Coveo Platform 7.0

Oracle Knowledge 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-141204-EN
Publication date:	1/3/2019

Table of Contents

1. Oracle Knowledge Connector

CES 7.0.7256+ (December 2014)

The Coveo connector for Oracle Knowledge (formerly known as InQuira Knowledge Management) allows you to index and integrate the content of your Oracle Knowledge instance into your Coveo unified index, making it easily searchable by end-users.

1.1 Features

- Content Indexing

  Retrieval and indexing of the following Oracle Knowledge items:

  - Content channel
  - Content record
  - Content record attachment
  - Discussion board
  - Forum
  - Topics and messages

    Note: The attachments of the topics and messages are not retrievable by the Oracle Knowledge APIs.

- Security

  The connector supports Oracle Knowledge security model by indexing Oracle Knowledge item permissions so that in Coveo search interfaces, a user searching Oracle Knowledge content only sees the content to which he has access in Oracle Knowledge.

- Pause/Resume

  When indexing an Oracle Knowledge instance, the connector can be paused and resumed.

- Partial Incremental Refresh

  Updated documents in a repository (content/security) are periodically re-indexed by the connector (see "Configuring and Indexing an Oracle Knowledge Source" on page 15).

  Note: Some deleted and unpublished items require a full refresh to be taken in account (see "Limitation" on page 1).

1.2 Limitation

- Limited incremental refresh capabilities:

  - A full refresh is needed to update deleted items
  - A full refresh is needed to update changes on unpublished content records

What's Next?

Get familiar with the connector deployment steps (see "Oracle Knowledge Connector Deployment Overview" on page 3).

2. Oracle Knowledge Connector Deployment Overview

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

To deploy the Oracle Knowledge connector

1. Validate that your environment meets the requirements (see "Oracle Knowledge Connector Requirements" on page 5).
2. On the Oracle Knowledge instance, create a Knowledge Administrator user to be used as a crawling account (see Create a Knowledge Administrator).
3. On the machine hosting Oracle Knowledge, copy the `IQServiceClientCS.dll` file located in the `MSFT` folder.

   Example: `C:\Oracle\Knowledge\IM\InfoManager\clientLibrary\MSFT\Release`

4. On the machine hosting CES, paste the `IQServiceClientCS.dll` file in the `Bin` folder of CES.

   Example: `C:\Program Files\Coveo Enterprise Search 7\Bin`

5. On the Coveo server:

   a. Create a user identity.

      The connector needs an account that has at least read access to all item types and security permissions of the Oracle Knowledge instance. Create a CES user identity that must contain the credentials (username and password) of a console user with one or more security roles (custom or built-in) allowing him to view all content and permissions of the Information Manager repository you want to index (see "Adding a User Identity" on page 6).

   b. (Optional) Create security providers

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

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

      i. Start by selecting or creating an Email or an Active Directory security provider that the Oracle Knowledge 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 10).
         - When authenticated with an Active Directory account, use an Active Directory security provider

(see "Configuring an Active Directory Security Provider" on page 12).

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. Then create an Oracle Knowledge security provider that the connector uses to resolve indexed permissions (see "Configuring an Oracle Knowledge Security Provider" on page 8).

c. Create an Oracle Knowledge field set.

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

d. Configure and index the Oracle Knowledge source.

The Coveo connector needs to know details about your Oracle Knowledge instance to be able to index its content (see "Configuring and Indexing an Oracle Knowledge Source" on page 15).

3. Oracle Knowledge Connector Requirements

Your environment must meet the following requirements to be able to use the Coveo connector for Oracle Knowledge:

- CES 7.0.7256+ (December 2014)
- Coveo license for the Oracle Knowledge connector

  Your Coveo license must include support for the Oracle Knowledge connector to be able to use this connector.
- Supported Oracle Knowledge version

  The connector supports Oracle Knowledge 8.4.2.2 to 8.5.1 installations.

What's Next?

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

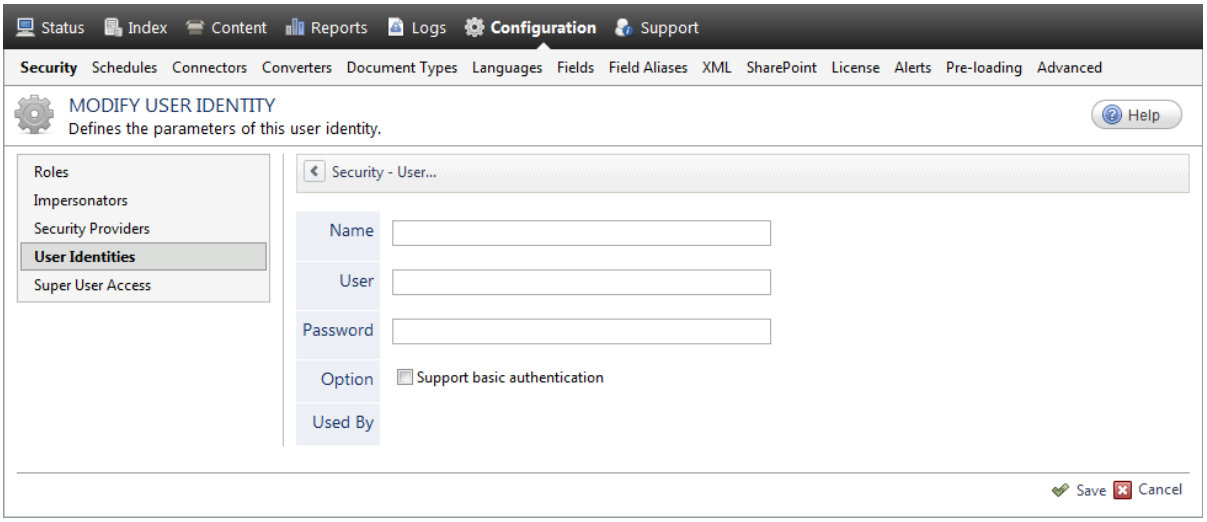
4. Adding a User Identity

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.

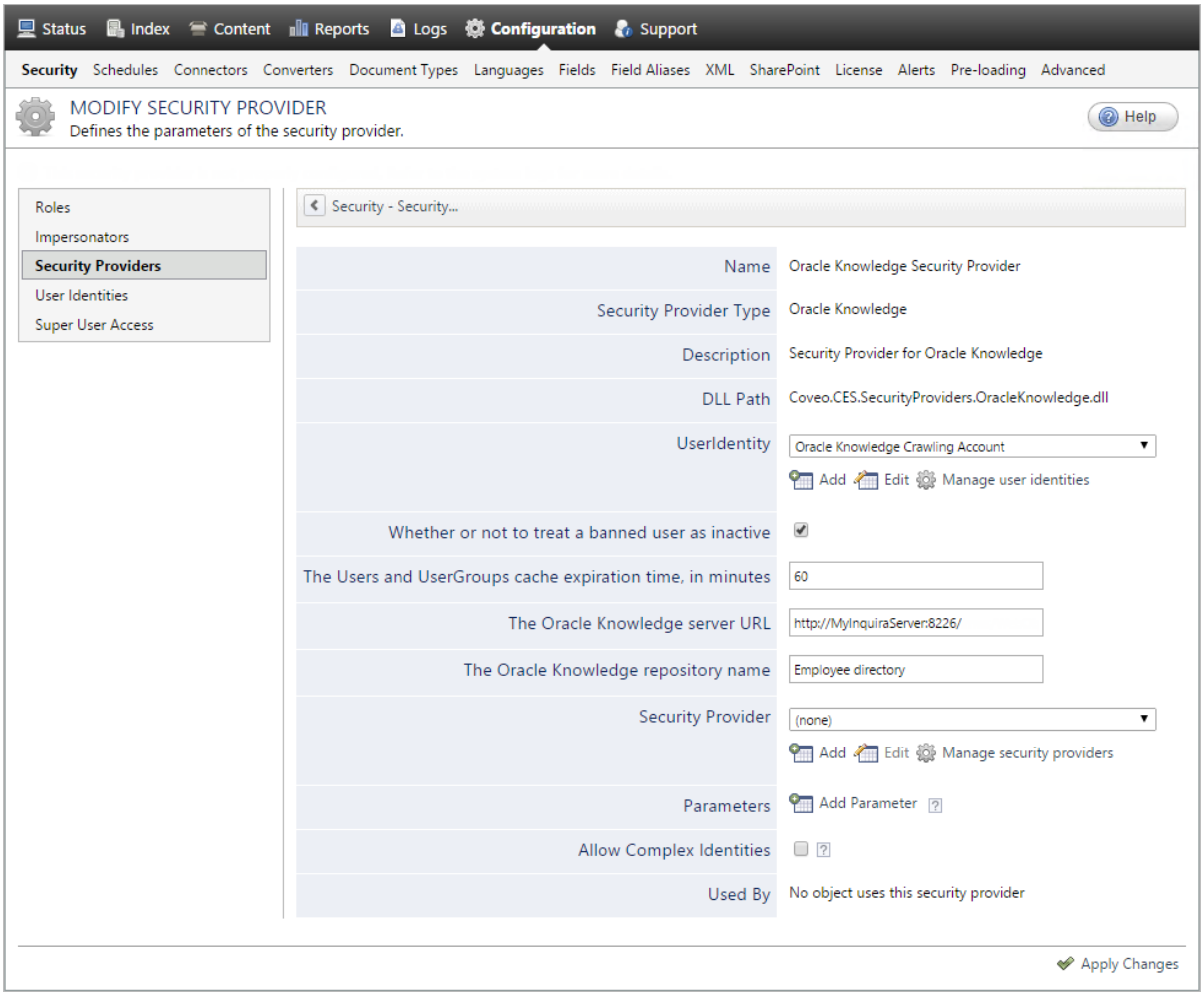
5. Configuring an Oracle Knowledge Security Provider

When you choose to index permissions associated with Oracle Knowledge items, the Coveo connector needs a security provider. When permissions are indexed, in Coveo search results, a user searching for Oracle Knowledge content only sees the content to which he has access in Oracle Knowledge.

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

To configure an Oracle Knowledge 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	Oracle Knowledge Security Provider
Security Provider Type	Oracle Knowledge
Description	Security Provider for Oracle Knowledge
DLL Path	Coveo.CES.SecurityProviders.OracleKnowledge.dll
UserIdentity	Oracle Knowledge Crawling Account
Whether or not to treat a banned user as inactive	☑
The Users and UserGroups cache expiration time, in minutes	60
The Oracle Knowledge server URL	http://MyInquiraServer:8226/
The Oracle Knowledge repository name	Employee directory
Security Provider	(none)
Parameters	
Allow Complex Identities	☐
Used By	No object uses this security provider

a. Configure the following required parameters:

Name

Choose a significant name to identify the security provider.

Example: `Oracle Knowledge Security Provider`

Security Provider Type

Select **Oracle Knowledge (x64)**.

User Identity

Select the Oracle Knowledge user identity that you created previously.

The Oracle Knowledge server URL

Enter the URL to the client API web service.

Example: `http://MyInquiraServer:8226`.

The connector auto-filled this URL with `/imws/WebObjects/imws.woa/ws/RequestProcessor`.

The Oracle Knowledge repository name

Enter the name of the Information Manager repository to index.

Note: The repository name is the same value that you enter in the Repository box when you log in to you Oracle Knowledge Information Manager.

Security Provider

When you want to index Oracle Knowledge security permissions, select the security provider that you selected or created to allow this security provider to resolve and expand the groups (see Oracle Knowledge Connector Deployment Overview).

b. Review the default value of the following check box:

Whether to treat a banned user as inactive

Whether to treat a banned user as inactive. By default, banned users are treat as active.

c. Review if you need to change the default values for the following parameter:

The Users and UserGroups cache expiration time

Enter the time before a cached object is marked as expirated and must be reindexed. The default value is `60` min.

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

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

f. Click **Apply Changes**.

What's Next?

Configure and index an Oracle Knowledge source (see "Configuring and Indexing an Oracle Knowledge Source" on page 15).

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

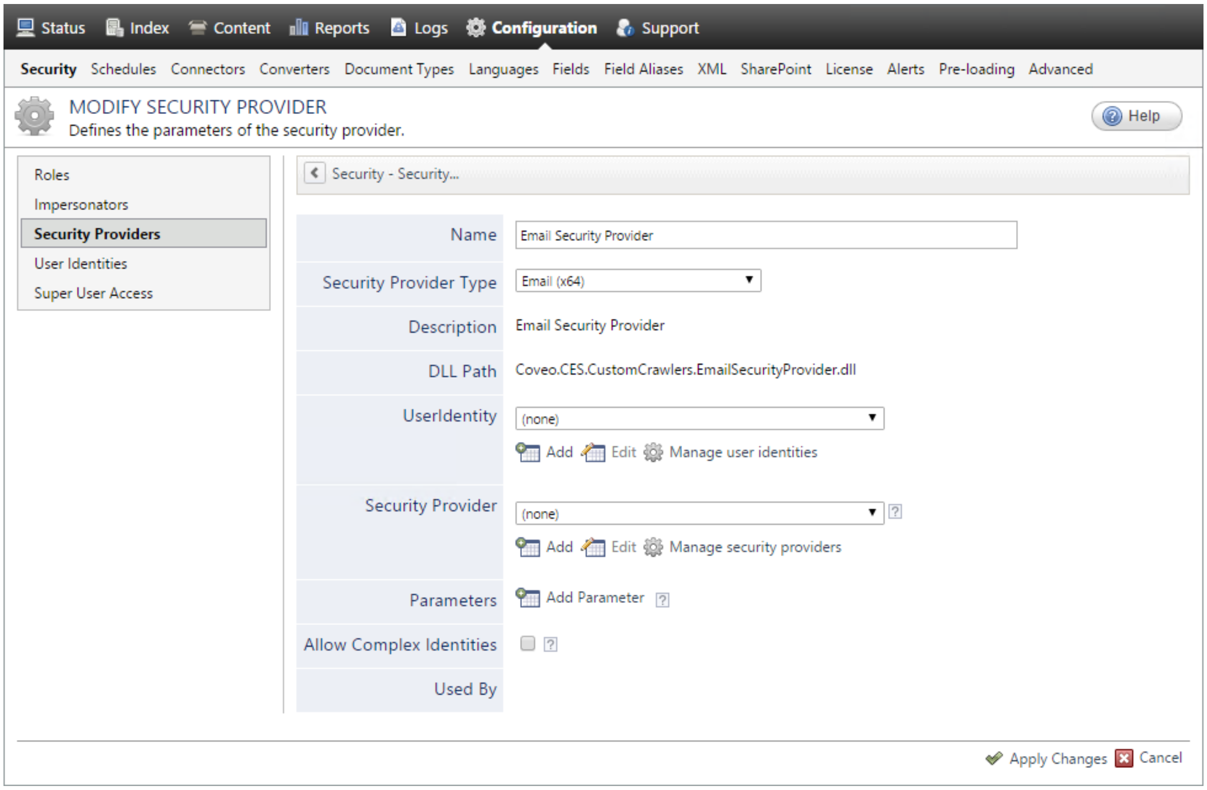
1. On the Coveo server, access the Administration Tool.

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:



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.

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.

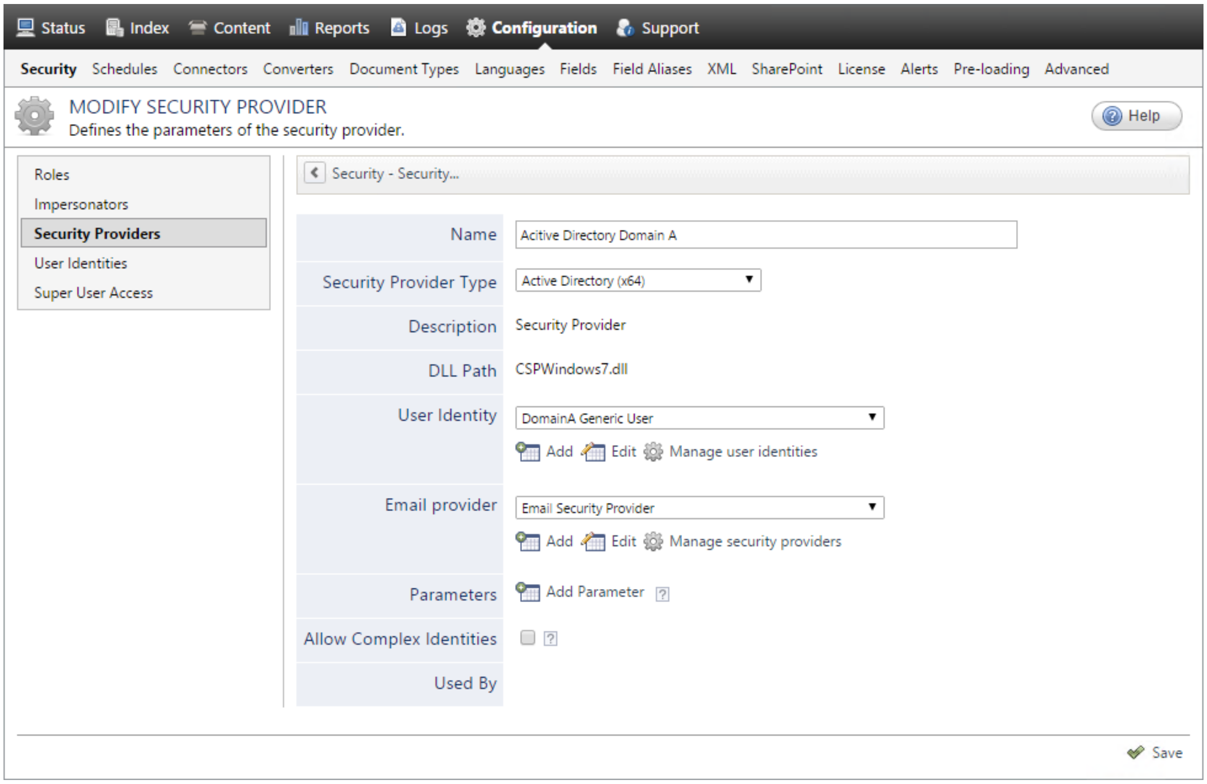
Note: You can get familiar with how Coveo components deal with permissions on documents both at indexing and query time.

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:



Name	Active Directory Domain A
Security Provider Type	Active Directory (x64)
Description	Security Provider
DLL Path	CSPWindows7.dll
User Identity	DomainA Generic User
Email provider	Email Security Provider
Parameters	
Allow Complex Identities	□
Used By	

   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 an Oracle Knowledge Source

A source defines a set of configuration parameters for a specific Oracle Knowledge instance. When you want to index more than one Information Manager repository, configure one source per repository.

To configure and index an Oracle Knowledge 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.

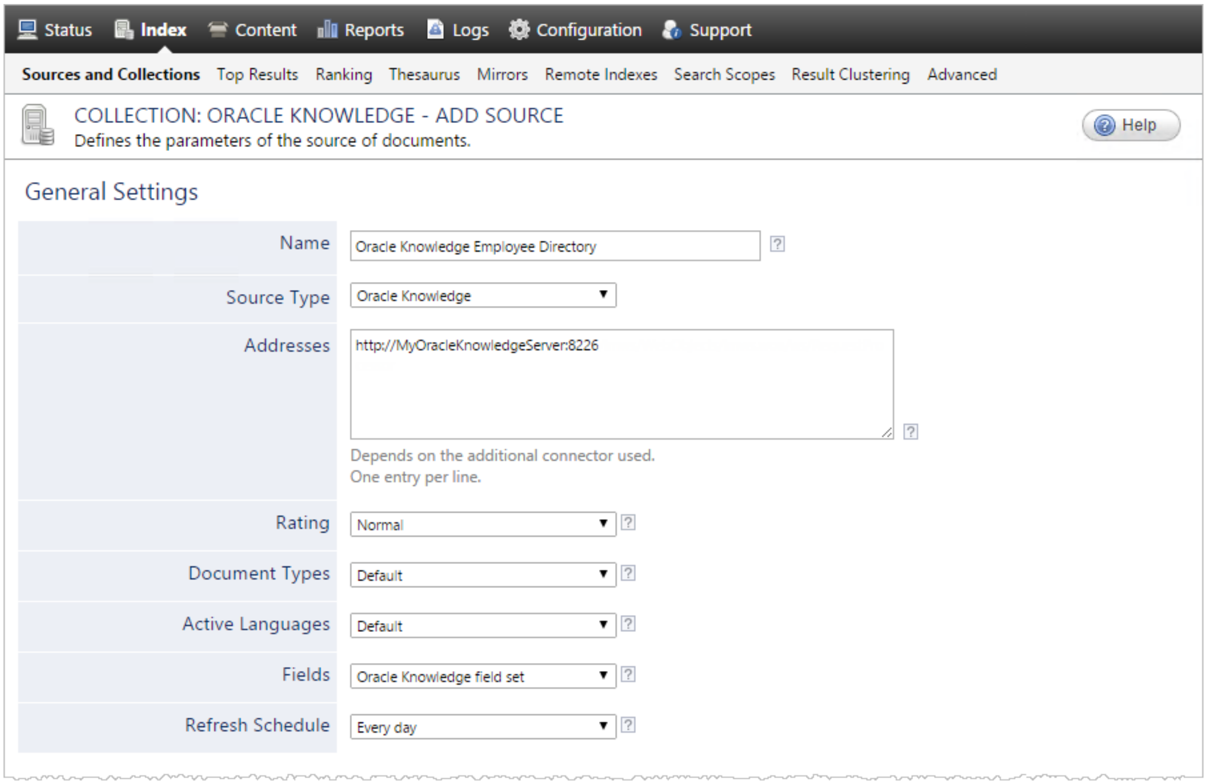
    OR

    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: ORACLE KNOWLEDGE - ADD SOURCE
Defines the parameters of the source of documents.

General Settings

Name	Oracle Knowledge Employee Directory
Source Type	Oracle Knowledge
Addresses	http://MyOracleKnowledgeServer:8226 Depends on the additional connector used. One entry per line.
Rating	Normal
Document Types	Default
Active Languages	Default
Fields	Oracle Knowledge field set
Refresh Schedule	Every day

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

Name

A descriptive name of your choice for the connector source.

Example: `Oracle Knowledge Employee Directory`

Source Type

The connector used by this source. In this case, select **Oracle Knowledge**.

Note: If you do not see **Oracle Knowledge** in the **Source Type** list, ensure that your environment meets the requirements (see "Oracle Knowledge Connector Requirements" on page 5).

Addresses

Enter the base URL of your Oracle Knowledge server.

Examples: `http://MyOracleKnowledgeServer:8226/`

Important: The starting address specified here must match the one entered in the security provider configuration page (see Configuring an Oracle Knowledge Security Provider).

Fields

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

b. The following parameters often do not need to be changed:

Rating

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

Example: When the source indexes a legacy repository, you may want to set this parameter to **Low**, so that in the search interface, results from this source appear lower in the list compared to those from active repository sources.

Document Types

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

Active Languages

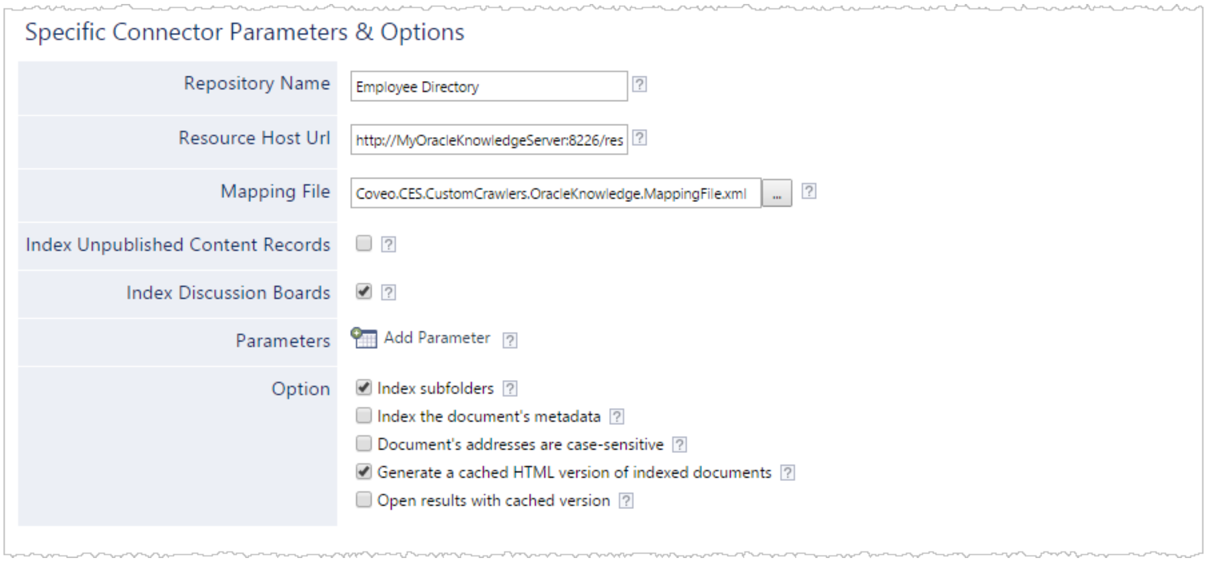
If you defined custom active language sets, ensure to select the most appropriate for this source.

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.

Note: The full refresh is a safety net to ensure all modifications are taken into account (see Oracle Knowledge Incremental Refresh Limitations).

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



Specific Connector Parameters & Options

Repository Name	Employee Directory
Resource Host Url	http://MyOracleKnowledgeServer:8226/res
Mapping File	Coveo.CES.CustomCrawlers.OracleKnowledge.MappingFile.xml
Index Unpublished Content Records	□
Index Discussion Boards	☑
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. Enter the appropriate value for the following required parameters:

Repository Name

Enter the name of the Information Manager repository to index.

Note: The repository name is the same value that you enter in the Repository box when you log in to you Oracle Knowledge Information Manager.

Example: `Employee Directory`

Important: The repository name specified must match the one entered in the security provider configuration page (see Configuring an Oracle Knowledge Security Provider).

Resource Host URL

Enter the root URL of the Oracle Knowledge server resources.

Example: `http://MyOracleKnowledgeServer:8226/resources/`

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. Review if you need to change the default values for the following options:

Index Unpublished Content Records

Whether to index the latest version of the content records, even if the version is unpublished. By default, only the latest published version is indexed.

Index Discussion Boards

Whether to index discussion boards. By default, discussion boards are indexed.

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

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

Index Subfolders

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

Index the document's metadata

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

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

Example: A document has two metadata:

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

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

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

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

Document's addresses are case-sensitive

Leave the check box cleared. This parameter needs to be checked only in rare cases for systems in which distinct documents may have the same name but different casing.

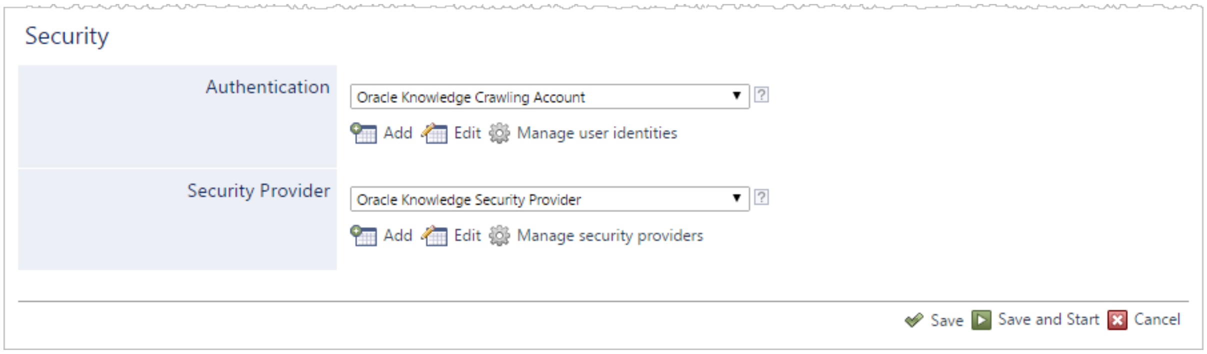
Generate a cached HTML version of indexed documents

When you select this check box (recommended), at indexing time, CES creates HTML versions of indexed documents. In the search interfaces, users can then more rapidly review the content by clicking the **Quick View** link rather than opening the original document with the original application. Consider clearing this check box only when you do not want to use **Quick View** links or to save resources when building the source.

Open results with cached version

Leave this check box cleared (recommended) so that in the search interfaces, the main search result link opens the original document with the original application. Consider selecting this check box only when you do not want users to be able to open the original document but only see the HTML version of the document as a Quick View. In this case, you must also select **Generate a cached HTML version of indexed documents**.

7. In the **Security** section of the **Add Source** page:



Security

Authentication: Oracle Knowledge Crawling Account

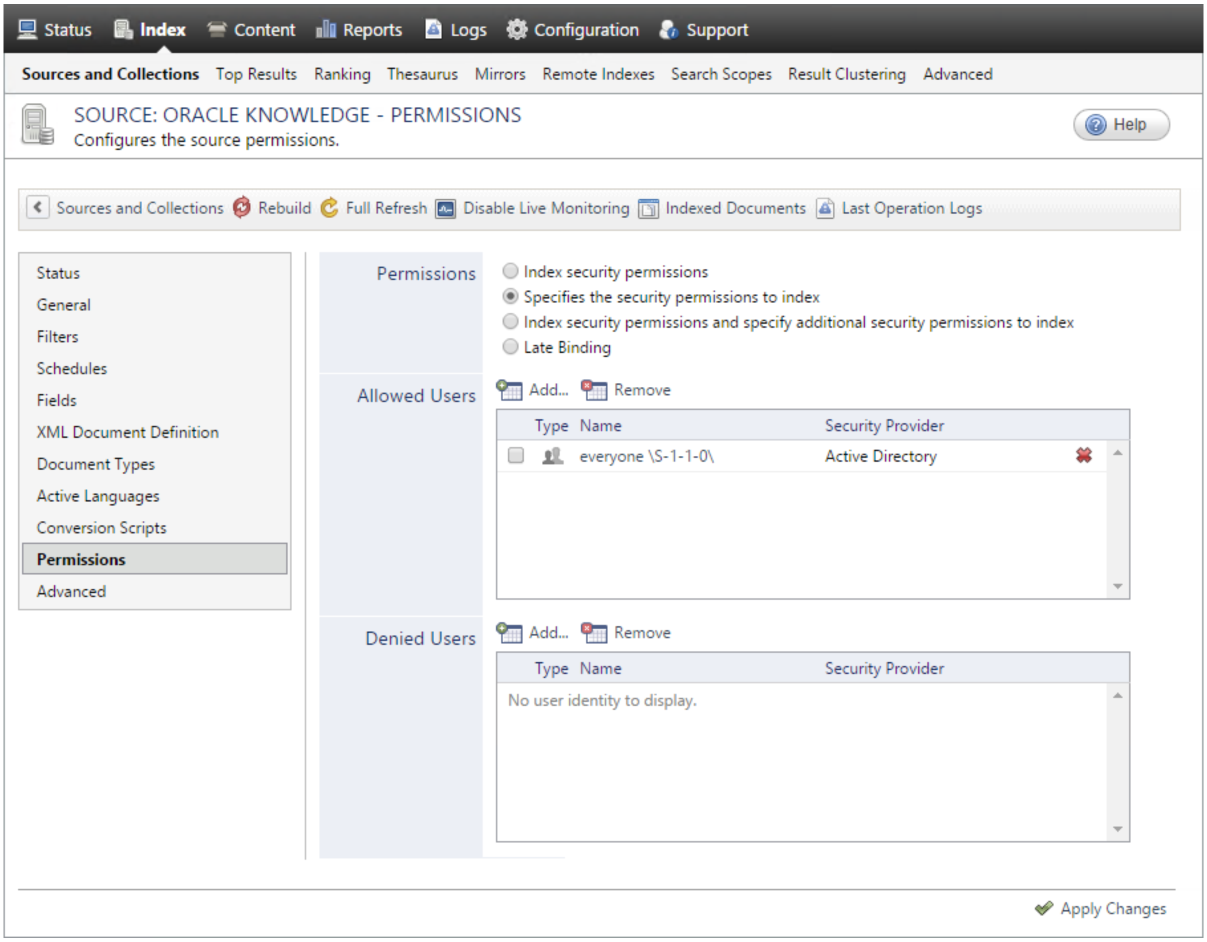
Security Provider: Oracle Knowledge Security Provider

   a. In the **Authentication** drop-down list, select the Oracle Knowledge crawling user identity that you created for this source (see Oracle Knowledge Connector Deployment Overview).

   b. In the **Security Provider** drop-down list, if you chose to index permissions, select the Oracle Knowledge security provider that you created for this source (see "Configuring an Oracle Knowledge Security Provider" on page 8). Otherwise, select **None**.

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

8. In the case your Oracle Knowledge content is all public and you chose to not index Oracle Knowledge permissions:



SOURCE: ORACLE KNOWLEDGE - PERMISSIONS

Configures the source permissions.

Permissions

○ Index security permissions
● Specifies the security permissions to index
○ Index security permissions and specify additional security permissions to index
○ Late Binding

Allowed Users

	Type	Name	Security Provider	
□	👥	everyone \S-1-1-0\	Active Directory	✖

Denied Users

Type	Name	Security Provider
No user identity to display.		

a. In the navigation menu on the left, select **Permissions**.

b. Next to **Permissions**, select the **Specifies the security permissions to index** option.

c. Next to **Allowed Users**, ensure that a well-known everyone group such as the Active Directory `everyone \S-1-1-0\` is added.

d. Click **Apply Changes**.

9. 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?

Consider modifying advanced source parameters (see "Modifying Hidden Oracle Knowledge Source Parameters" on page 21).

6.1 Modifying Hidden Oracle Knowledge 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 Oracle Knowledge 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 Oracle Knowledge sources. The parameter type (integer, string…) appears between parentheses following the parameter name.

DiscussionBoardCrawlerWebServiceUrl (String)

The URL to the discussion board hidden crawler. Auto-filled with the starting address. The default and recommended value is `http://MyOracleKnowlegeServer:8086/InfoManager/WebObjects/InfoManager.woa/ws/DiscussionBoardCrawler`.

ClientAPIWebServiceUrl (String)

The URL to the client API web service. The default and recommended value is `http://MyOracleKnowlegeServer:8086/`.

> **Note:** The connector auto-filled the value with `imws/WebObjects/imws.woa/ws/RequestProcessor`.

Locales (String)

The specific languages of the content to index, separated by semi-colons i.e.: `en_US;fr_FR`. The default value is `null`, meaning that the connector indexes all locales.

> **Example:** When you only want to index English documents, enter `en_US` .

ItemTypesToIgnore (String)

The type of Oracle Knowledge items to ignore while indexing, separated by semi-colons. The default value is `null`, meaning that the connector indexes all item types. Possible values are: `Channel`, `ContentRecord`, `ContentRecordAttachment`, `DBForum`, `DBMessage`, `DPTopic`, `DiscussionBoard` and `Repository`.

ChannelReferenceKeys (String) CES 7.0.7338+ (January 2015)

The Oracle Knowledge channels to index, identified by their reference keys and separated by semi-colons. The default value is `null`, meaning that the connector indexes all channels.

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

To modify hidden Oracle Knowledge source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 22 to add one or more Oracle Knowledge hidden source parameters.

2. For a new Oracle Knowledge 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 Oracle Knowledge 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 Oracle Knowledge 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 Oracle Knowledge 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.

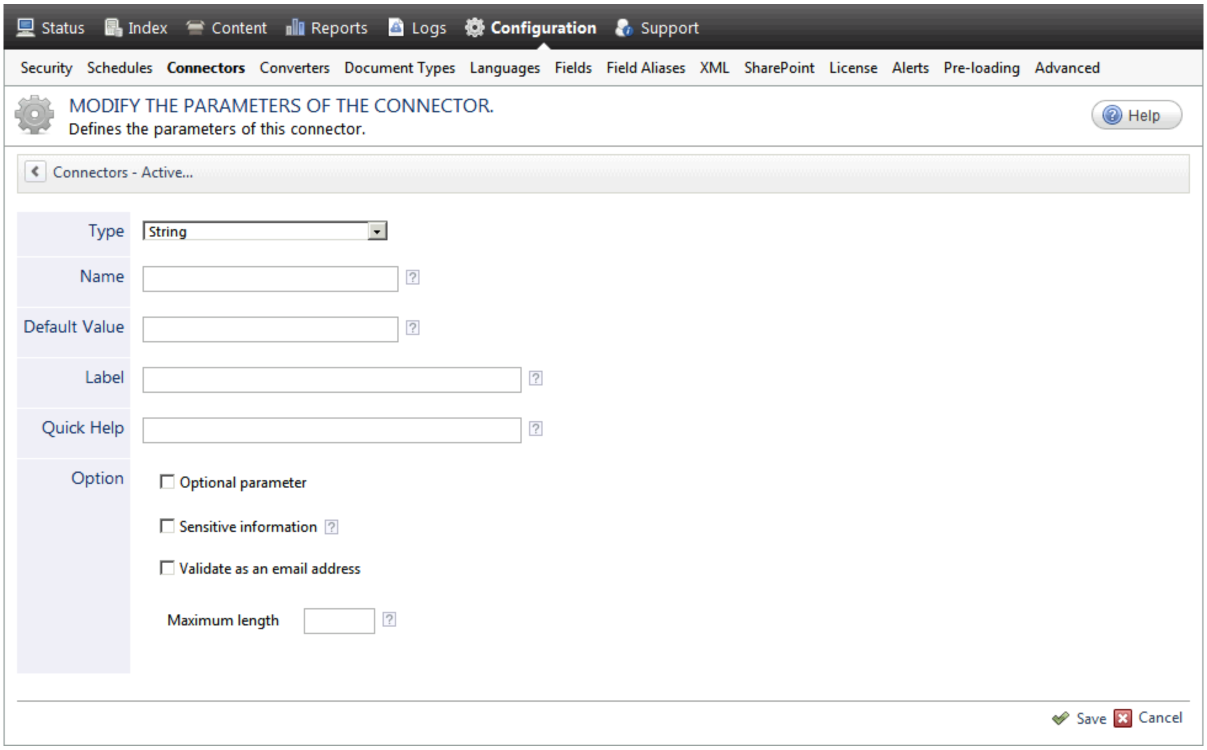
2. Select **Configuration** > **Connectors**.

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:



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.

7. Troubleshooting Oracle Knowledge Connector Issues

When configuring a security provider, the following error is displayed and the security provider is stated as Invalid:

```
An error occurred while initializing the Blade "Oracle Knowledge Security Provider" (ID
#37): Unexpected exception in method 'InitBlade': System.IO.FileLoadException: Could not
load file or assembly 'IQServiceClientCS. Version=8.1.1.32620. Culture=neutral. PublicKey
Token=44110d1682522' or one of its dependencies.
```

Possible cause

You did not have `IQServiceClientCS.dll` located on your machine hosting CES.

Possible solution

Add the client DLL in the CES 7 `Bin` folder:

1. Stop the CES service.
2. On the machine hosting Oracle Knowledge, copy the `IQServiceClientCS.dll` file located in the `MSFT` folder.

   Example: `C:\Oracle\Knowledge\IM\InfoManager\clientLibrary\MSFT\Release`

3. On the machine hosting CES, paste the `IQServiceClientCS.dll` file in the `Bin` folder of CES.

   Example: `C:\Program Files\Coveo Enterprise Search 7\Bin`

4. Restart the CES service.

When trying to index an Oracle Knowledge source, the following error is displayed and the operation is aborted:

```
Unable to establish a connection to the Service Client API at: http://
[MyInQuiraServer]:8226/imws/WebObjects/imws.woa/ws/RequestProcessor/imws/WebObjects/imws.
woa/ws/RequestProcessor, with user [Username]. Please ensure your configuration is
correct -> Client found response content type of '', but expected 'text/xml'. The request
failed with the error message: -- Your requested web service, namely
"RequestProcessor/imws/WebObjects/imws.woa/ws/RequestProcessor", cannot be found in
WOWebServiceRegistrar. --.
```

Possible cause

Your starting address ends with `/imws/WebObjects/imws.woa/ws/RequestProcessor/` (see Configuring and Indexing an Oracle Knowledge Source).

Note: The `/imws/WebObjects/imws.woa/ws/RequestProcessor/` part is automatically added by the connector to the end of your Oracle Knowledge server URL.

Possible solution

1. Remove `/imws/WebObjects/imws.woa/ws/RequestProcessor/` at the end of the starting address parameter value (see Configuring and Indexing an Oracle Knowledge Source).
2. Try rebuilding the source by clicking **Save and Start**.