Coveo Platform 7.0

Jive 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-130403-EN

Publication date: 1/3/2019

Table of Contents

1. Jive Connector

CES 7.0.5388+ (April 2013)

The Coveo connector for Jive 9 allows you to index and integrate the content of your Jive spaces and groups into your Coveo unified index, making it easily searchable by end-users.

Notes:

- Deprecated support versions: Jive 6, 7, and 8
- CES 7.0.8996+ (June 2017) Support for Jive 9.
- CES 7.0.8047+ (December 2015) Support for Jive 8.
- CES 7.0.7599+ (April 2015) Support for Jive 7.
- You can also index content from Jive 5, Jive SBS, or Clearspace using the Jive 5/SBS/Clearspace connector.

1.1 Connector Features Summary

Features	Supported	Additional information
Jive version	9 and Cloud	(For Jive Cloud only) Following available Jive Cloud releases
Searchable content types	✓	• Communities (also known as Spaces), social groups (also known as groups), projects, people and their profile, direct messages (requires Coveo plugin), documents (private and public), discussions (private and public), blog posts (for spaces, projects, users, groups and system blogs), announcements, polls, comments (for documents, blog posts, and polls), attachments (for documents, blog posts, and discussions), ideas (private and public), and videos (private and public). • Support phrase substitutions (requires Coveo plugin), tags, and categories.

Features		Supported	Additional information
Content update	Incremental refresh	✓	(Jive 8 and 9 only) Full refresh or rebuild needed to retrieve (due to Jive REST API limitations): • Comments on comments and replies on replies • Deleted file items. The Coveo plugin is required to: **Note:** The plugin cannot be installed in Jive Cloud. • Remove recently deleted Jive items • Properly refresh discussions
	Full refresh	✓	
	Rebuild	✓	
Document-level security		✓	• Requires the Coveo plugin for Jive on-premises instances. • Not supported for Jive Cloud. Permissions must be manually defined on the source. [more]

1.2 Features

- Content Indexing
  - Retrieval and indexing of the following Jive object types:
    - Spaces (also known as Communities)
    - Groups
    - Projects (with related Tasks and Checkpoints)
    - People and their profiles
    - Direct messages
    - Documents (private and public)
    - Discussions (private and public)
    - Blog posts (for spaces, projects, users, groups and system blogs)
    - Announcements
    - Polls
    - Comments (for documents, blog posts, and polls)
    - Attachments (for documents, blog posts, and discussions)

        - Ideas (private and public)
        - Videos (private and public)
    - Support for phrase substitution
    - Support for tags and categories
- Security

  The connector indexes the permissions on Jive objects. Consequently, Coveo search results only contain Jive objects that the end-user can access within the Jive communities. Permission indexing is done using an optional plugin.

  Note: You cannot install the Coveo plugin in Jive Cloud.

- Incremental refresh

  The connector periodically queries Jive for the latest edits, keeping the index content up-to-date.

  Notes:

  - CES 7.0.8691+ (December 2016) The incremental refresh takes account of deleted events (requires the Coveo plugin) (see "Installing the Coveo Plugin on Your Jive Server" on page 11).
  - CES 7.0.8541– (September 2016) A source full refresh or rebuild is required to remove deleted events from the index.
  - For Jive 8 (CES 7.0.8047+ (December 2015)) and 9 (CES 7.0.8996+ (June 2017)) spaces, due to a Jive REST API limitation, only the first level of comments on documents and replies on discussions are indexed by an incremental refresh, meaning that comments on comments and replies on replies cannot currently be retrieved unless performing a full refresh or source rebuild.
  - Since the Jive REST API does not provide the list of deleted File items, a source full refresh or rebuild is required to take the deletion of File items into account.

Feature history

CES version	Monthly release	Features
7.0.8996	June 2017	Support for Jive 9
7.0.8691	December 2016	Incremental refresh for events
7.0.8047	December 2015	Support for Jive 8
7.0.7599	April 2015	Support for Jive 7
7.0.6607	April 2014	Support for Jive Cloud (version 8)
7.0.5785	August 2013	Updated plugin to resolve incremental refresh issues
7.0.5388	April 2013	Connector introduction

What's Next?

Get familiar with the deployment steps (see "Jive Connector Deployment Overview" on page 5).

2. Jive Connector Deployment Overview

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

To deploy the Jive connector

1. Validate that your environment meets the requirements (see "Jive Connector Requirements" on page 7).

2. On the Jive server:

   a. Choose a Jive crawling account

      You must choose which Jive account the Coveo connector uses to crawl the content of your Jive communities (see "Creating a Jive Crawling Account" on page 8).

   b. Optionally install the Coveo for Jive plugin

      Install the Coveo plugin used by the connector on your Jive server. The plugin is optional but enables several connector features such as allowing to index permissions (see "Installing the Coveo Plugin on Your Jive Server" on page 11).

      Note: Because you cannot install the Coveo for Jive plugin in Jive cloud, Coveo cannot index permissions for this content.

      Tip: In rare cases where the Jive 6+ browse index is not synchronized with the master data, the Jive API may not return all documents to the Coveo connector. To prevent missing some Jive documents in your Coveo index, ensure that your Jive indexes are up to date (from the Jive Admin Console **System** > **Settings** > **Browse** > **Re-synchronize browse index**).

3. On the Coveo server:

   a. Create a user identity

      You must create a user identity to hold the credentials of the Jive crawling account that you selected.

   b. CES 7.0.7711+ (June 2015) Optionally create an email security provider

      When the primary email is defined for each of your users in Jive 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 Jive users to their email (see "Configuring an Email Security Provider" on page 33).

   c. Optionally create a Jive security provider

      When you installed the Coveo plugin and want to index Jive permissions, you must create a security provider that the connector uses to resolve indexed permissions into a list of Jive users and groups (see "Configuring a Jive Security Provider" on page 16).

   d. CES 7.0.8541+ (September 2016) Create a Jive field set

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

e. Create and index a source

   You must create a source describing the Jive community to index (see "Configuring and Indexing a Jive Source" on page 20).

4. Troubleshooting

   a. Review known issues (see "Troubleshooting Jive Connector Issues" on page 28).

   b. Consider modifying some hidden source parameters to try resolving other issues (see "Modifying Hidden Jive Source Parameters" on page 28).

5. Allow Jive users to be authenticated in a Coveo search interface

   When your Jive community is not integrated with Active Directory, your end-users need to sign in to Jive in a Coveo search interface to be able to see Jive content in search results. In this case, you need to add the Jive security provider to your search interface to allow end-user to sign in to Jive (see "Adding Security Providers to a .NET Search Interface" on page 35).

3. Jive Connector Requirements

Your environment must meet the following requirements to be able to use the Jive connector:

- Coveo license for the Jive connector

  Your Coveo license must include support for the Jive connector to be able to use this connector. You can see the currently supported connectors from the Administration Tool.

- CES 7.0.5388+ (April 2013)

- Jive product versions
  - Supported versions:
    - Jive Cloud (2015.2.2)

      The connector supports the cloud version of Jive, however because the optional Coveo plugin cannot be installed in this version of Jive, the plugin features such as indexing permissions are not available (see "Plugin Benefits" on page 11).

    - Jive 9 (CES 7.0.8996+ (June 2017))

      Note: The optional Coveo plugin can be installed on Jive-hosted and self-hosted instances.

  - Deprecated support versions: 6, 7, and 8

    Notes:

    - CES 7.0.7599+ (April 2015) Support for Jive 7.
    - The Jive 5/SBS/Clearspace connector supports previous versions of Jive.

What's Next?

Choose which Jive account the Coveo connector uses to crawl the content of your Jive communities (see "Creating a Jive Crawling Account" on page 8).

4. Creating a Jive Crawling Account

The Coveo connector needs a Jive account to be able to crawl the content of your Jive communities. The account must have access to the whole Jive content that you want to index. You can use an existing administrator account but the best practice is to create a dedicated user with **Full Access** permissions.

Example: When Jive users create private documents, the crawling account must have **Full Access** permissions to allow the crawler to see these documents and index their content and associated permissions so that the owners and users authorized to see the private documents can see them in search results.

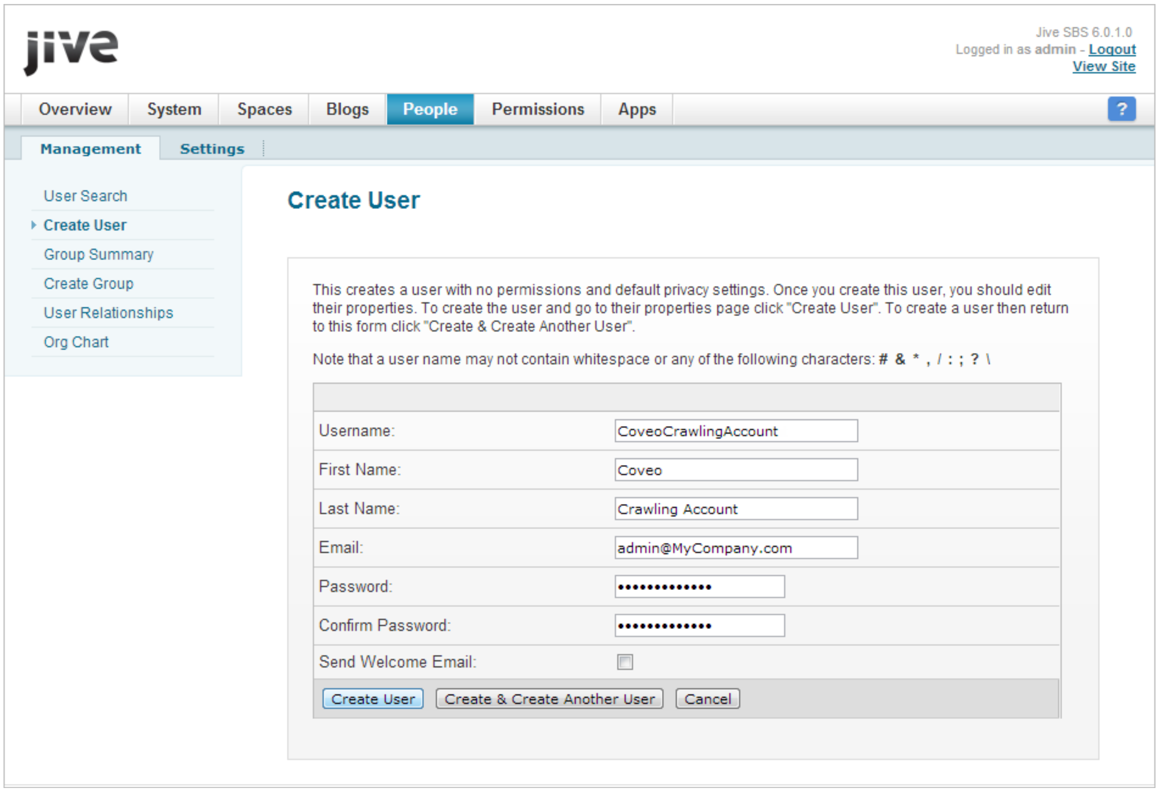
To create a Jive crawling account

1. Using an administrator account, with a browser, log in to the Jive Administration Console (`http://[MyJiveCommunity]/admin`).

2. When you want to create a dedicated crawling account:

   a. On the Jive Administration Console menu, select **People** > **Management** > **Create User**.

   b. In the **Create User** page, fill all the boxes to describing your crawling account, and then click **Create User**.



Create User

This creates a user with no permissions and default privacy settings. Once you create this user, you should edit their properties. To create the user and go to their properties page click "Create User". To create a user then return to this form click "Create & Create Another User".

Note that a user name may not contain whitespace or any of the following characters: **# & * , / : ; ? **

Username:	CoveoCrawlingAccount
First Name:	Coveo
Last Name:	Crawling Account
Email:	admin@MyCompany.com
Password:	•••••••••••••
Confirm Password:	•••••••••••••
Send Welcome Email:	□

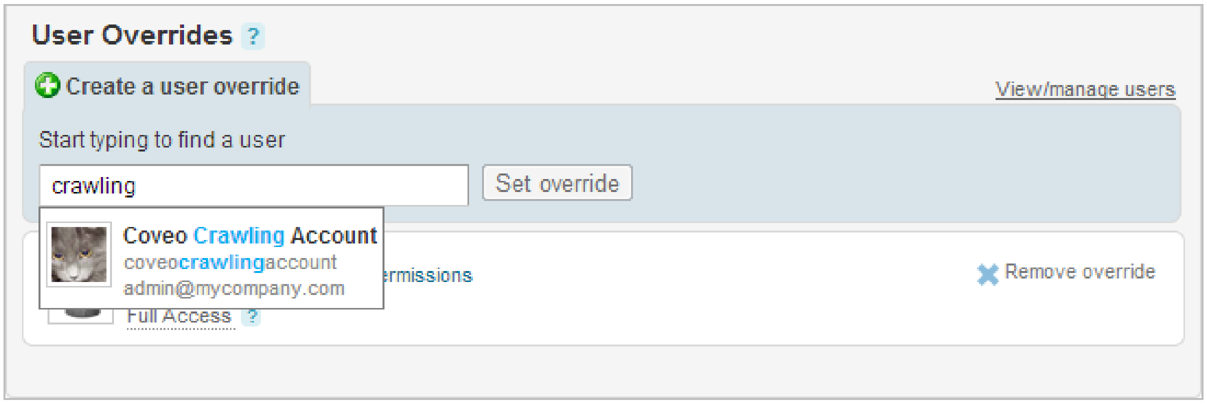
   c. At the bottom of the **User Summary** page, click **Save**.

3. On the Jive Administration Console menu, select **Permissions** > **System Administration**.

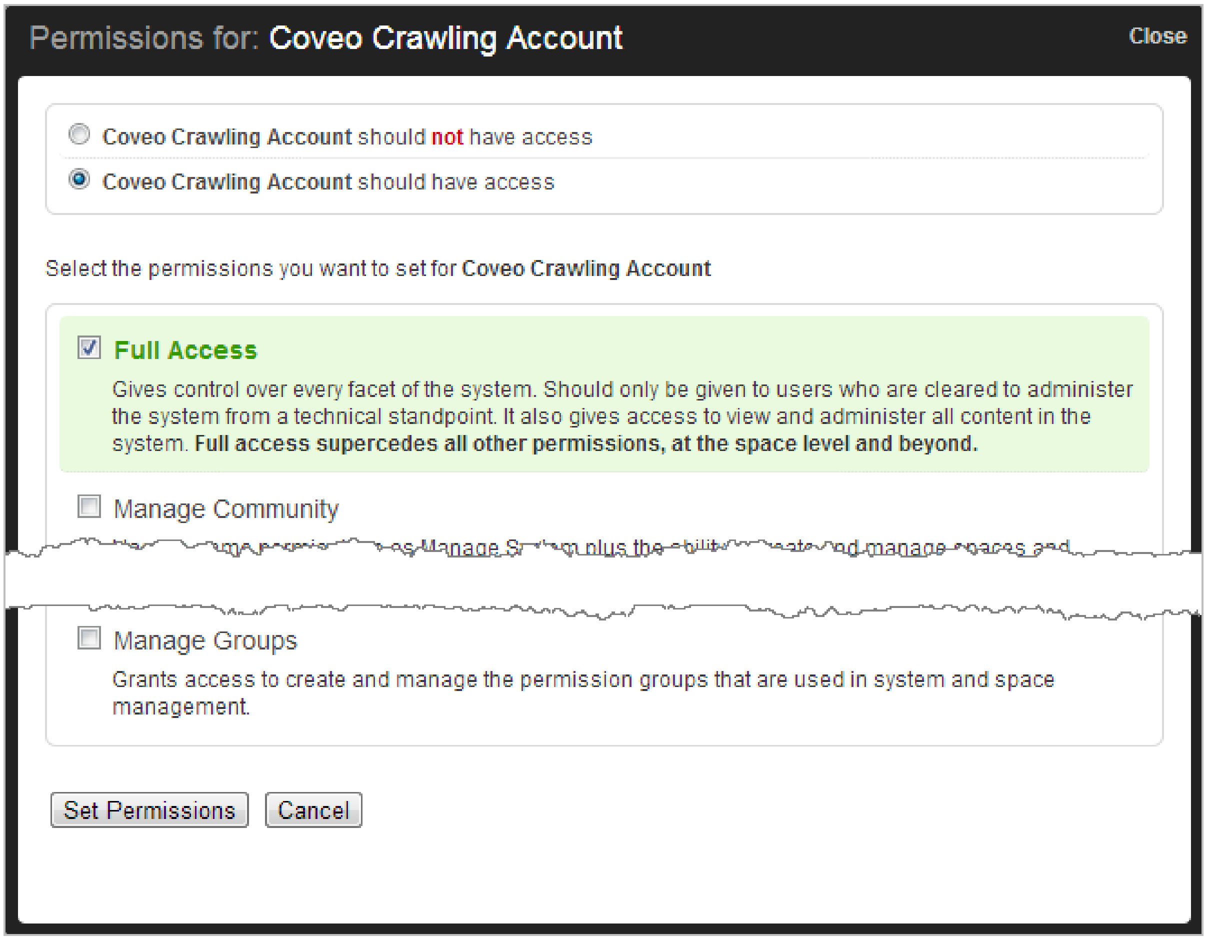
4. In the **System Administration Permissions** page, in the **Start typing to find a user** box, type the name of your

new or existing crawling account, select it, and then click **Set override**.

Note: Since the Jive REST API is not SSO-enabled, when your Jive instance is implemented with SSO, the crawling user you select must be a non-federated account (not an Active Directory user). Since it is not possible to authenticate against the REST API as a federated user, selecting such a user as the crawling account will return 401 status code errors. If the crawling account has already been set up as federated and changed to non-federated, the user has to be deleted and recreated (see 401 Unauthorized on .NET calls to v3 API).



5. In the **Permissions for** page, select the **Full Access** check box, and then click **Set Permissions**.



○ Coveo Crawling Account should **not** have access

● Coveo Crawling Account should have access

Select the permissions you want to set for **Coveo Crawling Account**

☑ **Full Access**

Gives control over every facet of the system. Should only be given to users who are cleared to administer the system from a technical standpoint. It also gives access to view and administer all content in the system. **Full access supercedes all other permissions, at the space level and beyond.**

□ Manage Community

Has the same permissions as Manage System plus the ability to create and manage spaces and

□ Manage Groups

Grants access to create and manage the permission groups that are used in system and space management.

What's Next?

Optionally install the Coveo plugin used by the connector on your Jive server (see "Installing the Coveo Plugin on Your Jive Server" on page 11).

5. Installing the Coveo Plugin on Your Jive Server

The Jive connector comes with an optional Coveo plugin that you can install on your Jive server to allow the Jive connector to access Jive features that are not available through the regular Jive 6+ APIs.

Note: You cannot install the Coveo plugin in Jive Cloud.

Plugin Benefits

The Jive connector can work without the plugin, but using the plugin enables the following connector features:

- Indexing permissions
- Indexing direct messages
- Removing recently deleted Jive items from the index during an incremental refresh

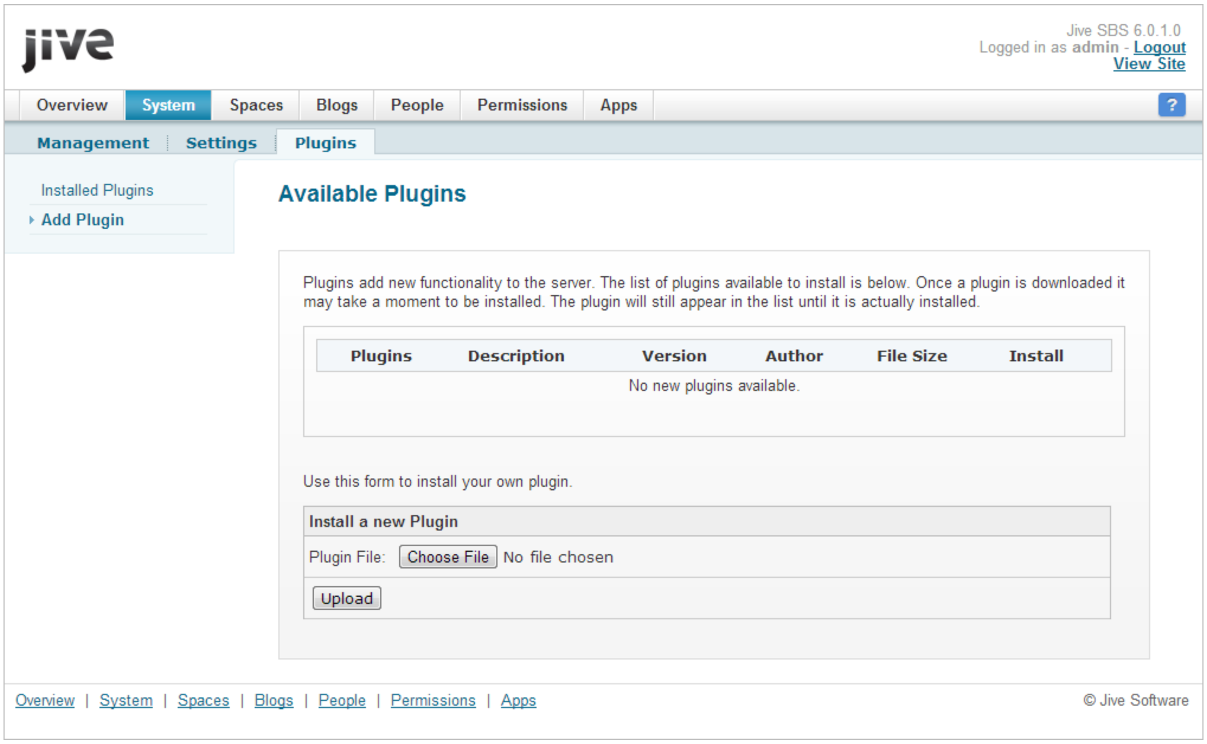
  Note: CES 7.0.8691+ (December 2016) Removal of deleted Jive events.

- Proper incremental refresh of discussions
- Phrase substitutions

Important: The plugin stores deleted item information on the Jive server in a database to allow incremental refresh to remove deleted items from the index. The items in this database are cleared after they are read by the crawler. If no source is set to crawl the Jive site, the plugin database will grow indefinitely.

To install the Coveo plugin on your Jive server

1. Using an administrator account, with a browser, log in to the Jive Administration Console (`http://[MyJiveCommunity]/admin`).
2. On the Jive Administration Console menu, select **System** > **Plugins** > **Add Plugin**.
3. In the **Available Plugins** page:



Jive SBS 6.0.1.0
Logged in as admin - Logout
View Site

Available Plugins

Plugins add new functionality to the server. The list of plugins available to install is below. Once a plugin is downloaded it may take a moment to be installed. The plugin will still appear in the list until it is actually installed.

Plugins	Description	Version	Author	File Size	Install
No new plugins available.					

Use this form to install your own plugin.

Install a new Plugin

Plugin File: Choose File No file chosen

Upload

Overview | System | Spaces | Blogs | People | Permissions | Apps
© Jive Software

a. Under **Install a new Plugin**, click **Choose File**.

b. Browse to the `[CES_Path]\Bin\` folder on the Coveo Master server and using the following table, select the `coveo-plugin-[Version]-for-jive[-6.0/8-1.0].jar` plugin file corresponding to your Jive installation.

Jive installation	Plugin file	Notes
Jive 8 and Jive 9	`coveo-plugin-for-jive-1.2.jar` CES 7.0.8996	
Jive 8	- `coveo-plugin-for-jive8-1.1.jar` CES 7.0 - `coveo-plugin-for-jive8-1.0.jar` CES 7.0	Supports incremental refresh of deleted events (v.8.1.1)
Jive 6.2+ and 7	- `coveo-plugin-1.5-for-jive.jar` CES 7.0. - `coveo-plugin-1.4-for-jive.jar` CES 7.0. - `coveo-plugin-1.3-for-jive.jar` CES 7.0. - `coveo-plugin-1.2-for-jive.jar` CES 7.0.	Supports incremental refresh of deleted events (v.1.5)
Jive 6.0 to 6.1	`coveo-plugin-1.1-for-jive-6.0.jar` CES 7.0	Resolves incremental refresh issues.

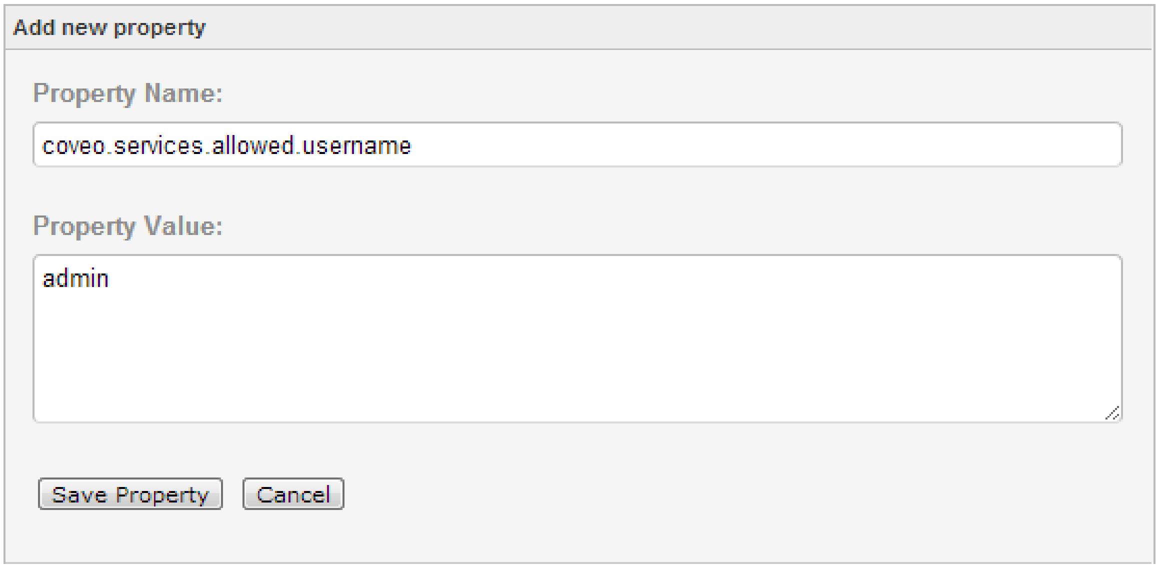
c. Click **Upload**.

4. Grant access to the Coveo plugin for the selected crawling account:

   Note: By default, for security reasons, no accounts can connect to the *Coveo for Jive* plugin.

   a. In the Administration Console, select **System** > **Management** > **System Properties**.

   b. At the bottom of the **System Properties** page, in the **Add new property** box:



Add new property

Property Name: coveo.services.allowed.username

Property Value: admin

   i. In the **Property Name** box, enter `coveo.services.allowed.username`.

   ii. In the **Property Value** box, enter the user name of the selected crawling account.

   iii. Click **Save Property**.

5. Stop and restart the Jive service (from the command prompt: `/etc/init.d/jive-application restart`).

What's Next?

Create a user identity to hold the credentials of the Jive crawling account that you selected.

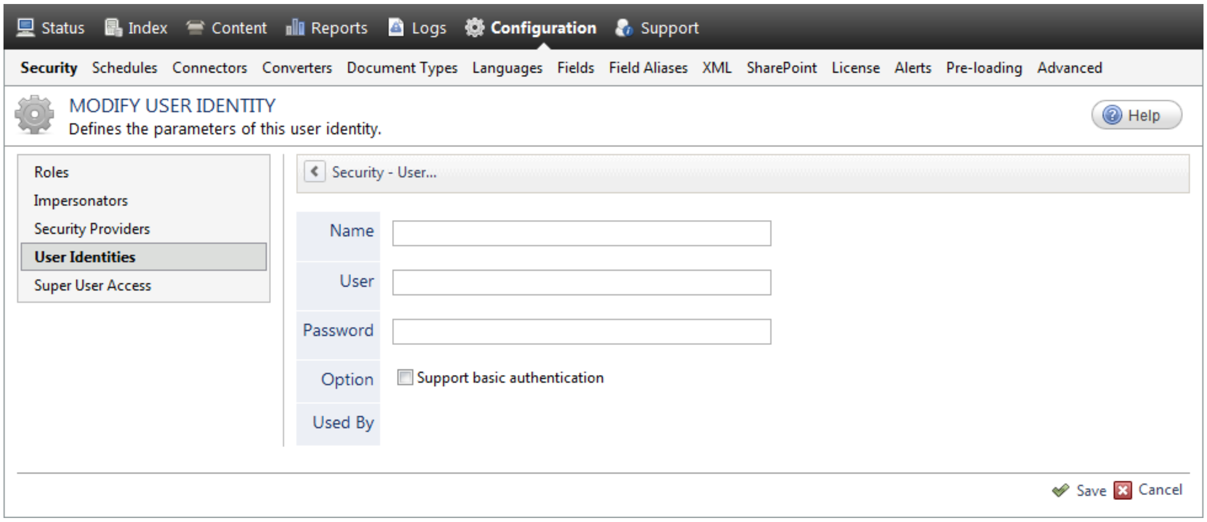
6. Adding a User Identity

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.

7. Configuring a Jive Security Provider

The Jive connector can index Jive 6+ permissions to ensure that in search results, users only see Jive content they are allowed to see directly in Jive.

When you choose to index permissions, the connector requires a security provider to resolve Jive user and group permissions and optionally to map them to Active Directory or Email identities.

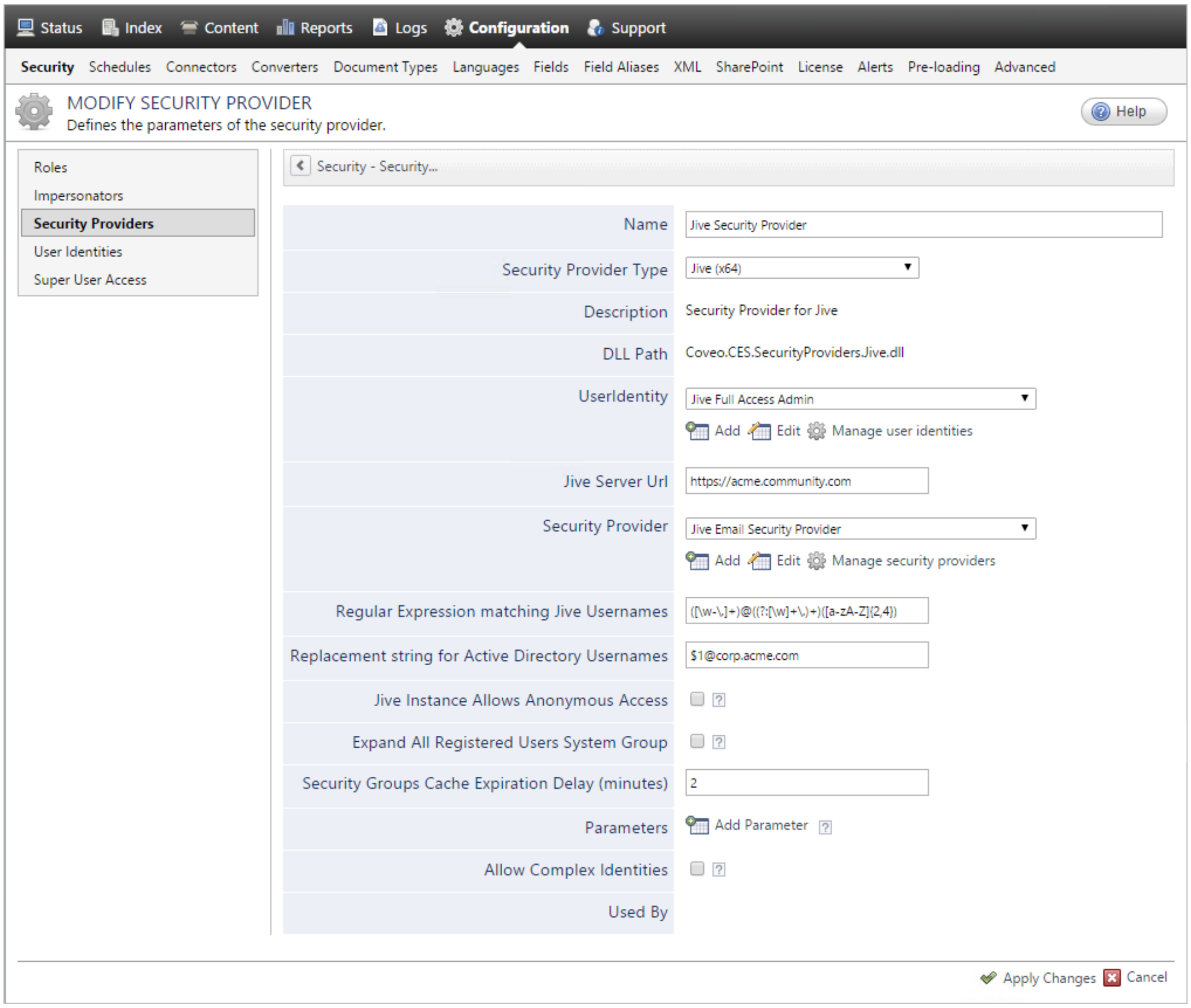
When you do not want to index permissions, skip this section.

Notes:

- The security provider requires the *Coveo for Jive* plugin to be installed on the Jive server. If not already done, install the plugin (see "Installing the Coveo Plugin on Your Jive Server" on page 11).
- You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.
- CES 7.0.7711+ (June 2015) Support for mapping Jive users to Email identities.

To configure a Jive security provider

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



MODIFY SECURITY PROVIDER

Defines the parameters of the security provider.

Name	Jive Security Provider
Security Provider Type	Jive (x64)
Description	Security Provider for Jive
DLL Path	Coveo.CES.SecurityProviders.Jive.dll
UserIdentity	Jive Full Access Admin
Jive Server Url	https://acme.community.com
Security Provider	Jive Email Security Provider
Regular Expression matching Jive Usernames	([\w-\.]+)@((?:[\w]+\.)+)([a-zA-Z]{2,4})
Replacement string for Active Directory Usernames	$1@corp.acme.com
Jive Instance Allows Anonymous Access	☐
Expand All Registered Users System Group	☐
Security Groups Cache Expiration Delay (minutes)	2
Parameters	
Allow Complex Identities	☐
Used By	

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

> **Example:** `Jive Security Provider`

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

> **Note:** You should not confuse the **Jive** security provider with the **Jive 5 / SBS / Clearspace** security provider that must be used with Jive versions older than Jive 6.0.

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. In the **Jive Server URL** box, enter your Jive server base address.

> **Example:** `http://acme.community.com`

e. Configure the identity type to which the Jive security provider maps Jive users depending on your CES version:

- CES 7.0.7711+ (June 2015) In the **Security Provider** drop-down list, optionally select another security provider to allow the Jive security provider to map Jive accounts to another user type with which people are authenticated when they perform a search:
    - Select **(none)** when you do not want to map Jive users to another user type.
    - When the Jive LDAP is synchronized with an Active Directory, select the out-of-the-box **Active Directory** security provider to map Jive users to AD users.
    - When a primary email is defined for all users in Jive and they are authenticated with this email when they perform a search in your CES search interface, select the Email security provider you previously created (see Jive Connector Deployment Overview).
- CES 7.0.7599– (April 2015)

    i. (Optional) Select the **Map Jive Users to Active Directory Users** check box when you want Microsoft Windows users to be able to see Jive content in search results without having to log in with their Jive credentials in the search interface.

    Clear this option when you want to allow Jive users to search for Jive secured documents in a non Microsoft Windows environment. In this case, you also need to add the security provider to your Jive search interface to allow users to log in to Jive in the search interface to be able to see Jive secured documents in search results .

    > **Note:** When this option is selected, permissions are stored in the index as Active Directory identities rather than as Jive identities.

    ii. When you select the **Map Jive Users to Active Directory Users** check box, in the **Security Provider for Jive User Mapping** section:

    A. In the drop-down list, select the **Active Directory** security provider that the Jive security provider will use to map Jive users and groups to Windows users and groups.

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

f. (Optional) When you select the **Active Directory** security provider (CES 7.0.7711+ (June 2015)) or when you select the **Map Jive Users to Active Directory Users** check box (CES 7.0.7599– (April 2015)) in the previous step, you must also configure the following two parameters that work together to build the Windows identity from the Jive identity (otherwise leave the default values):

A. In the **Regular Expression matching Jive Usernames** box, enter a regular expression that matches against Jive usernames. If you leave this box empty, the Windows identity will be a copy of the Jive identity.

> **Example:** The default value matches an email address and captures the part before the `@` character:
> `([\w-\.]+)@((?:[\w]+\.)+)([a-zA-Z]{2,4})`

B. In the **Replacement string for Active Directory Usernames** box, enter the pattern for Active

Directory identities using regular expression group substitutions in the `$[n]` form.

The string `$1` stands for the first group captured by the regular expression specified in the **Regular Expression matching Jive Usernames** box, while `$2`, `$3`, etc. stand for subsequent groups.

> **Example:** Your Jive and Windows identities are respectively in the `MyName@MyCompany.com` and `MyCompany\MyName` forms.
>
> Enter `$2\$1` in the **Replacement string for Active Directory Usernames** parameter to build the Windows identities with a regular expression such as `([\w-\.]+)@([\w]+)\.[a-zA-Z]{2,4}` in the **Regular Expression matching Jive Usernames** parameter.

g. CES 7.0.5556+ (June 2013) Select the **Jive Instance Allows Anonymous Access** option when you want to map the Jive `Everyone` user to the Active Directory `Everyone` user. This check box is cleared by default.

h. CES 7.0.8388+ (June 2016) Select the **Expand All Registered Users System Group** option when you want the security provider to treat the All Registered Users group in Jive as a security group that needs to be expanded. This check box is cleared by default, meaning that All Registered Users is considered as a well-known group (containing all users of a Jive space). Consider selecting the option when you assign the group in item permissions.

> **Note:** Selecting the option can impact the security cache performance if the number of group members increases rapidly.
>
> When the group contains thousands of users, it is recommended to set the `MaxAllowedTimeWithoutProgress` hidden parameter to a large value (ex: `600` seconds) [see Hidden Parameter Section]. The default value is `300` seconds.

i. In the **Security Group Cache Expiration Delay box**, leave the default value (`2` minutes) unless Coveo Support is instructing you to change it. This parameter sets the amount of idle time after which the crawler should flush its cache of security groups.

j. 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.

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

l. Click **Apply Changes**.

What's Next?

Configure and index a Jive source (see "Configuring and Indexing a Jive Source" on page 20).

8. Configuring and Indexing a Jive Source

A source defines a set of configuration parameters for a specific Jive 6+ server.

Note: In an environment with more than one Jive 6+ server, you need to define one source for each Jive server that you want to index.

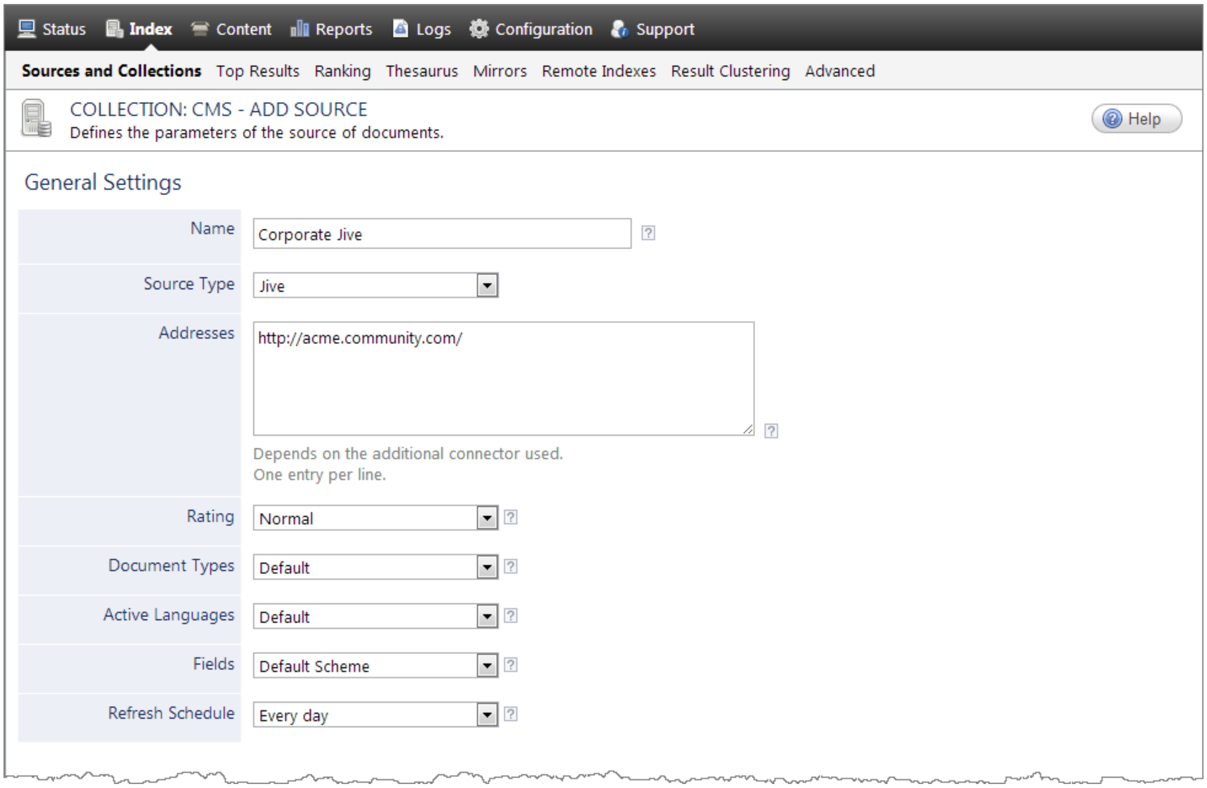
To configure and index a Jive source

1. On the Coveo server, access the Administration Tool.
2. Select **Index** > **Sources and Collections**.
3. In the **Collections** section:
   a. Select an existing collection in which you want to add the new source.

      OR

   b. Click **Add** to create a new collection.
4. In the **Sources** section, click **Add**.

   The **Add Source** page that appears is organized in three sections.
5. In the **General Settings** section of the **Add Source** page:



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

General Settings

Name	Corporate Jive
Source Type	Jive
Addresses	http://acme.community.com/ Depends on the additional connector used. One entry per line.
Rating	Normal
Document Types	Default
Active Languages	Default
Fields	Default Scheme
Refresh Schedule	Every day

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

Name

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

Example: `Corporate Jive`

Source Type

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

Notes:

- You should not confuse the **Jive** source with the **Jive 5 / SBS / Clearspace** source that must be used with Jive versions older than Jive 6.0.
- When you do not see **Jive**, your environment does not meet the requirements (see "Jive Connector Requirements" on page 7).

Addresses

Enter the root address of the Jive server that you want to index.

Example: `http://acme.community.com/`

Refresh Schedule

Select the 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: 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.

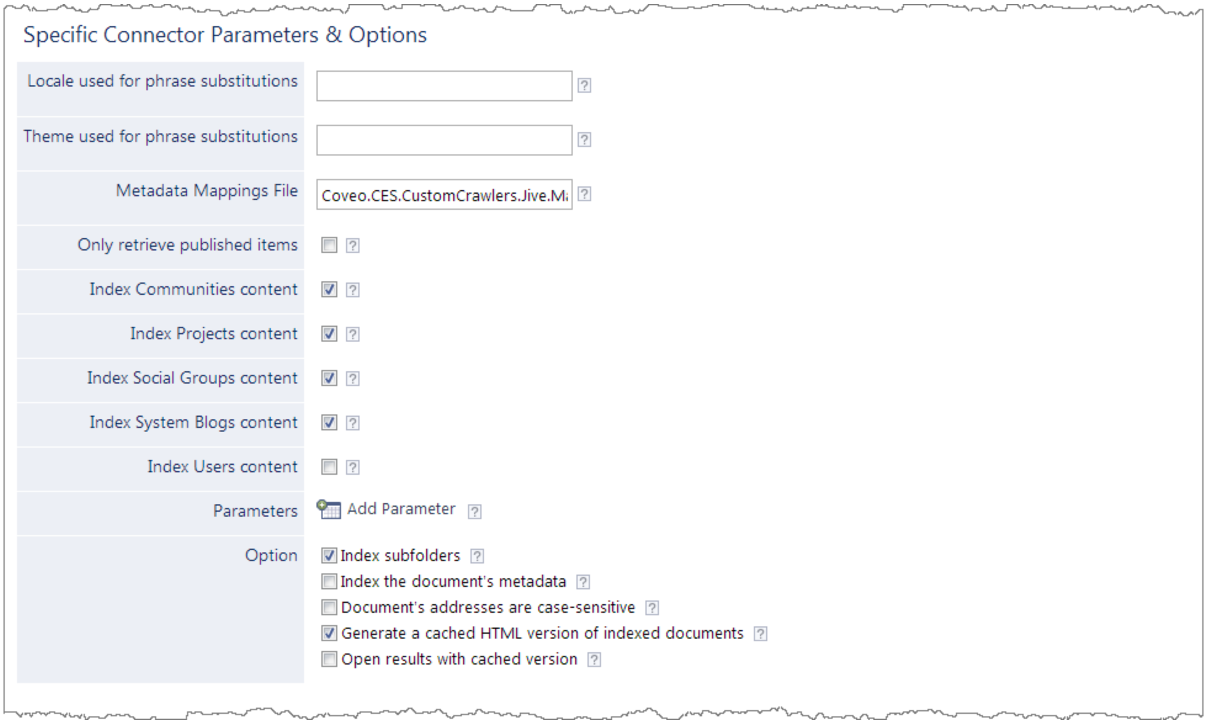
Fields

CES 7.0.8541+ (September 2016) Select the field set that you created earlier (see Jive Connector

Deployment Overview).

Note: CES 7.0.8388– (June 2016) 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:



Specific Connector Parameters & Options

Locale used for phrase substitutions	
Theme used for phrase substitutions	
Metadata Mappings File	Coveo.CES.CustomCrawlers.Jive.M
Only retrieve published items	□
Index Communities content	☑
Index Projects content	☑
Index Social Groups content	☑
Index System Blogs content	☑
Index Users content	□
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

a. When you use phrase substitutions in your Jive community (see the Jive document Substituting Phrases in the UI), you must set the following parameters. Otherwise, leave them blank.

Locale used for phrase substitutions

Enter the phrase substitution locale that the connector should use. The default locale is `default`, meaning that the actual machine locale is used.

Enter the locale in any of the following three formats:

- Language only (ex: `en`)
- Language and country (ex: `en_US`)
- Language, country, and variant (ex: `en_US_NY`)

Theme used for phrase substitutions

Enter the phrase substitution theme that the connector should use. The default theme is `custom`.

A metadata called `csPhraseSubstitution` will be available for use in the mapping file.

b. In the **Metadata Mapping File** box, enter the path to the mapping file that should apply to the items in this source (see "Creating and Using a Jive Mapping File" on page 26).

When you remove the default mapping file (`[CES_Path]\Bin\Coveo.CES.CustomCrawler.Jive.Mappings.xml` and leave this box empty, the connector maps no metadata to CES fields.

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

Only retrieve published items

Select to only index Jive items for which the status is `Published`. Items with other statuses (such as `Draft`, `Scheduled`, `Awaiting Moderation`, `Rejected`, `Abuse Hidden`, `Abuse Visible`, `Archived`, `Expired`, `Pending Approval`, `Deleted`, `Processing`, `Error`, `Unknown`) are not indexed.

Notes:

- Incremental refresh catches Jive item status changes and respects the configuration of this parameter.
- (Jive 6 only) Retrieving unpublished content requires Jive 6 API 3.3+ on the Jive server. When the Jive API does not support retrieving unpublished content, you get the following message in the CES Console:

```
Retrieving unpublished content requires at least the version 3.3 of the
Jive REST API to be installed on the Jive server.Please update your
version (n.n) if you want to use this feature or check the
'OnlyIndexPublishedContent' option.
```

Index Communities content

Select to index the Jive communities and any item they contain. Selected by default.

Index Projects content

Select to index the Jive projects and any item they contain. Selected by default.

Index Social Groups content

Select to index the Jive social groups and any item they contain. Selected by default.

Index System Blogs content

Select to index the Jive system blogs and any item they contain. Selected by default.

Index User content

Select to index the user profiles, personal blogs, and private items (messages, documents and discussions). Not selected by default.

Notes:

- CES 7.0.8541– (September 2016) The option is selected by default.
- Permission changes in Jive for **User content** type cannot be updated in the index with incremental refresh like for other types of Jive content. When you want to index **User content**, keep permissions as up-to-date as possible in the index, and optimize the load to your Jive server, it is recommended to create a separate source for **User content** using parameters suggested in the following table.

Source Options	Main source	Users content source
Index Communities content	Yes	No
Index Projects content	Yes	No
Index Social Groups content	Yes	No
Index System Blogs content	Yes	No
Index Users content	No	Yes
Refresh Schedule	Incremental (Every 5 minutes) Full Refresh (Every Sunday)	Full Refresh (Every day)

d. Click **Add Parameter** when you want to show and change the value of advanced source parameters (see "Modifying Hidden Jive Source Parameters" on page 28).

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

Index Subfolders

This parameter is not taken into account for this connector.

Index the document's metadata

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

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

Example: A document has two metadata:

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

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

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

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

Document's addresses are case-sensitive

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.

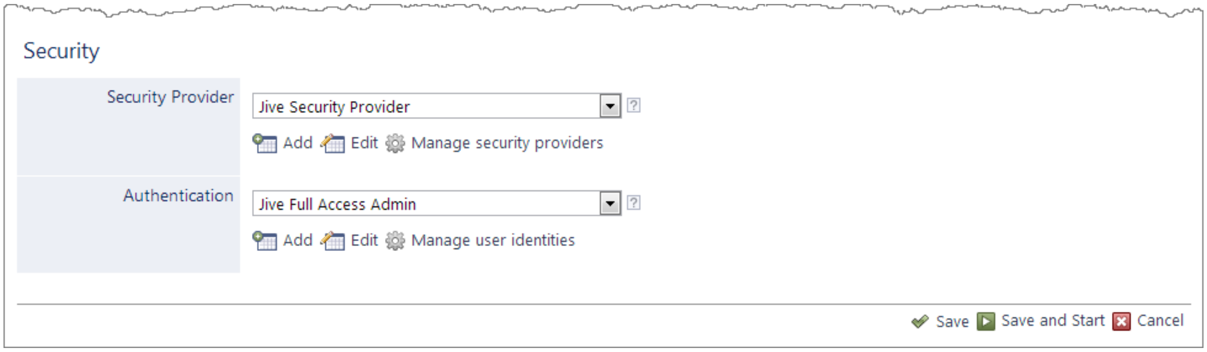
Generate a cached HTML version of indexed documents

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, perform the following actions if the plugin was installed.



Security

Security Provider: Jive Security Provider

Authentication: Jive Full Access Admin

   a. In the **Security Provider** drop-down list, when you chose to index Jive permissions, select the security provider that you created for this source (see "Configuring a Jive Security Provider" on page 16).

      Note: CES 7.0.8225+ (March 2016) When you want to only index public Jive content, select **None**.

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

      Note: CES 7.0.8225+ (March 2016) When you want to only index public Jive content, select **None**.

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

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

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

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

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

   d. Click **Apply Changes**.

9. When you are ready to start indexing the Jive source, click **Rebuild**.

10. 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.
- Review possible known issues (see "Troubleshooting Jive Connector Issues" on page 28).
- Consider modifying some hidden source parameters to try resolving other issues (see "Modifying Hidden Jive Source Parameters" on page 28).

8.1 Creating and Using a Jive Mapping File

By default, the Jive connector uses the default mapping file (`[CES_Path]\Bin\Coveo.CES.CustomCrawler.Jive.Mappings.xml`). When you want to customize how the connector maps Jive metadata to index fields, you can create a custom mapping file.

Note: The Jive connector uses the standard mapping file schema to configure what metadata from your original Jive documents are associated with fields for the documents in the Coveo index.

The first section of the mapping file, `CommonMappings`, defines fields that will apply to every document.

```
<?xml version="1.0" encoding="utf-8" ?>
<Mappings>
  <Version>1</Version>
  <CommonMapping>
    <Fields>
      <Field name="sysauthor">%[author.displayName]</Field>
      <!-- Jive system fields -->
      <Field name="syscstag">%[tags]</Field>
      <Field name="syscstaggroup">%[categories]</Field>
      <Field name="syscsplace">%[coveo.places.titles]</Field>
      <Field name="syscsplacetype">%[coveo.places.types]</Field>
    </Fields>
  </CommonMapping>
```

Example: The mapping `<Field name="sysauthor">%[author.displayName]</Field>` instructs the connector to copy the value of the `author.displayName` Jive metadata and paste it in the `sysauthor` Coveo index field for each indexed document.

The following sections of the Jive mapping file define fields for different types of Jive documents (`file`, `space`, `direct message`...).

Example: The fields for a Jive `person` type of documents are given in the following mapping file excerpt.

```
<Mapping type="person">
  <Title>%[displayName]</Title>
  <Body> %[displayName] %[emails(work).value] %[jive.profile(Title).value]</Body>
  <Fields>
    <Field name="UserProfile_FirstName">%[name.givenName]</Field>
    <Field name="UserProfile_LastName">%[name.familyName]</Field>
    <Field name="UserProfile_AccountName">%[jive.username]</Field>
    <Field name="UserProfile_Title">%[jive.profile(Title).value]</Field>
    <Field name="UserProfile_AboutMe">%[jive.profile(Biography).value]</Field>
    <Field name="UserProfile_PictureURL">%[thumbnailUrl]</Field>
    <Field name="UserProfile_WorkEmail">%[emails(work).value]</Field>
    <Field name="UserProfile_WorkPhone">%[phoneNumbers(work).value]</Field>
    <Field name="mobile">%[phoneNumbers(mobile).value]</Field>
    <Field name="syslocation">%[location]</Field>
    <Field name="sysfiletype">csuser</Field>
    <!-- Jive system fields -->
    <Field name="syscsitemtype">User</Field>
  </Fields>
</Mapping>
```

Note: The built-in mapping file includes only the standard Jive metadata, none of your Jive custom or *business* metadata. The connector however retrieves all metadata. If you create and assign to your Jive source a field set that includes field names that exactly match metadata names, they will be mapped automatically. It is therefore recommended to extend your Jive source field set to include matching fields for all useful metadata.

To create and use a custom mapping file

1. Using an administrator account, connect to the Coveo Master server.
2. Using a text editor:
   a. Create an XML file respecting the mapping file schema.

      Tip: You can use a copy of the default mapping file as a starting point.

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

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

3. Instruct the connector to use this mapping file for a given source by adding the path of the mapping file to the **Mapping File** source parameter (see "Configuring and Indexing a Jive Source" on page 20).

8.2 Troubleshooting Jive Connector Issues

This topic describes general issues you may encounter while using the Jive connector and attempts to provide the best course of action to resolve them.

8.2.1 Incremental Refresh

Incremental refresh is not detecting modifications made to Jive permissions

Modifications made to permissions in Jive do not impact the last modification date of objects affected by the permission modification. Since incremental refresh is using this last modification date to retrieve objects to update, the permission modification is not detected.

When Jive permissions are frequently modified, schedule a daily CES security cache update to keep the index permissions synchronized with Jive permissions.

Incremental refresh is not retrieving items that were deleted more than two weeks ago

The connector needs to keep track of items that were deleted from Jive in order for incremental refresh to keep the index up-to-date. Every time an incremental refresh run completes, items that were deleted more than two weeks ago are removed from the deleted history.

If incremental refresh was disabled on a source for a period greater than two weeks and you have more than one source performing incremental refresh on the same Jive server, you should perform a source refresh on the source where incremental refresh was disabled to make sure your index is fully up-to-date.

8.3 Modifying Hidden Jive 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 Jive 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 Jive 6 sources. The parameter type (Integer, String, Boolean) appears between parentheses following the parameter name.

IgnoreItemsOfTypes (String)

Semi-colon separated list of Jive item types to ignore while indexing. Possible values are: `Announcement`, `Attachment`, `Checkpoint`, `Comment`, `Discussion`, `Dm`, `Document`, `File`, `Group`, `Idea`, `Message`, `Poll`, `Project`, `Space`, `SystemBlog`, `Task`, `Update`, `Video`.

StartingSpaceUrl (String)

The URL of the space at which the crawling should start. Only content within this space and its subspaces will be available in the index. This does not affect social groups and people.

AdditionalHeaders (String) CES 7.0.5425+ (May 2013)

List of headers that should be added to the web requests made by the connector in the following format: `key1\=value1\;key2\=value2`

> **Example:** If you need to add a Web service authentication header with a key "User" and a value "CrawlingUser" you can enter the following string in this parameter: `user\=CrawlingUser`

IgnoreItemsOlderThan (String) CES 7.0.8225+ (March 2016)

Specifies the modified date from which older items are not indexed. The date string must be in a format recognized by the Microsoft .NET Framework (see Standard Date and Time Format Strings). By default there are no dates and all items are indexed.

RequestTimeout (Integer) CES 7.0.8996+ (June 2017)

The maximum amount of time (in seconds) a request can be executed before being canceled. The default and optimal value is 100.

BatchSize (Integer) CES 7.0.8996+ (June 2017)

The number of items to retrieve with each call to Jive server. The default and optimal value is 25 items.

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

To modify hidden Jive source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 30 to add one or more Jive hidden source parameters.

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

8.4 Adding an Explicit Connector Parameter

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

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

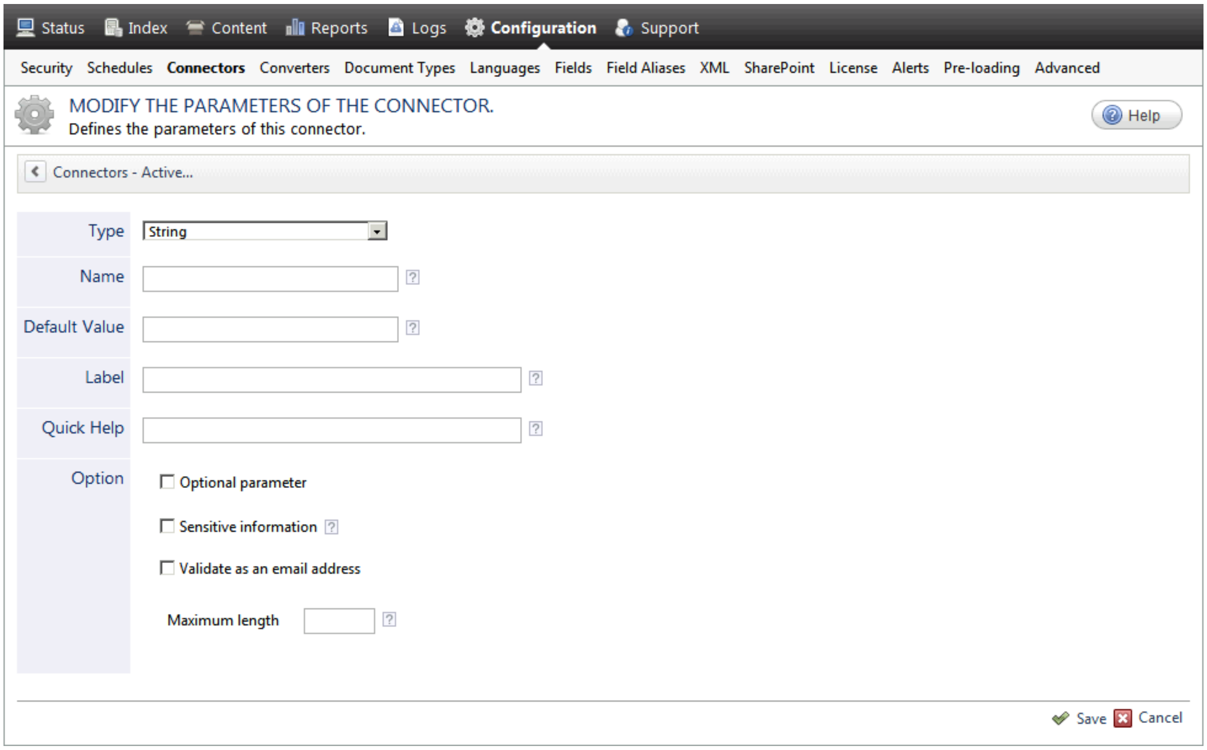
You can however choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value.

To add an explicit connector parameter

1. On the Coveo server, access the Administration Tool.
2. Select **Configuration** > **Connectors**.
3. In the list on the **Connectors** page, select the connector for which you want to show advanced hidden parameters.
4. In the **Parameters** section of the selected connector page, click **Add Parameter** for each hidden parameter that you want to modify.

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

●●●●

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

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

k. Click **Save**.

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

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

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

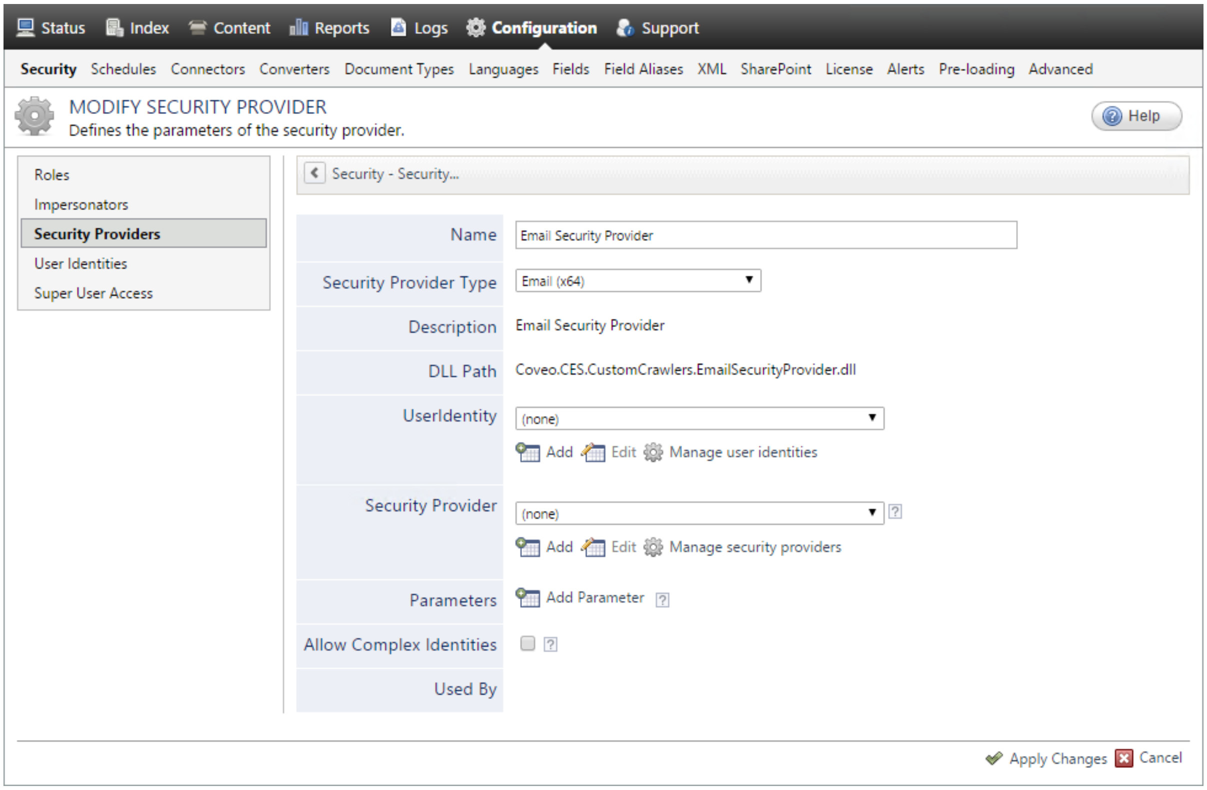
9. Configuring an Email Security Provider

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

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

To configure an Email security provider

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



MODIFY SECURITY PROVIDER
Defines the parameters of the security provider.

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

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

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

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

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

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

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

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

f. Click **Apply Changes**.

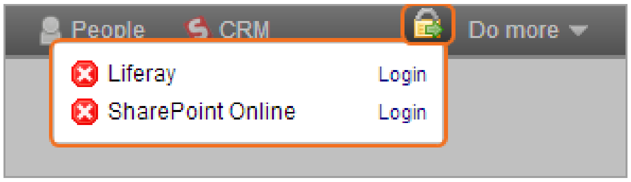
What's Next?

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

10. Adding Security Providers to a .NET Search Interface

A Coveo .NET Front-End search interface can get and pass to the Coveo Back-End server the identity of the user performing a query so that only documents this user has permissions to see are returned in search results.

Sometimes a user needs to search using multiple user identities at the same time. You can allow a user to do this by associating one or more security providers to the .NET search interface. When one or more security providers are added to a .NET search interface, a lock icon (🔒) appears in the top-right corner of the .NET search interface to allow the user to access a login form where they can enter additional credentials.

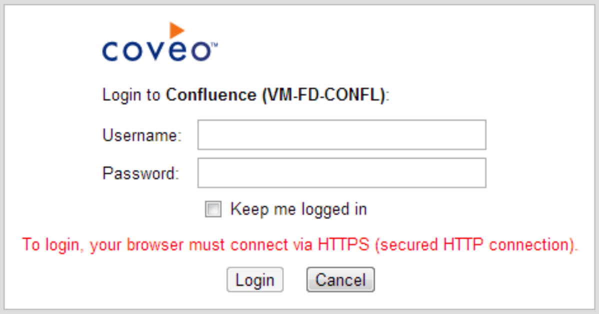


Example: A user is logged in with their Windows account and accesses the **All Content** .NET search interface in a Coveo Web access point. The user queries return only documents that their Active Directory account has permissions to see, not Claims-enabled SharePoint documents that the user should legitimately see.

You add the SharePoint Claims security provider to the .NET search interface. The user can log in to provide their SharePoint Claims credentials. When this is done, both his Active directory and Claims identities are passed to the Back-End server so that Claims-enabled SharePoint documents can also be returned in the search results.

Notes:

- You must first configure the security provider in the Administration Tool.
- The login form requires a secured .NET search interface access (HTTPS). When the search interface is accessed via HTTP, the login form includes a message indicating that HTTPS must be used.
- Coveo .NET Front-End 12.0.295+ (August 2013) The username and password are sent to the server via the SSL connection and an authorization token is stored in an end-user browser cookie (not the username and password). By default the cookie expires when the user closes the browser but to avoid having to log in for each new browser session, selecting the **Keep me logged in** check box makes the cookie valid for one month.
- When adding a Claims SharePoint security provider, ensure that the Coveo web service is installed on a SharePoint front-end server to allow the login to work.



coveo

Login to **Confluence (VM-FD-CONFL)**:

Username:

Password:

□ Keep me logged in

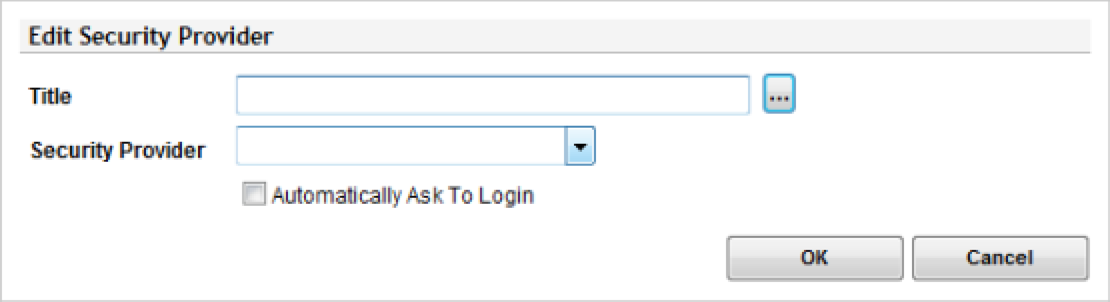
To login, your browser must connect via HTTPS (secured HTTP connection).

Login Cancel

To add security providers to the .NET search interface

1. Access the Coveo .NET Front-End Interface Editor.
2. Access the **Search Interfaces** tab.
3. Select **Advanced** > **Security Provider**.
4. Click **Add New**.

5. In the **Edit Security Provider** page:



   a. In the **Title** box, enter a descriptive name for the security provider. This name appears in the lock icon pop up window and in the login form.

   b. In the **Security Provider** drop-down list, select the appropriate security provider.

   Example: For Claims-based SharePoint server, select your Claims security provider.

   Note: The **Security Provider** lists only security providers of types supporting the login feature. By default only **Active Directory** is available. Ensure that one or more valid security providers of type supporting the login are configured in CES.

   c. Select the **Automatically Ask to Login** check box when you want to automatically display the login form in the search interface when a user starts a search session.

   It is generally recommended to select this check box to systematically propose to users to provide their additional credentials so that all search results to which they are entitled are returned. When the check box is cleared, the user must know and remember to manually click the lock icon 🔒 on the search interface top bar to open the login form and enter his credentials.

   Notes: The **Login** or **Cancel** user actions are persisted on a per user per browser basis. As long as a user is using the same browser session, he will not have to log in again or cancel an automatic form. For security reason, only an authorization token provided by CES is stored in a browser cookie, not the entered **Username** and **Password**.

   d. Click **OK**.

6. It is recommended to configure IIS to force an HTTPS search interface connection or automatically redirect HTTP to HTTPS to prevent users from seeing the login form error message (`To login, your browser must connect via HTTPS (secured HTTP connection).`) and having to manually change the search interface URL from `http://` to `https://` (see IIS7 : HOW TO force a website to use SSL? and HTTP Redirects <httpRedirect>).

What's Next?

Go back to the search interface, refresh the page, and then login with your additional identity to validate that you can now find documents secured with this additional identity.