File Category Restrictions

Files in CDM are categorized by file category. When file category restrictions are enforced and configured on a folder, only the configured file categories are allowed. You can only upload or copy files with the configured categories into that folder.

File categories are maintained within the global value set *CDM File Categories*.

Allow Changing of Filename on Upload

Sometimes, original file names contain a postfix text that the operating system adds when having multiple copies of the same file in a specific folder. In other situations, the filename does not reflect the file's contents, and you want to change it.

Whatever the reason, CDM allows you to change the filename from within the upload dialog when the *Allow Changing of Filename on Upload* setting is enabled.

File Handling Mode

Define how Cartularius processes files when a new upload has the same name as an existing file in the same folder. This setting ensures consistent version management and helps prevent accidental overwrites.

File Handling Mode	Description
Create New Version	Adds the uploaded file as a new version of the existing file. The file history is preserved, and users can access previous versions from the version list.
Create New File with Postfix	Uploads the file as a separate file and automatically adds a numeric postfix (e.g., *filename(1).pdf*) to distinguish it from existing files.

Button Style

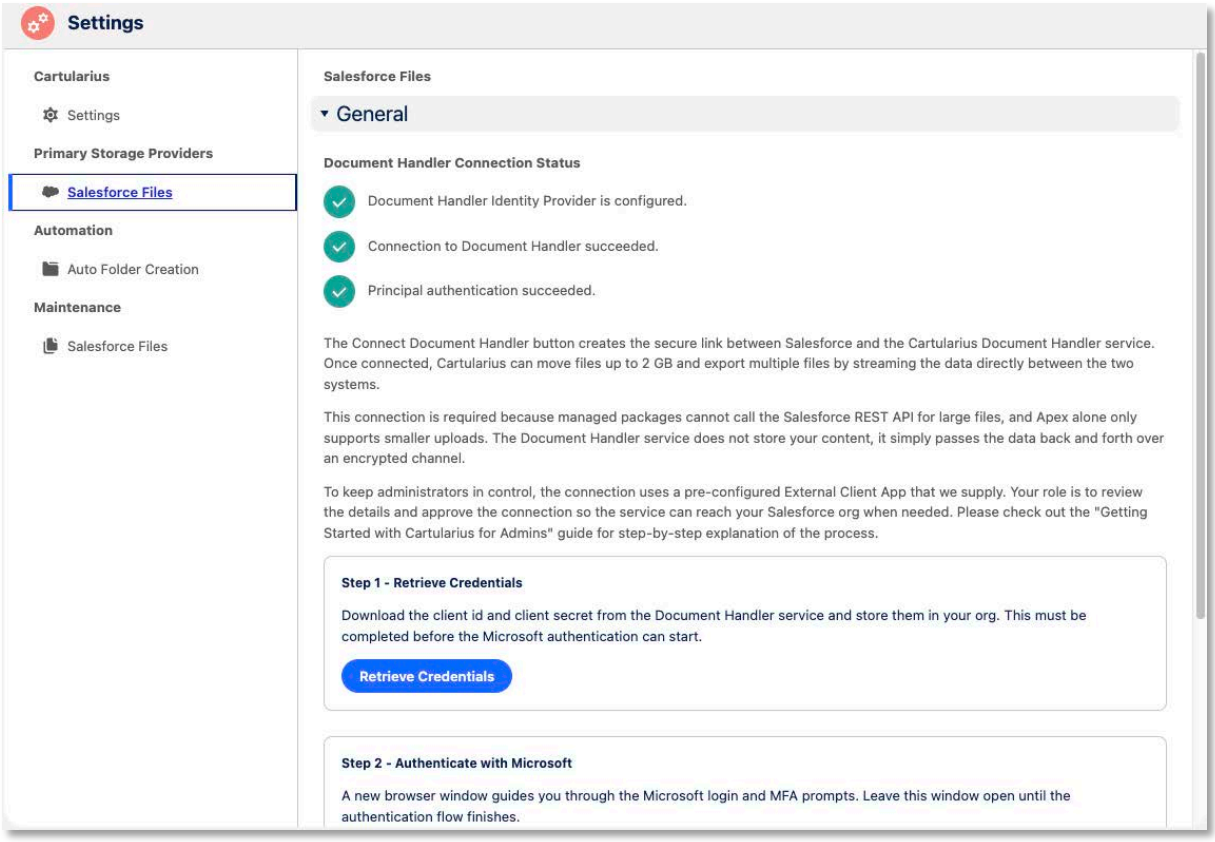
You can choose the preferred button style for the file library and the related files and folders list. Options are *Label only*, *Icon only,* and *Label and Icon*.

Daily Maintenance Scheduled Job

The *CDM Daily Maintenance Scheduled Job* is mandatory for the functioning of Cartularius and should always run once a day. The scheduled job is responsible for various maintenance tasks, such as cleaning expired *External Links*.

Salesforce Files

The **Salesforce Files** settings tab lets you securely connect your Salesforce org to the **Cartularius Document Handler** service. This connection enables Cartularius to handle large file uploads (up to 2 GB) and export multiple files by streaming data directly between Salesforce and the Document Handler service.



About the Connection

There are a few simple steps to follow to establish a secure link between Salesforce and the Cartularius Document Handler.

The first step is to retrieve the up-to-date credentials for the Document Handler. Click the **Retrieve Credentials** button to perform this action.

The second step is to authenticate with Microsoft. Clicking the **Authenticate** button starts the authentication flow. Enter your credentials so that Cartularius can send a file stream to the Cartularius Document Handler web service.

This connection is required because Apex alone cannot perform large-file uploads, and managed packages are not allowed to call the Salesforce REST API directly for such operations.

Note: The Document Handler service does **not** store any content; it securely transfers data between Salesforce and your browser through an encrypted channel.

Once the connection is configured, you can click the **Verify Connection** button to verify the connection and refresh the following indicators to confirm a successful setup:

- Document Handler Identity Provider is configured.
- Connection to Document Handler succeeded.
- Principal authentication succeeded.

Note: It happens sometimes that a timeout occurs while authenticating with Microsoft, and the Connection to the Document Handler isn't set up correctly. Don't worry; just perform the **Authenticate** step again, and it will most likely succeed.

Next, we'll walk you through the step-by-step configuration of the External Client App, which establishes the connection from the web service back to your Salesforce org.

Step-by-Step: Configure the External Client App

To connect the Cartularius Document Handler, you first need to verify and configure the External Client App in Salesforce Setup.

1. In Salesforce, go to **Setup**.

2. In the **Quick Find** box, type **External Client App**, then select **External Client App Manager**.

3. Locate and click **Cartularius Document Handler** to open its configuration page.

4. Scroll to the **OAuth Policies** section.
    - Under **Permitted Users**, select **Admin approved users are pre-authorized**.
    - Click **Save** if prompted.

5. Scroll to the **App Policies** section.
    - In **Custom Start URL**, enter *https://documents.upperspire.com*
    - Under **Selected Permission Sets**, choose **Cartularius Administrator Local** and **Cartularius User Local**.
    - Click **Save** to apply the changes.

6. Return to the **Cartularius Settings** page in Salesforce.

7. Click **Connect Document Handler**.
    - A Salesforce authorization screen appears. Review the details and approve the connection.

Once the connection is successfully established, all three indicators on the **Salesforce Files** tab will show a green checkmark, confirming that the Document Handler is configured correctly and ready for use.

Auto Folder Creation

What is Auto Folder Creation?

The Auto Folder Creation (AFC) feature is a great automation tool for structuring files and folders based on the relationship model and the state of records in your Salesforce instance.

In short, when a record is created in Salesforce, a folder hierarchy will be generated based on the AFC configuration.

Most of the configuration is stored in the following custom objects:

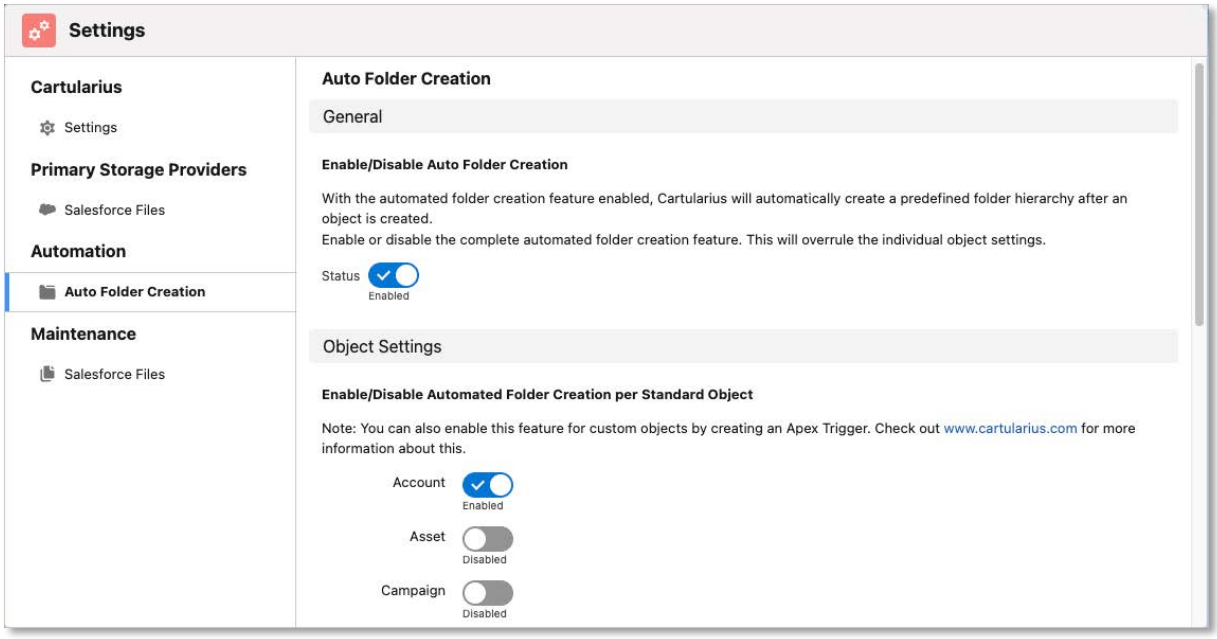
Object	Description
AFC Object	Basic object configuration per SObject and Record Type (Base Folder, Key Field, etc.).
AFC Folder	Basic folder configuration per SObject and Record Type (Folder Name, Parent Folder etc.).
AFC Folder File Category	List of File Categories that are allowed per AFC Folder.
Related Folder	Creates a folder relationship between two direct related records within a parent child relationship.
Indirect Related Folder	Creates a folder relationship between two records based on a junction record.

More information on AFC is available in the *Auto Folder Creation* chapter of the guide.

Object Settings

The AFC feature can be enabled or disabled per standard object. When a record is created, a trigger is fired to check if AFC is active for the object in question. If so, a folder hierarchy based on the AFC configuration is created.

Note: The section *Create Triggers for Custom Objects* describes how to enable AFC for custom *objects*.

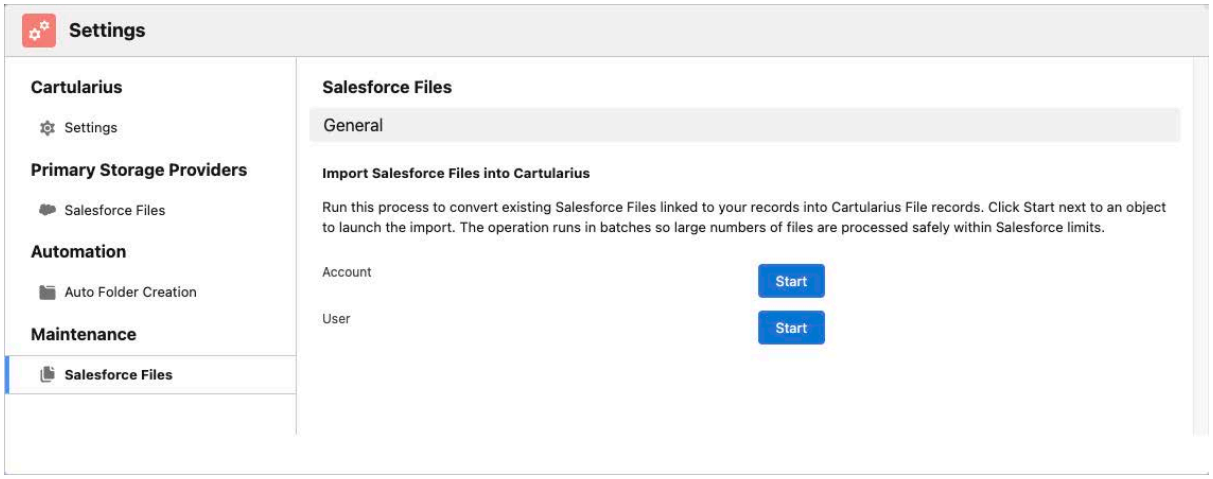


Salesforce Files Maintenance

The **Import Salesforce Files** tab allows you to bring existing Salesforce Files into Cartularius so they can be managed using the Cartularius folder structure and file features.

You can use this process when first setting up Cartularius or after enabling additional objects for file management. Clicking **Start** next to an object begins the import for that object. The process runs in batches, ensuring that even large volumes of files are safely converted within Salesforce limits.

After import, the files appear as **Cartularius File** records, allowing you to organize, preview, and manage them consistently within Cartularius.



CDM Settings (Professional and Enterprise Edition)

Default Internal Access

Choose the default internal access level for folders, files, and file versions.

Default Internal Access Level	Description
Private	CDM Files are only visible to the owner and users with the *CDM Admin* permission set. *
Controlled by Parent Record	CDM Files are only visible to a user if that user has access to the record that the file is related to.

* Regular sharing rules apply.

Recalculate Sharing

The **Recalculate Sharing** function allows administrators to manually refresh all Cartularius sharing rules and user access settings.

Whenever user permissions, roles, or organization-wide sharing configurations are updated in Salesforce, Cartularius automatically synchronizes these changes during its nightly maintenance process. In most cases, this automatic update ensures that all users have the correct access without any manual action.

If you need these changes to take effect immediately, such as after major permission adjustments, role restructuring, or troubleshooting access issues, you can trigger this process manually by clicking **Recalculate Sharing**. This will reapply Cartularius access rules across all items, ensuring users can see or edit the resources their new permissions allow.

Note: Running this process can temporarily increase system load. Use it only when necessary to apply recent permission changes without waiting for the next scheduled maintenance cycle.

External URL's

Cartularius supports configurable external URLs that define which online viewers are used to preview files directly from within the application. These settings give administrators control over the preview behavior and ensure compatibility even if external providers change their services in the future.

Two external URLs can be configured:

- **Google Docs URL** – Defines the base URL used for previewing file types supported by Google Docs. This enables inline previewing of compatible formats such as PDF or text-based files through Google's online document viewer.

- **Office Apps URL** – Defines the base URL used for previewing Microsoft Office file types (such as .docx, .xlsx, or .pptx) through the Office Apps viewer. This integration provides an alternative preview experience for users working primarily with Microsoft formats, without relying on the Microsoft 365 web application.

Administrators can update these URLs as needed to adapt to future changes in Google or Microsoft's viewing endpoints. The specific viewer used for each file type is determined internally by Cartularius, based on the configuration in the **File_Type** custom metadata. This metadata maps file extensions to their preferred preview method, ensuring a seamless and consistent user experience.

Note: These settings only affect *how* files are previewed. Actual file access, permissions, and storage locations remain fully managed by Cartularius and Salesforce.

External Links

Note: The External Links feature is available only in the **Cartularius Professional** and **Enterprise Editions**. If you are using the **Core Edition** and would like to access this feature, please contact us to discuss an upgrade.

The external links section contains various settings to configure *how External Links* are used to securely share files with external parties.

Enable/Disable External Links

You can enable or disable *External Links* with this switch. If there are any active *External Link Bundles,* they will be deactivated and, therefore, become inaccessible to the external party immediately.

Digital Experience Site URL

Enter the URL of the Digital Experience Site, which contains the *External Link* component.

Email Template for External Links

Select the *Email Template* to create an email message that will be sent to the external party when the *External Link* is activated.

Default Maximum Number of Downloads

The *Maximum Number of Downloads* is a safety measure used to prevent the abuse of download links. When an External Link Bundle is created, the user can override the default value.

Maximum Number of Files in a Bundle

To prevent system abuse, the maximum number of files that a user can add to a single External Link Bundle is limited.

Expiration Date Required

Enabling this setting forces the user to set an expiration date for the *External Link Bundle* upon creation. When the expiration date is exceeded, the *External Link Bundle* will become unavailable.

Default Expiration Period

Sets a default expiration period (in days) for when an *External Link Bundle* is active. The user can override this setting when creating the *External Link Bundle*.

Password Required

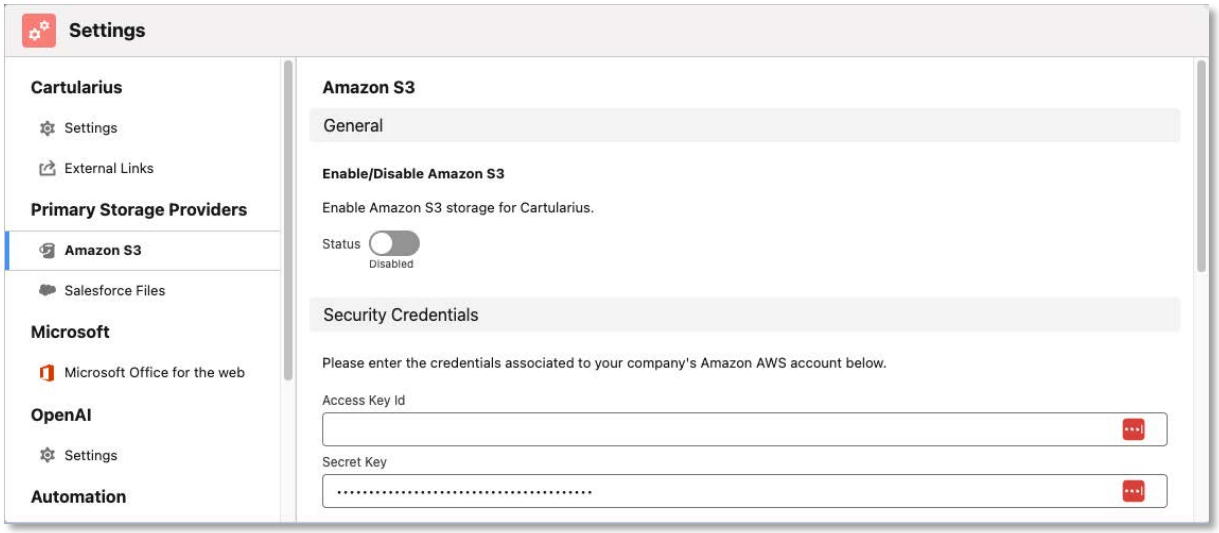
Enabling this setting to force the user to enter a password when creating an External Link Bundle is highly recommended. The external party needs this password to access the shared files.

Enforce Strong Password

Enabling this setting forces the user to enter a strong password when creating the *External Link Bundle*. A strong password is at least eight characters in length, contains both uppercase and lowercase letters, contains both letters and numbers, and contains at least one special character. It is highly recommended that this setting be enabled.

Amazon S3

Note: The Amazon S3 feature is available only in the **Cartularius Professional** and **Enterprise Editions**. If you are using the **Core Edition** and would like to access this feature, please contact us to discuss an upgrade.



Enable/Disable Amazon S3

In the **Professional** and **Enterprise** editions of Cartularius, files can be stored in **Amazon S3** rather than exclusively in Salesforce. This provides greater scalability, performance, and flexibility for organizations managing large volumes of documents.

To give administrators full control over when this capability becomes active, Cartularius includes an **Enable/Disable Amazon S3** switch in the settings page.

When the switch is **off**, Cartularius continues to operate entirely within Salesforce's native file storage model. No files are written to or retrieved from S3, even if the S3 integration has already been configured.

When the switch is **on**, Cartularius begins storing and retrieving files through the connected Amazon S3 environment according to your configuration. This activates all S3-based operations, including upload, download, and preview handling.

AWS Security Credentials

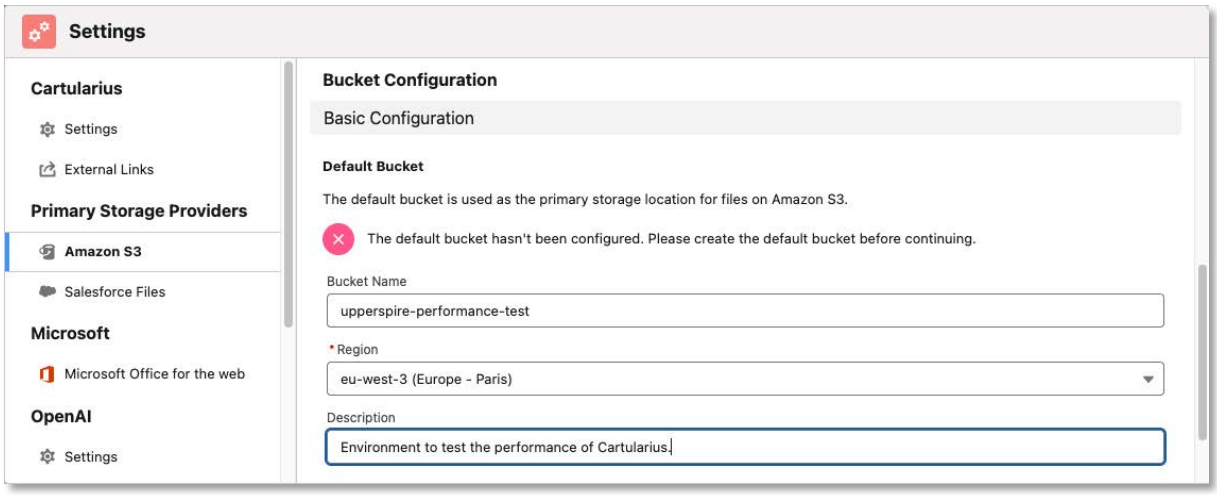
Enter the Amazon AWS Security Credentials created in the chapter *Setting up your Amazon AWS account,* and click **Save**.

The security credentials are stored in protected custom settings. The public part of the security credentials is shown in the Access Key Id field. For security reasons, the Secret Key can only be entered and will never be shown on the client side.

Bucket Configuration

First, a bucket needs to be created in the Amazon AWS console. After making it on Amazon S3, we can create a *default bucket* record in Salesforce. This bucket record stores the relationship between CDM and the bucket within Amazon.

Create a Default Bucket



Fill out the fields on the form shown to create a default bucket from within the Buckets section of the CDM Settings tab.

Field	Description
Bucket Name	Choose the same name as the bucket that was created on Amazon S3.
Region	Choose the same region as was configured on Amazon S3. *
Description	Enter the description of the bucket. This field is optional.

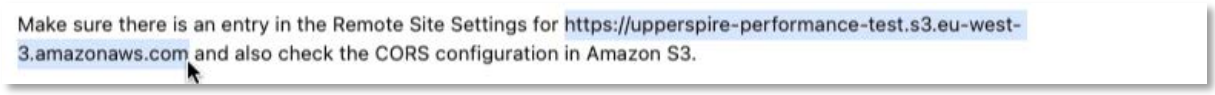
* If the region is unavailable, you can add it manually to the *CDM AWS Regions* Global Value Set.

Create Remote Site Settings

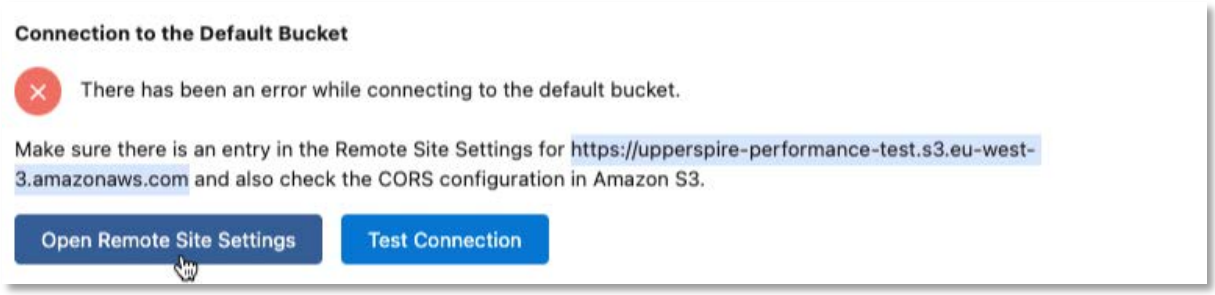
After the bucket has been created in Salesforce, an attempt is made to create a connection to it using the given bucket configuration and security credentials.

It is natural for the connection to fail the first time since setting up Remote Site Settings for the URL is mandatory. Perform the following steps to create the *Remote Site Settings* and set up a connection with the bucket on Amazon S3:

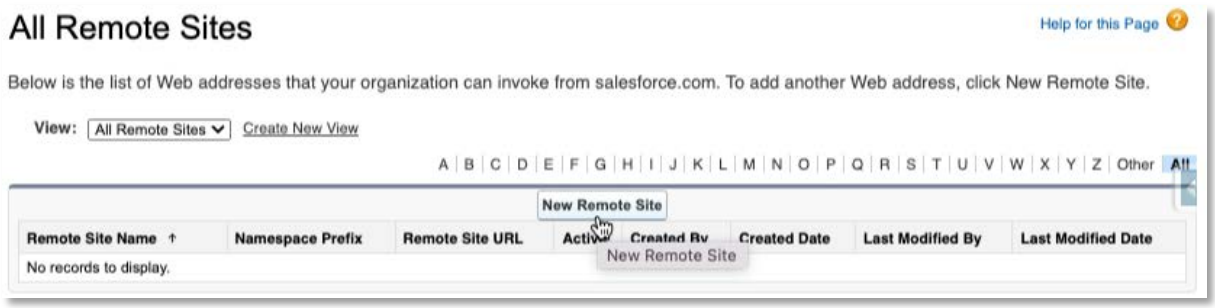
1. Copy the shown URL.



2. Click **Open Remote Site Settings**.



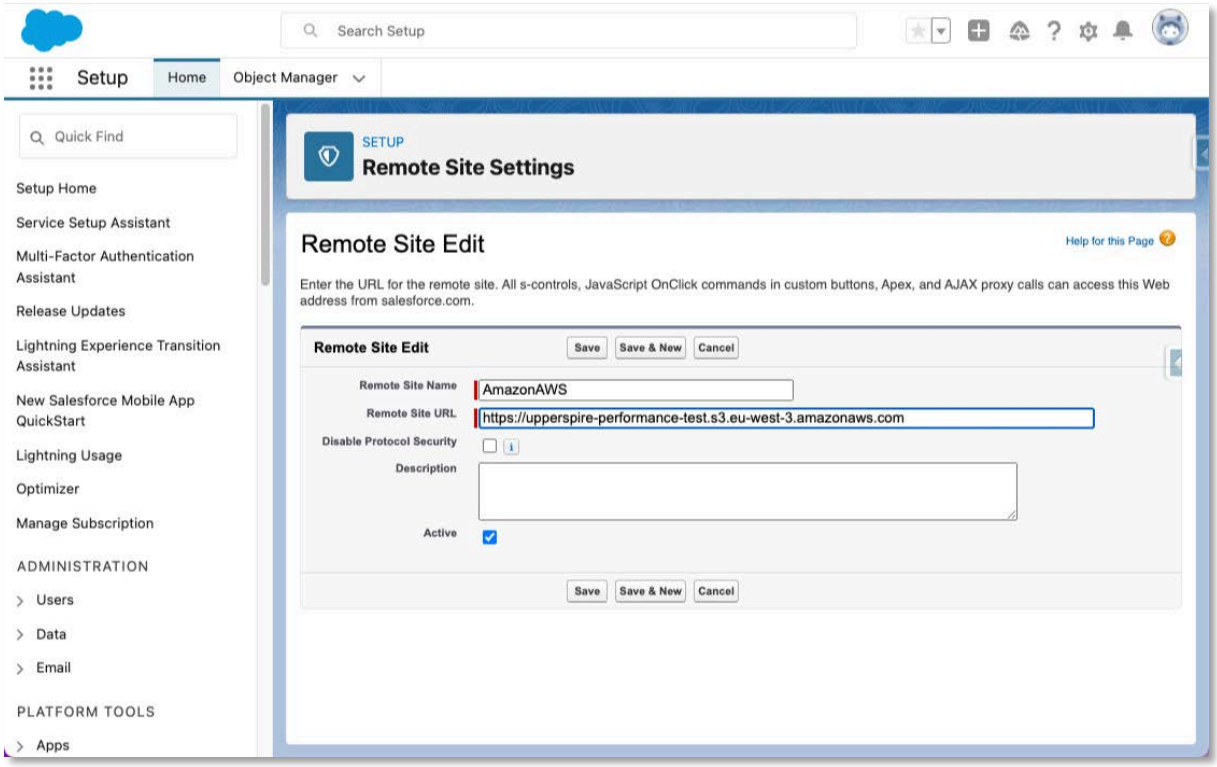
3. Click **New Remote Site**.



4. Enter a descriptive Remote Site Name.

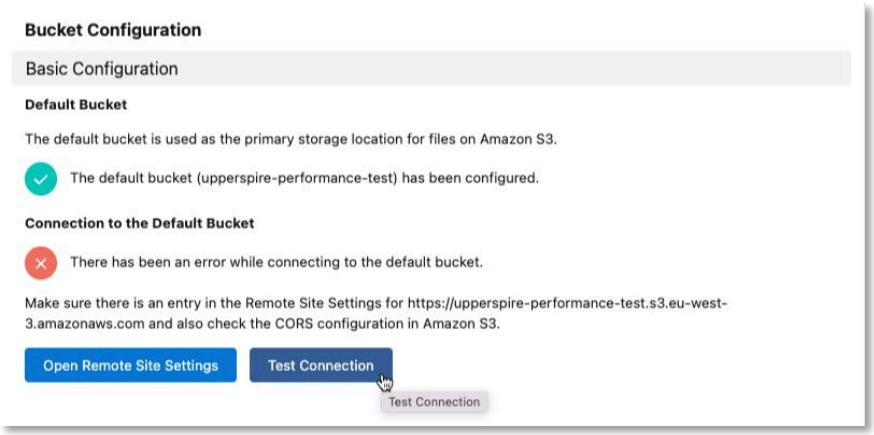
5. Paste the copied URL into the *Remote Site URL*.

6. Click **Save**.



7. Close the *Remote Site Settings* browser tab.

8. Click **Test Connection**.



If the connection still fails, the CORS configuration on Amazon S3 may not be correct. When the connection is successful, the encryption and versioning settings are shown, mirroring those configured on Amazon S3.

Server-Side Encryption

Server-Side Encryption encrypts files at rest. Although it can be disabled, it is best practice to enable Server-Side Encryption. More information on Server-Side Encryption can be read in the chapter *Configuring Amazon S3*.

Encryption Key Type

Amazon S3 supports the following Encryption Key Types:

- Amazon S3 key (SSE-S3) – An encryption key that Amazon S3 creates, manages, and uses for you
- AWS Key Management Service key (SSE-KMS) – An encryption key protected by AWS Key Management Service

If SSE-KMS is chosen, you need to enter the AWS KMS Key created using the AWS Key Management Service. Both the key id and the alias format are supported.

Versioning

With versioning enabled, multiple versions of a file can exist distinguished by a version id. If a file is uploaded into a folder that already contains a file with the same name, a prompt will ask if it is allowed to overwrite the existing file. The file gets overwritten when agreed upon, but the old version is still accessible from the *CDM File* Flexipage.

Microsoft Office for the web

Note: The Microsoft Office for the web feature is available only in the **Cartularius Professional** and **Enterprise Editions**. If you are using the **Core Edition** and would like to access this feature, please contact us to discuss an upgrade.

Cartularius supports native integration with **Microsoft Office for the web**, enabling users to open and edit Microsoft Office documents directly from within Salesforce. This integration allows both individual and collaborative document editing experiences while ensuring that administrators retain full control over the configuration.

This feature is intended for **commercial customers** and may **not** be used by:

- United States Federal, State, Local, or Tribal government entities.
- Contractors or organizations handling U.S. Government data subject to **FedRAMP**, **IRS 1075**, **CJIS**, or other regulatory data residency requirements.

By enabling Microsoft Office for the web, you confirm that your organization meets Microsoft's eligibility and compliance requirements for this feature.

Configuration Overview

Enable/Disable Microsoft Office for the Web

The **Enable/Disable Microsoft Office for the web** switch activates or deactivates the entire integration. When **disabled**, Cartularius will not initiate any WOPI requests, and Office documents will open using the standard preview methods configured in the Settings, as mentioned earlier in this document.

When **enabled**, Cartularius will use the WOPI URLs to route supported Microsoft Office files (e.g., .docx, .xlsx, .pptx) to Microsoft Office for the web for real-time editing and collaboration.

This switch is intentionally designed to give administrators full control. When upgrading from the Core Edition, the feature remains **disabled by default** until you explicitly enable it, ensuring the organization is ready to connect to Microsoft's services.

Enable/Disable Co-Authoring

Microsoft Office for the web supports **co-authoring**, allowing multiple users to edit the same document simultaneously. When **Co-Authoring** is enabled:

- Users see **real-time updates** from other editors.
- Presence indicators and cursor positions are displayed for each active user.
- Changes are synchronized immediately across all open sessions.

Disabling co-authoring limits document editing to a single user at a time but can be useful for organizations that prefer strict document locking.

WOPI URL's

Cartularius connects to Office for the web through the **WOPI (Web Application Open Platform Interface)** protocol.

The integration relies on three URLs that define how Cartularius discovers, hosts, and communicates with the WOPI services.

Setting	Description
WOPI discovery URL	The endpoint used by Cartularius to retrieve Office for the web's discovery metadata. This defines the available file types and associated actions (view/edit). Currently, the URL is set to https://onenote.officeapps.live.com/hosting/discovery.
WOPI Host URL	The public endpoint where Cartularius serves as a WOPI host for files managed within the organization. This URL typically corresponds to your Cartularius external file service. Currently, the URL is set to https://files.upperspire.com.
WOPI Server URL	The Cartularius-managed WOPI server endpoint that handles the communication between Salesforce, the file host, and Office for the web. Currently, the URL is set to https://wopi.upperspire.com.

Note: A corresponding **Remote Site Setting** must be created in Salesforce for each of the three URLs. This ensures that outbound callouts to these endpoints are allowed and that Cartularius can communicate with Microsoft's WOPI services securely.

OpenAI

Note: The OpenAI feature is available only in the **Cartularius Professional** and **Enterprise Editions**. If you are using the **Core Edition** and would like to access this feature, please contact us to discuss an upgrade.

Cartularius integrates with **OpenAI's GPT models** to provide advanced content analysis and intelligent document summarization.

This integration enables AI-powered automation across your document library, helping users quickly understand, categorize, and locate files through enriched metadata and content insights.

Administrators can configure the OpenAI connection in the **Settings** page to establish and manage the integration.

General Configuration

Enable/Disable OpenAI GPT

The **Enable/Disable OpenAI GPT** switch activates or deactivates all GPT-related features in Cartularius. When enabled, Cartularius uses the OpenAI API to analyze document content and enhance file management through automated category detection and summary generation.

When disabled, no external API calls are made to OpenAI, and all AI-based features are suspended.

Chat Completion Endpoint

The Chat Completion Endpoint defines the API endpoint used by Cartularius to communicate with OpenAI.

By default, this value is pre-filled with the standard OpenAI endpoint:
https://api.openai.com/v1/chat/completions

Administrators should verify this endpoint before enabling the integration and create a corresponding **Remote Site Setting** in Salesforce to authorize outbound API calls to this URL. If OpenAI changes its service endpoint in the future, this field allows you to update the connection without requiring a package update.

OpenAI Credentials

Cartularius requires authentication credentials to connect securely with OpenAI's API:

- **Organization ID** – Identifies your OpenAI organization.
- **API Key** – Provides secure access to OpenAI's API services.

Both values can be obtained from your OpenAI account dashboard. Enter these credentials in the provided fields to establish a trusted connection between Cartularius and OpenAI's systems.

The credentials are stored in protected custom settings. The public part of the credentials is shown in the Organization ID field. For security reasons, the API Key can only be entered and will never be shown on the client side.

AI Features

Cartularius offers two independent AI features that can be toggled on or off based on your organization's preferences and data governance requirements.

Enable/Disable File Category Analysis

When enabled, Cartularius adds an **"Analyze Categories"** option to the file upload process. This uses GPT to examine document content and suggest:

- The most relevant **file category**
- The most suitable **target folder** for storage

This feature improves information architecture consistency and reduces manual categorization effort for users. If disabled, users can still upload and organize files manually.

Enable/Disable Automated Summary Creation

When this option is enabled, Cartularius automatically generates concise summaries for uploaded documents using GPT. These summaries appear alongside file records, allowing users to quickly understand a document's content without opening it.

The generated summaries are also indexed for search, improving discoverability through Einstein Search and Cartularius' own query interfaces.

Disabling this feature prevents automated text generation while maintaining normal file upload behavior.

Model Selection

In Cartularius, you can choose the appropriate **GPT model** to perform all OpenAI-powered operations, including category analysis and automated summary generation.

Administrators can configure which model to use and define its **maximum token limit**, ensuring that the selected model aligns with the size and complexity of documents processed in the organization.

Select the GPT model that best suits your organization's requirements. A common choice would be **gpt-5**, which allows you to use a 128,000 maximum token limit.

Check out https://platform.openai.com/docs/models/ to find out if there are newer models or models that better suit your requirements.

Deleted Files

Instant Permanent Delete

Instant Permanent Deletes can be enabled or disabled. When enabled, when the user deletes a file or file version, the item is deleted instantly and cannot be recovered unless you have set up custom backup functionality in Amazon S3.

Note: Even when versioning is enabled, a file or file version gets permanently deleted when the *Instant Permanent Delete* feature is enabled.

Default Owner

With *Instant Permanent Delete* disabled, files and file versions will still exist in Salesforce and Amazon S3 upon deletion. These files and file versions will be marked as deleted within Salesforce. However, the deleted items will be hidden from the users' sight within the CDM components, and standard users will not be able to access them.

This is done by removing existing shares of a record. Since the record's owner can always access it, we switch the record's ownership to another user, *the default owner*.

It is best to change the *default owner* to a user who does not actively work with CDM, like an integration user.

Auto Delete

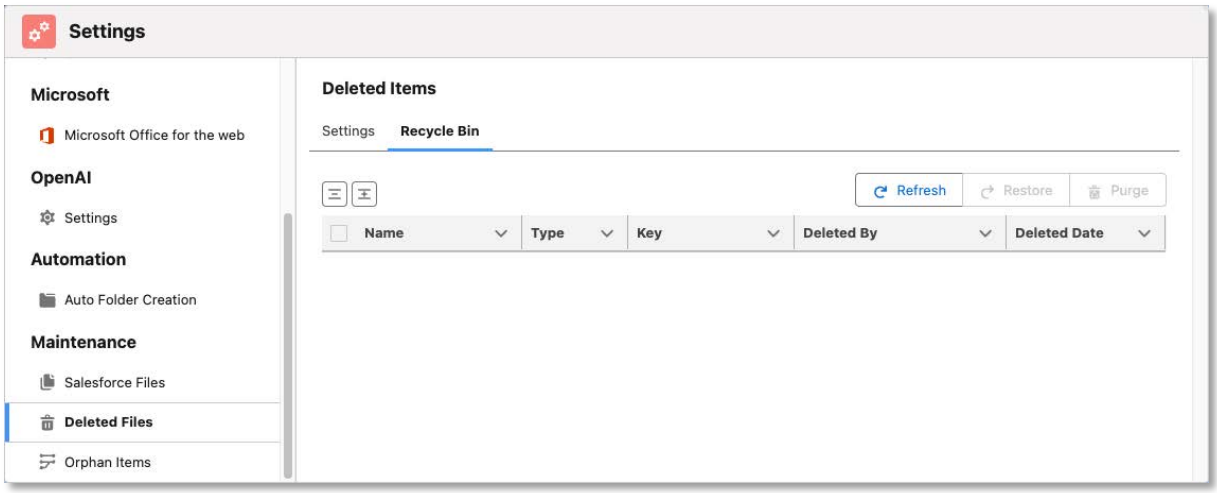
It is also possible to permanently delete files or file versions automatically after a certain period has passed since the item was marked as deleted.

This period can be set to any number of days, months, or years.

Make sure you schedule the *auto delete scheduled job* and choose your preferred start time. This scheduled job checks whether files or file versions marked for deletion longer ago than the set auto deletion period exist and deletes them if so.

Recycle Bin

The Recycle Bin shows all files and file versions marked as deleted. The admin can select one or more files or file versions and either restore or purge them by clicking the respective button.



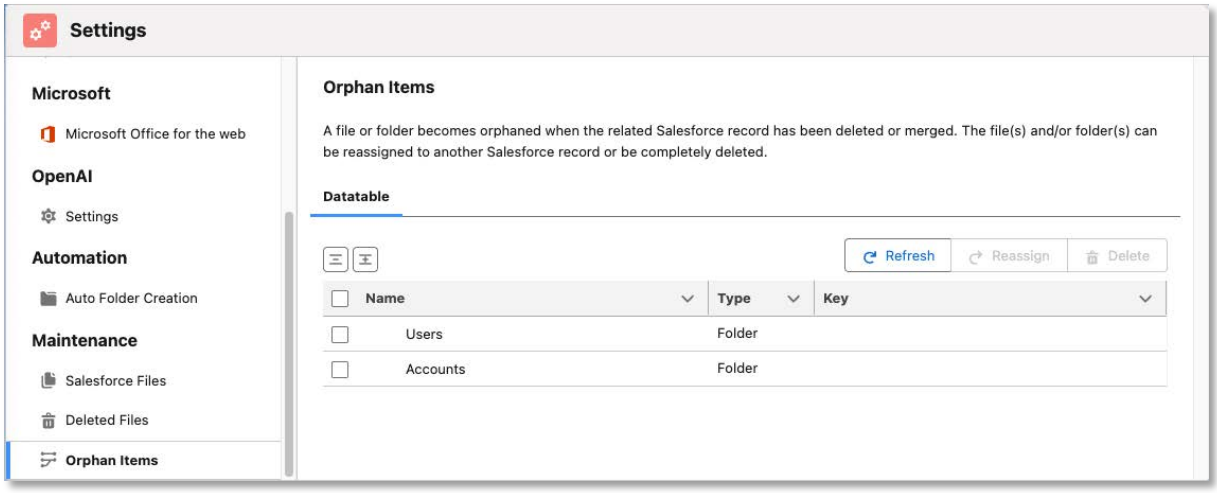
Protection Against Ransomware Attacks

Currently, the best protection against ransomware attacks is to have versioning enabled, and instant permanent delete and auto delete disabled. This means attackers should have admin access to the Salesforce instance before they can cause permanent harm to files.

While we constantly try to make it harder for malicious parties to access or harm your files, please be vigilant and implement your own strategies to further enhance security.

Please share any findings with us if you suspect any vulnerabilities within Salesforce, Amazon S3, and/or CDM.

Orphan Files



Over time, Salesforce records may be deleted or merged, leaving behind files and folders that are no longer associated with their original parent records.

Cartularius automatically identifies these unlinked resources and lists them on the **Orphan Items** page, giving administrators full control over how to manage them.

An **orphan item** is any file or folder in Cartularius that no longer has a valid parent relationship to a Salesforce record.

This typically occurs when:

- A Salesforce record (such as an Account, Opportunity, or custom object) is **deleted**.
- Two Salesforce records are **merged**, and the associated files were linked to the record that no longer exists.

Cartularius does **not** delete orphaned files or folders automatically. Instead, they remain safely stored and are surfaced in the Orphan Items page to allow administrators to review and decide what action to take.

Note: The presence of orphan items does not indicate data corruption. It simply reflects that certain files or folders are no longer tied to an active Salesforce record.

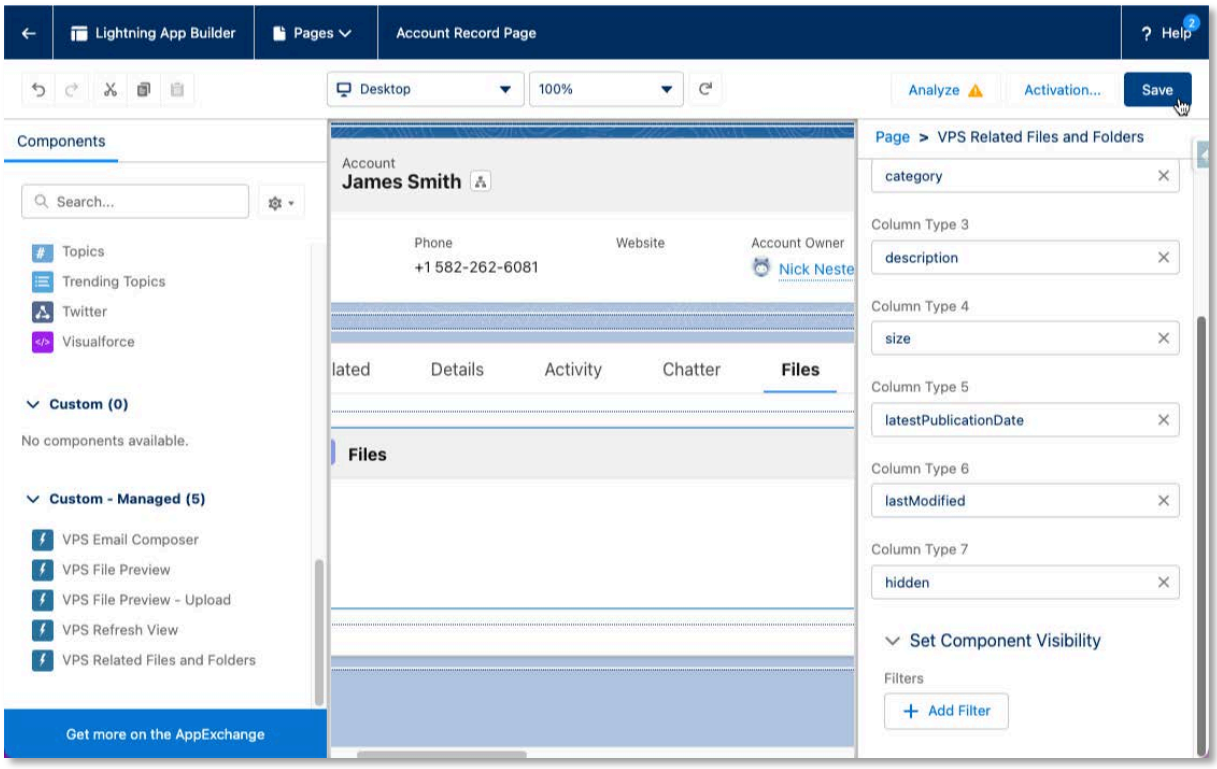
Chapter 8: Add components to Lightning Record Pages

CDM Related Files and Folders

When *Auto Folder Creation* is enabled and configured correctly, a base folder is generated for each created record, and a folder link connects that base folder to the Salesforce record. The base folder can contain multiple subfolders and/or files.

Follow the instructions below to add the *CDM Related Files and Folders* component to *Lightning Record Pages* and show the files and folders related to the record:

1. From Setup, open the *Object Manager*.
2. Select the Object where the component should be placed.
3. Select *Lightning Record Pages*.
4. Open the Record Page you want to edit or create a new one.
5. Click **Edit** to open the Lightning App Builder.
6. Add the *CDM Related Files and Folders* component to the desired location from the Custom – Managed section.
7. Click **Save**.



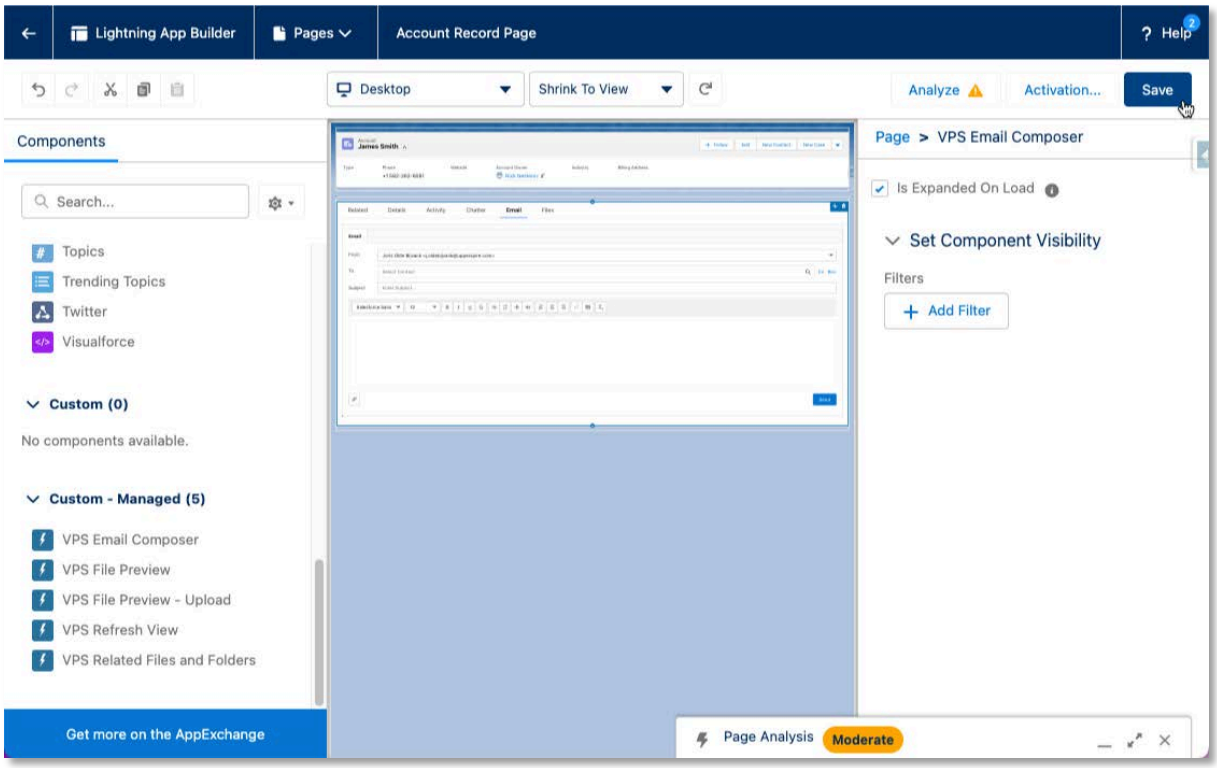
Component Properties

Property	Description
Height	Sets the height of component. It is possible to write the height as a CSS function like *calc(100vh – 428px)* or a static height like *400px*.
Columns	With the column configuration it is possible to change the order and the visibility of columns by clicking the cross in the dropdown.

CDM Email Composer

Follow the instructions below to add the *CDM Email Composer* component to *Lightning Record Pages* and show the files and folders related to the record:

1. From Setup, open the *Object Manager*.
2. Select the Object where the component should be placed.
3. Select *Lightning Record Pages*.
4. Open the Record Page you want to edit or create a new one.
5. Click **Edit** to open the Lightning App Builder.
6. Add the *CDM Email Composer* component from the *Custom – Managed* section into the desired location.
7. Click **Save**.



Component Properties

Property	Description
Is Expanded On Load	If enabled, the component will be shown in its expanded state when shown to the user. If disabled, only a collapsed version of the component will be shown that can be expanded when clicking on it.

Chapter 9: Auto Folder Creation

Earlier in this guide, we mentioned the aspects of Auto Folder Creation concerning the setup page of CDM.

Auto Folder Creation (AFC) is one of CDM's main features that can help structure files for any organization. For this reason, we decided to include this as a separate chapter in this getting-started guide.

SObject Configuration

On the setup page of CDM, you can enable/disable AFC for the following standard objects:

- Account
- Asset
- Campaign
- Case
- CollaborationGroup
- Contact
- Contract
- Event
- Lead
- Opportunity
- Product2
- Solution
- Task
- User

For each of the standard objects listed above, there is a trigger handler that starts the AFC process when the specific object is enabled in the setup.

When a record is created or updated, the trigger handler will execute the code to create or update the folder hierarchy configured within the corresponding *AFC Objects*, *AFC Folders,* and *AFC Folder File Categories*.

To have the same functionality for a custom object, the following steps must be taken.

- Add the custom object to the *CDM SObjects* Global Value Set
- Create a trigger for the custom object

Add Custom Objects to CDM SObjects (Global Value Set)

Take the following steps to add one or more Custom Objects to the *CDM SObjects* Global Value Set:

1. From Setup, enter *Picklist Value Sets* in the Quick Find box, then select **Picklist Value Sets**.

2. Open the *CDM SObjects* Global Value Set by clicking on its label.

3. Click **New**.

4. Enter the name of one or more custom objects (including the __c postfix).

5. Click **Save**.

After the Custom Objects have been added to the CDM SObjects Global Value Set, they are available when creating the AFC Objects and AFC Folders configuration.

Create Triggers for Custom Objects

The following example code shows how to enable the AFC feature for a custom object.

```
trigger AccountTrigger on Account (after insert, after update, after delete) {

    // After inserting the new record, create the folders according to the configuration.
    if (Trigger.isInsert) {
        try {
            GlobalDocumentManager.autoFolderCreation(Trigger.new);
        } catch (Exception e) {
            for (SObject record : Trigger.new) {
                record.addError('An error occurred during folder creation: ' +
e.getMessage());
            }
        }
    }

    // When the name of a record is updated, all corresponding folder resource path labels
should be updated accordingly.
    if (Trigger.isUpdate) {
        try {
            GlobalDocumentManager.renameRecords(Trigger.new, Trigger.oldMap);
        } catch (Exception e) {
            for (SObject record : Trigger.new) {
                record.addError('An error occurred while renaming folders for ' +
record.getSObjectType() + ': ' + e.getMessage());
            }
        }
    }


    // When a record is deleted, some maintenance needs to be performed.
    if (Trigger.isDelete) {
        try {
            GlobalDocumentManager.sfRecordDeletion(Trigger.old);
        } catch (Exception e) {
            for (SObject record : Trigger.old) {
                record.addError('An error occurred during the Salesforce record deletion
maintenance of Cartularius: ' + e.getMessage());
            }
        }
    }
}
```

Replace [TriggerName] and [CustomObject] with your values, and feel free to add any modifications to the code.

AFC Objects

Record Creation

When a new record is inserted, the AFC process will check the AFC Object configuration based on the given SObject and Record Type combination, and it will create a home folder.

Following is a list of CDM AFC Object fields:

Field Label	Field Name	Description
Active	upperspire__Active__c	If TRUE, AFC will create a home folder for the inserted record in the base folder.
Allow Uploads in Record Home	upperspire__Allow_Uploads_In_Record_Home__c	If TRUE, it is allowed to upload files in the home folder of the record.
Base Folder	upperspire__Base_Folder__c	Sets the base folder for the SObject, Record Type combination.
Folder	upperspire__Folder__c	This is a lookup field to the created base folder
Folder Creation Restriction	upperspire__Folder_Creation_Restriction__c	If FALSE, users with the permission set *CDM_User* are allowed to create new folders in the home folder of the record.
Key Field (deprecated)	upperspire__Key_Field__c (deprecated)	~~The Key Field is API name of the field of the SObject that is used to name the home folder.~~
Record Type	upperspire__RecordType__c	This is an optional field. The combination of an SObject and a Record Type results in the creation of a home folder based on the chosen Base Folder and Key Field for that combination. This way, files and folders related to an SObject using a different record type can be stored in a completely different location.
SObject	upperspire__SObject__c	Selects the SObject for which this CDM AFC Object record contains the configuration.

In Amazon S3, the Resource Path is used to uniquely identify the location of a file (or object, as it is called in AWS). However, Amazon S3 does not use folders to store data. When browsing through the Bucket within the AWS Console, it appears to have a folder structure, but it is actually a list of files separated by slashes (/) acquired from all Resource Paths in the Bucket.

CDM uses a different strategy. All files are related to a folder via a lookup relation. First, we create the folder, and then we can use that folder to store files. This way, we can make a folder hierarchy using a predefined structure.

When AFC is triggered because a record is inserted, the Resource Path to the new home folder will be created in the following format:

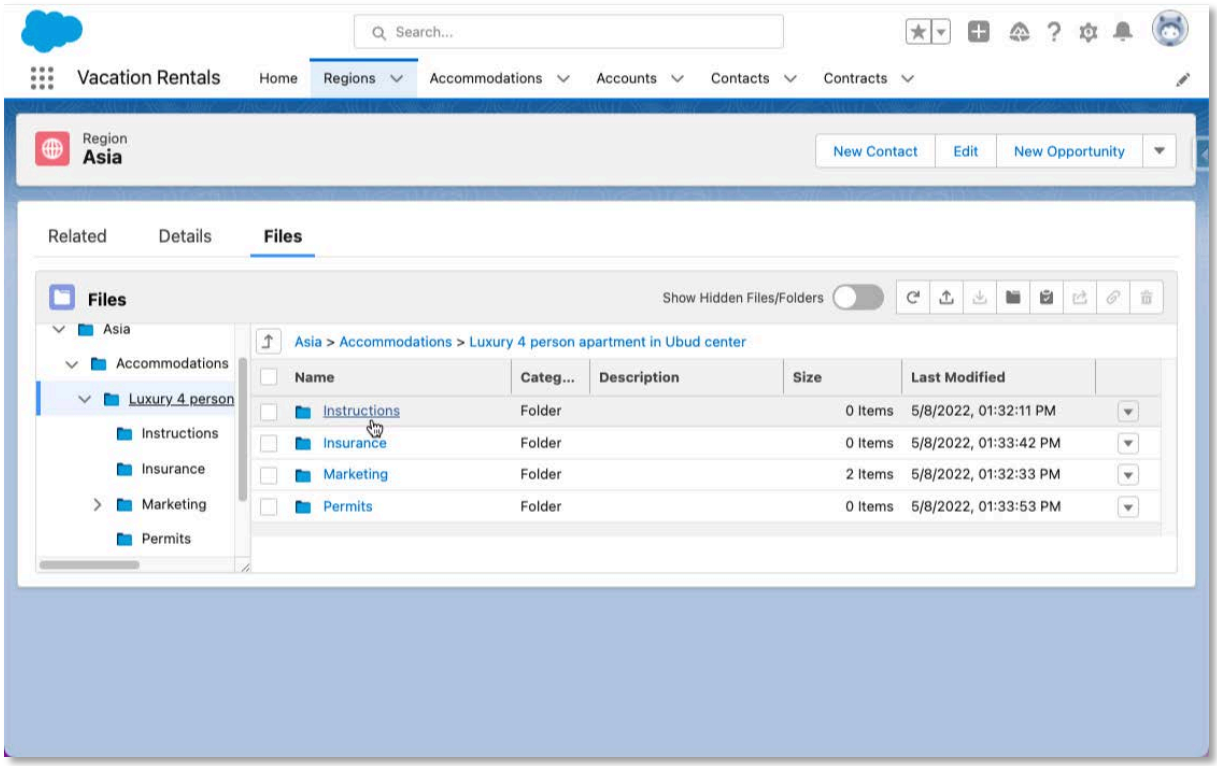
[BaseFolderId]/[RecordId]

If the folder does not exist, a folder and a Folder Link are created. If it already exists, only a Folder Link is created. The Folder Link links the folder with the record and is used in the Files and Folders component on the record page to show the contents of the home folder.

AFC Folders

Record Creation

When a new record is inserted in Salesforce, the AFC feature creates a home folder, as mentioned in the previous section. After creating the home folder, the AFC feature checks the AFC Folder configuration, generates a folder hierarchy based on this configuration, and adds it to the home folder.



Following is a list of AFC Folder fields:

Field Label	Field Name	Description
Composed Path (deprecated)	upperspire__Composed_Path__c (deprecated)	~~The Composed Path is a visual help which shows an example of how the generated key will look like for this CDM AFC Folder.~~ ~~[Account Base Folder]/[Account Key Field]/[Folder Name]~~
File Category Restriction	upperspire__File_Category_Restriction__c	If TRUE, it is only allowed to upload, copy, or move files into this folder with a File Category that matches the CDM Folder File Categories related to this folder.
Folder Creation Restriction	upperspire__Folder_Creation_Restriction__c	If FALSE, users with the permission set CDM_User are allowed to create new folders in this folder.
Folder Name	upperspire__Folder_Name__c	This is the name of the folder.
Import Id	upperspire__Import_Id__c	The Import Id is used to help with the import of the AFC configuration.
Indirect Related Folder Parent Object	upperspire__Indirect_Related_Folder_Parent_Object__c	If omitted, the folder is a Direct Folder. If an SObject is chosen, the folder is an Indirect Related Folder. More on Indirect Related Folders in the coming sections of this chapter.
Parent AFC Folder	upperspire__Parent_AFC_Folder__c	This field defines the hierarchical structure of folders by referencing the parent folder of the current AFC Folder. It is managed automatically by Cartularius and should not be edited manually.
Parent Folder (deprecated)	upperspire__Parent_Folder__c (deprecated)	~~This is a slash (/) separated list of folders that define the hierarchy of the folders.~~ ~~[Account Base Folder]/[Account Key Field]/Grandparent/Parent/[Folder Name]~~
Record Type	upperspire__RecordType__c	Record Type is an optional field. The combination of an SObject and a Record Type. Using the Record Type, files and folders related to an SObject can be stored in a completely different location then other Record Types of the same SObject.
SObject	upperspire__SObject__c	Selects the SObject for which this AFC Folder record contains the configuration.

AFC Folder Changes

It is important to define a folder hierarchy that matches the requirements of your organization. Even if this folder hierarchy is defined very well there is a good chance that the requirements will change over time.

The following sections show how the AFC feature handles these changes.

Insert a new AFC Folder

When a new AFC Folder is created, the folder will be added to the hierarchy for all new records matching the SObject and Record Type.

In addition to this, AFC will also automatically add the newly created folder to the hierarchy of all existing records by executing Batch Apex.

Update an existing AFC Folder

It is allowed to change the following fields for an existing AFC Folder:

- Folder Name
- Parent Folder
- Folder Creation Restriction
- File Category Restriction

Whenever one of the above fields has been changed, AFC will update all existing folders related to this AFC Folder. If the Folder Name or the Parent Folder is changed, all existing folders, including any related child folders, will be updated.

Delete an existing AFC Folder

When an existing AFC Folder is deleted, nothing changes for the existing folder hierarchy automatically. This is done because we do not know what needs to happen with the child folders and files related to that folder. Deletion of existing folders should be done manually.

For newly created records, the deleted AFC Folder will not be added to its folder hierarchy.

AFC Folder File Categories

Record Creation

AFC's final step when a new record is created is to add Folder File Categories to the generated folders according to the AFC Folder File Category configuration.

Following is a list of AFC Folder File Category fields:

Field Label	Field Name	Description
AFC Folder	upperspire__AFC_Folder__c	Lookup relation to the AFC Folder.
AFC Folder Name	upperspire__AFC_Folder_Name__c	Formula that shows the name of the selected AFC Folder which is displayed in the AFC Folder File Category List View.
File Category	upperspire__upperspire__File_Category__c	Picklist with File Categories (these File Categories are managed from the CDM File Categories Global Value Set).

CDM File Categories Global Value Set

Before selecting a File Category in an AFC Folder, you must add it to the CDM File Categories Global Value Set. To do this, take the following steps:

1. From Setup, enter *Picklist Value Sets* in the Quick Find box, then select **Picklist Value Sets**.
2. Open the *CDM File Categories* Global Value Set by clicking on its label.
3. Click **New**.
4. Enter one or more File Categories into the text field.

Click **Save**.

File Category Selection per SObject

A complete file repository often consists of dozens of file categories. Scrolling through a list of all file categories when uploading a new file can be very cumbersome. For this situation, we created the file category selection per SObject. By creating a dependency between the SObject type (which is home to the file) and the file category picklist, we filter out all irrelevant file categories.

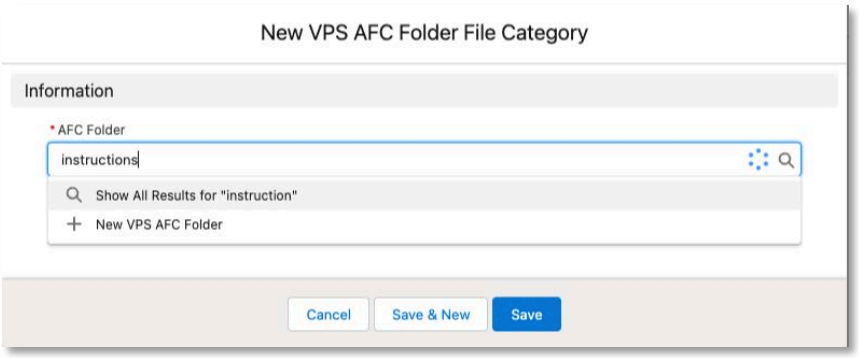
Follow the instructions below to create the SObject -> File Category dependency:

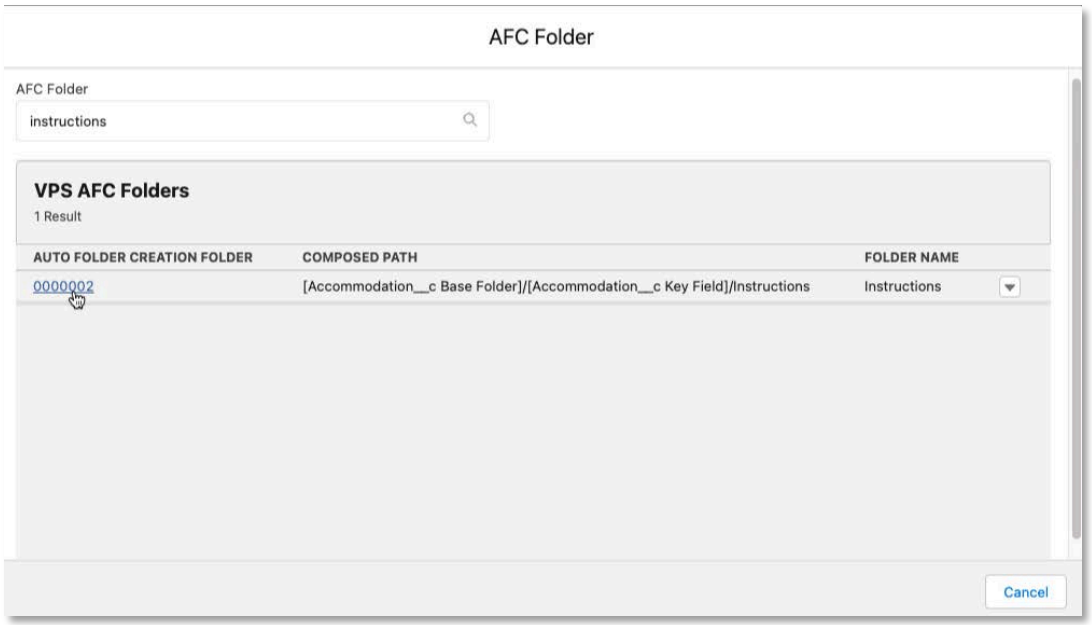
1. From Setup, open the *Object Manager*.
2. Select the *CDM File* Object.
3. Select *Fields & Relationships*.
4. Click **Field Dependencies**.
5. Click **New.**
6. Select *SObject* as the Controlling Field and *File Category* as the Dependent Field.
7. Click **Continue**.
8. Select one or more File Categories per SObject and click **Include Values.**
9. Repeat this until you've completed the setup.
10. Click **Save**.

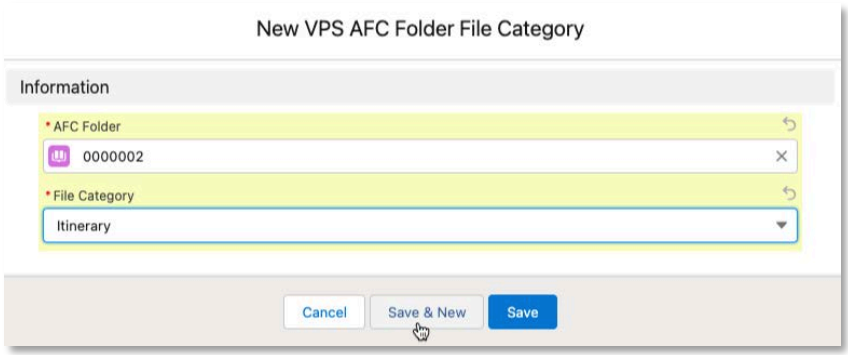
AFC Folder File Category CRUD Actions

Insert a new AFC Folder File Category

When a new AFC Folder File Category is inserted, AFC checks all folders related to the AFC Folder and adds the Folder File Category to those folders.







Update an existing AFC Folder File Category

When an existing AFC Folder File Category is created, all existing Folder File Categories matching the old AFC Folder File Category values are deleted. Simultaneously, new Folder File Categories are created to match the new values of the AFC Folder File Category.

Delete an existing AFC Folder File Category

When an existing AFC Folder File Category is deleted, all existing Folder File Categories related to this AFC Folder File Category are also deleted.

AFC Folder Translations

The **AFC_Folder_Translation__c** object is used to manually define translated names for folders managed by Cartularius. Each translation record is linked to a specific **AFC_Folder__c** via a lookup field and includes a target language (**Language__c**) and the translated name (**Translation__c**).

Admins can create multiple translation records per folder to support multilingual users. These records are automatically converted into **Folder_Translation__c** records, which Cartularius uses to display localized folder names in the user interface based on the user's language settings.

To manage folder translations:

1. Create an **AFC_Folder_Translation__c** record.
2. Link it to the target **AFC_Folder__c**.
3. Select the appropriate language code in **Language__c**.
4. Enter the translated name in **Translation__c**.

Folder names will appear translated for users whose language setting matches a defined translation.

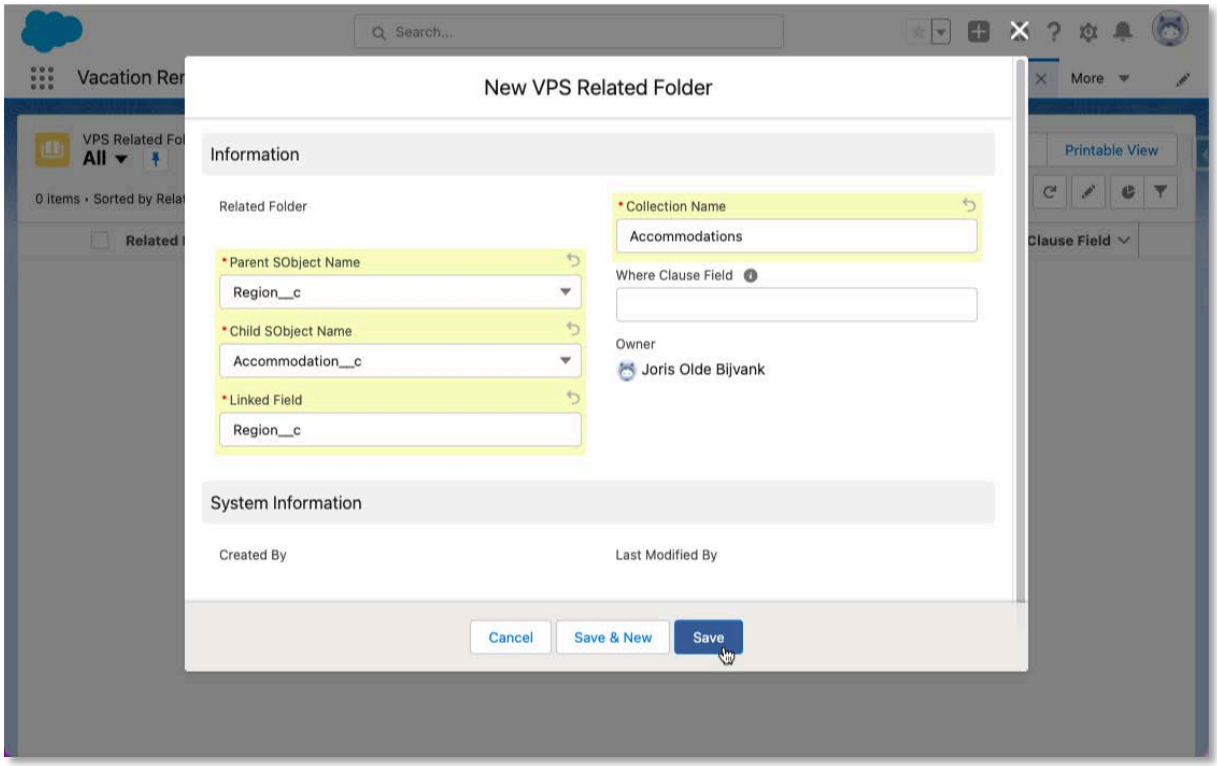
Following is a list of AFC Folder Translation fields:

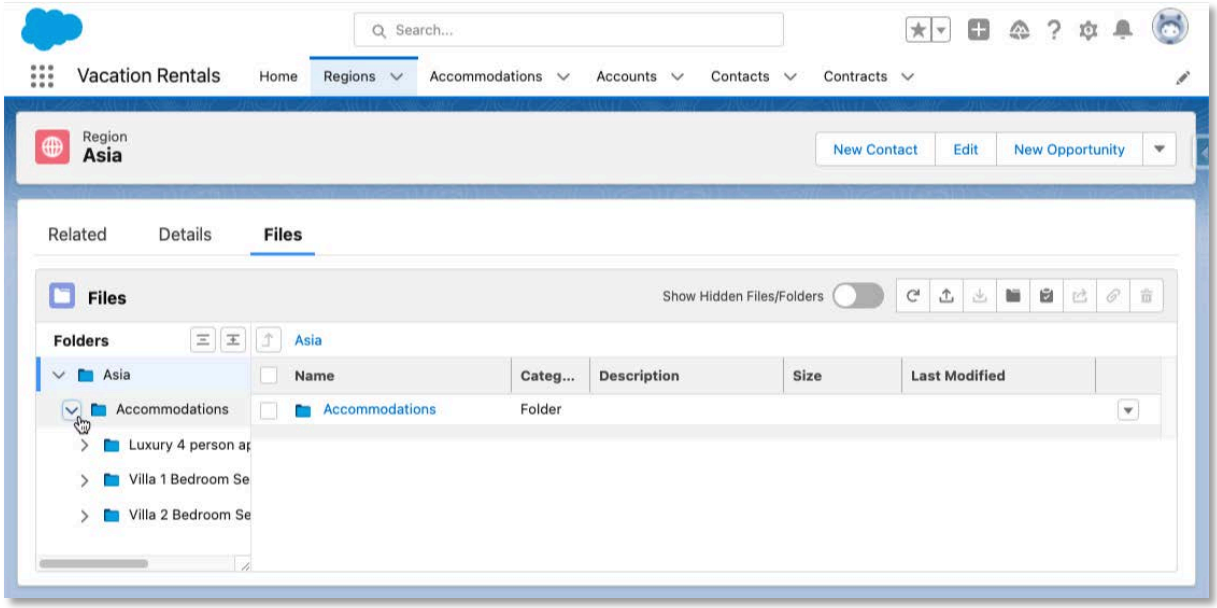
Field Label	Field Name	Description
AFC Folder	upperspire__AFC_Folder__c	Lookup relation to the AFC Folder.
Language	upperspire__Language__c	Picklist with language codes to choose from
Translation	upperspire__Translation__c	Translated folder name

Related Folders

A Related Folder is a folder that is linked to another folder based on a direct relationship between SObjects.

An example would be the relationship between an Account and a Contact via the AccountId field. If configured as a Related Folder, a collection of related Contact folders will be shown within the Files and Folders component on the Account record.





Following is a list of Related Folder fields:

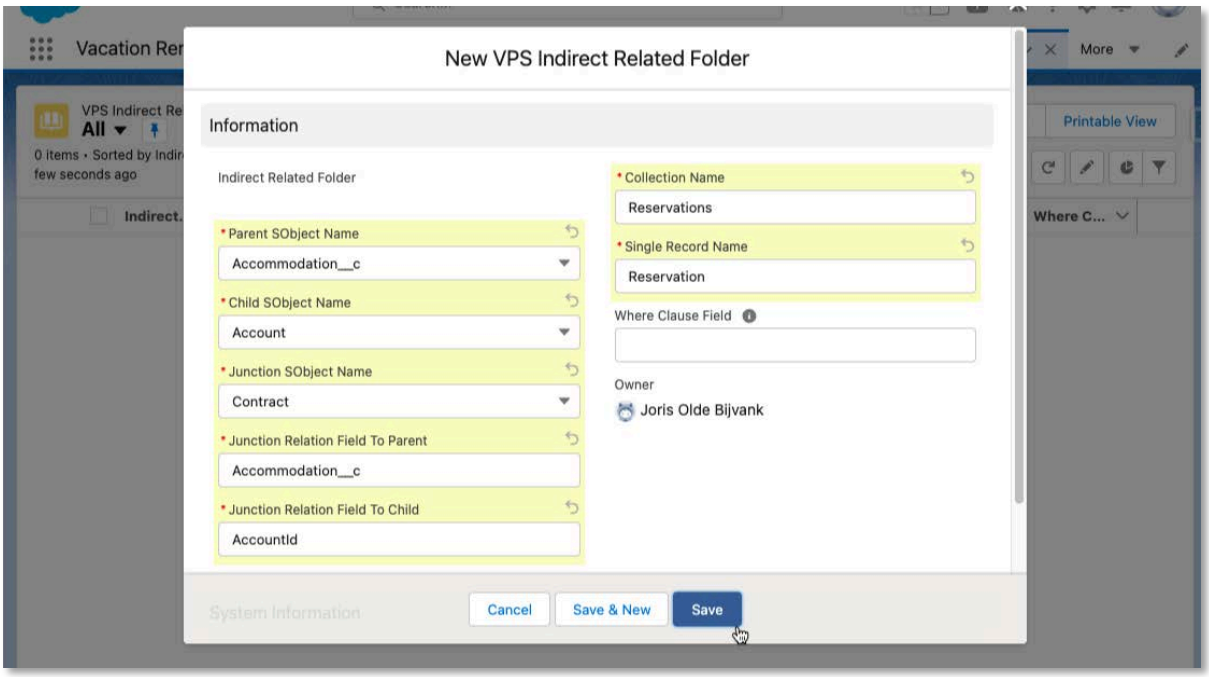
Field Label	Field Name	Description
Child SObject Name	upperspire__Child_SObject_Name__c	Name of the SObject of which the records will be displayed as a collection on the parent object's Record Page.
Collection Name	upperspire__Collection_Name__c	Name of the collection displayed on the parent object's Record Page.
Linked Field	upperspire__Linked_Field__c	Name of the field on the child object linking to the parent object.
Parent SObject Name	upperspire__Parent_SObject_Name__c	Name of the parent SObject.
Where Clause Field	upperspire__Where_Clause_Field__c	Optional field on the child object that returns a Boolean value indicating to show the record within the collection or not.

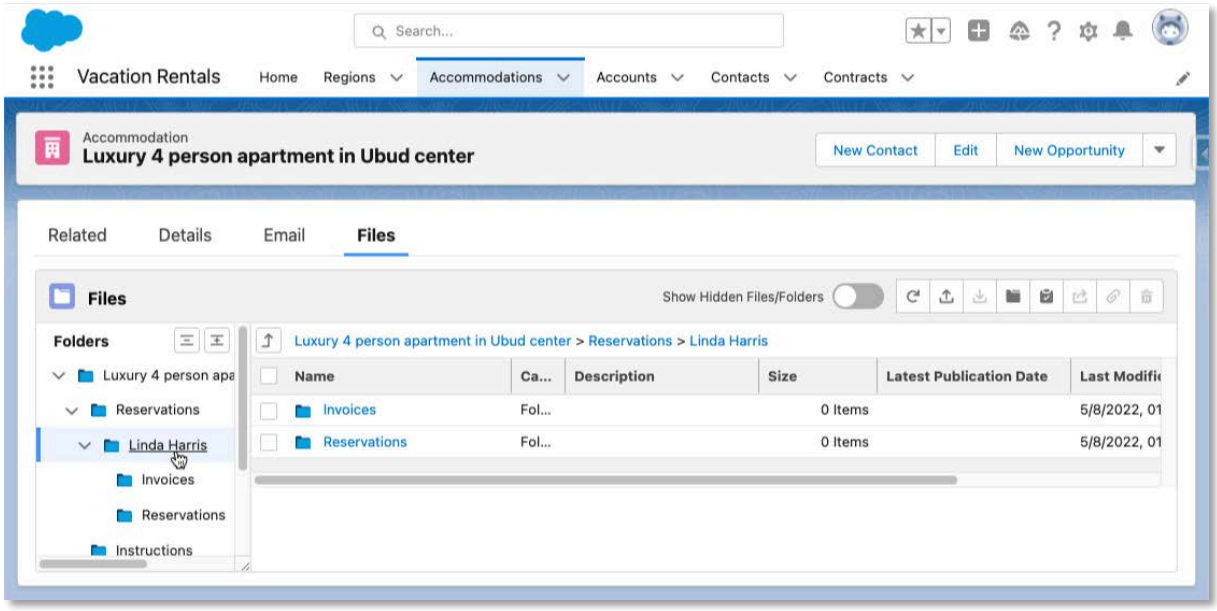
Indirect Related Folders

Note: The Indirect Related Folders feature is available only in the **Cartularius Enterprise Edition**. If you are using the **Core Edition** or **Professional Edition** and would like to access this feature, please contact us to discuss an upgrade.

An Indirect Related Folder is a folder linked to another folder based on an indirect relationship between SObjects. An indirect relationship involves three objects: a parent, a child object, and a junction object that connects the parent and the child object.

An example of this would be the relationship between an Account and a Contact, with the Contract serving as a junction. If configured as an Indirect Related Folder, a collection of related Contact folders will be shown within the Files and Folders component on the Account record. Additionally, the Files and Folders component on the Contract will display the folders of the related Contact record.




Search...
Vacation Rentals
Home
Regions
Accommodations
Accounts
Contacts
Contracts
Accommodation
Luxury 4 person apartment in Ubud center
New Contact
Edit
New Opportunity
Related
Details
Email
Files
Files
Show Hidden Files/Folders
Folders
Luxury 4 person apa
Reservations
Linda Harris
Invoices
Reservations
Instructions
Luxury 4 person apartment in Ubud center > Reservations > Linda Harris
Name
Ca...
Description
Size
Latest Publication Date
Last Modifi
Invoices
Fol...
0 Items
5/8/2022, 01
Reservations
Fol...
0 Items
5/8/2022, 01

Following is a list of Indirect Related Folder fields:

Field Label	Field Name	Description
Child SObject Name	upperspire__Child_SObject_Name__c	Name of the SObject of which the records will be displayed as a collection on the parent object's Record Page.
Collection Name	upperspire__Collection_Name__c	Name of the collection displayed on the parent object's Record Page.
Junction Relation Field To Child	upperspire__Junction_Relation_Field_To_Child__c	Name of the field on the junction object that creates the relation with the child object.
Junction Relation Field To Parent	upperspire__Junction_Relation_Field_To_Parent__c	Name of the field on the junction object that creates the relation with the parent object.
Junction SObject Name	upperspire__Junction_SObject_Name__c	Name of the SObject that creates the connection between the parent and the child object.
Parent SObject Name	upperspire__Parent_SObject_Name__c	Name of the parent SObject.
Single Record Name	upperspire__Single_Record_Name__c	Name of the container that is displayed in the Files and Folders component on the junction object's Record Page which shows the folders of the child object.
Where Clause Field	upperspire__Where_Clause_Field__c	Optional field on the child object that returns a Boolean value indicating to show the record within the collection or not.

Chapter 10: External Links

External Links securely share files with external parties. In this chapter, we show you how to set up your Salesforce Org to accommodate this feature.

First, we need to enable Digital Experiences, create, and configure a Digital Experience Site to host the CDM External Link component, add Guest User Sharing Rules to allow the guest users to access certain CDM Files, and finally create an Email Template for emails that will be sent to the external party.

Enable Digital Experiences

Perform the following steps to set up a Digital Experience Site:

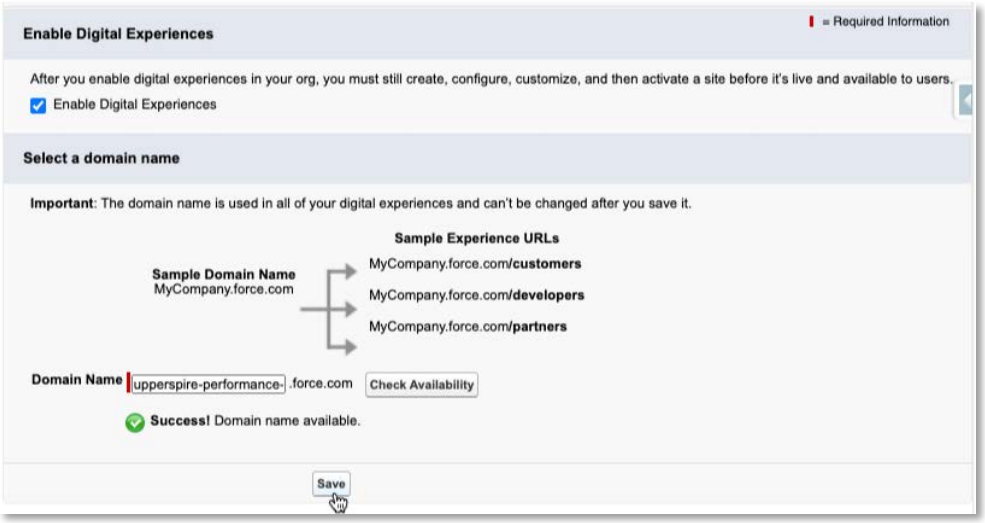
1. From Setup, enter *Digital Experiences* in the Quick Find box, then select **Settings**.

2. If Digital Experiences are enabled already, skip to the next section; otherwise, click **Enable Digital Experiences**.

3. Select a domain name.

Note: The domain name is used in all your digital experiences and cannot be changed after you save it. The chosen domain name will be part of the public URL. Make sure to select a sensible and meaningful name.

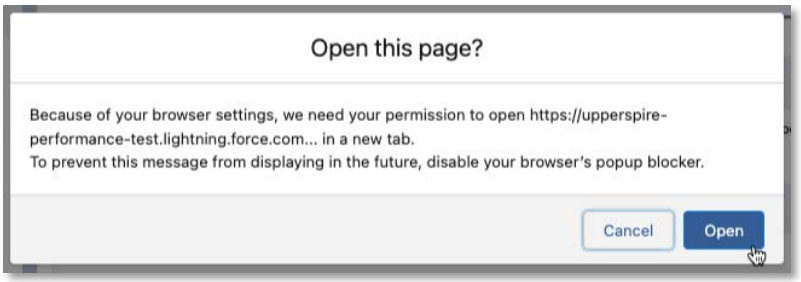
4. Click **Check Availability** to check whether the domain name is available.



5. Click **Save**.

6. Click **OK** in the confirmation window to enable digital experiences and register the selected domain name.

7. Depending on your browser settings, you may be asked for permission to open the digital experience in a new tab. Click **Open** to open the page.



Creating the Digital Experience Site

Follow the instructions below to set up a Digital Experience Site:

1. From Setup, enter *Digital Experiences* in the Quick Find box, then select **All Sites**.

2. Click **New**.

3. Select the **Build Your Own (LWR)** experience.

Note: LWR stands for Lightning Web Runtime and allows us to add Lightning Web Components to the site.

4. Click **Get Started**.

5. Choose a recognizable name for the Digital Experience Site, e.g., **Cartularius**.

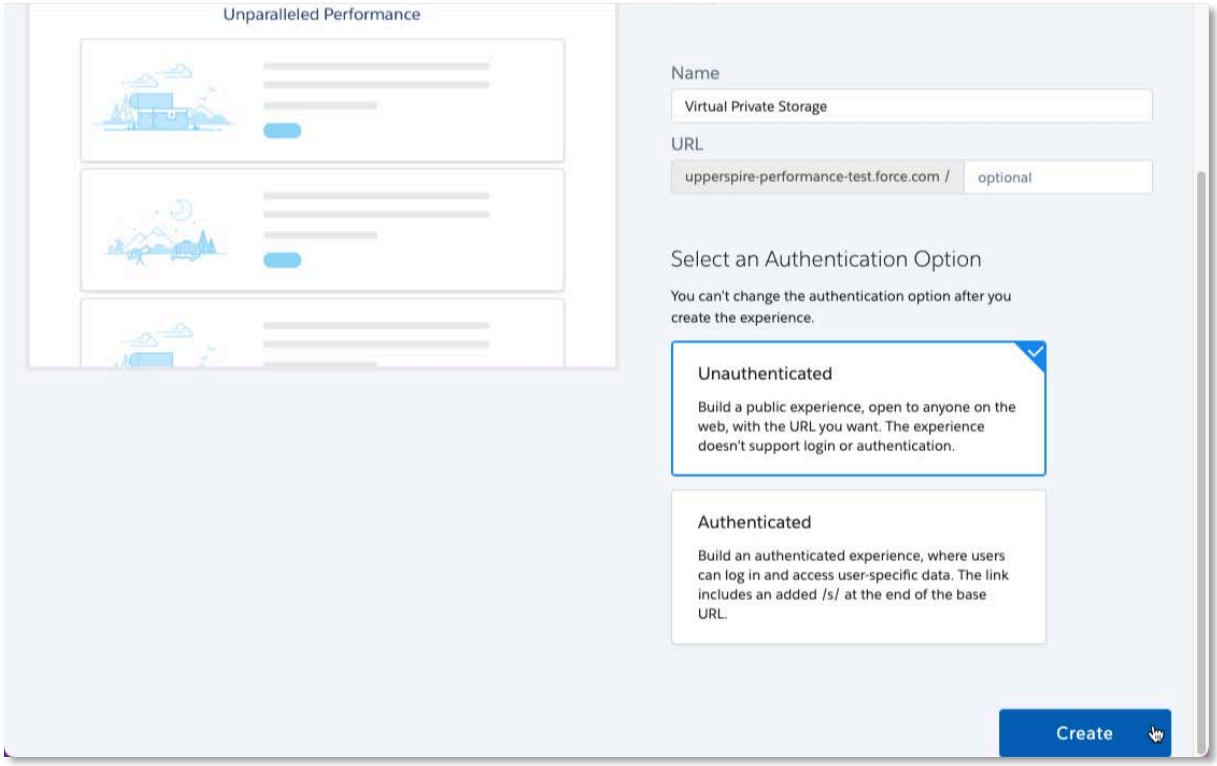
Note: This name is only for internal purposes and can be changed later.

6. Optionally, enter a subdirectory name.

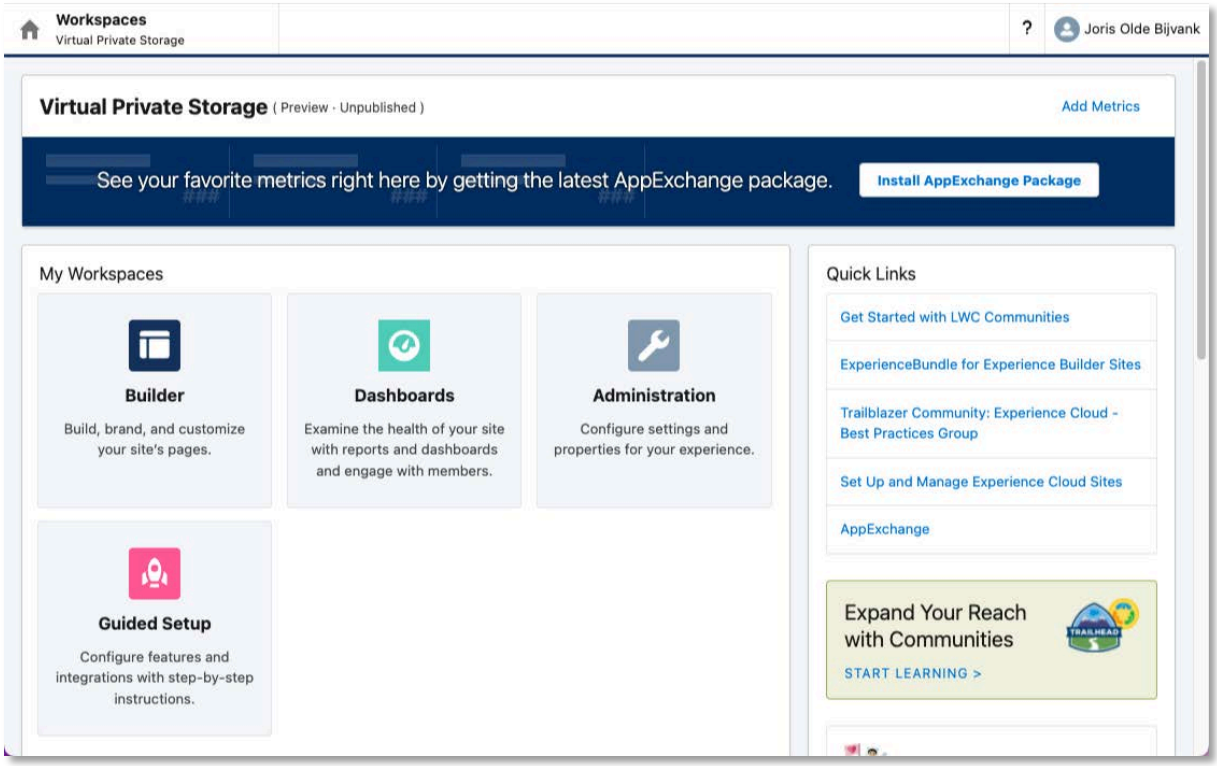
Note: This subdirectory name is mandatory if you have multiple active Digital Experience Site. The base URL for the experience site is formatted in the following format: *https://upperspire.force.com/[subdirectory]*

7. Click **Unauthenticated**.

8. Click **Create**.



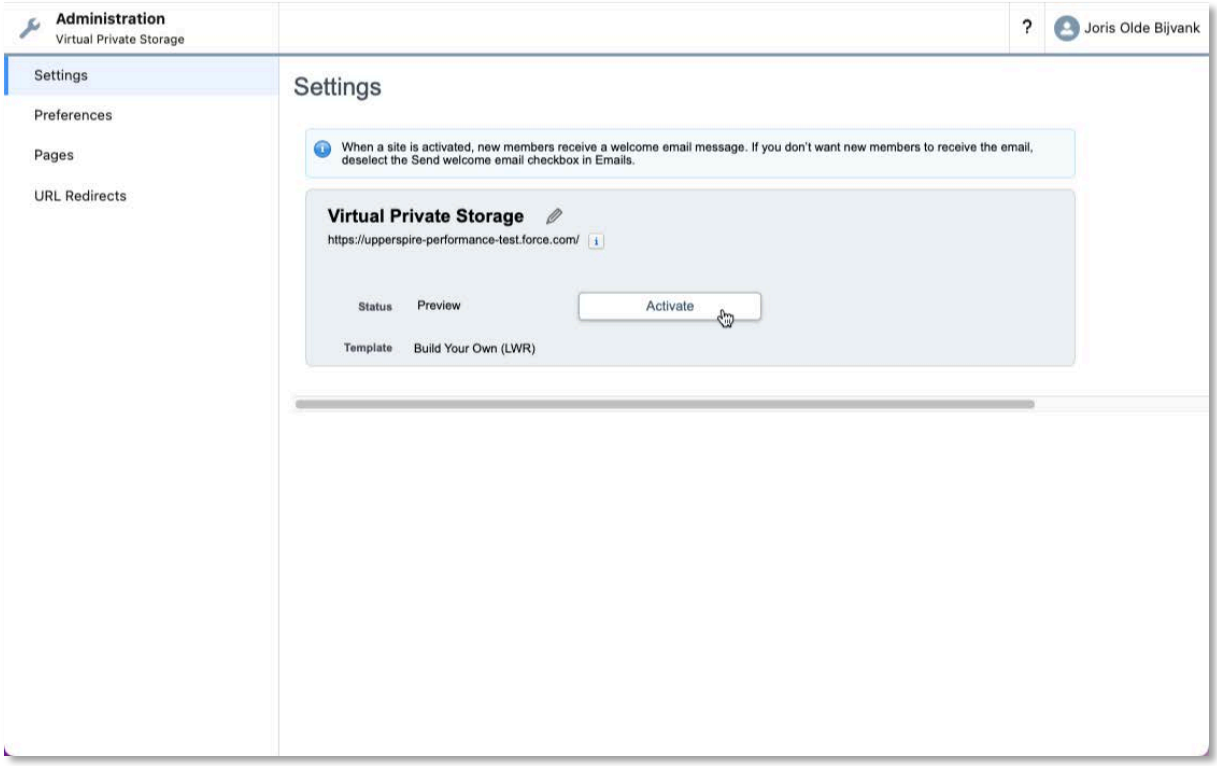
9. The Digital Experience Site has been created and is now ready to be configured.



Setting up the Digital Experience Site

Perform the following steps to set up the Digital Experience Site:

1. From Setup, enter *Digital Experiences* in the Quick Find box, then select **All Sites**.
2. Click on the **Workspaces** action of the Digital Experience that was created for Cartularius.
3. Go to the Administration panel by clicking **Administration** in the *My Workspaces* section.
4. Click **Activate** to activate the Digital Experience.

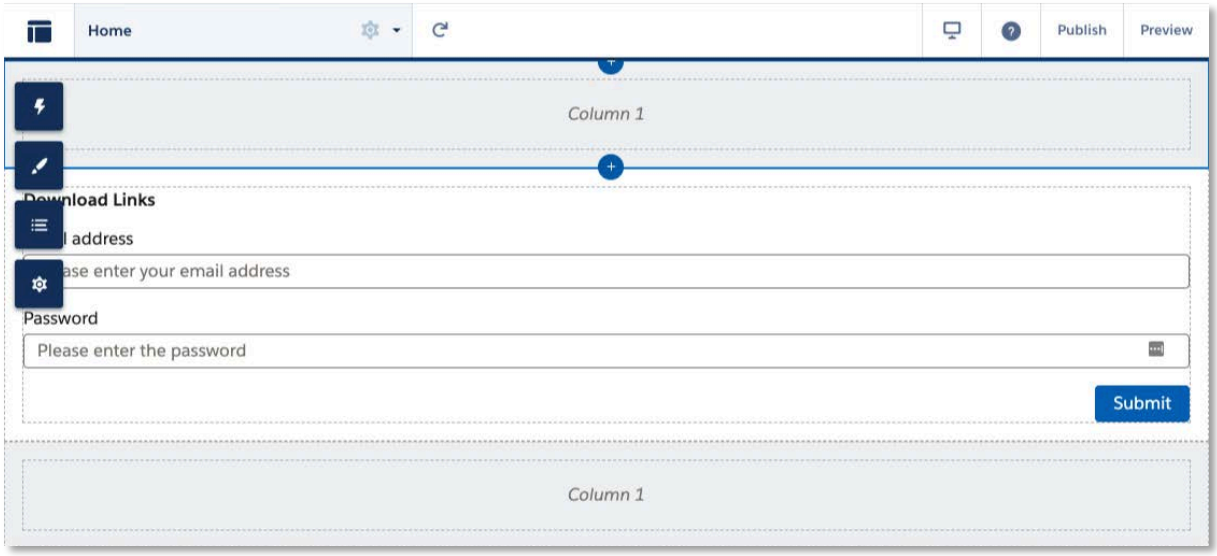


5. Click **OK** to confirm the activation of the Digital Experience.

Add the CDM External Link component to the homepage of the Digital Experience Site

Follow the instructions below to add the *CDM External Link* component to the homepage of the Digital Experience Site:

1. From Setup, enter *Digital Experiences* in the Quick Find box, then select **All Sites**.
2. Click on the **Builder** action of the Digital Experience that was created for Cartularius.
3. Click the cross in the top-right corner of the HTML Editor component that has been added to the page by default to delete it.
4. Click **Delete**.
5. Open the *Component* menu by clicking the **Lightning Bolt** icon.
6. Drag-and-drop the *CDM External Link* component into the middle section.
7. (Optional) Apply your company's branding to the homepage.



Note: In the section *Set up and enable External Links* we will publish the site, but first we need to assign the *CDM Guest User* permission set to the *Guest User* and create *Guest User Sharing Rules*.

Assign the CDM Guest User permission set to the Guest User

By default, guest users cannot access any data in the Salesforce environment without explicit permissions.

The *CDM Guest User* permission set, in combination with specific sharing rules, will provide the *Guest User* with access to CDM Files.

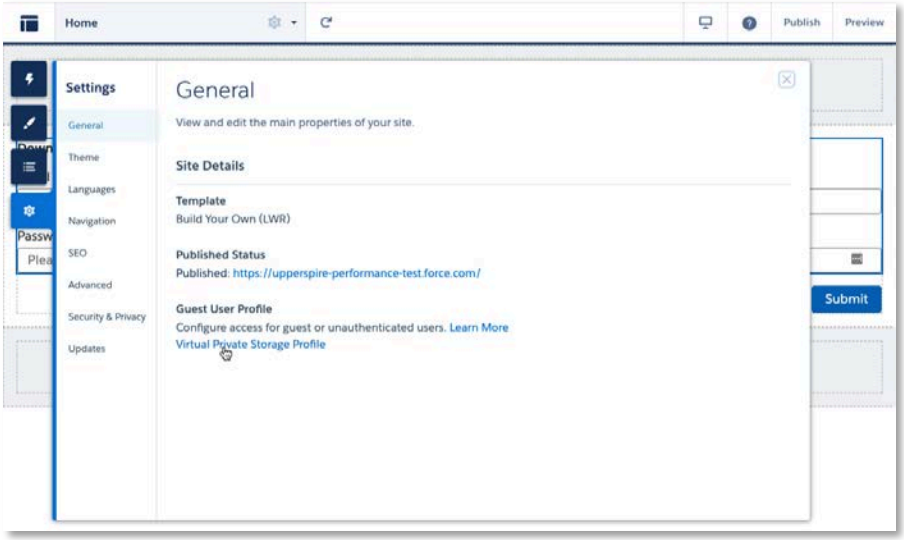
Perform the following instructions to add the *CDM Guest User* permission set to the *Guest User*:

1. From Setup, enter *Digital Experiences* in the Quick Find box, then select **All Sites**.

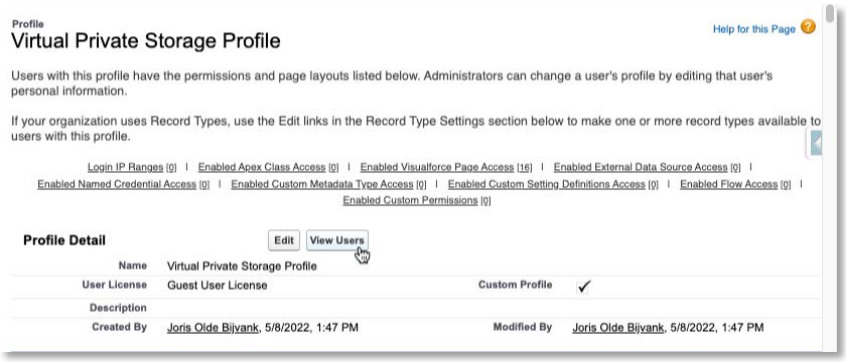
2. Click on the **Builder** action of the Digital Experience that was created for Cartularius.

3. Open the *Settings* by clicking on the **Gear** icon.

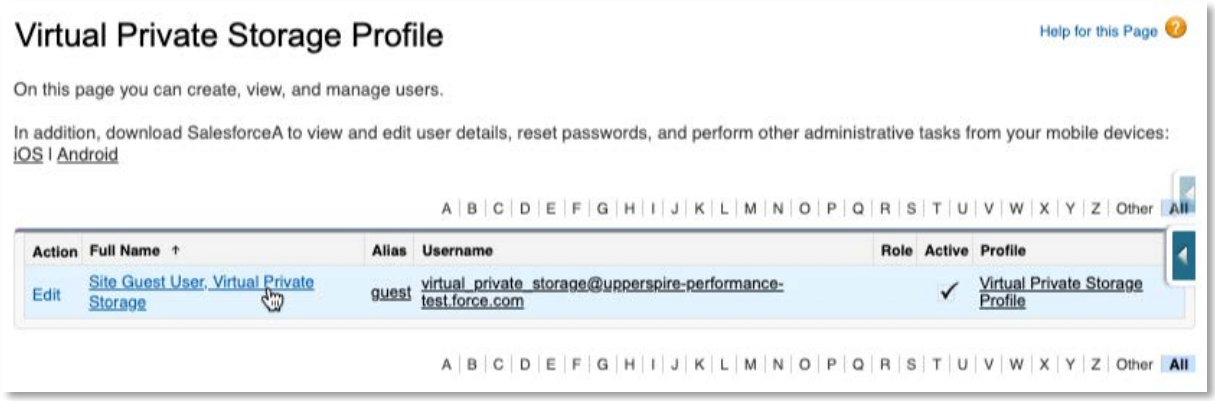
4. Open the profile by clicking its name within the *Guest User Profile* section.



5. Click **View Users**.

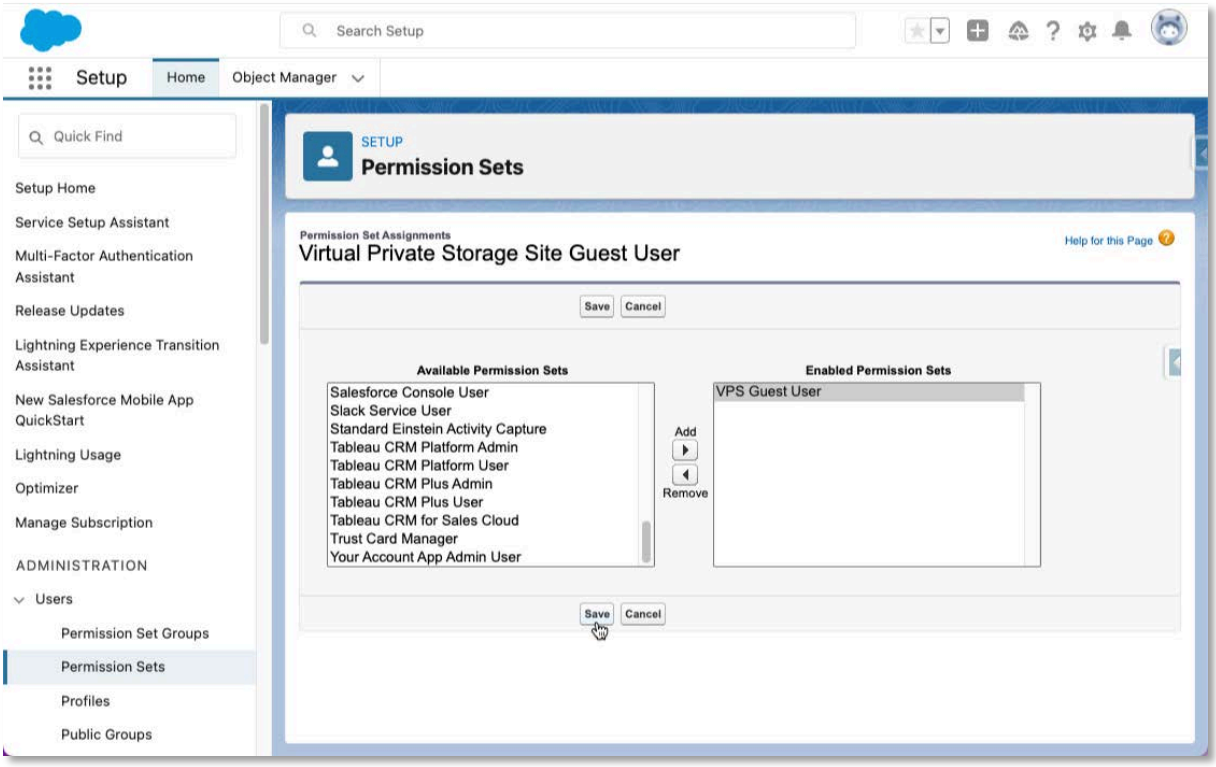


6. Open the *Site Guest User* page by clicking its name.



7. Click the **Edit Assignments** button within the *Permission Set Assignments* section.

8. Select *CDM Guest User* and click the **Add** button to add it to the *Enabled Permission Sets* list.



9. Click **Save**.

Guest User Sharing Rules

The *Organization-Wide Defaults* for internal and external access to CDM files are set to private. For internal access, a process is active to automatically create sharing rules for CDM Folders, files, and file Versions based on the settings made in CDM.

Explicit sharing rules must be set for the Digital Experience Site Guest User to share CDM files with external parties.

Follow the instructions below to set up these *Guest User Sharing Rules*:

1. From Setup, enter *Sharing Settings* in the Quick Find box, then select **Sharing Settings**.

2. Scroll down to *CDM Bucket Sharing Rules*.

3. Click **New**.

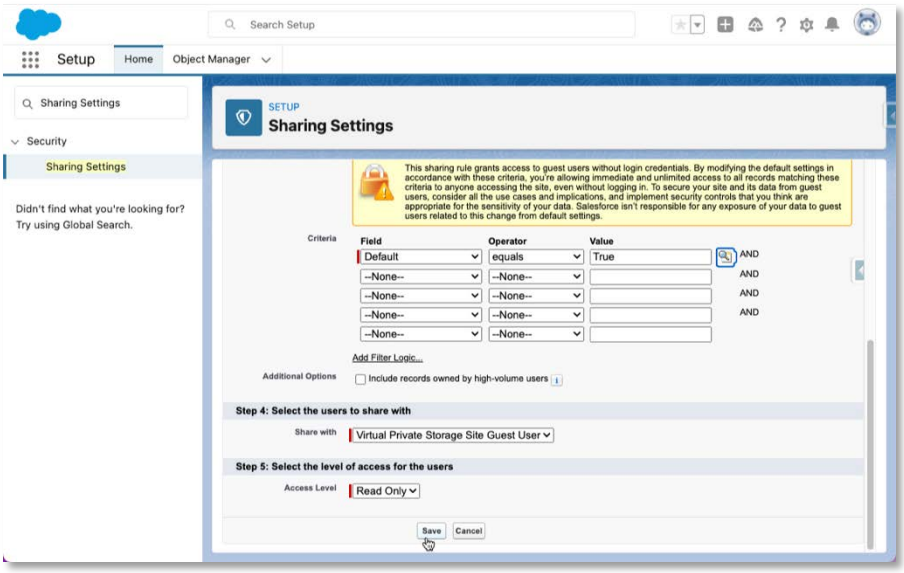
4. Enter a descriptive *Label* and *Rule Name*.

5. Select **Guest user access based on criteria** as the *rule type*.

6. Set up the following criteria:

    1. Field = Default
    2. Operator = equals
    3. Value = True

7. Ensure the correct *Site Guest User* is selected and set the *Access Level* to **Read Only**.



8. Click **Save**.

9. Click **OK** in the confirmation dialog to recalculate the sharing access based on the newly created sharing rule.

10. Scroll down to *CDM External Link Bundle Sharing Rules*.

11. Repeat steps 3 through 7 using the following criteria:

    1. Field = Status
    2. Operator = equals
    3. Value = Active

12. **Save** the sharing rule and confirm the recalculation by clicking the **OK** button.

13. Scroll down to CDM File Sharing Rules.

14. Repeat steps 3 through 7 using the following criteria:

    1. Field = Active Share
    2. Operator = equals
    3. Value = True

15. **Save** the sharing rule and confirm the recalculation by clicking the **OK** button.

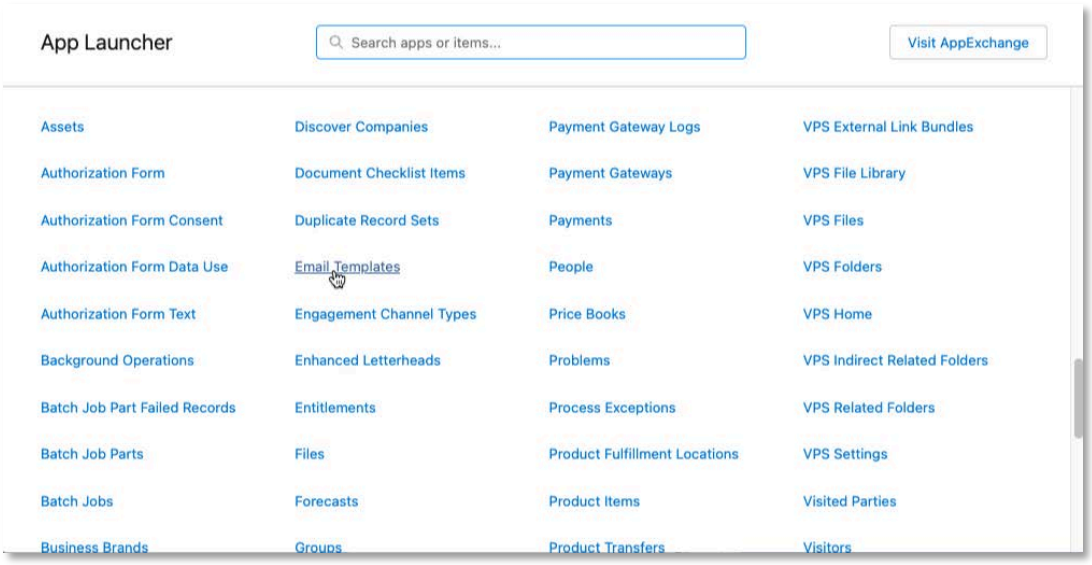
Now that the sharing of CDM Files has been taken care of, we need to create an *Email Template* that will be used as a template for emails sent to an external party when an *External Link Bundle* is activated.

Create an Email Template

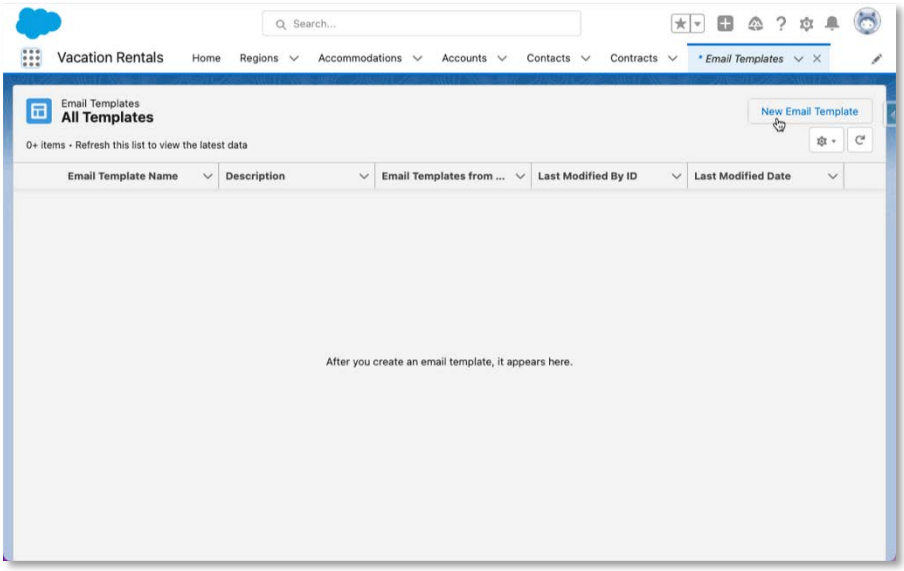
Follow the steps below to create an *Email Template*:

1. Open the *App Launcher* and select **View All**.

2. Click on **Email Templates** in the *All Items* section.



3. Click **New Email Template**.



4. Enter a descriptive *Email Template Name*.

5. Select **CDM External Link Bundle** as the *Related Entity Type*.

6. Select a public folder to store the *Email Template*.

7. Enter the *Subject* of the email.

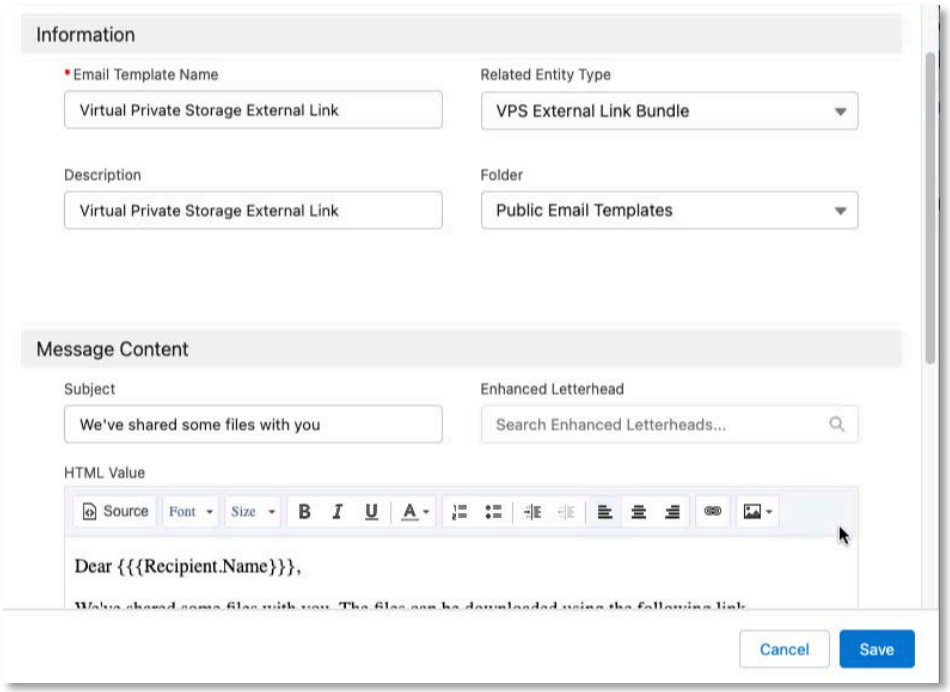
8. In the HTML Value field, create the template for the email's body. Below is an example of an email body using various merge fields.

```
Dear {{{Recipient.Name}}},

We have shared some files with you. The files can be downloaded using the following link.

{{{upperspire__External_Link_Bundle__c.upperspire__External_Link_URL__c}}}


Best regards,

{{{Sender.Name}}}
{{{Sender.CompanyName}}}
```

Note: *{{{upperspire__External_Link_Bundle__c.upperspire__External_Link_URL__c}}}* is the link to the External Link Bundle which should be shared with the external user to access the files.

Note: For security reasons, it is strongly recommended not to share the password to the External Link Bundle by email. Please use an alternative way of communication instead (e.g., SMS / WhatsApp message).

9. Click **Save**.



Set up and enable External Links

Perform the following instructions to make the final configuration changes, enable *External* Links, and publish the *Digital Experience Site*:

1. Open the *CDM Settings* tab, click the App Launcher at the top-left of the screen, and select ***CDM Settings*** from the *All Items* section.

2. Go to the **External Link** page.

3. Enable *External Links* by clicking the *status switch*.

4. Enter the URL to the *Digital Experience Site*.

5. Select the *Email Template*.

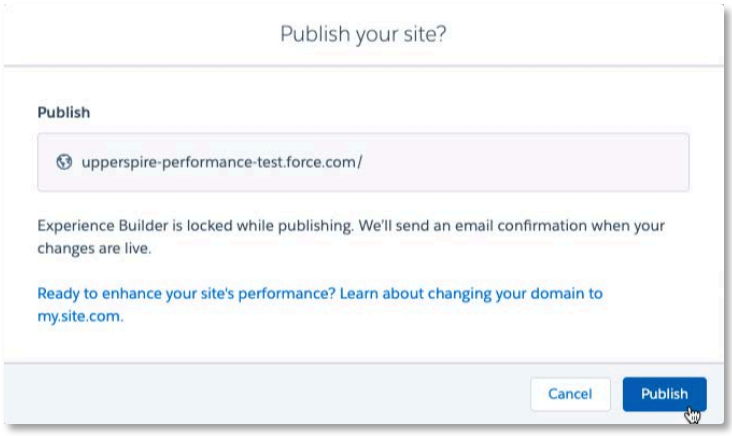
Note: For more details on the configuration choices, please read the *External Links* section of the chapter *Configuring Cartularius*.

6. Click **Save**.

7. From Setup, enter *Digital Experiences* in the Quick Find box, then select **All Sites**.

8. Click on the **Builder** action of the Digital Experience that was created for Cartularius.

9. Click **Publish** in the top right part of the screen.



10. Confirm to publish the site by clicking the **Publish** button in the modal dialog.

External Links are now active and can be used to send files securely to external parties. For more information on creating an External Link Bundle, please check out the *Getting Started with Cartularius for Users* guide.

FEEDBACK

Thank you for using Cartularius. If you encounter any problems, irregularities, or anything else while using our software or reading our documentation, do not hesitate to contact us at support@upperspire.com. Your feedback would be helpful in improving our products and services for you and other customers.

If you like CDM, we would be grateful if you could write a review in the review section of our AppExchange listing. This would help us reach a larger audience and allow our company to grow and develop better products and services.

MORE RESOURCES

CDM AppExchange listing
https://appexchange.salesforce.com/appxListingDetail?listingId=a0N4V00000GYhhhUAD

CDM website
https://www.cartularius.com/

Upper Spire website
https://www.upperspire.com

Amazon S3 user guide
https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html

Amazon S3 console URL
https://s3.console.aws.amazon.com/

Best Practices on Amazon AWS security
https://aws.amazon.com/premiumsupport/knowledge-center/security-best-practices/

Setup MFA for Amazon AWS
https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_virtual.html#enable-virt-mfa-for-root


UPPER
SPIRE
the summit of
Salesforce cloud apps