FILE 365



SET UP MANUAL

Connect Salesforce to Microsoft 365, set up SharePoint locations and give your users File 365 in one guided setup.

ADMINISTRATOR GUIDE · File 365 version 5.0 and higher · November 2026

A product by Vloeiend IT B.V.
Certified Salesforce AppExchange app

file365.nl

Contents

1. Connect Salesforce and Microsoft 365 (Azure AD) 4
1.1 Configure in Azure AD: Application Registration 4
Create a client secret 6
Configure the API permissions 8
1.2 Configure in Salesforce: Connection Setup 10
1.3 Complete the Connection Setup 13
1.3.1 Enable the Named Credentials for callouts 13
1.3.2 Authenticate the principals 14
1.3.3 Assign the principals 15
1.3.4 Migrating from the legacy setup 16
1.4 Manual Setup for multiple connections 16
1.5 Large File Uploads setup 17
1.6 Single Sign On (SSO) based on Microsoft authentication 18

2. Manual Setup: Multiple tenants and SharePoint Site locations 18
2.1 Configure in Azure AD: Application Registration 19
2.2 Configure in Salesforce: Authentication Provider 25
2.3 Configure in Azure AD: Add the Redirect URL to the Application Registration 28
2.4 Configure in Salesforce: Named Credential 29
2.4.1 Named Credential Identity Type 30
2.4.1a Named Principal 30
2.4.1b Per User 30
2.4.2 Create Named Credential 30
2.5 Add the SharePoint URLs to Trusted URLs 32
2.6 Multiple SharePoint Sites 32
2.7 Multiple Azure AD Tenants 32

3. File 365 User permissions and licenses 33
3.1 License 33
3.2 Permission sets for Users and Administrators 33
3.3 Authentication Settings for External Systems 34

4. Set up SharePoint Location: Sites and Folders 35
4.1 SharePoint Location 35
4.2 Types of File 365 Object Location 35
4.3 Create a File 365 SObject Location 35
4.4 File 365 Object Location type (1): Folder per Record 36
4.4.1 Salesforce Object Settings: Single or All 36
4.4.2 Single Object: Salesforce Object settings 36
4.4.3 Single Object: SharePoint Settings 37
4.4.4 All (wildcard) settings 37
4.4.5 SharePoint Folder structure: single object vs wildcard setting 38
4.5 File 365 Object location type (2): Site per record 39
4.6 File 365 Object location type (3): Folder per related Record in Site 40
4.7 File 365 Object location: Deployment of necessary Apex Triggers 41

5. Set up File 365 in the User Interface 44
5.1 Create a File 365 Lookup Field 44

5.2 Modify Page Layouts and Lightning Record Page 44
5.2.1 Page layout: Add and configure File 365 Related List 44
5.2.2 Lightning Record page: Add the File 365 Related List component, File 365 Toolbox 45
5.2.3 Lightning Record page: File 365 Gallery Related List 47

6. File 365 Document Templates 49
6.1 Set up File 365 Document Templates 49
6.2 Automatically create subfolders with the Subfolder Path 51

7. File 365 Administration App 54
7.1 File 365 Status 54
7.2 General Application log 54
7.3 Resolving Errors 54

Optional configuration and Release updates 54

User Instructions 54

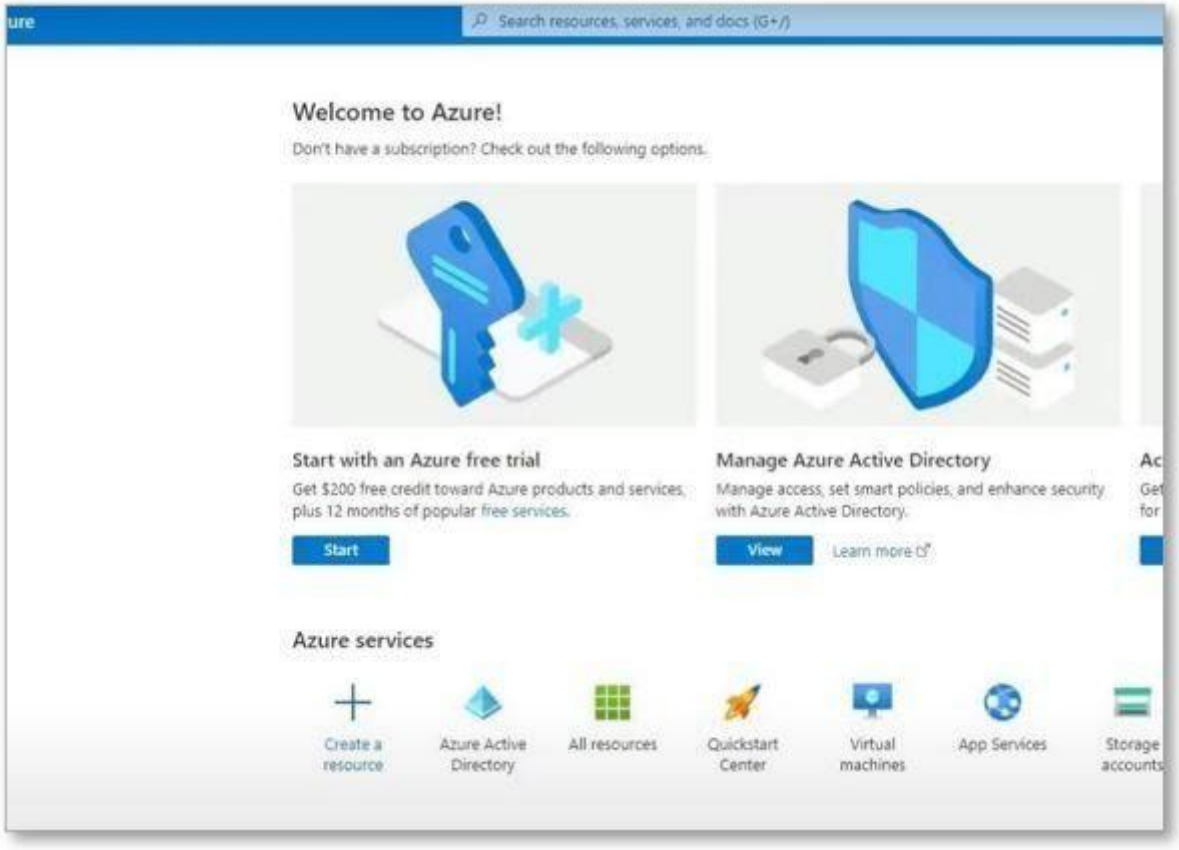
Appendix A 55
SharePoint supported languages, culture names and locale IDs 55
SharePoint Online Site Template ID 55

1. Connect Salesforce and Microsoft 365 (Azure AD)

For File 365 to work, a link between Salesforce and Microsoft 365 (Azure AD) must be set up. You can use the technology and features built into the Salesforce platform to authorize File 365 to access your files in SharePoint in a secure way.

1.1 Configure in Azure AD: Application Registration

First, we must register the application in your Azure tenant and assign the required API permissions. To do this, log in to your Azure Portal as an administrator and select the Azure Active Directory service. You can find it by clicking **All Services** and searching for **Azure Active Directory** in the search box.

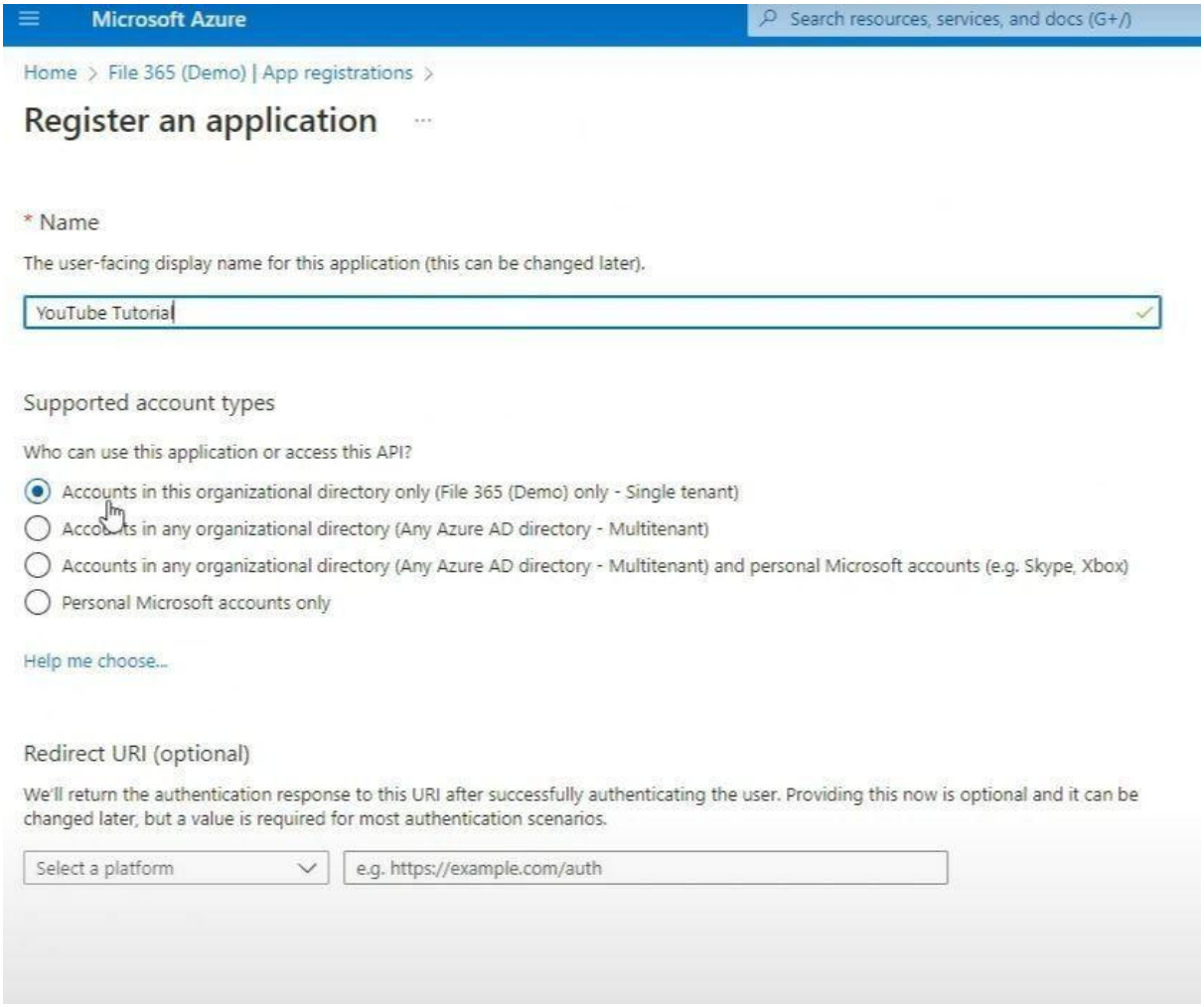


In the left menu, go to the **App registrations** [1] section, then click **New registration** [2].

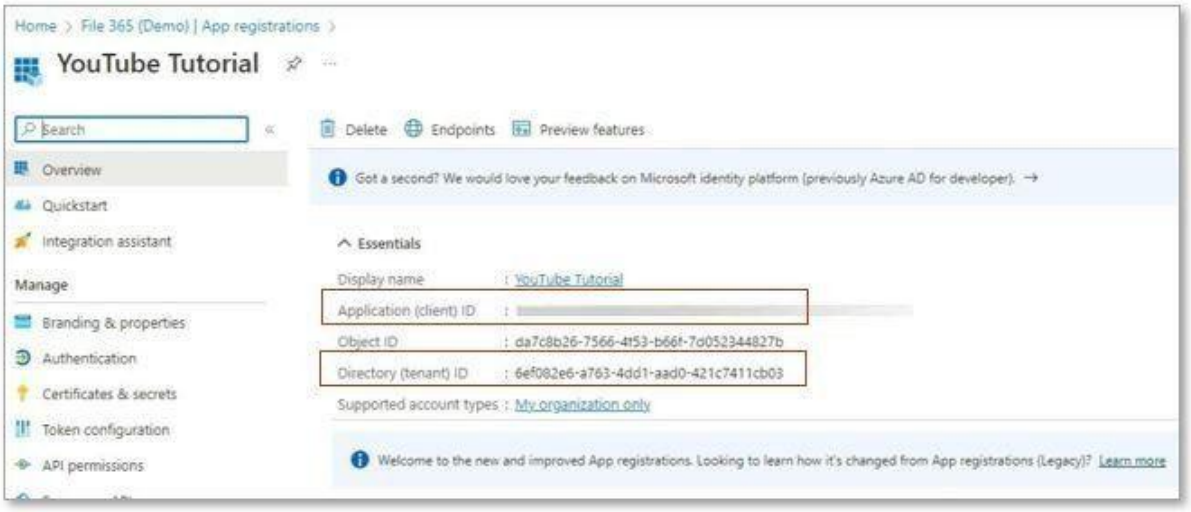


Give the application a name so you know where it is in use, for example File 365. Select Accounts in this organizational directory only in the supported account types section. Under Redirect URI, select Web as the platform and enter the standard Salesforce callback URL for your environment, using the table below. Click Register to create the application. The application page opens.

Environment	Redirect URI to enter
Sandbox and scratch orgs	https://test.salesforce.com/services/extidp/callback
Production	https://login.salesforce.com/services/extidp/callback



At the top of the application page you will find the **Application ID** and the **Tenant ID**. Take note of both, as you will need them for the Connection Setup in Salesforce (see section 1.2). Before moving to Salesforce, there are a few more things to set up on the application.

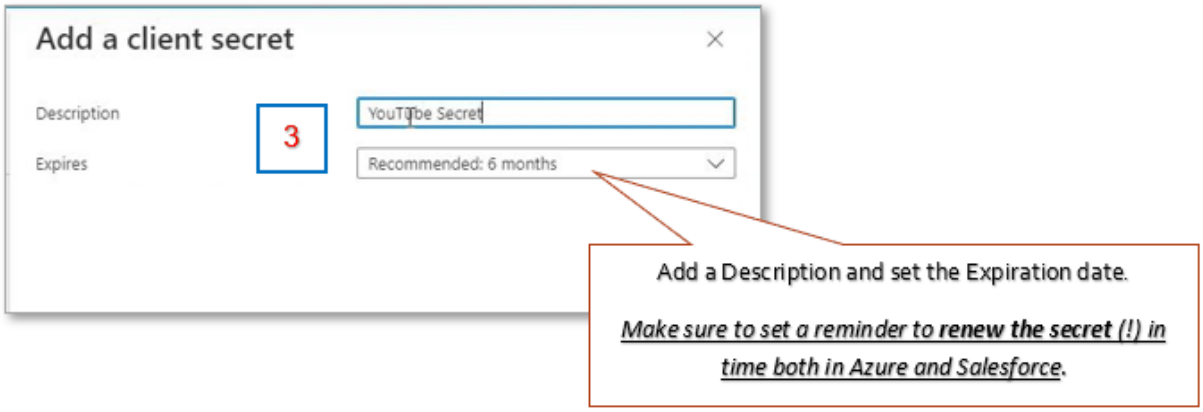


Create a client secret

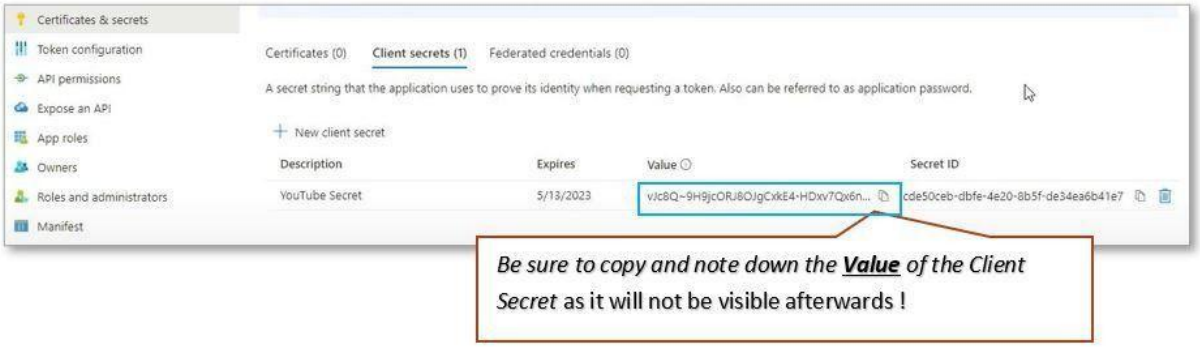
Go to the **Certificates & secrets** [1] section, and click **New client secret** [2]. This is the secret Salesforce will use in the authorization flow.



Add a **Description** and set an **Expiration date** [3]. ***Do not forget to set a reminder for yourself to renew the secret in both Azure and Salesforce.*** If the client secret expires, you will get an authentication (401) error. Finish by clicking **Add** at the bottom of the page.

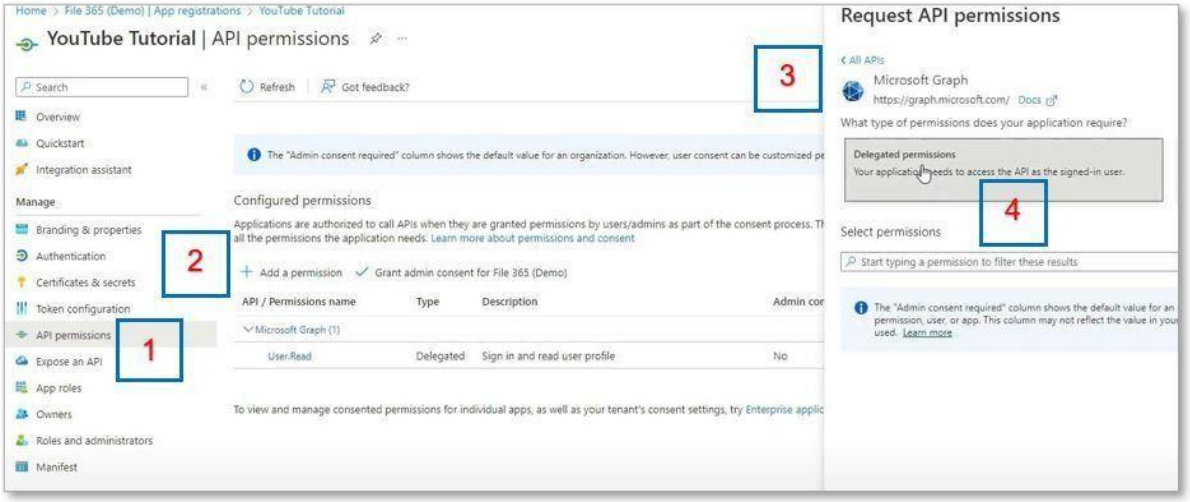


The secret is generated by the Azure portal. *Be sure to copy the Value of the generated secret and store it somewhere safe.* You will need it later for the Connection Setup in Salesforce (see section 1.2).

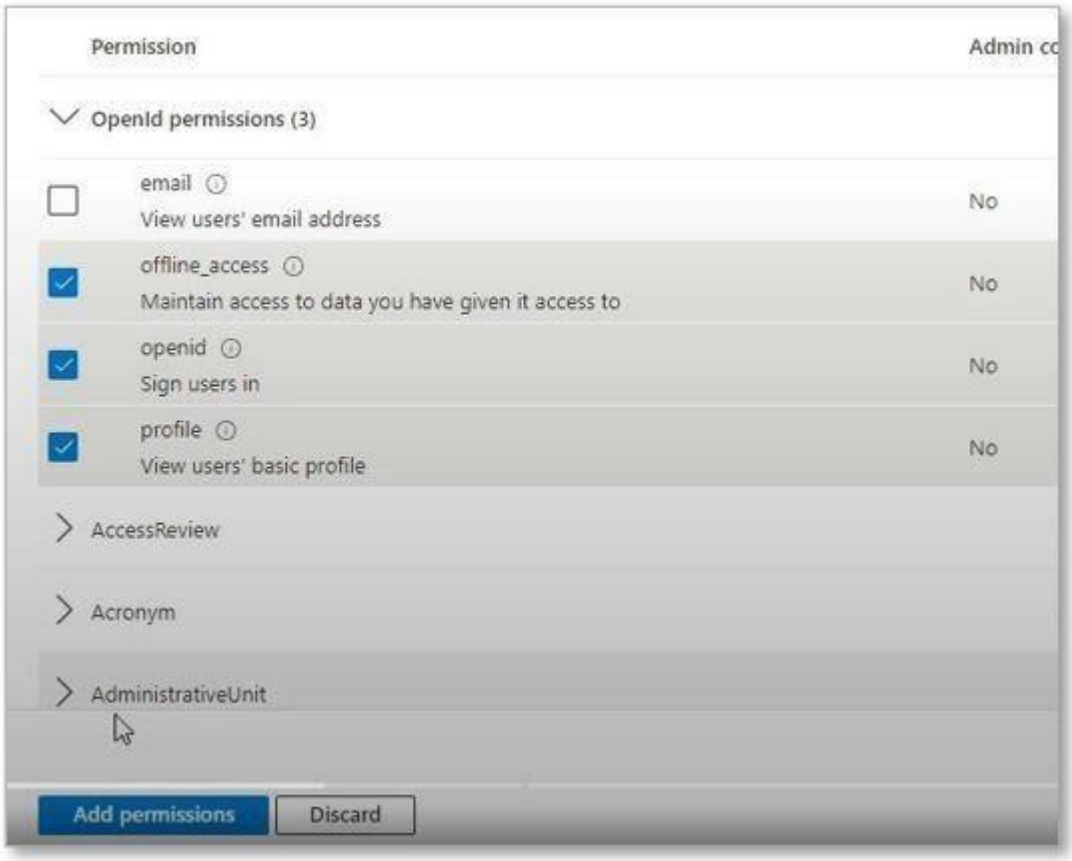


Configure the API permissions

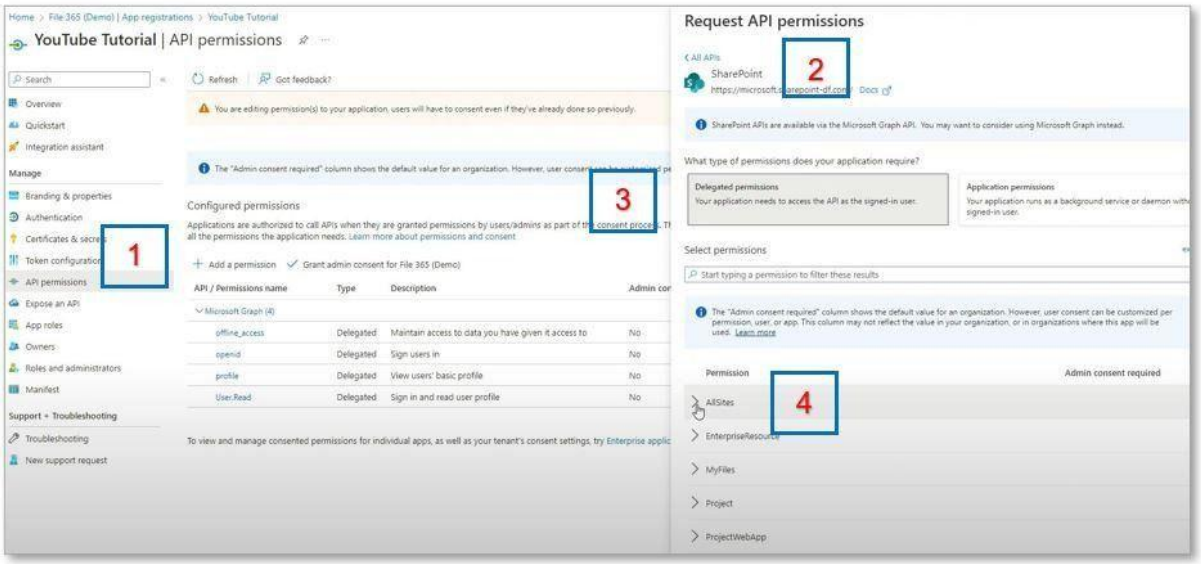
Now configure the API permissions the application requires. Go to the **API permissions** [1] section. Click **Add a permission** [2]**,** then **Microsoft Graph** [3], then **Delegated permissions** [4].



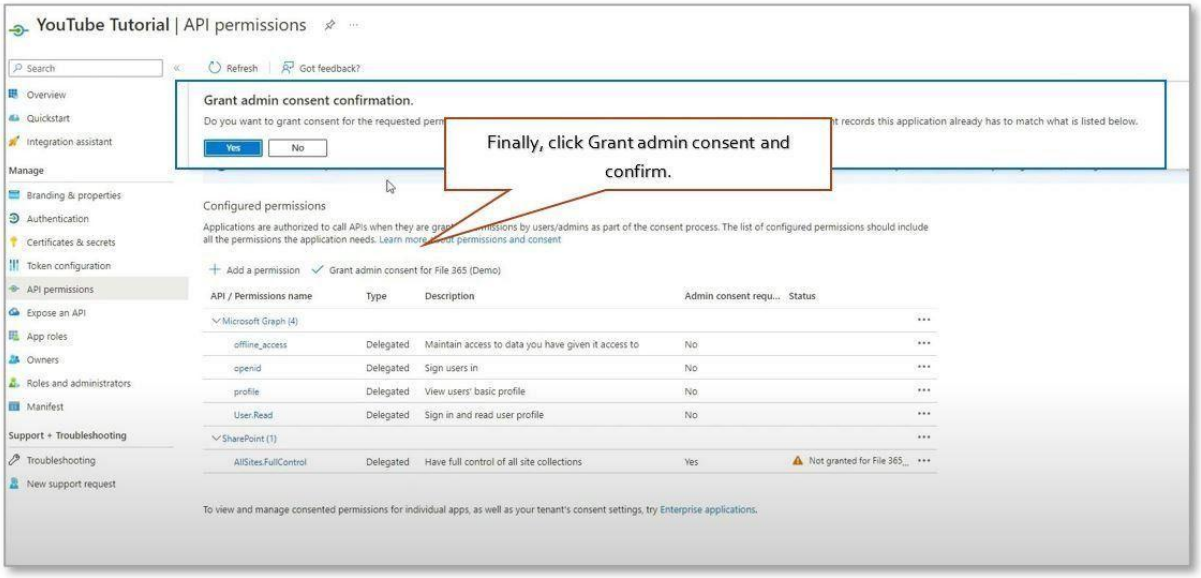
Under the OpenID permissions, select **offline_access**, **openid** and **profile**, then click **Add permissions**.



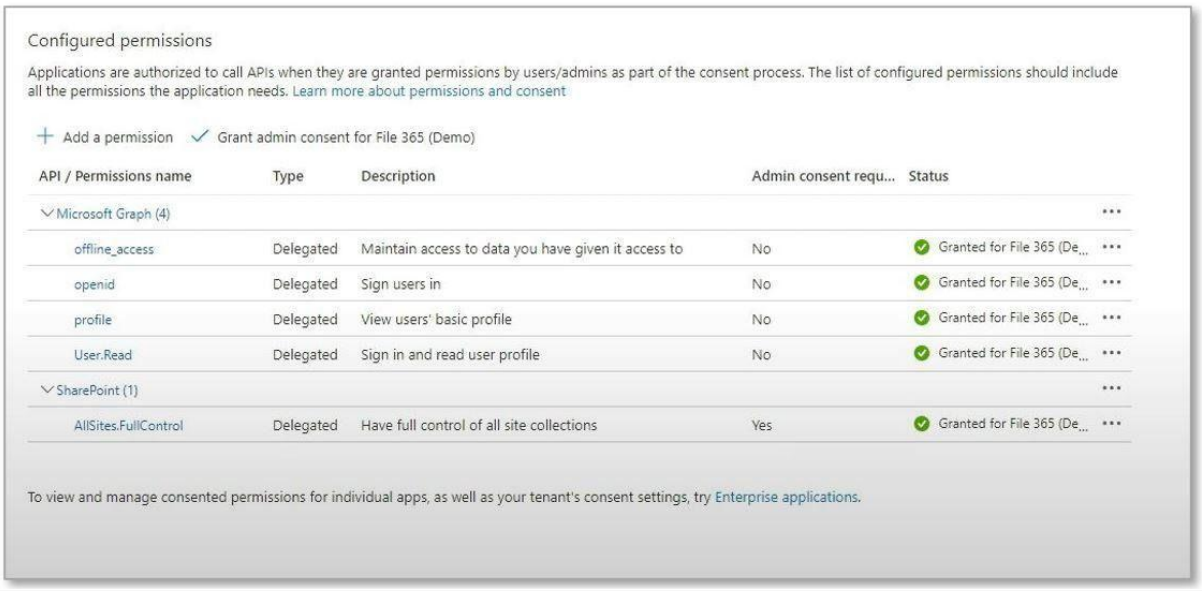
Do the same for the SharePoint delegated permissions. Click **Add a permission [1]**, click **SharePoint [2]**, then **Delegated permissions [3]**. Expand the **AllSites [4]** menu.



Select **AllSites.FullControl** and click **Add permissions**. Then, after confirming the configured permissions, click **Grant admin consent** for your directory and confirm in the pop up.



After you have granted admin consent, the permissions section should look like this:



You have now successfully registered the application in your Azure tenant and assigned all the required API permissions.

1.2 Configure in Salesforce: Connection Setup

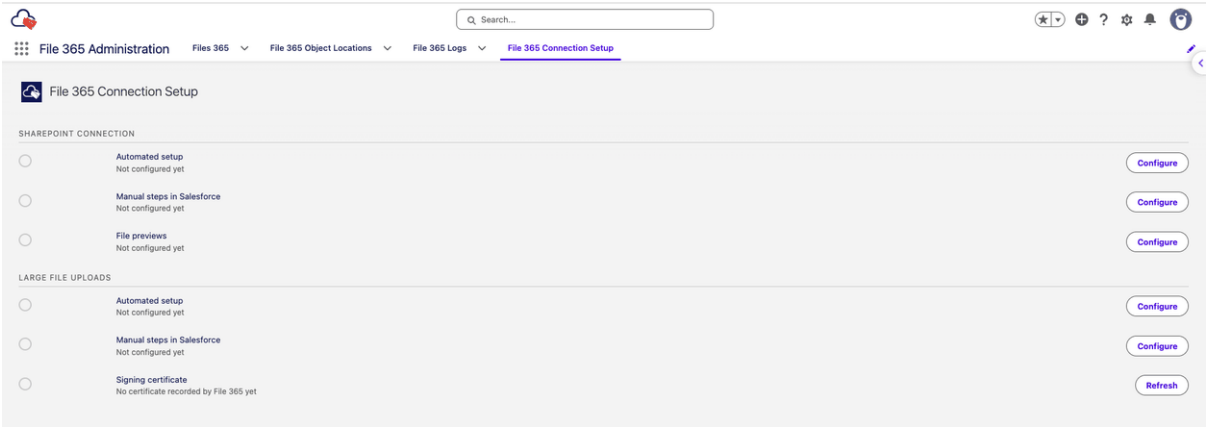
From File 365 version 5.0 onwards, connecting Salesforce to Microsoft 365 is much simpler. The manual steps that were previously required (creating an Authentication Provider, copying callback URLs between Salesforce and Azure, and setting up legacy Named Credentials by hand) are now handled for you inside the File 365 app.

> **Already using File 365?** If you set up File 365 before version 5.0 and configured the credentials the old way, you do not have to change anything. File 365 version 5.0 and higher stays backward compatible with the legacy Named Credentials. You can migrate to the new Named Credentials whenever it suits you, as described in section 1.3.4.

Before you begin, make sure you have the following four values to hand. Three of them come from the Azure application registration you completed in section 1.1, and the fourth is your SharePoint URL.

Field	Value
Application ID	**Application ID** of the registered application in Azure (section 1.1)
Client Secret	The **Value** of the secret you created in Azure (section 1.1), not the secret ID
Tenant ID	**Tenant ID** of your Azure tenant (section 1.1)
SharePoint URL	The root URL of your SharePoint Online environment, for example https://tenantname.sharepoint.com

Open the File 365 app in Salesforce and go to the **Connection Setup** tab. This starts a guided screen flow that walks you through the connection. The flow also includes a link back to this knowledge base article, so you can refer to the Azure steps in section 1.1 if you still need to collect any of the four values.

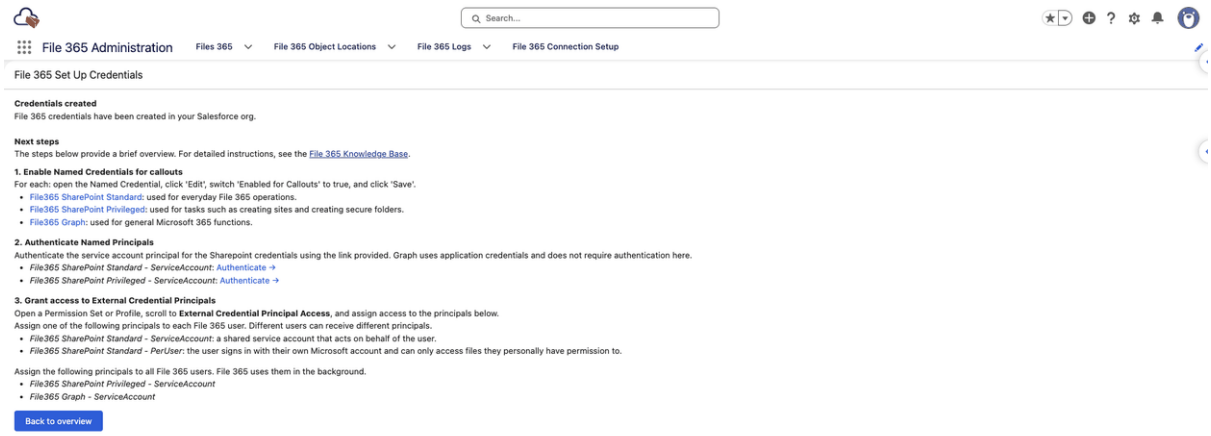


Selecting **Configure** next to **File Previews** creates a trusted URL automatically, which allows users to preview documents stored in SharePoint.

On the first screen, enter the four values, **Application ID**, **Client Secret**, **Tenant ID** and **SharePoint URL**, then click **Next**.



When you click **Next**, File 365 sets up the connection for you. Behind the scenes, the Authentication Provider and the Named Credentials are created automatically.



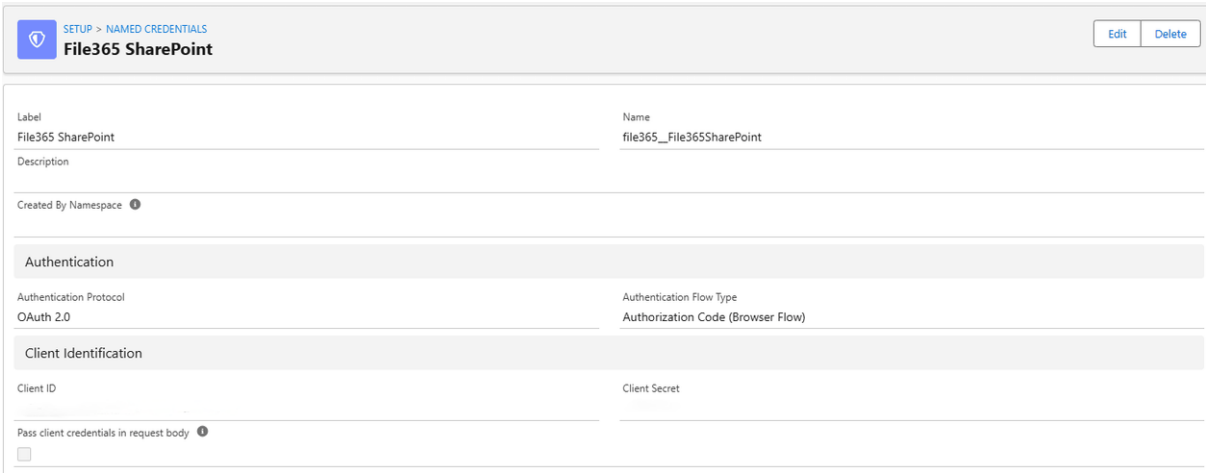
A few short steps remain to finish the setup. These are covered in section 1.3.

Note on the Client Secret:

Entering the secret in the flow is optional. A secret entered in the flow can show up in debug logs and flow error messages. The risk is small, but depending on the size of your org and the number of users (especially admins), you may want to avoid it. The alternative is to enter the secret manually after the setup flow has completed, which prevents this exposure.

To enter the secret manually, go to **Named Credentials** in Setup after the flow has completed, open the **External Auth Identity Providers** tab, and enter it there.





1.3 Complete the Connection Setup

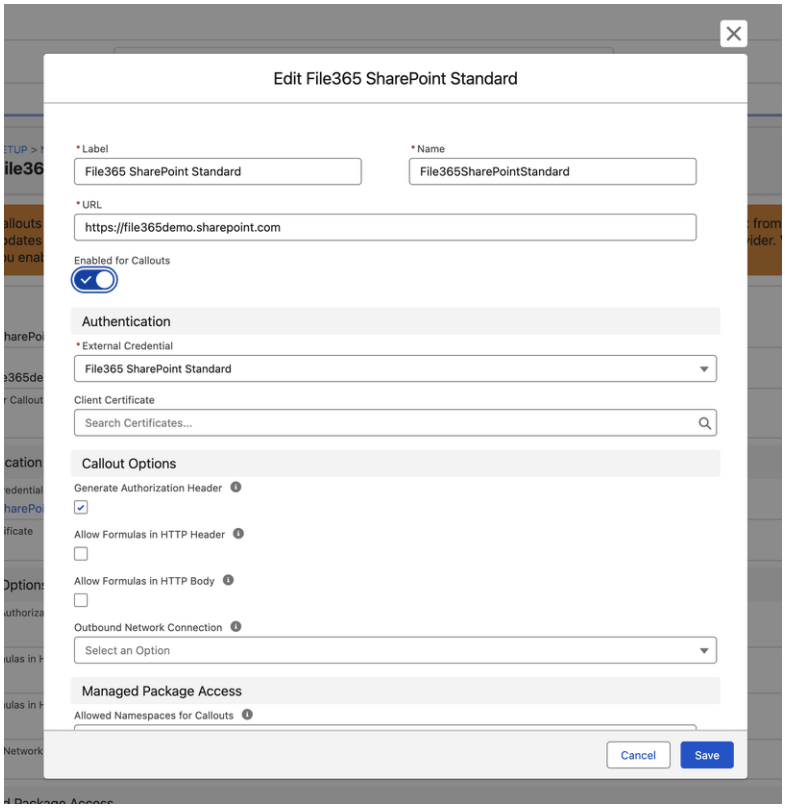
After the connection has been created, three steps remain: enabling the Named Credentials for callouts, authenticating the principals, and assigning the right permissions.

1.3.1 Enable the Named Credentials for callouts

When Named Credentials are created by a managed package, they are not automatically enabled for callouts, so you need to enable them before File 365 can use them. File 365 creates three Named Credentials:

- **Standard**, used for everyday File 365 operations.
- **Privileged**, used for tasks such as creating sites and creating secure folders.
- **Graph**, used for general Microsoft 365 functions.

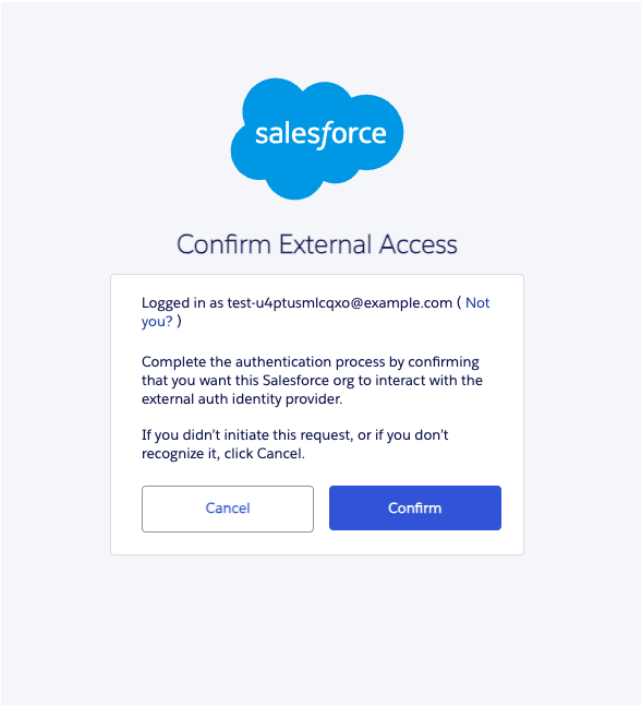
Open each Named Credential, select **Edit**, and toggle on **Enabled for Callouts**.



1.3.2 Authenticate the principals

File 365 works with two kinds of principals, **Named Principals** (a service account) and **Per User** principals. The difference between them, and how to decide which to use, is covered in section 1.3.3. At this point, the Named Principals have to be authenticated.

There are two Named Principals, for the SharePoint Standard and SharePoint Privileged credentials. Open the authentication link provided for each one and sign in with the relevant Microsoft account when prompted. You will need the SharePoint username and password for the service account.



Per User principals cannot be authenticated by an administrator. Each user authenticates themselves the first time they use File 365. That process is described in Authenticate User to SharePoint.

1.3.3 Assign the principals

Before assigning anything, it helps to understand the two kinds of principal File 365 can use.

Named Principal (service account)

Using a **Named Principal**, which we also call a service account, means File 365 connects to SharePoint with the same account for every Salesforce user. All connections, and therefore all SharePoint audit trail entries, are made under this single account rather than under the individual user who performed the action.

Per User

Using a **Per User** principal means File 365 connects to SharePoint as each user individually, by impersonating the Salesforce user who triggered the action. The SharePoint audit trail then shows the actual user instead of a service account.

Choosing which principal to assign

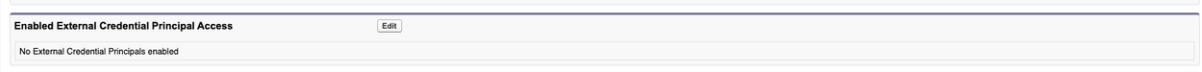
How the principals are assigned depends on the credential:

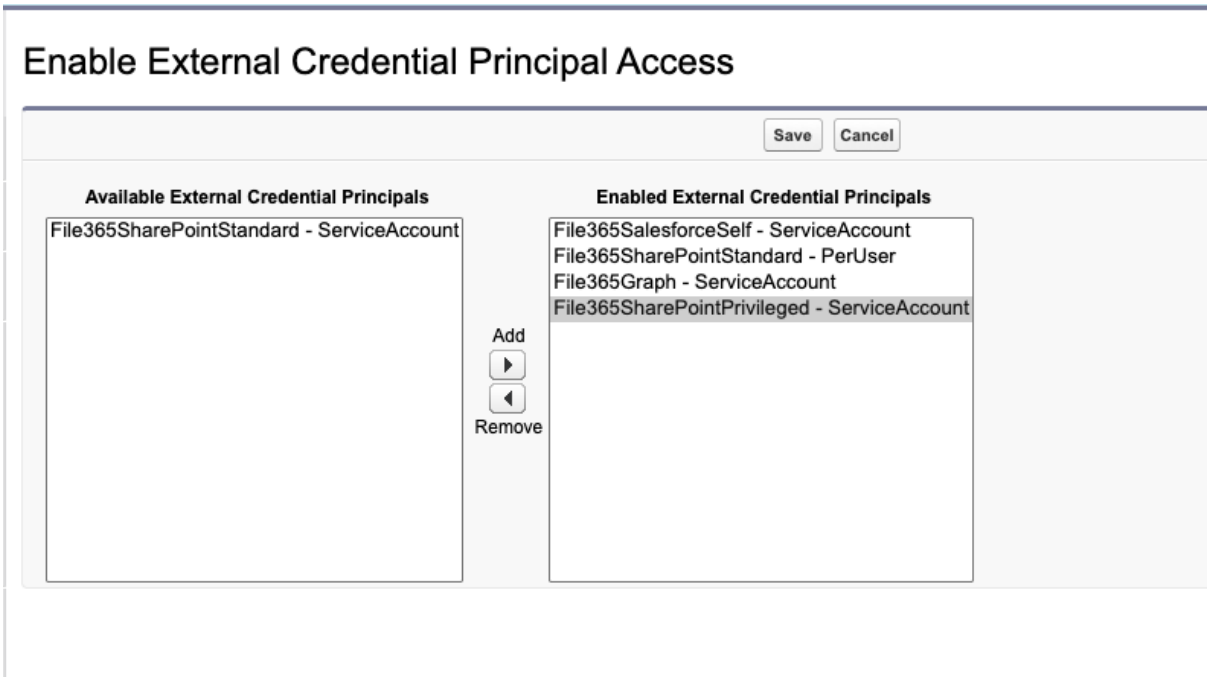
- **Privileged** and **Graph**: the service account (Named Principal) is the only principal available, so it must be assigned.
- **Standard**: you can assign a Named Principal, a Per User principal, or both. You must assign at least one. If you assign both, the order of the principals decides which one is used for the callout. File 365 gives the Per User principal priority during the setup process, so when both are assigned, File 365 uses Per User.

> **Our recommendation:** Use the Per User principal wherever possible, so that actions in SharePoint can be traced to the individual user. A Named Principal is the better choice for users who do not have their own access to SharePoint, such as external users. You can also create separate permission sets for different groups, for example a permission set with Per User access for internal users and a permission set with service account access for external users.

To assign the principals, go to **Permission Sets** in Setup and create a new permission set, for example File 365 Permissions. Open the permission set, find the **External Credential Principal Access** section, and enable the principals you need by following the rules above. Save the permission set, then assign it to the users who should have access to File 365.

We also recommend adding the **File365SalesforceSelf – ServiceAccount** principal at this point, as it is required later for Large File Uploads (section 1.5).





Once you have saved, the connection setup is complete.

1.3.4 Migrating from the legacy setup

Customers who set up File 365 before version 5.0 use the legacy Named Credentials together with an Authentication Provider. From version 5.0, File 365 stays backward compatible with this manual setup, so if it is working well you do not have to change anything. If you would like to move to the new Named Credentials, you can migrate at any time by following the steps below.

1. Create the new Named Credentials using the Connection Setup process described in sections 1.2 and 1.3.
2. Add the standard callback URL as a redirect URI in Microsoft (Azure AD), as described in section 1.1, if it is not already in place.
3. Update every existing object location so that it uses the newly created Named Credentials instead of the legacy ones. Each object where File 365 is in use has its own object location, so work through them all.
4. Once every object location points at the new Named Credentials, remove the legacy Named Credential and the Authentication Provider.

File 365 is now running entirely on the new Named Credentials.

1.4 Manual Setup for multiple connections

If you cannot use, or prefer not to use, the automatic Connection Setup, or if you need to connect more than one SharePoint site collection or Azure AD tenant, follow the manual setup in chapter 2, Manual Setup: Multiple tenants and SharePoint Site locations.

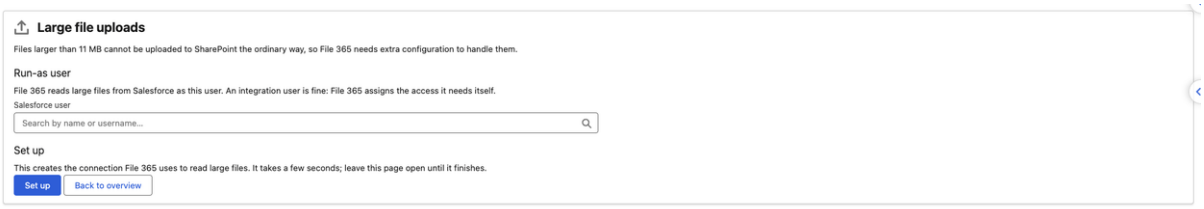
1.5 Large File Uploads setup

We recommend setting up Large File Uploads for every setup, including the manual setup in chapter 2. It is a recommendation, not a requirement.

Before starting the Large File Uploads setup, go to **Setup › Users** and create a new Integration User called *File365IntegrationUser*.

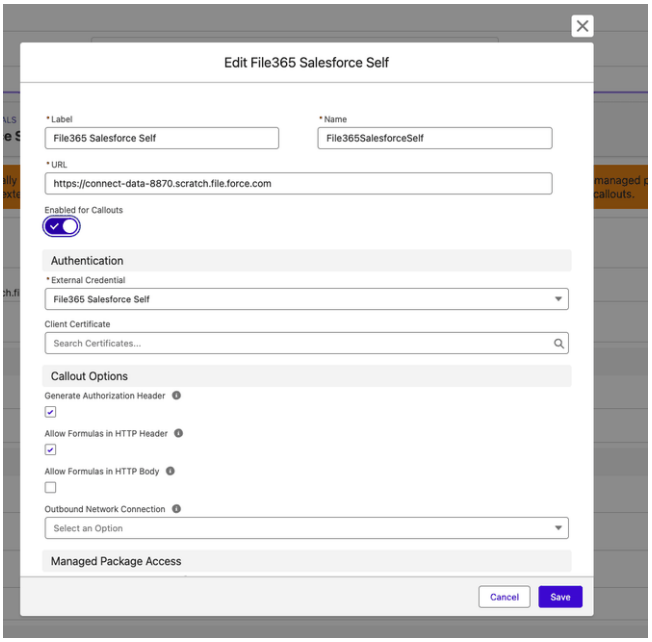
Next, go to **Permission Sets** in Setup and open the permission set **File 365 Integration User**. The principals required for Large File Uploads are already assigned to this permission set, so assigning it to the new integration user is all that is required.

On the File 365 **Connection Setup** tab, go to the **Large File Uploads** section and click **Configure** next to **Automated Setup**. On the screen that opens, select the integration user you just created.



Click **Setup** and wait for the success message. Then click **Back to Overview** and click **Configure** next to **Manual Steps**.

Click the **File365 Salesforce Self** link, select **Edit**, and toggle on **Enabled for Callouts**.



Go back to the File 365 **Connection Setup** tab, click **Refresh** next to **Signing Certificate**, and wait for the success message.

Note: after refreshing the certificate, save its expiry date and set a reminder to refresh it again before it lapses.

1.6 Single Sign On (SSO) based on Microsoft authentication

Single Sign On is a recommendation, not a requirement: File 365 works without it.

The file preview functionality in File 365 works by displaying a page from Microsoft SharePoint in the browser (using an iframe). For previews to work smoothly, the user should be logged into Azure AD with their credentials in their browser session. The easiest way to accomplish this is to set up Single Sign On in Salesforce, so users log in with their Microsoft work account.

We recommend this for every setup, whether you used the Connection Setup or the manual setup. To configure Single Sign On, follow the steps in Microsoft's tutorial Configure Salesforce for Single sign-on in Microsoft Entra ID.

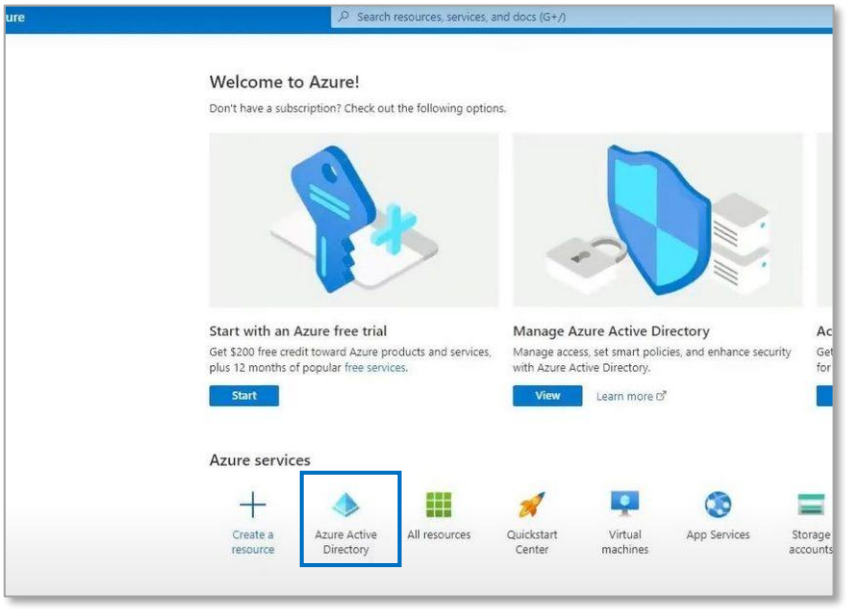
2. Manual Setup: Multiple tenants and SharePoint Site locations

Since File 365 version 5.0, the Connection Setup in the File 365 app connects Salesforce to Microsoft 365 for you, as described in chapter 1. This chapter describes the manual setup, in which you create the Authentication Provider and the legacy Named Credentials yourself.

Use the manual setup when:

- you cannot use, or prefer not to use, the automatic Connection Setup;
- you want to connect more than one SharePoint site collection (section 2.6);
- you want to connect more than one Azure AD tenant (section 2.7).

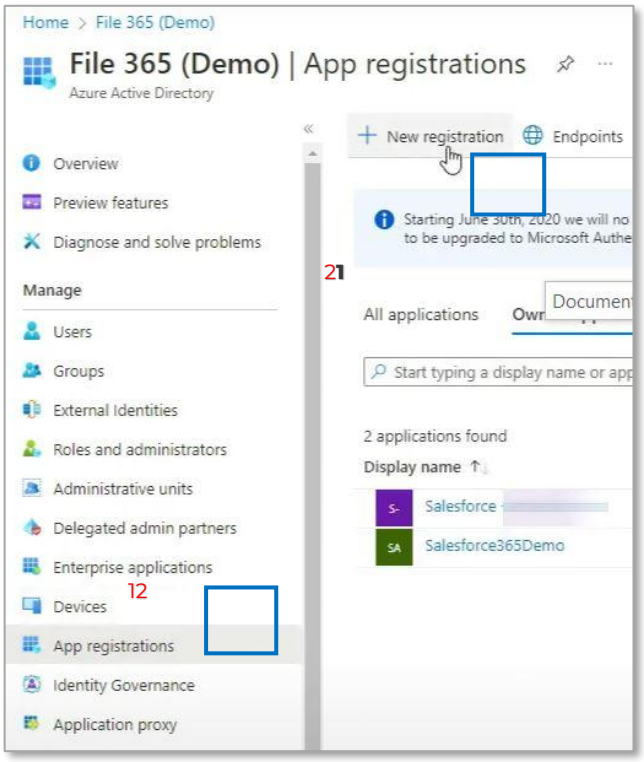
Recommended for every setup: whether you use the manual or the automatic setup, we recommend also setting up **Large File Uploads** (section 1.5) and **Single Sign On (SSO)** (section 1.6), both described in chapter 1. Both are recommendations, not requirements: File 365 works without them.



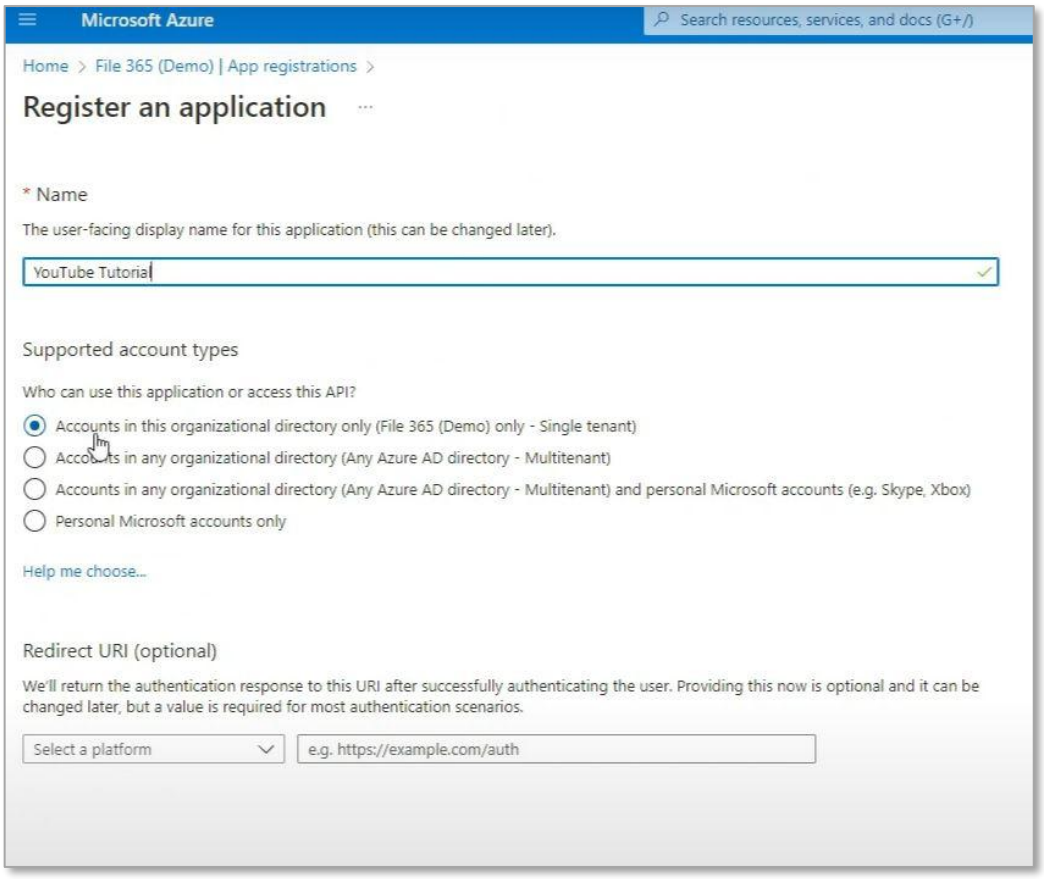
2.1 Configure in Azure AD: Application Registration

First, we must register the application in your Azure tenant and assign the required API Permissions. To do this, login to your Azure Portal as an administrator and select the Azure Active Directory Service.

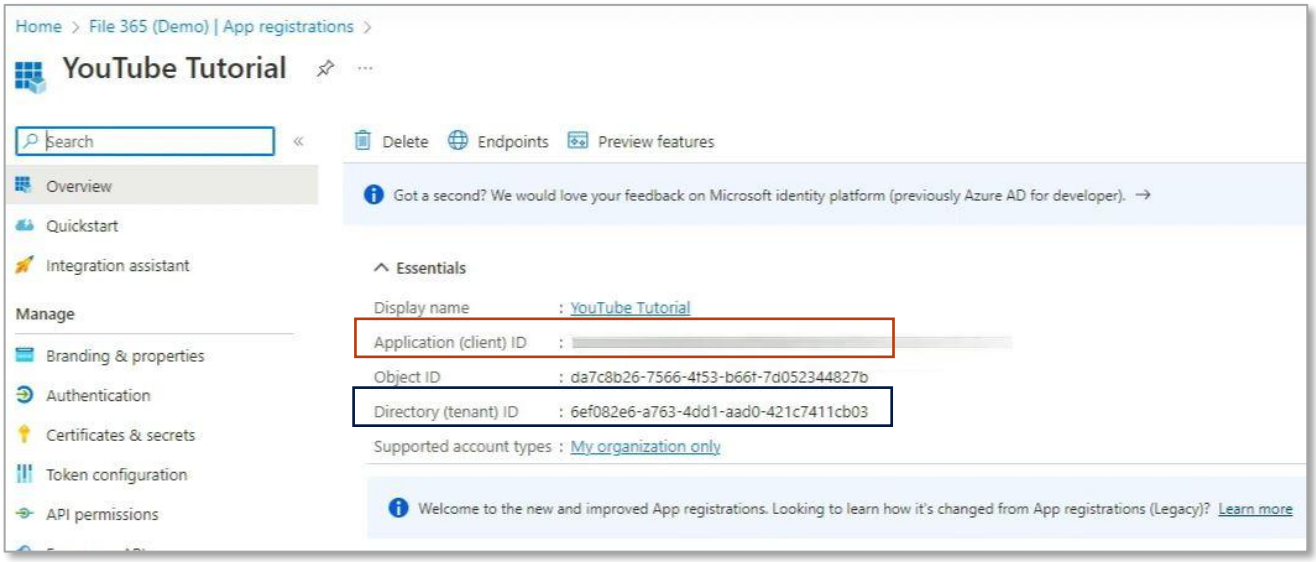
You can find it by clicking “All Services” and search for “Azure Active Directory” in the search box.



In the left menu, go to the “App registration” [1] section and click “New Registration”[2]

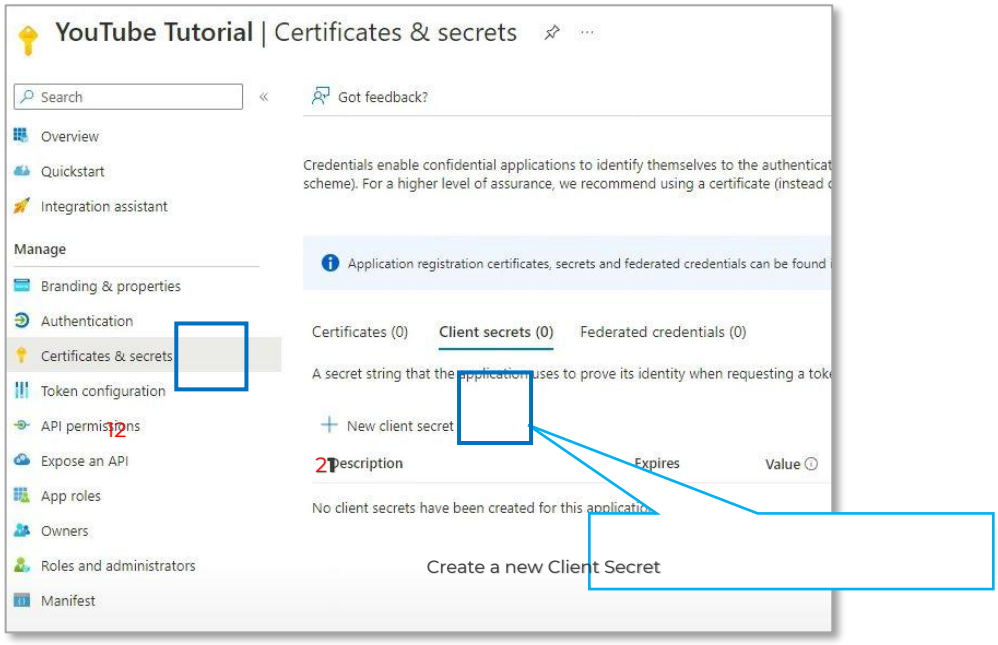


Type a name so you know where the application is in use. Here we will use: “YouTube Tutorial” and select “Accounts in this organizational directory only” in the supported account types section. Leave the Redirect URI blank for now, we’ll fill that later. Click **Register** to create the application, the application page opens.

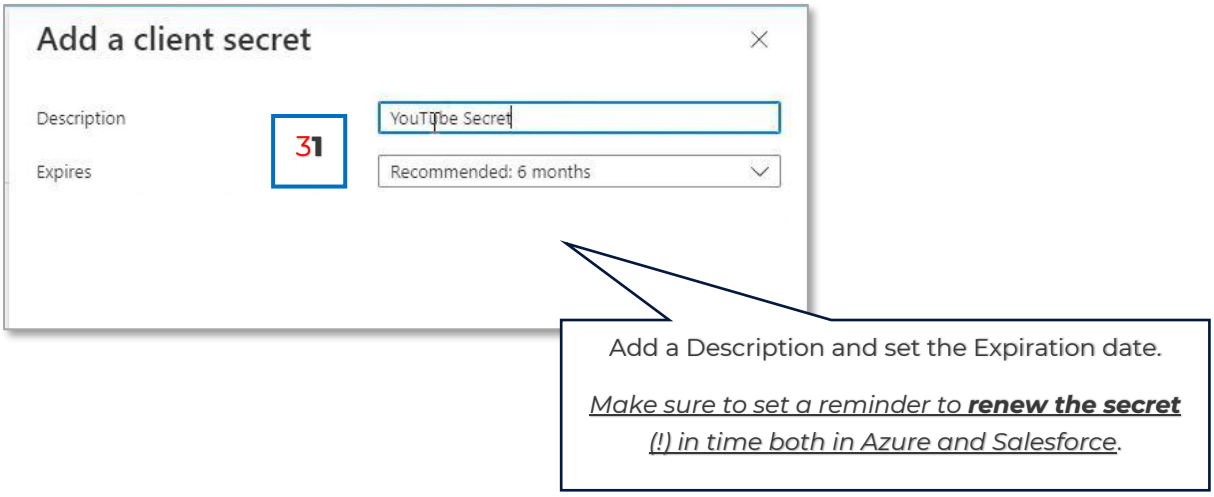


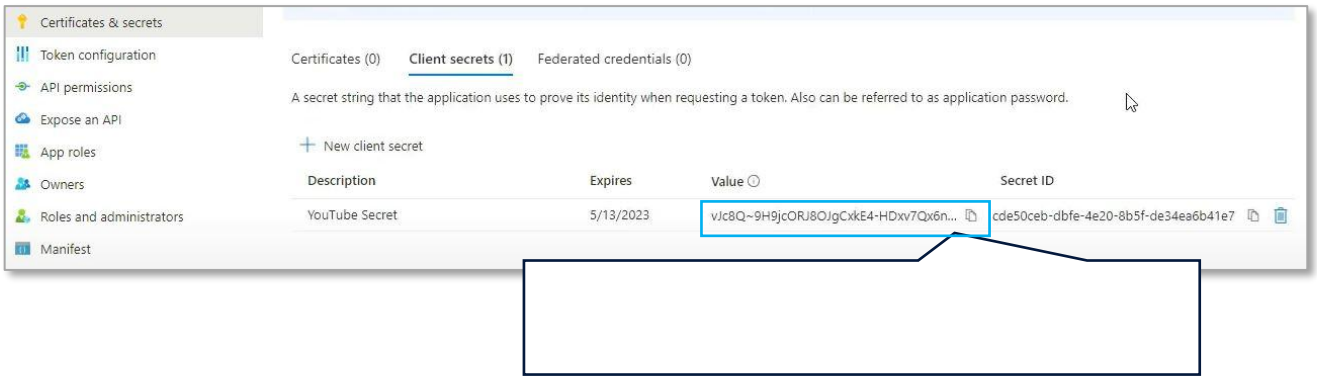
On top of the application page, you can find the Application and Tenant Ids. Take note of these as we need them to create the Authentication Provider in Salesforce. But before we go to Salesforce, we need to set up the application further.

Go to the **Certificates & secrets section** [1], and click **New client secret** [2]. Create a new client secret. This is the secret Salesforce will use in the authorization flow.



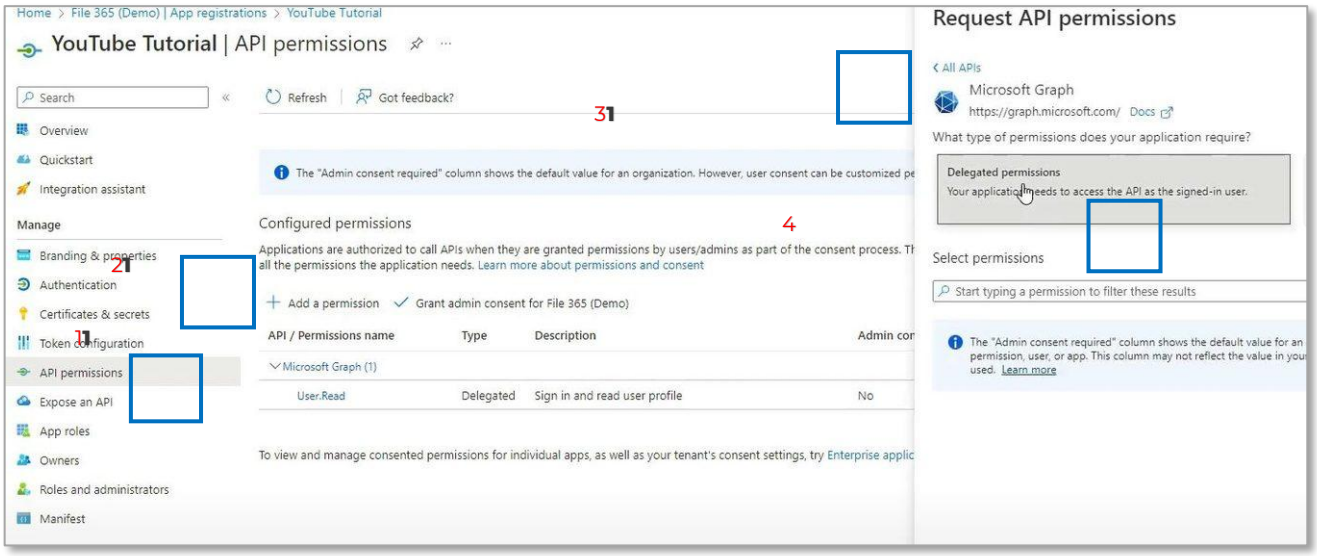
Add a **Description**, and set the **Expiration date** [3]. ***Do not forget to set a reminder for yourself to renew the secret both in Azure and Salesforce***. Please note that if the client secret is expired, you will get an authentication (401) error. Finish by clicking **Add** on bottom of the page.

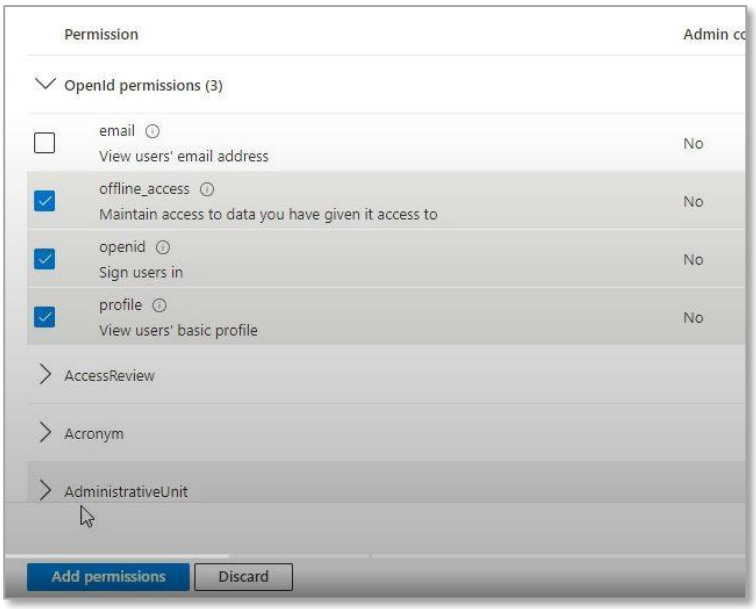




The secret will be generated by the Azure portal. ***Be sure to copy the value of the generated secret and store it at a safe location***, we will need this information later when creating an Authentication Provider in Salesforce (see section 2.2).

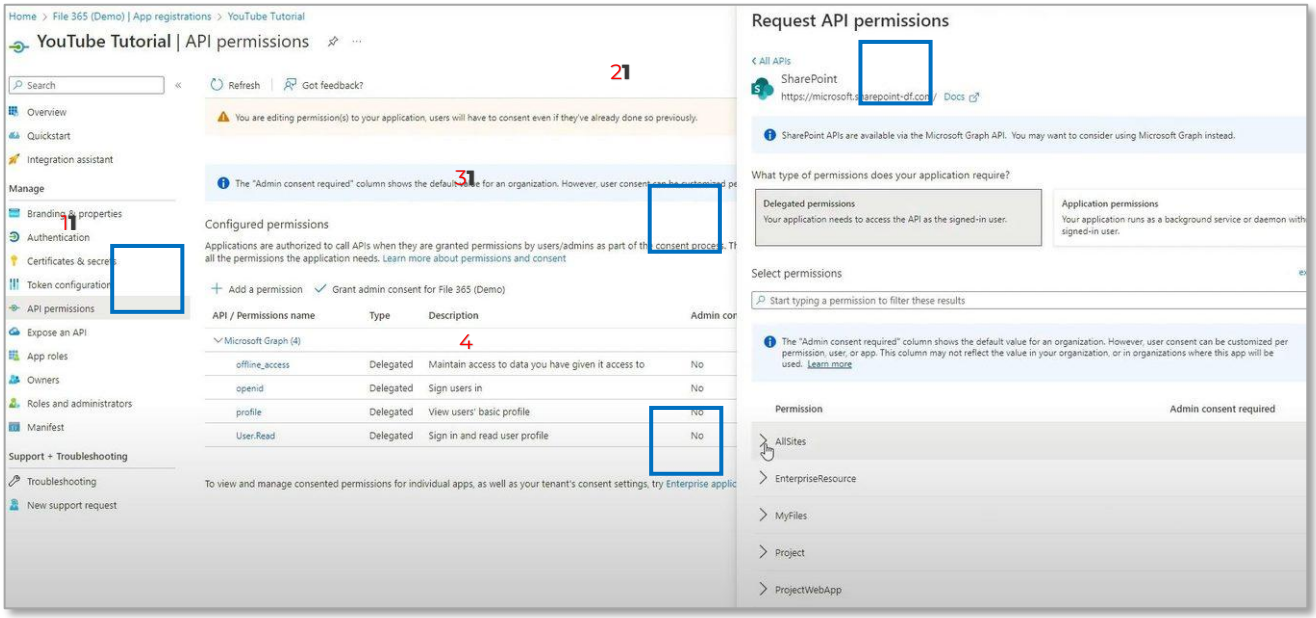
Now we need to configure the API permissions required by the application. Go to the **API permissions** [1] section. Click **Add a Permission** [2], **Microsoft graph** [3], and **Delegated permissions** [4].

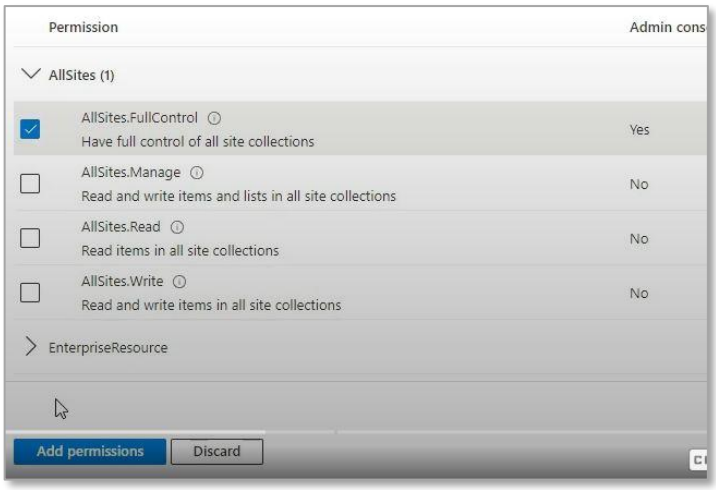




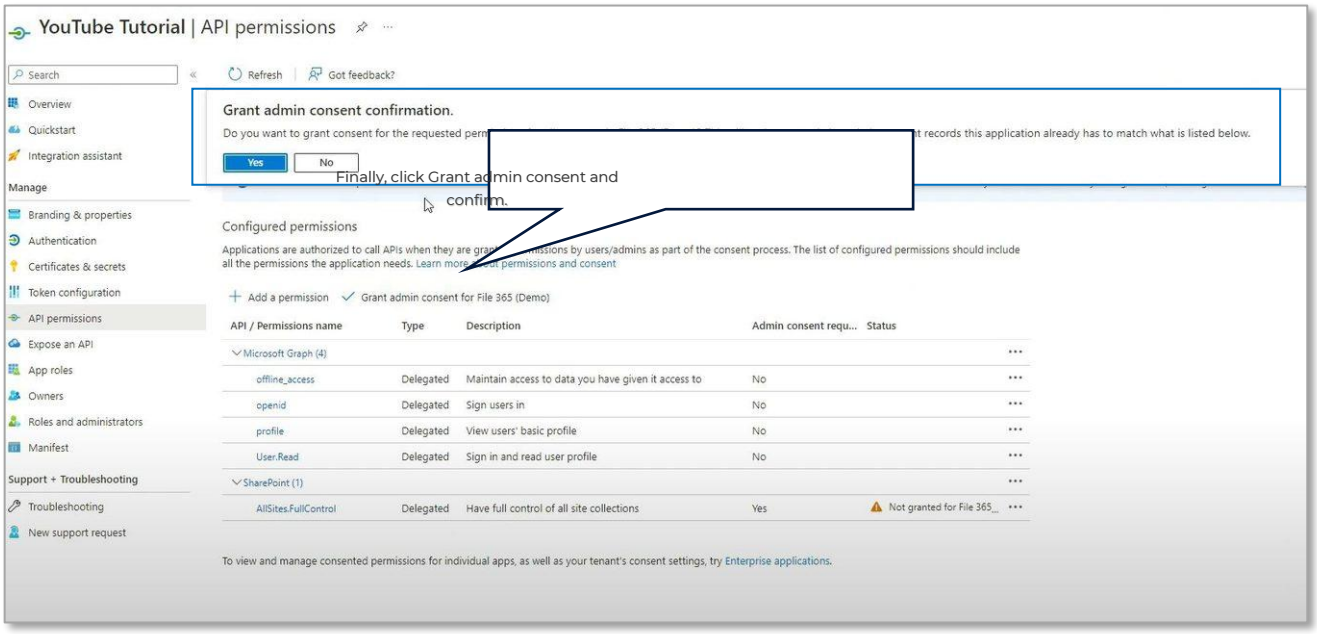
After clicking delegated permissions, under Openid permissions, select the following:
Offline_access, **openid** and **profile**.
Click **Add permissions**.

Do the same but then go to SharePoints delegate permissions: Click **Add a Permission [1]**, Click **SharePoint [2],** and **Delegated permissions [3]**. After clicking Delegated permissions, expand the **AllSites menu [4]**:

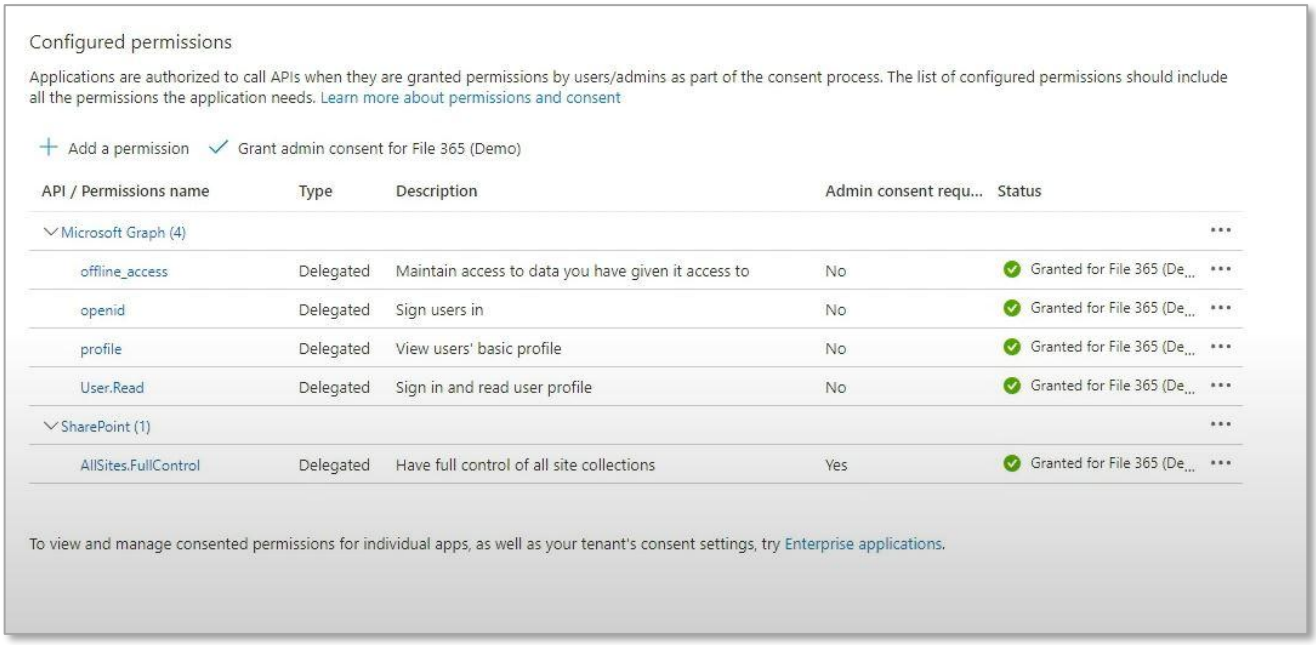




Select **AllSites.FullControl** and Click **Add permissions**. Now, after confirming the configured permissions, click **Grant admin consent** for File 365 (Demo) and confirm in the pop up.



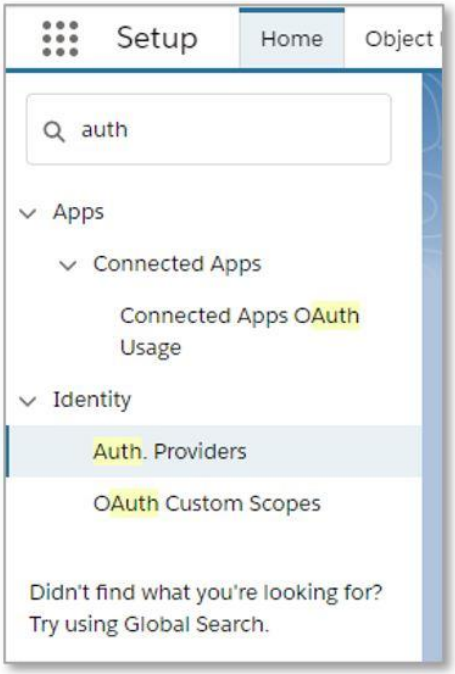
After you have granted admin consent, the permission section should look like this:



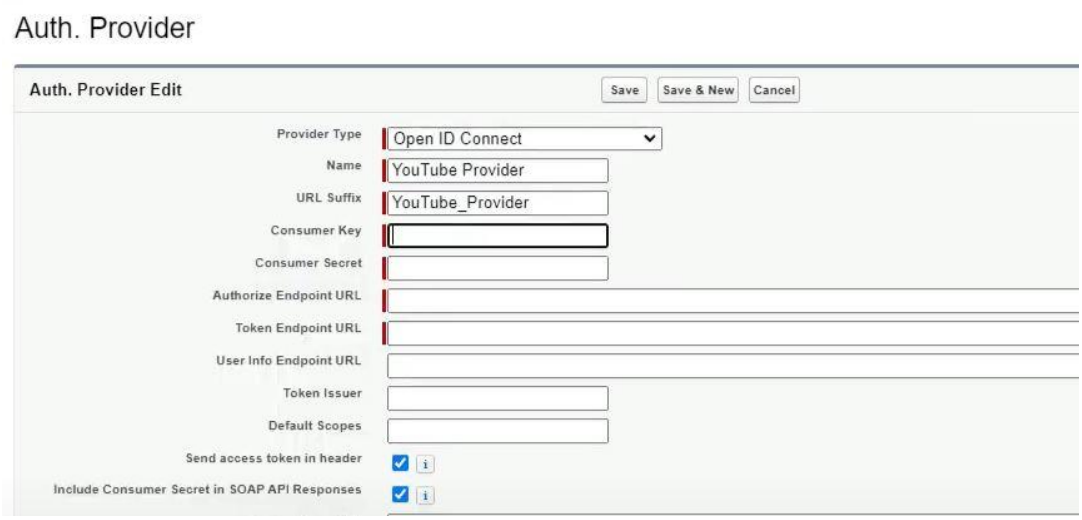
You have now successfully registered the application in your Azure tenant and assigned all the required API Permissions.

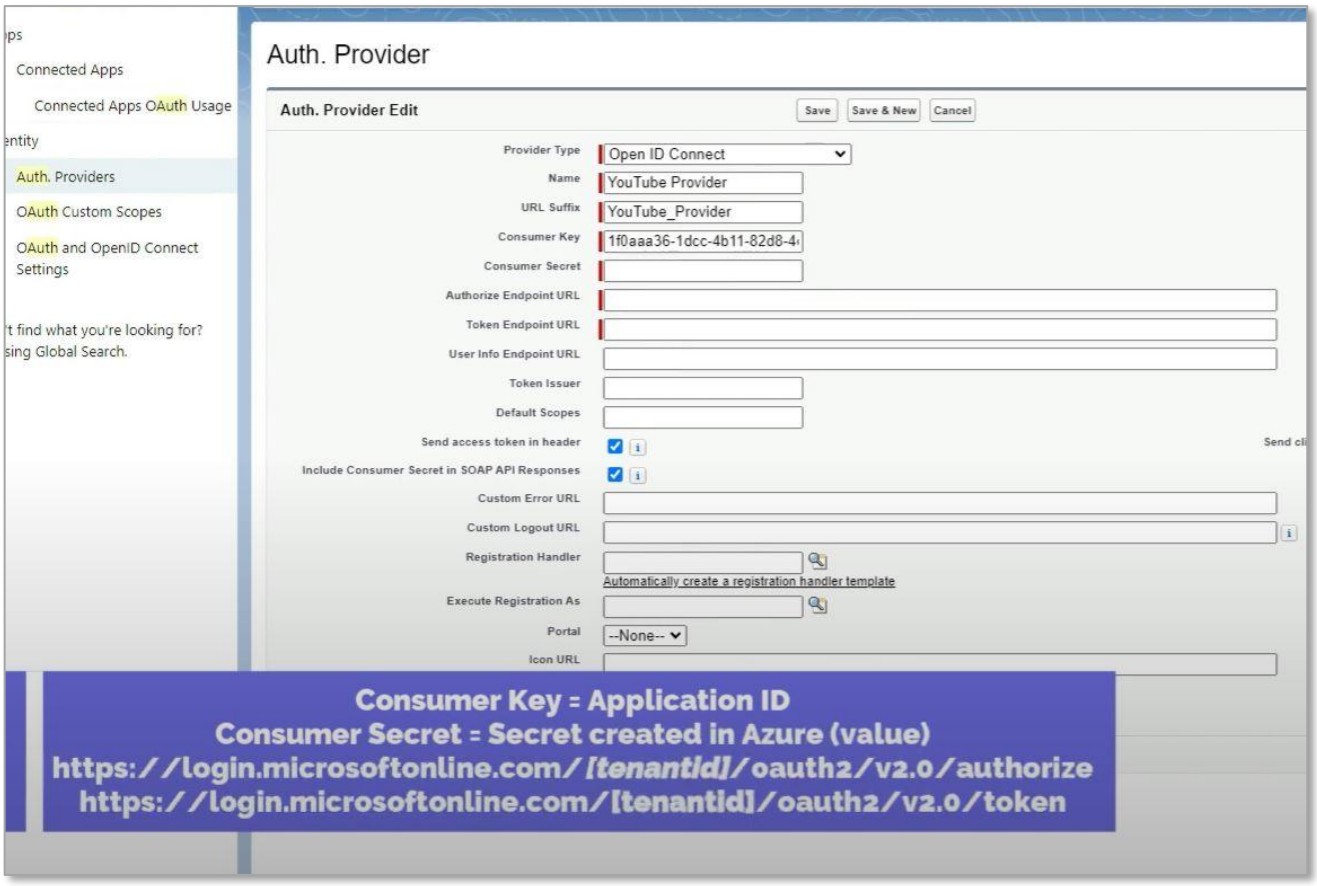
2.2 Configure in Salesforce: Authentication Provider

Now login to Salesforce as an administrator and open Setup. Find the “Auth. Providers” in the Identity section.



Add a new Auth. Provider with Provider Type **Open ID Connect**. Choose a name and a URL Suffix.

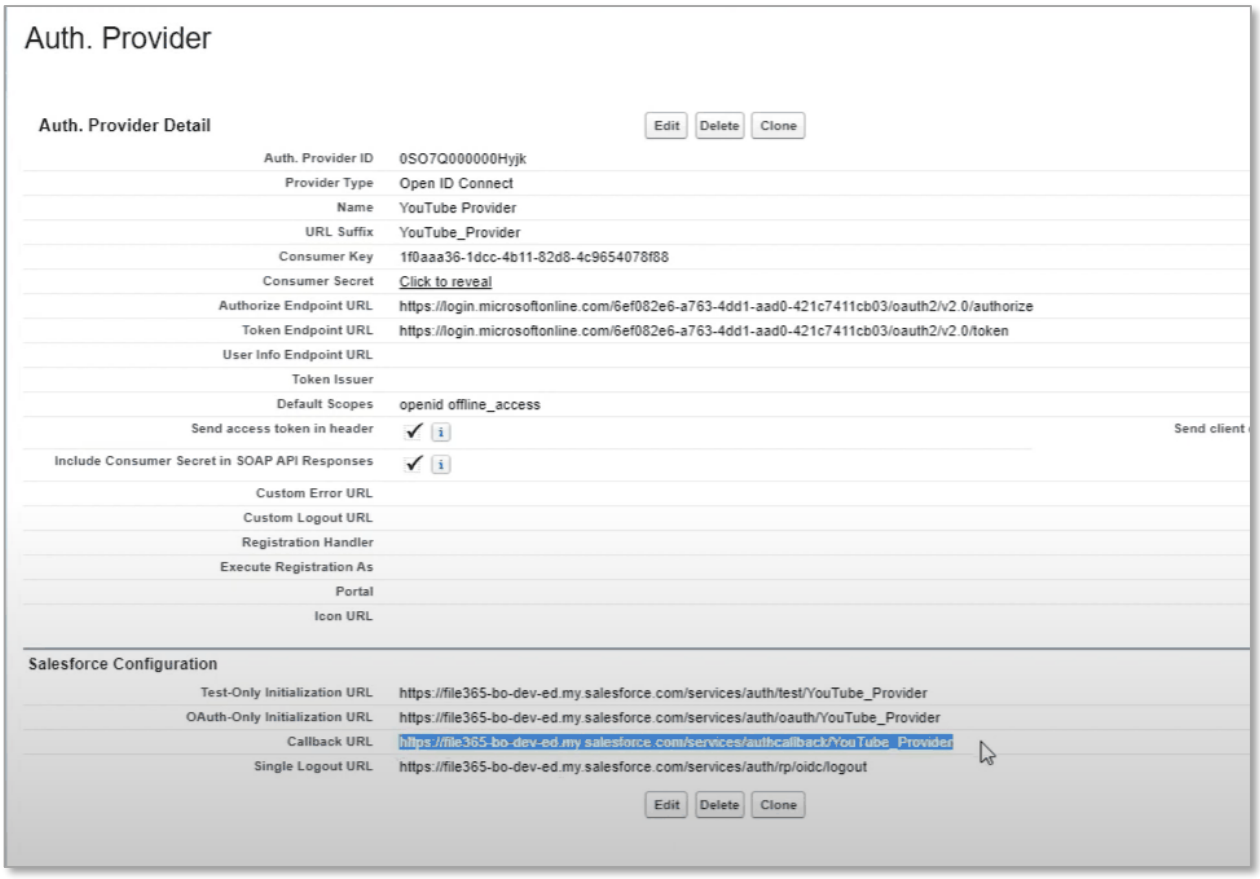




Next, fill in the **Consumer Key** and **Consumer Secret** and other required fields by following the instructions below. For the Authorize Endpoint URL and the Token Endpoint URL, copy the URL and replace **[tenantid]** by the tenant ID of your Azure tenant. Lastly, define the default Scopes as “openid offline_access”.

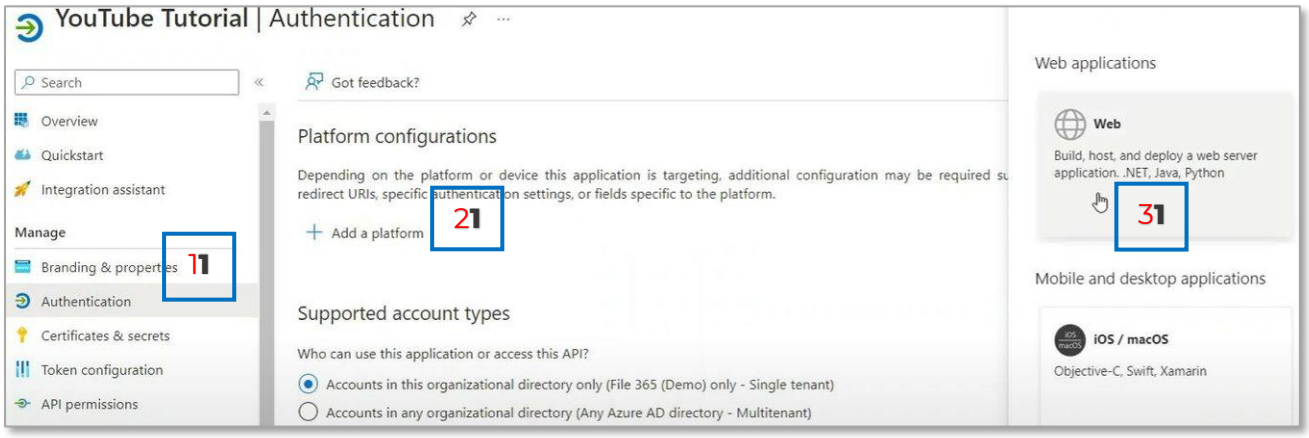
Consumer Key	Use the ***Application ID*** of the registered application in Azure
Consumer Secret	Use the ***Value of the Secret created in Azure*** for the application (not the ID)
Authorize Endpoint URL	https://login.microsoftonline.com/**[tenantid]**/oauth2/v2.0/authorize *
Token Endpoint URL	https://login.microsoftonline.com/**[tenantid]**/oauth2/v2.0/token *
Default Scopes	openid offline_access
Replace [tenantid] in the URL by the tenant Id of your Azure tenant. You can find this on the Application Registration Overview page	

When you click save, the Auth. Provider page opens. Copy the “Callback URL” in the “Salesforce Configuration” section near the bottom of the page. We need to enter that URL in the Azure Application registration (see section 2.3).

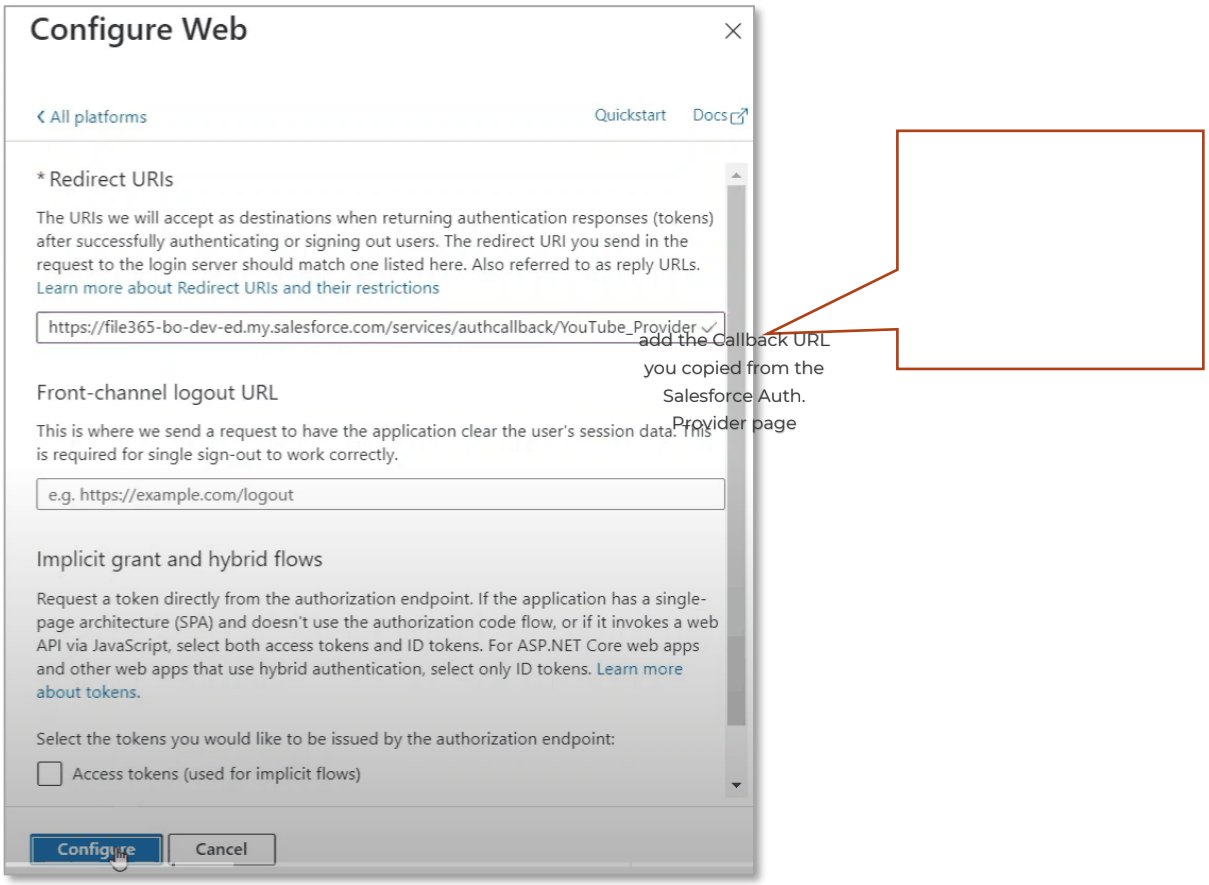


2.3 Configure in Azure AD: Add the Redirect URL to the Application Registration

Open the Application Registration you just created in Azure AD. Go to the Authentication section [1] and click “Add Platform [2] and choose Web [3].

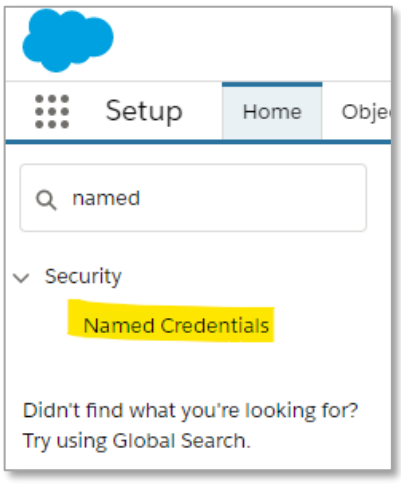


In the Web configuration, add the Callback URL you copied from the Salesforce Auth. Provider page in the Redirect URI field. Leave other options blank and click “Configure”. The Azure AD Application Registration is now complete.



2.4 Configure in Salesforce: Named Credential

Now go back to Salesforce Setup and find the “Named Credential” section in the menu. Use the dropdown arrow on the right and click New Legacy.





2.4.1 Named Credential Identity Type

Before creating a Named Credential, you will have to decide what Identity type to use. You can choose **Per User** or **Named Principal**.

2.4.1a Named Principal

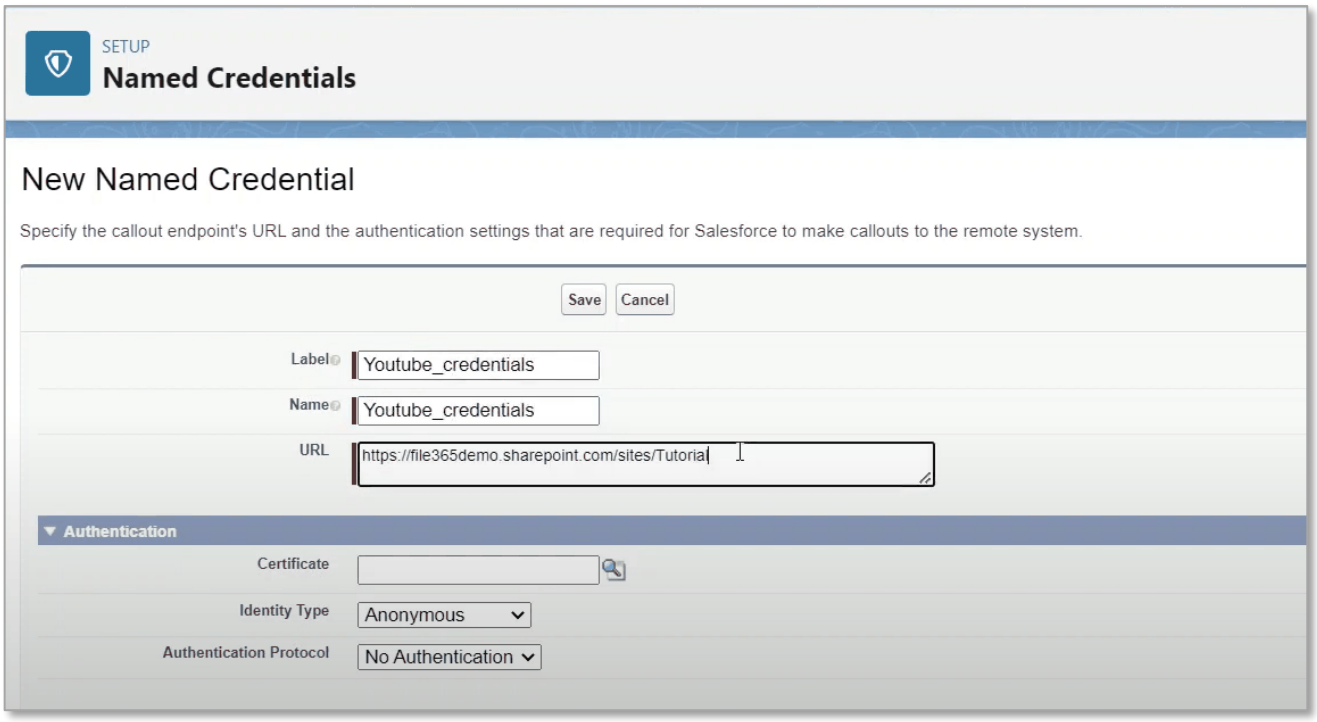
Using **Named Principal authentication and authorization** means File 365 will connect to SharePoint with the same account for all Salesforce users. This means all connections to SharePoint will be made from a single account. All Audit trails would log this account instead of the user that actually performed the actions that File 365 executes for your users.

2.4.1b Per User

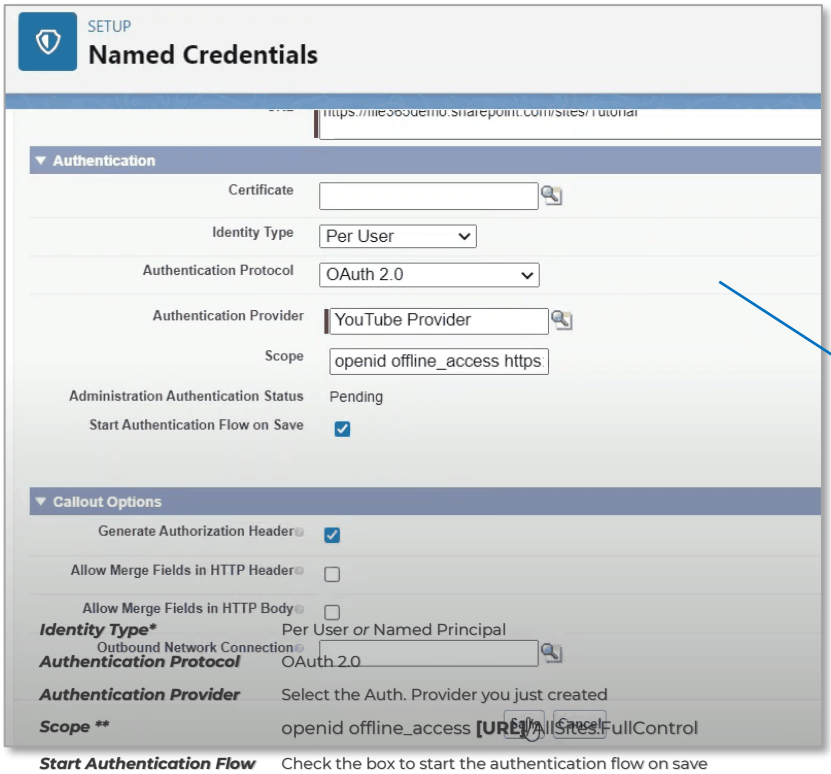
Using **Per User authentication and authorization** means File 365 will connect to SharePoint impersonating each user individually. What does this mean? Every action performed by File 365 in SharePoint will be done (from a SharePoint point of view) with the actual SharePoint user linked to their account.
For example. When a user uploads a document into Salesforce and File 365 is configured to move that document to SharePoint, the upload into SharePoint is done by impersonating the user that uploaded that document to Salesforce. Audit trails in SharePoint will show the actual username, instead of a service account.
If you choose the **Per User** Identity type, an extra step is required, which means that every user will have to authorize Salesforce to use their SharePoint credentials. How to do this is explained in the Authenticate User to SharePoint section (File 365 User Instructions paragraph 1.1).

2.4.2 Create Named Credential

Add a new Legacy Credential by clicking on the arrow next to ‘New’ and click New Legacy.
Provide a label and name for this credential. Choose a name that you and your users will recognize as your SharePoint environment. For File 365 you will create a named credential for each SharePoint site collection. The URL is the root path of your site collection. So, for example for the default Site Collection this would be: https://tenantname.sharepoint.com where “tenantname” is the name of your tenant.



Set the following values in the Authentication section:



Identity Type* Per User *or* Named Principal

Authentication Protocol OAuth 2.0

Authentication Provider Select the Auth. Provider you just created

Scope ** openid offline_access **[URL]**/.AllSites.FullControl

Start Authentication Flow on Save Check the box to start the authentication flow on save

** Identity Type : Choose Per User authentication or Named Principal (service account) for access to SharePoint (see section 2.4.1)*
***Scope: Replace **[URL]** in the Scope field by the URL to the root site collection of your own*

Leave other fields default. When you click Save, Salesforce will redirect to a Microsoft Authorization page to authorize Salesforce to use the application. If needed, login with your Microsoft administrator account to approve the authorization.

2.5 Add the SharePoint URLs to Trusted URLs

With the manual setup, the trusted URL for file previews is not created for you (the Connection Setup does this when you click Configure next to File Previews). For previews to work correctly, add every SharePoint URL you connect to the Trusted URLs in Salesforce Setup, for example https://tenantname.sharepoint.com. If you connect more than one site collection or Azure AD tenant (sections 2.6 and 2.7), add each of their URLs as well.

Follow the steps in Manage Trusted URLs in Salesforce Help. For every SharePoint URL you add, check that these CSP directives are selected:

- **frame-src** (iframe content)
- **img-src** (images)
- **media-src** (audio and video)

2.6 Multiple SharePoint Sites

You can configure File 365 to use more than one SharePoint Site Collection. You will need to create a separate Salesforce Named Credential entry for each Site Collection you want to use, as described in section 2.4. Each Named Credential should point to the root of a site collection.

2.7 Multiple Azure AD Tenants

You can also connect to multiple Azure AD tenants to use SharePoint locations in different tenants as the location to upload documents. To do this you will need to create a Microsoft Azure AD Application Registration and Salesforce Auth. Provider for all tenants you want to connect (sections 2.1 to 2.3). A Salesforce Named Credential should be created for each SharePoint Site Collection to access (section 2.4).

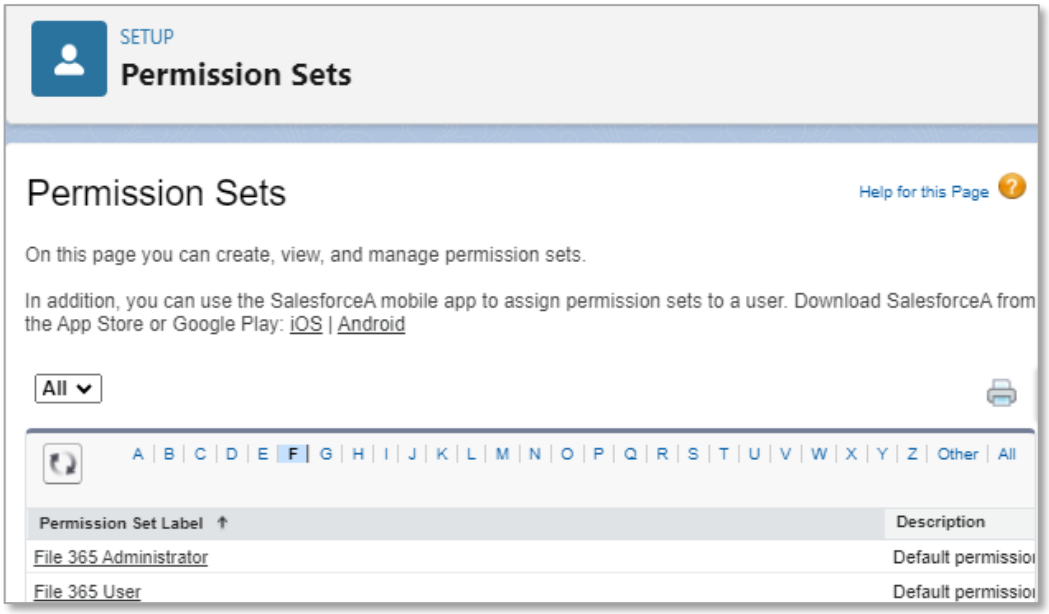
3. File 365 User permissions and licenses

3.1 License

First assign all users and administrator a license for the Package via the “Installed Package” section in Salesforce Setup by clicking Manage License next to the File 365 package.

3.2 Permission sets for Users and Administrators

File 365 creates two distinct Permission Sets on installation. One for users and one for administrators. All users that should be able to use File 365 features should be assigned the “File 365 User” permission set. These users also need access to the Named Credentials. With the Connection Setup, that access comes from the permission set with External Credential Principal Access described in section 1.3.3. With the manual setup (chapter 2), create a permission set that gives access to the Named Credential(s) you created.



We recommend creating a permission set group for all File 365 users. Add the File 365 User permission set and the permission set that gives access to the Named Credentials. Assign users to the permission set group.

Administrators that should be able to configure and troubleshoot File 365 should be assigned the “File 365 Administrator” permission set in addition to the above permission sets.

3.3 Authentication Settings for External Systems

If you use *Per User* authentication (a Per User principal assigned in the Connection Setup, see section 1.3.3, or a Per User legacy Named Credential in the manual setup, see section 2.4.1b), each user connects their own Microsoft account the first time they use File 365. See Authenticate User to SharePoint (*User Instructions* paragraph 1.1).

4. Set up SharePoint Location: Sites and Folders

4.1 SharePoint Location

File 365 works by linking files in a pre-defined folder location in SharePoint to a Salesforce record. Files uploaded to the Salesforce record are moved to this location, leaving only a reference record to the file in Salesforce, called ''File 365". For files placed into this SharePoint location reference will be automatically created in Salesforce, making it available to users in the context of the corresponding Salesforce record.

4.2 Types of File 365 Object Location

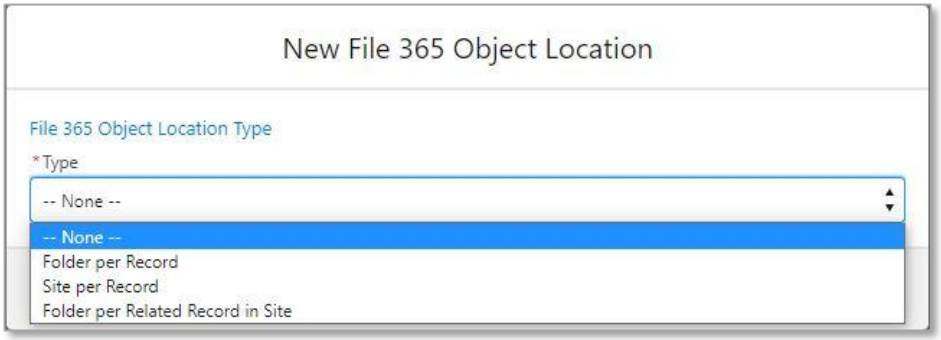
The location in SharePoint can be a SharePoint site or SharePoint folder. Creating a SharePoint site per record offers the advantages of better oversight and easier security management. Otherwise one may opt for creating folders per Record. The "Site per Record type" can be used in combination with a third configuration type : "Folder per Related Record in Site", to store files of related child records in subfolders of parent site.

By using scripting and site templates in SharePoint you can create sites with a standard layout and predefined rights. Contact your SharePoint administrator for more information.

4.3 Create a File 365 SObject Location

As File 365 Administrator, you control the location where files attached to Salesforce objects will be placed within SharePoint. This configuration is done by creating one or more "File 365 SObject Location" record(s). How to create an object location will be explained hereafter. After you have created an SObject Location, make sure to deploy the Apex Trigger and Apex Testclass for this object, see paragraph 4.7

Create at least one "File 365 SObject Location". Open the "File 365 Administrator" Salesforce App and select the tab "File 365 SObject Locations". Click New to add a new configuration record. First select the type of SObject Location: **Folder per record**, **Site per Record** or **Folder per related Record in Site**.



4.4 File 365 Object Location type (1): Folder per Record

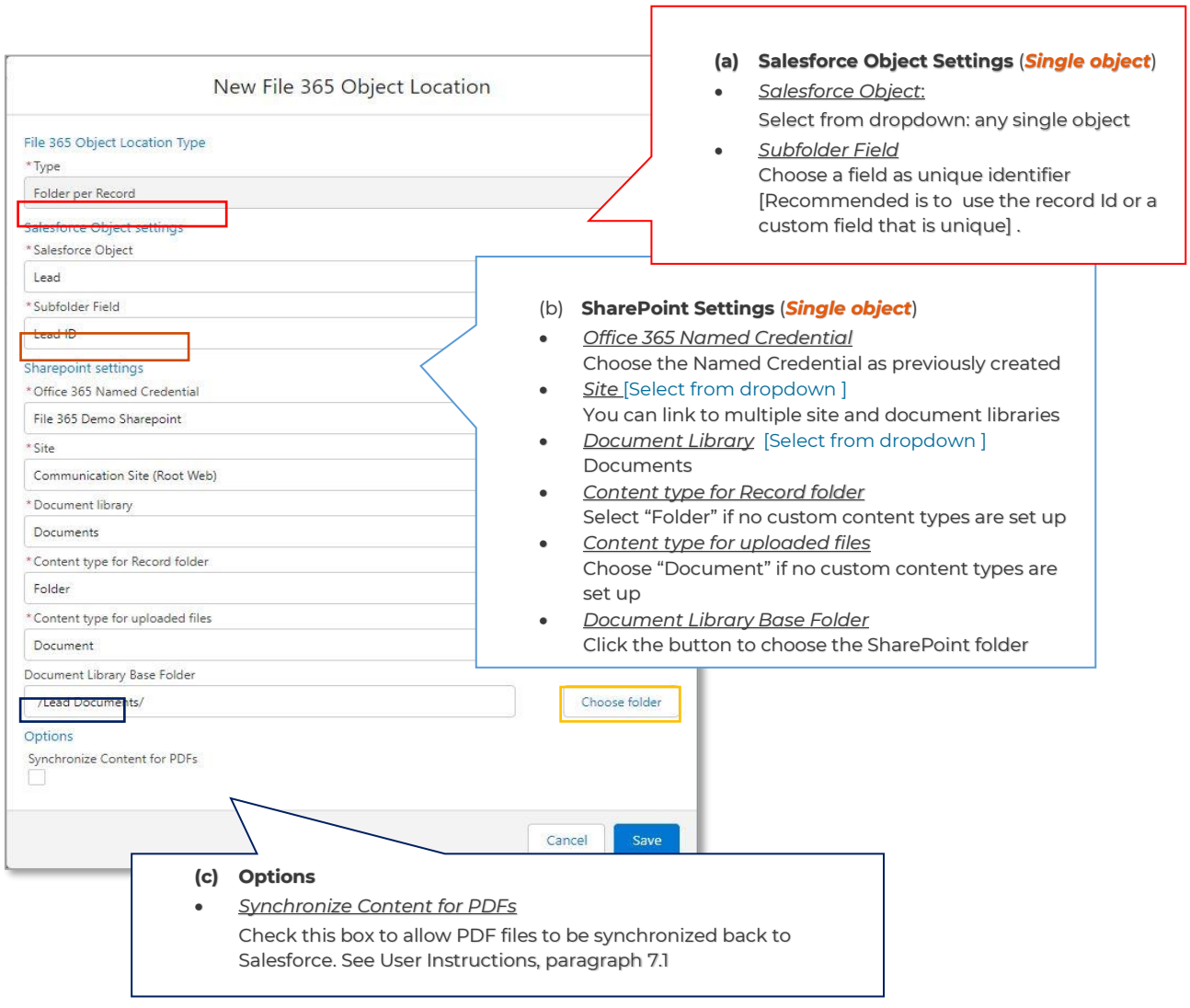
4.4.1 Salesforce Object Settings: Single or All

After selecting the type [in this case Folder per record], we will define the Salesforce Object and the SharePoint settings

You can choose to select a ***single*** Salesforce Object to define the settings for each object one by one. Or you can select "***All*** (wildcard)" to apply the setting to more than one Object. We will come back to this setting in paragraph 4.4.4.

4.4.2 Single Object: Salesforce Object settings

If you choose a Single Object type, first select the object you want to connect. You can select any standard or custom object. Next, you need to choose the "Subfolder Field". This is the field that will be used to create and identify the subfolder for each Salesforce record. This subfolder name needs to be unique, so only Unique or Autogenerated fields are listed to choose from. We recommend to use the Id field or to create a custom field that is unique and recognizable, as this will be the name of the SharePoint folder.



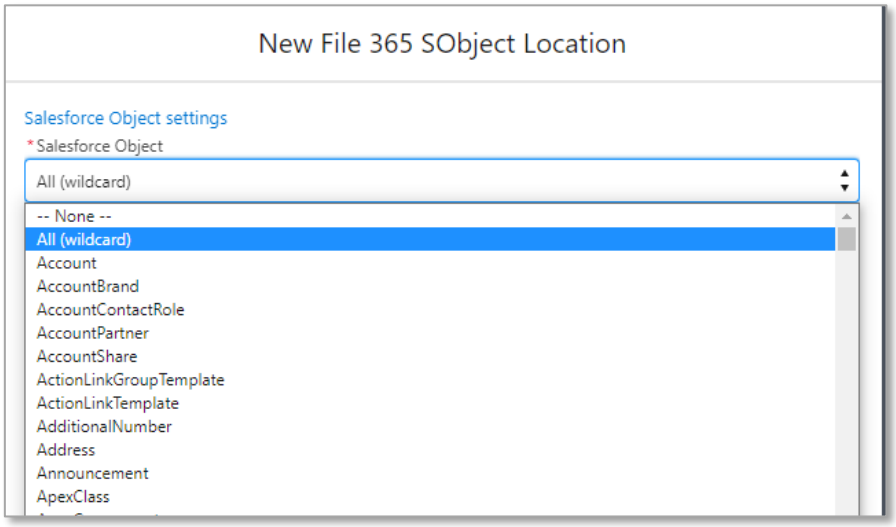
4.4.3 Single Object: SharePoint Settings

To specify the SharePoint location, first choose the Named Credential to use. You should select (one of) the Named Credentials you created during setup. Now the existing Sites on the SharePoint Site Collection are loaded so you can choose the root- or subsite to use. After selecting the site the existing Document Libraries are loaded, choose the one to use.
If you are using custom content types in the Document Library, you can select those in the Content Type selections. If not, just select Folder and Document respectively as the Content Types to use.
In the last field you can specify an existing SharePoint folder as the base location. File 365 will use that base folder to start building its own tree.

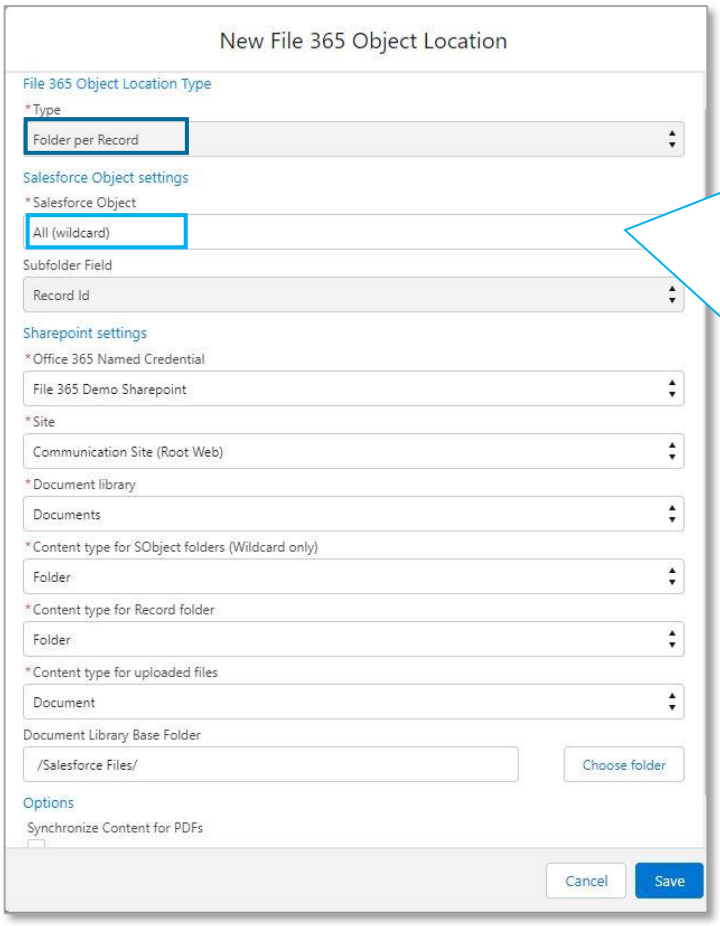
4.4.4 All (wildcard) settings

Instead of creating an SObject Location for each Salesforce object separately, you have an option to direct all files for multiple Salesforce Objects to the same SharePoint location. For this, you need to select the option “All (wildcard)” in the Salesforce Object settings.
This is essentially a fallback option, allowing you to specify one SharePoint location for multiple Salesforce Objects.

The All (wildcard) option is at the top of the dropdown list under Salesforce Object**.**



Salesforce Object Settings for wildcard
Note: When you create an Object location with All (wildcard) setting, you are *not* able to choose an identifier for the subfolder field, the **Record Id** must be used.



Salesforce Settings (Wildcard)
Salesforce Settings (***Wildcard***)
When you choose All (wildcard), you are not able to choose an identifier for the subfolder field, the *Record Id* must be used

SharePoint Settings (***Wildcard***)
Same as under Salesforce single object, except:

Content type for SObject (not available for single object)
[Select] Documents

Document Library Base Folder
Choose the SharePoint base folder where you want the files to be stored.

4.4.5 SharePoint Folder structure: single object vs wildcard setting

On the selected SharePoint folder a subfolder will be created with the Label of the Salesforce Object. In this *object* subfolder, another level of subfolders will be created with the name set to unique identifier of the Salesforce *Record*. The difference in structure between a single Salesforce object and the "wild card" setting, is illustrated by the following examples:

Example 1: Single Salesforce Object
You selected the Account object as Salesforce Object and an existing unique field "Account Code" as Subfolder Field.
The selected SharePoint Settings are the site collection https://company.sharepoint.com and the default "Documents" Document Library. You created a pre-created [SharePoint] folder "**Account Files**" in the Document Library.
If you now add a file "**contract.pdf**" to an Account Record with Account Code "**DS-05401**", the file will be moved to the SharePoint Location:

Site: https://company.sharepoint.com
Document Library: Documents
File location: **/Account Files/DS-05401/contract.pdf**

Example 2: All (wildcard) Salesforce Object Setting
You selected the Account object as Salesforce Object. The Record Id will be used for the Subfolder field.

The selected SharePoint Settings are the site collection https://company.sharepoint.com and the default “Documents” Document Library. You pre-created a [SharePoint] folder “**Salesforce Files**” in the Document Library.
If you now add a file “**contract.pdf**” to an Account Record with Record Id “**0015528a4328665AAA**”, the file will be moved to the SharePoint Location:

Site:	https://company.sharepoint.com
Document Library:	Documents
File location:	**/Salesforce Files/Account/ 0015528a4328665AAA/contract.pdf**

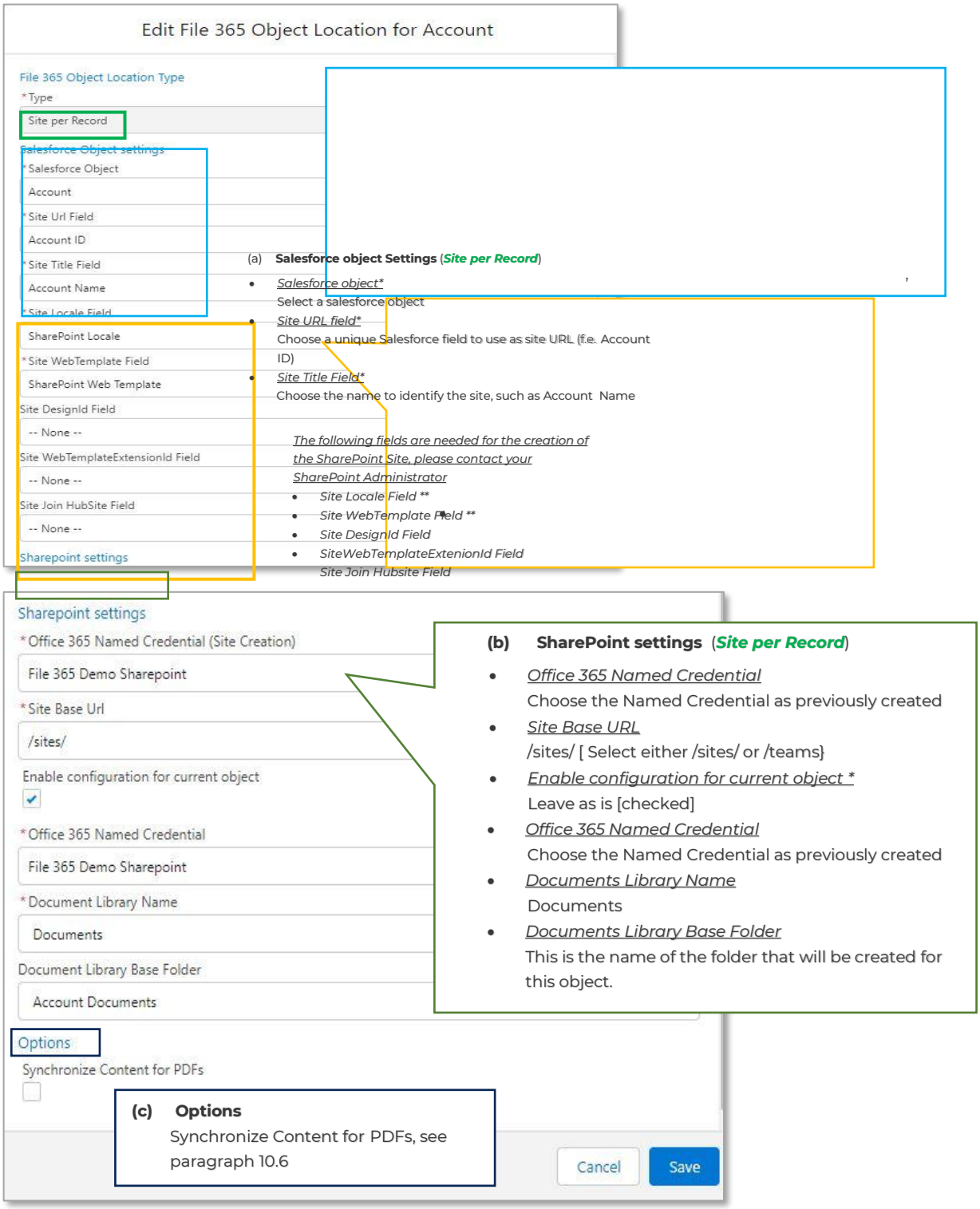
4.5 File 365 Object location type (2): Site per record

Instead of storing all files associated to object records in one SharePoint folder, it is possible to store all files of one record in a separate SharePoint site. For this we created the Object location type Site per Record.

After Choosing the Salesforce Object, choose the Site URL field. This field must be a unique identifier for the SharePoint Site. You can use the Record Id (f.e. Account ID if you want to create a SharePoint site per Account) or create a custom field that is unique (Auto number are always unique). You can fill this field automatically with a flow or formula, as long as it's always unique. After creating the unique field you can select this field in File 365 Object Location.

Make sure you fill this field for all records after creating the field, otherwise you will get error messages when fields are left blank and you want to upload files. If you already uploaded files make sure you change the existing folder names to the field value on the corresponding account records. Naming of the SharePoint folders works the same for al objects. So make sure you define this URL Field thoughtfully before you start configuring File 365 for the object. Especially when users need to access files through SharePoint, naming folders with recognizable names makes sense.

Next, fill out the other Salesforce Object settings as described in the illustration below.
Note that certain fields are needed for the creation of the SharePoint Site. We recommend to contact your SharePoint Administrator. Site Locale Field and Site WebTemplate are required fields; these field has to be created on the object first in order to be selected here.

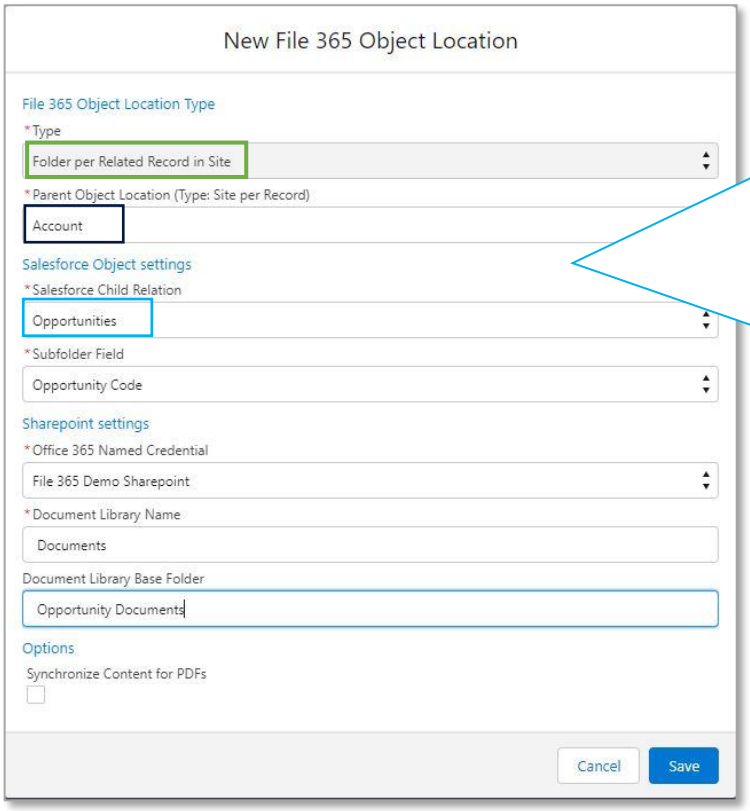


4.6 File 365 Object location type (3): Folder per related Record in Site

After setting up an Object location of the type Site per Record, it is possible to store files of related child records in subfolders of the parent site. To do this we must choose the Folder per related Record

in Site. In this way, we can store related Opportunity files, Contract files or Case files in the parent Account site.

After choosing the **Folder per Related Record in Site** type, configure the Salesforce and SharePoint settings as follows:



Salesforce Settings (Wildcard)
File 365 Object Location Type (***Folder per Related Record in Site***)

- *Parent Object Location*
  Select the parent object [Account]

Salesforce Object settings

- *Salesforce Child Relation*
  Select the Child object [f.e. Opportunities]
- *Subfolder Field*
  Choose a unique field to identify the record [e.g. Oppty Code, Case Nr]

SharePoint settings
Same as for Site Per Record, except:

- *Document Library Base Folder*
  This is the name of the **folder** that will be created for this child object in the SharePoint site

Click save to save the settings. The notation for this kind of Object Location is **Parentobject.Childobject**. So in the above example the created Object Location record is **Account.Opportunities**.

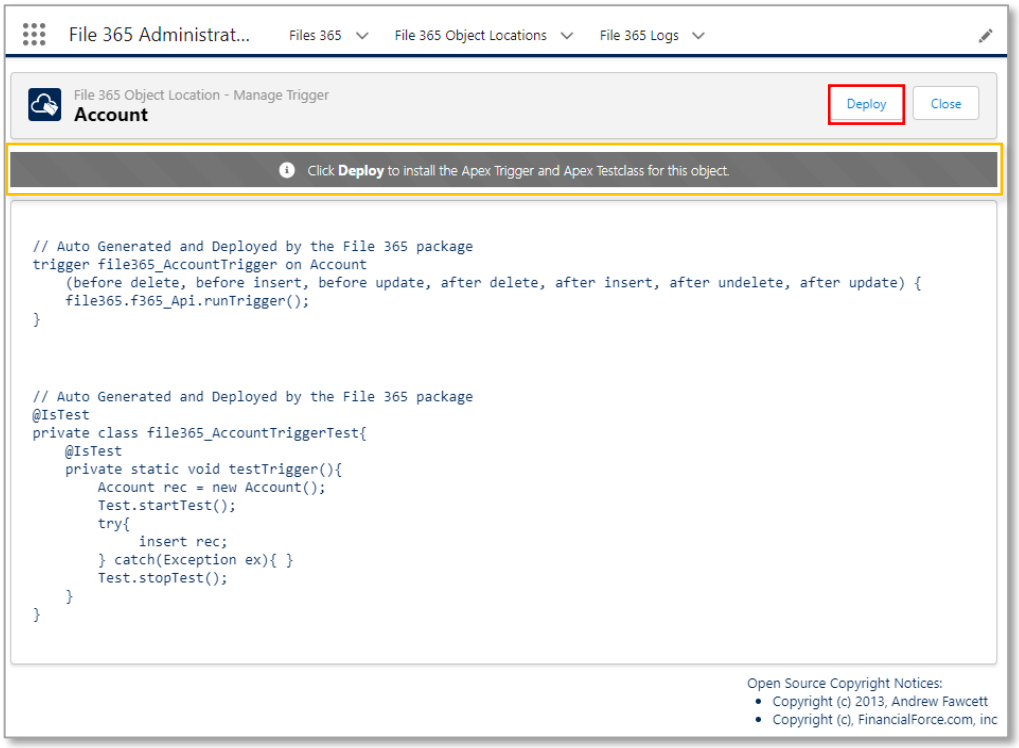
4.7 File 365 Object location: Deployment of necessary Apex Triggers

After the creation of a File 365 Object Location, it is necessary to deploy an Apex Trigger for every object that you configured with File 365. These triggers are necessary for advanced functionalities, such as merging records and renaming files and folders. Make sure you deploy the Apex Trigger for all Object Locations. *(Note: This section only applies to File 365 version 4.7.4 and higher. If you use a lower version no further action is required and you can continue using File 365.)*

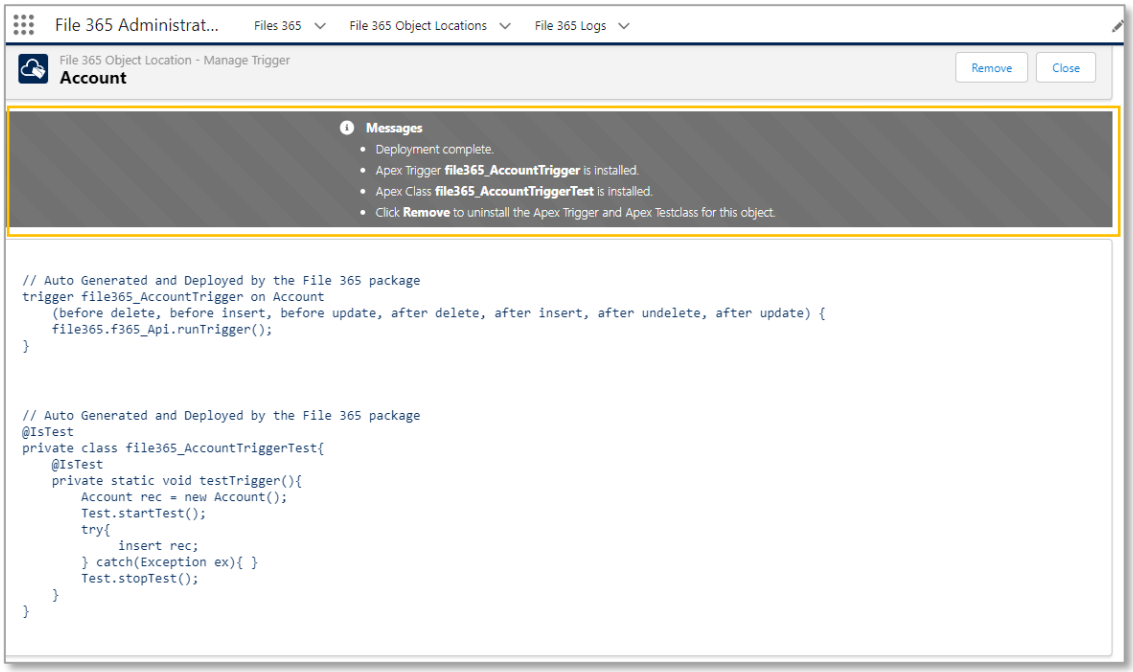
Installing the Apex Trigger can be done in a few simple steps. From the File 365 Object location you just created, click on the **Manage Trigger** button in the menu on the top right.



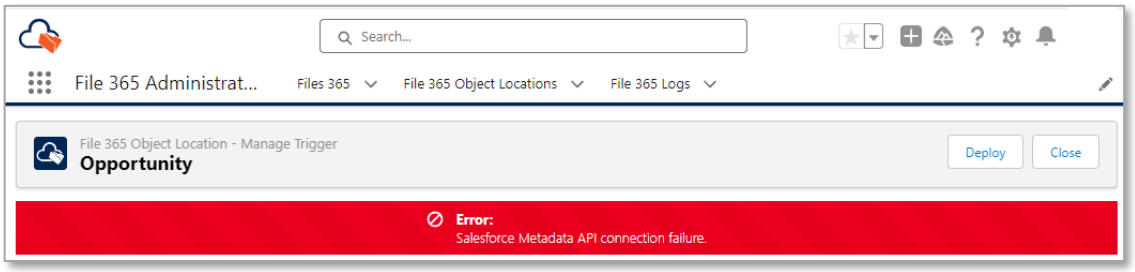
In the pop-up screen, click on the button **Deploy** to install the Apex Trigger and Apex Test class for this object.



After clicking on Deploy, you will see a message that the Deployment is complete and the Apex Trigger and Apex Test class has been installed. If necessary, the Apex Trigger and Test Class can be uninstalled with the button **Remove**.



Finally, deploying triggers can only be done by a user who has File 365 administrator permission. If you try to deploy as a user you will see the following error message.

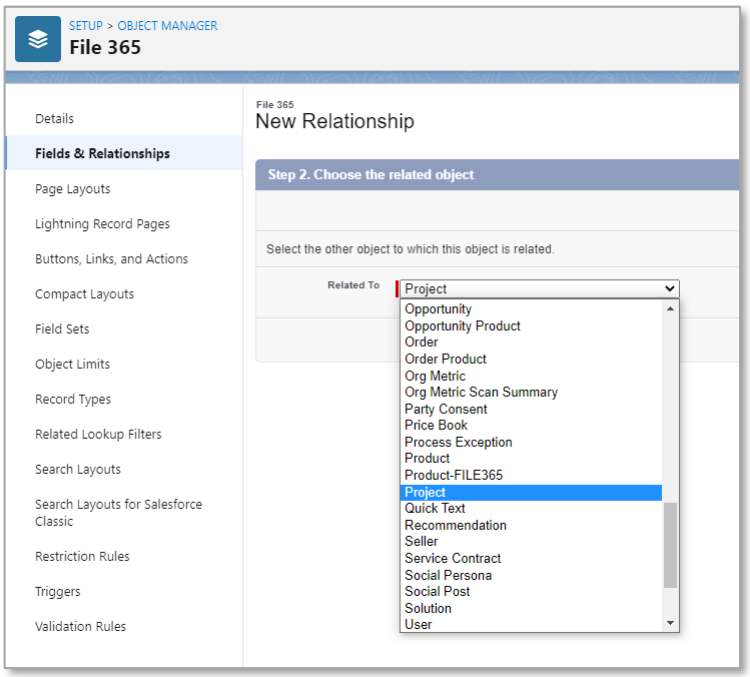


5. Set up File 365 in the User Interface

For each file in SharePoint a File 365 record will be created. To link the File 365 record to your Salesforce Objects, a lookup relation must be added to the File 365 record. Even if you specify the “All (wildcard)” option, you must add a lookup relationship to the File 365 object for all the Salesforce objects you want to use with File 365. Only for those objects that are linked to the File 365 object, File 365 will be active.

5.1 Create a File 365 Lookup Field

Go to Salesforce Setup and select the Object Manager. Search for the Object “File 365” (API: file365__f365_File365__c) and open the settings for that object. Go to “Fields & Relationships” and click ***New*** to add a new relationship.



Select Lookup Relationship and select Next. Choose the Object* to create the lookup relation to. This is the same Object as selected before in the “New File 365 SObject Location” screen. Set a custom label, name and child relationship name if needed.

You can leave other settings default and click Next. In the next screen select all profiles needing access to this relationship. On the next screen, where you can add the field to existing Page layouts, you should deselect all layouts and click Next.

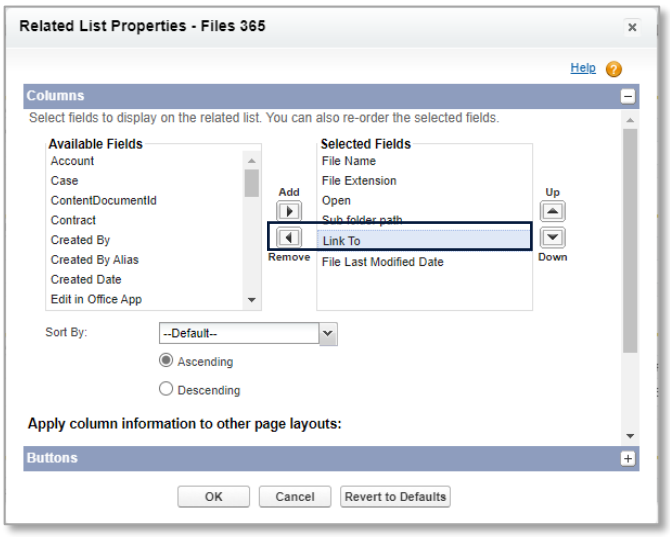
The last step is to add a “Files 365” related list to the existing layouts of your chosen object. Check all layouts where you want to see the related File 365 records and click Save.

5.2 Modify Page Layouts and Lightning Record Page

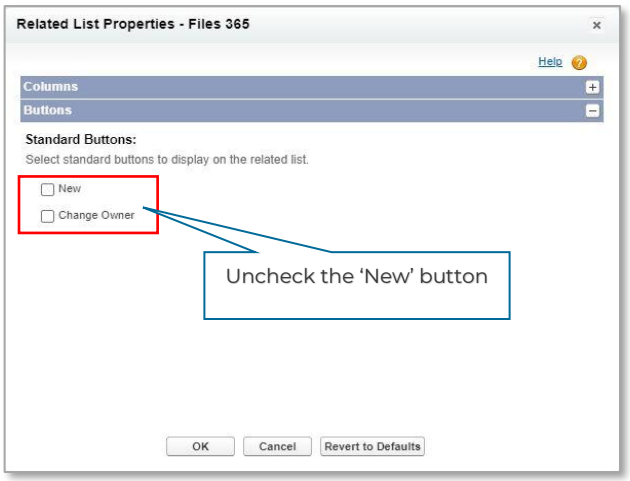
To use all features of File 365, ensure you add the following components specified below on the page layout(s) and Lightning Record pages as described in this section.

5.2.1 Page layout: Add and configure File 365 Related List

Add the File 365 Related List to the Page layout of the concerned object. When you created the lookup relationship as described above, you added the related list already on the last step of the field creation wizard.



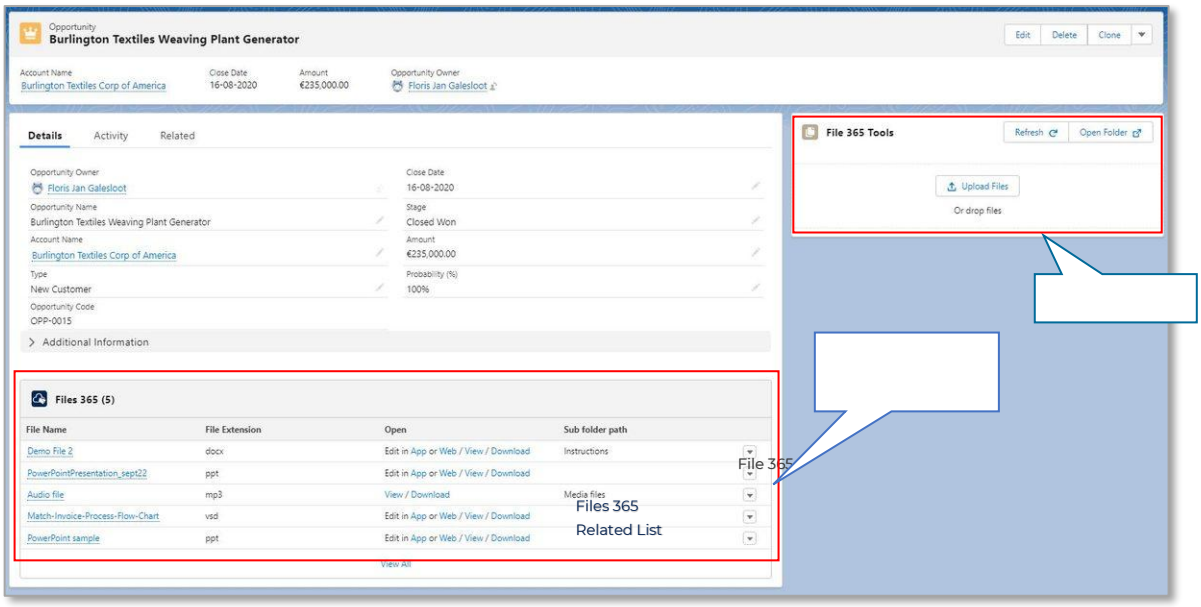
By default, in the File 365 related lists shows the Columns **File Name**, **File Extension**, **Open**, **Subfolder Path**, **Link To** and **File Last Modified Date**. As with all related lists, the administrator can configure which fields are shown in the File 365 related List. We recommend to remove the 'Link To' field, as the related list is already on the page layout of the affiliated record.



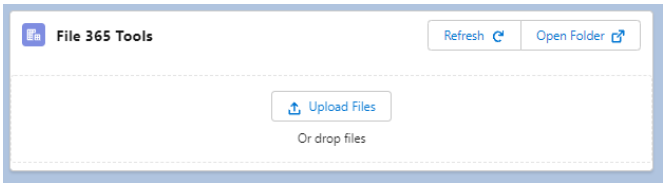
Always uncheck the "New" and Change Owner buttons from the File 365 related list. These should not be used by users.

5.2.2 Lightning Record page: Add the File 365 Related List component, File 365 Toolbox

You need to add two lightning components to the record page of the object you have configured to use File 365. First you need to add a **File 365 Related list component**. You can either show the Files 365 Related list in the Related Tab (in this case you do not need to do anything) or choose to add Single Related list component from the lightning components menu. Select File 365 as the related list you want to show in the lightning component.



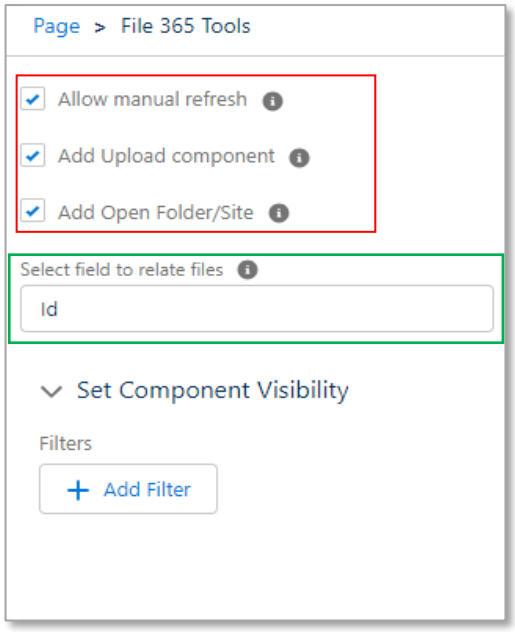
Second, add the **File 365 Tools** lightning component to your Lightning Record Pages for all the objects you configured.



The toolbox has three buttons. The **Upload Files**, the **Refresh** and the **Open Folder** button.

The **Upload Files** button allows the user to upload files to the related SharePoint folder. Uploading works also by using File Drag-and-drop to the toolbox.

The **Open folder** button opens the active record folder in SharePoint in a new browser tab, this is available by default. With the **Refresh** button you can refresh the file 365 related list after uploading files in Salesforce. Clicking this button will get all information from SharePoint linked to the record opened and create or update File 365 records accordingly.



After adding the Toolbox component to the lightning record page in the settings of the Toolbox component, you need to tick the checkboxes for Manual Refresh, the Upload, and Add Open Folder/Site component to show these buttons.

Select Field to relate Files

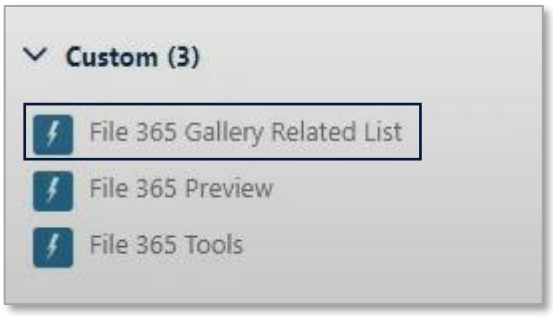
Default setting is **Id** for relating files to the record you are viewing. Alternative is to use a master-detail or look-up field to relate the file to a related record. (This property supports using an expression to define its custom label. The correct format is {!$Label.customLabelName}.)

If you want to show both the files related to the active record as well as files of a related record (the parent record f.e.), you need to add the toolbox *twice* and configure the 'Select Field to relate Files' accordingly. Note that adding

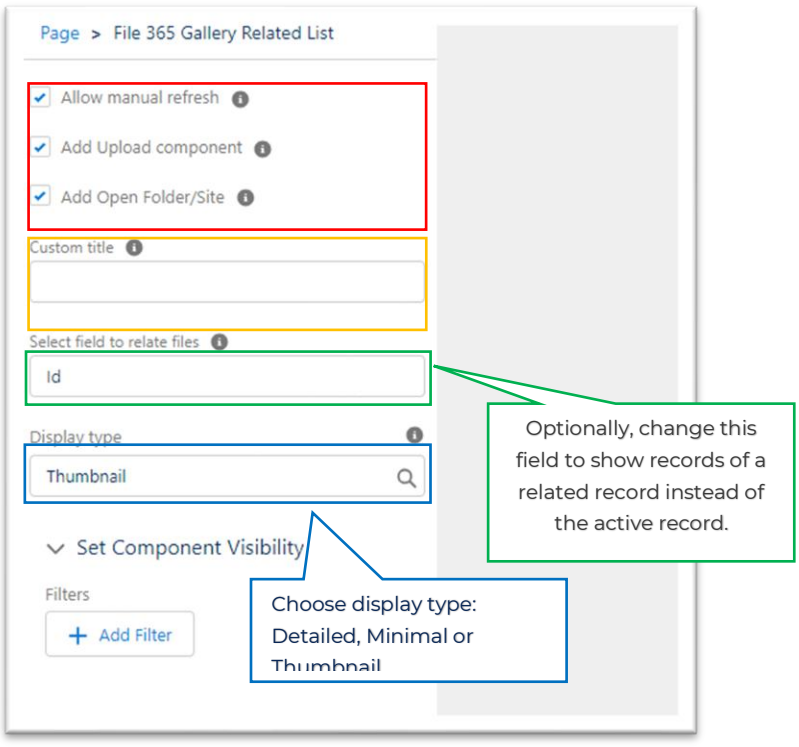
an extra toolbox is only necessary if you use the ***standard*** File 365 Related list. As the **File 365 Gallery Related List** component (see paragraph 5.2.3) features an upload button, the **Select Field to relate Files** can be configured in the settings of the File 365 Gallery Component itself. As should be clear, you do need to add the Gallery Component twice to show the two different sets of files.

5.2.3 Lightning Record page: File 365 Gallery Related List

To preview multiple related files in one glance, we have added a new type of Related List: the **File 365 Gallery Related List**. To use this, drag the 'File 365 Gallery Related List from the Custom Lighting components list onto the lightning record page.



File Gallery Related List component features all three buttons of the File 365 Toolbox (Upload Files, Refresh and Open Folder), so adding the toolbox to the record page is unnecessary if you use this type of Related list.



After adding the File 365 Gallery component, click on the component to show the component details in the right side bar.

Tick the checkboxes for **Manual Refresh**, the **Upload**, and **Add Open Folder/Site** component to show these buttons.

Optionally, add a custom title.

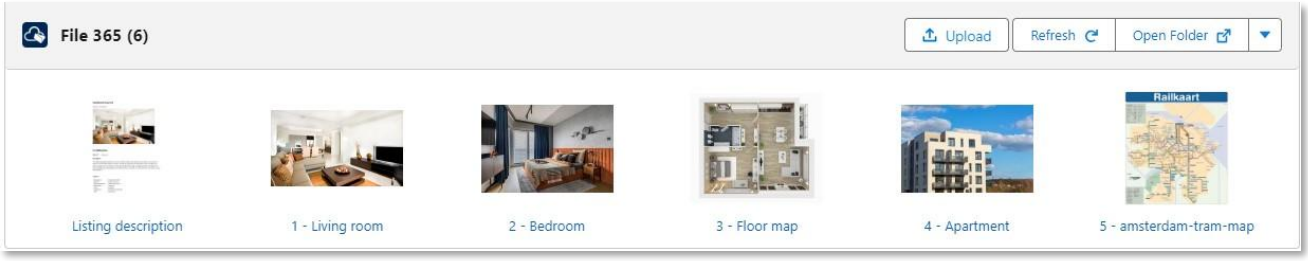
As explained in the previous paragraph, the Field '**Select field to relate files**' is used to determine which related files will be shown. Default for this field is **Id** to show the files of the active record. Optionally, a second File 365 Gallery Related List component can be added to the record page to show files of a *related* record instead of the active record, for example to show Account files on the Opportunity record. To do this, change the field name in '**Select**

field to relate files' to the field name (developer name) of the lookup field, in this case "AccountId". (For detailed information how to set this up, view the File 365 Gallery tutorial).

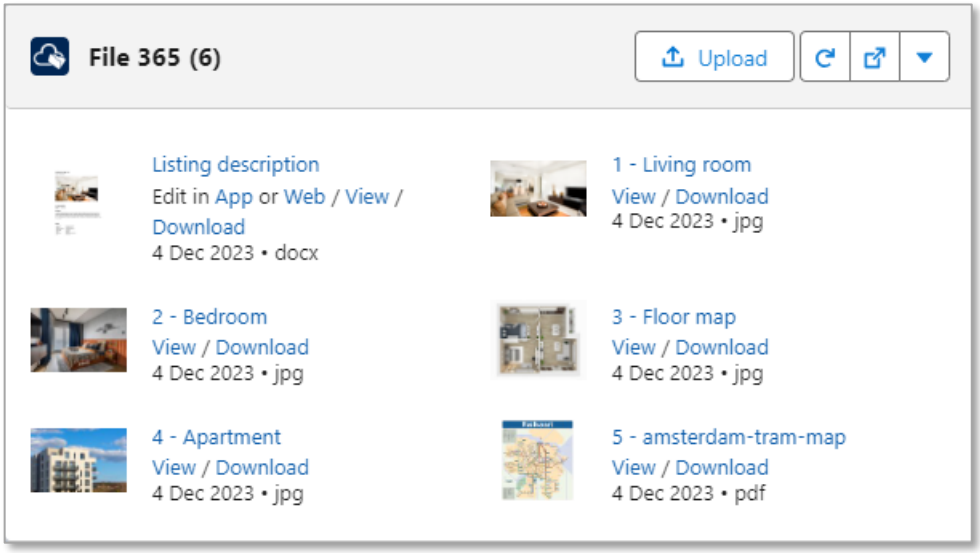


Choose a Display type to show more or less file details: Detailed, Minimal and Thumbnail. **Minimal** only shows a thumbnail. **Thumbnail** only shows the thumbnail and file name. With the **Detailed** type you can show File name, and additionally, File extension, Last Modified Date & SharePoint links.

File Gallery with Thumbnail display settings



File Gallery with Detailed display settings



6. File 365 Document Templates

Optionally, you can create Document Templates on an Object Location to make standard documents immediately available for users upon creation of a new record, for example a new contract. These document templates can then be used by the users as starting point for further editing.
As always File 365 will store the file in SharePoint and only leave a reference file in Salesforce, but the file can be opened/edited immediately in Salesforce by clicking on a link to open the file in SharePoint.

6.1 Set up File 365 Document Templates

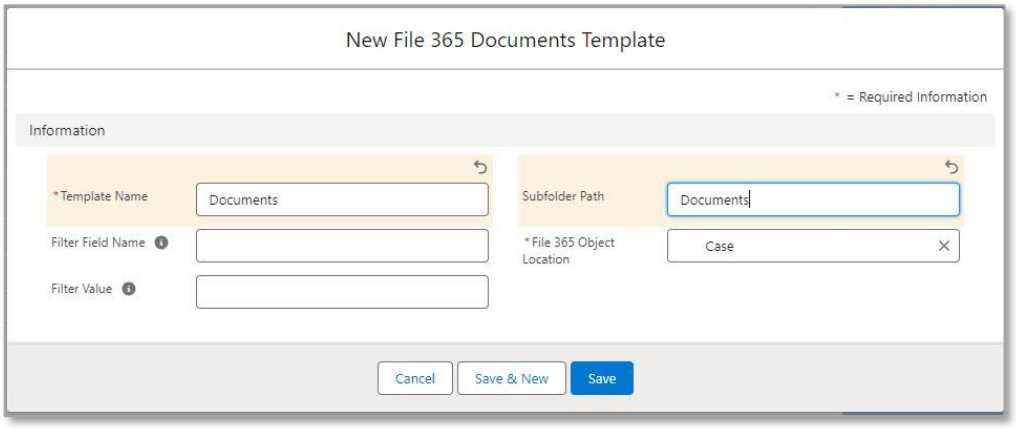
Document templates can be configured only by a user with File 365 administrator permission in the File 365 Administration app.

The first step is to create a File 365 Document Template Record. Go to the File 365 Object Location tab. Select the Object Location of the object for which you want to make the Document Template available. Click the dropdown arrow on in the File 365 Documents Template at the top right and click “New” .

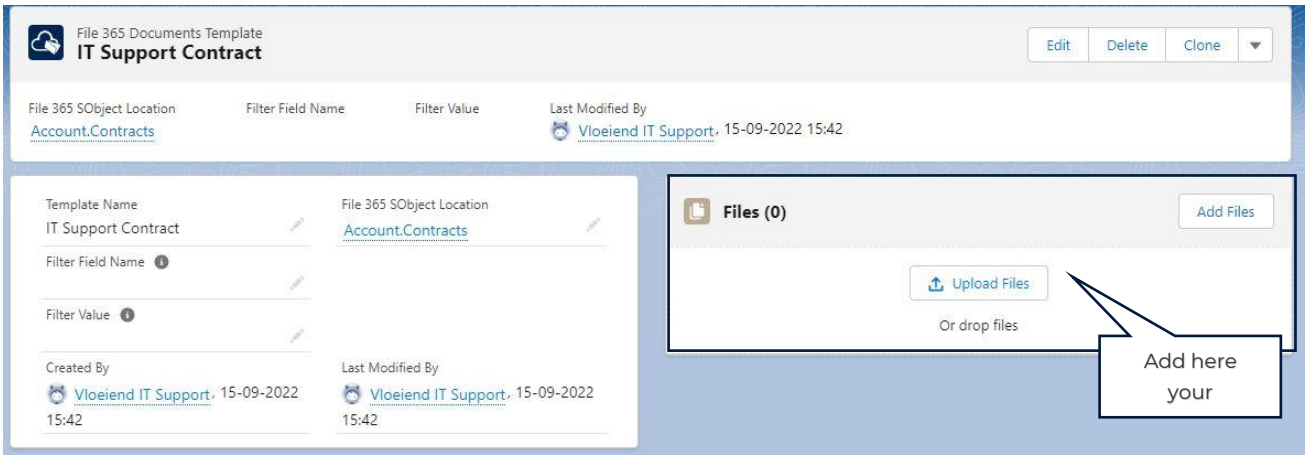


In the New File 365 Document Template screen fill out the necessary fields:

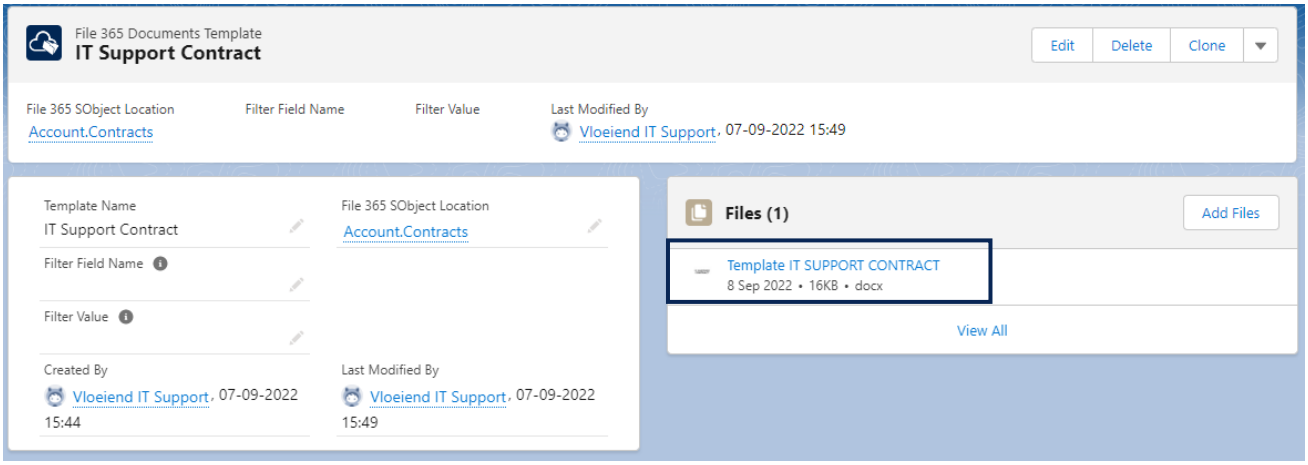
Template Name: Template Name is the only required field.
Subfolder path: If templates should be created in a subfolder fill in the Subfolder Path field.
Filter Field Name, Filter Value Optionally specify a Filter Field Name and Filter Value to determine if the document template should be available for all records. If no Filter is specified, the template is applied to all records
File 365 Object Location This field will be prefilled.



Click **Save** to save the Document Template record.



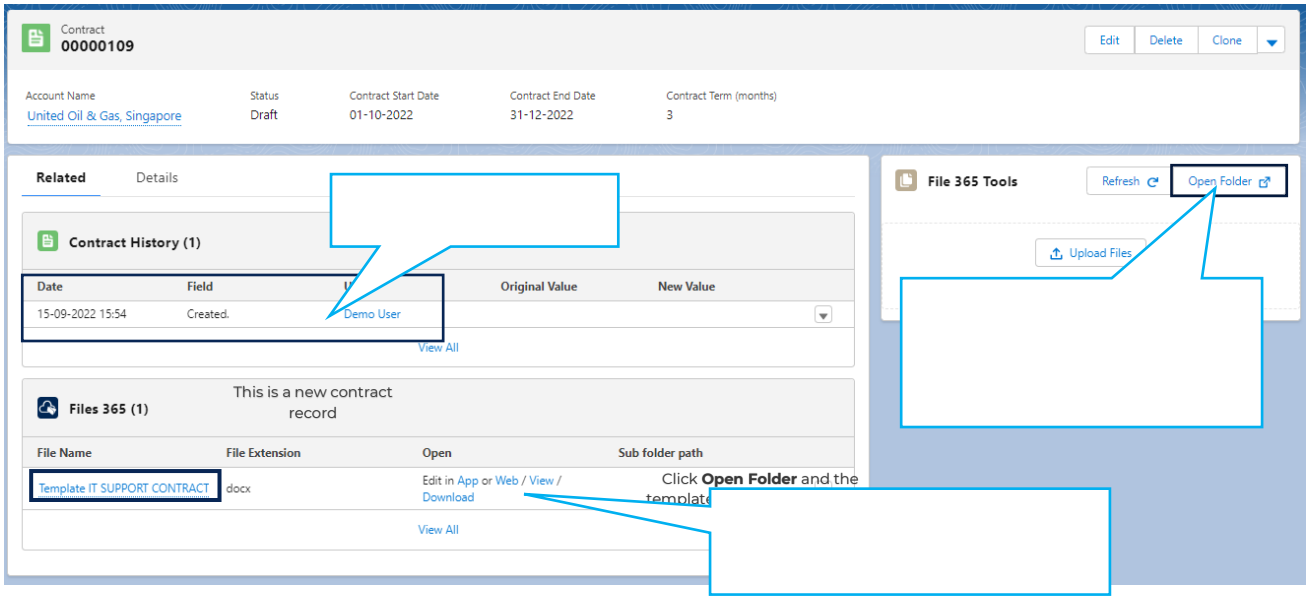
The second step is to upload the template files. In the created Document Template record, upload or add by drag-and-drop the desired files from your work station to the File 365 toolbox. After upload you should see the files.



The process can be repeated if you wish to make different templates, depending on the Filter Field, available for the chosen object.

By default File 365 only creates the document templates and subfolders after the first file is uploaded or the user clicks the Open Folder button in the File 365 Toolbox or Gallery List. This prevents the creation of large numbers of empty folders or unused template documents.
Contact our support team if you need to customize the behavior of the template document Apex Triggers.

Note that there will be a short time interval between the creation of the Salesforce record and the moment template can be seen in SharePoint or as a File 365 file. This may take up to 2 minutes.



You only need to click Open Folder the first time after creating a new record. The next time, you can access the template directly from Salesforce from the File 365 Related List. Open and edit the document with one click.

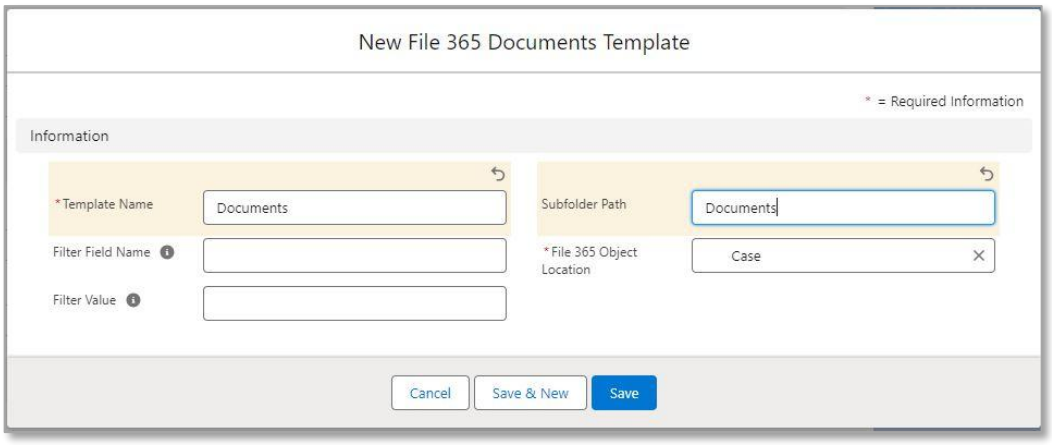
6.2 Automatically create subfolders with the Subfolder Path

To organize record files in a consistent way, File 365 can be configured to automatically create standard subfolders in the main folder for each record of the concerned object. To do this you need to create a document template on the File 365 Object location.

In the File 365 Administration app, go to the File 365 Object Location tab. Select the Object Location of the object for which you want to create a Document Template. Click the dropdown arrow in the File 365 Documents Template at the top right and click “New” .

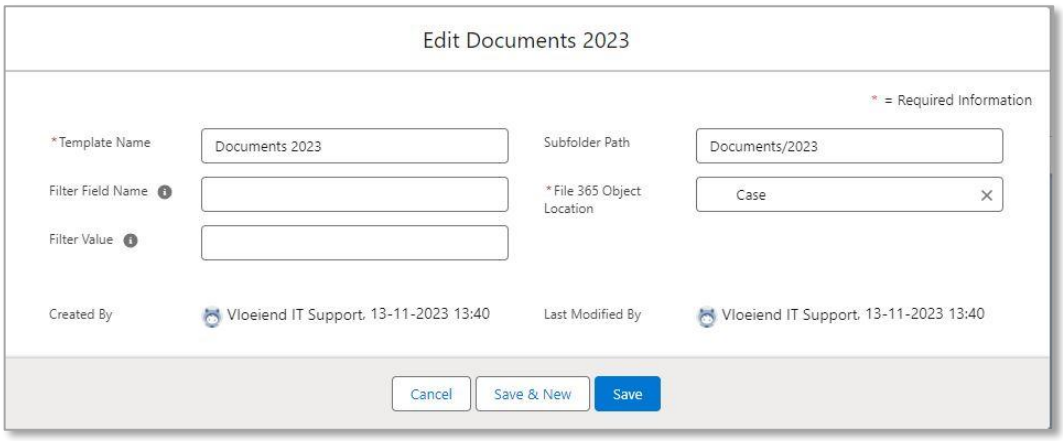


In the New File 365 Document Template screen, fill out the necessary fields.
Fill in **Template Name** and Subfolder Path. The Object Location is prefilled. Optionally specify a Filter Field Name and Filter Value to determine if the document template should be available for all records. If no Filter is specified, the template is applied to all records.

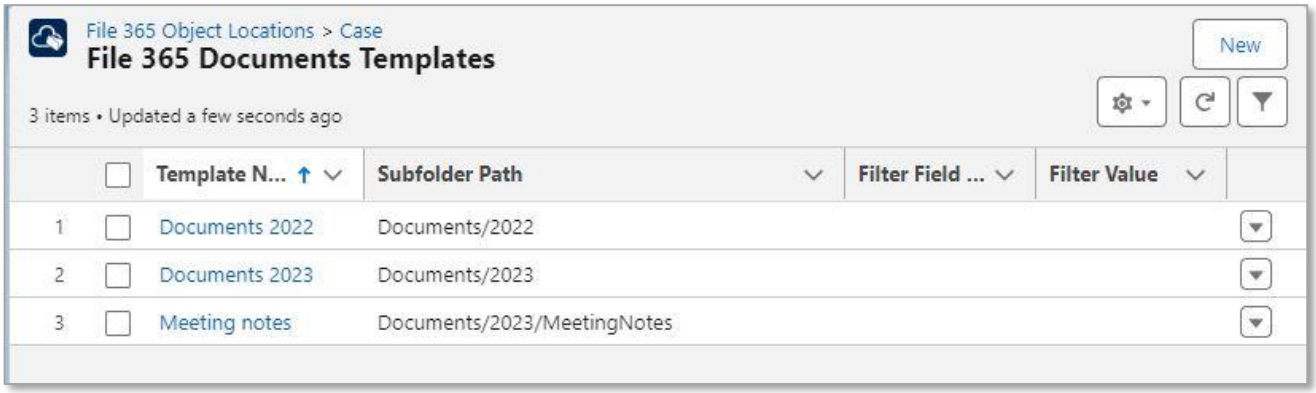


Click Save to save the Document Template record.

It is possible to create different levels of subfolders by using the forward slash as a separator in the Subfolder Path field. For example in the above example, Documents/2023 will create two folders at once for each new case record.



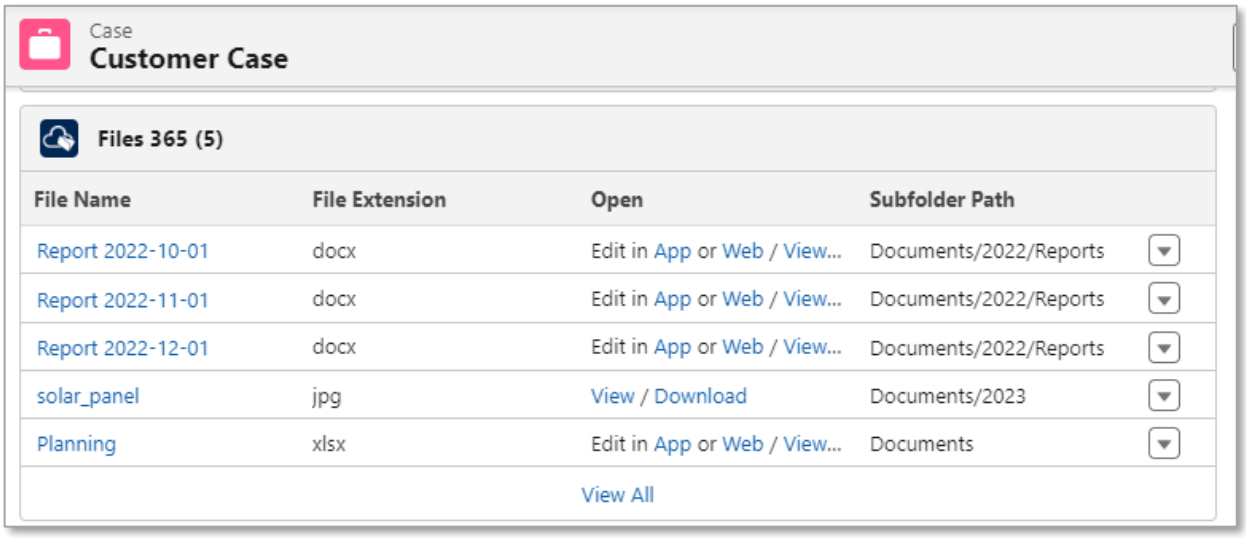
Several document templates can be added to the same File 365 object location to create a hierarchical folder structure.



The specified subfolder will be created only for a newly created records. After creating the record, the user has to upload a file or click **Open Folder** in the File 365 component of the new record and the

process will be started. *Note that there will be a short time interval between the creation of the Salesforce record and the moment subfolder or subfolders can be seen in SharePoint. This may take up to 2 minutes. To speed up the process, refresh the page in SharePoint.*

After files have been uploaded to the record (either via Salesforce or SharePoint), the subfolder path will be shown in the File 365 Related list under the Subfolder Path column.



7. File 365 Administration App

7.1 File 365 Status

When a record is configured for File 365, a File 365 record will be created immediately after the upload of the document to Salesforce. In the background an asynchronous process will process the file (upload to SharePoint) according to the settings you specified.
When the file is not uploaded yet to SharePoint, the File 365 record has the status “Queued”. In the File 365 Administration App you can select a List View that will display all File 365 records queued for upload to SharePoint.
When an error occurs during upload, the status changes to “Error”. For those record there also is a List view in the File 365 Administration App. When you have fixed the error (or simply want to try the upload again), click the Retry button.
Note: When clicking Retry as administrator and using the Named Credential identity type per user, the file will be uploaded to SharePoint using your credentials instead of the users’ own credentials.

7.2 General Application log

When an error occurs in the File 365 application, those errors will be logged in the File 365 Log Object. You can view those logs on the File 365 Administration App.

7.3 Resolving Errors

If you cannot resolve an error yourself, please contact our support team by using the Support form on our website or send an email to support@file365.nl .

Optional configuration and Release updates

Check the Knowledge Base for more optional setup configuration and the Release Notes for the latest features and enhancements on our website www.file365.nl.

User Instructions

After successfully installing File 365, please consult the **File 365 User Instructions** for further information.

Appendix A

SharePoint supported languages, culture names and locale IDs

Language Name	Culture Name	Locale ID
Arabic	ar-sa	1025
Bulgarian	bg-bg	1026
Catalan	ca-es	1027
Croatian	hr-hr	1050
Czech	cs-cz	1029
Danish	da-dk	1030
Dutch	nl-nl	1043
English	en-us	1033
Estonian	et-ee	1061
Finnish	fi-fi	1035
French	fr-fr	1036
German	de-de	1031
Greek	el-gr	1032
Hebrew	he-il	1037
Hindi	hi-in	1081
Hungarian	hu-hu	1038
Italian	it-it	1040
Japanese	ja-jp	1041
Kazakh	kk-kz	1087
Korean	ko-kr	1042
Latvian	lv-lv	1062
Lithuanian	lt-lt	1063
Norwegian (Bokmål)	nb-no	1044
Polish	pl-pl	1045
Portuguese (Brazil)	pt-br	1046
Portuguese (Portugal)	pt-pt	2070
Romanian	ro-ro	1048
Russian	ru-ru	1049
Serbian (Latin)	sr-latn-cs	2074
Slovak	sk-sk	1051
Slovenian	sl-si	1060
Spanish	es-es	3082
Swedish	sv-se	1053
Thai	th-th	1054
Turkish	tr-tr	1055
Ukrainian	uk-ua	1058

SharePoint Online Site Template ID

Template ID	Title	Description / Additional Info
STS#3	Team site (no Office 365 group)	A site with no connection to an Office 365 Group.