coveo™

Coveo Platform 7.0

Liferay 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-120818-EN

Publication date: 1/3/2019

Table of Contents

1. Liferay Connector

The Coveo beta connector for Liferay portals allows crawling and bringing Liferay content into the unified index, making it easily searchable by end-users.

1.1 Features

The following details the features available in the Liferay connector:

Content indexing

The connector can retrieve and index exclusively the following default Liferay portal entity types:

- Communities

- Organizations

- Users

- User groups

- Blogs

- Calendar events

- Document libraries

- Message boards

- Web content

- Wikis

- Comments and files attached to indexed entity types.

The connector can be customized to index other default Liferay entities (see "Customizing the Liferay Connector Mapping File" on page 24).

Fully supported security model

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

Partial incremental refresh

The Coveo Liferay portlet plugin registers events to quickly and efficiently index new, modified, and deleted Liferay items.

Note: Some item changes require a source full refresh to be taken into account (see Limitations).

1.2 Limitations

- Limited incremental refresh capabilities:

    - A full refresh is needed to update permission changes.

    - A full refresh is needed to update Wiki page attachment changes.

    - A full refresh is needed to update moved items.

1.3 Feature History

CES version	Date	Features
7.0.8047	December 2015	Support for Liferay 6.1
7.0.5388	April 2013	Support of permission levels and sets.

What's Next?

Review the deployment process (see "Liferay Connector Deployment Overview" on page 3).

2. Liferay Connector Deployment Overview

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

1. Validate that your environment meets the requirements (see "Liferay Connector Requirements" on page 5).

2. In Liferay:

   a. Deploy the Coveo Liferay portlet plugin.

      The Coveo connector communicates with this plugin to crawl and index the Liferay content (see "About the Coveo Liferay Portlet Plugin Deployment" on page 6).

   b. Select or create the crawling account.

      The Coveo connector needs a Liferay account with which it can fully crawl the Liferay content (see "Setting up a Liferay Crawling Account" on page 13).

3. In the Coveo Administration Tool:

   a. Configure a user identity.

      The Coveo connector needs to know the Liferay account that you previously selected or created (see "Setting up a Liferay Crawling Account" on page 13). You must create a CES user identity to use this account. Use either the **Screen Name** or the **Email Address** of the dedicated Liferay account (see "Adding a User Identity" on page 15). You will later assign this user identity to the security provider and the source used by the connector to crawl the Liferay content.(see "Configuring and Indexing a Liferay Source" on page 18).

   b. `CES 7.0.8047+ (December 2015)` Optionally create security providers

      When you want to index Liferay permissions, you need at least two security providers to get Liferay item permissions and resolve and expand groups.

      In Liferay, users are identified by their screen names. Consequently, permissions returned by the Liferay security provider for each document are screen names (may be expanded from groups). The Liferay security provider then requires another security provider to uniquely identify users from their screen names.

      i. Start by selecting or creating a security provider that the Liferay 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 Active Directory (AD) user logon name, which match their screen name in Liferay, use the out-of-the-box or create a custom Active Directory security provider (see Configuring an Active Directory Security Provider).

         - When authenticated with their Active Directory (AD) account in the `DOMAIN\username` format, use

a REGEX Transform Member Name security provider chained to an Active Directory security provider to map the two member types (see Configuring an Active Directory Security Provider and Configuring a REGEX Transformation Security Provider).

> **Important:** A regex rule must be able to transform the Liferay screen name, so that the screen name match the AD username. Contact Coveo Support for assistance.

- When authenticated with their email address, use a REGEX Transform Member Name security provider chained to an Email security provider to map the two member types (see Configuring an Email Security Provider and Configuring a REGEX Transformation Security Provider).

> **Important:** A regex rule must be able to transform the Liferay screen name, so that the screen name match the email address. Contact Coveo Support for assistance.

ii. Then create a Liferay security provider chained with the security provider(s) you just created that the connector uses to resolve indexed permissions (see "Configuring a Liferay Security Provider" on page 16).

> **Note:** CES 7.0.7914– (October 2015) You need to configure a Liferay security provider, and then add the security provider on your .NET search interface since you cannot map Liferay user identities to AD ones (see "Configuring a Liferay Security Provider" on page 16 and Adding Security Providers to a .NET Search Interface).
>
> **Important:** JavaScript search interfaces cannot contain secured Liferay content.

c. Configure and index the Liferay source

The Coveo connector needs to know details about the Liferay portal to be able to index its content (see "Configuring and Indexing a Liferay Source" on page 18).

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

Consider customizing the connector mapping file to fine-tune the indexed content or to index other entities in your Liferay portal (see "About the Liferay Connector Mapping File" on page 23 and "Customizing the Liferay Connector Mapping File" on page 24).

e. Optionally, modify hidden source parameters

Once your Liferay source is up and running, if you encounter issues, consider modifying some hidden source parameters to try resolving the issues (see "Modifying Hidden Liferay Source Parameters" on page 25).

4. In the Interface Editor, add the built-in Liferay facets

CES comes with a built-in Liferay Type facet that you can add to your search interface so that users can more easily refine search results based on file types (see "Managing Built-in Facets and Related Results Appearing in a .NET Search Interface" on page 31).

3. Liferay Connector Requirements

Your environment must meet the following requirements to be able to use the Coveo connector for Liferay portals:

- Coveo license for the Liferay connector

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

- Liferay version 6 or 6.1

  The connector was developed and tested with Liferay version 6.0.5.

  Note: CES 7.0.8047+ (December 2015) Support for Liferay 6.1.

What's Next?

Review the deployment process (see "Liferay Connector Deployment Overview" on page 3).

4. About the Coveo Liferay Portlet Plugin Deployment

The Coveo connector retrieves content from the Liferay portal by connecting to the Coveo Liferay portlet plugin. You must deploy the plugin on the Liferay server.

Depending on your Liferay version:

- "Deploying the Coveo Liferay Portlet Plug-in for Liferay 6.0" on page 6

- "Deploying the Coveo Liferay Portlet Plug-in for Liferay 6.1" on page 9

4.1 Deploying the Coveo Liferay Portlet Plug-in for Liferay 6.0

You must install the version 6.0.6.1 of the Coveo plugin for Liferay on your Liferay server to index Liferay 6.0 content.
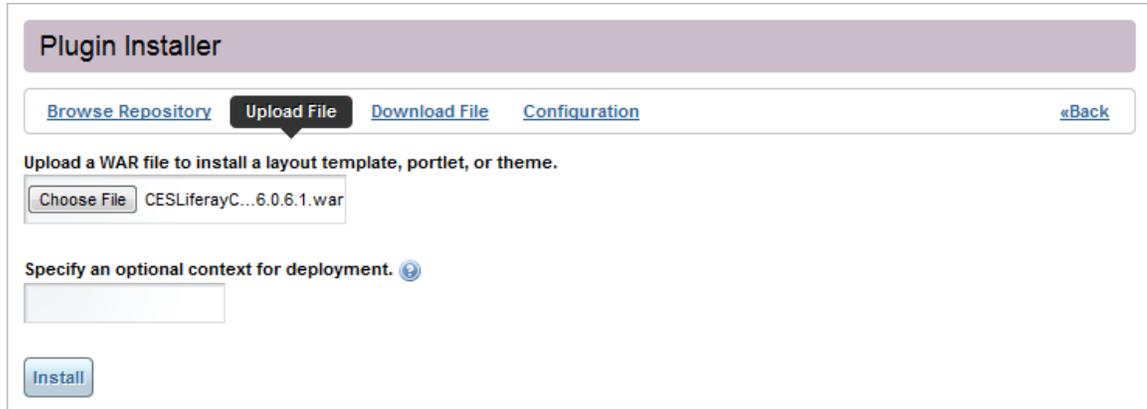
Note: CES 7.0.7914– (October 2015) You must install the 6.0.5.1 version of the plugin.

To deploy the Coveo Liferay portlet plugin

1. Using an administrator account, connect to the Coveo server.

2. From a browser, use an administrator account to connect to your Liferay portal.

3. On the menu bar of the Liferay portal, select **Manage** > **Control Panel**.

4. In the Liferay **Control Panel**:

   a. In the navigation panel on the left, under **Server**, click **Plugins Installation**.

   b. In the **Plugins Installation** page, select **Portlet Plugins**, and then click **Install More Portlets**.

   c. In the **Plugin Installer** page:

i. Select **Upload File**.

ii. Click **Choose File**, and then browse to and select the Coveo Liferay portlet plugin Web archive
   (WAR) file: `[CES_Path]\bin\CESLiferayConnector-portlet-6.0.6.1.war`

   CES 7.0.7914– (October 2015) `[CES_Path]\bin\CESLiferayConnector-portlet-6.0.5.1.war`

   Example: With the default installation path: `C:\Program Files\Coveo Enterprise Search 7\bin\CESLiferayConnector-portlet-6.0.6.1.war`

   CES 7.0.7914– (October 2015) `C:\Program Files\Coveo Enterprise Search 7\bin\CESLiferayConnector-portlet-6.0.5.1.war`

iii. Click **Install**.

d. End-users do not need to see the Coveo portlet. Consider hiding the Coveo portlet from users other than
   Administrator role members:

i. In the navigation panel on the left, under **Portal**, select **Plugins Configuration**.

ii. In the **Plugins Configuration** page, select the **CES Liferay Connector by Coveo Solutions Inc.**
   plugin.

iii. Under **Permissions**, for each user other than Administrator, click **Change**.

iv. In the **Roles** page, clear the **Add to page** check box, and then click **Save**.

v. Navigate back to the **Plugins Configuration** page for the Coveo plugin, and then click **Save**.

5. You must also enable access to the Liferay Web services for the Coveo server:

   a. Using an administrator account, connect to the Liferay server.

   b. Using a text editor:

      i. Open, or create if it does not already exist, the `[Liferay_Installation_Path]\tomcat-x.x.xx\webapps\ROOT\WEB-INF\classes\portal-ext.properties` text file.

      ii. Add the following lines to the file to allow access only to the Coveo Master server:

```
axis.servlet.hosts.allowed=[Coveo_Server_IP_Address]
 axis.servlet.https.required=false
 tunnel.servlet.hosts.allowed=[Coveo_Server_IP_Address]
 tunnel.servlet.https.required=false
```

      where you replace `[Coveo_Server_IP_Address]` by the IP address of the Coveo Master server.

      iii. Restart the Liferay server to apply changes to the properties and activate the listeners used for incremental refresh by shutting down and restarting the Web server:

Example: With a Tomcat server, in a command prompt window, run the following files:

```
C:\liferay-portal-6.0.6\tomcat-6.0.29\bin\shutdown.bat
C:\liferay-portal-6.0.6\tomcat-6.0.29\bin\startup.bat
```

Restarting the server is required to apply changes to the properties and activate the listeners used for incremental refresh.

What's Next?

Create a Liferay account with which the Coveo connector can fully crawl the Liferay content (see "Setting up a Liferay Crawling Account" on page 13).

4.2 Deploying the Coveo Liferay Portlet Plug-in for Liferay 6.1

CES 7.0.8047+ (December 2015)

You must install the version 6.1.1.1 of the Coveo plugin for Liferay on your Liferay server to index Liferay 6.1 content.

To deploy the Coveo Liferay portlet plugin

1. Using an administrator account, connect to the Coveo server.

2. From a browser, use an administrator account to connect to your Liferay portal.

3. On the menu bar of the Liferay portal, select **Go to** > **Control Panel**.

4. In the Liferay **Control Panel**:
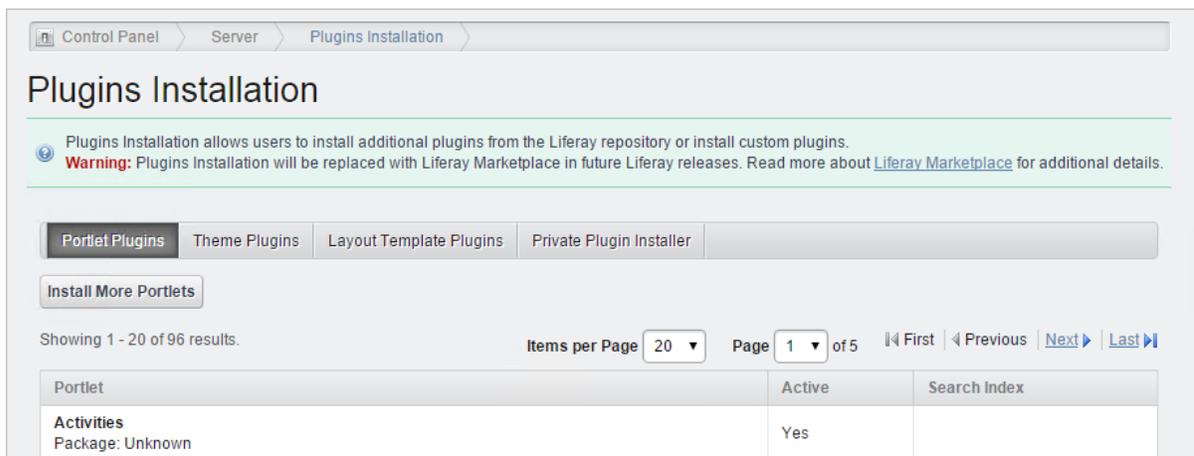
   a. In the navigation panel on the left, under **Server**, click **Plugins Installation**.

   b. In the **Plugins Installation** page, select the **Private Plugin Installer** tab, and then go to step e)

> **Note:** If you do not see the **Private Plugin Installer** tab:
>
> i. Select the **Portlet Plugins** tab, and then click **Install More Portlets**.
>
> ii. Follow the instructions starting at step c.

c. (When the Private Plugin Installer CE application is not installed on your Liferay portal) In the Liferay **Marketplace**:

    i. In the **Search** box, enter `private`, press `Enter`, and then select **Private Plugin Installer CE**.

    ii. In the **Private Plugin Installer CE** page, click **Free**.

    iii. In the **Purchase** page:

        A. Select an existing project or click **Add a New Project**.

        B. When you click **Add a New Project**:

            a. In the **New Project** dialog, enter a project name in the box, and then click **Add**.

            b. Select the project you just created.

        C. When you agree with the terms, select the **I have read and agree to the End User License Agreement and the Terms of Service** check box.

        D. In the box at the bottom of the page, enter a **Legal Entity Name**.

        E. Click **Purchase**.

        F. On the **Receipt** page, select **See Purchased**.

        G. In the **Purchased Apps** page, select the project in the **Owner** drop-down list, and then next to **Private Plugin Installer CE**, click **Install**.

    iv. In the navigation panel on the left, under **Server**, click **Plugins Installation**.

d. In the **Plugins Installation** page, select the **Private Plugin Installer** tab.
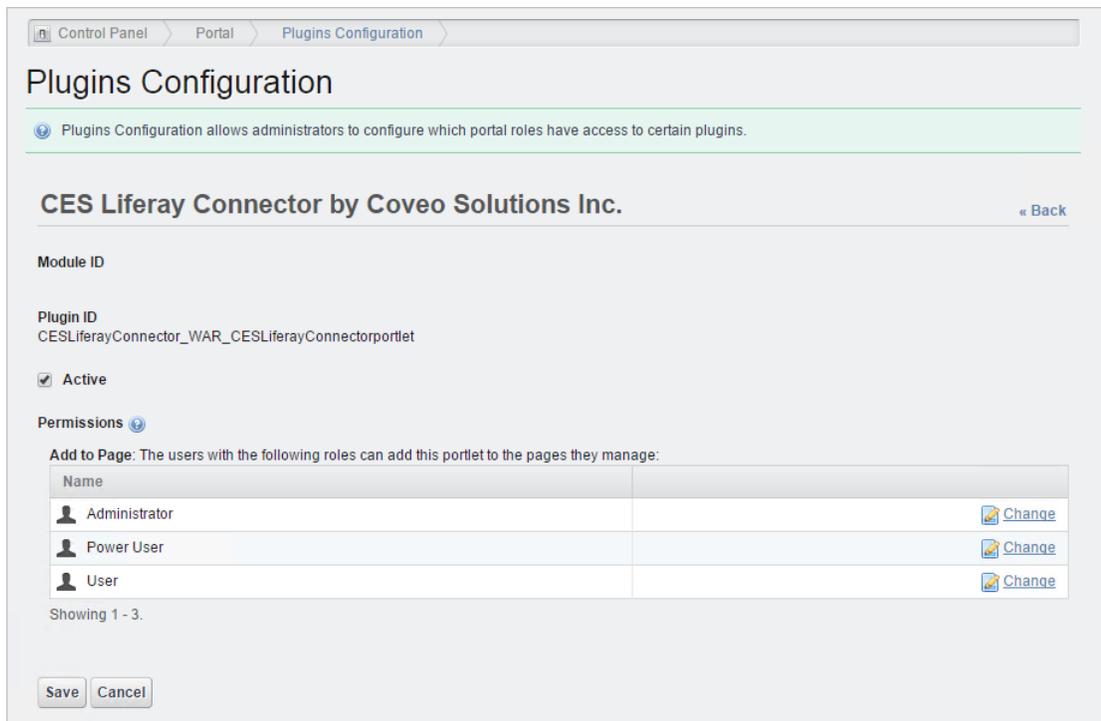
e. In the **Private Plugin Installer** page:
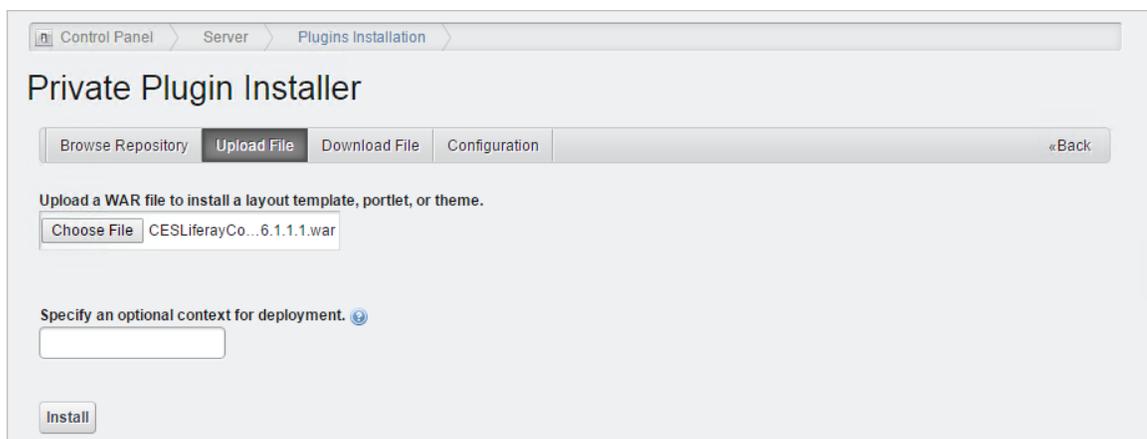
i. Select the **Upload File** tab.

ii. Click **Choose File**, and then browse to and select the Coveo Liferay portlet plugin Web archive (WAR) file: `[CES_Path]\bin\CESLiferayConnector-portlet-6.0.6.1.war` or `[CES_Path]\bin\CESLiferayConnector-portlet-6.1.1.1.war`.

> **Example:** With the default installation path: `C:\Program Files\Coveo Enterprise Search 7\bin\CESLiferayConnector-portlet-6.0.6.1.war`

iii. Click **Install**.

f. End-users do not need to see the Coveo portlet. Consider hiding the Coveo portlet from users other than Administrator role members:

i. In the navigation panel on the left, under **Portal**, select **Plugins Configuration**.

ii. In the **Plugins Configuration** page, select the **CES Liferay Connector by Coveo Solutions Inc.** plugin.

iii. Under **Permissions**, for each user other than Administrator, click **Change**.

iv. In the **Roles** page, clear the **Add to page** check box, and then click **Save**.

v. Navigate back to the **Plugins Configuration** page for the Coveo plugin, and then click **Save**.

5. You must also enable access to the Liferay Web services for the Coveo server:

a. Using an administrator account, connect to the Liferay server.

b. Using a text editor:

   i. Open, or create if it does not already exist, the `[Liferay_Installation_Path]\tomcat-x.x.xx\webapps\ROOT\WEB-INF\classes\portal-ext.properties` text file.

   ii. Add the following lines to the file to allow access only to the Coveo Master server:

```
axis.servlet.hosts.allowed=[Coveo_Server_IP_Address]
 axis.servlet.https.required=false
 tunnel.servlet.hosts.allowed=[Coveo_Server_IP_Address]
 tunnel.servlet.https.required=false
```

where you replace `[Coveo_Server_IP_Address]` by the IP address of the Coveo Master server.

   iii. Restart the Liferay server to apply changes to the properties and activate the listeners used for incremental refresh by shutting down and restarting the Web server:

Example: With a Tomcat server, in a command prompt window, run the following files:

```
C:\Liferay6.1.1GA2\tomcat-7.0.27\bin\shutdown.bat
C:\Liferay6.1.1GA2\tomcat-7.0.27\bin\startup.bat
```

Restarting the server is required to apply changes to the properties and activate the listeners used for incremental refresh.

What's Next?

Create a Liferay account with which the Coveo connector can fully crawl the Liferay content (see "Setting up a Liferay Crawling Account" on page 13).
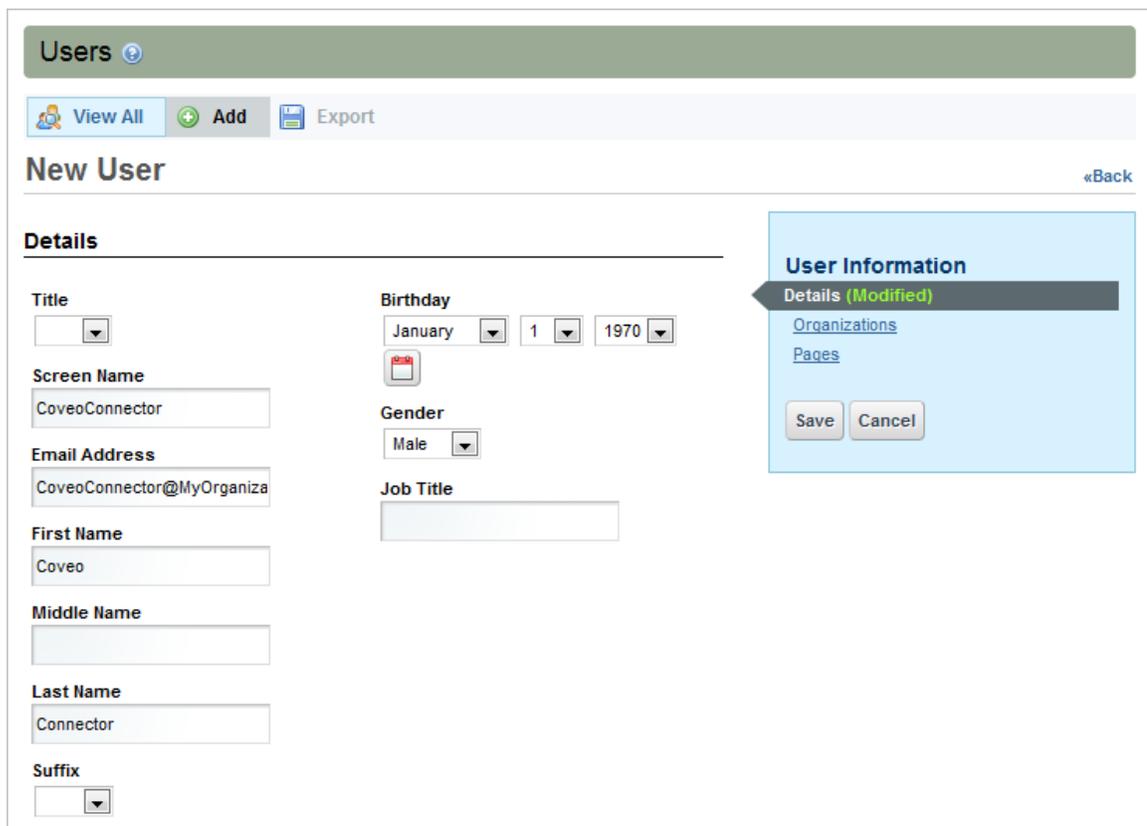
5. Setting up a Liferay Crawling Account

The Coveo connector needs to connect to the Liferay portal using an account that has read access to all the Liferay content that you want to index. The Coveo connector only reads and does not modify the Liferay content.

The best practice is to create a Liferay fixed password account used exclusively by the Coveo connector and assigned to the built-in Administrator role that has complete access to all Liferay content.

Setting up a dedicated Liferay full read account

1. Using a Liferay account that has an Administrator role, sign in to your Liferay portal.

2. On the menu bar, select **Manage** > **Control Panel**.

3. In the Liferay **Control Panel**, in the navigation panel on the left under **Portal**, click **Users**.

4. In the **Users** page:

   a. Click **Add** to create a new user.

   b. Under **New User**, enter arbitrary information describing the Coveo Connector user.

   c. In the navigation menu on the right, click **Save**.

   d. In the navigation menu on the right, under **User Information**, click **Roles**.

e. Under **Regular Roles**, click **Select**.

f. In the window that appears, under **Roles**, click the **Administrator**, to assign the Administrator role to the account.

g. If the **Power User** role has been assigned automatically, click **Remove** on the corresponding line, to ensure that only the Administrator role is assigned to this user.

h. In the navigation menu on the right, click **Save**.

i. In the navigation menu on the right, under **User Information**, click **Password**.

j. Enter a strong password in both the **New Password** and **Enter Again** boxes.

k. Leave the **Password Reset Required** checkbox cleared to prevent forcing the user to change the password when logging in the first time.

> **Note:** If the password changes in Liferay, you will also need to change it in the CES user identity (see "Adding a User Identity" on page 15).

l. In the navigation menu on the right, click **Save**.

What's Next?

On the Coveo server, configure a CES user identity for your Liferay crawling account (see "Adding a User Identity" on page 15).

Configure a security provider for your Liferay portal (see "Configuring a Liferay Security Provider" on page 16).

6. CES Configuration for the Liferay Connector

6.1 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:

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.

6.2 Configuring a Liferay Security Provider

The Coveo connector needs a security provider to be able to get the permissions for each indexed Liferay item, and therefore fully support the Liferay security model. This means that, in a Coveo search interface, a user searching for Liferay content only sees the content to which he has access in the Liferay portal.

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

To configure a Liferay security provider

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

2. Select **Configuration** > **Security**.

3. In the **Security** page, 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:

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

> **Example:** `Liferay Security Provider`

b. In the **Security Provider Type** drop-down list, select **Liferay (x64)**.

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

   i. In the drop-down list, select the user identity that you selected or created previously.

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

d. `CES 7.0.8047+ (December 2015)` (Optional) In the **Security Provider** section, in the drop-down list, select the security provider that you selected or created to allow this security provider to resolve and expand the groups (see Liferay Connector Deployment Overview).

e. In the **Liferay Portal Url** box, enter the address of the Liferay portal. This should be the same address as the one you will specify when you configure the source for the connector (see "Configuring and Indexing a Liferay Source" on page 18). Enter the URL in the `http://[LiferayPortal]:[port]` form.

> **Example:** `PortalUrl="http://MyLiferayPortal:8080"`

f. When you have more than one company defined in your Liferay Portal, in the **Portal Web Id** box, enter

which company to index. Otherwise, leave this box empty.

> **Note:** A company is associated with a WebId. You can find this ID in the Liferay **Control Panel**. Under **Server**, click **Portal Instances**, and then **Web Id**. There is a maximum of 1 ID per source. The default value is an empty string, which corresponds to the first WebId encountered.

    g. 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.

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

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

What's Next?

Configure and index a Liferay source (see "Configuring and Indexing a Liferay Source" on page 18).

6.3 Configuring and Indexing a Liferay Source

A source defines a set of configuration parameters for a specific Liferay portal.

> **Note:** In an environment with more than one Liferay portal, you need to define one source for each Liferay portal that you want to index.

To configure and index a Liferay 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:
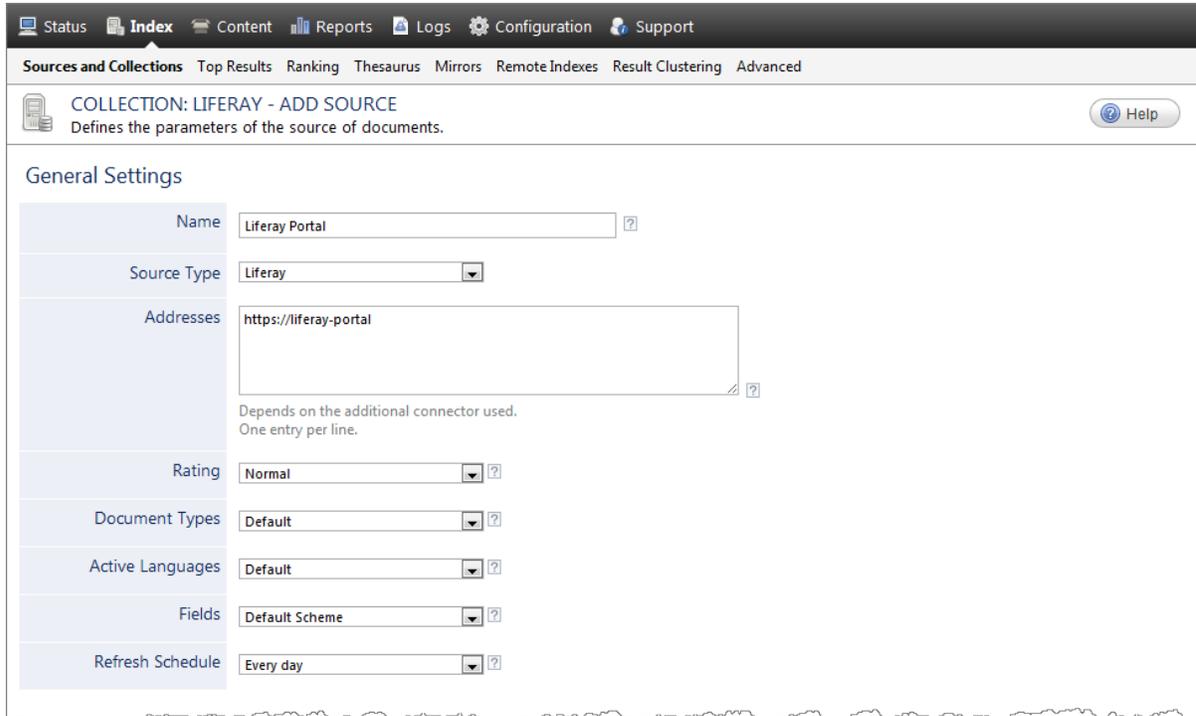
a. Enter the appropriate value for the following required parameters:

Name

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

Example: `Liferay Portal`

Source Type

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

Note: If you do not see **Liferay**, your environment does not meet the requirements (see "Liferay Connector Requirements" on page 5).

Addresses

Enter the root address of the Liferay portal in the format:

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

where you replace `[serverName]:[port]` by the host name and port of your Liferay portal. The default port is `8080`. The port is optional when equal to `80`.

Refresh Schedule

Time interval at which the source is automatically refreshed to keep the index content up-to-date. The recommended **Every day** option instructs CES to refresh the source everyday at 12 AM.

> **Note:** Incremental refresh does not catch changes to security and file attachment elements. Only a refresh does.

> **Note:** You can create new or modify existing source refresh schedules.

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

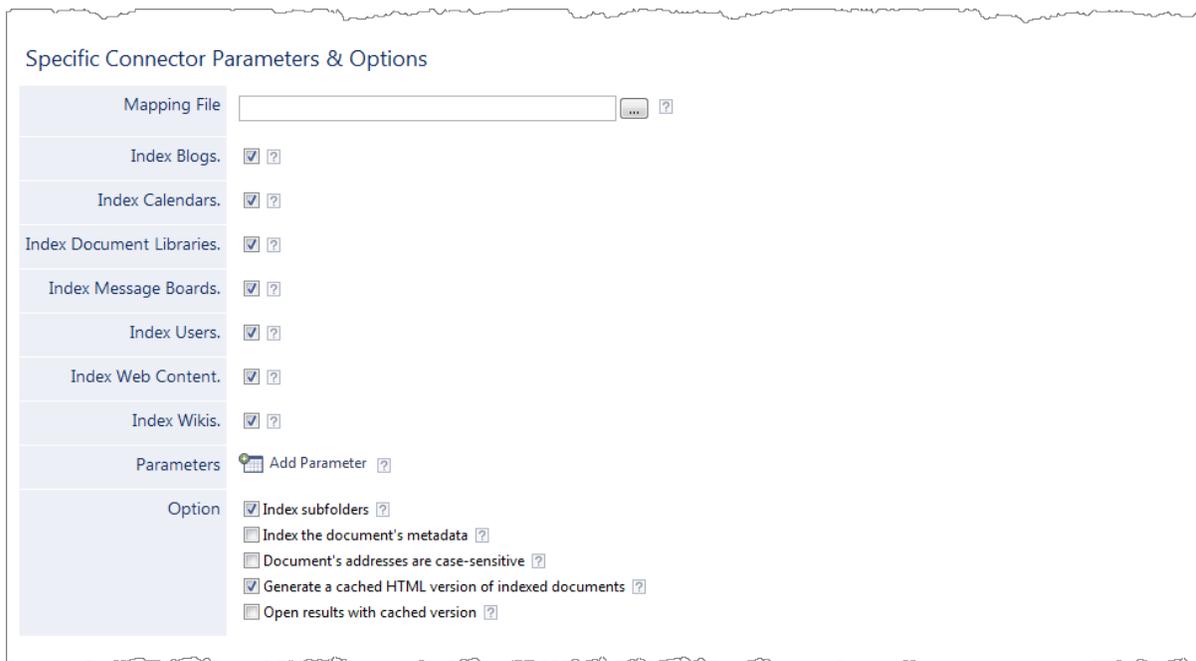If you defined a custom document type set for this source, select it.

Active Languages

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

Fields

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

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

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

Mapping File

Leave this field empty to use the default mapping file (see "About the Liferay Connector Mapping File" on page 23). When you create a custom mapping file, enter the absolute full path pointing to your file (see "Customizing the Liferay Connector Mapping File" on page 24).

Example: `C:\CES7\Config\MyLiferayMappingFile.xml`

Index Blogs

Whether blog entries, including their comments, should be indexed.

Index Calendars

Whether calendar events, including their comments, should be indexed.

Index Document Libraries

Whether document library files, including their comments, should be indexed.

Index Message Boards

Whether message board messages, including their attachments, should be indexed.

Index Users

Whether user profiles should be indexed.

Index Web Content

Whether web content, previously known as journals, should be indexed.

Index Wikis

Whether Wiki pages, including their attachments and comments, should be indexed.

Authentication

Select the user identity that you created previously for the Liferay portal.

Parameters

Click **Add Parameter** when you want to show advanced source parameters (see "Modifying Hidden Liferay Source Parameters" on page 25).

CES 7.0.8047+ (December 2015) When you crawl a Liferay 6.1 instance, you must add the `PluginUrl` hidden parameter:

Parameter name	Parameter value example
PluginUrl	`[LiferayServer:Port]/CESLiferayConnector-portlet/api/axis/Plugin_ CES_LiferayConnectorService`

In the **Option** section:

Index Subfolders

Keep this check box selected (recommended). By doing so, all subfolders from the specified portal address are indexed.

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 the 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.

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:
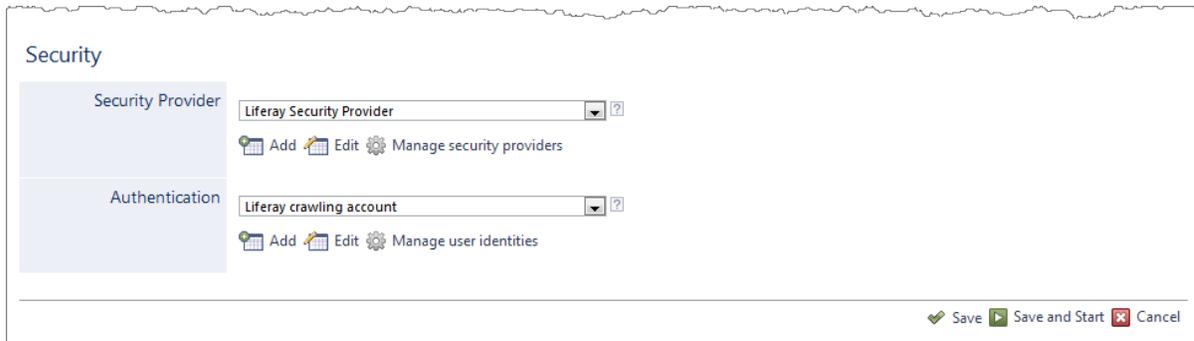
a. In the **Security Provider** drop-down list, select the security provider that you created for this source (see "Configuring a Liferay Security Provider" on page 16).

b. In the **Authentication** drop-down list, select the user identity that you created for the Liferay Portal.

c. Click **Save and Start** to save the source configuration and start indexing this source.

8. 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.

Add the built-in the Liferay facet to your search interface (see "Managing Built-in Facets and Related Results Appearing in a .NET Search Interface" on page 31).

6.4 About the Liferay Connector Mapping File

The Liferay connector mapping file determines exactly which Liferay entities are indexed, what metadata is retrieved, and where this information is added in the Coveo unified index. The default mapping file (`[CES_Path]\bin\Coveo.CES.CustomCrawlers.Liferay.DefaultMappingFile.xml`) is automatically used when no mapping file is specified in the source.

The default mapping file specifies to index the following Liferay default entity types:

- Attachment

- BlogEntry

- CalendarEvent

- Comment

- DocumentLibraryFile

- MessageBoardMessage

- User

- WebContentLocalized

- WikiPage

The mapping file is an XML file that contains various sections and subsections. The root element is `<LiferayMapping>`. It contains various `<Mapping>` nodes, each defining one entity type to be indexed with the corresponding metadata.

> **Example:** The following mapping element specifies to index the `BlogEntry` entity type.
>
> ```
> <Mapping type="BlogEntry">
>     <Fields>
>       <Title>%[title]</Title>
>       <Body>%[content]</Body>
>       <ClickableUri>%[coveo_url]</ClickableUri>
>       <ModifiedDateUtc>%[coveo_lastModifiedDate]</ModifiedDateUtc>
>       <CustomFields>
>         <CustomField name="sysauthor">%[userName]</CustomField>
>         <CustomField name="sysparents">%[coveo_breadcrumbs]</CustomField>
>       </CustomFields>
>     </Fields>
>   </Mapping>
> ```

A `<Mapping type="Default">` element applies to all retrieved items that do not have their own specific mapping element. Such an element exists but is commented out in the default mapping file.

> **Note:** You can create and use a custom mapping file to fine-tune the Liferay indexed content (see "Customizing the Liferay Connector Mapping File" on page 24).

6.5 Customizing the Liferay Connector Mapping File

The Coveo connector for Liferay portals comes with a default mapping file that makes the connector ready to index the default Liferay entities (see "About the Liferay Connector Mapping File" on page 23).

You can customize the mapping file to fine-tune the indexed content or to include other Liferay entities.

To customize the mapping file

1. Using an administrator account, connect to the Coveo Master server.

2. Using a text editor:

   a. Open the default mapping file: `[CES_Path]\bin\Coveo.CES.CustomCrawlers.Liferay.DefaultMappingFile.xml`

      > **Example:** With the default installation path: `C:\Program Files\Coveo Enterprise Search 7\Bin\Coveo.CES.CustomCrawlers.Liferay.DefaultMappingFile.xml`

   b. Save the file using a name of your choice in the `[Index_Path]\Config\` folder.

      > **Example:** With the default index path: `C:\CES7\Config\MyLiferayMappingFile.xml`

c. Respecting the mapping file format (see "About the Liferay Connector Mapping File" on page 23), customize the file. Use the `CustomFields` section to directly reference columns present on a Liferay entity.

d. Save your changes.

What's Next?

Specify your customized mapping file in your Liferay source (see "Configuring and Indexing a Liferay Source" on page 18).

6.6 Modifying Hidden Liferay 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 Liferay 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 Liferay sources. The parameter type (integer, string,…) appears between parentheses following the parameter name.

PluginUrl (String) CES 7.0.8047+ (December 2015)

(For Liferay 6.1 only) The URL of the Coveo Liferay 6.1 plugin. The default value is `null`.

Example: `[[LiferayServer:Port]]/CESLiferayConnector-portlet/api/axis/Plugin_CES_ LiferayConnectorService`

WebServiceBatchSize (Integer)

Number of items to fetch per request made to the Liferay portal. The default value is `300`. The minimum value is `1`. A small value forces the connector to make small but frequent queries to Liferay. A larger value leads to larger and less frequent queries.

CacheLifeSpan (Integer) OBSOLETE CES 7.0.8047– (December 2015)

The connector keeps a local cache of all the Liferay users. This way the connector doesn't have to retrieve all users from Liferay on every full or Incremental refresh run. This parameter controls the amount of time (in minutes) this user cache will remain valid. When this delay expires, all users will be fetched again, instead of being taken out of the cache. The default value is `480` minutes (8 hours).

The amount of time (in minutes) the user cache that exists within the crawler lives. When this delay expires, all users will be fetched again, instead of being taken out of the cache. The default value is `480` minutes (8 hours).

BlogPortletId (String)
CalendarPortletId (String)
DocumentLibraryPortletId (String)
MessageBoardPortletId (String)
WikiPortletId (String)

These parameters tell the connector what is the ID of the portlet to use when creating clickable URIs for the

different types of items. You must set these parameters only if your Liferay portal does not use the default values.

Example: `BlogPortletId` determines which portlet is used to present blogs. The default ID value is `33` for this portlet.

Note: You can find this information in the Liferay Control Panel. Under **Portal**, click **Plugins Configuration**. In the list of plugins that appears, click the desired plugin to see its information, including the **Plugin ID** (the information you must put in these parameters).

Languages (String)

The comma-separated list of languages to consider when retrieving Web Content. One item is returned per language. The parameter is empty by default and considers only the default portal language. Enter a `*` to specify all languages.

Example: `en_US,fr_FR,de_DE,it_IT,ja_JP,es_ES`

Note: You can find possible languages in the Liferay Control Panel. Under **Portal**, click **Portal Settings**. In the menu on the right, click **Display Settings**. Look in the **Available Languages** field for possible values.

SiteMinderFormLoginAction (String)

This parameter, along with the `SiteMinderFormLoginPage` parameter, is only required when Liferay resides inside a SiteMinder secure realm. These parameters enable the connector to authenticate with SiteMinder in order to gain access to the Liferay server so it can retrieve the content to index. This parameter contains the `POST` action that will be sent to the SiteMinder authentication form (`login.fcc`).

Example:
`USER=username&PASSWORD=password&SMAUTHREASON=0&TARGET=https%3a%2f%2fliferayportal`

Note: The `POST` action contains four parameters: `USER`, `PASSWORD`, `SMAUTHREASON`, and `TARGET`. `USER` and `PASSWORD` are the credentials to authenticate to SiteMinder. `SMAUTHREASON` is always equal to zero. The `TARGET` parameter is the secure resource you want to access, in this case the Liferay portal URL (`https://liferayportal`), and must be properly escaped.

SiteMinderFormLoginPage (String)

This parameter is the URL of the SiteMinder authentication form (`login.fcc`).

Example: `https://www.acme.com/siteminderagent/forms/login.fcc`

Note: Ask your SiteMinder administrator for the URL of the authentication form.

NumberOfRefreshThreads (Integer)

This determines the number of threads that simultaneously crawl the Liferay portal. The default value is `2`.

WebId (String)

This parameter determines which company to index. A company is associated with a WebId.

> **Note:** You can find this ID in the Liferay **Control Panel**. Under **Server**, click **Portal Instances**, and then **Web Id**. There is a maximum of 1 ID per source. The default value is an empty string, which corresponds to the first WebId encountered.

Use the following procedure only when you want to modify one or more of the above hidden source parameters.

To modify hidden Liferay source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 27 to add one or more Liferay hidden source parameters.

2. For a new Liferay 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 Liferay 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 Liferay 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 Liferay source to apply the changes to the parameters.

6.6.1 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:

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.

7. Managing Built-in Facets and Related Results Appearing in a .NET Search Interface

The Coveo .NET Front-End comes with a number of built-in facets and Related Results defined for various .NET search interfaces. You can modify which built-in facets and Related Results appear in each .NET search interface.

Important: The Related Results information is passed through the .NET search interface URL. When you add a few Related Results panels to a .NET search interface, the search interface URL can easily exceed the Internet Explorer URL length limit. Use the URL shortener feature to eliminate this issue.

To manage the built-in facets and Related Results appearing in a .NET search interface

1. Access the Coveo .NET Front-End Interface Editor.

2. Select the **Search Interfaces** tab.

3. On the menu bar:

   a. In the **Current Interface** drop-down list, select the search interface that you want to modify.

   b. Click the **Features** menu.

4. In the navigation panel on the left, click **Facets and Related Results**.

   In the panel on the right:

   - The facets and Related Results panels currently appearing in the selected search interface are listed under **Facets and Related Results** in the order that they appear in each of the facet and Related Results zones (**Hub default position**, **Right**, **Top** or **Left**).

   - The available built-in facets are listed under **Built-in Facets**. Several built-in facets based on system fields are applicable to content from any repository. Other facets are exclusive to the content of a specific type of repository.

     Examples: The **Author** facet is applicable to the content of any repository for which the `sysauthor` system field was populated. The **Liferay Type** facet is only applicable to Liferay content.

   - The available built-in Related Results are listed under **Built-in Related Results**.

5. You can perform one the following operations:

- Add a built-in facet to the search interface:

  In the **Built-in Facets** list, click the **Add "[FacetName]"** link corresponding to the facet that you want to add.

  > **Note:** For the **Type** facet, the default list of **Allowed Values** (facet items) is the following:
  > `audio,doc,html,image,mapimail,mime,mpp,msg,one,pdf,ppt,rtf,txt,video,wp,xls,zip.`
  >
  > If you want the **Type** facet to show other file types as facet items, simply add the needed file types to the default list in the **Allowed Values** parameter box.

  > **Example:**
  > `audio,doc,html,image,mapimail,mime,mpp,msg,one,pdf,ppt,rtf,txt,video,wp,xls,zip`
  > `,vsd`

  The corresponding facet appears at the end of the **Facets and Related Results** list.

- Add a built-in Related Results panel to the search interface:

  In the **Built-in Related Results** list, click the **Add "[RelatedResultsName]"** link corresponding to the Related Results panel that you want to add.

  The corresponding Related Results appears at the end of the **Facets and Related Results** list.

- Remove a facet or Related Results from the search interface:

  - In the **Facets and Related Results** list, select the check box of one or more facets or Related Results that you want to remove.

  - Click **Delete** (above the **Built-in Facets** list).

  - Click **Yes** when prompted to confirm the delete operation.

- Change the order in which facets and Related Results appear in the search interface:

  In the **Custom Facets** list:

  a. On the line corresponding to the facet or Related Results that you want to reorder, click **Up** or **Down** as many times as needed to relocate the facet or Related Results in relation with the others in the same zone.

  b. Repeat for each facet or Related Results that you want to reorder.

  > **Note:** When the position of a facet or a Related Results panel is **Default**, the position is inherited from the search interface or search hub default position.

6. Access and refresh the search interface, and then validate that the built-in facet and Related Results changes are as desired.