

# Coveo Enterprise Search 6.0

## Confluence Connector

Coveo's *Confluence* connector allows users to index the content of a *Confluence Wiki* site or space. By using an administrative account, the content of the site or space can be indexed, including *Confluence* wiki pages, news items, comments and attachments.

### Features

The *Confluence* connector can be used to index *Confluence Wiki* sites and spaces. It allows *Coveo Enterprise Search (CES)* to crawl and index the content of a *Confluence Enterprise Wiki 2.x* installation using the *Confluence SOAP remote API (Web service)*. The following details the features available in the *Confluence* connector:

- Extraction and indexing of all *Confluence* types:
  - Spaces;
  - Wiki pages;
  - News items (blog posts);
  - Comments;
  - Attachments (binary documents).
- Extraction and indexing of document permissions (supports LDAP integrations).
- Extraction and indexing of labels.
- Enhanced search including:
  - Bread crumbs;
  - Quick view;
  - Query refinement using:
    - Spaces;
    - Object types (Page, Comment, etc.);
    - Labels.

### Limitations

The *Confluence* connector does not support live indexing. A source refresh is required in order to update the source content.

### Requirements

The *Confluence* connector requires the *Confluence SOAP remote API (Web service)* to be enabled on your *Confluence* server. For more information, refer to:

<http://confluence.atlassian.com/display/DOC/Enabling+Remote+APIs>.

The *Confluence* connector allows anonymous crawling; however, if your *Confluence* server does not allow anonymous users to access the *SOAP remote API* or you want to crawl using a specific *Confluence* user, you must create a user identity and setup your *Confluence* source to use this user identity. For more information, refer to [How to Configure a User Identity \(optional\)](#).



To index the document permissions, the *Confluence* connector requires a valid database connection string in order to retrieve the security information from the *Confluence* database. Also, it is important to configure a security provider as well as your *Confluence* source in order to use the security provider. For more information, refer to [How to Configure a Security Provider \(optional\)](#).

If your *Confluence* server has a LDAP integration, the *Confluence* connector must also connect to the LDAP servers to extract the information of the LDAP members and to retrieve the members of LDAP groups. For more information concerning the *Confluence* LDAP integration, refer to: <http://confluence.atlassian.com/display/DOC/Add+LDAP+Integration>. The LDAP connection settings will be automatically extracted from the *Confluence* LDAP configuration file (*atlassian-user.xml*); hence, you only have to specify the path to this file using the *LDAPConfigFilePath* parameter and the *Confluence* connector will connect to your LDAP servers.

## Configuration

### ▶ How to Add a User Identity (optional)


To add a user identity, perform the following procedure:

1. In the Administration Tool, access the **Administrators** page (Configuration > Security).
2. In the left navigation pane, click **User Identities**. The **User Identities** page is displayed.
3. Click  **Add**. The **Modify User Identity** page is displayed.
4. In the **Name**, **User** and **Password** fields, enter the credentials of the user login account.
5. Click  **Save**.

<b>Name</b>	<input type="text" value="Confluence Admin"/>
<b>User</b>	<input type="text" value="Admin"/>
<b>Password</b>	<input type="password" value="••••••"/>
<b>Option</b>	<input type="checkbox"/> Support basic authentication
<b>Client certificate</b>	<input type="checkbox"/> Use client certificate
<b>Store</b>	<input type="text" value="Personal"/>
<b>Certificate</b>	<input type="text"/>
<b>Used By</b>	

### ▶ How to Configure a Security Provider (optional)

**Note:** This procedure is required to index the *Confluence* documents permissions.

1. In the Administration Tool, access the **Administrators** page (Configuration > Security).
2. In the left navigation pane, click **Security Providers**. The **Security Providers** page is displayed.
3. Click  **Add** to create a new security provider.
4. Enter the following information in the appropriate fields:





Field	Description
Name	Confluence Security Provider (or any significant name)
DLL Path	<Drive_Letter>:\Program Files\Coveo Enterprise Search x\Bin\Coveo.CES.CustomCrawlersSecurityProvider.dll
User Identity	Optional. Must be set if your <i>Confluence</i> site does not allow anonymous users to access the <i>SOAP remote API</i> .
Parameters	<b>AssemblyPath</b> ="<Drive_Letter>:\Program Files\Coveo Enterprise Search x\Bin\Coveo.CES.CustomCrawlers.Confluence.dll"; <b>WebServiceUrl</b> ="http://MyConfluenceServer:8080/"; <b>DBConnectionString</b> ="server=MyServer;database=MyDatabase;User=MyUser;Password=MyPassword"; <b>DBDriverType</b> ="SqlClient"; <b>LDAPConfigFilePath</b> ="\\server\c\$\confluence\WEB-INF\classes\atlassian-user.xml"
Options	Select the following checkboxes: <b>Support access list</b> , <b>Support expand group</b> and <b>Support expand user</b> .

5. Click  Save .

This table displays all the available parameters for a *Confluence* security provider:

Parameter	Required	Def. Value	Description
DBConnectionString	Yes		String to connect to the <i>Confluence</i> database.
DBDriverType	Yes		Driver type to use to connect to the <i>Confluence</i> database: <b>SqlClient</b> , <b>OleDb</b> or <b>Odbc</b> .
LDAPConfigFilePath	Yes*		Path of the <i>Confluence</i> LDAP configuration file ( <i>atlassian-user.xml</i> ). For example, <a href="http://server/c\$/confluence/WEB-INF/classes/atlassian-user.xml">\\server\c\$\confluence\WEB-INF\classes\atlassian-user.xml</a>
TimeToLive	No	300000	Number of milliseconds before refreshing the cache of members.
UserManagementFramework	No	Default	<i>Confluence</i> user management framework to use: <b>Default</b> , <b>AtlassianUser</b> or <b>OSUser</b> . For more information on <i>Confluence</i> user management, refer to: <a href="http://confluence.atlassian.com/display/DOC/Understanding+User+Management+in+Confluence">http://confluence.atlassian.com/display/DOC/Understanding+User+Management+in+Confluence</a>
WebServiceConnectionTimeout	No	30000	Maximum number of milliseconds a Web service call should wait.
WebServiceUrl	Yes		Address of your <i>Confluence</i> site. For example, <a href="http://MyConfluenceServer:8080/">http://MyConfluenceServer:8080/</a>


\* This parameter is required only if your *Confluence* server has a LDAP integration.

<b>Name</b>	<input type="text" value="Confluence Security Provider"/>
<b>DLL Path</b>	<input type="text" value="C:\Program Files\Coveo Enterprise Search 6\Bin\Co"/>
<b>User Identity</b>	<input type="text" value="Confluence Admin"/>  Add  Edit  Manage user identities
<b>Parameters</b>	<input type="text" value='AssemblyPath="C:\Program Files\Coveo Enterprise :'/>
<b>SAML Redirection URI</b>	<input type="text"/>
<b>SAML Artifact Resolver URI</b>	<input type="text"/>
<b>SAML Logout URI</b>	<input type="text"/>
<b>SAML Signature Certificate File Name</b>	<input type="text"/>
<b>SAML Signature Certificate Password</b>	<input type="text"/>
<b>SAML Artifact Argument Name</b>	<input type="text" value="SAMLart"/>
<b>SAML Post Response Argument Name</b>	<input type="text" value="SAMLResponse"/>
<b>SAML Back Target Argument Name</b>	<input type="text" value="TARGET"/>
<b>Authorization Cache Timeout</b>	<input type="text" value="3600"/>
<b>Authentication Cookie Expiration</b>	<input type="text" value="1"/> 
<b>Option</b>	<input type="checkbox"/> Do not block exceptions <input type="checkbox"/> Require authorization <input checked="" type="checkbox"/> Support access list <input checked="" type="checkbox"/> Support expand group <input checked="" type="checkbox"/> Support expand user <input type="checkbox"/> Run in 64 bits

▶ **How to Create a Confluence Source**

A *Confluence* source can target an entire *Confluence* site or specific *Confluence* spaces, depending on what must be indexed. To create a new *Confluence* source, perform the following procedure:

In the Administration Tool, access the **Sources and Collections** page (Index> Sources and Collections).

1. In the **Sources** section, click  **Add**. The **Add Source** page is displayed.
2. Enter the appropriate values of the selected *Confluence* site:

Field	Description	Required	Example
Name	Any descriptive name	Yes	My Confluence Server
Source Type	The connector used by this source.	Yes	Confluence
Addresses	List of starting points for the connector, one address per line.	Yes	To index a complete <i>Confluence</i> site, use the <i>Confluence</i> server root URL as the starting address. For example, <a href="http://MyConfluenceServer:8080/">http://MyConfluenceServer:8080/</a> To index specific spaces, add their URL as starting addresses. For example, <a href="http://MyConfluenceServer:8080/display/space1">http://MyConfluenceServer:8080/display/space1</a> <a href="http://MyConfluenceServer:8080/display/space2">http://MyConfluenceServer:8080/display/space2</a> To index document permissions, all your starting points must be located on a single <i>Confluence</i> site.
Authentication User identity	Use the previously created user identity.	No	Confluence Admin

3. Click  Save.

**Name**  ?

**Source Type**

**Addresses**


Depends on the additional connector used.  
One entry per line.

**Rating**  ?

**Document Types**  ?

**Fields**  ?

**Refresh Schedule**  ?



**Parameters**  Add Parameter ?

**Option**

- Index subfolders ?
- Index the document's metadata ?
- Document's addresses are case-sensitive ?
- Generate a cached HTML version of indexed documents
- Open results with cached version ?

**Authentication** User Identity

If you **do not** want to index the *Confluence* document permissions, it is important to manually specify which users should have access to the *Confluence* documents when performing queries. To do so, perform the following procedure:



1. In the Administration Tool, access the **Sources and Collections** page (Index > Sources and Collections).
2. In the **Collections** section, select the appropriate collection.
3. In the **Sources** section, select the **Confluence** source.
4. In the left navigation pane, click **Permissions**.
5. In the **Permissions** section, select **Specifies the security permissions to index**.
6. Select **everyone** from the **Allowed Users** list box and click  **Delete**.
7. Add specific users or groups using the **Allowed Users** list box.
8. Click  **Apply Changes**.

**Permissions**



- Index security permissions
- Specifies the security permissions to index
- Index security permissions and specify additional security permissions to index
- Use a security provider

**Allowed Users**

everyone

 **Add**  **Remove**


**Denied Users**

 **Add**  **Remove**

If you want to index the document permissions, it is important to:

- o Specify the security provider to use;
- o Add these two mandatory source parameters: **DBConnectionString** and **DBDriverType**. If your *Confluence* server has a LDAP integration, you must also add this source parameter: **LDAPConfigFilePath**.

To specify the security provider to use, perform the following procedure:

1. In the Administration Tool, access the **Sources and Collections** page (Index > Sources and Collections).
2. In the **Collections** section, select the appropriate collection.
3. In the **Sources** section, select the **Confluence** source.
4. In the left navigation pane, click **Permissions**.
5. In the **Permissions** section, select **Use a security provider**. If this option is not available, refer to [How to Configure a Security Provider \(optional\)](#) to create a security provider.
6. In the **Security Provider** section, select a security provider from the list.
7. Click  **Apply Changes**.

- Permissions**
- Index security permissions
  - Specifies the security permissions to index
  - Index security permissions and specify additional security permissions to index
  - Use a security provider

**Security Provider**

Follow this procedure to add source parameters:

1. In the Administration Tool, access the **Sources and Collections** page (Index > Sources and Collections).
2. In the **Collections** section, select the appropriate collection.
3. In the **Sources** section, select the **Confluence** source.
4. In the left navigation pane, click **General**.
5. In the **Parameters** section, click **Add Parameter**.
6. Enter the parameter name and value.
7. Click **Apply Changes**.

Parameters	Name	Value	
	<input type="text"/>	<input type="text"/>	Delete
	<b>Add Parameter</b>		

This table displays all the available parameters for a *Confluence* source:

Parameter	Required	Def. Value	Description
DBConnectionString	Yes*		String to connect to the <i>Confluence</i> database.
DBDriverType	Yes*		Driver type to use to connect to the <i>Confluence</i> database: <b>SqlClient</b> , <b>OleDb</b> or <b>Odbc</b> .
LDAPConfigFilePath	Yes*		Path of the <i>Confluence</i> LDAP configuration file ( <i>atlassian-user.xml</i> ). For example, <a href="#">\\server\c\$\confluence\WEB-INF\classes\atlassian-user.xml</a>
UserManagementFramework	No	Default	<i>Confluence</i> user management framework to use: <b>Default</b> , <b>AtlassianUser</b> or <b>OSUser</b> . For more information on <i>Confluence</i> user management, refer to: <a href="http://confluence.atlassian.com/display/DOC/Understanding+User+Management+in+Confluence">http://confluence.atlassian.com/display/DOC/Understanding+User+Management+in+Confluence</a>
WebServiceConnectionRetryCount	No	3	Maximum number of retries to perform when a Web service call fails.
WebServiceConnectionRetryDelay	No	30000	Number of milliseconds to wait before retrying when a Web service call fails.
WebServiceConnectionTimeout	No	30000	Maximum number of milliseconds a Web service call should wait.

\* These three parameters are required only to index document permissions. Furthermore, the *LDAPConfigFilePath* parameter is required only if your *Confluence* server has a LDAP integration.

▶ **How to Configure the Search Interface**

In order to ensure a great search experience, it is recommended to add the *Confluence* specific search facets and display fields. To add the *Confluence* specific search facets, perform the following procedure:

1. From the *Windows Start* menu, access the **Interface Editor** (All Programs > Coveo Enterprise Search 6 > Interface Editor).
2. Click the name of the Search Interface to update (e.g. *Default*).
3. In the menu, click **Refine Fields**.
4. In the right navigation pane, click the three following built-in search refinements:
  - Add "Confluence Space"
  - Add "Confluence Type"
  - Add "Confluence Label"
5. Click **Close** from the top menu.

To add the *Confluence Labels* display field, perform the following steps:

1. From the *Windows Start* menu, access the Interface Editor (All Programs > Coveo Enterprise Search 6 > Interface Editor).
2. Click the name of the Search Interface to update (e.g. *Default*).
3. In the menu, click **Display Fields**.
4. Click **Add New**.
5. Enter the following information in the appropriate fields:

<b>Fields</b>	<b>Description</b>
Title	Confluence Labels
Field to Display	@sysclabels

6. Click **OK** and **Close** from the top menu.