Coveo Platform 7.0

Zendesk 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-151003-EN

Publication date: 1/3/2019

Table of Contents

1. Zendesk Connector

CES 7.0.7914+ (October 2015)

The Coveo connector for Zendesk allows Coveo administrators to index and integrate the content of a Zendesk customer service website into the Coveo unified index. The connector indexes all items from a Zendesk customer service website so that in the Coveo search interfaces, a user can easily find Zendesk content.

1.1 Features

The Zendesk connector features are:

Content indexing

Extraction and indexing of the following Zendesk item types:

- Tickets
- Users
- Groups
- Organizations
- Articles
- Comments
- Attachments

Note: Since the part of the Zendesk API v2 for the Help Center is in beta, the content of Help Center communities (topics, questions, ideas and posts) cannot yet be indexed.

Mostly supported security model CES 7.0.8047+ (December 2015)

The connector depends on a part (User Segments) of the Zendesk API v2 to retrieve permissions for indexed items. Since the part of the API for the Help Center is in beta, the permissions can currently only be indexed for tickets and their sub-items (comments and attachments). This means that, in Coveo search interfaces, a user searching Zendesk content only sees the tickets to which they have access in Zendesk.

Notes:

- The Zendesk API v2 does not provide the permissions for the following item types: articles and their sub-items (comments and attachments). Most of the time, the Help Center content is public, meaning that the articles are made available to all end-users and agents, but in some cases, you may have restricted the access to some sections and categories (see Restricting access to knowledge base content).
- CES 7.0.9272+ (March 2018) The Access Policies API has been removed by Zendesk on December 15, 2017 and replaced by User Segments (see [Sunsetting] Access Policies for Help Center).

Incremental refresh CES 7.0.8047+ (December 2015)

Supports incremental refresh to periodically query Zendesk for the latest edits, keeping the index content up-to-

date.

Multithreading

The connector can run multiple threads, which can improve performances considerably (see Modifying Hidden Zendesk Source Parameters).

Partial Pause/Resume CES 7.0.8047+ (December 2015)

When indexing Zendesk ordered items such as tickets and articles, the connector can be paused and resumed.

1.2 Limitations

- CES 7.0.7914 (October 2015) The connector does not yet support Zendesk permissions.

  Important: In the Coveo search interface, a user searching Zendesk content could see content to which he has normally no access in Zendesk. Thus, it is currently highly recommended to only index Zendesk customer service websites with public content.

  Since Zendesk APIs can only be used by Zendesk admin users, it is currently impossible to limit the content to be indexed to a certain organization, group, or user (agent and end-user).

- CES 7.0.7914 (October 2015) A full refresh is needed to retrieve the latest items modifications (addition, edition, deletion).

What's Next?

Review the steps to deploy the Zendesk connector (see "Zendesk Connector Deployment Overview" on page 3).

2. Zendesk Connector Deployment Overview

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

To deploy the Zendesk connector

1. Validate that your environment meets the requirements (see "Zendesk Connector Requirements" on page 5).
2. (When you want the connector to connect to your Zendesk content using OAuth 2.0 - recommended method) On the Zendesk server, create an application to authorize the Coveo connector to access your Zendesk content (see "Authorizing the Coveo Connector to Access Your Zendesk Content" on page 6).
3. On the Coveo server, in the Coveo Administration Tool:
   a. CES 7.0.8047+ (December 2015) Optionally create security providers

      When you want to index Zendesk permissions, you must create two security providers to get Zendesk item permissions and resolve and expand groups. Due to a Zendesk API v2 limitation, not all permissions are currently retrievable (see Permission limitation).

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

      i. Start by selecting or creating a security provider that the Zendesk 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:

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

         - When authenticated with their email address, use an Email security provider (see "Configuring an Email Security Provider" on page 12).
         - When authenticated with an Active Directory account, use an LDAP Lookup security provider that maps LDAP identities to Active Directory ones. Contact Coveo Support for assistance.

           Note: This chain of security providers is required since the Zendesk security provider does not directly support to be chained with an Active Directory security provider.

      ii. Then, create a Zendesk security provider that the connector uses to resolve indexed permissions (see "Configuring a Zendesk Security Provider" on page 9).

   b. (When you want the connector to connect to your Zendesk content using a Zendesk API v2 token) Configure a user identity.

      The connector needs to know the username of a Zendesk admin account by creating a CES user identity that you will later associate to your Zendesk source.

Note: This method is not recommended since the Zendesk API token allows read and write permissions.

c. Create a Zendesk field set to take advantage of the available Zendesk metadata.

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

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

d. Configure and index a Zendesk source.

   The connector must know details to access and index the Zendesk content of your managed users (see "Configuring and Indexing a Zendesk Source" on page 16).

e. If you encounter issues, verify if modifying the default value of hidden source parameters can help resolve the problems (see "Modifying Hidden Zendesk Source Parameters" on page 21).

3. Zendesk Connector Requirements

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

- CES 7.0.7914+ (October 2015)
- Coveo license for the Zendesk connector

  Your Coveo license must include support for the Zendesk connector to be able to use this connector.
- A valid admin Zendesk account

  Using an administrator Zendesk account, you must create a Zendesk app and an OAuth 2.0 protocol to authorize Coveo to access the content of your Zendesk customer service website (see Authorizing the Coveo Connector to Access Your Zendesk Content).

What's Next?

Grant Coveo access to the content of your Zendesk customer service website by creating a Zendesk application (see "Authorizing the Coveo Connector to Access Your Zendesk Content" on page 6).

4. Authorizing the Coveo Connector to Access Your Zendesk Content

You can grant the Coveo connector access to your Zendesk customer service website content using a Zendesk API v2 token. It is however recommended to perform the complete OAuth 2.0 protocol for security reasons (can grant the access to your Zendesk content with only read permission).

The OAuth 2.0 protocol is a protocol used for granting access to external applications without exposing the user's real credentials. For the connector to be able to connect to the content of your Zendesk customer service website, it must acquire an access token.

To authorize the Coveo connector to access your Zendesk content

1. Log into your Zendesk customer service website with an administrator account.
2. Access the agent interface, by clicking the drop-down list menu in the top right of the page, and then selecting **Open agent interface**.
3. In the agent interface, access the **Zendesk API** page:
   a. In the navigation bar on the left, click the Admin icon  .
   b. In the admin setting menu, under **Channels**, click **API**.
4. In the **Zendesk API** page, depending on the way you want to grant access to your Zendesk content:
   - Using OAuth 2.0
     a. Click the **OAuth Clients** tab.
     b. In the **OAuth Clients** tab, click **add a client**.
     c. In the **New OAuth Client** page:
        i. In the **Client Name** box, enter a descriptive application name.

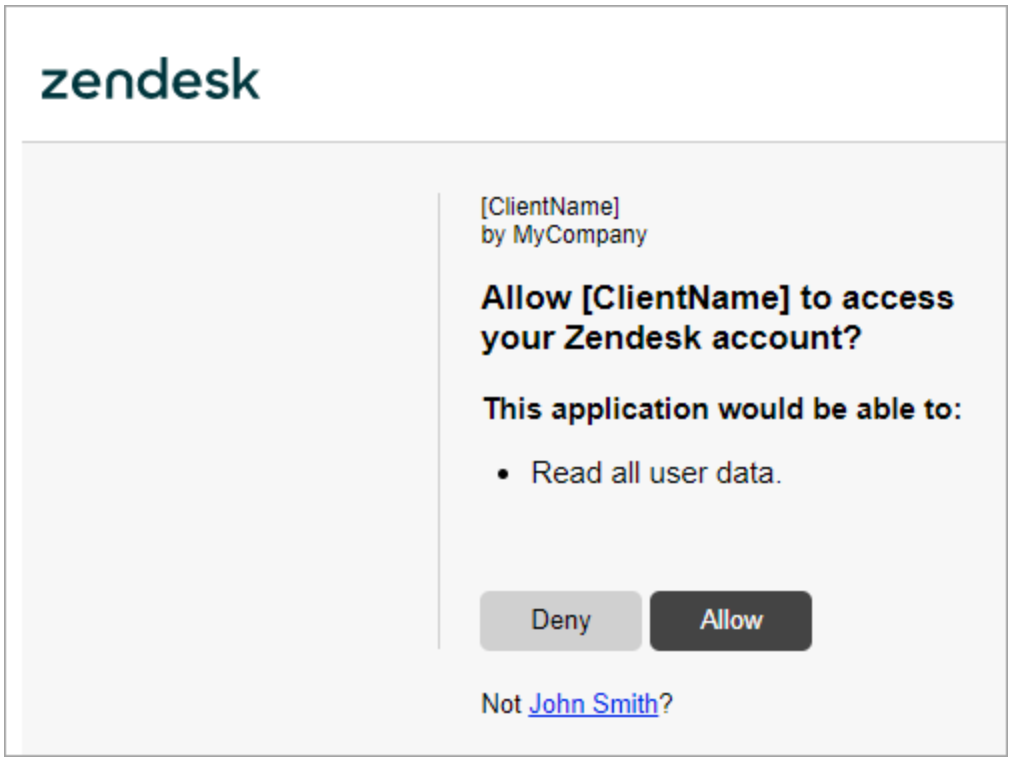
        Example: Coveo Connector

        ii. Take note of the **Unique Identifier** auto-populated. You need this value during the OAuth authentication process.
        iii. In the **Redirect URLs** box, enter `http://localhost/`.
        iv. Click **Save**.
        v. Take note of your application **Secret**.
        vi. Click **Save** again.
     d. Authorize your application to use your Zendesk administrator account:

i. Open another browser tab by pressing `CTRL+t`.

ii. In the new tab, copy and paste the following URL in the browser address bar after entering your website and client ID at the specified places: `https://[YOUR_WEBSITE].zendesk.com/oauth/authorizations/new?response_type=token&redirect_url=http://localhost/&client_id=[YOUR_UNIQUE_IDENTIFIER]&scope=read`.

iii. In the **Allow [ClientName] to access your Zendesk account** screen, click **Allow** to receive an authorization code from Zendesk.



You are redirected to the URI you specified when configuring the Zendesk app.

iv. In your browser address bar, take note of the access token returned by the Zendesk API. You need this value when configuring your Zendesk source (see Configuring and Indexing a Zendesk Source).

Example: `http://localhost/#access_token=[ACCESS_TOKEN]&scope=read&token_type=bearer`

- Using a Zendesk API v2 token:

a. In the **Zendesk API** page, in the **Settings** tab, next to **Token Access**, select the **Enabled** check box.

b. In the section that appears, click **add new token**.

c. In the **Enter a label for this API Token** dialog that appears, enter a descriptive name, and then click **Create**.

Example: `CoveoConnector`

d. Back in the **API** page, next to **Token Access**, select the **Enabled** check box.

e. Under **Active API tokens**, take note of the API token. You need this value when configuring your Zendesk source (see Configuring and Indexing a Zendesk Source).

f. Click **Save**.

What's Next?

Create a Zendesk source ("Configuring and Indexing a Zendesk Source" on page 16).

5. Configuring a Zendesk Security Provider

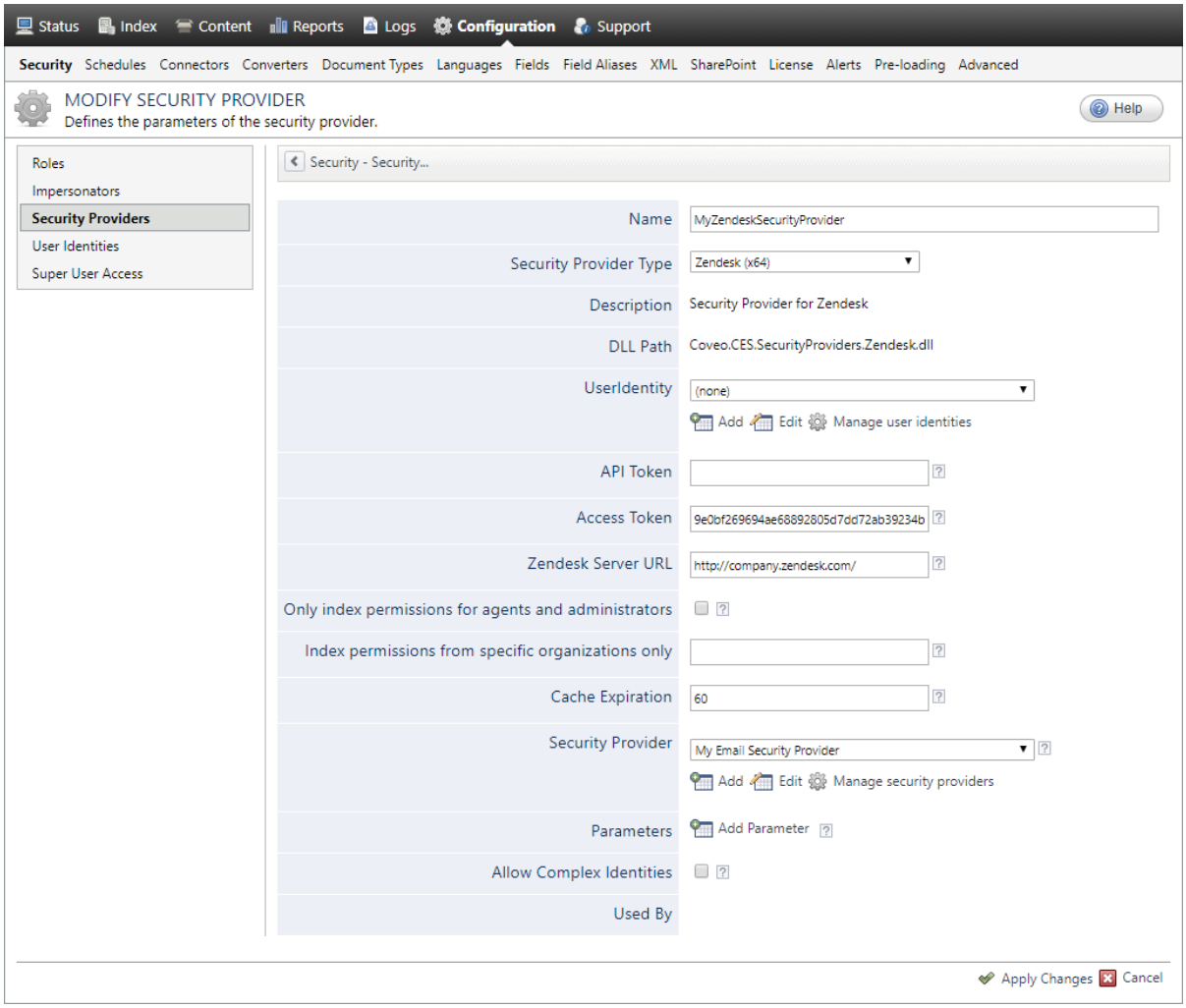
CES 7.0.8047+ (December 2015)

The Coveo Zendesk connector mostly supports the Zendesk security model. Due to a Zendesk API v2 limitation, not all permissions are currently retrievable (see Permission limitation). When you want users searching for Zendesk tickets and their sub-items (comments and attachments) in a Coveo search interface to only see the tickets to which they have access in Zendesk, the connector needs a security provider to be able to index the permissions for each indexed ticket.

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

To configure a Zendesk 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:



a. Configure the following required parameters:

Name

Choose a meaningful name to identify the security provider.

Example: `Zendesk Security Provider`

Security Provider Type

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

User Identity

Depending on the method you chose to retrieve your Zendesk content, in the drop-down list (see "Authorizing the Coveo Connector to Access Your Zendesk Content" on page 6):

- Using an OAuth 2.0 access token (recommended method), select **(none)**.
- Using a Zendesk API v2 token, select the user identity you previously created (see Zendesk Connector Deployment Overview).

b. Configure the following required parameters with the same values as the ones you will enter when configuring the source (see "Configuring and Indexing a Zendesk Source" on page 16):

API Token

(When you want the connector to retrieve your Zendesk content using a Zendesk API v2 token) Enter the API token previously obtained (see Authorizing the Coveo Connector to Access Your Zendesk Content).

Note: This method is not recommended since the Zendesk API token allows read and write permissions.

Example: `FAwrsE3RdyBxqkVDHJevqnJVr70TMlDzyUNIBpql`

Access Token

(When granting the connector access to your Zendesk content using OAuth 2.0) Enter the access token previously obtained (see Authorizing the Coveo Connector to Access Your Zendesk Content).

Example: `fdbefa0cb05bc3641481496d44af60b05cf3zj3406t299b6cc5789608d4d9f83`

Zendesk Server URL

Enter the base URL of your Zendesk customer service website.

Example: `https://company.zendesk.com`

CES 7.0.9272+ (March 2018) **Only index permissions for agents and administrators**

Select this checkbox to only retrieve Agent and Administrator entity permissions. End users permissions are not indexed when this option is selected.

CES 7.0.9272+ (March 2018) **Index permissions from specific organizations only**

Enter the Zendesk organizations of which you want to index the permissions. Use a semi-colon to separate your values.

Example: `MyOrganization1;MyOrganization2`

Cache Expiration CES 7.0.9167+ (December 2017)

Enter the absolute expiration (in minutes) for a cache entry. By default, a cache entry expires after 60 minutes.

Security Provider

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

c. Select the security provider that you selected or created to allow this security provider to resolve and expand the groups (see Zendesk Connector Deployment Overview).

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

e. Click **Apply Changes**.

What's Next?

Create and index a source (see "Configuring and Indexing a Zendesk Source" on page 16).

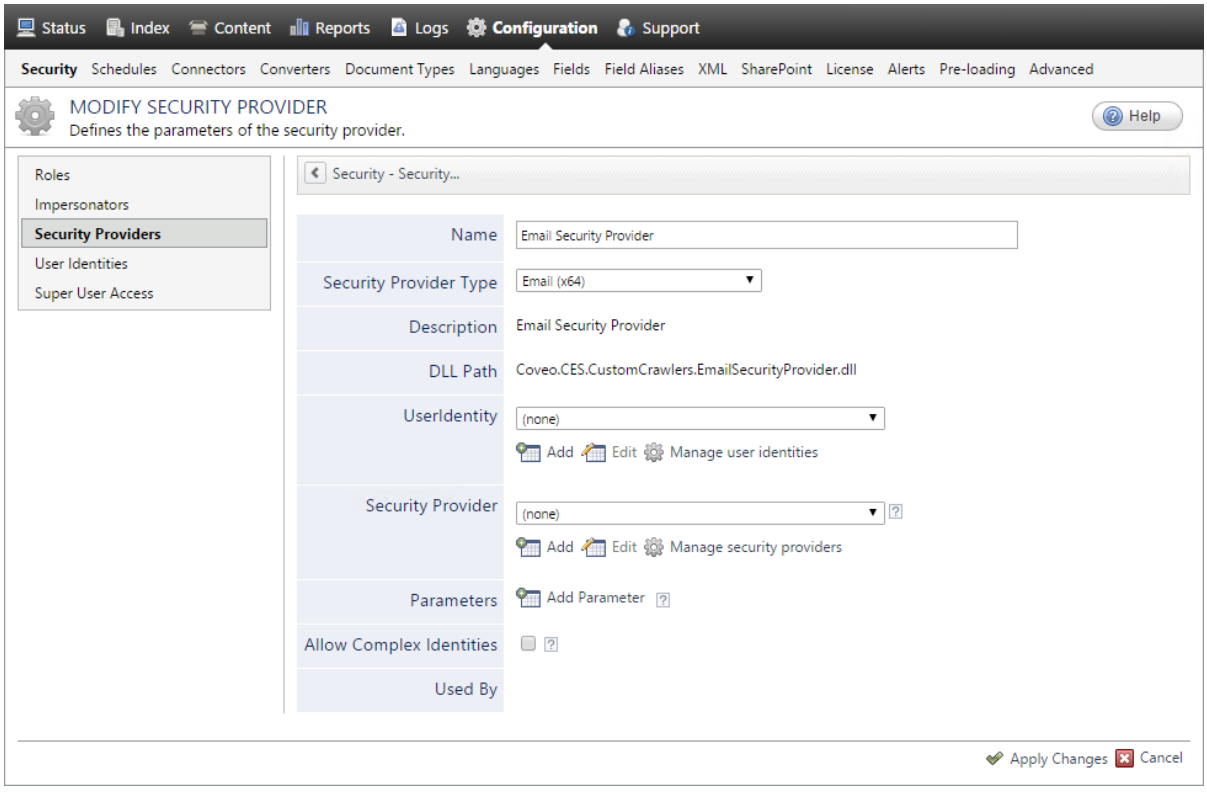
5.1 Configuring an Email Security Provider

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

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

To configure an Email security provider

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



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.

5.2 Configuring an Active Directory Security Provider

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

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

You may need to create another Active Directory security provider only when CES and AD are in different and untrusted domains. In this case, you only need to assign a user identity containing any user that has access to the

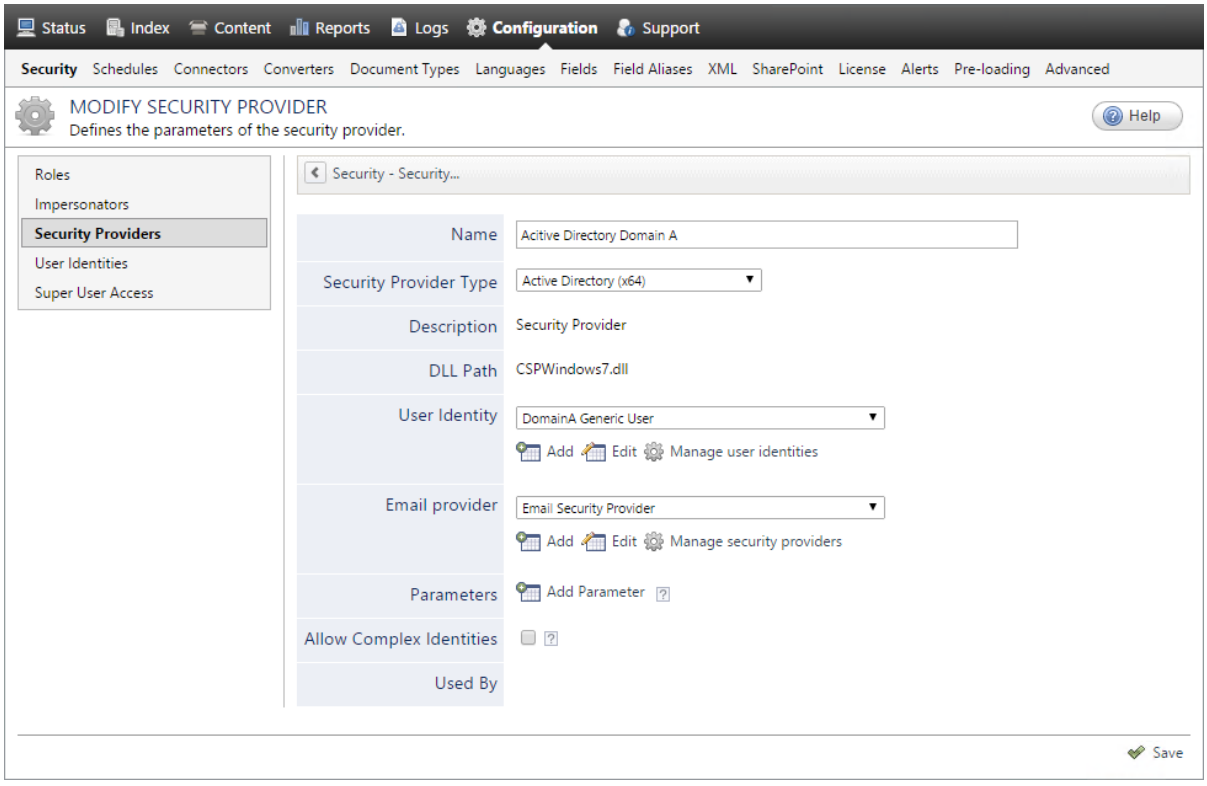
other domain to be able to use the security provider to expand, map, or resolve users or groups defined in Active Directory of this domain.

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

To create or modify an Active Directory security provider

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

What's Next?

When you are creating or modifying the security provider:

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

6. Configuring and Indexing a Zendesk Source

A source defines a set of configuration parameters for a specific Zendesk customer service website.

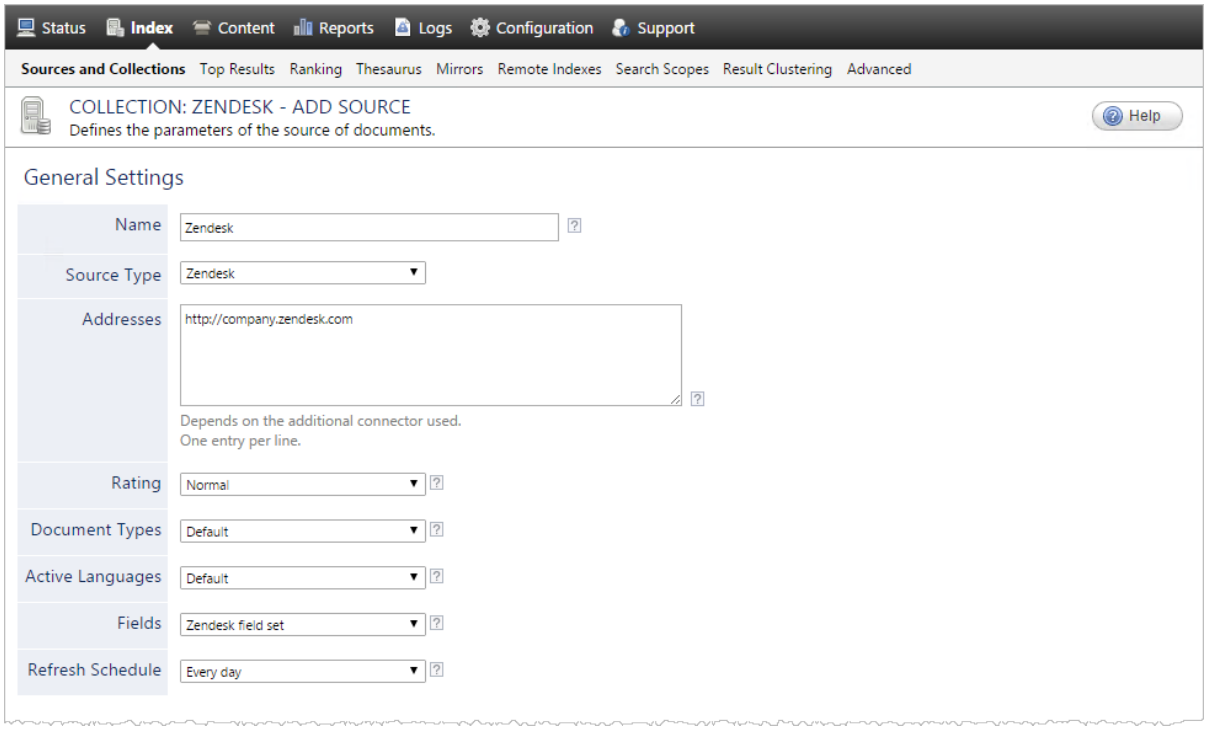
To configure and index a Zendesk source

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: `Zendesk`

Source Type

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

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

Addresses

Enter the base URL of your Zendesk customer service website.

Example: `https://company.zendesk.com`

Fields

Select the field set that you created earlier (see Zendesk Connector Deployment Overview).

Refresh Schedule

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

Note: CES 7.0.7914 (October 2015) Keep the **Every day** option as the incremental refresh is not supported.

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

Rating

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

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

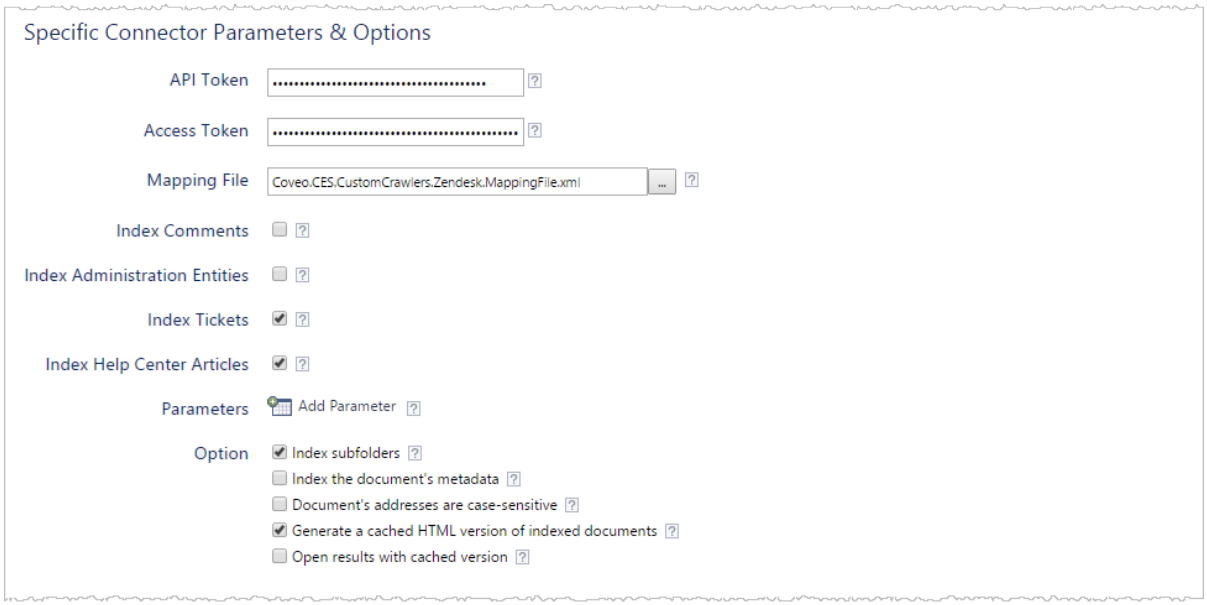
Document Types

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

Active Languages

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

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



a. Using the following parameters, authorize the Coveo crawler to access the content of your Zendesk customer service website:

API Token Security provider

(When you want the connector to retrieve your Zendesk content using a Zendesk API v2 token) Enter the API token to use that you previously obtained (see Authorizing the Coveo Connector to Access Your Zendesk Content).

Note: This method is not recommended since the Zendesk API token allows read and write permissions.

Access Token Security provider

(When granting the connector access to your Zendesk content using OAuth 2.0) Enter the access token to use that you previously obtained (see Authorizing the Coveo Connector to Access Your Zendesk Content).

b. In the **Mapping File** box, the path to the default mapping file that defines how the connector handles metadata often does not need to be changed.

c. The following options must be selected for certain Zendesk item types to be indexed.

Index Comments

Whether the comments on tickets and articles should be indexed.

Index Administration Entities CES 7.0.8047+ (December 2015)

Whether the users, groups and organizations should be indexed. By default, administration entities are not indexed.

Index Tickets CES 7.0.8996+ (June 2017)

Whether tickets should be indexed.

Index Help Center Articles CES 7.0.8996+ (June 2017)

Whether the articles in the Help Center should be indexed.

Index Help Center Items CES 7.0.8047 to CES 7.0.8850 (December 2015 to March 2017)

Whether the articles and their attachments should be indexed. By default, Help Center items are indexed.

d. (Optional) Click **Add Parameter** when you want to show and change the value of advanced source parameters (see "Modifying Hidden Zendesk Source Parameters" on page 21).

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

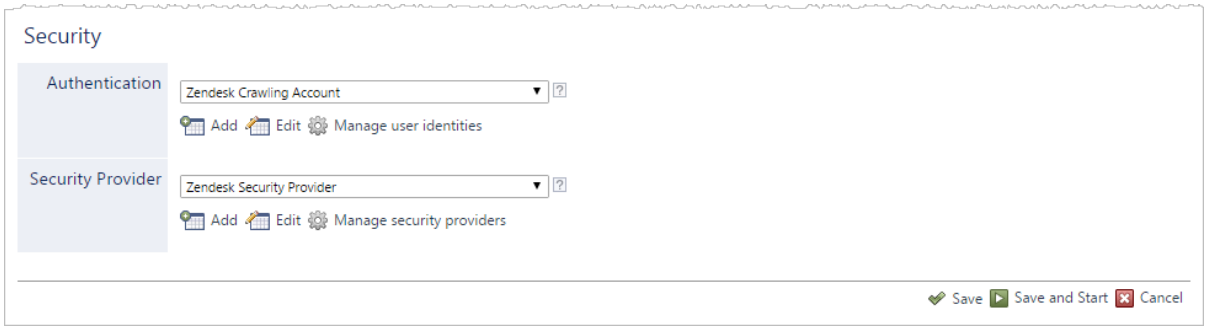
When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by

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:



Important: CES 7.0.7914 (October 2015) The connector does not yet support Zendesk permissions. It is thus strongly recommenced to only index Zendesk customer service websites with public content.

Note: A workaround is to manually define permissions on the source (see Permissions).

a. In the **Authentication** drop-down list, depending on your setup:

- When you grant the connector access to your content using OAuth, select **(none)**.
- When you grant the connector access to your content using the Zendesk API, select the user identity you previously created (see Zendesk Connector Deployment Overview).

b. CES 7.0.8047+ (December 2015) When you chose to index Zendesk permissions, in the **Security Provider** drop-down list, select the Zendesk security provider that you created for this source (see "Configuring a Zendesk Security Provider" on page 9 and Permission limitation).

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

9. When your Zendesk content is all public:

Important: CES 7.0.7914 (October 2015) The connector does not yet support Zendesk permissions. This means that, in the Coveo search interface, a user searching Zendesk content could see content to which he has normally no access in Zendesk.

Since Zendesk APIs can only be used by Zendesk admin users, it is currently impossible to limit the content to be indexed to a certain organization, group, or user (agent and end-user).

Note: When your Zendesk content is not public, a workaround is to enter the name of user(s) or group(s) you want to allow or deny access to your organization content in the **Allowed Users** and **Deny Users** boxes.

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

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

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

d. Click **Apply Changes**.

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

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

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

  OR

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

What's Next?

Set an incremental refresh schedule for your source.

Consider modifying some hidden source parameters to try resolving other issues (see "Modifying Hidden Zendesk Source Parameters" on page 21).

6.1 Modifying Hidden Zendesk 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 Zendesk 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 Zendesk sources. The parameter type (integer, string, etc.) appears between parentheses following the parameter name.

NumberOfRefreshThreads (Integer)

The number of refresh threads used by the crawler for this source. The default value is 4.

To modify hidden Zendesk source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 22 to add one or more Zendesk source parameters.
2. For a new Zendesk 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 Zendesk 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 Zendesk 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 Zendesk source to apply the changes to the parameters.

6.2 Adding an Explicit Connector Parameter

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

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

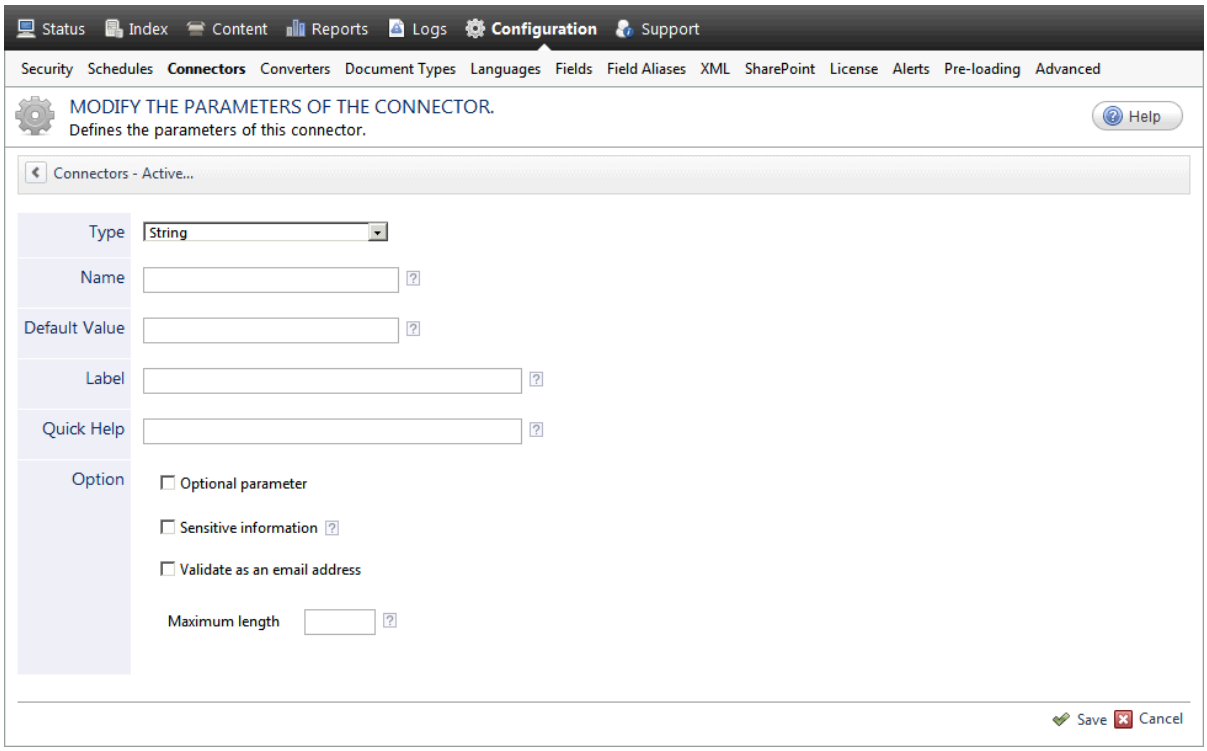
You can however choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value.

To add an explicit connector parameter

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

k. Click **Save**.

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

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

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