



Coveo Platform 7.0

Alfresco One 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.

© Coveo Solutions Inc., 2015

Coveo is a trademark of Coveo Solutions Inc. This document is protected by intellectual property laws and is subject to all restrictions specified in the Coveo Customer Agreement.

Document part number: PM-160307-EN

Publication date: 1/3/2019

Table of Contents

1. Alfresco One Connector	1
2. Alfresco One Connector Deployment Overview	3
3. Alfresco One Connector Requirements	5
4. Selecting an Alfresco One Full Read Account	6
5. Configuring an Alfresco One Security Provider	7
5.1 Configuring an Email Security Provider	9
6. Configuring and Indexing an Alfresco One Source	11
6.1 Modifying Hidden Alfresco One Source Parameters	15
6.2 Adding an Explicit Connector Parameter	16
6.3 Creating a Custom Alfresco One Mapping File	19

1. Alfresco One Connector

CES 7.0.8225+ (March 2016)

Alfresco One is an Enterprise Content Management (ECM) platform designed to store, share, and manage organization documents.

This Coveo connector for Alfresco One allows Coveo administrators to crawl and index the Alfresco content repository. The indexed content is then integrated into the Coveo unified index. The connector indexes all files and the attached permissions so that in the Coveo search interfaces, a user can easily find any but only content to which he has access in Alfresco One.

Note: The connector also supports Alfresco Community Edition, but not Alfresco Cloud Edition.

The features of the Alfresco One connector are:

Content Indexing

The connector can retrieve and index exclusively the following default Alfresco One content repository entity types:

- Documents
- Records
- AlfrescoFolders
 - Spaces
 - Sites
 - Folders
 - Categories

Note: Currently, only comments and likes on discussion forum topics are indexed, meaning that site, document library, document, and blog post comments and likes are ignored during the crawling process.

Fully Supported Security Model

The connector fully supports the Alfresco One security model. This means that, in the Coveo search interface, a user searching Alfresco One content only sees the content to which he has access in Alfresco One.

Incremental Refresh

Periodically queries the Alfresco One system for the latest items modifications (addition, edition, deletion), keeping the index content up-to-date.

Notes:

- Auditing must be enabled for indexed entities for the connector to be able to retrieve items modification (see [Enabling Auditing in Alfresco](#)).
- When auditing is not enabled, incremental refreshes are performed as full refreshes.

What's Next?

Review the deployment process (see "[Alfresco One Connector Deployment Overview](#)" on page 3).

2. Alfresco One Connector Deployment Overview

The following procedure outlines the steps needed to deploy the Alfresco One connector. The steps indicate the order in which you must perform configuration tasks on both the CES and Alfresco One systems.

1. Validate that your environment meets the requirements (see ["Alfresco One Connector Requirements" on page 5](#)).
2. In the Alfresco One system:
 - a. Select or create the crawling account.

The connector needs an Alfresco One account with which it can crawl all the Alfresco One content that you want to index (see ["Selecting an Alfresco One Full Read Account" on page 6](#)).

- b. Enable auditing of content

Note: When auditing is not enabled, incremental refreshes are performed as full refreshes.

- i. With a text editor, open the Alfresco One global properties file located in the Alfresco One folder.

Example: `C:\Program Files\Alfresco\tomcat\shared\classes\alfresco-global.properties`

- ii. Add one of the following property:

- `audit.enabled=true`
- `audit.cmischangelog.enabled=true`

to enable audit in general.

to implement the change log feature on your CMIS server.

Note: The logs contain all create, read, update, and delete operations that users performed on objects in the Alfresco One repository.

- iii. Save the file.
 - iv. Restart the Alfresco Enterprise service to apply changes.
3. On the Coveo server, in the Coveo Administration Tool:

- a. Configure the user identity

You must assign the selected Alfresco One full-read account to a Coveo user identity.

- b. Optionally create an Email security provider

When an email is defined for each of your users in Alfresco and this email is used to authenticate them in your Coveo search interface, you can create an Email security provider to allow you to map your Alfresco users to their email (see ["Configuring an Email Security Provider" on page 9](#)).

- c. Create a security provider.

When you want to index permissions, you must configure a security provider (see ["Configuring an Alfresco One Security Provider" on page 7](#)).

- d. Create an Alfresco One field set.

It is recommended to import the out-of-the-box Alfresco One field set (`[CES_Path]\Bin\Coveo.CES.CustomCrawlers.Alfresco2.FieldSet.xml`) to be able to easily add Alfresco One specific facets to your Coveo search interfaces.

- e. Configure and index the Alfresco One source

The connector needs to know details about the Alfresco One system to be able to index its content (see ["Configuring and Indexing an Alfresco One Source" on page 11](#)).

- f. Optionally, modify hidden source parameters

Once your Alfresco One source is up and running, if you encounter timeout or performance issues, consider modifying some hidden source parameters to try resolving the issues (see ["Modifying Hidden Alfresco One Source Parameters" on page 15](#)).

- g. Optionally, customize the mapping file to fine-tune indexed content

You can customize the connector mapping file to fine-tune the indexed content or to index other default entities in your Alfresco One system (see ["Creating a Custom Alfresco One Mapping File" on page 19](#)).

3. Alfresco One Connector Requirements

Your environment needs to meet the following requirements to be able to use the Coveo connector for Alfresco One systems:

- **CES 7.0.8225+ (March 2016)**

The connector was introduced with the CES 7.0.8225 March 2016 release.

- Coveo license for the Alfresco One connector

Your Coveo license must include support for the Alfresco One connector to be able to use this connector.

- Alfresco versions

- Supported versions:

- Alfresco One 4 to 4.2.5

Note: An Alfresco prototype connector is also available on demand to index the following versions:

- Alfresco Community 4.2.c and 4.2.d
- Deprecated support versions: Alfresco Community 3.3, 3.4
- Contact [Coveo Support](#) to ask the connector files.

Supported Alfresco products:

- Alfresco Document Management
- Alfresco Record Management
- Alfresco Share

What's Next?

Enable auditing on content (see [Alfresco One Connector Deployment Overview](#)).

4. Selecting an Alfresco One Full Read Account

The Coveo connector needs to connect to the Alfresco One system using an account that has access to all the Alfresco One content that you want to index. An account member of the administrator group (`ALFRESCO_ADMINISTRATORS`) is the simplest choice.

The connector only reads and does not modify Alfresco One content. Consequently, in your Alfresco One system, you can select an existing account or create a new account that has full access to the Alfresco One content that you want to index. A best practice is to create a fixed password account used exclusively by the Coveo connector.

5. Configuring an Alfresco One Security Provider

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

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

To configure an Alfresco One 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:

The screenshot displays the 'MODIFY SECURITY PROVIDER' configuration interface. The left sidebar contains a navigation menu with 'Security Providers' selected. The main content area shows the following configuration details:

Name	Alfresco One Security Provider
Security Provider Type	Alfresco One (x64)
Description	Alfresco One Security Provider
DLL Path	Coveo.CES.CustomCrawlers.Alfresco2.dll
Useridentity	Alfresco One Crawling Account
Alfresco Url	http://MyAlfrescoOneServer:8080
Alfresco CMIS 1.0 API URL	
Alfresco REST API URL	
Security Provider	Active Directory
Parameters	Add Parameter
Allow Complex Identities	<input type="checkbox"/>
Used By	

At the bottom right of the configuration area, there are buttons for 'Apply Changes' and 'Cancel'.

- a. Configure the following required parameters:

Name

Choose a meaningful name to identify the security provider.

Example: Alfresco One Security Provider

Security Provider Type

In the drop-down list, select **Alfresco One (x64)**.

User Identity

Select the Alfresco One user identity that you created previously (see [Alfresco One Connector Deployment Overview](#)).

- b. Configure the following required parameters:

Alfresco URL

The URL of your Alfresco One content repository server.

Example: `https://MyAlfrescoOneServer:[port]/share`

Note: You will enter the same value when configuring the source (see "[Configuring and Indexing an Alfresco One Source](#)" on page 11).

Alfresco CMIS 1.0 API URL

The URL of the CMIS 1.0 Atom endpoint of the Alfresco One instance. Leave blank to use the default one.

Example: `http://MyAlfrescoOneServer:[port]/api/[RepositoryName]/cmis/versions/1.0/atom`

Alfresco REST API URL

The URL of the REST API Endpoint of the Alfresco One Instance. Leave blank to use default one which is your Alfresco One repository server URL followed by `alfresco/service/cmis`.

Example: `https://MyAlfrescoOneServer:[port]/alfresco/service/cmis`

Security Provider

Select the security provider that you selected or created to allow this security provider to resolve and expand the groups (see [Alfresco One Connector Deployment Overview](#)).

Note: The Alfresco security provider can be chained with either an Active Directory or an Email security provider.

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

What's Next?

Create and index a source (see "[Configuring and Indexing an Alfresco One Source](#)" on page 11).

5.1 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:

The screenshot shows the 'MODIFY SECURITY PROVIDER' configuration page. The navigation menu on the left includes Roles, Impersonators, Security Providers (selected), User Identities, and Super User Access. The main content area has a breadcrumb 'Security - Security...' and a 'Help' button. The configuration fields are as follows:

Name	Email Security Provider
Security Provider Type	Email (x64)
Description	Email Security Provider
DLL Path	Coveo.CES.CustomCrawlers.EmailSecurityProvider.dll
UserIdentity	(none) [Add] [Edit] [Manage user identities]
Security Provider	(none) [Add] [Edit] [Manage security providers]
Parameters	[Add Parameter] [?]
Allow Complex Identities	<input type="checkbox"/> [?]
Used By	

At the bottom right, there are 'Apply Changes' and 'Cancel' buttons.

- 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. Configuring and Indexing an Alfresco One Source

A source defines a set of configuration parameters for a specific Alfresco One system.

To configure and index an Alfresco One 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**.
5. In the **General Settings** section of the **Add Source** page:

The screenshot shows the 'Add Source' configuration page for an Alfresco One collection. The page has a navigation bar with 'Index' selected. Below the navigation bar, there are tabs for 'Sources and Collections', 'Top Results', 'Ranking', 'Thesaurus', 'Mirrors', 'Remote Indexes', 'Search Scopes', 'Result Clustering', and 'Advanced'. The main content area is titled 'COLLECTION: ALFRESCO ONE - ADD SOURCE' and includes a 'Help' button. The 'General Settings' section contains the following fields:

- Name:** A text input field containing 'Alfresco One'.
- Source Type:** A dropdown menu set to 'Alfresco One'.
- Addresses:** A text area containing 'https://MyAlfrescoOneServer:8080'.
- Rating:** A dropdown menu set to 'Normal'.
- Document Types:** A dropdown menu set to 'Default'.
- Active Languages:** A dropdown menu set to 'Default'.
- Fields:** A dropdown menu set to 'Alfresco One field set'.
- Refresh Schedule:** A dropdown menu set to '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: Corporate Alfresco One Server

Source Type

Select the connector used by this source. In this case, select **Alfresco One**.

Note: If you do not see **Alfresco One** in the **Source Type** list, ensure that your environment meets the requirements (see "[Alfresco One Connector Requirements](#)" on page 5).

Addresses

The URL to the Alfresco One content repository server in the following format:

The root address of the Alfresco organization in the format:

```
http://[serverName]:[port]/share
```

where you replace `[serverName]:[port]` by the host name and port of your Alfresco One server.

Note: When you want to index more than one Alfresco One server or more than one organization, the best practice is to enter only one address here for one server/organization, and then create other sources for other servers or organizations.

- b. The following parameters generally do not need to be changed:

Rating

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

Example: If this source was for a legacy system, you may want to set this parameter to **Low**, so that in the search interface, results from this source appear later in the list compared to those from other sources.

Document Types

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

Active Languages

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

Fields

Select the field set that you created earlier (see [Alfresco One Connector Deployment Overview](#)).

Refresh Schedule

Time interval at which the source 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 (supported when auditing is enabled) takes care of maintaining the source up-to-date, you can select a longer interval such as **Every Sunday**.

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

Specific Connector Parameters & Options

Number of Refresh Threads	<input type="text" value="2"/> ?
Mapping File	<input type="text" value="Coveo.CES.CustomCrawlers.Alfresco2.MappingFile.xml"/> ?
Parameters	<input type="button" value="Add Parameter"/> ?
Option	<input checked="" type="checkbox"/> Index subfolders ? <input type="checkbox"/> Index the document's metadata ? <input type="checkbox"/> Document's addresses are case-sensitive ? <input checked="" type="checkbox"/> Generate a cached HTML version of indexed documents ? <input type="checkbox"/> Open results with cached version ?

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

Number of Refresh Threads

Determines the number of refresh threads that allow the connector to crawl web pages in parallel. The default value is 2 threads.

Mapping File

The path to the mapping file. Leave the default value to use the default mapping file that comes with the connector (`Coveo.CES.CustomCrawlers.Alfresco2.MappingFile.xml`). If you create a custom mapping file, enter the full path to your custom mapping file (see ["Creating a Custom Alfresco One Mapping File" on page 19](#)). Contact [Coveo Support](#) for assistance if you need to customize the mapping file.

- b. In the **Parameter** section, click **Add Parameter** when you want to show advanced source parameters (see ["Modifying Hidden Alfresco One Source Parameters" on page 15](#)).
- c. In the **Option** section, review the default value of the following check boxes:

Index Subfolders

Leave this check box cleared. The connector for this type of source does not use this parameter.

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

Leave this check box cleared. This parameter needs to be checked only in rare cases for systems in which distinct documents may have the same name but different casing (for example: `mydocument` and `MyDocument`).

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.

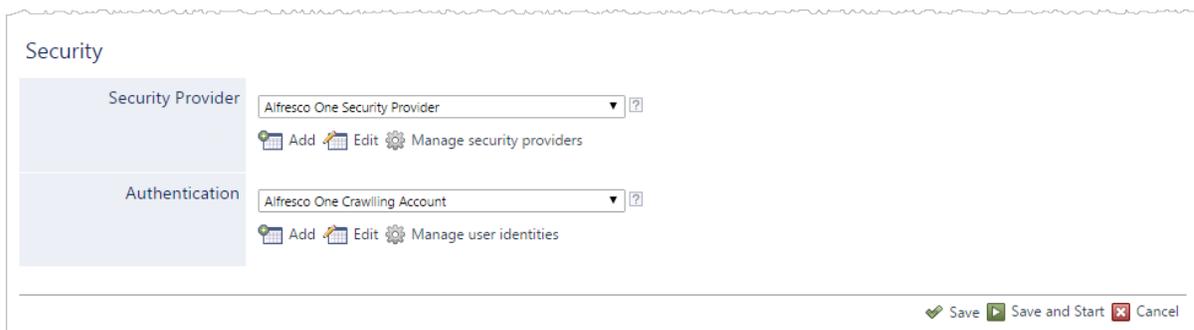
Consider clearing this check box only if you do not want to use Quick View links or to save resources when building the source.

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:



The screenshot shows the 'Security' configuration section of the 'Add Source' page. It contains two main sections: 'Security Provider' and 'Authentication'. The 'Security Provider' dropdown menu is set to 'Alfresco One Security Provider' and includes a help icon. Below this dropdown are three icons: 'Add', 'Edit', and 'Manage security providers'. The 'Authentication' dropdown menu is set to 'Alfresco One Crawling Account' and also includes a help icon. Below this dropdown are three icons: 'Add', 'Edit', and 'Manage user identities'. At the bottom right of the form, there are three buttons: 'Save' (with a green checkmark icon), 'Save and Start' (with a green play button icon), and 'Cancel' (with a red X icon).

- a. In the **Security Provider** drop-down list, when you chose to use a security provider, select the security provider that you created for this source (see ["Configuring an Alfresco One Security Provider" on page 7](#)).
 - b. In the **Authentication** drop-down list, select the user identity that you created previously for the Alfresco One system (see ["Selecting an Alfresco One Full Read Account" on page 6](#)).
8. Click **Save and Start** to save the source configuration and start indexing this source.
 9. 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.

6.1 Modifying Hidden Alfresco One 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 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 only when you encounter timeout error messages or performance issues.

There is only one advanced hidden parameter for Alfresco One sources. The parameter type (integer, string,...) appears between parentheses following the parameter name.

NumberOfRetries (Integer)

The number of retries allowed when a failed web request is recoverable. The default value is 3.

Timeout (Integer)

The number of seconds to wait before the request times out (i.e., the time for the server to respond to a request). The default value is 100 seconds.

ReadTimeout (Integer)

The timeout in seconds when reading the content from the server. The default value is 300 seconds.

RepositoryName (Integer)

The name of the repository to index. The default value is `-default-`.

BatchSize (Integer)

Number of items to fetch per request made to the Alfresco One server. The default value is 25. The minimum value is 1. A small value forces the connector to make small but frequent queries to the Alfresco One server. A larger value leads to larger and less frequent queries.

CacheTTLInMinutes (Integer)

The number of minutes an unused cached item (user or CMIS object) can remain in the cache. The default value is 5 minutes.

Use the following procedure only when you want to modify the above hidden source parameters.

To modify hidden Alfresco One source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 16 to add an Alfresco One hidden source parameter.
2. For a new Alfresco One 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 Alfresco One 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 Alfresco One 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, and then click **Apply Changes**.

6.2 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:

- 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.

6.3 Creating a Custom Alfresco One Mapping File

The Alfresco One mapping file exactly determines which types of Alfresco One documents are indexed and where this information is added to the Coveo unified index.

The default mapping file is embedded within the connector and is automatically used when no mapping file is specified in the source.

The default mapping file allows to index the following Alfresco document types:

- Documents
- Records
- AlfrescoFolders
 - Spaces
 - Sites
 - Folders
 - Categories

To create a custom Alfresco One mapping file

1. Using a text editor, create an XML file that respects the Alfresco One mapping file format (see the ["Mapping File Format" on page 19](#) section).
2. Save the file on the Coveo server (recommended folder and filename: [Index_Path]\Config\Coveo.CES.CustomCrawlers.Alfrescov2.config where by default [Index_Path] = C:\CES7).
3. Specify the mapping file path and filename in the Alfresco One source (see ["Configuring and Indexing an Alfresco One Source" on page 11](#)).

Mapping File Format

The mapping file is an XML file that contains various sections and subsections. The root node is <Mappings>. It contains various <CommonMapping> nodes, each defining one type to be indexed.

The first <DefaultMapping> node contains mappings that apply to all entities defined in the mapping file.

The following example contains mappings that add a descriptive title for data lists, todo lists and link items:

```
<Mappings>
  <Version>1</Version>
  <CommonMapping>
  </CommonMapping>
  <Mapping type="F:dl:dataList">
    <Title>%[cmis:description]</Title>
  </Mapping>
  <Mapping type="D:lnk:link">
```

```
<Title>[%[lnk:description]]</Title>
</Mapping>
<Mapping type="D:dl:todoList">
  <Title>[%[dl:todoTitle]]</Title>
</Mapping>
<Mapping type="D:dl:contact">
  <Title>[%[dl:contactFirstName] %[dl:contactLastName]]</Title>
</Mapping>
<DefaultMapping>
</DefaultMapping>
</Mappings>
```