



FileHold

Document & Record Lifecycle Software

LIBRARY ADMINISTRATION GUIDE

VERSION 15.1

Copyright ©2016 FileHold Systems Inc. All rights reserved.

For further information about this manual or other FileHold Systems products, contact us at Suite 250 - 4664 Lougheed Highway Burnaby, BC, Canada V5C5T5, via email sales@filehold.com, our website www.filehold.com, or call 604-734-5653.

FileHold is a trademark of FileHold Systems. All other products are trademarks or registered trademarks of their respective holders, all rights reserved. Reference to these products is not intended to imply affiliation with or sponsorship of FileHold Systems.

Proprietary Notice

This document contains confidential and trade secret information, which is proprietary to FileHold Systems, and is protected by laws pertaining to such materials. This document, the information in this document, and all rights thereto are the sole and exclusive property of FileHold Systems, are intended for use by customers and employees of FileHold Systems, and are not to be copied, used, or disclosed to anyone, in whole or in part, without the express written permission of FileHold Systems. For authorization to copy this information, please call FileHold Systems Product Support at 604-734-5653 or email sales@filehold.com.

TABLE OF CONTENTS

1. OVERVIEW	1
1.1. LOG IN.....	2
1.2. ADMINISTRATION PANEL	3
2. THE FILEHOLD LIBRARY	4
3. FILEHOLD SECURITY	4
3.1. FILE STRUCTURE AND ACCESS TO DOCUMENTS.....	5
3.2. EFFECTIVE PERMISSIONS.....	5
3.3. SECURITY RULES.....	5
4. CREATING THE LIBRARY	6
4.1. OVERVIEW	6
4.2. BEST PRACTICES FOR SETTING UP THE LIBRARY	6
4.3. BEST PRACTICES FOR DESIGNING THE DOCUMENT LIBRARY STRUCTURE.....	8
4.3.1. GUIDELINES FOR THE DOCUMENT LIBRARY STRUCTURE - SUMMARY.....	9
4.3.2. EFFECT OF LIBRARY SIZE ON PERFORMANCE - TECHNICAL INFORMATION	9
4.4. USER ROLES AND ACCESSING THE LIBRARY	11
4.5. CREATING A LIBRARY STRUCTURE.....	15
4.5.1. MANAGING CABINETS.....	15
4.5.2. MANAGING DRAWERS	20
4.5.3. MANAGING FOLDER GROUPS.....	24
4.5.4. MANAGING FOLDERS	26
5. DOCUMENT SCHEMAS	27
5.1. CREATING DOCUMENT SCHEMAS.....	27
5.1.1. CREATING DOCUMENT SCHEMAS FOR OFFLINE DOCUMENTS	29
5.1.2. VERSION 0 SWITCH FOR OFFLINE DOCUMENTS.....	29
5.2. DOCUMENT AND VERSION CONTROL NUMBERS	30
5.2.1. VERSION CONTROL NUMBERS	31
5.2.2. DOCUMENT CONTROL NUMBERS	31
5.3. ADDING GROUPS OR USERS TO A SCHEMA	32
5.4. CREATING METADATA FIELDS FOR DOCUMENT SCHEMAS	33
5.4.1. WHY METADATA IS IMPORTANT IN A DOCUMENT MANAGEMENT SYSTEM	34
5.4.2. CREATING METADATA FIELDS.....	34
5.4.3. CREATING DRILL DOWN MENUS	36
5.4.4. CREATING DROP-DOWN MENUS – FILEHOLD MANAGED.....	37

5.4.5.	CREATING DROP DOWN MENUS – DATABASE MANAGED	38
5.4.6.	ADDING METADATA FIELDS TO SCHEMAS.....	41
5.4.7.	EDITING AND DELETING METADATA	42
5.5.	WORKFLOW TEMPLATES	43
5.5.1.	AD-HOC WORKFLOW TEMPLATES	44
5.5.2.	WORKFLOW TEMPLATE EXAMPLES.....	45
5.5.3.	CREATING WORKFLOW TEMPLATES	48
5.5.4.	SETTING UP A WORKFLOW CUSTOM NAMING PATTERN	53
5.5.5.	CLONING WORKFLOW TEMPLATES	55
5.5.6.	ADDING WORKFLOW TEMPLATES TO DOCUMENT SCHEMAS	55
5.5.7.	AUTOMATICALLY STARTING WORKFLOWS	56
5.5.8.	EDITING WORKFLOW TEMPLATES	57
5.6.	COURIER	58
5.6.1.	CREATING COURIER TEMPLATES	58
5.6.2.	ADDING COURIER TEMPLATES TO A SCHEMA	66
5.7.	SETTING CUSTOM FILE NAMING.....	67
5.7.1.	INPUT MASKS FOR DATA CONTROL	69
5.8.	AUTO-FILING SETTINGS	70
5.9.	EVENT SCHEDULES.....	72
5.9.1.	USING CUSTOM METADATA FIELDS FOR RETENTION POLICIES.....	74
5.9.2.	APPLYING RETENTION POLICIES TO DOCUMENT SCHEMAS.....	75
5.9.3.	SETTING THE NUMBER OF USER DEFINED NOTIFICATIONS ALLOWED IN A SCHEMA	77
5.10.	DATABASE LOOKUP ON THE SCHEMA.....	77
6.	GENERAL LIBRARY SETTINGS	81
6.1.	PERMANENTLY DELETING DOCUMENTS.....	81
6.2.	DOCUMENT LINKS SETTINGS	81
6.3.	EMAIL ATTACHMENTS SETTINGS.....	83
6.4.	EMAIL NOTIFICATION	84
6.5.	AUTO-FILING	84
6.6.	WORKFLOW INITIATION CONFIGURATION	85
6.7.	RESTRICTING ACCESS TO THE DOCUMENT MANAGEMENT SYSTEM.....	85
6.8.	SERVER SIDE OCR	85
6.8.1.	CONFIGURATION OF SERVER SIDE OCR	86
6.8.2.	OCR STATUS	87
7.	SEARCH ENGINE CONFIGURATION.....	89

7.1. SEARCH ENGINE STATUS.....	89
7.2. UN-INDEXED FILES.....	90
7.3. SEARCH ENGINE ERRORS	91
7.4. EXCLUDING FILE TYPES FROM FULL-TEXT SEARCH	92
7.5. LIMITING FULL TEXT INDEXING TO SPECIFIC FILE FORMATS	92
8. WORKFLOW REPORTS AND DASHBOARD	94
8.1. WORKFLOW STATUS REPORT	94
8.2. WORKFLOW DASHBOARD	97
9. LIBRARY MANAGEMENT	99
9.1. CHECK-IN FOR USER	99
9.2. CHANGE DOCUMENT OWNER.....	100
9.3. CHANGE CABINET/FOLDER OWNER.....	100
9.4. RECOVER DOCUMENTS	102
10. ADMINISTRATION REPORTS.....	103
10.1. DOCUMENT USAGE LOG.....	103
10.2. LIBRARY AUDIT LOG	104
11. SERVER SIDE DOCUMENT IMPORTATION.....	105
11.1. USING INDIRECT METADATA IN AN IMPORT JOB	110
12. MANAGE IMPORTS TOOL.....	112
12.1. IMPORTING DOCUMENTS FROM A SCANNING APPLICATION.....	113
12.2. IMPORTING DOCUMENTS PREVIOUSLY EXPORTED FROM FILEHOLD	115
12.3. OPERATING MANAGED IMPORTS	116
13. EXTRACTION RULES	120
13.1. EMAIL HEADER EXTRACTION RULE	120
13.2. AUTOMATIC EXTRACTION OF METADATA VALUES FROM FILE PROPERTIES.....	121
13.3. AUTOMATIC EXTRACTION OF XML NODES FROM MICROSOFT WORD CONTENT CONTROLS.....	124
13.4. METADATA EXTRACTION FROM PDF FORMS	131
INDEX	135

1. OVERVIEW

The FileHold Library Administrator is a security role that provides for the management of the FileHold document library where the documents, files, and records are stored. The tasks for the Library Administrator include:

- Create and manage the document library hierarchy. The creation of the library structure and security to restrict access to content at all levels of the hierarchy.
- Create and manage document schemas. Document schemas determine how your documents are tagged and which users have access to them.
- Create and manage metadata fields, drop-down lists, date, currency, numeric and text fields. The creation of a simple or a sophisticated taxonomy allows users to quickly and easily categorize information.
- Manage and apply security membership of the various areas of the library hierarchy (cabinet, folders, and document schemas). Security levels include: cabinet membership, folder membership, and schema membership.
- Manage the workflow module (optional) by creating templates and tasks for document review and approval.
- Use reporting services to create and generate reports on usage metrics, library reports, and more.
- Manage Courier templates to send documents to external users for review and approval.

The library administrator should have general knowledge of the company operations and understand the need to create, archive, and retrieve documents. The best library administrators usually are individuals who understand:

- The organization — How the organization is structured and requirements for managing documents and records.
- Types of documents and records to be stored — Sensitivity of security concerns of each type or class of document and what access permissions are required to maintain secrecy or confidentiality.

Typically, an organization will require only one library administrator along with a backup for vacations and holidays. In a very document intensive environment, this could be a full-time job directing a team of document scanning and imaging personnel. See [Best Practices for Setting up the Library](#) for more information.

In this guide you will learn:

- [Log In](#)
- [FileHold Security](#)
- [Creating the Library](#)
- [Document Schemas](#)
- [General Library Settings](#)
- [Server Side OCR](#)
- [Search Engine Configuration](#)
- [Workflow Reports and Templates](#)

- [Courier](#)
- [Event Schedules/ retention policies](#)
- [Library Utilities](#)
- [Server Side Document Importation](#)
- [Extraction Rules](#)
- [Administration reports](#)
- [Manage Imports](#)

1.1. LOG IN

You can access Library Administration functions from both the Web Client and the FileHold Desktop Application (FDA). The Web Client has full access to all Library Administration functions while there is limited functionality in FDA.

The Library Administration features in FDA include:

- Schema management — Schemas, metadata fields, events, and document and version control number fields.
- Workflow — Workflow templates and the Workflow Status Report.
- Courier — Courier templates menu item takes you to the Administration Panel.
- Document usage log

These functions work fairly similarly to the original Web Client functions.

TO LOGIN TO LIBRARY ADMINISTRATOR IN THE WEB CLIENT

1. Open a Web Browser (Firefox and Internet Explorer are supported) and enter the path to the FileHold server. The Web Client Login path to the server follows this pattern:

`http://YOUR-FileHold-SERVERNAME/FH/FileHold/WebClient/LoginForm.aspx`

This may be set up as link on your desktop or from the FileHold Desktop Application (FDA) by selecting **Administration** > **Library Administration** from the menu bar.

2. Enter your Login, Password, and select the domain (if required) and click **Log In**.
3. Click the **Administration Panel** link at the top of the screen.



TO LOG OUT FROM LIBRARY ADMINISTRATOR IN THE WEB CLIENT

- Click **Log Out**.

TO ACCESS THE LIBRARY ADMINISTRATION FUNCTIONS IN FDA

1. Log into FDA and go to **Administration > Manage Schemas or Workflows**.

1.2. ADMINISTRATION PANEL

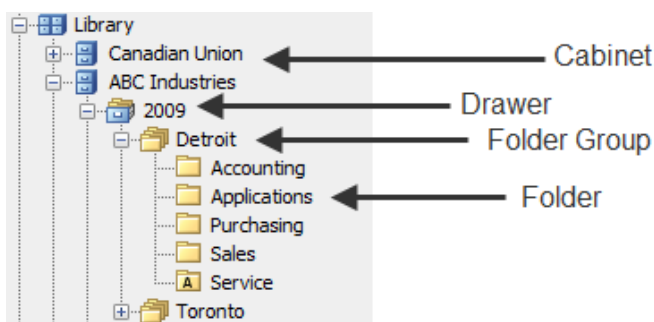
This Library Administration area in the Administration Panel is only available to users designated as Library Administrators. Non-administrator users will not see the Administration Panel link to the administration section.

The following areas in the Administration Panel is available to library administrators. Note that for Cabinet administration and Library administration roles, the menu items are only available for those cabinets they are an owner of in the library tree.

Menu item in Administration Panel	Minimum role required to view
Workflow management > Status Report	Read only
Workflow management > Dashboard	Read only
Workflow management > Courier transmission report	Document publisher
Administration reports > Document usage log	Cabinet Administration
Administration reports > Library audit log	Senior Library Administration
Library configuration > Control fields	Library Administration
Library configuration > Document schemas	Library Administration
Library configuration > Events	Library Administration
Library configuration > Extraction Rules	Senior Library Administration
Library configuration > General	Senior Library Administration
Library configuration > Metadata fields	Library Administration
Library configuration > Workflow templates	Library Administration
Library management > Change cabinet/folder owner	Cabinet administration
Library management > Change document owner	Cabinet administration
Library management > Recover documents	Cabinet administration
Library management > Undo checkout	Cabinet administration
System management > Full text search > Errors	Library Administration
System management > Full text search > Status	Library Administration
System management > Full text search > Unindexed files	Library Administration
System management > Import jobs	Senior Library Administration
System management > OCR queue status	Senior Library Administration

2. THE FILEHOLD LIBRARY

You will need to plan out how you want your library hierarchy structured. The hierarchy consists of cabinets, drawers, folders, folder groups, and document schemas. Users of FileHold will place documents into the structure you have created.



Cabinets, drawers, folders and folder groups are created in the FileHold Desktop Application (FDA) or in the Web Client. To access the FileHold Library in the Web Client, click the FileHold logo. For more information on how to set up your library structure, see [Creating a Library Structure](#).

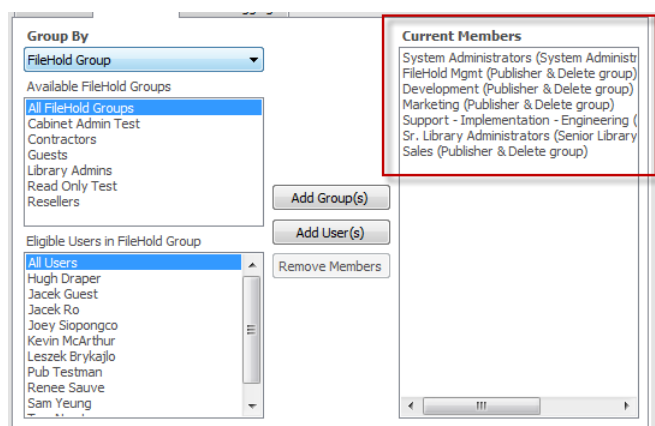
Document Schemas are created in the library administration area in the web application. Document Schemas allow the library administrator to classify documents. For more information, see [Document Schemas](#).

3. FILEHOLD SECURITY

FileHold has three levels of security:

- At the cabinet level.
- At the folder level.
- At the schema level.

If a user is having problems accessing cabinets, folders, or documents, make sure that they are members of the security groups that are set for that level.



Your system administrator manages the users and groups. See the [System Administration Guide](#) for more information.

[Cabinet security](#) can be managed by a user with a Cabinet Administrator role or a group of cabinet administrators or higher role. If a user or group is not a member of the cabinet, then the user will not see the cabinet or anything inside the cabinet when they log into the system.

[Folder security](#) can be managed by a user with Publisher rights or a group of publishers or higher role. If a user or group is not a member of the folder, then the user will not see the folder or anything inside the folder when they log into the system.

[Schema security](#) is managed by a user with Library Administrator rights or higher role. If a user is not a member of the schema, then the user cannot see, add, search, or use links to documents of that type.

3.1. FILE STRUCTURE AND ACCESS TO DOCUMENTS

One of the ways that security is built into the FileHold document management system is through the use of user and group membership to the different parts of the file structure hierarchy (library).

Except for the library, a user must be a member of a cabinet to even see it displayed in their view of the document management system's file structure.

Permissions are usually inherited by the other objects (drawers, folders and documents) that they contain, although each object may be customized.

NOTE: Permissions may be restricted at a lower level or taken entirely away.

3.2. EFFECTIVE PERMISSIONS

A user can be assigned to a folder or cabinet as a result of being assigned to one or more FileHold groups. The actual users with access to the folder or cabinet and their role on the folder or cabinet can be found by pressing the Effective Permissions button.

3.3. SECURITY RULES

- All users may see the library.
- All users that are given access to a cabinet will see all of the drawers inside that cabinet.
- However, the user may not have access to all of the folders inside of a drawer as permissions may again be restricted at the folder level.
- Permissions to documents are restricted by the document schema to which the document is assigned.
- Access to the library archives follows the same logic as the main library.

4. CREATING THE LIBRARY

After you have your document schemas created, you can start creating your cabinets, folders, folder groups, and drawers for your library hierarchy. You create the hierarchy directly in the FileHold library area of the Web Client or in the FileHold Desktop Application (FDA).

Before you start creating your hierarchy, you should plan out how you are going to organize the structure. Use the FileHold Library [Hierarchy Planning template](#) in the documentation section of our website as a guide.

TIP: Research shows that filing documents three to four levels deep is the most organized means to store files and provide for efficient retrieval. By expanding the various levels of the library or library archives users are able to browse down to the various folders in the system.

4.1. OVERVIEW

All documents in FileHold are stored under the Library icon (root folder). The library is filled with cabinets which contain drawers. Drawers can contain folder groups (optional) or folders. Folder groups contains folders and folders can contain documents. Documents can only be located in folders.

Access to the structure is controlled by group and user memberships at the cabinet and folder levels. Only users that are members of a cabinet can see the cabinet to access its contents. Once inside the cabinet a user must also be a member of the folders it contains in order to access documents contained within the folder. If the user is not a folder member they will not be able to see the folder. Users can see the membership associated with a particular cabinet or folder by right clicking on the cabinet or folder and selecting Properties. Once authenticated to access files inside a folder, access to individual document schemas is restricted by schema membership. Users must be a member of schema in order to view files associated with this document schema in the document management system. For example, users in the sales department can be restricted to only add, search, and access sales document schemas (invoices, purchase orders and contracts) while users in the HR department can be restricted to only add, search and access only HR document schemas (expense reports, vacation requests and performance reviews) even if they are located in the same folder.

NOTE: Users who are not members of a folder will not see the folder in the hierarchy. To gain access, the user will have to be added by the owner of the folder or a library or system administrator.

NOTE: Only a designated library administrator can change the membership associated with a document schema.

4.2. BEST PRACTICES FOR SETTING UP THE LIBRARY

The following are some best practices to consider when setting up and managing the Library.

1. Understand Your Documents and Users

We recommend that you obtain relevant samples of all documents, templates and records that your organization wishes to store in the repository. Take careful note of the documents and talk to the users that are working with these documents on a daily basis. Ask the following questions:

- Is it easy to understand the documents intent and contents at a glance?
- Size of your legacy repository in terms of numbers of documents?

- Are you going to only import the most recent version of legacy documents or all versions?
- Do they have cover sheets, common styles and naming convention?
- Do some documents change more often than others?

Should some documents be treated as records? Records typically never change and are stored as a snapshot in time of a particular transaction or event. (Marriage Certificate, Land Title Document, Birth Certificate, X-Ray Image, etc)

- What is the best kind of information or data can be used to classify a document by its type? For example, if the document is of type Purchase order, the purchase order number and purchase order date may be the best data that can be used to distinguish one PO from another.
- What kind of information would users want to search for documents by? This will help the library administrator to set metadata.

2. Organizing Documents for User Access

You will need to plan out which users are going to be able to access the documents in the different areas of the library. Ask the following questions:

- What kind of key information do groups of users rally around? For example, does everyone in engineering talk using part number code while users in accounting frequently make referenced to customer ID or invoice number. This sort of information can quickly form the foundation of what metadata should be associated with documents.
- Divide the documents into logical groups based on who will need to access the documents. Many times this is accomplished by organizing the files by either function or department. It is also important to note any of the common metadata documents share.
- Which groups of users should be able to access which types of documents?
- Which groups of users should NOT be able to access which types of documents?

3. Files from Outside

You will need to determine how documents will be added to the library from outside FileHold. Ask the following questions:

- Will files be added to the document management system from 3rd party systems?
- Do these systems have the ability to export the documents along with metadata for the documents?
- Do you have a collection of documents to be scanned before bringing them into records management system?
- Have you purchased document imaging and scanning systems?
- Are scan stations configured and running?

4. Setting Document Retention and Disposal Policies

You will need to determine how long documents will be stored in the Library and after a period of time, should be deleted.

- How long does each type of document have to be retained by the company before it is first archived then disposed of.

- Is your company public? If so, depending on where you are in the world you may be subject to Sarbanes-Oxley or other regulatory requirements that mandate various behaviors and accounting practices as well as strict policies towards information management and record and document retention.

5. Organizing Files and Configuring the Library

Plan your file structures, document schemas and controlled metadata vocabulary before building the system. Use the spreadsheet included in this guide to help plan out your structure. See [Creating a Library Structure](#) for more information..

- Configure document schemas and metadata fields and build a categorization system that works. Keep the document schemas simple. A simple schema would contain a single drop-down menu to further categorize the type of document and a comments field. You can make them complex to provide for the management of a legal contract and its complete lifecycle. It is recommended to keep the number of metadata fields to a maximum of 5 per schema.
- Determine the key metadata fields common to all schemas. These will provide for a powerful search when added to the appropriate schemas. For example, searching using the customer name metadata fields across Purchase Order, Invoice and Contract document schemas.
- Keep the system as simple as possible. When rolling out a document management system it is important to make the schemas easy to use and stick to a few key fields.
- Use required fields sparingly. In aerospace, financial, medical, healthcare, or legal environments, required fields may be mandatory and will be used heavily because the data about the document is important.

Stage the document management solution in a rollout. Take it one step at a time and be realistic. Start with one group or document collection at a time to avoid being overwhelmed. Work with the people who have the most pain with document management first, make that implementation a success then move on.

6. Time and System Requirements when Setting up a Document Management System

- Make sure you allot enough time for document scanning, classification and migration.
- Make sure you allot enough time for system training.
- Even with very simple technology, the move to electronic document management systems comes with some very specific requirements. Training users is paramount in making the move to a paperless office smooth and successful.

4.3. BEST PRACTICES FOR DESIGNING THE DOCUMENT LIBRARY STRUCTURE

When creating your library structure for FileHold, you need carefully plan the library design for the cabinet, drawer, and folder structure. A large number of cabinets and folders can lead to performance issues (slow performance down) so scalability and future growth needs to be taken into account. There are many factors that affect the performance of the system so the general guidelines provided are based on calculations, tests, and experience.

Below are the general guidelines for creating the library structure and the technical background information on the effect of library size on performance.

4.3.1. Guidelines for the Document Library Structure - Summary

1. It is important to predict the size of the library not only at the time of designing the structure, but also taking into account how it will grow in the following years, in order to avoid having to change the design in the future.
2. The best way to design the FileHold document library structure is to have a small library structure, even when the number of documents is very large. It is always better to rely on metadata values and search facilities in order to find relevant documents. Such approach is more flexible than using a fixed library structure. Separate cabinets and folders should only be used to control permissions to various parts of the system (for example, to separate Accounting department from Engineering documents) and to divide documents into large chunks (for example, a separate folder for each accounting year).
3. If there is a need to use a large number of folders (for example, one folder per client), the number of drawers and folder needs to be properly balanced, so that the total number of drawers is less than 500 and the number of folders in each drawer is less than 200. This can be achieved, for example, by distributing folders into separate drawers based on the first letter (or several letters) of their name. Folder groups may also help, although they do not improve performance, but only make the structure clearer.
4. The cost of calculating permissions for cabinets is relatively high, so there should only be as many cabinets as necessary. It's generally better to have 5 cabinets with 100 drawers each than 50 cabinets with 10 drawers each, even though the page size is similar (see the table below). It is also easier to manage such structure if permissions need to be changed. If more granular control over permissions is necessary, they can be controlled on folder level.
5. It is also very important to keep only as many drawers expanded as necessary. Drawers that are no longer needed should be collapsed. This also makes it easier to navigate the library tree, as there is no need to scroll through a large list of folders. As a general rule, no more than 1,000 items should be visible at any given time. It is also important to remember to collapse drawers before logging out from FileHold; this will make logging back in much faster.

4.3.2. Effect of Library Size on Performance - Technical Information

The size of the library affects performance in many different ways, including, but not limited to:

- The cost of SQL queries that retrieve data from database and calculate permissions.
- The cost of transferring data to the client (Web Client and FileHold Desktop Application).
- The size of HTML markup and JavaScript code that needs to be processed by the browser (Web Client).

Each of these factors may affect performance to a certain degree, but the overall performance will be as good (or as bad) as the weakest link in this chain.

To some degree, performance of the SQL queries can be improved by placing the database on a machine with a lot of RAM and processing power. The cost of transferring data to the client can be reduced by using HTTP compression (which FileHold uses) and broadband connections. However, the size of HTML markup will always affect the amount of memory used by the browser and the time required to process and display the page. That cost is difficult to avoid.

In FileHold, the structure of the library is retrieved in two steps:

- First, all cabinets and drawers are retrieved (whether they are expanded in the tree structure or not).
- Then, folder groups and folders from all expanded drawers are retrieved.

This means that having a lot of cabinets and/or drawers is not a good idea, as they all have to be loaded and sent to the client on every page load (in case of the Web Client). Even though loading drawers from the database is relatively cheap, as they don't have advanced permission settings, the amount of generated HTML markup may be very large. For each drawer it's about 2,500 bytes, so for 1,000 drawers the size of each page is at least 2.5 MB.

Having lots of folders in a single drawer can also seriously affect performance. Retrieving folders from the database is quite costly, because permissions must be calculated individually for each folder. Also the amount of HTML markup is 2,000 bytes per folder, so each expanded drawer with 1,000 folders is an additional 2 MB of page size. This cost grows dramatically as more drawers are expanded at the same time.

Page size can be a good estimate for performance, because it affects not only the amount of data that need to be transferred over the network (which is usually compressed). Generating HTML markup requires lots of memory and computing power on the server. Parsing and storing the data in the web browser is even more costly, because the browser needs many times more memory to store the data than the size of raw HTML markup. Although when using the FDA, the page size is no longer relevant, it is still a good measure of the amount of data that FDA needs to keep in memory and retrieve from the FileHold server. The FDA doesn't need to retrieve those data upon each operation, but loading them at startup, when logging on to the server, may still take a significant amount of time.

Assuming that there are C cabinets, D drawers in each cabinet and F folders in each drawer, and that E drawers are expanded (opened, showing the folder list), the size of the library page in bytes (without anything else that the library tree) can be estimated using the following equation:

$$\text{Page Size} = C * 2,500 + C * D * 2,500 + E * F * 2,000$$

The total number of folders in the library equals:

$$\text{Total Folders} = C * D * F$$

Let's assume that there are 25,000 folders in the library, and we divide them into cabinets and drawers in three different ways:

- Case 1: 5 cabinets, 10 drawers each, 500 folders per drawer
- Case 2: 5 cabinets, 100 drawers each, 50 folders per drawer
- Case 3: 5 cabinets, 1,000 drawers each, 5 folders per drawer

Depending on the distribution of folders into drawers, page size will change significantly:

C	D	E	F	Page Size	Total Folders
5	10	1	500	1,137,500	25,000
5	10	2	500	2,137,500	25,000
5	100	1	50	1,362,500	25,000
5	100	2	50	1,462,500	25,000
5	1,000	1	5	12,522,500	25,000
5	1,000	2	5	12,532,500	25,000

Each case is shown with one expanded drawer (E = 1) and two expanded drawers (E = 2).

In case of 1,000 drawers per cabinet, the page size is always over 12 MB, no matter how many drawers are expanded.

In case of 10 drawers per cabinet, the page size with one expanded drawer is slightly over 1 MB, but it grows very quickly when more drawers are expanded.

The case with 100 drawers per cabinet and 50 folders per drawer is most balanced. The initial page size is not very large compared to the third case, and it doesn't grow as rapidly as in the first case.

Folder Groups don't change a lot, since all folders from folder groups are retrieved at the same time when a drawer is expanded, even when the folder groups are not expanded. For example, instead of a flat list of 500 folders per drawer, we could have 10 groups with 50 folders each, but that wouldn't change the page size significantly.

4.4. USER ROLES AND ACCESSING THE LIBRARY

Only users with the correct role can manage certain parts of the library structure. The following user roles are shown in the order of least permission to most permission.

All roles provide document emailing capability. Roles higher than Document Publisher have the Courier functionality. These functions can be disabled on a role by role basis by a System Administrator in the FileHold Groups area. See the [System Administrator Guide](#) for more information.

NOTE: You can be logged into FDA and the Web Client at the same time but you cannot be logged into two FDAs or web clients at a time. Only one user account can log into FileHold at a time.

Role Name	Description
Guest User	A Guest User has read-only rights, meaning they can only get a copy or view documents. Unlike all other roles, many users with the guest user role can log into FileHold at once using a single guest username and password. If multiple people log into FileHold with the same guest user name, the log files records the same user regardless of the actual person that logged into the system. You can purchase low cost packs of guest user connection licenses in groups of 50 to be used with the portal. You will need at least one named user regardless of how many connection licenses are purchased. Guest users may be restricted from downloading or printing documents. With the guest user role you can optionally bypass the login process entirely by setting up a Self-Service Portal with a guest user account. The Self-Service Portal is an optional module that allows users to access FileHold with a special URL. The portal does not require a login as this is done programmatically. The user simply visits the URL and the portal page appears. For more information about guest user licenses, contact sales@filehold.com.
Read Only	A Read-Only user role may only download or open and read documents from FileHold. They cannot edit, delete, or create documents. They can email documents if given this functionality by system administrators. Read-only users may be restricted from downloading or printing documents. Read-only users can participate in workflows but cannot initiate workflows.
Document Publisher	Document Publisher user role can read, get a copy, add, check-in/check-out, edit documents, and metadata. They can move documents that are owned by them. They cannot delete any documents including those which they have added to the system. Document publishers can initiate workflows, participate in workflows, and initiate Courier transmissions.
Document Publisher + Delete	Document Publisher Plus Delete user role can do everything a Document Publisher can do and delete their own documents. They must be the owner of the document in order to delete it. To see the owner of a document, you can look at the version properties in the metadata pane.
Publisher	Publisher user role can do everything a Document Publisher can do plus: • Create new folders and folder groups. • Copy or move folders that they have already created. • Clone folders and folder groups created by other users and become the owners of the folders / folder groups. • Publishers cannot delete existing documents, folders or folder groups including those which they have added /created. All documents and folders created by the Publisher will be owned by them and they cannot change the ownership.
Publisher + Delete	Publisher plus Delete user role can do everything that a Publisher can do plus delete documents, folders and folders group owned (created) by them.

Organizer	The Organizer role is for users who are responsible for organizing documents that are scanned or imported into the system or who are assigned to organize documents added by other users. For example, organizers would move the documents generated by scanner operators to their correct folder in the library. Only trusted personnel should be given this role. Organizer role user can: • Move all documents (which they have an access to) in other places in the library including documents which they do not own. In other words, they can move documents that are owned by other users. • Move, copy or clone all folders and folder groups regardless of their ownership. In case of cloning they will become the owners of folder / folder groups. In case of copying and moving the original ownership of folders / folder groups is preserved. • Change folder properties regardless of ownership. • Add folders / folder groups (in which case they will become their owners) and rename folders and folder groups. • Delete documents that they own. • Change document owner regardless of ownership • Convert offline documents to electronic documents • Export documents
Organizer + Delete	Organizer plus Delete role can do everything that Organizers can do plus delete all documents, folders and folder groups regardless of their ownership. This organizer and delete role can only do this within Cabinets, Folders and Schemas that they are a member of. This role should be used by trusted personnel only.

Cabinet Administration	Cabinet Administrators can only administer the cabinets that they own; they cannot create cabinets for themselves. They can: • Create, edit, and delete drawers, folder groups and folders and manage their properties (i.e. membership structure). • Access all documents (in Publisher and Delete capacity) from anywhere in the library structure unless they are restricted from that area of the library structure. If they do not have access to the Cabinet and Folder they will not be able to access the documents. • Delete and move electronic records as long they are owners of the cabinet. Electronic records can only be moved to another Cabinet in which they own. • Move documents between cabinets as long as they are owners of the Cabinet. If users need to move documents between Cabinets that they do not own, then use an organizer role instead. • Have access to all document schemas. • Change document owner for documents in the cabinets that they own. • Convert electronic documents to electronic records and vice versa for cabinets that they own. • Convert electronic documents to offline documents for cabinets that they own. • Manually move document to and from the library archive as long as they are the Cabinet owner in the library archive.
Library Administration	Library administrators can perform, within their cabinets, the same functions as Cabinet Administrators plus: • Create cabinets for which they will be the owner of and manage them in the Library. • Access to Library Administration functionality where they can manage metadata fields, schemas, events, set up workflow templates, manage numerous global settings (i.e. viewer permissions, search engine settings, reporting services permissions and more), perform various managerial functions such (as check-in for user, change document owner, recover deleted document etc.) and access many useful reports and usage logs for the cabinets that they own. • Library administrators cannot create cabinets for Cabinet Administrators to own. If a library administrator creates a cabinet, then they are the owners.
Senior Library Administration	Senior library administrators have full control of the FileHold library itself and library administration area. Senior library administrators can create cabinets to be managed by any Library Administrator or Cabinet Administrator.

System Administration	System administrators have complete control of the system. They can perform all of the functions of all other roles. However, the main tasks of the system administrators are to add users to the system (including assigning the initial password and setting requirements for all new passwords and ability to self-register), assign users to their appropriate groups, enable document control numbers and version control numbers, manage user accounts, user groups and the system license pool. The system administrator also has access to various global settings (outbound e-mail, system wide configurations for managing the various documents format conversion permissions etc.) and as well as user activity reports.
-----------------------	--

4.5. CREATING A LIBRARY STRUCTURE

The file structure is typically created by the library administrator. In the document management system, the file structure serves the purpose of visually organizing the documents and providing security based on access.

Users of the system only have access to the portion of the file structure that they assigned by the Library Administrator. See [User Roles and Accessing the Library](#).

4.5.1. Managing Cabinets

Only library administrators, senior library administrators, and system administrators can create cabinets.

In order for a user to see a cabinet they must be a member of the cabinet. Only members of cabinets can see and access its content. In order to manage the access to a particular cabinet, the owner of the cabinet can add and remove member access and permissions.

Groups are created by systems administrators. Groups can be made to represent departments, divisions, functions, etc. For example users from sales, engineering and marketing could each be placed in their appropriate group and then these groups can be made members of their particular cabinets.

Permissions can be inherited from the cabinet by all of the folders and documents inside of it. It should be noted that the owner/administrator can then further adjust access and permissions at the folder and schema level to restrict specific users from specific folders/documents. Once the permissions are set at the cabinet level, you can give a new user access by adding them to a group that belongs to the cabinet. The new user will inherit all the access and permissions of the group they are assigned, and any minor adjustments to permissions can be made at the folder or schema level by the owner.

The following actions can be taken on cabinets:

Action / Function	What the function does	Who can access the function
Open Cabinet	Expands the drawers under the cabinet	All users with access to the cabinet.
Search	Starts an advanced search with the library location set to the cabinet	All users with access to the cabinet.
Properties	Opens the properties of the cabinet.	All users with access to the cabinet.

Action / Function	What the function does	Who can access the function
Set Default View	Allows user to select a default view that has been created in the View Preferences.	All users with access to cabinet.
Manage Folder Groups	Allows the user to add folder groups to the cabinet.	Users with Cabinet administration or higher access. Cabinet administrators and library administrators must be owners of the cabinet.
Add Drawer	Allows user to add a folder to the drawer.	Users with Cabinet administration or higher access. Cabinet administrators and library administrators must be owners of the cabinet.
Copy Cabinet	Makes a copy of the cabinet including all drawers, folder groups, folders and the documents it contains.	Users with Library administration or higher access. Library administrators must be owners of the cabinet.
Clone Cabinet Structure	Makes a copy of the cabinet including all drawers, folder groups, and folder structure only. Does not copy documents.	Users with Library administration or higher access. Library administrators must be owners of the cabinet.
Delete Cabinet	Deletes the cabinet and all items it contains.	Users with Library administration or higher access. Library administrators must be owners of the cabinet.
Archive Cabinet	Manually sends the contents of the cabinet to the Library Archive. Permission setting needs to be enabled by a system administrator.	Users with Library administration or higher access. Library administrators must be owners of the cabinet.
Export (FDA only)	Exports all documents in the cabinet.	Document publisher and higher roles. See Exporting documents in the FDA for more information.

TO CREATE A CABINET

1. In the FileHold library, right-click on the Library icon and select **Add Cabinet**.
2. In the Add Cabinet window, enter the following information in the General tab and click **Next**:
 - Name — Enter a name for the cabinet.
 - Owner — Select a user or group name from the list.
 - Description — Enter a description for the cabinet.

- **Default Schema** — Select the default schema for this cabinet. The default schema will be the schema that appears in the Metadata pane when documents are added to this cabinet.
- **Weight** — Select a weight for this cabinet from -10 to 10. -10 is the lightest so the cabinet will move to the top of the list. 10 is the heaviest so the cabinet will move to the bottom of the list. Leave this value at 0 if you want the cabinets sorted alphabetically.

The screenshot shows the 'Add Cabinet - New Cabinet' dialog box. It has three tabs: 'General', 'Security', and 'Auto-Tagging'. The 'General' tab is selected. Under the 'Attributes' section, there are fields for 'Name' (New Cabinet), 'Owner' (Sabine Marie), 'Description' (New cabinet), 'Default Schema' (Client Forms), and 'Weight' (0). Below this is a section titled 'This Cabinet Contains' which contains a table with the following data:

Drawers	0
Folder Groups	0
Folders	0
Files (latest version)	0
Size	0 MB
Files (all versions)	0
Size	0 MB

To the right of the table is a 'Calculate' button. At the bottom of the dialog are four buttons: '< Previous', 'Next >', 'OK', and 'Cancel'.

3. In the Security tab, enter the following information and click **Next**:

- In the Group By field, select how you want the available FileHold Groups displayed.
- In the Available FileHold Groups area, select the groups you want to be able to access the cabinet and click **Add Groups**. The group is added to the Current Members of Cabinet list.
- In the Eligible Users in the FileHold Group, select the user you want to be able to access the cabinet and click **Add User**. The user is added to the Current Members of Cabinet list.
- To remove a user or group from the cabinet, select the name from the Current Members of Cabinet list and click **Remove Members**.
- To view all Groups and Users, click **Group Members**. A new All Groups/Users panel opens on the right side of the window.
- To see which user roles the user or group belongs to, select the user or group name in the Current Members list and click **Effective Permissions**. The user role for that cabinet member will appear in the Effective Permissions list.
- To set advanced security options on a user or group, select the user or group name in the Current Members list and click **Advanced Security Options**. To modify the

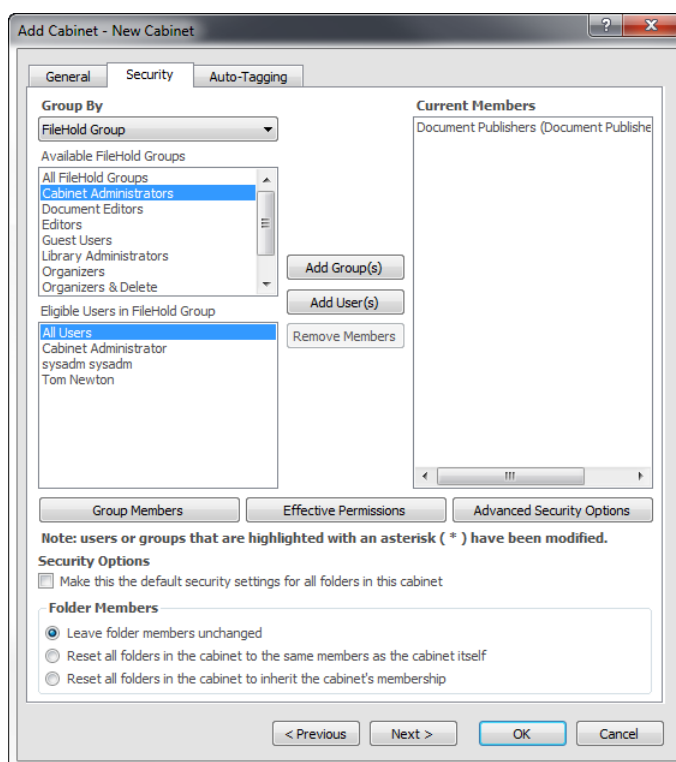
rights, select a user role from the list and click **Apply**. To revert to the default user role, click **Restore**.

- Select the **Security Options** check box if you want to make this the default security setting for this cabinet.

4. In the Folder Members area, select one of the options:

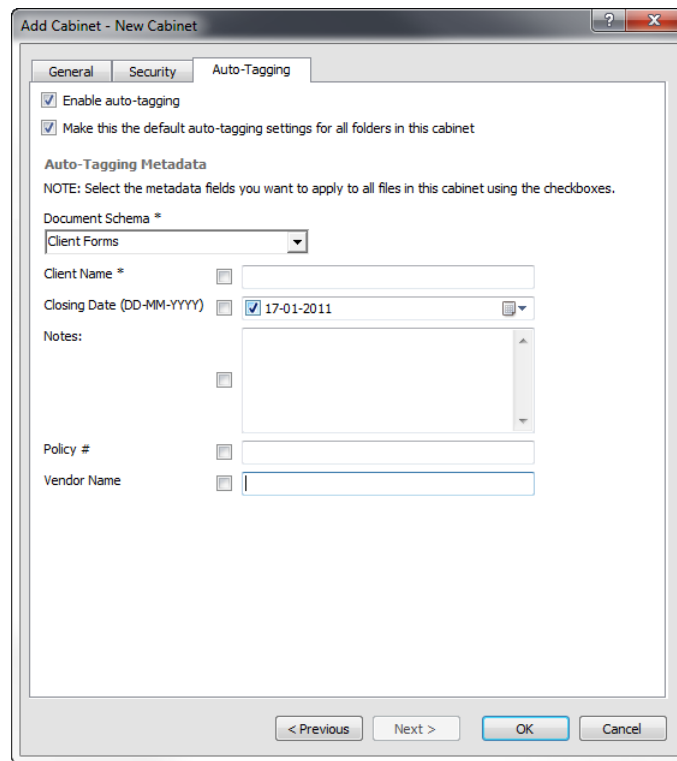
- Leave folder members unchanged.
- Reset all folders in the cabinet to the same members as the cabinet itself.
- Reset all folders in the cabinet to inherit the cabinet's membership.

WARNING: If you have a cabinet with hundreds or a few thousand folders, please be advised that changing large amounts of folders slow the system for a few minutes. It is advised to do this when the system is not busy.



5. In the Auto-Tagging tab, select the **Enable Auto-tagging** check box to have all documents in this folder automatically “tagged” with the same metadata based on the schema as they are added to this cabinet. This assumes that all of the documents that are being added to the cabinet have mostly the same metadata as all the other documents in the cabinet. This ensures a highly compliant filing system and standardization across all documents within the cabinet or folder. Users can select to have some standard repetitive metadata added automatically, manually, or a combination of both.
6. Select the **Make this the default auto-tagging settings for all folders in this cabinet** if desired.
7. In the Auto-Tagging Metadata area, select the document schema and the metadata. You do not have to set all the metadata fields; you can leave them blank for the user to enter them.

- Click **Save**.



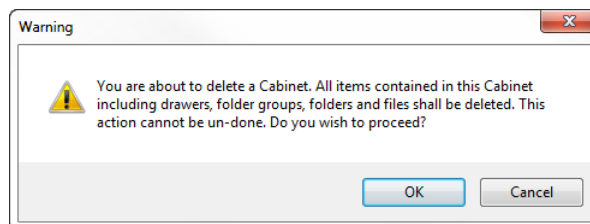
The screenshot shows the 'Add Cabinet - New Cabinet' dialog box with the 'Auto-Tagging' tab selected. The 'General' and 'Security' tabs are also visible. The 'Auto-Tagging' section has two checked options: 'Enable auto-tagging' and 'Make this the default auto-tagging settings for all folders in this cabinet'. Below this, the 'Auto-Tagging Metadata' section includes a note: 'NOTE: Select the metadata fields you want to apply to all files in this cabinet using the checkboxes.' The 'Document Schema' is set to 'Client Forms'. The 'Client Name' field is empty. The 'Closing Date (DD-MM-YYYY)' is set to '17-01-2011'. The 'Notes' field is empty. The 'Policy #' and 'Vendor Name' fields are also empty. At the bottom, there are buttons for '< Previous', 'Next >', 'OK', and 'Cancel'.

TO EDIT THE CABINET PROPERTIES

- Right-click on a cabinet in the library and select **Properties**. The cabinet properties window opens.
- Make any changes to the cabinet properties and click **Save**.

TO DELETE A CABINET

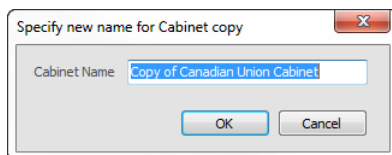
- Right-click on a cabinet in the library and select **Delete Cabinet**.
- You will receive a warning message. Click **OK** to delete the cabinet. The cabinet is removed from the library.



TO COPY A CABINET

- To copy a cabinet, its security, and all of its contents **including** drawers, folders, folder groups, and **documents**, right-click on the cabinet and select **Copy Cabinet**.

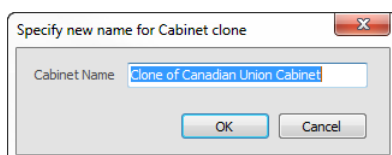
2. Enter a name for the copied cabinet and click **OK**. The copied cabinet appears in the library hierarchy.



WARNING: Copying large cabinets and its contents will cause the FileHold server to consume resources and may slow down the system. We recommend that you do this after business hours if copying cabinets containing tens of thousands or many hundreds of thousands of documents. The amount of time it will take to copy a cabinet and its contents is dependent on the server hardware that powers the system; the faster the server hardware the better.

TO CLONE THE CABINET STRUCTURE

- 1 To clone a cabinet, its security, and all of its contents including drawers, folders and folder groups, right-click on the cabinet and select **Clone Cabinet Structure**.
- 2 Enter a name for the cloned cabinet and click **OK**. The cloned cabinet appears in the library hierarchy.



NOTE: Cloning a cabinet structure does **NOT** copy the documents; only the Cabinet, Drawer, Folder Group, Folder structure and user/group permission is cloned. Use **Copy Cabinet** to copy drawers, folders, folder groups and documents.

TO CALCULATE THE CABINET STATISTICS

You are able to see how many drawers, folder groups, folders, documents, number of files and size of the repository by looking at the cabinet statistics.

1. Right-click on a cabinet in the tree structure and select **Properties**.
2. In the General tab, click **Calculate**. The number of drawers, folder groups, folders, files (latest version), size (in MB), files (all versions) and size of all versions (in MB) is shown.
3. Click **Cancel** to close the properties.

4.5.2. Managing Drawers

Only cabinet administrators, library administrators, senior library administrators, and system administrators can create drawers.

In order for a user to see a drawer they must be a member of the cabinet in which the drawer resides. The availability of actions is dependent on the rights that users have to the cabinet that the drawer resides unless further restrictions have been placed on the drawer by its owner, the library administrator or the systems administrator.

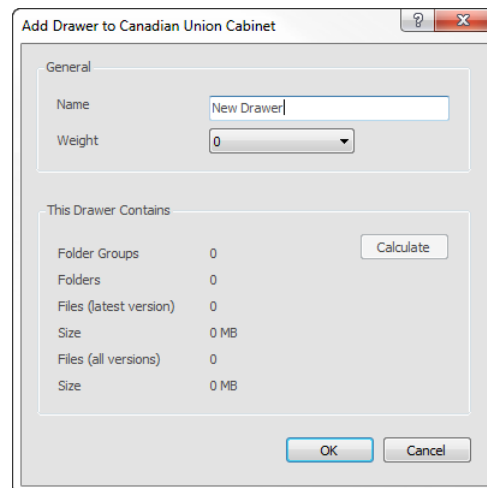
The following actions can be performed on drawers:

Action / Function	What the function does	Who can access the function
Open Drawer	Expands the Drawer revealing its contents.	All users with access to the Cabinet that the drawer belongs to.
Search	Allows users to restrict their search to documents located in the selected drawer.	All users with access to the drawer.
Properties	Displays the Drawer Properties.	All users with access to the Drawer.
Set Default View	Allows user to select a default view that has been created in the View Preferences.	All users with access to Folder.
Add Folder	Allows user to add a folder to the drawer.	Users with Publisher or higher access.
Move Drawer	Moves the drawer to a different Cabinet.	Users with Cabinet administration or higher access. Cabinet administrators and library administrators must be owners of the cabinet.
Copy Drawer	Makes Copy of the Drawer including all folder groups, folders and documents it contains.	Users with Cabinet administration or higher access. Cabinet administrators and library administrators must be owners of the cabinet.
Clone Drawer Structure	Makes a copy of the Drawer and folder groups and folders it contains. Does not copy documents in Drawer.	Users with Cabinet administration or higher access. Cabinet administrators and library administrators must be owners of the cabinet.
Delete Drawer	Deletes the Drawer and all items it contains.	Users with Cabinet administration or higher access. Cabinet administrators and library administrators must be owners of the cabinet.
Archive Drawer	Manually sends the contents of the folder group to the Library Archive.	Users with Library administration or higher access. Library administrators must be owners of the cabinet.
Export	Exports all documents under the drawer.	Document publisher and higher roles. See Exporting documents in the FDA for more information.

TO CREATE A DRAWER

1. Right-click on a cabinet and select **Add Drawer**.
2. In the Add Drawer to Cabinet Name window, enter a name for the drawer.

3. Select a weight for this drawer from -10 to 10. -10 is the lightest so the drawer will move to the top of the list. 10 is the heaviest so the drawer will move to the bottom of the list. Leave this value at 0 if you want the cabinets sorted alphabetically.
4. Click **OK**.



TO EDIT THE DRAWER PROPERTIES

1. Right-click on a drawer in the library and select **Properties**. The Edit Drawer Name window opens.
2. Make any changes to the drawer properties and click **OK**.

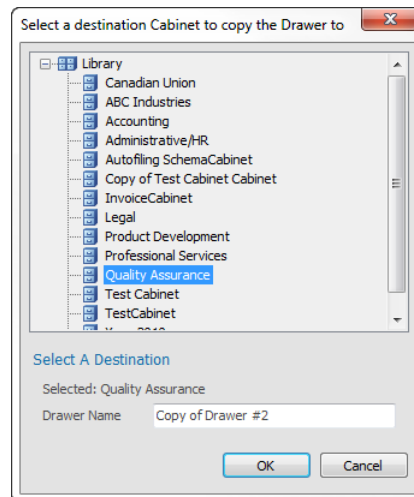
TO MOVE A DRAWER

1. Right-click on a drawer and select **Move Drawer**.
2. Select the destination cabinet to move the drawer to by navigating through the library in the dialog box and click **OK**. The drawer is moved to the new cabinet location.

TO COPY A DRAWER

1. To copy a drawer, its security, and all of its contents **including** folders, folder groups, and **documents**, right-click on the drawer and select **Copy Drawer**.
2. Select the destination for the copied drawer and its contents by navigating through the library.

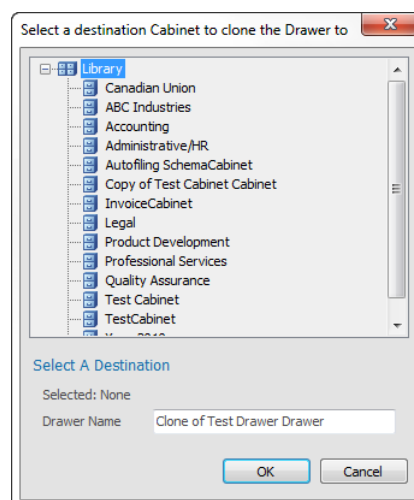
3. Enter a name for the copied drawer and click **OK**. The copied drawer appears in the library hierarchy.



WARNING: Copying large drawers and its contents will cause the FileHold server to consume resources and may slow down the system. We recommend that you do this after business hours if copying drawers containing tens of thousands or many hundreds of thousands of documents. The amount of time it will take to copy a drawer and its contents is dependent on the server hardware that powers the system; the faster the server hardware the better.

TO CLONE THE DRAWER STRUCTURE

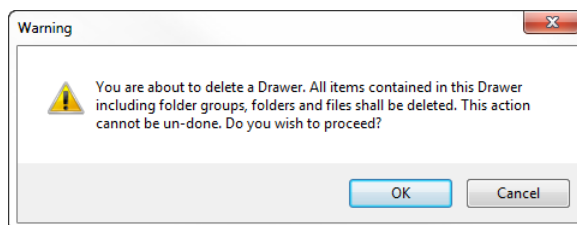
1. To clone a drawer, its security, and all of its contents including folders and folder groups (not documents), right-click on the drawer and select **Clone Drawer Structure**.
2. Select the destination for the cloned drawer and its contents by navigating through the library.
3. Enter a name for the cloned drawer and click **OK**. The cloned drawer appears in the library hierarchy.



NOTE: Cloning a drawer structure does **NOT** copy the documents; only the drawer, folder group, folder structure and user/group permission are cloned. Use [Copy Drawer](#) to copy drawers, folders, folder groups **and** documents.

TO DELETE A DRAWER

1. Right-click on a drawer in the library and select [Delete Drawer](#).
2. You will receive a warning message. Click [OK](#) to delete the drawer. The drawer is removed from the library.



TO CALCULATE THE DRAWER LEVEL STATISTICS

You are able to see how many folder groups, folders, documents, number of files and size of the repository that are contained within a drawer by looking at the statistics.

1. Right-click on a drawer in the tree structure and select [Properties](#).
2. In the drawer properties window, click [Calculate](#). The number of folder groups, folders, files (latest version), size (in MB), files (all versions) and size of all versions (in MB) is shown.
3. Click [Cancel](#) to close the properties.

4.5.3. Managing Folder Groups

Folder Groups are intended to be used as an extra layer of division in the library structure but their use is optional. Like drawers that divide cabinets into more manageable size; folder groups divide drawers into more suitably sized portions. Users with access to the drawers containing folders will have access to the folder groups as well. Folder groups contain only folders.

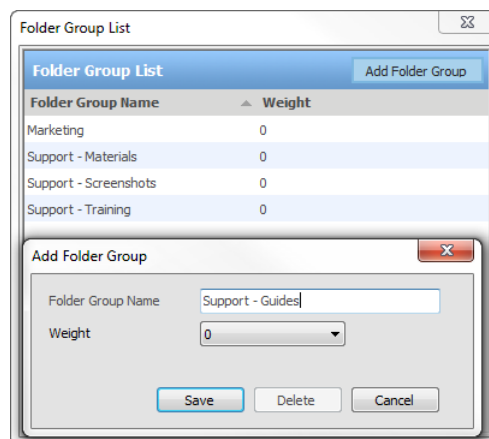
The following actions can be performed on folder groups.

Action / Function	What the Function Does	Who Can Access the Function
Open Folder Group	Expands the folder group revealing its contents.	All users with access to the cabinet that the folder group belongs to.
Search	Allows users to restrict their search to files located in the selected folder group.	All users with access to the folder group.
Properties	Displays the folder group Properties.	All users with access to the folder group.
Set Default View	Allows user to select a default view that has been created in the View Preferences .	All users with access to the folder group.

Action / Function	What the Function Does	Who Can Access the Function
Add Folder	Allows user to add a folder to the folder group.	Users with Publisher or higher access.
Move Folder Group	Moves the folder group to a different drawer.	Users with Organizer or higher access.
Copy Folder Group	Makes a copy of the folder group including all folders and files it contains.	Users with Organizer or higher access.
Clone Folder Group Structure	Makes a copy of the folder group and the folders it contains. Does not copy documents in folders.	Users with Publisher or higher access.
Delete Folder Group	Deletes the folder group and all items it contains.	Users with Organizer + Delete or higher access.
Archive Folder Group	Manually sends the contents of the folder group to the Library Archive .	Library Administrator or System Administrators only.
Export	Exports all documents in the folders contained in the folder group.	Users with Organizer or higher access.

TO MANAGE FOLDER GROUPS

1. Right-click on a cabinet and select **Manage Folder Groups**. The Folder Group list window opens with a list of existing folder groups.
2. To add a folder group, click **Add Folder Group**.
3. Enter a **Folder Group Name**.
4. Select a weight for this folder group from -10 to 10. -10 is the lightest so the folder group will move to the top of the list. 10 is the heaviest so the folder group will move to the bottom of the list. Leave this value at 0 if you want the cabinets sorted alphabetically.



5. Click **Save**. The folder group name is added to the list.

TO ASSIGN A FOLDER GROUP TO A DOCUMENT FOLDER

1. Right-click on a folder in the library and select **Properties**.
2. In the Folder Group field, do one of the following:
 - Select the folder group to which you want this folder to belong from the list.
 - To create a new folder group, select **Add a New Folder Group** and enter the name in the New Folder Group Name field.
3. Click **OK**. The folder is moved into the selected folder group.

TO EDIT OR DELETE A FOLDER GROUP NAME

1. Right-click on a folder group in the library and select **Properties**.
2. Click **Edit Folder Groups**.
3. To edit a folder group name, double-click on a folder group.
4. In the Edit Folder Group window, enter a new name for the folder group and a weight (optional). The higher the weight, the higher the cabinet name will appear in the library. Leave this value at 0 if you want the cabinets sorted alphabetically.
5. Click **Save**.
6. To delete the folder group, click **Delete**.

TO CALCULATE THE FOLDER GROUP LEVEL STATISTICS

You are able to see how many folders, documents, number of files and size of the repository that are contained within a folder group by looking at the statistics.

1. Right-click on a folder group in the tree structure and select **Properties**.
2. In the folder group properties window, click **Calculate**. The number of folders, files (latest version), size (in MB), files (all versions) and size of all versions (in MB) is shown.
3. Click **Cancel** to close the properties.

4.5.4. Managing Folders

Only users that are members of a particular folder can access the files that reside in that folder. Folders can be created by users with a role of publisher or higher.

When the library administrator creates a new folder they must associate groups (or users) with the folder in order to protect the contents of the folder from unauthorized users. ONLY groups (or users) associated with a folder will see and have access to the folder. Permissions can be further restricted once the groups or users are assigned as members.

The groups that are available to be members of the folder are inherited from the cabinet in which the folder resides. If you wish to add groups other than the ones that appear in the folder properties, the group must first be added at the cabinet level of the document management system. After the group is added at the cabinet level, the new group will appear in the Available FileHold Group listing in the folder properties security section.

For more information on creating folders, see the [FileHold User Guide](#) or the [Knowledge Base](#).

5. DOCUMENT SCHEMAS

Document schemas allow the library administrator to control the documents or files that are added to the library. Document schemas are a way to group like files together even when they are filed in desperate places across the library. Document schemas allow the library Administrator to manage how files are added to the library and what information is collected about them. For example, document schemas types can include: invoices, reports, contracts, legal, employee information, projects, and so on.

When adding a file to system, the user will select the schema they want to associate with the document by using the document schema field. The schema that is selected will determine what metadata is required and the format that the metadata will take.

Document schemas should be created to fit your business processes. They are mapped to either a specific class of documents, such as Executive, Compliance, or Record, or individual document schemas, such as Well Reports, Minutes and Packet Attachments. A publisher works with these document schemas when adding or checking a document into the library. For more information about publisher security rights, see [User Roles](#).

Providing descriptive schema names and descriptions will increase the effectiveness of the document management system. Once you have created a schema name, you cannot reuse a specific schema name, even if you have deleted the original schema from the system due to retention features within FileHold. Providing unique names for each schema also greatly reduces confusion for administrators and end-users of the system.

5.1. CREATING DOCUMENT SCHEMAS

In order to manage the documents properly, the library administrator creates schemas to manage the files. Schemas can be classified documents as one of three formats:

- Electronic Documents are files that will change over time or “working documents”. These documents typically undergo the full lifecycle of addition, revision and deletion. For this reason, files associated with these types of schemas will need to be version controlled. The FileHold library retains unique copies of each version of a document.
- Electronic Records prevents files associated with this schema from being versioned or modified by any user. Electronic records are files that will never change and are typically proof of some form of transaction that occurred within the company. Files of this nature can only be deleted by system administrators or by the archive and deletion policies as set for the schema. The storage of files using an electronic record schema is used mainly for compliance with record retention policies.
- Offline document schemas are effectively an entry in FileHold that point to a physical document that is stored outside of the electronic library. An example may be a large architectural document, rare periodical, large blueprint, map, or signed contract that has yet to be scanned.

Document schemas manage the following document features:

- [General](#) — Set schema name, format, and document numbering conventions.
- [Schema Membership](#) — Define which groups have access to this schema.
- [Metadata](#) — Define the metadata fields that are applied to a document.
- [Workflow](#) — Set up a review and approval process for a document that belongs to this schema.

- [Courier](#) — Send documents to external individuals or internal FileHold users for view and approval.
- [Custom Naming](#) — Set up naming conventions for the documents.
- [Auto-filing](#) — Define the destination folder in the library.
- [Event Schedule](#) — Determine when to convert the document to a record, archive, or delete the document.
- [Lookup](#) — Do a database lookup for all metadata fields in the schema.

TO CREATE A DOCUMENT SCHEMA

1. In the Web Client, go to **Administration Panel > Library Configuration > Document Schemas** and click **Add Schema**. The Document Schema Wizard opens.
 - Alternatively, in FDA go to **Administration > Manage Schemas > Document Schemas** and click **Add Schema** (+ sign)
2. In the General area, enter a schema Name, Description, and select the schema format:
 - Electronic Document – Documents can be checked out, modified and checked back in with a new version number.
 - Electronic Record – Records cannot be modified at any time. They are “locked down” and cannot be checked out.
 - Offline Document – Pointers to physical items that cannot be stored within the repository. See [Creating Document Schemas for Offline Documents](#) for more information.
3. In the Custom Document Numbering area, select or both of the following:
 - [Document Control Field](#) — Some organizations work with large and complex documents that need to be tightly controlled. With Document Control numbers, you can assign a specific number to a document and use it throughout its lifecycle. This field can ensure a unique document control number is assigned to each new document added under a schema. Document Control Numbers are mandatory, meaning they must be entered or created when adding a document to the system. Each Document Control Field has a prefix which must be different from all other Document Control prefixes. This ensures that each Document Control Number is unique across the entire library. Document control fields can be automatically generated or entered manually by a user. This is an optional setting that must be enabled before any documents are added to the schema. You will need to set up control fields in the [Control Fields](#) section.
 - [Version Control Field](#) — Version Control Numbers provide a facility to create a version number with a common prefix that can never be removed from the document. Version Control Numbers are always optional on a document. They are entered when adding a document, checking in a document, or at any time the document metadata is edited in the document management system. By default the version number is carried over from the last version when the document is checked in. Version Control Fields have a mandatory prefix which does not have to be unique. The prefix is always displayed with the field where ever the field is displayed. The value in the Version Control Field does not need to be unique. You will need to set up control fields in the [Control Fields](#) section. This is an optional setting.
4. Click **Next** in the Document Schema Wizard to add [group security rights](#) to the schema.

5.1.1. Creating Document Schemas for Offline Documents

In many instances organizations may choose to not scan or import all of their files into the document management system due to time constraints, file type, size, location or any number of reasons but would like to be able to manage those files via the system.

One of the most dynamic and powerful ways to have "offline" documents available to those working "online" is to create document schemas for the offline files. These schemas are associated with metadata fields that describe the file, the location of the file and any other relevant data about the files that is helpful for users to identify and locate documents that are kept in locations other than the document management system.

NOTE: Offline schemas are not meant to hold actual documents. The "files" associated with offline schemas are only pointers to the documents.

TO CREATE A SCHEMA FOR OFFLINE DOCUMENTS

1. Create a new schema and select the **Offline Document** schema format.
2. Create metadata fields for the offline documents. The following metadata fields are examples for offline documents:
 - Offline location — The location of the offline document such as Shelf in CTO's office, Cabinet #4, or Storage Facility Name. It is advisable to have multiple drop-down menus or a dynamic drop-down menu to organize your various record storage rooms and the locations within each room.
 - Type of Document — The document type such as book, video, or DVD.
 - Comments — Comments about the offline document.
3. Associate the metadata fields with the offline document schema.

5.1.2. Version 0 Switch for Offline Documents

When documents of any schema format (electronic document, electronic record, or offline document) are added to the library, the first initial version is set to version 1.

For documents that are Offline document schemas, you can set the initial version to be 0 instead of 1. In order to set the initial version to 0, you need to set the value to 0 in the Library Manager > web configuration file on the server.

This could be useful for organizations which use the process of Document ID/Number Reservation. Adding an Offline Document with version 0 would create a placeholder for the future electronic document version (yet to be created); however, the document ID will be issued by the system and can be used as a reference when creating the electronic version. For example, the document ID could be stated on the title page of the Microsoft Word document. By checking out the offline document and then checking back in with "Convert to Electronic Document" option enabled, the first version (version 1) of the document will be added to FileHold repository using the same document ID (initially created for the off-line document stub).

TO SET THE OFFLINE DOCUMENT VERSION TO START AT 0 INSTEAD OF 1

1. Log into the FileHold server using the administrator username and password.
2. Navigate to C:\Program Files\FileHold Systems\Application Server\LibraryManager for Windows 2008 server or C:\inetpub\wwwroot\FH\FileHold\LibraryManager for Windows 2003.

3. Open the **web.config** file using an editor such as Notepad.
4. In the **<appSettings>** section, enter the value of 0 for:

```
<add key="InitialOfflineVersion" value="0" />
```
5. To set the offline document version back to 1, change the value above to "1".

5.2. DOCUMENT AND VERSION CONTROL NUMBERS

You are able to set up document control numbers and version control numbers to meet your requirements for numbering schemes. Numbering schemes may be based on specific industry requirements and for compliance, such as for ISO compliance and other quality management systems.

Document and version control numbers are essentially special metadata fields. You can use one or both types of control numbers in a schema. If multiple document schemas use the same document or version control field, they are subject to the same numbering scheme. If schemas use separate document or version control numbering schemes, then separate document or version control numbers should be created and applied to the appropriate schema. The following screen shot shows both document and version control numbers being applied to the schema.

The following is an example of a version control number and a document control number shown in the folder list view.

Document Name	Type	Link...	Ver	Status	Last Modified On	Version Control No.	Document Control No.
  chc-example-for-pt-acuity-and-staffing-require...	Work Instructions		0	1	Checked In	8/2/2012 10:46 AM	REV-B
mechanical_example-imperial	Engineering Dr...		0	1	Checked In	8/2/2012 10:58 AM	ENG-001

WARNING: Once the version and document control numbers are enabled, they cannot be disabled. You also cannot change document schema types for documents that are using document/version control numbers to a schema that is not using document/version control numbers. This is to ensure the integrity of these features in very demanding environments (aerospace, manufacturing, engineering, defense contracting etc.) – without these strict controls the system is prone to human error.

NOTE: Document and version control numbers differs from the FileHold automatic versioning system. With FileHold automatic versioning, every time a document is checked out from FileHold, it becomes a candidate for automatic version control. Version control numbers allows managers to track the history of a document as it evolves; it records the date when the version was changed and by whom. This follows a simple versioning system of 1, 2, 3, 4, 5, and so on. The actual version numbering system starts at version #1 and is incremented by 1 number each time the document is changed and is checked back in.

5.2.1. Version Control Numbers

Version Control Numbers provide a facility to create a version number with a common prefix that can never be removed from the document. Version control numbers are always optional on a document. They are entered when adding a document, checking in a document or at any time the document metadata is edited in the document management system. By default the version number is carried over from the last version when the document is checked in.

Version control fields have a mandatory prefix which does not have to be unique. The prefix is always displayed with the field where ever the field is displayed. The value in the version control field does not need to be unique.

5.2.2. Document Control Numbers

Some organizations work with large and complex documents that need to be tightly controlled. With document control numbers, you can assign a specific number to a document and use it throughout its lifecycle. This field can ensure a unique document control number is assigned to a each new document added under a schema. Document control numbers are MANDATORY, meaning they need to be entered when adding a document to the system. Each document control field has a prefix which must be different from all other Document Control prefixes. This ensures that each document control number is unique across the entire library.

These document control numbers are not automatically incremented when a document is checked out/in nor can they be modified. The number is generated when the document is added and remains constant throughout the life of the document. They do not appear in the Metadata pane.

There are two ways to generate document control numbers:

- They can be auto-generated by the FileHold System. Auto-generation uses consecutive numeric values starting from a given initial value and a given number of digits. Auto-generated value is not shown before document is added. This to ensure document uniqueness. If FileHold provided a number in advance then there is a chance the user would not use the number or forget about it – and then you would need to manage unused and cancelled numbers. These numbers are not automatically incremented when a document is checked out/in. The number is generated when the document is added and remains constant throughout the life of the document.
- Entered manually by the user. Number uniqueness is checked upon adding the document. Manually edited numbers can be any alphanumeric strings with a given maximum length.

In either case, FileHold will ensure that the document control number is unique to the document and added to the schema. When used, document control numbers are mandatory. They must be assigned to a document when it's added and are unable to be modified later.

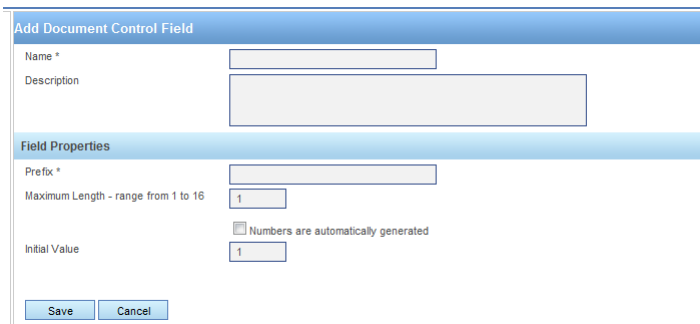
Document control numbers are visible in the version properties panel after they have been created.

TO ENABLE CONTROL FIELDS

1. In the Web Client, log in as System Administrator and go to **Administration Panel > System Configuration > General > Document/Version Control Fields**.
2. Select the **Enable Document Control Fields** check box, if applicable.
3. Select the **Enable Version Control Fields** check box, if applicable.
4. Click **Update**.

TO CREATE CONTROL FIELDS

1. In the Web Client, log in as a Library Administrator and go to **Administration Panel > Library Configuration > Control Fields**.
 - Alternatively, in FDA go to **Administration > Manage Schemas > Control Fields** and click **Add Control Field** (+ sign).
2. Do one of the following:
 - Click **Add Document Control Field**.
 - Click **Add Version Control Field**.



3. Enter a **Name** for the control field.
4. Enter a **Description** for the control field.
5. Enter a **Prefix** for the control field.
6. Enter the **Maximum Length** for the control number from 1 to 16 numbers.
7. For a Document Control Field, select the check box if numbers are to be automatically generated.
8. For a Document Control Field, enter the **Initial Value**. This is the value the numbering will start from.
9. Click **Save**.

5.3. ADDING GROUPS OR USERS TO A SCHEMA

Add groups and users to the schema membership to allow members to:

- Add documents of this type to the library
- Search for documents of this type
- View documents of this type
- Use links to documents of this type

FileHold groups are created by the system administrator. Groups can be made of one or more users. Members are individual users. For more information on FileHold groups and members, see the [FileHold System Administrator Guide](#).

Library administrators define membership at the cabinet, folder and schema level and can be a mixture of groups or individuals.

TIP: From an administrative perspective, it is easier to have cabinets, folders and schema memberships contain groups instead of individual user memberships as much as possible. This greatly reduces administrator overhead of adding users to many cabinets, folders and schemas. Adding a new user to a group automatically gives a user access to the cabinets, folders and schemas that they groups belong to.

TO ADD GROUPS OR USERS TO A SCHEMA

1. In the Web Client, go to **Administration Panel > Library Configuration > Document Schemas** and select **Membership**.
 - Alternatively, in FDA, go to **Administration > Manage Schemas > Document Schemas > Schema Name > Membership** tab.
2. In the Group By field, select a group from the list.
3. To add a group, select a group in the Available FileHold Groups area and click **Add Groups**.
4. To add individual users, select a user name in the Eligible Users in FileHold Group area and click **Add Users**.
5. The Current Members of the Schema Name displays the list of groups and users that are able to access the schema. To remove a group or user, select the name and click **Remove Members**.
6. Click **Next** in the Document Schema Wizard to add Metadata fields.

5.4. CREATING METADATA FIELDS FOR DOCUMENT SCHEMAS

Metadata is data that describes other data. You can create the metadata that you want to use for a schema in order to further define documents in the system. Using metadata allows you fine tune your searches for information. For example, if you are using metadata for your invoice type documents, not only can you search by document name but also the document status, type, date, invoice number, vendor name, or other important information. You can also use metadata for describing images, graphics, maps, schematics, or offline documents which do not contain any information. Assigning metadata to your documents makes searching and retrieving information considerably faster and easier.

Metadata data fields can be of various types. Each type has a unique set of properties associated with it. The different types of metadata fields are as follows:

- Text box
- Drill drop down menu
- Drop down menu (FileHold managed or database lookup)
- Date
- Number
- Currency
- Check Box

- URL

The library administrator can ensure that a minimum amount of metadata is captured for each document entered into the system.

5.4.1. Why Metadata is Important in a Document Management System

When a document management system contains thousands, hundreds of thousands, or millions of documents, a full-text search can result in an overwhelming amount of returned hits since many documents share common keywords and phrases. Additionally, assigning metadata makes searching for and retrieving files dramatically faster and easier. For more information on searching, see the [End User Guide](#).

Library administrators can ensure that appropriate metadata is added to files as they are brought into library. By setting centrally controlled metadata when creating document schemas, the Library Administrator provides for a controlled yet flexible method for defining the information that should be captured as the file is added to the library.

The metadata can be customized depending on what information is important to be captured. The metadata is captured when files are added to the document management system and can be updated as new versions are introduced. For example, consider a contract document. The metadata fields that are used to describe this document are: Type of Document, Document Name, Contract Number, and Contract Date.

Metadata fields may be used in multiple document schemas. This will allow users to search for all types of documents that relate to a given customer.

NOTE: Users will not have access to documents that they do not have security permissions to see.

5.4.2. Creating Metadata Fields

Metadata fields represent the information about a file that users think of when identifying a particular document, like the file name, the customer name, and unique identifiers such as invoice or purchase numbers or specialized codes. These bits of information, if captured, make finding the file simple and easy - even in a database of millions of files.

When adding a file to the document management system the user will select the schema they want to associate with the document by using the document schema pick list from the add document form. The schema that is selected will determine what metadata is required and the format that the metadata will take.

Metadata fields are created by the library administrator based on the needs and preferences of the organization. Metadata fields can be used in multiple schemas.

WARNING: Once a metadata field has been created and saved, the field type (text, numeric, date, and so on) cannot be modified. This is one of the few things that cannot be changed in FileHold.

WARNING: You cannot have duplicate metadata fields in FileHold. Simply rename the obsolete metadata field and create a new one.

IMPORTANT: There are a few character sequences that should not be used in values for metadata fields: <a through <z, <!, <?, commas (,)</, and &#. This applies to text, dropdown, drilldown, and URL fields. In some cases FileHold will prevent the user from entering these values, but this is not always possible with database dropdown or database lookup fields. They could be accidentally interpreted as HTML sequences in the web client.

TO CREATE METADATA FIELDS

1. In the Web Client, in the Library Admin area, go to **Administration Panel > Library Configuration > Metadata Fields**, and click **New Metadata Field**.
 - Alternatively, in FDA go to **Administration > Manage Schemas > Document Schemas** and click **Add Schema (+ sign)**.

TIP: You can also create metadata fields in **Manage Schemas > Metadata Fields** in the Library Admin hierarchy.

2. In the Add Metadata Field pane, enter a **Name** for the metadata.
3. Enter a **Description** for the metadata.
4. Select a **Field Type**. Refer to the following table for more information on how to enter the field properties.

Field Type	Description
Text	Set up a text box that ranges from 1 to 4000 characters. 1. Enter a minimum number of characters. 2. Enter the maximum number of characters. 3. Enter the number of lines for the text box. 4. Enter an initial value, if applicable. There are a few character sequences starting with the less-than sign (<) that cannot be used in a text field: <a through <z, <!, and <?.
Drill Drop Down Menu	See Creating Drill Down Menus for more information.
Drop Down Menu – FileHold Managed	For more information, see Creating Drop-Down Metadata Fields .
Drop Down Menu – Database Lookup	See Creating Drop Down Menu – Database Managed for more information.
Date	Configure a date field for the metadata properties. 1. Select the Date Display Format. 2. Select the Initial Value for the date. You can select the current date and time or leave the field blank. It is recommended that you set this value to Blank so that the user is forced to enter the correct date instead of defaulting to the current (today's) date and time.
Number	Set up a numeric field for the metadata properties. 1. Enter the number of Decimal Places. 2. Enter the Decimal Separator. 3. Enter the Group Separator. 4. Select an option for how Negative Numbers will be displayed. 5. Enter the Minimum Value. 6. Enter the Maximum Value. 7. Enter an initial value, if applicable.

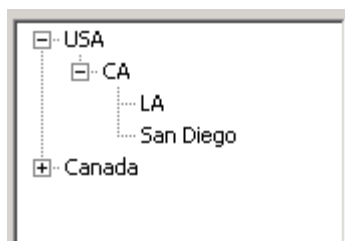
Field Type	Description
Currency	Set up a currency field for the metadata properties. 1. Enter the number of Decimal Places. 2. Enter the Decimal Separator. 3. Enter the Group Separator. 4. Select an option for how Negative Numbers will be displayed. 5. Select a Currency Symbol from the list. 6. If the currency symbol is to be displayed in front of the amount, select the check box. Clear the check box to display the currency symbol at the end of the amount. 7. Enter the Minimum Value. 8. Enter the Maximum Value. 9. Enter an initial value, if applicable.
Check Box	Set a check box field for the metadata properties. 1. Select an option for the check box: • Checked – The label for the check box will be True. • Unchecked – The label for the check box will be False.
URL	Set a URL field for the metadata properties. 1. Enter a caption for the URL. When defined, the caption is displayed in the metadata pane instead of the URL address. If the caption is not defined in the metadata field, the URL is displayed. 2. Enter a URL link, if applicable, in the format <code>http://www.urlname.com</code>

5. Click **Save**.

Once you have created all your metadata fields, you can add them to your schema

5.4.3. Creating Drill Down Menus

Drill down drop-down menus create a tree structure for the user to select the metadata value from. When a user makes a selection in the first list, a second, related list will appear. For example, there could be a drop-down menu that contains a list of the organization's positions and when a position is picked, a list of all people that hold that position displays.



TO CREATE DRILL DOWN DROP-DOWN MENUS

1. In the Web Client, go to **Administration Panel > Library Configuration > Metadata Fields**.
 - Alternatively, in the FDA, go to **Administration > Manage Schemas > Metadata Fields**.
2. In the Add Metadata Field pane, enter a **Name** for the metadata.
3. Enter a **Description** for the metadata.
4. Select a **Drill Drop Down Menu** type.
5. From the Web Client, click **Manage Menu Items**.
 - From the FDA, click the **Field Properties** tab. Add, Edit, Delete, and organize the order of the drop down list.
6. Type in the first entry for the drop-down menu and click **Add**. Continue to add menu items until all selections are added.
7. Select one of the existing drop-down menu items and to create the "branches" and/or "leaves" (sub menu items) of the drill down "tree" structure.
8. Type in the first "branch" or "leaf" name and click **Add**. The item will appear under the selected menu item and the selected menu item will display a plus sign next to it.
9. Continue to add sub menu items to all the menu items until completed.
10. Enter a Separator type such as -, _, < or /. The default is >.
11. If you want to show the full path of the "tree" structure in the metadata field box, select the **Show Full Path** check box. For example, if the check box is enabled, the value in the metadata field will show as "Canada > British Columbia > Vancouver". If the check box is disabled, the value in the metadata field will show as "Vancouver".
12. If you want only the last item in the sub menu (called "leaves") to be selected, select the **Select Only Leaves** check box. If the check box is not enabled, then users can select a value from any level in the "tree" structure.
13. Select an **Initial Value**, if applicable.
14. From the Web Client, click **Save**.
 - From the FDA, click **OK**.

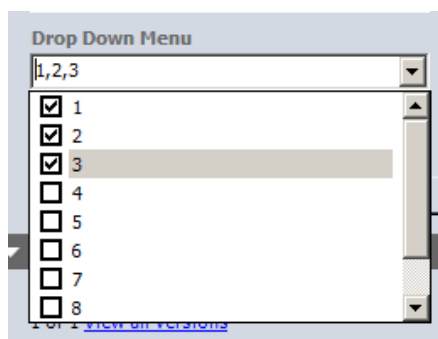
5.4.4. Creating Drop-Down Menus – FileHold Managed

These menus are created by the library administrator so that users can select from a list of choices rather than typing.

TO CREATE A FILEHOLD MANAGED DROP-DOWN MENU

1. In the Web Client, go to **Administration Panel > Library Configuration > Metadata Fields**.
 - Alternatively, in the FDA, go to **Administration > Manage Schemas > Metadata Fields**.
2. In the Add Metadata Field pane, enter a **Name** for the metadata.
3. Enter a **Description** for the metadata.
4. Select a **Drop Down Menu - FileHold Managed**.

5. From the Web Client, click **Manage Menu Items**. You can add, delete, and organize the order of the hierarchy by moving the items up and down.
 - From the FDA, click the **Field Properties** tab. Add, Edit, Delete, and organize the order of the drop down list.
6. If multiple selections are allowed, select the **Allow Multiple Selections** check box. **NOTE:** You can select multiple values on an entry by selecting the check boxes next to the value. For example:



7. If there are duplicates in the list and would like those removed, select the **Remove Duplicates** check box. This option is checked by default.
8. Enter or select an **Initial Value**, if applicable.
9. From the Web Client, click **Save**.
 - From the FDA, click **OK**.

5.4.5. Creating Drop Down Menus – Database Managed

A metadata field that is a drop down menu - database managed provides connectivity to external databases which allows retrieving drop down items from a table or a view. The following data providers are supported:

- Microsoft SQL 2005 and 2008
- .Net framework data provider for ODBC
- .Net framework data provider for OLE DB
- .Net framework data provider for Oracle
- .Net framework data provider for SQL Server

Database managed drop down menus are used in situations where values for the menu are stored and managed outside of the metadata setup dialog. A typical scenario is a customer using Microsoft CRM and needing their users to associate a client with documents that are filed into the document management system. The list of clients can be displayed as a drop-down menu that is dynamically populated from a central list of customers taken from an existing CRM system. If the names of the clients are already stored in a Microsoft SQL server this lookup could be done directly, if not, the CRM system could export (on a scheduled basis) the list values from another SQL server. This will allow them to link or tag documents with clients by using a controlled list of clients that is always current. It is possible to use [internal FileHold data in a database lookup drop down list](#).

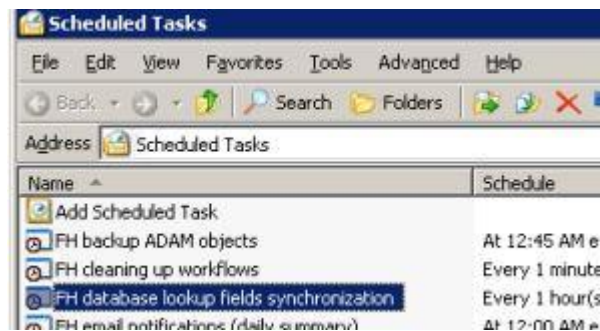
IMPORTANT: Database managed drop down menus is a topic that requires advanced knowledge. Library administrators should consult with Windows system administrators and or

database administrators when they are setting up these fields. The integration of FileHold with external systems is not included in FileCare. FileHold professional services is available to assist with this sort of integration work when needed.

FileHold does not directly retrieve data from the external database for a variety of reasons, but primarily the design wishes to avoid a situation where users would be unable to add a document or do other common functions using that metadata field if the external database was not available at the time of the request.

Instead, the document management server application has a scheduled task that runs hourly, and can also be run manually on demand, that populates all database managed drop down menus. We do not recommend that this task be run at intervals less than the 1 hour default. When you make changes to your external database you need to wait for the hourly scheduled task to run or go to the FileHold server and run the scheduled task manually. The name of this task is [FH database lookup fields synchronization](#).

Once the scheduled task completes, you will then see the information updated in the drop-down menu field as it is used in the product. Refresh the desktop client if using the FileHold Desktop Client or ensure that you have your browser cache disabled so that the Web Client is showing you current information. The exact behavior in the Web Client is dependent on the browser used.



The lookup is performed on the FileHold server in order to provide more security as the connection can be made using integrated authentication using the FH Service account, not the account of the user running the FileHold client application. Since the lookup is made on the server, the database server can be behind a firewall or if one of the additional data providers is used, it only needs to be installed on the server.

The document management system uses an intermediary Microsoft SQL database located within the FileHold Database(s), and a table is created for each individual drop down - lookup metadata field.

If you are creating a drop down list to be used with a database lookup at the schema level, see [Database Lookup](#) for more information.

The Library Administrator may need to work with the Systems Administrator or someone with Microsoft SQL Server experience to make sure that the server settings are correct and function.

Schema lookups can be configured using a Microsoft Access database, Microsoft Excel table, or text file. See [Solution Design Resources](#) for more information.

TO CREATE A DROP-DOWN DATABASE LOOKUP METADATA FIELD

1. In the Web Client, go to [Administration Panel > Library Configuration > Metadata Fields](#).

- Alternatively, in the FDA, go to **Administration > Manage Schemas > Metadata Fields**.
2. In the Add Metadata Field pane, enter a **Name** for the metadata.
3. Enter a **Description** for the metadata.
4. Select a **Drop Down Menu - Database Lookup** field type.
5. From the Web Client, click **Manage Menu Items**.
 - From the FDA, click the **Field Properties** tab.
6. Select the database source:
 - To connect to a SQL database server, select SQL Server.
 - To use ODBC, OLE DB, or Oracle select Custom Data Providers. This option is only available for FileHold 14 or greater and must be enabled in your license. To request a license with this option enabled, please email licensing@filehold.com.
7. Enter the **Server Name**. The Server Name field contains the name of the machine hosting the database from which you are getting the values. The format of the server name is the name only and does not require forward slashes. If the database is hosted on the same server as FileHold, you can use (local) (include parentheses).
8. Enter the **database username** and **password**. Select **Use Integrated Authentication** check box if applicable.
 - If you chose not to use integrated authentication and decide to enter the user name manually, the format for the database username field is just "username" (no quotes) (not "//domain/username"). The FileHold Service Account must be the db_owner of the database being looked up. This can be done in the database software management console looking at the database Security > Logins properties.
9. Click **Verify Connection**.
 - If the username and password is correct, you will get the message "Connection successful".
 - If the username and password is incorrect, you will get the message "Login failed for user "<username>".
 - If you receive a "Cannot connect to specified source" error, this indicates that there is a connection problem to the database. This means that the database name, server name, db admin user name or the db admin password is incorrect. It does not have to do with the select table, field caption or Field ID values. To troubleshoot this issue; confirm all database-related names are correct and ensure that the FileHold Service Account is at least a "data reader" of the MS SQL database being looked up. This can be done in Microsoft SQL Management Studio looking at the database Security > Logins properties.
10. Select the database to be used from the list.
11. Select one of the following options:
 - Single Table – If you are using a single table or view to connect to, select this option then select the table or view name from the list.
 - Custom SQL Query – If you need to use a specific query to return the information from the database, select this option. Note that FileHold does not provide support on writing custom database queries.
12. In the **Lookup By** field, select the database column to look up in the database. This should be the column with unique values or the primary key. If the Lookup By is not unique, there

is a risk of unexpected results and checking remove duplicates would not remove this problem. The Lookup By and Retrieve From fields can be the same database column.

NOTE: If you change the Lookup By field to use a different database column at a later time, this may result in data loss after documents using this field have already been added to the repository.

13. In the **Retrieve From** field, select the database column that you want to be retrieved. The values from this column will populate the drop down list in the metadata field. The Lookup By and Retrieve From fields can be the same database column.
14. Select the **Remove Duplicates** check box to remove any duplicate values from the metadata list.
15. Select the **Alpha Order** check box to have the list alphabetically sorted.
16. Select the **Prevent Deletion** check box so that existing values in metadata fields are never removed even when deleted from the source database. If disabled, any values in the source database that have been deleted will also be deleted inside of FileHold when synchronization occurs. For a deletion, this means the value will be immediately removed from any documents that may have been associated with the value. FileHold considers a deletion a permanent change in the document schema. The original value will no longer exist anywhere in FileHold.
17. If using the Web Client, click **Preview** to view a preview of the metadata field.
 - If using the FDA, select the **Preview** tab.
18. If multiple selections of values are allowed, select the **Allow Multiple Selections** check box.
19. Enter an initial value, if applicable.
20. From the Web Client, click **Save**.
 - From the FDA, click **OK**.

5.4.6. Adding Metadata Fields to Schemas

Once you have your metadata fields created, you can then add them to the schema in order to collect the high level information about the document and search for the specific values.

A good rule of thumb is to have 3-6 metadata fields per schema with at least 50% of them set to "Required". If metadata fields are not flagged as required in the schema, then users can add documents to the system without entering any tagging information. Then when you go to do a search, the document may not be found or may have less relevance in the search results. See [Why Metadata is Important in a Document Management System](#) for more information.

Name	Type	Visible	Required	Clear At Check In	Read Only	Order
Customer ID	Text	☒	☒	☐	☐	1
Customer Name	Text	☒	☒	☐	☐	2
Project	Text	☒	☐	☐	☐	3
Submission Date	Date	☒	☐	☐	☐	4
Comments	Text	☒	☐	☒	☐	5

TO ADD METADATA FIELDS TO THE SCHEMA

1. In the Available Metadata Fields list, select the field names that belong to this schema and click **Add to Schema**.
2. In the Metadata Fields Used by This Schema area, do the following:
 - If the field is to be visible, select the **Visible** check box. To not display the field, clear the check box.
 - If the field is required to be filled out by the user, select the **Required** check box. If the field is optional, clear the check box. If a field is allowed to be optional, then the value can be left blank when a user is adding or checking in a document.
 - To have the value in the field cleared upon check in, select the **Clear at Check In** check box. This is useful when metadata fields such as "Comments" or "Status" needs to be changed for each version.
 - If the field should not be edited by the user, select the **Read Only** check box. There can be an exception to this rule. See the permission setting "Allow the creator of a document to modify the initial value of read-only fields" in the *System Administration Guide*.
 - To set the order of the fields in the Metadata panel, select the order number from the list. For example, if you want the Name field to be first in the list, set this to order number 1. If you want the comments field to be last in the list, set this to the last available number in the list.
 - To remove the metadata, click the **X**.
3. Click **Next** in the Document Schema Wizard to configure Workflow.

5.4.7. Editing and Deleting Metadata

The document management software stores drill down and drop down metadata values as pointers to the actual values. This makes it very easy to changes these values after metadata has already been added to documents. Any changes to the selection text values for these metadata fields is automatically available to all documents that were previously tagged with the value. This is also true if you delete a selection text value. It will be deleted on all documents at the same time.

If you are using a FileHold managed list, there are a couple of different techniques that can be used if you would like to preserve a selection text value you would like to remove from the list.

- The order of the list can be easily controlled with the **Move Up** or **Move Down** buttons. The old value can be moved to the end of the list. You can add the text "do not use" or something similar to the value to let users know the value should not be used any more.
- Add a metadata field specially for preserving the old data. Add the field to any schemas you would like to save the data for. Use advanced search to find all the documents with the old metadata value, select them all, then open the metadata pane for editing. You will be able to edit all selected documents at the same time. Simply add the necessary value to your newly created field and click save. With all documents updated the selection text value can be deleted. The new field for preserving the data can be set to read only if desired.
- When a metadata menu value has been deleted it is automatically removed from every document that it was assigned to, so delete with caution. *There is no undo function.*

IMPORTANT: The same rules as above apply for a database managed list. A big difference is that it is possible to change or delete thousands of records in an instant. If records are deleted by mistake they cannot be recovered even if the original value is added back to the source

table. The values on the documents will already be gone. Depending on your overall solution design, it may be necessary or convenient to update the source table en masse by dropping the table then creating it again. This should be done with extreme caution to avoid the situation that the table is dropped, but not recreated before the synchronization task runs.

The correct method for doing this is to wait for the task to complete in case it is running, disable the task, make the source table change, and enable the task. Optionally the task can be run immediately to load the changes. If you need assistance to create this solution, FileHold Professional Services are available to help.

TO EDIT A METADATA FIELD

WARNING: Once a metadata field has been created and saved, the field type cannot be modified. This is one of the few things that cannot be changed in FileHold.

WARNING: You cannot have duplicate metadata fields in FileHold. Simply rename the obsolete metadata field and create a new one.

1. In Library Administrator, go to [Manage Schemas > Metadata Fields](#).
2. Double click on the metadata field name to edit.
3. Click [Edit Field](#) (Web Client only).
4. Make any changes to the metadata field and click [Save](#) when finished.

TO DELETE A METADATA FIELD

IMPORTANT: Deleting a metadata field is permanent and complete. All current and historical values for the metadata field will also be erased. The user will receive this warning immediately prior to deleting a metadata field that has values associated with it.

1. In Library Administrator, go to [Manage Schemas > Metadata Fields](#).
2. Double click on the metadata field name to edit.
3. Click [Edit Field](#) (Web Client only).
4. Click [Delete](#).
5. At the warning message prompt, click [OK](#). The metadata field is deleted from all associated schemas along with any values that existed prior to the deletion.

5.5. WORKFLOW TEMPLATES

Organizations typically have a number of internal processes for tasks such as order processing, purchase requests, travel expenses, and so on. The FileHold workflow module brings order to these independent processes in a transparent, dynamic, and robust fashion making it a key part of the document cycle.

The FileHold workflow engine is designed to streamline the review and approval process of documents as they proceed through their lifecycle. In collaborative work environments, this labor intensive growth stage of the document is where the most time savings can be realized through the use of workflow.

Workflow is an optional module of FileHold that can be purchased at any time. Contact sales@filehold.com to purchase the workflow module.

A workflow contains from one up to 20 activities. A workflow can be triggered in two ways:

- A user manually initiating a workflow for a version of a document stored in the library. This person is called the **workflow initiator** and is typically the owner of the document.
- **Automatically triggered** by a setting on the document schema.

The persons charged with reviewing or approving the documents are called **participants**. The participants can be defined in the workflow or can be left up to the initiator to select. There is no limit to the number of participants in a workflow.

Once a workflow has been initiated, the first activity begins and moves along in the process using the settings in the workflow template.

In a simple workflow process example, the first activity is to review a document. The participants in this activity are called **reviewers**. The reviewers are notified by email, and in their task list. The task can also be seen in the calendar. The review activity is designed to facilitate the collection of comments on a document from other users. The review activity is considered complete once one or more of the participants (dependent upon what has been configured in the template) have completed the task of reviewing the document.

Once all tasks in the activity are completed, the activity is considered complete and the next activity begins — the approval activity. The participants in this activity are called **approvers**. The approvers are notified by an email and in their task list and responsible for approving, postponing approval, or not approving the document. The task can also be seen in the calendar. The approval activity is designed to facilitate the formal collection of electronic signatures on behalf of its participants for an individual document version in the workflow. The approval activity is considered complete once one or all participants (dependent upon what has been configured in the template) have approved, postponed approval, or not approved the document. The system requires the user to enter their FileHold system password as a secure means of verifying their identity (electronic signature).

During the course of the workflow, **observers** can be designated to watch over the workflow instance. Observers are assigned to watch the workflow but do not participate. They usually do not submit reviews or approvals.

On completion of the last activity in the workflow, it is considered complete. If at any time a workflow approval is not approved, then the workflow is considered terminated and subsequent activities are cancelled.

5.5.1. Ad-hoc Workflow Templates

Library Administrators can create workflow templates that allow the initiator to define some or all of the aspects of the workflow template. This is called an ad-hoc workflow. For ad-hoc workflows, the Library Administrator can allow the workflow initiator to define the activities, participants, tasks, and other properties of a workflow instance.

At every step in the workflow template, the administrator can select the “Allow Initiator to Define” check box which makes the template ad-hoc so that the initiator can define the parameters which initiating a workflow. The check box “Initiator can modify (add/edit or delete activities) this workflow on initiation” can also be enabled. This allows the initiator to edit all aspects of an activity.

Workflow Management

Add Workflow Template

Workflow Name *

Workflow Description

Used in Schemas

☒ Initiator can modify (add / edit or delete activities) this workflow on initiation.

☐ Hide this version of the document until the document is approved.

Email notification ☒ Notify days and hours before for tasks that are going to be overdue.

☐ Repeat notification every hours

Allow Initiator to Define

☒

☒

☒

☒

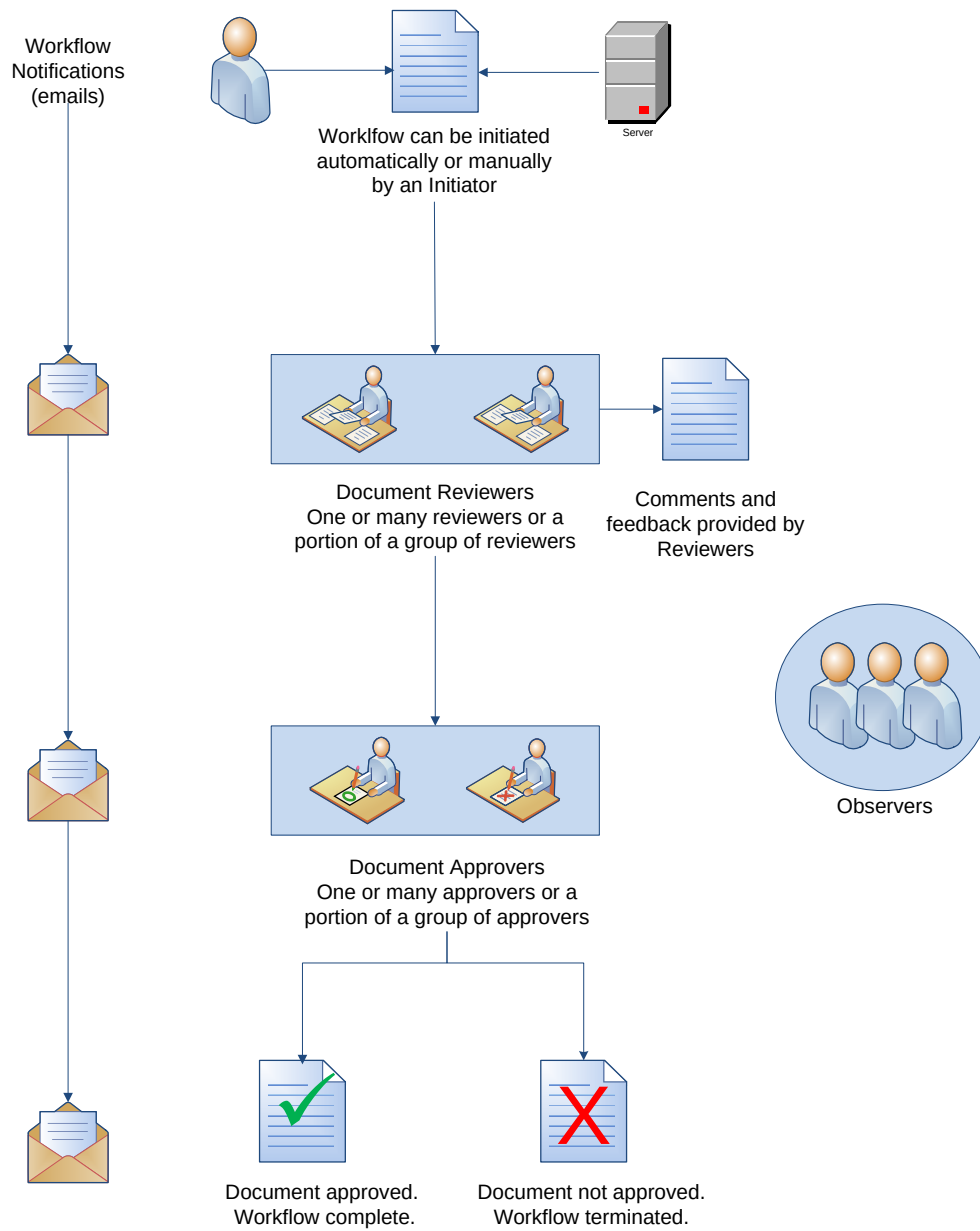
☒

5.5.2. Workflow Template Examples

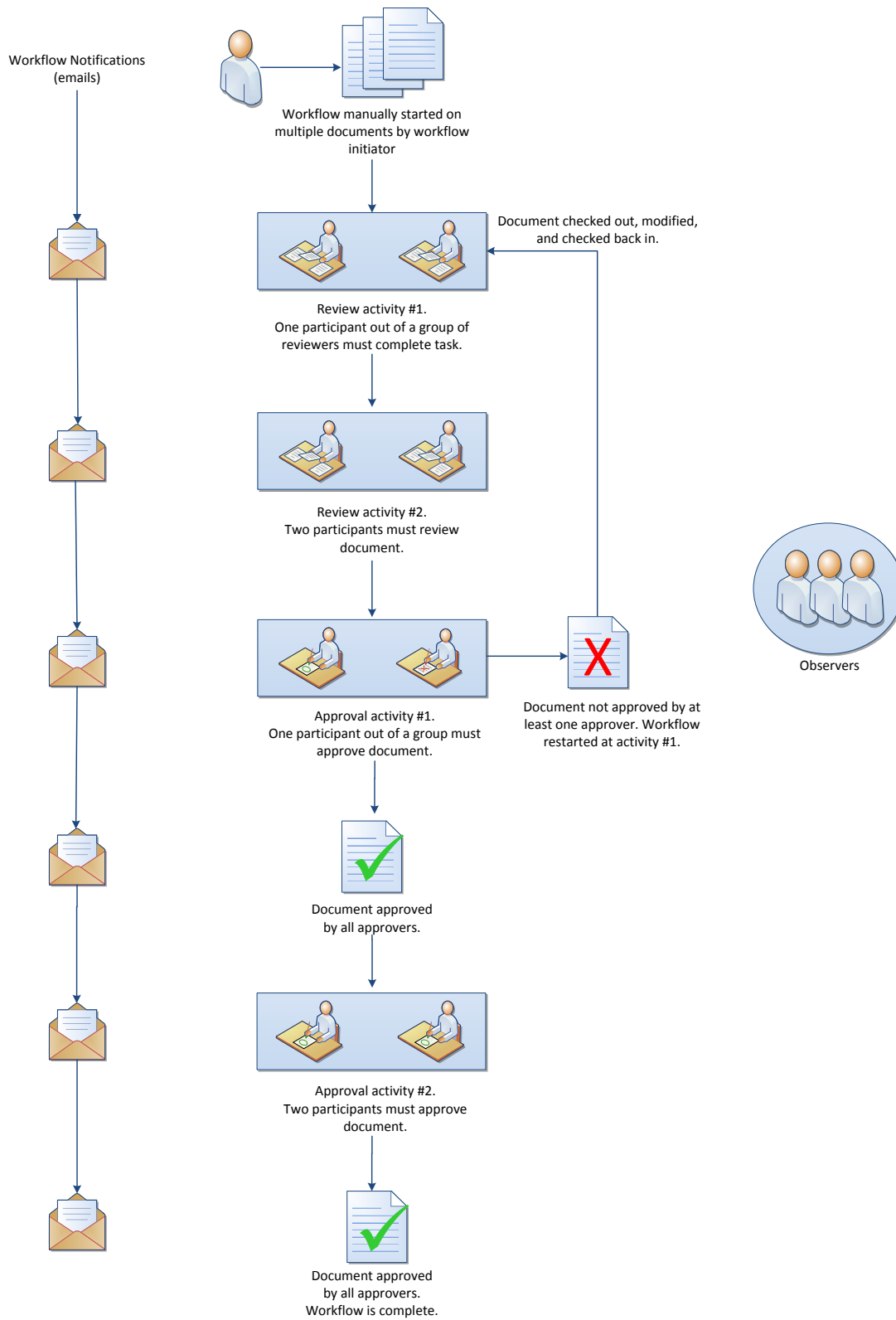
Workflow templates can be created to be as straight-forward or as complex as needed. Simple workflows may have a direct path from start to finish with few activities and minimum of participants involved. Complex workflows may involve one or more restarts, many participants, and several activities.

The flexibility of the document management workflow software allows you to customize your templates according to your organization's requirements. Below are two examples of workflow templates. There is one simple workflow process and one complicated workflow process.

Simple FileHold Workflow Process



Advanced FileHold Workflow Process



5.5.3. Creating Workflow Templates

You can create as many templates as needed for a particular document schemas. For example, you may need to create two different workflow templates for an engineering drawing review. One template sends the document to be reviewed internally and another for the document to be reviewed externally by the customer.

Once the workflow templates have been created, you add them to the [document schema](#). Workflow templates can be used in more than one schema.

When creating workflow templates you can:

- Create up to 20 review and approval activities or a combination of both in a template.
- Make the template “locked down” or “ad-hoc”. [Ad-hoc templates](#) allow the workflow initiator to specify activities, participants, the due date, and task instructions. Locked down templates cannot be modified by the initiator.
- Assign a single participant or a group of participants to an activity. There is no limit to the number of participants.
- Specify if all or only one of the participants need to complete the activity (1 of X).
- If only one of a group of participants is needed to complete the activity, a participant can be forced to reserve the task thereby removing the task from all other participants.
- Include document version owners and workflow initiators as participants in an activity.
- Allow a document to be checked out while it is under the workflow.
- Require a password upon completion of a review or approval activity.
- Restart a workflow from a selected activity. Completed workflows cannot be restarted.
- Specify the frequency of which reminder emails are sent if they are overdue.
- Specify how many days or hours a user has to complete a workflow.
- Include task instructions.
- Hide the current version of the document from other users (non participants and observers) until the document has been approved in the workflow process.
- Have the workflow initiated manually (see the [User Guide](#) for details) or [automatically](#).
- Allow workflow approvals to be postponed.

Approval activities provide a “closed system” electronic signature as required in many compliance environments.

TO CREATE A WORKFLOW TEMPLATE

1. In the Web Client, go to [Administration Panel > Library Configuration > Workflow Templates](#) and click [Add Workflow](#).
 - Alternatively, go to [Document Schema Wizard > Step 4 Workflow](#), click [New Workflow](#).
 - Alternatively, in FDA, go to [Administration > Workflows > Templates](#) tab.
2. Use the following table to fill out the template information:

Field Name	Description
Workflow Name	Enter a name for the workflow template. To set up a custom naming pattern for the workflow name (the name of the workflow that the user sees in notification emails and My Tasks list), click Custom Naming . Read more about setting up the custom naming pattern .
Description	Enter a description for the workflow. It is recommended that you enter as many details as necessary so that users will know exactly what this workflow template is for.
Used in Schemas	The Used in Schemas area states which document schemas this template is being used. This area cannot be edited.
Initiator can modify (add/edit or delete) this workflow on initiation	Select the check box if the initiator can modify all aspects of the workflow activities upon initiation (ad-hoc workflow). Leave this check box clear if no modifications to the activities are to be made.
Reset all activities when adding documents to a postponed workflow	Select the check box if the activities in an "approval postponed" workflow should restart from the first activity in the workflow template when new main documents are added. This allows all of the main documents including any newly added main documents to go through the entire workflow process once again. If the option is not enabled on the template then the workflow is restarted from the activity from which the approval was postponed. Select this option only if the "allow postpone approval" is enabled in the activity.
Hide the document version until the workflow is approved	Select the Hide the document version until the workflow is approved check box to hide the version of the document undergoing the workflow from all users except for the document owner, workflow participants, workflow observers, and designated Library Administrators until such time as it has gone through a workflow instance that contains at least one Approval activity and the result of this activity is that the document is signed off as "Approved". The document version is hidden only during the workflow process until the document version is approved. The document is available at all other times whether it has been approved or not. All other versions will be available for viewing. NOTE: The Hide the document... check box is only enabled when there is at least one approval activity in the workflow template. This check box is not available for review activities.
Email notification	Enter the number of days or hours before a task is overdue to send a task overdue notification email. To repeat the overdue task email notification after a specified period of time, enter the number of hours to resend the email. For example, if 8 hours is entered, an overdue email will be sent every 8 hours until the task is complete. If the repeat notification time is not set, the notification is sent only one time.
Observers	To select a list of observers, click the ... button. In the Select Workflow Observers window, select the groups and/or users to the Current Observers list. Click OK when done.

Field Name	Description
Allow document version owner to observe the workflow	Select the check box to allow the document owner to see the workflow.

3. To add an activity, click **Add Activity**. You can add up to 20 activities in a workflow.

Field Name	Description
Workflow Activity <i>n</i>	In the Workflow Activity <i>n</i> area, select if this activity is an Approval or Review from the drop down list. Click ... to select the users or groups who will be approving or reviewing the document. If you select an Approval activity, each participant is assigned the task of approving and signing off on the document. Users will be asked to enter their password when completing an approval activity to confirm their identity. The list of possible participants is limited to users that are able to access the document. Select the Review activity to solicit feedback on a given document version. As the participants in the activity (reviewers) complete their task, the initiator can collect comments and feedback on the document being reviewed. The list of possible participants is limited to users that are able to access the document. When adding groups to an activity, it will be expanded to individual users upon initiating the workflow. Adding or removing users from a group will not affect existing workflows. In the Select Task Participants window, select the groups and/or users to the Current Participants list. Click OK when done.
Include Document Version Owner	To include the document version owner as a participant in the activity, select the Include Document Version Owner check box. If this option is selected, the list of participants can be left empty.
Include Workflow Initiator	To include the workflow initiator as a participant in the activity, select the Include Workflow Initiator check box. If this option is selected, the list of participants can be left empty.
1 of X	If only one in a group of participants is required to approve or review the document, select the 1 of X check box. For example, if only 1 out of the 5 participants is required to approve the document. The first person to complete the task will void and remove the task from all other participants. Users are able to reserve a task with this option enabled.

Field Name	Description				
Force Reservation	If a single participant in a group is to be forced to “reserve” the task, select the Force Reservation check box. When this option is enabled, it is not possible to submit a review or approval without reserving the task by a single participant. While a task is “reserved” no other participants in the activity will be able to complete the task. If the Force Reservation option is not enabled, a user can still reserve the task. Note that this option is only available if the 1 of X check box is selected. The table below describes the effect of the 1 of X and Force Reservation settings. <table> <tr> <th>Workflow Template Settings</th><th>Effect on Workflow</th></tr> <tr> <td> 1 of X enabled Force Reservation disabled </td><td> - Only one participant in a group of participants in the activity can complete the task. - Participant may “reserve” the task but is not forced to; the task can still be completed without the reservation. - First participant to complete the task voids the task for all other participants. The task is removed from their task list. - The activity is considered complete after a single participant completes the task. If a participant reserves the task: - Only the participant who reserved the task can complete the task. - The status of the task changes to “Reserved” for the participant who reserved it. - The status of the other participants who did not reserve the task changes to “Blocked”. The participant who reserved the task can undo the reservation which frees the task for the other participants to complete. </td></tr> </table>	Workflow Template Settings	Effect on Workflow	1 of X enabled Force Reservation disabled	- Only one participant in a group of participants in the activity can complete the task. - Participant may “reserve” the task but is not forced to; the task can still be completed without the reservation. - First participant to complete the task voids the task for all other participants. The task is removed from their task list. - The activity is considered complete after a single participant completes the task. If a participant reserves the task: - Only the participant who reserved the task can complete the task. - The status of the task changes to “Reserved” for the participant who reserved it. - The status of the other participants who did not reserve the task changes to “Blocked”. The participant who reserved the task can undo the reservation which frees the task for the other participants to complete.
Workflow Template Settings	Effect on Workflow				
1 of X enabled Force Reservation disabled	- Only one participant in a group of participants in the activity can complete the task. - Participant may “reserve” the task but is not forced to; the task can still be completed without the reservation. - First participant to complete the task voids the task for all other participants. The task is removed from their task list. - The activity is considered complete after a single participant completes the task. If a participant reserves the task: - Only the participant who reserved the task can complete the task. - The status of the task changes to “Reserved” for the participant who reserved it. - The status of the other participants who did not reserve the task changes to “Blocked”. The participant who reserved the task can undo the reservation which frees the task for the other participants to complete.				

Field Name	Description	
Force Reservation	Workflow Template Settings	Effect on Workflow
	1 of X enabled Force Reservation enabled	- Only one participant in a group of participants in the activity can complete the task. - Participant may “reserve” the task but is not forced to; the task can still be completed without the reservation. - First participant to complete the task voids the task for all other participants. The task is removed from their task list. - The activity is considered complete after a single participant completes the task. If a participant reserves the task: - Only the participant who reserved the task can complete the task. - The status of the task changes to “Reserved” for the participant who reserved it. - The status of the other participants who did not reserve the task changes to “Blocked”. The participant who reserved the task can undo the reservation which frees the task for the other participants to complete.
Allow Check Out	Select the check box to allow a document(s) to be checked out while under the workflow process. In order for this option to be available on the workflow template, the permission setting “Enable checking out documents when workflow is active” must be enabled in the Administration Panel > System Configuration > General > Permission Settings area. The review or approval cannot be completed while a document in the activity is checked out and the document must be checked in before a review or approval can be submitted. When the document is checked in as a new version, the version number is increased and becomes the version associated with the workflow. If the 1 of X option is selected on the template, then the task is automatically reserved when it is checked out. The task remains reserved after the document is checked in so the user can complete the approval or review task.	

Field Name	Description
Allow Postpone Approval	Select the check box to allow documents to be marked as "Approval Postponed" for an approval activity . There are situations where a document cannot be approved because some conditions have not been met but there is nothing wrong with the document itself. The approval option called "Postpone Approval" can be used in these conditions. Once the "postpone approval" option is selected, the workflow is immediately terminated and the status of the document will be set to "Approval Postponed". A workflow can be started on the same version of a document that has been marked as "approval postponed". If this option is not enabled then the "approval postponed" option is not available when approving documents.
Require Password	This check box is controlled by the permission setting "Enable optional passwords in workflow templates" in the Administration Panel > System Configuration > General > Permission Settings area. If the permission setting is enabled, the Require Password check box is available for use. If the permission setting is disabled, the Require Password check box is unavailable. See the System Administration Guide for more information. Select the check box if the password is required on an approval or review activity. When enabled, users will be forced to enter their FileHold password when completing the review or approval activity. If disabled, no password is required upon completion of an activity.
Due By	In the Due By field, enter the number of days or hours after workflow initiation that the approval or review is due. • Due date is calculated when the workflow is launched, so this field should be configured for the number of days or hours from launch that the first task will be due. For example, if the task needs to be completed in 5 hours, you would enter 0 days and 5 hours. • An exact date and time (fixed) can be specified in the workflow template once the workflow is initiated via manual initiation (if ad-hoc). • In subsequent activities, you can enter the number of days or hours after the previous activity is marked as complete for the next activity to be completed.
Task Instructions	Enter the instructions for the reviewers or approvers.
Allow Initiator to Define	Select the check boxes next to the template items that the Initiator can define. This allows the initiator of the workflow to modify any of these areas upon initiation. See Ad-hoc templates for more information.

4. Repeat the above steps to add up to 20 activities to the workflow template.
5. The order of the activities can be changed using the number drop down list.
6. To remove an activity from the workflow template, click the red X.
7. Click **OK** or **Save** when the template is complete.

5.5.4. Setting up a Workflow Custom Naming Pattern

The custom naming pattern feature allows administrators to define how workflows will be named by default and whether or not to allow end users to edit those default names. The

desired workflow names can be unique and easily identifiable in the My Tasks area, workflow status report and email notifications.

In the naming pattern configuration, you can set the workflow name using the workflow template name, date it was started, workflow initiator, document name of the “initial document”, document version, document owner, FileHold ID, a custom text string, and any of the metadata in the system. This feature is similar to the custom naming pattern on a schema. The length of the workflow name is limited to 500 characters.

The document name of the “initial document” can be used as part of the custom workflow naming pattern. The “initial document” is defined by:

- If there is only one document in the workflow
- If there is more than one document in the workflow, then it is the first document selected

The document name of the “initial document” cannot be changed. It is also displayed in the workflow email notifications.

TO SET THE CUSTOM NAMING PATTERN

1. In a workflow template, click **Custom Naming**.
2. In the Workflow Custom Naming Pattern screen, select **Automatically rename workflows using the custom workflow naming pattern** settings option.
3. In the Constant column, set how values will be separated. The default is underscore (_). The maximum length is 3 characters. Illegal characters are: "/", "\", "|", ":", "*", "?", "\'", "<", ">".
4. In the Profile Field column, select a metadata field, a system value such as workflow name, date started, workflow initiator, document name, document version, document owner, FileHold ID, or a custom text string. All metadata fields in the system appears in the list of available profile fields.
5. In the Field Mask field, enter how the Profile Field will be formatted. See the tables in [Input Masks for Data Controls](#) for rules.
6. Once the custom naming pattern is set, click **OK**.

Workflow Custom Naming Pattern

☐ Do not rename workflows. Use the template name as the workflow name.

☒ Automatically rename workflows using the custom workflow naming pattern settings.

Constant	Profile Field	Field Mask
-	Workflow Name ▼	
-	Document Name ▼	
-	Date Started ▼	DD-MM-YYYY
-	Vendor ▼	
_	None Selected ▼	
_	None Selected ▼	
_	None Selected ▼	
_	None Selected ▼	
_	None Selected ▼	
_	None Selected ▼	

5.5.5. Cloning Workflow Templates

You are able to clone a workflow template instead of creating a new template from scratch. This saves time if you have very similar templates to create.

TO CLONE A WORKFLOW TEMPLATE

1. Do one of the following:
 - In the FDA, go to **Administration > Workflows > Templates**. Right-click on a workflow template name and select **Clone Workflow Template**.
 - In the FDA, go to **Administration > Document Schemas > Manage Schemas > Schema Name > Workflow** tab. Right-click on a workflow template name and select **Clone Workflow Template**.
 - In the Web Client, go to **Administration Panel > Library Configuration > Workflow Templates**. Click on the workflow template name. Click **Clone Template**.
2. The cloned workflow template opens. Make any necessary changes to the template and click **OK**. Note that the template name needs to be unique so needs to be modified. The cloned template is added to the workflow template list.

5.5.6. Adding Workflow Templates to Document Schemas

Library administrators can create workflow templates and associate these templates with different documents schemas. Workflow templates can contain up to 20 activities with an unlimited number of participants.

In order to make a workflow template available to end users for initiation, it must first be associated with a document schema. Users can only initiate workflows that are appropriate to the type of document on which they are working. For example, an 'invoice approval' workflow

template is associated with an 'invoice' document schema. Only library administrators can associate a workflow template with a document schema.

TO ADD A WORKFLOW TO A SCHEMA

1. In the Web Client, go to **Administration Panel > Library Configuration > Document Schemas > Schema Name > Step 4 Workflow**, select the workflow(s) to be associated with this schema and click **Add to Schema**.
 - Alternatively, go to **Library Admin > Manage Schemas > Document Schemas** and double-click on a schema name to edit. Click **Edit**.
 - In FDA, go to **Administration > Manage Schemas > Document Schemas > Schema Name > Workflow** tab.
2. In the Workflows Associated with this Schema area, set the order of the workflows using the **Order** field or delete the workflow by clicking **X**.
3. In the Workflow Settings area, select the **Hide all versions...** check box to hide any versions of the document that have not been approved. The document is automatically hidden upon the addition of the document or creation of a new version from any user not participating or observing in a workflow until that document version is approved. Once the document has been approved, the document is available to those users who have permission to the document. If the document is not approved, then the document version remains hidden.
4. Click **OK** to save your changes or click **Next** in the Document Schema Wizard to configure the Custom Naming.

5.5.7. Automatically Starting Workflows

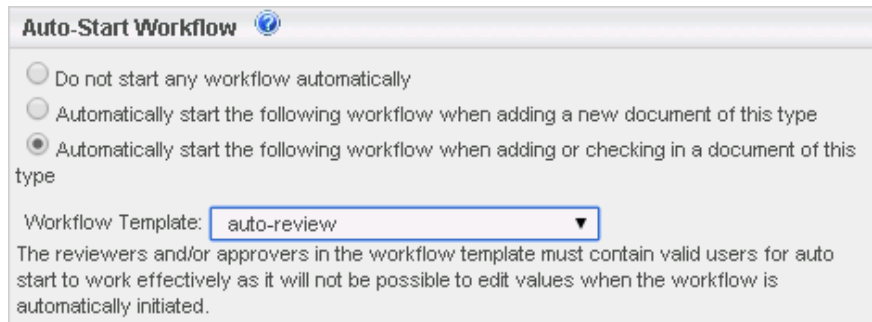
Workflows can be started automatically based on a document schema when they are added to the system or a new version of a document is checked in. Since the workflow is triggered automatically, you cannot use an ad-hoc workflow template. You will need to create a defined workflow template to use with this feature. A workflow cannot be automatically initiated when only metadata is edited.

NOTE: When adding a document through Mobile FileHold that uses automatic workflow initiation, the workflow templates cannot have any part marked as “user-defined” or the document will not be added to the library.

TO AUTOMATICALLY INITIATE A WORKFLOW

1. In the Web Client, in the **Administration Panel > Library Configuration > Document Schema**, select the workflow(s) to be associated with this schema and click **Add to Schema**.
 - In FDA, go to **Administration > Manage Schemas > Document Schemas > Schema Name > Workflow** tab.
2. In the Auto-Start Workflow area, select one of the following options:
 - Do not start any workflow automatically – This option should be selected for ad-hoc workflow templates.
 - Automatically start the following workflow when adding a new document of this type
 - Automatically start the following workflow when adding or checking in a document of this type

- From the drop-down list, select the workflow template you want to use. Only the workflows associated with the schema are available in the list. Note that this cannot be an ad-hoc template.
- Click **OK** or **Save** to save the changes.

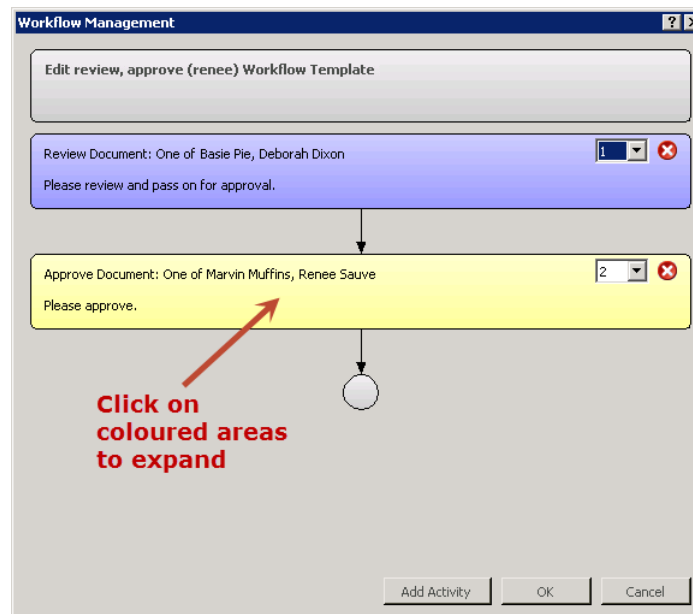


5.5.8. Editing Workflow Templates

You can modify a workflow template at any time. The FileHold Desktop Application has a graphical user interface whereas the Web Client does not.

TO EDIT A WORKFLOW TEMPLATE

- In the Web Client, go to **Administration Panel > Library Configuration > Workflow Templates** and double-click on a schema name to edit. Click **Edit**.
 - In FDA, go to **Administration > Workflows > Templates**. Double-click on a template name.
- In the FDA, click on the coloured areas to expand and contract the different areas of the workflow template.



- Make any changes to the templates and click **OK** or **Save**.

5.6. COURIER

FileHold customers need to send documents stored in the repository or approval tasks to employees, customers, partners, contractors, or associates who are not licensed users of the FileHold system. Courier allows you to transmit documents for viewing or approving to people inside or outside the FileHold system.

Some typical scenarios where this feature will be used include the following:

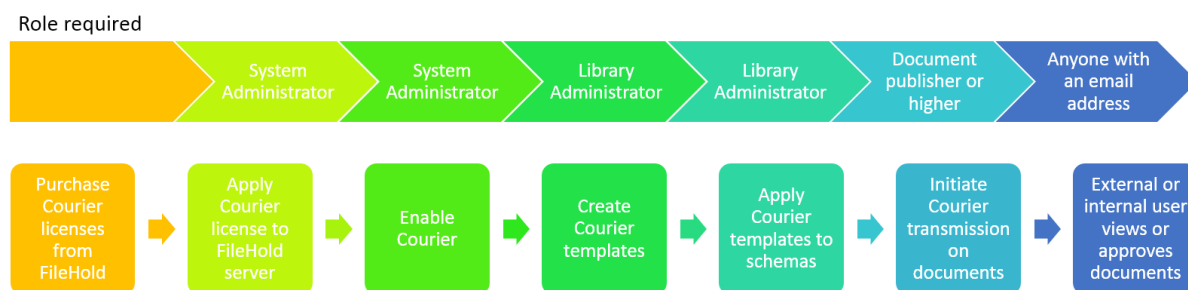
- Engineering transmittals
- Contract approvals
- Employee attestations
- Private document lists
- Expense reports

Courier is a “proof of delivery” system where unlike email it is a secure method of sending documents. With email, there is no way to know if the documents ever arrived, if the attachment could be opened by the recipient. Courier notifies recipients by email of a transmission and the transaction is fully tracked. If the recipient does not view the document by a specified time they can be sent a reminder and the sender can be notified. When they do view the document the viewing will be recorded in the log.

Courier is a pay per use system. Documents can be sent to an enabled FileHold registered user for “free” or customers can prepay for a certain number of “Courier license units” by non-registered users. As a “transmission” is sent to a non-registered user, the transmission is deducted from the amount of Courier units purchased. For more details on Courier licenses, see the [System Administration Guide](#). For pricing details on Courier license packs, contact sales@filehold.com.

Library administrators and higher roles can configure the Courier templates in order to route the documents for viewing or approving. Once the templates are created, they are assigned to document schemas. Anyone who has document publisher rights or higher can start a Courier workflow unless they are restricted to do so by an administrator. See the [End User Guide](#) for more information on initiating Courier transmissions.

The following diagram is a high level overview for setting up and using Courier.



5.6.1. Creating Courier Templates

Courier templates are set up for those users who will be transmitting documents for viewing or approving to internal or external users. Templates include the name, description, target date for the task, sender notifications, password options, actions for the recipients, transmission header and details, and notification email formatting. These templates are assigned to document

schemas which allows users with sufficient rights and permissions to route documents for viewing and approving.

There are two types of Courier recipients: those assigned a registered FileHold user license and those who will be granted Courier licenses as needed. To send transmissions to Courier users, each user must have an email address at minimum. Users are assigned either a viewing or approving activity. Courier license units are purchased for Courier users. An operation in FileHold that supports Courier users will consume one or more Courier user units when the operation is assigned to a Courier user. For example, viewing a document requires one unit and approving a document requires two units.

Once a Courier transmission has been initiated on one or more documents, the recipients in the Courier template receive an email notification. The email notification contains a link to the Courier portal where recipients can then view or approve the documents. A password can be made required when logging into the Courier portal. An additional password requirement can also be set for any approval activity meaning that a password is required when approving or not approving documents.

One time use has no inherent expiry, but the operation imposes an expiry. For example, if a user is asked to approve a document the one time use license will be fully consumed after the approval is complete. If the user is given a document to view, the document will remain viewable on the same license unless the right to view is explicitly removed. Target dates can be included on the transmission such as giving users 3 days to approve a document. Reminder emails can also be sent after a certain time. Transmissions can also expire after a certain time period. If the transmission expires before the user completed the activity, no usage units are consumed.

Library administrators and higher roles can create Courier templates. The templates can be locked down or “ad hoc” where the sender of the transmission can modify the template. For ad-hoc templates, the administrator can select the “Allow sender to define” check box which allows the sender to define the parameters of the Courier transmission.

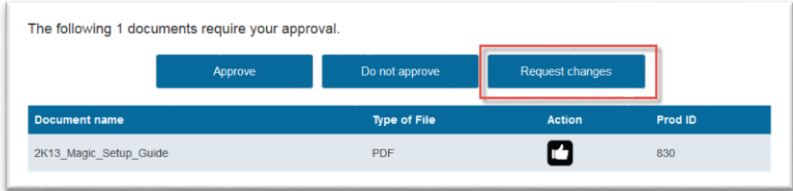
Once the templates are configured and [assigned to schemas](#), users can then initiate a Courier transmission.

NOTE: In a Courier template, the same person cannot have both a review and an approve task assigned to them. It must be one or the other.

TO CREATE A COURIER TEMPLATE

1. In the Web Client, go to **Administration Panel > Library Configuration> Document Schemas > Schema Name > Step 5 Courier**. Click **New Courier Template**.
 - Alternatively, in the Web Client go to **Administration Panel > Library Configuration > Courier templates**. In the List of Courier Templates, click **New Courier Template**.
 - In FDA, go to **Administration > Courier > Templates**.
2. Use the following table to fill out the template information:

Field Name	Description
Courier Name	Enter a name for the workflow template.
Description	Enter a description for the Courier template. It is recommended that you enter as many details as necessary so that users will know exactly what this Courier template is for.

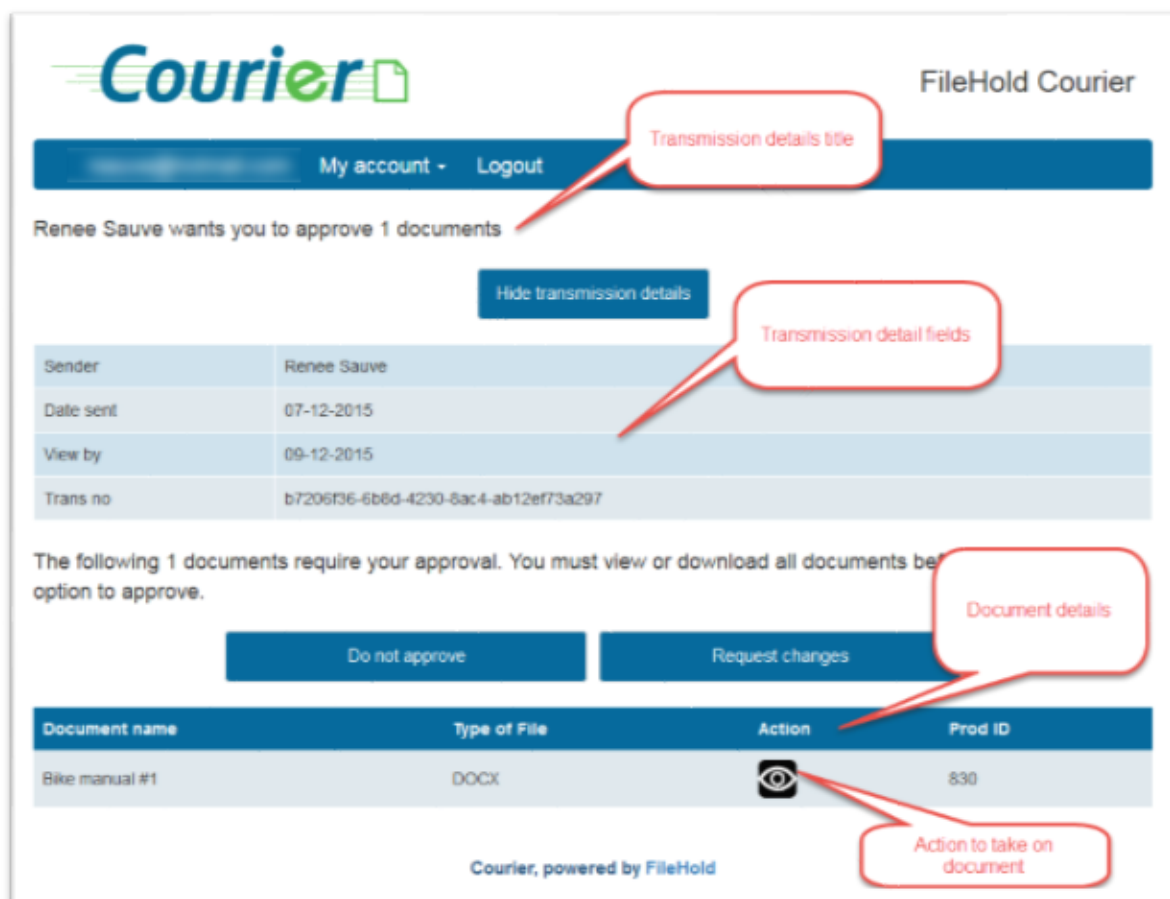
Field Name	Description
Schemas	States which document schemas this template is being used. This area cannot be edited.
Target date	Select the Approval or view due by check box and enter the number of days and hours the recipient has to complete the activity. - Due date is calculated when the workflow is launched, so this field should be configured for the number of days or hours from launch that the first task will be due. For example, if the task needs to be completed in 5 hours, you would enter 0 days and 5 hours. - An exact date and time (fixed) can be specified in the template once the transmission is initiated via manual initiation if Allow Sender to Define check box is enabled. To send reminders of the activity, select the Send reminders every check box and enter the number of days and hours. If the transmission is to expire after a certain time period, select the Transmission expires after check box and enter the number of days. After the transmission expires, the documents are no longer accessible through the Courier portal. An exact date and time (fixed) can be specified in the template once the transmission is initiated if Allow Sender to Define check box is enabled.
Sender notification	Select the Notify before transmission is overdue check box to send an email to the sender of the transmission prior to the due by date and time of the activity and enter the number of days and time. To repeat the overdue task email notification for the transmission sender after a specified period of time, enter the number of hours to resend the email in the Repeat notification every x days and x hours area. For example, if 8 hours is entered, an overdue email will be sent every 8 hours until the task is complete. If the repeat notification time is not set, the notification is sent only one time.
Options	Select the Allow postpone approval check box to allow documents to be marked as "Approval Postponed" for an approval activity. The "Postpone Approval" option can be used in circumstances where a document cannot be approved because some conditions have not been met but there is nothing wrong with the document itself. In the Courier portal, to postpone on an approval, click Request Changes. 

Field Name	Description
	Select the Require access password check box if the user must log into the Courier portal with a password in order to see the transmission. If a password is required to log into the portal, then the first time the user accesses the portal they are required to set their password. CAUTION: If the email address of the recipient is an email address of a user inside of FileHold, the password for the recipient is automatically set to the user's FileHold password.
	Select the Require approval password check box if the user must enter their password to complete the approval process. This is akin to an electronic signature and verifies the approver. CAUTION: If the email address of the recipient is an email address of a user inside of FileHold, the password for the recipient is automatically set to the user's FileHold password.

Field Name	Description
Recipients	The recipient's area is used to assign users to an activity. At least one recipient is required for the Courier template. Click Add  to assign a user a task. In the Add recipients page, select an Activity type: • View — Sends the documents to a user for viewing. A “view” occurs when the document is downloaded through the Courier portal. • Approve — Sends the documents to a user for approving. The user can “approve” or “not approve” the documents as needed in the Courier portal. A signature can also be enforced when approving documents if the Require approval password check box is enabled. Select the Source type and assign the recipients to the activity: • External — Users that do not have registered user accounts and are outside of the FileHold system. Enter the email addresses of the recipients of the activity separated by commas (,) or semi-colons (;). • Internal — Internal FileHold registered users. Select the users or groups and click Add Group or Add User. Assigned users show in the Current Recipients list. • Metadata — Select the metadata field that contains the email addresses for the users for the assigned activity. In the text type metadata field, multiple email addresses can be separated by semi-colons, comma, or newlines. The address can refer to an external user or a FileHold registered user. In the Instructions field, enter the instructions to be completed by the recipients in the activity. Click OK when done. The recipient's activity is added to the list in the template with the action type specified: • View  • Approve  Continue to add more recipients and activities to the list by clicking Add . To edit a recipient, click Edit . To remove a recipient, click Delete .

Field Name	Description
Transmission details	The transmission details is the header information displayed in the Courier portal for each assigned activity. Click Edit  to configure the transmission details. A separate header title can be created for a view activity and an approval activity. The following variables can be used to define the view and approve titles. Upon clicking into the field, a pop-up window opens with the variables displayed. These can be copied from the pop-up window and pasted into the fields for easy use. • [Sender] - name of the user who sent transmission • [Recipient] - name of transmission recipient • [DateSent] - date when transmission has been sent • [DueDate] - date when transmission is going to overdue • [WorkflowName] - name of the transmission • [Instructions] - instructions for recipient • [Action] - displays either "view" or "approve" • [NumberOfDocuments] - number of documents selected for transmission • [DocumentsLink] - displays text like "3 documents" as a link to the documents list For example: <pre>[Sender] wants you to [Action] [NumberOfDocuments] documents by [DueDate]</pre> In the Select Fields area you can determine what information that you want displayed in the transmission header. By default, the system values Sender, Date Sent, View by, and Trans no are shown. Click Add  to add additional fields to the transmission header. The Courier template name, template description, instructions, and any metadata field values can be added. You can continue to add more fields to the list by clicking Add . Change the sort order of the fields by using the Order drop downs. To edit a field, click Edit . To remove a field, click Delete . Click OK when done.

Field Name	Description
Document details	The document details determines what columns are displayed in the Courier portal. These can include Action, Document name, Type of file, or a Metadata field value. By default, document name, type of file, and action is displayed. Click Edit  to modify the information displayed in the document details in the Courier portal. In the Define Document Details screen, click Add  to add additional fields. System values include document name and type of file. Metadata fields can also be used. You can continue to add more fields to the list by clicking Add . Change the sort order of the fields by using the Order drop downs. To remove a column, click Delete . Click OK when done.
Notification emails	The subject line and body of the first, reminder, and cancelled notification emails can be defined. Click Edit  to modify the headers and bodies. The following variables can be used to define the headers and bodies. Upon clicking into the field, a pop-up window opens with the variables displayed. These can be copied from the pop-up window and pasted into the fields for easy use. • [Sender] - name of the user who sent transmission • [Recipient] - name of transmission recipient • [DateSent] - date when transmission has been sent • [DueDate] - date when transmission is going to overdue • [WorkflowName] - name of the transmission • [Instructions] - instructions for recipient • [Action] - displays either "view" or "approve" • [NumberOfDocuments] - number of documents selected for transmission • [DocumentsLink] - displays text like "3 documents" as a link to the documents list For example, the first email header: [Sender] has asked you [Action] [NumberOfDocuments] documents An example for the body of an email: On behalf of [Sender], please [Action] [NumberOfDocuments] documents by [DueDate]. Please review the following instructions for completing the transmission: [Instructions]
Allow sender to Define	Select the check boxes next to the template items that the sender can define. This allows the sender of the Courier transmission to modify any of these areas upon initiation.



3. Click **Save** to save the template. The template can now be [assigned to a schema](#).

TO CLONE A COURIER TEMPLATE

You are able to clone a Courier template instead of creating a new template from scratch. This saves time if you have very similar templates to create.

1. In the Web Client, go to **Administration Panel > Library Configuration > Courier Templates**.
 - In the FDA, go to **Administration > Courier > Templates**. You are taken to the Web Client and need to login if not already logged in.
2. Click on the Courier template name.
3. Click **Clone Template**.
4. The cloned template opens. Make any necessary changes to the template and click **Save**. Note that the template name needs to be unique so needs to be modified. The cloned template is added to the Courier template list.

TO DELETE A COURIER TEMPLATE

Deleting Courier templates will not affect any current transmissions in progress.

1. In the Web Client, go to [Administration Panel > Library Configuration> Courier Templates](#).
 - In the FDA, go to [Administration > Courier > Templates](#). You are taken to the Web Client and need to login if not already logged in.
2. Do one of the following:
 - Click **Delete**  in the Courier template list.
 - Click on the Courier template name and click **Delete**.
3. The message “*You are about to delete a Courier template. This will not affect any transmissions of this workflow that are currently in progress. To cancel or delete transmissions based on this template please go to the Courier transmission report.*” is shown. Click **OK**. The Courier template is deleted.

TO EDIT A COURIER TEMPLATE

You can modify a Courier template at any time without affecting any transmissions currently in progress.

1. In the Web Client, go to [Administration Panel > Library Configuration> Courier Templates](#).
 - In the FDA, go to [Administration > Courier > Templates](#). You are taken to the Web Client and need to login if not already logged in.
2. Double-click on a template name.
3. Click **Edit**.
4. Make any changes to the template and click **Save**. Changes will not affect any transmissions currently in progress.

5.6.2. Adding Courier Templates to a Schema

Once the Courier template has been created, a library administrator can assign the template to the schema. Several Courier templates can be added to the same schema if needed.

In order to make a Courier template available to end users for initiation, it must first be associated with a document schema. Users can only initiate Courier templates that are appropriate to the type of document on which they are working. For example, a “Contract Approval” Courier template is associated with a Contracts document schema.

TO ADD A COURIER TEMPLATE TO A SCHEMA

1. In the Web Client, go to [Administration Panel > Library Configuration> Document Schemas > Schema Name > Step 5 Courier](#).
 - In FDA, go to [Administration > Manage Schemas > Document Schemas > Schema Name > Courier](#) tab.
2. In the list of Available Courier Templates, select the template name and click **Add to Schema**. Add as many Courier templates as needed.
 - Alternatively, in the Web Client, click **New Courier Template** to [create a new Courier template](#).
3. In the Courier template associated with this schema area, set the order of the Courier templates using the **Order** field or delete the template by clicking **X**.

4. Click **Save** to save the changes or click **Next** to set the [Custom Naming](#) for the schema.

5.7. SETTING CUSTOM FILE NAMING

A descriptive, properly named file allows users to learn more about the content of a document without having to open it. Metadata fields can be further leveraged by setting up standardized naming conventions for a document schema. All files will be renamed according to the configured naming pattern once the file is added to the library.

For example, it is possible to have all documents that are added to the system associated with the purchase order schema have a naming convention that starts with a PO then will be followed a dash and then Purchase Order number such as PO-82749204.pdf. As documents are added to the library and associated with the purchase order schema they will be automatically renamed according to this naming convention using the metadata that is associated with the document.

Custom naming patterns can be added to all schema types: electronic records, electronic documents, and offline documents. Only the current version of the document will be renamed if custom file naming is enabled after documents have already been added to the schema.

IMPORTANT: If a metadata field does not have a value and it is used in the naming pattern, the renaming of the file name will be skipped until a value is entered into the metadata field.

IMPORTANT: To comply with Microsoft Windows file name and file path length limitations of 255 characters, Custom File Naming is limited to 100 characters. The following reserved characters cannot be used in file names:

- < (less than)
- > (greater than)
- : (colon)
- " (double quote)
- / (forward slash)
- \ (backslash)
- | (vertical bar or pipe)
- ? (question mark)
- * (asterisk)

TO SET CUSTOM FILE NAMING

1. In the Web Client, go to **Administration Panel > Library Configuration > Document Schemas > Schema Name > Step 5 Custom Naming**.
 - Alternatively, in FDA go to **Administration > Manage Schemas > Schema Name > Custom Naming** tab.
2. Select the **Automatically rename files using the custom file naming pattern settings** option.
 - If you do not want custom naming, select the **Do not rename files** option.
3. In the Custom File Naming Pattern Setting area, select one of the following options on how to manage blank spaces:
 - Leave blank spaces
 - Replace blank spaces with an underscore (_)
 - Replace blank spaces with a hyphen (-)
4. In the File Name Prefix field, enter a prefix (up to 15 characters) for the filename. For example, if you are setting up a purchase order, you can set this to P.O.
5. In the Constant column, set how values will be separated. The default is underscore (_).
6. In the Profile Field column, select a metadata field, a system value such as document version, owner, FileHold ID, created on date and so on, or a custom text string. A custom text string is a 3 character maximum field used to separate the metadata field values in a custom naming string. For example, a custom naming pattern is set to: invoice number (metadata field) - INV (custom text string) - customer name (metadata field) = 1254889-INV-ABCCorp.pdf

NOTE: In versions prior to FileHold 12, only the metadata fields that are set to "Required" in the schema will appear in the list.
7. In the Field Mask, enter how the Profile Field will be formatted. [See Input Masks for Data Control](#) for rules.
8. In the File Suffix Name field, enter a suffix up to 30 characters in length.

9. Click **Refresh** to see the sample naming pattern.

The screenshot shows two panels. The top panel, 'Custom File Naming Standardization', has a 'Rename files belonging to this Schema' section with two radio buttons: 'Do not rename files. Use the existing file name (default)' (unselected) and 'Automatically rename files using the custom file naming pattern settings' (selected). The bottom panel, 'Custom File Naming Pattern Settings', contains a 'Sample Naming Pattern' section with a text box 'AR Invoice Customer Name - InvOCR(L10)' and a 'Refresh' button. Below this is a 'Blank Spaces Handling' section with three radio buttons: 'Leave blank spaces' (selected), 'Replace blank spaces with an underscore (_)' (unselected), and 'Replace blank spaces with a hyphen (-)' (unselected). The 'File Name Prefix' section has a text box containing 'AR Invoice'. The 'Field Mask' section is a table with columns 'Constant', 'Profile Field', and 'Field Mask'.

Constant	Profile Field	Field Mask
	Customer Name - InvOCR	L10
	Invoice #	
	Invoice Date	DD MMM YYYY
_	None Selected	
_	None Selected	
_	None Selected	
_	None Selected	
_	None Selected	
_	None Selected	
_	None Selected	
_	None Selected	

At the bottom, the 'File Name Suffix' section has an empty text box.

10. Click **Next** in the Document Schema Wizard to configure Auto-Filing.

5.7.1. Input Masks for Data Control

Input masks provide a set format for data entry in a field by using characters and symbols. When you apply an input mask to a field, anyone who inputs data in that field must follow the specific pattern defined by the input mask.

The rules for setting field mask values based on the type of metadata field being used in a particular section of the naming structure can be found in the table below.

For Metadata Fields of Type Text, Drop Down Menu, Schema Name, Owner

R(number of limiting characters)	Specifies rightmost characters in a string. Enter the number of character to limit the field by. For example, if you are limiting a text field with the value of FileHold, a field mask of R3 would display "OLD" in the file name.
L(number of limiting characters)	Specifies leftmost characters in a string. Enter the number of character to limit the field by. For example, if you are limiting a text field with the value of FileHold, a field mask of L4 would display "FILE" in the file name.

For Metadata Fields of Type Number, Currency, Version Number, Document No, Size

9	Optional digit placeholder. -Specifies the location of a mandatory decimal point
.	Specifies the location of a mandatory decimal point.
0	Located left or right of a mandatory decimal point, forces padding with zeros.
()	Places parentheses around the mask if the number is less than 0
+	Places + in front of positive numbers, - (minus sign) in front of negative numbers.
-	Places ""(space) in front of positive, - (minus sign) in front of negative numbers.

For Metadata Fields of Type Date

d	Day of the month as digits; no leading zero for single-digit days
dd	Day of the month as digits; leading zero for single-digit days.
ddd	Day of the week as a three-letter abbreviation.
dddd	Day of the week as its full name.
m	Month as digits; no leading zero for single-digit months.
mm	Month as digits; leading zero for single-digit months.
mmm	Month as a three-letter abbreviation.
mmm	Month as its full name.
yy	Year as last two digits; leading zero for years less than 10.
yyyy	Year represented by four digits.

Custom Text Strings

A custom text string is a 3 character maximum field used to separate the metadata field values in a custom naming string. For example, a custom naming pattern is set to:

invoice number (metadata field) - INV (custom text string) - customer name (metadata field) = 1254889-INV-ABCCorp.pdf

5.8. AUTO-FILING SETTINGS

Auto-filing can take documents from the FDA inbox, Manage Imports, Print to FileHold, the Microsoft Office integration, the Add Document Wizard, and the WebCap scanner inbox, and file them into the appropriate folders based on predefined values. This feature helps reduce misfiling and enables faster mass importation of documents.

There are several steps necessary in preparation for using Auto-Filing.

1. Enable the auto-filing feature globally
2. Optional, install the auto-filing script if it is not one of the included scripts
3. Optional, configure the auto-filing script if configuration is required
4. Enable auto-filing on the schema and set the auto-filing script

Auto-filing can take documents from the Inbox and file them into the appropriate folders based on predefined values. This feature helps reduce misfiling and enables faster importation of mass files.

There are five preconfigured auto-filing scripts than can be used. They are:

- **Date-Based** — Documents are filed based on date. The format of the hierarchy is Year-Number > Month Name > Day-Number (Cabinet > Drawer > Folder). For example, if you are filing documents on December 14, 2010, the documents will be automatically filed in the Year-2010 cabinet, December drawer, and Day-14 folder.
- **FilePathFromMD** — Documents are filed based on a value entered in a metadata field. You will need to create a metadata field in the schema that is to be used for auto-filing. The auto-filing script will use the value entered in the metadata field to file the document in the hierarchy. You can enter the Cabinet/Drawer/Folder value in the schema using a predefined separator (such as /, >, -, and so on). For example, you can create a metadata field called “Auto-filing Location” for the Accounting schema. When tagging documents, you enter Accounting/Invoices/Dec2010/ in the “Auto-filing Location” metadata field. The documents will be automatically filed in the Accounting cabinet, Invoices Drawer and Dec2010 folder.
- **FixedDestination** — Documents are filed based on the schema name. The format of the hierarchy is SchemaName Cabinet > SchemaName Drawer > SchemaName Folder. For example, if you are filing documents using the Invoice schema, the documents would automatically be filed in the Invoice Cabinet/ Invoice Drawer/ Invoice Folder.
- **SchemaName-Date-Based** — Documents are filed based on the schema name, then the date. The format of the hierarchy is SchemaName-Year Number > Month Name > Day-Number (Cabinet > Drawer > Folder). For example, if you are filing documents on December 14, 2010, using the Accounting schema, the documents would automatically be filed in the Accounting-2010 cabinet, December drawer, and Day-14 folder.
- **Schema-Based** — A versatile script that can be used to file documents based on a combination of variables. Documents can be filed based on:
 - A document schema name. The schema name is used as the level in the library hierarchy.
 - A metadata field value. The value in the metadata field is used as a level in the library hierarchy.
 - A fixed value. A fixed value is defined in the configuration and is used as a level in the library hierarchy. Read more information on the Schema-based auto-filing script.
 - A system value. Allowed values are created date, document schema, and document name.

Multiple regular expressions can also be used. If one fails to return a non-empty string, the next one is tried and so on until the first match is found.

If you are using the Date-based, FilePathFromMD, or SchemaName-Date-Based auto-filing scripts, you will need to edit the [AutoFilingMembership.XML file](#) to set the proper membership (user or group) for the automatically created hierarchy. If you are using the Schema-Based

auto-filing script, you will need to edit the [Schema-BasedAuto-FilingScript.xml](#) file. If you are using the FixedDestination auto-filing script, no configuration is required.

Customers, partners, and FileHold Professional Services are able to create Auto-filing scripts to meet the needs of your organization. If you require customized auto-filing scripts, please contact sales@filehold.com. Review [Creating Your Own Auto-Filing Script](#) if you would like to make your own auto-filing script.

TO ENABLE AUTO-FILING

1. In the Web Client, go to **Administration Panel > Library Configuration> General**.
2. In the Auto-filing area, select the **Allow user to select auto-filing option when adding documents** check box.

TO SET AUTO-FILING

1. In the Web Client, go to **Administration Panel > Library Configuration > Document Schemas > Schema Name > Auto-Filing**.
 - Alternatively, in FDA go to **Administration > Manage Schemas > Schema Name > Auto-Filing** tab.
2. Select the **Automatically detect/create a destination folder based on auto-filing rules** option.
3. Select the auto-filing script you want to use from the list.



4. Click **Next** in the Document Schema Wizard to configure Event Scheduling.

5.9. EVENT SCHEDULES

You can configure the system to automatically delete, archive, or convert documents to records for a particular schema. You can also configure a notification for important events that are related to documents at some time the future. Event types include:

- **Archive** — The document is moved to the Library Archive in the hierarchy. See an example configuration below:

Edit Send to archive - 1 yr Event

Name *

Description

Event Properties

Type

Relative To

- ☐ Document created date
- ☒ Document last modified date
- ☐ Metadata last modified date
- ☐ Custom metadata field

Select:

Period years

Notifications ☒ Send days before the event occurs.

Recipients

- Delete — “Soft” deletes a document based on the event schedule date. The document can still be recovered in the “soft” deletion state. For more information on deleting documents, see [Permanently Deleting Documents](#).
- Convert to Record — No new versions of the document can be created (locks editing of the document) but remains in the Library.
- User defined – An email and/or document alert is sent to recipients to notify them of an important date or event. For example, for policies that must be updated or reinstated at least once every three years, the policy team wants to set up a notification on the policies’ expiry dates 60 days before the three year anniversary. The alert repeats every three years. No action is taken upon the document itself. See the example configuration below.

Add Event

Name *

Description

Event Properties

Type

Relative To

- ☐ Document created date
- ☐ Document last modified date
- ☐ Metadata last modified date
- ☒ Custom metadata field

Select:

Period years

☒ Recurring Event

Notifications ☒ Send days before the event occurs.

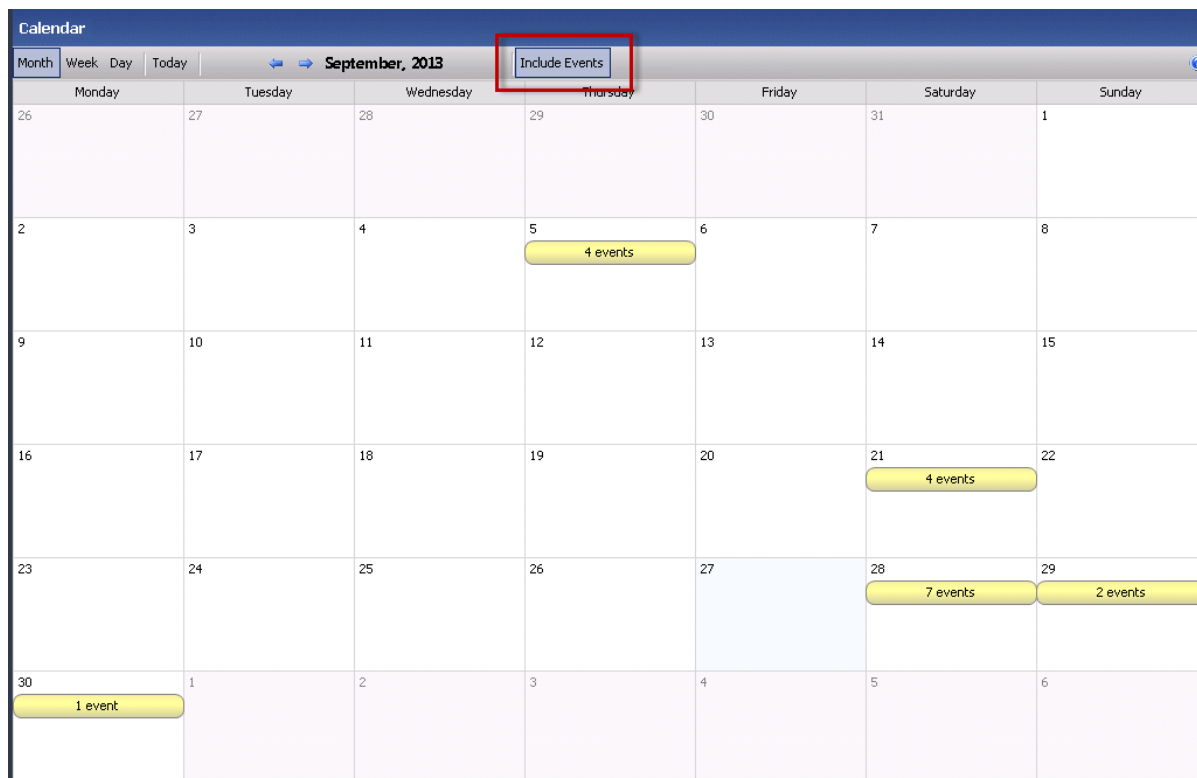
☒ Email message

☒ Document alert

Recipients ☒ Notify Document Owner

The events are triggered based on the document creation date, last modified date, metadata last modified, or a [custom date metadata field](#). These triggers can then be additionally offset for a period measured in days, weeks, months, or years.

Events can be viewed in the Calendar by clicking Include Events. They can only be viewed by Senior Library Administrators or higher roles.



Email notifications can be sent to other users to alert of a document event. These notifications are configured to go out to selected users an assigned number of days before the event takes place. Event notifications can only be sent to Library Administrators and higher roles.

In order to use the events features, the System Administrator must enable them. Library Administrators can then create and apply events to schemas. See the [System Administration Guide](#) for more information.

5.9.1. Using Custom Metadata Fields for Retention Policies

If you are using a custom date-type metadata field for an event schedule or retention policy, that metadata field must be made "read-only" in the document schema. This only applies to delete, archive, and convert to record event types.

NOTE: Using read-only metadata fields for custom dates does not apply to User defined event types.

The read-only setting prevents users from changing dates that triggers mass deletion or status changes for all those documents in a given schema. However, any user with a role of Cabinet Administration or higher can modify the "read-only" date value in the metadata pane.

You could also allow the modification of the read-only date value for when users (lower than Cabinet Administrators) are first adding the document to the system by enabling the permission "Allow the creator of a document to modify the initial value of read-only fields" which is set in

the **System configuration > General** permission settings area. After this initial date value change, the date is no longer editable by users with permissions lower than cabinet administrator. See the [System Administration Guide](#) for more information.

NOTE: A metadata field cannot be made Required and Read Only. In this context, it can only be set as Read Only.

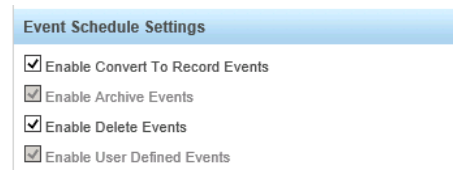
5.9.2. Applying Retention Policies to Document Schemas

To create an event schedule to a schema, you need to do the following:

- [Enable event schedules in the System Administrator view.](#)
- [Create event schedules in the Library Administrator view.](#)
- [Apply the event schedule to the schemas.](#)

TO ENABLE EVENT SCHEDULES

1. Log in as System Administrator, and go to **Administration Panel > System Configuration > General**.
2. In the Event Schedule Settings area, select the following check boxes, if applicable:
 - Enable Convert to Record Events — Allows documents to be automatically converted to a record after a specified period of time.
 - Enable Archive Events — Allows documents to be automatically sent to the archive after a specified period of time.
 - Enable Delete Events — Allows documents to be automatically deleted after a specified period of time.
 - Enable User Defined Events — Allows email and/or document alerts to be sent to specific administrative groups or users to notify them of an important document date or event.
3. Click **Update**.



Event Schedule Settings	
☒	Enable Convert To Record Events
☒	Enable Archive Events
☒	Enable Delete Events
☒	Enable User Defined Events

TO CREATE AN EVENT SCHEDULE

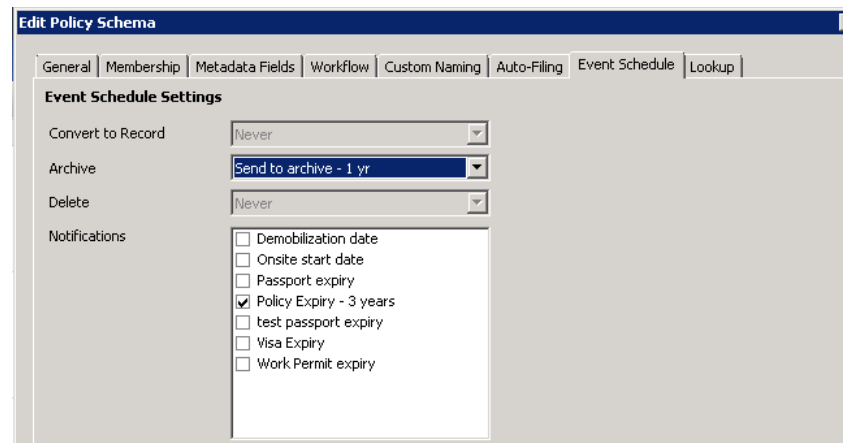
1. Do one of the following:
 - In the Web Client, log in as **Library Administrator** and go to **Administration Panel > Library Configuration > Events**.
 - In the FDA, go to **Administration > Manage Schemas > Events**.
2. Click **Add Event**.
3. In the Add Event window, enter a name.
4. Enter a description for the event.
5. Select one of the following event types:

- Archive — The document is moved to the Library Archive.
 - Delete — The document is deleted.
 - Convert to Record — The document is converted to a record. The document can no longer be edited or altered.
 - User Defined — Emails and/or triggers document alerts to notify specific users of an important document date or event.
6. Select the date that the event is relative to:
 - Document created date
 - Document last modified date
 - Metadata last modified date
 - Custom metadata field – Select the metadata field name from the list. For example, a policy expiry date field. See [Using Custom Metadata Fields for Retention Policies](#).
 7. In the Period area, do one of the following:
 - For archive, delete, or convert to record events, enter a period of time before the event takes place in days, weeks, months, or years. For example, you want the document to be converted to a record 1 year after the document was created.
 - For notification events, enter the period of time before the event will occur. For example, a policy document expires after three years. If this is a recurring event, select the **Recurring** check box. For example, the policy expires every 3 years.
 8. Select the **Notifications** check box if you want to send emails to users to notify them of the event.
 9. Enter the number of days prior to the event that you want the email notification to be sent.
 - If this a User defined event, select the Email Message and/or Document Alert check boxes to receive these types of alerts. For example, the specified users will receive an email and an alert 60 days before the expiry date.
 10. Click the ... button to select Recipients for the email notification. Any groups or users higher than Senior Library Administrator can be added.
 - For a User defined event, select the **Notify Document Owner** check box to send an alert and/or email notification to the document owner.
 11. Click **Save** or **OK**.

TO ADD AN EVENT SCHEDULE TO A SCHEMA

1. In the Web Client, go to **Administration Panel > Library Configuration > Document Schemas > Schema Name > 7. Event Schedule**.
 - Alternatively, in FDA go to **Administration > Manage Schemas > Document Schemas > Schema Name > Events tab..**
2. Select the event that you want to occur to the documents assigned to this schema from the list:
 - Convert to a record
 - Archive
 - Delete

- User Defined – Select the check box next to the user defined event. The number of events that can be selected is determined by a setting in a configuration file on the server. See [Setting the Number of User Defined Notifications in a Schema](#) for more information.



3. Click **Save** or **OK**.

5.9.3. Setting the Number of User Defined Notifications Allowed in a Schema

The number of user defined events that can be enabled in a schema is determined in a configuration file in the server. The default is 5 events.

To change the allowable number of user defined events in a schema, open the web.config file in *C:\Program Files\FileHold Systems\Application Server\LibraryManager*. Edit the following setting:

```
<add key="UserDefinedEventsMaxNum" value="5" />
```

5.10. DATABASE LOOKUP ON THE SCHEMA

The Lookup tab in the schema properties allows you to retrieve database information into additional metadata fields of a schema based on the value entered into the mapped metadata field. Once the user enters a value for the metadata field that is used as the “look up” value, a query can be executed on an external database to retrieve additional values that are mapped to the other metadata fields in the schema.

This mechanism does not require any synchronizing with the FileHold database because it is derived directly from the external database. The look up is performed on the FileHold server in order to provide more security as the connection is made using the FH Service account.

Only one database lookup is allowed per schema. The lookup can be performed when adding or editing the metadata of a **single document**. You cannot use the lookup when tagging multiple documents. See the [User Guide](#) for information on entering metadata based on database lookups.

After performing a lookup, users can still modify any of the retrieved values. The system will not verify if the values match the original data record and it will not update those values when the record is modified in the external database.

When creating metadata fields for the schema that is using database lookups, any type of metadata field can be used (text, number, drop down list) as long as it matches the format of the lookup column. For example, if you have a number type metadata field mapped to a lookup

column that uses letters then the lookup functionality will not work. In this case, using a text field for most metadata fields will work best as it accepts any letter or number combination.

Schema lookups can be configured using a Microsoft Access database, Microsoft Excel table, or text file. See [Solution Design Resources](#) for more information.

TO CONFIGURE DATABASE LOOKUP FOR THE SCHEMA

1. In the Web Client, go to **Administration Panel > Library Configuration > Document Schemas > Schema Name > 8. Lookup**.
 - Alternatively, in FDA go to **Administration > Manage Schemas > Schema Name > Lookup** tab.
2. To enable schema database lookup, select the **Enable Schema Lookup** check box.
3. Select the database source:
 - To connect to a SQL database server, select **FileHold Configured SQL Server Connection**.
 - To use ODBC, OLE DB, SQL, or Oracle select **User Configured Database Server Connection**.
4. If you selected **FileHold Configured SQL Server Connection**, do the following:
 - Enter the **Server Name**. The Server Name field contains the name of the machine hosting the database from which you are getting the values. The format of the server name is the name only and does not require forward slashes. If the database is hosted on the same server as FileHold, you can use (local) (include parentheses).
 - Enter the username for the SQL server.
 - Enter the password for the SQL server.
 - Select **Use Integrated Authentication** check box if applicable. If you chose not to use integrated authentication and decide to enter the user name manually, the format for the database username field is just "username" (no quotes) (not "//domain/username"). The FileHold Service Account must be the db_owner of the database being looked up. This can be done in the database software management console looking at the database Security > Logins properties.
5. If you selected **User Configured Database Server Connection** do the following;
 - Select the Data Provider from the list: .Net Framework for Data Provider for ODBC, .Net Framework Data Provider for OleDb, .Net Framework Data Provider for Oracle, .Net Framework for Data Provider for SqlServer.
6. Enter the **Connection String** to the external database. Click **Verify Connection**.
 - If the username and password is correct, you will get the message "Connection successful".
 - If the username and password is incorrect, you will get the message "Login failed for user "<username>".
 - If you receive a "Cannot connect to specified source" error, this indicates that there is a connection problem to the database. This means that the database name, server name, db admin user name or the db admin password is incorrect. It does not have to do with the select table, field caption or Field ID values. To troubleshoot this issue; confirm all database-related names are correct and ensure that the FileHold Service Account is at

least a "data reader" of the MS SQL database being looked up. This can be done in Microsoft SQL Management Studio looking at the database Security > Logins properties.

7. Select the **Database** to be used from the list.
8. Select one of the following options:
 - Single Table – If you are using a single table or view to connect to, select this option then select the table or view name from the list.
 - Custom SQL Query – If you need to use a specific query to return the information from the database, select this option. Note that FileHold does not provide free support on writing custom database queries. For assistance on custom queries, contact sales@filehold.com.
9. If **Single Table** was selected, do the following:
 - In the **Select Table** field, select the name of the table or view.
 - In the **Lookup By** field, select the database column to look up in the database. If you are using a drop down database managed metadata field, this value is set to the same value used as the Lookup By field defined in the drop down menu metadata field. This should be a column with unique values or the primary key.
10. If **Custom SQL Query** was selected, do the following:
 - Enter the **Query**. Note that FileHold does not provide support on writing custom database queries. If you need assistance, contact sales@filehold.com for a price quote.
 - Select the **Parameter Type** from the list.
 - Select the Parameter **Name** from the list and click **Verify Query**.
11. In the **Lookup Using** field, select the metadata field that corresponds to the metadata field used in the schema for the lookup drop down list. If you are using a document control number that is manually generated, you can use that value as the lookup field as long as there is a corresponding match in the lookup database.

WARNING: If you change the Lookup Using field to use a different database column at a later time, this may result in data loss after documents using this field have already been added to the repository.
12. Map the additional **Source Column** to the **Destination Metadata Fields** used in the schema.

TIP: It may be desirable to use database dropdown menu fields as destination fields in the lookup when those fields are extracted from the same data source used in the lookup. In this case the source column should be the same field set for the Lookup By value. For example, you have a table with three columns: Id, NameFld, TitleFld. You create two metadata fields Name and Title as database dropdown menus. In the lookup tab you set the Lookup By to Id, Lookup Using to Name. To set the Title field you use Id as the source column.

Edit Bicycle Manuals Schema

General | Membership | Metadata Fields | Workflow | Custom Naming | Auto-Filing | Event Schedule | **Lookup**

Lookup settings

☒ Enable Schema Lookup

☒ FileHold Configured SQL Server Connection ☐ User Configured Database Server Connection

Server Name * ☐ Use Integrated Authentication

Database Username *

Database Password *

Select Database *

☒ Single Table ☐ Custom SQL Query

Select Table *

Lookup By *

Lookup Using *

Source Column		Destination Metadata Field
ModelName	map to	Bike Model
Color	map to	Colour
ListPrice	map to	List Price
Size	map to	Size

13. From the Web Client, click **Save**.

- From the FDA, click **OK**.

6. GENERAL LIBRARY SETTINGS

Use the General Settings to configure features such as permanent deletion of records, email attachment settings, email notification, extraction of email metadata, and enabling auto-filing.

6.1. PERMANENTLY DELETING DOCUMENTS

The FileHold server deletes documents in two stages:

- **Soft delete** — The first stage is when a user deletes a document directly from the library or is deleted through a [deletion scheduled event](#). Files that have been soft deleted are no longer accessible from the library but still can be recovered by Library Administrators using the [Recover Documents](#) utility. This is considered to be a “soft deletion”.
- **Hard delete** — In the second stage, documents in the soft deletion state are permanently deleted after a set period of time. Documents that have been permanently deleted cannot be recovered. This is considered to be a “hard deletion”.

You can set the period of time after which documents should be permanently deleted after they surpass the “soft deletion” stage.

NOTE: You can schedule documents to be automatically deleted by scheduling an event and then adding it to a schema. Read more information about [scheduling events](#).

TO SET WHEN DOCUMENTS ARE HARD (PERMANENTLY) DELETED

1. In Web Client, go to **Administration Panel > Library Configuration> General**.
2. Under General Settings, enter the number of days that a document can be permanently deleted after it has been soft deleted. Enter a value between 1 and 1000 days with the default of 7 days.
3. Click **Update**.

6.2. DOCUMENT LINKS SETTINGS

Different types of document links can be configured for the FDA, Web Client, and the guest Web Portal. These links can be shown in the metadata pane or included in emails as link type attachments. You can also specify if the link should go to the latest version or a specific version. If the specific version option is configured, then the user is brought to the version history instead of directly to a document. The default URL can also be set.

For the web client and web portal (guest portal) type links, there are three modes for how the links are executed in the user interface:

- **Normal** goes directly to the document location and highlights the document through the Web Client.
- **Direct** mode opens the document directly in the FileHold Web Viewer or it will download directly to the browser if there is no Web Viewer or the document format is not supported by the Web Viewer.
- **Locked direct** (using the UI=Lock option) mode opens the document in the Web Viewer or browser (depending on the file type) but the rest of the FileHold interface (such as the Library tree and menus) is hidden. This option is meant to be used when integrating the Web Viewer with other applications.

For the FDA only normal mode is available.

The document links can be made visible to all users or to just the administrators in the metadata pane. If the links are made visible to all users, then the link "All URLs" is shown in the version properties. When clicked, the specific URLs are shown. By default, the Web Client and FDA links are already created when FileHold is installed with the Web Client link as the default.



The available link types for emails are set in the [Email Attachments Settings](#) area. Library administrators can determine which link types can be sent in an email. Email attachments can be sent out as a link or as a traditional "paperclip" attachment.

TO CREATE DOCUMENT LINKS

1. In Web Client, go to **Administration Panel > Library Configuration > General**.
2. In the Document Links Settings area, select the **"All links" option visible to everyone** check box if all the link types will be available to all users in the metadata pane. If this option is not enabled, then only Senior Library Administrators or higher will see these links in the metadata pane and users will have access to only the default URL.
3. By default, the Web Client and FDA links are already created when FileHold is installed. The Web Client link is the default. To create a new link do the following:
 - In the Name field, enter a name for the link.
 - In the Context field, select if the link is for the Web Client, FDA or Web Portal (guest portal).
 - In the User Interface field, select if the link is a Normal, Direct, or Locked Direct link type. Note that for FDA the only option is Normal.
 - In the Document Version field, select if the link will take you to the latest version or a specific version (version history).
4. Click the **+** (plus sign) to save the link and/or to add another link type.
5. To remove a link type, click the **-** (minus sign).
6. To edit a link, click the **Edit** (pencil).
7. To set the default URL, select the check box next to the link name or click **Edit** to set the default for an existing link.
8. To reorder the links so that they are displayed in a specific order in the metadata pane, click **Reorder**. In the Document Links Reordering window, drag and drop the link names to reorder. Click **Save Ordering** to save your changes.

- Click **Update** at the bottom of the page.

Document Links Settings

This section allows administrators to create and configure the custom types of the URLs.

☒ "All links" option visible to everyone

Is default	Name	Context	User interface	Document version
  	Default WebClient	Web Client	Normal	Latest
 	Default FDA	FDA	Normal	Latest
 	Guest Portal	Web Portal	Normal	Latest
 		Please Select	Please Select	Please Select

 Reorder

6.3. EMAIL ATTACHMENTS SETTINGS

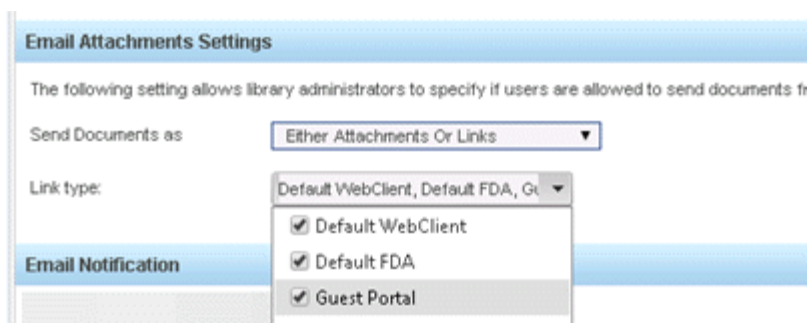
The email attachment settings allows you to specify if users are allowed to send documents from the Library as attachments or as a Document URL link when emailing documents from FileHold. You can also specify the types of links that can be included in the email. The links available depends on the links configured in the [Document link settings](#) area.

If documents are emailed as a document URL / links then only users with proper security membership can access the documents when they click on the link. A login is required and the user is taken to the area of the system where the document is located. The document is highlighted and can then be retrieved via get a copy or check out.

If documents are emailed as attachments, then the document can be modified outside of FileHold. If a document is modified outside of the document management system, then FileHold has no way of knowing what changes occurred.

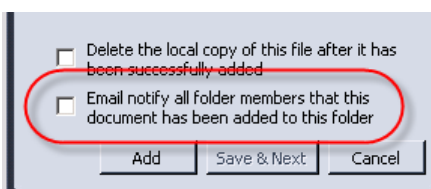
TO SET EMAIL ATTACHMENT SETTINGS

- In Web Client, go to **Administration Panel > Library Configuration > General**.
- In the Email Attachment Settings area > Send Documents As field, select one of the following:
 - Either Attachments or Links
 - Attachments Only
 - Links Only
- If links are allowed, then in the **Link Type** field, select the check boxes next to the document link name that can be used in email attachments. See [Document link settings](#) for more information.
- Click **Update** at the bottom of the page.



6.4. EMAIL NOTIFICATION

When enabled, the email notification displays a check box option that allows users to notify Folder members that a new file is added or checked in. This can be a useful tool for some environments but restricted in others. The check box option "Email notify all folder members that this document has been added to this folder" is available during adding and check-in events. If disabled, this check box is not available.



This does not end the ability for users to email documents, [set reminders on folders or documents, or receive email reminders, configuring general notifications in Library Administration](#) or other user subscription driven [alerts](#). This setting within Library Administration only globally removes the ability to notify all folder member(s) upon document add event or check in an existing document.

TO ALLOW EMAIL NOTIFICATION WHEN A DOCUMENT IS ADDED OR CHECKED IN

1. In the Web Client, go to **Administration Panel > Library Configuration> General**.
2. In the Email Notification area, select the **Allow Push Email Notification on Add File or Check in File Events** check box. This feature is enabled by default.
3. To disallow email notifications globally for all users, clear the check box. This will remove the "Email notify all folder members..." check box when adding or checking in new documents.
4. Click **Update**.

6.5. AUTO-FILING

Auto filing can streamline the importation of files from scanner or file share / network shared drive. See [Auto-filing Settings](#) for more information.

In order to enable auto-filing, select the **Allow user to select auto-filing option when adding documents** check box.

6.6. WORKFLOW INITIATION CONFIGURATION

In the workflow initiation settings, you can determine how workflows are initiated when multiple documents are selected:

- A separate workflow is initiated for each selected document resulting in multiple workflows being initiated.
- A single workflow is initiated containing multiple documents.
- A prompt for the user each time a workflow is initiated on multiple documents allowing them to choose an option.

TO SET THE WORKFLOW INITIATION SETTING

1. In the Administration Panel, go to **Library Configuration > General**.
2. In the Workflows area, select the option for when a user initiates workflows:
 - One workflow
 - Separate workflows
 - Prompt user
3. Click **Update**.

6.7. RESTRICTING ACCESS TO THE DOCUMENT MANAGEMENT SYSTEM

You can restrict access to the document management system at any time. This allows only Administrators to access to FileHold during an upgrade or when making major changes to the system. When access is restricted, users will not be able to log in.

If access has been restricted and a user attempts to log in they will receive a warning message *"You cannot log in because the system access is currently restricted by the administrator."*

TO RESTRICT ACCESS TO THE SYSTEM

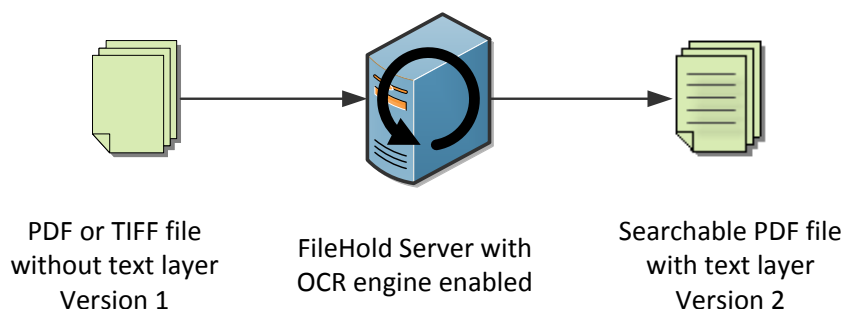
1. In the Web Client, go to **Administration Panel > Library Configuration > General > Restricted Access** area.
2. Set the level of restriction to one of the following options:
 - All Users – All users have access to the system. Both Library Administrators and System Administrators can set this option.
 - Library and System Administrators – Only Library and System Administrators have access to the system. Both Library Administrators and System Administrators can set this option.
 - System Administrators – Only System Administrators have access to the system. Only System Administrators can set this option.
3. Click **Update**. Remember to resume access to the system after your updates have been made.

6.8. SERVER SIDE OCR

The FileHold server side OCR feature can provide OCR (optical character recognition) for PDF and TIFF documents so that they can be indexed and searched. Once the mechanism completes the processes of OCR'ing the document, the document is checked in as a new

version that contains a text layer that allows the document to be indexed and searched within the document management system.

Only PDF and TIF/TIFF type documents are processed in the OCR process. TIFF images are converted to searchable PDF documents upon completion. Once the OCR mechanism completes, the OCR'd document is checked in as a new version with the owner remaining the same. This new version is then processed by the full text search engine so it becomes searchable.



Server side OCR can be a time consuming mechanism; therefore, documents are added to a queue to be processed. All new documents and new versions, manually added or through an import mechanism (such as watched folders or managed imports), are automatically added to the queue. Older documents can be added manually to the queue in the System Administrator > General page.

In order to use this feature, it must be enabled in the System Configuration > General page. See the [System Administration Guide](#) for more information.

6.8.1. Configuration of Server Side OCR

The languages supported “out of the box” by the OCR engine are: German, English, French, and Spanish. The language configuration can be modified by a setting in the web.config file server under *C:\Program Files\FileHold Systems\Application Server\DocumentRepository*.

Under <appSettings>, add the following parameters:

```
<add key="OcrLang" value="LanguageCode" />
<add key="OcrDpiResolution" value="123" />
```

The default configuration is a 300 DPI resolution and English language. Other languages may be available through FileHold Professional Services. Contact sales@filehold.com for more information.

The scheduled task “FH OCR documents” can be modified for the frequency and time frame when the OCR’ing occurs in the Task Scheduler. The default is set to repeat every 5 minutes.

The following items can be configured in the web.config file located in *C:\Program Files\FileHold Systems\Application Server\LibraryManager* if needed when OCR’ing documents.

- The entry is called `<add key="OcrCommandTimeoutSec" value="270" />`. This is the maximum amount of time in which the server side OCR task runs. The OCR process continues if this value is exceeded. This value does not usually need to be changed unless there are a large number of documents in the queue and more than one document needs to be processed per execution.

- The maximum number of documents that can be processed in the set amount of time can be configured in the same web.config file under the entry `<add key="OcrMaxDocuments" value="10" />`.
- For larger size documents (over 10 MB), the `WebServiceCallTimeoutSec` setting in the web.config file should be set to 3600. This forces the Library Manager to wait for a longer response time from other services in order to process the documents without timeouts.

Server side OCR is an optional feature that is controlled in the FileHold license. To purchase the server side OCR feature, contact sales@filehold.com.

6.8.2. OCR Status

In the OCR Status page, the current status of the OCR engine and any warnings or errors for documents that cannot be processed are shown.

In the General area, the following information is displayed: the status of the OCR engine (enabled/disabled), if the higher priority of newly added documents or versions is enabled, the number of pending documents, and the number of processing errors as well as the list of errors.

When an error or warning occurs while the server performs the OCR, the document is removed from the queue and added to the List of Errors. The List of Errors shows the type (warning or error), FileHold ID, date that the error occurred, and the error details. OCR errors can occur when:

- The document is checked out.
- The document is under an active workflow.
- The document is encrypted, password protected, or corrupted.
- The document does not have any valid text that can be recognized.
- A newer version of a document has been checked in.
- File has an invalid extension.

This information about the error is displayed in the Details column. If an error occurs for checked out or active workflow documents, these can be repaired by manually re-adding the documents to the queue at a later time.

Once the OCR mechanism completes, the OCR'd document is checked in as a new version. The OCR'd PDF is checked in with the same owner as the previous owner. This new version is then processed by the full text search engine so it becomes searchable.

TO VIEW THE OCR STATUS AND ERRORS

1. Go to **Administration Panel > System Management > OCR Queue Status**.
2. In the General area, the following is displayed:
 - OCR functionality status – Shows if the server side OCR engine is enabled or disabled. This is enabled in the System configuration > General page.
 - Higher priority for newly added or checked in documents – Shows if the priority for newly added documents or versions is enabled. If enabled, these documents take a higher priority in the queue. If the setting is not enabled, documents are taken from the queue in the order they are added without taking priority into account.
 - Number of pending documents – The number of documents that are waiting to be processed by the OCR engine.

- Number of errors while processing – The number of documents cannot be OCR'd.
- To review the list of warnings and errors, the documents that triggered an issue are displayed below. The list of errors displays:
 - Type — If the issue is a warning or an error. Warnings are displayed for non permanent or non-technical errors such as if a document has a workflow or checked out. Documents with warnings can be re-added to the OCR queue.
 - FileHold ID of the document.
 - Date and time the OCR error occurred.
 - Details of the problem. Warnings occur if the document is checked out, the document is under an active workflow. Errors occur when the document is encrypted, password protected, or corrupted, or the document does not have any valid text that can be recognized.
 - To restrict the list to a specific date(s) when the error(s) occurred, enter a date in the To and From fields and click **Apply**.
 - To reprocess a document with a warning, select the check box next to the warning and click **Re-add document(s) to OCR Queue**. Documents are re-added to the OCR queue for processing.
 - To clear any errors from the view, select the check box next to the error and click **Clear error(s)**. The errors are removed from the list.

OCR Status
Re-add document(s) to OCR Queue
Clear error(s)

General

OCR functionality status **Enabled**
 Higher priority for newly added or checked in documents **Yes**
 Number of pending documents **0**
 Number of error while processing **16**

List of errors

From: 8/31/2016 To: 9/7/2016 Apply Clear Filter

☐	Type	FileHold Id	Date	Details
☐	Warning	360	8/31/2016 2:37:06 PM	The document has an active workflow.
☐	Error	352	8/31/2016 2:37:06 PM	Document is encrypted.
☐	Warning	330	8/31/2016 2:32:05 PM	The document has an active workflow.
☐	Warning	311	8/31/2016 2:32:04 PM	The document has an active workflow.
☐	Warning	295	8/31/2016 2:27:03 PM	The document has an active workflow.
☐	Warning	290	8/31/2016 2:27:03 PM	The document has an active workflow.

7. SEARCH ENGINE CONFIGURATION

Library administrators can configure search engine settings, view search engine status, files that cannot be indexed files, and errors.

7.1. SEARCH ENGINE STATUS

On the Full Text Search (FTS) Status page you can view the status of the search engine. It shows information such as when the last document(s) were indexed, the number of words in the index, state of the last indexing batch, total file count, and so on.

You can also run a report from the Search Engine Status page that contains:

- All dtSearch settings
- All information from the status and error pages
- Number of documents in the library
- Version of the dtSearch dll file

NOTE: When doing a major re-indexing of FileHold, this report may not function as the Microsoft SQL Server locks key index related tables. Once the re-indexing is complete, this report will run properly.

TO VIEW THE SEARCH ENGINE STATUS

1. In the Web Client, go to **Administration Panel > Full Text Search > Status**.
2. The key status indicators are:
 - **Number of Documents Waiting to be Indexed** — How many documents are in the queue waiting for full text search indexing. Documents are normally indexed for full text content every 60 seconds by a Windows scheduled task. If this value is not decreasing or at 0 documents, it may indicate that the schedule task is not running. Please contact FileHold Support if this is the case.
 - **Total Documents in the Library and Archive** — The number of documents in the library (all versions) and the library archive.
 - **Total files in the Index** — Total files that have been indexed. This number may be different than the total number of documents in your repository as some documents such as Outlook messages or zipped documents may contain more than one file. It is also possible that some of your documents will be excluded from the indexing according to how you have configured your exclusion rules and whether or not you have encrypted documents in your repository.
 - **Index Size** - The size of the index in KB, MB or GB.
 - **Word Count** — The number of words that have indexed. Note that noise words are omitted from the index.
 - **Current Indexing State** — "Idle" or "Running" if processing documents.
 - **Last Indexing Batch Result** — Provides the results from processing the last batch of documents. Normal status should state "Succeeded".

TO RUN THE FULL TEXT SEARCH STATUS REPORT

1. In the **Administration Panel > Full Text Search > Status** page, click **Create Detailed Report**.
2. Your browser will download an HTML format report with the full FTS status details.

7.2. UN-INDEXED FILES

The FileHold full-text search engine cannot index files that are encrypted, digitally secured, or damaged. Documents that belong to [offline document schema](#) types also cannot be indexed and will appear here.

You are able to see a list of files that cannot be indexed. You can either remove it from the list or replace the files with a version that can be indexed.

List of Unindexed Files ?					
Document Name	Library Location	User Name	Date	Remove from the list	Replace
asp.net 1.1 vs 2.0	Marketing (JL)\Contracts\FileHold\09 - Contracts	Jacek Lipowski	5/19/2010 11:39:15 AM	Remove	Replace
P2F Test	Marketing (JL)\Contracts\FileHold\09 - Contracts	Jacek Lipowski	5/18/2010 2:27:13 PM	Remove	Replace

For example, a PDF can be encrypted/secured so that the text inside the document is locked/encrypted and cannot be searched. Another example is a Microsoft Excel worksheet that is protected with a password or macro level security. In this case, the search engine would also be blocked from indexing the contents of the file.

You can perform the following options on un-indexed files:

- Metadata and title search will still work on all of these files if you use metadata fields to index this type of document.
- Replace is so you can replace the file that cannot be indexed with a file capable of being indexed.
- Remove simply means to remove this warning from the unindexed files report so you won't have to be notified again about that particular file.

This feature can also warn of access permissions or other technical IT issues related to full text search operations. The Domain\FileHold Service account that runs the entire FileHold server system needs to have full control of the FullTextSearch collection. The report can warn if file permissions change and do not allow the FullTextSearch collection folder structure to be accessed as well, so this report is useful on several levels.

You can disable these alerts in the [System Configuration > Full Text Settings](#) if you do not wish to receive these daily reports. You can also change who these reports are sent to, and you can read about disabling or changing the recipients of the report.

Note that any [file types that have been excluded in the web.config file](#) will not be displayed in the Unindexed Files list.

TO VIEW UN-INDEXED FILES

1. Go to **Administration Panel > System Management > Full Text Search > Unindexed Files**.
2. Click **Remove** to remove it from the list of un-indexed files. This will not remove the document from the Library.
3. Click **Replace** to replace the document with one that can be indexed.

4. Click [Browse](#) to locate the file and click [OK](#).

7.3. SEARCH ENGINE ERRORS

The Search Engine Errors report proactively warns Librarians and System Administrators about documents that are not capable of being indexed due to encryption, macro security, or digital rights management. For example, a PDF can be encrypted so that the text inside the document is locked and cannot be searched. Another example is a Microsoft Excel worksheet that is protected with a password or macro level security. In this case, the search engine would also be blocked from indexing the contents of the file. Note that metadata and title searches still work on encrypted files.

This report can also warn of access permissions or other technical IT issues related to full text search operations. The Domain\FileHold Service account that runs the entire FileHold server system needs to have full control of the FullTextSearch collection. The report can warn if file permissions change and do not allow the FullTextSearch collection folder structure to be accessed.

The Full Text Search report is emailed out nightly via a scheduled task from the FileHold Server via SMTP to your email server for delivery. See [Search Engine Configuration](#) on how to set the email address.

Not all alerts are cause for action. These alert emails can include the following types:

- Files that are not capable of being indexed for a variety of reasons including encryption, macro security, and digital rights management.
 - For example, a PDF file can be encrypted so that the text inside the document is locked and cannot be searched. Another example is a Microsoft Excel worksheet that is protected with a password or macro level security. In this case, the search engine would also be blocked from indexing the contents of the file. Note that metadata and title searches still work on encrypted files.
- When a user searches for a word or phrase that is in the majority of the document collection in terms of full text search - i.e., an overly common word - that is in the body/contents of a file, there may be a message that looks like this

```
Search Job error(s): / $E 0137 Too many words retrieved in index
E:\FileHoldData\FullTextSearch\DTSIndex a*:2: 65530; financial: 6
```

- In this case - a user was searching for "a* financial*" - which meant that virtually every document in the 250,000 document repository because the word financial was in almost every document (they are an investment company) and a* is using the wildcard - so that meant that any letter "a" near the word financial is a candidate.
- A user trying to search using a single character with a wildcard would be given the message/warning "The full text search query has invalid syntax".
- There are also errors that log that at a specific point in time, that something in the FileHoldData repository could not be accessed by the FH_Service account.
 - The DTSearch\FTS folder that contains the Full Text Search (FTS) index files cannot be accessed by the Service account that runs FileHold. Sometimes this is stored locally on the FileHold Web Server, and sometimes it is stored on a NAS or SAN. Permissions can change or there may be a network issue. You need to work with your IT department to make sure the Service account that runs FileHold has full control over this directory structure. You can quickly check what Service account name is, by going to the FileHold server and examining which account runs the FTS Update Index scheduled task, or other FileHold tasks. You can also check the SQL

Server's security logs to confirm this, or the FH App Pool's account in IIS 6 or 7's administration console.

- Missing full text search files. Antivirus and security systems, rarely, will sometimes remove index files. This happens rarely, but is the prime culprit. These files are heavily used by system and FileHold processes, and some Antivirus software can view heavy file activities as being suspicious and take action.

TO MANAGE SEARCH ENGINE ERRORS

1. In Web Client, go to **Administration Panel > System Management > Full Text Search > Errors**.
2. To hide known errors, click **Hide / Hide All**.
3. To show all errors, click **Show / Show All**.
4. To create a report of all errors, click **Create CSV**. Save the file and open in Microsoft Excel to modify the report or send to support@filehold.com for analysis.

7.4. EXCLUDING FILE TYPES FROM FULL-TEXT SEARCH

The FileHold server administrator can define if certain file types should be excluded from the full-text search. Certain file types such as zip, rar, and database files can be quite large and cause performance issues on the server and therefore, should be excluded.

The file name and metadata for these file types are still indexed and searchable; only the contents of the file are omitted from the indexing.

The web.config file to be modified can be found in *C:\Program Files\FileHold Systems\Application Server\FullTextSearch*. Modify the following section in the web.config file:

```
<add key="ExcludedFilesList" value="" />
```

The excluded list includes compound files, such as a zip archive. For example, if you exclude *.XLSX, then a XLSX file inside a zip archive is not indexed. For example, "*.ZIP;*.RAR;*.MDB;*.XLSX;" would exclude ZIP, RAR, MDB, and XLSX files from being indexed. The format of each entry includes an asterisk (*), a period (.) in front of the extension and each file type is followed by a semicolon (;). For example:

```
<add key="ExcludedFilesList" value="*.ZIP;*.RAR;*.MDB;*.XLSX;" />
```

The change to the configuration will happen immediately in the application server after the web.config file is saved. However, it will only affect new documents added to the index. If a file with an excluded type already exists in the system the index can be manually rebuilt to exclude the file. See the [System Administration Guide](#) for details on rebuilding the full text search engine.

TIP: There may be circumstances where it is desirable to exclude a single file, but index all other similar files. Since the exclusion rules apply to all files of the same type you could create an exclusion type called ".donotindex". Then, whenever you have a file that you do not want to be included in the index you can append ".donotindex" to its file name before adding it to FileHold.

7.5. LIMITING FULL TEXT INDEXING TO SPECIFIC FILE FORMATS

The full text search index can be limited to only index certain file types in the system. This will ignore all other file extensions from being indexed. This can prevent from having a potentially

very large full text search index that does not contain much search value and cause search time-outs.

A Windows server administrator can define file types whose contents will be included in the FTS index. Excluded documents will still have their metadata and properties indexed; only the contents is excluded from the index.

The settings for file exclusions are maintained in the web.config file. This file will typically be found at the following location: *C:\Program Files\FileHold Systems\Application Server\FullTextSearch*

A list of file extensions which are exclusively indexed can be listed in the following entry. In the example, "*.MSG;*.DOCX;*.PDF;" would index only MSG, DOCX and PDF documents. The format of each entry includes an asterisk (*), a period (.) in front of the extension and each file type is followed by a semicolon (;). If the value is empty then all file types (excluding items in the [ExcludedFilesList](#) entry) are indexed. For example:

```
<add key="IncludedFilesList" value=" *.MSG;*.DOCX;*.PDF;" " />
```

For compound files, such as a zip archive, all files inside a zip are assumed to be included in the index unless specified. To specify that only certain file types inside a zip are indexed, the format is "*.ZIP>*.DOC; *.ZIP>*.XLS; *.ZIP>*.PDF;". This would index only file types of *.DOC, *.XLS, and *.PDF that are inside a zip archive.

For MSG or EML files, to index the email itself and only certain types of attachments, the format is "*.MSG;*.MSG>*.MSG;*.MSG>*.DOCX;*.MSG>*.PDF;". This would index only the emails and MSG, DOCX, and PDF attachments.

8. WORKFLOW REPORTS AND DASHBOARD

You are able to view workflow reports and templates.

8.1. WORKFLOW STATUS REPORT

In the Workflow Status Report, you can search for workflows and perform certain actions such as cancel a workflow, get a copy, clear completed and cancelled workflows, override tasks and activities and delegate tasks. The report shows the tasks from all activities, including those that have not yet started (future tasks).

The possible statuses of a workflow are:

- Blank (In progress) – If the workflow is in progress, the status will be blank (empty).
- Completed – If the workflow is completed the final approval or review status is shown. (Approved, Not Approved, Approval Postponed, or Reviewed).
- Cancelled – If the workflow has been cancelled, the status of Cancelled is shown.

The number of main documents in the workflow is shown in the workflow summary line. To view all of the documents that are involved in the workflow, click the [Show Documents](#) link. The documents appear in the “Documents associated with <workflow template name>” window. The documents are listed by main or supporting document types. See Multiple Document Workflows in the [User Guide](#) for more information. From here, documents can be checked out, emailed, viewed, downloaded, or deleted.

Cancel Workflow Clear Completed Clear Cancelled Reserve/Undo Reservation Override Task Delegate Task									
Reviews & Approvals Status Report									
	Workflow Name	Documents		Initiator	Started	Due	Completed	Status	
>	☐ review, approve	2	Show Documents	Marvin Muffins	7/15/2013 10:56 AM	7/17/2013 10:56 AM	0%		View Details
>	☐ review, approve	2	Show Documents	Marvin Muffins	7/12/2013 1:46 PM	7/16/2013 11:52 AM	50%		View Details
>	☐ review, approve	2	Show Documents	Basie Pie	7/11/2013 2:16 PM	7/12/2013 3:31 PM	7/11/2013 3:40 PM	Approved	View Details
>	☐ review, approve	2	Show Documents	Basie Pie	7/10/2013 3:16 PM	7/12/2013 3:16 PM	0%		View Details
>	☐ review, approve	2	Show Documents	sysadm	7/10/2013 2:34 PM	7/11/2013 2:40 PM	7/12/2013 1:25 PM	Approved	View Details
< < 1 > > Page size: 10 Displaying page 1 of 1, items 1 to 10 of 10.									

Under each workflow name, click on the + or > symbol to view all the activities in the workflow. The activity order, type (review or approval), the participant, on behalf of (if the task was delegated), comments, attachments, start date, due date, and completion date, the percent (%) completed, and if the task status. The possible statuses of a task are:

- In Progress (Blank) – If the task is in progress, then the status is blank (empty).
- Future (Blank) – If the task is in the future, then the status is blank (empty).
- Cancelled – The workflow has been cancelled.
- Overridden – The workflow task has been ignored and no action is taken. The workflow completed or moved on to the next activity in the workflow.
- Voided – The task was reserved and completed by another participant. The task was removed and voided from all other participants.
- Reserved – The task is currently reserved by a participant.
- Blocked – The task is currently reserved by another participant thereby blocking all other participants from the task.

An asterisk (*) appears next to the participant's names' for all tasks that are available to be reserved in the Workflow Status report.

Cancel Workflow | Clear Completed | Clear Cancelled | Reserve/Undo Reservation | Override Task | Delegate Task

Reviews & Approvals Status Report  Click > to expand the workflow details

Workflow Name	Documents	Initiator	Started	Due	Completed	Status			
> review, approve	2	Show Documents	Marvin Muffins	7/15/2013 10:56 AM	7/17/2013 10:56 AM	0% View Details			
▼ ☐ review, approve	2	Show Documents	Marvin Muffins	7/12/2013 1:46 PM	7/16/2013 11:52 AM	50% View Details			
☐ 1	Review	1	sysadm*		7/12/2013 1:46 PM	7/13/2013 1:46 PM	7/15/2013 11:52 AM	Voided	
☐ 1	Review	2	Marvin Muffins*	see feedback		7/12/2013 1:46 PM	7/13/2013 1:46 PM	7/15/2013 11:52 AM	Reviewed
☐ 2	Approval	1	Basie Pie*		7/15/2013 11:52 AM	7/16/2013 11:52 AM			
☐ 2	Approval	2	Marvin Muffins*		7/15/2013 11:52 AM	7/16/2013 11:52 AM			
> ☐ review, approve	2	Show Documents	Basie Pie	7/11/2013 2:16 PM	7/12/2013 3:31 PM	7/11/2013 3:40 PM	Approved	View Details	
> ☐ review, approve	2	Show Documents	Basie Pie	7/10/2013 3:16 PM	7/12/2013 3:16 PM	0%		View Details	
> ☐ review, approve	2	Show Documents	sysadm	7/10/2013 2:34 PM	7/11/2013 2:40 PM	7/12/2013 1:25 PM	Approved	View Details	

Page size: 10 | Displaying page 1 of 1, items 1 to 10 of 10.

To view comments that a participant has left for a document, double-click on [Comments](#) link. The Comment Details window displays the comments from that participant and task.

Comment Details

Reviewer: [Marvin Mallett](#)

Completed: 17/03/2011

Comments: I recommend that this PO is approved

OK

To download a copy of the feedback document, click the [Save](#) icon  in the Attachments column. In the FDA, select the location to save the feedback document and click [Save](#). The document is downloaded to that location. In the Web Client, the feedback document is saved to the browser's default download location.

The selected workflow in the Status Report list remains selected until the list is refreshed and the selected workflow is no longer in the list.

A user with a read only role or higher can use this report.

TO RUN THE WORKFLOW STATUS REPORT

1. In the Web Client, go to [Workflow Management > Status Report](#).
2. Select from the following filter options. Alternatively, to return a list of all workflow events, leave the check boxes clear.
 - Workflow Status Equals — Select one of the following: In Progress, Completed, Cancelled, Approval Postponed, Pending Approval, Approved, or Not Approved.

- Completed Between — Enter a minimum and maximum percentage for the amount of workflow completed.
 - Date Started — Enter a minimum and maximum date for when the workflow was started.
 - Due Date — Enter a minimum and maximum due date for the workflow.
 - Document Name Contains — Enter a text string for the name of the document in the workflow.
 - Workflow Name Contains — Enter a text string for the name of the workflow.
 - Initiator is — Select a user name from the list.
3. Click **Apply Filter**. The search results are displayed below. You can now take actions upon the workflow results.

TO TAKE ACTION ON WORKFLOW STATUS REPORT RESULTS

- Once you have workflow search results, you can take the following actions on a workflow in the list by selecting the check box next the workflow:
 - **Show Documents** – Opens the documents associated with the workflow (main documents and supporting documents) in a separate window.
 - **View Details** — Displays the workflow template.
 - **Restart a Workflow** – Select the completed activity from where to restart the workflow from. Workflows can be restarted on not approved, approval postponed, or an active workflow. Workflows marked as completed and approved cannot have their workflows restarted.
 - **Rename Workflow** – To rename the workflow instance, select the workflow from the list and click **Rename Workflow**. Enter the new workflow instance name and click **OK**. Workflows can only be renamed by the initiator or senior administrator.
 - **Cancel a Workflow** — Allows you to cancel the workflow. Confirm the cancellation by clicking **OK** at the message prompt.
 - **Clear Completed** — Clears completed workflows with a status of approved, not approved, approval postponed, reviewed, or overridden (if the last task in the workflow was overridden) from the Participant Workflow Status Report. See the *End Users Guide* for more information on the Participant Workflow Status Report. When clicked the message “Completed workflows will no longer be visible on your personal workflow status report. Check the box below to include postponed workflows”. To remove any postponed workflows from the status report, select the **Clear Postponed Workflows** check box. To retain any postponed workflows, clear the check box. Users may want to keep workflows with a status of approval postponed because the workflow isn’t truly completed.
 - **Clear Cancelled** — Removes the cancelled workflows from the Participant Workflow Status Report. See the *End Users Guide* for more information on the Participant Workflow Status Report.
 - **Override Task** — Overrides a task by moving it to the completed state without affecting the rest of the workflow. Use this feature when a workflow member is absent and the workflow needs to be completed. You will need to expand the workflow by clicking > next to the workflow name to select a task to override and click **Override Task**. At the message prompt, click **OK**. A task that is marked as “Reserved” cannot be overridden. Similarly, a task that is overridden cannot be reserved or delegated.
 - **Reserve/Undo Reservation** – Allows you to “reserve” or undo the reservation for the selected task. Once a task is reserved by a participant, it prevents all other participants

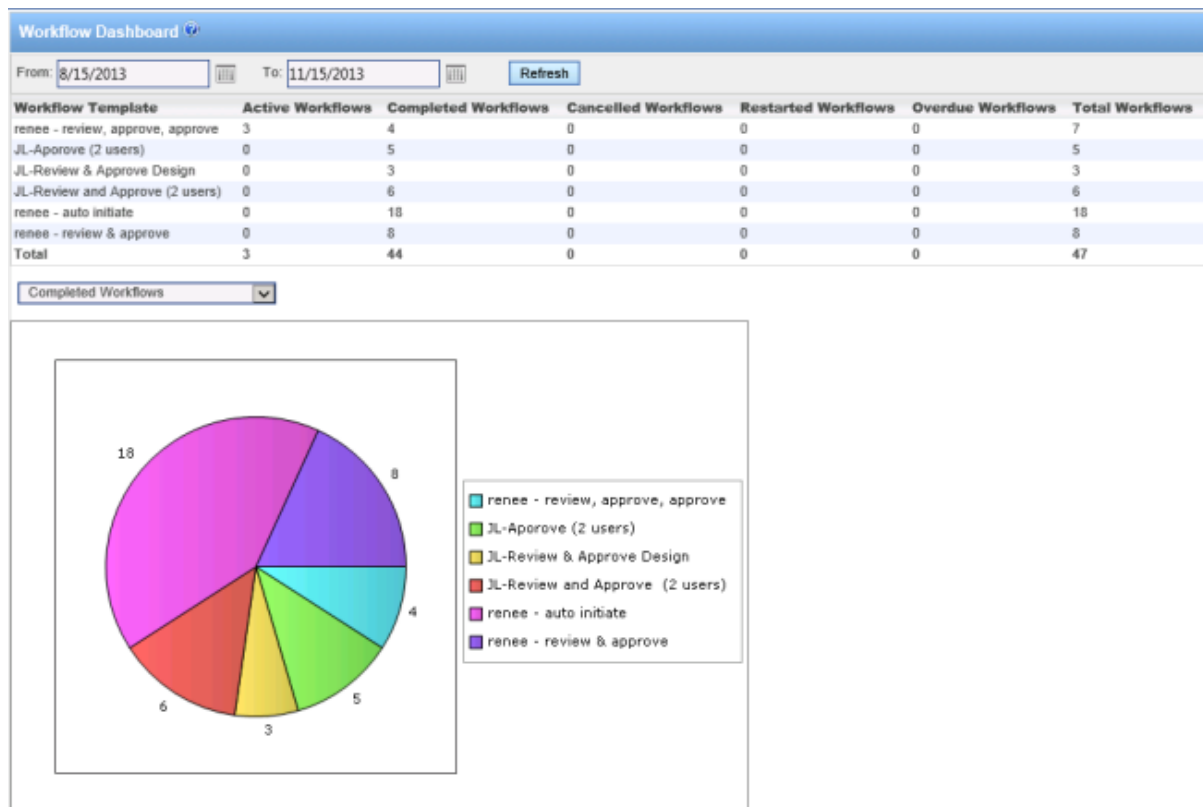
from completing the task and is removed from their task list. The status of the user who reserved the task is "Reserved". The status of the other users is "Blocked". Once the task is completed by the participant that reserved the task, the status changes to "Reviewed" or "Approved" and the status for all other participants is "Voided". If the reservation for the task is undone, then the task is available to all participants again. This function is available only if the option **Force Reservation** is enabled in the workflow template. See [Creating Workflow Templates](#) for more information. An asterisk (*) appears next to the participant's names for all tasks that are available to be reserved in the Workflow Status report.

- **Delegate Task** — Delegates a task to another user. You will need to expand the workflow by clicking > next to the workflow name to select override task to delegate and click **Delegate Task**. In the Find People window, enter a name or email address and click **Find Now**. In the Search Results, select the user and click **Select Users**. A message stating the task delegation was successful appears. Click **OK**. A task that is marked as "Reserved" cannot be delegated.
 - **Print** (FDA Only) – Prints an exact match of what is displayed on the screen.
 - **Export** (FDA Only) – When exporting the report, you can choose to export only the workflow or you can include both the workflows and the tasks. The report can be exported to CSV or HTML. Note that for the HTML report, the workflow must be expanded in the Workflow Status Report results to print the tasks. In other words, the HTML report will be exported to look exactly how it appears on the screen.
 - **Changes** link (Web Client only) — View the [workflow change log](#).
 - **View Details** link — Review the workflow template details. If you are using the FDA, click on the coloured areas to expand and contract the different areas of the workflow template.
2. To expand the workflow details, click the > or + next to the workflow name. To contract the list, click v or -.

8.2. WORKFLOW DASHBOARD

The Workflow dashboard gives a high level overview of all the active, completed, cancelled, overdue, and total workflows for all workflow templates in the system. This information is displayed in table and pie chart formats.

The workflow dashboard is only available in the Web Client. Users with read-only and above roles can view the workflow dashboard.



TO USE THE WORKFLOW DASHBOARD

1. In the Web Client, go to **Administration Panel > Workflow Management > Dashboard**.
2. To select the date range to display select or enter a date in the **From** and **To** fields. By default, data from the last 3 months is shown.
3. To determine which workflows are displayed in the pie chart, select one of the following options from the drop down list:
 - Active workflows
 - Completed workflows
 - Cancelled workflows
 - Overdue workflows
 - Total workflows
4. Click **Refresh** to update the information.

9. LIBRARY MANAGEMENT

Use the following utilities to manage the library:

- Check in documents for users
- Change document owners
- Change Cabinet or Folder owners
- Recover documents

9.1. CHECK-IN FOR USER

When users are away on vacation, have prolonged leave of absences, or are no longer within the organization, you can check in documents that they have checked out.

Library Administrators can search for users and remove the lock on the checked out file. This allows other users to then check out the file and resume the management of the document lifecycle.

The checkout is cancelled and the version number remains the same number that it was before the document was checked out.

The Find People search results allows you to check in for a user that may have been deleted, disabled, or whose permissions have been changed (invalid) in the system. When checking in for users, the following statuses will be included in the search results next to the user name, if applicable:

- (Deleted) — The user or group no longer exists in FileHold.
- (Disabled) — The user no longer has a FileHold license or has been disabled in Microsoft Active Directory.

TIP: To display a list of all users in the system in the search results, leave the First or Last Name field blank and click Find Now. This will aid you in finding any deleted, disabled, or invalid users.

TO CHECK IN A DOCUMENT FOR A USER

1. In Library Admin, go to **Administration Panel > Library Management > Undo Checkout**.
2. In the Find People area, enter the first or last name of the user and click **Find Now**. Alternatively, you can leave the name field blank to return a list of users with documents that are checked out.
3. Select the user from the results list and click **Select**.
4. In the list of checked out files by the user, select which files you want to check in and click **Check-In No Changes**.

The file is checked in without any changes made and the version number remains the same as it was before it was checked out.

5. Click **Done** when you have finished checking in files for other users.

9.2. CHANGE DOCUMENT OWNER

You can change the owner of documents in the event that an employee has left the organization or is on leave.

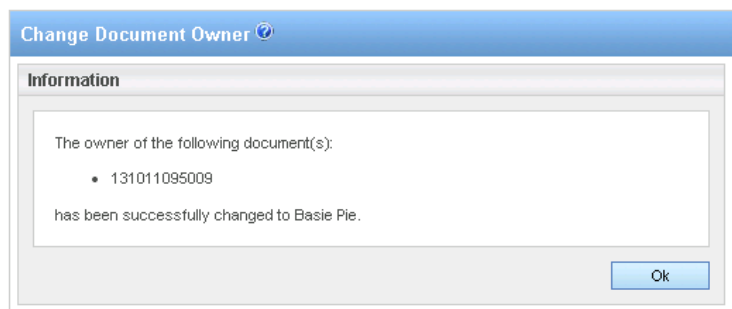
The Find People search results allows you to check in for a user that may have been deleted, disabled, or whose permissions have been changed (invalid) in the system. When changing document owners, the following statuses will be included in the search results next to the user name, if applicable:

- (Deleted) — The user or group no longer exists in FileHold.
- (Disabled) — The user no longer has a FileHold license or has been disabled in Microsoft Active Directory.

TIP: To display a list of all users in the system in the search results, leave the First or Last Name field blank and click Find Now. This will aid you in finding any deleted, disabled, or invalid users.

TO CHANGE THE OWNER OF A DOCUMENT

1. In Web Client, go to **Administration Panel > Library Management > Change Document Owner**.
2. In the Find People area, enter the first or last name of the user and click **Find Now**. Alternatively, you can leave the name field blank to return a list of users that are document owners.
3. Select the user from the results list and click **Select**.
4. Select the documents from the list of documents for which you want to change the owner.
5. Click **Change Document(s) Owner**.
6. In the Find People area, enter the first or last name of the user that you want to change ownership to and click **Find Now**.
7. Select the name in the search results and click **Select**.
8. To export the results, click **Export as CSV**.
9. Change the page size to 15, 30, or 60 documents per page using the **Page size** drop down.
10. A message will display stating that the document owner has changed. Click **OK**.



9.3. CHANGE CABINET/FOLDER OWNER

Like changing document owners, you can change cabinet and folder owners in the event that an employee has left the organization or is on an extended leave of absence.

- If you are changing ownership on hundreds or more folders, please be aware that this can require significant server resources, and we recommend that this operation be done later in the day when end-user usage of system is lower, or after hours when system usage is minimal.
- If you are planning to do Cabinet and Folder ownership changes, do one major change at a time, and wait for the first operation to be finished before starting the second job. (Example, Cabinet changes - then folder changes)

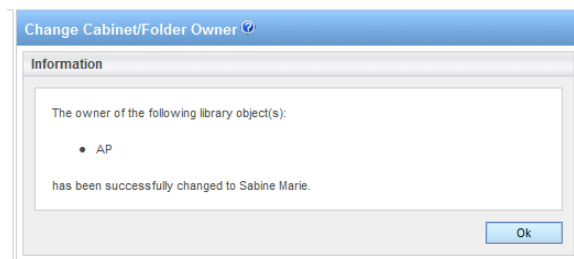
The Find People search results allows you to check in for a user that may have been deleted, disabled, or whose permissions have been changed (invalid) in the system. When changing document owners, the following statuses will be included in the search results next to the user name, if applicable:

- (Deleted) — The user or group no longer exists in FileHold.
- (Disabled) — The user no longer has a FileHold license or has been disabled in Microsoft Active Directory.

TIP: To display a list of all users in the system in the search results, leave the First or Last Name field blank and click Find Now. This will aid you in finding any deleted, disabled, or invalid users.

TO CHANGE THE OWNER OF A DOCUMENT

1. In Web Client, go to **Administration Panel > Library Management > Change Cabinet/Folder Owner**.
2. In the Find People area, enter the first or last name of the user and click **Find Now**. Alternatively, you can leave the name field blank to return a list of users that are cabinet/folder owners.
3. Select the user from the results list and click **Select**.
4. Select the cabinets/drawers/folders from the list for which you want to change the owner.
5. Click **Change Cabinet or Folder Owner**.
6. In the Find People area, enter the first or last name of the user that you want to change ownership to and click **Find Now**.
7. Select the name in the search results and click **Select**.
8. A message will display stating that the Cabinet/Folder owner has changed. Click **OK**.
9. To export the list as CSV, click **Export as CSV**.
10. Change the page size to 15, 30, or 60 documents per page using the **Page size** drop down.



9.4. RECOVER DOCUMENTS

You are able to recover documents that are in the “soft” deletion stage.

The deletion of files from the FileHold server occurs in two stages. The first stage is the “soft” deletion of files from the FileHold library. This can occur by any user with Publisher plus delete access rights or higher. Once deleted from the library, end users are no longer able to access them. The documents are temporarily stored in the “Recover Documents” area before being permanently “hard” deleted from a scheduled task by the server. For more information on hard deleting documents, see [Permanently Deleting Documents](#).

TO RECOVER DOCUMENTS THAT HAVE BEEN SOFT DELETED

1. In Web Client, go to **Administration Panel > Library Management > Recover Documents**.
2. Select the documents that you want to recover and click **Recover Documents**.
3. The documents are moved back to their original location in the Library.
4. Change the page size to 15, 30, or 60 documents per page using the **Page size** drop down.

10. ADMINISTRATION REPORTS

There are two reports available for library administrators:

- Document usage log – available for cabinet administrators or higher roles.
- Library audit log – available for senior library administrators only.

10.1. DOCUMENT USAGE LOG

The document usage log provides a permanent record of all of the interactions that users have with individual versions of a file stored in the document management system. You can quickly search the entire database to reveal all interactions that any user has had with any document and when the interaction occurred. Recorded actions include: check out, check in, downloaded, emailed, linked, moved, copied, viewed, printed, deleted, OCR'd, and many more.

Library Administrators can search and view usage of files even after the file has been deleted. This functionality is critical when complying with records management standards. Reports can be run against various actions and events, as well as keywords and other items to bring up detailed reports of users, what files they have accessed and what they did to the files.

The following information is displayed in the search results: document name, document schema, linked, FileHold ID number, action type, performed by, and the action date. If a user has been deleted from the system, the name of the deleted user appears as "John Smith (143) [deleted 2014-03-07]" in the Action Performer column. The deleted date is appended to the name automatically when a user is deleted.

This report is accessible to Cabinet administrator or higher roles. Only entries related to where the Cabinet administrator or Library administrator is an owner will be displayed in the log. This log is never deleted or overwritten.

TO VIEW THE USAGE OF A DOCUMENT

1. In the Web Client, go to **Administration Panel > Administration Reports > Document Usage Log**.
 - In the FDA, go to **Administration > Document Usage Log**.
2. In the **Search the Document Usage Log** area, enter the following criteria:
 - Document Name Contains — Select the check box and enter whole or part of the document name.
 - Type Contains — Select the check box and enter the schema name.
 - Action Type — Select the check box and select the action that was taken on the document such as checked in, checked out, downloaded, linked, and so on.
 - Action Date — Select the check box and select the date range from the date picker.
3. Click **Apply Filter**. The number of results and the report are shown below. The number of rows that are displayed in the report view can be adjusted using **Page Size** to show 15, 30, or 60 rows at a time. Click on the column to sort in ascending or descending order.
4. Click **Export to CSV** to save as a CSV file.

Document Usage Log

☐ Document name contains
☐ Document schema name
☐ Action type
☐ Performed by
☐ Action date

Application
 Add Document
 Accounting (12)*

From: 2014-10-29 To: 2014-10-29

[Apply Filter](#) [Export as CSV](#)

Search Results 1-15 of 134 Page size 15

Document name	Document schema	Linked	FileHold id	Action type	Performed by	Details	Action date
2014_10_29_11.01-word p2f	Application	0	46.1	CheckedOut	Basie Pie (9)		10/29/2014 2:47:18 PM
test email	Email	0	62.1	AddDocument	Basie Pie (9)	Location: Training and Support	10/29/2014 2:24:46 PM
test email (2)	Email	0	61.1	AddDocument	Basie Pie (9)	Location: Training and Support	10/29/2014 2:24:46 PM

10.2. LIBRARY AUDIT LOG

The Library Audit Log logs the following information:

- Deleting document versions (soft delete, hard delete, and restoring a document from the soft delete phase)
- Deleting library objects such as cabinets, drawers, folder groups and folders
- Deleting schemas
- Deleting metadata fields and removing metadata fields from schemas
- Adding, removing, and modifying cabinet and folder memberships
- Changing the owner of a cabinet, folder, or document version
- Creating, modifying, deleting, and cloning a workflow template. A *WorkflowDefinition.xml* file is available for download which contains the details for each added or modified workflow template.

Only entries related to where the Library Administrator is an owner will be displayed in the log. This log is never deleted or overwritten. The audit log can be filtered by user name, description, and to and from dates.

TO RUN THE LIBRARY AUDIT LOG

1. In the Web Client, go to **Administration Panel > Administration Reports > Library Audit Log**.
2. Use any of the following filters:
 - Username
 - Description contains – Enter a full or partial description such as "deleted folder" or "added"
 - From date to date
3. Click **Apply Filter**. The number of results and the report are shown below. The number of rows that are displayed in the report view can be adjusted to show 15, 30, or 60 rows at a time. Click on the column to sort in ascending or descending order.
4. Click **Export to CSV** to export to a CSV file.
5. To view the details of a workflow template, click **Workflow definition** to download the WorkflowDefinition.xml file. This file can be opened to see the settings of the workflow template.

11. SERVER SIDE DOCUMENT IMPORTATION

The Automatic Document Importation (ADI) mechanism allows importing a large number of documents into the document management system with minimal user intervention. It runs on the FileHold server to facilitate the mass migration of documents. Server Side Document Importation is similar to the Watched Folders functionality but can also be integrated with various custom migration tools using an API or an FTP site.

Several ADI “jobs” can be created by a Library Administrator or higher role. Each ADI “job” stores the configuration and status of the job. An administrator can configure the source type (Watched Folder, Watched FTP site, or API), a time restriction for the job to run, the user account that is adding the documents, the source folder, target location and so on.

Documents can be imported from three sources:

- If a Watched Folder is being used for the job, files from a specified directory are added to a queue. Once processed, they are imported into the destination folder in the library using the specified schema and metadata field values (direct), or using [indirect metadata](#). The files from the specified directory can be monitored and brought automatically into the system. The input files can also be deleted. See [To create an ADI job for a watched folder source](#) for more information.
- If a Watched FTP site is being used for the job, files from an FTP server can be downloaded and processed. This method is useful when for example a scanning company completes a batch of scans and wants to send them into their customer’s FileHold repository. The scans are zipped along with the metadata and stored on a FTP server. When the file is stored on the FTP server, the download is triggered from either the appearance of the file or a notification email is sent to a specific email inbox. Direct or [indirect metadata](#) methods can be used. See [To create an ADI job for a watched FTP site source](#) for more information.
- If the source is an API, documents along with their target location in the library and metadata values are added to the queue using API calls. See the [Knowledge Base for more information on API](#).

Once an import job is configured, the user specified in the job is the owner of the documents once the files are processed. This user must have a Document Publisher role or higher and must have access to the schema and destination folder.

For each job, the status which includes the number of processed documents, pending documents, and errors are shown. Within each job, the detailed list of documents, status (pending, completed, error), the date they were added to the queue, date they were processed, the source path and target folder are shown. These import details can be exported into a CSV file. Once a document has been successfully imported, the summary information and the document with associated metadata can be viewed. Summary information can be viewed for any pending documents or documents with errors.

The time at which documents are processed can be set on the job and for a scheduled task. In the job, you can specify when the specified directory is scanned for documents and puts them into the queue. However, when the documents are processed and imported into library is controlled by the scheduled task “FH automatic document importation”. For example, you can be adding documents to the queue all day (no time restriction in the job settings) but the actual process of importing the documents occurs only at night (via the scheduled task settings) so the FileHold server is not additionally burdened during the day. The default setting for the scheduled task “FH automatic document importation” is to run every 10 minutes indefinitely.

[Extraction rules](#) can be applied to documents that are imported. The extraction rule is used when the import job is set to use the same schema as the rule. The metadata values that are extracted through the extraction rule take precedence over the metadata values set in the

import job. If there is no value mapped in the rule, then the value set in the job is used. Note that if the metadata field is a drop down list, ensure that the value being extracted from the document exists in the list. If the value does not exist then the value set in the job is used.

Metadata field values can be extracted from a CSV file instead of using the static values when using a watched folder or watched ftp site type import job. This is called "indirect metadata". A text delimited file, such as a CSV, that contains the schema, full path and document name, and metadata fields and values, is used to define the values that populate the metadata fields. An auto-filing script can also be used if using indirect metadata. See [Using Indirect Metadata in an Import Job](#) for more information.

Server Side Document Importation is an optional feature that is controlled in the FileHold license. To purchase this feature, contact sales@filehold.com.

TO CREATE AN ADI JOB FOR A WATCHED FOLDER SOURCE

1. In the Web Client, go to **Administration Panel > System management > Import Jobs**.
2. In the List of Import Jobs, click **Add Job**.
3. Enter the Name of the job.
4. Enter a Description for the job.
5. Select the Source Type **Watched Folder**. Documents are imported from a specified folder path. This folder can be on the server or in a network location and the folder **must have the FH Service account as a member and have full control permissions**.
6. In the Job Settings area, select the **Job is enabled** check box to enable the job.
7. The Restrict operation time fields determine when the documents will be brought into the queue from the Watched Folder. Select the **Restrict operation for** check box and enter the start and end time that the job will run. If no time is entered, the job runs as a continuous process and documents are added to the queue as soon as they are added to the source (Watched Folder).
8. In the Max Documents Per Trigger field, enter the maximum number of documents that will be processed per import instance. For example, there can be 100 documents in the source folder but the maximum documents per trigger setting is set to 50 so only 50 documents will be processed when the scheduled task runs. The next 50 documents will be processed when the scheduled task runs again.
9. In the User Context field, select the **user name** from the list that will own the imported documents. This must be a user with a role of Document Publisher or higher.
10. In the Post Import Actions field, select an option from the list:
 - None — No changes are made to the document
 - Force document format to electronic record — The document format is converted into an electronic record.
11. Enter the **Source Folder Path**. This is the folder that is being "watched" for new documents and are brought into the queue.
 - You must use a UNC path for remote folder share locations, making sure that this remote folder has FH_Service account with full control, and that the remote folder is properly shared as well.
 - If using indirect metadata, ensure that the CSV file and documents being imported are in the same directory.

12. Select the **Delete Input Files** check box to delete the files from the source folder once they are imported into the library.
13. Select the **Automatically add new files to the queue** check box to run this job without user intervention; documents are automatically added to the queue when the scheduled task is executed. If this check box is not enabled, then the job is run [manually](#).
14. Select the **Use indirect metadata** check box if you are using a CSV file that contains the metadata field values for the documents. See [Indirect Metadata](#) for more information. Fill out the following information:
 - File extension - Enter **csv**, **tab**, **txt**, etc.
 - Field delimiter - Enter the field separator.
 - Value delimiter - Enter the value separator. Enter a character even if you are not using multiple values. Note that the field delimiter and the value delimiter cannot be the same.
 - Use auto-filing script – Select the check box to enable the use of an auto-filing script. To use the auto-filing script configured in the schema, select **Document schema default**. To use an alternate auto-filing script, select an option from the list. See [Auto-filing Settings](#) for more information.
15. Click **Select** to set the **Destination Folder** from the library tree. Note that if auto-filing is being used, a destination folder is not required and can be left blank.
16. Select the **Document Schema** from the list.
 - This is optional if you are using the [indirect metadata](#) option.
17. Enter the values in the metadata fields. All fields marked with an asterisk (*) are required.
18. Click **OK** to save the job. The job is added to the List of Import Jobs.

TO CREATE AN ADI JOB FOR A WATCHED FTP SITE SOURCE

When using a Watched FTP site as the source, documents and /or metadata are downloaded and imported from an FTP server. Downloads are triggered by the presence of a file or via an email.

1. Complete [steps 1-10](#) as above except select **Watched FTP site** as the Source Type.
2. In the FTP Site Settings area, in the Host field, enter the machine name or server IP address of the Source folder. Click **Test Connection** to verify the Host is accessible.
3. Enter the Port number. Uses standard port 21 by default.
4. Select the **Encrypted Connection** check box if encryption is used in the FTP connection.
5. In the Authentication area, select **Anonymous** if the logon type is anonymous. Leave unchecked if using a normal connection type.
6. If not using an anonymous connection type, enter a **User** name and **Password** for the FTP account.
7. In the FTP Folder Settings area, enter the **FTP source folder path**. Provide the full path to the Source folder in this field (for example: /FileHold/Data/Source). Make sure the path begins at the base directory to which the FTP server allows connection. The path must start with a forward slash (/).
8. In the Source Filter field, enter the acceptable file types to be transferred. This will filter out any files that do not match the specified source. To accept all file types, enter *.*. This field is unavailable if the option "Get filenames from the email body using a regular expression to search for filename details and form a complete filename with replace" is enabled.

9. In the Local Destination Folder Path field, specify the folder location when the files will be downloaded to on the local computer.
10. In the Post Download Operation area, select any of the following options:
 - Extract archived files — Extracts the downloaded files after they are downloaded. Enter the list of valid archive file extensions in the field.
 - Delete archive files after contents are extracted — Select the check box to delete the zipped files after the contents have been extracted.
 - Rename source files — Renames the source files on the FTP site with a new extension. Enter the new file extension in the New File Extension field. Cannot be used with the Delete source files option.
 - Delete source files — Deletes the source files from the FTP source folder. Cannot be used with the Rename source files option.
11. In the Watched Folder Trigger, select one of the following options:
 - File appears — Once a file appears in the FTP source folder path, the source files are downloaded to the local destination folder.
 - Email message received — Source files are downloaded when a notification email is received in a configurable email box. Use the following table to fill out the information:

Field	Description
POP3 Server	Enter the address for the POP3 server and click Test Connection to verify.
Port	Enter the port number. Uses standard port 110 by default.
Encrypted connection	Select the check box if the connection is encrypted.
Authentication	Select Anonymous or enter a User name and Password.
Get filenames for the email body using a regular expression to search for filename details and form a complete filename with replace	Select the option to use a regular expression in the Search and Replace options below.
Search	Provide a regular expression that finds each filename in the body of the email.
Replace	Include a regular expression to form a filename using characters found in the search above.

12. Continue to fill out the Local File Processing Settings from [step 12](#) to 17 above.
13. Click **OK** to save the job.

TO MANUALLY RUN A JOB ON A WATCHED FOLDER

If the “Automatically add new files to the queue” option is not enabled for the job, the job must be run manually for a watched folder.

1. In the Web Client, go to **Administration Panel > System management > Import Jobs**.

2. In the List of Import Jobs, click the name of the job to run.
3. In the Summary of job page, click **Watch Now**. Any files in the source folder are added to the queue for processing.

TO EDIT A JOB

1. In the Web Client, go to **Administration Panel > System management > Import Jobs**.
2. In the List of Import Jobs, click the name of the job to edit.
3. In the Summary of job page, click **Edit Job**.
4. Make the job changes and click **OK**.

TO DELETE A JOB

1. In the Web Client, go to **Administration Panel > System management > Import Jobs**.
2. In the List of Import Jobs, click the name of the job to delete.
3. In the Summary of job page, click **Delete Job**.
4. At the message prompt, click **OK**.

TO RESET A JOB

Resetting a job removes all pending and failed documents from the queue and job details and the import folder will be rescanned.

1. In the Web Client, go to **Administration Panel > System management > Import Jobs**.
2. Select the job from the list.
3. In the Summary of the job page, review if there are any errors. If present, click **Reset Job**.
4. The message “Are you sure you want to reset this import job? All pending and failed documents will be removed and the import folder will be rescanned.” is displayed. Click **OK** to reset the job.

TO VIEW JOB DETAILS

1. In the Web Client, go to **Administration Panel > System management > Import Jobs**.
2. In the List of Import Jobs, click the name of the job to edit.
3. In the Summary of job page, click **View Details**. In the Details of Job page, a list of the files that were processed are shown:
 - The document name, schema type, source location, destination folder, date the file was added to the queue, and the date the import was completed is displayed for each document.
 - The status of pending, completed, or error is displayed. In the case of an error, this indicated the import failed for that document and will need to be re-added to the queue.
 - Click **Export as CSV** to download the job details as a CSV file.
 - To view the details of a specific document, click the **document name**. In the Details of <file name> Document screen, the metadata fields and summary for the document are shown. In the case of an error, the Error Log message is displayed. Where the status of a document is “completed”, click **Go to Document** to view the document in the library. To reprocess the document and add back to the queue, click **Re-process Document**. Ensure

that the issue that caused the error has been corrected prior to attempting to reprocess the document. Click [Previous](#) or [Next](#) to move to the previous or next document in the details list. Click [Return to Job Details](#) to return to the previous screen.

- To clear the details of the successfully completed documents, click [Clear Completed](#).
 - To clear the details of unsuccessfully imported documents, click [Clear Errors](#).
 - To reprocess all the documents that generated errors, click [Re-process Errors](#). In the Reprocess Errors of <job name>, select the documents to be reprocessed. Ensure that the issue that caused the error has been corrected prior to attempting to reprocess the document. The documents are added back into the queue and reprocessed. If the documents were able to be processed, they will have a status of "completed" in the job details. If the documents were not able to be processed, they will have a status of "error" in the job details.
4. In the Details of Job page, click [Return to Summary](#) to return to the Job Summary page.
 5. In the Job Summary page, click [Return to List](#) to return to the List of Import Jobs.

TO ENABLE OR DISABLE A JOB

1. In the Web Client, go to [Administration Panel > System management > Import Jobs](#).
2. In the List of Import Jobs, click [Enable](#) or [Disable](#) next to the job name.

11.1. USING INDIRECT METADATA IN AN IMPORT JOB

For a Watched Folder type import job type, a text delimited file, such as a CSV, that contains the schema, full path and document name, and metadata fields and values, can be used to define the values that populate the metadata fields. This allows you to import documents that have metadata values that vary from document to document. Without indirect metadata, the values in the import job are static or [extraction rules](#) can be used.

The option "Use Indirect Metadata" is available in the import job. When selected, the file extension (typically csv), field delimiter (typically a comma or semicolon) and the value delimiter (typically a comma or semicolon) which is used for multiple selection type metadata fields. Note that the field delimiter and the value delimiter cannot be the same. Field and value delimiters can be any Unicode character. For metadata field names and drop down list values, they must match the configuration in FileHold exactly (for example, no spelling errors). If they do not match exactly, then the metadata field value will be left blank after importation.

Offline documents can be added with ADI using an API-based import or the indirect metadata method. For the indirect metadata method, the schema listed in the text delimited file must be an offline document schema.

An auto-filing script can also be used when the indirect metadata option is enabled. The auto-filing script configured in the schema or an alternate script can be used.

A sample CSV file is shown below in Microsoft Excel®. Do not change the position of the column headers or the import will not work. For offline documents, use only the filename and not the path in the ImportFilename column. In this example, the column headers are:

- ImportType - This is always set to Document.
- ImportFilename - The full path and name of the document to import. In the case of offline documents, use the document name only (not the path). **Important:** The FH_Service account must have full control to this directory.
- DocumentSchema - The name of the document schema being used

- First Name - The metadata field name in the schema.
- Last Name - The metadata field name in the schema. Use as many metadata fields as needed in additional columns.

	A	B	C	D	E
1	ImportType	ImportFilename	DocumentSchema	First Name	Last Name
2	Document	C:\Users\Administrator\Documents\IndirectMD\application1.docx	Application	Jim	Halpert
3	Document	C:\Users\Administrator\Documents\IndirectMD\application2.docx	Application	Pam	Beesly
4	Document	C:\Users\Administrator\Documents\IndirectMD\application3.docx	Application	Dwight	Shrute
5	Document	C:\Users\Administrator\Documents\IndirectMD\application4.docx	Application	Angela	Martin
6	Document	C:\Users\Administrator\Documents\IndirectMD\application5.docx	Application	Andy	Bernard
7	Document	C:\Users\Administrator\Documents\IndirectMD\application6.docx	Application	Kelly	Kapoor
8	Document	C:\Users\Administrator\Documents\IndirectMD\application7.docx	Application	Meredith	Palmer

The CSV file and documents must be in the same directory location when being imported and the FH_Service account must have full control.

There are three example files that can be downloaded in a zip file and used to create your own CSV files for indirect metadata imports [from here](#).

1. Indirect metadata, no value delimiters (no multi-select values).
2. Indirect metadata with value delimiters (multi-select values). Multiple values are separated by a semi-colon (;).
3. Offline documents.

NOTE: Arbitrary Unicode characters can be used as delimiters by prefixing a decimal Unicode value with a backslash. The most common delimiter characters will come from the ASCII Punctuation symbols. A tab character can be expressed as \9, a space as \32, and the \ (backslash) character as \92. A complete list of values is available [Unicode Consortium website](#).

12. MANAGE IMPORTS TOOL

The Manage Import Tool is provided as an interface between scanning software and FileHold. It is also known as the FileScan Bridge. In addition to providing an interface to scanning software it can also be used to import documents from Outlook watched folders, exported from FileHold, import documents from legacy document management systems, or just about any source that can describe what to import as XML.

Manage imports works using import profiles that can be defined by library administrators. An import profile contains the import name, description, location of the import files, job automation settings, map the metadata fields as needed, optionally perform database lookups for metadata field values, and set the filing location directly or indirectly.

All users with a document publisher role or higher can operate Manage Imports when import profiles have been created. Library administrators can define import profiles for a variety of purposes.

Use the Manage Imports Tool to import documents into the document management system from:

- [Documents from scanning application](#) - Use the Manage Imports tool to bring scanned documents via an XML import file into FileHold in the FileHold Desktop Application (FDA). Once files have been scanned they can be imported automatically into the document management system along with any Zonal OCR'd text.
- [Documents that were exported from a FileHold system in a compatible XML format](#) - Use the Manage Imports tool to import documents into the document management system that were exported using the Export function or using the FileHold Instrumentation Tool. This is useful when exporting and importing documents between a demo and production systems.
- Using Manage Imports to transfer files from another system - Manage Imports can be used when transferring data from other systems. These can be document management systems based on shared folders, third party applications, or just about anywhere. The key to importing data will be to stage it appropriately. Manage Imports works based on a description of what to do in an XML file and it copies documents into the repository from the file system. The following links on the FileHold website will provide information on how to create the descriptive XML file or setup auto-filing needed for Manage Imports.
 - [Creating the XML File Structure for Imports using Metadata Fields and Library Structure](#)
 - [Creating the XML File Structure for Document Imports using Only Metadata Field Values](#)
 - [Importing Microsoft Office Documents into FileHold with Metadata](#)
 - [Using Excel to Create an Import Script](#)
 - [Migrating a Folder Based Document Repository to FileHold](#)
 - [Auto-Filing in the Document Management System](#)

You can have as many import profiles as needed and use any combination of the imports above. However, if you have several import profiles that have the option "Watch for new files..." enabled, this could impact performance of the FDA. Care should be taken to ensure that the number of imports and the volume of documents is suitable for the performance of the workstation and network where the FDA is installed.

12.1. IMPORTING DOCUMENTS FROM A SCANNING APPLICATION

In the Managed Import profile, you set the import name, description, the import XML file, job automation settings, map the metadata fields (if applicable), perform database lookups for metadata fields, and set the filing location.

In the List of Document Imports view, the import name, description, import type (shared import or personal), the number of batches completed, the number of documents imported, the status (running, not running, or watching (Watch for new files... check box is enabled in profile)), destination, and what happens to the import files after they are imported (deleted or moved).

List of Document Imports							
Add Start Reset Show Log File Clear Log File							
Import Name	Description	Import Type	Batches Completed	Documents Imported	Status	Destination	After Import
import from prev build		Shared	0 of 0	0 of 0	Not running	Library	
scanning invoices	invoices	Personal	1 of 1	26 of 26	Watching	Library	Delete Source

TO IMPORT FILES FROM SCANNED DOCUMENTS (SUCH AS DOCUMENTS FROM QUICKSCAN PRO)

1. In FDA, go to **Tools > Manage Imports** and click **Add**.
2. In the General tab, enter an **Import Name** and **Description**.
3. In the Select folder containing Import File field, click **Browse** to locate the XML file that was created during the Zonal OCR scanning process.
4. Click **Retrieve XML Fields**. You should receive a message saying that XML fields were successfully retrieved.
5. To share the import with other users on the local machine, select **the Share this import with other users** check box. This will allow any imported documents to appear in the other user's Inbox as well as your Inbox for filing.
6. In the Job Automation Settings area, select the following check boxes if applicable:
 - Watch for new files to be imported and automatically tag and bring them into the Inbox - When enabled, the documents scanned into the import folder will be automatically tagged with metadata values and brought into the Inbox. If disabled, then the import has to be run manually using the Start button.
 - Delete input files after they have been successfully added to the FileHold Library - The folder where the documents were imported from will be deleted automatically. This keeps the import folder clean and reduces storage space needed.
 - Move input files to the selected folder - After files have been imported into FileHold, they can be moved from the file location from which they were imported from to another location on the local computer or network. If a file with the same name exists in the destination folder, a unique number will be appended to the file name. NOTE: This option cannot be used in conjunction with the "Delete input files after they have been successfully added to the FileHold Library" check box.
7. In the Field Mapping tab, select the schema to map the imported XML fields to from the **Select Destination Document Schema** drop-down list.
8. Once a schema is selected, map the corresponding Zonal OCR index fields to the metadata fields in the schema.
9. In the Database Lookup tab, select one of the following options:

- Perform server side lookup of metadata – Select this check box to perform a database lookup from the server instead of the client machine. This option is only available if the schema selected in the Field Mapping tab is a schema that is configured to use [database lookup](#). When importing, the values retrieved from the lookup will override any of the mapped field values from the XML file.
- Perform lookup of metadata from a database – Allows you to configure the database you want to use for the lookups on the client side. This option is not available if the “Perform server side lookup” option is selected. Fill out the following information:

Field	Description
Select XML Field to use for Lookup	From the drop down list, select the XML field to use as the database lookup.
Server Name	Enter the server name. Click Refresh to get a list of all servers.
Use Integrated Authentication	Select the check box if applicable.
Database Username	Enter the username that has access to the database.
Database Password	Enter the password that matches the username and click Verify Connection .
Database name	Select the database name from the list.
Select Lookup Table	Select the table or view to use for the lookup.
Database Lookup Field	Select the column in the table or view to use for retrieval for the XML field lookup value. Click Retrieve DB Fields .

10. In the Autofiling tab, you can select the location for the imported documents. Select from the following options:
 - Auto-filing off - Documents will be sent to the Inbox for processing.
 - Automatically send files to a single folder in FileHold - You can set the destination folder for all the documents in the import to a single folder location. Click Browse to select the folder in the Library.
 - Automatically detect / create destination folder for files based on Auto-filing rules - You can select an auto-filing script to create the folder location in which the documents will be sent. See Automatically Filing Documents into the System (Auto-Filing).
11. In the Job Automation Settings area, select the [Automatically "Send Files" to the FileHold Library with an Inbox Status of "Ready to Send"](#) to completely bypass the Inbox and go directly to the folder location set above. This way you do not have to go to the Inbox and click Send or Send All; the documents will be sent automatically to the set folder location.
12. Click [OK](#) to save the Import settings.
13. To delete an import, click the red [X](#) next to the import name in the List of Document Imports.

NOTE: Users can also edit, start an existing import wizard or show the log files from the List of Documents Imports.

12.2. IMPORTING DOCUMENTS PREVIOUSLY EXPORTED FROM FILEHOLD

The Manage Imports tool can be used to import documents into the document management system that were exported using the [Export](#) function or using the [Instrumentation Tool](#). This is useful when exporting and importing documents between a demo and production systems.

A checkbox labeled "Use the dynamic import format" on the Mapping tab allows for importing compatible XML files and documents back into the document management system along with their metadata and library location when enabled. During the import, the document schema is automatically selected for each document based on the XML file and all metadata fields are automatically mapped based on their name. Prior to importing the documents, the schemas and metadata fields need to exist in the system that you are importing into in order to capture the correct schemas and metadata fields. If the "Import files which were formerly exported from a FileHold System" is enabled for the document import, it is not possible to select a fixed destination or an auto-filing script. Instead the destination location will be determined for each document based on the library path field in the XML file. All cabinets, drawers and folders must exist in the library before importing the documents; the Manage Imports tool will not create the library structure.

TIP: Use the [Instrumentation Tools > Library Setup](#) to export and import out your library structure and schemas/metadata fields between systems.

You can enable the 'auto-send' feature for document imports using the FileHold compatible format so all documents are automatically sent to the library without using the Inbox; however, you can still send the documents to the Inbox in order to review the metadata.

IMPORTANT: When importing in documents that were exported from FileHold, only the actual files, and their metadata and library location will be preserved for the imports and exports in the XML file. Document information such as the owner, creation date, and version history will not be preserved during the export and import process.

TO IMPORT FILES PREVIOUSLY EXPORTED FROM A FILEHOLD SYSTEM

1. In FDA, go to [Tools > Manage Imports](#) and click [Add](#).
2. In the General tab, enter an [Import Name](#) and [Description](#).
3. In the Select folder containing Import File field, click [Browse](#) to locate the XML file that was created during the export process.
4. Click [Retrieve XML Fields](#). You should receive a message saying that XML fields were successfully retrieved.
5. To share the import with other users on the local machine, select the [Share this import with other users](#) check box. This will allow any imported documents to appear in the other user's Inbox as well as your Inbox for filing.
6. In the Job Automation Settings area, select the following check boxes if applicable:
 - Watch for new files to be imported and automatically tag and bring them into the Inbox - When enabled, the documents scanned into the import folder will be automatically tagged with metadata values and brought into the Inbox. If disabled, then the import has to be run manually using the Start button.
 - Delete input files after they have been successfully added to the FileHold Library - The folder where the documents were imported from will be deleted automatically. This keeps the import folder clean and reduces storage space needed.
 - Move input files to the selected folder - After files have been imported into FileHold, they can be moved from the file location from which they were imported from to another location on the local computer or network. If a file with the same name exists in the destination

folder, a unique number will be appended to the file name. NOTE: This option cannot be used in conjunction with the "Delete input files after they have been successfully added to the FileHold Library" check box.

7. In the Field Mapping tab, select the **Use the dynamic import format** check box. The rest of the tab is disabled since it will take the mapping information from the XML file.
8. The Database Lookup tab is disabled.
9. In the Autofiling tab, the Auto-Filing settings are disabled. The documents will get their file path from the XML file.
10. In the Job Automation Settings area, select the **Automatically "Send Files" to the FileHold Library with an Inbox Status of "Ready to Send"** to completely bypass the Inbox and go directly to the folder location set above. This way you do not have to go to the Inbox and click Send or Send All; the documents will be sent automatically to the set folder location.
11. Click **OK** to save the Import settings.

12.3. OPERATING MANAGED IMPORTS

Manage imports profiles can operate automatically in the background or they can be run manually. In both cases there are some basic rules and functions that can help to manage its operation. The screen below is the manage imports operation screen. You can get to this screen from the Tools > Manage Imports menu option in the FDA.

List of Document Imports							
Add Start Reset Statistics Show Log File Clear Log File							
Import Name	Description	ImportType	Batches Completed	Documents Imported	Status	Destination	After Import
Forms Publisher	Integration with forms publishing system	Personal	9 of 143	34 of 291	Watching	Inbox	
Invoice1	Scanned invoices from Abbyy	Personal	0 of 0	0 of 0	Not running	Inbox	
Invoice2	Scanned invoices from QSP	Personal	1234 of 1234	1234 of 1234	Not running	Inbox	Delete Source
Legacy	Legacy DMS migration	Personal	972 of 972	4120 of 4120	Watching	Library	Move Source
QA1	Paint line quality assurance station	Personal	3422 of 3475	9120 of 10027	Watching	Inbox	
QA2	Other quality assurance	Personal	0 of 0	0 of 0	Watching	Inbox	
Receipts	Good receipts documents	Personal	401 of 401	401 of 401	Not running	Inbox	Move Source
Status Reports	Outlook watched folder for status reports	Personal	3 of 7	3 of 7	Watching	Inbox	

The following table describes the actions available:

Operation	Description
Add	Add a new import profile. Import profiles are stored on the workstation where they are created. You must have library administrator rights to add a profile.
Start	Start processing any new documents associated with the selected import profile. This function is not necessary for any import profiles that have been setup to automatically watch a folder.

Operation	Description
Reset Statistics	Reset the Batches Completed and Documents Imported counters. If there has been an error in completing the batch or if there has been an accidental removal of documents in the batch, you can select the Reset the file tracking check box to clear the import log and reset the counter to zero. Once the counter is set to zero, the same batch can be imported again. IMPORTANT: By clearing the import log, the internal file duplication tracking information is also cleared. Therefore, documents that were already imported into the library prior to the batch failure may be imported again if they were not set to be deleted or moved in manage import settings.
Show Log File	Open the import log file in notepad. The import log is stored on the workstation.
Clear Log File	This will erase the contents of the import log file.
Delete	Click the red X to permanently remove an import profile from the workstation.
Change	Click the import profile name to edit the import profile. You must have library administrator rights to change a profile.

The manage imports screen contains a number of columns with important information about the functioning of each import profile which is described in the following table:

Column	Purpose	
Import Name	The name of the import profile. For library administrators this name will appear as a link.	
Description	If the creator of the import profile set a description it will be displayed here.	
Import Type	Imports can be personal or shared. A shared profile is available to all Windows users that log on to the workstation. Personal profiles can only be seen by the for the Windows user where the profile was created.	
Batches Completed	Each XML file seen by manage imports is a batch. These batches are processed by adding each document specified in each batch to the inbox or transfer queue. When all the documents from the batch have been placed in one of those two locations the batch will be complete. This does not mean the documents have been transferred to the FileHold library.	
Documents Imported	When all documents specified in a batch are available all the documents in the batch can be imported and will show in this total.	
Status	Value	Description
	Not Running	This import profile is completely idle. It can be started by selecting the profile then pressing the Start button.
	Running	Batches are being processed.
	Watching	When the FDA is logged on, manage imports is automatically checking for new batches every 15 seconds.
Destination	Value	Description
	Inbox	Documents from imported batches will be added to the Inbox for further processing.
	Library	Document will immediately be added to the transfer queue . If there is an error during the transfer the documents will be sent to the Inbox.
After Import	Value	Description
	Delete Source	When the document has successfully transferred to the library it will be deleted. Batch XML files will be deleted immediately when the batch has been completed regardless of whether or not the documents from the batch have been transferred. Deleted files will be placed in the Windows Recycle Bin if that option is checked in User Preferences .
	Move Source	When the document has successfully transferred to the library it will be moved to the configuration location. Batch XML files will be moved immediately when the batch has been completed regardless of whether or not the documents from the batch have been transferred.

TO START OR MANUALLY RUN THE IMPORT

1. In FDA, go to **Tools > Manage Imports** and select the import name from the list.
2. Click **Start**. The documents are imported according to the configuration in the import.
 - The import runs and automatically imports documents if the **Watch for new files...** setting is enabled.

- If the **Watch for new files...** setting is not enabled, the import will have to be run manually. In other words, you will have to click **Start** to run the import.
- 3. To reset the number of documents imported counter, click **Reset Statistics**. Use this setting if there has been an error in completing the batch or if there has been an accidental removal of documents in the batch, you can select the Reset the file tracking check box to clear the import log and reset the counter to zero. Once the counter is set to zero, the same batch can be imported again. IMPORTANT: By clearing the import log, the internal file duplication tracking information is also cleared. Therefore, documents that were already imported into the library prior to the batch failure may be imported again if they were not set to be deleted or moved in manage import settings. The counter in the Documents Imported column is reset to 0.

TO VIEW THE LOG FILE FROM THE IMPORTS

1. In FDA, go to **Tools > Manage Imports** and click **Show Log File**. The log file opens in Notepad.
2. To clear the log file, click **Clear Log File**.

13. EXTRACTION RULES

An Extraction Rules tool has been created in order to manage the extraction of metadata from Microsoft Office Outlook msg files, file properties of any file type, PDF forms, and Microsoft Office Word forms. This allows the information contained within the emails, file properties or forms to automatically populate the metadata fields within a document schema.

Extraction rules can be used in conjunction with the [Import Jobs](#) (Automatic Document Importation). The extraction rules are automatically applied when an import job is processing documents on the server. Any metadata values extracted take precedence over the metadata values defined in the import job.

Extraction rules are only accessible in FDA by Library Administrators or higher permissions.

TO ACCESS THE EXTRACTION RULES

1. Do one of the following:

- In the FDA, log in as a library administration and go to **Tools > Extraction Rules**.
- In the Web Client, go to **Administration Panel > Library configuration > Extraction Rules**.

There are four types of extraction rules that can be created:

- [Email Headers](#) - Values contained in the headers of Microsoft Outlook msg files.
- [File Properties](#) - File properties of any file type.
- [XML Nodes](#) - Values entered into a Microsoft Word content controls
- [PDF Forms](#) – Values in a PDF form can be extracted into the metadata fields of the schema.

When the extraction rules are properly configured, the values from emails, file properties or xml nodes can be automatically extracted into the metadata fields of a schema.

13.1. EMAIL HEADER EXTRACTION RULE

Automating the capture of email metadata allows users to easily store, search, and archive important emails. The document management system can automatically capture metadata from emails that are added to FileHold from Microsoft Outlook. The fields captured are To, CC, Date, From, Subject, and any attachment.

In order to extract email metadata, you must enable this feature. You will also need to create an email extraction schema and the metadata fields to map the fields CC, Date, From, Subject, and To. For example, you can name the fields “Email CC”, “Email Date”, “Email From”, “Email Subject”, and “Email To”.

After the feature is enabled and the schema is created, the values for the mapped fields are automatically populated as the emails are moved into Library and associated with email extraction schema. Emails are stored in the Microsoft Outlook .MSG format using the FileHold Desktop Application (FDA) and Microsoft Outlook. It will not remove the Email from Outlook unless you specific this setting in the FileHold Desktop Application (FDA) User Settings and Preferences.

Extraction rules can be used in conjunction with the [Import Jobs](#) (Automatic Document Importation). The extraction rules are automatically applied when an import job is processing documents on the server.

NOTE: Email extraction rules do not work when adding documents through the Web Client.

TO CREATE THE EMAIL SCHEMA AND METADATA

1. Create a new schema called Email or something similar. For more information on creating schemas, see [Creating Document Schemas](#) for more information.
2. Create text fields with 140 character maximum length for:
 - From:
 - To:
 - CC:
 - Subject:
 - Attachments
3. Create a date field for:
 - Date Sent:
4. Save the Email schema.

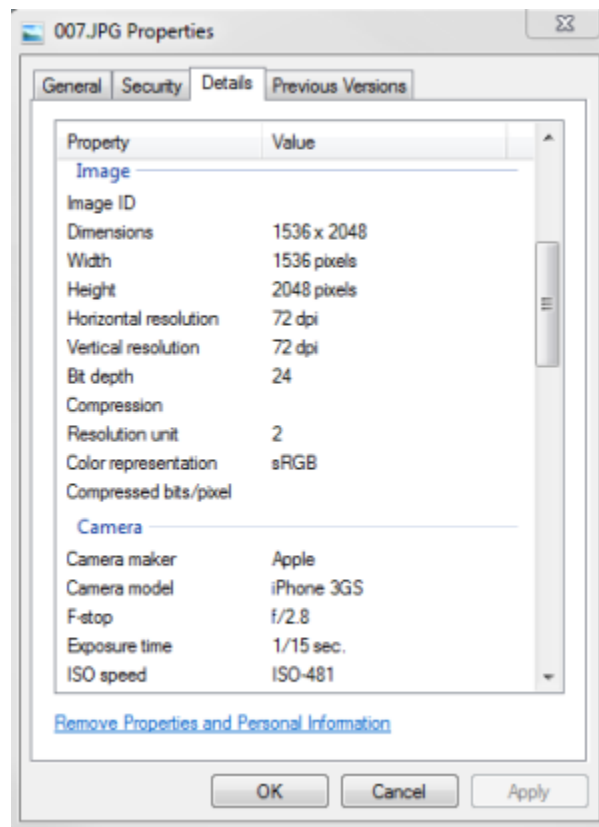
TO ENABLE THE EXTRACTION OF METADATA FROM EMAIL

1. Do one of the following:
 - In FileHold Desktop Application, go to **Tools > Extraction Rules**.
 - In the Web Client, go to **Administration Panel > Library configuration > Extraction Rules**.
2. In the List of Extraction Rules window, click **Add Email Headers Rule**.
3. In the Email Headers Rule window, enter a name for the rule such as "Email extraction rule".
4. Enter a description (optional).
5. To enable the rule, ensure the **Rule is Enabled** check box is selected.
6. In the Document Schema field, select the Email schema name from this list.
7. Map the metadata fields for From, To, CC, Subject, Attachments, and Date Sent to the metadata fields you created in the previous section.
8. Click **OK**.
9. To test the email settings, launch Microsoft Outlook and the FileHold Desktop Application (FDA). Login to the FDA. Open an email in Outlook so it is in full screen. From the Add-ins ribbon, click **Add to FileHold**. The metadata fields will be automatically populated based on the email content.

13.2. AUTOMATIC EXTRACTION OF METADATA VALUES FROM FILE PROPERTIES

The file properties of a file can be automatically extracted into metadata fields for a defined schema when an extraction rule for that file type is configured. Since all file types have file properties, you can extract metadata from any type of file. This is useful for file types such as images where you can extract information such as the size of the picture, the camera type, exposure time, resolution, and so on directly from the file.

The file properties that can be extracted are taken from the Details tab of the file properties which can be viewed from Microsoft Windows Explorer. These properties may vary for each file type and in operating systems such as Windows XP or Windows 7. The example below shows some of the file properties of an image file in Windows Explorer in Windows 7.



When creating extraction rules for files, you can create an extraction rule for each type of file that you want to extract data from. For example, you can set a separate rule for a docx, xlsx, pdf, jpg, tiff, and so on. You can create several extraction rules per file extension; however, only one extraction rule per file extension can be enabled at a time.

A document template is simply any file with the file type that you want to extract metadata from. The document template used will determine the type of file property extraction rule created; it is dependent on the file type such as a docx, xlsx, pdf, jpg and so forth. For example, to create a jpg file extraction rule, select a jpg file as the template.

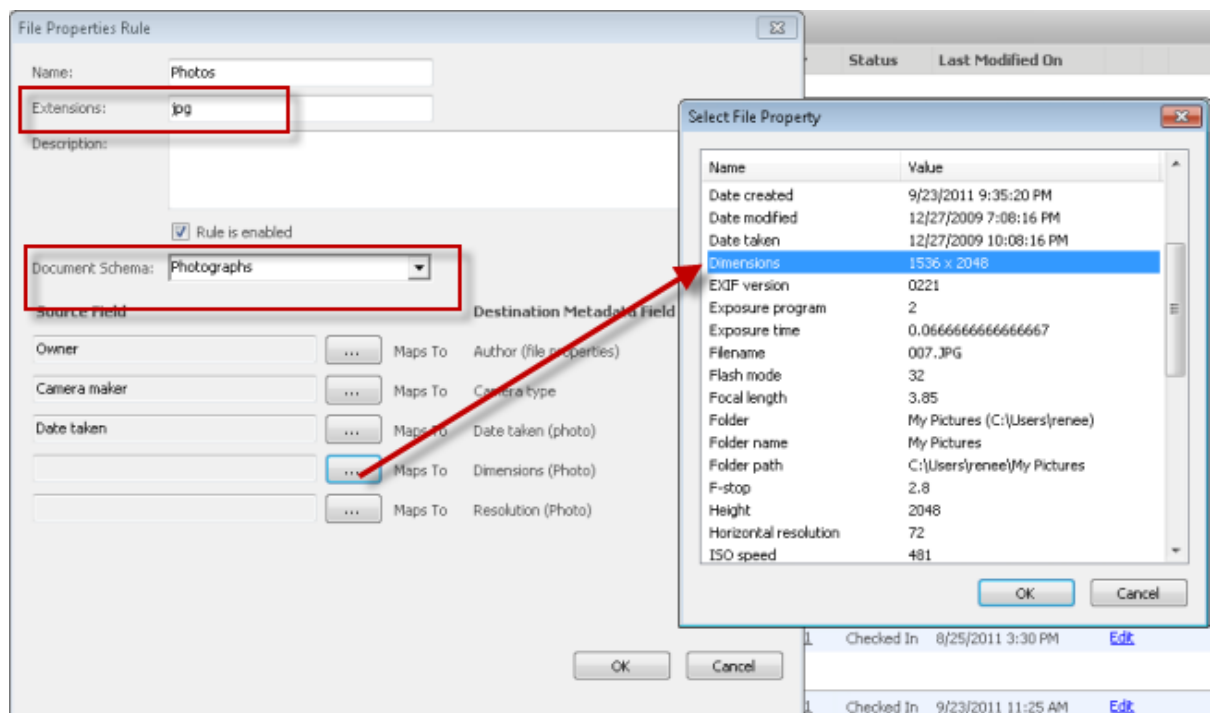
A document schema is also assigned to the rule and the metadata fields are mapped to the file properties. When a document of that type is added to FileHold using that schema then the file properties will be automatically extracted.

Only users with Library Administrator or higher permission can create extraction rules.

NOTE: There is an issue when extracting file properties into metadata fields in Microsoft Office applications using the integrated toolbar. Since Microsoft Office saves files as a temp file when you are working on documents within the application, any file properties related to the file name, location, or file type cannot be extracted when adding a document to FileHold using the FileHold toolbar. You will need to save the document, close it in the Microsoft Office application, and add the document from the FileHold Desktop Application (FDA) or Web Client.

TO CREATE A FILE PROPERTIES EXTRACTION RULE

1. Do one of the following:
 - In FileHold Desktop Application, go to **Tools > Extraction Rules**.
 - In the Web Client, go to **Administration Panel > Library configuration > Extraction Rules**.
2. Select the "template" file from your computer and click **OK**. The "template" file selected determines the type of file properties extraction rule that is created. For example, to create a rule for jpg files, select a jpg file template.
3. In the File Properties Rule window, enter a name for the rule.
4. The Extensions field is automatically filled out with the type of template file selected. For example, if the template file is a jpg file, then the extension is jpg.
5. Enter a description for the rule (optional).
6. To enable the rule, ensure the **Rule is Enabled** check box is selected.
7. In the Document Schema list, select the schema that is to be used for this rule. You may need to create a new schema.
8. Map the metadata fields to the File Properties. Click **...** to select the File Property in the Select File Property window. In the example below, an extraction rule was created for an image file (jpg) file type using the Photographs schema. The metadata fields in the Photograph schema are being mapped to the File Properties of the jpg "template" file.



9. When you have finished mapping the metadata fields to the File Properties fields, click **OK**.
10. The File Extraction rule appears in the List of Extraction Rules.

TO TEST THE FILE PROPERTIES EXTRACTION RULE

1. Log off and log back into FileHold.
2. Add a document of that file type to FileHold. For example, if you created a rule for a jpg file, add a jpg file to the system.
3. Check to make sure the file properties were extracted into the metadata fields. In the example below, a jpg file was added to the system using the Photographs schema and the mapped metadata was automatically extracted.

Metadata & File Properties

007

▼ Metadata

Type of Document *

Photographs

Format of Document *

Electronic Document

Document Name *

007

Author (file properties)

DC2008\renee

Camera type

Apple

Date taken (photo)

☒ 12/27/2009

Dimensions (Photo)

1536 x 2048

Resolution (Photo)

72

☐ Delete the local copy of this file after it has been successfully added

☐ Email notify all folder members that this document has been added to this folder

Add Save & Next Cancel

13.3. AUTOMATIC EXTRACTION OF XML NODES FROM MICROSOFT WORD CONTENT CONTROLS

You can create a "XML Node Extraction Rule" for a Microsoft Word document (e-Form) that has content controls. After the document has been properly configured, the values in the content controls can be extracted into the metadata fields when the e-Form is added to FileHold.

Using Microsoft Word 2007 or higher, you can create forms using the content controls available in Microsoft Word developer mode. FileHold will be offering e-Form creation as a professional service for a charge. Contact sales@filehold.com for more information.

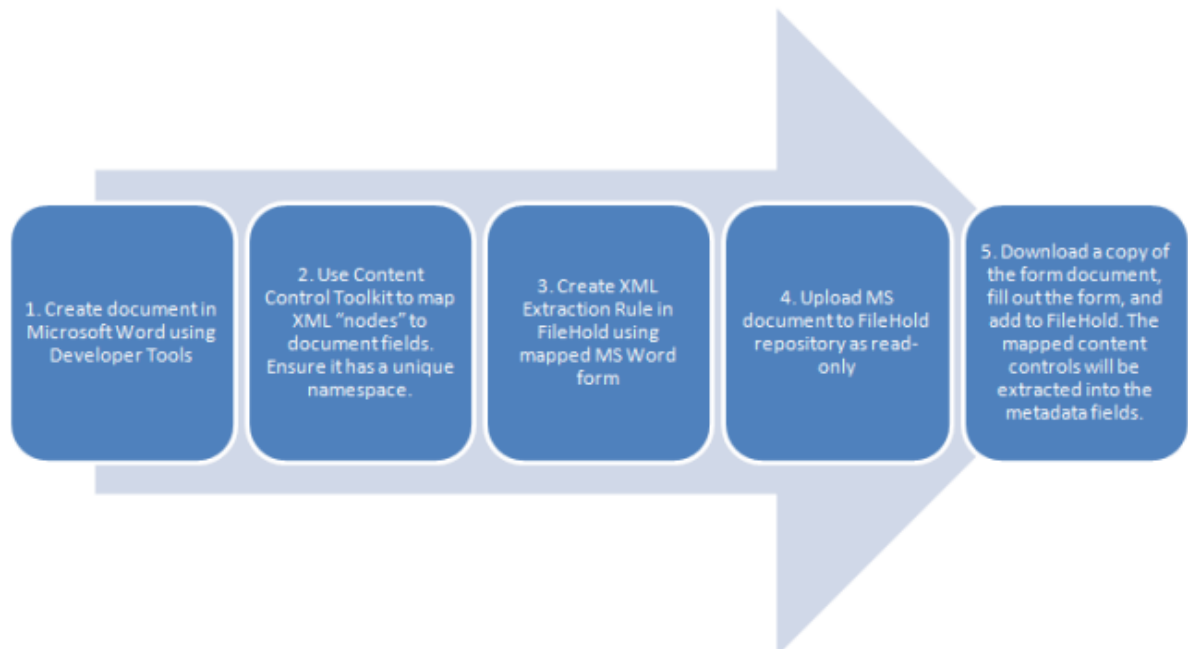
Once an e-Form is created in Microsoft Word, use the Word 2007 Content Control Toolkit to map the controls on the form to the custom XML parts. The free toolkit is made by Microsoft, is actively supported and available for download here: <http://dbe.codeplex.com/>

Once a Word form has its XML nodes mapped and given a unique namespace in the toolkit, you can then create the extraction rule in FileHold. You use the Microsoft Word e-Form that was mapped as the template.

After the extraction rule in FileHold added, the form can be used as a template available for download in FileHold. Users will get a copy of the form, fill out the form, save the form as a new file and add it to FileHold. When the form is added to FileHold, the mapped fields on the form will be automatically extracted to the metadata fields.

WARNING: XML Node Extraction should be configured by someone who is familiar with using the Developer Tools in Microsoft Word, writing XML, and the Content Control Toolkit. If you require assistance with setting this feature up, please contact sales@filehold.com for a quote.

The following are the steps to creating an XML Node extraction rule:



STEP 1: CREATE AN E-FORM IN MICROSOFT WORD USING DEVELOPER TOOLS

In the first step, you will need to create an e-Form using the Developer ribbon in Microsoft Word. Use the content controls in the e-Form fields as this is the information that will get extracted into the metadata fields of the document schema. FileHold is offering e-Form creation as a Professional Service. Contact sales@filehold.com if you would like more information on creating forms for your organization.

The following is an example of an e-Form created in Microsoft Word. You can see where the content controls are in the Invoice on the right side that says "Click here to enter text". On the Invoice on the left side, values have been entered into the content controls such as invoice

number, date, total and so on. These are the values that will be extracted into the metadata fields.

[illegible]

This help article is not going to explain how to create e-Forms using Microsoft Word. For more information on creating content controls in Microsoft Word, see the Microsoft Word online help. Be sure the document is saved as a docx.

STEP 2: USE CONTENT CONTROL TOOLKIT TO MAP "XML NODES" TO E-FORM CONTENT CONTROLS

As previously mentioned, the Microsoft Word e-Form will require some additional configuration before the values from the content controls can be extracted. After the e-Form is created, the second step is to use the Word 2007 Content Control Toolkit to map the content controls in the e-Form to the custom XML nodes created in the toolkit. The free toolkit is made by Microsoft, is actively supported and available for download here: <http://dbe.codeplex.com/>. The toolkit is a stand-alone, light-weight tool that opens any Word Open XML document (i.e. .docx) and lists all of the content controls inside of it.

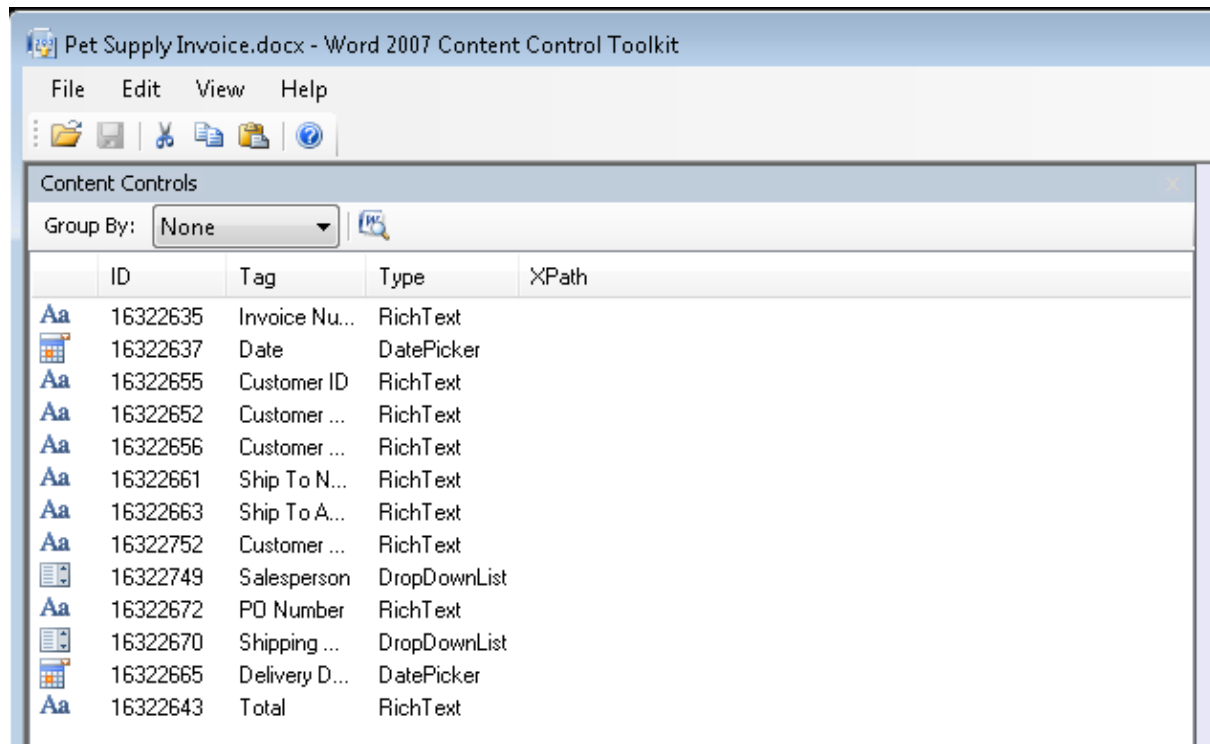
In the toolkit, a XML code is written that contains the “XML nodes” that will be mapped to the content controls on the e-form and assigned a unique namespace. The XML nodes define which content control values will be extracted to the metadata fields from the e-Form. The unique namespace is required in order to create the unique extraction rule in the document management software.

After creating the XML nodes in the XML code, the XML nodes are dragged and dropped to the content controls to "bind" the content together. Once they are "bound", the document is saved and used to create the extraction rule in the document management software.

TO MAP THE XML NODES TO THE CONTENT CONTROLS

1. Download the Content Control Toolkit from <http://dbe.codeplex.com>.

- Open the Microsoft Word e-Form you created in Step 1 in the toolkit. There is a list of all the content controls in the e-Form.

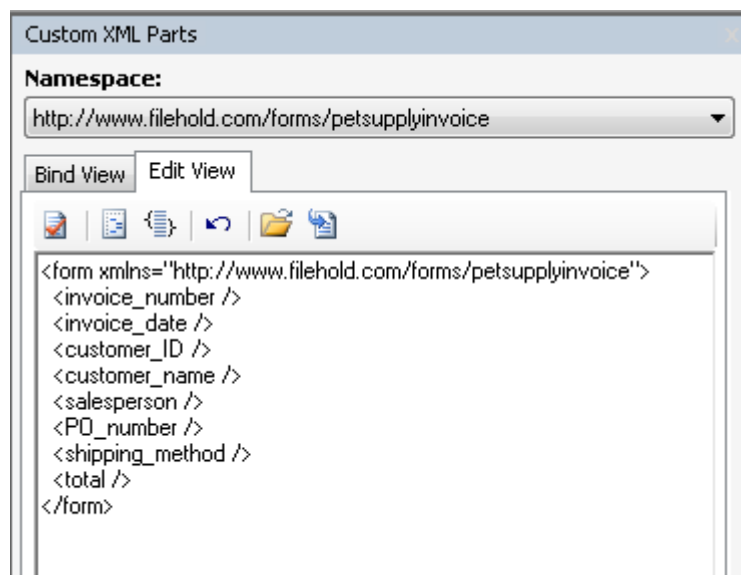


- Create an XML file that contains a unique namespace and the XML nodes that you want to bind to the content controls. The unique namespace must be unique and written in a format of:

```
<form xmlns="http://youruniquenamespace">
```

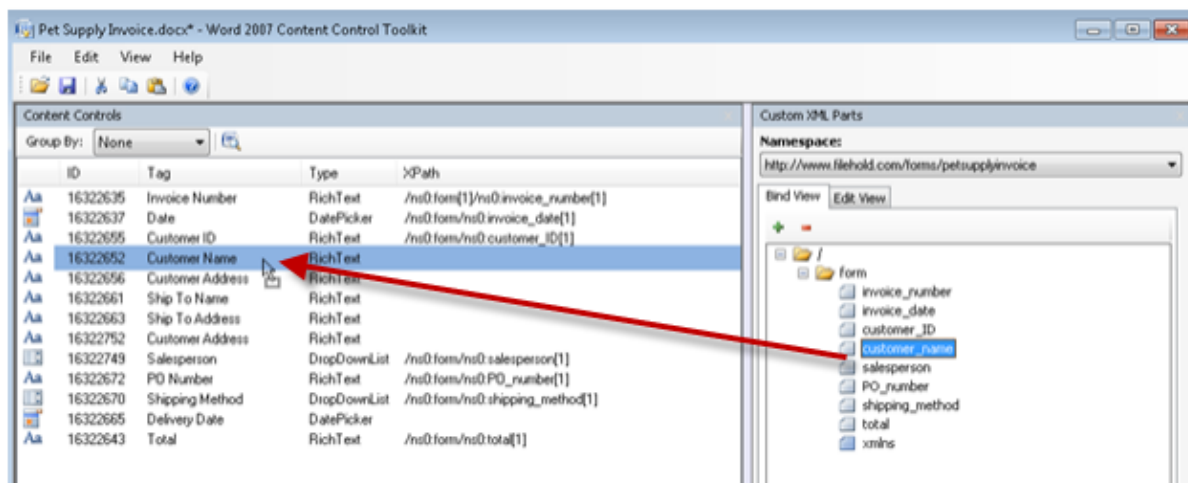
You can do this in the **Content Control Toolkit > Custom XML Parts > Edit View** tab or in another application such as Notepad and copy it over into the Edit View tab. For more information, see the Help in the Content Control Toolkit.

In the example below, the XML was written in the **Content Control Toolkit > Edit View** tab:



4. Once your XML code has been created and is valid, you can bind the content controls to the XML. Validate the XML code using the **Check Syntax** button (Checkmark button).
5. Click on the **Bind View** tab.
6. Bind the Custom XML Parts to the Content Controls by dragging and dropping the XML node to the content control. Note that you should drag and drop slowly to ensure that the items are "bound". The example below shows how to bind the XML nodes to the content controls in the Content Control Toolkit via dragging and dropping.

WARNING: This step in the process can be a bit "finicky". This is due to the Content Control Toolkit which FileHold cannot do anything about since it is a 3rd party product.



7. Save and Close the e-Form as a docx after the XML nodes have been bound to the content controls.
8. To ensure that the form has been mapped correctly, open the form again in the Content Control Toolkit.
9. In the **Namespace** area, click the down arrow to ensure there is only one namespace in the list. If there are additional namespaces, delete them.

10. Review the bound content controls and ensure the correct XML node has been mapped.
11. Save and Close the e-Form once you are sure everything is correct.

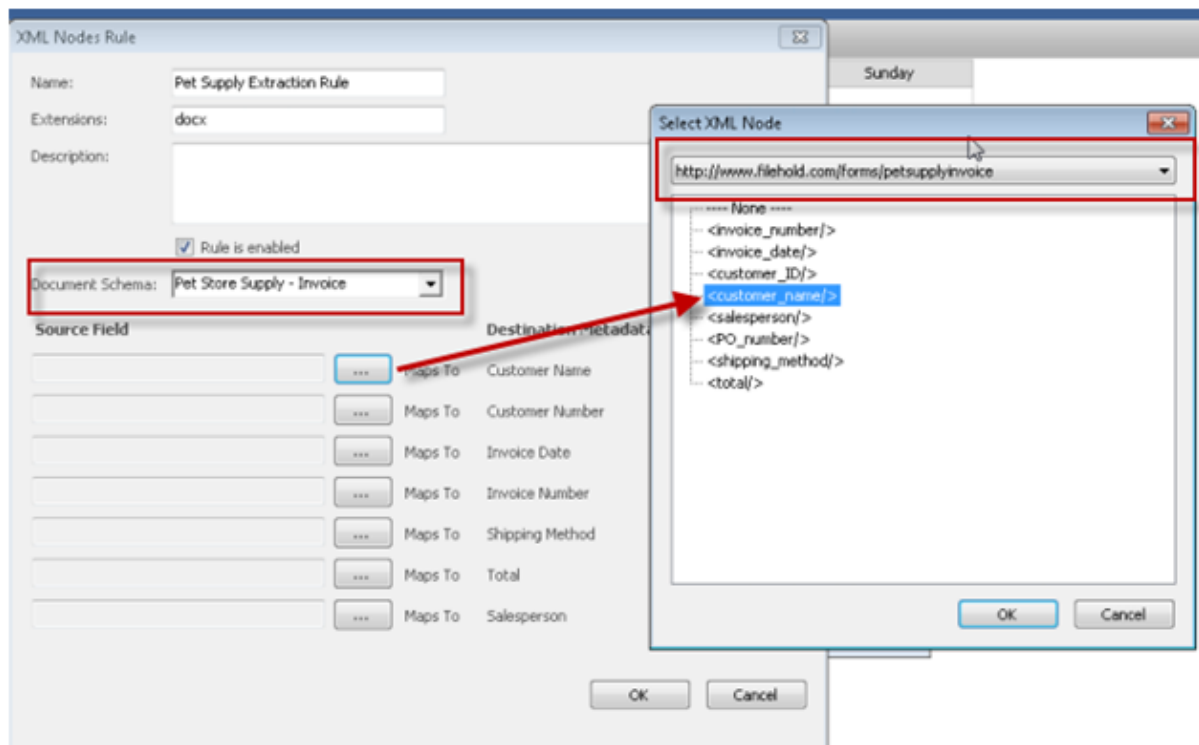
STEP 3: CREATE XML NODE EXTRACTION RULE IN FILEHOLD

The next step is to create the XML Node Extraction Rule in the document management software. When creating the rule, you will need to select the mapped Microsoft Word e-Form document as the template to create the rule from. The unique namespace that was given to the document in the Content Control Kit will allow the extraction rule to recognize that the values in that document can be extracted. Having a unique namespace allows you to create as many XML Node extraction rules for as many documents that you like as long as the namespace for each document is unique.

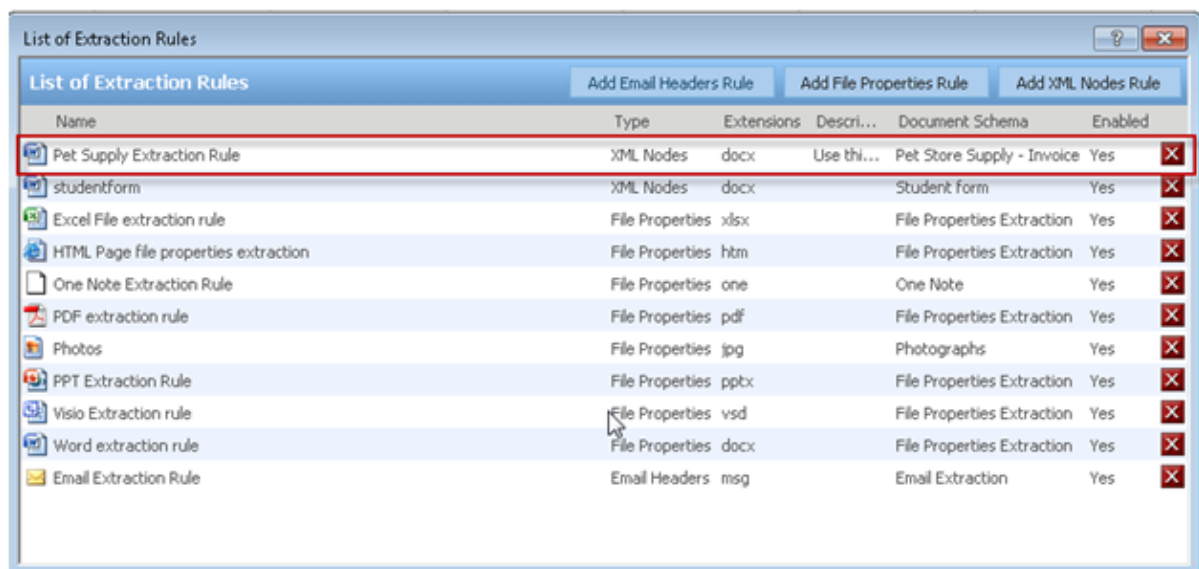
In the example, a specific schema called “Pet Store Supply – Invoice” was created to contain the metadata fields that will be extracted from the e-Form. When creating the XML Node extraction rule, you map the metadata field names in the schema to the “XML nodes” created in the Content Control Kit. Notice that the unique namespace is displayed in the Select XML Node window.

TO CREATE THE XML NODE EXTRACTION RULE

1. Do one of the following:
 - In FileHold Desktop Application, go to **Tools > Extraction Rules**.
 - In the Web Client, go to **Administration Panel > Library configuration > Extraction Rules**.
2. Click **Add XML Nodes Rule**.
3. In the Select Template File window, select the e-Form you configured in Step 2 using the Content Control Toolkit.
4. In the XML Nodes Rule window, enter a name for the rule.
5. Enter a description for the rule (optional).
6. To enable the rule, ensure the **Rule is Enabled** check box is selected.
7. In the Document Schema list, select the schema that is to be used for this rule. You may need to create a new schema.
8. Map the Source field to the Destination Metadata field. Click **...** to select the XML Node from the list. Ensure that the unique namespace is selected in the Select XML Node window. For example, map the <invoice_number /> XML node to the Invoice Number metadata field.



9. When all the fields are mapped, click **OK**.
10. The Extraction Rule will appear in the list of extraction rules.



11. ****Log off and log back into FileHold.**** Do not skip this step.

STEP 4: ADD THE FORM TO THE FILEHOLD REPOSITORY

A Library Administrator or someone with sufficient permissions can add the mapped Microsoft Word e-Form to the document management system. When the form is added to FileHold, the

rule will automatically recognize the e-form (due to the unique namespace) and the metadata fields values will be extracted from the form. This form can be set to read-only so that the form can only be downloaded by users.

STEP 5: DOWNLOAD AND FILL OUT THE E-FORM

Users can download the e-Form and fill out the information. When the filled out e-Form is added to FileHold, the rule will automatically recognize the e-Form and extract the values in the content controls into the metadata values. In the example below, the e-Form has been filled out and the contents of the content controls on the e-Form have been extracted into the corresponding metadata fields.

Metadata & File Properties

BasiePie_invoice

Metadata

Type of Document *
Pet Store Supply - Invoice

Format of Document *
Electronic Document

Document Name *
BasiePie_invoice

Customer Name *
Basie Pie

Customer Number *
4587474

Invoice Date *
09/21/2011

Invoice Number *
45639

Shipping Method *
Ground

Total *
17.89

Salesperson *
Tom Newton

☐ Delete the local copy of this file after it has been successfully added

☐ Email notify all folder members that this document has been added to this folder

Invoice

Pet Store Supply
Four cats and dogs love us!
370-4664 Inland Hwy
Burnaby BC V3C 7T5
9877-633-1202

Invoice Number: 45639
Date: 23/09/2011
Customer ID #: 4587474

Ship To:
Basie Pie
Basie's Pet Store
111 Marine Trnch
Vancouver BC V4R 3T5

SALESPERSON	PO NUMBER	SHIPPING METHOD	SHIPPING TERMS	DELIVERY DATE	PAYMENT TERMS
Tom Newton	42957	Ground		07/10/2011	Due on receipt

QTY	Item #	DESCRIPTION	UNIT PRICE	LINE TOTAL
1	4566-3455	Catnip	3.99	3.99
2	3244-9884	Kitty Litter	5.99	11.98
SUBTOTAL				15.97
SALES TAX				1.92
TOTAL				17.89

13.4. METADATA EXTRACTION FROM PDF FORMS

PDF forms contain fill-able fields which users can fill out using the free Adobe Acrobat Reader software. The values entered into the fields can be automatically extracted into the metadata fields of a schema thereby reducing the amount of time it takes to index or "tag" a document.

In order to create PDF forms, you will need software such as Adobe Acrobat Professional. You cannot create PDF forms using the FileHold document management software.

The PDF form extraction rule is created in the FileHold Desktop Application (FDA). The rule is based on the PDF form template used. Multiple PDF extraction rules can exist. This means that you can have as many PDF form extraction rules as needed. Both “classic” and Adobe XML Forms Architecture (XFA) are supported.

When mapping the fields on the PDF forms to the metadata fields in the schema, ensure that the values entered in a PDF form can be accepted into the metadata fields. For example, if the PDF form has a drop-down list and the metadata field it is mapped to is also a drop-down list, then the values of both must *match exactly*. Another example is if the value of a field in the PDF form is a text field and the metadata field it is mapped to is a numeric field, then the value of the PDF form may not populate the metadata field if there are alphabetical characters in the PDF form. To overcome these types of issues, simply make the metadata fields a text type so it can accept anything from the PDF form.

An example of a PDF form is shown below.

Invoice	
Invoice Number:	67890
Date:	2013/01/28
Order Number:	6789
Terms:	none
Company:	Basie's Pies
Address:	678 Street
State/Province:	BC
Zip/Postal code:	V5c5T5
Phone:	604-222-2222



FileHold Systems Inc
 250-4664 Lougheed Hwy
 Burnaby, BC
 Canada
 V5C 5T5
 Phone: 604-734-5653
 Fax: 111-222-4444
 www.filehold.com

TO CREATE A PDF FORM EXTRACTION RULE

12. Do one of the following:

- In FileHold Desktop Application, go to **Tools > Extraction Rules**.
- In the Web Client, go to **Administration Panel > Library configuration > Extraction Rules**.

13. In the Select Template File window, select the PDF form "template" file from your computer and click **OK**.

14. In the PDF Forms Rule window, enter a name for the rule.

15. The Extensions field is automatically filled out with the type of PDF.

16. Enter a description for the rule (optional).

17. To enable the rule, ensure the **Rule is Enabled** check box is selected.

18. In the Document Schema list, select the schema that is to be used for this rule. You may need to create a new schema.

19. Map the metadata fields to the fields on the PDF form. Click **...** to select the PDF form field.

Source Field	Destination Metadata Field
form1/InvoiceNumber	Invoice Number
form1/OrderNumber	Order #
form1/InvoiceDate	Date
form1/Company	Company (file properties)
form1/Address	Address
form1/StateProvince	State
form1/ZipCode	ZIP

20. Click **OK**.
21. ****Log off the FDA**** and log back in for the rule to take effect.
22. Test the PDF form extraction rule using the PDF form that was used as a template. Fill out the form, save it, and add it to the document management system.
23. The values entered in the form and mapped in the extraction rule will appear in the metadata pane.

Invoice_fillable_basie
This version is Checked In

Metadata

Type of Document *
Invoice

Format of Document *
Electronic Document

Document Name *
Invoice_fillable_basie

Invoice Number
67890

Order #
6789

Date
☒ 01/28/2013

Company (file properties)
Basie's Pies

Address
678 Street

Save Save & Next Cancel

INDEX

A

- ADI, 108
 - API source, 108
 - deleting jobs, 112
 - editing jobs, 112
 - enabling or disabling jobs, 113
 - extraction rules, 108
 - indirect metadata, 109, 113
 - job details, 112
 - manually run a job, 112
 - resetting jobs, 112
 - watched folder source, 108, 109
 - watched FTP site source, 108, 110
- auto-filing, 72
 - date-based, 72
 - enabling, 73, 86
 - filepathfrommd, 72
 - fixed destination, 72
 - schema-based, 72
 - schemaname-datebased, 72
 - setting, 73
- automatic document importation. *See* ADI
- Auto-Tagging, 18

C

- cabinet administrator role, 14
- cabinets
 - cloning, 20
 - copying, 19
 - creating, 16
 - deleting, 19
 - managing, 15
 - properties, 19
 - statistics, 20
- change cabinet/folder owner, 103
- change document owner, 102
- check in for user, 101
- Courier, 59
 - adding to schemas, 67
 - cloning templates, 66
 - creating templates, 60
 - deleting templates, 66
 - editing templates, 67
 - templates, 59
- custom file naming
 - custom text string, 71
 - input masks, 70
 - setting, 69

D

- database lookup, 79
- deleting
 - documents permanently, 83
- document control fields
 - creating, 33
 - enabling, 33
- document control numbers, 31, 32
- document links
 - email attachments, 85
 - settings, 83
- document publisher + delete role, 12
- document publisher role, 12
- document schemas, 4
- document URLs. *See* document links
- document usage log, 105
- documents
 - permanently deleting, 83
- drawers
 - cloning, 23
 - copying, 22
 - creating, 21
 - deleting, 24
 - managing, 20
 - moving, 22
 - properties, 22
 - statistics, 24

E

- email attachments
 - settings, 85
- email notifications
 - settings, 86
- event schedule, 29, 73
 - adding to schemas, 78
 - archive, 74
 - convert to record, 74
 - creating, 77
 - delete, 74
 - email notifications, 76
 - enabling, 77
 - setting number of user defined events, 79
 - user defined, 74
 - using custom metadata fields, 76
- extraction rules, 123
 - email, 123
 - file properties, 124
 - Outlook, 123
 - PDF forms, 134

XML node, 127

F

folder groups
 assigning to a folder, 26
 delete, 26
 edit, 26
 manage, 25
 managing, 24
 statistics, 26
 folders
 managing, 27

G

guest user role, 12

H

hard delete, 83

L

library, 4
 best practices, 6, 8
 creating, 6
 creating structure, 15
 general settings, 83
 guidelines, 9
 overview, 6
 performance considerations, 9
 permissions, 11
 sample planning guide, 6
 Library Administrator
 security role, 1
 tasks, 1
 library administrator role, 14
 library audit log, 106
 library management, 101
 change cabinet folder owner, 103
 change document owner, 102
 check in for user, 101
 recover documents, 104
 log in, 2

M

manage imports, 115
 importing files previously exported from FileHold, 118
 importing from scanning, 116
 importing previously exported files, 118
 log file, 122
 manually run, 121
 operating, 119
 QuickScan Pro, 116

metadata, 28
 adding to schemas, 43
 check box field, 37
 creating, 35
 currency field, 37
 date field, 36
 deleting, 43, 44
 drill down menu, 38
 drill drop down menu field, 36
 drop down list database, 39
 drop down list FileHold managed, 38
 drop down menu - database lookup field, 36
 drop down menu-FileHold managed field, 36
 editing, 43, 44
 importance, 35
 number field, 37
 text field, 36
 URL field, 37

O

offline documents
 version 0 switch, 30
 organizer + delete role, 13
 organizer role, 13

P

publisher + delete role, 13
 publisher role, 12

R

read-only role, 12
 recover documents, 104
 reports, 105
 document usage log, 105
 library audit log, 106
 restricting access
 FileHold, 87

S

schema membership, 28
 schemas, 28
 adding groups or users, 34
 adding workflows, 57
 auto-filing. *See* auto-filing
 creating, 29
 custom file naming, 68
 database lookup. *See* database lookup
 event schedules. *See* event schedule
 input masks for custom naming, 70
 metadata. *See* metadata
 offline documents, 30
 search engine
 errors, 93

- excluding file types, 94
- limiting fts to specific file types, 95
- managing errors, 94
- status, 91
- unindexed files, 92
- security
 - effective permissions, 5
 - file structure, 5
 - problems, 4
 - rules, 5
- Security, 4
- senior library administrator role, 14
- server side OCR
 - configuration, 88
 - OCR status, 89
 - overview, 88
- soft delete, 83
- system administrator role, 15

U

- user roles, 11

V

- version control fields
 - creating, 33

- enabling, 33
- version control numbers, 31, 32

W

- workflow, 28
 - actions on status reports, 98
 - adding to schemas, 57
 - ad-hoc workflows, 46
 - approvers, 45
 - automatically starting, 57
 - change log, 99
 - cloning templates, 56
 - configuring, 45
 - creating status reports, 97
 - creating templates, 49
 - custom naming pattern, 55
 - dashboard, 99
 - diagram, 47, 48
 - editing templates, 58
 - examples, 46
 - initiation configuration, 87
 - initiator, 45
 - observers, 45
 - participants, 45
 - reviewers, 45
 - workflow status report, 96