



Files Connect Setup Guide Winter'17 (“204”)

Version	Description
March 25th 2016	<ul style="list-style-type: none">Created from Summer'16 documentation.

Contents

[1. Related documents & videos](#)

[1.1. Documents](#)

[1.2. Videos](#)

[2. What's new in Winter'17 ?](#)

[3. Product description](#)

[4. Supported editions & licenses](#)

[5. General limitations](#)

[6. Architecture](#)

[7. Allowing the org admin to configure & use Files Connect](#)

[7.1. Files Connect cloud access vs on-premises integration](#)

[7.2. Turning on the Files Connect org preference](#)

[7.2.1. The "Reference" file sharing mode \(recommended\)](#)

[7.2.2. The "Copy" file sharing mode](#)

[7.3. Turning on the Files Connect user permissions for the org admin](#)

[7.3.1. Turning on the Files Connect cloud user permission for the org admin](#)

[7.3.1.1. Option #1: enabling the permission on a permission set \(preferred\)](#)

[7.3.1.2. Option #2: enabling the permission on a custom profile.](#)

[7.3.2. Turning on the Files Connect on-premises user permission for the org admin](#)

[7.4. Enabling the Files Connect external data sources for the org admin](#)

[7.4.1. Option #1 \(preferred\): using a permission set](#)

[7.4.2. Option #2: using a profile](#)

[8. Using the Secure Agent](#)

[9. Creating an auth provider](#)

[9.1. Creating a SharePoint 2010 or SharePoint 2013 auth provider](#)

[9.2. Creating a SharePoint Online or OneDrive for Business auth provider \(new in Winter'17\)](#)

[9.3. Creating a SharePoint Online or OneDrive for Business auth provider \(old method\)](#)

[9.5. Creating a Google Drive auth provider](#)

[9.6. Creating a Box auth provider](#)

[10. Creating a Files Connect external data source](#)

[10.1. Creating a SharePoint 2010/2013 on-premises external data source](#)

[10.2. Creating a SharePoint Online/OneDrive for Business external data source](#)

[10.3. Creating a Google Drive external data source](#)

[10.4. Creating a Box external data source](#)

[11. Allowing standard users to use a Files Connect external data source](#)

[11.1. Turning on the Files Connect user permissions for standard users](#)

[11.2. Enabling the Files Connect external data sources for the standard users](#)

[11.3. Letting the organization admin set user credentials on their behalf](#)

[12. Files Connect external objects](#)

[12.1. What is an external object ?](#)

[12.2. Creating an external object from a Files Connect external data source](#)

[12.3. Granting access to the external object](#)

[12.4. Adding custom fields to an external object](#)

[12.5. Global search using an external object](#)

[12.6. External object relationships](#)

[Appendix 1: Registering a Google Drive app](#)

[Appendix 2: Registering a Box app](#)

[Appendix 3: Registering a Azure web application \(new in Winter'17\)](#)

[Appendix 4: Registering an Office 365 app \(old method\)](#)

[Appendix 4: connecting to a SharePoint Online webapp](#)

[4.1. Limitations](#)

[4.2. Office365 app configuration](#)

[4.3. Salesforce authentication provider configuration](#)

[4.5. External data source configuration](#)

[Appendix 5: Querying on SharePoint custom properties](#)

[Configuring Custom Properties in SharePoint](#)

[Querying on custom properties](#)

[Known limitations](#)

[Appendix 6: Creating custom fields in SharePoint & using external objects relationships](#)

[Lookup relationship](#)

[Indirect Lookup relationship](#)

[Appendix 7: Checking if anonymous access is enabled in a SharePoint web application](#)

[Appendix 8: Cautions and Warnings](#)

1. Related documents & videos

1.1. Documents

- [Files Connect Setup Guide](#) (this document)
- [Files Connect User guide](#)
- [Files Connect API guide](#) (also check [this sample script](#))
- [Files Connect General Limitations](#)
- [Files Connect Agent Setup Guide](#)
- [Files Connect Agent Requirements & Limitations](#)
- [Files Connect Agent troubleshooting](#)

1.2. Videos

- [Files Connect Dreamforce'15 presentation](#)
- [How to use Files Connect on the desktop](#)
- [How to use Files Connect in Salesforce1](#)
- [Connecting Files Connect to SharePoint on-premises using the secure agent](#)
- [Connecting Files Connect to SharePoint Online](#)
- [Connecting Files Connect to Google Drive](#)
- [Connecting Files Connect to Box](#)
- [Authenticating against a Files Connect external data source](#)
- [Files Connect dynamic linking](#)

2. What's new in Winter'17 ?



Search for the “**new in Winter'17**” label to discover the chapters describing the new features.

- We simplified the Files Connect for SharePoint Online & OneDrive setup: you can now connect more easily using the Azure console.
- SharePoint system folders are now hidden when browsing the SharePoint folder hierarchy using Files Connect.
- In Lightning Experience, you can now attach multiple external files to Chatter posts.
- The SharePoint Online external data sources now use the SharePoint icon instead of using the generic Office 365 icon.

3. Product description

Files Connect allows you to connect Salesforce to your Enterprise Content Management (ECM) system. Currently supported ECM systems are:

- SharePoint 2010 & 2013 on-premises.
- SharePoint Online.
- OneDrive for Business.
- Google Drive
- Box

Using Files Connect:

- Salesforce users can navigate and search in their ECM system directly from Salesforce.
- Selected ECM documents can be shared with Salesforce records, users & Chatter groups by creating file references: this is called “static linking”.
- A file reference behaves like a standard Salesforce file, except that the external document content is not duplicated in Salesforce.
- Alternatively, lookup relationships can be configured between Salesforce records and ECM systems: this is called “dynamic linking”.

In this document an ECM system will simply be called an “external data source”.

4. Supported editions & licenses

Supported editions: Professional (only for external cloud data sources), Enterprise, Unlimited, Performance, Developer.

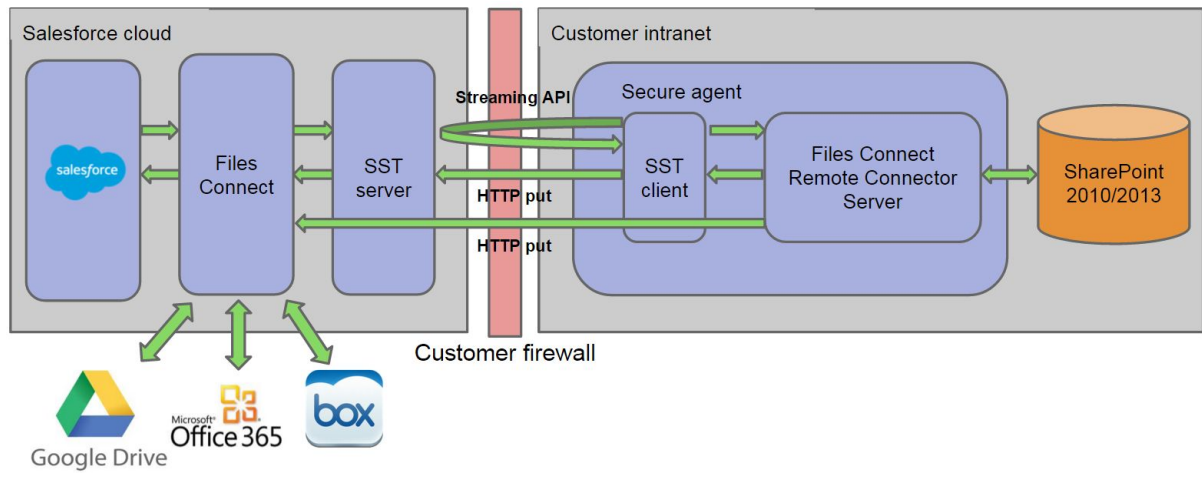
Supported licences:

- Internal licenses:
 - Salesforce
 - Chatter Only (aka “Chatter plus”)
 - Salesforce Platform
 - Salesforce Platform Light
 - Salesforce Platform One
 - Force.com - One App
 - Force.com App Subscription
 - Employee community license (internal org only)
- Community licenses:
 - Customer Community (CustomerCommunity-1.uld.xml)
 - Customer Community Login (CustomerCommunityLogin-1.uld.xml)
 - Customer Community Plus (CustomerCommunityPlus-1.uld.xml)
 - Customer Community Plus Login (CustomerCommunityPlusLogin-1.uld.xml)
 - Partner Community (PartnerCommunity-1.uld.xml)
 - Partner Community Login (PartnerCommunityLogin-1.uld.xml)
 - Authenticated Website (AuthenticatedWebsite-1.uld.xml)
 - Bronze Partner (BronzePartner-1.uld.xml)
 - CSP Lite Portal (CSPLitePortal-1.uld.xml)
 - Customer Portal Manager (CustomerPortalManager-1.uld.xml)
 - Customer Portal Manager Custom (CustomerPortalManagerCustom-1.uld.xml)
 - Customer Portal Manager Standard (CustomerPortalManagerStandard-1.uld.xml)
 - Customer Portal User (CustomerPortalUser-1.uld.xml)
 - External Identity Login (ExternalIdentityLogin-1.uld.xml)
 - Gold Partner (GoldPartner-1.uld.xml)
 - High Volume Customer Portal (HighVolumeCustomerPortal-1.uld.xml)
 - High Volume Portal (HighVolumePortal-1.uld.xml)
 - Ideas Only (IdeasOnly-1.uld.xml)
 - Ideas Only Portal (IdeasOnlyPortal-1.uld.xml)
 - Internal Portal User (InternalPortalUser-1.uld.xml)
 - Limited Customer Portal Manager Custom (LimitedCustomerPortalMgrCustom-1.uld.xml)
 - Limited Customer Portal Manager Standard (LimitedCustomerPortalMgrStandard-1.uld.xml)
 - Overage Authenticated Website (OverageAuthenticatedWebsite-1.uld.xml)
 - Overage Customer Portal Manager Custom (OverageCustomerPortalMgrCustom-1.uld.xml)
 - Overage Customer Portal Manager Standard (OverageCustomerPortalMgrStandard-1.uld.xml)
 - Overage High Volume Customer Portal (OverageHighVolumeCustomerPortal-1.uld.xml)
 - Partner (Partner-1.uld.xml)
 - Platform Portal (PlatformPortal-1.uld.xml)
 - Silver Partner (SilverPartner-1.uld.xml)

5. General limitations

Please refer to the “Files Connect General Limitations” document (see Chapter 02)

6. Architecture



7. Allowing the org admin to configure & use Files Connect

7.1. Files Connect cloud access vs on-premises integration

- The Files Connect **cloud** integration is bundled with most paid Salesforce licenses: see the full list at the beginning of this document.
- The Files Connect **on-premises** integration requires a paid add-on (permission set license): please contact your account executive for more information.

7.2. Turning on the Files Connect org preference

When Files Connect is enabled for your organization, the “Files Connect” node appears in your setup tree in the following Salesforce Classic location: *“Build > Customize > Salesforce Files > Settings > Files Connect”*.



If you don't see this node, it means that Files Connect doesn't support your org edition.

The Files Connect setup tree node in Salesforce Classic

1. Edit the page.
2. Click on the “Enable Files Connect” checkbox.
3. File Sharing: choose between “Reference” and “Copy”.
 - a. The recommended mode is “Reference” **and the rest of this document will assume that this option is selected.**
 - b. Before choosing “Copy”, make sure you read the following chapter.
4. Use External Object Search Layout: refer to the chapter describing how to use external objects for more information.

5. Click on “Save”.

7.2.1. The “Reference” file sharing mode (recommended)

This options allows Files Connect to create **references** to external data source files in Salesforce. File references behave like standard Salesforce files, however you need to authenticate against the external data source before being able to access the file content.

This is the best way to make sure that the external data source permission model is applied in Salesforce (when sharing the file in a group, not all group members may be able to access it though).

One of the common questions is “what is the difference between a file reference and an HTTP link?”. This table lists the main differences:

Feature	HTTP link	File reference
Requires Files Connect	No	Yes
Displays an icon representing the external system where the file is stored	No	Yes
Displays an icon showing the document type (word, powerpoint, pdf)	No	Yes
Is still usable after renaming the file in the external system	No (SharePoint) Yes (Google Drive)	Yes
Is usable even if the external system is not accessible from outside the company firewall	No	Yes (thanks to the on-premises agent)
Shows up in Salesforce reports	No	Yes
Shows up in the “files & attachments” section of any record	No	Yes
Shows up in the “group files” section of Chatter groups	No	Yes
Can be viewed in Salesforce ¹	No	Yes
Support previews	No	Yes (only in Lightning Experience for Google Drive)

7.2.2. The “Copy” file sharing mode

This options allows Files Connect to create **copies** of external data source files in Salesforce and this is not the recommended option: unless you have a strong reason to use this option, **we recommend using the “reference” sharing mode instead.**

If this file is then shared with a Chatter group, all group members will be allowed to access the file,

even if they don't have access to the file in the external data source: this is the best way to share an external data source file with **external** customers or partners when they don't have a valid account for the external data source.



Not matter what the sharing mode is, after a file copy or file reference is created in Salesforce:

- Renaming the external file will not automatically rename the file reference or the file copy.
- Renaming the file copy or reference name will not automatically rename the external file.
- However, since the content of file reference is not stored in Chatter, a file reference will always “point” to the content of the latest file revision in the external data source.

7.3. Turning on the Files Connect user permissions for the org admin

There are two Files Connect user permissions: the **Files Connect cloud** user permission and the **Files Connect on-premises** user permission. You need to turn on one of these two permissions for the org admin before being able to fully configure Files Connect.



The configuration steps are different depending on the user permission (cloud / on-premises) that you want to use, so make you fully read both chapter and do not skip any step.

7.3.1. Turning on the Files Connect cloud user permission for the org admin

7.3.1.1. Option #1: enabling the permission on a permission set (preferred)

Create a new permission set and turn on the “Files Connect Cloud” user permission:

Export Reports	<input type="checkbox"/>		Use Export Details and Printable View to export reports.
Files Connect Cloud	<input checked="" type="checkbox"/>		Access cloud-based external content sources, such as SharePoint Online.
Files Connect On-premises	<input type="checkbox"/>		Access on-premises external content sources, such as SharePoint.

When you create the permission set, make sure you do **not** link it to any user license:

Select the type of users who will use this permission set

Who will use this permission set? If you plan to assign this permission set to multiple users with different licenses, choose '--None--'. If only users with one type of license will use this permission set, choose the same license that's associated with them.

User License --None--

You then need to assign this permission set to the org admin.



Remember:

- When creating the permission set, do **not** link it to any user license.
- Make sure the permission set is assigned to the org admin, otherwise he will not be able to create any Files Connect external data source.

7.3.1.2. Option #2: enabling the permission on a custom profile.

If the organisation admin has a custom profile, you can edit it and enable the “Files Connect Cloud” user permission.

7.3.2. Turning on the Files Connect on-premises user permission for the org admin

Accessing on-premises repositories like SharePoint 2010 or SharePoint 2013 requires the purchase of a certain number of Files Connect on-premises permission set licenses (these are also known as “add-ons”).

Once the permission set licenses are purchased, the following row is displayed in “*Administer > Company Profile > Company information*”:

Permission Set Licenses Permission Set Licenses Help ?					
Name	Status	Total Licenses	Used Licenses	Remaining Licenses	Expiration Date
Files Connect for on-premises external data sources	Active	1	0	1	31/12/2015

Go to the org admin user details page, scroll down to the “Permission Set License Assignments” section, click on “Edit assignment” and make sure the checkbox is selected:

Permission Set License	Enabled	Description	Permissions Included
Files Connect for on-premises external data sources	<input checked="" type="checkbox"/>	Enables Files Connect users to be given access to on-premises data sources.	User Permissions <ul style="list-style-type: none"> Files Connect On-premises

From there: create a permission set, turn on the “Files Connect on-premises” user permission and

link the permission set to your org admin.

Files Connect Cloud	<input type="checkbox"/>	Access cloud-based external content sources, such as SharePoint Online.
Files Connect On-premises	<input checked="" type="checkbox"/>	Access on-premises external content sources, such as SharePoint.
Insert System Field Values for Chatter Feeds	<input type="checkbox"/>	Set the author or creation date for a Chatter post or comment.

When you create the permission set, make sure you do **not** link it to any user license:

Select the type of users who will use this permission set

Who will use this permission set? If you plan to assign this permission set to multiple users with different licenses, choose '--None--'. If only users with one type of license will use this permission set, choose the same license that's associated with them.

User License --None--

You then need to assign this permission set to the org admin.



- When creating the permission set, do **not** link it to any user license
- Make sure the permission set is assigned to the org admin, otherwise he will not be able to create or use any Files Connect external data source.
- When using an external data source for an on-premises repository, the “API enabled” user permissions also needs to be turned on.

7.4. Enabling the Files Connect external data sources for the org admin

By default the Files Connect external data sources using the “per-user” identity type are disabled, which means that they are not visible in Chatter. This chapter explains how to enable them.

7.4.1. Option #1 (preferred): using a permission set

Using the same permission set from the previous chapter, open the “External Data Source Access” section:

Permission Set Overview

Description	
User License	
Created By	Admin User, 2/3/2015 7:19 AM

Apps	
Settings that apply to Salesforce apps, such as Sales, and custom apps built on Force.com Learn More	
Assigned Apps Settings that specify which apps are visible in the app menu	
Assigned Connected Apps Settings that specify which connected apps are visible in the app menu	
Object Settings Permissions to access objects and fields, and settings such as tab availability	
App Permissions Permissions to perform app-specific actions, such as "Manage Call Centers"	
Apex Class Access Permissions to execute Apex classes	
Visualforce Page Access Permissions to execute Visualforce pages	
External Data Source Access Permissions to authenticate against external data sources	

Click on the edit button:

External Data Source Access <input type="button" value="Edit"/>	
External Data Source Name	Installed Package
GDrive	
SharePoint_online	

The list of the Files Connect external data sources configured using a "per-user" identity type is displayed in the "Available External Data Sources" column: move the ones that you want to enable in the "Enabled External Data Sources" column:

External Data Source Access <input type="button" value="Save"/> <input type="button" value="Cancel"/>	
Available External Data Sources	Enabled External Data Sources
SharePoint_online	GDrive
<div>Add ▶ Remove ◀</div>	



- By creating several permission sets containing various combinations of “enabled external data sources” you can configure which Files Connect users can see which external data sources.
- External data sources using a “named principal” identity type are not displayed in the left column, and as a result will be visible to all the Files Connect users.

7.4.2. Option #2: using a profile

Go to the profile details page, reach the “Enabled External Data Source Access” section and click on “Edit” button:

Enabled External Data Source Access

Edit

Enabled External Data Source Access Help ?

No External Data Sources enabled

7.4.3. Example

Enabled external data sources in setup tree	Files tab (Salesforce Classic)
<div><div>External Data Source Access</div><div><div>Save</div><div>Cancel</div></div><div><div>Available External Data Sources</div><div>SharePoint_Online</div></div><div><div>Enabled External Data Sources</div><div>Google_Drive</div></div><div><div>Add</div><div>Remove</div></div></div>	<div>EXTERNAL FILES</div> <div> Google Drive</div>
<div><div>External Data Source Access</div><div><div>Save</div><div>Cancel</div></div><div><div>Available External Data Sources</div><div>Google_Drive</div></div><div><div>Enabled External Data Sources</div><div>SharePoint_Online</div></div><div><div>Add</div><div>Remove</div></div></div>	<div>EXTERNAL FILES</div> <div> SharePoint Online</div>

External Data Source Access

Save

Cancel

Available External Data Sources

-None-

Add

►

◄


Remove


Enabled External Data Sources

Google_Drive

SharePoint_Online

EXTERNAL FILES

 Google Drive

 SharePoint Online

8. Using the Secure Agent

Please refer to the following documents

- Files Connect Agent Setup Guide
- Files Connect Agent Requirements & Limitations
- Files Connect Agent troubleshooting guide

9. Creating an auth provider



You need the “manage auth providers” user permission to accomplish the configuration steps described in this chapter.

9.1. Creating a SharePoint 2010 or SharePoint 2013 auth provider

You do not need to create any auth provider when connecting to an on-premises SharePoint 2010 or SharePoint 2013 server.

9.2. Creating a SharePoint Online or OneDrive for Business auth provider (new in Winter'17)



This is the recommended way of connecting Salesforce to Office 365 using Azure: [Click here for a video walkthrough](#)

If you don't want to use Azure, refer to the next chapter which describes an alternative method.

Before using this auth provider mechanism, make sure that one these statements is correct:

- All your users have at least “limited access” on the SharePoint root site collection
- On the associated external data source, the “exclude other site collection” option is **enabled**.

1. In Salesforce Classic, go to “*Administer > Security Controls > Auth. Providers*” and click on “New”. Create a new Microsoft Access Control Service auth. provider using placeholder values:

- Provider Type: select “**Open ID Connect**”.
- Name: your auth. provider name.
- URL Suffix: your auth. provider name.
- Consumer key: enter any placeholder value for the moment.
- Consumer Secret: enter any placeholder value for the moment.
- Authorize Endpoint URL: enter any dummy value starting with “https” for the moment.
- Token endpoint URL: enter any dummy value starting with “https” for the moment.
- Default Scopes: leave empty.

2. Click on “Save”: the auth. provider details page is displayed. Note down the value of the “Callback URL”:

Client Configuration	
Test-Only Initialization URL	https://login-blitz02.soma.salesforce.com/services/auth/test/00DD00000007E6zMAE/Office365
Oauth-Only Initialization URL	https://login-blitz02.soma.salesforce.com/services/auth/oauth/00DD00000007E6zMAE/Office365
Callback URL	https://login-blitz02.soma.salesforce.com/services/authcallback/00DD00000007E6zMAE/Office365

EditDeleteClone

3. Create an Azure web application as explained in appendix 3 : you will need to provide the Callback URL from the previous step.

4. Edit the auth. provider you just created and replace the dummy values with the ones generated by Azure:

- Consumer key: the client id retrieved after creating an Azure web application (see appendix 3).
- Consumer Secret: the key retrieved after creating an Azure web application (see appendix 3).
- Authorize Endpoint URL:
 - The format is
“https://login.microsoftonline.com/common/oauth2/authorize?resource=https%3A%2F%2F[YOUR_COMPANY_NAME].sharepoint.com&prompt=login”
 - Example:
“https://login.microsoftonline.com/common/oauth2/authorize?resource=https%3A%2F%2Fsalesforce.sharepoint.com&prompt=login”
 - In case you’re wondering, the part after “=” is the [URL encoded value](#) of your O365 root site collection.
- Token endpoint URL: “https://login.microsoftonline.com/common/oauth2/token”

5. Click on “Save”: your auth. provider is now ready to be used.



Look at [this article](#) to learn more about the possible values for the “prompt” parameter used in the authorize endpoint URL.

9.3. Creating a SharePoint Online or OneDrive for Business auth provider (old method)



This method is not recommended anymore: refer to the previous chapter for the recommended one.

This method should only be used if you do not want to use Microsoft Azure: [Click here for a video walkthrough](#)

1. In Salesforce Classic, go to “*Administer > Security Controls > Auth. Providers*” and click on “New”. Create a new Microsoft Access Control Service auth. provider using placeholder values:

- Provider Type: select “**Microsoft Access Control Service**”.
- Name: your auth. provider name.
- URL Suffix: your auth. provider name.
- Consumer key: enter any placeholder value for the moment.
- Consumer Secret: enter any placeholder value for the moment.
- Authorize Endpoint URL: enter any dummy value starting with “https” for the moment.
- Token endpoint URL: enter any dummy value starting with “https” for the moment.
- Default Scopes: leave empty.

2. Click on “Save”: the auth. provider details page is displayed. Note down the value of the “Callback URL”:

Client Configuration	
Test-Only Initialization URL	https://login-blitz02.soma.salesforce.com/services/auth/test/00DD00000007E6zMAE/Office365
Oauth-Only Initialization URL	https://login-blitz02.soma.salesforce.com/services/auth/oauth/00DD00000007E6zMAE/Office365
Callback URL	https://login-blitz02.soma.salesforce.com/services/authcallback/00DD00000007E6zMAE/Office365
<div>Edit Delete Clone</div>	

3. Create an Office 365 oauth client id as explained in appendix 4 : you will need to provide the Callback URL from the previous step.

4. Edit the auth. provider you just created and replace the dummy values with the correct ones:

- Consumer key: the client id retrieved after creating an Office365 app (see appendix 4).
- Consumer Secret: the client secret retrieved after creating an Office365 app (see appendix 4).
- Authorize Endpoint URL: the URL of the OAuthAuthorize.aspx page in Office365. The URL format is different for SharePoint Online and OneDrive for Business.
 - For **SharePoint Online**:
 - URL format is:
“https://[YOUR_COMPANY_NAME].sharepoint.com/[SITE_COLLECTION_PATH]/_layouts/15/OAuthAuthorize.aspx”
 - example:
https://salesforce.sharepoint.com/_layouts/15/OAuthAuthorize.aspx
 - For **OneDrive for Business**:

- URL format is:

`"https://[YOUR_COMPANY_NAME]-my.sharepoint.com/_layouts/15/OauthAuthorize.aspx"`

- example:

`https://salesforce-my.sharepoint.com/_layouts/15/OauthAuthorize.aspx`



Make sure that each user is allowed to access the "Authorize Endpoint URL" in Office 365: if this is not the case (which can happen if a user is allowed to access a subsite but not the site collection itself for example), users will not be able to use the external data source.

- Token endpoint URL: The URL format is different for SharePoint Online and OneDrive for Business.

- For **SharePoint Online**:

- URL format is:

`"https://accounts.accesscontrol.windows.net/[YOUR_COMPANY_NAME].onmicrosoft.com/tokens/OAuth/2?resource=00000003-0000-00ff1-ce00-000000000000/[YOUR_COMPANY_NAME].sharepoint.com@[YOUR_COMPANY_NAME].onmicrosoft.com"`

- example:

`https://accounts.accesscontrol.windows.net/salesforce.onmicrosoft.com/tokens/OAuth/2?resource=00000003-0000-00ff1-ce00-000000000000/salesforce.sharepoint.com@salesforce.onmicrosoft.com`

- For **OneDrive for Business**:

- URL format is:

`"https://accounts.accesscontrol.windows.net/[YOUR_COMPANY_NAME].onmicrosoft.com/tokens/OAuth/2?resource=00000003-0000-00ff1-ce00-000000000000/[YOUR_COMPANY_NAME]-my.sharepoint.com@[YOUR_COMPANY_NAME].onmicrosoft.com"`

- example:

`https://accounts.accesscontrol.windows.net/salesforce.onmicrosoft.com/tokens/OAuth/2?resource=00000003-0000-00ff1-ce00-000000000000/salesforce-my.sharepoint.com@salesforce.onmicrosoft.com`

5. Click on "Save": your auth. provider is now ready to be used.

9.5. Creating a Google Drive auth provider



[Click here for a video walkthrough](#)

First, make sure you've created a Google project as explained in appendix 1.

1. In Salesforce Classic, go to *"Administer > Security Controls > Auth. Providers"* and click on *"New"*. Create a new *"Open ID Connect"* Auth. provider.



Do **NOT** select the auth provider called *"Google"*, the one you need is *"Open ID Connect"*.

- Provider Type: select **"Open ID Connect"** (and NOT *"Google"*).
- Name: your auth. provider name.
- URL Suffix: your auth. provider name.
- Consumer key: the Client ID from your Google project (see appendix 1).
- Consumer Secret: the Client secret from your Google project (see appendix 1).
- Authorize Endpoint URL:
`"https://accounts.google.com/o/oauth2/auth?access_type=offline&approval_prompt=force"`
- Token endpoint URL: `"https://accounts.google.com/o/oauth2/token"`
- User Info Endpoint URL: `"https://www.googleapis.com/oauth2/v3/userinfo"`
- Default Scopes: `"openid email profile https://www.googleapis.com/auth/drive"`

2. Click on *"Save"*: the auth. provider details page is displayed. Note down the value of the *"Callback URL"*:

Client Configuration	
Test-Only Initialization URL	https://login-blitz02.soma.salesforce.com/services/auth/test/00DD00000007E6zMAE/google_drive
Oauth-Only Initialization URL	https://login-blitz02.soma.salesforce.com/services/auth/oauth/00DD00000007E6zMAE/google_drive
Callback URL	https://login-blitz02.soma.salesforce.com/services/authcallback/00DD00000007E6zMAE/google_drive
<div> Edit Delete Clone </div>	

3. Go back to the Google Developers Console, select the Google app created in appendix 1, go to the API manager, open the “Credentials” section and click on the previously created web application:

API
API Manager

Overview
Credentials

Credentials

OAuth consent screen

Domain verification

Add credentials
Delete

Create credentials to access your enabled APIs. Refer to the API documentation for details.

OAuth 2.0 client IDs

<input type="checkbox"/>	Name	Creation date	Type	Client ID
<input type="checkbox"/>	Web client 1	Nov 13, 2015	Web application	994736442522-ksehtnj4806m3t3kldei97l7ng2t08vm.apps.googleusercontent.com

Accessing the web application

4. Add the Callback URL of your auth. provider in the “Authorized redirect URIs” field:

API

API Manager

Overview

Credentials

Credentials

←

Download JSON

Reset secret

Delete

Client ID for Web application

Client ID	994736442522-ksehtnj4806m3t3kldei9717ng2t08vm.apps.googleusercontent.com
Client secret	gGpKt7hgmqH8F7YgPy2GedgWuS
Creation date	Nov 13, 2015, 3:54:38 PM

Name

Web client 1

Authorized JavaScript origins

Enter JavaScript origins here or redirect URIs below (or both) ?

Cannot contain a wildcard (http://*.example.com) or a path (http://example.com/subdir).

http://www.example.com

Authorized redirect URIs

Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

https://login.salesforce.com/services/authcallback/00DB00000000V1HLAU/GDrive

http://www.example.com/oauth2callback

Save

Cancel

Adding a new authorized redirect URI

5. Click on “Save”: your auth. provider is now ready to be used.



It can take a while for Google Drive to take into account the redirect URI. If you see the error message below during the OAuth dance, wait a few minutes and try again. If you still see the error, make sure that the “Authorized redirect URI” matches the auth provider callback URL.



400. That's an error.

Error: redirect_uri_mismatch

Application: Files Connect for Google Drive



9.6. Creating a Box auth provider



[Click here for a video walkthrough](#)

1. In Salesforce Classic, go to “*Administer > Security Controls > Auth. Providers*” and click on “New”. Create a new “Open ID Connect” Auth. provider.

- Provider Type: select “**Open ID Connect**”
- Name: your auth. provider name.
- URL Suffix: your auth. provider name.
- Consumer key: enter any placeholder value for the moment.
- Consumer Secret: enter any placeholder value for the moment.
- Authorize Endpoint URL: “*https://account.box.com/api/oauth2/authorize*”
- Token endpoint URL: “*https://api.box.com/oauth2/token*”
- User Info Endpoint URL: leave empty.
- Default Scopes: leave empty.



Box recently changed their authorize and token endpoints. The value listed below are the old endpoints that are still working correctly, unless you are part of the Box “Verified Enterprise” program: in this case you **need** to use the new values mentioned above.

- (Old) Authorize Endpoint URL: “*https://app.box.com/api/oauth2/authorize*”
- (Old) Token endpoint URL: “*https://app.box.com/api/oauth2/token*”

2. Click on “Save”: the auth. provider details page is displayed. Note down the value of the “Callback URL”:

Salesforce Configuration

Test-Only Initialization URL	https://login.salesforce.com/services/auth/test/00DB00000000V1HMAU/Box
OAuth-Only Initialization URL	https://login.salesforce.com/services/auth/oauth/00DB00000000V1HMAU/Box
Callback URL	https://login.salesforce.com/services/authcallback/00DB00000000V1HMAU/Box

Edit Delete Clone

3. Create a Box app using the instructions from appendix 2.

4. Edit the Salesforce auth provider and replace the following values with the one from the Box app:

- Consumer key: the Box client-id.
- Consumer Secret: the Box client-secret.

5. Click on “Save”: your auth. provider is now ready to be used.

10. Creating a Files Connect external data source

To connect your Salesforce to your external data source, you must first create a Files Connect external data source in the setup tree. In Salesforce Classic, go to “*Build > Develop > External Data Sources*” and click on “*New External Data Source*”.



If you only see “Simple URL” in the “Type” dropdown list, it means that the org administrator doesn’t have the needed Files Connect user permissions.

New External Data Source

Connect to another Salesforce organization or a third-party database or content system.

Not enough permission to create a Files Connect external data source

10.1. Creating a SharePoint 2010/2013 on-premises external data source



Connecting to SharePoint 2010 or SharePoint 2013 on-premises requires the Files Connect Agent: installing the agent is covered in another document (see chapter 1 for more information)

1. Fill-in the form like this:

- Label: This is the "friendly" name of the external data source that will be displayed to Chatter users
- Name: the internal name of the external data source
- Type: select “**Files Connect: SharePoint**”
- Secure Agent: select an available agent (see the corresponding documentation for more information)
- Site URL
 - The URL of the SharePoint webapp (which is also the URL of the root site collection), site collection or site.
 - connecting to a document library is **NOT** supported.
 - The URL **MUST** start with “https” **UNLESS** the external data source is linked to a

secure agent (in this case plain “http” is supported).

- o The URL you enter must end with the site name
 - do not add the name of a page like “mypage.aspx”.
 - generally speaking, do not simply copy and paste the value you see in your browser when accessing the native SharePoint UI: the site URL must end with the site name.



Connecting to a site will give you access to all the sub-sites. They will be displayed as sub-folders.

- Exclude other Site Collections:
 - o When enabled, only the site collection mentioned in the “Site URL” field is exposed in Salesforce
 - o The essentially means that if the “Site URL” is set to the root site collection URL, then only this site collection (and its sub-sites) will be exposed in Salesforce.
- Identity type: select “Per User” (see note below)



- In the “Per User” mode, each Chatter user needs to provide his own SharePoint on-premises credentials, which are going to be encrypted and stored in the Salesforce database.
- The other option is “Named Principal”: when using this option, the same credentials are shared by the all the external data source users.

- Authentication protocol: select “Password authentication”
 - o This option will also allow Files Connect to connect to SharePoint using the Basic or NTLM Windows authentication types. See <https://technet.microsoft.com/en-us/library/cc262350.aspx>
 - o The Windows Kerberos authentication type is not supported, although many SharePoint servers will fallback to NTLM if Kerberos is not supported by the client. See [http://technet.microsoft.com/en-us/library/cc779070\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc779070(v=ws.10).aspx)
- Administrator username: enter a valid SharePoint username
 - o The field name is a bit confusing: you actually don’t need to provide the username of a SharePoint **admin** account, just the username from a user that can access the site or site collection configured above.
- Administrator password: enter a valid SharePoint password
 - o These username/password combo will be used to test the connection to the SharePoint server.
 - o Each Chatter user will still need to provide his own credentials in order to use the external data source.

2. Click on “Save”: Files Connect validates the “Site URL” by connecting to the specified SharePoint site or site collection using the provided administrator username and password. If all values are correct, you are redirected to the external data source details page.

10.2. Creating a SharePoint Online/OneDrive for Business external data source

1. Fill-in the form like this:

- Label: This is the "friendly" name of the external data source that will be displayed to Chatter users.
- Name: the internal name of the external data source.
- Type: select “**Files Connect: SharePoint Online**” or “**Files Connect: OneDrive for Business**”
- Site URL
 - o For **SharePoint Online**:
 - the URL of your webapp, for ex:
“*https://[COMPANY_NAME].sharepoint.com*”
 - the URL of your site collection, for ex:
“*https://[COMPANY_NAME]/[SITE_COLLECTION_PATH]*”
 - The URL of your site, for ex:
“*https://[COMPANY_NAME].sharepoint.com/[SITE_COLLECTION_PATH]/site*”
 - o For **OneDrive for Business**: your OneDrive URL, for ex:
“*https://[YOUR_COMPANY_NAME]-my.sharepoint.com*”
 - o The URL **MUST** start with “https”.
 - o The URL you enter must end with the site name:
 - do **not** add the name of a page like “mypage.aspx”.
 - generally speaking, do not simply copy and paste the value you see in your browser when accessing the native SharePoint UI: the site URL must end with the site name.



Updating the “site URL” also requires updating the corresponding auth provider “authorize endpoint URL” property if you happen to be using an auth provider of type “Microsoft Access Service”.

This note does not apply to you if you use the new “Open ID Connect” auth provider that leverages Azure.

- Exclude other Site Collections:
 - o This option is only available when configuring a SharePoint Online external data source.
 - o See the previous chapter for the field description.



If you use the new “Open ID Connect” auth provider that leverages Azure AND if not all your users have access to the root site collection then you need to make sure that this “exclude other site collections” option is **enabled**.

- Identity type: select “**Per User**” (see the previous chapter explaining how to setup a SharePoint on-premises external data-source for more information).
- Authentication Protocol: select “**OAuth 2.0**”.
- Authentication Provider: use the lookup tool to select the auth provider that you created in one of the previous chapters.
- Scope: leave empty.
- Start authentication flow on save: click on the checkbox.

2. Click on “Save”: Files Connect starts the Oauth flow to validate that everything is correctly configured. Click on “Trust it” in the first screen (the list of displayed scopes will depend on the way the Office365 app has been configured).

Do you trust na1-blitz02.soma.salesforce.com?

Let it read items in all site collections.

Let it access basic information about the users of this site.



na1-blitz02.soma.salesforce.com

Trust It

Cancel

3. When the flow completes, you are redirected to the Salesforce and the external data source authentication status is “Authenticated”:

Authentication Status Authenticated

10.3. Creating a Google Drive external data source

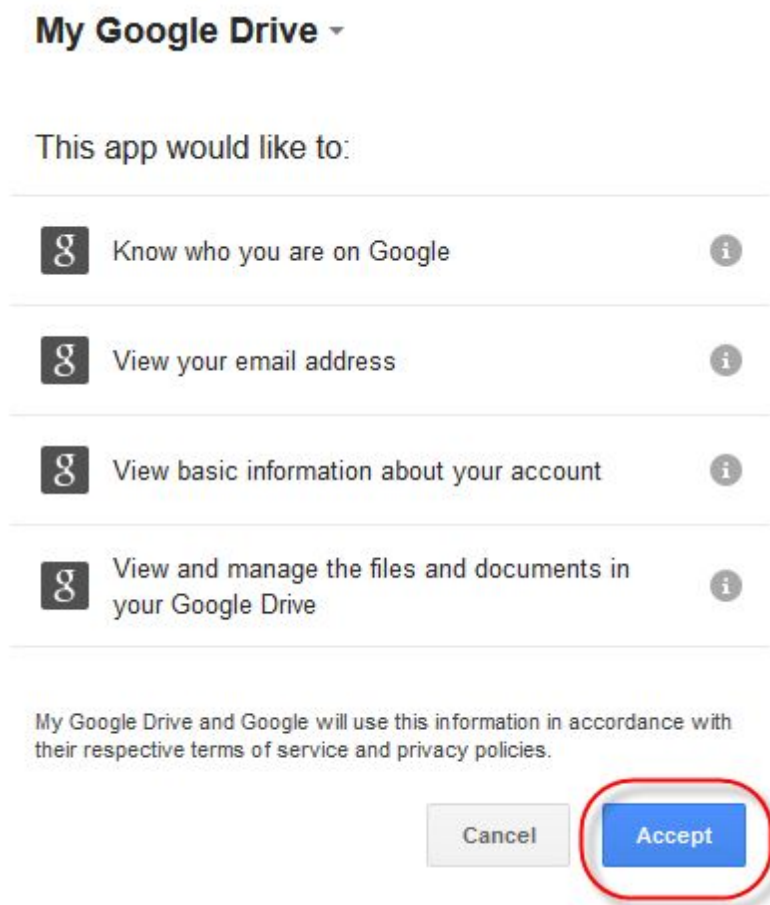
1. Fill-in the form like this:

- Label: This is the "friendly" name of the external data source that will be displayed to

Chatter users.

- Name: the internal name of the external data source.
- Type: select “**Files Connect: Google Drive**”.
- Identity type: select “**Per User**” (see the previous chapter explaining how to setup a SharePoint on-premises external data-source for more information).
- Authentication Protocol: select “**Oauth 2.0**”.
- Authentication Provider: use the lookup tool to select the auth. provider that you created in one of the previous chapters.
- Scope: leave this field empty.
- Start authentication flow on save: click on the checkbox.

2. Click on “Save”: Files Connect starts the Oauth flow to validate that everything is correctly configured. Click on “Accept” in the first screen:



3. When the flow completes, you are redirected to Salesforce and the external data source authentication status is “Authenticated”:

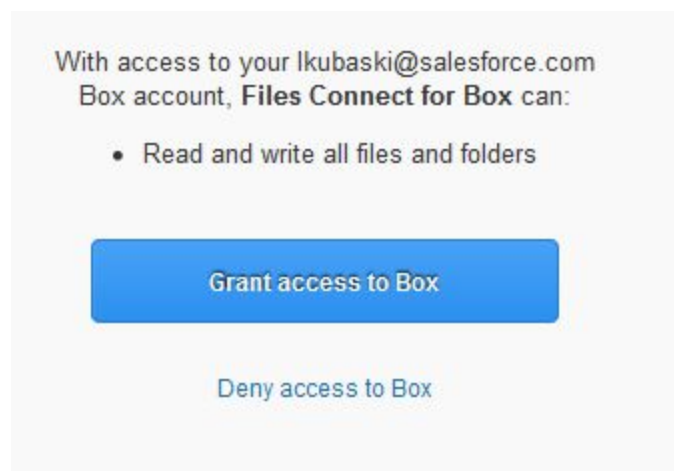
Authentication Status Authenticated

10.4. Creating a Box external data source

1. Fill-in the form like this:

- Label: This is the "friendly" name of the external data source that will be displayed to Chatter users.
- Name: the internal name of the external data source.
- Type: select "**Files Connect: Box**".
- Identity type: select "**Per User**" (see the previous chapter explaining how to setup a SharePoint on-premises external data-source for more information).
- Authentication Protocol: select "**Oauth 2.0**".
- Authentication Provider: use the lookup tool to select the auth. provider that you created in one of the previous chapters.
- Scope: leave this field empty.
- Start authentication flow on save: click on the checkbox.

2. Click on "Save": Files Connect starts the Oauth flow to validate that everything is correctly configured. Click on "Accept" in the first screen:



3. When the flow completes, you are redirected to Salesforce and the external data source authentication status is "Authenticated":

Authentication Status Authenticated

11. Allowing standard users to use a Files Connect external data source

You must now specify which standard users are allowed to use the newly created external data source. This is done in two steps:

1. First you must configure which users can use Files Connect as a whole.
2. Then you must configure the mapping between the users and the external data sources.

11.1. Turning on the Files Connect user permissions for standard users

Please refer to the chapter named *“Turning on the Files Connect user permissions for the org admin”*: the procedure is exactly the same. In fact, we recommend re-using the the same permission set or custom profile you already created.

11.2. Enabling the Files Connect external data sources for the standard users

Please refer to the chapter named *“Enabling the Files Connect external data sources for the org admin”*: the procedure is exactly the same.



- Using an external data sources for SharePoint on-premises requires the **“API enabled”** user permission.
- By creating several permission sets containing various combinations of “enabled external data sources” you can configure which Files Connect users can see which external data sources.
- External data sources using a “named principal” identity type are not displayed in the left column, and as a result **will be visible to all the Files Connect users**.

11.3. Letting the organization admin set user credentials on their behalf

In the “Files Connect User Guide” (see chapter 1 for the link), we explain how each user can connect to the external data source by authenticating themselves. However, the org admin also has the capability to **authenticate the users on their behalf**: this can be required in case you don’t

want the answers to know that the external data source credentials are.

To do this, go to “*Setup > administer > Manage Users > Users*”, open the user details page and scroll down to the “authentication settings for external systems” section:

Authentication Settings for External Systems New						Authentication Settings for External Systems Help ?
Action	Name	External System Definition	User	Username	Authentication Protocol	
Edit Del	SharePoint Online	External Data Source	the user	lkubaski@EntropySoft.onmicrosoft.com	Password Authentication	

Salesforce Classic: the “authentication settings for external systems” section in the user details page

From there you can:

- Authenticate a user on their behalf by clicking on the “new” button and providing the external data source credentials.
- Change the user credentials by clicking on “edit”.
- Disconnect a user from an external data source by clicking on “delete”.

For more information, refer to the “Managing your external data source credentials” chapter from the “Files Connect User Guide” document.

▼ Authentication

External System Definition

External Data Source

External Data Source

SharePoint Online

User

the user

Authentication Protocol

Password Authentication

Username

Password

Save

Cancel

Salesforce Classic: setting user credentials on their behalf



On the screenshot above, the “user” field will only appear for org admins: standard user will not see it since they can only set their own credentials.

12. Files Connect external objects

12.1. What is an external object ?

Creating an external object from a Files Connect external data source allows the external data source to behave like a Salesforce custom object, thus enabling the following features:

- Displaying documents stored in Files Connect external data sources in Salesforce global search results.
- Adding a tab linked to an external object and customizing the columns displayed when accessing it.
- Writing SOQL/SOQL queries that will return documents stored in Files Connect external data sources.
- Creating lookup relationships between Salesforce records and external data sources.



Note that creating an external object is **NOT** mandatory: this is only required if you want to enable one of the features mentioned above.

For more information concerning external objects, [please refer to the corresponding documentation](#). Files Connect simply leverages this framework and the goal of this documentation is not to describe its use in details.

12.2. Creating an external object from a Files Connect external data source

From a Files connect external data source details page, click on the “Validate and Sync” button:

External Data Source: SharePoint 2010

These settings identify an outside content system and let Salesforce access it.

[« Back to External Data Sources](#)

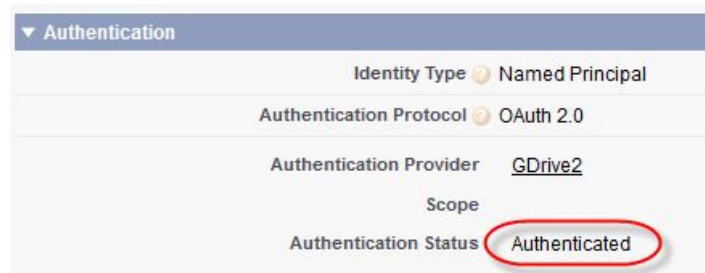
	Edit Validate and Sync Delete
Label	SharePoint 2010
Name	SharePoint_2010
Type	Content Hub SharePoint



If the “Validate and Sync” button is disabled, it usually means that the external data source is using the “OAuth 2.0” authentication protocol but that it’s authentication status is still “pending”.



The status needs to be “authenticated” for the button to be enabled:



To do this, edit the external data source, make sure that the “Start authentication flow on save” checkbox is selected and click on “save”.

From the “Validate External Data Source” screen, make sure the checkbox is selected and click on “Sync”.

Validate External Data Source: SharePoint 2010

Confirm that you can connect to the data source, and synchronize its table definitions with Salesforce.

Name	SharePoint_2010
Label	SharePoint 2010
Status	Success

Sync

<input type="checkbox"/>	Table Name	Table Label	Synced
<input checked="" type="checkbox"/>	items_SharePoint_2010	items_SharePoint_2010	<input type="checkbox"/>

This creates an external object which is listed in the “External Objects” node of the setup tree (“Build > Develop > External Objects”):

external objects

Expand All | Collapse All

Build

Develop

External Objects

External Objects

Help for this Page

Use external objects to virtually represent external data as Salesforce objects. External objects map to a table in a data source outside Salesforce and enable access to that data via custom tabs and search. Each external object requires an [external data source](#) definition for connection details.

New External Object

Action	Label	Deployed	External Data Source	Description
Edit Erase	items_SharePoint_2010	<input type="checkbox"/>	SharePoint_2010	

External Objects can be configured like any Salesforce custom objects. You can set field names and edit the object name, description or deployment status.

External Object

items_SharePoint_2010

[Standard Fields \[2\]](#) | [Custom Fields & Relationships \[11\]](#) | [Page Layouts \[1\]](#) | [Field Sets \[0\]](#) | [Compact Layouts \[1\]](#) | [Search Layouts \[5\]](#) | [Custom Links \[3\]](#)

External Object Definition Detail

Edit

Delete

Singular Label	items_SharePoint_2010	Description	
Plural Label	items_SharePoint_2010	Deployment Status	In Development
Object Name	items_SharePoint_2010		
API Name	items_SharePoint_2010__x		
External Data Source	SharePoint_2010		
Table Name	items_SharePoint_2010		
Repository Name			
Created By	laurent kubaski, 1/15/2014 6:51 AM	Modified By	laurent kubaski, 1/15/2014 6:51 AM

Standard Fields

Action	Field Label	Field Name	Data Type	Controlling Field
Edit	Display URL	DisplayUrl	URL(1000)	
Edit	External ID	ExternalId	External Lookup	

Custom Fields & Relationships

New

Action	Field Label	API Name	Data Type	Controlling Field	External Alias	Modified By
Edit Del	Author	Author__c	Text(255)		Author	laurent kubaski, 1/15/2014 6:51 AM
Edit Del	Comment	Comment__c	Long Text Area(32000)		Comment	laurent kubaski, 1/15/2014 6:51 AM
Edit Del	ContentLength	ContentLength__c	Number(18, 0)		ContentLength	laurent kubaski, 1/15/2014 6:51 AM
Edit Del	CreationDate	CreationDate__c	Date/Time		CreationDate	laurent kubaski, 1/15/2014 6:51 AM
Edit Del	DownloadUrl	DownloadUrl__c	Long Text Area(32000)		DownloadUrl	laurent kubaski, 1/15/2014 6:51 AM
Edit Del	IsFolder	IsFolder__c	Checkbox		IsFolder	laurent kubaski, 1/15/2014 6:51 AM
Edit Del	MimeType	MimeType__c	Text(255)		MimeType	laurent kubaski, 1/15/2014 6:51 AM
Edit Del	Name	Name__c	Text(255)		Name	laurent kubaski, 1/15/2014 6:51 AM
Edit Del	ParentId	ParentId__c	Text(255)		ParentId	laurent kubaski, 1/15/2014 6:51 AM
Edit Del	UpdateDate	UpdateDate__c	Date/Time		UpdateDate	laurent kubaski, 1/15/2014 6:51 AM
Edit Del	UpdatedBy	UpdatedBy__c	Text(255)		UpdatedBy	laurent kubaski, 1/15/2014 6:51 AM

External Objects generated from a Files Connect external data source will have these custom fields pre-generated for you. If needed, you can also create your own custom fields: the corresponding field in the external data source will need to already exist though (see one of the following chapters for more information).

- **Display URL:** a direct link to the object in the external data source.
 - If this field is added to the external object page layout, your users will be able to view the file in the external repository by clicking on it.
- **External ID:** the ID of the object in the external data source
- **Author:** the name of the object creator

- **Comment:** the object title (in SharePoint, that's the document title)
- **ContentLength:** the object size
- **CreationDate:** the object creation date
- **DownloadURL:** the download URL for the object
- **isFolder:** whether or not the object is a folder
- **MimeType:** the object mimetype
- **Name:** the object name
- **ParentId:**
- **UpdateDate:** the object last modification date
- **UpdatedBy:** the name of the person who last modified the object



Make sure the external object deployment status is “deployed” or non-admin users will not be able to use it.

External Object

items_SharePoint_online

[Standard Fields \[2\]](#)

[Custom Fields & Relationships \[12\]](#)

[Page Layouts \[1\]](#)

[Field Sets \[0\]](#)

[Compact Layouts \[1\]](#)

[Buttons, Links, and Actions \[0\]](#)

External Object Definition Detail

Edit

Delete

Singular Label	items_SharePoint_online	Description	
Plural Label	SharePoint online	Name Field	Name
Object Name	items_SharePoint_online	Deployment Status	Deployed
API Name	items_SharePoint_online__x		

The data source name that is displayed in the global search results page is the external object “plural label”. The default value is automatically generated, but you can change it if you want:

Edit External Object

items_SharePoint_2010

External Object Definition Edit

Save

Save & New

Cancel

External Object Information

The singular and plural labels are used in tabs, page layouts, and reports.

Be careful when changing the name or label as it may affect existing integrations and merge templates.

Label

items_SharePoint_2010

Example: Account

Plural Label

SharePoint 2010

Example: Accounts

Starts with vowel sound



12.3. Granting access to the external object

Go back to the permission set that you previously created and go to the Apps > Object Settings section:

Apps

Settings that apply to Salesforce apps, such as Sales, and custom apps built on Force.com
[Learn More](#)

Assigned Apps
Settings that specify which apps are visible in the app menu

Assigned Connected Apps
Settings that specify which connected apps are visible in the app menu

Object Settings
Permissions to access objects and fields, and settings such as tab availability

App Permissions
Permissions to perform app-specific actions, such as "Manage Call Centers"

Apex Class Access
Permissions to execute Apex classes

Visualforce Page Access
Permissions to execute Visualforce pages

External Data Source Access
Permissions to authenticate against External Data Sources

In the "Object settings" section, find the external object and click on it:

Reports	--	--	--
SharePoint 2010	No Access	13	--
Social Personas	--	7	--

Now enable all the following permissions:

Object Permissions

Permission Name	Enabled
Read	<input checked="" type="checkbox"/>

Field Permissions

Field Name	Read	Edit
Author	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Comment	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ContentLength	<input checked="" type="checkbox"/>	<input type="checkbox"/>
CreationDate	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Display URL	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DownloadUrl	<input checked="" type="checkbox"/>	<input type="checkbox"/>
External ID	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IsFolder	<input checked="" type="checkbox"/>	<input type="checkbox"/>
MimeType	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Name	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ParentId	<input checked="" type="checkbox"/>	<input type="checkbox"/>
UpdateDate	<input checked="" type="checkbox"/>	<input type="checkbox"/>
UpdatedBy	<input checked="" type="checkbox"/>	<input type="checkbox"/>

12.4. Adding custom fields to an external object

You can add a custom field to an external object exactly like you would add a custom field to a custom object: from the “custom fields & Relationships” section, click on the “New” button and follow the standard field creation wizard.

Custom Fields & Relationships New							
Action	Field Label	API Name	Data Type	Indexed	Controlling Field	External Alias	Modified By
Edit Del	Author	Author__c	Text(255)			Author	Admin User , 2/23/2015 9:43 AM
Edit Del	Comment	Comment__c	Long Text Area(32000)			Comment	Admin User , 2/23/2015 9:43 AM
Edit Del	ContentLength	ContentLength__c	Number(18, 0)			ContentLength	Admin User , 2/23/2015 9:43 AM
Edit Del	CreationDate	CreationDate__c	Date/Time			CreationDate	Admin User , 2/23/2015 9:43 AM
Edit Del	DownloadUrl	DownloadUrl__c	URL(255)			DownloadUrl	Admin User , 2/23/2015 9:43 AM
Edit Del	IsFolder	IsFolder__c	Checkbox			IsFolder	Admin User , 2/23/2015 9:43 AM
Edit Del	MimeType	MimeType__c	Text(255)			MimeType	Admin User , 2/23/2015 9:43 AM
Edit Del	Name	Name__c	Text(255)			Name	Admin User , 2/23/2015 9:43 AM
Edit Del	ParentId	ParentId__c	Text(255)			ParentId	Admin User , 2/23/2015 9:43 AM
Edit Del	UpdateDate	UpdateDate__c	Date/Time			UpdateDate	Admin User , 2/23/2015 9:43 AM
Edit Del	UpdatedBy	UpdatedBy__c	Text(255)			UpdatedBy	Admin User , 2/23/2015 9:43 AM

Once the custom field is created, it becomes available in SOQL/SOQL queries and you can also use

it in the external object search layouts.



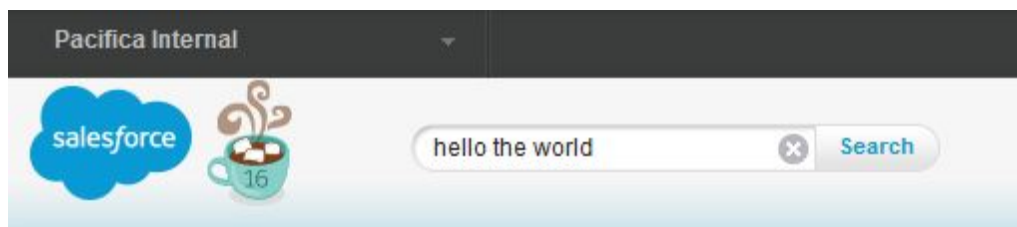
Before adding a custom field on the external object you need to make sure that the field also exist in the external data source.

Appendix 6 explains how to create custom fields in SharePoint.

12.5. Global search using an external object

Using an external object, you can use the Salesforce global search to search in Salesforce and in an external data source simultaneously.

Please refer to the “Files Connect User Guide” documentation.



Salesforce global search (in Salesforce Classic)

Note that in Salesforce Classic, Files Connect global search results are displayed by default using a hardcoded layout which does **not** follow the external object search layouts. This means two things:

1. Only the Name, Owner & Last Modified fields are displayed.
2. It is not possible to add or remove fields.

Search Results

[Guided Tour](#) | [Help for this Page](#)

Search Feeds

Records

SharePoint online (4)

GDrive (5+)

Accounts (1)

People (0)

Files (0)

Search All

RED

Search Again

Options...

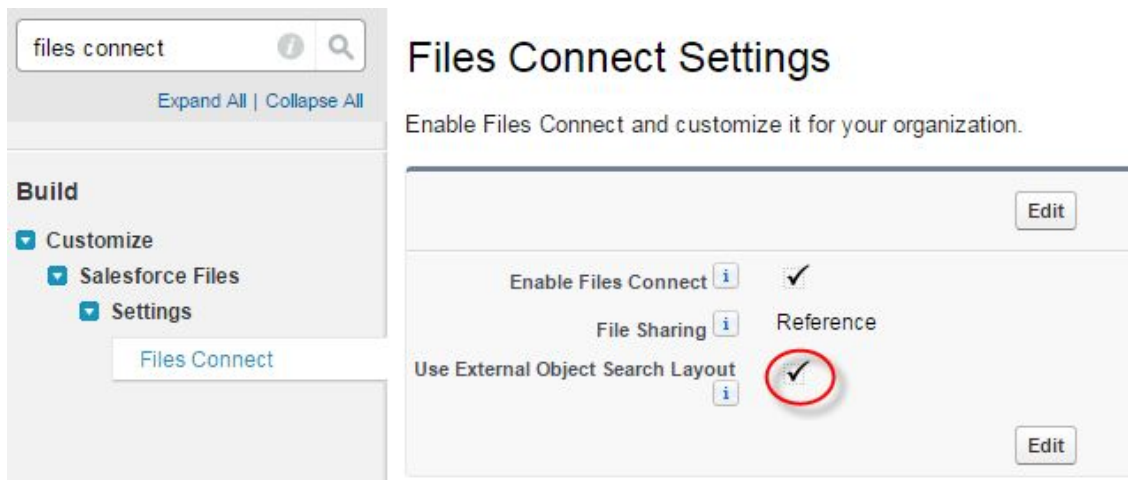
SharePoint online (4)

Actions	Name	Owner	Last Modified
▼	sample	Nicolas maquaire	10/9/2014
▼	sample	Nicolas maquaire	10/10/2007
▼	document01	Nicolas maquaire	10/31/2014
▼	document02	Nicolas maquaire	10/31/2014

The default external object search layout (in Salesforce Classic)

In order to customize the displayed fields, the “Use External Object Search Layout” option must be

enabled in “Salesforce Files > Settings > Files Connect”:



Once this option is enabled, the external object search layout is applied:

Search Layouts				
Action	Layout	Columns Displayed	Buttons Displayed	Modified By
Edit	Search Results	Name, my_xo_custom_field		Admin User, 4/1/2015 8:03 AM
Edit	Lookup Dialogs	External ID, Display URL	N/A	Admin User, 2/23/2015 9:43 AM
Edit	Lookup Phone Dialogs	External ID, Display URL	N/A	Admin User, 2/23/2015 9:43 AM
Edit	SharePoint online Tab	External ID, Display URL	N/A	Admin User, 2/23/2015 9:43 AM
Edit	SharePoint online List View	N/A	New	Admin User, 2/23/2015 9:43 AM
Edit	Search Filter Fields		N/A	Admin User, 2/23/2015 9:43 AM

Search Results

[Guided Tour](#) | [Help for this Page](#)

Search Feeds

Records

SharePoint online (4)

GDrive (5+)

Accounts (1)

People (0)

Files (0)

RED

Search Again

Options...

SharePoint online (4)

Action	Name	my_xo_custom_field
	sample.pdf	
	sample.doc	
	document01.docx	RED
	document02.docx	RED

A customized external object search layout

12.6. External object relationships

External objects support the following relationships, thus allowing you to dynamically link Salesforce records with documents stored in external data sources:

- Lookup relationships
- External lookup relationships
- Indirect lookup relationships

Appendix 6 describes how to use these various types of relationships.

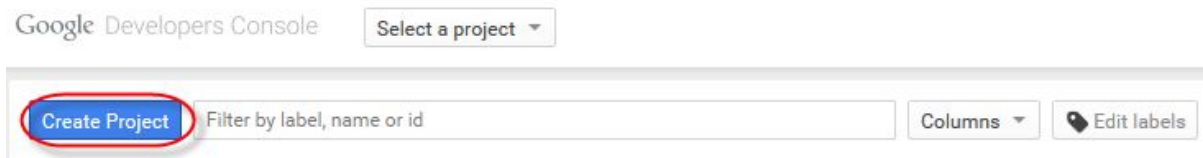
Appendix 1: Registering a Google Drive app



[Click here for a video walkthrough](#)

Before using a Files Connect Google Drive external data source, you must create a Google Drive app (or “project”) in the Google Developers console.

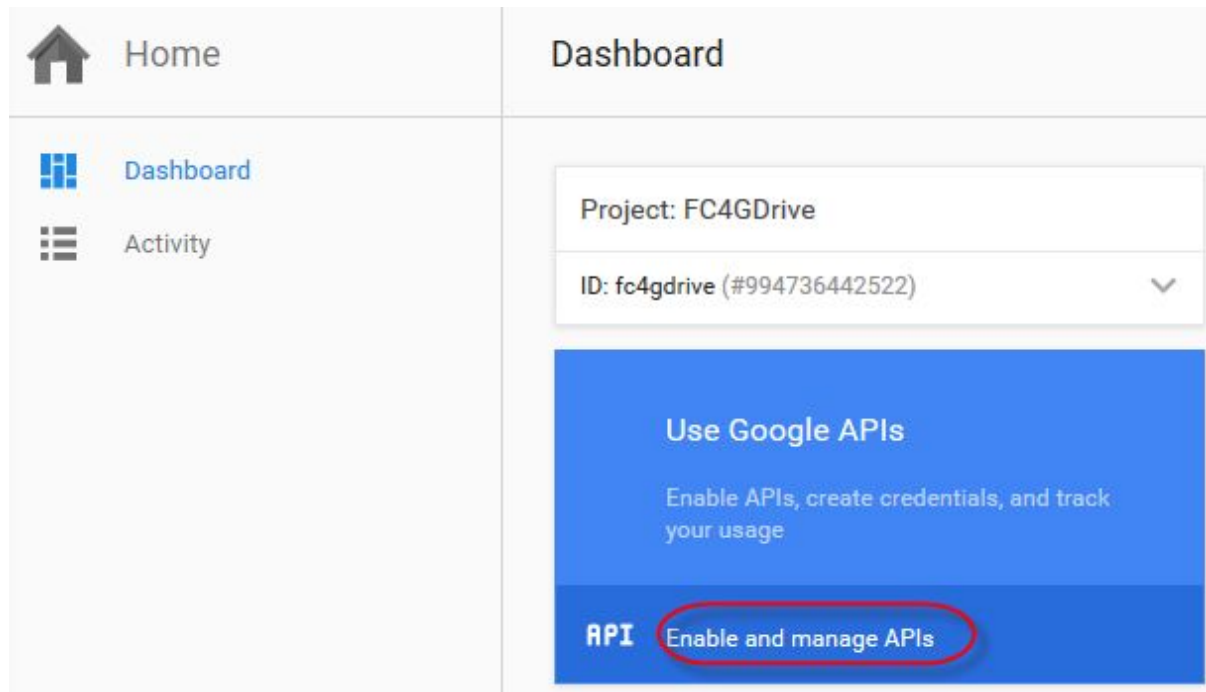
1. Using the credentials of your Google App for Work admin account, login to: <https://console.developers.google.com/project> and click on “Create Project”



2. Provide a project name and click on “Create”:

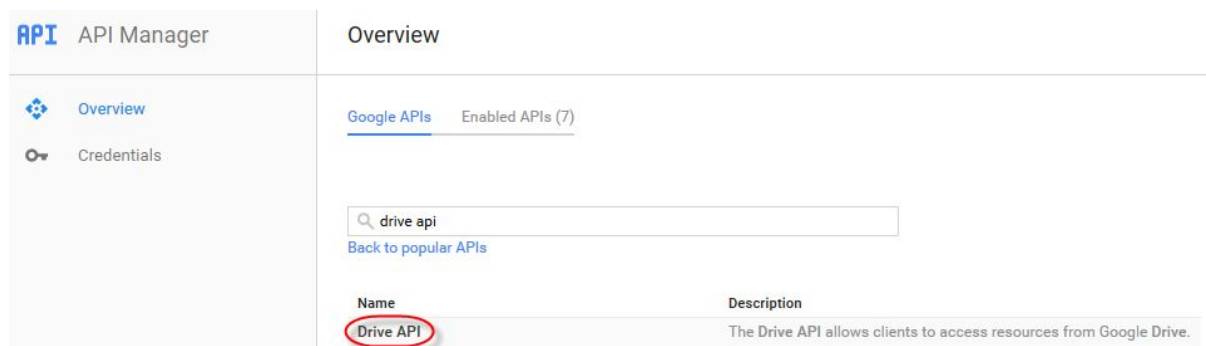
A screenshot of the "New Project" dialog box in the Google Developers Console. It has a title "New Project". Below it is a "Project name" field with a question mark icon, containing the text "FC4GDrive". Below the field, it says "Your project ID will be fc4gdrive" with a question mark icon and a blue "Edit" link. At the bottom, there is a link "Show advanced options..." and two buttons: "Create" (blue) and "Cancel" (grey).

3. On the project dashboard, click on “Enable and manage APIs” to open the API manager:

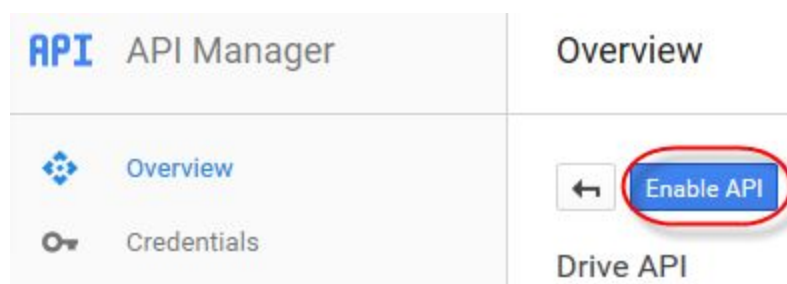


Accessing the API manager

4. In the search box, search for “Drive API”, click on the search result and click on “Enable API”

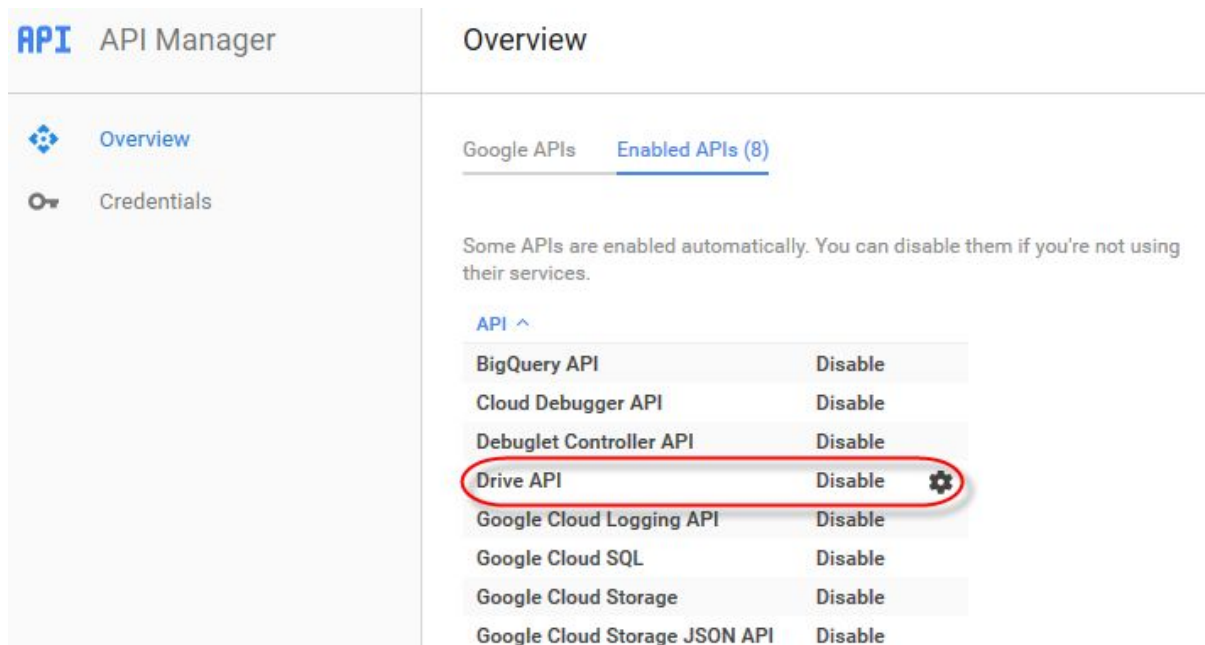


Searching for the “Drive API”



Enabling the “Drive API”

Optionally, go to the “Enabled APIs” tab and make sure that the “Drive API” is displayed in the list:



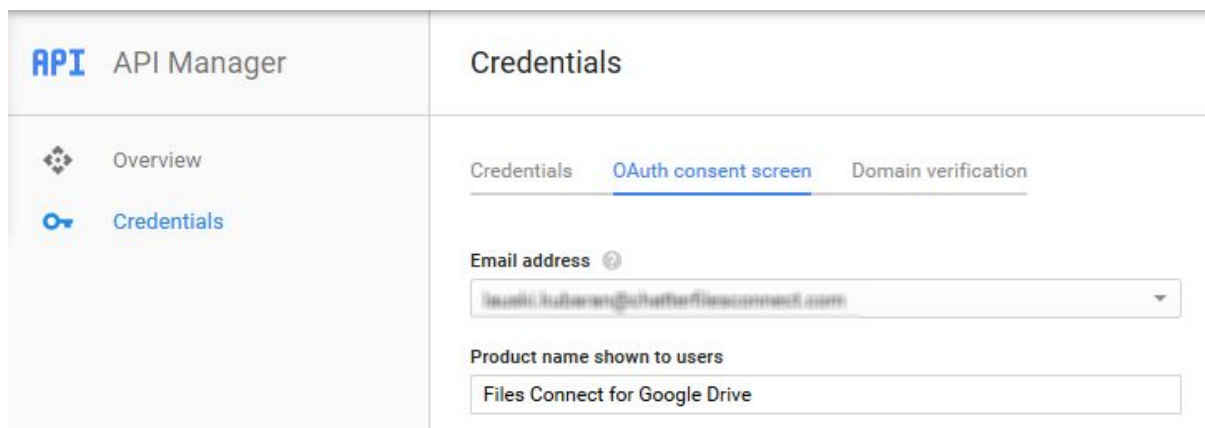
The screenshot shows the Google API Manager interface. On the left, the 'API Manager' header is visible with 'Overview' and 'Credentials' tabs. The main area is titled 'Overview' and shows 'Google APIs' with a sub-tab 'Enabled APIs (8)'. Below this, a message states: 'Some APIs are enabled automatically. You can disable them if you're not using their services.' A table lists the enabled APIs:

API	Disable
BigQuery API	Disable
Cloud Debugger API	Disable
Debuglet Controller API	Disable
Drive API	Disable
Google Cloud Logging API	Disable
Google Cloud SQL	Disable
Google Cloud Storage	Disable
Google Cloud Storage JSON API	Disable

The 'Drive API' row is highlighted with a red circle, and a gear icon is visible next to the 'Disable' link.

Checking that the “Drive API” is correctly enabled

4. Go to the “Credentials” section, click on the “OAuth consent screen” tab, provide valid values for the email address and the product name then click on “Save”:



The screenshot shows the Google API Manager interface with the 'Credentials' tab selected. The 'OAuth consent screen' sub-tab is active. The 'Email address' field is filled with 'kubaran@schatterfileconnect.com' and the 'Product name shown to users' field is filled with 'Files Connect for Google Drive'.

Configuring the OAuth consent screen

5. Go to the “Credentials” section, click on the “Credentials” tab and select “OAuth 2.0 client ID” in the dropdown:

APIs Credentials

You need credentials to access APIs. [Enable the APIs you plan to use](#) and then create the credentials they require. Depending on the API, you need an API key, a service account, or an OAuth 2.0 client ID. [Refer to the API documentation](#) for details.

Add credentials ▾

API key

Identifies your project using a simple API key to check quota and access. For APIs like Google Translate.

OAuth 2.0 client ID

Requests user consent so your app can access the user's data. For APIs like Google Calendar.

Service account

Enables server-to-server, app-level authentication using robot accounts. For use with Google Cloud APIs.

6. Select “Web application” and click on “Create”:

API API Manager

Overview

Credentials

Credentials

←

Create client ID

Application type

☒ Web application

☐ Android [Learn more](#)

☐ Chrome App [Learn more](#)

☐ iOS [Learn more](#)

☐ PlayStation 4

☐ Other

Name

Web client 1

Authorized JavaScript origins

Enter JavaScript origins here or redirect URIs below (or both) ⓘ
Cannot contain a wildcard (http://*.example.com) or a path (http://example.com/subdir).

http://www.example.com

Authorized redirect URIs

Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

http://www.example.com/oauth2callback

Create

Cancel

Creating a Web application

7. Your client ID is now created:

OAuth client

Here is your client ID

994736442522-ksehtnj4806m3t3kldei9717ng2t08vm.apps.googleusercontent.com

Here is your client secret

gopu175qrwqP1175gPpQ2w4qKs5

OK

Client ID & Client secret

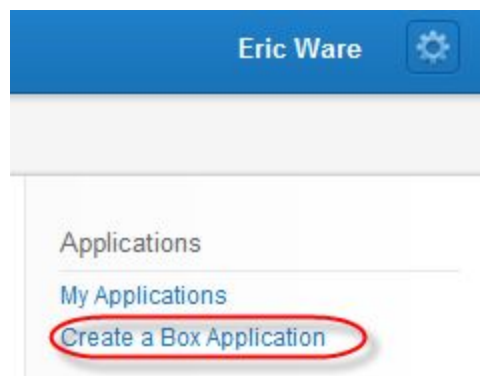
Note down the “Client ID” and “Client secret” values: you will need them when creating a “Open ID Connect” auth. provider in the Salesforce setup tree.

Appendix 2: Registering a Box app

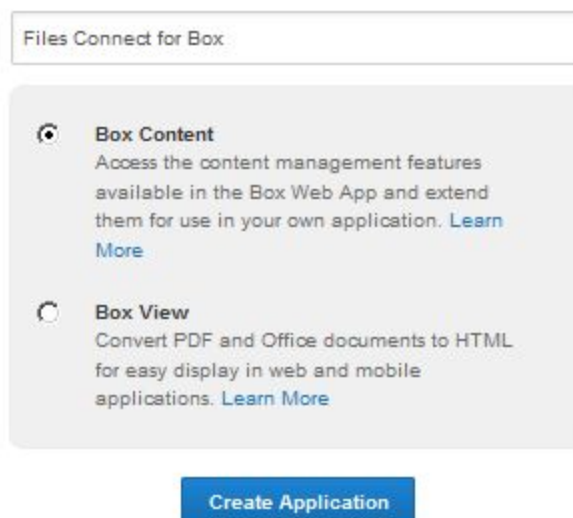


[Click here for a video walkthrough](#)

1. Using the credentials of your Box admin account, login to:
<https://app.box.com/developers/services> and click on “Create a Box application”



2. Provide a name for your application, make sure that “Box content” is selected and click on “Create application”



3. Click on “Configure your application”:

Success!

Your application has been successfully created! Take a look at the [getting started guide](#) or the [API documentation](#) for guidance.

[Configure your application](#)

4. In the redirect-uri field, paste the Salesforce callback URL.

5. Note down the “client_id” and “client_secret” values.

OAuth2 Parameters

client_id:	1rfvsdmycrldq7fi9ne16r9go39vh68	client_id as specified in the OAuth2 spec
client_secret:	cvPzmJ2ZGdKUL3tFWvu3SGc1zbERPkP8	client_secret as specified in the OAuth2 spec (leave blank to reset)
redirect_uri:	https://login.salesforce.com/services/authc	redirect_uri as specified in the OAuth2 spec

6. Go back to Salesforce and paste the values of the Box client-id and client-secret fields in the auth provider “Consumer Key” and “Consumer Secret” fields.

Appendix 3: Registering a Azure web application (new in Winter'17)



- Read the note at the beginning of chapter 9.2 before reading this chapter.
- For more detailed instructions, refer to [the official MSDN article](#)

Before using a SharePoint Online or OneDrive for Business external data source, you must create an Azure web application.

1. Login to <https://manage.windowsazure.com> as the admin of your O365 tenant.
2. In the left menu, scroll down and select “active directory”, then click on the row corresponding to your O365 tenant

The screenshot shows the Microsoft Azure portal interface. On the left, a vertical sidebar lists various services: SERVICE BUS, MOBILE ENGAGEMENT, VISUAL STUDIO TEAM SE..., CACHE, BIZTALK SERVICES, RECOVERY SERVICES, CDN, AUTOMATION, SCHEDULER, API MANAGEMENT, MACHINE LEARNING, STREAM ANALYTICS, OPERATIONAL INSIGHTS, NETWORKS, TRAFFIC MANAGER, REMOTEAPP, and MANAGEMENT SERVICES. At the bottom of this sidebar, 'ACTIVE DIRECTORY' is highlighted with a red box. The main content area is titled 'active directory' and contains a table with columns: NAME, STATUS, ROLE, SUBSCRIPTION, DATACENTER REGION, and COUNTRY OR REGION. The table has one row for 'EntropySoft', which is also highlighted with a red box. The status is 'Active', and the role is 'Global Administrator'.

NAME	STATUS	ROLE	SUBSCRIPTION	DATACENTER REGION	COUNTRY OR REGION
EntropySoft	Active	Global Administrator	Shared by all EntropySoft s...	United States	United States

3. Go to “applications” and click on “add”:

The screenshot shows the Microsoft Azure portal interface for EntropySoft. The top navigation bar includes 'Microsoft Azure', 'Check out the new portal', 'CREDIT STATUS', and a user profile. The left sidebar contains various Azure service icons. The main content area is titled 'entropysoft' and features a navigation menu with 'USERS', 'GROUPS', 'APPLICATIONS' (highlighted with a red box), 'DOMAINS', 'DIRECTORY INTEGRATION', 'CONFIGURE', 'REPORTS', and 'LICENSES'. Below the navigation menu is a search bar with the text 'Applications my company uses' and a search icon. A table of applications is displayed with the following columns: NAME, PUBLISHER, TYPE, and APP URL. The table lists several applications, including 'entropysofttestlmay13', 'Microsoft Intune', 'Office 365 Exchange Online', 'Office 365 Management APIs', 'Office 365 SharePoint Online', 'Office 365 Yammer', 'OneNote', 'Skype for Business Online (preview)', and 'WebApplication1.Office365App'. At the bottom of the interface, there is a dark blue bar with a '+ NEW' button, an 'ADD' button (highlighted with a red box), a 'VIEW ENDPOINTS' button, and a 'DELETE' button. A notification icon with the number '1' and a help icon are also present.

NAME	PUBLISHER	TYPE	APP URL
entropysofttestlmay13	EntropySoft	Web application	https://foo
Microsoft Intune	Microsoft Corporation	Web application	http://www.microsoft.com/en-us/server-cla...
Office 365 Exchange Online	Microsoft Corporation	Web application	http://office.microsoft.com/outlook/
Office 365 Management APIs	Microsoft Corporation	Web application	
Office 365 SharePoint Online	Microsoft Corporation	Web application	http://office.microsoft.com/sharepoint/
Office 365 Yammer	Microsoft Corporation	Web application	https://products.office.com/yammer/
OneNote	Microsoft Corporation	Web application	
Skype for Business Online (preview)	Microsoft Corporation	Web application	
WebApplication1.Office365App	Cloudsherpas	Web application	http://localhost:38908/

4. Choose “add an application”:

×

What do you want to do?

➔ Add an application my organization is developing

➔ Add an application from the gallery

5. Choose “web application”:

×

ADD APPLICATION

Tell us about your application

NAME

entropysofttestmay20

Type

☒ WEB APPLICATION AND/OR WEB API ?

☐ NATIVE CLIENT APPLICATION ?

➔

2

6. Enter the value of your O365 root site collection URL in the 2 fields:

ADD APPLICATION ×

App properties

SIGN-ON URL ?

✓

APP ID URI ?

✓


1

← ✓

7. Go to the “configure” section of your app:




8. Keep a copy of the client ID (you will need it when updating the Salesforce auth provider):




CLIENT ID 

9. Select a “one year” key:

keys				
1 year	5/20/2016	5/20/2017	THE KEY VALUE WILL BE DISPLAYED AFTER YOU SAVE IT.	
Select dur... 	VALID FROM	EXPIRES ON	THE KEY VALUE WILL BE DISPLAYED AFTER YOU SAVE IT.	

10. In the “permission to other application” section, delete the existing row:

permissions to other applications 

Windows Azure Active Directory	Application Permissions: 0 	Delegated Permissions: 1 	
--------------------------------	--	--	---

Add application

11. Then click on “add application”:

permissions to other applications 

No entries

Add application

12. And select “Office 365 SharePoint Online”:

Permissions to other applications

SHOW Microsoft Apps

NAME	APPLICATION PERMISSIONS	DELEGATED PERMISSIONS	
Microsoft Graph	16	40	
Microsoft Intune API	2	0	
Office 365 Exchange Online	9	19	
Office 365 Management AP...	5	5	
Office 365 SharePoint Onlin..	8	11	
Office 365 Yammer	0	1	
OneNote	0	6	
Power BI Service	0	9	
Skype for Business Online	0	3	
Windows Azure Active Dire...	4	8	

1 2

SELECTED
Office 365 SharePoint O...

13. Validate and set a delegated permission:

single sign-on

APP ID URI

https://foo

REPLY URL

https://foo

(ENTER A REPLY URL)

permissions to other applications

Office 365 SharePoint Online

Application Permissions: 0

- ☐ Read and write managed metadata
- ☐ Read managed metadata
- ☐ Run search queries as a user
- ☐ Read and write user files
- ☒ Read user files
- ☐ Have full control of all site collections
- ☐ Read and write items and lists in all site collections
- ☐ Read and write items in all site collections
- ☐ Read items in all site collections
- ☐ Read and write user profiles
- ☐ Read user profiles

Delegated Permissions: 1

Add application

14. The end result should look like this:

permissions to other applications ?

Office 365 SharePoint Online	Application Permissions: 0	Delegated Permissions: 1
------------------------------	----------------------------	--------------------------

[Add application](#)

15. Now hit “save”:

[+ NEW](#)
[VIEW ENDPOINTS](#)
[UPLOAD LOGO](#)
[MANAGE MANIFEST](#)
[DELETE](#)
[SAVE](#)
[DISCARD](#)
1
1

16. A key is generated: make sure you keep a copy of it before leaving the page since you won’t be able to retrieve it later.

keys ?

1 year	5/20/2016	5/20/2017	a0ocYTGBZxXTzf6Ms8/t30RR0sd5M/aQ+vU1Xqww3QE=	
Select dur...	VALID FROM	EXPIRES ON	THE KEY VALUE WILL BE DISPLAYED AFTER YOU SAVE IT.	

Copy and store the key value. You won't be able to retrieve it after you leave this page.

17. Edit the web application, go to “single sign-on” section and paste the Salesforce auth provider “callback URL” in the “REPLY URL” field:

single sign-on ?

APP ID URI ✓ ?

REPLY URL

?

?

18. Hit save: your Azure web application is now fully configured.

Appendix 4: Registering an Office 365 app (old method)



Read the note at the beginning of chapter 9.3 before reading this chapter.

Before using a SharePoint Online or OneDrive for Business external data source, you must create an Office365 app.

1. Login to your Office365 account as an admin

2. Go to the **appregnew** URL that corresponds to the external data source type:

- to configure a **SharePoint Online** app, go to:
“https://[YOUR_COMPANY_NAME].sharepoint.com/[SITE_COLLECTION_PATH]/_layouts/15/appregnew.aspx”
- to configure a **OneDrive for Business** app, go to:
“https://[YOUR_COMPANY_NAME]-my.sharepoint.com/_layouts/15/appregnew.aspx”

3. Fill in the form:

App Information

The app's information, including app id, secret, title, hosting url and redirect url.

App Type:

- ☒ An app running on a web server
☐ An app running on a client machine

Client Id:

931b7af8-e1fc-4418-92e1-374e0336!

Generate

Client Secret:

XwNmQpEwqpFfwdAk7p7vWqHtsB

Generate

Title:

Files Connect Client ID

App Domain:

na9-blitz02.soma.salesforce.com

Example: "www.contoso.com"

Redirect URI:

0000MQm2AM/O365_auth_provider

Example: "https://www.contoso.com/default.aspx"

- App Type: select “An app running on a web server”.
- Client Id: click on “Generate” and keep a copy of the generated value.
 - Note: this is what Salesforce calls the “Consumer Key”.
- Client Secret: click on “Generate” and keep a copy of the generated value.

- Note: this is what Salesforce calls the “Consumer Secret”.
- Title
- App Domain: the domain of your **Salesforce** organization.
 - For a production org: “na[INSTANCE_NUMBER].salesforce.com” (for example if your Salesforce organization is on the NA6 instance, you should use “na6.salesforce.com”).
 - For a sandbox org: “cs[INSTANCE_NUMBER].salesforce.com”.
- Redirect URI: the Callback URL that was generated after the initial creation of the auth provider in Salesforce.



You will need to provide the client ID and client secret values when finishing the configuration of the SharePoint online auth provider in Salesforce.

Click on “Create”.

4. You must now use the **appinv** tool to allow the newly created app to access SharePoint resources

- for **SharePoint Online**, go to
 “https://[YOUR_COMPANY_NAME].sharepoint.com/[SITE_COLLECTION_PATH]/_layouts/15/appinv.aspx” and fill the form.
- for **OneDrive for Business**, go to
 “https://[YOUR_COMPANY_NAME]-my.sharepoint.com/_layouts/15/appinv.aspx” and fill the form.

App Id and Title

The app's identity and its title.

App Id:

26540947-c8a9-40ab-8ebd

Lookup

Title:

na1-blitz03.soma.salesforce.com

App Domain:

na1-blitz03.soma.salesforce.com

Example: "www.contoso.com"

Redirect URL:

https://login-blitz03.soma.salesforce.com/se

Example: "https://www.contoso.com/default.aspx"

App's Permission Request XML

The permission required by the app.

Permission Request XML:

- App id: enter the client id that was generated during the previous step and click on the "Lookup" button.
- Title: keep the default value.
- App Domain: keep the default value.
- Redirect URL: keep the default value.
- Permission Request XML: see additional information just below.

4.1. Permission Request XML for SharePoint Online

```
<AppPermissionRequests>  
<AppPermissionRequest Scope="[SCOPE]" Right="[RIGHT]" />  
</AppPermissionRequests>
```

Replace [SCOPE] with one of these 3 values (don't try to modify them in any way: Office365 only recognises the 3 values below)

- **"http://sharepoint/content/sitecollection/web"** to allow the user to access a single site (and **not** its subsites).
 - When using this scope, make sure that the external data source URL is not the one of a sub-site: this scope prevents accessing them.
- **"http://sharepoint/content/sitecollection"** to allow the user to access a single site collection (including all subsites).
- **"http://sharepoint/content/tenant"** to allow the user to access all site collections.
 - Use this value if the external data source is connected to the webapp and if you want all the site collections to be displayed as sub-folders.

Replace [RIGHT] with one of these 4 values, depending on the level of access you need:

- **Read** (for read-only access in SharePoint from Salesforce)
- **Write** (for read-write access in SharePoint from Salesforce)
- **Manage**
- **Full Control**

4.2. Permission Request XML for OneDrive for Business

- The only supported scope in the list above is “**http://sharepoint/content/tenant**”
- You will also need this additional scope: “**http://sharepoint/social/tenant**”
- As a result, the Permission Request XML has this format:

```
<AppPermissionRequests>
<AppPermissionRequest Scope=" http://sharepoint/content/tenant " Right="[RIGHT]" />
<AppPermissionRequest Scope="http://sharepoint/social/tenant" Right="Read" />
</AppPermissionRequests>
```

Replace [RIGHT] with any of the 4 values described above in the SharePoint Online section.



- For more information about the syntax of the “permission request XML”, check [this MSDN article](#)
- If you need to modify the scope later on, you’ll need to create a new app: going back to appinv.aspx and changing the values of an existing app **will not work**, although Office 365 will not report any error if you try to do so.

5. If needed, use the **appprincipal** tool to list/delete the apps that have been granted access to a site collection:

- **SharePoint Online:**
“https://[YOUR_COMPANY_NAME].sharepoint.com/[SITE_COLLECTION_PATH]/_layouts/15/appprincipals.aspx” (also accessible from “Settings > Site Settings > Site collection app permissions” in Office365)
- **OneDrive for Business:**
“https://[YOUR_COMPANY_NAME]-my.sharepoint.com/_layouts/15/appprincipals.aspx”

Site Settings › Site Collection App Permissions ⓘ

App Display Name↑	App Identifier
AppBlitz3NM	i0ltjms.sp.ext 6f46c642-cf2b-42b7-8e63-6c6729518a01@5dda0faf-c020-4464-88b9-a9b2bfaafe31
gs0.salesforce.com	i0ltjms.sp.ext 0314a65f-1d0f-4c8b-8c04-74c8d167a8c2@5dda0faf-c020-4464-88b9-a9b2bfaafe31
Microsoft.SharePoint	i0ltjms.sp.ext 00000003-0000-0ff1-ce00-000000000000@5dda0faf-c020-4464-88b9-a9b2bfaafe31
na1-blitz03.soma.salesforce.com	i0ltjms.sp.ext 26540947-c8a9-40ab-8ebd-cc546d907c07@5dda0faf-c020-4464-88b9-a9b2bfaafe31

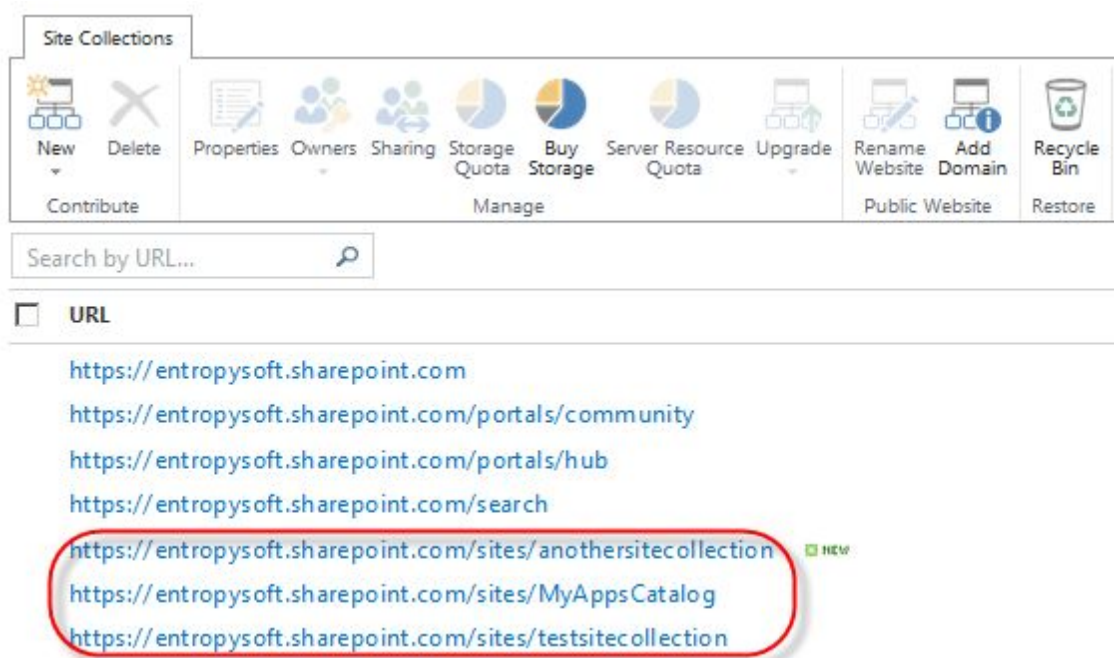


- The Client ID (or Consumer Key in Salesforce terminology) can be extracted from the value of the App Identifier: [PART1]||[PART2]||**CLIENT_ID**@[PART4]
- Appprincipal lists the apps that are linked to the site collection specified in the URL. This means that:
 - Listing the apps of the root site collection will **not** list the apps in all the site collections
 - Listing the apps in [SITE_COLLECTION]/[SITE] is the same as listing the apps in [SITE_COLLECTION]

Appendix 4: connecting to a SharePoint Online webapp

This appendix describes in more details how to configure Files Connect to connect to the SharePoint web app (“root site”) so that each site collection is displayed as a sub-folder.

Connecting to a SharePoint web app allows each user to access his site collections without having to create an external data source for each one. When using this approach, each site collection under [https://\[YOUR_COMPANY_NAME\].sharepoint.com/sites](https://[YOUR_COMPANY_NAME].sharepoint.com/sites) is displayed as a sub folder.



SharePoint site collections in SharePoint admin center

4.1. Limitations

- The list of site collections is retrieved using the SharePoint search service: a stopped or incorrectly configured search service will prevent the site collections from being discovered.
- Since the external data source entry point is the web app (“root site”), each user must be able to access it: if a user is only allowed to access a specific site collection but not the root site, he won’t be able to use the external data source.

4.2. Office365 app configuration

Create and configure the Office 365 app using these 2 URLs:

- [https://\[YOUR_COMPANY_NAME\].sharepoint.com/_layouts/15/appregnew.aspx](https://[YOUR_COMPANY_NAME].sharepoint.com/_layouts/15/appregnew.aspx)
- [https://\[YOUR_COMPANY_NAME\].sharepoint.com/_layouts/15/appinv.aspx](https://[YOUR_COMPANY_NAME].sharepoint.com/_layouts/15/appinv.aspx)

Use the following permission request XML:

```
<AppPermissionRequests>
<AppPermissionRequest Scope=" http://sharepoint/content/tenant " Right="[RIGHT]" />
</AppPermissionRequests>
```

4.3. Salesforce authentication provider configuration

Create a Microsoft Access Control Service auth provider and use the following authorize endpoint URL:

[https://\[YOUR_COMPANY_NAME\].sharepoint.com/_layouts/15/OauthAuthorize.aspx](https://[YOUR_COMPANY_NAME].sharepoint.com/_layouts/15/OauthAuthorize.aspx)

4.5. External data source configuration

Create a SharePoint Online external data source and connect to the web app using this URL:

[https://\[COMPANY_NAME\].sharepoint.com](https://[COMPANY_NAME].sharepoint.com)

Appendix 5: Querying on SharePoint custom properties

Configuring Custom Properties in SharePoint

To be able to search on custom properties via an external object, a corresponding Managed Property needs to be created by a Sharepoint Administrator to make it indexed.

- To display these properties in external object fields, or use them in SOQL or SOSL **SELECT** queries, set the corresponding Managed Property to **Retrievable**. (In Sharepoint 2010, this option is labeled, “Allow this property to be used in scopes.”)
- To filter on these properties in external objects, or use them as query criteria in a SOQL or SOSL **WHERE** clause, set the corresponding Managed Property to **Queryable**.



Before creating a new managed property in SharePoint, make sure that it is not already available.

For example, no need to create a new managed property to display the SharePoint document path or the SharePoint document extension since they're available by default: <https://technet.microsoft.com/en-us/library/jj219630.aspx>

In the rest of this chapter:

- “CustomProperty” will stand for the internal name of the CustomProperty defined in the Custom Content Type.
- “ManagedCustomProperty” will stand for the Managed Custom property name defined when creating the Managed Property.
- “Non indexed documents” will stand for documents of non searchable default file types. (e.g. jpg/png/pdf/...)

Querying on custom properties

Sharepoint 2010	<p>CustomProperty must be used in the SOQL SELECT clause, whereas the ManagedCustomProperty must be used in the SOQL WHERE clause. Thus two custom fields have to be created in the external object, one to be selected the other one to be used in filters.</p> <p>SOQL Example:</p> <pre>SELECT CustomProperty FROM items_sp2010_x WHERE ManagedCustomProperty=...</pre>
------------------------	--

Sharepoint 2013 SharePoint Online	<p>ManagedCustomProperty must be used both in the SOQL SELECT clause and the SOQL WHERE clause.</p> <p>SOQL Example:</p> <pre>SELECT ManagedCustomProperty FROM items_sp2013_x WHERE ManagedCustomProperty=...</pre> <p>For non indexed documents, it works the same way than for SP2010 (i.e. CustomProperty must be selected) A workaround for this can be to define an Alias on the Managed Property, that will be used both for SELECT and WHERE. (e.g SELECT Alias FROM items_sp2013/Online WHERE Alias=...)</p> <p>Custom properties are not displayed in the External Object record detail page. Defining an Alias is also a workaround for this issue.</p>
--------------------------------------	--

Known limitations

SharePoint 2010	<ul style="list-style-type: none"> properties of type "Number", "Choice Multiple" and "Currency" cannot be used in a SELECT clause. "Date" can be SELECTed but they are likely not to be returned in UTC, so the value can be in a different timezone than expected.
SharePoint 2013	<ul style="list-style-type: none"> properties of type "Multiple Line of text", "Url", "Date" and "Choice dropdown" cannot be used in a WHERE clause. properties of type "Choice Dropdown", "Choice Multiple", "URL" and "Date" cannot be used in a SELECT clause.
SharePoint Online	<ul style="list-style-type: none"> properties of type "Multiple Line of text", "Url" and "Date" cannot be used in a WHERE clause. properties of type "Choice Multiple" and "URL" cannot be used in a SELECT clause.
All versions	<ul style="list-style-type: none"> Properties of type "Number", "Currency" and "Choice Multiple" cannot be used in a SELECT clause for non-indexed documents. When using boolean custom properties (i.e. YesNo) if the corresponding Managed Property is defined as being type of "Text", then the corresponding External Object custom field has to be type of "Text" as well. Then "0"/"1" will have to be use for, respectively, false/true in filters (e.g. WHERE customBooleanWithTextManagedProperty="1"). "0"/"1" will also be displayed as results. If the boolean custom properties are properly mapped on Managed Properties type of YesNo, then the corresponding External Object custom field has to be "Checkbox"

	and will be queryable with usual true/false values. (e.g. WHERE customBooleanWithYesNoManagedProperty=true)
--	---

Appendix 6: Creating custom fields in SharePoint & using external objects relationships



[Click here for a video walkthrough](#)

Lookup relationship

In this example, we use a lookup relationship to dynamically display a list of SharePoint Online documents that are linked to a Salesforce account.

The SharePoint documents have a custom column containing the identifier of the associated Salesforce account.

Step #1: creating a custom column in SharePoint Online

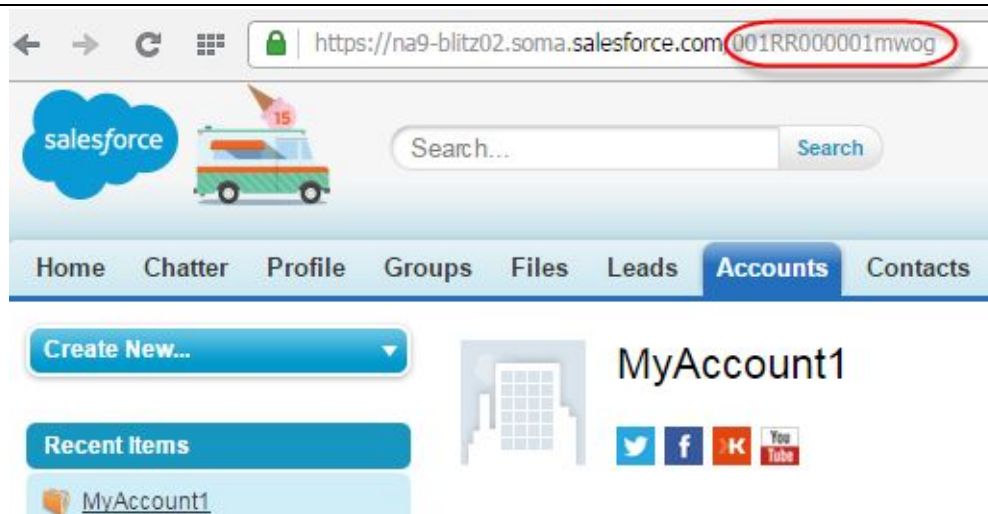
In this example we assume that we have a document library containing a custom column called “MyCustomColumn”.

In the case of a lookup relationship, the custom column contains a Salesforce record identifier: in our case, this is a Salesforce **account** identifier.

	New		Upload		Sync		Share	More ▾
All Documents	...	<input type="text" value="Find a file"/>						
✓		Name		Modified		Modified By		MyCustomColumn
	test lookup 01	...	About a minute ago	<input type="checkbox"/>	Nicolas maquaire	001RR000001mwogYAA		
	test lookup 02	...	About a minute ago	<input type="checkbox"/>	Nicolas maquaire	001RR000001mwogYAA		
	test lookup 03	...	About a minute ago	<input type="checkbox"/>	Nicolas maquaire	001RR000001mwogYAA		



- To retrieve the 15 character account identifier, go to the account details page in Salesforce: the identifier is displayed in your browser address bar.



- You then need to convert this 15 character identifier to an 18 character identifier, for example by using [this online converter](#).

Step #2: creating a managed property in SharePoint Online

In order to query this new column from Salesforce you need to create a new managed property in SharePoint. Let's assume that the managed property is also called MYCUSTOMCOLUMN:

SharePoint admin center

site collections
infopath
user profiles
bcs
term store
records management
search
secure store
apps
settings

Managed Properties | Crawled Properties | Categories

Use this page to view, create, or modify managed properties and map crawled properties to managed properties. Crawled properties are automatically extracted from crawled content. You can use managed properties to restrict search results, and present the content of the properties in search results. Changes to properties will take effect after the next full crawl. Note that the settings that you can adjust depend on your current authorization level.

Filter
Managed property

Total Count = 1

[New Managed Property](#)

PROPERTY NAME	TYPE	MULTI	QUERY	SEARCH	RETRIEVE	REFINE	SORT	SAFE	MAPPED CRAWLED PROPERTIES	ALIASES
MYCUSTOMCOLUMN	Text	-	Query	Search	Retrieve	-	-	-	ows_MyCustomColumn	

managed property

Step #3: creating a new custom field on the external object

Create a new custom field on your Files Connect external object and use "MYCUSTOMCOLUMN" as the value of the external column name (which is the value of the SharePoint managed property).

Custom Fields & Relationships New Custom Fields & Relationships Help ?							
Action	Field Label	API Name	Data Type	Indexed	Controlling Field	External Alias	Modified By
Edit Del	Author	Author__c	Text(255)			Author	Admin User, 6/18/2015 7:43 AM
Edit Del	Comment	Comment__c	Long Text Area(32000)			Comment	Admin User, 6/18/2015 7:43 AM
Edit Del	ContentLength	ContentLength__c	Number(18, 0)			ContentLength	Admin User, 6/18/2015 7:43 AM
Edit Del	CreationDate	CreationDate__c	Date/Time			CreationDate	Admin User, 6/18/2015 7:43 AM
Edit Del	DownloadUrl	DownloadUrl__c	URL(255)			DownloadUrl	Admin User, 6/18/2015 7:43 AM
Edit Del	IsFolder	IsFolder__c	Checkbox			IsFolder	Admin User, 6/18/2015 7:43 AM
Edit Del	MimeType	MimeType__c	Text(255)			MimeType	Admin User, 6/18/2015 7:43 AM
Edit Del	MyCustomField	MyCustomField__c	Text(255)			MYCUSTOMCOLUMN	Admin User, 6/18/2015 7:44 AM
Edit Del	Name	Name__c	Text(255)			Name	Admin User, 6/18/2015 7:43 AM
Edit Del	ParentId	ParentId__c	Text(255)			ParentId	Admin User, 6/18/2015 7:43 AM
Edit Del	UpdateDate	UpdateDate__c	Date/Time			UpdateDate	Admin User, 6/18/2015 7:43 AM
Edit Del	UpdatedBy	UpdatedBy__c	Text(255)			UpdatedBy	Admin User, 6/18/2015 7:43 AM

new custom field on the external object

Step #4 (optional): checking that the custom field can be queried

The fastest way to check that is to create a custom tab for the external object and create a filter that queries on the new custom field:

Step 2. Specify Filter Criteria

Filter By Additional Fields (Optional):


Field	Operator	Value	
MyCustomField	equals	001RR000001mwogYAA	AND
--None--	--None--		AND
--None--	--None--		AND
--None--	--None--		AND
--None--	--None--		

[Add Filter Logic...](#)

Step 3. Select Fields to Display

Available Fields	Selected Fields
ID	Name
Display URL	MyCustomField

filter criteria



All

Edit | Delete | Create New View

Name +	MyCustomField
test lookup 01.docx	001RR000001mwogYAA
test lookup 02.docx	001RR000001mwogYAA
test lookup 03.docx	001RR000001mwogYAA

filter results

Step #5: creating a lookup field on the external object

Create a new lookup field on the external object, the external column name is still "MYCUSTOMCOLUMN".

Custom Fields & Relationships New							
Action	Field Label	API Name	Data Type	Indexed	Controlling Field	External Alias	Modified By
Edit Del	Author	Author__c	Text(255)			Author	Admin User , 6/18/2015 7:43 AM
Edit Del	Comment	Comment__c	Long Text Area(32000)			Comment	Admin User , 6/18/2015 7:43 AM
Edit Del	ContentLength	ContentLength__c	Number(18, 0)			ContentLength	Admin User , 6/18/2015 7:43 AM
Edit Del	CreationDate	CreationDate__c	Date/Time			CreationDate	Admin User , 6/18/2015 7:43 AM
Edit Del	DownloadUrl	DownloadUrl__c	URL(255)			DownloadUrl	Admin User , 6/18/2015 7:43 AM
Edit Del	IsFolder	IsFolder__c	Checkbox			IsFolder	Admin User , 6/18/2015 7:43 AM
Edit Del	MimeType	MimeType__c	Text(255)			MimeType	Admin User , 6/18/2015 7:43 AM
Edit Del	MyCustomField	MyCustomField__c	Text(15)			MYCUSTOMCOLUMN	Admin User , 6/18/2015 9:06 AM
Edit Del	myLookupField	myLookupField__c	Lookup(Account)	✓		MYCUSTOMCOLUMN	Admin User , 6/18/2015 9:07 AM
Edit Del	Name	Name__c	Text(255)			Name	Admin User , 6/18/2015 7:43 AM
Edit Del	ParentId	ParentId__c	Text(255)			ParentId	Admin User , 6/18/2015 7:43 AM
Edit Del	UpdateDate	UpdateDate__c	Date/Time			UpdateDate	Admin User , 6/18/2015 7:43 AM
Edit Del	UpdatedBy	UpdatedBy__c	Text(255)			UpdatedBy	Admin User , 6/18/2015 7:43 AM

New lookup field on the external object

Step #6: viewing the list of SharePoint documents that are related to the account

Edit the account page layout and add the new related list:

MyAccount1

Customize Page | Edit Layout | Printable View | Help for this Page

Show Feed Click to add topics

« Back to List: Custom Object Definitions

items_SPOnline [3] | Contacts [0] | Open Activities [0] | Activity History [0] | Opportunities [0] | Cases [0] | Partners [0] | Notes & Attachments [0]

Account Detail Edit Delete Sharing

Account Owner Admin User [Change] Phone

Account Name MyAccount1 [View Hierarchy] Fax

Parent Account Website

Edit Delete Sharing

items_SPOnline items_SPOnline Help ?

Action	Name	MyCustomField
	test lookup 01.docx	001RR000001mwogYAA
	test lookup 02.docx	001RR000001mwogYAA
	test lookup 03.docx	001RR000001mwogYAA

related list on account using a lookup relationship

Indirect Lookup relationship

In this example, we use an indirect lookup relationship to dynamically display a list of SharePoint Online documents that are linked to a Salesforce account.

The SharePoint documents have a custom column containing the value of a Salesforce account **custom field** (in the “lookup relationship” chapter, this custom column was containing a Salesforce **account identifier**).

Step #1: creating a custom column in SharePoint Online

In this example we assume that we have a document library containing a custom column called “MyCustomColumn”.

In the case of an indirect lookup relationship, the custom column contains the value of a Salesforce record custom field. In our case, this is the value of a Salesforce **account** custom field.

New

Upload

Sync

Share

More ▾

All Documents

...

Find a file

✓	<div></div>	Name		Modified	Modified By	MyCustomColumn
	<div><div></div></div>	test lookup 01	<div></div>	A few seconds ago	<div><div></div></div> Nicolas maquaire	myCustomFieldValue1
	<div><div></div></div>	test lookup 02	<div></div>	A few seconds ago	<div><div></div></div> Nicolas maquaire	myCustomFieldValue1
	<div><div></div></div>	test lookup 03	<div></div>	A few seconds ago	<div><div></div></div> Nicolas maquaire	myCustomFieldValue1

Step #2: creating a managed property in SharePoint Online

Refer to the “lookup relationship” chapter.

Step #3: creating a new custom field on the external object

Refer to the “lookup relationship” chapter.

Step #4 (optional): checking that the custom field can be queried

Refer to the “lookup relationship” chapter.

Step #5: creating a custom field on the account

This field must be unique and have the “external ID” checkbox selected.

Account Custom Fields & Relationships						
		New	Field Dependencies	Account Custom Fields & Relationships Help ?		
Action	Field Label	API Name	Data Type	Indexed	Controlling Field	Modified By
Edit Del	myCustomField	myCustomField__c	Text(255) (External ID) (Unique Case Insensitive)	<input checked="" type="checkbox"/>		Admin User , 6/18/2015 9:31 AM

General Options

Required

☐ Always require a value in this field in order to save a record

Unique

☒ Do not allow duplicate values

☒ Treat "ABC" and "abc" as duplicate values (case insensitive)
 ☐ Treat "ABC" and "abc" as different values (case sensitive)

External ID

☒ Set this field as the unique record identifier from an external system

Default Value

[Show Formula Editor](#)

Use formula syntax: e.g., Text in double quotes: "hello", Number: 25, Percent as decimal: 0.10, Date expression: Today() + 7

new custom field on the account

Step #6: creating an indirect lookup field on the external object

Create a new indirect lookup field on the external object, the external column name is still “MYCUSTOMCOLUMN”.


Custom Fields & Relationships New							
Action	Field Label	API Name	Data Type	Indexed	Controlling Field	External Alias	Modified By
Edit Del	Author	Author__c	Text(255)			Author	Admin User, 6/18/2015 7:43 AM
Edit Del	Comment	Comment__c	Long Text Area(32000)			Comment	Admin User, 6/18/2015 7:43 AM
Edit Del	ContentLength	ContentLength__c	Number(18, 0)			ContentLength	Admin User, 6/18/2015 7:43 AM
Edit Del	CreationDate	CreationDate__c	Date/Time			CreationDate	Admin User, 6/18/2015 7:43 AM
Edit Del	DownloadUrl	DownloadUrl__c	URL(255)			DownloadUrl	Admin User, 6/18/2015 7:43 AM
Edit Del	IsFolder	IsFolder__c	Checkbox			IsFolder	Admin User, 6/18/2015 7:43 AM
Edit Del	MimeType	MimeType__c	Text(255)			MimeType	Admin User, 6/18/2015 7:43 AM
Edit Del	MyCustomField	MyCustomField__c	Text(15)			MYCUSTOMCOLUMN	Admin User, 6/18/2015 9:06 AM
Edit Del	myIndirectLookupField	myIndirectLookupField__c	Indirect Lookup(Account)	✓		MYCUSTOMCOLUMN	Admin User, 6/18/2015 9:33 AM
Edit Del	Name	Name__c	Text(255)			Name	Admin User, 6/18/2015 7:43 AM
Edit Del	ParentId	ParentId__c	Text(255)			ParentId	Admin User, 6/18/2015 7:43 AM
Edit Del	UpdateDate	UpdateDate__c	Date/Time			UpdateDate	Admin User, 6/18/2015 7:43 AM
Edit Del	UpdatedBy	UpdatedBy__c	Text(255)			UpdatedBy	Admin User, 6/18/2015 7:43 AM

new indirect lookup field on the external object





Step #7: viewing the list of SharePoint documents that are related to the account

Edit the account page layout and add the new related list.

Finally, don’t forget to enter a value in the account custom field: this value must be unique.



MyAccount1

[Customize Page](#) | [Edit Layout](#) | [Printable View](#) | [Help for this Page](#)


[Show Feed](#) | [Click to add topics](#)

[Back to List: Custom Object Definitions](#)


[Items_SPOnline \(3\)](#) | [Contacts \(0\)](#) | [Open Activities \(0\)](#) | [Activity History \(0\)](#) | [Opportunities \(0\)](#) | [Cases \(0\)](#) | [Partners \(0\)](#) | [Notes & Attachments \(0\)](#)

Account Detail

[Edit](#) | [Delete](#) | [Sharing](#)

Account Owner	 Admin User [Change]	Phone
Account Name	MyAccount1 [View Hierarchy]	Fax
Parent Account		Website
myCustomField	myCustomFieldValue1	

[Edit](#) | [Delete](#) | [Sharing](#)



items_SPOnline

[items_SPOnline Help](#)

Action	Name	MyCustomField
	test lookup 01.docx	myCustomFieldValue1
	test lookup 02.docx	myCustomFieldValue1
	test lookup 03.docx	myCustomFieldValue1

related list on account using an indirect lookup relationship

Appendix 7: Checking if anonymous access is enabled in a SharePoint web application

1. Central Administration -> Application Management -> Manage web applications
2. Select the web application
3. Click Authentication Provider in the ribbon
4. Click the Zone link
5. Check the "Enable anonymous access" checkbox in the Anonymous Access section

Note that enabling anonymous access does NOT mean that non-authenticated users can connect to your SharePoint farm.

If anonymous access is enabled, Files Connect will not be able to access your web application. Two possible options:

1. Disable anonymous access in Central Admin.
2. Modify the web.config in the ISAPI folder in the SharePoint hive and add the following section in the <configuration> tag:

```
<location path="search.asmx">

    <system.web>

        <authorization>

            <deny users="?"/>

        </authorization>

    </system.web>

</location>
```

This will disable anonymous access to the search.asmx web service.

Appendix 8: Cautions and Warnings

Once file references are created in Salesforce, they will be acted on by any API calls that act on Salesforce files. The most common instance where this could cause problems is in using the SObject or Chatter Connect API to retrieve lists of documents that are, say, owned by a certain user, in a certain group or record, etc.

The problem is, unlike native native Salesforce files, file references have no content, no previews, no thumbnails, etc. If you have any code that expects all Salesforce files to have content, **that code may break when it retrieves file references.**

If you add files references to your organization, you must make sure that any existing code that deals with Chatter files through any Salesforce API is modified to *recognize and handle file references*.

- SObject API: Recognize file references by checking the “ContentLocation” field. If the value is ‘E’, you have a reference file.
- Chatter Connect (REST) API: reference files will return with a 0 in the content size field in the JSON response body.
- Other APIs: Test to see how they perform on file references.