Coveo Platform 7.0

Google Drive for Work Connector Guide

Notice

The content in this document represents the current view of Coveo as of the date of publication. Because Coveo continually responds to changing market conditions, information in this document is subject to change without notice. For the latest documentation, visit our website at www.coveo.com.

Document part number: PM-131111-EN

Publication date: 1/3/2019

Table of Contents

1. Google Drive for Work Connector

CES 7.0.5989+ (October 2013)

The Coveo beta connector for Google Drive for Work allows Coveo administrators to index and integrate the Google Drive content into the Coveo unified index. The connector indexes all items and the attached permissions from all Google Drive domain users so that in the Coveo search interfaces, a user can easily find any but only content to which he has access in Google Drive.

1.1 Connector Features Summary

Features		Supported	Additional information
Google Drive for Work version		Latest cloud version	Following available Google Drive for Work releases
Searchable content types[1]		✓	Files, folders, comments and replies[2], and user profiles
Content update	Incremental refresh	✓	
	Full refresh	✓	
	Rebuild	✓	
Document-level security		✓	

*1- By default the Drive for Work source includes files of the **My Drive** folder for each user. Shared documents are included with the associated permissions, so that who ever is authorized to see the items can find them in Coveo search results.*

2- The comments and replies are included in the `coveo.comments` and `coveo.comments.authors` metadata of their parent item rather than as separate items. This way, users can search for the content of a comment or reply and find the parent document.

1.2 Features

The Google Drive for Work connector features are:

Content indexing

Extraction and indexing of all Google Drive object types:

- User profile
- Folders

- Files
- Comments and replies

  Note: CES 7.0.6830+ (July 2014) The comments and replies are indexed in the `coveo.comments` and `coveo.comments.authors` metadata of their parent document rather than as separate documents. This way, users can search for the content of a comment or reply and find the parent document.

Note: By default the Google Drive for Work connector indexes the content of the **My Drive** and **Shared with me** folders for each user. To minimize reindexing several times the same documents, all other documents shared more globally are indexed only from the owner's folder, but with the associated permissions, so that who ever is authorized to see the document can find it in Coveo search results.

Fully supported security model

The connector fully supports the Google Drive security model using a security provider to get permissions for each indexed item. This means that, in Coveo search interfaces, a user searching Google Drive content only sees the content to which he has access.

Incremental refresh

Supports incremental refresh to periodically query Google Drive for the latest edits, keeping the index content up-to-date.

Out-of-the-box configuration

The connector is ready to use with minimal configuration to indicate which items to index and which metadata to use.

Multithreading

The connector can run multiple threads, which can improve performances considerably (see Modifying Hidden Google Drive for Work Source Parameters).

Feature History

CES version	Monthly release	Features
7.0.7022+	September 2014	Supports refreshing or deleting from the index a specific folder or document
7.0.6767	June 2014	Populates `systo` and `sysfrom` fields allowing to create **Shared To** and **Shared From** facets.
7.0.6684	May 2014	Significant crawling performance improvement and additional source options [more]
7.0.5556+	June 2013	Beta version introduction

What's Next?

Review the steps to deploy the Google Drive for Work connector (see "Google Drive for Work Connector Deployment Overview" on page 4).

2. Google Drive for Work Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Google Drive for Work connector. The steps indicate the order in which you must perform configuration tasks on both the Google and Coveo servers.

To deploy the Google Drive for Work connector

1. Validate that your environment meets the requirements (see "Google Drive for Work Connector Requirements" on page 6).
2. On the Google server:
    a. Create a Google API Console project to authorize the Coveo connector to access the Google Drive of your users (see "Authorizing the Coveo Connector to Access Your Google Drive" on page 7).

    b. Modify security parameters in your Google Apps account to grant the connector access to your Google Apps for Work (see "Authorizing the Coveo Connector to Access Your Google Apps for Work" on page 10).
3. On the Coveo server, in the Coveo Administration Tool:
    a. Set up the crawling account

    The Coveo connector needs an account that can list the various drives and users of the domain. This is typically the administrator of the Google Apps domain. There are two methods available to get the permissions from the crawling account depending on your CES version:

    - CES 7.0.7433+ (February 2015) The method, that only requires your admin account email, uses the service account email and its PCKS12 private key file, both obtained in step 2a, to impersonate the admin account without having to create a user identity.
    - CES 7.0.7338– (January 2015) Create a CES user identity that contains the credentials (username and password) of your domain administrator (see "Adding a User Identity" on page 13).

    b. Optionally create security providers

    When you want to index Google Drive permissions, you must create two security providers to get Google Apps for Work item permissions and resolve and expand groups.

    In Google Drive, users are identified by their email addresses. Consequently, permissions returned by the Google Apps for Work security provider for each document are email addresses. The Google Apps for Work security provider then requires another security provider to uniquely identify users from their email addresses.

    i. Start by selecting or creating an Email or an Active Directory security provider that the Google Apps for Work security provider will use to resolve and expand groups. The security provider type to use depends on how users are authenticated when they access the search interface:

    - When authenticated with their email address, use an Email security provider (see "Configuring an Email Security Provider" on page 18).

- When authenticated with an Active Directory account, use an Active Directory security provider (see "Configuring an Active Directory Security Provider" on page 20).

  Notes:

  - CES comes with an Active Directory security provider that you can configure to connect to the default domain. When your environment contains more than one domain, you can select an Active Directory security provider that you created for other domains.
  - An Active Directory security provider is appropriate only when the User Principal Name (UPN) matches the email address for all users.

Note: You may require to also use a REGEX Transform Member Name security provider in between the two other security providers to map member types. Contact Coveo Support for assistance.

ii. Then create a Google Apps for Work security provider that the connector uses to resolve indexed permissions (see "Configuring a Google Drive for Work Security Provider" on page 15).

c. CES 7.0.6607+ (April 2014) Create a Google Drive field set to take advantage of the available Google Drive metadata.

i. It is recommended to start by importing the default Google Drive field set file (`[CES_Path]\Bin\Coveo.CES.CustomCrawlers.GoogleDrive.FieldSet.xml`) to create fields for all the metadata available by default from Google Drive documents.

ii. When you created custom metadata for your Google Drive documents, add corresponding fields to the field set.

d. Configure and index a Google Drive for Work source.

The connector must know details about the authorized access to the Google Drive of your users to index its content (see "Configuring and Indexing a Google Drive for Work Source" on page 23).

e. If you encounter issues, verify if modifying the default value of hidden source parameters can help resolve the problems (see "Modifying Hidden Google Drive for Work Source Parameters" on page 29).

3. Google Drive for Work Connector Requirements

Your environment must meet the following requirements to be able to use the Google Drive for Work connector:

- CES 7.0.5989+ (October 2013)
- Coveo license for the Google Drive (Google Apps for Work) connector

  Your Coveo license must include support for the Google Drive for Work connector to be able to use this connector.
- A valid Google Account

  Using a Google Account with administrator privilege, you must log in the Google API Console to authorize Coveo to access the Google Drive of your users (see Authorizing the Coveo Connector to Access Your Google Drive).
- Administrator credentials to your Google Apps account

  You must log in to your Google Apps account to modify security options and authorize Coveo to access your Google Apps for Work (see Authorizing the Coveo Connector to Access Your Google Apps for Work).
- Google Drive storage licenses for your Google Apps users

  In your Google Apps account, you must activate the Google Drive service (see Authorizing the Coveo Connector to Access Your Google Apps for Work).
- Coveo Master server free disk space for temporary files

  Before indexing your Google Drive, ensure that your Coveo Master server has sufficient free hard disk space to temporarily store indexed Google Drive content.

  Starting with the CES 7.0.6547 March 2014 monthly release, the Google Drive connector creates a BLOB store on the Coveo Master server (`[CES_Path]\Index\Crawlers\BlobStore` or `[CES_Path]\Index\Crawlers\BlobStore32`) where shared downloaded documents with sizes greater than 100 KB are temporarily saved. This mechanism prevents downloading and re-indexing all copies of shared documents and allows to index metadata associated with each shared document copy.

What's Next?

Grant Coveo access to the Google Drive of your users by creating a Google API Console project and modifying security options in your Google Apps account (see "Authorizing the Coveo Connector to Access Your Google Drive" on page 7).

4. Setting Google Permissions (Google for Work)

Before you start configuring the Coveo connector for Google Drive (Google for Work), you must first set appropriate Google permissions.

Refer to the following topics to perform the necessary Google security configuration:

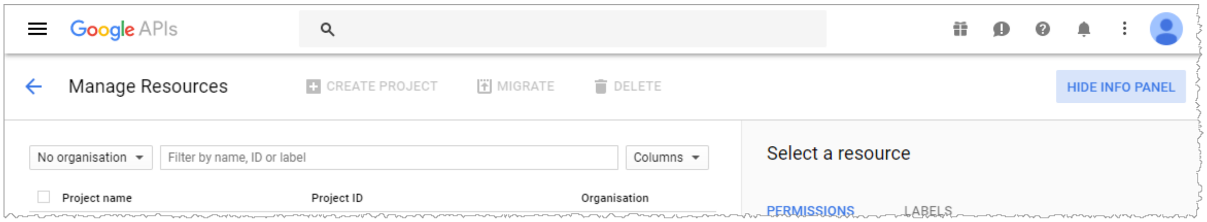
1. "Authorizing the Coveo Connector to Access Your Google Drive" on page 7
2. "Authorizing the Coveo Connector to Access Your Google Apps for Work" on page 10

4.1 Authorizing the Coveo Connector to Access Your Google Drive

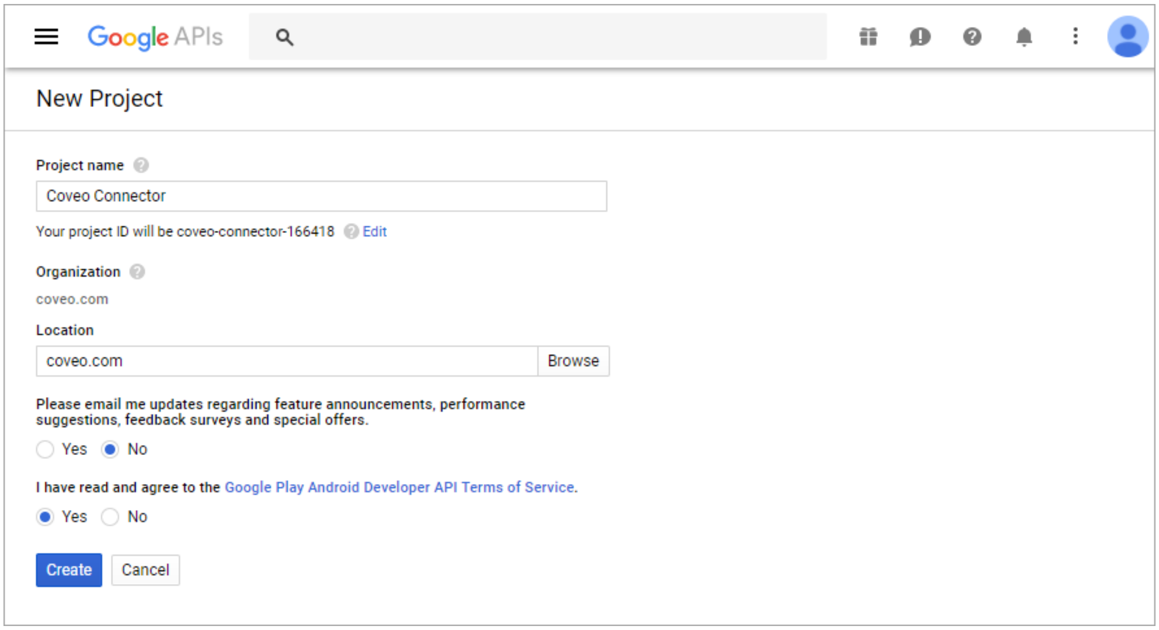
You must perform a G Suite domain-wide delegation of authority to authorize the Coveo connector to access the Google Drive content that you want to index.

To authorize the connector to access the Google Drive of your users

1. Go to the Google Developers Console, and log in using a Google Account with administrator credentials.



2. At the left of the **Filter by name, ID or label** input, click the drop-down menu, and then select the organization in which you want to create the Google Developer Console project.
3. Create an API project for the Coveo connector (CES 7) or source (Coveo Cloud):
   a. In the **Manage resources** panel, click **Create a project**.
   b. (When your project limit is exceeded) In the **Increase Project Limit** page, click **Request increase**, and then complete the form.
   c. In the **New Project** dialog page, enter the project required information:



New Project

Project name: Coveo Connector

Your project ID will be coveo-connector-166418 Edit

Organization: coveo.com

Location: coveo.com Browse

Please email me updates regarding feature announcements, performance suggestions, feedback surveys and special offers.

○ Yes ● No

I have read and agree to the Google Play Android Developer API Terms of Service.

● Yes ○ No

i. Enter a **Project name**.

> **Note:** The project ID is automatically created based on the project name. You can always modify the project ID by clicking **Edit**.

ii. (When you create the first project in your organization only) Answer the **Please email me updates regarding feature announcements, performance suggestions, feedback surveys and special offers.** question using the **Yes** or **No** checkbox.

iii. (When you create the first project in your organization only) After you **have read and agree to the Google Play Android Developer API Terms of Service**, click the **Yes** check box.

iv. Click **Create**.

4. Enable the required Google APIs:

   a. Access the API **Library** page by clicking **Google APIs** in the top menu.

   b. In the API **Library** page, enable the **Gmail API** and **Admin SDK** APIs:

      i. Under **Google APIs**, use the search box to search and select **Google Drive API** or **Admin SDK**.

      ii. In the **Google Drive API** or **Admin SDK** page, in the action bar, click **Enable**.

      iii. In the action bar, click the back button (←).

      iv. Repeat the procedure for the other API.

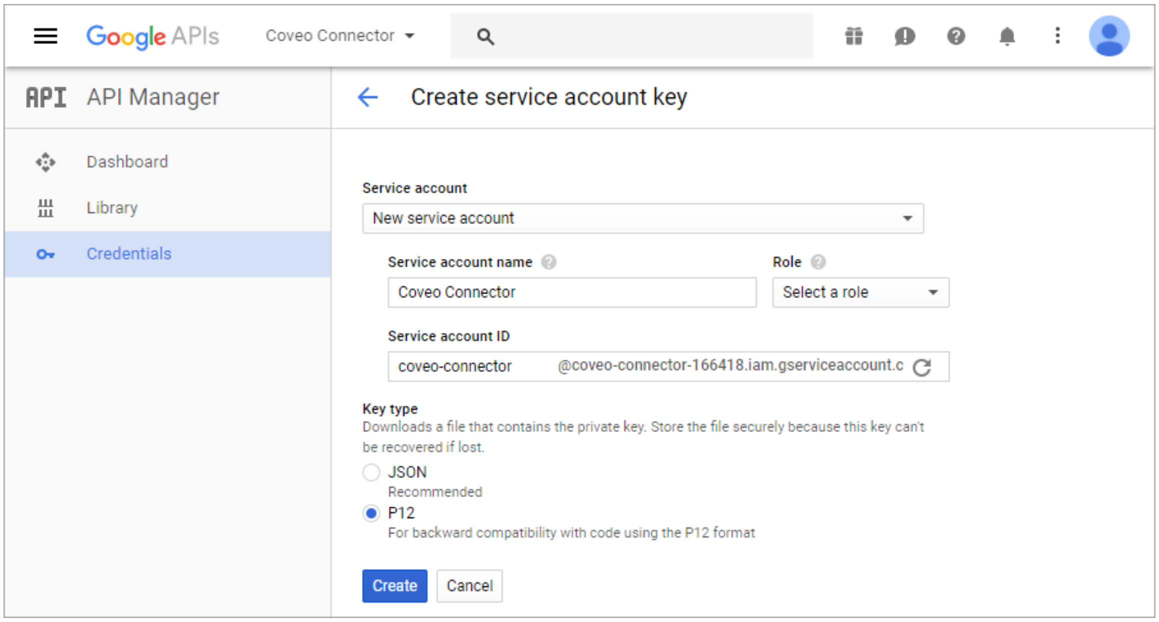
5. Create a service account project for the Coveo connector (CES 7) or source (Coveo Cloud).

   a. In the sidebar on the left, select **Credentials**.

   b. In the **Credentials** page, click the **Create credentials** drop-down list menu, and then select **Service**

account key.

c. In the **Create service account key** page:



Create service account key

Service account: New service account

Service account name: Coveo Connector

Role: Select a role

Service account ID: coveo-connector @coveo-connector-166418.iam.gserviceaccount.c

Key type

Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

○ JSON
Recommended

● P12
For backward compatibility with code using the P12 format

Create | Cancel

i. Click the **Service account** drop-down list menu, and then select **New service account**.

ii. Click the **Role** drop-down list menu, and then select **Service account** > **Service account admin**.

iii. In the first box, enter a **Service account name**.

> **Example:** `Coveo Connector`

iv. (Optionally) Edit the **Service account ID** or generate another one by clicking the refresh icon ↻.

> **Note:** The service account ID is automatically created based on the service account name.

v. Under **Key type**, select **P12**.

vi. Click **Create**.

> **Note:** A private key is automatically downloaded as a Personal Information Exchange (`.p12`) file in your browser download folder.

vii. In the **New private key** dialog box that appears, take note of the private key password, and then click **Close**.

6. (For CES 7 customers only) Using an administrator account, connect to your Coveo Master server, and then copy the downloaded private key `[GUID]-privatekey.p12` file to a folder accessible to Coveo Enterprise Search, typically in the [Index_Path]`\Config` folder.

7. Back in the **Credentials** page, perform a G Suite domain-wide delegation.

a. At the top right of the **Service account keys** table, click **Manage service accounts**.

b. At the right end of your service account row, click the more icon (⋮), and then select **Edit**.

c. In the **Edit service account** dialog that appears:

i. Click the **Enable G Suite Domain-wide Delegation** check box

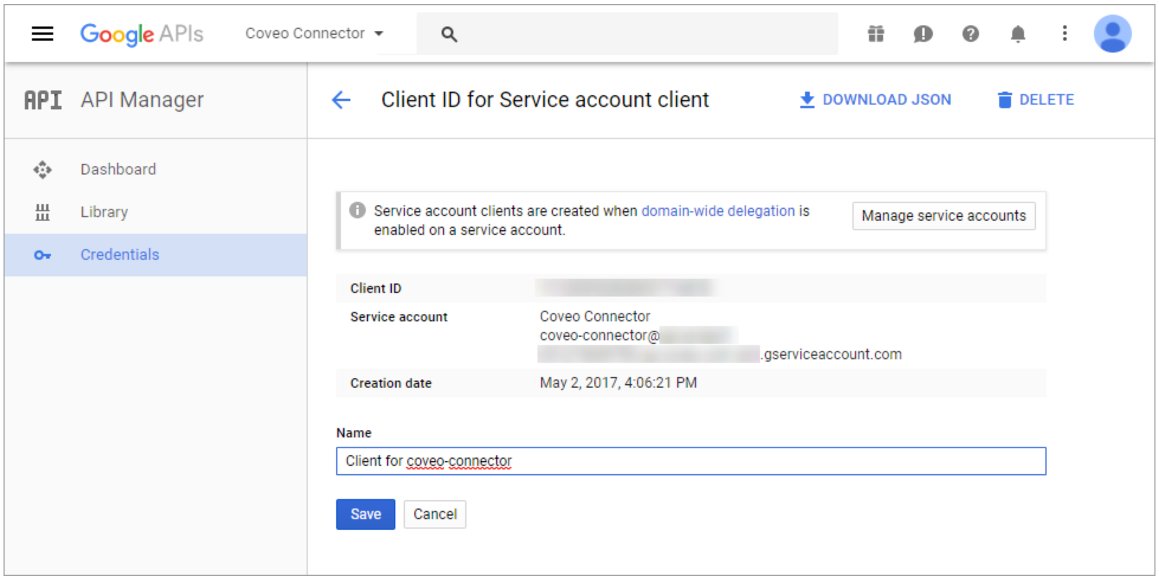
ii. In the **Product name for the consent screen** box, enter the product name (e.g., `Coveo Connector`) that will appear when the application requests read access to the users' data.

iii. Click **Save**.

8. Back in the **Service Accounts** page, on the service account row you just created, in the **Options** column of your service account row, click **View Client ID**.

9. In the **Client ID Service account client** page, then take note of the following information that you will need later to configure your Google Drive for Work source:

- **Client ID**
- **Email address** (under the **Service account** name)



Client ID for Service account client

Service account clients are created when domain-wide delegation is enabled on a service account.

Client ID	[redacted]
Service account	Coveo Connector coveo-connector@[redacted] [redacted].gserviceaccount.com
Creation date	May 2, 2017, 4:06:21 PM

Name

Client for coveo-connector

What's Next?

You must modify security parameters in your Google Apps account to grant the connector access to your Google Apps for Work (see "Authorizing the Coveo Connector to Access Your Google Apps for Work" on page 10).

4.2 Authorizing the Coveo Connector to Access Your Google Apps for Work

You must perform a Google Suite domain-wide delegation of authority to authorize the Coveo connector (CES 7) or source (Coveo Cloud) to access your Google Apps for Work.

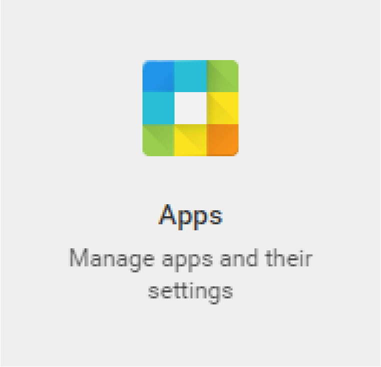
To authorize the connector to access your Google Apps for Work

1. Go to your Google Apps for Work domain Admin console:

   a. Access the User hub with an administrator account.

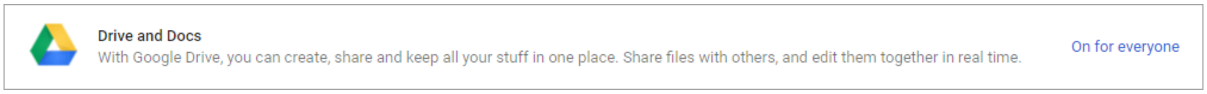
   b. In the hub, click **Admin Console**.

2. In the Google **Admin Console**, click **Apps**.



3. In the **Apps** page, select **Google Suite**.

4. In the **Google Apps** page, ensure that for **Drive and Docs**, the **Status** is set to **On for everyone**.



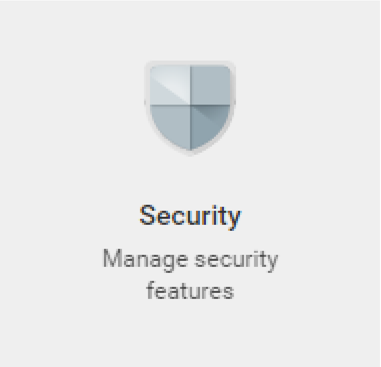
Drive and Docs
With Google Drive, you can create, share and keep all your stuff in one place. Share files with others, and edit them together in real time.

On for everyone

5. Grant access to users data for the Google API console project:

   a. Access the Admin console by clicking **Google Admin** in the top menu.

   b. In the **Admin console**, click **Security**.



   c. In the **Security** page, click **Show more**, and then select **Advanced Settings** > **Manage API client access**.

   d. In the **Manage API client access** page:

i. In the **Client Name** box, enter the previously obtained **Client ID** from the Google Console (see Authorizing the Coveo Connector to Access Your Google Drive).

ii. In the **One or More API Scopes** box, enter the following list of values, separating each with a comma:

> **Note:** When you use the same Google Developer Console project as another Coveo connector (i.e., Gmail for Work), you must reenter its scope here (`https://www.googleapis.com/auth/gmail.readonly`). If not, adding the following scopes will remove the ones that were already added for this Client ID.

- `https://docs.google.com/feeds/`
- `https://www.googleapis.com/auth/drive.readonly`
- `https://www.googleapis.com/auth/userinfo.email`
- `https://www.googleapis.com/auth/admin.directory.user.readonly`
- `https://www.googleapis.com/auth/admin.directory.group.readonly`

iii. Click **Authorize**.

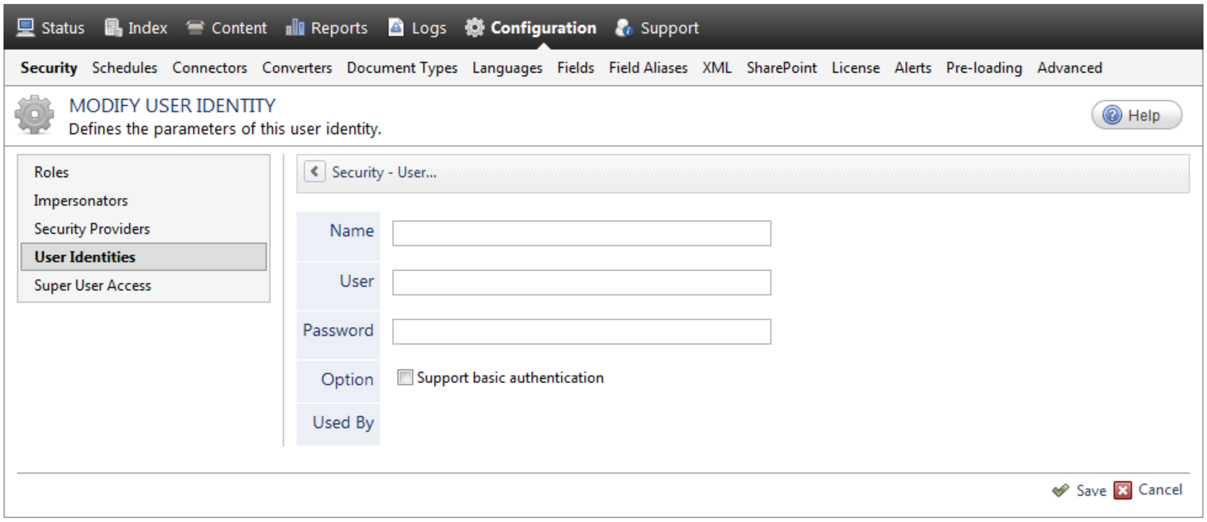
5. Adding a User Identity

A user identity is a set of credentials for a given repository or system that you enter once in CES and can then associate with one or more sources or security providers.

A user identity typically holds the credentials of an account that has read access to all the repository items that you want to index. It is a best practice to create an account to be used exclusively by the Coveo processes and for which the password does not change. If the password of this account changes in the repository, you must also change it in the CES user identity.

To add a user identity

1. On the Coveo server, access the Administration Tool.
2. In the Administration Tool, select **Configuration** > **Security**.
3. In the navigation panel on the left, click **User Identities**.
4. In the **User Identities** page, click **Add**.
5. In the **Modify User Identity** page:



MODIFY USER IDENTITY

Defines the parameters of this user identity.

Name

User

Password

Option □ Support basic authentication

Used By

   a. In the **Name** box, enter a name of your choice to describe the account that you selected or created in the repository to allow CES to access the repository.

   > **Note:** This name appears only in the Coveo Administration Tool, in the **Authentication** or **User Identity** drop-down lists, when you respectively define a source or a security provider.

   b. In the **User** box, enter the username for the account that you selected or created to crawl the repository content that you want to index.

   c. In the **Password** box, enter the password for the account.

   d. In the **Options** section, the **Support basic authentication** check box is deprecated and not applicable for most types of repositories. You should select it only when you need to allow CES to send the username and password as unencrypted text.

e. Click **Save**.

> **Important:** When you use Firefox to access the Administration Tool and it proposes to remember the password for the user identity that you just created, select to never remember the password for this site to prevent issues with automatic filling of username and password fields within the Coveo Administration Tool.

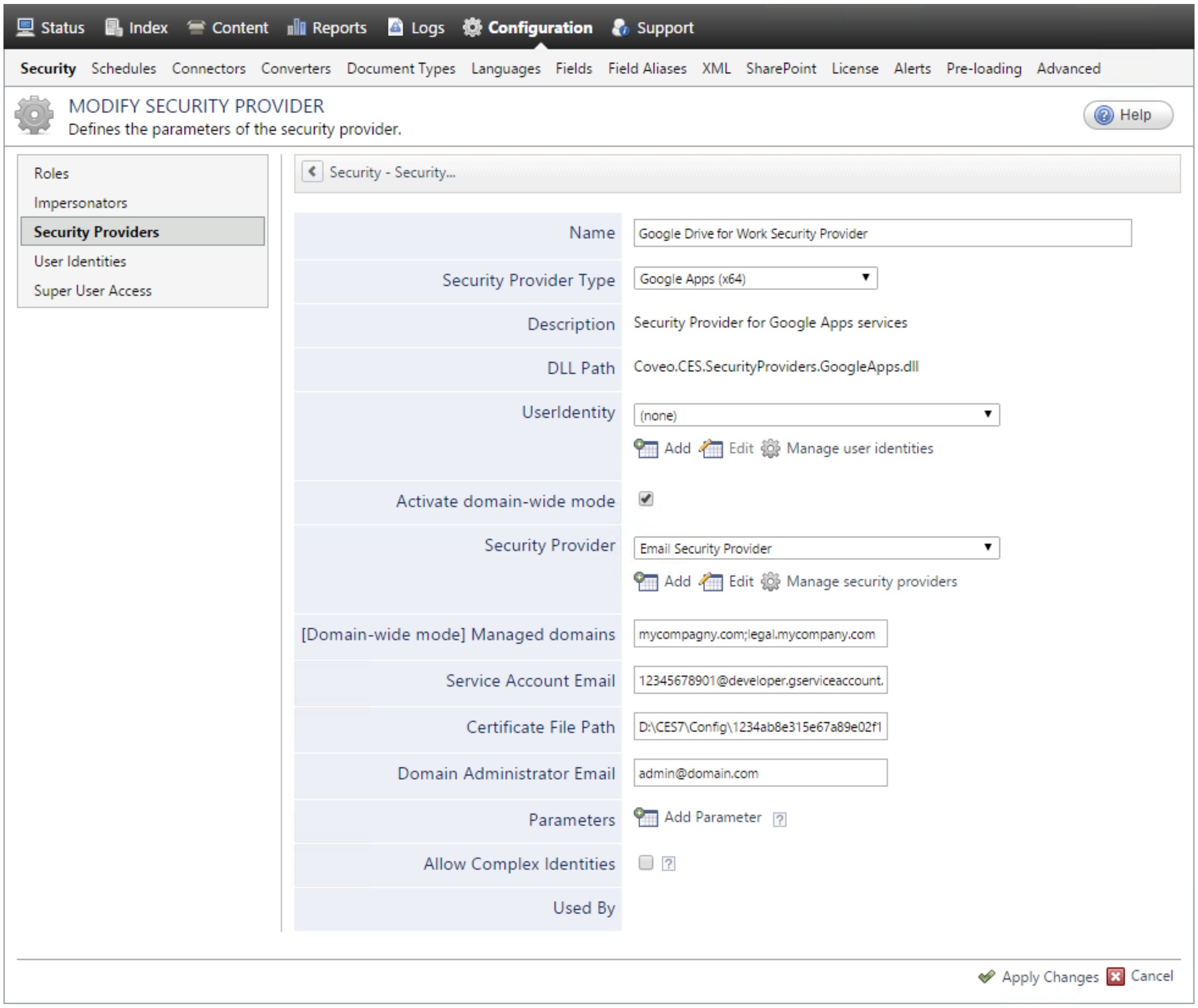
6. Configuring a Google Drive for Work Security Provider

The Coveo Google Drive for Work connector fully supports the Google security model. When you want users searching for Google Drive content in a Coveo search interface to only see the content to which they have access in Google Drive, the connector needs a security provider to be able to index the permissions for each indexed Google Drive item.

Note: You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure a Google Drive for Work security provider

1. On the Coveo server, access the Administration Tool.
2. Select **Configuration** > **Security**.
3. In the navigation panel on the left, click **Security Providers**.
4. In the **Security Providers** page, click **Add** to create a new security provider.
5. In the **Modify Security Provider** page:



MODIFY SECURITY PROVIDER

Defines the parameters of the security provider.

Name	Google Drive for Work Security Provider
Security Provider Type	Google Apps (x64) ▾
Description	Security Provider for Google Apps services
DLL Path	Coveo.CES.SecurityProviders.GoogleApps.dll
UserIdentity	(none) ▾ Add Edit Manage user identities
Activate domain-wide mode	☑
Security Provider	Email Security Provider ▾ Add Edit Manage security providers
[Domain-wide mode] Managed domains	mycompagny.com;legal.mycompany.com
Service Account Email	12345678901@developer.gserviceaccount.
Certificate File Path	D:\CES7\Config\1234ab8e315e67a89e02f1
Domain Administrator Email	admin@domain.com
Parameters	Add Parameter ?
Allow Complex Identities	□ ?
Used By	

a. Configure the following required parameters:

Name

Choose a meaningful name to identify the security provider.

Example: `Google Drive for Work Security Provider`

Security Provider Type

In the drop-down list, select **Google Apps (x64)**.

User Identity

In the drop-down list:

- CES 7.0.7433+ (February 2015) Select **(none)**.
- CES 7.0.7338– (January 2015) Select the user identity that you selected or created previously (see Google Drive for Work Connector Deployment Overview).

Activate domain-wide mode

You must select this option when you plan to use this security provider with a **Google Drive (Google Apps)** source type.

Security Provider

Select the security provider that you selected or created to allow this security provider to resolve and expand the groups (see Google Drive for Work Connector Deployment Overview).

[Domain-wide mode] Managed domains

Enter the domain that you want to index. When your Google Apps account contains more than one domain, you can enter a semicolon-separated list of domains to index. The security provider will resolve and expand groups for the specified domain(s).

Examples:

- One domain: `mysubdomain.mycompany.com`
- Multiple domains: `myfirstdomain.com;myseconddomain.com`

Important: The domain(s) specified in this list must match the one(s) specified in the source **Domain (s)** list (see Configuring and Indexing a Google Drive for Work Source).

b. CES 7.0.7433+ (February 2015) Configure the following required parameters:

Service Account Email Source

Enter the service account **Email address** previously obtained (see Authorizing the Coveo Connector to Access Your Google Drive).

Example: `12345678901@developer.gserviceaccount.com`

Certificate File Path Source

Note: CES 7.0.7599+ (April 2015) This parameter is no longer required and can be left empty when you use the `CertificateFileData` hidden parameter (see CertificateFileData).

Enter the path on the Coveo Master server where you saved the previously obtained service account's PCKS12 private key file (see Authorizing the Coveo Connector to Access Your Google Drive).

Example: `D:\CES7\Config\1234ab8e315e67a89e02f16ea38bd44d609471ff-privatekey.p12`

Domain Administrator Email Source

Enter the domain admin account email used to obtain the list of users in the domain.

Example: `admin@domain.com`

c. CES 7.0.7599+ (April 2015) (Optional) Click **Add Parameter** and then use the following hidden parameter when you let the **Certificate File Path** parameter box empty:

CertificateFileData

The service account's PKCS12 private key file data encoded in Base64. The default value is `null`.

> **Notes:**
>
> - You need to open the certificate in a text editor and use an encoding application such as Motobit to convert the certificate content to the Base64 format.
> - This parameter is only used when the Certificate File Path parameter box is empty (see Certificate File Path).

d. Leave the **Allow Complex Identities** cleared as it does not apply to this type of security provider.

e. Click **Apply Changes**.

What's Next?

Create and index a source (see "Configuring and Indexing a Google Drive for Work Source" on page 23).

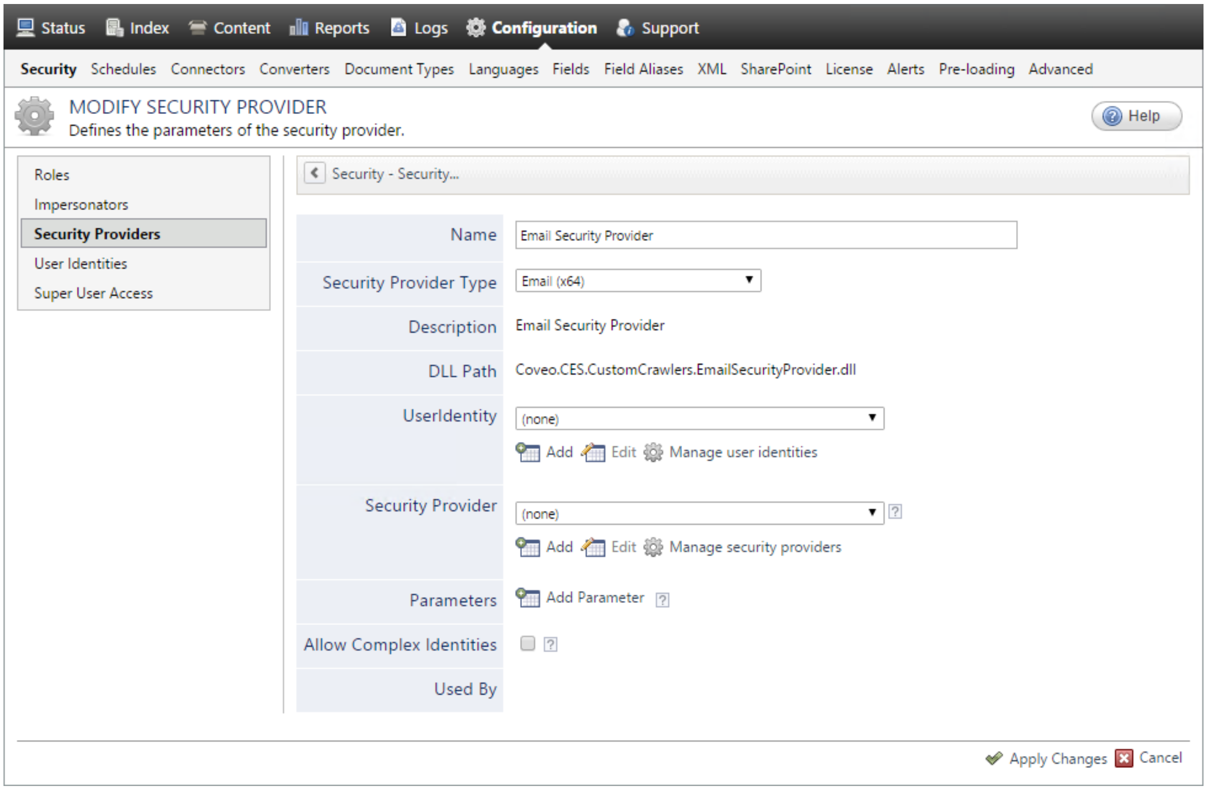
6.1 Configuring an Email Security Provider

An Email security provider is a simple email user identity container that can be used by another security provider to recognize users by their email addresses. When used by more than one security providers attached to sources of various types, an email security provider can act as a single sign-on system. An Email security provider does not connect to any system so it does not need a user identity.

> **Note:** You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To configure an Email security provider

1. On the Coveo server, access the Administration Tool.
2. On the menu, select **Configuration** > **Security**.
3. In the navigation panel on the left, select **Security Providers**.
4. In the **Security - Security Providers** page, click **Add**.
5. In the **Modify Security Provider** page:



MODIFY SECURITY PROVIDER

Defines the parameters of the security provider.

Name	Email Security Provider
Security Provider Type	Email (x64)
Description	Email Security Provider
DLL Path	Coveo.CES.CustomCrawlers.EmailSecurityProvider.dll
UserIdentity	(none)
Security Provider	(none)
Parameters	
Allow Complex Identities	□
Used By	

a. In the **Name** box, enter a name of your choice for your Email security provider.

b. In the **Security Provider Type** list, select **Email**.

> **Note:** CES 7.0.5785 to 7.0.5935 (August to September 2013) The Email security provider DLL file is missing in the CES distribution so you will not see the **Email** option in the **Security Provider Type** list.
>
> To resolve this issue:
>
> i. Contact Coveo Support to get a copy of the `Coveo.CES.CustomCrawlers.EmailSecurityProvider.dll` file.
>
> ii. When you receive the file, using an administrator account, connect to the Coveo Master server, and then copy the file to the `[CES_Path]\bin` folder.
>
> iii. When your Coveo instance includes a Mirror server, also copy the file to the `[CES_Path]\bin` folder on the Coveo Mirror server.
>
> iv. Restart the CES service so that the new DLL is recognized.

c. In the **User Identity** list, leave **(none)**.

d. CES 7.0.7814+ (August 2015) (Optional) In the **Security Provider** list, select another security provider to map Email identities to another identity type.

> **Example:** You want to map Email identities to Active Directory (AD) ones so you select an LDAP Lookup security provider that is chained to an AD security provider. The LDAP Lookup security provider is then able to find a user in AD from his email and extracts his User Principal Name (UPN), thus allowing a mapping of the Email identity to an AD one. Contact Coveo Support for assistance on how to create an LDAP Lookup security provider.

e. Leave the **Allow Complex Identities** option cleared as it does not apply to this type of security provider.

f. Click **Apply Changes**.

What's Next?

Configure a security provider that will use this Email security provider.

6.2 Configuring an Active Directory Security Provider

You must use an Active Directory (AD) security provider when you create a source to index the content of an Active Directory domain. Other security providers may need to use an Active Directory security provider to expand, map, or resolve users or groups defined in Active Directory.

Coveo Enterprise Search (CES) comes with a default **Active Directory** security provider to which no user identity is assigned. In this case, the **Active Directory** security provider takes the CES service account as the user to access AD. When CES is in the same domain as AD, you can use the default **Active Directory** security provider as is. No configuration is needed.

You may need to create another Active Directory security provider only when CES and AD are in different and untrusted domains. In this case, you only need to assign a user identity containing any user that has access to the other domain to be able to use the security provider to expand, map, or resolve users or groups defined in Active Directory of this domain.

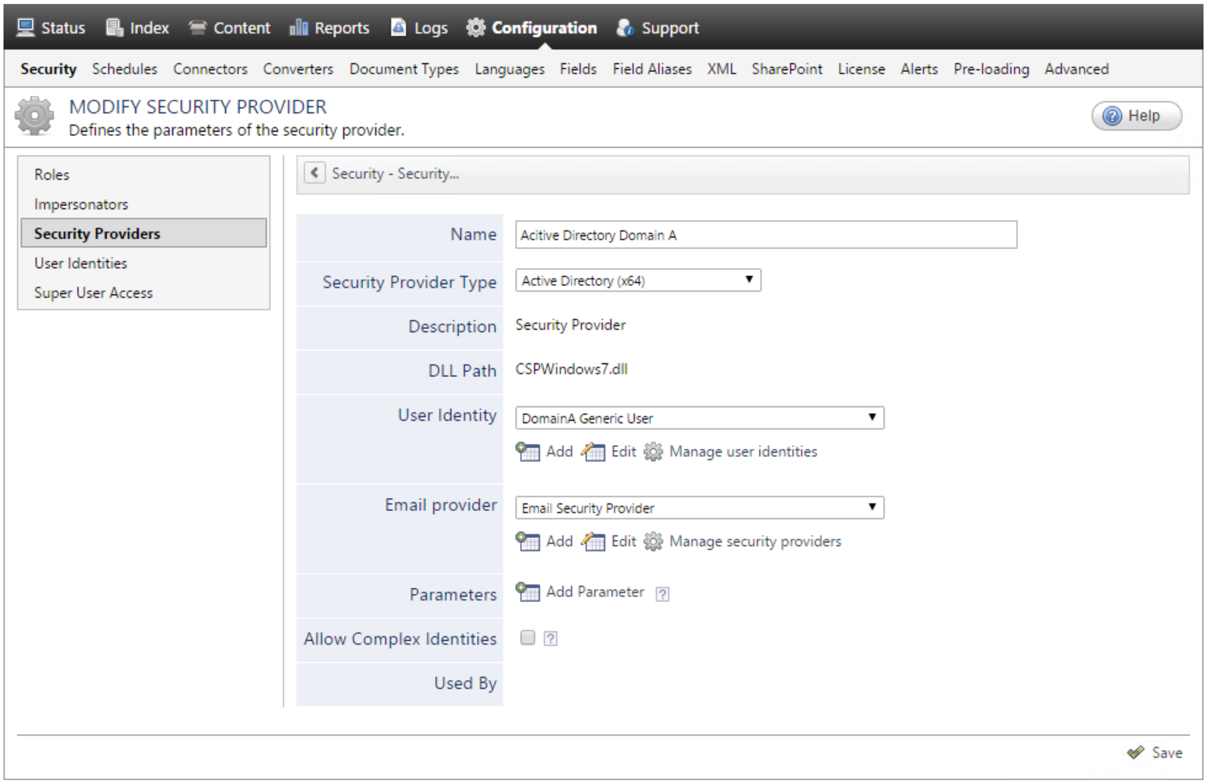
> **Note:** You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

To create or modify an Active Directory security provider

1. On the Coveo server, access the Administration Tool.
2. Select **Configuration** > **Security**.
3. In the navigation panel on the left, select **Security Providers**.
4. In the **Security Providers** page:
    - Click **Add** to create a new security provider.

      OR

    - Click an existing Active Directory security provider to modify it.
5. In the **Modify Security Provider** page:



MODIFY SECURITY PROVIDER

Defines the parameters of the security provider.

Name	Active Directory Domain A
Security Provider Type	Active Directory (x64)
Description	Security Provider
DLL Path	CSPWindows7.dll
User Identity	DomainA Generic User
Email provider	Email Security Provider
Parameters	
Allow Complex Identities	☐
Used By	

a. In the **Name** box, enter a name to identify this security provider.

b. In the **Security Provider Type** drop-down list:

   i. On a 32-bit server, select **Active Directory (x86)**.

   ii. On a 64-bit server, select **Active Directory (x64)**.

c. In the **User Identity** section:

   i. In the drop-down list, select a user identity containing an account that has access to the desired domain.

   > **Example:** When the user identity contains the `domainA\OneUsername` account, the security provider connects to *Domain A* Active Directory.

   > **Note:** When **User Identity** is set to **(none)**, the security provider takes the CES service account by default.

   ii. When needed, click **Add**, **Edit**, or **Manage user identities** respectively to create, modify, or manage user identities.

d. CES 7.0.7338+ (January 2015) In the **Email Provider** section:

i. In the drop-down list, select the email provider that recognizes your users by their email addresses.

> **Note:** When you do not want to map Active Directory (AD) users to their email, select **(none)**.

ii. When needed, click **Add**, **Edit**, or **Manage security providers** respectively to create, modify, or manage email security providers.

e. In the **Parameters** section, in rare cases the Coveo Support could instruct you to click **Add Parameters** to specify other security provider parameter names and values that could help to troubleshoot security provider issues.

f. Leave the **Allow Complex Identities** option cleared as it does not apply to this type of security provider.

g. Click **Save** or **Apply Changes**, depending whether you are creating or modifying a security provider.

What's Next?

When you are creating or modifying the security provider:

- For an Active Directory source, configure and index the source.
- To be used by another security provider, create or modify the other security provider.

7. Configuring and Indexing a Google Drive for Work Source

A source defines a set of configuration parameters for a specific Google Apps for Work account.

To configure and index a Google Drive for Work source

1. On the Coveo server, access the Administration Tool.
2. Select **Index** > **Sources and Collections**.
3. In the **Collections** section:

    a. Select an existing collection in which you want to add the new source.

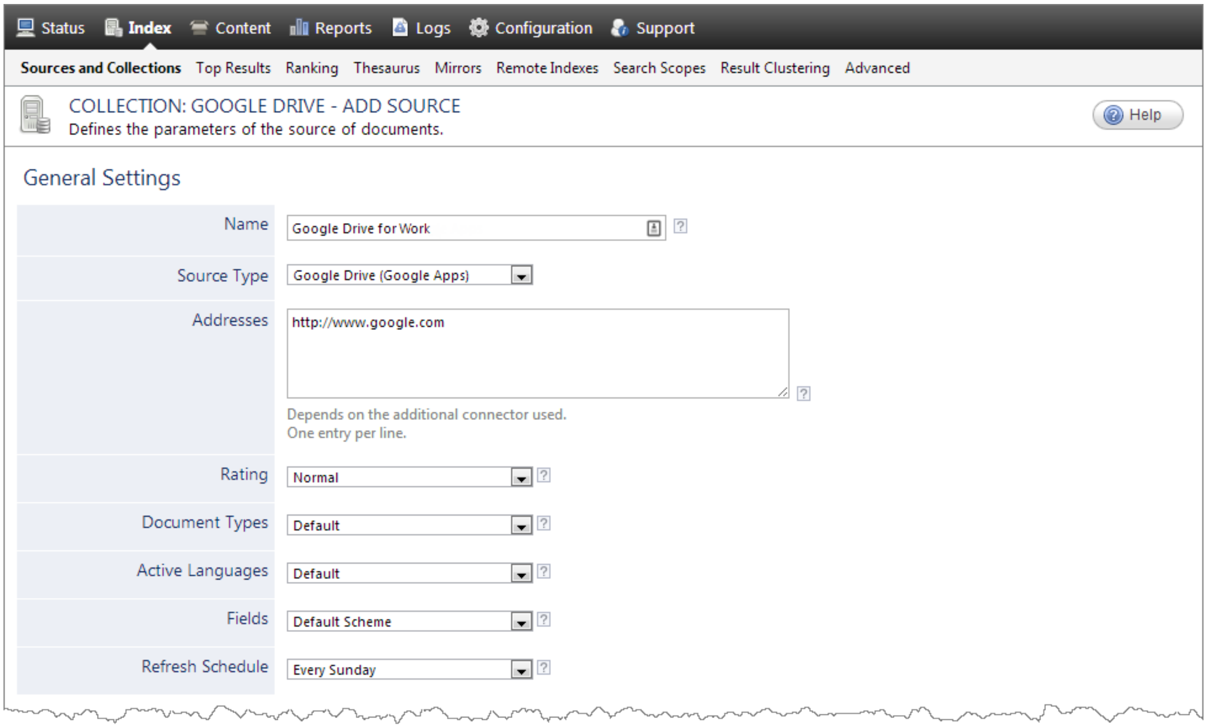
    OR

    b. Click **Add** to create a new collection.

4. In the **Sources** section, click **Add**.

    The **Add Source** page that appears is organized in three sections.

5. In the **General Settings** section of the **Add Source** page:



COLLECTION: GOOGLE DRIVE - ADD SOURCE
Defines the parameters of the source of documents.

General Settings

Name	Google Drive for Work
Source Type	Google Drive (Google Apps)
Addresses	http://www.google.com Depends on the additional connector used. One entry per line.
Rating	Normal
Document Types	Default
Active Languages	Default
Fields	Default Scheme
Refresh Schedule	Every Sunday

    a. Enter the appropriate value for the following required parameters:

    Name

    Enter a descriptive name of your choice for the connector source.

Example: `Google Drive for Work`

Source Type

Select the connector used by this source. In this case, select **Google Drive (Google Apps)**.

Notes:

- If you do not see **Google Drive (Google Apps)**, your environment does not meet the requirements (see "Google Drive for Work Connector Requirements" on page 6).
- Do not select the **Google Drive (Single User)** option.

Addresses

This parameter is not used, but must not be empty. Enter `http://www.google.com`.

Fields

Select the field set that you created for your Google Drive source (see Google Drive for Work Connector Deployment Overview).

Refresh Schedule

Time interval at which the index is automatically refreshed to keep the index content up-to-date. By default, the **Every day** option instructs CES to refresh the source everyday at 12 AM. Because the incremental refresh takes care of maintaining the source up-to-date, you can select a longer interval such as **Every Sunday**.

b. Review the value for the following parameters that often do not need to be modified:

Rating

Change this value only when you want to globally change the rating associated with all items in this source relative to the rating to other sources.

Example: When a source replaces a legacy system, you may want to set this parameter to **High**, so that in the search interface, results from this source appear earlier in the list compared to those from legacy system sources.

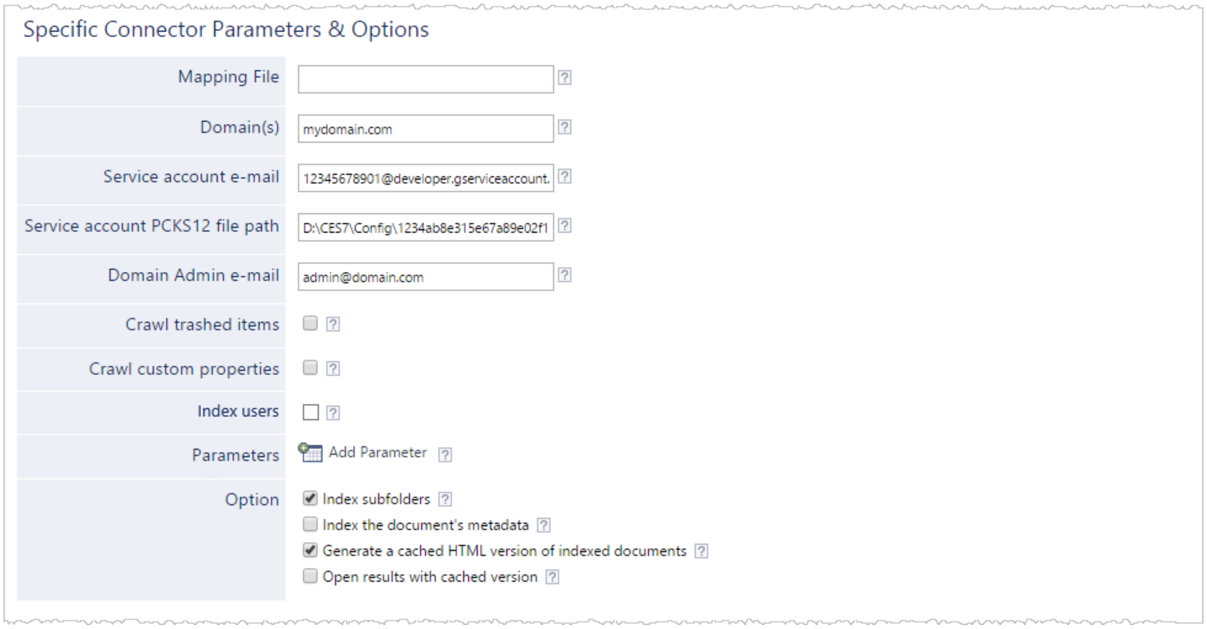
Document Types

If you defined a custom document type set for this source, select it.

Active Languages

If you defined custom active language sets, ensure to select the most appropriate for this source.

6. In the **Specific Connector Parameters & Options** section of the **Add Source** page:



Specific Connector Parameters & Options

Mapping File	
Domain(s)	mydomain.com
Service account e-mail	12345678901@developer.gserviceaccount.
Service account PCKS12 file path	D:\CES7\Config\1234ab8e315e67a89e02f1
Domain Admin e-mail	admin@domain.com
Crawl trashed items	☐
Crawl custom properties	☐
Index users	☐
Parameters	Add Parameter
Option	☑ Index subfolders ☐ Index the document's metadata ☑ Generate a cached HTML version of indexed documents ☐ Open results with cached version

a. In the **Mapping File** box, optionally enter the path to a mapping file that should apply to the items in this source.

   Leave this box empty to use the default mapping that should be appropriate in most cases.

   When the default mapping does not fulfill your needs, contact Coveo Support for assistance. Your XML mapping file must respect the standard Coveo mapping file schema.

   Example: `D:\CES7\Config\GoogleAppsMappingFile.xml`

b. CES 7.0.7433+ (February 2015) Configure this parameter:

   Domain Admin e-mail

   Enter the domain admin account email used to obtain the list of users in the domain.

   Example: `admin@domain.com`

   Note: The e-mail you enter here must be the same as the one you entered previously when configuring the security provider (see Configuring a Google Drive for Work Security Provider).

c. Using the following parameters, authorize the Coveo crawler to access the Google Drive of your users:

   Domain(s)

   Enter the Google Drive domain that you want to index. When your Google Apps account contains more than one domain, you can enter a semicolon-separated list of domains to index.

Examples:

- One domain: `mydomain.com`
- Multiple domains: `myfirstdomain.com;my.second.domain.com`

Important: The domain(s) specified in this list must match the one(s) specified in the security provider **[Domain-wide mode] Managed domains** list (see Configuring a Google Drive for Work Security Provider).

Service account e-mail

Enter the service account **Email address** previously obtained (see Authorizing the Coveo Connector to Access Your Google Drive). It must be the same email that you entered when configuring the security provider (see Configuring a Google Drive for Work Security Provider)

Example: `12345678901@developer.gserviceaccount.com`

Service account PCKS12 file path

Note: CES 7.0.7599+ (April 2015) This parameter is no longer required and can be left empty when you use the `ServiceAccountPkcs12FileData` hidden parameter (see Modifying Hidden Google Drive for Work Source Parameters).

Enter the path on the Coveo Master server where you saved the previously obtained service account's PCKS12 private key file (see Authorizing the Coveo Connector to Access Your Google Drive). It must be the same path that you entered when configuring the security provider (see Configuring a Google Drive for Work Security Provider)

Example: `D:\CES7\Config\1234ab8e315e67a89e02f16ea38bd44d609471ff-privatekey.p12`

d. Select the type of content to index using the following options:

Crawl trashed items

Select to index the items in the user's trash. Not selected by default.

Crawl custom properties

Select to index custom properties that Google applications or your custom applications added on items. Not selected by default.

Note: Crawling custom properties adds one API call per indexed document. Selecting this option can notably increase the number of calls to the Google Drive API and the crawling time.

Index Users CES 7.0.9167+ (December 2017)

Select to index Google Drive users as separate documents. Not selected by default.

e. Click **Add Parameter** when you want to show and change the value of advanced source parameters (see "Modifying Hidden Google Drive for Work Source Parameters" on page 29).

f. The **Option** check boxes generally do not need to be changed:

Index Subfolders

This parameter is not taken into account for this connector.

Index the document's metadata

When selected, CES indexes all the document metadata, even metadata that are not associated with a field. The orphan metadata are added to the body of the document so that they can be searched using free text queries.

When cleared (default), only the values of system and custom fields that have the **Free Text Queries** attribute selected will be searchable without using a field query.

Example: A document has two metadata:

- `LastEditedBy` containing the value `Hector Smith`
- `Department` containing the value `RH`

In CES, the custom field `CorpDepartment` is bound to the metadata `Department` and its **Free Text Queries** attribute is selected.

When the **Index the document's metadata** option is cleared, searching for `RH` returns the document because a field is indexing this value. Searching for `hector` does not return the document because no field is indexing this value.

When the **Index the document's metadata** option is selected, searching for `hector` also returns the document because CES indexed orphan metadata.

Document's addresses are case-sensitive

Ensure that this option is selected because Google Drive document IDs are case sensitive.

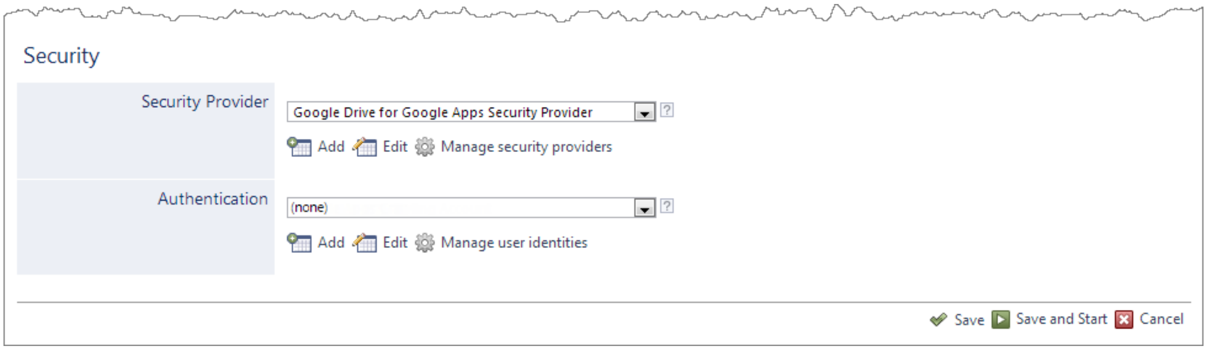
Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the **Quick View** link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use **Quick View** links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a **Quick View**. In this case, you must also select **Generate a cached HTML version of indexed documents**.

7. In the **Security** section of the **Add Source** page:



Security

Security Provider: Google Drive for Google Apps Security Provider

Authentication: (none)

a. When you chose to index Google Drive permissions, in the **Security Provider** drop-down list, select the Google Drive for Work security provider that you created for this source (see "Configuring a Google Drive for Work Security Provider" on page 15).

b. In the **Authentication** drop-down list:

- CES 7.0.7433+ (February 2015) Select **(none)**.
- CES 7.0.7338– (January 2015) Select the user identity that you created for this source (see Google Drive for Work Connector Deployment Overview).

8. Click **Save** to save the source configuration.

9. When you chose to not index Google Drive permissions, you can set source level permissions that apply to all documents in the source:

   a. In the navigation panel on the left, click **Permissions**.

   b. In the **Permissions** page, select **Specify the security permissions** to index.

   c. In the **Allowed Users** and **Denied Users** boxes, enter the users and groups that you respectively want to allow or deny to see search results from this source. The default is to allow `everyone \S-1-1-0\` (Active Directory Group).

   d. Click **Apply Changes**.

10. When you are ready to start indexing the Google Drive source, click **Rebuild**.

11. Validate that the source building process is executed without errors:

    - In the navigation panel on the left, click **Status**, and then validate that the indexing proceeds without errors.

      OR

    - Open the CES Console to monitor the source building activities.

What's Next?

Set an incremental refresh schedule for your source.

Consider modifying some hidden source parameters to try resolving other issues (see "Modifying Hidden Google Drive for Work Source Parameters" on page 29).

8. Modifying Hidden Google Drive for Work Source Parameters

The **Add Source** and **Source: ... General** pages of the Administration Tool present the parameters with which you can configure the connector for most Google Drive for Work setups. More advanced and more rarely used parameters are hidden. You can choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value. Consider changing values of hidden parameters when you encounter issues.

The following list describes the advanced hidden parameters available with Google Drive for Work sources. The parameter type (integer, string, etc.) appears between parentheses following the parameter name.

IgnoreLinkRequiredPermissions (Boolean) CES 7.0.8225.5+ (Mars 2016)

Whether to ignore permissions with a required link on the documents. The default value is `true`.

Notes:

- Permissions requiring links are either "Anyone with the link" or "Anyone at <domain> with the link" (see Share Google Drive files and folders).
- By default, in a Coveo search page, end-users cannot find Google Drive documents in search results with either the "Anyone with the link" or "Anyone at <domain> with the link" permissions.

NumberOfRefreshThreads (Integer)

The number of refresh threads used by the crawler for this source. The default value is `8`.

ResultsPerPage (Integer) CES 7.0.6684+ (May 2014)

Number of results to fetch per request made to Google Drive. The default value is `100`. The minimum value is `1` and the maximum value is `1000`. A small value (not recommended) forces the connector to make small but frequent queries to Google Drive. A larger value (recommended) leads to larger and less frequent queries.

Note: Queries to the Google Drive service are made per folder.

Example: With a value of `100`, if a folder contains 180 items, two queries will be necessary to obtain the items.

CommentsPerPage (Integer) CES 7.0.6684+ (May 2014)

Number of comments to fetch per request made to Google Drive. The default and maximum value is `100`. The minimum value is `1`.

CrawlSharedWithMeItems (Boolean) CES 7.0.6684+ (May 2014)

Whether to process items that have been shared with each user (`Shared with me`). The default value is `true`.

CrawlComments (Boolean) CES 7.0.6684+ (May 2014)

Whether to index comments from each item. The default value is `false`. Consider setting this parameter to `true` when you must have searchable comments. However, make comments searchable costs API calls and can increase crawling time depending on the number of comments in your Google Drive content.

Note: CES 7.0.6942– (August 2014) The `CrawlComments` hidden parameter default value is `true`.

UseFolderLinksInMyDrive (Boolean) CES 7.0.6684+ (May 2014)

Whether to use folder links that open directly in `My Drive` rather than in a folder view. The default value is `true`.

Example: In the search results breadcrumb for a *Shared with me* document, when a user clicks the parent folder and this parameter is set to `false`, the opened URL is in the form `https://drive.google.com/a/mydomain.com/folderview?id=[GUID]&usp=drivesdk#`, showing a file and folder view with a **Open in My Drive** link.

When set to `true`, the opened URL is in the form `https://drive.google.com/a/mydomain.com/?usp=folder#folders/[GUID]`, directly opening in **My Drive**, as if the user had clicked the **Open in My Drive** link, thus saving one click.

IndexGoogleAppsDocThumbnails (Boolean)

Whether to index thumbnails for Google Apps for Work documents. The default value is `false`. Setting this parameter to `true` to index document thumbnails would increase the crawling time by about 5%.

IndexNativeDocThumbnails (Boolean)

Whether to index thumbnails for native documents (PDF, DOC, XLS, etc.). The default value is `false`.

AddFromAndToFields (Boolean) CES 7.0.7022+ (September 2014)

Whether to add the `sysfrom` and `systo` fields to system fields. The default value is `true`. Adding these fields can have a significant impact on the crawling performance, so consider setting this parameter to `false` to improve crawling performance.

EnablePrefetcher (Boolean) CES 7.0.7104+ (October 2014)

Whether the prefetcher is used by the crawler. The default value is `false` in which case the connector processes the items of a folder retrieved with an API call before making the next API call for the next Google Drive folder.

It is recommended to enable the prefetcher that immediately makes the next API call and improves crawling performances, particularly when folders contain many documents.

NumberOfPrefetchedItems (Integer) CES 7.0.7104+ (October 2014)

The maximum number of items to prefetch will save in memory when the prefetcher is enabled (see EnablePrefetcher). The default value is `300`. The minimum value is `1` and the maximum value is `1000`.

Consider increasing the `NumberOfPrefechedItems` value if you increase the number of threads used by the crawler (see "NumberOfRefreshThreads (Integer)" on page 29).

ServiceAccountPkcs12FileData (Integer) CES 7.0.7599+ (April 2015)

The service account's PKCS12 private key file encoded data. The PKCS12 file encoded in Base64. The default value is `null`.

> **Notes:**
>
> - You need to open the certificate in a text editor and use an encoding application such as Motobit to convert the certificate content to the Base64 format.
> - This parameter is only used when the **Service account PKCS12 file path** parameter is empty (see Configuring and Indexing a Google Drive for Work Source).

FileMimeTypesWithComments (String) CES 7.0.7914+ (October 2015)

Semicolon separated list of document MIME types which support comments in Google Drive (see Supported MIME Types). The default value is `application/vnd.google-apps.document;application/vnd.google-apps.presentation;application/vnd.google-apps.spreadsheet;application/vnd.google-apps.drawing`.

To modify hidden Google Drive for Work source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 31 to add one or more Google Drive for Work source parameters.
2. For a new Google Drive for Work source, access the **Add Source** page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select **Index** > **Sources and Collections**.
   b. Under **Collections**, select the collection in which you want to add the source.
   c. Under **Sources**, click **Add**.
   d. In the **Add Source** page, edit the newly added advanced parameter value.
3. For an existing Google Drive for Work source, access the **Source: ... General** page of the Administration Tool to modify the value of the newly added advanced parameter:
   a. Select **Index** > **Sources and Collections**.
   b. Under **Collections**, select the collection containing the source you want to modify.
   c. Under **Sources**, click the existing Google Drive for Work source in which you want to modify the newly added advanced parameter.
   d. In the **Source: ... General** page, edit the newly added advanced parameter value.
4. Rebuild your Google Drive for Work source to apply the changes to the parameters.

8.1 Adding an Explicit Connector Parameter

Connector parameters applying to all sources indexed using this connector are called explicit parameters.

When you create or configure a source, the Coveo Enterprise Search (CES) 7.0 Administration Tool presents parameters with which you can configure the connector for most setups. For many connectors, more advanced and more rarely used parameters also exist but are hidden by default. CES then uses the default value associated with each of these hidden parameters.

You can however choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value.

To add an explicit connector parameter

1. On the Coveo server, access the Administration Tool.

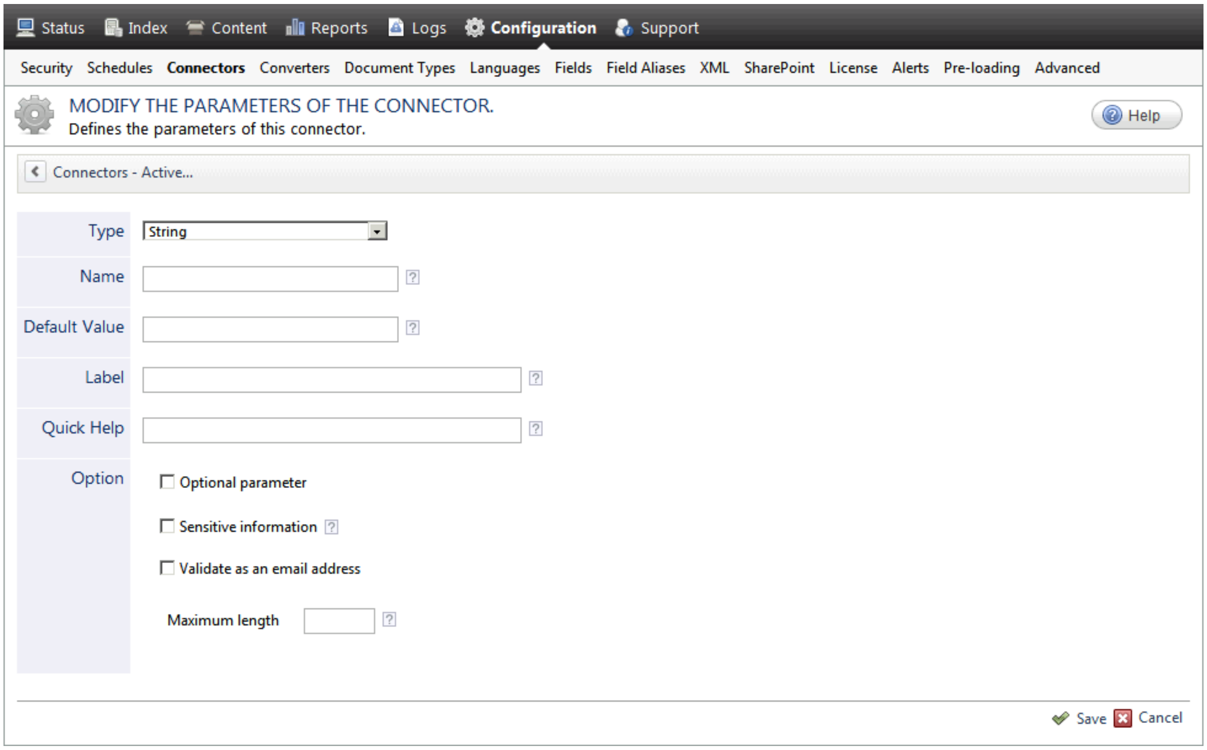
2. Select **Configuration** > **Connectors**.

3. In the list on the **Connectors** page, select the connector for which you want to show advanced hidden parameters.

4. In the **Parameters** section of the selected connector page, click **Add Parameter** for each hidden parameter that you want to modify.

   Note: The **Add Parameter** button is present only when hidden parameters are available for the selected connector.

5. In the **Modify the parameters of the connector** page:



MODIFY THE PARAMETERS OF THE CONNECTOR.
Defines the parameters of this connector.

Type: String
Name
Default Value
Label
Quick Help
Option: □ Optional parameter
□ Sensitive information
□ Validate as an email address
Maximum length

   a. In the **Type** list, select the parameter type as specified in the parameter description.

   b. In the **Name** box, type the parameter name exactly as it appears in the parameter description. Parameter names are case sensitive.

c. In the **Default Value** box, enter the default value specified in the parameter description.

Important: Do not set the value that you want to use for a specific source. The value that you enter here will be used for all sources defined using this connector so it must be set to the recommended default value. You will be able to change the value for each source later, in the **Add Source** and **Source: ... General** pages of the Administration Tool.

d. In the **Label** box, enter the label that you want to see for this parameter.

Example: To easily link the label to the hidden parameter, you can simply use the parameter name, and if applicable, insert spaces between concatenated words. For the **BatchSize** hidden parameter, enter `Batch Size` for the label.

Note: To create multilingual labels and quick help messages, use the following syntax: `<@ln>text</@>`, where *ln* is replaced by the language initials—the languages of the Administration Tool are English (en) and French (fr).

Example: `<@fr>Chemin d'accès du fichier de configuration</@><@en>Configuration File Path</@>` is a label which is displayed differently in the French and English versions of the Administration Tool.

Tip: The language of the Administration Tool can be modified by pressing the following key combination: `Ctrl+Alt+Page Up`.

e. Optionally, in **Quick Help**, enter the help text that you want to see for this parameter when clicking the question mark button ? that will appear beside the parameter value.

Tip: Copy and paste key elements of the parameter description.

f. When **Predefined values** is selected in the **Type** parameter, in the **Value** box that appears, enter the parameter values that you want to see available in the drop-down parameter that will appear in the Administration Tool interface. Enter one value per line. The entered values must exactly match the values listed in the hidden parameter description.

g. Select the **Optional parameter** check box when you want to identify this parameter as an optional parameter. When cleared, CES does not allow you to save changes when the parameter is empty. This parameter does not appear for **Boolean** and **Predefined values** parameter types.

h. Select the **Sensitive information** check box for password or other sensitive parameter so that, in the Administration Tool pages where the parameter appears, the typed characters appear as dots to mask them. This parameter appears only for the **String** type.

Example: When you select the **Sensitive information** check box for a parameter, the characters typed appear as follows in the text box:

●●●●

i. Select the **Validate as an email address** check box when you want CES to validate that the text string that a user enters in this parameter respects the format of a valid email address. This parameter appears only for the **String** type.

j. In the **Maximum length** box, enter the maximum number of characters for the string. This parameter appears only for the **String** type. When you enter `0`, the length of the string is not limited.

k. Click **Save**.

6. Back in the **Connector** page, click **Apply Changes**.

   The hidden parameter now appears in the **Add Source** and **Source: ... General** pages of the Administration Tool for the selected source. You can change the parameter value from these pages. Refer to the documentation for each connector for details.

Note: When you want to modify a hidden source parameter, you must first delete it, and then redefine it with the modified values.