Coveo Platform 7.0

Microsoft Active Directory 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-120819-EN

Publication date: 1/3/2019

Table of Contents

1. Microsoft Active Directory Connector

You can use the Microsoft Active Directory connector to index user information stored in Active Directory. The connector uses incremental refresh to periodically query Active Directory for the latest content modifications and keep the index up-to-date.

Deployment overview

1. Create a user identity for your Active Directory source

   The Active Directory content is accessible in read-only to any user from the domain or from a trusted domain. The Active Directory connector can therefore use any Active Directory user to crawl and index the Active Directory content. You must configure a CES user identity that contains information about the user you choose to use (see "Adding a User Identity" on page 2). You will later assign this user identity to your Active Directory source and security provider.

   Note: A best practice is to create an Active Directory user dedicated to the CES connector and for which the password never changes.

2. (Optional) Modify the default Active Directory security provider or create a new one

   Coveo Enterprise Search (CES) comes with a default Active Directory security provider. You can modify this security provider or create new ones to connect to a specific Active Directory domain (see "Configuring an Active Directory Security Provider" on page 4).

   Example: In your organization, there are several Microsoft Windows domains. You want to index the Active Directory content of *Domain A* while CES is running in *DomainC*. You can create a *Domain A* security provider and assign it to a *Domain A* Active Directory source to index only the Active Directory content of this domain.

3. Configure and index a Microsoft Active Directory source (see "Configuring and Indexing an Active Directory Source" on page 9).

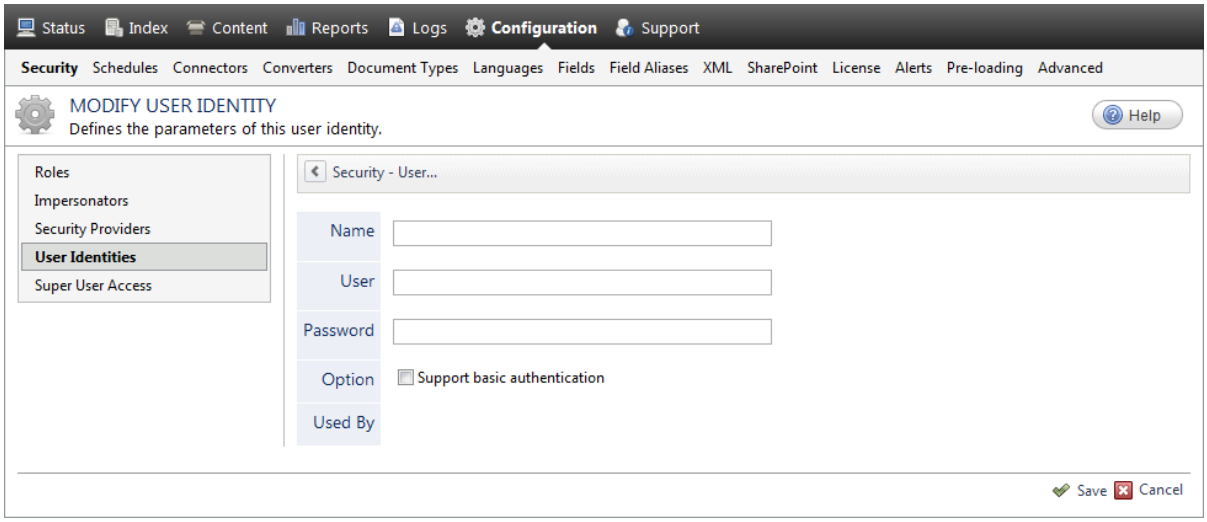
2. Adding a User Identity

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.

3. Configuring an Active Directory Security Provider

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

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

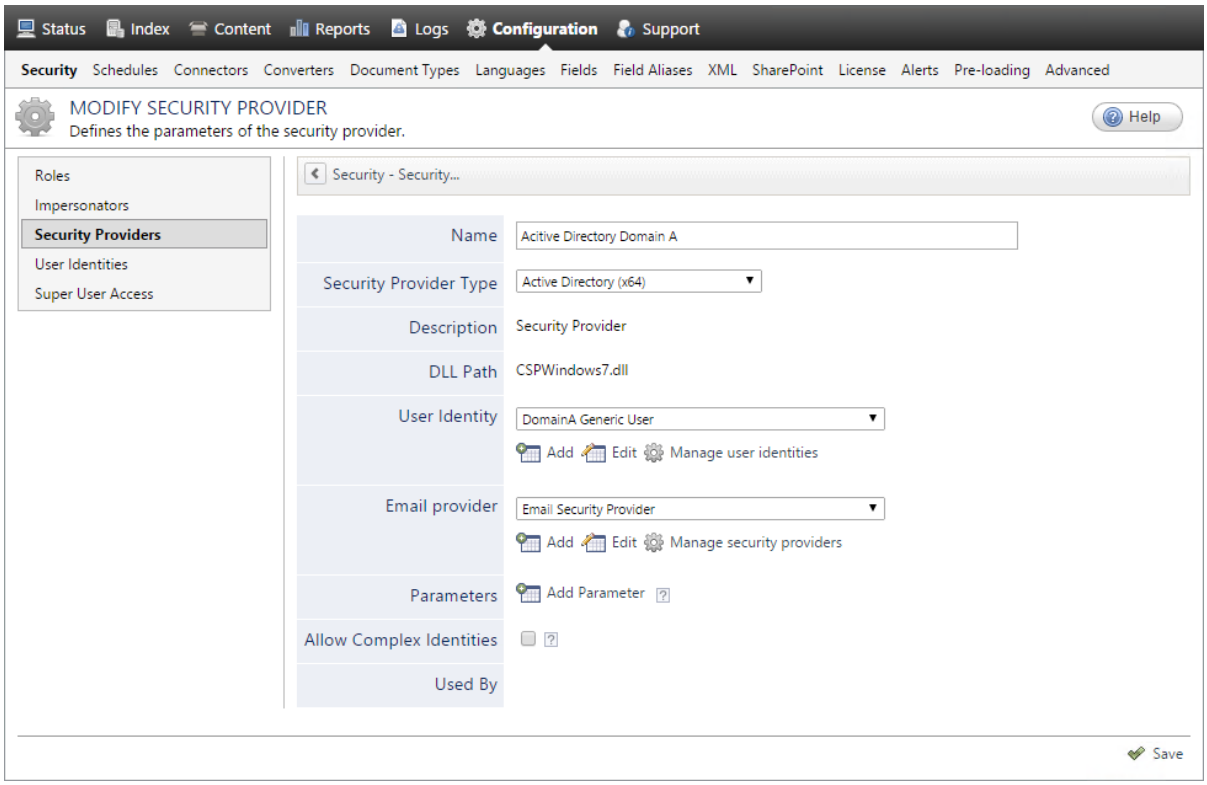
You may need to create another Active Directory security provider only when CES and AD are in different and untrusted domains. In this case, you only need to assign a user identity containing any user that has access to the other domain to be able to use the security provider to expand, map, or resolve users or groups defined in Active Directory of this domain.

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

To create or modify an Active Directory security provider

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

What's Next?

When you are creating or modifying the security provider:

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

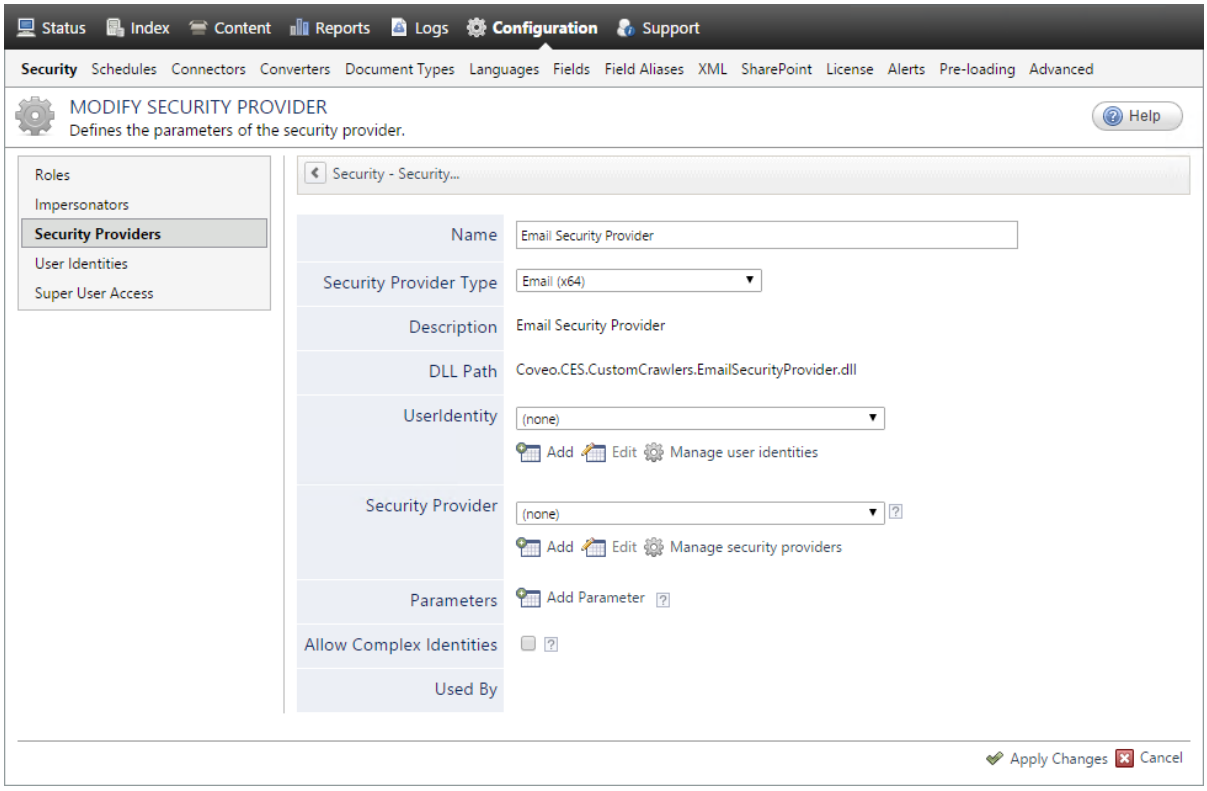
4. Configuring an Email Security Provider

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

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

To configure an Email security provider

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



   a. In the **Name** box, enter a name of your choice for your Email security provider.
   b. In the **Security Provider Type** list, select **Email**.

Note: CES 7.0.5785 to 7.0.5935 (August to September 2013) The Email security provider DLL file is missing in the CES distribution so you will not see the **Email** option in the **Security Provider Type** list.

To resolve this issue:

i. Contact Coveo Support to get a copy of the `Coveo.CES.CustomCrawlers.EmailSecurityProvider.dll` file.

ii. When you receive the file, using an administrator account, connect to the Coveo Master server, and then copy the file to the `[CES_Path]\bin` folder.

iii. When your Coveo instance includes a Mirror server, also copy the file to the `[CES_Path]\bin` folder on the Coveo Mirror server.

iv. Restart the CES service so that the new DLL is recognized.

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

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

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

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

f. Click **Apply Changes**.

What's Next?

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

5. Configuring and Indexing an Active Directory Source

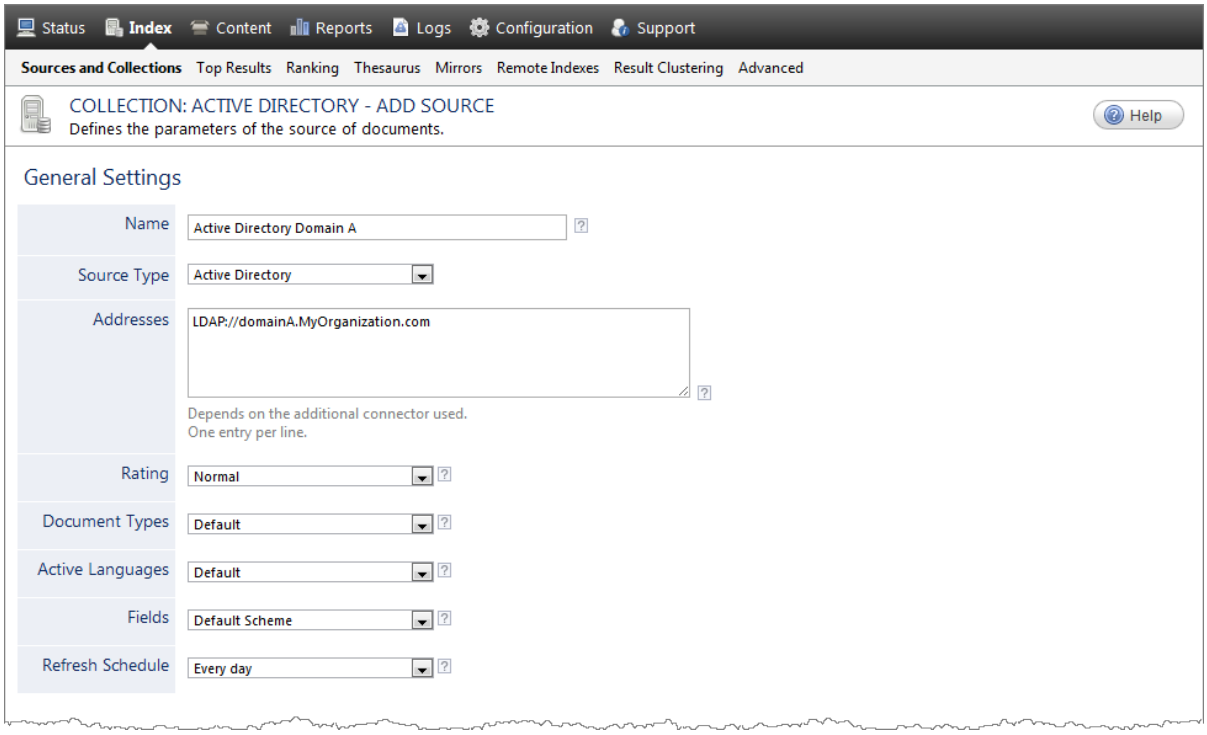
A source defines a set of connector parameters specifying where and how to crawl Active Directory in a given domain. The Coveo connector for Microsoft Active Directory uses the Lightweight Directory Access Protocol (LDAP) to read Active Directory content. The connector performs an LDAP search to find all the items to index.

To configure and index an Active Directory 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**.
5. In the **General Settings** section of the **Add Source** page:



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

Name

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

Example: `Active Directory Domain A`

Source Type

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

Addresses

The list of LDAP URIs indicating the starting locations to index, one entry per line.

Example: With the `domainA.MyOrganization.com` domain, acceptable values can be:

- `LDAP://MyOrganization`
- `LDAP://domainA.MyOrganization.com`
- `LDAP://DC=domainA,DC=MyOrganization,DC=com`

If you want to select only users from a particular organization unit (OU), enter the address in the form: `LDAP://OU=ouName,DC=domainA,DC=MyOrganization,DC=com`

Important: In the LDAP URLs, you must enter the keywords (LDAP, OU, DC...) in uppercase.

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

Rating

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

Document Types

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

Active Languages

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

Fields

If you defined custom field 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 recommended **Every day** option instructs CES to refresh the source everyday at 12 AM.

Note: You can create new or modify existing source refresh schedules.

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

a. Enter the appropriate value for the following parameters:

Incremental Refresh Delay

Determines the time interval in seconds between incremental refresh updates. The default and recommended value is `3600` seconds (1 hour).

LDAP Filters

The filters used to refine the LDAP query to Active Directory. You typically want to crawl all the users in Active Directory. Depending on the configuration of Active Directory, you may find that unwanted users are crawled. The default value is `mail=*`. It allows to get all users that also have an Exchange Mailbox.

> **Note:** The connector includes a built-in hidden filter: `(&(objectclass=user)(objectclass=person))`. This is a logical AND operation that finds users that are real persons, eliminating other mailboxes. The filter you enter in **LDAP Filters** is added to the AND operation of the built-in hidden filter (ex.: `(&(objectclass=user)(objectclass=person)(mail=*))`).

Parameters

Click **Add Parameter** when you want to show advanced hidden source parameters.

b. In the **Option** section, review the value for the following parameters that often do not need to be modified:

Index Subfolders

Check to index all subfolders below the specified starting addresses. Selected by default.

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

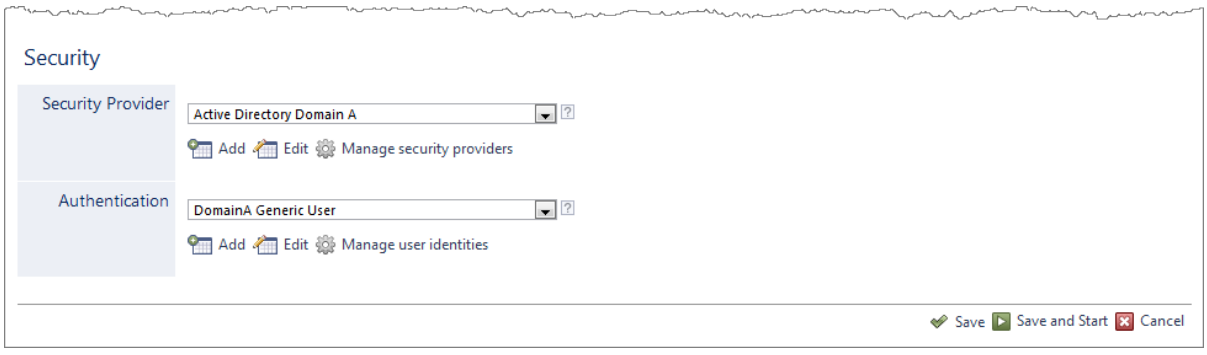
When you select this check box (recommended), at indexing time CES creates HTML versions of indexed documents and saves them in the unified index. In the search interfaces, users can then more rapidly review the content by clicking the Quick View link to open the HTML version of the item rather than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



a. In the **Security Provider** drop-down list, select the default, modified, or new Active Directory security provider that want for this source (see "Configuring an Active Directory Security Provider" on page 4).

b. In the **Authentication** drop-down list, select the user identity that you selected for this source (see "Adding a User Identity" on page 2).

c. Click **Save and Start** to save the source configuration and start indexing this source.

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

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

     OR

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

What's Next?

Set an incremental refresh schedule for your source.

Add the collection containing this new source to the scope of desired search interfaces.