Salesforce Files Connect Implementation Guide

Salesforce, Spring '17

'17

CONTENTS

FILES CONNECT FOR ADMINISTRATORS

The Files Connect Setup Process

The setup process for Files Connect differs for cloud-based and on-premises external data sources.

💡 **Tip:** For detailed visuals, tips, and troubleshooting, see the Files Connect *Setup Guide* and *User Guide*.

First, enable Files Connect, and let users access related external data sources

1. Enable Salesforce Files Connect for Your Organization.
2. Let Users and Administrators Access Files Connect Data Sources.

For cloud-based data sources, create an authentication provider, and then define the source

If you use Google Drive:

1. Create an Authentication Provider for Google Drive.
2. Define an External Data Source for Google Drive.

If you use Microsoft's cloud systems:

1. Create an Authentication Provider for SharePoint Online Using Azure (Preferred Method).
2. Define an External Data Source for SharePoint Online or OneDrive for Business.

If you use Box:

1. Create an Authentication Provider for Box
2. Define an External Data Source for Box

For on-premises data sources, set up a Secure Agent, and then define the source

✏️ **Note:** This process is available only to customers who have the paid permission set license, "Files Connect for on-premises external data sources." This license is no longer available for purchase.

1. Set Up a Secure Agent for SharePoint 2010 or 2013 on a Linux or Windows server to securely connect Salesforce to data stored behind your firewall.
2. Define an External Data Source for SharePoint 2010 or 2013.

Include the external data in global search

To let users access external data in global Salesforce searches, you'll need to create an external object and give users access to its fields. This is an optional step, but highly recommended to best integrate external data with Salesforce.

For per-user data sources, have users authenticate in Salesforce

If you specified per-user authentication for a data source and exposed it through profiles or permission sets, ask authorized users to provide their data source credentials.

Start accessing, sharing, and searching external files!

Now users can access and share external files via the Files tab and feed, and search for them right alongside their Salesforce content.

Enable Salesforce Files Connect for Your Organization

Let users search and share files from external systems like Google Drive and SharePoint.

1. From Setup, enter `Files Connect` in the `Quick Find` box, then select **Files Connect** under **Settings**.

2. Click **Edit**, and then select **Enable Files Connect**.

3. For File Sharing, select one of the following:

   - **Copy** stores a copy of external files in Salesforce. If files are shared with a Chatter group, all group members can access the files, even if they lack access to the external system.

   - **Reference** points to external files stored outside Salesforce. No file previews are available, and file downloads require user access to the external system. (Users must enter credentials for the system in the Authentication Settings for External Systems section of personal setup).

   💡 Tip: Choose the Copy mode if your organization shares files with external customers or partners. Choose the Reference mode to reflect access restrictions from the external system in Salesforce.

Regardless of sharing mode, files in Salesforce don't reflect file revisions in external systems. However, Reference mode points to the latest versions in those systems.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Files Connect for cloud-based external data sources is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Files Connect for on-premises external data sources is available for an extra cost in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To enable Salesforce Files Connect:
- "Customize Application"

Let Users and Administrators Access Files Connect Data Sources

After you enable Files Connect, give users and administrators permission to access specific external data sources from Salesforce.

> 💡 **Tip:** Though you can provide access to data sources via permission sets or profiles, permission sets let you more quickly adjust access for several types of users. Regardless of which method you choose, be sure to give administrators access so they can configure data sources.

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

2. Create a new permission set or profile, or click an existing one.

   If you use a permission set, User License must be set to the default option, "None."

3. For a permission set, click **System Permissions**, then click **Edit**.

   For a profile, click **Edit**, and scroll down to the Administrative Permissions section.

4. Do either of the following, and then click **Save**.

   - To access cloud-based data sources like SharePoint Online, select **Files Connect Cloud**.
   - To access on-premises data sources like SharePoint 2010 or 2013, select **Files Connect On-premises**.

   > 📝 **Note:** The on-premises permission is available with a paid permission set license, "Files Connect for on-premises external data sources." To enable Files Connect on-premises for a user:
   >
   > a. Assign the Files Connect license to the user.
   >
   > b. Create a permission set and add the "Files Connect On-premises" permission to it.
   >
   > c. Assign the permission set to the user.

5. For a permission set, click **Manage Assignments** in the toolbar at the top of the page. Then click **Add Assignments**, select users for the permission set, and click **Assign**.

   > 🛑 **Important:** Include any administrators who need to configure external data sources.

6. If you haven't already, define the external data sources for your organization:

   - Define an External Data Source for SharePoint Online or OneDrive for Business
   - Define an External Data Source for SharePoint 2010 or 2013
   - Define an External Data Source for Google Drive
   - Define an External Data Source for Box

   > 📝 **Note:** If you select an identity type of Named Principal for the data source, skip the steps below. But if you select Per User, read on.

7. In Setup, return to the detail page for the permission set or profile. Then do either of the following:

   - For a permission set, in the Apps section, click **External Data Source Access**.
   - For a profile, go to the Enabled External Data Source Access related list.

8. Click **Edit**, add specific data sources to the Enabled External Data Sources list, and click **Save**.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Files Connect for cloud-based external data sources is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Files Connect for on-premises external data sources is available for an extra cost in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To set permissions:
- "Customize Application"

To use Files Connect for on-premises external data sources:
- "API Enabled"

(Users enter their credentials when they first access external data sources, or from their personal settings on theAuthentication Settings for External Systems page.)

Create an Authentication Provider for Box

To use Box as an external data source, you must create an authentication provider for it in Salesforce.

> 💡 **Tip:** For detailed visuals, tips, and troubleshooting, see the Files Connect *Setup Guide* and *User Guide*.

Create an Authentication Provider in Salesforce

1. In Setup, enter `Auth. Providers` in the `Quick Find` box, then select **Auth. Providers**.

2. Click **New**.

3. For `Provider Type`, select **OpenID Connect**, and then set the following options:

   - `Name`—Enter the name you want to appear in Salesforce.

   - `URL Suffix`—Enter a suffix you want to appear at the end of the URL path. By default, the suffix reflects the Name entry.

   - `Consumer Key`—Enter any placeholder value. You will fill this in after you create the Box application in Step 5.

   - `Consumer Secret`—Enter any placeholder value. You will fill this in after you create the Box application in Step 5.

   - `Authorize Endpoint URL`—Enter `https://account.box.com/api/oauth2/authorize`

   - `Token Endpoint URL`— Enter `https://api.box.com/oauth2/token`

   - `User Info Endpoint URL`— Leave empty.

   - `Default Scopes`—Leave empty.

4. Click **Save**. Then, at the bottom of the Auth. Provider detail page, copy the `Callback URL` entry to a text file. (You'll use this when creating the Box application.)

5. Create a Box application. Then return to step 6.

6. When you have created the Box application, edit the Salesforce Auth Provider and replace the following values with those from the Box app.

   - `Consumer.Key`: the Box client_id.

   - `Consumer.Secret`: the Box client_secret.

7. Click **Save**. Your Box authentication provider is now ready to be used.

Create a Box Application

1. Using the credentials of your Box admin account, log in to `https://app.box.com/developers/services`.

2. Click **Create a Box Application**.

3. Enter a project name, select Box content, and click **Create Application**.

EDITIONS

Available in: Salesforce Classic

Available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To create authentication providers:
- "Customize Application"

  AND

  "Manage Auth. Providers"

4

4. Click **Configure your application**.

5. In the **redirect_uri** field, paste the Salesforce callback URL specified in the OAuth2 specification.

6. Copy the **client_id** and **client_secret** values to a text file. Enter these values at step 6 of Create an Authentication Provider in Salesforce.

Define an External Data Source for Box

Let users access their Box content from Files home, feed posts, and search.

1. From Setup in Salesforce Classic, enter `External Data Sources` in the Quick Find box, then select **External Data Sources**.

2. Click **New External Data Source**. Then set the following options.

Field	Description
Label	A user-friendly name for the data source displayed in the Salesforce user interface.
Name	A unique identifier used to refer to this external data source definition through the API. The **Name** field can contain only underscores and alphanumeric characters. It must be unique, begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.
Type	Choose **Files Connect: Box**
Identity Type	The identity type used to authenticate to the external data source. Select **Per User** to require separate credentials for each user who accesses the data source. (Administrators must enable the data source for specific permission sets and profiles. Users then enter their credentials when first accessing the data source.)
Authentication Protocol	The protocol used to access Box. Select **OAuth 2.0**.
Authentication Provider	Enter the Box Authentication Provider.
Scope	Leave blank.
Start Authentication Flow on Save	Select to immediately test the settings above.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To define an external data source:
- "Customize Application"

Create an Authentication Provider for Google Drive

To use Google Drive as an external data source, you must create an authentication provider for it in Salesforce. The process begins with creating a related project in the Google Developers console.

> 💡 **Tip:** For detailed visuals, tips, and troubleshooting, see the Files Connect *Setup Guide* and *User Guide*.

Create a Project in the Google Developers Console

1. Using the credentials of your Google App for Work admin account, log in to **`https://console.cloud.google.com`**.
2. In the title bar, expand **Go to Project** and click **Create Project**.
3. Enter a project name, and click **Create**.
4. In the project dashboard, click the menu icon in the top left, then click **API Manager**.
5. In the API manager, go to the Google APIs tab and search for `Google Drive API`.
6. Click **Google Drive API** in the search results, then click **Enable API**.
7. Click **Credentials**, located in the left-hand menu.
8. In the OAuth Consent Screen tab, enter a valid email address and product name. Then click **Save**.
9. In the Credentials tab, click **Add credentials** and select `OAuth client ID`.
10. Select `Web application` and click **Create**.
11. Copy the client ID and client secret values to a text file. You'll use these values when creating an authentication provider in Salesforce.

Create an Authentication Provider in Salesforce

1. In Setup, enter `Auth. Providers` in the `Quick Find` box, then select **Auth. Providers**.
2. Click **New**.
3. For `Provider Type`, select **OpenID Connect**, and then set the following options:
   - `Name`—Enter the name you want to appear in Salesforce.
   - `URL Suffix`—Enter the suffix at the end of the URL path. For example, in the path, `https://login.salesforce.com/services/authcallback/00Dx00000000001/MyGoogleProvider`, the suffix is "MyGoogleProvider"
   - `Consumer Key`—Enter the client ID you copied when creating the Google project.
   - `Consumer Secret`—Enter the client secret you copied when creating the Google project.
   - `Authorize Endpoint URL`—Enter `https://accounts.google.com/o/oauth2/auth?access_type=offline&approval_prompt=force`
   - `Token Endpoint URL`— Enter `https://accounts.google.com/o/oauth2/token`
   - `Default Scopes`—Enter `openid email profile https://www.googleapis.com/auth/drive`
4. Click **Save**. Then, at the bottom of the Auth. Provider detail page, copy the `Callback URL` entry to a text file. (You'll use this when editing the Google project.)

Edit the Project in the Google Developer Console

1. In the API Manager, click **Credentials**, located in the left-hand menu.

2. Click on the previously created Web application.

3. In the Authorized Redirect URIs section, add the Callback URL you copied when creating the authentication provider in Salesforce.

4. Click **Save**.

Define an External Data Source for Google Drive

Let Chatter users access their Google Drive content from the Files tab, feed posts, and search. Salesforce supports Google documents, spreadsheets, presentations, and drawings.

1. From Setup, enter `External Data Sources` in the `Quick Find` box, then select **External Data Sources**.

2. Click **New External Data Source**. Then set the following options.

Field	Description
Label	A user-friendly name for the data source displayed in the Salesforce user interface.
Name	A unique identifier used to refer to this external data source definition through the API. The **Name** field can contain only underscores and alphanumeric characters. It must be unique, begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.
Type	Choose **Files Connect: Google Drive**
Identity Type	The identity type used to authenticate to the external data source. Select **Per User** to require separate credentials for each user who accesses the data source. (Administrators must enable the data source for specific permission sets and profiles. Users then enter their credentials when first accessing the data source..) Select **Named Principal** to use the same set of credentials for every user who accesses the data source from Salesforce.
Authentication Protocol	The protocol used to access Google Drive. Select **OAuth 2.0**.
Authentication Provider	Enter the Google Drive authentication provider.

Field	Description
Scope	Leave blank.
Start Authentication Flow on Save	Select to immediately test the settings above.

Create an Authentication Provider for SharePoint Online Using Azure (Preferred Method)

To use one of Microsoft's cloud-based external data sources, you must create an authentication provider for it in Salesforce and register that provider in a Microsoft Azure web application.

💡 **Tip:** For detailed visuals, tips, and troubleshooting, see the Files Connect *Setup Guide* and *User Guide*.

To fully configure an authentication provider, complete these steps.

1. Create an Authentication Provider Using Placeholder Values

2. Register a Web Application in the Azure Management Console

✏️ **Note:** If you do not have access to the Azure Management Console, or you need to authenticate to OneDrive for Business, follow these instructions to register your app in Office 365: Create an Authentication Provider for SharePoint Online or OneDrive for Business Using Office 365 (Alternate Method).

3. Configure the Authentication Provider in Salesforce

Create an Authentication Provider Using Placeholder Values

The authentication provider provides the redirect URI you need to register your app.

1. In Setup, enter `Auth. Providers` in the `Quick Find` box, then select **Auth. Providers**.

2. Click **New**.

3. For `Provider Type`, select **OpenID Connect**, and then set the following options.

• `Name`—Enter the name you want to appear in Salesforce.

• `URL Suffix`—Enter a suffix you want to appear at the end of the URL path. By default, the suffix reflects the Name entry.

• `Consumer Key`—Enter a placeholder value.

• `Consumer Secret`—Enter a placeholder value.

• `Authorize Endpoint URL`—Enter a placeholder that begins with *https*.

• `Token Endpoint URL`—Enter a placeholder that begins with *https*.

• `Default Scopes`—Leave empty.

4. Click **Save**. Then, at the bottom of the Auth. Provider detail page, copy the `Callback URL` entry to a text file.

Register a Web Application in the Azure Management Console

1. Log in to Azure at `https://manage.windowsazure.com/`. (If you have any trouble, connect to Azure with your browser in "incognito" mode.)

2. In the left navigation panel, select **Active Directory**.

3. Select your active directory.

4. On the Active Directory page, select **Applications** from the header menu.

5. Click **Add** in the footer menu.

6. Choose **Add an application my organization is developing**.

7. Enter a name for your app, and choose **Web Application and/or Web API**. Click the arrow.

8. On the **App Properties** screen, enter:

   - `Sign-on URL`—Enter a URL. (You can change this value later.)
   - `App ID URI`—Enter a unique URI. (You can change this value later.)

9. Click the checkmark to complete.

10. Once the app is created, click **Configure** from the header menu.

11. Copy the `Client ID` to a text file—you need this ID to configure the auth provider in Salesforce.

12. Create a key with a duration of 1 year or 2 years. (You'll see the key value after you save.)

13. Update `Reply URL` with the callback URL that you copied from your Salesforce Authentication Provider.

14. Remove any existing application permissions.

15. Click **Add application** and add Office 365 Sharepoint Online.

16. Click **Delegated Permissions**, and then click the arrow to add the delegated permissions you want.

17. Click **Save** from the footer menu.

18. Copy the displayed key value to your text file.

Configure the Authentication Provider in Salesforce

In Salesforce, replace the original placeholder values with the correct ones from the Azure app.

1. In Setup, enter `Auth. Providers` in the `Quick Find` box, then select **Auth. Providers**.

2. Click **Edit** next to the authentication provider you created previously.

3. Change the following values.

   - `Consumer Key`—Enter the Client Id you copied to a text file.
   - `Consumer Secret`—Enter the key you copied to a text file.
   - `Authorize Endpoint URL`—Enter the URL as follows:
     `https://login.microsoftonline.com/common/oauth2/authorize?prompt=consent&`
     `resource=https%3A%2F%2FYOUR_TENANT.sharepoint.com%2F`
   - `Token Endpoint URL`—Enter the URL as follows:
     `https://login.microsoftonline.com/common/oauth2/token`

- **SharePoint Online example**
  ```
  https://login.microsoftonline.com/common/oauth2/authorize?prompt=consent&
  resource=https%3A%2F%2Fcontenthubblitz.sharepoint.com%2F
  ```

4. Click **Save**. Your authentication provider is now ready for use.

Create an Authentication Provider for SharePoint Online or OneDrive for Business Using Office 365 (Alternate Method)

To use one of Microsoft's cloud-based external data sources, you must create an authentication provider for it in Salesforce and register that provider in an Office 365 app.

> 💡 Tip: For detailed visuals, tips, and troubleshooting, see the Files Connect *Setup Guide* and *User Guide*.

To fully configure an authentication provider, complete these steps.

1. Create an Authentication Provider Using Placeholder Values

2. Register an Office 365 App

> 📝 Note: If you have access to the Azure Management Console, you can register your provider using Azure: Create an Authentication Provider for SharePoint Online Using Azure (Preferred Method) on page 8

3. Edit the Authentication Provider in Salesforce

Create an Authentication Provider Using Placeholder Values

1. In Setup, enter `Auth. Providers` in the `Quick Find` box, then select **Auth. Providers**.

2. Click **New**.

3. For `Provider Type`, select **Microsoft Access Control Service**, and then set the following options.

   - `Name`—Enter the name you want to appear in Salesforce.
   - `URL Suffix`—Enter a suffix you want to appear at the end of the URL path. By default, the suffix reflects the `Name` entry.
   - `Consumer Key`—Enter a placeholder value.
   - `Consumer Secret`—Enter a placeholder value.
   - `Authorize Endpoint URL`—Enter a placeholder that begins with *https*.
   - `Token Endpoint URL`—Enter a placeholder that begins with *https*.
   - `Default Scopes`—Leave empty.

4. Click **Save**. Then, at the bottom of the Auth. Provider detail page, copy the `Callback URL` entry to a text file. (You use this when registering an Office 365 app.)

Register an Office 365 App

1. Log in to your Office365 account as an administrator, and go to one of the following URLs.

SharePoint Online

```
https://your company name.sharepoint.com/site collection
path/_layouts/15/appregnew.aspx
```

OneDrive for Business

```
https://your company name-my.sharepoint.com/_layouts/15/appregnew.aspx
```

2. Set the following options.

- `Client Id`—Click **Generate**, and copy the generated value to a text file.

- `Client Secret`—Click **Generate**, and copy the generated value to a text file.

- `Title`—Enter a name for the app.

- `App Domain`—Enter the domain name of your Salesforce org.

- `Redirect URL`— Enter the Callback URL you copied when creating the Authentication Provider in Salesforce.

3. Click **Create**.

   Now you configure the newly created app to access SharePoint resources.

4. Go to one of the following URLs.

   SharePoint Online

   ```
   https://your company name.sharepoint.com/site collection
   path/_layouts/15/appinv.aspx
   ```

   OneDrive for Business

   ```
   https://your company name-my.sharepoint.com/_layouts/15/appinv.aspx
   ```

5. Set the following options.

   - `App Id`—Enter the Client Id you copied to a text file, then click **Lookup**.

   - `Title`—Keep the default value.

   - `App Domain`—Keep the default value.

   - `Redirect URL`—Keep the default value.

   - `Permission Request XML`—Enter a string with this format.

     SharePoint Online

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

     OneDrive for Business

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

6. For SharePoint Online, replace [SCOPE] with one of these values.

   🛑 Important: Office 365 recognizes only these scope URLs; copy them exactly, without changes.

   - `http://sharepoint/content/sitecollection/web` to let users access a single site (but not its subsites).

Files Connect for Administrators

Create an Authentication Provider for SharePoint Online or
OneDrive for Business Using Office 365 (Alternate Method)

- `http://sharepoint/content/sitecollection` to let users access a single site collection (including all subsites).
- `http://sharepoint/content/tenant` to let users access all site collections.

7. Replace [PLACEHOLDER] with one of these values:

- `Read`
- `Write`
- `Manage`
- `Full Control`

For details about the differences between permission levels above, see the Microsoft website.

8. Click **Create**.

Edit the Authentication Provider in Salesforce

In Salesforce, replace the original placeholder values with the correct ones from the Office 365 app.

1. In Setup, enter `Auth. Providers` in the `Quick Find` box, then select **Auth. Providers**.

2. Click **Edit** next to the authentication provider you created previously.

3. Change the following values:

- `Consumer Key`—Enter the Client Id you copied to a text file.
- `Consumer Secret`—Enter the Client Secret you copied to a text file.
- `Authorize Endpoint URL`—Enter the URL of the OAuthAuthorize.aspx page in Office 365. The URL format is as follows.

  SharePoint Online
  ```
  https://your company name.sharepoint.com/site collection
  path/_layouts/15/OauthAuthorize.aspx
  ```

  OneDrive for Business
  ```
  https://your company name-my.sharepoint.com/_layouts/15/OauthAuthorize.aspx
  ```

- `Token Endpoint URL`— Enter a URL in the following format.

  SharePoint Online
  ```
  https://accounts.accesscontrol.windows.net/your company
  nameonmicrosoft.com/tokens/OAuth/2?resource=00000003-0000-0ff1-ce00-000000000000/your
  company namesharepoint.com@your company name.onmicrosoft.com
  ```

  OneDrive for Business
  ```
  https://accounts.accesscontrol.windows.net/your company
  nameonmicrosoft.com/tokens/OAuth/2?resource=00000003-0000-0ff1-ce00-000000000000/your
  company name-my.sharepoint.com@your company name.onmicrosoft.com
  ```

4. Click **Save**. Your authentication provider is now ready for use.

12

Define an External Data Source for SharePoint Online or OneDrive for Business

With Files Connect and Chatter, Salesforce can access content from Microsoft's cloud-based systems.

1. From Setup, enter `External Data Sources` in the `Quick Find` box, then select **External Data Sources**.

2. Click **New External Data Source**. Then set the following options.

Field	Description
Label	A user-friendly name for the data source displayed in the Salesforce user interface.
Name	A unique identifier used to refer to this external data source definition through the API. The **Name** field can contain only underscores and alphanumeric characters. It must be unique, begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.
Type	Choose **Files Connect: Microsoft SharePoint Online** or **Files Connect: Microsoft OneDrive for Business**.

Site URL	The URL of your SharePoint site, site collection, or web app.
	
	⊘ Important: The URL must begin with *https*. It should look like this:
	`https://salesforce.sharepoint`
	`.com/HRSite`
	
	(Don't copy the URL seen in the browser when accessing SharePoint. It should not look like this:
	`https://salesforce.sharepoint.`
	`com/HRSite/SitePages`
	`/Home.aspx`)

Exclude Other Site Collections	Accesses only the site collection specified by the URL, ignoring any other site collections. This should always be enabled if any users are currently allowed to access the root site collection.
Identity Type	The identity type used to authenticate to the external data source. Select **Per User** to require separate credentials for each user who accesses the data source.

Field	Description
	(Administrators must enable the data source for specific permission sets and profiles. Users then enter their credentials when first accessing the data source.)
	Select **Named Principal** to use the same set of credentials for every user who accesses the data source from Salesforce.
Authentication Protocol	The protocol used to access SharePoint Online.
	Select **OAuth 2.0**.
Authentication Provider	Enter the SharePoint Online authentication provider.
Scope	Leave blank.
Start Authentication Flow on Save	Select to immediately test your settings or to create an external object for this external data source.

Set Up a Secure Agent for SharePoint 2010 or 2013

A Secure Agent provides secure communication between Salesforce and on-premises data in SharePoint 2010 or 2013. The Files Connect on-premises solution is available only to customers who already own the license.

📝 Note: The Secure Agent setup process is available only to customers who have the paid permission set license, "Files Connect for on-premises external data sources." This license is no longer available for purchase.

To fully configure a Secure Agent, complete these steps:

1. Create a Connected App for the Secure Agent
2. Create a Profile and User Specific to the Secure Agent
3. Create the Agent in Salesforce, and Download the Installer to Your Server
4. Install and Run the Agent on a Windows Server or a Linux Server
5. Install Secure Agent Plug-ins for Your On-premises Data Source
6. Update Previously Installed Plug-ins
7. Import Any Required Certificates
8. Track and Troubleshoot Secure Agent Activity

💡 Tip: For a visual walk-through, see this video tutorial of Secure Agent setup.

Create a Connected App for the Secure Agent

1. In Setup, enter *Apps* in the Quick Find box, then select **Apps**.
2. In the Connected Apps section, click **New**.

14

3. In the Basic Information section, enter the following settings:

   - `Connected App Name`—Enter a distinctive name like "Secure Agent App."
   - `API Name`—Leave the default value.
   - `Contact Email`—Enter your administrator's address.

4. In the API section, select **Enable OAuth Settings**, and enter the following settings:

   - `Callback URL`—Enter `https://login.salesforce.com` for a production instance, or `https://test.salesforce.com` for a sandbox.
   - `Use Digital Signatures`—*Deselect* this option.
   - `Selected OAuth Scopes`—Add "Access and manage your data (api)" and "Perform requests on your behalf at any time (refresh_token, offline_access)."

5. Click **Save**.

6. In Setup, enter *Connected Apps* in the `Quick Find` box, then select the option for managing connected apps.

7. Next to the new app, click **Edit**, and then enter the following settings:

   - `Permitted Users`—Select "Admin approved users are pre-authorized."
   - `IP Relaxation`—Select "Relax IP restrictions."

8. Click **Save**.

Create a Profile and User Specific to the Secure Agent

1. In Setup, enter *Profiles* in the `Quick Find` box, then select **Profiles**.

2. Next to the Standard User profile, click **Clone**.

3. For `Profile Name`, enter a distinctive name like "Secure Agent profile."

4. Click **Save**.

5. Next to the new profile, click **Edit**.

6. In the Connected App Access section, select the connected app you created for the agent.

7. In the Administrative Permissions section, select **Modify Secure Agents**.

8. Click **Save**.

9. In Setup, enter *Users* in the `Quick Find` box, then select **Users**.

10. Click **New User**.

11. For `Profile`, select the profile you created for the agent. Then complete the remaining required fields, and click **Save**.

    🛑 Important: Be sure to *deselect* "Generate new password and notify user immediately."

Create the Agent in Salesforce, and Download the Installer to Your Server

1. In Setup, enter *Secure Agents* in the `Quick Find` box, then select **Secure Agents**.

2. Click **New Secure Agent**.

3. Enter a **Label** for the user interface and **Name** for the API.

> ✏️ **Note:** Choose the label carefully, because you can't change it. Salesforce relies on a consistent label to remain connected to the agent.

4. For **Proxy User**, enter the user you created for the Secure Agent.

5. Click **Save**.

6. On the details page, click **Download Installer**, and then choose **Linux Agent** or **Windows Agent**.

7. In Setup, enter `Apps` in the `Quick Find` box, then select **Apps**, and click the name of the connected app you created. Then, in the API section, copy the Consumer Key value to a text file.

8. To your server, copy the text file and the downloaded installer file (sfdc-agent.zip for Windows, or sfdc-agent.run for Linux).

> ⛔ **Important:** Make sure the server can access both Salesforce and your on-premises data source, and has Java 6.x or 7.x installed.

Install and Run the Agent on a Windows Server

1. Extract the files in sfdc-agent.zip. Then double-click SecureAgentInstaller.exe

2. Click **Next**, and enter an installation folder. Click **Next** again, and finish initial installation.

3. When the configuration window appears, enter proxy settings used to connect to Salesforce.

> 💡 **Tip:** To change proxy settings after installation (due to a new password for example), enter the `agent:proxyconfig` command in the agent interface.

4. For Login Server Type, choose **Production** or **Sandbox**.

> 💡 **Tip:** To later change this and following configuration settings, you must uninstall and reinstall the agent.

5. For Oauth Client Key, enter the Consumer Key value you copied to the text file.

6. For Encryption Settings, select one of the following:

   - **Generate** to randomly generate a 1,024-bit public/private key pair. See the Re-use existing certificate setting if you need another key size. Then note the displayed path to the generated *.509 certificate file. You reference this path in the Salesforce connected app.

   - **Re-use existing keystore** to reuse a key pair from a previous agent installation. The keystore is in this location: `[agent installation folder]\etc\auth.jks`.

     > ✏️ **Note:** If you select an existing keystore, skip to step 10.

   - **Re-use existing certificate** to select your own certificate and private key. This option enables you to use a different key size. Contact Salesforce for more information.

7. In Salesforce, from Setup, enter `Apps` in the `Quick Find` box, then select **Apps**.

8. Click **Edit** next to the connect app, and select **Use Digital Signatures**.

9. Click **Choose File**, and select the *.509 certificate. Then click **Save**.

10. Return to the agent installer, and click **Next** to complete the installation.

11. Click **Install Agent as Service** to start the "Salesforce Secure Agent" service on your server.

> 💡 **Tip:** To access services in Windows, choose **Start** > **Administrative Tools** > **Services**.

Install and Run the Agent on a Linux Server

1. Run the installer using one of these commands:

   - Production instance:

     ```
     ./sfdc-agent.run
     ```

   - Sandbox instance:

     ```
     ./sfdc-agent.run -l https://test.salesforce.com
     ```

   - Production instance with your own public/private key pair:

     ```
     ./sfdc-agent.run -l https://login.salesforce.com -p [private key filename].PKCS8 -f
     [public key filename].X509
     ```

   - Production instance with a keystore generated during a previous installation:

     ```
     ./sfdc-agent.run -l https://login.salesforce.com -j [path to *.jks file]
     ```

     You'll find the *.jks file here: *[agent installation folder]/etc/auth.jks*

2. Follow the on-screen instructions to enter an installation folder and proxy settings.

   > 💡 **Tip:** To change proxy settings after installation, enter the `agent:proxyconfig` command in the agent interface.

3. When the installer prompts you for an Oauth Client Key, enter the Consumer Key value you copied to the text file.

   > 📝 **Note:** If you specified a keystore generated during a previous installation, skip to step 8.

4. If prompted, generate a random 1,024-bit public/private key pair. Then note the displayed path to the generated *.509 certificate file. You reference this path in the Salesforce connected app.

   > 📝 **Note:** Contact Salesforce if you need to use a different key size.

5. In Salesforce, from Setup, enter *Apps* in the `Quick Find` box, then select **Apps**.

6. Click **Edit** next to the connect app, and select **Use Digital Signatures**.

7. Click **Choose File**, and select the *.509 certificate. Then click **Save**.

8. Return to the agent installer, and press Enter to complete the installation.

9. Start the agent with this command: *[agent installation folder]/bin/start*

Install Secure Agent Plug-ins for Your On-premises Data Source

To connect a Secure Agent to an external data source in Salesforce, you need to install the necessary plug-ins.

1. In Setup, enter *Secure Agents* in the `Quick Find` box, then select **Secure Agents**.

2. Click an agent name to access its details page.

3. In the Secure Agent Plugins list, click **New**.

   For SharePoint 2010 or 2013, you'll need to install the following plug-ins:

   - Files Connect SharePoint

- Files Connect Remote Connector Service
- Secure Transport Client Service

4. To install a plug-in, select it from the Type menu, enter a distinctive name, and click **Save**. Repeat the process for each required plug-in.

Update Previously Installed Plug-ins

When plug-in updates are available, administrators receive weekly email notifications.

1. In Setup, enter `Secure Agents` in the `Quick Find` box, then select **Secure Agents**.

2. In the Secure Agent Plugins list, if the Update Available column states "Yes," click **Edit** for that plug-in.

3. Select **Update to the recommended version on save**, and click **Save**.

Import Any Required Certificates

In the agent interface, you can press the TAB key to access a variety of commands. If your SharePoint server requires a self-signed certificate, or a certificated signed by an unofficial authority, you must use the `rcs:importcert` command. Then enter the path to import the self-signed certificate, or the root certificate of the authority, into the Secure Agent trust store.

The `rcs:listcert` command lists all certificates currently in the trust store, while `rcs:deletecert` deletes the specified certificate from the store.

Track and Troubleshoot Secure Agent Activity

Download log files to precisely monitor agent events.

1. In Setup, enter `Secure Agents` in the `Quick Find` box, then select **Secure Agents**.

2. Click the name of a previously created Secure Agent to open its detail page.

3. Click either of the following:

- **Download Logs** to download a compressed .zip file containing text logs.
- **Download Diagnostics** to see the current agent state, including the list of installed plug-ins and Java virtual machine status.

Ensure Access with Secure Agent Clusters

Secure Agent clusters provide failover protection, ensuring that Salesforce users can always access on-premises external data sources like SharePoint 2010 or 2013.

> 📝 **Note:** The Secure Agent setup process requires a paid permission set license, "Files Connect for on-premises external data sources." This license is no longer available for purchase.

Create the Secure Agent Cluster

1. Create multiple Secure Agents on different servers by repeating this process: Set Up a Secure Agent.

2. From Setup, enter `Secure Agent Clusters` in the `Quick Find` box, then select **Secure Agent Clusters**.

3. Click **New Secure Agent Cluster**.

4. Enter a **Label** for the user interface and **Name** for the API.

5. To add available agents to the cluster, select them, and click **Add**.

   Change the priority order in which agents are used by moving them up or down in the Selected Secure Agents list. The accessible agent with highest priority is used first.

6. Click **Save**.

Check Cluster Status

1. From Setup, enter `Secure Agent Clusters` in the `Quick Find` box, then select **Secure Agents Clusters**.

2. Click a cluster name to access its details page.

3. Note the overall status for the cluster. Green indicates that all agents are accessible, yellow that some are, and red that none are.

4. Note the status of individual agents and these additional details:

   - The Priority column shows the order in which agents are used. To change priority, click **Edit**, and move agents up or down in the Selected Secure Agents list.

   - The Active column indicates which agent is currently in use.

Define an External Data Source for SharePoint 2010 or 2013

Let Salesforce access data in your on-premises system. Files Connect and Chatter make it possible. The Files Connect on-premises solution is available only to customers who already own the license.

📝 **Note:** This setup process is available only to customers who have the paid permission set license, "Files Connect for on-premises external data sources." This license is no longer available for purchase.

1. From Setup, enter `External Data Sources` in the `Quick Find` box, then select **External Data Sources**.

2. Click **New External Data Source**. Then set the following options.

Field	Description
Label	A user-friendly name for the data source displayed in the Salesforce user interface.
Name	A unique identifier used to refer to this external data source definition through the API. The **Name** field can contain only underscores and alphanumeric characters. It must be unique, begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.
Type	Choose **Files Connect: Microsoft SharePoint**
Secure Agent	A service running on a Linux or Windows server on your intranet that lets you securely connect Salesforce to your on-premises SharePoint server. See Set Up a Secure Agent for SharePoint 2010 or 2013.
Site URL	The URL of your SharePoint site, site collection, or web app. ⛔ **Important:** The URL must begin with *https* and end with the site name. (Don't copy the URL seen in the browser when accessing SharePoint.)
Identity Type	The identity type used to authenticate to the external data source. Select **Per User** to require separate credentials for each user who accesses the data source. (Administrators must enable the data source for specific permission sets and profiles. Users then enter their credentials when first accessing the data source.)

Field	Description
	Select **Named Principal** to use the same set of credentials for every user who accesses the data source from Salesforce.
Authentication Protocol	The protocol required to access SharePoint. Select **Password Authentication**. (This option supports HTTP Basic and NTLM authentication.)
Administration Username	The username Salesforce uses to test the connection to SharePoint. You don't need to enter a SharePoint administrator's username. However, ensure that the credentials you use have adequate privileges to access the data source, perform searches, and return information.
Administration Password	The password Salesforce uses to test the connection to SharePoint.

📝 **Note:** Salesforce users can't access SharePoint 2010 if anonymous access is enabled for the web application.

Include a Files Connect Data Source in Global Search

Combine searches for Salesforce data with external data from Google Drive, SharePoint, OneDrive for Business, or Box. Via the API, developers can automate the process with supported SOQL or SOSL queries.

To include external data in global searches or API queries, first create a related external object. External objects behave similarly to custom objects, but map to data stored outside Salesforce in an external system like SharePoint. Each external object maps to a data table, and the object fields map to accessible table columns.

💡 **Tip:** External objects support lookup relationships similar to custom objects, letting you integrate external data into related lists and other areas throughout Salesforce. For details, see External Object Relationships.

To fully configure global search, complete these steps:

1. Choose the Layout for Global Search Results
2. Create an External Object from an External Data Source
3. Give Users Access to the External Object Fields
4. Create a Custom Tab for the External Object (Lightning Experience Only)

To automate search with SOQL or SOSL, review the supported queries for your data source:

- SOQL and SOSL Support for SharePoint and OneDrive External Objects
- SOQL and SOSL Support for Google Drive External Objects

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Files Connect for cloud-based external data sources is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Files Connect for on-premises external data sources is available for an extra cost in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To create an external object and provide access to its fields:

- "Customize Application"

Choose the Layout for Global Search Results

By default, Files Connect external objects use the standard search results layout for Chatter and the Files tab. If you want to display customized search layouts for these objects, complete these quick steps.

1. From Setup, enter `Files Connect Settings` in the `Quick Find` box, then select **Files Connect Settings**.

2. Select **Use External Object Search Layout**.

Create an External Object from an External Data Source

1. Define an external data source that supports search:

   - SharePoint Online or OneDrive for Business
   - SharePoint 2010 or 2013
   - Google Drive
   - Box

2. In Setup, enter `External Data Sources` in the `Quick Find` box, then select **External Data Sources**.

3. Click the data source name to access the details page.

4. Click **Validate and Sync**.

   > **Note:** Note: If the **Validate and Sync** button is disabled, edit the **Authentication Settings for External Systems** to enable the `Start Authentication Flow on Save` checkbox.

5. Select the table named "items_[data source]." Then click **Sync** to create an external object that maps to the entire source.

   Now you deploy the object to make the data it contains available to users.

6. Choose **Build** > **Develop** > **External Objects**.

7. Click **Edit** next to the new external object.

8. At the bottom of the page, click **Deployed**, and then click **Save**.

Give Users Access to the External Object Fields

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

2. Click a permission set in which you enabled Files Connect.

3. In the Apps section, click **Object Settings**.

4. Click the name of the external object.

5. Click **Edit**, and enable the necessary Read permissions (for the object itself, and all fields you want to reveal in Salesforce).

6. Click **Save**.

Create a Custom Tab for the External Object (Lightning Experience Only)

1. In Setup, enter `Tabs` in the search bar, then select **Tabs**.

2. Click **New** in the `Custom Object Tabs` section.

3. In Step 1 of the setup wizard, enter the name of the custom object you created from your external data source.

4. In Step 2, choose the availability and visibility of the tab to profiles. The tab does not need to be visible, but it does need to be accessible—choose either **Default On** or **Tab Hidden**.

5. Complete Step 3 and click **Save**.

SOQL and SOSL Support for SharePoint and OneDrive External Objects

SharePoint and OneDrive external objects support these standard fields and any custom fields you enable.

📝 Note: Queries on specific fields return only documents that the external data source indexed.

Field Name	Queryable	Sortable
Author	Yes	Yes
Comment	No	Yes
ContentLength	Yes	Yes
CreationDate	Yes	Yes
DisplayUrl	No	Yes
DownloadUrl	No	No
ExternalId	Yes	Yes
IsFolder	Yes	Yes
	📝 Note: Not supported for SharePoint 2010 or 2013.	
MimeType	Yes	Yes
Name	Yes	Yes
UpdateDate	Yes	Yes
UpdatedBy	Yes	Yes

📝 Note: You can also use `ParentId_c` as query criteria to retrieve the list of documents in a folder. However, that field isn't displayed in query results unless your query specifies a `ParentId__c` value.

SOQL and SOSL Support for Google Drive External Objects

Files Connect supports all standard Google Drive properties, but not custom properties. The following properties have different field names in Salesforce external objects:

Google Property	Salesforce Field
alternateLink	DisplayUrl
createDate	CreationDate

Google Property	Salesforce Field
description	Comment
downloadURL	contentStreamUri
editable	readOnly
fileSize	ContentLength
id	ExternalId
lastModifyingUserName	UpdatedBy
mimeType	MimeType
modifiedDate	UpdateDate
ownerNames	Author
originalFilename	contentStreamFileName
title	Name

This subset of fields supports SOQL and SOSL queries. (None are sortable, reflecting limitations in the Google Drive API.)

- CreationDate
- lastViewedByMeDate
- MimeType
- Name

  > Note: Google Drive queries on the Name field support only one wildcard, %. Searches using this wildcard match only name prefixes. For example, the title "HelloWorld" would be returned with the query *Name LIKE "Hello%"* but not *Name LIKE "%World"*.

- sharedWithMe

  > Note: Queries on the sharedWithMe field with a value of "false" are not supported, protecting confidential data.

- starred
- UpdateDate

Include SharePoint Custom Properties in Search, SOQL, and SOSL Queries

After you create an external object for a SharePoint data source, some special steps are needed to search or query any custom properties it contains.

Configuring Custom Properties in SharePoint

External objects in Salesforce let you select and filter on these custom properties from SharePoint:

- Custom columns defined in a Custom Content Type
- Metadata from Microsoft Word, Excel, and other Office documents

To search on these custom properties in Salesforce, a corresponding Managed Property must be created by a Sharepoint administrator.

- 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`.

Querying Resulting Fields in Salesforce

In the examples below, `CustomProperty` stands for the Custom column name defined in the Custom Content Type, or the Office document metadata name. `ManagedCustomProperty` stands for the corresponding Managed Property name.

SharePoint 2010

Use `CustomProperty` in the `SELECT` clause and `ManagedCustomProperty` in the `WHERE` clause. Two corresponding fields must exist for the external object in Salesforce: one for selecting, the other for filtering.

Here's a SOQL example:

```
SELECT CustomProperty FROM items_sp2010_x WHERE ManagedCustomProperty=...
```

SharePoint 2013 and Online

In most cases, `ManagedCustomProperty` can be used for both the `SELECT` and `WHERE` clause.

Here's a SOQL example:

```
SELECT ManagedCustomProperty FROM items_sp2013_x WHERE ManagedCustomProperty=...
```

However, for file types SharePoint doesn't index for search, such as .jpg, .png, and .pdf files, you must use `CustomProperty` in the `SELECT` clause and `ManagedCustomProperty` in the `WHERE` clause. As a workaround, you can define an alias on the Managed Property in SharePoint and format queries like this:

```
SELECT Alias FROM items_sp2013/Online WHERE Alias=...
```

> 💡 **Tip:** Normally, custom properties aren't displayed on external object detail pages—defining an alias also addresses this issue.

Boolean Custom Properties

When using boolean (Yes/No) custom properties with a corresponding Managed Property set to the Text type, the corresponding external object field must be set to the Text type as well. In filters, the values "0" and "1" equal false and true, respectively. For example:

```
WHERE customBooleanWithTextManagedProperty="1"
```

"0" and "1" are also displayed as results, however, so boolean custom properties should use a Managed Property type of YesNo. Set the corresponding external object field to Checkbox to query it with standard `true` or `false` values. For example:

```
WHERE customBooleanWithYesNoManagedProperty=true
```

Metadata in Microsoft Office Documents

The Sharepoint Search service returns all metadata from Office documents as strings, so corresponding external object fields must be set to the Text type.

Dates are returned in the format, MM/DD/YYYY hh:mm:ss AM/PM, (for example, "3/31/2015 9:59:00 PM"). To query on fields using the Date type, the external object must include a corresponding Date field for filtering, and a Text field for selecting.

Limitations for Specific SharePoint Property Types in Salesforce

All versions

- Number, Currency, and Choice multiple properties can't be selected for file types SharePoint doesn't index for search. By default, this includes image, video, and .pdf files, although .pdf files are natively indexed starting with SharePoint 2013.

SharePoint 2010

- Number, Choice multiple, and Currency properties can't be selected.
- Date properties can be selected but results are unlikely to be formatted in UTC (Coordinated Universal Time), so values may reflect a different time zone than expected.

SharePoint 2013

- Multiple Line of Text, URL, Date, and Choice Dropdown properties aren't queryable.
- Choice Dropdown, Choice multiple, URL, and Date properties can't be selected.

SharePoint Online

- Multiple Line of Text, URL, and Date properties aren't queryable.
- Choice multiple and URL properties can't be selected.

FILES CONNECT FOR USERS

Set Up Authentication to an External Data Source

When you connect to a Files Connect external data system for the first time, set up your authentication in just a few clicks.

If you haven't set up your authentication to an external data system in My Settings, you are prompted to authenticate the first time you try to access an external system in Salesforce. Click the link or button to complete most of the authentication automatically.

- If you are connecting to Box, Google Drive, SharePoint Online, or OneDrive for Business:

  1. Select **OAuth 2.0** as the authentication protocol.

  2. When you see a message requesting permission for Salesforce to access information from your external system, click **Allow**.

  3. After the authentication process has finished, you are redirected to Salesforce.

- If you are connecting to SharePoint 2010 or SharePoint 2013:

  1. You are redirected to Authentication Settings for External Systems.

  2. Enter your username and password credentials for the external system.

Manage Your External Data Source Authentication Credentials

You or your Salesforce admin can set up and manage your authentication settings for external data sources using Files Connect. With valid authentication settings, you can access files from external systems right from Salesforce.

Your admin defines external systems in external data sources and named credentials. Before you begin, your administrator:

- Sets up the external data source or named credential to use per-user authentication.
- Grants you access to the external data source or named credential.
- Tells you the authentication settings to enter.

If you don't see the expected settings or options, ask your admin for help.

1. From My Settings, enter `Authentication` in the `Quick Find` box, then select Authentication Settings for External Systems.

2. Click **New** to set up a new connection. Click **Edit** to modify an existing external data source.

3. From the `External System Definition` menu, select "External Data Source."

4. From the `External Data Source` menu, select a data source created by your administrator.

5. Select the authentication protocol required by the external system.

   For SharePoint 2010 or 2013, set the following options.

Field	Description
Authentication Protocol	Choose **Password Authentication**
Username **and** password	Enter your SharePoint username and password

   For Box, Google Drive, SharePoint Online, or OneDrive for Business, set the following options.

Field	Description
Authentication Protocol	Choose **OAuth 2.0**
Authentication Provider	Choose the provider created for this data source by your administrator
Scope	Leave blank
Start Authentication Flow on Save	Select to immediately verify your login credentials with the external data source.
	When you click **Save**, the external system prompts you to log in. After successful login, the external system grants you an OAuth token for accessing its data from this org.
	Redo the OAuth flow when you need a new token—for example, when the token expires—or if you edit the Scope or Authentication Provider fields.

6. Click **Save**.

Access and Share External Files Using Files Connect

After your admin enables Files Connect, you can access files from external sources like Google Drive and SharePoint, or share them via feeds and Files home.

Download or Share Files on Files Home

Download external files to your local system or share them with a general set of people in your organization from Files home.

1. Navigate to Files home.

2. The External Files list in the left column shows available external data sources. Select one and navigate through the folders, or use the search bar to find a file.

> 📝 Note: Salesforce supports Google documents, spreadsheets, presentations, and drawings. In the Recent list, Google Drive content is limited to the 24 most recently accessed documents from the last 30 days.

3. Click ▼ next to the file name, and choose one of the following:

- **Open** the file in the external data source, such as SharePoint.
- **Download** the file to your local system. (From on-premises systems like SharePoint 2010, 2 GB is the maximum download size.)
- **Share** the file either as a copy or as a reference. Your admin has determined which type of sharing is used at your organization. When sharing, you do one of the following:
  - **Share a copy** of the external file stored in Salesforce. If files are shared with a Chatter group, all group members can access the files, even if they lack access to the external system. Salesforce Files doesn't reflect any revisions to the file in external systems.
  - **Share a reference** to the external file stored outside Salesforce. Only users with access to the external system can download files. (Users must enter credentials for the system in the Authentication Settings for External Systems section of personal setup). Salesforce Files doesn't reflect any revisions to the file in external systems, but the reference does point to the latest version of the file in those systems.

EDITIONS

Available in: both Salesforce Classic and Lightning Experience

Files Connect for cloud-based external data sources is available in: **Professional**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

Files Connect for on-premises external data sources is available for an extra cost in: **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To access cloud-based data sources like SharePoint Online:
- "Files Connect Cloud"

To access on-premises data sources like SharePoint 2010:
- "Files Connect On-premises"

> 📝 Note: To download files referenced from an external system, users must enter credentials for the system in the Authentication Settings for External Systems section of personal setup.

When a user selects an external file from the file selector, a file reference or copy is created in Salesforce. If a file reference already exists, it is reused.

Share Files in the Feed

If you want to include external files in a specific Chatter conversation, use the feed. All files shared in the feed are either copies or references, as determined by your administrator.

In Salesforce Classic

1. While authoring a post, click **File** above the feed, and then click **Select a file from Salesforce**.

2. In the left column, click the external source, such as SharePoint.

3. Next to the file you want to share, click **Attach**.

4. In the body of your post, @mention the groups or people you want to share with.
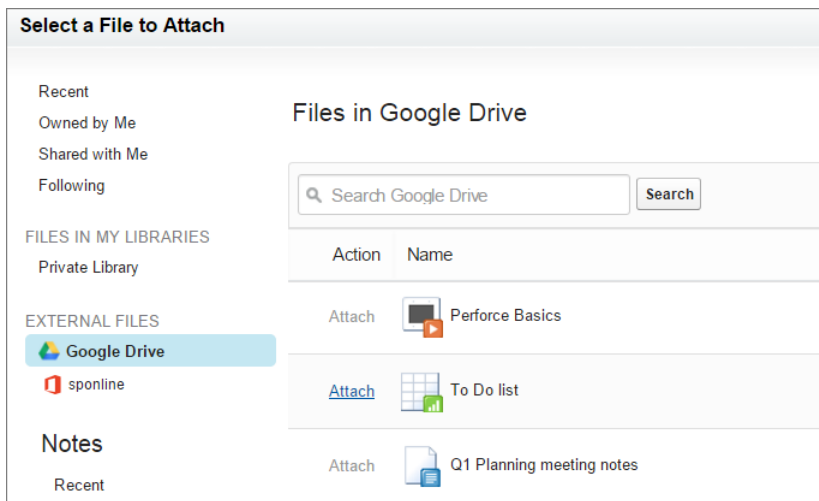
In Lightning Experience

1. While authoring a post, click the paperclip icon below the post to open the Select File window.

2. From the left column, click the external source, such as SharePoint or Google Drive.

3. Select the file you want to share and click **Add**.

4. In the body of your post, @mention groups or people that you want to share with.
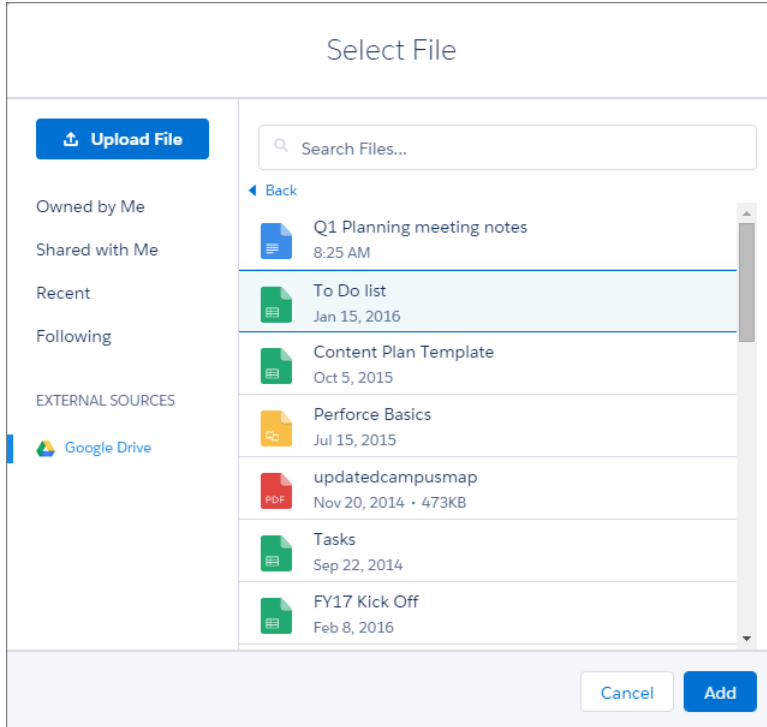
When you paste a link to an external document into a Chatter post, it's converted into a Files Connect file reference. Under the body of your post, the file title and icon appear. Click the icon to open the file preview right from your feed. A file reference is created for the first link in each post. File references are not created for links in comments.
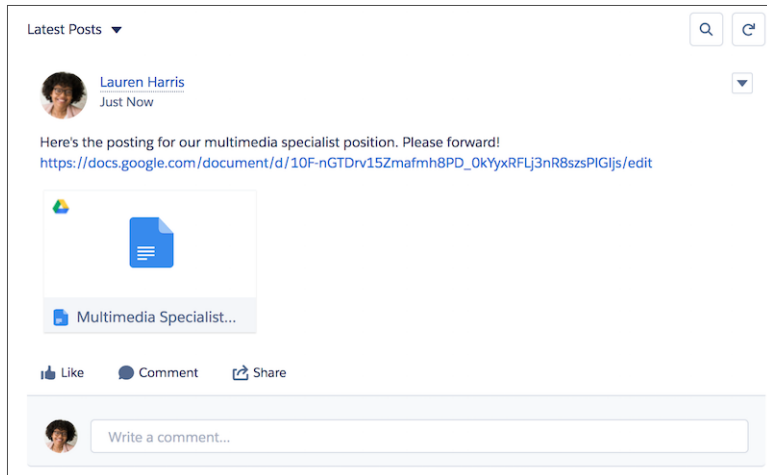
Search for External Files with Files Connect

Search an external data source like Google Drive, Box, or SharePoint right within Salesforce.

Search in a Specific External Data Source

In Salesforce Classic

1. From the left column of Files home or your Chatter feed, click the data source name.

2. In the search box, enter terms such as *document title* or *author*. (The specific information you can search for depends on the configuration of the external data source.)

Files in Sharepoint Online

🔍 Search Sharepoint Online   **Search**

> 📝 **Note:** You can also search external data sources from the file selector when attaching a file to a Chatter post. In Salesforce Classic, click **File** above the feed, and then select a file from Salesforce. In Lightning Experience, click the paperclip icon below the post to open the Select File window.

Search Globally for Salesforce and External Data

If your administrator enables global search for an external data source, you can conveniently search its contents along with your Salesforce data.

In Salesforce Classic

1. In the global search box at the top of the Salesforce window, enter your search terms.

2. To filter the results down to a specific external data source, click its name in the left column (for example, "SharePoint Online").

Search Results

🔵 Search Feeds	pacifica	**Search Sharepoint Online**
📁 Records	**📁 Sharepoint Online (1)**	
People (0)	Actions Name	
Sharepoint Online (1)	▾ 📄 Pacifica Overview	
Search All		

> 💡 **Tip:** If you often want to see content from a specific external data source, pin it to the top of global search results: In the left column, hover over the data source name, and click the pin icon. (If you don't see the data source listed, click Search All.)

In Lightning Experience

1. From Files home, enter a search term into the global search box in the header.

2. You can filter your search results to return only Files by selecting "in Files" after entering your search in the global search box, or by doing a global search and then selecting Files from the global search results.