Coveo Platform 7.0

PTC Windchill 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-141120-EN

Publication date: 1/3/2019

Table of Contents

1. PTC Windchill Connector

CES 7.0.7256+ (December 2014)

Deprecated

The Coveo connector for PTC Windchill allows you to integrate the content of your PTC Windchill site together with associated permissions into your Coveo unified index, making this content easily and securely searchable by end-users.

The Coveo connector accesses the PTC Windchill product lifecycle management (PLM) content by indexing the PTC Windchill PDMLink data.

Note: As of March 2, 2017, the PTC Windchill connector is deprecated (see What Does Deprecated Mean for a Coveo Connector?).

1.1 Features

- Content indexing:
  - Site
  - Organizations (`WTOrganization`)
  - Products (`PDMLinkProduct`)
  - Libraries (`WTLibrary`)
  - Parts (`WTPart`)
    - Part usage
    - Alternate parts
    - Substitute parts
    - Reference documents
    - Described by documents
  - Documents (`WTDocument`)
  - CAD documents (`EPMDocument`)
- Security model support

  The connector and the security provider support the PTC Windchill security model by indexing permissions associated with each PTC Windchill entity, so that search results only contain documents the user performing the search has the rights to see.

  The connector resolves the following security model entities:

    - Ad Hoc access control lists (ACL)
    - Policy access control lists (ACL)
    - Owner and All pseudo-roles (well-known), system and user-defined groups and dynamic roles

- Language support

  The connector retrieves the content of the PTC Windchill default locale language which can be English, Chinese (Traditional and Simplified), French, German, Italian, Japanese, Korean, Spanish, and Russian.

- Incremental Refresh

  Updated (added, edited, deleted) content items [Part, Document, EPM Document (CAD Part)] in a PTC Windchill site content holder are periodically re-indexed by the connector.

  Notes:

    - The delete events must be audited to be taken into account (see PTC Windchill Connector Deployment Overview).
    - CES 7.0.7256 (December 2014) Deleted items require a full refresh to be taken into account.

1.2 Limitations

- Custom Soft Type attributes for parts, documents and CAD documents

  The connector can index the most common types (list)

- Security limitations

  The connector does not support the following security model aspect:

    - Security Labels (including Authorization agreements)
    - The connector and security provider do not take into account the following security aspects:
        - Profiles (only hide elements from the PTC Windchill interface without affecting the permissions)
        - Administrative lock (Do not affect the Read permission)
    - Users performing the search have the rights to see the document if they have at least the `Read` or the `Full control (All)` permission. In the case of application data content items, the users must also have the `Download` permissions to see them.

Connector Feature History

Coveo Platform version	Date	Features
7.0.7338	January 2015	Improved incremental refresh support
7.0.7256	December 2014	Connector introduction

What's Next?

Review the steps for the deployment of the PTC Windchill connector (see "PTC Windchill Connector Deployment Overview" on page 4).

2. PTC Windchill Connector Deployment Overview

The following procedure outlines the steps needed to deploy the PTC Windchill connector. The steps indicate the order in which you must perform key PTC Windchill and CES configurations. When needed, the step refers to a detailed procedure.

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

2. On your PTC Windchill server:

   a. Create a dedicated crawling account on the PTC Windchill server

      The connector needs an account that has read access to all the PTC Windchill content that you want to index. It is recommended to create a dedicated PTC Windchill account for this purpose.

   b. Copy PTC Windchill certificate files

      The Coveo connector needs to have access to a copy of the PTC Windchill client and server certificate files to be authorized to communicate with your PTC Windchill server (see "Copying the PTC Windchill Certificates to the Coveo Master Server" on page 8).

   c. Install (or update) the Coveo plugin

      You must install the Coveo plugin on your PTC Windchill server to allow the connector to communicate with PTC Windchill (see "Installing or Updating the Coveo Plugin for PTC Windchill" on page 10).

   d. When you want the incremental refresh to capture content items deletion, you must audit the delete events:

      Note: CES 7.0.7338+ (January 2015) The incremental refresh supports deleted items.

      i. With a text editor, open the XML PTC Windchill configAudit file located in the `Windchill` folder.

         Example: `C:\Program Files\Windchill\conf\auditing\configAudit.xml`

      ii. Ensure that the first line of the configAudit file is the following:

         ```
         <EventConfiguration enabled="true">
         ```

         meaning that the auditing is enabled within your PTC Windchill site.

      iii. Under the `<ConfigEntry class="" enabled="true">` node, add the following line to audit the delete events:

         ```
         <KeyedEventEntry eventKey="*/wt.events.summary.DeleteSummaryEvent/"
         enabled="true" handler="wt.audit.configaudit.DefaultAuditEventRecorder"/>
         ```

      iv. Under the `<ConfigEntry class="" enabled="false">` node, remove the previous line.

         Note: By default, delete events are not audited.

        v. Save the file.

        vi. Restart the method server to apply the new configuration.

3. On your Coveo server:

    a. Configure a user identity

    The Coveo connector needs to know the credentials of the PTC Windchill crawling account that you created (see "Adding a User Identity" on page 12).

    b. Optionally, but recommended, create a PTC Windchill field set from the default XML field set file to be able to leverage PTC Windchill metadata for example to create more useful facets.

        i. With a text editor, open the `[CES_Path]\Bin\Coveo.CES.CustomCrawlers.Windchill.FieldSet.xml` default XML PTC Windchill field set file and copy its content.

        ii. Create a PTC Windchill field set by importing the XML file content.

    c. Create a custom document type set

    > **Note:** Some Windchill file types such as CAD and CAM files are big in size. By default, those large files are downloaded, but not converted by the connector, causing a serious crawling delay. It is thus strongly recommended to index only the metadata of those documents to significantly improve the crawling performance.

        i. Create a document type set.

        The document type set is a copy of the **Default** one that you need to customize.

        ii. In the **Document Type Sets** page, click the document type set that you just created.

        iii. In the **Document Type** page, in the toolbar, click **Add**.

        iv. In the configuration page, only three parameters are relevant to fulfill:

            i. In the first box, enter a descriptive **Name** for the this document type.

            > **Example:** Windchill Files

            ii. In the **File Extensions** box, enter the following list: `.3dm; .acs; .asm; .CATPart; .CATProduct; .cgm; .cgr; .des; .dgm; .dwg; .ed; .edn; .edp; .edz; .emn; .emp; .evs; .exp; .frm; .g; .gbf; .hdr; .iam; .ibl; .icm; .idx; .igs; .imf; .ipt; .jt; .lay; .mdc; .mdf; .mem; .mfg; .model; .neu; .nwf; .obj; .pdt; .plt; .prt; .pts; .pvs; .pvt; .pvz; .rep; .rla; .sec; .session; .set; .shd; .sldasm; .sldprt; .step; .stl; .stp; .tsh; .tx1; .tx3; .tx4; .u3d; .vda; .wrl; .x_b; .x_n; .x_t; .xmt; .xmt_bin; .xmt_neu; .xmt_txt; .xpr`

iii. Next to **Indexing Failure Action**, select the **Index file information only** radio button.

iv. Click **Save**.

d. Configure a security provider

The Coveo connector requires a PTC Windchill security provider to expand PTC Windchill groups and resolve mappings between users and groups from the PTC Windchill system and other systems like Microsoft Active Directory (see "Configuring a PTC Windchill Security Provider" on page 14).

e. Configure and index a PTC Windchill source

The Coveo connector needs to know details about the PTC Windchill site to be able to index its content (see "Configuring and Indexing a PTC Windchill Source" on page 22).

f. Optionally, modify hidden source parameters

If you encounter issues, review if modifying the default value of available hidden source parameters can resolve the issue you are facing (see "Modifying Hidden PTC Windchill Source Parameters" on page 27).

g. In a Coveo search interface, validate that you and your end-users can see the allowed PTC Windchill documents in search results.

Note: You may need to manually update the CES security cache to see PTC Windchill documents in the search results.

What's Next?

Review the connector requirements (see "PTC Windchill Connector Requirements" on page 7).

3. PTC Windchill Connector Requirements

Your environment must meet the following requirements to be able to use the Coveo connector for PTC Windchill.

- Coveo license for the PTC Windchill connector

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

- CES 7.0.7256+ (December 2014)

- Supported PTC Windchill version

  The connector supports PTC Windchill PDMLink version 10.1 M010 and 10.1 M040 features.

- PTC Windchill security policy

  The connector plugin must be installed on a foreground method server that runs with the `userNameAuthSymmetricKeys` security policy and that has a keystore and a truststore (see "Copying the PTC Windchill Certificates to the Coveo Master Server" on page 8 and "Installing or Updating the Coveo Plugin for PTC Windchill" on page 10).

What's Next?

Copy the PTC Windchill certificate files on the Coveo server (see "Copying the PTC Windchill Certificates to the Coveo Master Server" on page 8).

4. Copying the PTC Windchill Certificates to the Coveo Master Server

The Coveo connector and security provider need to have access to a copy of the PTC Windchill client and server certificate files to be able to communicate with your PTC Windchill foreground method server. The Coveo connector will use the certificate file copies to authenticate itself with PTC Windchill to be able to connect to the Coveo plugin.

You must perform the following procedure only once after creating or updating your PTC Windchill certificates.

To copy the PTC Windchill foreground method server certificate to the Coveo Master server

1. If your PTC Windchill deployment contains more than one foreground method server, select one to be used by the Coveo connector.

2. Using an administrator account, connect to the PTC Windchill foreground method server.

3. Open a Windchill shell.

   Example: When PTC Windchill runs on a Windows Server, from the **Start** menu, select **Windchill Shell**.

4. When the keystore and truststore do not yet exist on your PTC Windchill foreground method server (with the `userNameAuthSymmetricKeys` default security policy), create them as follows:

   a. In the Windchill shell, run the following command:

   ```
   ant -f jws-stores.xml
   ```

   Note: When the ant path is not set in the environment variable, you must include the path where ant is installed on your system.

   Example: When ant is installed in the `.\ant\bin\` folder, the command is:

   ```
   .\ant\bin\ant -f jws-stores.xml
   ```

   b. Answer to the prompts of the script using the default or appropriate values (based on the `security.properties` file content).

   Note: Refer to the *Understanding the Security Requirements* topic in the Windchill Help Center on your PTC Windchill server for more information.

5. Copy the PTC Windchill certificate files to the Coveo Master server:

   a. From the PTC Windchill foreground method server, copy the following files:

   - `%WT_HOME%\prog_examples\jws\stores\client.cer`
   - `%WT_HOME%\prog_examples\jws\stores\server.cer`

   where `%WT_HOME%` is the PTC Windchill home folder, such as `C:\ptc\Windchill_10.x\Windchill`.

b. Using an administrator account, connect to the Coveo Master server.

c. Paste the certificate files on the Coveo Master server in a `[Index_Path]` subfolder such as `\CertStore\PTC_Windchill\`.

> **Example:** On the Coveo Master server, copy the certificate files to the `D:\CES7\CertStore\PTC_Windchill\` folder.

What's Next?

Install or update the Coveo plugin on your PTC Windchill server (see "Installing or Updating the Coveo Plugin for PTC Windchill" on page 10).

5. Installing or Updating the Coveo Plugin for PTC Windchill

The Coveo connector for PTC Windchill needs a plugin to be able to access the PTC Windchill API. You must install the Coveo plugin on the PTC Windchill foreground method server.

When you upgrade CES, if the included PTC Windchill plugin is updated, you must also use this procedure update it on your PTC Windchill foreground method server.

To install or update the Coveo plugin on the PTC Windchill foreground method server

1. If your PTC Windchill deployment contains more than one foreground method server, select one to be used by the Coveo connector from which you also copy the certificates (see "Copying the PTC Windchill Certificates to the Coveo Master Server" on page 8).

2. Using an administrator account, connect to your Windchill Server foreground method server.

3. Open a Windchill shell.

   Example: When PTC Windchill runs on a Windows Server, from the **Start** menu, select **Windchill Shell**.

4. When the Coveo plugin is already installed on your PTC Windchill foreground method server and you are updating the plugin, you must first:

   Important: Do not perform this step if you are installing the Coveo plugin for the first time.

   a. Uninstall the previous plugin version by running the following command in a Windchill shell:

      ```
      ant -f %WT_HOME%\bin\adminTools\WebServices\build.xml -Dservlet.name=CoveoWindchillWebService
      undeployService
      ```

   b. It is recommended to rename the previous version of the plugin file as a backup.

      Example: Rename the plugin `.jar` file to `%WT_HOME%\codebase\WEB-INF\lib\CoveoWindchillWebService.jar.OLD`

5. Copy the Coveo plugin file from the Coveo Master server to the PTC Windchill foreground method server:

   a. On the Coveo Master server, copy the PTC Windchill plugin file:

      `[CES_Path]\bin\CoveoWindchillWebService.jar`

   b. Paste the plugin file on the PTC Windchill foreground method server in the following folder:

      `%WT_HOME%\codebase\WEB-INF\lib\`

6. On the PTC Windchill foreground method server, install the plugin by running the following command in a Windchill shell:

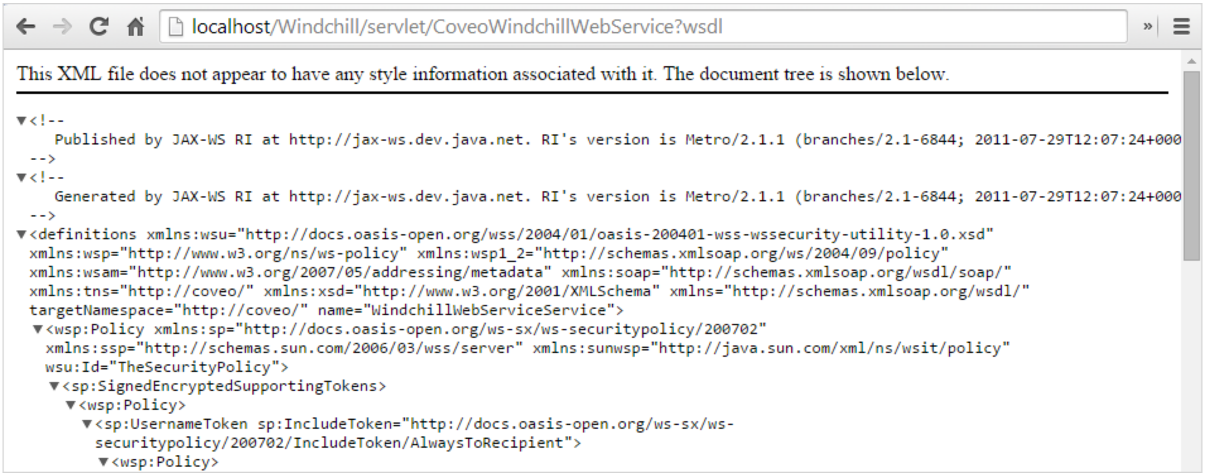
   ```
   ant -f %WT_HOME%\bin\adminTools\WebServices\build.xml -Dservlet.name=CoveoWindchillWebService -
   Dwebservice.class=coveo.WindchillWebService -Dsecurity.policy=userNameAuthSymmetricKeys
   deployFromJava
   ```

7. In a browser, you can validate that the installation completed successfully by ensuring the service WSDL is

available with the following URL:

```
http://[WindchillWebServer]/Windchill/servlet/CoveoWindchillWebService?wsdl
```

The plugin Web Services Description Language (WSDL) similar to the following capture should appear.



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<!--
    Published by JAX-WS RI at http://jax-ws.dev.java.net. RI's version is Metro/2.1.1 (branches/2.1-6844; 2011-07-29T12:07:24+000
 -->
▼<!--
    Generated by JAX-WS RI at http://jax-ws.dev.java.net. RI's version is Metro/2.1.1 (branches/2.1-6844; 2011-07-29T12:07:24+000
 -->
▼<definitions xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
 xmlns:wsp="http://www.w3.org/ns/ws-policy" xmlns:wsp1_2="http://schemas.xmlsoap.org/ws/2004/09/policy"
 xmlns:wsam="http://www.w3.org/2007/05/addressing/metadata" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
 xmlns:tns="http://coveo/" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="http://schemas.xmlsoap.org/wsdl/"
 targetNamespace="http://coveo/" name="WindchillWebServiceService">
  ▼<wsp:Policy xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702"
   xmlns:ssp="http://schemas.sun.com/2006/03/wss/server" xmlns:sunwsp="http://java.sun.com/xml/ns/wsit/policy"
   wsu:Id="TheSecurityPolicy">
    ▼<sp:SignedEncryptedSupportingTokens>
      ▼<wsp:Policy>
        ▼<sp:UsernameToken sp:IncludeToken="http://docs.oasis-open.org/ws-sx/ws-
          securitypolicy/200702/IncludeToken/AlwaysToRecipient">
          ▼<wsp:Policy>
```

What's Next?

Configure a CES user identity for the PTC Windchill crawling account credentials (see "Adding a User Identity" on page 12).

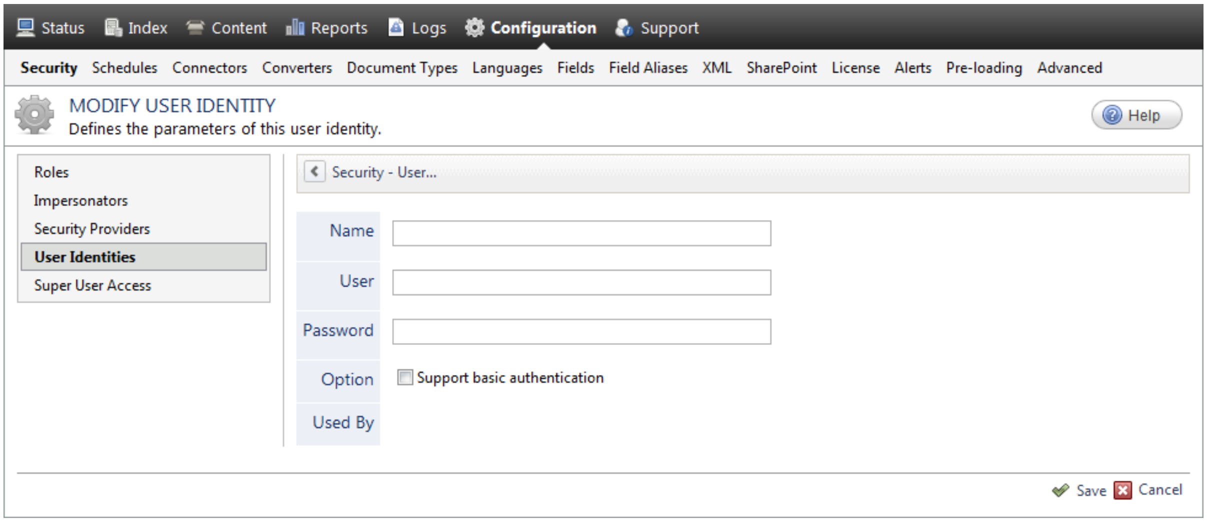
6. Adding a User Identity

A user identity is a set of credentials for a given repository or system that you enter once in CES and can then associate with one or more sources or security providers.

A user identity typically holds the credentials of an account that has read access to all the repository items that you want to index. It is a best practice to create an account to be used exclusively by the Coveo processes and for which the password does not change. If the password of this account changes in the repository, you must also change it in the CES user identity.

To add a user identity

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



MODIFY USER IDENTITY
Defines the parameters of this user identity.

Name
User
Password
Option ☐ Support basic authentication
Used By

   a. In the **Name** box, enter a name of your choice to describe the account that you selected or created in the repository to allow CES to access the repository.

   > **Note:** This name appears only in the Coveo Administration Tool, in the **Authentication** or **User Identity** drop-down lists, when you respectively define a source or a security provider.

   b. In the **User** box, enter the username for the account that you selected or created to crawl the repository content that you want to index.

   c. In the **Password** box, enter the password for the account.

   d. In the **Options** section, the **Support basic authentication** check box is deprecated and not applicable for most types of repositories. You should select it only when you need to allow CES to send the username and password as unencrypted text.

e. Click **Save**.

Important: When you use Firefox to access the Administration Tool and it proposes to remember the password for the user identity that you just created, select to never remember the password for this site to prevent issues with automatic filling of username and password fields within the Coveo Administration Tool.

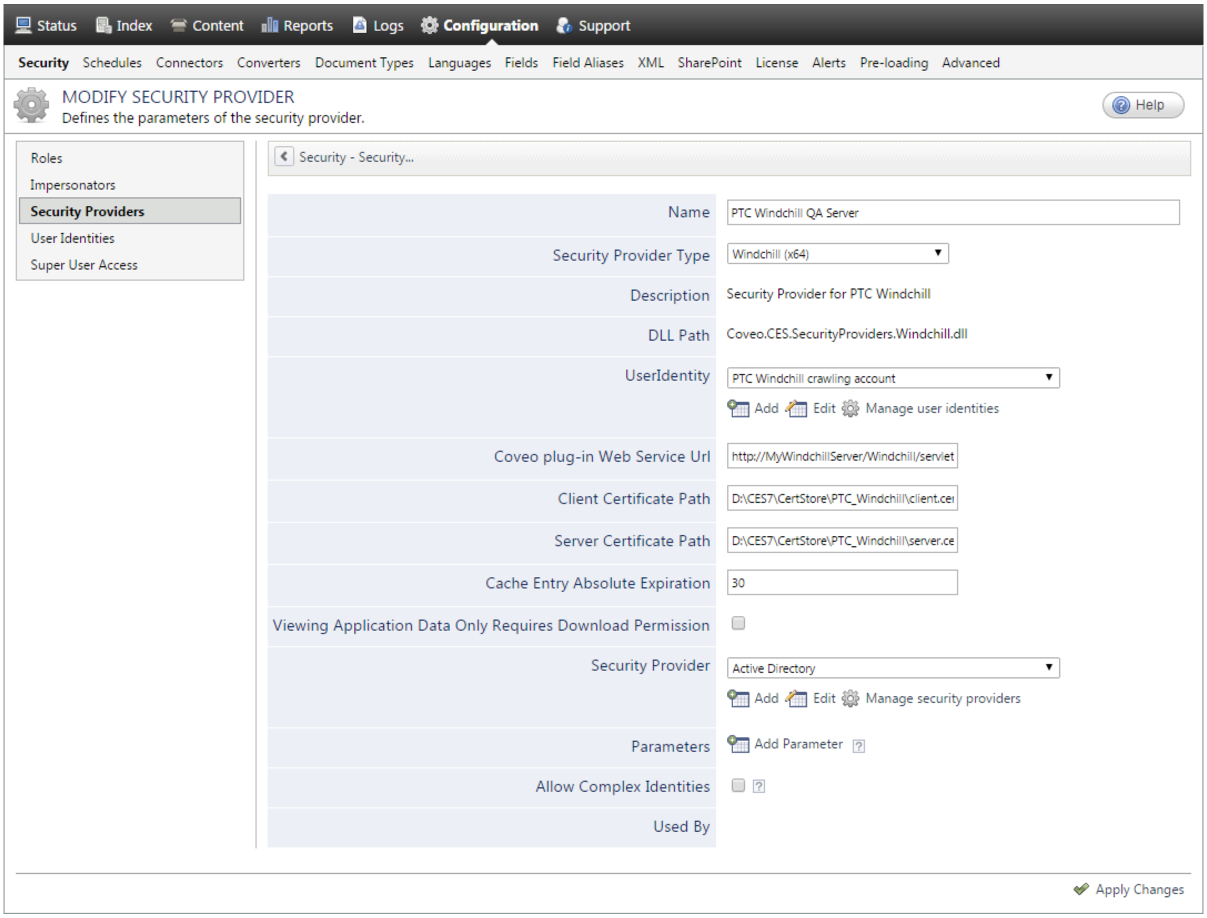
7. Configuring a PTC Windchill Security Provider

The PTC Windchill connector needs a security provider to manage the user permissions on PTC Windchill entities. The PTC Windchill security provider performs tasks such as expanding groups to users and mapping PTC Windchill users to emails or to Active Directory users. The connector creates and sets several virtual groups on indexed documents to support the access policies defined in PTC Windchill.

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

To Configure a PTC Windchill security provider

1. On the Coveo server, access the Administration Tool.
2. Select **Configuration** > **Security**.
3. In the **Security** page, 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:



Name	PTC Windchill QA Server
Security Provider Type	Windchill (x64)
Description	Security Provider for PTC Windchill
DLL Path	Coveo.CES.SecurityProviders.Windchill.dll
UserIdentity	PTC Windchill crawling account Add Edit Manage user identities
Coveo plug-in Web Service Url	http://MyWindchillServer/Windchill/servlet
Client Certificate Path	D:\CES7\CertStore\PTC_Windchill\client.ce
Server Certificate Path	D:\CES7\CertStore\PTC_Windchill\server.ce
Cache Entry Absolute Expiration	30
Viewing Application Data Only Requires Download Permission	□
Security Provider	Active Directory Add Edit Manage security providers
Parameters	Add Parameter ?
Allow Complex Identities	□ ?
Used By	

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

   Example: `PTC Windchill Security Provider`

b. In the **Security Provider Type** drop-down list, select **Windchill**.

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

   i. In the drop-down list, select the user identity that you created previously with the PTC Windchill crawling account credentials (see PTC Windchill Connector Deployment Overview).

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

d. In the **Coveo plug-in Web Service Url** box, enter the URL in the following format:

```
http://[myWindchillServer]/Windchill/servlet/CoveoWindchillWebService
```

   where you replace `[myWindchillServer]` with the name of your PTC Windchill server.

e. In the **Client Certificate Path** and **Server Certificate Path** boxes, enter the path and file name where you copied these files on the Coveo Master server (see "Copying the PTC Windchill Certificates to the Coveo Master Server" on page 8).

   Example: When the files were copied with their original names in the `D:\CES7\CertStore\PTC_Windchill\` folder, respectively enter:

   - `D:\CES7\CertStore\PTC_Windchill\client.cer`
   - `D:\CES7\CertStore\PTC_Windchill\server.cer`

f. In the **Cache Entry Absolute Expiration** box, leave the `30` seconds default value unless instructed to change it by Coveo Support.

   This parameter indicates at what interval the security provider cache is reset. The use of this cache minimizes calls made to the plugin to retrieve policies. A value of `0` means no cache is used.

g. Select the **Viewing Application Data Only Requires Download Permission** check box only when you want the security provider to allow access to `ApplicationData` type documents (Windchill local files) when a user has only the `Download` permission, rather than by default, when the user has the `Read+Download` permissions.

   Note: When you select this parameter, you must also add the `ViewingApplicationDataOnlyRequiresDownloadPermission` source parameter and set it to `true` (see Modifying Hidden PTC Windchill Source Parameters).

h. In the **Security Provider** section, optionally select another security provider to allow the PTC Windchill security provider to map PTC Windchill accounts to another user type with which people are authenticated when they perform a search:

   - Select **None** when you do not want to map PTC Windchill users to another user type.

     The security provider creates user members with the LDAP distinguished name (DN) retrieved from PTC Windchill.

- When the Windchill LDAP is synchronized with an Active Directory, select the out-of-the-box **Active Directory** security provider to map PTC Windchill users to AD users.

  The PTC Windchill security provider maps users to Active Directory by extracting the `UID` of the LDAP distinguished name (DN) provided by Windchill.

  Example: When a PTC Windchill user distinguished name (DN) is `uid=jbaker,ou=people,cn=administrativeldap,cn=windchill_10.1,o=ptc`, the security provider outputs a `SID` declarator with the name `jbaker` by extracting the `UID` of this DN.

  Note: When a user exists in PTC Windchill, but does not exist in the Active Directory, a `SID` declarator is still created, but the Active Directory security provider will throw a `SecurityInvalidUserGroupException` because no mapping exists between this account and Active Directory.

- When the email property is defined for all users in PTC Windchill and your users authenticated with this email when they perform a search, you can click **Add** to create, and then select an Email security provider (see "Configuring an Email Security Provider" on page 17).

Note: When none of the above security provider types fulfill your needs, it may be possible to use a custom security provider like the **REGEX Transform Member Name** to bridge the gap between PTC Windchill accounts and another type of users (see "Configuring a REGEX Transformation Security Provider" on page 18).

i.

(Optional) In the **Parameters** section, click **Add Parameter** and then use the following hidden parameter when you want to map your PTC Windchill usernames to their Windows usernames:

ActiveDirectoryDomainNameForMappings CES 7.0.7433+ (February 2015)

Enter the Active Directory domain name used to map users in the Active Directory security provider. The default value is `null`. Consider changing the value when the Active Directory domain on which CES runs is not the desired domain.

Example: When the `ActiveDirectoryDomainNameForMappings` parameter value is `MyCompany` and you expand the PTC Windchill user `John`, the security provider will expand this user to the AD user `MyCompany\John`.

Note: This parameter is only used if you selected **Active Directory** in the **Security Provider** section (see step h).

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

k. Click **Apply Changes**.

What's Next?

Configure and index your PTC Windchill source (see "Configuring and Indexing a PTC Windchill Source" on page 22).

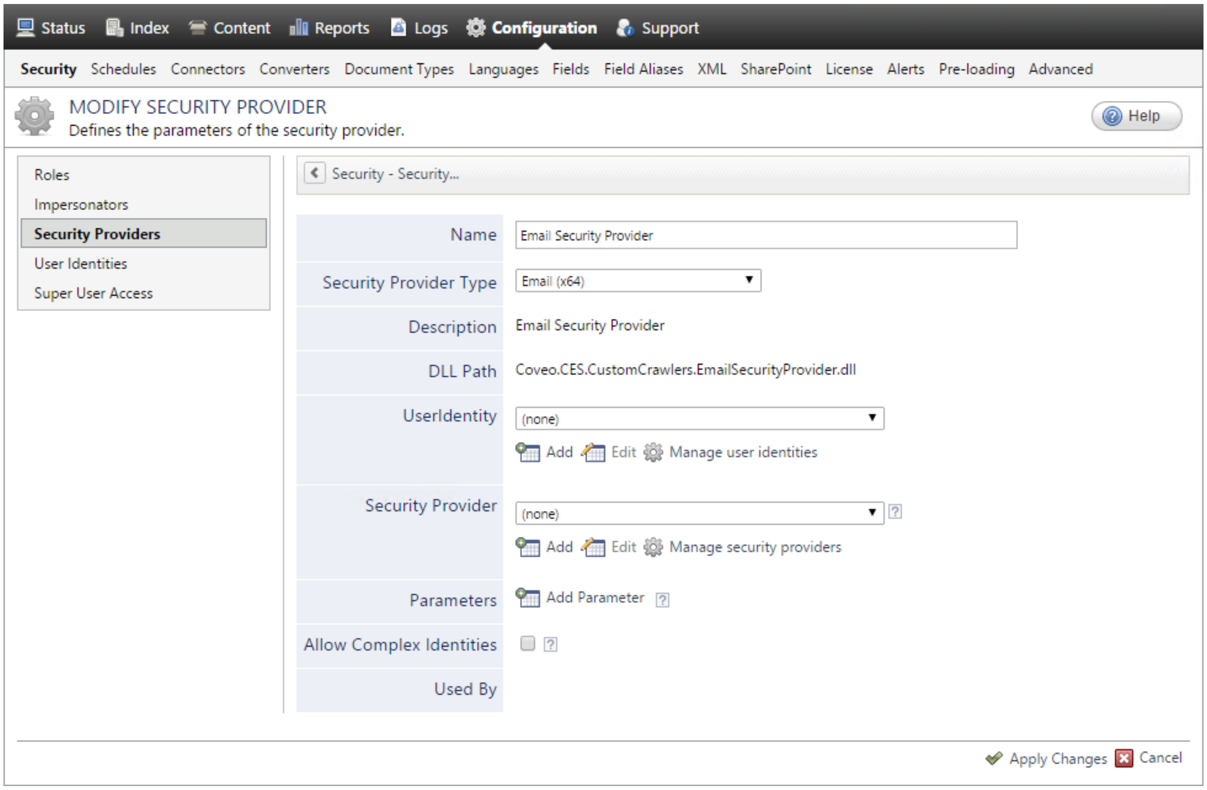
7.1 Configuring an Email Security Provider

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.

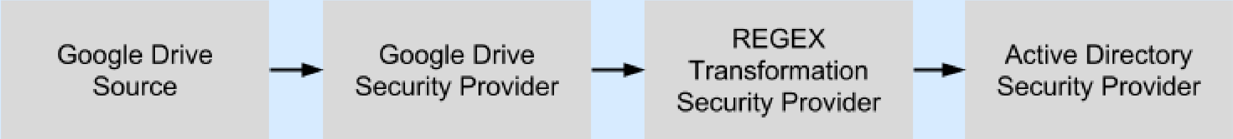
7.2 Configuring a REGEX Transformation Security Provider

The *Coveo Member Name Regex Transformation* security provider, is a special type of security provider that uses matching and replacement regular expressions (REGEX) to only transform member names received from one security provider type to another name format for another security provider type. A REGEX Transformation security provider is always configured in sandwich between two other security providers.

Some kind of rule must allow to transform the member name from its input format to the output format using regular expressions. You must be proficient with regular expressions to configure this type of security provider.

Example: You have a Google Drive source in which account names are user emails (`username@mycompany.com`), but your users are authenticated with their Active Directory (AD) account (`mycompany\username`) when they access a Coveo search interface. For users to be granted to see Google Drive documents in search results, document permissions must be associated to their AD account, otherwise, no results will be returned.

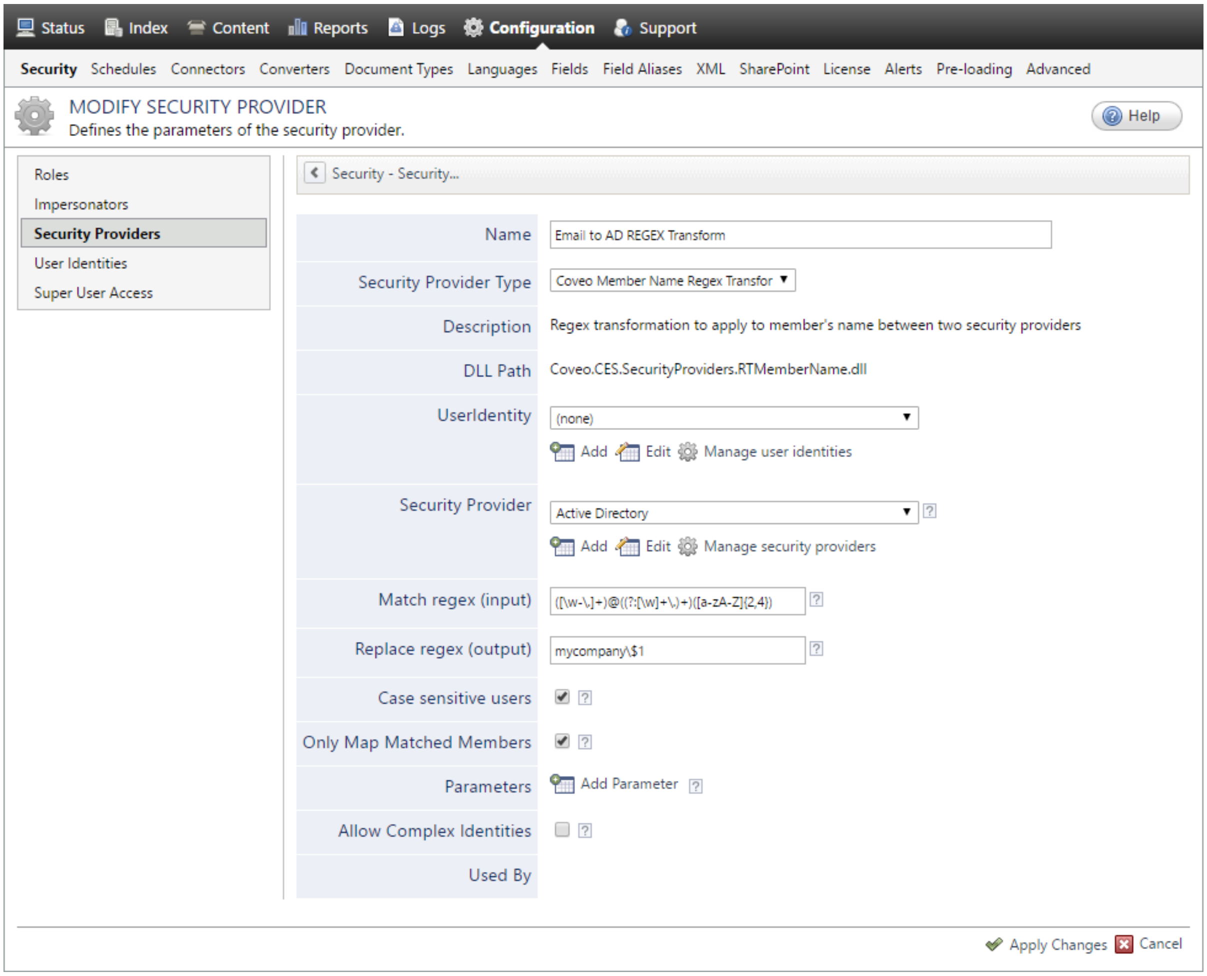
As shown in the following diagram, you can accomplish this by configuring your Google Drive source to get permissions from a Google Drive security provider that sends output members to the REGEX Transformation security provider, which finally outputs transformed member names to the Active Directory security provider, so that at the end, the permissions of the Google Drive account are available in the security cache for the equivalent AD account.


Google Drive Source
Google Drive Security Provider
REGEX Transformation Security Provider
Active Directory Security Provider

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

To configure a REGEX Transformation security provider

1. On the Coveo server, access the Administration Tool.
2. Select **Configuration** > **Security**.
3. In the **Security** page, 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	Email to AD REGEX Transform
Security Provider Type	Coveo Member Name Regex Transfor
Description	Regex transformation to apply to member's name between two security providers
DLL Path	Coveo.CES.SecurityProviders.RTMemberName.dll
UserIdentity	(none)
Security Provider	Active Directory
Match regex (input)	([\w-\.]+)@((?:[\w]+\.)+)([a-zA-Z]{2,4})
Replace regex (output)	mycompany\$1
Case sensitive users	☑
Only Map Matched Members	☑
Parameters	
Allow Complex Identities	☐
Used By	

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

> **Example:** If you configure the security provider to transform names from the email format to the AD format:
>
> `Email to AD REGEX Transform`

b. In the **Security Provider Type** drop-down list, select **Coveo Member Name Regex Transformation**.

c. In the **User Identity** drop-down list, leave the selection to **(none)**, because this parameter is not applicable to this type of security provider.

d. In the **Security Provider** section, select the output security provider to which transformed names will be sent.

> **Example:** When this security provider output name format is AD, select the out-of-the-box **Active Directory** security provider.

e. In the **Match regex (input)** box, enter the regular expression to match and select appropriate parts of your input name format.

> **Example:** To match parts of an email address:
>
> `([\w-\.]+)@((?:[\w]+\.)+)([a-zA-Z]{2,4})`

f. In the **Replace regex (output)** box, enter the replacement regular expression for your output name format.

> **Example:** To convert the email name to an Active Directory name for the `mycompany` domain:
>
> `mycompany\$1`

> **Important:** Fully test your matching and replacement regular expressions to ensure they transform member names as expected for all member name cases.

g. Select the **Case sensitive users** check box when the account names are case sensitive.

h. CES 7.0.8996+ (June 2017) Select the **Only Map Matched Members** check box if you wish to map only members whose name matches the regex specified by the **Match Regex (Input)** parameter.

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

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

k. Click **Apply Changes**.

What's Next?

Assign this REGEX Transformation security provider as an output for the appropriate other security provider.

8. Configuring and Indexing a PTC Windchill Source

A source defines a set of configuration parameters for indexing the content of a specific PTC Windchill site.

To configure and index a PTC Windchill 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.

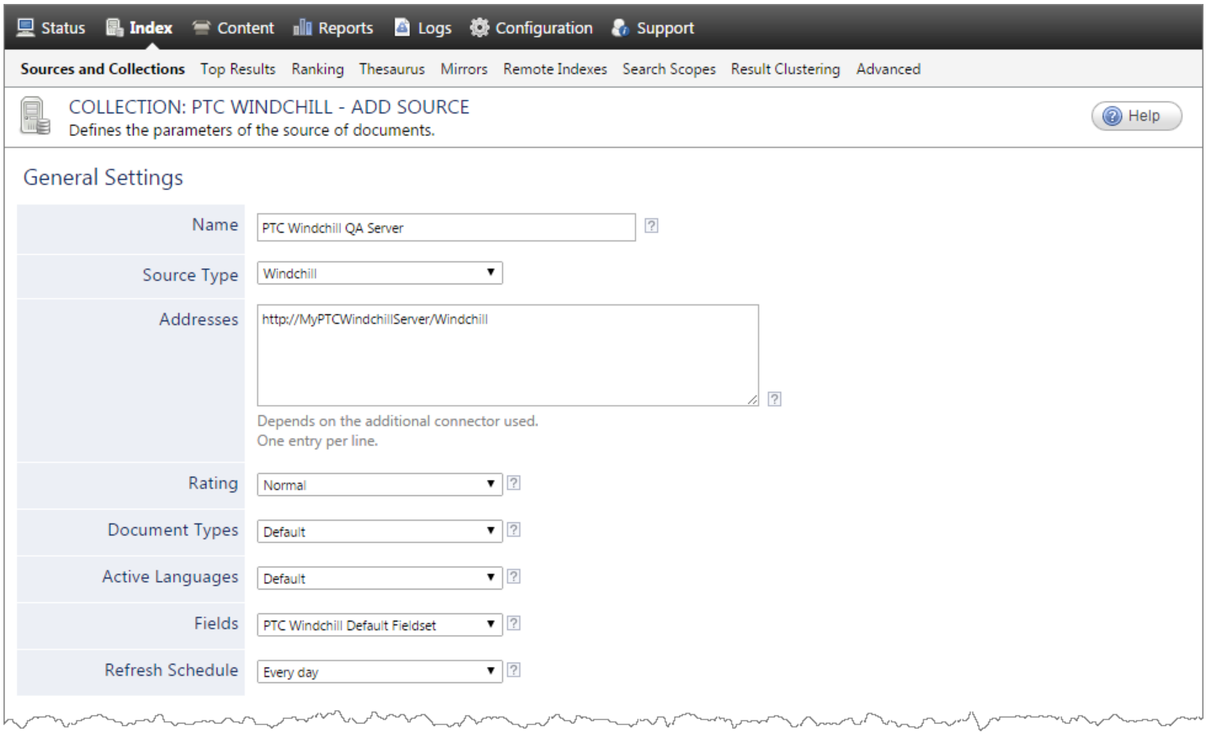
      OR

   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: PTC WINDCHILL - ADD SOURCE

Defines the parameters of the source of documents.

General Settings

Name	PTC Windchill QA Server
Source Type	Windchill
Addresses	http://MyPTCWindchillServer/Windchill Depends on the additional connector used. One entry per line.
Rating	Normal
Document Types	Default
Active Languages	Default
Fields	PTC Windchill Default Fieldset
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:** `PTC Windchill Site`

Source Type

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

Addresses

The address of the PTC Windchill site in the form:

```
http://[PTCWindchillServer]/Windchill
```

where you replace `[PTCWindchillServer]` by your actual PTC Windchill server host name.

Fields

If you defined a PTC Windchill field set, select it (see PTC Windchill 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:** You can create a new or modify an existing source refresh schedule.

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 ranking associated with all items in this source relative to the rating of other sources.

> **Example:** If this source is for a legacy PLM, you may want to set this parameter to **Low**, so that in the search interface, results from this source appear later in the list compared to those from other sources.

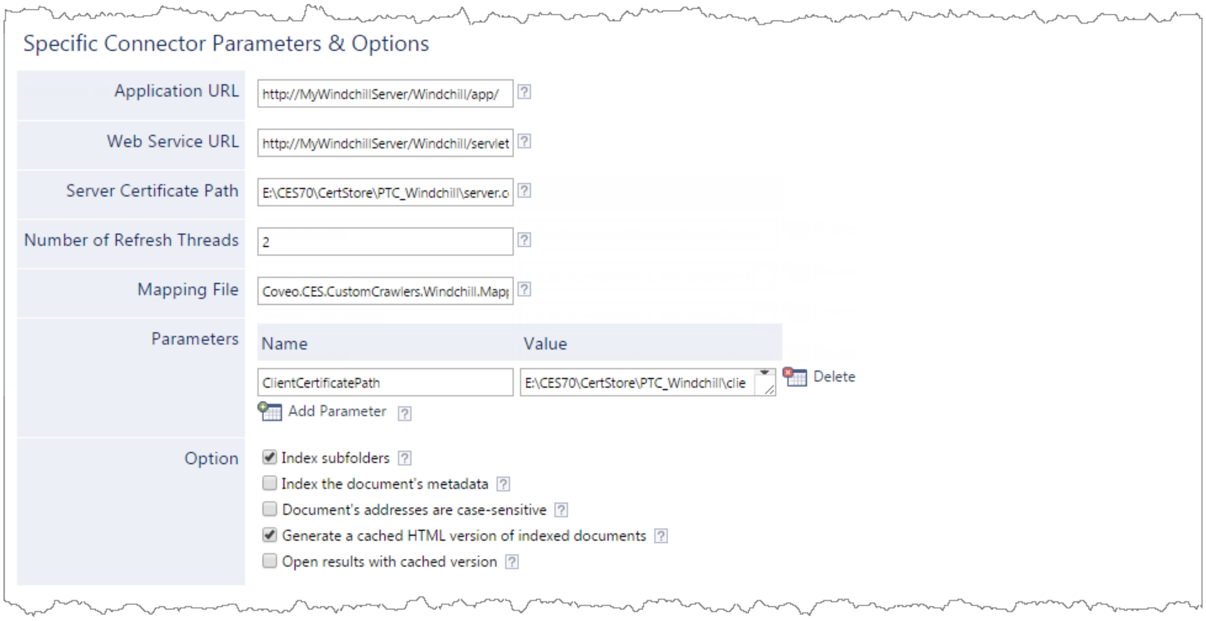
Document Types

Select the custom document type set that you created for this source (see PTC Windchill Connector Deployment Overview). Otherwise, leave **Default**.

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

Application URL	http://MyWindchillServer/Windchill/app/
Web Service URL	http://MyWindchillServer/Windchill/servlet
Server Certificate Path	E:\CES70\CertStore\PTC_Windchill\server.c
Number of Refresh Threads	2
Mapping File	Coveo.CES.CustomCrawlers.Windchill.Mapp

Parameters

Name	Value
ClientCertificatePath	E:\CES70\CertStore\PTC_Windchill\clie

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:

Application URL

Enter the URL of the PTC Windchill application used to open search results.

Example: `http://MyWindchillServer/Windchill/app/`

Web Service URL

Enter the URL to the Coveo plug-in web service.

Example: `http://MyWindchillServer/Windchill/servlet/CoveoWindchillWebService`

Server Certificate Path

Enter the path of the server X.509 certificate used to connect to the Coveo plug-in web service.

Example: `E:\CES70\CertStore\PTC_Windchill\server.cer`

b. In the **Number of Refresh Threads** box, consider changing the number of simultaneous connections established with the PTC Windchill site by the connector. The default value is `2`. Increasing this value may improve source refresh speed but puts more load on the PTC Windchill server.

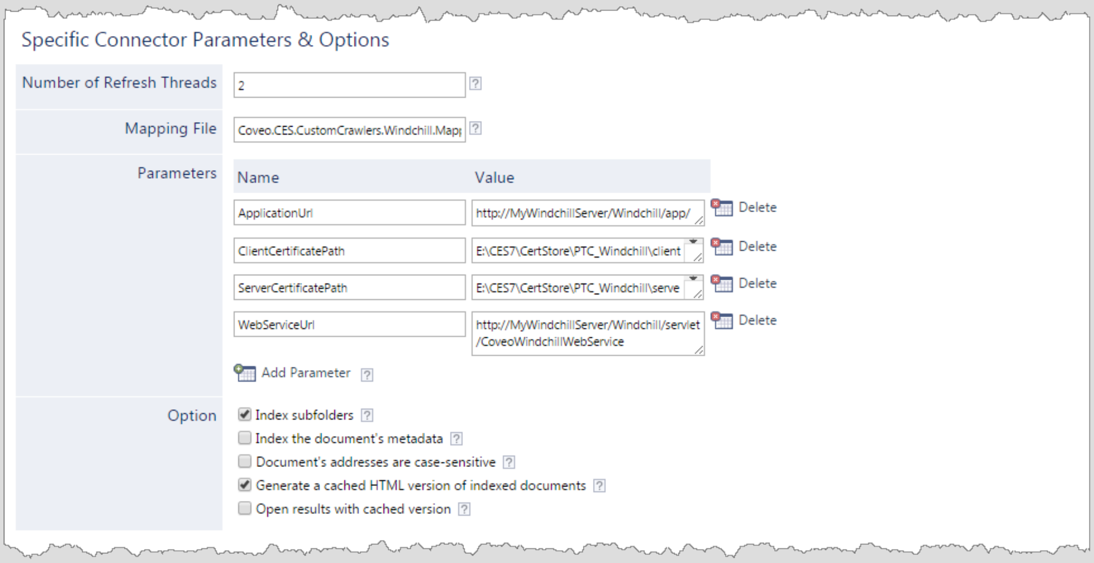
c. In the **Mapping File** box, leave the default mapping file name (`Coveo.CES.CustomCrawlers.Windchill.MappingFile.xml`) unless you created a custom mapping file, in which case, enter the full path of your valid mapping file.

d. Click **Add Parameter** when you want to show and change the value of hidden source parameters (see "Modifying Hidden PTC Windchill Source Parameters" on page 27).

Notes:

- In rare cases, Coveo Support can instruct you to click **Add Parameter** to enter the name and value of other hidden parameters that can help in troubleshooting issues (see "Modifying Hidden PTC Windchill Source Parameters" on page 27).
- CES 7.0.7256– (December 2014) The following required parameters must be added manually:

Parameter name	Parameter value example
`ApplicationUrl`	`http://MyWindchillServer/Windchill/app/`
`ClientCertificatePath`	`E:\CES70\CertStore\PTC_Windchill\client.cer`
`ServerCertificatePath`	`E:\CES70\CertStore\PTC_Windchill\server.cer`
`WebServiceUrl`	`http://MyWindchillServer/Windchill/servlet/CoveoWindchillWebService`



Specific Connector Parameters & Options

Number of Refresh Threads: 2

Mapping File: Coveo.CES.CustomCrawlers.Windchill.Mapp

Parameters

Name	Value
ApplicationUrl	http://MyWindchillServer/Windchill/app/
ClientCertificatePath	E:\CES7\CertStore\PTC_Windchill\client
ServerCertificatePath	E:\CES7\CertStore\PTC_Windchill\serve
WebServiceUrl	http://MyWindchillServer/Windchill/servlet /CoveoWindchillWebService

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

e. In the **Option** section, the state of check boxes generally does not need to be changed:

Index Subfolders

Check to index all subfolders below the specified starting addresses.

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 case sensitive systems in which distinct documents may have the same file name but with different casing.

Generate a cached HTML version of indexed documents

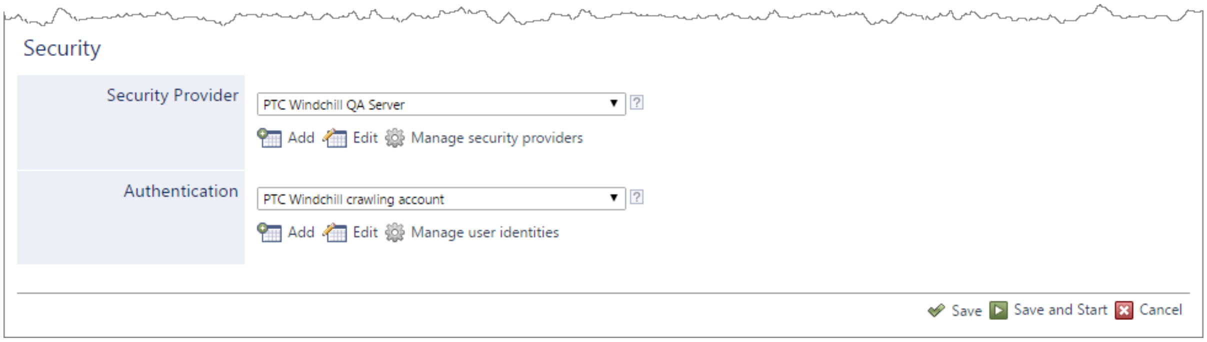
When you select this check box (recommended), at indexing time CES creates HTML versions of indexed documents and saves them in the unified index. In the search interfaces, users can then more rapidly review the content by clicking the **Quick View** link to open the HTML version of the item rather than opening the original document with the original application.

Consider clearing this check box only if 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. When this option is selected, you must also select the **Generate a cached HTML version of indexed documents** check box.

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



Security

Security Provider: PTC Windchill QA Server

Authentication: PTC Windchill crawling account

   a. In the **Security Provider** drop-down list, select the PTC Windchill security provider that you created for this source (see "Configuring a PTC Windchill Security Provider" on page 14).

   b. In the **Authentication** drop-down list, select the PTC Windchill user identity that you created for this source (see PTC Windchill Connector Deployment Overview).

   c. Click **Save and Start** to save the source configuration and build the source.

8. Validate that the indexing proceeds without errors:

   a. In the navigation panel on the left, click **Status** to monitor the indexing progress.

   b. On the Coveo Master server, open the CES Console to review indexing logs.

8.1 Modifying Hidden PTC Windchill 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 PTC Windchill sites. 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.

The following list describes the available advanced hidden parameters for PTC Windchill sources. The parameter type (integer, string…) appears between parentheses following the parameter name.

BatchSize (Integer)

The number of items to retrieve with each call to the web service. The default value is `100`.

UseVirtualGroupsPermissionModel (Boolean)

Whether to use the permission model with virtual groups expanded by the security provider. The default value is `true`.

By default, each permission set on documents to support policy access control lists (ACL) contains virtual groups as members. These virtual groups are expanded by the security provider to fill allowed and denied members and are maintained in the security cache. The connector can directly expand members when this parameter is set to `false` so that permissions are stored directly in the index.

It can be useful to set this parameter to `false` if the permission model gets too complex and may not scale. The disadvantage is that you must rebuild the source to catch permission changes rather than simply update the security cache.

ViewingApplicationDataOnlyRequiresDownloadPermission (Boolean)

Whether the `Download` permission is sufficient to access `Application Data` type documents, rather than the default `Read+Download` permissions. The default value is `false`.

The Coveo security provider cannot currently resolve the combined `Read+Download` permissions so by default, users will never see `Application Data` type documents in search results. Set this parameter to `true` when you want to allow users having the `Download` permission (with or without the `read` permission) for documents of this type to see them in search results.

When you change this parameter you must also select the **Viewing Application Data Only Requires Download Permission** security provider option (see Configuring a PTC Windchill Security Provider).

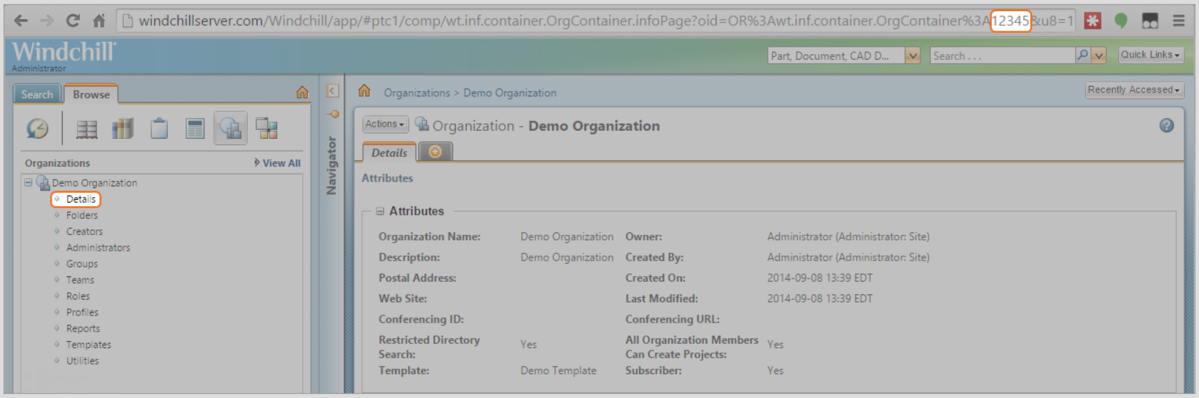
WebAppUrlFragment (String)

The web app URL fragment of the PTC Windchill application used to open search results. The default value is `/app/#ptc1`. Change this value only if you use a web app other than the default one.

OrganizationIdentifiers (String) CES 7.0.7711+ (June 2015)

The list of organization container IDs (separated by a semicolon) of the organization you wish to index.

> **Note:** To find the organization ID, as a Windchill Admin, access the **Details** page of an organization and looks at the URL of the page. In the following capture, the container ID is 12345.



windchillserver.com/Windchill/app/#ptc1/comp/wt.inf.container.OrgContainer.infoPage?oid=OR%3Awt.inf.container.OrgContainer%3A12345&u8=1

Organization Name:	Demo Organization	Owner:	Administrator (Administrator: Site)
Description:	Demo Organization	Created By:	Administrator (Administrator: Site)
Postal Address:		Created On:	2014-09-08 13:39 EDT
Web Site:		Last Modified:	2014-09-08 13:39 EDT
Conferencing ID:		Conferencing URL:	
Restricted Directory Search:	Yes	All Organization Members Can Create Projects:	Yes
Template:	Demo Template	Subscriber:	Yes

To modify hidden PTC Windchill source parameters

1. Refer to "Adding an Explicit Connector Parameter" on page 29 to add one or more PTC Windchill hidden source parameters.

2. For a new PTC Windchill 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 PTC Windchill 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 PTC Windchill 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.

8.2 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.

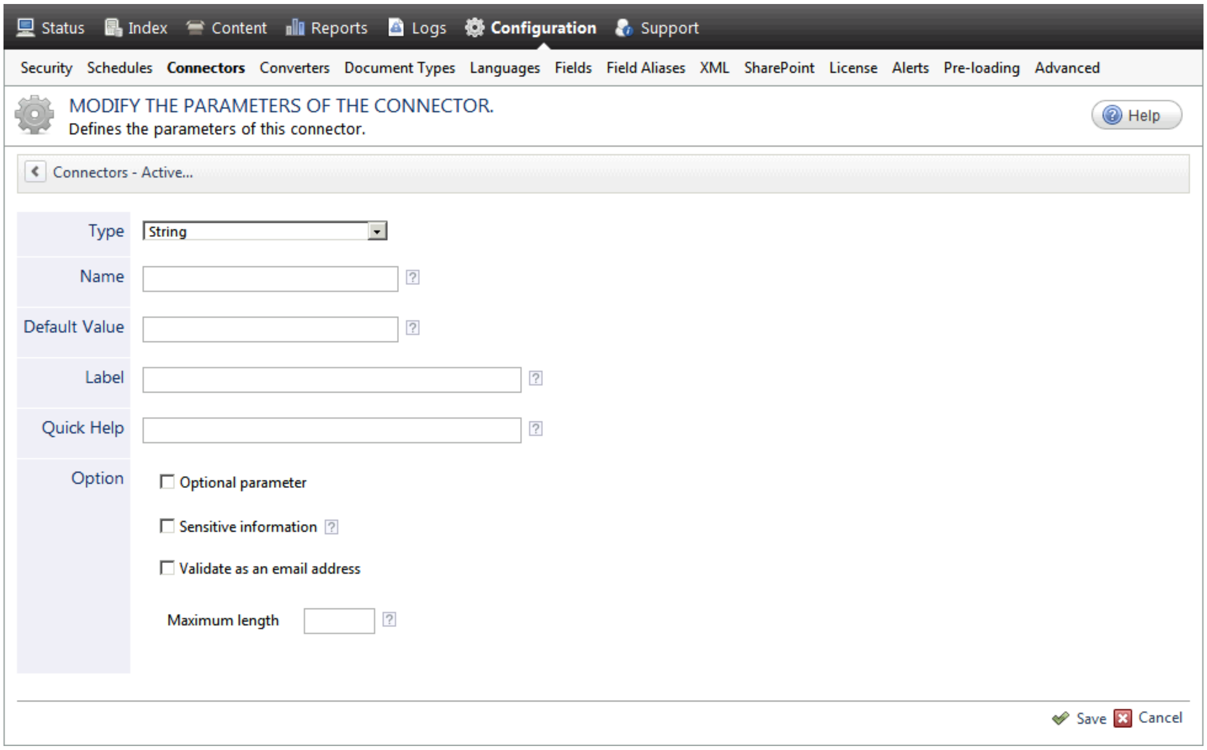
You can however choose to make one or more of these parameters appear in the **Add Source** and **Source: ... General** pages of the Administration Tool so that you can change their default value.

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.