



---

## **Coveo Platform 7.0**

Box 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](http://www.coveo.com).

© Coveo Solutions Inc., 2015

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

Document part number: PM-15-08-06-EN

Publication date: 1/3/2019

## Table of Contents

<b>1. Adding an Explicit Connector Parameter</b> .....	<b>iv</b>
<b>2. Configuring an Email Security Provider</b> .....	<b>vii</b>
<b>3. Configuring an Active Directory Security Provider</b> .....	<b>ix</b>
<b>4. Modifying the Document Type Set Used by a Source</b> .....	<b>xii</b>
<b>5. Box Connector Deployment Overview</b> .....	<b>xiii</b>
<b>6. Authorizing the Coveo Connector to Access the Box of Your Managed Users</b> .....	<b>xv</b>
<b>7. Modifying Hidden Box Source Parameters</b> .....	<b>xviii</b>
<b>8. Configuring and Indexing a Box Source</b> .....	<b>xx</b>
<b>9. Box Connector</b> .....	<b>xxvi</b>
9.1 Connector Features Summary .....	xxvi
9.2 Features .....	xxvi
9.3 Limitations .....	xxvii
<b>10. Configuring a Box Security Provider</b> .....	<b>xxix</b>
<b>11. Box Connector Requirements</b> .....	<b>xxxii</b>

# 1. Adding an Explicit Connector Parameter

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

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

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

To add an explicit connector parameter

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

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

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

- a. In the **Type** list, select the parameter type as specified in the parameter description.
- b. In the **Name** box, type the parameter name exactly as it appears in the parameter description. Parameter names are case sensitive.
- c. In the **Default Value** box, enter the default value specified in the parameter description.

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


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

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

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

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

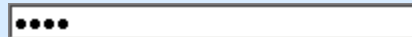
**Tip:** The language of the Administration Tool can be modified by pressing the following key combination: Ctrl+Alt+Page Up.

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

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

- f. When **Predefined values** is selected in the **Type** parameter, in the **Value** box that appears, enter the parameter values that you want to see available in the drop-down parameter that will appear in the Administration Tool interface. Enter one value per line. The entered values must exactly match the values listed in the hidden parameter description.
- g. Select the **Optional parameter** check box when you want to identify this parameter as an optional parameter. When cleared, CES does not allow you to save changes when the parameter is empty. This parameter does not appear for **Boolean** and **Predefined values** parameter types.
- h. Select the **Sensitive information** check box for password or other sensitive parameter so that, in the Administration Tool pages where the parameter appears, the typed characters appear as dots to mask them. This parameter appears only for the **String** type.

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



- i. Select the **Validate as an email address** check box when you want CES to validate that the text string that a user enters in this parameter respects the format of a valid email address. This parameter appears only for the **String** type.
  - j. In the **Maximum length** box, enter the maximum number of characters for the string. This parameter appears only for the **String** type. When you enter 0, the length of the string is not limited.
  - k. Click **Save**.
6. Back in the **Connector** page, click **Apply Changes**.

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

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

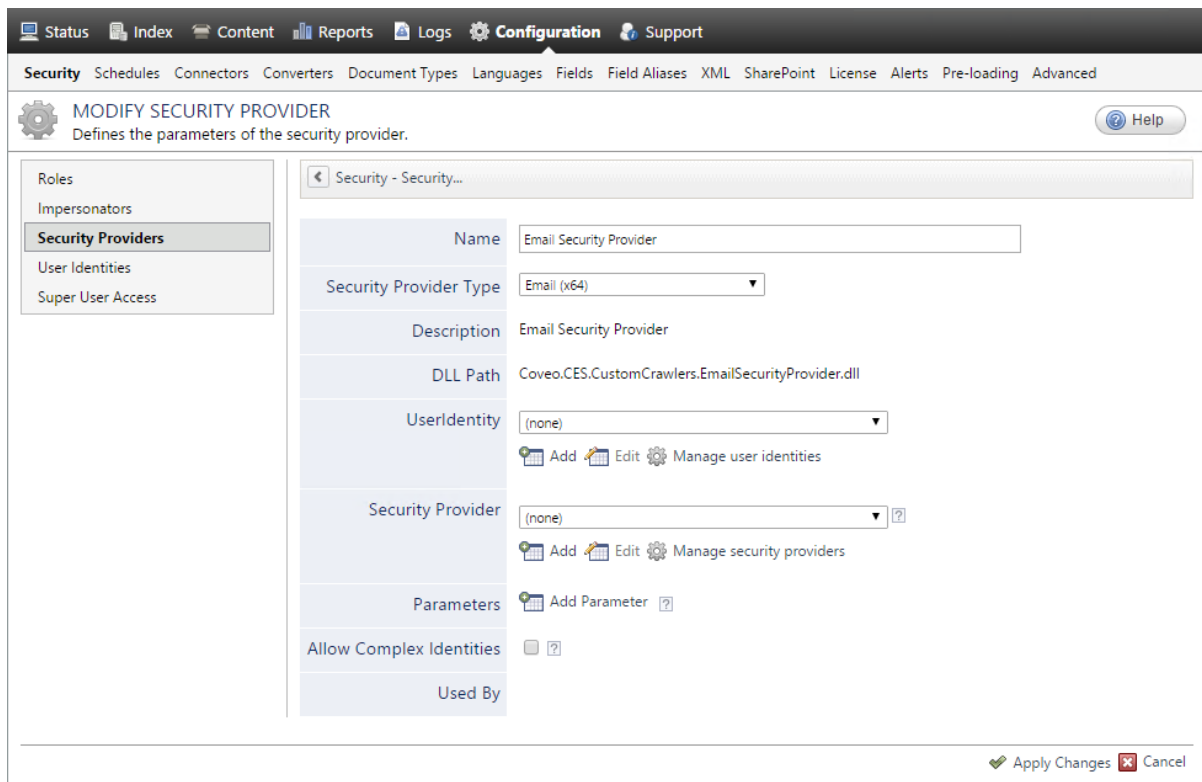
## 2. Configuring an Email Security Provider

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.



### 3. 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.

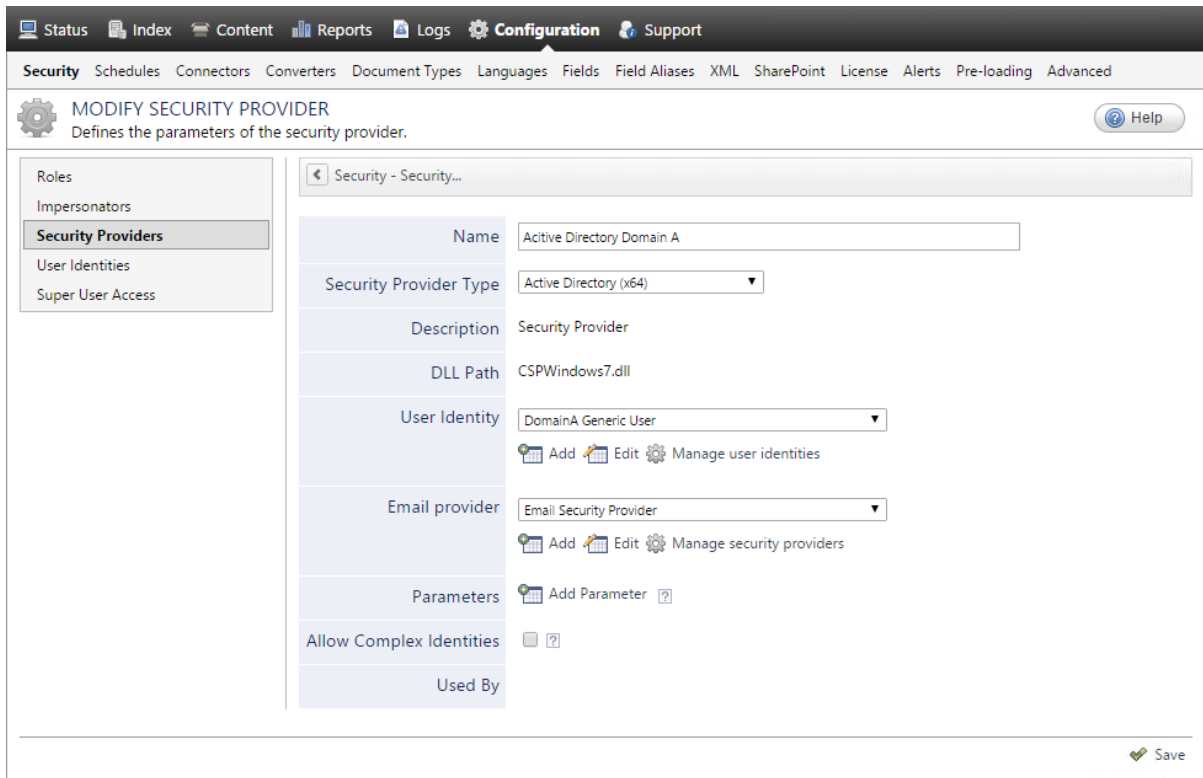
Coveo Enterprise Search (CES) comes with a default **Active Directory** security provider to which no user identity is assigned. In this case, the **Active Directory** security provider takes the CES service account as the user to access AD. When CES is in the same domain as AD, you can use the default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

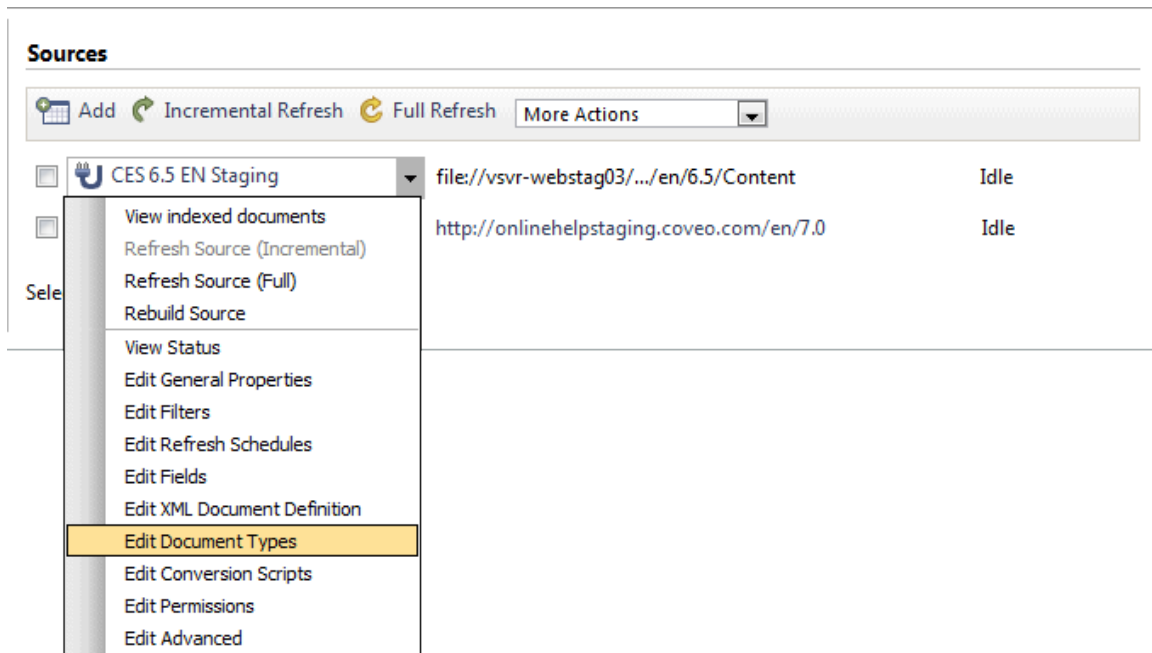
- For an Active Directory source, configure and index the source.
- To be used by another security provider, create or modify the other security provider.

## 4. Modifying the Document Type Set Used by a Source

You can create a specific document type set and associate it to a source to control how the source handles particular document types when indexing files.

To modify the document type set used by a source

1. On the Coveo server, access the Administration Tool.
2. Select **Index > Sources and Collections**.
3. In the **Sources and Collections** page:
  - a. In the **Collections** section, select the collection that contains the source that you want to modify.
  - b. In the **Sources** section, expand the drop-down list for the source that you want to modify, and then select **Edit Document Types**.



4. In the **Document Types** page corresponding to the selected source:
  - a. In the **Document Type Set** drop-down list, select the appropriate document type set.
  - b. Click **Apply Changes**.

## 5. Box Connector Deployment Overview

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

To deploy the Box connector

1. Validate that your environment meets the requirements (see ["Box Connector Requirements" on page xxxii](#)).
2. On the Box server, authorize the Coveo connector to access the content of your managed users (see ["Authorizing the Coveo Connector to Access the Box of Your Managed Users" on page xv](#)).
3. On the Coveo server, in the Coveo Administration Tool:

- a. **CES 7.0.8850+ (March 2017)** Optionally create security providers

When you want to index Box permissions, you must create two security providers to get Box item permissions and resolve and expand groups.

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

- i. Select or create an Email or an Active Directory security provider that the Box security provider will use to resolve and expand groups. The security provider type to use depends on how users are authenticated when they access the search interface:
  - When authenticated with their email address, use an Email security provider (see ["Configuring an Email Security Provider" on page vii](#)).
  - When authenticated with an Active Directory account, use an Active Directory security provider (see ["Configuring an Active Directory Security Provider" on page ix](#)).

### Notes:

- CES comes with an Active Directory security provider that you can configure to connect to the default domain. When your environment contains more than one domain, you can select an Active Directory security provider that you created for other domains.
- An Active Directory security provider is appropriate only when the User Principal Name (UPN) matches the email address for all users.

**Note:** You may require to also use a REGEX Transform Member Name security provider in between the two other security providers to map member types. Contact [Coveo Support](#) for assistance.

- ii. Create a Box security provider that the connector uses to resolve indexed permissions (see ["Configuring a Box Security Provider" on page xxix](#)).
- b. Create a Box field set to take advantage of the available Box metadata.

- i. It is recommended to start by importing the default Box field set file (`[CES_Path]\Bin\Coveo.CES.CustomCrawlers.Box.FieldSet.xml`) to create fields for all the metadata available by default from Box documents.
  - ii. When you created custom metadata for your Box documents, add corresponding fields to the field set.
- c. Configure and index a Box source.
- The connector must know details to access and index the Box content of your managed users (see ["Configuring and Indexing a Box Source" on page xx](#)).
- d. If you encounter issues, verify if modifying the default value of hidden source parameters can help resolve the problems (see ["Modifying Hidden Box Source Parameters" on page xviii](#)).

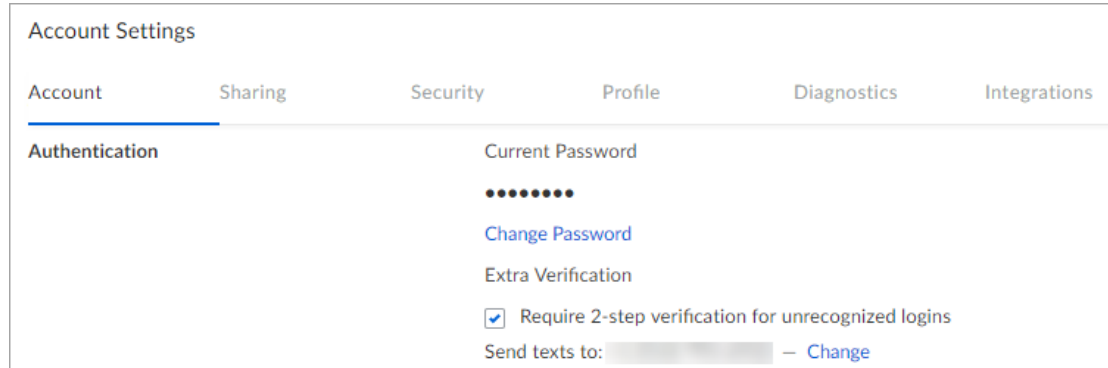
## 6. Authorizing the Coveo Connector to Access the Box of Your Managed Users

You must perform the server authentication (OAuth 2.0 with JSON Web Token) protocol to authorize the Coveo connector to access the Box content of your managed users.

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 managed users, it must acquire a client ID and a client secret. You must also create a RSA private-public keypair to sign and authenticate the JSON Web Token (JWT) assertion.

To authorize the Coveo connector to access the Box of your managed users

1. Create an application on a Box account:
  - a. Log in to [Box](#) with an administrator or developer account.
  - b. Enable two-step login verification:
    - i. In the menu on the left hand-side of the page, under **Account**, click **Admin Console**.
    - ii. On the **Admin Console** page, click the gear icon at the top right, and then click **Business Settings**.
    - iii. In the settings, click the **Custom Setup** tab.
    - iv. In the **Custom Setup** tab, next to **Company Profile**, enter a **Company Name** and a **Custom Subdomain**, and then, at the bottom of the page, click **Save**.
    - v. Click the **Security** tab.
    - vi. In the **Security** tab, under **Signup and Login**, select the **Login verification** checkbox, and then, at the bottom of the page, click **Save**.
    - vii. Access the **Account Settings** page:
      - A. At the top of the page, click **My account**.
      - B. On the **All Files** page, in the top right corner, click the drop-down menu with your initials, and then click **Account Settings**.
    - viii. On the **Account Settings** page, in the **Account** tab, under **Authentication**, click **Change**.



- ix. In the **Enable Login Verification** dialog, enter your **Country** and **Mobile Phone Number**, and then click **Continue**.  
 You should receive a verification code on your mobile phone shortly.
- x. In the **Confirmation Code** box, enter the verification code you just received, and then click **Continue**.
- c. Access the **My Apps** page, in the menu on the left-hand side of the page, by clicking **Dev Console**.
- d. In the **My Apps** page, click **Create New App**.
- e. In the **Create a New Box App** page:
  - i. Select **Custom App**, and then click **Next**.
  - ii. Select **OAuth 2.0 with JWT (Server Authentication)**, and then click **Next**.
  - iii. In the **Give your app a unique name** box, enter a descriptive application name, and then click **Create App**.
  - iv. Click **View Your App**.
- f. In the **Configuration** page:
  - i. In the **OAuth 2.0 Credentials** section, take note of the **client\_id** and **client\_secret** values.

**Note:** You will need these values when configuring the Box security provider and source (see [Configuring a Box Security Provider](#) and [Configuring and Indexing a Box Source](#)).

- ii. In the **Application Scopes** section, make sure the **Read and write all files and folders stored in Box** and **Manage groups** check boxes are selected. Optionally, if your enterprise uses the App User account feature, also select the **Manage users** check box.
- iii. In the **Advanced Features** section, make sure **Perform Actions as Users** is enabled.
- iv. In the **Add and Manage Public Keys** section, click **Generate a Public/Private Keypair** (see [Generating an RSA Keypair](#)).
- v. Save the generated `config.json` file containing your private key, as it will be required later in the Box security provider and source configuration (see [Configuring a Box Security Provider](#) and [Configuring and Indexing a Box Source](#)).



- vi. Note your **Public Key ID**, as it will be required later in the Box security provider and source configuration (see [Configuring a Box Security Provider](#) and [Configuring and Indexing a Box Source](#)).
- vii. At the top of the page, if you made changes, click **Save Changes**.
- g. Grant access to your enterprise application (see [Granting Access in Enterprise Admin Console](#)):
  - i. In the menu on the left hand-side of the page, click **My Apps**.
  - ii. In the menu on the left hand-side of the page, under **Account**, click **Admin Console**.
  - iii. On the **Admin Console** page, click the gear icon at the top right, and then click **Business Settings**.
  - iv. Click the **Apps** tab.
  - v. In the **Apps** tab, under **Custom Applications**, click **Authorize New App**.
  - vi. In the **App Authorization** dialog that appears, enter your app **client\_id** that you noted previously, and then click **Next** (see [client\\_id](#)).
  - vii. Click **Authorize**.

### What's Next?

- Create a Box security provider ("[Configuring a Box Security Provider](#)" on page xxix).
- Create a Box source ("[Configuring and Indexing a Box Source](#)" on page xx).

## 7. Modifying Hidden Box 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 Box 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 Box sources. The parameter type (integer, string, etc.) appears between parentheses following the parameter name.

### **RetrieveGlobalFileMetadata (Integer)**

Whether to retrieve the global metadata (properties) of files. The default value is `false`.

### **RetrieveFileCommentsMetadata (Integer)**

Whether to retrieve the file comments as a metadata. The default value is `false`.

### **IgnoreSharedLinkPermissions (Boolean)** CES 7.0.8850+ (March 2017) Security provider

Whether to ignore Shared Link permissions. The default value is `true`.

**Important:** Setting this parameter to `false` can potentially expose sensitive information as all documents that were shared using a Share Link will be considered public.

### **IgnoreSharedLinkPasswordProtection (Integer)** CES 7.0.8850+ (March 2017) Security provider

Whether to ignore Shared Link password protection when `IgnoreSharedLinkPermissions` is `false`. The default value is `false`.

To modify hidden Box source parameters

1. Refer to "[Adding an Explicit Connector Parameter](#)" on page iv to add one or more Box source parameters.
2. For a new Box 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 Box 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 Box 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 Box source to apply the changes to the parameters.

## 8. Configuring and Indexing a Box Source

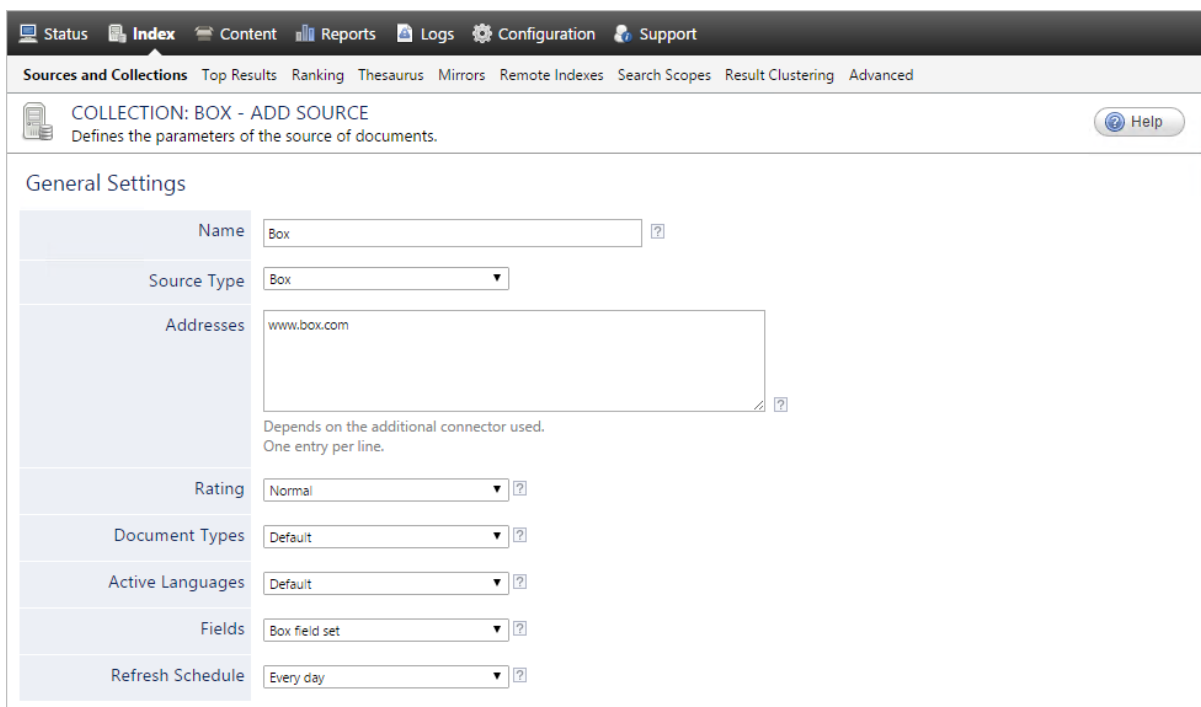
A source defines a set of configuration parameters for a specific Box account.

To configure and index a Box 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:



The screenshot shows the 'Add Source' configuration page for a Box collection. The page is titled 'COLLECTION: BOX - ADD SOURCE' and includes a 'Help' button. The 'General Settings' section contains the following fields:

- Name:** Box
- Source Type:** Box
- Addresses:** www.box.com
- Rating:** Normal
- Document Types:** Default
- Active Languages:** Default
- Fields:** Box field set
- 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:** `Box`

### Source Type

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

**Note:** If you do not see **Box**, your environment does not meet the requirements (see "[Box Connector Requirements](#)" on page xxxii).

### Addresses

This parameter is not used, but must not be empty. Enter `http://www.box.com`.

### Fields

Select the field set that you created earlier (see [Box 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**.

- 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:

### Specific Connector Parameters & Options

Client ID	<input type="text"/>	<a href="#">?</a>
Client Secret	<input type="password"/>	<a href="#">?</a>
Refresh Token	<input type="password"/>	<a href="#">?</a>
Enterprise ID	<input type="text"/>	<a href="#">?</a>
Public Key ID	<input type="text"/>	<a href="#">?</a>
Private Key File	<input type="text"/>	<a href="#">?</a>
Private Key Password	<input type="password"/>	<a href="#">?</a>
Number of Refresh Threads	<input type="text" value="8"/>	<a href="#">?</a>
Index Managed Users' Content	<input type="checkbox"/>	<a href="#">?</a>
Index Custom File Metadata	<input type="checkbox"/>	<a href="#">?</a>
Index users	<input type="checkbox"/>	<a href="#">?</a>
Parameters	<input type="button" value="Add Parameter"/> <a href="#">?</a>	
Option	<input checked="" type="checkbox"/> Index subfolders <a href="#">?</a> <input type="checkbox"/> Index the document's metadata <a href="#">?</a> <input type="checkbox"/> Document's addresses are case-sensitive <a href="#">?</a> <input checked="" type="checkbox"/> Generate a cached HTML version of indexed documents <a href="#">?</a> <input type="checkbox"/> Open results with cached version <a href="#">?</a>	

- a. Using the following parameters, authorize the Coveo crawler to access the content of your managed users:

**Client ID** Security provider

Enter the client identifier to use that you previously obtained (see [Authorizing the Coveo Connector to Access the Box of Your Managed Users](#)).

**Client Secret** Security provider

Enter the client secret to use that you previously obtained (see [Authorizing the Coveo Connector to Access the Box of Your Managed Users](#)).

**Refresh Token**

The parameter is not needed when indexing Box Enterprise content.

**Enterprise ID** CES 7.0.8850+ (March 2017)

Enter the enterprise identifier as displayed in your Box Enterprise Settings page. It must be the same ID that you entered when configuring the security provider (see [Configuring a Box Security Provider](#)).

**Public Key ID** CES 7.0.8850+ (March 2017) Security provider

Enter the public key unique identifier you previously obtained (see [Authorizing the Coveo Connector to Access the Box of Your Managed Users](#)). It must be the same ID that you entered when configuring the security provider (see [Configuring a Box Security Provider](#)).

### Private Key File **CES 7.0.8850+ (March 2017)** **Security provider**

Enter the full path of the valid PEM private key file you previously obtained (see [Authorizing the Coveo Connector to Access the Box of Your Managed Users](#)). It must be the same file path that you entered when configuring the security provider (see [Configuring a Box Security Provider](#)).

- b. The default value for the following parameter generally does not need to be changed:

#### Number of refresh threads

Determines the number of files that the connector can refresh simultaneously. The default and recommended value is 8.

- c. The following option must be selected for your managed users content to be indexed.

#### Index Managed Users' Content

**Note:** **CES 7.0.9093– (September 2017)** The parameter was labeled **Index All Managed Users**.

Whether the content of all your managed users should be indexed. When the option is cleared, only your content is indexed.

- d. **CES 7.0.9167+ (December 2017)** When you want Box users to be indexed as separate documents, select the following option:

#### Index Users

- e. Select additional content to be indexed using the following option:

#### Index Custom File Metadata

Whether the custom metadata specified in the Global Properties should be indexed.

- f. (Optional) Click **Add Parameter** when you want to show and change the value of advanced source parameters (see ["Modifying Hidden Box Source Parameters" on page xviii](#)).
- g. 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

Ensure that this option is selected because Dropbox team member IDs are case sensitive.

### 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**.

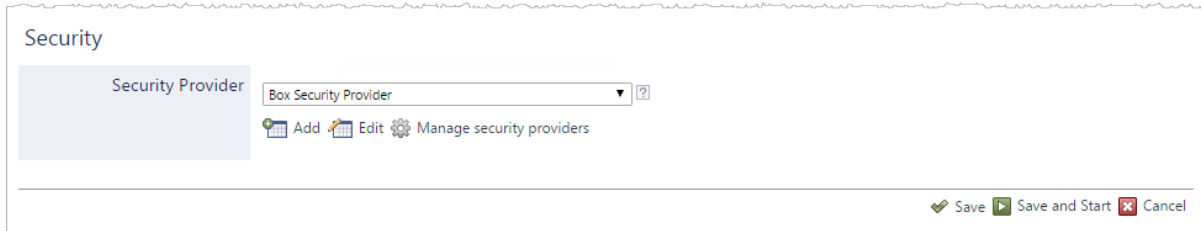
7. When you chose to index Box permissions, in the **Security** section, in the **Security Provider** drop-down list, select the Box security provider that you created for this source (see "[Configuring a Box Security Provider](#)" on page xxix).

**Note:** **CES 7.0.8691– (December 2016)** Since the Box permission model is not supported, select **(none)**.

**Important:** The connector does not support Box permissions. It is thus strongly recommended to only index Box accounts with public content.

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





8. Click **Save** to save the source configuration.
9. When your Box content is all public or when you use **CES 7.0.8691– (December 2016)**:
  - 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 Box 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 Box Source Parameters](#)" on page xviii).

## 9. Box Connector

**CES 7.0.7814+ (August 2015)**

The Coveo connector for Box allows Coveo administrators to index and integrate the Box content of their managed users into the Coveo unified index. The connector indexes all items and the attached permissions from all managed users so that in Coveo search interfaces, a user can easily find any but only content to which he has access in Box.

### 9.1 Connector Features Summary

Features		Supported	Additional information
Box version		Latest cloud version	Following available Box releases
Searchable content types		✓	Enterprises, users, folders, files, and web links
Content update	Incremental refresh	✓	Full refresh or rebuild needed to: <ul style="list-style-type: none"> <li>Remove deleted users in Box</li> <li>Update the subitems of a renamed folder</li> </ul>
	Full refresh	✓	
	Rebuild	✓	
Document-level security		✓	<p><b>CES 7.0.8850+ (March 2017)</b> Support Box permissions.</p> <p><b>Note:</b> <b>CES 7.0.8691– (December 2016)</b> Permissions can only be defined manually on source level <a href="#">[more]</a></p>

### 9.2 Features

The Box connector features are:

#### Content indexing

Extraction and indexing of the following Box item types:

- Enterprise
- Users
- Folders
- Files
- Web links

**Mostly supported security model** CES 7.0.8850+ (March 2017)

The connector mostly supports the Box security model using a security provider to get almost all permissions for each indexed item. This means that, in Coveo search interfaces, a user searching Box content only sees the content to which he has access except items that the user can see using shared links.

**Note:** By default, shared link permissions are ignored, meaning that a document only shared with a link is only visible by its owner in your Coveo search interface. Contact [Coveo Support](#) for assistance on how to take shared link permissions into account.

**Incremental refresh**

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

**Note:** Some changes need a full refresh or a source rebuild to be taken into account (see [Limitations](#)).

**Multithreading**

The connector can run multiple threads, which can improve performances considerably (see [Configuring and Indexing a Box Source](#)).

**Pause/Resume**

When indexing Box content, the connector can be paused and resumed.

## 9.3 Limitations

- Limited incremental capabilities:
  - A full refresh or rebuild is needed to remove deleted users in Box.
  - A full refresh or rebuild is needed to update the subitems of a renamed folder.
  - CES 7.0.8047– (December 2015) When an incremental refresh captures the deletion of a folder in which a collaboration or shared event occur, a warning ("Exception during item expansion") is thrown.
  - CES 7.0.7914– (October 2015) A full refresh or rebuild is needed to retrieve the content (folder and documents) added by a new user in Box.

- Shared link changes are not yet updated.
- CES 7.0.8691– (December 2016) The connector does not support Box permissions.

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

- CES 7.0.8047– (December 2015) Google docs and Google sheets are not indexed by default. The workaround is to add the Google docs and Google sheet document types manually to the Document Type set used by your Box source (see "[Modifying the Document Type Set Used by a Source](#)" on page xii).
- CES 7.0.7914– (October 2015) Deleting the folder that represents a specific user in the Index browser is not

possible.

## Feature History

CES version	Monthly release	Features
7.0.8850	March 2017	Box Enterprise support
7.0.7814	August 2015	Connector introduction

## What's Next?

Review the steps to deploy the Box connector (see ["Box Connector Deployment Overview"](#) on page xiii).

## 10. Configuring a Box Security Provider

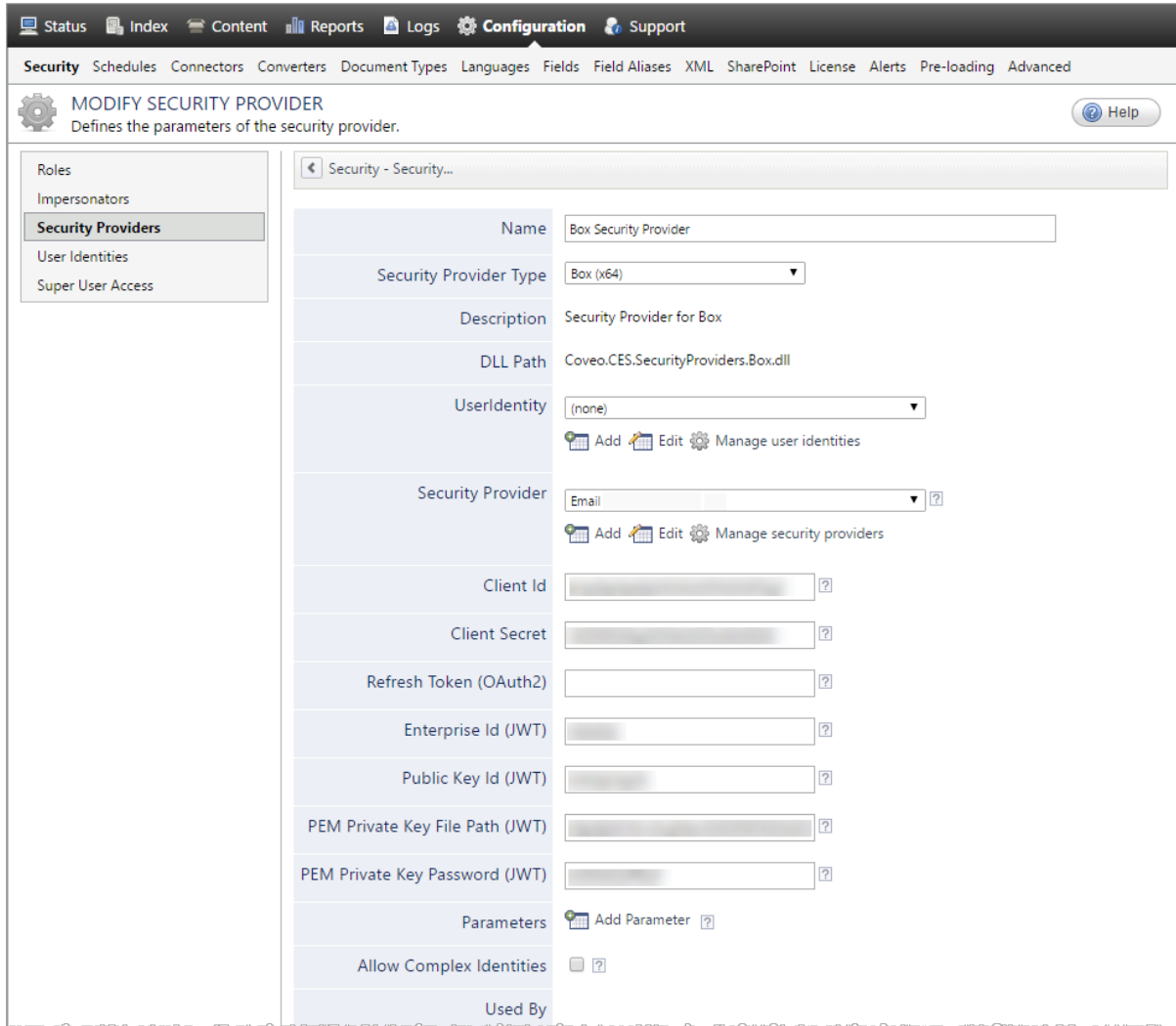
CES 7.0.8850+ (March 2017)

The Coveo Box connector mostly supports the Box security model (see [Shared Link Limitation](#)). When you want users searching for Box content in a Coveo search interface to only see the content to which they have access in Box, the connector needs a security provider to be able to index the permissions for each indexed Box item.

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

To configure a Box security provider

1. On the Coveo server, access the Administration Tool.
2. Click **Configuration**, and then **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:** Box Security Provider

**Security Provider Type**

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

**User Identity**

In the drop-down list, select **(none)**.

**Security Provider**

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

**Client Id** [Source](#)

The client identifier to use that you previously obtained (see [Authorizing the Coveo Connector to Access the Box of Your Managed Users](#)).

**Client Secret** [Source](#)

The client secret to use that you previously obtained (see [Authorizing the Coveo Connector to Access the Box of Your Managed Users](#)).

**Enterprise ID** [Source](#)

The Box Enterprise unique identifier as displayed in your Box Enterprise Admin Console **Business Settings** page and on the app **General** settings page.

**Public Key ID** [Source](#)

The public key unique identifier that you previously obtained (see [Authorizing the Coveo Connector to Access the Box of Your Managed Users](#)).

**Private Key File** [Source](#)

The full path of the valid PEM private key file that you previously obtained (see [Authorizing the Coveo Connector to Access the Box of Your Managed Users](#)).

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

## What's Next?

Create and index a source (see "[Configuring and Indexing a Box Source](#)" on page xx).

## 11. Box Connector Requirements

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

- [CES 7.0.7814+ \(August 2015\)](#)

- Coveo license for the Box connector

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

- A valid Box Enterprise or Box Business admin, or [developer account](#)

Using a Box Enterprise or Box Business admin, or [developer account](#), you must create a [Box app](#) and set up an OAuth 2.0 protocol to authorize Coveo to access the Box content of your managed users (see "[Authorizing the Coveo Connector to Access the Box of Your Managed Users](#)" on page xv).

### What's Next?

Grant Coveo access to the Box content of your managed users by creating a Box application (see "[Authorizing the Coveo Connector to Access the Box of Your Managed Users](#)" on page xv).