WEST KM

ADMINISTRATOR GUIDE

VERSION 5.0.7

DECEMBER 2015

THOMSON REUTERS™

Customer Service

Technical Assistance

If you have general, research, or technical questions about Thomson Reuters West km, call Customer Technical Support at 1-888-937-8561, Monday through Friday, 7:00 a.m. to 7:00 p.m. central time. You can also visit our contact page at legalsolutions.thomsonreuters.com/law-products/support/west-km.

If you're researching an area of law you are unfamiliar with, it's not without its speed bumps. That's why we offer our customers free, unlimited, 24/7 access to Reference Attorneys, the industry's premier team of legal research assistance professionals. For research help, call the Reference Attorneys at 1-800-REF-ATTY (1-800-733-2889).

Billing and Account Assistance

For billing and account assistance, call Customer Service at 1-800-328-4880 or email customerservice@thomsonreuters.com. Billing and account assistance is also available online at legalsolutions.thomsonreuters.com/customer-service.

Reference Materials

For free reference materials, visit legalsolutions.thomsonreuters.com/guides. Our products also contain comprehensive, searchable instruction available via the **Help** menu in the application.

Disclaimer

Thomson Reuters disclaims any and all liability arising from the use of this document and does not guarantee that any information contained herein is accurate or complete. This document contains information proprietary to Thomson Reuters and may not be reproduced, transmitted, or distributed in whole or part, in any form or by any means, without the express written permission of Thomson Reuters.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

This book expresses the author’s views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Thomson Reuters, nor its resellers or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Information in this guide is current through December 2015 (version 5.0.7). L-375677.

610 Opperman Drive
Eagan, MN 55123-1396

Contents

1 West km Overview

Welcome to West km, a knowledge management product that allows staff members at your legal organization to easily find and reuse your organization's best work.

West km Packages

Depending on your West km package (see following table), you will have the following West km product components, which are provided by the installation of various West km software components:

Package	Product Component	Software Component
West km Foundation Services	West km (Delivery and Indexing)	West km
	Search Component	Search Component
West km for Litigation	RID (Reference Identifier)	West km RID
	CaRE (Categorization and Recommendation Engine)	West km CaRE
	KeySearch	West km CaRE
	Document Analysis	Analyzer Component
West km for Transactions	Document Analysis	Document Analyzer
Other West km Tools	Vetting Toolkit	West km

- West km Foundation Services provides the core software components for West km. It integrates with your document management system (DMS) or stand-alone document collection and provides the following functions: security, administration, DMS integration, and indexing and search capabilities.
- West km for Litigation integrates KeyCite, full-text search technology, and KeySearch with your organization's internal documents, such as briefs, pleadings, and memos. Members of your organization can build a citations list of your organization's documents that cite a WestlawNext document. They can also retrieve documents using full-text search methods and the KeySearch hierarchy of legal topics. In the WestlawNext interface, they can access your organization's internal documents and WestlawNext content simultaneously.

  With Drafting Assistant, members of your organization can use BriefTools to embed citation links and KeyCite status flags in word-processing documents, providing instantaneous views of the validity of legal citations in the document, as well as easily search internal litigation documents while working in their word processor and then add that information to an existing draft document
- West km for Transactions provides searching and drafting capabilities based on your organization's internal transactional documents, such as agreements, forms, and regulatory filings. Members of your organization can search by documents, clauses, and defined terms.

  With Drafting Assistant, members of your organization can easily find internal documents, clauses, and defined terms while working in their word processor and then add that information to an existing draft document.
- The West km Vetting Toolkit helps you fine-tune the selection of documents from your DMS before indexing them in West km for Litigation or West km for Transactions.

Product Information

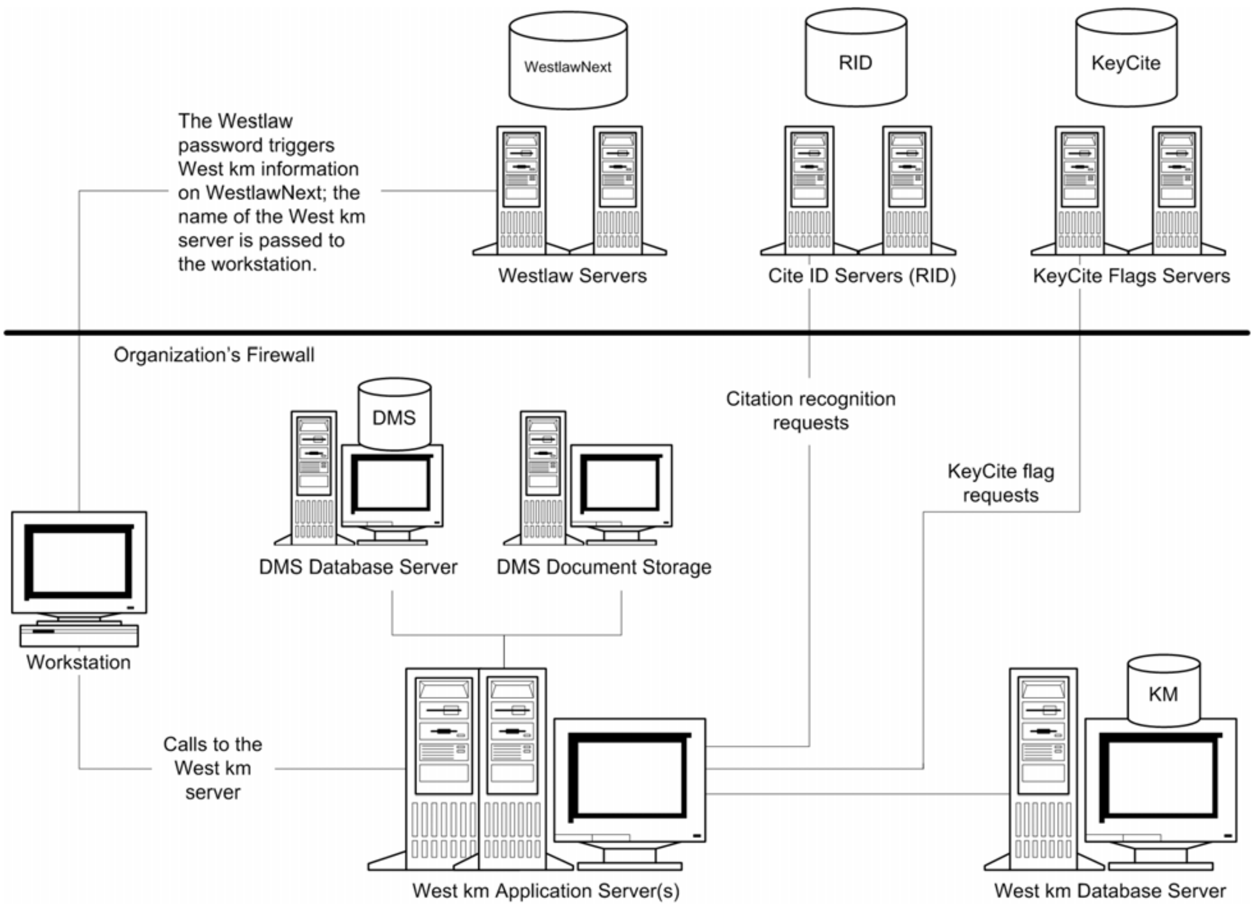
West km product information is available at these locations:

- Help is available in the West km interface. Click **Help** on the toolbar at the top of pages for general help information. Click Help next to a page heading for information about tasks related to that page.
- The website for West km is available at legalsolutions.thomsonreuters.com/law-products/solutions/westkm.
- The West km Knowledge Base is available at kbportal.thomson.com/westsolutions (A username and password is required and can be obtained by calling 1-888-WESTKM1.)
- The Drafting Assistant Installation Guide is available at http://legalsolutions.thomsonreuters.com/law-products/c/Drafting-Assistant-Installation-Guide.

System Overview

SYSTEM DIAGRAM

A system diagram of West km:



For detailed hardware and software requirements for West km, visit legalsolutions.thomsonreuters.com/law-products/solutions/westkm and click View System Requirements under Product Support.

SERVER COMPONENTS

When West km software components are installed, these West km server components are created:

Delivery server: The West km delivery server is the center of West km operations. It provides the front- end administration, schedules indexing, and uses the Internet to access and display indexed documents.

Indexing server: The West km indexing server converts documents to HTML, finds citations in documents, assigns documents to KeySearch legal topics, mines document data, and records document information (e.g., citation locations, KeySearch assignments) in the West km database.

- RID (reference identifier) engine software identifies citations.
- West's categorization and recommendation engine (CaRE) software assigns documents to KeySearch legal topics.
- Document analysis software extracts and tags significant content in documents. It provides metadata that is searchable and displayed in search results and summaries.

West km database server:

- The West km database stores metadata about documents (e.g., KeyCite data about document citations, KeySearch topic assignments), document profile metadata, data for indexing scheduling, and KeySearch data.
- The West km RID database stores WestlawNext document references for citation identification. Once a citation is found, a call is made to the Cite ID (RID) servers at Thomson Reuters to validate the citation and return serial numbers and other metadata for the target document.

- The search component uses these databases for full-text indexing and searching:
  - The CCI database contains information about how documents are indexed and searched.
  - The Doc database contains information about the documents that are indexed.
  - The Persist database contains search state information.

HTML repository/search server: The West km HTML repository/search server stores HTML renderings of indexed documents, stores .rdf files, which contain profile metadata at the file level, and performs full-text indexing and searching of documents.

DMS server: West km gets your organization's documents and related metadata from where documents are housed on your organization's document management system.

Cite ID servers (RID): RID servers at Thomson Reuters validate citations found in documents and return serial numbers and other metadata for linking to the target documents on WestlawNext.

Westlaw servers: Westlaw servers at Thomson Reuters host Westlaw services.

KeyCite flags servers: KeyCite flags servers at Thomson Reuters determine the current KeyCite status of a citation. When a West km document is opened that contains citations, KeyCite flags servers are called to get the latest status flags.

Accessing West km

You can retrieve documents that you index with West km via:

- The West km interface.
- WestlawNext (West km for Litigation).
- Your word processor (Drafting Assistant).

The West km interface is also used to administer the application and to index documents.

To access the West km interface after installation, open your web browser and go to *hostname/km*, where *hostname* is the name by which your delivery server is known on your network.

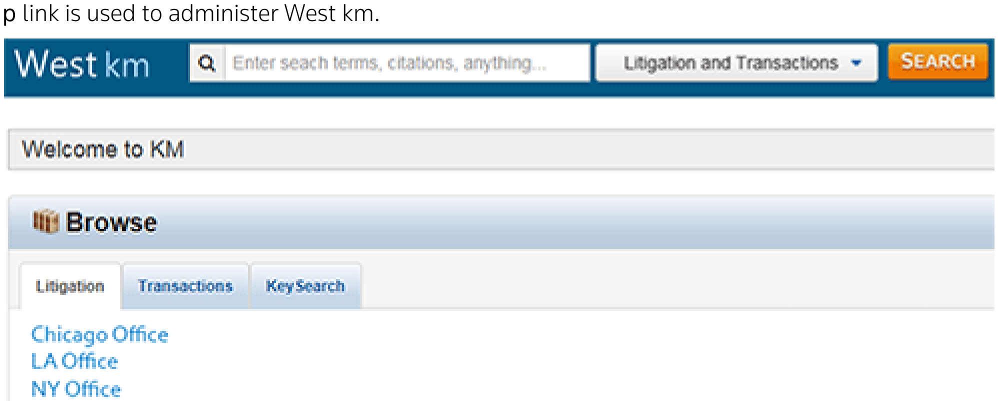
WESTLAWNEXT INTERFACE

With West km for Litigation, you can retrieve indexed West km documents via the WestlawNext interface. West km members can search just your organization's documents, or they can search your organization's documents and WestlawNext documents simultaneously.

WEST KM INTERFACE

West km includes the following product tabs and administrative links:

- The Litigation Libraries tab is used to retrieve indexed documents in West km for Litigation.
- The Transactions Libraries tab is used to retrieve documents configured to be processed by the transactional analysis component in West km for Transactions.
- The KeySearch tab is used to retrieve documents that are relevant to your research topic by selecting from a hierarchy of legal topics in West km for Litigation.
- The Setup link is used to administer West km.



WEST KM SETUP PAGES

To access the setup pages for West km, click the Setup link on the toolbar and then click the tab for the feature you want to access.

The setup page allows you to perform administrative functions for West km, including the following:

- Field Display: Set display settings for West km fields. For details, see "Changing Field Display Settings" on page 13.
- User Interface: Access and change user interface settings. For details, see "Changing User Interface Settings" on page 14.
- System Settings: Access and change system settings and view your West km configuration, including available product components and the versions of installed software components. For details, see "Changing System Settings" on page 21.
- Professionals: Administer your West km users. For details, see "Managing Users" on page 85.
- HTML Storage: Schedule or launch full-text indexing of documents. For details, see "Full-Text Indexing" on page 37.
- Data Source Management: Designate DMS databases or libraries that contain the document collections you want indexed. For details, see "Adding Data Source Connections" on page 39.
- Indexing: Define and index document collections and set up your indexing servers. For details, see "Indexing Documents" on page 71 and "Setting Up the Indexing Server" on page 43.
- Vetting: Access the West km Vetting Toolkit to identify and tag documents from select document management systems for inclusion in West km. For details, see "Vetting Documents" on page 54.
- Usage Reporting: View West km usage data for your organization. For details, see "Reporting on Usage" on page 99.

To access all functionality in the West km setup pages, you must have administrator rights in the system.

Configuring Antivirus and Browser Software

CONFIGURING ANTIVIRUS SOFTWARE

Due to the design of Microsoft ASP.NET (included with the .NET Framework), antivirus software with real-time monitoring enabled may cause random restarts of the .NET application. This problem occurs because some antivirus applications write information back to the files they scan, causing the application to restart.

To resolve this problem, exclude the following from the antivirus scan list:

- *[West km installation folder]*\Global.asax
- *[West km installation folder]*\Web.config
- *[West km installation folder]*\bin*.*
- %SystemRoot%\Microsoft.NET\Framework*[.NET version]*\CONFIG\machine.config

For more information about this issue, see the Microsoft knowledge base article 312592.

CONFIGURING BROWSER SECURITY

Depending on the browser that end users will use to access West km, make the following changes to the browser security configuration on end-user systems. These changes will add West km and Westlaw services to the list of trusted sites.

Microsoft Internet Explorer

If your end users will access West km on Internet Explorer, make the following security configuration changes on end-user systems.

1. On the Internet Explorer Tools menu, click Internet Options.
2. On the Security tab, select Trusted sites and then click Sites.
3. In the Trusted Sites dialog box, add these websites to the zone and then click Close:
   - *.westlaw.com
   - help.westkm.com
   - the URL to your West km server, e.g., http://westkmservername
4. On the Security tab, click Custom Level.
5. In the Security Settings–Trusted Sites Zone dialog box, scroll to the Miscellaneous section. Under Display Mixed Content, select Enable and click OK.

Firefox

If your end users will access West km on Firefox, make the following security configuration changes on end-user systems.

1. Type `about:config` in the address bar and press Enter.
2. Click the I'll be careful I Promise! button.
3. Set security.mixed_content.block_active_content to false by double-clicking the entry.

Google Chrome

If your end users will access West km on Chrome, make the following security configuration changes on end-user systems.

1. Right-click a Chrome shortcut and select **Properties**.
2. In the **Target** field, add `--allow-running-insecure-content` to the end of the field value (e.g. `C:\Program Files (x86)\Google\Chrome\Application\chrome.exe --allow- running-insecure-content`).

Enabling Features for End-Users

ENABLING SEARCH FUNCTIONS

When you first install West km, search functions are disabled in case you want to index documents before making the search pages available to your end users.

To enable the search functions,

1. Access the West km interface. For details, see "Accessing West km" on page 3.
2. Click **Setup**.
3. Click the **User Interface** tab.
4. In the left frame, click **General**.
5. Under General Settings, select these settings:
    - Activate West km for Litigation
    - Activate West km for Transactions
6. Click **Save**.

After the search functions are enabled, your end users can search documents in West km by opening a supported web browser and going to *hostname*/km, where *hostname* is the name of your West km delivery server on your network.

ENABLING EMAIL CAPABILITY

Your West km end users have the capability to email documents from West km. To enable this feature, you must enter information about the SMTP server that will be used to email documents.

To enter your SMTP server information,

1. Access the West km interface. For details, see "Accessing West km" on page 3.
2. Click **Setup**.
3. Click the **User Interface** tab.
4. In the left frame, click **Email**.
5. In the right frame, enter information for your SMTP server. For details about the settings, see "Changing System Settings" on page 21.
6. Click **Save**.

2 Configuring Data Source Integration

If your organization is indexing documents that are managed by a document management system, make the following configuration changes as indicated below, depending on your product.

- See your product's section under Setup, Data Source Management, Settings (see "Changing Data Source Settings" on page 24 for more information) to make changes to West km system settings to control communication between your document management server and West km components.
- See "Appendix D: Authentication and Document Security Configuration" on page 118 for details about the configuration that is required for West km document security and authentication to function properly with your document management system.

Additional setup steps may also be necessary, depending on your product. Refer to the following sections for details:

Configuring eDocs DB

To access and change settings for the eDOCS DB integration,

1. Click **Setup**.
2. Click the **Data Source Management** tab.
3. Under **Settings**, click **eDOCS DB**.
4. Make the changes you want to the settings on that page. Settings are described in the following table.
5. Click **Save**.

Field Name	Description
Security Lump Size	SQL statement group size parameter used when retrieving security attributes for documents. The recommended range is 75-250. The default value is *100*.
Security Cache Groups	If selected, group permissions are checked for users on a per-process basis. This setting is not selected by default.
Use Client Matter Metadata	If selected, client matter metadata is loaded from the DMS database. This setting is selected by default.
Use Combined Client Matter	If selected, creates a combined client and matter ID and a combined client and matter name in West km. This setting is selected by default. Note: You can set the separator character (e.g., a hyphen "-") between IDs and names using *Client-Matter Separator* at the Setup, User Interface, General page.
Use Sub Versions	If selected, sub-versions are used for documents. Changing this setting requires re-indexing. This setting is not selected by default.
Use Matter Custom Sql	If selected, the client ID, client name, matter ID, and matter name are retrieved from custom fields instead of the default fields. This setting is not selected by default.
Matter Custom Sql	A valid SQL query used to retrieve the client ID, client name, matter ID, and matter name from custom fields. The following aliases must be used: • client_id • client_name • matter_id • matter_name

Field Name	Description
	This setting is ignored if *Use Matter Custom Sql* is not selected.
Use Document Type (Class) Custom Sql	If selected, the document type (class) is retrieved from a custom field instead of the default field. This setting is not selected by default.
Document Type (Class) Custom Sql	A valid SQL query used to retrieve the document type (class) from a custom field. The custom_class alias must be used. This setting is ignored if *Use Document Type (Class) Custom Sql* is not selected.
Custom Fields	Allows you to map a custom field in West km to data in eDOCS DM. • In the table, find an empty row that matches the content type of the custom field: String, Boolean, Date/Time, or Integer. • Type the name of the field as it is known in eDOCS DM in *databaseowner.tablename.fieldname* format in the **DMS Field** text box. • If the field is not part of the Profile, People, DocumentTypes, Components, or Versions table in eDOCS DM, specify how the field's table is joined to one of those tables by typing a SQL statement in the **JOIN** text box.

Configuring NTFS File System

To add a connection for the NT file system,

1. Click **Setup**.
2. Click the **Data Source Management** tab.
3. On the **Connections** page, click **New Data Source**.
4. Enter the information in the following table.

Field Name	Description
Type	The data source used to manage the documents (i.e., **NTFS**)
Server	The name of the server containing the documents you want to index. The server name must use only alphanumeric characters; underscores are not allowed.
Library	The shared location used to store documents on the server. For example, if the server and share is `\\pheasant\documents`, then type `documents`.

5. If you want to select a library group for this data source, see "Library Groups" on page 72.
6. Click **Save**.

Configuring iManage Work

If you are indexing documents stored in (iManage Work), make the following configuration changes.

Because the West km servers and your iManage Work product are installed on separate machines, you need to register the iManage .dll file on each West km server that has the delivery or the indexing component installed. This .dll file allows West km servers to communicate with your organization's document management server.

1. Locate a computer that has the iManage Work client installed on it. If you have a 64-bit iManage Work server product, access a 64-bit iManage Work client. If you have a 32-bit iManage Work server product, access a 32- bit iManage Work client.
2. On the client computer, find a file named iManage.dll (assuming you have not renamed the file). To find the .dll you can do one of the following:
   - Go to the installation folder for the iManage Work client (e.g., *[Drive]*:\Program Files\Interwoven\ iManage Work). Look for iManage Work.dll in that folder.
   - Click the **Start** button, choose **Run**, type **regedit**, and then search for iManage.dll. When found, it will show you the location of the .dll.
   - Search the hard drive for iManage Work.dll.
3. Copy the iManage Work.dll file to the bin subfolder of the installation folder on the West km server, e.g., *[Drive]*:\Program Files\Thomson\KM\bin.

4. At a command prompt on the West km server, type `regsvr32 [West km installation folder]\bin\iManage Work.dll` and click OK.
5. For example, type `regsvr32 "D:\program files\thomson\KM\bin\iManage Work.dll"`.
6. Repeat steps 3-4 for each West km server that has the delivery or the indexing component installed.
7. Adjust the value for the Version setting at Setup, Data Source Management, Settings, iManage Work according to your iManage Work client .dll version. (For instructions on setting system options, see "Changing System Settings" on page 21.)
8. The supported values for this setting are 1.0 and 8.0. If the .dll is numbered in a format of 1.#.#.#, set the value to 1.0. If the .dll is numbered in a format of 8.#.#.# or higher, set the value to 8.0.

To determine the iManage Work client .dll version, right-click iManage.dll, choose Properties, and click the Version tab. The .dll version is listed at the top of the dialog box as the File Version.

Configuring iManage Work in the Cloud

If you are indexing documents stored in iManage Work in the Cloud, you cannot also maintain physical connections to iManage Work. That is, legacy connections to iManage Work need to be removed in order to set up connections to iManage Work in the Cloud.

A proxy configuration is required before indexing documents in iManage Work in the Cloud.

PROXY SETTINGS

Go to the Setup, System Settings, Server Configuration page (see "Changing System Settings" on page 21 for more information) and enter the following:

- Web Proxy Host: The IP address or URL for your proxy server.
- Web Proxy Port: The port number used by the proxy server.

Entering your proxy server settings enables West km to communicate through your firewall to access documents from iManage Work in the Cloud.

Note iManage Work in the Cloud also requires a DMS User ID. To enable and test security, you need to select this option.

Configuring NetDocuments

Be sure to set the following West km system options before indexing documents stored in NetDocuments.

PROXY SETTINGS

Go to the Setup, System Settings, Server Configuration page (see "Changing System Settings" on page 21 for more information) and enter the following:

- Web Proxy Host: The IP address or URL for your proxy server.
- Web Proxy Port: The port number used by the proxy server.

Entering your proxy server settings enables West km to communicate through your firewall to access documents from NetDocuments.

NETDOCUMENTS SETTINGS

Go to the Setup, Data Source Management, Settings, NetDocuments page (see "Changing Data Source Settings" on page 24 for more information) and enter the following:

- Categories List Search: Identify a NetDocuments saved search that retrieves a list of other saved searches (or categories) for retrieving the documents you want to index in West km. The individual saved searches can be selected in West km for creating and indexing document collections. The individual saved searches retrieved by this global search must meet these requirements: (1) They must be sorted by last modified date, descending, and (2) The documents retrieved must be publicly available to West km users.
- REST API Host: The path for the REST API Host. This setting is entered for you by default.
- REST API Version: The current REST API Version. This setting is entered for you by default.
- Redirect Proxy: The authentication server location for NetDocs to be used when a new token is required. This setting is entered for you by default.
- Days to Warn Before Token Expiration: Type the number of days before your token expires that you want to receive messaging. The default value is *90* days before the expiration date.
- User ID Required: Enable this option to require a DMS user ID for all users. This option will allow you to enable full security.

- **Field Mappings**: Type the name of the NetDocuments field you want to use for each West km field. If your organization has multiple cabinets in NetDocuments, the field names that you map to West km must match across cabinets.

Note If you do not see the NetDocuments option under Setup, Data Source Management, Settings, first add a data source connection for NetDocuments. For more information, see "Adding Data Source Connections" on page 39.

Configuring ProLaw

To access and change settings for ProLaw integration,

1. Click **Setup**.
2. Click the **Data Source Management** tab.
3. Under **Settings**, click **ProLaw**.
4. Make the changes you want to the settings on the page. Settings are described in the table below.
5. Click **Save**.

Author	Determines which author field is used from ProLaw when indexing a document *Adding Professional* (the default) will use the name of the person who added the document to ProLaw. *Prof Set* will use the name of the person set in the ProLaw document metadata field.
Custom Fields	Allows you to map a custom field in West km to data in ProLaw. • In the table, find an empty row that matches the content type of the custom field: String, Boolean, Date/Time, or Integer. • Type the name of the field as it is known in ProLaw in tablename.fieldname format in the DMS Field box. • If the field is not part of the Events, EventTypes, Professionals, EventMatters, or Matters table in ProLaw, specify how the field's table is joined to one of those tables by typing a SQL statement in the JOIN text box.

Using an Intermediate Database

If you store documents in a document management system that is not currently supported by West km, you can use an intermediate database (“generic database”) to index those documents in West km. To implement this solution, you

1. Create a database in Microsoft SQL Server.
2. Import data about the documents and attachments you want to index into this “generic” database.
3. Designate the database and document collection in West km for indexing.

Import utilities are available for populating the database when documents are stored using West km as a Web-hosted application. For additional information about these import utilities, request documentation from your West km representative.

To set up the generic database in Microsoft SQL Server, complete the instructions in the following subsections to create a database, a database user account, and the DocProfile table.

Note These instructions reflect procedures for Microsoft SQL Server 2008 R2.

CREATING A GENERIC DATABASE

Create a database in SQL Server by completing the following steps:

1. On a database server, click **Start** , click **All Programs**, click **Microsoft SQL Server 2008 R2**, and then click **SQL Server Management Studio**.
2. In the Connect to Server dialog box, verify the default settings, and then click **Connect**.
3. In the Object Explorer section of the SQL Server Management Studio window, connect to the SQL server that will contain the generic database.
4. Right-click the **Databases** folder and then click **New Database**.
5. In the New Database dialog box, in the **Database name** box, type a database name.
6. In the Database files grid under Path (you may need to scroll to the right), edit the path to the desired location for both the database and database log file.
7. You can either type the path in the text box or click the **Browse** button next to the text box and navigate to the path.
8. Click **OK**.

CREATING A DATABASE USER ACCOUNT

Create a database user account in SQL Server that has db_owner rights to access the generic database you created by completing the following steps:

1. In the Object Explorer section of the SQL Server Management Studio window, expand the folder for the new database you created, and then expand its **Security** folder.
2. Under the Security folder for the database, right-click **Users** and click **New User**.
3. In the Database User - New dialog box, complete these steps:
   - In the **User name** box, type a database username (e.g., `kmuser`).
   - In the **Login name** list, select your login name. Select a SQL Server authentication account, not a Windows authentication account.
   - In the **Database role membership/Role Members** list, select **db_owner**.
   - Click **OK**.

CREATING THE DOCPROFILE TABLE

Create a table named DocProfile within the generic database to house data about your documents by completing the following steps:

1. In the SQL Server Management Studio window, from the **File** menu, point to **Open**, and then click **File**.
2. In the Open File dialog box, navigate to the GenericDMS.sql file, select it, and click **Open**.
3. The GenericDMS.sql file is located in the DB subfolder in the West km installation folder on the delivery server.
4. In the Connect to Database Engine dialog box, type or select the name of your SQL server, select **SQL Server Authentication**, type the user name and password of a login account assigned to the dbcreator server role or higher, and click **Connect**.
5. From the drop-down list on the SQL Server Management Studio toolbar, select the generic database you created.
6. Click the **Execute** button on the toolbar. This step creates a table named DocProfile within the generic database to house data about your documents.
7. From the **File** menu, choose **Close**.

For more information, see "DocProfile Table Fields" on page 10.

DocProfile Table Fields

Column one in the following table lists the fields in the DocProfile table. Column two lists the West km field names that are used for displaying information about your documents.

Field Name[1]	West km Field	Data Type	Character Limit
DocID		text	450
DocFileName		text	255
DocFilePath		text	255
DocFile		bit	
DocCreatedDate	Created Date Time	datetime	
DocModifiedDate	Modified Date Time	datetime	
DocTitle	Title	text	255
DocNumber	Doc No	text	255
DocVersion	Version	text	20
DocAbstract	Abstract	text	max
DocClass	Document Type	text	255
AuthorName	Author	text	255
MatterID	Matter ID	text	100
MatterDesc	Matter Name	text	max
ClientDesc	Client Name	text	max
ToDelete		bit	
ClientID	Client ID	text	50
DMSQueryName		text	254
DMSQueryID		text	254
Deleted		bit	
Dirty		bit	
DocProfile		bit	
Custom1	Custom1	text	255
Custom2	Custom2	text	255

Field Name[1]	West km Field	Data Type	Character Limit
Custom3	Custom3	text	255
CustomBool	Custom Bool	bit	
CustomDate	Custom Date	datetime	
CustomInt	Custom Int	int	

[1] Required fields are shown in bold.

IMPORTING DOCUMENT DATA INTO THE GENERIC DATABASE

After you've created the generic database and the DocProfile table, populate the table with a record for each document you want indexed in West km.

- In addition to the required fields shown in bold (DocID, DocFileName, and DocModifiedDate) you must populate either DocFilePath or DocFile. DocFilePath is the full NTFS path, including the file name, where the physical document can be found (e.g., \\MyServer\MyDocument.doc). DocFile is used for inserting the physical document into the table. Choose the method you prefer.

Note If you opt to use DocFilePath and documents are stored on a Windows server, the file path must be a location to which a Windows domain user account has access. This account is designated under Remote Access at Setup, System Settings, Security.

- DocFileName is the name of the document, including the file extension (e.g., MyDocument.doc). DocTitle is the name of the document that appears in West km results. If DocTitle is not populated, then DocFileName will appear in West km results.
- The DMSQueryName and DMSQueryID fields are used to group documents into different document collections (e.g., office locations or practice categories). If you are using the West km DMS Import Utility these fields are populated when the utility is run. If you are not using a utility, you can populate DMSQueryName with collection names (e.g., Regulatory) and DMSQueryID with unique identifiers that define the locations of collections (e.g., *server:library*).
- The collection names in the DMSQueryName field are listed for selection on the Add Collection page when you add a document collection in West km. For more information, see "Adding Document Collections" on page 71. A document collection can also be tied to a library group, which allows your West km members to restrict searches of your internal documents by groupings. For more information, see "Library Groups" on page 72.
- The Deleted and Dirty fields are used by the West km DMS Import Utility when updating the database.
- The ToDelete field is not used.
- The DocProfile field automatically generates a GUID that is used by the West km DMS Import Utility.
- The Custom1, Custom2, Custom3, CustomBool, CustomDate, and CustomInt fields are optional. If you are using one or more custom fields in West km, you can populate these fields with the appropriate field data from your document management system. For more information, see "Custom Fields" on page 30.
- Populate the remaining fields as they correspond to fields used in your document management system.

ADDING THE DATABASE AND DOCUMENT COLLECTION TO WEST KM

To add a data source connection for the generic database in West km,

1. Access the West km interface. For details, see "Accessing West km" on page 3.
2. Click Setup.
3. Click the Data Source Management tab.
4. At the Data Source Management page, click Add New Source.
5. Enter the requested information, as indicated in the following table.

Field Name	Description
Type	The data source used to manage the documents (i.e., Generic Database).
Use Windows Authentication	You can choose whether West km accesses the generic database in Microsoft SQL Server via a database account or a Windows account. A database account is used by default. To use a Windows account instead, select this option and contact your West km representative for more information.
User Name and Password	When using database account credentials to access the generic database, the user name and password for the database user account (e.g., kmuser, kmgenericuser).

Field Name	Description
Server Name	The name of the server containing the generic database. (The server name must use only alphanumeric characters; underscores are not allowed.)
Library	The name of the generic database in Microsoft SQL Server.

6. If you want to select a library group for this data source, see "Library Groups" on page 72.
7. Click Save.
8. Define one or more document collections for the data source as usual from the Indexing Options page (for details, see "Rearranging Document Collections" on page 83).

It is your responsibility to keep the generic database in synchronization with your document management system; no mechanisms are built into West km to do so. As you update the generic database, West km synchronization processes work as usual.

3 Changing System Settings and Configuration Files

System settings and configuration files determine the configuration of West km. In the West km interface, you can change the following types of system settings:

- Field Display Settings (see "Changing Field Display Settings" on page 13 for more information)
- User Interface Settings (see "Changing User Interface Settings" on page 14 for more information)
- System Settings (see "Changing System Settings" on page 21 for more information)
- Data Source Settings (see "Changing Data Source Settings" on page 24 for more information)
- Index Settings (see "Changing Index Settings" on page 28 for more information)

In configuration files, you can set property values that control communication among the various West km components. For more information, see "Changing Configuration Files" on page 32.

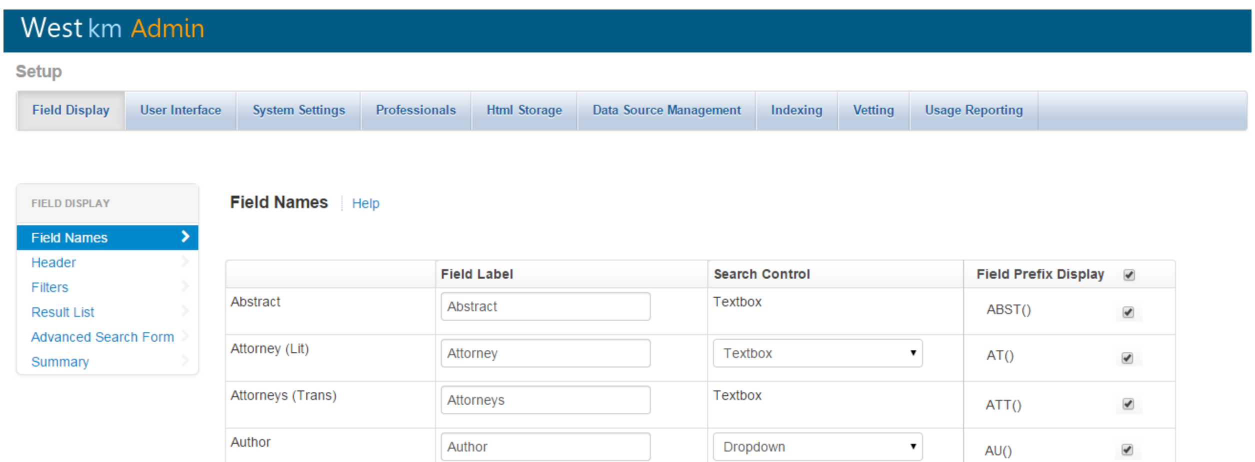
You can also map metadata to custom West km fields (see "Mapping Fields" on page 29 for more information) and set the document sort order (see "Setting Document Sort Order" on page 31 for more information).

Changing Field Display Settings

You can set display settings for West km fields, including field names and the particular fields that are displayed in various locations in the product interface.

To access and change field display settings,

1. Access the West km interface. For details, see "Accessing West km" on page 3.
2. Click **Setup**.
3. Click the **Field Display** tab.



4. In the left frame, click the type of settings you want to change.
5. In the right frame, make the changes you want to the settings. For details, see the following subsections.
6. Click **Save**. Changes take effect immediately.

For more information about fields and how to customize them in West km, see "Mapping Fields" on page 29.

Field Names: In West km, you can customize field labels for profile fields, analyzer fields, and West km fields (e.g., Library Group, Exemplar Document, and Exemplar Form). For several fields, you can also set the type of search control for the field on the Fields panel in the West km interface.

Field Label: In the Field Label column on the Field Names page, type the labels to use throughout West km when the corresponding field is used in the product interface. Labels with 10–15 characters are recommended for the best display, but more characters are allowed. The following characters are not allowed: " (quotation mark), ' (apostrophe), ; (semicolon), < (less than), > (greater than), & (ampersand).

Labels must be unique. In addition, the label for the Library Group field must not duplicate the name of any filter categories (e.g., Document Type) or searches will produce an error.

Search Control: In the Search Control column on the Field Names page, select the type of search control that you want to be displayed for the corresponding field on the Fields panel in the West km interface.

- Textbox: Search criteria can be typed in a text box. Terms from the documents or issues the user is researching, as well as connectors that specify the relationship between those terms, can be entered.
- Dropdown: A single option can be selected from a drop-down list. The options are unique values generated from the metadata about your West km documents. (This option is not recommended for fields having more than 100 unique values.)
- Lookup: Up to ten options can be selected from a look-up dialog box. The options are unique values generated from metadata about your West km documents.

The selected search controls do not display in the WestlawNext interface.

Field Prefix Display: In the Field Prefix Display column on the Field Names page, uncheck the box next to a field prefix to hide the display of the prefix in Advanced Search. Uncheck the box at the top of the Field Prefix column to hide all field prefixes.

Field name settings apply to both West km for Litigation and West km for Transactions.

Field Selections

You can select which fields are displayed in various locations in the product interface. The following table lists the locations.

Display of fields

Field Display Category	Field Display Location
Header[1]	Fields displayed in the document header when a document or document summary is viewed
Filters	Fields displayed as options for filtering your organization's document results
Result List[1]	Fields displayed in result lists and available as sortable categories after searching your organization's documents
Advanced Search Form	Fields displayed as possible field restrictions on the search form when searching your organization's documents
Summary	Fields displayed when a profile or summary of your organization's document is viewed

[1] The DMS Title and Modified Date fields are always displayed in the header and result lists, so they are not listed as options.

Litigation settings apply to West km for Litigation, and Transactions settings apply to West km for Transactions.

Move fields to the Selected box that you want displayed in the user interface. To move a single field to the Selected box, click it. To move all fields to the Selected box, click Select All.

Fields are displayed in the order in which you list them in the Selected box. To change the order, drag the field to a new location.

To remove a single field from the Selected box, click the X next to the field name. To remove all fields from the Selected box, click Remove All.

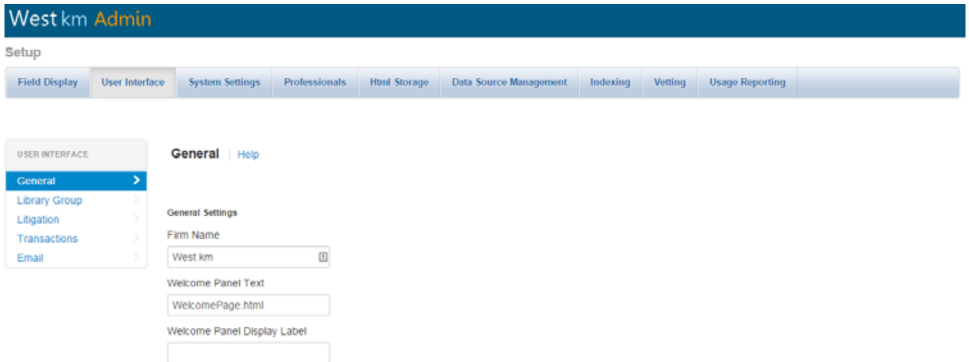
For the Result List subcategory, the ordering of fields in the Litigation section applies only to result lists in the West km interface. It does not apply to result lists in the WestlawNext interface.

Changing User Interface Settings

To access and change user interface settings,

1. Access the West km interface.
2. Click Setup.

3. Click the User Interface tab. The User Interface page is displayed.



4. In the left frame, click the type of settings you want to change.
5. In the right frame, make the changes you want to the settings. Settings are described in the following table.
6. Click Save.

User interface settings:

GENERAL	
General Settings	
Firm Name	The text to display for your organization's name in the WestlawNext interface. Space is limited to approximately 20 characters.
Welcome Panel Text	The file containing the text that is displayed in the West km interface on the Welcome panel and on WestlawNext as scope information on the West km home page. The default value is *WelcomePage.html*. This file is located within the custom subfolder of the installation folder (e.g., `[Drive]:\Program Files\Thomson\KM\Content\custom`). You may include HTML tags in the file to mark up text, but don't include elements such as html, head, title, and body. West km style will automatically be applied. You can change the file to customize the welcome text for your organization. So that your changes are not overridden upon upgrade, use a different file name and change this property value to match. The file must remain in the custom subfolder.
Enable West km Help	If selected, West km Help is available to all users.
Welcome Panel Display Label	The text that is used for the following: • The name of the Welcome panel in the West km interface. If no label is entered, the Welcome panel is not displayed. • The scope information label on the West km home page on WestlawNext. If no label is entered, the scope icon is not displayed. The default value is blank.
Expand Welcome Panel by Default	Determines whether the Welcome panel is expanded or collapsed by default when a West km user session is started. This is setting is not selected (the panels are collapsed) by default. Note: If *Welcome Panel Display Label* is not populated, then *Expand Welcome Panel by Default* is not available.
Prompt for Client ID	If selected, West km members are prompted to enter a client ID when accessing the West km interface. This ID is tracked with West km transactions, providing you with greater control over billing allocation. This setting is not selected by default.

Record Count Label	Determines the count of resulting documents from a full-text search and how that count is displayed. Options are as follows: • Default: Display is "Showing ## documents." The number is a definite count of the documents the user can access in the result list. • Approximate: Display is "Approx. ## documents." The number is an approximate count of the documents the user can access in the result list based on the results of the first set of documents processed. • More Than: Display is "More than ## documents." The number is the minimum documents the user can access in the result list based on the number of documents that have been processed, regardless of security. • None: No record count displayed. Note: With the Default and More Than options, no record count could be displayed on the initial result page when (1) results are displayed before all documents are processed (see the following *Search Process Count* setting), or (2) when full security is on, in which case the user may not have rights to all the resulting documents.
Activate West km for Litigation	If selected, searching for Litigation documents in West km is available to all users. If not selected, Litigation searching is not available to end users (it may be available to administrators). This setting is not selected by default.
West km for Litigation Label	In the West km interface, the name for content that is searched in West km for Litigation. The default value is *Litigation*.
Activate West km for Transactions	If selected, searching for Transactions documents in West km is available to all users. If not selected, Transactions searching is not available to end users (it may be available to administrators). This setting is not selected by default.
West km for Transactions Label	In the West km interface, the name for content that is searched in West km for Transactions. The default value is *Transactions*.
Enable Image View tab for Documents	If selected, users can click the Image View tab in West km to view image-based files (e.g., PDF) in their native file format. This setting is not selected by default.
Results List Page Size	The number of documents to list on each page of a result in the West km interface for both West km for Litigation and West km for Transactions. The default value is *20* (recommended). For best results, do not exceed 100.
Default Result List	When searching both litigation and transactional content sets, the result set that is displayed by default. The default value is *Litigation*.
Display only Litigation Content in Litigation Results	Select this option to hide transactional content in litigation search/browsing results.
Display only Transactional Content in Transactional Results	Select this option to hide litigation content in transactional search/browsing results.
Search Process Count	The number of documents to process before displaying results for full-text searches. The default value is *200*.

<table>
<tr><td></td><td>Notes about search performance:
Values above the default (200) may degrade performance.
For best performance, maintain a 1:5 ratio between Search Process Count and Search Max Hits (e.g., 200:1000). If you have a powerful processor, you may want to increase the ratio (e.g., 100:1000).
For NetDocuments users, it is recommended you set this value to 100, and set the Search Max Hits value to 200 for best performance.
When the Search Process Count setting is less than the Search Max Hits setting (recommended), results may display before all documents are processed. See the Record Count Label setting for more information about how the document count displays in the user interface.</td></tr>
<tr><td>Search Max Hits</td><td>The maximum number of documents to process for full-text searching. (Searches using the Natural Language search method return a maximum of 100 documents, even if the value is set over 100.)

The default value is 1000.

Note: For best performance, maintain a 1:5 ratio between Search Process Count and Search Max Hits (e.g., 200:1000). If you have a powerful processor, you may want to increase the ratio (e.g., 100:1000). For NetDocuments users, it is recommended you set this value to 200, and set the Search Process Count value to 100.</td></tr>
<tr><td>Search Query Timeout</td><td>Maximum amount of time in seconds to wait for SQL queries to complete. If the time-out period is exceeded, an exception is generated and the document is not indexed.

The default value is 60.</td></tr>
<tr><td colspan="2">LIBRARY GROUPS</td></tr>
<tr><td>Use Library Groups</td><td>If selected, displays library groups in the West km interface, in the WestlawNext interface, and on setup pages.

This setting is selected by default.

(For the change to take effect for any currently running West km sessions, the Web browser must be closed and reopened.)</td></tr>
<tr><td>Persist Library Groups</td><td>If selected, the library groups that a user has searched previously will be remembered when the user performs a new search. If not selected, all library groups are selected for new searches. (When an existing search is edited, library groups always persist from the original search.)

This setting is selected by default. This value is only used if the Use Library Groups setting is selected.</td></tr>
<tr><td>Do not display Litigation Library Groups on Transactions Tab

Do not display Transactions Library Groups on Litigation Tab</td><td>If Do not display Litigation Groups on Transaction Tab is selected, library groups are hidden from end users in West km for Transactions if no document collections within the library group are processed by the transactional analysis component. This setting is selected by default.

If Do not display Transactions Groups on Litigation Tab is selected, library groups are hidden from end users in West km for Litigation if all document collections within the library group are processed by the transactional analysis component. This setting is not selected by default.

If both options are selected, library groups are displayed or hidden as follows:
<table>
<tr><th>Library Group</th><th>Transactions</th><th>Litigation</th></tr>
<tr><td>Library Group A includes:
Collection 1 – trans analyzed
Collection 2 – trans analyzed</td><td>Displayed</td><td>Hidden</td></tr>
<tr><td>Library Group B includes:
Collection 1 – not trans analyzed</td><td>Hidden</td><td>Displayed</td></tr>
</table></td></tr>
</table>

Collection 2 – not trans analyzed		
Library Group A includes: Collection 1 – trans analyzed Collection 2 – trans analyzed	Displayed	Displayed

Unassigned Library Group Label	Text label used for documents that are in a collection without an assigned library group. This unassigned library group is only displayed on search pages if a collection exists that does not have a library group assigned to it. The default value is *Unassigned*. (For the change to take effect for any currently running West km sessions, the Web browser must be closed and reopened.)
Use Active Directory Groups to Hide/Show Library Groups	Select this option to limit access to library groups to assigned Active Directory groups. This setting is available only if Integrated Windows Authentication (IWA) is being used. If this option is selected, the table of **Current Library Groups** displays an Active Directory Groups column and provides the ability to add, and edit Active Directory Group assignments. To show all Active Directory Groups assigned to a library group, click **Show Details**. • To provide Active Directory Groups with access to the library group, click **Add**, select one or more Active Directory Groups, and click **Save**. • To edit the Active Directory Groups with access to the library group, click **Edit**, select or uncheck one or more Active Directory Groups, and click **Save**. When this option is selected, administrators can see all library groups, regardless of the administrator's associated Active Directory access. To apply the Active Directory group security to administrators, select the **Apply Active Directory Security to Administrators** option.
Current Library Groups	Allows you to add, rename, or delete library groups. • To add a library group, click **Add Library Group**, type a library group name, and click **OK**. • To rename an existing library group, click **Rename** next to the library group name, type a new name, and click **OK**. • To delete an existing library group, click the red **X** next to the library group name. Note: A library group cannot be deleted if it is being used by one or more document collections. In this situation, first edit those document collections so they use a different library group. To view the library groups currently in use, access the Indexing, Manage Collections page and check the Library Group column in the table.
LITIGATION	
Show Attorney links Show Company links Show Expert links Show Law Firm links Show Judge links	If selected, references to validated content in documents and document summaries will link to profiles on Westlaw Profiler. Content includes attorneys, companies, experts, law firms, and judges (primary or secondary). In documents, the name is linked. In document summaries, a "Westlaw Profile" link is displayed after the name. Links are not displayed in headers or result lists. Setting are selected by default. Note: • If you enable settings, accessing a profile is a billable transaction if you don't have a subscription to Westlaw Profiler. • Links are inserted into documents during rendering, so enabling settings does not require reindexing.
Show Secondary Judge	When selected, shows the Include Secondary Judge References check box on advanced search pages beneath Judge–Primary. (Primary judges are identified in document captions. Secondary judges are referenced in the text of documents.) In addition, when the Show Secondary Judge

	option is selected, the Judge–Primary drop-down list and look-up control include names of secondary judges. Note For the Include Secondary Judge References check box to display, the judge field must also be selected to display at Setup, Field Display, Advanced Search Form, Litigation. This setting is selected by default.
Show Search Terms in Results List (Litigation)	Determines whether the result list shows and highlights search terms in West km for Litigation. This setting affects result lists in both the West km and WestlawNext interfaces. This setting is selected by default.
Number of Words to Display before and after Search Terms in Result List (Litigation)	When searching full text, indicates the amount of text (in number of words) to show before and after each search term in West km for Litigation. Note: Surrounding text is not displayed beyond the boundaries of a paragraph, a table cell, or text that defines metadata for a title, attorney, law firm, governing law, or party For this setting to function, *Show Search Terms in Result List* must be selected. The default value is *20*.
Number of Search Term Hits to Display in a Result List (Litigation)	When searching full text or titles, indicates how many search term references to show in West km for Litigation. For this setting to function, *Show Search Terms in Result List* must be selected. The default settings is the first three search terms.
Terms and Connectors Search Result Sort Order (Litigation)	In West km for Litigation, determines the sort order for West km results from a full-text search using terms and connectors. (The sort order affects the West km and WestlawNext interfaces.) The default value is *Modified Date & Time*.
Maximum Number of Search Terms to Highlight	Determines the maximum number of search terms that are highlighted in the document. Large documents with a search term that is present often may take a long time to load. Restricting the maximum number of search terms in such a case results in shorter document loading time. The default value is *500*.
Citing References	
Display Mouseover Text for Flags	If selected, mouseover text is displayed when pointing to KeyCite status flags within the text of documents in the West km and WestlawNext interfaces. This setting is selected by default.
Show West km Citing References Icon	If selected, KM icons are inserted after citations, indicating when a citation is referenced in indexed documents. This setting affects documents displayed in the West km and WestlawNext interfaces. This setting is selected by default.
Show West km Citing References Icon in Clients	If selected, KM icons are inserted after citations, indicating when a citation is referenced in indexed documents. This setting affects BriefTools when KeyCite status flags are inserted. (For icons to be inserted with BriefTools, both *Show West km Citing Ref Icon* and *Show West km Citing Ref Icon in Clients* must be selected.) This setting is selected by default.
Target for West km Citing References Icon in Client	Defines the target interface of the KM icon when BriefTools is the source interface. Possible values are *West km Intranet* (the default) or *Westlaw* (WestlawNext). Note: When the West km intranet or WestlawNext is the source interface, the icon's target automatically corresponds with the source.
Firm Citing Reference Threshold	Determines the number of indexed documents that must reference a citation before a KM icon is displayed after a citation. When there are more than *n* number of citing documents, the

	icon is displayed. For example, if the threshold value is *1*, at least one other document must reference the citation in order for the icon to be displayed. The default value is *1*.
Depth of Treatment Settings	
Category One Category One Minimum Category One Maximum Category Two Category Two Minimum Category Two Maximum Category Three Category Three Minimum Category Three Maximum Category Four Category Four Minimum Category Four Maximum	Controls depth of treatment categories for citing documents. Modify these settings to change the depth of treatment categories. KeyCite depth of treatment categories indicate the extent to which each of your organization's documents discusses a WestlawNext document. The designation is based on the number of times your organization's document cites the WestlawNext document. The default settings for the depth of treatment categories are as follows: (see table below) Change the minimum and maximum settings to indicate the range of times your organization's document must cite the WestlawNext document in order to belong to a particular depth of treatment category. Note: You can set whether depth of treatment categories are displayed in a result at Setup, Field Display. For more information, see "Changing Field Display Settings" on page 13.
TRANSACTIONS	
Document Label Clause Label Defined Term Label	Determines the text used for the links to search documents, clauses, and defined terms on the basic and advanced search templates in West km for Transactions. The default values are as follows: • Documents • Clauses • Defined Terms
Show Search Terms in Results List (Transactions)	Determines whether the result list shows and highlights search terms in West km for Transactions. This setting is selected by default.
Number of Words to Display before and after Search Terms in Result List (Transactions)	When searching full text, indicates the amount of text (in number of words) to show before and after each search term in West km for Transactions. Note: Surrounding text is not displayed beyond the boundaries of a paragraph, a table cell, or text that defines metadata for a title, attorney, law firm, governing law, or party For this setting to function, *Show Search Terms in Result List* must be selected. The default value is *20*.

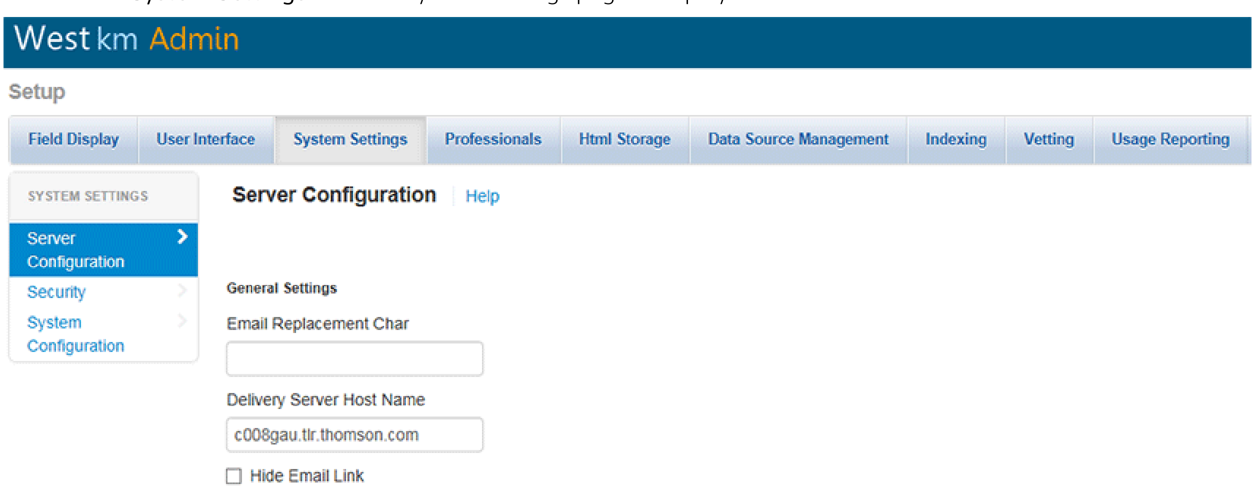
Category	Default Definition	Default Range
One	Mentioned	Your organization's document cites the displayed WestlawNext document 1 time.
Two	Cited	Your organization's document cites the displayed WestlawNext document 2-5 times.
Three	Discussed	Your organization's document cites the displayed WestlawNext document 6-9 times
Four	Examined	Your organization's document cites the displayed WestlawNext document 10 or more times

Number of Search Term Hits to Display in a Result List (Transactions)	When searching full text or titles, indicates how many search term references to show in West km for Transactions. For this setting to function, *Show Search Terms in Result List* must be selected. The default settings is the first three search terms.
Terms and Connectors Search Result Sort Order (Transactions)	In West km for Transactions, determines the sort order for West km results from a full-text search using terms and connectors. (The sort order affects the West km and WestlawNext interfaces.) The default value is Modified Date & Time.
Maximum Number of Search Terms to Highlight	Determines the maximum number of search terms that are highlighted in the document. Large documents with a search term that is present often may take a long time to load. Restricting the maximum number of search terms in such a case results in shorter document loading time. The default value is *500*.
EMAIL	
SMTP Server	The name of the SMTP server that will be used to email documents from West km.
SMTP Port	The port number associated with the SMTP server.
SMTP Username and Password	A valid username and password on the SMTP server for sending emails.
Default From Address	An email address to be used as the originating address for documents that are emailed from West km. The email must have a valid format and conform to rules on your SMTP server. For example, to prevent emails from being categorized as spam or junk mail, use an email address your email system will recognize. The default value is *westkm@westkm.com*.
Use SSL	Select this option if your SMTP server requires a secure connection.

Changing System Settings

To access and change system settings:

1. Access the West km interface. For details, see "Accessing West km" on page 3.
2. Click Setup.
3. Click the System Settings tab. The System Settings page is displayed.



4. In the left frame, click the type of settings you want to change.
5. In the right frame, make the changes you want to the settings. Settings are described in the following table.
6. Click Save.

SERVER CONFIGURATION SETTINGS	
General Settings	
Email Replacement Character	When a user e-mails a document from West km, a legal character that replaces all illegal characters (i.e., \ / : * ? “ > < |) in the file name for the document attachment. (The file name is generated from the title of the document in the document management system, which may include illegal characters.) The default value is a space. The value cannot contain an illegal character
Delivery Sever Host Name	The full server name with the domain of your West km delivery server (e.g., kmsrv.yourcompany.com). If you do not provide the host name, it will be populated with the delivery server name (e.g., kmsrv) during the installation.
Hide Email Link	When selected, the Email Document link is removed from the user interface. This setting is not selected by default.
Proxy Settings	
Web Proxy Host	IP address or URL for the proxy server.
Web Proxy Port	The port number used by the proxy server.
Bypass Proxy on Local	If selected, bypasses the proxy server for local addresses. This setting is selected by default.
Server Settings	
Bulk Load Controller Port server	Open TCP communications port for the indexing service on the indexing. The default value is *8085*.
Profile Sync Controller Port	Open TCP communications port for full-text indexing on the indexing server. The default value is *8085*.
CaRE Indexing Doc Server Port	The indexing service sets this port in the CaRE integration layer to listen for document requests from the CaRE engine. The default value is *5050*.
SECURITY SETTINGS	
Document Security	
None Always Display Tiles Full	Controls the access that active West km members have to indexed documents. The security levels are based on the security implemented in your organization’s document management system. • None: All matching organization documents are listed in West km results, and all active West km members can view and load them. This is the lowest security level and is the default setting. • Always Display Titles: All matching organization documents are listed in West km results, including full profile information, but members can only view and load documents if they have the necessary access rights. • Full: Only documents to which the members have necessary access rights are listed in West km results. This is the highest security setting. The performance you experience in West km is inversely proportional to the security level you select. The lowest security level may produce the best performance; the highest security level may negatively affect performance. Note: This setting does not apply to document collections in NetDocuments.

	Note: For details about the configuration that is required for West km document security and authentication to function properly with your document management system, see "Appendix D: Authentication and Document Security Configuration" on page 118.
Apply Security to the West km Icon	Controls the display of the West km icon in WestlawNext that indicates there are citing documents at your organization. If selected, the West km icon is displayed only after checking that the user has access to at least one document in your organization's document list. If not selected, the West km icon is displayed regardless of the user's access to your organization's document list. The user may be restricted from accessing organization documents, but the icon display informs the user that organization documents containing the citation exist. This setting is selected by default.
Confidentiality Message	An optional warning message detailing privacy concerns that is displayed to members. The message is displayed in a pop-up window when a user views the first organization document in a session. To prevent display of the message, leave the text box blank. Space is limited to 1000 characters.
Remote Access	
User Name Password	The name and password for a Windows domain user account (or several local user accounts) with access to all West km server components and to all NTFS documents that West km will access directly for indexing, including NTFS documents and documents managed by eDOCS DM, ProLaw, and generic database solutions.
SYSTEM CONFIGURATION	
Product Key	Allows you to view your existing product key and enter a new product key. If you add a West km product component that does not require installation of a software component (e.g., the West km Vetting Toolkit), the product component can be enabled on the System Configuration page. Type your new product key in the **Product Key** box and click **Save**. Note: If the additional product component requires installation of a software component (e.g., Document Analysis), then the product key needs to be updated during the software installation process.
Product Components	A listing of available West km product components.
Versions of Installed Components	A listing of installed software components with versions.
PROFESSIONALS	
Manage Groups	Allows administrators to manage groups of users through Active Directory when West km is using Integrated Windows Authentication (IWA). Active Directory authenticates and authorizes users for your windows domain networks. The West km rights you assign to a group are automatically assigned to all users in that group.
Manage Users	Allows administrators to manage users through Active Directory when West km is using Integrated Windows Authentication (IWA). Active Directory authenticates and authorizes users for your windows domain networks. Settings for individual users override the settings for groups to which is user belongs.
Import Users	Allows you to import user data to the system using by creating an input file of comma-separated values (.csv) and then running the import. This option can be used when you have an extensive list of user to add to West km.

HTML STORAGE	
Collections	Allows users to manually launch full-text indexing processes. Changes are only applied to newly indexed content. To apply changes to all content, run Reindex All Content.
Scheduling	Allows users to define the indexing windows for the search service. You may want to define multiple time windows to account for different frequencies (e.g., weekdays vs. weekends).
Search Component Engine	Allows users to edit the HTML server and index file location. It is recommended that you contact your West km representative for these procedures.
Document Store Locations	This setting lists the folder locations where HTML documents are stored. These are the documents that are converted to HTML from their native file formats for use in West km. You can complete several actions on the Document Store Locations page, including adding, editing, and removing storage locations. However, it is recommended that you contact your West km representative before completing these actions.
Full Text Statistics	Allows users to monitor Full Text indexing statistics. Each indexing collection is listed, and counts represent the number of documents in each status. This page gives counts for the following statuses: • Queued • Removed Queued • In Progress • Success • Failure • Suspended To update the counts while full-text indexing is running, click Refresh.
Event Log	Allows users to view the event log information for full text indexing. Information and error events are logged for: • Full-text indexing • Reclaiming • Searching To change the sort order of event log records, click a column heading (e.g., Date/Time or Severity) to sort by that category. To clear the event log page and delete log records from the database, click Purge Event Log.

Changing Data Source Settings

To access and change settings for data source integration,

1. Access the West km interface.
2. Click Setup.
3. Click the Data Source Management tab.
4. Under Settings, click the data source for which you want to access settings.
5. Make the changes you want to the settings. Settings for each data source are described in the following table.
6. Click Save.

Generic Database	
Custom Fields	Allows you to map a custom field in West km to data in a generic intermediate database. In the table, find an empty row that matches the content type of the custom field: String, Boolean, Date/Time, or Integer. Then type the name of the field in the generic database in the DMS Field box. For more information, see "Custom Fields" on page 30.

eDOCS DB (eDOCS DM)	
Security Lump Size	SQL statement group size parameter used when retrieving security attributes for documents. The recommended range is 75–250. The default value is *100*.
Security Cache Groups	If selected, group permissions are checked for users on a per-process basis. This setting is not selected by default.
Use Client Matter Metadata	If selected, client matter metadata is loaded from the document management database. This setting is selected by default.
Use Combined Client Matter	If selected, creates a combined client and matter ID and a combined client and matter name in West km. This setting is selected by default. Note: You can set the separator character (e.g., a hyphen "-") between IDs and names using the *Client-Matter Separator* at the Setup, Indexing, Index Settings page.
Use Sub Versions	If selected, sub-versions are used for documents. Changing this setting requires re-indexing. This setting is not selected by default.
Use Matter Custom SQL	If selected, the client ID, client name, matter ID, and matter name are retrieved from custom fields instead of the default fields. This setting is not selected by default.
Matter Custom SQL	A valid SQL query used to retrieve the client ID, client name, matter ID, and matter name from custom fields. The following aliases must be used: client_id client_name matter_id matter_name This setting is ignored if *Use Matter Custom sql* is not selected.
Use Document Type (Class) Custom SQL	If selected, the document type (class) is retrieved from a custom field instead of the default field. This setting is not selected by default.
Document Type (Class) Custom SQL	A valid SQL query used to retrieve the document type (class) from a custom field. The custom_class alias must be used. This setting is ignored if *Use Document Type (Class) Custom Sql* is not selected.
Custom Fields	Allows you to map a custom field in West km to data in eDOCS DM. • In the table, find an empty row that matches the content type of the custom field: String, Boolean, Date/Time, or Integer. • Type the name of the field as it is known in eDOCS DM in *databaseowner.tablename.fieldname* format in the **DMS Field** box. • If the field is not part of the Profile, People, DocumentTypes, Components, or Versions table in eDOCS DM, specify how the field's table is joined to one of those tables by typing a SQL statement in the **JOIN** box. For more information, see "Custom Fields" on page 30.

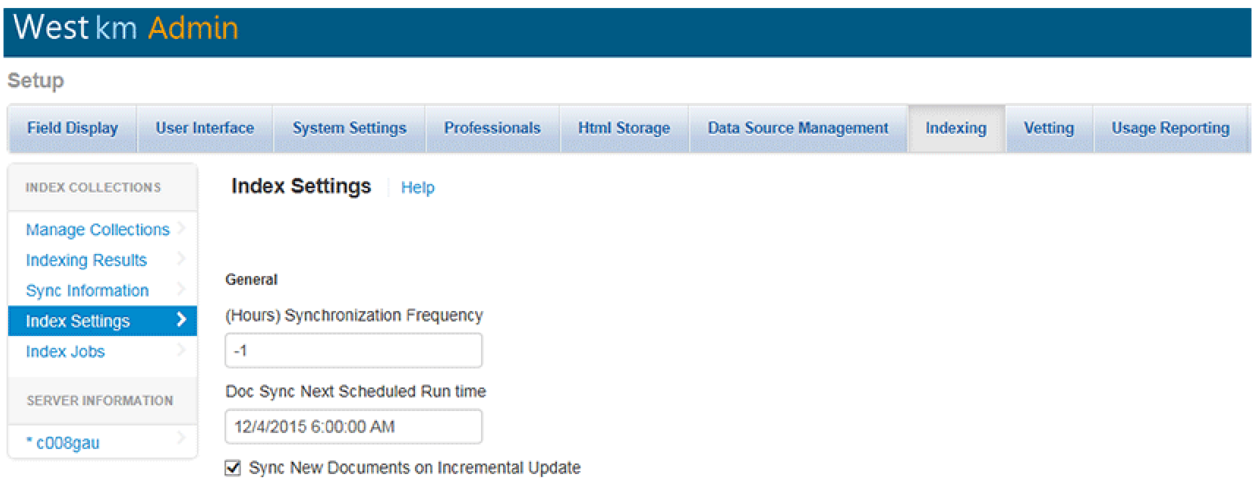
iManage Work	
Version	The iManage Work client .dll version. Supported values are 1.0 and 8.0. • If the .dll is numbered in a format of 1.#.#.#, set the value to 1.0. If the .dll is numbered in a format of 8.#.#.# or higher, set the value to 8.0.
Maximum Rows for Search	The maximum number of records to return for a iManage Work saved search. The default value is *20000*.
Session Timeout	The session time-out value in seconds for the iManage Work connection. The default value is *3600*.
User IDs Required User Passwords Required	Controls usage of iManage Work virtual user accounts and passwords for authenticating members. You may need to select these options (and populate the columns) if you use iManage Work for your document management system and use virtual logins rather than Windows integrated logins. If selected, iManage Work security will determine document access rights. If not selected, internal security logic is used to determine document access rights. By default, neither value is selected. • When *User ID Required* is selected, a DMS User ID column is added to the Professionals table, as well as a Server\DB column for the server and database to which the member has access. • When *User Password Required* is selected, a DMS Password column is added to the Professionals table. (If not present already, this will also add a Server\DB column for the server and database to which the member has access.) More than one database may be accessible to one member; in this situation, a drop-down list is displayed in the Server\DB column. When adding or editing a member's information, you need to click the databases in the *Server\DB* drop- down list to which you want the member to have access and specify the member's login information for the document management system. The login information will apply to all selected databases. Settings are not selected by default.
Use Combined Client Matter	If selected, creates a combined client and matter ID and a combined client and matter name in West km. This setting is selected by default. Note: You can set the separator (e.g. a hyphen) between IDs and names using Client-Matter Separator at the Setup, User Interface, General page.
Attr Mapping Title Attr Mapping Abstract Attr Mapping Class Attr Mapping Matter Attr Mapping Matter Description Attr Mapping Client Attr Mapping Client Description Attr Mapping Author	Indicates how to map iManage Work document profile fields to associated West km fields.
Custom Fields	Allows you to map a custom field in West km to data in iManage Work. In the table, find an empty row that matches the content type of the custom field: String, Boolean, Date/Time, or Integer. Then type the name of the iManage Work document profile field in the DMS Field box. The field must be provided as part of the document profile through the iManage Work API. For more information, see "Custom Fields" on page 30.
Exemplar Form Field	Allows the admin to select which custom field is used for the Exemplar Form.

iManage Work in the Cloud	
AppUuid	This setting is not currently used by West km.
Domain	This setting is not currently used by West km.
Use SSL	Select this option to encrypt iManage Work in the Cloud network traffic using SSL.
Base Path	The path for the iManage Work in the Cloud API. This setting is entered by default.
Document Page Size	Type the number of items retrieved in each call to the API. The default value is *1000*.
Custom Fields	Allows you to map to a custom field in West km to data in iManage Work in the Cloud DM. Type the name of the document profile field in the DMS Field box provided in the row that matches the content type of the custom field (String, Boolean, Date/Time, or Integer). This field must be provided as part of the document profile through the iManage Work in the Cloud API.
Server Version	This setting is already entered for you and does not need to be changed.
User ID Required	Enable this option to require a DMS user ID for all users. This option will allow you to enable full security.
NetDocuments	
Categories List Search	The name of a NetDocuments saved search that retrieves a list of other saved searches (or categories), which in turn retrieve the documents you want to index in West km. The individual saved searches retrieved by this global search must meet these requirements: (1) They must be sorted by last modified date, descending, and (2) The documents retrieved must be publicly available to West km users.
REST API Host	The path for the REST API Host. This setting is entered for you by default.
REST API Version	The current REST API Version. This setting is entered for you by default.
Redirect Proxy	The authentication server location for NetDocs to be used when a new token is required. This setting is entered for you by default.
Days to Warn Before Token Expiration	Type the number of days before your token expires that you want to receive messaging. The default value is *90* days before the expiration date.
User ID Required	Controls whether NetDocuments user accounts will be used to control document security. If selected, NetDocuments security determines document access rights. If not selected, no document security is used. When *User ID Required* is selected, a DMS UserID column is added to the Professionals table in which you can enter a NetDocuments user GUID for each West km member to set document access rights. This setting is selected by default. Note: NetDocuments user GUIDs entered in the DMS UserID column are not required to be unique. You can enter the same user GUID for multiple West km members.
Custom Fields	Allows you to map a custom field in West km to data in NetDocuments. In the table, find an empty row that matches the content type of the custom field: String, Boolean, Date/Time, or Integer. Then type the name of the NetDocuments field in the **DMS Field** box. If your organization has multiple cabinets in NetDocuments, the field names that you map to West km must match across cabinets. For more information, see "Custom Fields" on page 30.

ProLaw	
Author	Determines which author field is used from ProLaw when indexing a document. *Adding Professional* (the default) will use the name of the person who added the document to ProLaw. *Prof Set* will use the name of the person set in the ProLaw document metadata field.
Fields	Allows you to map a custom field in West km to data in ProLaw. • In the table, find an empty row that matches the content type of the custom field: String, Boolean, Date/Time, or Integer. • Type the name of the field as it is known in ProLaw in *tablename.fieldname* format in the **DMS Field** box. • If the field is not part of the Events, EventTypes, Professionals, EventMatters, or Matters table in ProLaw, specify how the field's table is joined to one of those tables by typing a SQL statement in the *JOIN* text box. For more information, see "Custom Fields" on page 30.

Changing Index Settings

1. Access the West km interface. For details, see "Accessing West km" on page 3.
2. Click **Setup**.
3. Click the **Indexing** tab.
4. In the left frame, click **Index Settings**. The Index Settings page is displayed.



5. In the right frame, make the changes you want to the settings. Settings are described in the following table.
6. Click **Save**.

General Settings	
(Hours) Synchronization Frequency	This settings is currently not used. The default value is *-1*.
Doc Sync Next Scheduled Run Time	Contains the date and time at which the next Synchronization job will run.
Sync New Docs on Incremental Update	If selected, the incremental update process will also find and index any new documents in the collection that have a date and time prior to when the collection was last indexed. You may want to select this setting if (1) you change your saved search criteria in your document management database for a document collection after it was indexed, or (2) you add older documents to a NT file system location that is an indexed document collection. This setting is selected by default.

Work in Progress Time Span (days)	Prevents documents that are works in progress from being indexed during bulk indexing or incremental updates. A document is a work in progress if the difference between the last modified date and the date of indexing is less than the number of days in this setting. Note: If an existing West km document is edited, it is not removed from West km during the work-in-progress period. The original document remains until the edited document is incorporated after the work-in-progress period. Note: This setting does not apply to document collections in NetDocuments. For a change to this setting to take effect, an incremental update is required. The default value is *0*.
Client Matter Separator	Allows you to set the separator character (e.g., hyphen "-") for Client Matter.
Analysis Indexing	
Run Non-Captioned Doc Type Process	If selected, documents that don't have court captions are still processed by the analyzer component and assigned to a document type (e.g., within the Internal Memos category) rather than to "Unassigned." This setting is selected by default. Note: If you change this setting, documents require reindexing through the analyzer component for the change to take effect.
Cite Recognition Indexing	
Underline Citations Underline Citations and Descriptions	Determines the portions of a citation that become hypertext links during West km RID processing. These links are displayed in the HTML rendering of indexed documents and when citation links are inserted in a word-processing document using BriefTools. • If *Underline Citations* is selected, a hypertext link for only the numeric portion of the citation is created. • If *Underline Citations and Descriptions* is selected (default), a hypertext link for the title of the citation, as well as the numeric portion of the citation, is created. For a change to this setting to take effect, an incremental update for citation recognition is required.
Classification Indexing	
Start and Stop CaRE Service	If selected, the indexing service will start and stop the CaRE service. If not selected, the CaRE service must be started manually. If CaRE is installed, this setting is selected by default.
Show Document Counts (End-User) Show Document Counts (Administrative)	If *Show Document Counts (End-User)* is selected, counts are displayed after topics in the KeySearch hierarchy that is viewed by end users in the West km interface. If *Show Document Counts (Administrative)* is selected, counts are displayed after topics in the KeySearch administrative view. These counts indicate the number of unique documents at your organization that have been assigned to the KeySearch topic and its subtopics via manual classification or CaRE. (Counts do not include documents retrieved via Terms and Connectors queries.) Document counts for each topic in the KeySearch hierarchy are updated daily at the end of the document indexing window. Document counts are not immediately updated when a document is manually classified to a topic, removed from a topic, or deleted from West km. To update the document counts immediately, regardless of the document indexing window, see "Manually Launching Indexing Jobs" on page 77.

Mapping Fields

Metadata from your document management system (DMS) is used in West km to help search for and identify documents. Some metadata is mapped to West km fields by default. You can also define the mapping of metadata to custom West km fields.

For a list of field mappings that West km uses by default from your document management system, see "Appendix E: West km–DMS Field Mappings" on page 120.

For information about field mappings in an intermediate database, see "Using an Intermediate Database" on page 9. For NetDocuments, there are no default field mappings. You can set field mappings at Setup, Data Source Management, Settings, NetDocuments (see "Configuring NetDocuments" on page 8 for more information).

CUSTOM FIELDS

If you have valuable document metadata in DMS fields other than those listed in "Appendix E: West km–DMS Field Mappings" on page 120 you can define up to six custom fields in West km by mapping a custom field to data in your DMS. You can then use these custom fields when searching and browsing documents in West km.

Custom fields are available for a Boolean field, a date field, an integer field, and up to three string fields.

To define a custom field,

1. Access the West km interface.
2. Click **Setup**.
3. Click the **Data Source Management** tab.
4. Under Settings, click your DMS type.
5. In the Custom Fields mappings table, find an empty row that matches the content type of the custom field: String, Boolean, Date/Time, or Integer.
6. In the **DMS Field** box, enter the location of the DMS field that contains the data for the custom field.

For this DMS[1]:	Type this in the DMS Field box:
eDOCS DM	The name of the field as it is known in eDOCS DM in *databaseowner.tablename.fieldname* format, for example, DOCSADM.ACTIVITYLOG.VERSION_LABEL.
Generic Database	The name of the field in the generic intermediate database, for example, Custom1.
iManage Work and iManage Work in the Cloud	The name of the iManage Work document profile field, for example, imProfileCustom2Description. The field must be provided as part of the document profile through the iManage Work API.
NetDocuments	The name of the field in NetDocuments.
ProLaw	The name of the field as it is known in ProLaw in tablename.fieldname format, for example, MattersComponents.NoBill.

[1]Custom fields cannot be mapped to NTFS.

7. In the JOIN text box (if provided), specify in a SQL statement how the field's table is joined.

For this DMS[1]:	Type this in the Joinbox:
eDOCS DM	If the field is not part of the Profile, People, DocumentTypes, Components, or Versions table in eDOCS DM, specify in a SQL statement how the field's table is joined to one of those tables. For example, `JOIN DOCSADM.ACTIVITYLOG ON DOCSADM.PROFILE.DOCUMENT = DOCSADM.ACTIVITYLOG.DOCNUMBER`
ProLaw	If the field is not part of the Events, EventTypes, Professionals, EventMatters, or Matters table in ProLaw, specify in a SQL statement how the field's table is joined to one of those tables. For example, `INNER JOIN MattersComponents ON MattersComponents.Matters = EventMatters.Matters`

[1] If you provide table join information for one custom field, you do not need to provide the same table join information again for other custom fields.

8. Click **Save**.
9. If you have data source connections in West km for multiple DMSs, repeat these steps for all the DMSs integrated with West km that contain data corresponding to the custom field.

Notes:

- You can rename the custom field labels in West km at the Setup, Field Display, and Field Names page. For more information, see "Changing Field Display Settings" on page 13.
- Custom fields that you define are not automatically added to the West km Vetting Toolkit. If you want to use the same field for vetting purposes, you must also add it on the Vetting tab. For details, see "Configuring Vetting Fields" on page 57.
- If you change DMS field mappings, you need to run indexing to update profile metadata.

Setting Document Sort Order

Documents in a result are sorted by default in different ways, depending on:

- The method used to retrieve the documents.
- The settings chosen on the User Interface tab for West km for Litigation and West km for Transactions.

WEST KM FOR LITIGATION

The following table shows the sort order in West km for Litigation.

Document Retrieval Method	Document Sort Options	User Interface Setting
KeyCite	Depth of treatment	*no setting*
Search- Terms and Connectors	Reverse chronological (default)	Terms and Connectors Search Result Sort Order = Modified Date & Time
	Ranking based on the occurrence of search terms in documents	Terms and Connectors Search Result Sort Order = Number of Hits
	Relevance	Terms and Connectors Search Result Sort Order= Relevancy–Weight[1]
Search—Natural Language	Reverse chronological	*no setting*
	Relevance (default)	Natural Language Search Result Sort Order= Relevancy–Weight[1]
KeySearch	• With full-text search: Relevance • Without full-text search: CaRE score	*no setting*

[1] For Relevancy–Weight, lower relevance numbers indicate higher relevancy.

The search result sort order settings are located at Setup, User Interface, Litigation. For more information, see "Changing User Interface Settings" on page 14.

WEST KM FOR TRANSACTIONS

The following table shows the sort order in West km for Transactions.

Document Retrieval Method	Document Sort Options	User Interface Setting
Search- Terms and Connectors	Reverse chronological (default)	Terms and Connectors Search Result Sort Order = Modified Date & Time
	Ranking based on the occurrence of search terms in documents	Terms and Connectors Search Result Sort Order = Number of Hits
	Relevance	Terms and Connectors Search

		Result Sort Order= Relevancy–Weight[1]
Search—Natural Language	Reverse chronological	*no setting*
	Relevance (default)	Natural Language Search Result Sort Order= Relevancy–Weight[1]

[1] For Relevancy–Weight, lower relevance numbers indicate higher relevancy.

The search result sort order settings are located at Setup, User Interface, Transactions. For more information, see "Changing User Interface Settings" on page 14.

Changing Configuration Files

West km has several configuration files, listed in the table below, whose properties control communication among the various West km components.

You can access and change settings in these configuration files.

Configuration File	Location and File Name[1]	Associated Service	Associated Server
Analyzer Component (Litigation)	*[Analyzer component installation folder]*\ Thomson.West.Dexter.Service.exe.config	KM Entity Extraction Service	Indexing
Citation Service	*[West km installation folder]*\bin\ KM.CiteRecognitionService.exe.config	KM Cite Recognition Service	Indexing
Document Analyzer (Transactions)	*[Document analyzer installation folder]*\bin\ Elite.DocAnalysis.Service.exe.config	Elite Document Analysis service	Indexing
HTML Conversion Service	*[West km installation folder]*\bin\ KM.HtmlConversionService.exe.config	KM Html Conversion Service	Indexing
IIS	*[West km installation folder]*\ Web.config	*No associated service; refresh the Web page*	Delivery
Indexing Service	*[West km installation folder]*\bin\ KM.IndexingService.exe.config	KM Indexing Service	Indexing
Monitor Service	*[Monitor Service installation folder]*\bin\ Thomson.Westkm.MonitorService.exe.config	West km Monitor Service	Delivery; Indexing; HTML repository/search
Search Service	*[West km installation folder]*\bin\ KM.SearchService.exe.config	KM Search Service	Delivery; Indexing; HTML repository/search
Shared	*[West km installation folder]*\bin\ Shared.config	KM Indexing Service; KM Worker Service	Delivery, Indexing
Worker Service	*[West km installation folder]*\bin\ KM.WorkerService.exe.config	KM Worker Service	Indexing

1 The default installation folder for the analyzer component (Litigation) is [Drive]:\Program Files\Thomson\Dexter. The default installation folder for West km is [Drive]:\Program Files\Thomson\KM.

The default installation folder for the document analyzer (Transactions) is [Drive]:\Program Files\Thomson\DocAnalysis. The default installation folder for the Monitor Service is [Drive]:\Program Files\Thomson\Westkm\Monitor.

Properties in configuration files include a lockItem attribute that determines whether the property value will be replaced during installation and upgrade procedures.

- If you set the lockItem attribute for a property to *false* (default), the property value will be replaced during installation and upgrade procedures with the default value for the release being installed.
- If you set the lockItem attribute for a property to *true*, the property value will not be replaced during installation and upgrade procedures.

To open a configuration file and view or change its properties,

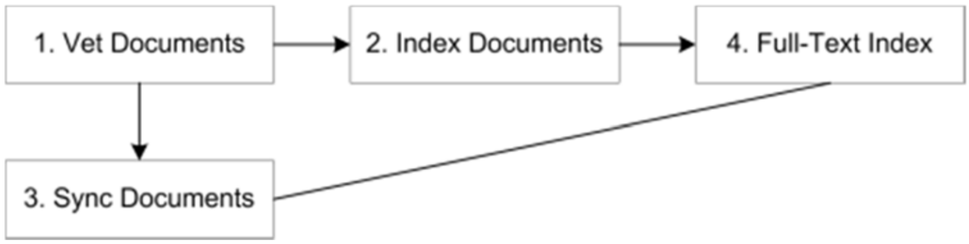
1. Open the configuration file you want to view or change in Notepad. If your West km server components are distributed across machines, make sure you open the file on the configuration file's associated server.
2. Make the necessary adjustments to properties in the configuration file.
3. Save the configuration file.
4. Stop and then start the associated West km service for the configuration file you've changed:
    a. Click the **Start** button, click **Programs**, click **Administrative Tools**, and then click **Services**.
    b. Right-click the service and choose **Stop**.
    c. Right-click the service and choose **Start**.

Note If you've made changes to the Web.config file, you do not need to restart a service; just refresh the Web page.

4 Vetting and Indexing Overview

Vetting is the process of selecting documents from your document management system for inclusion in West km. Indexing is the process in West km that prepares documents for searching and retrieval. It includes the indexing, synchronization, and full-text indexing processes.

The vetting and indexing process:



Vetting

The vetting toolkit is an optional product package that helps you fine-tune the selection of documents from iManage Work or eDOCS DM before indexing the documents in West km. This process provides a visual method for identifying and tagging documents for inclusion in West km and serves to improve search accuracy and precision within West km.

With the vetting toolkit, you can identify valuable, reusable documents by:

- Defining vetting groups that can automatically and periodically run against your source collection.
- Defining both inclusionary and exclusionary rules for the vetting group (collection). Inclusionary rules define which documents should be included, and exclusionary rules define which documents should be excluded.
- Identifying documents using document profile attributes and full-text searches (iManage Work only).
- Testing the vetting process, using visual feedback to refine and spot-check the collection.

The toolkit creates and maintains document vetting information in the West km database.

Indexing

Documents are organized into document collections for indexing in West km. A document collection is defined by (1) a vetting group in the West km Vetting Toolkit, (2) a saved search or query in a document management system, or (3) a folder of documents on your file system.

Indexing can run on a document collection in two ways:

- Bulk indexing: All documents in the collection are indexed.
- Incremental update: Documents in the collection are indexed if they are new or modified and have a date and time after the collection was last indexed. In addition, the update process applies collection characteristic changes (e.g., RID newly enabled) that have been made to a document collection since the last indexing.

Indexing includes the following indexing components, listed in the order in which processing occurs by default:

HTML Conversion: Documents that you have designated from your organization's document management system or file system (NTFS) are converted to HTML for use in West km. Stellent Outside In is a third-party software package that is used by West km to convert documents to HTML. (The original documents remain unchanged.)

Profile Metadata–DMS: Document metadata originating from your document management system and file system—including created date, last modified date, document title, and author—is collected and saved to the West km database. Select metadata is also stored in .rdf files along with HTML renderings.

Profile Metadata–km: Document metadata originating from West km—including library group, exemplar markings, indication of comments, and comment text—is saved to the West km database. Select metadata is also stored in .rdf files along with HTML renderings.

Manual Classification: Documents are assigned to the KeySearch topics that you have indicated.

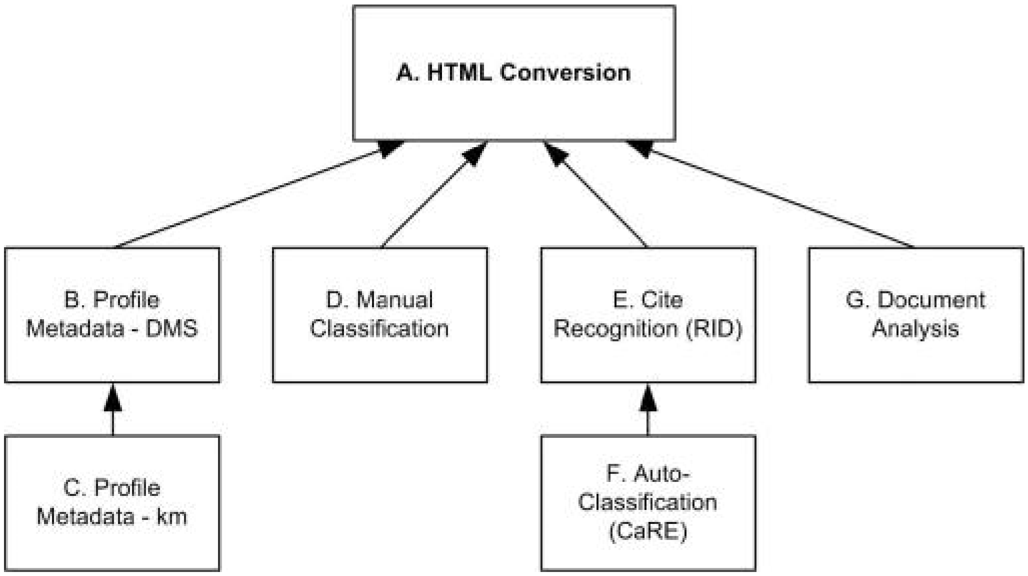
Cite Recognition (RID): Citations in documents are identified using RID (reference identification) software, and reference IDs are retrieved to link the documents to WestlawNext.

Auto-Classification (CaRE): Documents are automatically assigned to KeySearch topics using West's categorization and recommendation engine (CaRE).

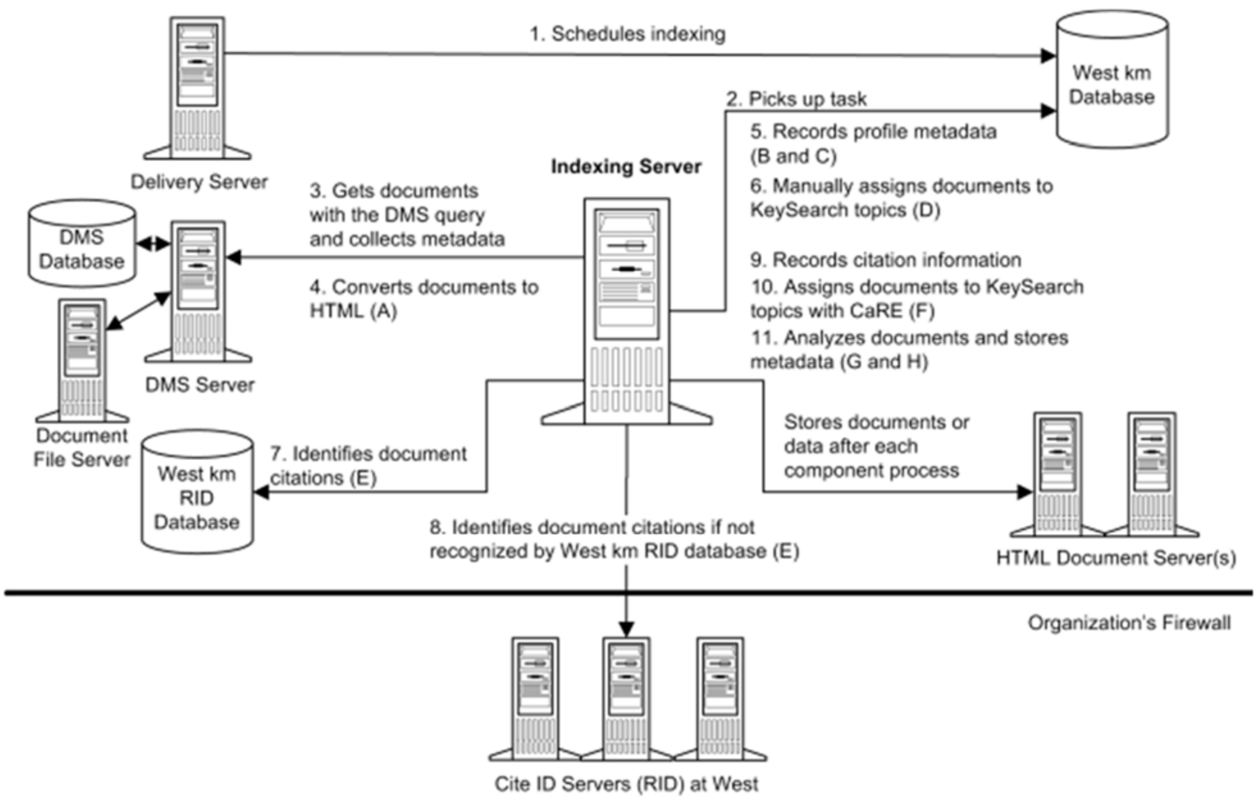
Document Analysis: Documents are mined to extract and tag significant content.

In West km for Litigation, the analyzer component extracts and tags content such as title, document type, judges, jurisdiction, and court. For more information, see "Litigation Document Analysis" on page 36.

In West km for Transactions, the document analyzer engine extracts and tags content such as title, attorney, law firm, and governing law. For more information, see "Transactional Document Analysis" on page 36.



If all indexing components are set to run for a document collection, the indexing process operates as shown in the following figure.



LITIGATION DOCUMENT ANALYSIS

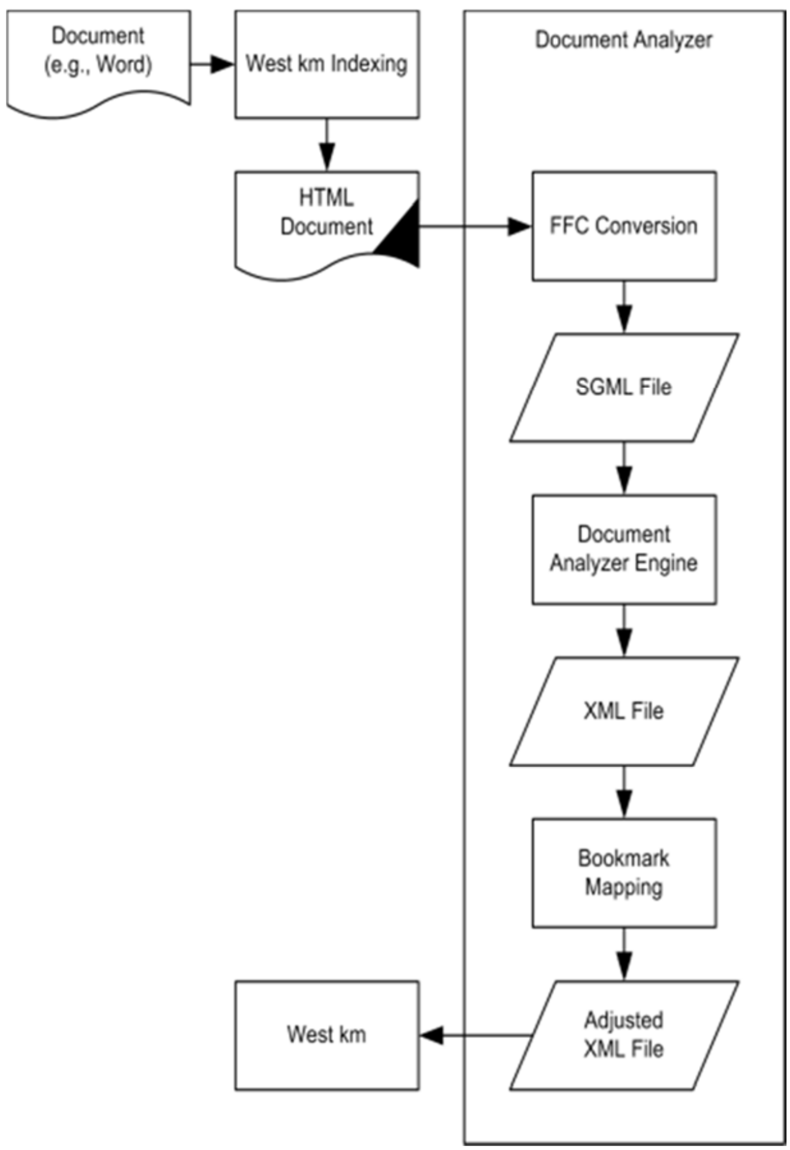
During the West km indexing process, the analyzer component extracts and tags significant document content in West km for Litigation, including title, document type, judges, jurisdiction, and court. The analyzer component uses a system of data extraction and textual entity resolution (Dexter) that employs a mixture of the following methods:

- Rule-based extractors use deductive rules that are applied to the text word by word. For example, if honorifics such as Honorable, Hon., or Judge are in the document, then the names that follow or precede them are candidates to be extracted as judges.
- List-based extractors tag all mention of elements compared to a list. For example, after judge names are extracted using rules, they are then resolved to an authority files. This file has a single entry for each unique individual, as well as further information that may be relevant, such as the judge's jurisdiction and court information.
- Statistical extractors use a set of cues that receive weights and whose weights are combined based on probability and statistical concepts. The statistics are derived from training on labeled text examples. For example, titles are extracted using a statistical model based on formatting, case, position in the document, and length.

TRANSACTIONAL DOCUMENT ANALYSIS

During the West km indexing process, the document analyzer extracts and tags significant document content in West km for Transactions. The data is also used to create document, clause, and defined term indexing collections and to enable concept title searching, which automatically expands a title search to include synonyms, root expanders, and related concepts.

The transactional document analysis process:



The West km indexing process creates an HTML document from the native document (e.g., Word, WordPerfect, PDF). During analysis, the document analyzer calls the FFC (file format converter) component, which converts the HTML document to an SGML file. The document analyzer engine processes the SGML file and writes the results to an XML file. Each element found is identified within the XML file. Then the bookmark mapping component adds length and offset information to the XML file elements. These lengths and offsets map to items in the HTML document, so that West km can effectively navigate and display it.

Synchronization

Synchronization removes documents from West km if they have been deleted from your organization's file system or if they are no longer part of document collections you have defined to be indexed with West km.

Full-Text Indexing

Full-text indexing builds and updates the indexes that are used to search your organization's documents by terms.

Supported Document Formats for Indexing

The supported document formats for indexing documents in West km are listed in the following table.

Document Format	File Extension
Microsoft Word	.doc or .docx
Corel WordPerfect	.wpd
Adobe Portable Document Format	.pdf
Microsoft PowerPoint for Windows	.ppt
Rich Text Format	.rtf

For information regarding support for other formats, call West km Technical Support at 1-888-WESTKM1.

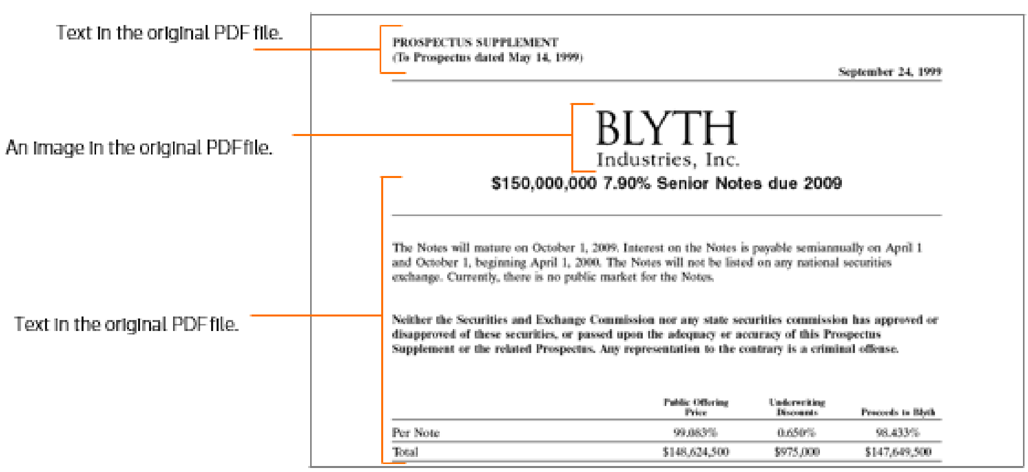
INDEXING AND DISPLAY OF .PDF AND .PPT FILES

The indexing and display of converted .pdf and .ppt files in West km depends on the method used to create the original files.

- Text-based files include mostly text and are created in PDF from a word-processing document or in Microsoft PowerPoint format with the use of text boxes.
- OCR-based files contain a mix of text and images and are created from scanned documents.
- Image-based files contain only images and are created from scanned documents.

Only text from the original file (not images) is indexed and searchable in West km. For image-based files, only document metadata is indexed and searchable.

An example of a PDF file:



The display of converted .pdf and .ppt files in West km also depends on the template that West km uses to convert the files to HTML.

Text Template: The default template converts only text, not images, from the original file. When viewing the converted file in West km, images are not displayed and formatting may be lost. The text includes citation links and KeyCite status flags as appropriate and is used for document searches.

Images Template: An alternate template converts the original file—both text and images—as a series of images page by page, with the text duplicated between images. The text-only portion includes citation links and KeyCite status flags as appropriate and is used for document searches. Using this template creates very large files, so it is recommended only if your files contain images, formatting, or tabular information that must be preserved "as is" for display in West km.

Note You designate the conversion template for .pdf and .ppt files using the HtmlConversionTemplate property in Shared.config. For more information about setting configuration file properties, see "Changing Configuration Files" on page 32.

Integration with Document Management Systems

West km supports the document management systems listed in the following table. (For specific versions, go to legalsolutions.thomsonreuters.com/law-products/solutions/westkm and click **View System Requirements** under Product Support) The table also provides the method by which West km integrates with each product to access documents during indexing and for the Load Copy function.

Document Management System	Integration Method for Accessing Documents
iManage Work	West km uses the iManage Work API to access documents. West km directly access the iManage Work database for vetting and to verify document security rights[1].
iManage Work in the Cloud	West km uses the iManage Work in the Cloud web services API (REST) to access the iManage server.
eDOCS DM	West km directly accesses the SQL Server database for eDOCS DM. A West km domain user account is used to access the documents in NTFS.
ProLaw	West km directly accesses the ProLaw database. A West km domain user account is used to access documents in NTFS.
NetDocuments	West km uses the NetDocuments web services API (REST) to access the NTFS NetDocuments server and uses HTTP to communicate with the NetDocuments local document store.
NTFS	A West km domain user account is used to directly access documents.

[1] If you prefer to use the iManage Work API to check document security, change the value of the iManage WorkSecurityViaApi property in Web.config to y. For more information about setting properties in configuration files, see "Changing Configuration Files" on page 32..

If you store documents in an unsupported document management system, you can use a generic intermediate database to index those documents in West km. For more information, see "Using an Intermediate Database" on page 9.

5 Configuring Indexing

To configure West km for indexing, you must add connections to the data sources that contain the document collections you want to index. For example, you may have documents in a document management system (DMS) or NTFS folders.

In addition, several options are available for configuring how, when, and which documents are indexed. You may want to change these settings either before or after you index documents for the first time. For example, you can perform these tasks:

Change the setup of your indexing server, such as the timing of indexing and the processing of indexing components (see "Setting Up the Indexing Server" on page 43 for more information).

Customize the KeySearch hierarchy for your organization (see "Customizing the KeySearch Hierarchy" on page 46 for more information).

Follow best practices for setting up major indexing or routine indexing updates (see "Performing Major Indexing Updates" on page 49 for more information).

Set system options related to indexing (see "Changing Index Settings" on page 28 for more information).

Indexing Requirements

In preparing West km to index your organization's documents, you need the following:

- Document collections identifiable for indexing in NTFS folders or in saved searches in DMS databases.
- A user ID and password for an account that has the necessary read-only rights to access your organization's document management system and the documents you are going to index.
- A decision on when and how often to update West km indexes and full-text indexes after the initial indexing of documents.

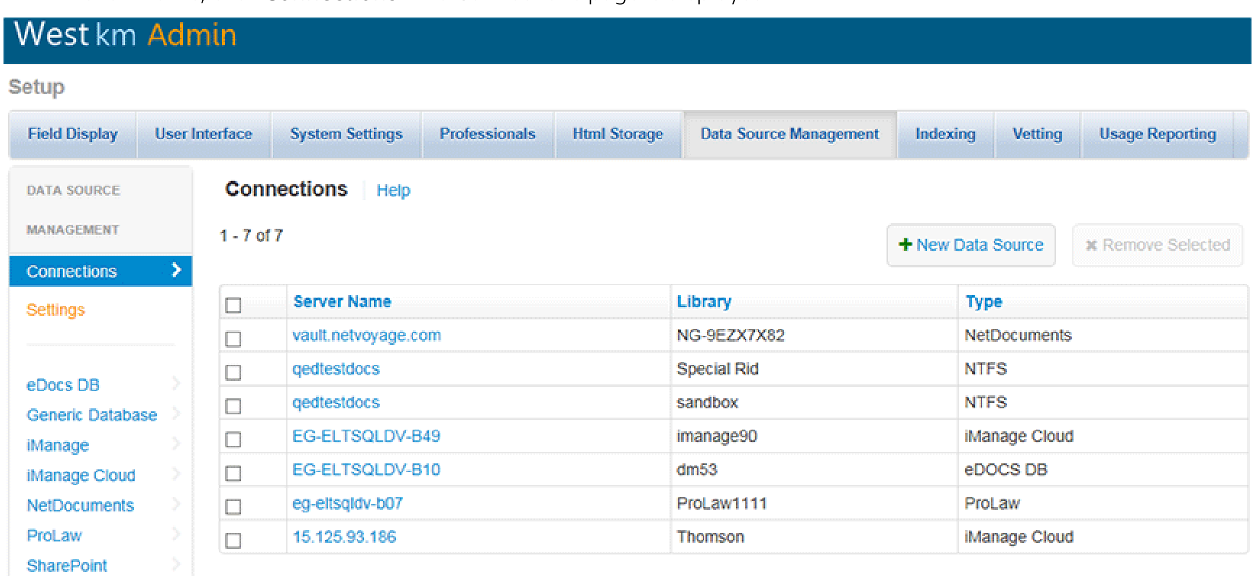
Adding Data Source Connections

Before indexing documents in West km, you must first add connections to the data sources that contain the document collections you want to index. You create these connections whether you have documents defined by (1) a vetting group in the West km Vetting Toolkit, (2) a saved search in a document management system, or (3) a folder of documents on your file system.

Note: If you want to index documents in a document management system not supported by West km, see "Using an Intermediate Database" on page 9.

To add data source connections,

1. Access the West km interface. For details, see "Accessing West km" on page 3.
2. Click **Setup**.
3. Click the **Data Source Management** tab.
4. In the left frame, click **Connections**. The Connections page is displayed.



5. Click **New Data Source**. The Add New Data Source page is displayed.
6. In the Type list, select the source of the documents.
7. Enter the requested information for the source. For a description of the information you need to provide, see these subsections:
   - If you use eDOCS DM, see "Adding an EDOCS DM Data Source Connection" on page 40.
   - If you use iManage Work or iManage Work in the Cloud, see "Adding an iManage Work Data Source Connection" on page 40.
   - If you use the NT file system, see "Adding an NT File System Data Source Connection" on page 41.
   - If you use ProLaw, see "Adding a ProLaw Data Source Connection" on page 41.
   - If you use NetDocuments, see "Adding a NetDocuments Data Source Connection" on page 41.
8. If you'd like to select a library group for this data source, see "Selecting a Library Group Collection" on page 42.
9. Click **Save**.
10. Repeat steps 5-9 for each data source that contains document collections you want to index.

ADDING AN EDOCS DM DATA SOURCE CONNECTION

Provide the information listed in the following table when adding a data source connection for eDOCS DM.

Field Name	Description
Type	The data source used to manage the documents (i.e., **eDocs DB**).
User Name and Password	The user name and password for a database user account with access to the database for eDOCS DM.
Server Name	The name of the server where the database for eDOCS DM is located. (The server name must use only alphanumeric characters; underscores are not allowed.)
Version	The full version and point release used. For example, for eDOCS version 10, type `10.0` in the version box.
Library	The name of the database or library containing the documents you want to index.

ADDING AN IMANAGE WORK DATA SOURCE CONNECTION

Before adding data source connections for iManage Work, note the following West km requirements:

- iManage Work saved searches that are used to identify documents in West km should be restricted to only the database on which the search exists. For example, if search folder *Search1* exists on database *DB1*, then the search database specified should be *DB1* and only *DB1*. Specifying any database other than DB1 may lead to duplicate documents being indexed by West km and may slow down the indexing process.
- iManage Work saved searches must be saved under My Folders or Other Folders in iManage Work Explorer. Saved searches that are saved outside of iManage Work Explorer (e.g., My Matters) or in subfolders will not appear in West km.
- West km does not process searches in iManage Work workspaces (a new feature in iManage Work 8.0).
- It is recommended that sub-searches (a new feature in iManage Work 8.0) not be used with West km, because duplicate documents that are retrieved by both the main search and the sub-search will cause errors during indexing.
- Only one version of iManage Work can work with West km at one time. West km will not function correctly if you have document collections from more than one version.

Provide the information listed in the following table when adding a data source connection for iManage Work.

Field Name	Description
Type	The data source used to manage the documents (i.e., **iManage Work**).
User Name and Password (iManage Work)	The user name and password for the iManage Work server login.
Server Name (iManage Work)	The name of the server where iManage Work is located. (The server name must use only alphanumeric characters; underscores are not allowed.)
Library	The name of the database or library containing the documents you want to index.

Field Name	Description
Server Name (Database)	The name of the server where the database for iManage Work is located.
Database Name	The name of the database for iManage Work.
User Name and Password (Database)	The user name and password for a database user account with access to the database for iManage Work.
Use UNC Path for Document Copy	When this option is cleared (the default), West km uses the iManage Work API to access documents. When this option is selected, West km uses the UNC path to access documents. Select this option if the HTML Conversion indexing component fails when processing by component. When this option is selected, West km uses the remote access account configured on the West km system to access documents; the user account requires read and execute permissions to the iManage Work file server where the documents reside.

ADDING AN IMANAGE WORK IN THE CLOUD DATA SOURCE CONNECTION

Provide the information listed in the following table when adding a data source connection for iManage Work in the Cloud.

Field Name	Description
Type	The data source used to manage the document (i.e., iManage Work in the Cloud).
Server Name	The name of the server where iManage Work is located.
Library	The name of the database or library containing the documents you want to index.
User Name and Password	The user name and password for a database user account with access to the database for iManage Work in the Cloud.
Workspace	The name of the workspace where saved searches are located.

ADDING A NETDOCUMENTS DATA SOURCE CONNECTION

Provide the information listed in the following table when adding a data source connection for NetDocuments.

Field Name	Description
Type	The data source used to manage the documents (i.e., NetDocuments).
Server Name	The URL to your organization's local document store for NetDocuments. This is an internal website.
Library	The GUID for the NetDocuments cabinet (e.g., NG-4JPJW7B0) that contains the documents you want to index. You can get the cabinet GUID from the URL while you are on a cabinet's home page in NetDocuments.
Refresh Token	NetDocuments provides a connection token to be renewed once a year. To renew the token, click **Authenticate with NetDocuments**.

ADDING AN NT FILE SYSTEM DATA SOURCE CONNECTION

Provide the information listed in the following table when adding a data source connection for the NT file system.

Field Name	Description
Type	The data source used to manage the documents (i.e., NTFS).
Server Name	The name of the server containing the documents you want to index. (The server name must use only alphanumeric characters; underscores are not allowed.)
Library	The shared location used to store documents on the server. For example, if the server and share is: `\\pheasant\documents`, then type `documents`.

ADDING A PROLAW DATA SOURCE CONNECTION

Provide the information listed in the following table when adding a data source connection for ProLaw.

Field Name	Description
Type	The data source used to manage the documents (i.e., ProLaw).
ProLaw 11 or Later	If your organization uses ProLaw 11 or later, select this option.

Field Name	Description
Server Name	The name of the server where the database for ProLaw is located. (The server name must use only alphanumeric characters; underscores are not allowed.)
Library	The name of the database or library containing the documents you want to index.
Use Windows Authentication	A database account is used by default to access the database for ProLaw and the documents are you going to index. If you want to use a Windows account instead, select this option and contact your West km representative for more information.
User Name and Password	The user name and password for a database user account with access to the database for ProLaw.
Collection	Use this feature to add or edit document collections for this database. (You also have this option when you add document collections to West km. For more information, see "Adding Document Collections" on page 71.) To add a collection, click **New** from the drop-down list and type a collection name. To edit a collection already defined, click the collection name from the drop-down list. Enter any ProLaw criteria you want used to select documents for inclusion in this collection. You can enter dates in a variety of formats (e.g., 11/30/2012; 11-30-2012; November 30, 2012; 30 November 2012) and West km will recognize the date. If you don't enter any criteria, all documents in the database will be included.

Selecting a Library Group Collection

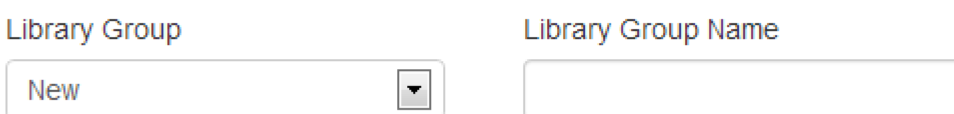
When adding or editing a data source connection, you can select a library group collection to have a library group different from the library group for the data source containing the collection.

Note When adding or editing a document collection, you can also select a library group if you want the Library groups allow your West km members to restrict searches of your internal documents, for example, to search within office locations or practice categories.

To select an existing library group for a data source connection, in the **Library Group** list, select the library group name.

To define a new library group for a data source connection,

1. In the **Library Group** list, click **New**.



2. In the **Library Group Name** box, type a name for the library group.

You can manage library groups at Setup, User Interface, Library Group, Current Library Groups. As well as adding library groups, you can edit and delete library groups at that location.

Note Changes to a document collection's library group will not be reflected in full-text searches until you re-index the document collection (incremental or bulk) and update full-text indexes. New library groups will not appear in the end-user interface for any currently running West km sessions until the user closes and re-opens the Web browser.

Changing Data Source Connections

You can edit and remove data source connections from the Connections page. To access the Connections page,

1. Access the West km interface.
2. Click **Setup**.
3. Click the **Data Source Management** tab.
4. In the left frame, click **Connections**.

EDITING A DATA SOURCE CONNECTION

To edit a data source connection, click the server name of the connection you want to edit on the Connections page. Then edit the values and click **Save**. If you cannot click in a text box or select a value, the field cannot be edited.

REMOVING DATA SOURCE CONNECTIONS

You can permanently remove data source connections. Note the following:

- When you remove a data source connection, any associated document collections are also removed. The system automatically schedules synchronization to run when the next synchronization window opens, at which point the documents are removed.
- When you remove a data source connection, the connection is also removed in the West km Vetting Toolkit and documents associated with the connection are removed when vetting synchronization occurs during vetting.
- If you wish to avoid re-indexing of documents, it is recommended that you seek assistance from your West km representative before removing data source connections.

To permanently remove one or more data source connections,

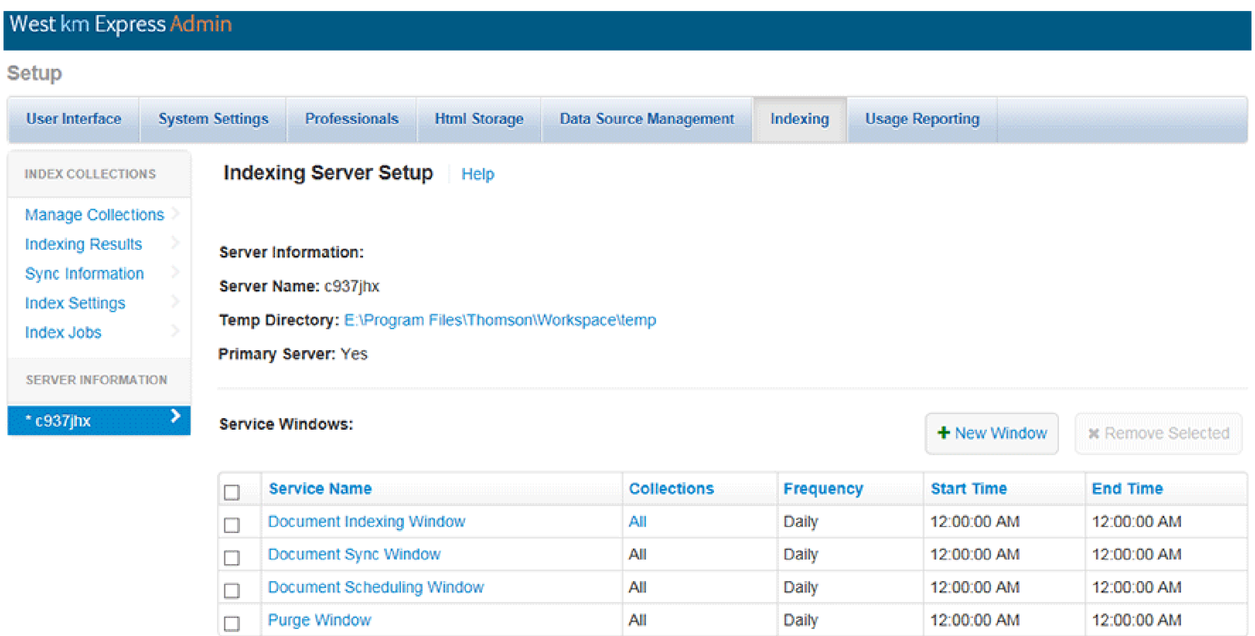
1. On the Connections page, select the check box to the left of each connection that you want to remove.
2. Click Remove Selected.

Setting Up the Indexing Server

You can define indexing service windows, indicate how indexing components should be processed, and add or remove indexing servers. To set up the indexing server,

1. Access the West km interface.
2. Click Setup.
3. Click the Indexing tab.
4. In the left frame, click the server name under Server Information...

The Indexing Server Setup page is displayed. Information is shown for your primary indexing server, which schedules and controls indexing and any other indexing servers. If more than one indexing server is defined, the primary indexing server is marked with an asterisk (*) in the left frame.



Indexing Service Windows

Indexing service windows define the time period during which indexing processes can occur. West km will not perform indexing processes until you define the necessary service windows.

The following table describes the available indexing service windows and what they do.

Service Window	Description
Vetting Window	The time window during which vetting can run. By default, no window is defined.
Vetting Scheduling Window	The time window during which vetting groups can be automatically scheduled for vetting processes. By default, no window is defined. (Note that automatic scheduling occurs only when both the vetting scheduling window and the vetting window are open.)

Service Window	Description
Document Indexing Window	The time window during which indexing can run. By default, no window is defined.
Document Scheduling Window	The time window during which document collections can be automatically scheduled for incremental indexing updates. By default, a 24-hour window is defined. (Note that automatic scheduling occurs only when both the document scheduling window and the document indexing window are open.)
Document Sync Window	The time window during which synchronization can be automatically scheduled and can run. By default, no window is defined.
Purge Window	The time window during which indexing job information that's no longer needed can be cleaned up.

Note: These windows do not define time windows for full-text indexing. For more information, see "Full-Text Indexing" on page 79.

For more information about:

- Recommended scheduling of indexing processes, see "Performing Major Indexing Updates" on page 49.
- Vetting processes, see "Managing Vetting Groups" on page 61.
- Indexing processes, see "Indexing Document Collections" on page 75.
- Synchronization processes, see "Synchronizing Document Collections" on page 78.

ADDING INDEXING SERVICE WINDOWS

To add an indexing service window,

1. At the Indexing Server Setup page, in the left frame, click the name of the server for which you want to add windows.

You can add document indexing windows on primary or secondary indexing servers; you can add other windows on the primary indexing server only.

2. Click New Window.
3. In the Add Service Window dialog box, enter the following information and click Save.
   - Service Name: Select the indexing service for which you'd like to define a window.
   - Frequency: Select the frequency for the window. Weekdays refer to Monday through Friday. Weekends refer to Saturday and Sunday.
   - Start Time and End Time: Type the start time and the end time for the window in hours and minutes and indicate whether the time is a.m. or p.m. A window's start time always occurs on the day specified for the Frequency. The end time may occur the day afterward, depending on whether the start time is set before or after the end time.

     Note: A 24-hour open window has both a start time and end time of 12:00:00 AM.
4. If you are adding a vetting window, click All in the Collections column for that window. In the Select Servers and Collections dialog box, select the vetting groups for which you want the window to apply and click Save.

If no selections are made for a window, the window applies to all vetting groups and is referred to as an "All" window.

For more information about using this feature, see the following subsection: "Using Multiple Indexing Service Windows."

5. If you are adding a document indexing window and want the window to apply only to specific data sources or document collections, click All in the Collections column for that window. In the Select Servers and Collections dialog box, select the sources or collections you want and click Save.

If no selections are made for a window, the window applies to all sources or collections and is referred to as an "All" window.

For more information about using this feature, see the following subsection: "Using Multiple Indexing Service Windows."

To edit an indexing service window, click the service window name, make your changes, and click Save.

To edit the sources or document collections that are selected for an indexing service window, click All in the Collections column for the window, make your changes, and click Save.

To remove one or more indexing service window, select the check boxes next to the window listings and click Remove Selected.

USING MULTIPLE INDEXING SERVICE WINDOWS

You may want to set up multiple vetting windows or document indexing windows in these situations:

- You want to control vetting and indexing for DMS servers in different time zones. Set up as many windows as you need for the different servers and time zones. When you enter the start and end times for a window, convert times to the time zone of the indexing server. Then select the applicable data sources for each window.
- You want windows to apply only to specific vetting groups, data sources, or document collections. For example, if you want document collections to be updated at different times, then define as many document indexing windows as you need for the different times. Then select the sources/ collections you want for each.

- You want processes to run during different times on weekdays and weekends. For example, if you want indexing to run at one time on weekdays and another time on weekends, define two document indexing windows. Choose a frequency of Weekdays for one window and Weekends for the other.

SELECTING VETTING GROUPS AND COLLECTIONS

- When you add a vetting group (see "Managing Vetting Groups" on page 61 for more information), it is automatically added to “All” vetting windows.
- When you add a data source connection or document collection (see "Adding Document Collections" on page 71 for more information), it is automatically added to “All” document indexing windows.
- When you add a vetting group and there is no “All” window, you must manually select the group in a vetting window for vetting to occur.
- When you add a data source connection or document collection and there is no “All” window, you must manually select the connection/collection in a document indexing window for indexing to occur. This is true for a collection even if the corresponding data source is already selected.

AUTOMATIC SCHEDULING OF VETTING AND INDEXING

The following items are required for automatic scheduling of vetting to occur for a vetting group:

- Both a vetting scheduling window and a vetting window are open
- The vetting group is selected in a vetting window (or you have an “All” window)
- The vetting group is not being processed by indexing

The following items are required for automatic scheduling of indexing to occur for a document collection:

- Both a document scheduling window and a document indexing window are open
- The document collection is selected in a document indexing window (or you have an “All” window)
- The document collection is not being processed by vetting

For both vetting and indexing, the oldest available jobs are scheduled first.

INTEROPERATING VETTING AND INDEXING WINDOWS

- Vetting windows and document indexing windows were built to interoperate. For example, vetting will not run for a vetting group while the collection is being scheduled for indexing. As a result, you can overlap the times of vetting and document indexing windows to maximize indexing efficiency.
- Vetting and indexing follow each other seamlessly for automatic processing of a document collection, but not after vetting is manually launched. This exception allows you to view vetting results before indexing scheduling occurs. If you manually launch vetting for a collection and then want it indexed, manually launch indexing of the collection. Upon indexing, normal interoperation for automatic processing between vetting and indexing then resumes.

Processing at the Close of Windows

If processing isn’t finished when a window closes, the indexing service windows perform as indicated in the following table.

Service Window	Processing Behavior When Window Closes
Vetting Window	Processing stops within 10–15 minutes and then continues when the window reopens.
Document Indexing Window	Processing continues until delegated documents are finished. No additional documents are delegated from the queue.
Document Sync Window	Processing continues beyond the close of the window until synchronization is finished.

INDEXING COMPONENTS

By default, West km is set up so that it processes a subset of documents through all the indexing components before it moves to the next subset of documents.

To change the options for indexing components,

1. At the Indexing Server Setup page, in the left frame, click the name of the server for which you want to set options.
2. Select the options you want in the Indexing Components table.
    - Suspend: If you select Suspend for an indexing component, processing for the component is suspended for all document collections during indexing, regardless of the settings for the individual document collections. (If you select this option, it will stay selected until you clear it.)

      If not selected (the default), processing for the component proceeds during indexing according to the settings for the individual document collections.

- **Process by Component**: If you select Process by Component for an indexing component, processing for the component will continue until no more documents are available to be indexed before moving on to process the next component. (If you select this option, it will stay selected until you clear it.)

  If not selected (the default), a subset of documents to be indexed is processed by all the indexing components (according to the settings for the document collection) before moving on to the next subset of documents. The number of documents in the subset is determined by the thread count. By default, 10 threads are used, with a maximum of 10 documents processed per thread.

INDEXING SERVERS

You can add or remove indexing servers from the West km system, as well as change the server that is designated as primary.

Adding an Indexing Server

To add an indexing server,

1. On any new indexing servers, run the necessary setup programs. See the West km Administrator Installation Guide for detailed instruction.
2. At the Indexing Server Setup page, click **New Server**.
3. In the New Server dialog box, type the name of the server in the **Name** box, change the server's temporary folder in the **Temp Directory** box, if desired, and click **Save**.

The server is added to the list of indexing servers in the left frame. To access a server's information, click its name.

To change a server's temporary folder, click the folder path, type your changes, and click **Update**.

Removing an Indexing Server

To remove an indexing server,

1. If the indexing server you want to remove is your primary indexing server, first complete the steps in the following subsection, "Changing the Primary Indexing Server," to designate a different indexing server as primary.
2. At the Indexing Server Setup page, in the left frame, click the name of the server you want to remove.
3. Click **Remove Server**.

If the removed indexing server will no longer be used in West km, see the West km Administrator Installation Guide for instructions on removing West km software.

Changing the Primary Indexing Server

The primary indexing server schedules and controls indexing. If more than one indexing server is defined, you can change the indexing server that is designated as primary.

To set an indexing server as primary,

1. At the Indexing Server Setup page, in the left frame, click the name of the server you want to designate as primary.
2. Click **Make Primary**.

The selected server is made primary and the indexing service windows are copied from the old primary indexing server to the new indexing server.

Customizing the KeySearch Hierarchy

As a KeySearch editor, you can customize the KeySearch hierarchy for your organization.

Note To designate a West km member as KeySearch editor, see "Managing Users" on page 85.

KeySearch is a tool from Thomson Reuters that helps researchers easily and precisely retrieve documents relevant to a particular legal topic. Your West km members can use the KeySearch hierarchy in the West km interface to retrieve documents at your organization.

The categorization and recommendation engine (CaRE) automatically assigns your organization's documents to KeySearch topics when you index your documents in West km. You can also

- customize the existing KeySearch hierarchy for your organization's specific needs
- create and edit queries that use full-text searching to retrieve documents on KeySearch topics
- manually assign a document collection to KeySearch topics (an option during indexing)

To access the KeySearch hierarchy of legal topics so you can customize it for your organization,

1. Access the West km interface. For details, see "Accessing West km" on page 3.
2. Click the **KeySearch** tab.
3. Click **Administration** at the top of the KeySearch hierarchy.

The KeySearch topics are listed alphabetically on the KeySearch tab. In this KeySearch administrative view, you can customize the KeySearch hierarchy, as well as perform all KeySearch search functions.

To browse the list of KeySearch topics and subtopics, click the hypertext links.

- Links without Edit and Delete icons represent standard topics and subtopics.
- Links followed by Edit and Delete icons represent customized topics and subtopics that you have created.
- Links in gray text represent standard or customized topics and subtopics that you have hidden from the view of West km members at your organization.

When you browse to a topic, a bread crumb trail at the top of the tab shows your location in the KeySearch hierarchy. You can click a hypertext link in the bread crumb trail to move to that location in the hierarchy.

Home > Bankruptcy > Assets

Counts after topics in the KeySearch hierarchy indicate the number of unique documents at your organization that have been assigned to that topic via manual classification or the categorization and recommendation engine (CaRE). Counts do not include documents retrieved via Terms and Connectors queries.

To exit the administrative view of the KeySearch hierarchy and view the hierarchy as it is displayed to West km members, click **End Administration** at the top of the hierarchy.

ADDING A KEYSEARCH TOPIC

You can create a customized KeySearch topic by adding it to the KeySearch hierarchy:

1. In the administrative view of the KeySearch hierarchy, browse to the topic or subtopic above the point where you want to add the new topic. You can add a topic from any standard or customized topic within the hierarchy.
2. Click **New Topic**.
3. On the New Topic page, enter the following information for the new topic:
   - **Category name**: The topic name that is to be displayed in the KeySearch hierarchy. The category name is limited to 128 characters, and the following characters are not allowed: \, /, ", @, %, !, #, +.
   - **Shortcut name**: An optional name for the topic that is displayed as a hypertext link on the page one level above the new topic.
   - **Location**: The location in the KeySearch hierarchy where the topic will be added. To select a different location, click Browse and then click the link for the topic you want. Leave the location blank to add the topic to the top level.
   - **Query**: An optional full-text query that is used to retrieve documents for the topic, in addition to automatic and manual classification methods. Your query can include field restrictions.
4. Click **Save**.

The hierarchy is displayed at the topic above the newly created topic.

Note When you are indexing your documents and CaRE is configured to run, CaRE will not assign documents to customized KeySearch topics.

Field restrictions:

Field Restriction	Abbreviation	Examples
Abstract	abst	abst("summary judgment")
Attorney (Lit)	at	at(nelson)
Author	au	au(john /3 maxwell)
Client ID	cid	cid(1587)
Client Name	cn	cn(reardon)
Client-Matter ID	cmid	cmid(1587-2228)
Client-Matter Name	cmn	cmn(reardon & pritchard)
Company	comp	comp(microsoft)
Court[1]	co	co(united states supreme court)

Field Restriction	Abbreviation	Examples
Created Date[2]	cd	specific date:cd(1/14/2011) after:cd(aft 1/14/2011)
		before:cd(bef 1/30/2011)
		after & before:cd(aft 12/12/2007 & bef 1/1/2011)
DMS Doc Type	dt	dt(brief)
DMS Number	dn	dn(32027)
Doc Type[1]	docty	docty(brief)
Exemplar Documents and Exemplar Forms	exem	exem(1) Use one of these values in the parentheses: 0 = no marking 1 = exemplar document marking 2 = exemplar form marking
Expert	ex	ex(martinez)
File Name	ti	ti(nevada & blueson)
Judge–Primary[3]	jp	jp(anderson /3 barry)
Judge–Secondary[3]	js	js(halbrooks)
Jurisdiction[1]	jur	jur(federal)
Law Firm (Lit)	lf	lf(bendini & lambert)
Library Group	lg	lg("ny office")
Litigation Doc Title	docti	docti("dole food" /5 patrickson)
Matter ID	mi	mi(1587-2228)
Matter Name	mn	mn(pritchard)
Modified Date[2]	md	specific date:md(2/14/2011) after:md(aft 2/14/2011) before:md(bef 2/27/2011) after & before:md(aft 12/12/2007 & bef 1/1/2011
Notes	annos	annos(power +3 attorney)
Results with Notes	com	com(true) Use one of these values in the parentheses: true = has comments false = has no comments
Custom 1[4] Custom 2 Custom 3	cust1 cust2 cust3	cust1(antitrust) cust2(expert!) cust3("form-agrmt-lit")

[1] The litigation court, doc type, and jurisdiction fields are phrase indexed, so you must search for the terms exactly, including punctuation and spacing. As an alternative to typing the complete exact phrase, you can use the root expander (!) at the end of the term, e.g., docty(memo!).

[2] The Created Date and Modified Date fields are not inclusive when you search a range of documents. For example, if you search for documents modified after 1/1/2010, documents modified on January 1, 2010, won't be retrieved.

[3] To search both judge fields simultaneously, type jp,js(halbrooks).

[4] The data in custom fields depends on the DMS fields that your administrator has mapped. The examples shown assume Custom 1 is mapped to a practice area field, Custom 2 is mapped to a document sub-type field, and Custom 3 is mapped to a form type field.

EDITING AND COPYING A KEYSEARCH TOPIC

You can edit a KeySearch topic you have created or create a customized KeySearch topic by copying it from another topic.

Editing a KeySearch topic:

1. In the administrative view of the KeySearch hierarchy, browse to the topic or subtopic that you want to edit. You can edit any topic you have created, whether it is shown or hidden.
2. Next to the topic you want to edit, click the Edit icon.
3. Edit the information for the topic and click Save.

The hierarchy is displayed at the topic above the edited topic.

Copying a Keysearch Topic

1. In the administrative view of the KeySearch hierarchy, browse to the topic or subtopic that you want to copy. You can copy from any standard or customized topic within the hierarchy.
2. Next to the topic you want to copy, click the Copy icon.
3. Enter a category name and shortcut name (if desired) for the new topic.

4. The location is populated from the topic you are copying. To select a new location, click Browse and then click the link for the topic you want.
5. The query is populated from the topic you are copying. Edit the query if desired.
6. Click Save.

The hierarchy is displayed at the topic above the newly created topic.

Note When you are indexing your documents and CaRE is configured to run, CaRE will not assign documents to customized KeySearch topics.

HIDING AND SHOWING A KEYSEARCH TOPIC

You can hide any KeySearch topic from the view of West km members at your organization:

1. In the administrative view of the KeySearch hierarchy, browse to the topic or subtopic that you want to hide. You can hide any standard or customized topic within the hierarchy.
2. Next to the topic you want to hide, click the Hide/Show icon.

The hierarchy is displayed at the topic above the hidden topic. The topic and its subtopics are represented by gray text.

To show a topic that you have previously hidden, browse to the topic or subtopic that you want to show and click the Hide/Show icon.

Note Hiding a topic will not hide the same topic appearing elsewhere in the KeySearch hierarchy. For example, hiding Searches and Seizures under Constitutional Law will not automatically hide Searches and Seizures under Criminal Justice.

Note When you are indexing your documents and CaRE is configured to run, CaRE will assign documents to hidden KeySearch topics.

DELETING A KEYSEARCH TOPIC

You can delete a KeySearch topic you have created:

1. In the administrative view of the KeySearch hierarchy, browse to the topic or subtopic that you want to delete. You can delete any topic you have created, whether it is shown or hidden.
2. Next to the topic you want to delete, click the Delete ✖ icon.
3. Click OK to confirm the deletion.

The hierarchy is displayed at the topic above the deleted topic.

Note Deleting a KeySearch topic does not delete the indexed documents that you assigned to the topic.

Performing Major Indexing Updates

Follow the guidelines in this section for indexing updates that involve major changes to document collections, such as significant numbers of new, updated, or removed documents.

1. Set aside a large block of time, such as a weekend, when end users are not accessing West km.
2. At the Indexing Server Setup page, delete the following windows to prevent indexing processes from occurring automatically:
   - vetting scheduling windows
   - document scheduling windows
   - document sync windows

For more information, see "Indexing Service Windows" on page 43.

3. Remove full-text indexing windows to turn off full-text indexing. For more information, see "Full-Text Indexing" on page 79.
4. Define a vetting window at the Indexing Server Setup page for all vetting groups. Make it a 24-hour open window.

Service	Start and End Time
Vetting Window	12:00:00 AM–12:00:00 AM

5. Run vetting rules for your vetting groups in the West km Vetting Toolkit. To do this, on the Manage Vetting Groups page, select the check box to the left of each vetting group whose rules you want to run and click Run Selected. For more information, see "Managing Vetting Groups" on page 61.
6. When vetting is complete, define a document indexing window at the Indexing Server Setup page for all document collections. Make it a 24-hour open window.

Service	Start and End Time
Document Indexing Window	12:00:00 AM–12:00:00 AM

7. Consider using the Suspend and Process by Component options at the Indexing Server Setup page to control how and when indexing components are processed (see "Indexing Components" on page 45 for more information).
8. Run an incremental update on all your document collections. To do this, select the document collections at the Manage Collections page, click Actions, and then click Start Incremental Jobs (see "Indexing Document Collections" on page 75 for more information)
9. When the incremental update is complete, synchronize your document collections. To do this, first add a document sync window at the Indexing Server Setup page. Then while the window is open, go to Setup, Indexing, Indexing Jobs and click Sync Documents. For more information, see "Synchronizing Document Collections" on page 78.
10. When synchronization is complete, run another incremental update on all your document collections.

When the second incremental update is complete, build full-text indexes. To do this, first add a full-text indexing window. Then while the window is open, go to Setup, HTML Storage, Collections, and for each collection, select Reindex All Content and click Start. For more information, see "Full-Text Indexing" on page 79.

11. When full-text indexing is complete, reset all your windows according to the scheduling guidelines in the "Routine Indexing Maintenance" on page 50.

Routine Indexing Maintenance

The guidelines in this section show you how routine indexing updates can be set up. Routine indexing updates don't involve major changes to document collections.

To schedule routine updates, you define windows that set the time during which vetting, indexing, synchronization, and full-text indexing occur. For details on setting vetting, indexing, and synchronization windows, see "Indexing Service Windows" on page 43. For details on setting full-text indexing windows, see "Full-Text Indexing" on page 79.

You typically want indexing processes to run outside your organization's regular business hours and outside maintenance and backup processes on the server. Identify your nightly downtime when the West km servers are available for indexing—for example, 12 a.m. to 8 a.m.—and set up West km indexing windows during that downtime.

Note As an alternative to setting up indexing windows outside regular business hours, you may consider setting up 24-hour open windows for document indexing and then manually suspend the HTML conversion component during regular business hours. Unlike other components, the HTML conversion component accesses your document management system to retrieve documents, so running it during business hours should be avoided. For more information about the Suspend option, see "Indexing Components" on page 45.

The following subsections contain sample schedules for routine indexing updates. Note that all examples assume a 24-hour open window for the vetting scheduling window, the document scheduling window, and the purge window.

Indexing Schedule—Daily

The following table shows a sample schedule for routine indexing updates. It exemplifies the following best practices:

- If possible, run indexing and vetting processes daily.
- For the greatest efficiency, run vetting and indexing processes at the same time. However, avoid overlapping the vetting/indexing, synchronization, and full-text indexing windows for configurations running on one server.
- Set up windows incrementally in this order: vetting/indexing, synchronization, and full-text indexing.
- Run the full-text indexing reclaim process weekly.

Example of a Daily Indexing Schedule[1]:

<table>
<tr><th></th><th>Monday</th><th>Tuesday</th><th>Wednesday</th><th>Thursday</th><th>Friday</th><th>Saturday</th><th>Sunday</th></tr>
<tr><td>12 a.m.</td><td colspan="7" rowspan="6">Vetting Window, Daily, 12:00:00 AM–5:59:59 AM
Document Indexing Window, Daily, 12:00:00 AM–5:59:59 AM[2]</td></tr>
<tr><td>1 a.m.</td></tr>
<tr><td>2 a.m.</td></tr>
<tr><td>3 a.m.</td></tr>
<tr><td>4 a.m.</td></tr>
<tr><td>5 a.m.</td></tr>
<tr><td>6 a.m.</td><td colspan="7">Document Sync Window, Daily, 6:00:00 AM–6:59:59 AM</td></tr>
<tr><td>7 a.m.</td><td colspan="7">Full-Text Indexing Scheduling, Daily, 7:00:00 AM–7:59:59 AM</td></tr>
<tr><td>8 a.m.</td><td colspan="5" rowspan="14">Regular Business Hours</td><td></td><td rowspan="14">Full-Text Indexing Reclaim Process, Sunday, 8:00:00 AM–9:59:59 PM</td></tr>
<tr><td>9 a.m.</td><td></td></tr>
<tr><td>10 a.m.</td><td></td></tr>
<tr><td>11 a.m.</td><td></td></tr>
<tr><td>12 p.m. noon</td><td></td></tr>
<tr><td>1 p.m.</td><td></td></tr>
<tr><td>2 p.m.</td><td></td></tr>
<tr><td>3 p.m.</td><td></td></tr>
<tr><td>4 p.m.</td><td></td></tr>
<tr><td>5 p.m.</td><td></td></tr>
<tr><td>6 p.m.</td><td></td></tr>
<tr><td>7 p.m.</td><td></td></tr>
<tr><td>8 p.m.</td><td></td></tr>
<tr><td>9 p.m.</td><td></td></tr>
<tr><td>10 p.m.</td><td colspan="5" rowspan="2">Maintenance and Backups</td><td></td><td></td></tr>
<tr><td>11 p.m.</td><td></td><td></td></tr>
</table>

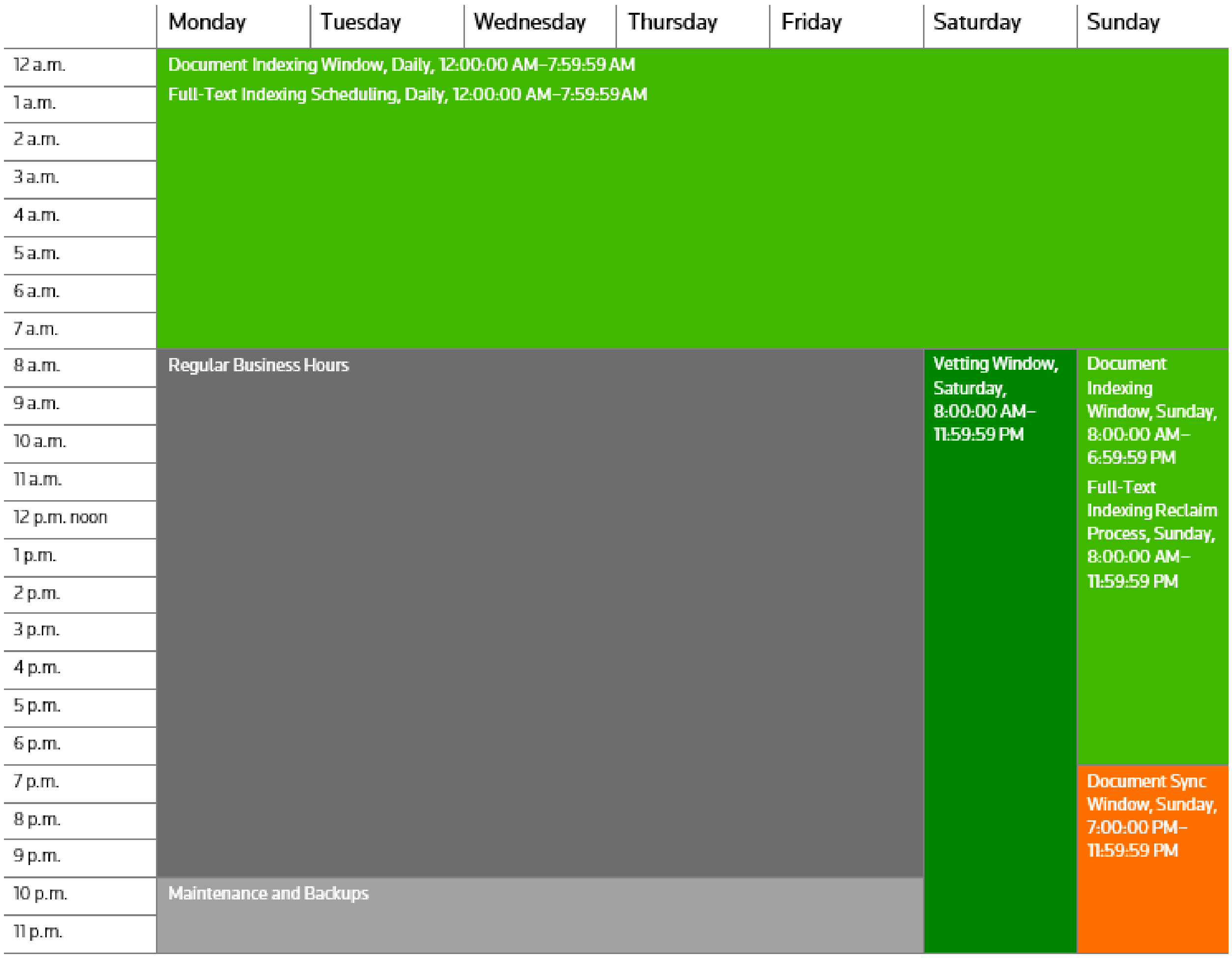
[1] The example assumes a 24-hour open window for the document scheduling window and the purge window.

[2] If you experience SQL Server timeout errors or observe that indexing does not complete when the vetting and indexing windows overlap, split the time between the windows and increment them, e.g., the Vetting Window 12:00:00 AM–2:59:59 AM and Document Indexing Window 3:00:00 AM–5:59:59 AM.

Indexing Schedule—Daily and Weekends

If you have a distributed environment for West km, you have greater flexibility in setting up indexing windows. For example, you can run full-text indexing simultaneously with indexing as shown in the following table. This configuration, which uses both daily and weekend windows, is also useful if you have a large source collection and indexing processes do not complete with only daily windows.

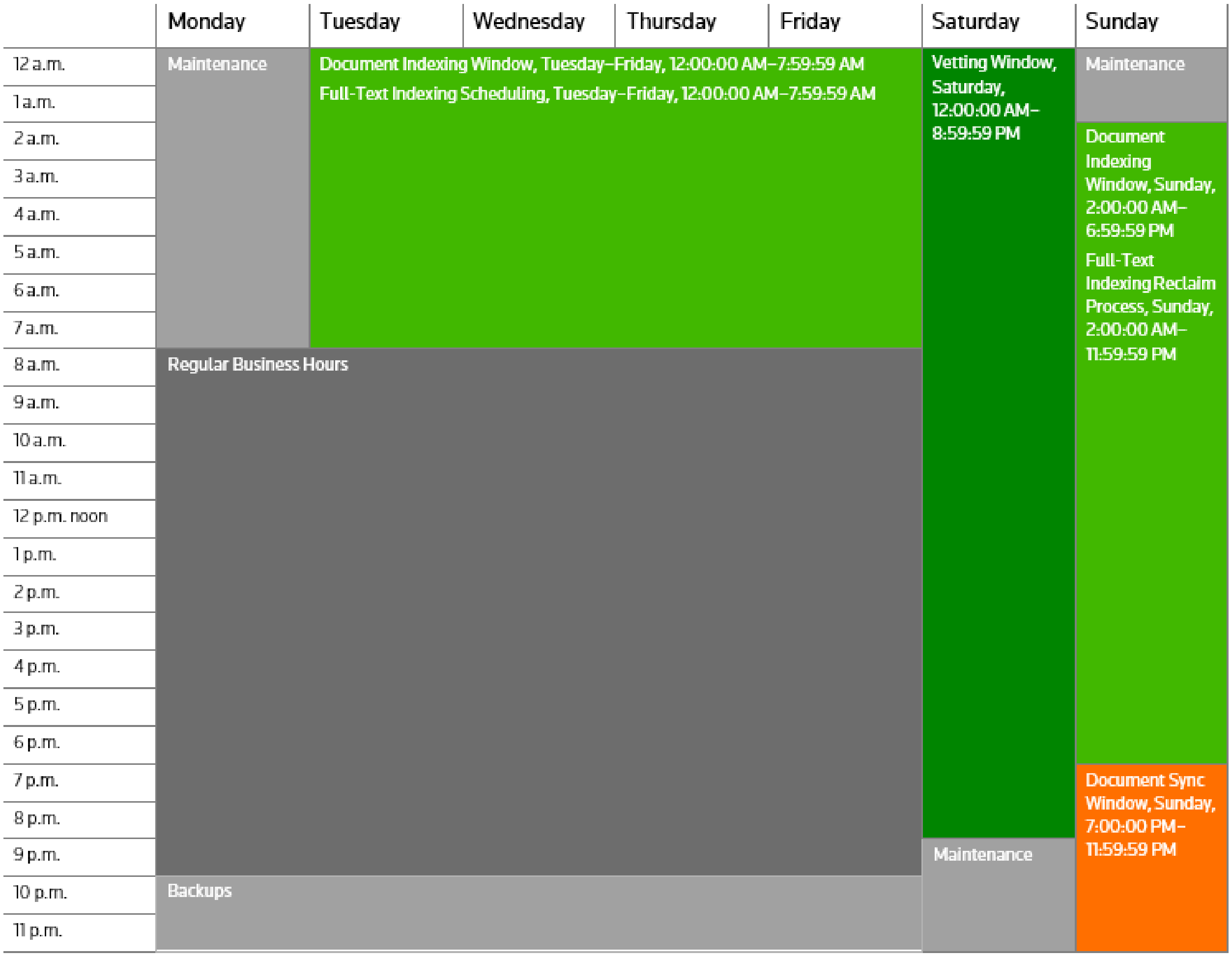
Example of a Daily and Weekend Indexing Schedule:



Indexing Schedule—Custom

If you have a server maintenance and backup schedule that would prevent you from setting up daily windows, you can design a West km indexing schedule that works around these time periods. For example, the following table shows a configuration that does not run West km indexing processes on Mondays because of scheduled maintenance.

Example of a Custom Indexing Schedule:



6 Vetting Documents

Before you index documents in West km, the West km Vetting Toolkit can help you fine-tune the selection of documents from these document management systems (DMSs): iManage Work, and eDOCS DM. This process provides a visual method for identifying and tagging documents for inclusion in West km and serves to improve search accuracy and precision within West km.

If you are a vetting editor in West km, you can access the vetting toolkit.

Developing a Vetting Strategy

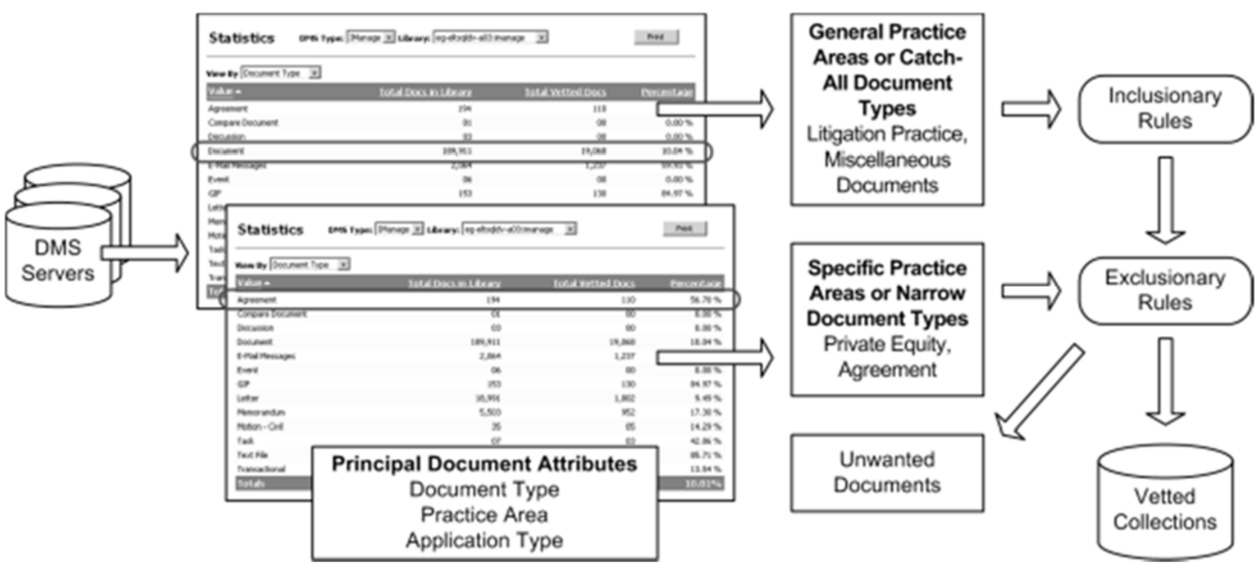
This section discusses strategies for using the vetting toolkit to select documents for inclusion in West km.

Your vetting strategy can take advantage of a range of DMS profile and full-text search mechanisms, resulting in one or more content-rich document collections. Document collections are oriented towards general litigation, court papers, or transactions so they can benefit from the indexing processes most suitable for those documents. Typically, an organization builds its vetting strategy by first classifying practices into general litigation or transactional groups, and then office locations and document types; or they may use specific practice groupings and document types.

To start, it can be helpful to gather document statistics from your document management system. After installation, the Statistics page in the vetting toolkit highlights how users tend to store their documents in the document management system. You'll see large numbers of documents profiled using catch-all document types; you'll also see more refined sets of documents that are profiled using well-defined or "narrow" document types. The Statistics page also highlights document collections by authors, client number, and other fields that could be helpful in crafting rules and exceptions to those rules during the iterative vetting process.

Knowing these statistics can help you develop a strategy that applies filtering by document name to the catch-all document types. This strategy allows documents profiled with narrow document types into the vetting collections, so long as any of the documents are not excluded by the exclusionary rules.

To implement your strategy, you create vetting groups in the vetting toolkit to manage individual sets of inclusionary and exclusionary rules. The system then uses these vetting groups to create the vetted collections, on which indexing is run. This process is shown below.



Vetting Considerations

When developing a vetting strategy, making key strategic and tactical choices, understanding the data contained in your DMS fields, taking into account potential documents that are stored outside your document management system, and prioritizing collections are important considerations.

KEY CONSIDERATIONS

Making key strategic and tactical choices will help you develop your vetting strategy.

Strategic Choices

These key strategic choices can be made by asking questions of your organization's lawyers and high- level IT administrators.

- Select appropriate practice areas. Focus generally on litigation and transactional practice areas with a breakdown of specific practice groups to create narrowly defined content.
- Determine whether the collections should be limited to public documents or if they should also include private documents. If you are including private documents, select an appropriate document security level in West km.
- Decide how far back in time to collect documents. Organizations typically include documents within the last five to seven years. They may go back further for some practices, such as employee benefits. They may select more recent documents for transactional practices with frequent, repetitive deal documentation.
- Determine whether documents that are works in progress should be included in the collection. Because organizations generally do not have processes to mark final documents, you can restrict included documents to those that haven't been edited within a set period of days, for example, three days.
- Decide which, if any, fact-specific documents should come into the system, such as affidavits and interrogatories.

Tactical Choices

These key tactical choices can be made by asking questions of your organization's content managers, such as librarians.

- Should the organization's documents be grouped into collections in West km by practice area or by office?
- What percentage of documents from the entire document management system is the appropriate breadth or focus of the vetting rules? (Most organizations experience between 10 and 20 percent.)
- In addition to word processors, which application types should be included? For example, an increasing number of litigation practices are adding PDF documents, and transactional and litigation practices are adding PowerPoint slides.
- What specific exclusions are needed? For example, do you want to exclude documents based on clients or matters, billing groups, or the author's staff status (e.g., non-practitioner)? Using lists of authors or editors, you can exclude documents created by administrative staff. You can exclude documents under certain ethical wall restrictions. Or you can allow the documents to be indexed but then rely on tight DMS security integration with West km to secure documents from view in West km if users cannot see them in the document management system.

DMS FIELDS AND CONSIDERATIONS

As described in the following table, understanding the data contained in your DMS fields can also help you develop and implement a vetting strategy.

Vetting considerations for DMS fields:

DMS Field	Considerations
DMS Server/Library	From which DMS servers and libraries are you going to be gathering documents?
Practice Area	Do you use practice area, group, or team fields on your document profiles in the DMS to define the relevant practice? Practice area fields are helpful in the vetting process, because vetting collections can reference them to form practice-specific collections that are selectable and searchable in West km.
Document Type	Which document types are most likely to be content-rich? Which document types are used as well-defined, "narrow" categories? Which document types are most likely to be reused by attorneys? Which document types have the most value in training new hires? Which document types contain legal strategy? (Examples could include pleadings, legal memos, opinion letters, and briefs.) Which document types are used as catch-all or "broad" categories (and would therefore need additional criteria applied before considering them for inclusion)?
Document Name	If you use this field to flag "bad" documents, for example, by adding the text "DO NOT USE" or "DELETE", then you may want to exclude documents with certain text in this field.

	"Bad" documents could include templates, boilerplates, old versions, or drafts.
Author	Are key documents always saved in the author field under attorney names or also under support staff names? Do you have mentor attorneys who are known to produce exemplar documents? Do you have attorneys who have left the organization and whose documents should be excluded? Can you segment your authors into lists of litigation and transactional attorneys? Or areas of practice? Using author lists can help you create clean collections of documents specific for litigation or transactional indexing.
Client	Are there certain clients whose documents are confidential or sensitive, such as ethical walls, although end users may not have used DMS security? Do you represent competing clients, such as Microsoft and Cisco, for which different attorney teams should not see certain documents, and end users may not have used DMS security?
Matter	Are there certain matters for which documents are confidential or sensitive, although end users may not have used DMS security?
Document Number	If certain documents need to be excluded from indexing and your document management system allows you to exclude them, then you can list these documents in this field.
Application	Including only the document formats supported by West km will narrow your search and speed up the indexing process. For more information, see the West km Administrator Installation Guide.
Date Modified	What is the earliest date documents were modified in your document management system from which you would like to include documents (i.e., modified on that date or later)? Has the law changed significantly, warranting use of a more recent date to retrieve documents? Has the organization's culture changed or have personnel or work product procedures changed, warranting excluding documents before a certain date?
Work in Progress (delay n days before inclusion in West km)	Do you want to delay entry of documents into West km because they are presumed not finished? For example, do you want to delay entry of a document (or remove an existing document) if it's been edited within the last three days? Note If users save documents even if they haven't made changes, the edit date will change and the document will be flagged as a work-in-progress.
Secured Documents	If you have applied security to documents in your document management system, West km can mirror that security. If you have concerns about whether users have correct security settings in your document management system and would rather exclude all secure documents from the West km population, do not select Secured Documents in the document management system. Note iManage Work may not allow you to exclude secure documents in your search; a possible solution is to have West km index documents while using an iManage Work login with limited security.

DOCUMENT SOURCE CONSIDERATIONS

In addition to documents that are stored in your document management system, your vetting strategy should take into account potential documents that are stored outside your document management system.

- Approximately how many document collections do you have stored outside your document management system and where are they stored?
- Approximately how many folders (including sub-folders) contain these documents?
- If only a portion of these documents are to be indexed for West km, how will they be identified?

For more information about adding a collection of documents to West km that are outside your document management system and not vetted using the vetting toolkit, see "Adding Document Collections" on page 71.

PRIORITIZATION

Part of your vetting strategy should be to prioritize collections to maximize available indexing resources while minimizing the impact on end users. First, determine which vetted collections would have the most immediate value for the end users. Second, run vetting on those collections using a narrow date parameter in the rules to assure that the content is good. Third, associate the vetting collections with West km indexing collections and library groupings and index those collections first.

Accessing the Vetting Toolkit

To access the West km Vetting Toolkit,

1. Access the West km interface.
2. Click Setup.
3. Click the Vetting tab

Perform vetting functions using the following pages in the vetting toolkit:

- Toolkit Configuration: Define the fields from your document management system that you want to use in the vetting toolkit. These fields are used to define vetting rules. For more information, see "Configuring Vetting Fields" on page 57.
- Vetting Display: Set how fields are displayed in the vetting toolkit. For more information, see "Setting the Vetting Display" on page 60.
- Manage Vetting Groups: Define groups of vetting rules that result in a document collection. Also set up scheduled times to run the vetting rules for the collection, view the status of the vetting process for each vetting group and DMS database/library, and run vetting rules in a single DMS database/library. For more information, see "Managing Vetting Groups" on page 61.
- Vetting Rules: Add inclusionary and exclusionary rules to a vetting group. These vetting rules determine which documents will be included and which will be excluded from a collection. For more information, see "Administering Vetting Rules" on page 63.
- View Collection: View the documents included in a collection based on the vetting rules, and mark documents for exclusion, if desired. For more information, see "Viewing Collections" on page 68.
- Excluded Documents: View the documents manually excluded from a collection, and mark documents for inclusion, if desired. For more information, see "Viewing Excluded Documents" on page 69.
- Statistics: Compare the number of vetted documents to the total number of documents in the DMS database/library. For more information, see "Viewing Statistics" on page 70.

When you have vetted a document collection to your satisfaction, you can index it in West km. When adding a collection from the Indexing Options page, select Vetting Group. For more information, see "Adding Document Collections" on page 71.

Vetting Tips

- For the vetting toolkit to function, your data sources must be connected correctly at the Data Source Management page. For more information, see "Adding Data Source Connections" on page 39.
- Vetting rules will run only within the vetting windows defined on the Indexing Server Setup page.
- For best performance, set up more vetting groups containing fewer documents rather than fewer vetting groups containing more documents.
- To avoid overwriting someones data, it is recommended that only one vetting editor at your organization work in the toolkit at a time.

Configuring Vetting Fields

Define the fields from your document management system that you want to use in the vetting toolkit at the Toolkit Configuration page. You then have access to these fields when adding vetting rules, which determine the documents that will be included and excluded from a collection.

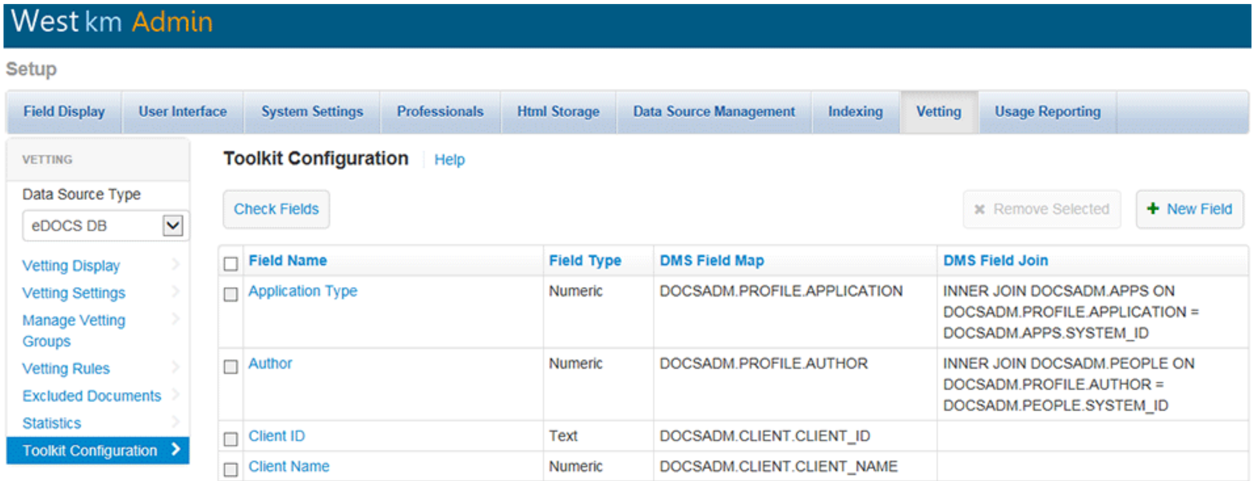
The following fields are included by default:

- iManage Work and eDOCS DM: application type, created date, document name, document author, document number, last doc modified date, version.
- iManage Work and eDOCS DM: client ID, client name, document abstract, document type, matter ID, matter name.
- iManage Work: document size.

A field that you add must meet these criteria:

- iManage Work: be connected to the document master table.
- eDOCS DM: be connected to the profile table.

To access the Toolkit Configuration page, click Toolkit Configuration in the left frame.



ADDING A FIELD

To add a field,

1. In the Data Source Type list, click your document management system.
2. Click New Field.
3. In the New Field dialog box, type or select the field information. For additional instructions, see the following "Field Information" section.
4. Click Save. The field is added to the Fields table.

Field Information

When adding a field, enter the following field information:

- Field Name (required): Type a name for the field (e.g., Subdocument Type).
- Field Type (required): Select the type of information contained in the field—text, date, or numeric. This selection determines the type of search control that is displayed for the field when adding a vetting rule. For example, Date results in a "less than/greater than or equal to" search control.
- DMS Field Map (required): Type the name of the field as it is known in your document management system.
  - For iManage Work and eDOCS DM, type the name of the field in databaseowner.tablename.fieldname format, for example,
    `MHGROUP.DOCMASTER.SUBCLASS_ALIAS`
- DMS Description Field Map: If a description field exists for the DMS field map and you want to display the description value for the field in toolkit test results, type the name of the field as it is known in your document management system.
  - For iManage Work and eDOCS DM, type the name of the field in databaseowner.tablename.fieldname format, for example,
    `MHGROUP.DOCSUBCLASSES.CLASSDESCRIPT`

Note To view the DMS Description Field Map value in the Fields table, hover over the DMS Field Map value.

- DMS Field Join (iManage Work and eDOCS DM only): If you want a look-up feature for the field to be available when adding a vetting rule, specify how the child table is joined to the parent table, for example,
  `LEFT OUTER JOIN MHGROUP.DOCSUBCLASSES ON MHGROUP.DOCMASTER.SUBCLASS_ALIAS = MHGROUP.DOCSUBCLASSES.SUBCLASS_ALIAS`

An outer join, not an inner join, is required whenever the field in question might not have data. With an outer join, if the field is not part of rule criteria, the vetting process ignores it. With an inner join, only documents that have a value in the field will be returned, even if the field is not part of the vetting criteria.

Consider the document data in the following table.

Document examples for vetting:

Document Name	Document Number	Optional Office Location
Pleading	1	NY
Fax	2	
Memo	3	NY
Will	4	

If an inner join is used to add the optional office location field, only documents 1 and 3 could be returned by any vetting rule, even if the field is not used in the rule. Unless an outer join is used, documents 2 and 4 could never be returned.

Notes:

- If you don't specify a field join, values corresponding to the DMS field map, not the DMS description field map, must be entered for field criteria when adding a vetting rule.
- For iManage Work, fields from the document master table must have the MHGROUP.DOCMASTER portion of the field entered in upper case.

Lookup Query (iManage Work and eDOCS DM only): If you want to display multiple fields from your document management system as columns in the FieldLookup dialog box that is used when defining field criteria for a vetting rule, then enter a SELECT DISTINCT statement that includes the fields you want as columns. Use a format such as this:

select distinct *databaseowner.tablename.fieldname1* as FieldKey,
databaseowner.tablename.fieldname2 as '*Parent*',
databaseowner.tablename.fieldname3 as '*Value*' from *databaseowner.tablename*
order by '*Parent*', '*Value*'

FieldKey is required and needs to be tied to the system ID for the child field. You can use any meaningful text for *Parent* and *Value*.

Notes:

- If you don't specify a lookup query, then the field defined for DMS Field Map will be displayed in the FieldLookup dialog box.
- In general, the lookup query does not join to the document master table (iManage Work) or profile table (eDOCS DM). Join these tables only if the desired result is to see only those values in the FieldLookup dialog box that are associated with actual documents in the library.
- Typically an inner join, not an outer join, is used for the lookup query. In the above example, an inner join ensures that only subdocument types that relate to document types are retrieved. (An outer join would retrieve all subdocument types, even if they don't relate to document types.)

Search Type: If you selected `Text` as the field type, select how you would like the text to be searched for this field when you add a vetting rule—contains, equals, starts with, or ends with.

CHECKING FIELDS

To verify the DMS field mappings on a server, click Check Fields, select a server from the Server list, and click Check. The result (*Success* or *Failure*) is displayed above the Server list. A failure indicates that fields are invalid or the server connection failed.

EDITING A FIELD

To edit a field, click the field name in the Fields table. In the Edit Field dialog box, make your changes and click Save.

For instance, you may want to edit the Document Type field to add a lookup query, for example,

```
SELECT DISTINCT C_ALIAS AS FieldKey,
CLASSDESCRIPT AS 'Document Type'
FROM MHGROUP.DOCCLASSES
ORDER BY 'Document Type'
```

Note You cannot edit the Document Number field.

DELETING A FIELD

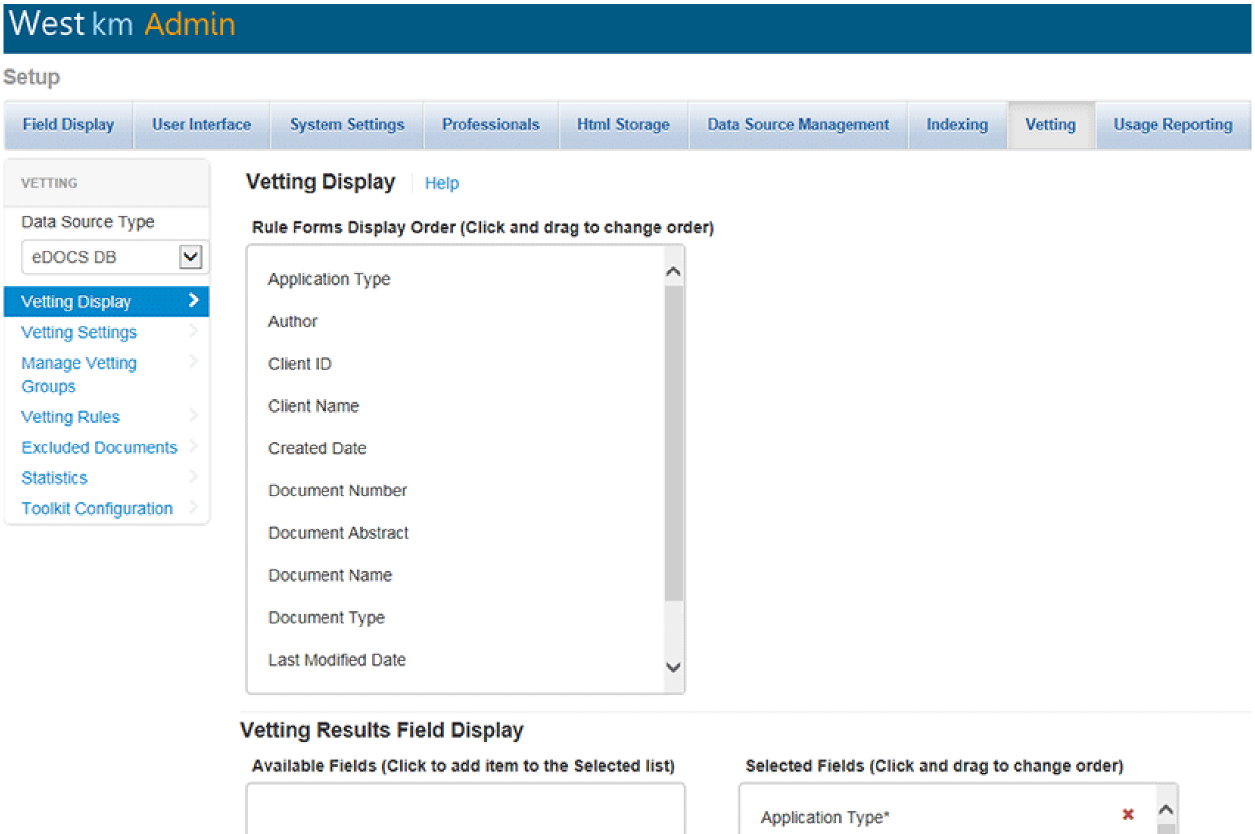
To delete a field, select the check box to the left of the field name in the Fields table and click Remove Selected.

Note You cannot delete default fields and fields being used by a vetting rule.

Setting the Vetting Display

Set how fields are displayed in the vetting toolkit at the Vetting Display page.

To access the Vetting Display page, click **Vetting Display** in the left frame. To change display settings, make your changes and click **Save**.



RULE FORMS DISPLAY ORDER

The order of fields in the Rule Forms Display Order box determines the order of fields on rule forms when adding or editing a vetting rule.

Move a field by dragging it to a new location. (The available fields match the fields you defined on the Toolkit Configuration page.)

VETTING RESULTS FIELD DISPLAY

Available Fields/Selected Fields: Move fields to the Selected Fields box that you want displayed in document result lists on these pages:

- Test Results page
- View Collection page
- Excluded Documents page

To move a field to the Selected Fields box, click it. Fields are displayed in result lists in the order in which you list them in the Selected Fields box. To change the order, drag the field to a new location.

To remove a field from the Selected Fields box, click the X next to the field name.

Note On the Test Results page, all selected fields are displayed. On the View Collection and Excluded Documents pages, the system displays only the selected fields that are included by default on the Toolkit Configuration page. These default fields are marked with an asterisk (*).

- **Display Server Name**: If selected, a column for Server Name is included on the View Collection and Excluded Documents pages.
- **Display Library Name**: If selected, a column for Library Name is included on the View Collection and Excluded Documents pages.

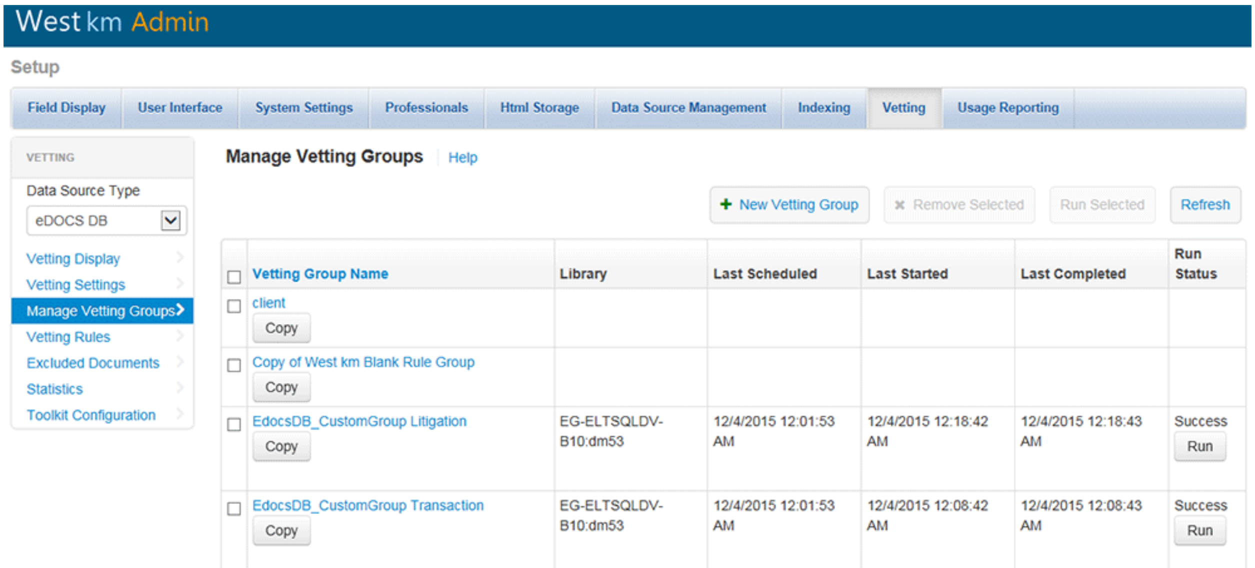
Managing Vetting Groups

On the Manage Vetting Groups page, you can:

- Define vetting groups
- Manually run vetting for selected vetting groups or for a single DMS database/library
- View the status of vetting processes for each vetting group and DMS database/library

Each vetting group generates a collection of documents that you index in West km. One vetting group can be set as a global exclusionary group. This vetting group doesn't generate a collection of documents for indexing; rather it is a central repository of exclusionary rules that can be applied as desired to other vetting groups.

To access the Manage Vetting Groups page, click Manage Vetting Groups in the left frame.



Note For best performance, set up more vetting groups containing fewer documents rather than fewer vetting groups containing more documents.

ADDING A VETTING GROUP

To add a vetting group,

1. In the Data Source Type list, click your document management system.
2. Click New Vetting Group. The New Vetting Group dialog box is displayed.
3. In the Vetting Group Name box, type a name for the vetting group. A name is required.
4. In the Description box, for your reference, type a description of the vetting group.
5. To set this vetting group as the global exclusionary group, select Set As Global Exclusionary Group. This option is available only if no other vetting group is set as global exclusionary.
6. To apply global exclusionary rules to the vetting group, select Include Global Exclusionary Rules.
7. Click Save.

The vetting group is added to the Vetting Groups table. Note that a set of inclusionary vetting rules is automatically added to the group for you. (The new group includes all the inclusionary vetting rules from all the default groups.)

EDITING, COPYING, AND DELETING A VETTING GROUP

To edit a vetting group, click the vetting group name in the Vetting Groups table. In the Edit Vetting Group dialog box, make your changes and click Save.

To copy a vetting group and its rules, click Copy next to the vetting group name. In the Copy Vetting Group dialog box, enter a new name, a description, and the options you want, and then click Save.

To delete a vetting group, select the check box to the left of the vetting group name and click Remove Selected.

Notes:

- You must have at least one vetting group at all times.
- When the vetting status is InProgress or WaitingForWindow for a vetting group, you cannot edit or delete the vetting group or its rules. In addition, the global exclusionary group cannot be edited or deleted when it's applied to a vetting group in this state.
- If you edit, copy, or delete a vetting rule, vetting must run for the changes to take effect.

DEFAULT VETTING GROUPS

The following vetting groups are included in the vetting toolkit by default, but are not set to run automatically:

- West km Litigation: the group's rules are designed to vet litigation documents.
- West km Transactions Docs: the group's rules are designed to vet transactional documents.
- West km Transactions Clauses: the group's rules are designed to vet transactional documents that are appropriate for clause and defined term analysis.
- West km LAE: the group's rules are designed to vet captioned documents that are appropriate for processing by the litigation analysis engine, such as documents that have been filed with the court (e.g., pleadings, probate documents).
- West km Global Exclusions: the group's rules are a central repository of exclusionary rules that are administered in one place and that can be applied as desired to other vetting groups.
- West km Blank Rule Group: the group contains no rules and can be used as a blank template for adding only the rules you want. You can selectively copy rules from other vetting groups or add your own rules.

At your request, your West km representative can work with you to create practice-specific vetting groups. Several sets of exemplary rules have been developed that can be custom tuned to meet your organization's needs. This work can be completed as part of the vetting strategy during installation or as a separate vetting review stage after installation. Practice areas for which rules have been developed include the following:

- Antitrust
- Banking
- Environmental and regulatory
- Finance
- Intellectual property
- Labor
- Real estate
- Tax

For more information about these or other practice-specific vetting groups, please contact your West km representative.

RUNNING VETTING RULES

When vetting rules are run, the vetting database is updated. You can run vetting manually or set it to run on a schedule.

When you run vetting, it adds information about new documents, updates information about existing documents, and removes information about deleted documents and documents no longer part of the vetted collection. It also adds information about new documents that result from adding, modifying, or deleting a rule.

Vetting runs as follows:

- Vetting is run by vetting group (i.e., by collection). Inclusionary rules are processed first, followed by exclusionary rules. If global exclusionary rules are applied, they are run after the group's specific inclusionary and exclusionary rules. For more information, see "Vetting Rules Example" on page 67.
- For both manual and scheduled launches, vetting runs only within the vetting window that is defined for the vetting group on the Indexing Server Setup page. By default, a 24-hour vetting window is defined. For details, see the following section "Scheduling Vetting for a Vetting Group."
- Vetting can run while end users are accessing West km.

Manually Running Vetting for Vetting Groups

You can manually run vetting rules for selected vetting groups. In the Vetting Groups table on the Manage Vetting Groups page, select the check box to the left of each vetting group whose rules you want to run and click Run Selected.

When you confirm the request, vetting begins in accordance with the vetting windows (the time and type of vetting process) that are set up for the vetting group on the Indexing Server Setup page.

Manually Running Vetting Rules by Database/Library

You can manually run vetting rules for a particular DMS database/library in a vetting group. In the Run Status column in the Vetting Groups table, **click** Run next to the DMS database/library in which you want vetting rules to run.

Vetting begins in accordance with the vetting windows (the time and type of vetting process) that are set up for the vetting group on the Indexing Server Setup page.

Scheduling Vetting for a Vetting Group

To set a schedule to automatically run the rules for a vetting group, define a vetting scheduling window on the Indexing Server Setup page. When both a vetting scheduling window and a vetting window for the vetting group are open, vetting groups will be scheduled for vetting. To create separate schedules for different sets of vetting groups, define multiple vetting windows. For details, see "Setting Up the Indexing Server" on page 43.

When you set up automatic vetting, it is recommended that you set the vetting scheduling window to a 24-hour open window (e.g., 12:00:00 AM–12:00:00 AM) and the vetting windows outside regular business hours. For more information about scheduling vetting, see "Routine Indexing Maintenance" on page 50.

VIEWING THE STATUS OF VETTING

The Run Status column in the Vetting Groups table displays the status for each vetting group. Each DMS database/library is listed.

Job status indicators for the vetting process are listed in the following table:

Job Status	Description
Scheduled	Vetting rules are scheduled to run
InProgress	Vetting rules are currently running
WaitingForWindow	The vetting process has stopped at the close of the vetting window and is waiting for the window to reopen
Success	The vetting process has completed successfully
Error	An error occurred during the vetting process

Note When the vetting status is InProgress or WaitingForWindow for a vetting group, you cannot edit or delete the group or the vetting rules for the group.

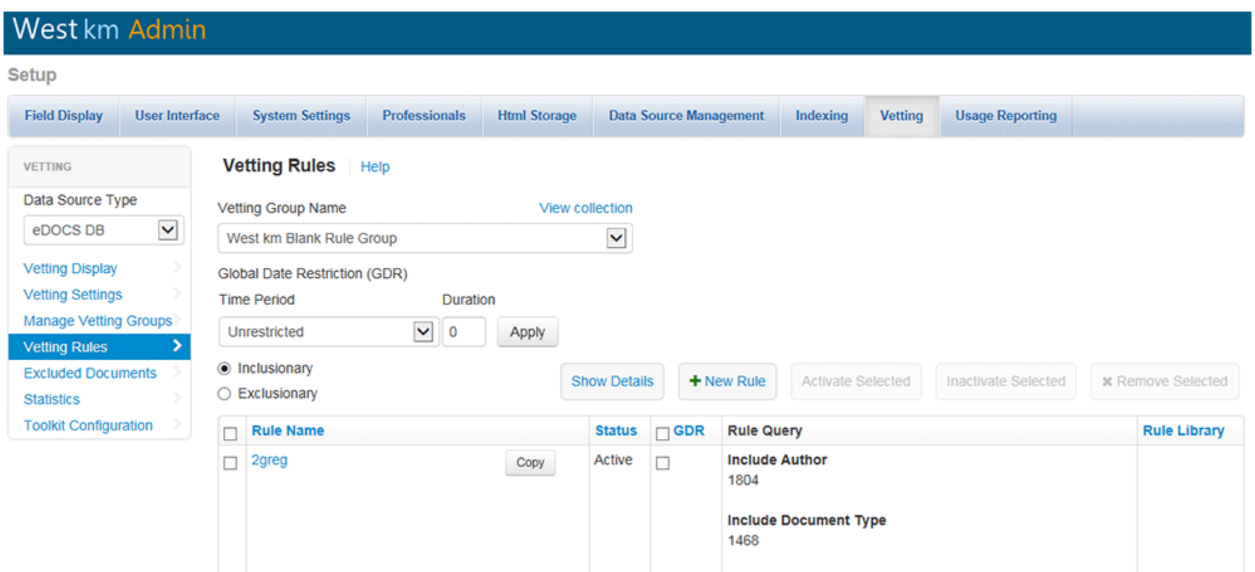
To update the status indicators while the vetting process is running, click **Refresh**. (The page is not refreshed automatically.)

Administering Vetting Rules

Administer inclusionary and exclusionary rules for a vetting group at the Vetting Rules page. Vetting rules determine which documents will be included and which will be excluded from a document collection.

When a vetting group is created, a set of inclusionary vetting rules is automatically added to the group for you. (The new group includes all the inclusionary vetting rules from all the default groups). You can edit or remove these vetting rules and add more.

To access the Vetting Rules page, click **Vetting Rules** in the left frame.



To administer vetting rules for a vetting group,

1. In the Data Source Type list, click your document management system.
2. In the Vetting Group Name list, click the vetting group you want to administer.
3. To view inclusionary rules for the vetting group, select Inclusionary Rules. To view exclusionary rules for the vetting group, select Exclusionary Rules.
4. Rules are listed alphabetically by name. The Rule Query column in the Vetting Rules table lists the fields used by the rule.
5. To print the displayed vetting rules, click the Print icon.
6. Perform the actions you want. For details, see the following subsections.

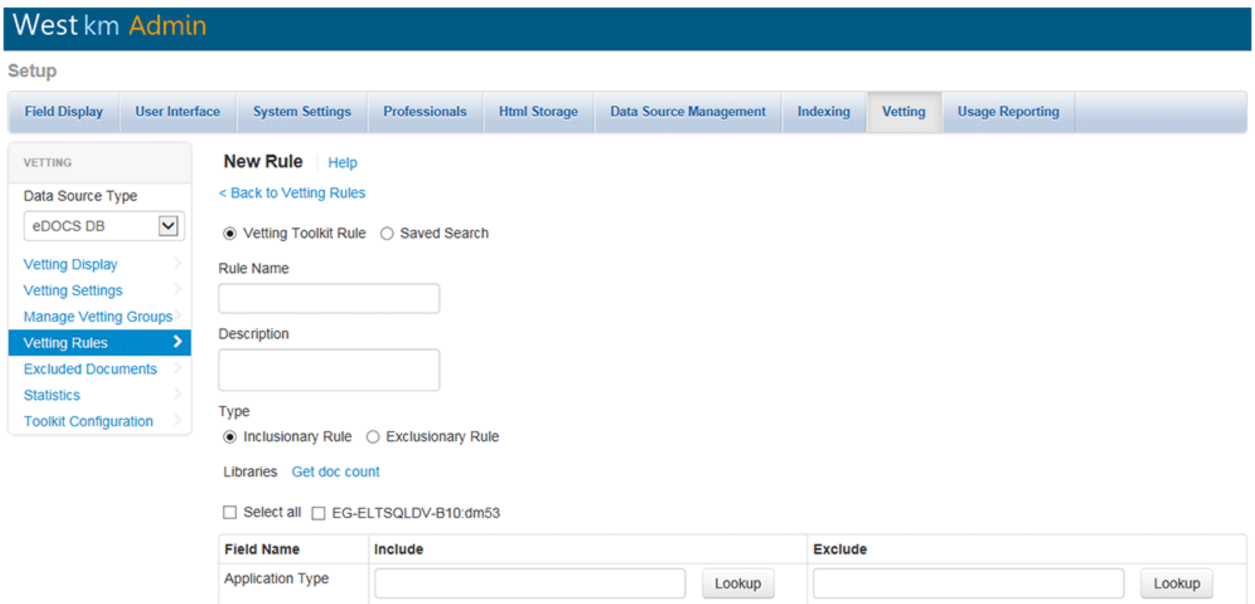
ADDING AND EDITING RULES

Vetting rules are associated with a vetting group. Inclusionary rules define which documents should be included in a collection, and exclusionary rules define which documents should be excluded from a collection.

To add or edit a vetting rule in a vetting group,

1. Do one of the following:
   - Click New Rule at the Vetting Rules page to add a rule.
   - Click the rule name at the Vetting Rules page to edit a rule.

The New Rule page or Edit Rule page is displayed.



2. In the Vetting Group Name box, select the vetting group to which you want to add the vetting rule.

Note When editing a vetting rule, you cannot change its vetting group.

3. Select the rule type you want:
   - Vetting Toolkit Rule: Select this option if you want to create a new rule that is not already a saved search in your document management system.
   - Saved Search: Select this option if you want to use a saved search in your document management system as a rule.
4. In the Rule Name box, type a name for the rule.
5. In the Description box, type a description of the rule for your reference.
6. If you are using a DMS saved search as a rule in the vetting toolkit, in the Saved Search Name box, type the name of the saved search.
7. Select whether you want to create an inclusionary rule or an exclusionary rule.
8. In the Libraries section, select the databases/libraries that you want your field criteria or saved search to run against. The databases/libraries for which you've created a data source connection are listed.
9. To see how many documents that are retrieved by your rule, select the databases/libraries you want to check and click Get doc count. As you modify the rule, you can click this option again to get updated results.

10. If you are creating a new vetting toolkit rule (not using a saved search), enter the field criteria you want. The fields, look-up functions, and search controls available to you are dependent on the fields you defined at the Toolkit Configuration page (see "Configuring Vetting Fields" on page 57 for more information).

To enter multiple values within a field, separate the values with a comma. If available, you can also click **Lookup**, select the check boxes next to the values you want, and click **Save**.

Search methods for field types in a vetting rule:

Field Type	Search Method
Text	Contains, equals, starts with, or ends with the text you type, depending on the search type you selected when you added the field (see "Adding a Field" on page 58 for more information). For information about available connectors, see the following subsection, "Using Connectors in Text Fields."
Date	Exactly matches the date you type. Enter dates in `MM/DD/YYYY` format.
Numeric	Exactly matches the number(s) or is within the range you type. The following value types are allowed: single number (`1`) multiple numbers (`1,3,5,7`) range of numbers (`1-7`) combination (`1,3,5-7`)

For more information about vetting rules, see "Vetting Rules Example" on page 67.

11. To test the rule, click **Test Rule**. For more information, see "Testing Rules" on page 67.
12. To print the rule, click the **Print** icon.
13. To save the rule, click **Save**.

Notes:

- When the vetting status is InProgress or WaitingForWindow for a vetting group, you cannot edit vetting rules for the group or the group itself. For more information about vetting status, see "Viewing the Status of Vetting" on page 63.
- When you add or edit a vetting rule, vetting must run for the changes to take effect.

Using Connectors in Text Fields

When entering search criteria in a text field for a vetting rule, you can use the connectors listed in the following table.

Connectors for text fields in a vetting rule:

Connector	Description
&&	a double ampersand is an AND operator, where the document must contain both terms
,	a comma is an OR operator, where the document must contain either term or both terms
" "	a quotation mark that surrounds text designates an exact phrase, where the document must contain the terms in the same order as in the quotation marks

Notes:

- Wildcard characters are not allowed.
- Values are case-insensitive.
- Spaces are considered literally, except when preceding or succeeding an exact phrase in quotation marks (in which case they are ignored).

Example:

Document Name Includes:

`pacific&&gas&&electric,"pg & e",pg&e`

Document Titles Retrieved	Document Titles Not Retrieved
pacific gas & electric	pacific electric
pacific gas and electric	pg and e
pacific electrical gas company	
pg & e	
pg&e	

INACTIVATING, ACTIVATING, AND REMOVING RULES

To inactivate one or more vetting rules so that they don't run for the selected vetting group, select the check box to the left of each vetting rule you want to inactivate in the Vetting Rules table and click Inactivate Selected. By default, all rules are active.

To activate one or more rules for the selected vetting group, select the check box to the left of each vetting rule you want to activate in the Vetting Rules table and click Activate Selected.

To remove one or more rules from the selected vetting group, select the check box to the left of each vetting rule you want to remove in the Vetting Rules table and click Remove Selected.

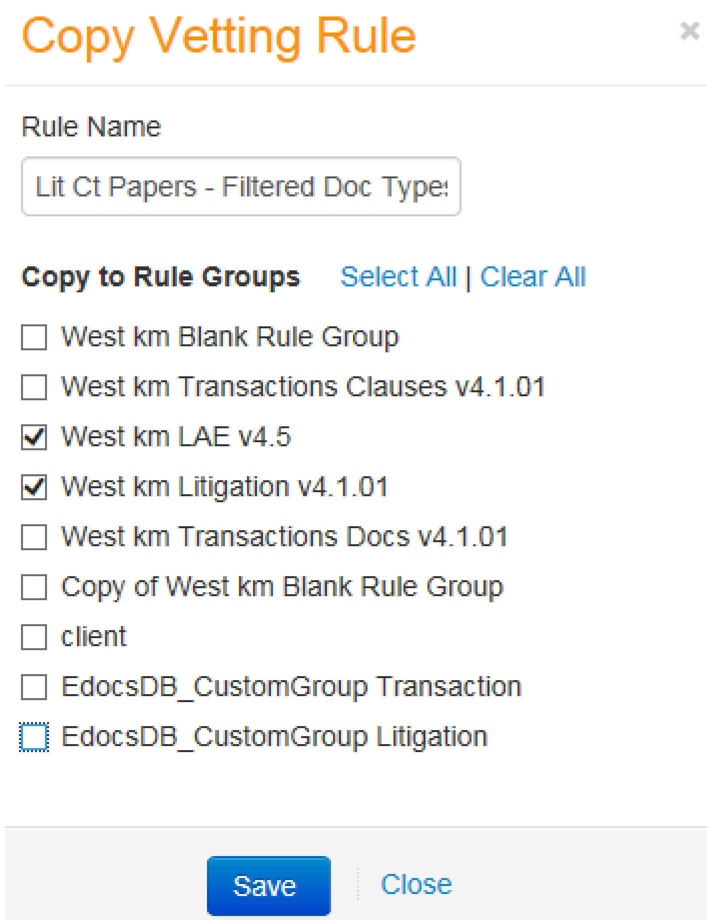
Notes:

- When the vetting status is InProgress or WaitingForWindow for a vetting group, you cannot remove vetting rules for the group or remove the group itself. For more information, see "Viewing the Status of Vetting" on page 63.
- When you remove a vetting rule, vetting must run for the change to take effect.

COPYING A VETTING RULE

To copy a vetting rule to one or more vetting groups (within the same data source type),

1. Click Copy next to the rule name in the Vetting Rules table. The Copy Vetting Rule dialog box is displayed.



1. If you want to change the name of the rule when it is copied, in the Rule Name box, type a new name for the rule.
2. Select the vetting groups to which you want to copy the rule.
3. Click Save.

The rule is copied to all the vetting groups you selected and is automatically set to active.

Note Inclusionary rules are not copied to the vetting group that is set as global exclusionary.

APPLYING A DATE RESTRICTION TO RULES

To apply a date restriction to one or more vetting rules, do the following:

- In the Global Date Restriction (GDR) section, select the time period and type the duration you want and then click Set to record the restriction in the system.
- Select the GDR check box next to each rule in the Vetting Rules table that you want to restrict.

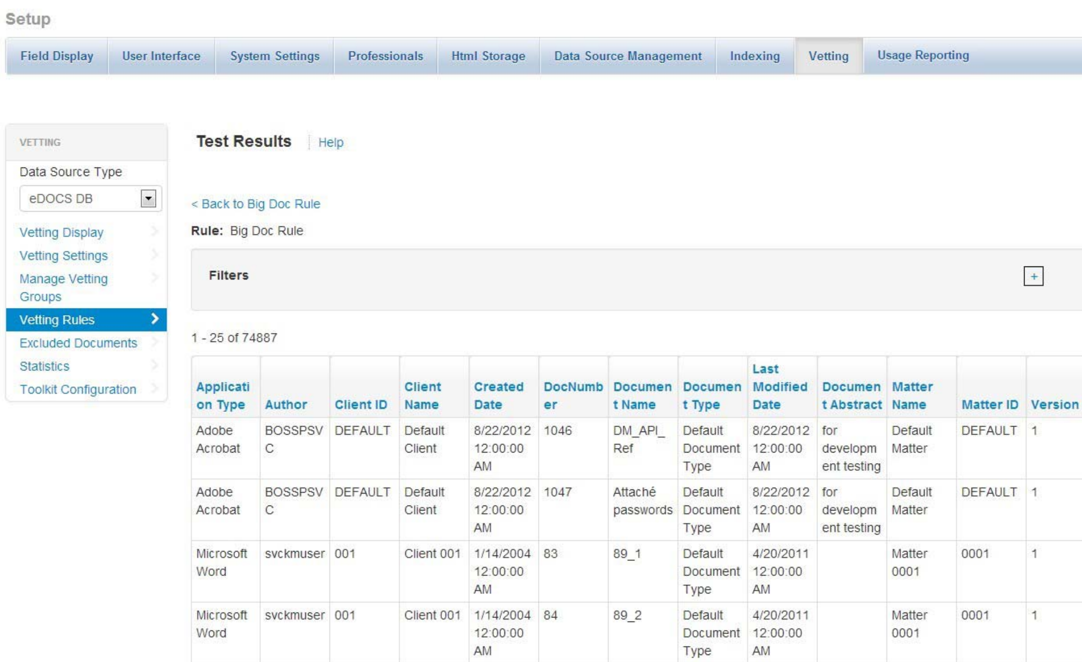
When rules are run, the recorded restriction is compared to the Last Modified Date field in the document management system and is applied to all the selected rules. Date restrictions that are defined within an individual rule also remain in effect.

TESTING RULES

You can test a vetting rule to see which documents it retrieves. When you test a rule, results are returned for one DMS database/library at a time at the Test Results page. By default, up to 1,000,000 are retrieved.

To access the Test Results page:

- Click Test next to a rule at the Vetting Rules page; or
- Click Test Rule at the New Rule or Edit Rule page.



Application Type	Author	Client ID	Client Name	Created Date	DocNumber	Document Name	Document Type	Last Modified Date	Document Abstract	Matter Name	Matter ID	Version
Adobe Acrobat	BOSSPSVC	DEFAULT	Default Client	8/22/2012 12:00:00 AM	1046	DM_API_Ref	Default Document Type	8/22/2012 12:00:00 AM	for development testing	Default Matter	DEFAULT	1
Adobe Acrobat	BOSSPSVC	DEFAULT	Default Client	8/22/2012 12:00:00 AM	1047	Attaché passwords	Default Document Type	8/22/2012 12:00:00 AM	for development testing	Default Matter	DEFAULT	1
Microsoft Word	svckmuser	001	Client 001	1/14/2004 12:00:00 AM	83	89_1	Default Document Type	4/20/2011 12:00:00 AM		Matter 0001	0001	1
Microsoft Word	svckmuser	001	Client 001	1/14/2004 12:00:00 AM	84	89_2	Default Document Type	4/20/2011 12:00:00 AM		Matter 0001	0001	1

You can perform the following actions at the Test Results page:

- To access the next or previous set of documents, click a page link or type a page number at the bottom of the Test Results table.
- To view retrieved documents for the rule from a different DMS database/library, from the Library list, select a DMS database/library.
- To change the sort order of the retrieved documents, click a column heading (e.g., Last Modified Date) to sort by that category.
- To view a copy of a document in its original format, click the document name.
- To filter the test results, click Add Filter, type your criteria in the text boxes, and click Apply. For more information, see "Filtering a Result List" on page 70.
- To print the displayed test results, click the Print icon.
- To return to the rule page (e.g., Vetting Rules, New Rule, or Edit Rule page), click Back to Rule.

VETTING RULES EXAMPLE

In a vetting group, inclusionary rules are processed first, followed by exclusionary rules. If global exclusionary rules are applied, they are run after the group’s specific inclusionary and exclusionary rules.

For example, consider a vetting group with the following inclusionary and exclusionary rules:

Vetting Group Inclusionary Rule

Document Name Includes: agreement,brief,pleading
Document Name Should Not Include: draft

Vetting Group Exclusionary Rule

Document Name Should Not Include: keep
Last Doc Modified Date Less Than or Equal To: 12/31/1999

Global Exclusionary Rule

Document Name Includes: old
Last Doc Modified Date Less Than or Equal To: 12/31/2005

These rules would result in documents 1, 5, and 9 from the following table:

Included?	Number	Document Name	Last Modified Date
yes	1	employment_agreement.doc	1/1/2002
no	2	joint_venture_draft_keep.doc	10/10/1998
no	3	real_estate_partnership_draft.doc	5/5/1995
no	4	trial_brief_draft.doc	6/6/2001
yes	5	pleading_keep.doc	7/7/1997
no	6	loan_agreement.doc	8/8/1995
no	7	fax_cover_sheet.doc	2/2/2004
no	8	employment_agreement_old.doc	10/8/2001
yes	9	loan_agreement_old.doc	7/8/2006

After the vetting group's inclusionary rule is processed, documents 1, 5, 6, 8, and 9 are included because their names contain *agreement*, *brief*, or *pleading*. Documents 2, 3, and 7 are not included because their names don't contain *agreement*, *brief*, or *pleading*. Even though document 4 contains brief in its name, it's not included because its name also contains *draft*.

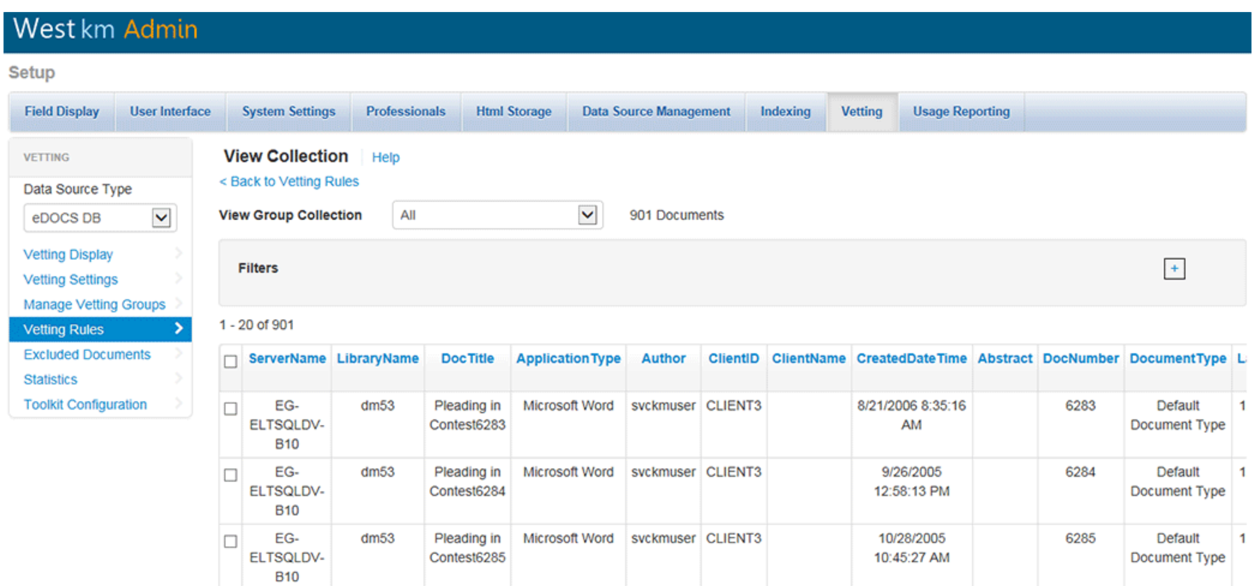
After the vetting group's exclusionary rule is processed, document 6 is excluded because its last modified date is on or before 12/31/1999. Even though the last modified date of document 5 is also on or before 12/31/1999, it's retained because its name contains *keep*.

After the global exclusionary rule is processed, document 8 is excluded because its name contains *old* and its last modified date is on or before 12/31/2005. Even though the name of document 9 contains *old*, it's retained because its last modified date is after 12/31/2005.

VIEWING COLLECTIONS

View all the documents in a collection at the View Collection page. The rules in the vetting group determine the documents in the collection.

To access the View Collection page, click **View Collection** at the Vetting Rules page.



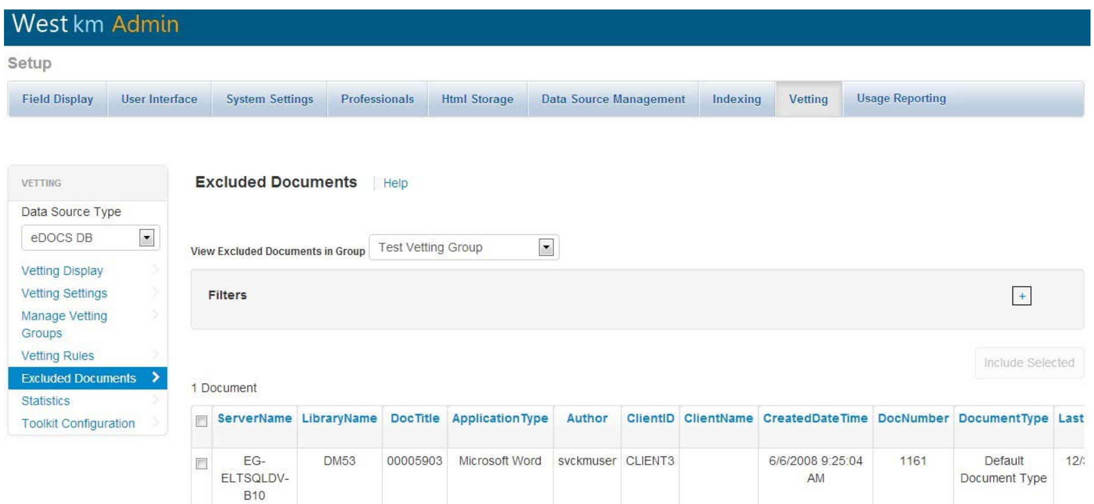
To view documents in a collection,

1. In the **Data Source Type** list, click your document management system.
2. In the **View Group Collection** list, click the vetting group for which you want to view the document collection. The list is determined by the groups you set up on the Manage Vetting Groups page (see "Managing Vetting Groups" on page 61 for more information).
3. Perform any of the following actions:
   - To access the next or previous set of documents, click a page link or type a page number at the bottom of the View Collection table.
   - To change the sort order of the retrieved documents, click a column heading (e.g., Author) to sort by that category.
   - To exclude a document from the collection, select the check box next to the document listing. To select all items in the result list (including items on other pages), select the check box in the heading. Then click **Exclude Selected**.
   - To view a copy of a document in its original format, click the document name.
   - To see the complete listing of inclusionary rules that brought a document into the vetting collection, in the Group Rule column in the View Collection table, click **More**.
   - To filter the list of vetted documents, click **Add Filter**, type your criteria in the text boxes, and click **Apply**. For more information, see "Filtering a Result List" on page 70.
   - To print the displayed document listing, click the **Print** icon.

The toolkit automatically retrieves the highest version of a document. Also, if a document exists in more than one collection, West km will handle the duplicates during the indexing process.

Viewing Excluded Documents

View the documents that have been manually excluded from a collection at the Excluded Documents page. To access the Excluded Documents page, click **Excluded Documents** in the left frame.

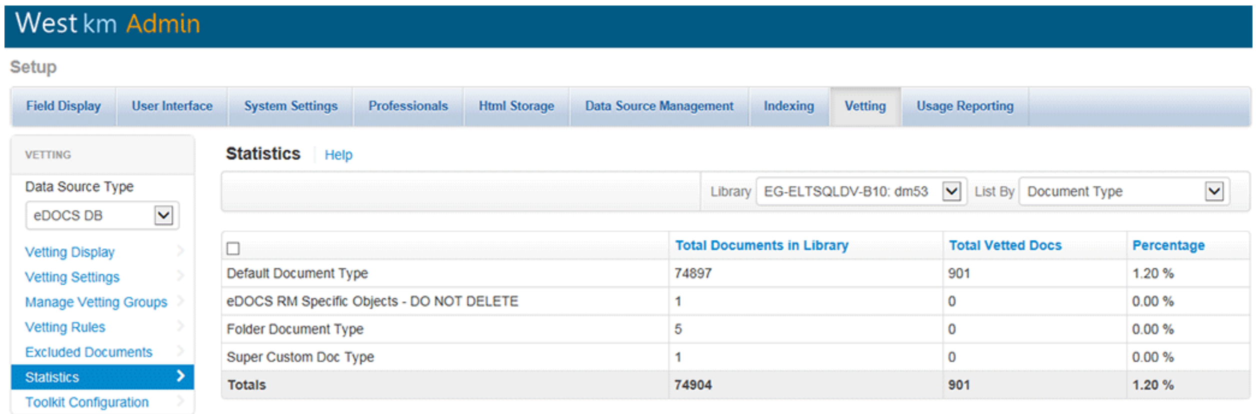


To view excluded documents in a collection,

1. In the **Data Source Type** list, click your document management system.
2. From the **View Group Collection** list, select the vetting group for which you want to view the documents that you have manually marked for exclusion (see "Adding and Editing Rules" on page 64 for more information). The list is determined by the groups you set up on the Manage Vetting Groups page (see "Managing Vetting Groups" on page 61 for more information).
3. Perform any of the following actions:
   - To access the next or previous set of documents, click a page link.
   - To change the sort order of the excluded documents, click a column heading (e.g., Author) to sort by that category.
   - To restore an excluded document to the collection, first select the check box next to the document listing. To select all items in the list (including items on other pages), select the check box in the heading. Then click **Include Selected**.
   - To view a copy of a document in its original format, click the document name.
   - To filter the list of excluded documents, click **Add Filter**, type your criteria in the text boxes, and click **Apply**. For more information, see "Filtering a Result List" on page 70.
   - To print the displayed document listing, click the **Print** icon.

Viewing Statistics

Compare the number of vetted documents to the total number of documents in your DMS database/ library at the Statistics page. To access the Statistics page, click **Statistics** in the left frame.



To view statistics,

1. In the **Data Source Type** list, click your document management system.
2. In the **Library** list, click the DMS database/library for which you want to view statistics.
3. In the **List By** list, click a display category. You can group statistics by any field for which a DMS description field map is defined (see "Configuring Vetting Fields" on page 57 for more information).

Statistics are listed in alphabetical order for the category you selected.

- **Total Documents in Library** indicates the number of documents available in the DMS database/ library that could be included by the vetting toolkit.
- **Total Vetted Docs** indicates the number of documents in the DMS database/library currently set for inclusion by the vetting toolkit (for all vetting groups).
- **Percentage** indicates the percentage of included documents in the DMS database/library out of the available documents in the library.

To change the order of the statistics, click a column heading (e.g., Percentage) to sort by that category. To print the displayed statistics, click the **Print** icon.

Filtering a Result List

You can filter a result list to restrict the listed documents at the following pages in the vetting toolkit:

- Test Results
- View Collection
- Excluded Documents

To filter a result list,

1. Click the plus sign to expand the filters panel at the top of the result list.
2. Enter the field criteria you want to use to filter the result list. Field types are filtered as indicated in the following table.

Field Type	Filter Method
text	contains the text you type
date	is greater than or equal to the date you type; enter dates in MM/DD/YYYY format
numeric	exactly matches the number(s) or is within the range you type; the following value types are allowed: • single number (1) • multiple number (1,3,5,7) • range of numbers (1-7) • combination (1,3,5-7)

Wildcard characters are not allowed. Values are case-insensitive.

3. Click **Apply**. The documents that match your criteria are displayed in the listing. To cancel the filter and return to the original result list, click **Clear**.

7 Indexing Documents

Index documents in West km by setting up and indexing document collections, synchronizing indexed documents with your file system and document management system (DMS), and creating and updating full-text indexes.

Adding Document Collections

Add document collections and index them on the Manage Collections page.

Note You must add connections for the data sources and libraries that contain your documents before you add a document collection (see "Adding Data Source Connections" on page 39 for more information). If you are using the West km Vetting Toolkit, you must vet the document collection before you add it on the Manage Collections page (see "Vetting Documents" on page 54 for more information).

To access the Manage Collections page,

1. Access the West km interface.
2. Click **Setup**.
3. Click the **Indexing** tab.

A list of your indexed document collections is displayed.

To add a new document collection,

1. At the Manage Collections page, click **New Collection**.
2. Make your selections for the document collection. For details on selecting options when adding a document collection, see the subsections below.
3. Click **Save**.
4. If a document scheduling window and a document indexing windows are open, within five minutes the collection is scheduled and a Next Run date appears in the Scheduling column.

If a collection hasn't been scheduled (i.e., no Next Run date appears in the Scheduling column), click the name of the server under **Server Information** in the left frame to access the Indexing Server Setup page and the indexing service windows where collections are scheduled.

Indexing service windows set the schedule for automatic indexing to occur. For more information, see "Indexing Service Windows" on page 43.

GENERAL INFORMATION

In the General Information section on the Add Collection page, you define the location of documents and general collection information. Depending on how the documents are managed - a document management system or the NT file system - the information needed is slightly different.

DMS Sources

1. From the **Server** list, select the server or location containing the DMS documents you want to index.
2. From the **Library** list, select the library or database containing the document collection.
3. If you have the West km Vetting Toolkit (and the toolkit supports your document management system), select an option:
   - **Saved Search**: the document collection is defined by a DMS saved search.
   - **Vetting Group**: the document collection is defined by a vetting group in the West km Vetting Toolkit.
4. Select the document collection you want to index from the list box (e.g., folders, quick searches, vetting groups).
5. To customize the collection name, in the **Collection Name** box, type the name you want. This name will be listed on the Manage Collections page. (If you don't enter a name, the saved search, vetting group, or NTFS path you selected as the source of documents will be used as the collection name, along with the server and library.)
6. To add a description for the collection, in the **Collection Description** box, type the description you want. This description is displayed when you hover over the collection's name on the Manage Collections page.

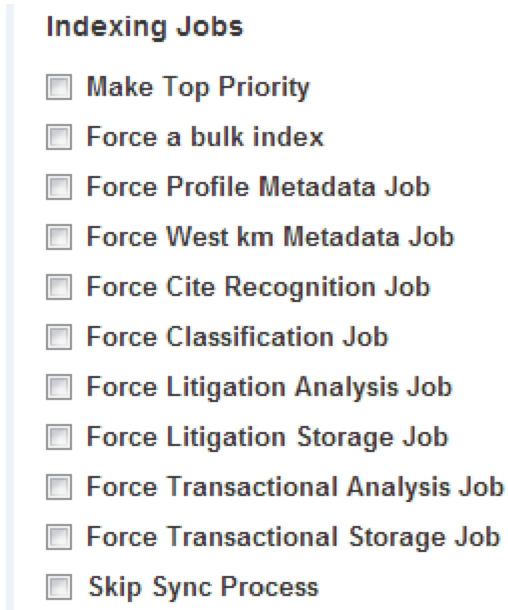
File System Sources

1. From the **Server** list, select the server containing the documents you want to index.
2. From the **Library** list, select the location on the server that contains the documents.
3. In the **Location** box, enter the path to the folder whose documents you want to index as a collection. Enter the server and share using a UNC path (\\server\share\)—not a mapped drive. You can either type the path or navigate to the folder in the list box below.

4. If you want all subfolders at the location to be indexed as part of this collection, select the Include documents within subfolders check box.
5. To customize the collection name, in the Collection Name box, type the name you want. This name will be listed on the Manage Collections page. (If you don't indicate a name, the NTFS path you selected as the source of documents will be used as the collection name, along with the server and library.)
6. To add a description for the collection, in the Collection Description box, type the description you want. This description is displayed when you hover over the collection's name on the Manage Collections page.

INDEXING JOBS

In the Indexing Jobs section on the Add Collection page, you select indexing job options for the collection.



1. To give this collection priority over other collections being indexed at the same time, select the Make Top Priority check box. If multiple collections are marked top priority, then priority is given to the oldest collection, based on the date it was last indexed.
2. To completely re-index this collection the next time an incremental update occurs, select the Force a Bulk Index check box. This option is useful if you want to fully re-index collections on a staggered schedule.

Note This option clears automatically after the bulk indexing occurs.

3. To force one or more indexing components to process all documents in the collection the next time an incremental update occurs (instead of just processing the new or modified documents), select the Force check boxes for the appropriate indexing components.

For example, selecting the Force Cite Recognition Job check box could be useful if you receive a new version of RID and would like to index citation information for the entire collection. Similarly, the Force West km Metadata Job check box could be useful if you've changed the library group for your collection and you want to update it and all other West km–related metadata for the collection, but you do not want to update all DMS-related metadata for the collection.

Note After the next incremental update occurs, selected options clear automatically.

4. To prevent the synchronization process from running on the collection, select the Skip Sync Process check box. If you select this option, documents in the collection will not be removed from West km, even if they have been deleted from your organization's file system or are no longer part of the defined document collection.

LIBRARY GROUPS

When adding or editing a document collection, you can select a library group if you want the collection to have a library group different from the library group for the data source containing the collection.

Library groups allow your West km members to restrict searches of your internal documents by groupings (e.g., office locations or practice categories).

To select an existing library group for a document collection, in the Library Group list, select the library group name.

To define a new library group for a document collection,

1. In the Library Group list, click New.

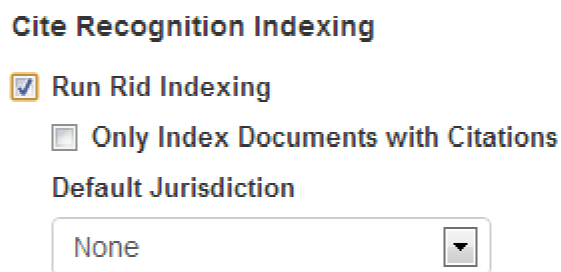
2. In the Library Group Name box, type a name for the library group.

You can manage library groups at Setup, User Interface, Library Group, Current Library Groups. As well as adding library groups, you can edit and delete library groups at that location. For more information, see "Adding Data Source Connections" on page 39.

Note Changes to a document collection's library group will not be reflected in full-text searches until you re-index the document collection (incremental or bulk) and update full-text indexes. New library groups will not appear in the end-user interface for any currently running West km sessions until the user closes and re-opens the Web browser.

CITATION RECOGNITION INDEXING

In the Cite Recognition Indexing section on the Add Collection page, you set options for how the cite recognition component runs for the collection.



1. To run the cite recognition component and index the citation information within documents, select the Run RID Indexing check box. (If you clear this selection, only the text of documents, not citation information, will be indexed.)
2. To index only documents that contain one or more citations, select the Only Index Documents with Citations check box.
3. In the Default Jurisdiction list, select a default jurisdiction for this document collection. You can select from the following options:
   - None: No default jurisdiction is used. Citations are not linked if they are missing jurisdictional information or contain publications valid in multiple jurisdictions.
   - All: RID performs additional processing to identify citations that contain publications valid in multiple jurisdictions. RID checks the publication in each valid jurisdiction. If only one jurisdiction is identified with high confidence, the citation is linked to that jurisdiction. If more than one jurisdiction (or no jurisdiction) is identified with high confidence, the citation is not linked.

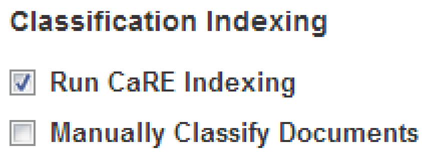
     For example, the publication name PS is valid in Pennsylvania (Pennsylvania statutes, e.g., 20 P.S. s. 908) and Maryland (public safety code, e.g., P.S. s. 3-101). With the All option selected, RID

     Note Using the All option may increase the time required for indexing.
   - A state abbreviation: A default jurisdiction is used to identify citations that are missing jurisdictional information or that contain publications valid in multiple jurisdictions. RID can often use the state in which the referenced document was created to uniquely identify citations when a citation is generic or several publications share the same publication name.

     For example, if a document refers to Code section 100, the publication name Code is generic. A state must be specified to identify the statute being referenced. If a document refers to IC sec 100, the publication name IC is used for both Idaho and Indiana statutes. Idaho or Indiana must be specified to identify which statute set is being referenced.

CLASSIFICATION INDEXING

In the Classification Indexing section on the Add Collection page, you select the options for assigning documents in the collection to KeySearch legal topics. (If you disabled CaRE during the installation process, classification options are not available.)



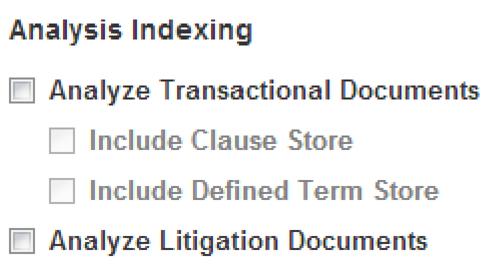
- To automatically assign documents to KeySearch topics, select the Run CaRE Indexing check box. (If you bypass RID indexing, CaRE classification results may not be as accurate.)
- To assign all documents to a selected list of KeySearch topics, select the Manually Classify Documents check box. Click Add Topics, select the topics you want, and click Add. To remove a topic from the list, click the X next to the topic name. To remove all topics, click Remove All.

Note To assign documents to a custom KeySearch topic, you must first create the topic. For more information, see "Adding a KeySearch Topic" on page 47.

- By default, CaRE only assigns documents with at least one case law citation. Note that CaRE may be less accurate at categorizing documents without citations.

ANALYSIS INDEXING

In the Analysis Indexing section on the Add Collection page, you can set options for how litigation and transactional documents are analyzed.



1. To run the transactional analysis component (i.e., the document analyzer) and mine document data for West km for Transactions, select the Analyze Transactional Documents check box.
   - If the transactional analysis component processes the collection (i.e., the Analyze Transactional Documents check box is selected), documents in the collection can be retrieved from the WestlawNext interface and both the Litigation and Transactions categories in the West km interface.
   - If the transactional analysis component does not process the collection (i.e., the Analyze Transactional Documents check box is cleared), documents in the collection can be retrieved from the WestlawNext interface and the Litigation category in the West km interface—but not from the Transactions category in the West km interface.
2. To create indexing collections for clauses or defined terms for this document collection, select the Include Clause Store check box or the Include Defined Term Store check box.

Note Even if you do not create clause or defined term indexing collections, West km members can still search by clause or defined term when searching for Transactions documents using the Advanced Search page.

3. To run the litigation analysis component (i.e., analyzer component) and mine document data for West km for Litigation, select the Analyze Litigation Documents check box.

Note Documents that are converted to HTML and that are configured to be processed by the document analyzer are always made available for searching by full text or by DMS and West km field restrictions, even if document analysis metadata is not available. For example, metadata might not be available because of partial processing, an error, or an unsupported document type. Note that for these documents, analysis metadata is not searchable nor displayed in the result.

Managing Document Collections

FILTERING THE LIST OF DOCUMENT COLLECTIONS

To filter the list of document collections, type or select values at the top of the Manage Collections page and click Apply.

- In the Data Sources and Library Groups lists, select the values you want.
- In the Filter box, type a search string. Document collections that contain the search string in the collection name, data source name, or library group name are found. To display all document collections, click Clear.

EDITING DOCUMENT COLLECTIONS

To edit a single document collection, click the collection name on the Manage Collections page. Then edit the values and click Save. If you cannot click in a text box or select a value, the field cannot be edited.

Changes will be processed during the next indexing of the collection.

Note If CaRE has classified documents in a collection and you then edit the collection by clearing the Run RID Indexing check box (when this check box was formerly selected), CaRE will reclassify all the documents in the collection, and the classification results may not be as accurate.

To edit the indexing job options for multiple collections at once, select the check boxes to the left of each collection that you want to edit on the Manage Collections page. Then click the Actions list and select the indexing job option that you want to apply.

- The Priority option sets the Make Top Priority check box for the collection so that the collection receives indexing priority over other collections.
- The indexing job options (i.e., Profile Metadata, Cite Recognition, Classification, Litigation Analysis, Litigation Storage, Transactional Analysis, Transactional Storage) set the corresponding component check box for the collection so that the component processes all documents in the collection the next time an incremental update occurs (instead of just processing the new or modified documents).
- The Clear Forced Jobs option clears the check boxes for all the indexing job options for the collection.

To remove an indexing job option for a single collection, in the Scheduling column, click the X next to the Forced Jobs option that you want to remove.

REMOVING DOCUMENT COLLECTIONS

To permanently remove one or more document collections,

1. On the Manage Collections page, select the check box to the left of each collection you want to remove.
2. Click Remove Selected.

If you remove a document collection that has already been indexed, it will prevent the collection from being re-indexed. However, note the following:

- The documents as they were last indexed are available to members until the document collection is synchronized (see "Synchronizing Document Collections" on page 78 for more information).
- The documents are represented in full-text indexes until full-text indexes are updated (see "Full-Text Indexing" on page 79 for more information).
- Documents that are duplicated in other collections are not removed.

Indexing Document Collections

Once you add a document collection, you need to index its documents. You can do this by scheduling automatic incremental updates or by manually launching indexing. You can also suspend indexing.

Note If the document collection is defined by a vetting group in the West km Vetting Toolkit, the initial run of the vetting rules must occur before indexing. For more information, see "Running Vetting Rules" on page 62.

SCHEDULING INDEXING

To set a schedule to automatically run incremental updates for a document collection, define a document scheduling window on the Indexing Server Setup page. When both a document scheduling window and a document indexing window for a document collection are open, scheduling occurs. To create separate schedules for specific data source connections or document collections, define multiple document indexing windows. For more information, see "Indexing Service Windows" on page 43.

When you set up automatic indexing, it is recommended that you set the document scheduling window to a 24-hour open window (e.g., 12:00:00 AM–12:00:00 AM) and the indexing windows outside regular business hours. For more information about scheduling indexing, see "Routine Indexing Maintenance" on page 50.

MANUALLY LAUNCHING BULK OR INCREMENTAL INDEXING

When you manually launch indexing, you can do any of the following:

- bulk index newly added document collections
- bulk index (i.e., fully re-index) previously indexed collections
- incrementally update previously indexed collections

To manually launch indexing for one or more document collections,

1. If desired, configure indexing to meet the specific needs of your organization. For more information, see "Configuring Indexing" on page 39.
2. Make sure a document indexing window is defined for the document collection you want to index (see "Indexing Service Windows" on page 43 for more information).
3. On the Manage Collections page, select the check box to the left of each collection that you want to index.
4. Click the Actions list and then click one of the following:
   - Start Incremental Job: Update the index for a previously indexed collection. During an incremental update, documents in the collection are indexed if they are new or modified and they have a date and time after the collection was last indexed.
   - Start Bulk Job: Index a newly defined collection or fully re-index a previously indexed collection. During a bulk index, all documents in the collection are indexed.

     Note When bulk indexing, consider using the Suspend and Process by Component options on the Indexing Server Setup page to control how and when indexing components are processed (see "Indexing Components" on page 45 for more information).

The indexing job is scheduled immediately, and indexing will start according to the collection’s document indexing window.

To monitor indexing progress, click Indexing Results in the left frame. For more information, see "Monitoring Indexing" on page 91. Once indexing has occurred on a document collection, from the Indexing Results page you can manually launch indexing of selected documents.

Note During bulk indexing and incremental updates, full-text indexes are not created or updated. For information on updating full-text indexes, see "Full-Text Indexing" on page 79.

INDEXING DOCUMENTS WITH MULTIPLE VERSIONS

If your document management system tracks document versions, the highest version of a document is indexed in West km. However, West km uses a document’s last modified date, regardless of version, to determine whether the document is indexed during incremental updates.

If your document management system does not mandate new versions of documents, it is possible that an older dated DMS version of the document will be indexed in West km. For example, suppose you have versions 1 and 2 of a document in your document management system and then modify version 1 without creating a new version. The document will be marked for an incremental update because the last modified date for version 1 has been updated, but version 2 will actually be indexed because it is the higher version.

INDEXING DOCUMENTS IN MULTIPLE DOCUMENT COLLECTIONS

Documents that belong to multiple document collections inherit indexing options from all document collections that contain them. Indexing options include the indexing components that process the document.

The first (primary) document collection processes the document according to its indexing options. When another document collection that contains the document is indexed, additional processing occurs for the document as necessary. Processing that was completed previously by the primary document collection is not duplicated for the document, unless the document was modified in the interim.

SUSPENDING INDEXING

You can temporarily suspend indexing in two ways:

- suspend indexing of all document collections
- suspend one or more indexing components for all document collections

Note Indexing will be automatically suspended if you reach your maximum storage for HTML document renderings.

To temporarily suspend indexing of all document collections, on the Manage Collections page, click the Actions list and click Suspend Indexing.

To remove the suspension, click the Actions list and click Unsuspend Indexing.

To temporarily suspend one or more indexing components, go to the Indexing Server Setup page. In the Indexing Components table, in the Suspend column, select the check boxes for the components you want to suspend. As long as Suspend is selected, processing for that component is suspended for all document collections during indexing, regardless of what is set for the individual document collections.

If an indexing component is set to process for a collection (e.g., concept searching indexing) and it is dependent on a suspended component (e.g., transactional analysis), then the dependent component (e.g., concept searching indexing) does not process.

If you suspend HTML conversion (upon which all other components are dependent), the following behavior occurs when indexing is attempted on a document collection:

- During a bulk indexing, nothing is processed.
- During an incremental update, documents new to the collection are not processed. However, characteristic changes that have been made to the collection since the last indexing are processed.

If the cite recognition component is suspended and you can't unsuspend it, your data validation key may be invalid or missing. The data validation key is required for the cite recognition component to communicate with the cite ID (RID) and KeyCite flags servers at Thomson Reuters during indexing. Contact your West km representative for a new product key and enter it on the System Configuration page at Setup, System Settings, System Configuration. For more information, see "Changing System Settings" on page 21.

MANUALLY LAUNCHING INDEXING JOBS

During indexing, several indexing jobs occur automatically. On the Index Jobs page, you can launch these indexing jobs manually at any time.

To manually launch indexing jobs,

1. Access the West km interface.
2. Click **Setup**.
3. Click the **Indexing** tab.
4. In the left frame, click **Index Jobs**. The indexing jobs are displayed, including the dates/times that jobs were last started and completed and their status.
5. Click the link for the indexing job you want to launch. The following table describes the available options.
6. When the job starts, the Last Started Job date/time is updated.
7. While the job is running, the Last Job Status indicates *In Progress*.
8. When the job is complete, the Last Completed Job date/time is updated, and the Last Job Status indicates *Done*.

INDEXING JOB	DESCRIPTION
General	
Search Metadata—Update	If clicked, the system immediately updates the database tables that store and query metadata used during a search. (The tables automatically update at the close of the document indexing window; you may want to invoke this process if that update fails.) By default, an incremental update is performed, which updates profile data for documents that have changed since the last update. To perform a bulk update, which updates search metadata for all documents, select the Update for all documents check box before you click Update. Depending on the size of your document collection, the update may take several minutes to complete.
Search Form Data—Update	If clicked, the system immediately updates the database tables that store the options available in drop-down lists and look-up controls on the Advanced Search page. (The tables automatically update at the close of the document indexing window.)
Cite Recognition	
Firm Citing Ref Doc Counts—Update	If clicked, the system immediately updates the citing reference counts, regardless of the document indexing window. The KM iconis used in your documents to indicate when a citation references other indexed documents at your organization. When there are more than n number of documents (set by the Firm Citing Reference Threshold setting), the icon is displayed.

INDEXING JOB	DESCRIPTION
	Citing reference counts are automatically updated daily at the end of the document indexing window. The process runs after the process of updating document counts for the KeySearch hierarchy. Counts are not immediately updated when an administrator manually deletes a document from West km.
Classification	
Document Counts—Update	If clicked, the system immediately updates the KeySearch document counts, regardless of the document indexing window. These counts indicate the number of unique documents at your organization that have been assigned to the KeySearch topic and its subtopics via manual classification or CaRE. (Counts do not include documents retrieved via Terms and Connectors queries.) Document counts for each topic in the KeySearch hierarchy are updated daily at the end of the document indexing window. Document counts are not immediately updated when a document is manually classified to a topic, removed from a topic, or deleted from West km.
Document Synchronization	
Sync Documents	If clicked, synchronization processes start. If the document sync window is not open, synchronization starts once the window opens.

STOPPING INDEXING

To stop the indexing process while it is running, stop the West km services and the World Wide Web Publishing Service. For each service, complete these steps on the service's associated server to stop the service:

1. Click the Start button, choose Administrative Tools, and then choose Services.
2. In the Services window, right-click the name of the service (e.g., KM Indexing Service) and choose Stop.

To restart services after they have been stopped, restart the World Wide Web Publishing Service and then start the West km services.

UNDERSTANDING INDEXING PERFORMANCE

The time required for indexing is affected by several factors, including the following:

- hardware processor and memory (i.e., CPU and RAM)
- number and size of documents
- average number of citations per document
- fluctuations in RID performance
- number of documents in the West km database
- the data source used to store the documents
- Internet connection speed
- configuration of West km (e.g., thread count)
- other activities on the server

Indexing performance by component:

Indexing Component	Documents per Hour[1]
Concept Search Indexing	300-500

[1] These numbers are estimates only. Performance may vary at your organization

Synchronizing Document Collections

The synchronization feature compares the list of your currently indexed documents in West km to the list of documents in your document management system or on your file system. It then removes indexed documents from West km that:

- Have been deleted from your organization's file system.
- Are no longer part of document collections you have defined to be indexed with West km?
- Have been identified as having no citations after RID processing, and that are part of document collections set to index only documents that contain one or more citations.

The synchronization process evaluates one document collection at a time. When every document has been identified in a collection, the appropriate documents are removed. If a data source connection is down or synchronization fails for a collection, synchronization proceeds with the next document collection.

When removing documents, synchronization deletes entries in the West km database, HTML document renderings, and profile metadata. Documents are still represented in full-text indexes, however, until full-text indexes are updated (see "Full-Text Indexing" on page 79 for more information).

SCHEDULING SYNCHRONIZATION

To schedule synchronization, define a document sync window. By default, a 24-hour open window is used. For the fastest processing speed, set the window's start time outside regular business hours. To prevent potential conflicts, avoid overlapping the document sync window with vetting and indexing windows.

For more information about scheduling synchronization, see "Performing Major Indexing Updates" on page 49.

MANUALLY LAUNCHING SYNCHRONIZATION

To manually launch synchronization at any time during the open window, go to the page at Setup, Indexing, Indexing Jobs, and click Sync Documents. See also "Indexing Document Collections" on page 75. If the document sync window is not open, synchronization starts once the window opens.

Full-Text Indexing

Full-text indexes are used to retrieve your organization's documents when a West km member at your organization performs a term search. The full-text indexing capability in West km is provided by the search component, and is based on full-text indexing collections for different types of documents.

Indexing collections are listed in the following table.

This Collection	Indexes
KM	files (i.e., documents)
KMClause	clauses
KMDefinedTerm	defined terms

When full-text indexes are created, all documents are processed. When full-text indexes are updated, processing occurs for new, modified, and deleted documents since the last full-text indexing.

During full-text indexing, searches can simultaneously be performed in West km. Note, however, that search performance may be negatively affected. For this reason, it is recommended that you schedule or launch full-text indexing outside regular business hours. In addition, you should not simultaneously run full-text indexing and other West km indexing and synchronization processes.

The time required for full-text indexing is affected by several factors, including your system configuration and the content collection being indexed. Approximately 20,000 documents can be full- text indexed per hour, although this number is an estimate and performance may vary at your organization.

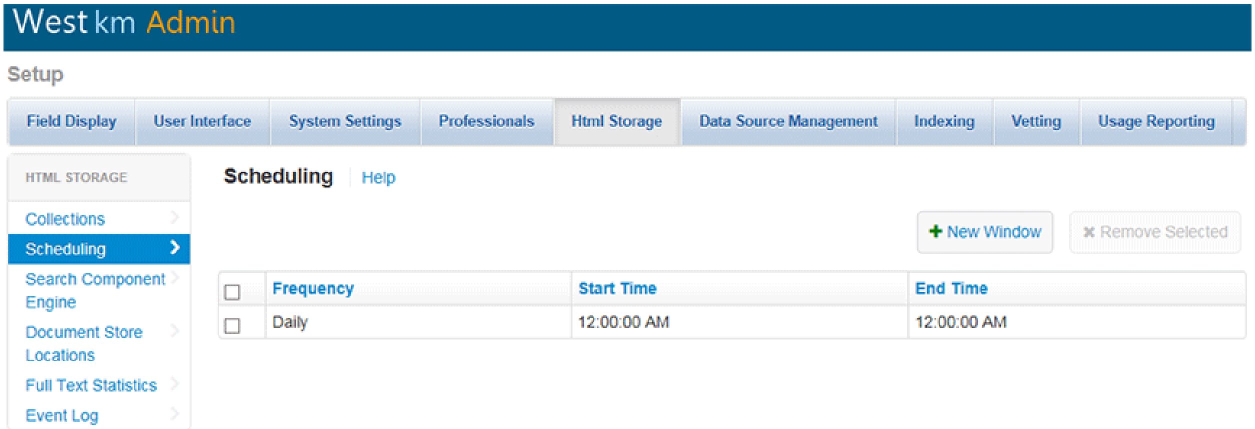
SCHEDULING FULL-TEXT INDEXING

Full-text indexing is scheduled by defining indexing time windows for the search service. You may want to define multiple time windows to account for different frequencies (e.g., weekdays vs. weekends). Windows affect all full-text indexing collections.

To schedule full-text indexing,

1. Access the West km interface.
2. Click Setup.
3. Click the HTML Storage tab.

4. In the left frame, click Scheduling. The full-text indexing windows are displayed in the right frame.



5. Click New Window.
6. In the Add Service Window dialog box, do the following and click Save.
   - Frequency: Choose the frequency for which you'd like the window to be in effect. Weekdays refer to Monday through Friday. Weekends refer to Saturday and Sunday.
   - Start time and End time: Type the start time and the end time for the window in hours and minutes and indicate whether the time is a.m. or p.m.
   - A window's start time always occurs on the day specified by the frequency. The end time may occur the day afterward, depending on whether the start time is set before or after the end time.

     Note The start time and end time should not be the same, or the window is considered to be open for zero time instead of 24 hours. For example, use a start time of 12:00:00 AM and an end time of 11:59:59 PM if you want a 24-hour window.
7. Repeat steps 4–5 for each full-text indexing window you want to schedule.

For example, if you want full-text indexing to run twice each day, define two windows with a frequency type of Daily, but with different start and end times.

If you want full-text indexing to run during one window on weekdays and another on weekends, define two windows and choose a frequency type of Weekdays for one window and Weekends for the other, with different start and end times for each.

Full-text indexing will start automatically within ten minutes after reaching the start of the window. At the close of the window, the search component will finish full-text indexing the currently processing documents (which takes approximately five to ten minutes) before stopping.

To remove one or more full-text indexing windows, select the check boxes next to the windows you want to remove and click Remove Selected.

To change an existing full-text indexing window, remove the window and then add another window with the settings you want.

MANUALLY LAUNCHING FULL-TEXT INDEXING PROCESSES

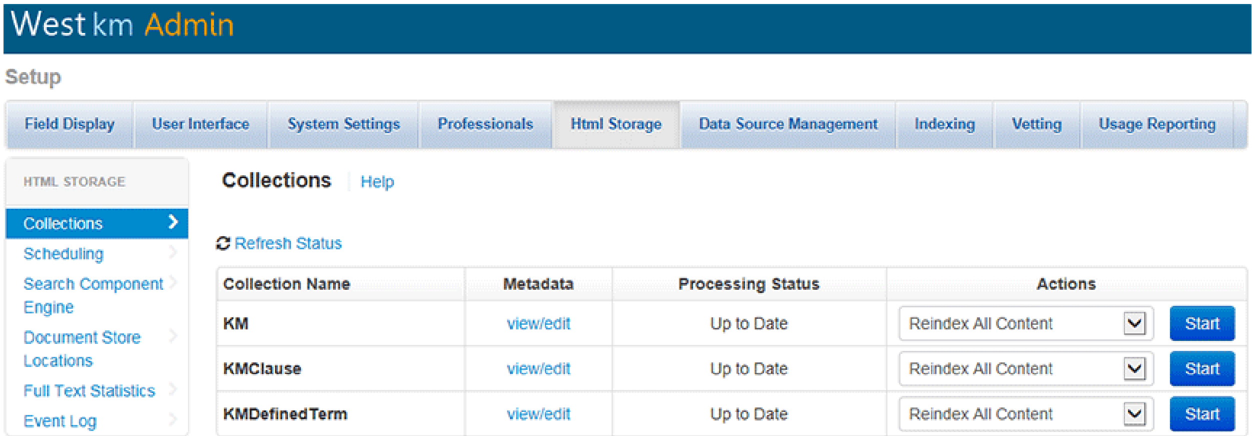
You can manually launch full-text indexing processes at your organization. The manual method is unlike the regularly scheduled windows in that:

- You can specify which full-text indexing collections to process. (Via the regularly scheduled windows, processing occurs for all indexing collections.)
- Processing occurs for all documents in the indexing collection. (Via the regularly scheduled windows, processing occurs only for new, modified, and deleted documents.)
- You can launch a specific full-text indexing process for an indexing collection.

To manually launch a full-text indexing process,

1. Access the West km interface.
2. Click Setup.
3. Click the HTML Storage tab.

4. In the left frame, click **Collections**. The Collections page is displayed.



5. Select a full-text indexing process from the **Actions** list and click **Start**.
   - **Reindex All Content**: This process runs full-text indexing for all documents in the indexing collection. If the full-text indexing window is not open, processing starts once the window opens.
   - **Reindex Failed Content**: This process attempts to reprocess documents that failed full-text indexing in the indexing collection. If the full-text indexing window is not open, processing starts once the window opens.

     Note The search component will automatically attempt reprocessing of failed documents. The Reindex Failed Content process could be useful, for example, if the search component was down and you want to manually launch reprocessing attempts.
   - **Clear Indexed Data**: Do not run this process without the assistance of a West km representative. This process deletes all search component index files and document content from the search component databases. It should be used only in certain troubleshooting situations. Processing occurs immediately. After running this process, you must run Reindex All Content or searches will fail to find content.

     Note When you clear indexed data, note that content remains in the HTML document stores, and documents records are placed in suspended status.
   - **Update Collection Definition**: This process updates the indexing collection's XML files, which contain high-level and field metadata for the indexing collection. It is used for troubleshooting purposes, but will have no ill effect if used at other times. Processing occurs immediately.

     Changes are applied to newly indexed content. To apply changes to all content, run Reindex All Content.

To view or edit XML field metadata for an indexing collection, in the Metadata column of the Collections table, click **View/Edit** next to the indexing collection. Make the changes you want in the Edit Metadata dialog box and click Save. This action is comparable to the Update Collection Definition process.

Changes are applied to newly indexed content. To apply changes to all content, run Reindex All Content.

VIEWING THE SEARCH COMPONENT ENGINE

The Search Component Engine page lists the following information:

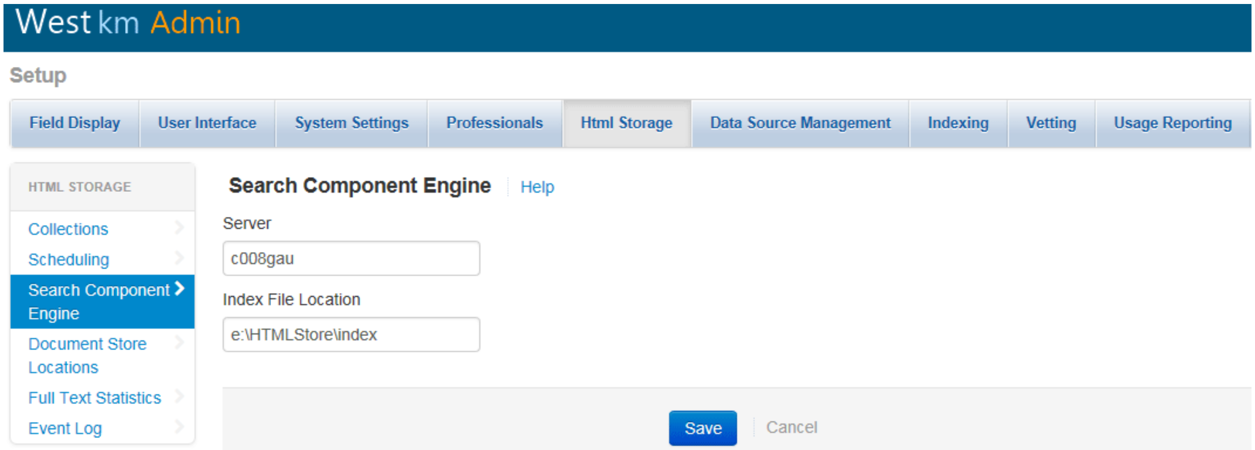
- **Server**: The server on which the search component is installed and that acts as your HTML respository/search server
- **Index File Location**: the folder location (e.g., *[Drive]*:\HTMLStore\index) on the HTML respository/ search server where index files for the search component are placed

Note If you don't want index files on a local drive, a server and share can be designated using a UNC path (*server**share*\).

To access the Search Component Engine page,

1. Access the West km interface.
2. Click **Setup**.
3. Click the **HTML Storage** tab.

4. In the left frame, click **Search Component Engine**. The Search Component Engine page is displayed.



You can edit the server and index file location on the Search Component Engine page by changing the values in the text boxes and clicking **Save**; however, this action updates only the West km database and should be completed only in context with other procedures for

- moving the search component to another server
- moving the index file location

It is recommended that you contact your West km representative for these procedures because they will involve one or more of the following actions:

- Installing the search component on a new server.
- Manually copying index files to a new server or to a new location on the same server.
- Stopping and starting services.
- Manually updating the CCI search component database to reflect the new index file location.
- Moving the HTML storage location to another server.

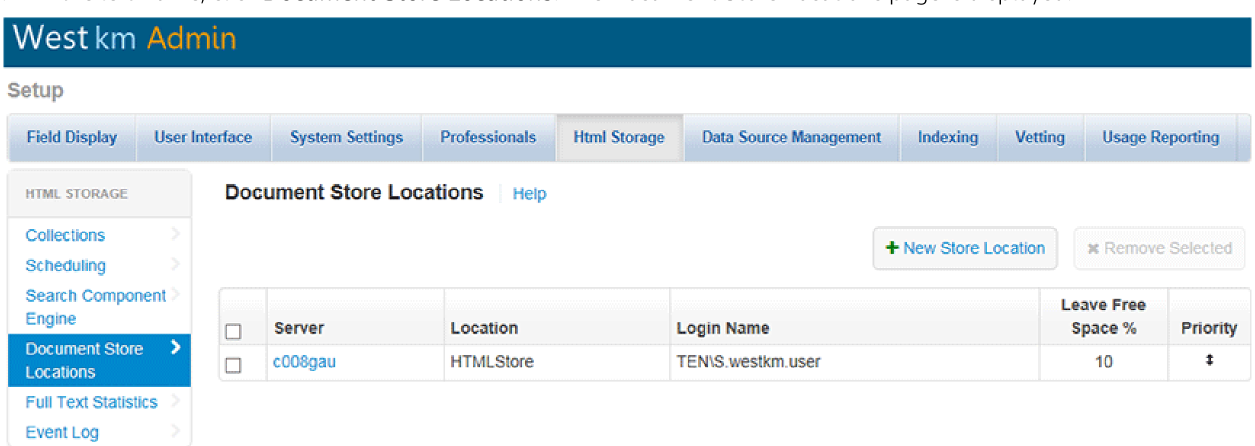
MANAGING DOCUMENT STORE LOCATIONS

The Document Store Locations page lists the folder locations where HTML documents are stored. These are the documents that are converted to HTML from their native file formats for use in West km.

You can complete several actions on the Document Store Locations page, including adding, editing, and removing storage locations. However, it is recommended that you contact your West km representative before completing these actions. Many should be completed only in context with other procedures.

To access the Document Store Locations page,

1. Access the West km interface.
2. Click **Setup**.
3. Click the **HTML Storage** tab.
4. In the left frame, click **Document Store Locations**. The Document Store Locations page is displayed.



Adding a Storage Location

When you install West km, you designate a folder location (e.g., *[Drive]*:\HTMLStore) on the HTML repository/search server that will store HTML documents. If that location fills, you can

- clear drive space at the existing storage location
- lower the percentage of free space to leave at the existing storage location
- add a storage location

To add a storage location,

1. Click New Store Location.
2. In the New Store Location dialog box, enter the following:
   - Server: The server containing the new storage location for HTML documents
   - Location: The folder location (e.g., *[Drive]*:\HTMLStore) on the server that will store HTML documents

     Note If you don't want the storage location on a local drive, you can enter a server and share using a UNC path (*server**share*\).
   - Login Name and Password: Usually the credentials for the remote access account that is configured on the West km system
   - Leave Free Space %: The percentage of free space to leave at the storage location when it fills
3. Click Save.

If you have multiple storage locations, the system uses the first storage location listed until it fills. The storage limit is set by the Leave Free Space % value. When a location fills, the system begins using the next storage location listed. You can change the priority by dragging a row using the Priority icon.

If all storage locations are full, indexing is automatically suspended. After addressing the storage situation, you can unsuspend indexing at the Indexing, Manage Collections page. For more information, see "Indexing Document Collections" on page 75.

Editing a Storage Location

You can edit a storage location on the Document Store Location page. For example, you can change the percentage of free space to leave at a storage location. Click the server name, change the value in the Leave Free Space % box, and click Save.

It is recommended that you contact your West km representative before changing the server or location values for a storage location. If you want to move a storage location, changing these values should be completed only in context with other procedures such as suspending indexing, manually copying files, and setting permissions.

Removing a Storage Location

It is recommended that you contact your West km representative before removing a storage location.

If you remove a document store location that has content, a complete re-indexing of your West km system is required, including indexing and full-text indexing.

To remove a storage location, select the check boxes to the left of each storage location that you want to remove and click Remove Selected.

Rearranging Document Collections

Once you have set up your document collections and indexed them in West km, it is possible that you might later want to rearrange the way collections are set up. For example, you might want to delete and add collections, change library groups, or move documents between collections. The following methods are recommended to implement these common changes and to avoid unnecessary re- indexing of documents.

Note For changes that require you to remove data source connections, it is recommended that you seek assistance from your West km representative if you wish to avoid re-indexing documents.

ADDING AND DELETING DOCUMENT COLLECTIONS

To add new collections and delete the old, complete the following steps:

1. Add the new vetting groups in the vetting toolkit (see "Adding a Vetting Group" on page 61 for more information).
2. Run vetting on the new vetting groups (see "Running Vetting Rules" on page 62 for more information).
3. Add the new document collections (see "Adding Document Collections" on page 71 for more information).
4. Run bulk indexing on the new document collections (see "Indexing Document Collections" on page 75 for more information).

5. Delete the old vetting groups (see "Editing, Copying, and Deleting a Vetting Group" on page 61 for more information).
6. Remove the old document collections (see "Managing Document Collections" on page 75 for more information).
7. Run synchronization (see "Synchronizing Document Collections" on page 78 for more information).
8. Run an incremental update on all the document collections (see "Indexing Document Collections" on page 75 for more information).
9. Run full-text indexing (see "Full-Text Indexing" on page 79 for more information).

ADDING AND DELETING LIBRARY GROUPS

To add new library groups and assign them to existing collections, complete the following steps:

1. Add the new library groups and assign them to document collections (see "Library Groups" on page 72 for more information).
2. Run incremental update on the affected document collections (see "Indexing Document Collections" on page 75 for more information).
3. Delete the old library groups (see "Library Groups" on page 72 for more information).
4. Run full-text indexing (see "Full-Text Indexing" on page 79 for more information).

MOVING DOCUMENTS BETWEEN COLLECTIONS

To move documents between document collections, complete the following steps:

1. Change the vetting groups in the vetting toolkit (see "Editing, Copying, and Deleting a Vetting Group" on page 61 for more information).
2. Run vetting on the affected vetting groups (see "Running Vetting Rules" on page 62 for more information).
3. Run an incremental update on all the document collections (see "Indexing Document Collections" on page 75 for more information).
4. Run synchronization (see "Synchronizing Document Collections" on page 78 for more information).
5. Run an incremental update on all the document collections (see "Indexing Document Collections" on page 75 for more information).
6. Run full-text indexing (see "Full-Text Indexing" on page 79 for more information).

DELETING DOCUMENTS FROM A COLLECTION

To delete documents from a collection, complete the following:

1. Do one of the following:
   - Delete (or move) documents from your file system so they are no longer in folders indexed by West km.
   - Remove documents from document collections you have defined to be indexed with West km. For example, you could change the criteria for your vetting group or DMS saved search to exclude the documents.
2. Run synchronization (see "Synchronizing Document Collections" on page 78 for more information).

8 Managing Users

You can control who can access West km at your organization by managing users on the Professionals tab.

Note For more information about West km authentication methods, see the West km Administrators Installation Guide. For details about the configuration that is required for authentication to function properly, see "Appendix D: Authentication and Document Security Configuration" on page 118.

To access the Professionals tab,

1. Access the West km interface.
2. Click **Setup**.
3. Click the **Professionals** tab.

Understanding User Rights

You can assign your West km users different levels of system rights, which are listed in the following table.

Administrator	The user has rights to the West km setup pages, has rights to manually delete documents from West km, and has the rights of a KeySearch Editor, Annotator, and Vetting Editor. In addition, if Administrator is selected, the system automatically selects Active User.
KeySearch Editor	The user has rights to administer the KeySearch hierarchy in West km for Litigation.
Annotator	The user is able to add notes and mark files as exemplar. The user is also able to edit and delete all annotations.
Vetting Editor	The user has access to the West km Vetting Toolkit.
User	The user is able to search and display your indexed documents in West km.

In addition, you control the access that your active users have to your indexed documents by setting a document security level in West km. The security levels are based on the security implemented in your organization's document management system.

You can select a document security level using the Document Security Level setting at the Setup, System Settings, Security page. For more information, see "Changing System Settings" on page 21.

Managing Users with Active Directory Integration

If you are using the Integrated Windows Authentication (IWA) method for West km, you will manage West km users via integration with Active Directory, which authenticates and authorizes users for your Windows domain networks. (For more information about West km authentication methods, see the West km Administrator Installation Guide.)

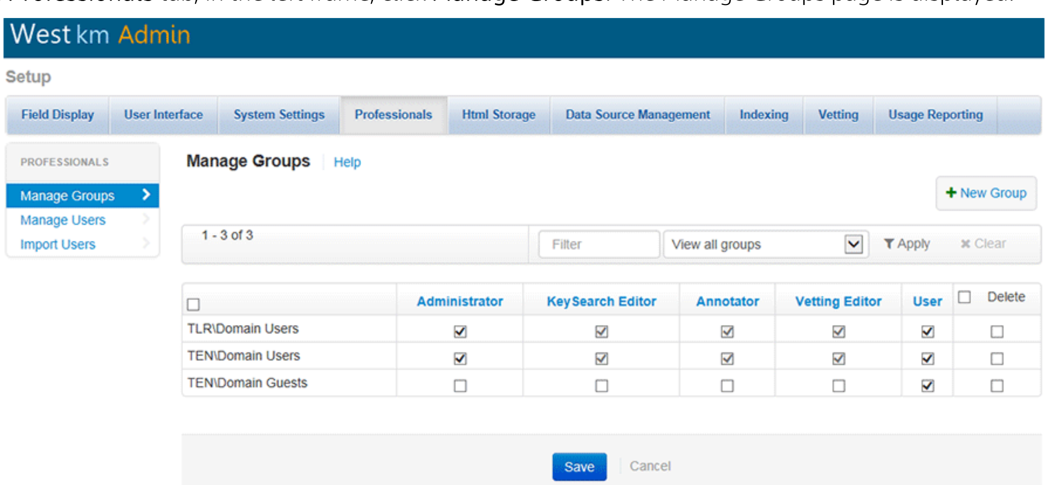
Active Directory integration allows you to easily assign West km rights for Active Directory groups, as well as customize rights for individual users within Active Directory.

MANAGING GROUPS

You can manage users in West km based on Active Directory groups. The West km rights you assign to a group are automatically assigned to all users in that group.

To add an Active Directory group of users,

1. On the **Professionals** tab, in the left frame, click **Manage Groups**. The Manage Groups page is displayed.



2. Click New Group.
3. In the Find Groups dialog box, in the Search Query box, type the name of the group that you want to add and click Search. Groups that contain the search string in the group name are found.
4. Select the check box preceding each group in the list that you want to add.
5. Click Save.

By default, new groups have Active User rights. To assign additional rights for a group, select the appropriate rights check boxes for the group. For more information, see "Understanding User Rights" on page 85.

To remove an Active Directory group of users,

1. On the Professionals tab, in the left frame, click Manage Groups.
2. For the groups you want to remove, select the check box in the Delete column.
3. Click Save.

To filter the list of groups, type or select values at the top of the Manage Groups page and click Apply. In the Filter box, type a search string to retrieve groups that contain the search string in the name. To display all groups, click Clear.

Note Active users have User selected. Inactive users do not have User selected. To sort the group listing, click a column heading.

MANAGING USERS

As well as groups, you can add individual users from Active Directory. The rights assigned for an Active Directory group are the default settings for all users within the group. Settings for individual users override the settings for groups to which users belong.

To add an individual user,

1. On the Professionals tab, in the left frame, click Manage Users. The Manage Users page is displayed.
2. Click New User.
3. In the Find Users dialog box, in the Search Query box, type the name of the user that you want to add and click Search. Users that contain the search string in the user name are found.
4. Select the check box preceding each user in the list that you want to add.
5. Click Save.

By default, new users have Active User rights. To assign additional rights for a user, select the appropriate rights check boxes for the user (see "Understanding User Rights" on page 85 for more information).

Note Only users who have been added individually are displayed on the Manage Users page. Users who been added only as part of an Active Directory group are not displayed on the Manage Users page.

To view a list of groups to which the user belongs (and which have been added to West km), click User Groups next to the user's name.

To remove an individual user,

1. On the Professionals tab, in the left frame, click Manage Users.
2. For the users you want to remove, select the check box in the Delete column.
3. Click Save.

To filter the list of users, type or select values at the top of the Manage Users page and click Apply. In the Filter box, type a search string to retrieve users that contain the search string in the username or name. To display all users, click Clear.

To sort the user listing, click a column heading.

Managing Users without Active Directory Integration

If you are using the West km custom authentication method, you will manage West km users without Active Directory integration. Instead you will control user access to West km via usernames and passwords administered in West km. (For more information about West km authentication methods, see the West km Administrator Installation Guide.)

To add a user,

1. On the Professionals tab, in the left frame, click Manage Users. The Manage Users page is displayed.
2. Click New User.

3. In the **User Details** dialog box, type the information for the user. All fields are required except Middle Name and Network ID.

First Name;Last Name; and Middle Name	the user's first, last, and middle names
Network ID	the user's ID to log on to your organization's Windows network, including the domain (e.g., USA\W010)
Email Address	the user's email address
User Name	a username for the user to log on to West km
Password	a password for the user to log on to West km; passwords are case-sensitive and must be at least six characters

4. Click **Save**.

By default, new users have Active User rights. To assign additional rights for a user, select the appropriate rights check boxes for the user. For more information, see "Understanding User Rights" on page 85.

To edit a user's information, click the user's name, make your changes, and click **Save**.

To remove a user,

1. On the **Professionals** tab, in the left frame, click **Manage Users**.
2. For the users you want to remove, select the check box in the **Delete** column.
3. Click **Save**.

To filter the list of users, type or select values at the top of the Manage Users page and click **Apply**. In the **Filter** box, type a search string to retrieve users that contain the search string in the username. To display all users, click **Clear**.

To sort the user listing, click a column heading.

Importing Users

If you have an extensive list of users to add to West km, you can import the user data to the system. Importing user data requires creating an input file of comma-separated values (.csv) and then running the import.

CREATING AN INPUT FILE

The first step when importing user data is to create an input file in .csv format with the data for the users to be imported. In .csv files, data is separated by commas, and each row of data ends in a carriage return.

In the file, include the following data for each user you want to import, in the order listed:

- Network ID
- User Name
- Password (plain text)
- Email Address
- First Name
- Middle Name
- Last Name
- DMS User ID
- DMS Password (plain text)
- Active User
- Administrator
- KeySearch Editor
- Annotator
- Vetting Editor

When creating the input file, observe the following:

- If you are using Integrated Windows Authentication (IWA) for West km, you must enter a value for the Network ID. You must include the domain (e.g., fish\u0023), and the value must uniquely identify the user.
- If you are using West km custom authentication, you must enter a value for User Name. The value must uniquely identify the user.
- For each user, you must enter a value for Email Address.
- If you want to leave a category blank (e.g., Middle Name), don't enter a value but insert a comma in the .csv file to represent the data category. If you are using Excel to create the .csv file, the data cell for that category can be left blank; the comma will be inserted during the save process.

- When setting a value for Active User, Administrator, KeySearch Editor, Annotator, or Vetting Editor, it must be either `0` (not selected) or `1` (selected).
- Values cannot be imported for DMS UserID, DMS Password, or Server\DB (see "Adding DMS User ID and Password" on page 89 for more information). You must use the Manage Users page to enter this information after the import.

Input File Creation Tips

Because Microsoft Excel can save data in .csv format, you may find Excel a useful tool in preparing your import data. For example, you might receive user data from a variety of sources or in a variety of formats: users from your account manager, authors and network IDs from DMS output, or network domain information from your IT department. As necessary, Excel can be used to separate columns, to append two columns into one, or to order columns.

Separating Columns in Excel

You can use Excel to separate the data in a column. For example, you might have full names in one column.

To create separate columns for first, middle, and last names in Excel,

1. Select the column you want to separate and copy it to the last empty column of your worksheet (see the following subsection, "Moving and Copying Cells in Excel.")
2. Select the newly copied column. From the **Data** tab, choose **Text to Columns**.
3. At the Convert Text to Columns Wizard, select **Delimited** and click **Next**.
4. Select Space as the only delimiter, click **Next**, and then click **Finish**.

Appending Columns in Excel

You can use Excel to append two columns into one. For example, you might have first names and last names in separate columns and need to create a single column for full name.

To place first and last names in one column in Excel,

1. In a blank column of your worksheet, select the first cell.
2. In the formula bar, type `=A1&B1`, where `A` is the column containing the first name and `B` is the column containing the last name. Then press **Enter**.
3. In the newly appended column, copy the formula to the remaining rows in the worksheet by dragging the fill handle from the first cell over the remaining cells.
4. If you want to delete the original separated columns, first copy the values in the newly appended column without the formulas to a blank column in your worksheet. To do so, select the new appended column, right-click and choose **Copy**. Select the blank column, right-click and choose **Paste Special**. Select **Values** as the only Paste option and click **OK**.

Moving and Copying Cells in Excel

You can use Excel to reorder columns of data so that they are in the order required.

To move and copy cells in Excel,

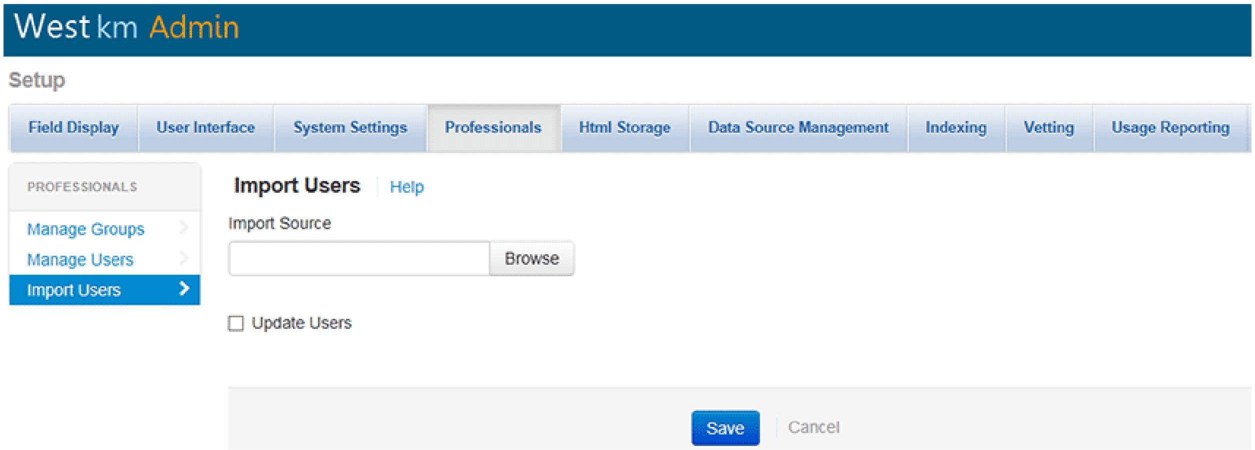
1. Select the cells you want to move or copy.
2. Point to the border of the selection.
3. Do one of the following:
   - To move the cells, drag the selection to the new location on the worksheet. Excel will ask if you want to replace any existing data.
   - To copy the cells, hold down the CTRL key as you drag.
   - To insert cells between existing cells, hold down the SHIFT key (if moving) or SHIFT+CTRL (if copying) as you drag.
   - To drag the selection to a different worksheet, hold down the ALT key and drag over a sheet tab.

RUNNING THE IMPORT

The second step when importing user data is running the import, which reads the input file you created in .csv format and adds the unique users to the system.

To import users,

1. On the **Professionals** tab, in the left frame, click **Import Users**. The Import Users page is displayed.



2. In the **Import Source** box, indicate the location of your .csv file. You can do one of the following:
   - Type the path and filename of the .csv file you created.
   - Click **Browse** and navigate to the .csv file you created. Your .csv file can be located locally or on a network.
3. If a user you are importing already exists in the system and you want to update that user's information, select the **Update Users** check box.

For each user to be imported, the system checks either the Network ID or the User Name, depending on your West km authentication method. If the value being compared already exists for an entry, then information for the user is either imported or not, depending on your selection.

4. Review the records to be imported and verify their accuracy.

If you are using IWA for your authentication method, the Network ID is displayed. If you are using West km custom authentication, the User Name is displayed. (Passwords are not displayed.)

5. To proceed with the import, click **Save**.

The Manage Users page is displayed, with the new user data at the bottom of the listing.

Exporting Users

You can export user data to a file of comma-separated values. You can then compile that data in another program, such as Excel, to analyze your West km user data in a more usable format.

To export user data to a file,

1. On the **Professionals** tab, in the left frame, click **Manage Users**.
2. Click **Options**, and then click **Export Users**.
3. Follow your browsers on-screen instructions to save the file.

The file contains the same data that is needed to create an input file for importing users (see "Importing Users" on page 87 for more information).

Adding DMS User ID and Password

The Manage Users page will include columns for DMS UserID or DMS Password (or both) if your organization

- uses iManage Work for its document management system and uses virtual logins rather than NT integrated logins
- uses NetDocuments for its document management system and uses NetDocuments security to determine document access rights

In this situation, you need to add either a DMS user ID or DMS password (or both) to the appropriate columns.

For iManage Work, you need to indicate the server and database to which the user has access in the `Server\DB` column. A user may be able to access more than one database; in this situation, a drop-down list is displayed in the `Server\DB` column. When adding or editing a user’s information, you need to choose the databases from the `Server\DB` drop-down list to which you want the user to have access and specify the user’s DMS login information. The login information will apply to all selected databases.

You can adjust the columns on the Manage Users page by using the settings for your document management system at Setup, Data Source Management, Settings. For details, see "Adding an iManage Work Data Source Connection" on page 40 or "Adding a NetDocuments Data Source Connection" on page 41.

9 Tracking Program Activity

The following West km features provide a log of West km activity and allow you to monitor program processes and troubleshoot errors:

- Indexing statistics allow you to monitor indexing processes.
- The event viewer allows you to monitor program events.
- Trace logs allow you to gather information and troubleshoot program activity.
- The usage reporting feature allows you to track West km usage.

Monitoring Indexing Processes

You can monitor the progress of indexing, full-text indexing, and synchronization processes. To monitor the progress of vetting, see "Viewing Statistics" on page 70.

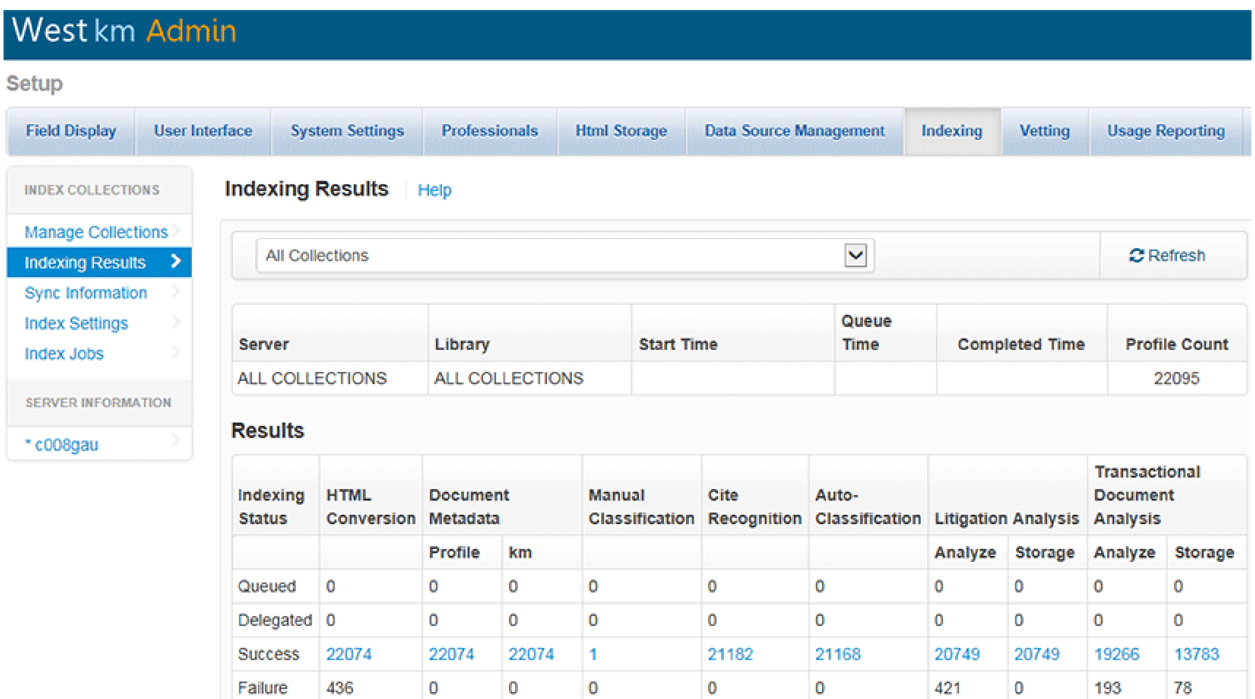
MONITORING INDEXING

You can monitor the indexing progress of a document collection. Indexing results are shown for both bulk indexing and incremental update processes, whether automatically or manually initiated.

To monitor the indexing progress of a document collection,

1. Access the West km interface.
2. Click Setup.
3. Click the Indexing tab.
4. In the left frame, click Indexing Results.
5. From the drop-down list at the top of the page, select the document collection for which you want to view indexing results. To view results for all document collections, select All Collections.

Indexing results for the documents in the selected document collections are displayed. To update the results while the indexing process is running, click Refresh. (The page is not refreshed automatically.)



Understanding Indexing Results

The Indexing Results page provides information about the indexing results for a collection, including results for both successes and failures.

Collection Information

The following table lists the information that is provided at the top of the Indexing Results page.

Label	Description
Server	The server containing the documents in the document collection.
Library	The database or library containing the documents in the document collection.
Start Time	The time the last indexing process started scheduling. The time is displayed as soon as the indexing process is started.
Queue Time	The time the last indexing process was scheduled. The time is displayed as soon as indexing is scheduled.
Completed Time	The time the last indexing process completed. The time is displayed as soon as indexing completes.
Profile Count	The number of document profiles in the document collection. Note This count may be less than the count shown in the Total row in the Results table (and for your DMS saved search) if documents are duplicated in multiple collections and were previously processed by another (primary) document collection. These documents are accounted for in the Duplicate row in the Indexing Results table.

Results

The Results table shows the current indexing results for the selected document collection. For each indexing component, the number of documents at each status is indicated. The following table explains each status.

This status	Shows how many documents in the collection
Queued	Are currently scheduled and remain to be processed.
Delegated	Are currently in process.
Success	Have processed successfully.
Failure	Have not been processed because of errors.
Not applicable	Will not be processed because the component doesn't apply or a component on which it is dependent has failed.

Success Breakdown

The Success Breakdown table shows a breakdown of the current indexing results for the documents that successfully processed. For each indexing component, the number of documents at each status is indicated. The following table explains each status.

This status	Shows how many documents in the collection
Success	Have processed successfully.
Analyzer partial analysis	Have processed successfully, but a failure occurred in the analyzer component (Litigation) while identifying a specific entity, e.g., jurisdiction.
Identified as secured	Have not been processed because they are within a secured subfolder within an NTFS share.
Invalid document structure	Have not been processed because the document's structure doesn't allow the document analysis component to proceed with the analysis.
No cites – deleted[1]	Have been deleted from West km during synchronization because they have no citations.
No cites – pending deletion[1]	Have been scheduled to be deleted from West km because they have no citations; documents will be deleted during the next synchronization process.
RID partial error	Have processed successfully, but with an error in identifying citations with RID; at least one citation in each document was identified.
Unsupported file type	Have not been processed by the document analysis component because the document file is an unsupported file type—for example, an unsupported version of an application format that is supported in other versions by other components.
Work in progress	Have not been processed because they have been modified or added to the collection within the number of days set in the Work in Progress Time Span setting at Setup, Indexing, Index Settings, General.

[1] When a document collection is set to index only documents that contain one or more citations (the Citations Only check box is selected for the collection), documents with no citations are deleted from West km during the synchronization process. A document is identified as having no citations after the document is converted to HTML and processed by the cite recognition component (RID).

Failure Breakdown

The Failure Breakdown table shows a breakdown of the current indexing results for the documents that failed processing. For each indexing component, the number of documents at each status is indicated. The following table explains each status.

This status	Shows how many documents in the collection	Automatic reprocessing?
Analyzer failure	Have not been processed because of a failure for unknown reasons in the document analysis component or the analyzer component.	X
Analyzer FCC failure	Have not been processed because the FFC (file format converter) component of the document analysis component failed. (See the FFC logs for further details.) This component converts documents from native format to SGML format.	X
Analyzer initialization failure	Have not been processed because the analyzer component (Litigation) failed to initialize.	
Analyzer mapping failure	Have not been processed because the BKM (bookmark mapping) component of the document analysis component failed. (See BKM logs for further details.) This component adjusts (maps) bookmarks. Mapping is required because analysis occurs on the SGML version of the native document, not on the SGML version of the HTML document, and bookmarks need to be inserted into the HTML version of the document.	
Document size exceeded	Have not been processed because the documents exceed the maximum size of files allowed into West km. (The default threshold is 50 megabytes.)	
Full text abstraction failure	Have not been processed because the indexing service encountered a problem and could not copy or retrieve a document from the HTML storage location.	X
General error	Have not been processed because of a general failure.	X
Conversion error	Have not been processed because of a failure to convert them to HTML.	
Identified as corrupt	Have not been processed because they are corrupt.	
No concept search information	Have not been processed because the document analysis service failed when attempting to insert SDX (smart data indexing) information into the document for concept title searching.	
Partial analysis	Have been only partially processed by the document analysis component. Either FFC failed to convert the native document or the HTML document to SGML, or the BKM mapping algorithm failed when the two SGML files were compared. Note This error could occur if too many processes are running simultaneously on your server.	X
RID error	Have not been processed because of a failure in RID to identify citations; no citations in the documents were identified.	X
RID timed out	Have not been processed because RID failed to communicate for 120 seconds.	
Store is full	Have not been processed because the maximum was reached for your designated HTML document storage.	X
Unable to access file or physical file missing	Have not been processed because the document file could not be found.	
Well-formed conversion error	Have not been processed because the HTML conversion of the document does not conform to the syntax rules of XML.	

Viewing and Reprocessing Documents

To view a listing of documents for a particular indexing component and status, on the Indexing Results page, click a hyperlinked number in the Success Breakdown or the Failure Breakdown table.

Manual Reprocessing

When you view a listing of documents, you can choose to manually reprocess the documents. This option is useful if the documents failed and you want to reprocess them immediately.

To manually reprocess documents,

1. Select the check box preceding each document in the list that you want to reprocess. To select all documents in the list, select the check box in the heading.
2. Click **Actions** and then click the reprocessing option you want.
   - To reprocess the selected documents for the indexing component being viewed, click **Reprocess Component**.
   - To reprocess the selected documents for all indexing components that have been set for that document collection, click **Reprocess All Components**.

Documents are rescheduled immediately, and indexing will start according to the collection's document indexing window.

Note If you reprocess the HTML conversion component, all components that have been set for that document collection will be reprocessed.

To filter the list of documents, type or select values at the top of the Indexing Results page and click **Apply**. In the **Filter** box, type a search string to retrieve documents that contain the search string in the document name or in the data source name. To display all documents, click **Clear**.

To edit the collection to which a document belongs, click **View** in the Collection column.

Automatic Reprocessing

If you don't manually reprocess documents, West km will attempt to reprocess documents in some status categories after six hours (360 minutes), as indicated by the value of the `indexer_ErrorReprocessThresholdMinutes` property in the Thomson.Westkm.IndexingService.exe.config file. Status categories that are reprocessed automatically by default are indicated in the Automatic Reprocessing column in the Success Breakdown and Failure Breakdown tables above.

Delegated documents can become "stranded" if they fail while in the delegated state but cannot be marked as failed. West km will attempt to reprocess stranded delegated documents after six hours (360 minutes), as indicated by the value of the `indexer_DelegatedReprocessThresholdMinutes` property in the Thomson.Westkm.IndexingService.exe.config file.

Note If the West km indexing service is stopped, all documents in the delegated state (included stranded delegated documents) will be rescheduled immediately when the service is restarted.

Reprocessing attempts continue at the set rate in relation to the last failed attempt until documents are indexed or until another indexing process is run and attempts to process the documents. At that point, the result of the most recent indexing process affecting the documents determines reprocessing attempts going forward.

Regardless of the result of a previous indexing process, the following occurs:

- During bulk indexing, all documents in the collection will be re-indexed.
- During an incremental update, documents in the collection will be re-indexed only if they are new or modified and have a date and time after the collection was last indexed. (New or modified documents with an earlier date and time will only be indexed if the Sync New Docs In Incremental Update setting is selected.)

Troubleshooting

To see more detailed information about West km indexing activity, for example, if several documents had errors, you can:

- Access the event log. For more information, see "Monitoring Program Events" on page 97.
- See the program trace logs. For more information, see "Using Trace Logs" on page 97.

MONITORING SYNCHRONIZATION

To monitor the progress of synchronization processes,

1. Access the West km interface.
2. Click **Setup**.
3. Click the **Indexing** tab.
4. In the left frame, click **Sync Information**. The Sync Information page is displayed.

The following statistics are provided on the Sync Information page.

Sync Counts

The Sync Counts table shows the cumulative number of documents that have been deleted from West km. Documents are deleted because they are in one of two states, which are explained in the following table.

Deleted from Synchronization with Data Source	The total number of documents deleted from West km during synchronization processes. These include documents that were deleted from your organization's file system, that were no longer part of a document collection, or that had no citations and were part of a document collections set to index only documents that contain one or more citations.
Deleted Manually from West km Interface	The total number of documents deleted from West km using the West km interface. For details, see "Deleting Documents" on page 111.

To view a listing of documents for a particular delete state, click a hyperlinked number in the Sync Counts table.

To filter the list of documents, type or select values at the top of the page and click **Apply**. In the **Filter** box, type a search string to retrieve documents that contain the search string in the name. To display all documents, click **Clear**.

Sync Jobs

The Sync Jobs table lists synchronization processes that have run, including the date and time the job started, the date and time the job completed, and the number of documents deleted.

If the synchronization job is not successful, a blank entry in the Completed column of the Sync Jobs table could indicate that the synchronization process had a problem accessing a particular collection of documents.

To view more information about a synchronization job, click View Detailed Record for the listing. The Sync Job Details page is displayed, which includes the Active Document Verification Checks table for the synchronization job. This table can be useful for monitoring synchronization jobs, because it lists the results of document verification by each collection. The possible collection status indicators are explained in the following table.

	Success
	Skipped Synchronization was skipped because the Skip Sync Process option is selected for the collection; or Synchronization was skipped because the number of documents marked for deletion matches the existing document count for the collection in West km. This logic prevents an entire collection of documents from being wrongly deleted if a DMS reports to West km that zero documents exist in a collection when documents actually do exist.[1]
	Failure For example, synchronization could fail if vetting rules are currently running for a collection. (At the next attempt, synchronization will likely succeed if vetting rules are not running.)
[blank]	In Process or Stopped Synchronization of the collection is in process or the indexing service was stopped before it was able to finish.

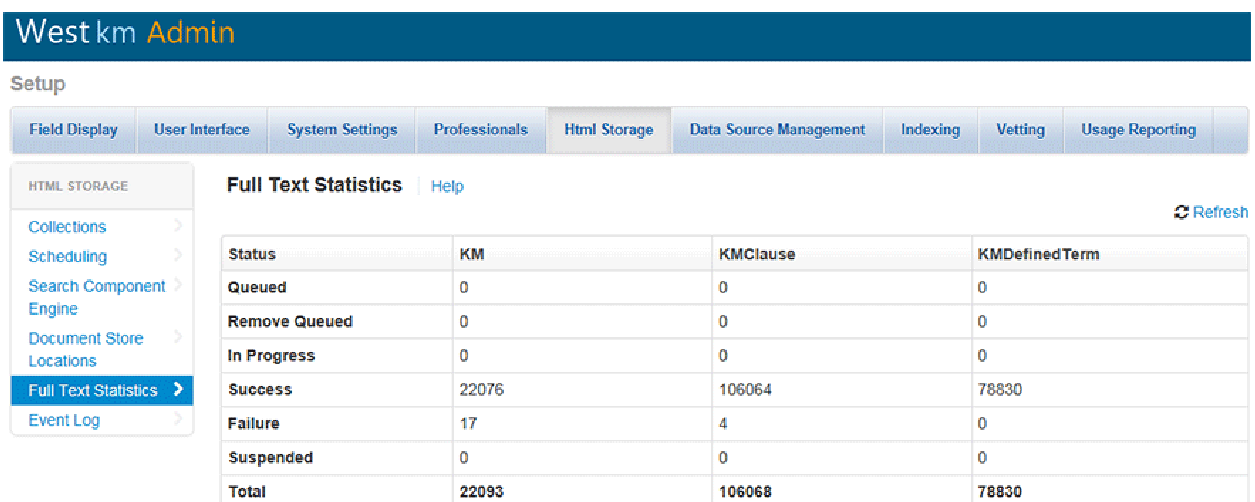
[1] Because of this logic, always have one active document indexed for each collection. If an active collection no longer contains any West km documents, delete the collection from West km to delete its documents.

To update the statistics while the synchronization process is running, click Refresh. (The page is not refreshed automatically.)

MONITORING FULL-TEXT INDEXING

To monitor the progress of full-text indexing,

1. Access the West km interface.
2. Click Setup.
3. Click the HTML Storage tab.
4. In the left frame, click Full-Text Statistics. The Full-Text Statistics page is displayed.



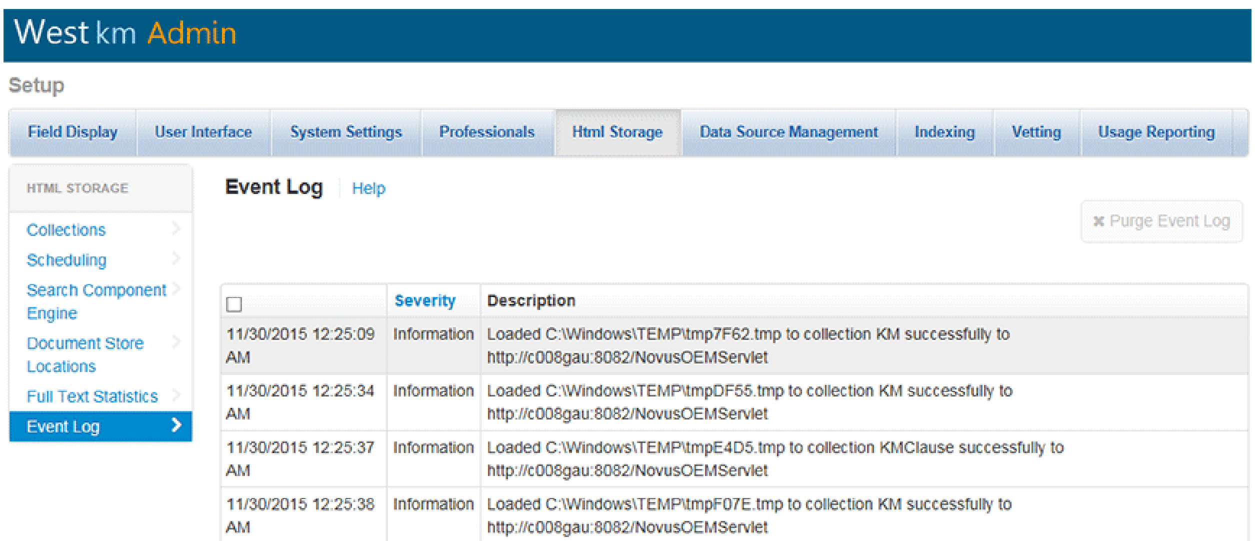
On the Full-Text Statistics page, each indexing collection is listed. Counts represent the number of documents in each status, which are described in the following table.

This status	Shows how many documents
Queued	Are currently scheduled and remain to be processed.
Removed Queued	Are currently scheduled for removal and remain to be processed.
In Progress	Are currently in process.
Success	Have processed successfully.
Failure	Have not been processed because of errors.
Suspended	Are on hold and will process when you run the Reindex All Content process. Documents are put in this state when you run the Clear Indexed Data process. For details, see "Manually Launching Full-Text Indexing Processes" on page 80.

To update the counts while full-text indexing is running, click **Refresh**. (The page is not refreshed automatically.)

View event log information for full-text indexing in one location. To view the event log for full-text indexing,

1. Access the West km interface.
2. Click **Setup**.
3. Click the **HTML Storage** tab.
4. In the left frame, click **Event Log**. The Event Log table is displayed.



Information and error events are logged for these activities:

- full-text indexing
- reclaiming
- searching

To change the sort order of the event log records, click a column heading (i.e., Severity) to sort by that category.

To clear the event log page and delete event log records from the West km database, click **Purge Event Log**.

Full-text indexing events are also logged in the Thomson West event viewer on the HTML repository/ search server. For instructions on accessing the Thomson West event log, see the following section, "Monitoring Program Events".

Monitoring Program Events

Events are logged in West km when significant milestones are reached during the indexing process or when an error occurs. Logging begins in the Thomson West event log when services are started. It records events for West km delivery, West km indexing services, the search service, and the document analysis service.

Events are categorized as information, warning, or error events. In particular, you should monitor the event viewer for error events, which indicate that a West km server component has failed a required function.

If you have a distributed architecture, event logs are created on the delivery server, indexing server, and HTML repository/search server. Event logs on the indexing server contain more specific indexing messages, which make up the bulk of event logging.

To access an event log,

1. On the appropriate server, click the **Start** button, click **Administrative Tools**, and then click **Event Viewer**.
2. In the Event Viewer window, click **Thomson West**.
3. To view more information about an event, double-click it.

Informational Events

Following are activities that cause informational events to be logged:

- The West km indexing service is started.
- The West km indexing service is stopped.
- Indexing of a document collection is started.
- Indexing of a document collection is finished.

Warning Events

Following are activities that cause warning events to be logged:

- A West km server component fails to read its configuration property for starting one of the West km services.
- The processing of a document failed.
- A worker thread was aborted because it received a stop service command while processing a document. This could occur because West km didn't have rights to read the document or the document couldn't be found.
- The indexer encounters a corrupt document. This occurs when a document fails to be converted to HTML within the configured time-out. In this instance, the service will automatically restart.
- Search logic retrieves too many documents, the search criteria are invalid, or a time-out exception occurs.

Error Events

Error events are logged when West km failures occur. Failures could occur for these reasons:

- The West km indexing service fails to extract a collection of documents from the document management system for indexing.
- A critical thread within the service has failed and the service needs to be restarted to function properly.
- A thread responsible for processing a group of documents fails.
- One of the West km services fails to start.
- The delivery server could not access or communicate with another West km server component, e.g., the West km database server, the indexing server, or the HTML repository/search server.

Using Trace Logs

If you encounter error events in the event log, you can use trace logs to gather additional information about program activity, allowing you to troubleshoot problems more effectively. This logging occurs while West km services are running.

To view a trace log, go to the location designated in the trace file's associated configuration file and open the log file in Notepad.

TRACE LOG LISTING

KM Cite Recognition Service Trace Log	
Log File[1]	*[Drive]*:\Program Files\Thomson\KM\logs\CitationService.xml
Description	Records activity on the KM Cite Recognition Service.
Configured in These Files	KM.CiteRecognitionService.exe.config (indexing server) and Logging.config.

KM Html Conversion Service Trace Log	
Log File	*[Drive]*:\Program Files\Thomson\KM\logs\HtmlService.xml
Description	Records activity on the KM Html Conversion Service.
Configured in These Files	M.HtmlConversionService.exe.config (indexing server) and Logging.config.
KM Indexing Service Trace Log	
Log File	*[Drive]*:\Program Files\Thomson\KM\logs\IndexingService.xml
Description	Records activity on the KM Indexing Service, including most of the indexing activity.
Configured in These Files	KM.IndexingService.exe.config (indexing server) and Logging.config.
KM Worker Service Trace Log	
Log File	*[West km installation folder]*\bin\Thomson.Westkm.WorkerService.log
Description	Records activity on the KM Worker Service.
Configured in These Files	KM.WorkerService.exe.config (indexing server) and Logging.config.
West km Monitor Service Trace Log	
Log File	*[Monitor Service installation folder]*\bin\monitor.log
Description	Records activity on the West km Monitor Service.
Configured in These Files	Thomson.Westkm.MonitorService.exe.config and Logging.config.
Elite Document Analyzer Trace Log	
Log File[3]	*[Document analyzer installation folder]*\logs\DocAnalysisService.log
Description	Records activity on the Elite Document Analysis service.
Configured in These Files	Elite.DocAnalysis.Service.exe.config (indexing server) and Logging.config.
Analyzer Component (Litigation) Trace Logs	
Log File Folder[4]	*[Analyzer component installation folder]*\dexter_logs
Description	dexter.log: Records all activity on the KM Entity Extraction Service. dextererror.log: Records errors on the KM Entity Extraction Service.
Configured in These Files	[Analyzer component installation folder]\Lib\log4j.properties (indexing server) and Logging.config.

[1] The default installation folder for West km is [Drive]:\Program Files\Thomson\KM.
[2] The default installation folder for the West km Monitor Service is [Drive]:\Program Files\Thomson\Westkm\Monitor.
[3] The default installation folder for the document analyzer is [Drive]:\Program Files\Thomson\DocAnalysis.
[4] The default installation folder for the analyzer component (Litigation) is [Drive]:\Program Files\Thomson\Dexter.

WEST KM AND ELITE TRACE LOGS

For the West km trace logs (i.e., those whose names begin with *KM* or *West km* in the previous section), you can control the level of activity that is recorded, the name and path of the trace log, and the maximum size and maximum number of log files that are created.

For the Elite trace log (i.e., the Elite Document Analyzer Trace Log), you can control the level of activity that is recorded, plus the name and path of the trace log.

Turn on the logs when necessary, view the log files, and then turn off the logs when you are finished troubleshooting. Because trace logs increase in size quickly, be sure to turn them off as soon as you are finished troubleshooting.

To access and change trace log settings,

1. Open the configuration file (listed in the previous section) in Notepad for the trace log you want to adjust. For the servers and locations associated with configuration files, see "Changing Configuration Files" on page 32.
2. To set the tracing level, locate the level property in the log4net section (root subsection), in the configuration file and change the value to correspond to the activity you'd like to record in the trace log. For example,

```
<log4net>
...
 <root>
 <level value="OFF"/>
 <appender-ref ref="KMEventLogAppender"/>
 <appender-ref ref="UIFileAppender"/>
</root></log4net>
```

Trace log values

Tracing Value
OFF (no tracing is logged)
FATAL
ERROR
WARN
INFO
DEBUG
ALL (all tracing is logged)

When you set a tracing level (e.g., WARN), it covers all higher levels of tracing as well (i.e., WARN, ERROR, and FATAL).

Note For the `Elite.DocAnalysis.Service.exe.config` file, use the `EliteSwitch` property to set the tracing level.

3. By default, 50 megabytes is the maximum size a log file is allowed to reach before being rolled over to backup files. To change the maximum file size, change the value of the `maximumFileSize` property in the log4net section, appending the letters “KB”, “MB”, or “GB” so that the size is interpreted respectively in kilobytes, megabytes, or gigabytes.
   `<maximumFileSize value="50MB" />`
4. Save the configuration file.
5. Stop and then start the associated West km service on the appropriate server for the configuration file. (For details on configuration files, see "Setting Document Sort Order" on page 31.)

ANALYZER COMPONENT TRACE LOGS

For the analyzer component (Litigation) trace log, you can control the level of activity that is recorded, plus the name and path of the trace log.

Turn on the logs when necessary, view the log files, and then turn off the logs when you are finished troubleshooting.

Note Because trace logs increase in size quickly, be sure to turn them off as soon as you are finished troubleshooting.

To access and change trace log settings for the analyzer component,

1. Open the log4j.properties configuration file in Notepad.
2. Locate the `Loggers` section in the configuration file.
3. Depending on the trace log you want to affect, change the value to another value option: off, debug, error, fatal, warn, info, or all.
   `log4j.logger.dexter=off, dexterloggingfilelog4j.logger.error=off, dextererrorfile`
4. To change the location and name of trace logs, locate these properties and change the path and file name.
   ```
   log4j.appender.dexterloggingfile.File=dexter_logs/dexter.log
   log4j.appender.dextererrorfile.File=dexter_logs/dextererror.log
   ```
5. Save the `log4j.properties` configuration file.
6. Stop and then start the KM Entity Extraction Service on the indexing server.

Reporting on Usage

You can track, query, print, export, and archive your organization’s West km usage data. Usage data includes the type and date of the West km document transaction, the user completing the transaction, and the related West km client ID (for billing allocation) and document number.

To access the Usage Reporting page to view West km usage data for your organization, complete these steps:

1. Open Internet Explorer and go to *hostname*`/km/pldefault.aspx,` where *hostname* is the name of your West km delivery server on your network.
2. Click the Setup link and then choose Usage Reporting.
3. Click the report you want to view in the *Summary Reports* list in the left frame, e.g., Detailed Report.

To display your usage data, enter your criteria in the text boxes at the top of the Usage Reporting page and click View Report. For details, see the following section “Querying Usage Data."

QUERYING USAGE DATA

To query your usage data, enter your criteria in the text boxes at the top of the Usage Reporting page for the report you are viewing and click Go. The transactions that match your criteria are displayed in the usage reporting table. (For a description of usage transactions, see the following section "Understanding Usage Transactions.")

- For the document number and West km client ID criteria, transactions whose values start with the letters you type will be found.
- For network ID, custom username, and name criteria, transactions whose values contain the letters you type will be found.
- For the date criteria, click the Calendar icon, click a date, and click OK.
- If you select the Cost Recovery check box, transactions that are most pertinent to cost recovery purposes are retrieved. Transactions designated for cost recovery purposes are indicated with a *Y* in the *Cost Recovery Y/N* column in the table in following section "Understanding Usage Transactions."
- If you choose an option from the Type of Usage drop-down list, transactions that apply only to a particular West km module (i.e., litigation, transactions) are retrieved.

To retrieve all usage transactions, clear any values in the text boxes and click Go.

To print the usage transactions you have retrieved, click Print Report.

To export data for the retrieved usage transactions to a file of comma-separated values, click Export Report. For more information, see the following section, "Querying Usage Data."

EXPORTING USAGE DATA

You can export data for the retrieved usage transactions to a file of comma-separated values. You can then open and compile that data in another program, such as Microsoft Excel, to create customized usage reports for your organization.

To export usage data, complete these steps:

1. Click Export Report in the right frame of a displayed usage report.
2. In the File Download dialog box that is displayed, click Save.
3. In the Save As dialog box, navigate to the folder where you want to save the file, type a new file name if you want to change the name, and click Save.

By default, the file name contains the date to prevent overwriting of previously exported data and for easy retrieval.

4. In the Download Complete dialog box (if displayed), click Close.

The usage data that is exported for the Detailed Report includes the following:

- Document number
- Client ID
- Name (full name)
- Cost Recovery
- Network ID
- Transaction
- Transaction description
- Source
- Date and Time

The usage data that is exported for the other reports corresponds to the data that is displayed onscreen.

If you intend to compile the data in Microsoft Excel, you can import the data in two ways:

- To open the data file and convert it automatically, use the Open command in Excel (from the File menu, choose Open).
- To open the data file using the Text Import Wizard, use the Import Data command in Excel (from the Data menu, choose Import External Data, and then choose Import Data). The wizard provides additional flexibility and options before converting the file. For example, you can choose not to import (skip) columns you don't need.

Note The data files are delimited with commas.

If you would like assistance in compiling your organization's usage data, call your West km representative at 1-888-WESTKM1.

ARCHIVING USAGE DATA

To purge usage data from the West km system and save it to another location, complete these steps:

1. Click **Archive Usage** in the *Tasks* list in the left frame of the Usage Reporting page.
2. On the Archive Usage page, enter a date in the **Date End** text box. To enter a date, click the **End Date** box, and click a date. The date you enter, along with the value in the **Date Start** text box, creates a date range of data to be archived.

The Date Start reflects the oldest usage data and cannot be modified.

3. To retrieve the usage data you want to archive, click **Go**.
4. Click **Create Archive**.
5. At the warning message, click **OK**.
6. In the File Download dialog box that is displayed, click **Save**.
7. In the Save As dialog box, navigate to the folder where you want to save the file, type a new file name if you want to change the name, and click **Save**.
8. In the Download Complete dialog box (if displayed), click **Close**.

For back-up purposes, a copy of the archive file is also saved on the West km delivery server from which the data was archived. It is saved in the Reports subfolder of the installation folder, e.g., D:\Program Files\Thomson\Westkm\Reports.

To view the archive history, click **Admin Usage** in the left frame of the Usage Reporting page, select **Archiving** from the **Type of Usage** drop-down list, and run the report. The table below lists the information that is tracked:

Item Tracked	Description
Date Time	The date and time archiving occurred.
Name	The person who performed the archiving activity.
Description	An explanation of the activity performed (i.e., archiving).
Usage Detail: FilePath	The path and file name to a back-up location of the archive file on the West km delivery server from which the data was archived. To open or save a copy of the back-up file, click the link.
Usage Detail: MachineName	The machine name of the West km delivery server from which the data was archived.
Usage Detail: UsageTimeSearch	The starting date from which usage data was archived.
Usage Detail: UsageTimeSearchEnd	The ending date at which usage data was archived.

UNDERSTANDING USAGE TRANSACTIONS

Usage Transaction	Explanation[1]	Cost Recovery Y/N	Transaction Description
KeyCite			
kmInsertFlags	In client software, the user clicks Insert or Update Flags and the entire document is processed	Y	West km Insert/Update KeyCite Flags
kmUpdateFlags	In Litigation client software, the user clicks Update Flags and the entire document is processed	Y	West km Update KeyCite Flags
kmKeyCiteLocate	In the West km user interface, the user restricts his or her West km KeyCite results using Search	N	West km KeyCite Locate
kmKeyCiteLocateExt	From an external client, the user restricts his or her West km KeyCite results by searching within a search	N	West km KeyCite Locate - External Client
kmLitigationKeyCiteSearchResults	In the West km user interface, the user views a KeyCite search result list	Y	West km KeyCite Search Results
kmKeyCiteSortResults	In the West km user interface, the user sorts a KeyCite result list	N	West km Litigation KeyCite Search - Sort
kmFilterKeyCiteSearchResults	In the West km user interface, the user restricts his or her KeyCite results using document metadata	N	West km KeyCite Filter
kmKeyCiteLimitsExt	From an external client, the user restricts his or her West km KeyCite results using document metadata	N	West km KeyCite Limits - External Client

Usage Transaction	Explanation[1]	Cost Recovery Y/N	Transaction Description
kmKeyCiteWL	In the WestlawNext interface, the user views West km citing references	Y	West km KeyCite - Westlaw
kmKeyCiteCountWL	In the WestlawNext interface, the user views a document and West km citing documents are found for that document	Y	West km KeyCite - Westlaw
View Document			
kmTransactionBrowse	In the West km interface, the user browses a Transactional library	Y	West km Transactions Browse
kmLitigationBrowse	In the West km interface, the user browses a Litigation library	Y	West km Litigation Browse
kmViewTransactionsClause	In the West km Transactions user interface, the user views an HTML representation of a clause	Y	West km Open Transactions Clause
kmViewTransactionsClauseExt	From an external client, the user clicks a clause link and views an HTML representation of a clause	Y	West km Open Transactions Clause - External Client
kmTransactionsClauseSummary	In the West km interface, the user views a clause summary	N	West km Open Transactions Clause Summary
kmTransactionsClauseSummaryExt	From an external client, the user views a clause summary	N	West km Open Transactions Clause Summary - External Client
kmViewTransactionsDefinedTerm	In the West km Transactions user interface, the user views an HTML representation of a defined term	Y	West km Open Transactions Defined Term
kmViewTransactionsDefinedTermExt	From an external client, the user clicks a defined term link and views an HTML representation of a defined term	Y	West km Open Transactions Defined Term - External Client
kmTransactionsDefinedTermSummary	In the West km interface, the user views a defined term summary	N	West km Open Transactions Defined Term Summary
kmTransactionsDefinedTermSummaryExt	From an external client, the user views a defined term summary	N	West km Open Transactions Defined Term Summary - External
kmViewLitigationDocumentExt	From an external client, the user clicks a Litigation document link and views an HTML representation of a document	Y	West km Open Litigation Document - External Client
kmViewLitigationDocument	In the West km Litigation user interface, the user views an HTML representation of a document	Y	West km Open Litigation Doc
kmLitigationDocumentSummary	In the West km interface, the user views a Litigation document summary	N	West km Open Litigation Summary
kmLitigationDocumentSummaryExt	From an external client, the user views a Litigation document summary	N	West km Open Litigation Document Summary - External Client
kmViewTransactionsDocument	In the West km Transactions user interface, the user views an HTML representation of a document	Y	West km Open Transactions Document
kmViewTransactionsDocExt	From an external client, the user clicks a Transactions document link and views an HTML representation of a document	Y	West km Open Transactions Document - External Client

Usage Transaction	Explanation[1]	Cost Recovery Y/N	Transaction Description
kmTransactionsDocumentSummary	In the West km interface, the user views a Transactions document summary	N	West km Open Transactions Document Summary
kmTransactionsDocumentSummaryExt	From an external client, the user views a Transactions document summary	N	West km Open Transactions Document Summary - External Client
kmTransactionsDocumentOutline	In the West km interface, the user views a Transactions document's Outline tab	N	West km Open Transactions Document Outline
kmTransactionsDocumentDefinedTerms	In the West km interface, the user views a Transactions document's Defined Terms tab	N	West km Open Transactions Document Defined Terms tab
kmTransactionsDocumentReferencedDocuments	In the West km interface, the user views a Transactions document's Referenced Documents tab	N	West km Open Transactions Document Referenced Documents tab
Load Copy of Document			
kmLoadCopyLitigation	In the West km user interface, the user clicks Open a copy of this document for a Litigation document, and the document is downloaded and displayed in its original format	Y	West km Load Copy - Litigation
kmLoadCopyLitigationExt	From an external client, the user clicks Load Copy, the native document is copied to the server from the DMS, and the document is displayed in its original format	Y	West km Litigation Load Copy - External Client
kmLoadCopyTransactions	In the West km user interface, the user clicks Open a copy of this document for a Transactions document, and the document is downloaded and displayed in its original format	Y	West km Load Copy - Transactions
Print Document/List			
kmPrintLitigationDocuments	In the West km interface, the user prints one or more Litigation documents using the Print command	Y	West km Print Litigation Documents
kmPrintLitigationList	In the West km interface the user prints a Litigation result list using the Print command	Y	West km Print Litigation Result List
kmPrintTransactionsDocuments	In the West km interface, the user prints one or more Transactions documents using the Print command	Y	West km Print Transactions Documents
kmPrintTransactionsList	In the West km interface, the user prints a Transactions result list using the Print command	Y	West km Print Transactions Result List
Email Document/List			
kmEmailLitigationDocument	In the West km interface, the user e-mails a Litigation document	Y	West km Email Litigation Document
kmEmailLitigationDocuments	In the West km interface, the user e-mails more than one Litigation documents from a result list	Y	West km Email Litigation Documents
kmEmailLitigationList	In the West km interface, the user emails a Litigation result list	Y	West km Email Litigation List

Usage Transaction	Explanation[1]	Cost Recovery Y/N	Transaction Description
kmEmailTransactionsDocument	West km Email Transactions Document In the West km interface, the user e-mails a Transactions document	Y	West km Email Transactions Document
kmEmailTransactionsDocuments	In the West km interface, the user e-mails more than one Transactions documents from a result list	Y	West km Email Transactions Documents
kmEmailTransactionsDefinedTermDocument	In the West km interface, the user e-mails a Transactions document containing a specific defined term	Y	West km Email Transactions Defined Term Document
kmEmailTransactionsDefinedTermDocuments	In the West km interface, the user e-mails more than one Transactions documents from a defined term result list	Y	West km Email Transactions Defined Term Documents
kmEmailTransactionsClauseDocument	In the West km interface, the user e-mails a Transactions document containing a specific clause	Y	West km Email Transactions Clause Document
kmEmailTransactionsClauseDocuments	In the West km interface, the user e-mails more than one Transactions documents from a clause result list	Y	West km Email Transactions Clause Documents
kmEmailTransactionsList	In the West km interface, the user emails a Transactions result list	Y	West km Email Transactions List
KeySearch			
kmKeysearch	In the West km user interface, the user performs a KeySearch search	Y	West km KeySearch
kmKeySearchBrowse	In the West km interface, the user opens a KeySearch folder	Y	West km KeySearch Browse
kmKeySearchLocate	In the West km user interface, the user restricts his or her KeySearch results using Search Within Results	N	West km KeySearch Locate
kmKeySearchSortResults	In the West km user interface, the user sorts a KeySearch result list	N	West km Litigation KeySearch - Sort
kmLitigationKeySearchSearchResults	In the West km user interface, the user views a KeySearch search result list	Y	West km Litigation KeySearch Results
kmFilterKeySearchResults	In the West km user interface, the user restricts his or her KeySearch results using document metadata	N	West km Litigation KeySearch Filter
kmKeySearchMIIMTask	On the Litigation tab, an information management task is performed (documents are removed from a topic or deleted) from a KeySearch result	N	West km Information Manager Update - KeySearch
General Search			
kmLitigationAndTransactionsSearch	In the West km interface, the user runs a search across both Litigation and Transactions content	Y	West km Search
kmClauseSearchLocateExt	From an external client, the user restricts his or her Clause search results by searching within a search	N	West km Clause Search Locate - External Client
kmFilterClauseSearchResultsExt	From an external client, the user restricts his or her Clause search results using document metadata	N	West km Clause Search Limits - External Client
kmDefinedTermLocateExt	From an external client, the user restricts his or her Defined Term search results by searching within a search	N	West km Defined Term Search Locate - External Client

Usage Transaction	Explanation[1]	Cost Recovery Y/N	Transaction Description
kmFilterDefinedTermSearchResultsExt	From an external client, the user restricts his or her Defined Term search results using document metadata	N	West km Defined Term Search Limits - External Client
Litigation Search			
kmLitigationSearch	In the West km interface, the user runs a search across Litigation content	Y	West km Search
kmLitigationSearchResults	In the West km user interface, the user views a Litigation search result	Y	West km Litigation Search Results
kmLitigationSearchFirmOnlyExt	From an external client, the user performs a full-text West km search on the organization's Litigation documents; the search completes and results are viewed	Y	West km Litigation Search - External Client
kmLitigationSearchFederatedWL	In the WestlawNext interface, the user performs a full text search on both West km documents and Westlaw documents	Y	West km Federated Litigation Search - Westlaw
kmViewResultListFederatedWL	In the WestlawNext interface, after the user performs a full-text search on both West km documents and Westlaw documents, the West km results are viewed	N	West km Federated Litigation Search Results
kmLitigationLocate	In the West km interface, the user restricts his or her Litigation search results using Search Within Results	N	West km Litigation Search Locate
kmLitigationSearchLocateExt	From an external client, the user restricts his or her West km search results by searching within a search	N	West km Litigation Search Locate - External Client
kmLitigationSortResults	In the West km user interface, the user sorts a Litigation result list	N	West km Litigation Search - Sort
kmLitigationFilterSearchResults	In the West km interface, the user restricts his or her Litigation search results using document metadata	N	West km Litigation Search Filter
kmLitigationFilterSearchResultsExt	From an external client, the user restricts his or her West km search results using document metadata	N	West km Litigation Search Limits - External Client
kmDeleteLitigationDocument	A Litigation document is deleted from a search result	N	West km Information Manager Update - Litigation Search Result
Transactions Search			
kmTransactionsSearch	In the West km interface, the user runs a search across Transactions content	Y	West km Search
kmTransactionsLocate	In the West km interface, the user restricts his or her Transactions document search results using Search Within Results	N	West km Transactions Search Locate
kmTransactionsDocumentSearchResults	In the West km user interface, the user views a Transactions document search result	Y	West km Transactions Document Search
kmTransactionsDocumentSearchExt	From an external client, the user performs a search (basic or advanced) for Transactions documents; the search completes and results are viewed	Y	West km Transactions Document Search - External Client

Usage Transaction	Explanation[1]	Cost Recovery Y/N	Transaction Description
kmTransactionsDocumentSortResults	OIn the West km user interface, the user sorts a Transactions document result list	N	West km Transactions Document Search - Sort
kmTransactionsDocumentSearchLocateExt	From an external client, the user restricts his or her Transactions document search results by searching within a search/P>	N	West km Transactions Document Search Locate - External Client
kmTransactionalDocumentFilterSearchResults	In the West km interface, the user restricts his or her Transactions document search results using document metadata	N	West km Transactions Document Search Filter
kmTransactionsFilterDocumentSearchResultsExt	From an external client, the user restricts his or her Transactions document search results using document metadata	N	West km Transactions Document Search Limits - External Client
kmTransactionsClauseSearchResults	In the West km user interface, the user views a clause search result	Y	West km Transactions Clause Search
kmTransactionsClauseSearchExt	From an external client, the user performs a search (basic or advanced) for clauses; the search completes and results are viewed	Y	West km Transactions Clause Search - External Client
kmTransactionsClauseSortResults	In the West km user interface, the user sorts a Transactions clause result list	N	West km Transactions Clause Search - Sort
kmTransactionalClauseLocateSearchResults	In the West km interface, the user restricts his or her Transactions clause search results using Search Within Results	N	West km Transactions Clause Search Locate
kmTransactionalClauseFilterSearchResults	In the West km interface, the user restricts his or her Transactions clause search results using document metadata	N	West km Transactions Clause Search Filter
kmTransactionsDefinedTermSearchResults	In the West km user interface, the user views a defined terms search result	Y	West km Transactions Defined Term Search
kmTransactionsDefinedTermSearchExt	From an external client, the user performs a search (basic or advanced) for defined terms; the search completes and results are viewed	Y	West km Transactions Defined Term Search - External Client
kmTransactionalDefinedTermLocateSearchResults	In the West km interface, the user restricts his or her Transactions defined term search results using Search Within Results	N	West km Transactions Defined Term Search Locate
kmTransactionsDefinedTermSortResults	In the West km user interface, the user sorts a Transactions defined terms result list	N	West km Transactions DefinedTerm Search - Sort
kmTransactionalDefinedTermFilterSearchResults	In the West km interface, the user restricts his or her Transactions defined term search results using document metadata	N	West km Transactions Defined Term Search Filter
kmDeleteTransactionsDocument	A Transactions document is deleted from a search result	N	West km Information Manager Update -

Usage Transaction	Explanation[1]	Cost Recovery Y/N	Transaction Description
			Transactions Search Result
Other Administrative Transactions			
EditVettingDisplay	Change Vetting Display	N	Change Vetting Display
TestVettingRule	Test Vetting Rule	N	Test Vetting Rule
DeleteVettingRule	Delete Vetting Rule	N	Delete Vetting Rule
VettingIncludeDoc	Vetting - Include Document	N	Vetting - Include Document
VettingExcludeDoc	Vetting - Exclude Document	N	Vetting - Exclude Document
EditVettingRuleGroups	Edit Vetting Group	N	Edit Vetting Group
EditVettingField	Edit Vetting Field	N	Edit Vetting Field
DeleteVettingField	Delete Vetting Field	N	Delete Vetting Field
DeleteVettingRuleGroups	Delete Vetting Group	N	Delete Vetting Group
ChangeGlobalDateBoolean	Apply or Remove Global Date Restriction	N	Apply or Remove Global Date Restriction
GlobalDateRestrictionChange	Change Global Date Restriction	N	Change Global Date Restriction
AddVettingRuleGroups	Add Vetting Group	N	Add Vetting Group
AddVettingField	Add Vetting Field	N	Add Vetting Field
AddVettingRule	Add Vetting Rule	N	Add Vetting Rule
EditVettingRule	Edit Vetting Rule	N	Edit Vetting Rule
DeleteUser	Delete User	N	Delete User
DeleteGroup	Delete Group	N	Delete Group
EditGroupPermissions	Edit Group	N	Edit Group
ExportUsers	Export Usere	N	Export User
EditUserPermissions	Edit User	N	Edit User
AddUser	Add User	N	Add User
AddUsersFromActiveDirectory	Add Users from Active Directory	N	Add Users from Active Directory
AddGroup	Add Group	N	Add Group
UpdatedVersion	Upgrade	N	Upgrade
ChangeProductKey	Change Product Key	N	Change Product Key
ChangeHiddenOptions	Change Hidden Options	N	Change Hidden Options
ChangeSystemOptions	Change System Settings	N	Change System Settings
RemoveIndexingServer	Remove Indexing Server	N	Remove Indexing Server
AddIndexingServer	Add Indexing Server	N	Add Indexing Server
IndexingProcessByComponent	Process By Component	N	Process By Component
SuspendIndexingComponent	Suspend Component	N	Suspend Component
AddServiceWindow	Add Service Window	N	Add Service Window
EditServiceWindow	Edit Service Window	N	Edit Service Window
EditTempIndexingDirectory	Edit Temp Directory	N	Edit Temp Directory
EditCollection	Edit Collection	N	Edit Collection
DeleteCollection	Delete Collection	N	Delete Collection
DeleteServiceWindow	Delete Service Window	N	Delete Service Window
AddCollection	Add Collection	N	Add Collection
EditConnection	Edit Connection	N	Edit Connection
DeleteConnection	Delete Connection	N	Delete Connection
AddConnection	Add Connection	N	Add Connection
ArchiveUsage	Archive Usage	N	Archive Usage

Usage Transaction	Explanation[1]	Cost Recovery Y/N	Transaction Description
ScheduleBulkJob	Schedule Bulk Job	N	Schedule Bulk Job
ScheduleIncrementalJob	Schedule Incremental Job	N	Schedule Incremental Job
SetPriorityFlag	Set Priority Flag	N	Set Priority Flag
SetProfileMetaDataFlag	Set Profile MetaData Flag	N	Set Profile MetaData Flag
SetCiteRecognitionFlag	Set Cite Recognition Flag	N	Set Cite Recognition Flag
SetClassificationFlag	Set Classification Flag	N	Set Classification Flag
SetLitigationAnalysisFlag	Set Litigation Analysis Flag	N	Set Litigation Analysis Flag
SetLitigationStorageFlag	Set Litigation Storage Flag	N	Set Litigation Storage Flag
SetTransactionalAnalysisFlag	Set Transactional Analysis Flag	N	Set Transactional Analysis Flag
SetTransactionalStorageFlag	Set Transactional Storage Flag	N	Set Transactional Storage Flag
ClearForcedJobs	Clear Forced Jobs	N	Clear Forced Jobs

[1] Client software refers to West BriefTools and the West km Add-In Tool.

The *Report Units* column is displayed in the usage reporting table and is contained in exported reports. This column indicates the number of countable transactions at the document level. For example, if the transaction kmPrintLitigationDocsMI or kmPrintLitigationDocsWL indicates a unit number of 5, then five documents were printed. If kmInsertFlags indicates a unit number of 1, then KeyCite status flags were inserted in one word-processing document.

Reporting on Administrative Changes

You can track, print, and export the changes that have been made to the system by your organization's West km administrators. Data includes the name of the person who made the change, the date, and a detailed description of the change.

To access the administrator usage reports, complete these steps:

1. Open Internet Explorer and go to *hostname*`/km/pldefault.aspx`, where `hostname` is the name by which your West km delivery server is known on your network.
2. Click the Setup link and then choose Usage Reporting.
3. Click Admin Usage in the left frame.
4. Enter your criteria in the text boxes at the top of the Admin Usage page.
   - For the date criteria, click the Calendar icon, click a date, and click OK.
   - If you select an option other than All from the Type of Usage and Specific Usage drop-down lists, administrative changes applying to those categories are retrieved. For a description of the usage types, see the following table.
5. Click Search. The administrative changes that match your criteria are displayed in the admin usage table.

To retrieve all changes, clear any values in the text boxes and click Search.

To print the list of changes you have retrieved, click Print Report.

To export data the data you have retrieved to a file of comma-separated values, click Export Report. For details, see "Reporting on Usage" on page 99.

Type of Usage	Description
Administer Fields	A field defined in the vetting toolkit from your DMS is added, changed, or deleted.
Vetting Display	The display of fields in the vetting toolkit is changed.
Administer Rule Groups	A rule group is added, edited, or deleted, or the global exclusionary rule group has been applied or removed from a rule group in the vetting toolkit.
Vetting Groups	Any of the following changes to a vetting rule in the vetting toolkit: • a vetting rule is added, edited, or deleted

Type of Usage	Description
	• the global date restriction is changed • the global date restrictions is applied or removed
Vetting Docs	A document is excluded from the vetting collection or an excluded document is restored from the vetting collection in the vetting toolkit.
DMS Connection	A data source connection is added, changed, or deleted.
Indexing Options	Indexing of a document collection is manually launched, or a document collection is added or edited.
Indexing Server	Any of the following changes to the setup of the indexing server: • the temp directory is updated • a server is added or deleted • a service window is added, edited, or deleted • an indexing component is suspended • the "process by component" option is changed for an indexing component
Upload Files	A file is added, removed, or uploaded in the West km Web-hosted application.
Professionals	A West km professional profile is added or edited, or the list of professionals is exported.
Archiving	Usage data is purged from the West km system and saved to another location.
System Options	A value is changed for a system option.
Update Versions	The product key is changed or the version of a West km software component is changed due to an upgrade.
Hidden Options	A value is changed for a system option that is accessible only by West km Technical Support.

10 Maintaining West km

To maintain West km, you can manually classify one or more documents to KeySearch topics, remove documents from KeySearch topics, add notes to a document, mark a document exemplar, edit all annotations in the West km interface, permanently delete one or more documents from the system, and observe a number of maintenance best practices.

Managing Documents in KeySearch

As a KeySearch editor in West km, you can do the following in West km for Litigation:

- manually assign documents to a KeySearch topic
- manually remove a document from a KeySearch topic

CLASSIFYING DOCUMENTS TO KEYSEARCH TOPICS

After your organization's documents are indexed in West km, you can manually classify one or more documents to KeySearch topics. Classifying a document to a KeySearch topic ensures that the document appears in the result list when a West km user accesses that topic.

To manually classify documents to KeySearch topics,

1. In the West km interface, generate a result list of your organization's documents.
2. In the result list, select the check box preceding each document that you want to classify to KeySearch topics. To select all documents in the result list, select the Select all items check box at the top of the result list.
3. Click Actions at the top of the page, and then click Classify Selected Documents.
4. In the Select Topics dialog box, select the check boxes for the KeySearch topics to which you want the documents classified and click Save.

If a document collection containing a manually classified document is re-indexed, the document stays classified to the topics you've specified.

Note If you manually classify a document to a topic, the document count for that topic is not updated until the end of the indexing time window.

REMOVING A DOCUMENT FROM A KEYSEARCH TOPIC

After your organization's documents are indexed in West km, you can manually remove a document from a KeySearch topic. Removing a document from a KeySearch topic ensures that the document will not appear in the result list when a West km user at your organization accesses that topic.

To manually remove a document from a KeySearch topic, access the document's summary page and then click the Remove icon next to the listed KeySearch topic.

If a document collection containing a manually removed document is re-indexed and CaRE is enabled, the document will be reclassified.

Note If you manually remove a document from a topic, the document count for that topic is not updated until the end of the indexing time window.

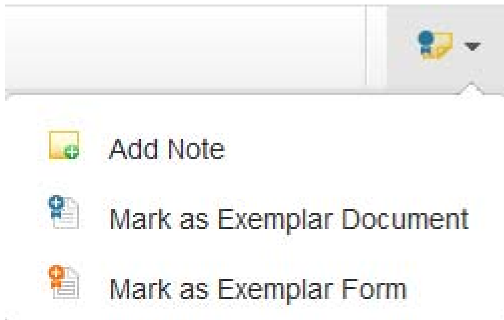
Annotating Documents

If you are an annotator in West km, you can add notes to a document, mark a document exemplar, and edit all annotations in the West km interface. Other West km users can view your annotations.

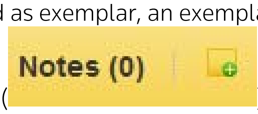
Note In West km for Transactions, notes and exemplar markings you add to a document are also viewable from all clauses and defined terms originating from that document.

To annotate a document,

1. When you are viewing the text or summary of a document in the West km interface, click the Annotations icon at the top of the document.



2. Do one of the following:
   - To mark the document as an exemplar document, click Mark As Exemplar Document.
   - To mark the document as an exemplar form, click Mark As Exemplar Form.
   - To add note, click Add Note, type your note in the text box, and click Save.

If a document is marked as exemplar, an exemplar icon () is displayed next to the document title. If a note is added to a document, a Notes bar (

) is displayed at the top of the document. To view the note, click the Notes bar.

To remove an exemplar marking from a document, click the Annotations icon at the top of the document and then click either Unmark As Exemplar Document or Unmark As Exemplar Form.

To edit an existing note for a document, click the Expand icon in the Notes bar at the top of the document, click the note text, make your changes, and click Save.

To delete an existing note for a document, click the Expand icon in the Notes bar at the top of the document, click the note text, and then click the red X.

When changes are made to a document's annotations, the document is flagged for a profile metadata update at the next incremental update. In order for searches on annotations to work, indexing and full- text indexing are required.

Deleting Documents

As an administrator in West km, you can permanently delete one or more documents from the system using the West km interface.

You should delete no more than 10 documents at a time via the West km interface because it is time consuming. The preferred method is to remove documents from West km by either deleting the documents from your organization's file system or by modifying your defined document collections to exclude the documents.

Note When you delete documents via the West km interface, they cannot be re-added to West km unless you add a new data source connection and define and index a document collection containing that document.

To delete documents from West km,

1. In the West km interface, generate a result list of your organization's documents.
2. In the result list, select the check box preceding each document you want to delete from West km. To select all documents in the result list, select the Select all items check box at the top of the result list.
3. Click Actions at the topic of the page, and then click Delete Selected Documents from West km.
4. At the confirmation message, click OK.

The document is deleted immediately from West km. To see a count and listing of all documents that have been deleted from West km, access the Sync page at Setup, Statistics. For details, see "Synchronizing Document Collections" on page 78.

Note If you delete a document from West km that was assigned to a KeySearch topic, the document count for that topic is not updated until the end of the indexing time window.

System Maintenance

For optimal performance and as a standard precaution, it is recommended that you observe the following best practices for maintaining your West km system. In the event of a conflict with your organization's established best practices, adhere to your own best practices.

WEST KM-SPECIFIC BEST PRACTICES FOR MAINTENANCE

Task	Frequency	West km Location
Verify vetting	Daily (or based on service window settings)	Setup, Vetting, Statistics
Verify incremental indexing	Daily (or based on service window settings)	Setup, Indexing, Indexing Results
Verify synchronization	Daily (or based on service window settings)	Setup, Indexing, Sync Information
Verify full-text indexing	Daily (or based on service window settings)	Setup, HTML Storage, Full-Text Statistics
Monitor West km logs in the event viewer for any errors or issues	Daily	Computer Management, Event Viewer, Thomson West
Add and modify users	As needed	Setup, Professionals
Verify the core functionality of West km (e.g., document retrieval by citation, term searching, WestlawNext integration)	Weekly	Run searches in the WestlawNext and West km interfaces (Litigation and Transactions tabs)

GENERAL MAINTENANCE BEST PRACTICES

Task	Frequency
Monitor the system, security, and application event viewers for errors.	Daily
Back up and monitor SQL databases.	Daily
Back up files. As well as West km databases, back up the following West km items: • documents in the HTML storage locations • index files of the search component • West km installation folder and all subfolders Backups of the databases, the HTML storage locations, and the index files must be synchronized. To ensure data integrity, you must restore these items from backups with the same date and time. It is also recommended that you perform complete system backups that include the registry and file system in the event of a hard disk failure.	Daily
Optimize SQL by performing the following SQL database maintenance tasks: • check database integrity • rebuild indexes • update statistics When setting up database maintenance operations for West km databases, observe these guidelines: • Begin weekly maintenance after you initially index your document collections. • Perform maintenance operations after indexing a large number of documents with the document analyzer. • Do not perform maintenance operations while indexing, synchronization, or full-text indexes processes are running. (Therefore, schedule database maintenance outside the indexing service windows for the	Weekly

Task	Frequency
document indexing window and the document sync window and outside the indexing time windows in the search service.)	
Verify data backups. Restore backups to a test system to ensure your backup strategy and restores will work when needed.	Monthly
Monitor and install patches.	Weekly
Monitor disk space to ensure you have adequate space on all drives. The recommended level is at least 25 percent free space.	Weekly
Defragment disk drives as follows (from Microsoft). • **Analyze before defragmenting a volume**: Analyze volumes before defragmenting them. After analyzing a volume, a dialog box tells you the percentage of fragmented files and folders on the volume and recommends whether to defragment the volume. Analyze volumes regularly and defragment them only when Disk Defragmenter recommends it. A good guideline is to analyze volumes at least once a week. If you seldom need to defragment volumes, analyze volumes monthly instead of weekly. • **Analyze after large numbers of files are added**: Volumes might become excessively fragmented when users add a large number of files or folders, so be sure to analyze volumes after this happens. Generally, volumes on busy file servers should be defragmented more often than those on single-user workstations. • **Ensure that your volume has at least 15 percent free space**: A volume must have at least 15 percent free space for Disk Defragmenter to completely and adequately defragment it. Disk Defragmenter uses this space as a sorting area for file fragments. If a volume has less than 15 percent free space, Disk Defragmenter will only partially defragment it. To increase the free space on a volume, delete unneeded files or move them to another disk. Defragment during low-usage periods. • **Defragment during low-usage periods**: Defragment file server volumes during low-volume usage periods to minimize the effect that the defragmentation process has on file server performance. The time that Disk Defragmenter takes to defragment a volume depends on several factors, including the size of the volume, the number of files on the volume, the number of fragmented files, and available system resources. • **Defragment after installing software or installing Windows**: Defragment volumes after installing software or after performing an upgrade or clean install of Windows. Volumes often become fragmented after installing software, so running Disk Defragmenter helps to ensure the best file system performance.	Weekly
Assess any environment changes (e.g., DMS updates, network changes, server updates) that may impact West km.	As needed
Check for West km updates and upgrade the system if needed.	Quarterly

11 Appendix A: Running Database Scripts Manually

During installation of a software component that requires updates to a West km database, you can opt to have the Setup program run SQL scripts to update the database, or you can opt to run the scripts yourself manually.

If you opted to run database scripts manually, then you must complete the steps in this appendix to update West km databases. On the other hand, if you opted to let the installation run database scripts, then your databases are already updated and you can skip this appendix.

Note If you have a distributed environment, you must access most West km script files on the delivery server. Either copy the script files from the delivery server or create a share.

Running Scripts for the Search Component

If you chose not to update databases during installation of the search component, the updates have to be performed after installation or the search component cannot be used.

To update the databases separately, do the following in the order listed:

- Use the administrative page at http://localhost:8082/admin/config/database to submit any missing or changed database information. (This step is necessary only if there are changes to the database server, database names, and database username and password.)
- Run two scripts in a DOS window at the root of the installed folder to (1) update the databases, and (2) install the search component defaults (see the following examples). If the installation ran without updating databases, then the scripts can be obtained from the installation log file at *[search component installation folder]*`\Thomson\novus\logs\novusoem_install.YYYYMMDD_HHMMSS.log`.

Sample script to update database:

```
"D:\oeminstall\Thomson\Novus\java\jre\bin\javaw" -
Dxml.config.file.path="D:\oeminstall\Thomson\Novus\conf\NovusConfi g.xml" -Dnovusldaprepository=off -
Djava.ext.dirs="D:\oeminstall\Thomson\Novus\lib\novus;D:\oeminstal
l\Thomson\Novus\lib\system;D:\oeminstall\Thomson\Novus\lib\endorse
d;D:\oeminstall\Thomson\Novus\lib\db\sqlserver2005;" com.westgroup.novus.oem.install.OemInstall
D:\oeminstall\Thomson\Novus D:\oeminstall\Thomson\Novus\scripts\script.xml sqlserver2005 CCI DOC PERSIST
```

Sample script to install search component defaults:

```
"D:\oeminstall\Thomson\Novus\java\jre\bin\javaw" -
Dxml.config.file.path="D:\oeminstall\Thomson\Novus\conf\NovusConfi g.xml" -
Djava.ext.dirs="D:\oeminstall\Thomson\Novus\lib\novus;D:\oeminstal
l\Thomson\Novus\lib\db\sqlserver2005;D:\oeminstall\Thomson\Novus\l ib\system"
com.westgroup.novus.cci.CciUtility cdns "D:\oeminstall\Thomson\Novus\defaults\novusdefaults.zip"
```

Running Scripts for West km and CaRE

1. To manually run a database script in Microsoft SQL Server,
2. On a database server, click the Start button, click All Programs, click Microsoft SQL Server 2008 R2, and then click SQL Server Management Studio.
3. In the Connect to Server dialog box, verify the default settings, and then click Connect.
4. In the Object Explorer section of the SQL Server Management Studio window, connect to the SQL server that contains the West km databases.
5. In the SQL Server Management Studio window, from the File menu, click Open, and then click File.
6. In the Open File dialog box, go to the script file location for the script you want to run, select it, and click Open.
7. In the Connect to Database Engine dialog box, type or select the name of your SQL server, verify the default authentication and logon settings, and then click Connect. (Your logon account must be assigned to the dbcreator server role or higher.)
8. Click the Execute button on the toolbar.
9. Repeat steps 4-7 for each script you want to run.
10. Close the SQL Server Management Studio window.

Listing of Scripts

Script File	Description	Subfolder in West km Installation Folder[1]
km.sql	populates the km database	DB

[1] The default installation folder for West km is [Drive]:\Program Files\Thomson\KM. Scripts are available on the delivery server.

CaRE scripts

Script File	Description	Subfolder in West km Installation Folder[1]
ScriptImport_KSH.sql	imports KeySearch data	Db
kshupdate.sql	fixes KeySearch node errors	db

[1] The default installation folder for CaRE is [Drive]:\Program Files\Thomson\Westkm\Care. The CaRE scripts are available on any server with the West km CaRE engine installed.

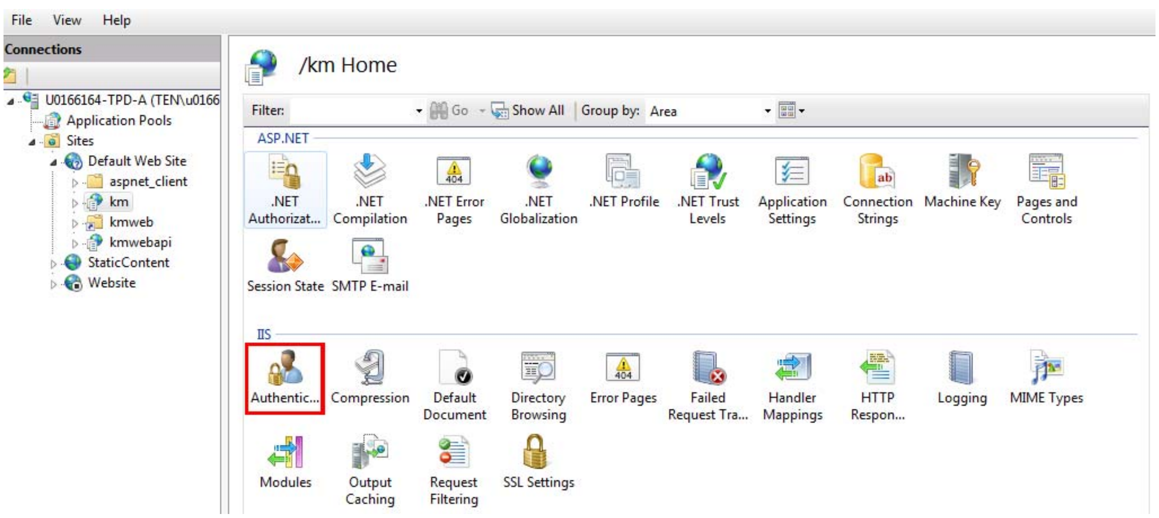
12 Appendix B: Changing the Authentication Method

West km automatically configures itself and IIS for the authentication method you select during installation. This document explains how to change the authentication method after installation.

Setting the IIS Authentication Method

Complete these steps on the West km delivery server.

1. Click the **Start** button, choose **Programs**, choose **Administrative Tools**, and then choose **Internet Information Services (IIS) Manager**.
2. In the left frame of the Internet Information Services (IIS) Manager window, expand the server name, the **Sites** item, and the **Default Web Site** item, and click **km**.
3. In the main window, under the IIS section, double-click **Authentication**.
4. In the Authentication Methods dialog box, do the following in accordance with your West km authentication method:
   - If you are using IWA, verify that **Integrated Windows Authentication** is enabled.
   - If you are using West km custom authentication, verify that Anonymous Authentication is enabled and credentials are entered (by default, the Internet Guest Account is used).



Changing the Configuration File Property

In the Web.config file, locate the "membership" and "roleManager" properties. Each will have two options for authentication ("FormsAuthentication" and "WindowsAuthentication"), one of which will be commented out with "!--" as shown below.

Membership:

```
<membership defaultProvider="WindowsAuthenticationMembershipProvider"><providers>
<clear />
<!--<add
name="FormsAuthenticationMembershipProvider"type="KM.UI.Business.Membership.FormsAuthenticationMembershi
pProvider, KM.UI" userIsOnlineTimeWindow="30" connectionStringName="MembershipServices"
enablePasswordRetrieval="false" enablePasswordReset="true" requiresQuestionAndAnswer="false"
requiresUniqueEmail="true" maxInvalidPasswordAttempts="5" minRequiredPasswordLength="6"
minRequiredNonalphanumericCharacters="0" passwordAttemptWindow="10" applicationName="/" />


-->


<add name="WindowsAuthenticationMembershipProvider"
type="KM.UI.Business.Membership.WindowsAuthenticationProvider, KM.UI"
connectionStringName="ActiveDirectoryServices"
```

13 Appendix C: West km Ports

The ports used by West km are listed below. You may need to change port settings if a conflict exists with another service already using that port or if a firewall blocks a port.

In addition, for communication to occur between West km and Westlaw servers, your West km servers must allow HTTP and port 80 access through your firewall to these URLs:

- kcflags.westlaw.com
- rid.westlaw.com
- web2.westlaw.com
- westkmservices.westlaw.com

Database Management Server Ports

1433 Microsoft SQL Server's default port

Note Microsoft SQL Server must be configured to use a static port.

West km Ports

5050	CaRE Indexing Doc Server Port
5364	PLDmsServicePort TaskCompilerPort
8082	Search component port
8085	Bulk Load Controller Port Profile Sync Controller Port indexer_VettingSyncControllerPort
8086	indexer_IndexingHelperControllerPort
8087	indexer_HtmlSearchControllerPort
8088	indexer_QuickSiftControllerPort
8089	Elite Document Analysis service port
8091	MonitorServiceControllerPort
8101	KM Search Service port
8093	indexer_IndexingWorkerControllerPort
8094	KM Entity Extraction Service port

14 Appendix D: Authentication and Document Security Configuration

Depending on your document management system (DMS) and West km authentication method, the following table lists the configuration that is required for West km document security and authentication to function properly.

For more information about:

- Selecting an authentication method for West km, see the West km Administrator Installation Guide.
- Administering West km users in the Professionals table, see "Managing Users" on page 85.
- Controlling access to your West km documents via the document security implemented in your DMS, see "Changing System Settings" on page 21.

Note All NTFS documents are treated as public in West km.

DMS	West km Security Model	Configuration Details
eDOCS DM	IWA	The Network ID in the Professionals table must match the Windows network ID (qualified by domain) for each user.
eDOCS DM	Custom	Each user must have a custom user name and custom user password in the Professionals table. To use the Full or Always Display Titles document security, the Network ID in the Professionals table must match the Windows network ID (qualified by domain) for each user.
iManage Work	IWA	The DMS library information in Data Source Management must contain an admin username and password. The Network ID field in the Professionals table must match the Windows network ID (qualified by domain) for each user. If iManage Work is configured to use virtual usernames, one of the following must be configured: • All users must have their iManage Work virtual usernames entered into the Professionals table, and West km must be configured at Setup, Data Source Management, Settings, iManage Work. *User ID Required* must be selected to enable this field. This configuration relies on West km logic to apply document level security. • All users must have their iManage Work virtual usernames and passwords entered into the Professionals table. *User ID Required* and *User Password Required* must be selected to enable these fields. This configuration relies on iManage Work to apply security. Note that if a user changes his or her iManage Work password, it must also be changed in the Professionals table.
iManage Work	Custom	The DMS Library information in Data Source Management must contain an admin username and password. Each user must have a custom user name and custom user password in the Professionals table. If iManage Work is configured to use virtual usernames, one of the following must be configured: • All users must have their iManage Work virtual usernames entered into the Professionals table, and West km must be configured at Setup, Data Source Management, Settings, iManage Work. *User ID Required* must be selected to enable this field. This configuration relies on West km logic to apply document level security. • All users must have their iManage Work virtual usernames and passwords entered into the Professionals table. *User ID Required* and *User Password Required* must be selected to enable these fields. This configuration relies on iManage Work to apply security. Note that if a user changes his or her iManage Work password, it must also be changed in the Professionals table. If iManage Work is configured to use network usernames,

DMS	West km Security Model	Configuration Details
		• The Network ID in the Professionals table must match the network ID for each user.
NetDocuments	IWA	The Network ID in the Professionals table must match the Windows network ID (qualified by domain) for each user. To use NetDocuments document security, all users must have a NetDocuments user GUID entered in the DMS UserID field in the Professionals table. (To enable this field, the *User ID Required* settings must be selected.) NetDocuments user GUIDs are not required to be unique. You can enter the same user GUID for multiple West km users.
NetDocuments	Custom	Each user must have a custom user name and custom user password in the Professionals table. To use NetDocuments document security, all users must have a NetDocuments user GUID entered in the DMS UserID field in the Professionals table. (To enable this field, the *User ID Required* settings must be selected.) NetDocuments user GUIDs are not required to be unique. You can enter the same user GUID for multiple West km users.
NTFS	IWA	The Network ID in the Professionals table must match the Windows network ID (qualified by domain) for each user.
NTFS	Custom	Each user must have a custom user name and custom user password in the Professionals table.
ProLaw	IWA	The Network ID in the Professionals table must match the Windows network ID (qualified by domain) for each user.
ProLaw	Custom	The Network ID in the Professionals table must match the network ID or Windows network ID (qualified by domain) for each user. Each user must have a custom user name and custom user password in the Professionals table.

15 Appendix E: West km–DMS Field Mappings

Following are the fields that West km uses by default from your document management system.

West km Field	eDOCS DM	iManage Work[1]	ProLaw	NTFS
Abstract	profile.abstract	imProfileComment	Notes	*not available*
Author	people.full_name	Author	*configurable*[2]	*not available*
Client ID	client.client_id[3]	Client	parsed from the matter ID	*not available*
Client Name	client.client_name[3]	imProfileCustom1 Description	Matters.ClientSort	*not available*
Doc No	profile.docnumber	DocNum	DocNo	*not available*
Document Type	documenttypes.description	Extension	Type	*not available*
Created Date Time	profile.creation_date +z profile.creation_time	VersionCreationDate	Events.EventDate	created datetime
Matter ID	matter.matter_id[3]	Matter	Matters.MatterID	*not available*
Matter Name	matter.matter_name[3]	imProfileCustom2 Description	Matters.ShortDesc	*not available*
Modified Date Time	profile.last_edit_date + profile.last_edit_time	EditDate	Modified date is pulled from the physical	modified datetime
Title	Document Name	Description	Notes	document name
Version	versions.version *or* versions.versions + versions.subversions *(if using subversions)*	Version	*not available*	*not available*

[1] For iManage Work, you can override the default field mapping for the Abstract, Author, Client ID, Client Name, Document Type, Matter ID, Matter Name, and Title fields. Override mappings by adjusting the DMS settings at Setup, Data Source Management, Settings, iManage Work (see "Changing Data Source Settings" on page 24 for more information). For the West km field whose mapping you want to change, type the Caption of the iManage Work field that you want to use. To change the mapping for Document Type, contact your West km representative.

[2] The Author field is configurable in ProLaw and can be the professional that is modifiable via the user interface or the professional who added the document.

[3] This is the default field. It can be customized.

16 Index